AX MANAGER

The next dimension of Locking System Management

AXM Plus

Handbuch

25.03.2025

Simons Voss technologies

ALLEGION

Inhaltsverzeichnis

1. Allgemeine Sicherheitshinweise ... 10
2. Produktspezifische Sicherheitshinweise ... 11
3. Bedeutung der Textformatierung ... 12
4. Bestimmungsgemäße Verwendung ... 13
5. Allgemein ... 14
6. Informationen zum Datenschutz ... 15
6.1 IT-Grundschutz ... 15
6.1.1 Welchen Schutzbedarf haben die im System verarbeiteten Daten? ... 15
6.1.2 Welche Anforderungen an die IT-Infrastruktur sind empfohlen? ... 15
6.2 Verschlüsselung ... 15
6.2.1 Sind die Daten im System 3060 verschlüsselt? ... 15
6.2.2 Welche Daten werden dabei verschlüsselt? ... 16
6.2.3 Sind die Übertragungswege z.B. per Funk auch verschlüsselt? ... 16
6.3 Datenschutzkonformes Arbeiten nach DSGVO ... 16
6.3.1 Welche personenbezogenen Daten werden in der Software gespeichert? ... 16
6.3.2 Zu welchem Zweck werden personenbezogene Daten in der Software gespeichert? ... 17
6.3.3 Wie lange werden personenbezogene Daten in der Software gespeichert? ... 17
6.3.4 Kann das Leserecht von Zutrittslisten zusätzlich gesichert werden? ... 17
6.3.5 Sind personenbezogene Daten in der Software vor dem Zugriff Dritter geschützt? ... 17
6.3.6 Können die gespeicherten Daten als Kopie zur Verfügung gestellt werden? ... 18
6.3.7 Können personenbezogene Daten aus der Software gelöscht werden? ... 18
7. Funktionsumfang AXM Plus ... 19
8. Systemvoraussetzungen ... 21
8.1 AXM-Dienste und verwendete Ports ... 21
9. Versionshinweise ... 22
9.1 Version 2.0.24303.0902 ... 22
9.2 Version 2.0.25083.0801 ... 22
10. Installation ... 24
10.1 AXM als Administrator ausführen (empfohlen) ... 25
10.2 AXM aktualisieren ... 28

11. Erste Schritte nach der Installation ... 30
11.1 Best Practice: Schließanlage aufbauen ... 32
11.2 Best Practice: AX2Go einrichten ... 33
11.3 Best Practice: Schutz der Datenbank ... 33
12. Registrierung ... 34
12.1 Registrierung als Testversion ... 34
12.2 Registrierung mit Lizenz ... 39
12.3 Aktualisieren Ihrer Lizenz ... 45
13. Aufbau der AXM ... 46
13.1 Sortieren und Filtern ... 49
13.2 Assistenten ... 51
13.3 Mehrere Möglichkeiten, gleiches Ergebnis ... 51
13.4 Globale Suche ... 52
13.5 Effizienter arbeiten mit der AXM ... 53
13.5.1 Tab-Bedienung ... 53
13.5.2 Hotkeys ... 53
13.5.3 Weitere Objekte erstellen ... 54
14. Organisationsstruktur ... 55
14.1 Berechtigungsgruppen erstellen ... 55
14.2 Personengruppe erstellen ... 56
14.3 Zeitplan erstellen ... 58
14.4 Zeitgruppe erstellen ... 61
14.5 Zeitgruppe löschen ... 66
14.6 Zeitpläne löschen ... 69
14.7 Zeitumschaltung erstellen ... 71
14.8 Feiertage erstellen und bearbeiten ... 74
14.9 Feiertagslisten erstellen und bearbeiten ... 78
14.10 Standort erstellen ... 83
14.11 Gebäude erstellen und zu Standort zuweisen ... 86
14.12 Bereich erstellen ... 89
14.13 Hashtag erstellen ... 91
15. Personen und Identmedien ... 94
15.1 Identmedien erstellen ... 94
15.1.1 Transponder und Karten erstellen ... 95
15.1.2 PinCode-Tastaturen erstellen ... 102
15.1.3 Spezielle Identmedien erstellen ... 108

15.1.4 AX2Go-Schlüssel erstellen ... 113
15.2 Identmedium duplizieren (inkl. Berechtigungen und Einstellungen) ... 113
15.3 Identmedium löschen ... 115
15.3.1 Transponder/Karte löschen ... 115
15.3.2 PIN löschen (PinCode-Tastatur AX) ... 120
15.3.3 AX2Go-Schlüssel sperren ... 121
15.4 Identmedium doppelt so lange öffnen lassen ... 121
15.5 Für ein Identmedium alle Schließungen stummschalten ... 123
15.5.1 Für einen Transponder oder eine Karte alle Schließungen stummschalten ... 123
15.5.2 Für einen AX2Go-Schlüssel alle Schließungen stummschalten ... 124
15.6 Zugänge durch Identmedium mitschreiben lassen (Begehungsliste) ... 125
15.7 Berechtigungen des Identmediums auf bestimmte Zeiten beschränken (Zeitgruppe) ... 126
15.8 Identmedium einmalig an bestimmten Zeitpunkten aktivieren oder deaktivieren (Aktivierungs- und Verfallsdatum) ... 126
15.9 Defekte Identmedien behandeln ... 130
15.9.1 Instandsetzen/neu synchronisieren ... 134
15.9.2 Zurücksetzen und austauschen ... 139
15.9.3 Löschen und austauschen ... 142
15.9.4 Außer Betrieb nehmen und in Projekt lassen ... 150
15.9.5 Außer Betrieb nehmen und aus Projekt löschen ... 157
15.10 Vergessenes Identmedium temporär duplizieren ... 163
15.10.1 Vergessenen Transponder oder vergessene Karte temporär duplizieren ... 163
15.11 Verlorenes/gestohlenes Identmedium dauerhaft sperren ... 168
15.11.1 Verlorenen/gestohlenen Transponder/Karte dauerhaft sperren und austauschen ... 169
15.11.2 Verlorene/gestohlene PinCode-Tastatur dauerhaft sperren ... 174
15.12 Zurückgegebenes Identmedium vermerken und zurücksetzen (wieder ins Inventar) ... 179
15.12.1 Zurückgegebenen Transponder/Karte vermerken und zurücksetzen (wieder ins Inventar) ... 179
15.13 Identmediums-Verwaltungsaufgaben planen und nachverfolgen ... 182
15.13.1 Ausgabedatum notieren ... 183
15.13.2 Batteriewechsel planen und protokollieren ... 186
15.13.3 Rückgabe planen und protokollieren ... 191
15.14 Identmedium oder Schließung in der Matrix wiederfinden ... 194
15.15 Identmedien als Liste exportieren ... 195
15.15.1 AX2Go-Schlüssel/Transponder/Karten als Liste exportieren ... 195
15.15.2 PINs und PinCode-Tastaturen als Liste exportieren ... 197
15.16 Seriennummer und/oder TID eines Identmediums einsehen ... 198

15.16.1 Seriennummer und TID eines Transponders/Karte einsehen ... 198
15.16.2 Seriennummer einer PinCode-Tastatur einsehen ... 200
15.17 Personen zu Personengruppen zuordnen ... 202
15.17.1 Einzelne Person/Identmedium zu Personengruppe zuordnen (im Transponder-Fenster) ... 203
15.17.2 Mehrere Personen/Identmedien zu Personengruppe zuordnen (im Personengruppen-Fenster) ... 205
15.18 Identmedium in mehreren Schließanlagen verwenden ... 209
15.18.1 Identmedium im gleichen Projekt wiederverwenden ... 212
15.18.2 Identmedium in anderen Projekten/Datenbanken wiederverwenden ... 217
15.19 Verwaltung von AX2Go-Schlüsseln ... 220
15.19.1 Vergabe von Schlüsseln ab AXM Plus ... 220
15.19.2 AX2Go-Schlüssel sperren ... 227
15.19.3 AX2Go-Schlüssel löschen ... 231
15.20 PIN-Länge einstellen (PinCode AX) ... 233
15.21 PIN ändern (PinCode AX) ... 236
16. Türen und Schließungen ... 238
16.1 Schließung erstellen ... 238
16.2 Schließung duplizieren (inkl. Berechtigungen und Einstellungen) ... 248
16.3 Schließung löschen ... 250
16.3.1 Einzelne Schließung über die Matrix löschen ... 251
16.3.2 Mehrere Schließungen über den Tab löschen ... 252
16.4 Schließungstyp nachträglich ändern ... 255
16.5 Defekte Schließungen behandeln ... 257
16.5.1 Neu synchronisieren (Instandsetzen) ... 262
16.5.2 Zurücksetzen und austauschen ... 264
16.5.3 Löschen und austauschen ... 268
16.5.4 Zurücksetzen ... 273
16.5.5 Bereinigen (nur in Datenbank zurücksetzen / Software-Reset) ... 275
16.6 Schließungen zu Gebäuden/Standorten zuordnen ... 277
16.7 Schließungen in Bereiche verschieben ... 279
16.7.1 Einzelne Schließung einem anderen Bereich zuordnen (im Fenster der Schließung) ... 281
16.7.2 Mehrere Schließungen einem anderen Bereich zuordnen (im Bereichsfenster) ... 282
16.8 Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) ... 286
16.9 Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln ... 287
16.10 Zugänge durch Schließung protokollieren lassen (Zutrittsliste) ... 293
16.11 Schließung länger, kürzer oder dauerhaft öffnen lassen ... 295

16.12 Lesereichweite der Schließung begrenzen (Nahbereichsmodus) ... 297
16.13 Schließung stummschalten (für Batteriewarnungen und Programmierungen) ... 298
16.14 Kartenleser aktivieren und deaktivieren ... 300
16.15 Aktivierungs- und Verfallsdatum von Identmedien ignorieren ... 302
16.16 Türüberwachung (DoorMonitoring) einrichten ... 303
16.16.1 DoorMonitoring für Schließzylinder einrichten ... 304
16.17 SmartRelais-Einstellungen ändern ... 310
16.17.1 Interne und externe Antenne gleichzeitig verwenden ... 312
16.17.2 Ausgänge invertieren ... 313
16.17.3 Serielle Schnittstelle verwenden ... 314
16.17.4 Signalisierung ändern ... 315
16.18 Schließungs-Verwaltungsaufgaben planen und nachverfolgen ... 316
16.18.1 Einbau-, Austausch- oder Ausbaudatum notieren ... 318
16.18.2 Batteriewechsel planen und protokollieren ... 320
16.19 Alle Schließungen eines Projekts anzeigen ... 322
16.20 Schließungen als Liste exportieren ... 324

17. Berechtigungen ... 327
17.1 Einzelne Berechtigungen ändern (Kreuz) ... 327
17.2 Viele Berechtigungen ändern (an Identmedien und/oder Schließungen) ... 328
17.2.1 Alle zulassen oder alle sperren ... 328
17.2.2 Berechtigungsgruppen ... 332
17.2.3 Berechtigungen zeitlich steuern (Zeitpläne) ... 348
17.3 Bedeutung der Berechtigungskreuze in der Matrix ... 358

18. Schließanlagen ... 360
18.1 Schließanlage erstellen ... 360
18.1.1 Kartenkonfiguration anlegen ... 365
18.2 Schließanlagenpasswort ändern ... 395
18.3 Schließanlage wechseln ... 399
18.4 Karten bzw. Transponder freischalten ... 401
18.5 Übergreifende Schließebene verwenden ... 405
18.5.1 Übergreifende Schließebene erstellen ... 405
18.5.2 Transponder für übergreifende Schließebene erstellen ... 410
18.5.3 Transponder mit übergreifender Schließebene berechtigen ... 413

19. Synchronisierung: Abgleich zwischen Schließplan und Realität ... 415
19.1 Schließung synchronisieren (inkl. Zutrittsliste auslesen) ... 416
19.1.1 Schließungsausstattung und -zustand anzeigen ... 419
19.1.2 Zutrittsliste einer Schließung anzeigen und exportieren ... 421
19.2 Unbekannte Schließung erkennen ... 423

19.3 Schließung zurücksetzen ... 425
19.4 Identmedium synchronisieren ... 427
19.4.1 Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) ... 428
19.4.2 PinCode-Tastatur synchronisieren ... 433
19.4.3 AX2Go-Schlüssel synchronisieren ... 436
19.5 Unbekanntes Identmedium erkennen ... 438
19.5.1 Unbekannte Transponder/Karten erkennen ... 438
19.5.2 Unbekannte PinCode-Tastatur erkennen ... 440
19.6 Identmedien zurücksetzen ... 443
19.6.1 Transponder/Karten zurücksetzen ... 443
19.6.2 PinCode-Tastatur zurücksetzen ... 446
19.7 Angeschlossene/unterstützte Programmiergeräte anzeigen ... 449
19.8 Verbindung zwischen Datenbank und Cloud überprüfen ... 451

20. Ihre individuelle AXM-Oberfläche ... 452
20.1 Türen und Personen in der Matrix vertauschen (transponieren) ... 452
20.2 Spalten und Zeilen in der Matrix hervorheben (Fadenkreuz aktivieren/deaktivieren) ... 453
20.3 Klick für Berechtigungen ändern ... 454
20.4 Deaktivierte und defekte Identmedien ausblenden ... 456
20.5 Spalten/Zeilen in der Matrix einblenden oder ausblenden ... 457
20.6 Zutrittsliste/Begehungsliste während der Synchronisierung auslesen ... 459
20.7 Anzahl der Einträge der Zutrittsliste in der Datenbank begrenzen ... 460
20.8 Tabs pinnen ... 461
20.9 Automatische Nummerierung ändern ... 463
20.10 Sprache ändern ... 465
20.11 Berichte und Exporte personalisieren ... 465
20.12 Erzeugte Berichte nicht automatisch öffnen ... 468
20.13 Eigenschaften für Personendetails personalisieren ... 469
20.13.1 Vorhandene Felder ausblenden und einblenden ... 470
20.13.2 Eigene Felder anlegen ... 475

21. Administrative Aufgaben ... 485
21.1 Backup erstellen ... 485
21.2 Backup wiederherstellen ... 488
21.3 Fehler-Protokolle exportieren ... 489
21.4 Versionsnummer und Lizenzschlüssel der installierten AXM anzeigen ... 490
21.5 Benutzer-Management ... 492
21.5.1 Benutzerkennwort ändern ... 492

21.5.2 Kennwortsicherheit erhöhen ... 494
21.5.3 Person zu AXM-Benutzer ernennen ... 498
21.5.4 AXM-Benutzern Aufgaben/Benutzerrollen zuweisen ... 500
21.6 AX2Go-Einstellungen ... 507

22. Statistiken und Protokolle ... 511

22.1 Zutrittsliste einer Schließung anzeigen und exportieren ... 511
22.2 Begehungsliste für Transponder/Karten anzeigen und exportieren ... 513
22.3 Türen anzeigen, an denen ein bestimmtes Identmedium berechtigt ist ... 515
22.4 Identmedien anzeigen, die an einer bestimmten Tür berechtigt sind ... 516
22.5 Ausstattungsmerkmale einer Schließung anzeigen ... 517
22.6 Statistiken und Warnungen anzeigen (Dashboard) ... 518
22.7 Aktivitäten an der Datenbank nachverfolgen (Protokoll) ... 520
22.7.1 Archivierungsdauer des Protokolls einstellen ... 522
22.8 Berichte ... 523
22.8.1 Bericht zur Identmedien-Ausgabe ausgeben ... 524
22.8.2 Datenschutzbericht (DSGVO) ausgeben ... 527

23. Hintergrundwissen und Erklärungen ... 532

23.1 Identmedien, Schließungen und der Schließplan ... 532
23.1.1 PinCode G1 vs. PinCode AX ... 534
23.1.2 AX2Go ... 537
23.1.3 Spezielle Identmedien und deren Funktionen ... 540
23.2 Schließanlagen ... 541
23.3 Übergreifende Schließebenen ... 543
23.4 "Einkuppeln", "Öffnen", "Verriegeln" usw. ... 544
23.5 Synchronisierung von Datenbank und Realität ... 546
23.6 Begehungs- und Zutrittslisten ... 547
23.7 Zeitmanagement ... 548
23.7.1 Zeitgruppen und Zeitpläne ... 548
23.7.2 Zeitumschaltungen ... 552
23.7.3 Zeitbudget (AX2Go und virtuelles Netzwerk) ... 560
23.8 Berechtigungsgruppen ... 564
23.9 Personengruppen ... 565
23.10 Verwendete Passwörter ... 567
23.11 Gebäude und Standorte ... 568
23.12 Bereiche ... 569
23.13 Hashtags ... 570
23.14 DoorMonitoring ... 570

23.14.1 Mögliche DoorMonitoring-Zustände Schließzylinder ... 571
23.14.2 Mögliche DoorMonitoring-Zustände SmartHandle ... 571
23.14.3 Mögliche DoorMonitoring-Zustände SmartRelais 3 ... 571
23.15 Berichte ... 572
23.15.1 Skalierung der Bilddateien ... 572
23.16 Karten und Schließungs-IDs ... 573
23.16.1 Kartentemplates ... 577
24. Hilfe und weitere Informationen ... 579

1. Allgemeine Sicherheitshinweise

Signalwort: Mögliche unmittelbare Auswirkungen bei Nichtbeachtung
WARNUNG: Tod oder schwere Verletzung (möglich, aber unwahrscheinlich)
ACHTUNG: Sachschäden oder Fehlfunktionen
HINWEIS: Geringe oder keine

WARNUNG

Versperrter Zugang

Durch fehlerhaft montierte und/oder programmierte Komponenten kann der Zutritt durch eine Tür versperrt bleiben. Für Folgen eines versperrten Zutritts wie Zugang zu verletzten oder gefährdeten Personen, Sachschäden oder anderen Schäden haftet die SimonsVoss Technologies GmbH nicht!

Versperrter Zugang durch Manipulation des Produkts

Wenn Sie das Produkt eigenmächtig verändern, dann können Fehlfunktionen auftreten und der Zugang durch eine Tür versperrt werden.

- Verändern Sie das Produkt nur bei Bedarf und nur in der Dokumentation beschriebenen Art und Weise.

HINWEIS

Bestimmungsgemäßer Gebrauch

SimonsVoss-Produkte sind ausschließlich für das Öffnen und Schließen von Türen und vergleichbaren Gegenständen bestimmt.

- Verwenden Sie SimonsVoss-Produkte nicht für andere Zwecke.

Qualifikationen erforderlich

Die Installation und Inbetriebnahme setzt Fachkenntnisse voraus.

- Nur geschultes Fachpersonal darf das Produkt installieren und in Betrieb nehmen.

Änderungen bzw. technische Weiterentwicklungen können nicht ausgeschlossen und ohne Ankündigung umgesetzt werden.

Die deutsche Sprachfassung ist die Originalbetriebsanleitung. Andere Sprachen (Abfassung in der Vertragssprache) sind Übersetzungen der Originalbetriebsanleitung.

Lesen Sie alle Anweisungen zur Installation, zum Einbau und zur Inbetriebnahme und befolgen Sie diese. Geben Sie diese Anweisungen und jegliche Anweisungen zur Wartung an den Benutzer weiter.

2. Produktspezifische Sicherheitshinweise

ACHTUNG

Änderungen in der Schließanlage erst nach Synchronisierung wirksam

Wenn Sie die Schließanlage mit der AXM Plus bearbeiten, dann sind die Änderungen zunächst nur in Ihrer Datenbank gespeichert.

Ihre realen Komponenten erfahren von diesen Änderungen erst mit einer Synchronisierung.

1. Prüfen Sie die Komponenten in der Matrix regelmäßig auf Synchronisierungsbedarf (siehe *Aufbau der AXM [▸ 46]*).
2. Führen Sie insbesondere bei kritischen Vorfällen (z.B. Identmedium verloren) sofort nach der Reaktion auf den Vorfall eine Synchronisierung durch (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*).

3. Bedeutung der Textformatierung

Diese Dokumentation verwendet Textformatierung und Gestaltungselemente, um das Verständnis zu erleichtern. Die Tabelle erklärt die Bedeutung möglicher Textformatierungen:

Beispiel	Schaltfläche
☑ Beispiel ☐ Beispiel	Checkbox
◉ Beispiel	Option
[Beispiel]	Registerkarte/Tab
"Beispiel"	Name eines angezeigten Fensters
| Beispiel |	Obere Programmleiste
Beispiel	Eintrag in der ausgeklappten oberen Programmleiste
Beispiel	Kontexmenü-Eintrag
▼ Beispiel	Name eines Dropdown-Menüs
"Beispiel"	Auswahlmöglichkeit in einem Drop-down-Menü
"Beispiel"	Bereich
Beispiel	Feld
Beispiel	Name eines (Windows-)Dienstes
Beispiel	Befehle (z.B. Windows-CMD-Befehle)
`Beispiel`	Datenbank-Eintrag
[Beispiel]	MobileKey-Typauswahl

4. Bestimmungsgemäße Verwendung

Der AX Manager Plus (AXM Plus) ist eine Software für die übersichtliche Schließanlagenverwaltung. Diese vereinfacht die Administration und Steuerung der Schließkomponenten und Berechtigungen im System 3060. Große und komplexe Schließanlagen können mithilfe der SQL-Datenbank einfach gepflegt werden.

5. Allgemein

Der AX-Manager, kurz AXM, tritt die Nachfolge der bewährten LSM an.

Eine völlig neue, intuitive und übersichtliche Bedienoberfläche erleichtert die Arbeit mit allen unterstützten Komponenten (siehe Funktionsumfang).

Neu in der AXM

Im Vergleich zur LSM bringt die AXM wesentliche Neuerungen:

- Microsoft SQL-Datenbank als weit verbeiteter Unterbau für Datenbanken
- Zukunftsfähige Bedienung durch Touchscreen-Optimierung
- Einfaches Arbeiten durch benutzerfreundliche Assistenten
- Berechtigungsgruppen: Sammelbecken für Identmedien und Schließungen. Alle enthaltenen Identmedien sind an allen enthaltenen Schließungen berechtigt.
- Alles im Blick: Globale Suche in der gesamten Software

Plus Edition

Mit der Plus Edition betreten wir nun die nächste Dimension der Schließanlagenverwaltung. Es handelt sich dabei um eine Edition mit ausgesuchten Funktionen (vg. LSM Basic Online).

Ihnen stehen 64.000 Schließungen und 64.000 Identmedien (Transponder/Karten) pro Schließanlage zur Verfügung.

6. Informationen zum Datenschutz

6.1 IT-Grundschutz

6.1.1 Welchen Schutzbedarf haben die im System verarbeiteten Daten?

Generell werden in der Software nur unkritische Daten mit sog. normalem Schutzbedarf verarbeitet und gespeichert. Also Daten, bei deren hypothetischem Verlust weder der Ruf einer Person noch das Image eines Unternehmens geschädigt wird. Auch ein hoher finanzieller Schaden ist nicht zu erwarten.

6.1.2 Welche Anforderungen an die IT-Infrastruktur sind empfohlen?

Daher ist der IT-Grundschutz laut Bundesamt für Sicherheit in der Informationstechnik (BSI) für eine SimonsVoss Schließanlage als Sicherheitskonzept ausreichend und gilt als empfohlene Mindestanforderung an Ihre IT-Infrastruktur.

6.2 Verschlüsselung

6.2.1 Sind die Daten im System 3060 verschlüsselt?

Ja. Innerhalb der systemeigenen Kommunikation sind Datenpakete End-to-End verschlüsselt. Es kommen mehrstufige Datenschutzmethoden zum Einsatz, welche wir in letzter Instanz mit Standard-Verschlüsselungsverfahren (AES, 3DES) sichern. Mit den neuesten Versionen unserer Produkte erhöhen Sie den Grad der Sicherheit, da diese stets dem aktuellen Stand der Technik entsprechen..

HINWEIS

Schließanlagenpasswort als Teil des Sicherheitskonzepts

Das von Ihnen vergebene Schließanlagenpasswort (nicht Benutzer) ist Teil des gesamten Sicherheitskonzepts. Mit einem komplexen Passwort erhöhen Sie automatisch auch die Schlüssellänge des verwendeten Verschlüsselungsverfahrens und somit die Sicherheit Ihrer Daten. Wir empfehlen dabei mindestens 12 Zeichen und die Verwendung von Ziffern, Klein-, Groß- und Sonderzeichen. Bitte verwahren Sie das Schließanlagenpasswort an einem sicheren Ort (z.B. Safe), zu dem nur befugte Personen Zugang haben.

6.2.2 Welche Daten werden dabei verschlüsselt?

Innerhalb der systemeigenen Kommunikation werden keine personenbezogene Daten verarbeitet, sondern mit Hilfe von Identifikationsnummern pseudonymisiert. Auch ohne Verschlüsselung ist keine Zuordnung zu einer realen Person möglich.

6.2.3 Sind die Übertragungswege z.B. per Funk auch verschlüsselt?

Nein. Dank der konsequenten End-to-End Verschlüsselung kann unsere sichere Kommunikation unabhängig vom Übertragungsweg erfolgen. Abgefangenen Daten können ohne den dazu passenden, geheimen Schlüssel nicht gelesen werden. Mit der End-to-End Verschlüsselung können systemeigene Übertragungswege ohne Leistungsverluste genutzt werden.

6.3 Datenschutzkonformes Arbeiten nach DSGVO

6.3.1 Welche personenbezogenen Daten werden in der Software gespeichert?

Es besteht die Möglichkeit folgende Daten einer Person in der Software zu speichern:

- Vorname
- Nachname*
- Titel
- Adresse
- Telefon
- E-Mail
- Personalnummer*
- Benutzername
- Abteilung
- Ort/Gebäude
- Eingestellt von/bis
- Geburtsdatum
- Kostenstelle
- Foto

Davon sind nur Nachname und Personalnummer sogenannte *Pflichtfelder und bei der Verwendung der Software erforderlich.

Besonders sensible Kategorien personenbezogener Daten nach Art. 9 DSGVO werden nicht gespeichert.

6.3.2 Zu welchem Zweck werden personenbezogene Daten in der Software gespeichert?

Um die Funktionen einer elektronischen Schließanlage vollumfänglich nutzen zu können, ist es notwendig die verwendeten Identifikationsmedien (z. B. Transponder) einem bestimmten Nutzer (z. B. Mitarbeiter) zuordnen zu können.

6.3.3 Wie lange werden personenbezogene Daten in der Software gespeichert?

Die Daten werden mindestens über die Dauer der Inbesitznahme eines Identifikationsmediums innerhalb der Schließanlage gespeichert (z. B. Firmenzugehörigkeit).

Die Dauer der Speicherung von Daten (z. B. in Protokollen und Zutrittslisten) kann vom Schließanlagenverwalter verändert und an betriebliche Vorgaben angepasst werden.

6.3.4 Kann das Leserecht von Zutrittslisten zusätzlich gesichert werden?

Bei Verwendung der optionalen ZK-Funktion in unseren Schließkomponenten, kann der Zugriff auf die damit erhobenen Daten mit erhöhten Benutzerrechten ausgestattet werden.

Beispiel: Es wird ein separater Benutzer für den Betriebsrat angelegt. Nur dieser Benutzer erhält Leserechte auf die Zutrittslisten im Verdachtsfall. Zusätzlich kann dieser Benutzer mit einem geteilten Passwort geschützt werden. 2 oder mehr Personen des Betriebsrats ist jeweils nur ein Teil des Passworts bekannt.

6.3.5 Sind personenbezogene Daten in der Software vor dem Zugriff Dritter geschützt?

Grundsätzlich ist der Nutzer (Endkunde) der Schließanlage und der Software für die Verwaltung und Sicherstellung der Zugriffsrechte verantwortlich.

Im Schließsystem selbst, werden alle Daten über ein mehrstufiges Verschlüsselungsverfahren gesichert. Ein Öffnen der grafischen Benutzeroberfläche, um auf die Daten zugreifen zu können, ist ohne Passwort und entsprechende Benutzerrechte nicht möglich.

Eine automatische Übermittlung an Dritte, eine Nutzung oder Verarbeitung durch SimonsVoss findet im Rahmen des Geschäftsbetriebes nicht statt.

6.3.6 Können die gespeicherten Daten als Kopie zur Verfügung gestellt werden?

Alle gesammelten Daten zu einer betroffenen Person können (ab Version 3.4), entsprechende Benutzerrechte vorausgesetzt, per Exportfunktion als Kopie durch den Kunden (z.B. im Rahmen eines Audits) zur Verfügung gestellt werden. Dies ermöglicht dem Kunden die Erfüllung des Auskunftsrechts nach Art. 15 DSGVO Absatz 3.

6.3.7 Können personenbezogene Daten aus der Software gelöscht werden?

Personenbezogene Daten können durch den Kunden auf Verlangen einer betroffenen Person nach Art. 17 DSGVO aus der Software (ab Version 3.4 SP1) und der dazugehörigen Datenbank endgültig gelöscht werden.

7. Funktionsumfang AXM Plus

Projekte/Schließanlagen	Mehrere Projekte mit mehreren Schließanlagen
Benutzer	Zwei Benutzer (Admin/AdminAL)
Anzahl Schließungen	64.000 pro Schließanlage
Anzahl Identmedien	64.000 pro Schließanlage
Unterstützte Schließungen und Identmedien	▪ G2-Komponenten ▪ AX-Komponenten
	▪ Digital Cylinder AX ▪ Schließzylinder 3061 ▪ SmartHandle AX ▪ SmartHandle 3062 ▪ SmartRelais 3063 (G2) ▪ SmartRelais 2 3063 ▪ Vorhängeschloss ▪ Padlock AX ▪ SmartLocker AX ▪ Möbelschloss (G2) ▪ AX2Go
Programmiergeräte	▪ SmartCD.G2/SmartCD2.G2 ▪ SmartCD.MP ▪ SmartStick AX

Webdienste	▪ Registrierung ▪ AX2Go-Invites ▪ Cloud-Dienste (nur Datenübertragung, end-to-end-verschlüsselt)

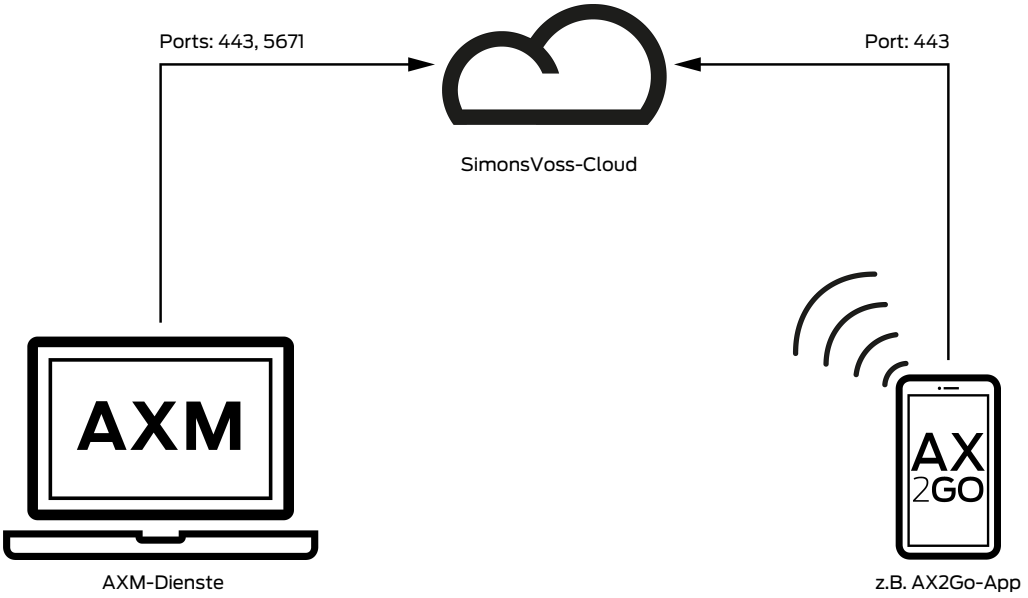
Wenn Sie an die Grenze Ihrer Version stoßen, dann können Sie jederzeit upgraden.

8. Systemvoraussetzungen

AXM Plus

Betriebssystem	Windows 10 Windows 11
Prozessor	2,66 GHz oder schneller (Intel, AMD) Keine Unterstützung von ARM-Prozessoren im System 3060
Arbeitsspeicher	4 GB oder mehr
Freier Speicher	500 MB (physisch), während der Installation ca. 1 GB
Display	13 Zoll (≈ 33 cm) oder mehr 1280×1024 oder mehr
Unterstützte MS-SQL-Edition	SQL Server Express Local DB

8.1 AXM-Dienste und verwendete Ports



Port	Funktion
443	HTTPS-Datenübertragung (Standard-Internetverbindung)
5671	Identifizierung (falls nicht verfügbar, wird auf Port 443 ausgewichen)

9. Versionshinweise

9.1 Version 2.0.24303.0902

Freigegeben am 30.11.2024

Verbesserungen

1. Ende der Public Preview und allgemeine Verfügbarkeit

9.2 Version 2.0.25083.0801

Freigegeben am 24.03.2025

Komponente	Datei	Version
GUI Version	AXM.exe	2.0.24346.0301
Platform Version	Axm.Server.Api.exe	2.0.24346.0501
SVDriver	AXWDrv.dll	7.63.0
SVDriver for AX2Go	AXWDrv_V3.dll	8.24.0.3

Verbesserungen

1. Optimierter Wiederherstellungsprozess für Sicherungen/Backups bei z.B. Systemabsturz, Re-Connect-Prozess mit Entscheidungshilfe für den Administrator (Beheben des sog. Out-of-Sync, Datenbank und Cloud nicht mehr synchron)
2. Hand-Over-Funktion, geplanter Umzugsprozess von AXM Installationen und Projekten auf ein neues System, Pausieren des Cloud-Zustandes und Re-Connect ohne Einschränkungen oder Verluste
3. Unterstützung von neuer AX Hardware
   - SREL AX Classic, Türöffner inkl. BLE für AX2Go
   - SREL 3 als Türöffner (Offline)

Bugfixes

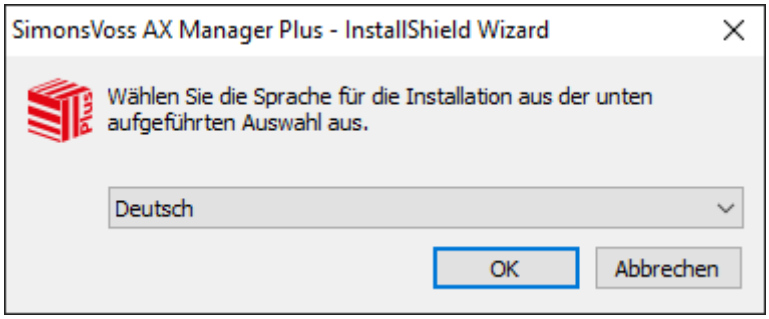
1. Das Setup-Problem wurde behoben, wenn ASP.Net x64 bereits installiert ist
2. Problem mit Programmierbedarf und Aktualisierung des Zugangsstatus behoben
3. Anwendungsfehler aufgrund fehlender Schließanlage behoben
4. Problem beim Bearbeiten „Spezielle Transponder“ behoben
5. Problem beim Zurücksetzen der PinCode AX behoben
6. Fehlerhafte Berechnung der freien AX2Go-Floating-Lizenzen behoben
7. Problem beim Arbeiten mit der Cloud direkt nach der Installation/Registrierung behoben

8. Problem beim Trennen der Cloud nach längerer Inaktivität behoben

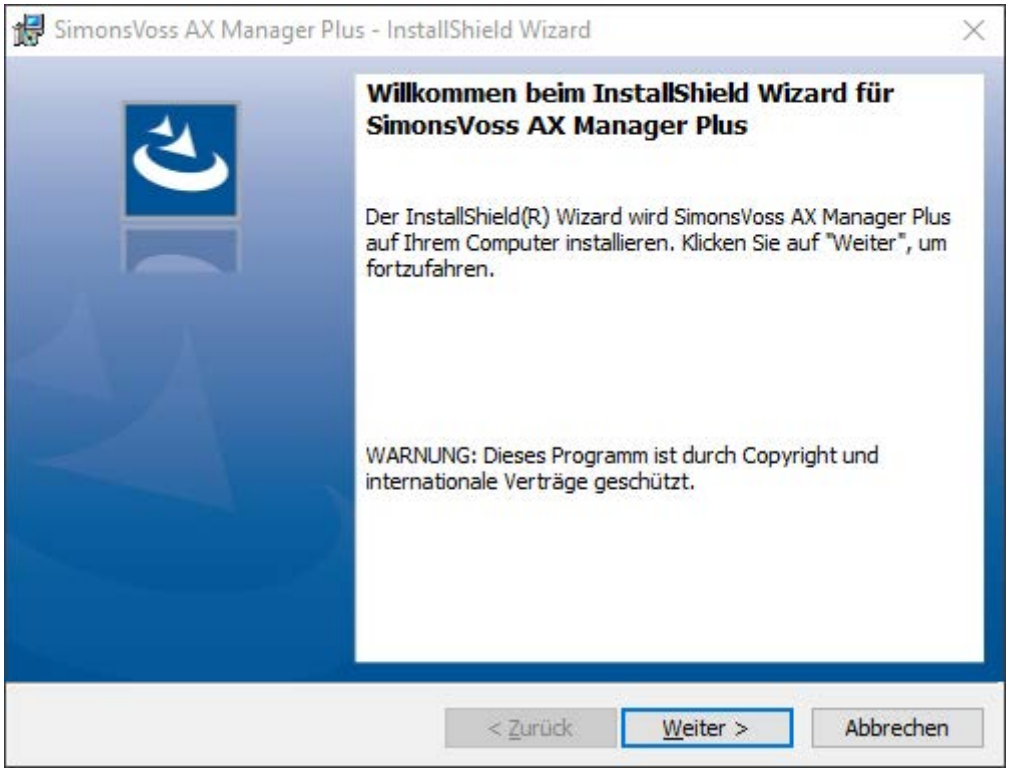
10. Installation

✓ Systemvoraussetzungen für die AXM Plus erfüllt (siehe *Systemvoraussetzungen [▸ 21]*).

1. Führen Sie die Setup-Datei aus.
   ↳ InstallShield Wizard öffnet sich.



2. Wählen Sie die Sprache aus, in der die AXM Plus installiert werden soll.
   ↳ Setup prüft, ob zusätzlich Software installiert werden muss.
3. Installieren Sie ggfs. die angezeigte zusätzliche Software.
   ↳ Setup der AXM Plus öffnet sich.



4. Folgen Sie dem Setup der AXM Plus.

↳ AXM Plus ist installiert.

10.1 AXM als Administrator ausführen (empfohlen)

SimonsVoss empfiehlt Ihnen, die AXM Plus grundsätzlich als Administrator zu starten. Damit können mögliche Probleme aufgrund von fehlenden Zugriffs- und Schreibrechten von vornherein vermieden werden:

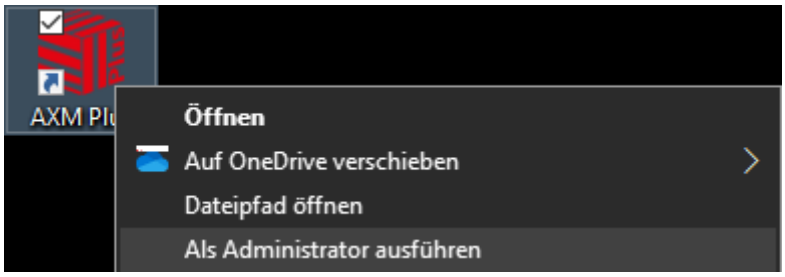
Manueller Start als Administrator

✓ AXM Plus installiert.

✓ Administratorrechte vorhanden.

1. Suchen Sie die Verknüpfung bzw. das Symbol der AXM Plus.

2. Öffnen Sie mit einem Rechtsklick auf die Verknüpfung das Kontextmenü.
3. Klicken Sie auf den Eintrag Als Administrator ausführen.



↳ AXM Plus wird als Administrator ausgeführt.

Automatischer Start als Administrator

Das manuelle Starten als Administrator hat zwei Nachteile:

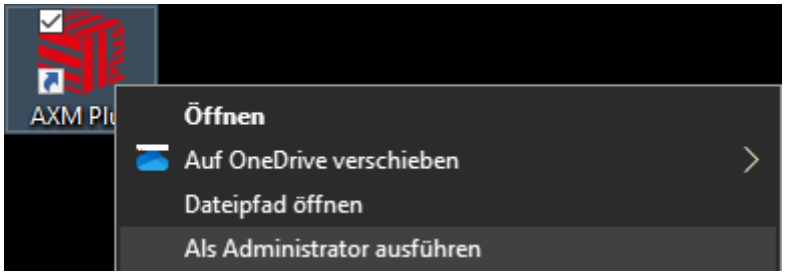
- Unkomfortabel.
- Sie könnten vergessen, die AXM Plus als Administrator zu starten.

Deshalb empfiehlt SimonsVoss, die Eigenschaften der Verknüpfung zur AXM Plus so einzustellen, dass die AXM Plus über diese Verknüpfung immer als Administrator ausgeführt wird.

✓ AXM Plus installiert.
✓ Administratorrechte vorhanden.

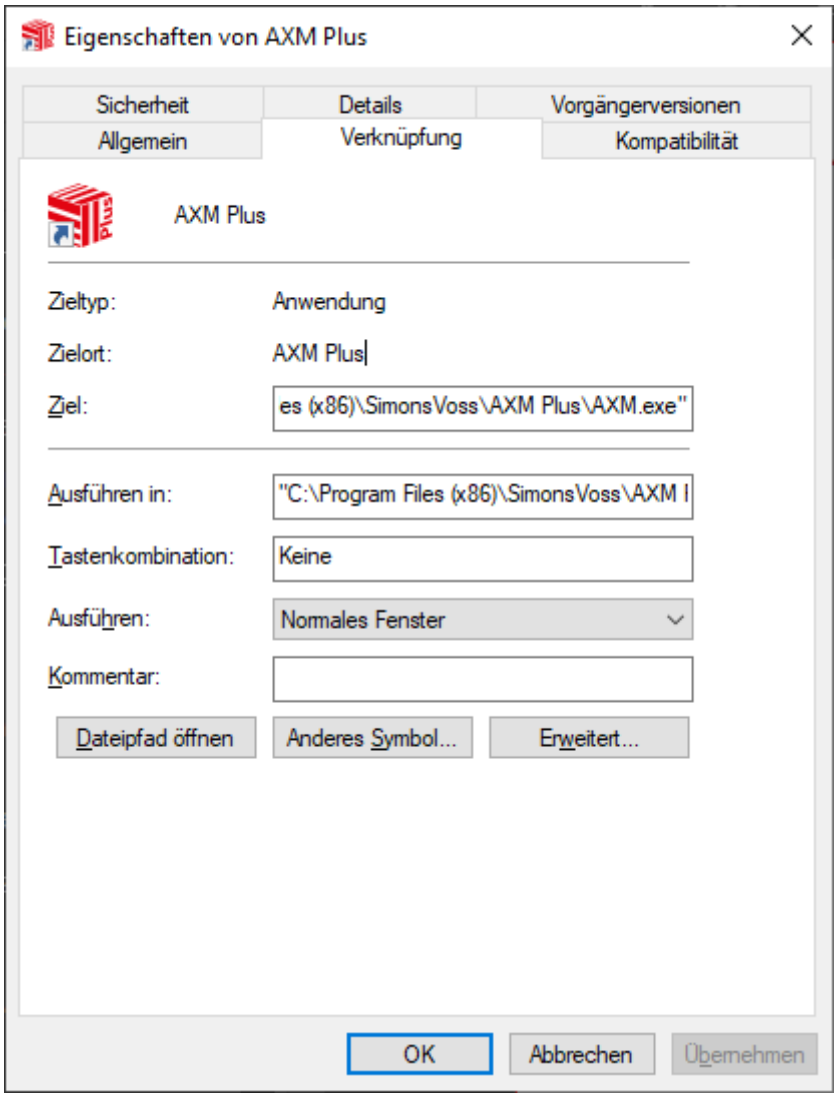
1. Suchen Sie die Verknüpfung bzw. das Symbol der AXM Plus.

2. Öffnen Sie mit einem Rechtsklick auf die Verknüpfung das Kontextmenü.
3. Klicken Sie auf den Eintrag Eigenschaften.

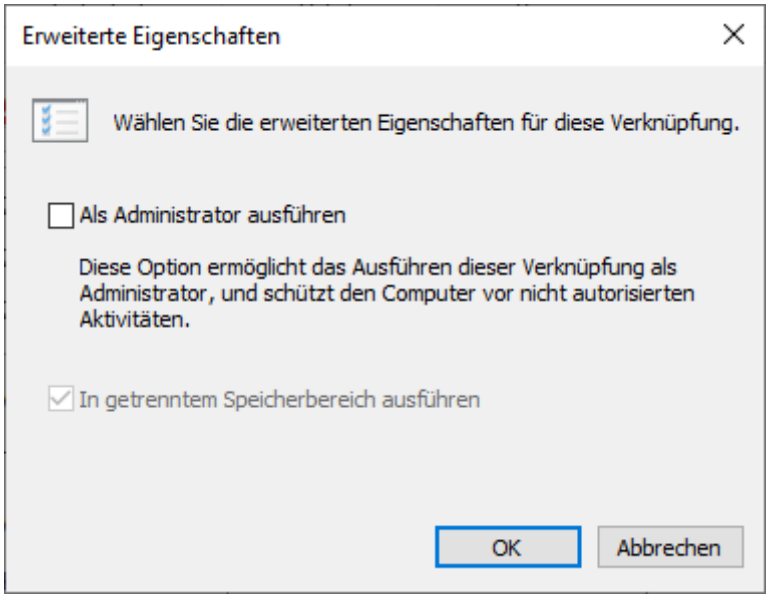


↳ Fenster "Eigenschaften von AXM ..." öffnet sich.

4. Wechseln Sie zum Tab [Verknüpfung].



5. Klicken Sie auf die Schaltfläche Erweitert... .
   ↳ Fenster "Erweiterte Eigenschaften" öffnet sich.



6. Aktivieren Sie die Checkbox ☑ Als Administrator ausführen.
7. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Erweiterte Eigenschaften" schließt sich.
8. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Eigenschaften von AXM ..." schließt sich.

↳ Wenn Sie zukünftig die AXM Plus über diese Verknüpfung starten, dann wird die AXM Plus automatisch als Administrator ausgeführt.

10.2 AXM aktualisieren

Mit der aktuellsten AXM Plus haben Sie die beste Software- und Hardwareunterstützung. Ihre AXM Plus prüft deshalb bei jedem Start, ob Updates vorhanden sind, und bietet diese auch gleich zur Installation an. Sichern Sie vor einem Update Ihre Datenbank (siehe *Backup erstellen* *[▸ 485]*).

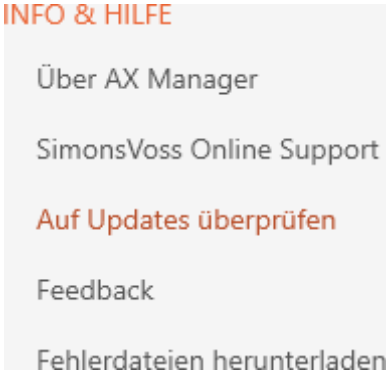
Um stattdessen die aktuell installierte Version Ihrer AXM Plus anzuzeigen siehe *Versionsnummer und Lizenzschlüssel der installierten AXM anzeigen* *[▸ 490]*.

Natürlich können Sie auch manuell überprüfen, ob ein Update vorliegt und dieses installieren.

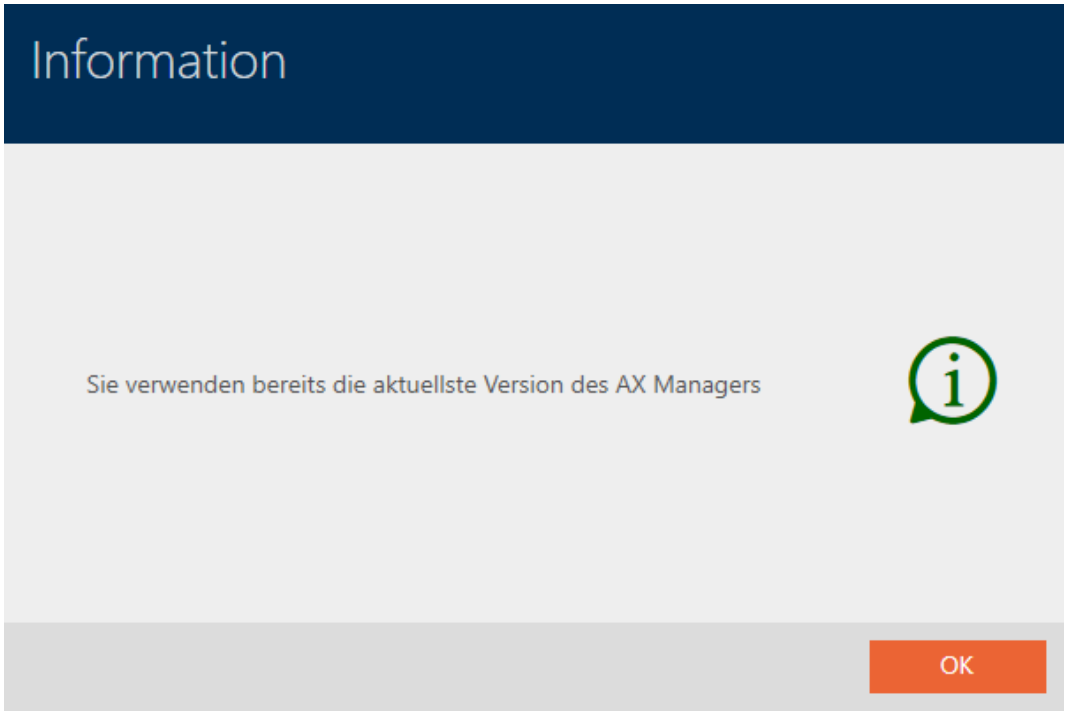
✓ Datenbank gesichert.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Klicken Sie in der Gruppe | INFO & HILFE | auf den Eintrag Auf Updates prüfen.

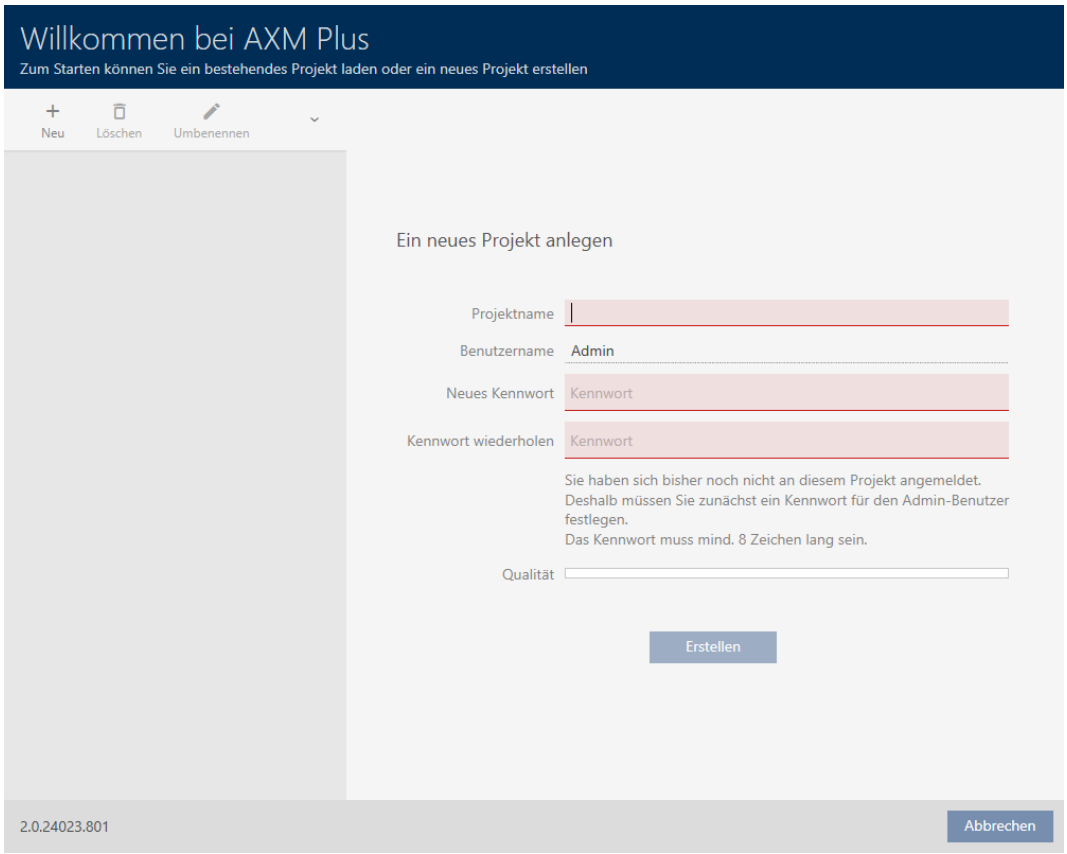


↳ Falls ein Update vorhanden ist, wird dieses angezeigt und zur Installation angeboten. Falls Ihre AXM Plus aktuell ist, sehen Sie dieses Fenster:



11. Erste Schritte nach der Installation

Die AXM Plus begrüßt Sie nach der Installation mit der Anmeldemaske.



Sie sehen folgende Eingabefelder:

- *Projektname*
- *Benutzername*
- *Neues Kennwort*
- *Kennwort wiederholen*

1. Geben Sie in das Feld *Projektname* einen Projektnamen ein.
2. Geben Sie in das Feld *Neues Kennwort* ein Kennwort mit mindestens 8 Zeichen ein, um Ihr Projekt zu schützen.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

3. Wiederholen Sie im Feld *Kennwort wiederholen* das eingegebene Kennwort.
4. Klicken Sie auf die Schaltfläche Erstellen.

↳ Neues Projekt ist erstellt.

Sie können das soeben erstellte Benutzerkennwort bei Bedarf ändern (siehe *Benutzerkennwort ändern [▸ 492]*).

Das Schließanlagenpasswort lässt sich ändern (siehe *Schließanlagenpasswort ändern [▸ 395]*).

ACHTUNG

Schließanlagenpasswort zugänglich und sicher aufbewahren

Das Schließanlagenpasswort ist das wichtigste Passwort überhaupt. Aus Sicherheitsgründen kann auch SimonsVoss keine Komponenten ohne Schließanlagenpasswort oder Backup zurücksetzen. Einen Generalschlüssel gibt es nicht.

Komponenten, zu denen kein Schließanlagenpasswort mehr bekannt oder über ein Backup wiederherstellbar ist, können nicht mehr programmiert werden. Sie müssen aufwendig aus Schlössern entfernt und entsorgt werden.

1. Stellen Sie sicher, dass das Schließanlagenpasswort jederzeit durch befugte Personen einsehbar und/oder zugänglich ist.
2. Berücksichtigen Sie dabei auch sowohl vorhersehbare Ereignisse (z.B. Schließanlagenverwalter geht in Rente) und unvorhersehbare Ereignisse (z.B. Schließanlagenverwalter kündigt).

Der erste Start der AXM Plus

Die AXM Plus bietet Ihnen jetzt nacheinander mehrere Assistenten an:

1. Schließanlage anlegen
2. Schließung anlegen
3. Transponder anlegen

Mit diesen Assistenten können Sie direkt anfangen, Ihre Schließanlage aufzubauen und sich mit der Oberfläche der AXM Plus vertraut zu machen.

Erledigen Sie jedoch vor dem Aufbau einer großen Schließanlage organisatorische Vorarbeiten (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*).

Wenn Sie das erste Mal mit einer Schließanlage arbeiten, dann finden Sie hier Erklärungen und Hintergrundwissen: *Hintergrundwissen und Erklärungen [▸ 532]*.

11.1 Best Practice: Schließanlage aufbauen

Sie ersparen sich viel Zeit und Arbeit, wenn Sie Ihre Schließanlage in einer Reihenfolge aufbauen, in der Sie die Fenster möglichst nur einmal aufrufen müssen.

Grundsätzlich ist es am einfachsten, wenn Sie die Organisationsstruktur als Erstes vorbereiten (siehe *Organisationsstruktur [▸ 55]*).

Erfahrungsgemäß hat sich folgendes Konzept bewährt:

1. Standorte erstellen (siehe *Standort erstellen [▸ 83]*).
2. Gebäude erstellen (siehe *Gebäude erstellen und zu Standort zuweisen [▸ 86]*).
3. Bereiche erstellen (siehe *Bereich erstellen [▸ 89]*).
4. Ersten Zeitplan erstellen (siehe *Zeitplan erstellen [▸ 58]*).
5. Alle benötigten Zeitgruppen erstellen (siehe *Zeitgruppe erstellen [▸ 61]*).
6. Weitere Zeitpläne erstellen und dabei die Zeitgruppen direkt für den jeweiligen Zeitplan einstellen.
7. Berechtigungsgruppen erstellen (siehe *Berechtigungsgruppen [▸ 332]*).
8. Personengruppen erstellen (siehe *Personengruppe erstellen [▸ 56]*).
9. Ggfs. Karten in der Schließanlage einrichten (siehe *Karten bzw. Transponder freischalten [▸ 401]*).
10. Identmedien erstellen und direkt bei der Erstellung den Berechtigungsgruppen, Personengruppen und Zeitgruppen zuweisen (siehe *Transponder und Karten erstellen [▸ 95]*, *Personengruppe erstellen [▸ 56]* und *Berechtigungen des Identmediums auf bestimmte Zeiten beschränken (Zeitgruppe) [▸ 126]*)
11. Schließungen erstellen und direkt bei der Erstellung den Berechtigungsgruppen, Bereichen und Zeitplänen zuweisen (siehe *Schließung erstellen [▸ 238]*, *Bereich erstellen [▸ 89]* und *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]*).
12. Schließungen synchronisieren (siehe *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).
13. Identmedien synchronisieren (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).

In dieser Reihenfolge verwenden Sie die Ergebnisse aus den vorherigen Schritten direkt in den nächsten Schritten:

- Zeitgruppen für neu erstellte Zeitpläne direkt im Fenster des erstellten Zeitplans einstellen
- Zeitgruppe und Berechtigungsgruppen direkt im Fenster des erstellten Identmediums

- Zeitplan und Berechtigungsgruppe direkt im Fenster der erstellten Schließung

Hintergrundwissen für Ihre Überlegungen zum Zeitmanagement und zu Berechtigungsgruppen:

- *Zeitmanagement [▸ 548]*
- *Berechtigungsgruppen [▸ 564]*

Selbstverständlich können Sie von dieser Reihenfolge auch abweichen und zum Beispiel zuerst Identmedien und Schließungen ohne Zeitgruppe erstellen. Wenn Sie später allerdings doch Zeitmanagement benötigen, dann müssen Sie:

- Jeder Schließung, die im Zeitmanagement vorgesehen ist, einen Zeitplan zuweisen und
- Jedem Transponder eine Zeitgruppe zuweisen.

11.2 Best Practice: AX2Go einrichten

Bei der Einrichtung und Inbetriebnahme von AX2Go (mobile Schlüssel) hat sich folgendes Konzept bewährt:

1. AXM Plus installieren (siehe *Installation [▸ 24]*).
2. AXM Plus registrieren (siehe *Registrierung [▸ 34]*).
3. Richten Sie Ihre Schließanlage mit Schließungen und Transpondern ein (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*).
4. Legen Sie Ihre AX2Go-Einstellungen fest (siehe *AX2Go-Einstellungen [▸ 507]*).

↳ AX2Go ist einsatzbereit. Erstellen und verschicken Sie beispielsweise Einladungen (siehe *Verwaltung von AX2Go-Schlüsseln [▸ 220]*).

11.3 Best Practice: Schutz der Datenbank

Sie erhöhen das Sicherheitsniveau Ihrer AXM Plus weiter, indem Sie den Zugriff auf Ihre SQL-Datenbank schützen.

1. Erstellen Sie ein separates Windows-Benutzerkonto für den Schließanlagenverwalter.
2. Verwenden Sie für alle Windows-Benutzerkonten ein starkes Passwort.
3. Verschlüsseln Sie die Festplatte, auf der die Datenbank gespeichert ist.

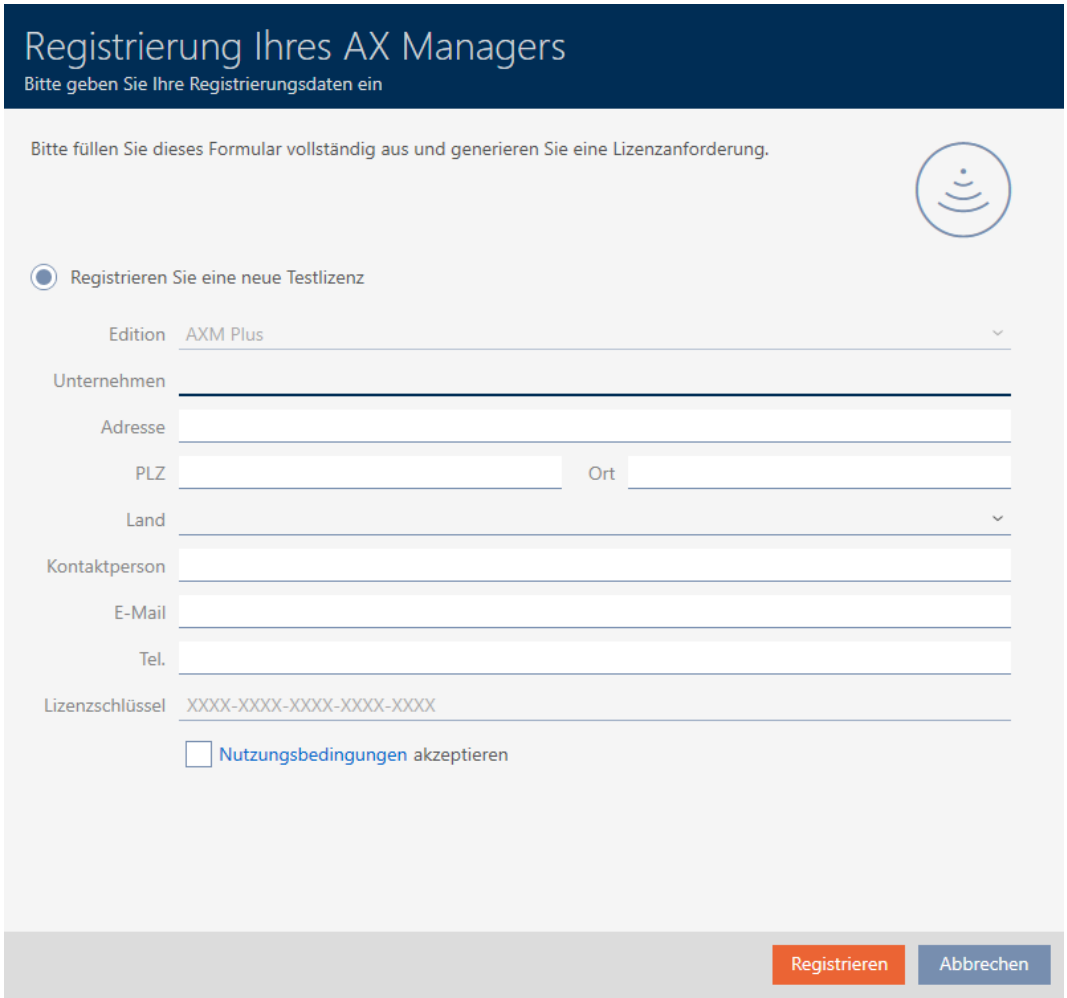
12. Registrierung

12.1 Registrierung als Testversion

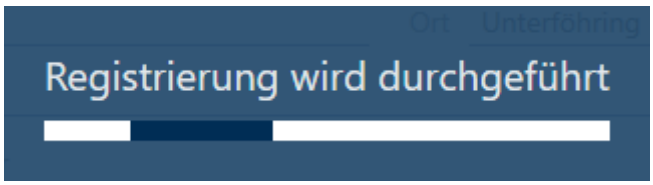
1. Starten Sie die AXM Plus.
   ↳ Ihre AXM Plus weist Sie darauf hin, dass Sie sie noch registrieren müssen.

2. Klicken Sie auf die Schaltfläche Starte {0}-tägige Testphase.
   ↳ Ihre AXM Plus weist Sie darauf hin, dass Sie auch während der Testphase eine SimonsVoss-ID benötigen.

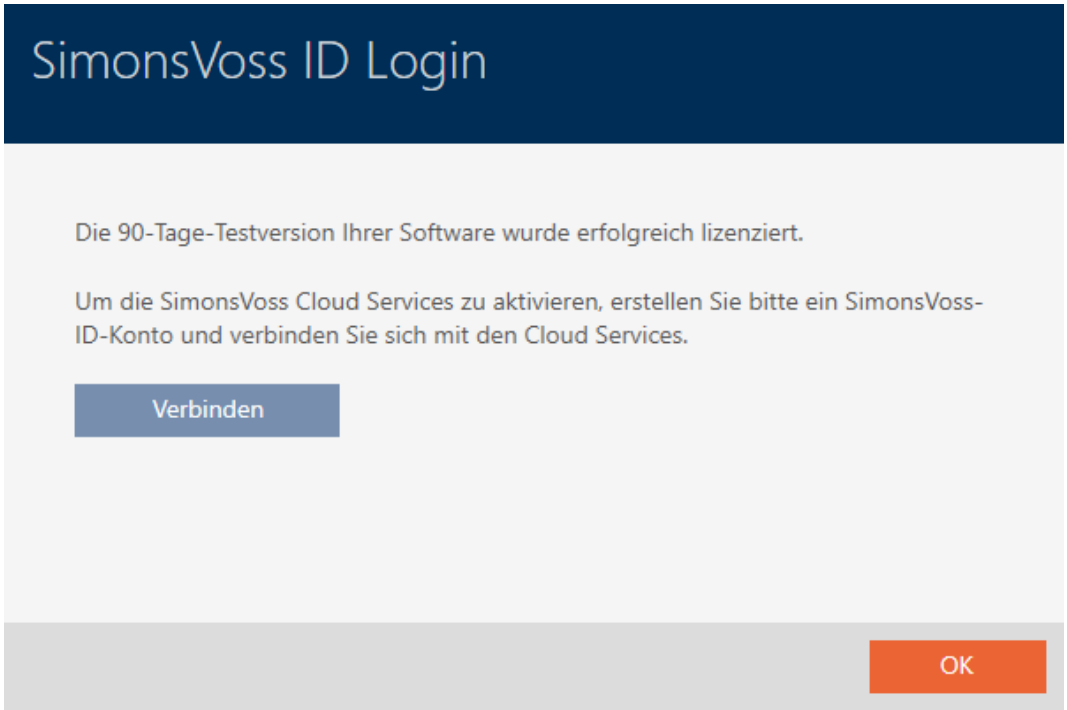
3. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Registrierungsformular öffnet sich.



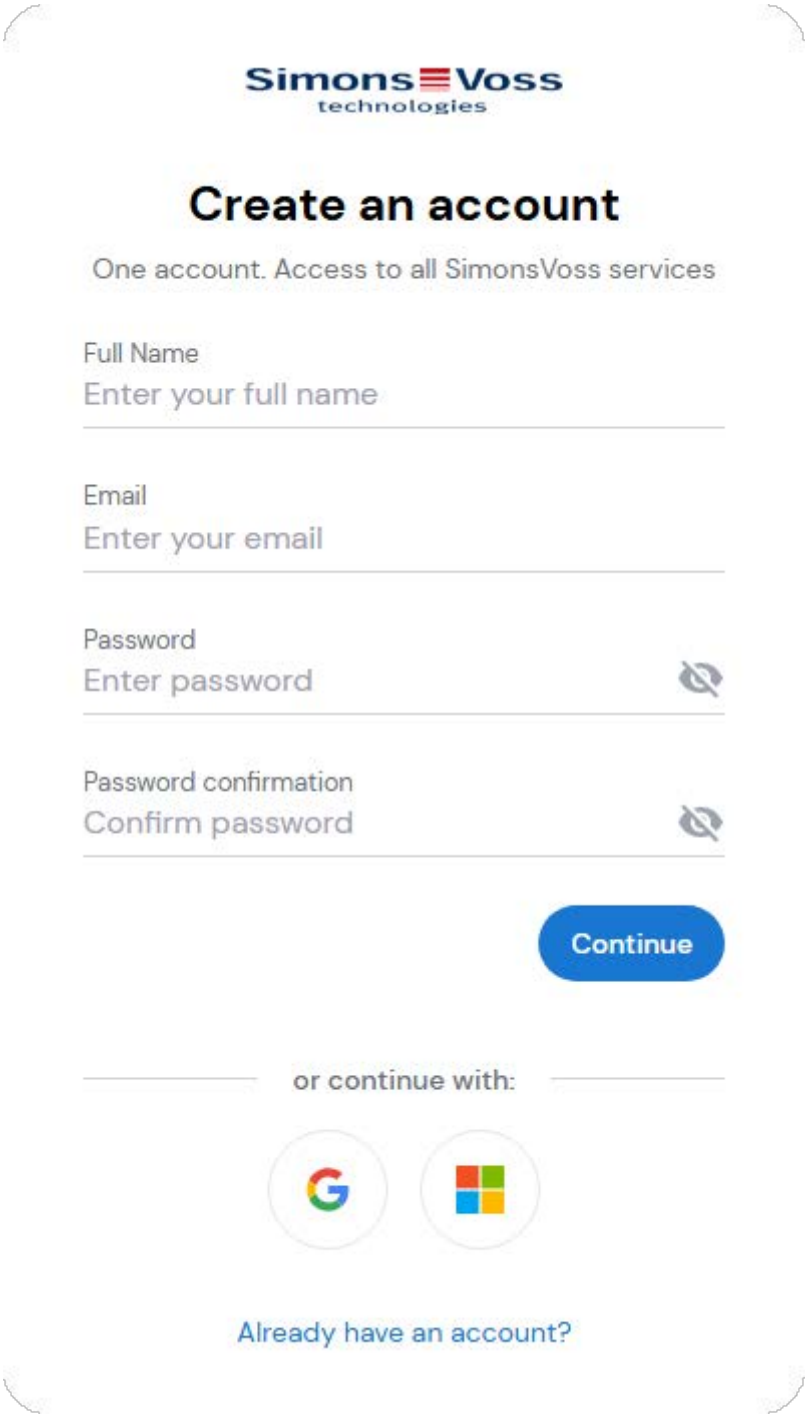
4. Füllen Sie das Registrierungsformular aus (Für die Testphasen-Registrierung ist das Feld *Lizenzschlüssel* ausgegraut).
5. Akzeptieren Sie die Nutzungsbedigungen.
6. Klicken Sie auf die Schaltfläche Registrieren.
   ↳ Registrierung wird durchgeführt.



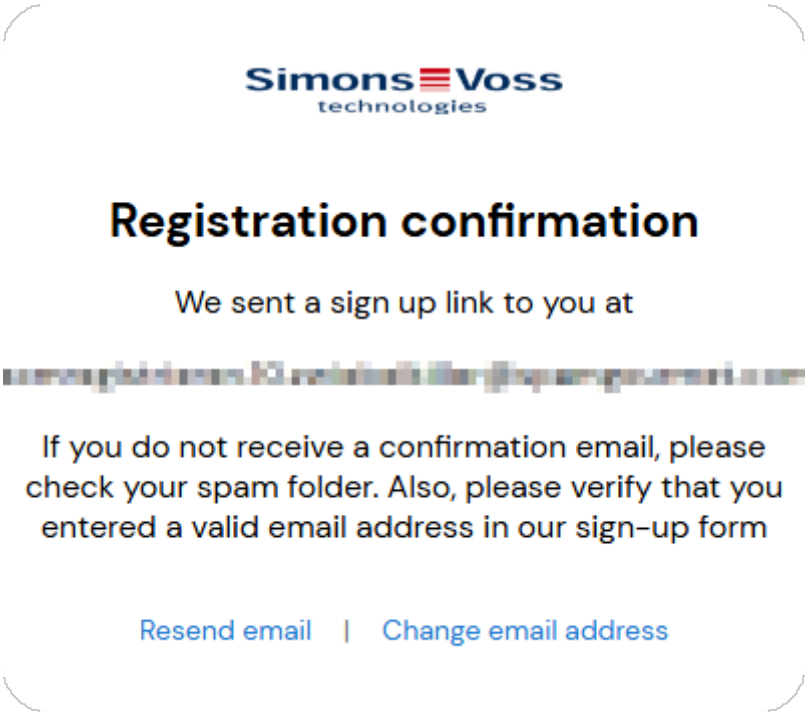
   ↳ Registrierung erfolgreich.
   ↳ Ihre AXM Plus fordert Sie auf, eine SimonsVoss-ID zu erstellen.



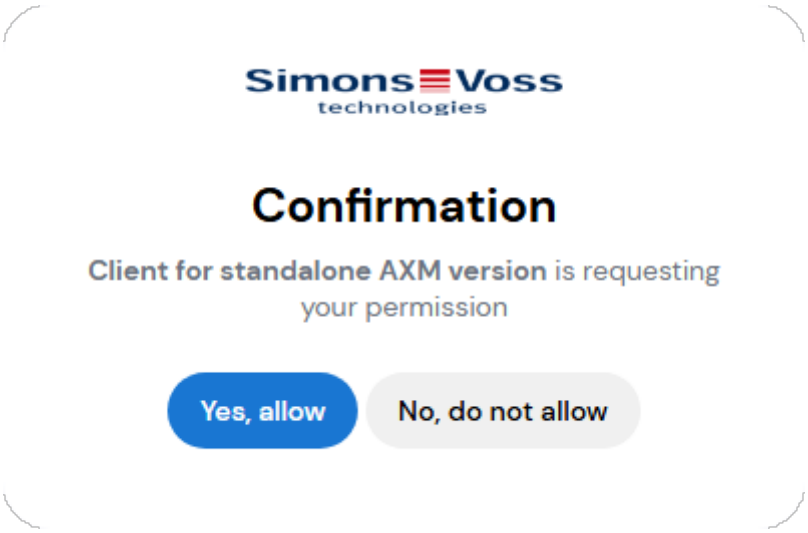
7. Klicken Sie auf die Schaltfläche Verbinden.
   ↳ Website zur Erstellung einer SimonsVoss-ID öffnet sich.



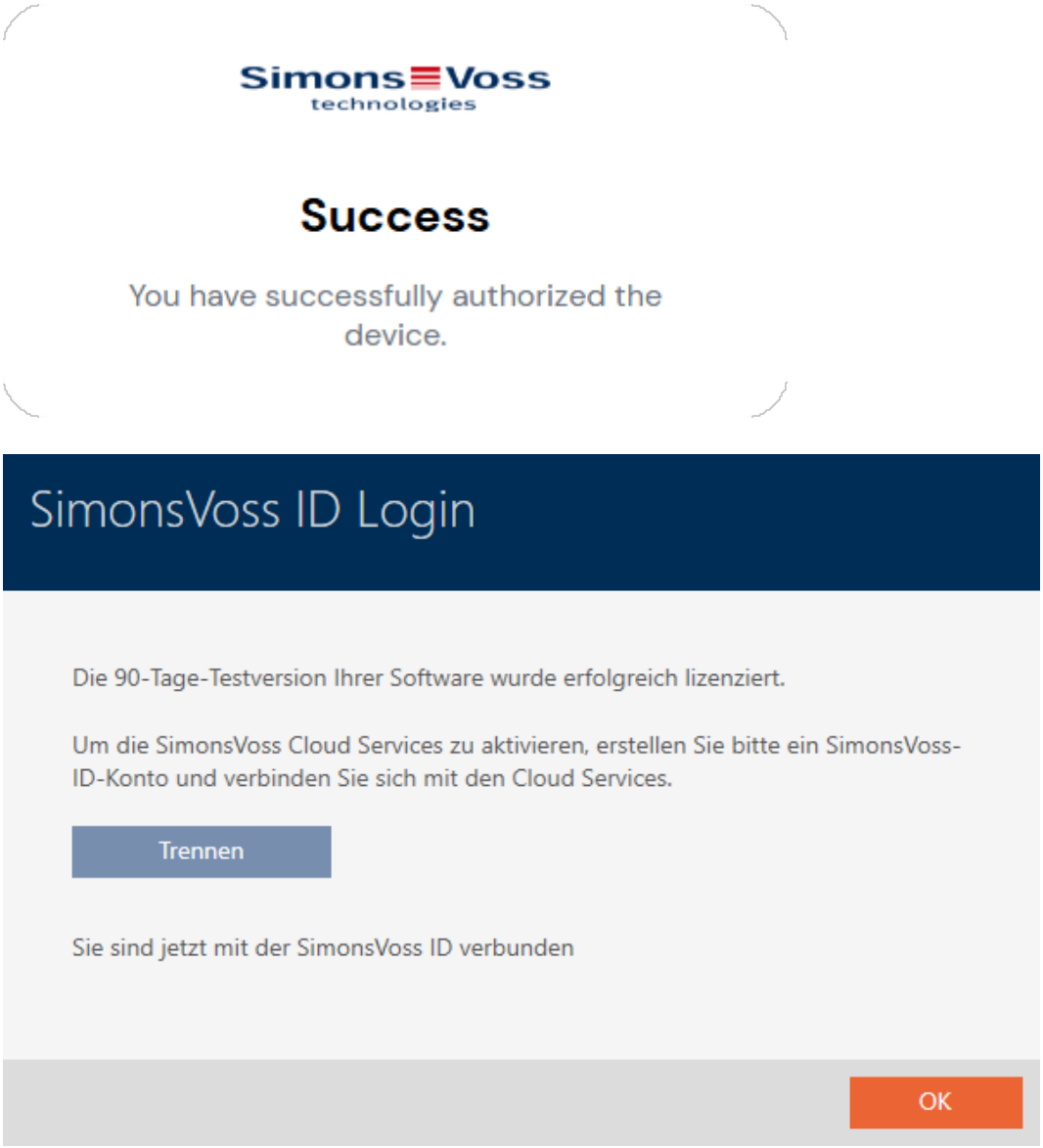
8. Geben Sie die benötigten Daten ein oder verwenden Sie Ihr Google-/Microsoft-Konto.
   Wenn Sie bereits eine SimonsVoss-ID haben, können Sie diese verwenden und müssen keine neue erstellen.
9. Senden Sie Ihre Angaben mit "Continue" ab.
   ↳ Registrierungsanfrage für SimonsVoss-ID ist versendet.



10. Prüfen Sie Ihr E-Mail-Postfach und klicken Sie auf den Bestätigungslink.
    ↳ Website zur Verknüpfung Ihrer SimonsVoss-ID mit Ihrer AXM Plus öffnet sich.



11. Klicken Sie auf "Yes, allow", um Ihre SimonsVoss-ID und AXM Plus zu verknüpfen.
    ↳ Website und AXM Plus informieren Sie über die erfolgreiche Verknüpfung.



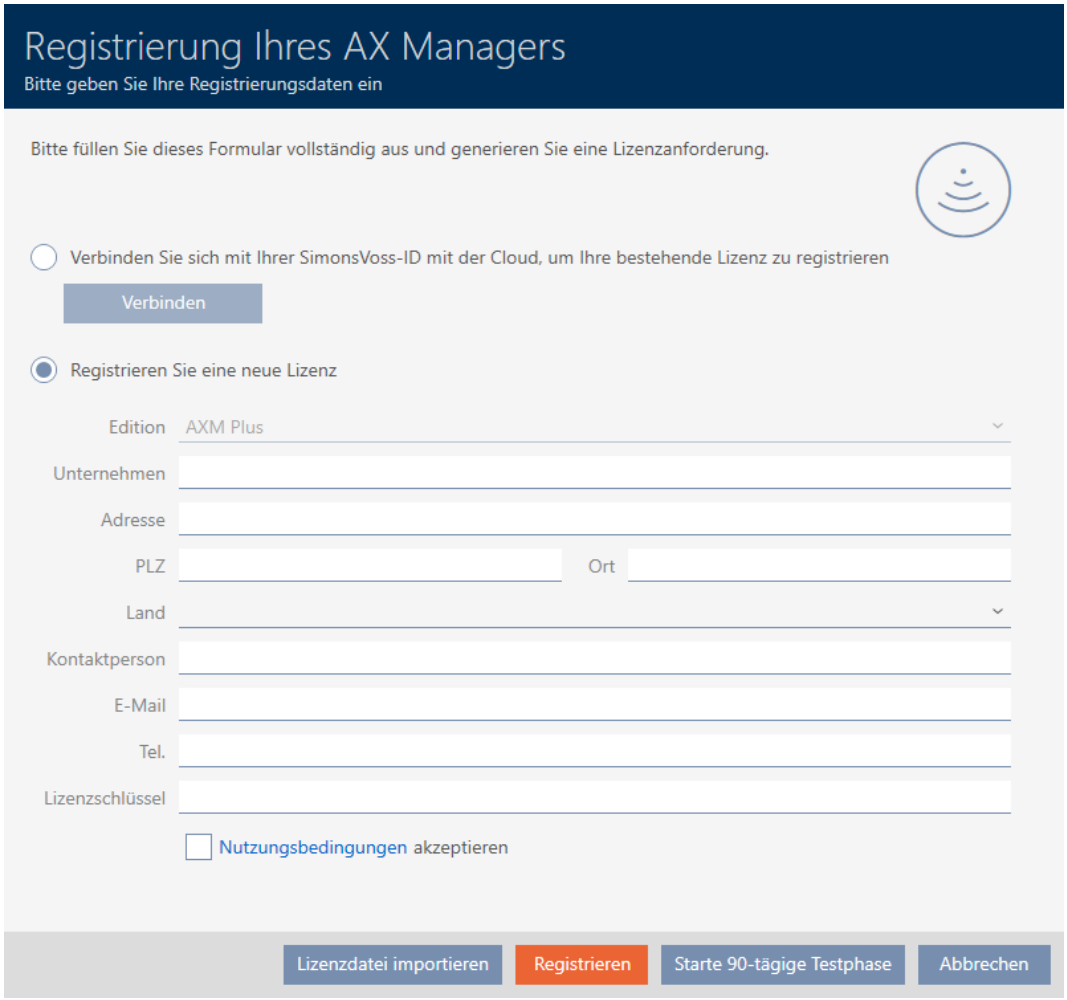
12. Klicken Sie auf die Schaltfläche OK.
↳ Registrierung abgeschlossen und für 90 Tage gültig.
↳ AXM Plus öffnet ein Anmeldefenster, damit Sie sich anmelden können.

12.2 Registrierung mit Lizenz

Für die Registrierung benötigen Sie einen Lizenzschlüssel. Diesen erhalten Sie über einen unserer Fachhandelspartner.

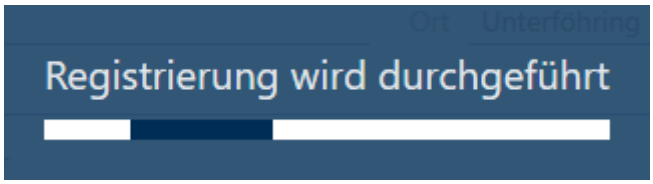
1. Starten Sie die AXM Plus.
   ↳ Ihre AXM Plus weist Sie darauf hin, dass Sie sie noch registrieren müssen.

2. Klicken Sie auf die Schaltfläche Vorhandene Lizenz registrieren.
   ↳ Registrierungsformular öffnet sich.

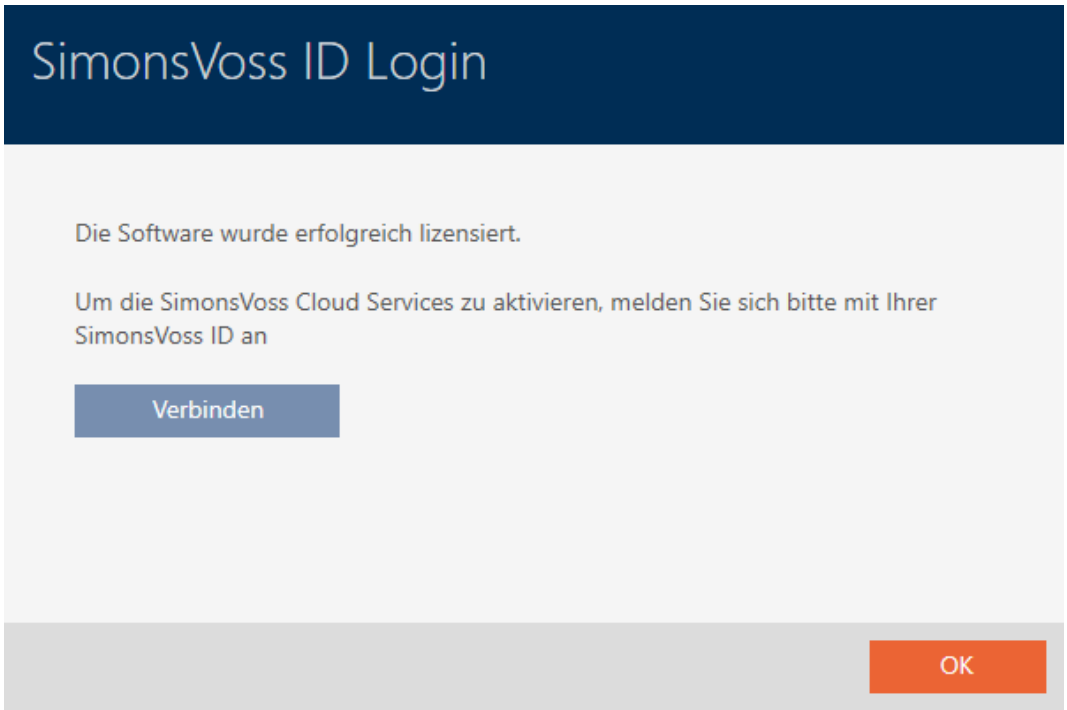


3. Füllen Sie das Registrierungsformular einschließlich des Felds *Lizenzschlüssel* aus.
   Wenn Sie die AXM Plus früher bereits einmal registriert und mit Ihrer SimonsVoss-ID verknüpft hatten, dann können Sie die Registrierung überspringen und sich direkt mit Ihrer SimonsVoss-ID verbinden. Die Lizenz wird dann aus der SimonsVoss-ID übernommen.
4. Akzeptieren Sie die Nutzungsbedigungen.

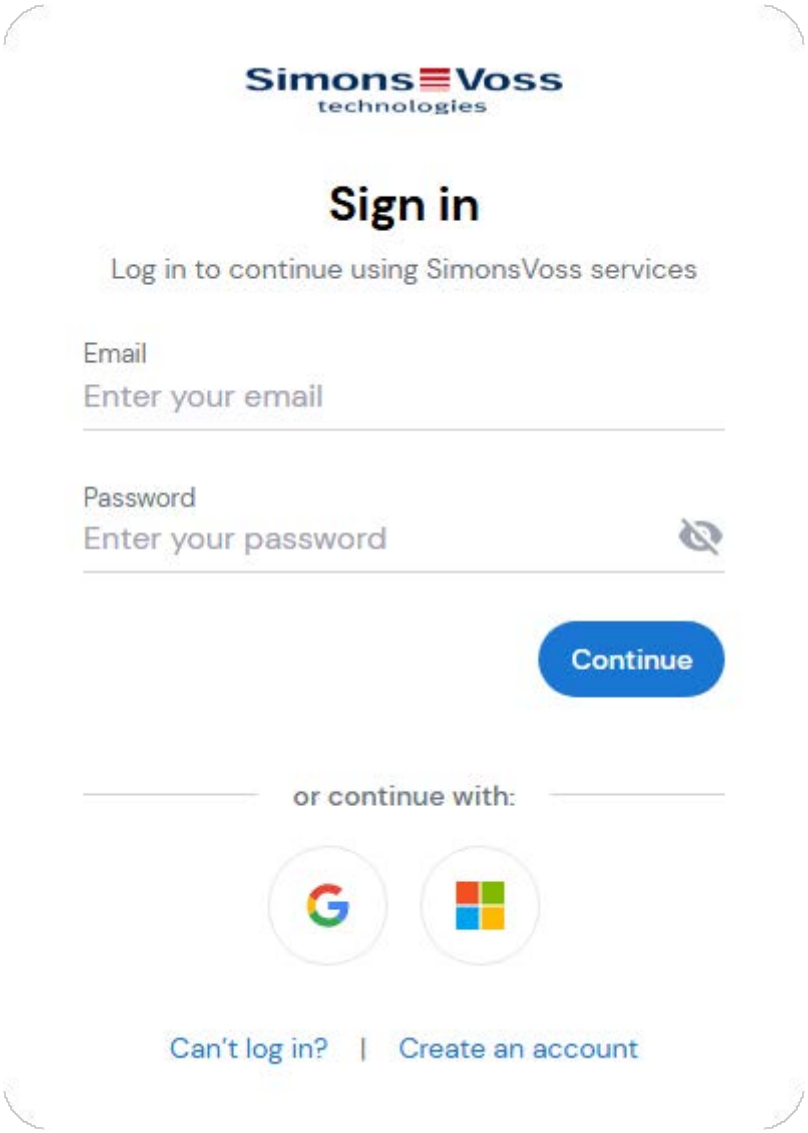
5. Klicken Sie auf die Schaltfläche Registrieren.
   ↳ Registrierung wird durchgeführt.



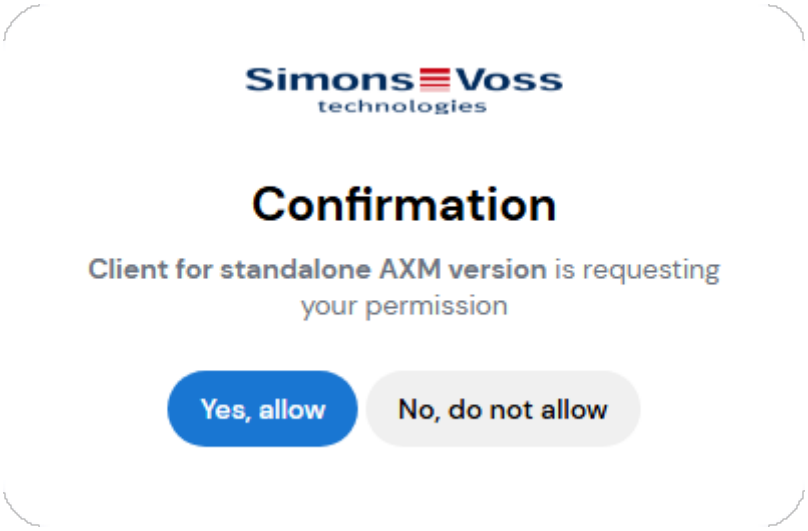
   ↳ Registrierung erfolgreich.
   ↳ Ihre AXM Plus fordert Sie auf, sich mit Ihrer SimonsVoss-ID anzumelden.



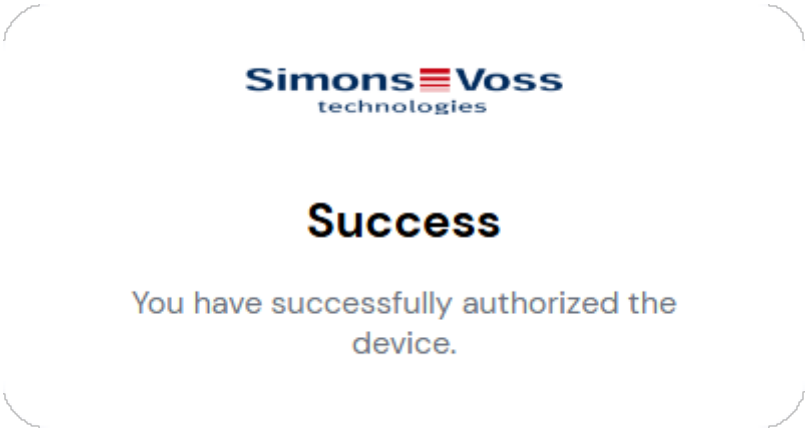
6. Klicken Sie auf die Schaltfläche Verbinden.
   ↳ Website zur Anmeldung mit SimonsVoss-ID öffnet sich.

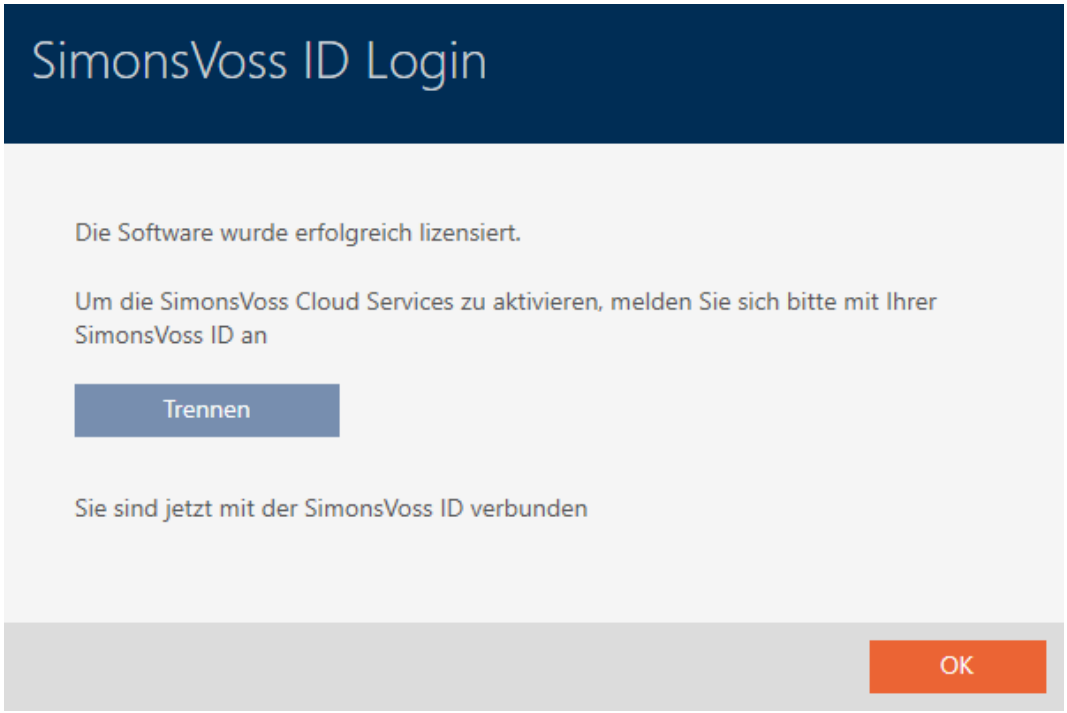


7. Geben Sie die benötigten Daten ein oder verwenden Sie Ihr Google-/Microsoft-Konto.
   Wenn Sie bereits eine SimonsVoss-ID haben, können Sie diese verwenden und müssen keine neue erstellen.
8. Senden Sie Ihre Angaben mit "Continue" ab.
   ↳ Website zur Verknüpfung Ihrer SimonsVoss-ID mit Ihrer AXM Plus öffnet sich.

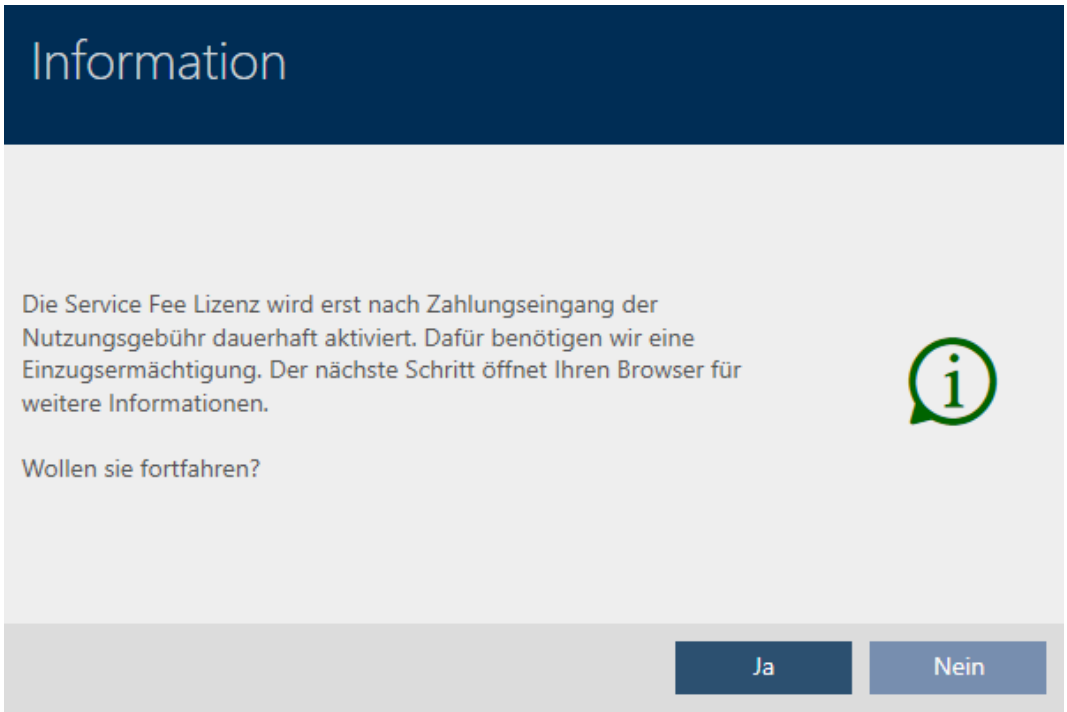


9. Klicken Sie auf "Yes, allow", um Ihre SimonsVoss-ID und AXM Plus zu verknüpfen.
   ↳ Website und AXM Plus informieren Sie über die erfolgreiche Verknüpfung.





10. Klicken Sie auf die Schaltfläche OK.
    ↳ Es erscheint ein Hinweis zum Status der Service Fee Lizenz.



11. Klicken Sie auf Ja, um den Browser zu öffnen oder klicken Sie auf Nein, um ein Projekt zu erstellen.
    (Beispiel: Ja)
    ↳ Website mit weiteren Informationen öffnet sich.

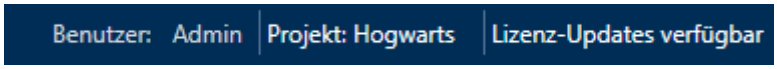
↳ Registrierung und Verknüpfung mit SimonsVoss-ID abgeschlossen.

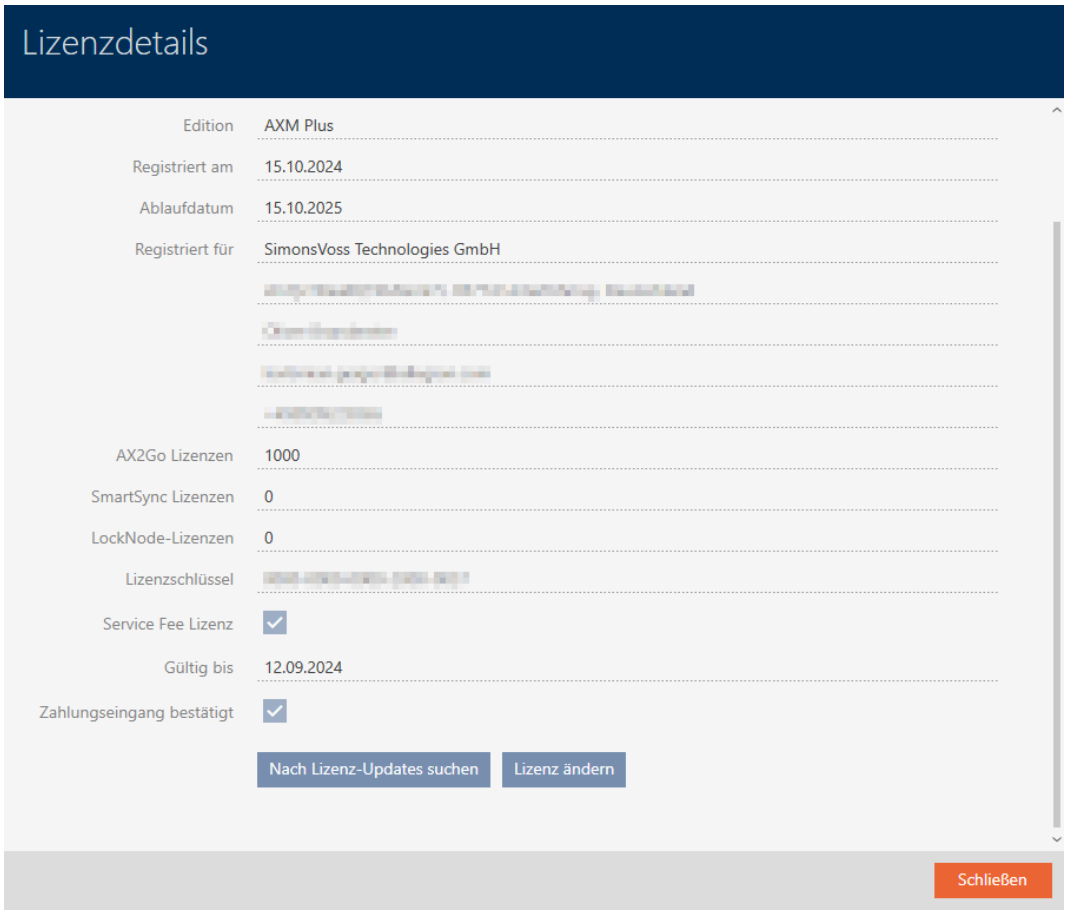
12.3 Aktualisieren Ihrer Lizenz

Durch die Verbindung mit unserem Lizenz-Service sind die Informationen zu Ihrer Software-Lizenz immer aktuell.

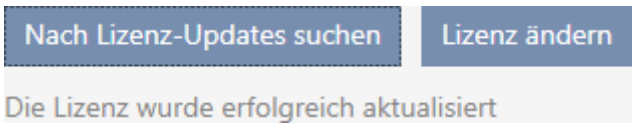
Sobald sich Änderungen ergeben (z.B. durch Erweiterung des Leistungsumfangs), wird Ihnen die Änderung in der Fußleiste der AXM Plus beim Anwendungsstart angezeigt.

Sie können die Änderungen übernehmen, indem Sie auf *Lizenz-Updates verfügbar* klicken.



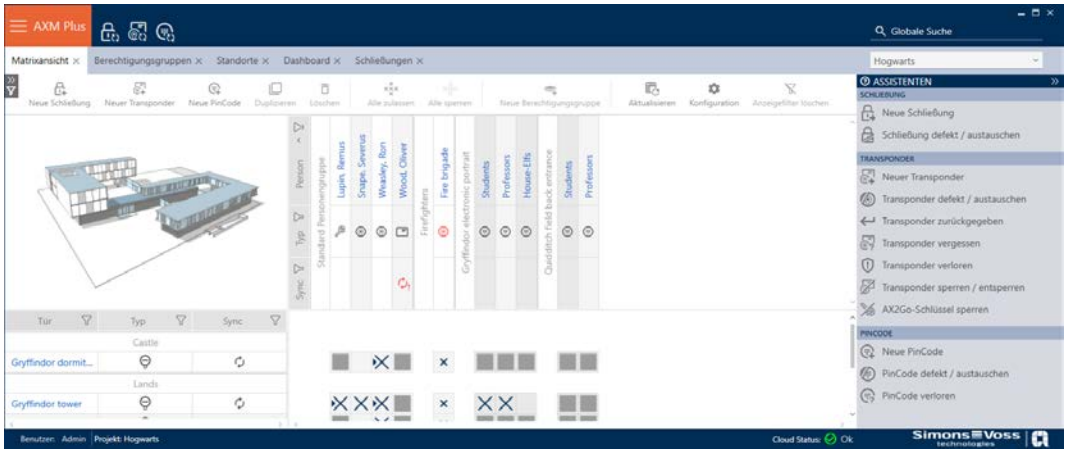


Scrollen Sie im sich öffnenden Fenster nach unten und klicken Sie auf Nach Lizenz-Updates suchen.



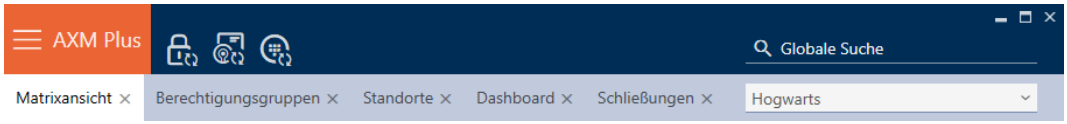
Die Lizenz wurde erfolgreich aktualisiert

13. Aufbau der AXM



Die Oberfläche der AXM Plus besteht vor allem aus vier großen Teilen:

AXM-Leiste und Tabs



Mit der orangenen AXM-Schaltfläche AXM klappen Sie die AXM-Leiste aus:

Hier haben Sie Zugang zu allen verfügbaren Tabs.

Darunter sehen Sie die geöffneten Tabs. Innerhalb eines Tabs spielt sich eine Aufgabe ab. So gibt es zum Beispiel einen Tab für [Berechtigungsgruppen], einen Tab für [Standorte] und so weiter.

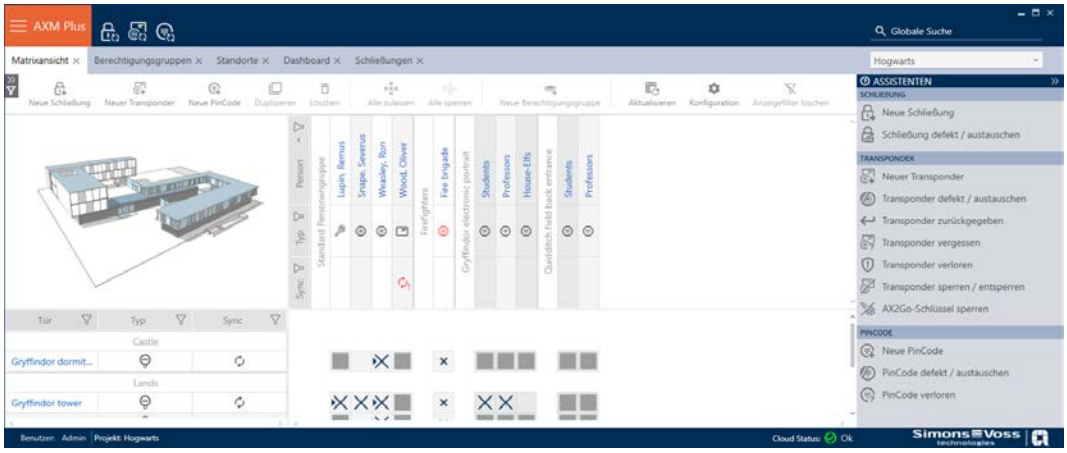
Die Tabs lassen sich grundsätzlich so bedienen, wie Sie es vielleicht schon von Ihrem Browser gewohnt sind (siehe *Tab-Bedienung [▸ 53]*).

Neben der AXM-Schaltfläche gibt es drei Schaltflächen, um direkt zur Synchronisierung von Schließungen und Identmedien zu springen.

Sie sind eine Alternative, um die Synchronisierung zu starten, ohne zuerst in die Eigenschaften der Schließung bzw. des Identmediums zu gehen.

Auf der rechten Seite finden Sie eine globale Suchfunktion. Hier können Sie in der gesamten Datenbank nach Einträgen aller Art suchen (siehe *Globale Suche [▸ 52]*).

Matrixbereich



Der Matrixbereich ist der Maschinenraum Ihrer AXM Plus. Hier sehen Sie alle Schließungen und Identmedien. Mit der Filterfunktion blenden Sie Einträge aus und verschaffen sich so einen Überblick (siehe *Sortieren und Filtern [▸ 49]*).

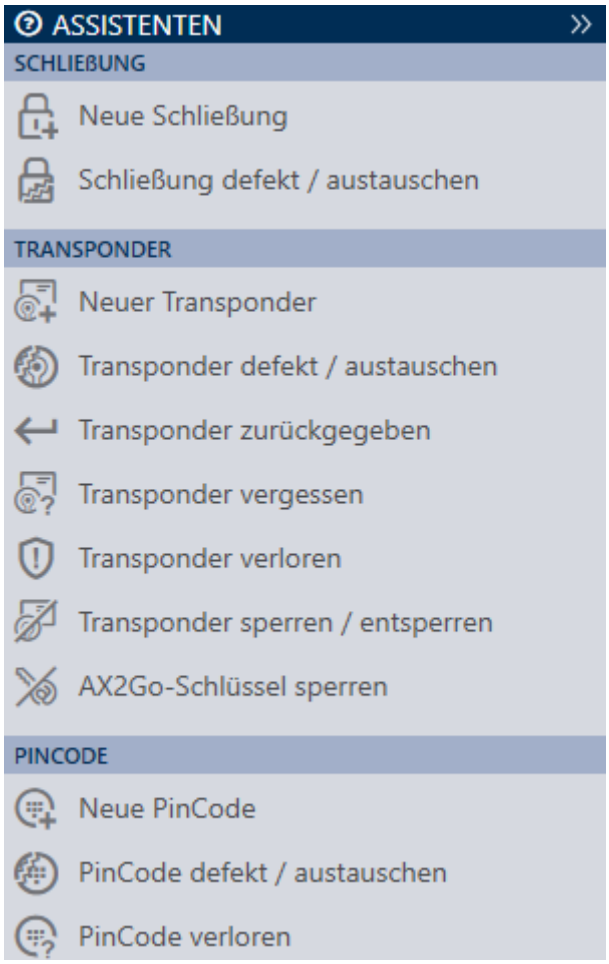
Normalerweise steht jede Zeile für eine Schließung und jede Spalte für ein Identmedium. Dort, wo sich Zeilen und Spalten treffen, wird die Berechtigung dieses Identmediums für diese Schließung angegeben (siehe *Berechtigungen [▸ 327]*). Grundsätzlich gibt es zwei verschiedene Hauptzustände:

- Berechtigung gesetzt (Kreuz)
- Keine Berechtigung gesetzt (kein Kreuz)

In der Matrix können verschiedene Informationen angezeigt werden. Eine davon ist der Synchronisierungszustand. Wenn hier das Synchronisieren-Symbol ⟲/⟲) zu sehen ist, dann müssen Sie synchronisieren (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*). Mit einem Klick auf ⟲/⟲ starten Sie sofort die Synchronisierung des jeweiligen Eintrags.

Außerdem steht Ihnen im Matrixbereich eine Aktionsleiste zur Verfügung, mit der Sie die Matrix bearbeiten können:

Assistenten-Menü



Auf der rechten Seite Ihrer AXM Plus befindet sich ein Assistenten-Menü. Hier finden Sie Assistenten, die Ihnen bei häufig auftretenden Situationen zur Seite stehen (z.B. bei verlorenen Identmedien).

Falls Sie mehr Platz brauchen, können Sie das Assistenten-Menü mit `>>` ausblenden und mit `<<` einblenden.

Fußleiste

Am unteren Bildschirmrand sehen Sie den Benutzer- und den Projektnamen.

Dashboard

Ein neues Feature der AXM Plus ist das sogenannte Dashboard (siehe *Statistiken und Warnungen anzeigen (Dashboard) [▸ 518]*). Es liefert Ihnen Statistiken über Ihre Datenbank und zeigt Ihnen Warnungen an, wenn beispielsweise eine Aufgabe noch nicht abgeschlossen ist.

Das Dashboard ist über die AXM-Leiste erreichbar.

Protokoll

Mit dem Protokoll behalten Sie jederzeit den Überblick darüber, wer wann was an der Datenbank verändert (siehe *Aktivitäten an der Datenbank nachverfolgen (Protokoll) [▸ 520]*).

Das Protokoll ist ebenso über die AXM-Leiste erreichbar.

13.1 Sortieren und Filtern

Große Listen und Tabellen können unübersichtlich werden.

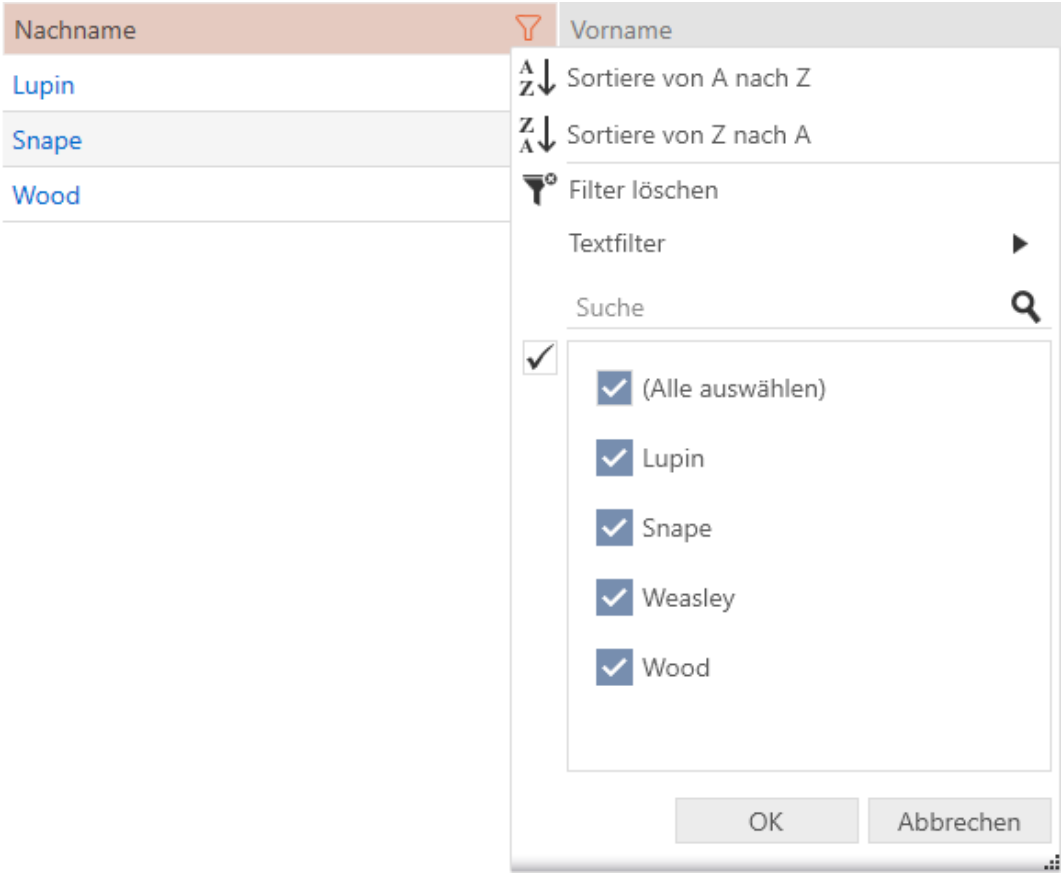
Die AXM Plus stellt Ihnen deshalb Funktionen zum Sortieren und Filtern zur Verfügung.

Sortieren

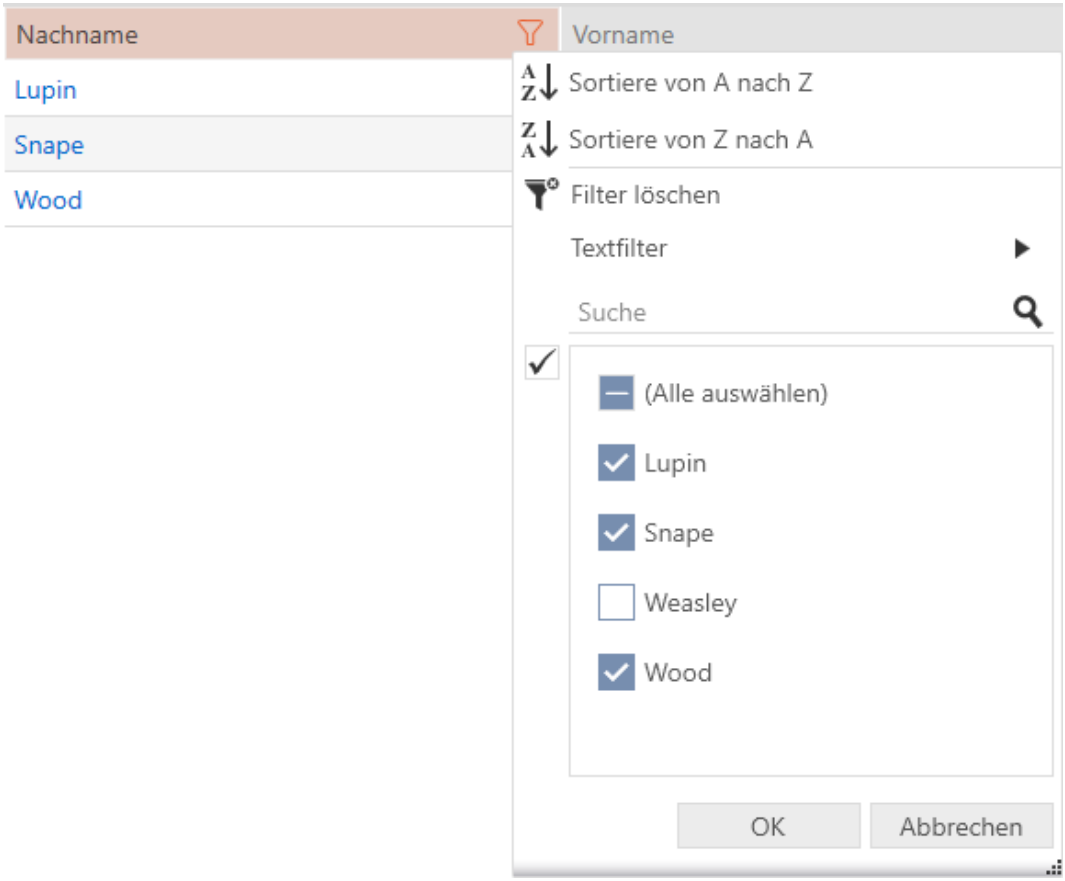
1. Klicken Sie auf eine der Spalten- oder Zeilenüberschriften.
   ↳ Einträge werden nach dieser Spalte/Zeile sortiert.
2. Klicken Sie erneut auf dieselbe Überschrift.
   ↳ Sortierreihenfolge wird umgekehrt.

Filtern

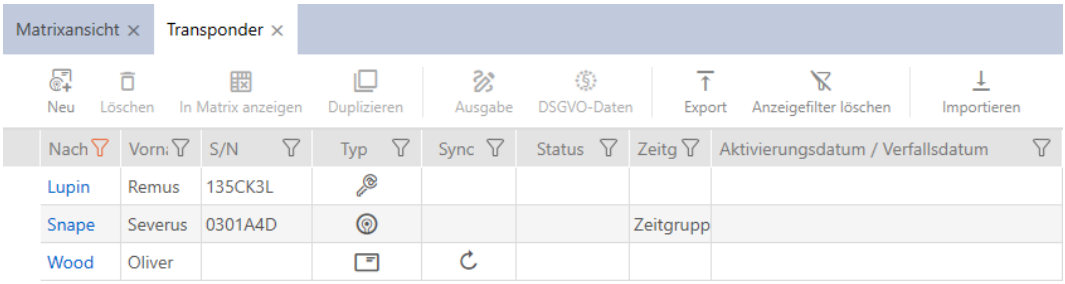
1. Klicken Sie in einer der angezeigten Spalten- oder Zeilenüberschriften auf die Schaltfläche ▽.
   ↳ Filtermenü öffnet sich.



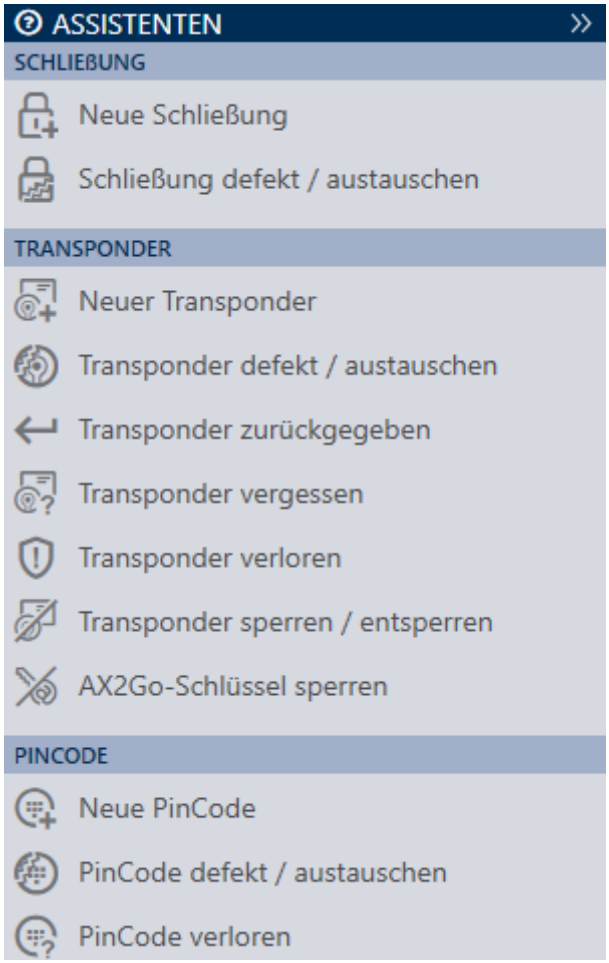
2. Stellen Sie die Filter ein.



3. Klicken Sie auf die Schaltfläche OK.
   ↳ Filtermenü schließt sich.
   ↳ Einträge werden gefiltert angezeigt.



13.2 Assistenten



Die Assistenten im Assistentenbereich helfen Ihnen, bestimmte Aufgaben schnell und sicher durchzuführen. Klicken Sie einfach auf den entsprechenden Assistenten. Der Assistent stellt Fragen und gibt Hintergrundinformationen. Anhand Ihrer Antworten führt Sie der Assistent durch die Problemlösung.

Falls Sie mehr Platz brauchen, können Sie das Assistenten-Menü mit `>>` ausblenden und mit `<<` einblenden.

13.3 Mehrere Möglichkeiten, gleiches Ergebnis

In diesem Handbuch wird in der Regel nur ein Weg beschrieben, um etwas Bestimmtes zu tun. Das bedeutet aber nicht, dass dies der einzige Weg ist.

Oft haben Sie mehrere Möglichkeiten, dasselbe Ergebnis zu erreichen.

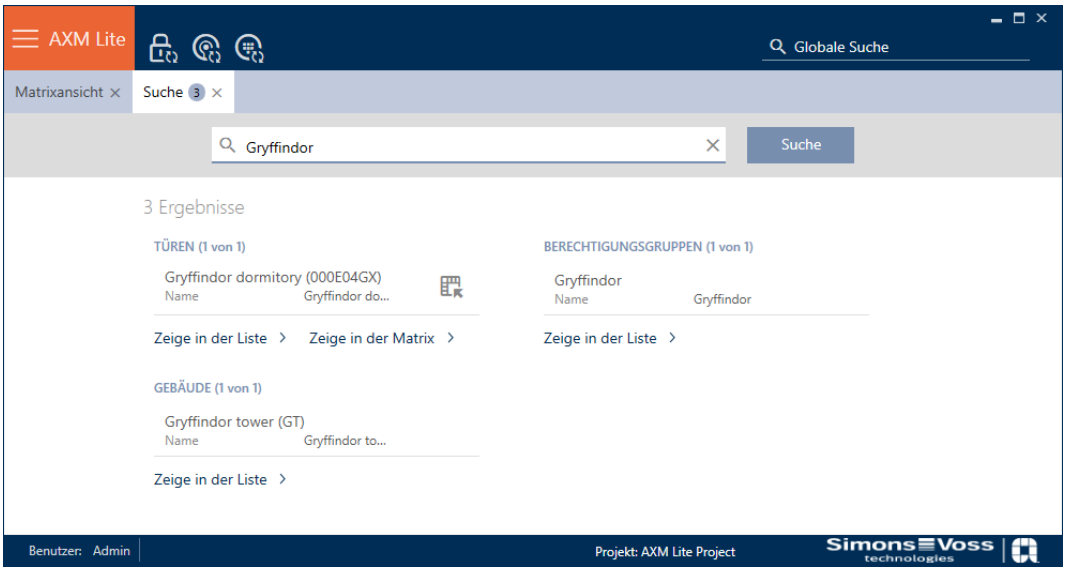
Sie können zum Beispiel einen Eintrag in der Matrix auf zwei Wege löschen:

1. Über die Matrixleiste: Löschen
2. Über das Kontextmenü: Löschen

Beide Wege löschen den Eintrag.

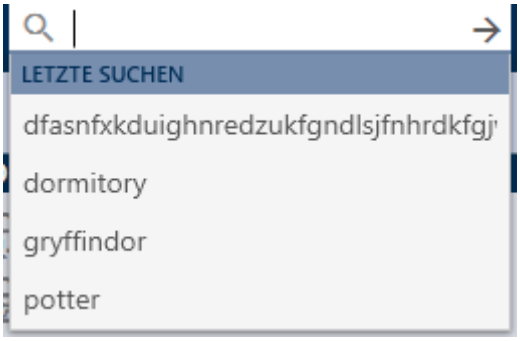
13.4 Globale Suche

Die globale Suche in der AXM Plus durchsucht alle Einträge und listet sie in einer Übersicht auf:



Über die Schaltflächen Zeige in der Matrix bzw. [Zeige in der Liste] kommen Sie direkt zum gesuchten Eintrag in der Matrix- oder der Listenansicht.

Bei der Suche unterstützt Sie die AXM Plus, indem Ihnen letzten Suchbegriffe im Suchfeld automatisch als Dropdown-Menü angeboten werden:



13.5 Effizienter arbeiten mit der AXM

13.5.1 Tab-Bedienung

Die AXM Plus ermöglicht es Ihnen mit einer innovativen Tab-Steuerung, mehrere Aufgaben gleichzeitig zu bearbeiten. Lassen Sie einfach mehrere Tabs gleichzeitig geöffnet.

Häufig benutzte Tabs können Sie auch automatisch beim Start öffnen lassen (siehe *Tabs pinnen [▸ 461]*).

Manche Tabs werden im Vordergrund als Fenster geöffnet und müssen erst wieder geschlossen werden, bevor Sie etwas anderes machen können. Dazu gehören unter anderem diese Tabs:

- [Projektsicherung]
- [Benutzerkennwort ändern]
- [EINSTELLUNGEN]
- [Programmiergeräte]
- [Über AX Manager]

Sie erkennen solche Tabs daran, dass beim Öffnen der Rest der AXM Plus ausgegraut wird.

13.5.2 Hotkeys

Tastenkombination	Reaktion
Tab	Springt zum nächsten Eingabefeld.
Shift+Tab	Springt zum vorherigen Eingabefeld.
Strg+Tab	Springt zum nächsten Tab.

Tastenkombination	Reaktion
Strg+Shift+Tab	Springt zum vorherigen Tab.
Strg+Z	Macht die letzte Aktion rückgängig (z.B. versehentliches Text löschen in einem Eingabefeld)

13.5.3 Weitere Objekte erstellen

Häufig ist es so, dass Sie mehrere Objekte mit denselben oder ähnlichen Einstellungen erstellen wollen.

Ein Beispiel wären mehrere Identmedien, die zum Beispiel dieselben zeitlichen Regelungen haben sollen.

Hier hilft Ihnen die AXM Plus und bietet in vielen Fenstern die Checkbox ☑ Weiteres Objekt erstellen an. Wenn Sie diese Checkbox aktivieren, dann bleibt das aktuelle Fenster mit denselben Einstellungen geöffnet.

Beispiel: Sie erstellen einen Transponder und aktivieren die Checkbox. Jetzt klicken Sie auf die Schaltfläche Fertigstellen. Der gewünschte Transponder wird angelegt, gleichzeitig bleibt aber das Fenster mit denselben Einstellungen weiter geöffnet. So müssen Sie für den nächsten Transponder nicht alles erneut einstellen, sondern nur einen neuen Namen eingeben.

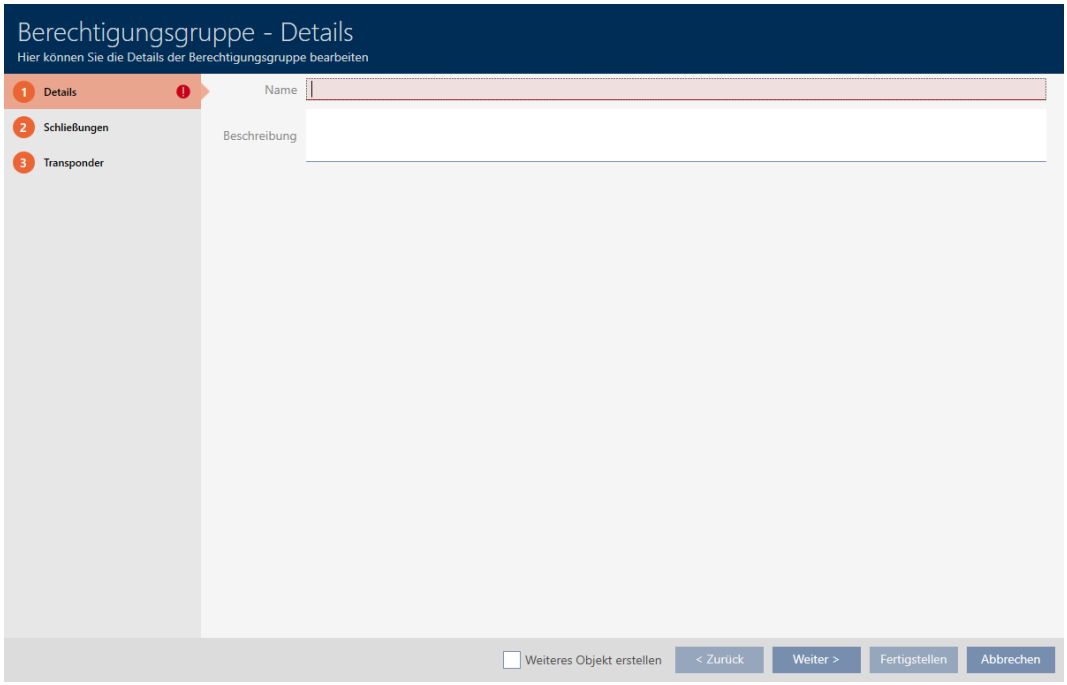
14. Organisationsstruktur

14.1 Berechtigungsgruppen erstellen

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Berechtigungsgruppen aus.
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Berechtigungsgruppen] öffnet sich.

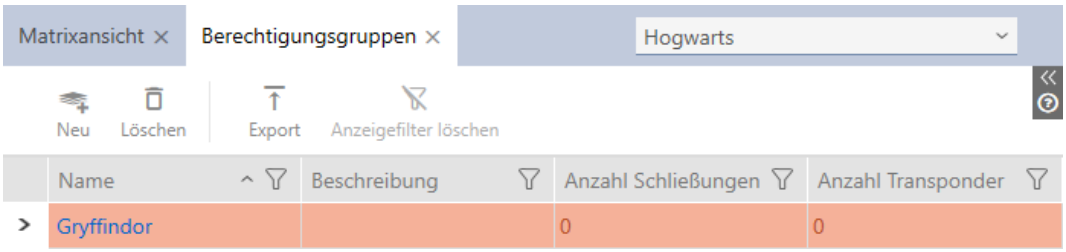
3. Klicken Sie auf die Schaltfläche Neu.
   ↳ Fenster einer neuen Berechtigungsgruppe öffnet sich.



4. Geben Sie im Feld *Name* einen Namen für Ihre Berechtigungsgruppe ein.

5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der neuen Berechtigungsgruppe schließt sich.

↳ Neue Berechtigungsgruppe wird aufgelistet.

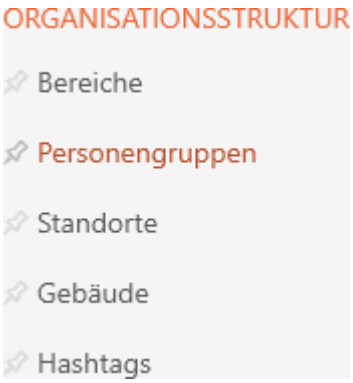


14.2 Personengruppe erstellen

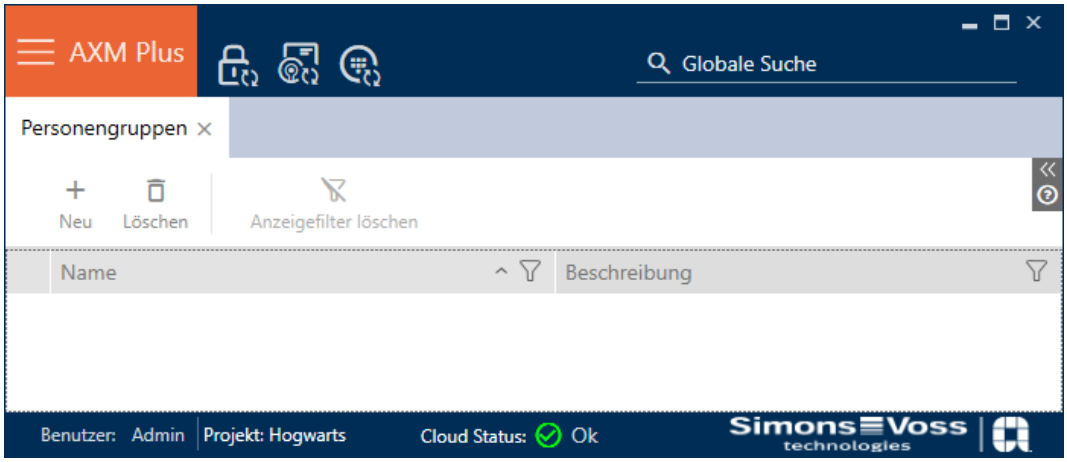
Personengruppen sind eine sehr nützliche Strukturierung Ihrer Schließanlage (siehe auch *Personengruppen [▸ 565]*).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

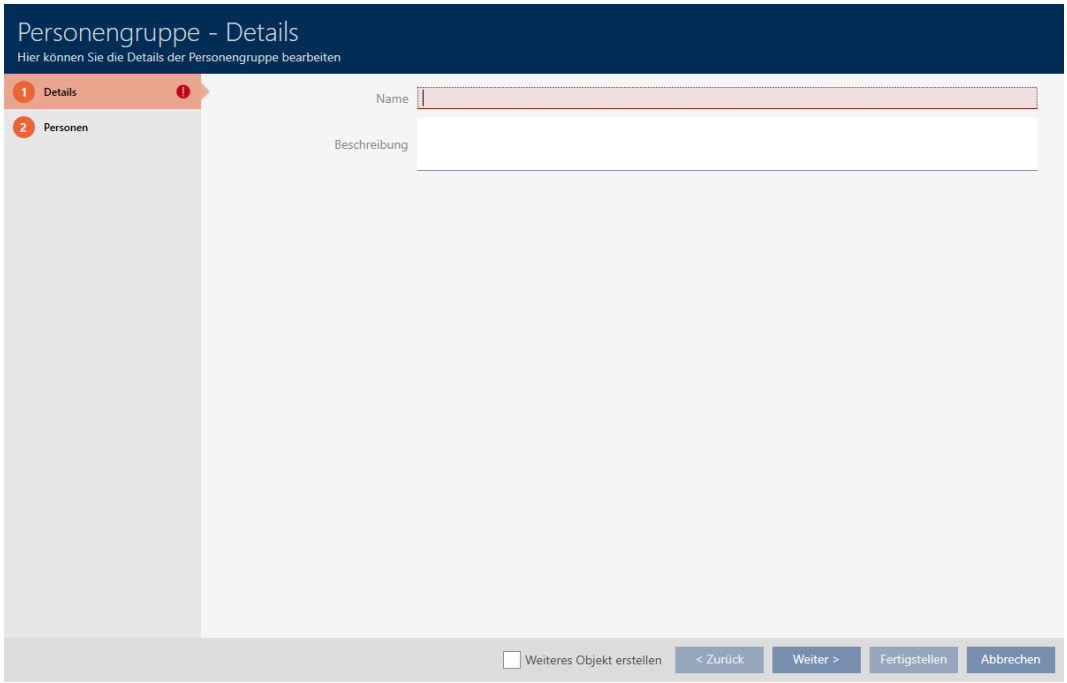
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Personengruppen aus.



   ↳ Tab [Personengruppen] öffnet sich.

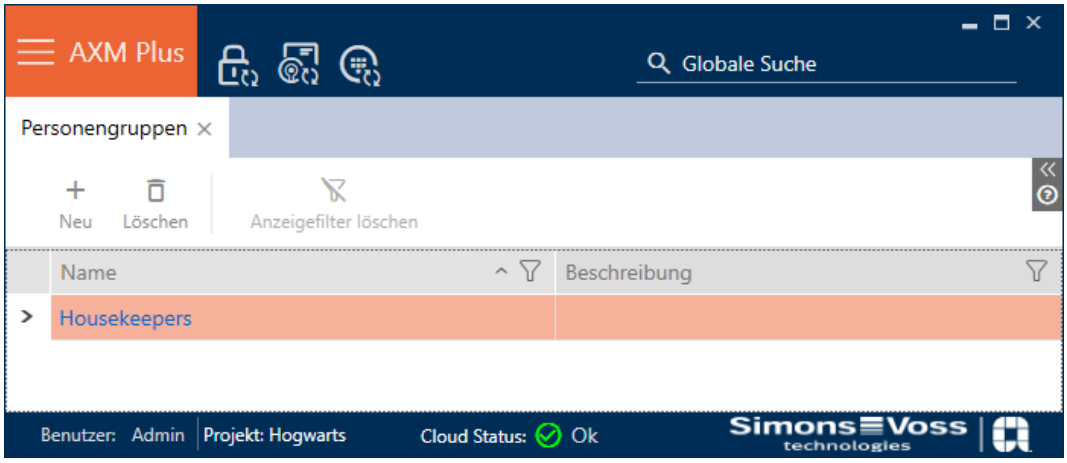


3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster "Personengruppe" öffnet sich.



4. Geben Sie im Feld *Name* den Namen Ihrer Personengruppe ein.
5. Geben Sie im Feld *Beschreibung* ggfs. eine Beschreibung Ihrer Personengruppe ein.
6. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Personengruppe" schließt sich.

↳ Neu erstellte Personengruppe wird aufgelistet.



14.3 Zeitplan erstellen

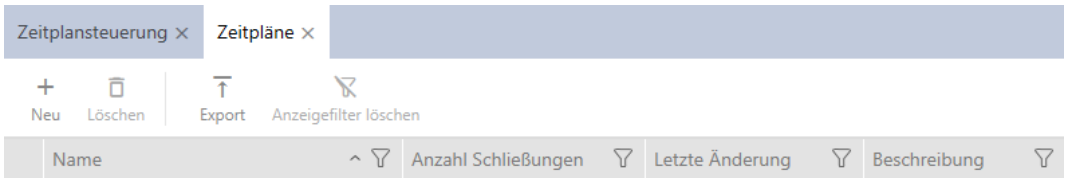
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

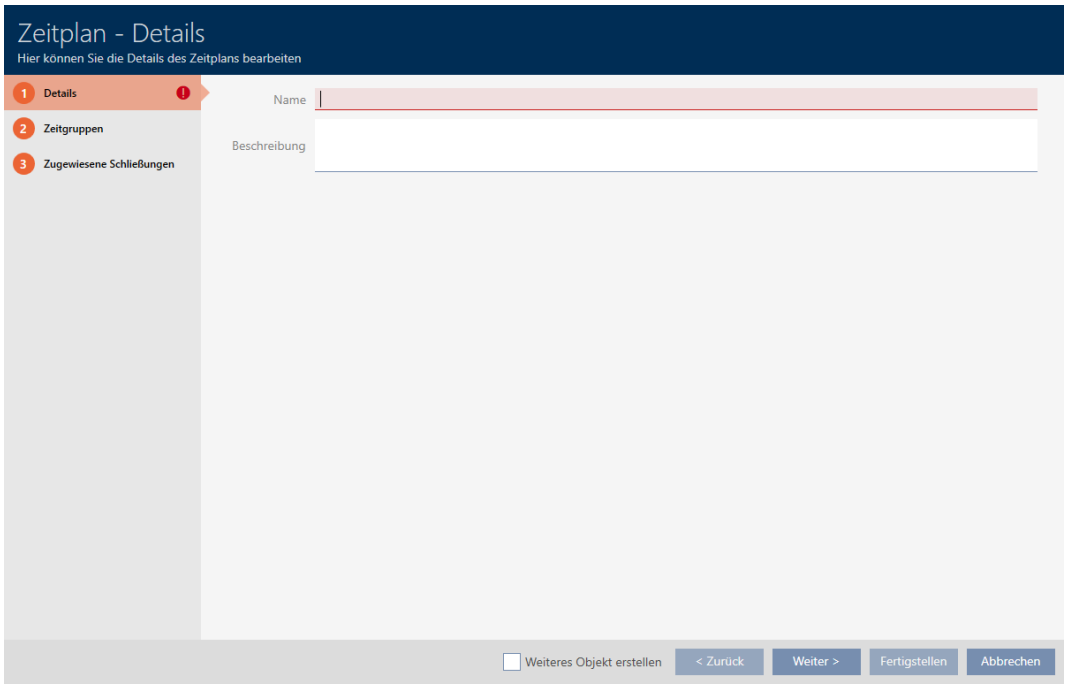
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Zeitplansteuerung] öffnet sich.

3. Klicken Sie auf die Schaltfläche Zeitpläne.

↳ Tab [Zeitpläne] öffnet sich.

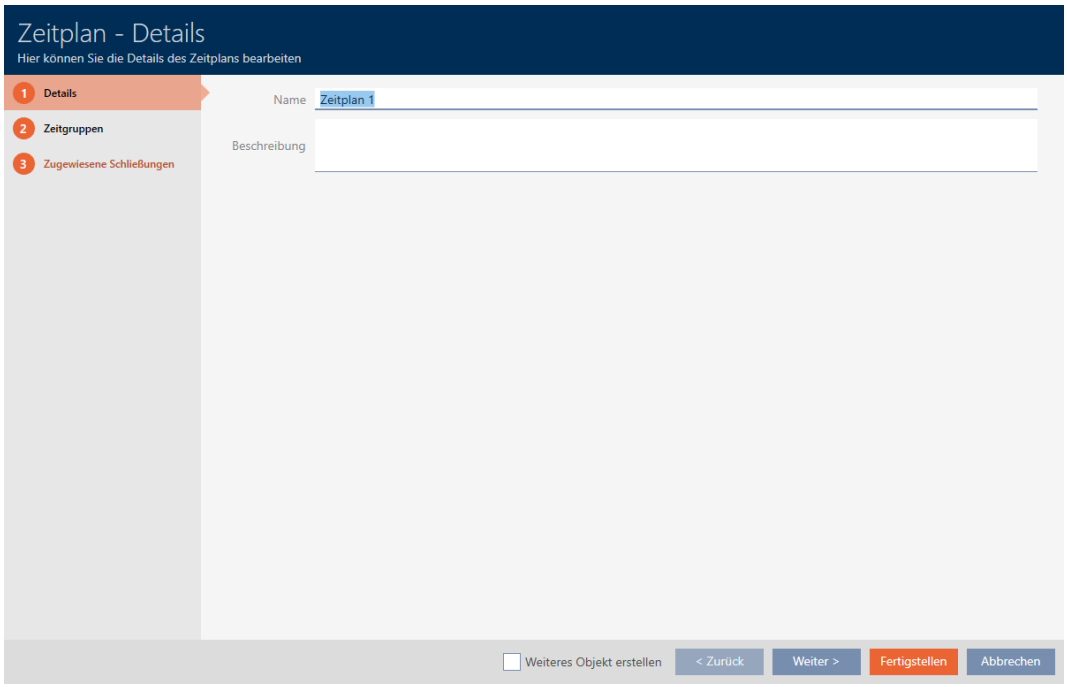


4. Klicken Sie auf die Schaltfläche Neu.
   ↳ Fenster zum Erstellen eines Zeitplans öffnet sich.

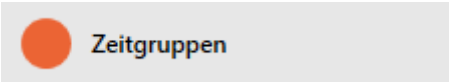


5. Geben Sie im Feld *Name* einen Namen für den Zeitplan ein.

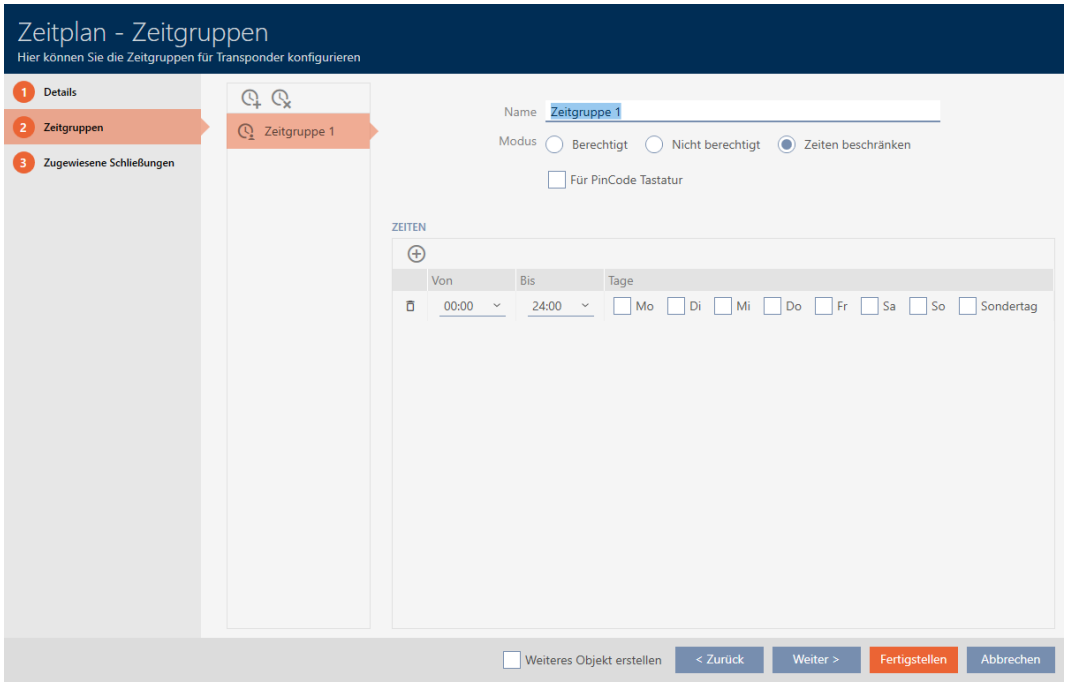
6. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.



7. Klicken Sie auf en Reiter Zeitgruppen.



↳ Fenster wechselt zum Reiter "Zeitgruppen".



HINWEIS

Erste Zeitgruppe automatisch erstellt

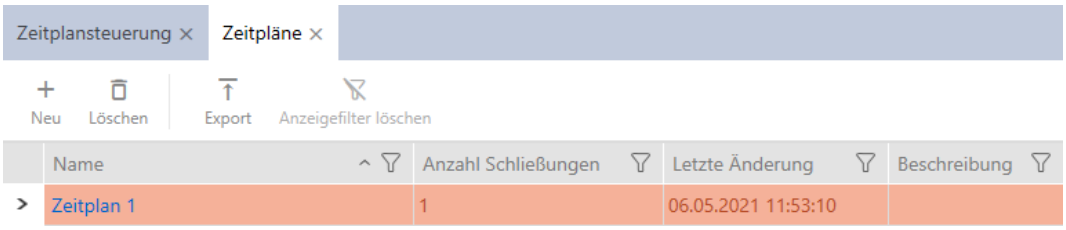
Für das Zeitmanagement der AXM Plus benötigen Sie mindestens eine Zeitgruppe. Deshalb erstellt die AXM Plus automatisch eine Zeitgruppe für Sie.

- Aktivieren Sie in dieser Zeitgruppe mindestens einen Tag.

↳ Die automatisch erstellte Zeitgruppe ist gültig und der Zeitplan kann fertiggestellt werden.

8. Wenn Sie Ihre Zeitgruppen noch nicht erstellt haben: Erstellen Sie die Zeitgruppen (siehe *Zeitgruppe erstellen [▸ 61]*).
   Wenn Sie Ihre Zeitgruppen bereits in einem anderen Zeitplan erstellt haben: Stellen Sie die Zeitgruppen für diesen Zeitplan ein.
   ↳ Zeitplan ist erstellt und das Fenster zum Erstellen eines Zeitplans schließt sich. Fahren Sie ggfs. mit *Identmedium zur Zeitgruppe hinzufügen [▸ 351]* und *Schließungen zum Zeitplan hinzufügen [▸ 348]* fort.

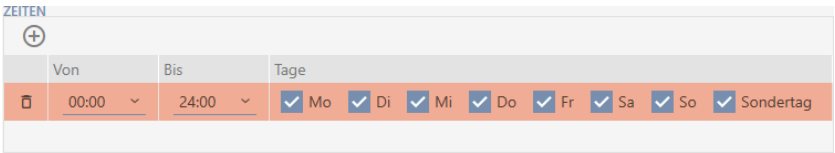
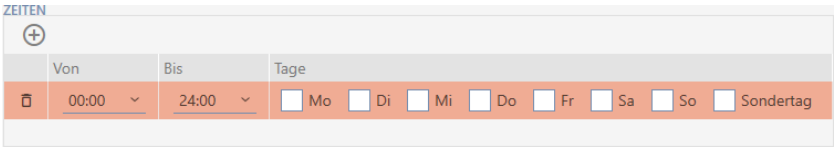
↳ Zeitplan ist erstellt und wird aufgelistet.

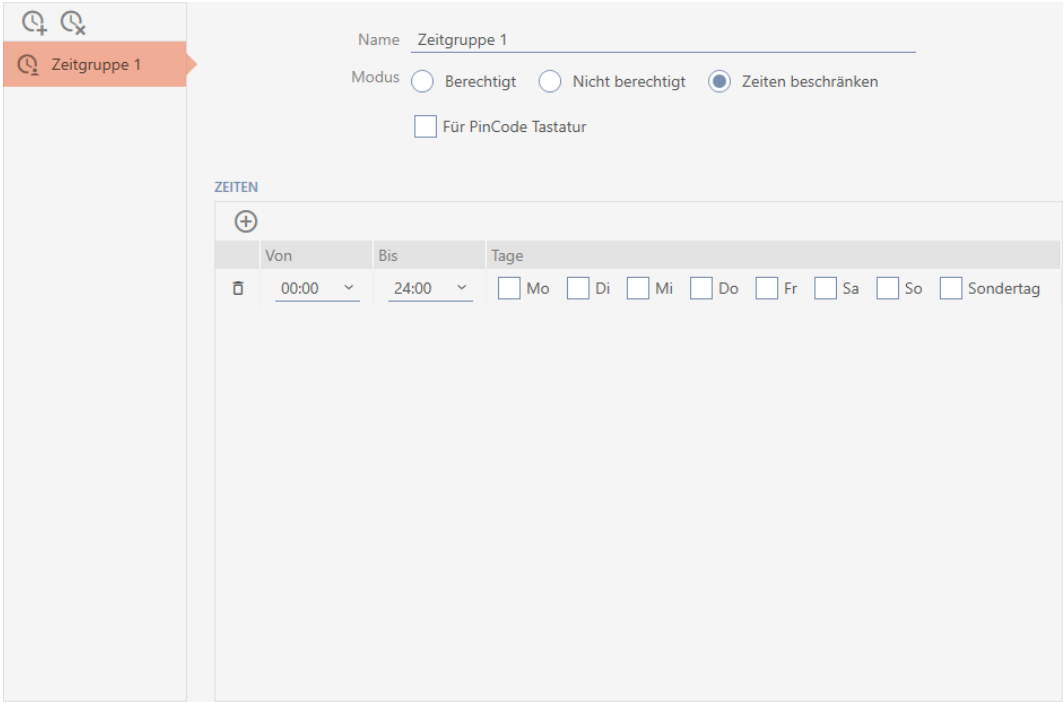


14.4 Zeitgruppe erstellen

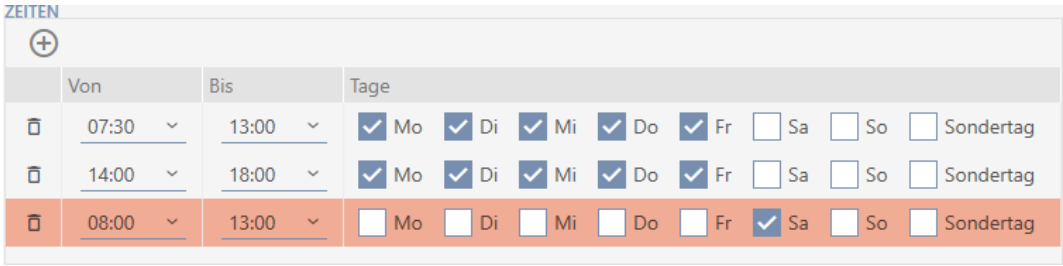
Grundsätzlich gilt: Alle Einstellungen in einer Zeitgruppe gelten pro Zeitplan.

Innerhalb einer Zeitgruppe können Sie für jeden Zeitplan aus einem der drei Modi wählen:

◉ Berechtigt	Alle Identmedien in dieser Zeitgruppe sind an allen Schließungen in diesem Zeitplan wie in der Matrix bzw. Berechtigungsgruppen angegeben berechtigt. ◉ Berechtigt entspricht einer Zeitenbeschränkung, die an allen Tagen und 0-24 Uhr zulässt (also effektiv gar keine Beschränkung ist), siehe Bild:  Wenn Sie versuchen, diese Zeitenbeschränkung so abzuspeichern, dann ändert die AXM Plus den Modus automatisch in ◉ Berechtigt.
◉ Nicht berechtigt	Alle Identmedien in dieser Zeitgruppe sind an keiner der Schließungen in diesem Zeitplan berechtigt, auch dann nicht, wenn sie in der Matrix berechtigt wären. ◉ Nicht berechtigt entspricht einer Zeitenbeschränkung, die an keinem Tag zulässt (also effektiv immer beschränkt), siehe Bild: 
◉ Zeiten beschränken	Alle Identmedien in dieser Zeitgruppe sind an allen Schließungen in diesem Zeitplan wie in der Matrix bzw. Berechtigungsgruppen angegeben berechtigt, wenn eines der eingestellten Zeitintervalle zutrifft.



Das raffinierte Konzept der Zeitintervalle und Tage erlaubt Ihnen auch Kombinationen aus Intervallen und Tagen, zum Beispiel:



- Unterschiedliche Zeitintervalle für dieselben Tage (z.B. ein Geschäft hat zwischen 13:00 und 14:00 Mittagspause)
- Unterschiedliche Zeitintervalle für unterschiedliche Tage (z.B. ein Geschäft ist samstags nur vormittags geöffnet)

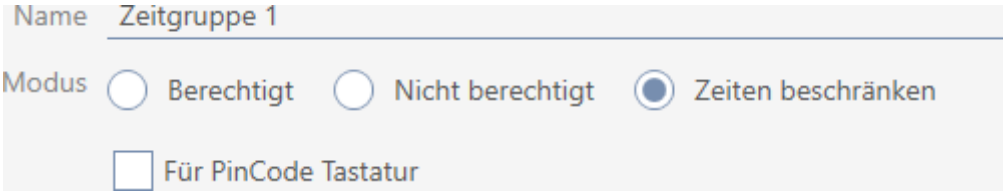
Weitere Informationen siehe *Zeitgruppen und Zeitpläne [▸ 548]*.

Die Checkbox ☑ Sondertag spielt für Feiertage eine Rolle. Sie legen Feiertage fest und können diese entweder als Wochentag oder als Sondertag behandeln. Wenn das aktuelle Datum ein Feiertag ist und dieser Feiertag als Sondertag behandelt werden soll, dann gilt die Sondertagregelung der Zeitgruppe (siehe *Feiertage erstellen und bearbeiten [▸ 74]*).

Zeitgruppen können Sie über das Zeitplan-Fenster erstellen und einstellen:

✓ Zeitplan erstellt (siehe *Zeitplan erstellen [▸ 58]*).
✓ Zeitplan-Fenster geöffnet (siehe *Zeitplan erstellen [▸ 58]*).

1. Klicken Sie auf die Schaltfläche (außer Sie stellen die automatisch erstellte Zeitgruppe ein).
   ↳ Neue Zeitgruppe wird erstellt.
2. Geben Sie in das Feld *Name* einen Namen für die Zeitgruppe ein.
3. Wählen Sie den Modus Zeiten beschränken.



4. Wenn Sie diese Zeitgruppe für PinCode-Tastatur 3068 (mit G1-Protokoll) verwenden wollen: Aktivieren Sie die Checkbox Für PinCode G1.

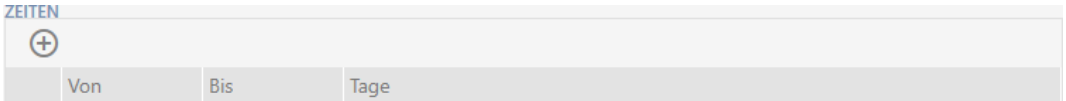
HINWEIS

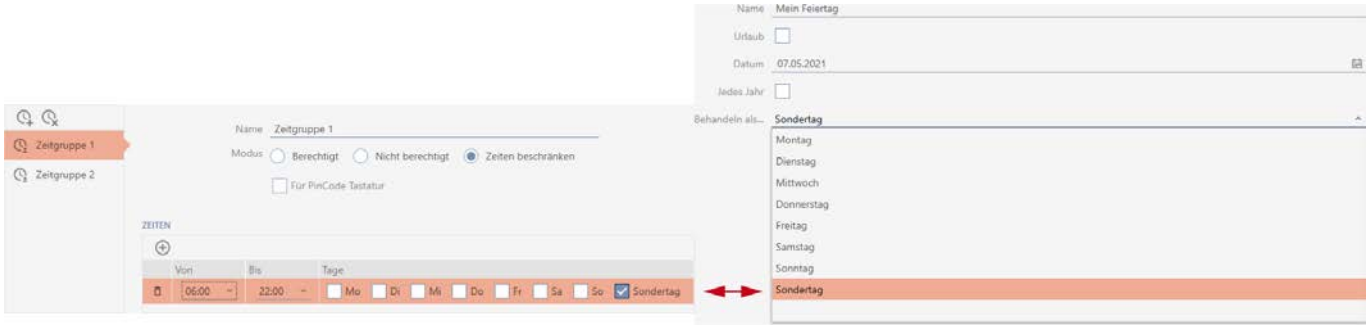
Zeitgruppen für PinCode-Tastaturen

PinCode-Tastaturen verwenden das G1-Protokoll. Deshalb sind für PinCode-Tastaturen eigene Zeitgruppen erforderlich. Diese Zeitgruppen können auch ausschließlich für PinCode-Tastaturen verwendet werden.

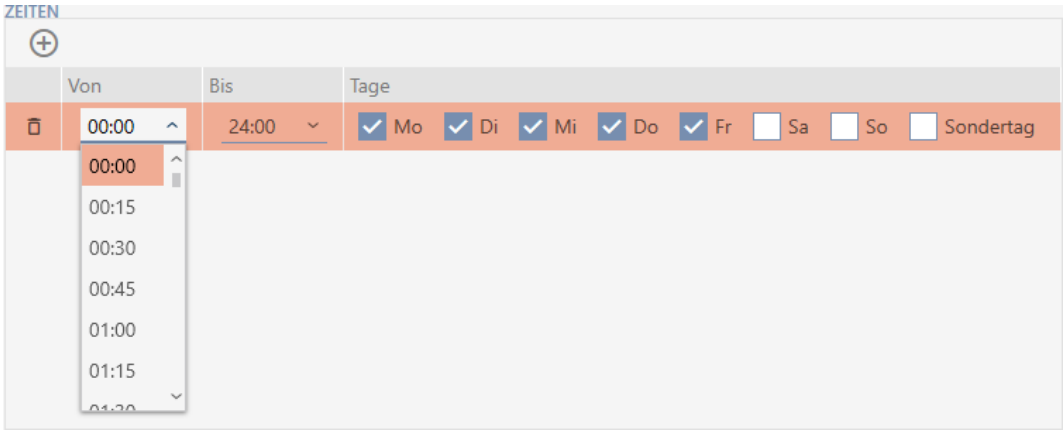
Bereits erstellte Zeitgruppen können nicht nachträglich für PinCode-Tastaturen verwendet werden.

5. Aktivieren Sie die Tage für das erste Zeitintervall (Checkboxen Mo, Di, Mi, Do, Fr, Sa, So und Sondertag).



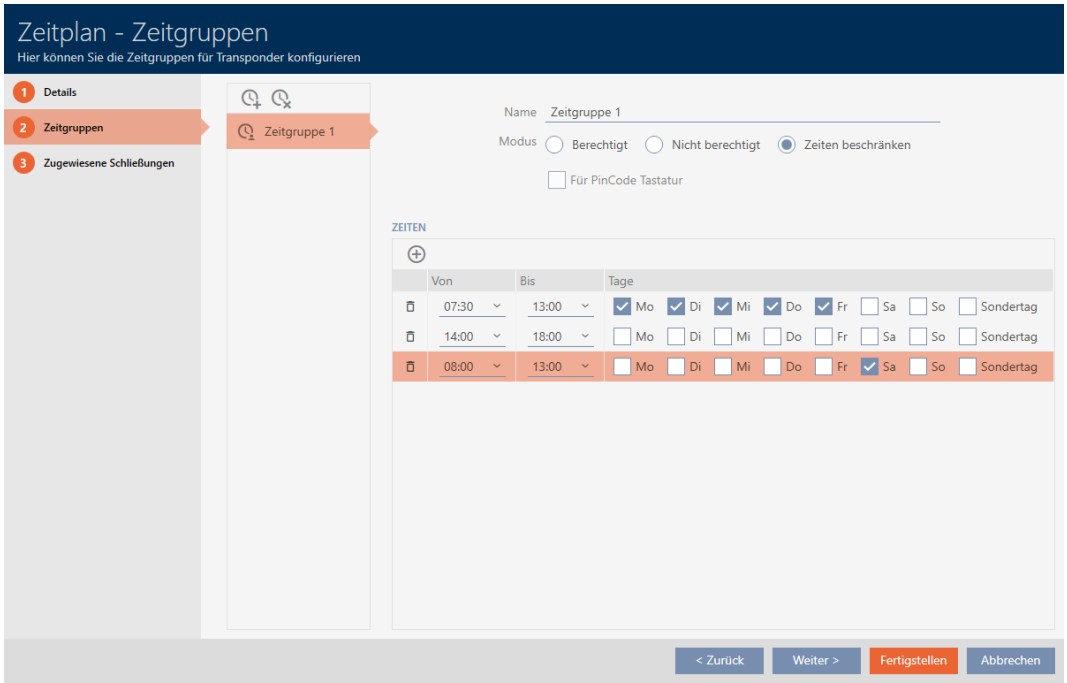


6. Stellen Sie die Zeit für die markierten Tage ein.



↳ Erstes Zeitintervall festgelegt.

7. Legen Sie ggfs. über die Schaltfläche ⊕ weitere Zeitintervalle an.



8. Klicken Sie auf die Schaltfläche Fertigstellen oder erstellen Sie ggfs. mit der Schaltfläche weitere Zeitgruppen.

↳ Zeitgruppe ist erstellt und für den aktuell ausgewählten Zeitplan eingestellt.

HINWEIS

Neue Zeitgruppen für andere Zeitpläne einstellen

Zeitgruppen sind global. Eine neu erstellte Zeitgruppe existiert deshalb auch in allen anderen Zeitplänen Aus Sicherheitsgründen haben alle Zeitgruppen in einem neuen Zeitplan standardmäßig den Modus Nicht berechtigt.

1. Wechseln Sie nach dem Erstellen einer Zeitgruppe in die anderen Zeitpläne und stellen Sie die Zeitgruppe auch dort ein.
2. Sie können natürlich auch mehrere Zeitgruppen erstellen und erst nachher in den anderen Zeitgruppen einstellen.

14.5 Zeitgruppe löschen

HINWEIS

Zeitgruppen aus allen Zeitplänen löschen

Zeitgruppen sind global für alle Schließanlagen innerhalb eines Projekts verfügbar. Eine gelöschte Zeitgruppe ist im gesamten Projekt gelöscht, nicht nur für einen Zeitplan.

Alle Identmedien, die bisher der gelöschten Zeitgruppe zugeordnet waren, sind dann keiner Zeitgruppe mehr zugeordnet und müssen ggfs. einzeln wieder einer Zeitgruppe hinzugefügt werden (siehe *Identmedium zur Zeitgruppe hinzufügen [▸ 351]*).

- Falls Sie eine Zeitgruppe nur für einen Zeitplan nicht mehr verwenden wollen, stellen Sie die Zeitgruppe auf den Modus Berechtigt.

↳ Identmedien dieser Zeitgruppe können jederzeit die Schließungen öffnen, an denen sie berechtigt sind.

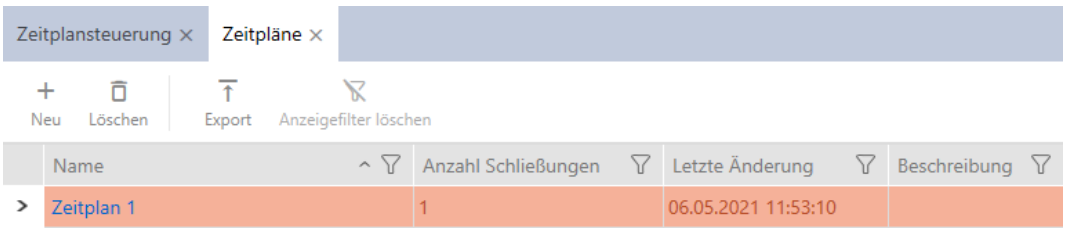
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

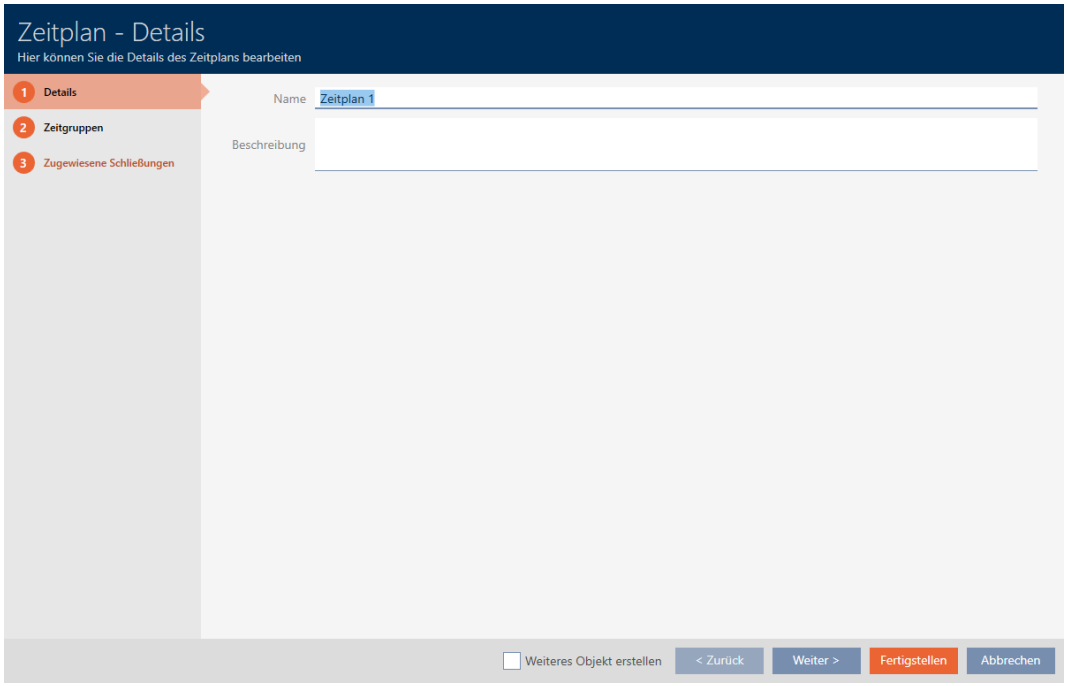
↳ AXM-Leiste klappt zu.
↳ Tab [Zeitplansteuerung] öffnet sich.

3. Klicken Sie auf die Schaltfläche Zeitpläne.

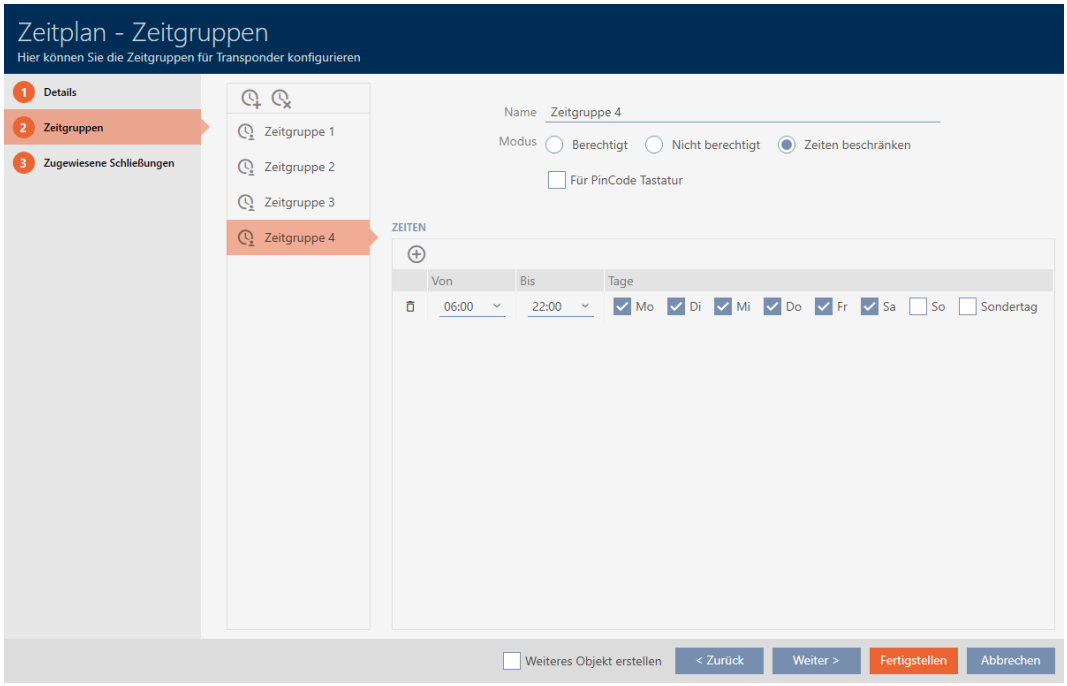
↳ Tab [Zeitpläne] öffnet sich.



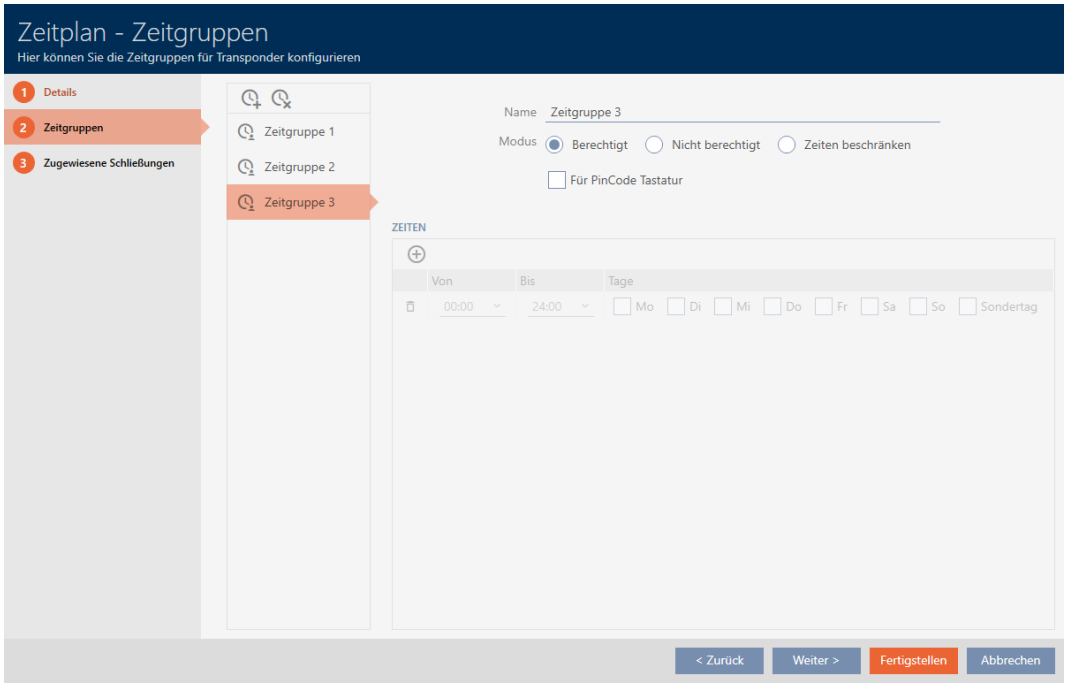
4. Klicken Sie auf einen beliebigen Zeitplan, um dessen Fenster zu öffnen.
↳ Fenster des Zeitplans öffnet sich.



5. Klicken Sie auf den Reiter Zeitgruppen.
   ↳ Fenster wechselt zum Reiter "Zeitgruppen".



6. Markieren Sie die Zeitgruppe, die Sie löschen wollen.
7. Klicken Sie auf die Schaltfläche .
   ↳ Zeitgruppe ist gelöscht.
8. Klicken Sie auf die Schaltfläche Fertigstellen.



14.6 Zeitpläne löschen

✓ Zeitplänen sind keiner Schließung mehr zugewiesen (Zugewiesene Schließungen bearbeiten siehe *Schließungen zum Zeitplan hinzufügen* *[▸ 348]*).

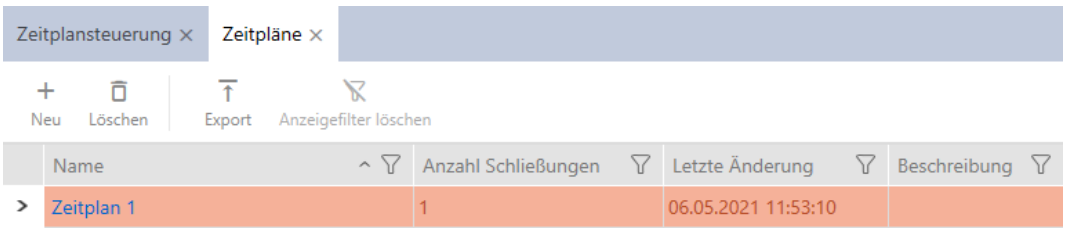
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

↳ AXM-Leiste klappt zu.
↳ Tab [Zeitplansteuerung] öffnet sich.

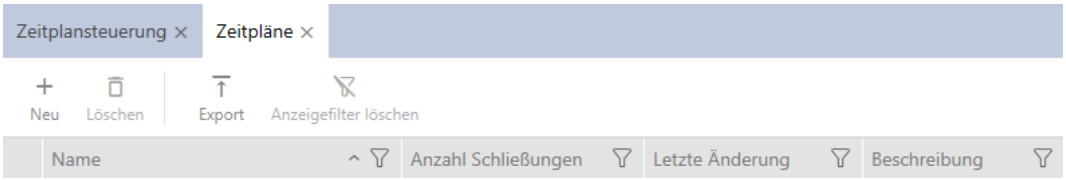
3. Klicken Sie auf die Schaltfläche Zeitpläne.

↳ Tab [Zeitpläne] öffnet sich.



4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
5. Markieren Sie die Zeitpläne, die Sie löschen wollen (Strg+Mausklick für einzelne, Shift+Mausklick für mehrere).
6. Klicken Sie auf die Schaltfläche Löschen.

↳ Zeitpläne sind gelöscht.



14.7 Zeitumschaltung erstellen

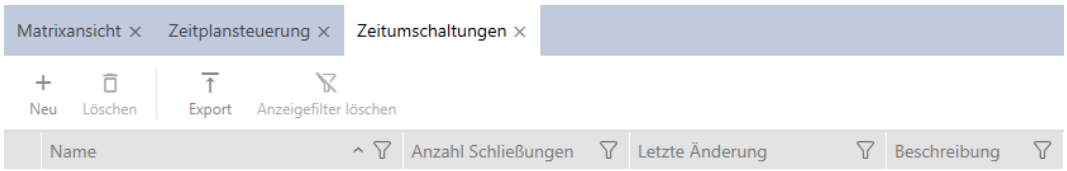
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

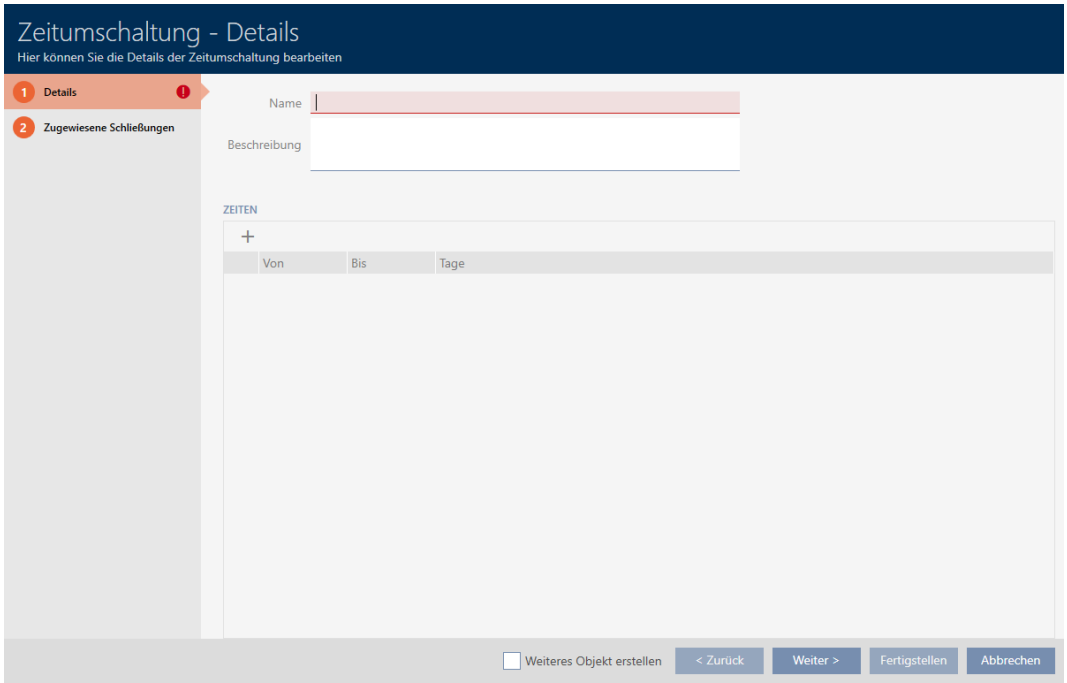
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Zeitplansteuerung] öffnet sich.

3. Klicken Sie auf die Schaltfläche Zeitumschaltungen.

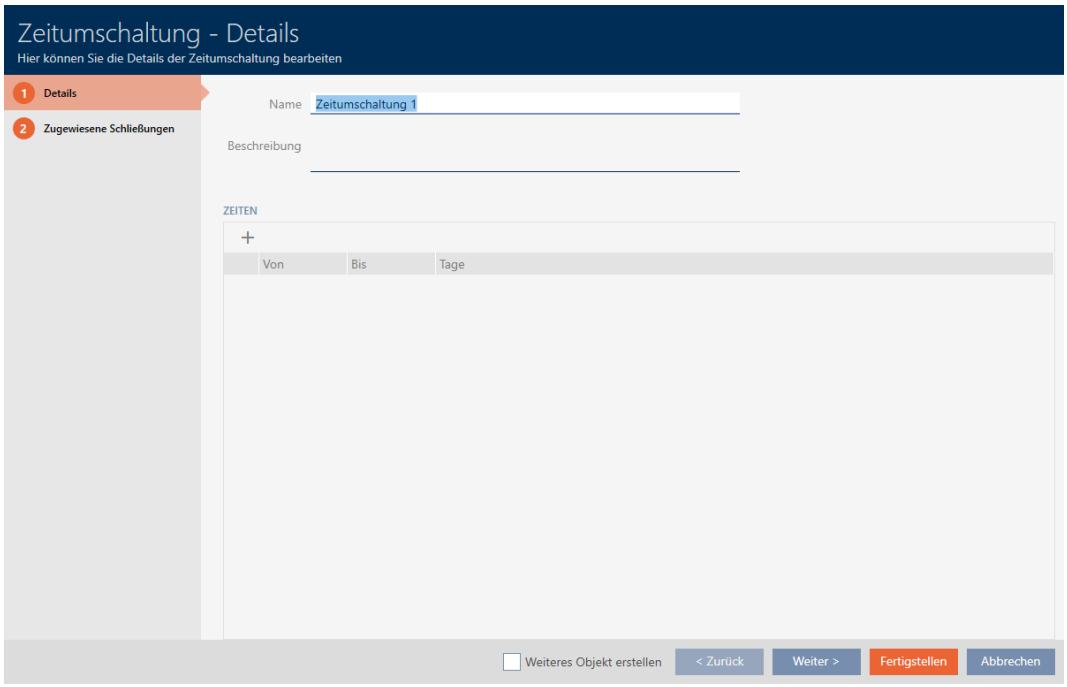
↳ Tab [Zeitumschaltungen] öffnet sich.



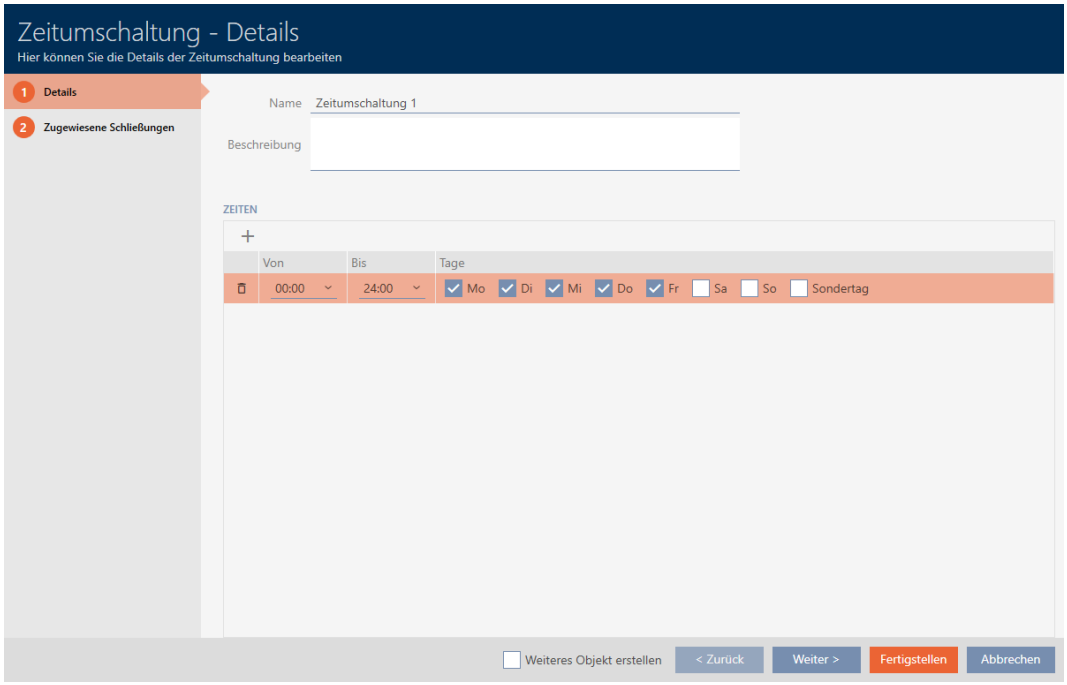
4. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster zum Erstellen einer Zeitumschaltung öffnet sich.



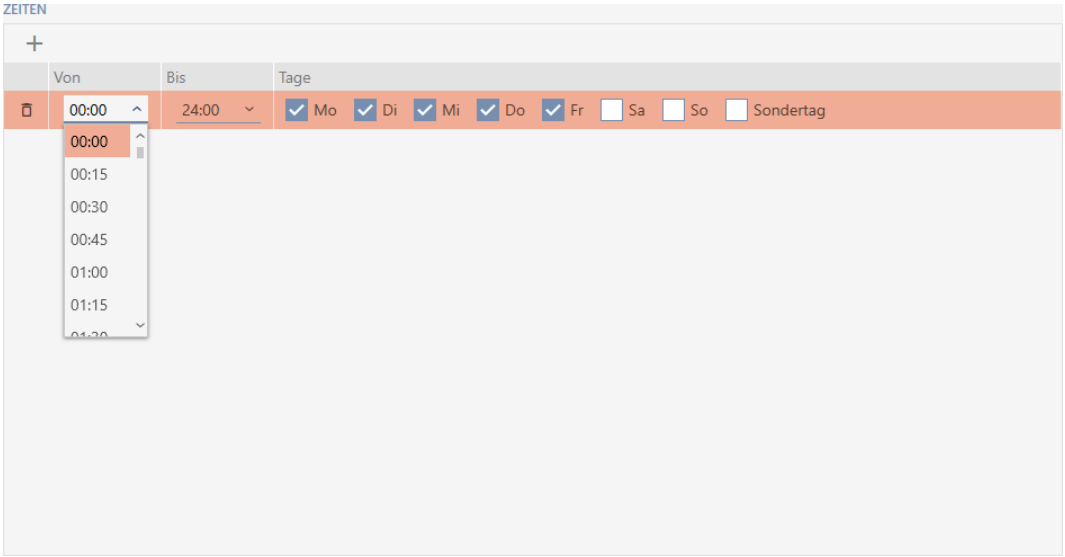
5. Geben Sie im Feld *Name* einen Namen für Ihre Zeitumschaltung ein.



6. Geben Sie ggfs. im Feld *Beschreibung* eine Beschreibung ein.
7. Klicken Sie auf das Symbol **+**, um ein neues Intervall für Ihre Zeitumschaltung anzulegen.
8. Aktivieren Sie die Checkboxen der Wochentage, an denen die Schließung einkuppeln soll (☑ Mo, ☑ Di, ☑ Mi, ☑ Do, ☑ Fr, ☑ Sa, ☑ So, ☑ Sondertag).

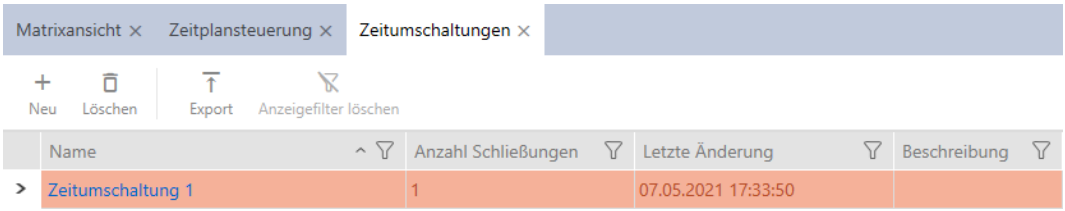


9. Stellen Sie in den Dropdown-Menüs ▼ **Von** und ▼ **Bis** das Zeitintervall für diese Tage ein.



10. Legen Sie ggfs. weitere Zeitintervalle fest.
11. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster zum Erstellen einer Zeitumschaltung schließt sich.

↳ Zeitumschaltung ist erstellt und wird aufgelistet. Fahren Sie ggfs. mit *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]* fort.



14.8 Feiertage erstellen und bearbeiten

HINWEIS

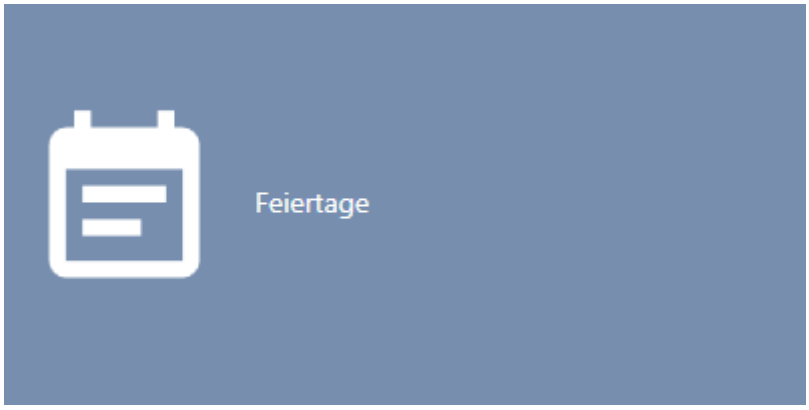
Feiertage in allen Schließanlagen verfügbar

Die Liste der Feiertage ist für alle Schließanlagen innerhalb eines Projekts gleich. Hier erstellte Feiertage sind somit auch in allen anderen Schließanlagen verfügbar.

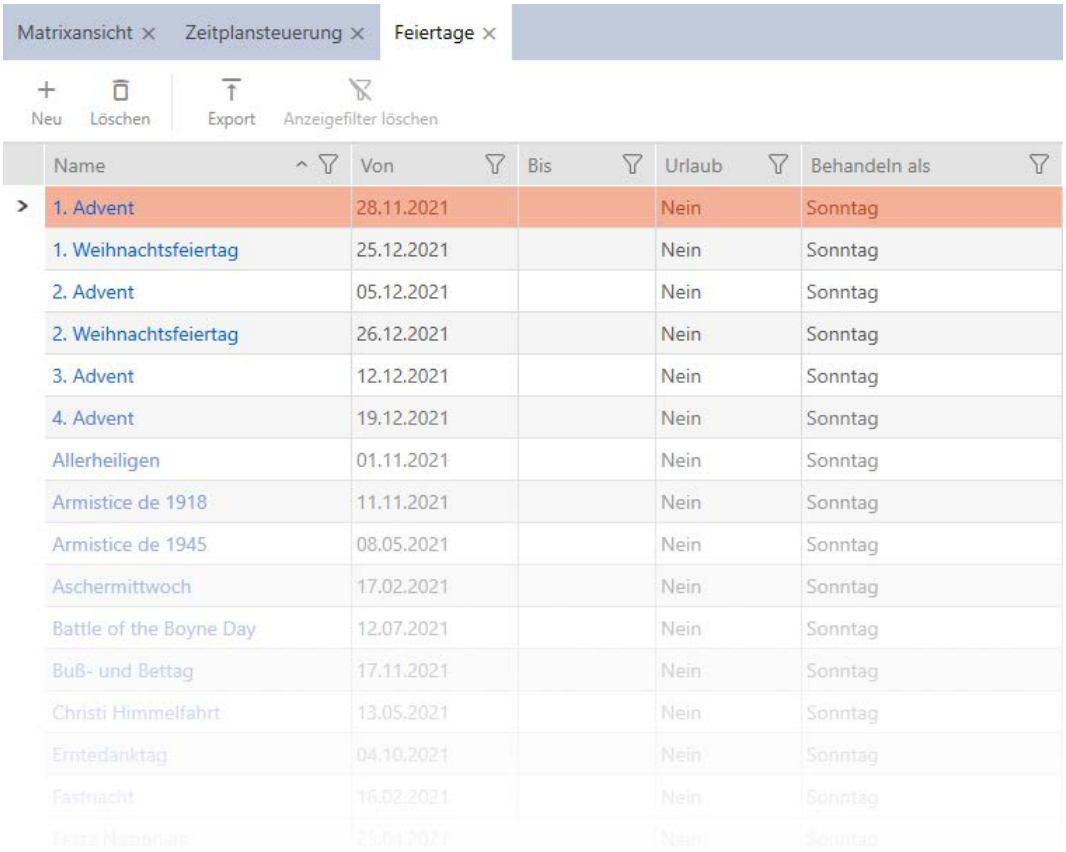
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

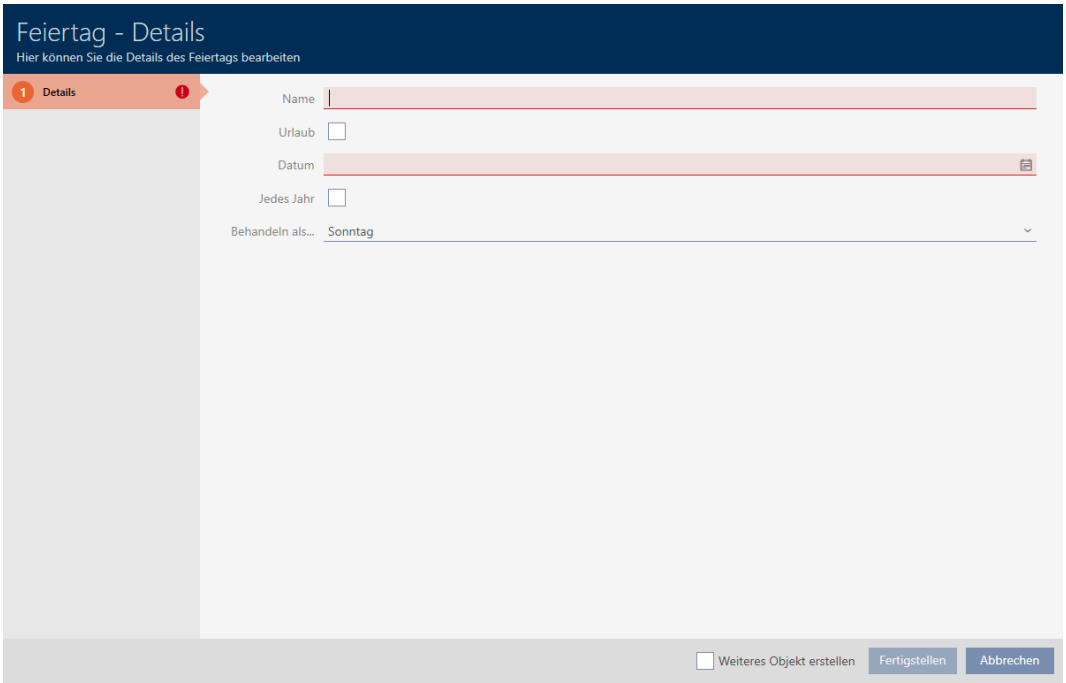
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Zeitplansteuerung] öffnet sich.
3. Klicken Sie auf die Schaltfläche Feiertage.



   ↳ Tab [Feiertage] öffnet sich.

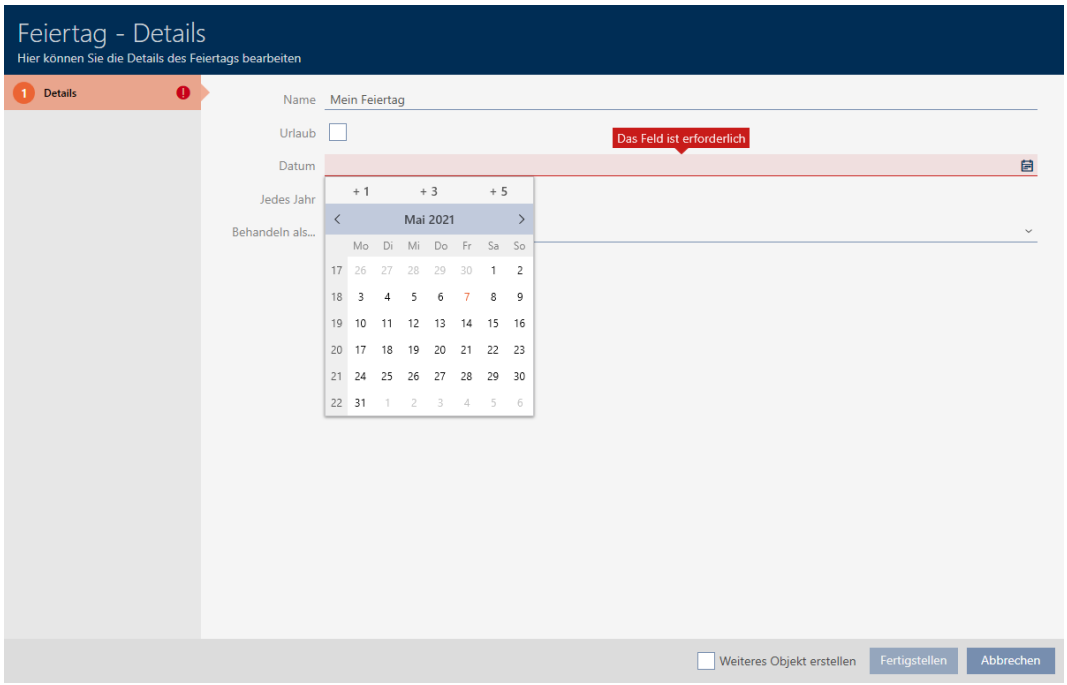


4. Klicken Sie auf die Schaltfläche Neu ➕.
   ↳ Fenster zum Erstellen eines Feiertags öffnet sich.

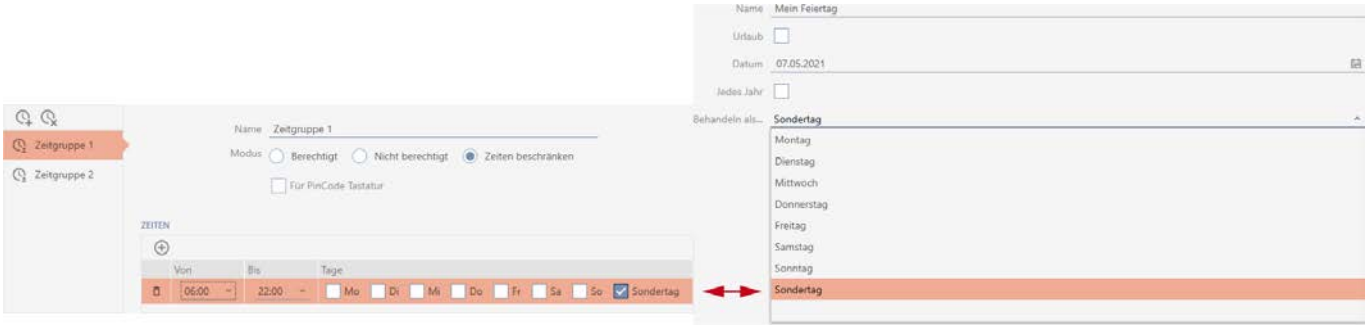


5. Geben Sie im Feld *Name* einen Namen für Ihren Feiertag ein.
6. Wenn Ihr Feiertag ein Urlaubstag ist: Aktivieren Sie die Checkbox ☑ Urlaub.

7. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske auszuklappen.



8. Wählen Sie im Dropdown-Menü ▼ **Behandeln als...** aus, welcher der möglichen Tage im Zeitplan für Ihren Feiertag verwendet werden soll ("Montag", "Dienstag", "Mittwoch", "Donnerstag", "Freitag", "Samstag", "Sonntag", "Sondertag").



9. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster zum Erstellen eines Feiertags schließt sich.

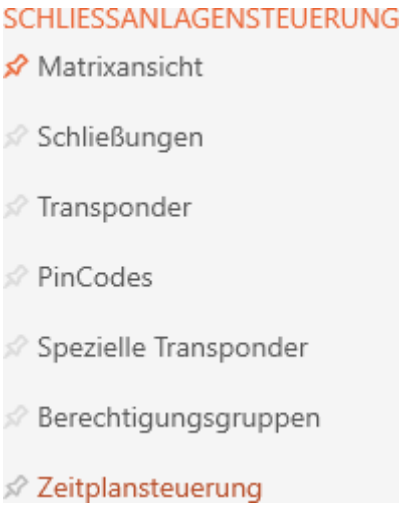
↳ Feiertag ist erstellt und wird aufgelistet.

Heiliger Abend	24.12.2021		Nein	Sonntag
Karfreitag	02.04.2021		Nein	Sonntag
Maifeiertag	01.05.2021		Nein	Sonntag
Maria Empfängnis	08.12.2021		Nein	Sonntag
Maria Himmelfahrt	15.08.2021		Nein	Sonntag
> Mein Feiertag	07.05.2021		Nein	Sonntag
Neujahr	01.01.2021		Nein	Sonntag
Ostermontag	05.04.2021		Nein	Sonntag
Ostersonntag	04.04.2021		Nein	Sonntag
Pfingstmontag	24.05.2021		Nein	Sonntag
Pfingstsonntag	23.05.2021		Nein	Sonntag

14.9 Feiertagslisten erstellen und bearbeiten

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

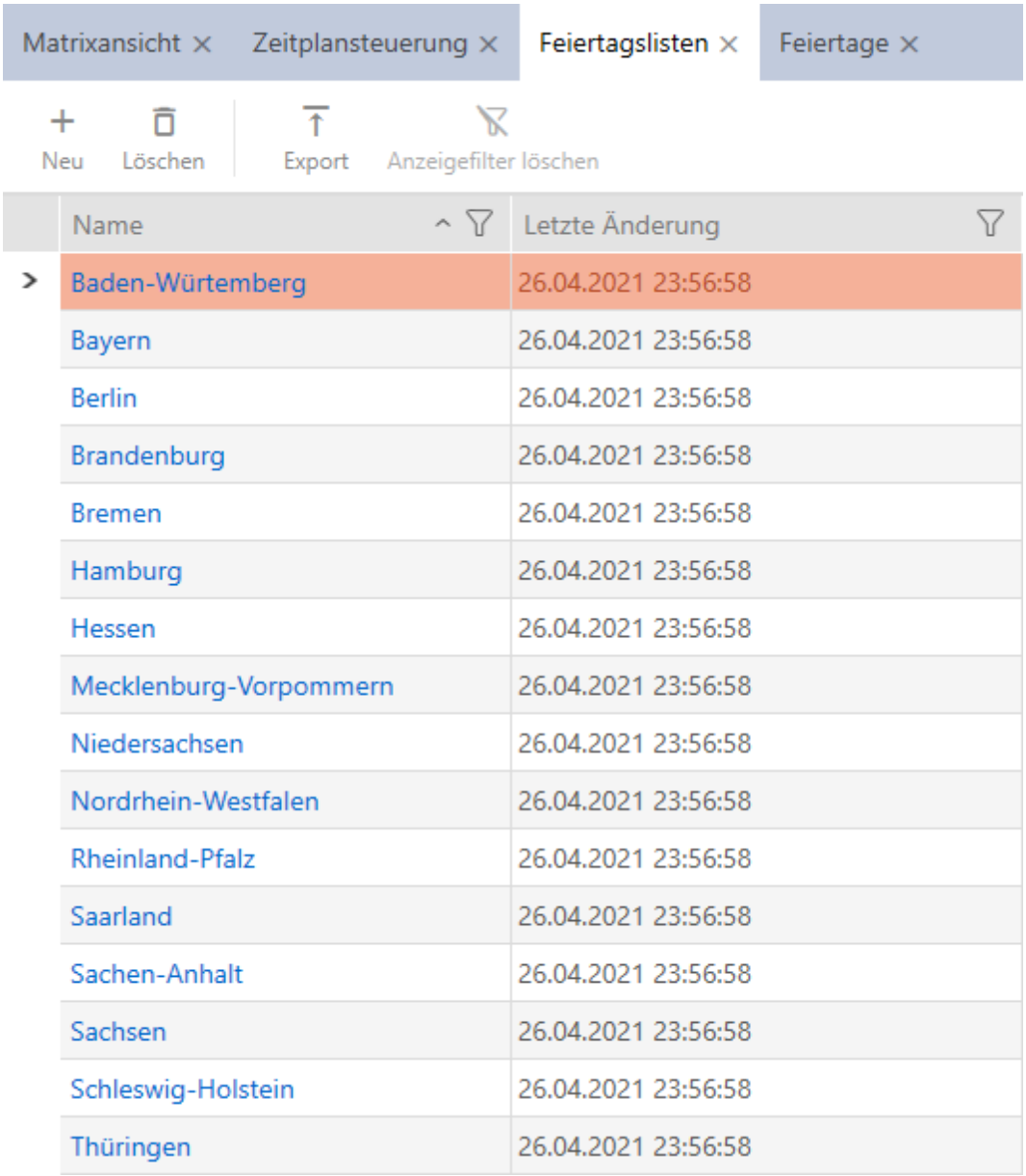
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.



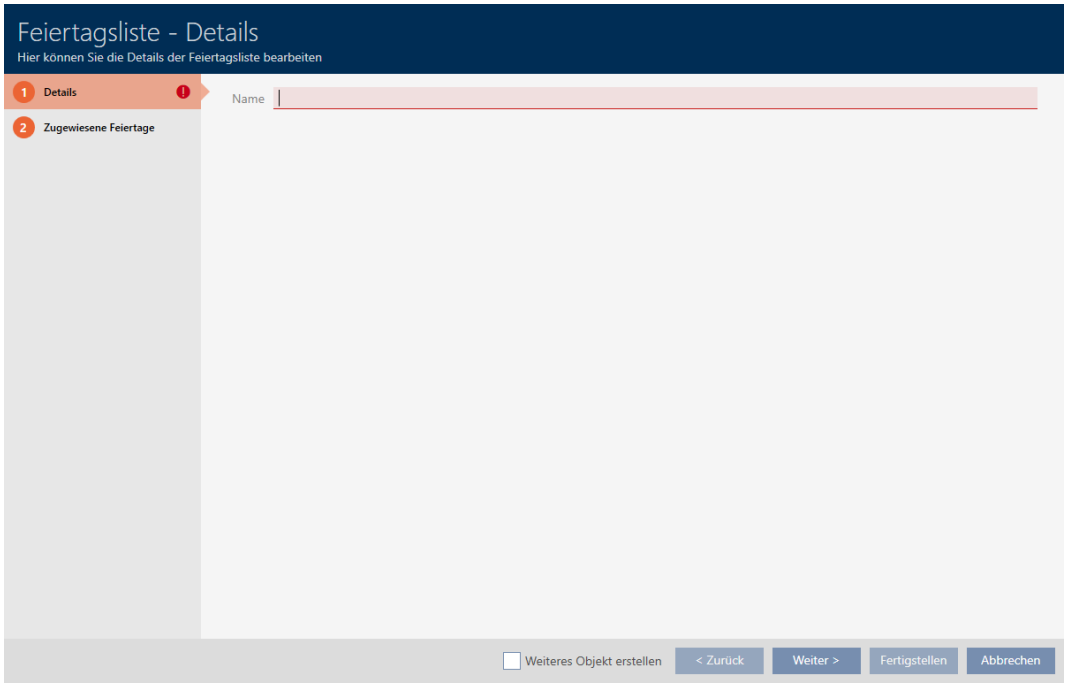
↳ AXM-Leiste klappt zu.
↳ Tab [Zeitplansteuerung] öffnet sich.

3. Klicken Sie auf die Schaltfläche Feiertagslisten.

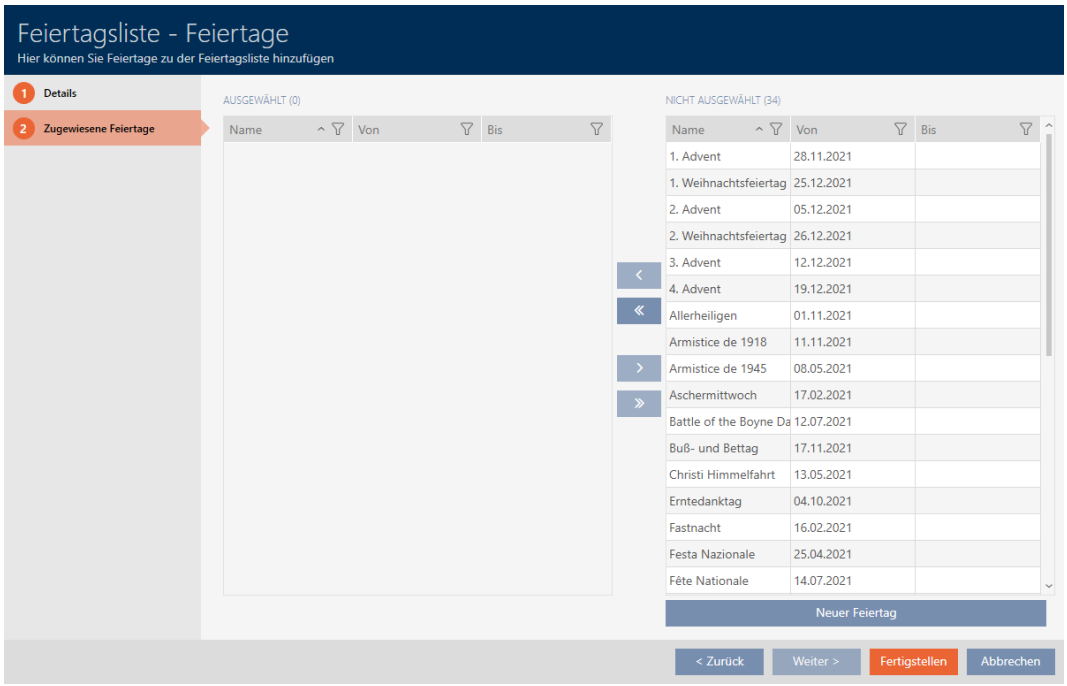
↳ Tab [Feiertagslisten] öffnet sich.



4. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster zum Erstellen einer Feiertagsliste öffnet sich.



5. Geben Sie im Feld *Name* einen Namen für Ihre Feiertagsliste ein.
6. Klicken Sie auf den Reiter Zugewiesene Feiertage.
   ↳ Fenster wechselt zum Reiter "Zugewiesene Feiertage".



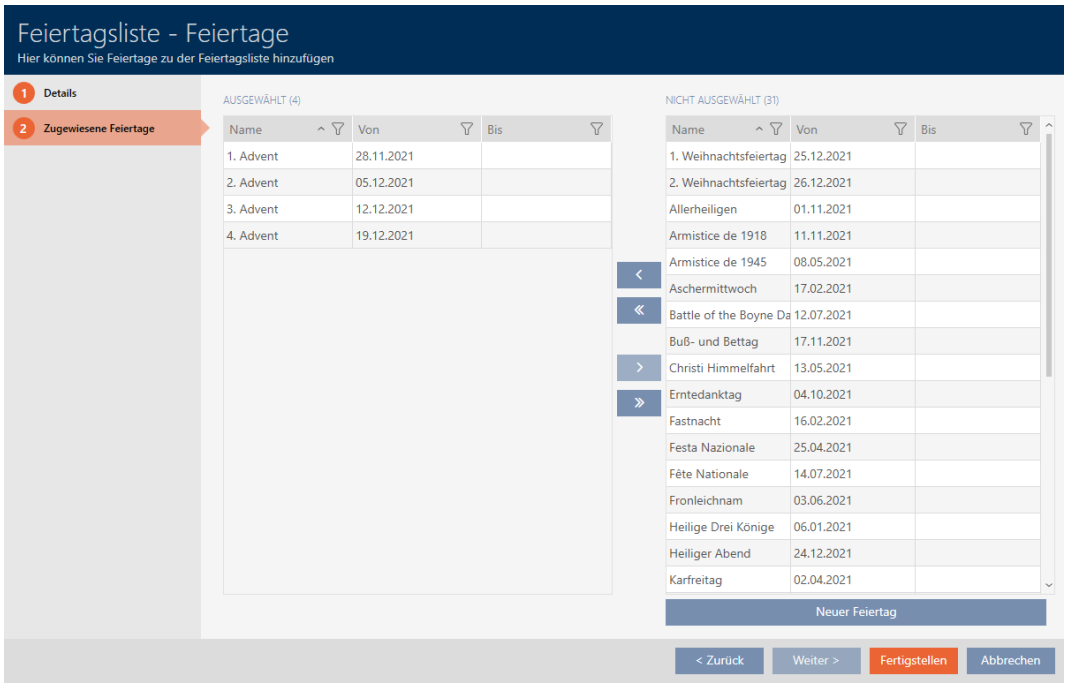
7. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
8. Markieren Sie alle Feiertage, die Sie Ihrer Feiertagsliste zuweisen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

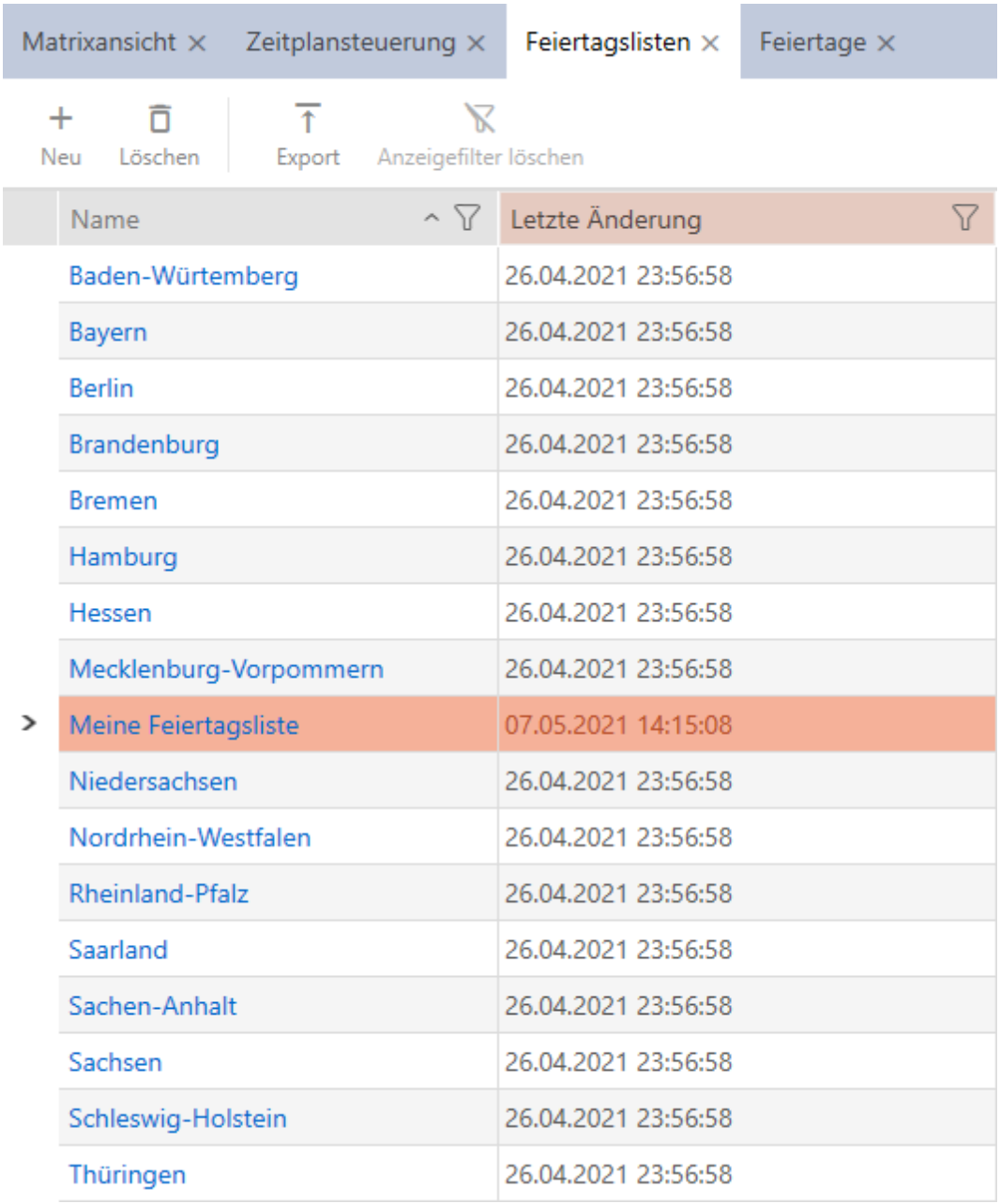
Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

9. Verschieben Sie mit [<] nur die ausgewählten Feiertage oder verschieben Sie mit [«] alle angezeigten Feiertage.
   ↳ Die markierten Feiertage in der linken Spalte werden Ihrer Feiertagsliste hinzugefügt.



10. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster zum Erstellen einer Feiertagsliste schließt sich.

↳ Feiertagsliste ist erstellt und wird aufgelistet.



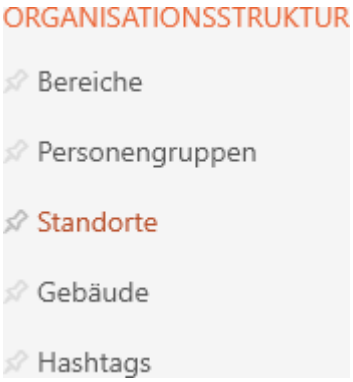
Jetzt können Sie die erstellte Feiertagsliste zum Beispiel Ihren Schließungen hinzufügen: *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]*.

14.10 Standort erstellen

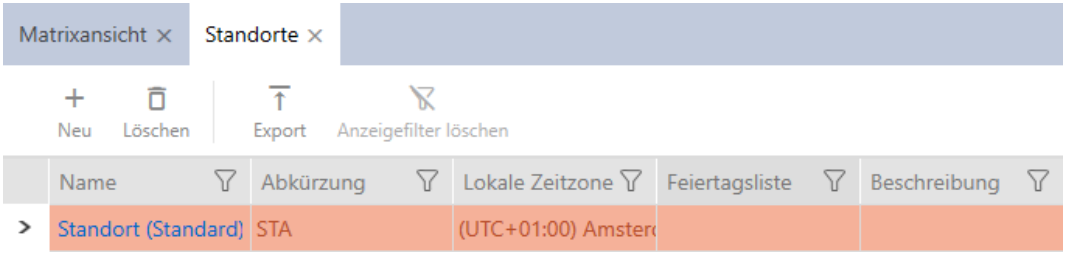
In der Datenbank muss mindestens ein Standort vorhanden sein. Die AXM Plus legt deshalb einen Standard-Standort für Sie an.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

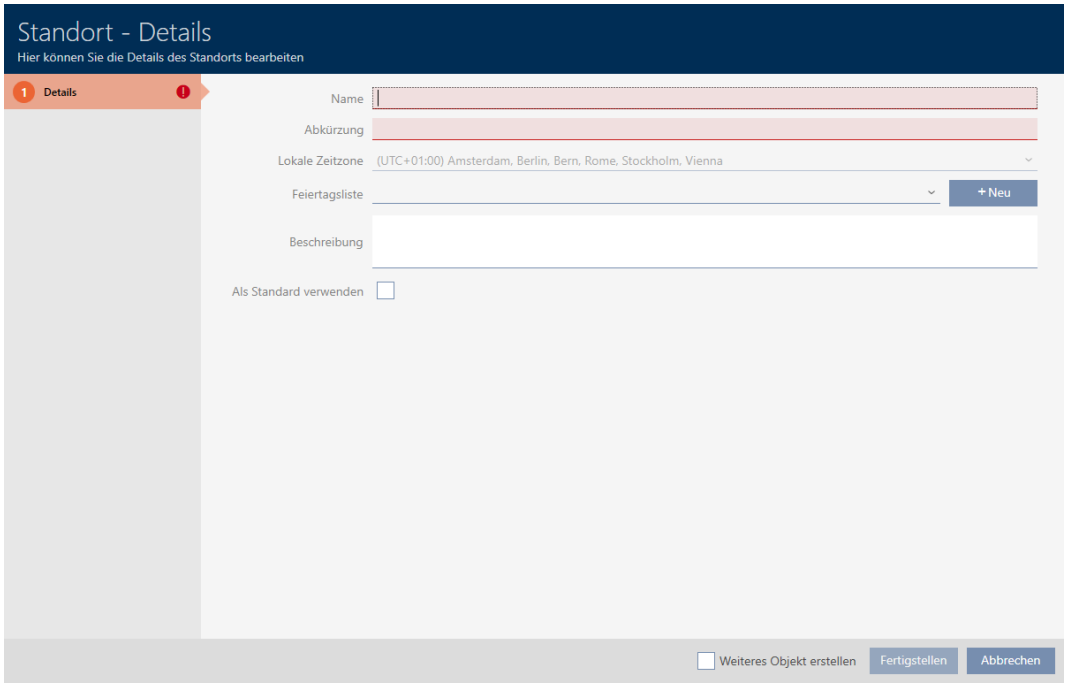
2. Wählen Sie in der Gruppe | ORGANISATIONSSTRUKTUR | den Eintrag Standorte aus.



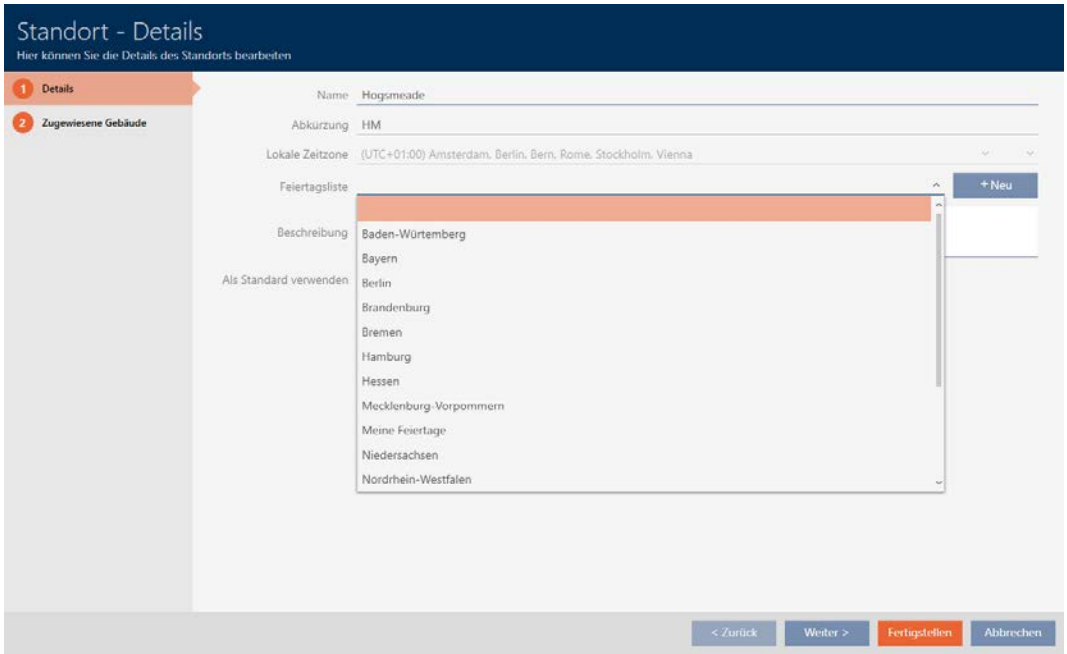
   ↳ Tab [Standorte] öffnet sich.



3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster zum Erstellen eines neuen Standorts öffnet sich.



4. Geben Sie im Feld *Name* den Namen Ihres Standorts ein.
5. Geben Sie im Feld *Abkürzung* die Abkürzung Ihres Standorts ein (max. 5 Zeichen).
6. Wählen Sie im Dropdown-Menü ▼ **Lokale Zeitzone** die Zeitzone Ihres Standorts aus (erst ab AXM Classic einstellbar).
7. Wählen Sie im Dropdown-Menü ▼ **Feiertagsliste** die Feiertagsliste aus, die für Ihren Standort genutzt werden soll (siehe auch *Feiertagslisten erstellen und bearbeiten [▸ 78]*).



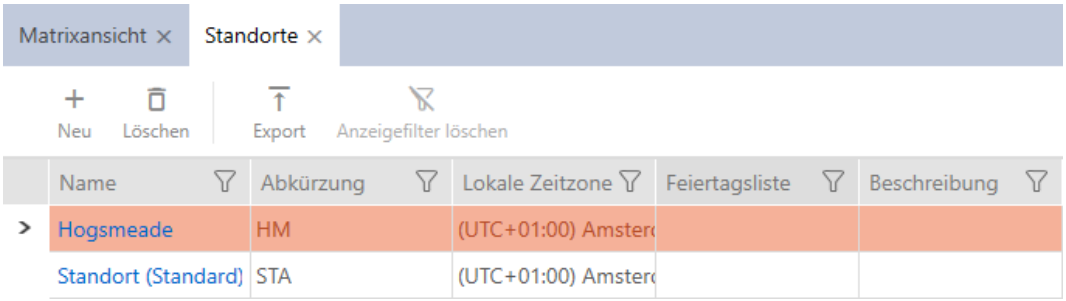
HINWEIS

Feiertagslisten in Schließung und Standorten

Sie können Feiertagslisten sowohl einer Schließung als auch dem Standort der Schließung zuweisen. In diesem Fall wird die Feiertagsliste in der Schließung verwendet und die Feiertagsliste im Standort ignoriert.

Wenn statt der Schließung dem Standort eine Feiertagsliste zugewiesen ist, dann wird die Feiertagsliste des Standorts für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

8. Geben Sie ggfs. im Feld *Beschreibung* eine Beschreibung Ihres Standorts ein.
9. Wenn dieser Standort bei neuen Schließungen/Türen vorausgewählt werden soll, dann markieren Sie die Checkbox Als Standard verwenden.
10. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster zum Erstellen eines neuen Standorts schließt sich.
    ↳ Neu erstellter Standort wird aufgelistet.

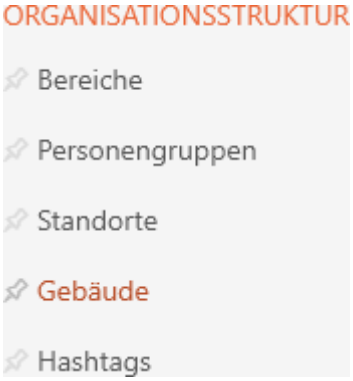


14.11 Gebäude erstellen und zu Standort zuweisen

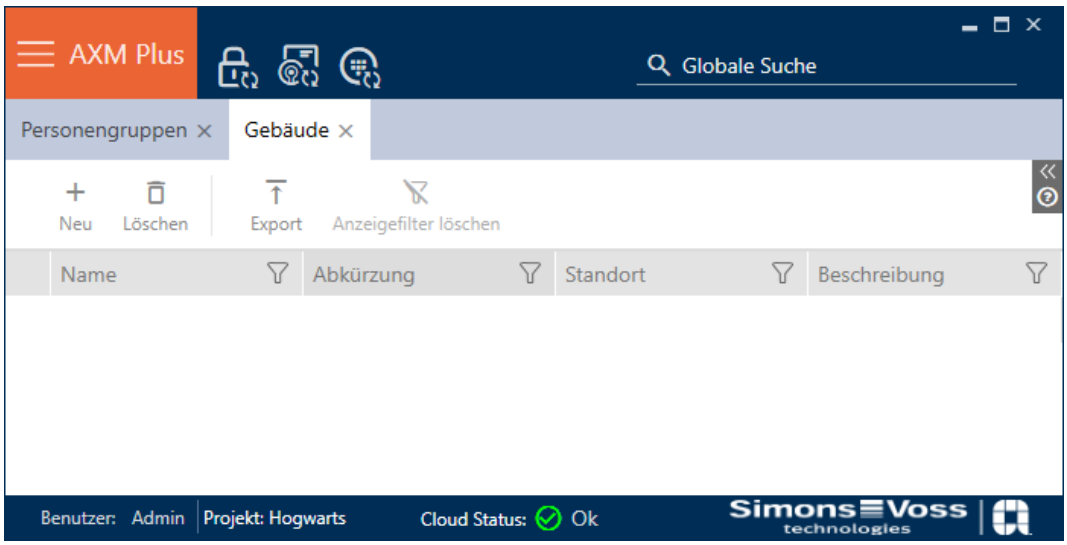
In der Datenbank muss mindestens ein Gebäude vorhanden sein. Die AXM Plus legt deshalb ein Standard-Gebäude für Sie an. Sie können natürlich weitere Gebäude anlegen.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

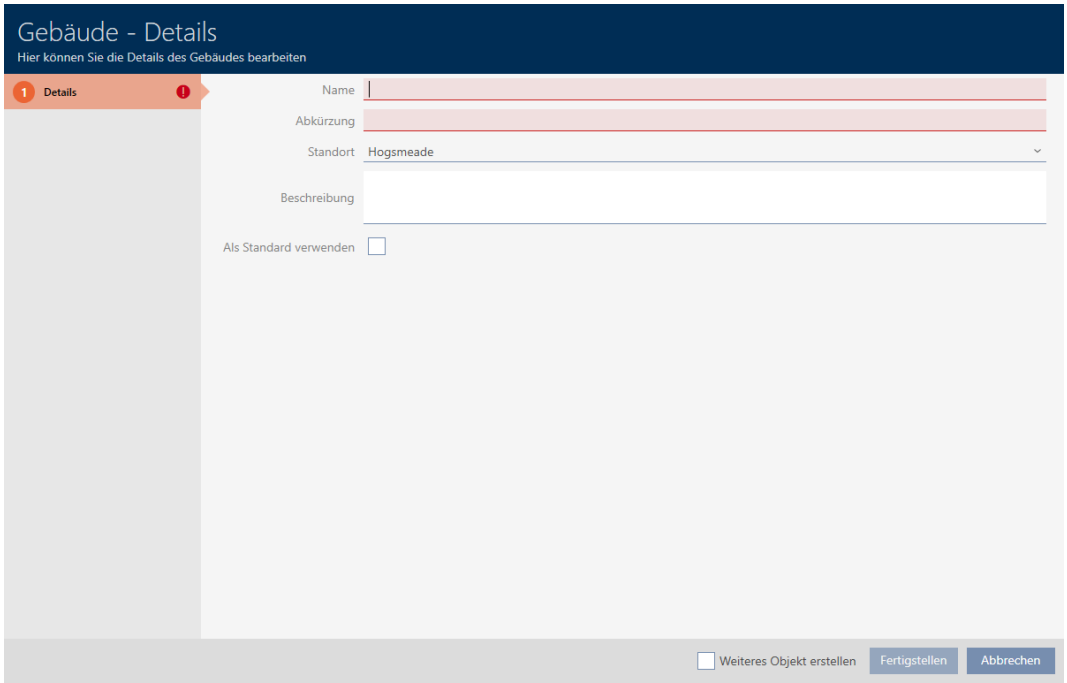
2. Wählen Sie in der Gruppe | ORGANISATIONSSTRUKTUR | den Eintrag Gebäude aus.



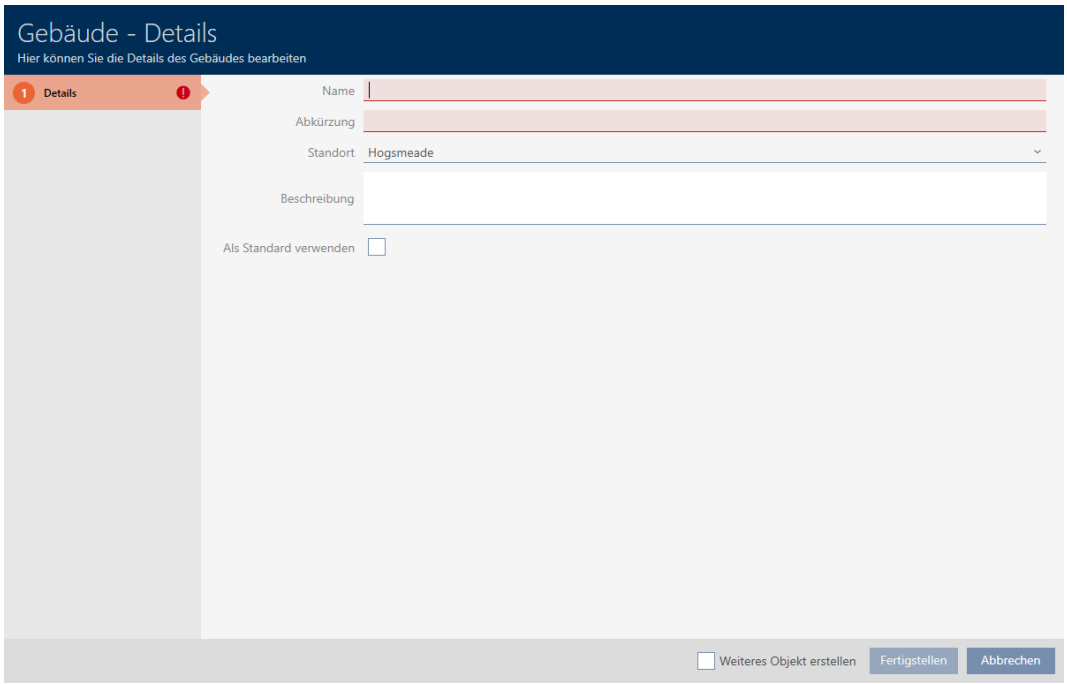
↳ Tab [Gebäude] öffnet sich.



3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster zum Erstellen eines neuen Gebäudes öffnet sich.

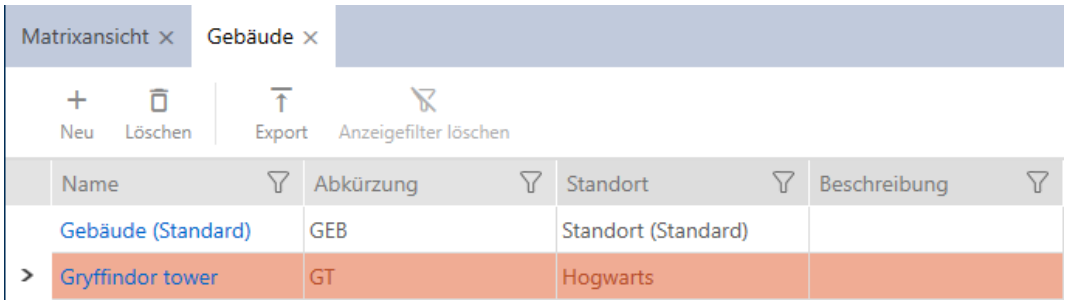


4. Geben Sie im Feld *Name* den Namen Ihres Gebäudes ein.
5. Geben Sie im Feld *Abkürzung* die Abkürzung Ihres Gebäudes ein (max. 5 Zeichen).
6. Wählen Sie im Dropdown-Menü ▼ **Standort** den Standort aus, zu dem Ihr Gebäude gehört.



7. Geben Sie ggfs. im Feld *Beschreibung* eine Beschreibung Ihres Gebäudes ein.
8. Wenn dieses Gebäude bei neuen Schließungen/Türen vorausgewählt werden soll, dann markieren Sie die Checkbox Als Standard verwenden.

9. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster zum Erstellen eines neuen Gebäudes schließt sich.
   ↳ Neu erstelltes Gebäude wird aufgelistet.

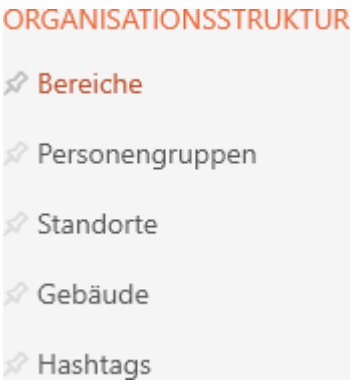


14.12 Bereich erstellen

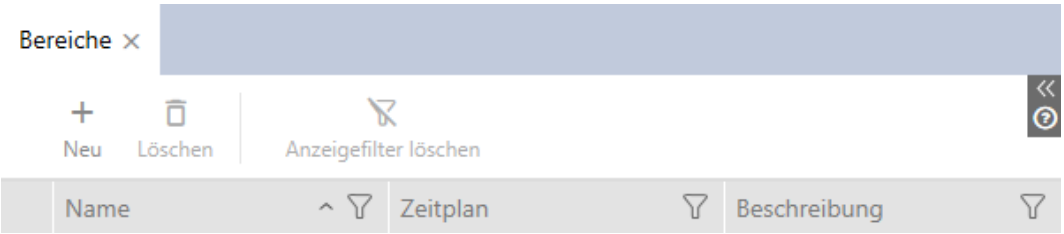
Bereiche sind eine sehr nützliche Strukturierung Ihrer Schließanlage (siehe auch *Bereiche [▸ 569]*).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

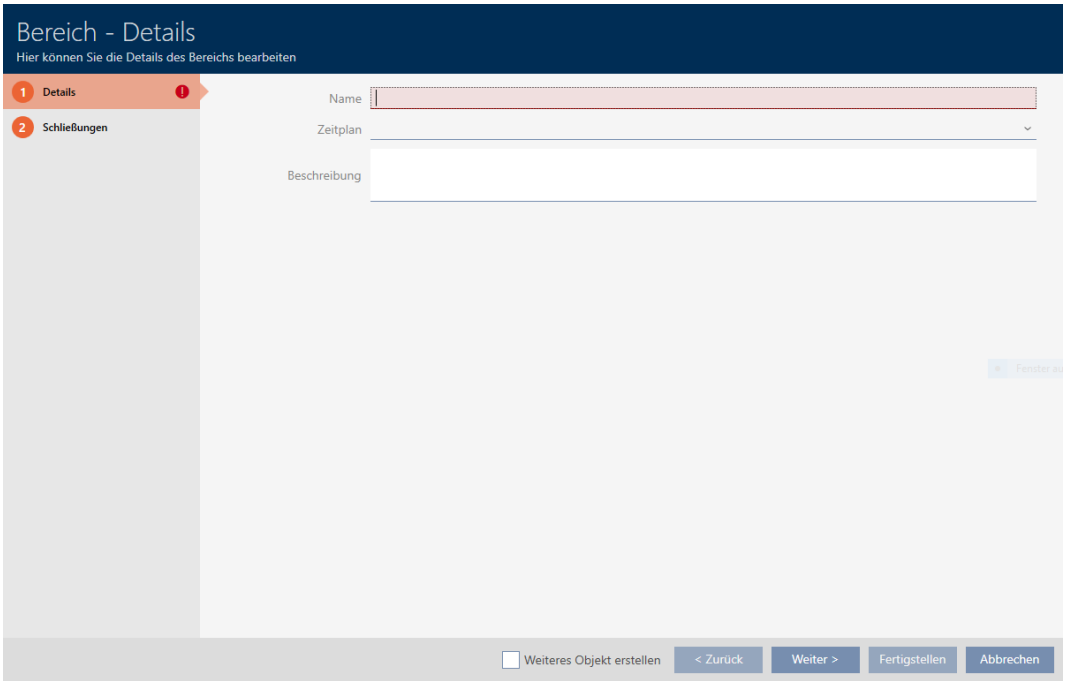
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Bereich aus.



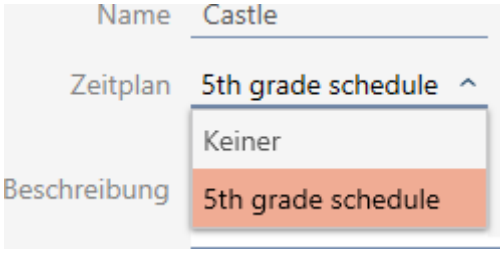
   ↳ Tab [Bereiche] öffnet sich.



3. Klicken Sie auf die Schaltfläche Neu ✚.
   ↳ Fenster "Bereich" öffnet sich.



4. Geben Sie im Feld *Name* den Namen Ihres Bereichs ein.
5. Wählen Sie ggfs. im Dropdown-Menü ▼ **Zeitplan** einen Zeitplan aus, den Sie für die Schließungen in diesem Bereich verwenden wollen.



HINWEIS

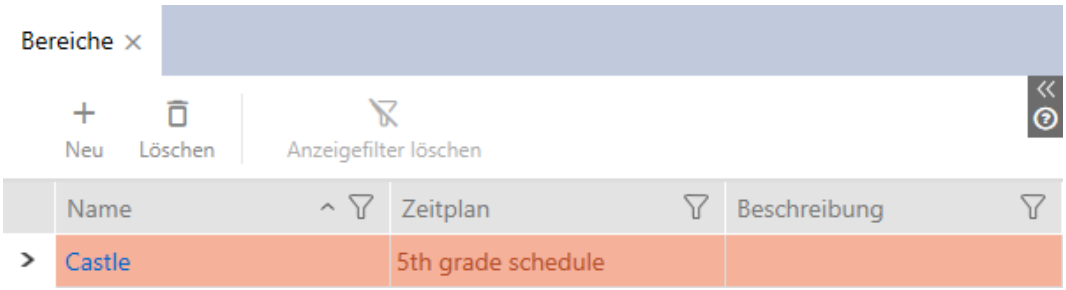
Verfügbare Zeitpläne

Zeitpläne, die Sie für einen Bereich verwenden wollen, müssen natürlich vorhanden sein. Wenn in Ihrer Schließanlage keine Zeitpläne vorhanden sind, dann ist das Dropdown-Menü ▼ **Zeitplan** ausgegraut.

- Erstellen Sie in diesem Fall vorher mindestens einen Zeitplan (siehe *Zeitplan erstellen [▸ 58]*).

6. Geben Sie im Feld *Beschreibung* ggfs. eine Beschreibung Ihres Bereichs ein.
7. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Bereich" schließt sich.

↳ Neu erstellter Bereich wird aufgelistet.



HINWEIS

Zeitpläne in Schließung und Bereichen

Sie können Zeitpläne sowohl einer Schließung als auch dem Bereich der Schließung zuweisen. In diesem Fall wird der Zeitplan in der Schließung verwendet und der Zeitplan des Bereichs ignoriert.

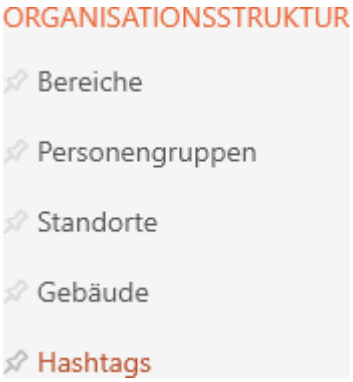
Wenn statt der Schließung dem Bereich ein Zeitplan zugewiesen ist, dann wird der Zeitplan des Bereichs für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

14.13 Hashtag erstellen

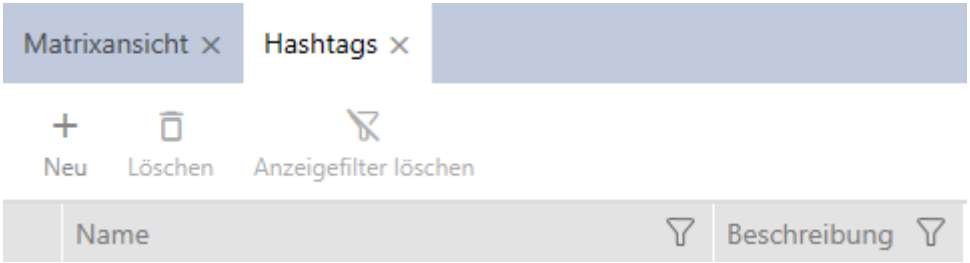
Hashtags können beliebig als Schlagwörter für Personen und/oder Türen eingesetzt werden (siehe *Hashtags [▸ 570]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

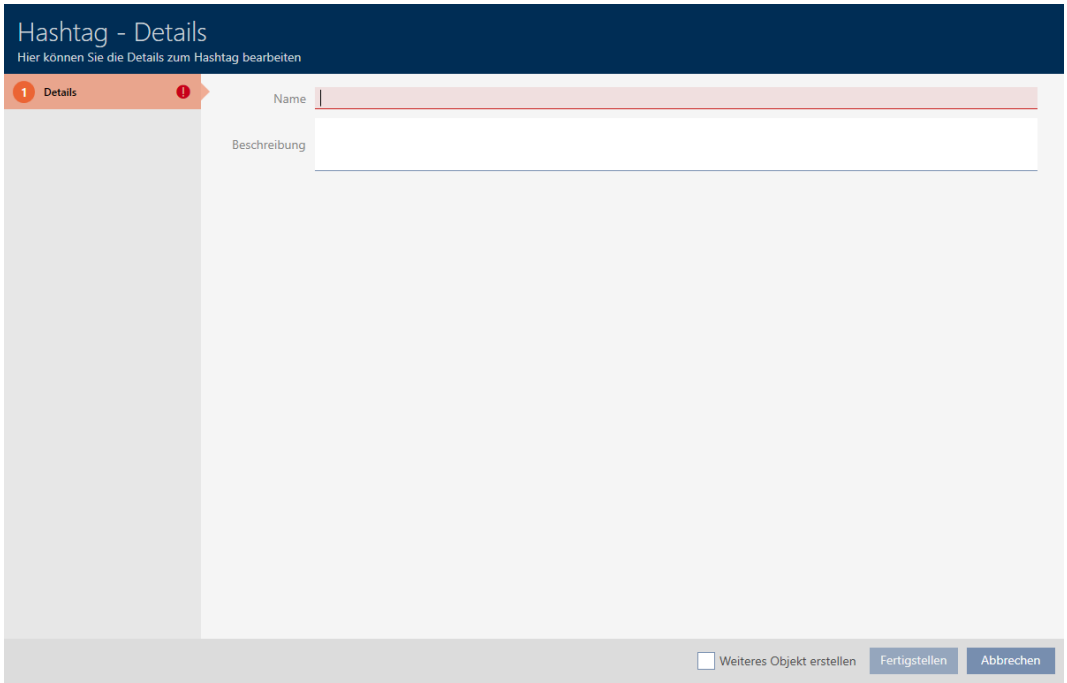
2. Wählen Sie in der Gruppe | ORGANISATIONSSTRUKTUR | den Eintrag Hashtags aus.



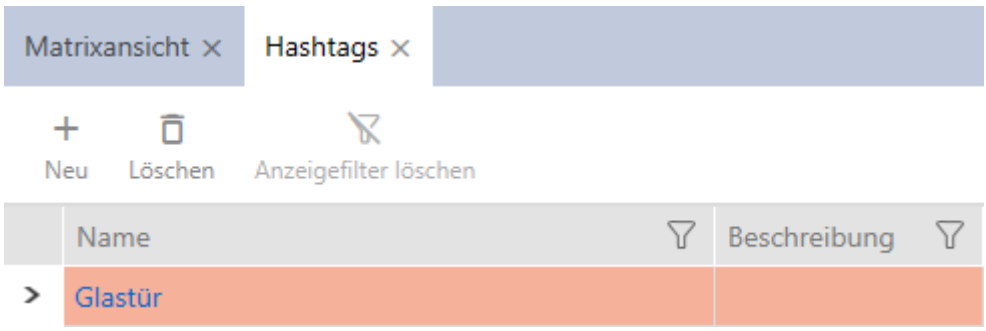
   ↳ Tab [Hashtags] öffnet sich.



3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster zum Erstellen eines neuen Hashtags öffnet sich.



4. Geben Sie im Feld *Name* Ihren Hashtag ein (keine Leerzeichen).
5. Geben Sie ggfs. im Feld *Beschreibung* eine Beschreibung Ihres Hashtags.
6. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster zum Erstellen eines neuen Hashtags schließt sich.
   ↳ Neu erstellter Hashtag wird aufgelistet.



15. Personen und Identmedien

Alle Änderungen, die Sie an der Schließanlage vornehmen, werden erst mit der Synchronisation wirksam (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).

15.1 Identmedien erstellen

Mit Identmedien können Ihre Nutzer Schließungen ein- und auskuppeln (siehe auch *Identmedien, Schließungen und der Schließplan [▸ 532]*).

Ihre AXM Plus stellt Ihnen folgende Identmedien zur Auswahl:

- Transponder
- Karten
- PinCode-Tastatur AX
- PinCode-Tastatur 3068 mit G1-Protokoll
- AX2Go-Schlüssel

Diese Identmedien unterscheiden sich voneinander:

	Transponder/Karten	PinCode-Tastatur AX PinCode-Tastatur 3068 mit G1-Protokoll	AX2Go-Schlüssel
Bedienbare Schließungen	Alle Schließungen, die die erforderliche Schnittstelle haben (aktiv/passiv).	Nur die in der AXM Plus zugewiesene Schließung.	Alle Schließungen, die die erforderliche Schnittstelle und die nötige Firmware haben (BLE ab 1.1.1148).
Verfügbare Einstellungen	Alle	▪ Zeitgruppen ▪ Aktivierungs- und Verfallsdatum	▪ ☑ Langes Öffnen ▪ ☑ Akustisches Öffnungssignal ▪ ☑ ab sofort ▪ ☑ ohne Verfallsdatum
Übergreifende Schließebenen	Für Transponder	Nein	Nein
Vorgehen beim Erstellen	Siehe *Transponder und Karten erstellen [▸ 95]*.	Siehe *PinCode-Tastaturen erstellen [▸ 102]*.	Siehe *Vergabe von Schlüsseln ab AXM Plus [▸ 220]*.

Weitere Informationen zu den verschiedenen Identmedien und deren Unterschieden finden Sie im Kapitel *Identmedien, Schließungen und der Schließplan [▸ 532]*.

15.1.1 Transponder und Karten erstellen

HINWEIS

Transponder bzw. Karten für Schließanlage freischalten

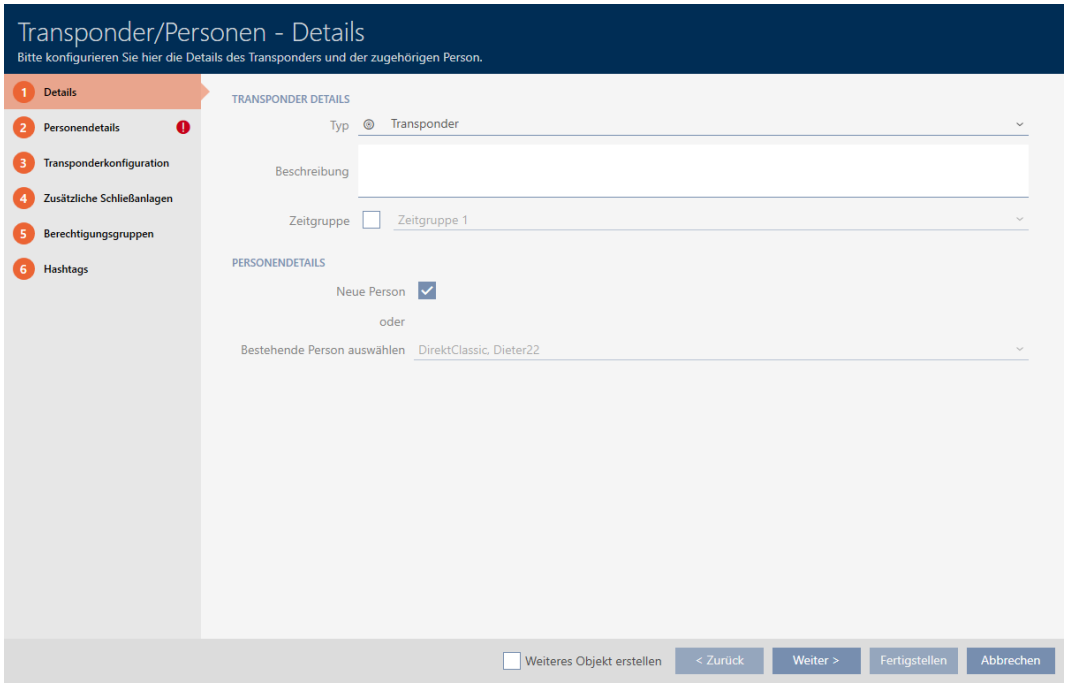
Ihnen stehen nur die Identmedien-Typen zur Verfügung, die in Ihrer Schließanlage freigeschalten sind.

- Schalten Sie ggfs. Karten bzw. Transponder in den Eigenschaften der Schließanlage frei (siehe *Karten bzw. Transponder freischalten [▸ 401]*).

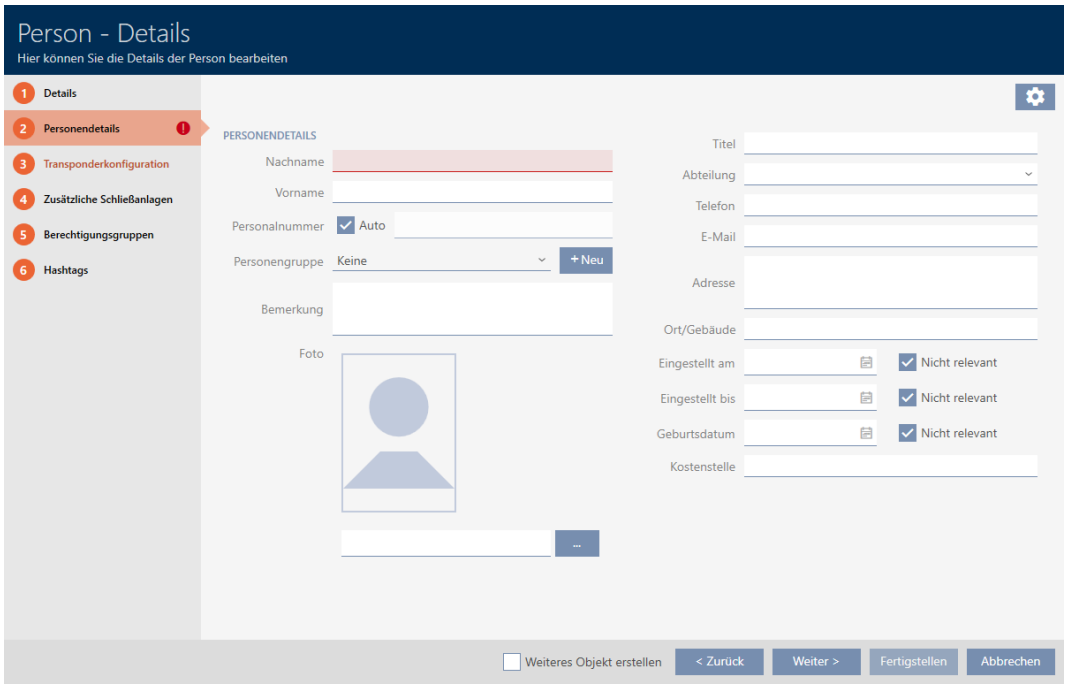
Im Rahmen der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) empfiehlt SimonsVoss, dass Sie zuerst Berechtigungsgruppen, Personengruppen und Zeitpläne/Zeitgruppen einrichten:

- *Berechtigungsgruppen [▸ 332]* (Hintergrundinformationen siehe *Berechtigungsgruppen [▸ 564]*)
- *Personengruppe erstellen [▸ 56]* (Hintergrundinformationen siehe *Personengruppen [▸ 565]*)
- *Zeitplan erstellen [▸ 58]* bzw. *Zeitgruppe erstellen [▸ 61]* (Hintergrundinformationen siehe *Zeitgruppen und Zeitpläne [▸ 548]*)

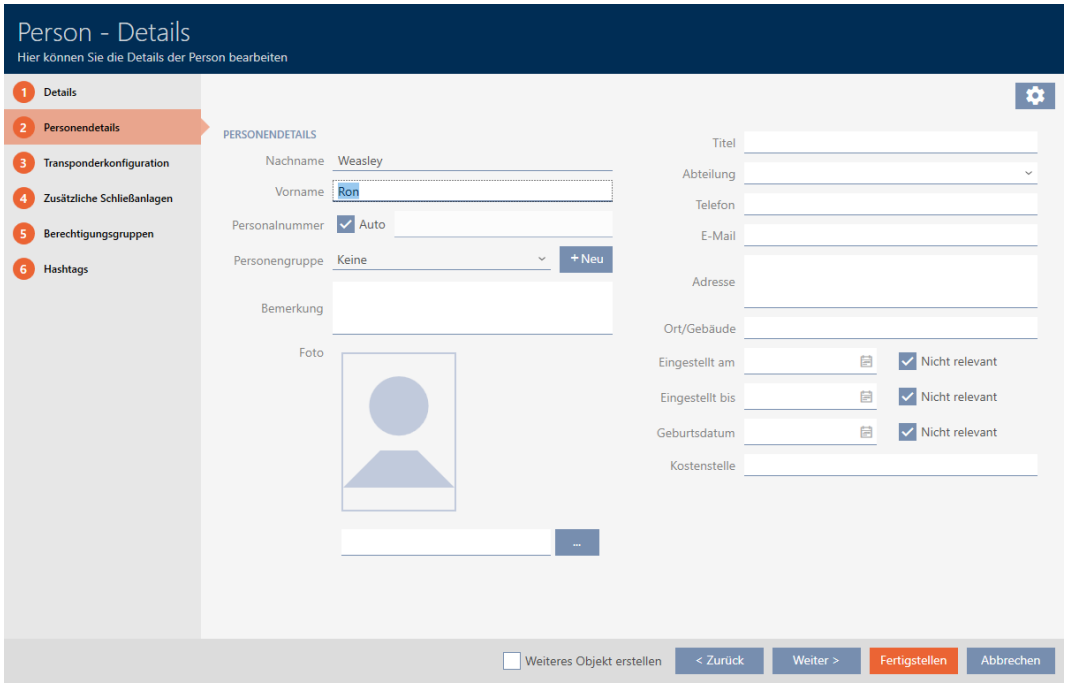
1. Klicken Sie auf die Schaltfläche Neuer Transponder.
   ↳ Fenster zum Erstellen eines Identmediums öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Typ** das Identmedium aus, das Sie erstellen wollen.
3. Geben Sie ggfs. eine Beschreibung ein.
4. Wenn das Identmedium zeitgesteuerte Berechtigungen haben soll: Aktivieren Sie die Checkbox ☑ Zeitgruppe.
5. Wählen Sie aus dem Dropdown-Menü ▼ **Zeitgruppe** die Zeitgruppe aus (z.B. "Zeitgruppe").
6. Aktivieren Sie die Checkbox ☑ Neue Person.
   ↳ Die AXM Plus erstellt für das neue Identmedium automatisch eine neue Person. Deaktivieren Sie diese Checkbox, um eine bereits vorhandene Person auszuwählen (z.B. für ein Zweit-Identmedium oder ein Ersatz-Identmedium).
   ↳ Reiter "Personendetails" wird angezeigt.
7. Klicken Sie auf den Reiter ● Personendetails.



8. Geben Sie in den Feldern *Nachname* und *Vorname* den Nachnamen und Vornamen der Person ein, die das Identmedium besitzen wird.
   ↳ Nachname und Vorname wird später in der Matrix angezeigt.
   ↳ Die Personalnummer wird automatisch erzeugt.



HINWEIS

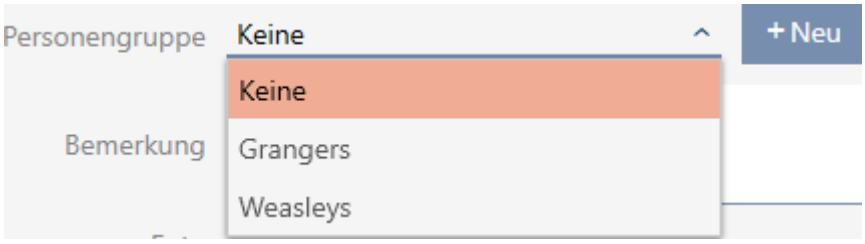
Schema der Personalnummern oder manuelle Eingabe

Die AXM Plus erzeugt die Personalnummern nach folgendem Schema: PN-1, PN-2, PN-X. Das Kürzel *PN* kann bei Bedarf geändert werden (siehe *Automatische Nummerierung ändern [▸ 463]*).

Alternativ können Sie die Personalnummern auch manuell eingeben:

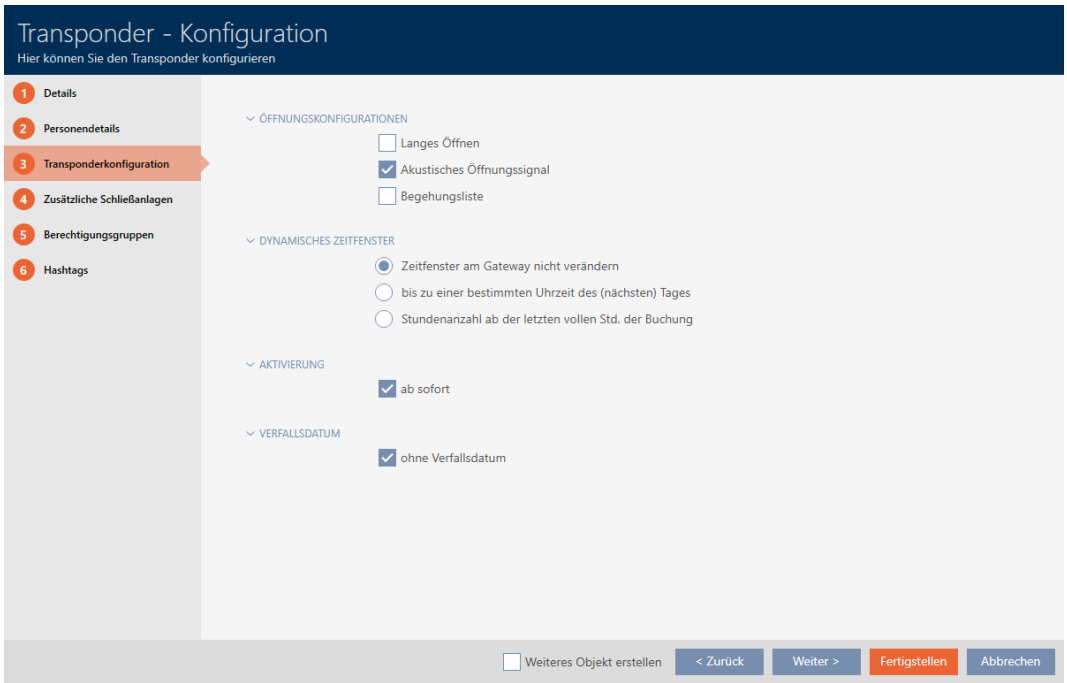
1. Deaktivieren Sie die Checkbox ☐ Auto.
   ↳ Feld *Personalnummer* wird freigeschalten.
2. Geben Sie in das Feld *Personalnummer* die Personalnummer ein.

9. Wenn Sie diese Person einer Personengruppe zuweisen wollen: Wählen Sie aus dem Dropdown-Menü ▼ **Personengruppe** die Personengruppe aus, zu der diese Person gehört.



10. Machen Sie ggfs. weitere Angaben zur Person.
    ↳ Angaben, die Sie im Feld *Abteilung* machen, können Sie anschließend bei anderen Personen einfach aus einer Liste auswählen.

11. Wenn Sie die Felder *Eingestellt am*, *Eingestellt bis* oder *Geburtsdatum* bearbeiten wollen: Deaktivieren Sie die jeweilige Checkbox ☐ Nicht relevant.
12. Wechseln Sie mit der Schaltfläche Weiter > zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.



13. Wenn Schließungen für dieses Identmedium doppelt so lange öffnen sollen (Verdoppelung auf max. 25 s): Aktivieren Sie die Checkbox ☑ Langes Öffnen.
14. Wenn Schließungen für dieses Identmedium nicht piepen sollen: Deaktivieren Sie die Checkbox ☐ Kein akustisches Öffnungssignal.
15. Wenn auf dem Identmedium gespeichert werden soll, an welchen Schließungen es benutzt wurde: Aktivieren Sie die Checkbox ☑ Begehungsliste.
16. Wählen Sie eine der drei Optionen im Bereich "Dynamisches Zeitfenster" aus (siehe *Zeitbudget (AX2Go und virtuelles Netzwerk) [▸ 560]*):
    Option ◉ Zeitfenster am Gateway nicht verändert: Verwendet keine Zeitbudgets.
    Option ◉ bis zu einer bestimmten Uhrzeit des (nächsten) Tages: Berechtigungen dieses Identmediums laufen zu einer bestimmten Uhrzeit ab und können erst dann am Gateway erneuert werden.
    Option ◉ Stundenanzahl ab der letzten vollen Std. der Buchung: Berechtigungen dieses Identmediums laufen nach der angegebenen Anzahl Stunden ab, sie können aber jederzeit am Gateway verlängert oder erneuert werden.

HINWEIS

Gateway zum Erneuern der Zeitbudgets

Wenn Sie die Option ◉ bis zu einer bestimmten Uhrzeit des (nächsten) Tages oder ◉ Stundenanzahl ab der letzten vollen Std. der Buchung auswählen, dann benötigen Ihre Anwender ein Gateway, um ihre Zeitbudgets wieder aufzuladen.

17. Wenn der Transponder nicht sofort verwendbar sein soll: Deaktivieren Sie die Checkbox ☐ ab sofort. Geben Sie dann ein Aktivierungsdatum ein.
18. Wenn der Transponder nur befristet verwendbar sein soll: Deaktivieren Sie die Checkbox ☐ ohne Verfallsdatum. Geben Sie dann ein Verfallsdatum ein.
19. Wechseln Sie mit der Schaltfläche Zusätzliche Schließanlagen zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.
20. Wenn Sie das Identmedium in weiteren Schließanlagen dieses Projekts verwenden wollen: Fügen Sie mit der Schaltfläche Hinzufügen weitere Schließanlagen hinzu (siehe *Identmedium in mehreren Schließanlagen verwenden [▸ 209]*).

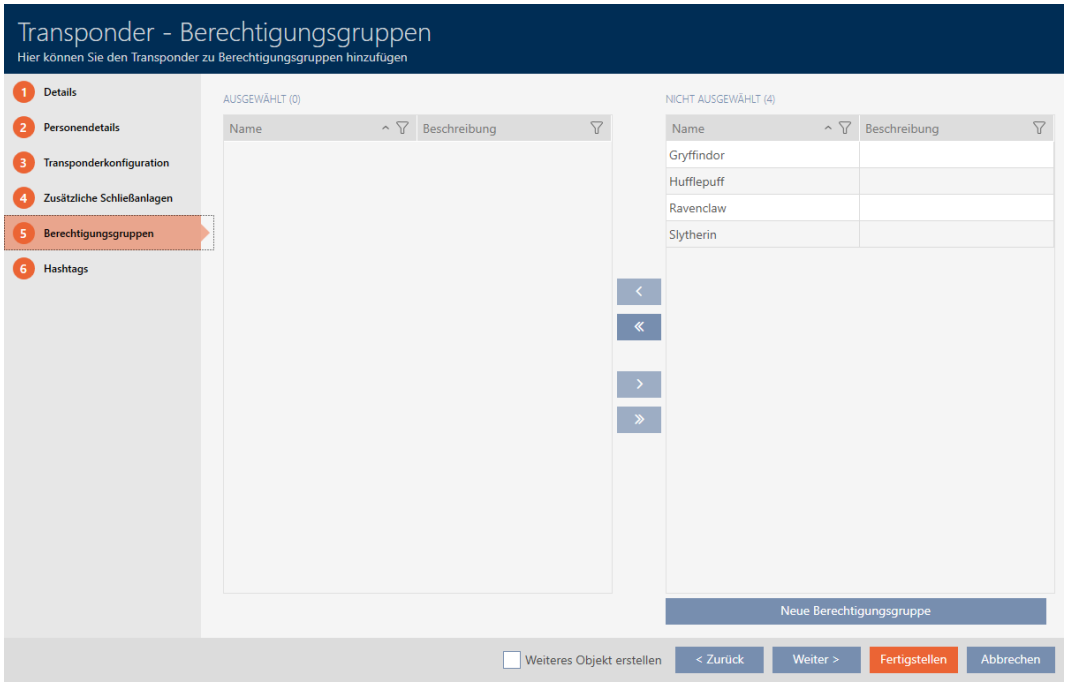
HINWEIS

Einschränkungen für Transponder - Zusätzliche Schließanlagen

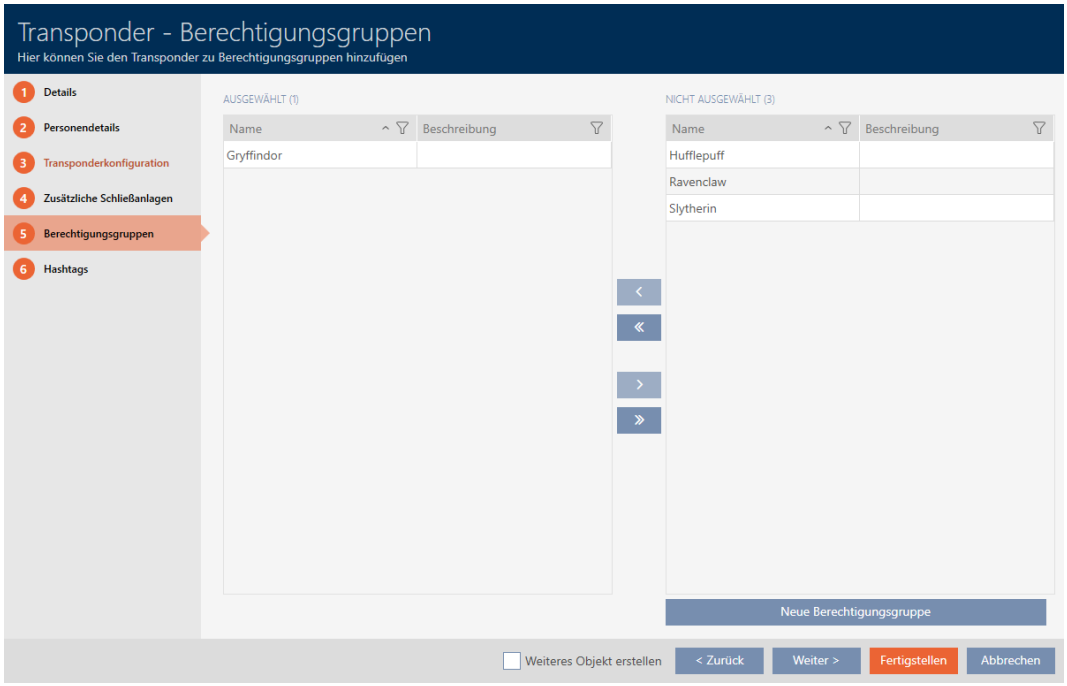
Je nach Art des Identmediums steht unterschiedlich viel Speicherplatz für weitere Schließungen zur Verfügung (Bsp.: G2-Transponder können vier G2-Schließanlagen speichern). Außerdem muss die Schließanlage das Identmedium unterstützen (Bsp.: Transponder können nicht in reinen Karten-Schließanlagen verwendet werden).

1. Stellen Sie sicher, dass auf Ihrem Identmedium ausreichend Speicherplatz vorhanden ist.
2. Stellen Sie sicher, dass die gewünschte Schließanlage Ihr Identmedium unterstützt. Erweitern Sie ggfs. die Schließanlage (siehe *Karten bzw. Transponder freischalten [▸ 401]*).
3. Stellen Sie bei Karten sicher, dass sich die Speicherplätze der Schließanlagen nicht überschneiden.

21. Wechseln Sie mit der Schaltfläche Weiter > zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.



22. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
23. Markieren Sie die gewünschten Berechtigungsgruppen in der rechten Spalte (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).
24. Verschieben Sie mit < nur die ausgewählten Berechtigungsgruppen oder verschieben Sie mit « alle angezeigten Berechtigungsgruppen.
    ↳ Das Identmedium wird den markierten Berechtigungsgruppen zugeordnet.

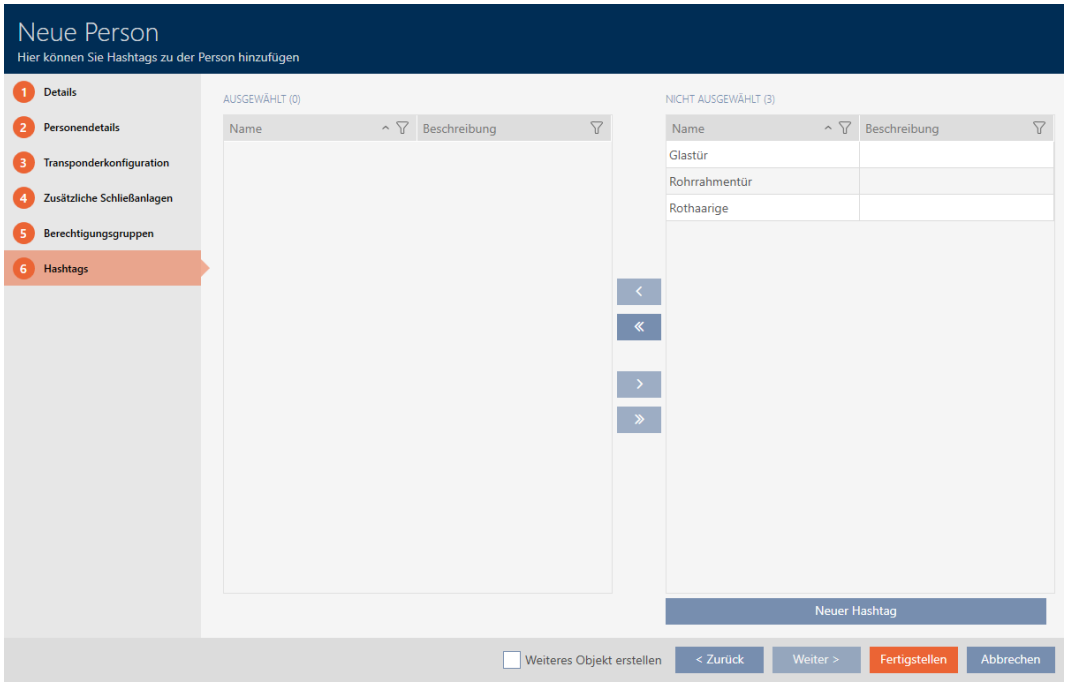


HINWEIS

Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

25. Wechseln Sie mit der Schaltfläche Weiter > zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.



26. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

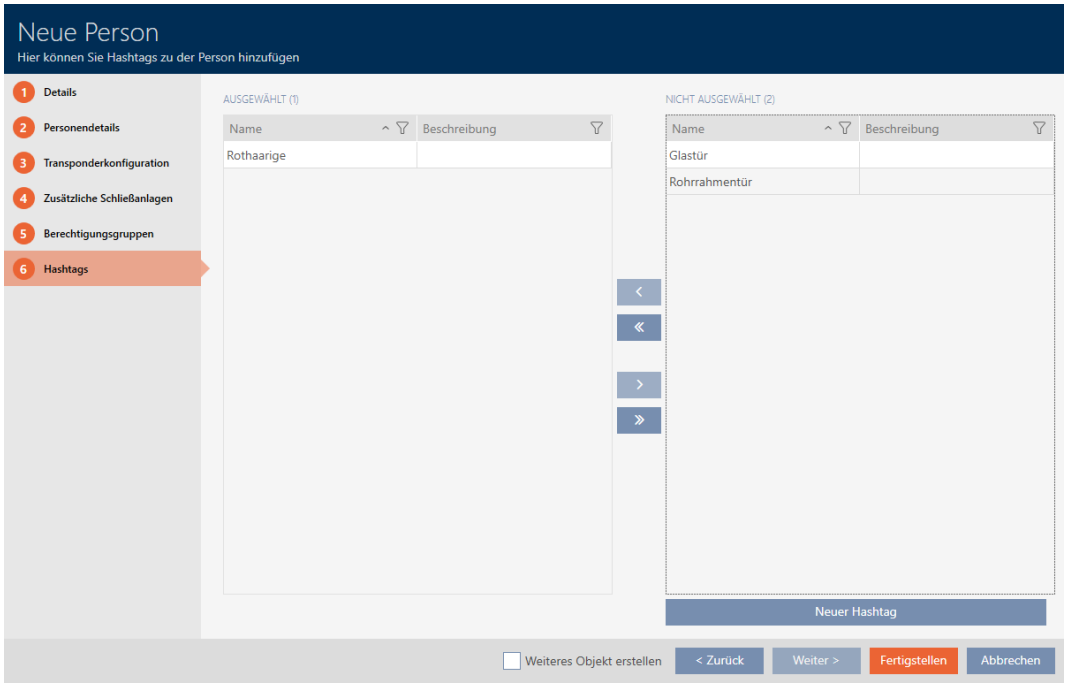
27. Markieren Sie die gewünschten Hashtags in der rechten Spalte (Strg+-Mausklick für einzelne oder Shift+Mausklick für mehrere).
28. Verschieben Sie mit [<] nur die ausgewählten Hashtags oder verschieben Sie mit [«] alle Hashtags.

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

↳ Die markierten Hashtags in der linken Spalte werden für dieses Identmedium angewendet.



29. Aktivieren Sie die Checkbox ☑ Weiteres Objekt erstellen, um für das nächste zu erstellende Identmedium das Fenster mit denselben Einstellungen geöffnet zu lassen.
30. Klicken Sie auf die Schaltfläche Fertigstellen, um das Identmedium zu erstellen.
    ↳ Fenster zum Erstellen eines neuen Identmediums schließt sich.

↳ Neu erstelltes Identmedium wird aufgelistet bzw. in der Matrix angezeigt.

15.1.2 PinCode-Tastaturen erstellen

Mit PinCode-Tastaturen können Ihre Nutzer Schließungen mithilfe eines Zahlencodes (PIN) ein- und auskuppeln (siehe auch *Identmedien, Schließungen und der Schließplan [▸ 532]*).

Im Rahmen der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) empfiehlt SimonsVoss, dass Sie zuerst Zeitpläne/Zeitgruppen einrichten:

- *Zeitplan erstellen [▸ 58]* bzw. *Zeitgruppe erstellen [▸ 61]* (Hintergrundinformationen siehe *Zeitgruppen und Zeitpläne [▸ 548]*)

In diesem Beispiel wird eine PinCode-Tastatur AX erstellt. Eine PinCode-Tastatur 3068 erstellen Sie genauso, allerdings können Sie die Länge der PINs und die PINs nicht in Ihrer AXM Plus festlegen (siehe auch *PinCode G1 vs. PinCode AX [▸ 534]*).

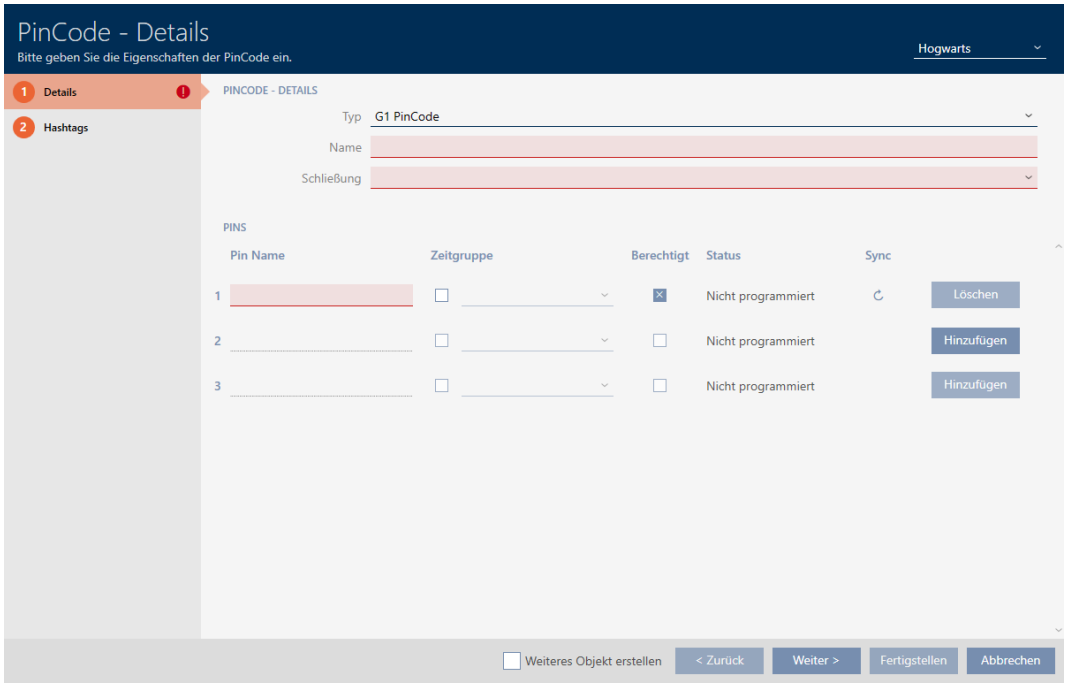
HINWEIS

Berechtigungen automatisch gesetzt

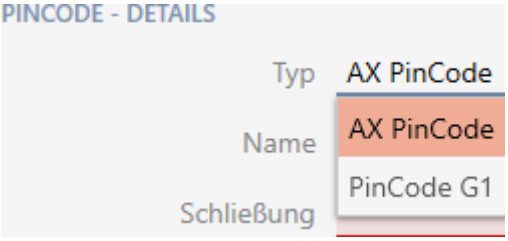
Ihre AXM Plus geht davon aus, dass Sie neu erstellte PINs auch berechtigen wollen. Neu erstellte PINs erhalten deshalb automatisch eine Berechtigung an der zugewiesenen Schließung.

✓ Schließung für die PinCode-Tastatur ist angelegt (siehe *Schließung erstellen [▸ 238]* im AXM-Handbuch).

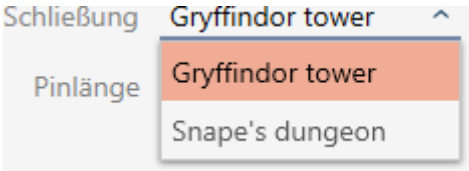
1. Klicken Sie auf die Schaltfläche Neue PinCode.
   ↳ Fenster "PinCode - Details" öffnet sich.



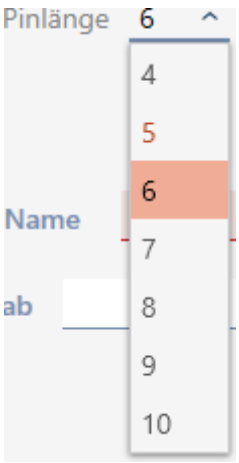
2. Wählen Sie im Dropdown-Menü ▼ **Typ** die PinCode-Tastatur aus, die Sie erstellen wollen.



3. Geben Sie im Feld *Name* einen Namen für die PinCode-Tastatur ein.
4. Wählen Sie im Dropdown-Menü ▼ **Schließung** die Schließung aus, an der Sie die PinCode-Tastatur verwenden wollen.



5. Wenn Sie eine PinCode-Tastatur AX anlegen: Wählen Sie im Dropdown-Menü ▼ **Pinlänge** die Länge der PINs aus.



6. Geben Sie im Feld *Pin Name* den Namen ein, der in der Matrix für diese PIN angezeigt werden soll.
7. Geben Sie eine PIN an.
   ↳ Berechtigung wird automatisch gesetzt.

HINWEIS

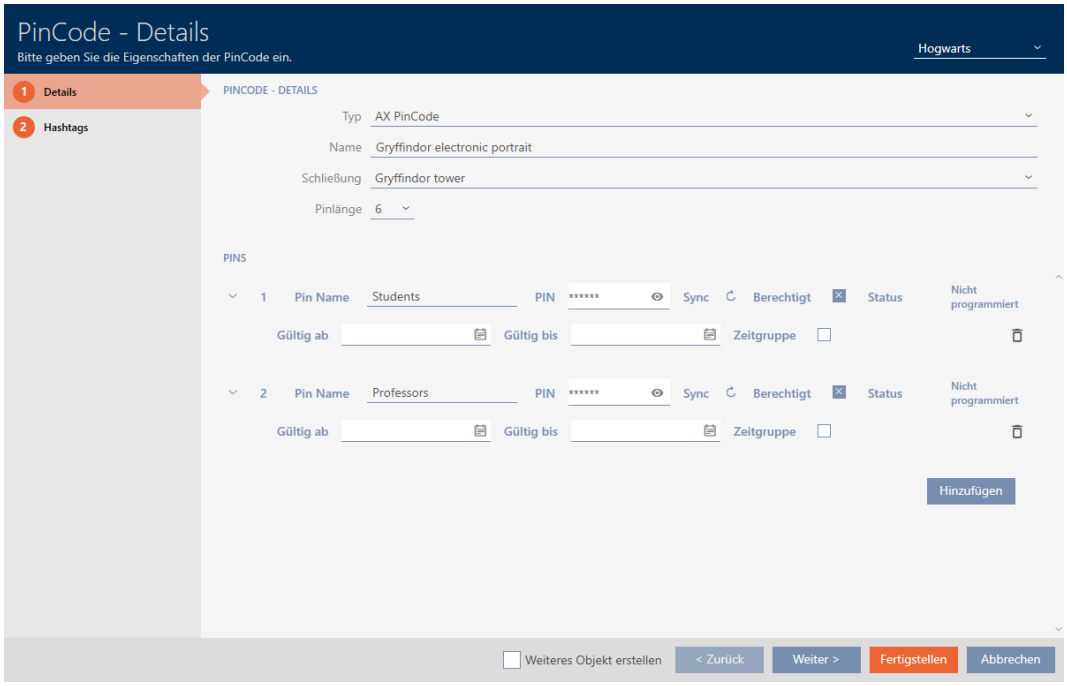
Doppelte PINs bei PinCode-Tastatur AX nicht zulässig

Zur Sicherheit und Nachverfolgbarkeit müssen bei einer PinCode-Tastatur alle PINs unterschiedlich sein.

Ihre AXM Plus erkennt doppelte PINs und markiert sie mit *Der Pin ist nicht eindeutig* rot.

8. Wenn Sie die PIN erst später berechtigen wollen: Deaktivieren Sie die Checkbox ☐ Berechtigt.
9. Wenn Sie ein Aktivierungs-/Verfallsdatum oder die Berechtigung zeitlich steuern wollen, dann klappen Sie die Einstellungen der PIN mit ⌄ aus.
10. Geben Sie ggfs. in den Feldern *Gültig ab* bzw. *Gültig bis* das Aktivierungs-/Verfallsdatum an.
    (PinCode-Tastatur AX: Tagesgenau möglich, PinCode-Tastatur 3068: Stundengenau möglich)
11. Aktivieren Sie ggfs. die Checkbox ☑ Zeitgruppe.
    ↳ Dropdown-Menü erscheint.
12. Wählen Sie im Dropdown-Menü ▼ **Zeitgruppe** die Zeitgruppe aus, die Sie für diese PIN verwenden wollen.

13. Klicken Sie ggfs. auf die Schaltfläche Hinzufügen, um weitere PINs anzulegen.



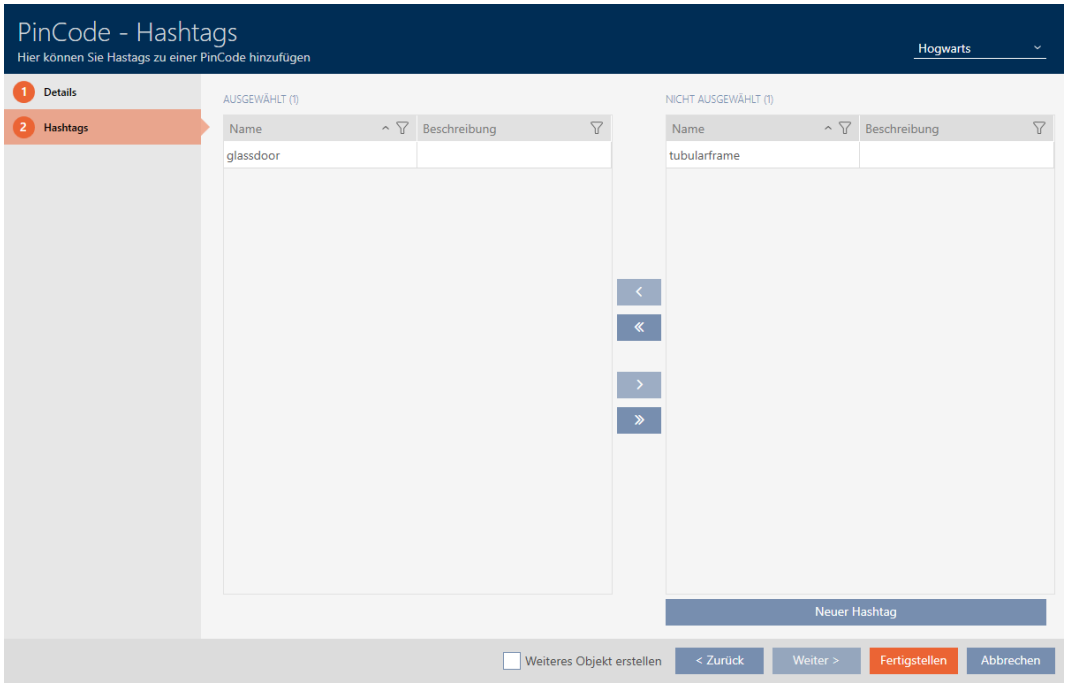
14. Wechseln Sie mit der Schaltfläche Weiter > zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.
15. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
16. Markieren Sie die gewünschten Hashtags in der rechten Spalte (Strg+-Mausklick für einzelne oder Shift+Mausklick für mehrere).
17. Verschieben Sie mit < nur die ausgewählten Hashtags oder verschieben Sie mit « alle Hashtags.

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

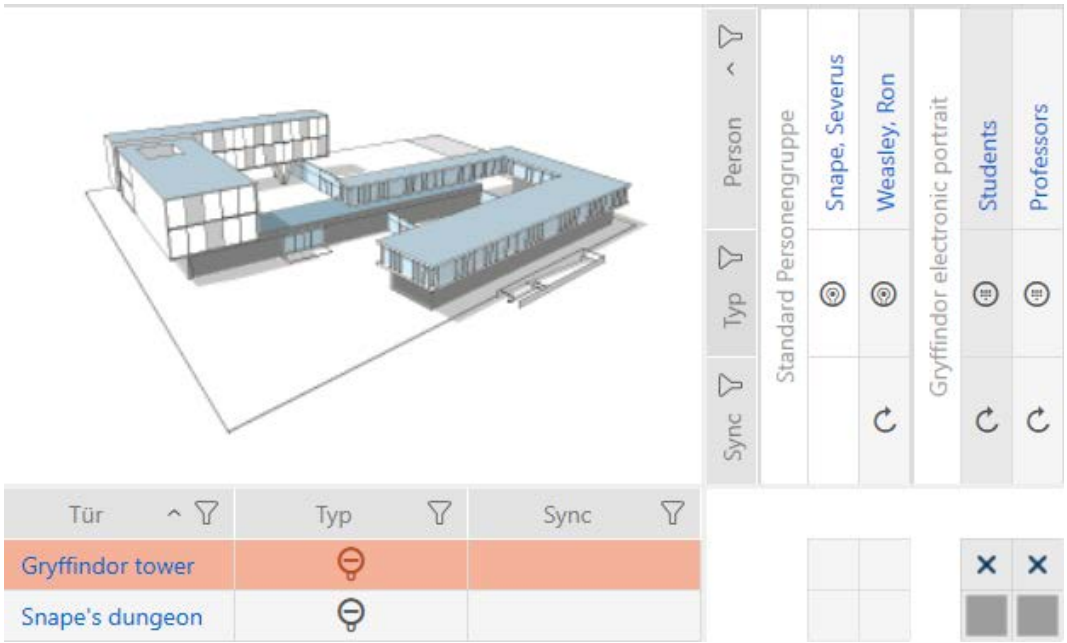
Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

↳ Die markierten Hashtags in der linken Spalte werden für diese PinCode angewendet.



18. Aktivieren Sie die Checkbox ☑ Weiteres Objekt erstellen, um für die nächste zu erstellende PinCode das Fenster mit denselben Einstellungen geöffnet zu lassen.
19. Klicken Sie auf die Schaltfläche Fertigstellen, um die PinCode zu erstellen.
    ↳ Fenster "PinCode - Details" schließt sich.

↳ Neu erstellte PinCode und dazugehörige PINs werden aufgelistet bzw. in der Matrix angezeigt.

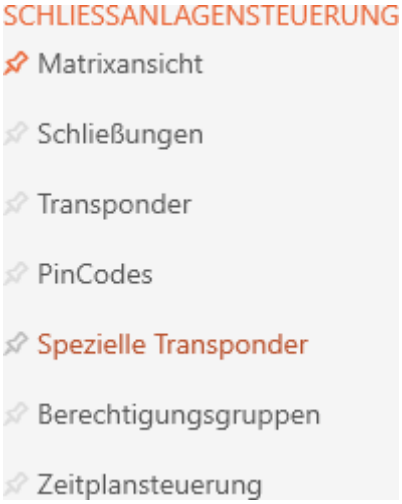


15.1.3 Spezielle Identmedien erstellen

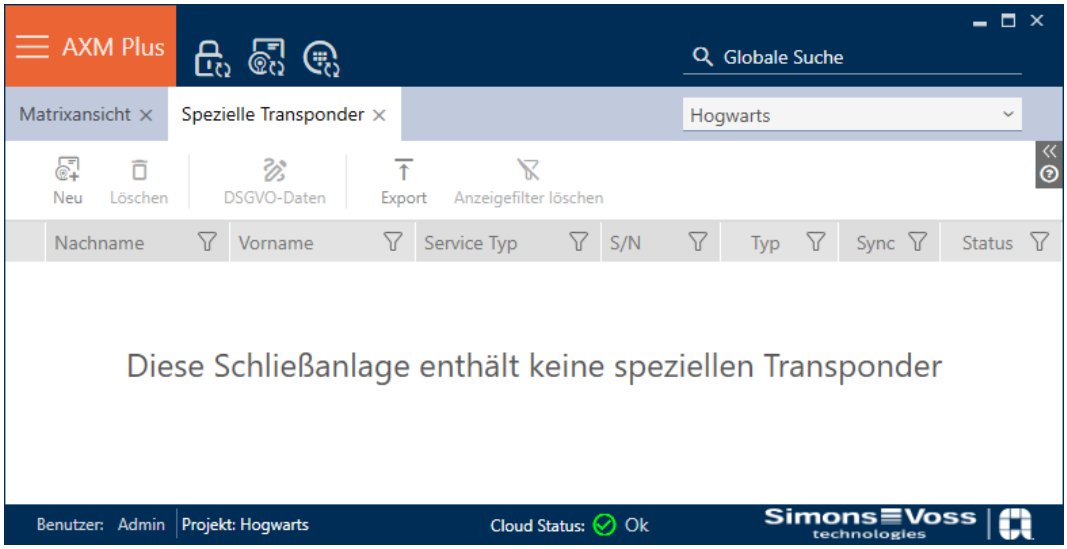
Sie können einem speziellen Identmedium genau eine Funktion zuweisen, nämlich Batteriewechsel oder Schließungsaktivierung (siehe *Spezielle Identmedien und deren Funktionen [▸ 540]*). Dieses Identmedium ist danach in diesem Projekt nicht mehr für andere Zwecke nutzbar.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

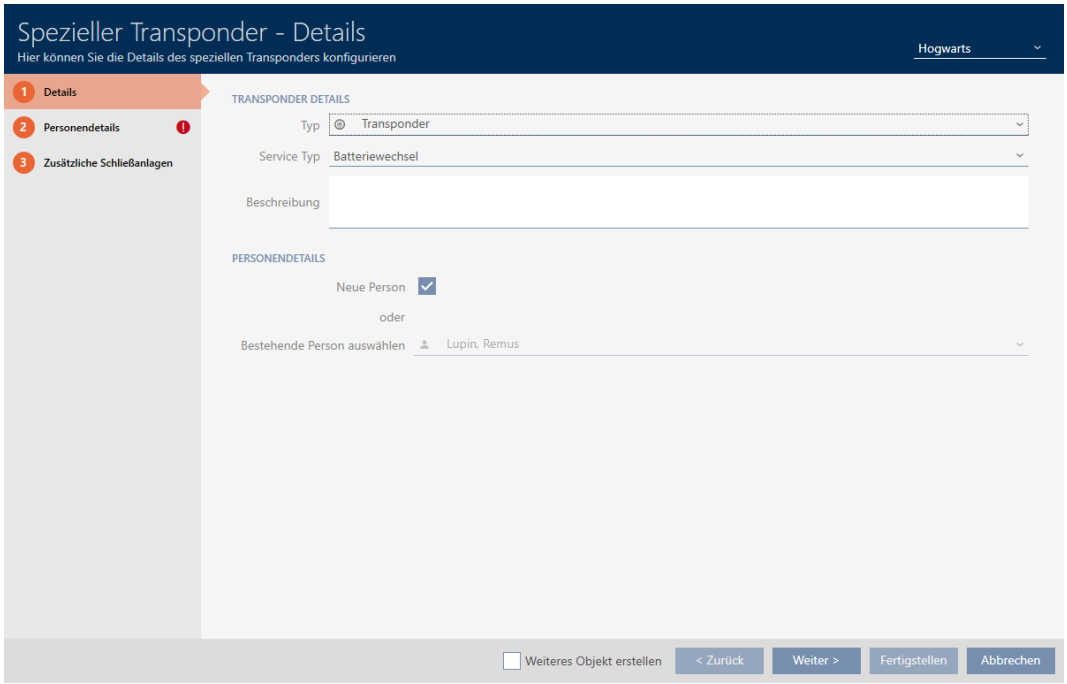
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Spezielle Transponder aus.



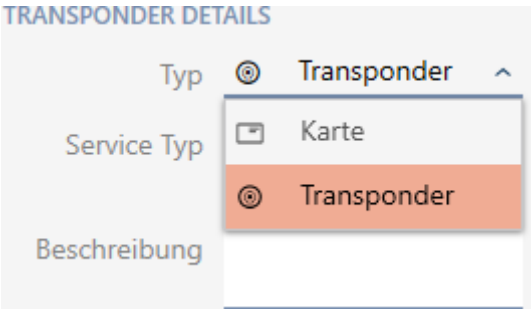
   ↳ Tab [Spezielle Transponder] öffnet sich.



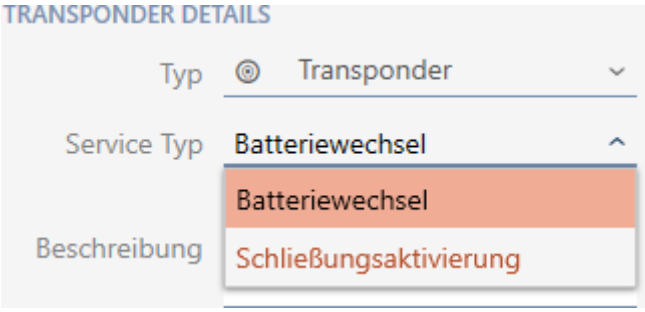
3. Klicken Sie auf die Schaltfläche Neu.
   ↳ Fenster "Spezieller Transponder" öffnet sich.



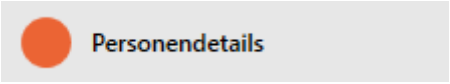
4. Wählen Sie im Dropdown-Menü ▼ **Typ** aus, welchen Typ von Identmedium Sie zu einem speziellen Identmedium machen wollen.



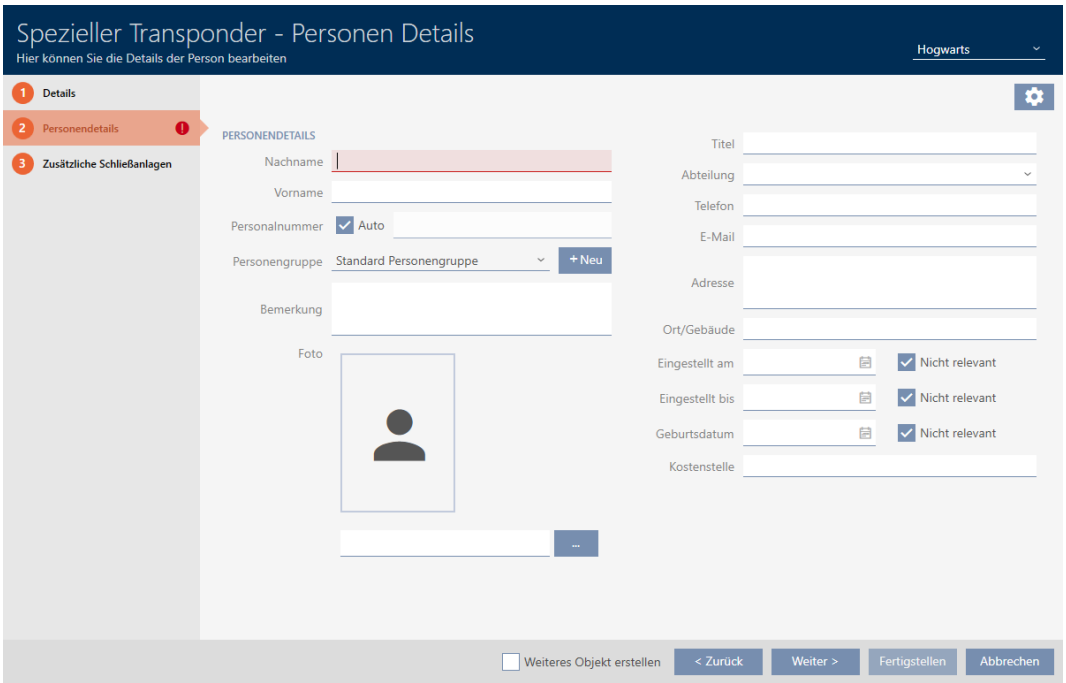
5. Wählen Sie im Dropdown-Menü ▼ **Service Typ**, welche Funktion dieses Identmedium bekommen soll ("Batteriewechsel" oder "Schließungsaktivierung").



6. Geben Sie ggfs. eine Beschreibung ein.
7. Aktivieren Sie die Checkbox ☑ Neue Person.
   ↳ Die AXM Plus erstellt für das neue Identmedium automatisch eine neue Person. Deaktivieren Sie diese Checkbox, um eine bereits vorhandene Person auszuwählen (z.B. für ein Zweit-Identmedium oder ein Ersatz-Identmedium).
   ↳ Reiter "Personendetails" wird angezeigt.
8. Klicken Sie auf den Reiter Personendetails.



9. Geben Sie in den Feldern *Nachname* und *Vorname* den Nachnamen und den Vornamen der Person ein, die das Identmedium besitzen wird.
   ↳ Die Personalnummer wird automatisch erzeugt.



HINWEIS

Schema der Personalnummern oder manuelle Eingabe

Die AXM Plus erzeugt die Personalnummern nach folgendem Schema: PN-1, PN-2, PN-X. Das Kürzel *PN* kann bei Bedarf geändert werden (siehe *Automatische Nummerierung ändern [▸ 463]*).

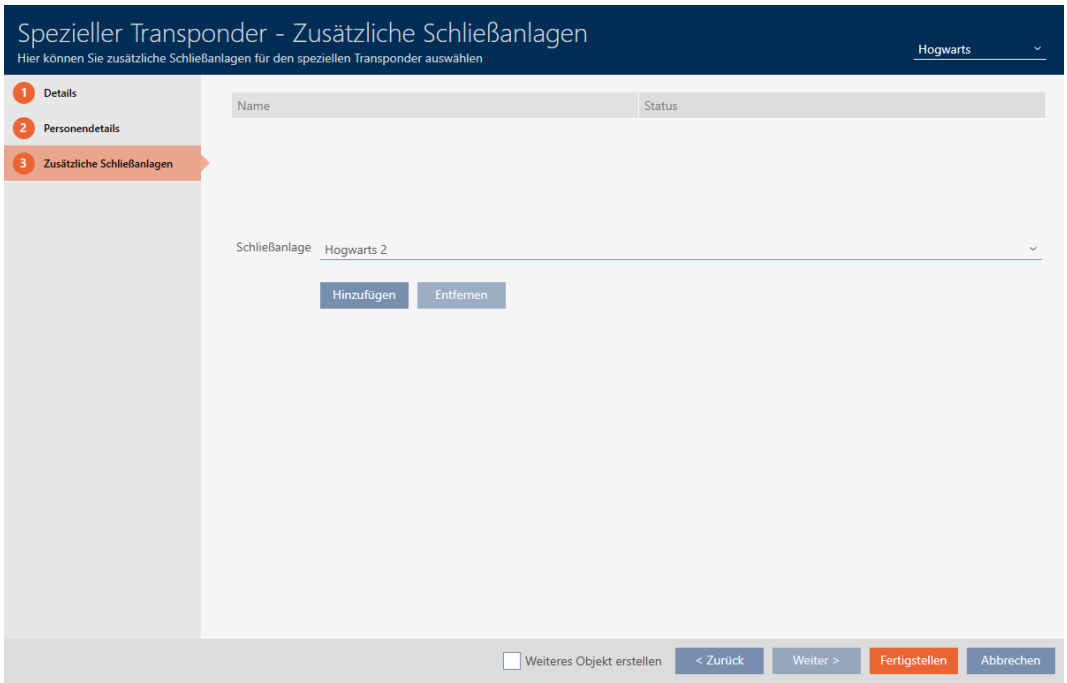
Alternativ können Sie die Personalnummern auch manuell eingeben:

1. Deaktivieren Sie die Checkbox ☐ Auto.
   ↳ Feld *Personalnummer* wird freigeschalten.
2. Geben Sie in das Feld *Personalnummer* die Personalnummer ein.

10. Wenn Sie diese Person einer Personengruppe zuweisen wollen: Wählen Sie aus dem Dropdown-Menü ▼ **Personengruppe** die Personengruppe aus, zu der diese Person gehört.

11. Machen Sie ggfs. weitere Angaben zur Person.
    ↳ Angaben, die Sie im Feld *Abteilung* machen, können Sie anschließend bei anderen Personen einfach aus einer Liste auswählen.
12. Wenn Sie die Felder *Eingestellt am*, *Eingestellt bis* oder *Geburtsdatum* bearbeiten wollen: Deaktivieren Sie die jeweilige Checkbox ☐ Nicht relevant.

13. Wechseln Sie mit der Schaltfläche Zusätzliche Schließanlagen zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.



14. Wenn Sie dieses spezielle Identmedium in weiteren Schließanlagen verwenden wollen: Fügen Sie mit der Schaltfläche Hinzufügen weitere Schließanlagen hinzu.

HINWEIS

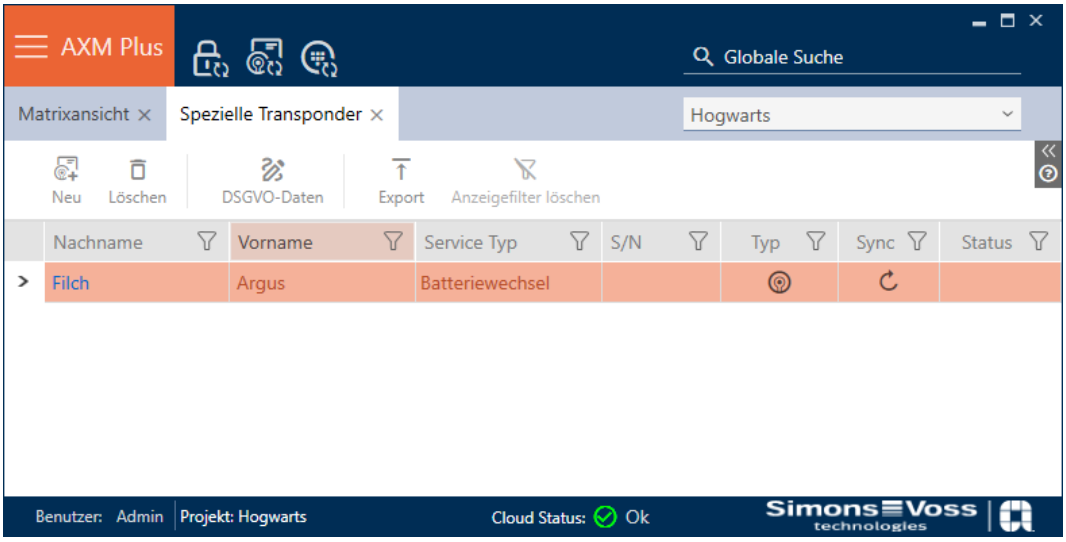
Einschränkungen für Transponder - Zusätzliche Schließanlagen

Je nach Art des Identmediums steht unterschiedlich viel Speicherplatz für weitere Schließungen zur Verfügung (Bsp.: G2-Transponder können vier G2-Schließanlagen speichern). Außerdem muss die Schließanlage das Identmedium unterstützen (Bsp.: Transponder können nicht in reinen Karten-Schließanlagen verwendet werden).

1. Stellen Sie sicher, dass auf Ihrem Identmedium ausreichend Speicherplatz vorhanden ist.
2. Stellen Sie sicher, dass die gewünschte Schließanlage Ihr Identmedium unterstützt. Erweitern Sie ggfs. die Schließanlage (siehe *Karten bzw. Transponder freischalten* [▸ 401]).
3. Stellen Sie bei Karten sicher, dass sich die Speicherplätze der Schließanlagen nicht überschneiden.

15. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Spezielle Transponder" schließt sich.

↳ Neu erstelltes Identmedium mit spezieller Funktion wird aufgelistet.

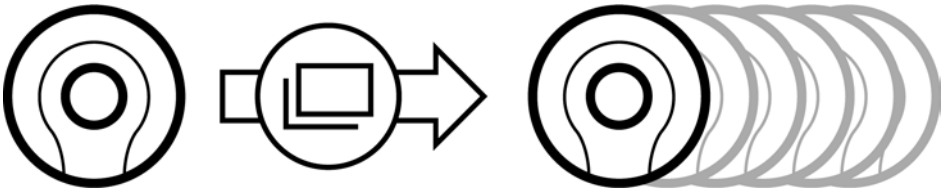


Identmedien mit speziellen Funktionen werden nicht in der Matrix angezeigt.

15.1.4 AX2Go-Schlüssel erstellen

Siehe *Vergabe von Schlüsseln ab AXM Plus [▸ 220]*.

15.2 Identmedium duplizieren (inkl. Berechtigungen und Einstellungen)



Statt ein Identmedium neu zu erstellen können Sie auch einfach ein vorhandenes Identmedium duplizieren. Die AXM Plus übernimmt dabei auch die Eigenschaften, die in der AXM Plus geändert werden können.

Dupliziert werden:

- Transpondertyp
- Zeitgruppe
- Personendetails (außer Personalnummer, diese wird automatisch mit dem einstellbaren Kürzel fortgesetzt, siehe auch *Automatische Nummerierung ändern [▸ 463]*)
- Personengruppe
- Transponderkonfiguration
- Transponder - Zusätzliche Schließanlagen
- Berechtigungsgruppen
- Hashtags

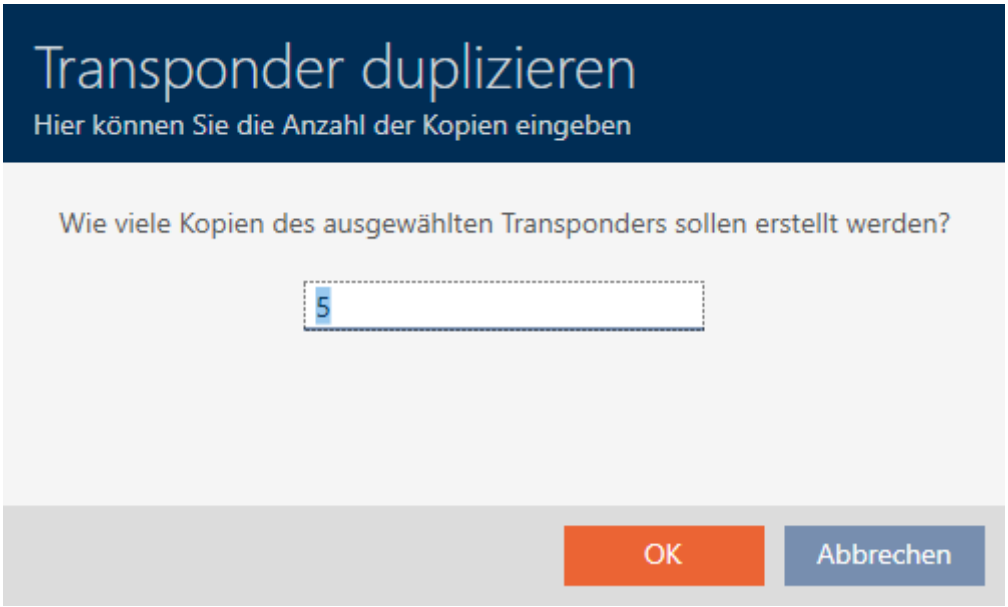
Nicht dupliziert werden:

- Eingaben im Tab [Aktionen]
- Informationen, die hardwareseitig gespeichert sind und bei der Synchronisation ausgelesen werden:
  - Seriennummer
  - Firmware Version
  - Batteriestatus
  - Begehungsliste

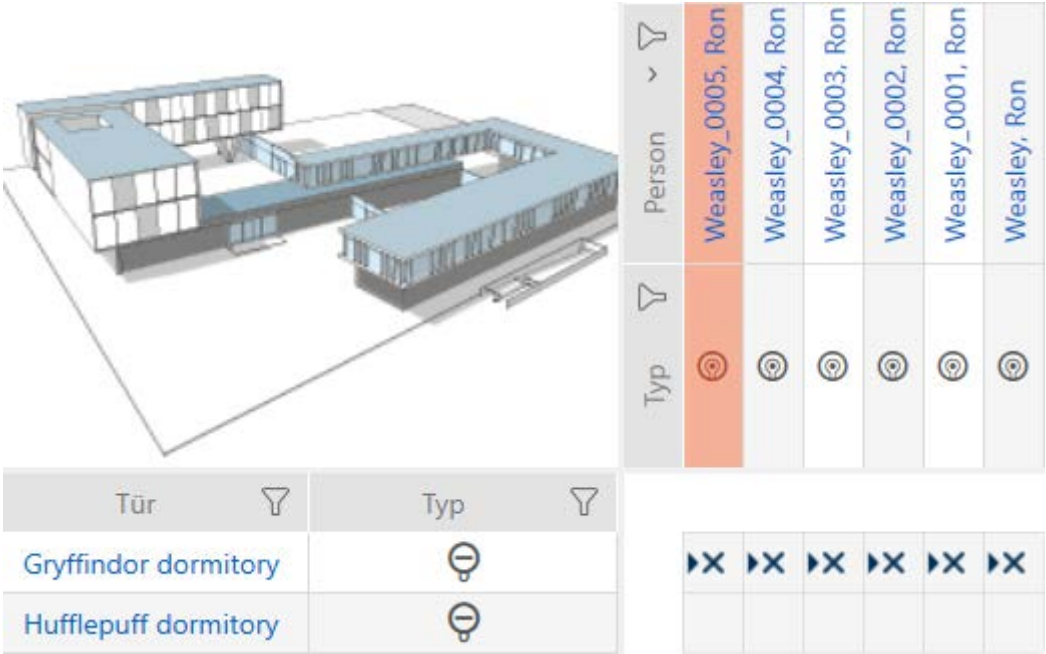
✓ Identmedium vorhanden.

1. Markieren Sie das zu duplizierende Identmedium.

2. Klicken Sie auf die Schaltfläche Duplizieren.
   ↳ Fenster zur Angabe der Kopien öffnet sich.



3. Klicken Sie auf die Schaltfläche OK.
↳ Identmedum ist dupliziert.



15.3 Identmedium löschen

15.3.1 Transponder/Karte löschen

Sie haben zwei Möglichkeiten, um Identmedien wieder zu löschen:

1. Löschen über die Matrixansicht (*Einzelnes Identmedium über die Matrix löschen [▸ 116]*)
2. Löschen über den Tab für die Identmedien (*Mehrere Identmedien über den Tab löschen [▸ 117]*)

Im Tab können Sie auch mehrere Identmedien gleichzeitig löschen.

HINWEIS

Gelöschte Identmedien in Schließungen weiter bekannt/berechtigt

Das Löschen entfernt ein Identmedium nur aus der Datenbank, aber nicht aus den Schließungen. Dort bleibt es bekannt (und ggfs. auch berechtigt) bis es auch dort gelöscht wird (z.B. durch Synchronisieren).

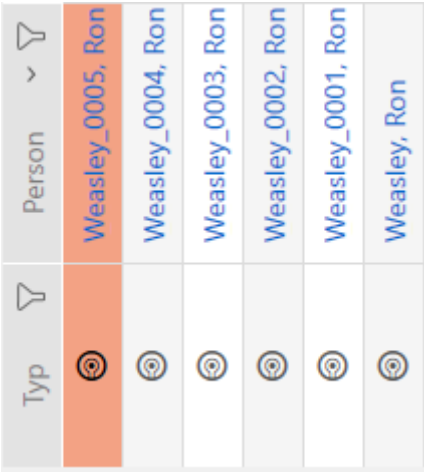
- Sorgen Sie in Ihrer Anlage mit geeigneten Maßnahmen (z.B. Synchronisierung) dafür, dass das Identmedium auch in den Schließungen nicht mehr bekannt ist.

15.3.1.1 Einzelnes Identmedium über die Matrix löschen

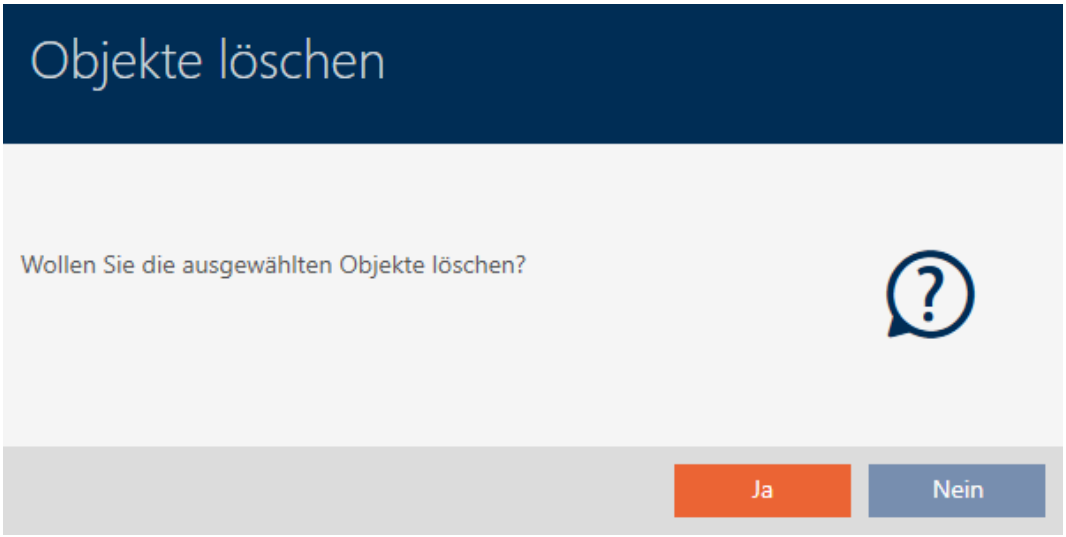
✓ Matrixansicht geöffnet.

✓ Zu löschendes Identmedium ist unprogrammiert oder zurückgesetzt (Zurücksetzen siehe *Transponder/Karten zurücksetzen [▸ 443]*).

1. Markieren Sie das Identmedium, das Sie löschen wollen.

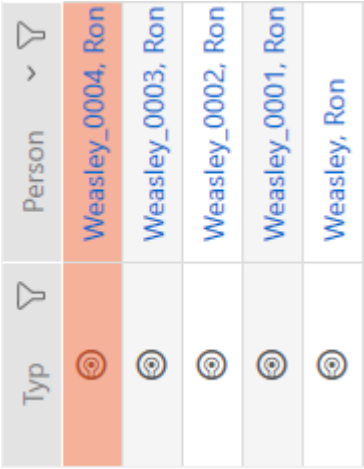


2. Klicken Sie auf die Schaltfläche Löschen.
   ↳ Rückfrage zum Löschen öffnet sich.



3. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Löschen schließt sich.

↳ Identmedium ist gelöscht.

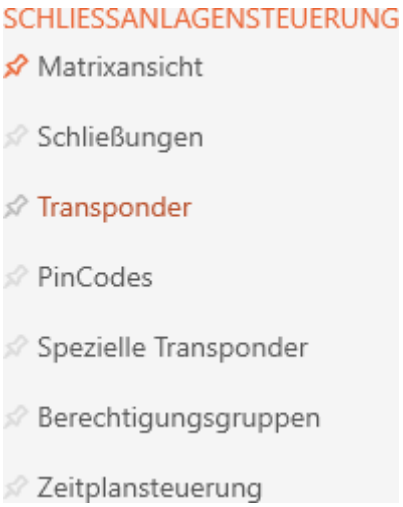


15.3.1.2 Mehrere Identmedien über den Tab löschen

✓ Zu löschende Identmedien sind unprogrammiert oder zurückgesetzt (Zurücksetzen siehe *Transponder/Karten zurücksetzen [▸ 443]*).

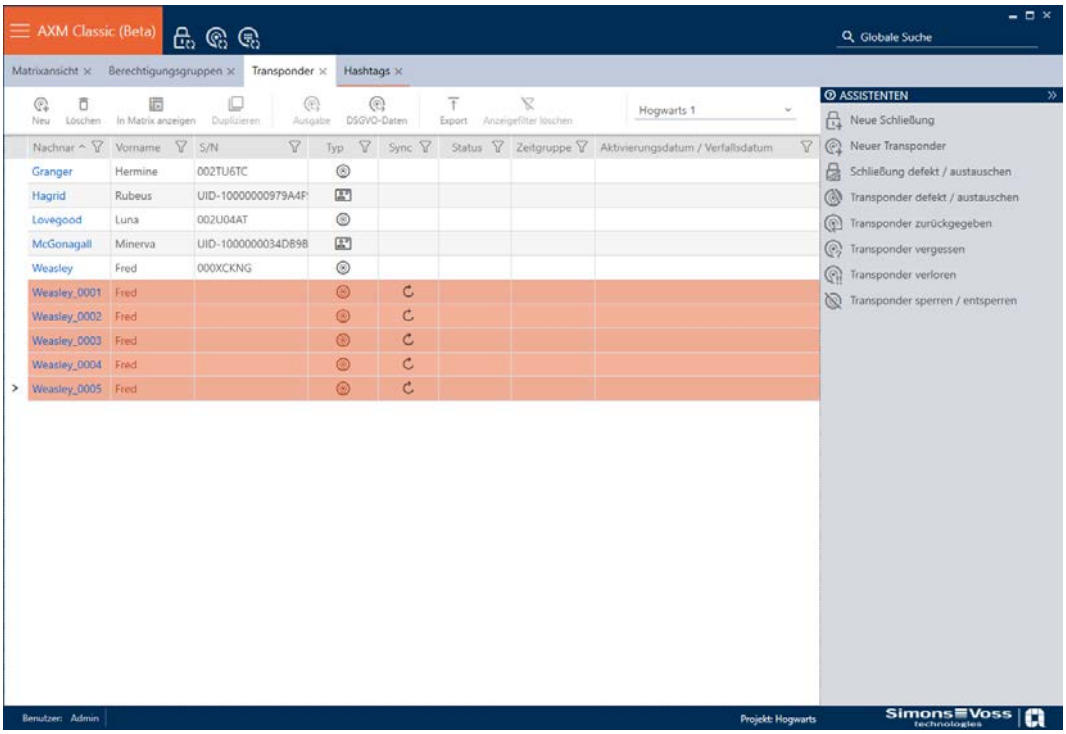
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.

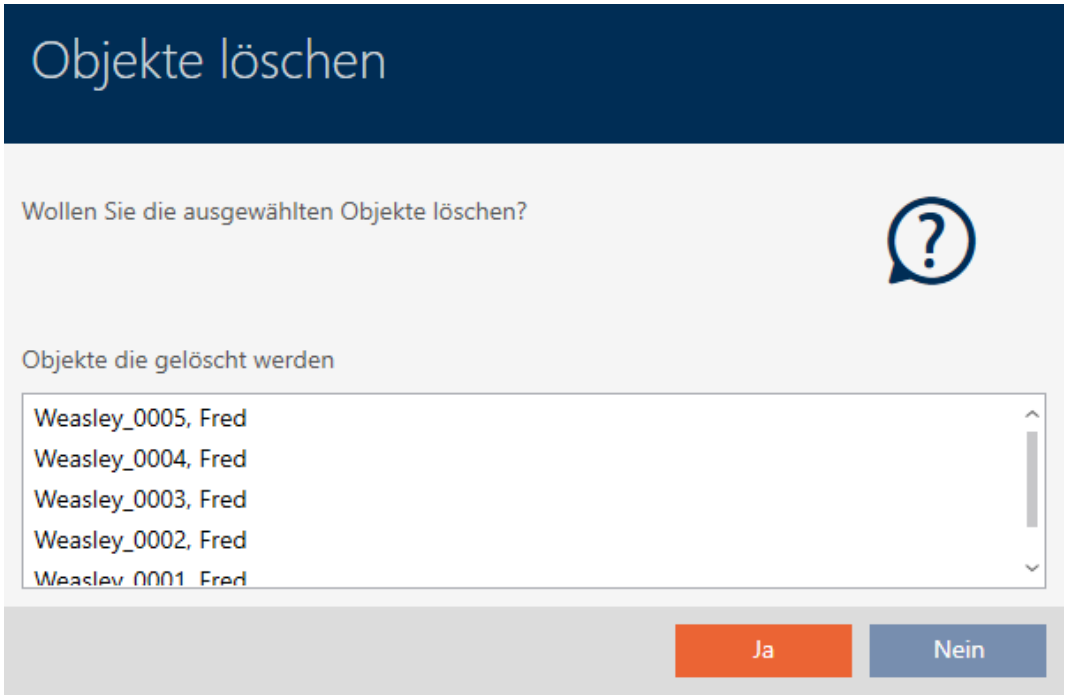


   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Transponder] öffnet sich.

3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
4. Markieren Sie alle Identmedien, die Sie löschen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

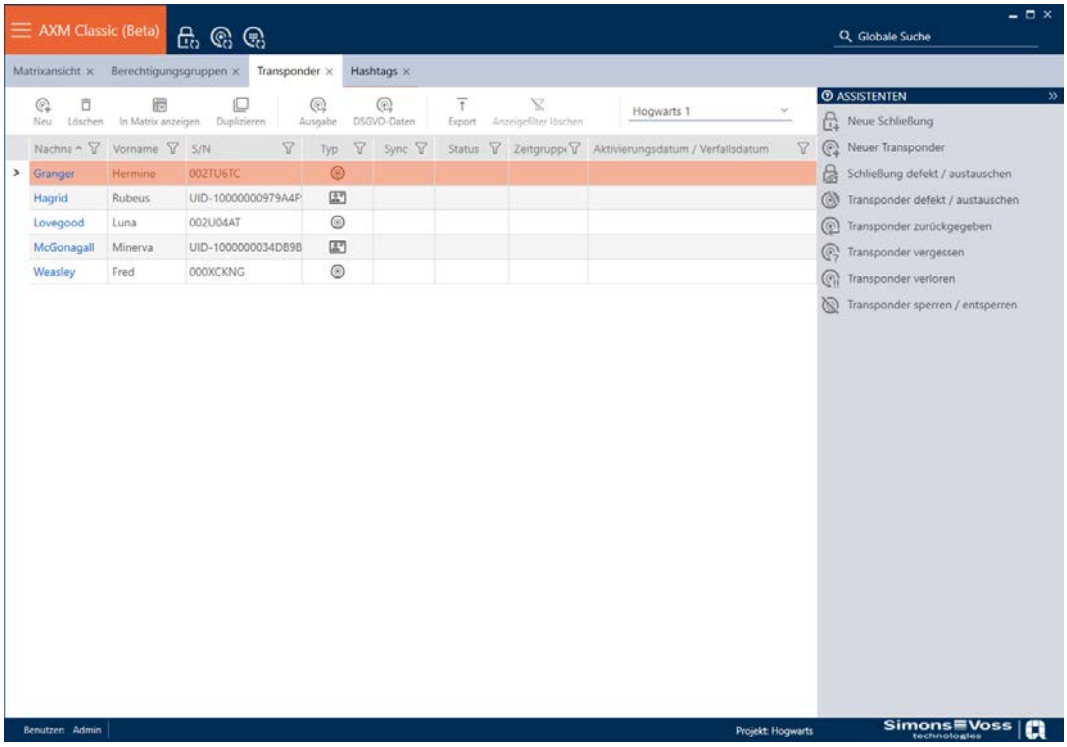


5. Klicken Sie auf die Schaltfläche Löschen 🗑.
   ↳ Rückfrage mit Liste der zu löschenden Identmedien öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage mit Liste der zu löschenden Identmedien schließt sich.

↳ Identmedien sind gelöscht.



HINWEIS

Gelöschte Identmedien in Schließungen weiter bekannt/berechtigt

Das Löschen entfernt ein Identmedium nur aus der Datenbank, aber nicht aus den Schließungen. Dort bleibt es bekannt (und ggfs. auch berechtigt) bis es auch dort gelöscht wird (z.B. durch Synchronisieren).

- Sorgen Sie in Ihrer Anlage mit geeigneten Maßnahmen (z.B. Synchronisierung) dafür, dass das Identmedium auch in den Schließungen nicht mehr bekannt ist.

15.3.2 PIN löschen (PinCode-Tastatur AX)

HINWEIS

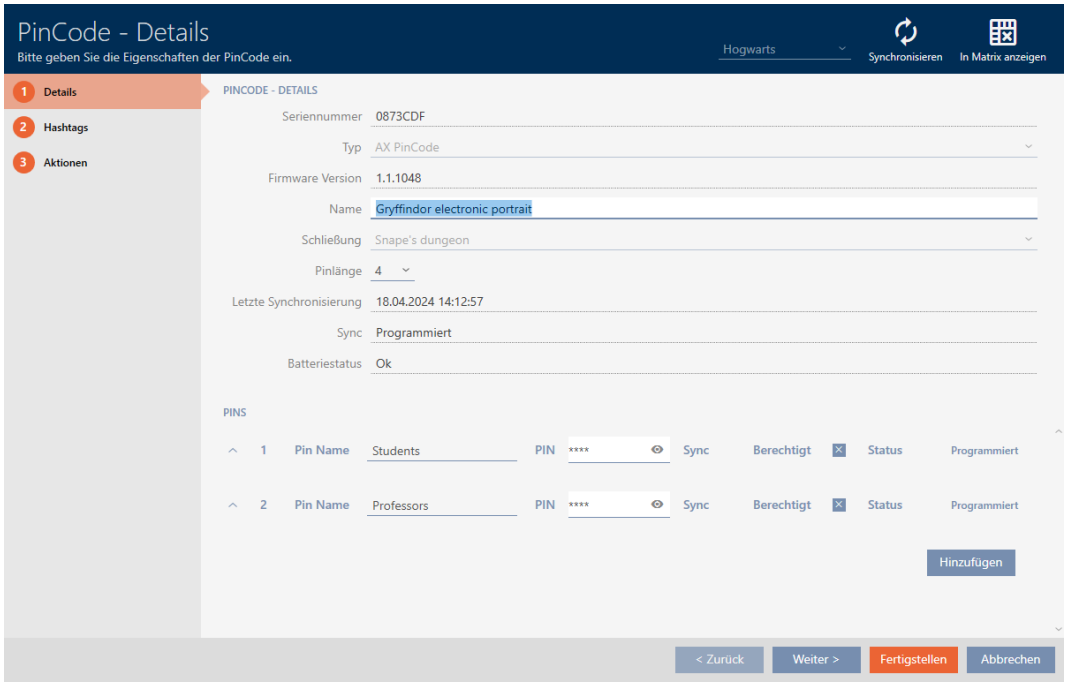
Beschreibung nur für PinCode-Tastatur AX gültig

Die hier beschriebene Einstellung steht in Ihrer AXM Plus nur für die PinCode-Tastatur AX zur Verfügung. An der PinCode-Tastatur 3068 verändern Sie diese Einstellung mithilfe der Master-PIN direkt an der PinCode-Tastatur 3068.

✓ Matrixansicht geöffnet.

✓ PinCode-Tastatur AX erstellt (siehe *PinCode-Tastaturen erstellen* *[▸ 102]*).

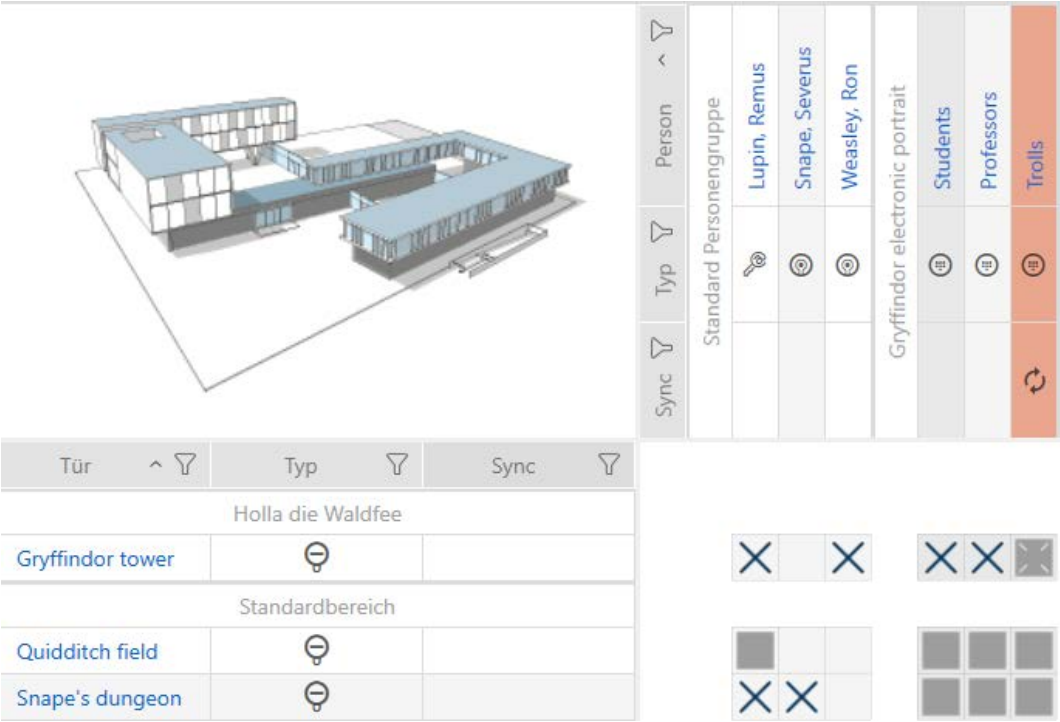
1. Klicken Sie auf eine beliebige PIN, um die Details Ihrer PinCode-Tastatur AX zu öffnen.
   ↳ Fenster "PinCode - Details" öffnet sich.



2. Klappen Sie die Einstellungen der zu löschenden PIN mit ⌄ aus.
3. Klicken Sie auf 🗑, um die PIN zum Löschen zu markieren.
   ↳ Feld *Status* zeigt *Löschen vorbereitet*.

4. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ Gelöschte PIN wird mit ausgegrauter Berechtigung und Programmierbedarf in der Matrix gezeigt.



Nach der Synchronisierung verschwindet die gelöschte PIN.

15.3.3 AX2Go-Schlüssel sperren

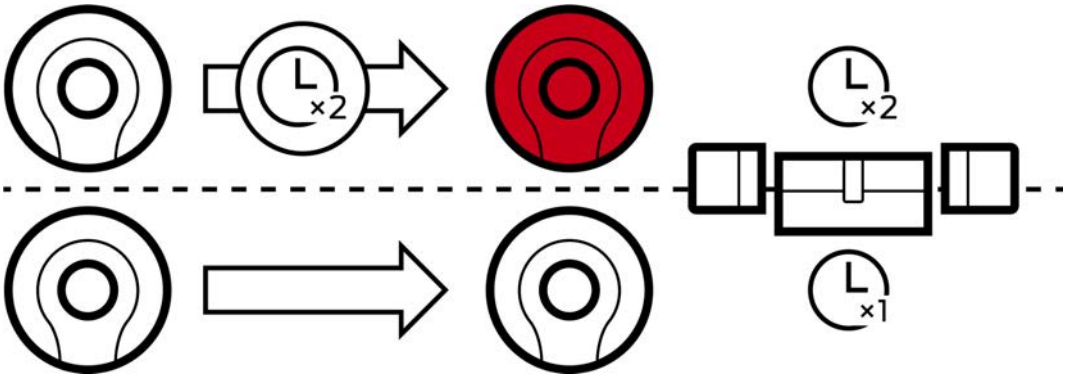
Siehe *AX2Go-Schlüssel sperren [▸ 227]*.

15.4 Identmedium doppelt so lange öffnen lassen

Normalerweise öffnen Schließungen im Impulsbetrieb für die eingestellte Dauer.

Für einzelne Personen ist es hilfreich, wenn eine Schließung nach der Betätigung länger eingekuppelt bleibt.

Deshalb kann das Identmedium beim Öffnen jeder Schließung mitteilen, dass sie für dieses Identmedium doppelt so lange einkuppeln sollen.

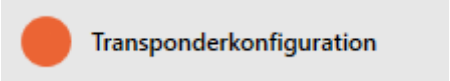


Die maximale Einkupplungsdauer liegt dabei weiterhin bei 25 s:

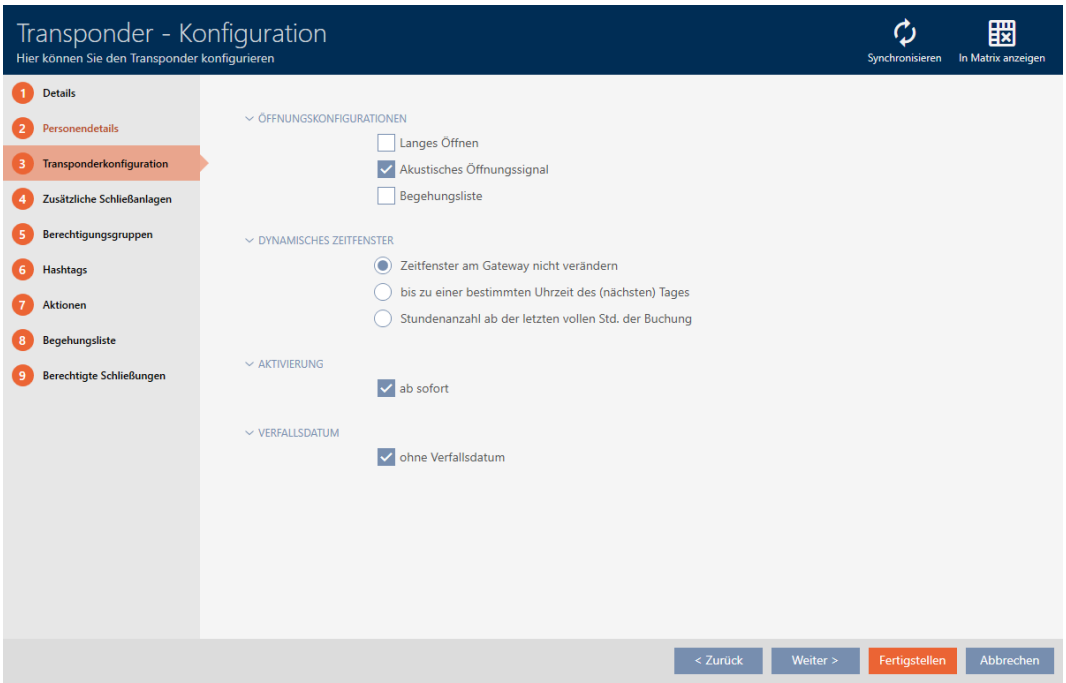
- 5 s werden zu 10 s
- 10 s werden zu 20 s
- 20 s werden aber nur zu 25 s

✓ Identmedium vorhanden.

1. Klicken Sie auf das Identmedium, das doppelt so lange öffnen soll.
   ↳ Fenster des Identmediums öffnet sich.
2. Klicken Sie auf den Reiter Transponderkonfiguration.



↳ Fenster wechselt zum Reiter "Transponderkonfiguration".



3. Aktivieren Sie die Checkbox ☐ Langes Öffnen.

4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

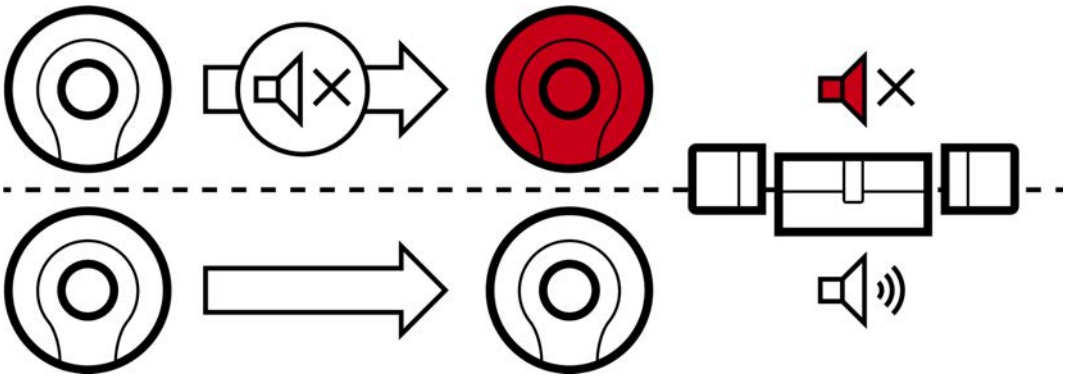
↳ Alle Schließungen öffnen für dieses Identmedium doppelt so lange.

15.5 Für ein Identmedium alle Schließungen stummschalten

Normalerweise piepen Schließungen, wenn ein Identmedium verwendet wird, um die Schließung einzukuppeln.

In manchen Situationen ist dieses akustische Öffnungssignal unerwünscht. Beispiel: Eine Krankenschwester soll nachts in einem Krankenhaus ein Zimmer betreten können, ohne den Patienten durch das akustische Öffnungssignal aufzuwecken.

Deshalb kann das akustische Öffnungssignal für einzelne Identmedien auch abgeschaltet werden. Diese Einstellung bezieht sich nur auf das Identmedium.



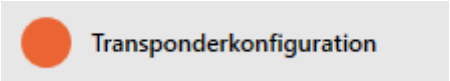
Das bedeutet:

- Identmedien, bei denen ☐ Akustisches Öffnungssignal deaktiviert ist, öffnen alle Schließungen ohne Piepen.
- Andere Identmedien öffnen weiterhin alle Schließungen wie gewohnt mit Piepen.

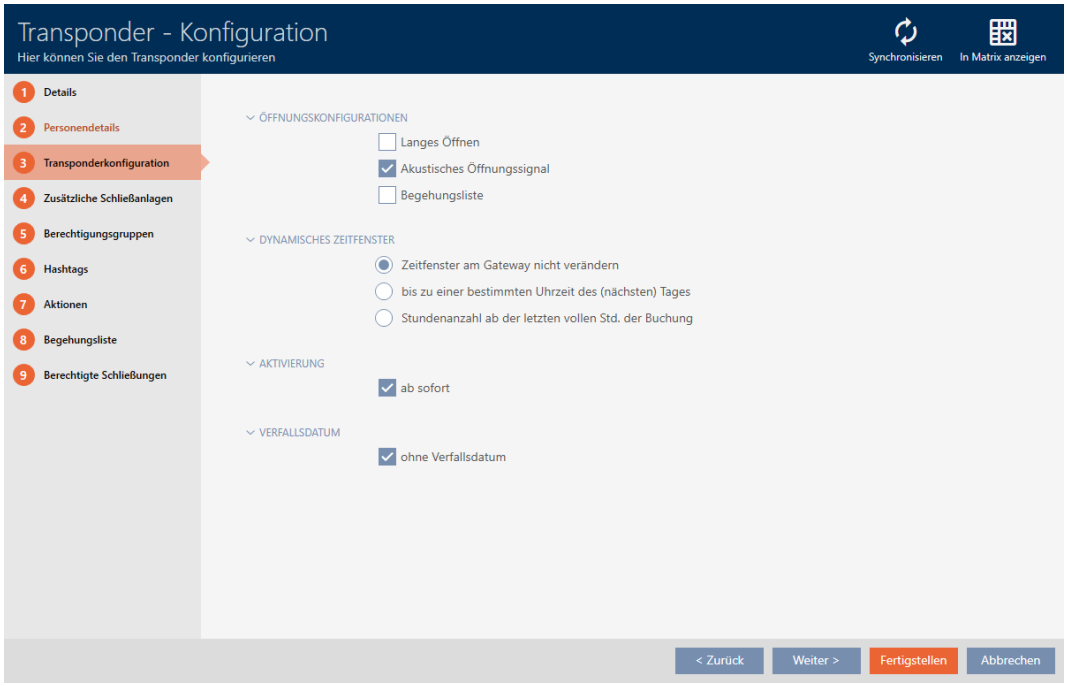
15.5.1 Für einen Transponder oder eine Karte alle Schließungen stummschalten

✓ Identmedium vorhanden.

1. Klicken Sie auf das Identmedium, das Sie stummschalten wollen.
   ↳ Fenster des Identmediums öffnet sich.
2. Klicken Sie auf den Reiter ● Transponderkonfiguration.



   ↳ Fenster wechselt zum Reiter "Transponderkonfiguration".



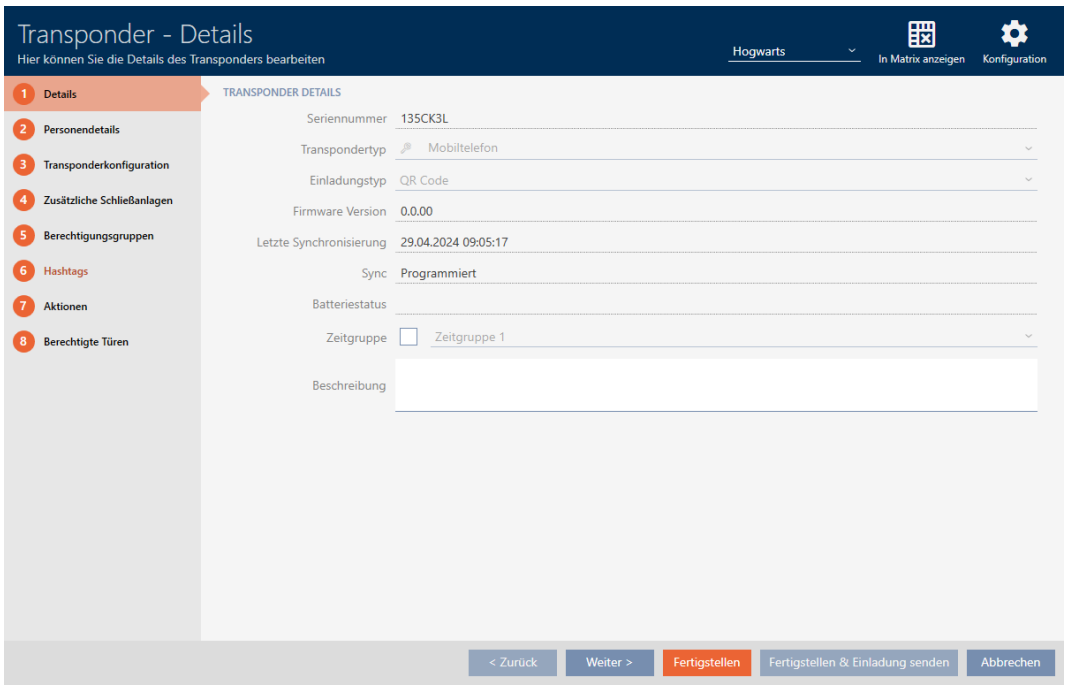
3. Deaktivieren Sie die Checkbox ☐ Akustisches Öffnungssignal.
4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

↳ Alle Schließungen sind für dieses Identmedium stummgeschalten.

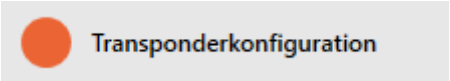
15.5.2 Für einen AX2Go-Schlüssel alle Schließungen stummschalten

✓ AX2Go-Schlüssel vorhanden.

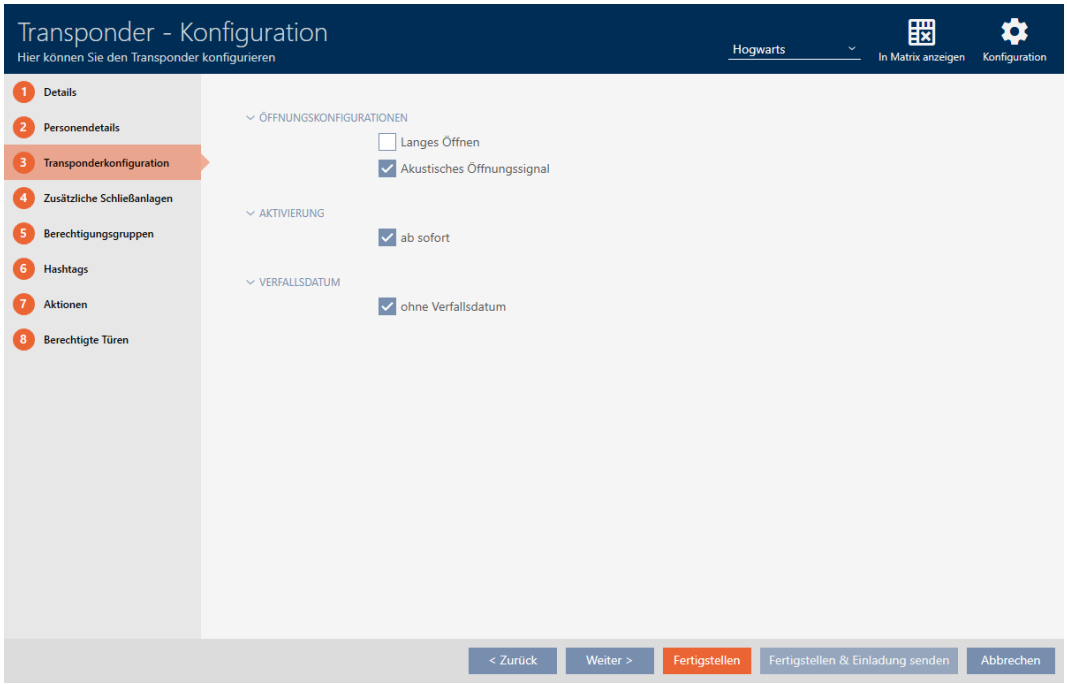
1. Klicken Sie auf den AX2Go-Schlüssel, den Sie stummschalten wollen.
   ↳ Fenster des AX2Go-Schlüssels öffnet sich.



2. Klicken Sie auf den Reiter Transponderkonfiguration.



↳ Fenster wechselt zum Reiter "Transponderkonfiguration".



3. Deaktivieren Sie die Checkbox ☐ Akustisches Öffnungssignal.
4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des AX2Go-Schlüssels schließt sich.

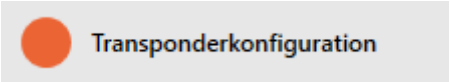
↳ Alle Schließungen sind für diesen AX2Go-Schlüssel stummgeschalten.

15.6 Zugänge durch Identmedium mitschreiben lassen (Begehungsliste)

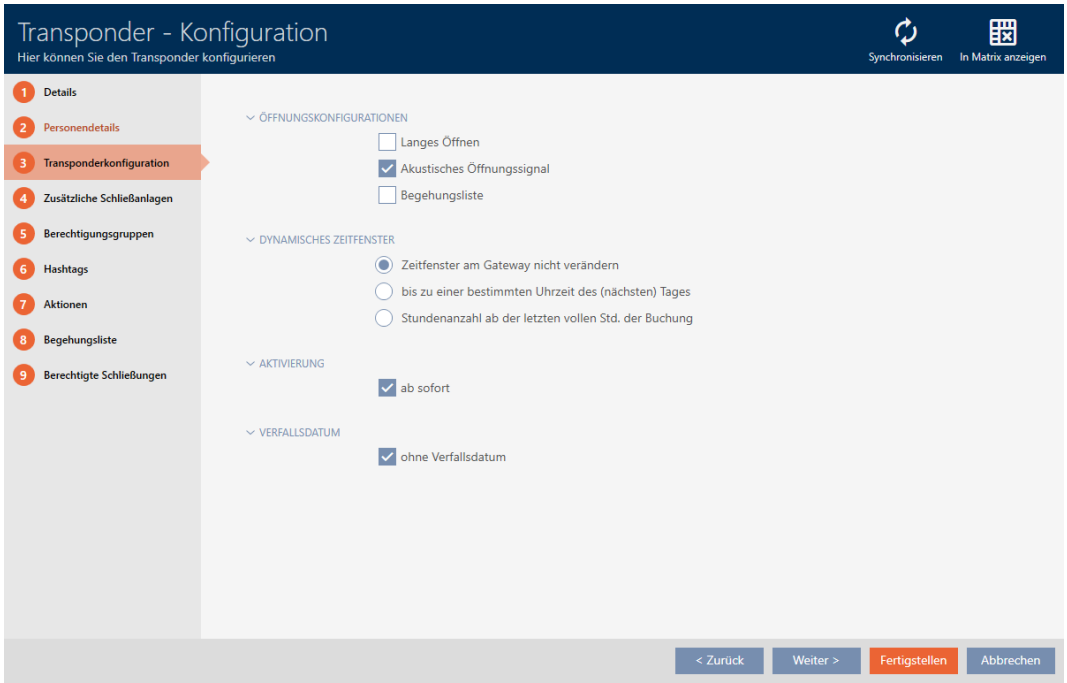
Hier schalten Sie die Begehungsliste ein. Damit protokolliert Ihr Identmedium, an welchen Schließungen es betätigt wurde (siehe auch *Begehungs- und Zutrittslisten [▸ 547]*).

✓ Identmedium vorhanden.

1. Klicken Sie auf das Identmedium, dessen Begehungsliste Sie aktivieren wollen.
   ↳ Fenster des Identmediums öffnet sich.
2. Klicken Sie auf den Reiter Transponderkonfiguration.



↳ Fenster wechselt zum Reiter "Transponderkonfiguration".



3. Aktivieren Sie die Checkbox ☑ Begehungsliste.
4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

↳ Identmedium schreibt in der Begehungsliste mit, an welchen Schließungen es betätigt wurde.

15.7 Berechtigungen des Identmediums auf bestimmte Zeiten beschränken (Zeitgruppe)

Die Berechtigungen eines Identmediums steuern Sie mit einer Zeitgruppe. Die Zeitgruppe ist ein Bestandteil des Zeitmanagements (siehe *Zeitmanagement [▸ 548]*). Zur Einrichtung des Zeitmanagements für Identmedien siehe *Zeitgruppe erstellen [▸ 61]* und *Identmedium zur Zeitgruppe hinzufügen [▸ 351]*.

15.8 Identmedium einmalig an bestimmten Zeitpunkten aktivieren oder deaktivieren (Aktivierungs- und Verfallsdatum)

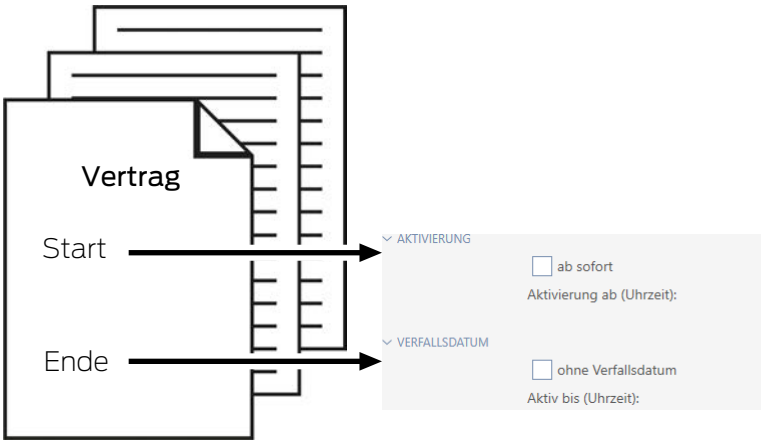
Ihre AXM Plus kennt zwei Zeitpunkte für Identmedien:

- Aktivierungsdatum
- Verfallsdatum

Diese Daten sind geeignet, wenn Identmedien erst ab einem bestimmten Zeitpunkt und/oder bis zu einem bestimmten Zeitpunkt verwendbar sein sollen. Alternativ können Sie natürlich auch erst zum Aktivierungsdatum die Berechtigungen vergeben und zum Verfallsdatum wieder entziehen. Der entscheidende Unterschied ist, dass Sie dann zu diesen Zeitpunkten aber alle beteiligten Schließungen oder das Identmedium synchronisieren müssen.

Mit einem Aktivierungs- bzw. einem Verfallsdatum ersparen Sie sich diesen Aufwand. Das Identmedium wird automatisch zu einem bestimmten Zeitpunkt an berechtigten Schließungen akzeptiert (Aktivierungsdatum) oder eben nicht mehr akzeptiert (Verfallsdatum).

Diese Funktion eignet sich zum Beispiel für befristete Arbeitsverhältnisse:



1. Synchronisieren Sie das Identmedium bequem im Voraus.
2. Setzen Sie das Aktivierungsdatum auf den Beginn des Arbeitsverhältnisses und das Verfallsdatum auf das Ende des Arbeitsverhältnisses.

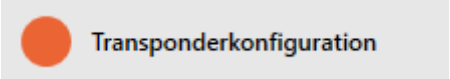
Beide Daten werden normalerweise für die Zukunft gesetzt. Wenn Sie für ein bereits bestehendes Identmedium diese Daten ändern:

- Aktivierungsdatum in der Vergangenheit: Identmedium wird mit dem nächsten Synchronisieren sofort aktiv.
- Verfallsdatum in die Vergangenheit: Identmedium wird mit dem nächsten Synchronisieren sofort inaktiv.

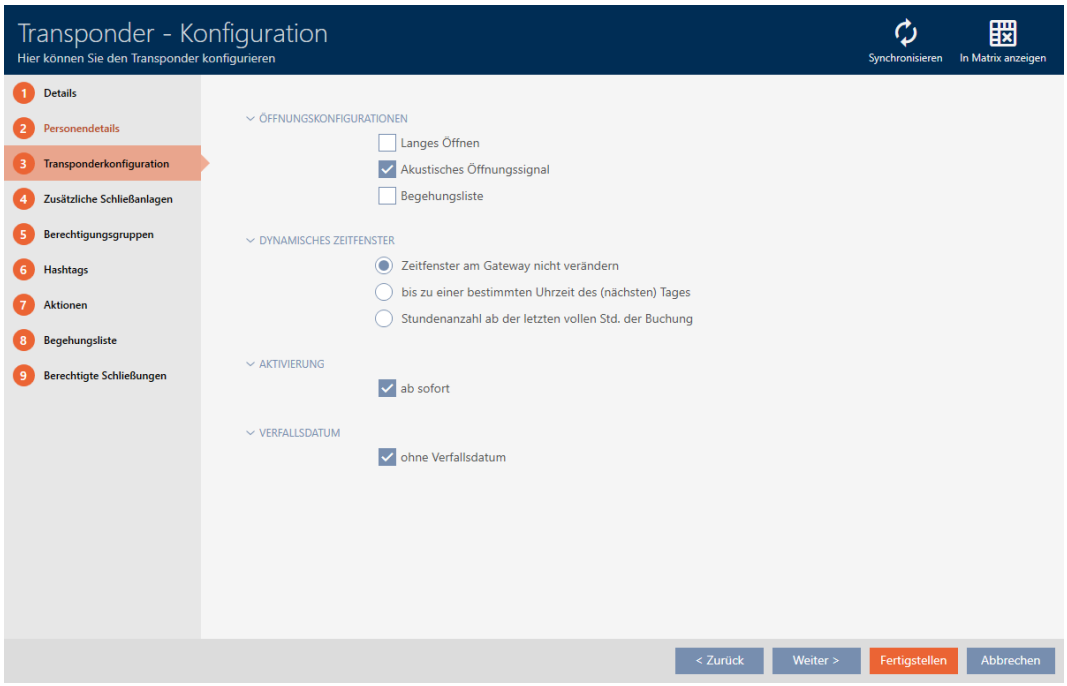
In diesem Fall zeigt die AXM eine Warnung an, z.B.:

✓ Identmedium vorhanden.

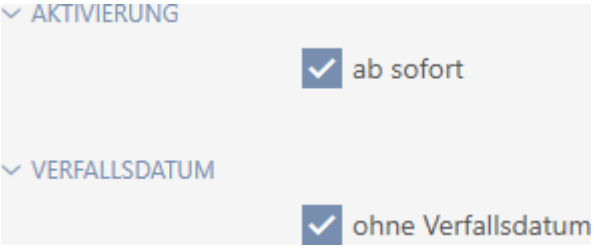
1. Klicken Sie auf das Identmedium, dessen Aktivierungs- bzw. Verfallsdatum Sie einstellen wollen.
   ↳ Fenster des Identmediums öffnet sich.
2. Klicken Sie auf den Reiter Transponderkonfiguration.



↳ Fenster wechselt zum Reiter "Transponderkonfiguration".



3. Klappen Sie ggfs. die Menüs "Aktivierung" und "Verfallsdatum" aus.



4. Wenn Sie ein Aktivierungsdatum einstellen wollen: Deaktivieren Sie die Checkbox ☐ ab sofort.
5. Stellen Sie im Dropdown-Menü ▼ **Aktivierung ab (Uhrzeit):** das Aktivierungsdatum ein oder klicken Sie auf das Symbol, um eine Kalendermaske auszuklappen.

6. Wenn Sie ein Verfallsdatum einstellen wollen: Deaktivieren Sie die Checkbox ☐ ohne Verfallsdatum.

7. Stellen Sie im Dropdown-Menü ▼ **Aktiv bis (Uhrzeit):** das Verfallsdatum ein oder klicken Sie auf das Symbol , um eine Kalendermaske auszuklappen.

8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

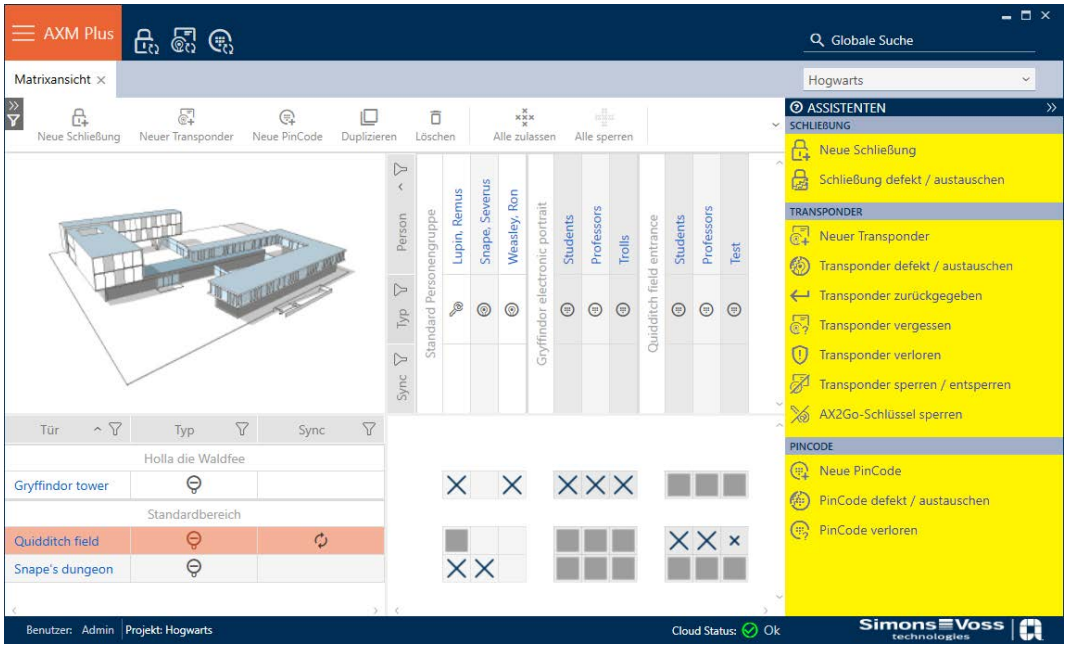
↳ Identmedium wird zu den angegebenen Zeiten aktiv bzw. inaktiv.

15.9 Defekte Identmedien behandeln

Identmedien können Defekte erleiden:

- Softwaredefekt
- Hardwaredefekt

Grundsätzlich lassen sich alle Aktionen über den Assistenten-Bereich auf der rechten Seite erreichen:



Falls das Identmedium durch Diebstahl oder Verlust abhanden gekommen ist, müssen Sie es sperren (siehe *Verlorenen/gestohlenen Transponder/ Karte dauerhaft sperren und austauschen [▸ 169]*).

Die folgende Übersicht hilft Ihnen, sich für das richtige Vorgehen zu entscheiden. Hilfreich ist es, wenn Sie wissen, wie Identmedien und TID zusammenhängen (siehe *Identmedien, Schließungen und der Schließplan [▸ 532]*).

Transponder/Ersatztransponder wird unmittelbar wieder benötigt:

Geeignet für:

Neu synchronisieren (Instandsetzen)	Zurücksetzen und austauschen	Löschen und austauschen
Identmedien mit undefiniertem Softwarezustand.	▪ Äußerlich beschädigte Identmedien (z.B. verkratzt). ▪ Identmedien, die vorsichtshalber ersetzt werden sollen (z.B. nass geworden).	Endgültig zerstörte Identmedien (z.B. verbrannt), für die Ersatz benötigt wird.

Situationsbeispiel:

Neu synchronisieren (Instandsetzen)	Zurücksetzen und austauschen	Löschen und austauschen
	Transponder des Mitarbeiters in Pool gefallen. Folge: Transponder funktionsfähig, aber durch Wassereinwirkung ausfallgefährdet.	Transponder des Mitarbeiters in Lagerfeuer gefallen. Folge: Transponder geschmolzen und endgültig zerstört.

Ablauf:

Neu synchronisieren (Instandsetzen)	Zurücksetzen und austauschen	Löschen und austauschen
Transponder/Karte instandsetzen (Neu synchronisieren) [▸ 134] 1. Zurücksetzen (= TID in Datenbank wieder frei) 2. Neu synchronisieren (= TID wird sofort wieder in dasselbe Identmedium geschrieben) Das Identmedium funktioniert nach der Instandsetzung wieder wie vorher.	*Transponder/Karte zurücksetzen und austauschen [▸ 139]* 1. Zurücksetzen (= TID in Datenbank als defekt markiert und aus Original-Identmedium entfernt) 2. Austausch-Identmedium mit neuer TID synchronisieren Durch das Zurücksetzen ist die TID nicht mehr im Identmedium vorhanden. Das Identmedium ist daher nicht mehr verwendbar. Es kann aber neu synchronisiert werden. Dabei wird eine neue TID in das Identmedium geschrieben.	*Transponder/Karte löschen und austauschen [▸ 142]* 1. Löschen (= TID in Datenbank als defekt markiert) und aus Projekt entfernt 2. Austausch-Identmedium mit der neuen TID synchronisieren Ein zerstörtes Identmedium kann logischerweise nicht zurückgesetzt werden, da es nicht mehr ansprechbar ist. Damit bleibt die TID im Identmedium. Durch das Löschen können Sie Ihr Projekt "aufräumen". Die als "defekt" markierte TID bleibt unabhängig davon dauerhaft in der Datenbank gespeichert und wird nicht mehr neu vergeben. Alternativ zum Löschen können Sie defekte oder deaktivierte Identmedien auch ausblenden (siehe *Deaktivierte und defekte Identmedien ausblenden [▸ 456]*).

Transponder/Ersatztransponder wird nicht benötigt:

Geeignet für:

Außer Betrieb nehmen und im Projekt lassen	Außer Betrieb nehmen und aus Projekt entfernen
Endgültig zerstörte Identmedien (z.B. verbrannt), für die kein Ersatz benötigt wird (z.B. Mitarbeiter gekündigt)	Endgültig zerstörte Identmedien (z.B. verbrannt), für die kein Ersatz benötigt wird (z.B. Mitarbeiter gekündigt)

Situationsbeispiel:

Außer Betrieb nehmen und im Projekt lassen	Außer Betrieb nehmen und aus Projekt entfernen
Transponder des Mitarbeiters bei Abschiedsfeier von Mitarbeiter in Lagerfeuer gefallen. Folge: Transponder geschmolzen und endgültig zerstört, Mitarbeiter nicht mehr vorhanden.	Transponder des Mitarbeiters bei Abschiedsfeier von Mitarbeiter in Lagerfeuer gefallen. Folge: Transponder geschmolzen und endgültig zerstört, Mitarbeiter nicht mehr vorhanden.

Ablauf:

Außer Betrieb nehmen und im Projekt lassen	Außer Betrieb nehmen und aus Projekt entfernen
Transponder/Karte außer Betrieb nehmen und in Projekt lassen [▸ 150] 1. Als außer Betrieb genommen markieren (= TID in Datenbank als defekt markiert) Das zerstörte Identmedium behält zwar seine TID, in der Datenbank wird die TID aber dauerhaft als "defekt" markiert. Neue Identmedien können nicht mit dieser TID angelegt werden. Somit kann dieselbe TID nicht zweimal in Umlauf kommen.	*Transponder/Karte außer Betrieb nehmen und aus Projekt löschen [▸ 157]* 1. Löschen (= TID in Datenbank als defekt markiert) und aus Projekt entfernt Durch das Löschen können Sie Ihr Projekt "aufräumen". Die als "defekt" markierte TID bleibt unabhängig davon dauerhaft in der Datenbank gespeichert und wird nicht mehr neu vergeben. Alternativ zum Löschen können Sie defekte oder deaktivierte Identmedien auch ausblenden (siehe *Deaktivierte und defekte Identmedien ausblenden [▸ 456]*).

Defekte PinCode-Tastatur behandeln

Analog zu Transpondern und Karten haben Sie auch bei einer defekten PinCode-Tastatur verschiedene Möglichkeiten:

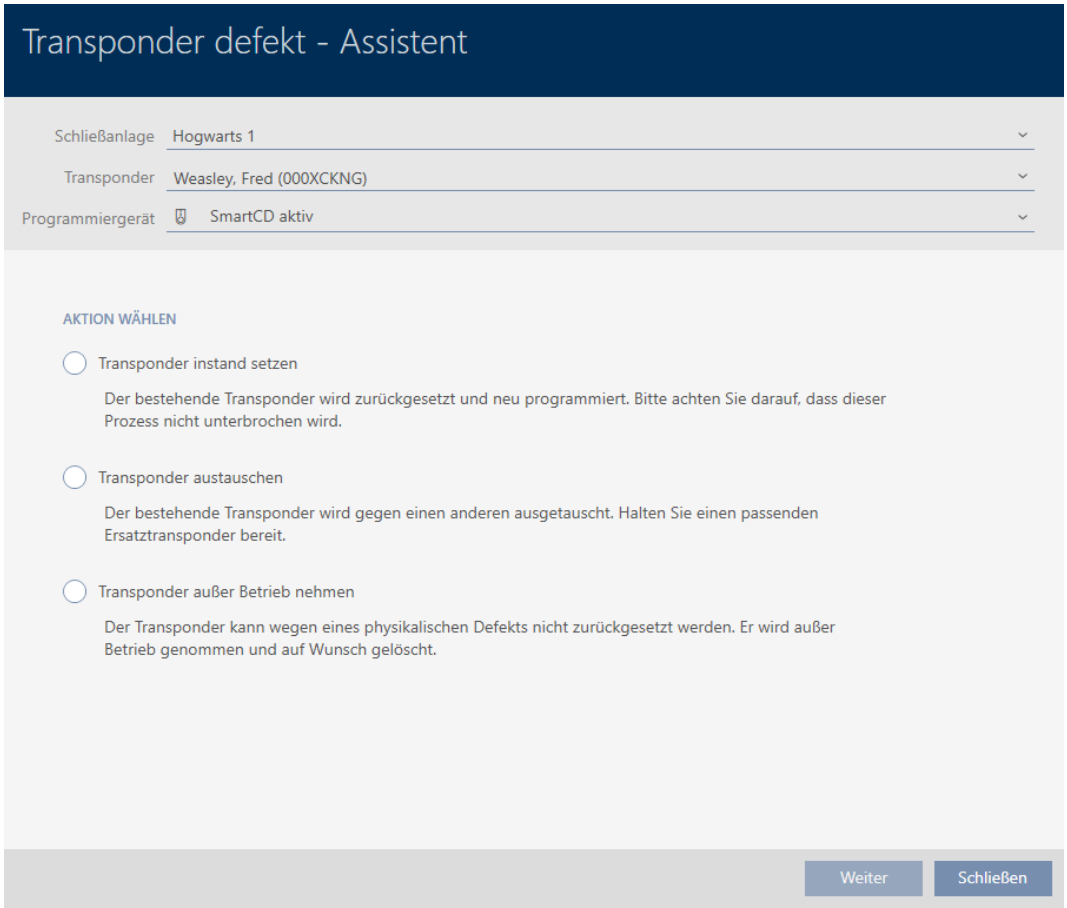
- PinCode instand setzen (siehe *PinCode-Tastatur instandsetzen (Neu synchronisieren) [▸ 135]*
- Zurücksetzen und PinCode austauschen (manuell, nicht über Assistent - siehe *PinCode-Tastatur zurücksetzen und austauschen [▸ 142]*)
- Löschen und PinCode austauschen (siehe *PinCode-Tastatur löschen und austauschen [▸ 145]*)
- PinCode außer Betrieb nehmen und im Projekt lassen (siehe *PinCode-Tastatur außer Betrieb nehmen und in Projekt lassen [▸ 153]*)
- PinCode außer Betrieb nehmen und aus Projekt entfernen (siehe *PinCode-Tastatur außer Betrieb nehmen und aus Projekt löschen [▸ 159]*)

15.9.1 Instandsetzen/neu synchronisieren

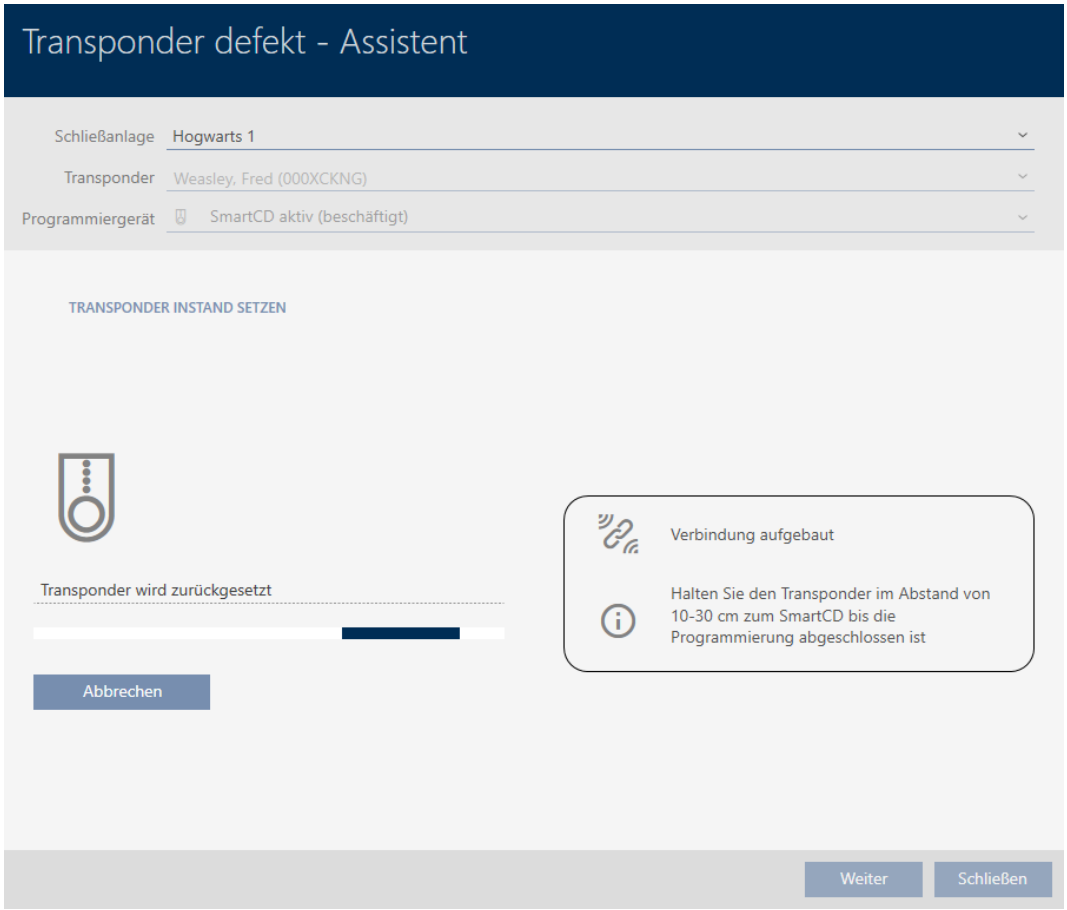
15.9.1.1 Transponder/Karte instandsetzen (Neu synchronisieren)

- ✓ Identmedienliste oder Matrix geöffnet.
- ✓ Identmedium vorliegend.
- ✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das defekte Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder defekt / austauschen.
   ↳ Assistent zum Behandeln eines defekten Identmediums öffnet sich.

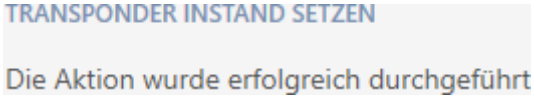


4. Wählen Sie die Option Transponder instand setzen.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Identmedium wird zurückgesetzt.



↳ Identmedium wird synchronisiert.

↳ Identmedium wurde mit denselben Einstellungen neu synchronisiert.



15.9.1.2 PinCode-Tastatur instandsetzen (Neu synchronisieren)

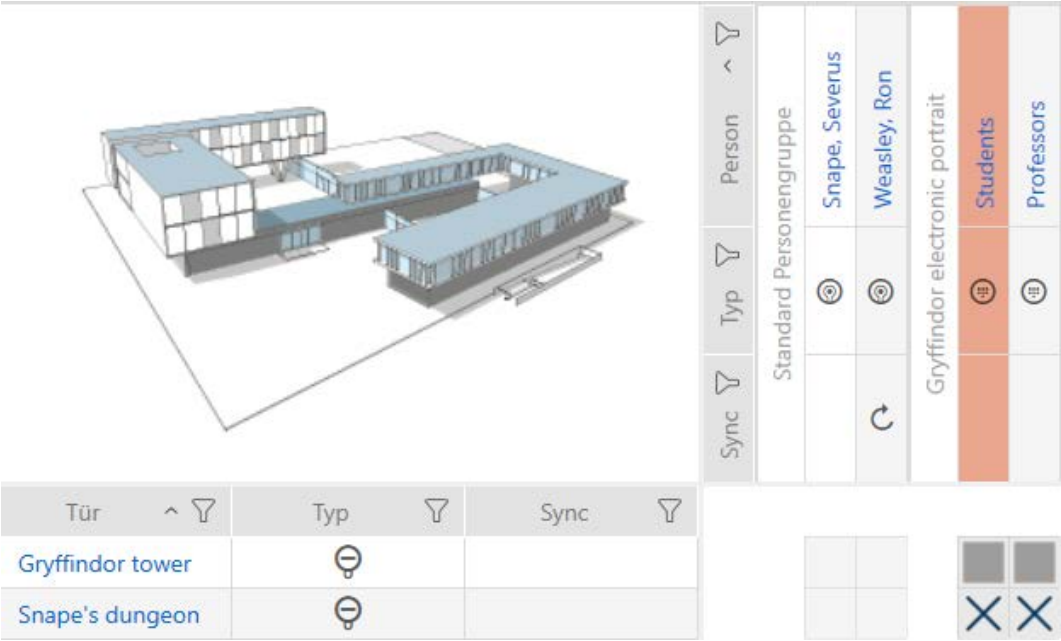
✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

✓ PinCode-Tastatur vorliegend.

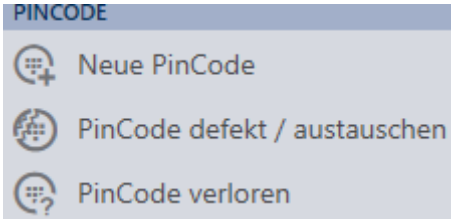
✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

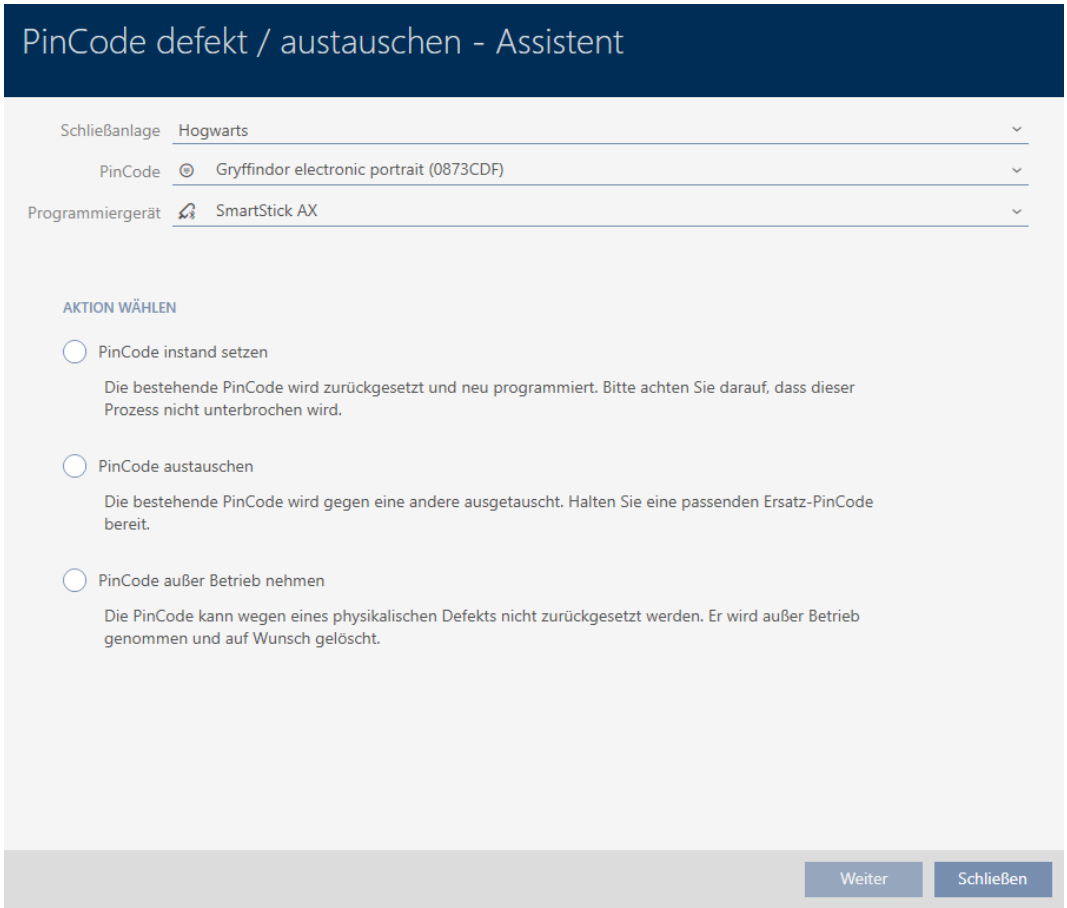
2. Markieren Sie eine PIN der defekten PinCode-Tastatur.



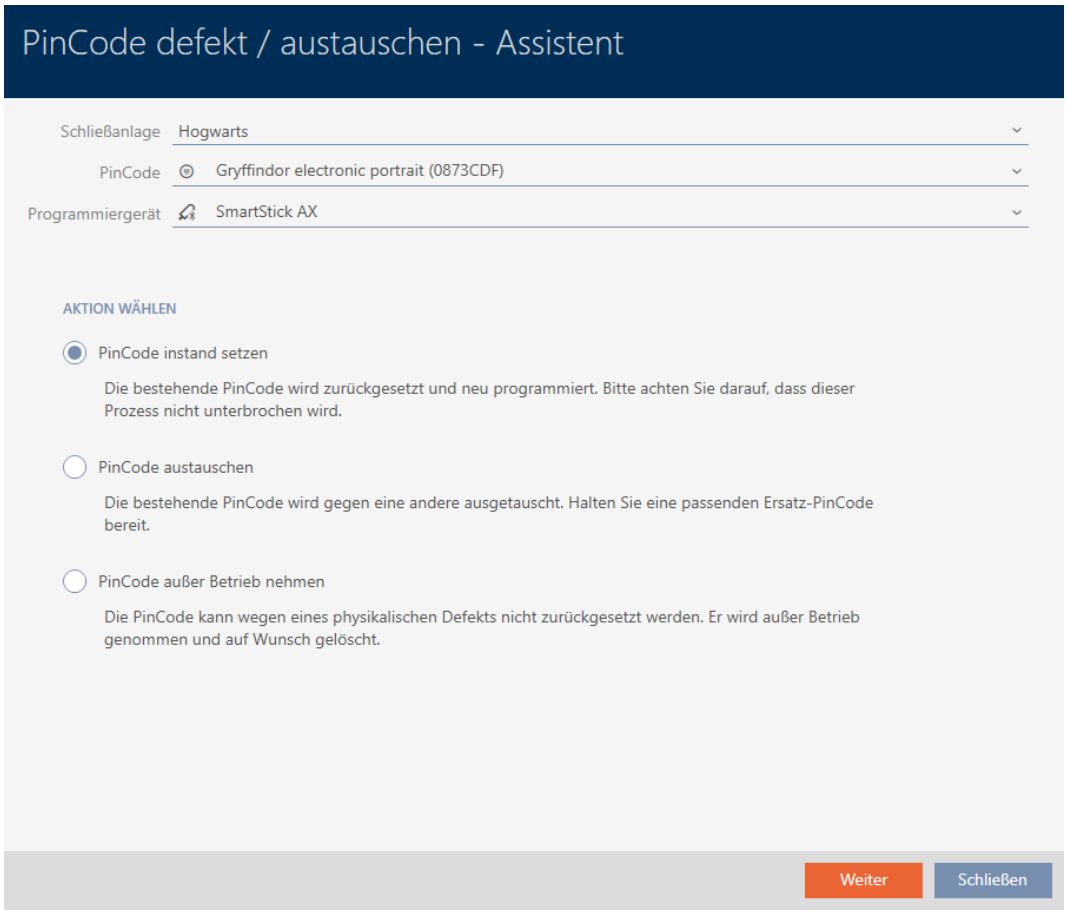
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche PinCode defekt / austauschen.



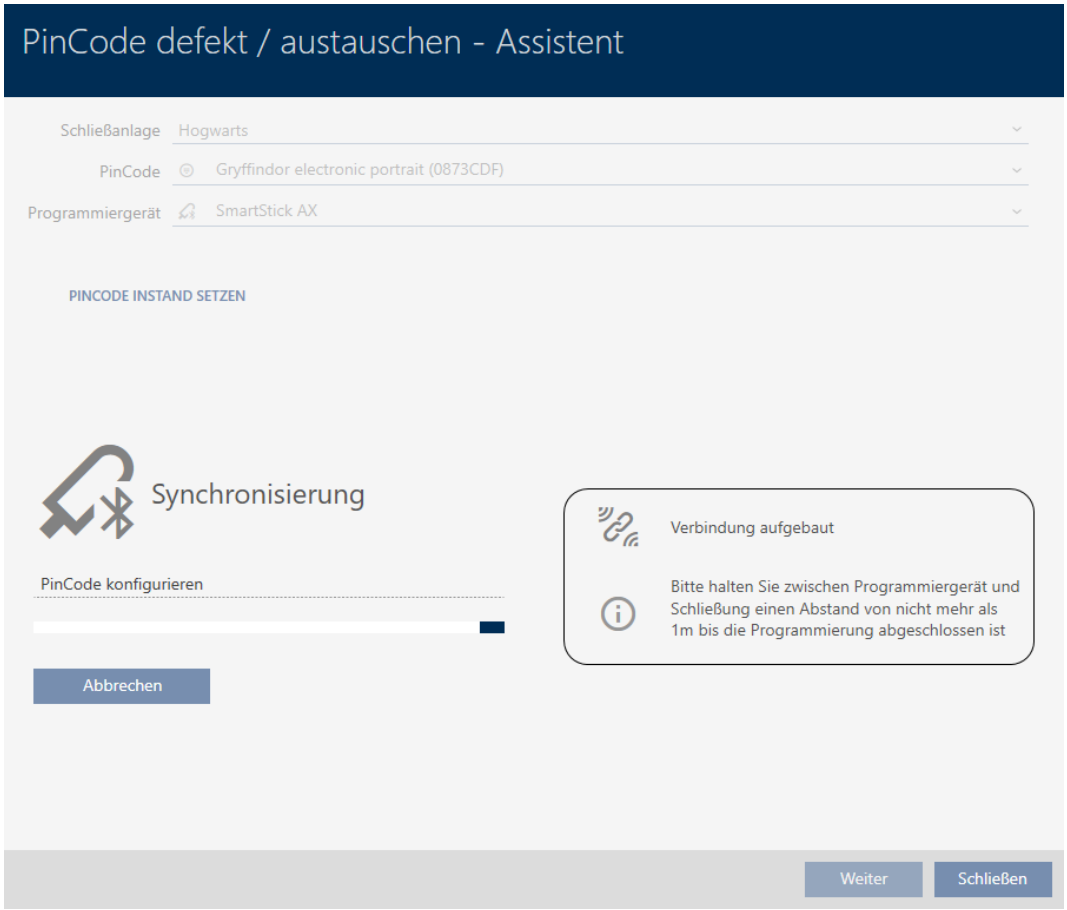
↳ Assistent zum Behandeln einer defekten PinCode-Tastatur öffnet sich.


PinCode defekt / austauschen - Assistent
Schließanlage
Hogwarts
PinCode
Gryffindor electronic portrait (0873CDF)
Programmiergerät
SmartStick AX
AKTION WÄHLEN
PinCode instand setzen
Die bestehende PinCode wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.
PinCode austauschen
Die bestehende PinCode wird gegen eine andere ausgetauscht. Halten Sie eine passenden Ersatz-PinCode bereit.
PinCode außer Betrieb nehmen
Die PinCode kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Er wird außer Betrieb genommen und auf Wunsch gelöscht.
Weiter
Schließen

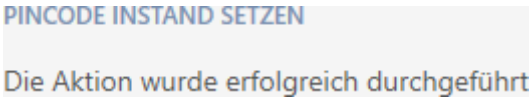
4. Wählen Sie die Option PinCode instand setzen.



5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ PinCode-Tastatur wird zurückgesetzt.



6. Folgen Sie den Anweisungen.
↳ PinCode-Tastatur wurde mit denselben Einstellungen neu synchronisiert.

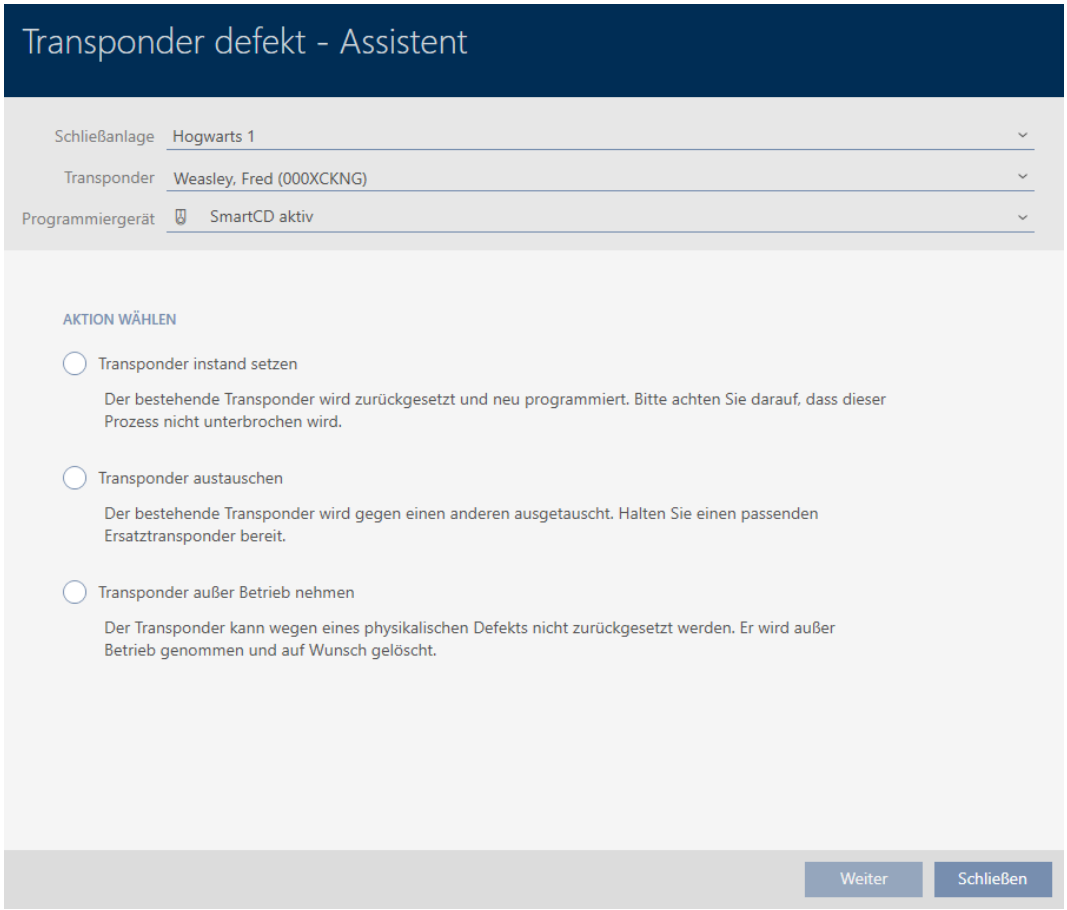


15.9.2 Zurücksetzen und austauschen

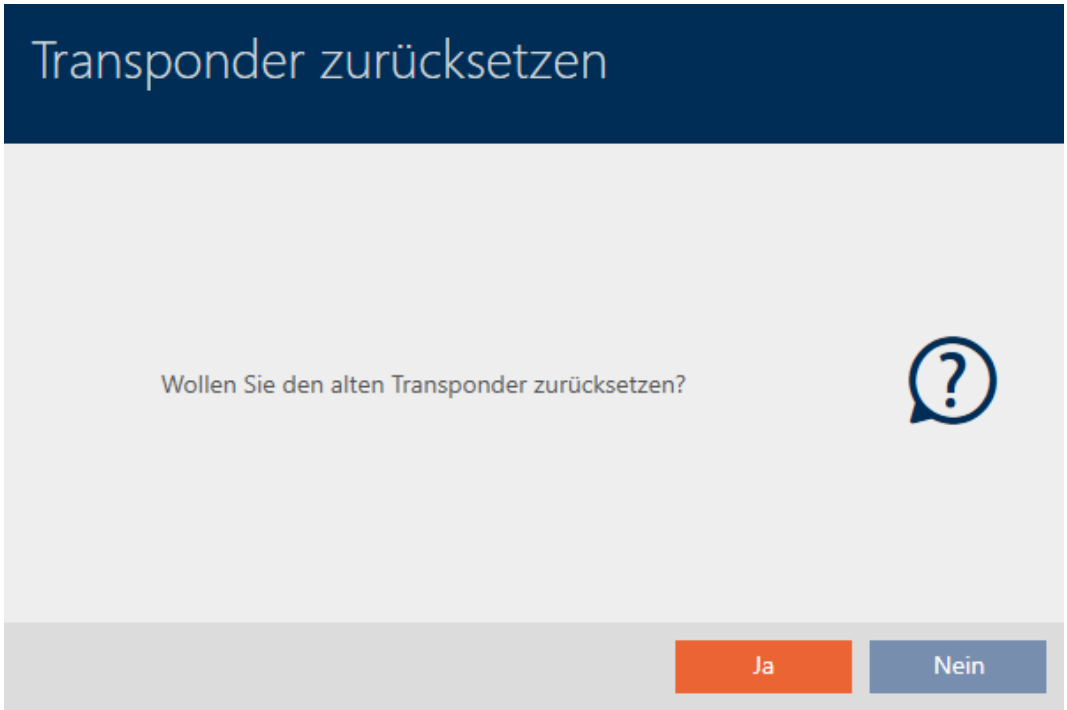
15.9.2.1 Transponder/Karte zurücksetzen und austauschen

✓ Identmedienliste oder Matrix geöffnet.
✓ Identmedium vorliegend.
✓ Austausch-Identmedium vorliegend.
✓ Geeignetes Programmiergerät angeschlossen.

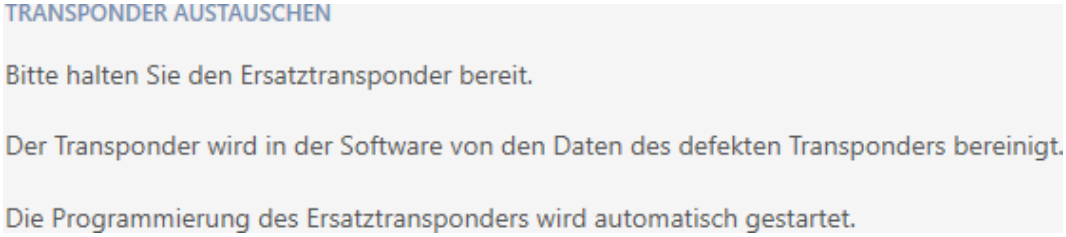
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das defekte Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder defekt / austauschen.
   ↳ Assistent zum Behandeln eines defekten Identmediums öffnet sich.



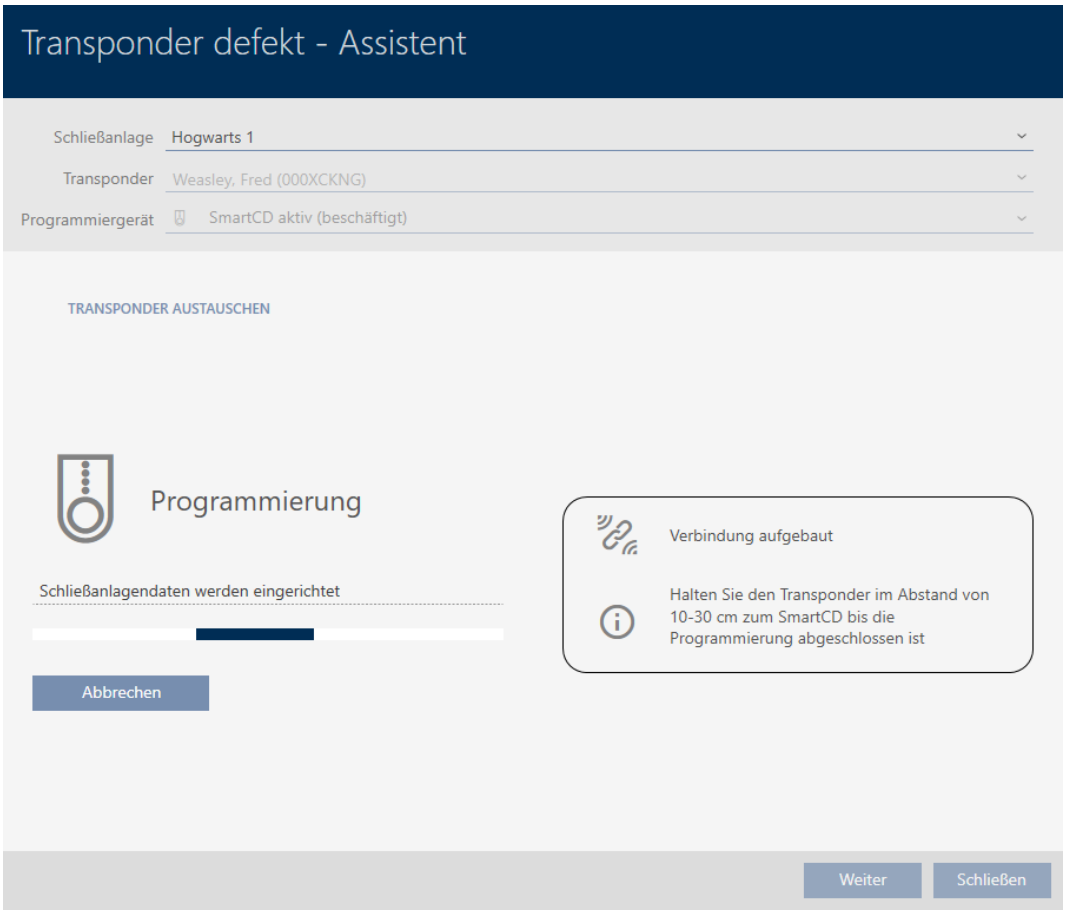
4. Wählen Sie die Option ◉ Transponder austauschen.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.



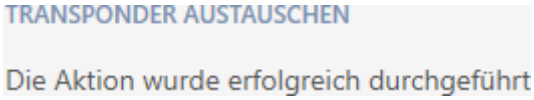
6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Identmedium wird zurückgesetzt.
   ↳ Assistent bereitet Programmierung des Austausch-Identmediums vor.



7. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Austausch-Identmedium wird programmiert.



↳ Austausch-Identmedium ist synchronisiert.



15.9.2.2 PinCode-Tastatur zurücksetzen und austauschen

Für dieses Prozedere gibt es keinen Assistenten. Gehen Sie stattdessen wie folgt vor:

- ✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.
- ✓ PinCode-Tastatur vorliegend.
- ✓ Geeignetes Programmiergerät angeschlossen.
- ✓ Austausch-PinCode-Tastatur vorliegend.

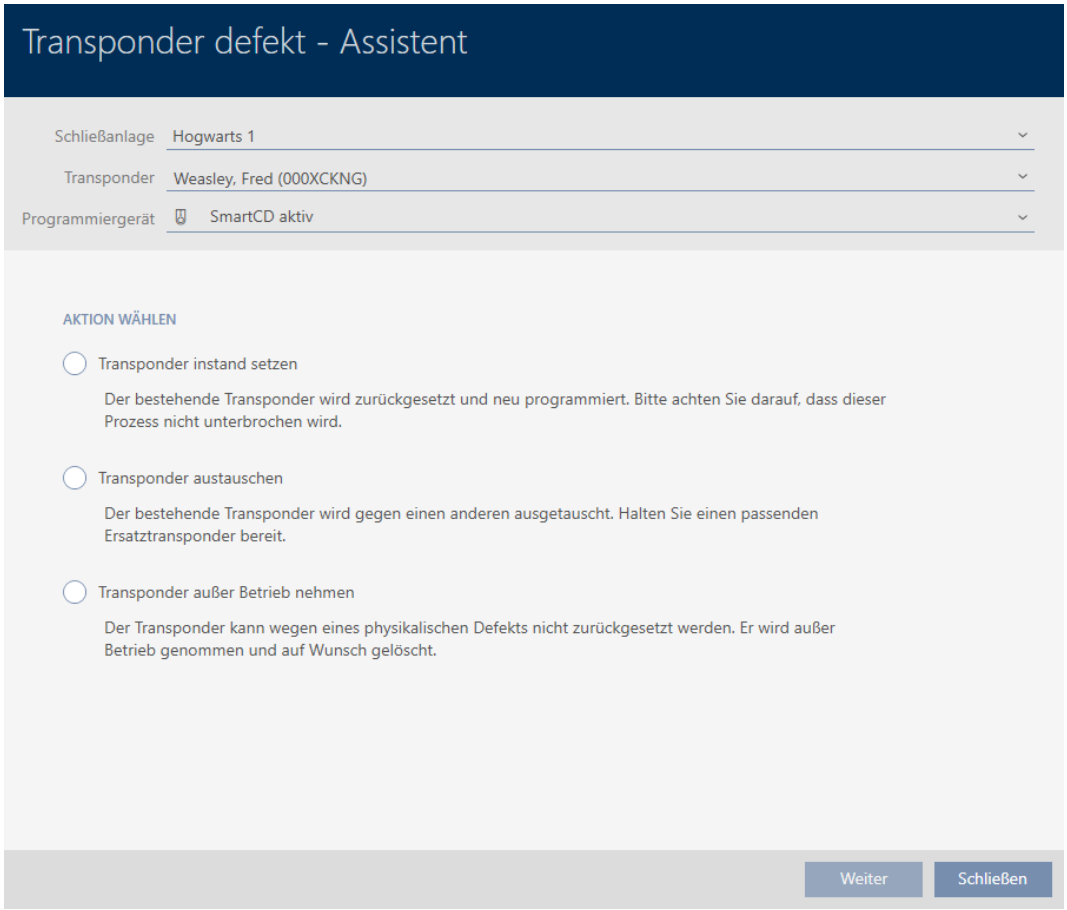
1. Setzen Sie die defekte PinCode-Tastatur zurück (siehe *Transponder/ Karten zurücksetzen [▸ 443]*).
2. Legen Sie eine neue PinCode-Tastatur an (siehe *PinCode-Tastaturen erstellen [▸ 102]*).
3. Synchronisieren Sie die neue PinCode-Tastatur (siehe *PinCode-Tastatur synchronisieren [▸ 433]*).

15.9.3 Löschen und austauschen

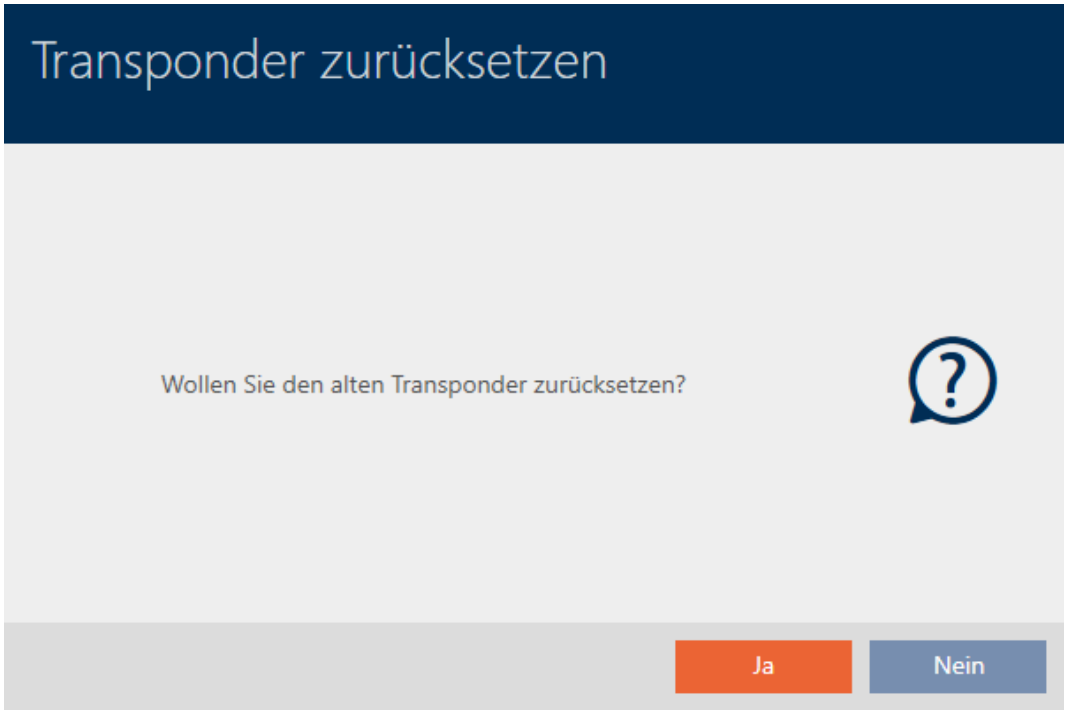
15.9.3.1 Transponder/Karte löschen und austauschen

- ✓ Identmedienliste oder Matrix geöffnet.
- ✓ Identmedium vorliegend.
- ✓ Austausch-Identmedium vorliegend.
- ✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das defekte Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder defekt / austauschen .
   ↳ Assistent zum Behandeln eines defekten Identmediums öffnet sich.

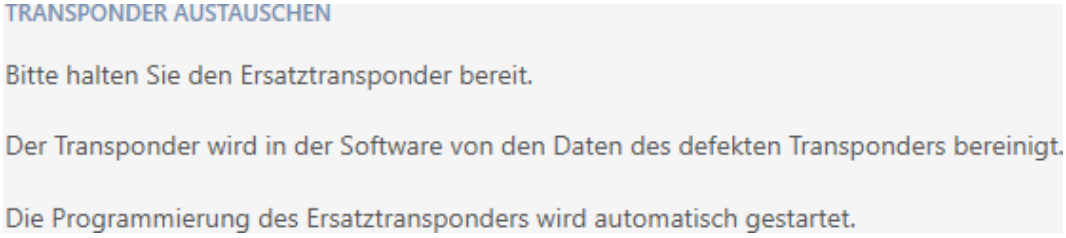


4. Wählen Sie die Option ◉ Transponder austauschen.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.

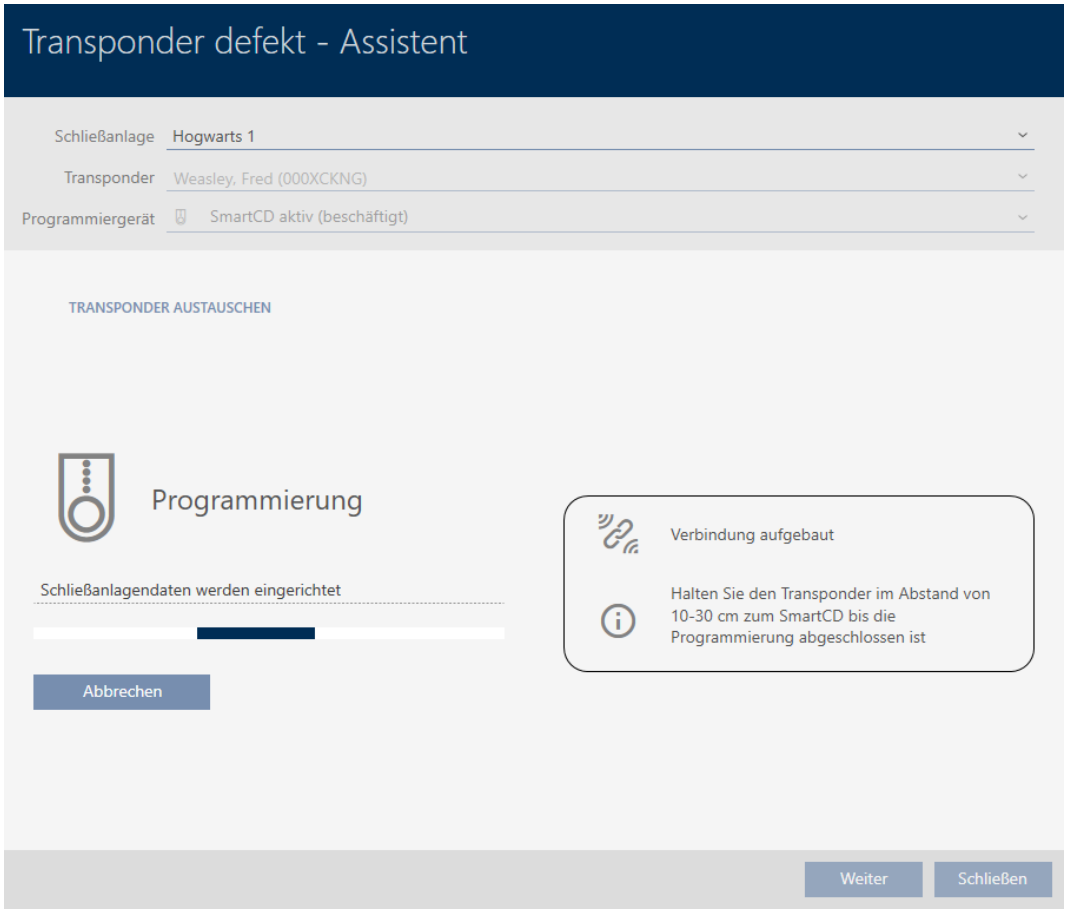


6. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Hinweis zur Prüfung des Defekts öffnet sich.

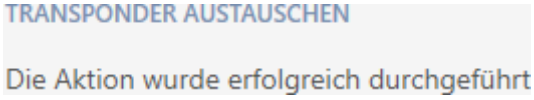
7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Hinweis zur Prüfung des Defekts schließt sich.
   ↳ Assistent bereitet Programmierung des Austausch-Identmediums vor.



8. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Austausch-Identmedium wird synchronisiert.



↳ Austausch-Identmedium ist synchronisiert.



Sie können das Identmedium jetzt löschen (siehe *Identmedium löschen [▸ 115]*).

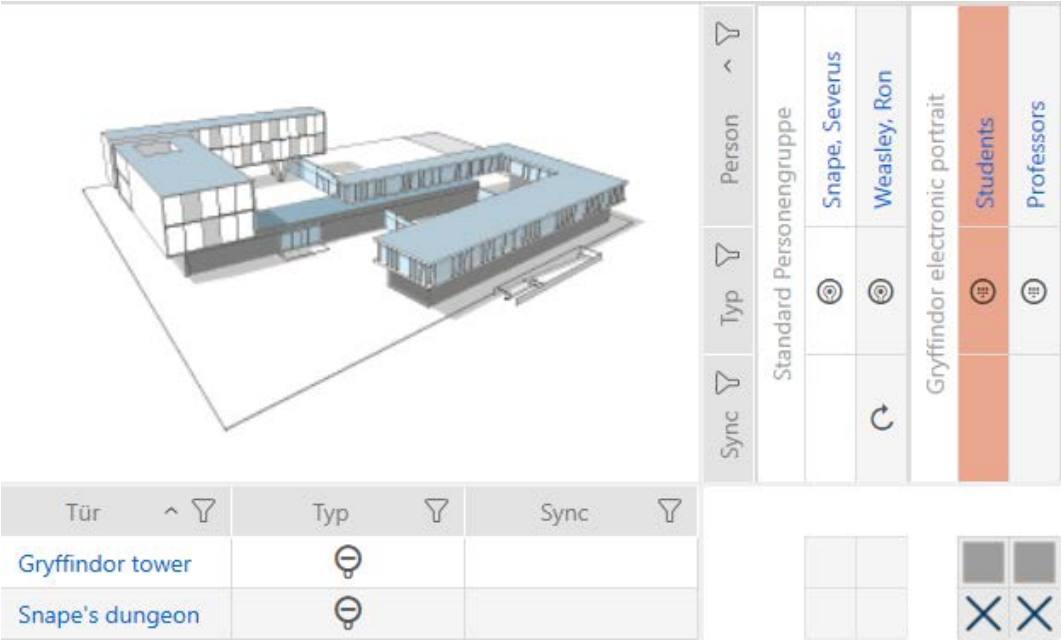
15.9.3.2 PinCode-Tastatur löschen und austauschen

✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

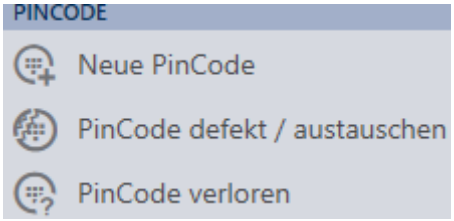
✓ Austausch-PinCode-Tastatur vorliegend.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

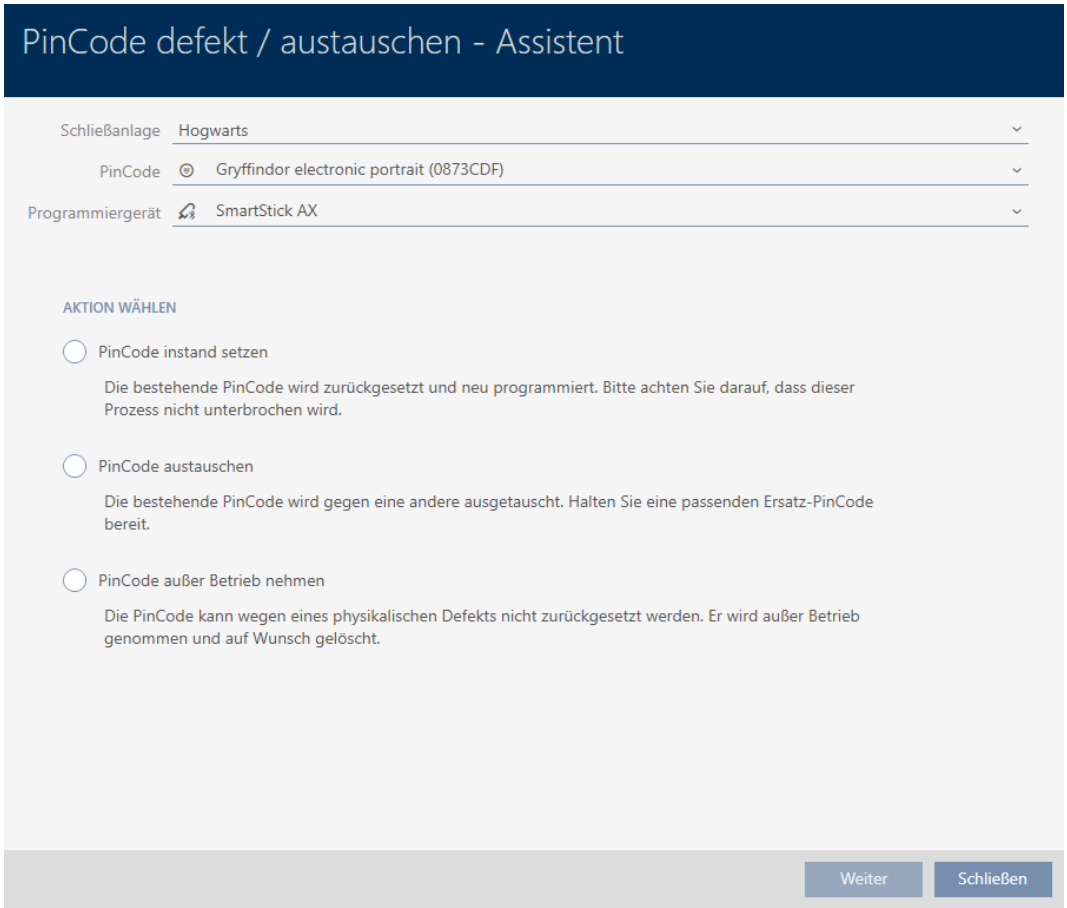
2. Markieren Sie eine PIN der defekten PinCode-Tastatur.



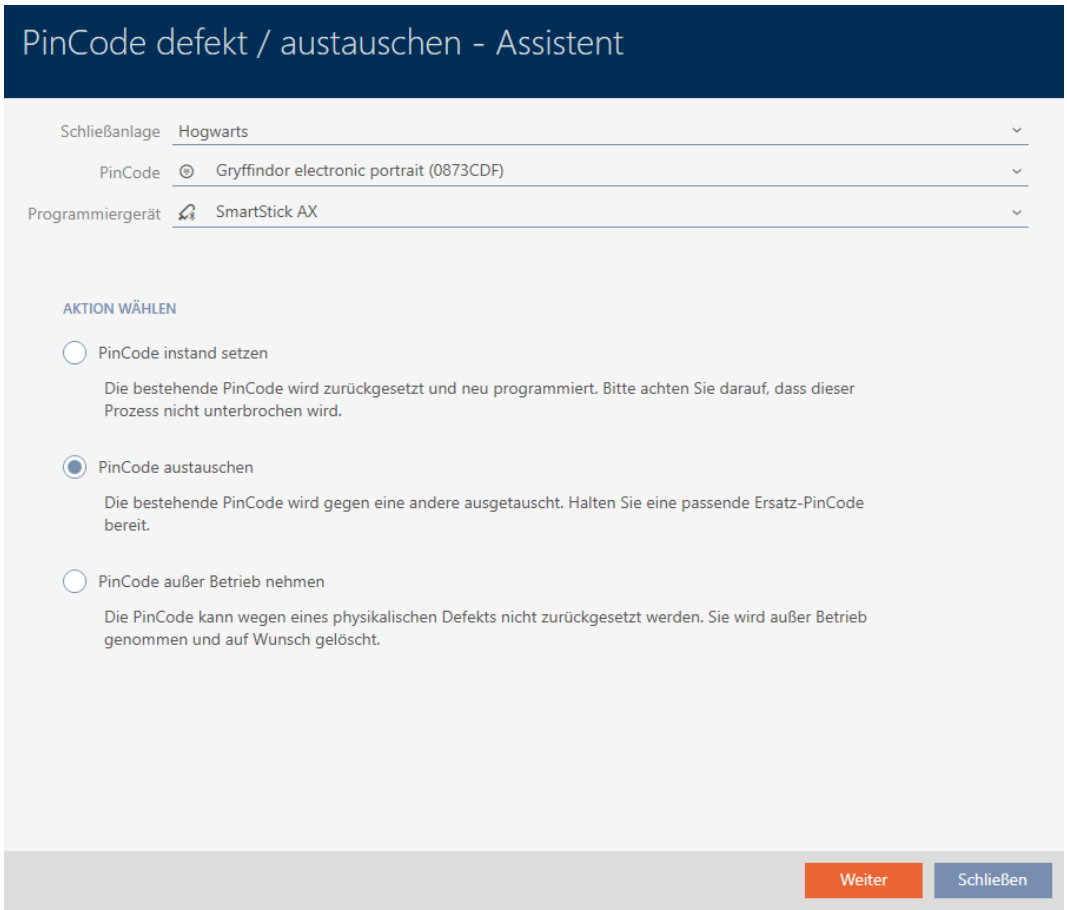
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche PinCode defekt / austauschen.



↳ Assistent zum Behandeln einer defekten PinCode-Tastatur öffnet sich.

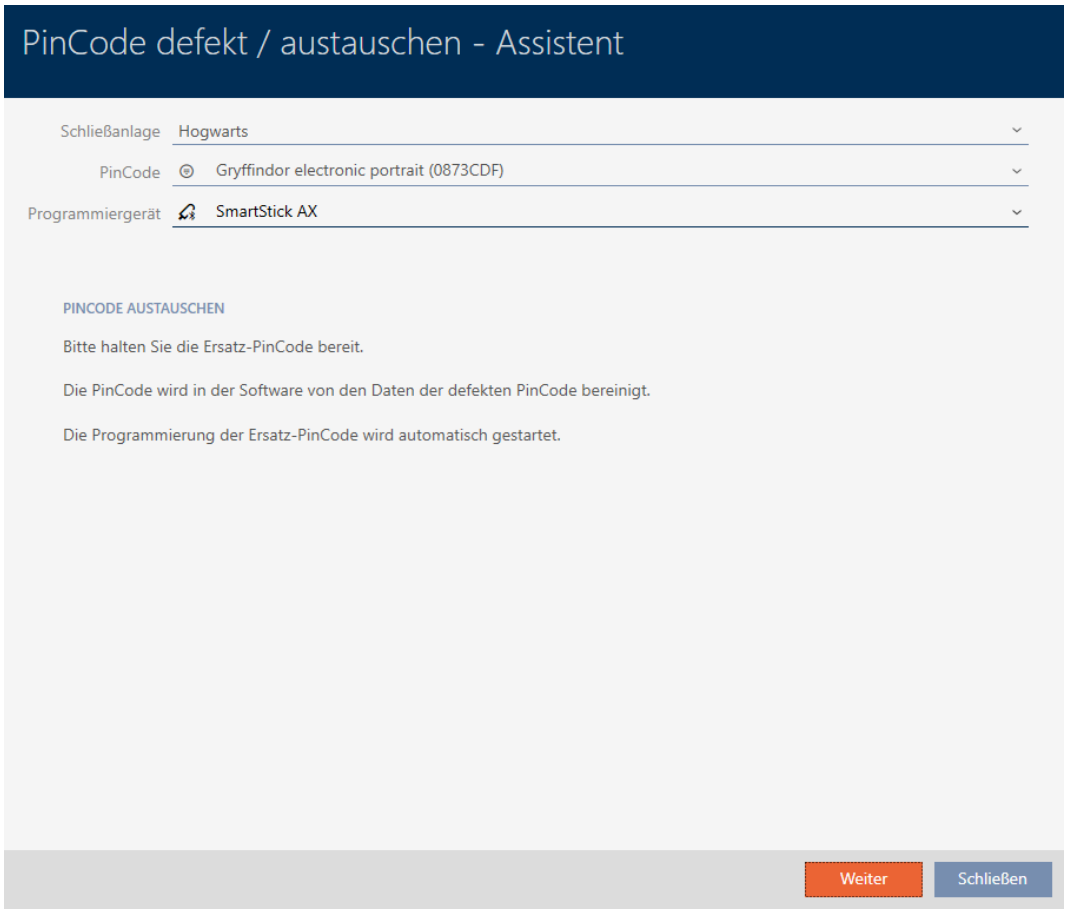

PinCode defekt / austauschen - Assistent
Schließanlage
Hogwarts
PinCode
Gryffindor electronic portrait (0873CDF)
Programmiergerät
SmartStick AX
AKTION WÄHLEN
PinCode instand setzen
Die bestehende PinCode wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.
PinCode austauschen
Die bestehende PinCode wird gegen eine andere ausgetauscht. Halten Sie eine passenden Ersatz-PinCode bereit.
PinCode außer Betrieb nehmen
Die PinCode kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Er wird außer Betrieb genommen und auf Wunsch gelöscht.
Weiter
Schließen

4. Wählen Sie die Option ◉ PinCode austauschen.

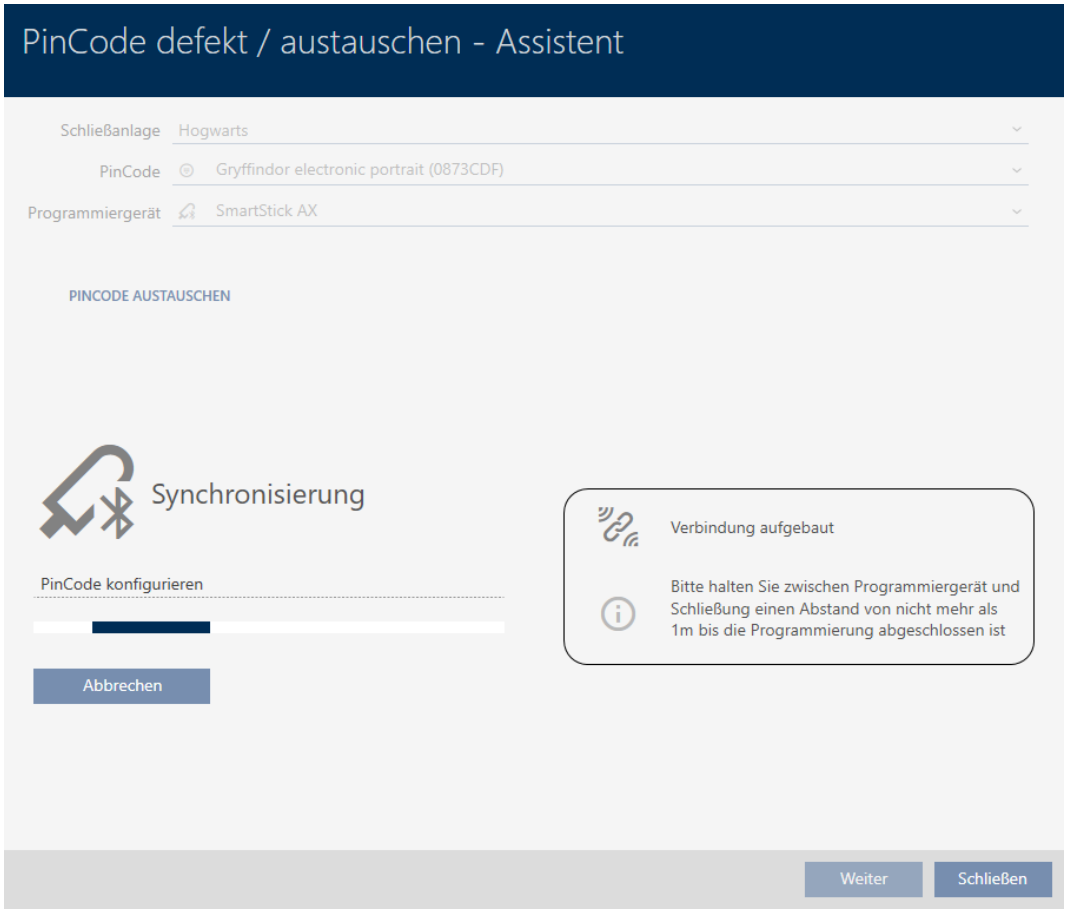


5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Austausch öffnet sich.

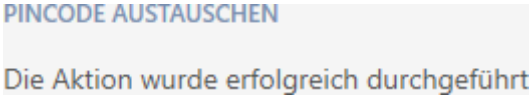
6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Synchronisierung der Ersatz-PinCode-Tastatur wird vorbereitet.



7. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Ersatz-PinCode-Tastatur wird synchronisiert.



↳ PinCode-Tastatur ist ausgetauscht.

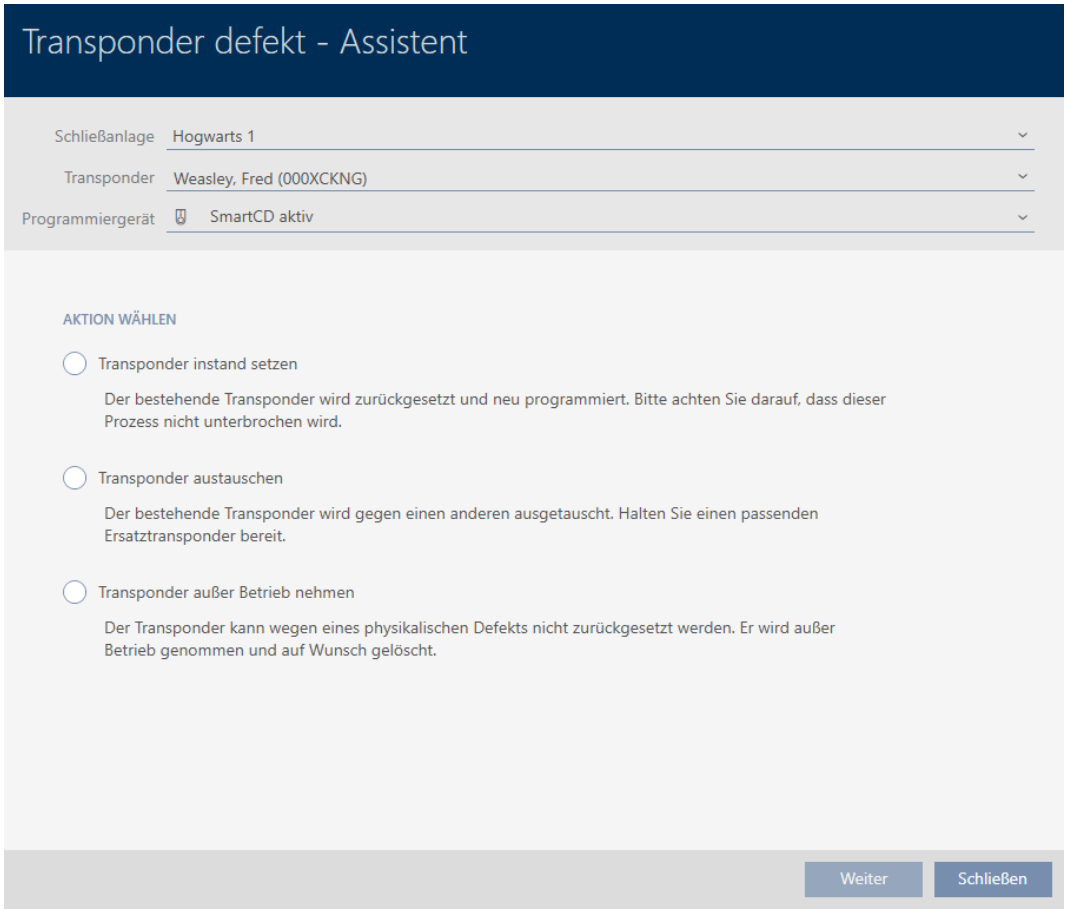


15.9.4 Außer Betrieb nehmen und in Projekt lassen

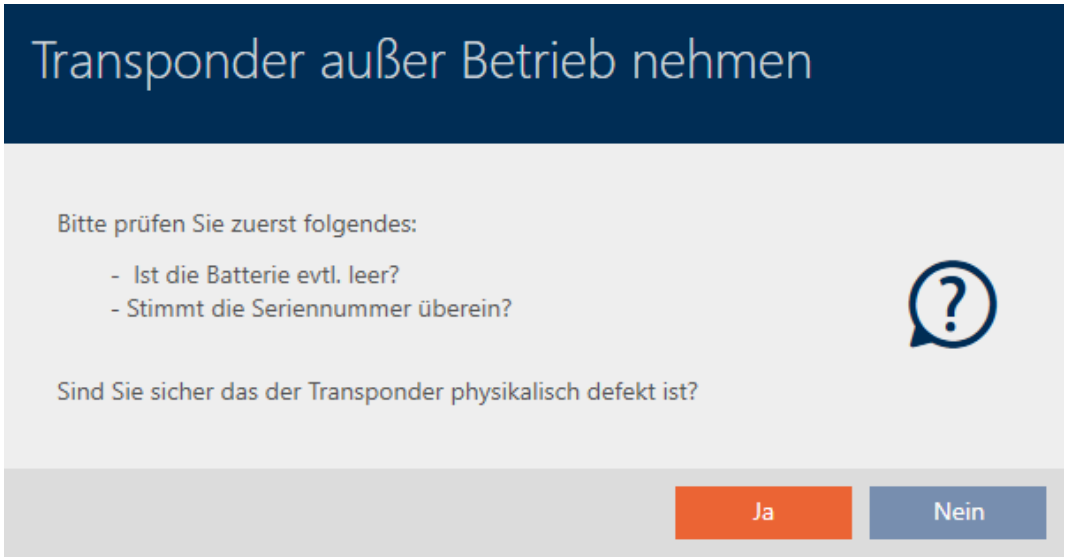
15.9.4.1 Transponder/Karte außer Betrieb nehmen und in Projekt lassen

✓ Identmedienliste oder Matrix geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das defekte Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder defekt / austauschen.
   ↳ Assistent zum Behandeln eines defekten Identmediums öffnet sich.



4. Wählen Sie die Option ◉ Transponder außer Betrieb nehmen.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zur Außerbetriebnahme öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zur Außerbetriebnahme schließt sich.
   ↳ Rückfrage zum Löschen des Identmediums öffnet sich.

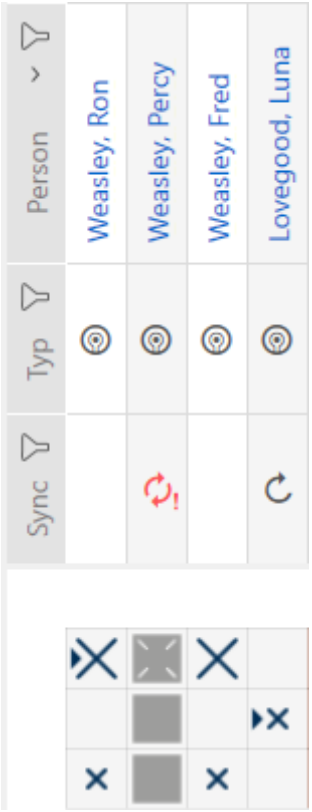
7. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Löschen des Identmediums schließt sich.

↳ Identmedium ist außer Betrieb genommen.

TRANSPONDER AUßER BETRIEB NEHMEN

Die Aktion wurde erfolgreich durchgeführt

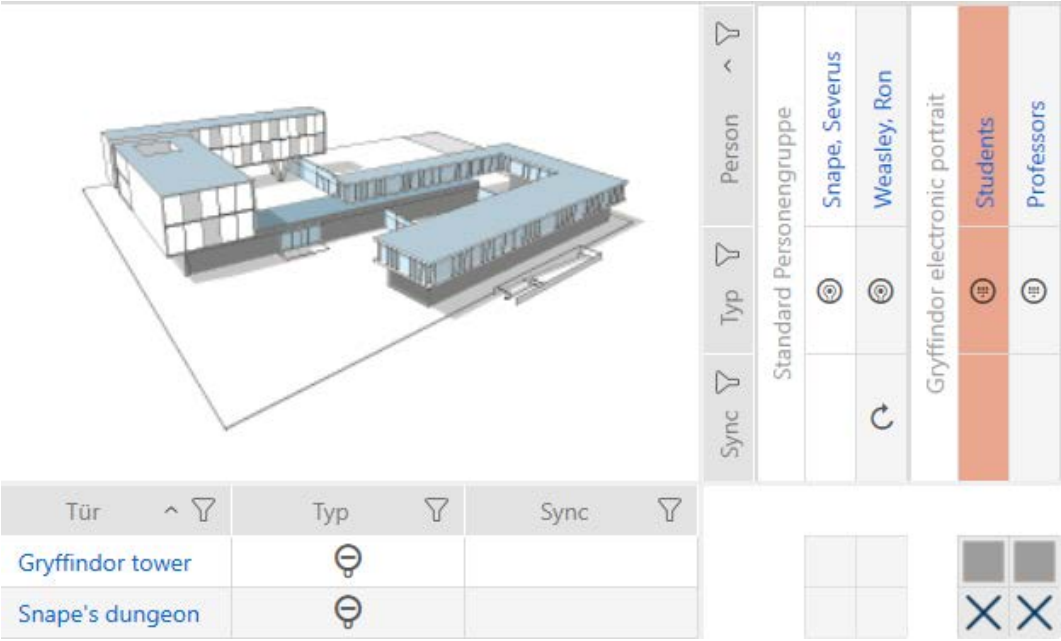
Identmedien, die außer Betrieb genommen wurden, aber nicht gelöscht wurden, können Sie in der Matrix erkennen:



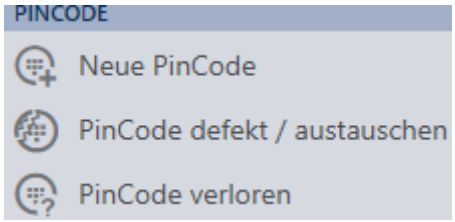
15.9.4.2 PinCode-Tastatur außer Betrieb nehmen und in Projekt lassen

✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

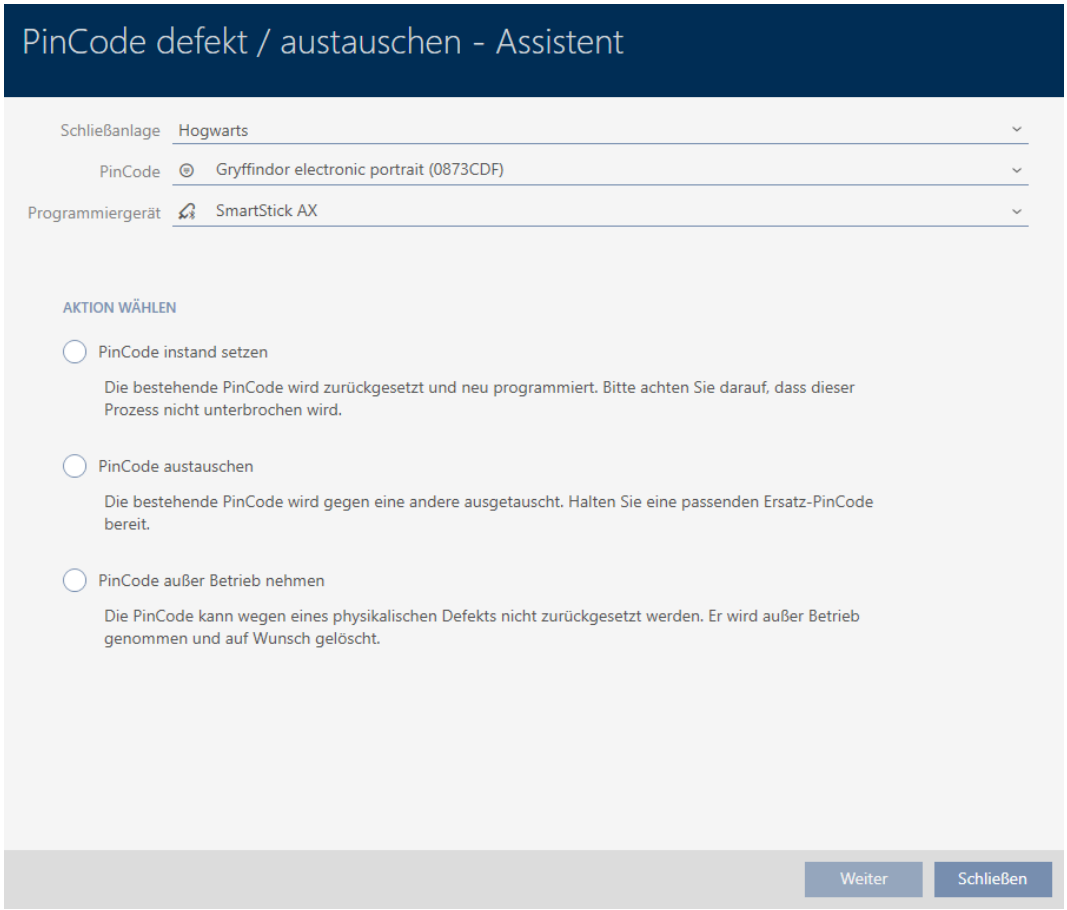
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie eine PIN der defekten PinCode-Tastatur.



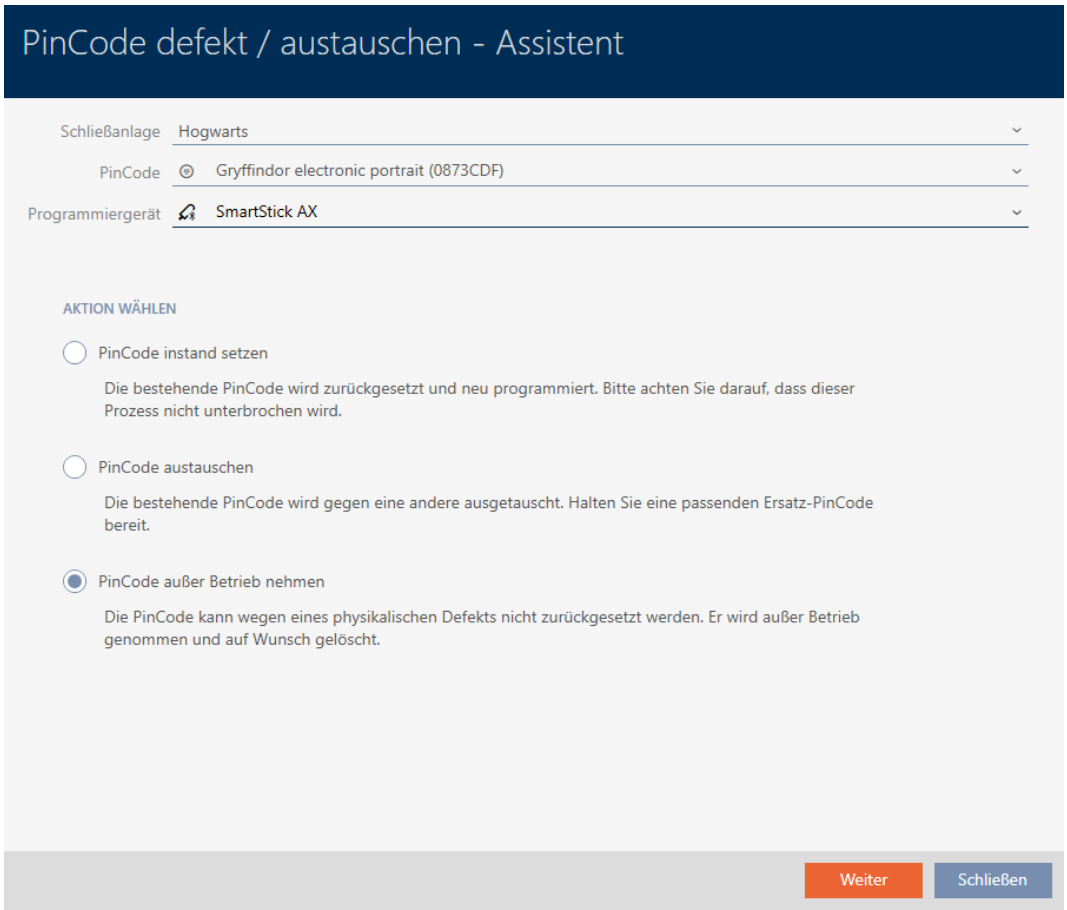
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche PinCode defekt / austauschen.



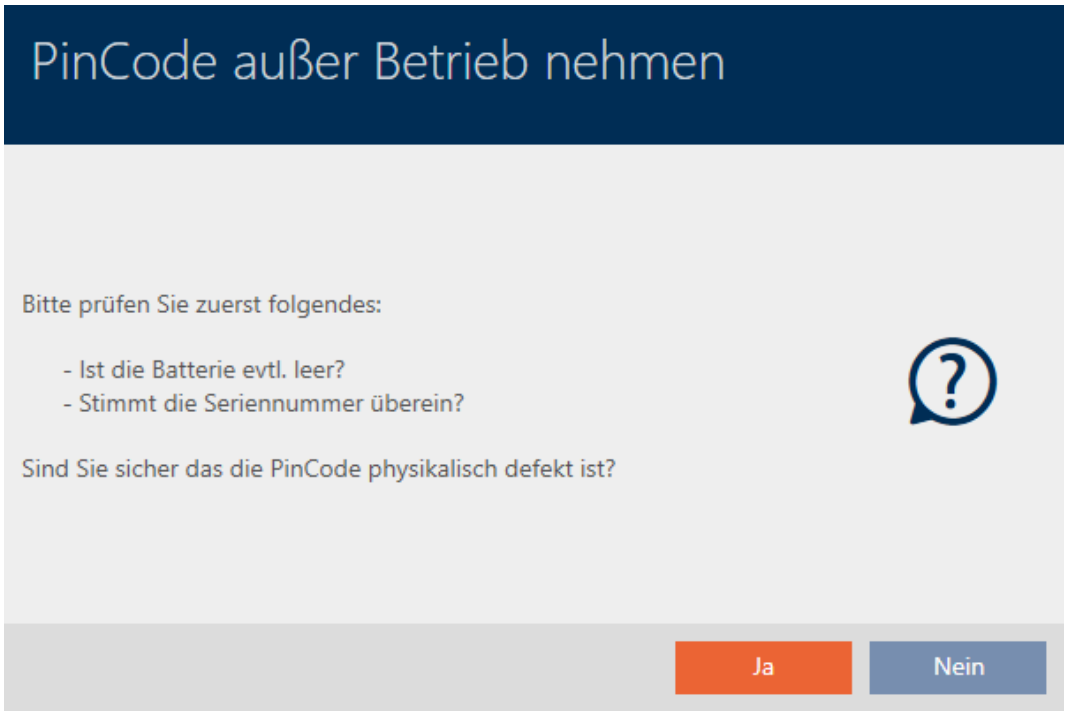
↳ Assistent zum Behandeln einer defekten PinCode-Tastatur öffnet sich.



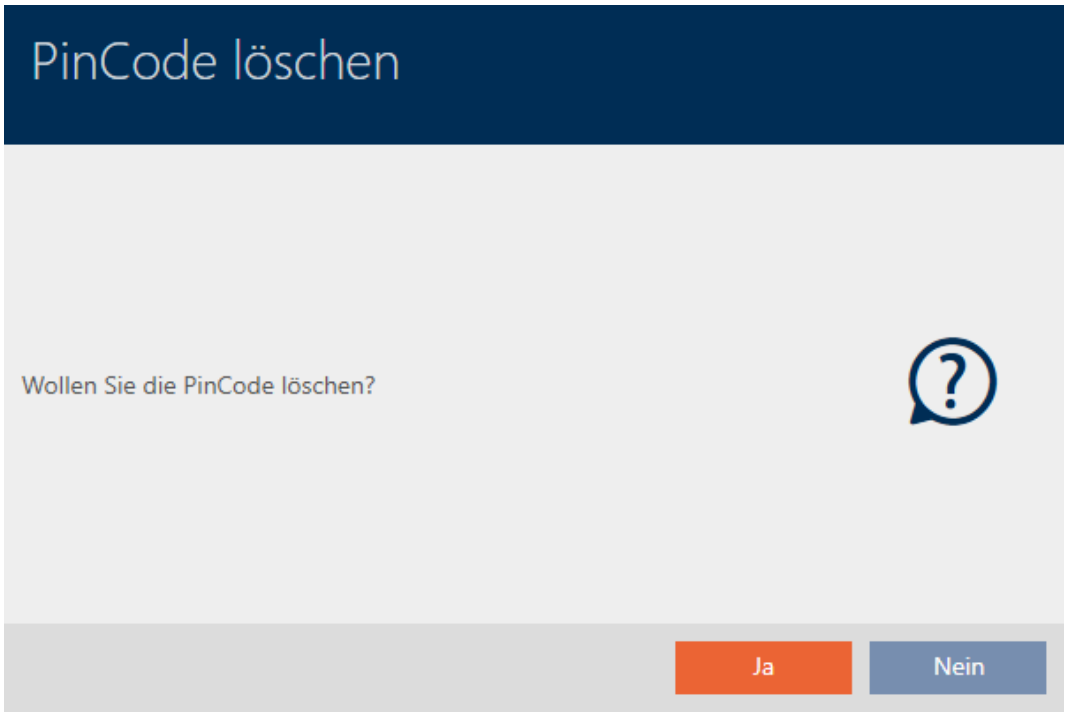
4. Wählen Sie die Option PinCode außer Betrieb nehmen.



5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zur Außerbetriebnahme öffnet sich.

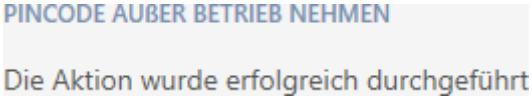


6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zur Außerbetriebnahme schließt sich.
   ↳ Rückfrage zum Löschen der PinCode-Tastatur öffnet sich.

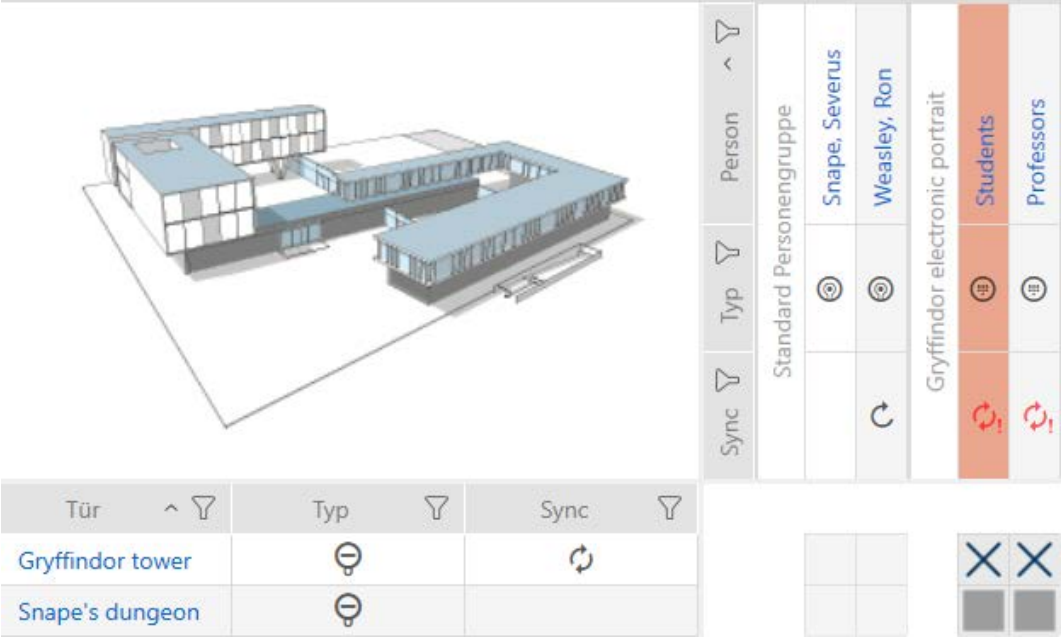


7. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Löschen der PinCode-Tastatur schließt sich.

↳ PinCode-Tastatur ist außer Betrieb genommen.



PinCode-Tastaturen, die außer Betrieb genommen, aber nicht gelöscht wurden, können Sie in der Matrix erkennen:

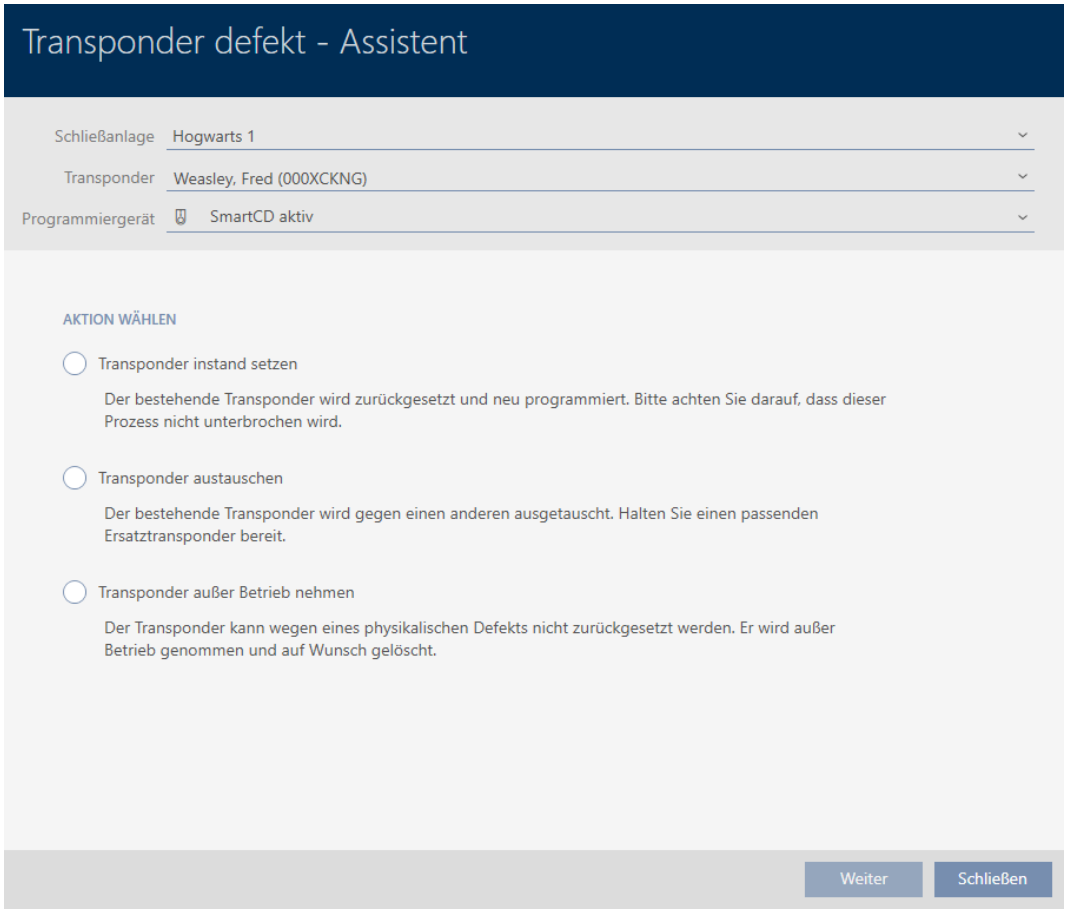


15.9.5 Außer Betrieb nehmen und aus Projekt löschen

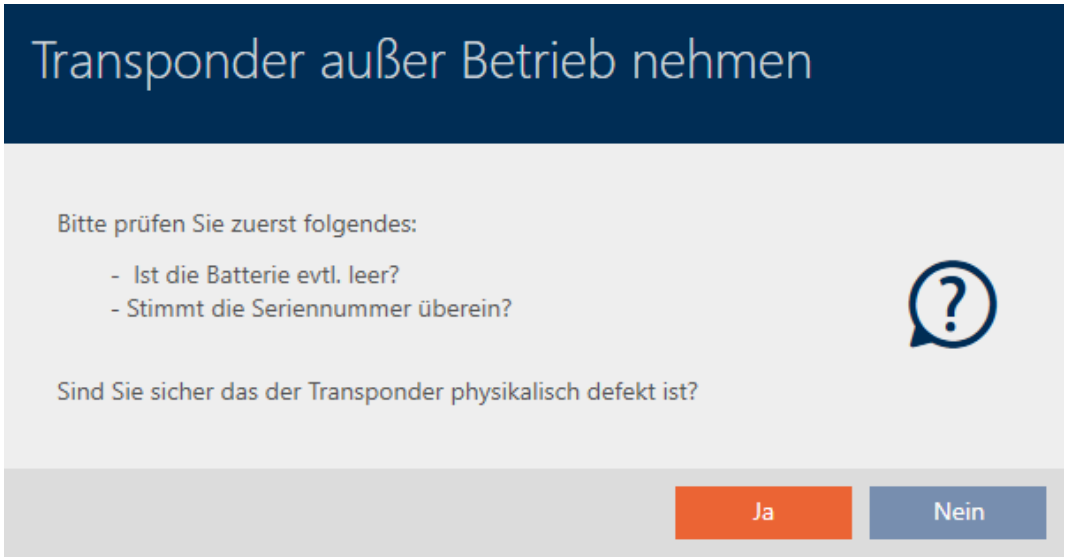
15.9.5.1 Transponder/Karte außer Betrieb nehmen und aus Projekt löschen

✓ Identmedienliste oder Matrix geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das defekte Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder defekt / austauschen.
   ↳ Assistent zum Behandeln eines defekten Identmediums öffnet sich.



4. Wählen Sie die Option ◉ Transponder außer Betrieb nehmen.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zur Außerbetriebnahme öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zur Außerbetriebnahme schließt sich.
   ↳ Rückfrage zum Löschen des Identmediums öffnet sich.

7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Löschen des Identmediums schließt sich.

↳ Identmedium ist ersatzlos gelöscht.

TRANSPONDER AUßER BETRIEB NEHMEN

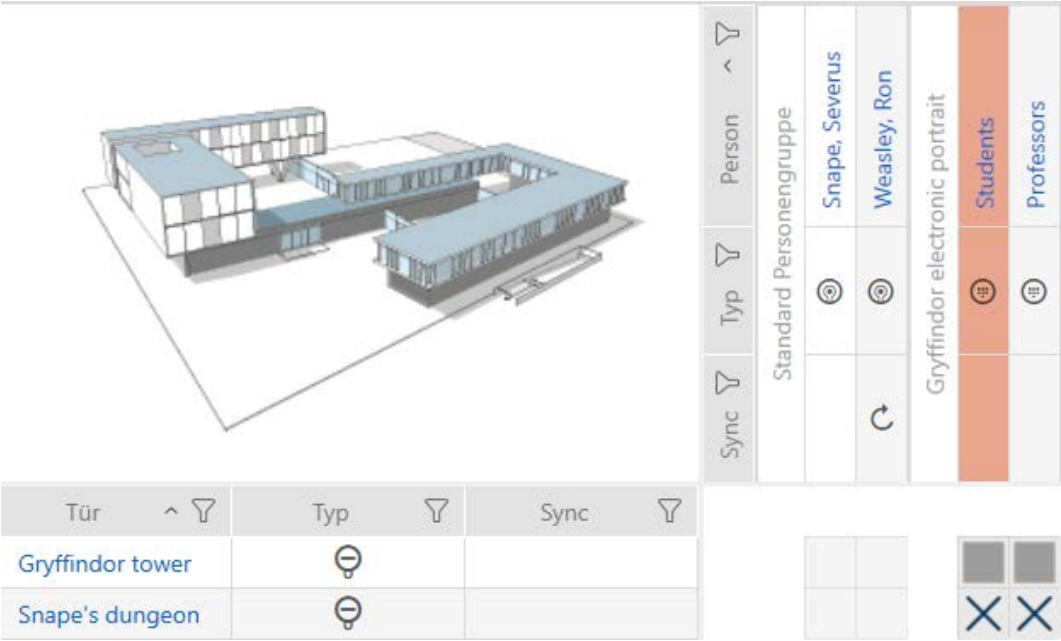
Die Aktion wurde erfolgreich durchgeführt

15.9.5.2 PinCode-Tastatur außer Betrieb nehmen und aus Projekt löschen

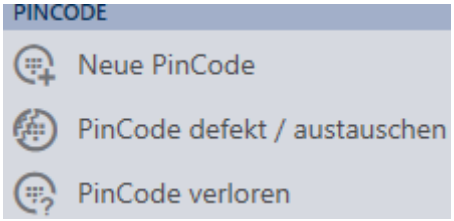
✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

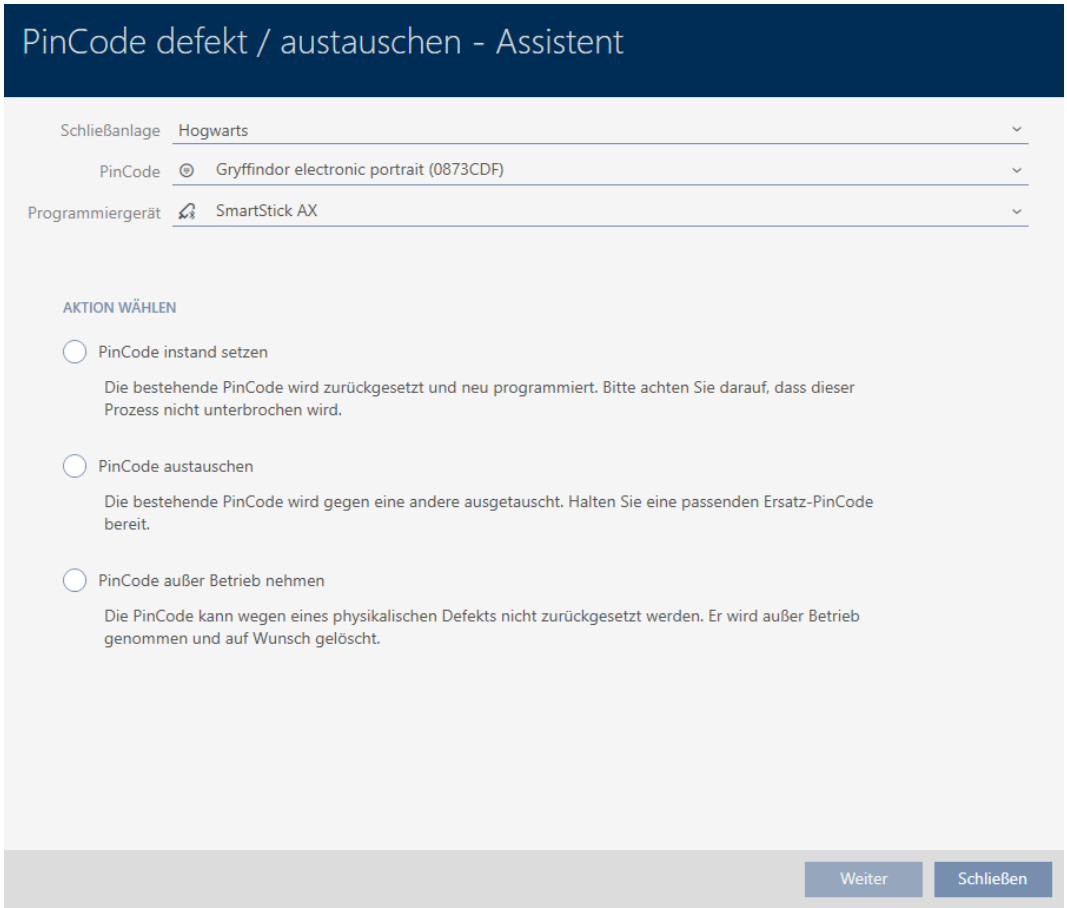
2. Markieren Sie eine PIN der defekten PinCode-Tastatur.



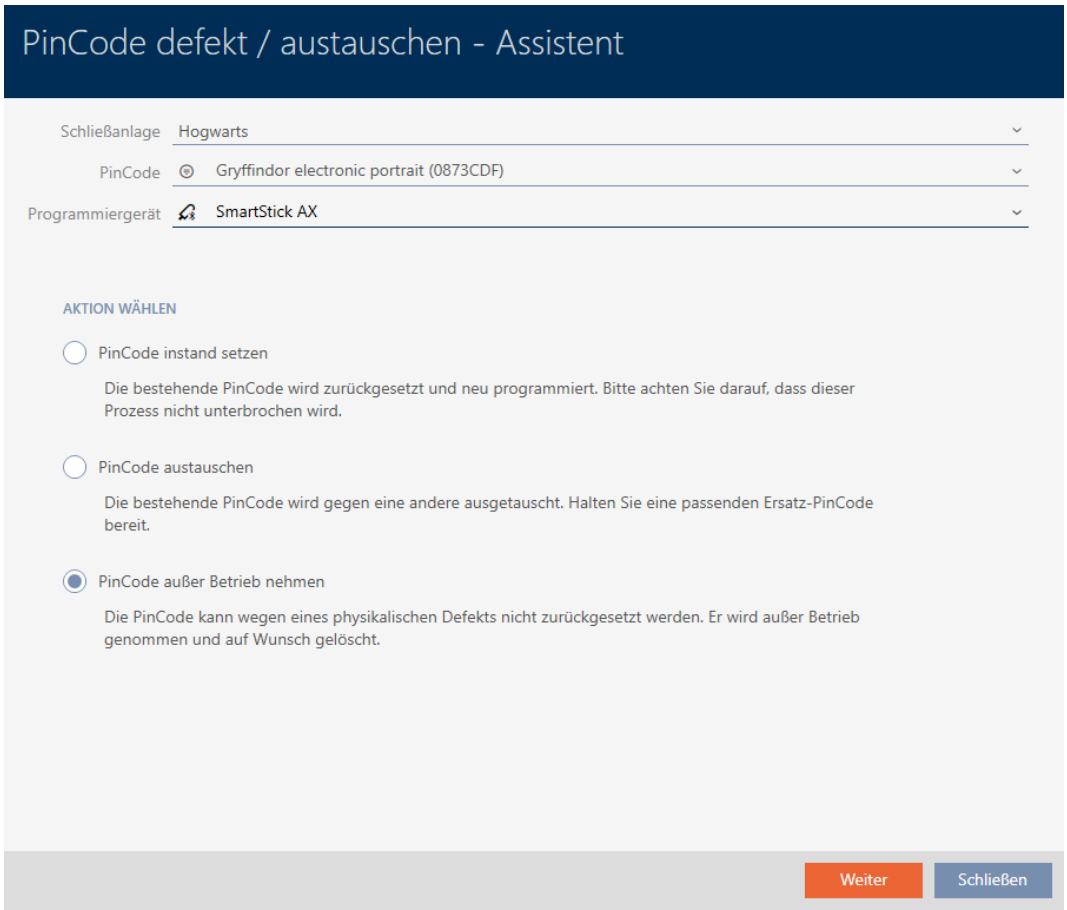
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche PinCode defekt / austauschen.



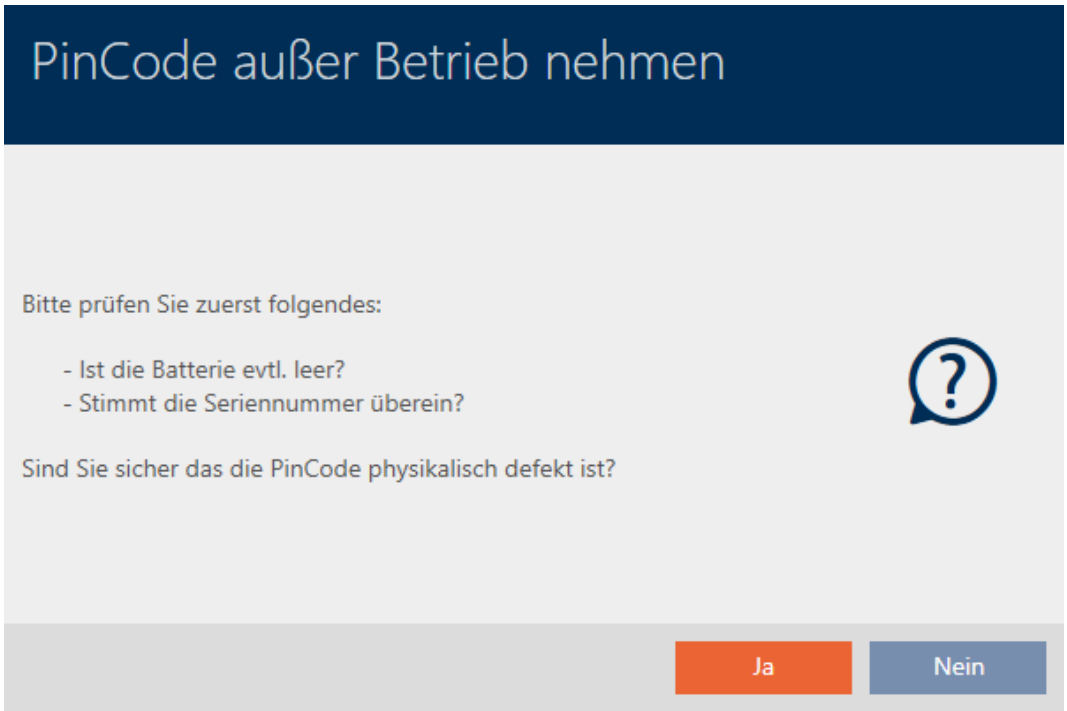
↳ Assistent zum Behandeln einer defekten PinCode-Tastatur öffnet sich.


PinCode defekt / austauschen - Assistent
Schließanlage
Hogwarts
PinCode
Gryffindor electronic portrait (0873CDF)
Programmiergerät
SmartStick AX
AKTION WÄHLEN
PinCode instand setzen
Die bestehende PinCode wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.
PinCode austauschen
Die bestehende PinCode wird gegen eine andere ausgetauscht. Halten Sie eine passenden Ersatz-PinCode bereit.
PinCode außer Betrieb nehmen
Die PinCode kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Er wird außer Betrieb genommen und auf Wunsch gelöscht.
Weiter
Schließen

4. Wählen Sie die Option PinCode außer Betrieb nehmen.

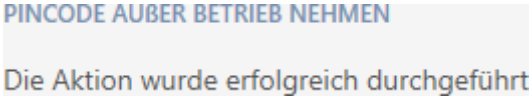


5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zur Außerbetriebnahme öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zur Außerbetriebnahme schließt sich.
   ↳ Rückfrage zum Löschen der PinCode-Tastatur öffnet sich.

7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Löschen der PinCode-Tastatur schließt sich.
8. PinCode-Tastatur ist außer Betrieb genommen und ersatzlos gelöscht.



15.10 Vergessenes Identmedium temporär duplizieren

15.10.1 Vergessenen Transponder oder vergessene Karte temporär duplizieren

Vergessene Identmedien unterscheiden sich von defekten oder gestohlenen/verlorenen Identmedien wie folgt:

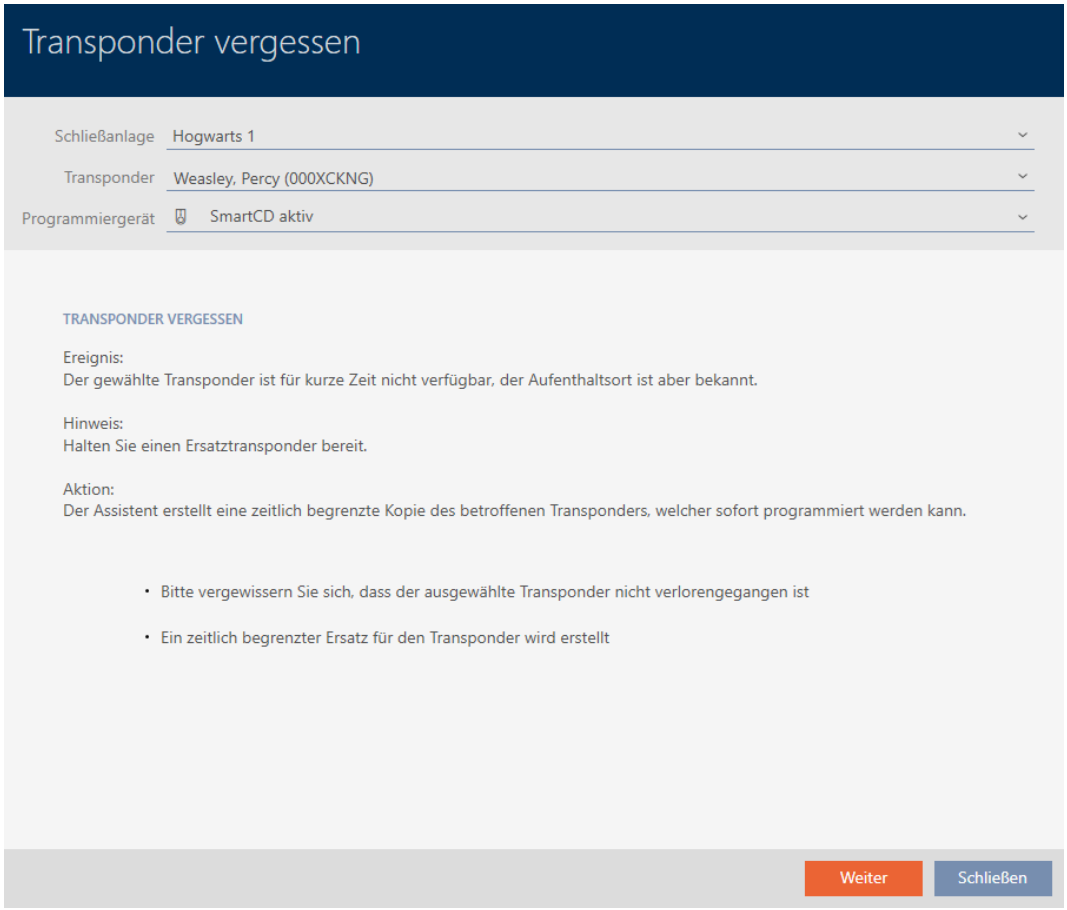
- Im Gegensatz zu defekten Identmedien sind vergessene Identmedien voll funktionsfähig.
- Im Gegensatz zu gestohlenen/verlorenen Identmedien ist das Identmedium an einem bekannten/sicheren Ort.

Mitarbeiter, die ihr Identmedium vergessen haben, können eine Kopie mit Verfallsdatum erhalten. Das Zurücksetzen oder Löschen entfällt in diesem Fall, da auf das vergessene Identmedium kein Unbefugter Zugriff hat.

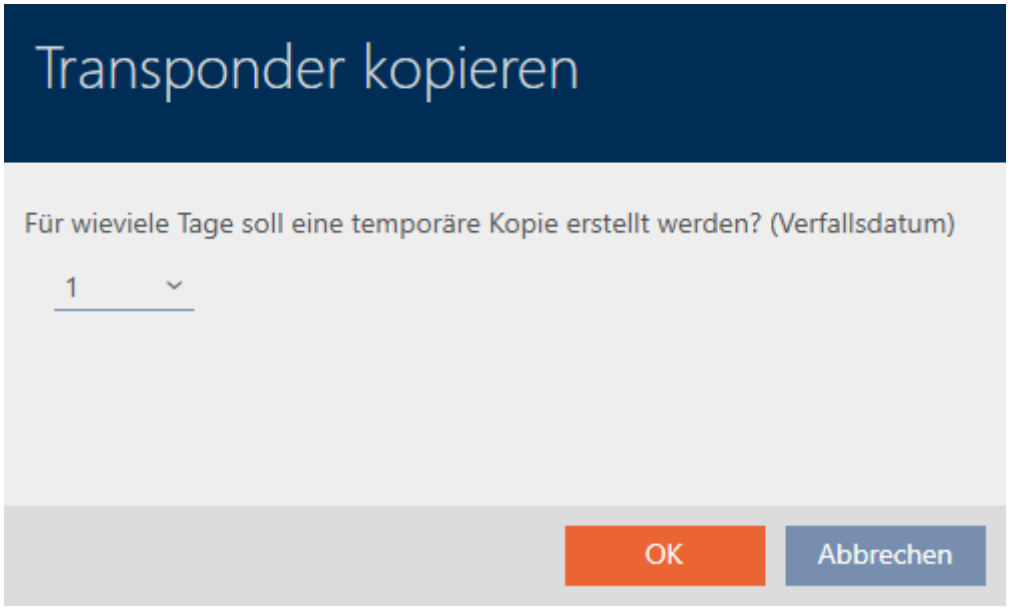
Das Duplikat erhält eine andere TID und ist damit aus Schließungssicht ein eigenständiges Identmedium (Informationen zum Zusammenhang zwischen TID und Identmedium siehe *Identmedien, Schließungen und der Schließplan [▸ 532]*).

- ✓ Identmedienliste oder Matrix geöffnet.
- ✓ Identmedium für temporäres Duplikat zur Programmierung verfügbar.
- ✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das vergessene Identmedium.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder vergessen.
   ↳ Assistent für vergessene Identmedien öffnet sich.

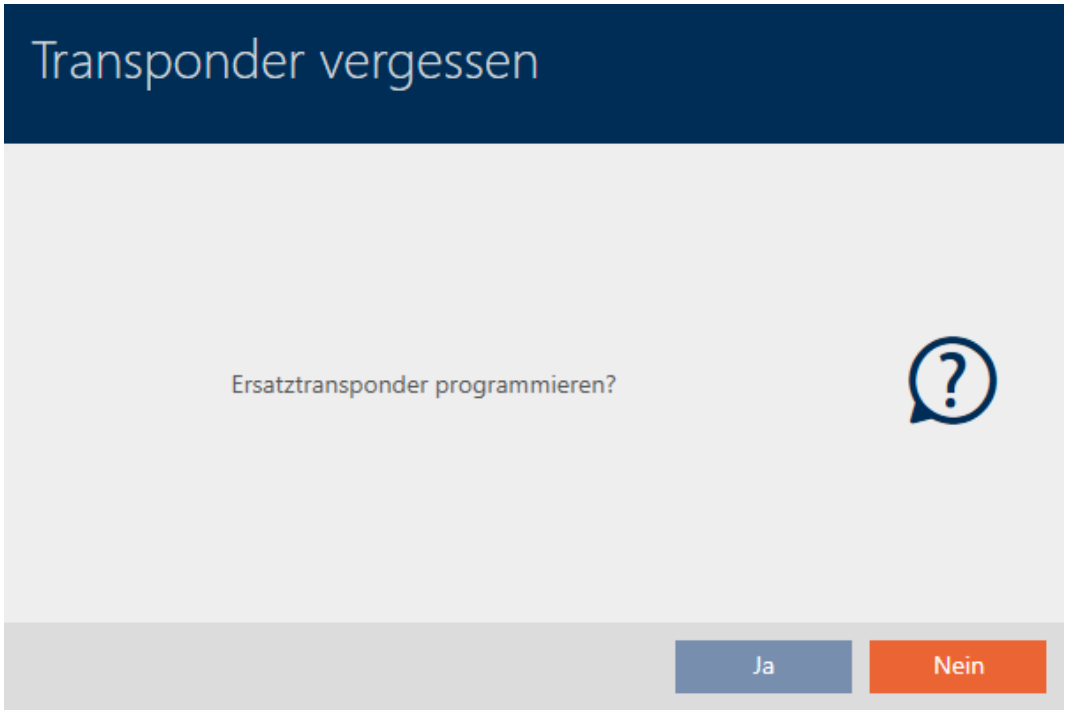


4. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Verfallsdatum des Duplikats öffnet sich.

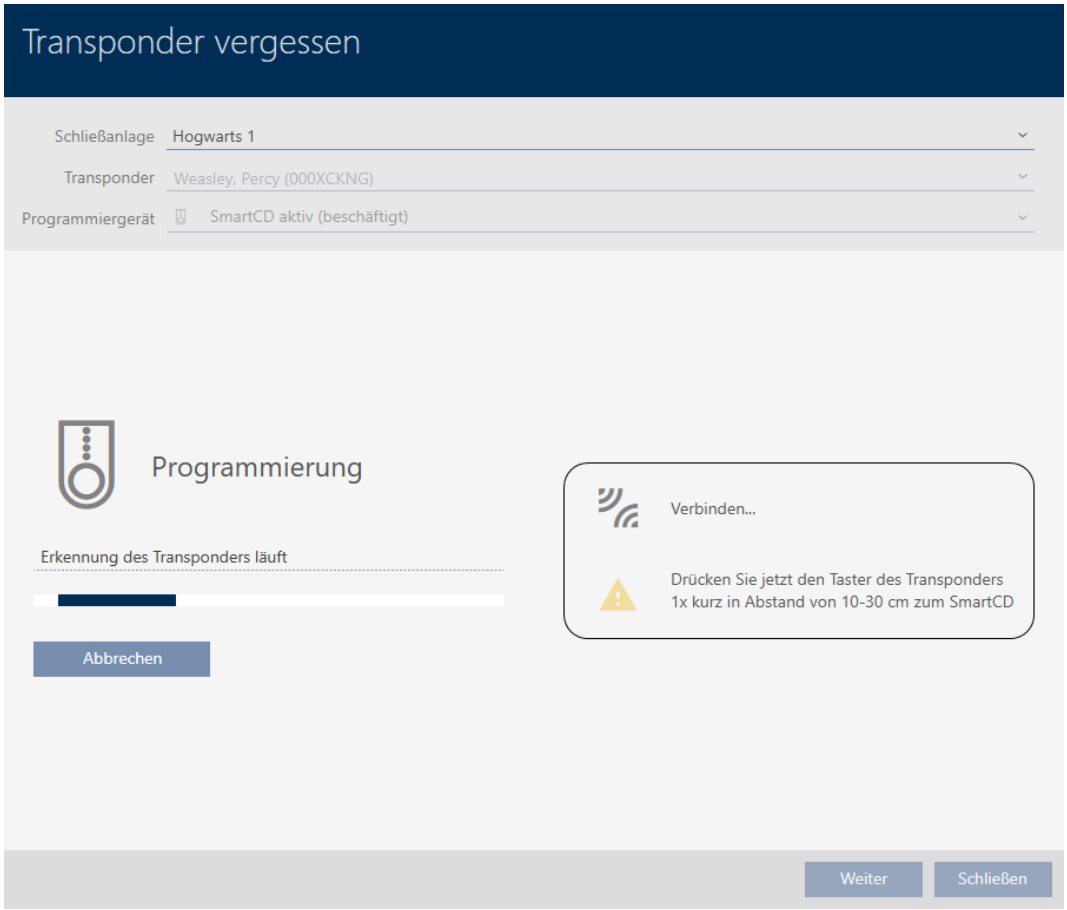


5. Geben Sie die Dauer an, während der das Duplikat aktiv sein soll (max. 7 Tage).

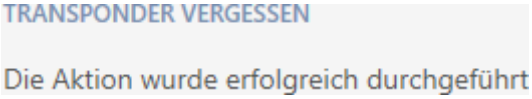
6. Klicken Sie auf die Schaltfläche OK.
   ↳ Rückfrage zum Verfallsdatum des Duplikats schließt sich.
   ↳ Rückfrage zum sofortigen Synchronisieren öffnet sich.



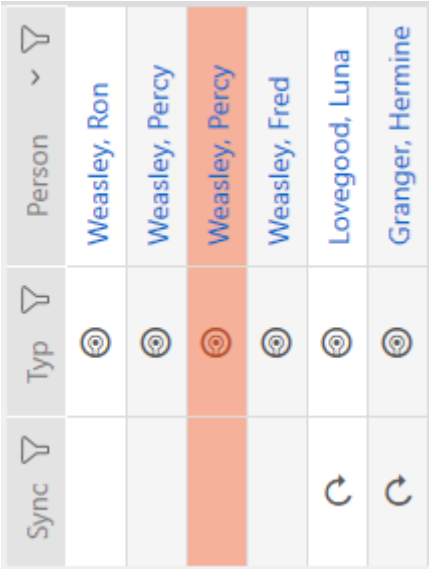
7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum sofortigen Synchronisieren schließt sich.
   ↳ Duplikat wird synchronisiert.



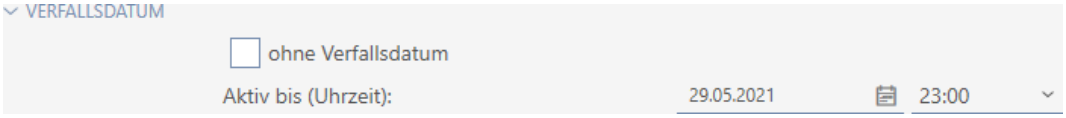
↳ Vergessenes Identmedium ist mit Verfallsdatum dupliziert.



Duplizierte Identmedien werden auch in der Matrix angezeigt:



In den Eigenschaften des Duplikats können Sie das Verfallsdatum einsehen und bei Bedarf verlängern (siehe *Identmedium einmalig an bestimmten Zeitpunkten aktivieren oder deaktivieren (Aktivierungs- und Verfallsdatum) [▸ 126]*):



In diesem Beispiel wurde das Duplikat am 28.05.2021 um 23:00 für einen Tag erstellt. Das Verfallsdatum des Duplikats ist deshalb der 29.05.2021 um 23:00.

Sollte ein Identmedium länger vergessen bleiben (und damit vielleicht nicht mehr nur vergessen, sondern verloren sein), kann es ratsam sein, das Identmedium zu sperren (siehe *Verlorenen/gestohlenen Transponder/Karte dauerhaft sperren und austauschen [▸ 169]*).

15.11 Verlorenes/gestohlenes Identmedium dauerhaft sperren

Ein Identmedium, das nicht mehr auffindbar ist, stellt ein Sicherheitsrisiko für Ihre Schließanlage dar. Im Gegensatz zu einem vergessenen Identmedium ist hier der Aufenthaltsort nicht mehr bekannt und Unbefugte könnten sich mit diesem Identmedium Zutritt verschaffen.

Sperren Sie ein solches Identmedium sofort (siehe *Verlorenen/gestohlenen Transponder/Karte dauerhaft sperren und austauschen [▸ 169]*). Dabei können Sie für den betroffenen Mitarbeiter auch gleich ein Ersatz-Identmedium mit einer anderen TID, aber gleichen Einstellungen und Berechtigungen erstellen. Ihre Schließungen erkennen das Ersatz-Identmedium als neues Identmedium (Informationen zu TIDs siehe *Identmedien, Schließungen und der Schließplan [▸ 532]*).

Verlorene und gestohlene PinCode-Tastaturen

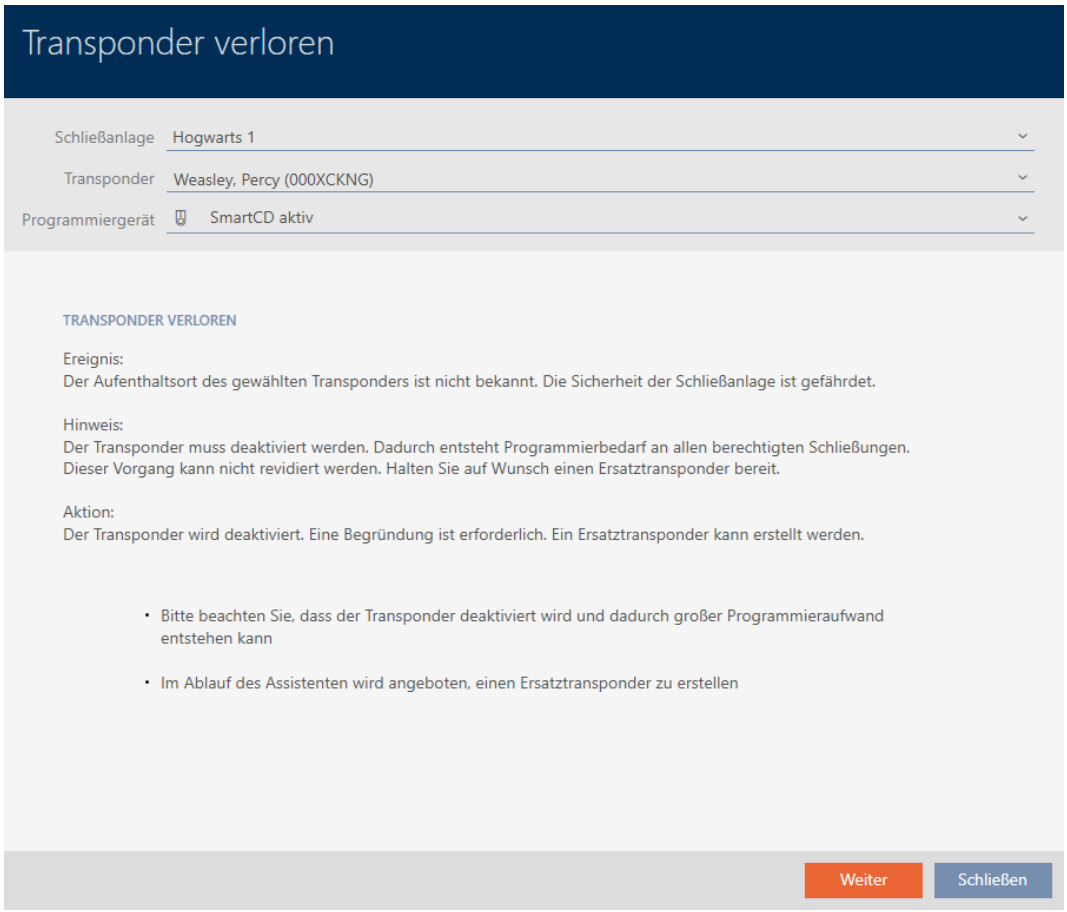
Eine PinCode-Tastatur ist nach der Montage fest an einem Platz und kann nicht mehr verloren gehen. Sie kann allerdings auf dem Weg zu ihrem Platz verloren gehen und danach gewaltsam gestohlen werden. Ein Dieb könnte so zum Beispiel in einem ungesicherten Bereich verschiedene PINs ausprobieren, um eine gültige PIN zu finden.

Da Sie nicht wissen können, welche PIN der Dieb durch Ausprobieren herausgefunden hat, müssen Sie immer die ganze PinCode-Tastatur sperren (siehe *Verlorene/gestohlene PinCode-Tastatur dauerhaft sperren [▸ 174]*). Falls nur eine PIN bekannt wurde und deshalb unsicher ist, können Sie diese PIN ändern (siehe *PIN ändern (PinCode AX) [▸ 236]*).

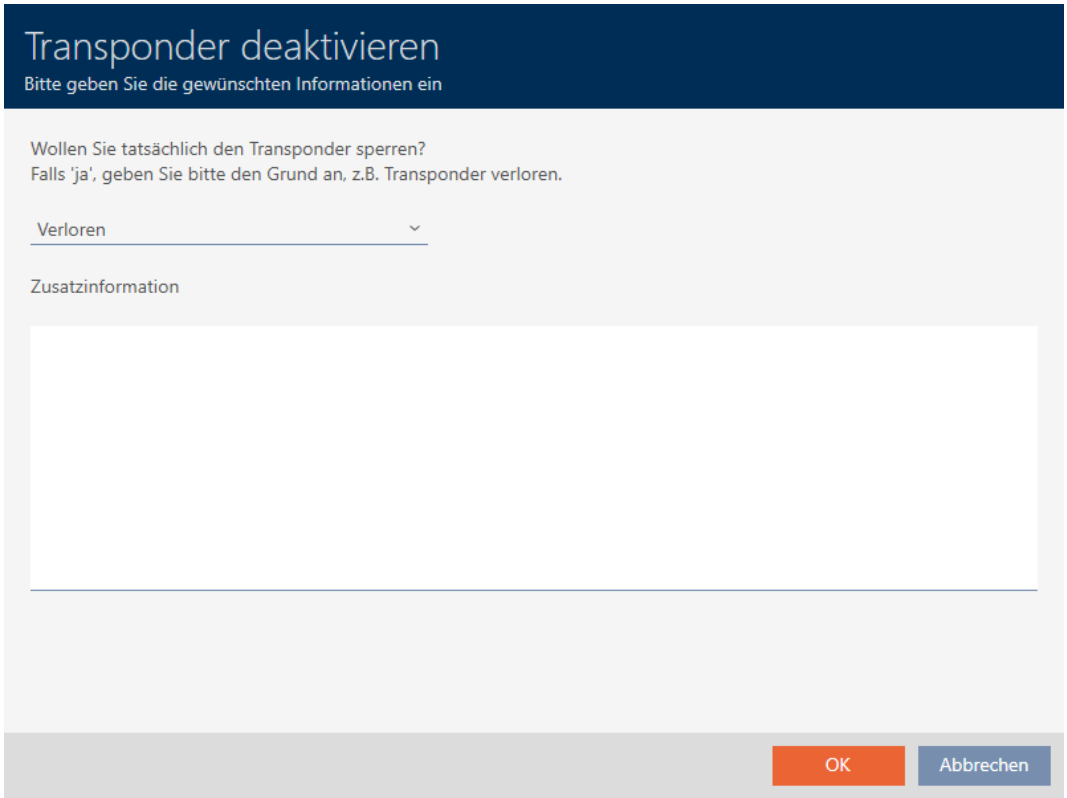
15.11.1 Verlorenen/gestohlenen Transponder/Karte dauerhaft sperren und austauschen

- ✓ Identmedienliste oder Matrix geöffnet.
- ✓ Austausch-Identmedium vorliegend.
- ✓ Geeignetes Programmiergerät angeschlossen.

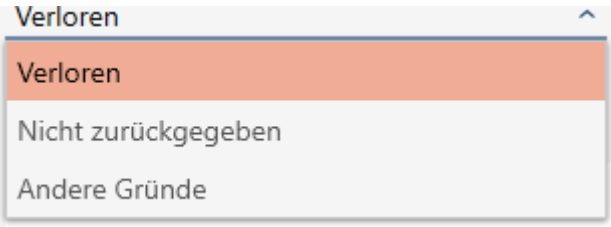
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie das Identmedium, das verloren/gestohlen wurde.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Transponder verloren.
   ↳ Assistent zum Behandeln eines verlorenen Identmediums öffnet sich.



4. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Begründungsfenster öffnet sich.



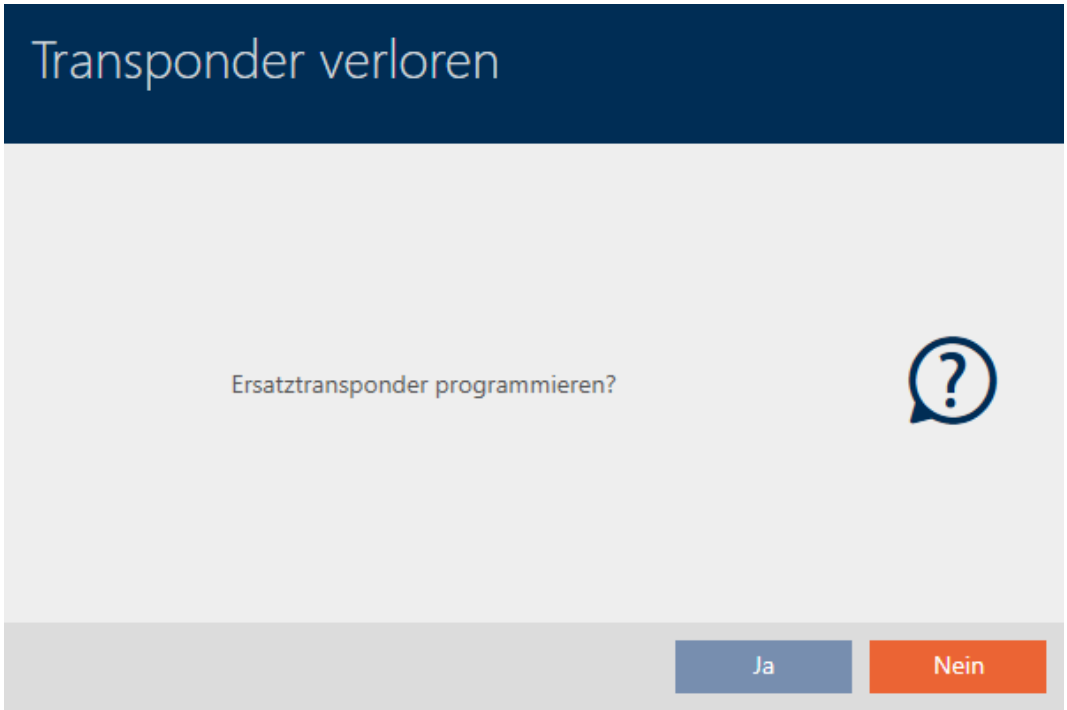
5. Geben Sie im Dropdown-Menü den Grund ein.



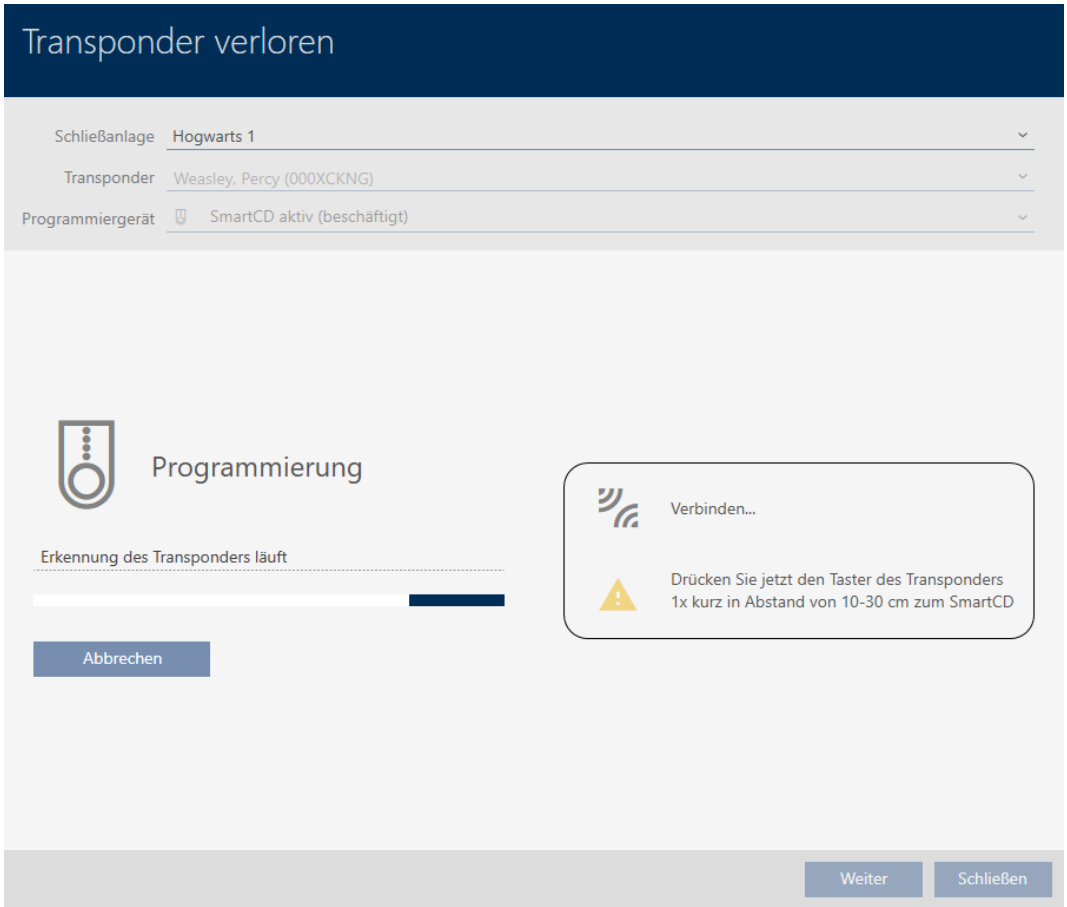
6. Klicken Sie auf die Schaltfläche OK.
   ↳ Rückfrage nach Ersatz-Identmedium öffnet sich.

7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage nach Ersatz-Identmedium schließt sich.
   ↳ Ersatz-Identmedium ist bereits im Hintergrund in der Matrix zu sehen.

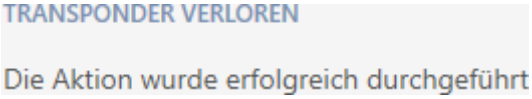
   ↳ Rückfrage nach Synchronisierung des Ersatz-Identmediums öffnet sich.



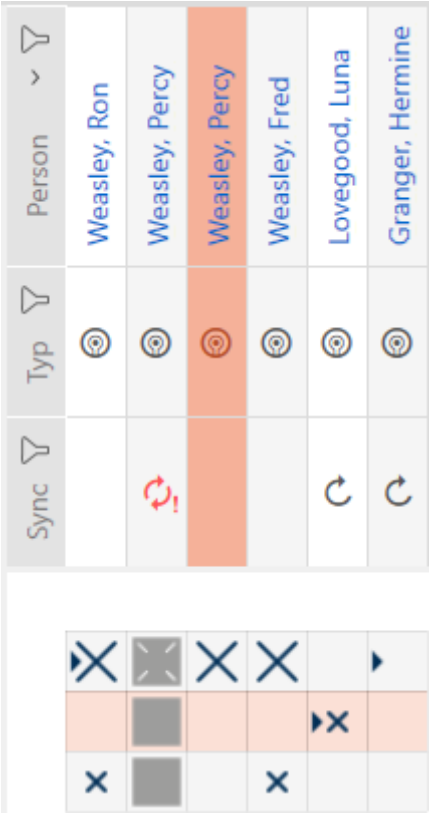
8. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage nach Synchronisierung des Ersatz-Identmediums schließt sich.
   ↳ Synchronisierung beginnt.



↳ Verlorenes Identmedium ist gesperrt.
↳ Ersatz-Identmedium ist synchronisiert.



↳ Ersatz-Identmedium wird in der Matrix neben dem verlorenen Identmedium angezeigt.



ACHTUNG

Änderungen in der Schließanlage erst nach Synchronisierung wirksam

Wenn Sie die Schließanlage mit der AXM Plus bearbeiten, dann sind die Änderungen zunächst nur in Ihrer Datenbank gespeichert.

Ihre realen Komponenten erfahren von diesen Änderungen erst mit einer Synchronisierung.

1. Prüfen Sie die Komponenten in der Matrix regelmäßig auf Synchronisierungsbedarf (siehe *Aufbau der AXM [▸ 46]*).
2. Führen Sie insbesondere bei kritischen Vorfällen (z.B. Identmedium verloren) sofort nach der Reaktion auf den Vorfall eine Synchronisierung durch (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*).

ACHTUNG

Sperr-ID automatisch auf Ersatztransponder geschrieben

Wenn Sie einen Ersatztransponder für einen verlorenen/gestohlenen Transponder erstellen, dann schreibt Ihre AXM Plus die Sperr-ID des gesperrrten Transponders automatisch auf diesen Ersatztransponder.

Mithilfe dieses Ersatztransponders können Sie so auch ohne virtuelles Netzwerk die Sperr-ID zu den Schließungen übertragen. Somit müssen Sie auch mit einer Lite-/Classic-Edition nicht zwingend mit einem Programmiergerät zur Schließung gehen.

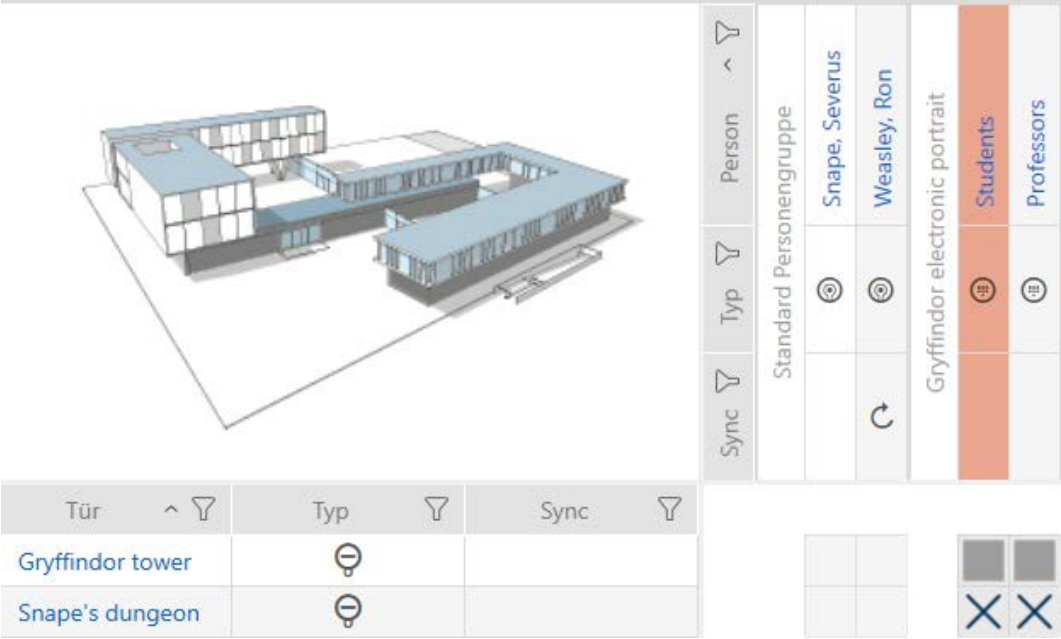
1. Betätigen Sie den Ersatztransponder an den Schließungen.
2. Alternativ: Synchronisieren Sie die Schließungen vor Ort.

15.11.2 Verlorene/gestohlene PinCode-Tastatur dauerhaft sperren

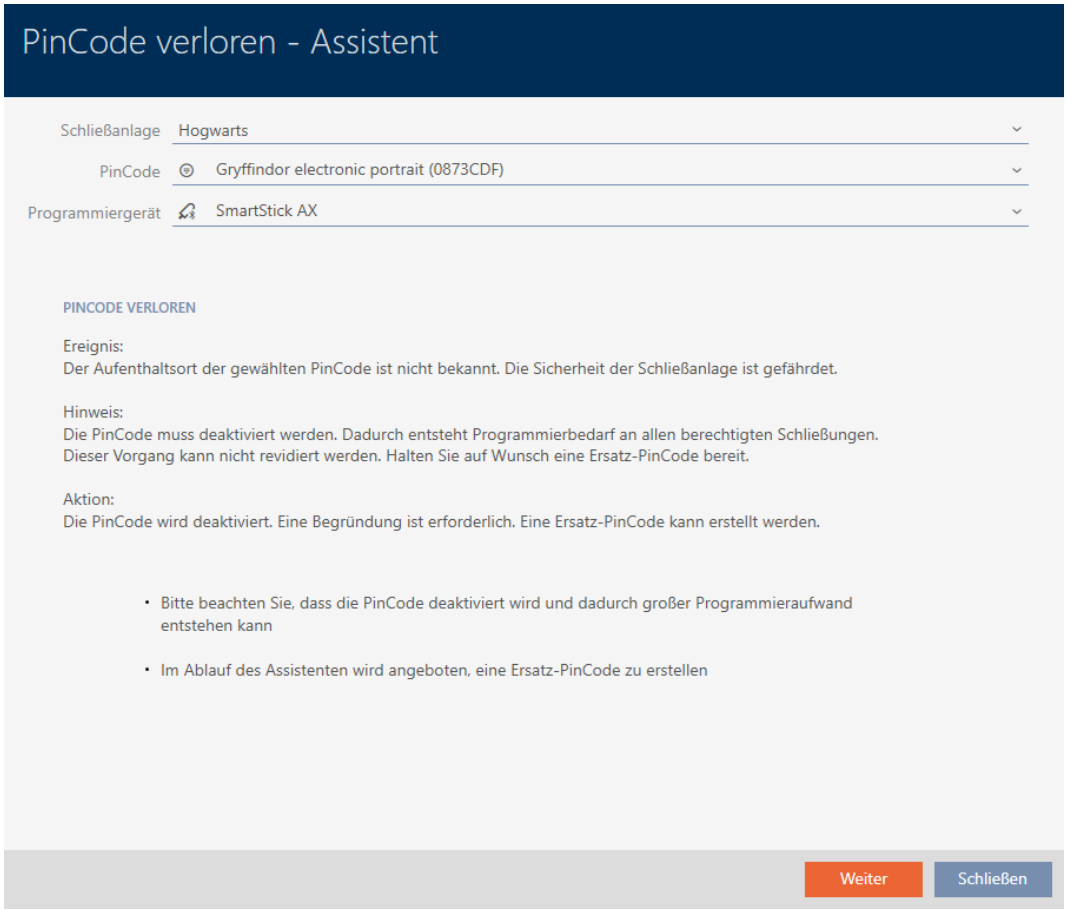
✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

✓ Für Ersatz-PinCode-Tastatur: Geeignetes Programmiergerät angeschlossen.

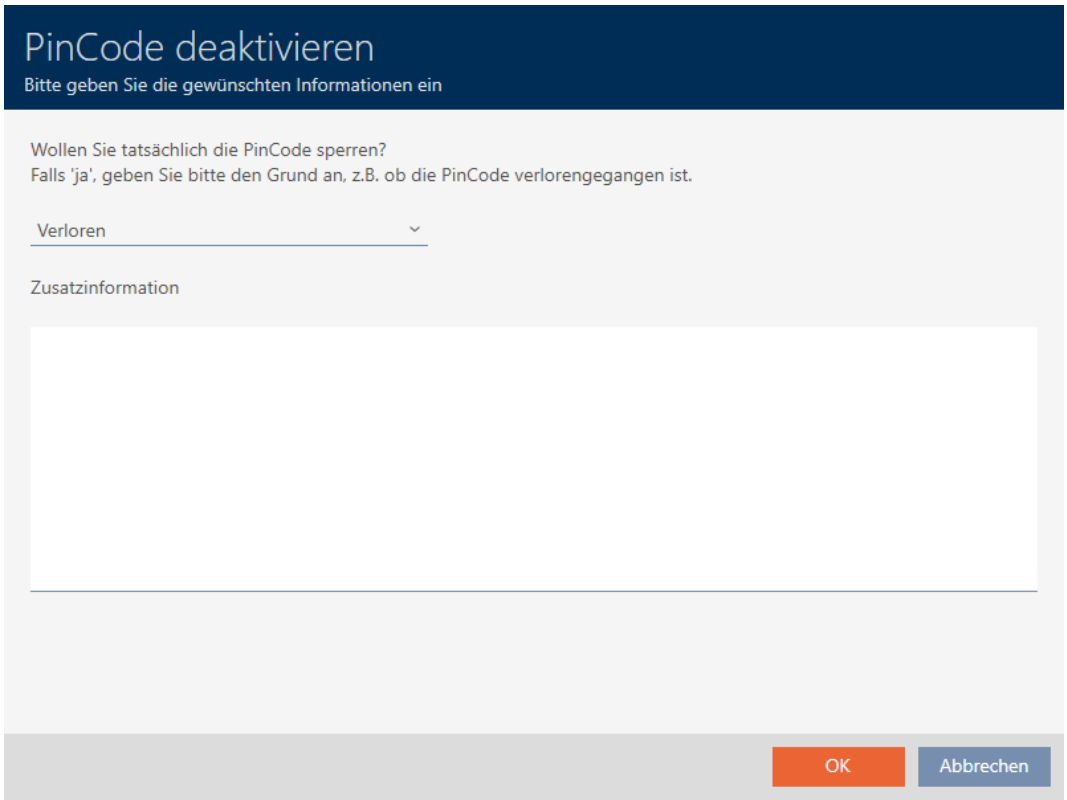
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie eine PIN der verlorenen PinCode-Tastatur.



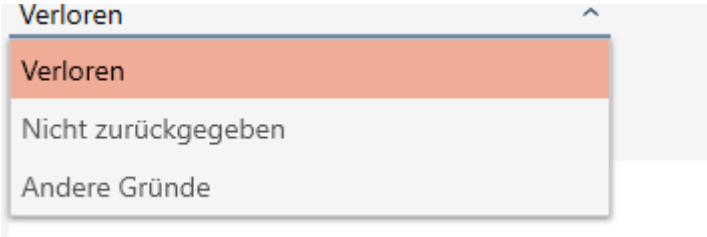
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche PinCode verloren.
   ↳ Assistent zum Behandeln einer verlorenen PinCode-Tastatur öffnet sich.



4. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage-Fenster öffnet sich.



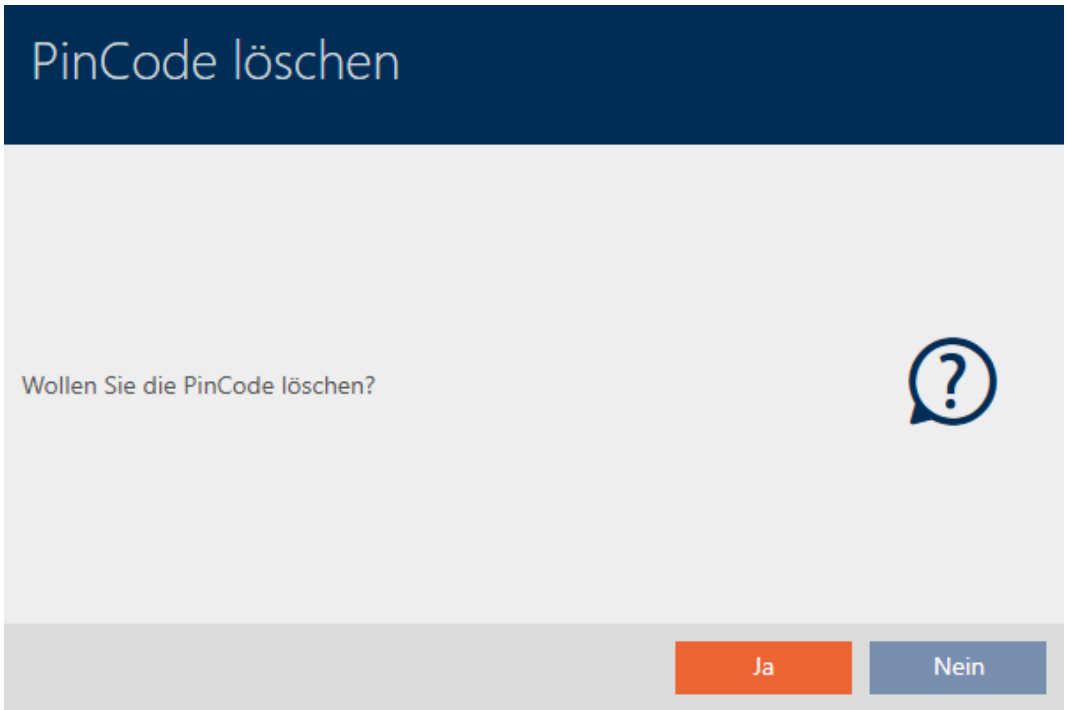
5. Wählen Sie ggfs. im Dropdown-Menü einen anderen Grund als "Verloren" aus.



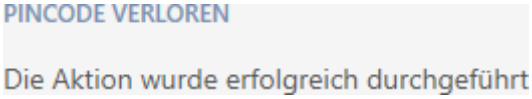
6. Geben Sie im Feld *Zusatzinformation* weitere Informationen an.
7. Klicken Sie auf die Schaltfläche OK.
   ↳ Rückfrage-Fenster schließt sich.
   ↳ AXM Plus bietet an, eine Ersatz-PinCode-Tastatur zu erstellen.

8. Wenn Sie einen Ersatz benötigen, dann klicken Sie auf die Schaltfläche Ja, ansonsten auf die Schaltfläche Nein.
   (Beispiel: Ja)
   ↳ AXM Plus erstellt im Hintergrund eine Ersatz-PinCode-Tastatur.
   ↳ AXM Plus bietet an, die Ersatz-PinCode-Tastatur auch gleich zu synchronisieren.

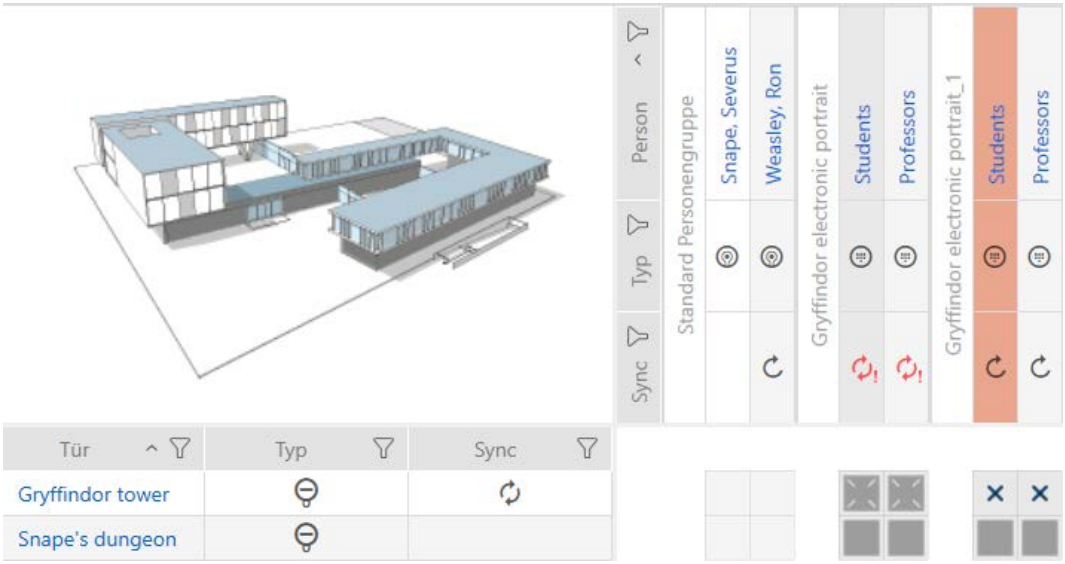
9. Klicken Sie auf die Schaltfläche Ja.
   ↳ Synchronisierung der Ersatz-PinCode-Tastatur startet.
   ↳ AXM Plus bietet an, die verlorene PinCode-Tastatur zu löschen.



10. Klicken Sie auf die Schaltfläche Nein.
   ↳ PinCode-Tastatur wurde gesperrt und eine Ersatz-PinCode-Tastatur synchronisiert.



Beide PinCode-Tastaturen sind in der Matrix sichtbar.



Für den Ersatz benötigen Sie eine andere PinCode-Tastatur. Beim Versuch, die gleiche PinCode-Tastatur zu verwenden, zeigt Ihre AXM Plus eine Fehlermeldung:

Alternative dazu: Instandsetzung der PinCode-Tastatur, siehe *PinCode-Tastatur instandsetzen (Neu synchronisieren) [▸ 135]*.

15.12 Zurückgegebenes Identmedium vermerken und zurücksetzen (wieder ins Inventar)

Ein Identmedium wurde an die Schließanlagenverwaltung übergeben und soll aus dem Verkehr gezogen werden.

Im Gegensatz zum Zurücksetzen und Löschen wird das physische Identmedium zwar zurückgesetzt, bleibt aber weiterhin in Ihrer Schließanlage. Stattdessen trägt die AXM Plus einen Vermerk über die Rückgabe in die Historie des Identmediums ein.

Natürlich können Sie das Identmedium nach dem Zurücksetzen auch aus der Schließanlage löschen. Damit ginge allerdings die Aktionsliste ("Historie") verloren.

PINs einer PinCode-Tastatur nicht zurücknehmbar

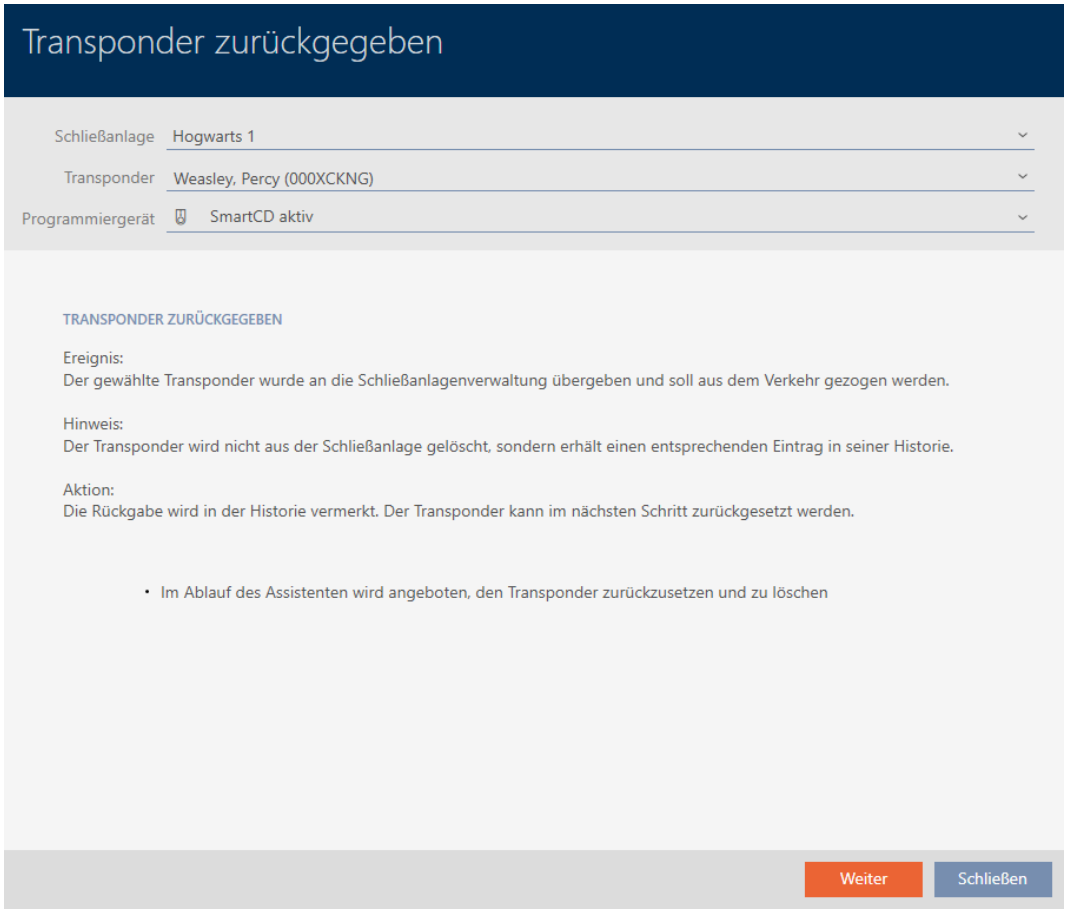
Die PINs einer PinCode-Tastatur sind nicht physisch und können deshalb nicht zurückgenommen werden. Stattdessen haben Sie die Möglichkeit, die PIN zu ändern (siehe *PIN ändern (PinCode AX) [▸ 236]*).

15.12.1 Zurückgegebenen Transponder/Karte vermerken und zurücksetzen (wieder ins Inventar)

Um einen Transponder oder eine Karte zurückzunehmen, ohne die Aktionsliste zu verlieren, gehen Sie wie folgt vor:

✓ Geeignetes Programmiergerät angeschlossen.

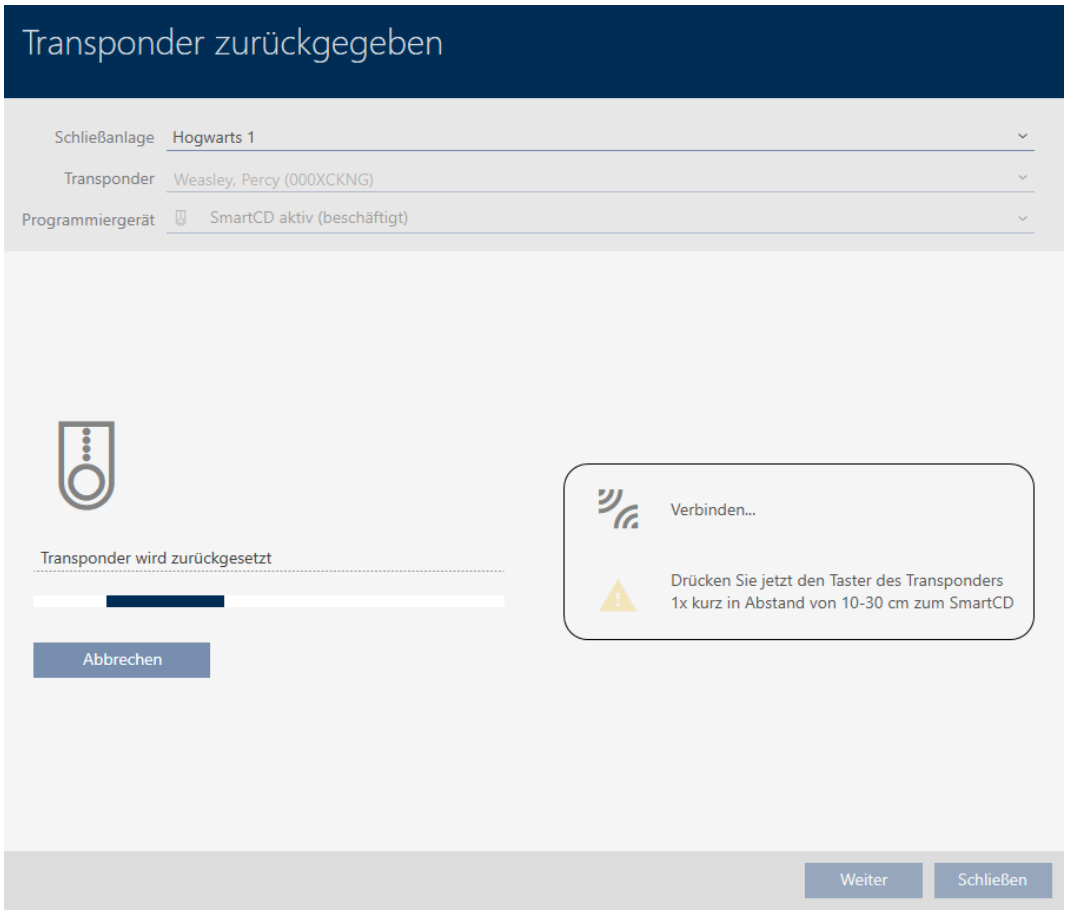
1. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche ↵ Transponder zurückgegeben .
   ↳ Assistent für die Identmedien-Rückgabe öffnet sich.



2. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen des Identmediums öffnet sich.

3. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Zurücksetzen des Identmediums schließt sich.

↳ Identmedium wird zurückgesetzt.



↳ Rückfrage zum Löschen des Identmediums öffnet sich.

4. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Löschen des Identmediums schließt sich.

↳ Identmedium ist zurückgesetzt, aber nicht gelöscht.

TRANSPONDER ZURÜCKGEGEBEN

Die Aktion wurde erfolgreich durchgeführt

Die erfolgreiche Rückgabe wird in der Aktionsliste des Identmediums vermerkt (siehe auch *Transponder-/Karten-Rückgabe planen und protokollieren [▸ 191]*).

Datum	Typ	Benutzer	Beschreibung
29.05.2021 00:08:58	Zurückgesetzt	Admin	
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin	
20.05.2021 20:40:08	Letzte Programmierung	Admin	
20.05.2021 20:39:14	Letzte Programmierung	Admin	
05.05.2021 14:08:04	Erstellt	Admin	

15.13 Identmediums-Verwaltungsaufgaben planen und nachverfolgen

Die zentrale Anlaufstelle für die Verwaltung Ihres Identmediums ist der Reiter "Transponder - Aktionen". Hier werden folgende Einträge gesammelt angezeigt:

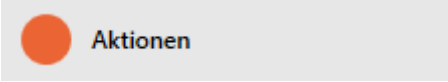
- Erstellt
- Programmierung
- Ausgegeben
- Planmäßiger Batteriewechsel
- Letzter Batteriewechsel
- Geplante Rückgabe
- Erfolgte Rücknahme

Je nach Art des Identmediums sind nicht alle Einträge verfügbar. Da eine PIN beispielsweise nicht wie ein Transponder zurückgenommen werden kann, gibt es die Einträge "Geplante Rückgabe" und "Erfolgte Rücknahme" bei PinCode-Tastaturen nicht.

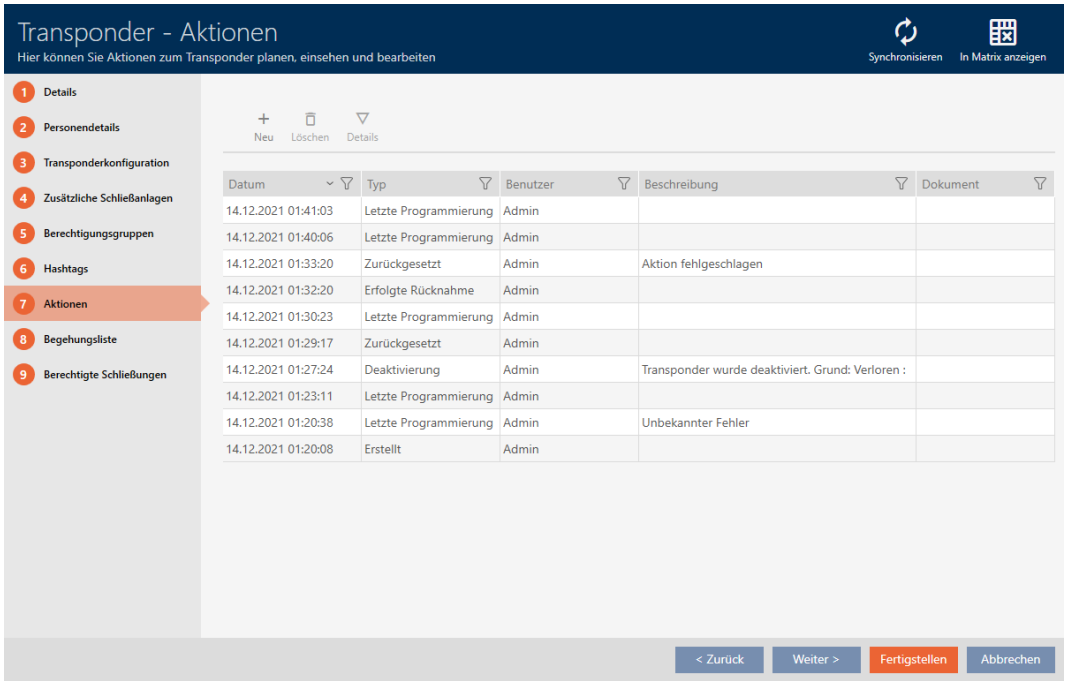
✓ Identmedienliste oder Matrix geöffnet.
✓ Identmedium vorhanden.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

2. Klicken Sie auf das Identmedium, das verwaltet werden soll.
   ↳ Fenster des Identmediums öffnet sich.
3. Klicken Sie auf den Reiter Aktionen.



   ↳ Fenster wechselt zum Reiter "Aktionen".



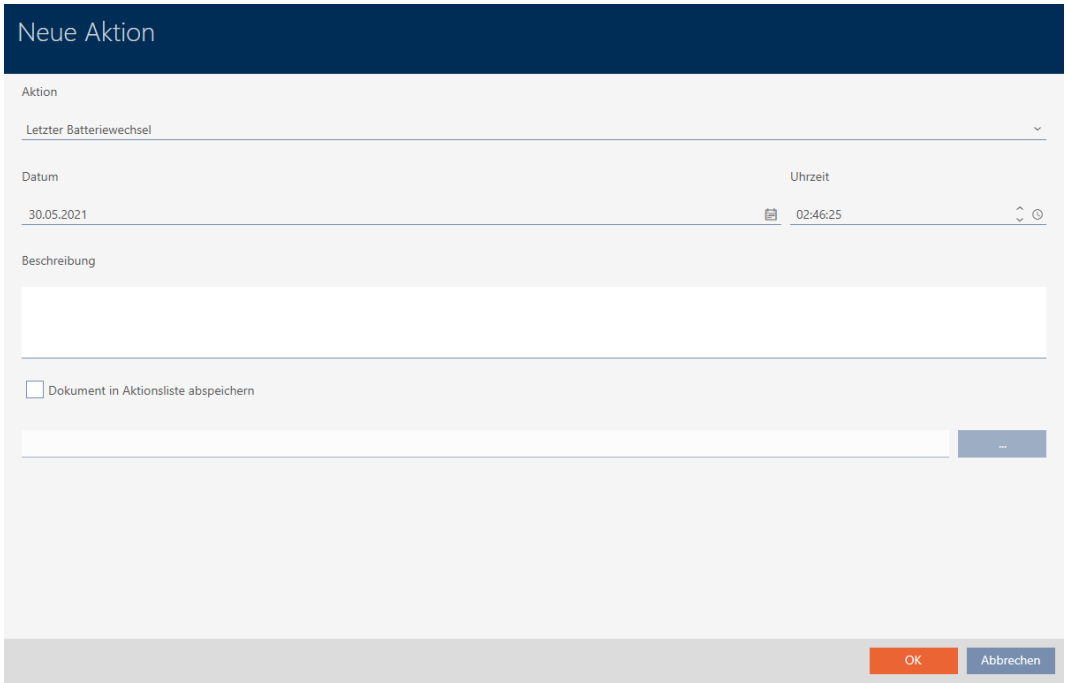
4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

15.13.1 Ausgabedatum notieren

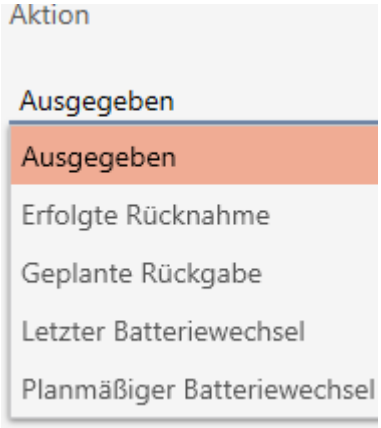
15.13.1.1 Transponder-/Karten-Ausgabedatum notieren

Die AXM Plus kann nicht wissen, wann Sie das Identmedium übergeben haben. Diese Information können Sie deshalb beim jeweiligen Identmedium manuell eintragen.

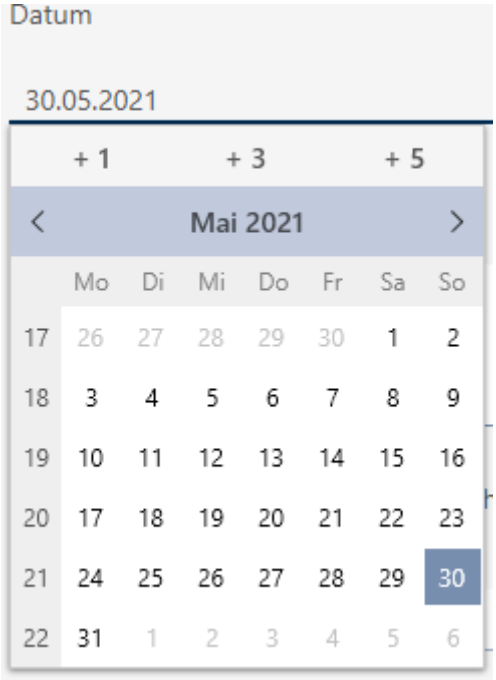
1. Klicken Sie auf die Schaltfläche + Neu.
   ↳ Fenster einer neuen Aktion öffnet sich.



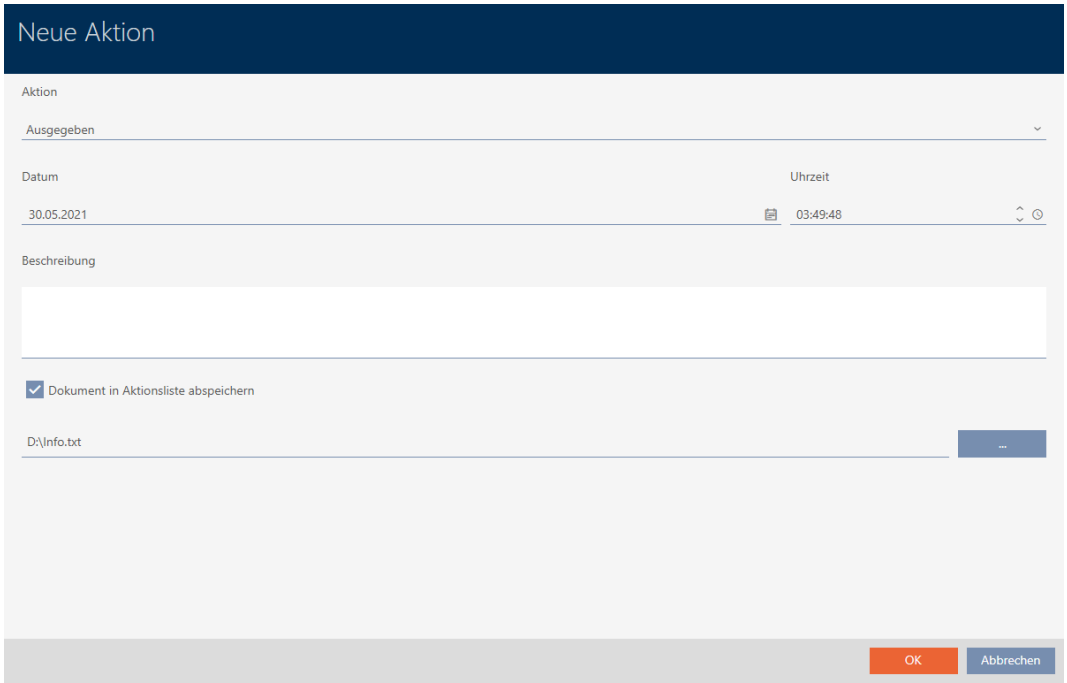
2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Ausgegeben" aus.



3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.
7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

↳ Aktion ist erstellt und wird aufgelistet.

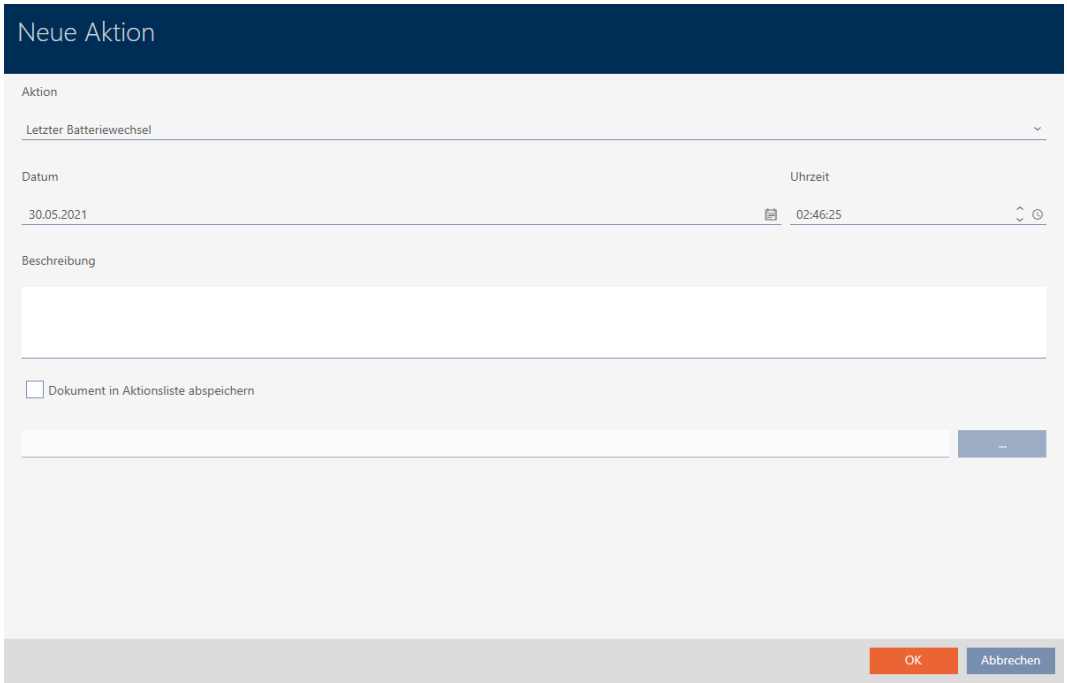
Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 03:49:48	Ausgegeben	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14	Letzte Programmierung	Admin		
05.05.2021 14:08:04	Erstellt	Admin		

Als Vorbereitung auf die Übergabe des Identmediums können Sie einen passenden Bericht mit Unterschriftsfeldern erzeugen (siehe *Bericht zur Identmedien-Ausgabe ausgeben* [▸ 524]).

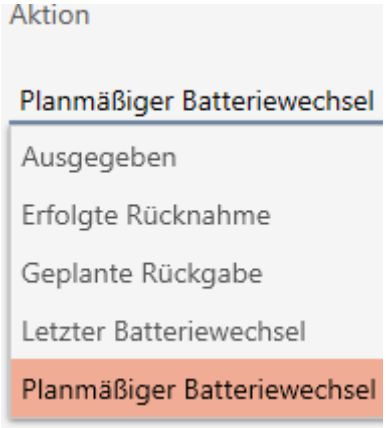
15.13.2 Batteriewechsel planen und protokollieren

15.13.2.1 Transponder-/Karten-Batteriewechsel planen und protokollieren

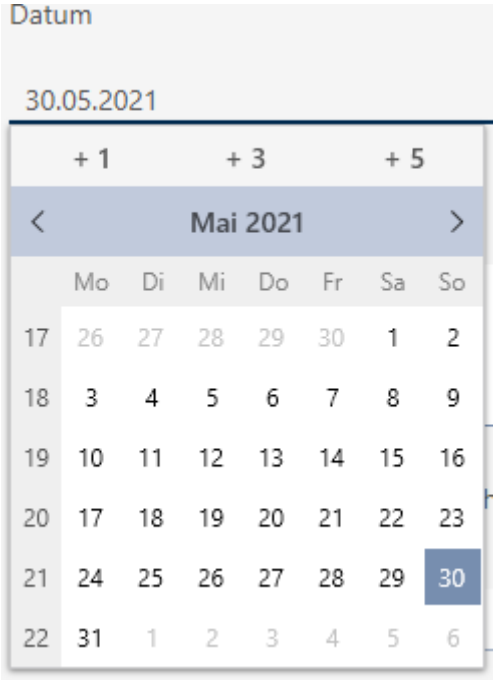
1. Klicken Sie auf die Schaltfläche ✚ Neu.
   ↳ Fenster einer neuen Aktion öffnet sich.



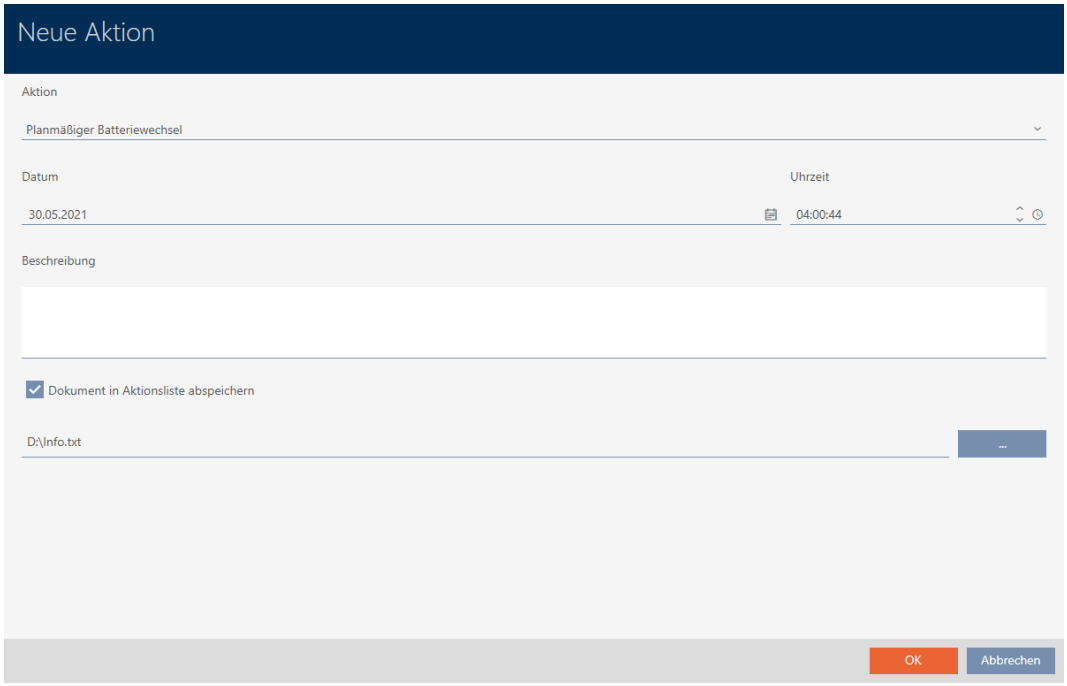
2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Planmäßiger Batteriewechsel" bzw. "Letzter Batteriewechsel" aus.



3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.
7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



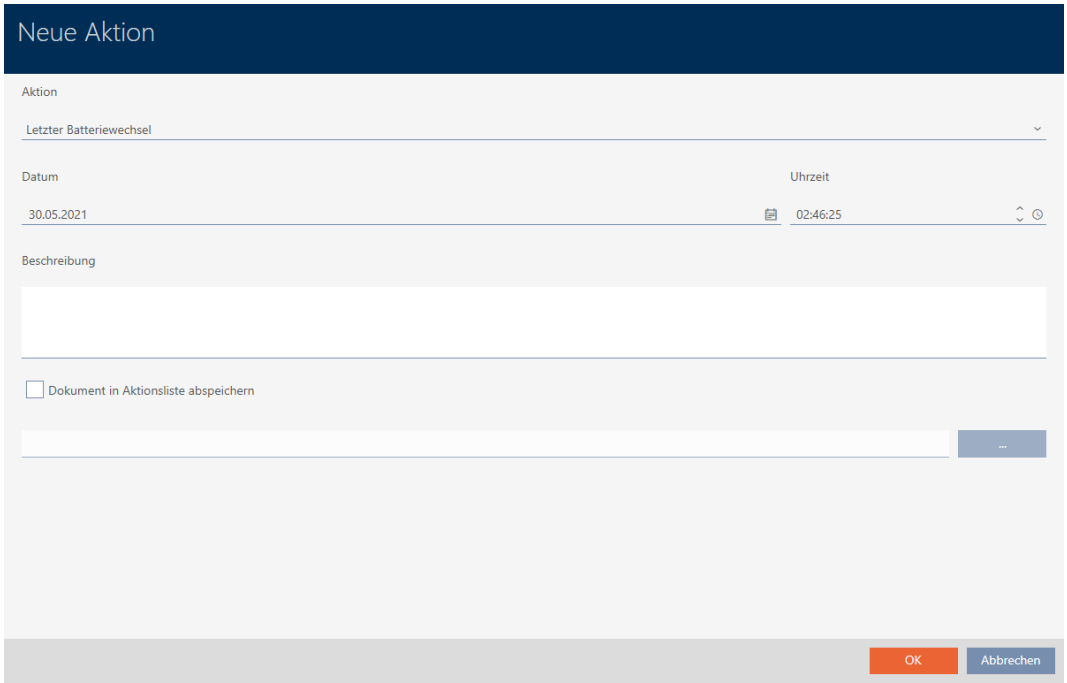
9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

↳ Aktion ist erstellt und wird aufgelistet.

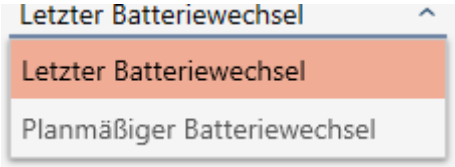
Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 04:00:44	Planmäßiger Batteriewec	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14	Letzte Programmierung	Admin		
05.05.2021 14:08:04	Erstellt	Admin		

15.13.2.2 PinCode-Tastatur-Batteriewechsel planen und protokollieren

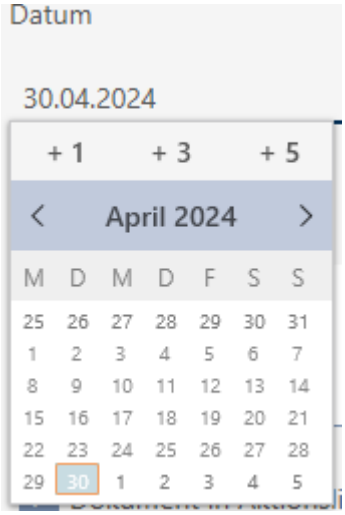
1. Klicken Sie auf die Schaltfläche + Neu.
   ↳ Fenster einer neuen Aktion öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Planmäßiger Batteriewechsel" bzw. "Letzter Batteriewechsel" aus.

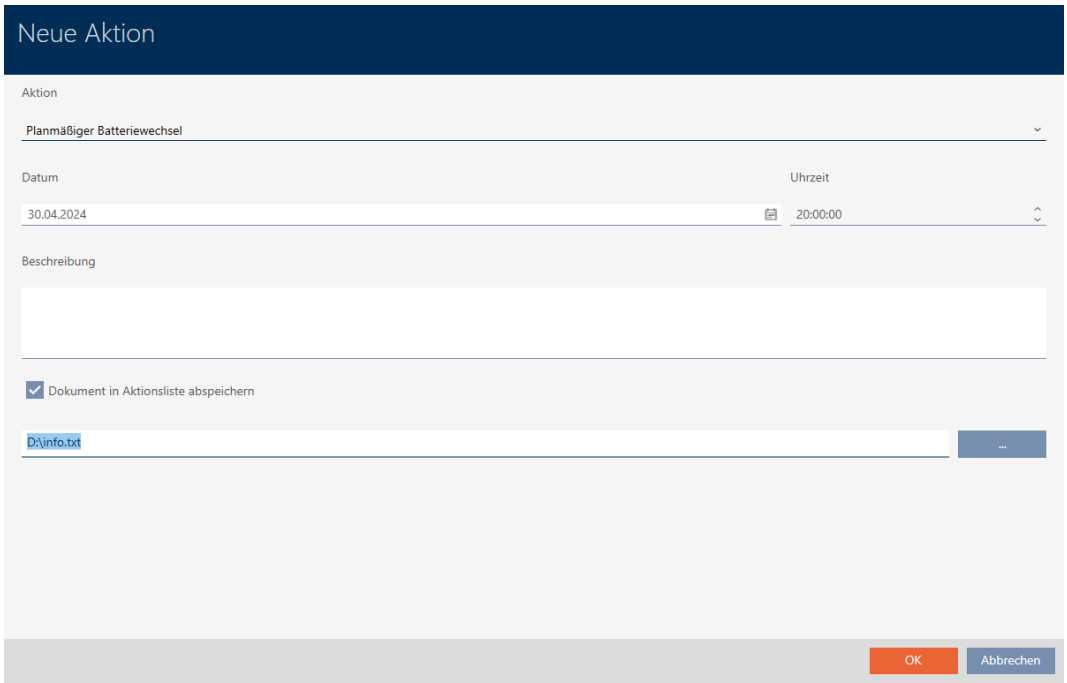


3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.

7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

↳ Aktion ist erstellt und wird aufgelistet.

Datum	Typ	Benutzer	Beschreibung	Dokument
30.04.2024 20:00:00	Planmäßiger Batteriewec	Admin		D:\info.txt
30.04.2024 14:34:39	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:34:03	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:31:23	Zurückgesetzt	Admin	ErrorCode = NoError	
30.04.2024 14:30:50	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:30:36	Letzte Programmierung	Admin	ErrorCode = WrongDevice	
30.04.2024 14:30:24	Zurückgesetzt	Admin	ErrorCode = NoError	
30.04.2024 14:29:59	Letzte Programmierung	Admin	ErrorCode = NoError	

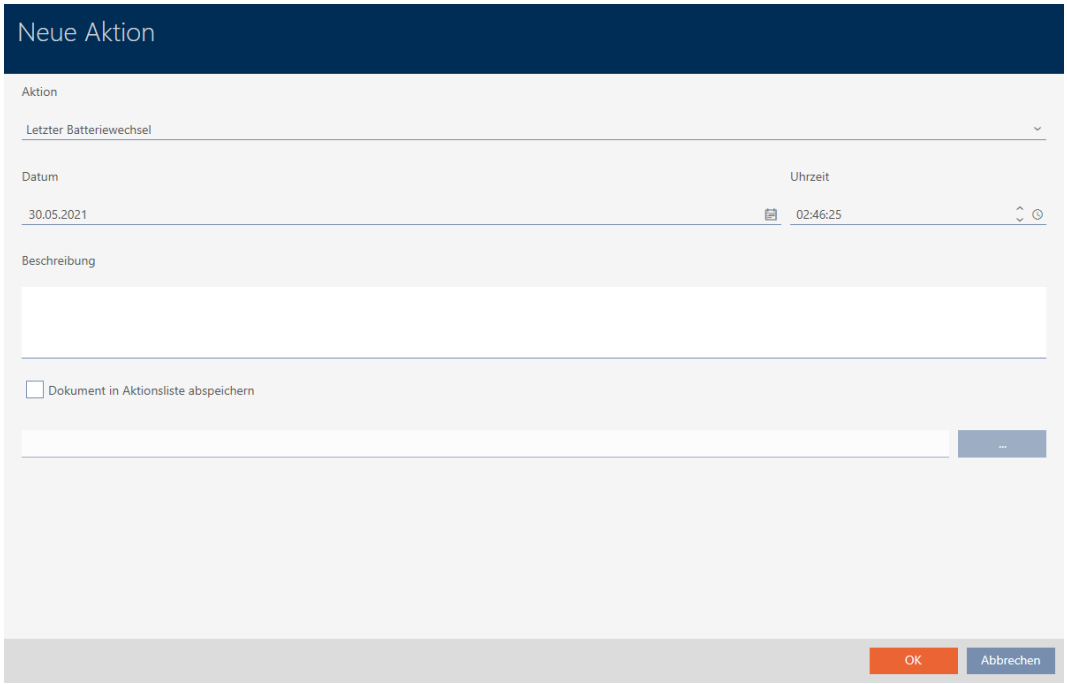
15.13.3 Rückgabe planen und protokollieren

15.13.3.1 Transponder-/Karten-Rückgabe planen und protokollieren

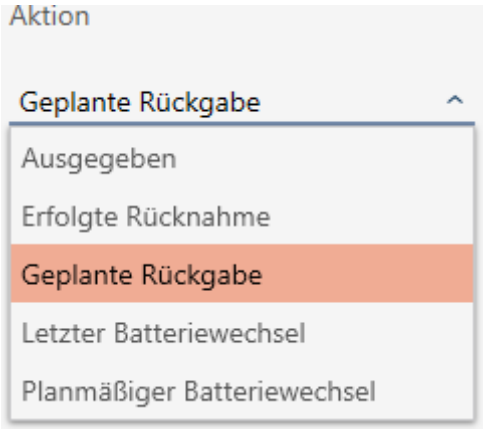
Um den Überblick darüber zu behalten, wann welche Identmedien zurückgegeben werden sollen, können Sie in der Aktionsliste einen entsprechenden Vermerk eintragen.

In der Aktionsliste können Sie auch eintragen, wann ein Identmedium tatsächlich zurückgegeben wurde. Hier müssen Sie das Identmedium aber manuell zurücksetzen. Stattdessen bietet sich der Assistent für die Rückgabe an: *Zurückgegebenen Transponder/Karte vermerken und zurücksetzen (wieder ins Inventar)* *[▸ 179]*. Der resultierende Eintrag in der Aktionsliste ist derselbe - unabhängig davon, ob mit oder ohne Assistent eingetragen.

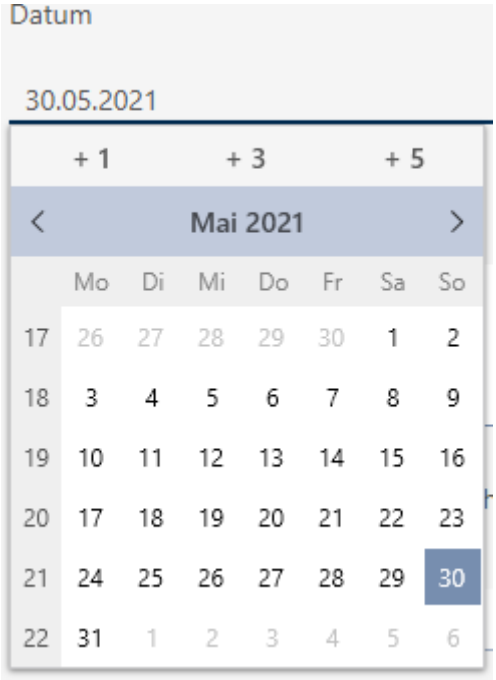
1. Klicken Sie auf die Schaltfläche + Neu .
   ↳ Fenster einer neuen Aktion öffnet sich.



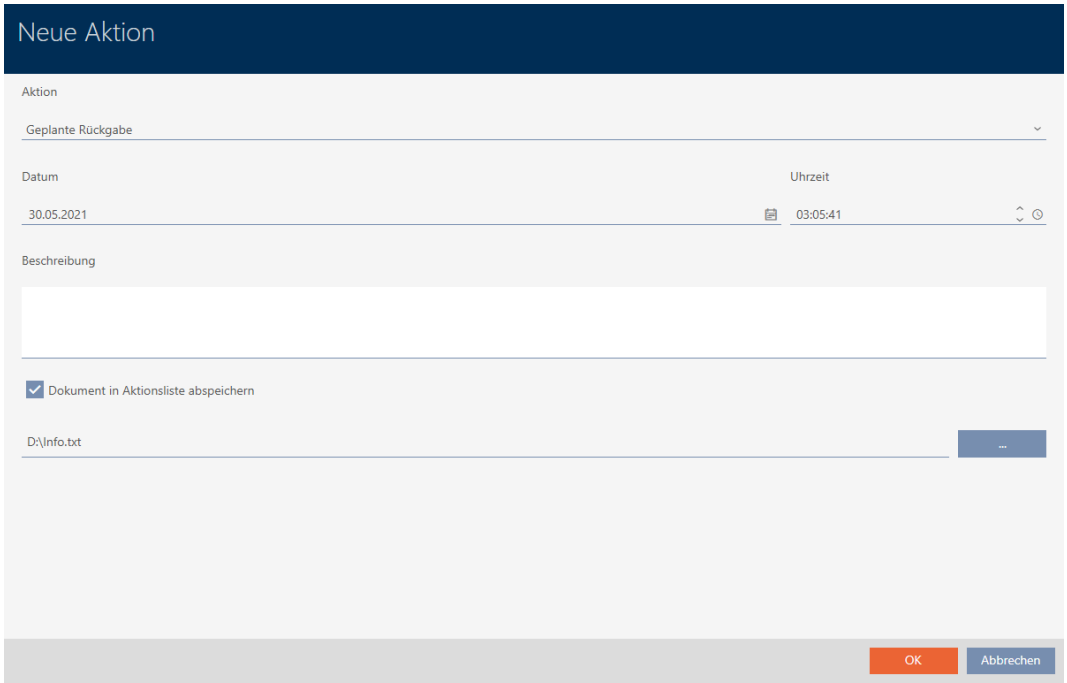
2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Geplante Rückgabe" bzw. "Erfolgte Rücknahme" aus.



3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.
7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

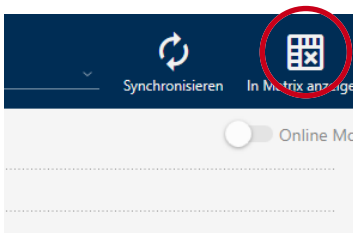
↳ Aktion ist erstellt und wird aufgelistet.

Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 03:05:41	Geplante Rückgabe	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14	Letzte Programmierung	Admin		
05.05.2021 14:08:04	Erstellt	Admin		

15.14 Identmedium oder Schließung in der Matrix wiederfinden

Ihnen stehen verschiedene Möglichkeiten zur Verfügung, um in die Einstellungen Ihrer Identmedien und Schließungen zu gelangen. Manchmal wollen Sie schnell wieder zum Eintrag in der Matrix springen, um zum Beispiel "noch schnell" eine Berechtigung zu ändern.

Das Einstellungsfenster stellt Ihnen immer folgende Schaltfläche zur Verfügung: In Matrix anzeigen



Diese Schaltfläche:

1. Öffnet immer die Matrixansicht.
2. Wählt den Eintrag des Identmediums bzw. der Schließung aus.

Damit sehen Sie sofort, welches Identmedium bzw. welche Schließung gemeint ist.

15.15 Identmedien als Liste exportieren

Alle Identmedien in Ihrer Schließanlage lassen sich als PDF exportieren.

Im PDF werden genau dieselben Identmedien in genau derselben Reihenfolge wie in der AXM Plus angezeigt.

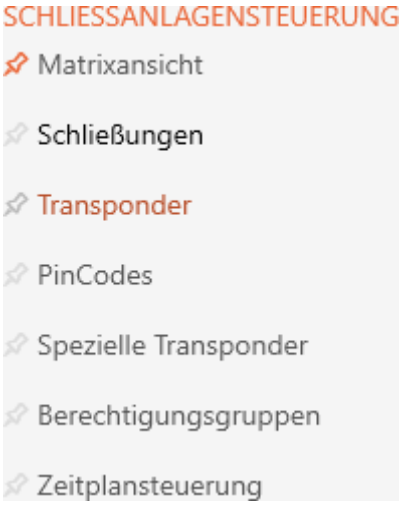
Das bedeutet, dass Sie die Anzeige vor dem Export sortieren und filtern können. Damit sortieren und filtern Sie auch die exportierte Liste.

15.15.1 AX2Go-Schlüssel/Transponder/Karten als Liste exportieren

✓ Identmedium vorhanden.

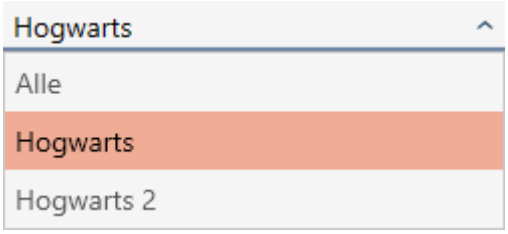
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

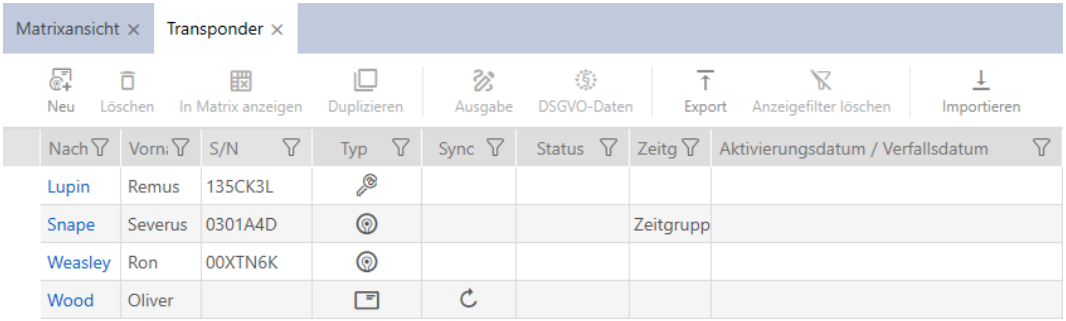
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.



   ↳ Liste mit allen in der Schließanlage vorhandenen Identmedien öffnet sich.

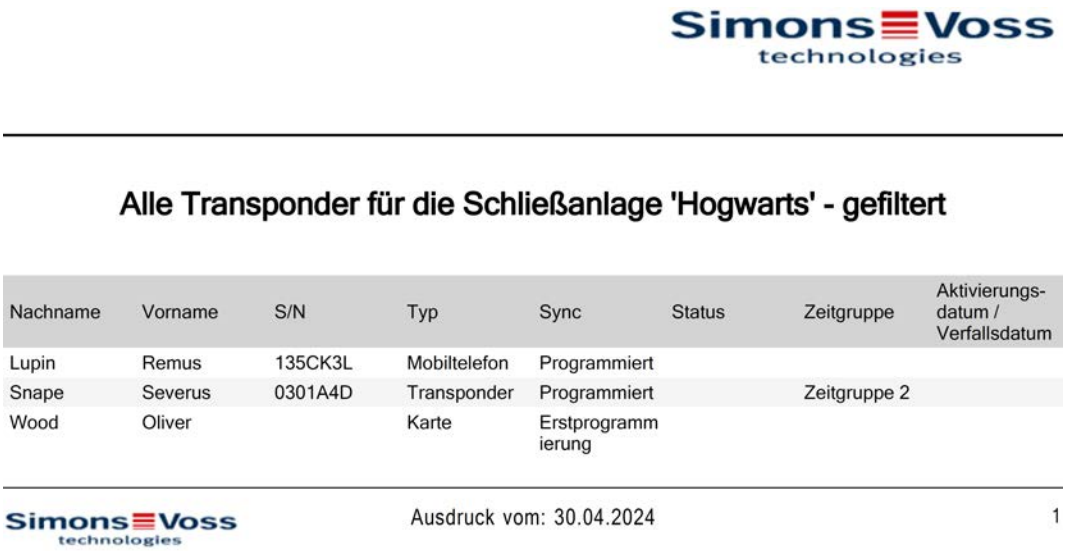
3. Wählen Sie rechts oben die Schließanlage aus, deren Identmedien Sie exportieren wollen (alternativ: "Alle").





4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
5. Klicken Sie auf die Schaltfläche Export ↑.
   ↳ Explorer-Fenster öffnet sich.
6. Speichern Sie die PDF-Datei in einem Dateiverzeichnis Ihrer Wahl.

↳ Angezeigte Identmedien werden als PDF-Datei (DIN A4) exportiert.



Alle Transponder für die Schließanlage 'Hogwarts' - gefiltert

Nachname	Vorname	S/N	Typ	Sync	Status	Zeitgruppe	Aktivierungs-datum / Verfallsdatum
Lupin	Remus	135CK3L	Mobiltelefon	Programmiert			
Snape	Severus	0301A4D	Transponder	Programmiert		Zeitgruppe 2	
Wood	Oliver		Karte	Erstprogramm ierung			

Ausdruck vom: 30.04.2024 1

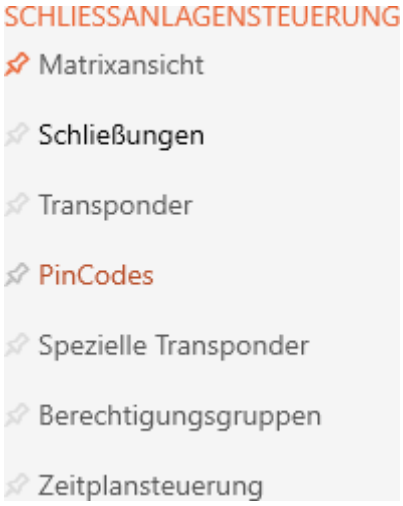
Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

15.15.2 PINs und PinCode-Tastaturen als Liste exportieren

✓ PinCode-Tastatur erstellt (siehe *PinCode-Tastaturen erstellen [▸ 102]*).

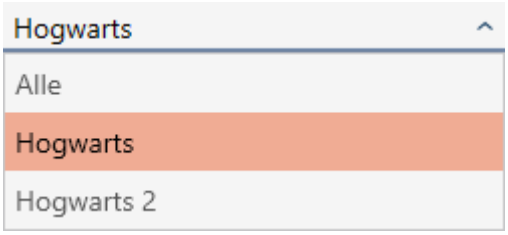
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

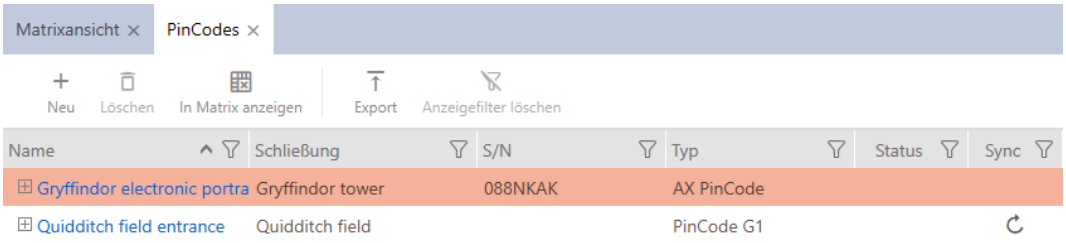
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag PinCodes.



   ↳ Liste mit allen in der Schließanlage vorhandenen PinCode-Tastaturen öffnet sich.

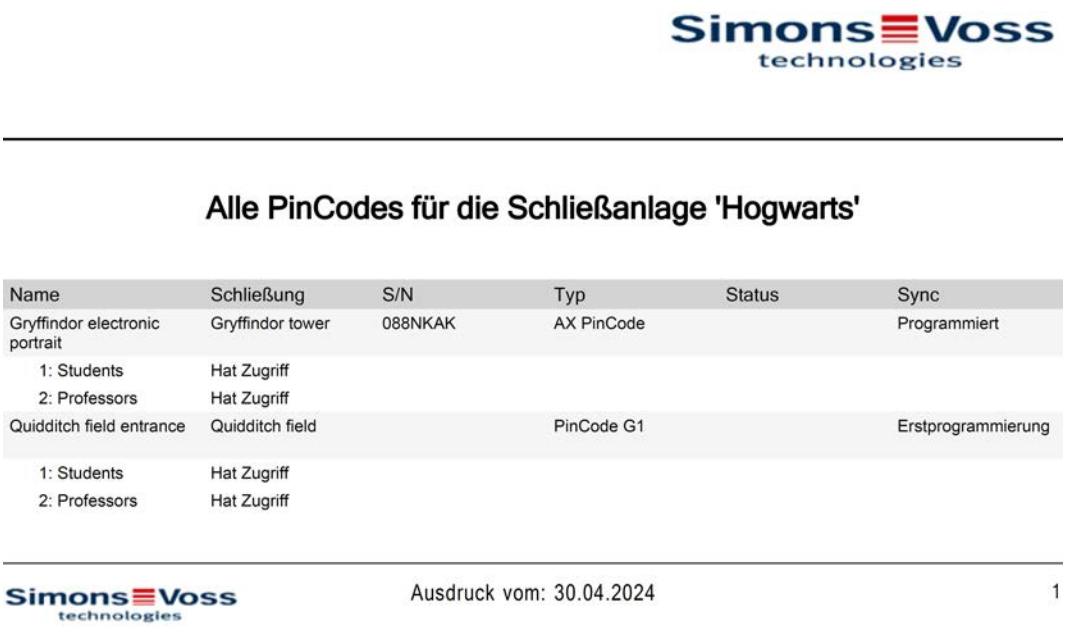
3. Wählen Sie rechts oben die Schließanlage aus, deren Identmedien Sie exportieren wollen (alternativ: "Alle").





4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
5. Klicken Sie auf die Schaltfläche Export .

↳ Angezeigte Identmedien werden als PDF-Datei (DIN A4) exportiert.



Alle PinCodes für die Schließanlage 'Hogwarts'

Name	Schließung	S/N	Typ	Status	Sync
Gryffindor electronic portrait	Gryffindor tower	088NKAK	AX PinCode		Programmiert
1: Students	Hat Zugriff				
2: Professors	Hat Zugriff				
Quidditch field entrance	Quidditch field		PinCode G1		Erstprogrammierung
1: Students	Hat Zugriff				
2: Professors	Hat Zugriff				

Ausdruck vom: 30.04.2024 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

15.16 Seriennummer und/oder TID eines Identmediums einsehen

15.16.1 Seriennummer und TID eines Transponders/Karte einsehen

Ihre Transponder und Karten haben zwei Nummern, die wichtig sind:

- Seriennummer (fest im Identmedium gespeichert, wird während der Synchronisierung ausgelesen)
- TID (flexibel durch AXM Plus vergeben, wird während der Synchronisierung auf das Identmedium geschrieben)

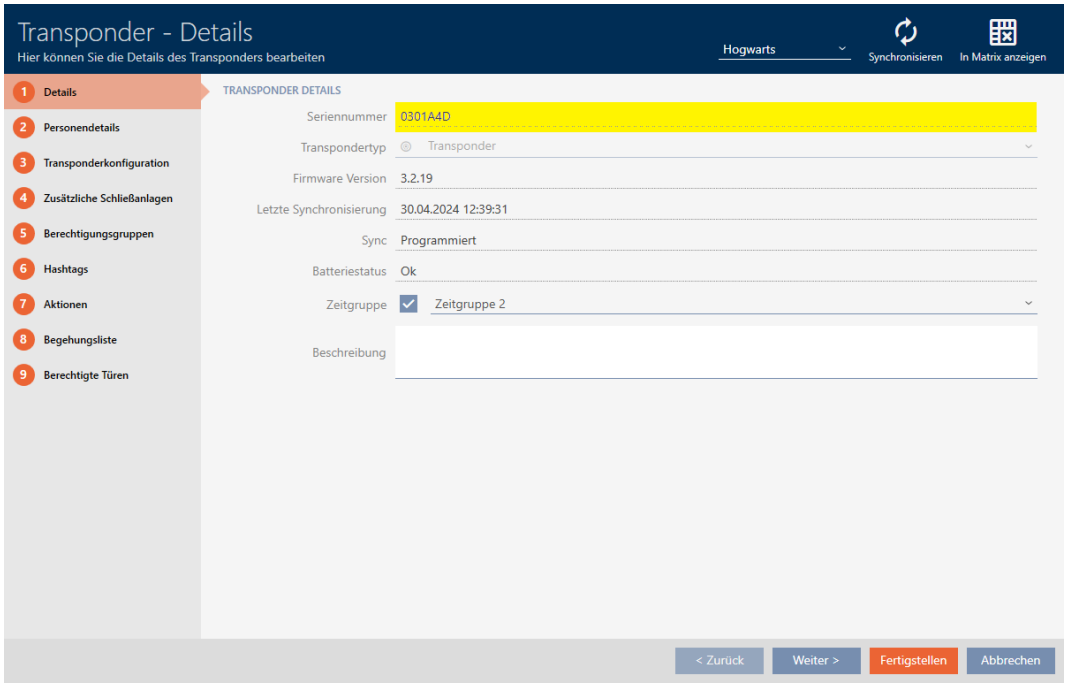
Die Seriennummer ist eine für jedes Identmedium einzigartige Nummer, während die TID nur in Ihrer Schließanlage einzigartig ist.

Wenn Sie die TID z.B. für Supportzwecke brauchen, dann können Sie die TID bei synchronisierten Identmedien über das Synchronisierungsfenster einsehen:

✓ Identmedienliste oder Matrix geöffnet.

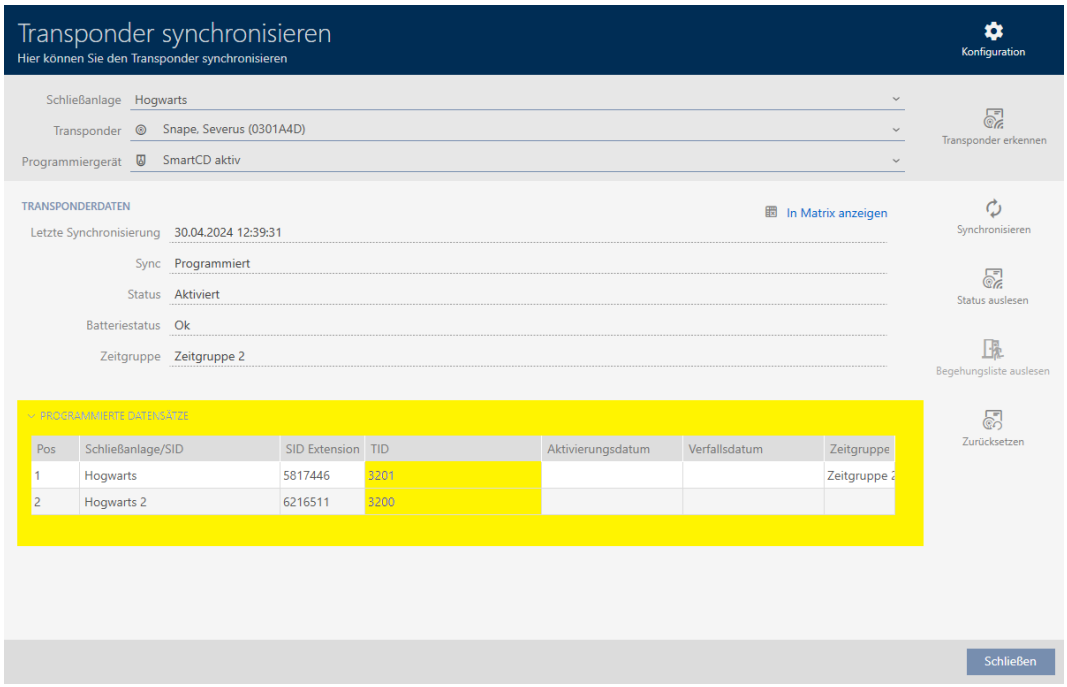
✓ Identmedium synchronisiert.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie auf das Identmedium, dessen Seriennummer und/oder TID Sie einsehen wollen.
   ↳ Fenster des Identmediums öffnet sich.
   ↳ Seriennummer wird angezeigt.



3. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Fenster wechselt zur Synchronisierung.

4. Klappen Sie das Feld "Programmierte Datensätze" aus.



↳ TIDs werden in Tabelle angezeigt. Wenn Sie das Identmedium in mehreren Schließanlagen verwenden, dann wird Ihnen für jede Schließanlage die verwendete TID angezeigt.

15.16.2 Seriennummer einer PinCode-Tastatur einsehen

Ihre PinCode-Tastaturen haben keine direkt einsehbaren TIDs. Sie finden die Seriennummer ähnlich wie bei Karten und Transpondern in den Details:

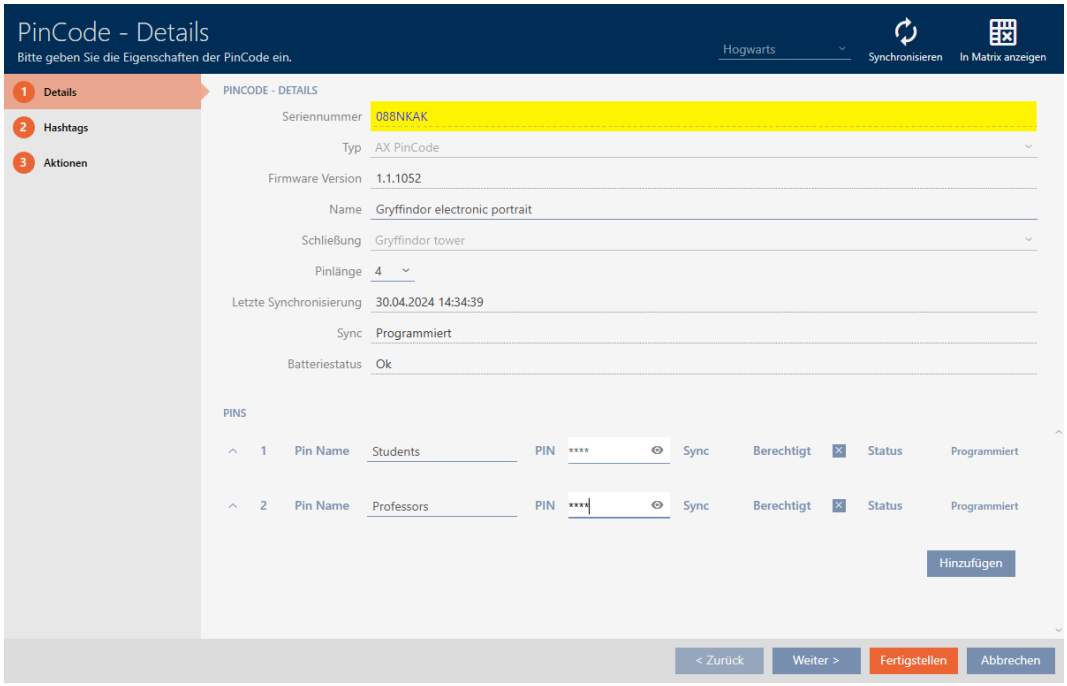
✓ PinCode-Tastatur erstellt und synchronisiert.

✓ Liste mit PinCode-Tastaturen oder Matrix geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

2. Klicken Sie auf eine PIN der PinCode-Tastatur, deren Seriennummer Sie einsehen wollen.

↳ Fenster der PinCode-Tastatur öffnet sich.
↳ Seriennummer wird angezeigt.



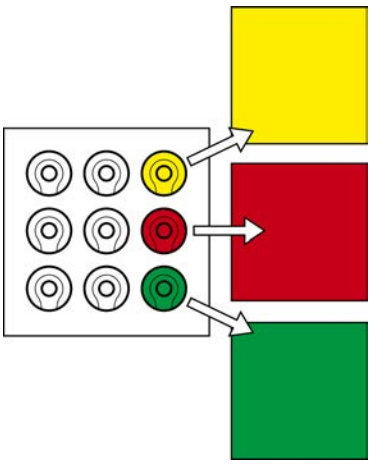
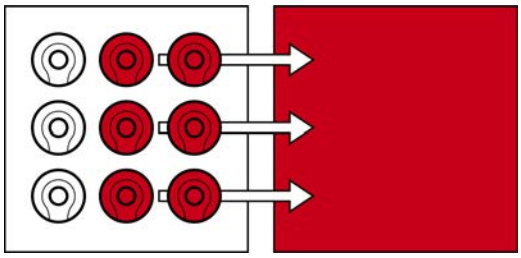
15.17 Personen zu Personengruppen zuordnen

Identmedien sind mit Personen verknüpft. In der Regel werden Sie zusammen mit einem Identmedium auch eine Person anlegen, der dieses Identmedium gehört.

PinCode-Tastaturen sind hier eine Ausnahme. Diese sind darauf ausgelegt, von mehreren Personen benutzt zu werden und können deshalb nicht einer Personengruppe zugeordnet werden. Stattdessen können Sie aber die PINs einer Zeitgruppe zuweisen (siehe *PINs einer PinCode-Tastatur zur Zeitgruppe hinzufügen [▸ 354]*).

Sobald Sie eine Person anlegen, müssen Sie eine Personengruppe angeben. Idealerweise folgen Sie der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) und erledigen alle organisatorischen Vorarbeiten bereits vor dem Erstellen Ihrer Personen (siehe *Organisationsstruktur [▸ 55]*). So müssen Sie Fenster nur einmal aufrufen.

Selbstverständlich können Sie Ihre Personen aber auch nachträglich in eine andere Personengruppe verschieben.

Einzelne Person verschieben	Mehrere Schließungen verschieben
Einzelne Person/Identmedium zu Personengruppe zuordnen (im Transponder-Fenster) [▸ 203] Geeignet für das Verschieben weniger Personen in viele verschiedene Personengruppen: 	*Mehrere Personen/Identmedien zu Personengruppe zuordnen (im Personengruppen-Fenster) [▸ 205]* Geeignet für das Verschieben mehrerer Personen in wenige verschiedene Personengruppen: 

HINWEIS

Maximal ein Bereich pro Schließung

Eine Schließung kann nur zu maximal einem Bereich gehören. Überlappende Bereiche gibt es in der AXM Plus nicht. Wenn Sie einer Schließung einen anderen Bereich zuweisen, dann wird diese Schließung ggfs. automatisch aus ihrem bisherigen Bereich entfernt.

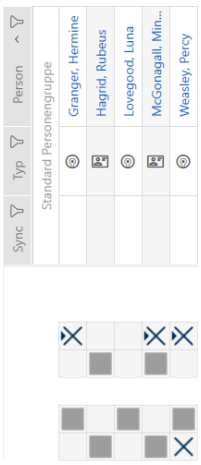
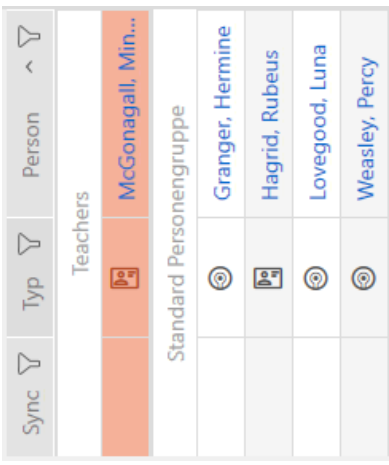
- Im Fenster "Bereich - Details" können Sie mithilfe der Spalte Bereich - Details prüfen, ob eine Schließung bereits einem Bereich zugewiesen ist.

Kein Einfluss von Personengruppen auf Berechtigungen

Berechtigungen sind nicht unmittelbar mit Personengruppen verknüpft. Wenn also eine Person in eine andere Personengruppe verschoben wird, dann ändern hat das zunächst keinen Einfluss auf Berechtigungen. Personengruppen sind aber ein nützliches Werkzeug, um Berechtigungen schneller zu ändern.

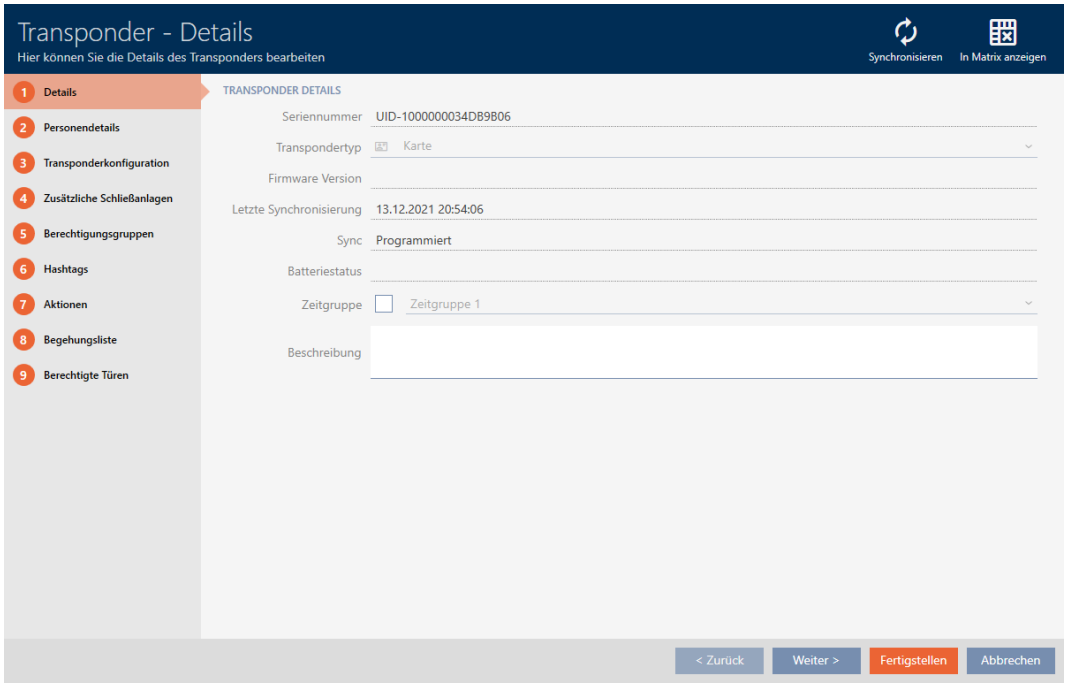
- Nutzen Sie Personengruppen, um Personen schneller zu Berechtigungsgruppen hinzuzufügen (siehe *Bereiche und Personengruppen zu Berechtigungsgruppen hinzufügen [▸ 341]*).

15.17.1 Einzelne Person/Identmedium zu Personengruppe zuordnen (im Transponder-Fenster)

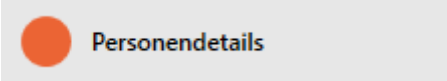
Person in "alter" Personengruppe	Person in "neuer" Personengruppe
	

✓ Mindestens eine Personengruppe erstellt (siehe *Personengruppe erstellen [▸ 56]*).

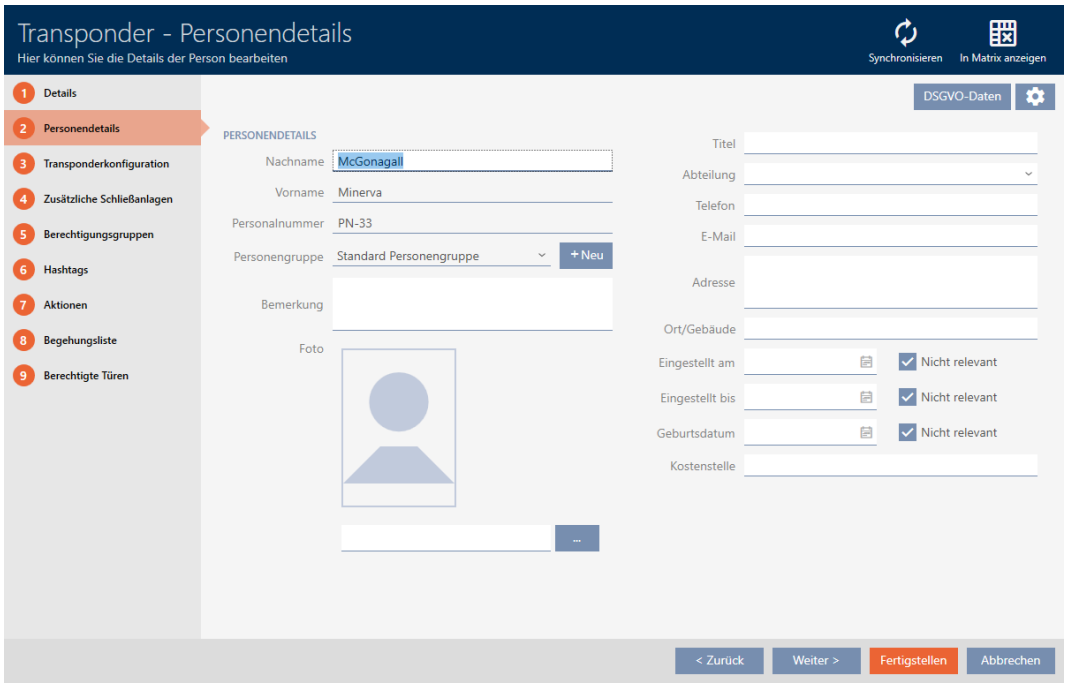
1. Klicken Sie auf das Identmedium der Person, die Sie einer neuen Personengruppe zuordnen wollen.
   ↳ Fenster des Identmediums öffnet sich.



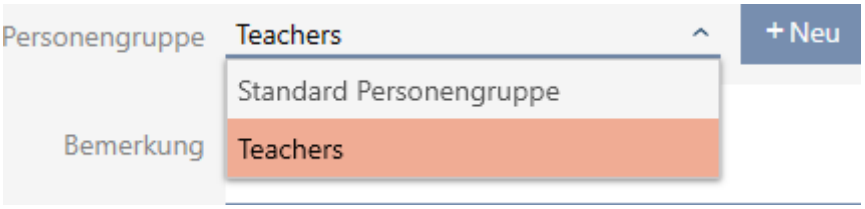
2. Klicken Sie auf den Reiter Personendetails.



↳ Reiter "Personendetails" wird angezeigt.

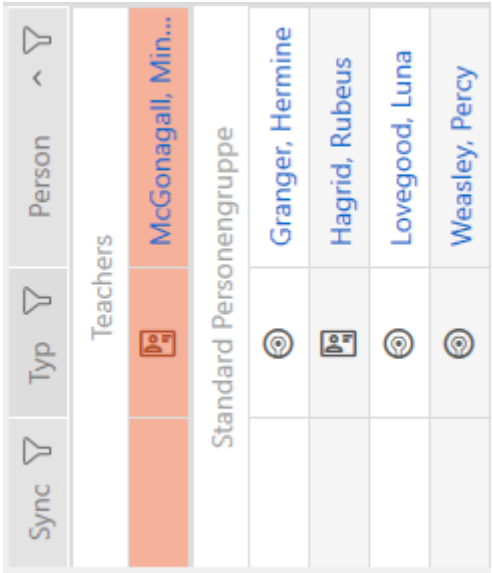


3. Wählen Sie im Dropdown-Menü ▼ **Personengruppe** die Personengruppe aus, zu der die Person künftig gehören soll.

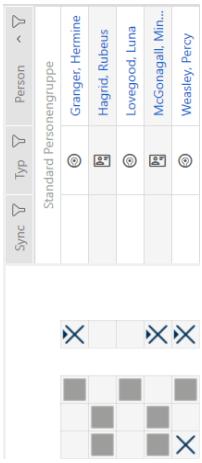
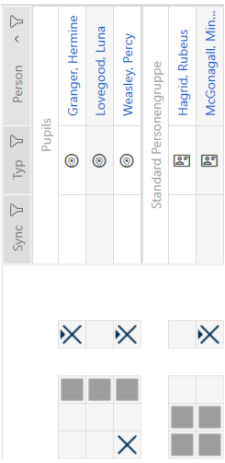


4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

↳ Person gehört zu neuer Personengruppe.



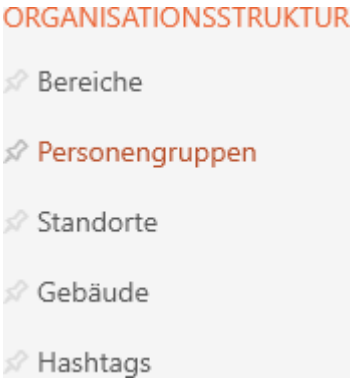
15.17.2 Mehrere Personen/Identmedien zu Personengruppe zuordnen (im Personengruppen-Fenster)

Personen in "alter" Personengruppe	Personen in "neuer" Personengruppe
	

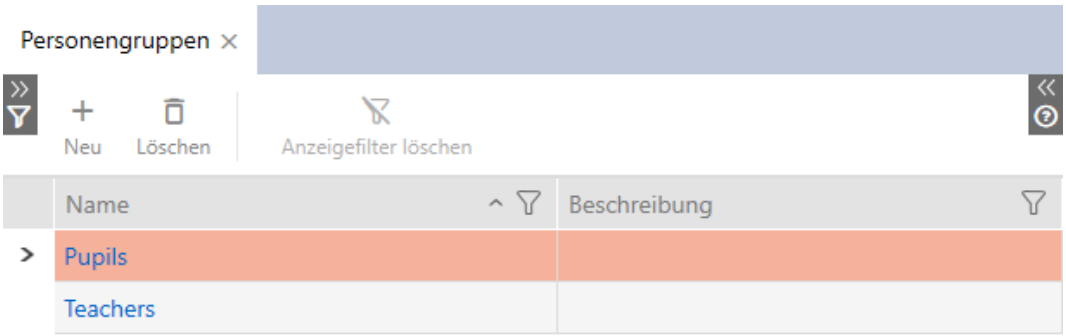
✓ Mindestens eine Personengruppe erstellt (siehe *Personengruppe erstellen [▸ 56]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

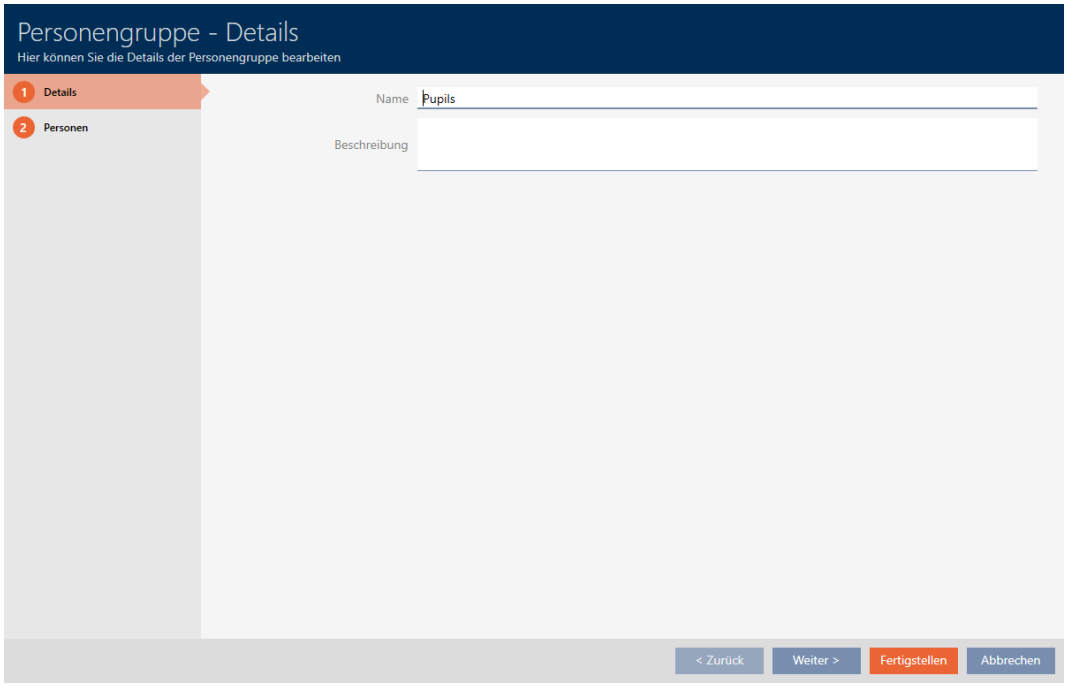
2. Wählen Sie in der Gruppe | ORGANISATIONSSTRUKTUR | den Eintrag Personengruppen.



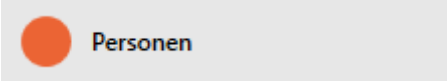
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Personengruppen] öffnet sich.



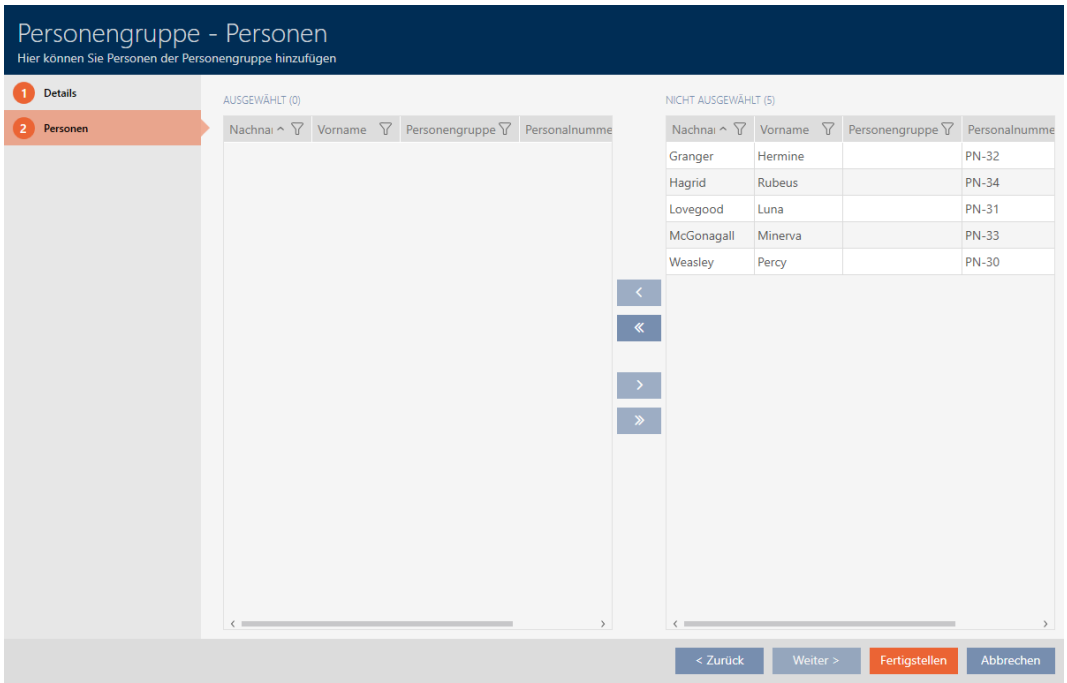
3. Klicken Sie auf die Personengruppe, der Sie die Personen zuweisen wollen.
   ↳ Fenster "Personengruppe" öffnet sich.



4. Klicken Sie auf den Reiter Personen.

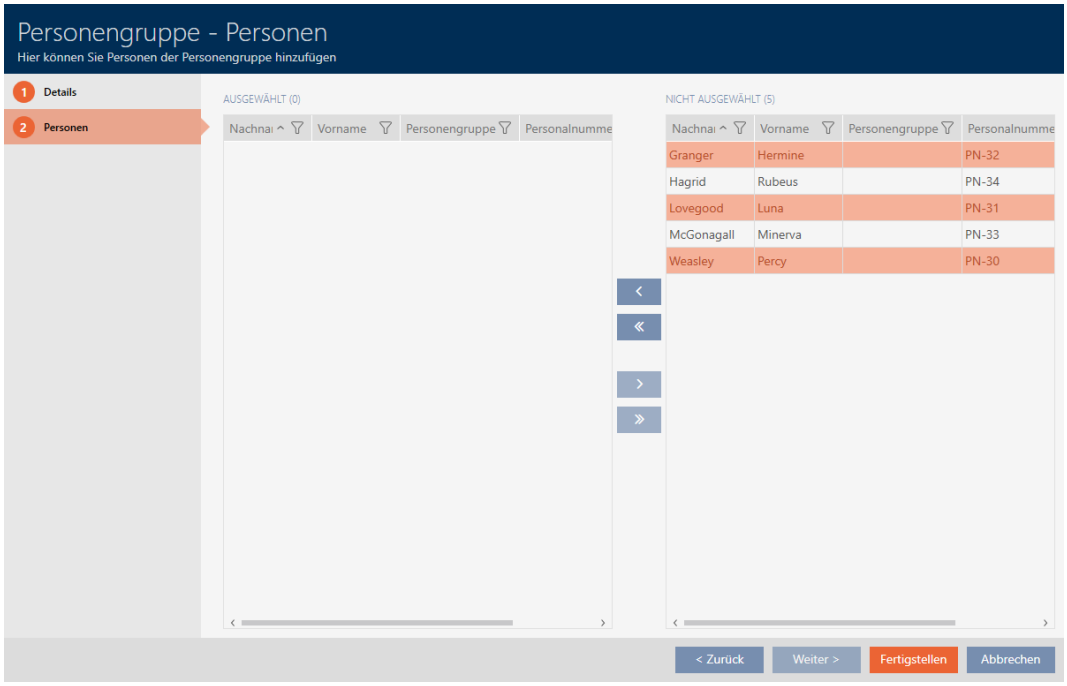


↳ Fenster wechselt zum Reiter Personen.



5. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

6. Markieren Sie alle Personen, die Sie zum Bereich hinzufügen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).



7. Verschieben Sie mit [<] nur die ausgewählten Personen oder verschieben Sie mit [«] alle angezeigten Personen.

HINWEIS

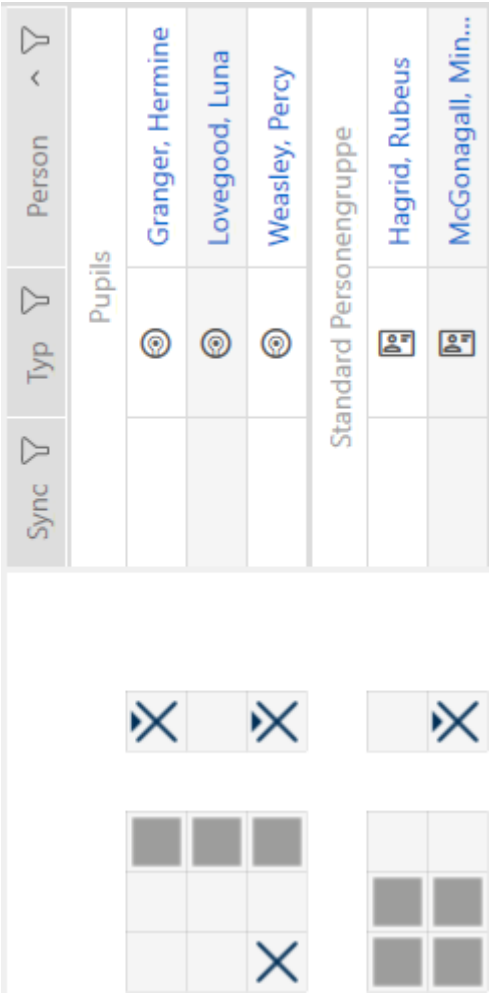
Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

↳ Die markierten Personen in der linken Spalte werden der Personengruppe hinzugefügt.

8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Personengruppe" schließt sich.
   ↳ Personen sind der neuen Personengruppe zugeordnet.

↳ Matrix zeigt Strukturierung mit neuen Personengruppen an.



15.18 Identmedium in mehreren Schließanlagen verwenden

In bestimmten Fällen ist der Einsatz mehrerer Schließanlagen sinnvoll (siehe *Schließanlagen [▸ 541]*).

Hier ist es praktisch, wenn ausgewählte Benutzer dasselbe Identmedium in mehreren Schließanlagen verwenden können.

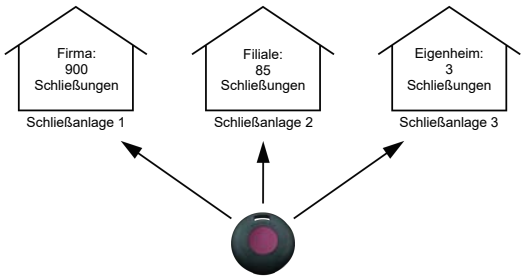
Die Verwendung in mehreren Schließanlagen unterscheidet sich von der übergreifenden Schließebene:

Verwendung in mehreren Schließ-anlagen	Übergreifende Schließebenen
▪ Mehrere voneinander unabhängige Schließanlagen werden auf Identmedium gespeichert ▪ Können aus verschiedenen Projekten und Datenbanken kommen ▪ Anzahl von möglichen Schließanlagen im Identmedium begrenzt ▪ TID in jeder dieser Schließanlagen unabhängig von TIDs in anderen Schließanlagen	▪ Übergreifende Schließebene wird erstellt und Schließanlagen zugewiesen ▪ Transponder wird in einer dieser Schließanlagen erstellt. AXM Plus erstellt den Transponder automatisch auch in den anderen zugewiesenen Schließanlagen ▪ Anzahl an so zugewiesenen Schließanlagen nicht begrenzt ▪ Berechtigungen werden in zugewiesenen Schließanlagen gesetzt Zur Einrichtung einer übergreifenden Schließebene siehe *Übergreifende Schließebene verwenden [▸ 405]*.

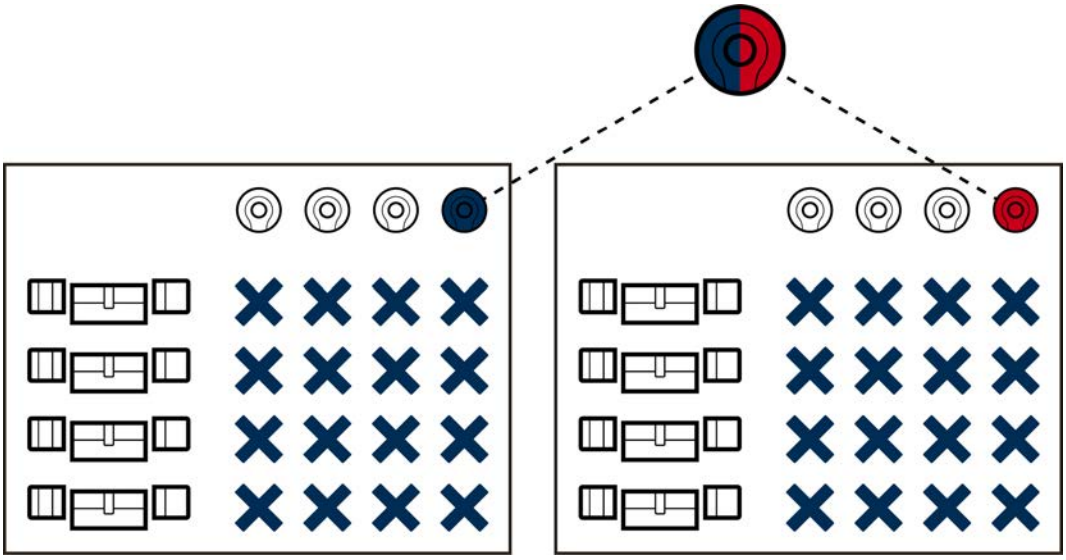
Weitere Informationen zur übergreifenden Schließebene finden Sie hier: *Übergreifende Schließebenen [▸ 543]*.

Eine PinCode-Tastatur wird genau einer Schließung fest zugewiesen und ist nicht mobil. Die Verwendung in mehreren Schließanlagen oder in übergreifenden Schließebenen ist deshalb nicht sinnvoll und für PinCode-Tastaturen nicht möglich.

Beispiel: Ein Hausmeister soll Zutritt zu Türen in verschiedenen Schließanlagen bekommen.

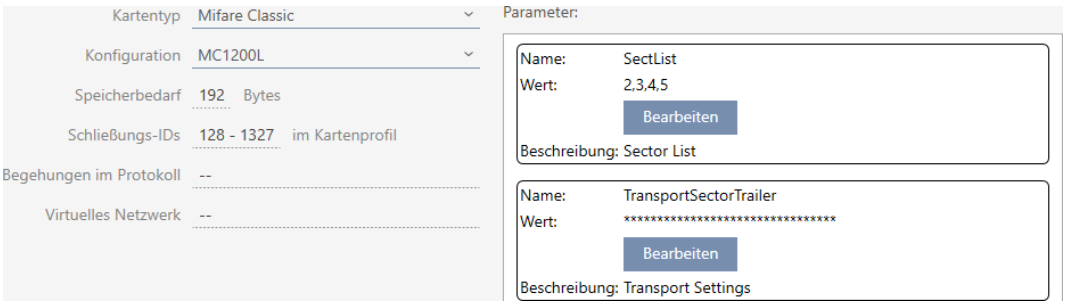


Er muss dabei nicht mit mehreren Identmedien hantieren. Stattdessen legen Sie das Identmedium des Hausmeisters in jeder Schließanlage an, synchronisieren anschließend aber den gleichen Transponder.



- G2-Transponder können bis zu fünf Schließanlagen speichern (3 G2-Schließanlagen und 2 G1-Schließanlagen).
- Karten können je nach verfügbarem Speicher und Kartenkonfiguration ebenfalls mehrere Schließanlagen speichern (siehe *Kartentemplates [▸ 577]*). In der AXM Plus stellen Sie Kartenkonfigurationen nicht mehr projektweit, sondern schließanlagenweit ein (siehe *Karten bzw. Transponder freischalten [▸ 401]*). Das hat zwei Vorteile:
  - Mehrere Schließanlagen auf einer Karte sind kein Problem - behandeln Sie eine bereits vorhandene Schließanlage wie eine Fremdanwendung und wählen Sie für die zusätzliche Schließanlage freie Sektoren bzw. App-IDs aus (*MIFARE Classic (bereits verwendete Karte) [▸ 373]* bzw. *MIFARE DESFire (bereits verwendete Karte) [▸ 387]*).

  - Solange Sie den gleichen Kartentyp (Classic / DESFire) verwenden, können Sie sogar verschiedene Kartenkonfigurationen in Ihren Schließanlagen nutzen.



Transponder sind einfacher als Karten in mehreren Schließanlagen zu betreiben, da hier keine Sektoren bzw. App-IDs berücksichtigt werden müssen.

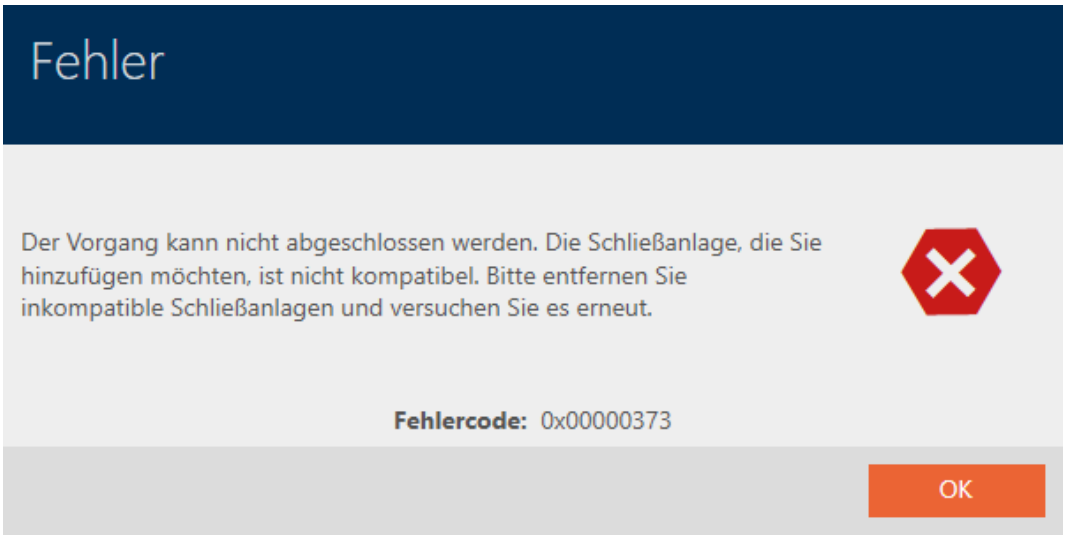
Es gibt zwei Möglichkeiten, ein Identmedium wiederzuverwenden:

- *Identmedium im gleichen Projekt wiederverwenden [▸ 212]*
- *Identmedium in anderen Projekten/Datenbanken wiederverwenden [▸ 217]*

15.18.1 Identmedium im gleichen Projekt wiederverwenden

Mit der AXM Plus können Sie ganz einfach dasselbe Identmedium für mehrere Schließanlagen verwenden.

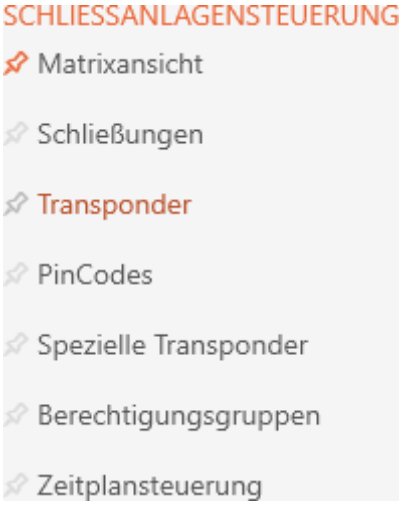
Falls Sie mit Karten arbeiten, prüft die AXM Plus sogar, ob die eingestellten Kartenkonfigurationen miteinander kompatibel sind oder ob sich zum Beispiel die Sektoren überschneiden würden:



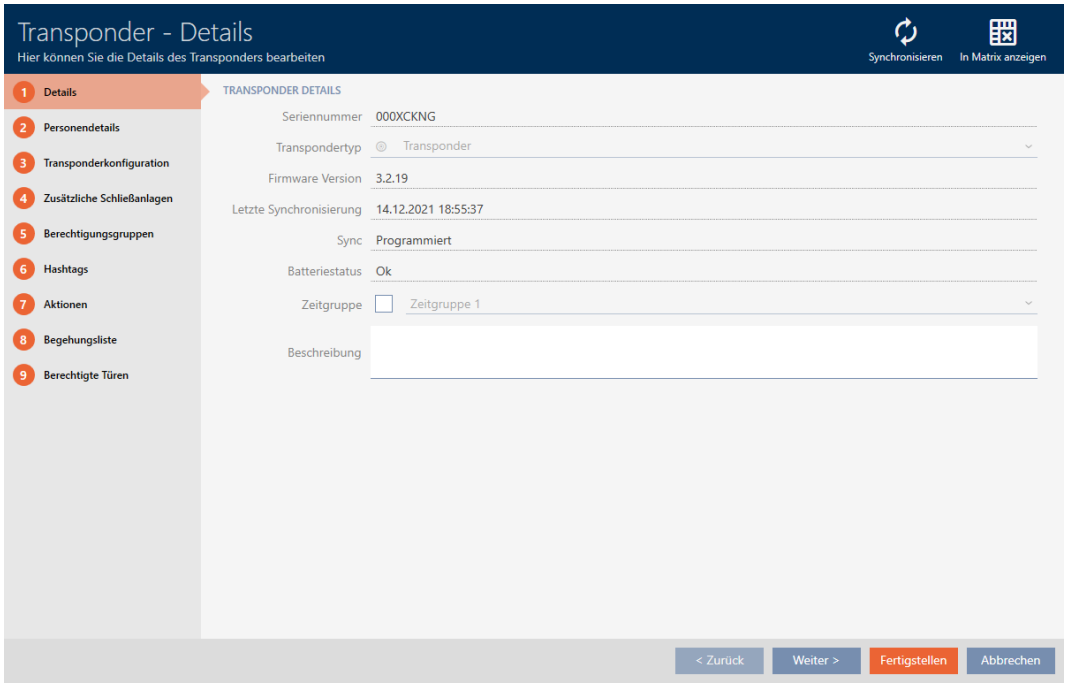
✓ Mindestens zwei Schließanlagen im gleichen Projekt erstellt (siehe *Schließanlage erstellen [▸ 360]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

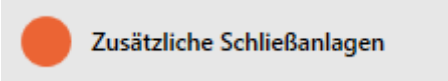
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.



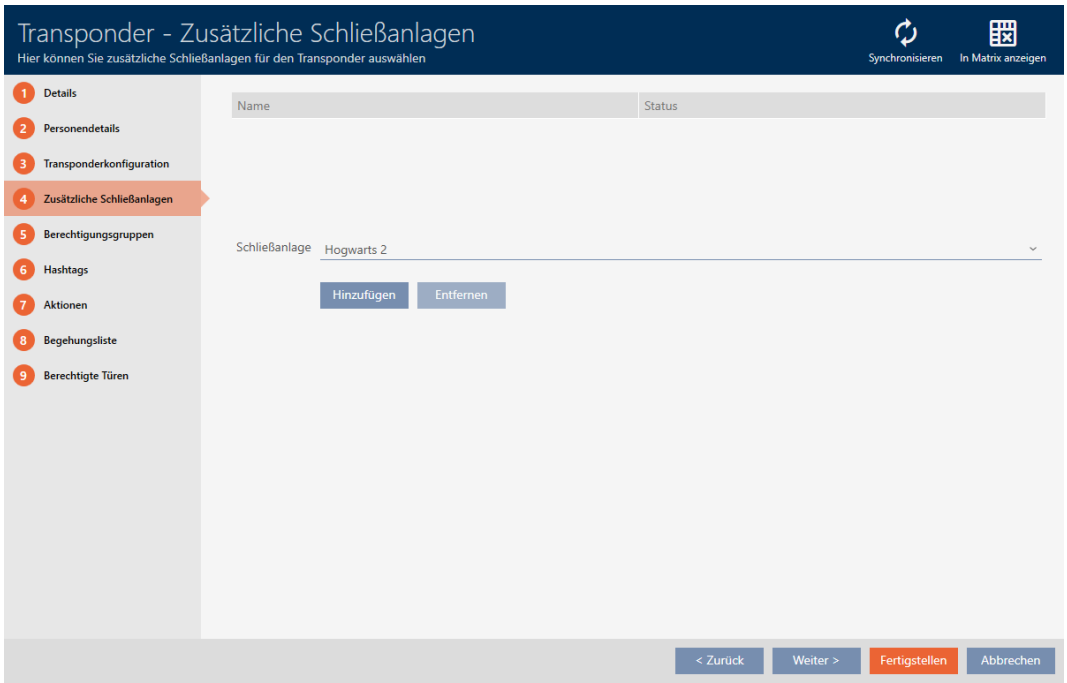
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Transponder] öffnet sich.
3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
4. Klicken Sie auf das Identmedium, das Sie auch in einer anderen Schließanlage verwenden wollen.
   ↳ Fenster des Identmediums öffnet sich.



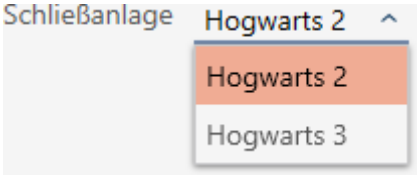
5. Klicken Sie auf den Reiter Zusätzliche Schließanlagen.



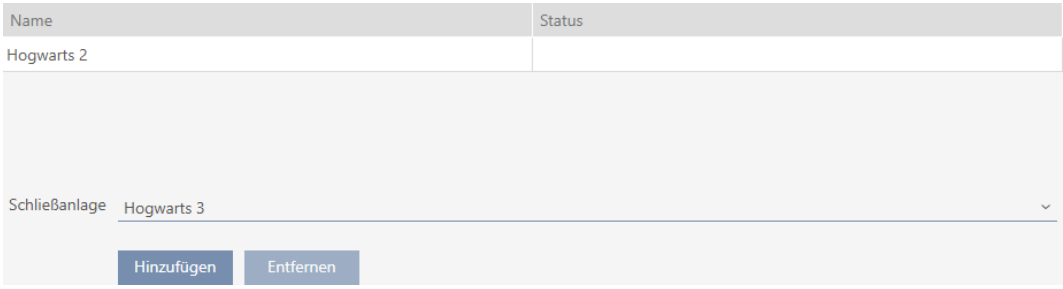
↳ Fenster wechselt zum Reiter "Zusätzliche Schließanlagen".



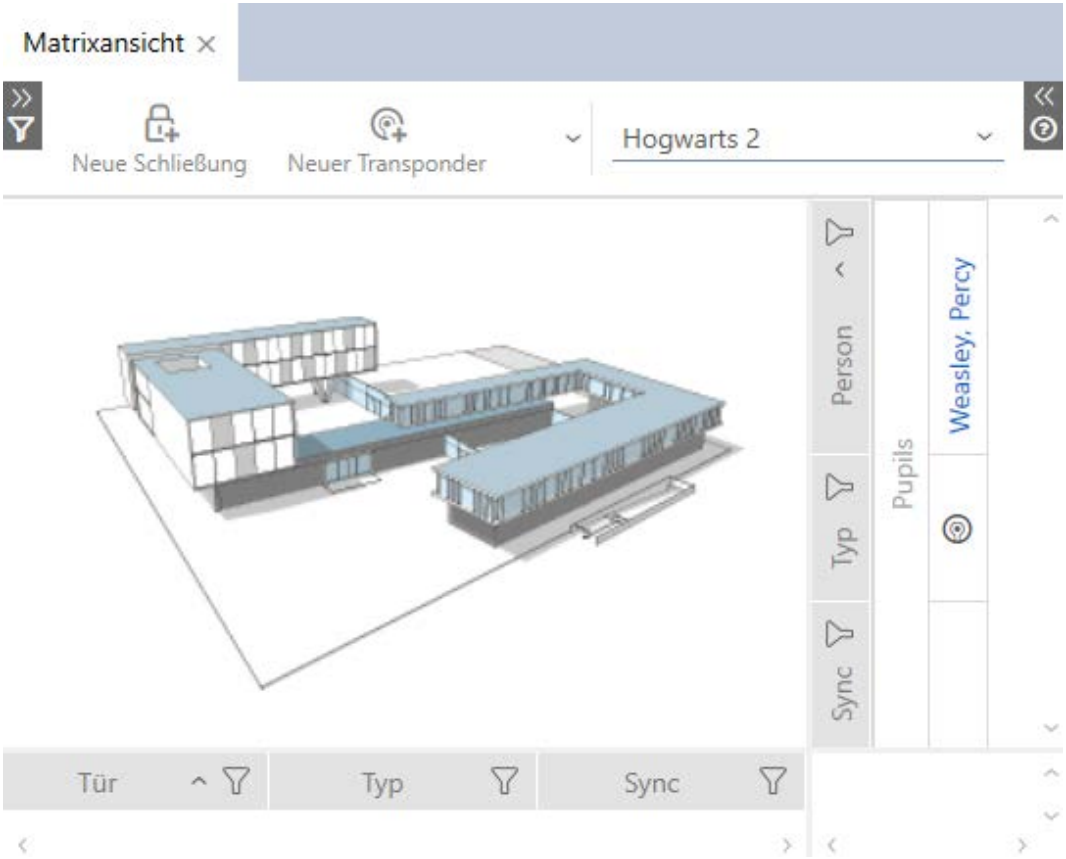
6. Wählen Sie im Dropdown-Menü ▼ **Schließanlage** die Schließanlage aus, in der Sie das Identmedium wiederverwenden wollen.



7. Klicken Sie auf die Schaltfläche Hinzufügen.
   ↳ Die ausgewählte Schließanlage wird in der Tabelle aufgelistet.



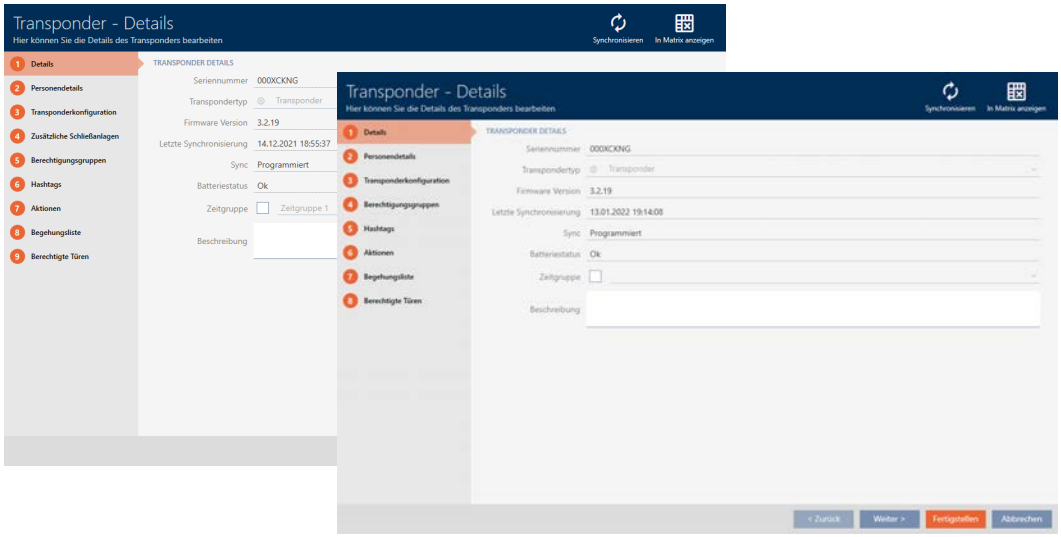
8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Ihre AXM Plus prüft für Sie, ob die Schließanlagen kompatibel sind.
   ↳ Fenster des Identmediums schließt sich.
   ↳ Wiederverwendetes Identmedium wird automatisch zu den weiteren Schließanlagen hinzugefügt.



9. Synchronisieren Sie das Identmedium (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).
↳ Alle Schließanlagen, in denen das Identmedium verwendet wird, werden automatisch mitsynchronisiert.

Erkennung an der Seriennummer

Beide Identmedien haben im Fenster "Transponder" im Feld *Seriennummer* den gleichen Eintrag.



Ein Blick auf den programmierten Transponder verrät Ihnen, dass es wirklich ein und derselbe Transponder ist:

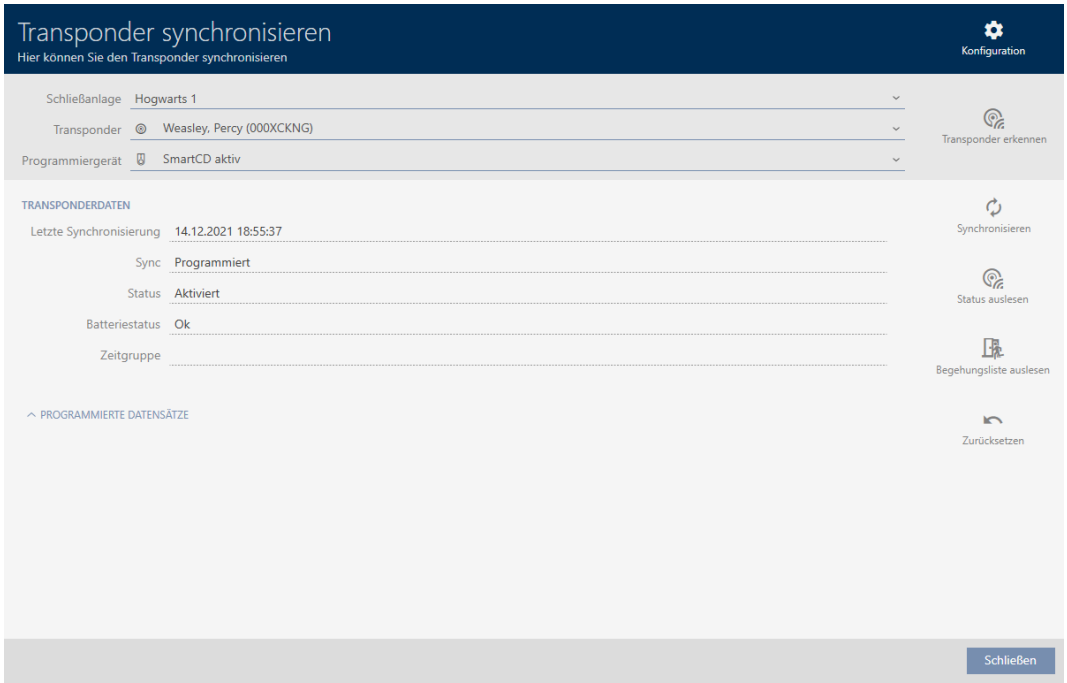
(Voraussetzung: Das Transponder-Gehäuse ist im Auslieferungszustand.)

Erkennung an den programmierten Datensätzen

Sie erkennen die Verwendung in anderen Schließanlagen auch an den programmierten Datensätzen:

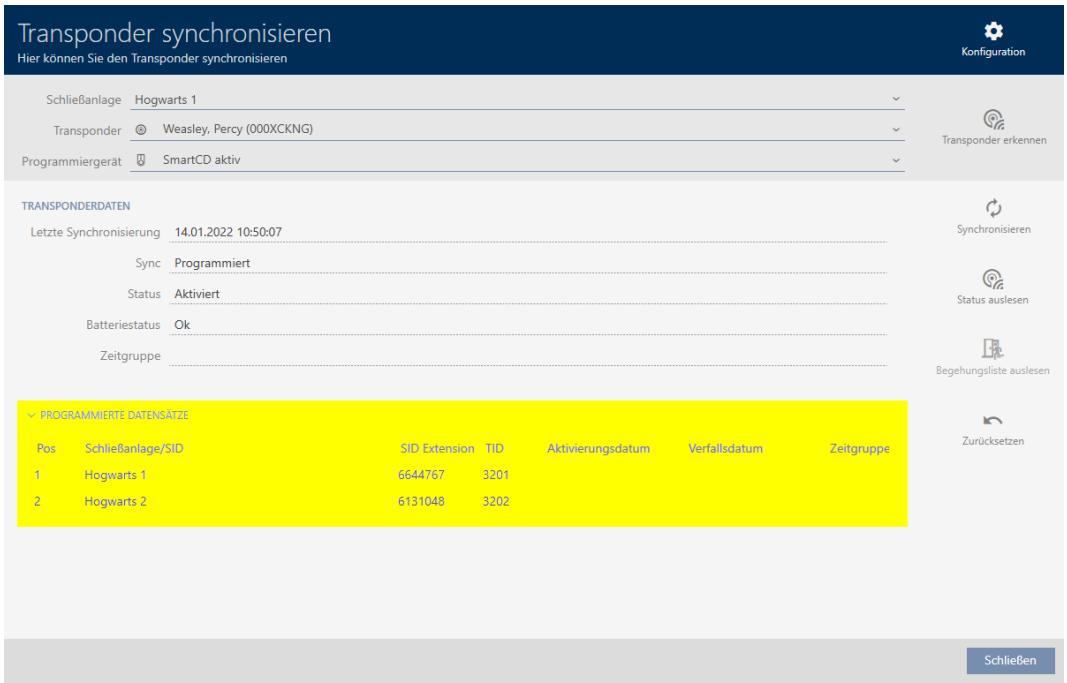
✓ "Transponder" geöffnet.

1. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Fenster "Transponder synchronisieren" öffnet sich.



2. Klappen Sie den Bereich "Programmierte Datensätze" aus.

↳ Sie sehen in den programmierten Datensätzen die Schließanlage, die Sie vorhin hinzugefügt haben.



15.18.2 Identmedium in anderen Projekten/Datenbanken wiederverwenden

Verwendung desselben Identmediums in unterschiedlichen Projekten/ Datenbanken

Sie können dasselbe Identmedium aber nicht nur innerhalb eines Projekts verwenden (siehe *Identmedium im gleichen Projekt wiederverwenden* [▸ 212]).

Zusätzlich haben Sie auch die Möglichkeit, dasselbe Identmedium nicht nur in unterschiedlichen Schließanlagen zu verwenden, sondern sogar in verschiedenen Datenbanken:

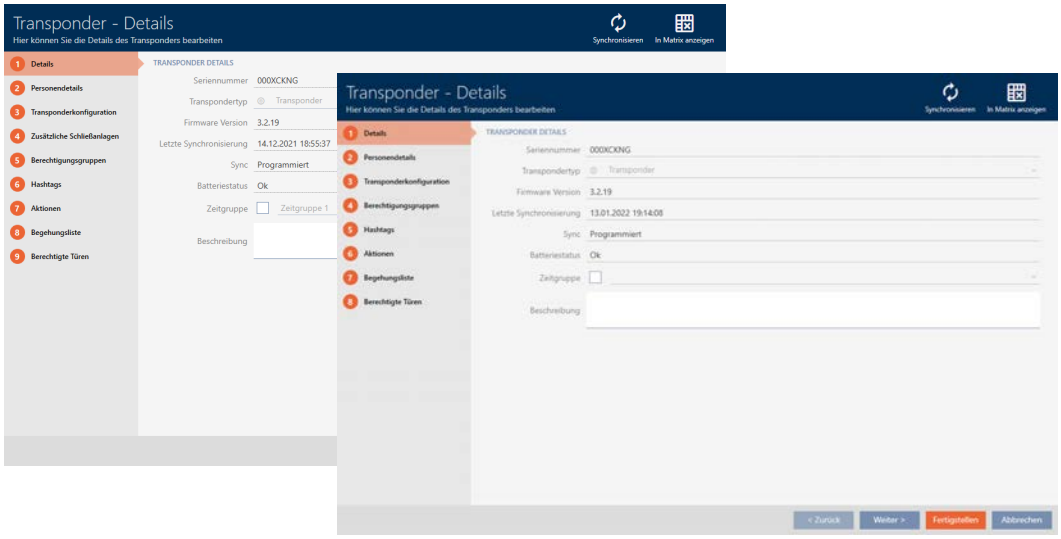
- Verwendung in unterschiedlichen AXM-Projekten (Projekte haben eine eigene Datenbank)
- Verwendung in einer AXM- und einer LSM-Schließanlage

1. Synchronisieren Sie das Identmedium in Ihrem Projekt (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).
2. Synchronisieren Sie dasselbe Identmedium in einem anderen Projekt oder in einer anderen Datenbank.

↳ Identmedium wird in mehreren Schließanlagen verwendet, die unabhängig voneinander sind.

Erkennung an der Seriennummer

Beide Identmedien (obwohl sie in verschiedenen Projekten sind) haben im Fenster "Transponder" im Feld *Seriennummer* den gleichen Eintrag.



Ein Blick auf den programmierten Transponder verrät Ihnen, dass es wirklich ein und derselbe Transponder ist:

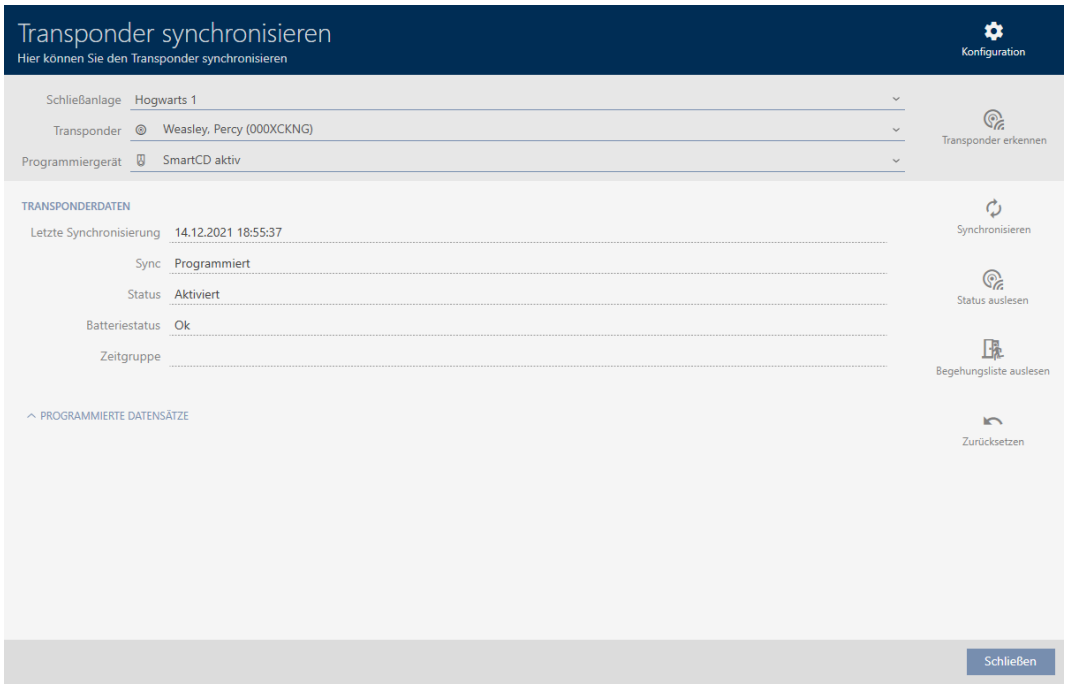
(Voraussetzung: Gehäuse ist identisch mit dem werkseitig ausgelieferten Gehäuse.)

Erkennung an den programmierten Datensätzen

Sie erkennen die Verwendung in anderen Datenbanken auch an den programmierten Datensätzen:

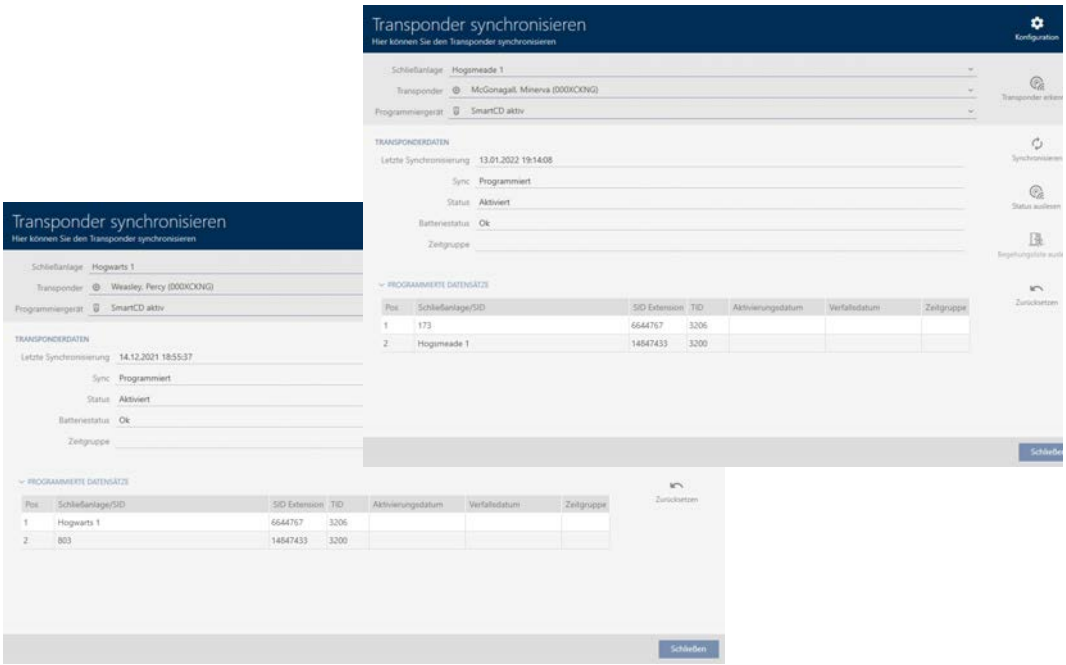
✓ "Transponder" geöffnet.

1. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Fenster "Transponder synchronisieren" öffnet sich.



2. Synchronisieren Sie den Transponder (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).
3. Klappen Sie den Bereich "Programmierte Datensätze" aus.

↳ Je nachdem, in welcher Schließanlage Sie sich befinden, sehen Sie in den programmierten Datensätzen eine zweite Schließanlage. Im Gegensatz zur Wiederverwendung im gleichen Projekt (siehe *Identmedium im gleichen Projekt wiederverwenden [▸ 212]*) sehen Sie aber nur die Schließanlagen-ID. Die Schließanlagen-ID ist auch im Identmedium gespeichert und deshalb bekannt. Der Name der Schließanlage ist aber in einer anderen Datenbank gespeichert und kann deshalb nicht angezeigt werden.



15.19 Verwaltung von AX2Go-Schlüsseln

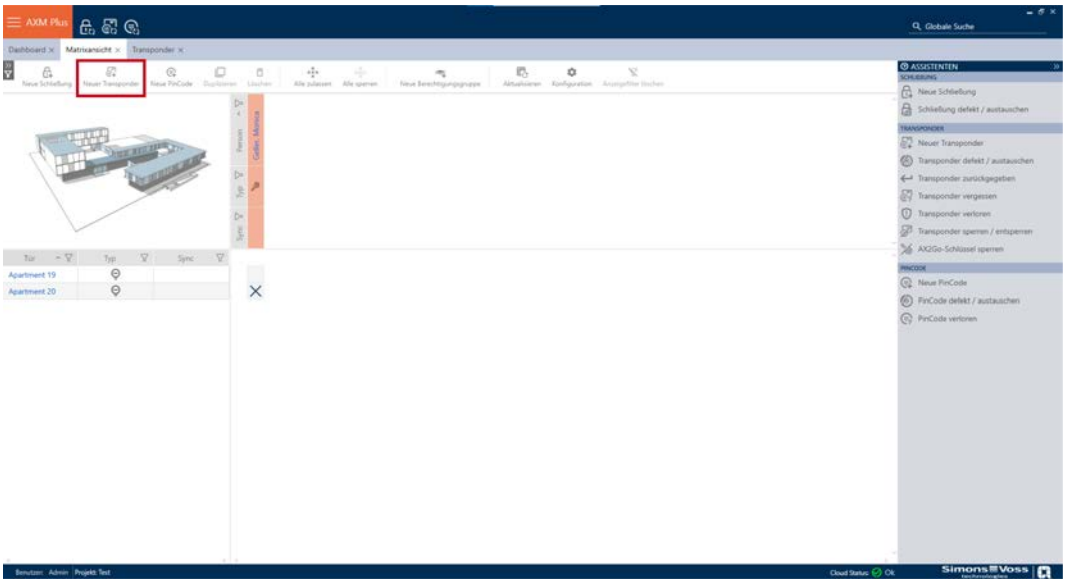
15.19.1 Vergabe von Schlüsseln ab AXM Plus

Im Rahmen der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) empfiehlt SimonsVoss, dass Sie zuerst Berechtigungsgruppen, Personengruppen und Zeitpläne/Zeitgruppen einrichten:

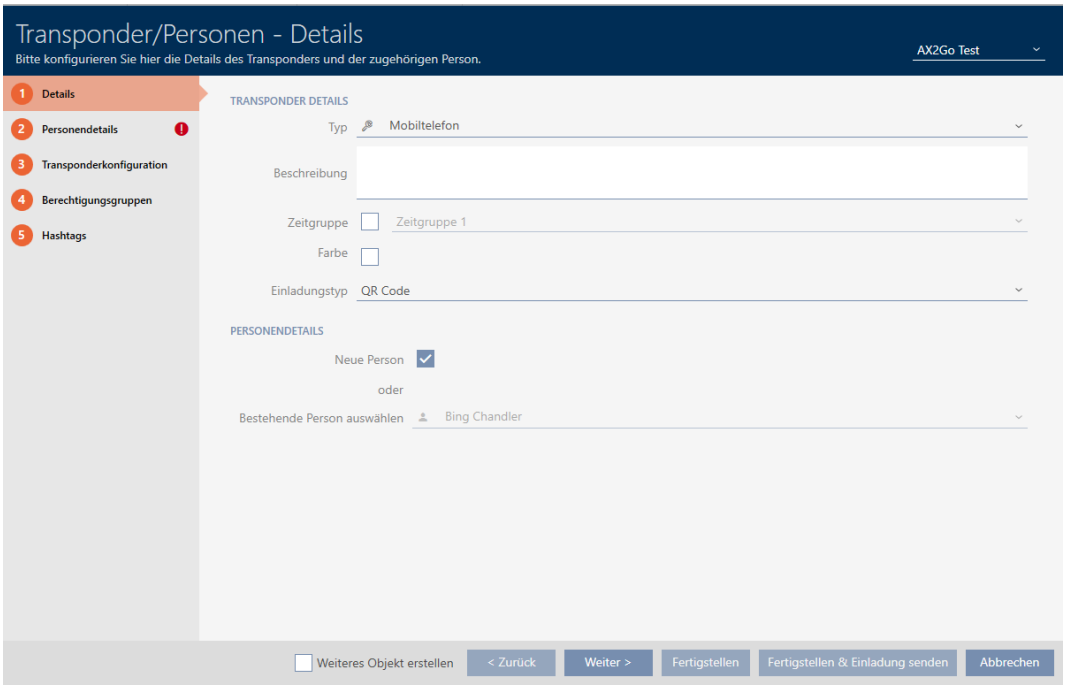
- *Berechtigungsgruppen [▸ 332]* (Hintergrundinformationen siehe *Berechtigungsgruppen [▸ 564]*)
- *Personengruppe erstellen [▸ 56]* (Hintergrundinformationen siehe *Personengruppen [▸ 565]*)
- *Zeitplan erstellen [▸ 58]* bzw. *Zeitgruppe erstellen [▸ 61]* (Hintergrundinformationen siehe *Zeitgruppen und Zeitpläne [▸ 548]*)

Als Schließanlagenverwalter können Sie an Nutzer auch mobile Schlüssel versenden, die als Zutrittsberechtigungen in der AX2Go App gespeichert werden. Das Anlegen von Schlüsseln für AX2Go funktioniert genauso, wie das Anlegen von Transpondern.

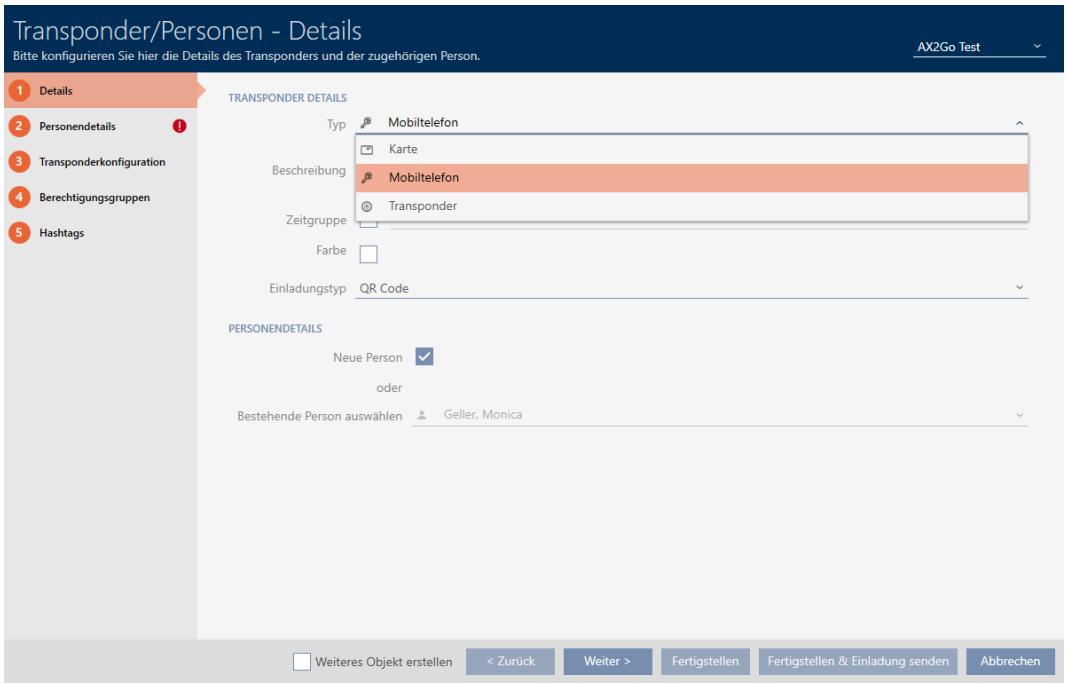
1. Klicken Sie in der Matrixansicht Ihrer Schließanlage auf die Schaltfläche Neuer Transponder.



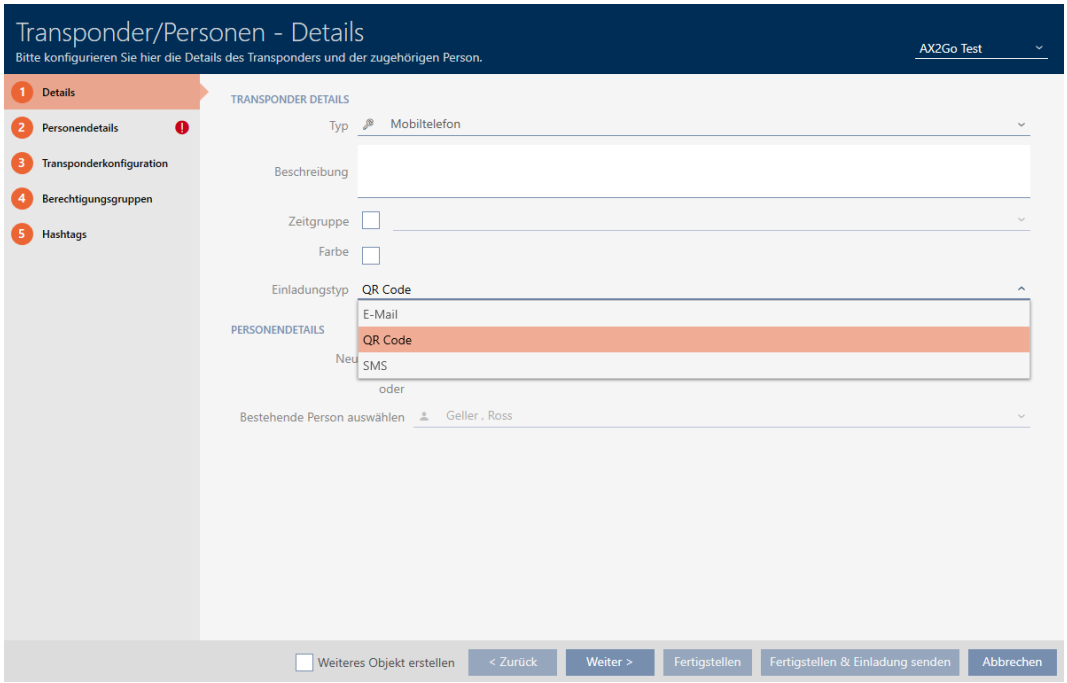
↳ Es öffnet sich eine Maske, in der Sie die Schlüssel- und Nutzereinstellungen konfigurieren können.



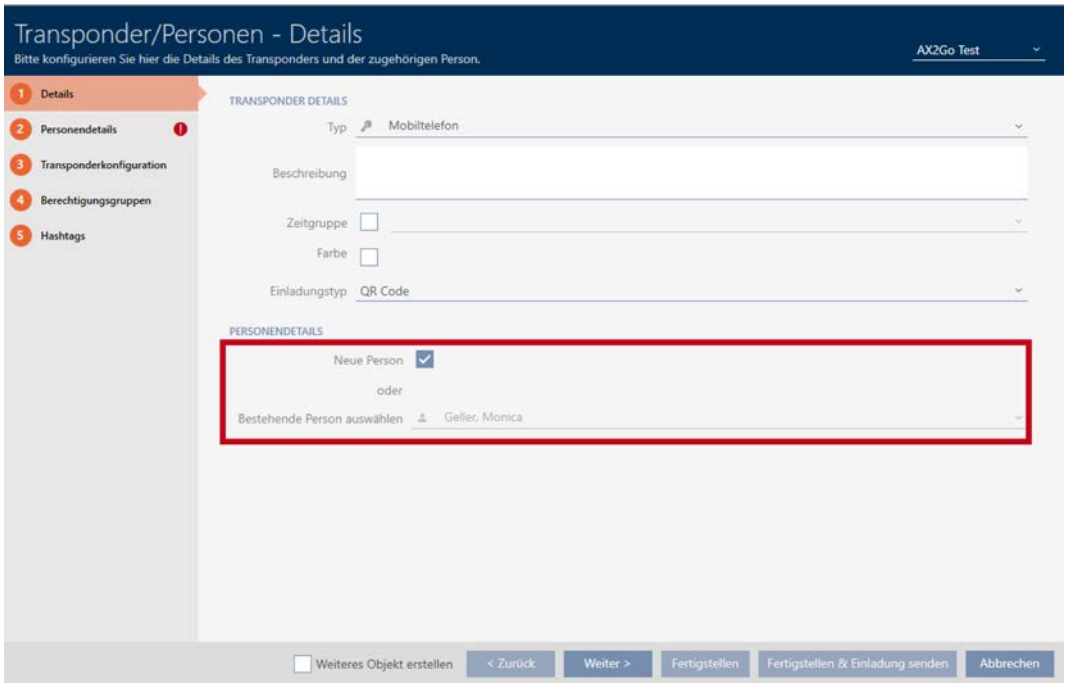
2. Wählen Sie als Transpondertyp "Mobiltelefon" aus



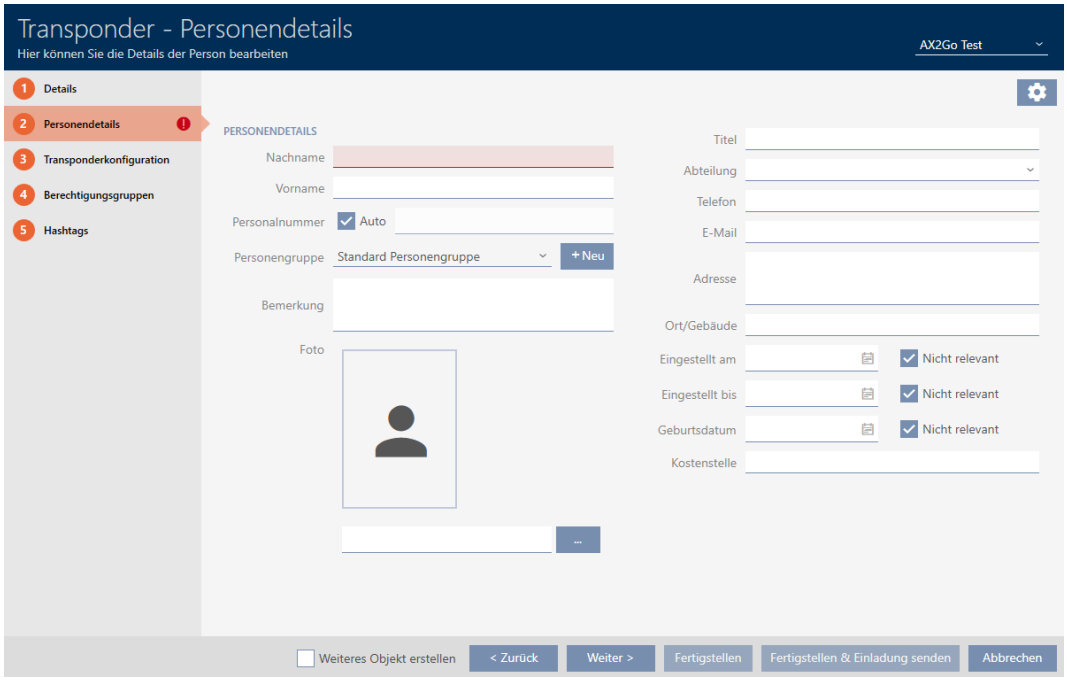
3. Wählen Sie bei ▼ **Einladungstyp** Ihre gewünschte Option aus.
   Sie können hier zwischen "E-Mail", "QR Code" und SMS wählen.



4. Um eine neue Person anzulegen, setzen Sie bitte den Haken bei ☑ Neue Person im Bereich Personendetails.
   Alternativ können Sie auch aus der Liste bereits bestehender Personen wählen, sollten Sie einer Person einen zweiten Schlüssel zuweisen wollen. Klicken Sie anschließend auf Weiter >.



5. Füllen Sie im Reiter Personendetails die rot markierten Pflichtfelder aus. Alle weiteren Angaben sind optional. Klicken Sie anschließend auf Weiter >.

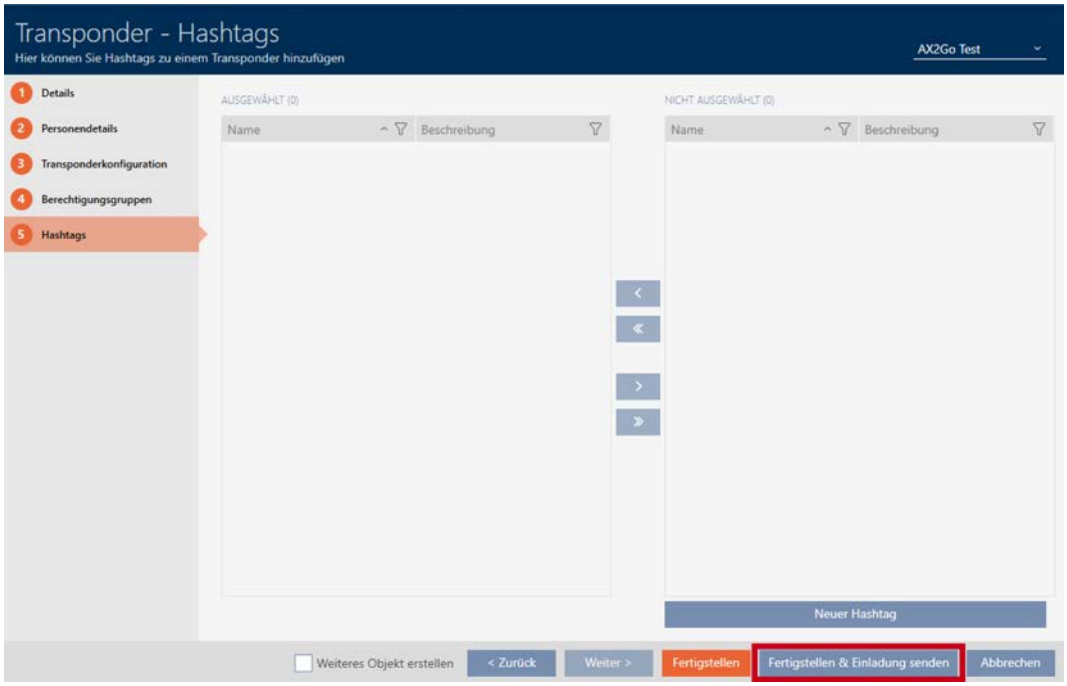


HINWEIS

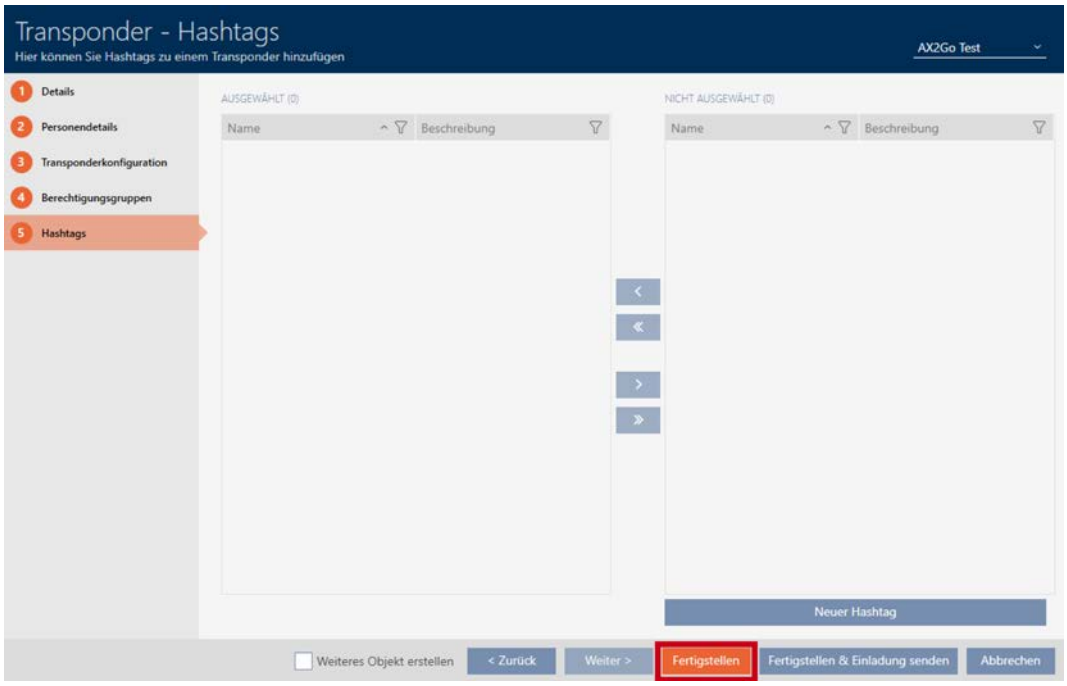
Pflichtangaben je nach Einladungstyp

Beachten Sie, dass je nach Auswahl des Einladungstyps, die auszufüllenden Pflichtfelder variieren.

6. In den Reitern Transponderkonfiguration, Berechtigungsgruppen und Hashtags **können** Sie weitere Einstellungen vornehmen. Weitere Informationen siehe *Transponder und Karten erstellen [▸ 95]*, *Hashtag erstellen [▸ 91]* und *Berechtigungsgruppen [▸ 332]*.
7. Wenn Sie alle für Sie relevanten Einstellungen vorgenommen haben, können Sie die Konfiguration fertigstellen und sofort eine Einladung verschicken. Klicken Sie hierfür auf die Schaltfläche Fertigstellen & Einladung senden.



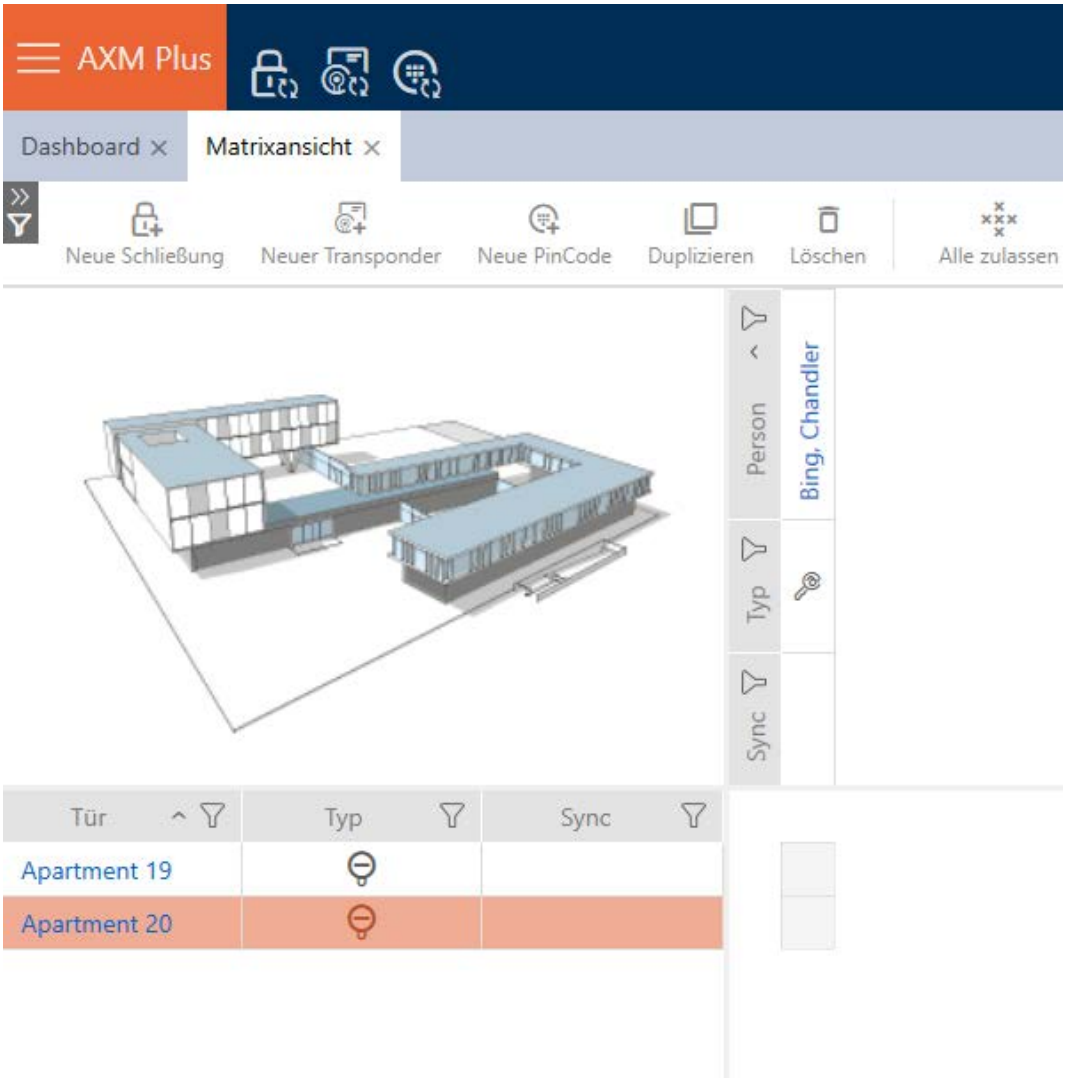
8. **Optional** können Sie die Konfiguration mit der Schaltfläche Fertigstellen fertigstellen und zu einem späteren Zeitpunkt in den Transponder-einstellungen die Einladung verschicken.



9. Klicken Sie auf den jeweiligen Nutzer.
   ↳ Es öffnen sich die Transponder-Details. Es erscheint ebenfalls die Meldung, dass zu diesem Nutzer noch keine Einladung registriert wurde.

10. Klicken Sie auf die Schaltfläche Fertigstellen & Einladung senden um die Einladung zu versenden.
    ↳ ▼ **Einladungstyp** erscheint ein weiteres Fenster, z.B. mit einem QR-Code und einem Link.

↳ Sie haben erfolgreich die Einladung versendet und einen AX2Go-Schlüssel angelegt.



15.19.2 AX2Go-Schlüssel sperren

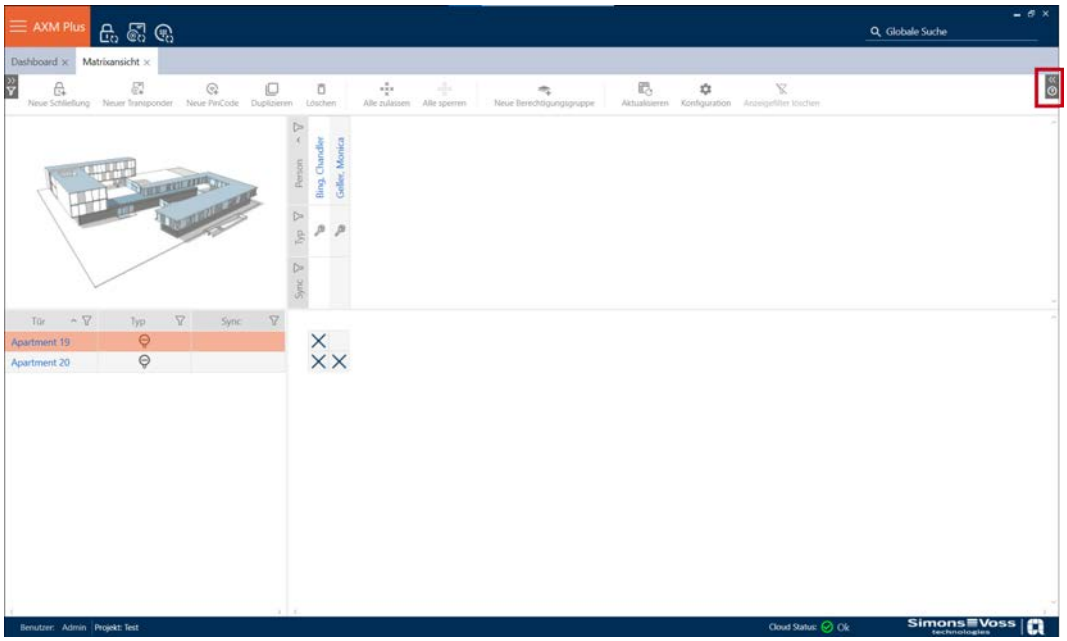
Zugewiesene Schlüssel können vom Schließanlagenverwalter auch wieder entzogen und somit gesperrt werden.

HINWEIS

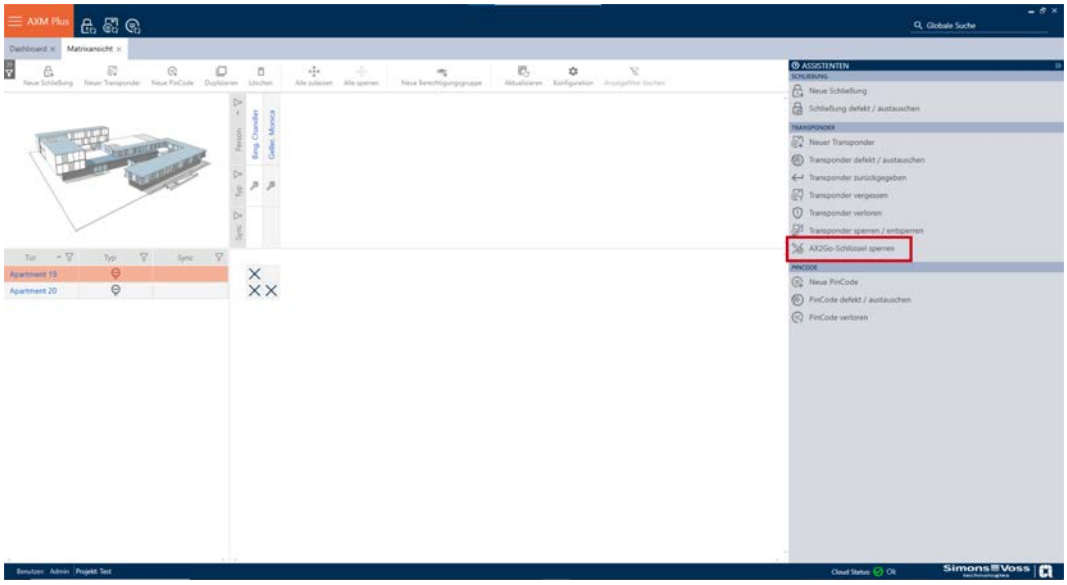
Sperrung kann nicht rückgängig gemacht werden

Wenn Sie einen AX2Go-Schlüssel gesperrt haben, dann können Sie diesen nicht wieder entsperren.

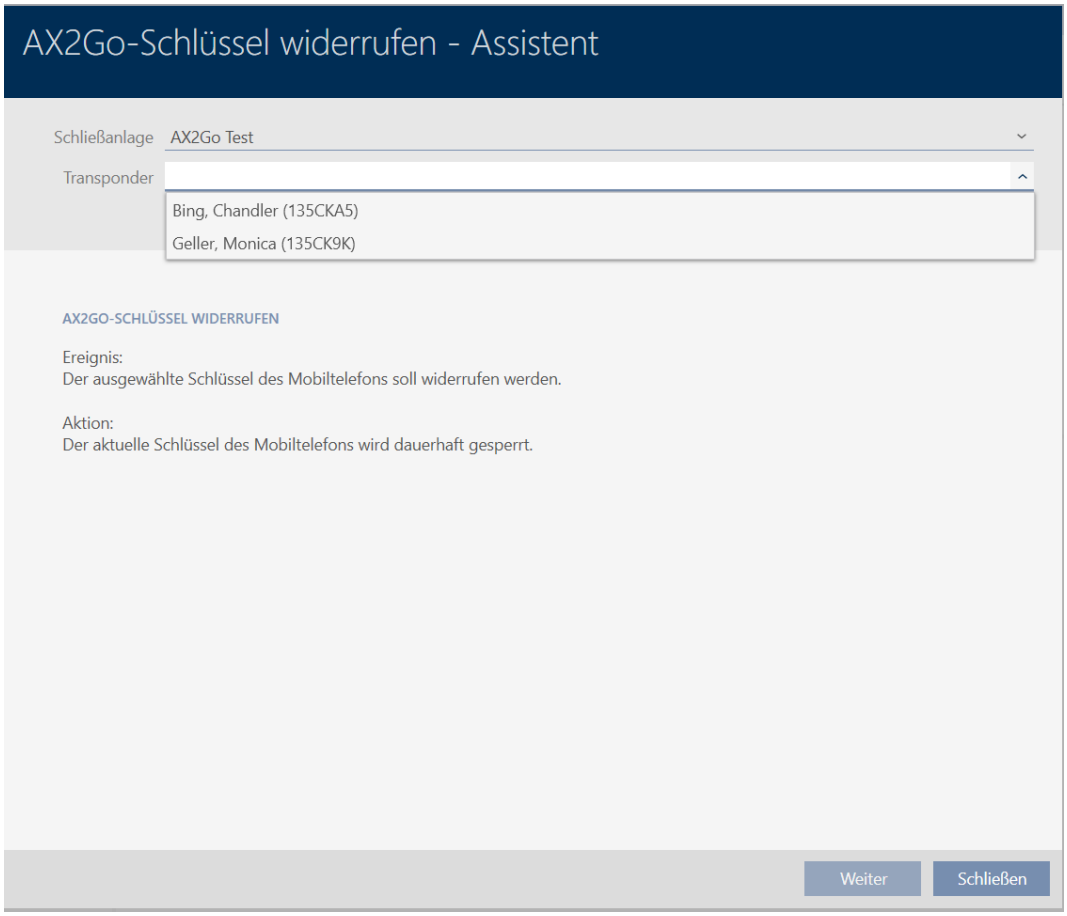
1. Öffnen Sie die Assistenten auf der rechten Seite Ihrer Matrixansicht.



2. Klicken Sie auf den Punkt AX2Go-Schlüssel sperren .

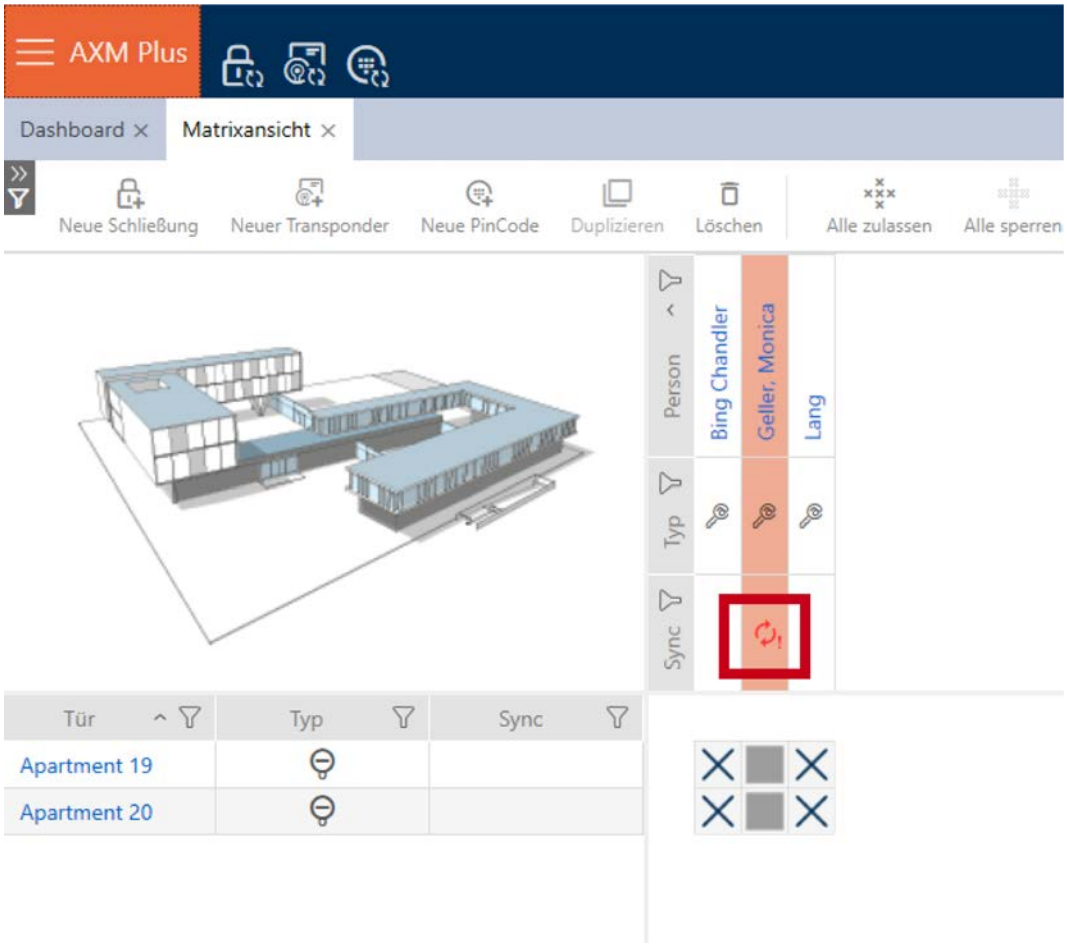


3. Wählen Sie unter Transponder die Person, deren AX2Go-Schlüssel Sie sperren möchten und klicken Sie auf Weiter .



4. Es erscheint ein Fenster, in dem Sie gefragt werden, ob Sie wirklich den Schlüssel sperren möchten. Klicken Sie auf Ja .

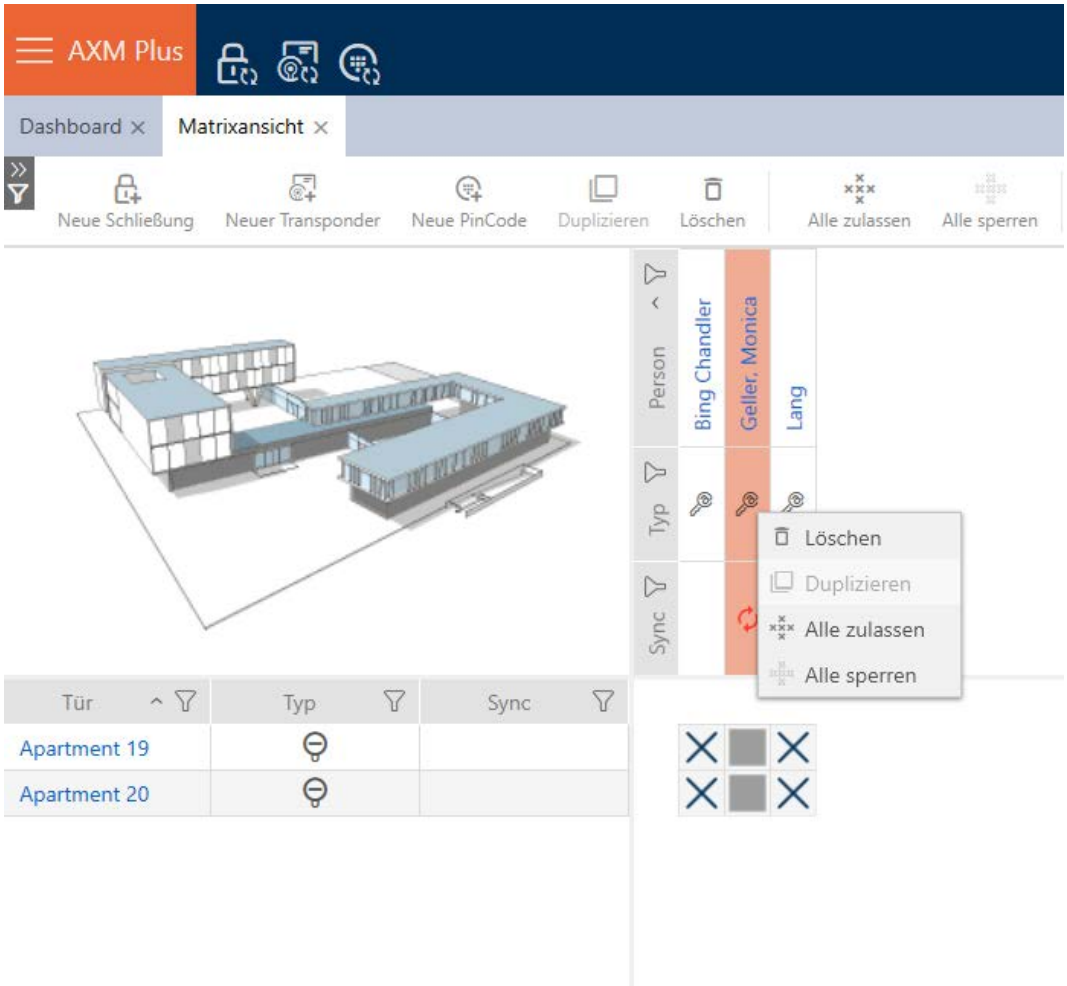
↳ Der von Ihnen ausgewählte AX2Go-Schlüssel wurde erfolgreich gesperrt.



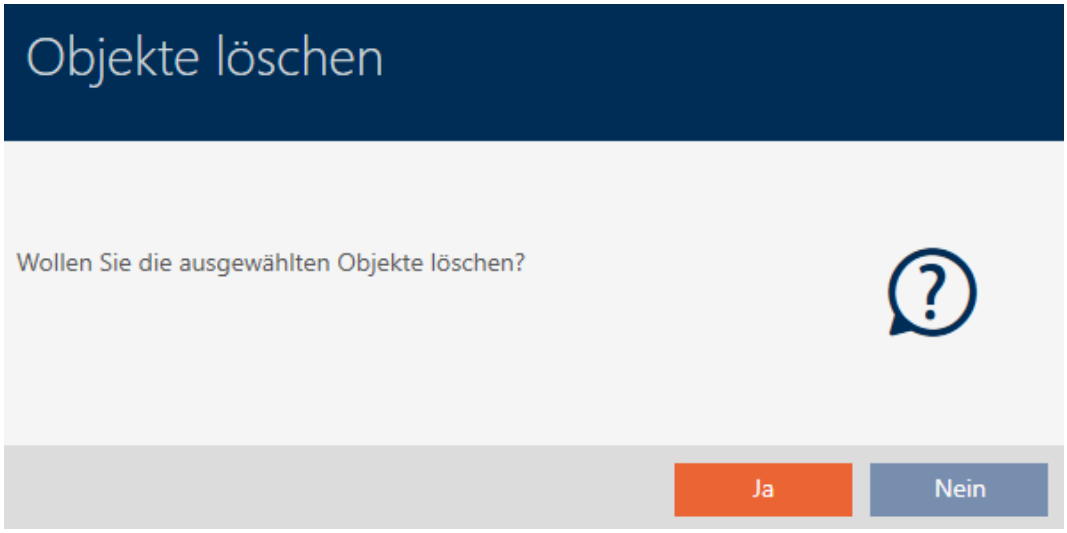
15.19.3 AX2Go-Schlüssel löschen

Nach dem Sperren des Schlüssels, können Sie diesen auch löschen und somit vollständig entfernen. Um den AX2Go-Schlüssel aus der Matrix-Ansicht zu entfernen, gehen Sie bitte wie folgt vor:

1. Machen Sie einen Rechtsklick auf den Schlüssel und klicken Sie auf Löschen.

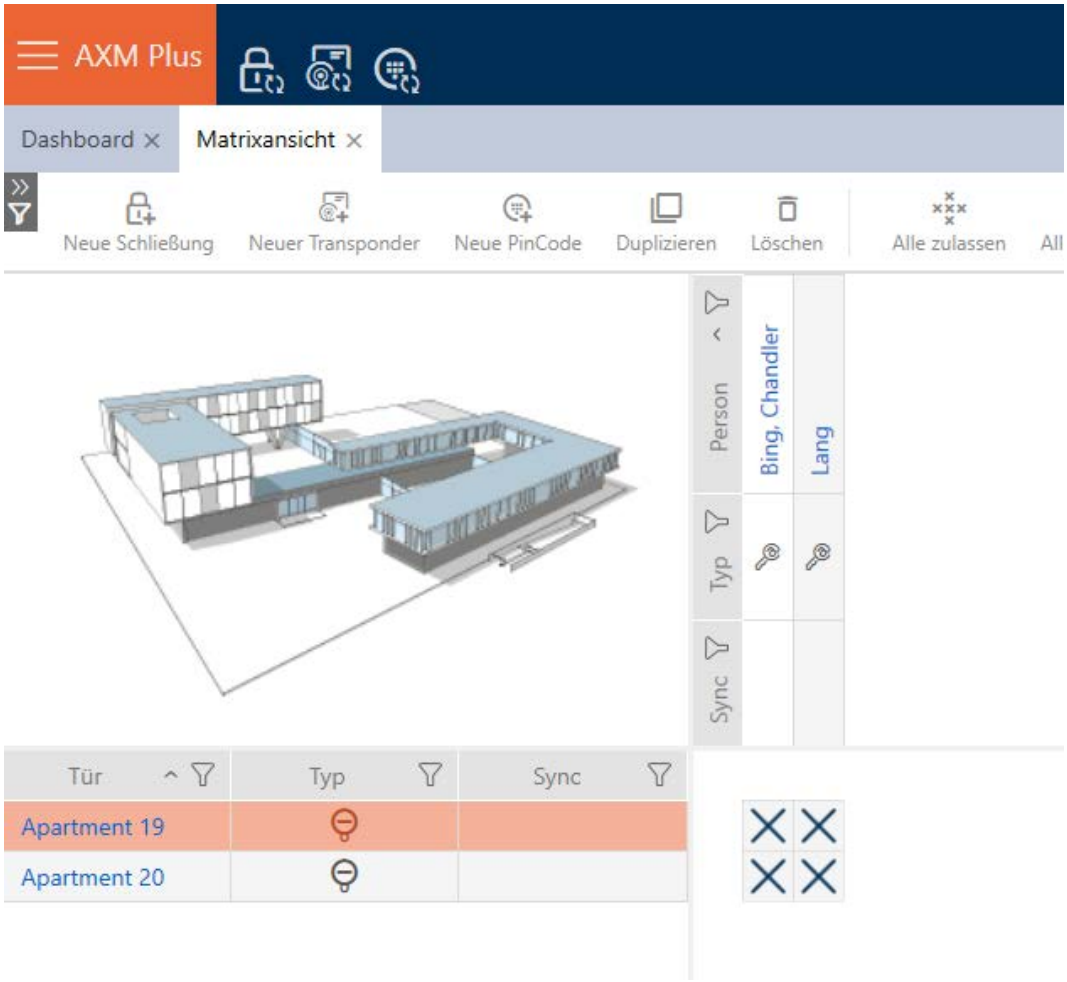


↳ Es öffnet sich eine Maske, in der Sie gefragt werden, ob Sie das Objekt wirklich löschen möchten.



2. Klicken Sie auf die Schaltfläche Ja.

↳ Sie haben den ausgewählten Schlüssel erfolgreich gelöscht. Dieser ist in der Matrixansicht nicht mehr sichtbar.



15.20 PIN-Länge einstellen (PinCode AX)

HINWEIS

Beschreibung nur für PinCode-Tastatur AX gültig

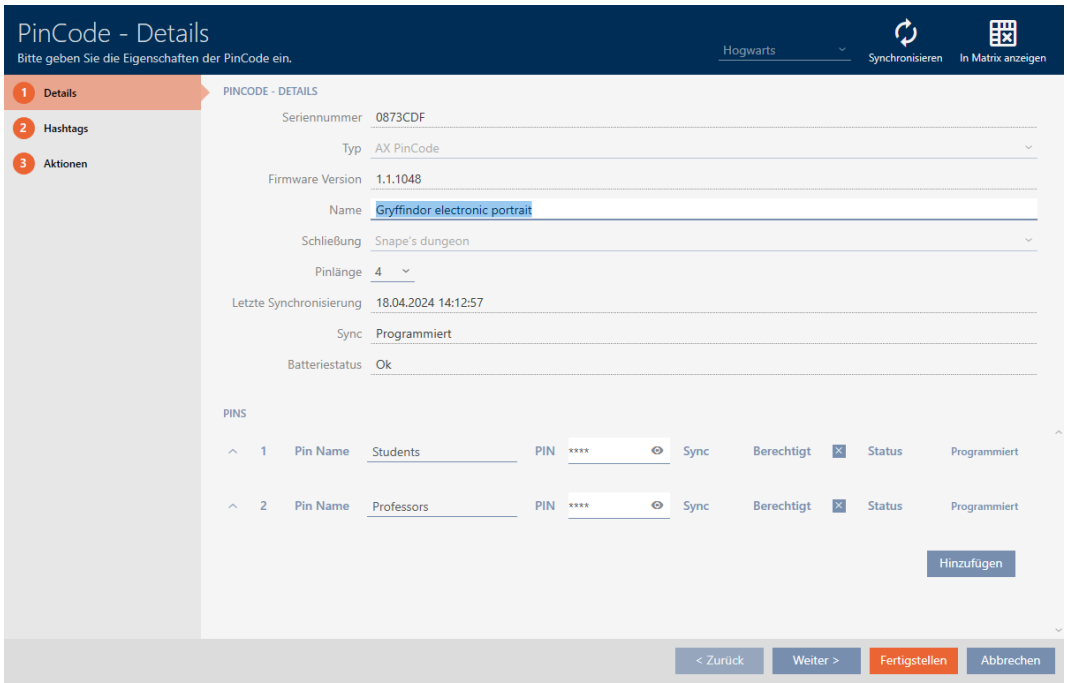
Die hier beschriebene Einstellung steht in Ihrer AXM Plus nur für die PinCode-Tastatur AX zur Verfügung. An der PinCode-Tastatur 3068 verändern Sie diese Einstellung mithilfe der Master-PIN direkt an der PinCode-Tastatur 3068.

Sie stellen die PIN-Länge immer für die gesamte PinCode-Tastatur AX ein, d.h. für alle PINs gleichzeitig. Deshalb müssen Sie im Anschluss jede PIN neu vergeben und die PinCode-Tastatur AX synchronisieren.

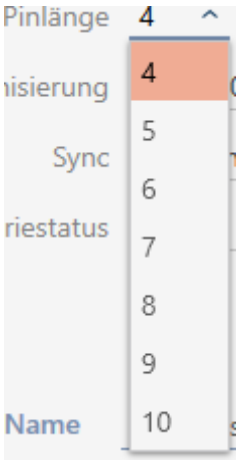
✓ Matrixansicht geöffnet.

✓ PinCode-Tastatur AX erstellt (siehe *PinCode-Tastaturen erstellen* *[▸ 102]*).

1. Klicken Sie auf eine beliebige PIN, um die Details Ihrer PinCode-Tastatur AX zu öffnen.
   ↳ Fenster "PinCode - Details" öffnet sich.



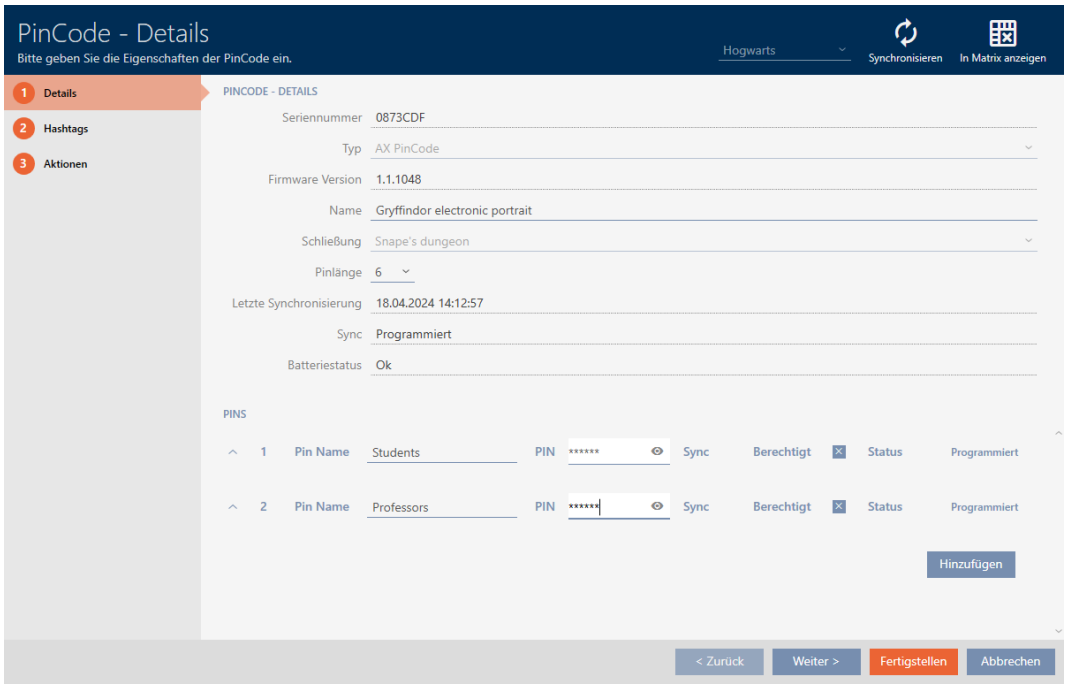
2. Wählen Sie im Dropdown-Menü ▼ **Pinlänge** die neue gewünschte PIN-Länge aus.



↳ Ihre AXM Plus weist sie auf den entstehenden Arbeitsaufwand hin.

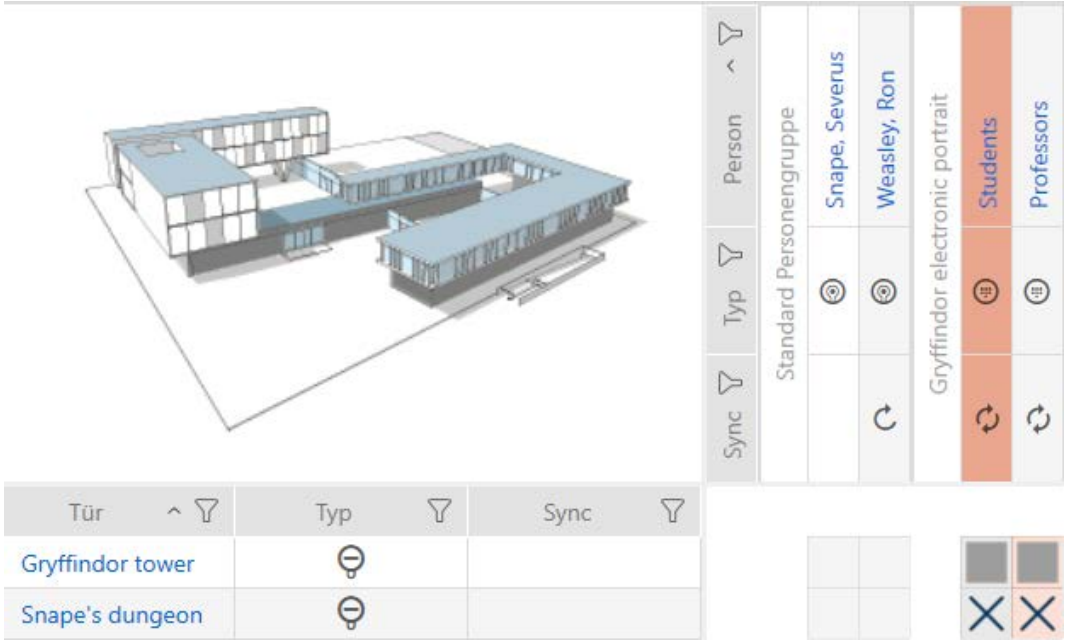
3. Klicken Sie auf die Schaltfläche OK.
   ↳ Alle PINs sind rot und müssen neu vergeben werden.

4. Vergeben Sie die PINs neu.



5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "PinCode - Details" schließt sich.

↳ PIN-Länge und PINs sind geändert und der dadurch entstandene Programmierbedarf wird in der Matrix angezeigt.



15.21 PIN ändern (PinCode AX)

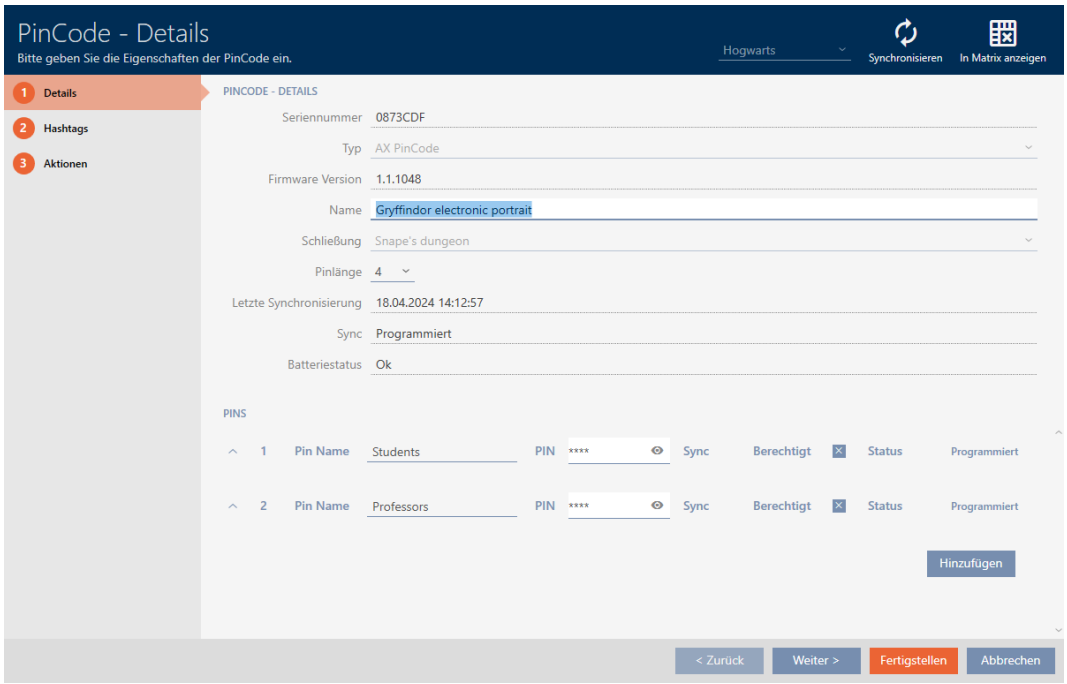
HINWEIS

Beschreibung nur für PinCode-Tastatur AX gültig

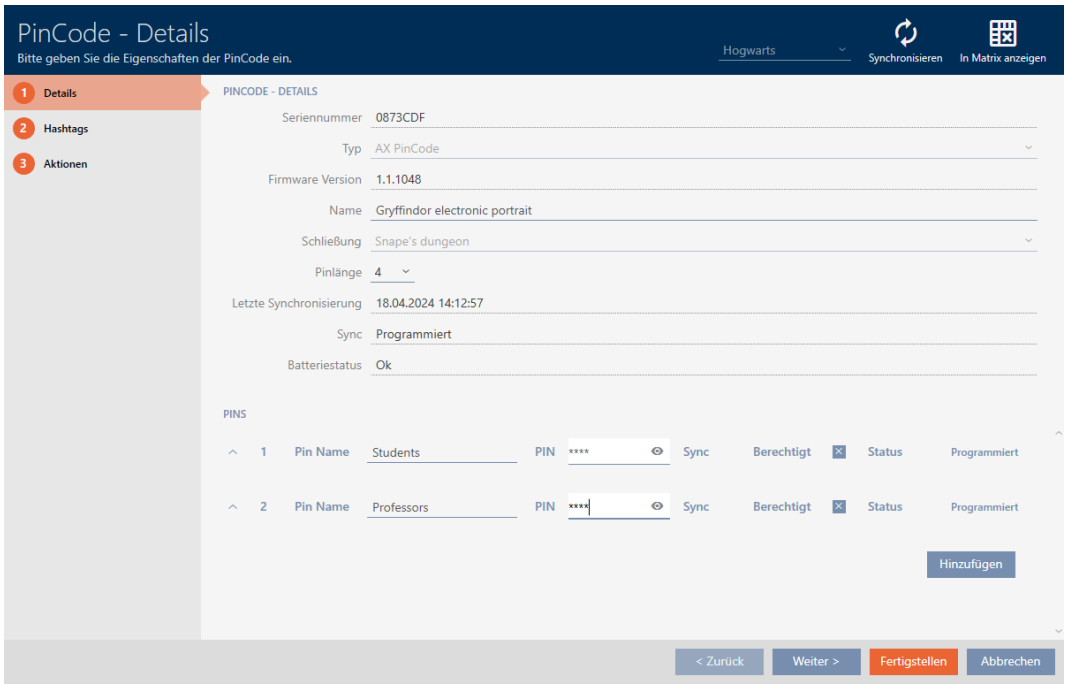
Die hier beschriebene Einstellung steht in Ihrer AXM Plus nur für die PinCode-Tastatur AX zur Verfügung. An der PinCode-Tastatur 3068 verändern Sie diese Einstellung mithilfe der Master-PIN direkt an der PinCode-Tastatur 3068.

- ✓ Matrixansicht geöffnet.
- ✓ PinCode-Tastatur AX erstellt (siehe *PinCode-Tastaturen erstellen* *[▸ 102]*).

1. Klicken Sie auf eine beliebige PIN, um die Details Ihrer PinCode-Tastatur AX zu öffnen.
   ↳ Fenster "PinCode - Details" öffnet sich.

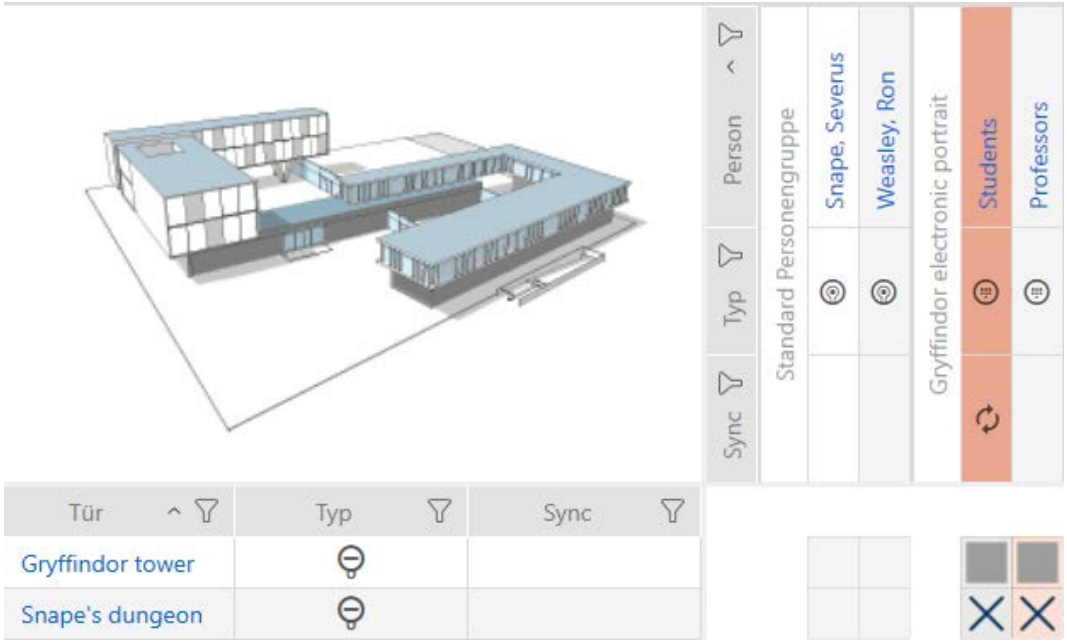


2. Geben Sie im entsprechenden Feld *Pin Name* die neue PIN ein.



3. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ PIN ist geändert und der dadurch entstandene Programmierbedarf wird in der Matrix angezeigt.



16. Türen und Schließungen

Alle Änderungen, die Sie an der Schließanlage vornehmen, werden erst mit der Synchronisation wirksam (siehe *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).

16.1 Schließung erstellen

Schließungen können je nach Art der Schließung:

- Mit einem Identmedium eingekuppelt werden. Der Nutzer kann dann mit der Schließung die Tür öffnen (Zylinder, SmartHandle).
- Mit einem Identmedium entriegelt werden, d.h. der Riegel fährt ohne Zutun des Nutzers ein. Der Nutzer kann dann die Tür öffnen (SmartLocker).
- Mit einem Identmedium geschaltet werden. Der Schaltkontakt kann dann eine Tür öffnen (SmartRelais).

Weitere Informationen zum Thema siehe *"Einkuppeln", "Öffnen", "Verriegeln" usw. [▸ 544]*.

Im Rahmen der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) empfiehlt SimonsVoss, dass Sie zuerst organisatorische Vorarbeiten erledigen:

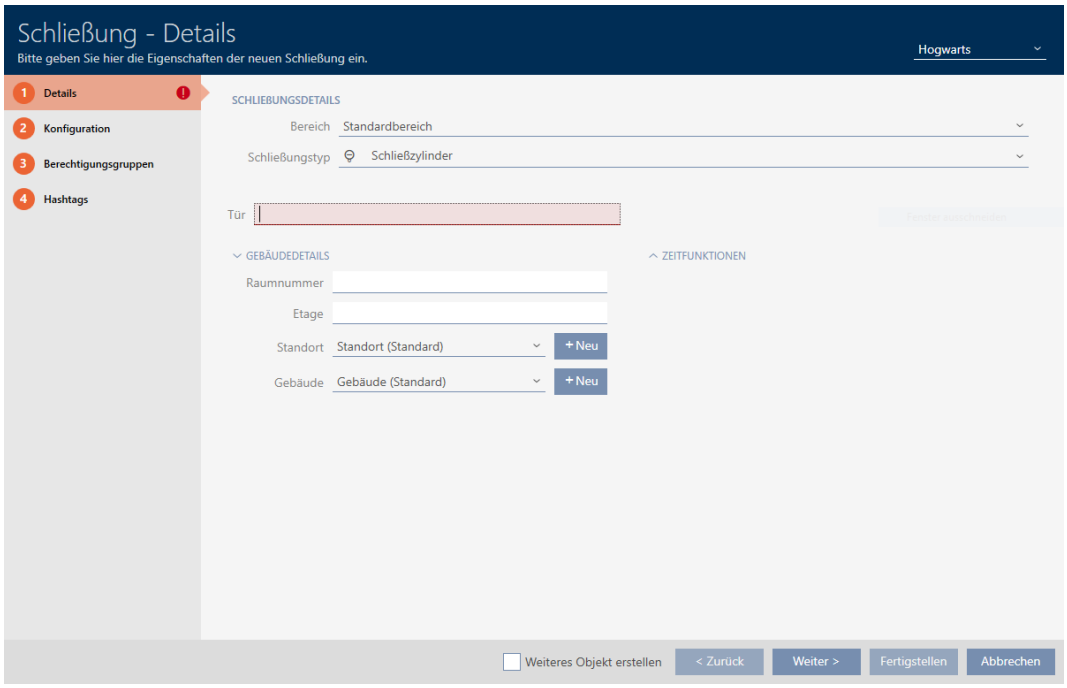
- *Berechtigungsgruppen [▸ 332]* (Hintergrundinformationen siehe *Berechtigungsgruppen [▸ 564]*)
- *Bereich erstellen [▸ 89]* (Hintergrundinformationen siehe *Bereiche [▸ 569]*)
- *Zeitplan erstellen [▸ 58]* bzw. *Zeitgruppe erstellen [▸ 61]* (Hintergrundinformationen siehe *Zeitgruppen und Zeitpläne [▸ 548]*)
- *Zeitumschaltung erstellen [▸ 71]* (Hintergrundinformationen siehe *Zeitumschaltungen [▸ 552]*)
- *Standort erstellen [▸ 83]* bzw. *Gebäude erstellen und zu Standort zuweisen [▸ 86]* (Hintergrundinformationen siehe *Gebäude und Standorte [▸ 568]*)
- *Hashtag erstellen [▸ 91]* (Hintergrundinformationen siehe *Hashtags [▸ 570]*)

HINWEIS

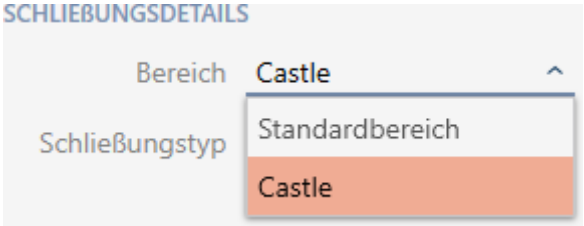
Ausgeblendete Einstellungen

Sobald Sie die Schließung erstellt und auf die Schaltfläche Fertigstellen geklickt haben, kennt die AXM Plus Ihren Schließungstyp. Sie blendet dann alle nicht relevanten Einstellungen aus.

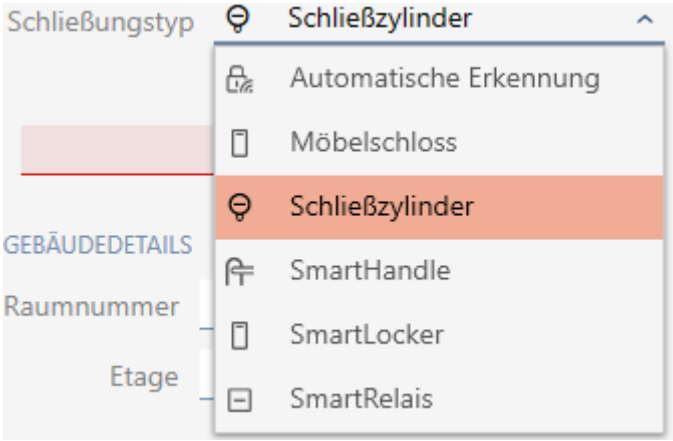
1. Klicken Sie auf die Schaltfläche Neue Schließung.
   ↳ Fenster zum Erstellen einer neuen Schließung öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Bereich** den Bereich aus, zu dem Ihre Schließung gehört.



3. Wählen Sie im Dropdown-Menü ▼ **Schließungstyp** aus, welche Schließung Sie anlegen.



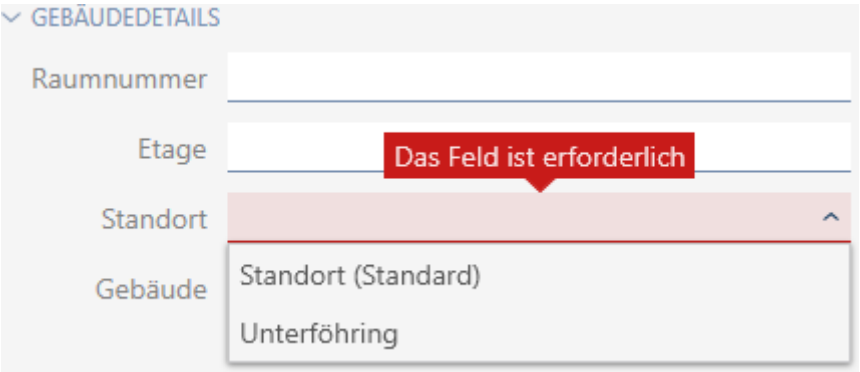
HINWEIS

Schließung automatisch erkennen

Vielleicht wissen Sie noch nicht, welchen Eintrag Sie in der Dropdown-Liste ▼ **Schließungstyp** auswählen sollen. Die AXM Plus stellt Ihnen auch den Eintrag "Automatische Erkennung" zur Verfügung.

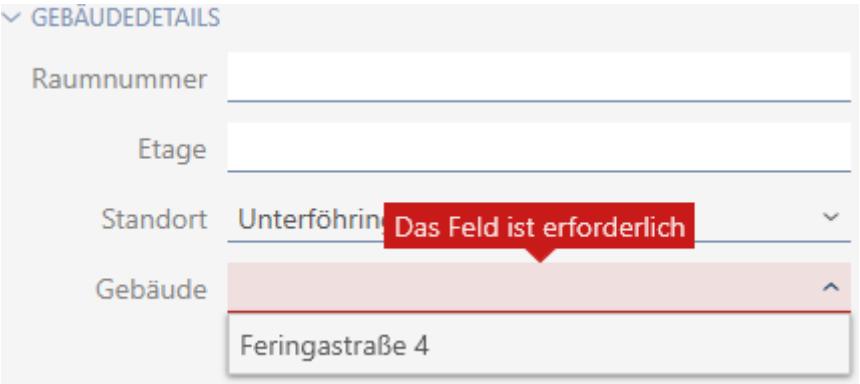
Erst dann, wenn Sie die Schließung tatsächlich programmieren, speichert die AXM Plus den erkannten Schließungstyp. In diesem Moment werden auch die Optionen im Reiter "Konfiguration" passend zum Schließungstyp erweitert oder ausgeblendet.

4. Benennen Sie Ihre Schließung im Feld *Tür*.
5. Geben Sie ggfs. im Feld *Raumnummer* die Nummer des Raums ein, in dem Ihre Schließung verbaut wird.
6. Geben Sie ggfs. im Feld *Etage* die Etage ein, in der Ihre Schließung verbaut wird.
7. Wählen Sie im Dropdown-Menü ▼ **Standort** den Standort aus, an dem Ihre Schließung verbaut wird.



↳ Auswahl im Dropdown-Menü ▼ **Gebäude** wird auf die Gebäude beschränkt, die zum ausgewählten Standort gehören.

8. Wählen Sie im Dropdown-Menü ▼ **Gebäude** das Gebäude aus, in dem Ihre Schließung verbaut wird.



9. Wenn Sie Zeitfunktionen einsetzen wollen: Klappen Sie das Menü "Zeitfunktionen" aus und nehmen Sie die Einstellungen vor (Details siehe *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]* und *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]*).

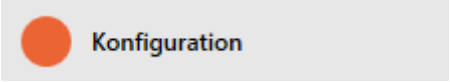
HINWEIS

Feiertagslisten in Schließung und Standorten

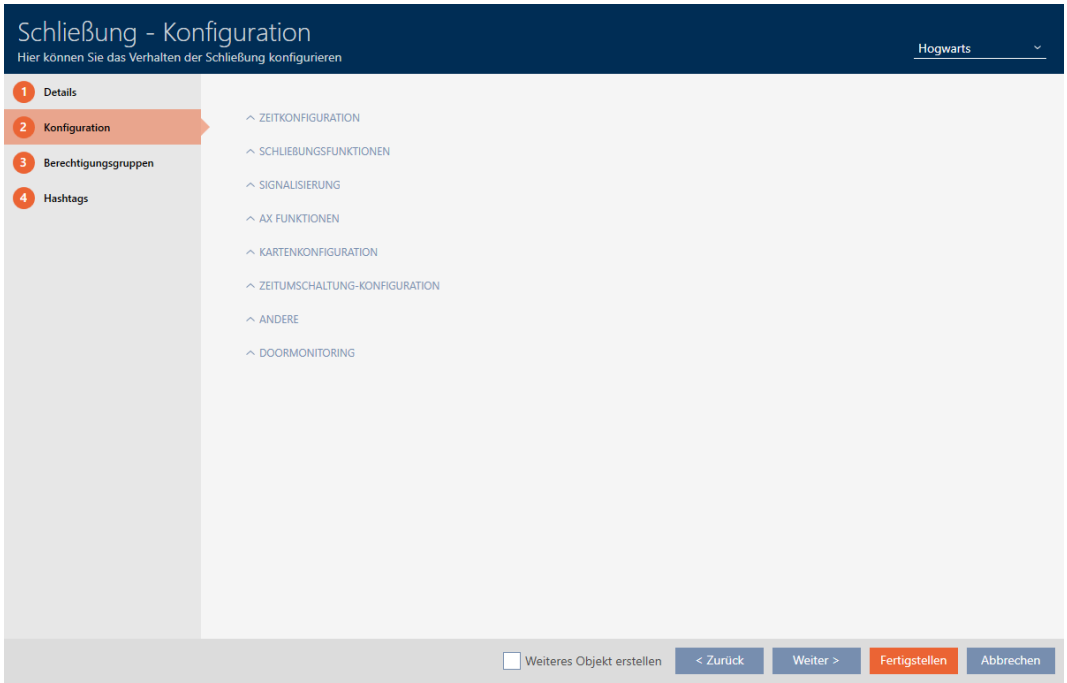
Sie können Feiertagslisten sowohl einer Schließung als auch dem Standort der Schließung zuweisen. In diesem Fall wird die Feiertagsliste in der Schließung verwendet und die Feiertagsliste im Standort ignoriert.

Wenn statt der Schließung dem Standort eine Feiertagsliste zugewiesen ist, dann wird die Feiertagsliste des Standorts für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

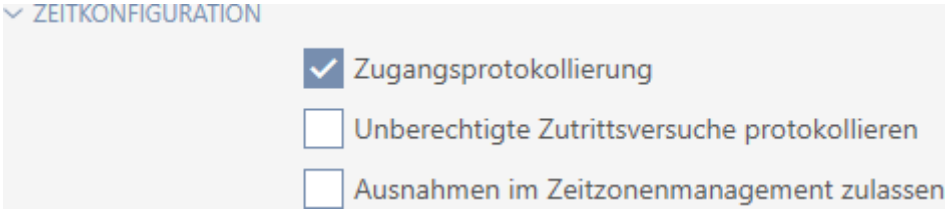
10. Klicken Sie auf den Reiter Konfiguration.



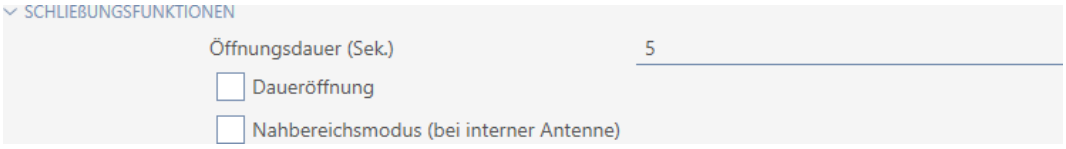
↳ Fenster wechselt zum Reiter "Konfiguration".



11. Wenn Sie Zutrittsversuche protokollieren wollen: Klappen Sie das Menü "Zeitkonfiguration" aus und nehmen Sie die Einstellungen vor (siehe *Zugänge durch Schließung protokollieren lassen (Zutrittsliste) [▸ 293]*).



12. Wenn Sie die Öffnungsdauer ändern oder den Nahbereichsmodus verwenden wollen: Klappen Sie das Menü "Schließungsfunktionen" aus und nehmen Sie die Einstellungen vor (siehe *Schließung länger, kürzer oder dauerhaft öffnen lassen [▸ 295]* und *Lesereichweite der Schließung begrenzen (Nahbereichsmodus) [▸ 297]*).

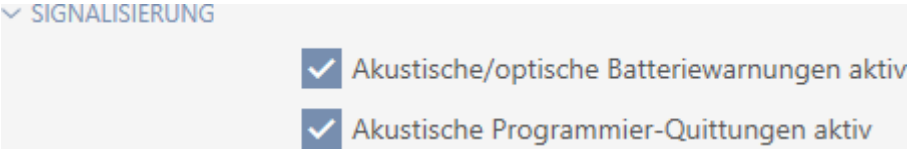


HINWEIS

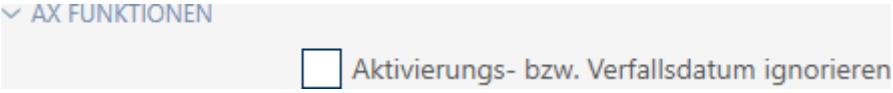
Tastersteuerung nicht einstellbar

Manche Schließzylinder sind mit einem Taster auf dem Innenknauf ausgestattet (Option .TS). Wenn Ihre AXM Plus einen solchen Schließzylinder erkennt, dann wird die Checkbox ☑ Tastersteuerung angezeigt. Diese ist aber nicht einstellbar, d.h. Sie können die Taster nicht deaktivieren.

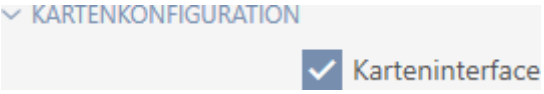
13. Wenn Sie die Signalisierung von Batteriewarnungen oder Programmierquittungen ändern wollen: Klappen Sie das Menü "Signalisierung" aus und nehmen Sie die Einstellungen vor (siehe *Schließung stummschalten (für Batteriewarnungen und Programmierungen) [▸ 298]*).



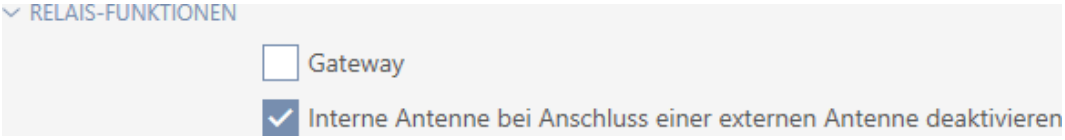
14. Wenn Sie das Aktivierungszeitfenster ignorieren wollen (siehe Aktivierungsdatum / Verfallsdatum): Klappen Sie das Menü "AX Funktionen" aus und nehmen Sie die Einstellungen vor (siehe *Aktivierungs- und Verfallsdatum von Identmedien ignorieren [▸ 302]*).



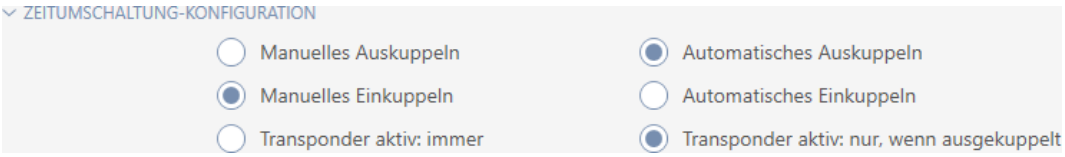
15. Wenn Sie für die Schließung den Kartenleser aktivieren/deaktivieren wollen: Klappen Sie das Menü "Kartenkonfiguration" aus und nehmen Sie die Einstellungen vor (siehe *Kartenleser aktivieren und deaktivieren [▸ 300]*).



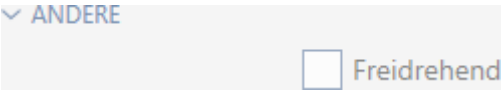
16. Wenn Sie bei einem SmartRelais die interne und externe Antenne zusammen verwenden wollen: Klappen Sie das Menü "Relais-Funktionen" aus und nehmen Sie die Einstellungen vor (siehe *Interne und externe Antenne gleichzeitig verwenden [▸ 312]*).



17. Wenn Sie Ihre Schließung automatisch ein- und auskuppeln wollen: Klappen Sie das Menü "Zeitumschaltung-Konfiguration" aus und nehmen Sie die Einstellungen vor (siehe *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]*).
Die hier festgelegte Einstellung gilt nur für diese eine Schließung, nicht für die gesamte Schließanlage.



18. Wenn Sie einen freidrehenden Digital Cylinder AX verwenden wollen: Klappen Sie das Menü "Andere" aus und aktivieren Sie die Checkbox ☑ Freidrehend.



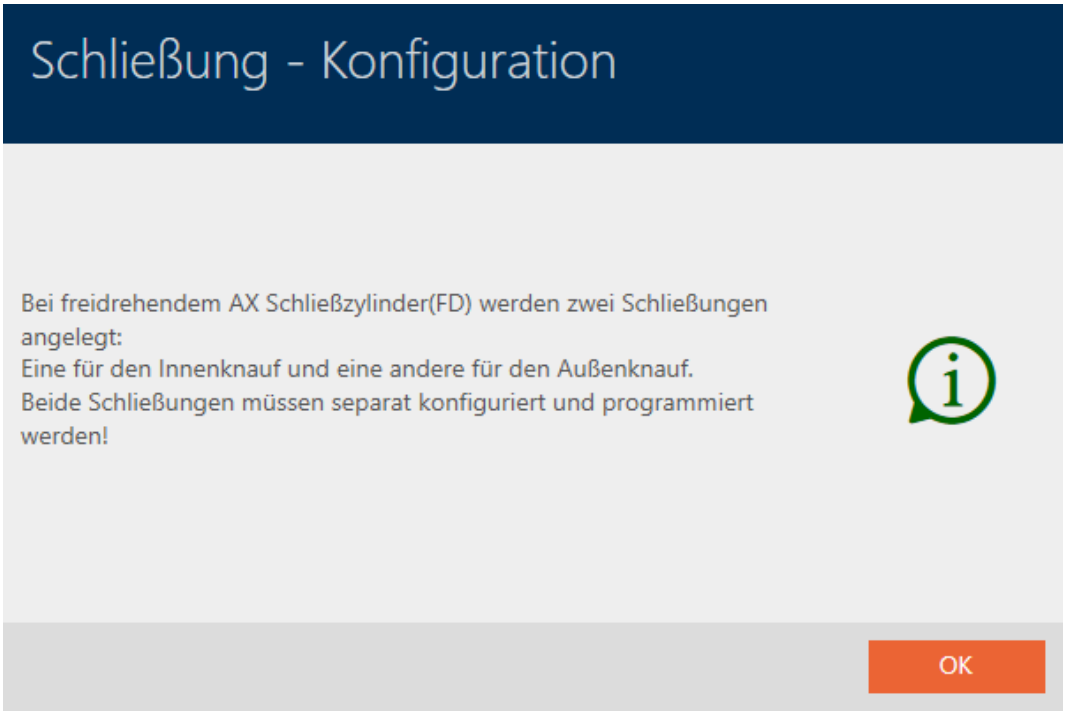
HINWEIS

Freidrehend nur für unprogrammierte Digital Cylinder AX auswählbar

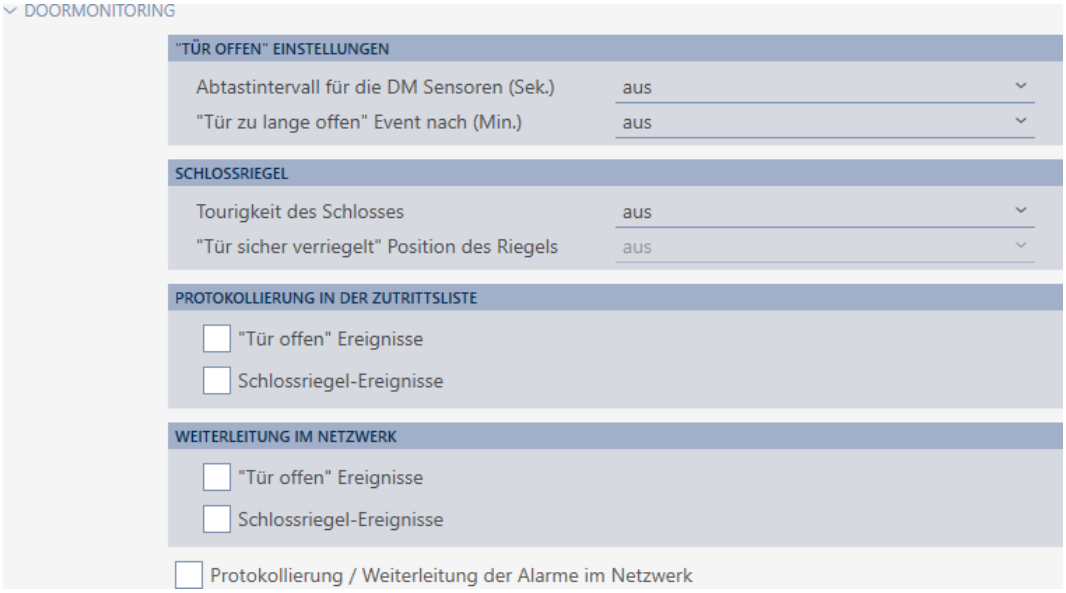
Bereits programmierte Digital Cylinder AX können nicht nachträglich zu freidrehenden Digital Cylinder AX umkonfiguriert werden.

1. Duplizieren Sie den Digital Cylinder AX, um eine unprogrammierte Kopie mit den gleichen Einstellungen zu erhalten.
2. Aktivieren Sie an der Kopie die Checkbox ☑ Freidrehend.
3. Setzen Sie den bisherigen Digital Cylinder AX zurück und synchronisieren Sie die freidrehende Kopie.
4. Löschen Sie anschließend den bisherigen Digital Cylinder AX.

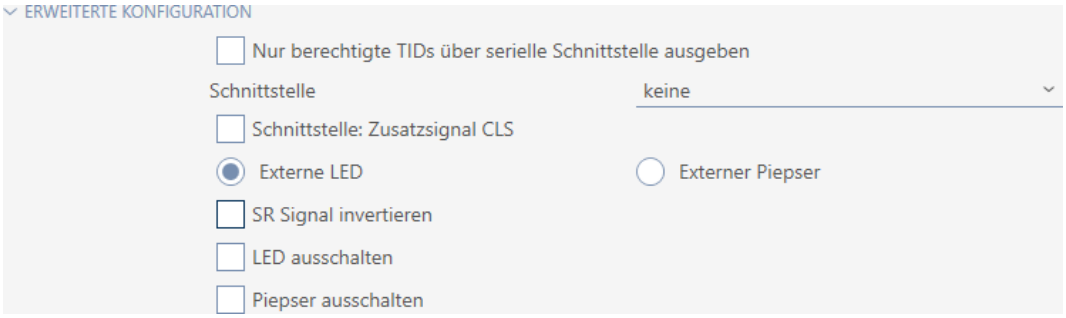
↳ AXM Plus legt einen zweiten Digital Cylinder AX an und aktiviert für beide automatisch die Checkbox ☑ Nahbereichsmodus. Beide Schließungen sind voneinander unabhängig und müssen separat synchronisiert werden.



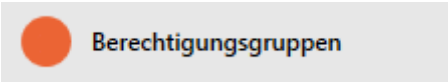
19. Wenn Sie für eine geeignete Schließung die Türüberwachung aktivieren wollen: Klappen Sie das Menü "DoorMonitoring" aus und nehmen Sie die Einstellungen vor (siehe *Türüberwachung (DoorMonitoring) einrichten [▸ 303]*).



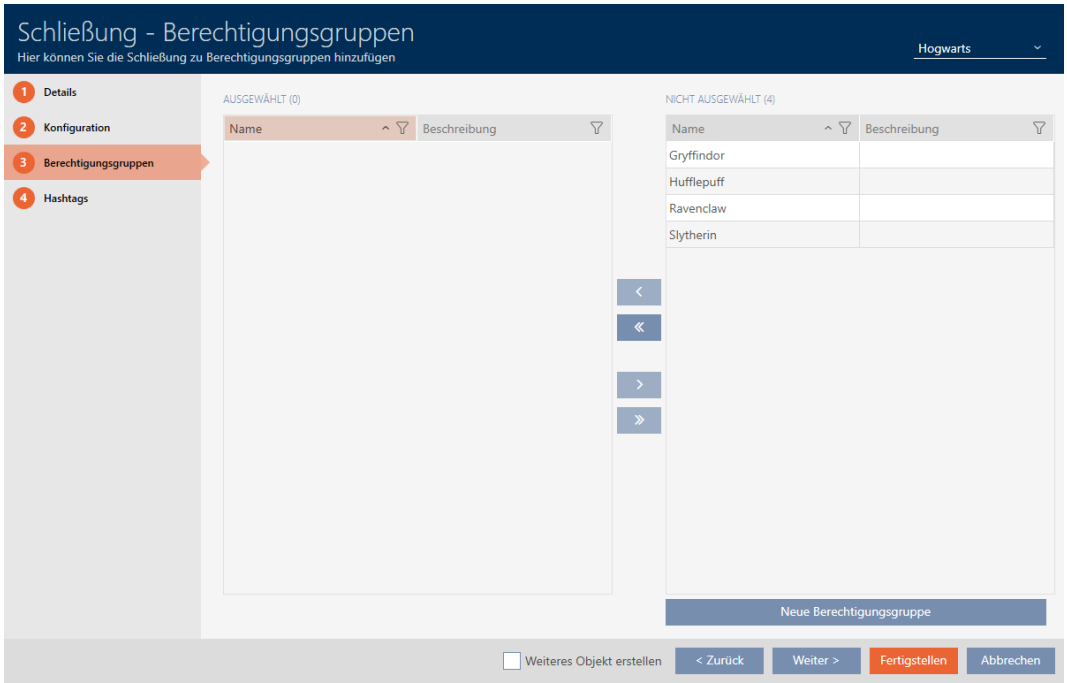
20. Wenn Sie bei einem SmartRelais die Signalisierung ändern wollen oder die serielle Schnittstelle verwenden wollen: Klappen Sie das Menü "Erweiterte Konfiguration" aus und nehmen Sie die Einstellungen vor (siehe *SmartRelais-Einstellungen ändern [▸ 310]*).



21. Klicken Sie auf den Reiter Berechtigungsgruppen.



↳ Fenster wechselt zum Reiter "Berechtigungsgruppen".



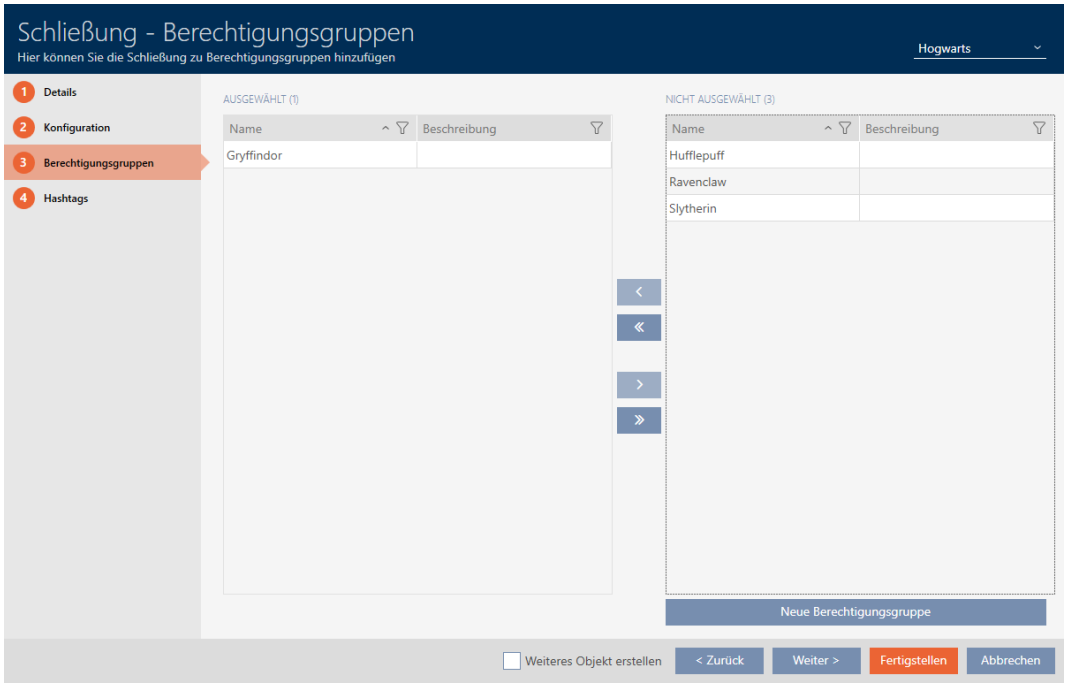
22. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
23. Markieren Sie alle Berechtigungsgruppen, denen Sie Ihre Schließung zuweisen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

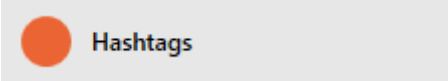
Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

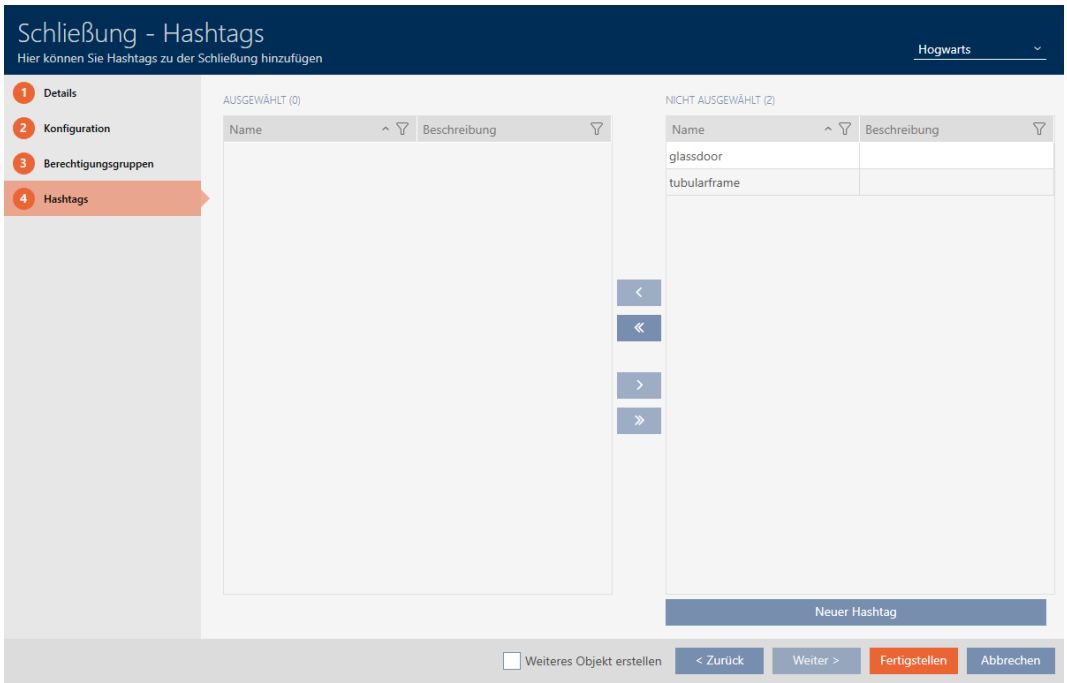
24. Verschieben Sie mit [<] nur die ausgewählten Berechtigungsgruppen oder verschieben Sie mit [«] alle angezeigten Berechtigungsgruppen.
    ↳ Ihre Schließung wird den Berechtigungsgruppen in der linken Spalte hinzugefügt.



25. Klicken Sie auf den Reiter Hashtags.



↳ Fenster wechselt zum Reiter "Hashtags".



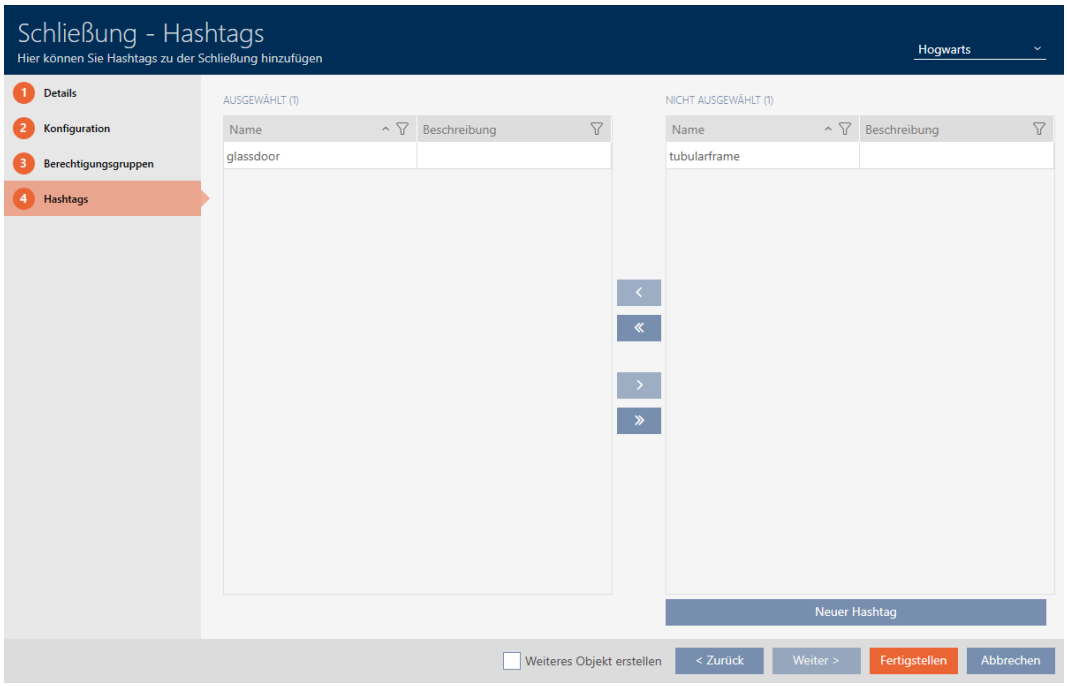
26. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
27. Markieren Sie alle Hashtags, die Sie Ihrer Schließung zuweisen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

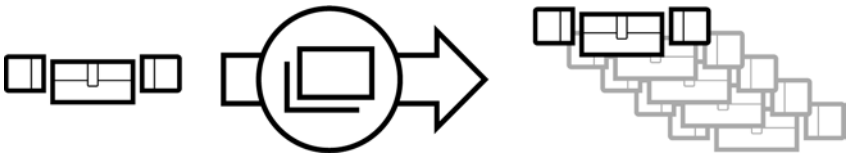
28. Verschieben Sie mit < nur die ausgewählten Hashtags oder verschieben Sie mit « alle angezeigten Hashtags.
    ↳ Die Hashtags in der linken Spalte werden Ihrer Schließung hinzugefügt.



29. Aktivieren Sie die Checkbox ☑ Weiteres Objekt erstellen, um für die nächste zu erstellende Schließung das Fenster mit denselben Einstellungen geöffnet zu lassen.
30. Klicken Sie auf die Schaltfläche Fertigstellen, um die Schließung zu erstellen.
    ↳ Fenster zum Erstellen einer neuen Schließung schließt sich.

↳ Neu erstellte Schließung wird aufgelistet bzw. in der Matrix angezeigt.

16.2 Schließung duplizieren (inkl. Berechtigungen und Einstellungen)



Statt eine Schließung neu zu erstellen können Sie auch einfach eine vorhandene Schließung duplizieren. Die AXM Plus übernimmt dabei auch die Eigenschaften, die in der AXM Plus geändert werden können.

Dupliziert werden:

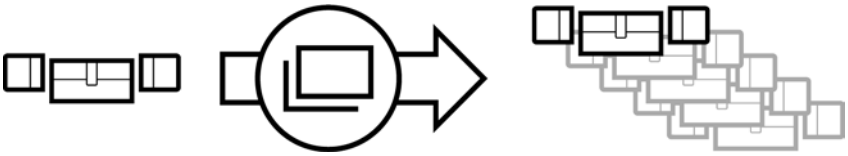
- Gebäudedetails
- Türdetails (außer Türnummer, diese wird automatisch mit dem einstellbaren Kürzel fortgesetzt, siehe auch *Automatische Nummerierung ändern [▸ 463]*)
- Zeitfunktionen
- Konfiguration
- Berechtigungsgruppen
- Hashtags

Nicht dupliziert werden:

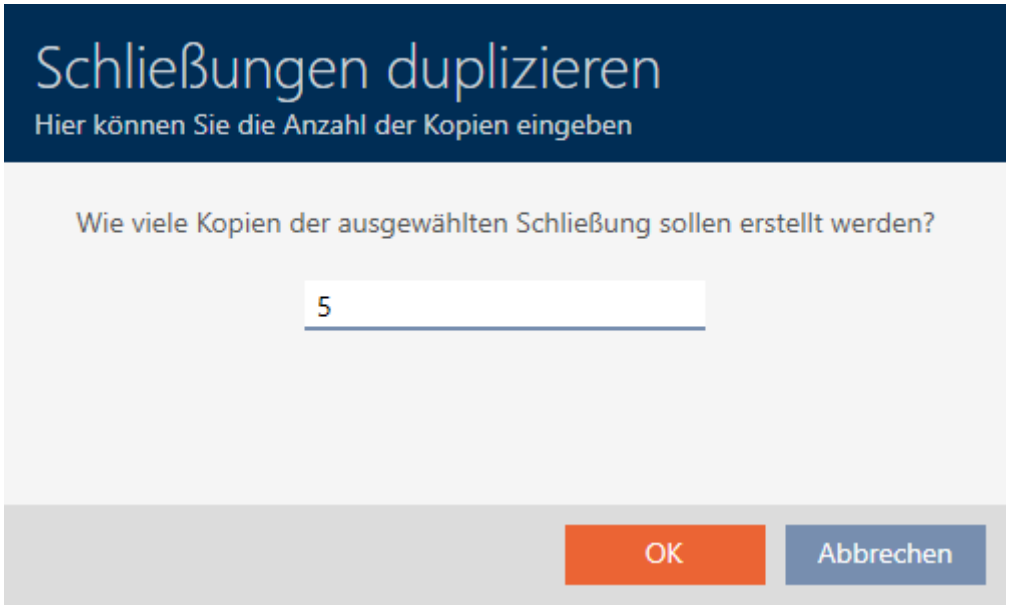
- Eingaben im Tab [Aktionen]
- Informationen, die hardwareseitig gespeichert sind und bei der Synchronisation ausgelesen werden:
  - Seriennummer
  - Firmware Version
  - Batteriestatus
  - Zutrittsliste
  - Zugewiesene PinCode-Tastatur

✓ Schließung vorhanden.

1. Markieren Sie die zu duplizierende Schließung.

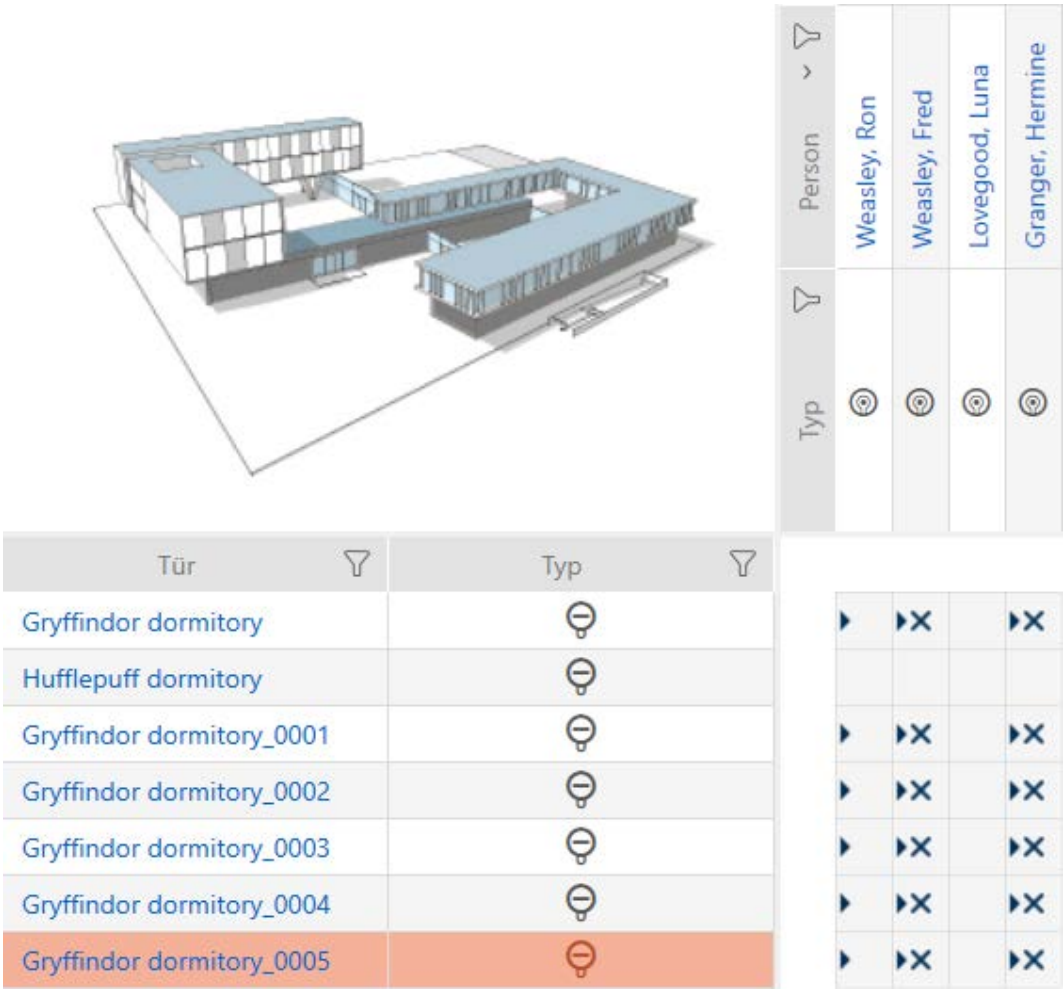


2. Klicken Sie auf die Schaltfläche Duplizieren.
   ↳ Fenster zur Angabe der Kopien öffnet sich.



3. Klicken Sie auf die Schaltfläche OK.

↳ Schließung ist dupliziert.



16.3 Schließung löschen

Sie haben zwei Möglichkeiten, um Schließungen wieder zu löschen:

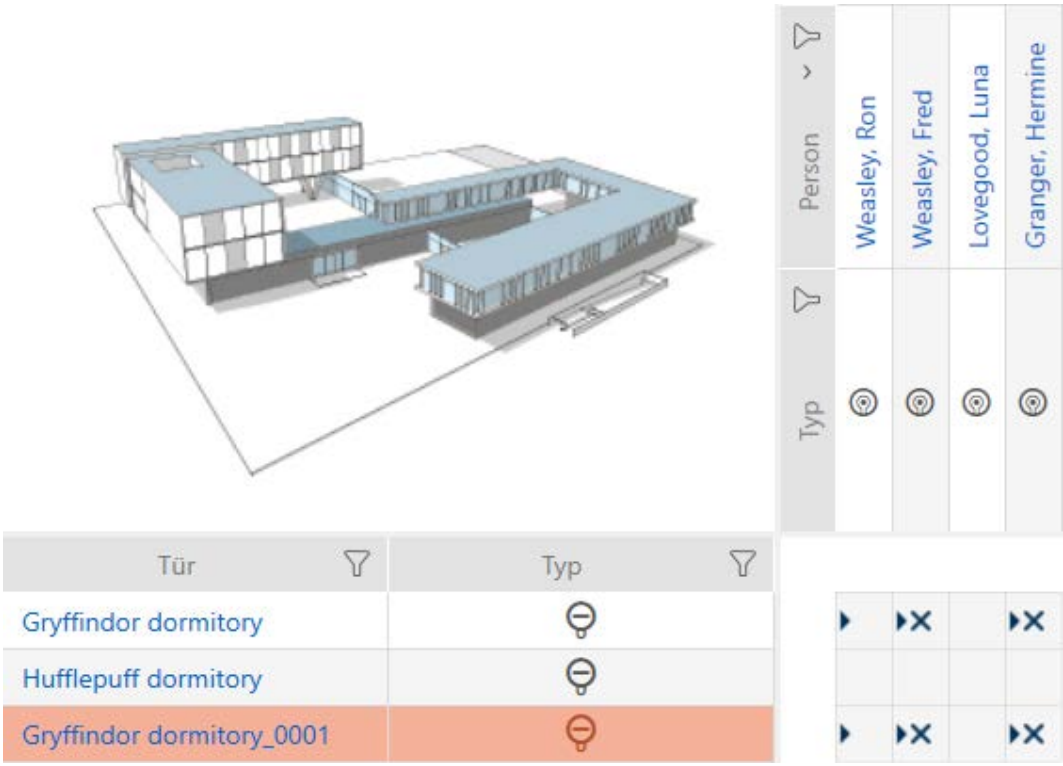
1. Löschen über die Matrixansicht (*Einzelne Schließung über die Matrix löschen [▸ 251]*)
2. Löschen über den Tab für die Schließungen (*Mehrere Schließungen über den Tab löschen [▸ 252]*)

Im Tab können Sie auch mehrere Schließungen gleichzeitig löschen.

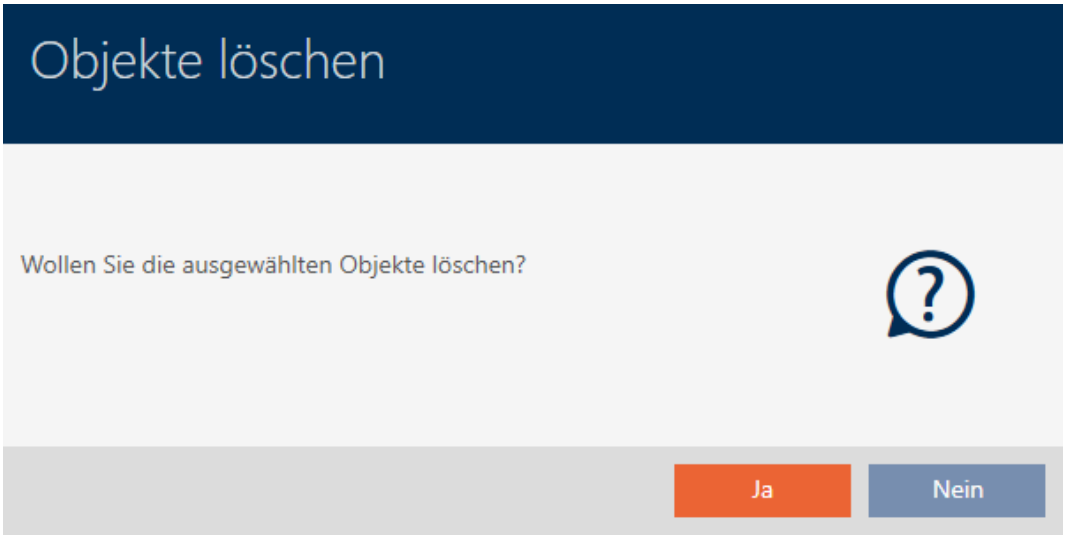
16.3.1 Einzelne Schließung über die Matrix löschen

✓ Matrixansicht geöffnet.

1. Markieren Sie die Schließung, die Sie löschen wollen.

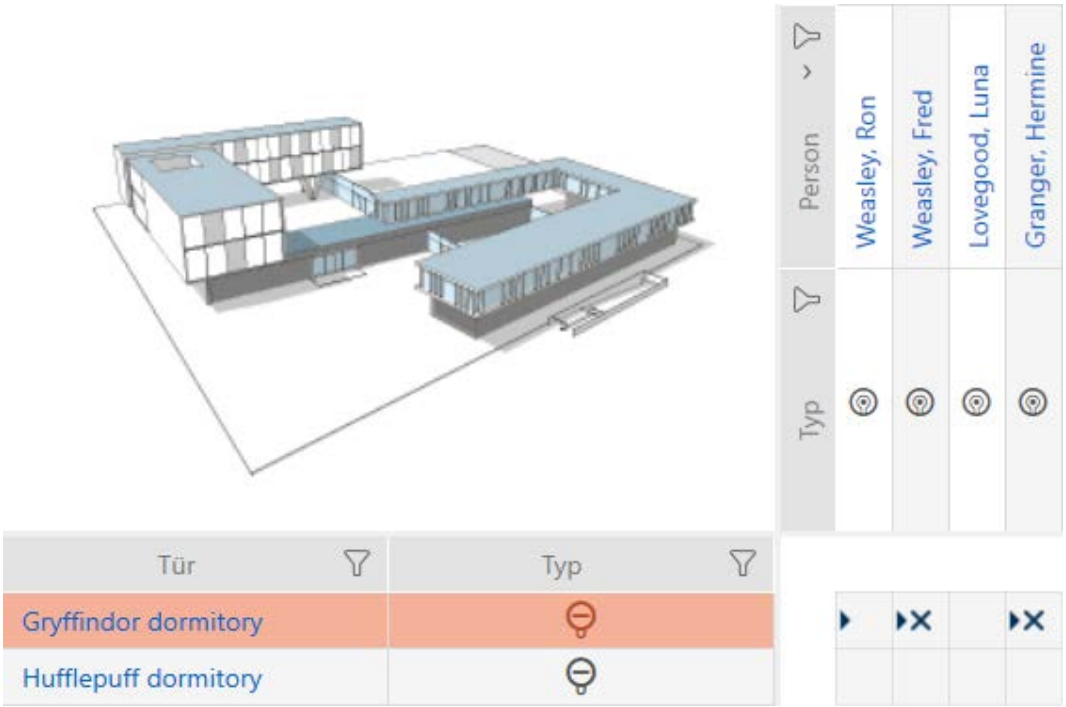


2. Klicken Sie auf die Schaltfläche Löschen 🗑.
   ↳ Rückfrage zum Löschen öffnet sich.



3. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Löschen schließt sich.

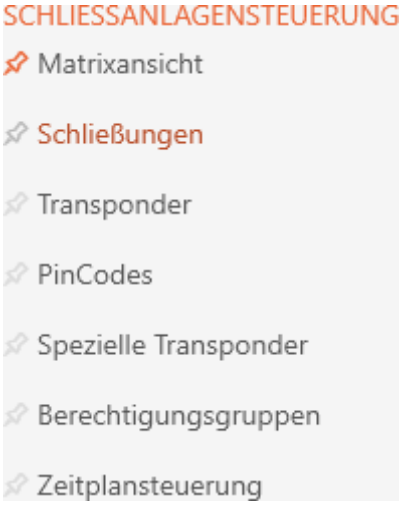
↳ Schließung ist gelöscht.



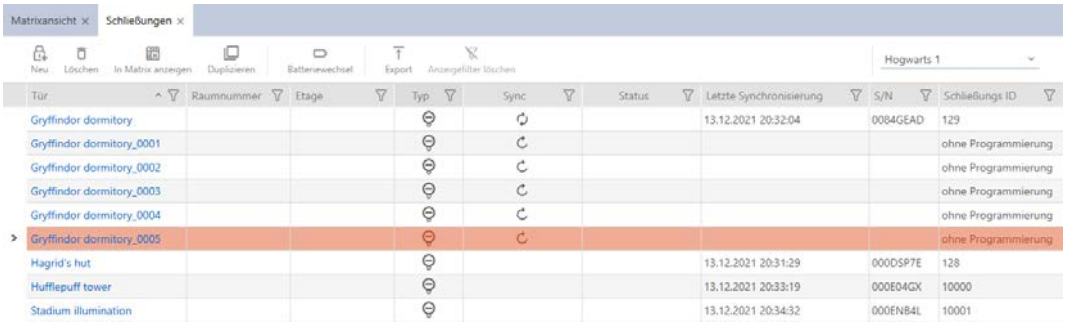
16.3.2 Mehrere Schließungen über den Tab löschen

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Schließungen aus.

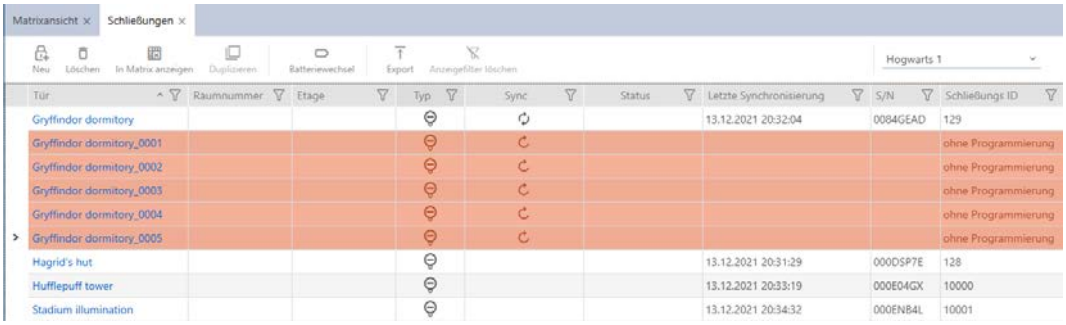


↳ AXM-Leiste klappt zu.
↳ Tab [Schließungen] öffnet sich.



3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

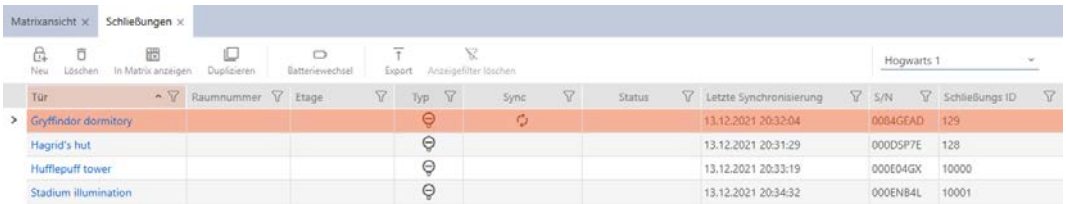
4. Markieren Sie alle Schließungen, die Sie löschen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).



5. Klicken Sie auf die Schaltfläche Löschen 🗑.
   ↳ Rückfrage mit Liste der zu löschenden Schließungen öffnet sich.

6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage mit Liste der zu löschenden Schließungen schließt sich.

↳ Schließungen sind gelöscht.



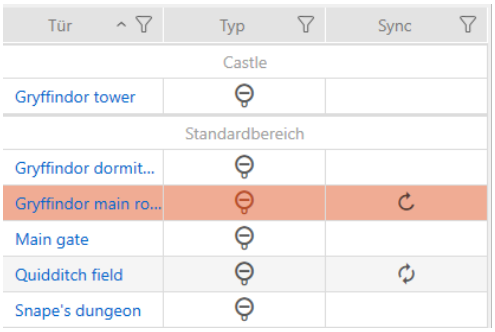
16.4 Schließungstyp nachträglich ändern

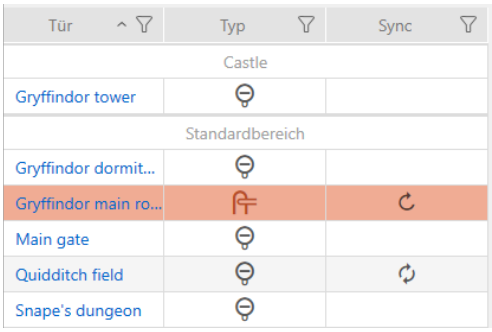
Manchmal stellt sich erst später heraus, dass ein anderer Schließungstyp für einen Einsatzort besser geeignet ist. Denkbar wäre zum Beispiel, dass ein Zylinder aus Komfortgründen durch ein SmartHandle ersetzt werden soll.

Die AXM Plus gibt Ihnen die Möglichkeit, nachträglich einen anderen Schließungstyp auszuwählen. Dabei bleibt die Schließung, insbesondere alle Berechtigungen und kompatible Einstellungen, erhalten.

- Einstellungen, die sowohl beim ursprünglichen als auch beim neuen Schließungstyp vorhanden sind, bleiben erhalten.
- Einstellungen aus dem ursprünglichen Schließungstyp, die es beim neuen Schließungstyp nicht gibt, verfallen.
- Einstellungen, die es nur beim neuen, aber nicht beim ursprünglichen Schließungstyp gibt, werden auf einen Standardwert gesetzt.

	Ursprünglicher Schließungstyp	Neuer Schließungstyp	Ergebnis
Einstellung A (z.B. *Öffnungsdauer (Sek.)*)	Einstellbar	Einstellbar	Wird übernommen
Einstellung B (z.B. ☑ SR Signal invertieren)	Einstellbar	Nicht einstellbar	Verfällt
Einstellung C	Nicht einstellbar	Einstellbar	Wird auf Standardwert gesetzt

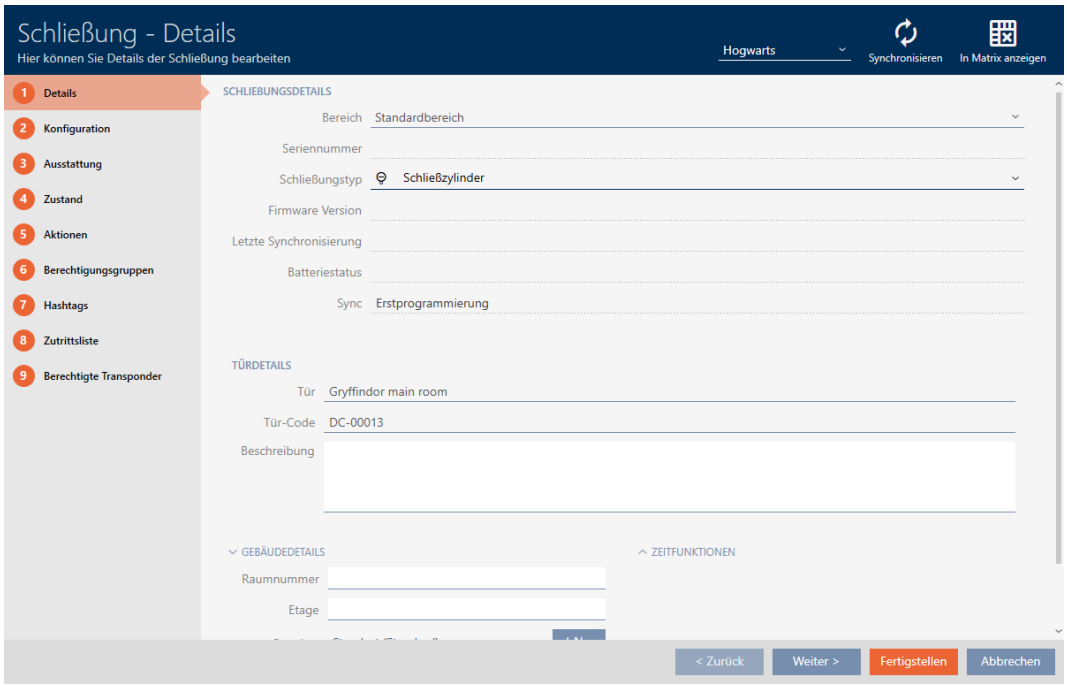




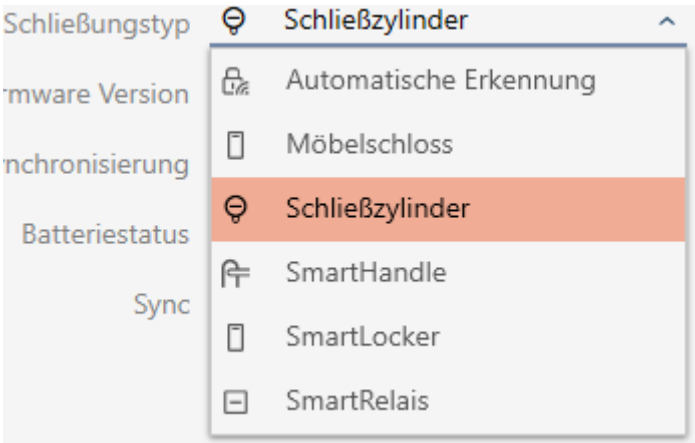
Der Schließungstyp kann nur für unsynchronisierte Schließungen geändert werden.

✓ Schließungsliste oder Matrixansicht geöffnet.
✓ Schließung vorhanden.
✓ Schließung nicht synchronisiert (ggfs. zurücksetzen, siehe *Schließung zurücksetzen [▸ 425]*).

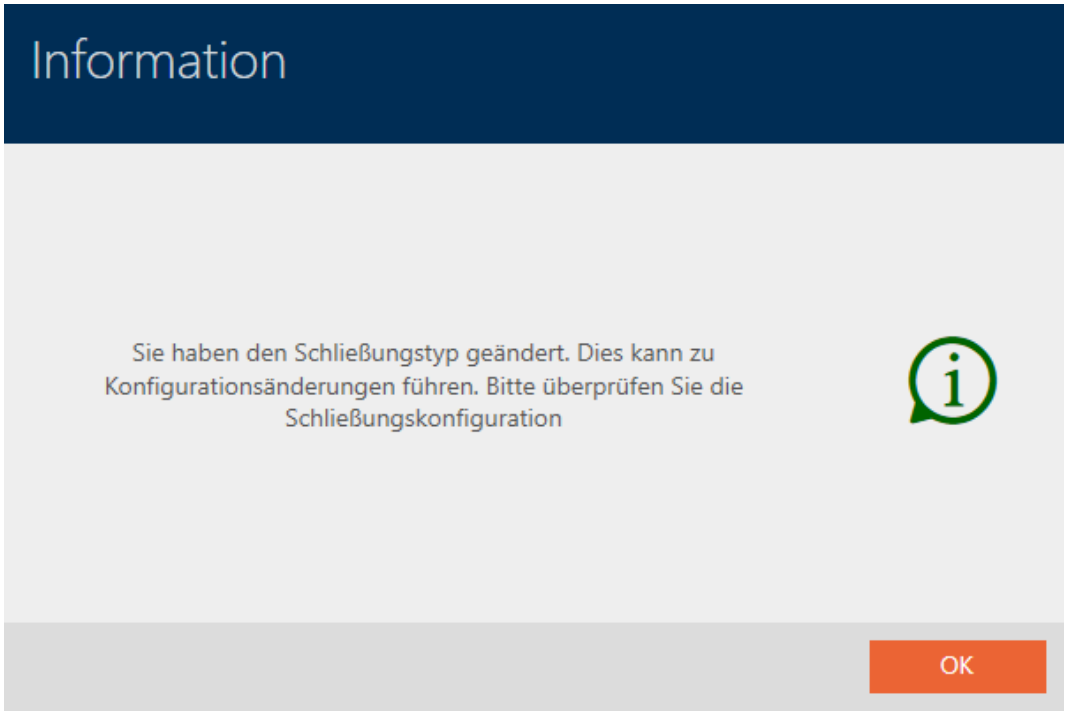
1. Klicken Sie auf die Schließung, deren Typ Sie ändern wollen.
   ↳ Fenster der Schließung öffnet sich.



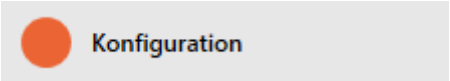
2. Wählen Sie im Dropdown-Menü ▼ **Schließungstyp** den neuen Schließungstyp aus.



   ↳ Warnung über die Konfigurationsänderung öffnet sich.



3. Klicken Sie auf die Schaltfläche OK.
   ↳ Warnung über die Konfigurationsänderung schließt sich.
4. Klicken Sie auf den Reiter Konfiguration.



   ↳ Fenster wechselt zum Reiter "Konfiguration".
5. Prüfen und ändern Sie ggfs. die Konfiguration.
6. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

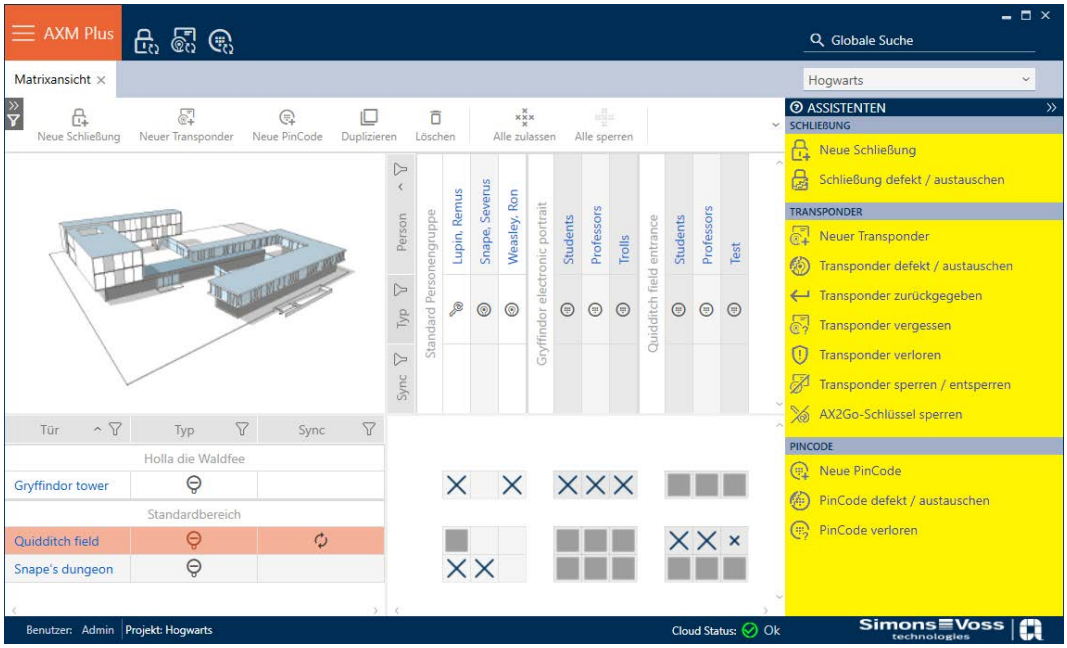
↳ Schließungstyp ist geändert.

16.5 Defekte Schließungen behandeln

Defekte Schließungen sind ärgerlich. Ausfallursachen können dabei sein:

- Softwaredefekte
- Hardwaredefekte

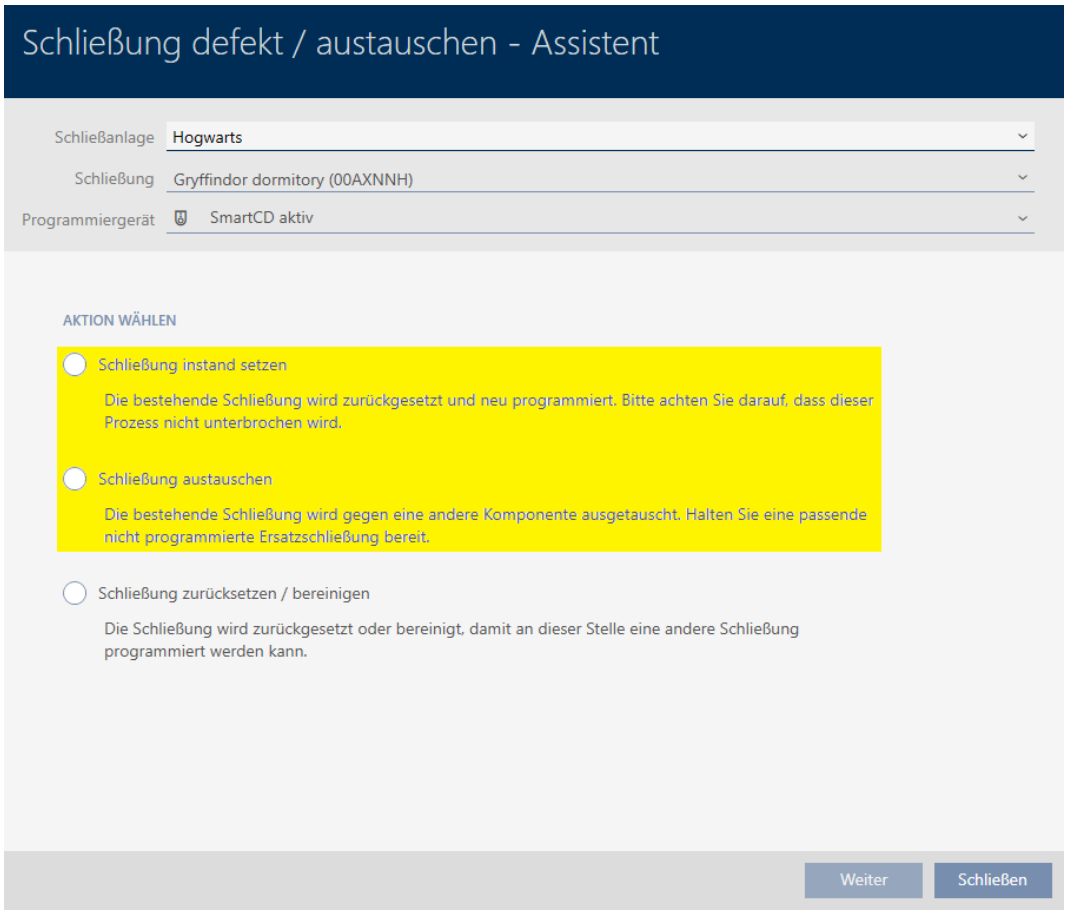
Grundsätzlich lassen sich alle Aktionen über den Assistenten-Bereich auf der rechten Seite erreichen:



Die AXM Plus unterstützt Sie mit einem Assistenten bei der Reparatur defekter Schließungen.

Die folgende Übersicht hilft Ihnen, sich für das richtige Vorgehen zu entscheiden (Informationen über den Zusammenhang zwischen Schließung und intern im Projekt gespeicherter Schließungs-ID (=Lock-ID bzw. LID)): *Identmedien, Schließungen und der Schließplan [▸ 532]*

Schließung wird unmittelbar wieder benötigt:



Geeignet für:

Instandsetzen	Zurücksetzen und austauschen	Löschen und austauschen
Schließungen mit undefiniertem Softwarezustand	▪ Äußerlich beschädigte Schließungen (z.B. verkratzt). ▪ Schließungen, die vorsichtshalber ersetzt werden sollen (z.B. nass geworden).	Endgültig zerstörte Schließungen (z.B. Knauf abgebrochen), für die Ersatz benötigt wird.

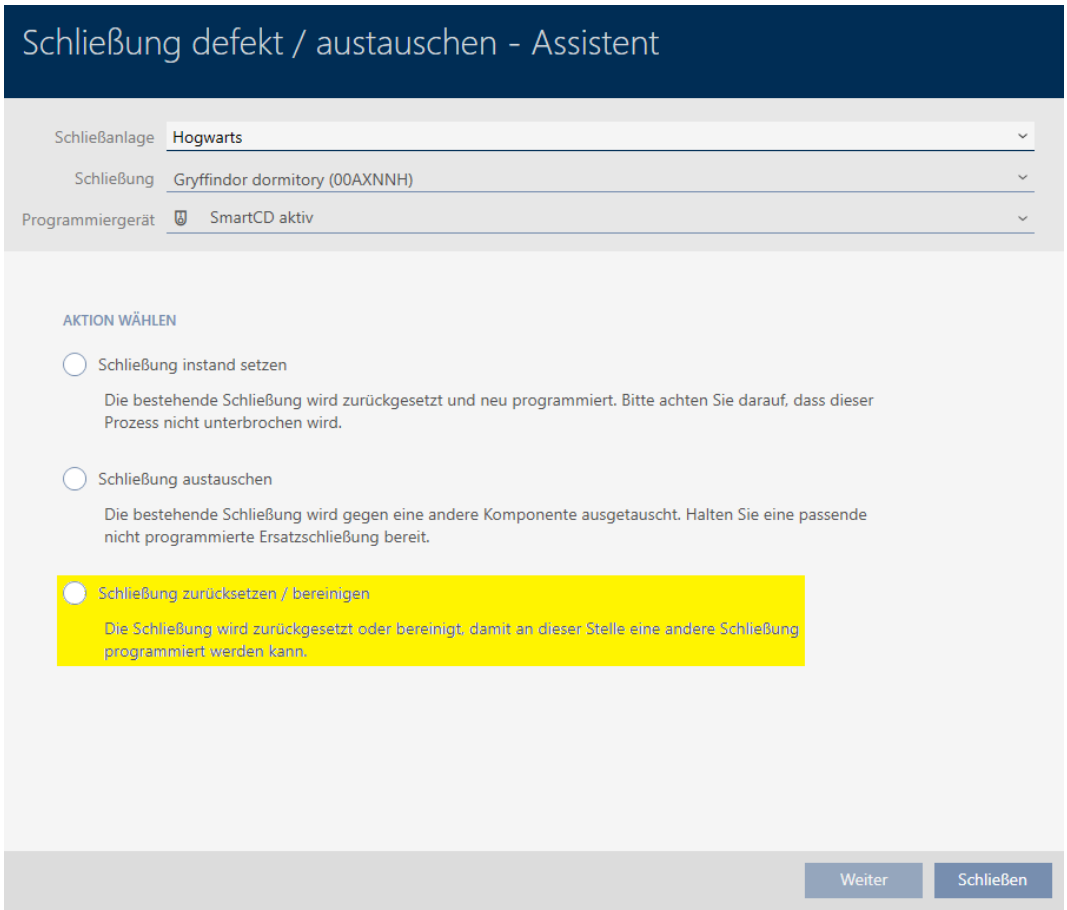
Situationsbeispiel:

Instandsetzen	Zurücksetzen und austauschen	Löschen und austauschen
	Krankenbett gegen Knauf gestoßen, Knauf verbogen	Krankenbett gegen Knauf gestoßen, Knauf abgebrochen

Ablauf:

Instandsetzen	Zurücksetzen und austauschen	Löschen und austauschen
Neu synchronisieren (Instandsetzen) [▸ 262] 1. Zurücksetzen (= LID in Datenbank wieder frei) 2. Neu synchronisieren (= LID wird sofort wieder in dieselbe Schließung geschrieben) Die Schließung funktioniert nach der Instandsetzung wieder wie vorher.	*Zurücksetzen und austauschen [▸ 264]* 1. Zurücksetzen (= LID in Datenbank als defekt markiert und aus Original-Schließung entfernt) 2. Austausch-Schließung mit neuer LID synchronisieren Durch das Zurücksetzen ist die LID nicht mehr in der Schließung vorhanden. Die Schließung ist daher nicht mehr verwendbar. Sie kann aber neu synchronisiert werden. Dabei wird eine neue LID in die Schließung geschrieben. Die bisherige Schließung verbleibt mit ihrer LID in der Datenbank und wird als defekt markiert.	*Löschen und austauschen [▸ 268]* 1. Austausch-Schließung mit neuer LID synchronisieren 2. Defekte Schließung löschen Eine zerstörte Schließung kann logischerweise nicht mehr zurückgesetzt werden. Sie wird deshalb durch eine Ersatzschließung mit einer neuen LID ersetzt. Die LID der defekten Schließung kann zukünftig wieder für eine andere Schließung verwendet werden.

Schließung wird nicht unmittelbar wieder benötigt:



Geeignet für:

Zurücksetzen	Bereinigen (Software-Reset)
▪ Äußerlich beschädigte Schließungen (z.B. verkratzt). ▪ Schließungen, die vorsichtshalber ersetzt werden sollen (z.B. nass geworden).	Schließungen mit undefiniertem Softwarezustand

Situationsbeispiel:

Zurücksetzen	Bereinigen (Software-Reset)
Krankenbett gegen Knauf gestoßen, Knauf verbogen. Tür muss repariert werden, daher kein unmittelbarer Bedarf für einen Schließzylinder.	Abgebrochene Programmierung

Ablauf:

Zurücksetzen	Bereinigen (Software-Reset)
Zurücksetzen [▸ 273] Mit dem Zurücksetzen entfernen Sie die LID aus der Schließung. Später können Sie eine andere Schließung mit diesem Eintrag synchronisieren, die dieselbe LID erhält.	*Bereinigen (nur in Datenbank zurücksetzen / Software-Reset) [▸ 275]* Das Bereinigen bezieht sich nur auf die Datenbank in Ihrer AXM Plus. Die reale Schließung bleibt davon unberührt. Vereinfacht gesagt setzen Sie die Schließung in der Datenbank zurück, ohne die reale Schließung auch tatsächlich zurückzusetzen. Die LID wird beim Bereinigen in der Datenbank von der LID der bisher verwendeten Schließung getrennt (im Istzustand). Nach dem Bereinigen eines Eintrags können Sie später wieder eine beliebige Schließung mit diesem Eintrag synchronisieren, die dieselbe LID erhält. Ihre AXM Plus kann nach dem Software-Reset nicht mehr wissen, dass die LID bereits vergeben ist. Achten Sie deshalb darauf, ggfs. die bisher für diesen Eintrag verwendete Schließung zurückzusetzen (siehe *Schließung zurücksetzen [▸ 425]*). Damit löschen Sie die LID aus der alten Schließung und verhindern, dass dieselbe LID zweimal im Umlauf ist.

HINWEIS

AX-Komponenten: SmartCD.MP oder SmartStick AX für erste Synchronisierung

Während der ersten Synchronisierung von AX-Komponenten werden sehr viele Daten übertragen. Die Trägerfrequenz und damit die Übertragungsgeschwindigkeit ist beim SmartCD.MP oder beim SmartStick AX deutlich höher.

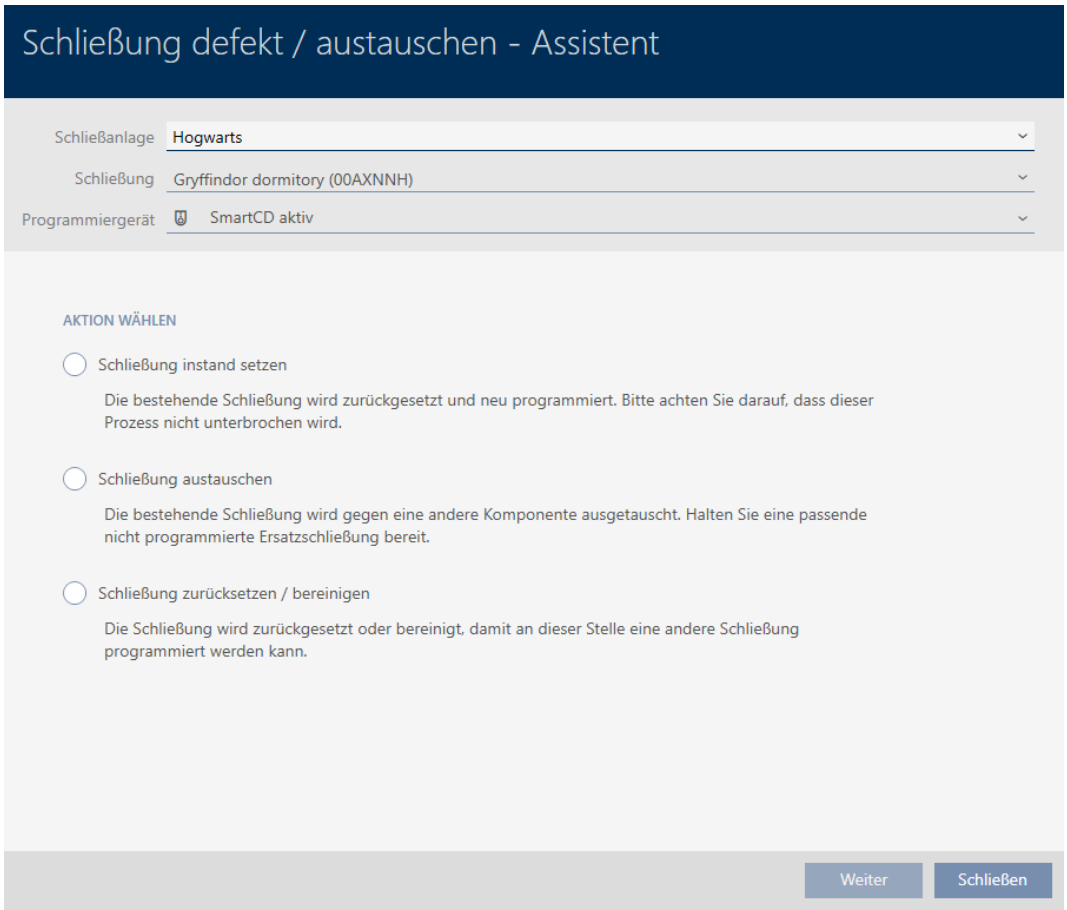
- Verwenden Sie insbesondere für die erste Synchronisierung von AX-Komponenten bevorzugt ein SmartCD.MP oder einen SmartStick AX.

16.5.1 Neu synchronisieren (Instandsetzen)

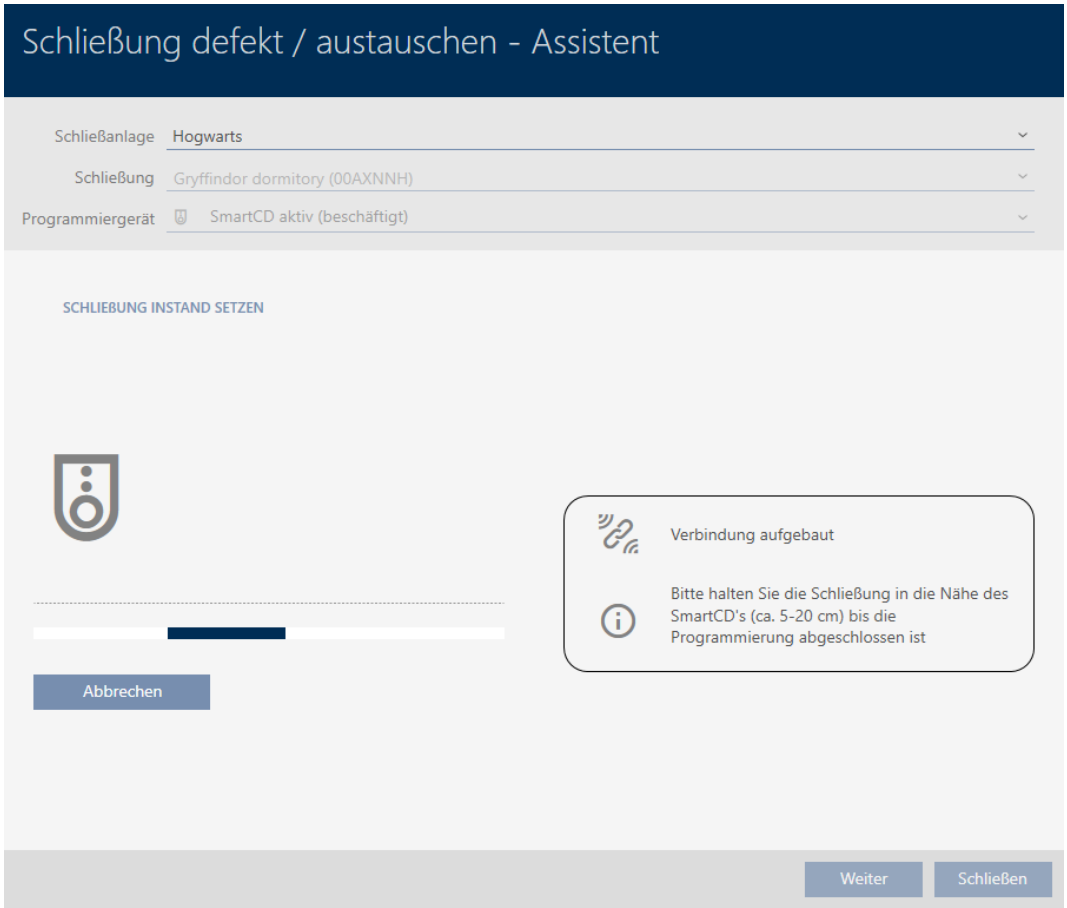
- ✓ Schließungsliste oder Matrixansicht geöffnet.
- ✓ Schließung vorliegend.
- ✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

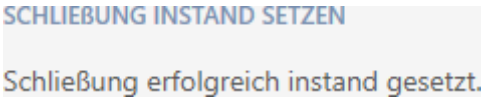
2. Markieren Sie die defekte Schließung.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Schließung defekt / austauschen.
   ↳ Assistent zum Behandeln einer defekten Schließung öffnet sich.



4. Wählen Sie die Option Schließung instand setzen aus.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Schließung wird neu synchronisiert.



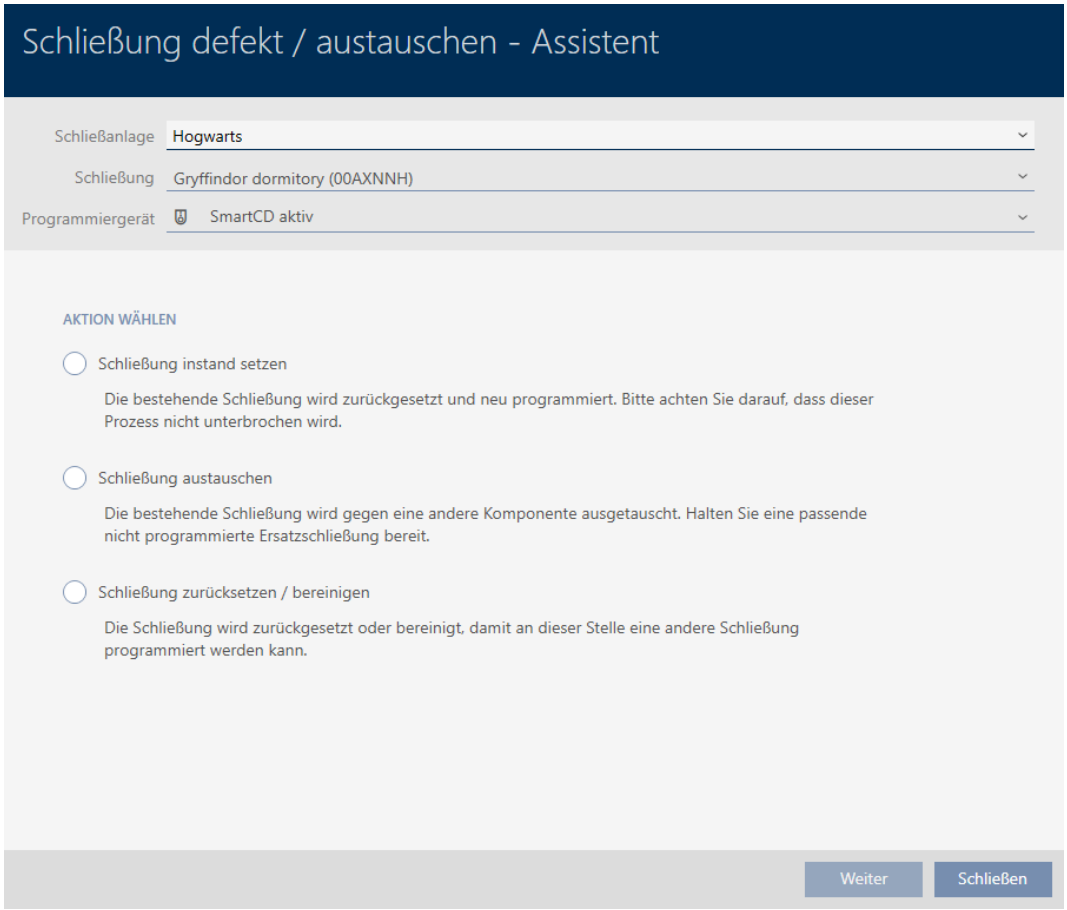
↳ Schließung ist neu synchronisiert.



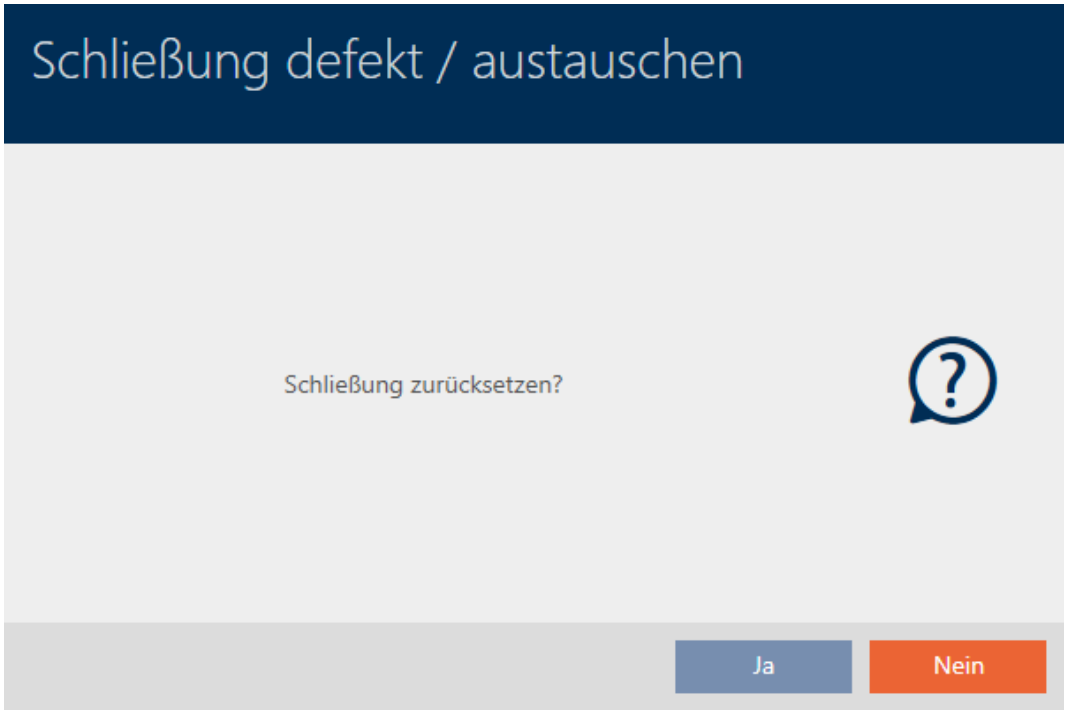
16.5.2 Zurücksetzen und austauschen

✓ Schließungsliste oder Matrixansicht geöffnet.
✓ Schließung vorliegend.
✓ Geeignete Ersatzschließung vorhanden.
✓ Geeignetes Programmiergerät angeschlossen.

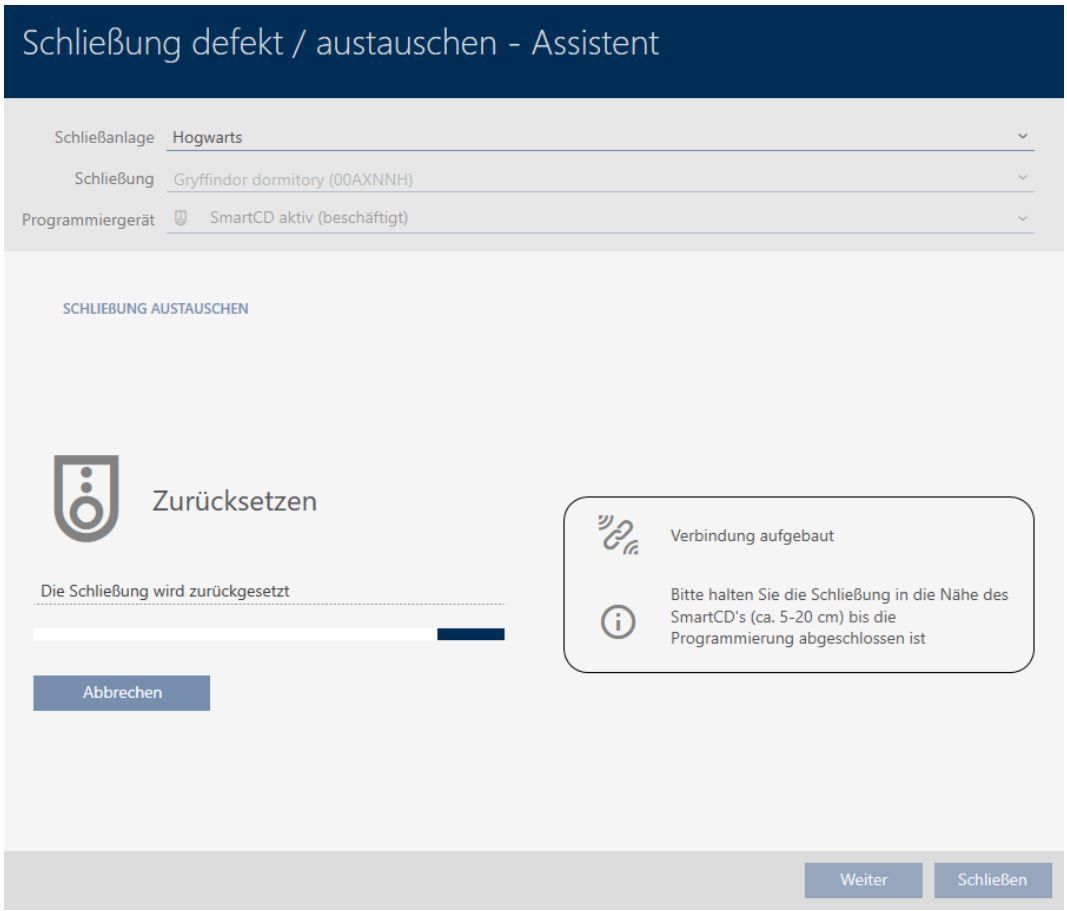
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie die defekte Schließung.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Schließung defekt / austauschen.
   ↳ Assistent zum Behandeln einer defekten Schließung öffnet sich.



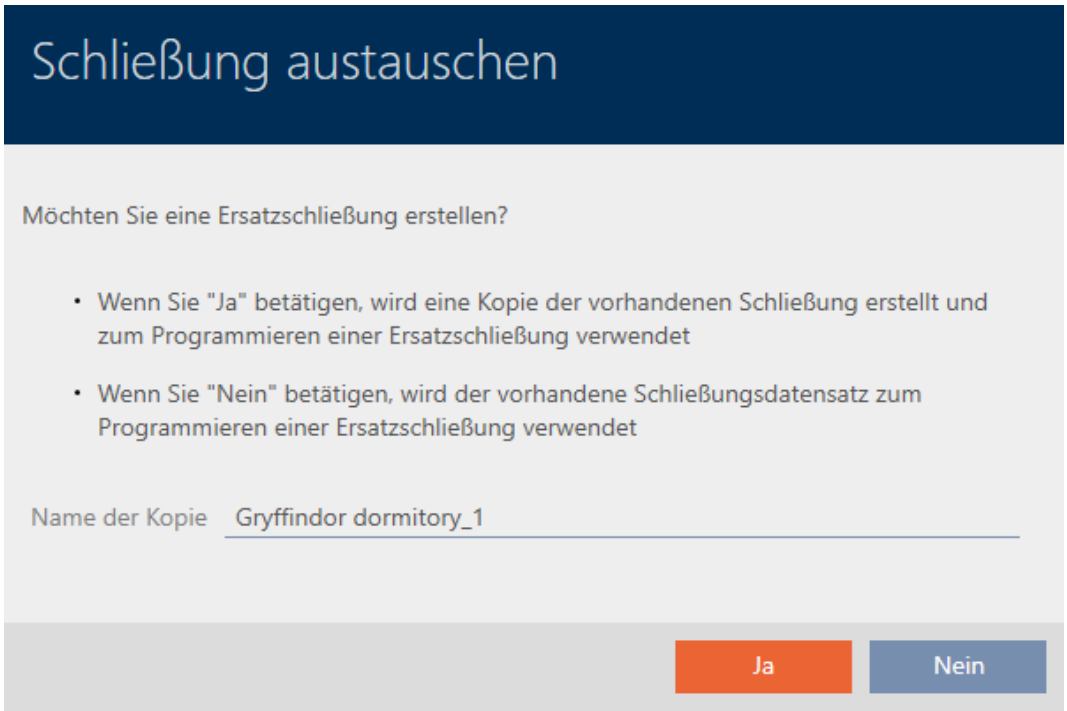
4. Wählen Sie die Option ◉ Schließung austauschen aus.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Schließung wird zurückgesetzt.

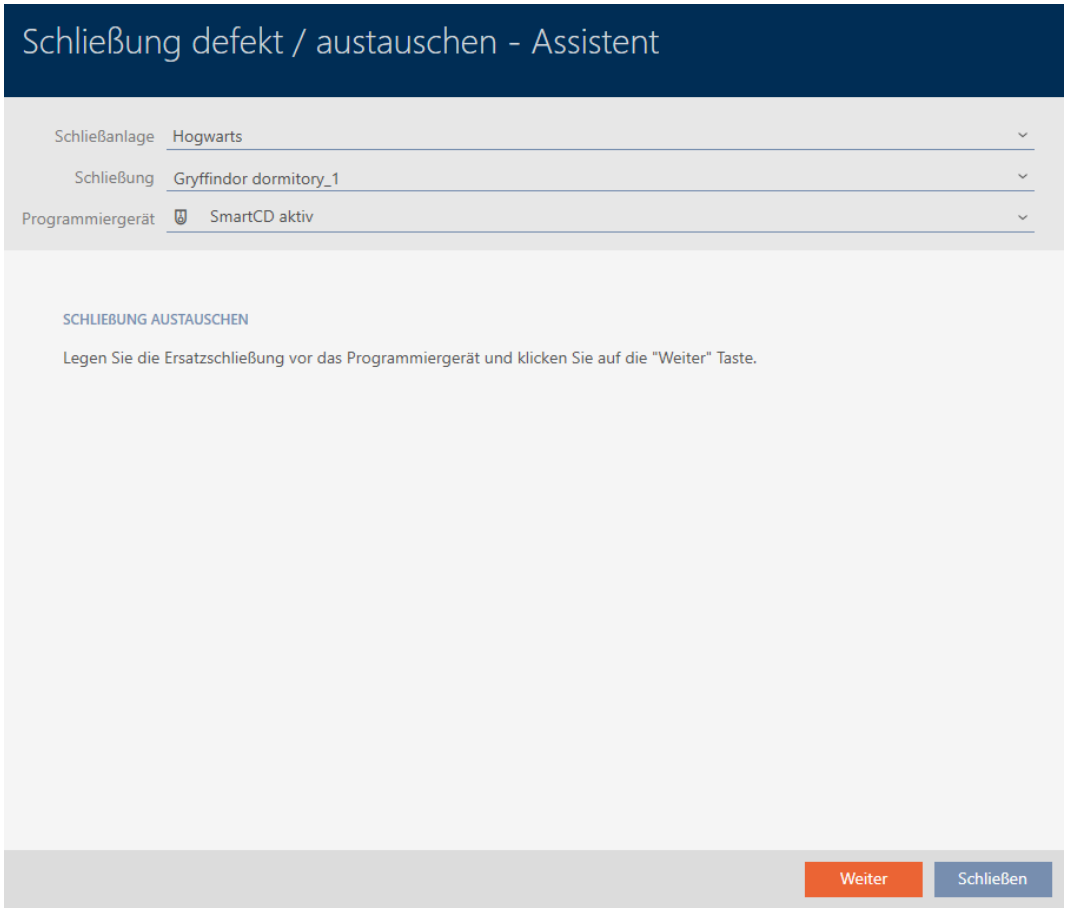


   ↳ Rückfrage zum Erstellen einer Ersatzschließung öffnet sich.

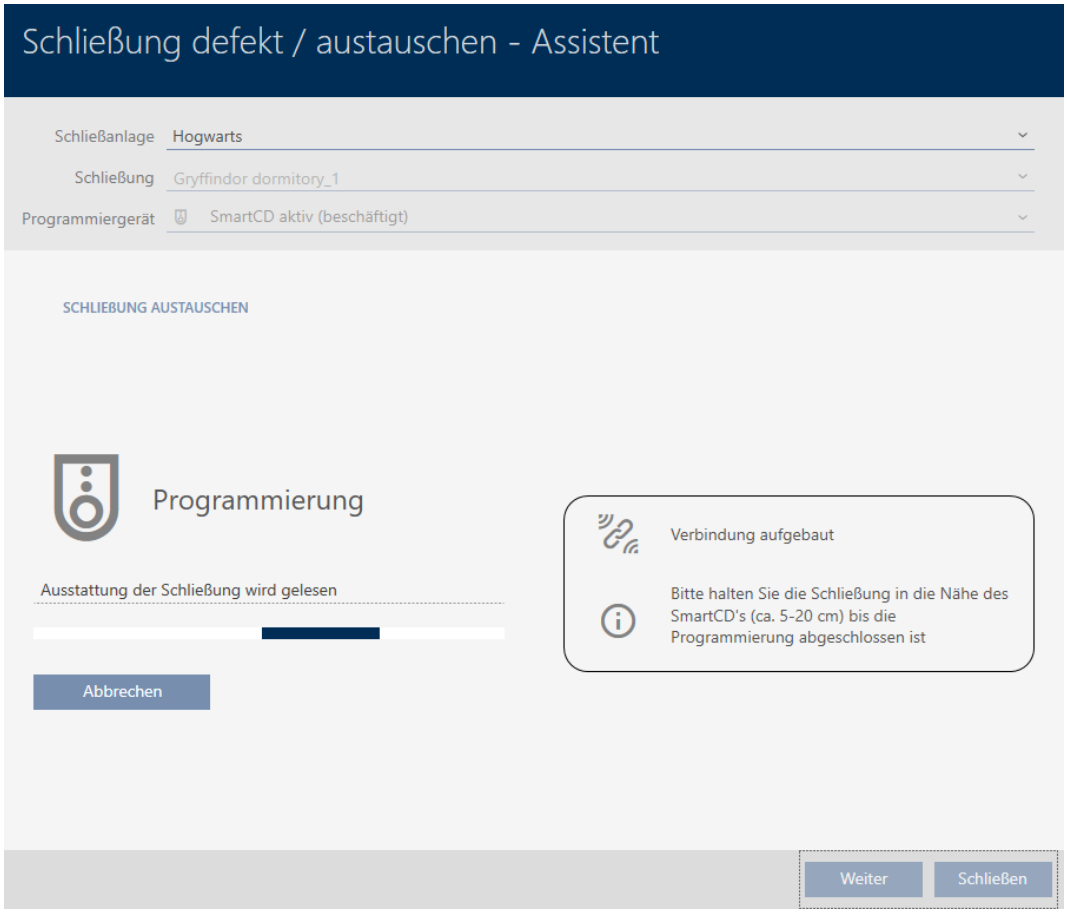


7. Ändern Sie ggfs. den Eintrag im Feld *Name der Kopie*.
8. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Erstellen einer Ersatzschließung schließt sich.
   ↳ Ersatzschließung ist bereits im Hintergrund in der Matrix sichtbar.

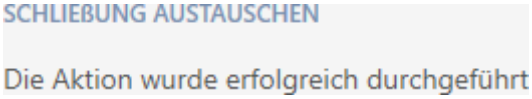
   ↳ Assistent bereitet Synchronisierung der Ersatzschließung vor.



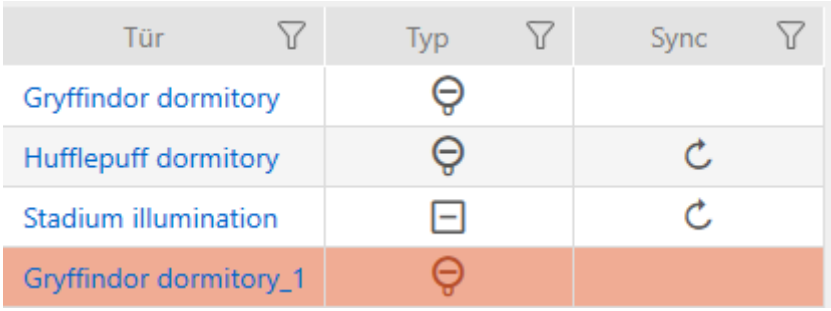
9. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Ersatzschließung wird synchronisiert.



↳ Ersatzschließung ist synchronisiert.



↳ Ersatzschließung wird in der Matrix angezeigt.

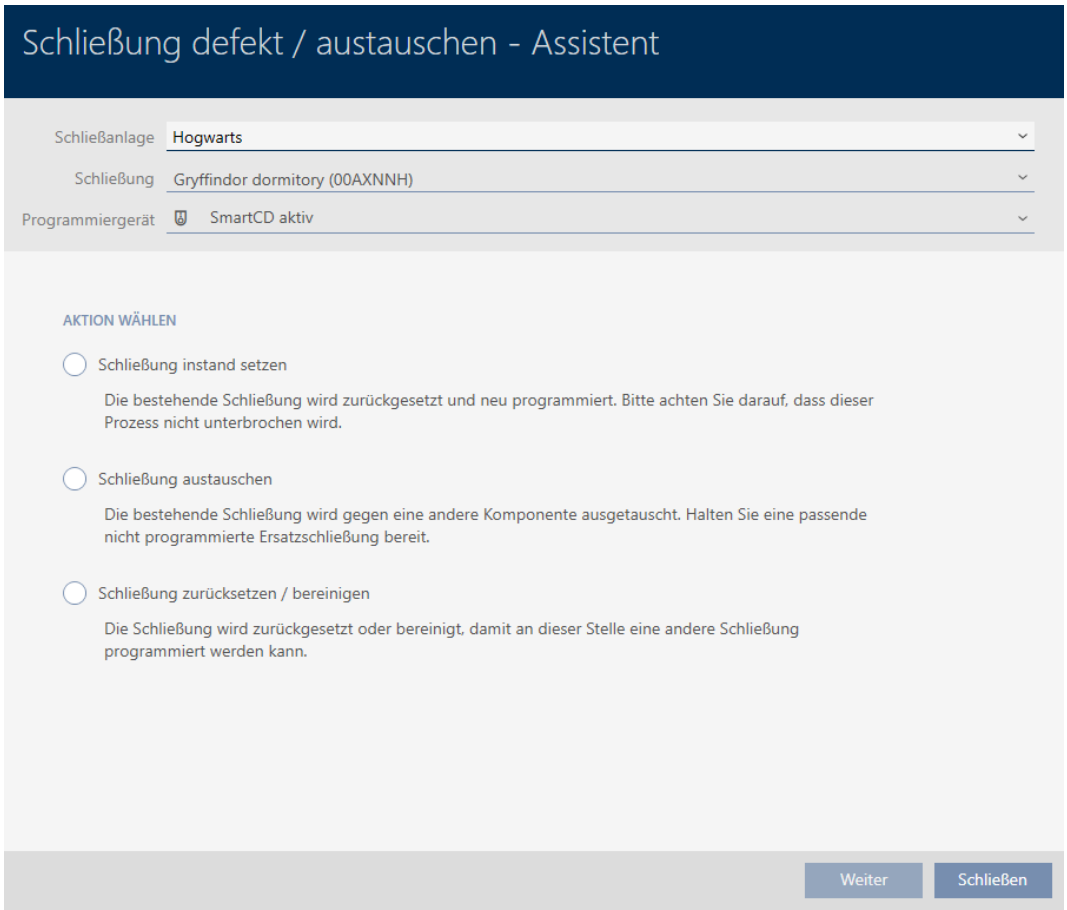


16.5.3 Löschen und austauschen

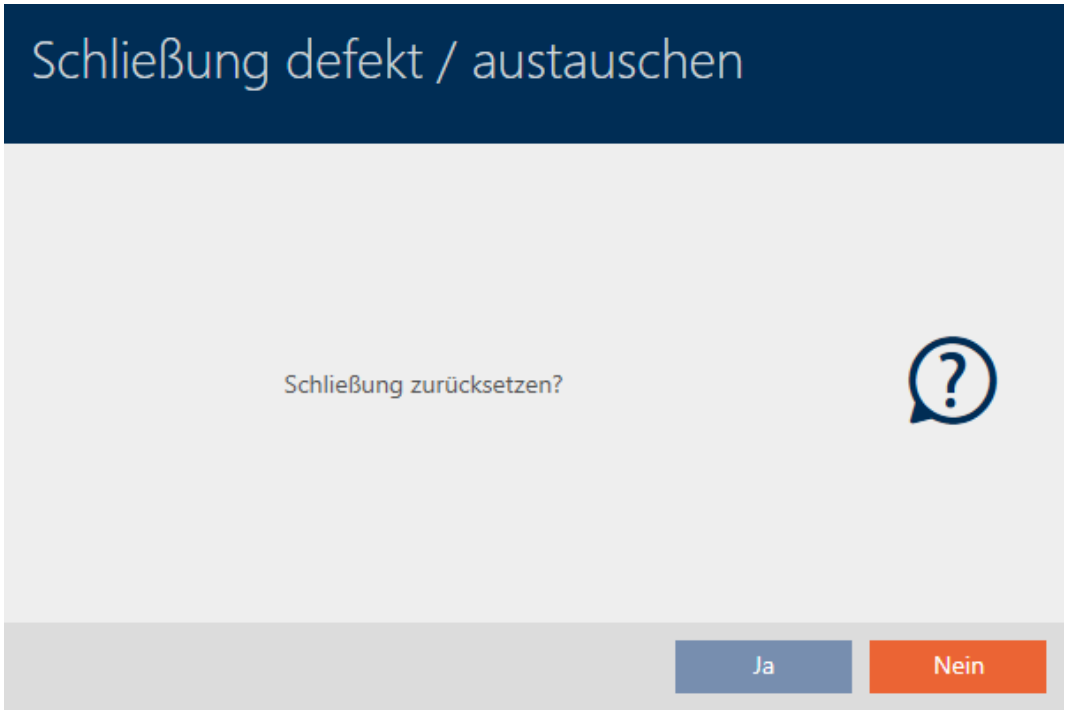
✓ Schließungsliste oder Matrixansicht geöffnet.
✓ Geeignete Ersatzschließung vorhanden.
✓ Geeignetes Programmiergerät angeschlossen.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

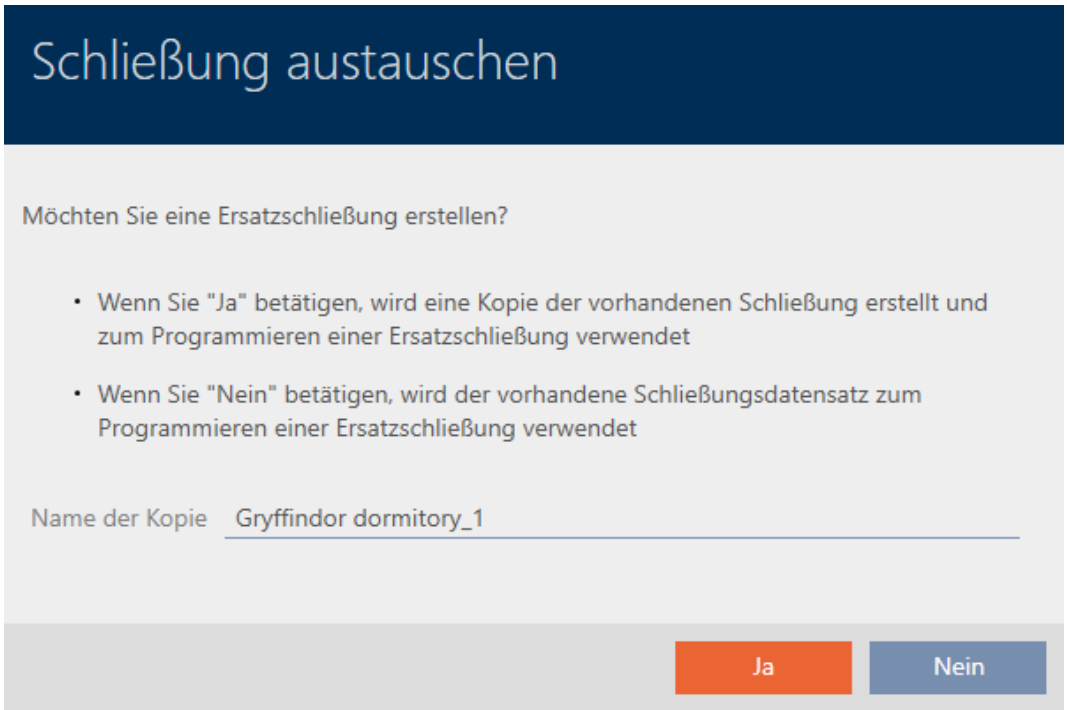
2. Markieren Sie die defekte Schließung.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Schließung defekt / austauschen.
   ↳ Assistent zum Behandeln einer defekten Schließung öffnet sich.



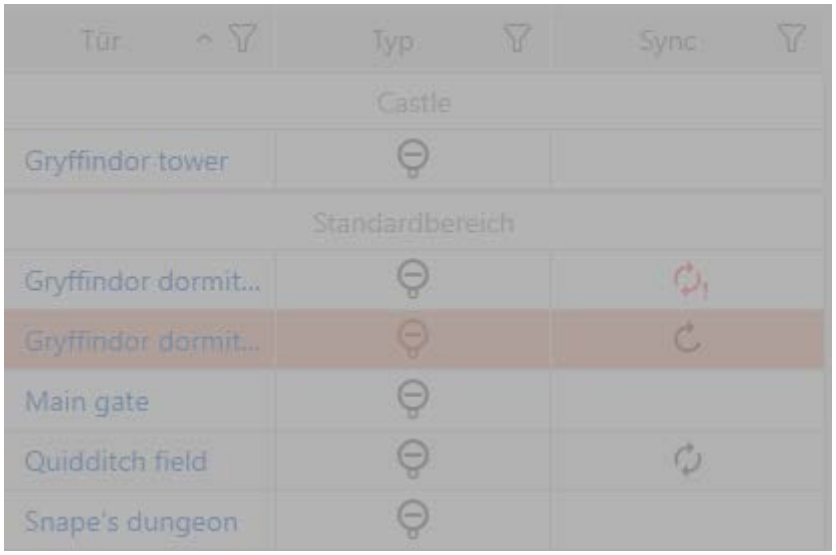
4. Wählen Sie die Option Schließung austauschen aus.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.



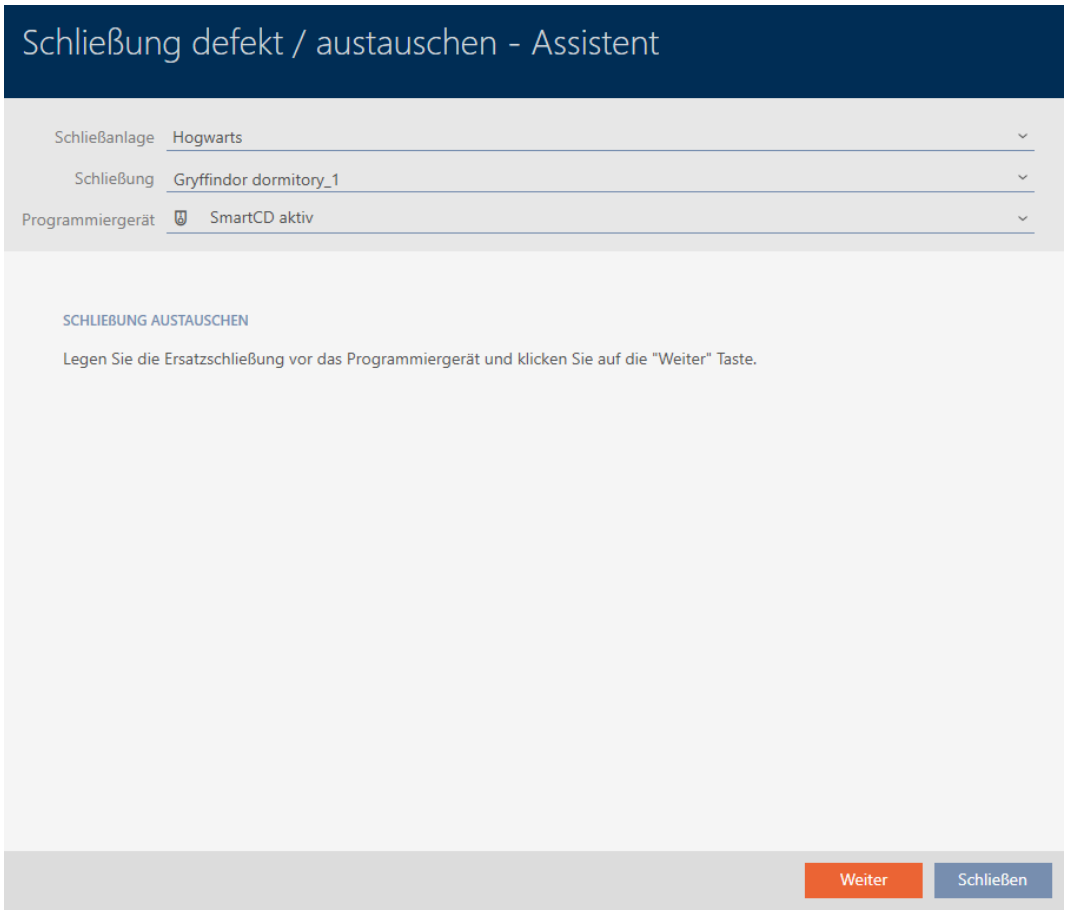
6. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Rückfrage zum Erstellen einer Ersatzschließung öffnet sich.



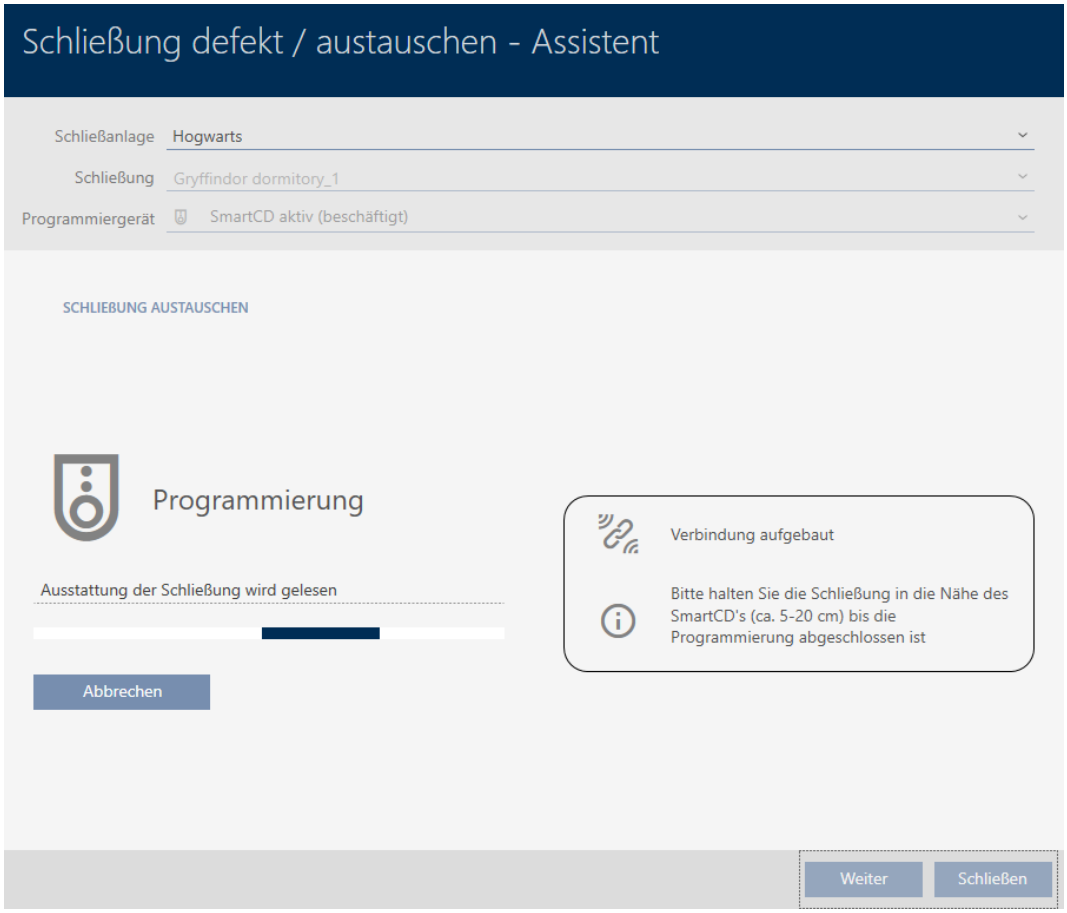
7. Ändern Sie ggfs. den Eintrag im Feld *Name der Kopie*.
8. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Erstellen einer Ersatzschließung schließt sich.
   ↳ Ersatzschließung ist bereits im Hintergrund in der Matrix sichtbar.



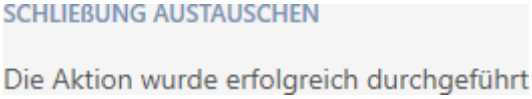
↳ Assistent bereitet Synchronisierung der Ersatzschließung vor.



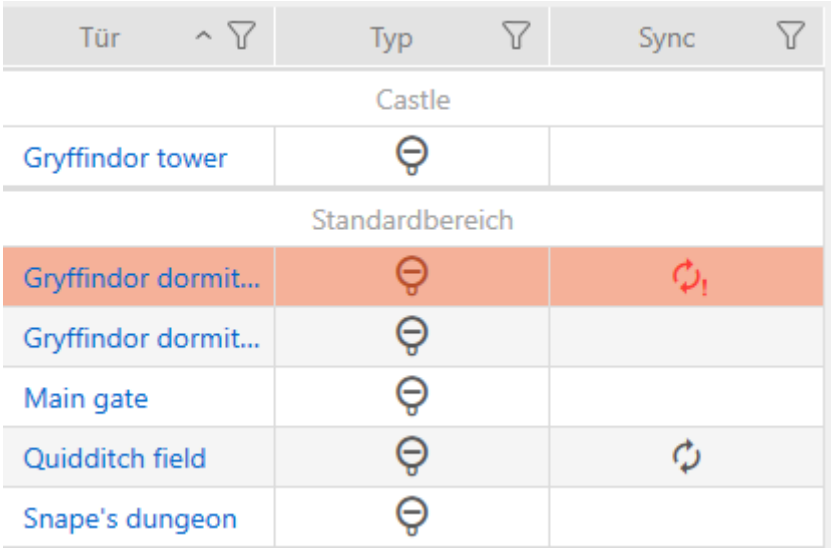
9. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Ersatzschließung wird synchronisiert.



↳ Ersatzschließung ist synchronisiert.



10. Klicken Sie auf die Schaltfläche Schließen.
    ↳ Assistent zum Behandeln einer defekten Schließung schließt sich.
11. Markieren Sie die defekte Originalschließung.



12. Klicken Sie auf die Schaltfläche Löschen.
    ↳ Defekte Schließung wird aus Schließplan gelöscht.

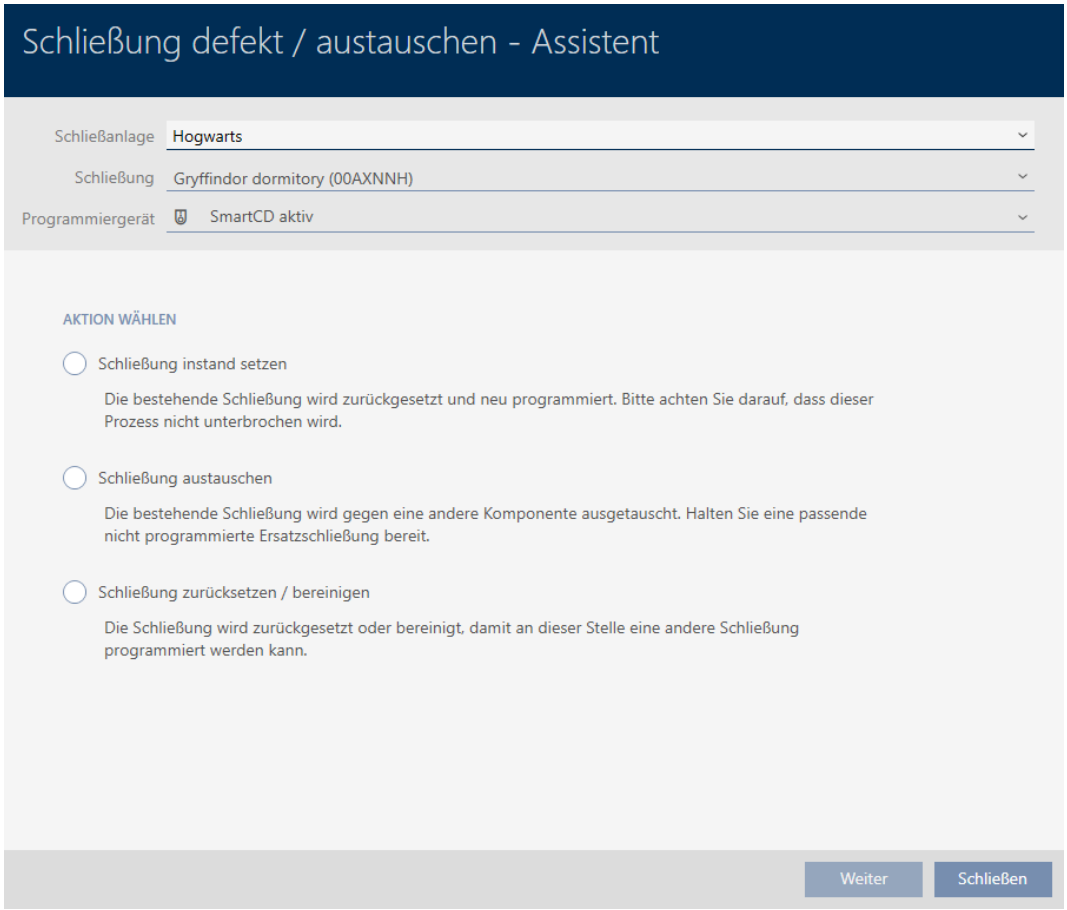
↳ Ersatzschließung wird in der Matrix angezeigt.

Tür	Typ	Sync
	Castle	
Gryffindor tower		
	Standardbereich	
Gryffindor dormit...		
Main gate		
Quidditch field		
Snape's dungeon		

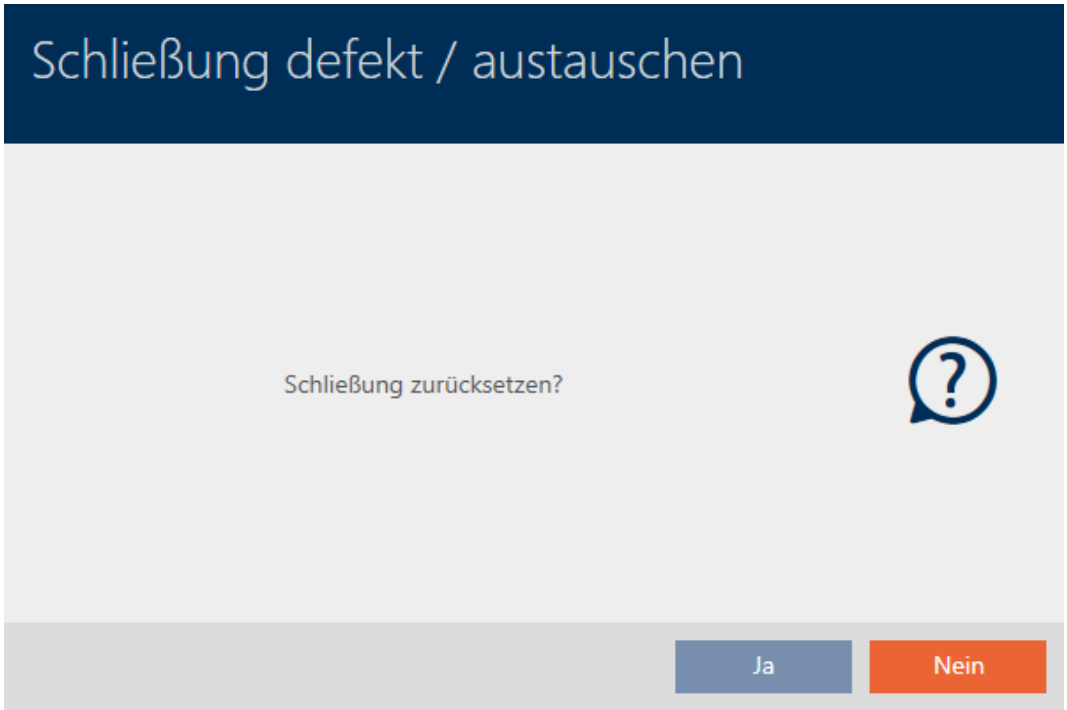
16.5.4 Zurücksetzen

✓ Schließungsliste oder Matrixansicht geöffnet.
✓ Schließung vorliegend.
✓ Geeignetes Programmiergerät angeschlossen.

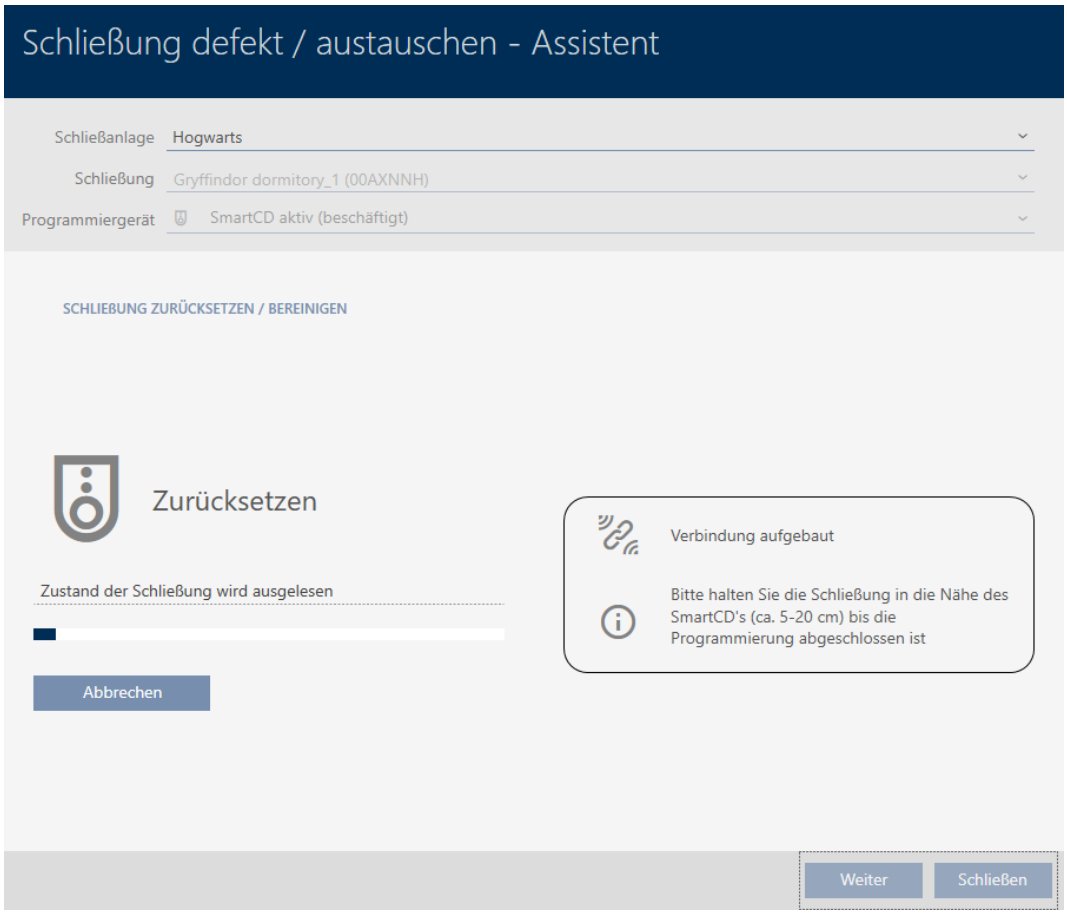
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie die defekte Schließung.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Schließung defekt / austauschen.
    ↳ Assistent zum Behandeln einer defekten Schließung öffnet sich.



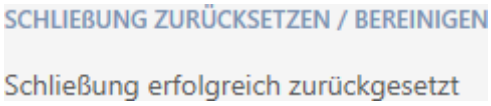
4. Wählen Sie die Option ◉ Schließung zurücksetzen / bereinigen aus.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.



6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Schließung wird zurückgesetzt.



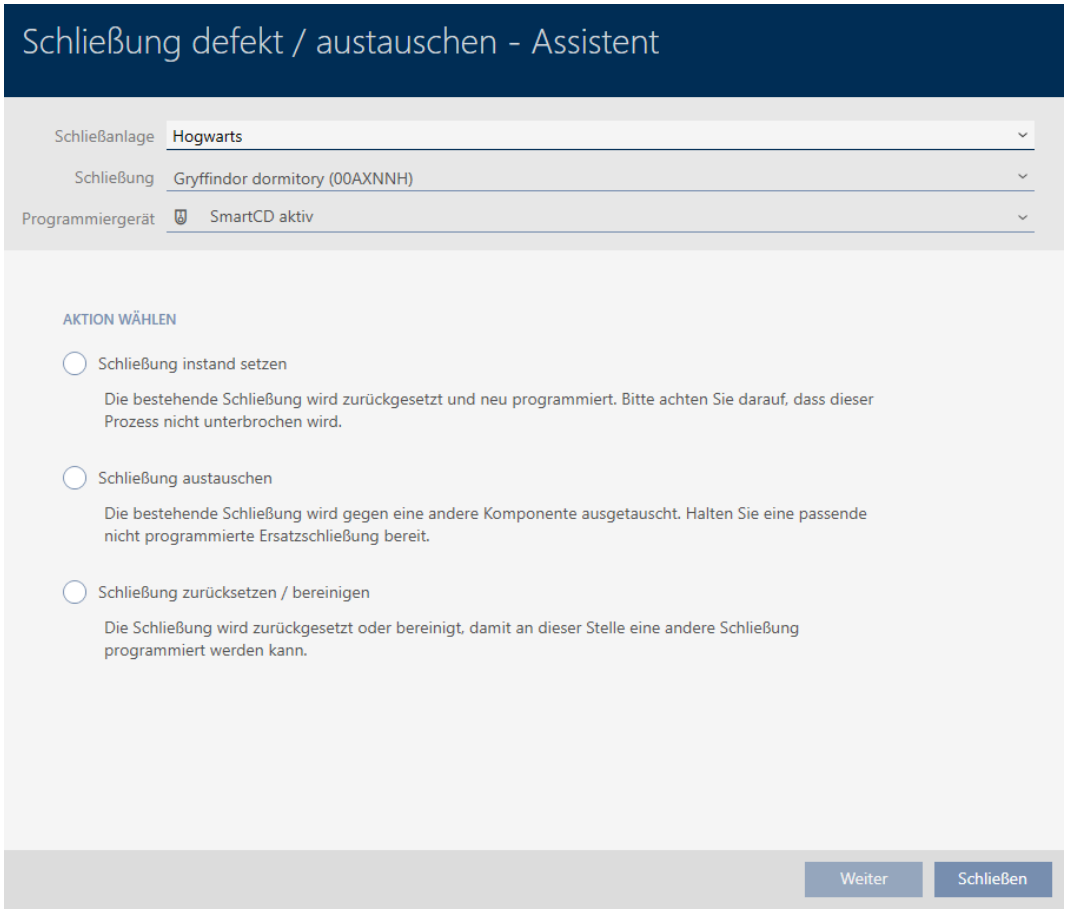
↳ Schließung ist zurückgesetzt.



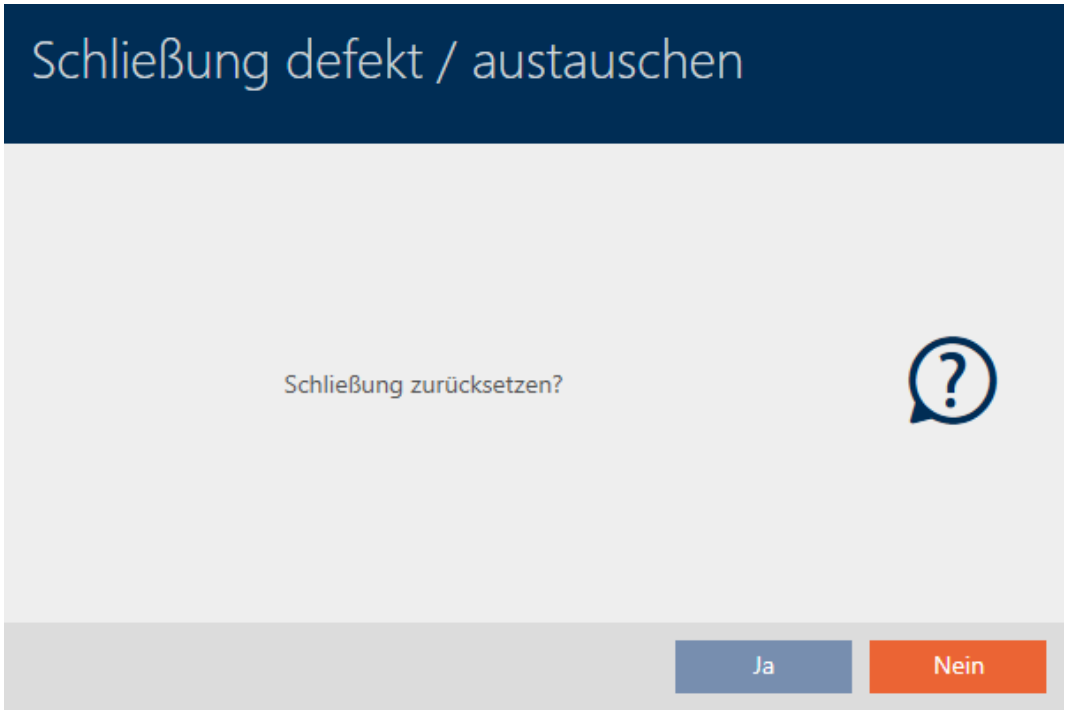
16.5.5 Bereinigen (nur in Datenbank zurücksetzen / Software-Reset)

✓ Schließungsliste oder Matrixansicht geöffnet.

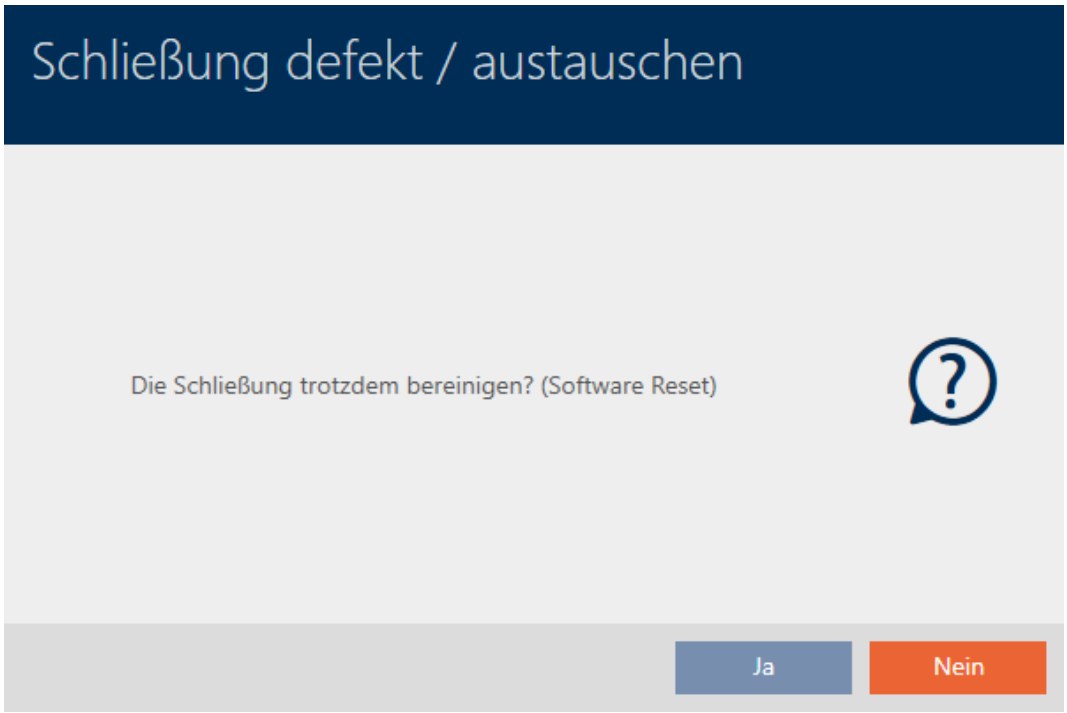
1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Markieren Sie die defekte Schließung.
3. Klicken Sie im Bereich "Assistenten" auf die Schaltfläche Schließung defekt / austauschen.
   ↳ Assistent zum Behandeln einer defekten Schließung öffnet sich.



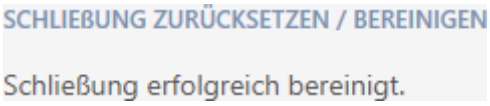
4. Wählen Sie die Option ◉ Schließung zurücksetzen / bereinigen aus.
5. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Rückfrage zum Zurücksetzen öffnet sich.



6. Klicken Sie auf die Schaltfläche Nein.
   ↳ Rückfrage zum Zurücksetzen schließt sich.
   ↳ Rückfrage zum Bereinigen öffnet sich.



7. Klicken Sie auf die Schaltfläche Ja.
   ↳ Schließung ist unabhängig von der realen Schließung in der Datenbank zurückgesetzt.



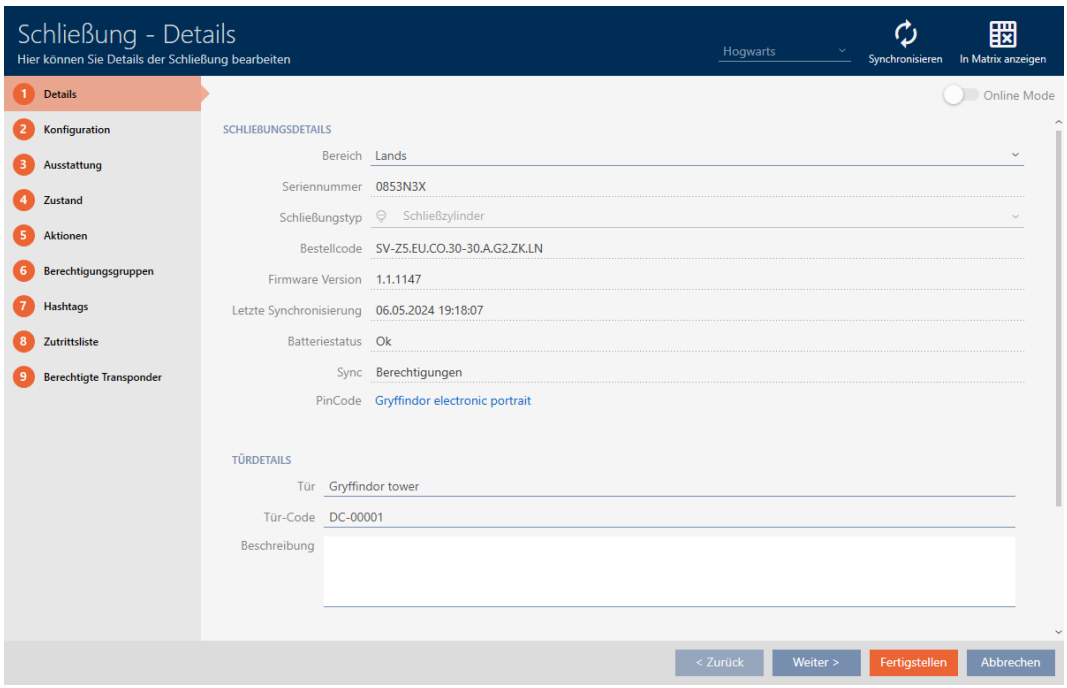
16.6 Schließungen zu Gebäuden/Standorten zuordnen

Sobald Sie eine Schließung anlegen, müssen Sie einen Standort und ein Gebäude angeben. Idealerweise folgen Sie der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) und erledigen alle organisatorischen Vorarbeiten bereits vor dem Erstellen Ihrer Schließungen (siehe *Organisationsstruktur [▸ 55]*). So müssen Sie Fenster nur einmal aufrufen.

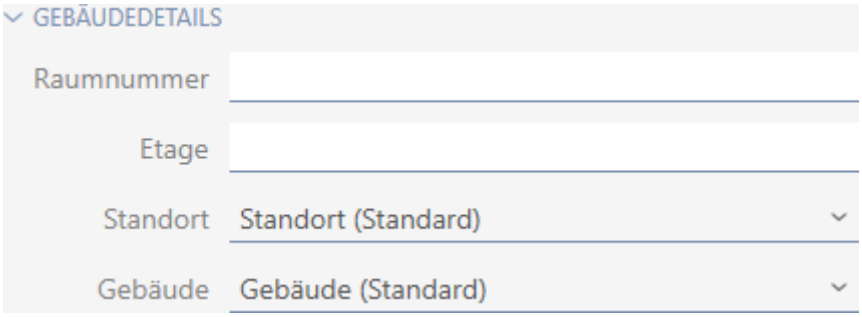
Selbstverständlich können Sie Ihre Schließungen aber auch nachträglich anderen Gebäuden zuordnen:

✓ Mindestens ein Standort erstellt (siehe *Standort erstellen [▸ 83]*).
✓ Mindestens ein Gebäude erstellt (siehe *Gebäude erstellen und zu Standort zuweisen [▸ 86]*).

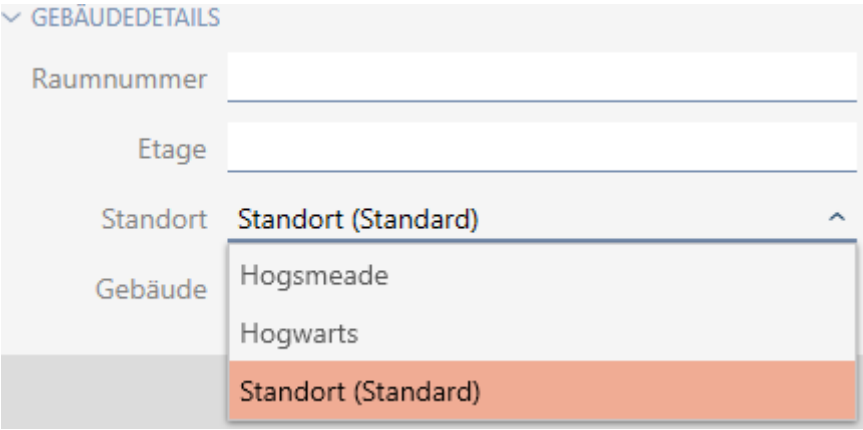
1. Klicken Sie auf die Schließung, die Sie zu einem Standort und einem Gebäude zuordnen wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klappen Sie ggfs. das Menü "Gebäude - Details" aus.



3. Wählen Sie im Dropdown-Menü ▼ **Standort** den Standort aus, an dem Ihre Schließung eingesetzt wird.



   ↳ Gebäudeauswahl im Dropdown-Menü ▼ **Gebäude** werden auf die Gebäude eingeschränkt, die zum gewählten Standort gehören.

4. Wählen Sie im Dropdown-Menü ▼ **Gebäude** das Gebäude aus, in dem Ihre Schließung eingesetzt wird.
5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Schließung ist einem anderen Gebäude/Standort zugeordnet.

HINWEIS

Feiertagslisten in Schließung und Standorten

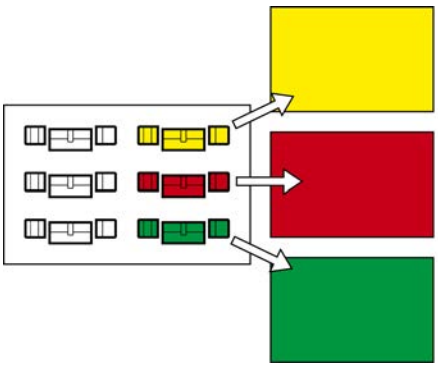
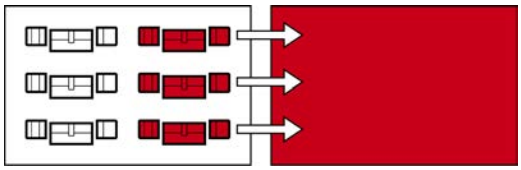
Sie können Feiertagslisten sowohl einer Schließung als auch dem Standort der Schließung zuweisen. In diesem Fall wird die Feiertagsliste in der Schließung verwendet und die Feiertagsliste im Standort ignoriert.

Wenn statt der Schließung dem Standort eine Feiertagsliste zugewiesen ist, dann wird die Feiertagsliste des Standorts für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

16.7 Schließungen in Bereiche verschieben

Sobald Sie eine Schließung anlegen, müssen Sie einen Bereich angeben. Idealerweise folgen Sie der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) und erledigen alle organisatorischen Vorarbeiten bereits vor dem Erstellen Ihrer Schließungen (siehe *Organisationsstruktur [▸ 55]*). So müssen Sie Fenster nur einmal aufrufen.

Selbstverständlich können Sie Ihre Schließungen aber auch nachträglich in einen anderen Bereich verschieben.

Einzelne Schließung verschieben	Mehrere Schließungen verschieben
Einzelne Schließung einem anderen Bereich zuordnen (im Fenster der Schließung) [▸ 281] Geeignet für das Verschieben weniger Schließungen in viele verschiedene Bereiche: 	*Mehrere Schließungen einem anderen Bereich zuordnen (im Bereichsfenster) [▸ 282]* Geeignet für das Verschieben mehrerer Schließungen in wenige verschiedene Bereiche: 

HINWEIS

Maximal ein Bereich pro Schließung

Eine Schließung kann nur zu maximal einem Bereich gehören. Überlappende Bereiche gibt es in der AXM Plus nicht. Wenn Sie einer Schließung einen anderen Bereich zuweisen, dann wird diese Schließung ggfs. automatisch aus ihrem bisherigen Bereich entfernt.

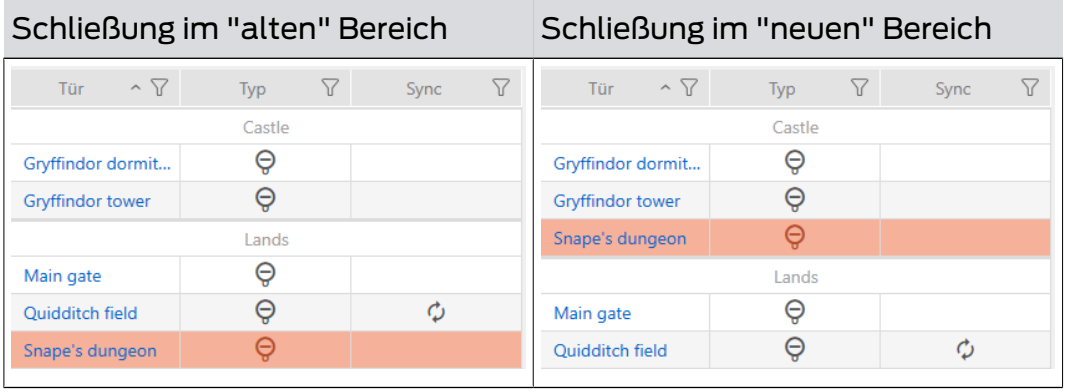
- Im Fenster "Bereich - Details" können Sie mithilfe der Spalte Bereich - Details prüfen, ob eine Schließung bereits einem Bereich zugewiesen ist.

Kein Einfluss von Bereichen auf Berechtigungen

Berechtigungen sind nicht unmittelbar mit Bereichen verknüpft. Wenn also eine Schließung in einen anderen Bereich verschoben wird, dann ändern hat das zunächst keinen Einfluss auf Berechtigungen. Bereiche sind aber ein nützliches Werkzeug, um Berechtigungen schneller zu ändern.

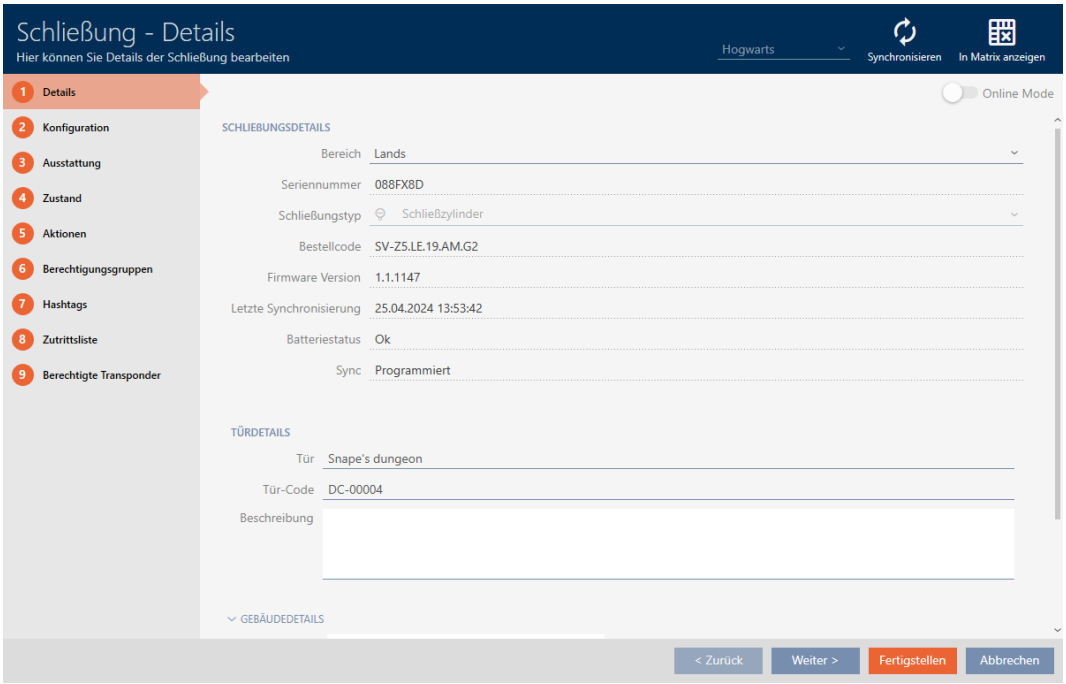
- Nutzen Sie Bereiche, um Schließungen schneller zu Berechtigungsgruppen hinzuzufügen (siehe *Bereiche und Personengruppen zu Berechtigungsgruppen hinzufügen [▸ 341]*).

16.7.1 Einzelne Schließung einem anderen Bereich zuordnen (im Fenster der Schließung)

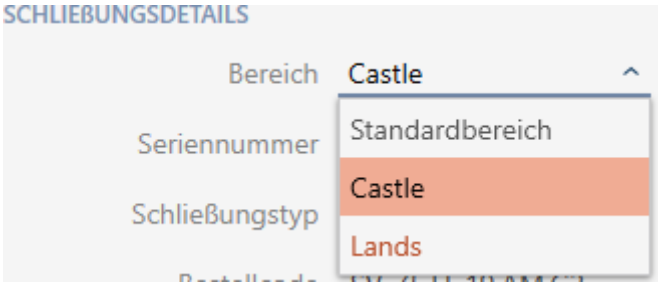


✓ Mindestens ein Bereich erstellt (siehe *Bereich erstellen [▸ 89]*).

1. Klicken Sie auf die Schließung, die Sie in einen anderen Bereich verschieben wollen.
   ↳ Fenster der Schließung öffnet sich.

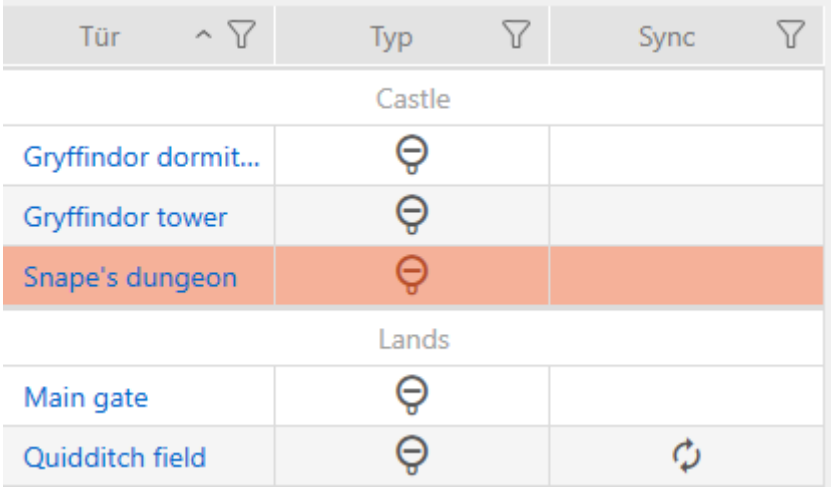


2. Wählen Sie im Dropdown-Menü ▼ **Bereich** den Bereich aus, in den Sie die Schließung verschieben wollen.



3. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Schließung befindet sich im neuen Bereich.



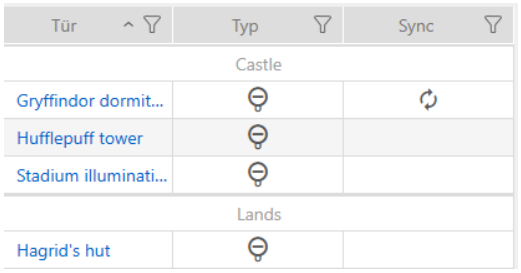
HINWEIS

Zeitpläne in Schließung und Bereichen

Sie können Zeitpläne sowohl einer Schließung als auch dem Bereich der Schließung zuweisen. In diesem Fall wird der Zeitplan in der Schließung verwendet und der Zeitplan des Bereichs ignoriert.

Wenn statt der Schließung dem Bereich ein Zeitplan zugewiesen ist, dann wird der Zeitplan des Bereichs für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

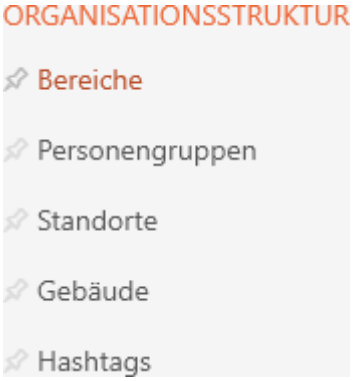
16.7.2 Mehrere Schließungen einem anderen Bereich zuordnen (im Bereichsfenster)

Schließung im "alten" Bereich	Schließung im "neuen" Bereich
	

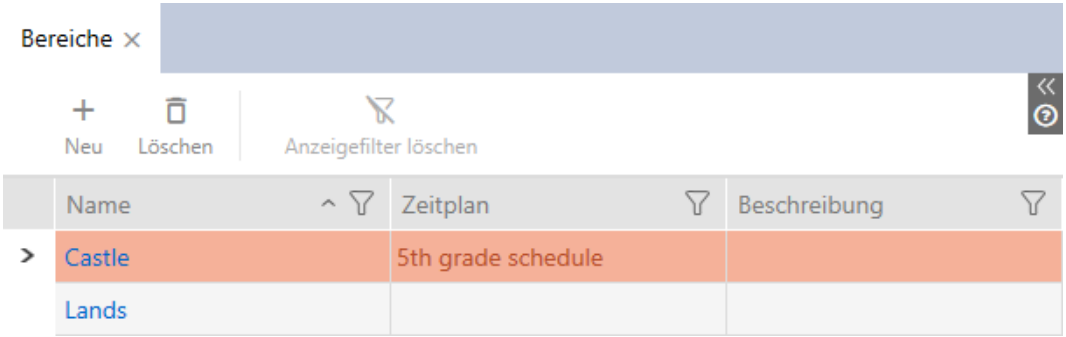
✓ Mindestens ein Bereich erstellt (siehe *Bereich erstellen [▸ 89]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

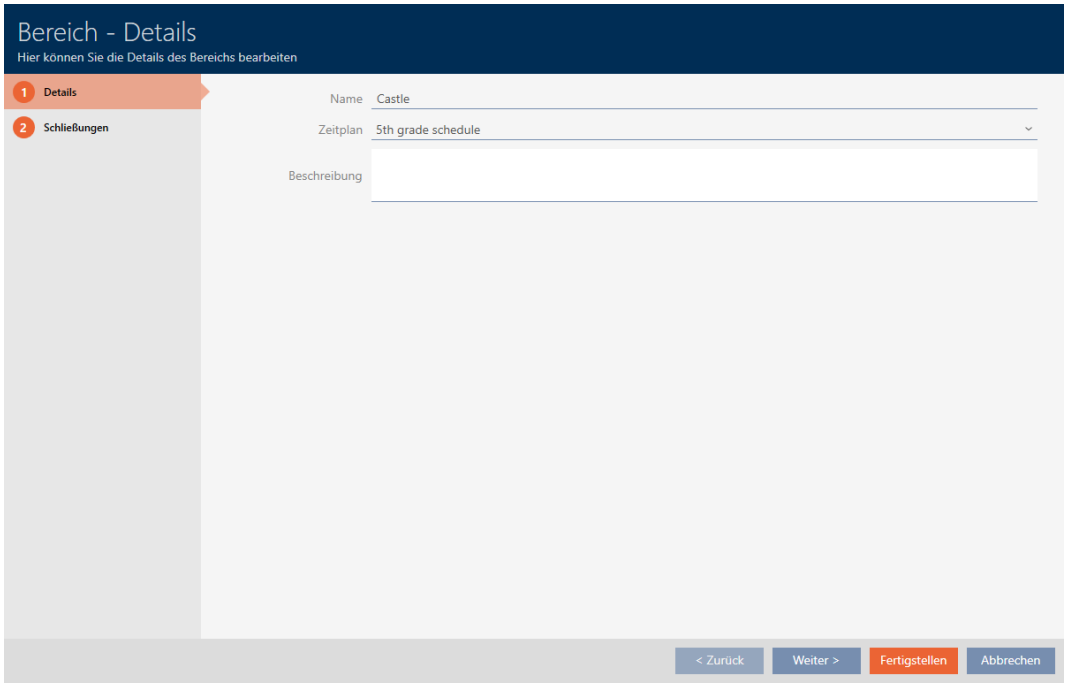
2. Wählen Sie in der Gruppe | ORGANISATIONSSTRUKTUR | den Eintrag Bereiche.



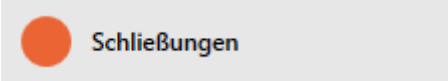
↳ AXM-Leiste klappt zu.
↳ Tab [Bereiche] öffnet sich.



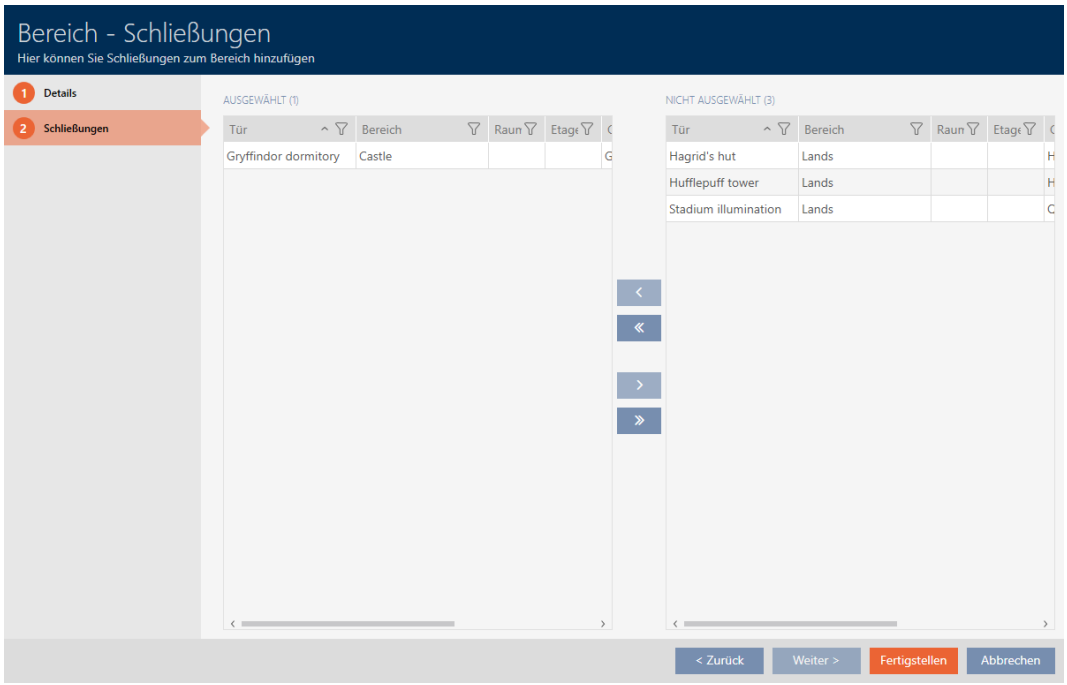
3. Klicken Sie auf den Bereich, in den Sie die Schließungen verschieben wollen.
   ↳ Fenster "Bereich" öffnet sich.



4. Klicken Sie auf den Reiter Schließungen.



↳ Fenster wechselt zum Reiter "Schließungen".



5. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
6. Markieren Sie alle Schließungen, die Sie zum Bereich hinzufügen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

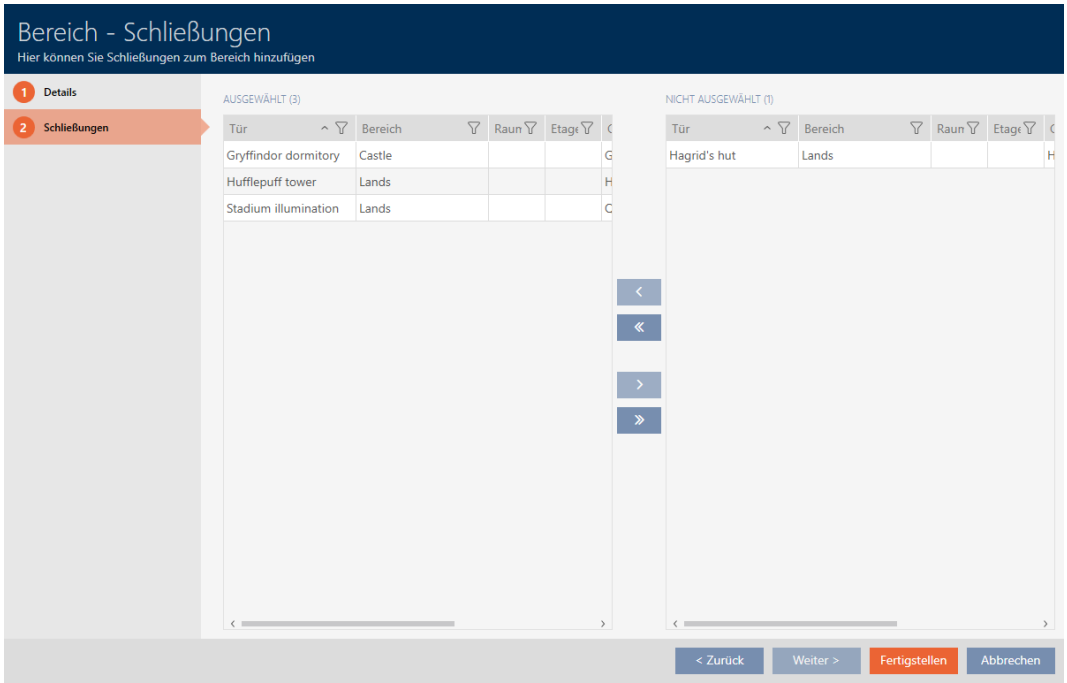
7. Verschieben Sie mit [<] nur die ausgewählten Schließungen oder verschieben Sie mit [«] alle angezeigten Schließungen.

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

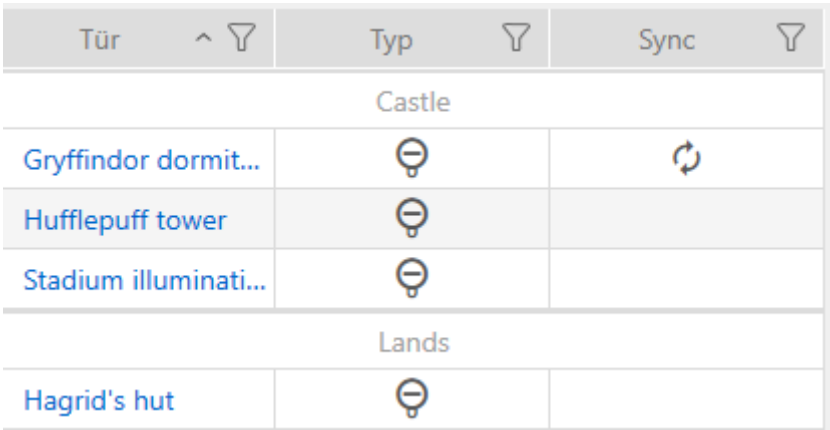
Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

↳ Die markierte Schließung in der linken Spalte wird dem Bereich hinzugefügt.



8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Bereich" schließt sich.
   ↳ Schließungen sind in den neuen Bereich verschoben.

↳ Matrix zeigt Strukturierung mit neuen Bereichen an.



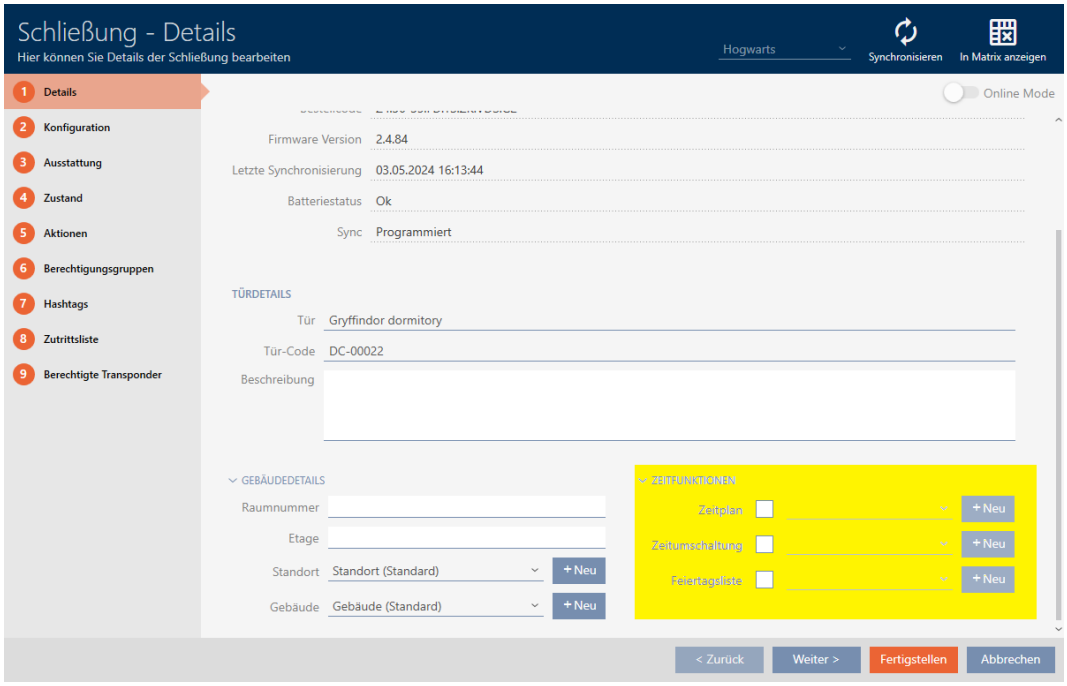
16.8 Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan)

Mit einem Zeitplan für Ihre Schließung beschränken Sie die Berechtigungen auf bestimmte Tage und Uhrzeiten (siehe *Zeitmanagement [▸ 548]*).

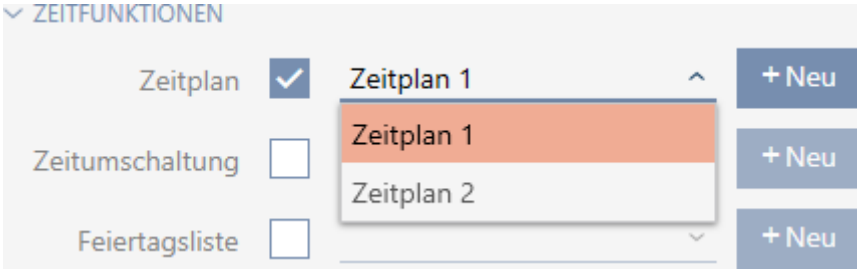
In diesem Kapitel erfahren Sie, wie Sie einzelne Schließungen über das Fenster der Schließung zu einem Zeitplan hinzufügen. Mehrere Schließungen lassen sich schneller im Zeitplan selbst hinzufügen: *Schließungen zum Zeitplan hinzufügen [▸ 348]*.

✓ Schließung erstellt (siehe *Schließung erstellen [▸ 238]*).
✓ Schließung mit .ZK-Option ausgestattet.
✓ Zeitplan erstellt (siehe *Zeitplan erstellen [▸ 58]*).

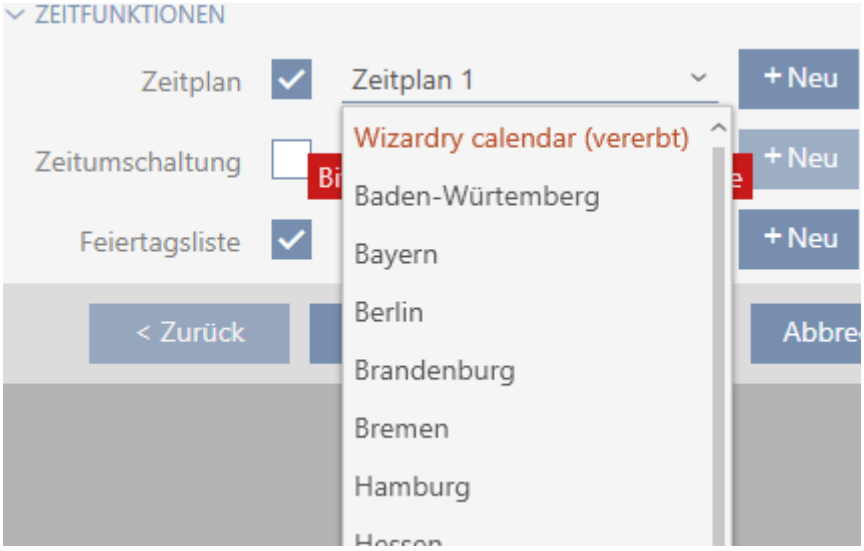
1. Klicken Sie auf die Schließung, die Sie hinzufügen wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klappen Sie ggfs. das Menü "Zeitfunktionen" auf.
3. Aktivieren Sie die Checkbox ☑ Zeitplan.
4. Wählen Sie im Dropdown-Menü ▼ **Zeitplan** den Zeitplan für Ihre Schließung aus.



5. Aktivieren Sie die Checkbox ☑ Feiertagsliste.
6. Wählen Sie im Dropdown-Menü ▼ **Feiertagsliste** die Feiertagsliste für Ihre Schließung aus.



HINWEIS

Feiertagslisten in Schließung und Standorten

Sie können Feiertagslisten sowohl einer Schließung als auch dem Standort der Schließung zuweisen. In diesem Fall wird die Feiertagsliste in der Schließung verwendet und die Feiertagsliste im Standort ignoriert.

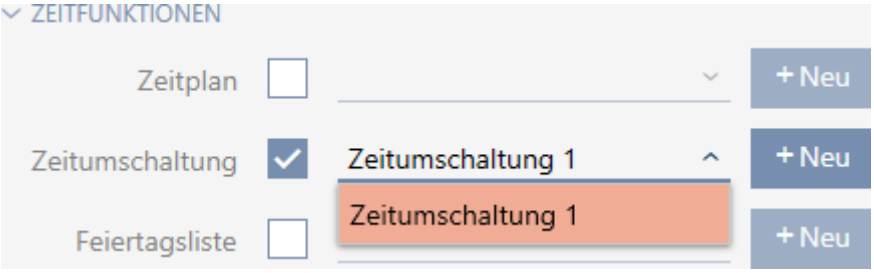
Wenn statt der Schließung dem Standort eine Feiertagsliste zugewiesen ist, dann wird die Feiertagsliste des Standorts für die Schließung übernommen. Im Fenster der Schließung erkennen Sie das am Zusatz "(vererbt)".

7. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Schließung ist dem Zeitplan hinzugefügt.

16.9 Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln

Idealerweise haben Sie Ihre Zeitumschaltungen bereits vor dem Erstellen der Schließungen erstellt (siehe *Best Practice: Schließanlage aufbauen* *[▸ 32]* und *Zeitumschaltung erstellen* *[▸ 71]*). Damit können Sie direkt beim Erstellen der Schließungen die Zeitumschaltungen direkt in den Eigenschaften der Schließung einstellen:



Selbstverständlich können Sie Ihre Schließungen aber auch nachträglich zu den Zeitumschaltungen hinzufügen:

✓ Schließung mit .ZK-Option ausgestattet.

✓ Zeitumschaltung erstellt (siehe *Zeitumschaltung erstellen [▸ 71]*).

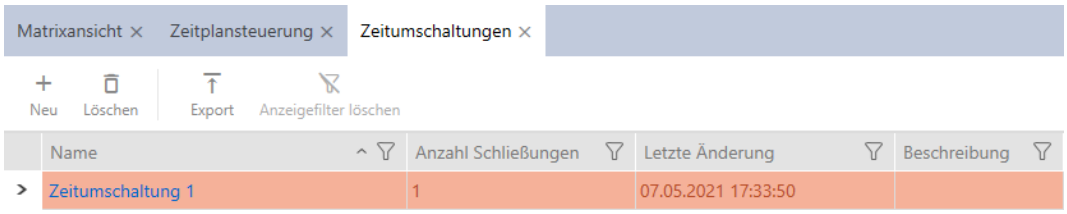
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Zeitplansteuerung aus.

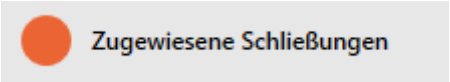
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Zeitplansteuerung] öffnet sich.

3. Klicken Sie auf die Schaltfläche Zeitumschaltungen.

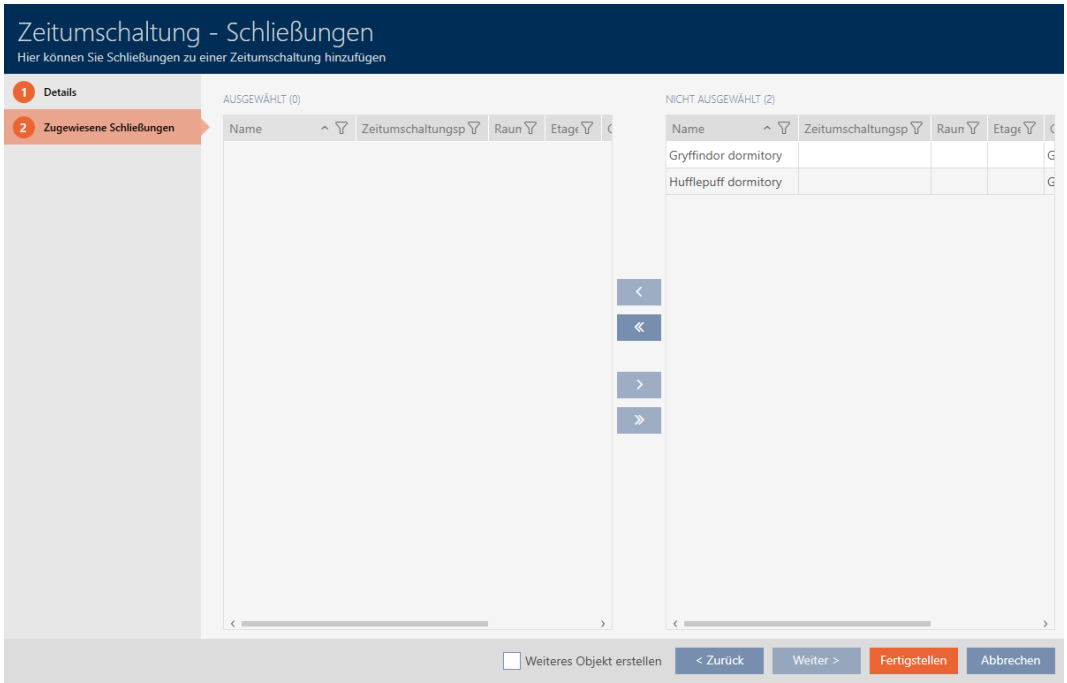
↳ Tab [Zeitumschaltungen] öffnet sich.



4. Klicken Sie auf die Zeitumschaltung, zu der Sie Ihre Schließungen hinzufügen wollen.
   ↳ Fenster der Zeitumschaltung öffnet sich.
5. Klicken Sie auf den Reiter Zugewiesene Schließungen.



↳ Fenster wechselt zum Reiter "Zugewiesene Schließungen".



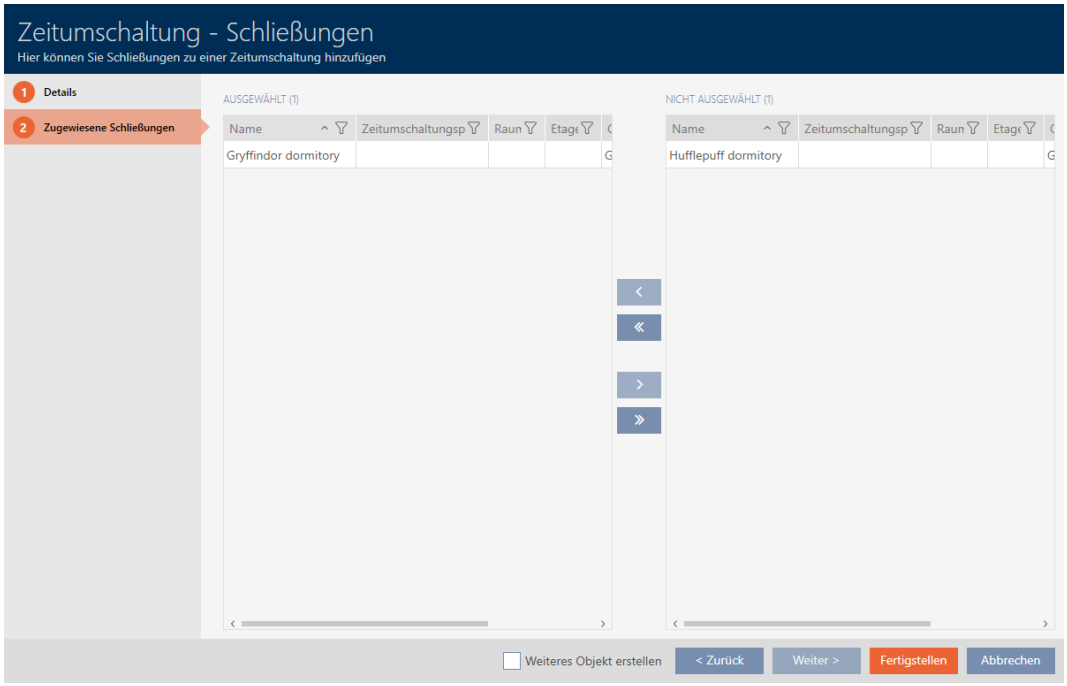
6. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
7. Markieren Sie alle Schließungen, die Sie mit dem Zeitplan öffnen und schließen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

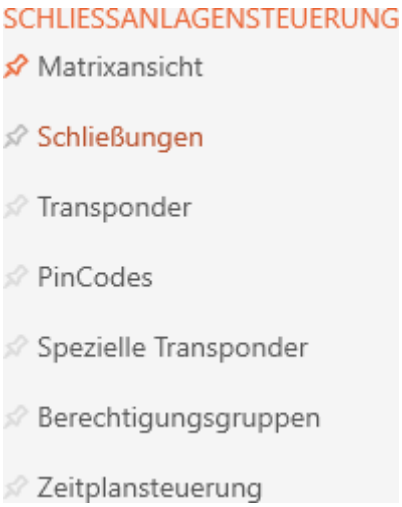
Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

8. Verschieben Sie mit [<] nur die ausgewählten Schließungen oder verschieben Sie mit [«] alle angezeigten Schließungen.
   ↳ Die markierten Schließungen in der linken Spalte werden der Zeitumschaltung hinzugefügt.



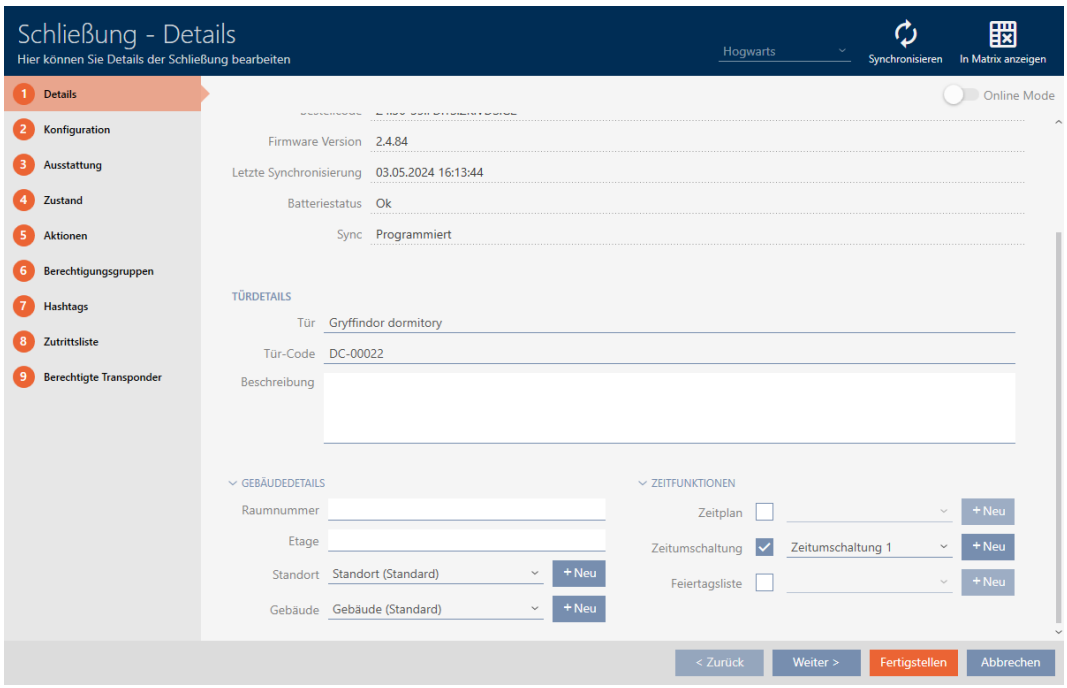
9. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Zeitumschaltung schließt sich.
10. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

11. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Schließungen aus.

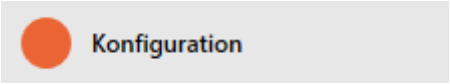


↳ AXM-Leiste klappt zu.
↳ Tab [Schließungen] öffnet sich.

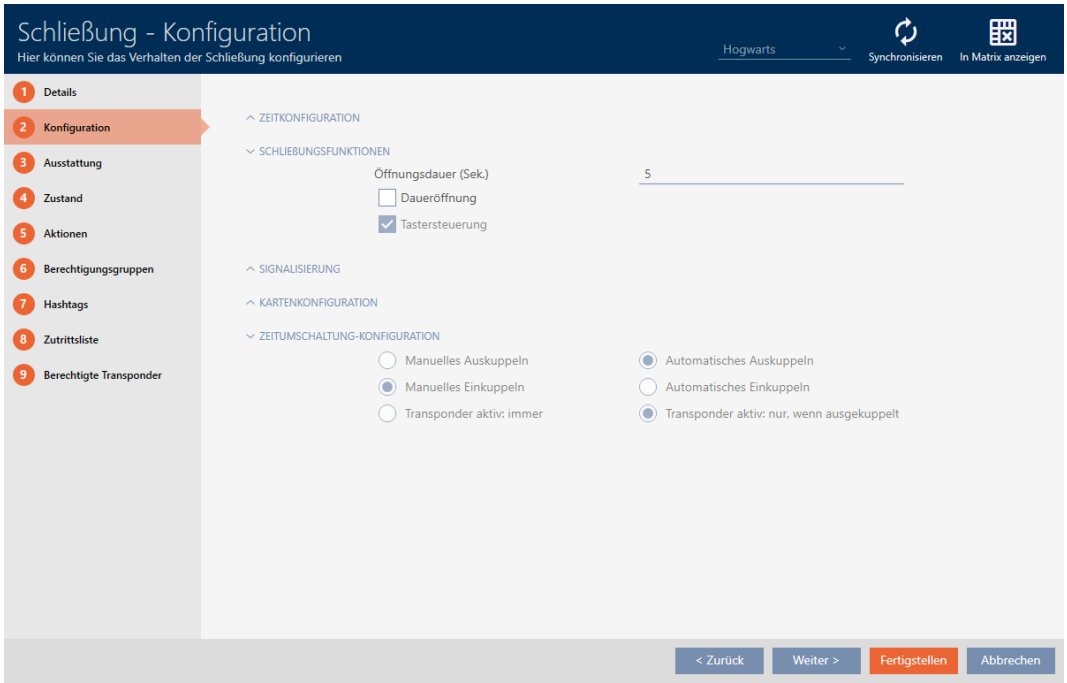
12. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
13. Klicken Sie auf die Tür, die mit der Zeitumschaltung gesteuert werden soll.
    ↳ Fenster der Schließung öffnet sich.



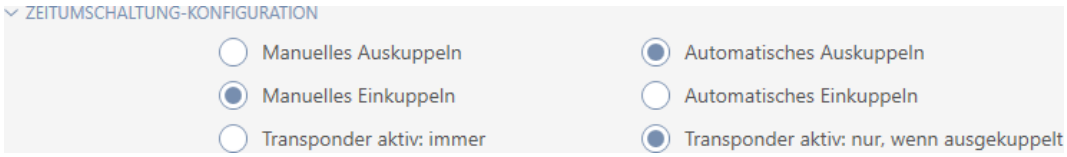
14. Klicken Sie auf den Reiter Konfiguration.



↳ Fenster wechselt zum Reiter "Konfiguration".



15. Stellen Sie im Ausklappmenü "Zeitumschaltung-Konfiguration" das gewünschte Verhalten ein (siehe *Zeitumschaltungen [▸ 552]*).



16. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster der Schließung schließt sich.

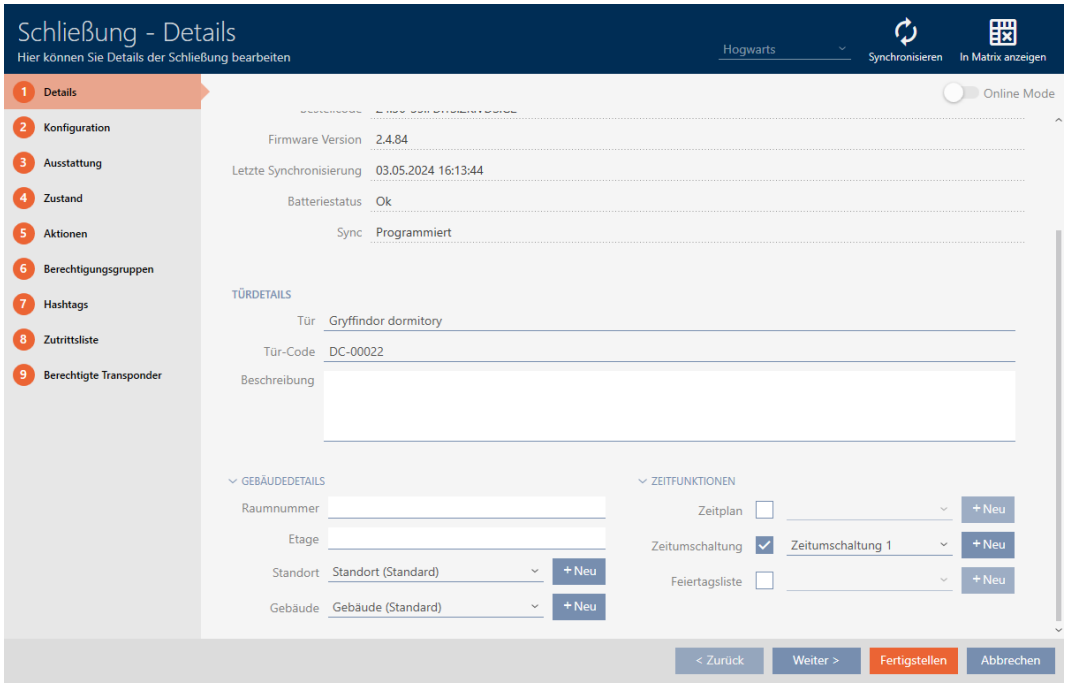
↳ Zeitumschaltung ist eingerichtet.

16.10 Zugänge durch Schließung protokollieren lassen (Zutrittsliste)

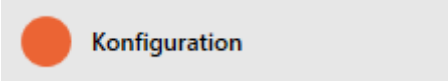
Hier schalten Sie die Zutrittsliste ein. Damit protokolliert Ihre Schließung, welche Identmedien betätigt wurden (siehe auch *Begehungs- und Zutrittslisten [▸ 547]*).

✓ Schließung mit .ZK-Option ausgestattet.

1. Klicken Sie auf die Schließung, die Zugänge protokollieren soll.
   ↳ Fenster der Schließung öffnet sich.

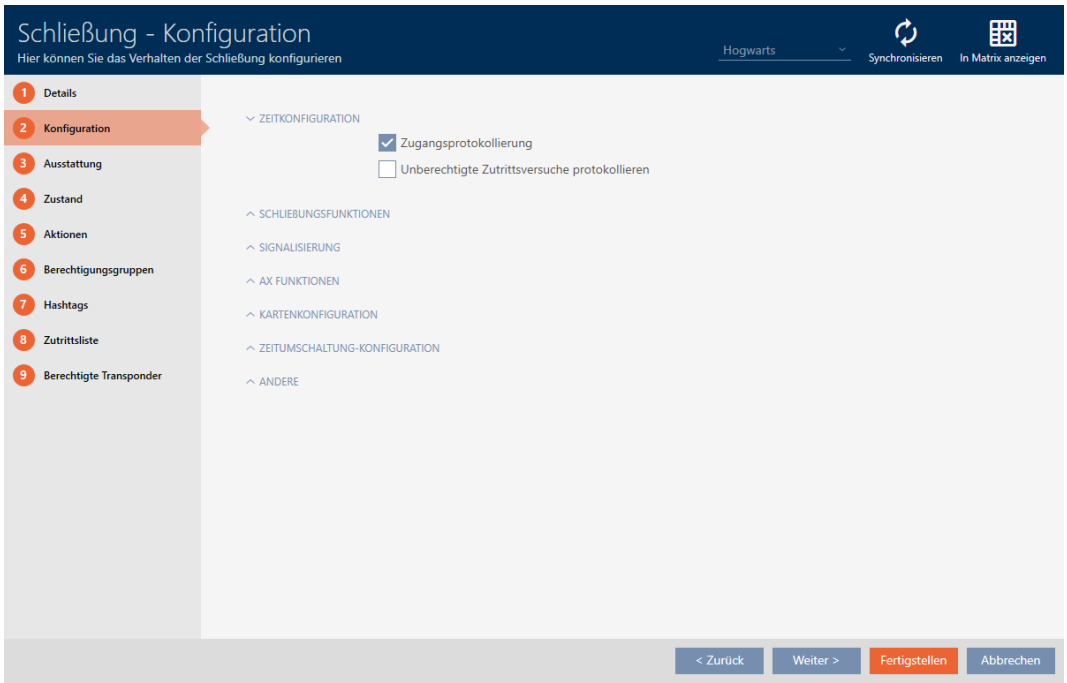


2. Klicken Sie auf den Reiter Konfiguration.



↳ Fenster wechselt zum Reiter "Konfiguration".

3. Klappen Sie das Menü "ZEITKONFIGURATION" auf (nur bei .ZK-Schließungen angezeigt).



4. Aktivieren Sie die Checkbox ☑ Zugangsprotokollierung (standardmäßig für .ZK-Schließungen aktiviert).

5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Zugangsprotokollierung für diese Schließung aktiviert.

Die protokollierten Zugänge werden bei der Synchronisation ausgelesen (siehe *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).

Danach ist die Zutrittsliste in dem Fenster der Schließung über den Reiter [Zutrittsliste] abrufbar (siehe *Zutrittsliste einer Schließung anzeigen und exportieren [▸ 421]*).

16.11 Schließung länger, kürzer oder dauerhaft öffnen lassen

In der Werkseinstellung programmiert die AXM Plus Ihre Schließungen so, dass sie für 5 Sekunden einkuppeln. Ihnen stehen aber auch andere Einstellungen zur Verfügung:

- Impulsöffnung zwischen 0 s und 25 s: Nach der Betätigung eines Identmediums bleibt die Schließung für diese Zeit eingekuppelt. Danach kuppelt sie von selbst wieder aus.
- Daueröffnung: Nach der Betätigung eines Identmediums kuppelt die Schließung ein und bleibt eingekuppelt. Erst wenn wieder ein Identmedium betätigt wird, dann kuppelt die Schließung aus.

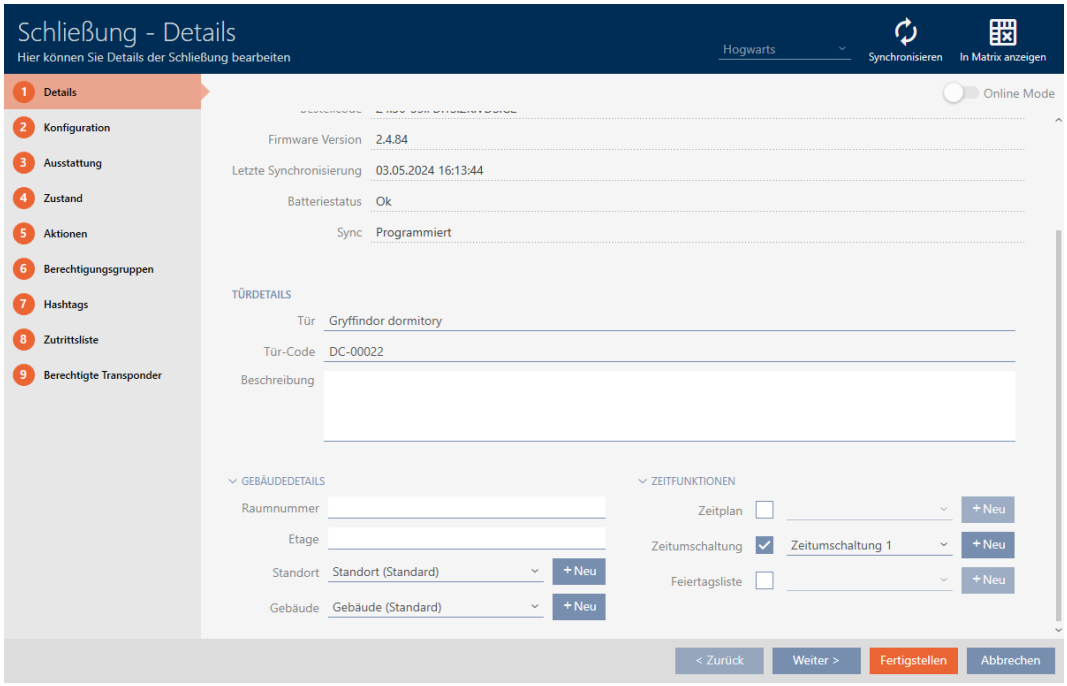
Außerdem können Sie noch mit Einstellungen arbeiten, die nicht schließungsbezogen sind:

- *Identmedium doppelt so lange öffnen lassen [▸ 121]*
- *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]*

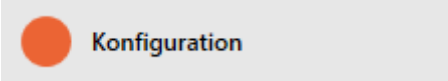
Dieses Kapitel beschreibt, wie Sie die Impulsdauer einstellen oder eine Daueröffnung aktivieren:

✓ Schließung erstellt.

1. Klicken Sie auf die Schließung, deren Öffnungsdauer Sie einstellen wollen.
   ↳ Fenster der Schließung öffnet sich.

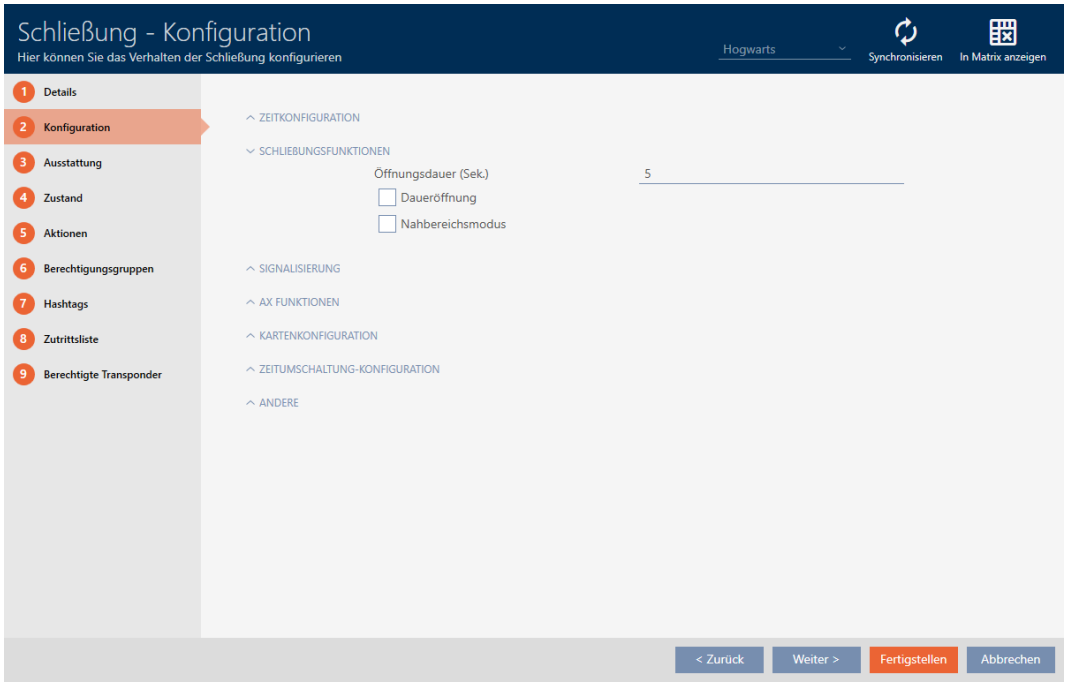


2. Klicken Sie auf den Reiter Konfiguration.



↳ Fenster wechselt zum Reiter "Konfiguration".

3. Klappen Sie das Menü "Schließungsfunktionen" auf.
4. Geben Sie in das Feld *Öffnungsdauer (Sek.)* die gewünschte Einkupplungsdauer ein.



5. Aktivieren Sie alternativ die Checkbox ☑ Daueröffnung, um eine Dauer-öffnung einzurichten.
6. Klicken Sie auf die Schaltfläche Fertigstellen
   ↳ Fenster der Schließung schließt sich.

↳ Öffnungsdauer der Schließung ist eingestellt.

16.12 Lesereichweite der Schließung begrenzen (Nahbereichsmodus)

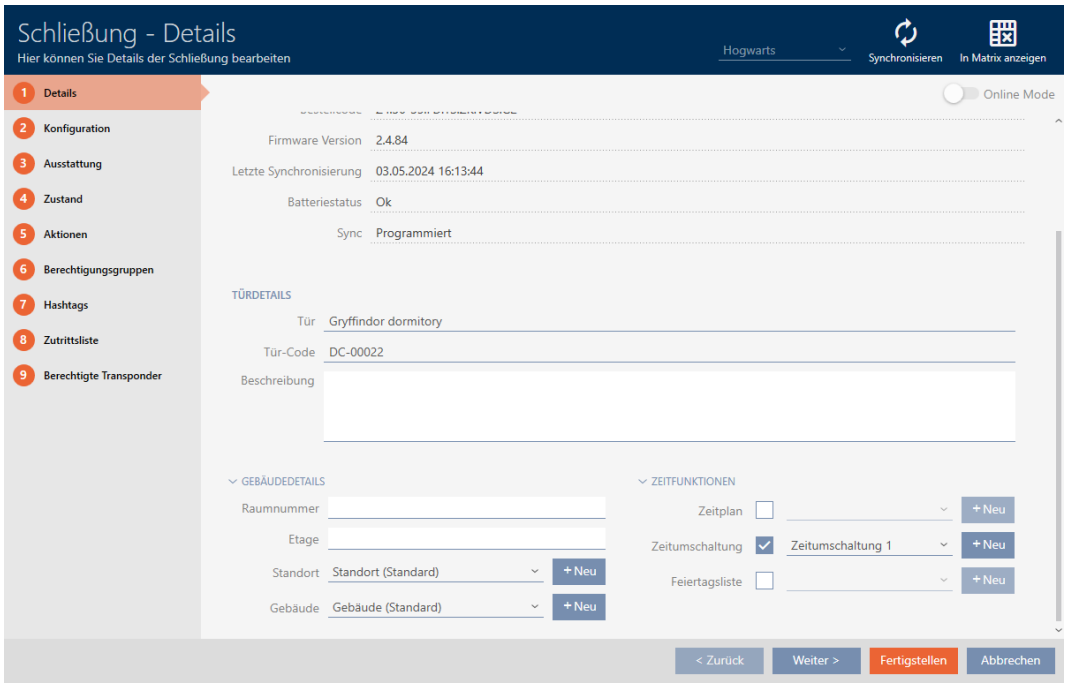
Der Nahbereichsmodus reduziert die Lesereichweite der Schließungen. Insbesondere der freidrehende Digital Cylinder AX muss im Nahbereichsmodus betrieben werden. Er ist mit zwei elektronischen Knäufen ausgestattet, die ohne Nahbereichsmodus zeitgleich angesprochen werden würden.

HINWEIS

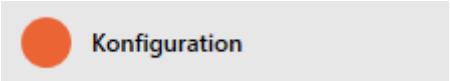
Nahbereichsmodus für freidrehende Digital Cylinder AX automatisch aktiviert

Sobald Sie die Option ☑ Freidrehend an einem Digital Cylinder AX aktivieren, wird die AXM Plus automatisch auch die Checkbox ☑ Nahbereichsmodus aktivieren.

1. Klicken Sie auf die Schließung, deren Lesereichweite begrenzt werden soll.
   ↳ Fenster der Schließung öffnet sich.

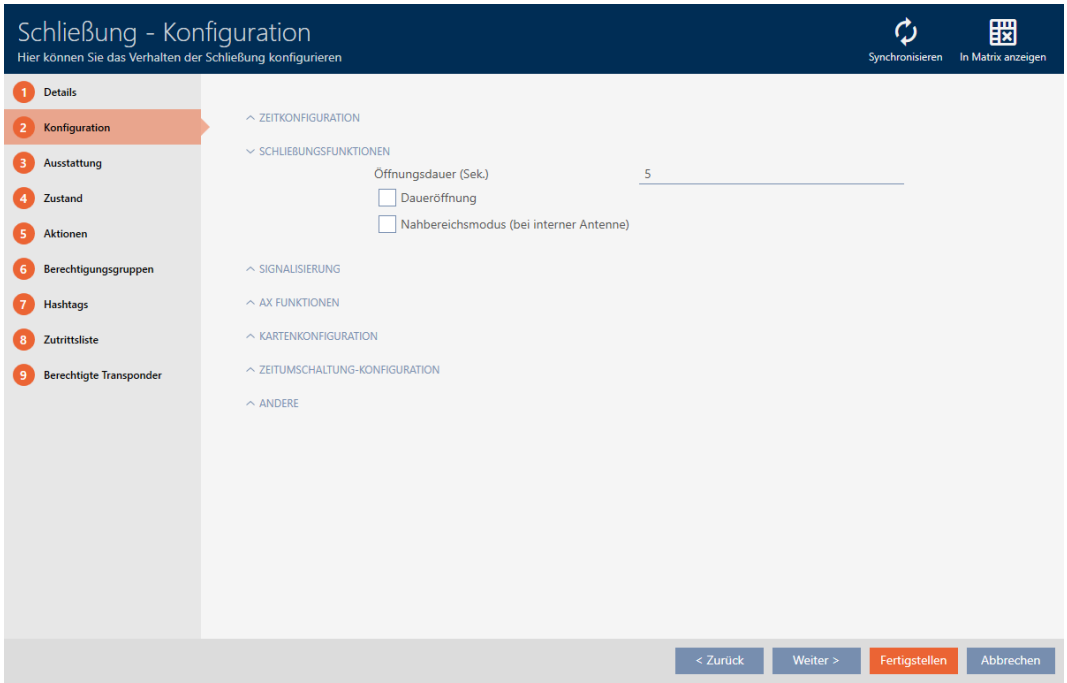


2. Klicken Sie auf den Reiter Konfiguration.



↳ Fenster wechselt zum Reiter [Konfiguration].

3. Klappen Sie das Menü "Schließungsfunktionen" aus.



4. Aktivieren Sie die Checkbox ☑ Nahbereichsmodus (nur bei geeigenten Schließungen angezeigt).
5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Nahbereichsmodus für diese Schließung aktiviert.

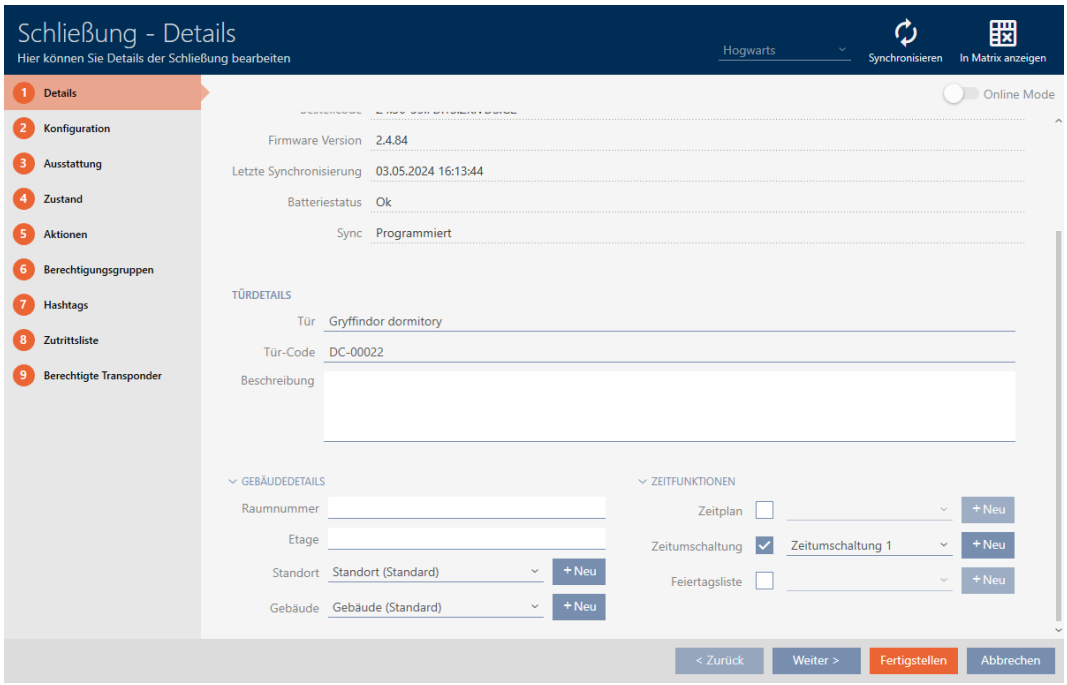
16.13 Schließung stummschalten (für Batteriewarnungen und Programmierungen)

In den Schließungseigenschaften können Sie folgende Signalisierungen deaktivieren:

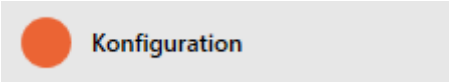
- Akustische und optische Batteriewarnungen
- Akustische Programmierquittungen

Wenn ein Identmedium betätigt wird, dann signalisiert die Schließung das Einkuppeln wie gehabt. Sie können aber auch für jedes Identmedium außer für PinCode-Tastaturen einstellen, dass Schließungen keine Betätigung dieses Identmediums signalisieren sollen (siehe *Für einen Transponder oder eine Karte alle Schließungen stummschalten [▸ 123]*).

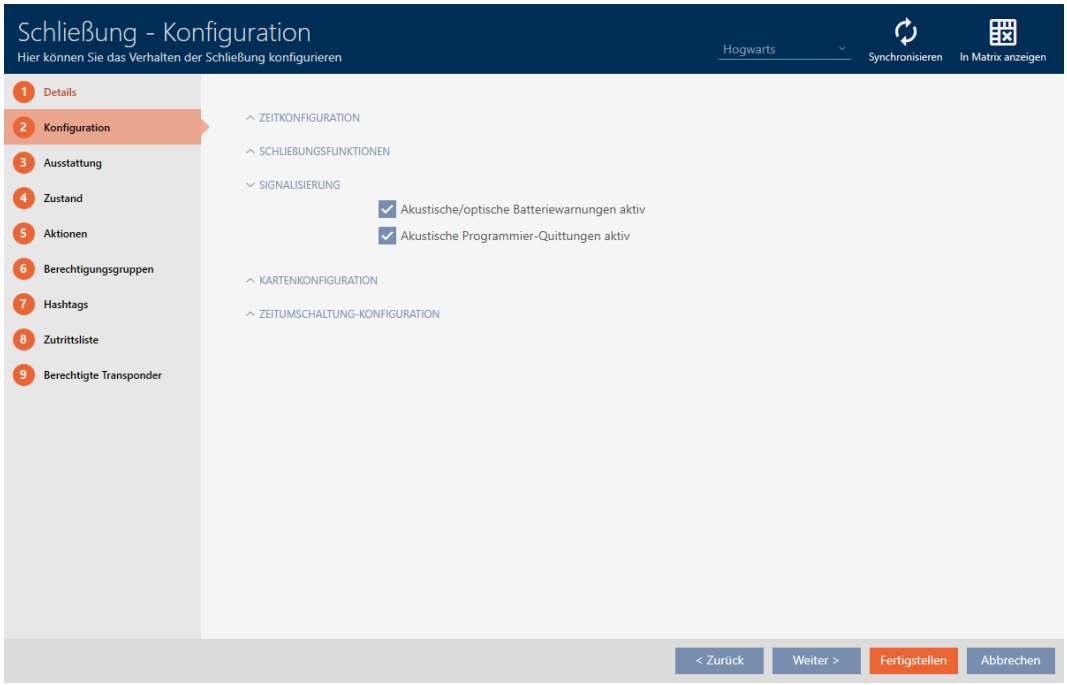
1. Klicken Sie auf die Schließung, die stummgeschaltet werden soll.
   ↳ Fenster der Schließung öffnet sich.



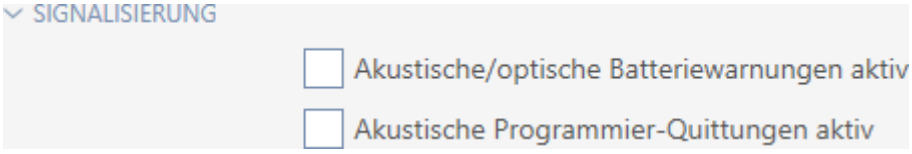
2. Klicken Sie auf den Reiter Konfiguration.



   ↳ Fenster wechselt zum Reiter [Konfiguration].
3. Klappen Sie das Menü "Signalisierung" aus.



4. Deaktivieren Sie die Checkboxen ☐ Akustische/optische Batteriewarnungen aktiv und ☐ Akustische Programmier-Quittungen aktiv.



5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Schließung wird keine Batteriewarnungen oder akustische Programmierquittungen mehr signalisieren.

16.14 Kartenleser aktivieren und deaktivieren

In der Werkseinstellung aktiviert die AXM Plus unter bestimmten Voraussetzungen den Kartenleser Ihrer Schließungen automatisch:

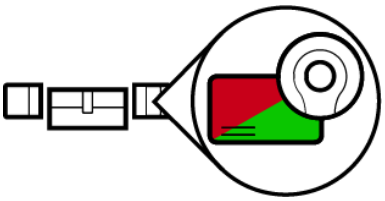
- Schließung befindet sich in einer passiven oder hybriden Schließanlage

  Der Kartenleser wird nur gebraucht, wenn in der Schließanlage auch Karten vorhanden sein können. In einer aktiven Schließanlage gibt es nur Transponder.

- Schließung hat einen eingebauten Kartenleser.

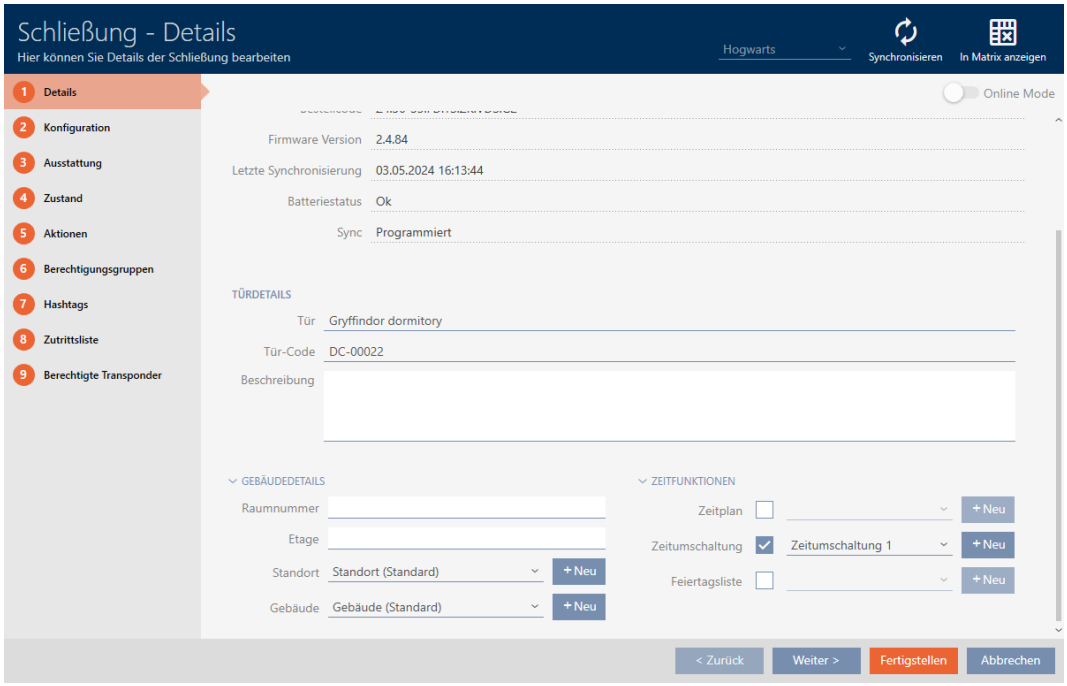
  Bei Schließungen ohne Kartenleser kann kein Kartenleser aktiviert werden.

Bei hybriden Schließungen in hybriden Schließanlagen kann es sein, dass die Schließung gar nicht mit einer Karte bedient werden muss. Mit Ihrer AXM Plus können Sie in diesem Fall den Kartenleser deaktivieren. So sparen Sie Strom und können die Batteriestandzeit verlängern.

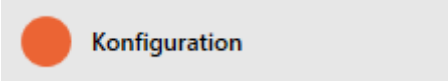


✓ Schließung erstellt.

1. Klicken Sie auf die Schließung, deren Kartenleser Sie aktivieren/deaktivieren wollen.
   ↳ Fenster der Schließung öffnet sich.

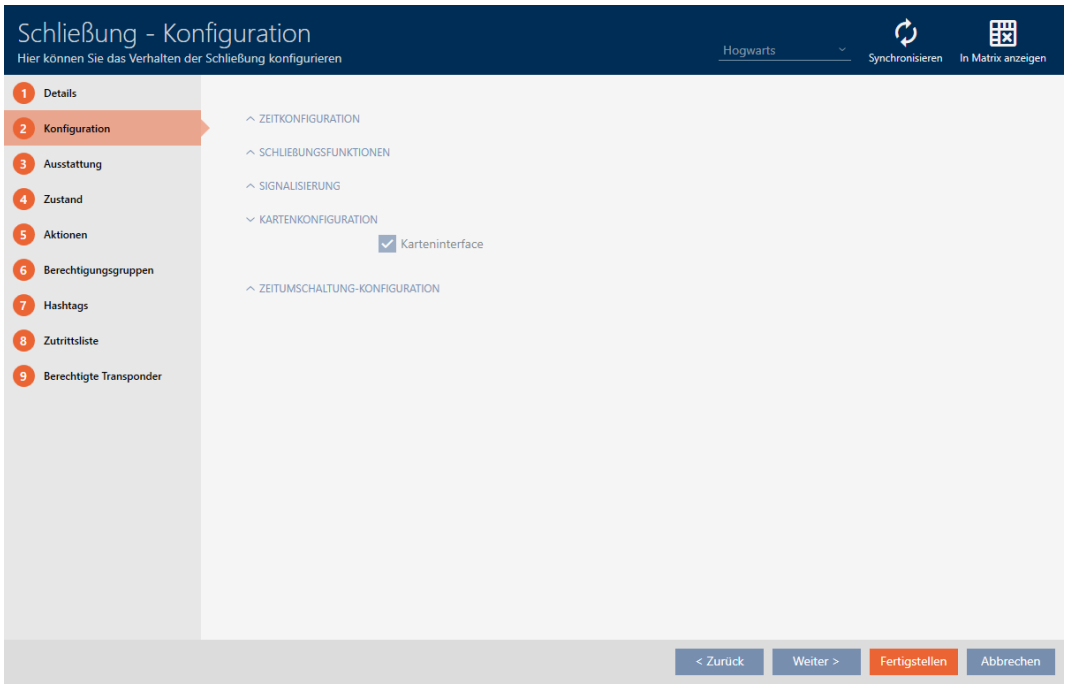


2. Klicken Sie auf den Reiter Konfiguration.



↳ Fenster wechselt zum Reiter "Konfiguration".

3. Klappen Sie das Menü "Kartenkonfiguration" auf.



4. Aktivieren bzw. deaktivieren Sie die Checkbox ☑ Karteninterface.

5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Kartenleser der Schließung ist aktiviert/deaktiviert.

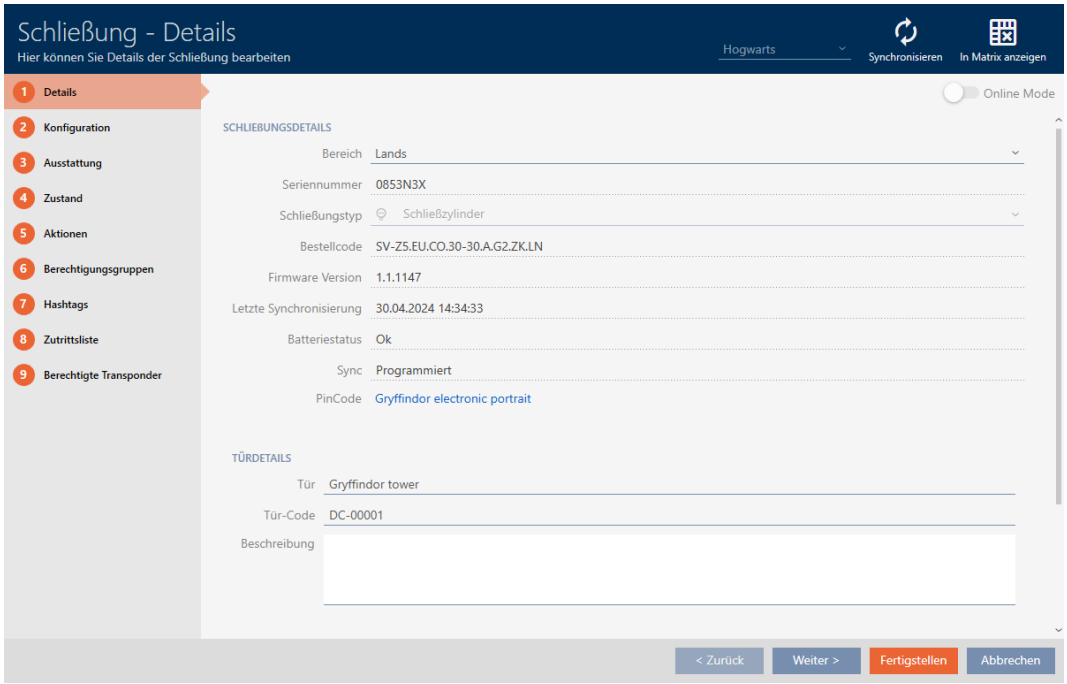
16.15 Aktivierungs- und Verfallsdatum von Identmedien ignorieren

In den Eigenschaften Ihrer Identmedien können Sie festlegen, dass diese zu einem bestimmten Datum aktiviert werden bzw. deaktiviert werden (siehe *Identmedium einmalig an bestimmten Zeitpunkten aktivieren oder deaktivieren (Aktivierungs- und Verfallsdatum) [▸ 126]*).

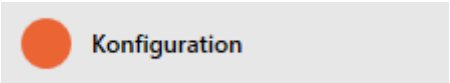
AX-Schließungen ignorieren dieses Aktivierungs- und Verfallsdatum auf Wunsch und akzeptieren dann betroffene Identmedien trotzdem.

✓ Schließung AX-basiert.

1. Klicken Sie auf die Schließung, die stummgeschaltet werden soll.
   ↳ Fenster der Schließung öffnet sich.

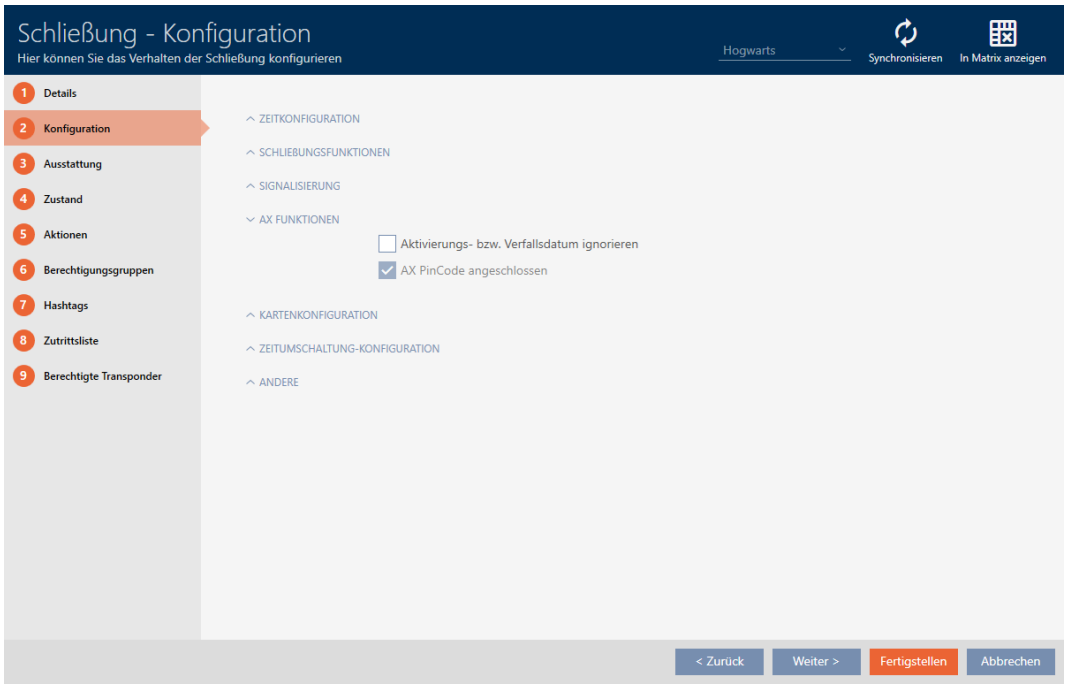


2. Klicken Sie auf den Reiter Konfiguration.

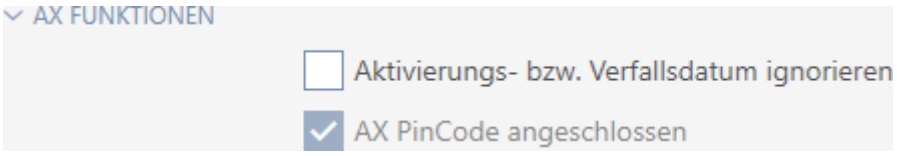


   ↳ Fenster wechselt zum Reiter [Konfiguration].

3. Klappen Sie das Menü "AX Funktionen" aus.



4. Aktivieren Sie die Checkbox ☑ Aktivierungs- bzw. Verfallsdatum ignorieren.



5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ Schließung lässt sich auch mit Identmedien betätigen, die nicht in ihrem Aktivierungszeitraum sind.

16.16 Türüberwachung (DoorMonitoring) einrichten

Mit DoorMonitoring können Sie den Zustand Ihrer Schließungen und Türen überwachen (siehe auch *DoorMonitoring [▸ 570]*).

HINWEIS

DoorMonitoring ohne Direktvernetzung ("WaveNet") eingeschränkt verfügbar

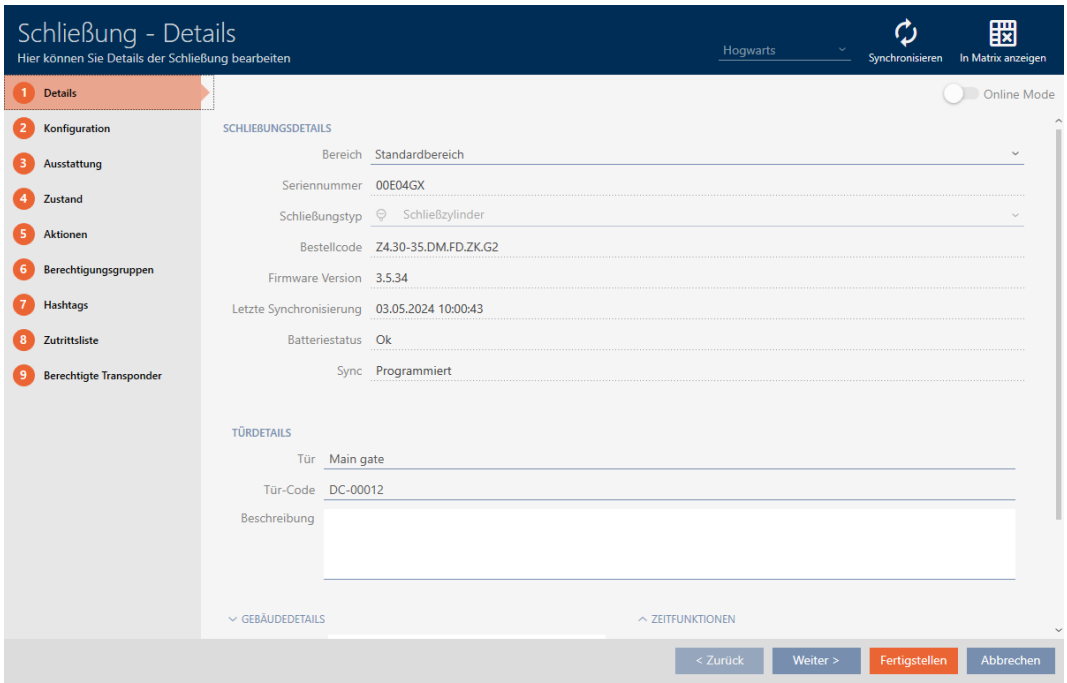
In einer direktvernetzten Schließanlage können Schließungen, die an das WaveNet angeschlossen sind, ihre DoorMonitoring-Ereignisse sofort über das Netzwerk übertragen. Sie sehen diese Ereignisse in kürzesteter Zeit in Ihrer Schließplansoftware (z.B. AXM).

Ohne WaveNet protokollieren Schließungen ihre DoorMonitoring-Ereignisse ebenfalls und speichern diese in der Zutrittsliste. Sie sehen diese Ereignisse erst nach dem Auslesen der Zutrittsliste in Ihrer Schließplansoftware.

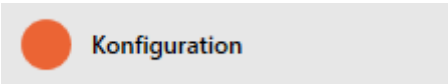
16.16.1 DoorMonitoring für Schließzylinder einrichten

✓ Schließung ist DoorMonitoring-fähig (Artikelnummer enthält .DM).

1. Klicken Sie auf die Schließung, für die Sie DoorMonitoring einrichten wollen.
   ↳ Fenster der Schließung öffnet sich.

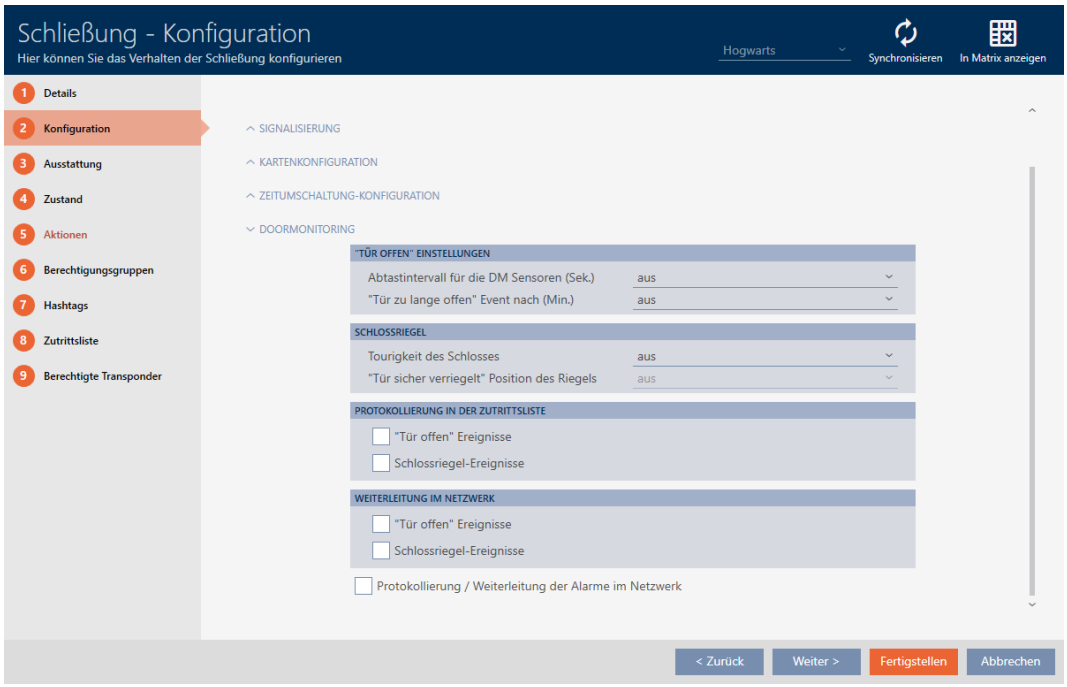


2. Klicken Sie auf den Reiter Konfiguration.



   ↳ Fenster wechselt zum Reiter [Konfiguration].

3. Klappen Sie das Menü "DoorMonitoring" aus.

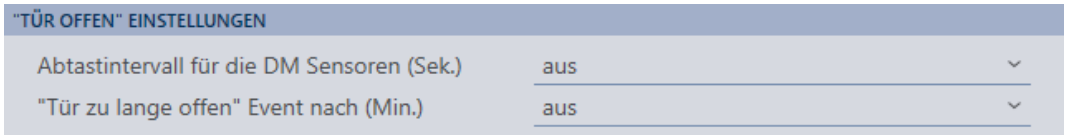


4. Nehmen Sie die gewünschten Einstellungen vor.
5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Schließung schließt sich.

↳ DoorMonitoring ist für diese Schließung eingerichtet.

Ihnen stehen folgende Einstellungen zur Auswahl:

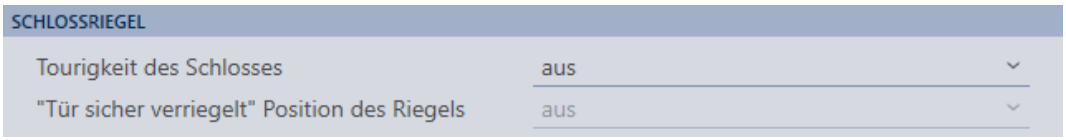
"Tür offen" Einstellungen



Mithilfe einer speziellen Stulpschraube und eines Magnetplättchens erkennen Ihre DoorMonitoring-Schließzylinder, ob die Tür offen oder geschlossen ist.

Einstellung	Erläuterung
Abtastintervall für die DM Sensoren (Sek.)	Die Häufigkeit, mit der Schließzylinder prüft, ob sich das Magnetplättchen vor der Stulpschraube befindet. In diesem Fall gilt die Tür als geschlossen. Mögliche Werte: ▪ 0.5 Sekunden ▪ 1.0 Sekunde ▪ 2.0 Sekunden ▪ 3.0 Sekunden ▪ 4.0 Sekunden ▪ 5.0 Sekunden ▪ 10.0 Sekunden Häufigere Überprüfungen führen zu einer schnelleren Erkennung einer geöffneten Tür, aber auch zu einem erhöhten Stromverbrauch.
"Tür zu lange offen" Event nach (Min.)	Sicherheitsrelevante Türen wie Brandschutztüren dürfen nicht dauerhaft geöffnet sein. Mit dieser Einstellung können Sie erkennen, ob eine Tür länger als üblich geöffnet ist. Diese Tür könnte z.B. verkeilt sein. Nach Ablauf der eingestellten Zeit löst das Ereignis Tür zu lange offen aus. Mögliche Zeiten: ▪ 0.2 Minuten ▪ 0.5 Minuten ▪ 1.0 Minute ▪ 2.0 Minuten ▪ 5.0 Minuten ▪ 8.0 Minuten

Schlossriegel



Mit einem speziellen Sensor erfasst Ihr DoorMonitoring-Schließzylinder, wie oft der Mitnehmer herumgedreht wurde. Zusammen mit den folgenden Einstellungen weiß das System dann, wie weit der Riegel herausgefahren ist.

Einstellung	Erläuterung
Tourigkeit des Schlosses	Die Anzahl der Umdrehungen, die erforderlich sind, um den Riegel des Einsteckschlosses vollständig aus-zufahren. Mögliche Werte: ▪ aus ▪ 1-tourig ▪ 2-tourig ▪ 3-tourig ▪ 4-tourig

Einstellung	Erläuterung
"Tür sicher verriegelt" Position des Riegels	Bei zwei- oder mehrtourigen Einsteckschlössern kann es sein, dass die Tür zwar verriegelt ist, aber der Riegel noch nicht so weit ausgefahren ist, dass er sicher in der Verankerung der Tür ruht. In diesem Fall gilt die Tür nur als Tür ist verriegelt, aber nicht als Tür ist sicher verriegelt. Mit dieser Einstellung legen Sie fest, wieviele Umdrehungen notwendig sind, bis der Riegel weit genug in der Tür ist und die Verriegelung als sicher gilt. Die verfügbaren Einstellungen hängen davon ab, was Sie bei Tourigkeit des Schlosses angegeben haben: ▪ aus ▪ 1 ▪ 2 ▪ 3 ▪ 4

Protokollierung in der Zutrittsliste

Sie können DoorMonitoring-Ereignisse in Ihrer Zutrittsliste mitprotokollieren. So können Sie DoorMonitoring in eingeschränktem Umfang auch ohne direkte Vernetzung nutzen.

Mit diesen Einstellungen legen Sie fest, welche Ereignisse in die Zutrittsliste Ihrer DoorMonitoring-Schließung geschrieben werden.

Einstellung	Erläuterung
"Tür offen" Ereignisse	Aktivieren Sie diese Checkbox, um "Tür offen" Ereignisse in die Zutrittsliste Ihrer Schließung zu schreiben. Das gilt für diese Ereignisse: ▪ Tür ist geöffnet ▪ Tür ist geschlossen ▪ Tür steht lange offen
Schlossriegel-Ereignisse	Aktivieren Sie diese Checkbox, um Schlossriegel-Ereignisse in die Zutrittsliste Ihrer Schließung zu schreiben. Das gilt für diese Ereignisse: ▪ Tür ist verriegelt ▪ Tür ist sicher verriegelt

Weiterleitung im Netzwerk

DoorMonitoring funktioniert am besten mit einer direkt vernetzten Anlage (WaveNet). Um die für Ihre Situation beste Einstellung zu finden, können Sie selbst festlegen, welche Ereignisse Sie über Ihr WaveNet an Ihre Datenbank weiterleiten.

Zusätzliche Weiterleitungen bedeuten erhöhten Funkverkehr und somit einen erhöhten Stromverbrauch.

Einstellung	Erläuterung
"Tür offen" Ereignisse	Aktivieren Sie diese Checkbox, um "Tür offen" Ereignisse an die Datenbank weiterzuleiten. Das gilt für diese Ereignisse: ▪ Tür ist geöffnet ▪ Tür ist geschlossen ▪ Tür steht lange offen Wenn Sie diese Checkbox aktivieren, werden die Ereignisse automatisch auch in die Zutrittsliste gespeichert.
Schlossriegel-Ereignisse	Aktivieren Sie diese Checkbox, um Schlossriegel-Ereignisse an die Datenbank weiterzuleiten. Das gilt für diese Ereignisse: ▪ Tür ist verriegelt ▪ Tür ist sicher verriegelt Wenn Sie diese Checkbox aktivieren, werden die Ereignisse automatisch auch in die Zutrittsliste gespeichert.
Protokollierung / Weiterleitung der Alarme im Netzwerk	Ihre DoorMonitoring-Schließung erkennt diverse Alarmsituationen. Diese können Sie an Ihre Datenbank weiterleiten. Solche Situationen sind zum Beispiel: ▪ Tür zu lange offen ▪ Manipulationsversuch (z.B. Stulpschraube wurde manipuliert) ▪ Tür wurde geöffnet, obwohl sie als verriegelt oder sicher verriegelt gilt

16.17 SmartRelais-Einstellungen ändern

Sie sehen die Einstellungen für SmartRelais nur, wenn Sie:

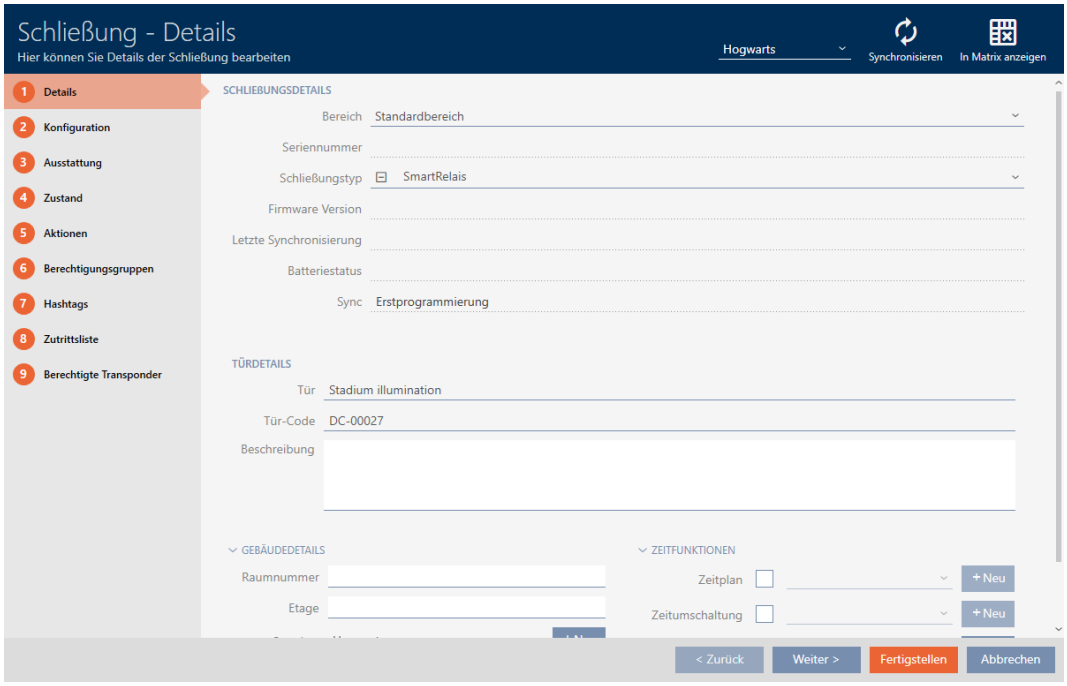
- Eine Schließung neu erstellen und noch nicht auf Fertigstellen geklickt haben oder

- Eine Schließung vom Typ "SmartRelais" geöffnet haben.

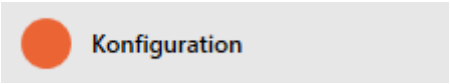
Alle Einstellungen des SmartRelais werden im Reiter "Konfiguration" geändert:

✓ Schließungsliste oder Matrixansicht geöffnet.

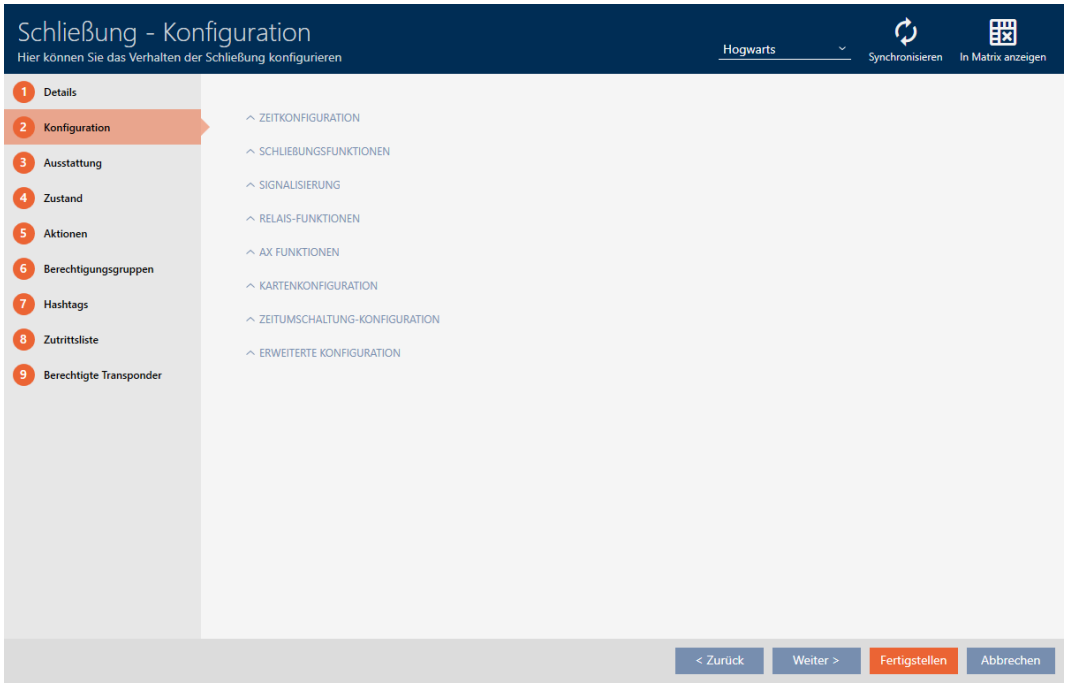
1. Klicken Sie auf das SmartRelais.
   ↳ Fenster des SmartRelais öffnet sich.



2. Klicken Sie auf den Reiter Konfiguration.



   ↳ Fenster wechselt zum Reiter "Konfiguration".



16.17.1 Interne und externe Antenne gleichzeitig verwenden

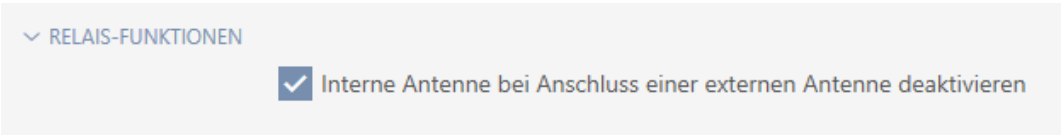
Für manche SmartRelais steht eine externe Antenne zur Verfügung (SREL.AV).

Normalerweise wird die interne Antenne deaktiviert, sobald das SmartRelais eine externe Antenne erkennt.

In der AXM Plus können Sie aber auch einstellen, dass beide Antennen gleichzeitig verwendet werden:

✓ Reiter "Konfiguration" geöffnet (siehe *SmartRelais-Einstellungen ändern [▸ 310]*).

1. Klappen Sie ggfs. das Menü "Relais-Funktionen" aus.



2. Deaktivieren Sie die Checkbox ☐ Interne Antenne bei Anschluss einer externen Antenne deaktivieren.
3. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des SmartRelais schließt sich.

↳ Interne Antenne des SmartRelais bleibt auch beim Anschluss einer externen Antenne aktiv.

16.17.2 Ausgänge invertieren

Ein Relais kennt zwei Zustände:

- Angezogen (Spule bestromt)
- Nicht angezogen (Ruhezustand)

Normalerweise befindet sich das Relais im Ruhezustand und zieht an, wenn ein Identmedium betätigt wird.

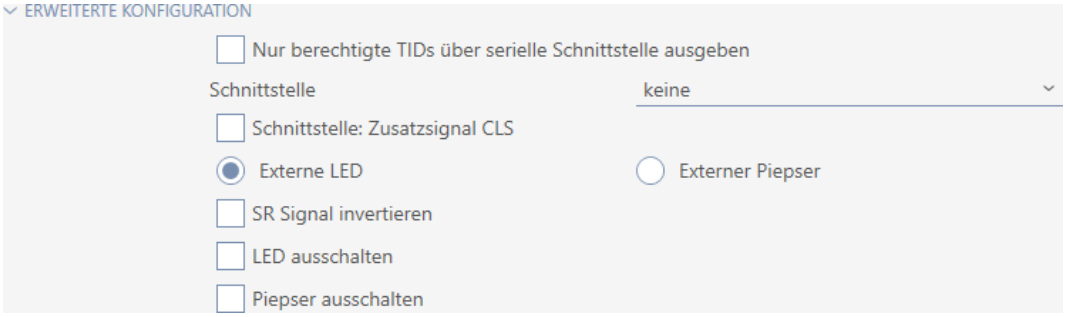
Je nach Art des Ausgangs (Schließer oder Wechselkontakt) ändert die Checkbox ☑ SR Signal invertieren das Verhalten des SmartRelais:

Wechselkontakt	Schließer
SREL SREL.ADV SREL.W SREL.G2 SREL.W.G2 SREL 3 SREL 3 Advanced SREL AX Classic	SREL2.G2
☐ SR Signal invertieren Identmedium betätigt: Relais zieht an, COM mit NO verbunden Identmedium nicht betätigt: Relais im Ruhezustand, COM mit NC verbunden	☐ SR Signal invertieren Identmedium betätigt: Relais zieht an, Kontakte verbunden Identmedium nicht betätigt: Relais im Ruhezustand, Kontakte nicht verbunden

Wechselkontakt	Schließer
☑ SR Signal invertieren ▪ Identmedium betätigt: Relais im Ruhezustand, COM mit NC verbunden ▪ Identmedium nicht betätigt: Relais zieht an, COM mit NO verbunden	☑ SR Signal invertieren ▪ Identmedium betätigt: Relais im Ruhezustand, Kontakte nicht verbunden ▪ Identmedium nicht betätigt: Relais zieht an, Kontakte verbunden

✓ Reiter "Konfiguration" geöffnet (siehe *SmartRelais-Einstellungen ändern [▸ 310]*).

1. Klappen Sie ggfs. das Menü "Erweiterte Konfiguration" aus.



2. Aktivieren Sie die Checkbox ☑ SR Signal invertieren.
3. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des SmartRelais schließt sich.

↳ Ausgänge des SmartRelais werden invertiert.

16.17.3 Serielle Schnittstelle verwenden

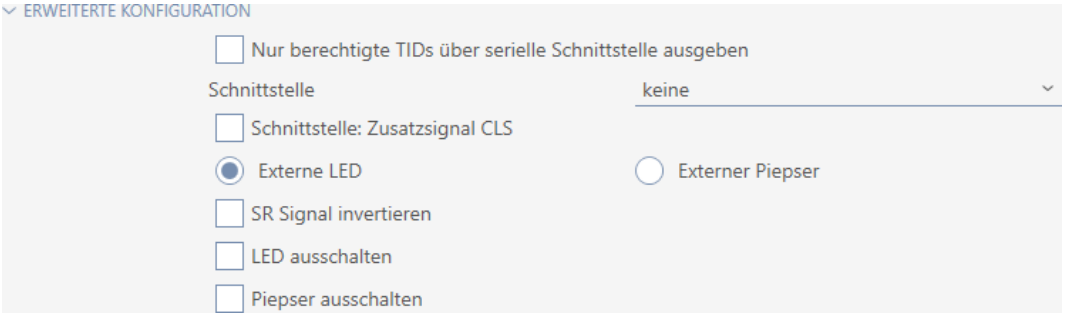
SmartRelais mit einer seriellen Schnittstelle können Daten von Identmedien an Fremdsysteme weitergeben. Folgende Systeme stehen zur Auswahl:

- "keine"
- "Wiegand 33-bit"
- "Wiegand 26-bit"
- "Primion"
- "Siemens"
- "Kaba Benzing"
- "Gantner Legic"
- "Isgus"

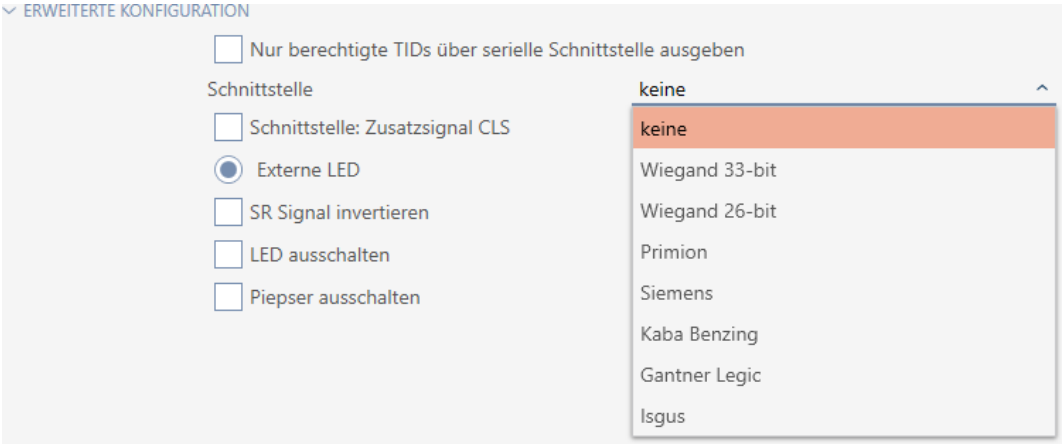
Stellen Sie dazu die serielle Schnittstelle so ein, dass Sie zum gewünschten Fremdsystem passt. Details zur Verkabelung finden Sie im Handbuch des jeweiligen SmartRelais.

✓ Reiter "Konfiguration" geöffnet (siehe *SmartRelais-Einstellungen ändern [▸ 310]*).

1. Klappen Sie ggfs. das Menü "Erweiterte Konfiguration" aus.



2. Wenn Sie unberechtigte Identmedien gar nicht erst an das Fremdsystem weitergeben wollen: Aktivieren Sie die Checkbox ☑ Nur berechtigte TIDs über serielle Schnittstelle ausgeben.
3. Wählen Sie im Dropdown-Menü ▼ **Schnittstelle** das Fremdsystem aus:"Wiegand 33-bit", "Wiegand 26-bit", "Primion", "Siemens", "Kaba Benzing", "Gantner Legic" oder "Isgus".



4. Wenn Sie für Ihr Fremdsystem ein Card-Load-Signal brauchen: Aktivieren Sie die Checkbox ☑ Schnittstelle: Zusatzsignal CLS.
5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des SmartRelais schließt sich.

↳ Serieller Anschluss des SmartRelais ist aktiviert.

16.17.4 Signalisierung ändern

Verschiedene Situationen können verschiedene Signalisierungen erfordern.

Deshalb können Sie in der AXM Plus die Signalisierung Ihres SmartRelais einstellen.

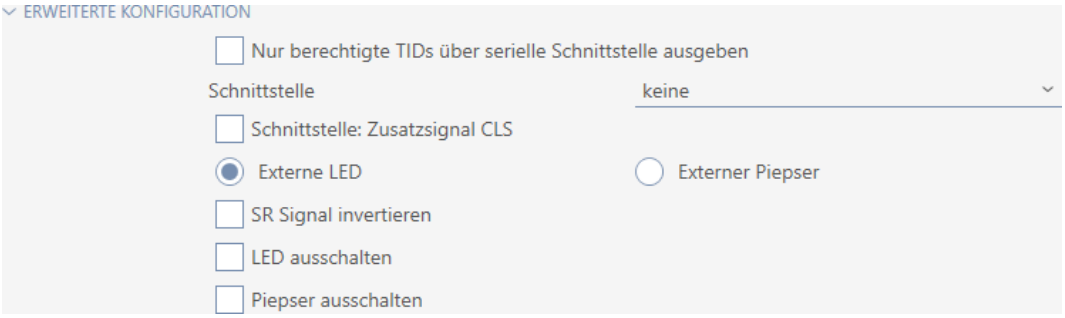
Am SREL.ADV und SREL2.G2 ist ein Anschluss für eine externe LED bzw. einen externen Piepser vorhanden. Details zum Anschluss finden Sie im jeweiligen SmartRelais-Handbuch.

Mit der Option ◉ Externe LED oder ◉ Externer Piepser stellen Sie ein, ob der Anschluss während einer Öffnung dauerhaft oder nur beim Umschalten nach Masse schaltet.

◉ Externe LED	◉ Externer Piepser
Anschluss schaltet während einer Öffnung dauerhaft gegen Masse. Die LED leuchtet, solange das SmartRelais geschalten ist.	Anschluss schaltet nur beim Umschalten. Der Piepser piepst nur, wenn das SmartRelais umschaltet. Ein dauerhaftes Piepsen wäre störend.

✓ Reiter "Konfiguration" geöffnet (siehe *SmartRelais-Einstellungen ändern [▸ 310]*).

1. Klappen Sie ggfs. das Menü "Erweiterte Konfiguration" aus.



2. Wählen Sie zwischen den Optionen ◉ Externe LED und ◉ Externer Piepser.
3. Schalten Sie ggfs. mit den Checkboxen ☑ LED ausschalten bzw. ☑ Piepser ausschalten die LED oder den Piepser Ihres SmartRelais aus (gilt auch für externe LEDs bzw. externe Piepser).
4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des SmartRelais schließt sich.

↳ Signalisierung des SmartRelais ist geändert.

16.18 Schließungs-Verwaltungsaufgaben planen und nachverfolgen

Die zentrale Anlaufstelle für die Verwaltung Ihrer Schließung ist der Reiter "Aktionen".

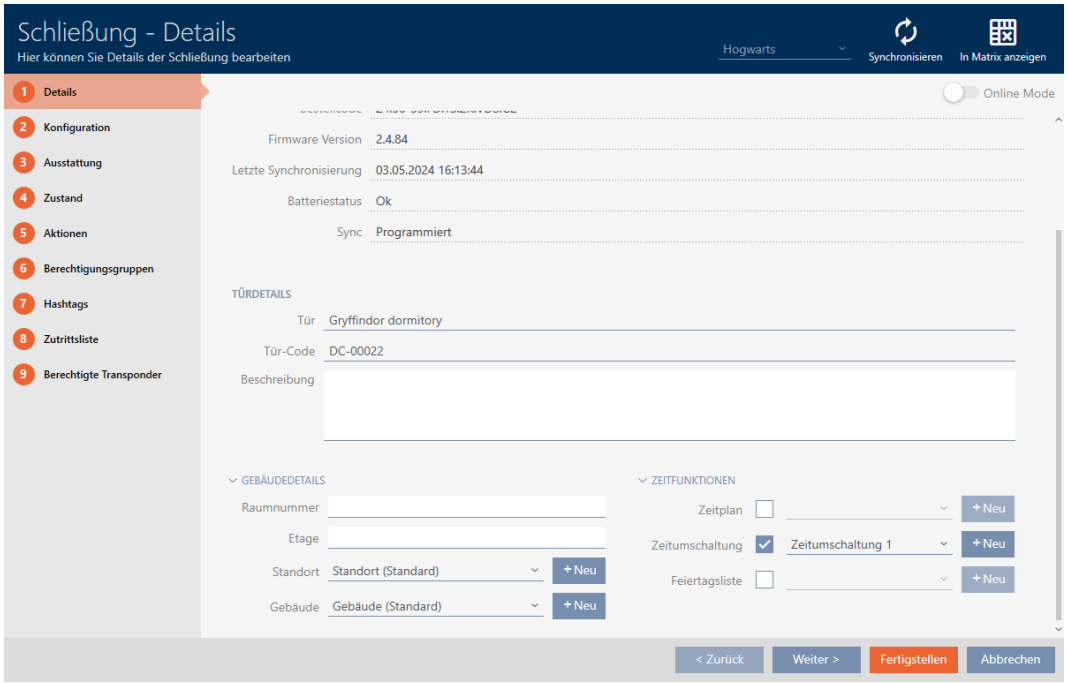
Hier werden folgende Einträge gesammelt angezeigt:

- Erstellt

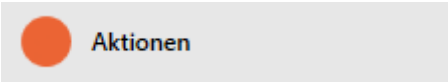
- Programmierung
- Eingebaut
- Ausgetauscht
- Ausgebaut
- Planmäßiger Batteriewechsel
- Letzter Batteriewechsel

✓ Schließung ist angelegt.

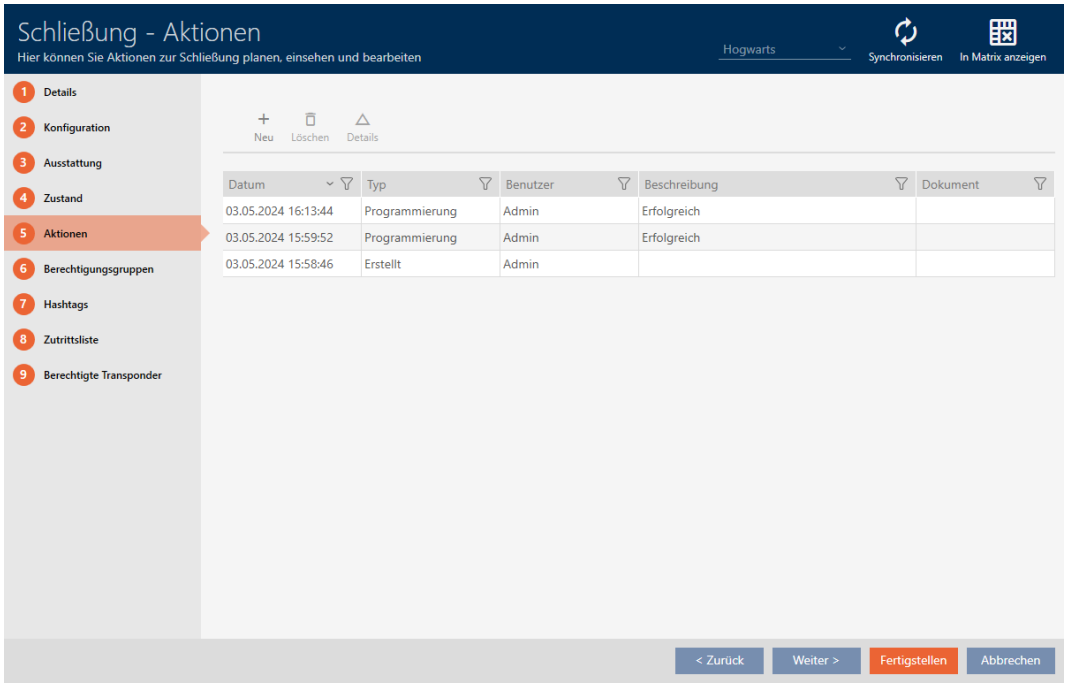
1. Klicken Sie auf die Schließung, die Sie verwalten wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klicken Sie auf den Reiter Aktionen.



   ↳ Fenster wechselt zum Reiter "Aktionen".

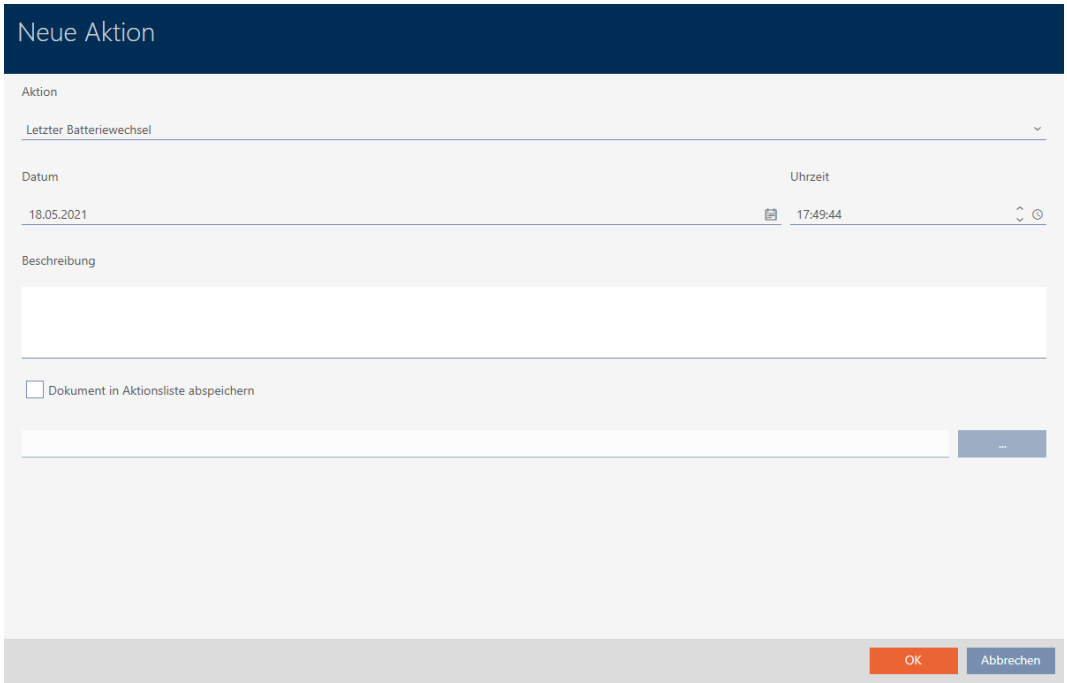


3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

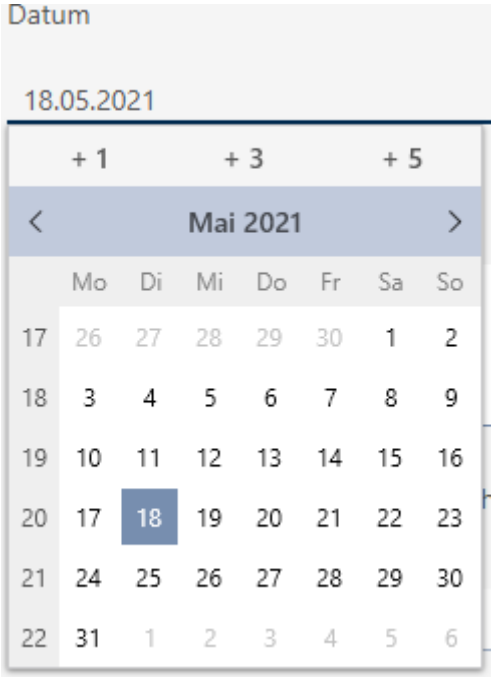
16.18.1 Einbau-, Austausch- oder Ausbaudatum notieren

✓ Fenster der Schließung zeigt Reiter "Aktionen" (siehe *Schließungs-Verwaltungsaufgaben planen und nachverfolgen [▸ 316]*).

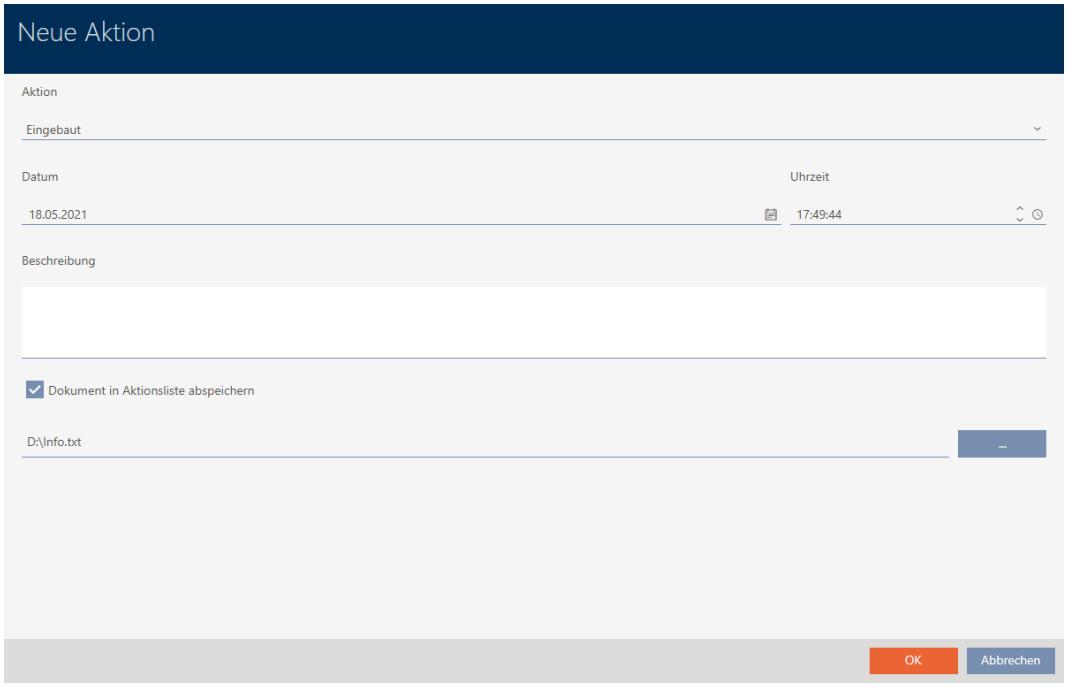
1. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster einer neuen Aktion öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Eingebaut", "Ausgetauscht" oder "Ausgebaut" aus.
3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.
7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

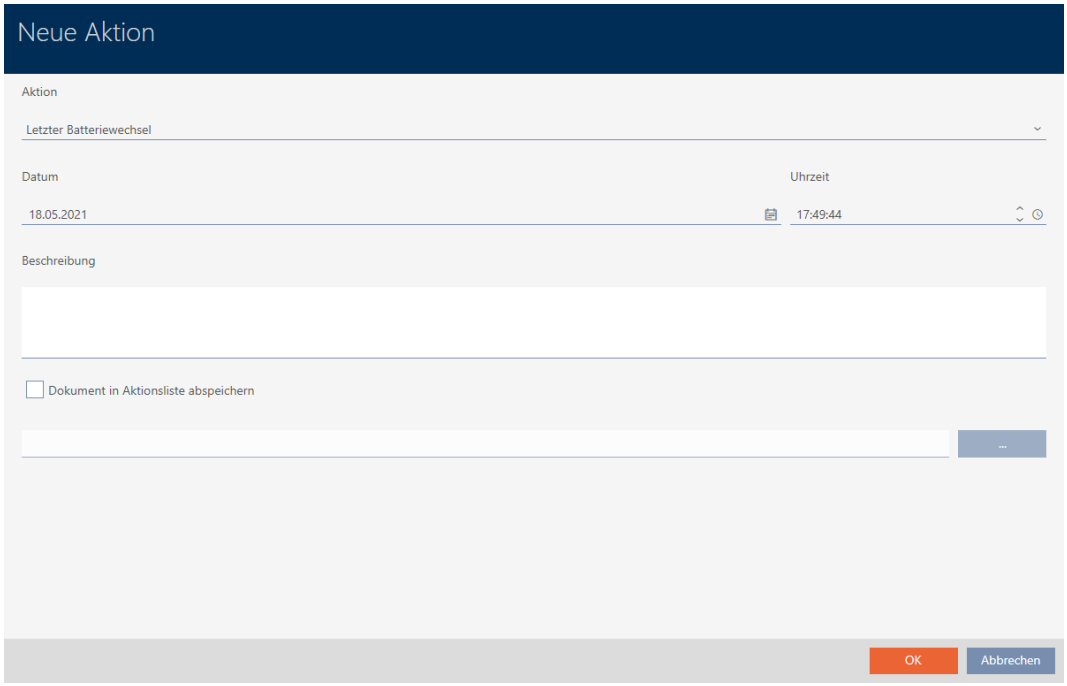
↳ Aktion ist erstellt und wird aufgelistet.

Datum	Typ	Benutzer	Beschreibung	Dokument
18.05.2021 17:49:44	Eingebaut	Admin		txt
18.05.2021 17:13:31	Programmierung	Admin		
29.04.2021 17:53:00	Planmäßiger Batteriewec	Admin		
29.04.2021 16:54:38	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 18:34:59	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 15:16:18	Erstellt	Admin		

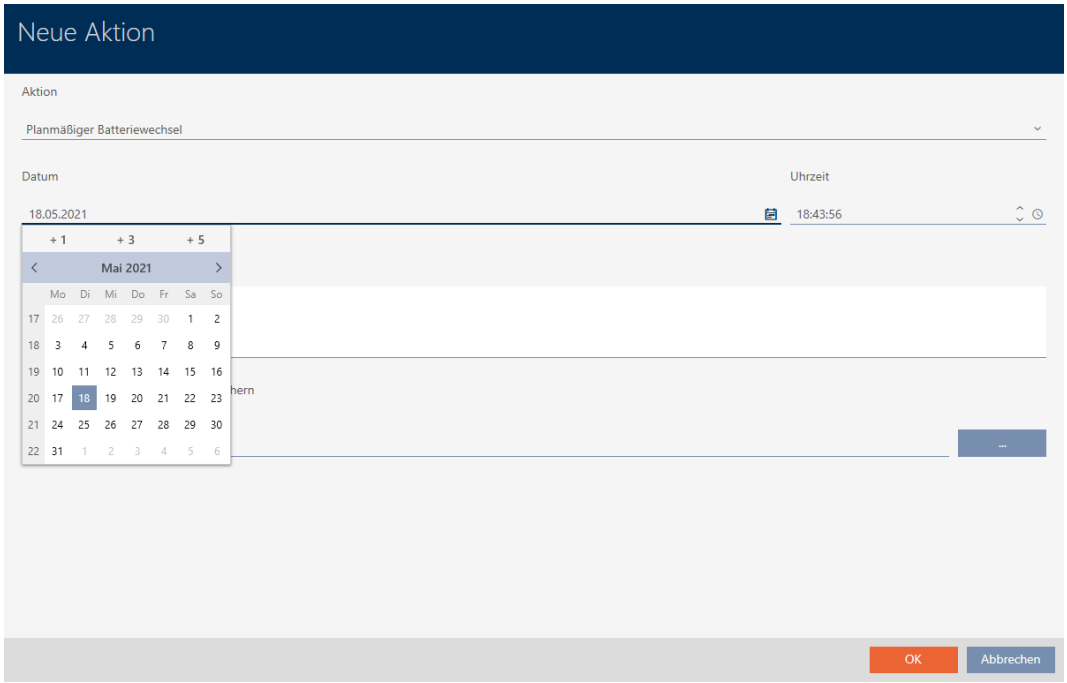
16.18.2 Batteriewechsel planen und protokollieren

✓ Fenster der Schließung zeigt Reiter "Aktionen" (siehe *Schließungs-Verwaltungsaufgaben planen und nachverfolgen [▸ 316]*).

1. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster einer neuen Aktion öffnet sich.

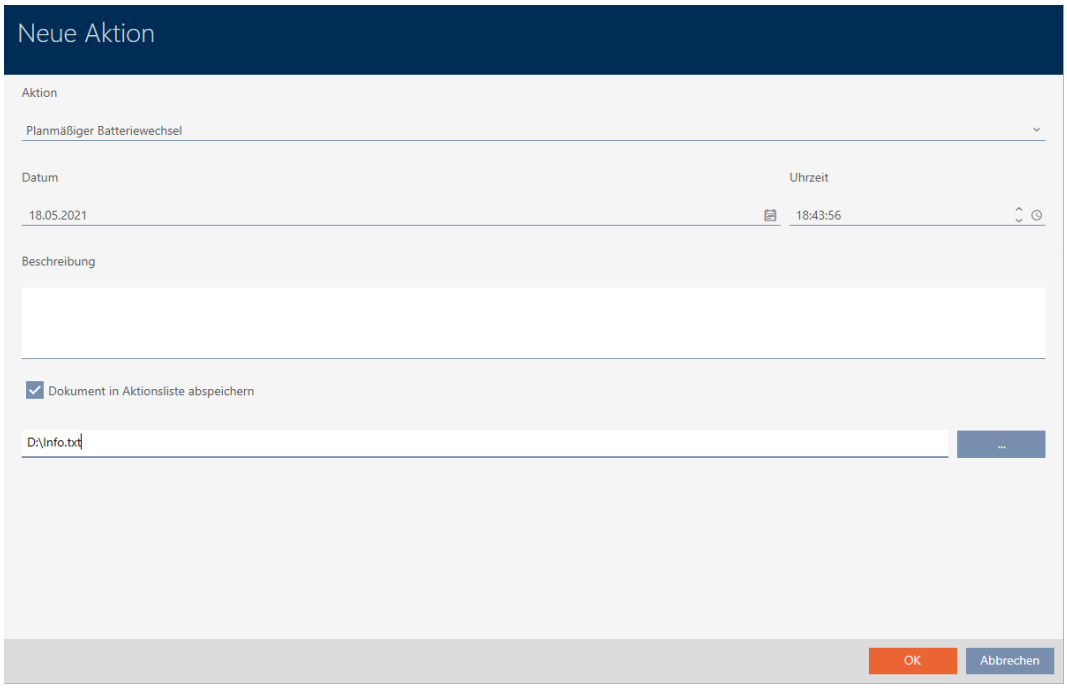


2. Wählen Sie im Dropdown-Menü ▼ **Aktion** den Eintrag "Planmäßiger Batteriewechsel" bzw. "Letzter Batteriewechsel" aus.
3. Geben Sie im Feld *Datum* ein Datum ein oder klicken Sie auf das Symbol , um eine Kalendermaske aufzuklappen.



4. Geben Sie im Feld *Uhrzeit* eine Uhrzeit ein.
5. Geben Sie im Feld *Beschreibung* optional eine Beschreibung ein.
6. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Aktivieren Sie die Checkbox ☑ Dokument in Aktionsliste abspeichern.

7. Wenn Sie ein Dokument zu Ihrer Aktion speichern wollen: Klicken Sie auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
8. Wählen Sie Ihr Dokument aus.
   ↳ Explorer-Fenster schließt sich.



9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster der neuen Aktion schließt sich.

↳ Aktion ist erstellt und wird aufgelistet.

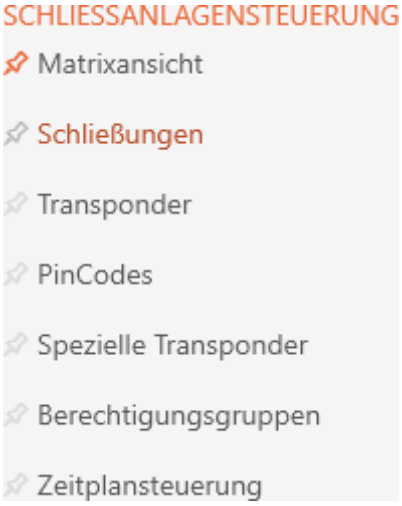
Datum	Typ	Benutzer	Beschreibung	Dokument
18.05.2021 18:43:56	Planmäßiger Batteriewec	Admin		txt
18.05.2021 17:49:44	Eingebaut	Admin		txt
18.05.2021 17:13:31	Programmierung	Admin		
29.04.2021 17:53:00	Planmäßiger Batteriewec	Admin		
29.04.2021 16:54:38	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 18:34:59	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 15:16:18	Erstellt	Admin		

16.19 Alle Schließungen eines Projekts anzeigen

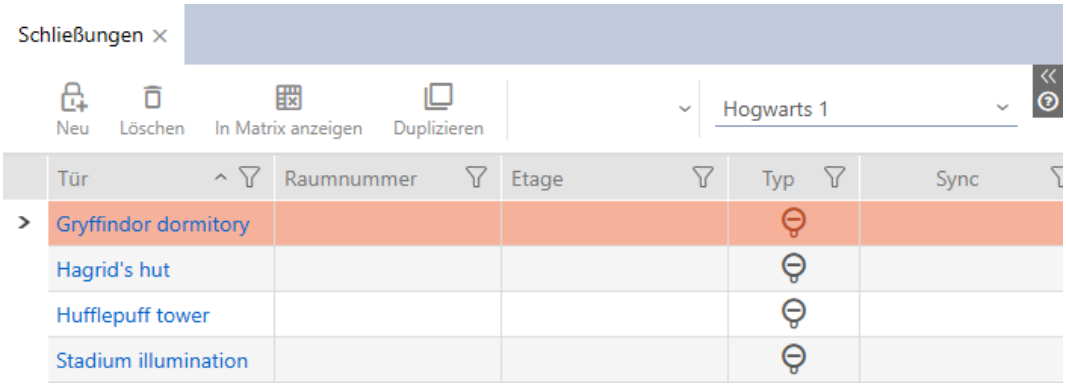
✓ Mindestens eine Schließung erstellt (siehe *Schließung erstellen* [▸ 238]).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

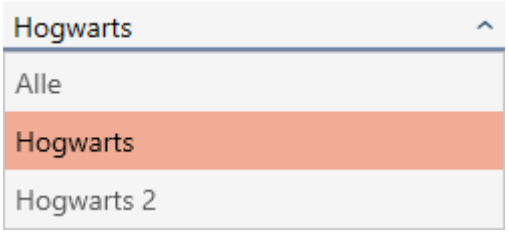
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Schließungen aus.



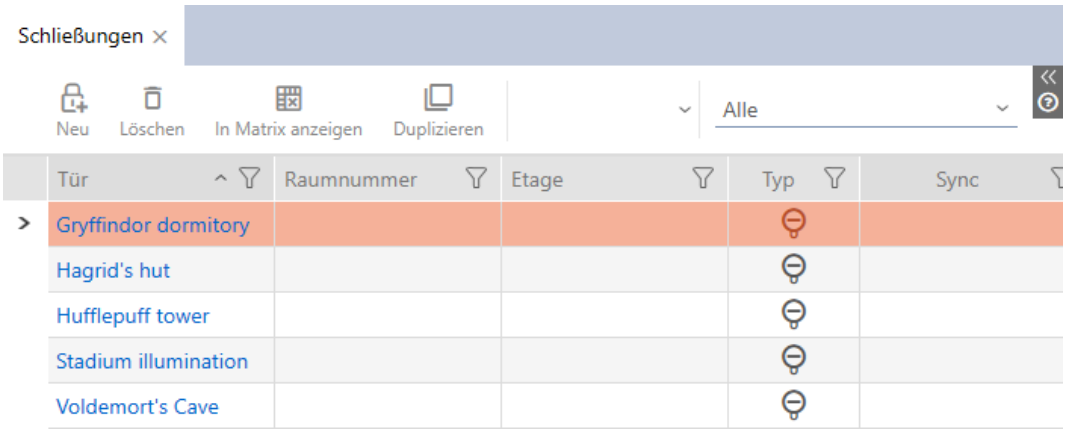
↳ AXM-Leiste klappt zu.
↳ Tab [Schließungen] öffnet sich.



3. Wählen Sie im Dropdown-Menü für die Schließanlage den Eintrag "Alle".



↳ Alle Schließungen aus allen Schließanlagen im gleichen Projekt werden angezeigt.



Die angezeigten Schließungen können Sie auch als Liste exportieren (siehe *Schließungen als Liste exportieren [▸ 324]*).

16.20 Schließungen als Liste exportieren

Alle Schließungen in Ihrer Schließanlage lassen sich als PDF exportieren.

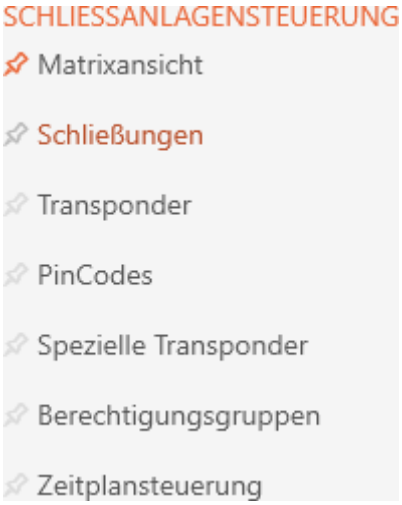
Im PDF werden genau dieselben Schließungen in genau derselben Reihenfolge wie in der AXM Plus angezeigt.

Das bedeutet, dass Sie die Anzeige vor dem Export sortieren und filtern können. Damit sortieren und filtern Sie auch die exportierte Liste.

✓ Schließung ist erstellt.

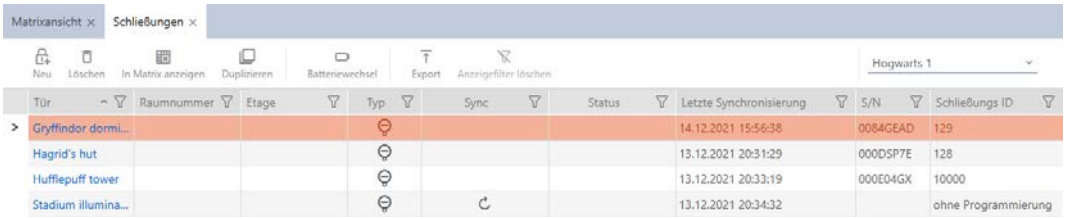
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Schließungen aus.



   ↳ Liste mit allen in der Schließanlage vorhandenen Schließungen öffnet sich.

3. Wechseln Sie ggfs. mit dem Dropdown-Menü zu einer anderen Schließanlage oder wählen Sie den Eintrag "Alle", um die Schließungen aller Schließanlagen anzuzeigen.



4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
5. Klicken Sie auf die Schaltfläche Export ⤒.
   ↳ Explorer-Fenster öffnet sich.
6. Speichern Sie die PDF-Datei in einem Dateiverzeichnis in der Wahl.

↳ Angezeigte Identmedien werden als PDF-Datei (DIN A4) exportiert.

Simons Voss technologies

Alle Schließungen für die Schließanlage 'Hogwarts 1'

Tür	Raumnummer	Etage	Typ	Sync	Status	S/N
Gryffindor dormitory			Schließzylinder	Programmiert		0084GEAD
Hagrid's hut			Schließzylinder	Programmiert		000DSP7E
Hufflepuff tower			Schließzylinder	Programmiert		000E04GX
Stadium illumination			Schließzylinder	Erstprogrammierung		

Simons Voss technologies Gedruckt am: 14.12.2021 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

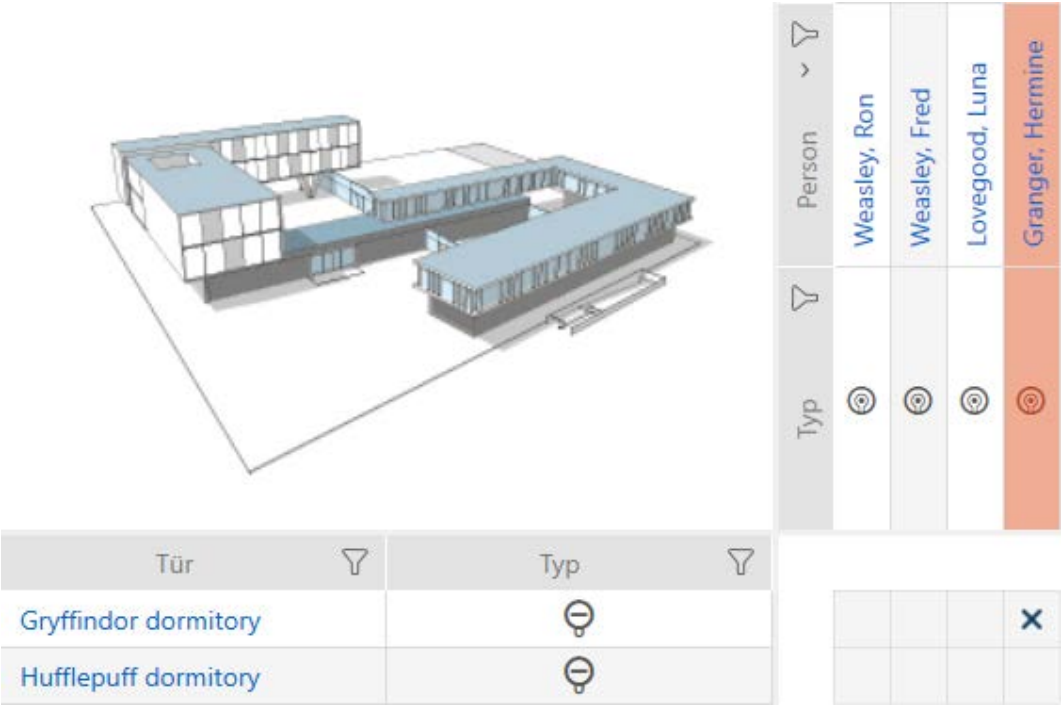
17. Berechtigungen

17.1 Einzelne Berechtigungen ändern (Kreuz)

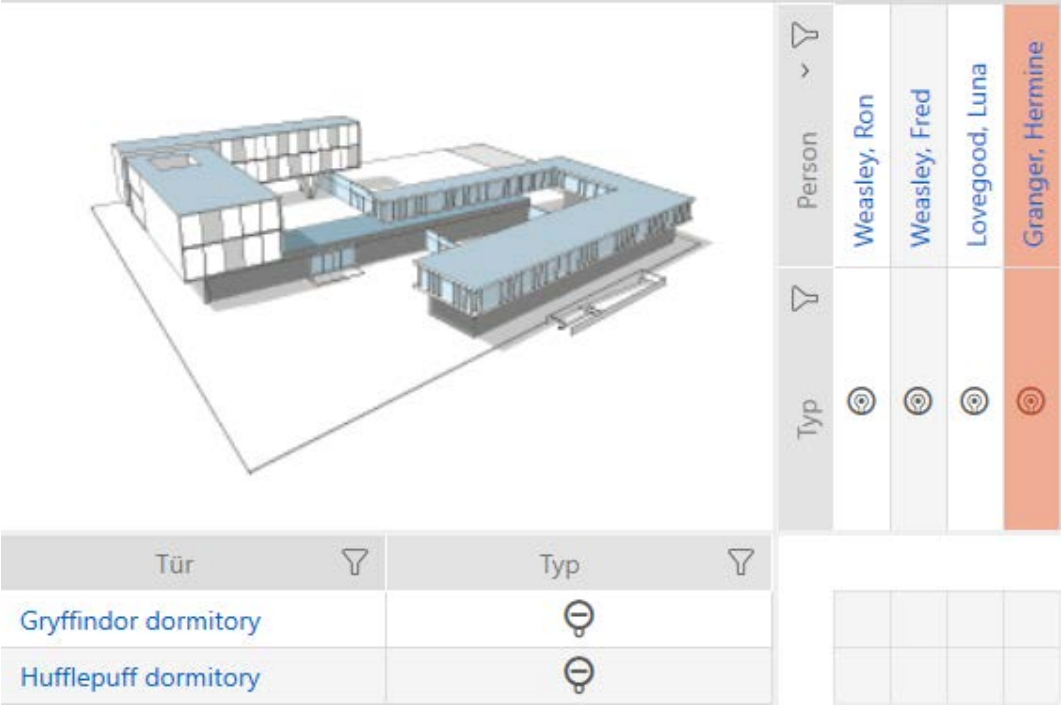
Einzelne Berechtigungen an einzelnen Türen vergeben Sie am schnellsten direkt in der Matrix.

✓ Matrixansicht geöffnet.

1. Klicken Sie auf ein Kästchen in der Matrix.
   ↳ Berechtigung wird für das entsprechende Identmedium (Spalte) an der entsprechenden Schließung (Zeile) vergeben.



2. Klicken Sie erneut auf dasselbe Kästchen.
   ↳ Berechtigung wird wieder entzogen.



↳ Einzelne Berechtigung ist vergeben bzw. entzogen.

HINWEIS

Geänderte Berechtigungen erst nach Synchronisation wirksam

Geänderte Berechtigungen sind zunächst nur in der Datenbank gespeichert und haben keinen Einfluss auf die realen Identmedien und Schließungen.

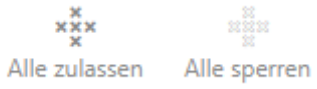
- Synchronisieren Sie die Identmedien und/oder die Schließungen, nachdem Sie Berechtigungen geändert haben.

Standardmäßig wird die Berechtigung nach einem einfachen Klick vergeben. Sie können aber einstellen, nach welchem Klick die Berechtigung vergeben wird (siehe *Klick für Berechtigungen ändern [▸ 454]*):

- Einfacher Mausklick
- Doppelklick
- Strg + einfacher Mausklick

17.2 Viele Berechtigungen ändern (an Identmedien und/oder Schließungen)

17.2.1 Alle zulassen oder alle sperren



Anstelle von einzelnen Berechtigungen können Sie auch:

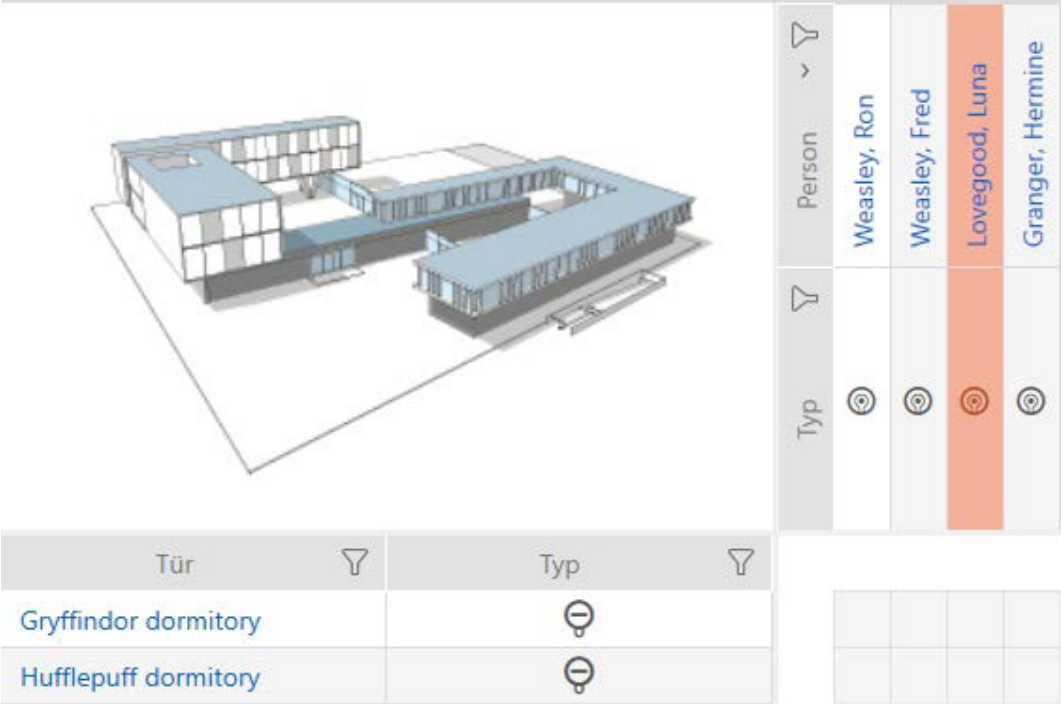
- Alle aktuell angezeigten Identmedien an einer Schließung zulassen oder sperren
- Ein Identmedium an allen aktuell angezeigten Schließungen zulassen oder sperren

Die Funktionen Alle zulassen und Alle sperren beziehen sich auf die angezeigten Identmedien bzw. Schließungen. Sie können also Filter einsetzen, um nur bestimmte Identmedien bzw. Schließungen zuzulassen.

Diese Beschreibung bezieht sich darauf, alle angezeigten Identmedien an einer Schließung zuzulassen. Analog funktioniert auch:

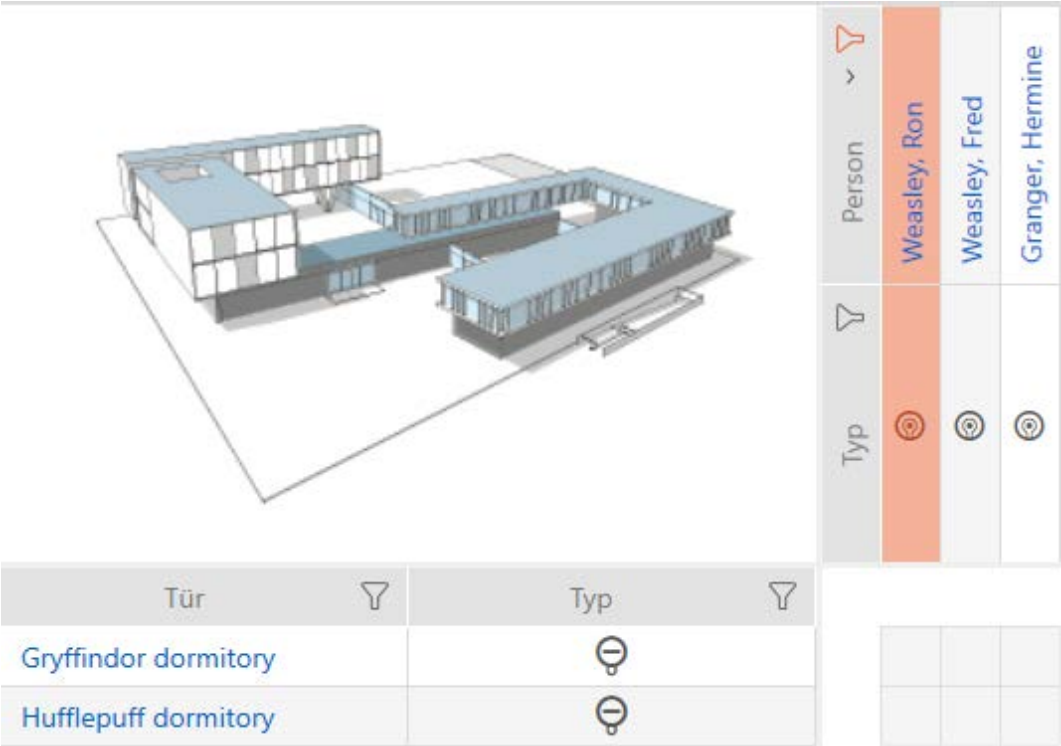
- Alle angezeigten Identmedien an einer Schließung sperren
- Ein Identmedium an allen aktuell angezeigten Schließungen zulassen
- Ein Identmedium an allen aktuell angezeigten Schließungen sperren

Ausgangssituation:

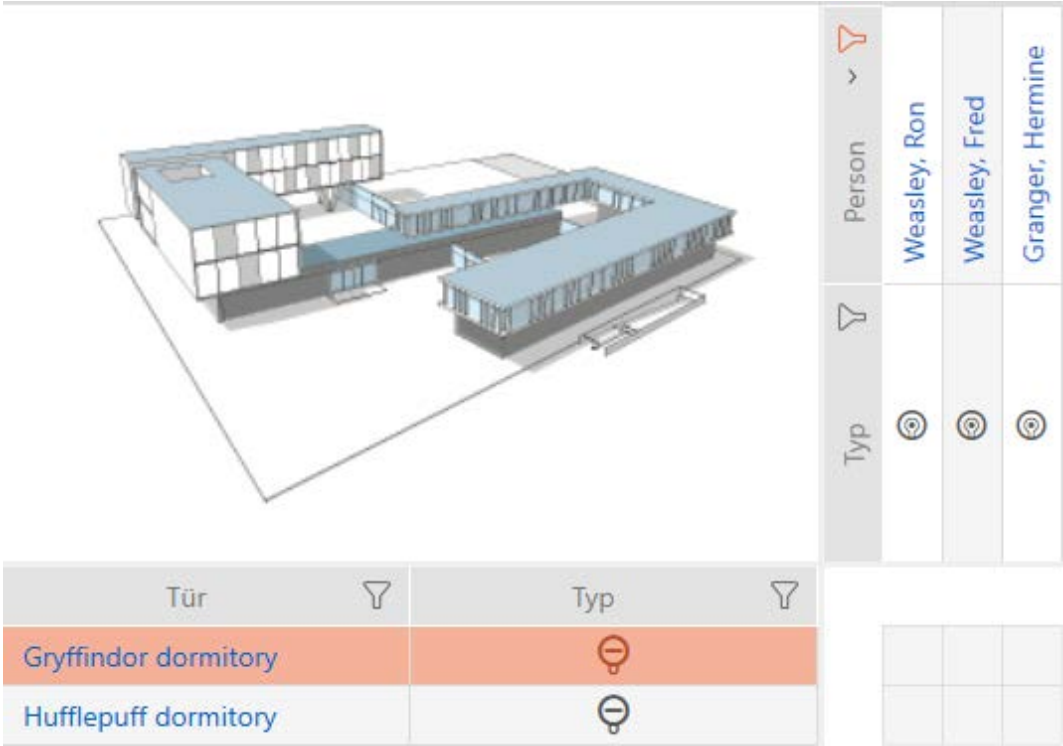


- ✓ Matrixansicht geöffnet.
- ✓ Identmedium vorhanden.
- ✓ Schließung vorhanden.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

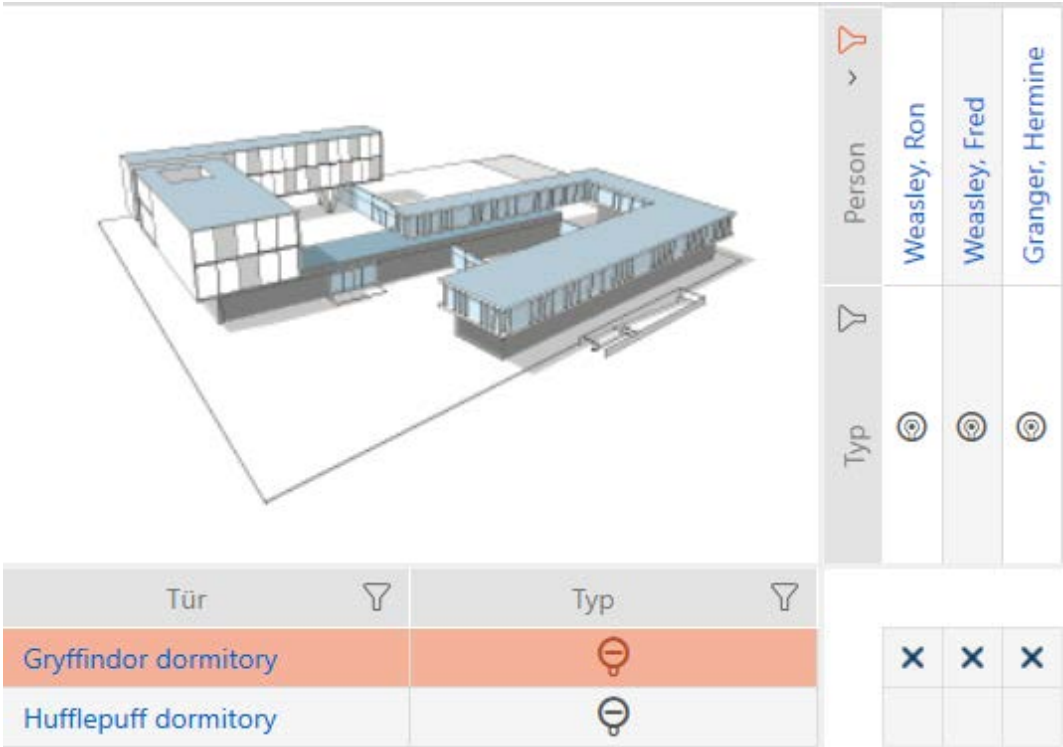


2. Markieren Sie die Schließung, an der Sie alle angezeigten Identmedien zulassen wollen.

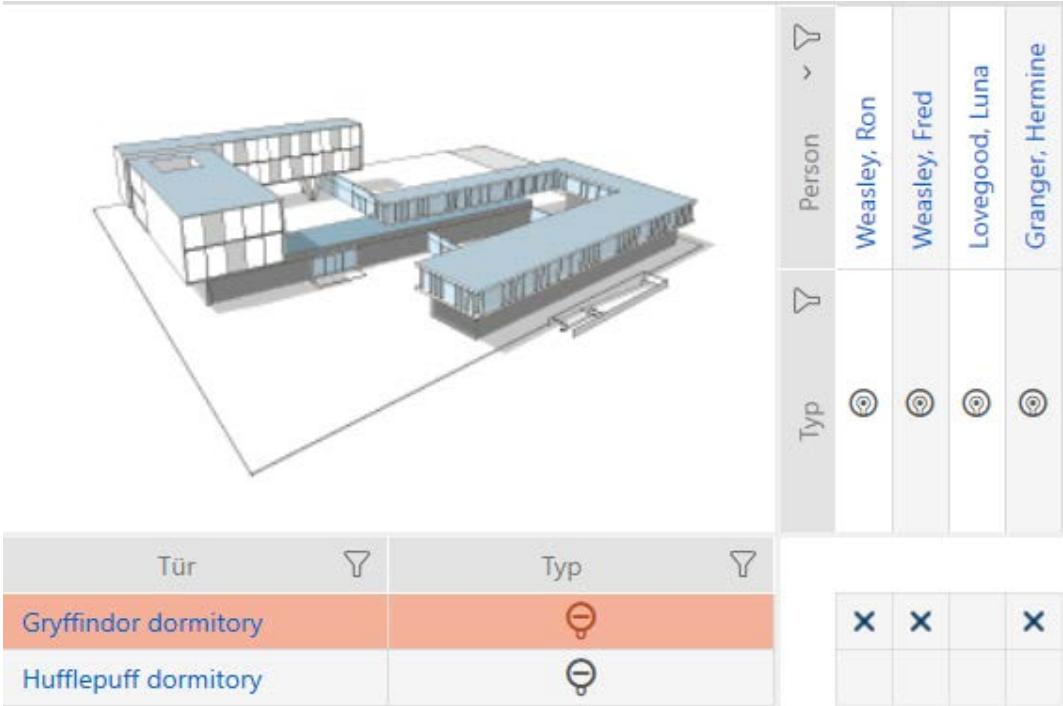


3. Klicken Sie auf die Schaltfläche Alle zulassen.

↳ Alle angezeigten Identmedien sind an der markierten Schließung zugelassen.



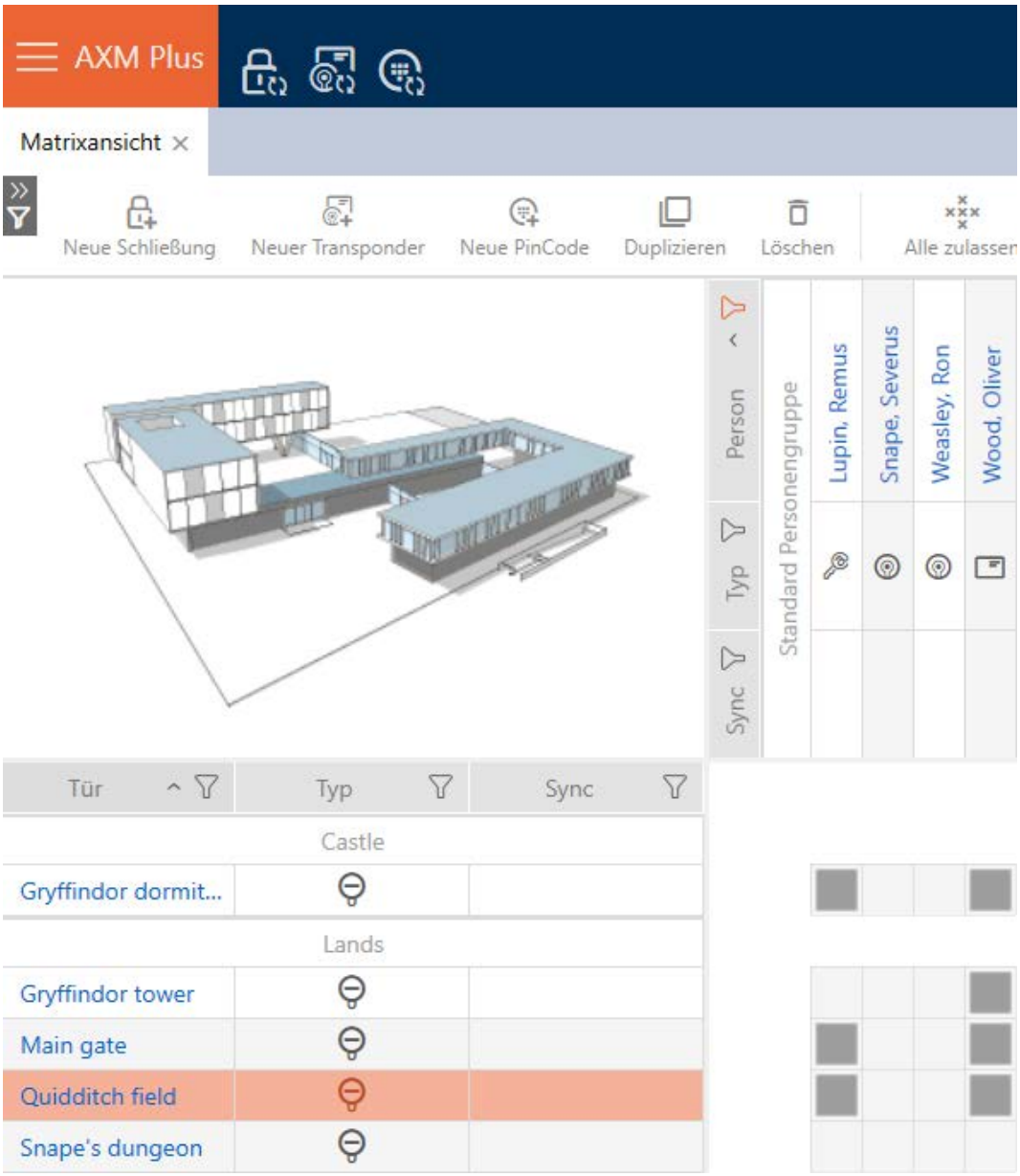
Wenn Sie den Filter anschließend mit der Schaltfläche Anzeigefilter löschen wieder entfernen, dann stellen Sie fest, dass die weggefilterten Identmedien tatsächlich nicht zugelassen wurden:



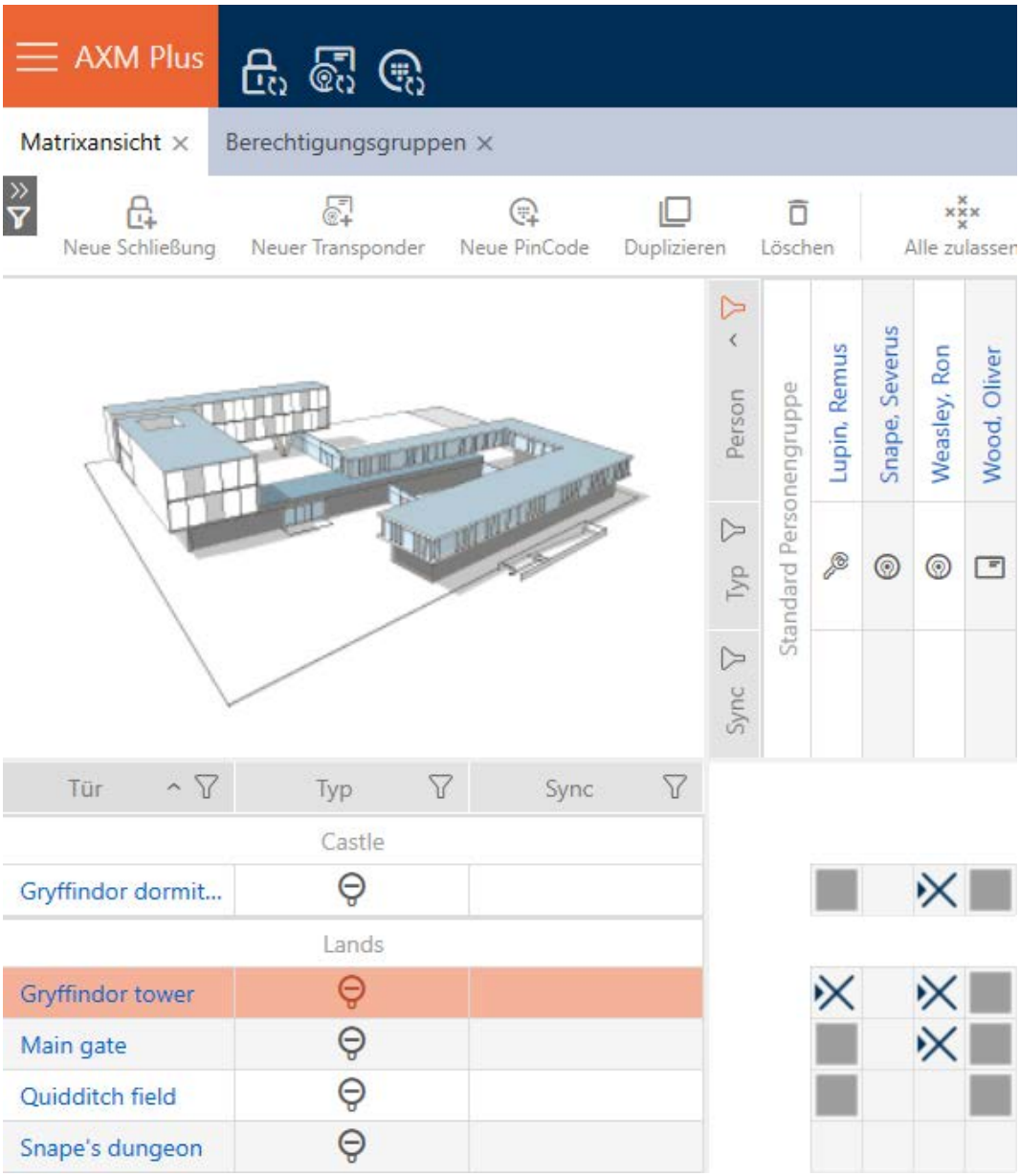
17.2.2 Berechtigungsgruppen

Berechtigungsgruppen sind eine einfache Möglichkeit für Sie, um Berechtigungen für mehrere Türen und Identmedien gleichzeitig einzurichten (siehe *Berechtigungsgruppen [▸ 564]*).

Matrix ohne Berechtigungen

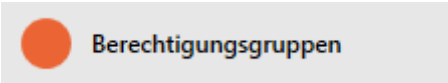


Matrix mit Berechtigungsgruppe



17.2.2.1 Schließungen und Identmedien zu Berechtigungsgruppen hinzufügen

Idealerweise haben Sie Ihre Berechtigungsgruppen bereits vor dem Erstellen der Schließungen erstellt (siehe *Best Practice: Schließanlage aufbauen [▸ 32]* und *Berechtigungsgruppen erstellen [▸ 55]*). Damit können Sie direkt beim Erstellen der Schließungen und Identmedien die Berechtigungsgruppen in den Eigenschaften der Schließungen und Identmedien einstellen:

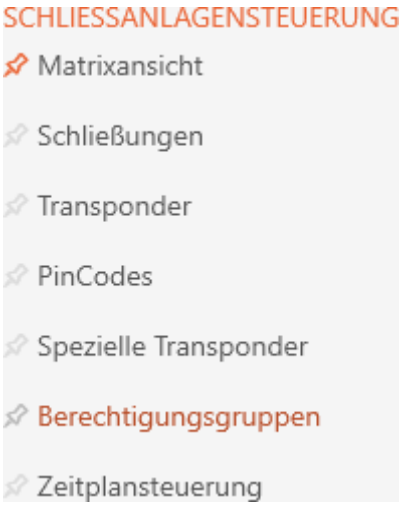


Selbstverständlich können Sie Ihre Schließungen und Identmedien aber auch nachträglich zu den Berechtigungsgruppen hinzufügen:

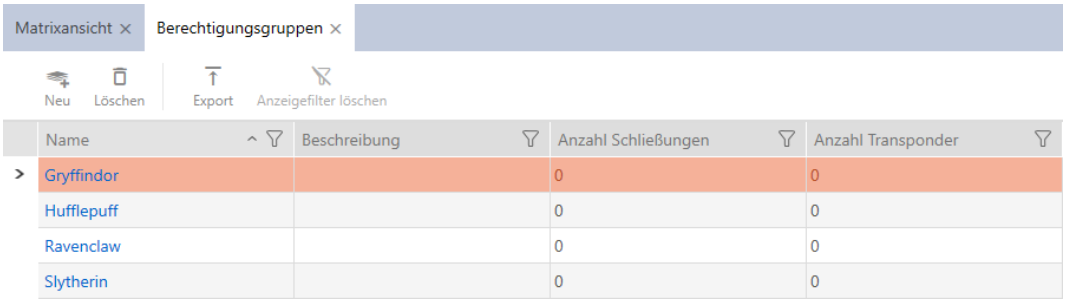
✓ Berechtigungsgruppe erstellt (siehe *Berechtigungsgruppen erstellen* [▸ 55]).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

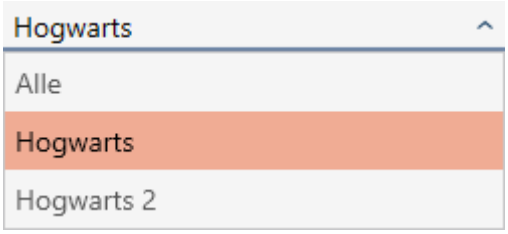
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Berechtigungsgruppen aus.



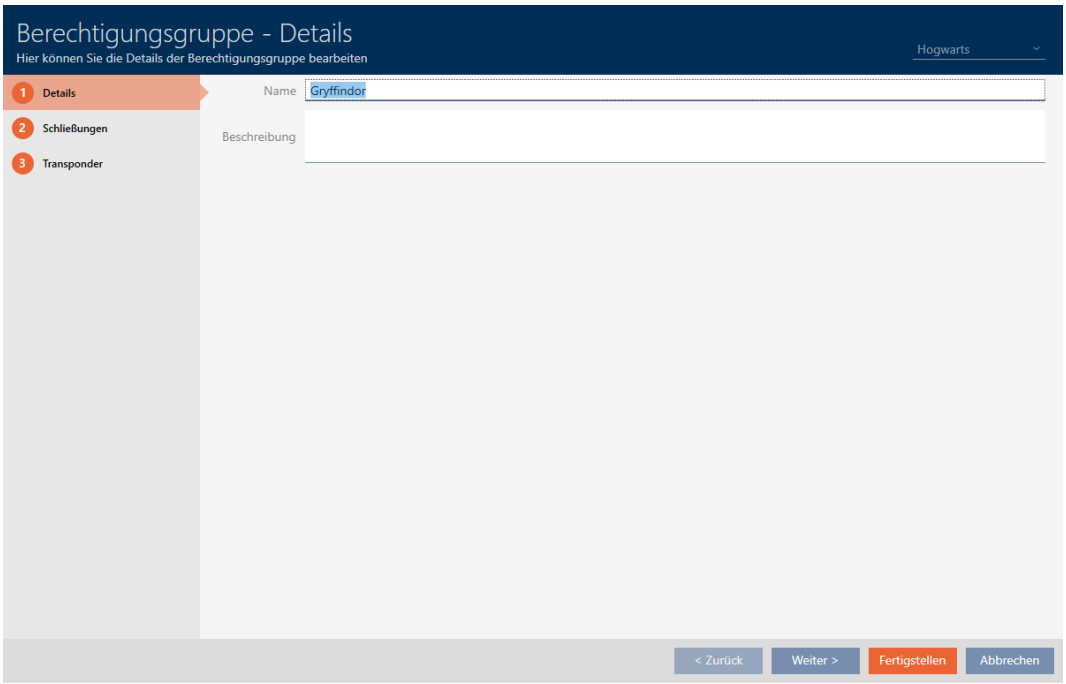
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Berechtigungsgruppen] öffnet sich.



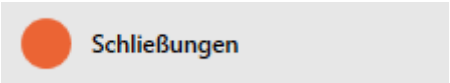
3. Wählen Sie im Dropdown-Menü ggfs. eine andere Schließanlage aus oder wählen Sie den Dropdown-Eintrag "Alle", um die Berechtigungsgruppen aller Schließanlagen anzuzeigen.



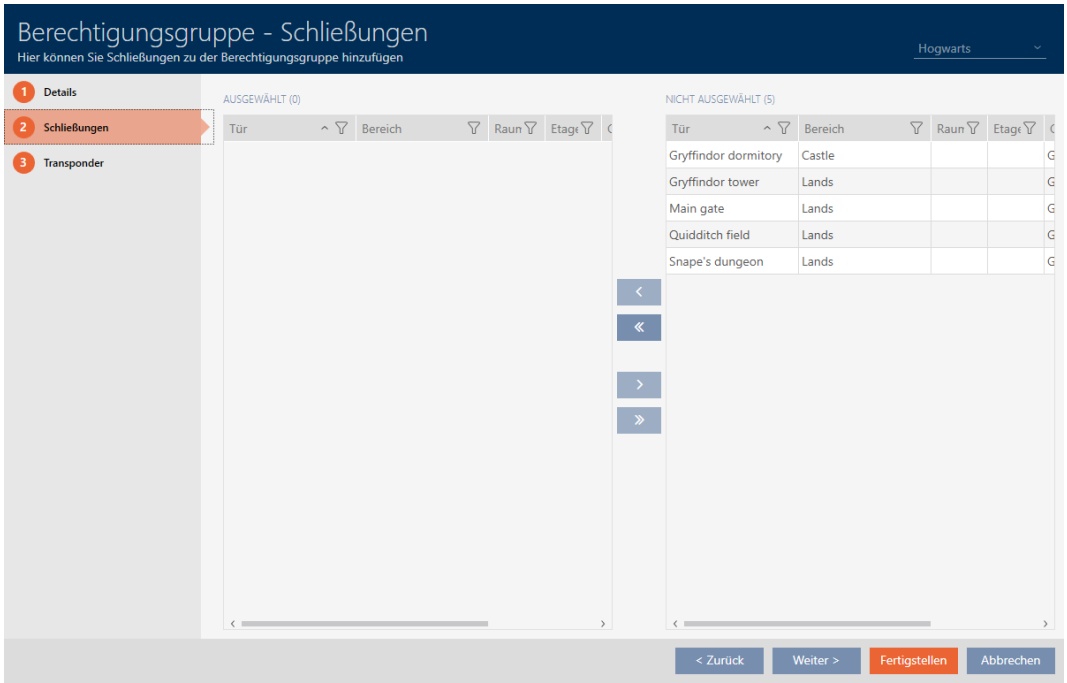
4. Klicken Sie auf die Berechtigungsgruppe, zu der Sie Schließungen und Identmedien hinzufügen wollen.
   ↳ Fenster der Berechtigungsgruppe öffnet sich.



5. Klicken Sie auf den Reiter Schließungen.



   ↳ Fenster wechselt zum Reiter "Schließungen".



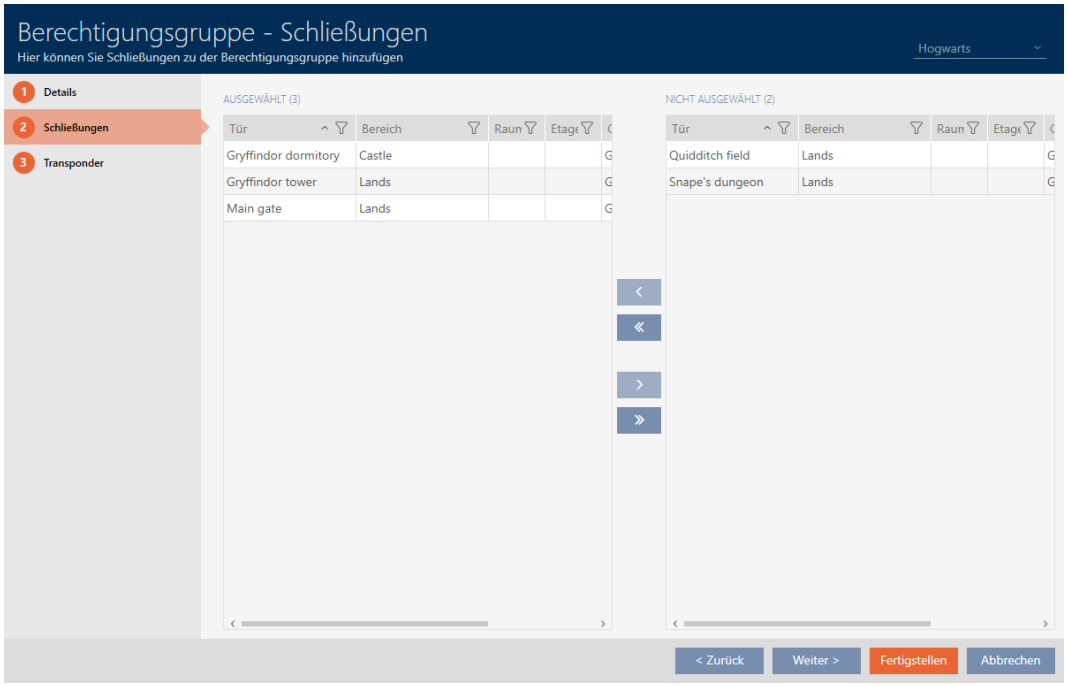
6. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
7. Markieren Sie alle Schließungen, die Sie zur Berechtigungsgruppe hinzufügen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

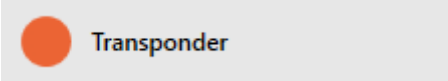
Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

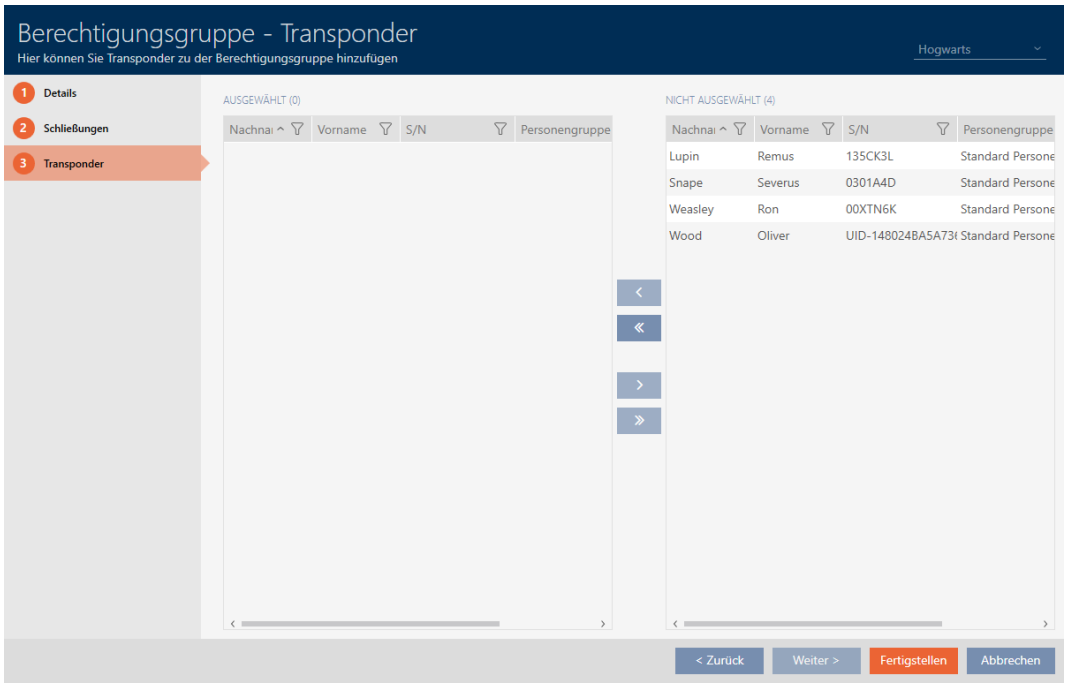
8. Verschieben Sie mit [<] nur die ausgewählten Schließungen oder verschieben Sie mit [«] alle angezeigten Schließungen.
   ↳ Die markierte Schließung in der linken Spalte wird der Berechtigungsgruppe hinzugefügt.



9. Klicken Sie auf den Reiter Transponder.



↳ Fenster wechselt zum Reiter "Transponder".



10. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

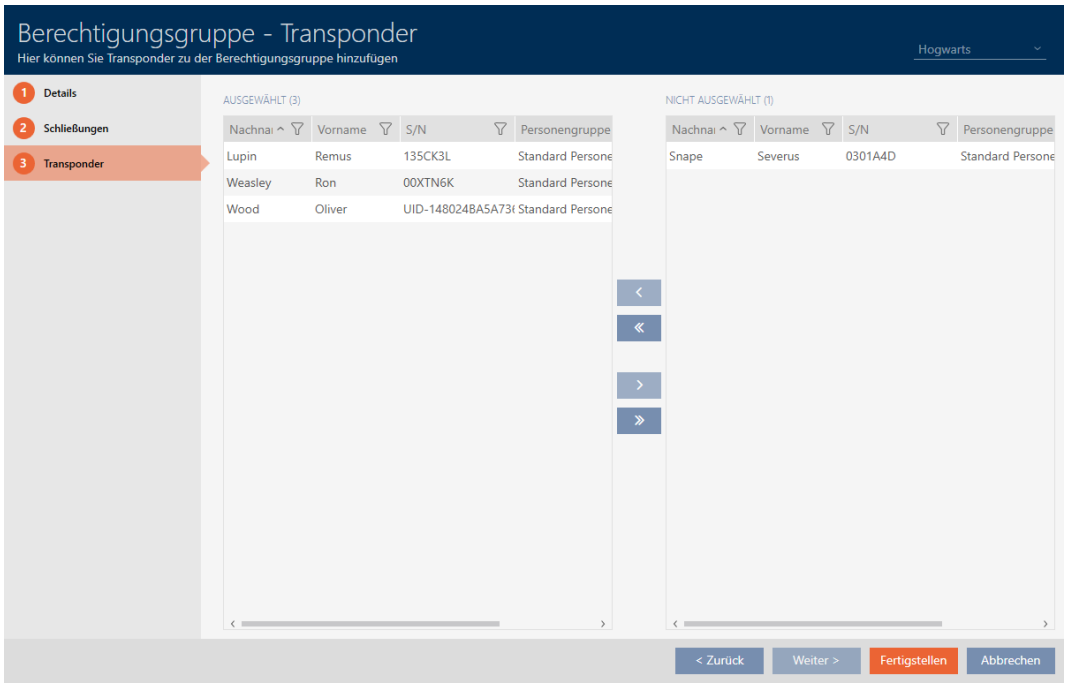
11. Markieren Sie alle Identmedien, die Sie zur Berechtigungsgruppe hinzufügen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

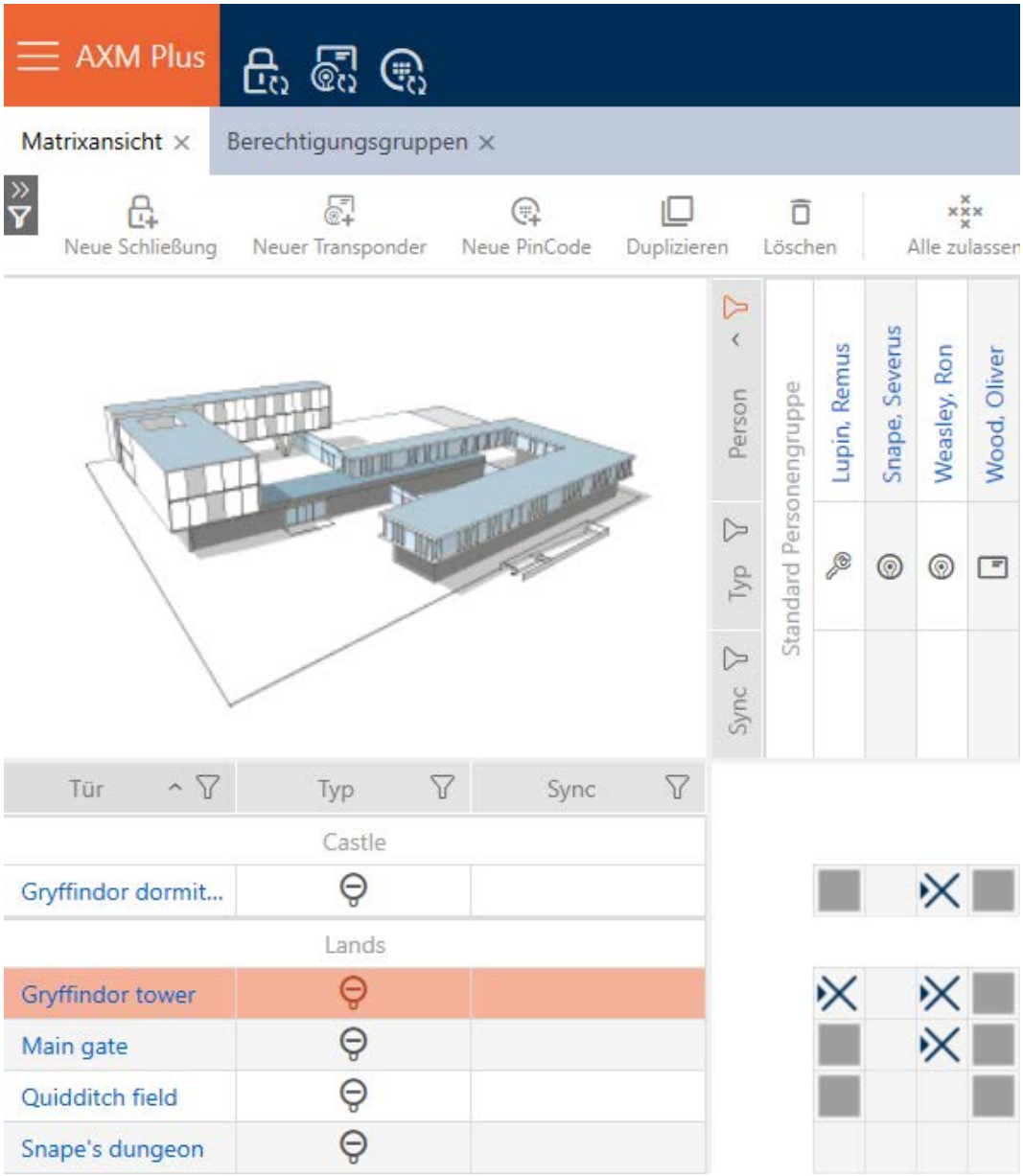
Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

12. Verschieben Sie mit < nur die ausgewählten Identmedien oder verschieben Sie mit « alle angezeigten Schließungen.
    ↳ Die markierten Identmedien in der linken Spalte werden der Berechtigungsgruppe hinzugefügt.



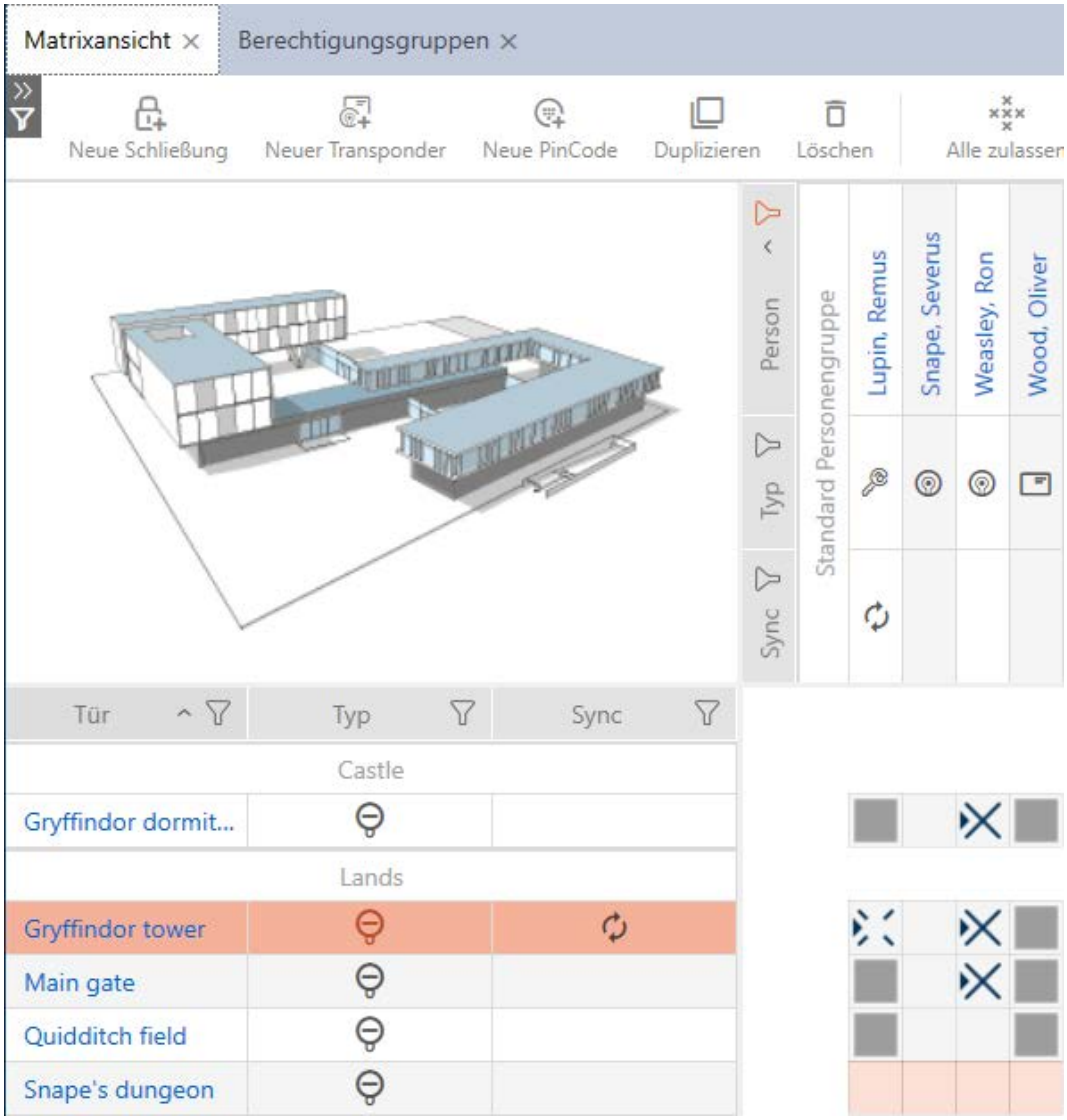
13. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster der Berechtigungsgruppe schließt sich.
    ↳ Alle Identmedien in dieser Berechtigungsgruppe sind an allen Schließungen in dieser Berechtigungsgruppe berechtigt.
    ↳ Matrixansicht ist wieder sichtbar.
14. Klicken Sie auf die Schaltfläche Aktualisieren.

↳ Matrix zeigt Berechtigungen aus Ihrer Berechtigungsgruppe an (an kleinem Dreieck neben dem Kreuz erkennbar).



Sie können einzelne Berechtigungen aus Berechtigungsgruppen auch manuell überschreiben. Zum Beispiel gibt es die Möglichkeit, einem Identmedium, das eigentlich an einer Schließung berechtigt wäre, die Berechtigung wegzunehmen.

Gehen Sie dazu wie bei der normalen Vergabe von Einzelberechtigungen vor (siehe *Einzelne Berechtigungen ändern (Kreuz) [▸ 327]*). In diesem Fall verschwindet nur das Kreuz, nicht aber das Dreieck:

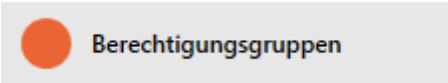


Das Dreieck zeigt weiterhin an, dass hier eigentlich eine Berechtigung aus einer Berechtigungsgruppe vorliegt.

17.2.2.2 Bereiche und Personengruppen zu Berechtigungsgruppen hinzufügen

In diesem Kapitel erfahren Sie, wie Sie mithilfe von Bereichen schnell mehrere Schließungen zu Berechtigungsgruppen hinzufügen. Das Vorgehen für Personengruppen/Identmedien ist ähnlich.

Idealerweise haben Sie Ihre Berechtigungsgruppen bereits vor dem Erstellen der Schließungen erstellt (siehe *Best Practice: Schließanlage aufbauen [▸ 32]* und *Berechtigungsgruppen erstellen [▸ 55]*). Damit können Sie direkt beim Erstellen der Schließungen und Identmedien die Berechtigungsgruppen direkt in den Eigenschaften der Schließungen und Identmedien einstellen:

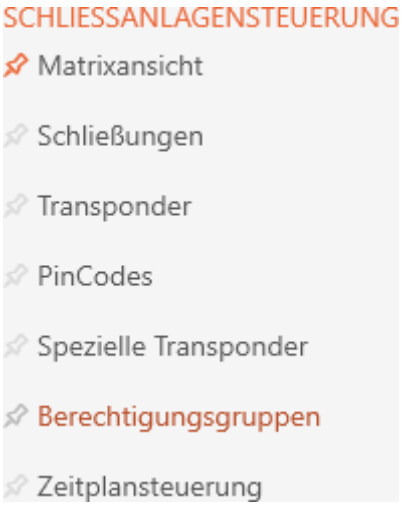


So können Sie mithilfe von Bereichen mehrere Schließungen schnell zu Berechtigungsgruppen hinzufügen:

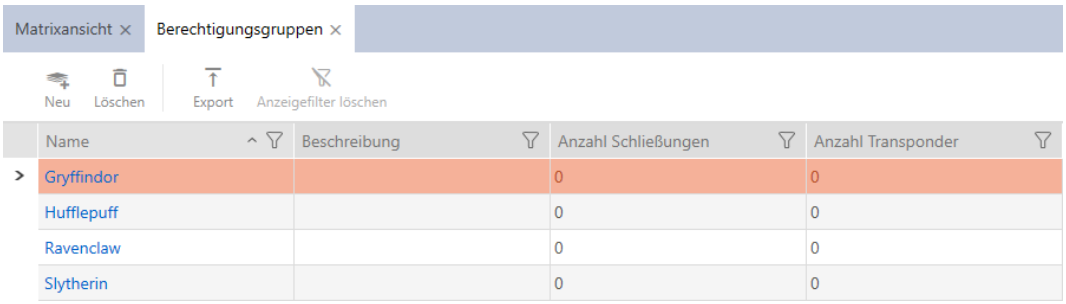
- ✓ Berechtigungsgruppe erstellt (siehe *Berechtigungsgruppen erstellen [▸ 55]*).
- ✓ Mindestens ein Bereich erstellt (siehe *Bereich erstellen [▸ 89]*).
- ✓ Bereich wurde mindestens eine Schließung zugewiesen (siehe *Schließungen in Bereiche verschieben [▸ 279]*).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

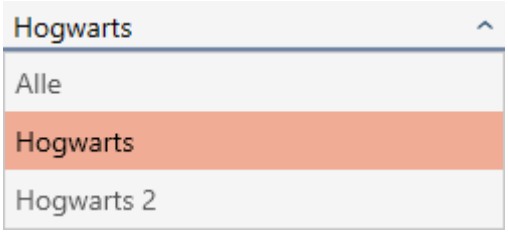
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Berechtigungsgruppen aus.



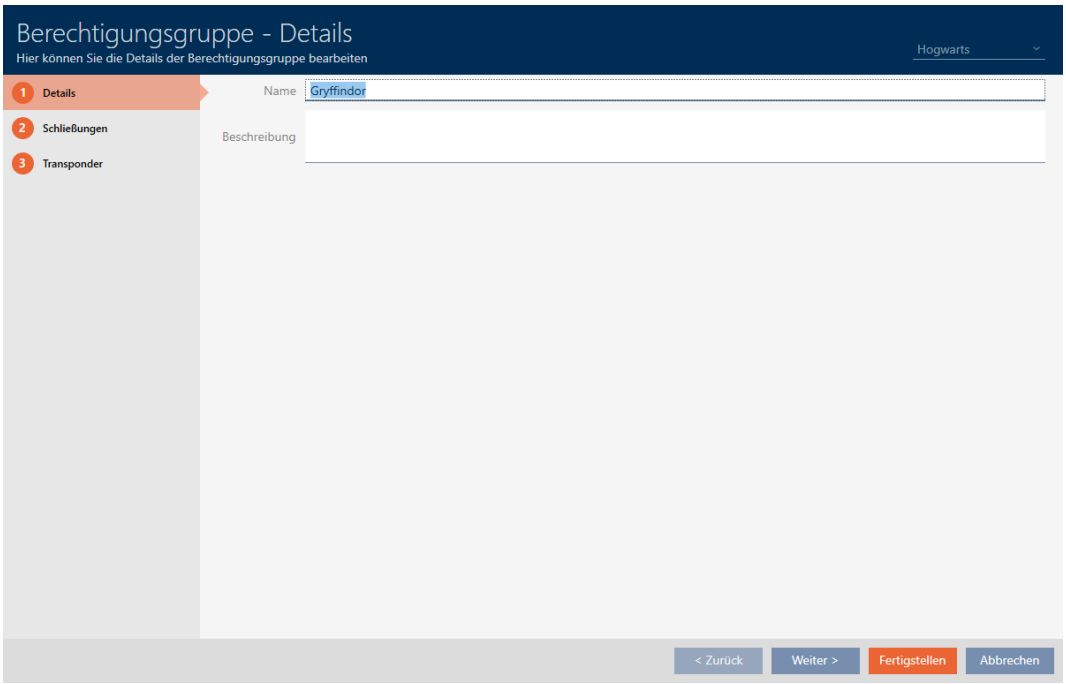
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Berechtigungsgruppen] öffnet sich.



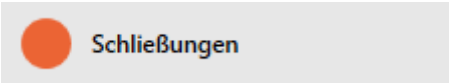
3. Wählen Sie im Dropdown-Menü ggfs. eine andere Schließanlage aus oder wählen Sie den Dropdown-Eintrag "Alle", um die Berechtigungsgruppen aller Schließanlagen anzuzeigen.



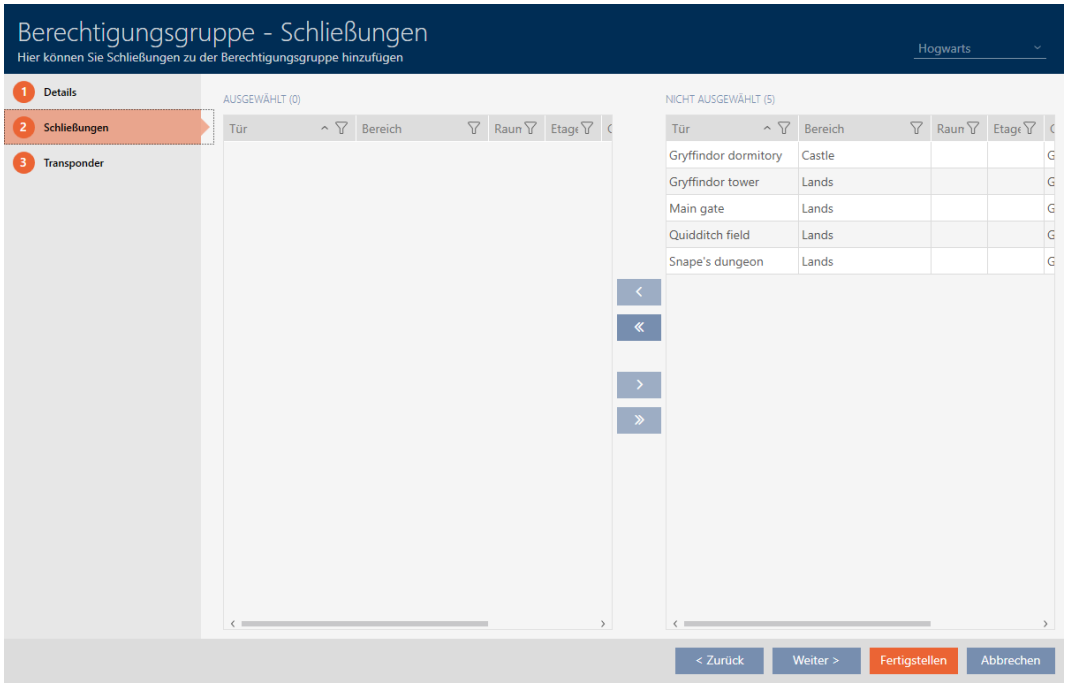
4. Klicken Sie auf die Berechtigungsgruppe, zu der Sie Schließungen und Identmedien hinzufügen wollen.
   ↳ Fenster der Berechtigungsgruppe öffnet sich.



5. Klicken Sie auf den Reiter Schließungen.



   ↳ Fenster wechselt zum Reiter "Schließungen".



6. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

HINWEIS

Bereiche als Filterkriterium

Bereiche können als Filterkriterium eingesetzt werden und vereinfachen so die Auswahl Ihrer Schließungen.

1. Klicken Sie die in der Spalte *Bereich* auf das Filtersymbol.
2. Wählen Sie einen oder mehrere Bereiche aus.

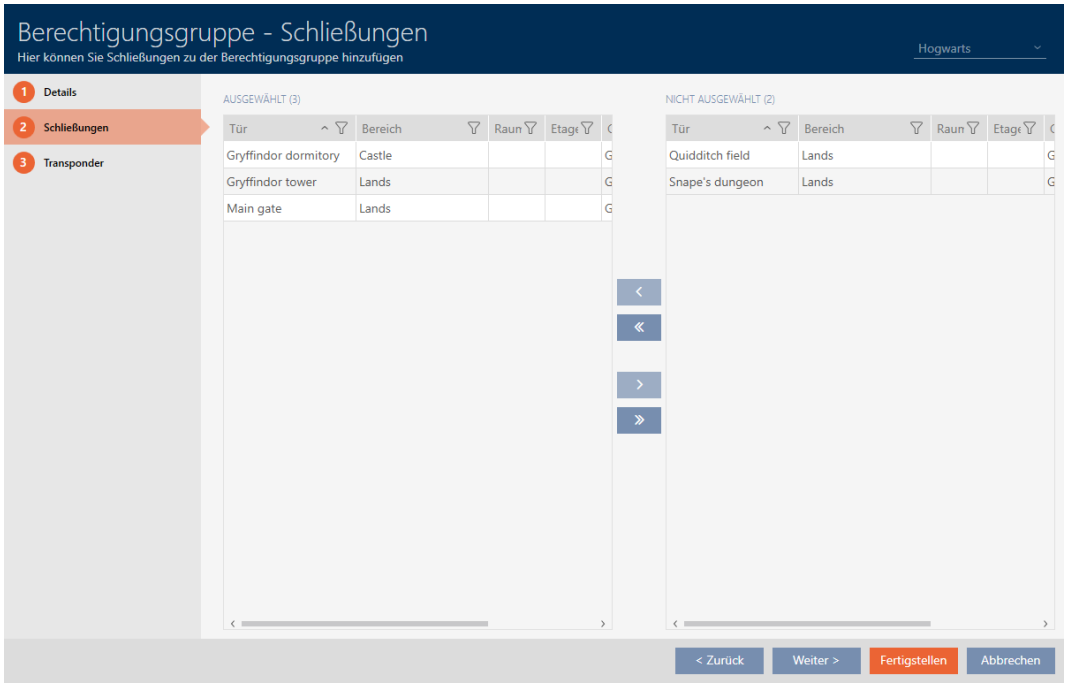
7. Markieren Sie alle Schließungen, die Sie zur Berechtigungsgruppe hinzufügen wollen (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

8. Verschieben Sie mit [<] nur die ausgewählten Schließungen oder verschieben Sie mit [«] alle angezeigten Schließungen.
   ↳ Die markierte Schließung in der linken Spalte wird der Berechtigungsgruppe hinzugefügt.



9. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der Berechtigungsgruppe schließt sich.
   ↳ Alle Identmedien in dieser Berechtigungsgruppe sind an allen Schließungen in dieser Berechtigungsgruppe berechtigt.
   ↳ Matrixansicht ist wieder sichtbar.
10. Klicken Sie auf die Schaltfläche Aktualisieren.

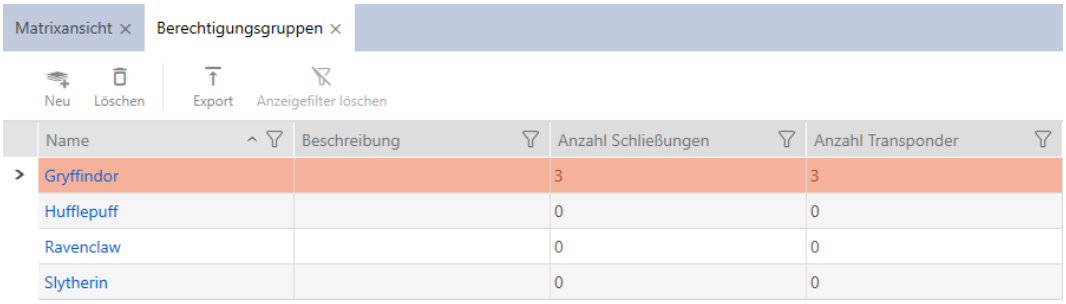
↳ Matrix zeigt Berechtigungen aus Ihrer Berechtigungsgruppe an (an kleinem Dreieck neben dem Kreuz erkennbar).

17.2.2.3 Alle Berechtigungsgruppen eines Projekts anzeigen

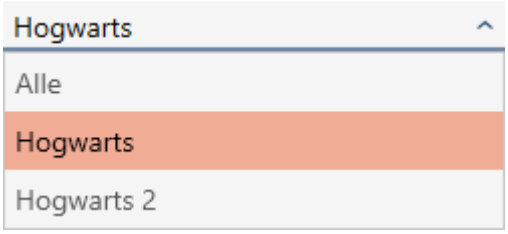
✓ Mindestens eine Berechtigungsgruppe erstellt (siehe *Berechtigungsgruppen erstellen [▸ 55]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

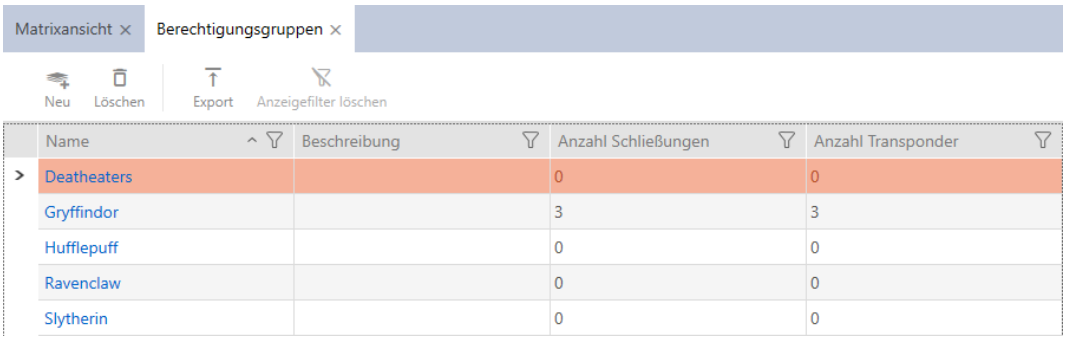
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Berechtigungsgruppen aus.
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Berechtigungsgruppen] öffnet sich.



3. Wählen Sie im Dropdown-Menü für die Schließanlage den Eintrag "Alle".



↳ Alle Berechtigungsgruppen aus allen Schließanlagen im gleichen Projekt werden angezeigt.



Die angezeigten Berechtigungsgruppen können Sie auch als Liste exportieren (siehe *Berechtigungsgruppen als Liste exportieren [▸ 346]*).

17.2.2.4 Berechtigungsgruppen als Liste exportieren

Alle Berechtigungsgruppen in Ihrer Schließanlage lassen sich als PDF exportieren.

Im PDF werden genau dieselben Berechtigungsgruppen in genau derselben Reihenfolge wie in der AXM Plus angezeigt.

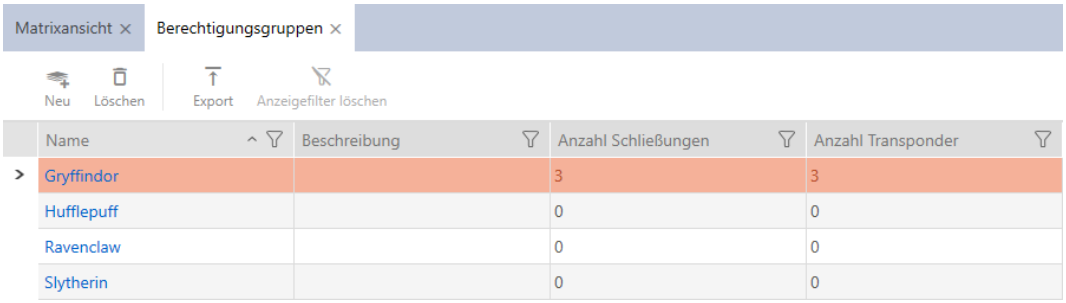
Das bedeutet, dass Sie die Anzeige vor dem Export sortieren und filtern können. Damit sortieren und filtern Sie auch die exportierte Liste.

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

✓ Mindestens eine Berechtigungsgruppe erstellt (siehe *Berechtigungsgruppen erstellen [▸ 55]*).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Berechtigungsgruppen aus.
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Berechtigungsgruppen] öffnet sich.
3. Wählen Sie im Dropdown-Menü ggfs. eine bestimmte oder alle Schließanlagen mit den zu exportierenden Berechtigungsgruppen aus.



4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
5. Klicken Sie auf die Schaltfläche Export ⤒.
   ↳ Explorer-Fenster öffnet sich.
6. Speichern Sie die PDF-Datei in einem Dateiverzeichnis Ihrer Wahl.
   ↳ Explorer-Fenster schließt sich.

↳ Angezeigte Berechtigungsgruppen werden als PDF-Datei (DIN A4) exportiert.

Simons Voss technologies

Alle Berechtigungsgruppen für die Schließanlage 'Hogwarts 1'

Name	Anzahl Schließungen	Anzahl Transponder
Gryffindor	1	3
Hufflepuff	0	0
Ravenclaw	0	0
Slytherin	0	0

Simons Voss technologies Gedruckt am: 13.01.2022 1

17.2.3 Berechtigungen zeitlich steuern (Zeitpläne)

Das Zeitmanagement in der AXM Plus setzt sich zusammen aus:

- Zeitplänen für Schließungen
- Zeitgruppen für Transponder

Eine detaillierte Beschreibung und ein Beispiel finden Sie hier: *Zeitmanagement [▸ 548]*.

Zeitgruppen können Sie in der AXM Plus nur über einen Zeitplan erstellen. Der erste Schritt nach dem Erstellen eines Konzepts ist deshalb ein Zeitplan: *Zeitplan erstellen [▸ 58]*.

Zeitpläne und Zeitgruppen in mehreren Schließanlagen

In einer Schließanlage erstellte Zeitpläne und Zeitgruppen sind projektweit einstellbar. Sie werden diese auch in anderen Schließanlagen zur Auswahl finden, sofern diese Schließanlage sich im gleichen Projekt befindet. Änderungen an Zeitplänen und Zeitgruppen gelten deshalb auch für alle Schließanlagen innerhalb eines Projekts gleichermaßen.

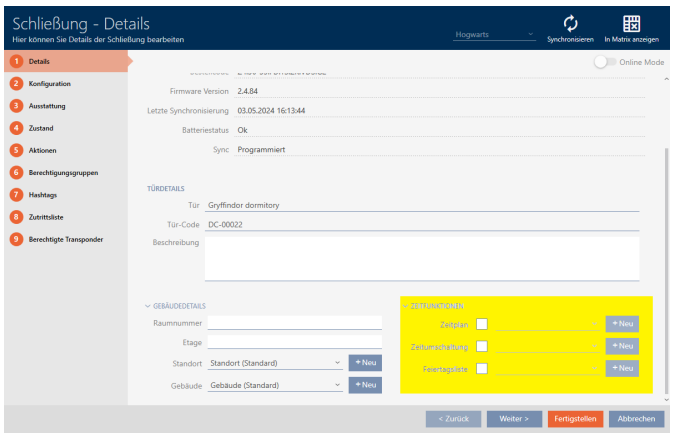
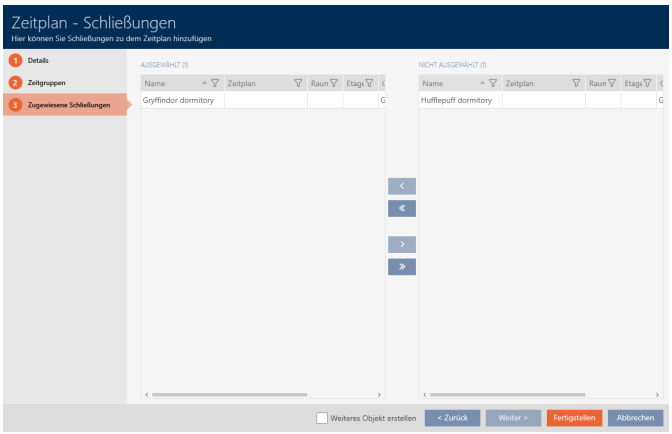
Schließanlagen, die sich in anderen Projekten befinden, sind davon unabhängig. Zeitpläne und Zeitgruppen aus anderen Projekten können Sie nicht sehen oder einstellen.

17.2.3.1 Schließungen zum Zeitplan hinzufügen

Idealerweise erstellen Sie Ihre Zeitpläne noch vor den Schließungen (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*). Dann können Sie Ihre Schließungen schon dem Zeitplan hinzufügen, während Sie die Schließung gerade anlegen (siehe *Schließung erstellen [▸ 238]*).

Manchmal haben Sie aber bereits Schließungen erstellt und entscheiden sich zum Beispiel erst später, die Berechtigungen zeitlich zu steuern. In diesem Fall fügen Sie die Schließungen einfach nachträglich zu Ihren Zeitplänen hinzu.

Dafür haben Sie zwei Möglichkeiten:

Fenster der Schließung	Fenster des Zeitplans
 - Direkt beim Erstellen der Schließung verwendbar - Nur eine Schließung pro Durchgang möglich	 - Direkt beim Erstellen des Zeitplans verwendbar - Mehrere Schließungen pro Durchgang möglich - Einsatz von Bereichen als Filterkriterium möglich (siehe *Bereich mitsamt Schließungen zu einem Zeitplan hinzufügen [▸ 355]*).

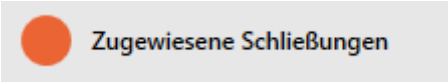
In diesem Kapitel erfahren Sie, wie Sie Schließungen über das Fenster des Zeitplans zu einem Zeitplan hinzufügen (Hinzufügen einzelner Schließungen über die Schließungseigenschaften siehe *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]*).

✓ Zeitplan erstellt (siehe *Zeitplan erstellen [▸ 58]*).

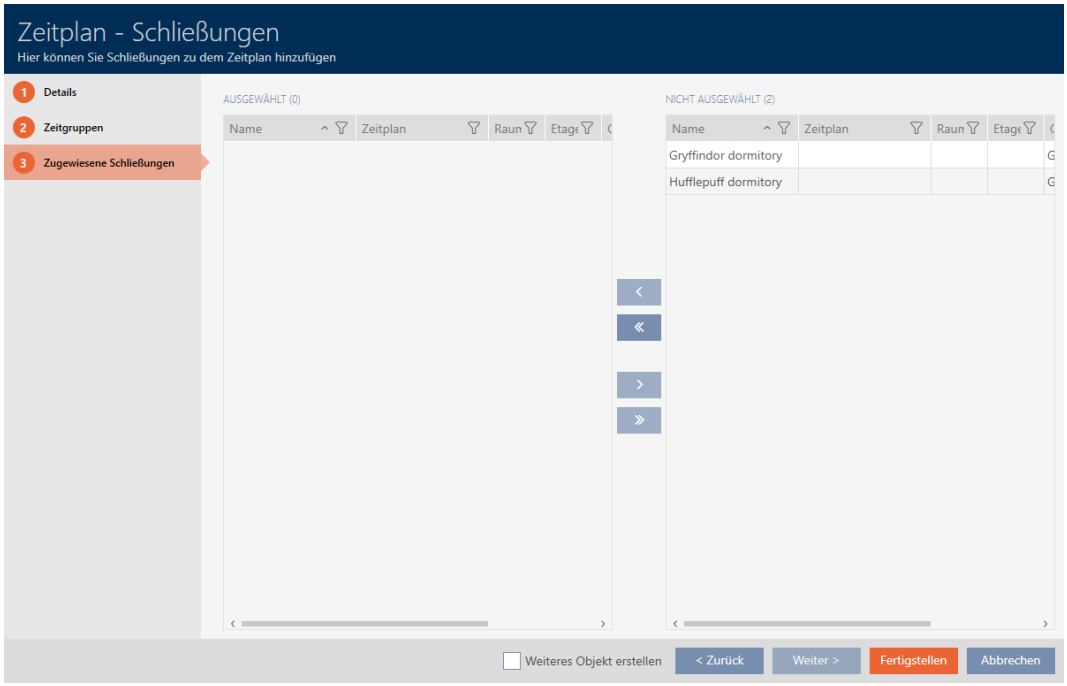
✓ Zeitplan-Fenster geöffnet (siehe *Zeitplan erstellen [▸ 58]*).

✓ Schließung mit .ZK-Option ausgestattet.

1. Klicken Sie auf den Reiter Zugewiesene Schließungen.



↳ Fenster des Zeitplans wechselt zum Reiter "Zugewiesene Schließungen".



2. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
3. Markieren Sie alle Schließungen, die Sie zuweisen wollen (Strg+-Mausklick für einzelne oder Shift+Mausklick für mehrere).

HINWEIS

Doppelklick als Alternative zu Pfeiltasten

Mit einem Doppelklick auf einen Eintrag in der Liste verschieben Sie diesen Eintrag ebenfalls in die andere Spalte.

4. Verschieben Sie mit [<] nur die ausgewählten Schließungen oder verschieben Sie mit [«] alle angezeigten Schließungen.

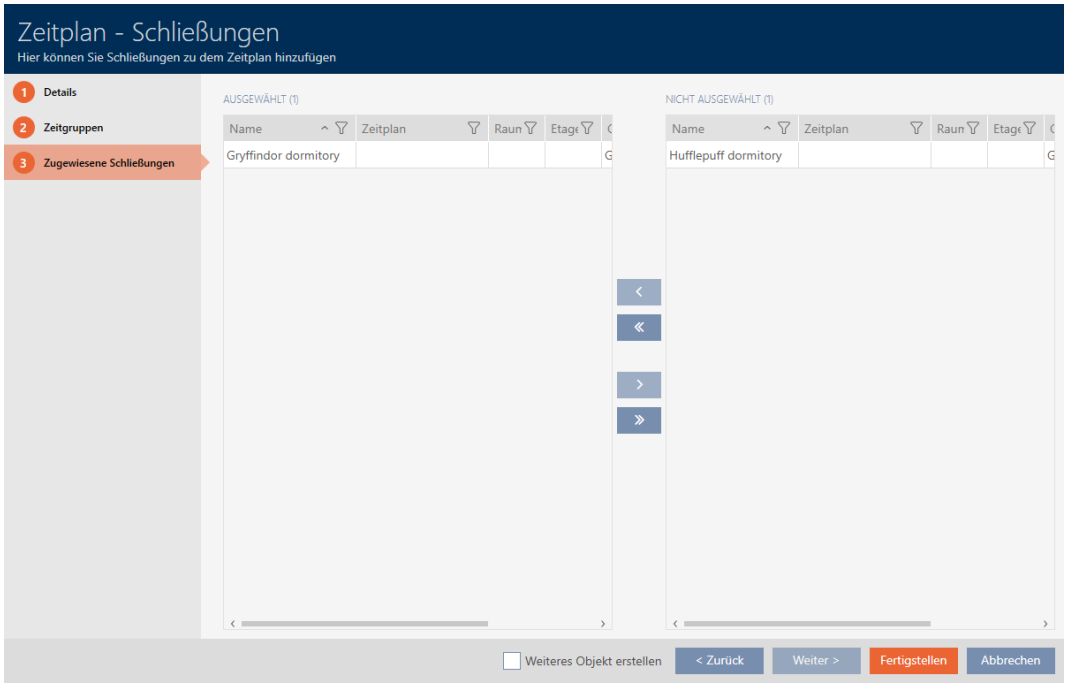
HINWEIS

Schließungen aus anderen Zeitplänen

Schließungen aus anderen Zeitplänen werden ebenfalls aufgelistet. Damit können sie auch aus anderen Zeitplänen in den aktuellen Zeitplan verschoben werden.

1. Filtern/Sortieren Sie die angezeigten Schließungen.
2. Prüfen Sie, ob die markierten Schließungen bereits in einem anderen Zeitplan verwendet werden.

↳ Die Schließungen in der linken Spalte werden dem Zeitplan hinzugefügt.



5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster für Zeitplan schließt sich.

↳ Schließungen sind dem Zeitplan hinzugefügt.

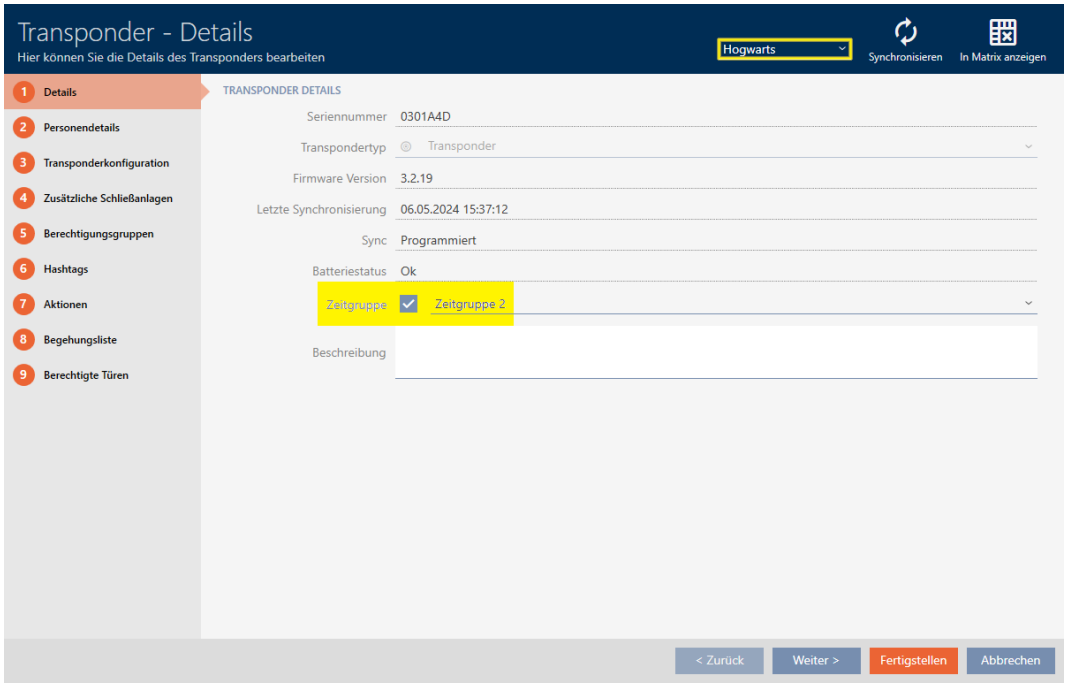
17.2.3.2 Identmedium zur Zeitgruppe hinzufügen

Idealerweise erstellen Sie Ihre Zeitgruppen noch vor den Identmedien (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*). Dann können Sie Ihre Identmedien schon beim Anlegen den Zeitgruppen hinzufügen (siehe *Identmedien erstellen [▸ 94]*).

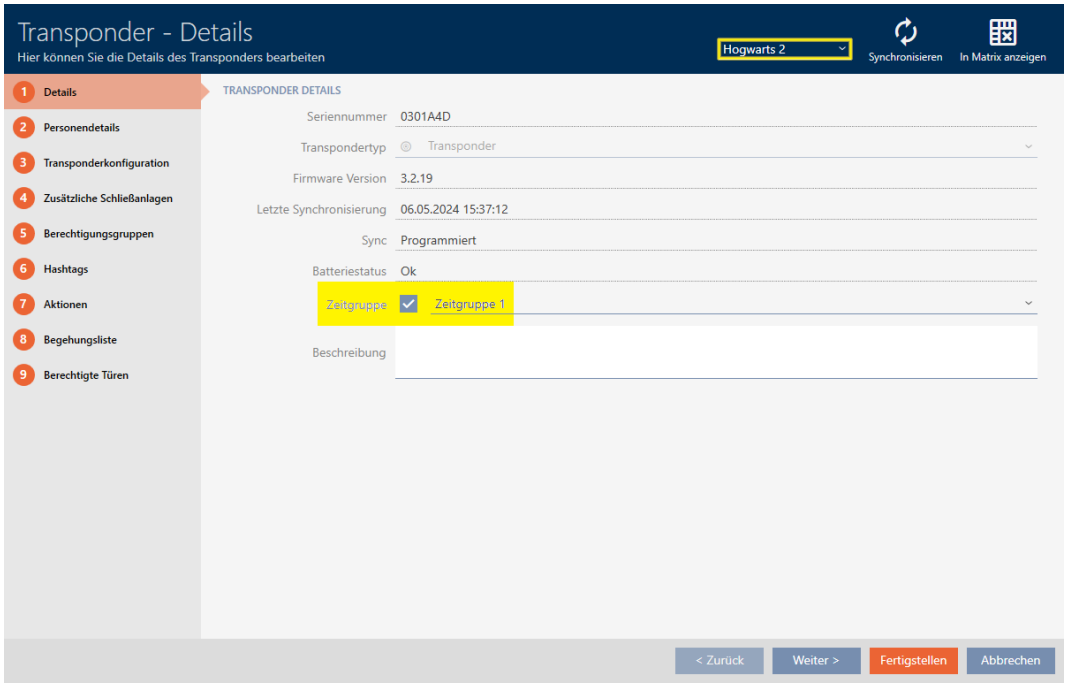
Ein Identmedium kann nur über seine Eigenschaften zu einer Zeitgruppe hinzugefügt werden.

Zeitgruppen in mehreren Schließanlagen

Sie können Identmedien in mehreren Schließanlagen nutzen (siehe *Identmedium im gleichen Projekt wiederverwenden [▸ 212]* und *Identmedium in anderen Projekten/Datenbanken wiederverwenden [▸ 217]*). Dasselbe Identmedium kann in jeder Schließanlage eine andere Zeitgruppe haben. Daher können Sie in den Details des Identmediums rechts oben die Schließanlage auswählen und die Eigenschaften für diese Schließanlage auswählen.

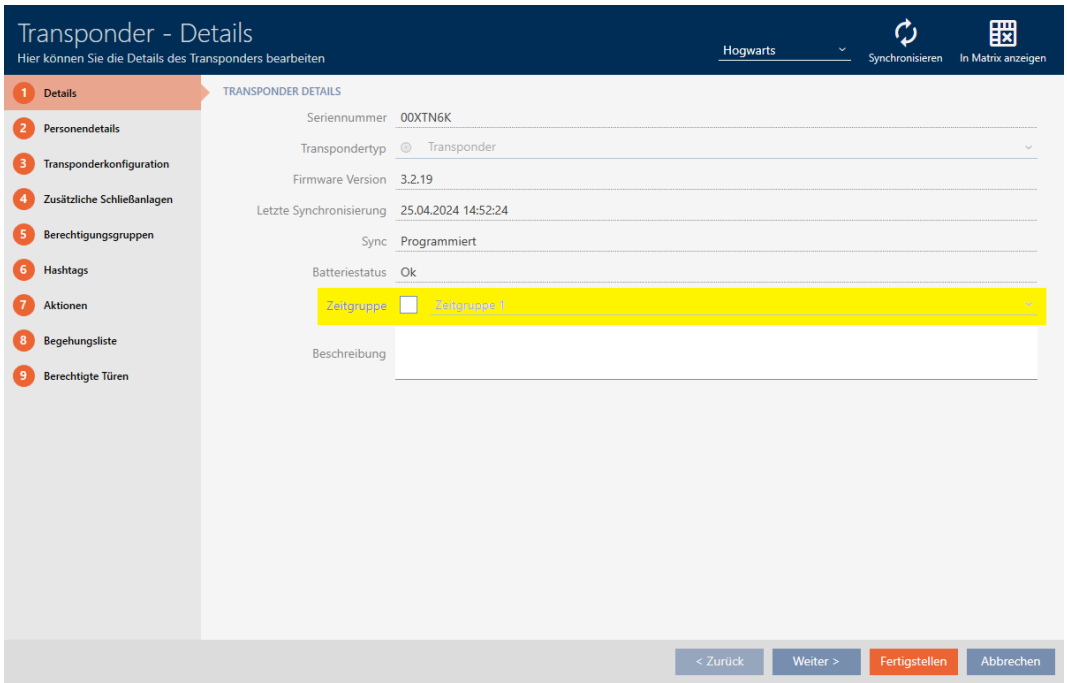


Wenn Sie im Dropdown-Menü die Schließanlage wechseln, können Sie für das Identmedium in dieser Schließanlage eine andere Zeitgruppe auswählen.



PinCode-Tastaturen sind nur einer Schließanlage verwendbar. Daher können Sie für PinCode-Tastaturen genau eine Zeitgruppe pro Pin auswählen.

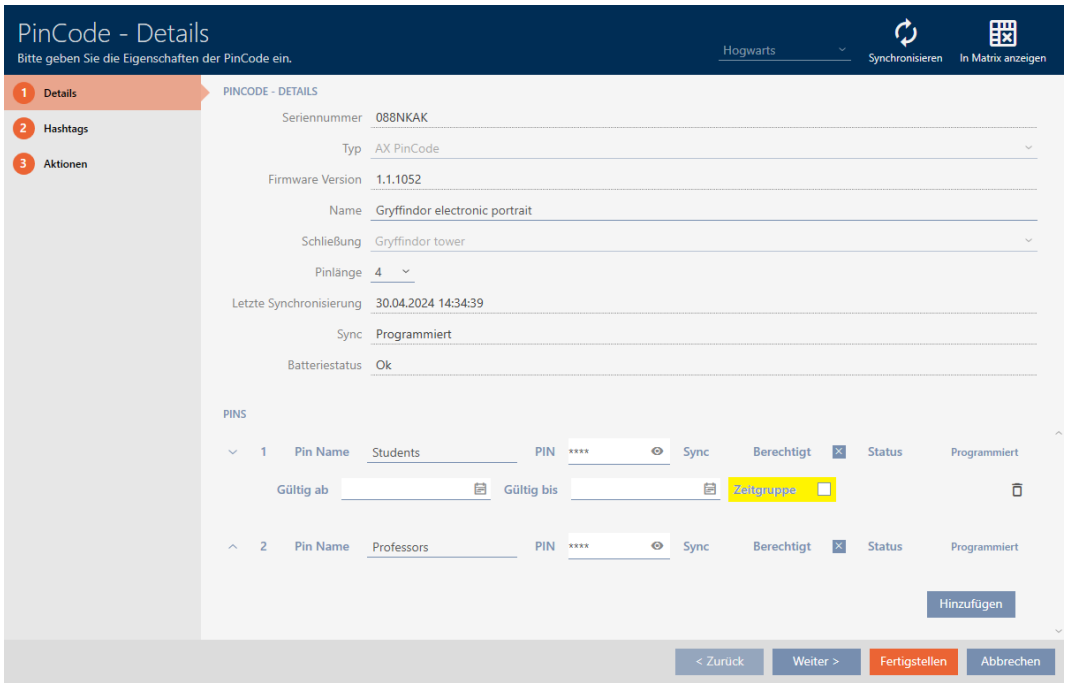
Transponder/Karte/AX2Go-Schlüssel zur Zeitgruppe hinzufügen



1. Klicken Sie auf das Identmedium, das einer Zeitgruppe hinzugefügt werden soll.
   ↳ Fenster des Identmediums öffnet sich.
2. Aktivieren Sie die Checkbox ☑ Zeitgruppe.
3. Wählen Sie im Dropdown-Menü ▼ **Zeitgruppe** die Zeitgruppe aus (z.B. "Zeitgruppe").
4. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster des Identmediums schließt sich.

↳ Identmedium ist zur Zeitgruppe hinzugefügt.

PINs einer PinCode-Tastatur zur Zeitgruppe hinzufügen



✓ PinCode-Tastatur mit PINs angelegt (siehe *PinCode-Tastaturen erstellen [▸ 102]*).

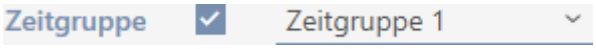
✓ Zeitgruppen erstellt (siehe *Zeitgruppe erstellen [▸ 61]*).

1. Klicken Sie auf die PIN, die einer Zeitgruppe hinzugefügt werden soll.
   ↳ Fenster der zugehörigen PinCode-Tastatur öffnet sich.
2. Klappen Sie die Einstellungen der PIN mit der Schaltfläche ⌄ aus.
3. Aktivieren Sie die Checkbox ☑ Zeitgruppe
   ↳ Dropdown-Menü erscheint.

4. Wählen Sie die gewünschte Zeitgruppe aus.

5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster der PinCode-Tastatur schließt sich.

↳ PIN ist der Zeitgruppe hinzugefügt.



17.2.3.3 Bereich mitsamt Schließungen zu einem Zeitplan hinzufügen

Idealerweise erstellen Sie Ihre Zeitpläne noch vor den Schließungen (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*). Dann können Sie Ihre Schließungen schon dem Zeitplan hinzufügen, während Sie die Schließung gerade anlegen (siehe *Schließung erstellen [▸ 238]*).

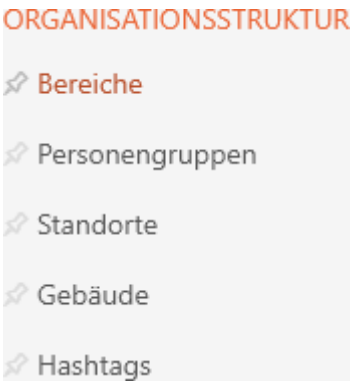
Manchmal haben Sie aber bereits Schließungen erstellt und entscheiden sich zum Beispiel erst später, die Berechtigungen zeitlich zu steuern. In diesem Fall fügen Sie die Schließungen einfach nachträglich zu Ihren Zeitplänen hinzu.

In diesem Kapitel erfahren Sie, wie Sie einen ganzen Bereich mitsamt Schließungen zu einem Zeitplan hinzufügen (Hinzufügen einzelner Schließungen über die Schließungseigenschaften siehe *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]*).

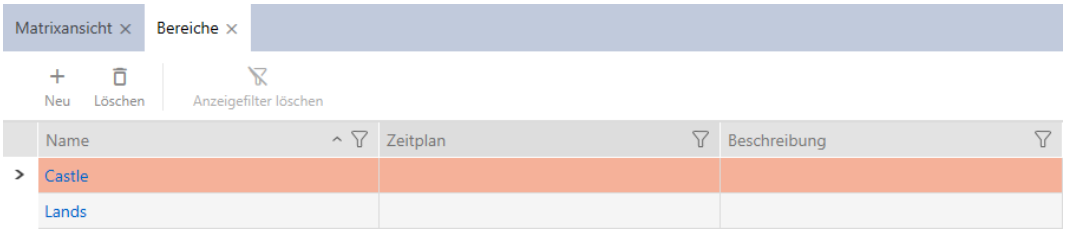
- ✓ Zeitplan erstellt (siehe *Zeitplan erstellen [▸ 58]*).
- ✓ Bereich erstellt (siehe *Bereich erstellen [▸ 89]*).
- ✓ Schließungen im Bereich (siehe *Schließungen in Bereiche verschieben [▸ 279]*).
- ✓ Schließung mit .ZK-Option ausgestattet.

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

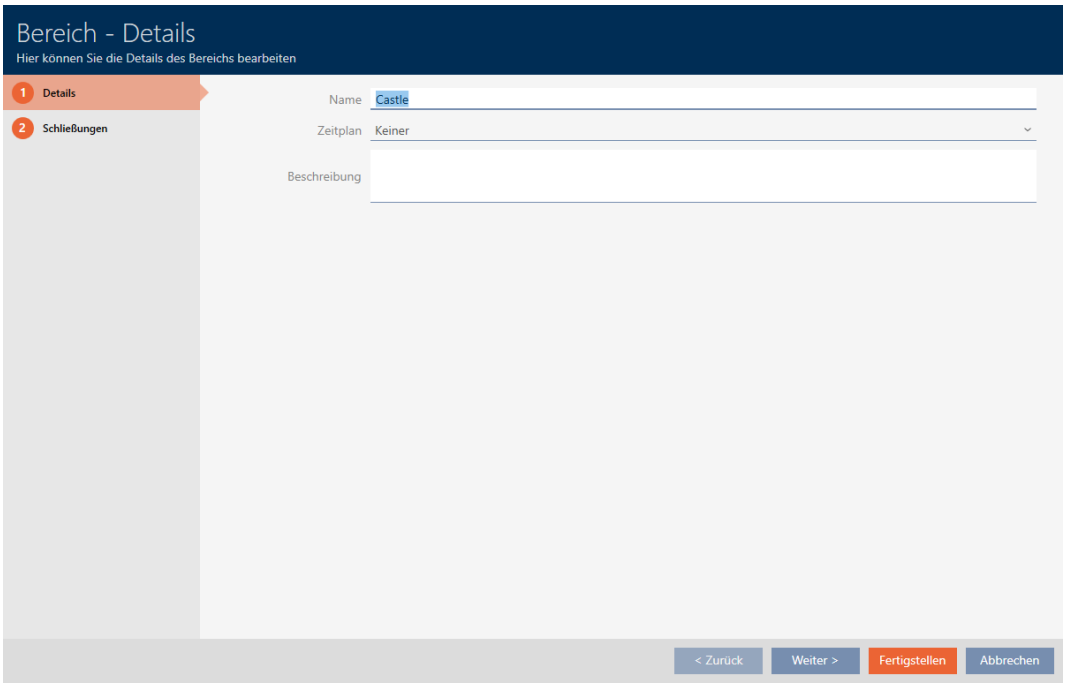
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Bereich aus.



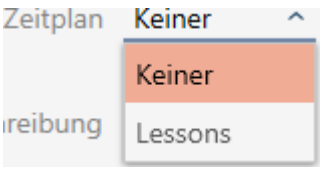
   ↳ Tab [Bereiche] öffnet sich.



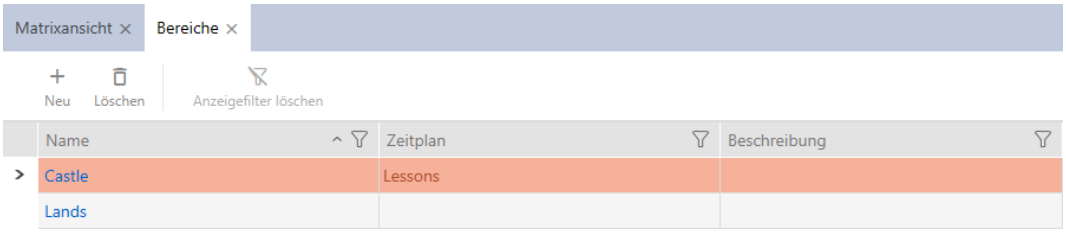
3. Wählen Sie rechts oben die Schließanlage mit dem Bereich aus, den Sie einer Zeitgruppe zuweisen wollen (alternativ: "Alle").
4. Klicken Sie auf den Bereich, den Sie einer Zeitgruppe zuweisen wollen.
   ↳ Fenster "Bereich" öffnet sich.



5. Wählen Sie im Dropdown-Menü ▼ **Zeitplan** den gewünschten Zeitplan aus.



6. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Bereich" schließt sich.
   ↳ Bereich mit Schließungen ist dem Zeitplan hinzugefügt.



Schließungen innerhalb eines Bereichs mit einem Zeitplan können auch einen anderen oder keinen Zeitplan bekommen. Wählen Sie dazu im Dropdown-Menü ▼ **Zeitplan** einen anderen Zeitplan aus.

Verhalten von vererbten Zeitplänen

Sie erkennen vererbte Zeitpläne am Zusatz ("vererbt").

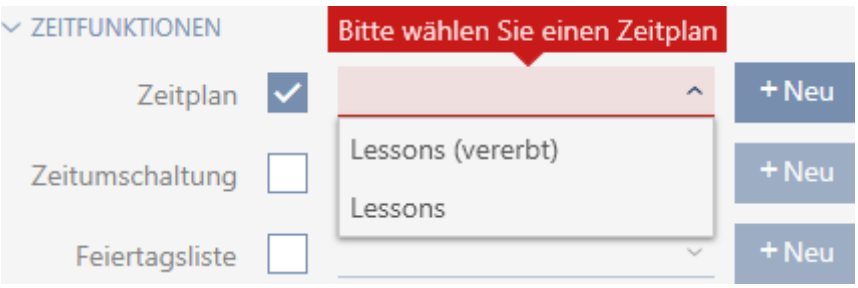
- Neu erstellte Schließungen erben den Zeitplan, wenn sie während der Erstellung einem Bereich mit Zeitplan zugewiesen werden.
- Bereits erstellte, aber noch nie synchronisierte Schließungen erben den Zeitplan, wenn Sie einem Bereich mit Zeitplan zugewiesen werden.
- Schließungen mit vererbten Zeitplänen übernehmen den Zeitplan des Bereichs, auch wenn dieser im Bereich geändert wird

  - Wenn der Zeitplan aus dem Bereich entfernt wird, dann verlieren auch Schließungen, die diesen geerbt haben, den Zeitplan.
  - Wenn Sie dem Bereich einen anderen Zeitplan zuweisen, dann ändert sich der Zeitplan auch bei den Schließungen, die den Zeitplan erben.
- Bereits synchronisierte Schließungen mit geerbtem Zeitplan erben den Zeitplan des neuen Bereichs, wenn ihnen ein neuer Bereich mit Zeitplan zugewiesen wird.
- Bereits synchronisierte Schließungen mit geerbtem Zeitplan verlieren den Zeitplan, wenn ihnen ein neuer Bereich ohne Zeitplan zugewiesen wird.
- Bereits synchronisierte Schließungen in einem Bereich ohne Zeitplan erben den Zeitplan, wenn ihrem Bereich ein Zeitplan zugewiesen wird.
- Schließungen mit manuell zugewiesenem Zeitplan behalten diesen, auch wenn sie einem Bereich mit Zeitplan zugewiesen werden.

Bestehende und synchronisierte Schließungen einen Zeitplan erben lassen

In manchen Fällen erben Schließungen den Zeitplan aus Sicherheitsgründen nicht automatisch. Sie können diese "Vererben"-Beziehung für den Zeitplan dennoch manuell einstellen:

1. Aktivieren Sie in den Details der jeweiligen Schließungen die Checkbox ☑ Zeitplan.
2. Wählen Sie danach den Eintrag mit dem Zusatz "vererbt" aus.



3. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ Schließung erbt den Zeitplan des Bereichs.

17.3 Bedeutung der Berechtigungskreuze in der Matrix

Kreuz	Bedeutung
	Nicht berechtigt.
×	In der Datenbank berechtigt, aber noch nicht programmiert.
✕	Berechtigt und programmiert.
	Berechtigung entzogen, aber Entfernen der Berechtigung noch nicht programmiert.
▸×	In der Datenbank durch eine Berechtigungsgruppe berechtigt, aber noch nicht programmiert.
▸✕	Durch eine Berechtigungsgruppe berechtigt und programmiert.
▸	Berechtigung durch eine Berechtigungsgruppe vorhanden und programmiert, diese Berechtigung wurde manuell entfernt. Entfernen der Berechtigung noch nicht programmiert.
▸	Berechtigung durch eine Berechtigungsgruppe vorhanden, diese Berechtigung wurde aber vor dem Programmieren manuell entfernt.
	Berechtigt und programmiert, Identmedium wurde aber (z.B. nach Diebstahl) gesperrt.

Kreuz	Bedeutung
	Nicht berechtigt, Identmedium wurde (z.B. nach Diebstahl) gesperrt. Oder: Nicht möglich, z.B. PinCode-Tastatur wurde anderer Schließung zugewiesen.

18. Schließanlagen

18.1 Schließanlage erstellen

Mit der AXM Plus haben Sie die Freiheit, mehrere Schließanlagen einzusetzen (Hintergrundinformationen zum Thema Schließanlagen siehe *Schließanlagen [▸ 541]*).

Ihre erste Schließanlage haben Sie wahrscheinlich schon mit dem Assistenten nach dem ersten Start Ihres Projekts erstellt (siehe *Erste Schritte nach der Installation [▸ 30]*). Weitere Schließanlagen erstellen Sie im Tab [Schließanlagen]:

ACHTUNG

Schließanlagenpasswort zugänglich und sicher aufbewahren

Das Schließanlagenpasswort ist das wichtigste Passwort überhaupt. Aus Sicherheitsgründen kann auch SimonsVoss keine Komponenten ohne Schließanlagenpasswort oder Backup zurücksetzen. Einen Generalschlüssel gibt es nicht.

Komponenten, zu denen kein Schließanlagenpasswort mehr bekannt oder über ein Backup wiederherstellbar ist, können nicht mehr programmiert werden. Sie müssen aufwendig aus Schlössern entfernt und entsorgt werden.

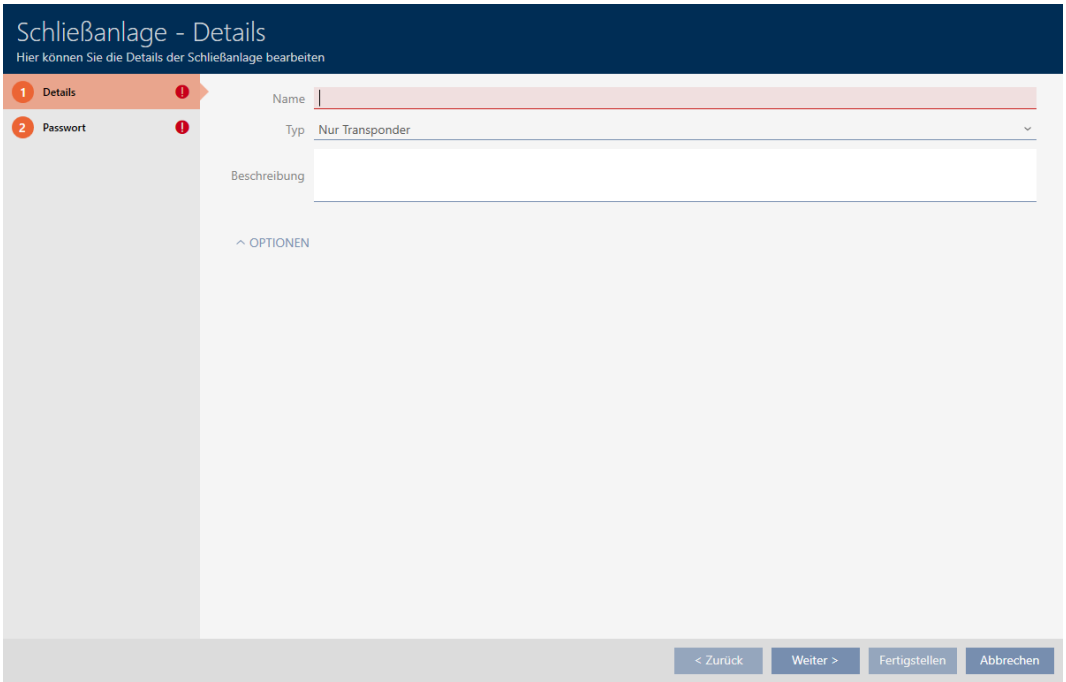
1. Stellen Sie sicher, dass das Schließanlagenpasswort jederzeit durch befugte Personen einsehbar und/oder zugänglich ist.
2. Berücksichtigen Sie dabei auch sowohl vorhersehbare Ereignisse (z.B. Schließanlagenverwalter geht in Rente) und unvorhersehbare Ereignisse (z.B. Schließanlagenverwalter kündigt).

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

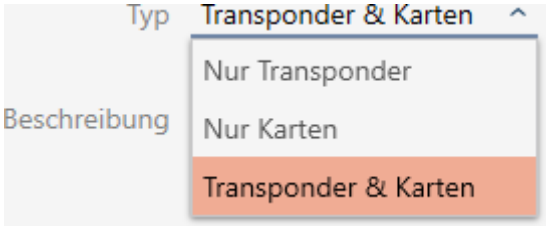
2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Schließanlagen aus.

↳ Tab [Schließanlagen] mit einer Auflistung aller Schließanlagen in der Datenbank öffnet sich.

3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster Schließanlage öffnet sich.



4. Geben Sie im Feld *Name* einen Namen für Ihre Schließanlage ein.
5. Wählen Sie im Dropdown-Menü ▼ **Typ** aus, welche Identmedien Ihre Schließanlage unterstützen soll ("Nur Transponder", "Nur Karten" oder "Transponder & Karten").



HINWEIS

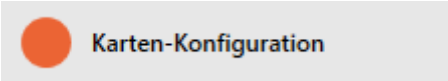
Karten nicht "vorsichtshalber" aktivieren

Karten (oder RFID-Inlays, Tags, etc...) haben einen begrenzten Speicherplatz. Deshalb kann nur eine begrenzte Menge an Schließungs-IDs aus Ihrer Schließanlage mit Karten verwendet werden (siehe *Karten und Schließungs-IDs [▸ 573]*). Die genaue Anzahl entnehmen Sie dem Kapitel *Kartentemplates [▸ 577]* - die Schließungs-IDs 0 bis 127 sind für interne Zwecke reserviert.

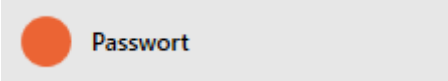
Beispiel: MC1000L_AV verwendet die Schließungs-IDs 0-1127. Sie können zwar 64.000 Schließungen erstellen und für Transponder nutzen, aber nur 1.000 davon für Ihre Karten nutzen (nämlich die mit einer Schließungs-ID zwischen 128 und 1127).

1. Wählen Sie "Transponder", wenn Sie voraussichtlich keine Karten o.ä. RFID-Identmedien verwenden werden.
2. Aktivieren Sie Karten bei Bedarf später (siehe *Karten bzw. Transponder freischalten [▸ 401]*).

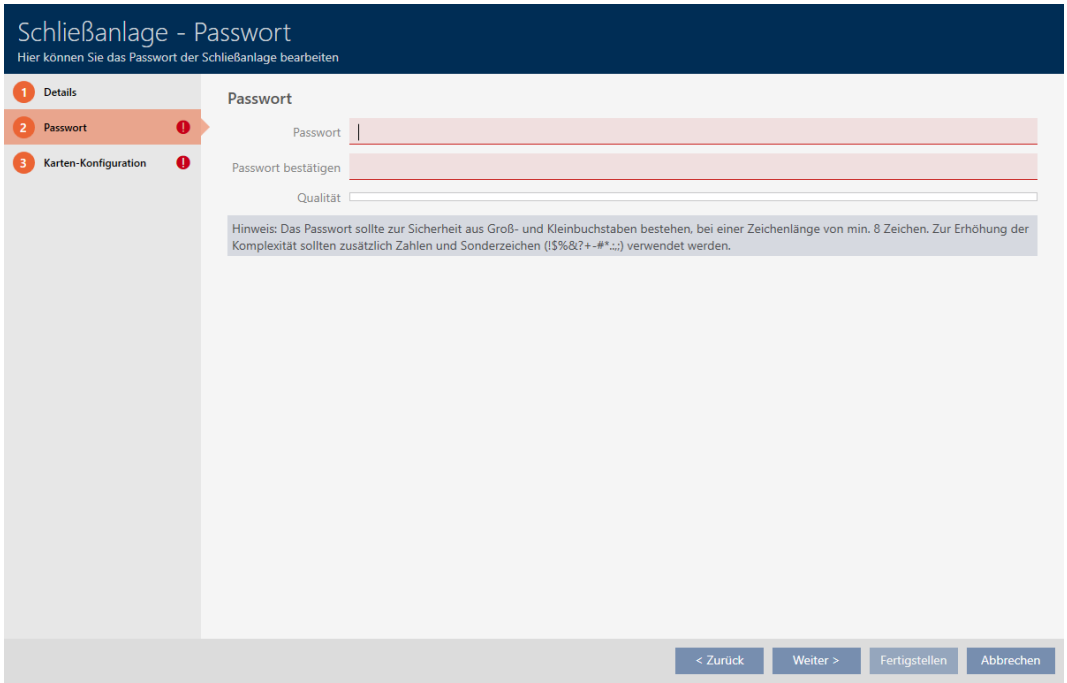
↳ Bei "Nur Karten" oder "Transponder & Karten" wird der Reiter ● Karten-Konfiguration eingeblendet.



6. Geben Sie ggfs. im Feld *Beschreibung* eine Beschreibung ein.
7. Klicken Sie auf den Reiter ● Passwort

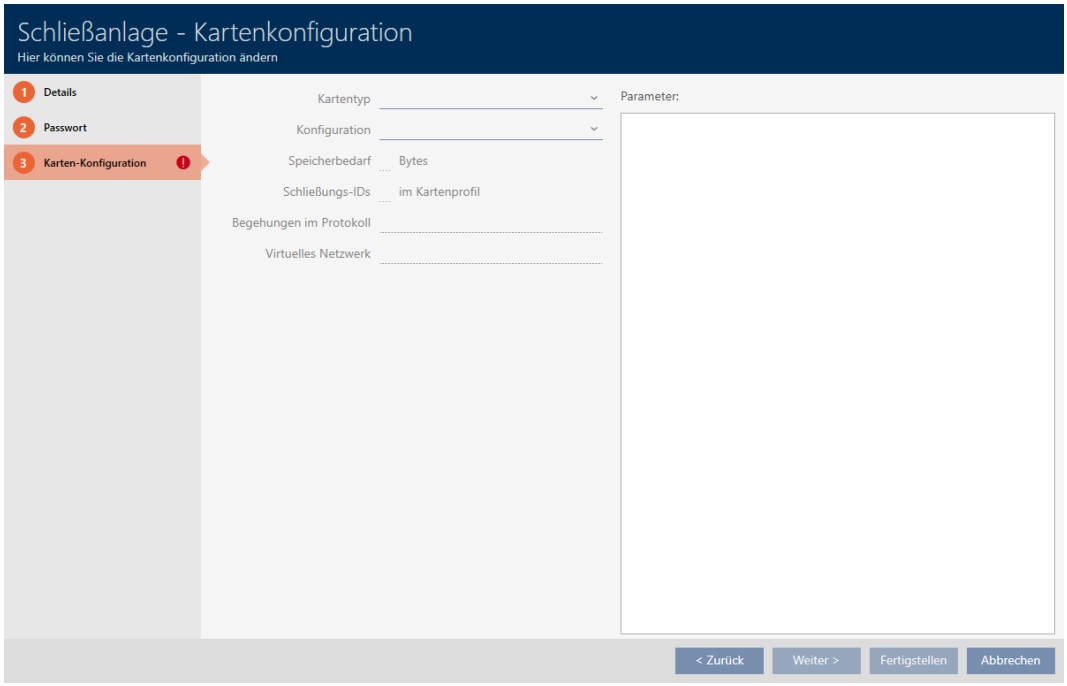


↳ Fenster wechselt zum Reiter "Passwort".

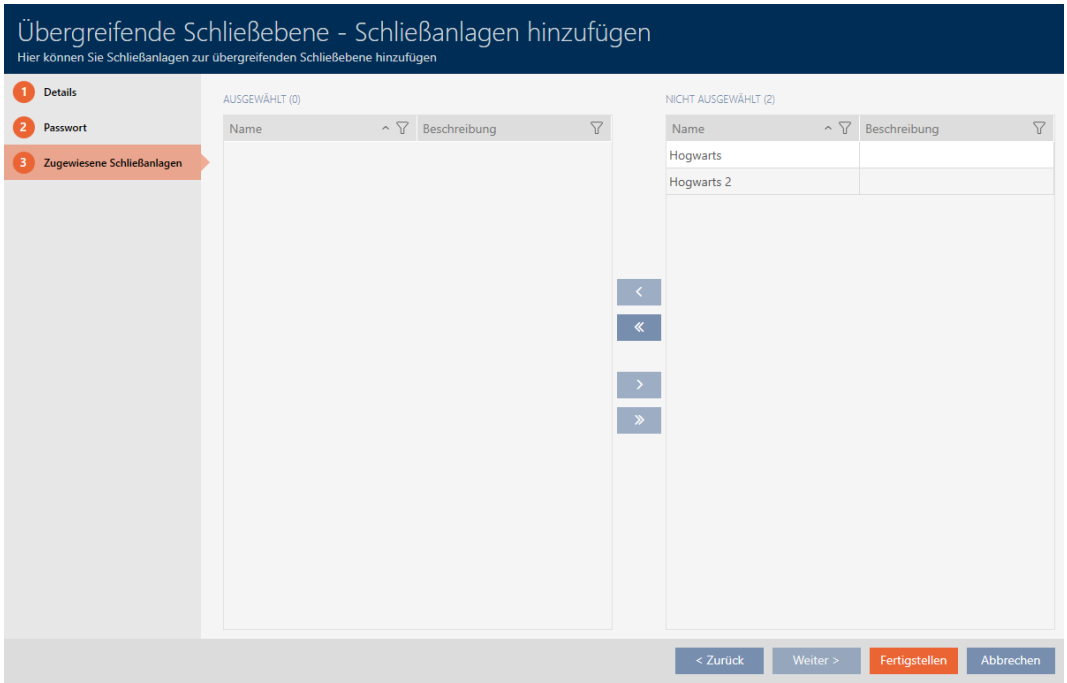


8. Geben Sie im Feld *Passwort* das Schließanlagenpasswort für Ihre neue Schließanlage ein.
9. Wiederholen Sie das Schließanlagenpasswort im Feld *Passwort bestätigen*.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

   ↳ Wenn Ihre Schließanlage den Typ "Nur Transponder" hat und Sie keine übergreifende Schließebene nutzen wollen, sind Sie jetzt fertig.
10. Wechseln Sie mit der Schaltfläche Karten-Konfiguration zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.
   ↳ Fenster wechselt zum Reiter "Karten-Konfiguration".

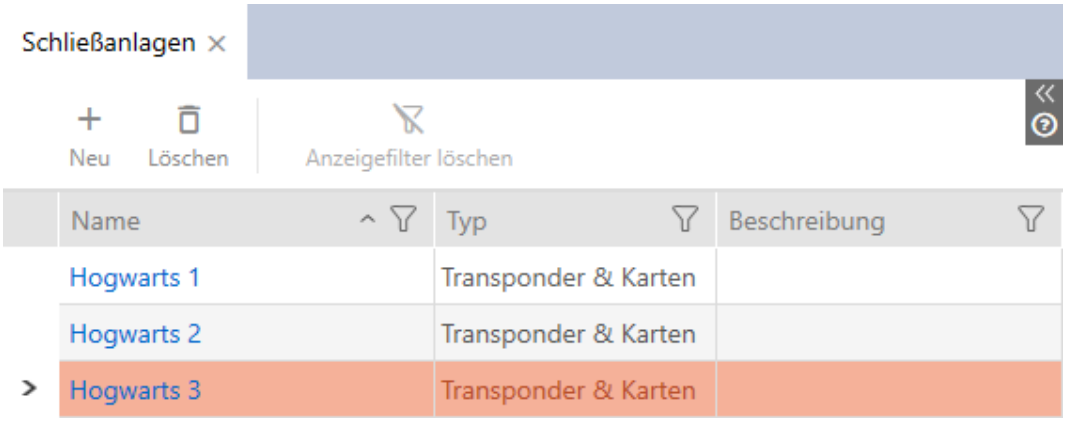


11. Geben Sie hier Ihre Kartenkonfiguration ein (Zur Kartenkonfiguration siehe *Kartenkonfiguration anlegen [▸ 365]*).
12. Klicken Sie auf die Schaltfläche Fertigstellen oder Weiter >, um die Schließanlage gleich einer übergreifenden Schließebene zuzuweisen.



13. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Schließanlage" schließt sich.

↳ Neue Schließanlage wird aufgelistet.

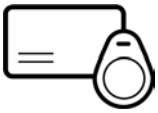


Informationen zur Aufbaureihenfolge Ihrer Schließanlage finden Sie hier: *Best Practice: Schließanlage aufbauen [▸ 32]*.

18.1.1 Kartenkonfiguration anlegen

Die folgenden Kapitel beschreiben, wie Sie eine Kartenkonfiguration für Ihre Schließanlage ermitteln und in Ihrer AXM Plus einstellen.

Verfügbare RFID-Identmedien



Die Beschreibung bezieht sich auf "Karten". Das Vorgehen ist aber bei allen unterstützten RFID-Identmedien ähnlich, z.B.:

- Karten
- SmartTags
- RFID-Inlays

HINWEIS

Kartenanalyse durch SimonsVoss

Die Analyse Ihrer Karten und das Ermitteln der richtigen Kartenkonfiguration für einen reibungslosen Betrieb kann anspruchsvoll sein, insbesondere im Zusammenhang mit bereits eingesetzten Karten.

Deshalb können Sie sich auch einfach von SimonsVoss helfen lassen.

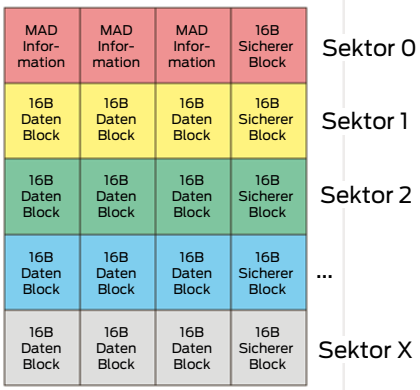
1. Wenn Sie sich für eine Kartenprüfung durch SimonsVoss entscheiden: Wenden Sie sich gerne an einen unserer Vetriebs-Außendienstmitarbeiter in Ihrer Region.
2. Wenn Sie die Kartenkonfiguration selbst ermitteln wollen: Lesen Sie die folgenden Kapitel sorgfältig durch.

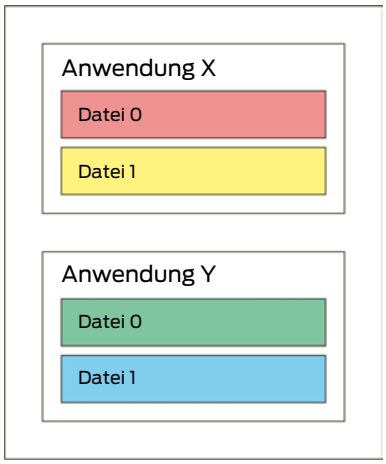
Grundlagen: MIFARE DESFire und MIFARE Classic

Bei RFID-Identmedien sind die Verschlüsselungstechniken MIFARE DESFire und MIFARE Classic die wichtigsten:

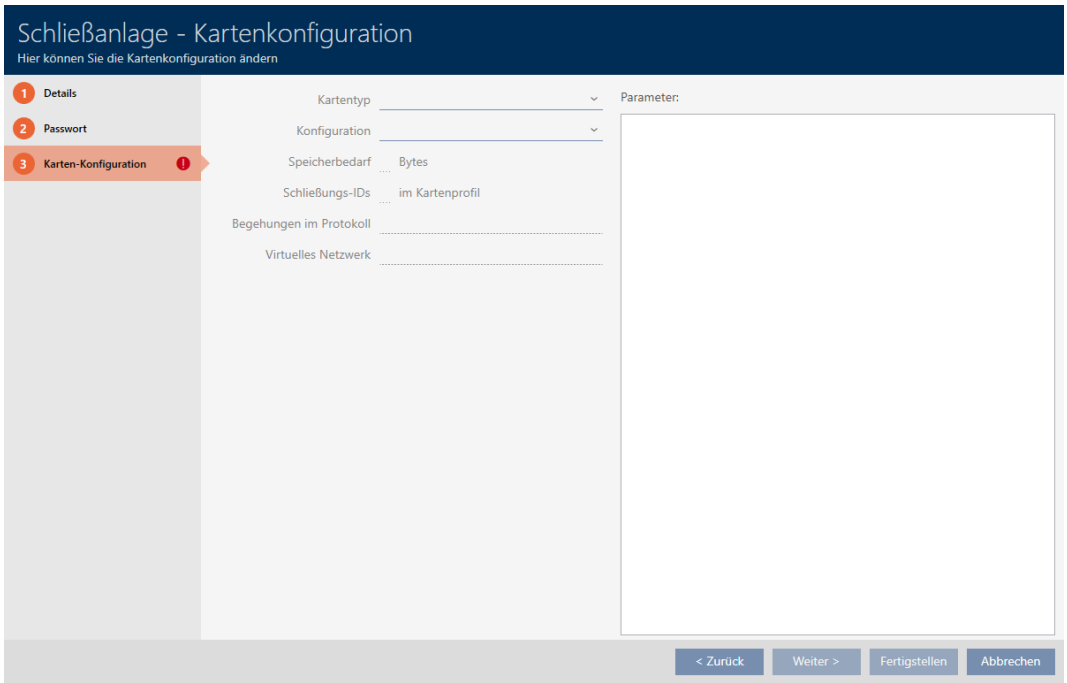
MIFARE Classic	MIFARE DESFire
▪ Einfacher Schutz ▪ Preiswerte Identmedien ▪ Begrenzte Leistungsfähigkeit ▪ Speicher als Zahlen/ Buchstabenfolge	▪ Guter Schutz ▪ Leistungsfähige Identmedien ▪ Speicher als Dateisystem ▪ Flexiblere Handhabung
Die Verschlüsselung von MIFARE Classic gilt mittlerweile als unsicher. Deshalb rät SimonsVoss dazu, nur noch MIFARE DESFire einzusetzen.	

MIFARE Classic	MIFARE DESFire
▪ Daten in Sektoren gespeichert ▪ Adressierung mit Sektoren in Sektorenliste ▪ Sektorschutz über letzten Block im Sektor ▪ MIFARE-Classic-Verschlüsselung gehackt und inzwischen unsicher	▪ Daten in Dateien gespeichert ▪ Adressierung mit Application ID ▪ Datei durch Leseschlüssel der Datei gesichert ▪ Schließanlagendaten müssen in einer Datei einer Applikation gespeichert sein, Lesezugriff auf die Datei ist notwendig ▪ Verschlüsselung mit AES (128 Bit)
Aufteilung des Speichers:	Aufteilung des Speichers:





Einzugebende Werte vorab ermitteln



Vor der Eingabe müssen Sie die Werte erst ermitteln. Zum Auslesen Ihrer Karten bietet sich ein NFC-fähiges Smartphone an. In den Beispielen wird Android mit der NXP-App "TagInfo" gezeigt (*https://play.google.com/store/apps/details?id=com.nxp.taginfolite*). Der benötigte Report ist der "Full Report".

Notieren Sie sich die ermittelten Werte. Je nachdem, welche Situation vorliegt, gehen Sie dazu anders vor:

- *MIFARE Classic (neue/leere Karte) [▸ 368]*
- *MIFARE Classic (bereits verwendete Karte) [▸ 373]*
- *MIFARE DESFire (neue/leere Karte) [▸ 381]*

- *MIFARE DESFire (bereits verwendete Karte) [▸ 387]*

Anschließend können Sie die Werte für die Kartenkonfiguration eingeben.

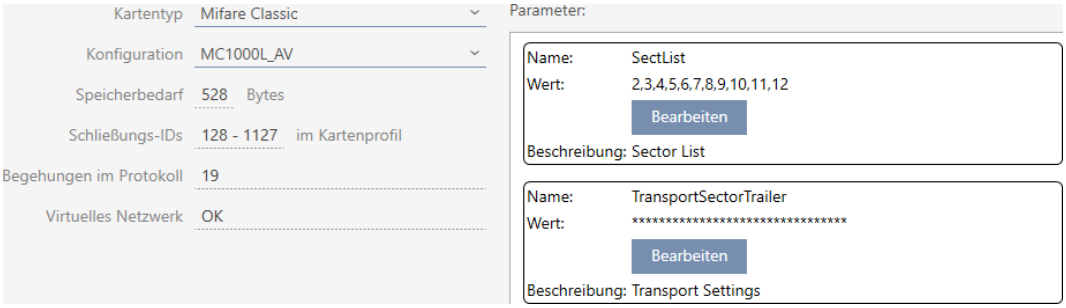
Kartenkonfiguration eingeben

✓ Reiter "Schließanlage - Kartenkonfiguration" geöffnet (siehe *Schließanlage erstellen [▸ 360]* oder *Karten bzw. Transponder freischalten [▸ 401]*)

1. Wählen Sie im Dropdown-Menü ▼ **Kartentyp** Ihren Kartentyp aus.
2. Wählen Sie im Dropdown-Menü ▼ **Konfiguration** Ihre gewünschte Konfiguration aus.
3. Geben Sie die restlichen zuvor ermittelten, Parameter im rechten Bereich ein.
4. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ Kartenkonfiguration ist eingestellt.

18.1.1.1 MIFARE Classic (neue/leere Karte)



Während der Konfiguration werden folgende Parameter ermittelt:

- ▼ **Kartentyp**: MIFARE Classic oder DESFire
- ▼ **Konfiguration**: Kartentemplate (siehe *Kartentemplates [▸ 577]*)

  Das Kartentemplate bestimmt über:

  - *Speicherbedarf*: Muss an freiem Speicherplatz auf der Karte zur Verfügung stehen.
  - *Schließungs-IDs*: Zeigt die Anzahl möglicher Schließungs-IDs für diese Karte an. AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert.

    Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
  - *Begehungen im Protokoll*: Zeigt die Anzahl an Einträgen, die in die Begehungsliste dieser Karte geschrieben werden können. Nur für AV-Templates (**A**udit trail & **V**irtual network).

- *Virtuelles Netzwerk*: Zeigt an, ob ein virtuelles Netzwerk möglich ist. Nur für AV-Templates.

Für MIFARE Classic werden außerdem ermittelt:

- *SectList*: Liste der Sektoren, auf denen die Daten Ihrer Schließanlage gespeichert werden.
- *TransportSectorTrailer*: Verschlüsselung der Daten Ihrer Schließanlage auf der Karte

✓ Kartentyp: MIFARE Classic

1. Lesen Sie die Karte aus oder konsultieren Sie das Datenblatt.
   ↳ Full Report wird angezeigt.
2. Ermitteln Sie den verfügbaren Speicherplatz bzw. die verfügbaren Sektoren (Abschnitt *EXTRA # Memory size*).

```
-- EXTRA ------------------------------
# Memory size:
1 kB
* 16 sectors, with 4 blocks per sector
* 64 blocks, with 16 bytes per block
```

   ↳ Karte enthält 16 Sektoren.
   ↳ Sektor 0 ist bei MIFARE Classic intern und Sektor 1 sollte nicht genutzt werden, also stehen 14 Sektoren zur Verfügung.

HINWEIS

Sektorstruktur kartenspezifisch

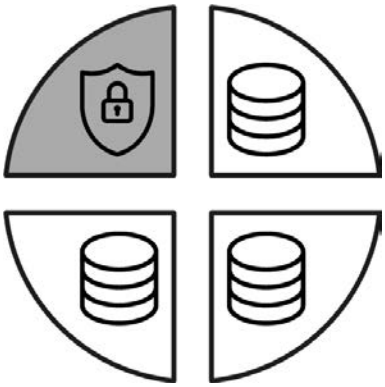
Die Sektorstruktur kann bei Ihrer Karte abweichen. Insbesondere Karten mit größerem Speicher können weitere Mastersektoren haben (z.B. häufig Sektor 16) und haben andere Sektorgrößen, d.h. mehr Speicherplatz pro Sektor.

Selbst auf neuen Karten können Sektoren vom Hersteller gesperrt sein und müssen erst entsperrt werden.

Beispiel: MIFARE Classic EV1 4k: 4kB Speicher, aufgeteilt in Sektoren 0-31 mit jeweils 4 Blöcken und Sektoren 32-39 mit jeweils 16 Blöcken. Sektor 16 ist dabei ein weiterer Mastersektor.

1. Lesen Sie den Report sorgfältig, um Mastersektoren und die Sektorgröße zu bestimmen.
2. Wenn Sie sich für eine Kartenprüfung durch SimonsVoss entscheiden: Wenden Sie sich gerne an einen unserer Vetriebs-Außendienstmitarbeiter in Ihrer Region.

↳ Jeder Sektor besteht aus drei beschreibbaren Blöcken und einem Block für die Verschlüsselung: 3*16 Byte = 48 Byte pro Sektor.



↳ Verfügbare Sektoren sind im Report an drei Blöcken mit [rwi] erkennbar: *read/write/increment* - der vierte Block ist für die Verschlüsselung.

```
Sector 1 (0x01)
[04] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[05] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[06] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[07] wxx  FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
          Factory default key           Factory default key (readable)
```

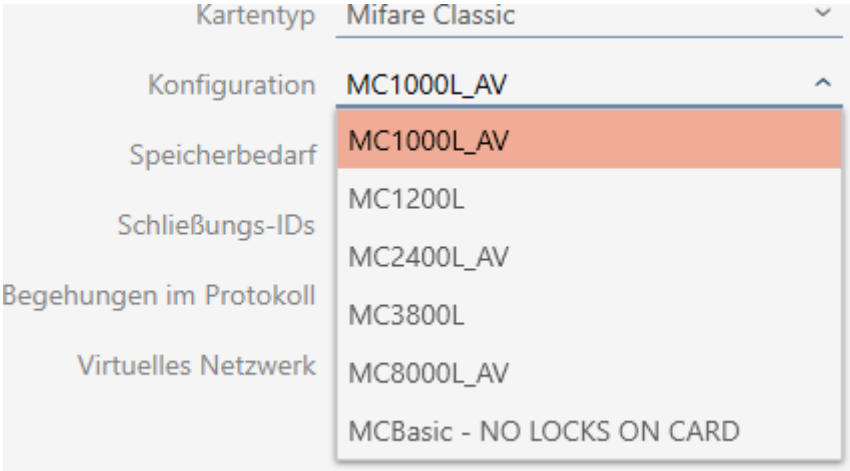
↳ Karteninterne Sektoren sind im Report daran erkennbar, dass nicht alle drei Blöcke mit [rwi] gekennzeichnet sind:

```
Sector 0 (0x00)
[00] r--  50 07 32 57 32 88 04 00 46 8F 74 D0 65 40 23 11 |P.2W2...F.t.e@#.|
[01] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[02] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[03] wxx  FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
          Factory default key           Factory default key (readable)
```

3. Berechnen Sie den verfügbaren Speicherplatz: Bytes pro Sektor * verfügbare Sektoren (Beispiel: 48 Byte * 14 Sektoren = 672 Byte).
4. Wählen Sie im Dropdown-Menü ▼ **Kartentyp** den Eintrag "Mifare Classic".

5. Überlegen Sie, ob Sie eine Begehungsliste oder ein virtuelles Netzwerk für Ihre Karten brauchen.
   ↳ Wenn ja: Sie benötigen ein AV-Template (="**A**udit trail und "**V**irtual network").

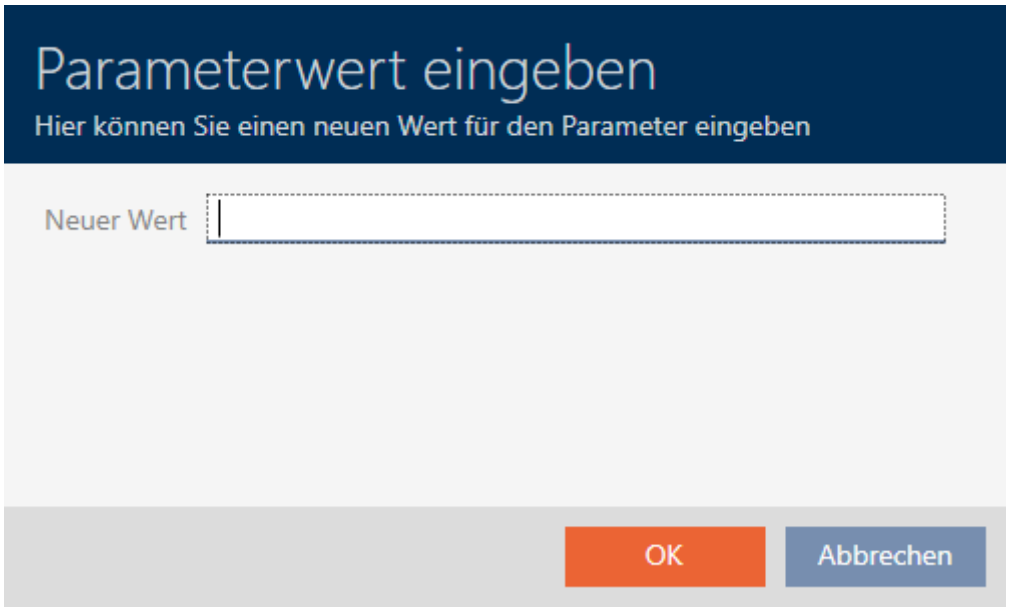
6. Bestimmen Sie die größte Kartenkonfiguration, die in den verfügbaren Speicherplatz passt (siehe *Kartentemplates [▸ 577]* - Beispiel für AV: MC1000L_AV mit 528 Byte).



7. Wählen Sie im Dropdown-Menü ▼ **Konfiguration** die eben bestimmte Konfiguration aus (Beispiel: MC1000L_AV).
   - *Speicherbedarf* zeigt den Speicherbedarf auf der Karte.
   - *Schließungs-IDs* zeigt die Anzahl möglicher Schließungs-IDs für diese Karte (AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert). Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
   - *Begehungen im Protokoll* zeigt die Anzahl möglicher Einträge in der Begehungsliste (nur für AV-Templates).

   - Anzahl der Einträge für Schließungen in der Matrix wird auf die Anzahl der möglichen Schließungs-IDs begrenzt. Dabei können Schließungen auch mehr als einen Eintrag verbrauchen, z.B. freidrehende Digital Cylinder AX.
   - Begehungsliste wird rollierend überschrieben, ist also nicht limitiert.
   - Virtuelles Netzwerk ist möglich.

8. Berechnen Sie die Anzahl tatsächlich nötiger Sektoren: *Speicherbedarf* / Bytes pro Sektor (Beispiel: 528 Byte / 48 Byte = 11 Sektoren). Runden Sie das Ergebnis ggfs. auf die nächste ganze Zahl auf.
9. Klicken Sie im Feld *SectList* auf die Schaltfläche Bearbeiten.
   ↳ Fenster "Parameterwert eingeben" öffnet sich.



10. Geben Sie im Feld *Neuer Wert* so viele freie Sektoren ein, wie Sie benötigen (Beispiel: 2,3,4,5,6,7,8,9,10,11,12). Verwenden Sie dabei keine Sektoren, die nicht beschreibbar sind oder als Mastersektor genutzt werden (Beispiel: Sektor 0 ist nicht beschreibbar und Sektor 1 ist ein Mastersektor).
    Zahlen durch Kommata getrennt, ohne Leerzeichen.

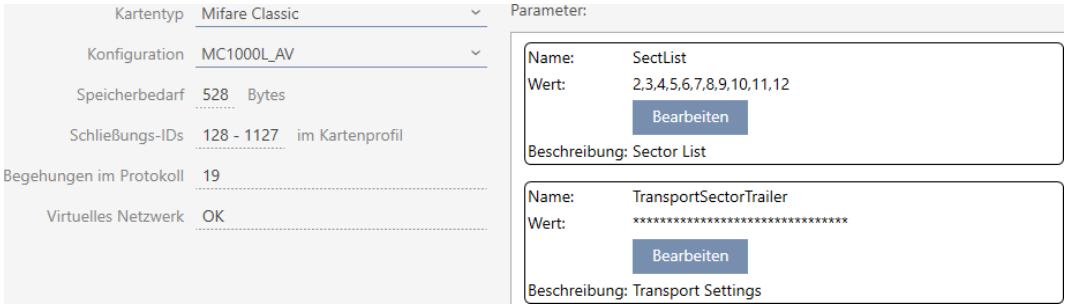
HINWEIS

Gesparter Speicherplatz durch eigene Sektorliste

Sie können selbstverständlich auch die standardmäßig eingetragene Sektorliste verwenden. Allerdings kann es sein, dass gar nicht alle Sektoren aus dieser Liste benutzt werden, weil die Kartenkonfiguration auch in weniger Sektoren passt.

- Tragen Sie eine eigene Sektorliste ein.
  ↳ Damit können Sie Sektoren auf Ihren Karten sparen, die Sie in Zukunft vielleicht für andere Anwendungen nutzen wollen.

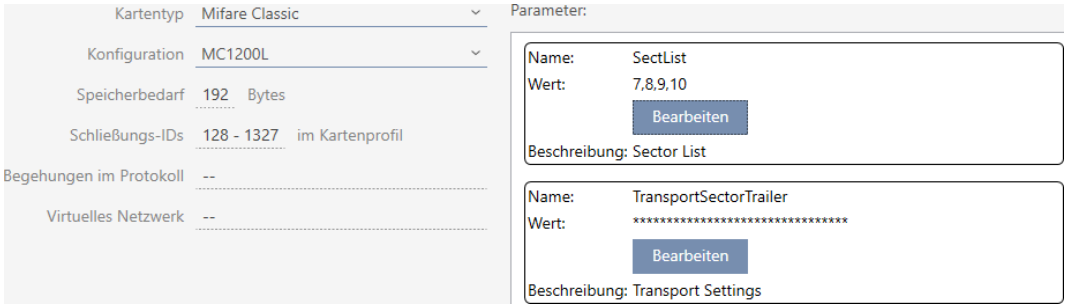
11. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
12. Lassen Sie das Feld *TransportSectorTrailer* unverändert.
    ↳ TransportSectorTrailer ist ein Bestandteil der Verschlüsselung der Karte. Ihre AXM Plus erzeugt diesen Eintrag automatisch für Sie.



13. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Schließanlage" schließt sich.

↳ Kartenkonfiguration gespeichert.

18.1.1.2 MIFARE Classic (bereits verwendete Karte)



- ▼ **Kartentyp**: MIFARE Classic oder DESFire
- ▼ **Konfiguration**: Kartentemplate (siehe *Kartentemplates [▸ 577]*)

  Das Kartentemplate bestimmt über:

  - *Speicherbedarf*: Muss an freiem Speicherplatz auf der Karte zur Verfügung stehen.
  - *Schließungs-IDs*: Zeigt die Anzahl möglicher Schließungs-IDs für diese Karte an. AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert.

    Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
  - *Begehungen im Protokoll*: Zeigt die Anzahl an Einträgen, die in die Begehungsliste dieser Karte geschrieben werden können. Nur für AV-Templates (**A**udit trail & **V**irtual network).
  - *Virtuelles Netzwerk*: Zeigt an, ob ein virtuelles Netzwerk möglich ist. Nur für AV-Templates.

Für MIFARE Classic werden außerdem ermittelt:

- *SectList*: Liste der Sektoren, auf denen die Daten Ihrer Schließanlage gespeichert werden.

- *TransportSectorTrailer*: Verschlüsselung der Daten Ihrer Schließanlage auf der Karte

✓ Kartentyp: MIFARE Classic

1. Lesen Sie die Karte aus oder konsultieren Sie das Datenblatt.
   ↳ Full Report wird angezeigt.
2. Ermitteln Sie den verfügbaren Speicherplatz bzw. die verfügbaren Sektoren (Abschnitt *EXTRA # Memory size*).

```
-- EXTRA ------------------------------
# Memory size:
1 kB
* 16 sectors, with 4 blocks per sector
* 64 blocks, with 16 bytes per block
```

   ↳ Karte enthält 16 Sektoren.
   ↳ Sektor 0 ist bei MIFARE Classic intern und Sektor 1 sollte nicht genutzt werden, also stehen 14 Sektoren zur Verfügung.

HINWEIS

Sektorstruktur kartenspezifisch

Die Sektorstruktur kann bei Ihrer Karte abweichen. Insbesondere Karten mit größerem Speicher können weitere Mastersektoren haben (z.B. häufig Sektor 16) und andere Sektorgrößen, d.h. mehr Speicherplatz pro Sektor.

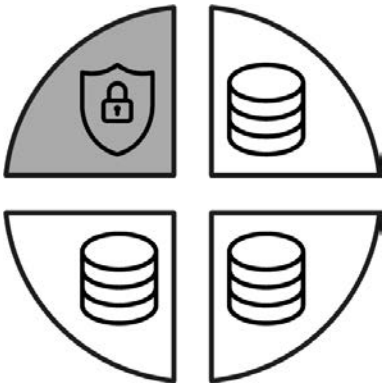
Selbst auf neuen Karten können Sektoren vom Hersteller gesperrt sein und müssen erst entsperrt werden.

In manchen Fällen blockieren Fremdanwendungen auch alle Sektoren, obwohl gar nicht alle Sektoren genutzt werden.

Beispiel: MIFARE Classic EV1 4k: 4kB Speicher, aufgeteilt in Sektoren 0-31 mit jeweils 4 Blöcken und Sektoren 32-39 mit jeweils 16 Blöcken. Sektor 16 ist dabei ein weiterer Mastersektor.

1. Lesen Sie den Report sorgfältig, um Mastersektoren und die Sektorgröße zu bestimmen.
2. Wenn Sie sich für eine Kartenprüfung durch SimonsVoss entscheiden: Wenden Sie sich gerne an einen unserer Vetriebs-Außendienstmitarbeiter in Ihrer Region.
3. Entsperren Sie bei Bedarf blockierte ungenutzte Sektoren mit dem TransportSectorTrailer.

   ↳ Jeder Sektor besteht aus drei beschreibbaren Blöcken und einem Block für die Verschlüsselung: 3*16 Byte = 48 Byte pro Sektor.



↳ Verfügbare Sektoren sind im Report an drei Blöcken mit [rwi] erkennbar: *read/write/increment* - der vierte Block ist für die Verschlüsselung.

```
Sector 1 (0x01)
[04] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[05] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[06] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[07] wxx  FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
          Factory default key           Factory default key (readable)
```

↳ Karteninterne Sektoren sind im Report daran erkennbar, dass nicht alle drei Blöcke mit [rwi] gekennzeichnet sind:

```
Sector 0 (0x00)
[00] r--  50 07 32 57 32 88 04 00 46 8F 74 D0 65 40 23 11 |P.2W2...F.t.e@#.|
[01] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[02] rwi  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |................|
[03] wxx  FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
          Factory default key           Factory default key (readable)
```

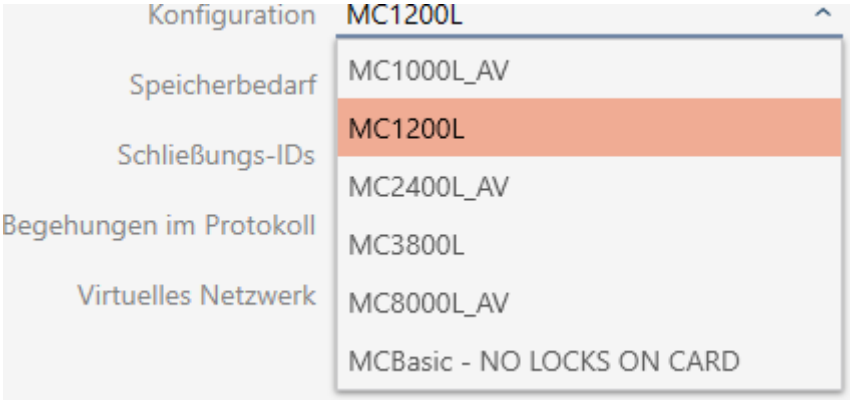
↳ Bereits genutzte Sektoren sind daran erkennbar, dass die Daten nicht mehr im Klartext lesbar sind:

```
Sector 2 (0x02)
[08] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[09] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0A] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0B] ???  XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
          (unknown key)                 (unknown key)

Sector 3 (0x03)
[0C] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0D] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0E] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0F] ???  XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
          (unknown key)                 (unknown key)

Sector 4 (0x04)
[10] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[11] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[12] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[13] ???  XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
          (unknown key)                 (unknown key)

Sector 5 (0x05)
[14] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[15] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[16] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[17] ???  XX:XX:XX:XX:XX:XX --:--:-- -- XX:XX:XX:XX:XX:XX
          (unknown key)                 (unknown key)
```

- ↳ Sektoren 2, 3, 4 und 5 sind bereits beschrieben (z.B. durch eine andere Anwendung) und nicht für die Schließanlage verfügbar.
- ↳ Sektoren 0 und 1 können auch nicht genutzt werden. Verfügbar sind also diese Sektoren: 6, 7, 8, 9, 10, 11, 12, 13, 14 und 15 (= 10 Sektoren für die Schließanlage verfügbar).

3. Berechnen Sie den verfügbaren Speicherplatz: Bytes pro Sektor * verfügbare Sektoren (Beispiel: 48 Byte * 10 Sektoren = 480 Byte).
4. Wählen Sie im Dropdown-Menü ▼ **Kartentyp** den Eintrag "Mifare Classic".

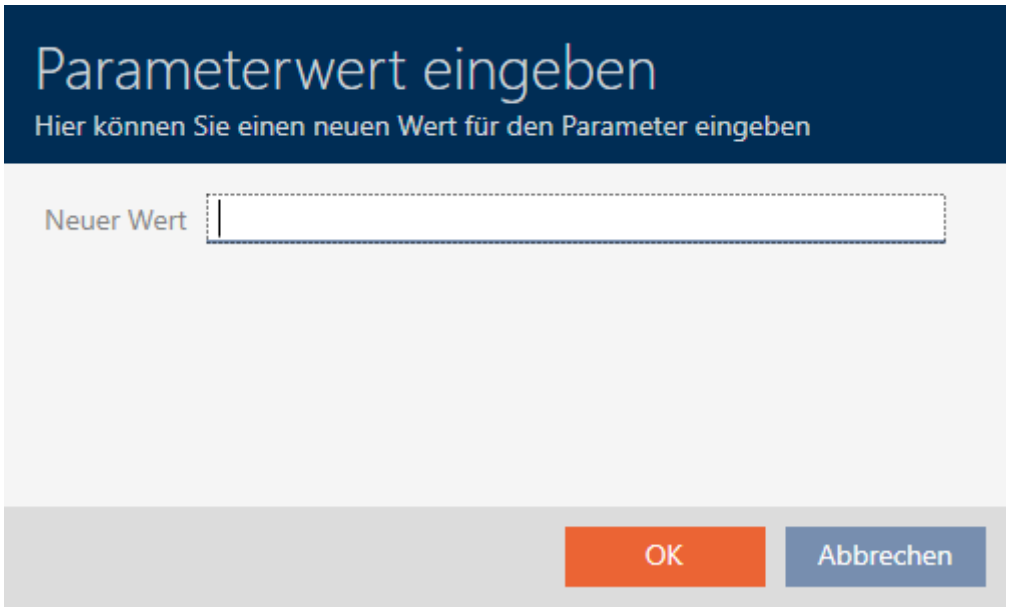
5. Überlegen Sie, ob Sie eine Begehungsliste oder ein virtuelles Netzwerk für Ihre Karten brauchen.
   ↳ Wenn ja: Sie benötigen ein AV-Template (="**A**udit trail und "**V**irtual network").
6. Bestimmen Sie die größte Kartenkonfiguration, die in den verfügbaren Speicherplatz passt (siehe *Kartentemplates [▸ 577]* - Beispiel: MC1200L mit 192 Byte).
7. Wählen Sie im Dropdown-Menü ▼ **Konfiguration** die eben bestimmte Konfiguration aus (Beispiel: MC1200L).



   ↳ *Speicherbedarf* zeigt den Speicherbedarf auf der Karte.
   ↳ *Schließungs-IDs* zeigt die Anzahl möglicher Schließungs-IDs für diese Karte (AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert). Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.

   ↳ Anzahl der Einträge für Schließungen in der Matrix wird auf die Anzahl der möglichen Schließungs-IDs begrenzt. Dabei können Schließungen auch mehr als einen Eintrag verbrauchen, z.B. freidrehende Digital Cylinder AX.
   ↳ Begehungsliste nicht verfügbar (ist kein AV-Template).
   ↳ Virtuelles Netzwerk nicht möglich.

8. Berechnen Sie die Anzahl tatsächlich nötiger Sektoren: *Speicherbedarf* / Bytes pro Sektor (Beispiel: 192 Byte / 48 Byte = 4 Sektoren). Runden Sie das Ergebnis ggfs. auf die nächste ganze Zahl auf.
9. Klicken Sie im Feld *SectList* auf die Schaltfläche Bearbeiten.
   ↳ Fenster "Parameterwert eingeben" öffnet sich.



10. Geben Sie im Feld *Neuer Wert* so viele freie Sektoren ein, wie Sie benötigen (Beispiel: 7,8,9,10). Verwenden Sie dabei keine Sektoren, die nicht beschreibbar sind oder als Mastersektor genutzt werden (Beispiel: Sektor 0 ist nicht beschreibbar und Sektor 1 ist ein Mastersektor).
    Zahlen durch Kommata getrennt, ohne Leerzeichen.

HINWEIS

Gesparter Speicherplatz durch eigene Sektorliste

Sie können selbstverständlich auch die standardmäßig eingetragene Sektorliste verwenden. Allerdings kann es sein, dass gar nicht alle Sektoren aus dieser Liste benutzt werden, weil die Kartenkonfiguration auch in weniger Sektoren passt.

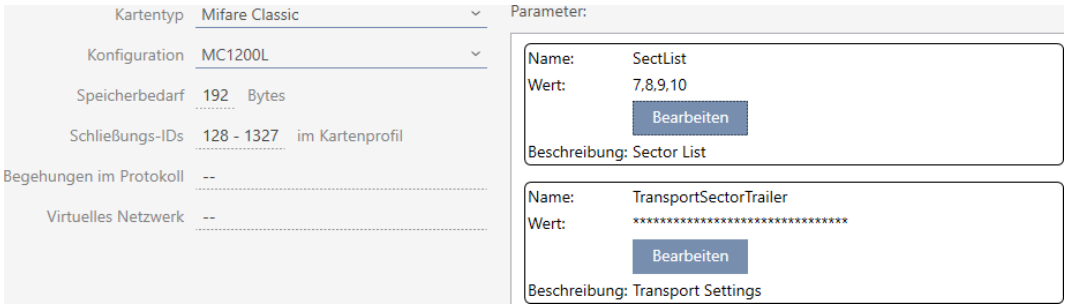
- Tragen Sie eine eigene Sektorliste ein.
  ↳ Damit können Sie Sektoren auf Ihren Karten sparen, die Sie in Zukunft vielleicht für andere Anwendungen nutzen wollen.

HINWEIS

Sektoren müssen nicht zusammenhängend sein

Die Sektorliste muss nicht zusammenhängend sein. Falls Sektoren in der Mitte der Sektorliste anderweitig genutzt werden, ist das für die AXM Plus kein Problem.

11. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
12. Lassen Sie das Feld *TransportSectorTrailer* unverändert.
    ↳ TransportSectorTrailer ist ein Bestandteil der Verschlüsselung der Karte. Ihre AXM Plus erzeugt diesen Eintrag automatisch für Sie.



13. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Schließanlage" schließt sich.

↳ Kartenkonfiguration gespeichert.

Die AXM Plus schreibt nur auf die in der Sektorliste angegebenen Sektoren. Alle anderen Sektoren bleiben unverändert.

Andere Anwendungen (z.B. eine Kantinen-Abrechnung) schreiben einfach weiterhin auf ihre "eigenen" Sektoren. Sie funktionieren - völlig unabhängig von Ihrer AXM Plus wie bisher.

Blockierte Sektoren mit dem TransportSectorTrailer entsperren

In Ausnahmefällen kann es sein, dass eine andere Anwendung Sektoren blockiert, aber tatsächlich gar nicht nutzt. In diesem Fall können Sie diese Sektoren durch Ihre AXM Plus "entsperren" und für Ihre Schließanlage nutzen.

HINWEIS

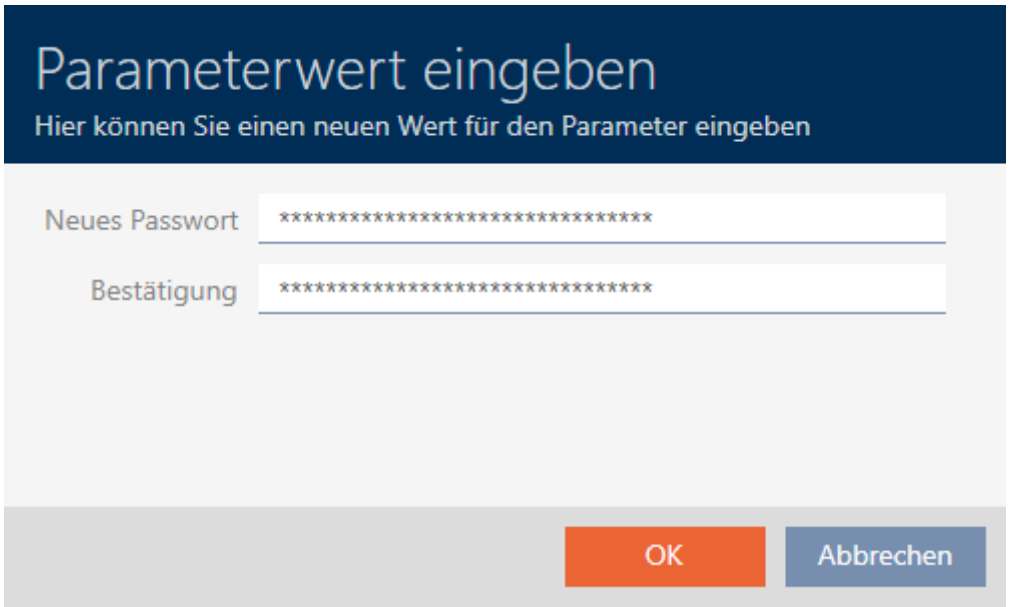
Fehlfunktionen anderer Anwendungen und/oder Ihrer Schließanlage

Daten in Sektoren, die von einer Anwendung genutzt werden, dürfen ausschließlich von dieser Anwendung verändert werden.

Wenn zum Beispiel Ihre Schließanlage die Daten in einem Sektor verändert, der von Ihrem Kantinensystem genutzt wird, dann kann das Kantinensystem die Daten höchstwahrscheinlich nicht mehr verarbeiten. Umgekehrt kann auch das Kantinensystem die Daten Ihrer Schließanlage unbrauchbar machen.

1. Stellen Sie vor dem Entsperren "fremder" Sektoren sicher, dass diese wirklich nicht genutzt werden.
2. Halten Sie Rücksprache mit dem Betreiber der Fremdanwendung bzw. dem Inhaber der Sektoren.
3. Wenn Sie sich für eine Kartenprüfung durch SimonsVoss entscheiden: Wenden Sie sich gerne an einen unserer Vetriebs-Außendienstmitarbeiter in Ihrer Region.

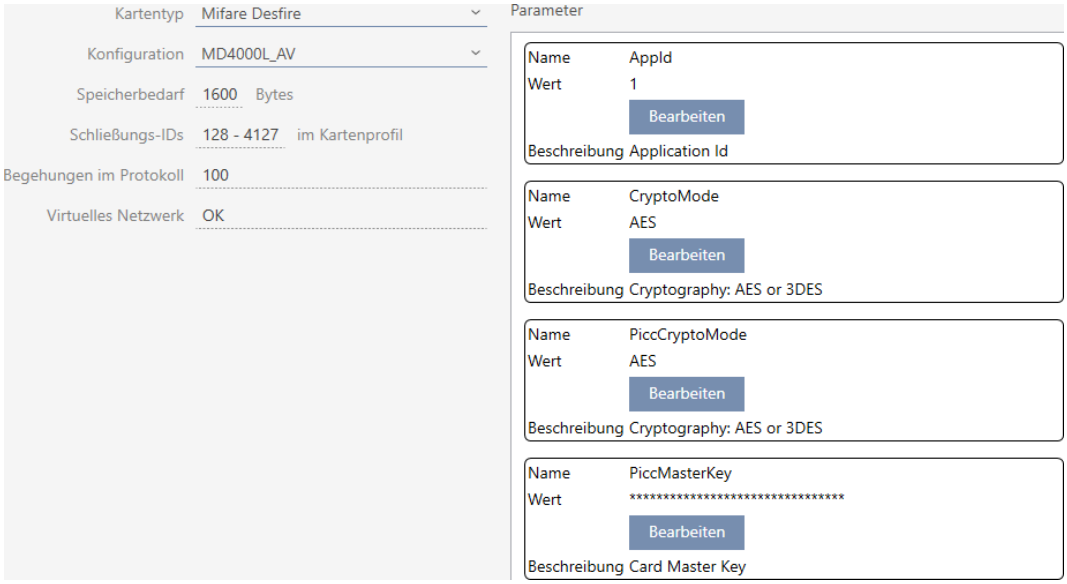
1. Klicken Sie im Bereich TransportSectorTrailer auf die Schaltfläche Bearbeiten .
   ↳ Fenster "Parameterwert eingeben" öffnet sich.



2. Geben Sie im Feld *Neues Passwort* den TransportSectorTrailer ein, den die andere Anwendung nutzt.

3. Wiederholen Sie im Feld *Bestätigung* die Eingabe.
4. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Parameterwert eingeben" schließt sich.
   ↳ AXM Plus entsperrt blockierte Sektoren und nutzt diese für die Schließanlage.

18.1.1.3 MIFARE DESFire (neue/leere Karte)



- ▼ **Kartentyp**: MIFARE Classic oder DESFire
- ▼ **Konfiguration**: Kartentemplate (siehe *Kartentemplates [▸ 577]*)

  Das Kartentemplate bestimmt über:

  - *Speicherbedarf*: Muss an freiem Speicherplatz auf der Karte zur Verfügung stehen.
  - *Schließungs-IDs*: Zeigt die Anzahl möglicher Schließungs-IDs für diese Karte an. AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert.

    Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
  - *Begehungen im Protokoll*: Zeigt die Anzahl an Einträgen, die in die Begehungsliste dieser Karte geschrieben werden können. Nur für AV-Templates (**A**udit trail & **V**irtual network).
  - *Virtuelles Netzwerk*: Zeigt an, ob ein virtuelles Netzwerk möglich ist. Nur für AV-Templates.

Für MIFARE DESFire werden außerdem ermittelt:

- *App-ID*: App-ID, in der die Daten Ihrer Schließanlage gespeichert werden.

- *CryptoMode*: Verschlüsselungsverfahren für die Daten Ihrer Schließanlage (Verschlüsselung der Inhalte Ihrer App-ID - Empfehlung: AES)
- *PiccCryptoMode*: Generelles Verschlüsselungsverfahren (Verschlüsselung der gesamten Karte - Empfehlung: AES)
- *PiccMasterKey*: Schlüssel, der die Karte vor vollständiger Formatierung schützt.

✓ Kartentyp: MIFARE DESFire

1. Lesen Sie die Karte aus oder konsultieren Sie das Datenblatt.
   ↳ Full Report wird angezeigt.
2. Ermitteln Sie den verfügbaren Speicherplatz (Abschnitt *# Memory information*).

```
# Memory information:
Size: 2 kB
Available: 2.3 kB
```

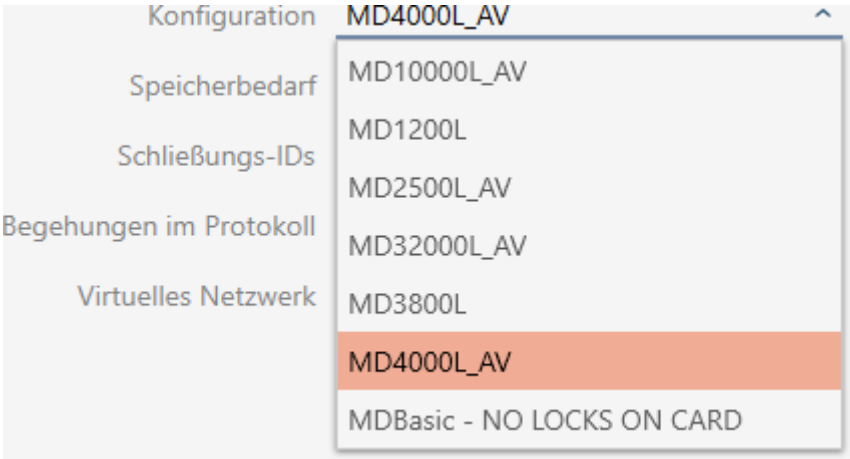
   ↳ Bei neuen/leeren Karten ist nur die AppID 0 belegt:

```
Application ID 0x000000 (PICC)
* Default master key
* Key configuration:
  - 1 (3)DES key
  - Master key changeable
  - Master key required for:
    ~ directory list access: no
    ~ create/delete files: no
  - Configuration changeable
```

3. Wählen Sie im Dropdown-Menü ▼ **Kartentyp** den Eintrag "Mifare Desfire".

4. Überlegen Sie, ob Sie eine Begehungsliste oder ein virtuelles Netzwerk für Ihre Karten brauchen.
   ↳ Wenn ja: Sie benötigen ein AV-Template (="**A**udit trail und "**V**irtual network").

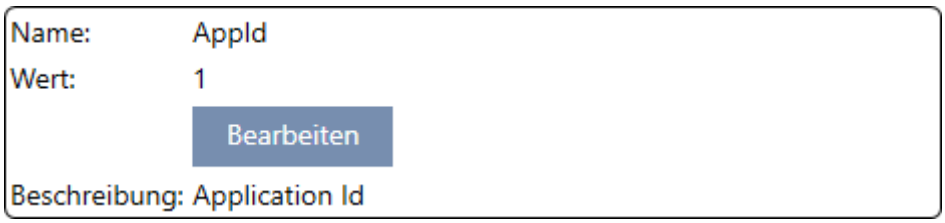
5. Bestimmen Sie die größte Kartenkonfiguration, die in den verfügbaren Speicherplatz passt (siehe *Kartentemplates [▸ 577]* - Beispiel für AV: MD4000L_AV mit 1600 Byte).
6. Wählen Sie im Dropdown-Menü ▼ **Konfiguration** die eben bestimmte Konfiguration aus (Beispiel: MD4000L_AV).



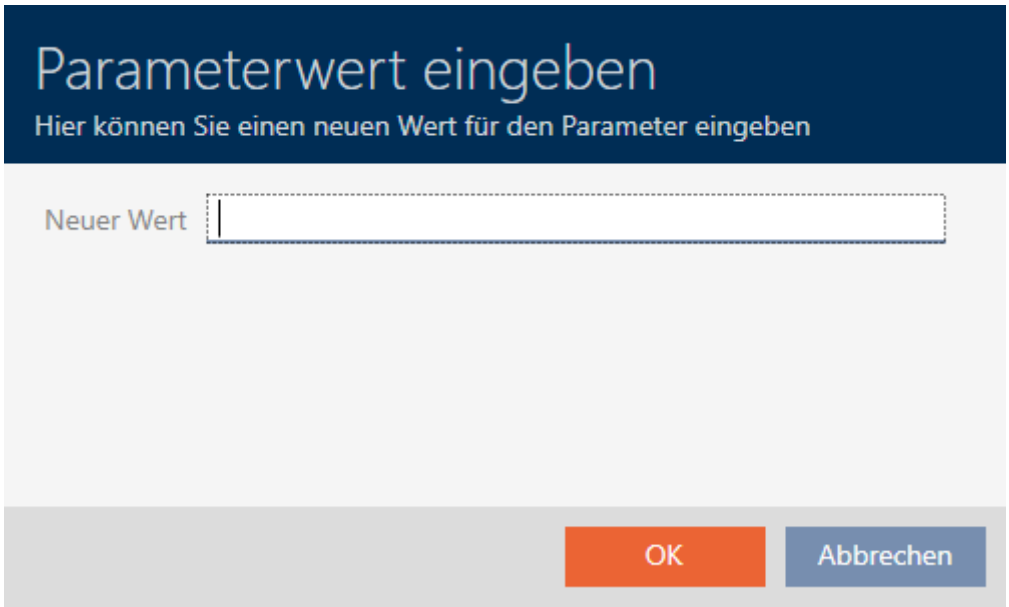
↳ *Speicherbedarf* zeigt den Speicherbedarf auf der Karte.
↳ *Schließungs-IDs* zeigt die Anzahl möglicher Schließungs-IDs für diese Karte (AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert). Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
↳ *Begehungen im Protokoll* zeigt die Anzahl möglicher Einträge in der Begehungsliste (nur für AV-Templates).

↳ Anzahl der Einträge für Schließungen in der Matrix wird auf die Anzahl der möglichen Schließungs-IDs begrenzt. Dabei können Schließungen auch mehr als einen Eintrag verbrauchen, z.B. freidrehende Digital Cylinder AX.
↳ Begehungsliste wird rollierend überschrieben, ist also nicht limitiert.
↳ Virtuelles Netzwerk ist möglich.

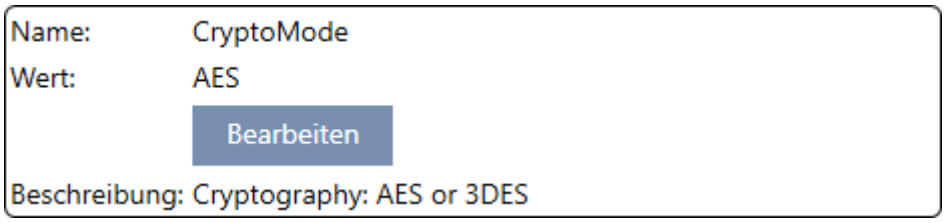
7. Klicken Sie bei den Parametern neben AppId auf die Schaltfläche Bearbeiten.



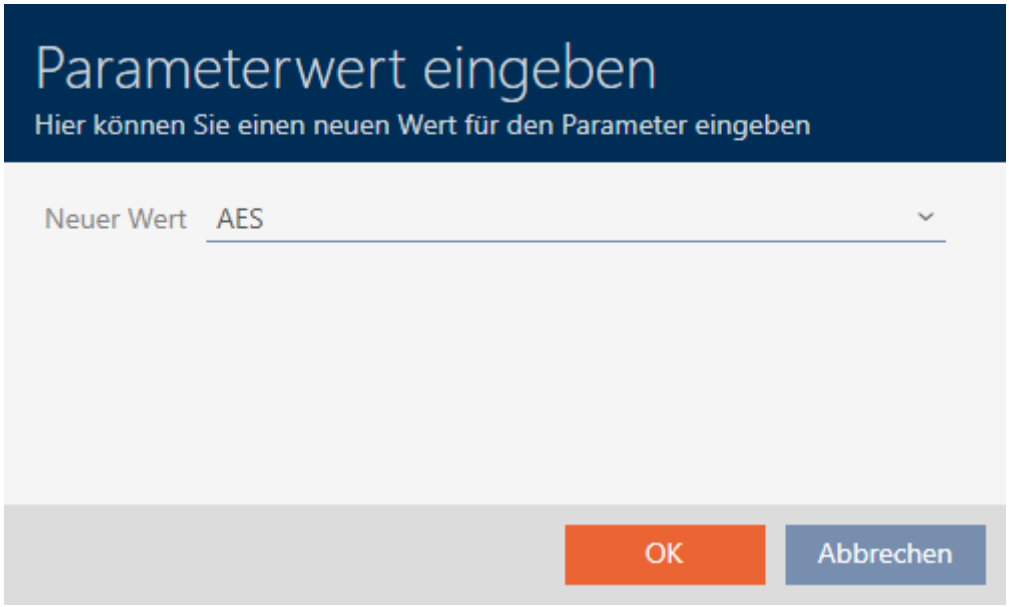
↳ Fenster "Parameterwert eingeben" öffnet sich.



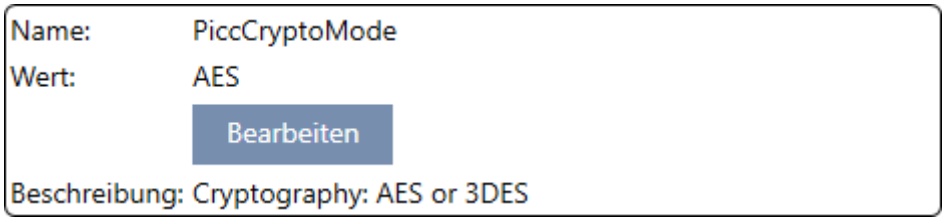
8. Geben Sie im Feld *Neuer Wert* eine App-ID ein (Dezimalsystem) oder lassen Sie den Wert auf dem Standardwert 1.
9. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "Parameterwert eingeben" schließt sich.
10. Klicken Sie bei den Parametern neben CryptoMode auf die Schaltfläche Bearbeiten.



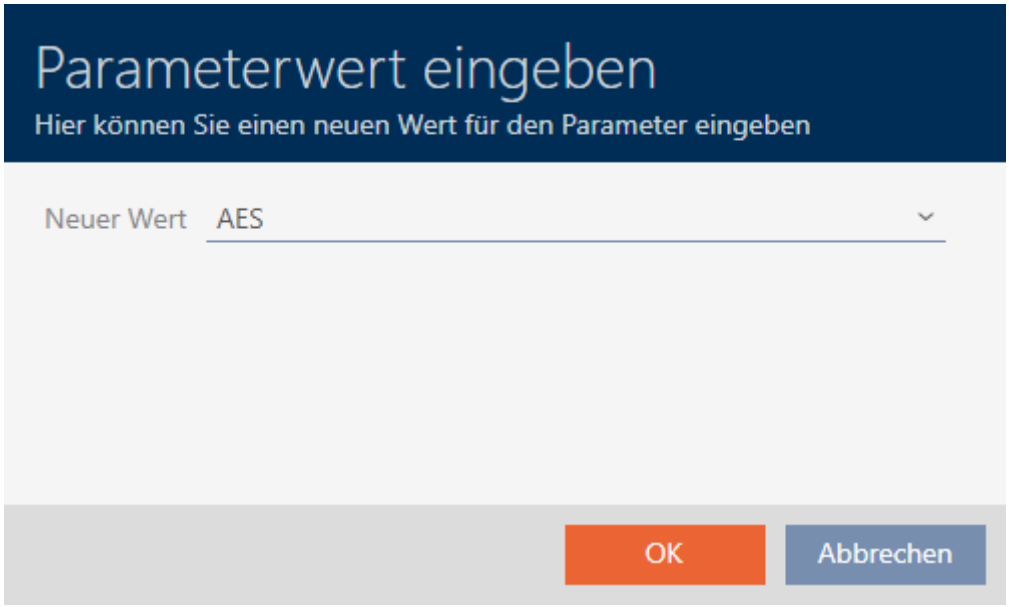
↳ Fenster "Parameterwert eingeben" öffnet sich.



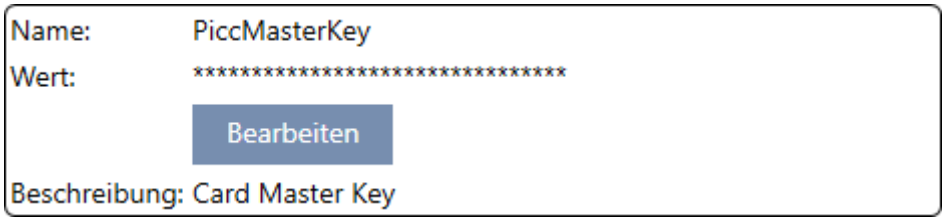
11. Wählen Sie im Dropdown-Menü ▼ **Neuer Wert** den Eintrag AES aus.
12. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
13. Klicken Sie bei den Parametern neben PiccCryptoMode auf die Schaltfläche Bearbeiten.



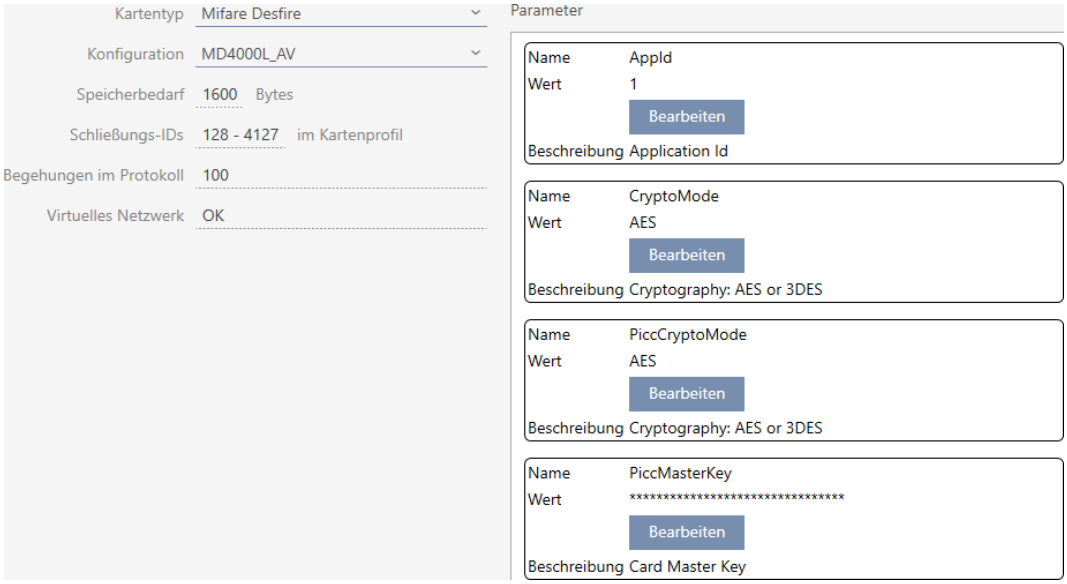
↳ Fenster "Parameterwert eingeben" öffnet sich.



14. Wählen Sie im Dropdown-Menü ▼ **Neuer Wert** den Eintrag AES aus.
15. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
16. Bearbeiten Sie den PiccMasterKey nur dann, wenn der PiccMasterKey vom Hersteller nicht auf einem Standardwert belassen wurde.



    ↳ Ihre AXM Plus ermittelt den passenden PiccMasterKey selbst. Wenn Sie einen PiccMasterKey angeben, dann wird die AXM Plus nur diesen verwenden und keinen ermitteln.



17. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Schließanlage" schließt sich.

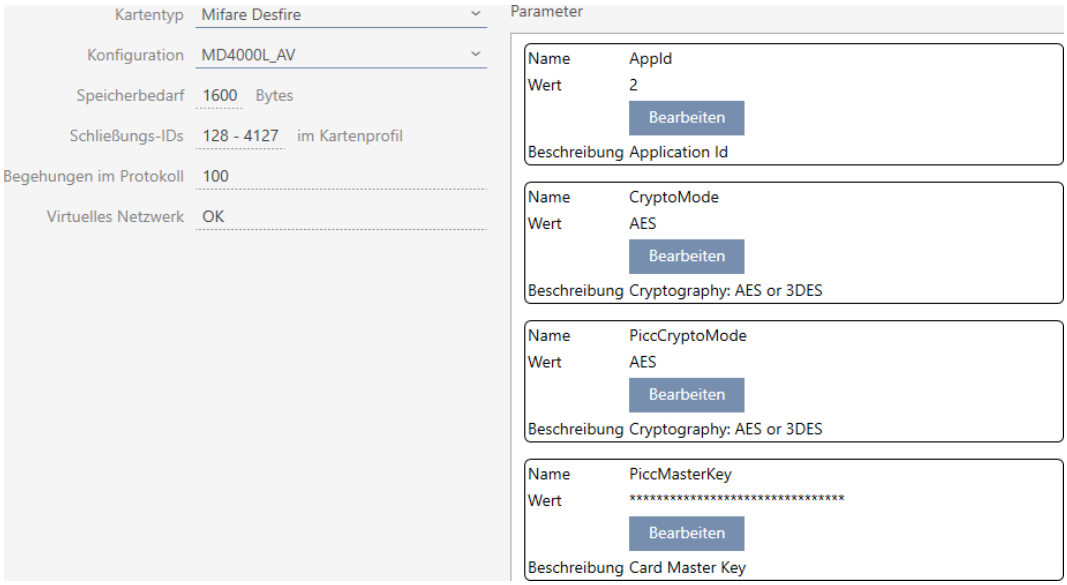
↳ Kartenkonfiguration gespeichert.

HINWEIS

PiccMasterKey schließanlagenweit gleich

Innerhalb einer Schließanlage muss für alle Karten der gleiche PiccMaster-Key verwendet werden.

18.1.1.4 MIFARE DESFire (bereits verwendete Karte)



- ▼ **Kartentyp**: MIFARE Classic oder DESFire
- ▼ **Konfiguration**: Kartentemplate (siehe *Kartentemplates [▸ 577]*)

  Das Kartentemplate bestimmt über:

  - *Speicherbedarf*: Muss an freiem Speicherplatz auf der Karte zur Verfügung stehen.
  - *Schließungs-IDs*: Zeigt die Anzahl möglicher Schließungs-IDs für diese Karte an. AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert.

    Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
  - *Begehungen im Protokoll*: Zeigt die Anzahl an Einträgen, die in die Begehungsliste dieser Karte geschrieben werden können. Nur für AV-Templates (**A**udit trail & **V**irtual network).
  - *Virtuelles Netzwerk*: Zeigt an, ob ein virtuelles Netzwerk möglich ist. Nur für AV-Templates.

Für MIFARE DESFire werden außerdem ermittelt:

- *App-ID*: App-ID, in der die Daten Ihrer Schließanlage gespeichert werden.
- *CryptoMode*: Verschlüsselungsverfahren für die Daten Ihrer Schließanlage (Verschlüsselung der Inhalte Ihrer App-ID - Empfehlung: AES)
- *PiccCryptoMode*: Generelles Verschlüsselungsverfahren (Verschlüsselung der gesamten Karte - Empfehlung: AES)

- *PiccMasterKey*: Schlüssel, der die Karte vor vollständiger Formatierung schützt.

✓ Kartentyp: MIFARE DESFire

1. Lesen Sie die Karte aus oder konsultieren Sie das Datenblatt.
   ↳ Full Report wird angezeigt.
2. Ermitteln Sie den verfügbaren Speicherplatz (Abschnitt *# Memory information*).

```
# Memory information:
Size: 2 kB
Available: 1.9 kB
```

   ↳ Auf dieser Karte steht nicht mehr der volle Speicherplatz zur Verfügung. Daraus lässt sich schließen, dass mindestens eine andere Anwendung aktiv ist und Speicherplatz beansprucht.

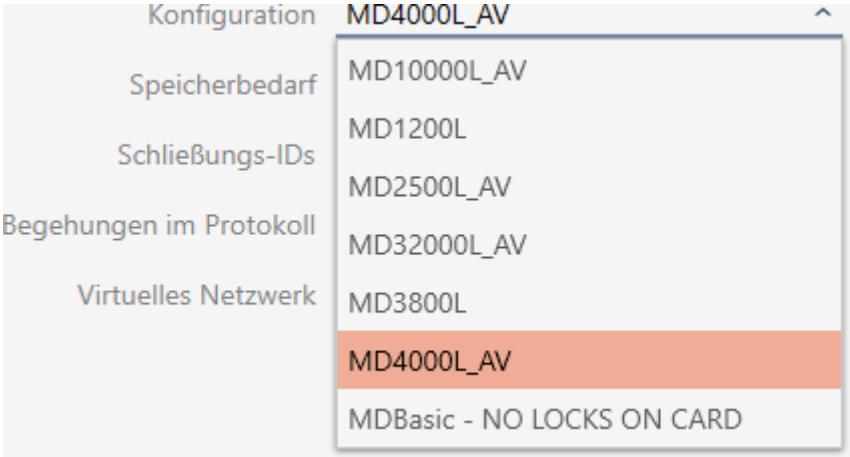
3. Ermitteln Sie aus dem Full Report die App-IDs der bereits vorhandenen Anwendungen:

```
Application ID 0x000000 (PICC)
* Key configuration:
  - 1 (3)DES key
  - Master key changeable
  - Master key required for:
    ~ directory list access: no
    ~ create/delete files: yes
  - Configuration changeable

Application ID 0x010000
* Key configuration:
  - 2 AES keys
  - Master key changeable
  - Master key required for:
    ~ directory list access: no
    ~ create/delete files: yes
  - Configuration changeable
  - Master key required for changing a key
  - Key versions:
    ~ Master key: 0
    ~ Key #1: 0

  - File ID 0x00: Standard data, 192 bytes
    ~ Communication: encrypted
    ~ Read key: key #1
    ~ Write key: key #1
    ~ Read/Write key: key #1
    ~ Change key: master key
    ~ (No access)
```

↳ Die App-ID 0 ist werkseitig belegt, die App-ID 1 ist eine Fremdanwendung mit 192 Byte Speicher.

4. Wählen Sie im Dropdown-Menü ▼ **Kartentyp** den Eintrag "Mifare Desfire".

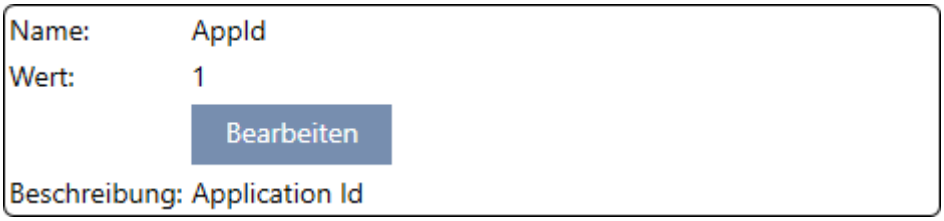
5. Überlegen Sie, ob Sie eine Begehungsliste oder ein virtuelles Netzwerk für Ihre Karten brauchen.
   ↳ Wenn ja: Sie benötigen ein AV-Template (="**A**udit trail und "**V**irtual network").
6. Bestimmen Sie die größte Kartenkonfiguration, die in den verfügbaren Speicherplatz passt (siehe *Kartentemplates [▸ 577]* - Beispiel für AV: MD4000L_AV mit 1600 Byte).
7. Wählen Sie im Dropdown-Menü ▼ **Konfiguration** die eben bestimmte Konfiguration aus (Beispiel: MD4000L_AV).



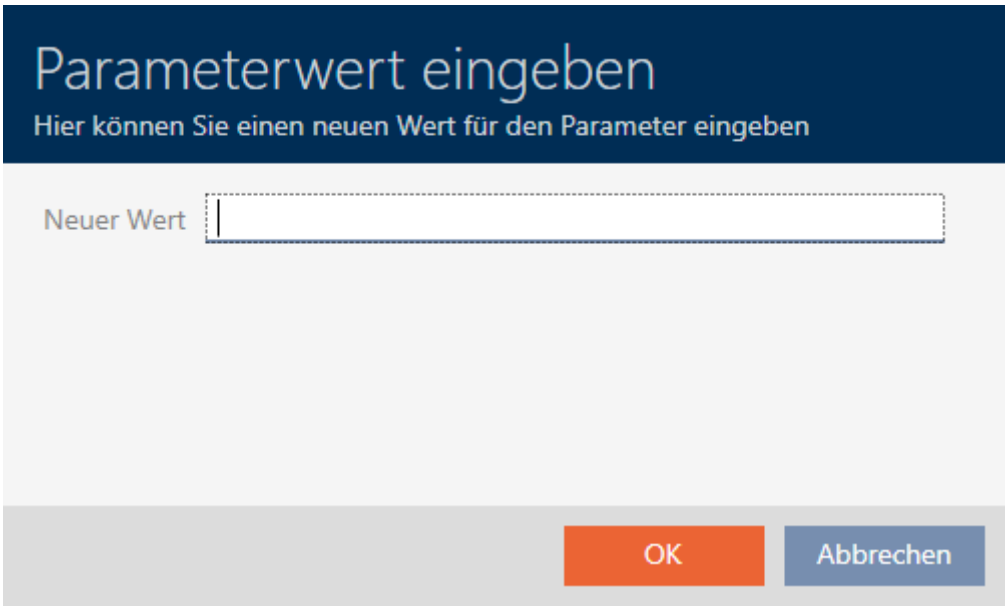
   ↳ *Speicherbedarf* zeigt den Speicherbedarf auf der Karte.
   ↳ *Schließungs-IDs* zeigt die Anzahl möglicher Schließungs-IDs für diese Karte (AXM Plus ordnet Lock-IDs automatisch zu, dabei werden LID 0-127 für interne Funktionen reserviert). Hintergrundinformationen siehe *Karten und Schließungs-IDs [▸ 573]*.
   ↳ *Begehungen im Protokoll* zeigt die Anzahl möglicher Einträge in der Begehungsliste (nur für AV-Templates).

- ↳ Anzahl der Einträge für Schließungen in der Matrix wird auf die Anzahl der möglichen Schließungs-IDs begrenzt. Dabei können Schließungen auch mehr als einen Eintrag verbrauchen, z.B. freidrehende Digital Cylinder AX.
- ↳ Begehungsliste wird rollierend überschrieben, ist also nicht limitiert.
- ↳ Virtuelles Netzwerk ist möglich.

8. Klicken Sie bei den Parametern neben AppId auf die Schaltfläche Bearbeiten.



- ↳ Fenster "Parameterwert eingeben" öffnet sich.



9. Geben Sie im Feld *Neuer Wert* eine nicht belegte App-ID als Dezimalwert ein (Im Beispiel sind 0 und 1 belegt - 2 wäre also möglich).

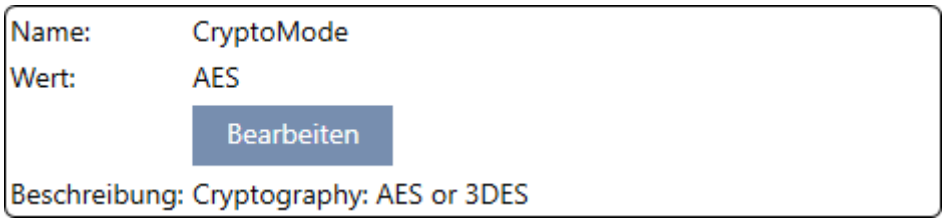
HINWEIS

Anzahl der Anwendungen bei DESFire EV1 und EV2

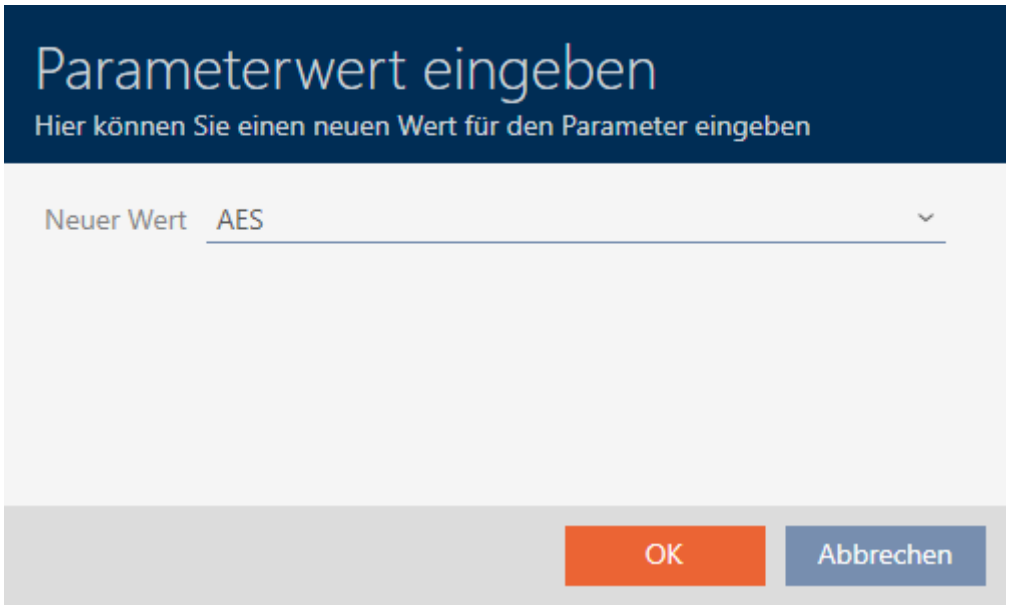
MIFARE DESFire EV1 unterstützt maximal 28 Anwendungen (0-27). Die höchste App-ID ist deshalb die App-ID 27.

MIFARE DESFire EV2 hat hier keine Einschränkung.

10. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
11. Klicken Sie bei den Parametern neben CryptoMode auf die Schaltfläche Bearbeiten.

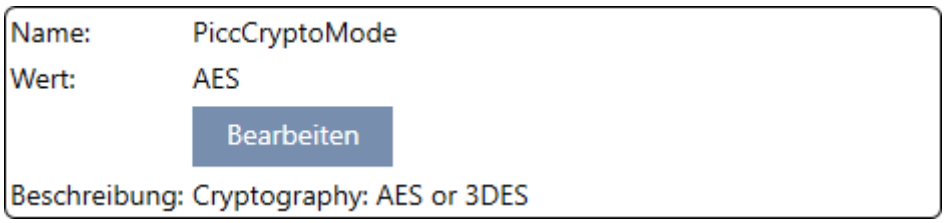


↳ Fenster "Parameterwert eingeben" öffnet sich.

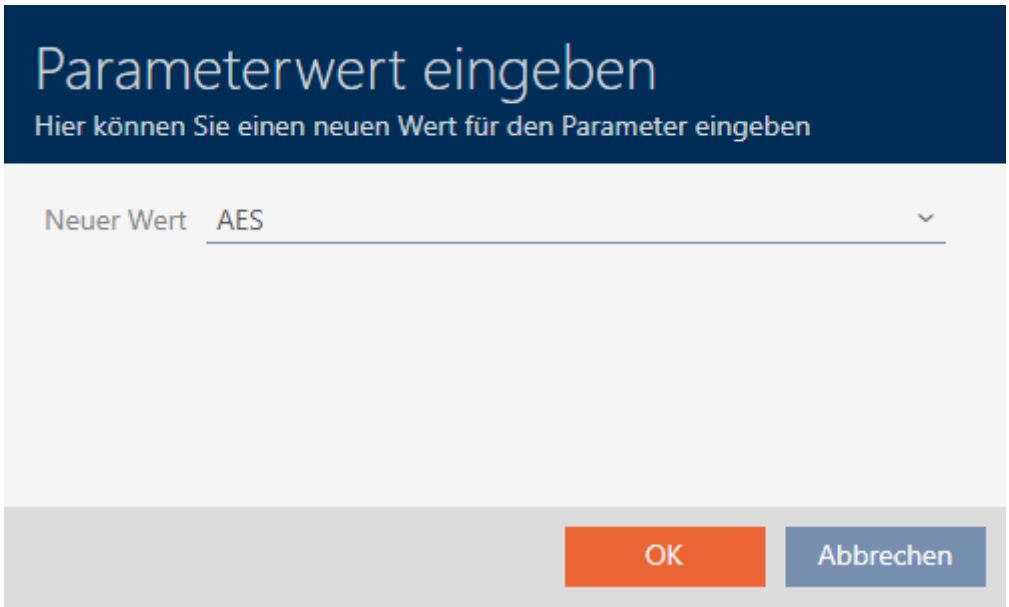


12. Wählen Sie im Dropdown-Menü ▼ **Neuer Wert** den Eintrag AES aus.
13. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.

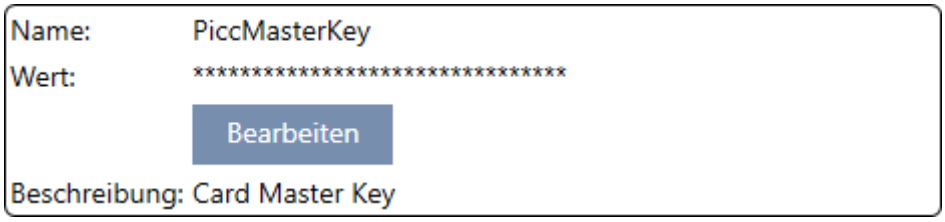
14. Klicken Sie bei den Parametern neben PiccCryptoMode auf die Schaltfläche Bearbeiten.



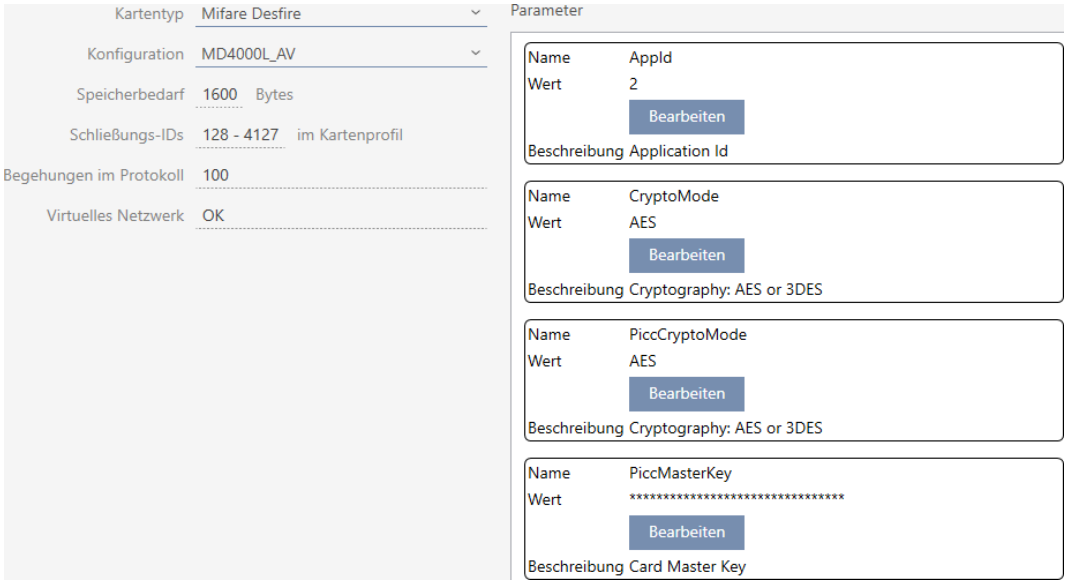
↳ Fenster "Parameterwert eingeben" öffnet sich.



15. Wählen Sie im Dropdown-Menü ▼ **Neuer Wert** den Eintrag AES aus.
16. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Parameterwert eingeben" schließt sich.
17. Bearbeiten Sie den PiccMasterKey nur dann, wenn der PiccMasterKey vom Hersteller nicht auf einem Standardwert belassen wurde.



↳ Ihre AXM Plus ermittelt den passenden PiccMasterKey selbst. Wenn Sie einen PiccMasterKey angeben, dann wird die AXM Plus nur diesen verwenden und keinen ermitteln.



18. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Schließanlage" schließt sich.

↳ Kartenkonfiguration gespeichert.

HINWEIS

PiccMasterKey schließanlagenweit gleich

Innerhalb einer Schließanlage muss für alle Karten der gleiche PiccMaster-Key verwendet werden.

Bei verwendeten DESFire-Karten können auch folgende Phänomene auftreten:

- Fremdanwendungen ändern den PiccMasterKey (Betreiber der Fremdanwendung kontaktieren)
- Kartenhersteller ändern den PiccMasterKey (Datenblatt lesen)
- Predefined-Karten: Organisationen beschreiben zentral die Karten mit "leeren" App-IDs (Zentrale Organisationsverwaltung kontaktieren).

18.2 Schließanlagenpasswort ändern

ACHTUNG

Schließanlagenpasswort zugänglich und sicher aufbewahren

Das Schließanlagenpasswort ist das wichtigste Passwort überhaupt. Aus Sicherheitsgründen kann auch SimonsVoss keine Komponenten ohne Schließanlagenpasswort oder Backup zurücksetzen. Einen Generalschlüssel gibt es nicht.

Komponenten, zu denen kein Schließanlagenpasswort mehr bekannt oder über ein Backup wiederherstellbar ist, können nicht mehr programmiert werden. Sie müssen aufwendig aus Schlössern entfernt und entsorgt werden.

1. Stellen Sie sicher, dass das Schließanlagenpasswort jederzeit durch befugte Personen einsehbar und/oder zugänglich ist.
2. Berücksichtigen Sie dabei auch sowohl vorhersehbare Ereignisse (z.B. Schließanlagenverwalter geht in Rente) und unvorhersehbare Ereignisse (z.B. Schließanlagenverwalter kündigt).

HINWEIS

Programmieraufwand nach geändertem Schließanlagenpasswort

Sämtliche Daten, die zwischen Schließungen und Identmedien ausgetauscht werden, sind verschlüsselt. Das Schließanlagenpasswort wird für diese Verschlüsselung benötigt. Das bedeutet, dass ein geändertes Schließanlagenpasswort allen Schließungen und allen Identmedien mitgeteilt werden muss.

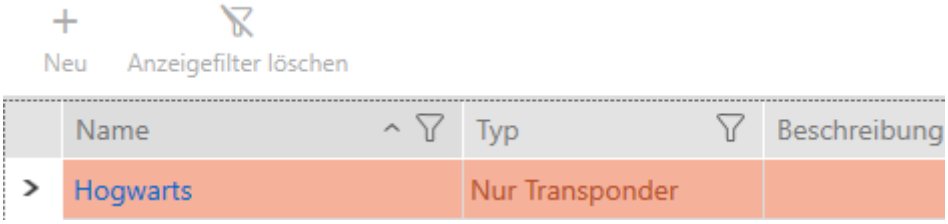
Die Änderung des Schließanlagenpasswords verursacht von allen möglichen Änderungen in Ihrer Datenbank den größten Programmierbedarf.

✓ Altes Schließanlagenpasswort ist bekannt.

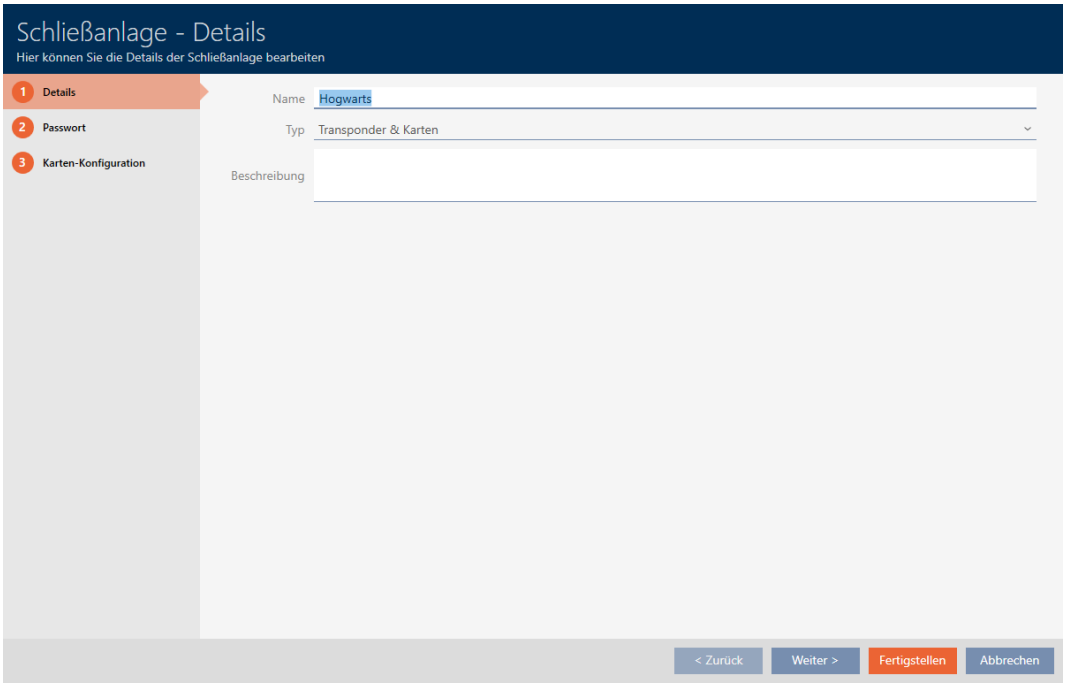
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Schließanlagen aus.

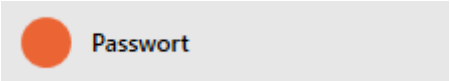
↳ Tab [Schließanlagen] mit einer Auflistung aller Schließanlagen in der Datenbank öffnet sich.



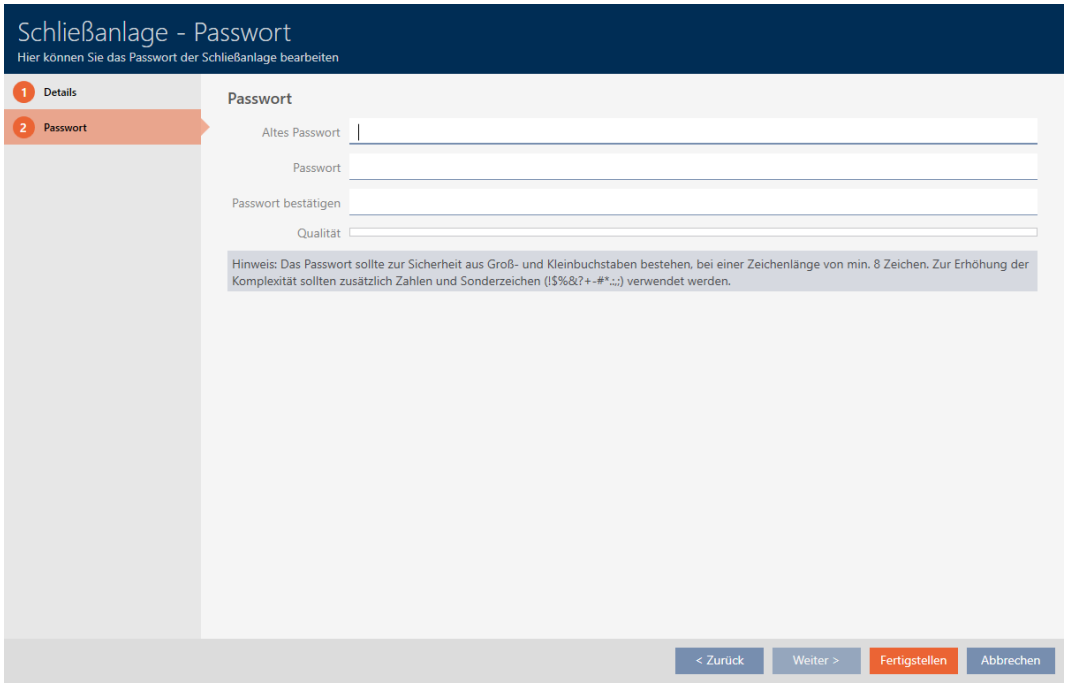
3. Klicken Sie auf die Schließanlage, deren Passwort Sie ändern wollen.
   ↳ Fenster der Schließanlage öffnet sich.



4. Klicken Sie auf den Reiter Passwort.

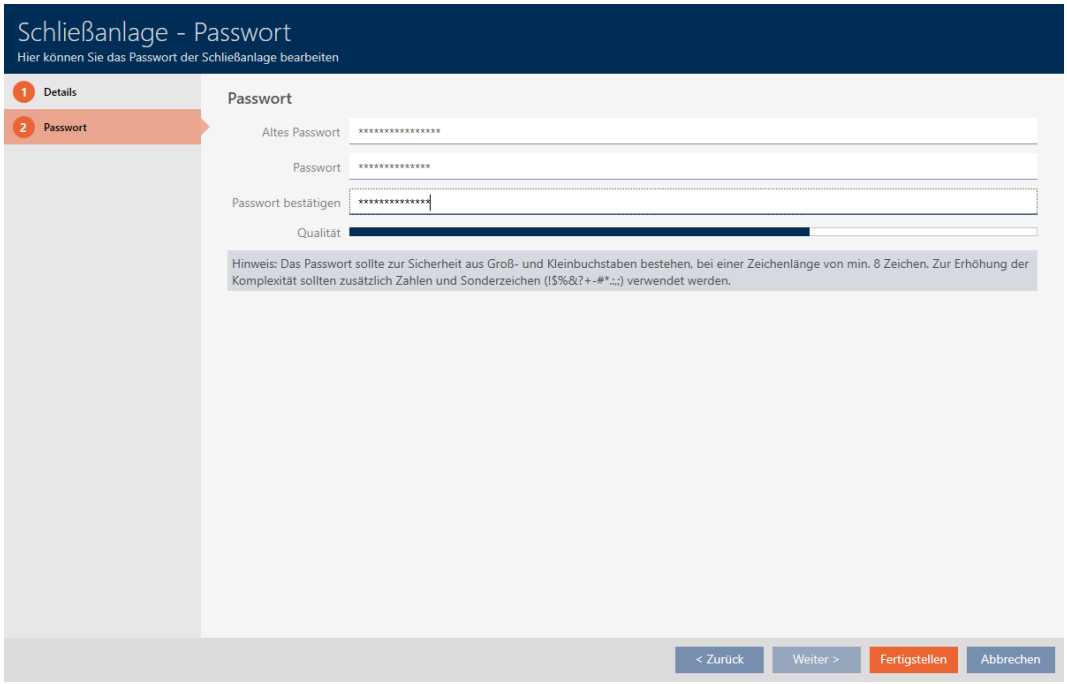


↳ Fenster wechselt zum Reiter "Passwort".

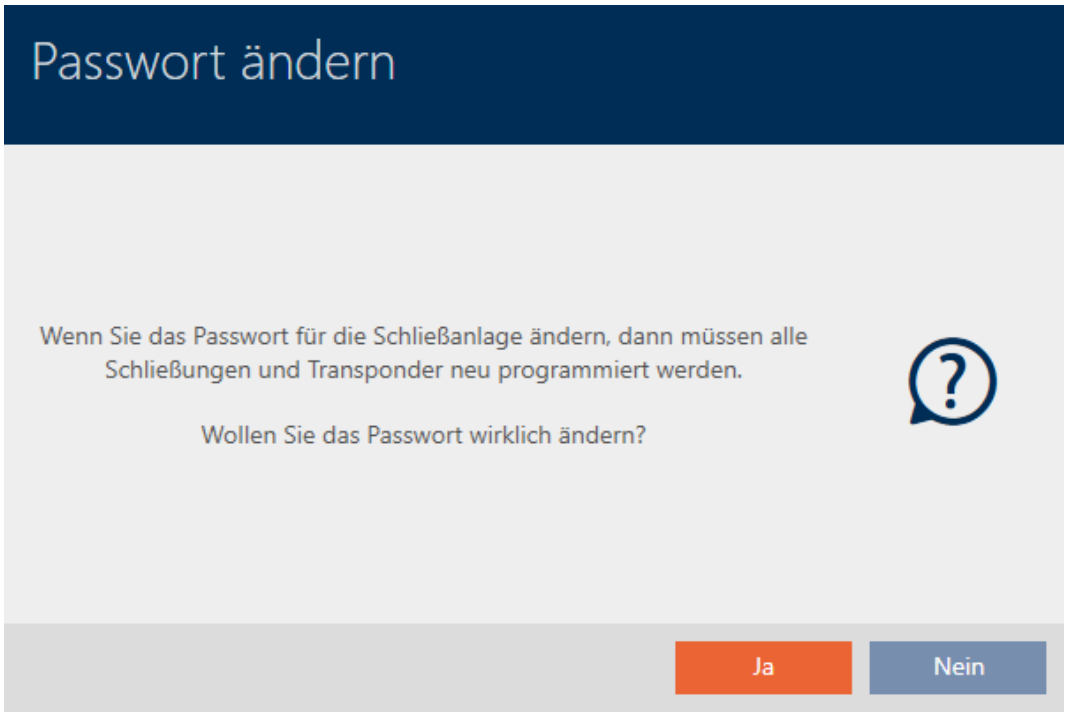


5. Geben Sie in das Feld *Altes Passwort* das alte Schließanlagenpasswort ein.
6. Geben Sie in das Feld *Passwort* ein neues Schließanlagenpasswort mit mindestens 8 Zeichen ein.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

7. Bestätigen Sie im Feld *Passwort bestätigen* das neue Schließanlagen-passwort.

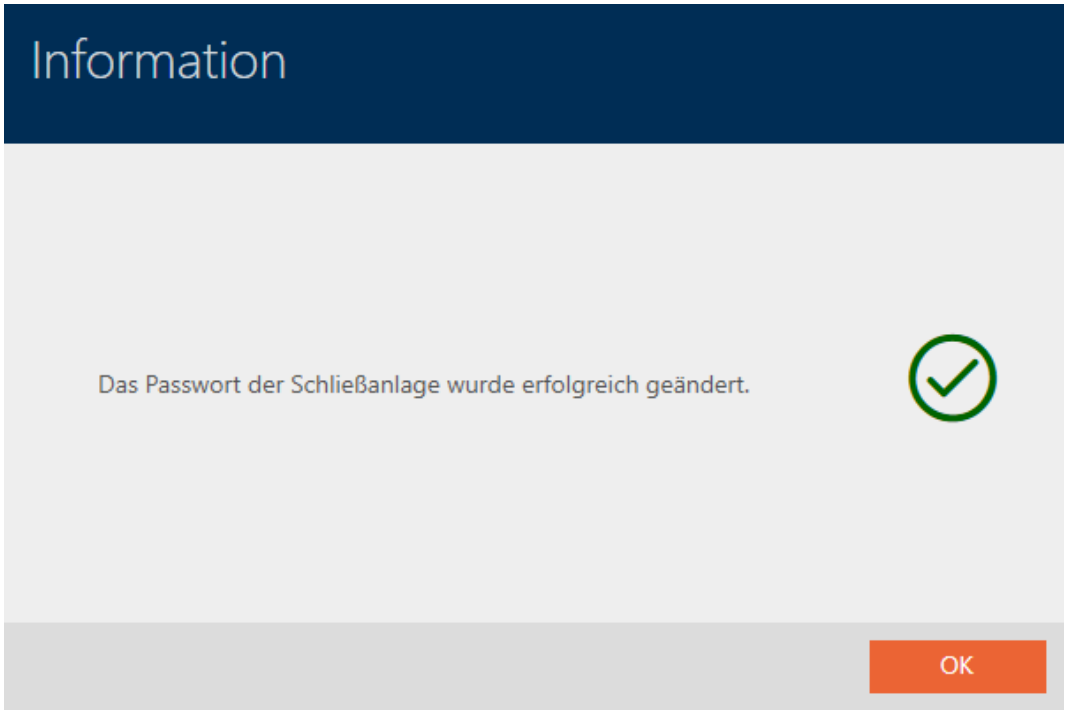


8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Warnmeldung über den zu erwartenden Programmieraufwand erscheint.



9. Klicken Sie auf die Schaltfläche Ja.
   ↳ Warnmeldung schließt sich.

↳ Schließanlagenpasswort ist geändert.



18.3 Schließanlage wechseln

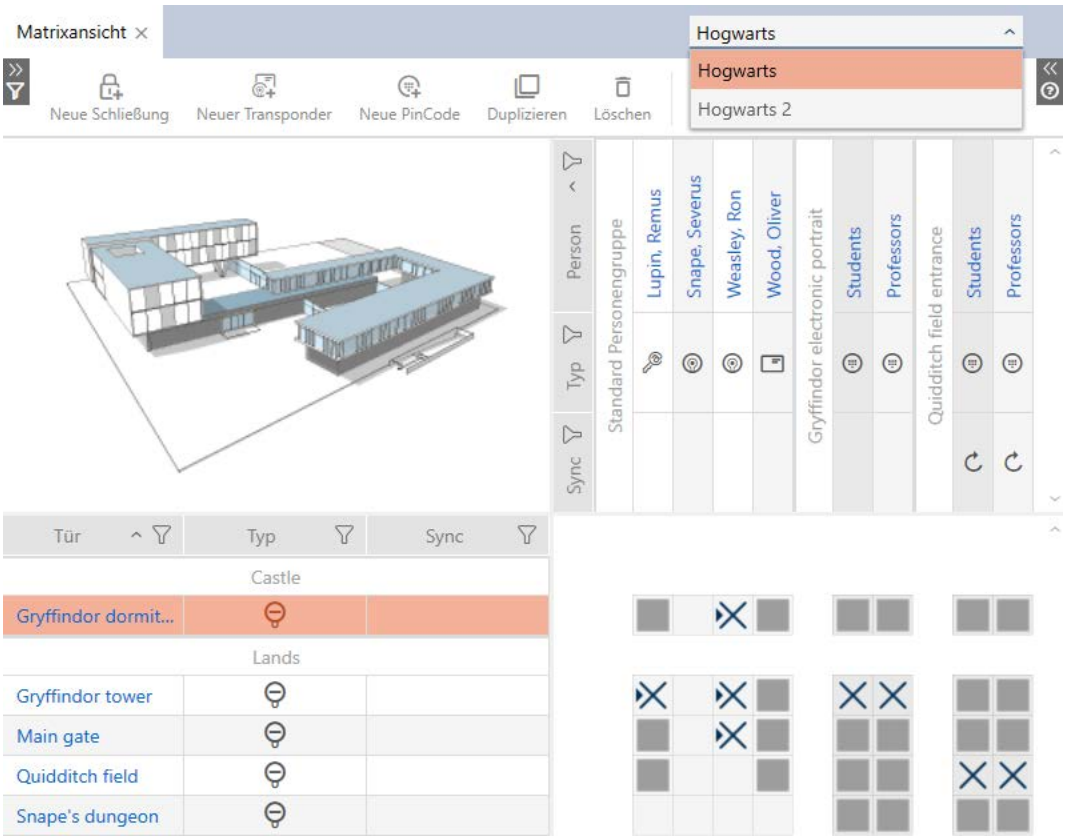
Das Arbeiten mit mehreren Schließanlagen kann Ihnen Vorteile bieten (siehe *Schließanlagen [▸ 541]*). Ihre AXM Plus präsentiert Ihnen ein aufgeräumtes Interface und zeigt Ihnen deshalb normalerweise nur die Einträge, die zu der ausgewählten Schließanlage gehören.

In manchen Tabs haben Sie aber die Möglichkeit, selbst zu entscheiden, welche Einträge Sie sehen möchten:

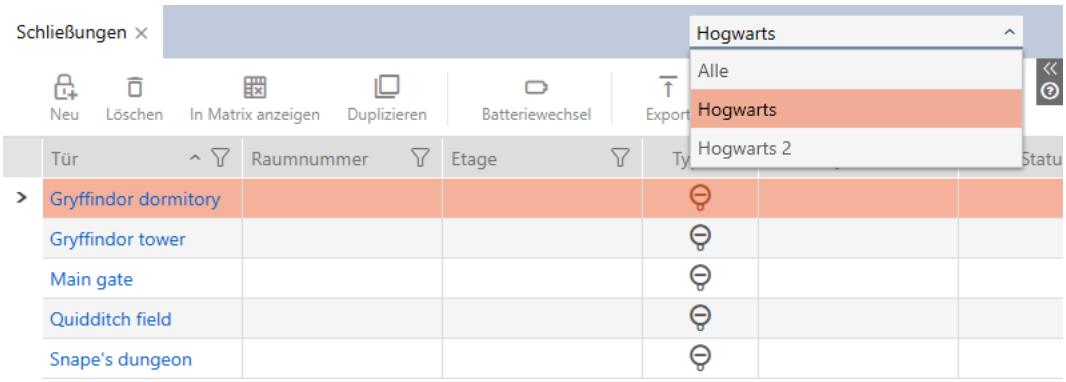
- Nur die Einträge einer bestimmten Schließanlage (z.B. alle Identmedien eines Unternehmens mit eigener Schließanlage)
- Alle Einträge aus allen Schließanlagen (z.B. alle Identmedien in einem Gebäude mit mehreren Unternehmen, die jeweils eine eigene Schließanlage haben)

Klappen Sie dazu in den entsprechenden Tabs einfach das Dropdown-Menü aus und wählen Sie eine oder alle Schließanlagen aus. Als Beispiel sehen Sie einige Tabs, in denen Sie die Schließanlage wechseln können.

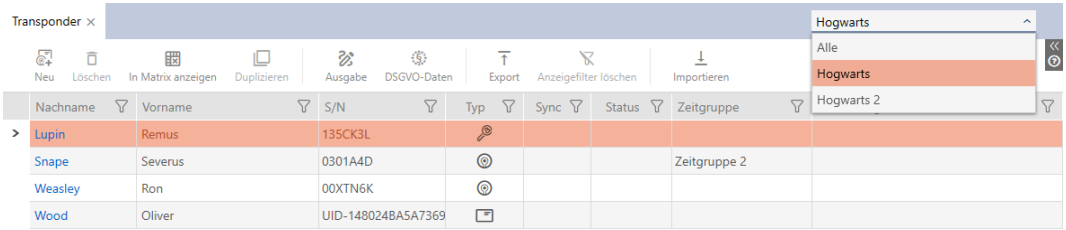
[Matrixansicht]



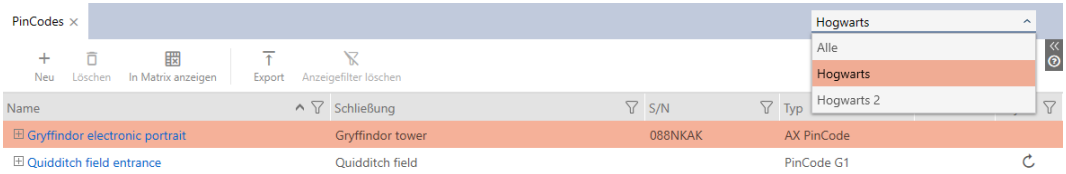
[Schließungen]



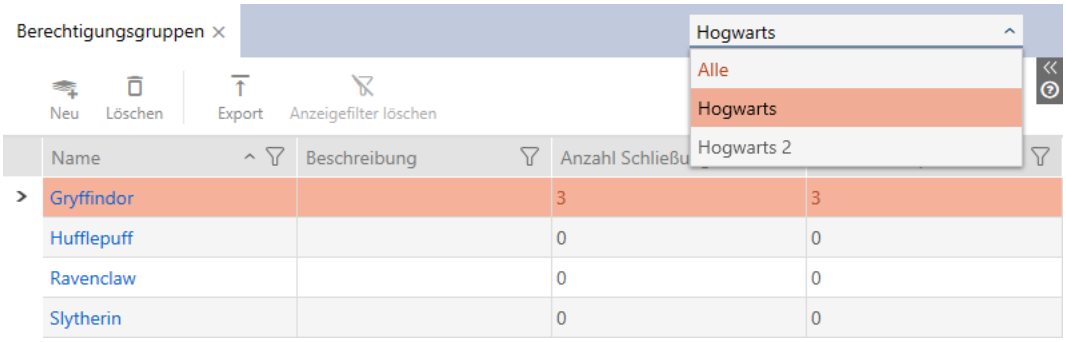
[Transponder]



[PinCodes]

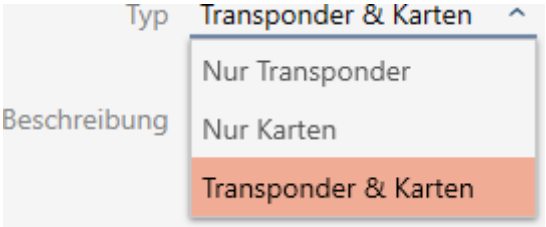


[Berechtigungsgruppen]



18.4 Karten bzw. Transponder freischalten

Als Sie Ihre Schließanlage erstellt haben, haben Sie sich im Dropdown-Menü ▼ **Typ** entschieden, welche Art von Identmedien in Ihrer Schließanlage verwendet werden sollen:



Vielleicht haben sich inzwischen die Umstände geändert und Sie möchten jetzt z.B. auch Karten in Ihrer Schließanlage verwenden. Sie stellen also Ihre Schließanlage von aktiv (= nur Transponder) auf hybrid (= Transponder + Karten) um. Mit der AXM Plus ist das kein Problem, denn hier können Sie einfach zusätzlich Karten oder Transponder freischalten.

Beachten Sie dabei, dass Sie bei der nachträglichen Freischaltung von Karten nur eine begrenzte Anzahl von Schließungen mit Karten ansprechen können (siehe *Karten und Schließungs-IDs [▸ 573]*).

Dieses Problem haben Sie bei der nachträglichen Freischaltung von Transpondern nicht.

Karten freischalten

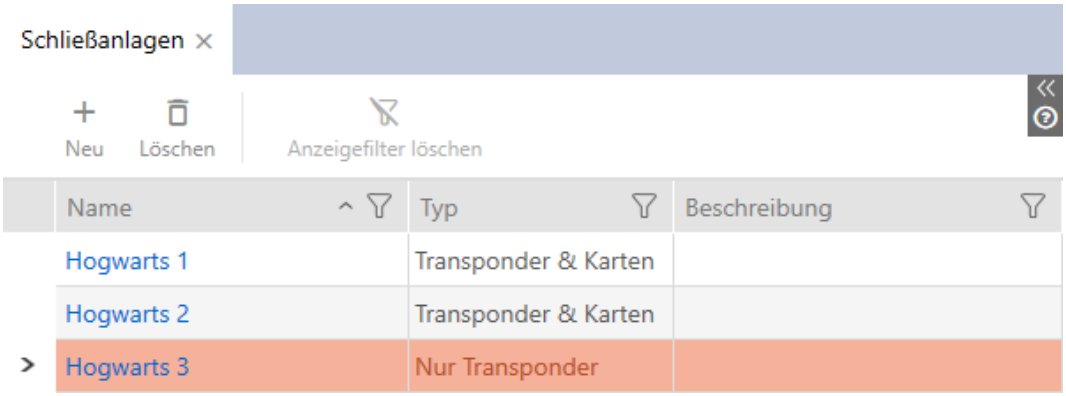
Das folgende Beispiel beschreibt, wie Sie in einer reinen Transponder-Schließanlage auch Karten verwendet werden können. Mit Karten sind dabei auch andere RFID-Identmedien gemeint, z.B. SmartTags oder RFID-Inlays. Im Beispiel wird das Template MC1000L_AV genutzt.

✓ Mindestens eine Schließanlage erstellt (siehe *Schließanlage erstellen* [▸ 360]).

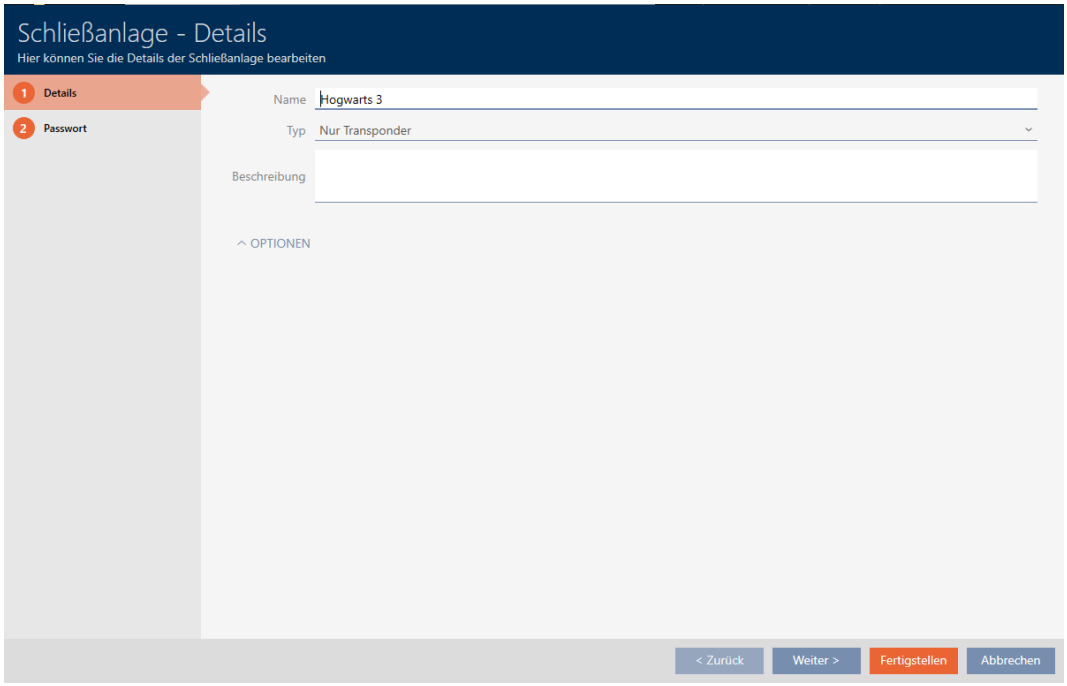
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Schließanlagen aus.

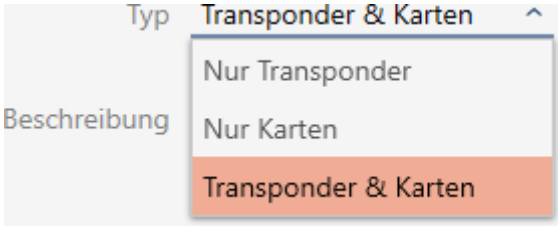
   ↳ Tab [Schließanlagen] mit einer Auflistung aller Schließanlagen in der Datenbank öffnet sich.



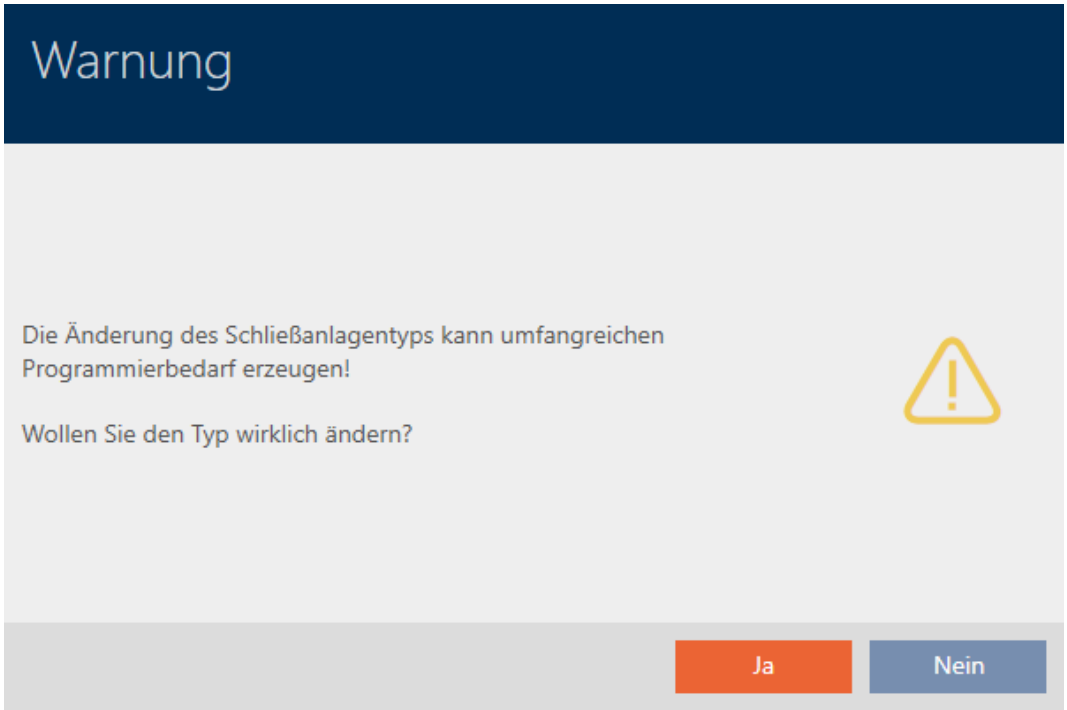
3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
4. Wählen Sie die Schließanlage aus, in der Sie Karten bzw. Transponder freischalten wollen.
   ↳ Fenster Schließanlage öffnet sich.



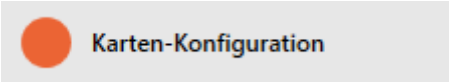
5. Wählen Sie im Dropdown-Menü ▼ **Typ** den Typ Ihrer Schließanlage aus: "Nur Transponder", "Transponder & Karten" oder "Nur Karten".



   ↳ Warnungsfenster öffnet sich.

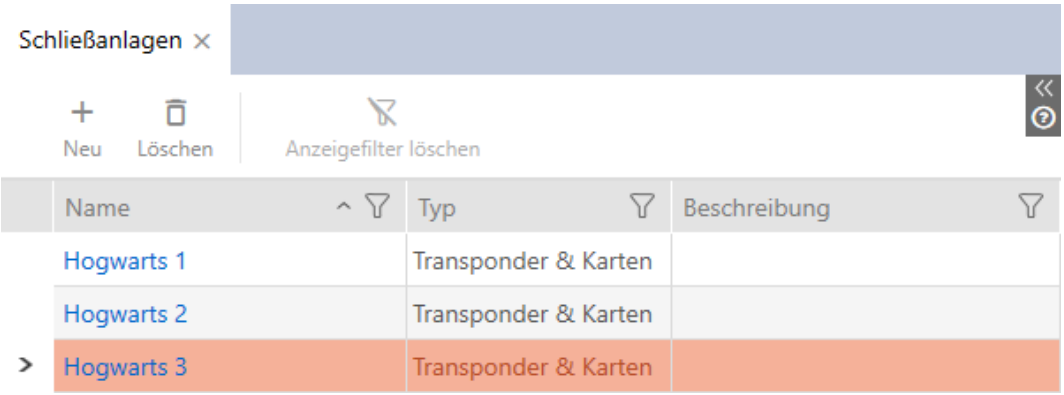


6. Klicken Sie auf die Schaltfläche Ja.
   ↳ Warnungsfenster schließt sich.
   ↳ Ggfs. erscheint der Reiter Karten-Konfiguration.



7. Wenn Sie auf den Typ "Transponder & Karten" oder "Nur Karten" umgestellt haben, dann geben Sie die Kartenkonfiguration ein (siehe *Kartenkonfiguration anlegen [▸ 365]*).
8. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Schließanlage" schließt sich.

↳ Schließanlage wird mit neuem Schließanlagentyp aufgelistet.



18.5 Übergreifende Schließebene verwenden

Mit einer übergreifenden Schließebene können Sie einen Transponder in mehreren Schließanlagen des gleichen Projekts verwenden (z.B. für Feuerwehrtransponder). Weitere Informationen zu übergreifenden Schließebenen siehe Detailfunktion der übergreifenden Schließebenen.

Die Einrichtung einer übergreifenden Schließebene besteht aus mehreren Teilen:

1. Erstellen Sie eine übergreifende Schließebene und weisen Sie dieser Schließanlagen zu (siehe *Übergreifende Schließebene erstellen [▸ 405]*).
2. Erstellen Sie in einer der zugewiesenen Schließanlagen einen Transponder (siehe *Transponder für übergreifende Schließebene erstellen [▸ 410]*).
   ↳ Transponder ist automatisch in allen Schließanlagen angelegt, die der übergreifenden Schließebene zugewiesen wurden.
3. Berechtigen Sie den Transponder jeweils in den zugewiesenen Schließanlagen (siehe *Transponder mit übergreifender Schließebene berechtigen [▸ 413]*).

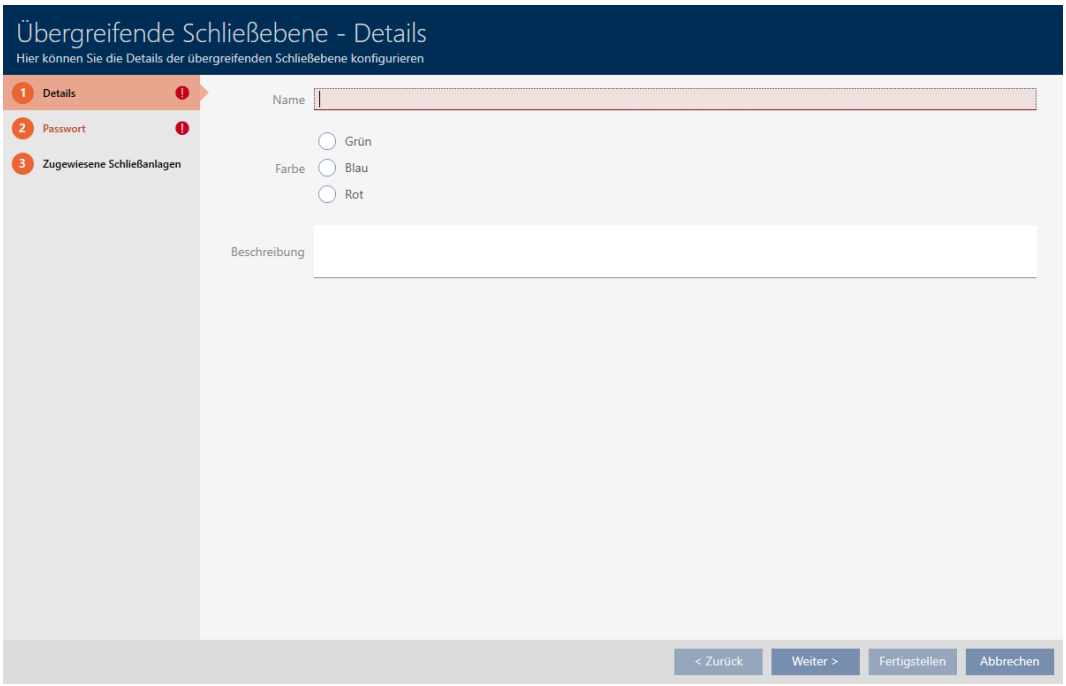
18.5.1 Übergreifende Schließebene erstellen

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Übergreifende Schließebenen aus.

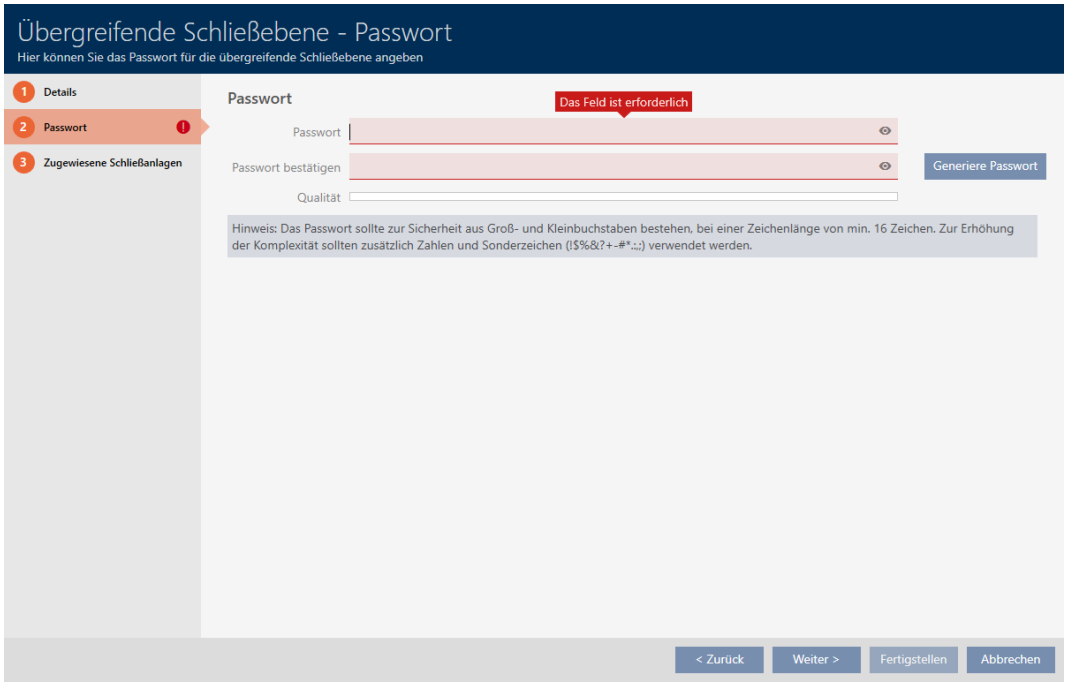
↳ Tab [Übergreifende Schließebenen] öffnet sich.

3. Klicken Sie auf die Schaltfläche Neu +.
   ↳ Fenster "Übergreifende Schließebene" öffnet sich.



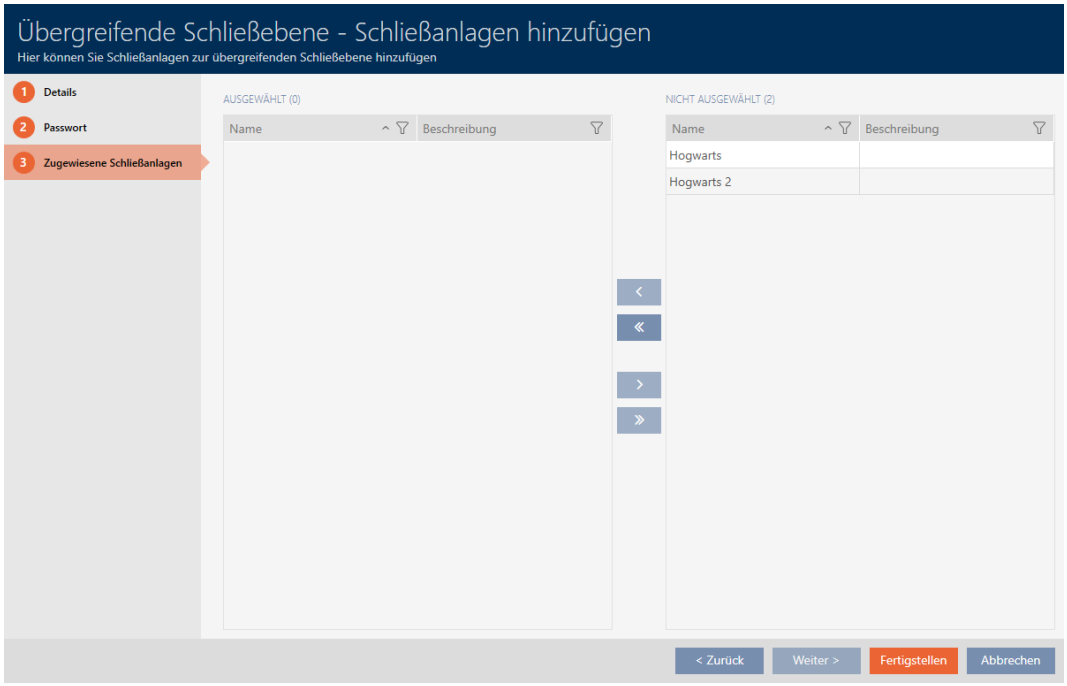
4. Geben Sie im Feld *Name* den Namen Ihrer übergreifenden Schließebene ein.
5. Wählen Sie die Farbe Ihrer übergreifenden Schließebene (Grün, Blau oder Rot).

6. Geben Sie ggfs. eine Beschreibung ein.
7. Klicken Sie auf die Schaltfläche Weiter.
   ↳ Fenster wechselt zum Reiter "Passwort".

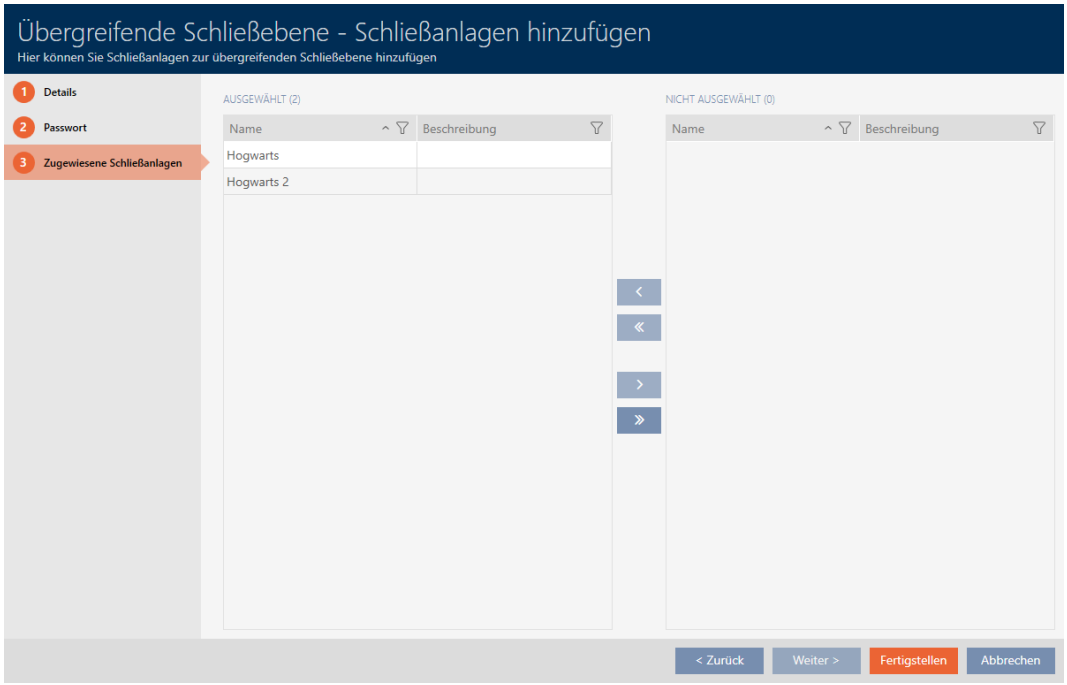


8. Geben Sie im Feld das Passwort für Ihre übergreifende Schließebene ein.
9. Wiederholen Sie das Passwort im Feld *Passwort bestätigen*.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

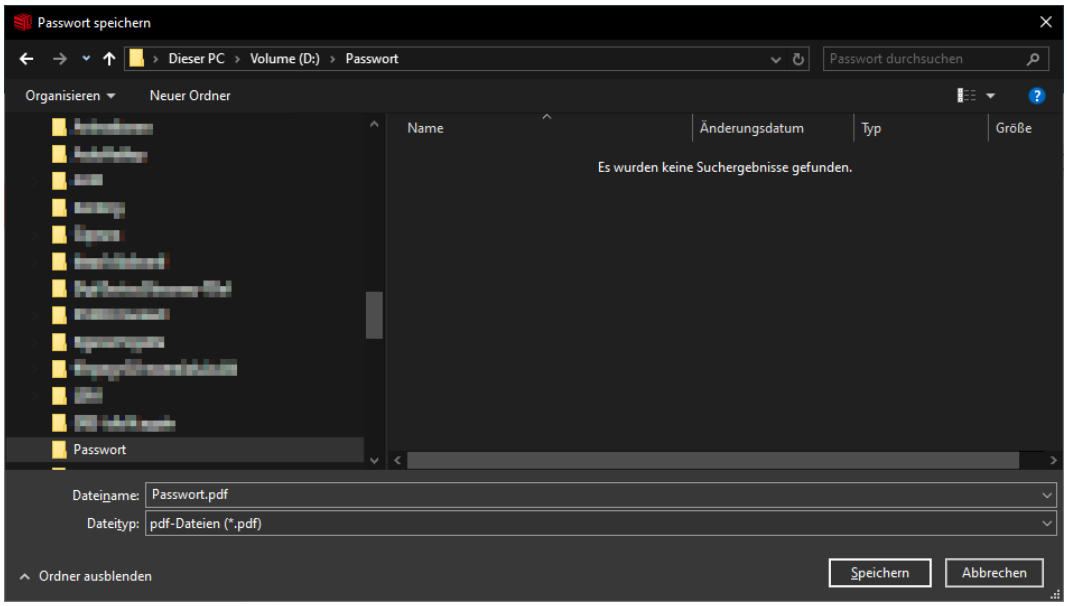
10. Klicken Sie auf die Schaltfläche Weiter.
    ↳ Fenster wechselt zum Reiter "Zugewiesene Schließanlagen".



11. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
12. Markieren Sie die gewünschten Schließanlagen in der rechten Spalte (Strg+Mausklick für einzelne oder Shift+Mausklick für mehrere).
13. Verschieben Sie mit [<] nur die ausgewählten Schließanlagen oder verschieben Sie mit [«] alle angezeigten Schließanlagen.
    ↳ In den zugewiesenen Schließanlagen wird später das Identmedium verfügbar sein.



14. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Explorer-Fenster zum Speichern des Passworts als PDF öffnet sich.



15. Speichern Sie das PDF mit dem Passwort an einem Ort Ihrer Wahl und verwahren Sie das Passwort sicher.
    ↳ Passwort ist als PDF gespeichert.

Passwort Informationen

Dies ist das Passwort für die übergreifende Schließebene: Firefighters im Projekt: Hogwarts

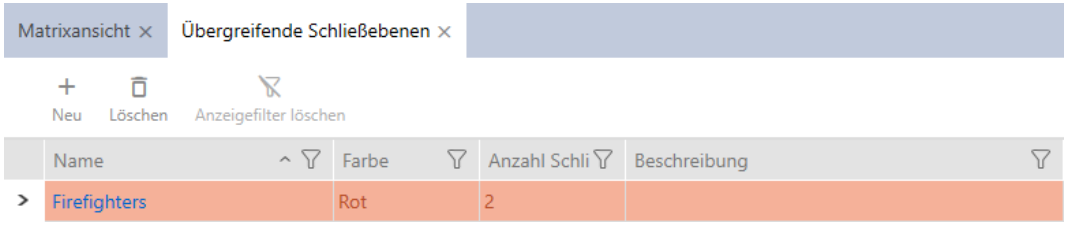
Das Passwort lautet: [redacted]

Bitte sichern Sie diese Datei oder drucken Sie sie aus.

Simons Voss technologies Ausdruck vom: 17.05.2024 1

    ↳ Fenster *Übergreifende Schließebene* schließt sich.

↳ Übergreifende Schließebene ist erstellt und wird im Tab [Übergreifende Schließebenen] aufgelistet.



Sie können jetzt mithilfe dieser übergreifenden Schließebene Transponder erstellen, die in allen zugewiesenen Schließanlagen erscheinen werden (siehe *Transponder für übergreifende Schließebene erstellen [▸ 410]*).

18.5.2 Transponder für übergreifende Schließebene erstellen

HINWEIS

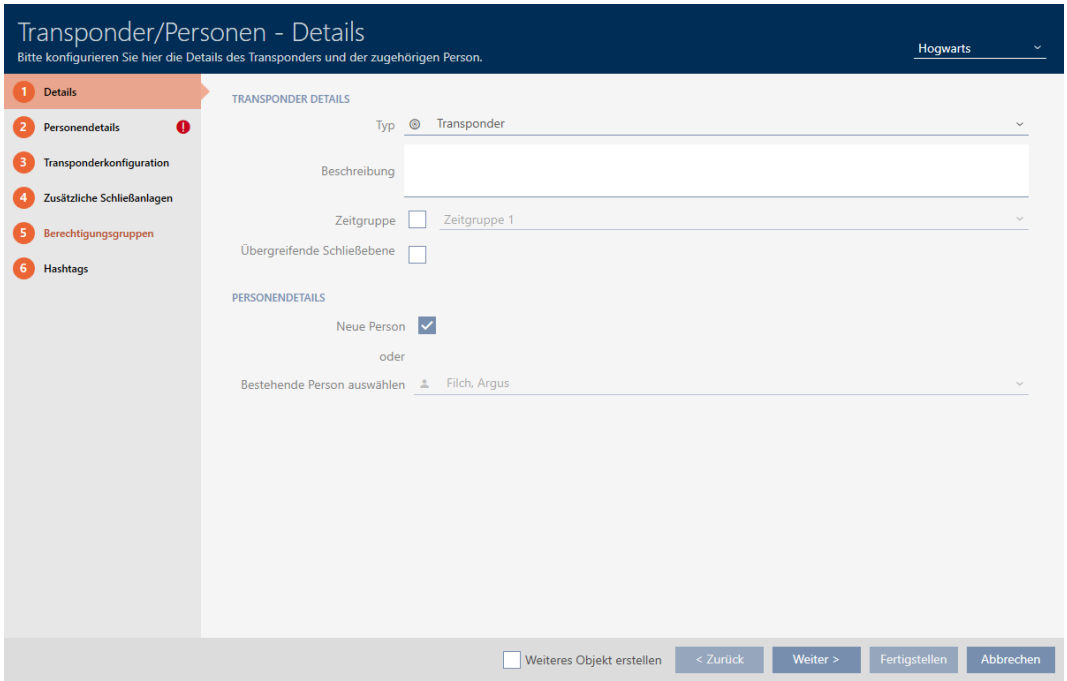
Transponder bzw. Karten für Schließanlage freischalten

Ihnen stehen nur die Identmedien-Typen zur Verfügung, die in Ihrer Schließanlage freigeschalten sind.

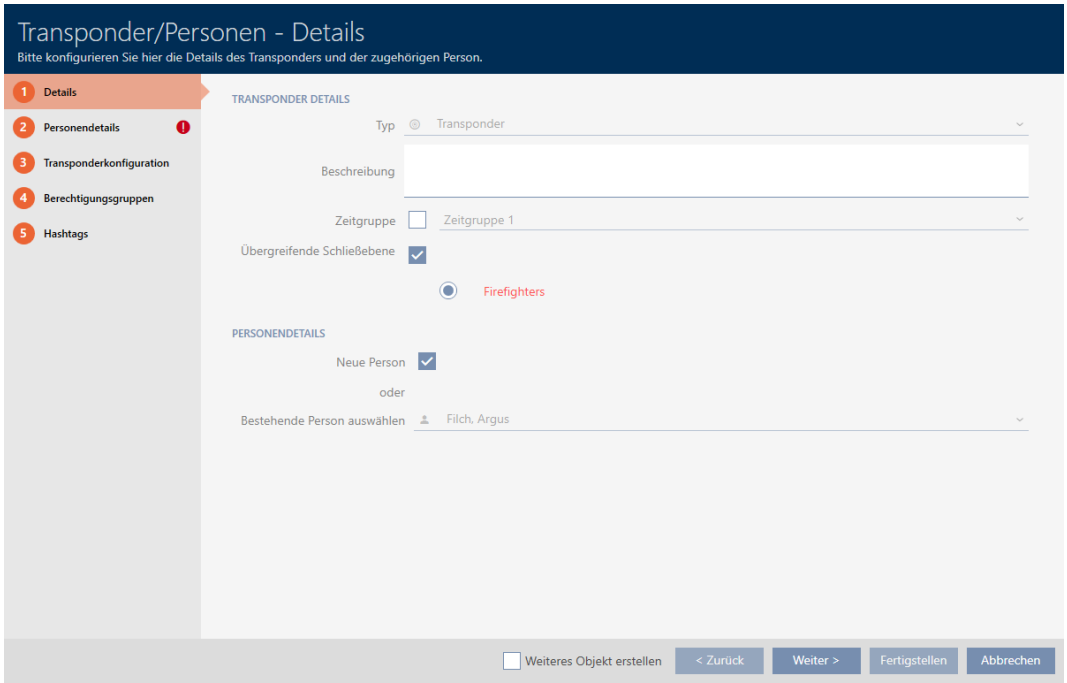
- Schalten Sie ggfs. Karten bzw. Transponder in den Eigenschaften der Schließanlage frei (siehe *Karten bzw. Transponder freischalten [▸ 401]*).

✓ Liste mit Transpondern oder Matrixansicht geöffnet.
✓ Übergreifende Schließebene erstellt und Schließanlage zugewiesen (siehe *Übergreifende Schließebene erstellen [▸ 405]*).

1. Wechseln Sie in eine Schließanlage, die Sie der übergreifenden Schließebene zugewiesen haben.
2. Klicken Sie auf die Schaltfläche Neuer Transponder.
   ↳ Fenster zum Erstellen eines Identmediums öffnet sich.



3. Aktivieren Sie die Checkbox ☑ Übergreifende Schließebene.
   ↳ Optionen zur Auswahl der übergreifenden Schließebene werden eingeblendet.
   ↳ Reiter Zusätzliche Schließanlagen verschwindet.

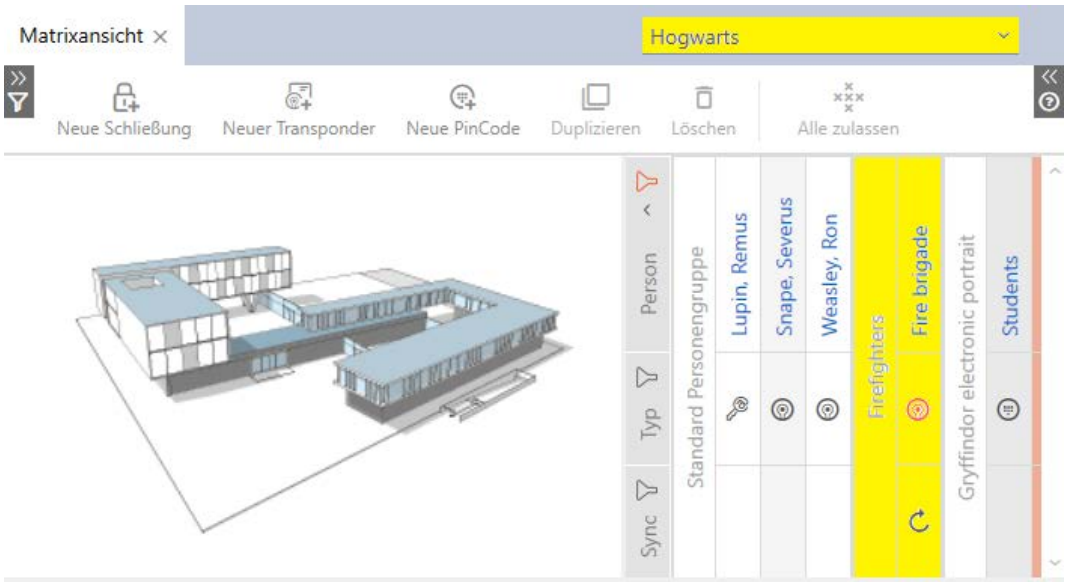


4. Füllen Sie die verbleibenden Optionen wie bei einem normalen Transponder aus (siehe *Transponder und Karten erstellen [▸ 95]*).
5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster zum Erstellen eines neuen Identmediums schließt sich.

↳ Der Transponder wird in allen zugewiesenen Schließanlagen erstellt.

↳ Da er zu einer übergreifenden Schließebene gehört, wird er in der Farbe der Schließebene dargestellt (im Beispiel rot).

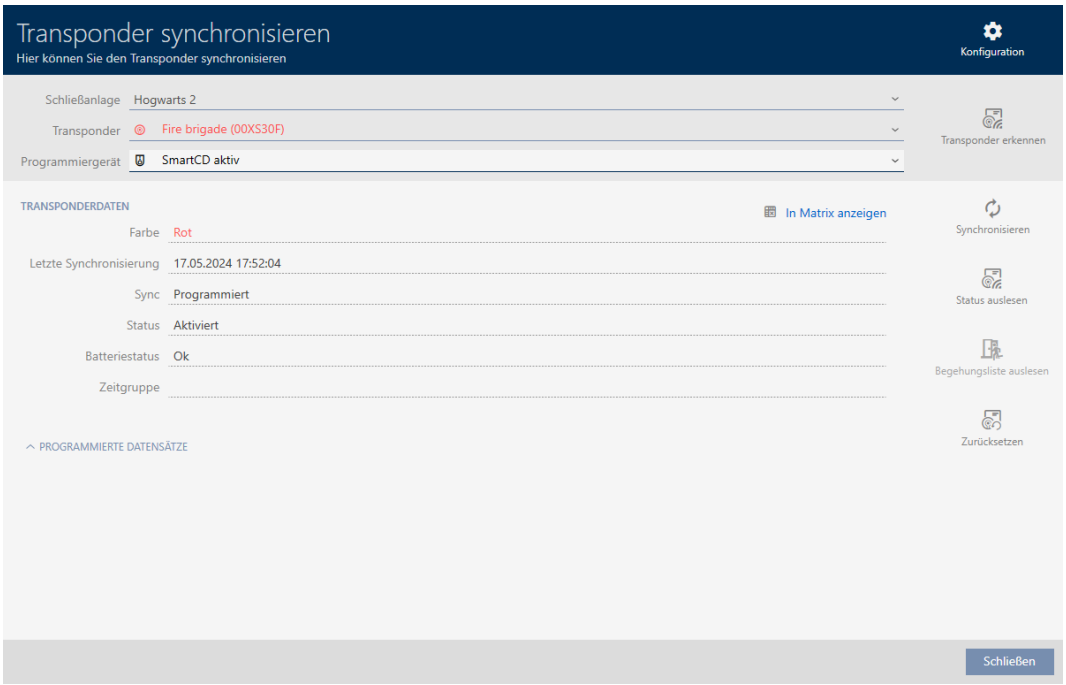
Transponder in der ersten Schließanlage:



Transponder in der zweiten Schließanlage:

Den in mehreren Schließanlagen erstellten Transponder können Sie jetzt an den verschiedenen Schließungen in den Schließanlagen berechtigen (siehe *Transponder mit übergreifender Schließebene berechtigen [▸ 413]*).

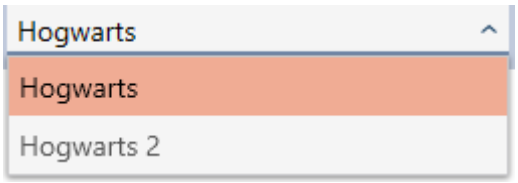
Nach der erfolgreichen Synchronisation werden die Felder *Transponder* und *Farbe* in der Farbe der übergreifenden Schließebene angezeigt (Beispiel: Rot).



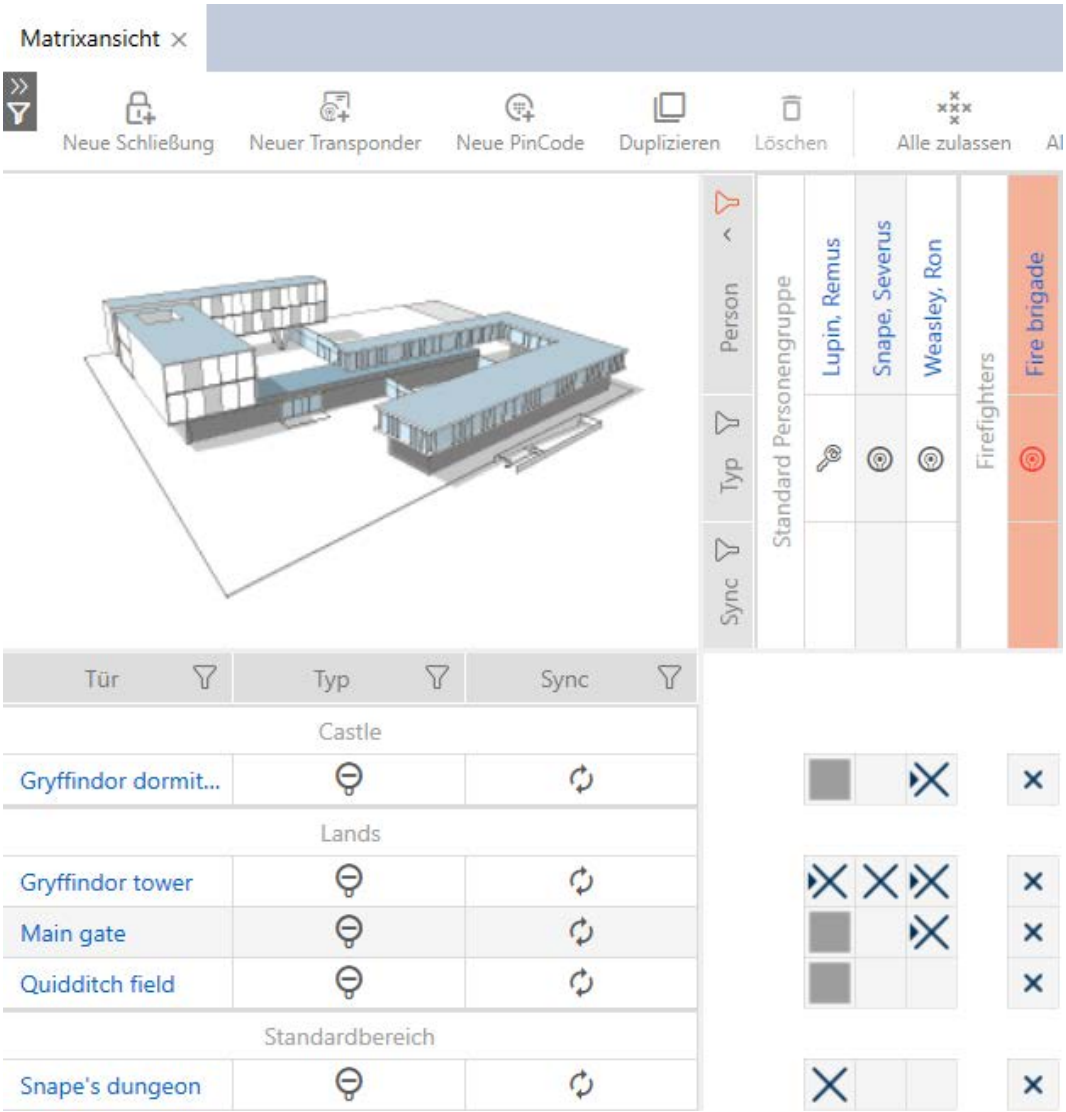
18.5.3 Transponder mit übergreifender Schließebene berechtigen

- ✓ Matrixansicht geöffnet.
- ✓ Übergreifende Schließebene erstellt (siehe *Übergreifende Schließebene erstellen [▸ 405]*).
- ✓ Transponder in übergreifender Schließebene erstellt (siehe *Transponder für übergreifende Schließebene erstellen [▸ 410]*).

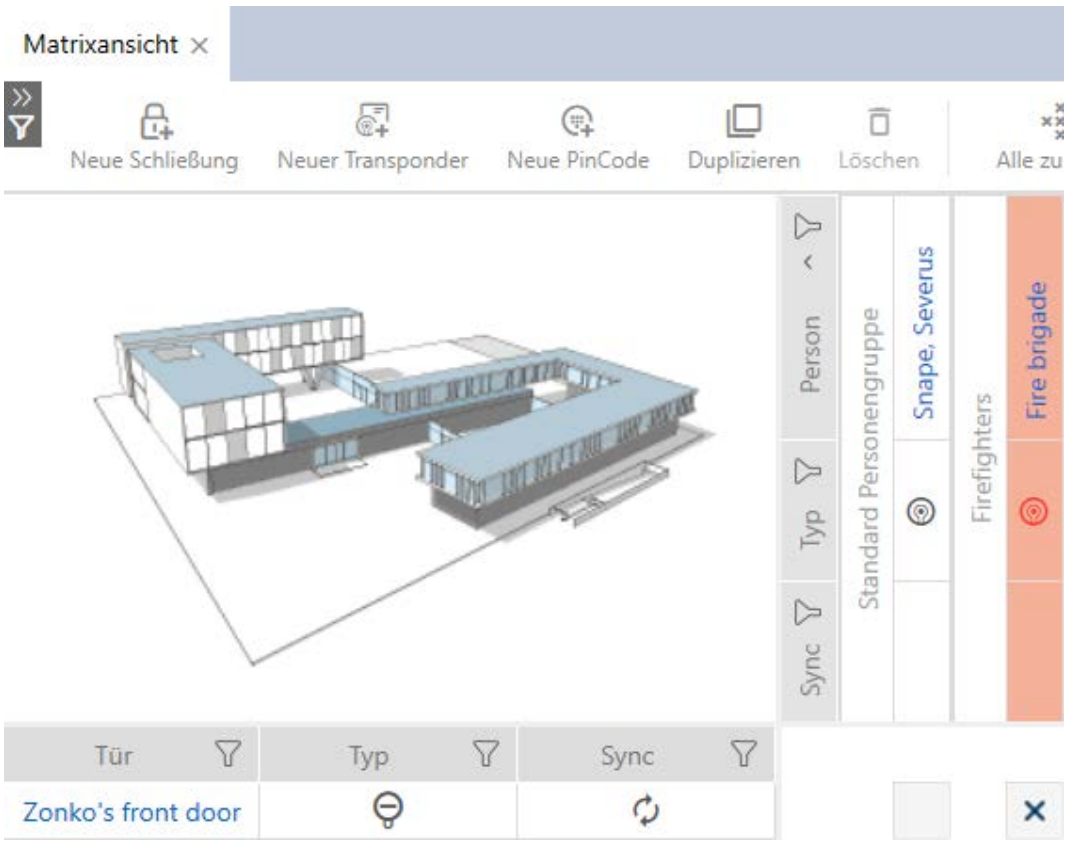
1. Wechseln Sie im Dropdown-Menü zur Schließanlage aus der übergreifenden Schließebene.



2. Vergeben Sie alle gewünschten Berechtigungen in dieser Schließanlage.



3. Wechseln Sie im Dropdown-Menü zur nächsten Schließanlage, die Sie der übergreifenden Schließebene zugewiesen haben.
4. Vergeben Sie auch dort alle gewünschten Berechtigungen.

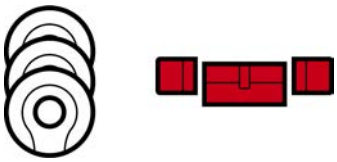
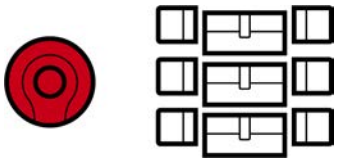


5. Synchronisieren Sie die Schließungen und Transponder wie gewohnt (siehe *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]* und *Identmedium synchronisieren [▸ 427]*).

↳ Dank der übergreifenden Schließebene kann derselbe Transponder Schließungen aus verschiedenen Schließanlagen betätigen.

19. Synchronisierung: Abgleich zwischen Schließplan und Realität

Seit der Einführung des G2-Protokolls ist es Ihnen überlassen, ob Sie zum Beispiel bei einer neuen Berechtigung die Schließung oder das Identmedium synchronisieren.

Schließung synchronisieren	Identmedium synchronisieren
Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]	*Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*
Sinnvoll, wenn viele Identmedien an einer Schließung berechtigt wurden. In dem Fall muss statt vielen Identmedien nur eine Schließung synchronisiert werden. 	Sinnvoll, wenn ein Identmedium an vielen Schließungen berechtigt wurde. In dem Fall muss statt vielen Schließungen nur ein Identmedium synchronisiert werden. 

Auch andere Faktoren spielen eine Rolle bei dieser Entscheidung, z.B.:

- Verfügbare Programmiergeräte
- Schließung oder Identmedium vor Ort
- Zutrittsliste oder Begehungsliste auslesen

Synchronisierung aus der Matrix heraus

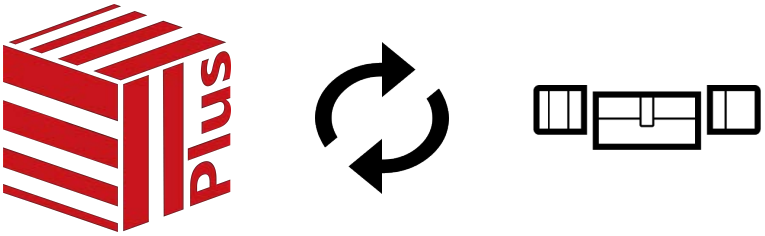
In der Matrix können Sie sich den Synchronisierungsbedarf anzeigen lassen. Wenn Sie direkt auf das Symbol ⟲ klicken, dann starten Sie sofort die Synchronisierung des jeweiligen Eintrags.

Erstsynchronisierung oder reguläre Synchronisierung

Eine Erstsynchronisierung (Symbol: ↻) unterscheidet sich von anderen Synchronisierungen (Symbol: ⟲) durch die größere Datenmenge. Verwenden Sie daher bei AX-Schließungen insbesondere bei Erstsynchronisierungen vorzugsweise einen SmartStick AX oder ein SmartCD.MP.

SmartStick AX	SmartCD.MP

19.1 Schließung synchronisieren (inkl. Zutrittsliste auslesen)



Die Synchronisierung ist bidirektional:

- Auslesen von Daten, die in der Schließung gespeichert sind (z.B. Batteriezustand)
- Schreiben von neuen Daten in die Schließung (z.B. Berechtigungen)

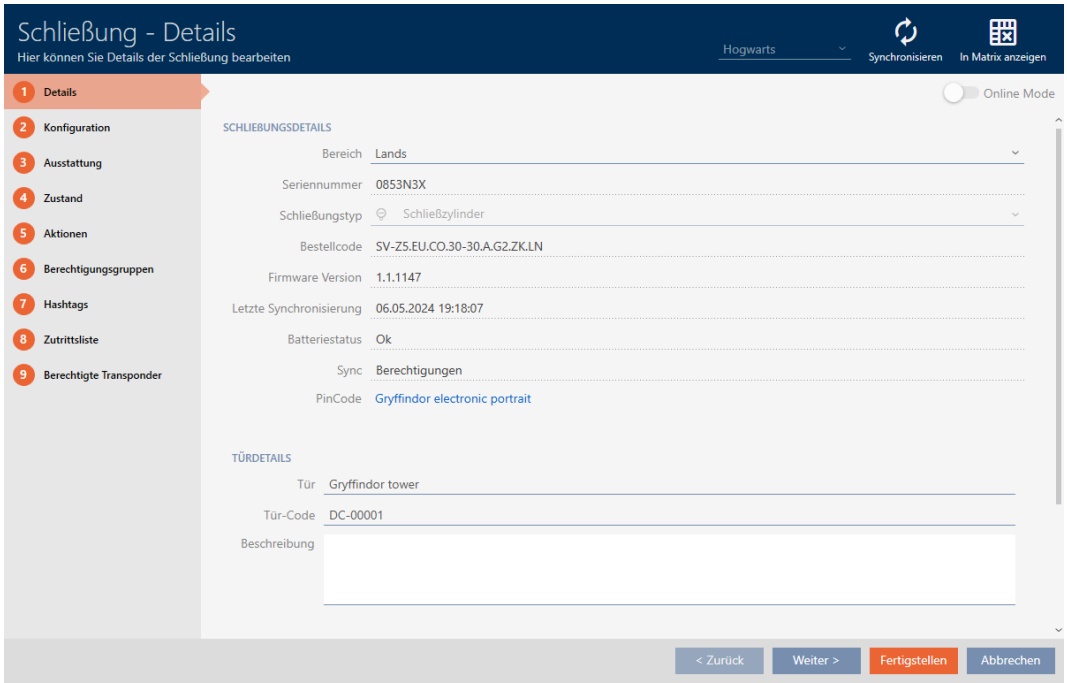
Zutrittslisten können separat ausgelesen werden (Schaltfläche Zutrittsliste auslesen). Optional können Zutrittslisten aber auch einfach während der Synchronisierung mit ausgelesen werden (siehe *Zutrittsliste/ Begehungsliste während der Synchronisierung auslesen [▸ 459]*).

Ausgelesene Daten können anschließend angezeigt werden (siehe z.B. *Schließungsausstattung und -zustand anzeigen [▸ 419]* oder *Zutrittsliste einer Schließung anzeigen und exportieren [▸ 421]*).

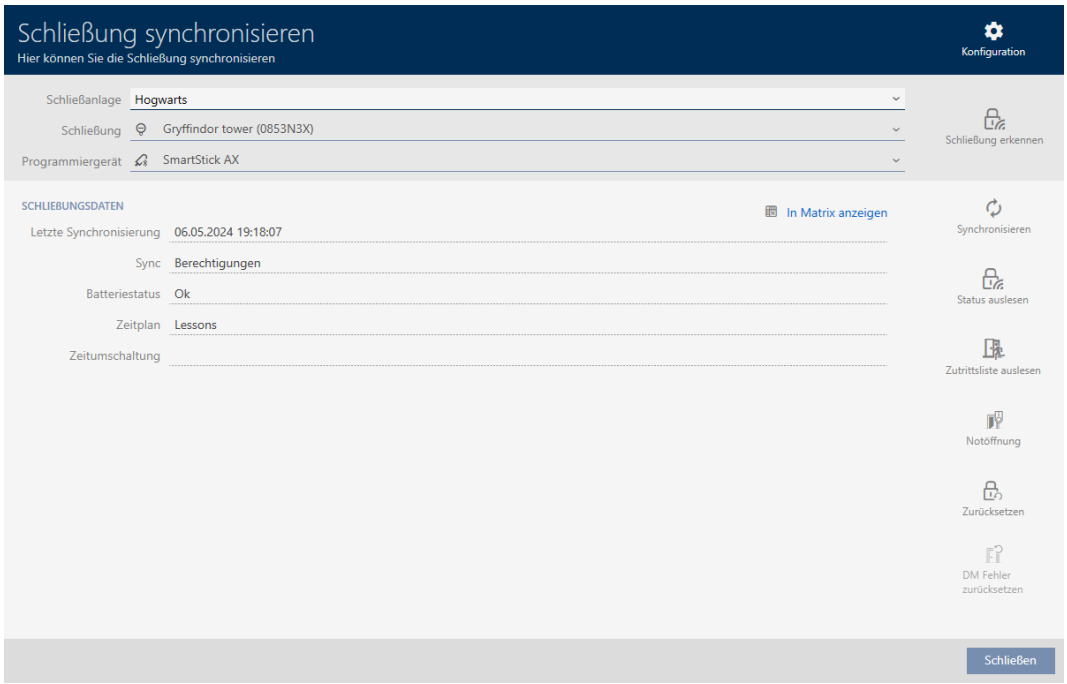
✓ Schließungsliste oder Matrixansicht geöffnet.

✓ Geeignetes Programmiergerät angeschlossen.

1. Klicken Sie auf die Schließung, die Sie synchronisieren wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Synchronisieren-Fenster öffnet sich.



3. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie synchronisieren wollen.

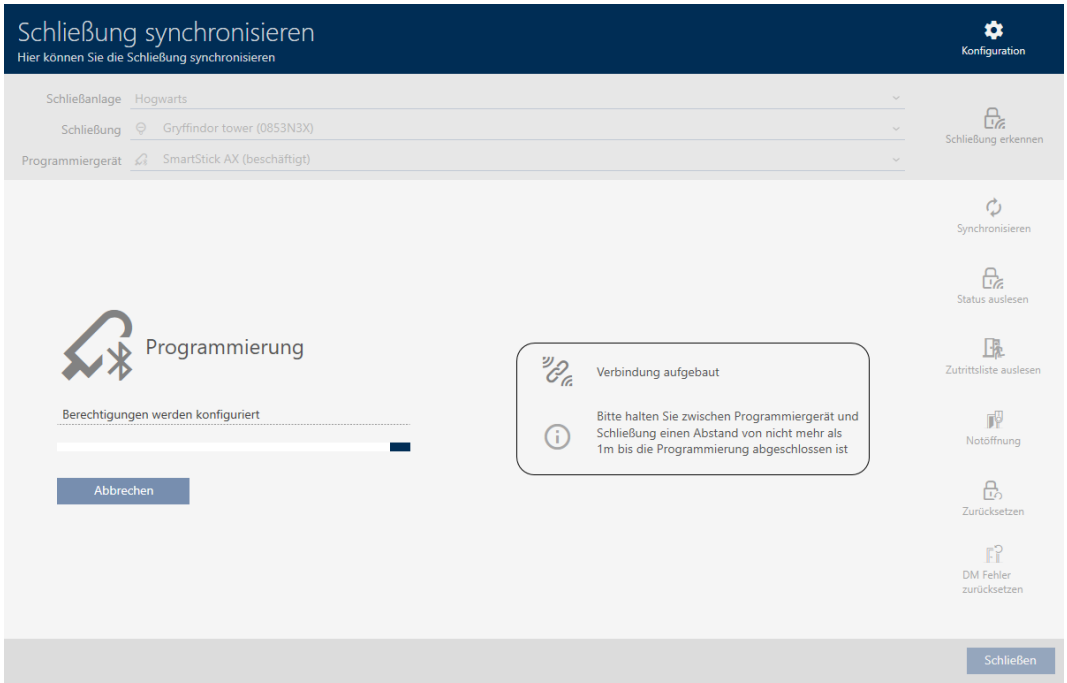
HINWEIS

AX-Komponenten: SmartCD.MP oder SmartStick AX für erste Synchronisierung

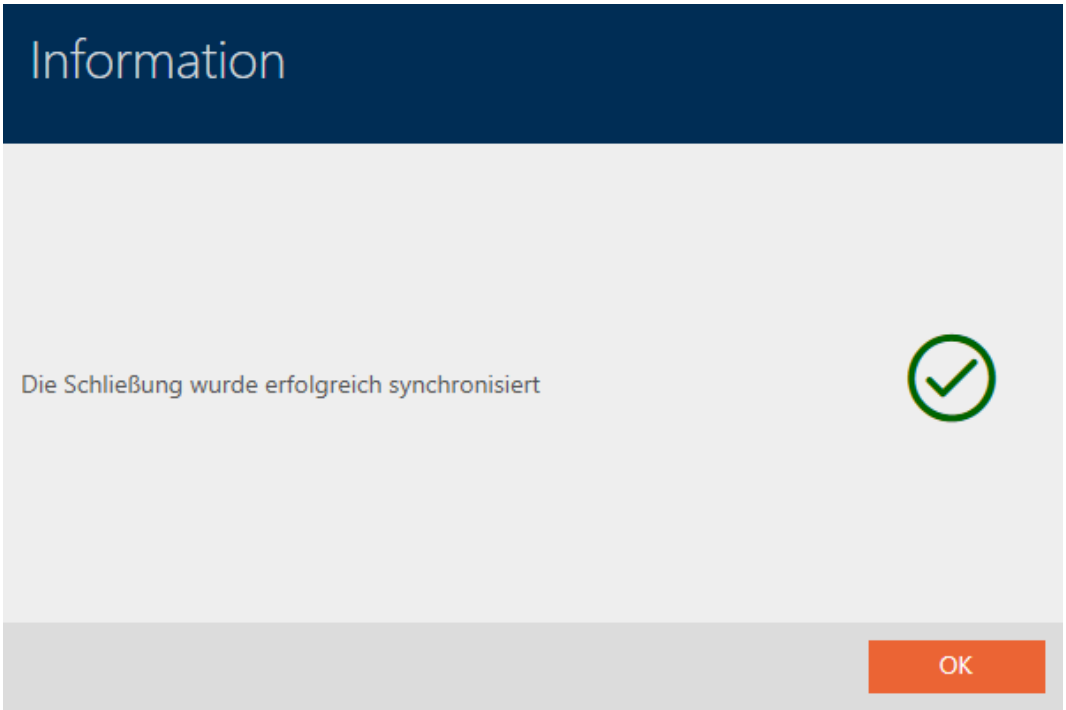
Während der ersten Synchronisierung von AX-Komponenten werden sehr viele Daten übertragen. Die Trägerfrequenz und damit die Übertragungsgeschwindigkeit ist beim SmartCD.MP oder beim SmartStick AX deutlich höher.

- Verwenden Sie insbesondere für die erste Synchronisierung von AX-Komponenten bevorzugt ein SmartCD.MP oder einen SmartStick AX.

4. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Schließung wird synchronisiert.



↳ Schließung ist synchronisiert.



HINWEIS

Abweisung der ersten Transponderbetätigung nach Erstprogrammierung von AX-Produkten

Wenn das erste betätigte Identmedium nach der Erstprogrammierung ein Transponder ist, dann kann der Transponder einmalig abgewiesen werden und im Hintergrund mit der Schließung synchronisiert werden. Danach funktionieren Transponder wie gewohnt.

19.1.1 Schließungsausstattung und -zustand anzeigen

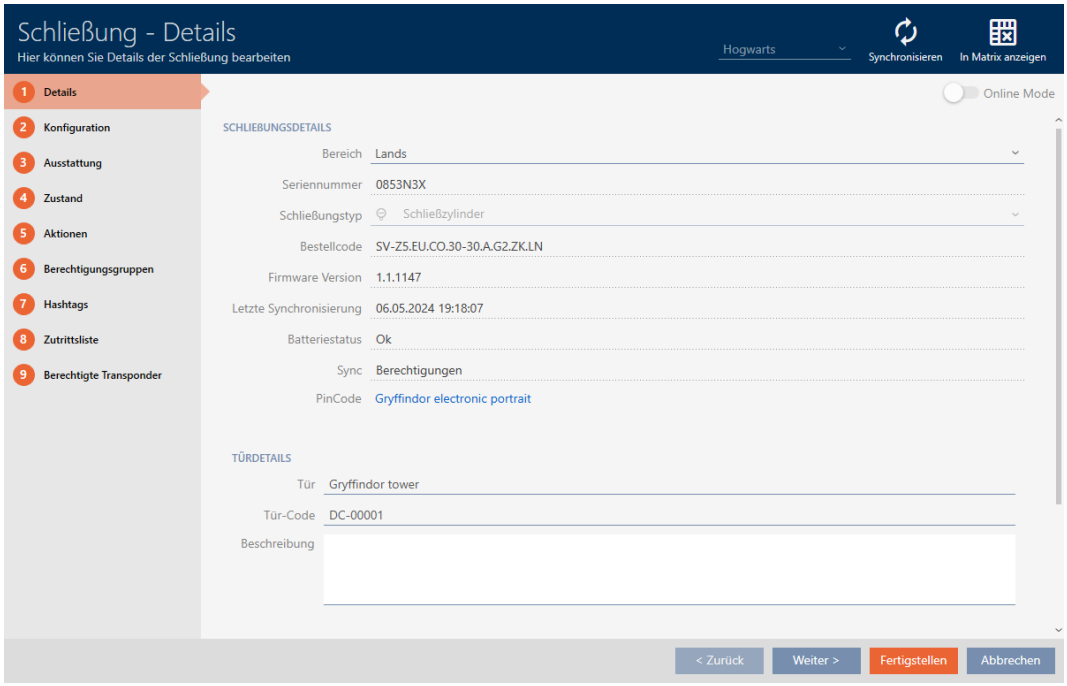
HINWEIS

Angezeigter Zustand entspricht letzter Synchronisation

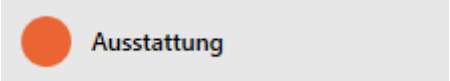
Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

✓ Schließung mindestens einmal synchronisiert.

1. Klicken Sie auf die Schließung, deren Zustand Sie anzeigen wollen.
   ↳ Fenster der Schließung öffnet sich.



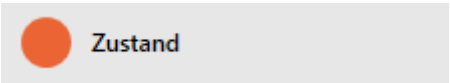
2. Klicken Sie auf den Reiter Ausstattung.



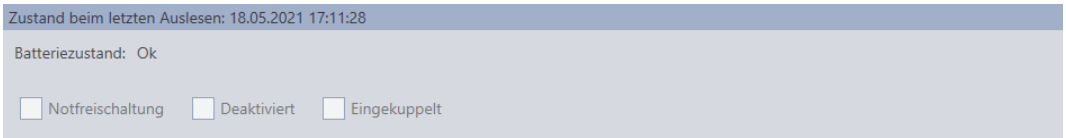
↳ Fenster wechselt zum Reiter "Ausstattung".
↳ Ausgelesene Ausstattungsmerkmale werden angezeigt (nur bei bereits synchronisierten Schließungen).

Abkürzung	Beschreibung
Z5	Digital Zylinder AX
EU	Europrofil
CO	Comfort
30-30	Baulänge - Außenlänge 30 mm - Innenlänge 30 mm
A	Aktiv
G2	Produktgeneration G2
ZK	Zutrittsprotokollierung / Zeitzonensteuerung
LN	LockNode

3. Klicken Sie auf den Reiter Zustand.



↳ Fenster wechselt zum Reiter "Zustand".
↳ Ausgelesener Zustand wird angezeigt (nur bei bereits synchronisierten Schließungen).



19.1.2 Zutrittsliste einer Schließung anzeigen und exportieren

Mit der ZK-Funktion (=Zutrittskontrolle) können Ihre Schließungen protokollieren, welche Identmedien betätigt wurden (siehe *Zugänge durch Schließung protokollieren lassen (Zutrittsliste) [▸ 293]*). Anschließend können die protokollierten Zutritte zum Beispiel während der Synchronisierung ausgelesen und in die Datenbank geschrieben werden (siehe *Zutrittsliste/Begehungsliste während der Synchronisierung auslesen [▸ 459]* und *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).

Die in der Datenbank vorhandene Zutrittsliste können Sie anzeigen und exportieren.

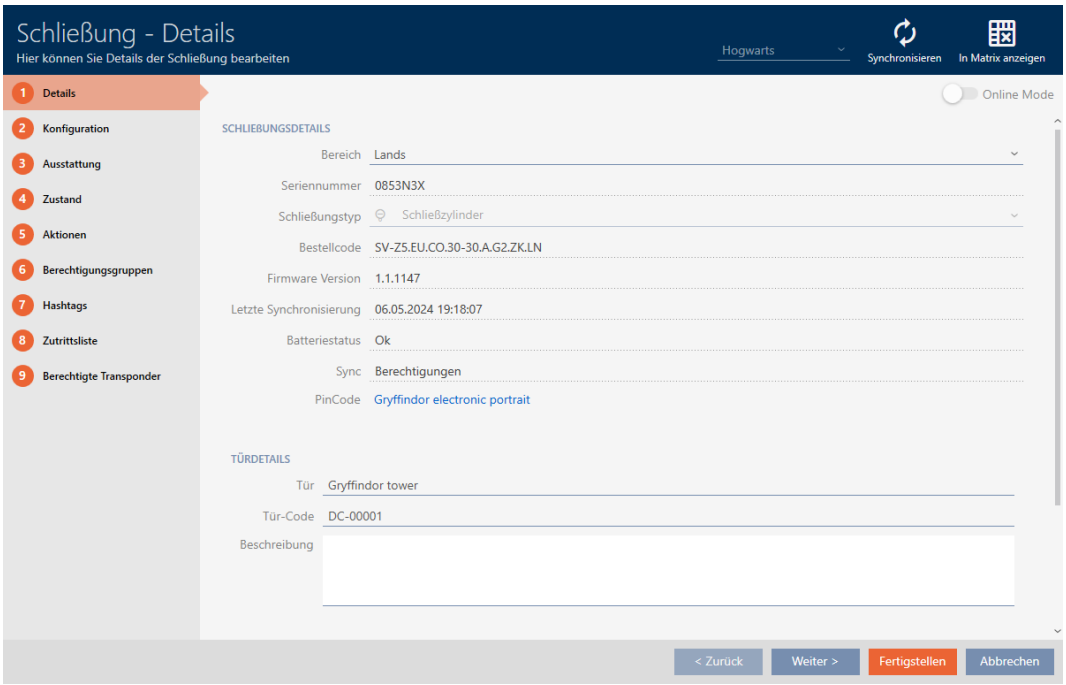
HINWEIS

Angezeigter Zustand entspricht letzter Synchronisation

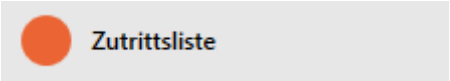
Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

✓ Schließung mindestens einmal synchronisiert.

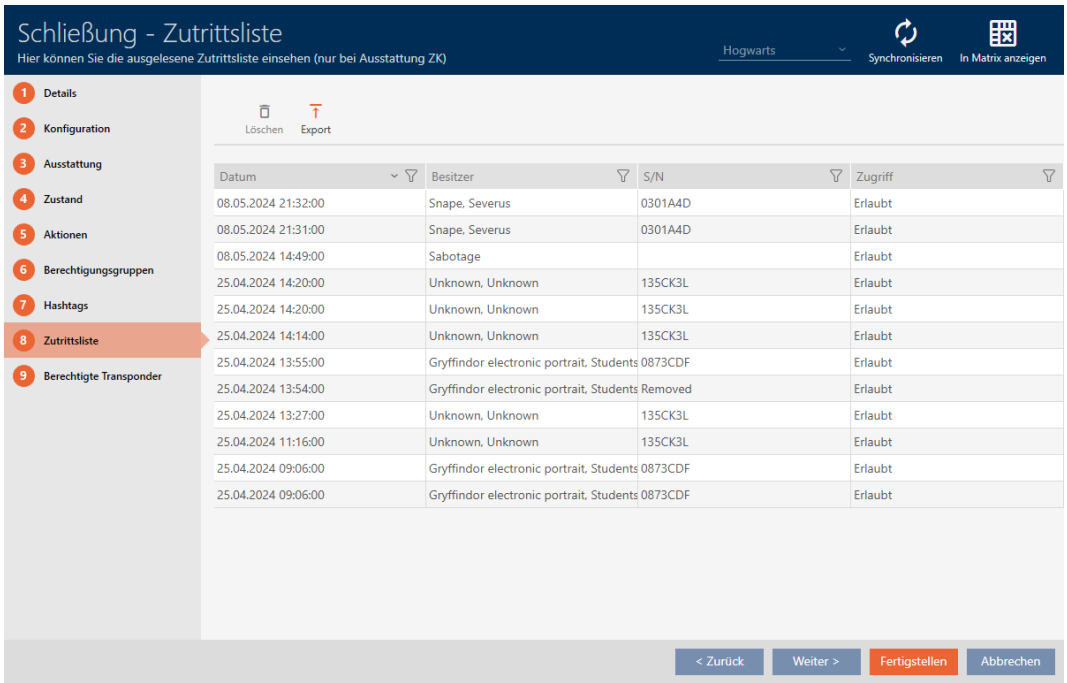
1. Klicken Sie auf die Schließung, deren Zutrittsliste Sie anzeigen wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klicken Sie auf den Reiter Zutrittsliste.



↳ Fenster wechselt zum Reiter "Zutrittsliste".
↳ Ausgelesene Zutrittsliste wird angezeigt (nur bei bereits synchronisierten Schließungen).



1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie auf die Schaltfläche Export ↑.
   ↳ Explorer-Fenster öffnet sich.
3. Speichern Sie die exportierte Zutrittsliste in ein Dateiverzeichnis Ihrer Wahl.
   ↳ Explorer-Fenster schließt sich.

↳ Zutrittsliste wird exportiert.

Beispiel:

Simons Voss technologies

Zutrittsliste für die Schließung 'Gryffindor dormitory'

Datum	Besitzer	S/N	Zugriff	Schließungskomponente
14.12.2021 17:52:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 17:51:00	McGonagall, Minerva	UID-1000000034DB9B06	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
13.12.2021 20:32:00	##ServiceTId_IDS_AX_SETTIME		Erlaubt	Master

Simons Voss technologies Gedruckt am: 14.12.2021 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

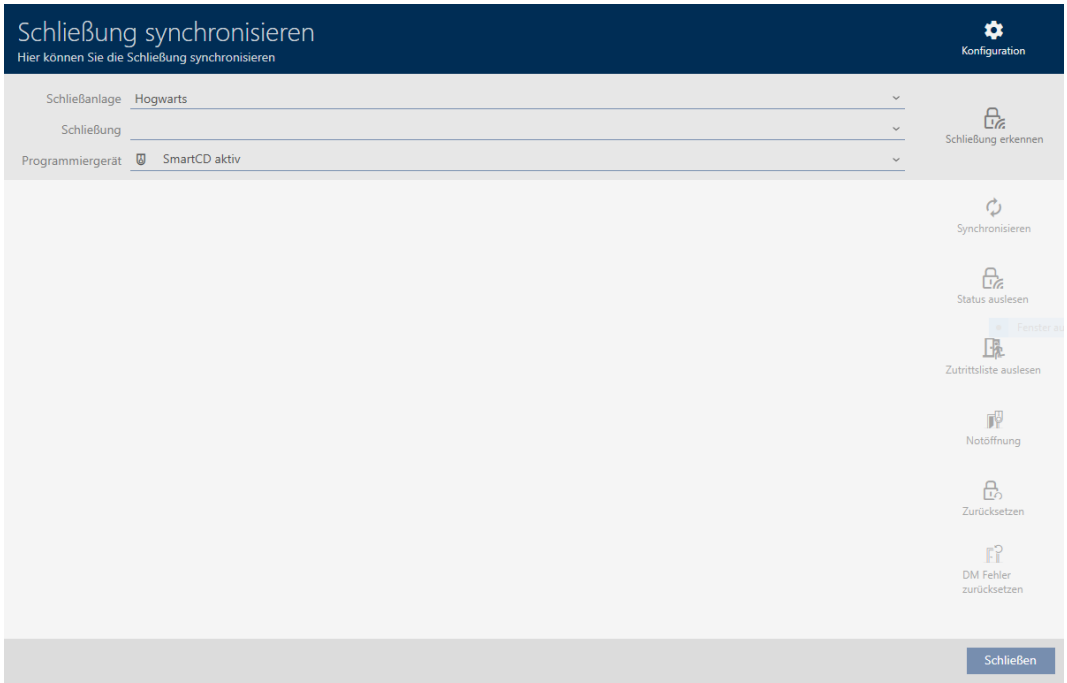
19.2 Unbekannte Schließung erkennen

Wenn Ihnen eine unbekannte Schließung vorliegt, dann können Sie diese beispielsweise über das Synchronisieren-Symbol ( ) identifizieren und ggfs. zurücksetzen (siehe *Schließung zurücksetzen [▸ 425]*).

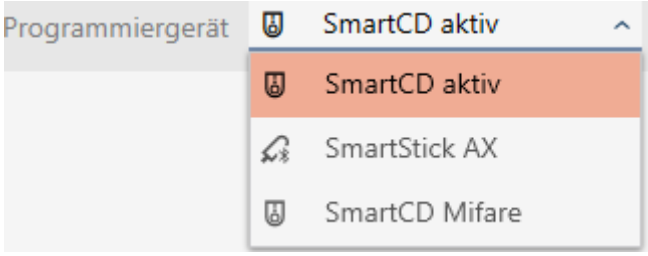
✓ Geeignetes Programmiergerät angeschlossen.

1. Klicken Sie in der Kopfzeile auf das Icon .

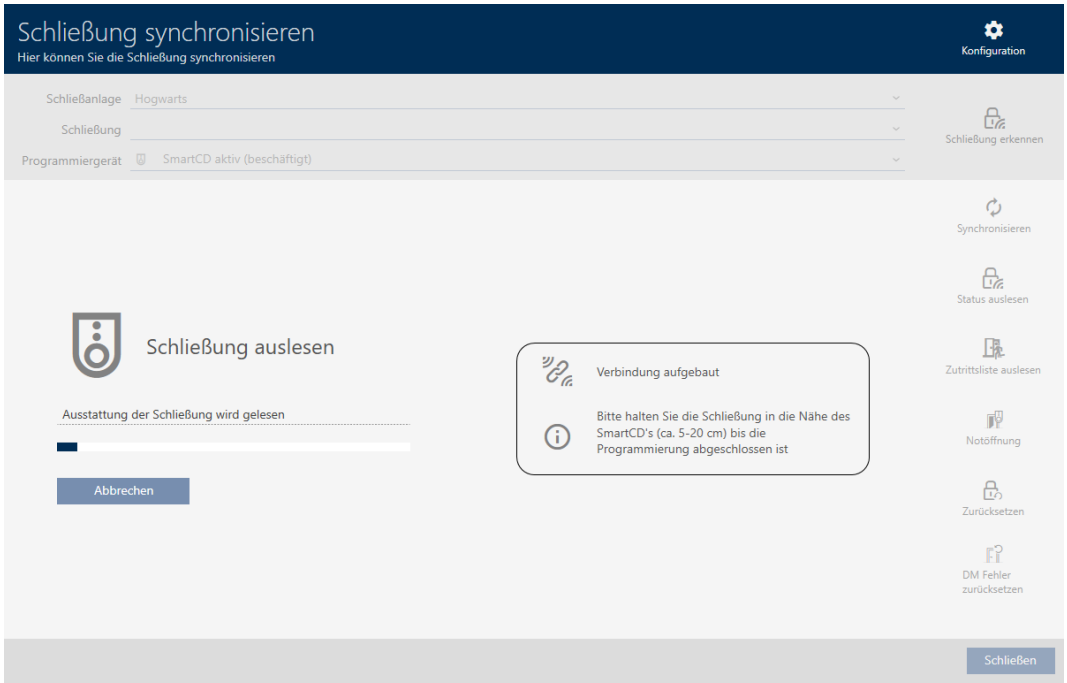
↳ Fenster "Schließung synchronisieren" öffnet sich.



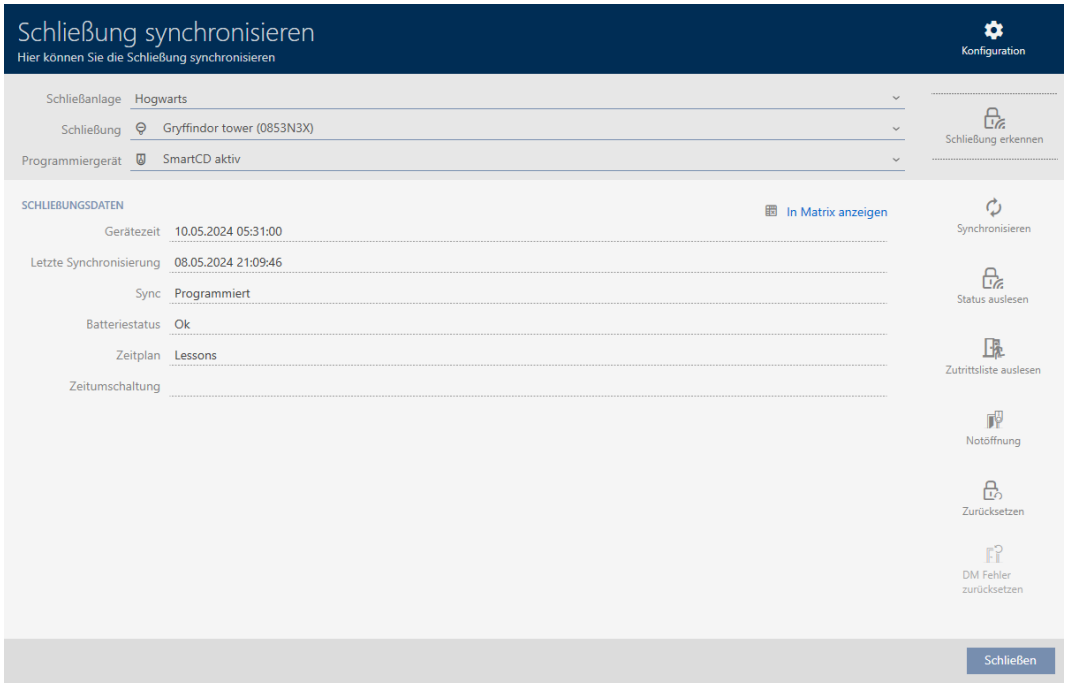
2. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihre Schließung erkennen wollen.



3. Klicken Sie auf die Schaltfläche Schließung erkennen.
   ↳ Schließung wird erkannt.



↳ Schließungsinformationen werden Ihnen im Fenster der Schließung angezeigt.



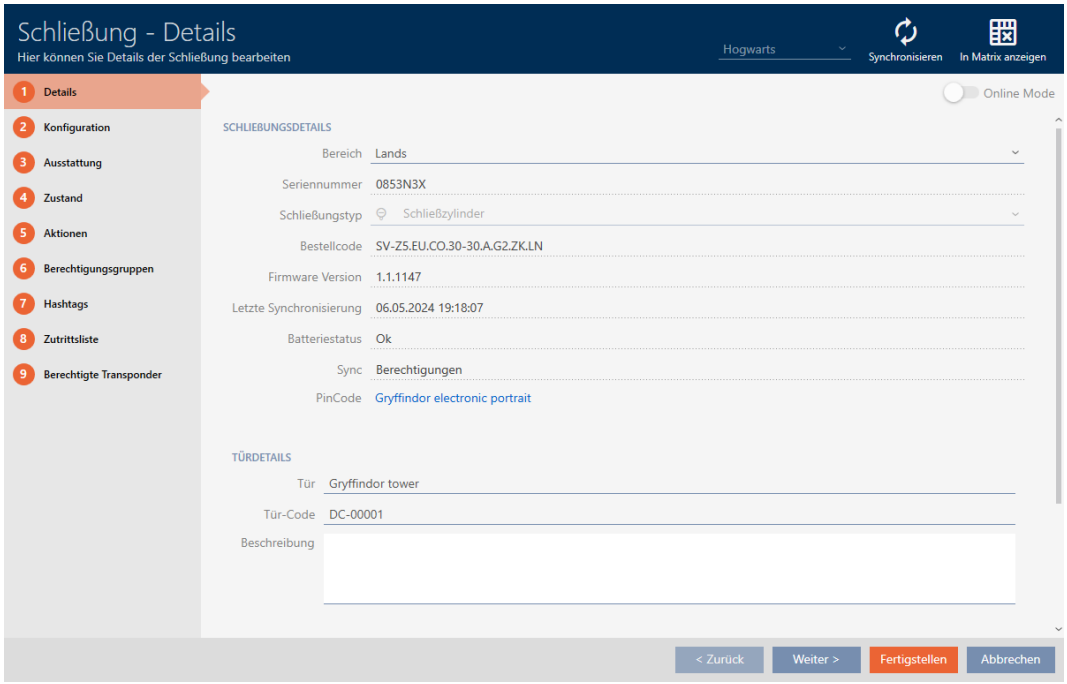
Sie können die Schließung jetzt beispielsweise zurücksetzen (siehe *Schließung zurücksetzen [▸ 425]*).

19.3 Schließung zurücksetzen

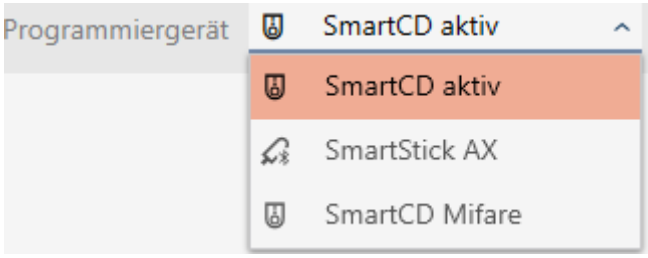
Bevor Sie eine Komponente wie einen Schließzylinder wieder für eine andere Schließung oder eine andere Schließanlage verwenden können, müssen Sie sie zurücksetzen.

✓ Geeignetes Programmiergerät angeschlossen.
✓ Schließungsliste oder Matrixansicht geöffnet.

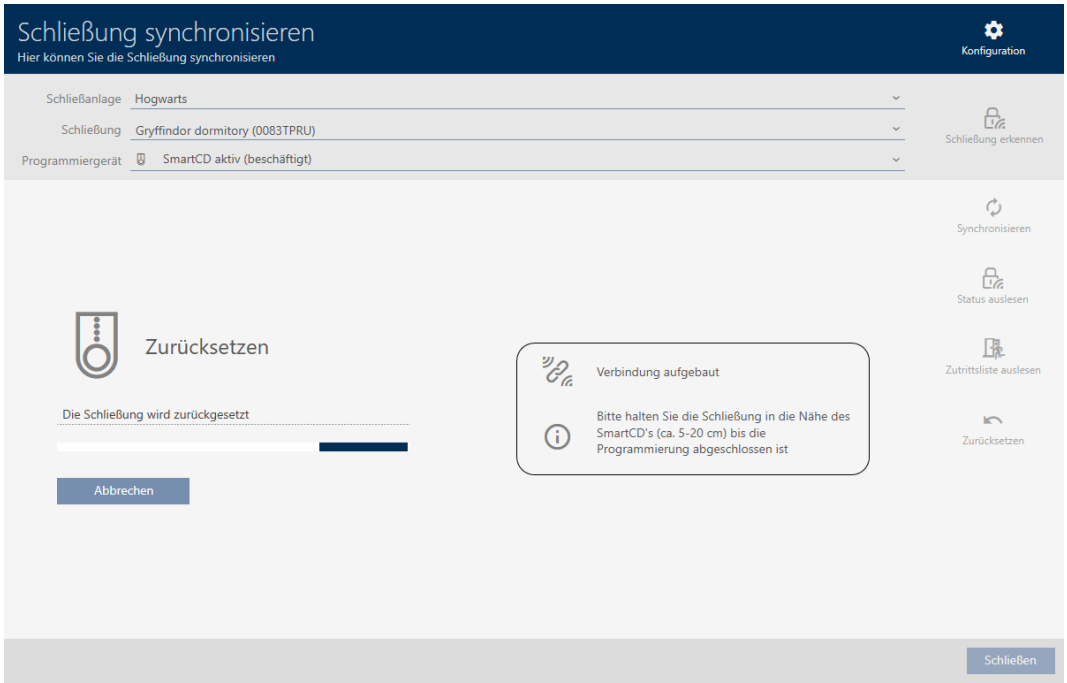
1. Klicken Sie auf die Schließung, die Sie zurücksetzen wollen.
   Wenn Ihnen die Schließung nicht bekannt ist: Klicken Sie auf irgendeine Schließung und identifizieren Sie die Schließung (siehe *Unbekannte Schließung erkennen [▸ 423]*). Fahren Sie dann fort.
   ↳ Fenster der Schließung öffnet sich.



2. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Synchronisieren-Fenster öffnet sich.
3. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihre Schließung zurücksetzen wollen.

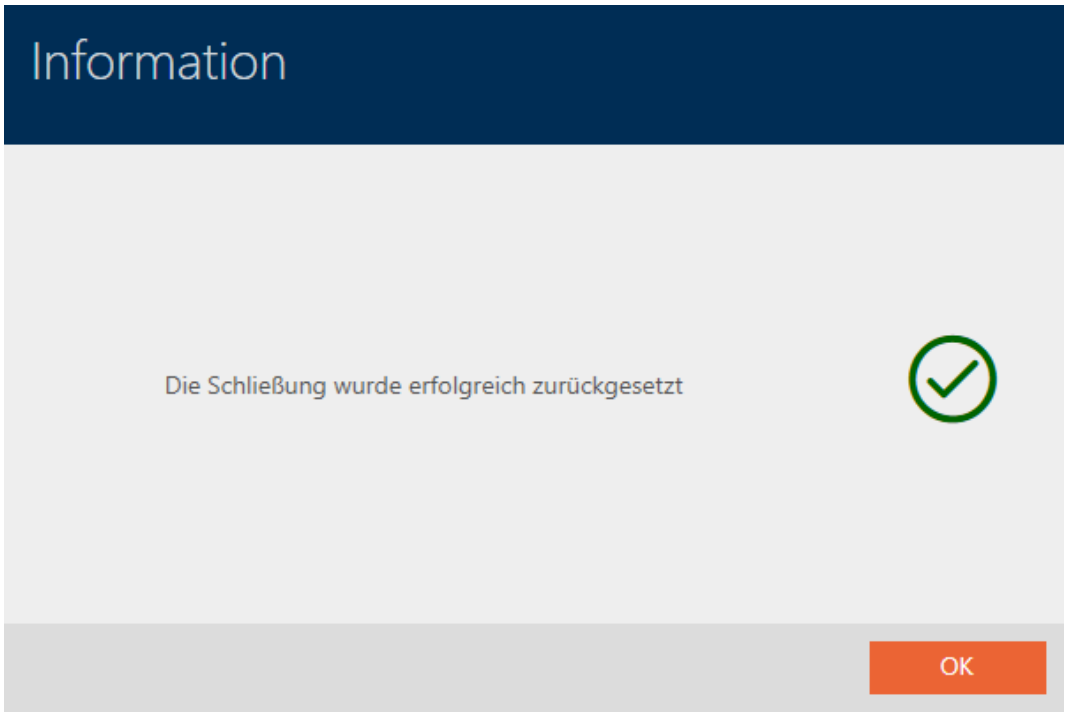


4. Klicken Sie auf die Schaltfläche Zurücksetzen.
   ↳ Schließung wird zurückgesetzt.



5. Bestätigen Sie ggfs. die Rückfrage, ob die Zutrittslisten vorher nochmals ausgelesen werden sollen.

↳ Schließung ist zurückgesetzt.



19.4 Identmedium synchronisieren

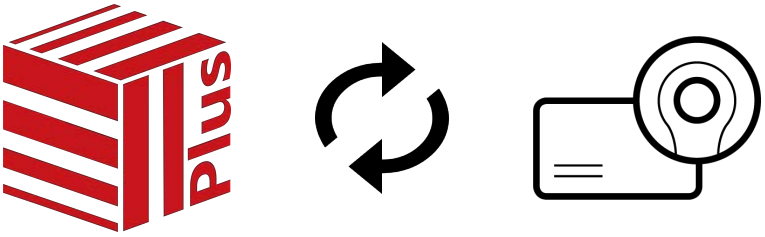
Die Synchronisierung ist bidirektional:

- Auslesen von Daten, die im Identmedium gespeichert sind (z.B. Batteriezustand)
- Schreiben von neuen Daten ins Identmedium (z.B. Berechtigungen)

Begehungslisten können separat ausgelesen werden (Schaltfläche Begehungsliste auslesen). Optional können Begehungslisten aber auch einfach während der Synchronisierung mit ausgelesen werden (siehe *Zutrittsliste/Begehungsliste während der Synchronisierung auslesen* *[▸ 459]*).

Ausgelesene Daten können anschließend angezeigt werden (siehe z.B. *Identmedium-Batteriestatus anzeigen* *[▸ 430]* oder *Begehungsliste für Transponder/Karten anzeigen und exportieren* *[▸ 431]*).

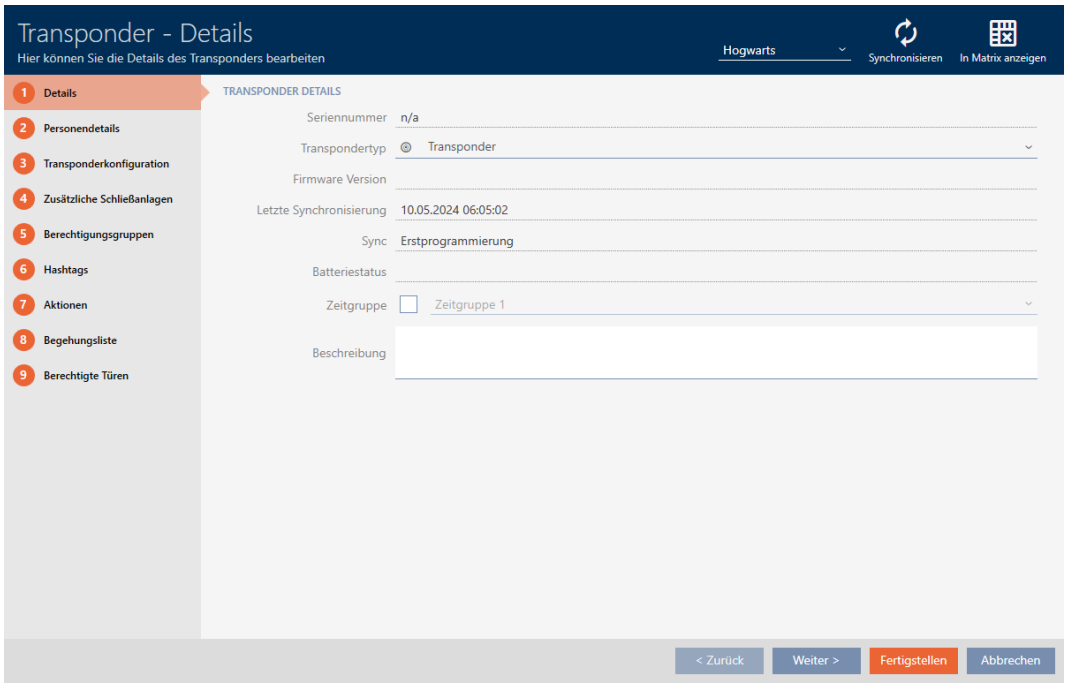
19.4.1 Transponder/Karte synchronisieren (inkl. Begehungsliste lesen)



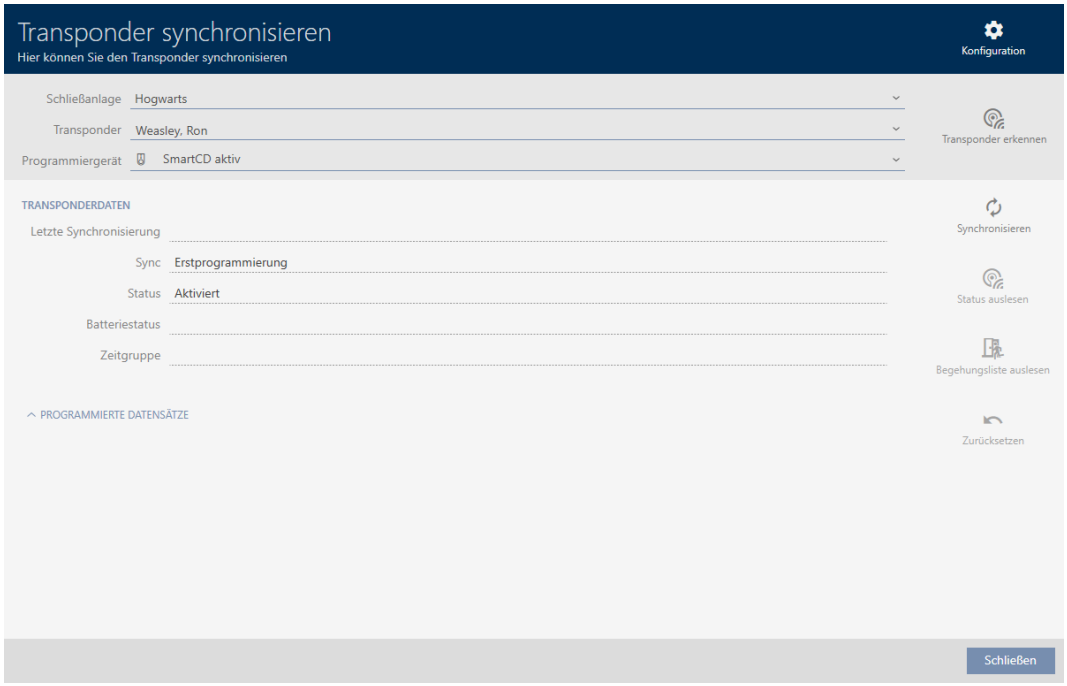
Das folgende Beispiel zeigt die Synchronisierung eines Transponders.

✓ Geeignetes Programmiergerät angeschlossen.
✓ Identmedienliste oder Matrixansicht geöffnet.

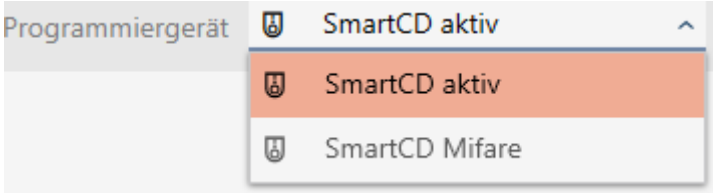
1. Klicken Sie auf das Identmedium, das Sie synchronisieren wollen.
   ↳ Fenster des Identmediums öffnet sich.



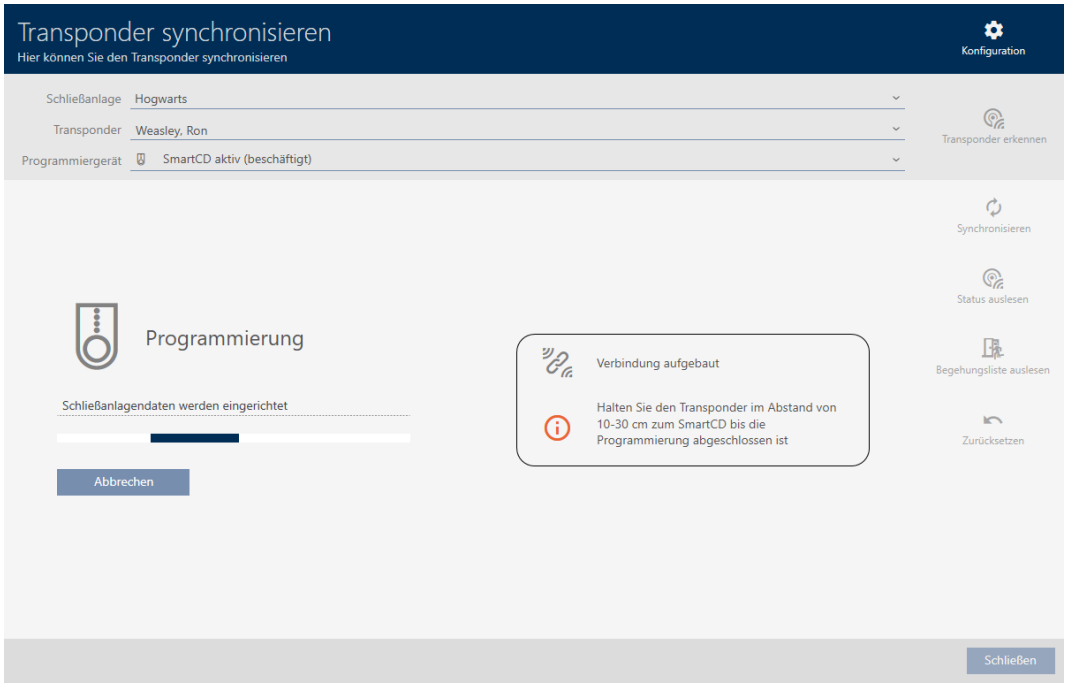
2. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Synchronisieren-Fenster öffnet sich.



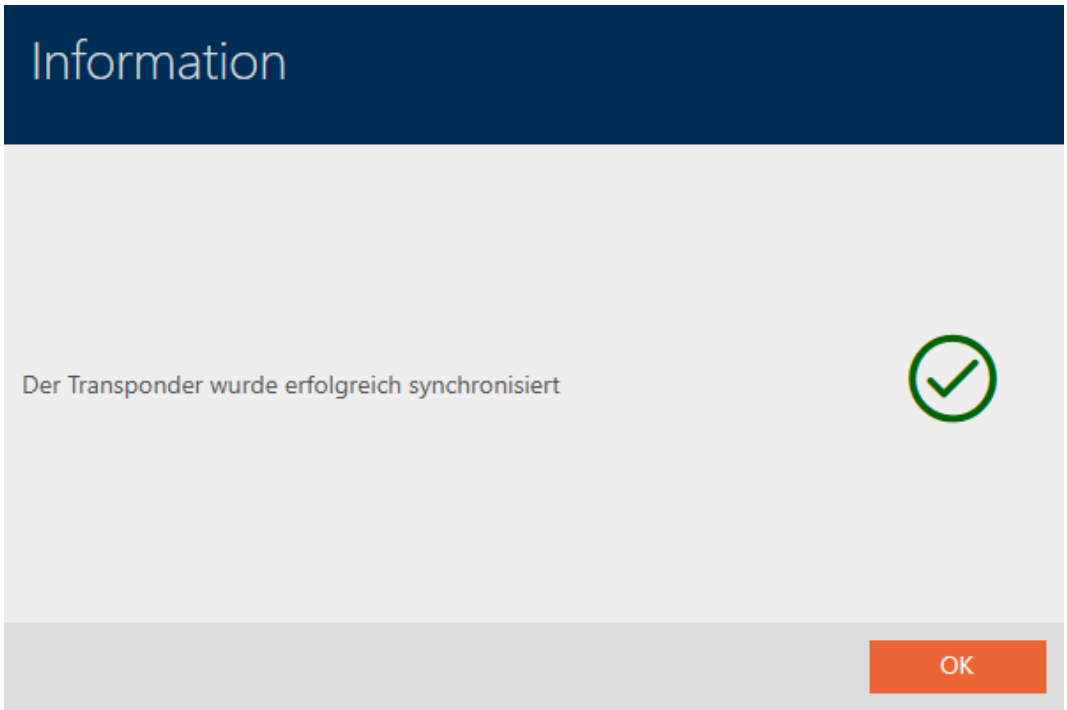
3. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie synchronisieren wollen.



4. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Identmedium wird synchronisiert.



↳ Identmedium ist synchronisiert.



19.4.1.1 Identmedium-Batteriestatus anzeigen

HINWEIS

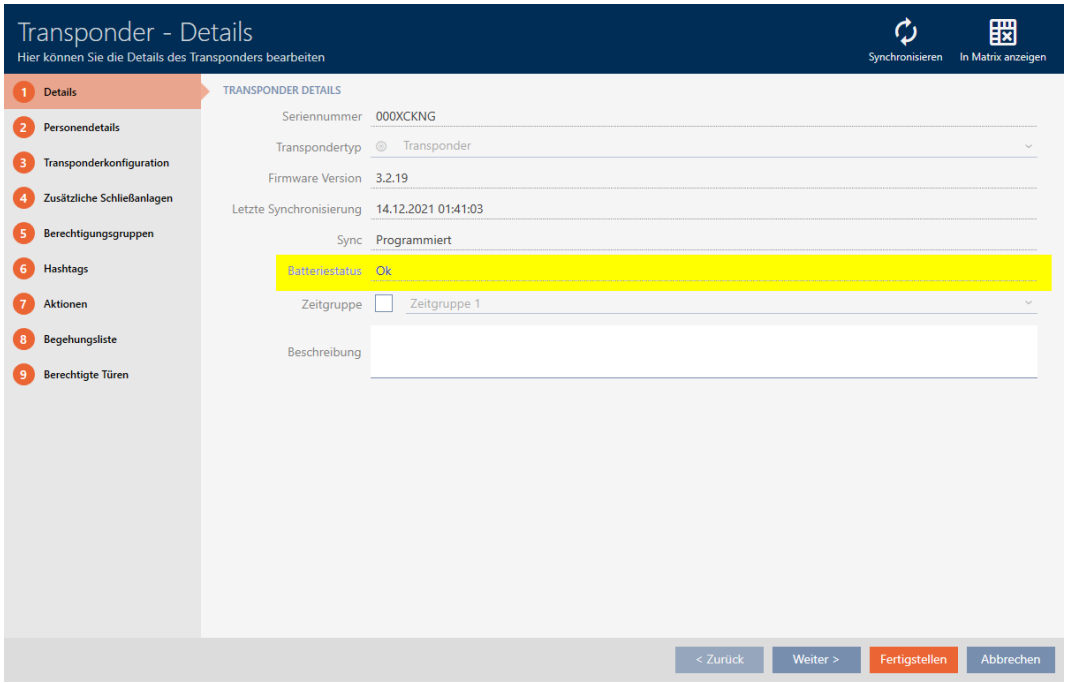
Angezeigter Zustand entspricht letzter Synchronisation

Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

✓ Identmedium mindestens einmal synchronisiert.

Klicken Sie auf das Identmedium, dessen Zustand Sie anzeigen wollen.

↳ Fenster des Identmediums öffnet sich.



↳ Batteriestatus wird angezeigt.

19.4.1.2 Begehungsliste für Transponder/Karten anzeigen und exportieren

Ihre Identmedien können auf Wunsch protokollieren, an welchen Schließungen sie betätigt wurden (siehe *Zugänge durch Identmedium mitschreiben lassen (Begehungsliste) [▸ 125]*). Anschließend werden die gespeicherten Einträge in dieser Begehungsliste zum Beispiel während einer Synchronisation in die Datenbank übertragen (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).

Die in der Datenbank gespeicherten Begehungslisten können Sie anzeigen und exportieren.

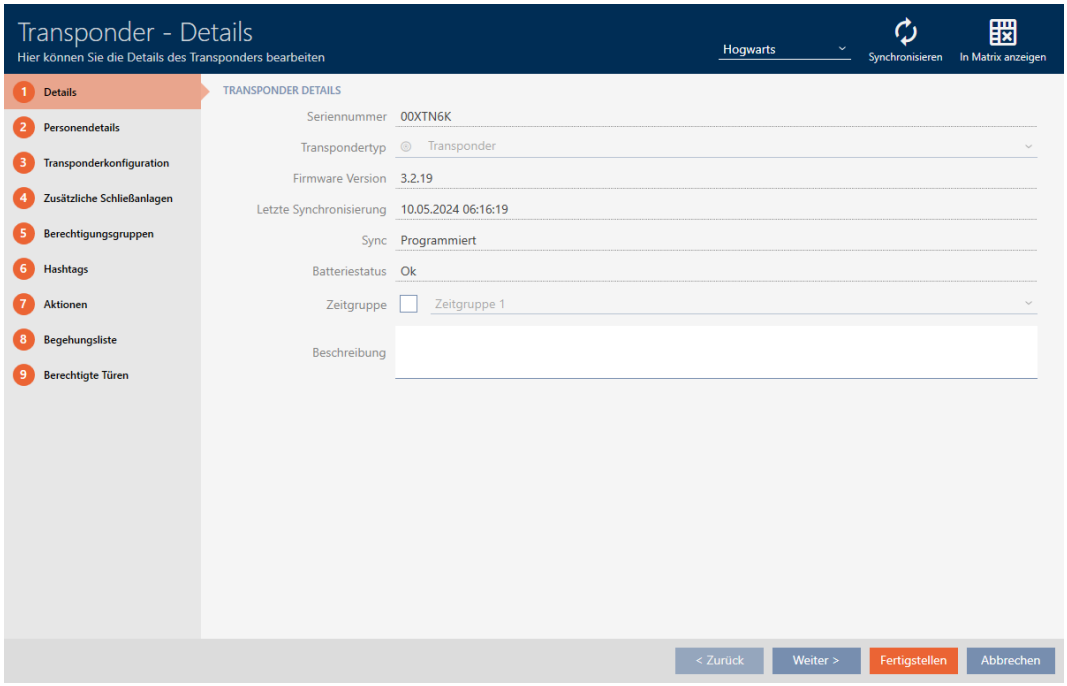
HINWEIS

Angezeigter Zustand entspricht letzter Synchronisation

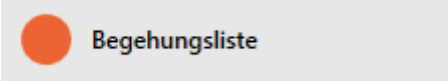
Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

✓ Identmedium mindestens einmal synchronisiert.

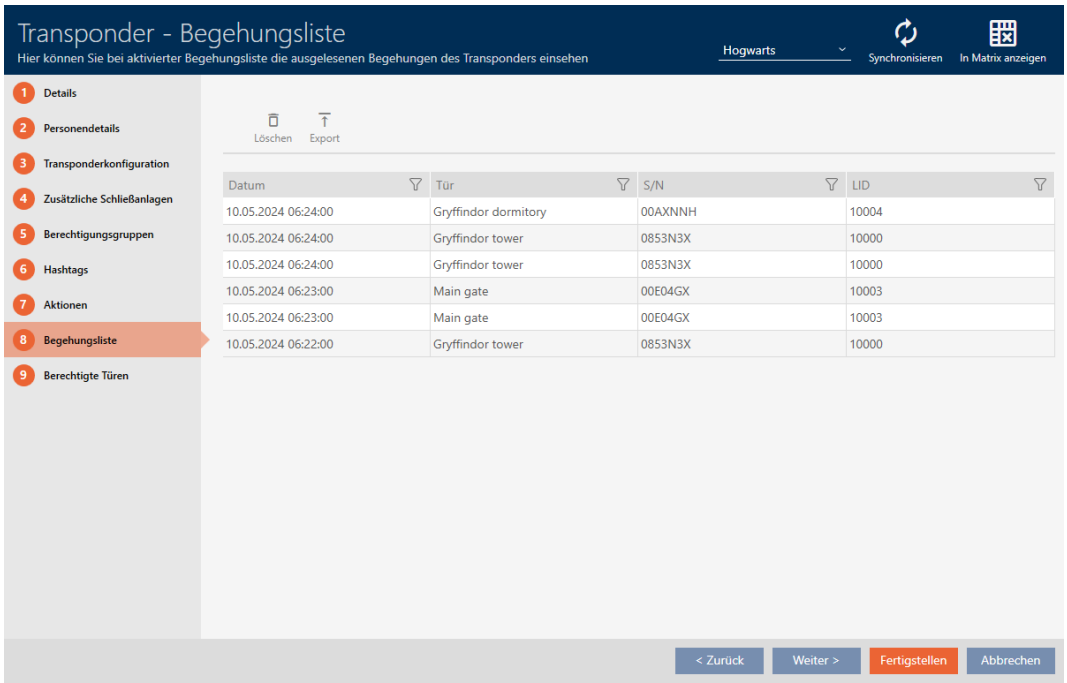
1. Klicken Sie auf das Identmedium, dessen Begehungsliste Sie anzeigen wollen.
   ↳ Fenster des Identmediums öffnet sich.



2. Klicken Sie auf den Reiter Begehungsliste



↳ Fenster wechselt zum Reiter "Begehungsliste".



3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
4. Klicken Sie auf die Schaltfläche Export ⤒.
   ↳ Explorer-Fenster öffnet sich.

5. Speichern Sie die exportierte Begehungsliste in einem Dateiverzeichnis Ihrer Wahl.
   ↳ Explorer-Fenster schließt sich.

↳ Begehungsliste ist exportiert.

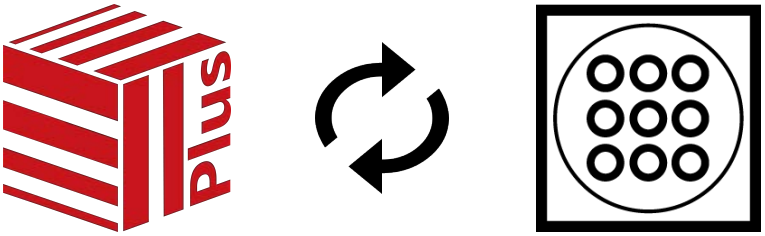
Begehungsliste für den Transponder Weasley '00XTN6K'

Datum	Tür	S/N	LID
10.05.2024 06:24:00	Gryffindor dormitory	00AXNNH	10004
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:22:00	Gryffindor tower	0853N3X	10000

Ausdruck vom: 10.05.2024 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

19.4.2 PinCode-Tastatur synchronisieren



Änderungen an einer PinCode-Tastatur) können auch zu Programmierbedarf an der zugewiesenen Schließung führen (siehe *PinCode G1 vs. PinCode AX [▸ 534]*). In diesem Fall synchronisieren Sie stattdessen die Schließung (siehe *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).

Die Synchronisierung zwischen den beiden PinCode-Tastaturen unterscheidet sich. Ihre AXM Plus unterstützt Sie während der Synchronisierung mit Anweisungen.

HINWEIS

Synchronisierung der PinCode-Tastatur 3068 benötigt Master-PIN und User-PINs

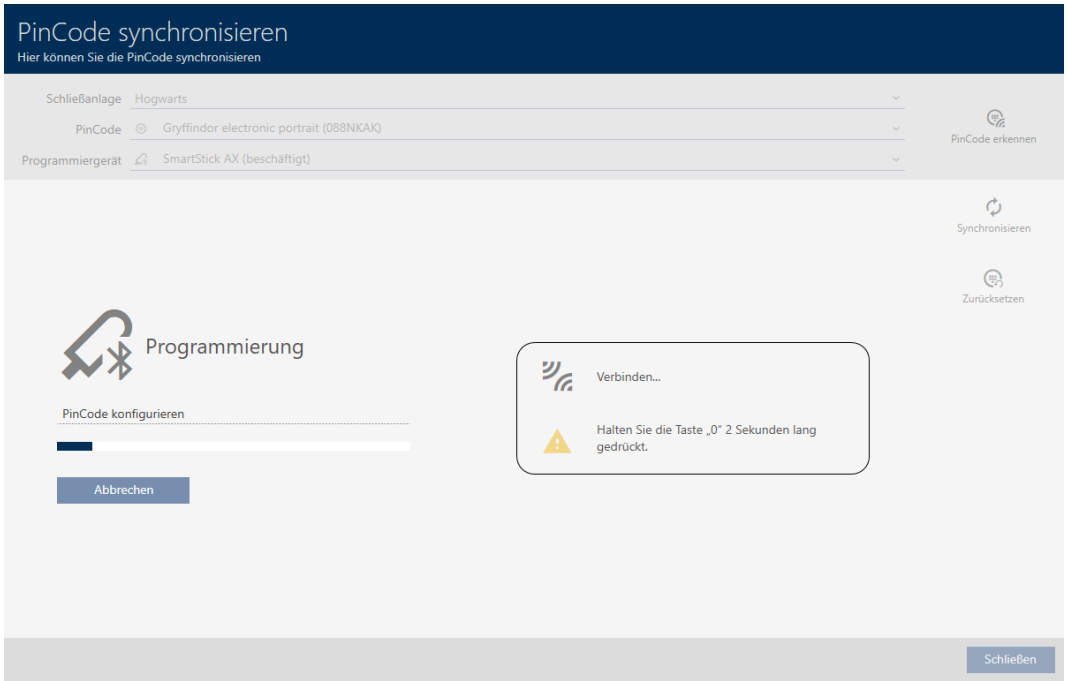
In der PinCode-Tastatur 3068 sind die User-PINs mit einer G1-ID verbunden. Ohne eingerichtete User-PINs sind die G1-IDs nicht ansprechbar und synchronisierbar.

1. Ändern Sie die werkseitige Master-PIN (siehe Handbuch zur PinCode-Tastatur 3068).
2. Vergeben Sie mindestens eine User-PIN.

Im folgenden Beispiel wird eine PinCode-Tastatur AX synchronisiert.

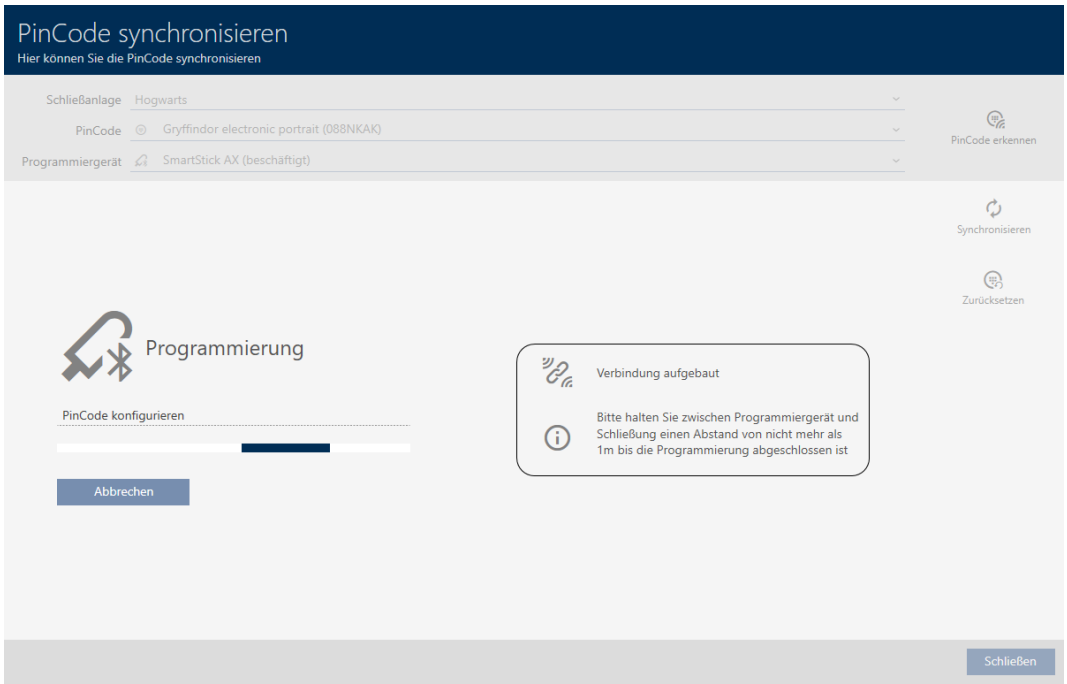
- ✓ PinCode-Tastatur AX erstellt und zugewiesen (siehe *PinCode-Tastaturen erstellen [▸ 102]*).
- ✓ Programmierbedarf an PinCode-Tastatur AX, z.B. durch eine Berechtigungsänderung.
- ✓ Geeignetes Programmiergerät angeschlossen (SmartStick AX).
- ✓ Matrixansicht geöffnet.

1. Klicken Sie auf das Synchronisieren-Icon ⟲ einer beliebigen PIN der betroffenen PinCode-Tastatur AX.
   ↳ Fenster "PinCode synchronisieren" öffnet sich und Synchronisation startet.



2. Halten Sie auf der PinCode-Tastatur AX die Taste "0" für mindestens zwei Sekunden gedrückt.

3. Positionieren Sie den SmartStick AX in der Nähe der PinCode-Tastatur AX (max. 1 m).
   - ↳ LED flackert grün und PinCode-Tastatur AX piept.
   - ↳ BLE-Schnittstelle ist aufgeweckt.
   - ↳ PinCode-Tastatur AX wird synchronisiert.

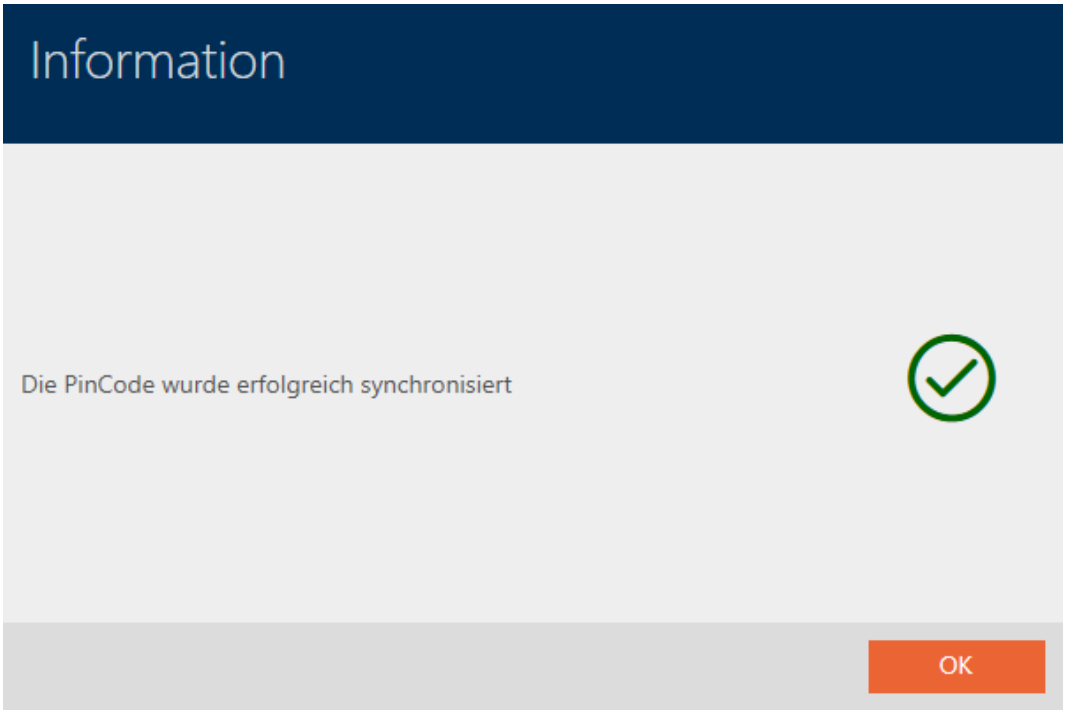


   - ↳ PinCode-Tastatur AX ist synchronisiert.

HINWEIS

PinCode-Tastatur AX nach Synchronisierung im Programmiermodus

Nach der abgeschlossenen Synchronisierung ist die PinCode-Tastatur AX noch etwa 30 Sekunden nicht funktionsfähig, da sie sich noch im Programmiermodus befindet.

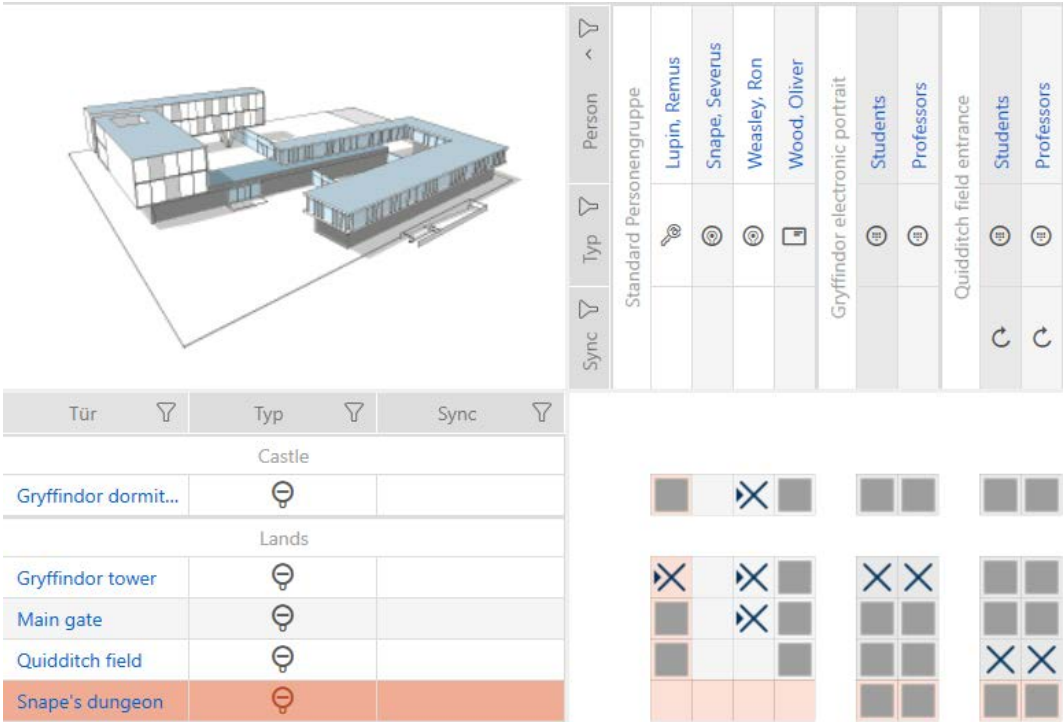


19.4.3 AX2Go-Schlüssel synchronisieren

Nach der erstmaligen Einrichtung von AX2Go werden Änderungen komfortabel über die SimonsVoss-Cloud übertragen (weitere Informationen dazu siehe *Synchronisation der AX2Go-Schlüssel über die Cloud* [▸ 538]).

Das folgende Beispiel beschreibt den Ablauf der Synchronisation, wenn an einer Schließung zum ersten Mal ein AX2Go-Schlüssel berechtigt wird.

In der Ausgangssituation ist noch kein AX2Go-Schlüssel an der Schließung berechtigt:



✓ Gültige ☑ Service Fee Lizenz (siehe *Registrierung mit Lizenz [▸ 39]*).

✓ Verbindung zwischen SimonsVoss-ID und AXM Plus (siehe *Registrierung mit Lizenz [▸ 39]*).

✓ Matrixansicht geöffnet.

- Berechtigen Sie einen AX2Go-Schlüssel an der gewünschten Schließung.
  - ↳ Programmierbedarf an Schließung und AX2Go entsteht.
  - ↳ AX2Go-Schlüssel wird über Cloud automatisch synchronisiert.
  - ↳ Programmierbedarf verschwindet.

↳ AX2Go-Schlüssel ist an Schließung berechtigt.

Sollte die Berechtigungsänderung nicht übertragen werden: Starten Sie den AXM-Dienst neu und verbinden Sie dann Ihre AXM Plus erneut mit Ihrer SimonsVoss-ID (siehe *Verbindung zwischen Datenbank und Cloud überprüfen [▸ 451]*).

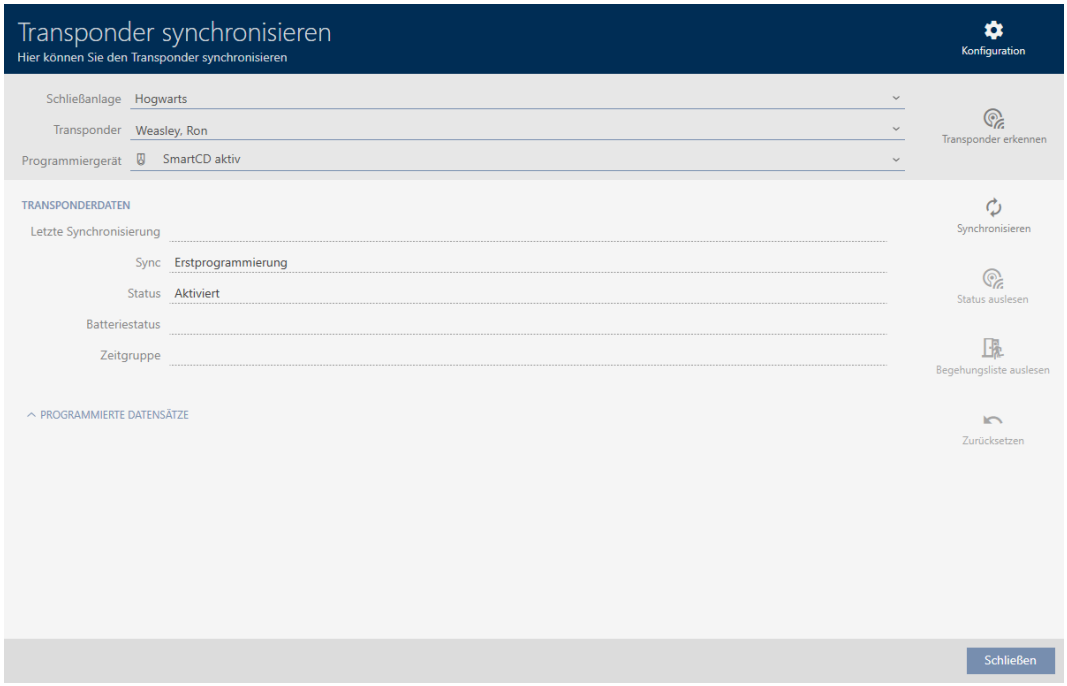
19.5 Unbekanntes Identmedium erkennen

19.5.1 Unbekannte Transponder/Karten erkennen

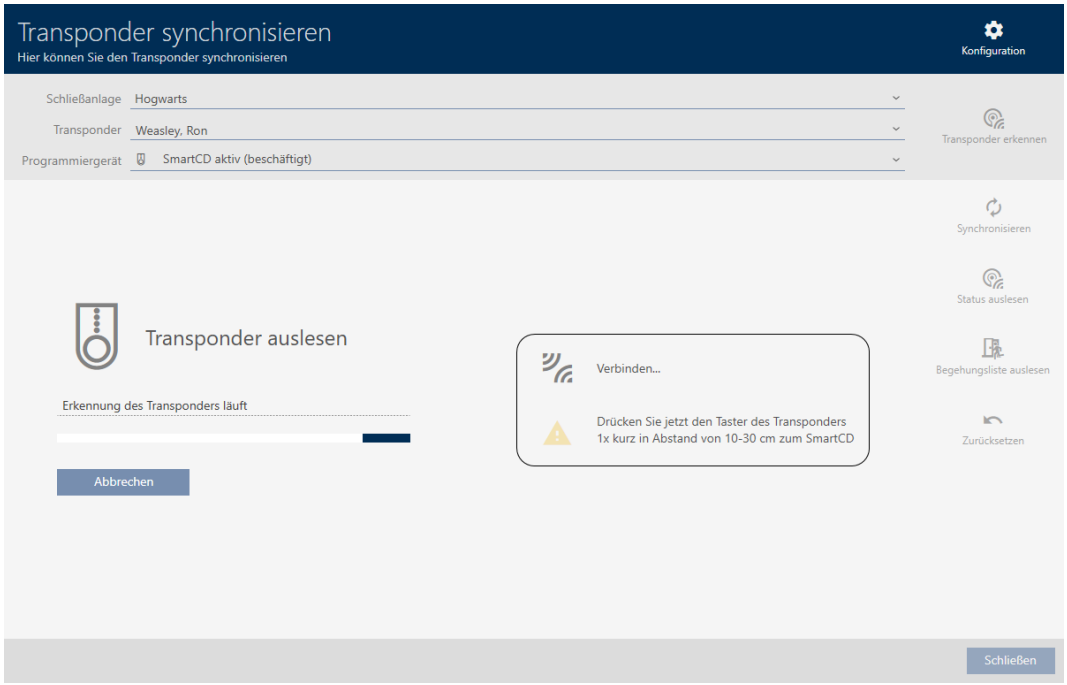
✓ Geeignetes Programmiergerät angeschlossen.

1. Klicken Sie in der Kopfzeile auf das Icon .

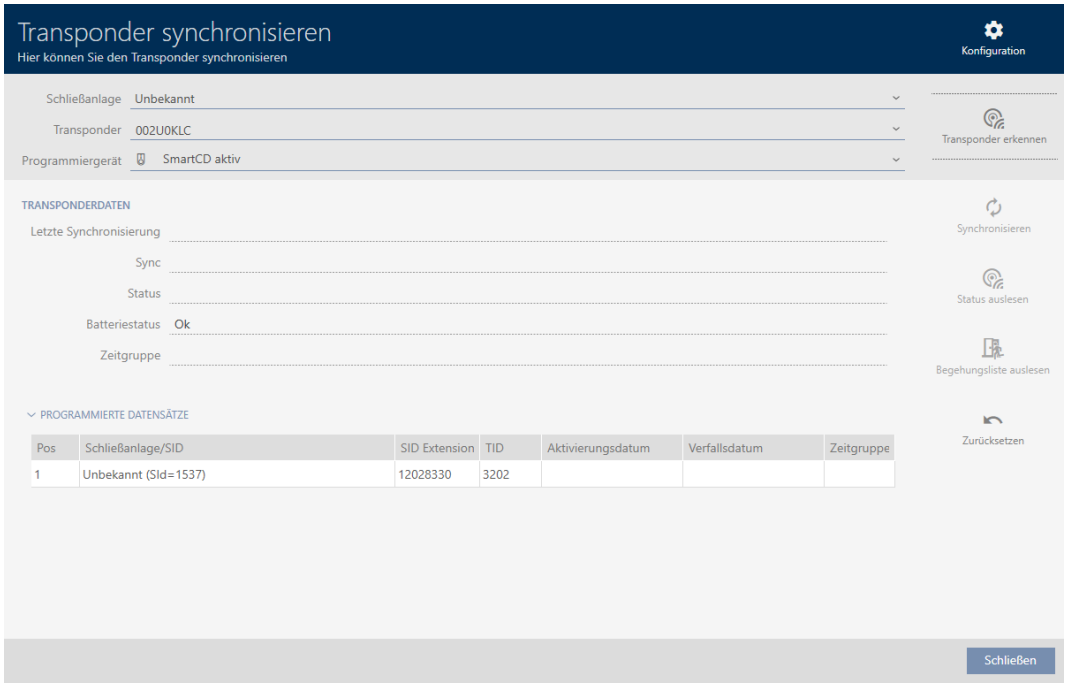
↳ Fenster "Transponder synchronisieren" öffnet sich.



2. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihr Identmedium erkennen wollen.
3. Klicken Sie auf die Schaltfläche Transponder erkennen
4. Folgen Sie ggfs. den Anweisungen.
   ↳ Identmedium wird erkannt.



↳ Informationen zum Identmedium werden Ihnen im Fenster angezeigt.



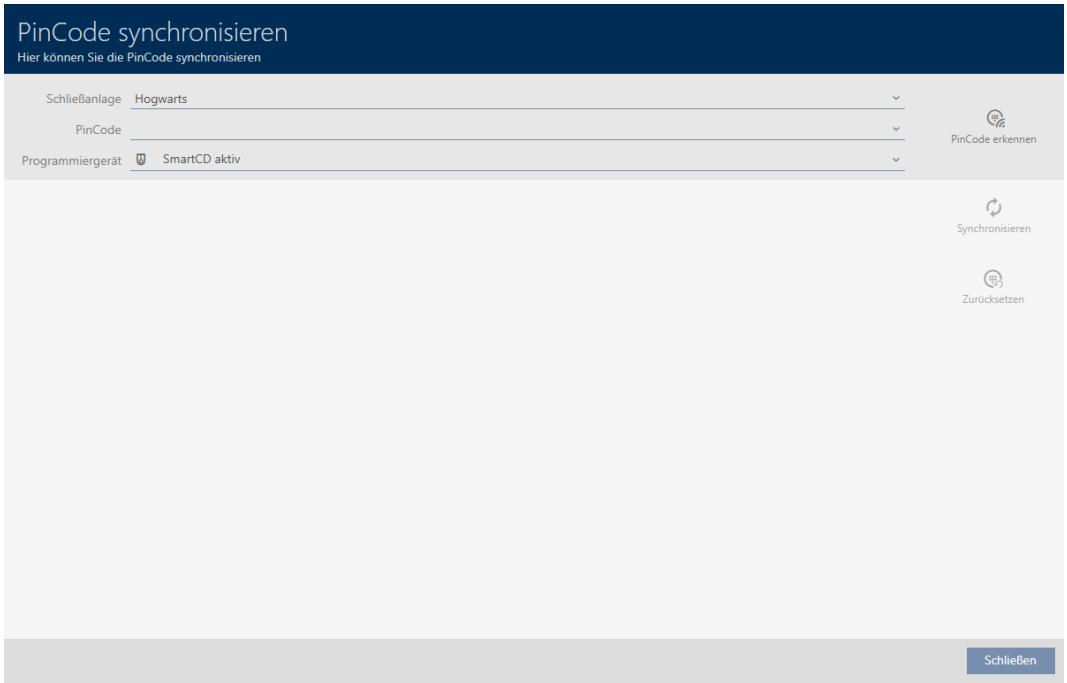
Sie können das Identmedium jetzt beispielsweise zurücksetzen (siehe *Transponder/Karten zurücksetzen [▸ 443]*).

19.5.2 Unbekannte PinCode-Tastatur erkennen

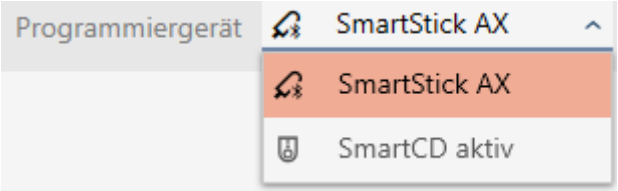
✓ Geeignetes Programmiergerät angeschlossen (SmartStick AX für PinCode-Tastatur AX, SmartCD2.G2 für PinCode-Tastatur 3068)

1. Klicken Sie in der Kopfzeile auf das Icon .

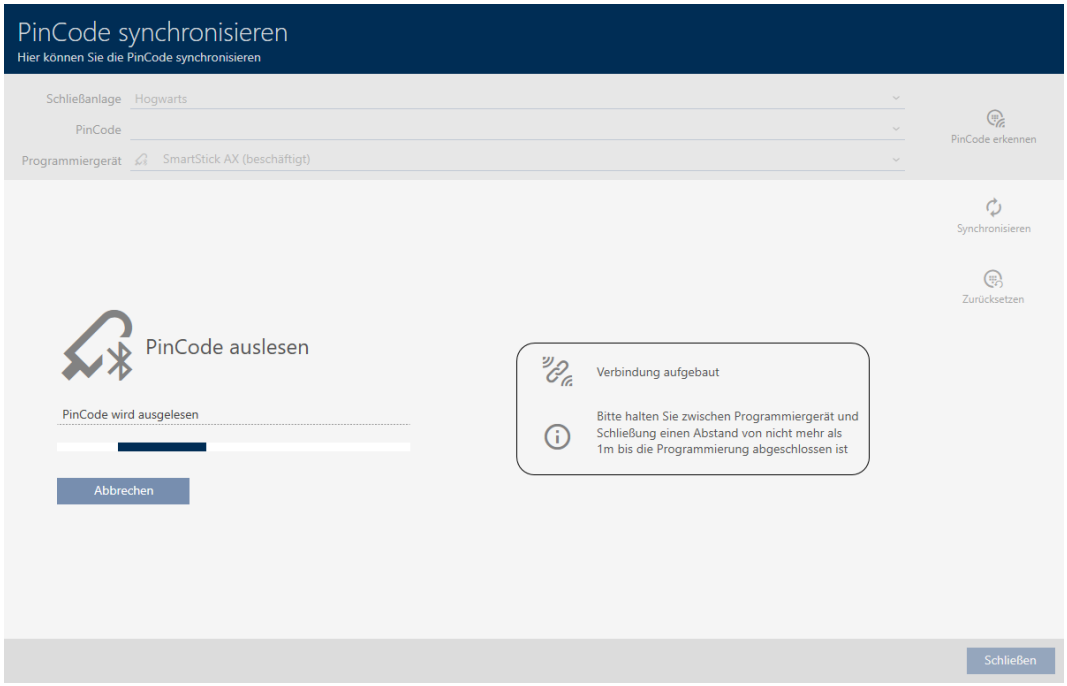
↳ Fenster "PinCode synchronisieren" öffnet sich.



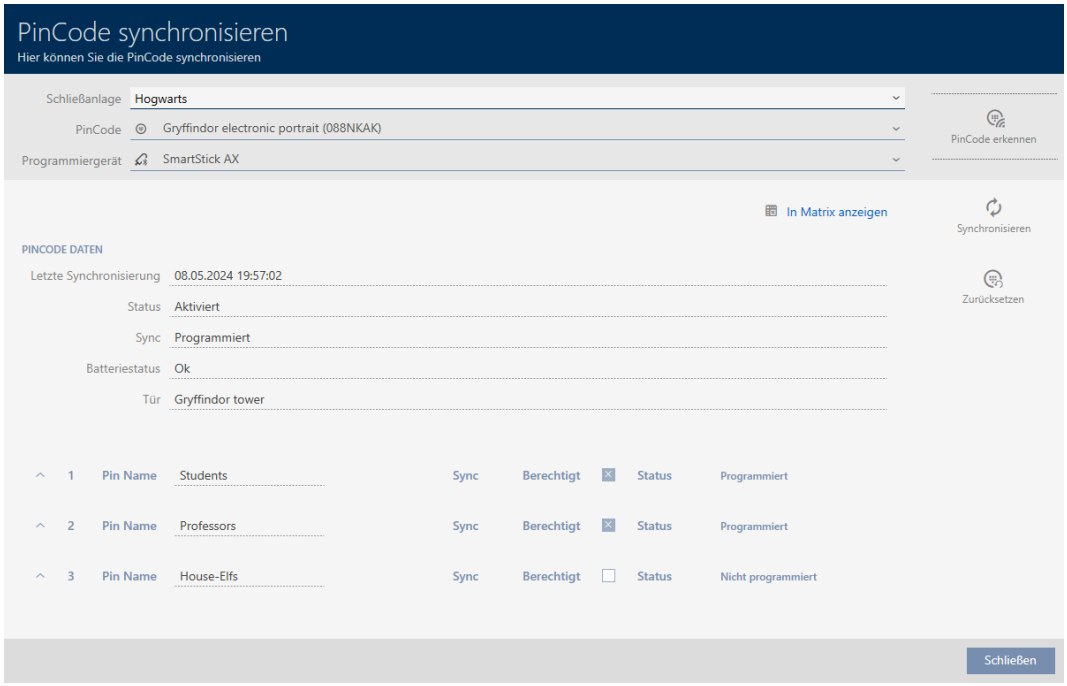
2. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihre PinCode-Tastatur erkennen wollen.



3. Klicken Sie auf die Schaltfläche PinCode erkennen.
4. Folgen Sie ggfs. den Anweisungen.
   ↳ PinCode-Tastatur wird ausgelesen.



↳ Informationen zur PinCode-Tastatur werden Ihnen im Fenster angezeigt.



Sie können die PinCode-Tastatur jetzt beispielsweise zurücksetzen (siehe *PinCode-Tastatur zurücksetzen [▸ 446]*).

19.6 Identmedien zurücksetzen

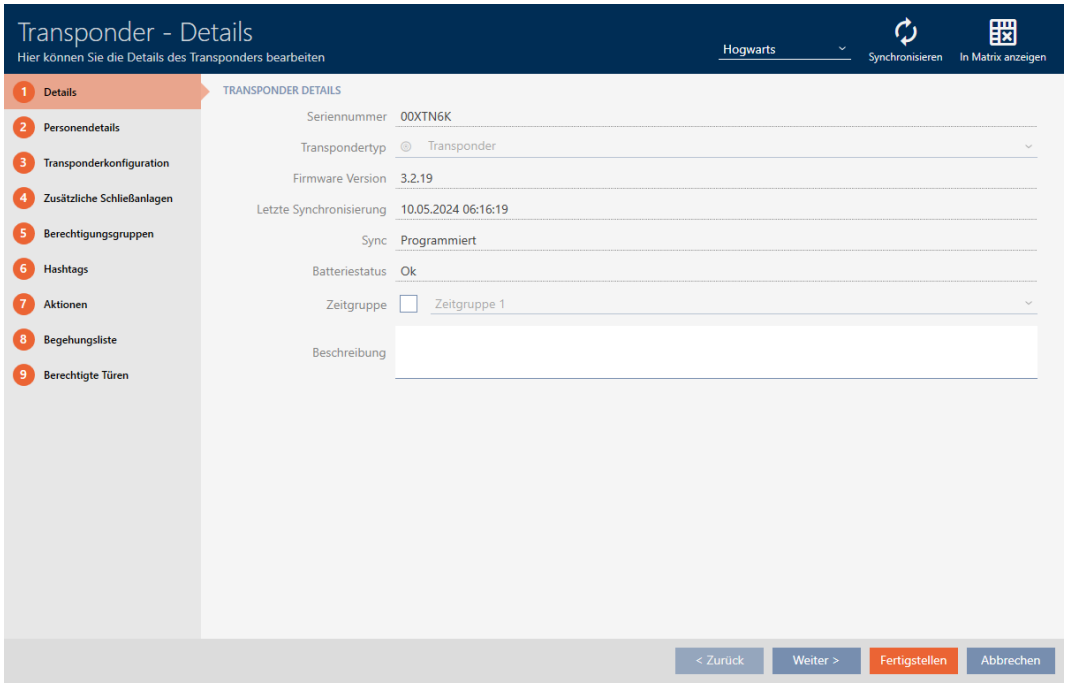
19.6.1 Transponder/Karten zurücksetzen

Bevor Sie eine Komponente wie einen Transponder wieder für ein Identmedium oder eine andere Schließanlage verwenden können, müssen Sie sie zurücksetzen.

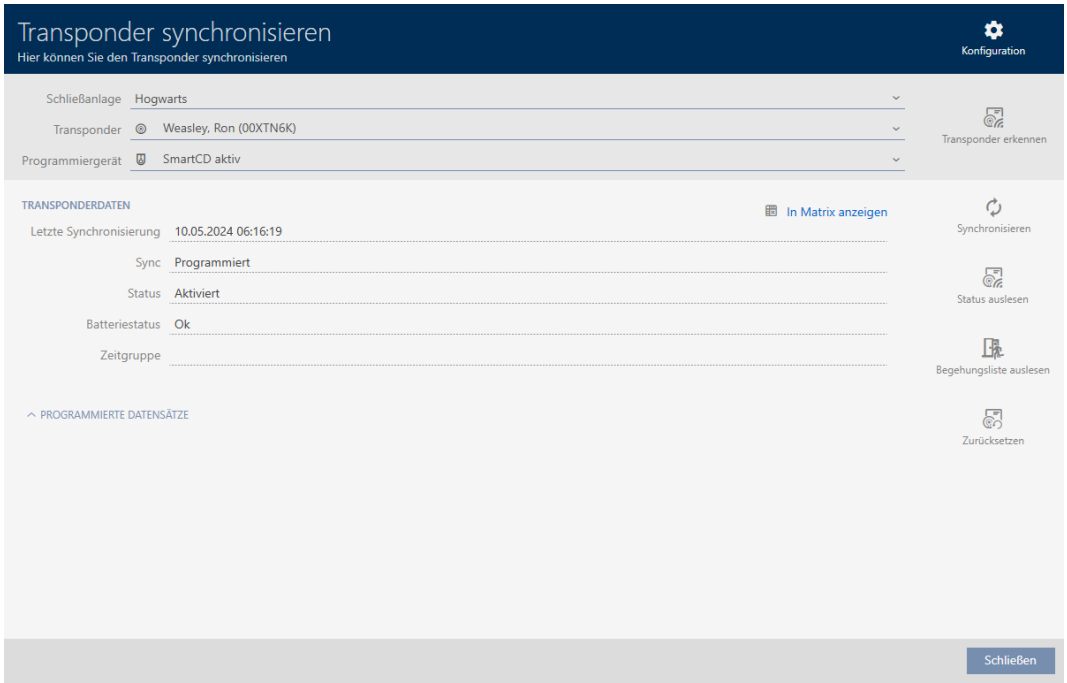
✓ Geeignetes Programmiergerät angeschlossen.

✓ Identmedienliste oder Matrixansicht geöffnet.

1. Klicken Sie auf das Identmedium, das Sie zurücksetzen wollen.
   Wenn das Identmedium nicht in Ihrer Schließanlage vorhanden ist: Identifizieren Sie das Identmedium (siehe *Unbekannte Transponder/Karten erkennen [▸ 438]*). Fahren Sie dann fort.
   ↳ Fenster des Identmediums öffnet sich.



2. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Synchronisieren-Fenster öffnet sich.



3. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihr Identmedium zurücksetzen wollen.
4. Klicken Sie auf die Schaltfläche Zurücksetzen.
5. Wählen Sie ggfs. aus, welche der vorhandenen Datensätze Sie zurücksetzen wollen.

	Pos	Schließanlage	TID	Zeitgruppennummer	Deaktivierung
☐	1	SID: 8974	3200	0	
☑	2	Hogwarts	3209	0	

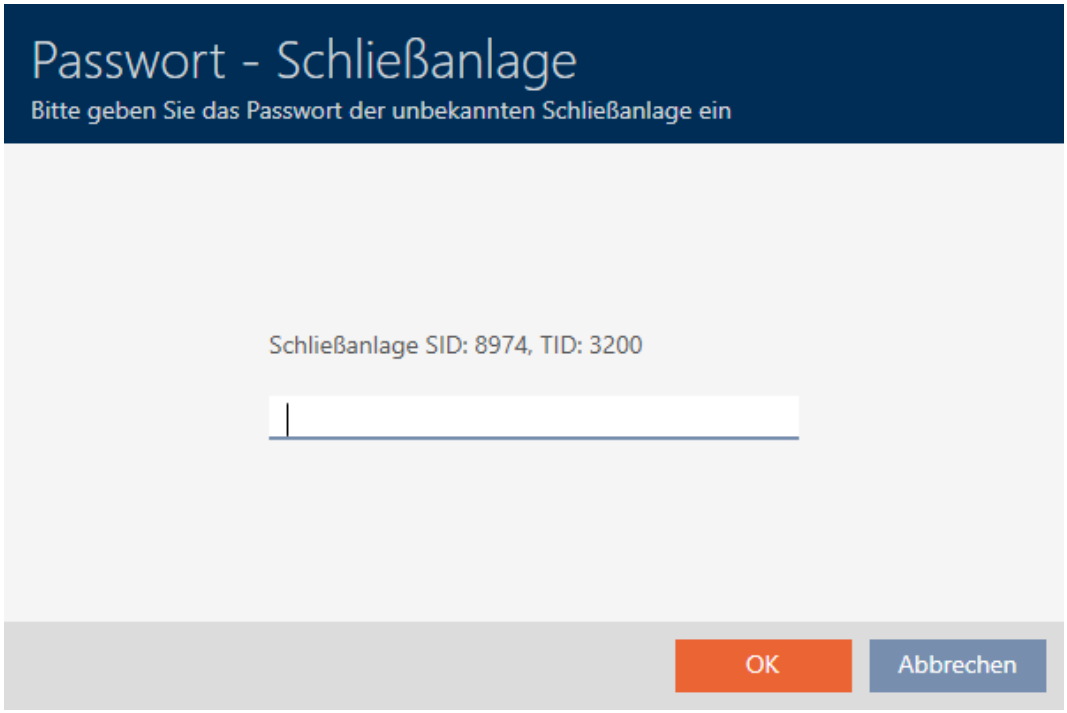
HINWEIS

Datensätze aus unbekannten Schließanlagen zurücksetzen

Wenn auf dem Identmedium ein Schließplan gespeichert ist, der nicht aus dem gleichen Projekt stammt, dann kennt Ihre AXM Plus diese Schließanlage nicht und zeigt `Unbekannt` an.

Mit der Checkbox in der Spalte "Pos" können Sie auch solche Datensätze auswählen. Da Ihre AXM Plus die Schließanlage und somit auch das Schließanlagenpasswort nicht kennt, müssen Sie in diesem Fall das Schließanlagenpasswort der unbekannten Schließanlage eingeben.

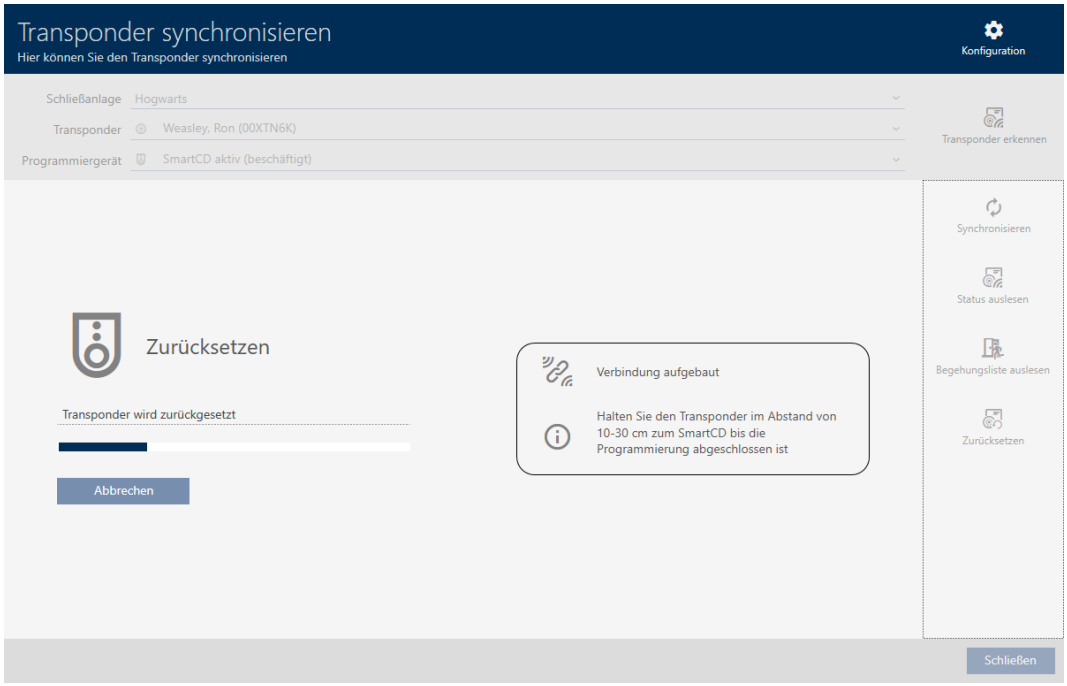
6. Geben Sie ggfs. das Schließanlagenpasswort der Schließanlage ein, zu der dieser Datensatz gehört.



↳ Checkbox am zurückzusetzenden Datensatz wird aktiviert.

	Pos	Schließanlage	TID	Zeitgruppennummer	Deaktivierung
☑	1	SID: 8974	3200	0	
☑	2	Hogwarts	3209	0	

7. Klicken Sie auf die Schaltfläche OK.
8. Folgen Sie ggfs. den weiteren Anweisungen.
   ↳ Identmedium wird zurückgesetzt.



↳ Identmedium ist zurückgesetzt.

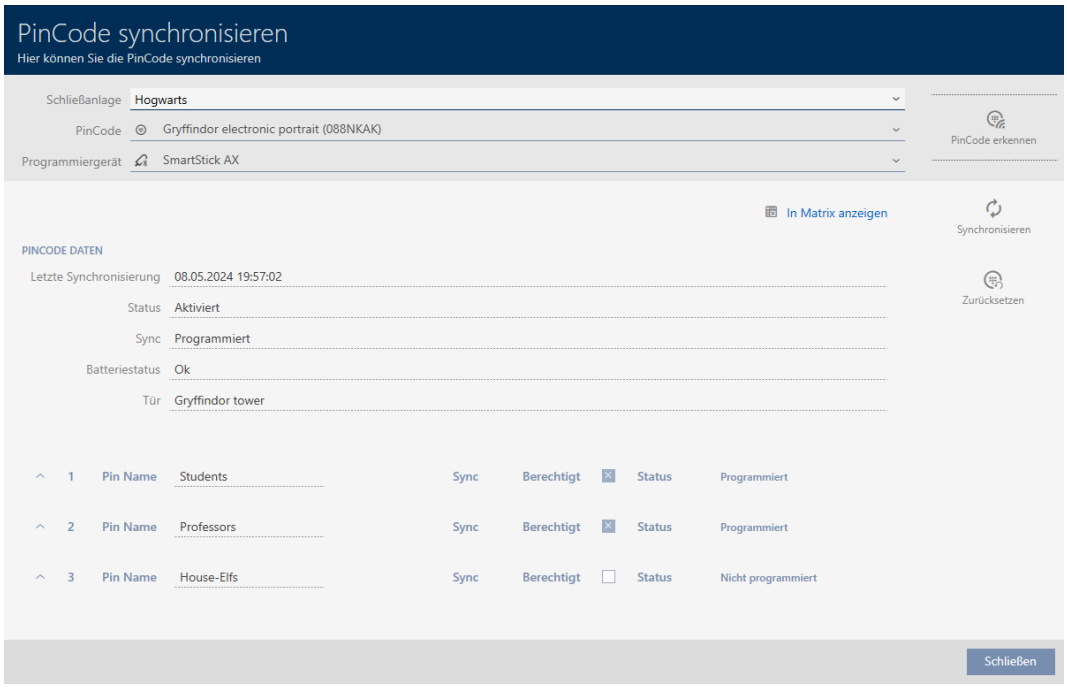
19.6.2 PinCode-Tastatur zurücksetzen

Bevor Sie eine Komponente wie eine PinCode-Tastatur wieder für ein Identmedium oder eine andere Schließanlage verwenden können, müssen Sie sie zurücksetzen.

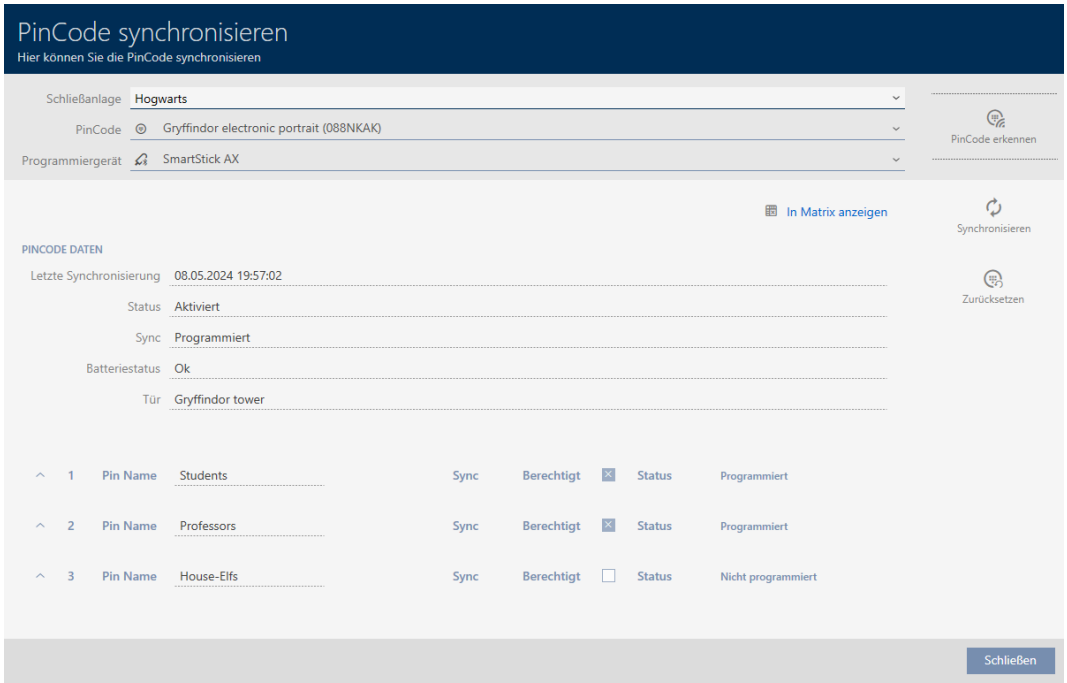
✓ Geeignetes Programmiergerät angeschlossen (SmartStick AX für PinCode-Tastatur AX, SmartCD2.G2 für PinCode-Tastatur 3068)

✓ PinCode-Liste oder Matrixansicht geöffnet.

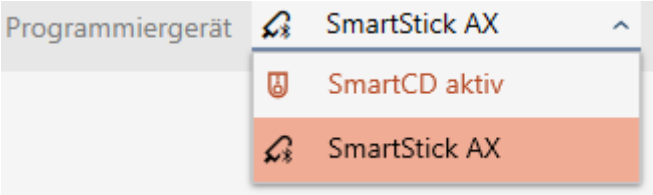
1. Klicken Sie auf die PinCode-Tastatur, die Sie zurücksetzen wollen. Wenn die PinCode-Tastatur nicht in Ihrer Schließanlage vorhanden ist: Identifizieren Sie die PinCode-Tastatur (siehe *Unbekannte PinCode-Tastatur erkennen [▸ 440]* im AXM-Handbuch). Fahren Sie dann fort.
   ↳ Fenster der PinCode-Tastatur öffnet sich.



2. Klicken Sie auf die Schaltfläche Synchronisieren.
   ↳ Synchronisieren-Fenster öffnet sich.



3. Wählen Sie im Dropdown-Menü ▼ **Programmiergerät** das Programmiergerät aus, mit dem Sie Ihre PinCode-Tastatur zurücksetzen wollen.



4. Klicken Sie auf die Schaltfläche Zurücksetzen .

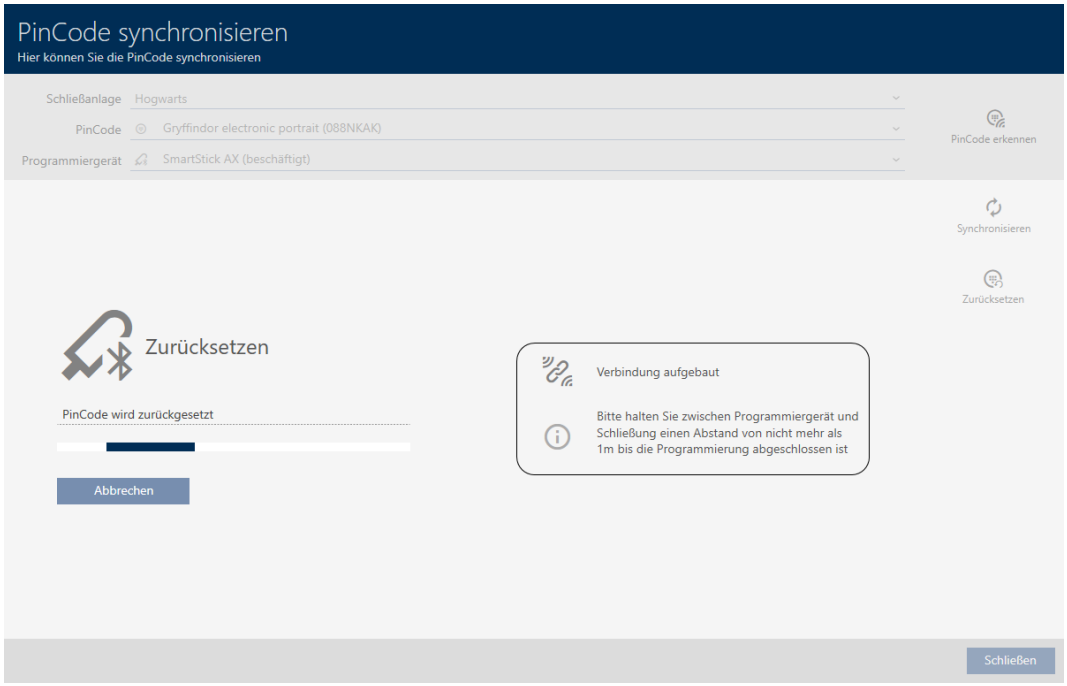
HINWEIS

Zurücksetzen von PinCode-Tastaturen, die nicht im Projekt sind

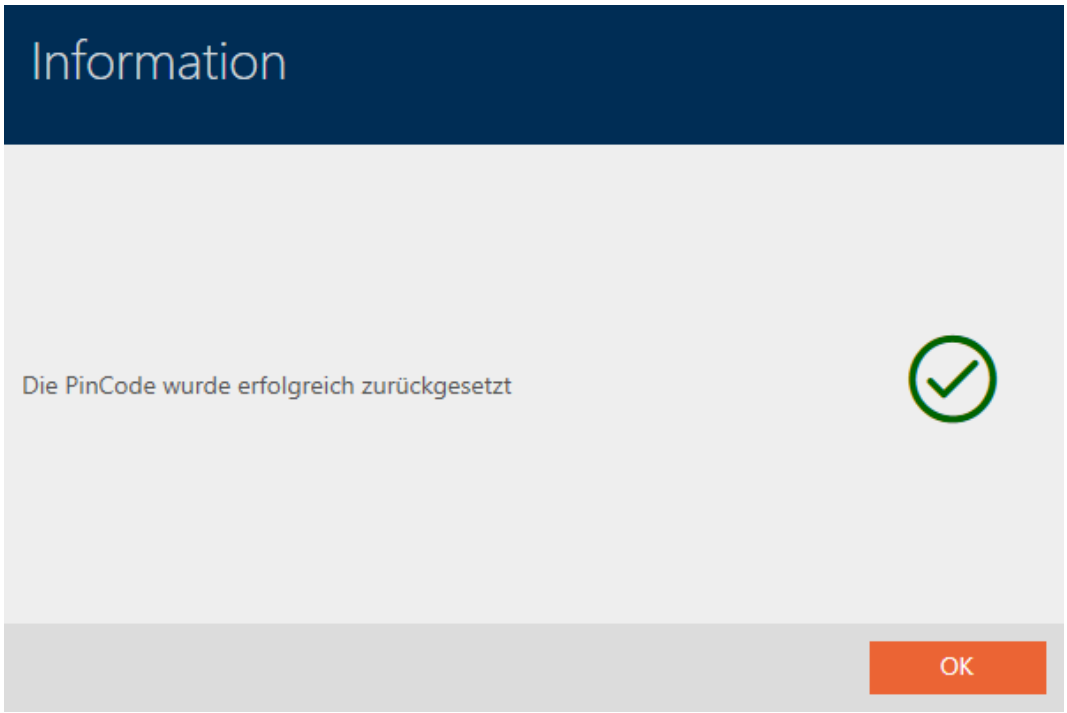
Ihre AXM Plus kann auch PinCode-Tastaturen zurücksetzen, die nicht im gleichen Projekt erstellt wurden. In diesem Fall kennt Ihre AXM Plus aber das verwendete Schließanlagenpasswort nicht.

- Geben Sie in diesem Fall nach Aufforderung das Schließanlagenpasswort ein.

5. Geben Sie ggfs. das Schließanlagenpasswort der Schließanlage ein, zu der diese PinCode-Tastatur gehört.
6. Folgen Sie ggfs. den weiteren Anweisungen.
   ↳ PinCode-Tastatur wird zurückgesetzt.



↳ PinCode-Tastatur ist zurückgesetzt.



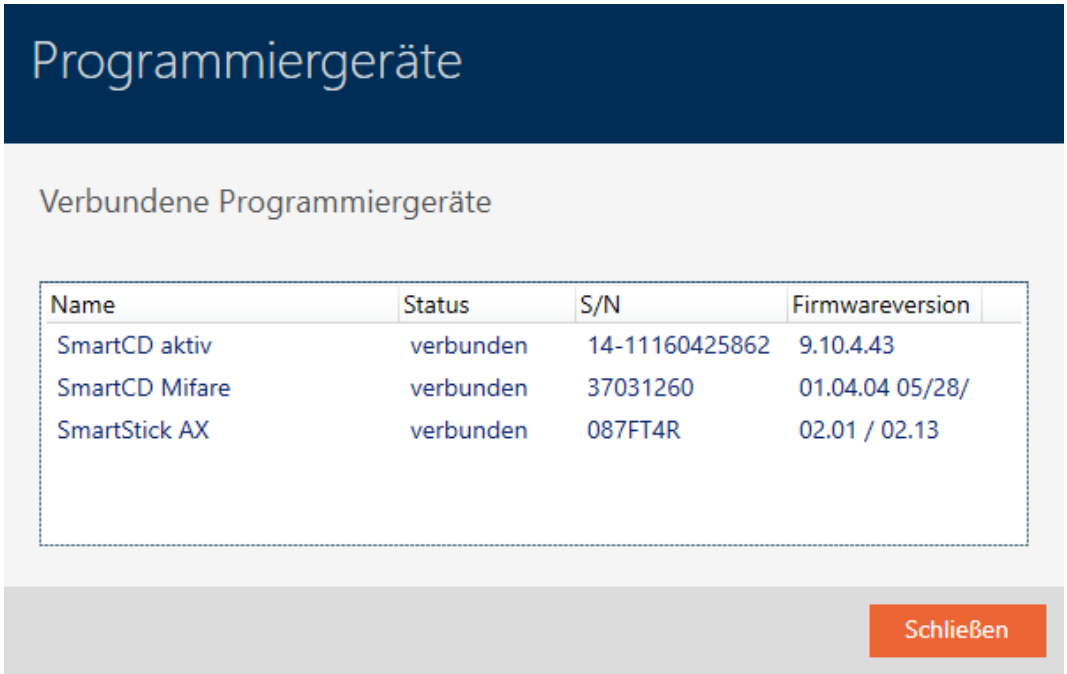
19.7 Angeschlossene/unterstützte Programmiergeräte anzeigen

Mit diesem Fenster können Sie überprüfen, ob ein angeschlossenes Programmiergerät funktionsfähig ist und erkannt wird.

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Programmiergeräte aus.

↳ Fenster mit Programmiergeräten öffnet sich.



Dieses Fenster zeigt alle unterstützten Programmiergeräte an. Je nachdem, welche Edition der AXM Sie verwenden, werden andere Programmiergeräte unterstützt (siehe Funktionsumfang AXM Lite). In der Status-Spalte sehen Sie, ob ein Programmiergerät angeschlossen ist und von der AXM Plus erkannt wird.

19.8 Verbindung zwischen Datenbank und Cloud überprüfen

Bestimmte cloudgestützte Funktionen funktionieren nur, wenn die Datenbank Ihrer AXM Plus, der AXM-Dienst und die SimonsVoss-Cloud verbunden sind.

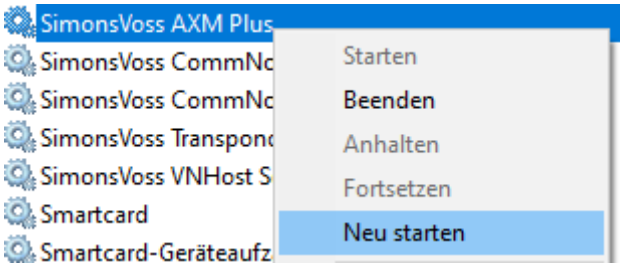
Diese Verbindung können Sie ganz einfach in der Fußleiste Ihrer AXM Plus überprüfen:

Der Eintrag Cloud Status: zeigt entweder *Ok* oder *Fehler*.

Bei *Fehler* können Sie die Verbindung erneuern, indem Sie den AXM-Dienst neu starten und Ihre AXM Plus erneut mit Ihrer SimonsVoss-ID verknüpfen:

✓ Administratorrechte vorhanden.
✓ AXM nicht geöffnet.

1. Öffnen Sie das Windows-Fenster "Dienste" mit Administratorrechten.
2. Suchen Sie den Dienst *SimonsVoss AXM Plus*.
3. Öffnen Sie mit einem Rechtsklick auf den Dienst das Kontextmenü und starten Sie den Dienst neu.

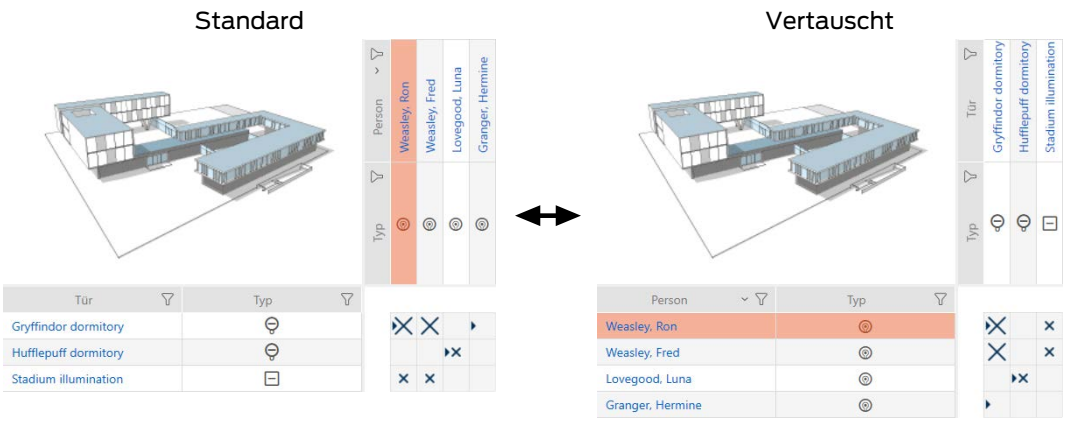


↳ *SimonsVoss AXM Plus* startet neu.

4. Starten Sie die AXM Plus und melden Sie sich am Projekt an.
5. Verbinden Sie Ihre SimonsVoss-ID erneut mit Ihrer AXM Plus (wie in *Registrierung [▸ 34]* beschrieben).
6. Prüfen Sie anschließend erneut den Eintrag bei Cloud Status:.

20. Ihre individuelle AXM-Oberfläche

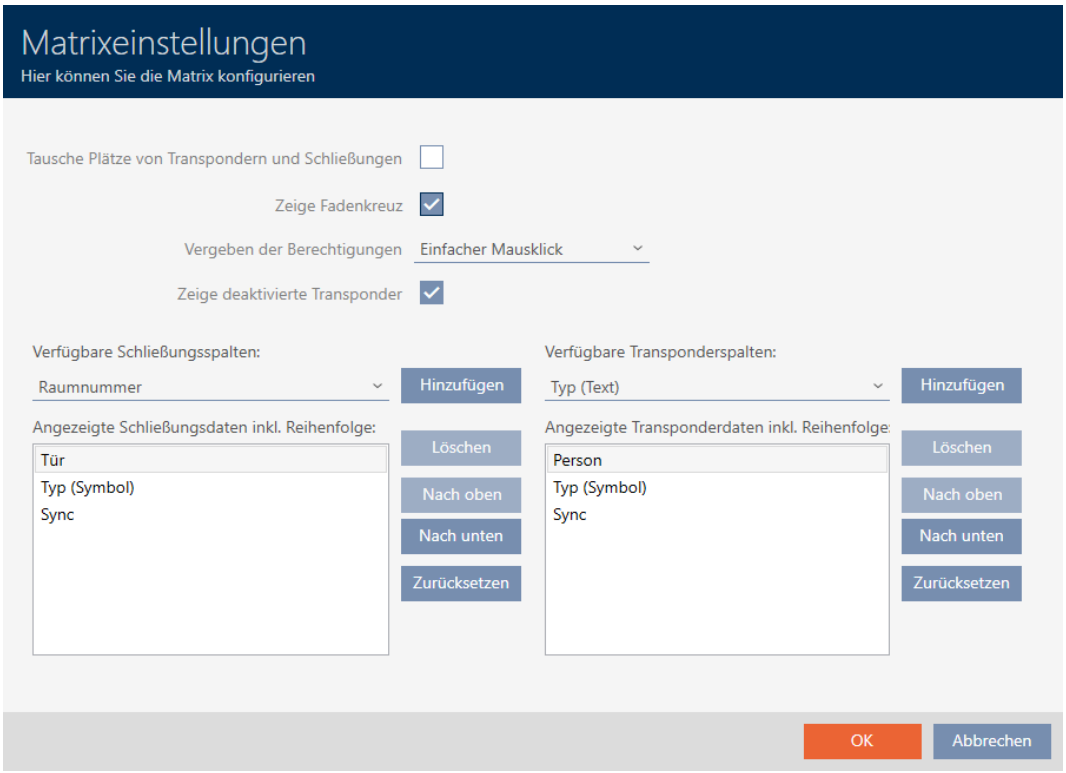
20.1 Türen und Personen in der Matrix vertauschen (transponieren)



In der Standard-Ansicht werden die Türen als Zeilen dargestellt und die Personen als Spalten. Das können Sie auch ändern.

✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Schaltfläche ⚙ Konfiguration.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus öffnet sich.



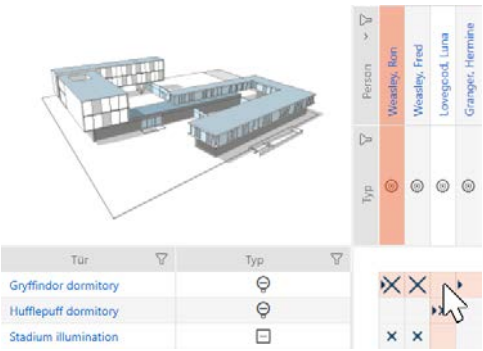
2. Aktivieren Sie die Checkbox ☑ Tausche Plätze von Transpondern und Schließungen.

3. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus schließt sich.

↳ Türen und Personen werden in der Matrixansicht getauscht.

20.2 Spalten und Zeilen in der Matrix hervorheben (Fadenkreuz aktivieren/deaktivieren)

Fadenkreuz aktiv (Standard)



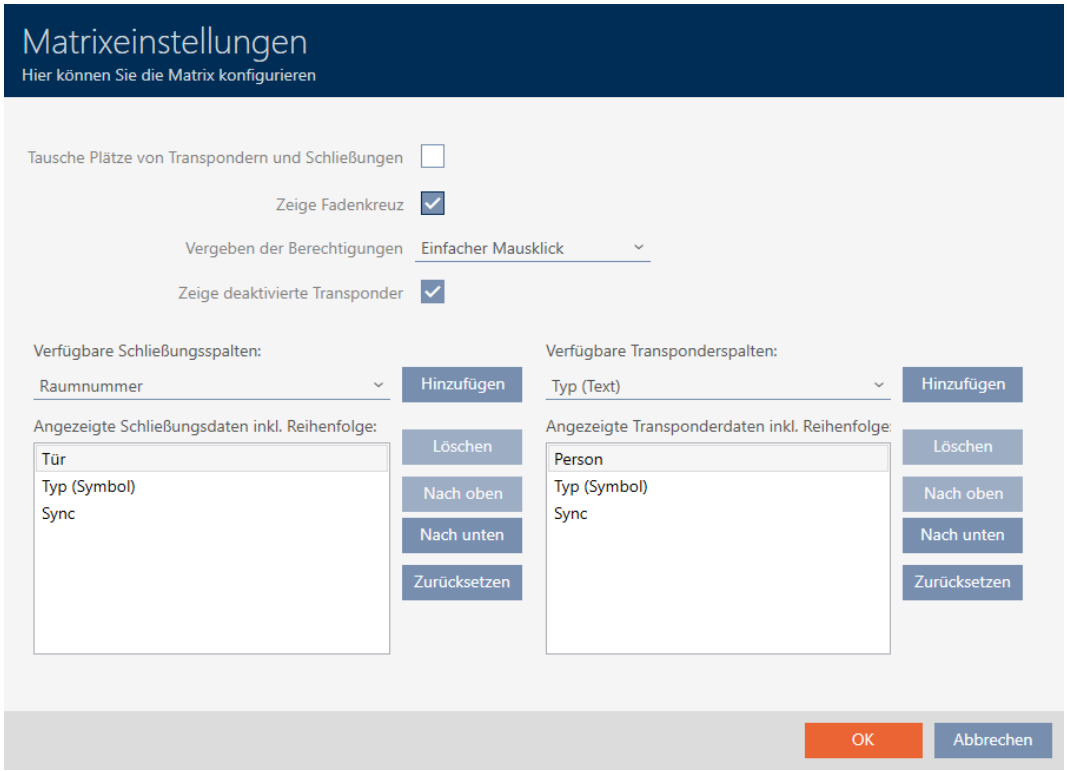
Fadenkreuz deaktiviert

Das Kästchen, über dem sich der Mauszeiger gerade befindet, gehört zu einer Schließung bzw. zu deinem Identmedium. In der Standardeinstellung wird die ganze Zeile und die ganze Spalte farbig hervorgehoben. So finden Sie schnell die entsprechende Schließung bzw. das entsprechende Identmedium. Diese Funktion heißt Fadenkreuz.

Alternativ können Sie das Fadenkreuz auch deaktivieren. In diesem Fall wird unabhängig vom Mauszeiger die Spalte bzw. die Zeile hervorgehoben, zu der die ausgewählte Schließung bzw. das ausgewählte Identmedium gehört.

✓ Matrixansicht geöffnet.

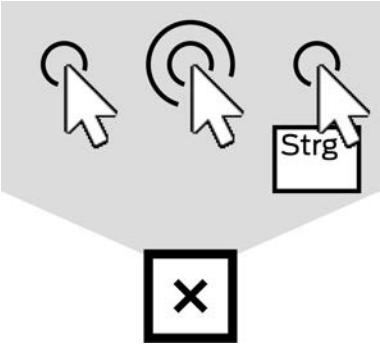
1. Klicken Sie auf die Schaltfläche ⚙ Konfiguration.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus öffnet sich.



2. Aktivieren bzw. deaktivieren Sie die Checkbox ☑ Zeige Fadenkreuz.
3. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus schließt sich.

↳ Fadenkreuz wird nicht mehr angezeigt.

20.3 Klick für Berechtigungen ändern

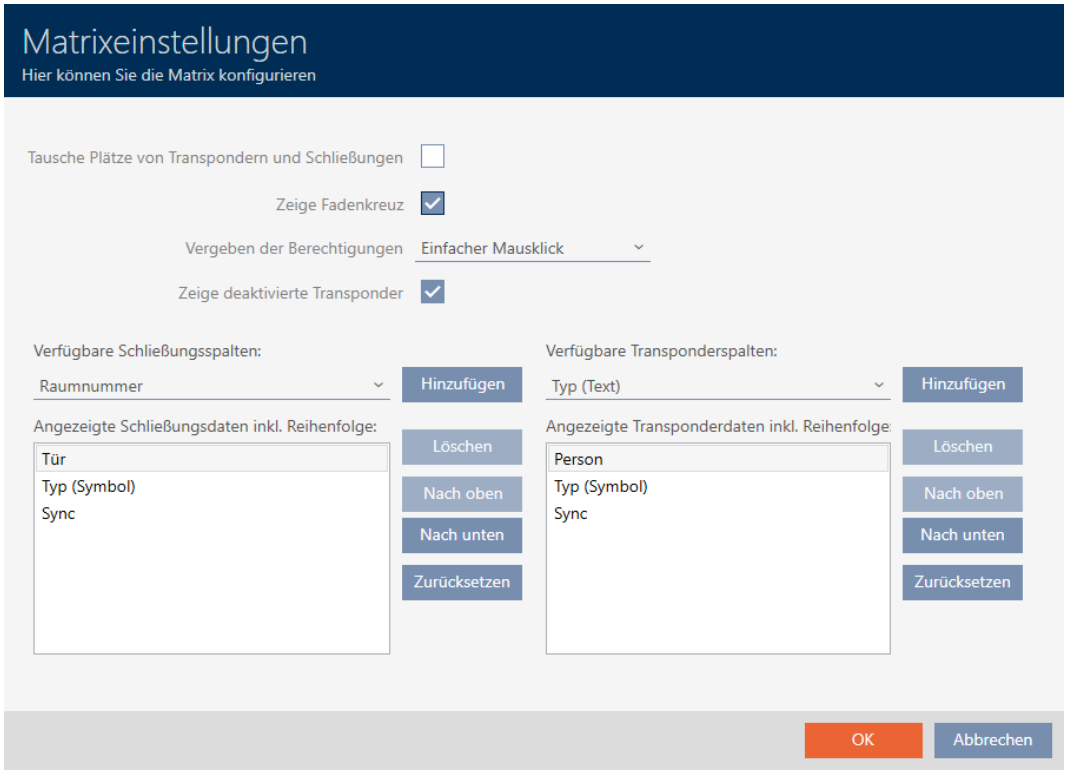


Ihnen stehen drei Möglichkeiten zur Verfügung, um eine Einzelberechtigung durch Klicken in der Matrix zu setzen:

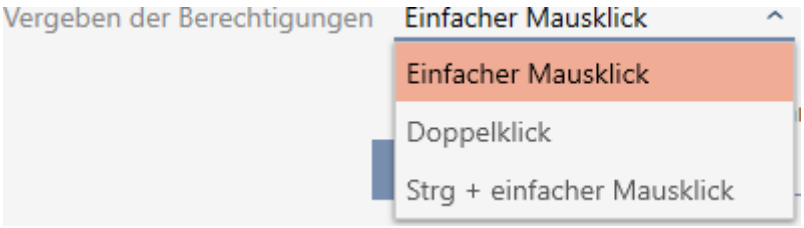
- Einfacher Mausklick (Standard)
- Doppelklick
- Strg + einfacher Mausklick

✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Schaltfläche ⚙ Konfiguration.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus öffnet sich.



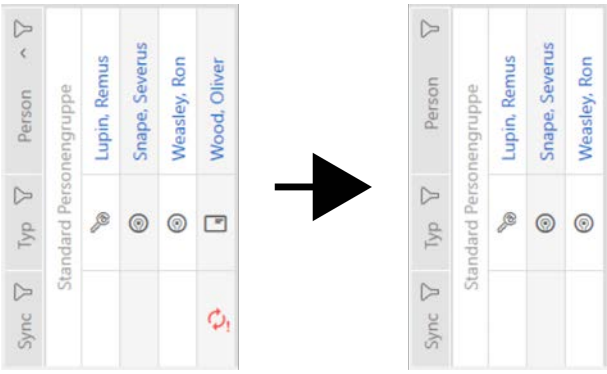
2. Wählen Sie im Dropdown-Menü ▼ **Vergeben der Berechtigungen** zwischen den Einträgen "Einfacher Mausklick", "Doppelklick" oder "Strg + einfacher Mausklick".



3. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus schließt sich.

↳ Klick für Berechtigungen ist geändert.

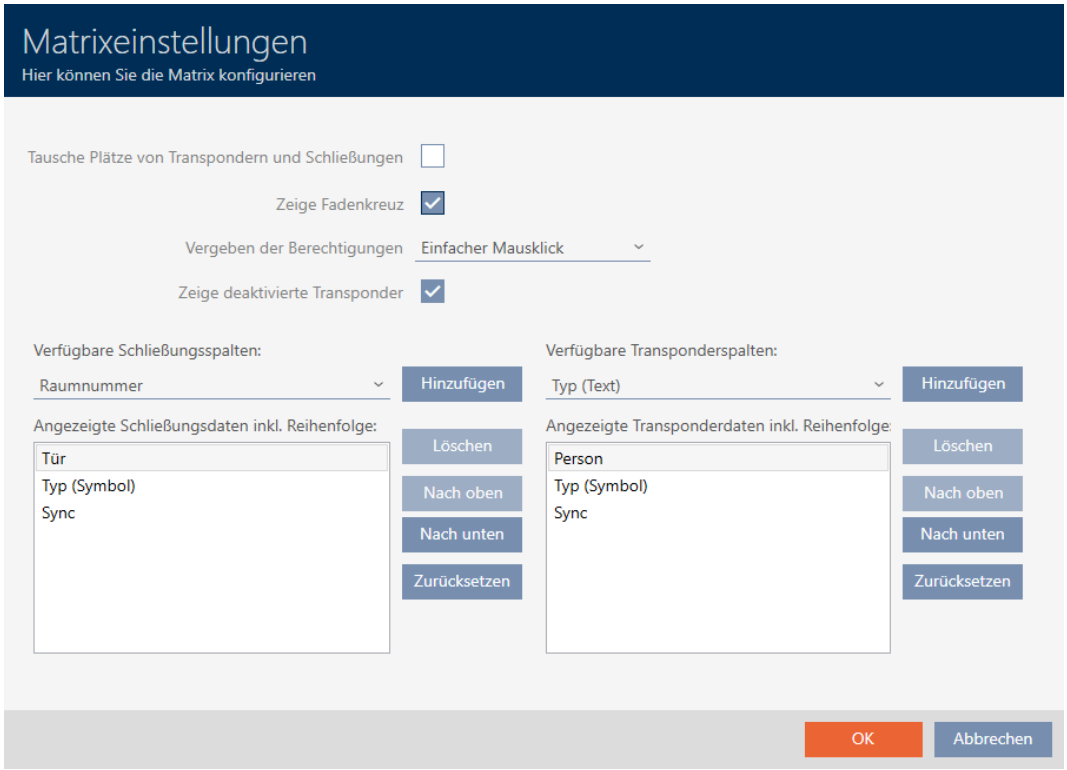
20.4 Deaktivierte und defekte Identmedien ausblenden



Hier haben Sie die Möglichkeit, Ihre Matrix "aufzuräumen" und alle defekten oder deaktivierten Identmedien auszublenden. Sie erkennen solche Identmedien am Symbol und daran, dass diese sich nicht mehr synchronisieren lassen.

✓ Matrixansicht geöffnet.

1. Klicken Sie auf die Schaltfläche Konfiguration.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus öffnet sich.

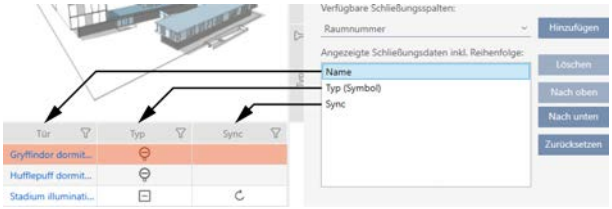


2. Deaktivieren Sie die Checkbox Zeige deaktivierte Transponder.
3. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus schließt sich.

↳ Deaktivierte und defekte Identmedien werden ausgeblendet.

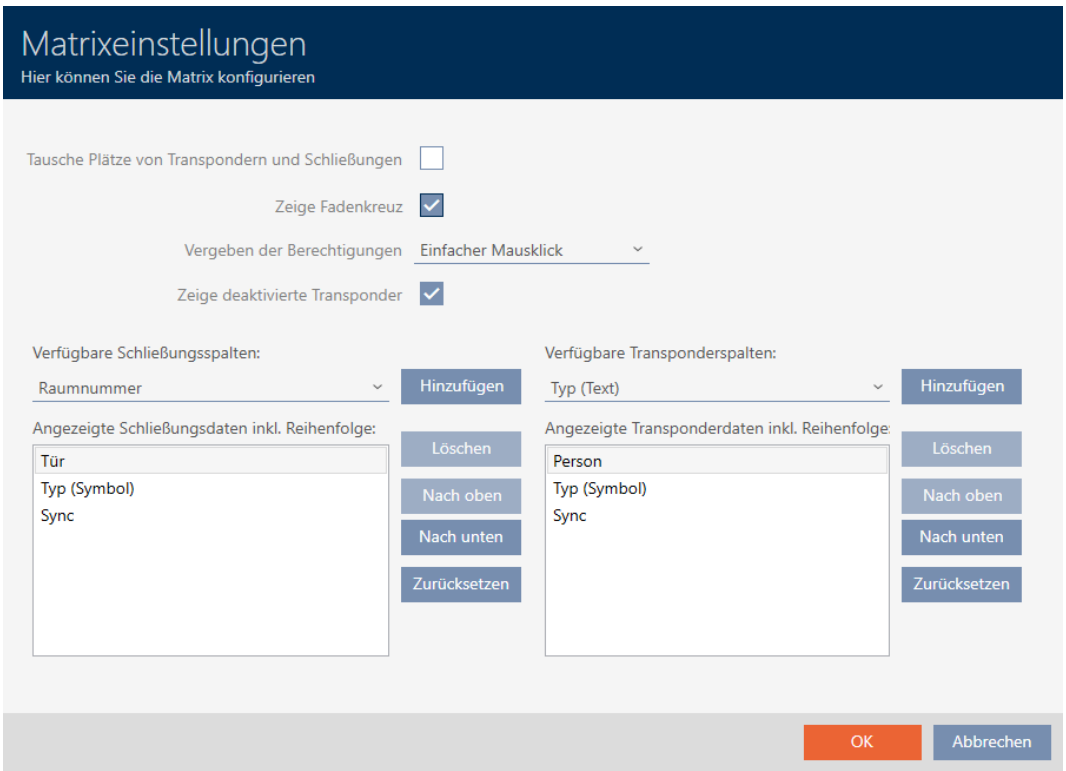
20.5 Spalten/Zeilen in der Matrix einblenden oder ausblenden

Die folgende Beschreibung gilt für die angezeigten Spalten bei Schließungen. Die Zeilen der Identmedien können analog bearbeitet werden.

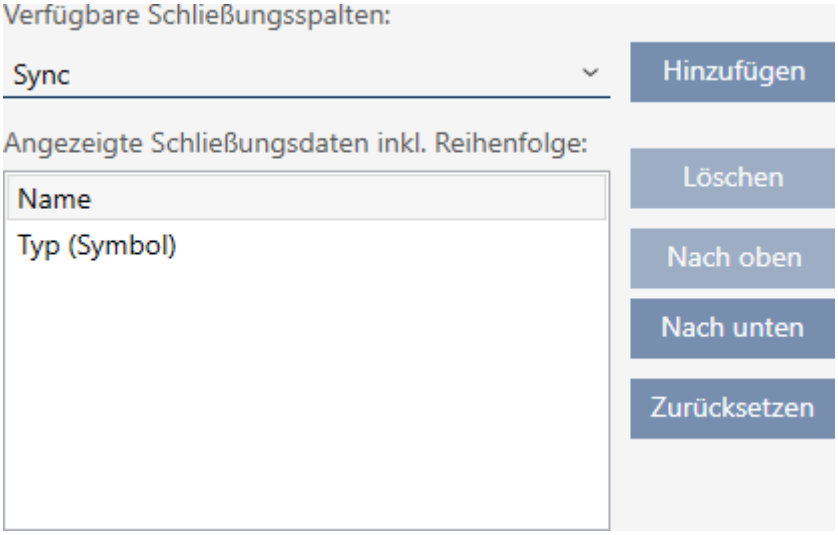


✓ Matrixansicht geöffnet.

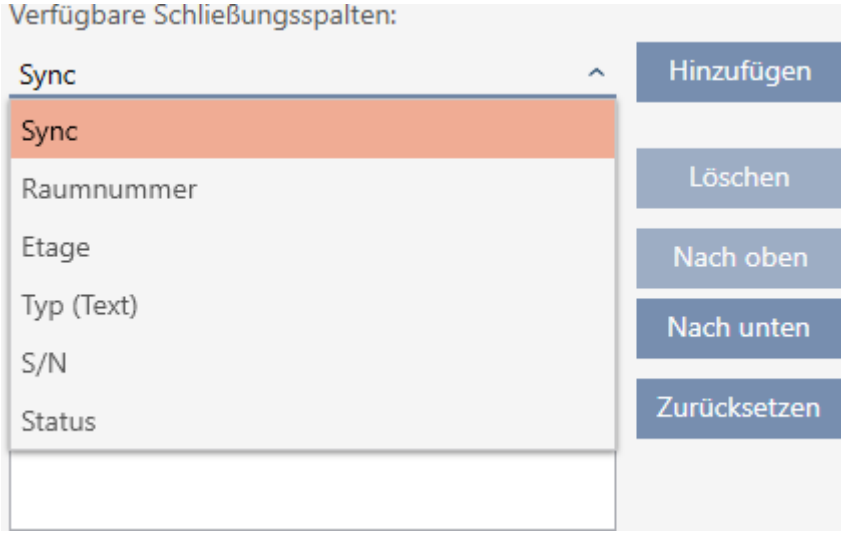
1. Klicken Sie auf die Schaltfläche ⚙ Konfiguration.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus öffnet sich.



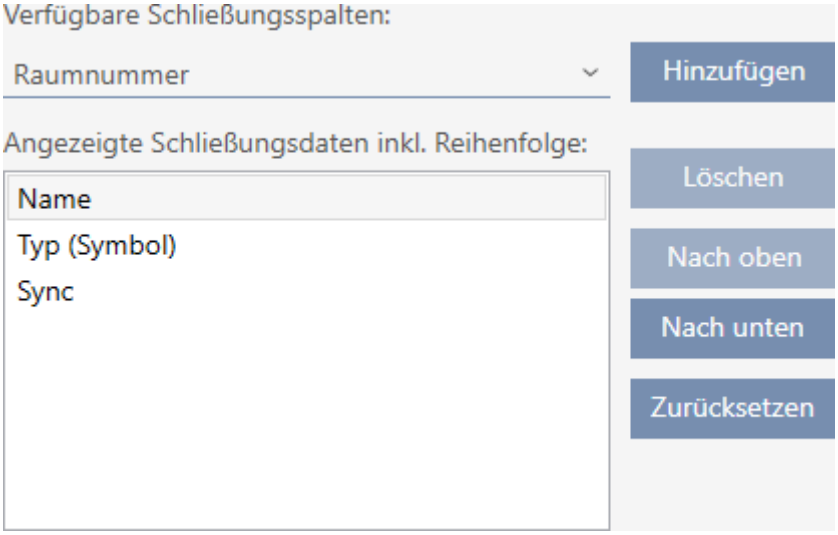
   ↳ Aktuell angezeigte Schließungsspalten werden aufgelistet.



2. Wählen Sie im Dropdown-Menü ▼ **Verfügbare Schließungsspalten:** die Spalten aus, die in der Matrix angezeigt werden sollen.



3. Ergänzen und löschen Sie Spalten mit den Schaltflächen Hinzufügen oder Löschen.



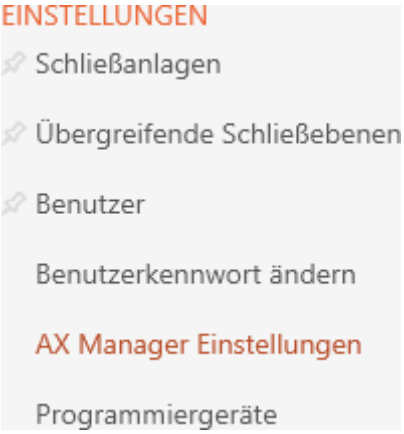
4. Ändern Sie die Reihenfolge mit den Schaltflächen Nach oben oder Nach unten.
5. Mit der Schaltfläche Zurücksetzen können Sie auch die Standard-Anzeige wiederherstellen.
6. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Matrixeinstellungen der AXM Plus schließt sich.

↳ Spalten sind wie gewünscht geändert.

20.6 Zutrittsliste/Begehungsliste während der Synchronisierung auslesen

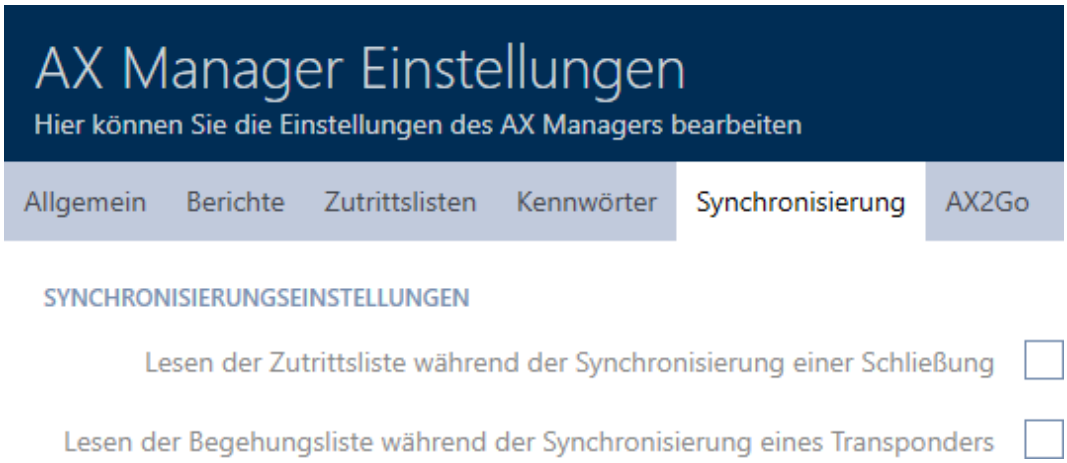
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.



   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.

3. Wechseln Sie zum Tab [Synchronisierung].



4. Aktivieren Sie ggfs. die Checkboxen ☑ Lesen der Zutrittsliste während der Synchronisierung einer Schließung oder ☑ Lesen der Begehungsliste während der Synchronisierung eines Transponders.
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

↳ Zutrittsliste bzw. Begehungsliste wird künftig bei der Synchronisierung mit ausgelesen.

20.7 Anzahl der Einträge der Zutrittsliste in der Datenbank begrenzen

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.

   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.
3. Wechseln Sie zum Tab [Zutrittslisten].

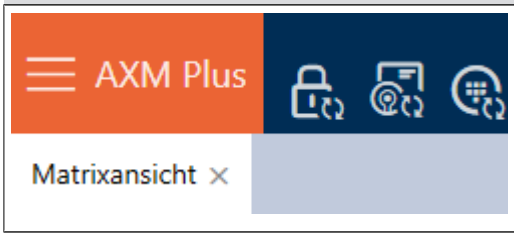
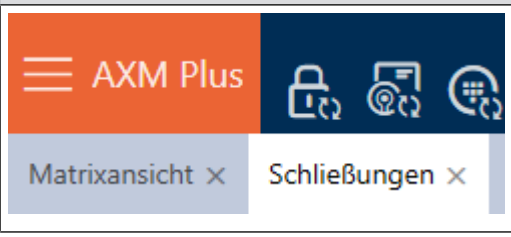
4. Wählen Sie eine der drei Optionen ◉ unbegrenzt, ◉ zeitlich (max. 2000 Tage) oder ◉ nach Anzahl (max. 10.000 Einträge).
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

↳ Zutrittslistenbegrenzung ist eingestellt.

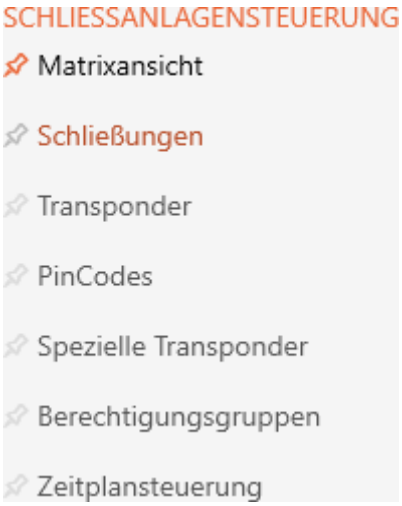
20.8 Tabs pinnen

Erfahrungsgemäß werden Sie feststellen, dass Sie einige Einträge aus der AXM-Leiste häufiger brauchen.

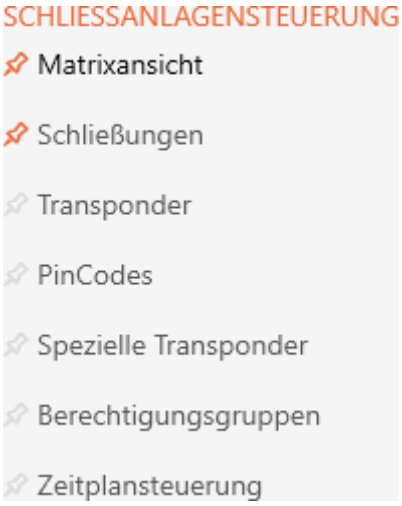
Neben einigen Einträgen sehen Sie eine graue Pinnadel. Mit dieser Pinnadel können Sie den entsprechenden Eintrag pinnen und beim nächsten Start der AXM Plus automatisch öffnen.

Start (Eintrag Schließungen nicht gepinnt)	Start (Eintrag Schließungen gepinnt)
	

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.
2. Klicken Sie auf die graue Pinnadel neben dem Eintrag, den Sie pinnen wollen.



   ↳ Pinnadel wird orange.



↳ Gepinnter Eintrag wird beim nächsten Start der AXM Plus automatisch geöffnet.

20.9 Automatische Nummerierung ändern

Die AXM Plus übernimmt standardmäßig die Nummerierung von Personal und Türen für Sie.

Personalnummern	Türnummern
PERSONENDETAILS Nachname Weasley Vorname Ron Personalnummer PN-1	TÜRDETAILS Name Gryffindor dormitory Tür-Code DC-00001
PN-1	**DC-**00001
PN-2	**DC-**00002
PN-X	**DC-**XXXXX

Die Kürzel *PN*- (Personal Number) und *DC*- (Door Code) können in den Eigenschaften der AXM Plus geändert werden:

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.

   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.
3. Wechseln Sie zum Tab [Allgemein].

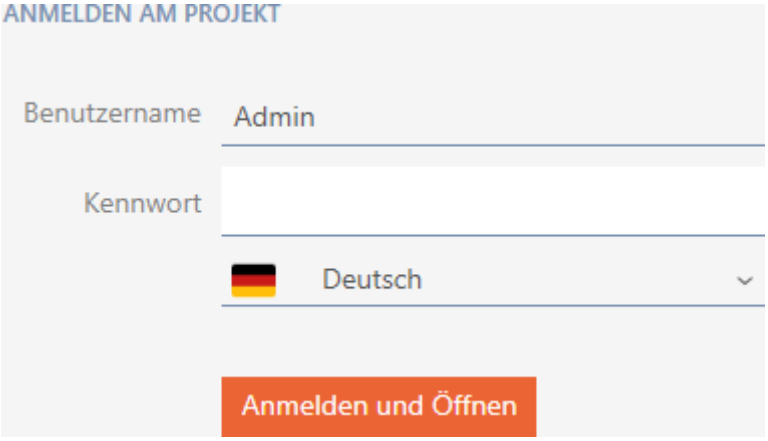
4. Geben Sie in die Felder *Personalnummer* bzw. *Tür-Code* die gewünschten Kürzel ein.
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

↳ Personalnummern und Tür-Codes werden zukünftig mit dem geänderten Kürzel erzeugt.
↳ Bereits bestehende Personalnummern oder Tür-Codes bleiben unverändert.

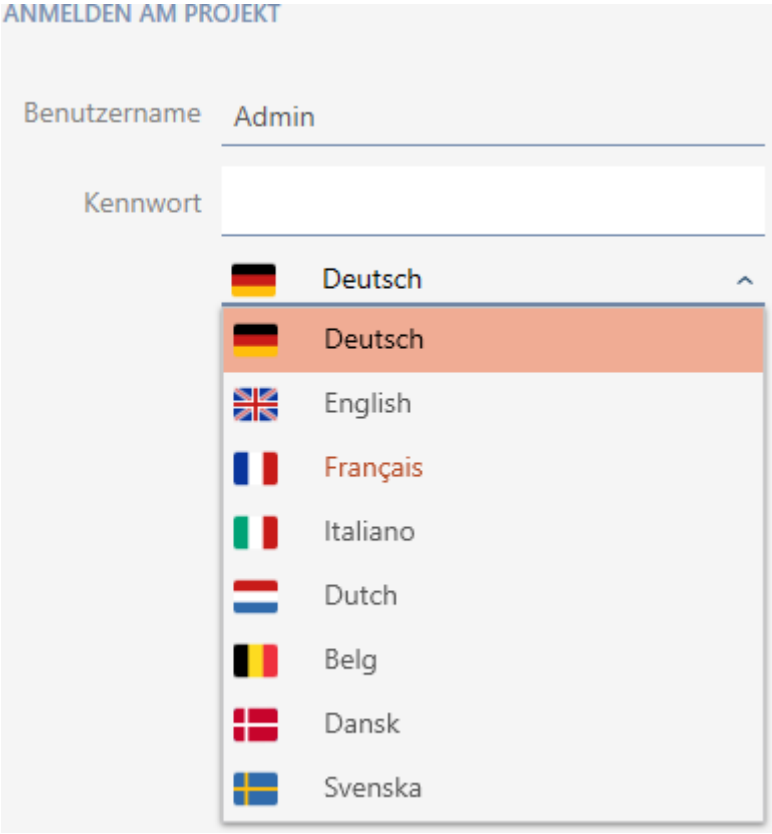
20.10 Sprache ändern

Die AXM Plus ist in verschiedenen Sprachen verfügbar. Bei der Installation werden automatisch alle verfügbaren Sprachen mitinstalliert.

Beim ersten Start sehen Sie ein spezielles Fenster, in dem Sie Ihr erstes Projekt einrichten können. Danach erscheint das normale Anmeldefenster:



Wählen Sie hier unter dem Feld *Kennwort* Ihre bevorzugte Sprache aus.



20.11 Berichte und Exporte personalisieren

In der AXM Plus können Sie Ihre Berichte und Exporte personalisieren:

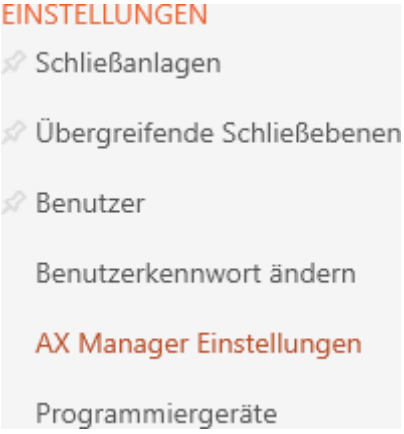
- Logo für Kopfzeile

  - Zulässige Formate: .bmp, .jpg, .png
  - Automatische Skalierung (Rahmenformat: 25:10,5, siehe auch *Skalierung der Bilddateien [▸ 572]*)
- Angaben für die Kopfzeile
  - Unternehmen
  - Straße
  - PLZ, Ort
  - Telefon
  - E-Mail
  - Kontakt
- Logo für Fußzeile (Rahmenformat: 3:1, siehe auch *Skalierung der Bilddateien [▸ 572]*)
  - Zulässige Formate: .bmp, .jpg, .png

Diese Angaben werden zugunsten eines einheitlichen Erscheinungsbilds global für alle Berichte übernommen.

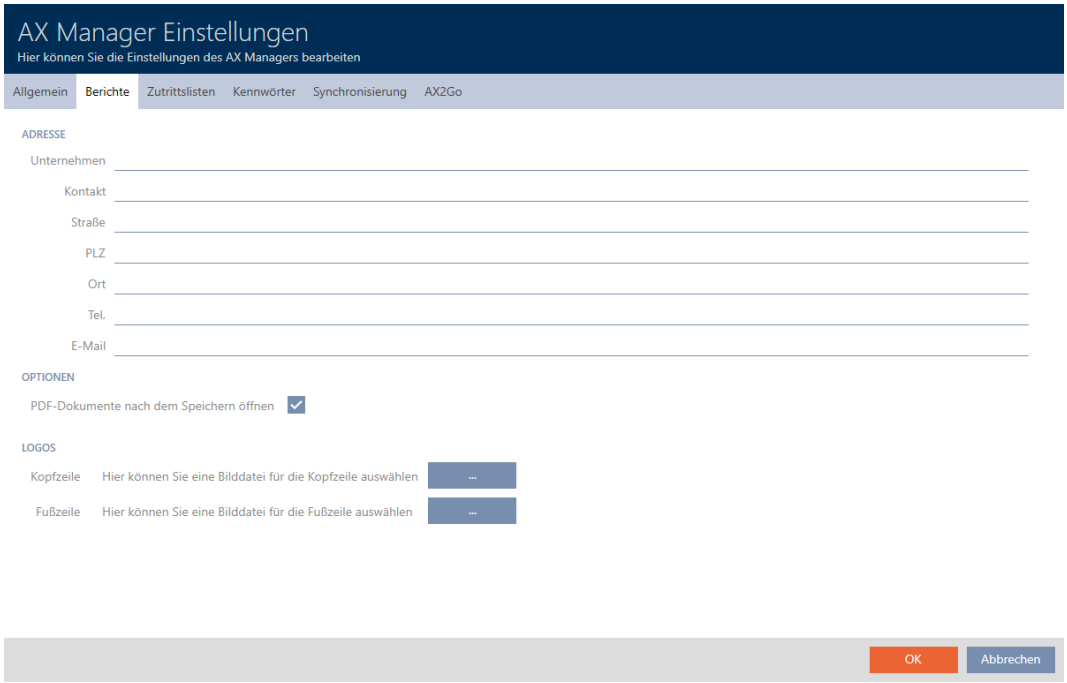
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.



↳ AXM-Leiste klappt zu.
↳ Fenster "AX Manager Einstellungen" öffnet sich.

3. Wechseln Sie zur Registerkarte [Berichte].



4. Füllen Sie die Felder im Bereich "Adresse" aus.
   ↳ Nicht befüllte Felder werden im Bericht ausgeblendet.
5. Klicken Sie im Bereich "Logos" auf die Schaltfläche ...
   ↳ Explorer-Fenster öffnet sich.
6. Wählen Sie eine geeignete Bilddatei für die Kopfzeile bzw. Fußzeile aus.
   ↳ Explorer-Fenster schließt sich.
   ↳ Ausgewählte Bilddateien werden im Bereich "Logos" angezeigt.

7. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "AX Manager Einstellungen" schließt sich.

↳ Berichte werden zukünftig mit Ihren eigenen Angaben und Logos ausgegeben.

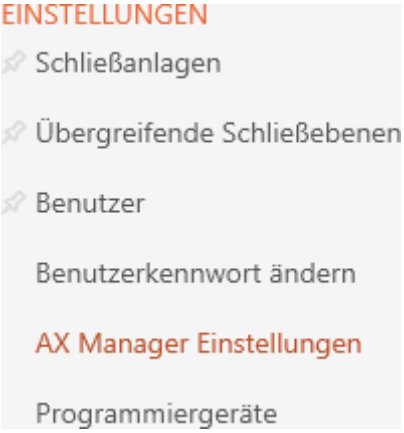
20.12 Erzeugte Berichte nicht automatisch öffnen

Standardmäßig öffnet Ihre AXM Plus erstellte Berichte sofort, damit Sie sie lesen können.

Bei vielen Berichten kann dies aber Ihren Arbeitsfluss stören. Deshalb können Sie einstellen, ob Berichte automatisch geöffnet werden sollen:

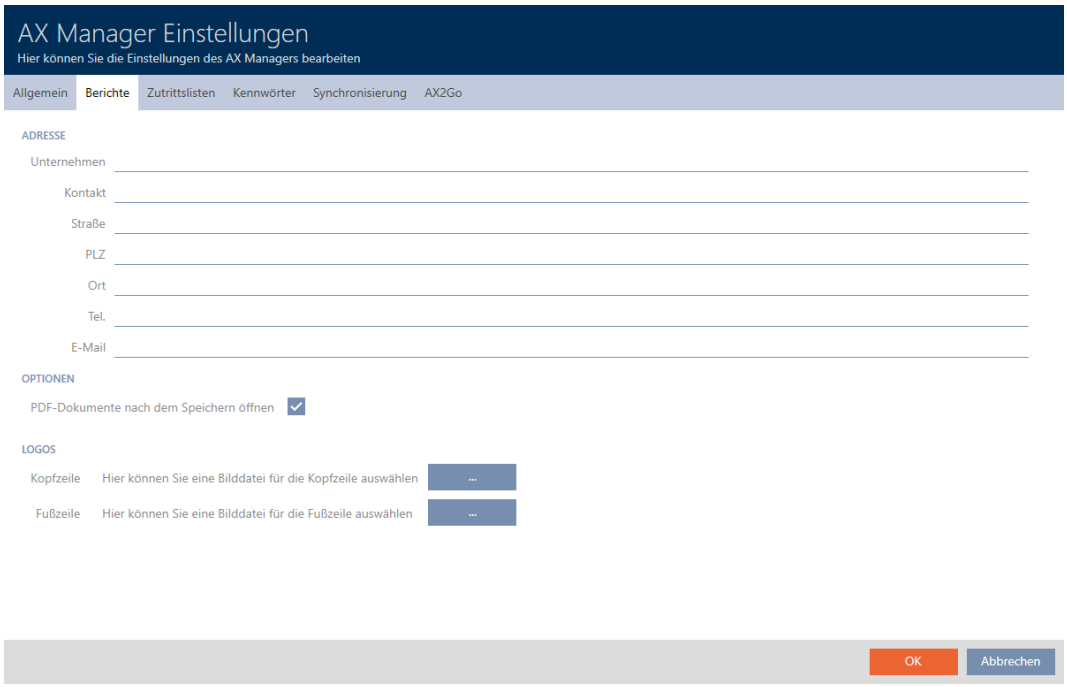
1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.



   ↳ AXM-Leiste klappt zu.
   ↳ Fenster "AX Manager Einstellungen" öffnet sich.

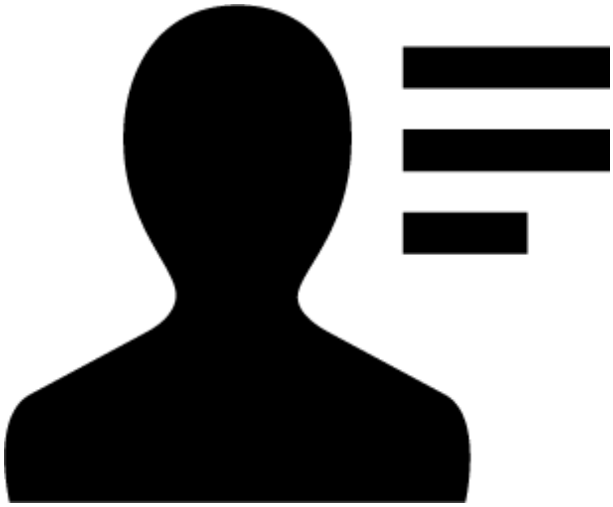
3. Wechseln Sie zur Registerkarte [Berichte].



4. Deaktivieren Sie die Checkbox ☐ PDF-Dokumente nach dem Speichern öffnen.
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster "AX Manager Einstellungen" schließt sich.

↳ Berichte werden künftig nach dem Speichern nicht mehr automatisch geöffnet.

20.13 Eigenschaften für Personendetails personalisieren



Vielleicht sind die Standard-Eigenschaften, die die AXM Plus für Personen und Schließungen mitbringt, für Ihren Anwendungsfall nicht passend.

Zum Beispiel hätten Sie gerne statt des Standard-Felds *Titel* eine Büronummer.

Hier gibt Ihnen die AXM Plus die Freiheit, selbst zu entscheiden, mit welchen Eigenschaften Sie arbeiten wollen:

- Blenden Sie nicht benötigte Eigenschaften einfach aus. Später können Sie die Eigenschaften jederzeit wieder einblenden (siehe *Vorhandene Felder ausblenden und einblenden [▸ 470]*).

  Im Beispiel blenden Sie das Standard-Feld *Titel* aus.
- Erstellen Sie eigene Eigenschaften (siehe *Eigene Felder anlegen [▸ 475]*).

  Im Beispiel erstellen Sie ein eigenes Feld namens Büronummer.

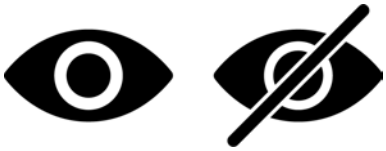
HINWEIS

Versehentliche Bearbeitung von projektweit eingestellten Eigenschaftenn

Die Personalisierung von Eigenschaften gilt für alle Schließanlagen innerhalb des gleichen Projekts. Zum Beispiel wird eine Eigenschaft, die Sie innerhalb einer Schließanlage löschen, auch in allen anderen Schließanlagen gelöscht.

- Überlegen Sie vor der Bearbeitung, ob Sie die Eigenschaften auch in allen anderen Schließanlagen mitbearbeiten wollen.

20.13.1 Vorhandene Felder ausblenden und einblenden



Die AXM Plus enthält standardmäßig folgende Felder:

Personendetails

☑ Titel	☑ Eingestellt bis	☑ Abteilung
☑ Adresse	☑ Geburtstag	☑ E-Mail
☑ Ort/Gebäude	☑ Kostenstelle	☑ Telefon
☑ Eingestellt am	☑ Foto	

Davon können Sie folgende Felder ausblenden und wieder einblenden:

- Titel

- Adresse
- Ort/Gebäude
- Eingestellt am
- Eingestellt bis
- Geburtstag
- Kostenstelle
- Foto
- Abteilung

Folgende Felder sind fixiert:

- E-Mail
- Telefon

HINWEIS

Ausblenden löscht Inhalt nicht

Wenn Sie ein Feld nur ausblenden, dann bleibt der Inhalt des Felds in der Datenbank erhalten. Sobald das Feld wieder eingeblendet wird, wird der Inhalt wiederhergestellt.

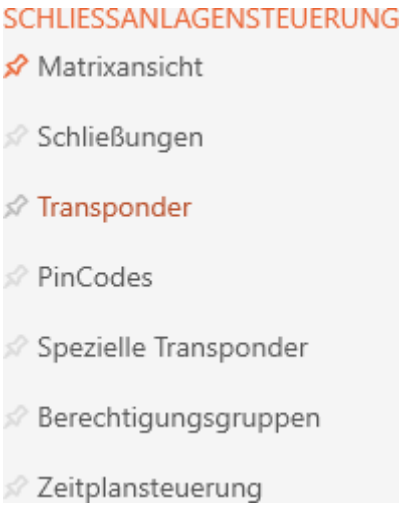
Ausgeblendete Felder mit Inhalt werden weiterhin für Berichte verwendet. So ist sichergestellt, dass z.B. beim DSGVO-Bericht (siehe *Datenschutzbericht (DSGVO) ausgeben [▸ 527]*) wirklich alle gespeicherten Daten ausgegeben werden.

1. Verwenden Sie die Ausblenden-Funktion nicht, wenn Sie Daten tatsächlich löschen wollen.
2. Löschen Sie stattdessen den Inhalt des einzelnen Felds oder die ganze Person bzw. deren Identmedium (siehe *Transponder/Karte löschen [▸ 115]*).

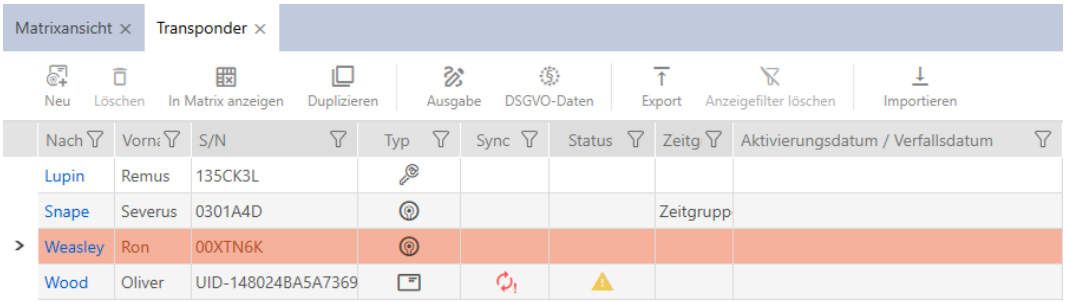
✓ Identmedium vorhanden.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

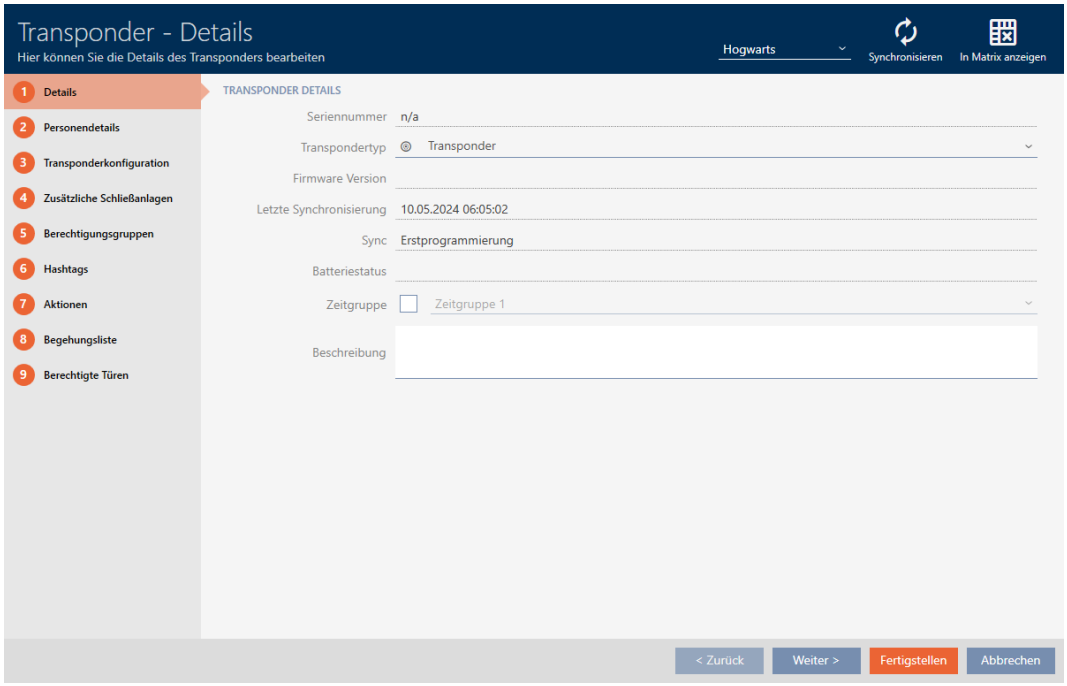
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.



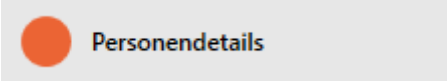
↳ AXM-Leiste klappt zu.
↳ Fenster mit Identmedien öffnet sich.



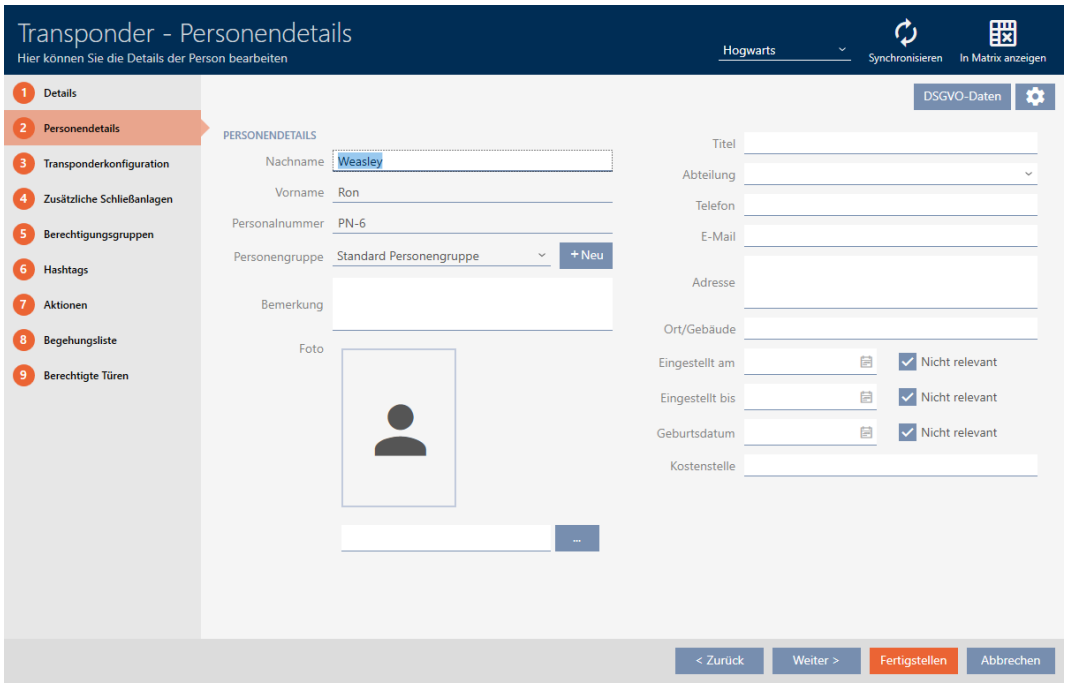
3. Klicken Sie auf ein beliebiges nicht gesperrtes/deaktiviertes Identmedium.
↳ Fenster des Identmediums öffnet sich.



4. Klicken Sie auf den Reiter Personendetails.

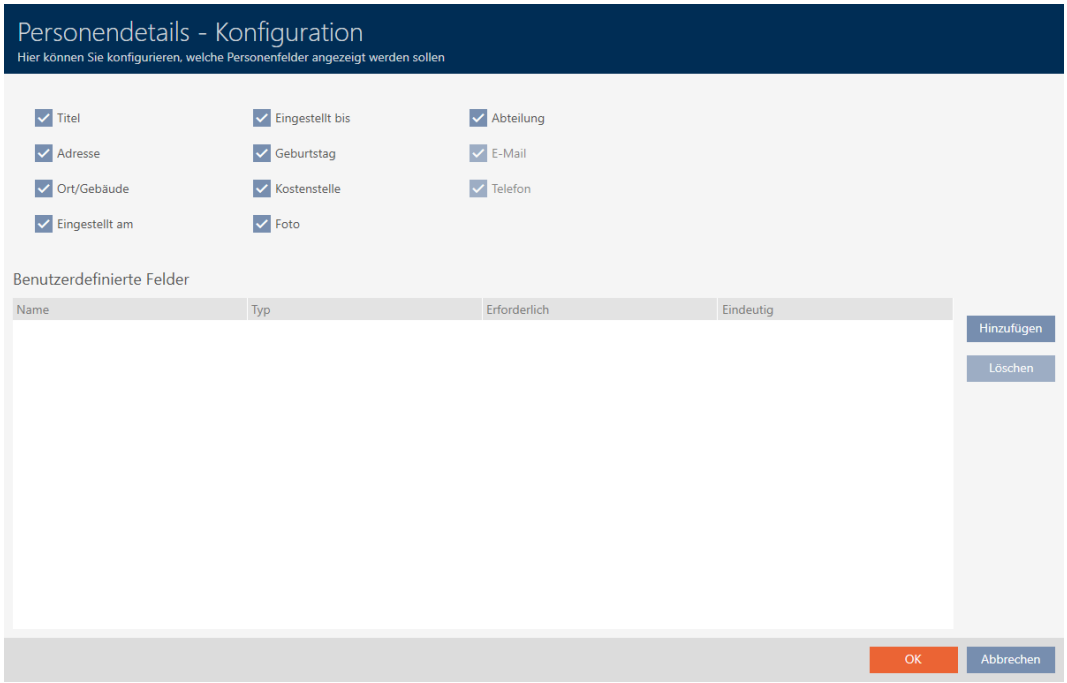


↳ Fenster wechselt zum Reiter "Personendetails".

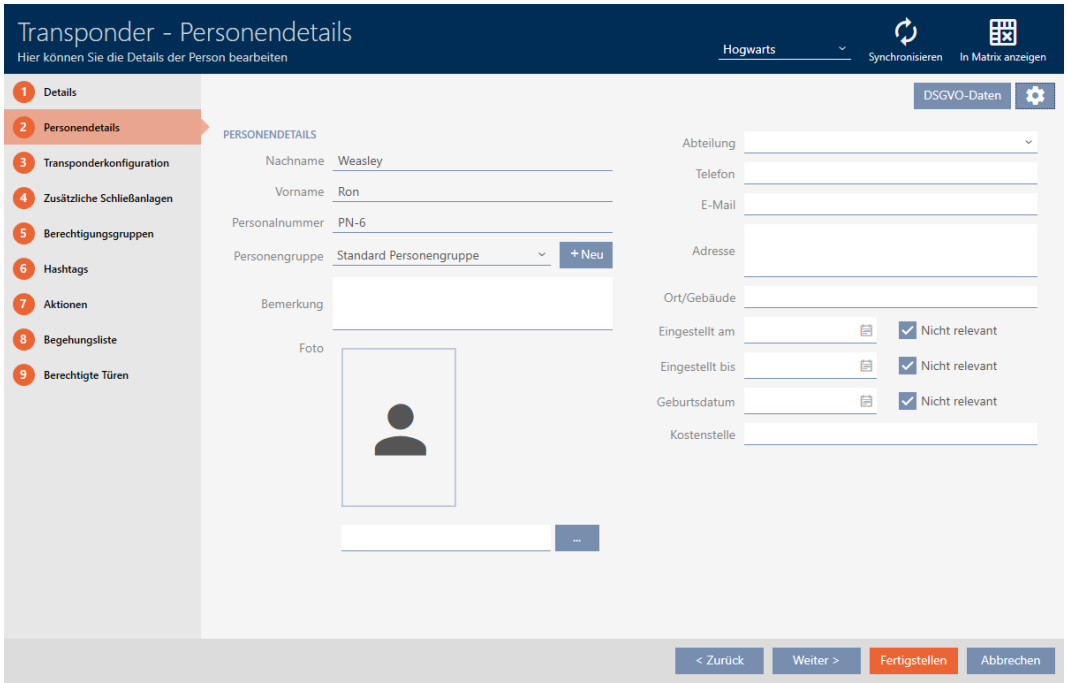


5. Klicken Sie auf die Konfigurations-Schaltfläche ⚙.

6. Fenster "Konfiguration" öffnet sich.



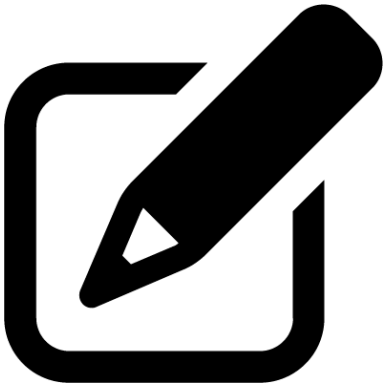
7. Aktivieren bzw. deaktivieren Sie die gewünschten Felder (Beispiel: Deaktivieren Sie die Checkbox ☐ Titel).
8. Klicken Sie auf die Schaltfläche OK.
9. Fenster "Konfiguration" schließt sich.
   ↳ Das Fenster des Identmediums zeigt im Reiter "Personendetails" die geänderten Felder an (Beispiel: Das Feld *Titel* fehlt).



10. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ Felder sind in allen Schließanlagen des gleichen Projekts ein- bzw. ausgeblendet.

20.13.2 Eigene Felder anlegen



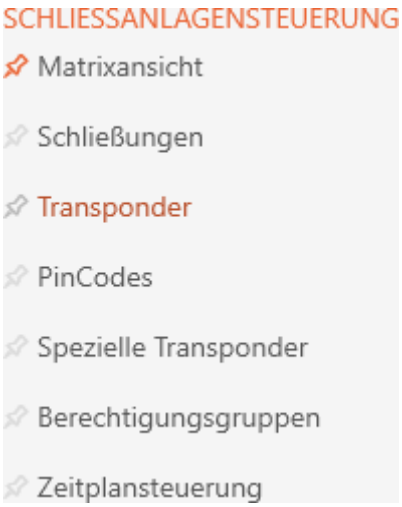
In manchen Fällen brauchen Sie andere oder zusätzliche Felder als die, die Ihre AXM Plus zur Verfügung stellt. Zusätzliche Felder für Personeneigenschaften werden auch im DSGVO-Bericht ausgegeben (siehe *Datenschutzbericht (DSGVO) ausgeben [▸ 527]*).

Deshalb können Sie auch eigene Felder erstellen (weitere Informationen zu den Eigenschaften Ihrer eigenen Felder siehe *Nachträglich geänderte benutzerdefinierte Felder [▸ 481]*):

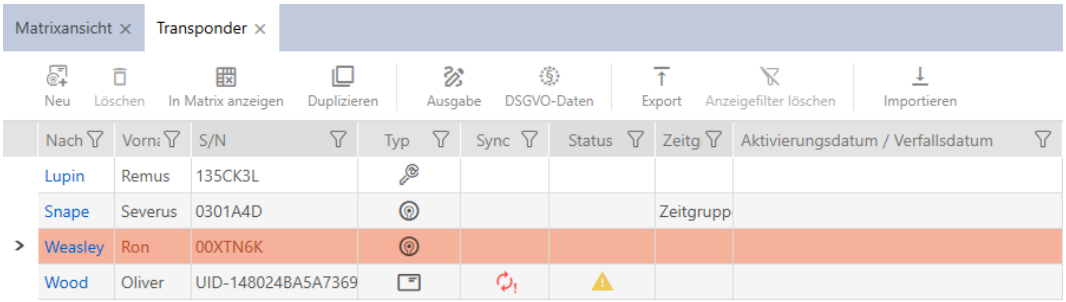
✓ Identmedium vorhanden.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

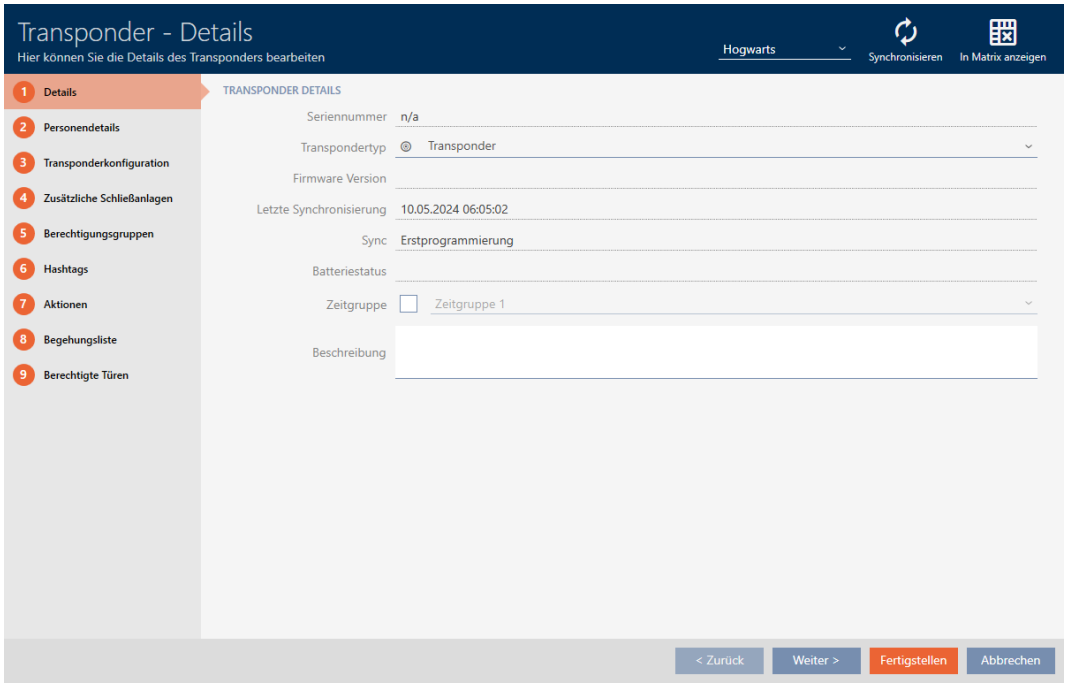
2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.



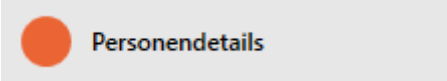
   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit Identmedien öffnet sich.



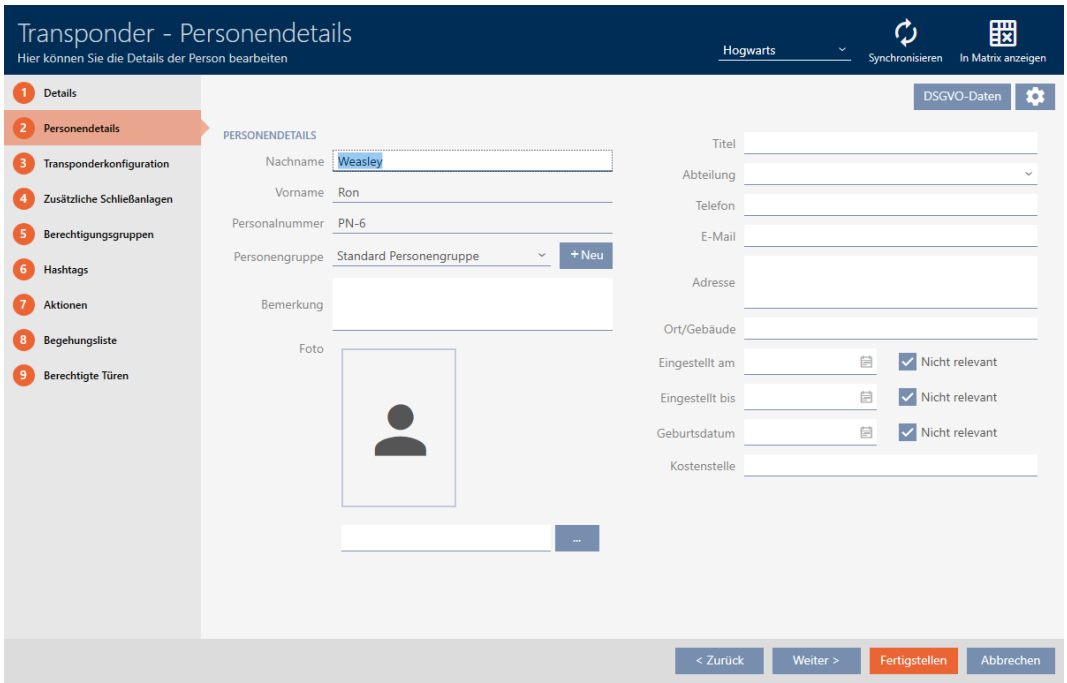
3. Klicken Sie auf ein beliebiges Identmedium.
   ↳ Fenster des Identmediums öffnet sich.



4. Klicken Sie auf den Reiter Personendetails.

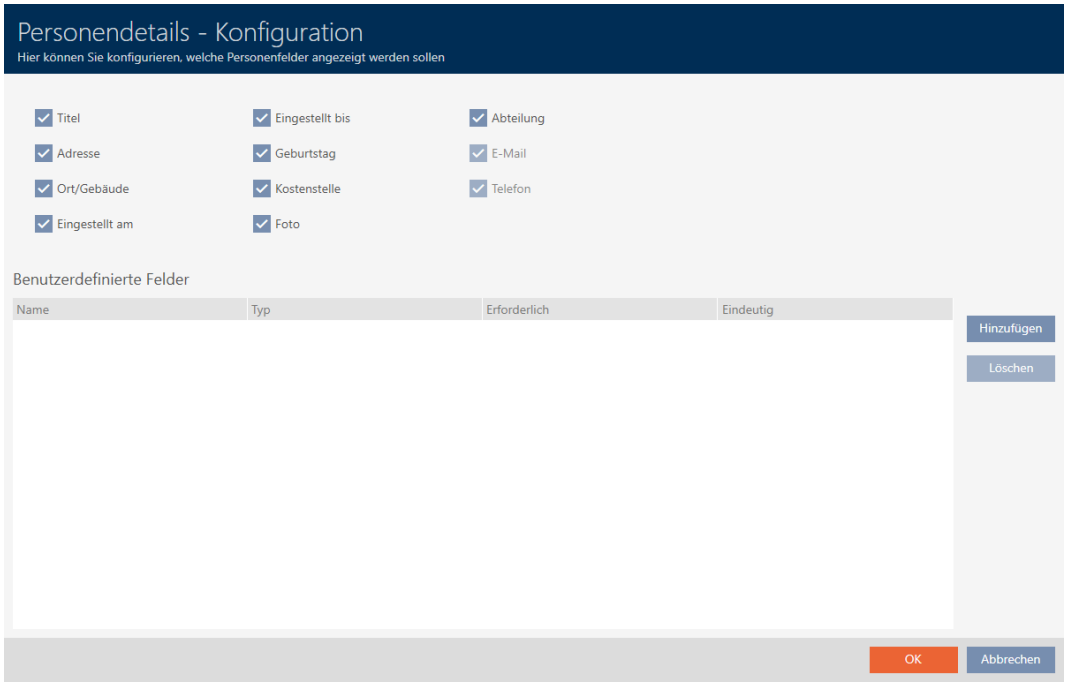


↳ Fenster wechselt zum Reiter "Personendetails".

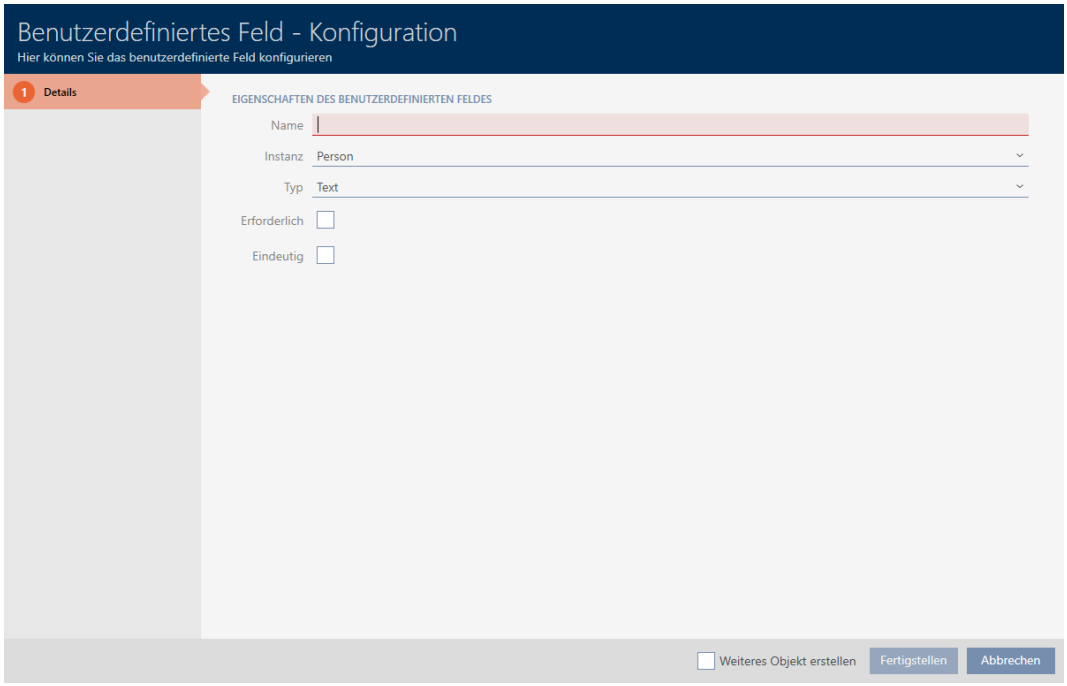


5. Klicken Sie auf die Konfigurations-Schaltfläche ⚙.

6. Fenster "Konfiguration" öffnet sich.

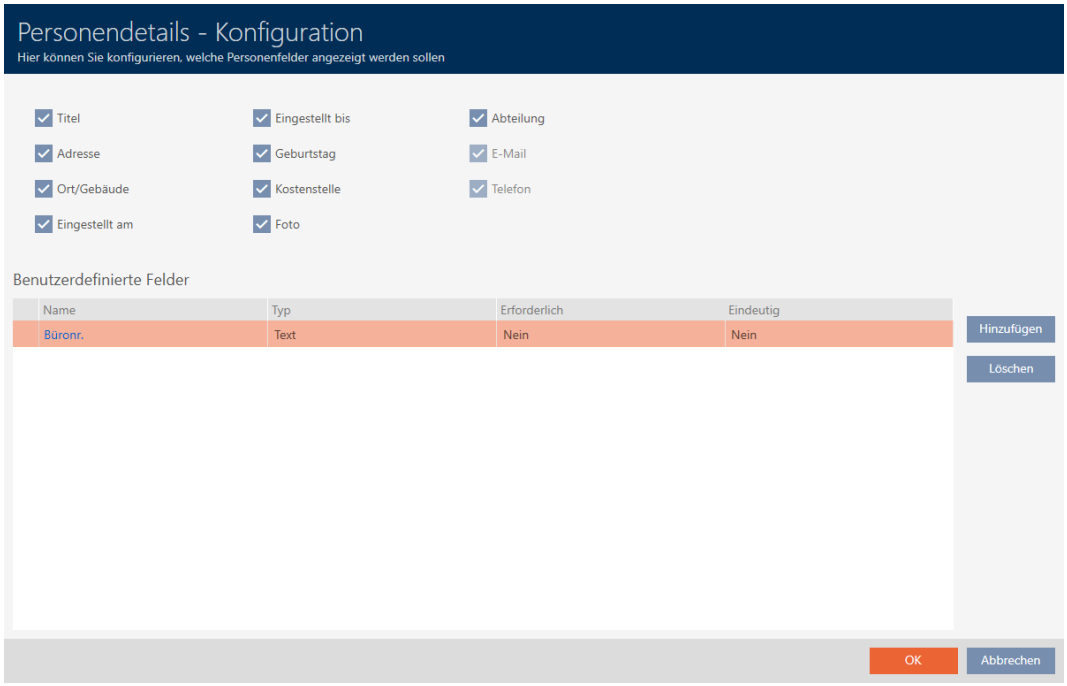


7. Klicken Sie auf die Schaltfläche Hinzufügen.
   ↳ Fenster "Konfiguration" öffnet sich.

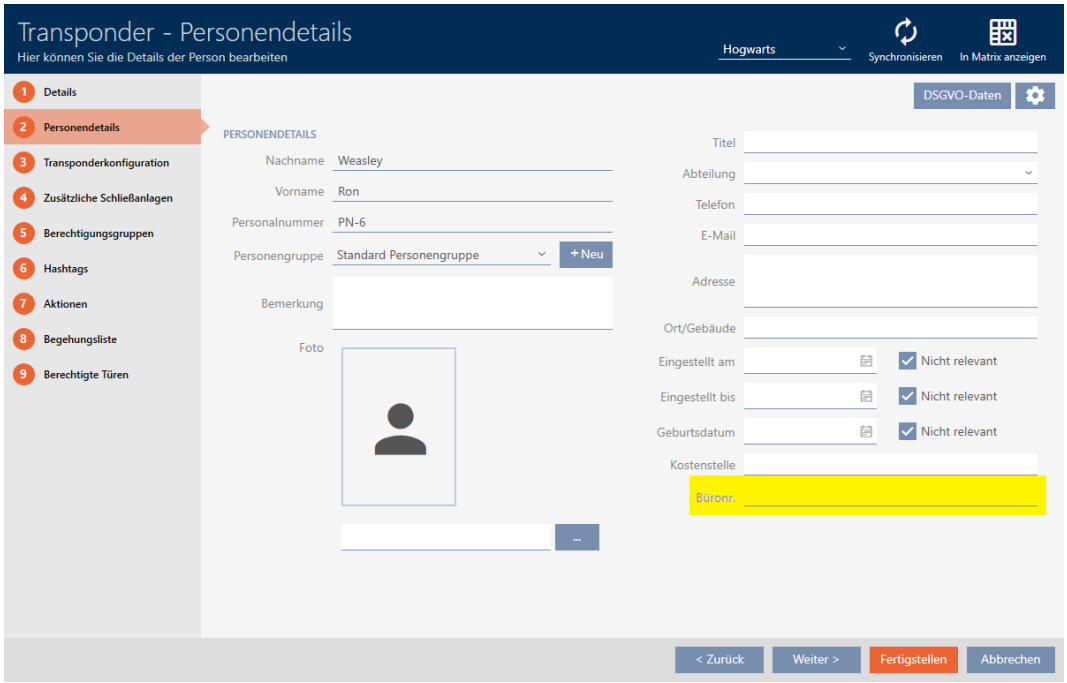


8. Geben Sie im Feld *Name* den Namen Ihres benutzerdefinierten Felds an (Beispiel: *Büronr.*).
   ↳ Dieser Name wird später vor dem Eingabefeld angezeigt.

9. Wenn eine Eingabe in Ihrem Feld zwingend erforderlich sein soll: Aktivieren Sie die Checkbox ☑ Erforderlich (Beispiel: Büronr. ist nicht zwingend erforderlich - nicht jeder Mitarbeiter hat ein Büro mit einer Nummer).
10. Wenn eine Eingabe in Ihrem Feld für dasselbe Feld bei einer anderen Person nicht nochmals verwendet werden darf: Aktivieren Sie die Checkbox ☑ Eindeutig Beispiel: Büronr. ist nicht eindeutig - mehrere Mitarbeiter sitzen im gleichen Büro - Checkbox deshalb nicht aktivieren).
11. Klicken Sie auf die Schaltfläche Fertigstellen.
    ↳ Fenster "Konfiguration" schließt sich.
    ↳ Ihr neues benutzerdefiniertes Feld wird aufgelistet.



12. Klicken Sie auf die Schaltfläche OK.
13. Fenster "Konfiguration" schließt sich.
    ↳ Das Fenster des Identmediums zeigt im Reiter "Personendetails" Ihr neues benutzerdefiniertes Feld an (Beispiel: Das Feld *Büronr.* wird angezeigt).



14. Klicken Sie auf die Schaltfläche Fertigstellen.

↳ Ihr neues benutzerdefiniertes Feld ist in allen Schließanlagen des gleichen Projekts vorhanden.

HINWEIS

Verhalten der AXM Plus bei nachträglich angelegten oder geänderten benutzerdefinierten Feldern

Benutzerdefinierte Felder können jederzeit angelegt werden oder nachträglich geändert werden. Beispiel: Sie legen ein erforderliches Feld an, obwohl schon einige Personen in der Schließanlage vorhanden sind.

Das führt dazu, dass dieses neu erstellte erforderliche Feld bei bereits existierenden Personen leer ist, obwohl es als ☑ Erforderlich markiert ist.

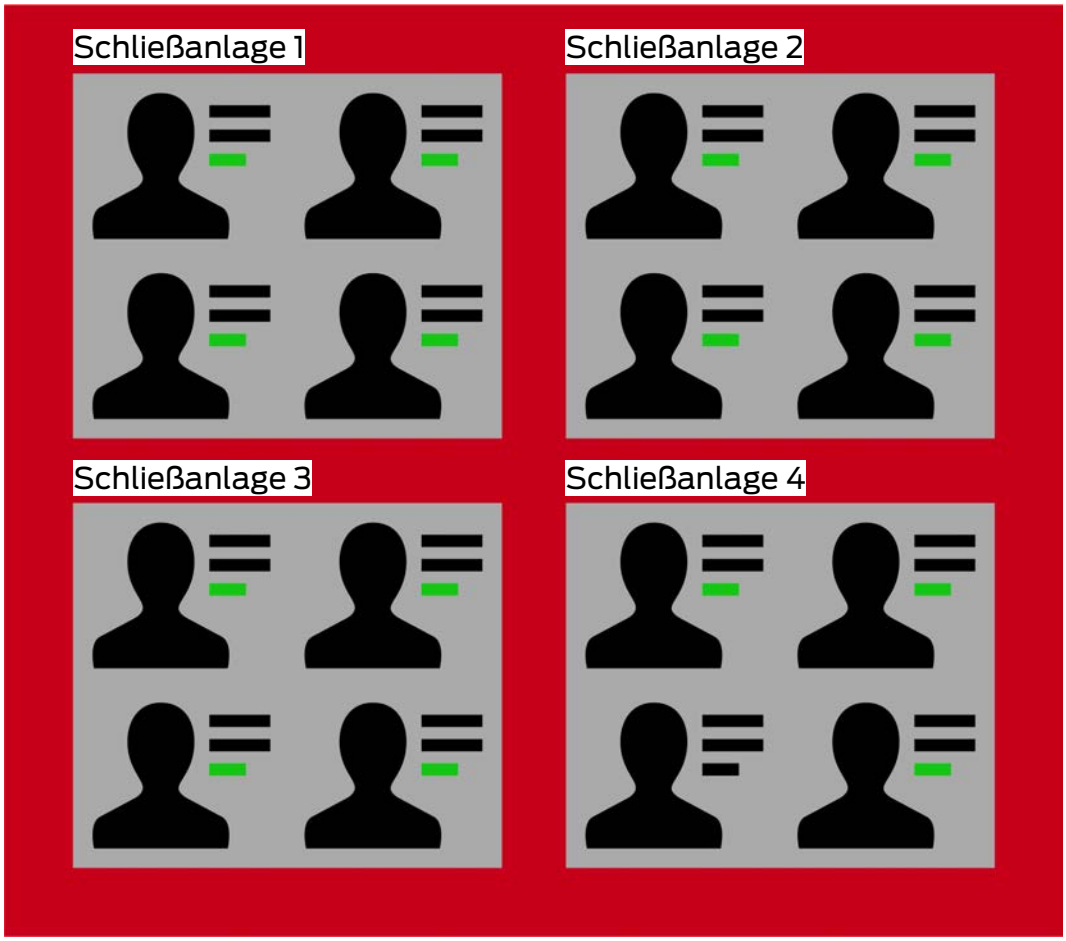
- Informieren Sie sich in solchen Fällen über das Verhalten der AXM Plus (siehe *Nachträglich geänderte benutzerdefinierte Felder [▸ 481]*).

20.13.2.1 Nachträglich geänderte benutzerdefinierte Felder

Ihre AXM Plus erlaubt Ihnen, jederzeit benutzerdefinierte Felder zu erstellen (siehe *Eigene Felder anlegen [▸ 475]*).

Benutzerdefinierte Felder gelten immer projektweit - das heißt, sie gelten in allen Schließanlagen eines Projekts für alle betroffenen Objekte. In der Beispielgrafik wurde das grüne benutzerdefinierte Feld neu angelegt und gilt für alle betroffenen Personen.

Projekt



Beispiel: Sie erstellen für "Personendetails" ein benutzerdefiniertes Feld. Dieses Feld gibt es also zukünftig:

- In allen Personen
- aus allen Schließanlagen
- innerhalb Ihres Projekts.

Benutzerdefinierte Felder können zwei wichtige Eigenschaften haben: ☑ Erforderlich und ☑ Eindeutig.

Die folgenden Beispiele und Erklärungen beziehen sich auf benutzerdefinierte Eigenschaften für Personen.

Benutzerdefinierte Eigenschaften bei neuen Personen

Erforderlich	Eindeutig
Wenn Ihnen ein als erforderlich markiertes und nicht ausgefülltes Feld angezeigt wird, dann wird die Schaltfläche Fertigstellen ausgegraut. Erst nachdem Sie das Feld ausgefüllt haben, können Sie die Eingabe abschließen. Erforderliche Felder, die nicht ausgefüllt sind, werden rot markiert. Im Beispiel wurde Büronr. als ☑ Erforderlich markiert: 	Wenn Ihnen ein als eindeutig markiertes Feld angezeigt wird, dann akzeptiert die AXM Plus zunächst jede Eingabe. Sobald aber die Eingaben mit der Schaltfläche Fertigstellen gespeichert werden, prüft die AXM Plus, ob es im selben Feld bei einem anderen Objekt schon die gleiche Eingabe gibt. Wenn ja, wird die Schaltfläche Fertigstellen ausgegraut. Erst nachdem Sie keinen oder einen eindeutigen Wert angegeben haben, können Sie die Eingabe abschließen. Im Beispiel wurde Büronr. als ☑ Eindeutig markiert:

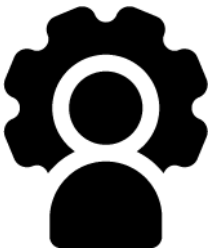
Neue benutzerdefinierte Eigenschaften bei bereits vorhandenen Personen

Erforderlich	Eindeutig
Personen, die schon vorher angelegt wurde, haben natürlich noch keine Büronr. Sobald Sie eine solche Person öffnen, wird das jetzt neu vorhandene Feld rot markiert: Erst nachdem Sie das Feld ausgefüllt haben, können Sie die Eingabe abschließen. Leere Werte sind bei neu angelegten erforderlichen Feldern also möglich!	Keine Probleme. Ein Feld, das neu erstellt wird, kann gar nicht mit doppelten Werten befüllt sein. Alle neu eingegebenen Werte werden vor dem Speichern geprüft.

Geänderte benutzerdefinierte Eigenschaften bei bereits vorhandenen Personen

Erforderlich	Eindeutig
Nachträglich erforderlich gemachte Felder werden wie neu erstellte erforderliche Felder behandelt: Personen, die schon vorher angelegt wurden, haben natürlich noch keine Büronr. Sobald Sie eine solche Person öffnen, wird das jetzt neu vorhandene Feld rot markiert: Erst nachdem Sie das Feld ausgefüllt haben, können Sie die Eingabe abschließen. Leere Werte sind bei nachträglich als erforderlich markierten Feldern also möglich!	Nachträglich eindeutig gemachte Felder werden wie neu erstellte eindeutige Felder behandelt: Personen, die schon vorher angelegt wurden, können im gleichen Feld mehrmals denselben Eintrag haben - bisher war ja keine Eindeutigkeit erforderlich. Sobald Sie jetzt eine Person öffnen und auf die Schaltfläche Fertigstellen klicken, prüft die AXM Plus, ob alle eindeutigen Felder mit eindeutigen Werten befüllt sind. Falls nicht, werden betroffene Felder rot markiert: Erst nachdem Sie keinen oder einen eindeutigen Wert eingegeben haben, können Sie die Eingabe abschließen.

21. Administrative Aufgaben

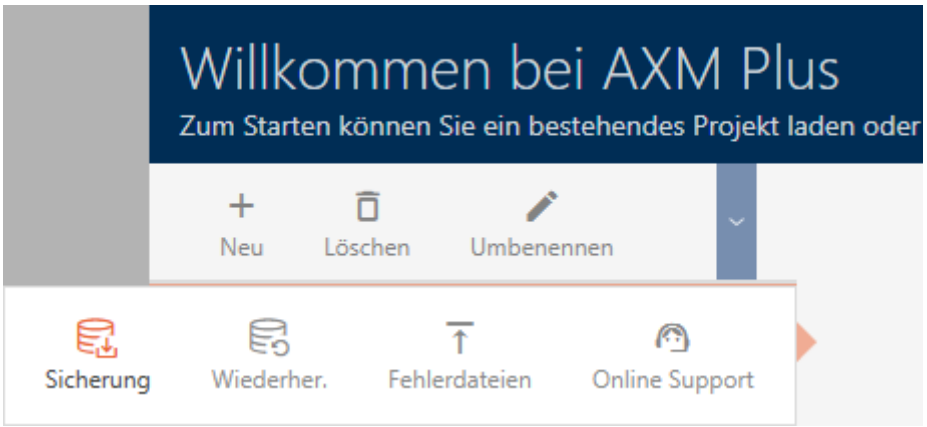


21.1 Backup erstellen

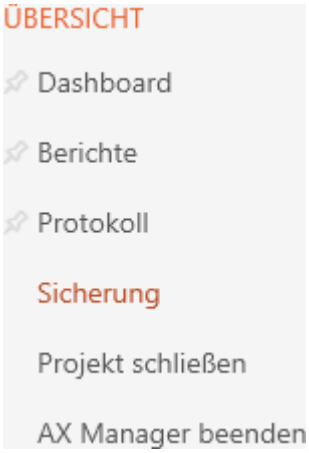
Mit einem regelmäßigen Backup ist Ihre Datenbank und damit Ihr Arbeitsaufwand schnell wiederherstellbar.

Das Backup können Sie bequem in der AXM Plus selbst erstellen:

In der Anmeldemaske (Schaltfläche Projektsicherung):



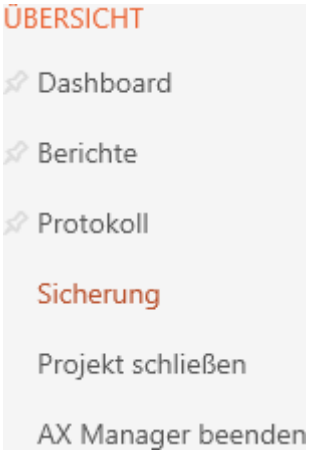
Alternativ: In der ausklappbaren AXM-Leiste (Schaltfläche Projektsicherung):



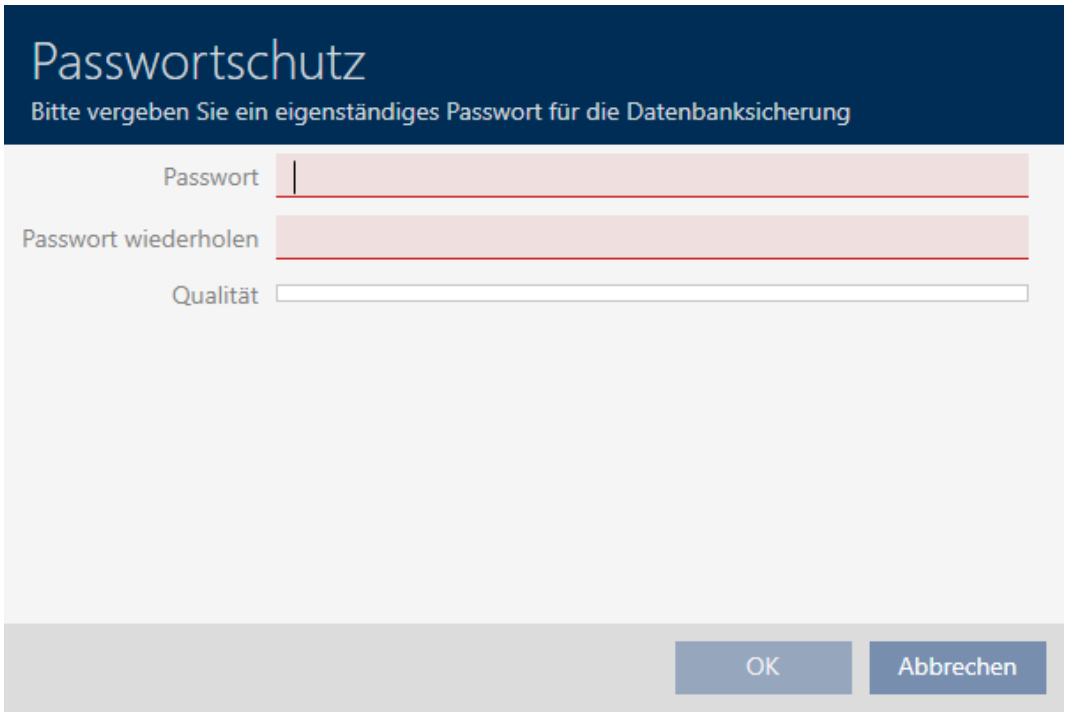
In diesem Abschnitt erfahren Sie, wie Sie ein Backup der Datenbank mit der ausklappbaren AXM-Leiste erstellen.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Klicken Sie in der Gruppe | ÜBERSICHT | auf den Eintrag Projektsicherung.

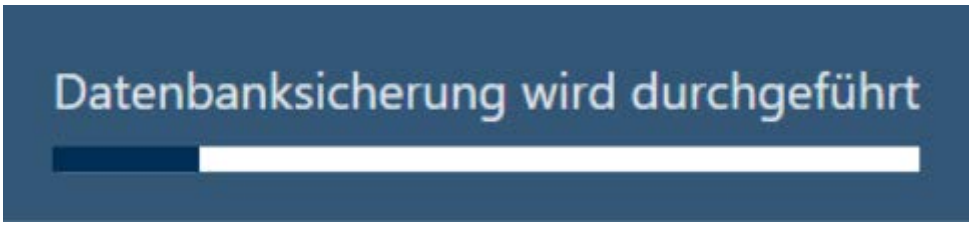


   ↳ AXM-Leiste klappt zu.
   ↳ Fenster zur Passwortvergabe öffnet sich.

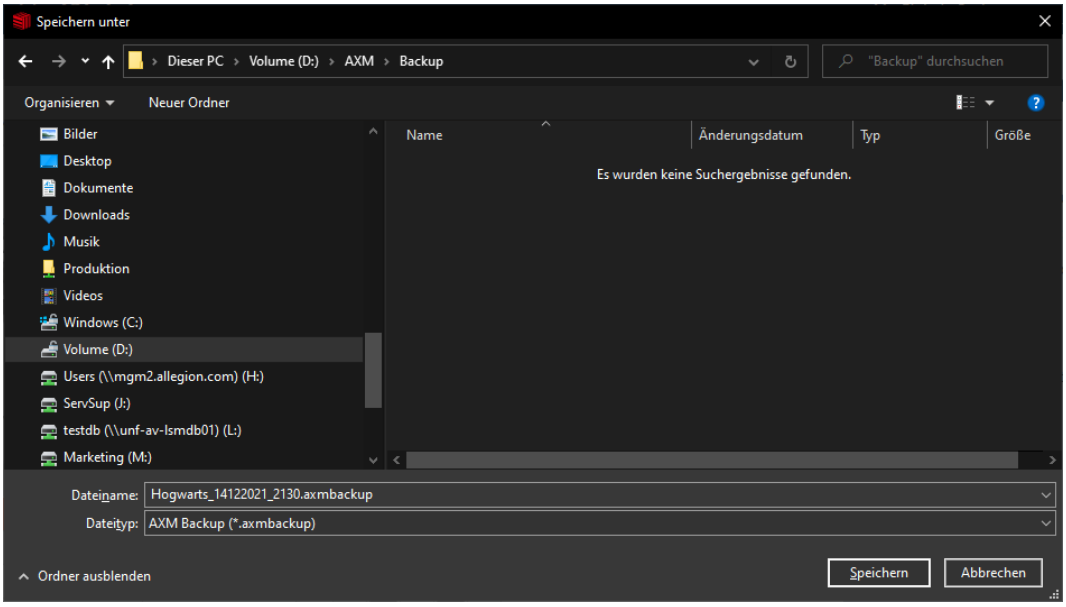


3. Geben Sie in das Feld *Passwort* ein Passwort ein, um dieses Backup zu schützen.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

4. Wiederholen Sie im Feld *Passwort wiederholen* das eingegebene Passwort.
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster zur Passwortvergabe schließt sich.
   ↳ Backup wird erstellt.

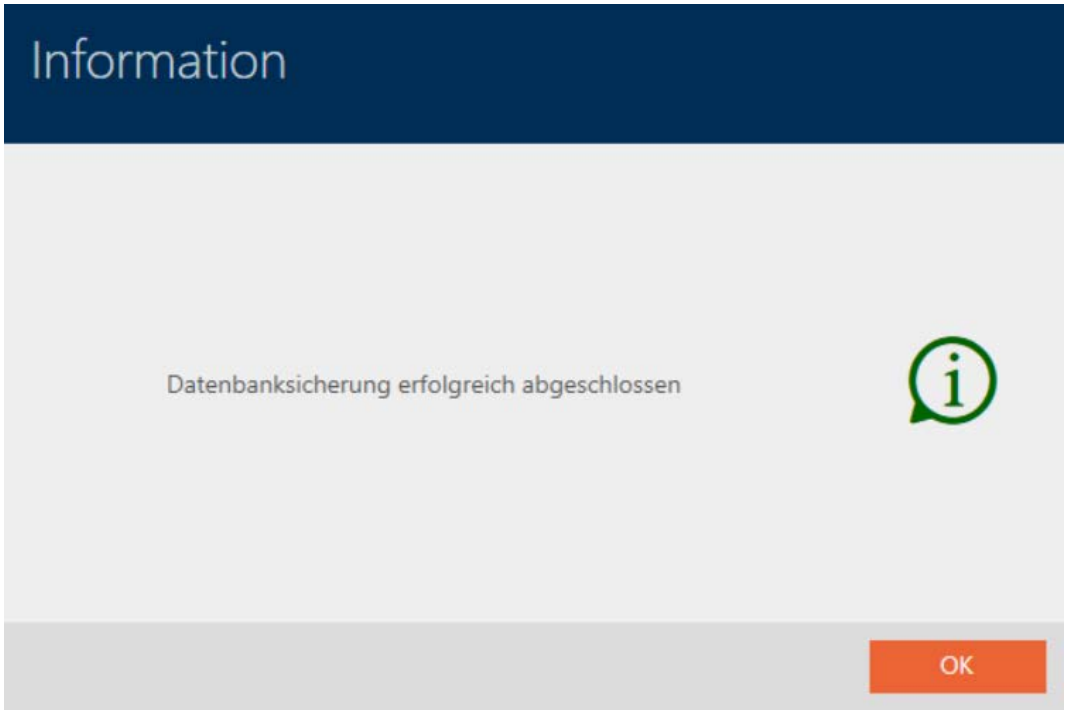


   ↳ Explorer-Fenster öffnet sich.
6. Speichern Sie die Backup-Datei (Endung: .axmbackup) in einem Dateiverzeichnis Ihrer Wahl.

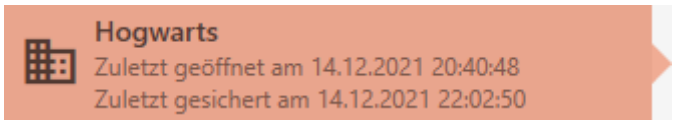


   ↳ Explorer-Fenster schließt sich.

↳ Backup ist abgeschlossen.



In der Anmeldemaske der AXM Plus sehen Sie auch, wann Sie zuletzt ein Backup erstellt haben:



21.2 Backup wiederherstellen

Wenn Sie ein Backup wiederherstellen, dann setzen Sie die Datenbank auf einen vorher gesicherten Stand zurück.

HINWEIS

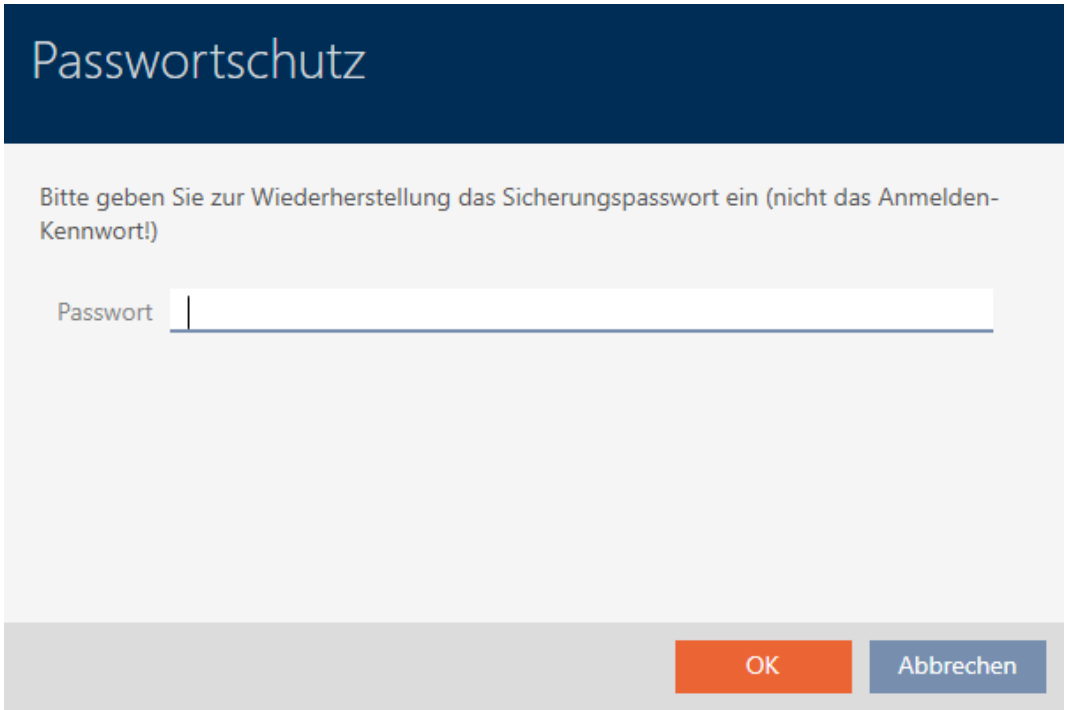
Backup hat keinen Einfluss auf die Schließungen

Die Wiederherstellung bezieht sich nur auf die Datenbank. Sie hat keinen Einfluss auf vorhandene Identmedien und Schließungen.

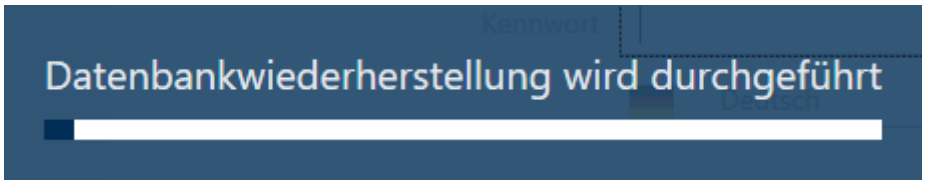
- Synchronisieren Sie ggfs. Identmedien und Transponder (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*).

✓ Backup vorhanden (siehe *Backup erstellen [▸ 485]*).

1. Klicken Sie in der Anmeldemaske auf die Schaltfläche Wiederher.
   ↳ Explorer-Fenster öffnet sich.
2. Navigieren Sie zu Ihrem Backup.
   ↳ Explorer-Fenster schließt sich.
   ↳ Passwortabfrage-Fenster öffnet sich.

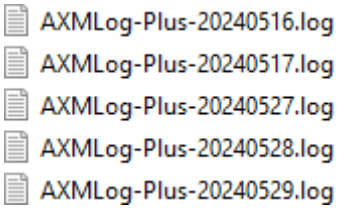


3. Geben Sie im Feld *Passwort* das Passwort ein, das Sie während der Erstellung des Backups eingegeben haben.
4. Klicken Sie auf die Schaltfläche OK.
   ↳ Passwortabfrage-Fenster schließt sich.
   ↳ Datenbank wird wiederhergestellt.



21.3 Fehler-Protokolle exportieren

Fehler-Protokolle tragen dazu bei, Supportfälle schneller zu klären und auftretende Probleme schneller einzugrenzen.

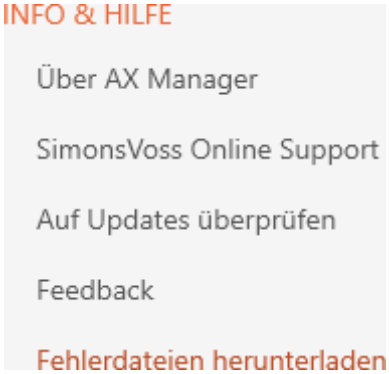


Sie können Fehler-Protokolle entweder in der Anmeldemaske (Schaltfläche Fehlerdateien ↑) oder in der AXM-Leiste exportieren (Schaltfläche Fehlerdateien herunterladen).

In der folgenden Beschreibung erfahren Sie, wie Sie mit der AXM-Leiste die Fehler-Protokolle exportieren können:

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | INFO & HILFE | den Eintrag Fehlerdateien herunterladen aus.

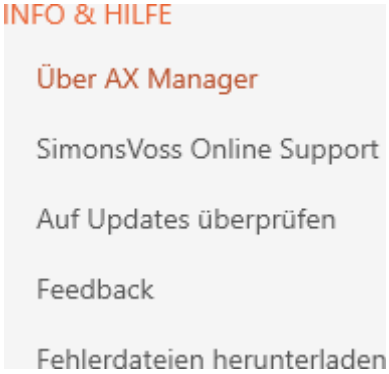


   ↳ Explorer-Fenster öffnet sich.
3. Speichern Sie das Fehler-Protokoll (Endung: .zip) in einem Dateiverzeichnis Ihrer Wahl.
   ↳ Fehler-Protokoll ist exportiert.

21.4 Versionsnummer und Lizenzschlüssel der installierten AXM anzeigen

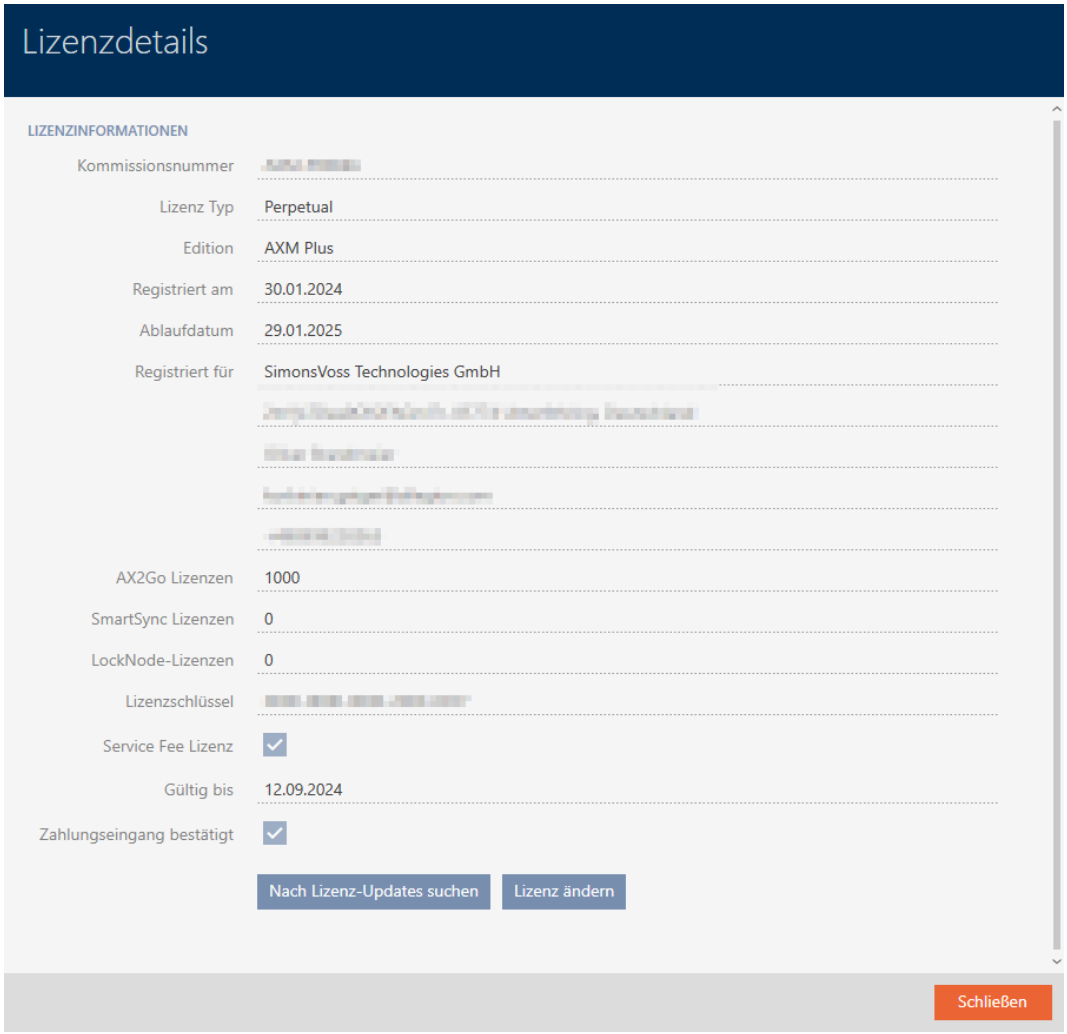
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | INFO & HILFE | den Eintrag Über AX Manager.



↳ Infofenster über AXM Plus öffnet sich.

3. Klicken Sie auf die Schaltfläche Lizenzdetails.
   ↳ Infofenster über AXM Plus schließt sich.
   ↳ Infofenster über Lizenz öffnet sich.



4. Klicken Sie auf die Schaltfläche Schließen.
   ↳ Infofenster über Lizenz schließt sich.

Hier können Sie Ihre AXM Plus auch registrieren (siehe *Registrierung [▸ 34]*).

21.5 Benutzer-Management

21.5.1 Benutzerkennwort ändern

Ihr Benutzerkennwort muss folgende Anforderungen erfüllen:

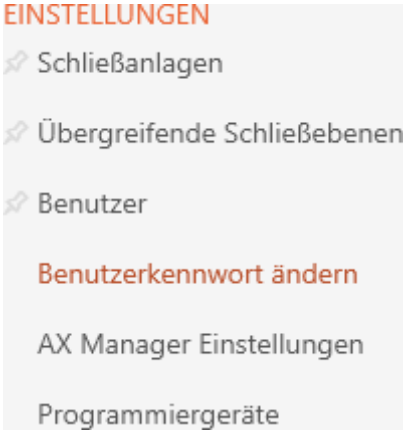
- Ist mindestens 8 Zeichen lang
- Enthält Groß- und Kleinbuchstaben

Noch mehr Sicherheit erhalten Sie, wenn Sie auch Nummern (1234...) und Sonderzeichen (!$%&?...) verwenden.

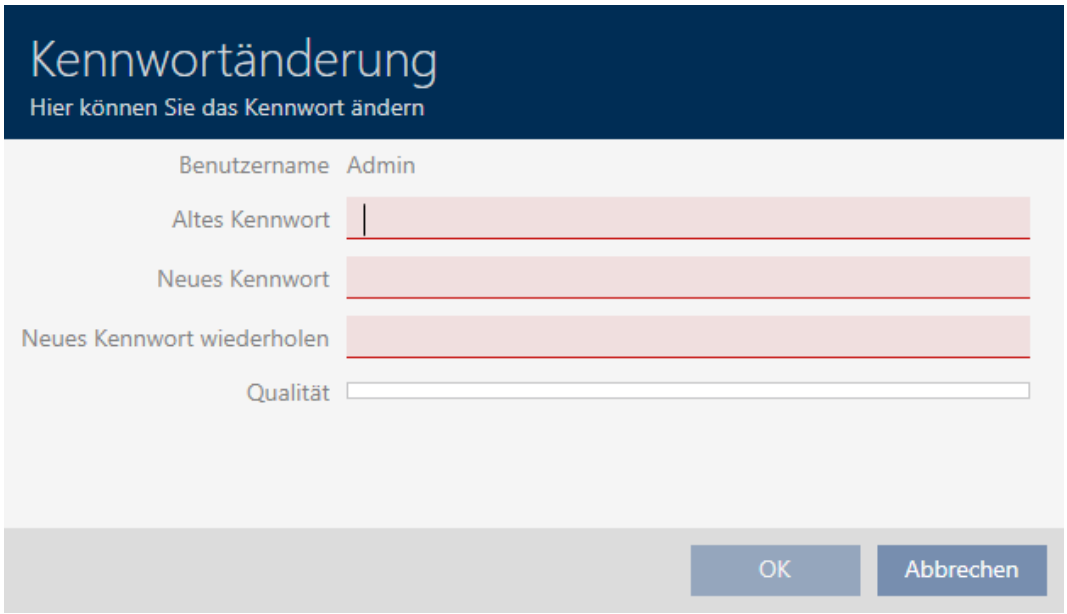
Selbstverständlich kann jeder Benutzer nur sein eigenes Benutzerkennwort ändern. Administratoren können mit erhöhten Anforderungen an Benutzerkennwörter die Sicherheit erhöhen (siehe *Kennwortsicherheit erhöhen [▸ 494]*).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Benutzerkennwort ändern.

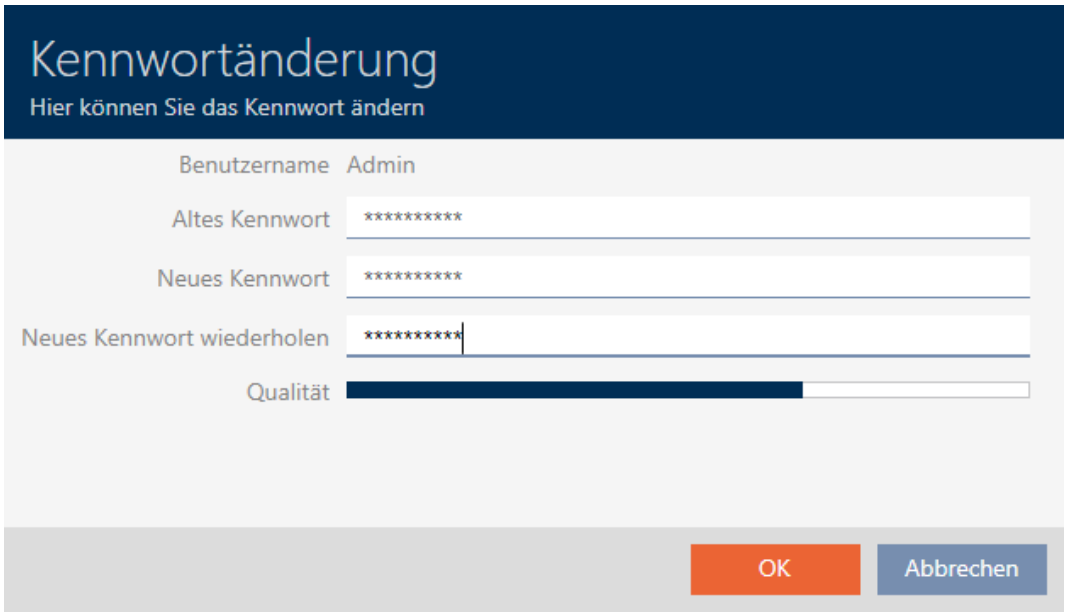


   ↳ Fenster zum Ändern des Benutzerpasswords öffnet sich.

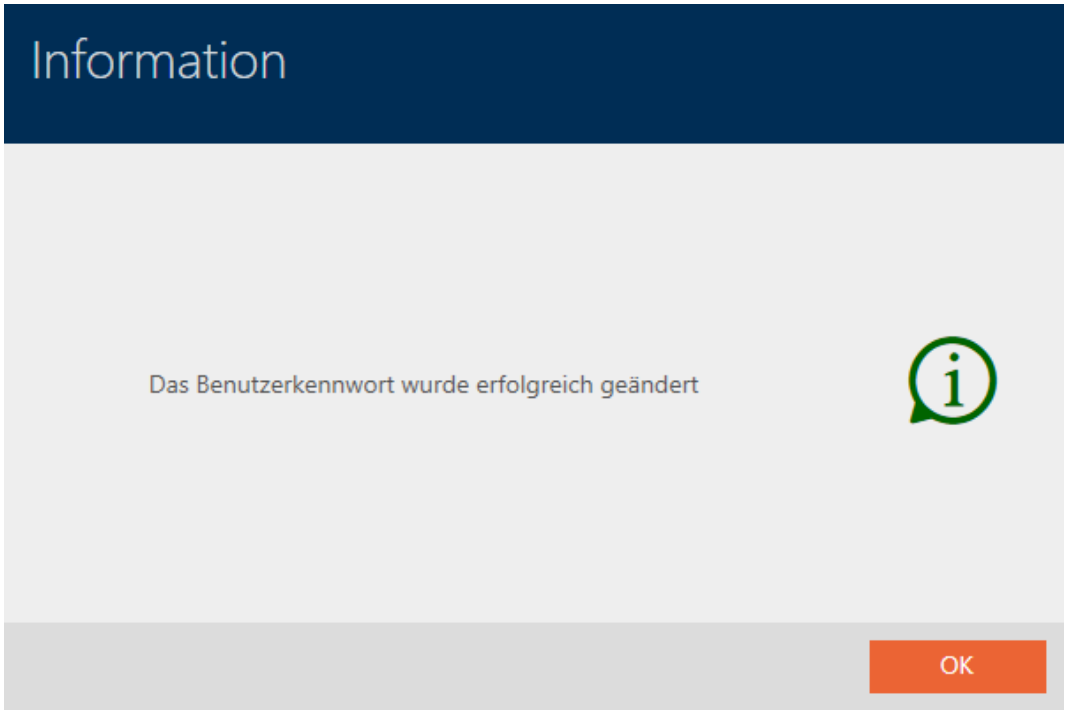


3. Geben Sie im Feld *Altes Kennwort* Ihr aktuelles Benutzerkennwort ein.

4. Geben Sie in die Felder *Neues Kennwort* und *Neues Kennwort wiederholen* Ihr neues Kennwort ein.
   ↳ Ein farbiger Balken zeigt Ihnen, wie sicher Ihr Kennwort ist.

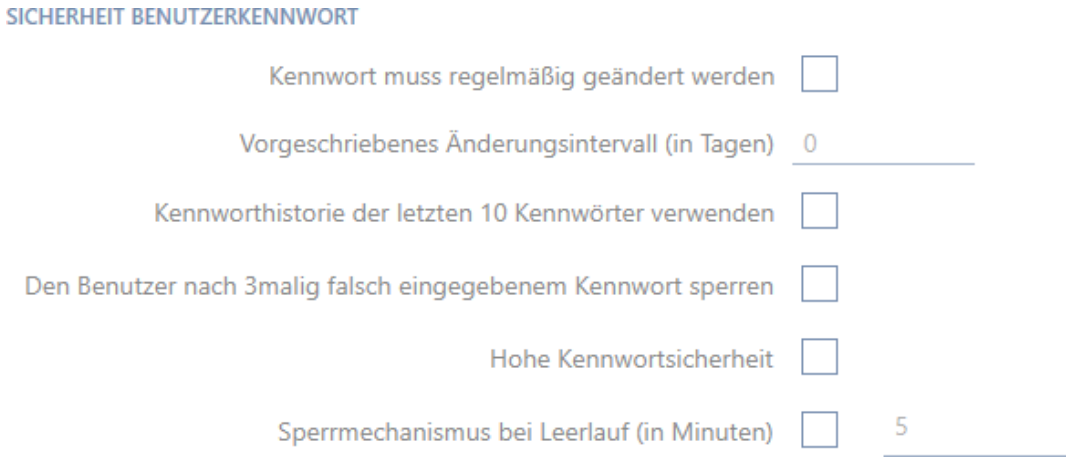


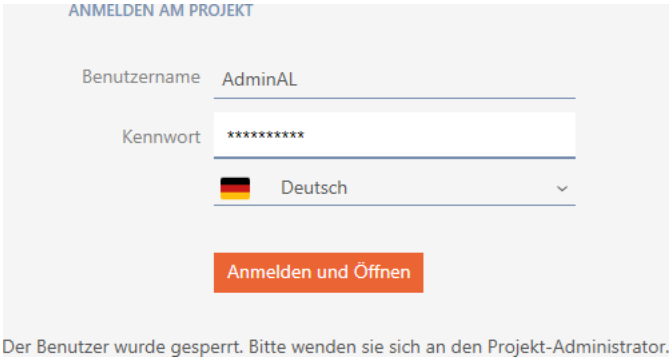
↳ Benutzerkennwort ist geändert.

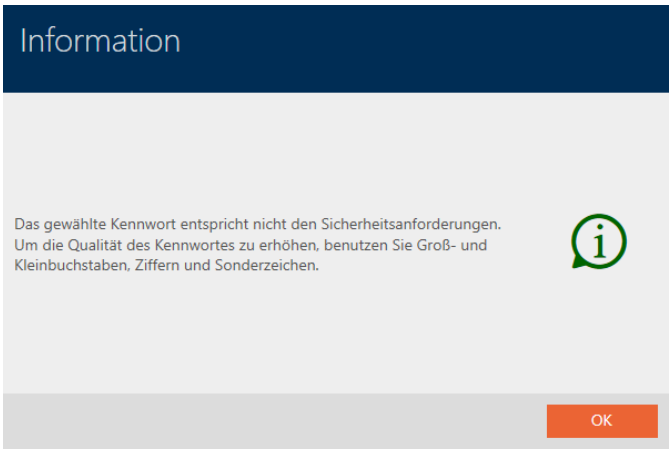
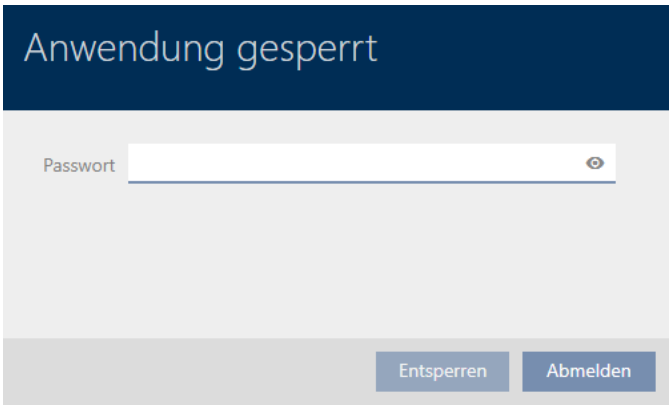


21.5.2 Kennwortsicherheit erhöhen

Kennwörter sind ein wichtiger Baustein Ihres Sicherheitskonzepts. Mit verschiedenen Einstellungen können Sie die Sicherheit erhöhen:



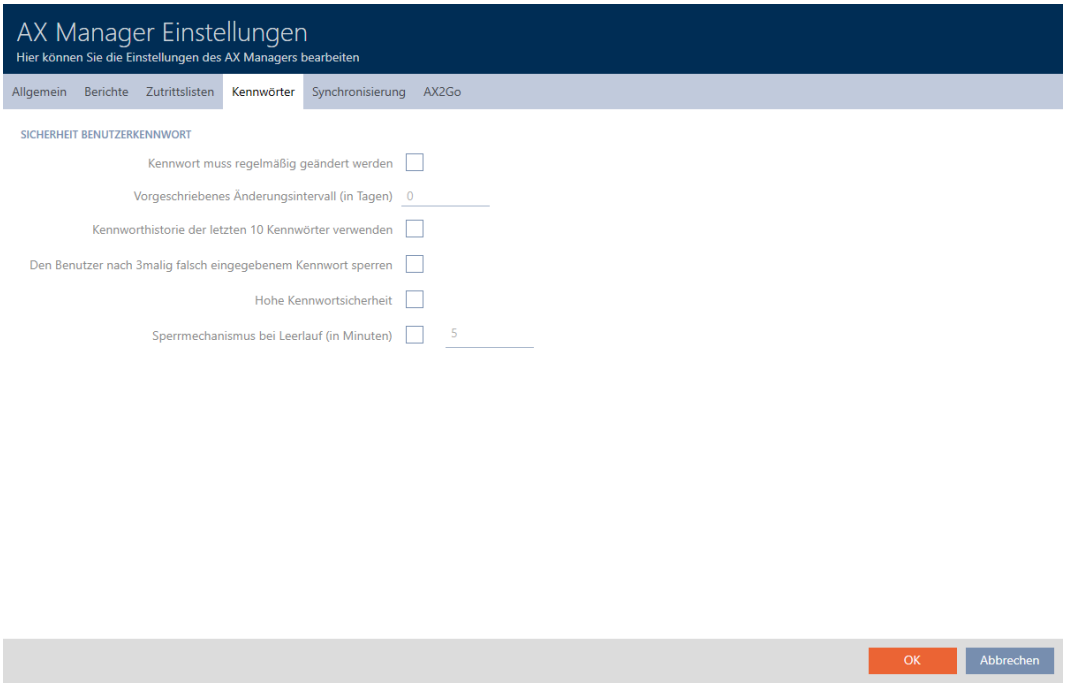
☑ Kennwort muss regelmäßig geändert werden	Nach Ablauf des eingestellten Änderungsintervalls muss der Benutzer ein neues Kennwort vergeben. Das Änderungsintervall stellen Sie mit *Vorgeschriebenes Änderungsintervall (in Tagen)* selbst ein.
☑ Den Benutzer nach 3malig falsch eingegebenem Kennwort sperren	Das neue Kennwort darf nicht mit einem der letzten zehn Kennwörtern übereinstimmen.
☑ Kennworthistorie der letzten 10 Kennwörter verwenden	Wenn ein Benutzer das Kennwort dreimal falsch eingegeben hat, kann er sich nicht mehr anmelden, bis er entsperrt wurde.  In der AXM Plus müssen Sie als *Admin* den Benutzer *AdminAL* löschen und neu erstellen.

☑ Hohe Kennwortsicherheit	Die AXM Plus lehnt Trivialkennwörter wie "12345678" automatisch ab. 
☑ Sperrmechanismus bei Leerlauf (in Minuten)	Wenn Ihre AXM Plus innerhalb der eingestellten Leerlaufzeit keine Aktionen feststellt, dann wird Ihre AXM Plus automatisch gesperrt. 

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.

   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.
3. Wechseln Sie zum Kennwörter-Tab.



4. Aktivieren Sie die gewünschten Checkboxen.
5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

↳ Neue Anforderungen an Kennwörter sind aktiv.

21.5.3 Person zu AXM-Benutzer ernennen

Um die Übersicht über die Benutzer der AXM Plus zu wahren, können Sie Personen in Ihrem Projekt zu AXM-Benutzern ernennen. Eine Person kann mehreren Benutzern zugewiesen werden. Gleichzeitig werden die Kontaktdaten dieser Person direkt aus der Datenbank übernommen und automatisch auch für den jeweiligen Benutzer angezeigt.

Unterschied zwischen Admin und AdminAL

In der AXM Plus gibt es nur zwei Benutzer: Admin und AdminAL.

- **Admin** ist der Standard-Benutzer.
- **AdminAL** bedeutet AdminAccessList und ist ein stark eingeschränkter Benutzer. AdminAL kann vor allem Zutrittslisten auszulesen, ohne dabei vollen Zugriff auf die Schließanlage zu haben. Somit können andere Personen Zutrittslisten auslesen, ohne dabei die Schließanlage selbst manipulieren zu können.

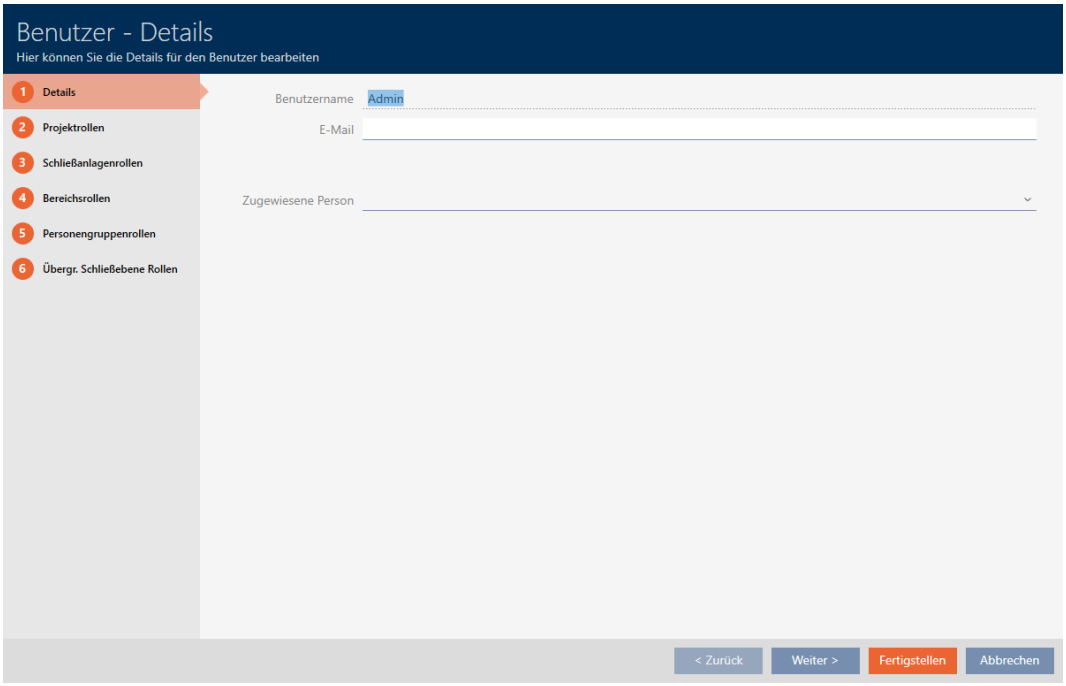
✓ Mindestens ein Identmedium bzw. mindestens eine Person erstellt.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

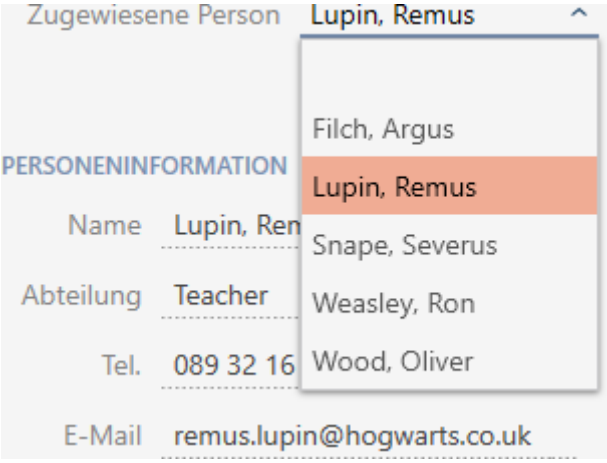
2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Benutzer aus.

↳ AXM-Leiste klappt zu.
↳ Tab [Benutzer] öffnet sich.

3. Klicken Sie auf den Benutzer, dem Sie eine Person aus der Schließanlage zuweisen wollen.
↳ Fenster "Benutzer" öffnet sich.



4. Wählen Sie im Dropdown-Menü ▼ **Zugewiesene Person** die Person aus Ihrem Projekt aus, die Sie dem Benutzer zuweisen wollen.



   ↳ Der Bereich "Personeninformation" wird automatisch mit den Informationen befüllt, die für diese Person hinterlegt sind (*Name*, *Abteilung*, *Tel.* und *E-Mail*).

5. Klicken Sie auf die Schaltfläche Fertigstellen.
   ↳ Fenster "Benutzer" schließt sich.

↳ Zugewiesene Person wird neben dem Benutzer angezeigt.

21.5.4 AXM-Benutzern Aufgaben/Benutzerrollen zuweisen

Benutzerrollen sind Berechtigungen für bestimmte Aufgabenbereiche. Mit Benutzerrollen können Sie einstellen, welcher Benutzer was an Ihrer Schließanlage machen darf. Sie können damit die Sicherheit in Ihrer Schließanlage erhöhen.

Geben Sie jedem Benutzer nur die Rechte, die er zur Erfüllung der vorgesehenen Aufgaben braucht. Jemand, der nur Zutrittslisten auslesen wird, braucht zum Beispiel die Schließanlagenrolle ☐ Zutrittslisten Administration nicht. Schließlich soll er nur Zutrittslisten auslesen und nicht darüber entscheiden, wer Zutrittslisten auslesen darf.

In Ihrer AXM Plus gibt es folgende Benutzerrollen:

In der AXM Plus sind nur die Benutzerrollen ☑ Zutrittslisten und ☑ Zutrittslisten Administration bei den "Schließanlagenrollen" veränderbar.

Projektrollen

Protokoll	Ermöglicht das Lesen und Exportieren des Datenbank-Protokolls. Beispiel: *Aktivitäten an der Datenbank nachverfolgen (Protokoll) [▸ 520]*
Zeitplansteuerung	Ermöglicht die Bearbeitung von Zeitplänen. Beispiele: ▪ *Zeitplan erstellen [▸ 58]* ▪ *Zeitgruppe erstellen [▸ 61]* ▪ *Zeitpläne löschen [▸ 69]*
Standort/Gebäude Verwaltung	Ermöglicht das Bearbeiten der entsprechenden Organisationsstrukturen. Beispiele: ▪ *Standort erstellen [▸ 83]* ▪ *Gebäude erstellen und zu Standort zuweisen [▸ 86]*
SmartSync benutzen	Ermöglicht die Verwendung von SmartSync.
Hashtags	Ermöglicht das Bearbeiten von Hashtags. Beispiel: *Hashtag erstellen [▸ 91]*
Benutzerverwaltung	Ermöglicht das Zuweisen von Personen zu Benutzern und das Bearbeiten von Benutzerrollen. Beispiele: ▪ *Person zu AXM-Benutzer ernennen [▸ 498]* ▪ *AXM-Benutzern Aufgaben/ Benutzerrollen zuweisen [▸ 500]*
AX Manager Einstellungen	Ermöglicht die Bearbeitung der Einstellungen Ihrer AXM Plus. Beispiel: *Ihre individuelle AXM-Oberfläche [▸ 452]*

Schließanlagenrollen

Schließanlagen	Ermöglicht das Bearbeiten von Schließanlagendetails. Beispiele: - *Schließanlage erstellen [▸ 360]* - *Schließanlagenpasswort ändern [▸ 395]* - *Karten bzw. Transponder freischalten [▸ 401]*
Berechtigungen	Ermöglicht das Lesen und das Ändern von Zugangsberechtigungen. Beispiele: - *Einzelne Berechtigungen ändern (Kreuz) [▸ 327]* - *Viele Berechtigungen ändern (an Identmedien und/oder Schließungen) [▸ 328]*
Personalverwaltung	Ermöglicht die Bearbeitung von personenbezogenen Daten. Beispiel: *Personen und Identmedien [▸ 94]*
Berichtswesen	Ermöglicht den Export von Berichten. Beispiele: - *Datenschutzbericht (DSGVO) ausgeben [▸ 527]* - *Bericht zur Identmedien-Ausgabe ausgeben [▸ 524]*
Zutrittslisten Administration	Ermöglicht das Ändern der Benutzerrollen Zutrittslisten und Zutrittslisten Administration. Wer diese Benutzerrollen nicht hat, kann weder sich selbst noch anderen das Lesen von Zutrittslisten erlauben.

Zutrittslisten	Ermöglicht das Auslesen von Zutrittslisten und Begehungslisten. Beispiele: ▪ *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]* ▪ *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*

Bereichsrollen

Schließungen auslesen	Ermöglicht das generelle Auslesen von Schließungen. Beispiel: *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*
Schließungen programmieren	Ermöglicht das Synchronisieren von Schließungen. Beispiel: *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*
Schließungen und Bereiche einsehen/bearbeiten	Ermöglicht das Bearbeiten von Schließungen und Bereichen. Beispiele: ▪ *Schließung erstellen [▸ 238]* ▪ *Schließungen in Bereiche verschieben [▸ 279]* ▪ *Bereich erstellen [▸ 89]*

Personengruppenrollen

Transponder auslesen	Ermöglicht das generelle Auslesen von Identmedien. Beispiele: ▪ *Unbekannte Transponder/Karten erkennen [▸ 438]* ▪ *Identmedium-Batteriestatus anzeigen [▸ 430]*

Transponder programmieren	Ermöglicht das Programmieren von Identmedien. Beispiel: *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*
Transponder und Gruppen einsehen/bearbeiten	Ermöglicht das Betrachten und Bearbeiten von Identmedien und Personengruppen. Beispiele: ▪ *Identmedium duplizieren (inkl. Berechtigungen und Einstellungen) [▸ 113]* ▪ *Berechtigungen des Identmediums auf bestimmte Zeiten beschränken (Zeitgruppe) [▸ 126]* ▪ *Personen zu Personengruppen zuordnen [▸ 202]*

Übergr. Schließebene Rollen

Übergreifende Schließebene Verwaltung	Ermöglicht das Einrichten und Ändern von übergreifenden Schließebenen Beispiele: ▪ *Übergreifende Schließebene verwenden [▸ 405]*

Benutzerrollen können Sie über die Benutzerverwaltung vergeben. Im Beispiel soll AdminAL nicht mehr entscheiden dürfen, ob andere Benutzer Zutrittslisten auslesen dürfen. Deshalb deaktivieren wir für ihn die Benutzerrolle ☐ Zutrittslisten.

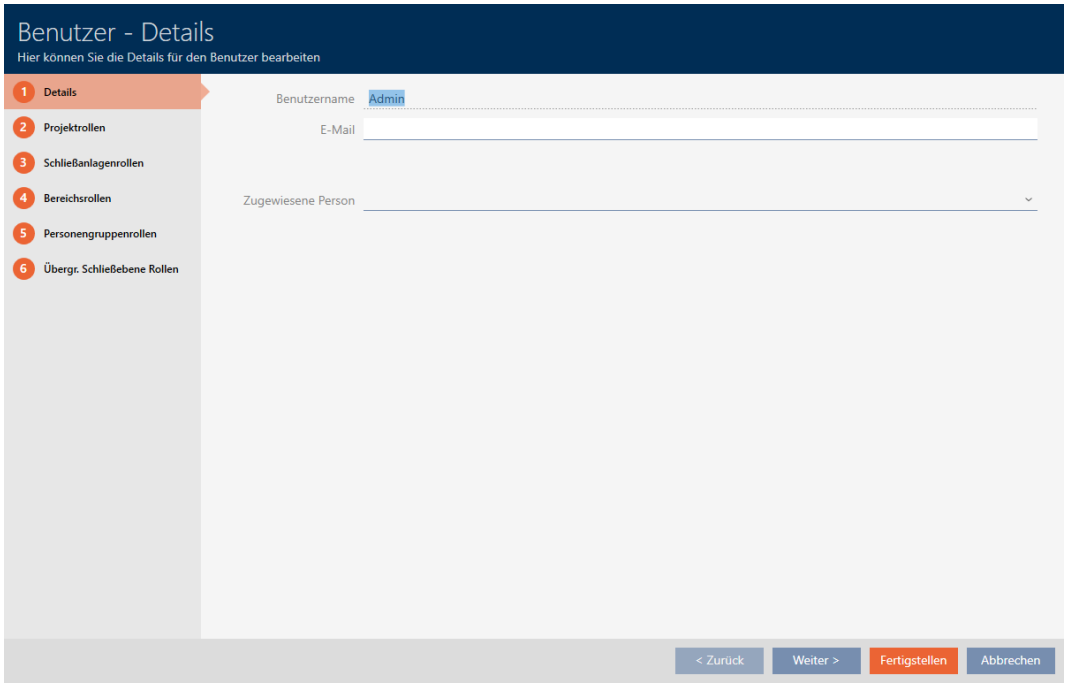
✓ Mindestens ein Identmedium bzw. mindestens eine Person erstellt.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

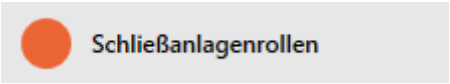
2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag Benutzer aus.

↳ AXM-Leiste klappt zu.
↳ Tab [Benutzer] öffnet sich.

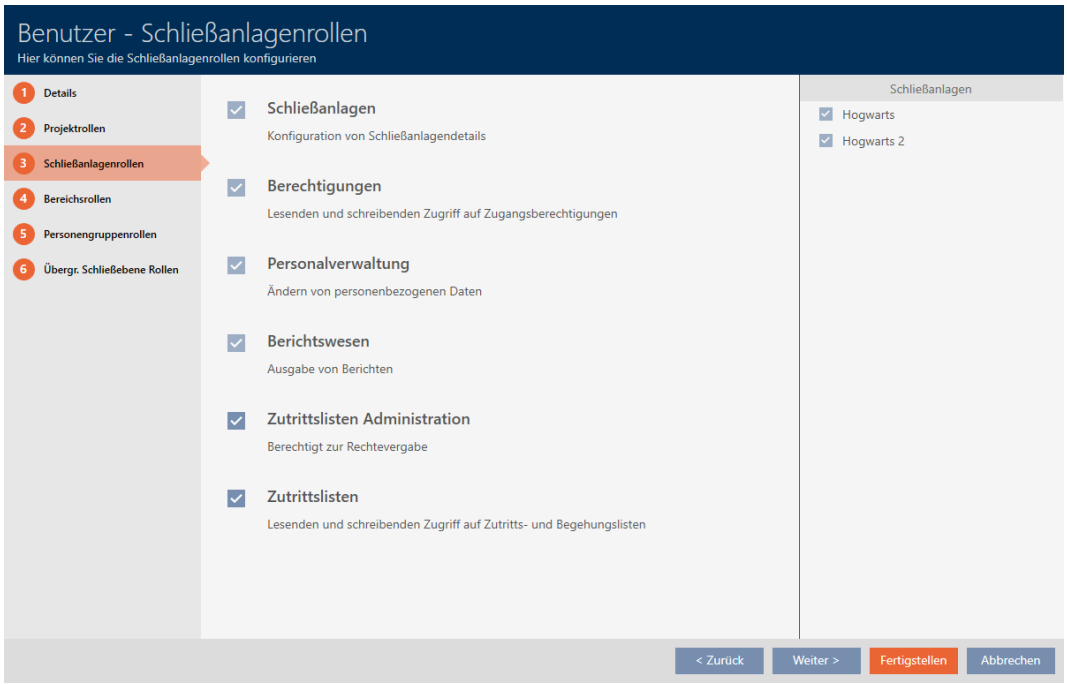
3. Klicken Sie auf den Benutzer, dessen Benutzerrollen Sie bearbeiten wollen (Beispiel: AdminAL).
   ↳ Fenster "Benutzer" öffnet sich.



4. Klicken Sie auf den Reiter mit der Rolle, die Sie ändern wollen (Beispiel: Reiter Schließanlagenrollen).



↳ Fenster wechselt zum Reiter "Schließanlagenrollen".



5. Aktivieren bzw. deaktivieren Sie die gewünschten Benutzerrollen (Beispiel: Deaktivieren Sie die Checkbox ☐ Zutrittslisten Administration).

6. Wechseln Sie mit der Schaltfläche Weiter > zum nächsten Reiter oder schließen Sie die Eingaben mit der Schaltfläche Fertigstellen ab.
   ↳ Fenster "Benutzer" schließt sich.

↳ Neue Benutzerrollen sind vergeben (Beispiel: AdminAL kann die Checkboxen ☐ Zutrittslisten und ☐ Zutrittslisten Administration nicht mehr verändern).

HINWEIS

"Aussperren" des eigenen Benutzers

Benutzer können auch ihre eigenen Benutzerrollen einschränken. Je nachdem, welche davon betroffen sind, können diese Benutzer diese Benutzerrollen nicht mehr selbst wiederherstellen.

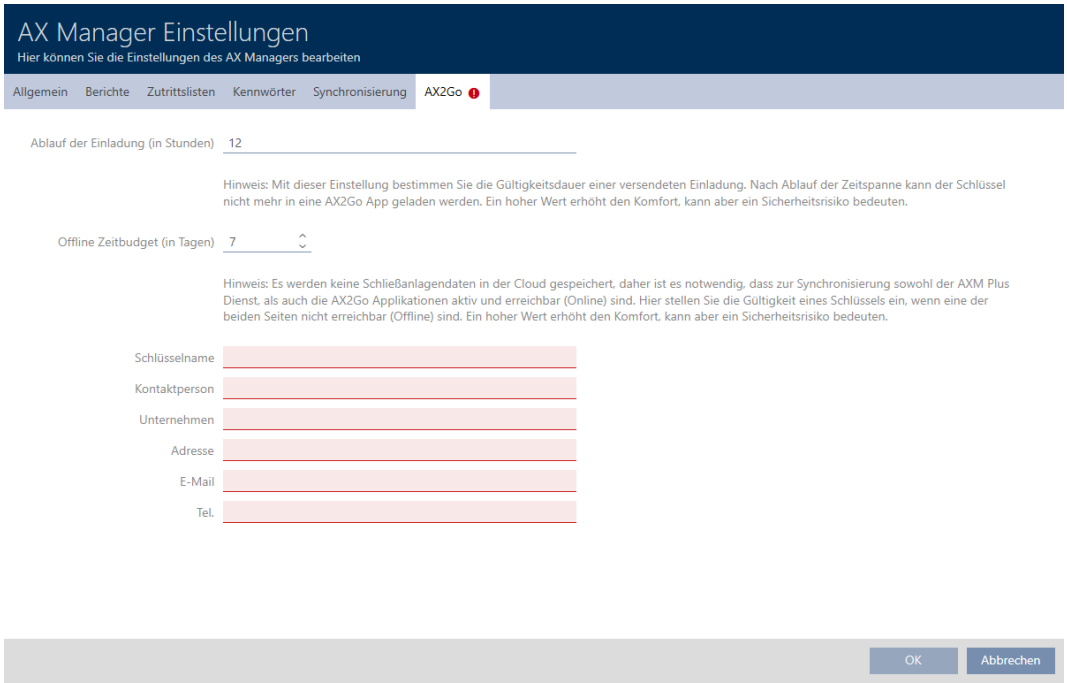
Beispiel: Wenn Sie sich selbst die Benutzerrollen Zutrittslisten und Zutrittslisten sperren, dann fehlen Ihnen die Rechte, um Zutrittslisten-Benutzerrollen zu ändern. Sie haben sich also aus diesen Benutzerrollen ausgesperrt.

Die AXM Plus verhindert, dass sich alle Benutzer gleichzeitig von einer Benutzerrolle aussperrren. Wenn das der Fall wäre, dann ist die entsprechende Checkbox ausgegraut.

1. Prüfen Sie sorgfältig, welche Benutzerrollen Sie aktivieren oder deaktivieren.
2. Bitten Sie in diesem Fall einen anderen berechtigten Benutzer, Ihnen die gewünschte Benutzerrolle wieder zuzuweisen.

21.6 AX2Go-Einstellungen

AX2Go ist individuell auf Ihre persönlichen Bedürfnisse einstellbar.



Folgende Einstellungen stehen Ihnen zur Verfügung:

Einstellung	Bedeutung
Ablauf der Einladung (in Stunden)	Je länger eine Einladung gültig ist, desto mehr Zeit haben die Benutzer, diese in ihre AX2Go-App zu importieren. Länger gültige Einladungen sind komfortabler, aber risikoreicher. Der Maximalwert beträgt 120 Stunden (= 5 Tage).
Offline Zeitbudget (in Tagen)	Diese Einstellung legt fest, wie lange die AX2Go auf dem Mobilgerät funktioniert, wenn keine Verbindung zwischen AX2Go und dem AXM-Dienst Ihrer AXM Plus aufgebaut werden kann. Ein längeres Offline-Zeitbudget ist komfortabler, aber risikoreicher. Der Maximalwert beträgt 30 Tage. Hinweis: In der Cloud werden keine Schließanlagendaten gespeichert. Für die Synchronisierung muss die AX2Go deshalb zur Cloud und von dort aus zum AXM-Dienst kommunizieren können. Das heißt, beide müssen aktiv und erreichbar (online) sein. Sie können die Verbindung zwischen dem AXM-Dienst und der Cloud prüfen: *Verbindung zwischen Datenbank und Cloud überprüfen [▸ 451]*.

HINWEIS

Unterschiede der Zeitbudgets in AX2Go und virtuellem Netzwerk

AX2Go: Das Zeitbudget wird vom AXM-Dienst wieder voll aufgeladen, sobald sich die AX2Go mit diesem verbunden hat.
Hauptzweck: Verhindern, dass mithilfe des Flugmodus eine AX2Go-Berechtigung dauerhaft genutzt wird.

Virtuelles Netzwerk: Das Zeitbudget wird vom Gateway wieder wie eingestellt aufgeladen, sobald das Identmedium an diesem betätigt wird.
Hauptzweck: Identmedien regelmäßig ans Gateway zu holen, um Daten übertragen zu können.

- Weitere Informationen zu Zeitbudgets siehe *Zeitbudget (AX2Go und virtuelles Netzwerk) [▸ 560]*.

Bitte geben Sie hier außerdem einen geeigneten Ansprechpartner für Ihren internen Support an (z.B. Schließanlagenverwalter). Diese Informationen werden in den mobilen Schlüsseln in der AX2Go App angezeigt.

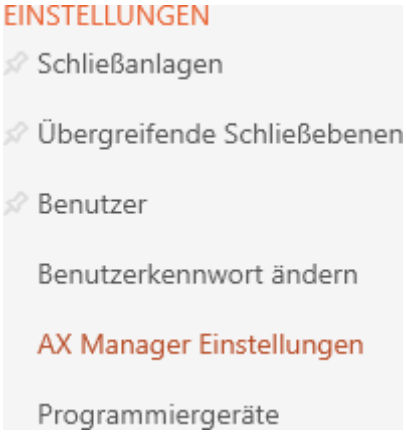
- Schlüsselname (z.B. Schließanlage oder Firmenname)
- Kontaktperson
- Unternehmen

- Adresse
- E-Mail
- Telefonnummer

Verändern der AX2Go-Einstellungen

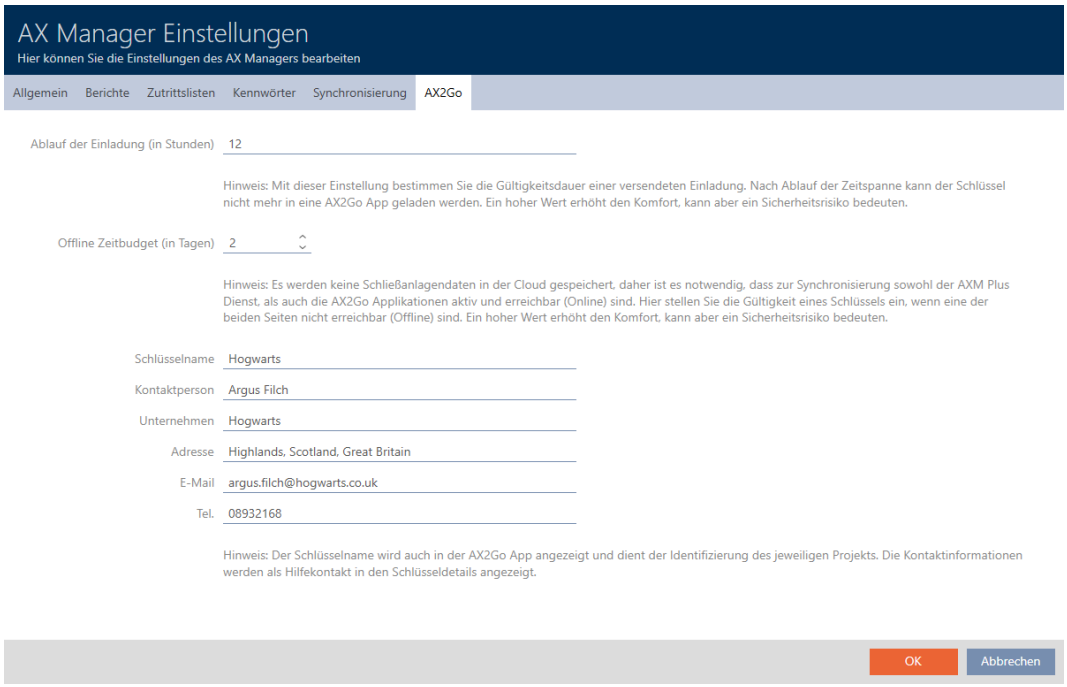
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.



   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.
3. Wechseln Sie zum Tab "AX2Go".

4. Legen Sie die gewünschten Einstellungen fest.



5. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

↳ Einstellungen für Ihre AX2Go sind festgelegt und werden für neue AX2-Go-Keys angewendet. Bestehende AX2Go-Keys erhalten das Update halbtäglich mit dem AXM-Dienst oder nach einer Änderung am AX2Go-Key.

22. Statistiken und Protokolle

22.1 Zutrittsliste einer Schließung anzeigen und exportieren

Mit der ZK-Funktion (=Zutrittskontrolle) können Ihre Schließungen protokollieren, welche Identmedien betätigt wurden (siehe *Zugänge durch Schließung protokollieren lassen (Zutrittsliste) [▸ 293]*). Anschließend können die protokollierten Zutritte zum Beispiel während der Synchronisierung ausgelesen und in die Datenbank geschrieben werden (siehe *Zutrittsliste/Begehungsliste während der Synchronisierung auslesen [▸ 459]* und *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*).

Die in der Datenbank vorhandene Zutrittsliste können Sie anzeigen und exportieren.

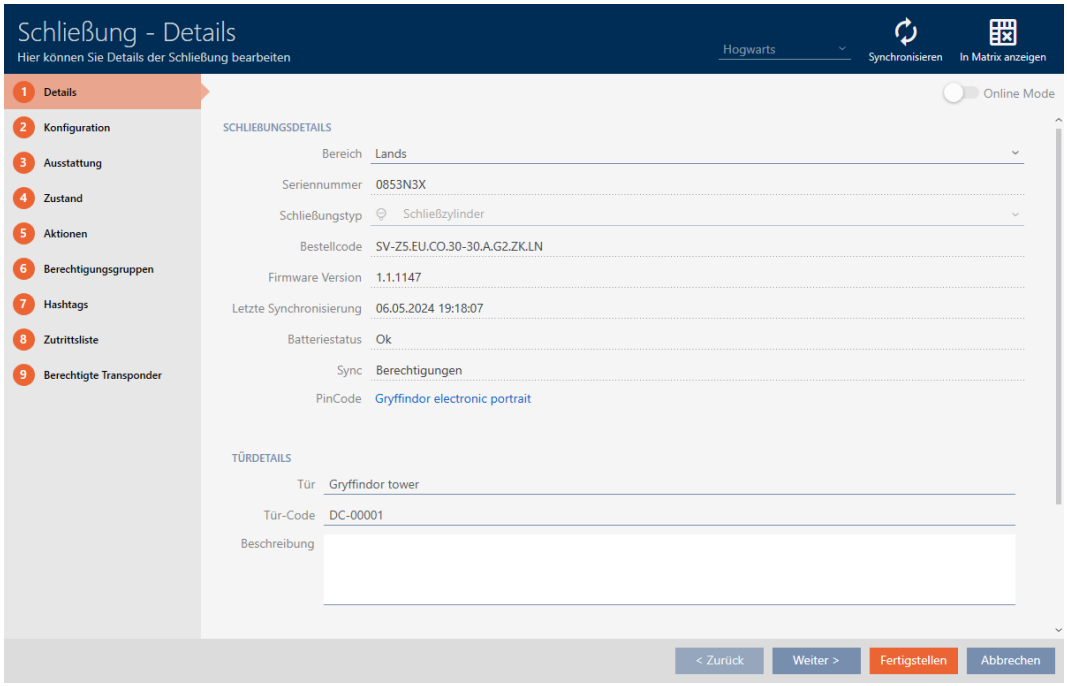
HINWEIS

Angezeigter Zustand entspricht letzter Synchronisation

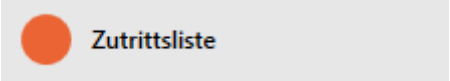
Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

✓ Schließung mindestens einmal synchronisiert.

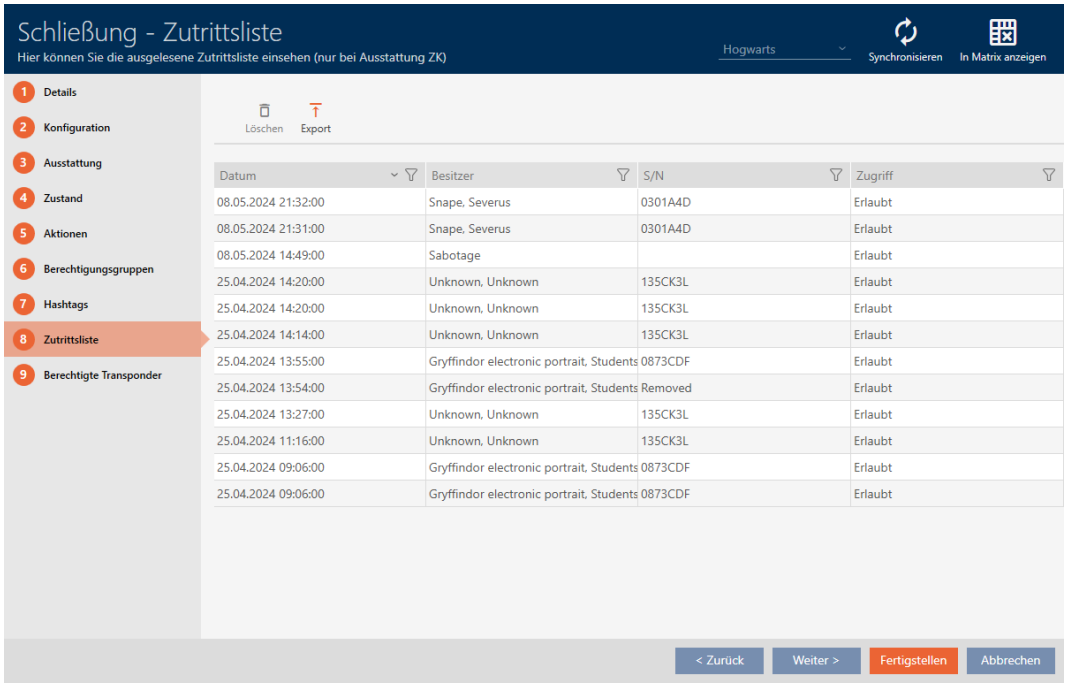
1. Klicken Sie auf die Schließung, deren Zutrittsliste Sie anzeigen wollen.
   ↳ Fenster der Schließung öffnet sich.



2. Klicken Sie auf den Reiter Zutrittsliste.



↳ Fenster wechselt zum Reiter "Zutrittsliste".
↳ Ausgelesene Zutrittsliste wird angezeigt (nur bei bereits synchronisierten Schließungen).



1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

2. Klicken Sie auf die Schaltfläche Export ↑.
   ↳ Explorer-Fenster öffnet sich.
3. Speichern Sie die exportierte Zutrittsliste in ein Dateiverzeichnis Ihrer Wahl.
   ↳ Explorer-Fenster schließt sich.

↳ Zutrittsliste wird exportiert.

Beispiel:

Simons Voss technologies

Zutrittsliste für die Schließung 'Gryffindor dormitory'

Datum	Besitzer	S/N	Zugriff	Schließungskomponente
14.12.2021 17:52:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 17:51:00	McGonagall, Minerva	UID-1000000034DB9B06	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
13.12.2021 20:32:00	##ServiceTId_IDS_AX_SETTIME		Erlaubt	Master

Simons Voss technologies Gedruckt am: 14.12.2021 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

22.2 Begehungsliste für Transponder/Karten anzeigen und exportieren

Ihre Identmedien können auf Wunsch protokollieren, an welchen Schließungen sie betätigt wurden (siehe *Zugänge durch Identmedium mitschreiben lassen (Begehungsliste) [▸ 125]*). Anschließend werden die gespeicherten Einträge in dieser Begehungsliste zum Beispiel während einer Synchronisation in die Datenbank übertragen (siehe *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*).

Die in der Datenbank gespeicherten Begehungslisten können Sie anzeigen und exportieren.

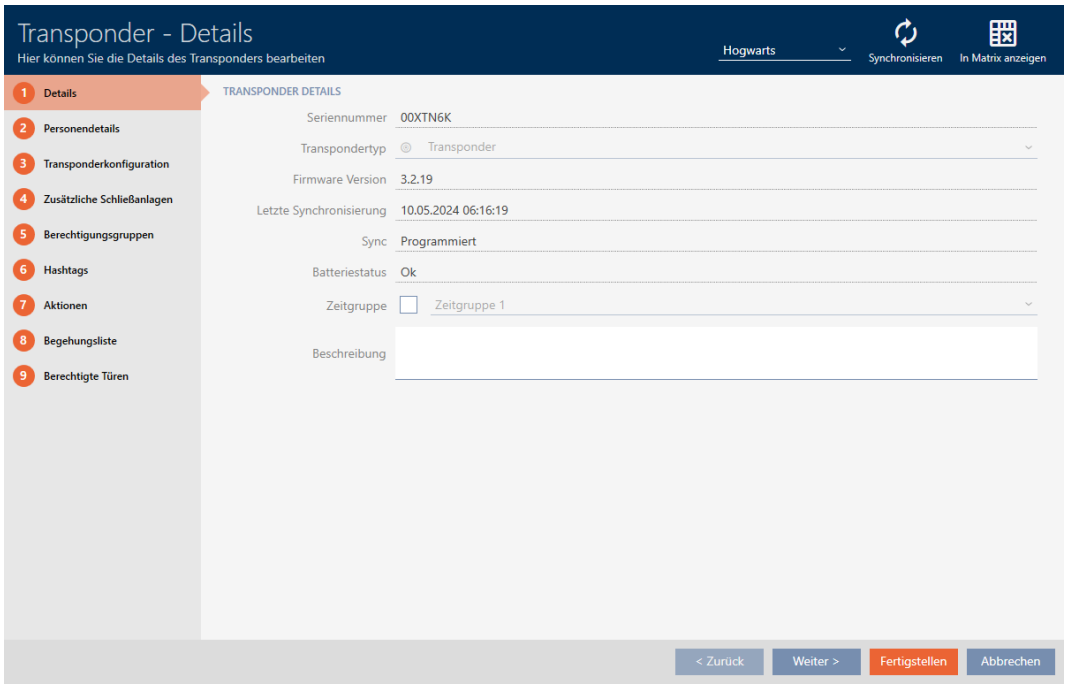
HINWEIS

Angezeigter Zustand entspricht letzter Synchronisation

Die AXM Plus zeigt an dieser Stelle den Zustand an, der in der Datenbank gespeichert ist.

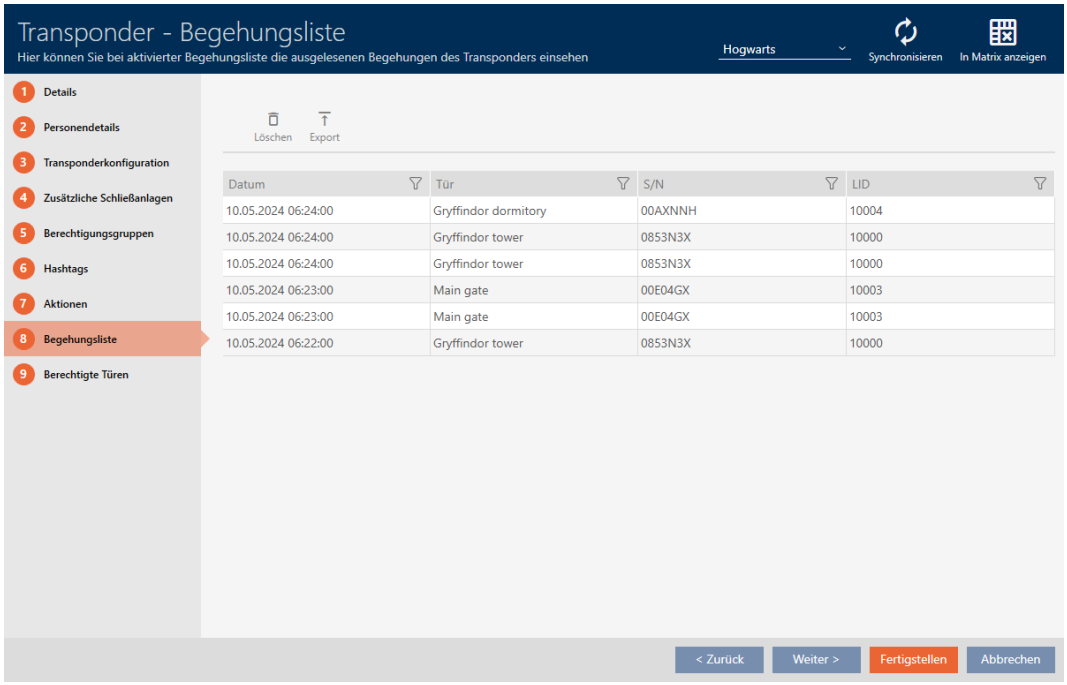
✓ Identmedium mindestens einmal synchronisiert.

1. Klicken Sie auf das Identmedium, dessen Begehungsliste Sie anzeigen wollen.
   ↳ Fenster des Identmediums öffnet sich.



2. Klicken Sie auf den Reiter Begehungsliste

   ↳ Fenster wechselt zum Reiter "Begehungsliste".



3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
4. Klicken Sie auf die Schaltfläche Export .
   ↳ Explorer-Fenster öffnet sich.
5. Speichern Sie die exportierte Begehungsliste in einem Dateiverzeichnis Ihrer Wahl.
   ↳ Explorer-Fenster schließt sich.

↳ Begehungsliste ist exportiert.

Begehungsliste für den Transponder Weasley '00XTN6K'

Datum	Tür	S/N	LID
10.05.2024 06:24:00	Gryffindor dormitory	00AXNNH	10004
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:22:00	Gryffindor tower	0853N3X	10000

Ausdruck vom: 10.05.2024 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

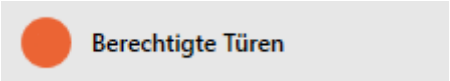
22.3 Türen anzeigen, an denen ein bestimmtes Identmedium berechtigt ist

Alternativ können Sie auch die an einer Tür berechtigten Identmedien anzeigen: *Identmedien anzeigen, die an einer bestimmten Tür berechtigt sind [▸ 516]*

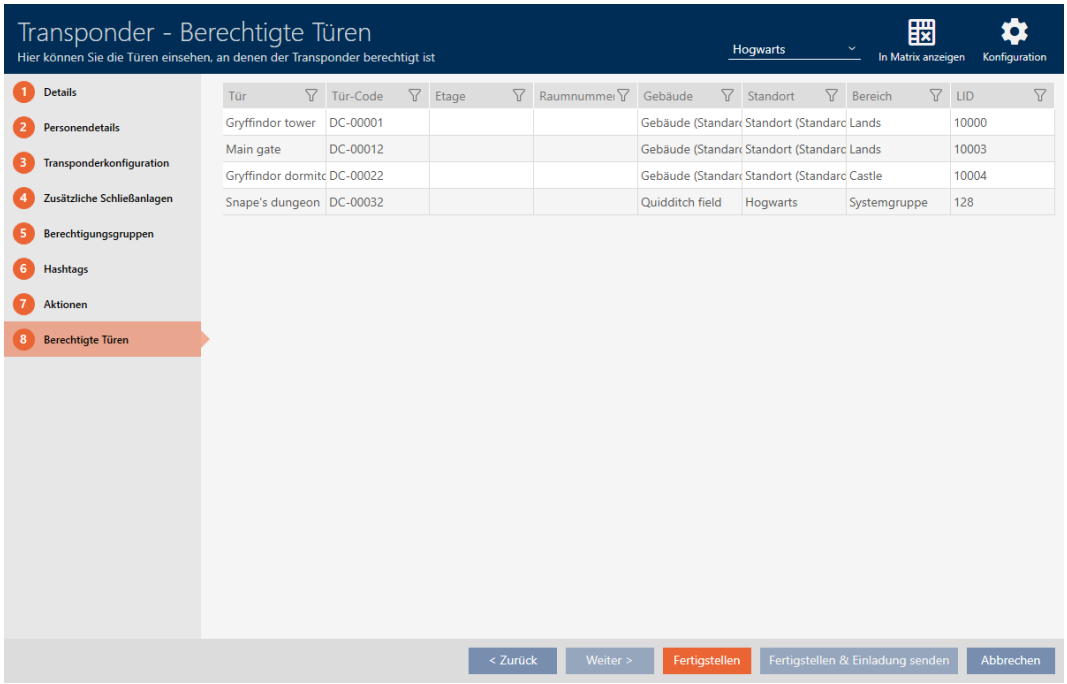
✓ Identmedium vorhanden.
✓ Schließung vorhanden.
✓ Identmedienliste oder Matrix geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie auf das Identmedium, bei dem Sie wissen wollen, an welchen Türen es berechtigt ist.
   ↳ Fenster des Identmediums öffnet sich.

3. Klicken Sie auf den Reiter Berechtigte Türen.



↳ Fenster wechselt zum Reiter "Berechtigte Türen".



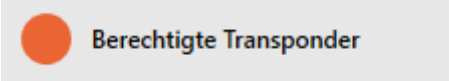
↳ Türen, an denen das Identmedium berechtigt ist, werden angezeigt.

22.4 Identmedien anzeigen, die an einer bestimmten Tür berechtigt sind

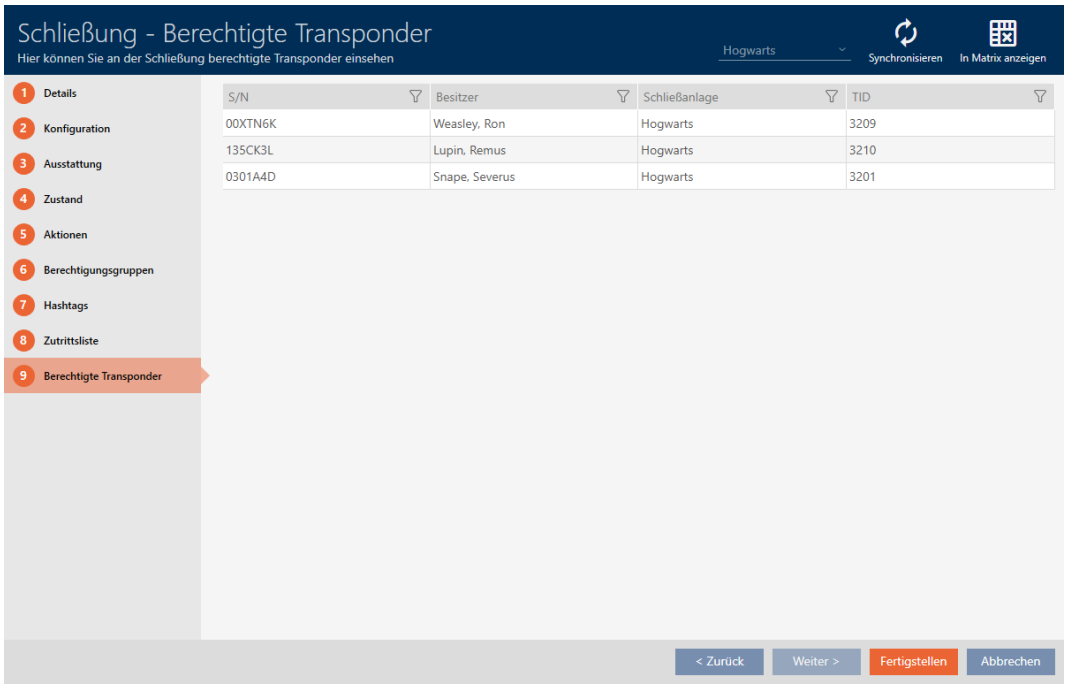
Alternativ können Sie auch die Türen anzeigen, an denen ein bestimmtes Identmedium berechtigt ist: *Türen anzeigen, an denen ein bestimmtes Identmedium berechtigt ist [▸ 515]*

✓ Identmedium vorhanden.
✓ Schließung vorhanden.
✓ Schließungsliste oder Matrixansicht geöffnet.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie auf die Schließung, deren berechtigte Identmedien Sie anzeigen wollen.
   ↳ Fenster der Schließung öffnet sich.
3. Klicken Sie auf den Reiter Berechtigte Transponder.



↳ Fenster wechselt zum Reiter "Berechtigte Transponder".



↳ Identmedien, die an der Tür berechtigt sind, werden angezeigt.

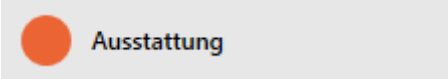
22.5 Ausstattungsmerkmale einer Schließung anzeigen

Während der Synchronisierung werden auch die Ausstattungsmerkmale einer Schließung ausgelesen. So kann die AXM Plus überprüfen, ob die Schließung die gewünschten Einstellungen überhaupt beherrscht (z.B. ob eine ZK-Funktion vorhanden ist).

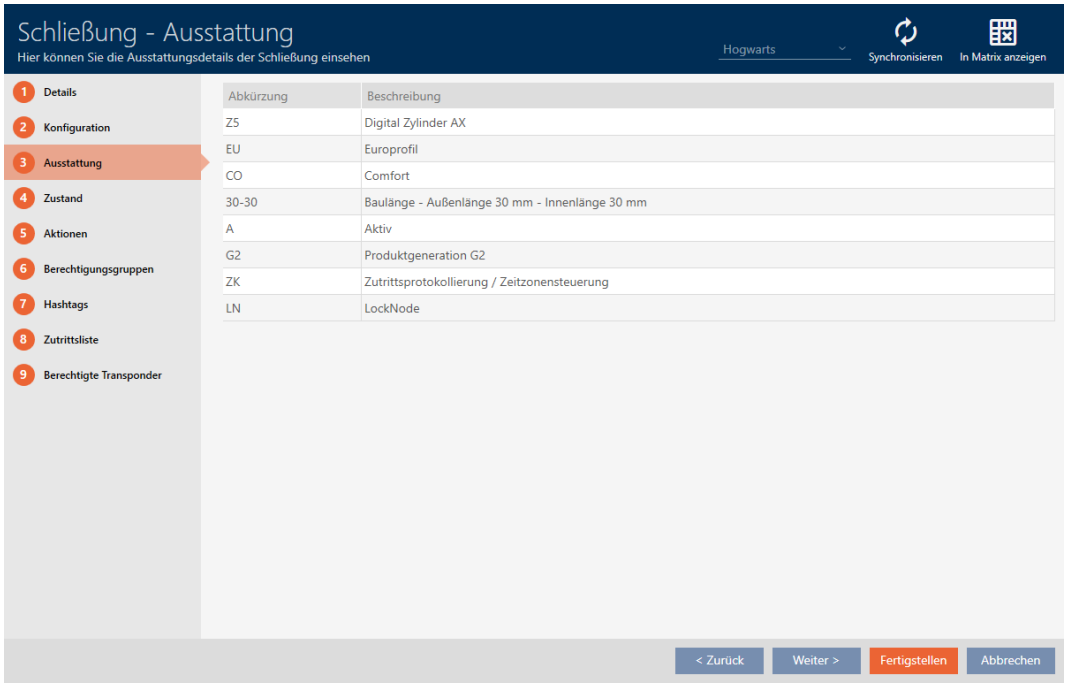
Sie können die ausgelesenen Ausstattungsmerkmale in der AXM Plus anzeigen:

✓ Schließung vorhanden.
✓ Schließungsliste oder Matrixansicht geöffnet.
✓ Schließung synchronisiert.

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie auf die Schließung, deren Ausstattungsmerkmale Sie anzeigen wollen.
   ↳ Fenster der Schließung öffnet sich.
3. Klicken Sie auf den Reiter ● Ausstattung.



↳ Fenster wechselt zum Reiter "Ausstattung".



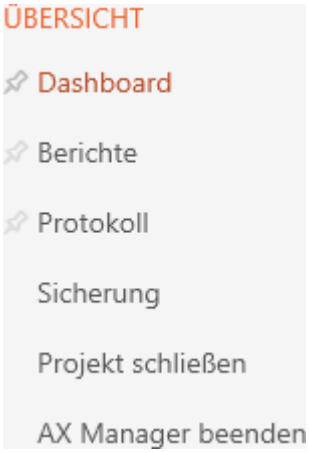
↳ Ausstattungsmerkmale werden angezeigt.

22.6 Statistiken und Warnungen anzeigen (Dashboard)

Die AXM Plus bringt ein neues Dashboard mit, das Ihnen auf einen Blick eine Statistik über Ihre Datenbank anzeigt.

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | ÜBERSICHT | den Eintrag Dashboard aus.

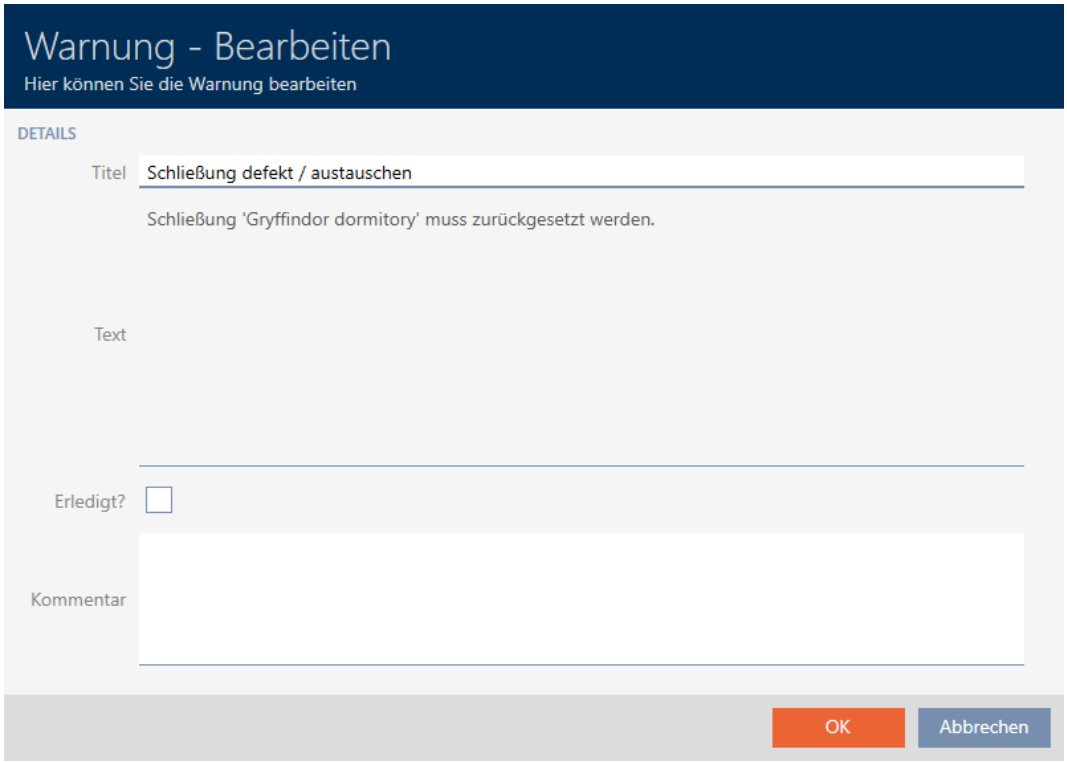


↳ AXM-Leiste klappt zu.
↳ Tab [Dashboard] öffnet sich.

↳ Dashboard wird angezeigt.

Auf der rechten Seite sehen Sie die Statistiken über Ihre Datenbank und auf der linken Seite werden Ihnen Warnungen angezeigt:

1. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
2. Klicken Sie in der Spalte Warnung auf den Eintrag der Warnung.
   ↳ Warnung öffnet sich.



3. Ändern Sie ggfs. die Felder *Titel* und *Text* nach Bedarf.
4. Erledigen Sie ggfs. die Warnung. Kehren Sie dann zur Warnung zurück und aktivieren Sie die Checkbox ☑ Erledigt?.
5. Geben Sie im Feld *Kommentar* ggfs. etwas ein.
6. Klicken Sie auf die Schaltfläche OK.
   ↳ Warnung schließt sich.

↳ Warnung erscheint im Dashboard mit einem Haken als erledigt.

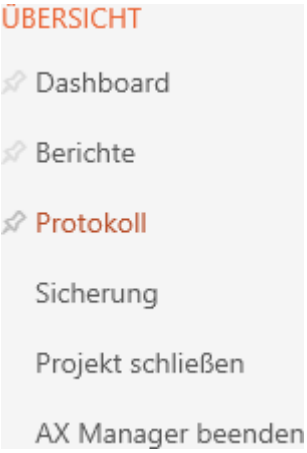
22.7 Aktivitäten an der Datenbank nachverfolgen (Protokoll)

In der AXM Plus wird jede Änderung und jede Einstellung an der Datenbank protokolliert. So können Sie immer nachvollziehen, wer wann was an der Datenbank verändert hat.

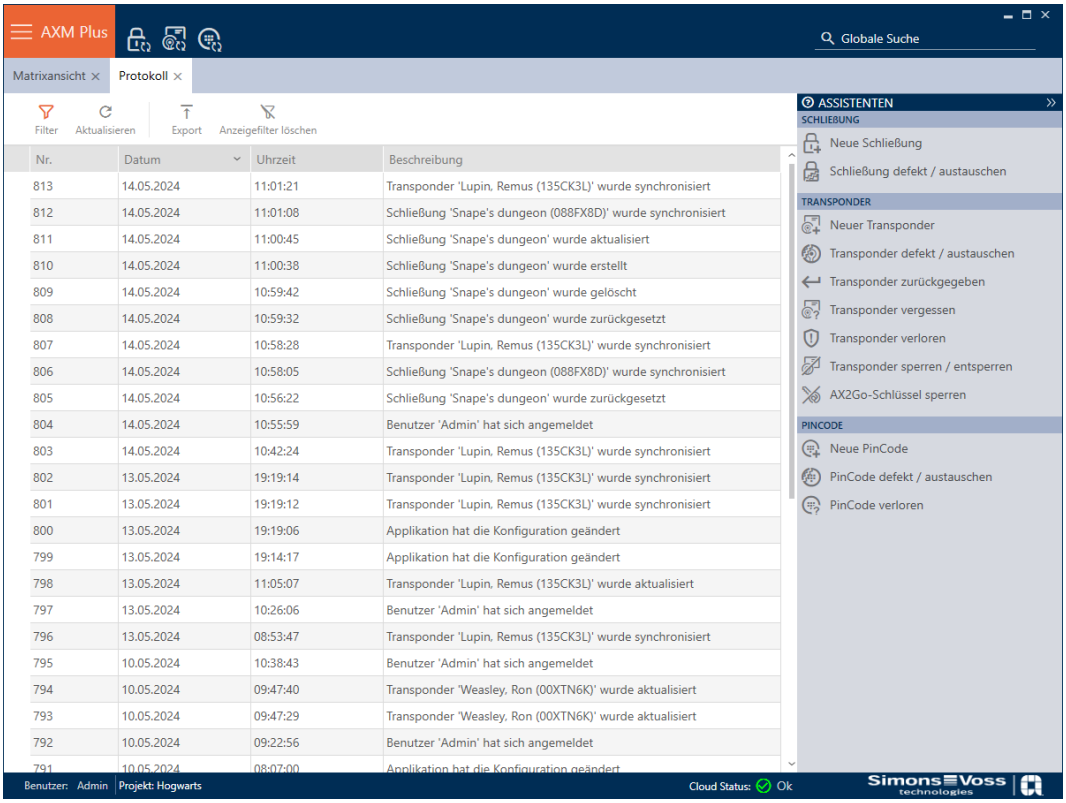
Die Archivierungsdauer des Protokolls ist einstellbar (siehe *Archivierungsdauer des Protokolls einstellen [▸ 522]*).

1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | ÜBERSICHT | den Eintrag Protokoll aus.



↳ AXM-Leiste klappt zu.
↳ Tab [Protokoll] öffnet sich.



3. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).

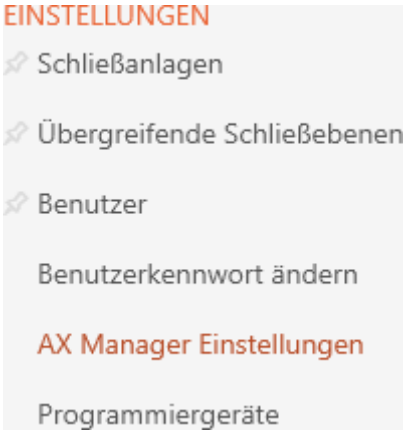
↳ Protokoll wird angezeigt.

Mit der Schaltfläche Exportieren ⤒ haben Sie auch die Möglichkeit, das Protokoll zu exportieren und so dauerhaft zu sichern.

22.7.1 Archivierungsdauer des Protokolls einstellen

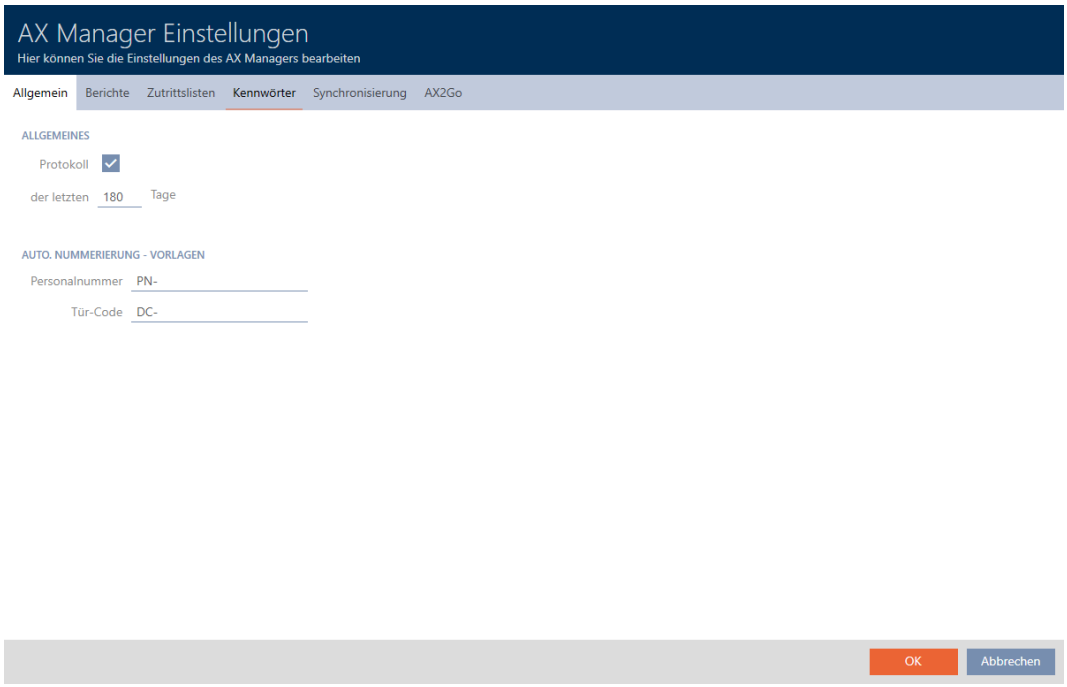
1. Klicken Sie auf die orangene AXM-Schaltfläche AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | EINSTELLUNGEN | den Eintrag AX Manager Einstellungen aus.



   ↳ AXM-Leiste klappt zu.
   ↳ Fenster mit den Einstellungen der AXM Plus öffnet sich.

3. Wechseln Sie zum Tab [Allgemein].



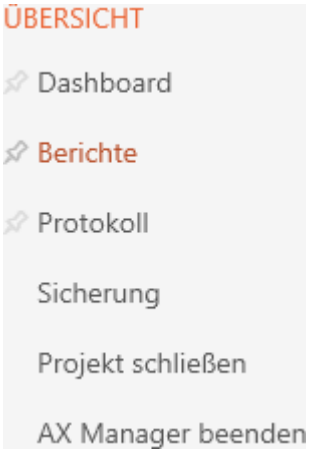
4. Falls Sie die Änderungen an der Datenbank gar nicht protokollieren wollen: Deaktivieren Sie die Checkbox ☐ Protokoll.
5. Geben Sie die gewünschte Archivierungsdauer ein (max. 670 Tage).
6. Klicken Sie auf die Schaltfläche OK.
   ↳ Fenster mit den Einstellungen der AXM Plus schließt sich.

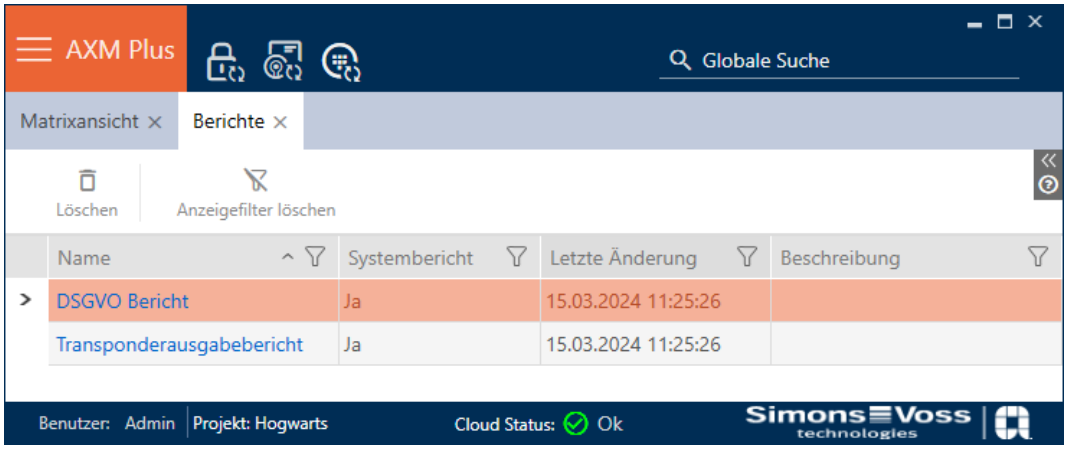
↳ Protokoll wird auf die gewünschte Dauer begrenzt.

22.8 Berichte

Berichte sind ein nützliches Werkzeug, mit dem Sie immer jederzeit Ihre Schließanlage im Blick haben.

Einige dieser Berichte (nämlich die Systemberichte) finden Sie im Tab [Berichte]:





In diesem Tab können Sie die Berichte aber nicht ausgeben. Stattdessen haben Sie die Möglichkeit, in den Feldern *Name* und *Beschreibung* eigene Werte einzugeben. Eingaben im Feld *Name* werden als Überschrift in den jeweiligen Bericht übernommen.

Die eigentlichen Berichte können Sie an den jeweiligen sinnvollen Stellen in der AXM Plus ausgeben.

Beispiel: Den Datenschutzbericht finden Sie an mehreren Stellen.

- Im Identmedien-Fenster beim Reiter "Personendetails" unter der Schaltfläche DSGVO-Daten.
- Im Tab [Transponder] unter der Schaltfläche DSGVO-Daten.

22.8.1 Bericht zur Identmedien-Ausgabe ausgeben

Mit diesem Bericht können Sie nachweisen, dass jemand von Ihnen ein bestimmtes Identmedium und eine Einweisung erhalten hat.

Daher können Sie diesen Bericht nur für genau ein ausgewähltes Identmedium gleichzeitig exportieren.

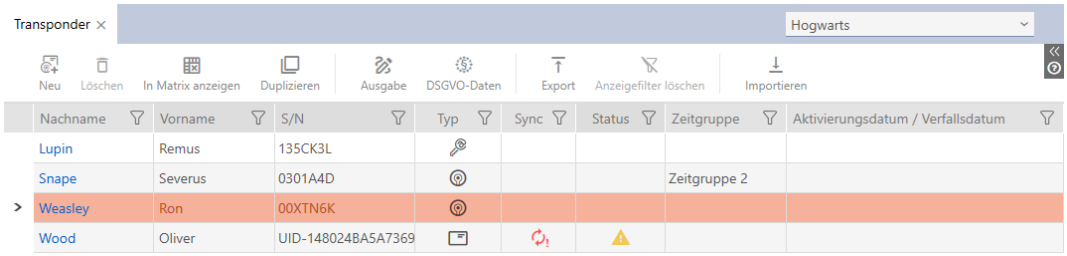
Als Schließanlagenbetreiber können Sie somit die TID festhalten und sich absichern. Auf dem Bericht sind dafür Unterschriftsfelder vorgesehen.

Der Bericht enthält folgende Daten:

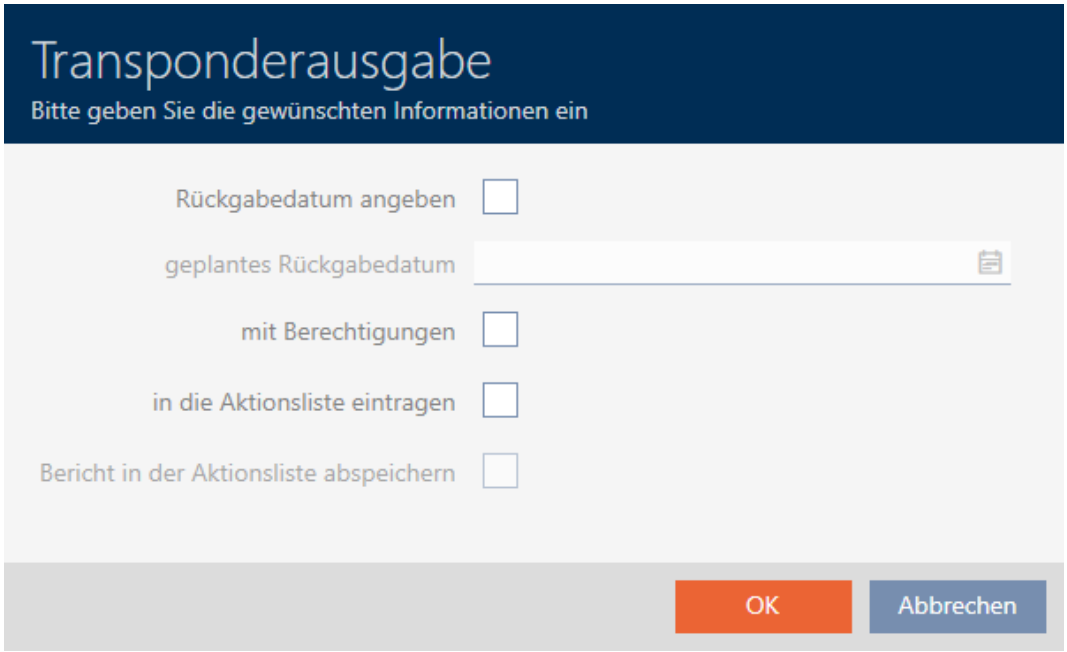
- Name der Person, die das Identmedium erhalten hat
- Seriennummer des ausgegebenen Identmediums
- Telefonnummer des Schließanlagenverwalters (Quelle: AX-Manager Einstellungen, siehe *Berichte und Exporte personalisieren [▸ 465]*)
- E-Mail-Adresse des Schließanlagenverwalters (Quelle: AX-Manager Einstellungen, siehe *Berichte und Exporte personalisieren [▸ 465]*)
- Adresse des Schließanlagenverwalters
- Datum, an dem der Bericht erstellt wurde
- Optional: Geplantes Rückgabedatum
- Optional: Berechtigungen (inkl. Bereichen)

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.
   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Transponder] öffnet sich.
3. Wechseln Sie ggfs. im Dropdown-Menü rechts oben zur Schließanlage, die das gewünschte Identmedium enthält.
4. Sortieren/Filtern Sie ggfs. die angezeigten Einträge mit ▽ (siehe *Sortieren und Filtern [▸ 49]*).
5. Markieren Sie das Identmedium, das Sie ausgeben wollen.
   ↳ Markierte Zeile wird orange eingefärbt.



6. Klicken Sie auf die Schaltfläche Ausgabe.
   ↳ Fenster "Transponderausgabe" öffnet sich.



7. Wenn Sie ein ggfs. festgelegtes Rückgabedatum mit ausgeben wollen: Aktivieren Sie die Checkbox ☑ Rückgabedatum angeben und wählen Sie das Rückgabedatum mit einem Klick auf den Kalender aus.
8. Wenn Sie ggfs. vorhandene Berechtigungen mit ausgeben wollen: Aktivieren Sie die Checkbox ☑ mit Berechtigungen.
9. Wenn Sie die Ausgabe des Identmediums auch in dessen Aktionsliste eintragen wollen: Aktivieren Sie die Checkbox ☑ in die Aktionsliste eintragen und speichern Sie mit der Checkbox ☑ Bericht in der Aktionsliste abspeichern ggfs. auch den dazugehörenden in der Aktionsliste (Zur Aktionsliste siehe auch *Identmediums-Verwaltungsaufgaben planen und nachverfolgen* *[▸ 182]*).
10. Klicken Sie auf die Schaltfläche OK.
    ↳ Fenster "Transponderausgabe" schließt sich.
    ↳ Explorer-Fenster öffnet sich.
11. Speichern Sie die PDF-Datei in einem Dateiverzeichnis Ihrer Wahl.
    ↳ Ausgabe-Bericht zum ausgewählten Identmedium wird als PDF-Datei (DIN A4) exportiert.

SimonsVoss technologies

Transponderausgabe

Weasley, Ron / 6

Ich bestätige hiermit, dass ich heute den Transponder mit der nachfolgend aufgeführten Seriennummer erhalten habe und die üblichen Sicherheitsvorkehrungen beim Benutzen und Aufbewahren beachten werde.

Seriennummer: **00XTN6K**

* Bei Verlust des Transponders ist die zuständige Schließanlagenverwaltung sofort zu informieren.
* Eine Weitergabe an Dritte ist unzulässig.
* Der Transponder ist beim Austritt des Mitarbeiters wieder an die Schließanlagenverwaltung zurückzugeben.

Eintragungen im obigen Textfeld beruhen auf betrieblichen Vereinbarungen/Vorgaben der Betreibergesellschaft. Die SimonsVoss Technologies GmbH übernimmt keine Gewähr für diese Angaben

14.05.2024 _____
Weasley, Ron

zurückgenommen: _____

SimonsVoss technologies Ausdruck vom: 14.05.2024 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

Zusätzlich können Sie auch das Ausgabedatum direkt in der Aktionsliste des jeweiligen Identmediums vermerken (siehe *Transponder-/Karten-Ausgabedatum notieren [▸ 183]*).

22.8.2 Datenschutzbericht (DSGVO) ausgeben

Der Datenschutzbericht (=DSGVO Bericht) informiert Sie darüber, welche personenbezogenen Daten zu einer Person in der AXM Plus gespeichert sind. Diesen Bericht können Sie für mehrere Personen gleichzeitig ausgeben. Dabei wird für jede Person eine eigene PDF-Datei exportiert.

Mit dem vorhandenen Unterschriftsfeld kann der Bericht bestätigt werden.

Er setzt sich aus folgenden Abschnitten zusammen:

Personendetails

Personendetails

Titel	Junior Assistant
Vorname	Percy
Nachname	Weasley
Personalnummer	PN-30
Abteilung	Department of International Magical Cooperation
Telefon	+44 020 3492 32113 85
E-Mail	pweasley@ministryofmagic.com
Adresse	Whitehall London, England Great Britain
Ort/Debäude	Ministry
Eingestellt am	03.02.2010 00:00:00
Eingestellt bis	11.02.2022 00:00:00
Geburtsdatum	07.06.2000 00:00:00
Kostenstelle	57324

Dieser Abschnitt enthält die gespeicherten personenbezogenen Daten.

- Vorname
- Nachname
- Personalnummer
- Telefon
- E-Mail
- Adresse

Einträge, die in der AXM Plus leer sind, werden im Bericht automatisch ausgeblendet.

Personenhistorie

Personenhistorie

Personalnummer	Datum	Vorname	Nachname
PN-30	14 Dezember 2021 1:20	Fred	Weasley
PN-30	14 Dezember 2021 1:32	Percy	Weasley

Dieser Abschnitt protokolliert die Änderungen an folgenden Daten:

- Vorname
- Nachname
- Personalnummer

Protokoll

Protokoll

Nr.	Datum	Uhrzeit	Beschreibung
1661	14 Dezember 2021	18:55:18	Transponder 'Weasley, Percy (000XCKNG)' wurde aktualisiert
1662	14 Dezember 2021	18:55:37	Transponder 'Weasley, Percy (000XCKNG)' wurde synchronisiert
1663	14 Dezember 2021	19:27:05	Transponder 'Weasley, Percy (000XCKNG)' wurde Zugriffsliste wurden synchronisiert
1672	03 Januar 2022	18:40:47	Transponder 'Weasley, Percy (000XCKNG)' wurde aktualisiert

Dieser Abschnitt ist ein Änderungsprotokoll. Hier werden alle Einträge der Datenbank ausgegeben, die diese Person bzw. deren Identmedium betreffen (siehe auch *Aktivitäten an der Datenbank nachverfolgen (Protokoll) [▸ 520]*).

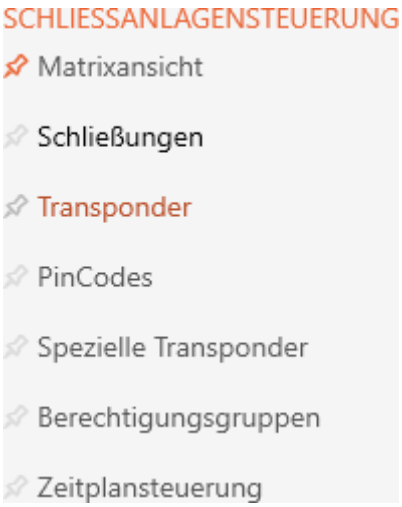
HINWEIS

Ausgabe benutzerdefinierter Felder

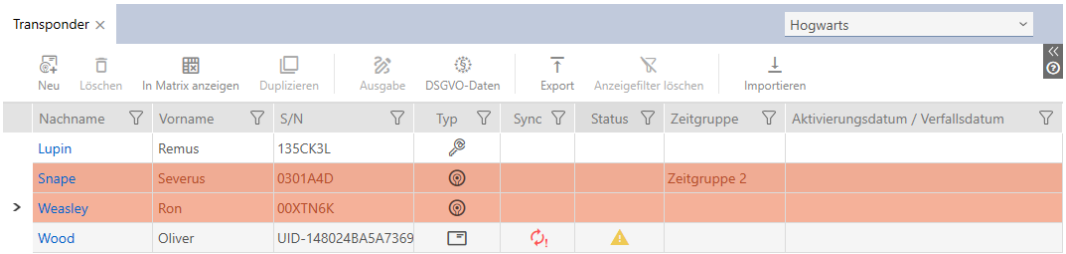
Sie können bei den Personendetails auch benutzerdefinierte Felder erstellen (siehe *Eigenschaften für Personendetails personalisieren [▸ 469]*). Diese werden dann ebenfalls ausgegeben.

1. Klicken Sie auf das orangene AXM-Symbol AXM.
   ↳ AXM-Leiste klappt auf.

2. Wählen Sie in der Gruppe | SCHLIESSANLAGENSTEUERUNG | den Eintrag Transponder aus.



   ↳ AXM-Leiste klappt zu.
   ↳ Tab [Transponder] öffnet sich.
3. Wechseln Sie ggfs. im Dropdown-Menü rechts oben zur Schließanlage, die das gewünschte Identmedium enthält.
4. Markieren Sie ein oder mehrere Identmedien, deren Datenschutzberichte Sie ausgeben wollen.
   ↳ Markierte Zeilen werden orange eingefärbt.



5. Klicken Sie auf die Schaltfläche DSGVO-Daten.
   ↳ Explorer-Fenster öffnet sich.
6. Speichern Sie den Bericht in einem Verzeichnis Ihrer Wahl.
   ↳ Datenschutzbericht wird als PDF (DIN A4) exportiert.
   ↳ Wenn Sie mehrere Identmedien markiert haben, dann öffnet sich das Explorer-Fenster sofort wieder und Sie können den nächsten Bericht abspeichern.

Simons Voss technologies

DSGVO-Bericht

Personendetails

Vorname	Ron
Nachname	Weasley
Personalnummer	PN-6
Abteilung	Pupils
Telefon	08932168
E-Mail	ron.weasley@hogwarts.co.uk
Adresse	The Burrow Devon
Ort/Gebäude	Gryffindor rooms
Kostenstelle	310
Büronr.	23523

Personenhistorie

Personalnummer	Datum	Vorname	Nachname
PN-6	10.05.2024 07:37	Ron	Weasley

Protokoll

Nr.	Datum	Uhrzeit	Beschreibung
775	10.05.2024	04:06	Transponder 'Weasley, Ron' wurde zurückgesetzt
776	10.05.2024	04:08	Transponder 'Weasley, Ron (00XTN6K)' wurde synchronisiert
777	10.05.2024	04:15	Transponder 'Weasley, Ron (00XTN6K)' wurde aktualisiert

14.05.2024 _____

Simons Voss technologies Ausdruck vom: 14.05.2024 1

Sie haben die Möglichkeit, Berichte zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

Weitere generelle Informationen zum Datenschutz im System 3060 siehe *Informationen zum Datenschutz [▸ 15]*.

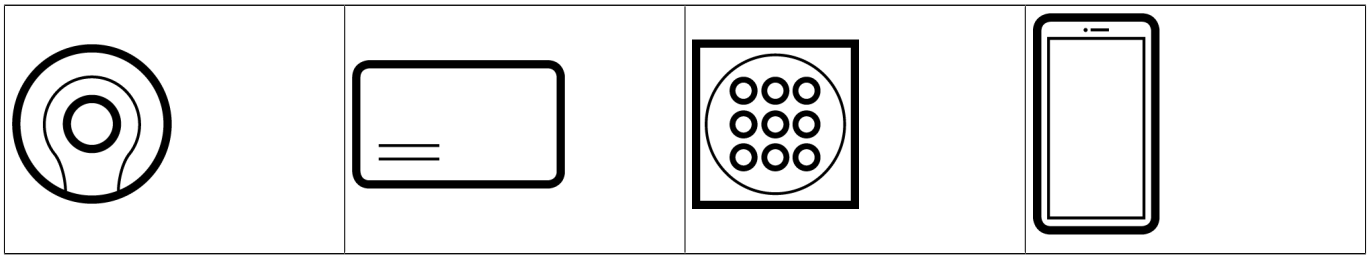
23. Hintergrundwissen und Erklärungen

23.1 Identmedien, Schließungen und der Schließplan

Über Identmedien

Unter dem Sammelbegriff Identmedium versteht man alle Komponenten, mit denen sich eine Person an einer Schließung ausweisen kann. Dazu gehören in erster Linie:

- Transponder
- Karten (SmartCard)
- Tags (SmartTag)
- PinCode-Tastaturen
- AX2Go-App auf Smartphone



Identmedien können mit folgenden Technologien kommunizieren:

- Aktiv-Technologie (25 kHz)
- Passiv-Technologie (RFID, 13,56 MHz)
- Bluetooth Low Energy (BLE, 2,4 GHz)
- Aktive Identmedien (= Transponder, PinCode-Tastatur 3068) haben eine Batterie und können selbst (aktiv) die Kommunikation mit einer Schließung beginnen.
- Passive Identmedien (= Karten, Tags) haben keine Batterie und müssen durch die Schließung durch ein Induktionsfeld mit Strom versorgt werden. Erst dann können Sie mit der Schließung kommunizieren.
- Identmedien mit BLE (= PinCode-Tastatur AX und AX2Go) haben wie aktive Identmedien eine Batterie, kommunizieren aber über BLE mit der Schließung.

Je nach Anwendung bietet jede dieser Technologien Vorteile.

Ihre Transponder und Karten haben zwei Nummern, die wichtig sind:

- Seriennummer (fest im Identmedium gespeichert, wird während der Synchronisierung ausgelesen)
- TID (flexibel durch AXM Plus vergeben, wird während der Synchronisierung auf das Identmedium geschrieben)

Die Seriennummer ist eine für jedes Identmedium einzigartige Nummer, während die TID nur in Ihrer Schließanlage einzigartig ist.

Während der Synchronisierung wird in der Datenbank eine Verknüpfung zwischen der ausgelesenen Seriennummer und der TID (=Transponder-ID) hergestellt. Die AXM Plus weiß also, welche Seriennummer und welche TID zusammengehören.

		TID
Seriennummer	002TU6TC	3203

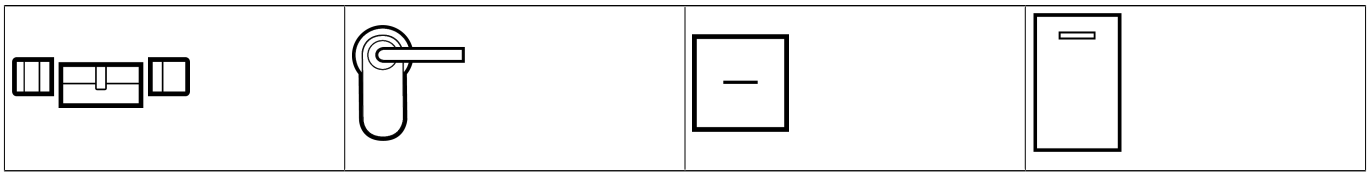
Diese Verknüpfung bleibt aber in der AXM Plus und wird nicht auf Identmedien oder Schließungen geschrieben. Eine Schließung prüft mit der TID (und nicht mit der Seriennummer), ob ein Identmedium berechtigt ist oder nicht.

In der Praxis haben passive Identmedien physikalisch bedingt Einschränkungen (siehe *Karten und Schließungs-IDs [▸ 573]*).

Über Schließungen

Unter dem Sammelbegriff Schließungen versteht man alle Komponenten, die mit einem Identmedium "betätigt" werden. Schließungen werden in der Regel in eine Tür eingebaut (außer SmartRelais). Zu Schließungen gehören in erster Linie:

- Schließzylinder
- SmartHandles
- SmartRelais
- SmartLocker



Auch Schließungen können mit mehreren Technologien mit den Identmedien kommunizieren:

- Aktiv
- Passiv
- BLE

Wichtig ist, dass die verwendeten Technologien zusammenpassen. Eine passive Schließung kann normalerweise nicht mit einem aktiven Identmedium geöffnet werden, sondern nur mit einem passiven.

Jede Schließung hat - ähnlich wie ein Identmedium auch - zwei wichtige Nummern:

S/N	Schließungs ID
000C1957	129
000DSP7E	128
000E04GX	10000
000DC331	10001

- Seriennummer (fest in der Schließung gespeichert, wird während der Synchronisierung ausgelesen)
- Schließungs-ID (abgekürzt LID für Lock-ID, flexibel durch AXM Plus vergeben, wird während der Synchronisierung auf die Schließung geschrieben)

Während der Synchronisierung wird in der Datenbank eine Verknüpfung zwischen der ausgelesenen Seriennummer und der LID hergestellt. Die AXM Plus weiß also, welche Seriennummer und welche LID zusammengehören. Diese Verknüpfung bleibt aber in der AXM Plus und wird nicht auf Identmedien oder Schließungen geschrieben. Eine Schließung prüft mit der TID (und nicht mit der Seriennummer), ob ein Identmedium berechtigt ist oder nicht.

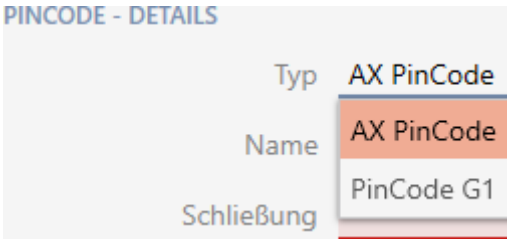
Normalerweise brauchen Sie sich mit TID und LID nicht zu beschäftigen, da Ihre AXM Plus alles im Hintergrund erledigt.

Über den Schließplan

Im Schließplan wird stark vereinfacht gesagt die Matrix abgebildet und gespeichert. Er enthält unter anderem die Berechtigungen. Dank des Schließplans wissen Schließungen und Identmedien, wer aneinander berechtigt ist.

23.1.1 PinCode G1 vs. PinCode AX

Die AXM Plus bietet Ihnen zwei verschiedene PinCode-Tastaturen an:



- PinCode-Tastatur 3068

- PinCode-Tastatur AX

Diese beiden PinCode-Tastaturen sind äußerlich fast gleich. Sie erkennen die PinCode-Tastatur AX an einem Bluetooth-Symbol:

Die Programmierung und die verwendete Schnittstelle sind allerdings unterschiedlich:

	PinCode-Tastatur AX	PinCode-Tastatur 3068
Schnittstelle	BLE (=Bluetooth Low Energy)	Aktiv (=25 kHz) mit G1-Protokoll
Reichweite	Gute Reichweite an AX-Schließungen	Gute Reichweite an Nicht-AX-Schließungen Geringere Reichweite an AX-Schließungen
Vergabe der PINs	Programmierung der PINs direkt in der AXM Plus Login in der AXM Plus als Legitimation für Programmierung	Programmierung der PINs direkt an der PinCode-Tastatur 3068 Aufteilung in eine Master-PIN und bis zu drei User-PINs Master-PIN als Legitimation für Programmierung

	PinCode-Tastatur AX	PinCode-Tastatur 3068
Synchronisation	Ihre AXM Plus unterstützt Sie beim Synchronisieren mit Anweisungen. Der Ablauf in Kurzform: 1. Synchronisation starten. 2. 0 für mindestens zwei Sekunden gedrückt halten, um in den Programmiermodus zu gehen. 3. Warten, bis Synchronisation abgeschlossen ist.	Ihre AXM Plus unterstützt Sie beim Synchronisieren mit Anweisungen. Der Ablauf in Kurzform: 1. Master-PIN an der PinCode-Tastatur 3068 erstellen. 2. An PinCode-Tastatur 3068 mit Master-PIN die User-PINs erstellen. 3. Synchronisation starten. An PinCode-Tastatur 3068 00 und Master-PIN eingeben. 4. In AXM Plus mit Synchronisation fortfahren. 5. An PinCode-Tastatur 3068 die Taste der entsprechenden User-PIN eingeben (z.B. 1 für die erste User-PIN). 6. Warten, bis Synchronisation abgeschlossen ist.

Verhalten bei erster Synchronisation, zusätzlichen PINs und Berechtigungsänderungen

Ein wesentlicher Unterschied zwischen der PinCode-Tastatur AX und der PinCode-Tastatur 3068 ist auch das Verhalten bei der ersten Synchronisation und bei Berechtigungsänderungen.

Dieser Unterschied liegt an der unterschiedlichen Kommunikation der beiden PinCode-Tastaturen mit der Schließung:

- PinCode-Tastatur AX: Verwendet einen fest zugeordneten BLE-Kanal, um Informationen an die Schließung zu senden.

  Eine solche Information könnte zum Beispiel "Eingegebene PIN berechtigt" sein.
- PinCode-Tastatur 3068: Verwendet das G1-Protokoll und für jede PIN eine eigene G1-ID.

	PinCode-Tastatur AX	PinCode-Tastatur 3068
Erste Synchronisation	Der fest zugeordnete BLE-Kanal muss sowohl für die PinCode-Tastatur AX als auch für die Schließung eingerichtet werden. Dies geschieht im Hintergrund bei der Zuordnung einer PinCode-Tastatur AX. Daher entsteht nach der Zuordnung einer PinCode-Tastatur AX **Programmierbedarf an der PinCode-Tastatur und an der Schließung**.	Die PinCode-Tastatur 3068 erhält eine G1-ID pro PIN und die Schließung erhält einen Schließplan mit der Information, ob diese G1-ID berechtigt ist. Daher entsteht nach der Zuordnung einer PinCode-Tastatur 3068 **Programmierbedarf an der PinCode-Tastatur und an der Schließung.**
Zusätzliche PINs	Neue PINs werden in der PinCode-Tastatur AX gespeichert. Der bereits eingerichtete BLE-Kanal wird unverändert weiterhin für Befehle an die Schließung genutzt. Der PinCode-Tastatur AX werden die neuen PINs mitgeteilt, deshalb entsteht nur **Programmierbedarf an der PinCode-Tastatur**.	Neue PINs werden in der PinCode-Tastatur 3068 mit einer G1-ID pro PIN gespeichert. Diese G1-ID wird anschließend im Schließplan als berechtigt gespeichert. Die neuen G1-IDs werden der PinCode-Tastatur 3068 mitgeteilt und der geänderte Schließplan wird in der Schließung gespeichert. Daher entsteht **Programmierbedarf an der PinCode-Tastatur und an der Schließung**.
Berechtigungsänderungen	Die PinCode-Tastatur AX nutzt den bereits eingerichteten Kanal unverändert weiterhin für Befehle an die Schließung. Deshalb muss die AXM Plus nur der PinCode-Tastatur AX mitteilen, wann sie z.B. die Information "Eingegebene PIN berechtigt" an die Schließung senden soll. Es entsteht nur **Programmierbedarf an der PinCode-Tastatur**.	Die PinCode-Tastatur 3068 behält unverändert die G1-ID. Die geänderte Berechtigung wird im Schließplan in der Schließung gespeichert. Daher entsteht nur **Programmierbedarf an der Schließung**.

23.1.2 AX2Go

23.1.2.1 Allgemein

AX2Go ist ein mobiler Schlüssel zum Öffnen von digitalen Schließkomponenten von SimonsVoss über Bluetooth Low Energy (BLE). Bei Bluetooth Low Energy handelt es sich um einen Funkstandard, der Bluetooth-Verbindungen auch mit geringen Sendeleistungen und geringem Stromverbrauch möglich macht.

Sind die Schließberechtigungen in der App hinterlegt, kann das Smartphone wie eine Zutrittskarte oder ein Transponder genutzt werden. So einfach geht es: Smartphone entsperren, die Schließung damit berühren und die Tür öffnen. Die AX2Go App läuft im Hintergrund und muss dafür nicht aufgerufen werden.

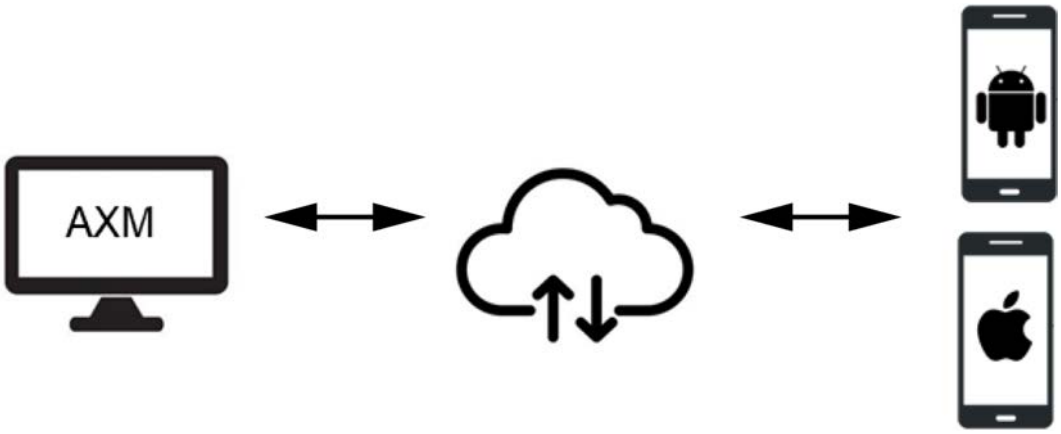
Funktionen

- Bis zu 5 unterschiedliche Schließanlagen (AX2Go-Schlüssel) auf einem Smartphone
- Schlüsselberechtigungen übertragen via **E-Mail**, **SMS** oder **QR-Code** aus dem **AX Manager** (Verwaltungssoftware)
- Einfaches Einrichten macht die App in weniger als einer Minute startbereit
- Übersichtlicher Zutrittsstatus und schnelle Lösungshilfe
- Keine Registrierung oder Verifizierung nötig

23.1.2.2 Synchronisation der AX2Go-Schlüssel über die Cloud

Sie verteilen Änderungen wie Berechtigungen, Zeit, etc. komfortabel über eine Cloudverbindung an Ihre AX2Go-Nutzer.

Die SimonsVoss-Cloud **überträgt** die Daten von Ihrer AXM Plus zur AX2Go, **ohne** dass Daten in der SimonsVoss-Cloud **gespeichert** werden (Tunnel, keine ruhenden Kundendaten).



Die AX2Go nutzt eine direkte Verbindung über Bluetooth Low Energy (=BLE-Kanal). Für die Nutzung dieses BLE-Kanals muss die Firmware der Schließung die Version 1.1.1148 oder neuer haben. Mit einem dafür bereitgestellten vereinfachten Patchtool können Sie die Firmware selbst aktualisieren (außer bei direkt vernetzten Schließungen = WaveNet).

Datenübertragung

Ein AX2Go-Schlüssel ist prinzipiell ein virtueller G2-Transponder auf dem Smartphone. Wie bei einem normalen G2-Identmedium können Sie sich auch hier aussuchen, ob Sie lieber die Schließung oder den AX2Go-Schlüssel synchronisieren. Durch die Cloud-Verbindung ist Ihre AXM Plus jedoch quasi direkt mit den AX2Go-Schlüsseln verbunden und überträgt z.B. Berechtigungsänderungen mithilfe eines im Hintergrund laufenden Dienstes praktisch sofort.

Weniger priorisierte Daten (z.B. Änderungen an den Kontaktdaten des Schließanlagenadministrators) werden ebenfalls automatisch über die Cloud übertragen, allerdings nicht sofort:

- Beim nächsten Push-Zyklus des AXM-Dienstes (halbtäglich) oder
- Zusammen mit höher priorisierten Daten (z.B. einer Berechtigungsänderung)

Da es sich bei der AXM Plus - ähnlich wie bei einer LSM Basic Online - um eine lokale Installation handelt, läuft der AXM-Dienst nur, wenn Sie den Rechner gestartet haben. Die AXM Plus selbst muss dazu nicht geöffnet sein.

Voraussetzungen für Nutzung der Cloud-Dienste

- Verbindung zwischen Ihrer AXM Plus und Ihrer SimonsVoss-ID (siehe *Verbindung zwischen Datenbank und Cloud überprüfen [▸ 451]*)
- Gültige Registrierung mit Service Fee Lizenz (siehe *Registrierung [▸ 34]*)

23.1.2.3 Zeitbudget in AX2Go

Ein Smartphone könnte in den Flugmodus versetzt werden und so die Verbindung zum AXM-Dienst beabsichtigt unterbrochen werden. Eine Berechtigungsänderung (insbesondere auch das Sperren des AX2Go-Schlüssels) würde in diesem Fall die AX2Go nie erreichen.

"Offline Zeitbudget (in Tagen)" zwingt alle AX2Go-Nutzer dazu, regelmäßig eine Verbindung zwischen der AX2Go und AXM-Dienst zu ermöglichen. Der Smartphone-Nutzer muss dazu nicht selbst aktiv werden. Damit kann der Flugmodus nicht missbraucht werden, um eine Berechtigung ungewollt dauerhaft zu nutzen.

Das Offline Zeitbudget (in Tagen) unterscheidet sich vom Zeitbudget in einem virtuellen Netzwerk (Details siehe *Zeitbudget (AX2Go und virtuelles Netzwerk) [▸ 560]*).

23.1.2.4 Sicherheit

Können Daten manipuliert oder kopiert werden?

Nein. Neben den bereits erwähnten Bausteinen verwenden wir noch zufällige Zahlenreihen (sog. Counter), die jedem Datenpaket bei jeder Übertragung einmalig angehängt werden. Eine spätere Übertragung mit manipulierten oder kopierten Daten tragen den falschen Counter und sind unbrauchbar.

Jeder Baustein für sich selbst stellt eine hohe Sicherheit dar und schützt unsere Daten damit verlässlich, nachhaltig und redundant.

Wie stelle ich sicher, dass die von mir eingeladene Person auch wirklich den AX2Go-Schlüssel erhält? / Was ist, wenn die E-Mail abgefangen oder unbemerkt weitergeleitet wird?

Um die Gefahr von abgefangenen E-Mails auszuschließen, bietet es sich an, den Einladungslink aus der AXM Verwaltungssoftware über einen End-to-end-verschlüsselten Kommunikationsweg wie beispielsweise eine verschlüsselte E-Mail zu versenden. Wählen Sie dazu den Einladungstyp "QR Code" aus und kopieren sie den erzeugten dynamischen Link in Ihr E-Mail-Programm.

Sie können die Einladung auch vorerst ohne Berechtigungen versenden und diese erst zu einem späteren Zeitpunkt (wenn Sie wissen, dass der richtige Nutzer die Einladung erhalten hat) über Gruppen- oder Einzelberechtigungen hinzufügen.

23.1.3 Spezielle Identmedien und deren Funktionen

Im System 3060 gibt es Identmedien mit besonderen Funktionen. Diese Identmedien haben ausschließlich eine besondere Funktion, d.h. z.B. ein Batteriewechsel-Transponder kann nicht gleichzeitig ein Aktivierungs-Transponder werden.

Batteriewechsel	Schließungsaktivierung
G2-Schließungen wechseln bei sehr niedrigen Batteriezuständen in den Freezemodus. Im Freezemodus reagieren die Schließungen nicht mehr auf berechtigte Transponder. Mit einem Identmedium zum Batteriewechsel können Sie an G2-Schließungen den Freezemodus vorübergehend aufheben. Danach können Sie mit einem zweiten, berechtigten Identmedium die Schließung einkuppeln, um die Tür zu öffnen und die Batterien zu wechseln. AX-Schließungen sind hiervon nicht betroffen, da die Batterien hier auch im völlig entleerten Zustand erreichbar und wechselbar sind.	Mit einem Identmedium zur Schließungsaktivierung können Sie eine deaktivierte Schließung wieder aktivieren. Danach können Sie mit einem zweiten, berechtigten Identmedium die Schließung einkuppeln.

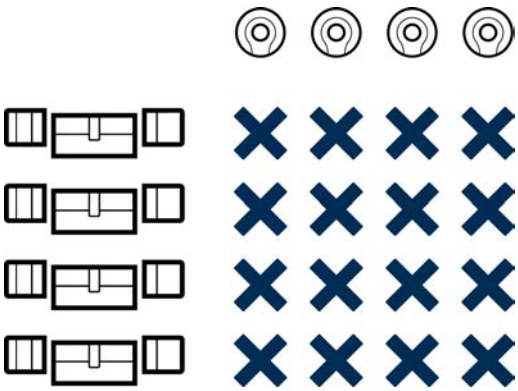
23.2 Schließanlagen

Eine Schließanlage ist eine zusammenhängende Struktur aus:

- Schließplan
- Organisationsbestandteilen

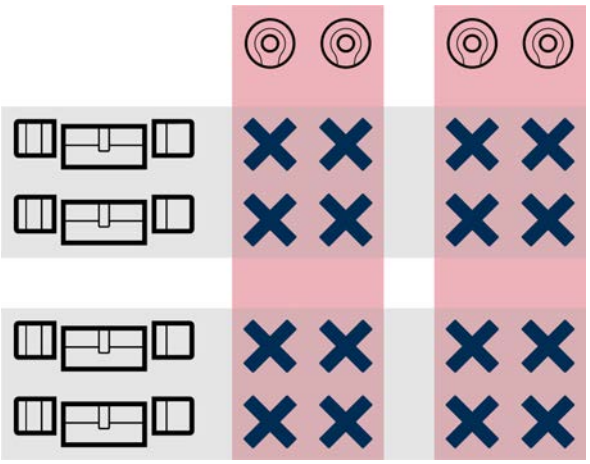
Schließplan

Im Schließplan sind Schließungen, Identmedien und Berechtigungen gespeichert (siehe auch *Identmedien, Schließungen und der Schließplan* *[▸ 532]*).



Mit weiteren Organisationsbestandteilen wird aus dem Schließplan eine Schließanlage:

- *Bereiche [▸ 569]*
- *Personengruppen [▸ 565]*
- *Berechtigungsgruppen [▸ 564]*
- *Zeitgruppen und Zeitpläne [▸ 548]*
- *Zeitumschaltungen [▸ 552]*
- *Hashtags [▸ 570]*



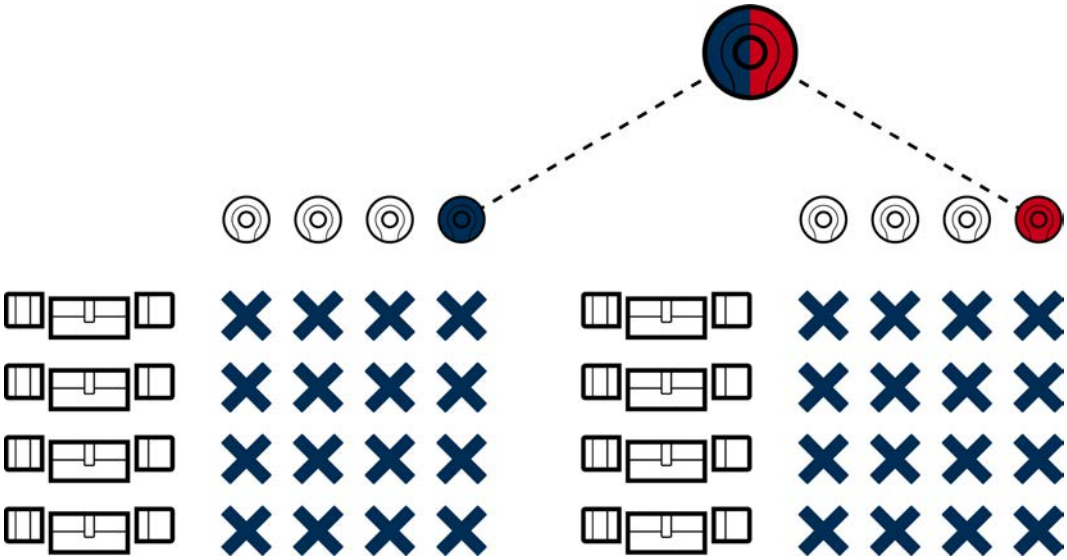
Mehrere Schließanlagen im gleichen Projekt

Manchmal kann es sinnvoll sein, mit mehr als einer Schließanlage zu arbeiten. Vielleicht wollen Sie in Ihrer AXM Plus zwei Unternehmen im gleichen Gebäude verwalten und wünschen sich eine striktere organisatorische Trennung?

Dann können Sie das zweite Unternehmen in einer eigenen Schließanlage aufbauen. So haben Sie eine bessere Trennung zwischen beiden Unternehmen.

Dabei haben Sie sogar die Möglichkeit, ein und dasselbe Identmedium in mehreren Schließanlagen zu benutzen (siehe *Identmedium in mehreren Schließanlagen verwenden [▸ 209]*). Grundsätzlich sind je nach Identmedium mehrere Schließanlagen möglich. Die Schließanlagen sind dabei voneinander völlig unabhängig und beeinflussen sich gegenseitig nicht.

One transponder to rule them all:



23.3 Übergreifende Schließebenen

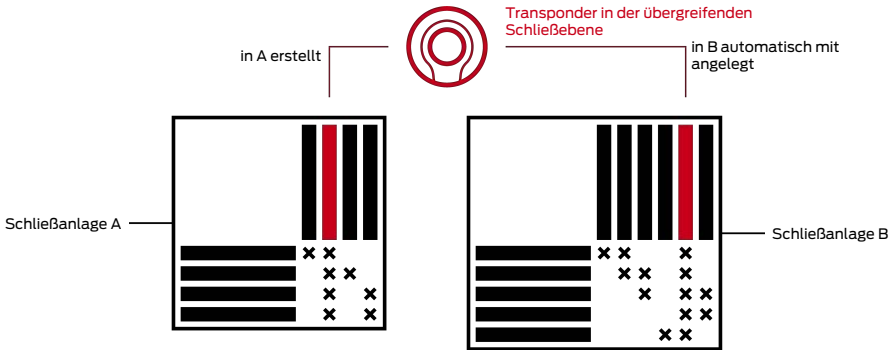
Mit übergreifenden Schließebenen können Sie Identmedien an Schließungen berechtigen, die aus vielen unterschiedlichen Schließanlagen stammen.

Vorteil

Vielleicht haben Sie beispielsweise ein Industrieareal, das aus mehreren Teilen mit vielen Gebäuden besteht. Für die Feuerwehr soll am Haupttor ein Feuerwehrschlüsselrohr mit Feuerwehrtransponder deponiert werden. Gleichzeitig möchten Sie die einzelnen Teile jeweils mit einer eigenen Schließanlage verwalten. Wenn Sie dann zuviele Schließanlagen haben, dann können Sie nicht mehr alle auf den Feuerwehrtransponder schreiben.

Hier hilft Ihnen das Konzept der übergreifenden Schließebenen.

Funktion



Zunächst legen Sie Ihre Schließanlagen mit Identmedien und Schließungen wie gewohnt an.

Anschließend erstellen Sie eine übergreifende Schließebene, z.B. eine rote. Dieser übergreifenden Schließebene weisen Sie dann Schließanlagen zu.

In einer dieser Schließanlagen erstellen Sie einen Transponder und aktivieren für diesen Transponder die übergreifende Schließebene. Dadurch erstellt die AXM Plus den Transponder in allen Schließanlage, die Sie dieser übergreifenden Schließebene zugewiesen haben.

Anschließend vergeben Sie wie gewohnt Ihre Berechtigungen innerhalb der jeweiligen Schließanlage.

Voraussetzungen und Hinweise

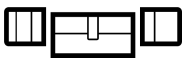
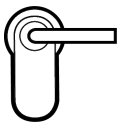
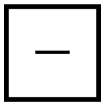
- Für die übergreifenden Schließebenen stehen Ihnen mehrere Farben zur Verfügung: Rot, Blau und Grün.

  SimonsVoss empfiehlt, die rote übergreifende Schließebene nur für Notfallzwecke zu verwenden (Feuerwehr, Rettungskräfte etc.).

  Transponder der roten übergreifenden Schließebene sind in der Lage, auch deaktivierte Schließungen zu betätigen.
- Das Passwort für die übergreifende Schließebene können Sie frei wählen, es muss nicht mit den Schließanlagenpasswörtern identisch sein.
- Passive Identmedien (z.B. Karten) können nicht in einer übergreifenden Schließebene eingesetzt werden.

23.4 "Einkuppeln", "Öffnen", "Verriegeln" usw.

Verschiedene Schließungstypen reagieren prinzipbedingt unterschiedlich auf ein berechtigtes Identmedium:

Schließung	Reaktion	Handlung des Benutzers
Schließzylinder 	Einkuppeln: Der elektronische Knauf verbindet sich mechanisch mit dem Mitnehmer.	Öffnen: 1. Knauf drehen. 2. Türdrücker nehmen. 3. Tür mit Türklinke aufziehen.
SmartHandles 	Einkuppeln: Der Drücker auf der elektronischen Seite verbindet sich mechanisch mit dem Vierkant.	Öffnen: 1. Drücker betätigen. 2. Tür mit Türdrücker aufziehen.
SmartRelais 	Schalten: Der Relaiskontakt im SmartRelais schaltet. Je nach SmartRelais ist das ein Schließkontakt oder ein Wechselkontakt. Angeschlossene elektrische Türen öffnen jetzt.	Keine weitere Handlung nötig. In der Regel ist die Tür jetzt schon geöffnet.

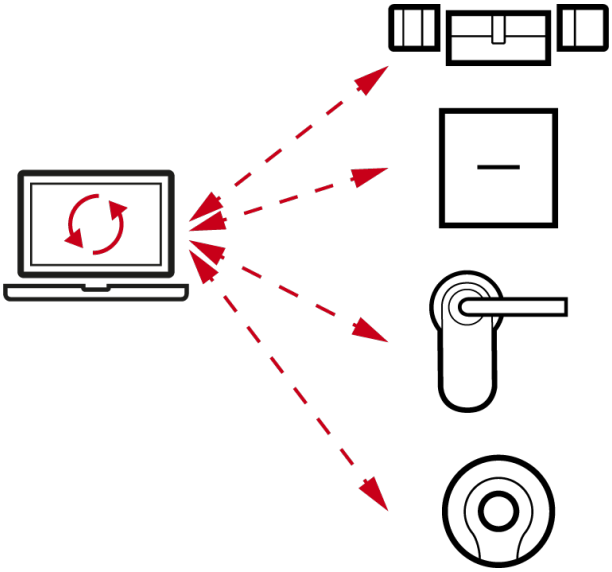
Schließung	Reaktion	Handlung des Benutzers
SmartLocker AX	Riegel einfahren: Der Motorblock im SmartLocker zieht den Riegel nach innen und gibt die Tür frei.	Öffnen: 1. Tür aufziehen.

Ganz grundsätzlich gilt: Außer dem SmartRelais ist keine Schließung in der Lage, eine Tür zu öffnen, zu schließen oder zu verriegeln. Dazu ist immer eine Aktion des Benutzers erforderlich (z.B. Knauf drehen und Tür aufziehen). Selbst das SmartRelais benötigt eine angeschlossene Türsteuerung, einen angeschlossenen Motor o.ä.

Ausdruck	Bedeutung
Betätigen	Ein Identmedium wird an einer Schließung betätigt.
Einkuppeln	Schließzylinder und SmartHandle: Der elektronische Knauf bzw. der elektronische Drücker verbinden sich mit dem Mitnehmer bzw. dem Vierkant.
Öffnen	Eine Tür wird (nachdem z.B. ein Schließzylinder eingekuppelt wurde) vom Benutzer geöffnet.
Schließen	Eine Tür wird vom Benutzer geschlossen und fällt ins Schloss. Der Riegel des Einsteckschlosses ist noch nicht ausgefahren.
Auskuppeln	Schließzylinder und SmartHandle: Der elektronische Knauf bzw. der elektronische Drücker lösen sich vom Mitnehmer bzw. vom Vierkant.
Schalten	Nur für SmartRelais: Das Relais schaltet und die Relaiskontakte schließen bzw. wechseln.
Verriegeln	Nur für Schließzylinder: Der Schließzylinder ist eingekuppelt, der Knauf wird einmal gedreht. Der Riegel des Einsteckschlosses fährt heraus.

Ausdruck	Bedeutung
Sicher verriegeln	Nur für Schließzylinder: Der Schließzylinder ist eingekuppelt, der Knauf wird zweimal gedreht. Der Riegel des Einsteckschlosses fährt vollständig heruas.

23.5 Synchronisierung von Datenbank und Realität



Alles, was Sie in der AXM Plus ändern, wird (vorerst) nur in der Datenbank gespeichert. Es besteht keine automatische Verbindung zwischen der Datenbank und Ihren Schließungen oder Identmedien.

Erst mit der Synchronisierung (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*) werden die Änderungen wirksam. Sie erkennen in der Matrix am Symbol ⟲, dass sich hier seit der letzten Synchronisierung etwas geändert hat und eine Schließung bzw. ein Identmedium synchronisiert werden muss.

Während der Synchronisierung werden Daten in beide Richtungen übertragen:

- Von der Datenbank in die Schließung / ins Identmedium, z.B. Berechtigungsänderungen
- Von der Schließung / vom Identmedium in die Datenbank, z.B. Batteriezustände

ACHTUNG

Änderungen in der Schließanlage erst nach Synchronisierung wirksam

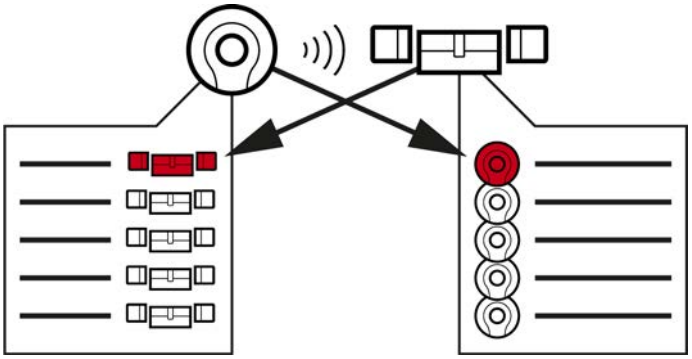
Wenn Sie die Schließanlage mit der AXM Plus bearbeiten, dann sind die Änderungen zunächst nur in Ihrer Datenbank gespeichert.

Ihre realen Komponenten erfahren von diesen Änderungen erst mit einer Synchronisierung.

1. Prüfen Sie die Komponenten in der Matrix regelmäßig auf Synchronisierungsbedarf (siehe *Aufbau der AXM [▸ 46]*).
2. Führen Sie insbesondere bei kritischen Vorfällen (z.B. Identmedium verloren) sofort nach der Reaktion auf den Vorfall eine Synchronisierung durch (siehe *Synchronisierung: Abgleich zwischen Schließplan und Realität [▸ 415]*).

Die AX2Go ist aufgrund der Cloudverbindung ein Sonderfall, siehe *Synchronisation der AX2Go-Schlüssel über die Cloud [▸ 538]*.

23.6 Begehungs- und Zutrittslisten



Begehungsliste Zutrittsliste

Wenn ein Identmedium mit einer Schließung spricht, dann kann das von beiden mitprotokolliert werden (Voraussetzung für die Schließung ist die ZK-Funktion).

Für Karten ist eine Kartenkonfiguration mit AV-Template Voraussetzung.

- Im Identmedium wird dabei die beteiligte Schließung in einer Begehungsliste gespeichert.
- In der Schließung wird dabei das beteiligte Identmedium in einer Zutrittsliste gespeichert.

Beide Listen können zum Beispiel bei der Synchronisierung ausgelesen und in die Datenbank importiert werden:

- *Schließung synchronisieren (inkl. Zutrittsliste auslesen) [▸ 416]*
- *Transponder/Karte synchronisieren (inkl. Begehungsliste lesen) [▸ 428]*

Anschließend können Sie beide Listen einsehen:

- *Zutrittsliste einer Schließung anzeigen und exportieren [▸ 421]*
- *Begehungsliste für Transponder/Karten anzeigen und exportieren [▸ 431]*

23.7 Zeitmanagement

Das Zeitmanagement im System 3060 ist sehr umfangreich und bietet sehr viele Einstellungsmöglichkeiten. Ganz grundsätzlich gibt es zwei voneinander unabhängige Zeitfunktionen:

- Berechtigungen auf bestimmte Zeiten beschränken (*Zeitgruppen und Zeitpläne [▸ 548]*)
- Schließungen automatisch einkuppeln (*Zeitumschaltungen [▸ 552]*)

HINWEIS

Sommerzeit und Winterzeit

Für alle zeitgesteuerten Funktionen werden Uhrzeit und Umschaltzeitpunkte des Geräts, von dem aus synchronisiert wird, verwendet und in der Schließung gespeichert.

- Prüfen Sie vor der Synchronisierung, ob das eingestellte Datum und die eingestellte Uhrzeit korrekt sind.

23.7.1 Zeitgruppen und Zeitpläne

Erfahren Sie hier in einem Beispiel, wie Zeitplan und Zeitgruppe zusammenspielen:

Ausgangssituation

Der Einfachheit halber besteht Ihr Beispielunternehmen aus drei Personen:

1. Angestellter
2. Praktikant
3. Reiningungskraft

Außerdem hat Ihr Beispielunternehmen zwei Türen:

1. Haupteingang
2. Labor

Zusätzlich gibt es folgende wichtige Zeitspannen in Ihrem Beispielunternehmen:

- Gleitzeit von 7:00 bis 22:00
- Kernzeit von 9:00 bis 16:00

- Reinigungszeit an Dienstagen und Donnerstagen von 17:00 bis 19:00

Überlegungen zur zeitlichen Beschränkung der Berechtigungen

Als verantwortungsvoller Unternehmer treffen Sie folgende Überlegungen:

Überlegungen zu:	Haupteingang	Labor
Angestellter	Ihr Angestellter darf während der gesamten Gleitzeit und auch am Wochenende von 7:00 bis 22:00 das Gebäude betreten.	Ihr Angestellter darf während der gesamten Gleitzeit und auch am Wochenende von 7:00 bis 22:00 das Labor betreten.
Praktikant	Ihr Praktikant soll bei schlechtem Wettter nicht draußen warten müssen, bis Ihr Angestellter kommt. Deshalb darf Ihr Praktikant an Werktagen ebenfalls während der gesamten Gleitzeit von 7:00 bis 22:00 das Gebäude betreten.	Das Labor ist ein gefährlicher Arbeitsplatz. Um Ihren Praktikanten zu schützen, wollen Sie, dass er nur unter Aufsicht Ihres Angestellten ins Labor kann. Sie beschränken deshalb den Laborzugang Ihres Praktikanten auf Werktage und auf die Kernarbeitszeit Ihrer Angestellten (9:00 bis 16:00).
Reinigungskraft	Ihre Reinigungskräfte dürfen während der Reinigungszeiten an Dienstagen und Donnerstagen von 17:00 bis 19:00 das Gebäude betreten.	Das Labor ist gefährlich und darf deshalb nur von unterwiesenen Personen betreten werden. Es ist möglich, dass Reinigungskräfte wechseln und deshalb nicht zu den unterwiesenen Personen gehören. Daher wollen Sie, dass Ihre Reinigungskraft das Labor überhaupt nicht betritt.

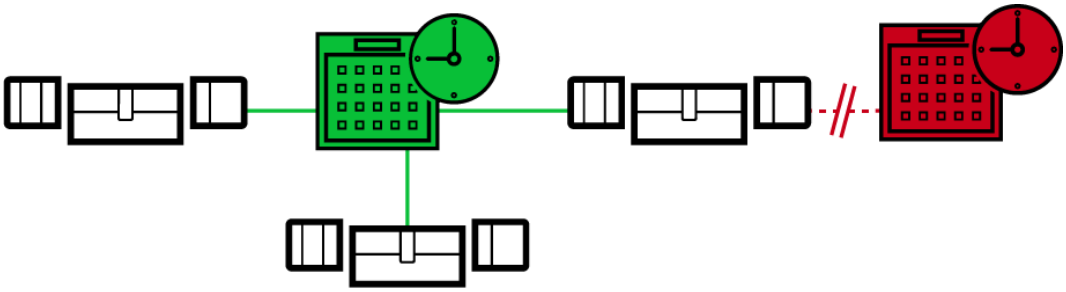
Sie erkennen, dass es zwei Türen gibt, an denen die Berechtigungen mit drei verschiedenen Zeiten gesteuert werden sollen. Daher benötigen Sie:

- Zwei Zeitpläne für die Türen bzw. Schließungen:
  - Zeitplan "Haupteingang"
  - Zeitplan "Labor"
- Drei Zeitgruppen für die Personen im Unternehmen:
  - Zeitgruppe "Angestellter"
  - Zeitgruppe "Praktikant"

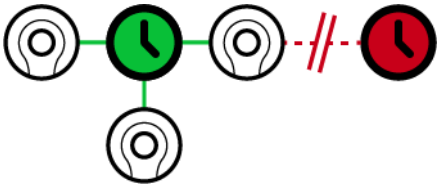
- Zeitgruppe "Reinigungskraft"

Neuer Zeitplan oder neue Zeitgruppe?

- Ein Zeitplan pro Schließung, aber beliebig viele Schließungen pro Zeitplan zuweisbar.



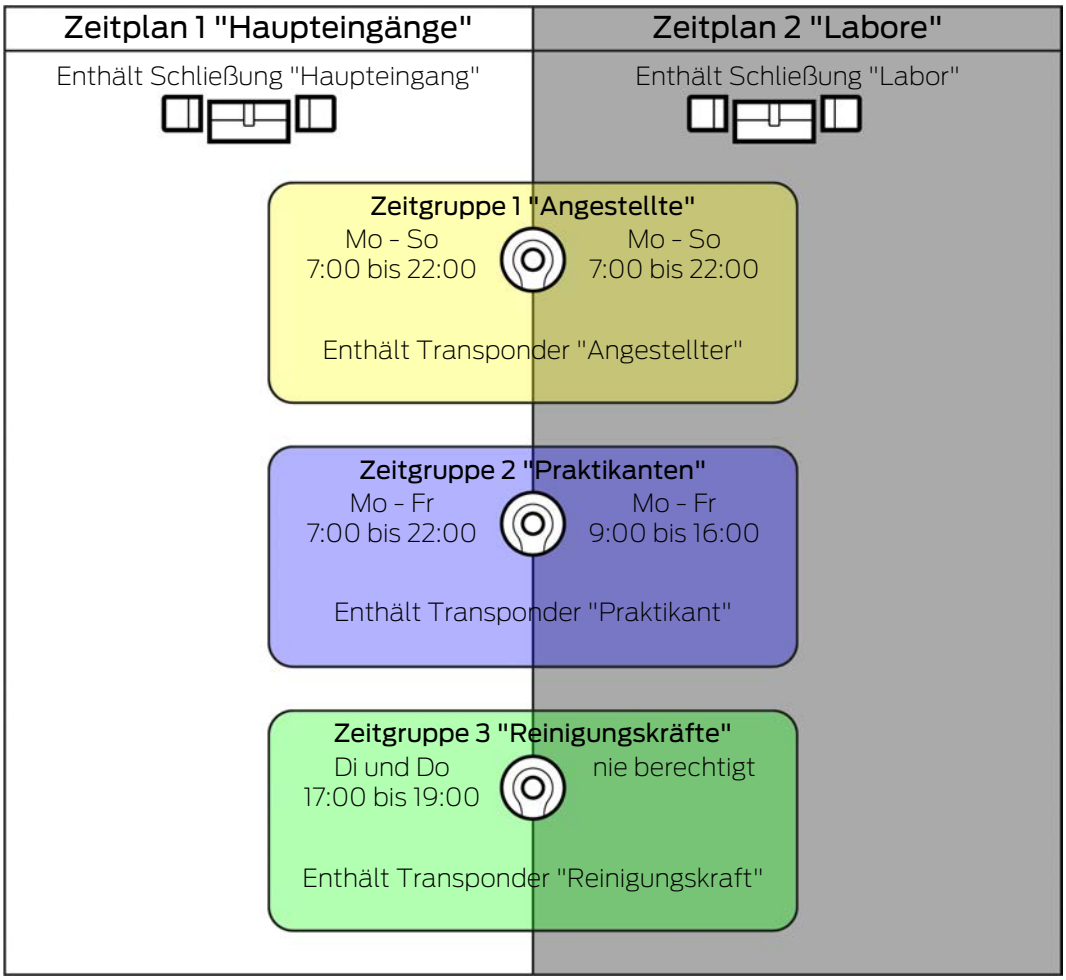
- Eine Zeitgruppe pro Identmedium, aber beliebig viele Identmedien pro Zeitgruppe zuweisbar.



- Alle Zeitgruppen sind in allen Zeitplänen sichtbar/auswählbar, werden aber für jeden Zeitplan einzeln eingestellt. Wenn Sie in einem Zeitplan eine Zeitgruppe neu erstellen und einstellen, dann erscheint die Zeitgruppe auch in allen anderen Zeitplänen. Sie ist dort aber nur vorhanden und aus Sicherheitsgründen standardmäßig als "nicht berechtigt" eingestellt.

Neuer Zeitplan	Neue Zeitgruppe
Sobald dasselbe Identmedium zwei Schließungen zu unterschiedlichen Zeiten betreten können soll. Da Sie pro Identmedium nur eine Zeitgruppe zuweisen können, weisen Sie in diesem Fall den Schließungen einen eigenen Zeitplan zu. Beispiel: Der Transponder des Praktikanten darf zwar den Haupteingang von 7:00 bis 22:00 öffnen, aber derselbe Transponder darf das Labor nur von 9:00 bis 16:00 öffnen.	Sobald zwei Identmedien dieselbe Schließung zu unterschiedlichen Zeiten betreten können sollen. Da Sie pro Schließung nur einen Zeitplan zuweisen können, weisen Sie in diesem Fall den Identmedien eine eigene Zeitgruppe zu. Beispiel: Die Schließung Haupteingang darf vom Angestellten täglich von 7:00 bis 22:00 geöffnet werden, aber dieselbe Schließung darf vom Praktikanten nur werktags von 7:00 bis 22:00 geöffnet werden.

Schematische Darstellung



	Haupteingang	Labor
Angestellter	▪ Transponder Ihres Angestellten: Zeitgruppe "Angestellte" ▪ Schließung Haupteingang: Zeitplan "Haupteingänge" ▪ Zeitgruppe "Angestellte" in Zeitplan "Haupteingänge" täglich von 7:00 bis 22:00 berechtigt Ihr Angestellter kann den Haupteingang täglich von 7:00 bis 22:00 betreten.	▪ Transponder Ihres Angestellten: Zeitgruppe "Angestellte" ▪ Schließung Labor: Zeitplan "Labore" ▪ Zeitgruppe "Angestellte" in Zeitplan "Labore" täglich von 7:00 bis 22:00 berechtigt Ihr Angestellter kann das Labor täglich von 7:00 bis 22:00 betreten.

	Haupteingang	Labor
Praktikant	▪ Transponder Ihres Praktikanten: Zeitgruppe "Praktikanten" ▪ Schließung Haupteingang: Zeitplan "Haupteingänge" ▪ Zeitgruppe "Praktikanten" in Zeitplan "Haupteingänge" werktags von 7:00 bis 22:00 berechtigt Ihr Praktikant kann den Haupteingang werktags von 7:00 bis 22:00 betreten.	▪ Transponder Ihres Praktikanten: Zeitgruppe "Praktikanten" ▪ Schließung Labor: Zeitplan "Labore" ▪ Zeitgruppe "Praktikanten" in Zeitplan "Labore" werktags von 9:00 bis 16:00 berechtigt Ihr Praktikant kann das Labor werktags von 9:00 bis 16:00 betreten.
Reinigungskraft	▪ Transponder Ihrer Reinigungskraft: Zeitgruppe "Reinigungskräfte" ▪ Schließung Haupteingang: Zeitplan "Haupteingänge" ▪ Zeitgruppe "Reinigungskräfte" in Zeitplan "Haupteingänge" dienstags und donnerstags von 17:00 bis 19:00 berechtigt Ihre Reinigungskraft kann den Haupteingang dienstags und donnerstags von 17:00 bis 19:00 betreten.	▪ Transponder Ihrer Reinigungskraft: Zeitgruppe "Reinigungskräfte" ▪ Schließung Haupteingang: Zeitplan "Labore" ▪ Zeitgruppe "Reinigungskräfte" in Zeitplan "Labore" nie berechtigt Ihre Reinigungskraft kann das Labor nie betreten.

23.7.2 Zeitumschaltungen

Mit Zeitumschaltungen können Sie Ihre Schließungen automatisch einkuppeln und auskuppeln lassen.

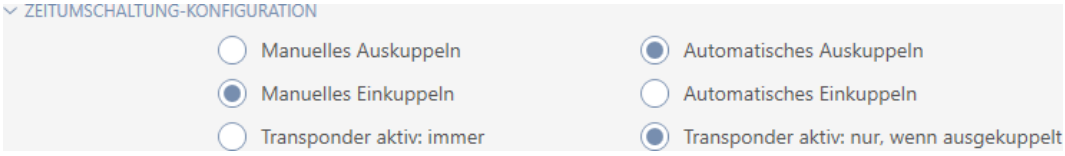
1. Legen Sie dazu in einer Zeitumschaltung Tage und Zeitintervalle fest (siehe *Zeitumschaltung erstellen [▸ 71]*).
2. Fügen Sie anschließend Ihre gewünschten Schließungen zu dieser Zeitumschaltung hinzu (siehe *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]*).
3. Bestimmen Sie abschließend für jede einzelne Ihrer gewünschten Schließungen das gewünschte Verhalten (siehe *Schließungen mit Zeitumschaltung automatisch einkuppeln und auskuppeln [▸ 287]*).

Grundsätzlich gilt:

- Innerhalb eines Zeitintervalls verhalten sich Ihre Schließungen wie im Daueröffnungsmodus.

- Außerhalb eines Zeitintervalls verhalten sich Ihre Schließungen wie im Impulsöffnungsmodus.

Das Verhalten lässt sich mit diesen Optionen noch genauer regeln:



Manuelles Auskuppeln

Schließung kuppelt aus, wenn:

- Außerhalb der Zeitintervalle und
- Berechtigtes Identmedium betätigt wird

Bleibt ausgekuppelt. Mit einem berechtigten Identmedium können Sie die die Schließung aber auch außerhalb der Zeitintervalle für die eingestellte Impulsdauer einkuppeln (Impulsdauer einstellen siehe *Schließung länger, kürzer oder dauerhaft öffnen lassen [▸ 295]*).

Automatisches Auskuppeln

Schließung kuppelt aus, wenn:

- Zeitintervall endet

Bleibt ausgekuppelt. Mit einem berechtigten Identmedium können Sie die die Schließung aber auch außerhalb der Zeitintervalle für die eingestellte Impulsdauer einkuppeln (Impulsdauer einstellen siehe *Schließung länger, kürzer oder dauerhaft öffnen lassen [▸ 295]*).

Manuelles Einkuppeln

Schließung kuppelt ein, wenn:

- Innerhalb der Zeitintervalle und
- Berechtigtes Identmedium betätigt wird

Beispiel: Geschäft im Einkaufszentrum, dessen Schiebetür nicht automatisch zu den Öffnungszeiten des Einkaufszentrums aufgehen soll. Der Inhaber des Geschäftes könnte aufgrund von Stau verspätet sein und das Geschäft würde unkontrolliert geöffnet werden.

Schließung bleibt für das Zeitintervall eingekuppelt.

Mit einem berechtigten Identmedium können Sie die Schließung aber auch während des Zeitintervalls auskuppeln (Ausnahme: Option ⦿ Transponder aktiv: Nur, wenn ausgekuppelt aktiviert).

Schließung bleibt dann ausgekuppelt bis:

- Sie während demselben Zeitintervall erneut ein Identmedium betätigen: Schließung kuppelt wieder ein, Zeitumschaltung läuft wie gewohnt weiter.
- Bei Option Manuelles Einkuppeln: Ein neues Zeitintervall beginnt und ein Identmedium betätigt wird.
- Bei Option Automatisches Einkuppeln: Ein neues Zeitintervall beginnt.

Automatisches Einkuppeln

Schließung kuppelt ein, wenn:

- Zeitintervall beginnt

Schließung bleibt für das Zeitintervall eingekuppelt.

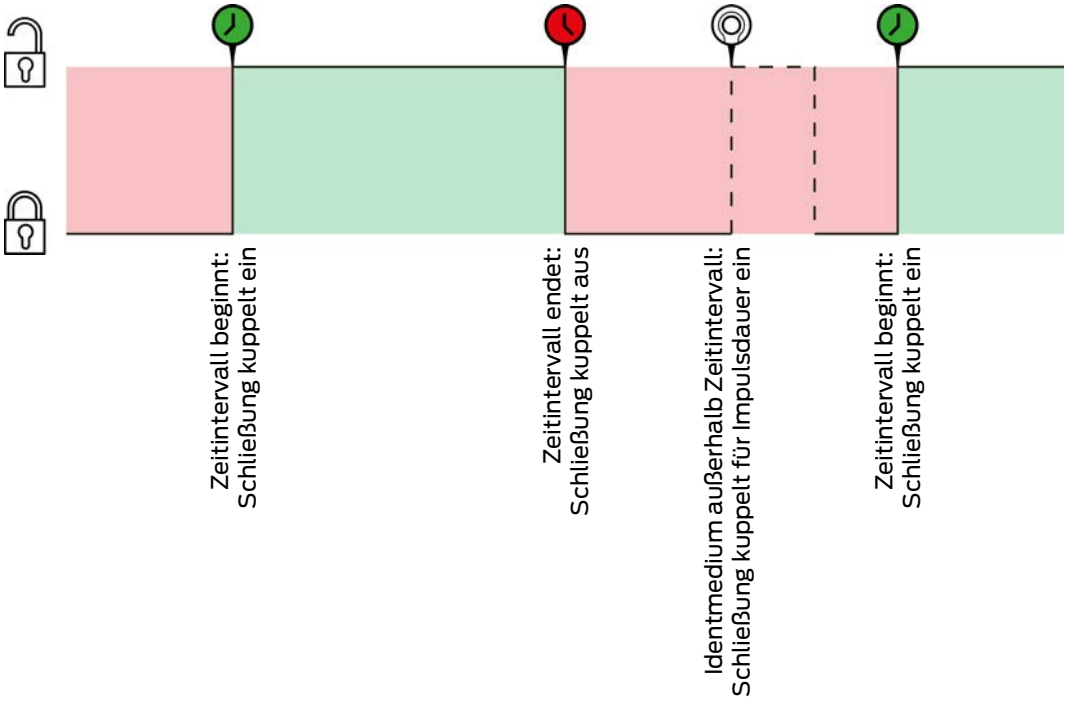
Mit einem berechtigten Identmedium können Sie die Schließung aber auch während des Zeitintervalls auskuppeln (Ausnahme: Option Transponder aktiv: Nur, wenn ausgekuppelt aktiviert).

Schließung bleibt dann ausgekuppelt bis:

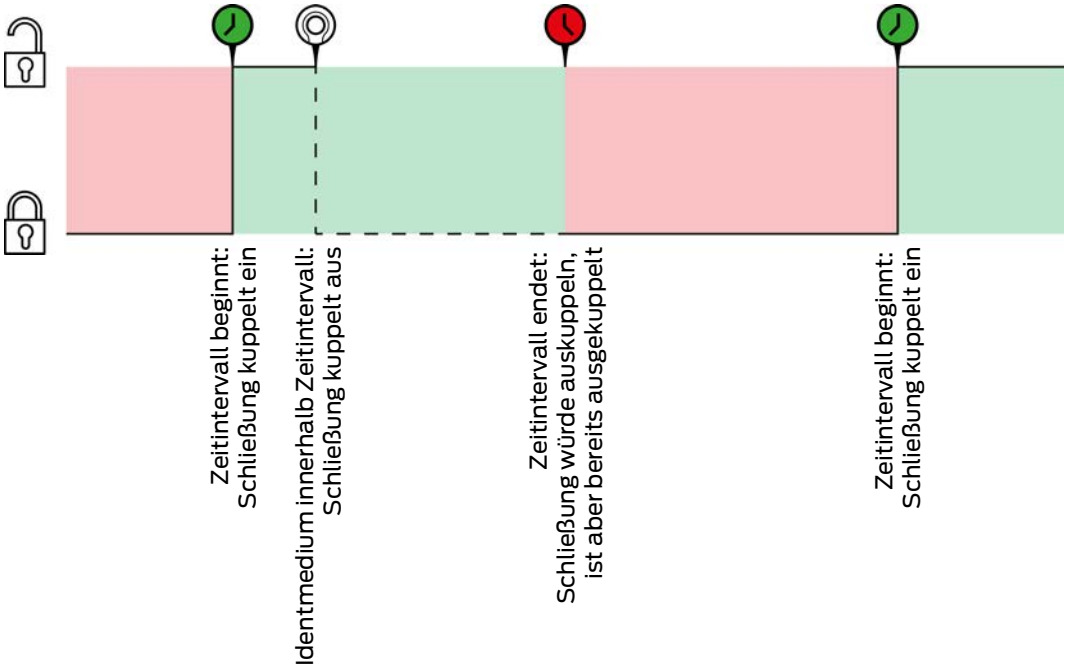
- Sie während demselben Zeitintervall erneut ein Identmedium betätigen: Schließung kuppelt wieder ein, Zeitumschaltung läuft wie gewohnt weiter.
- Bei Option Manuelles Einkuppeln: Ein neues Zeitintervall beginnt und ein Identmedium betätigt wird.
- Bei Option Automatisches Einkuppeln: Ein neues Zeitintervall beginnt.

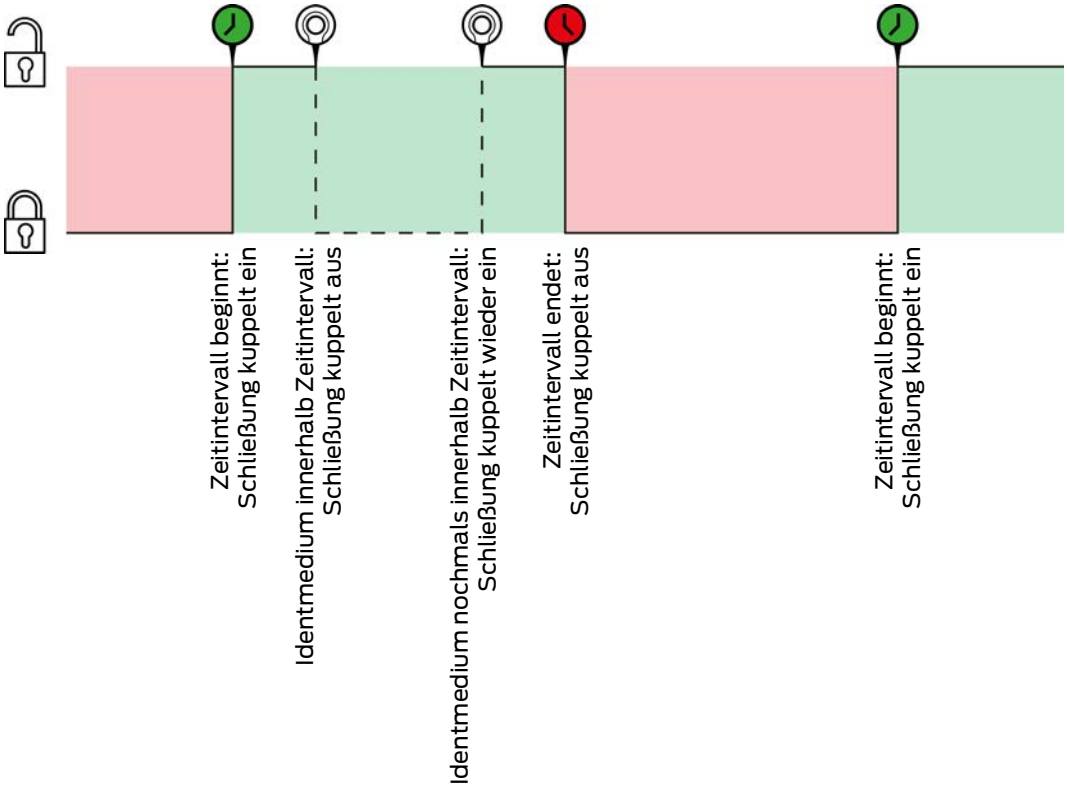
23.7.2.1 Beispiele

Automatisches Einkuppeln, Automatisches Auskuppeln

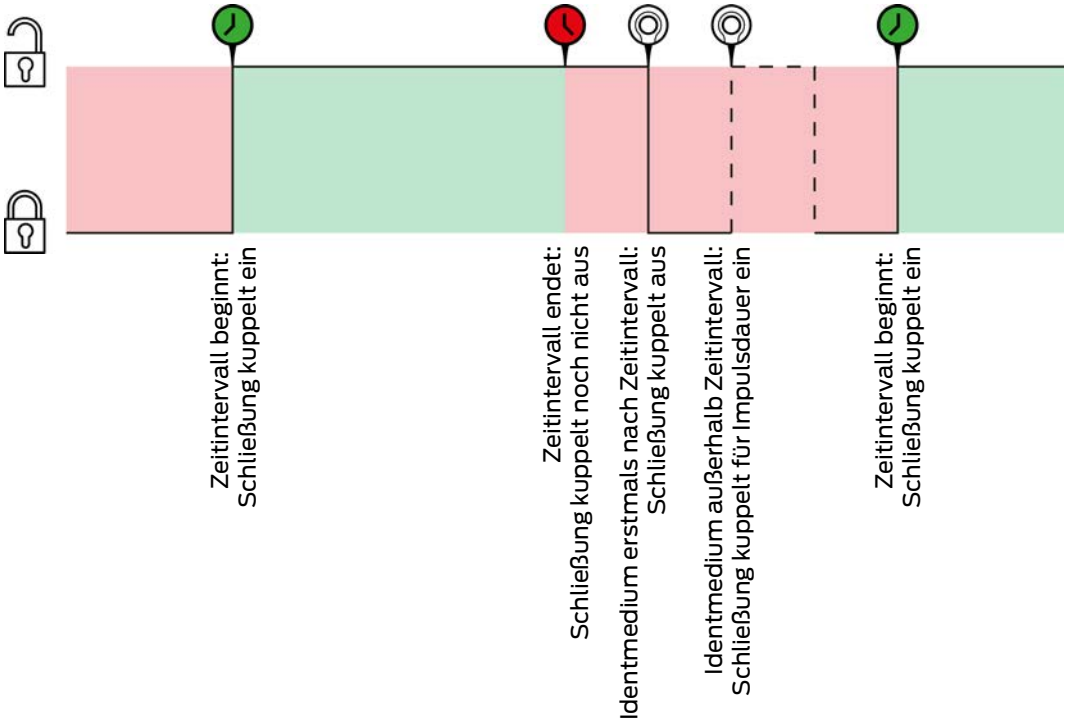


Für die beiden folgenden Beispiele muss die Option Transponder aktiv: immer ausgewählt sein, da sonst das Identmedium nicht innerhalb des Zeitintervalls betätigt werden kann.

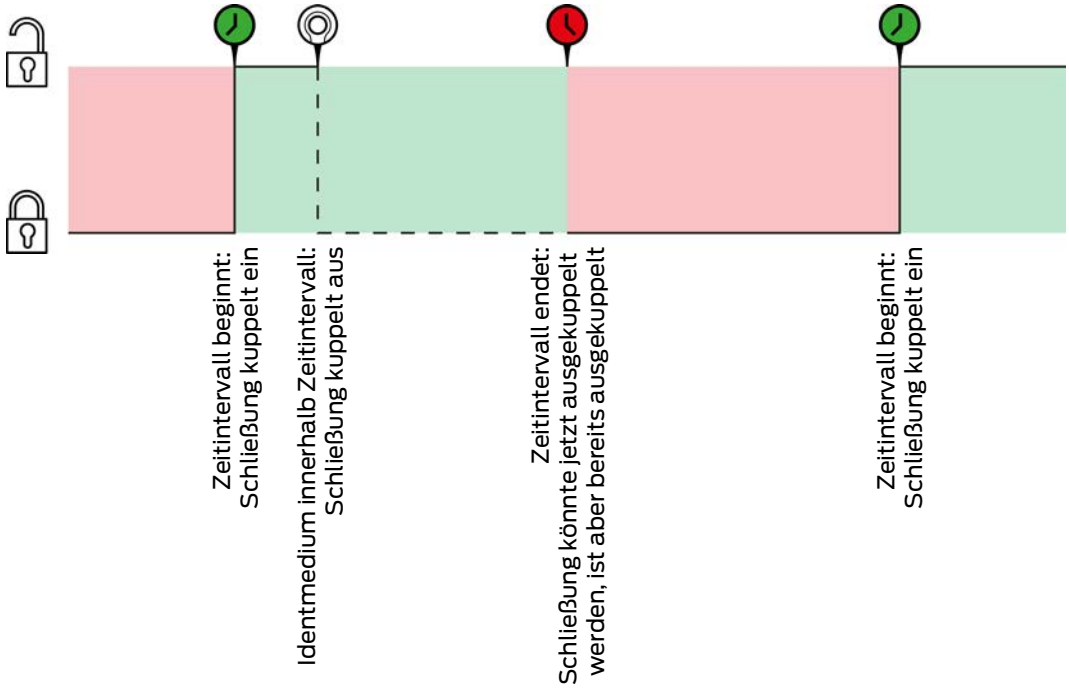


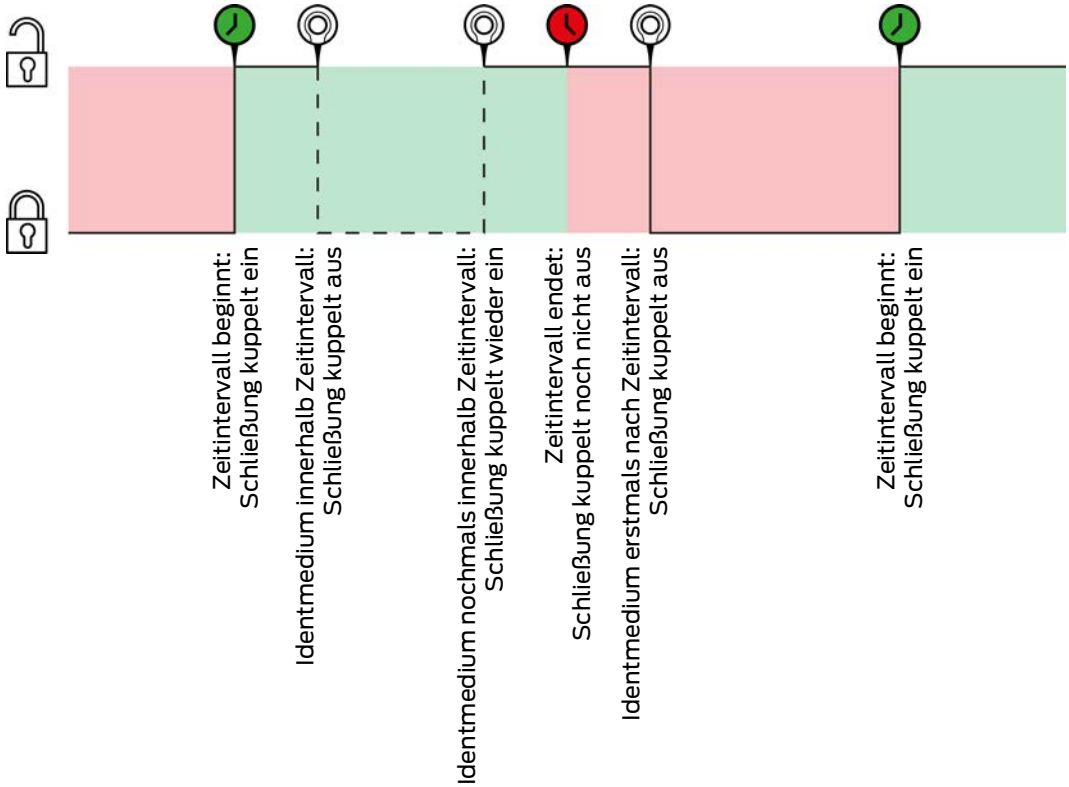


Automatisches Einkuppeln, Manuelles Auskuppeln

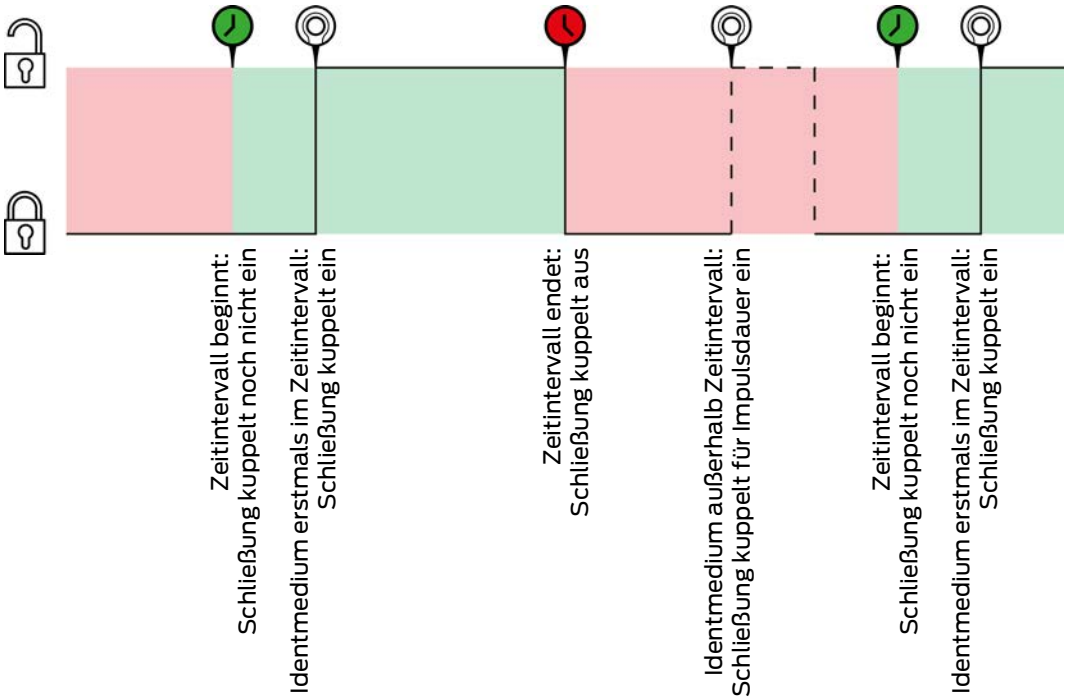


Für die beiden folgenden Beispiele muss die Option ⊙ Transponder aktiv: immer ausgewählt sein, da sonst das Identmedium nicht innerhalb des Zeitintervalls betätigt werden kann.

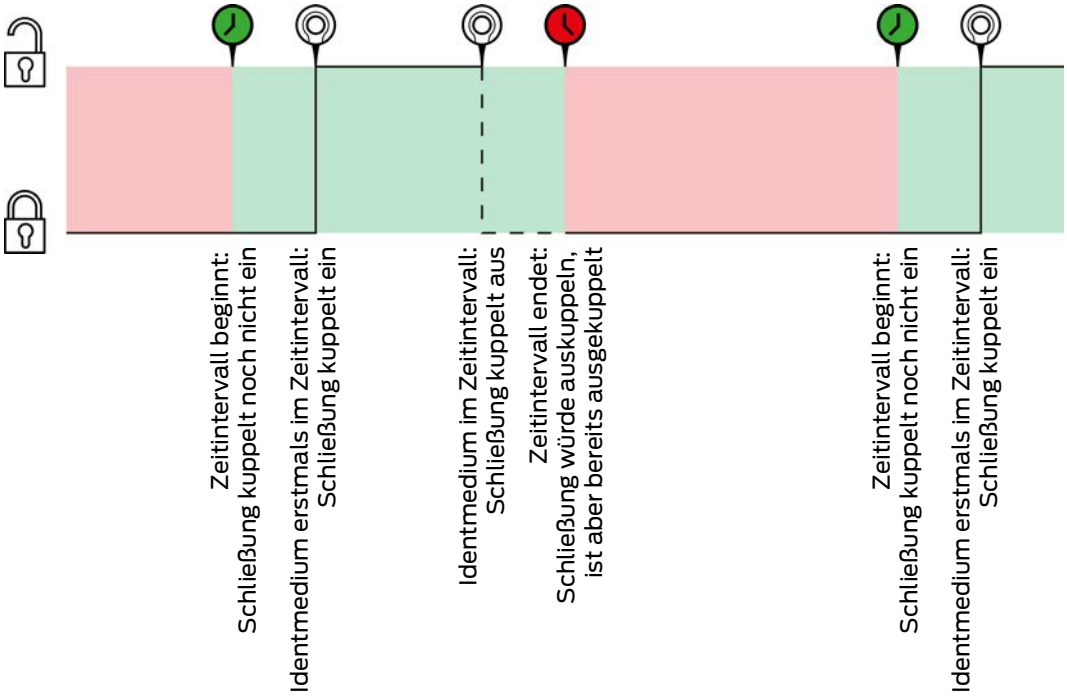

Zeitintervall beginnt:
Schließung kuppelt ein
Identmedium innerhalb Zeitintervall:
Schließung kuppelt aus
Zeitintervall endet:
Schließung könnte jetzt ausgekuppelt
werden, ist aber bereits ausgekuppelt
Zeitintervall beginnt:
Schließung kuppelt ein

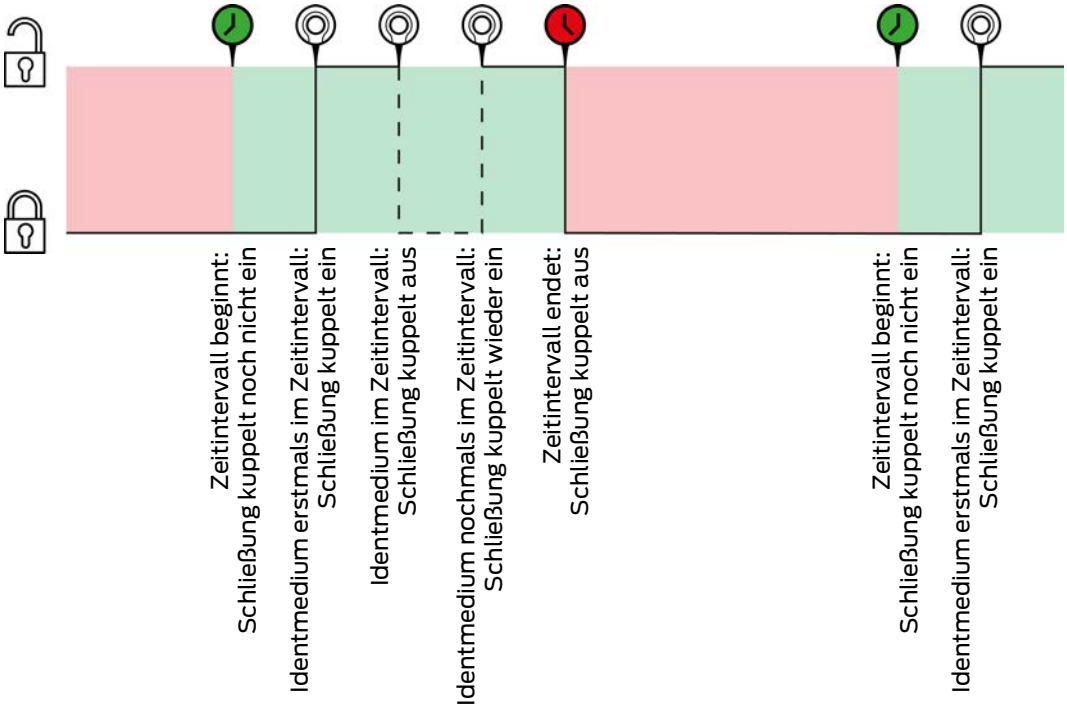

Zeitintervall beginnt:
Schließung kuppelt ein
Identmedium innerhalb Zeitintervall:
Schließung kuppelt aus
Identmedium nochmals innerhalb Zeitintervall:
Schließung kuppelt wieder ein
Zeitintervall endet:
Schließung kuppelt noch nicht aus
Identmedium erstmals nach Zeitintervall:
Schließung kuppelt aus
Zeitintervall beginnt:
Schließung kuppelt ein

Manuelles Einkuppeln, Automatisches Auskuppeln

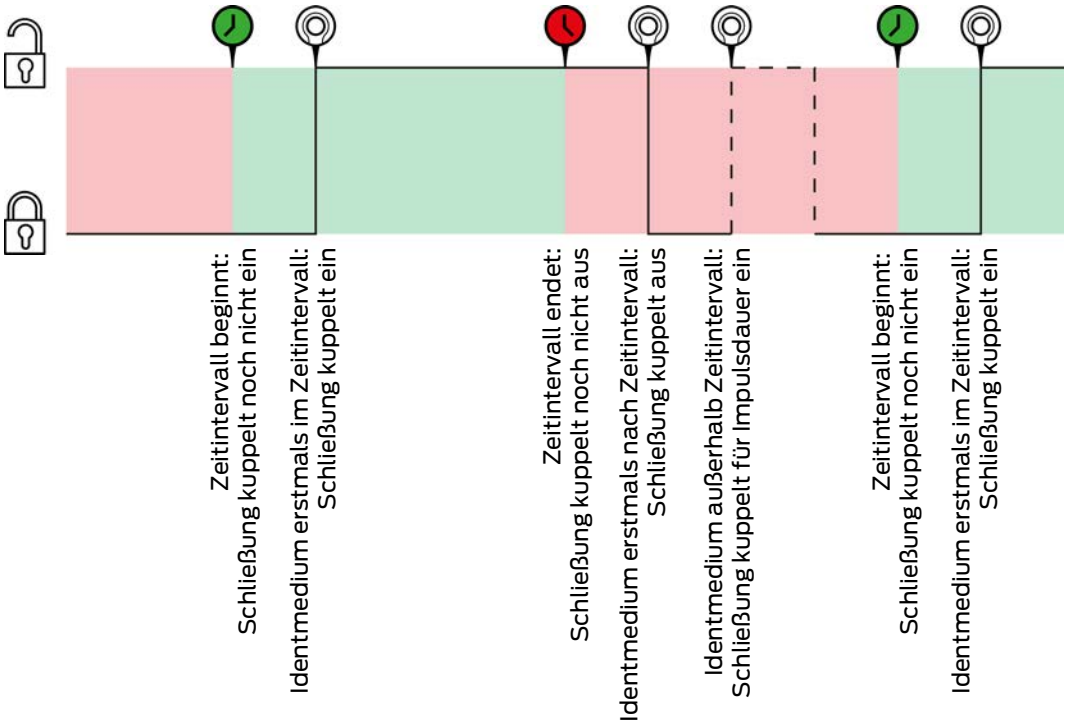


Für die beiden folgenden Beispiele muss die Option Transponder aktiv: immer ausgewählt sein, da sonst das Identmedium nicht innerhalb des Zeitintervalls betätigt werden kann.

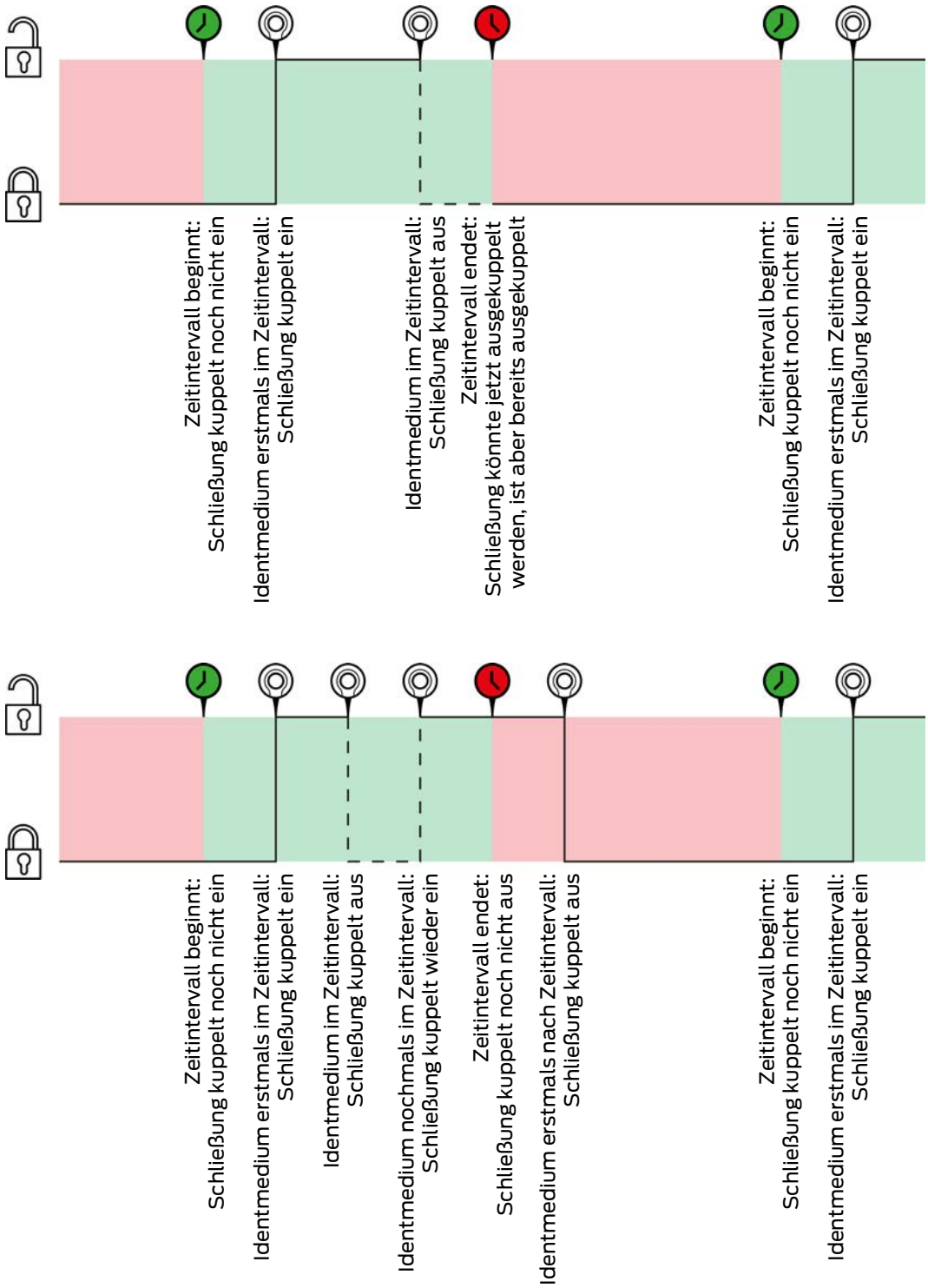




Manuelles Einkuppeln, Manuelles Auskuppeln



Für die beiden folgenden Beispiele muss die Option ⊙ Transponder aktiv: immer ausgewählt sein, da sonst das Identmedium nicht innerhalb des Zeitintervalls betätigt werden kann.



23.7.3 Zeitbudget (AX2Go und virtuelles Netzwerk)

Der Begriff "Zeitbudget" kommt in zwei verschiedenen Zusammenhängen vor:

- AX2Go: Offline Zeitbudget (in Tagen)
- Virtuelles Netzwerk: Dynamisches Zeitfenster

Beides bedeutet, dass ein Identmedium nur für eine begrenzte Zeit einsetzbar ist, bevor das Zeitbudget wieder aufgeladen muss. Beim Wiederaufladen wird geprüft, ob Berechtigungsänderungen vorliegen oder das Identmedium sogar gesperrt wurde.

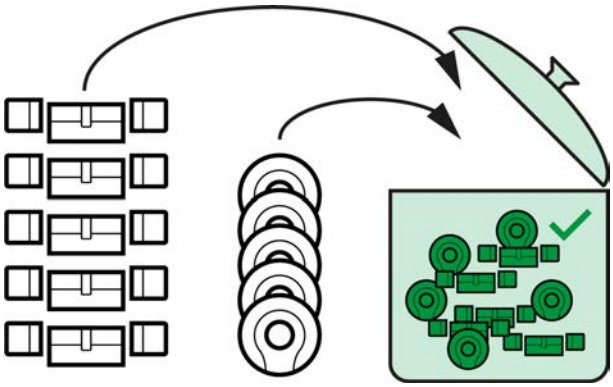
	AX2Go: Offline Zeitbudget (in Tagen)	Virtuelles Netzwerk: Dynamisches Zeitfenster
Einstellbarkeit	▪ Max. 30 Tage ab letzter Aufladung ▪ Taggenau einstellbar	▪ Max. 120 Stunden (=5 Tage) oder ▪ Bis zu einem gegebenen Zeitpunkt ab Aufladung (z.B. ab Aufladung bis 20:00) ▪ Stundengenau einstellbar
Aufladung von	AXM-Dienst. Sobald die AX2Go und der AXM-Dienst beide auf die Cloud zugreifen und sich somit sehen, wird das Zeitbudget wieder voll aufgeladen.	Gateways des virtuellen Netzwerks
Häufigkeit der Aufladung	Das Smartphone mit der AX2Go ist bis auf wenige Ausnahmen permanent mit dem Internet und damit mit der Cloud verbunden. Somit wird jedes Mal, wenn sich der AXM-Dienst mit der Cloud verbindet, das Zeitbudget wieder voll aufgeladen. Der AXM-Dienst verbindet sich bei wichtigen Änderungen (z.B. Berechtigungsänderungen) sofort mit der Cloud, ansonsten etwa halbtäglich.	Sobald das Identmedium am Gateway betätigt wird und nicht gesperrt wurde, wird das Zeitbudget wieder aufgeladen.

	AX2Go: Offline Zeitbudget (in Tagen)	Virtuelles Netzwerk: Dynamisches Zeitfenster
Einsatzzweck	Ein Smartphone könnte in den Flugmodus versetzt werden und so die Verbindung zum AXM-Dienst beabsichtigt unterbrochen werden. Eine Berechtigungsänderung würde in diesem Fall die AX2Go nie erreichen. "Offline Zeitbudget (in Tagen)" zwingt alle AX2Go-Nutzer dazu, regelmäßig eine Verbindung zwischen der AX2Go und AXM-Dienst zu ermöglichen. Damit kann der Flugmodus nicht missbraucht werden, um eine Berechtigung ungewollt dauerhaft zu nutzen.	Im virtuellen Netzwerk erfüllt "Dynamisches Zeitfenster" zwei Aufgaben: 1. Identmedien ans Gateway zwingen 2. Zeitliche Begrenzung der Berechtigung bei verlorenen Identmedien Im virtuellen Netzwerk werden Daten mithilfe der Identmedien vom Gateway zu den Schließungen und zurück transportiert. Je öfter die Identmedien dabei am Gateway sind, desto besser funktioniert der Datenaustausch. Mit dem begrenzten Zeitbudget stellen Sie sicher, dass alle Nutzer regelmäßig ans Gateway gehen. Zusätzlich kann ein gestohlenes Identmedium nach der Sperre nicht mehr länger als das eingestellte Zeitbudget verwendet werden. Ganz unabhängig davon, ob die Sperre an die Schließungen getragen wurde. Das Zeitbudget des gestohlenen Identmediums kann nicht mehr erneuert werden und läuft somit ab.

	AX2Go: Offline Zeitbudget (in Tagen)	Virtuelles Netzwerk: Dynamisches Zeitfenster
Beispiel (Normalbetrieb)	Beispiel: 30 Tage Zeitbudget eingestellt. Die AX2Go eines Nutzers verbindet sich über die Cloud mit dem AXM-Dienst. Da der Nutzer weiterhin berechtigt ist, erneuert sich das Zeitbudget wieder auf die vollen 30 Tage. Der Schließanlagenadministrator schließt den Laptop und geht für drei Wochen in den Urlaub. Da die AX2Go des Nutzers aber für 30 Tage Zeitbudget hat, kann die AX2Go während der gesamten Urlaubszeit des Schließanlagenadministrators problemlos verwendet werden. Nach der Rückkehr des Schließanlagenadministrators fährt dieser seinen Laptop wieder hoch. Der AXM-Dienst verbindet sich mit der Cloud und das Zeitbudget des Nutzers wird erneuert. Die AX2Go des Nutzers funktioniert während der gesamten Zeit unterbrechungsfrei.	Beispiel: 8 Stunden Zeitbudget eingestellt. Ein Nutzer betätigt sein Identmedium am Gateway. Das Gateway verbindet sich mit der Datenbank und stellt fest, dass das Identmedium nicht gesperrt wurde und erneuert das Zeitbudget. Der Nutzer kann anschließend für 8 Stunden sein Identmedium nutzen. Anschließend betätigt er sein Identmedium erneut am Gateway und erhält ein neues Zeitbudget.

	AX2Go: Offline Zeitbudget (in Tagen)	Virtuelles Netzwerk: Dynamisches Zeitfenster
Beispiel (Problem)	Beispiel: 7 Tage Zeitbudget eingestellt. Einem AX2Go-Nutzer wird eine Berechtigung entzogen. Da der Nutzer aber weiß, dass ihm diese Berechtigung entzogen werden soll und er später unerkannt die Schließung betätigen will, schaltet er den Flugmodus ein, um zu verhindern, dass ihm die Berechtigung entzogen wird. Die AX2Go kann keine Verbindung mehr zur Cloud aufbauen, daher wird das Zeitbudget des betroffenen Nutzers nicht mehr erneuert. Nach Ablauf der 7 Tage kann der Nutzer keine Schließung mehr mit seiner AX2Go betätigen und ist gezwungen, eine Online-Verbindung zuzulassen. Damit erreicht auch die entzogene Berechtigung seine AX2Go.	Beispiel: 8 Stunden Zeitbudget eingestellt. Ein Identmedium wird als gestohlen gemeldet und vom Schließanlagenadministrator gesperrt. Im Laufe der Zeit werden die Sperr-IDs im virtuellen Netzwerk an die Schließungen verteilt. Einige abgelegenere Schließungen haben jedoch auch acht Stunden nach der Sperre noch keine Sperr-ID erhalten. Das gestohlene Identmedium kann aber auch an diesen Schließungen nicht mehr verwendet werden. Das Zeitbudget ist abgelaufen und wird aufgrund der Sperre auch nicht mehr erneuert.

23.8 Berechtigungsgruppen



Berechtigungsgruppen sind mit Einführung der AXM Plus erstmals verfügbar.

Das Prinzip einer Berechtigungsgruppe ist ganz einfach, ähnlich wie bei einem Schmelztiegel ("melting pot"). Innerhalb einer Berechtigungsgruppe sind normalerweise alle Schließungen an allen Identmedien berechtigt.

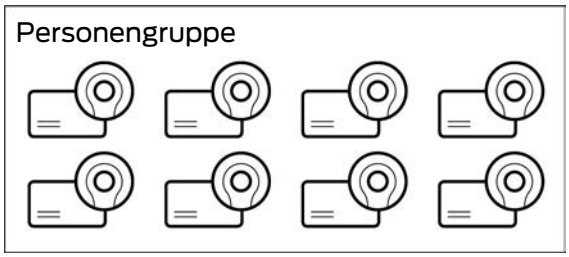
"Normalerweise" deshalb, weil Sie auch einzelnen Identmedien manuell Berechtigungen wegnehmen können. Damit haben Sie die volle Entscheidungsfreiheit über die Berechtigungen, können aber den Großteil der Arbeit über eine Berechtigungsgruppe erledigen.

Identmedien und Schließungen können mehrere Berechtigungsgruppen zugeordnet werden.

Berechtigungsgruppen sind ein organisatorischer Bestandteil. Idealerweise richten Sie Ihre Berechtigungsgruppen noch vor Ihren Schließungen und Identmedien ein (siehe *Best Practice: Schließanlage aufbauen [▸ 32]* und *Berechtigungsgruppen erstellen [▸ 55]*).

23.9 Personengruppen

Personengruppen sind eine organisatorische Einheit. Mit einer Personengruppe können Sie Personen (bzw. deren Identmedien), die zusammengehören, auch in der AXM Plus zusammenfassen.



Das klassische Beispiel für den Einsatz von Personengruppen sind Abteilungen. Es ist sehr wahrscheinlich, dass innerhalb einer Abteilung alle Mitarbeiter die gleichen Berechtigungen bekommen (z.B. sollte jeder Mechaniker alle Schließungen in der Werkstatt betätigen können). Anstatt jedem Identmedium einzeln die nötigen Berechtigungen zuzuweisen: Gruppieren Sie die Identmedien zu einer Personengruppe zusammen und berechtigen Sie die ganze Personengruppe auf einmal.

Personengruppen bieten außerdem weitere Vorteile:

- Filtern nach Identmedien, die Teil einer Personengruppe sind
- Berechtigen ganzer Personengruppen (siehe *Bereiche und Personengruppen zu Berechtigungsgruppen hinzufügen [▸ 341]*)
- Matrix-Strukturierung
- Identmedien nachträglich in eine andere Personengruppe verschieben (siehe *Personen zu Personengruppen zuordnen [▸ 202]*)

Personengruppen sind ein organisatorischer Bestandteil. Idealerweise richten Sie Ihre Personengruppen noch vor den Identmedien ein (siehe *Best Practice: Schließanlage aufbauen [▸ 32]* und *Personengruppe erstellen [▸ 56]*).

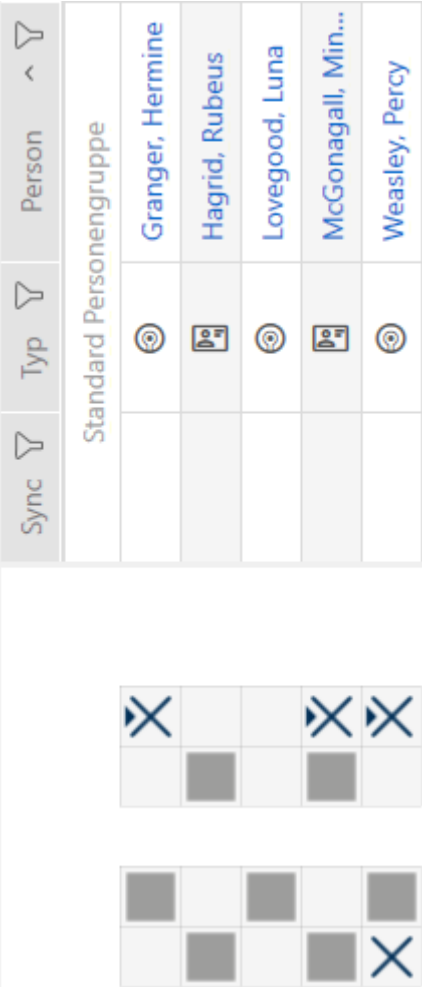
HINWEIS

Maximal eine Personengruppe pro Identmedium

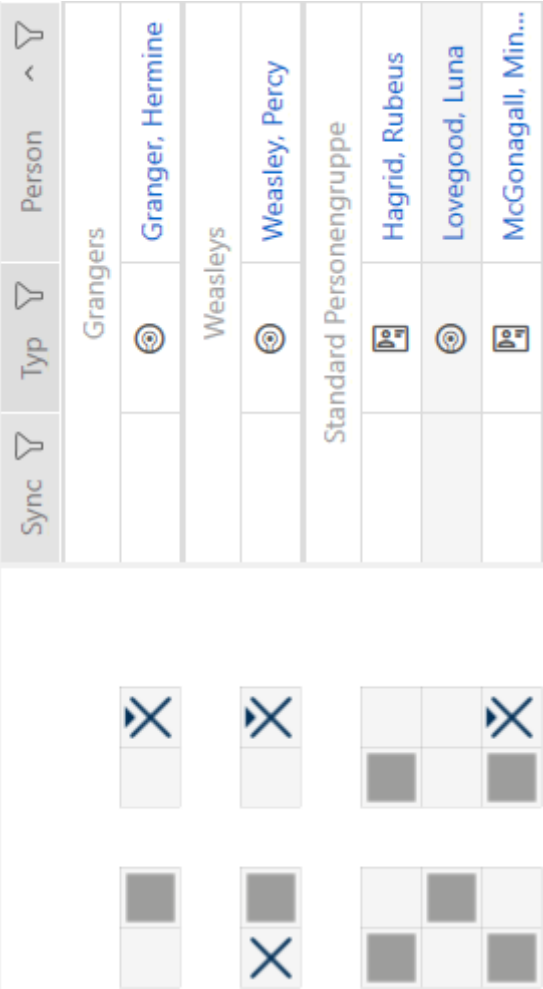
Ein Identmedium kann nur zu maximal einer Personengruppe gehören. Personen, die zu mehreren Abteilungen gehören, gibt es in der AXM Plus nicht. Wenn Sie einem Identmedium eine andere Personengruppe zuweisen, dann wird dieses Identmedium ggfs. automatisch aus ihrer bisherigen Personengruppe entfernt.

- Im Fenster "Personengruppe" können Sie mithilfe der Spalte Personengruppe prüfen, ob ein Identmedium bereits einer Personengruppe zugewiesen ist.

Matrix ohne Personengruppen



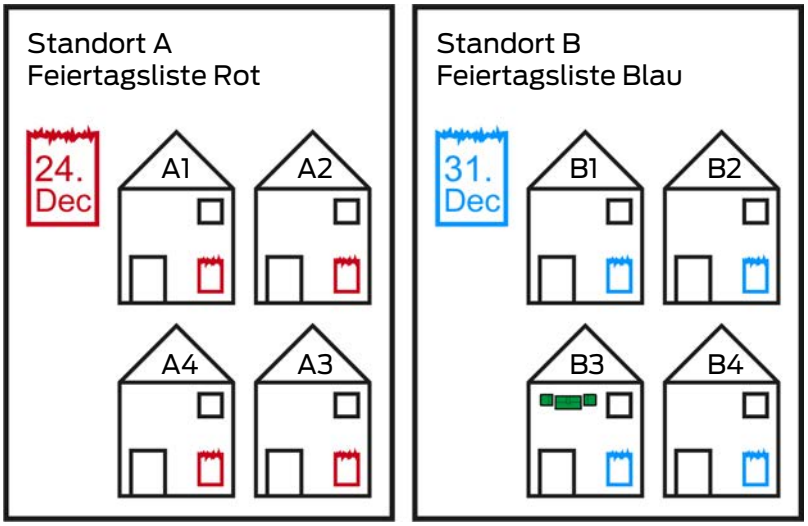
Matrix mit Personengruppen



23.10 Verwendete Passwörter

- Benutzerkennwort: Schützt Ihre AXM Plus davor, dass sich Unbefugte anmelden und Ihre Schließanlage verändern.
- Schließanlagenpasswort: Schützt die Kommunikation zwischen den verschiedenen Komponenten Ihrer Schließanlage (z.B. zwischen Transponder und Schließzylinder).
- Backup-Passwörter: Schützt Ihre AXM Plus davor, dass veraltete Schließanlagenzustände wiederhergestellt werden können.

23.11 Gebäude und Standorte



Ein Standort enthält Gebäude und optional eine Feiertagsliste.

Ein Gebäude gehört immer zu einem Standort. Deshalb muss in Ihrer Datenbank auch immer mindestens ein Standort vorhanden sein. In einem neuen Projekt legt die AXM Plus daher einen Standard-Standort an. Diesen können Sie löschen, sobald Sie eigene Standorte angelegt haben.

Standorte und Gebäude sind besonders zur Organisation nützlich. Daher sollten sie im Rahmen der Best Practice (siehe *Best Practice: Schließanlage aufbauen [▸ 32]*) auch noch vor den Schließungen angelegt werden (siehe *Standort erstellen [▸ 83]* und *Gebäude erstellen und zu Standort zuweisen [▸ 86]*).

Feiertagslisten und Standorte

In der Regel ordnen Sie einem Standort nur Gebäude zu, die auch tatsächlich am selben Standort sind. Es ist also sehr wahrscheinlich, dass für all diese Gebäude dieselben gesetzlichen Feiertage gelten (z.B. alle Gebäude am Standort München: Für alle Gebäude gelten die bayrischen Feiertage).

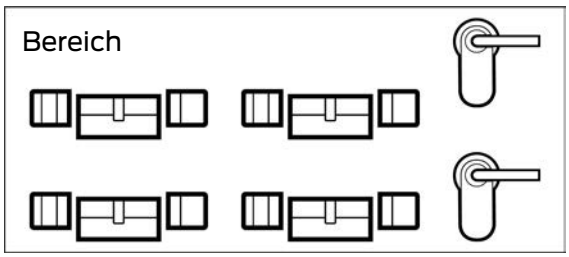
Die Feiertagslisten sind vor allem für zeitgesteuerte Schließungen interessant. Praktischerweise sind Schließungen immer einem Gebäude zugewiesen, das wiederum einem Standort zugewiesen ist (verpflichtende Angaben). Jeder Schließung einzeln eine Feiertagsliste zuzuweisen ist mühsam. Stattdessen können Sie allen Schließungen in Gebäuden mit dem gleichen Standort dieselbe Feiertagsliste zuweisen, indem Sie einfach dem ganzen Standort eine Feiertagsliste zuweisen.

Die so zugewiesene Feiertagsliste gilt für alle Schließungen dieses Standorts. Im Beispiel wurde dem Standort A die rote Feiertagsliste zugewiesen und Standort B die blaue Feiertagsliste.

Falls für einzelne Schließungen (aus welchem Grund auch immer) doch andere Feiertage gelten sollen, können Sie die Feiertagsliste aus dem Standort in den Eigenschaften der Schließung überschreiben (siehe *Berechtigungen an Schließungen auf bestimmte Zeiten beschränken (Zeitplan) [▸ 286]*. Im Beispiel wurde einer Schließung im Gebäude B3 am Standort B eine grüne Feiertagsliste zugewiesen. Für alle anderen Schließungen im Gebäude B3 und an den anderen Gebäuden des Standorts B gilt weiterhin die blaue Feiertagsliste.

23.12 Bereiche

Bereiche sind eine organisatorische Einheit für Ihre Schließungen. Mit einem Bereich können Sie Schließungen, die zusammengehören, auch in der AXM Plus zusammenfassen.



Ein klassisches Beispiel für den Einsatz von Bereichen sind Räumlichkeiten, zum Beispiel ein Eingangsbereich. Ein Eingangsbereich kann mehrere Türen und Schließungen beinhalten. Hier wäre es praktisch, wenn Sie bei Arbeiten an Ihrer Schließanlage nicht jede dieser Schließungen "anfassen" müssten. Der Einsatz von Bereichen ermöglicht Ihnen genau das und zusätzliche Komfortfunktionen:

- Mehrere Schließungen auf einmal berechtigen
- Filtern nach Schließungen, die Bestandteil eines Bereichs sind
- Matrix-Strukturierung
- Berechtigungen an ganzen Bereichen (siehe *Bereiche und Personengruppen zu Berechtigungsgruppen hinzufügen [▸ 341]*)
- Schließung nachträglich in einen anderen Bereich verschieben (siehe *Schließungen in Bereiche verschieben [▸ 279]*)
- Zeitplan einem ganzen Bereich statt einzelnen Schließungen zuweisen (siehe *Bereich mitsamt Schließungen zu einem Zeitplan hinzufügen [▸ 355]*)

Bereiche sind ein organisatorischer Bestandteil. Idealerweise richten Sie Ihre Bereiche noch vor den Schließungen ein (siehe *Best Practice: Schließanlage aufbauen [▸ 32]* und *Bereich erstellen [▸ 89]*).

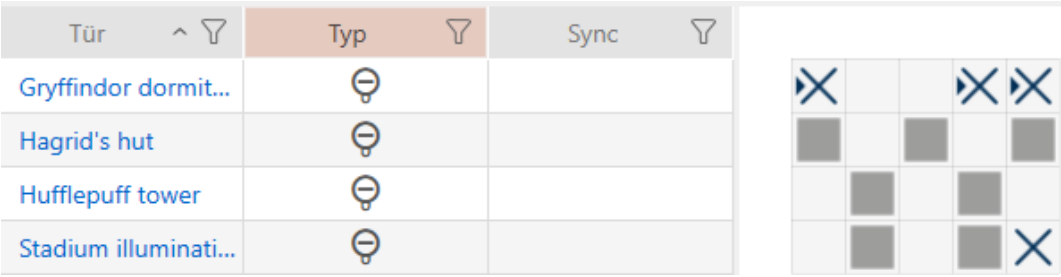
HINWEIS

Maximal ein Bereich pro Schließung

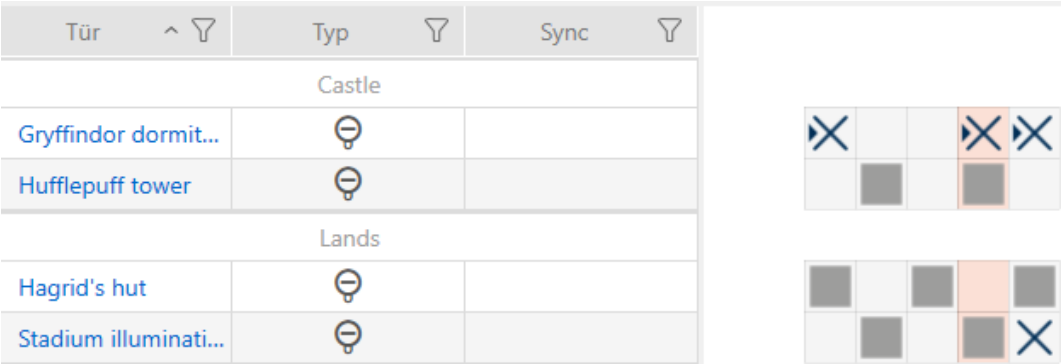
Eine Schließung kann nur zu maximal einem Bereich gehören. Überlappende Bereiche gibt es in der AXM Plus nicht. Wenn Sie einer Schließung einen anderen Bereich zuweisen, dann wird diese Schließung ggfs. automatisch aus ihrem bisherigen Bereich entfernt.

- Im Fenster "Bereich - Details" können Sie mithilfe der Spalte Bereich - Details prüfen, ob eine Schließung bereits einem Bereich zugewiesen ist.

Matrix ohne Bereiche



Matrix mit Bereichen



23.13 Hashtags

Hashtags sind eine zusätzliche Möglichkeit, Ihre Schließanlage zu organisieren. Setzen Sie Sie beliebig als Schlagworte zu Schließungen und Identmedien ein.

Denkbar wäre zum Beispiel die Einbausituation: #glastür

23.14 DoorMonitoring

DoorMonitoring ist ein Zusatzfeature, um Türzustände zu erfassen und in Ihrer AXM Plus anzuzeigen.

Voraussetzung dafür sind Schließungen mit der entsprechenden Sensorik (=DoorMonitoring-Schließungen).

HINWEIS

DoorMonitoring ohne Direktvernetzung ("WaveNet") eingeschränkt verfügbar

In einer direktvernetzten Schließanlage können Schließungen, die an das WaveNet angeschlossen sind, ihre DoorMonitoring-Ereignisse sofort über das Netzwerk übertragen. Sie sehen diese Ereignisse in kürzesteter Zeit in Ihrer Schließplansoftware (z.B. AXM).

Ohne WaveNet protokollieren Schließungen ihre DoorMonitoring-Ereignisse ebenfalls und speichern diese in der Zutrittsliste. Sie sehen diese Ereignisse erst nach dem Auslesen der Zutrittsliste in Ihrer Schließplansoftware.

DoorMonitoring-Schließzylinder sind beispielsweise unter anderem mit einer speziellen Sensor-Stulpschraube ausgestattet.

23.14.1 Mögliche DoorMonitoring-Zustände Schließzylinder

- Tür offen/geschlossen
- Tür verriegelt
- Tür sicher verriegelt
- Tür zu lange offen
- Stulpschraube manipuliert

23.14.2 Mögliche DoorMonitoring-Zustände SmartHandle

- Tür offen/geschlossen
- Tür zu lange offen
- Verriegelt (nur bei selbstverriegelnden Einsteckschlössern)
- Drücker gedrückt/nicht gedrückt

23.14.3 Mögliche DoorMonitoring-Zustände SmartRelais 3

- Input 1 aktiv/inaktiv
- Input 2 aktiv/inaktiv
- Input 3 aktiv/inaktiv
- Sabotage-Erkennung

23.15 Berichte

23.15.1 Skalierung der Bilddateien

Die AXM Plus bietet Ihnen die Möglichkeit, Ihre Berichte mit Ihren eigenen Bilddateien in der Kopf- und Fußzeile zu personalisieren (siehe *Berichte und Exporte personalisieren [▸ 465]*).

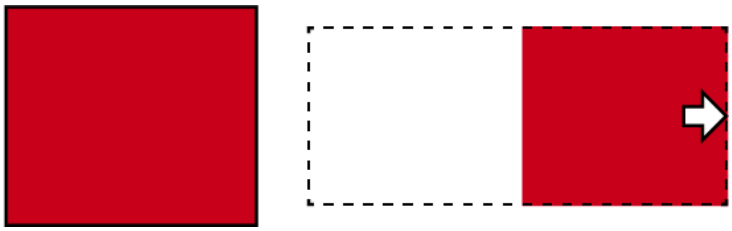
Hier können Sie beispielsweise Ihr eigenes Logo einfügen.

Die Bilddatei können Sie frei auswählen. In den ausgegebenen Berichten ist für Ihre Bilddateien ein bestimmter Rahmen vorgesehen. Die AXM Plus skaliert Ihre Bilder automatisch, um sie in den Rahmen einzupassen:

Bild zu schmal und zu niedrig

Das Bild wird proportional vergrößert und rechtsbündig in den Rahmen eingepasst.

Bild zu hoch

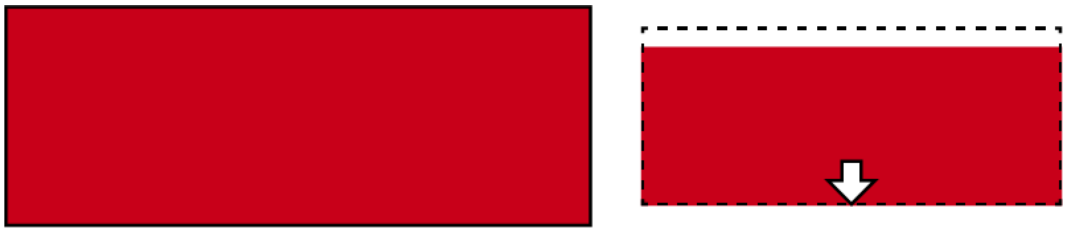


Das Bild wird proportional verkleinert und rechtsbündig in den Rahmen eingepasst.

Bild zu breit

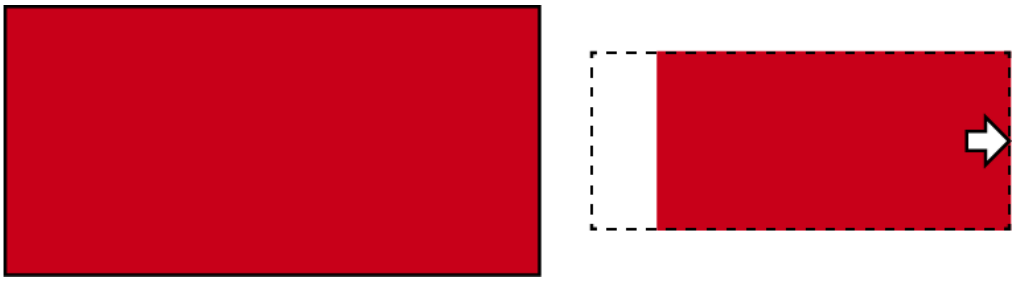
Das Bild wird proportional verkleinert und nach unten bündig in den Rahmen eingepasst.

Bild zu hoch und deutlich zu breit



Das Bild wird proportional verkleinert und nach unten bündig in den Rahmen eingepasst.

Bild zu breit und deutlich zu hoch



Das Bild wird proportional verkleinert und rechtsbündig in den Rahmen eingepasst.

23.16 Karten und Schließungs-IDs

Mit "Karten" sind in dieser Dokumentation alle Arten von passiven Identmedien gemeint.

Karten bieten zwar Vorteile wie:

- Kein Batteriewechsel
- Bedruckbar

Gleichzeitig haben Karten aber auch Nachteile:

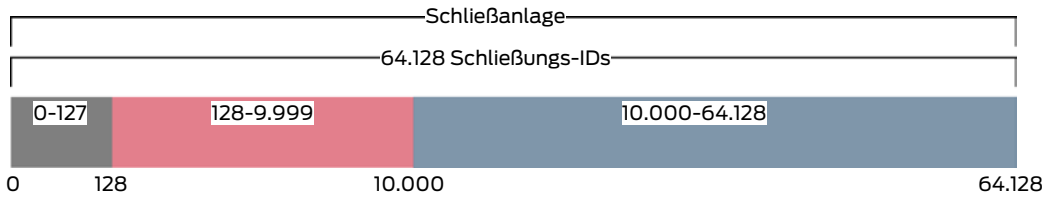
- Geringe Reichweite (wenige Millimeter)
- Weniger Speicherplatz

Vor allem auf den geringen Speicherplatz müssen Sie Rücksicht nehmen.

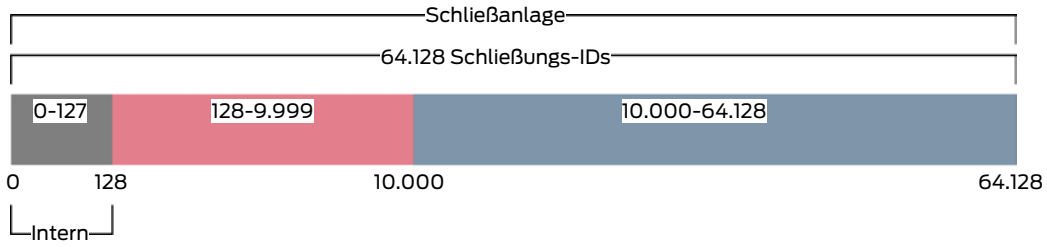
Verteilung von Schließungs-IDs in der AXM Plus

Grundsätzlich erhält jede Zeile in der Spalte mit Schließungen eine eigene LID (= Lock-ID bzw. auf deutsch Schließungs-ID). Eine Schließung kann auch mehrere Schließungs-IDs verbrauchen - zum Beispiel dann, wenn beim freidrehenden Digital Cylinder AX zwei unabhängige Leseknäufe vorhanden sind. In dem Fall wird pro Leseknauf eine Schließungs-ID verbraucht.

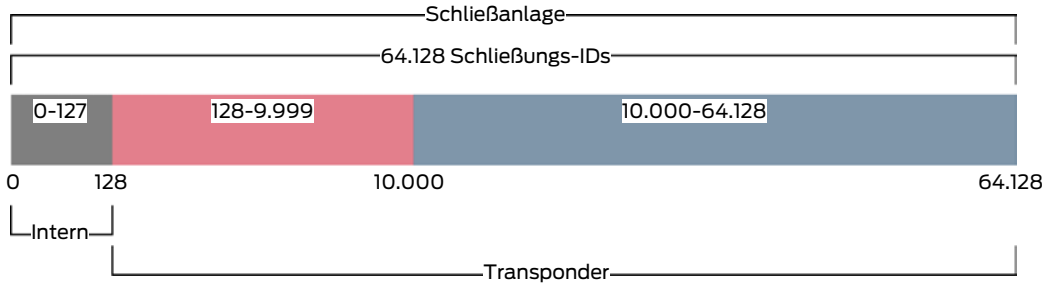
In einer aktiven Schließanlage gibt es 64.128 Schließungs-IDs (0 bis 64.128).



Die ersten 128 Schließungs-IDs (0 bis 127) sind dabei für interne Zwecke reserviert und können nicht verwendet werden.



Mit einem Transponder können Sie die Schließungs-IDs 128 bis 64.128 nutzen. Mit einem einzigen Transponder können Sie mit nur einer einzigen Schließanlage 64.000 Schließungen verwalten.



Bei Karten ist das anders. Handelsübliche Karten haben viel weniger Speicherplatz als ein Transponder. Das müssen Sie einerseits bei der Kartenkonfiguration berücksichtigen (siehe *Kartentemplates [▸ 577]* und *Kartenkonfiguration anlegen [▸ 365]*). Andererseits spielt die Größe Ihrer Karten auch eine Rolle bei der Anzahl der Schließungen, die Sie tatsächlich mit Ihren Karten verwalten können.

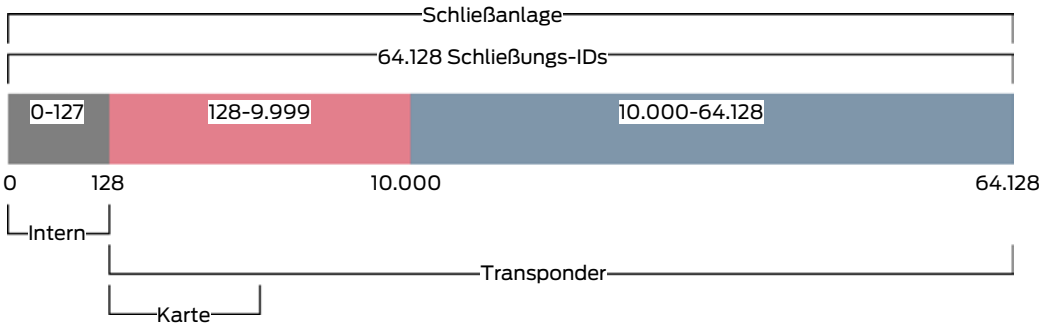
Karten können nur zusammen mit einem Kartentemplate verwendet werden. Kartentemplates unterscheiden sich durch mehrere Eigenschaften, die wichtigsten Eigenschaften sind aber ganz klar:

- Speicherbedarf
- Bereich der Schließungs-IDs

Speicherbedarf und Bereich der Schließungs-IDs hängen zusammen: Je mehr Schließungs-IDs in die Karte passen, desto mehr Speicher wird benötigt. Beispiel: Das Template MC8000L_AV kann zwar achtmal mehr Schließungen verwalten, dafür braucht es auch viermal so viel Speicher auf der Karte:

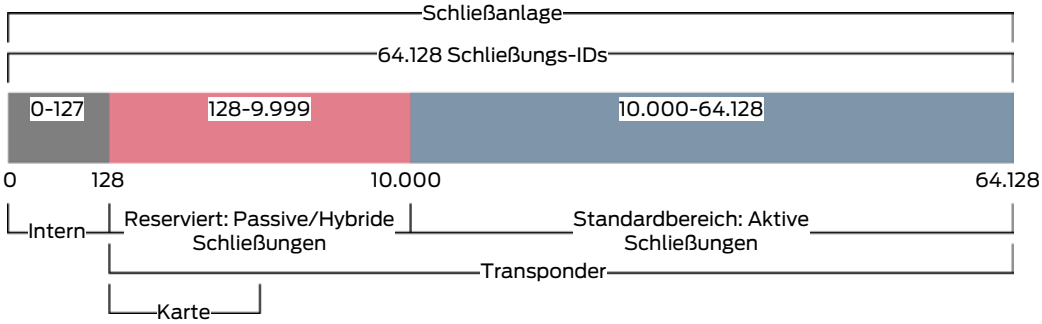
MC1000L_AV	MC8000L_AV
Kartentyp: Mifare Classic Konfiguration: MC1000L_AV Speicherbedarf: 528 Bytes Schließungs-IDs: 128 - 1127 im Kartenprofil Begehungen im Protokoll: 19 Virtuelles Netzwerk: OK	Kartentyp: Mifare Classic Konfiguration: MC8000L_AV Speicherbedarf: 2048 Bytes Schließungs-IDs: 128 - 8127 im Kartenprofil Begehungen im Protokoll: 125 Virtuelles Netzwerk: OK
528 Byte	2048 Byte
Schließungs-IDs 128 bis 1127 (= 1000 Einträge)	Schließungs-IDs 128 bis 8127 (= 8000 Einträge)

Klar wird: Karten können aus dem ganzen Bereich für Schließungs-IDs nur die niedrigeren Schließungs-IDs aus dem unteren Teil ansprechen.



Diese unteren Schließungs-IDs sind deshalb besonders "wertvoll". Aktive Schließungen sind im unteren Bereich fehl am Platz - sie können ohnehin nicht mit Karten kommunizieren, also brauchen sie auch keine der "wertvollen" niedrigen Schließungs-IDs besetzen.

Ihre AXM Plus denkt hier für Sie mit. Aktive Schließungen werden grundsätzlich erst ab der Schließungs-ID 10.000 erstellt. Somit werden die Schließungs-IDs 128 bis 9.999 für passive und hybride Schließungen freigehalten - unabhängig davon, ob Sie überhaupt Karten verwenden.



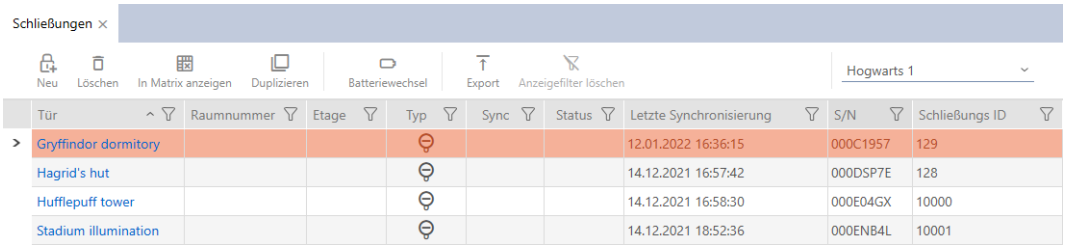
In großen Schließanlagen kann es natürlich vorkommen, dass die getrennten Bereiche zu klein werden. In solchen Fällen wird die AXM Plus den vorgesehenen Bereich verlassen:

"Zuviele" passive/hybride Schließungen	"Zuviele" aktive Schließungen
Falls Sie alle Schließungs-IDs von 128 bis 9999 mit passiven oder hybriden Schließungen belegen, ist der "reservierte" Bereich belegt. Dann würden neu erstellte Schließungen gleich behandelt und erhalten die nächsthöhere freie Schließungs-ID - unabhängig davon, ob sie aktiv oder passiv sind. Sobald eine Schließungs-ID im unteren Bereich wieder frei wird (z.B. Schließung zurückgesetzt, siehe *Zurücksetzen [▸ 273]*), wird diese wieder ausschließlich mit einer passiven oder hybriden Schließung belegt.	Sobald wenn alle Schließungs-IDs von 10.000 bis 64.128 vergeben wären, dann würde die AXM Plus auch die wertvollen Schließungs-IDs im unteren Bereich mit aktiven Schließungen besetzen. Sobald eine Schließungs-ID im oberen Bereich wieder frei wird (z.B. Schließung zurückgesetzt, siehe *Zurücksetzen [▸ 273]*), kann diese wieder mit einer aktiven Schließung belegt werden.

Schließungs-IDs im Tab [Schließungen]

Sie erkennen die Aufteilung auch im Tab [Schließungen] an der Spalte "Schließungs ID".

In diesem Beispiel sind die ersten beiden Schließungen hybride Schließungen und mit einer Schließungs-ID im wertvollen Bereich belegt (128 und 129). Die letzten beiden Schließungen sind aktive Schließungen und deshalb mit einer Schließungs-ID ab 10.000 belegt (10.000 und 10.001).



Ihr Vorteil des Konzepts für die Schließungs-IDs

Sie können sich auch später dazu entscheiden, Karten zu verwenden (siehe *Karten bzw. Transponder freischalten [▸ 401]*). Alle Schließungen, die Sie mit den Karten ansprechen können, befinden sich im unteren Bereich der Schließungs-IDs. Die aktiven Schließungen, die Sie mit Ihren Karten ohnehin nicht ansprechen könnten, befinden sich außerhalb des Bereichs der meisten Kartentemplates.

Damit wird kein Speicherplatz in den Karten unnötig durch aktive Schließungen belegt. Sie können so alle Schließungs-IDs, die in Ihre Karte passen, auch tatsächlich mit passiven oder hybriden Schließungen nutzen.

23.16.1 Kartentemplates

Konfiguration	G1/G2	Schließungs-IDs	Anzahl Schließungen	Begehungen im Protokoll	Sektoren	Speicherbedarf (Bytes)	Virtuelles Netzwerk
MCBasic	G1	-	-	-	2-15	48	-
MC1200L	G2	128-1327	1200	-	2-15	192	-
MC3800L	G2	128-3927	3800	-	2-15	528	-
MC1000L_AV	G2	128-1127	1000	19	2-15	528	√
MC_2400L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	√
MC8000L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	√
MBasic	G1	-	-	-	2-15	48	-
M1200L	G2	128-1327	1200	-	2-15	192	-
M3800L	G2	128-3927	3800	-	2-15	528	-
M1000L_AV	G2	128-1127	1000	16	2-15	528	√
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	√

Konfigu-ration	G1/G2	Schlie-ßungs-IDs	Anzahl Schlie-ßungen	Begehun-gen im Protokoll	Sektoren	Speicher-bedarf (Bytes)	Virtuelles Netzwerk
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	√
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	√
MDBasic	G1	-	-	-	2-15	48	-
MD1200L	G2	128-1327	1200	-	2-15	192	-
MD3800L	G2	128-3927	3800	-	n.a. (DES-Fire)	528	-
MD2500L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	√
MD4000L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	√
MD10000L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	√
MD32000L_AV	G2	128-32127	32000	470	n.a. (DES-Fire)	7000	√
MD2400L_AV	G2	128-2527	2400	34	n.a. (DES-Fire)	830	√
MD3650L_AV	G2	128-3777	3650	2	n.a. (DES-Fire)	830	√

24. Hilfe und weitere Informationen

Infomaterial/Dokumente

Detaillierte Informationen zum Betrieb und zur Konfiguration sowie weitere Dokumente finden Sie auf der Homepage:

https://www.simons-voss.com/de/dokumente.html

Software und Treiber

Software und Treiber finden Sie auf der Website:

https://www.simons-voss.com/de/service/software-downloads.html

Konformitätserklärungen und Zertifikate

Konformitätserklärungen und Zertifikate finden Sie auf der Homepage:

https://www.simons-voss.com/de/zertifikate.html

Technischer Support

Unser technischer Support hilft Ihnen gerne weiter (Festnetz, Kosten abhängig vom Anbieter):

+49 (0) 89 / 99 228 333

E-Mail

Sie möchten uns lieber eine E-Mail schreiben?

support-simonsvoss@allegion.com

FAQ

Informationen und Hilfestellungen finden Sie im FAQ-Bereich:

https://faq.simons-voss.com/otrs/public.pl

Adresse

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Deutschland

Das ist SimonsVoss

SimonsVoss, der Pionier funkgesteuerter, kabelloser Schließtechnik, bietet Systemlösungen mit breiter Produktpalette für die Bereiche SOHO, kleine und große Unternehmen sowie öffentliche Einrichtungen. SimonsVoss-Schließsysteme verbinden intelligente Funktionalität, hohe Qualität und preisgekröntes Design Made in Germany.

Als innovativer Systemanbieter legt SimonsVoss Wert auf skalierbare Systeme, hohe Sicherheit, zuverlässige Komponenten, leistungsstarke Software und einfache Bedienung. Damit wird SimonsVoss als ein Technologieführer bei digitalen Schließsystemen angesehen.

Mut zur Innovation, nachhaltiges Denken und Handeln sowie hohe Wertschätzung der Mitarbeiter und Partner sind Grundlage des wirtschaftlichen Erfolgs.

SimonsVoss ist ein Unternehmen der ALLEGION Group – ein global agierendes Netzwerk im Bereich Sicherheit. Allegion ist in rund 130 Ländern weltweit vertreten (www.allegion.com).

Made in Germany

Für SimonsVoss ist „Made in Germany“ ein ernsthaftes Bekenntnis: Alle Produkte werden ausschließlich in Deutschland entwickelt und produziert.

© 2025, SimonsVoss Technologies GmbH, Unterföhring

Alle Rechte vorbehalten. Texte, Bilder und Grafiken unterliegen dem Schutz des Urheberrechts.

Der Inhalt dieses Dokuments darf nicht kopiert, verbreitet oder verändert werden. Technische Änderungen vorbehalten.

SimonsVoss und MobileKey sind eingetragene Marken der SimonsVoss Technologies GmbH.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION