AX MANAGER

The next dimension of Locking System Management

AXM Lite

Manual

12.02.2025

Simons Voss technologies

ALLEGION

Contents

1. General safety instructions ... 8
2. Product-specific safety instructions ... 9
3. Meaning of the text formatting ... 10
4. Intended use ... 11
5. General ... 12
6. Information on data protection ... 13
6.1 IT basic protection ... 13
6.1.1 What protection requirements do the data processed in the system have? ... 13
6.1.2 What IT infrastructure requirements are recommended? ... 13
6.2 Encryption ... 13
6.2.1 Is the data in System 3060 encrypted? ... 13
6.2.2 What data is encrypted? ... 13
6.2.3 Are the transmission paths via radio, for example, also encrypted? ... 14
6.3 Working in compliance with data protection regulations (GDPR) ... 14
6.3.1 What personal data is stored in the software? ... 14
6.3.2 For what purpose is personal data stored in the software? ... 14
6.3.3 How long is personal data stored in the software? ... 14
6.3.4 Can the right to read access lists be additionally secured? ... 15
6.3.5 Is personal data in the software protected against access by third parties? ... 15
6.3.6 Can the stored data be made available as a copy? ... 15
6.3.7 Can personal data be deleted from the software? ... 15
7. Range of functions for AXM Lite ... 16
8. System requirements ... 17
9. Release notes ... 18
9.1 Version 1.0.2306.1402 ... 18
9.2 Version 1.0.2205.2402 ... 18
9.3 Version 1.0.2401.0501 ... 18
9.4 Version 1.0.2402.2701 ... 18
9.5 Version 1.0.2502.0602 ... 19
10. Installation ... 20
10.1 Run AXM as the administrator (recommended) ... 21
10.2 Updating AXM ... 25
11. First steps after a new installation ... 27

11.1 Best practice: setting up the locking system ... 29
11.2 Best practice: Database protection ... 30

12. Registration ... 31

13. The AXM's structure ... 35

13.1 Sorting and filtering ... 37
13.2 Installation wizards ... 40
13.3 Multiple options, same result ... 40
13.4 Global search ... 41
13.5 Working with AXM more effectively ... 41
13.5.1 Tab operation ... 41
13.5.2 Hotkeys ... 42
13.5.3 Creating additional objects ... 43

14. Organisational structure ... 44

14.1 Creating access levels ... 44
14.2 Creating a schedule ... 45
14.3 Create time group ... 49
14.4 Deleting a time group ... 53
14.5 Deleting schedules ... 56
14.6 Creating a time switchover ... 58
14.7 Creating and editing public holidays ... 61
14.8 Creating and editing public holiday lists ... 65
14.9 Creating a location ... 69
14.10 Creating a building and assigning it to a location ... 72
14.11 Creating a hashtag ... 74

15. Persons and identification media ... 77

15.1 Creating an identification medium ... 77
15.1.1 Creating transponders and cards ... 77
15.1.2 Creating PIN code keypads ... 83
15.1.3 Creating special identification media ... 88
15.2 Duplicating an identification medium (including authorisations and settings) ... 93
15.3 Deleting an identification medium ... 94
15.3.1 Deleting a card/transponder ... 94
15.3.2 Deleting a PIN (PIN code keypad AX) ... 99
15.4 Allowing an identification medium to open twice as long ... 100
15.5 Muting all locking devices for an identification medium ... 101
15.5.1 Muting all locking devices for a transponder or a card ... 102

15.6 Allow accesses to be recorded by identification media (physical access list) 103
15.7 Restricting identification medium authorisations to specific times (time group) 104
15.8 Activating or deactivating identification medium once at specific times (activation and expiry date) 104
15.9 Handling defective identification media 107
15.9.1 Repairing/resynchronising 111
15.9.2 Resetting and replacing 116
15.9.3 Delete and replace 119
15.9.4 Take out of use and leave in project 127
15.9.5 Taking out of use and deleting from the project 134
15.10 Duplicating forgotten identification medium temporarily 140
15.10.1 Duplicating a forgotten transponder or card temporarily 140
15.11 Blocking lost/stolen identification media permanently 145
15.11.1 Blocking and replacing lost/stolen card/transponder permanently 146
15.11.2 Blocking a lost/stolen PIN code keypad permanently 151
15.12 Flag and reset returned identification medium (back to inventory) 156
15.12.1 Flagging and resetting returned card/transponder (back to inventory) 156
15.13 Planning and tracking identification medium management tasks 158
15.13.1 Noting the issue date 160
15.13.2 Planning and logging battery replacement 162
15.13.3 Planning and logging return 167
15.14 Finding the identification medium or locking device again in the matrix 170
15.15 Exporting identification media as a list 170
15.15.1 Export cards/transponders as a list 170
15.15.2 Exporting PINs and PIN code keypads as a list 172
15.16 Viewing an identification medium's serial number and/or TID 173
15.16.1 Viewing a card's/transponder's serial number and TID 173
15.16.2 Viewing a PIN code keypad's serial number 175
15.17 Setting the PIN length (PinCode AX) 177
15.18 Changing a PIN (PinCode AX) 180
16. Doors and locking devices 182
16.1 Creating a locking device 182
16.2 Duplicating the locking device (including authorisations and settings) 191
16.3 Delete locking device 193
16.3.1 Deleting an individual locking device using the matrix 194
16.3.2 Deleting several locking devices using the tab 195
16.4 Changing locking device type at later stage 197
16.5 Handling defective locking devices 200
16.5.1 Re-synchronise (repair) 203

16.5.2 Resetting and replacing ... 205
16.5.3 Delete and replace ... 210
16.5.4 Reset ... 214
16.5.5 Purge (only reset in database/software reset) ... 216
16.6 Assigning locking devices to buildings/locations ... 218
16.7 Limiting authorisations for locking devices to specific times (schedule) ... 220
16.8 Engaging and disengaging locking devices automatically with time switchover ... 222
16.9 Have accesses logged by locking device (access list) ... 228
16.10 Leaving the locking device open for longer, less time or permanently ... 229
16.11 Limit locking device read range (close range mode) ... 231
16.12 Muting a locking device (for battery warnings and programming) ... 233
16.13 Ignoring activation and expiry date of identification media ... 234
16.14 Setting up door monitoring (DoorMonitoring) ... 236
16.14.1 Setting up DoorMonitoring for locking cylinders ... 236
16.15 Changing the SmartRelay settings ... 242
16.15.1 Using internal and external antenna simultaneously ... 243
16.15.2 Invert outputs ... 244
16.15.3 Using the serial interface ... 246
16.15.4 Changing the signalling ... 247
16.16 Planning and tracking locking device management tasks ... 248
16.16.1 Note installation, replacement or removal date ... 250
16.16.2 Planning and logging battery replacement ... 252
16.17 Exporting locking devices as a list ... 253

17. Permissions ... 256

17.1 Changing individual authorisations (cross) ... 256
17.2 Changing many authorisations (on identification media and/or locking devices) ... 257
17.2.1 Allowing all or blocking all ... 257
17.2.2 Access levels ... 261
17.2.3 Controlling authorisations in terms of time (schedules) ... 272
17.3 Meaning of the authorisation crosses in the matrix ... 279

18. Locking systems ... 280

18.1 Changing locking system password ... 280
18.2 Using a common locking level ... 284
18.2.1 Creating a common locking level ... 285
18.2.2 Creating transponders for common locking level ... 287
18.2.3 Authorising a transponder with common locking level ... 288

19. Synchronisation: Comparison between locking plan and reality ... 290

19.1 Synchronising the locking device (including reading access list) ... 291

19.1.1 Display locking device equipment and status ... 294
19.1.2 Displaying and exporting a locking device's access list ... 296
19.2 Identifying an unknown locking device ... 298
19.3 Re-setting the locking device ... 300
19.4 Synchronising an identification medium ... 303
19.4.1 Synchronise a card/transponder (including importing physical access list) ... 304
19.5 Identifying an unknown ID medium ... 309
19.5.1 Recognise unknown cards/transponders ... 309
19.5.2 Identifying unknown PIN code keypad ... 311
19.6 Resetting identification media ... 312
19.6.1 Resetting cards/transponders ... 312
19.6.2 Resetting the PIN code keypad ... 316
19.7 Viewing connected/supported programming devices ... 319

20. Your personalised AXM interface ... 321
20.1 Interchanging (transposing) doors and persons in the matrix ... 321
20.2 Select columns and rows in the matrix (enable/disable crosshairs) ... 322
20.3 Click to change authorisations ... 323
20.4 Hiding deactivated and defective identification media ... 324
20.5 Showing or hiding rows/columns in the matrix ... 325
20.6 Reading access list/physical access list during synchronisation ... 327
20.7 Limiting the number of access list entries in the database ... 329
20.8 Pinning tabs ... 330
20.9 Changing automatic numbering ... 332
20.10 Changing the language ... 333
20.11 Preventing generated reports from opening automatically ... 334

21. Administrative tasks ... 336
21.1 Creating a backup ... 336
21.2 Restoring the backup ... 338
21.3 Exporting error logs ... 340
21.4 Displaying version number and licence key for the AXM installed ... 341
21.5 User management ... 343
21.5.1 Changing the user password ... 343
21.5.2 Increase password security ... 345

22. Statistics and logs ... 348
22.1 Displaying and exporting a locking device's access list ... 348
22.2 Displaying and exporting physical access lists for cards/transponders ... 350

22.3 Display doors for which a specific identification medium is authorised 352
22.4 Displaying identification media which are authorised for a specific door 353
22.5 Displaying a locking device's equipment features 354
22.6 View statistics and warnings (dashboard) 355
22.7 Tracking activities in the database (log) 356
22.7.1 Setting the log archiving period 358

23. Background knowledge and explanations 360

23.1 Identification media, locking devices and the locking plan 360
23.2 "Engaging", "opening", "locking", etc. 362
23.3 Synchronisation of database and actual state 364
23.4 Access and physical access lists 365
23.5 Event management 366
23.5.1 Time groups and schedules 366
23.5.2 Time switchovers 370
23.6 Access levels 378
23.7 Passwords used 379
23.8 Buildings and locations 379
23.9 Hashtags 380
23.10 DoorMonitoring 380
23.10.1 Possible DoorMonitoring states of locking cylinders 381
23.10.2 Possible DoorMonitoring states of SmartHandles 381
23.10.3 Possible DoorMonitoring states of SmartRelais 3 381

24. Help and other information 382

1. General safety instructions

Signal word: Possible immediate effects of non-compliance
WARNING: Death or serious injury (possible, but unlikely)
IMPORTANT: Property damage or malfunction
NOTE: Low or none

WARNING

Blocked access

Access through a door may stay blocked due to incorrectly fitted and/or incorrectly programmed components. SimonsVoss Technologies GmbH is not liable for the consequences of blocked access such as access to injured or endangered persons, material damage or other damage!

Blocked access through manipulation of the product

If you change the product on your own, malfunctions can occur and access through a door can be blocked.

- Modify the product only when needed and only in the manner described in the documentation.

NOTE

Intended use

SimonsVoss-products are designed exclusively for opening and closing doors and similar objects.

- Do not use SimonsVoss products for any other purposes.

Qualifications required

The installation and commissioning requires specialized knowledge.

- Only trained personnel may install and commission the product.

Modifications or further technical developments cannot be excluded and may be implemented without notice.

The German language version is the original instruction manual. Other languages (drafting in the contract language) are translations of the original instructions.

Read and follow all installation, installation, and commissioning instructions. Pass these instructions and any maintenance instructions to the user.

2. Product-specific safety instructions

IMPORTANT

Changes to the locking system only take effect after synchronisation

If you edit the locking system with the AXM Lite, the changes are initially only saved to your database.

Your actual components will not know about these changes until they are synchronised.

1. Regularly check the components in the matrix for synchronisation requirements (see *The AXM's structure [▸ 35]*).
2. In the event of critical incidents (e.g. identification medium lost), it is particularly important to synchronise immediately after responding to the incident (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*).

NOTE

Do not use Alt+F4 to close open windows

Windows open in the foreground block the remaining ones AXM Lite for further input. If you do not close such a window properly using the available buttons, but use Alt+F4 instead, then the window is closed, but the rest of AXM Lite remains greyed out. You will therefore lock yourself out of the AXM Lite.

- Do not use Alt+F4 to close windows in the foreground.

3. Meaning of the text formatting

This documentation uses text formatting and design elements to facilitate understanding. The table explains the meaning of possible text formatting:

Example	button
☑ Example ☐ Example	checkbox
◉ Example	Option
[Example]	Tab
"Example"	Name of a displayed window
| Example |	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
Example	Field
Example	Name of a (Windows) service
Example	Commands (e.g. Windows CMD commands)
`Example`	Database entry
[Example]	MobileKey type selection

4. Intended use

The AX Manager Lite (AXM Lite) is a software for uncomplicated locking system management. It simplifies administration and control of locking components and authorisations in System 3060. Large and complex locking systems can be easily maintained using the SQL database.

5. General

The AX manager, abbreviated AXM, follows the footsteps of the well-proven LSM.

The interface is redesigned from scratch, intuitive and clear. It helps with daily tasks regarding all supported components (see Scope of AXM Lite).

New in AXM

In comparison to the LSM the AXM comes with the following major innovations:

- Microsoft SQL database as widespread substructure for databases
- Future-proof operation through touchscreen-operation
- Simplified tasks with user-friendly assistents
- Authorization groups: Collecting tank for identification media and closures. All contained identification media are automatically authorized to all contained closures.
- Keep an eye on everything: Global search in the whole software

Lite edition

With the lite edition we are evolving to the next level of locking system management. This edition comes with selected features and a limited size for the locking system. (see LSM Starter edition).

You may manage up to 20 locks and 100 transponders.

6. Information on data protection

6.1 IT basic protection

6.1.1 What protection requirements do the data processed in the system have?

In general, only non-critical data with so-called normal protection requirements are processed and stored in the software. This means data whose hypothetical loss neither damages the reputation of a person nor the image of a company. A high financial loss is also not to be expected.

6.1.2 What IT infrastructure requirements are recommended?

According to the German Federal Office for Information Security (BSI), basic IT security is therefore sufficient as a security concept for a SimonsVoss locking system and is regarded as a recommended minimum requirement for your IT infrastructure.

6.2 Encryption

6.2.1 Is the data in System 3060 encrypted?

Yes. Data packets are encrypted end-to-end within the system's own communication network. We utilise multi-level data protection techniques, which we ultimately secure with standard encryption methods (AES, 3DES). The latest versions of our products increase the level of security, as they always reflect the current state of the art.

NOTE

Locking system password as part of the security concept

The locking system password you assign (not the user) is part of the overall security concept. With a complex password, you automatically increase the length of the encryption key used and thus the security of your data. We recommend a minimum of 12 characters and the use of numbers, lower case, upper case and special characters. Please store the locking system password in a secure place (e.g. in a safe) to which only authorised persons have access.

6.2.2 What data is encrypted?

Within the system's own communication network, no personal data is processed. It pseudonymised instead using the identification numbers. They cannot be associated with a real person even without encryption.

6.2.3 Are the transmission paths via radio, for example, also encrypted?

No. Thanks to consistent end-to-end encryption, our secure communication is independent of the transmission method. Intercepted data cannot be read without the appropriate secret key. End-to-end encryption allows the use of system-specific transmission paths without loss of performance.

6.3 Working in compliance with data protection regulations (GDPR)

6.3.1 What personal data is stored in the software?

It is possible to store the following data of a person in the software:

- First name
- Last name*
- Title
- Address
- Phone
- E-Mail
- Personnel number*
- User name
- Department
- City/Building
- Set From/To
- Date of birth
- Cost center
- Photo

Only the last name and personnel number (*mandatory fields) are required when using the software. Special categories of personal data according to Art. 9 GDPR are not stored.

6.3.2 For what purpose is personal data stored in the software?

In order to be able to make full use of the functions of an electronic locking system, it is necessary to be able to assign the identification media used (e.g. transponder) to a specific user (e.g. employee).

6.3.3 How long is personal data stored in the software?

The data is stored within the locking system for at least the duration of the occupation of an identification medium (e.g. company affiliation).

The duration of data storage, e.g. in logs and access lists, can be changed at will by the locking system administrator.

6.3.4 Can the right to read access lists be additionally secured?

When using the optional ZK function in our locking components, access to the data collected with it can be equipped with increased user rights.

Example: A separate user is created for the works council. Only this user is given reading rights to the access lists in case of suspicion. In addition, this user can be protected with a shared password. Only one part of the password is known to two or more members of the works council.

6.3.5 Is personal data in the software protected against access by third parties?

In principle, the user (end customer) of the locking system and the software is responsible for managing and securing access rights.

In the locking system itself, all data is secured using a multi-level encryption process. Opening the graphical user interface to access the data is not possible without a password and appropriate user rights.

There shall be no automatic transmission to third parties, use or processing by SimonsVoss.

6.3.6 Can the stored data be made available as a copy?

All collected data on a data subject can be made available as a copy by means of an export function (Art. 15 GDPR).

6.3.7 Can personal data be deleted from the software?

Personal data can be validly deleted from the software (from version 3.4 SP1) and the associated database at the request of a data subject in accordance with Art. 17 GDPR.

7. Range of functions for AXM Lite

Projects/locking systems	A project with a locking system
Users	One user
Number of locking devices	20
Number of credentials	100 (transponders only)
Locking devices and identification media supported	■ G2 components ■ AX components
	■ Digital Cylinder AX ■ Locking Cylinder 3061 ■ SmartHandle AX ■ SmartHandle 3062 ■ SmartRelay 3063 (G2) ■ SmartRelay 2 3063 ■ Padlock ■ Padlock AX ■ SmartLocker AX ■ Furniture lock (G2)
Programming devices	■ CD.Starter.G2 ■ SmartCD.G2/SmartCD2.G2 ■ SmartStick AX

You can upgrade at any time if your version reaches its limits.

8. System requirements

AXM Lite

Operating system	■ Windows 10 ■ Windows 11
Processor	1,44 GHz or faster (Intel, AMD) No support for ARM processors under System 3060
Random access memory	4 GB or more (recommended: 8 GB)
Free space	500 MB (physically)
Display	■ 10" or bigger ■ 1280×768 or more
.NET Framework	4.7
Supported MS SQL edition	SQL Server Express Local DB 2019

9. Release notes

9.1 Version 1.0.2306.1402

Released on 14.06.2023

Improvements

1. Function Distribution of lock ID and battery warning by receipts
2. Optimisation of the entire backup process

Bugfixes

1. Correction of target status of transponder when assigning to access levels
2. Faulty programming requirements - Duplicated transponder and changed time control
3. Display and configuration of cylinder 3061 with push-button control
4. Various text corrections
5. Display and configuration of cylinder 3061 with push-button control

9.2 Version 1.0.2205.2402

Released on 05.01.2023

Improvements

1. Support for all further developments of our AX components (HP2)

Bugfixes

1. Correction in the display of numbers in foreign languages
2. Erroneous programming requirements - Changing public holidays
3. Correction of the battery status display

9.3 Version 1.0.2401.0501

Released on 05.01.2024

Bugfixes

1. Expiry date 01.01.2024 removed

9.4 Version 1.0.2402.2701

Released on 01.03.2024

Improvements

1. Support for the new SmartHandle AX Advanced

9.5 Version 1.0.2502.0602

Released on 07.02.2025

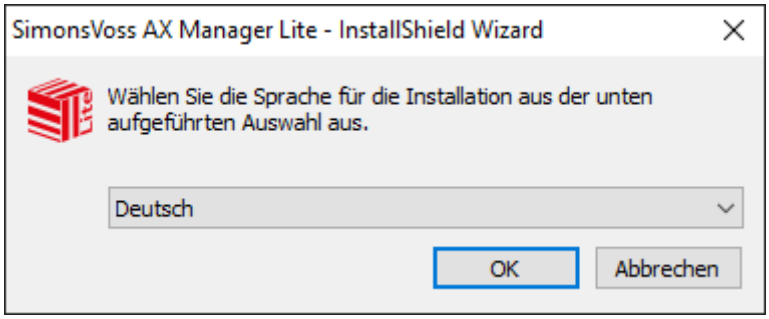
Bugfixes

1. Expiry date 01.02.2025 removed

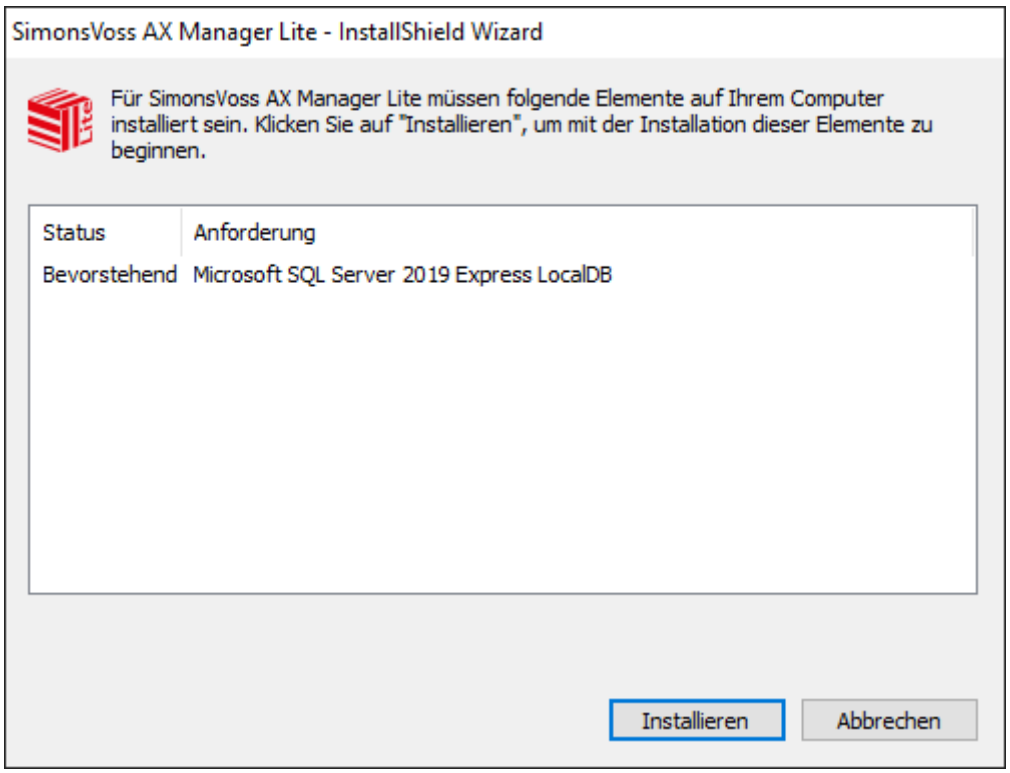
10. Installation

✓ System requirements fulfilled for the AXM Lite (see *System requirements [▸ 17]*).

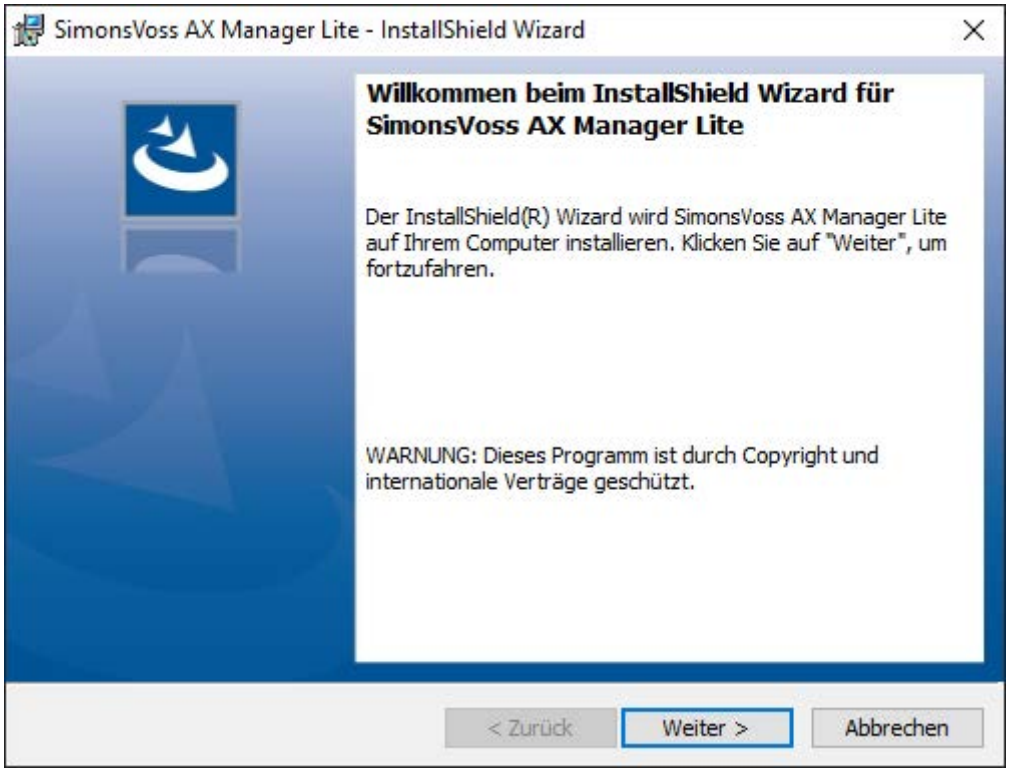
1. Execute the set-up file.
   ↳ The InstallShield wizard will open.



2. Select the language in which the is AXM Lite to be installed.
   ↳ Set-up checks whether additional software needs to be installed.



3. Install the additional software displayed if required.
   ↳ The AXM Lite set-up will open.



4. Follow the AXM Lite set-up.

↳ AXM Lite is installed.

10.1 Run AXM as the administrator (recommended)

SimonsVoss recommends that you always start AXM Lite as the administrator. This ensures potential problems due to lack of access and write permissions can be avoided from the outset:

Manual start as administrator

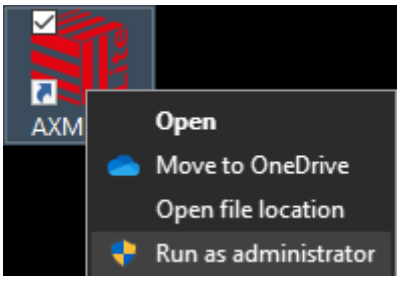
✓ AXM Lite installed.

✓ Administrator rights available.

1. Locate the shortcut or the AXM Lite icon.

2. Right-click on the shortcut menu to open the context menu.

3. Click on the Run as administrator entry with your name.



↳ AXM Lite runs as the administrator.

Automatic start-up as the administrator

Starting manually as the administrator has two disadvantages:

- Inconvenient.
- You might forget to start AXM Lite as the administrator.

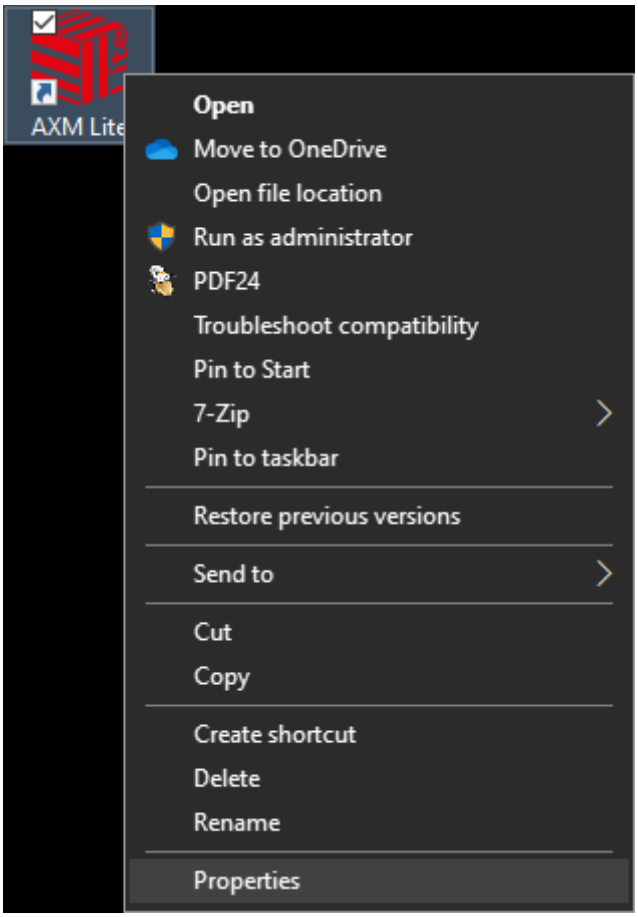
Consequently, SimonsVoss recommends that the properties of the link to AXM Lite be set so that the AXM Lite is always run as administrator using this shortcut.

✓ AXM Lite installed.
✓ Administrator rights available.

1. Locate the shortcut or the AXM Lite icon.

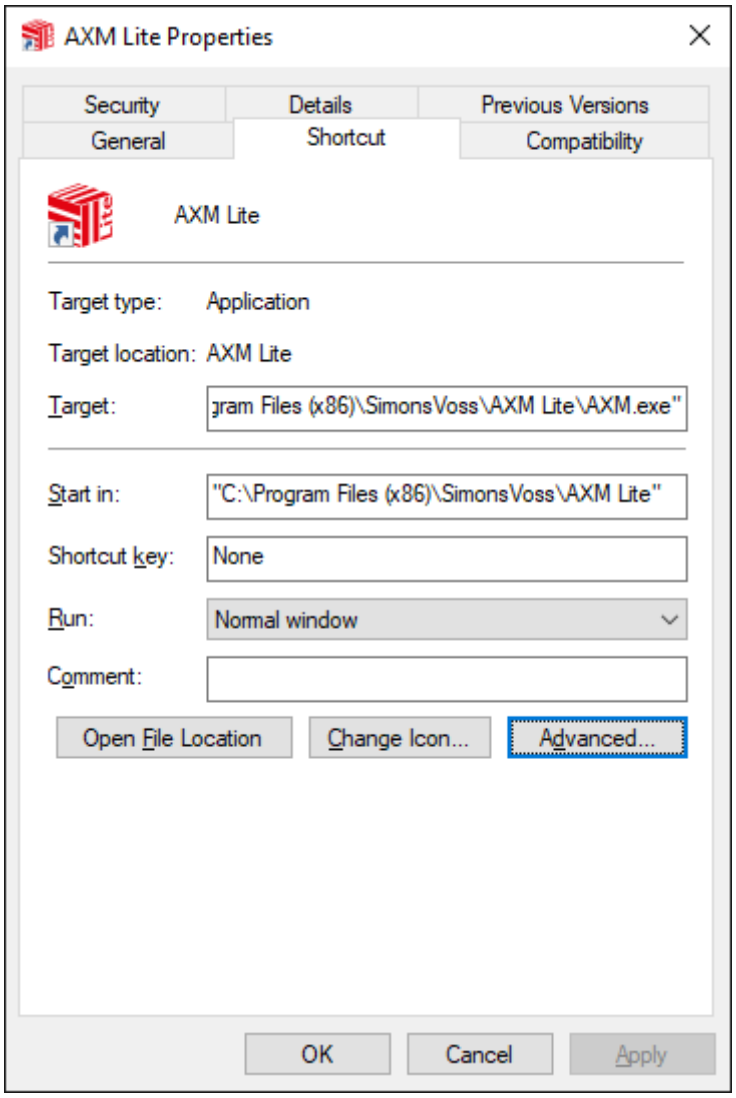
2. Right-click on the shortcut menu to open the context menu.

3. Click on the Properties entry with your name.

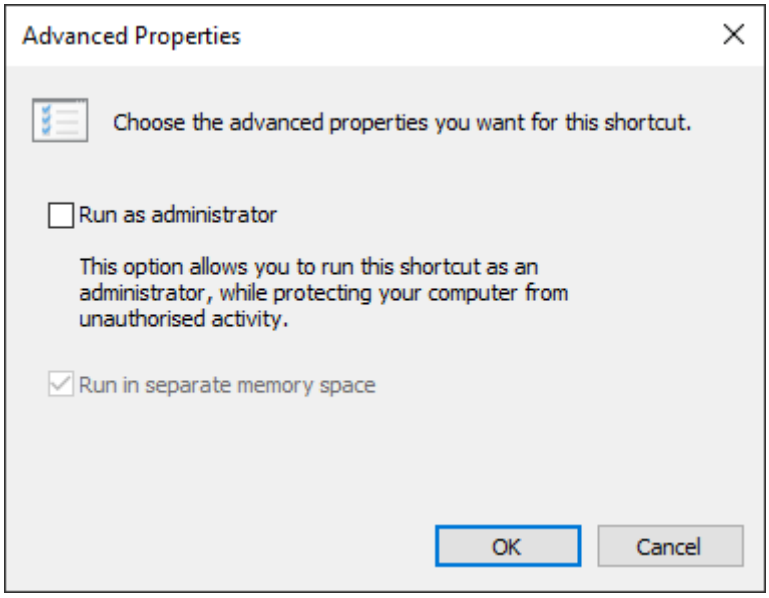


↳ The "AXM ... Properties" window will open.

4. Go to the [Link] tab.



5. Click on the Advanced... button.
   ↳ The "Advanced Properties" window will open.



6. Activate the ☑ Run as administrator checkbox.
7. Click on the OK button.
   ↳ Window "Advanced Properties" closes.
8. Click on the OK button.
   ↳ Window "AXM ... Properties" closes.

↳ If you start AXM Lite via this link in the future, AXM Lite will automatically run as the administrator.

10.2 Updating AXM

With the latest AXM Lite, you have the best software and hardware support. This is why your AXM Lite checks whether updates are available and also offer them for installation every time it launches. Back up your database (see *Creating a backup [▸ 336]*) before updating.

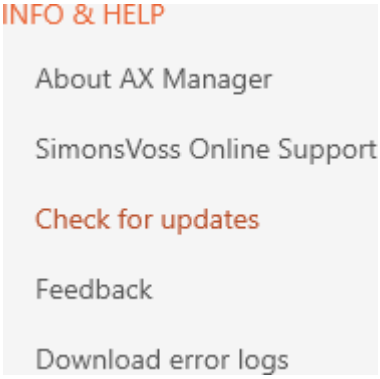
See *Displaying version number and licence key for the AXM installed [▸ 341]* to view the currently installed version of your AXM Lite instead.

Obviously, you can also check manually whether an update is available and install it.

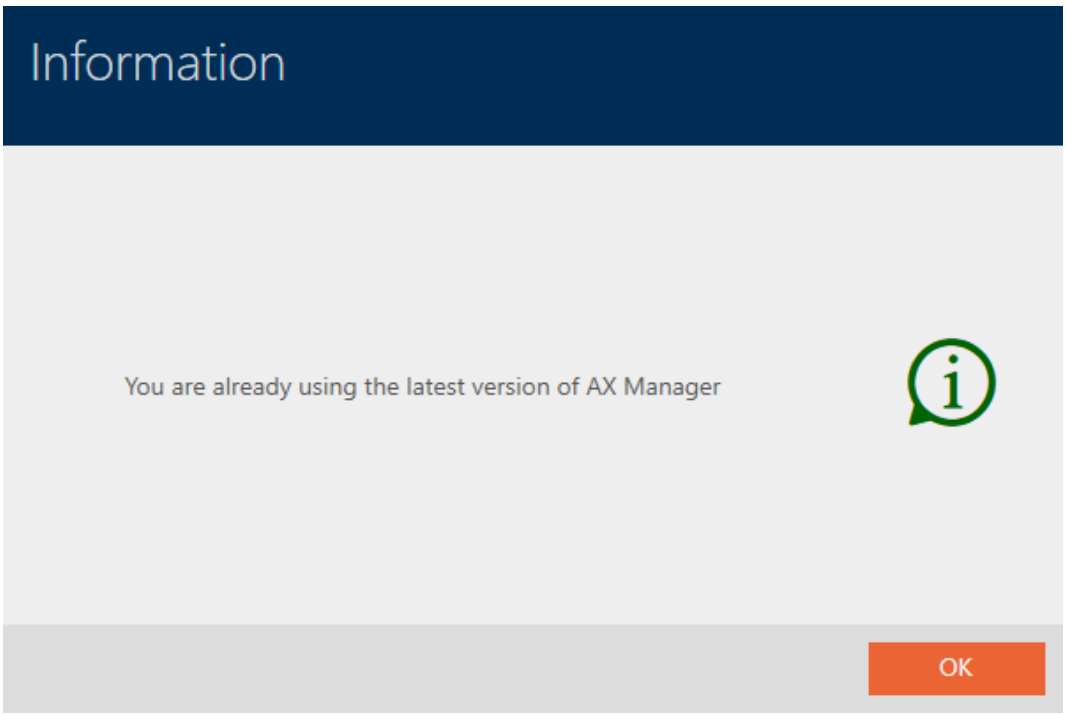
✓ AXM Lite open.
✓ Database backed up.

1. Click on the orange AXM icon ☰ AXM.
   ↳ AXM bar opens.

2. Click on the Check for updates entry in the | INFO & HELP | group.

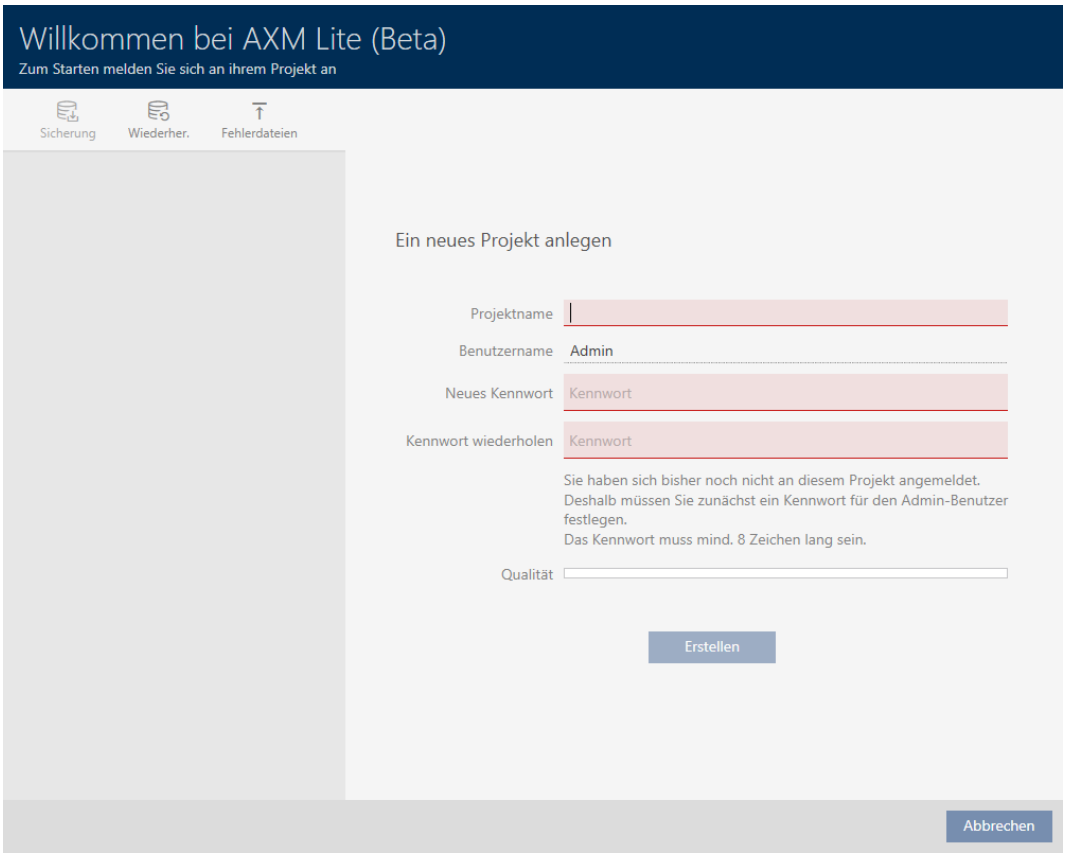


↳ If an update is available, it is displayed and offered for installation. If your AXM Lite is up to date, you will see this window:



11. First steps after a new installation

AXM Lite will greet you with the login screen after installation.



You will see the following input fields:

- *Project name*
- *Username*
- *New password*
- *Repeat password*

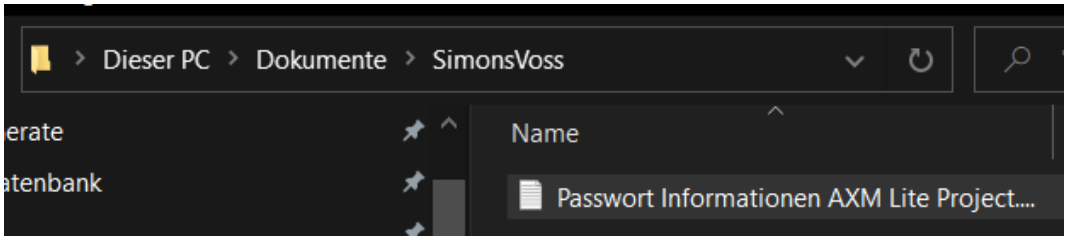
1. Enter a project name in the *Project name* field.
2. Enter a password of at least 8 characters in the *New password* field to protect your project.
   ↳ A coloured bar shows you how secure your password is.

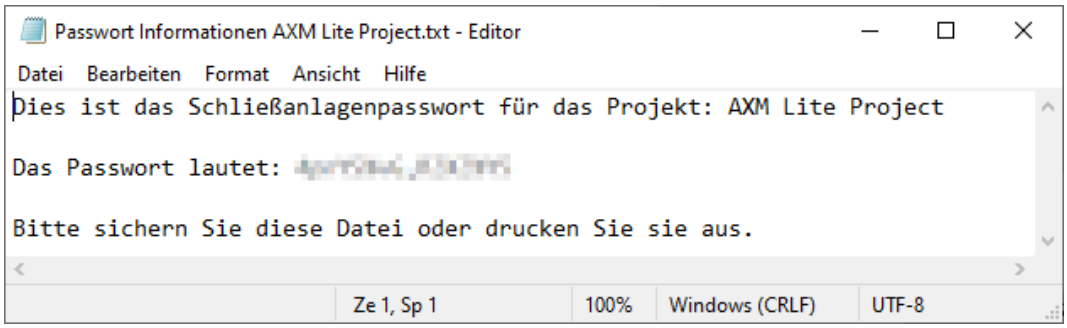
3. Repeat the password entered in the *Repeat password* field.
4. Click on the Create button.

↳ The new project is protected.

You can change the user password you have just created if required (see *Changing the user password [▸ 343]*).

The first locking system password is generated automatically and saved in a text file (`Documents/SimonsVoss`).





You can change the locking system password (see *Changing locking system password [▸ 280]*).

IMPORTANT

Keep locking system password accessible and secure

The locking system password is the most important password of all. For security reasons, SimonsVoss is not able to reset any components without a locking system password or backup. There is no general master key.

It is no longer possible to program components if the locking system password is no longer known or can no longer be recovered from a backup. The components must be removed from locks and disposed of, which takes a great deal of effort.

1. Ensure that authorised persons can be view and/or access the locking system password at any time.
2. Take into account both foreseeable events (e.g. locking system administrator retires) and unforeseeable events (e.g. locking system administrator leaves post).

Launching AXM Lite for the first time

AXM Lite now offers you several wizards one after the other:

1. Add locking device
2. Add transponder

These wizards allow you to start building your locking system directly and familiarise yourself with the AXM Lite interface.

However, before setting up a large locking system, plan things out first in preparation (see *Best practice: setting up the locking system [▸ 29]*).

If you are working with a locking system for the first time, you will find explanations and background information here: *Background knowledge and explanations [▸ 360]*.

11.1 Best practice: setting up the locking system

You will save a great deal of time and effort if you set up your locking system systematically in an order sequence where you only need to open the windows once as far possible.

As a basic rule, the easiest way is to prepare the organisational structure first (see *Organisational structure [▸ 44]*).

Experience has shown that the following approach is best:

1. Create locations (see *Creating a location [▸ 69]*).
2. Create building (see *Creating a building and assigning it to a location [▸ 72]*).
3. Create the first schedule (see *Creating a schedule [▸ 45]*).
4. Create all required time groups (see *Create time group [▸ 49]*).
5. Create additional schedules, setting the time groups directly for each schedule while doing so.
6. Create access levels (see *Access levels [▸ 261]*).
7. Create identification media and assign them directly to the access levels and time groups when they are created (see *Creating transponders and cards [▸ 77]* and *Restricting identification medium authorisations to specific times (time group) [▸ 104]*).
8. Create locking devices and assign them directly to access levels and schedules when they are created (see *Creating a locking device [▸ 182]* and *Limiting authorisations for locking devices to specific times (schedule) [▸ 220]*).

9. Synchronise locking devices (see *Synchronising the locking device (including reading access list) [▸ 291]*).
10. Synchronise identification media (see *Synchronise a card/transponder (including importing physical access list) [▸ 304]*).

If you use this order sequence, you can use the results from the previous steps directly in the next steps:

- Setting up time groups for newly created schedules directly in the Created Schedule window
- Time group and access levels directly in the window for the created identification medium
- Schedule and access level directly in the window for the created locking device

Background knowledge for you to take into account for time management and access levels:

- *Event management [▸ 366]*
- *Access levels [▸ 378]*

Obviously, you can deviate from this sequence and first create identification media and locking devices without a time group, for example. However, if you need time management at a later stage, you will need to:

- Assign a schedule to each locking device included in time management
- Assign a time group to each transponder.

11.2 Best practice: Database protection

You can further enhance the security level of your AXM Lite by protecting access to your SQL database.

1. Create a separate Windows user account for the locking system administrator.
2. Use a strong password for all Windows user accounts.
3. Encrypt the hard disk where the database is stored.

12. Registration

You can try AXM Lite out for 90 days after initial installation. After the trial period, you will need to register the software to continue using it.

Create licence request

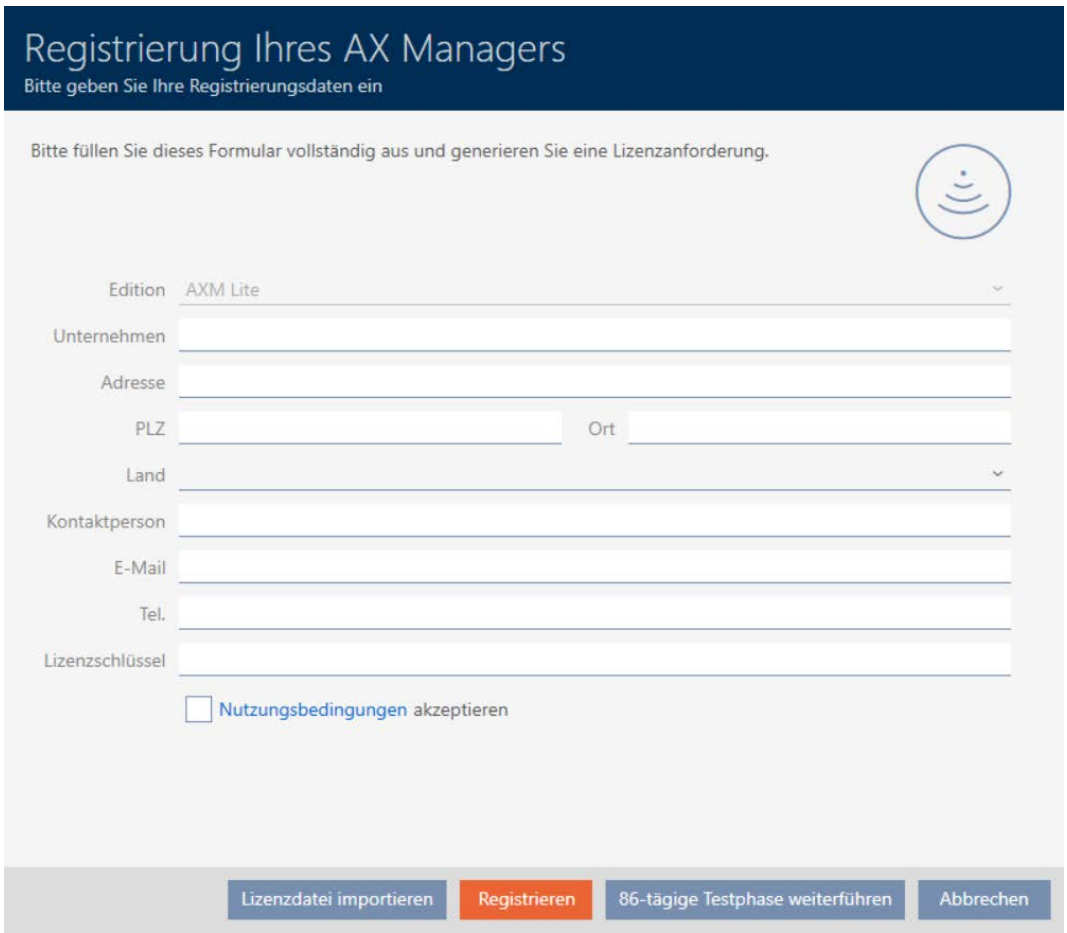
First of all, you make a licence request. To do this, you will need:

- Licence key
- Consignment number
- Order number

✓ AXM Lite open.

1. Click on the < Register now button at the bottom of AXM Lite .

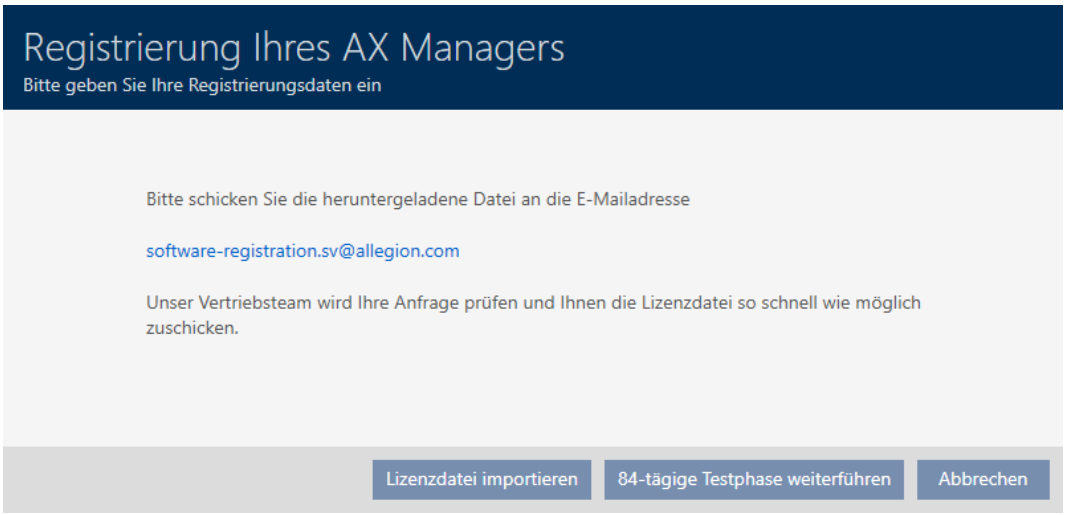
↳ The registration form will open.



2. Complete the registration form in full.
3. Enter your licence key (XXXX-XXXX-XXXX-XXXX).

4. Select the ☑ Terms of Use accept checkbox.

5. Click the Register button.
   ↳ The Explorer window will open.
6. Save the registration file (extension: .rgo) to a file directory of your choice.
   ↳ Explorer window closes.
   ↳ Registration form will display an email address.

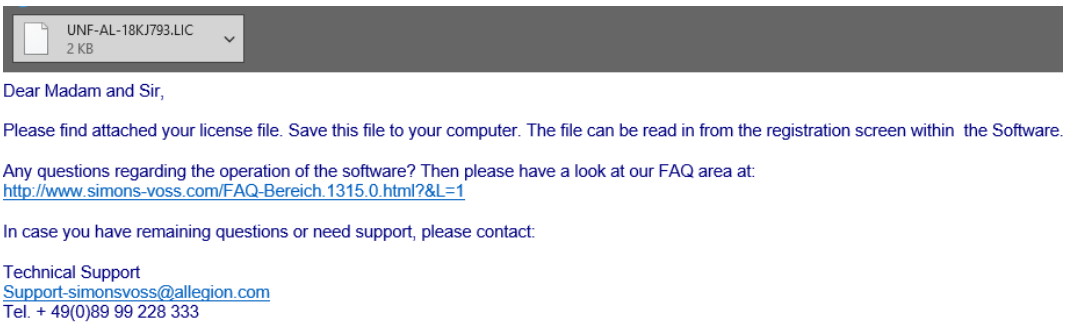


7. Send an email with the registration file, order number and consignment number to software-registration.sv@allegion.com.

↳ SimonsVoss will check your licence request.

Importing the licence file

Once your licence request has been checked and accepted, you will receive an email from SimonsVoss containing a licence file (extension: .lic).



Register your AXM Lite by importing this licence file.

✓ AXM Lite open.

1. Save the licence file you received in a file directory of your choice.
2. Click on the < Register now button at the bottom of AXM Lite .

↳ The registration form will open.

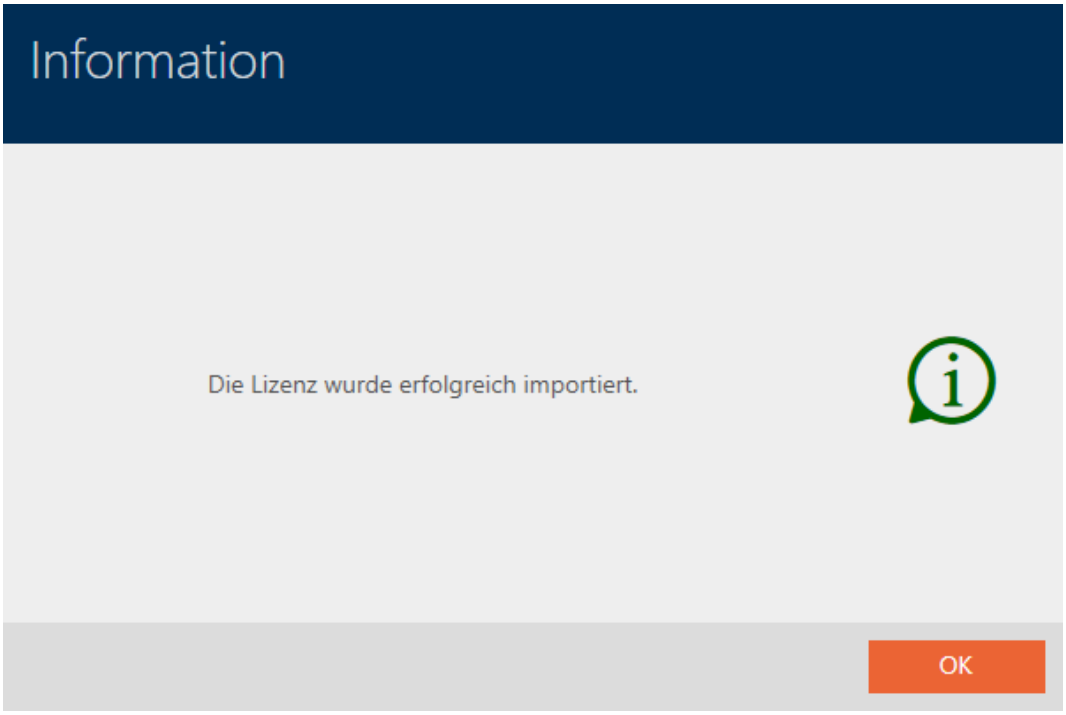
NOTE

No need to complete twice

You do not need to fill out the registration form again.

3. Click on the Importing the licence file button.
   ↳ The Explorer window will open.
4. Navigate to your licence file.
5. Select your licence file.
6. Click on the Open button.
   ↳ Explorer window closes.
   ↳ Licence file is imported.

↳ AXM Lite is registered.

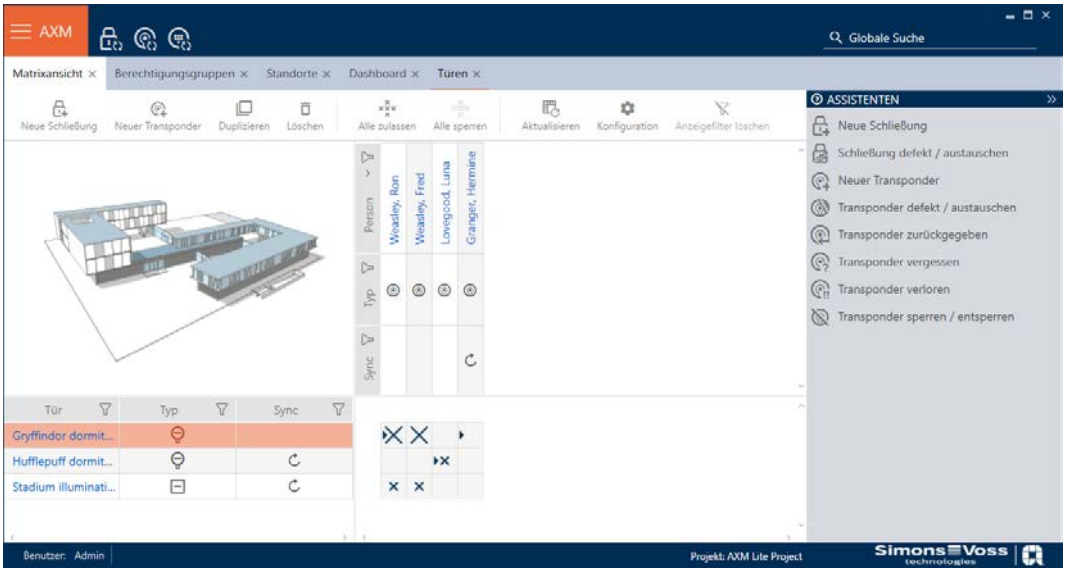


SimonsVoss ID for cloud services

You need to create and link a SimonsVoss ID to access the cloud functions available to you for AXM Plus and higher. A window will open immediately after registration for you to do this (see *Registration [▸ 31]*).

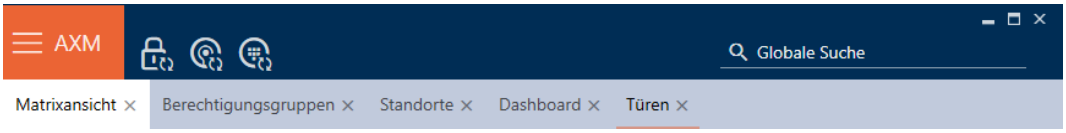
You also need to have issued a SEPA direct debit mandate for the service fee.

13. The AXM's structure



The AXM Lite interface consists primarily of four large sections:

AXM bar and tabs



Use the orange AXM button to expand the AXM bar:

This gives you access to all available tabs.

Below you will see the open tabs. Each task takes place within a tab. For example, there is a tab for [Access levels], a tab for [Locations] and so on.

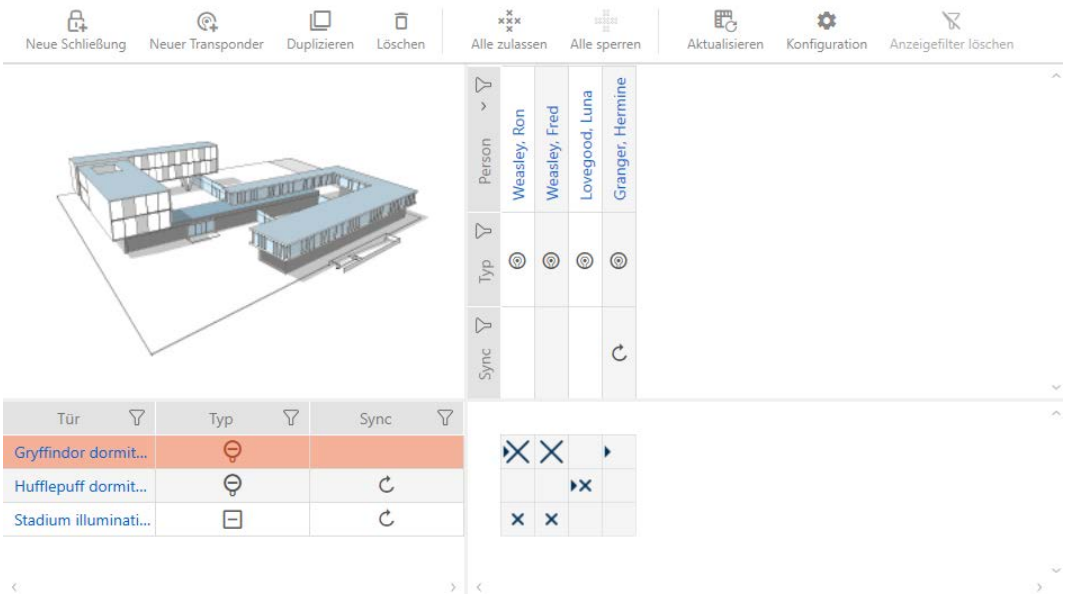
Basically, you can operate the tabs in the same way that you would use your browser (see *Tab operation [▸ 41]*).

There are three buttons next to the AXM button to skip directly to synchronisation of locking devices and identification media.

These can be used as an alternative to start synchronisation without entering the locking device or identification medium properties first.

On the right, you will find a global search function. This is where you can search the entire database for entries of all types (see *Global search [▸ 41]*).

Matrix section



The matrix section is the engine room behind your AXM Lite. This is where you can see all locking devices and identification media. You can use the filter function to hide entries, giving you an overview (see *Sorting and filtering [▸ 37]*).

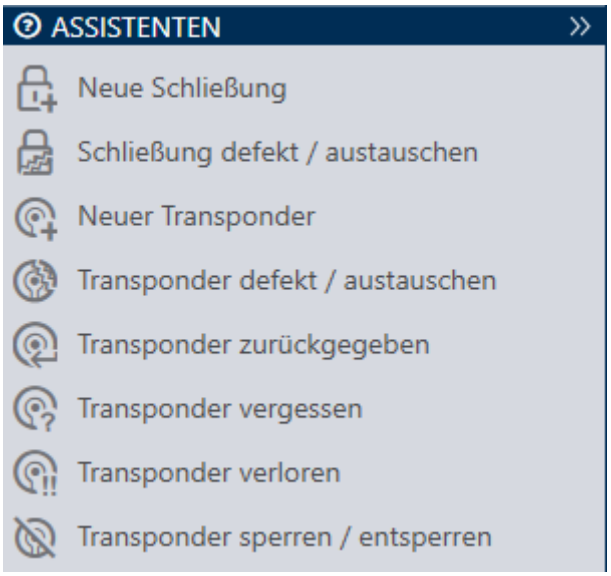
Each row normally represents a locking device and each column represents an identification medium. This identification medium's authorisation for this locking device is indicated where rows and columns meet (see *Permissions [▸ 256]*). There are basically two different main states:

- Authorisation set (cross)
- No authorisation set (no cross)

Various details can be displayed in the matrix. One is the synchronisation state. You need to synchronise if you see the synchronise icon ⟳/⟳ here (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*). Click on ⟳/⟳ to start synchronising the entry concerned immediately.

The matrix section also contains an action bar that you can use to edit the matrix:

Wizard menu



There is a wizard menu on the right side of your AXM Lite. This is where you will find wizards to assist you in situations that occur frequently (e.g. lost identification media).

If you need more space, you can use `>>` to hide the wizard menu and `<<` to show it.

User/project Bar

You can see the user and project names at the bottom of the screen.

Dashboard

One new feature in AXM Lite is the dashboard (see *View statistics and warnings (dashboard) [▸ 355]*). The dashboard provides you with statistics on your database and gives you warnings – when a task has not yet been completed, for example.

The dashboard can be accessed via the AXM bar.

Log

The log allows you to keep track of who changes what in the database and when they make the change (see *Tracking activities in the database (log) [▸ 356]*).

The log can also be accessed via the AXM bar.

13.1 Sorting and filtering

Large lists and tables can become confusing.

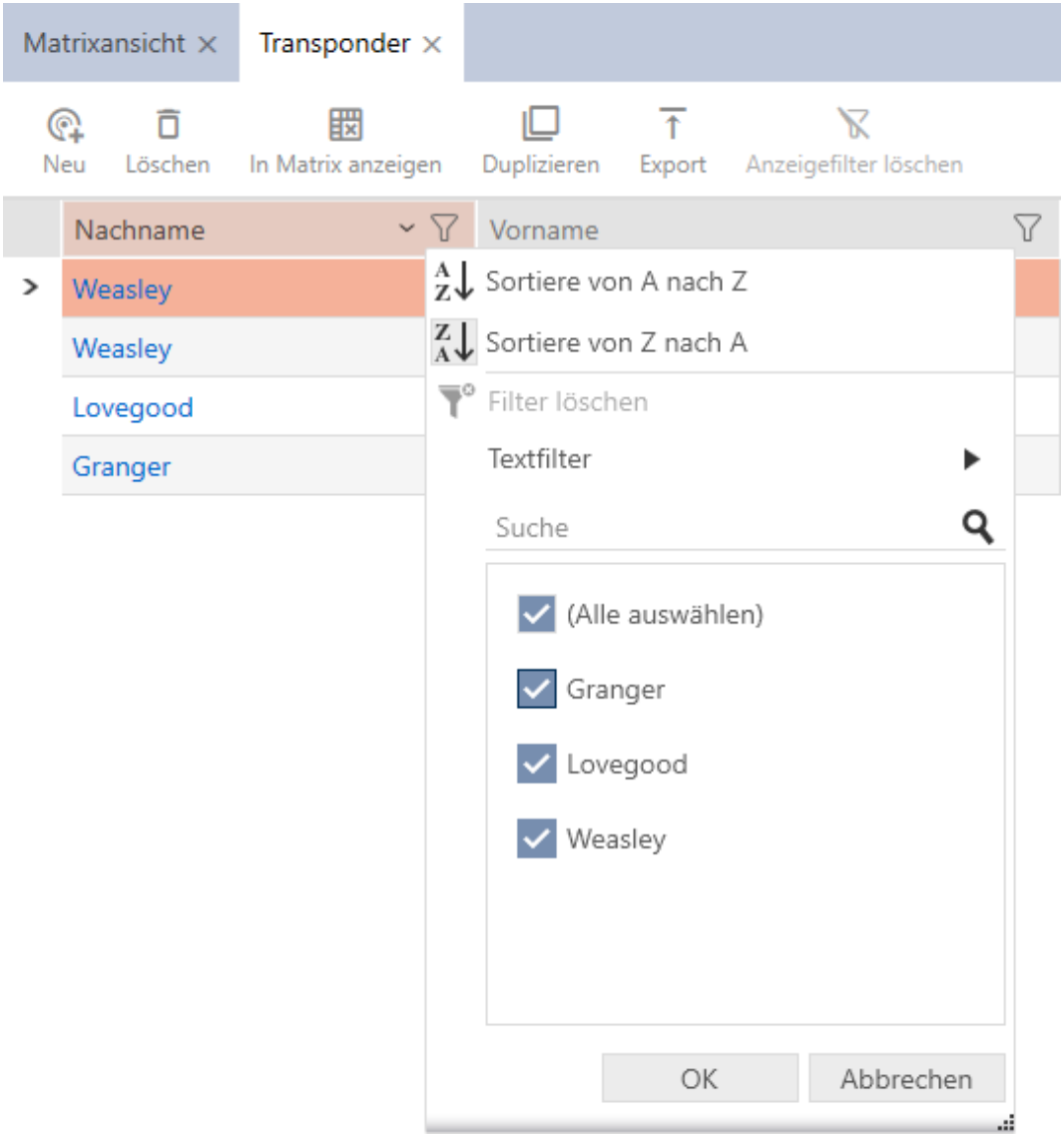
The AXM Lite provides you with sorting and filtering functions to simplify things.

Sorting

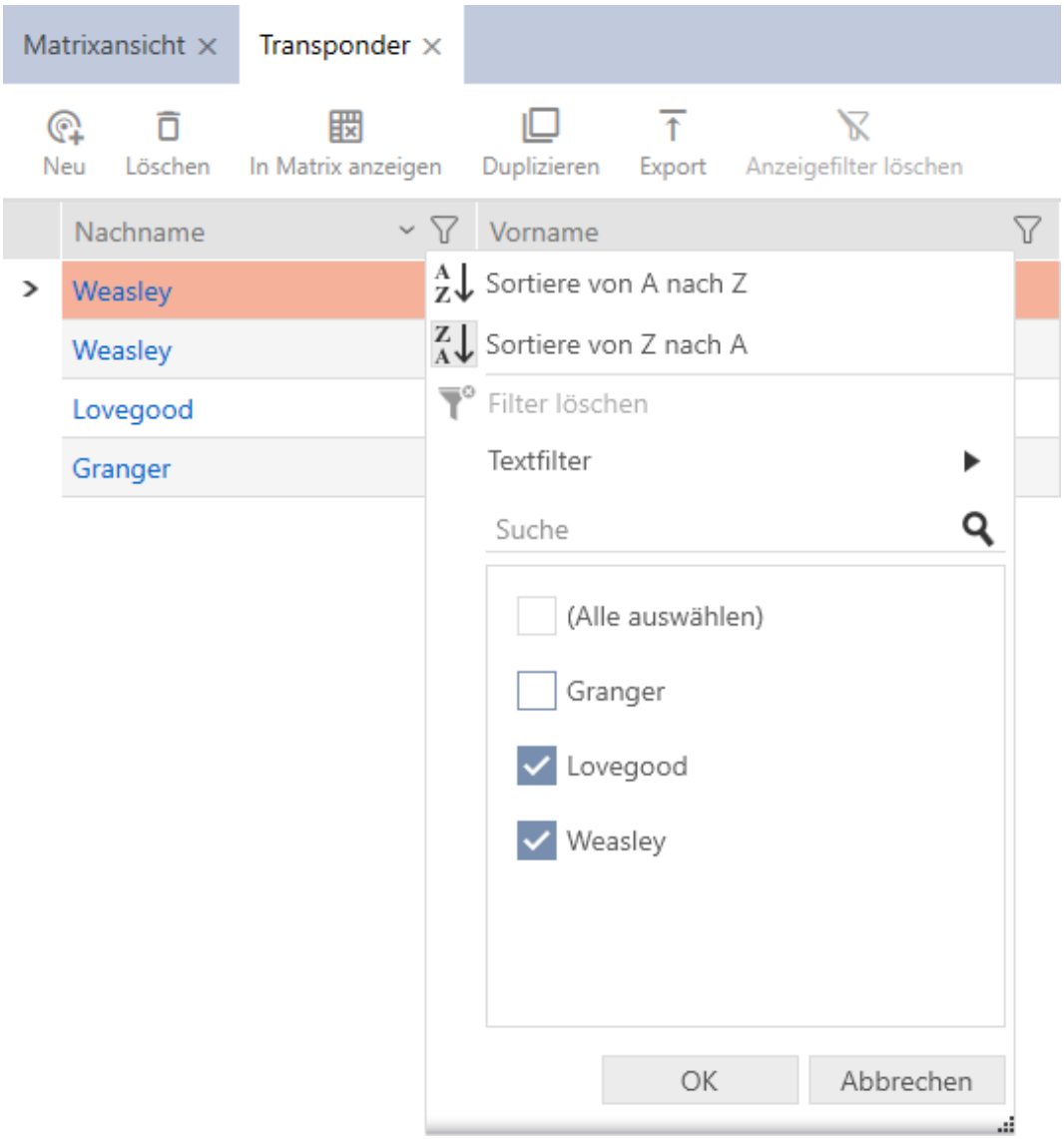
1. Click on one of the column or row headings.
   ↳ Entries will then be sorted by this column/row.
2. Click on the same heading again.
   ↳ The sort order is reversed.

Filtering

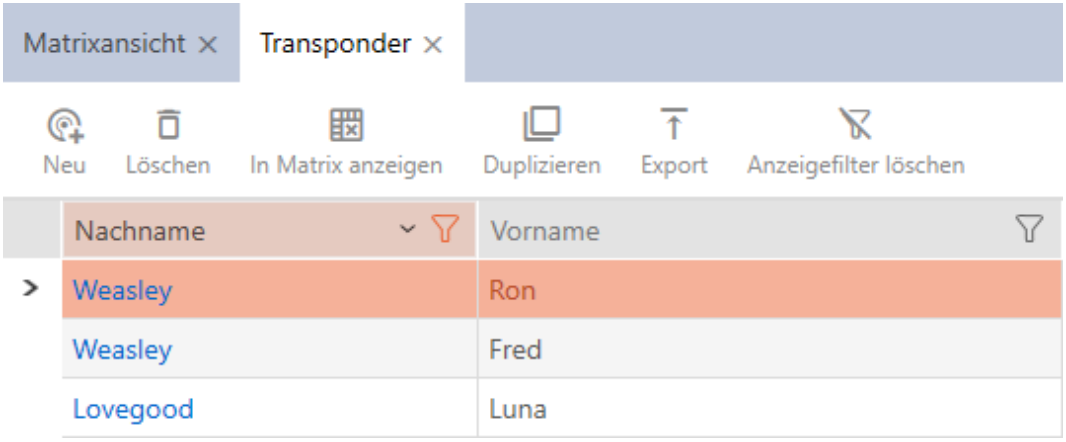
1. Click on the ▽ button in one of the displayed column or row headers.
   ↳ The filter menu will open.



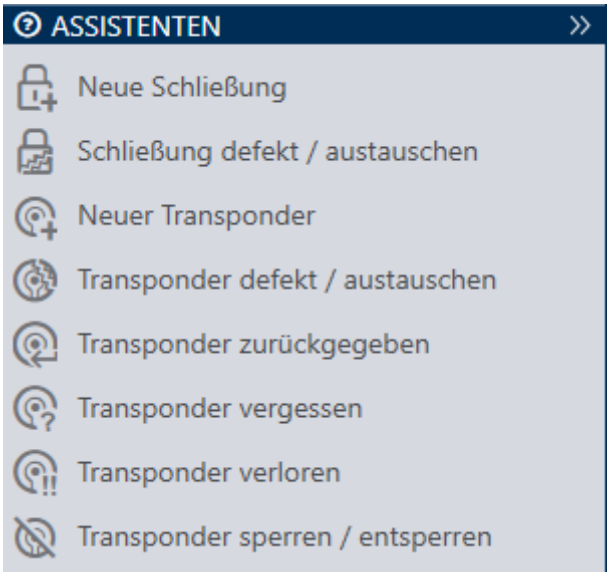
2. Adjust the filters.



3. Click on the OK button.
   ↳ The filter menu will close.
   ↳ Entries will now be filtered when displayed.



13.2 Installation wizards



The wizards in the wizard section will help you complete certain tasks quickly and reliably. Just click on the corresponding wizard. The wizard asks questions and provides background information. The wizard will guide you through the solution to your problem based on your answers.

If you need more space, you can use `>>` to hide the wizard menu and `<<` to show it.

13.3 Multiple options, same result

This manual usually only describes one way to do something specific. However, this does not mean the described approach is the only way to complete the task.

There are often several ways to achieve the same result.

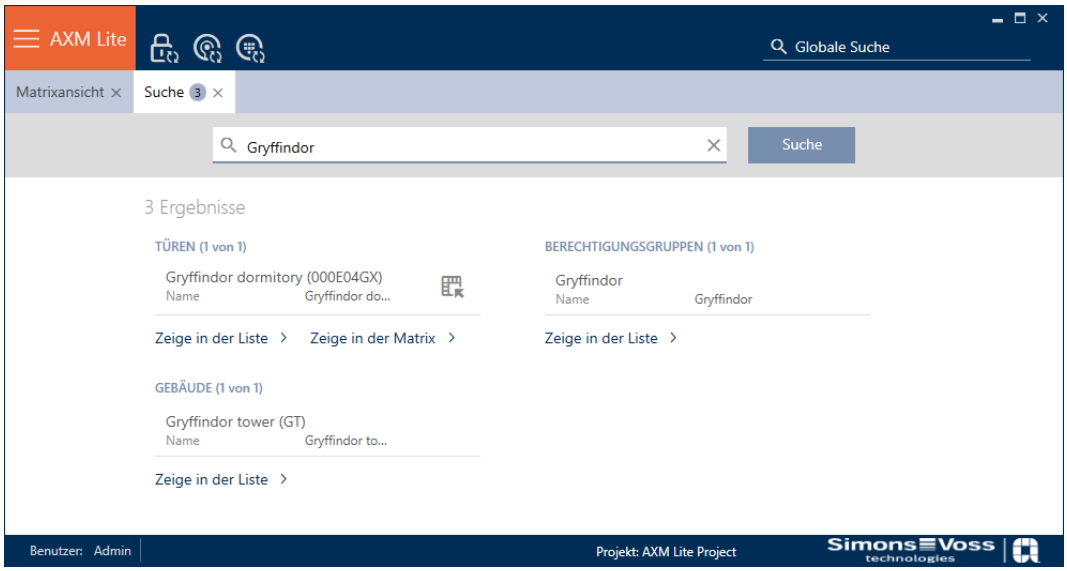
For example, you can delete an entry in the matrix in two ways:

1. Using the matrix bar: `Löschen`
2. Using the context menu: `Löschen`

Both ways delete the entry.

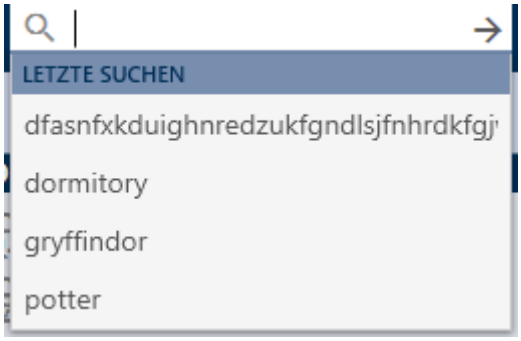
13.4 Global search

The global search in AXM Lite searches all entries and lists them in an overview:



Use the Zeige in der Matrix or [Zeige in der Liste] buttons to go directly to the required entry in the matrix or list view.

AXM Lite will help you in your search by automatically offering you the last items entered in the search field as a drop-down menu:



13.5 Working with AXM more effectively

13.5.1 Tab operation

AXM Lite allows you to handle multiple tasks at the same time with an innovative tab control function. Simply leave several tabs open at the same time.

Frequently used tabs can also be opened automatically when the program is launched (see *Pinning tabs [▸ 330]*).

Some tabs are opened in the foreground as windows and must first be closed again before you can do anything else. These include but are not limited to:

- [Project backup]
- [Change user password]
- [SETTINGS]
- [Programming devices]
- [About AX Manager]

You can recognise such tabs by the fact that the rest of AXM Lite is greyed out when opened.

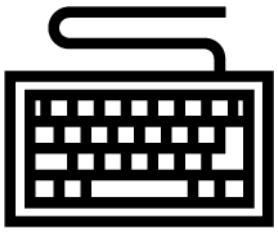
NOTE

Do not use Alt+F4 to close open windows

Windows open in the foreground block the remaining ones AXM Lite for further input. If you do not close such a window properly using the available buttons, but use Alt+F4 instead, then the window is closed, but the rest of AXM Lite remains greyed out. You will therefore lock yourself out of the AXM Lite.

- Do not use Alt+F4 to close windows in the foreground.

13.5.2 Hotkeys



Key shortcut	Response
Tab	Skips to next input field.
Shift + Tab	Skips to the previous input field.
Ctrl + tab	Skips to next tab.
Ctrl + Shift + tab	Skips to the previous tab.
Ctrl + Z	Undoes the last action (e.g. deletes text entered in an input field by mistake)

13.5.3 Creating additional objects

It is often the case that you will want to create multiple objects with the same or similar settings.

One example is a number of identification media which need to have the same time rules.

This is where AXM Lite helps you and offers the ☑ Create additional objects checkbox in many windows. If you activate this box, the current window with the same settings will remain open.

Example: you create a transponder and activate the checkbox. Now click on the Finish button. The required transponder is now created but the window remains open with the same settings. This means that you do not need to set up everything again for the next transponder. You simply need to enter a new name.

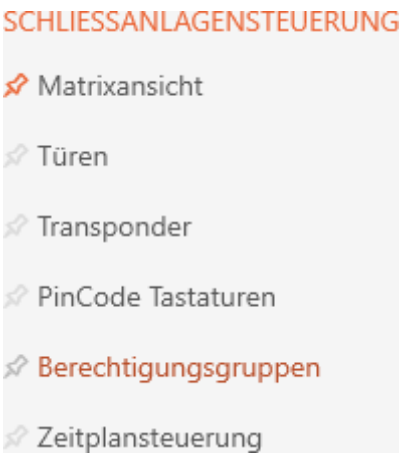
14. Organisational structure

14.1 Creating access levels

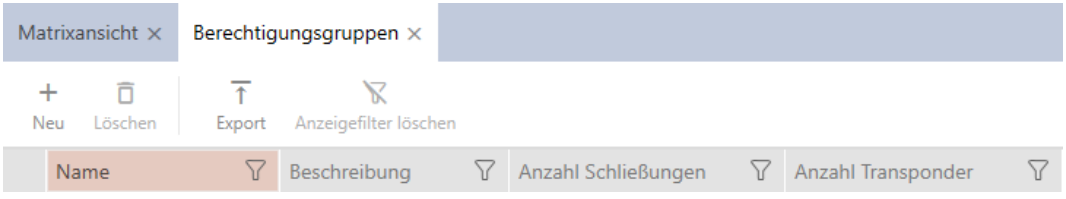
✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

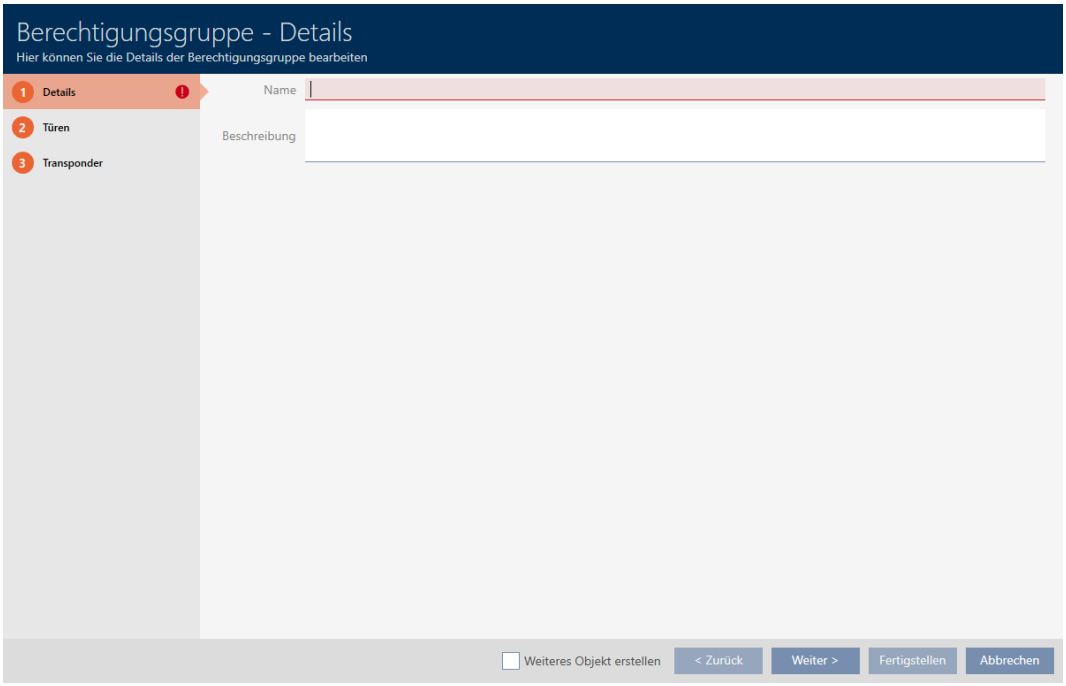
2. Select the Access levels entry in the | LOCKING SYSTEM CONTROL | group.



   ↳ The AXM bar will close.
   ↳ The [Access levels] tab will open.

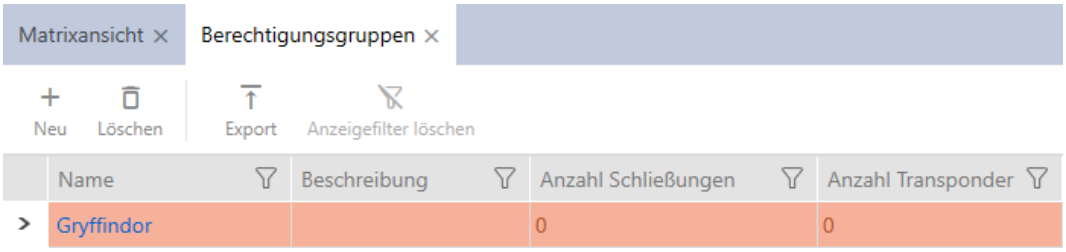


3. Click on the New + button.
   ↳ The window for a new access level will open.



4. Enter a name for your access level in the *Name* field.
5. Enter a description in the *Description* field.
6. Click on the Finish button.
   ↳ The window for the new access level will close.

↳ The new access level is listed.

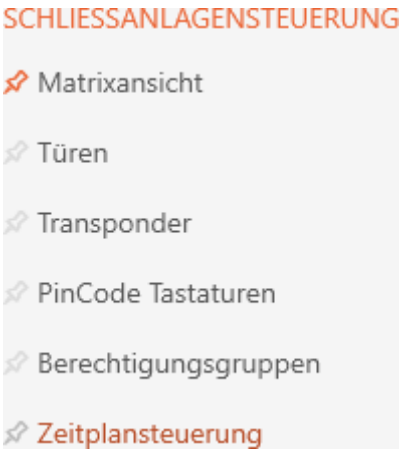


14.2 Creating a schedule

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

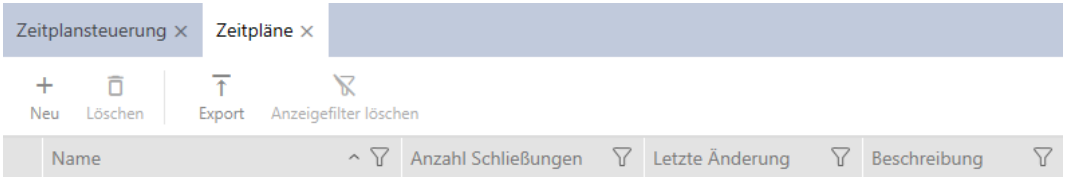
2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



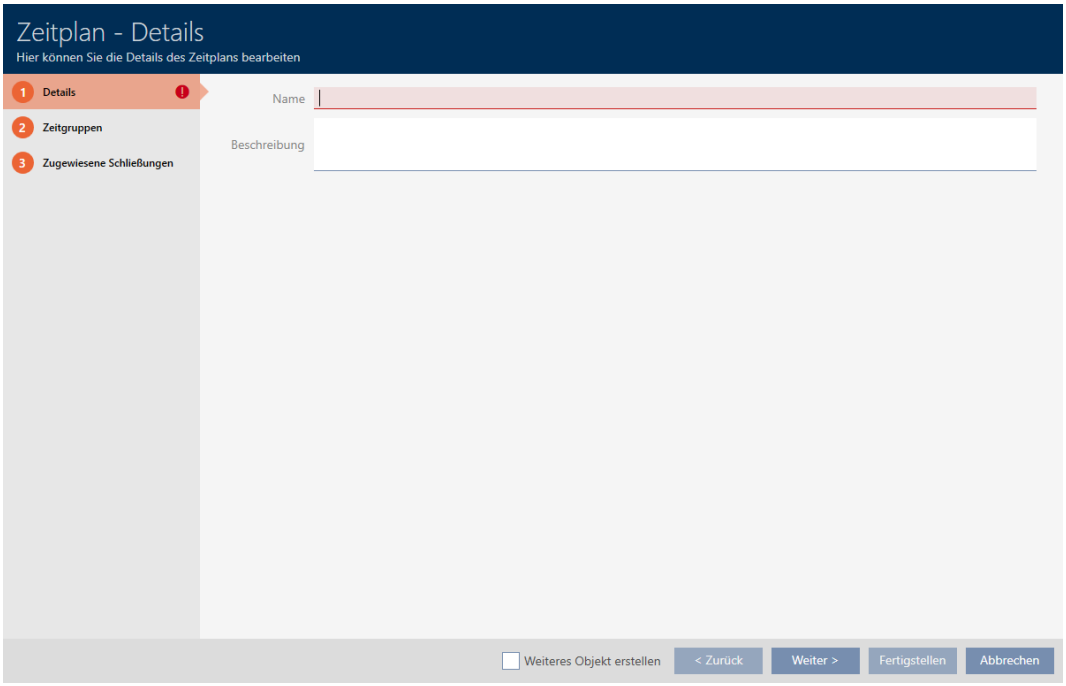
   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.

3. Click on the Time schedules button.

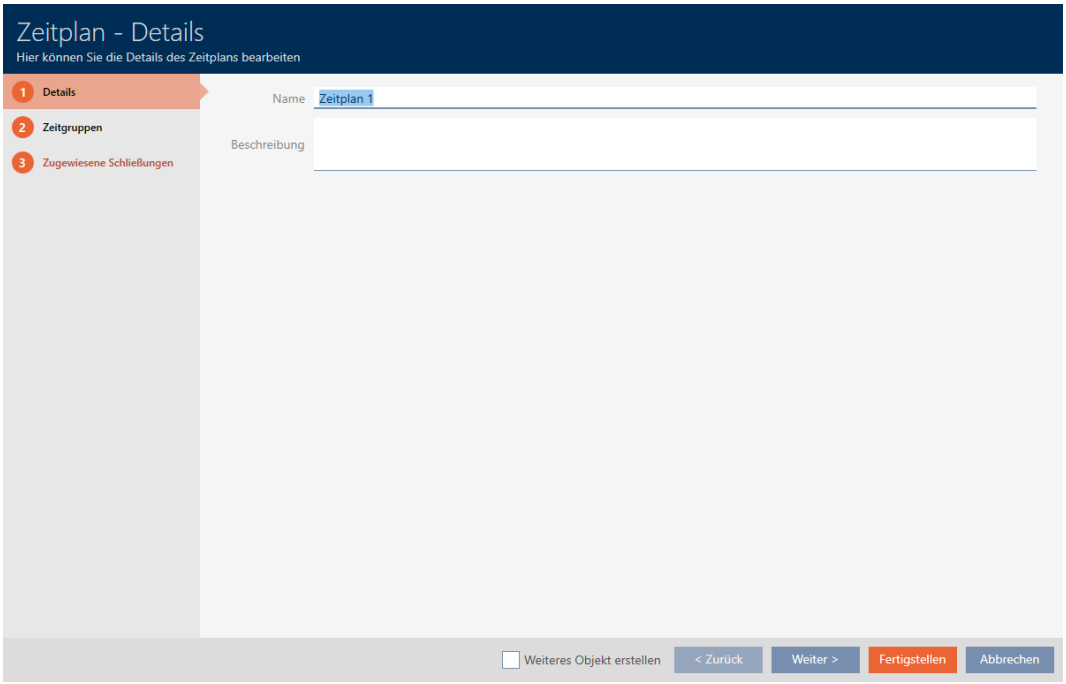
   ↳ The [Time schedules] tab will open.



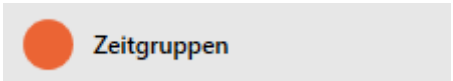
4. Click on the New button.
   ↳ The window for creating a schedule will open.



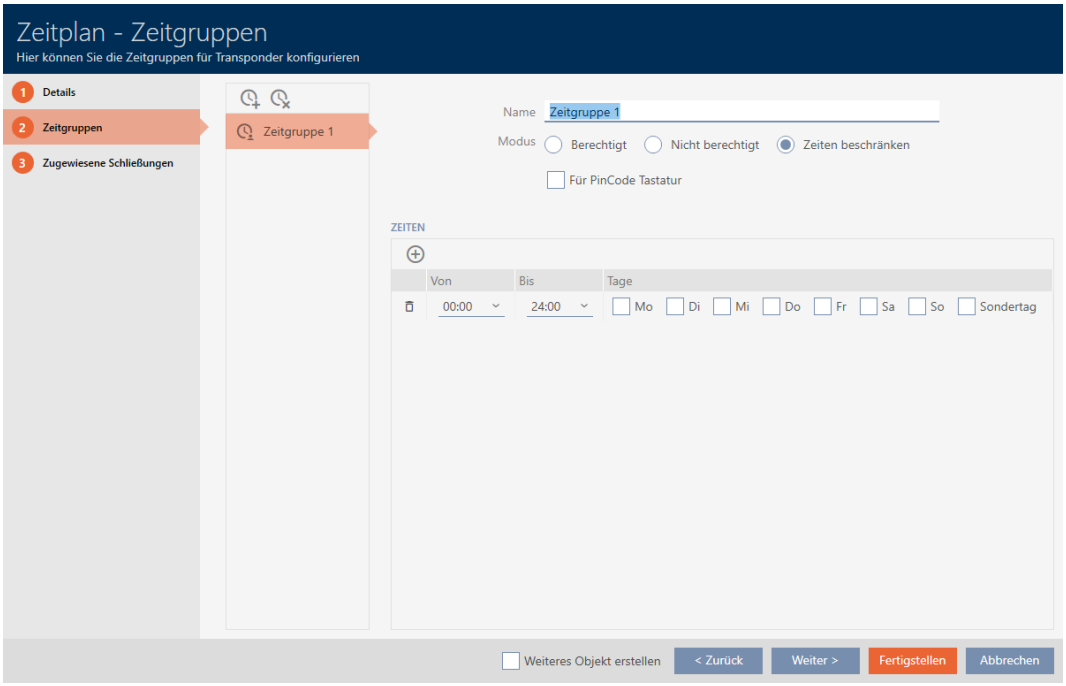
5. Enter a name for the schedule in the *Name* field.
6. Enter a description in the *Description* field.



7. Click on the Time groups tab.



↳ Window switches to the "Time groups" tab.



NOTE

First time group created automatically

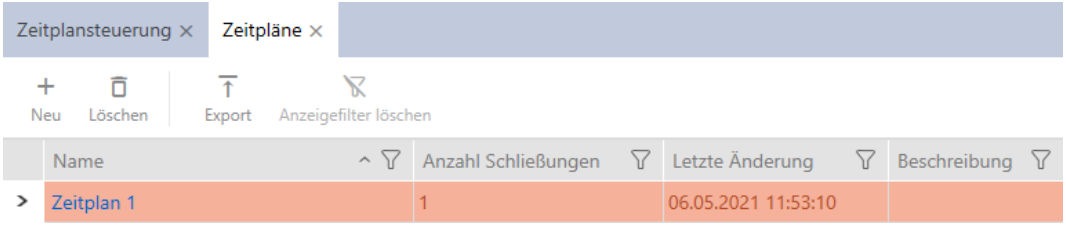
You need at least one time group for AXM Lite time management. AXM Lite therefore automatically creates a time group for you.

- Activate at least one day in this time group.

↳ The automatically created time group is valid and the schedule can be completed.

8. If you have not created your time groups yet: Create time groups (see *Create time group [▸ 49]*).
   If you have already created your time groups in another schedule: Set the time groups for this schedule.
   ↳ Schedule has been created and the Create Schedule window closes. Continue with *Adding identification medium to time group [▸ 275]* and *Adding locking devices to the schedule [▸ 272]* if required.

↳ Schedule has been created and is listed.

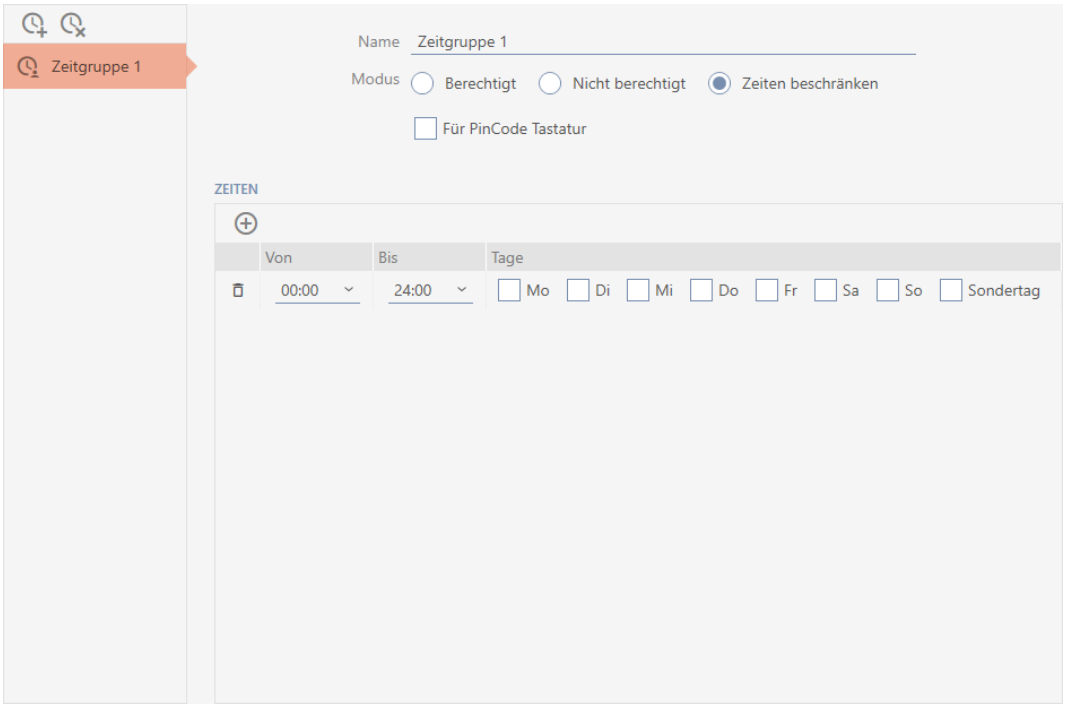


14.3 Create time group

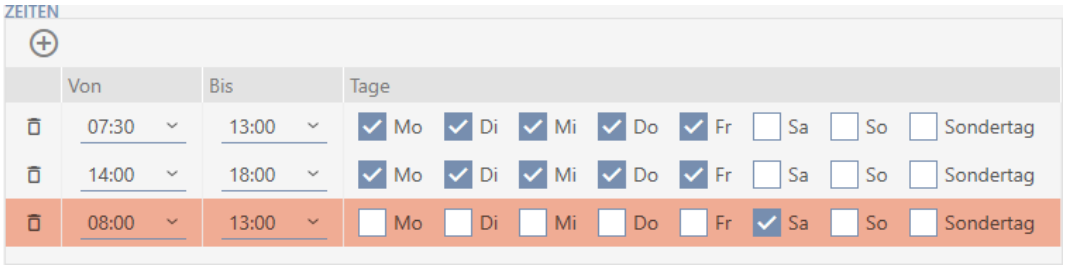
As a general rule, the following applies: All settings in a time group apply to each schedule.

You can choose from one of the three modes for each schedule within a time group:

◉ Authorised	All identification media in this time group are authorised for all locking devices in this schedule as specified in the matrix or access levels. ◉ Authorised corresponds to a time limit that permits use between 0-24 hours every day (i.e. it is effectively not a limit at all); see screenshot: If you try to save this time limit in this way, the AXM Lite automatically changes the mode to ◉ Berechtigt.
◉ Not authorised	No identification media in this time group are authorised for any of the locking devices in this schedule, even if they were authorised in the matrix. ◉ Not authorised corresponds to a time limit that does not allow use on any day (i.e. effectively restricted at all times); see screenshot:
◉ Limit times	All identification media in this time group are authorised for all locking devices in this schedule as specified in the matrix or authorisation groups if one of the configured time intervals applies.



The sophisticated concept of time intervals and days also allows you to combine intervals and days, for example:



- Different time intervals for the same days (e.g. a store has its lunch break between 13:00 and 14:00)
- Different time intervals for different days (e.g. a store is only open in the morning on Saturdays)

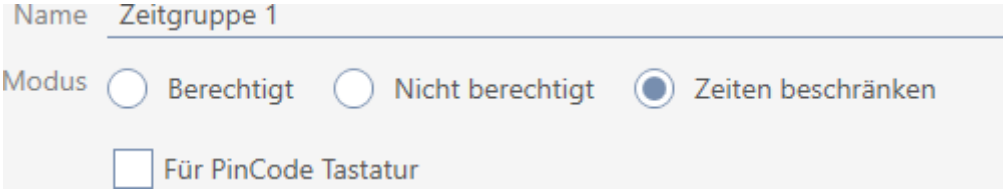
More information; see *Time groups and schedules [▸ 366]*.

The ☑ Special day checkbox is used for public holidays. You can specify public holidays and treat them either as a weekday or a special day. If the current date is a public holiday and this public holiday is to be treated as a special day, then the time group's special day rule applies (see *Creating and editing public holidays [▸ 61]*).

You can create and configure time groups using the schedule window:

✓ AXM Lite open.
✓ Schedule created (see *Creating a schedule [▸ 45]*).
✓ Schedule window open (see *Creating a schedule [▸ 45]*).

1. Click the button (except if you are reconfiguring the automatically created time group).
   ↳ New time group is now created.
2. Enter a name for the time group in the *Name* field.
3. Select Limit times mode.



4. If you wish to use this time group for PIN code keypad 3068 (with G1 protocol): Activate the For PinCode G1 checkbox.

NOTE

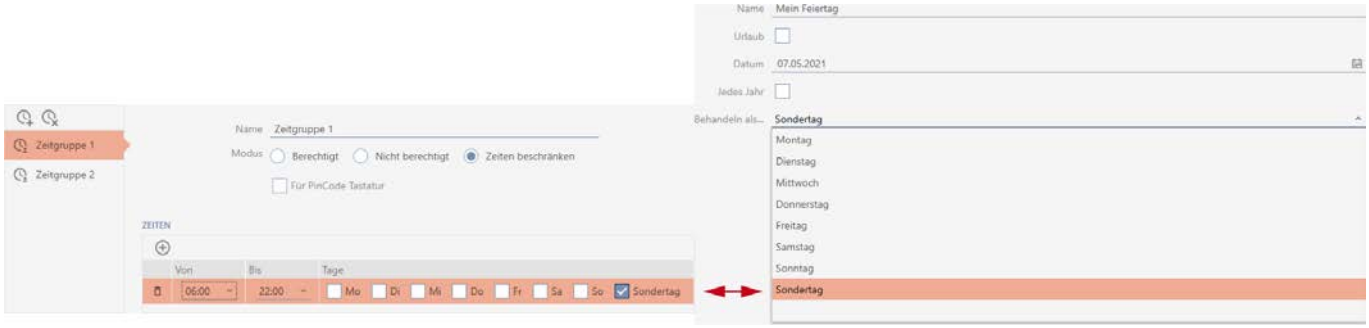
Time groups for PIN code keypads

PIN code keypads use the G1 protocol. This is why PIN code keypads require their own time groups. These time groups can also only be used for PIN code keypads.

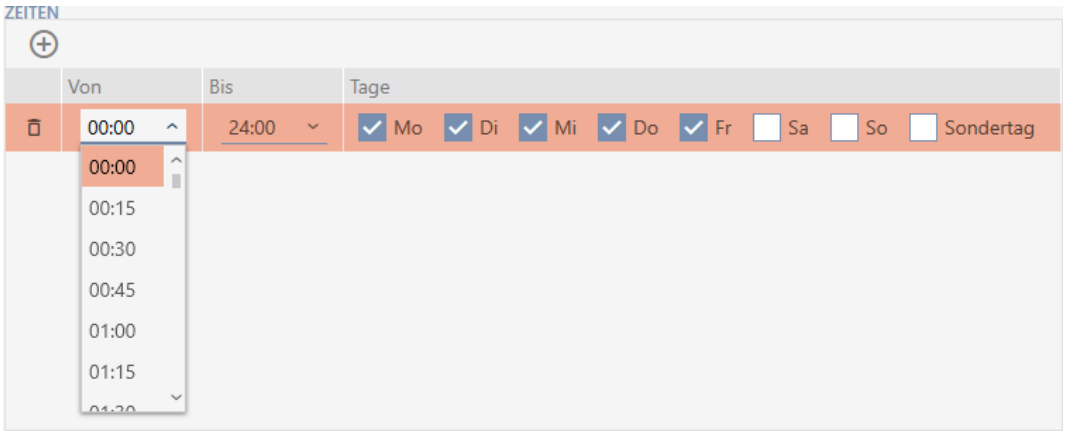
If you have not activated the PIN code keypad in your locking system at all (see Enabling PIN code keypads), then the For PinCode G1 checkbox does not exist.

Time groups that have already been created cannot be subsequently used for PIN code keypads.

5. Activate the days for the first time interval (checkboxes Mon Tue, Wed, Thu, , Fri, Sat, Sun and Special day).

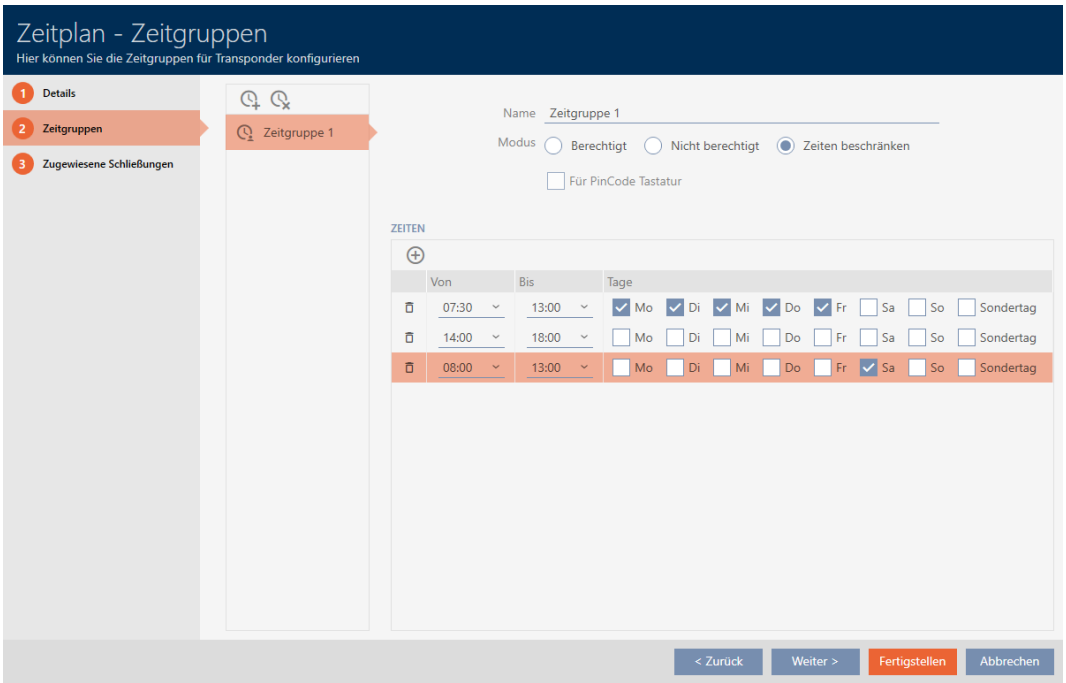


6. Set the time for the selected days.



↳ First time interval defined.

7. Click on the ⊕ button to display further time intervals if required.



8. Click on the Finish button or create additional time groups with the button if required.

↳ Time group is created and configured for the currently selected schedule.

NOTE

Configure new time groups for other schedules

Time groups are global. A newly created time group therefore also exists in all other schedules. For security reasons, all time groups in a new schedule are assigned Not authorised mode by default.

1. After creating a time group, switch to the other schedules and configure the time group in them as well.
2. Obviously, you can also create several time groups and not configure them in the other time groups until after.

14.4 Deleting a time group

NOTE

Deleting time groups from all schedules

Time groups are universally available for all locking systems within a project. A deleted time group is deleted from the entire project, not just for a schedule.

All identification media that were previously assigned to the deleted time group are then no longer assigned to a time group and must be added to one on an individual basis where necessary (see *Adding identification medium to time group [▸ 275]*).

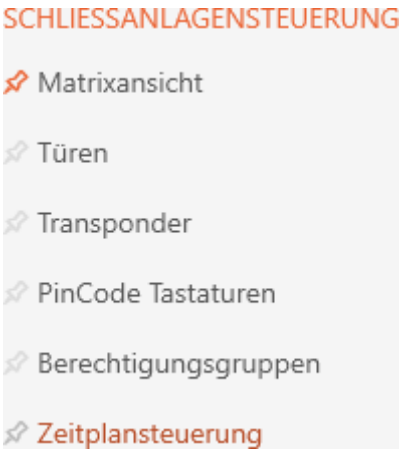
- If you do not wish to use a time group for just one schedule, set the time group to Authorised mode.

↳ Identification media in this time group can open the locking devices for which they are authorised at any time.

✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

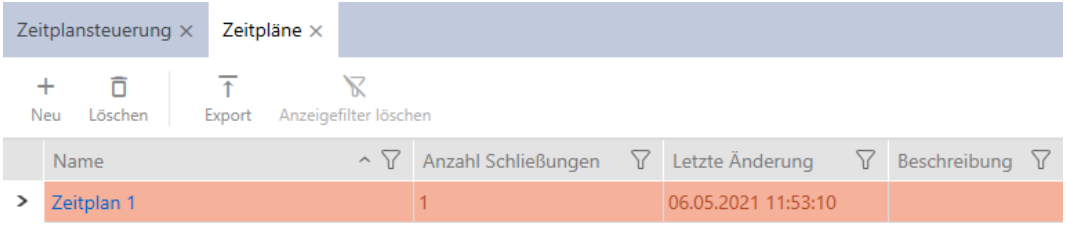
2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



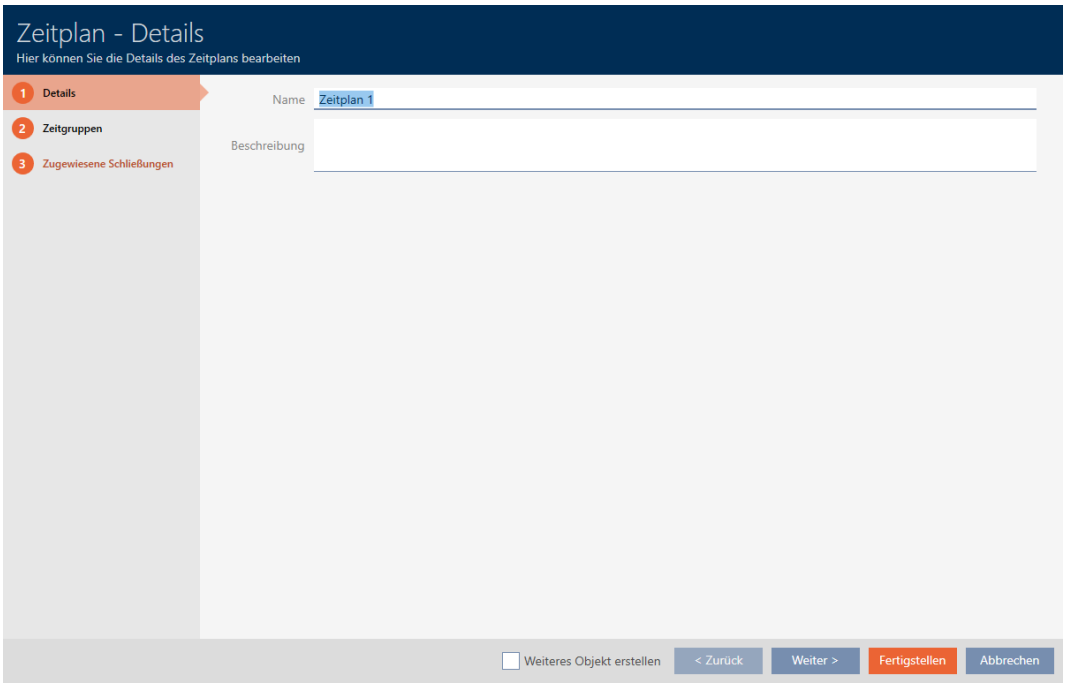
   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.

3. Click on the Time schedules button.

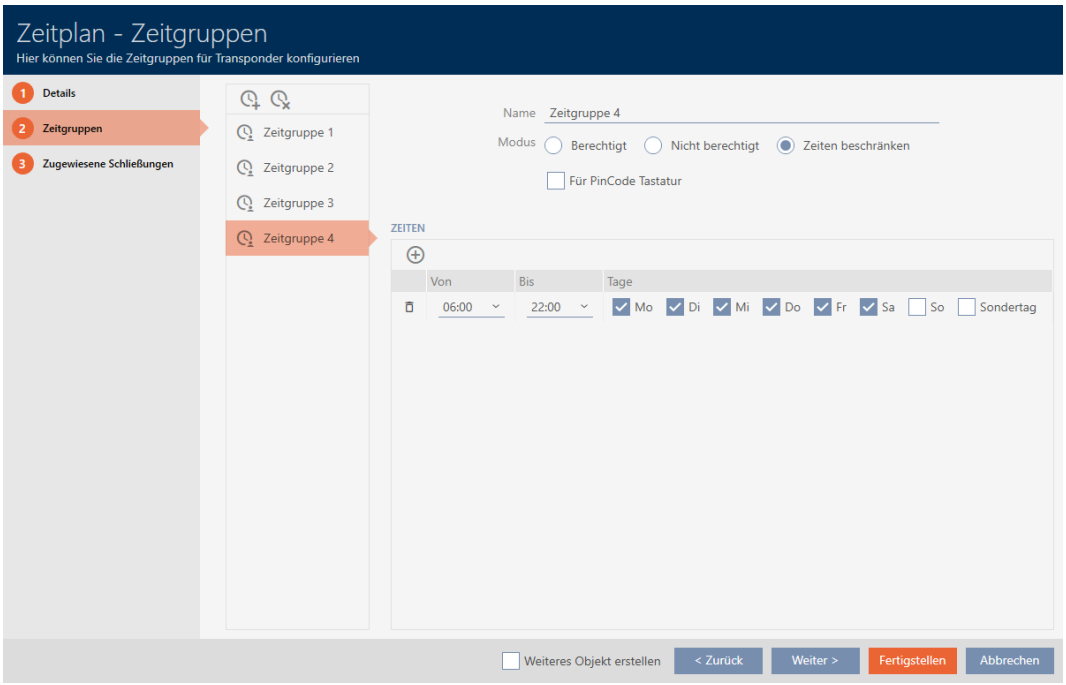
   ↳ The [Time schedules] tab will open.



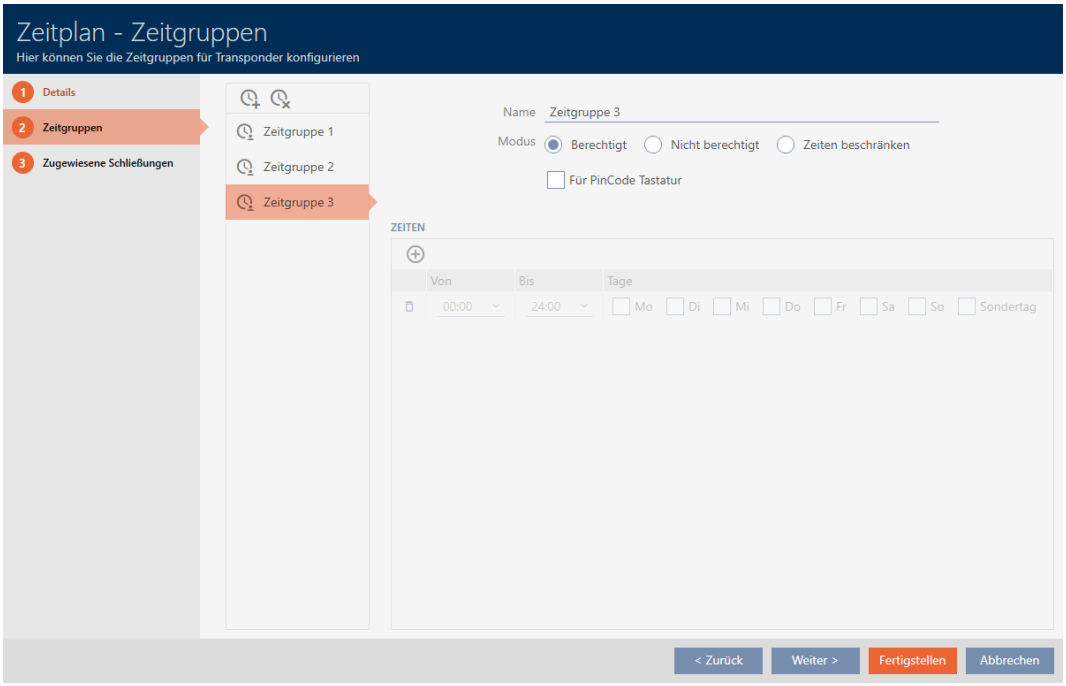
4. Click on any schedule to open its window.
   ↳ The schedule window will open.



5. Click on the Time groups tab.
   ↳ Window switches to the "Time groups" tab.



6. Select the time group you wish to delete.
7. Click on the button.
   ↳ Time group is now deleted.
8. Click on the Finish button.

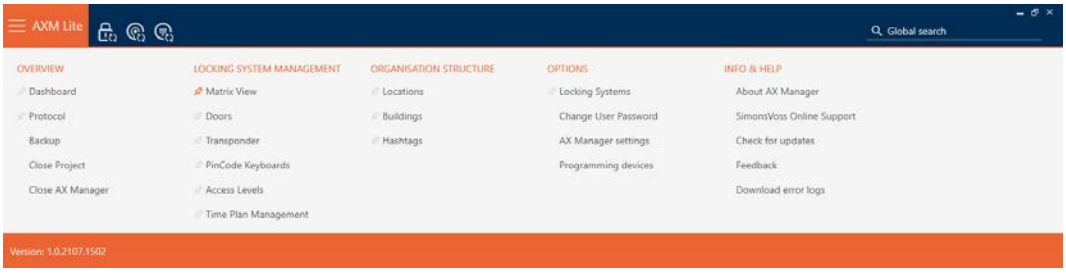


14.5 Deleting schedules

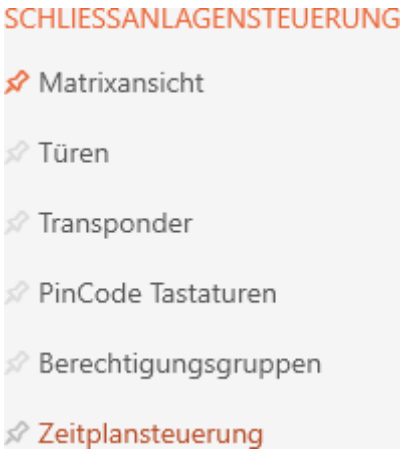
✓ AXM Lite open.

✓ Schedules are no longer assigned to a locking device (see *Adding locking devices to the schedule [▸ 272]* for instructions on how to edit assigned locking devices).

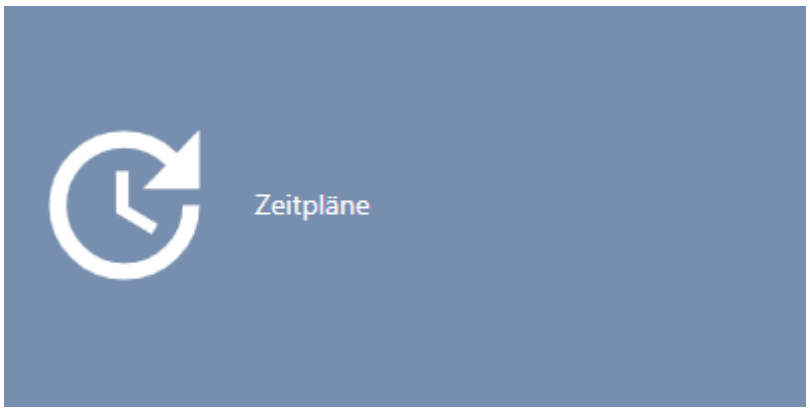
1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.



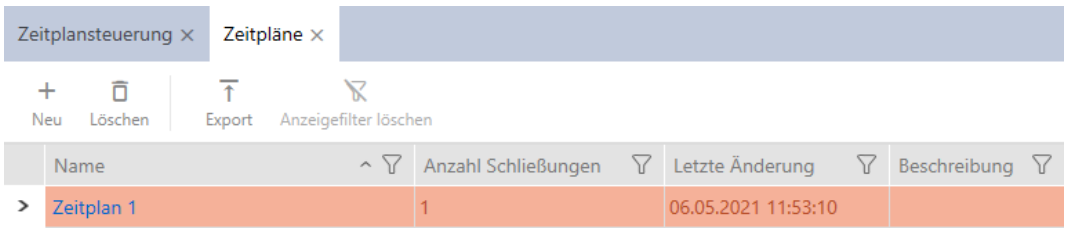
2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.
3. Click on the Time schedules button.

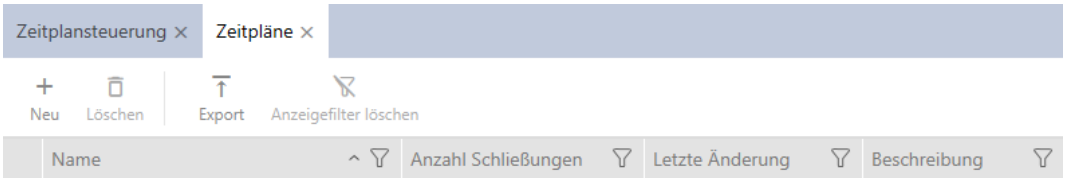


   ↳ The [Time schedules] tab will open.



4. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
5. Select the schedules you wish to delete (Ctrl+click for individual schedules, Shift+click for multiple schedules).
6. Click on the Delete button.

↳ Schedules are now deleted.

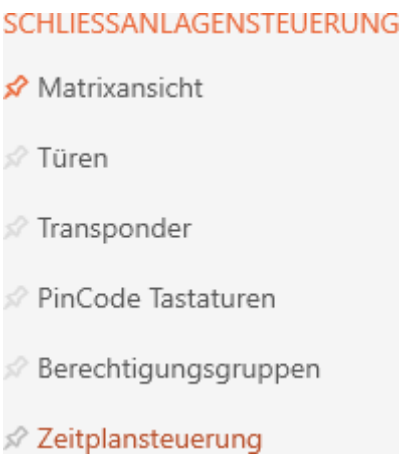


14.6 Creating a time switchover

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

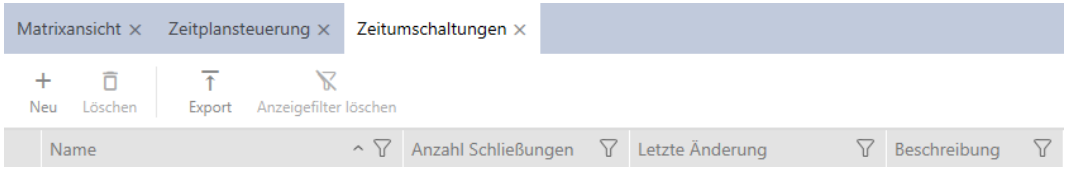
2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



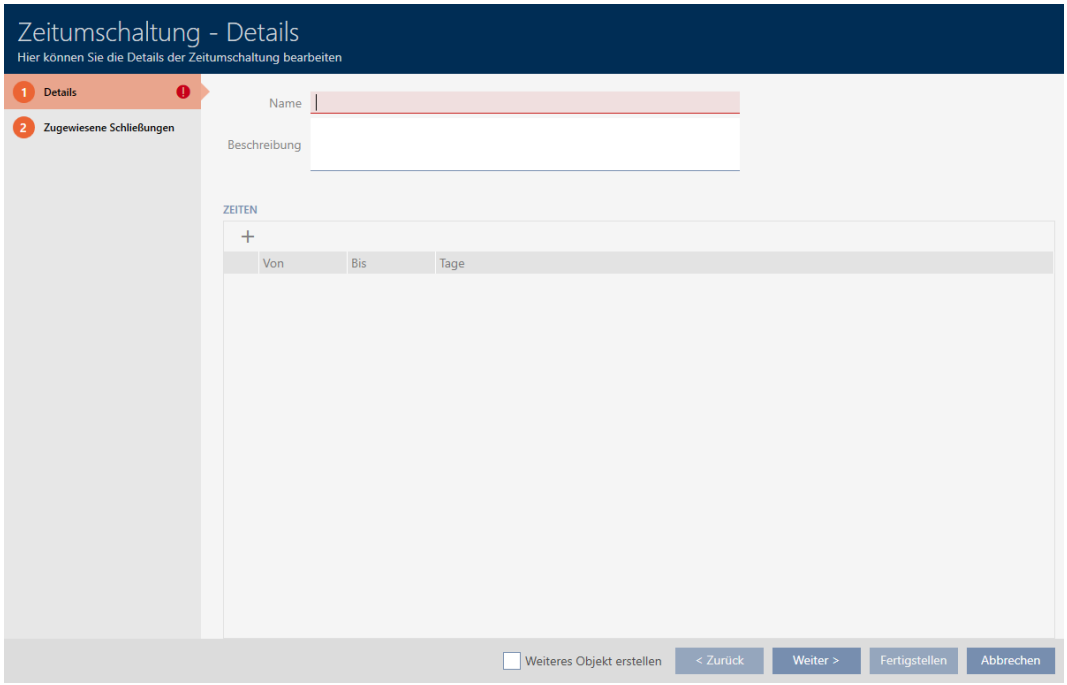
   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.

3. Click on the Time switching button.

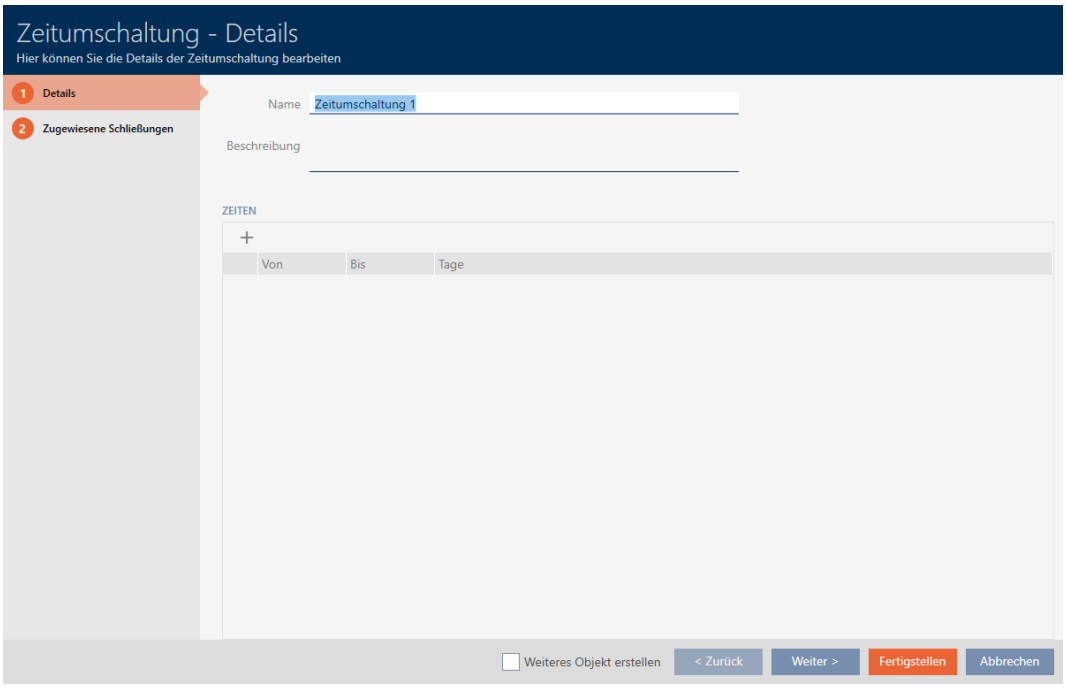
↳ The [Time switching] tab will open.



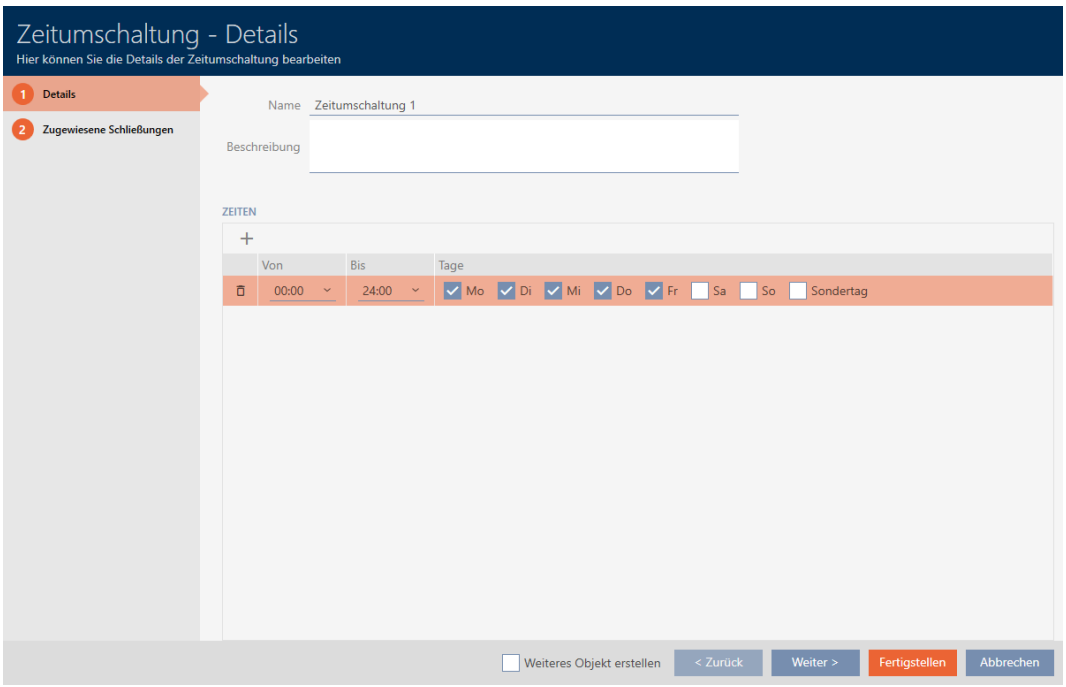
4. Click on the New button.
↳ The window for creating a time switchover will open.



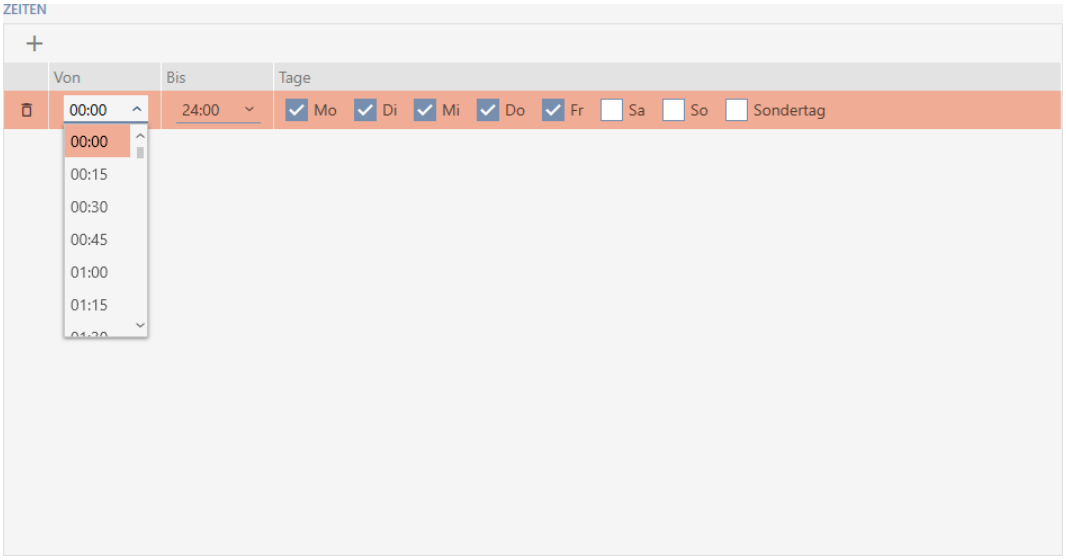
5. Enter a name for your time switchover in the *Name* field.



6. Enter a description in the *Description* field if required.
7. Click on the + icon to create a new interval for your time switchover.
8. Activate the checkboxes for the weekdays on which the locking device should engage (☑ Mon, ☑ Tue, ☑ Wed, ☑ Thu, , ☑ Fri, ☑ Sat, ☑ Sun & ☑ Special day).

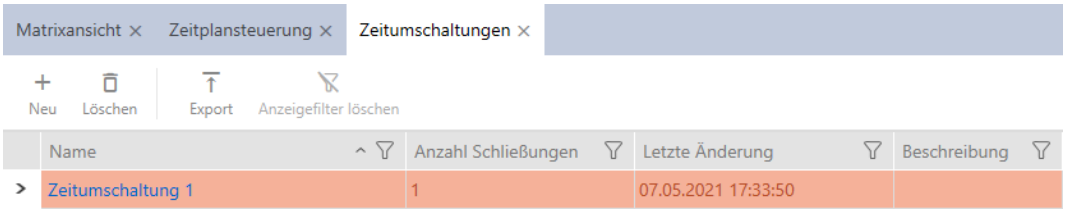


9. Set the time interval for these days in the ▼ **Until** and ▼ **From** drop-down menus.



10. Set other time intervals if required.
11. Click on the Finish button.
    ↳ Window for creating a time switchover closes.

↳ Time changeover is created and listed. Continue with *Engaging and disengaging locking devices automatically with time switchover [▸ 222]* if required.

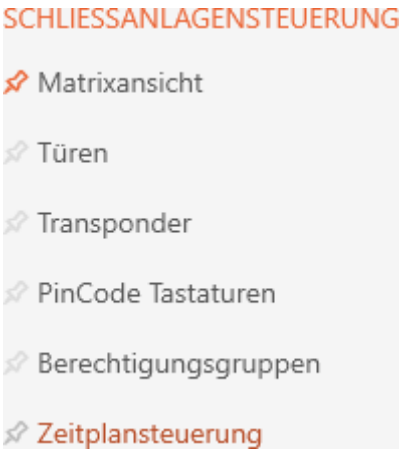


14.7 Creating and editing public holidays

✓ AXM Lite open.

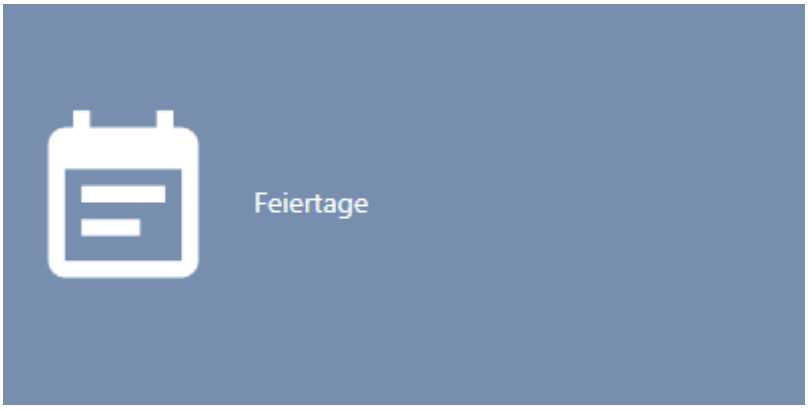
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.

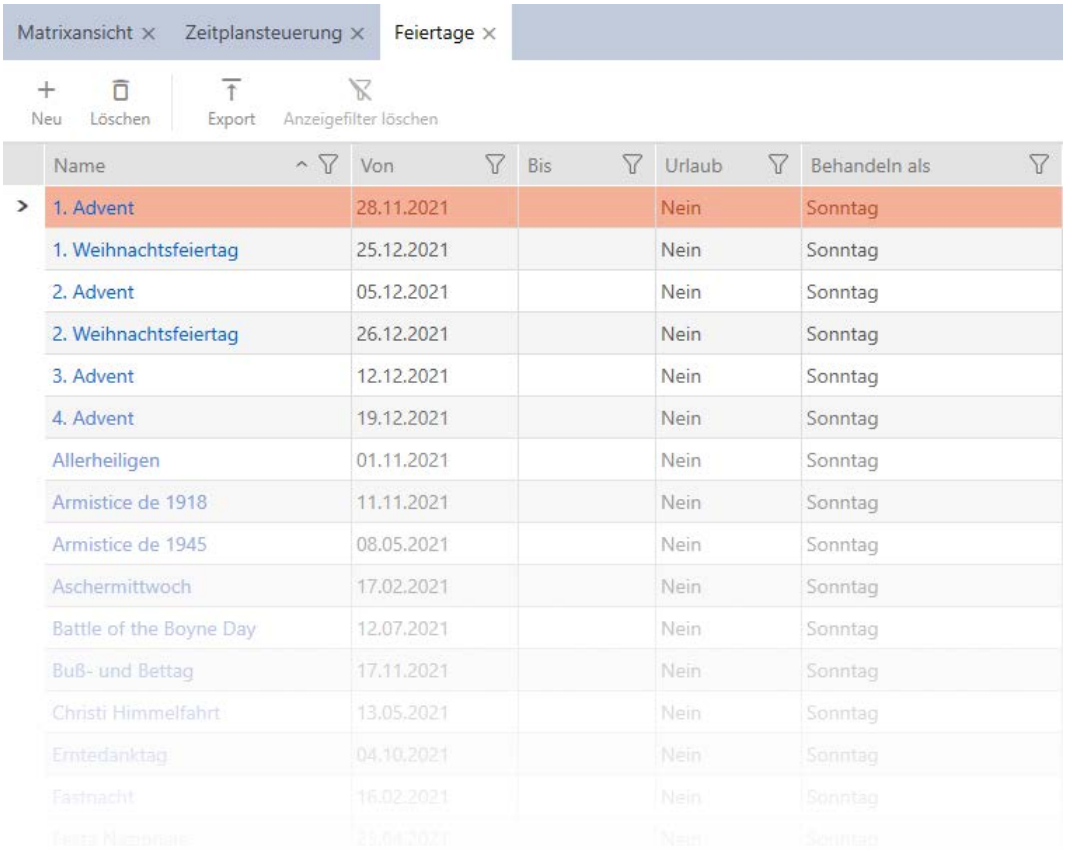


   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.

3. Click on the Public holidays button.

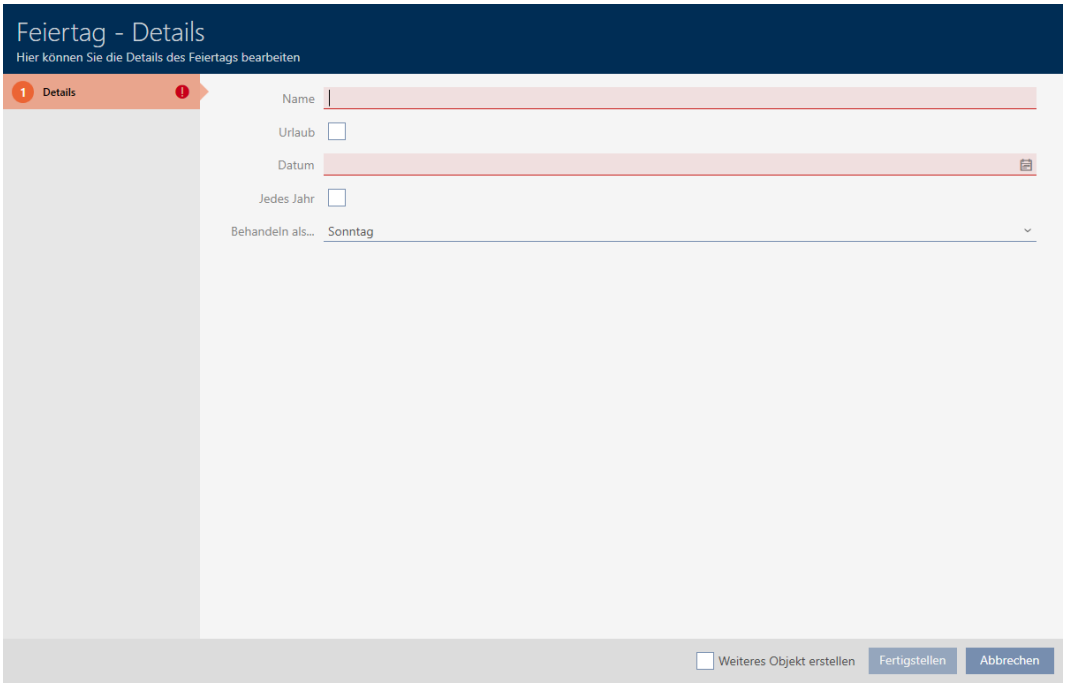


   ↳ The [Public holidays] tab will open.



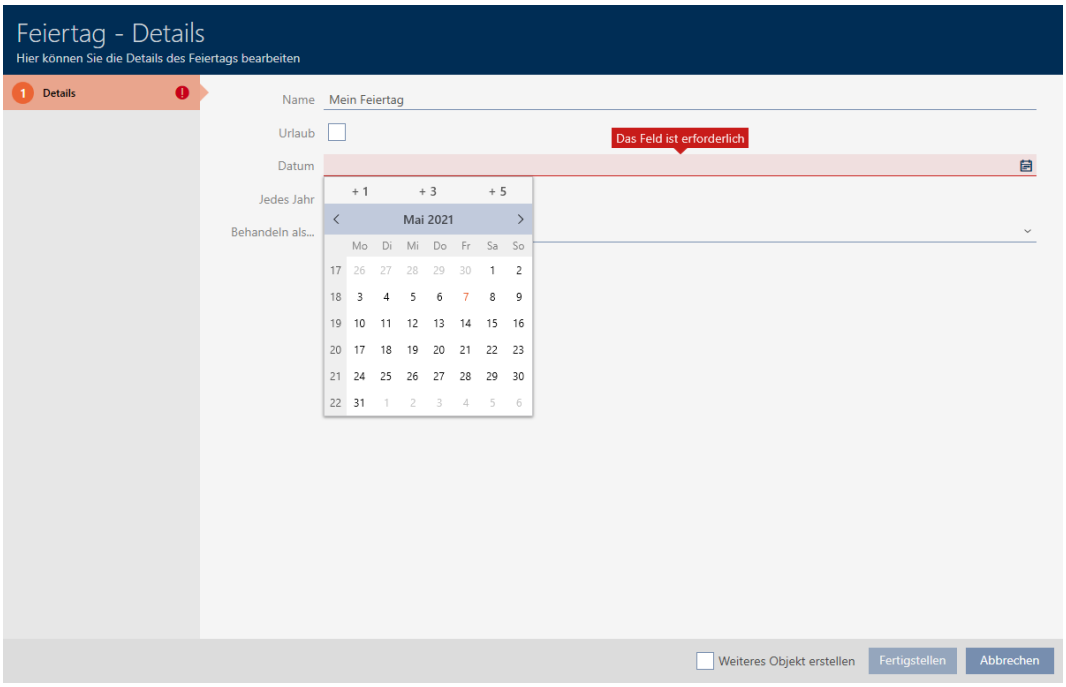
Name	Von	Bis	Urlaub	Behandeln als
1. Advent	28.11.2021		Nein	Sonntag
1. Weihnachtsfeiertag	25.12.2021		Nein	Sonntag
2. Advent	05.12.2021		Nein	Sonntag
2. Weihnachtsfeiertag	26.12.2021		Nein	Sonntag
3. Advent	12.12.2021		Nein	Sonntag
4. Advent	19.12.2021		Nein	Sonntag
Allerheiligen	01.11.2021		Nein	Sonntag
Armistice de 1918	11.11.2021		Nein	Sonntag
Armistice de 1945	08.05.2021		Nein	Sonntag
Aschermittwoch	17.02.2021		Nein	Sonntag
Battle of the Boyne Day	12.07.2021		Nein	Sonntag
Buß- und Bettag	17.11.2021		Nein	Sonntag
Christi Himmelfahrt	13.05.2021		Nein	Sonntag
Erntedanktag	04.10.2021		Nein	Sonntag
Fastnacht	16.02.2021		Nein	Sonntag
Feiertag Name	21.04.2021		Nein	Sonntag

4. Click on the New ✚ button.
   ↳ The window for creating a public holiday will open.

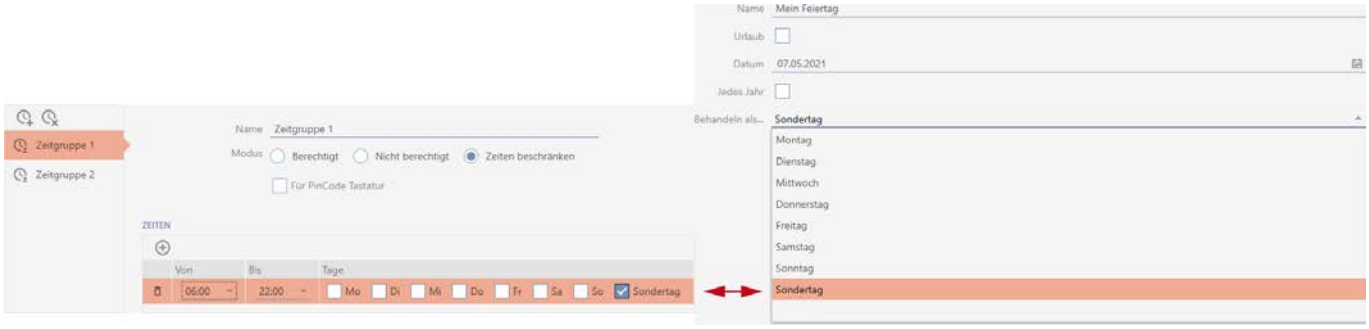


5. Enter a name for your public holiday in the *Name* field.
6. If your public holiday is a holiday: Activate the ☑ Vacation checkbox.

7. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



8. Select which of the available days should be used in the schedule for your holiday from the ▼ **Handle as...** drop-down menu ("Monday", "Tuesday", "Wednesday", "Thursday", "Friday", "Saturday", "Sunday" & "Special day").



9. Click on the Finish button.
   ↳ The window for creating a public holiday will close.

↳ The public holiday has been created and is listed.

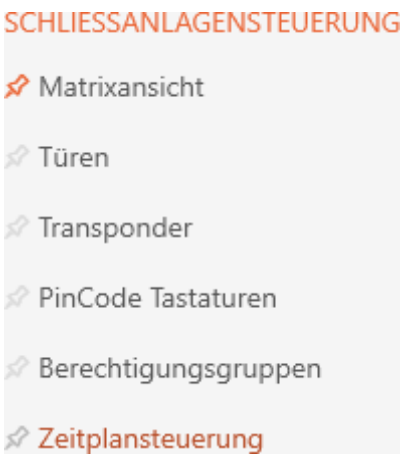
	Heiliger Abend	24.12.2021	Nein	Sonntag
	Karfreitag	02.04.2021	Nein	Sonntag
	Maifeiertag	01.05.2021	Nein	Sonntag
	Maria Empfängnis	08.12.2021	Nein	Sonntag
	Maria Himmelfahrt	15.08.2021	Nein	Sonntag
>	Mein Feiertag	07.05.2021	Nein	Sonntag
	Neujahr	01.01.2021	Nein	Sonntag
	Ostermontag	05.04.2021	Nein	Sonntag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

14.8 Creating and editing public holiday lists

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



   ↳ The AXM bar will close.

↳ The [Time schedule control] tab will open.

3. Click on the Public holiday lists button.

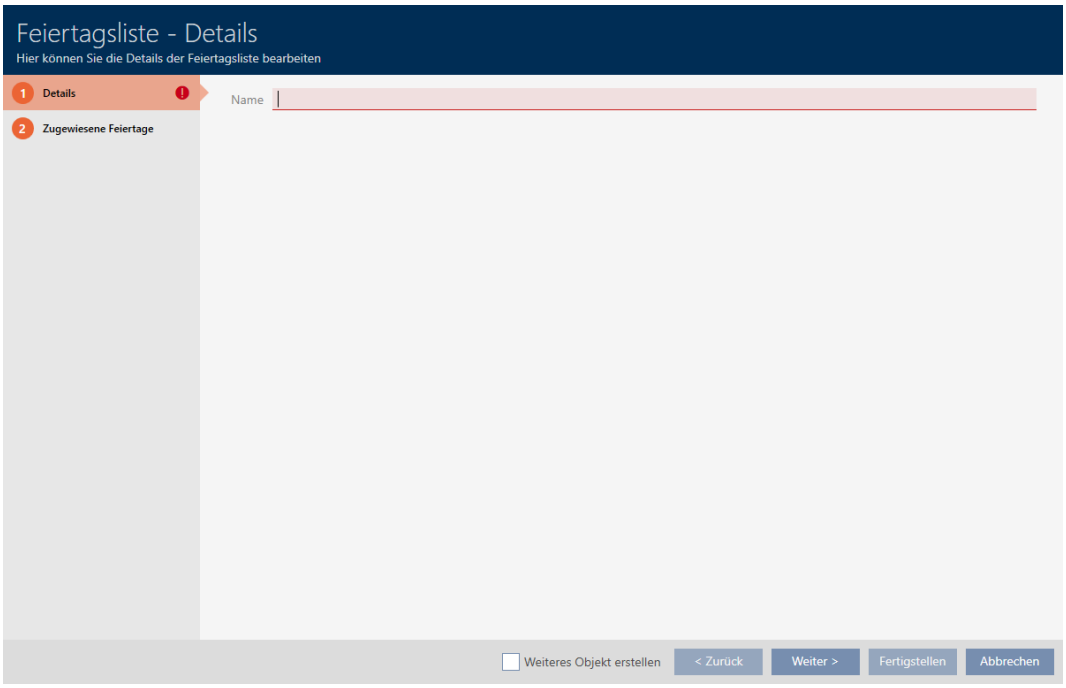
↳ The [Public holiday lists] tab will open.

Matrixansicht × | Zeitplansteuerung × | Feiertagslisten × | Feiertage ×

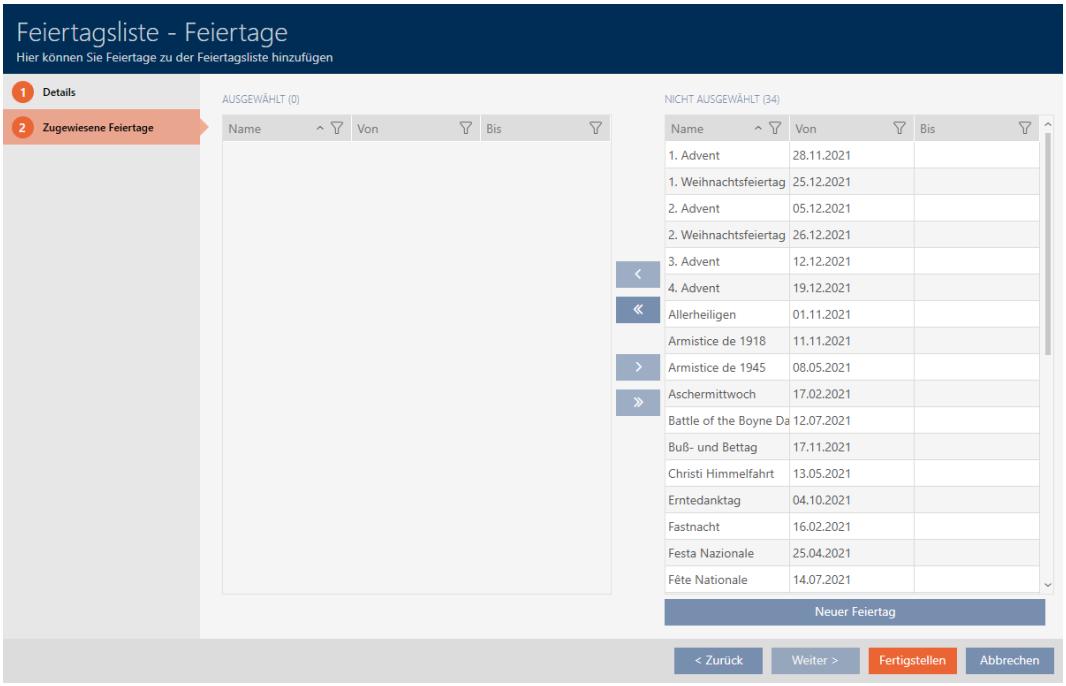
Neu | Löschen | Export | Anzeigefilter löschen

Name	Letzte Änderung
Baden-Würtemberg	26.04.2021 23:56:58
Bayern	26.04.2021 23:56:58
Berlin	26.04.2021 23:56:58
Brandenburg	26.04.2021 23:56:58
Bremen	26.04.2021 23:56:58
Hamburg	26.04.2021 23:56:58
Hessen	26.04.2021 23:56:58
Mecklenburg-Vorpommern	26.04.2021 23:56:58
Niedersachsen	26.04.2021 23:56:58
Nordrhein-Westfalen	26.04.2021 23:56:58
Rheinland-Pfalz	26.04.2021 23:56:58
Saarland	26.04.2021 23:56:58
Sachen-Anhalt	26.04.2021 23:56:58
Sachsen	26.04.2021 23:56:58
Schleswig-Holstein	26.04.2021 23:56:58
Thüringen	26.04.2021 23:56:58

4. Click on the New + button.
   ↳ The window for creating a public holiday list will open.



5. Enter a name for your public holiday list in the *Name* field.
6. Click on the Assigned public holidays tab.
   ↳ Window switches to the "Assigned public holidays" tab.



7. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

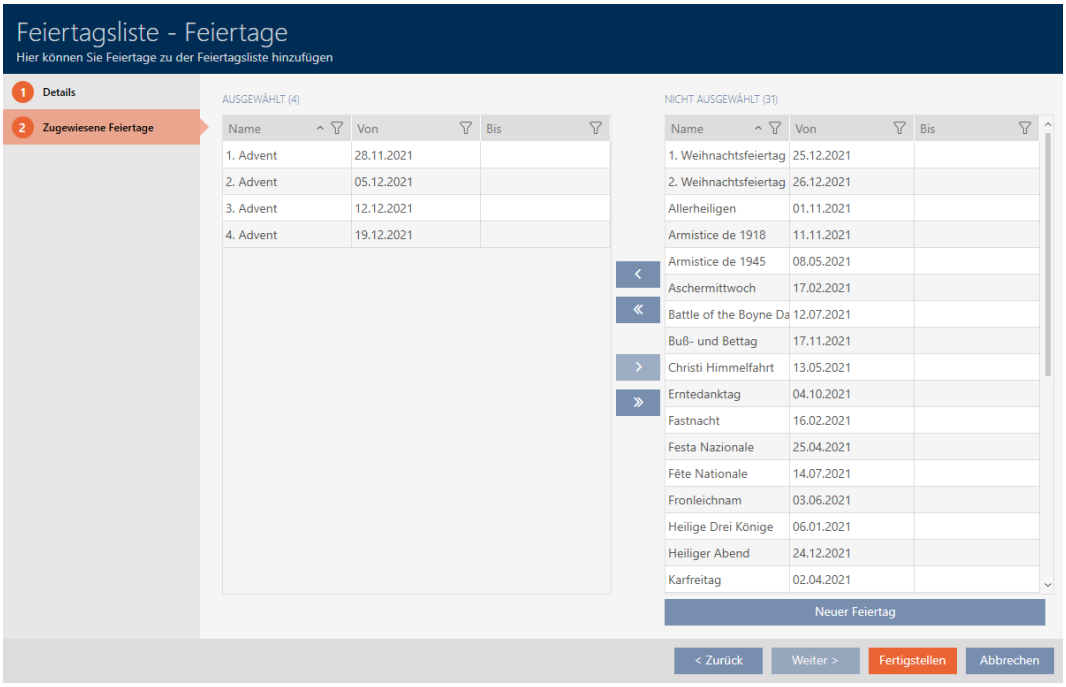
8. Select all public holidays that you wish to assign to your public holiday list (Ctrl+click for single days or Shift+click for multiple days).

NOTE

Double-clicking as an alternative to arrow keys

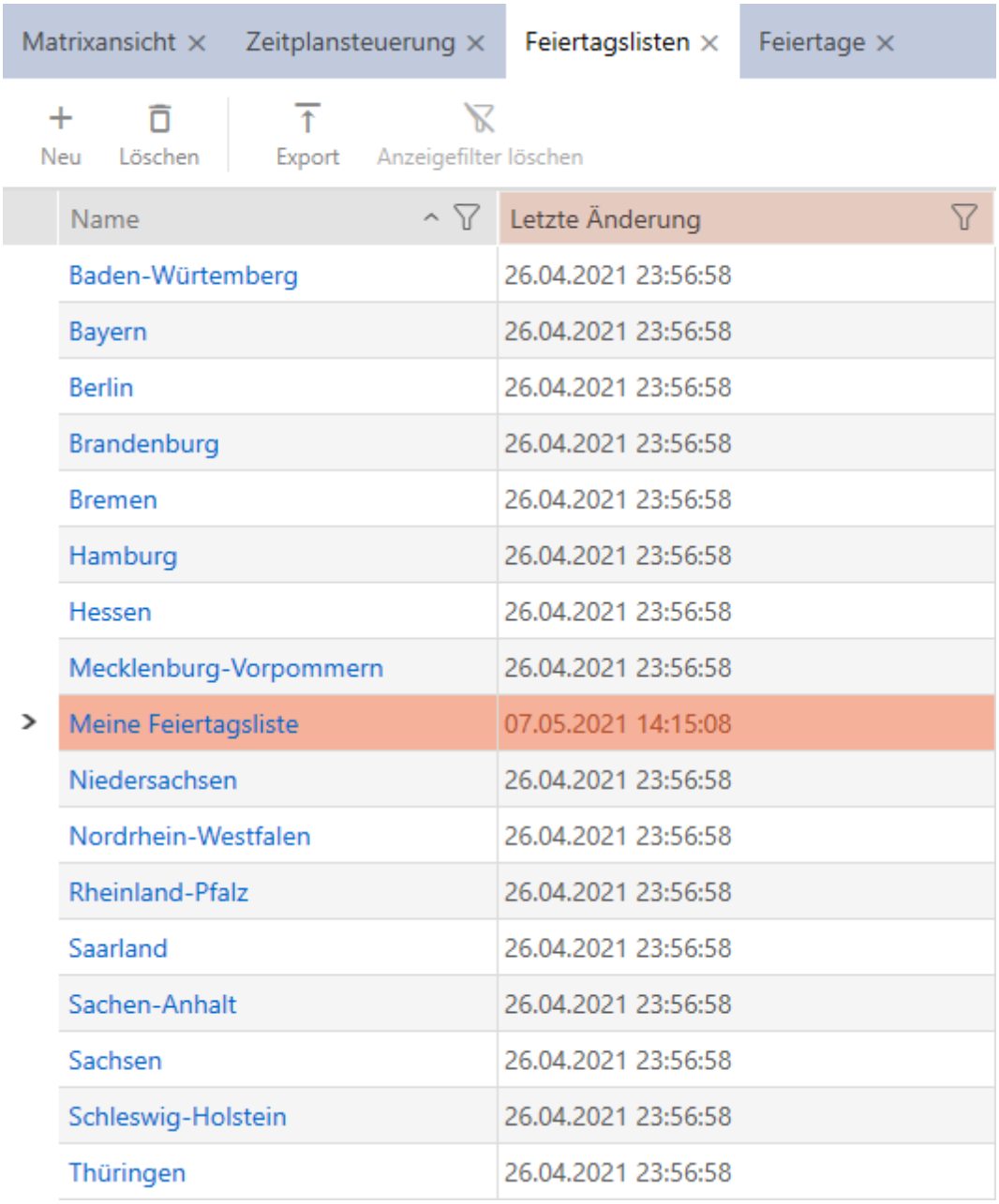
Double-clicking an entry in the list will also move this entry to the other column.

9. Use [<] to move only the selected public holidays or [<<] to move all displayed public holidays.
   ↳ The public holidays highlighted in the left-hand column are added to your public holiday list.



10. Click on the Finish button.
    ↳ The window for creating a public holiday list closes.

↳ The public holiday list has been created and is listed.



Name	Letzte Änderung
Baden-Würtemberg	26.04.2021 23:56:58
Bayern	26.04.2021 23:56:58
Berlin	26.04.2021 23:56:58
Brandenburg	26.04.2021 23:56:58
Bremen	26.04.2021 23:56:58
Hamburg	26.04.2021 23:56:58
Hessen	26.04.2021 23:56:58
Mecklenburg-Vorpommern	26.04.2021 23:56:58
> Meine Feiertagsliste	07.05.2021 14:15:08
Niedersachsen	26.04.2021 23:56:58
Nordrhein-Westfalen	26.04.2021 23:56:58
Rheinland-Pfalz	26.04.2021 23:56:58
Saarland	26.04.2021 23:56:58
Sachen-Anhalt	26.04.2021 23:56:58
Sachsen	26.04.2021 23:56:58
Schleswig-Holstein	26.04.2021 23:56:58
Thüringen	26.04.2021 23:56:58

You can now add the created public holiday list to your locking devices, for example: *Limiting authorisations for locking devices to specific times (schedule) [▸ 220].*

14.9 Creating a location

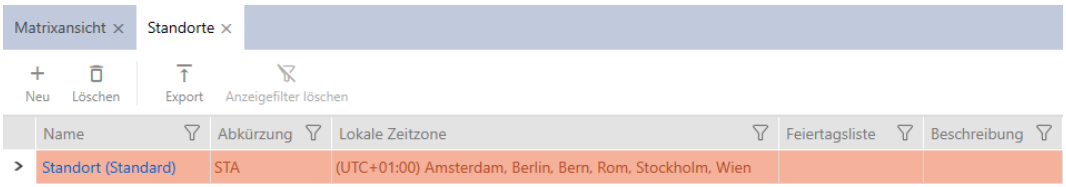
There must be at least one location in the database. AXM Lite therefore creates a default location for you.

✓ AXM Lite open.

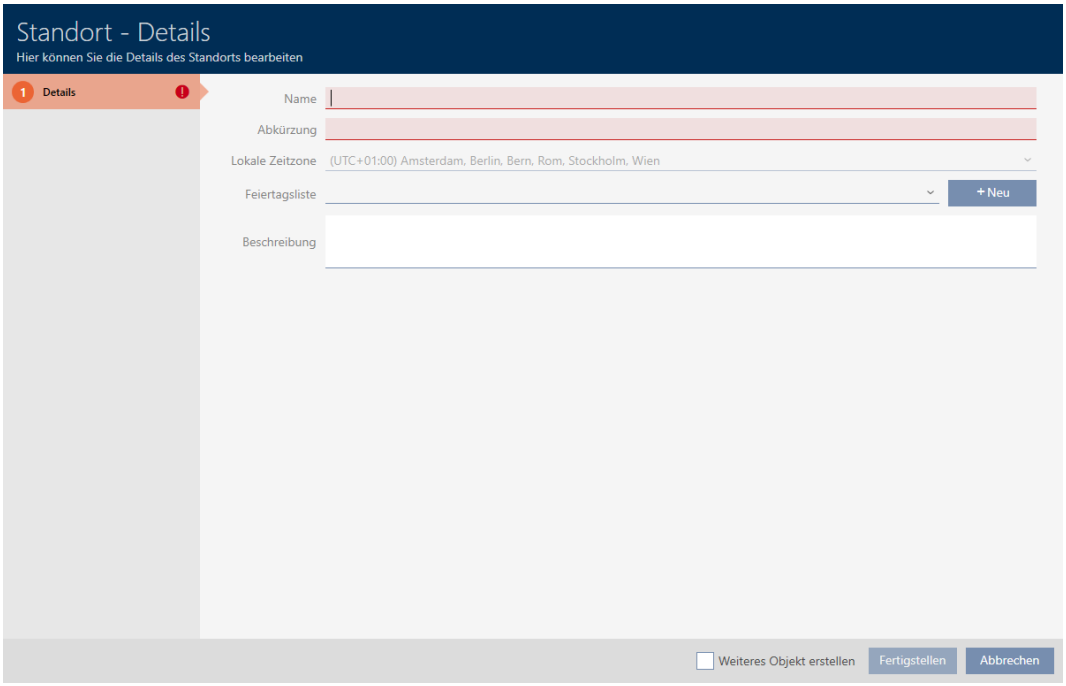
1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

2. Select the Locations entry in the | ORGANISATIONAL STRUCTURE | group.

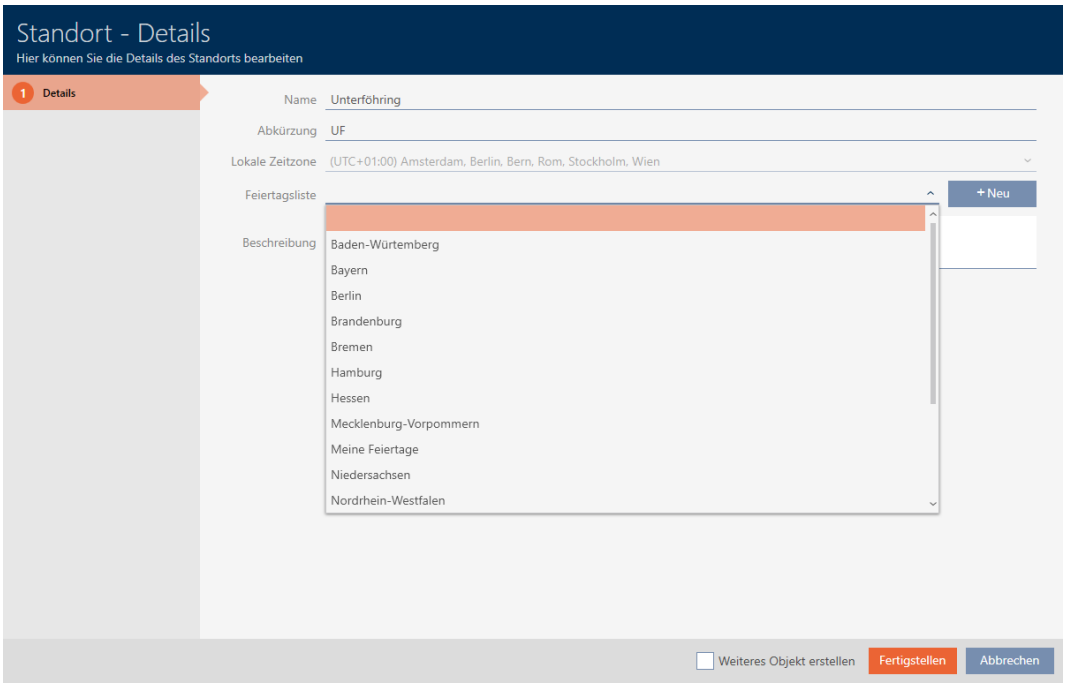
   ↳ The [Locations] tab will open.



3. Click on the New + button.
   ↳ The window for creating a new location will open.



4. Enter a name for your location in the *Name* field.
5. Enter the abbreviation for your location in the *Shortcut* field (max. 5 character).
6. Select the time zone for your location in the ▼ **Local time zone** drop-down menu (can only be configured in AXM Classic or higher).
7. Select the public holiday list to be used for your location from the ▼ **Holiday list** drop-down menu (also see *Creating and editing public holiday lists [▸ 65]*).



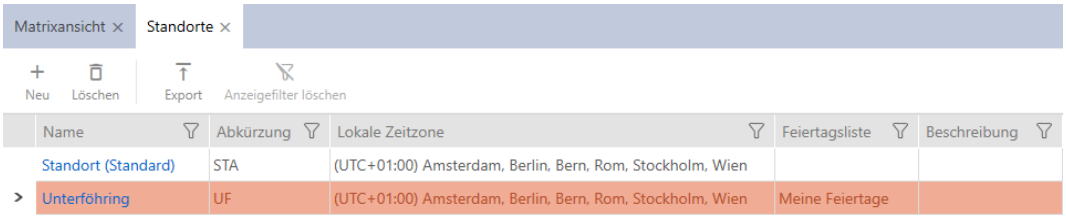
NOTE

Public holiday lists in locking device and locations

You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

If a public holiday list is assigned to the location instead of the locking device, the public holiday list for the location is applied to the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

8. Enter a description of your location in the *Description* field if required.
9. Click on the Finish button.
   ↳ The window for creating a new location closes.
   ↳ The newly created location is listed.



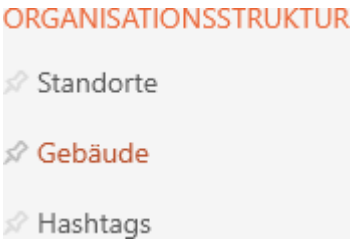
14.10 Creating a building and assigning it to a location

There must be at least one building in the database. AXM Lite therefore creates a default building for you. Obviously, you can create additional buildings.

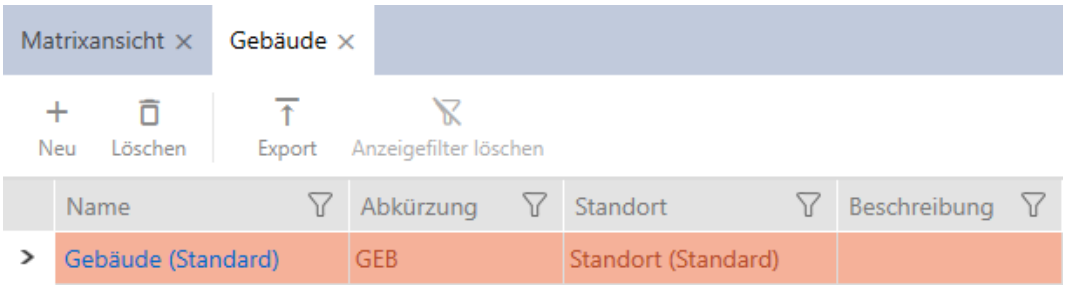
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

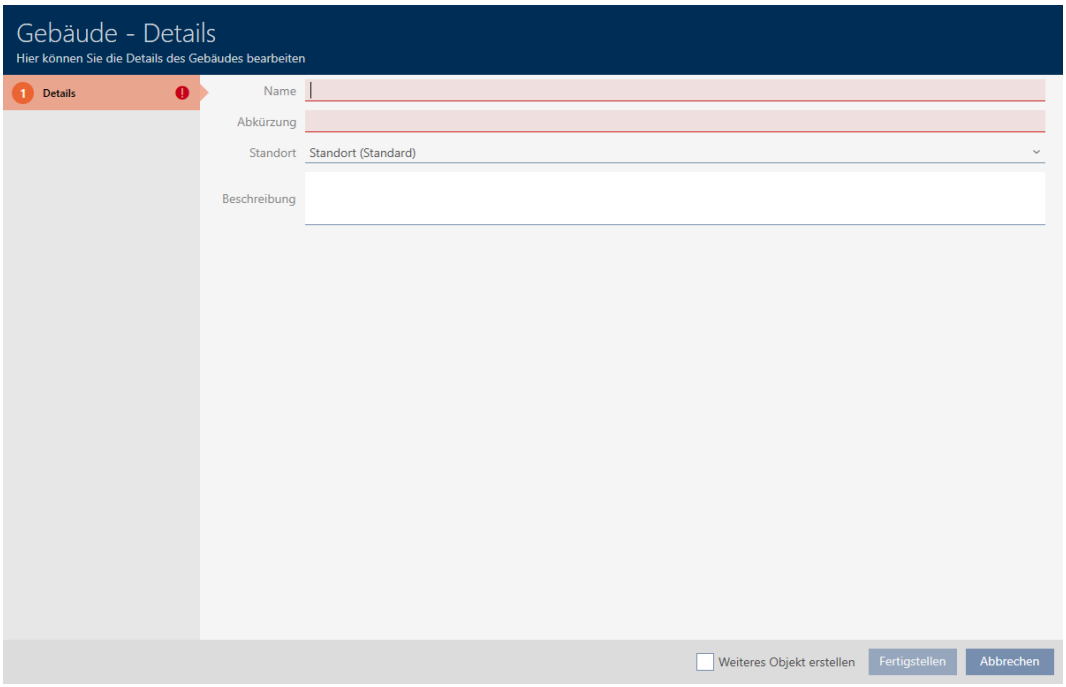
2. Select the Building entry in the | ORGANISATIONAL STRUCTURE | group.



↳ The [Building] tab will open.

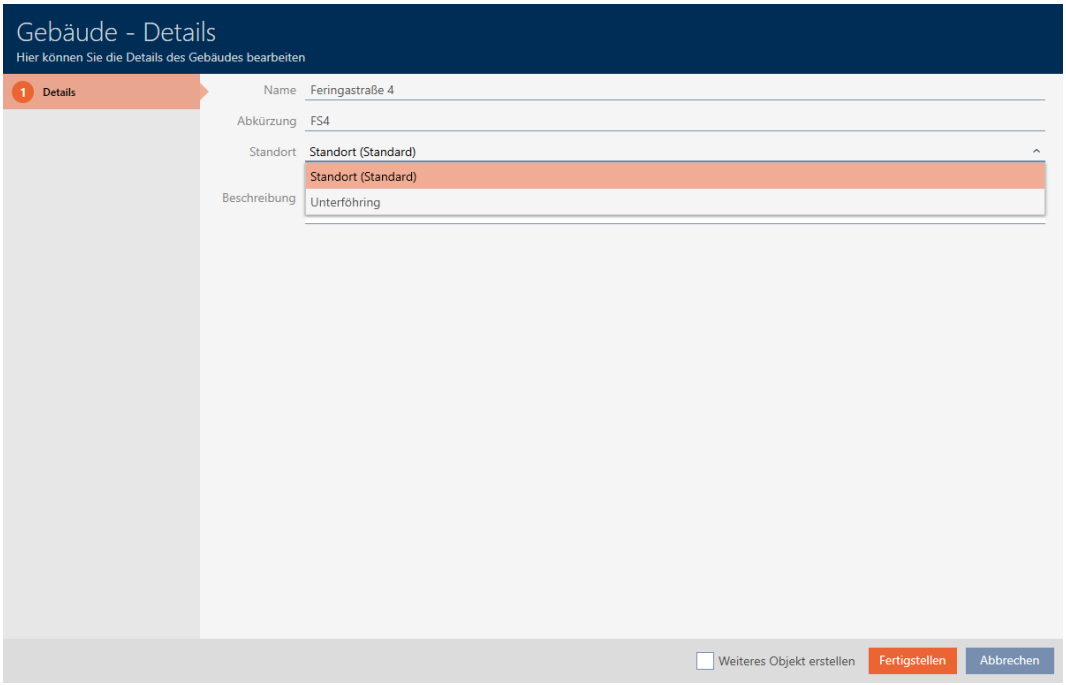


3. Click on the New + button.
↳ The window for creating a new building will open.

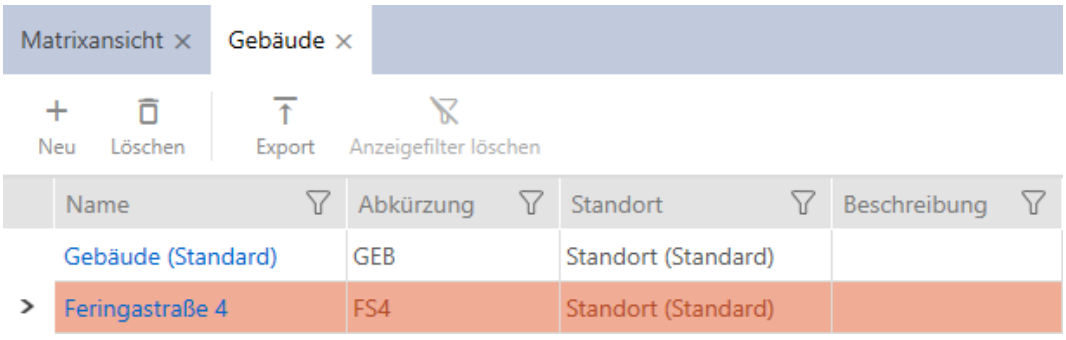


4. Enter a name for your building in the *Name* field.
5. Enter the abbreviation for your building in the *Shortcut* field (max. 5 characters).

6. Select the location to which your building belongs from the ▼ **Location** drop-down menu.



7. Enter a description of your building in the *Description* field if required.
8. Click on the Finish button.
   ↳ Window for creating a new building closes.
   ↳ The newly created building is listed.



14.11 Creating a hashtag

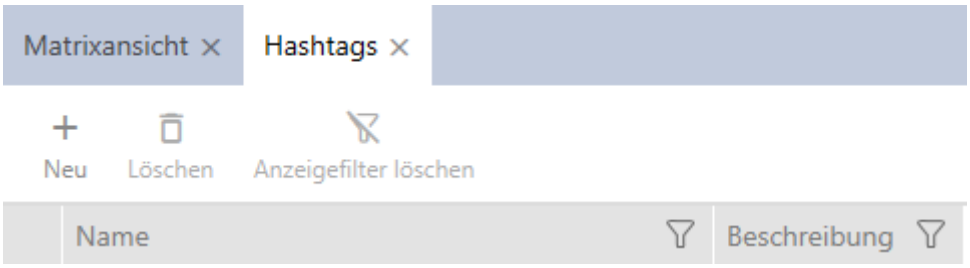
Hashtags can be used as keywords for persons and/or doors (see *Hashtags [▸ 380]*).

✓ AXM Lite open.

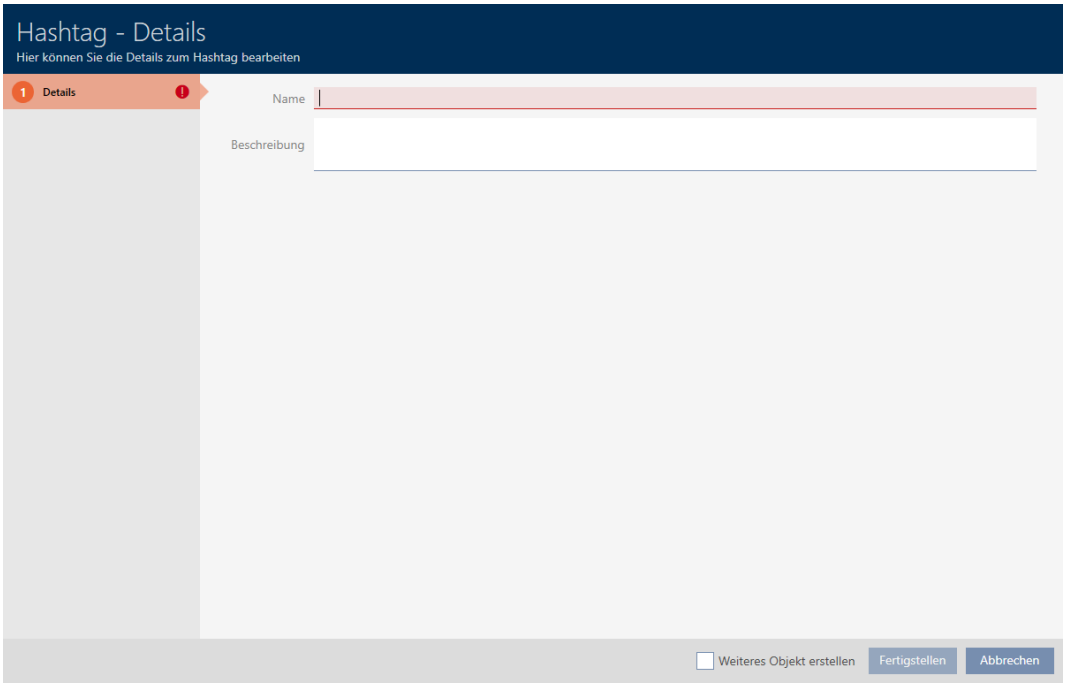
1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

2. Select the Hashtags entry in the | ORGANISATIONAL STRUCTURE | group.

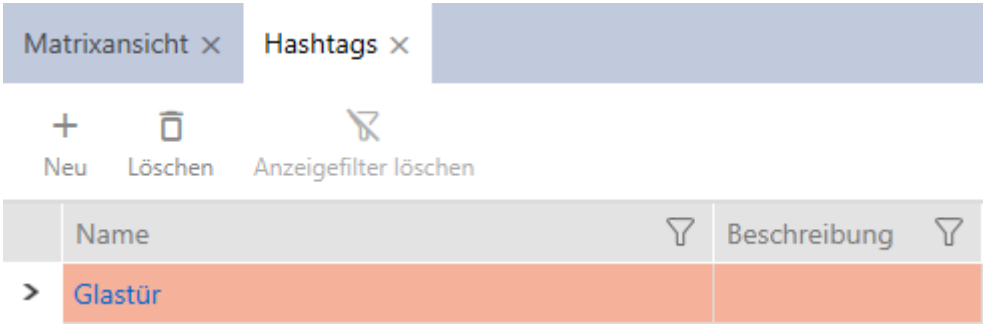
   ↳ The [Hashtags] tab will open.



3. Click on the New + button.
   ↳ The window for creating a new hashtag will open.



4. Enter your hashtag in the *Name* field (no spaces).
5. Enter a description of your hashtag in the *Description* field if required.
6. Click on the Finish button.
   ↳ The window for creating a new hashtag closes.
   ↳ The newly created hashtag is listed.



15. Persons and identification media

Any changes you make to the locking system will only take effect when synchronised (see *Synchronise a card/transponder (including importing physical access list) [▸ 304]*).

15.1 Creating an identification medium

Your users can use identification media to engage and disengage locking devices (also see *Identification media, locking devices and the locking plan [▸ 360]*).

Your AXM Lite will provide you with the following identification media to choose from:

- Transponder
- Cards
- PIN code keypad AX
- PIN code keypad 3068 with G1 protocol

These identification media differ from one another:

Further information on the different identification media and their differences can be found in Section *Identification media, locking devices and the locking plan [▸ 360]*.

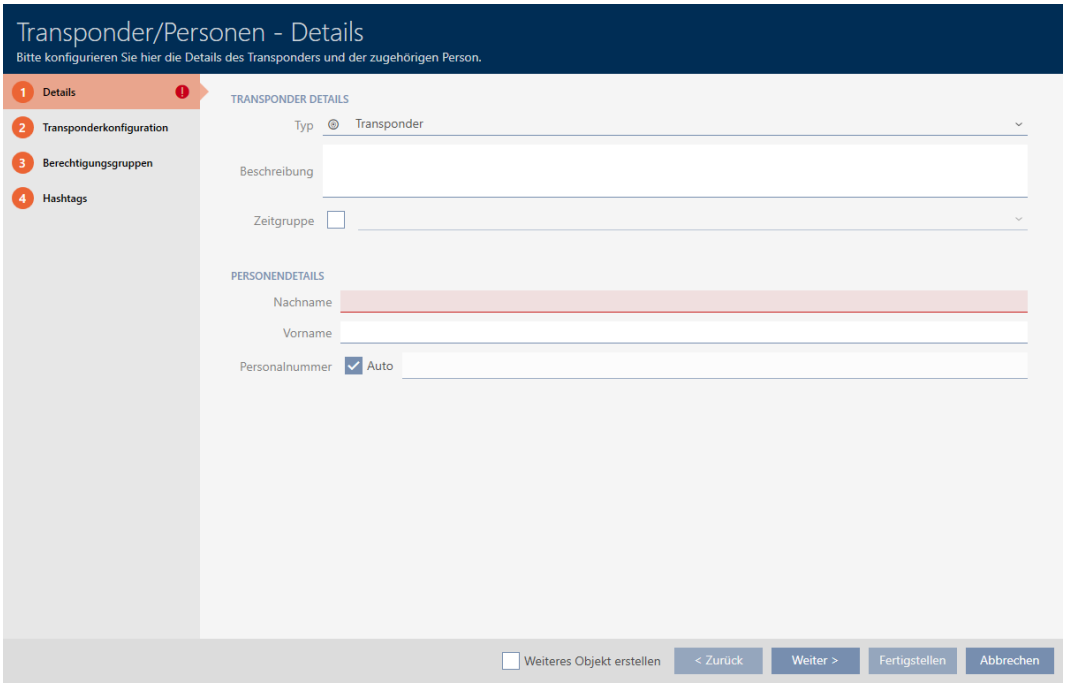
15.1.1 Creating transponders and cards

In the interests of best practice (see *Best practice: setting up the locking system [▸ 29]*), SimonsVoss recommends that you configure access levels and schedules/time groups:

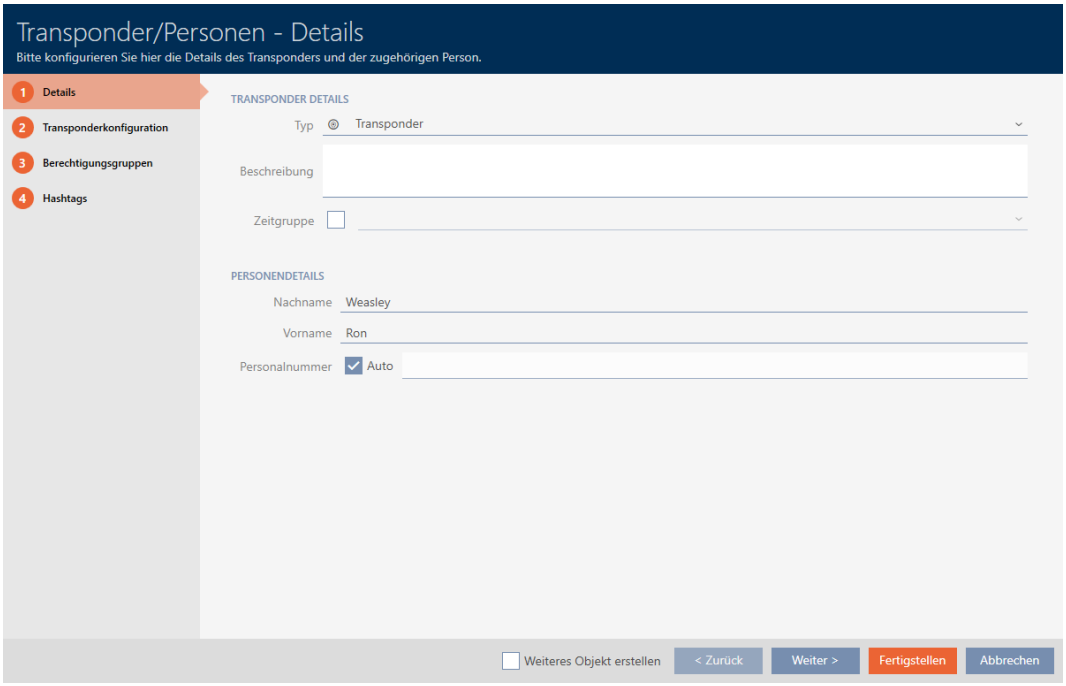
- *Access levels [▸ 261]* (see *Access levels [▸ 378]* for background information)
- *Creating a schedule [▸ 45]* or *Create time group [▸ 49]* (see *Time groups and schedules [▸ 366]* for background information)

✓ AXM Lite open.

1. Click on the New transponder button.
   ↳ The window for creating an identification medium will open.



2. Enter a description if required.
3. If the identification medium is to feature time-controlled authorisations: select the ☑ Time group checkbox.
4. Select the time group from the ▼ **Time group** drop-down list (e.g. "Time group").
5. Enter the surname and first name of the person who will receive the identification medium in the *Last name* and *First name* fields.
   ↳ The surname and first name will be displayed in the matrix at a later point in time.
   ↳ The personnel number is generated automatically.



NOTE

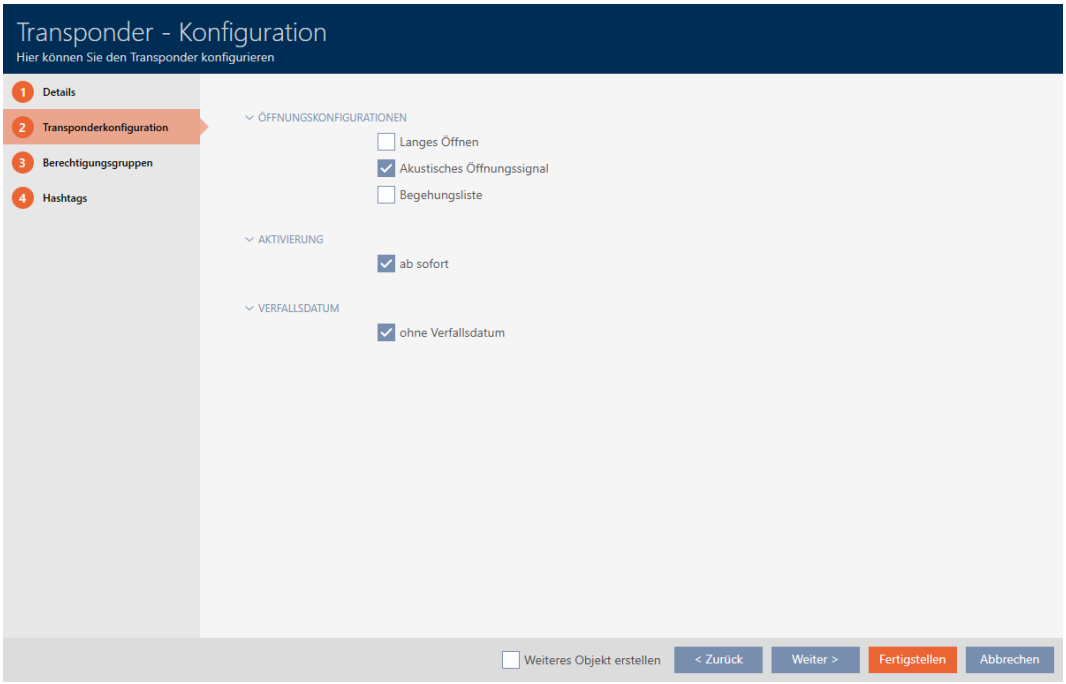
Personnel number formula or manual entry

The AXM Lite generates personnel numbers based on the following formula: PN-1, PN-2, PN-X. The abbreviation *PN* can be changed if required (see *Changing automatic numbering [▸ 332]*).

Alternatively, you can enter personnel numbers manually:

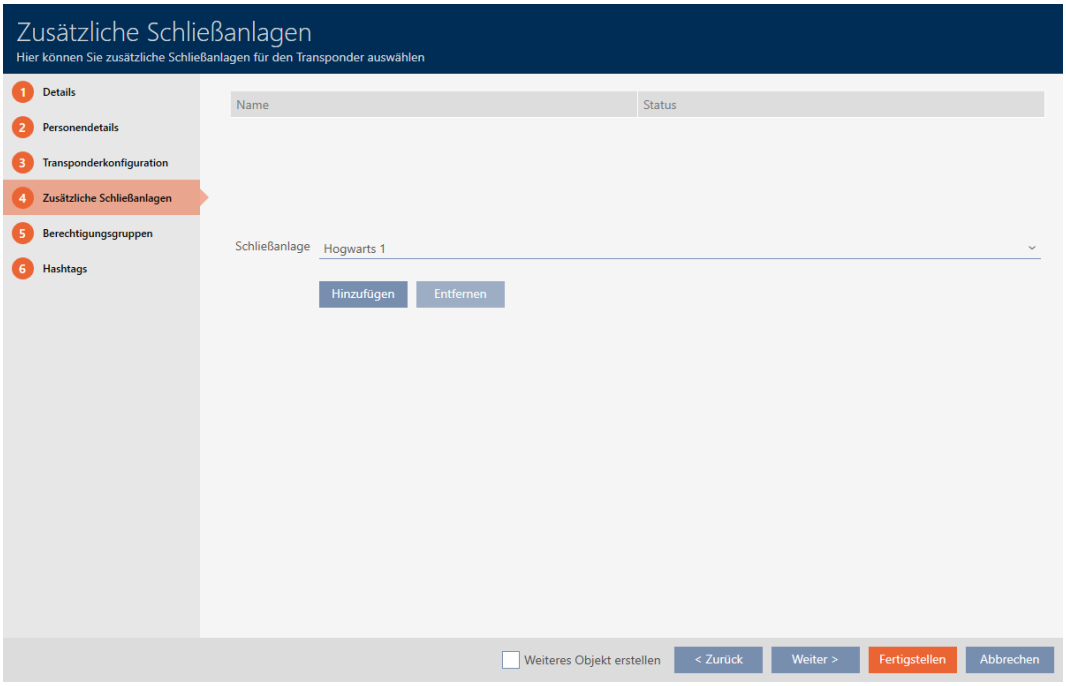
1. Activate the ☐ Auto check box.
   ↳ The *Personnel number* field is activated.
2. Enter the personnel number in the *Personnel number* field.

6. Use the Next > button to switch to the next tab or complete the entries with the Finish button.

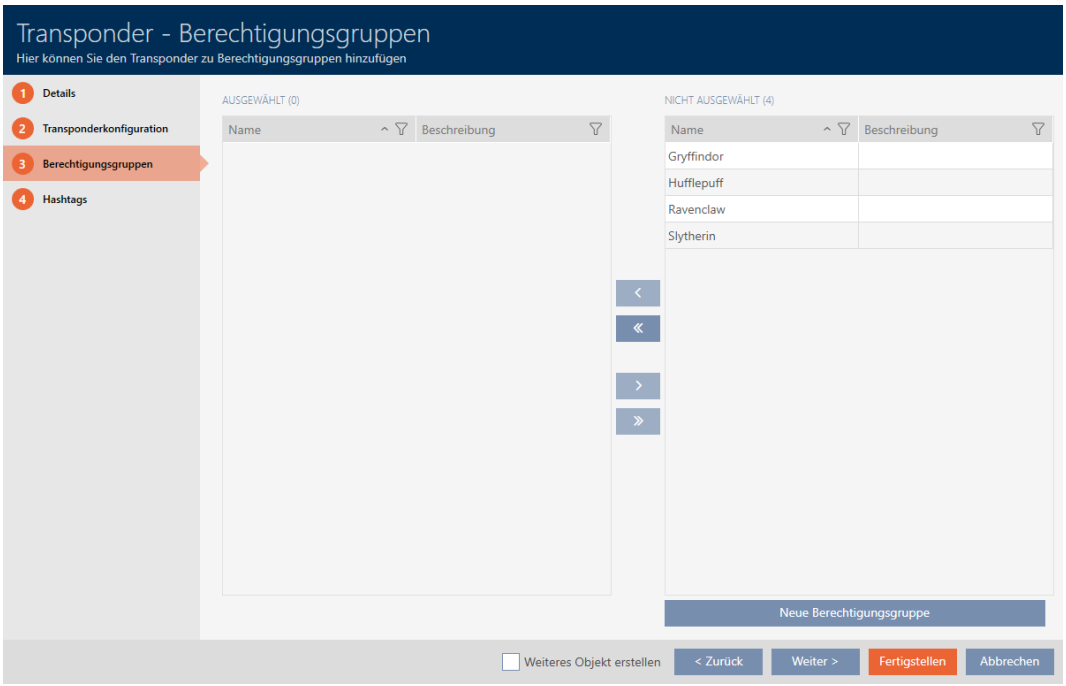


7. If locking devices need to open twice as long for this identification medium (doubling to max. 25 s): select the ☑ Long opening checkbox.
8. If you don't wish locking devices for this identification medium to beep: disable the ☐ No acoustic opening signal checkbox.
9. If you need to save the locking devices on which the identification medium was used on the identification medium: select the ☑ Personal audit trail checkbox.
10. If you do not want the transponder to be usable immediately: disable the ☐ from now checkbox. Then enter an activation date.

11. If the transponder is only to be used for a limited period of time, disable the ☐ without expiry date checkbox. Then enter an expiry date.

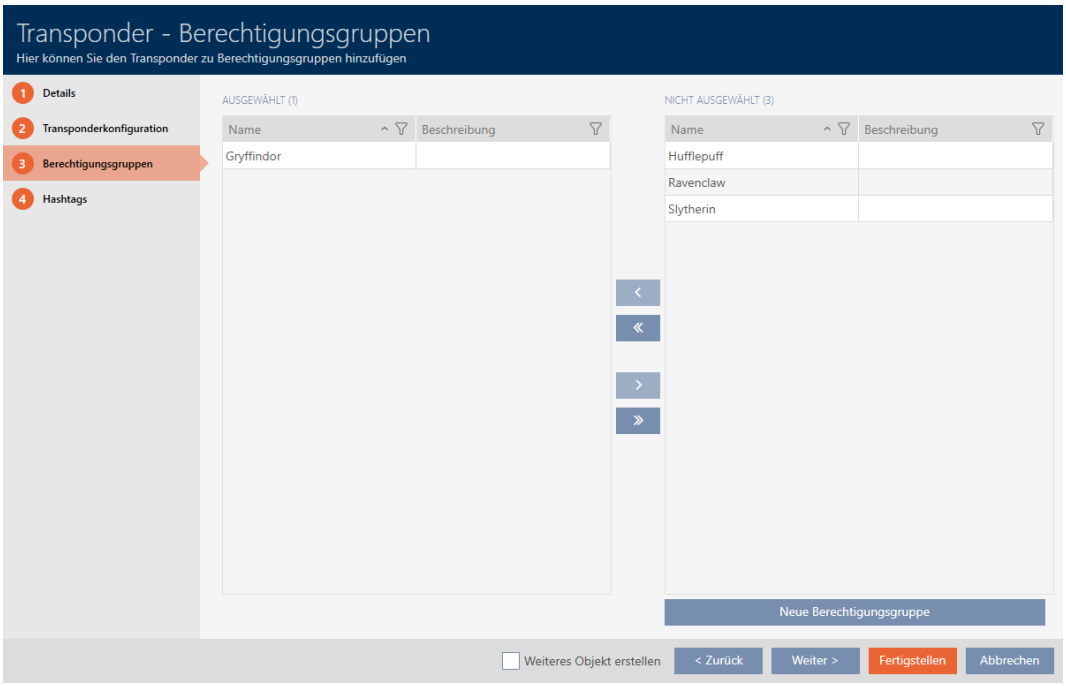


12. Use the Next > button to switch to the next tab or complete the entries with the Finish button.



13. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
14. Select the required access levels in the right column (Ctrl+click for single groups or Shift+click for multiple groups).

15. Use < to move the selected access levels only or << to move all displayed access levels.
    ↳ The identification medium is assigned to the highlighted access levels.

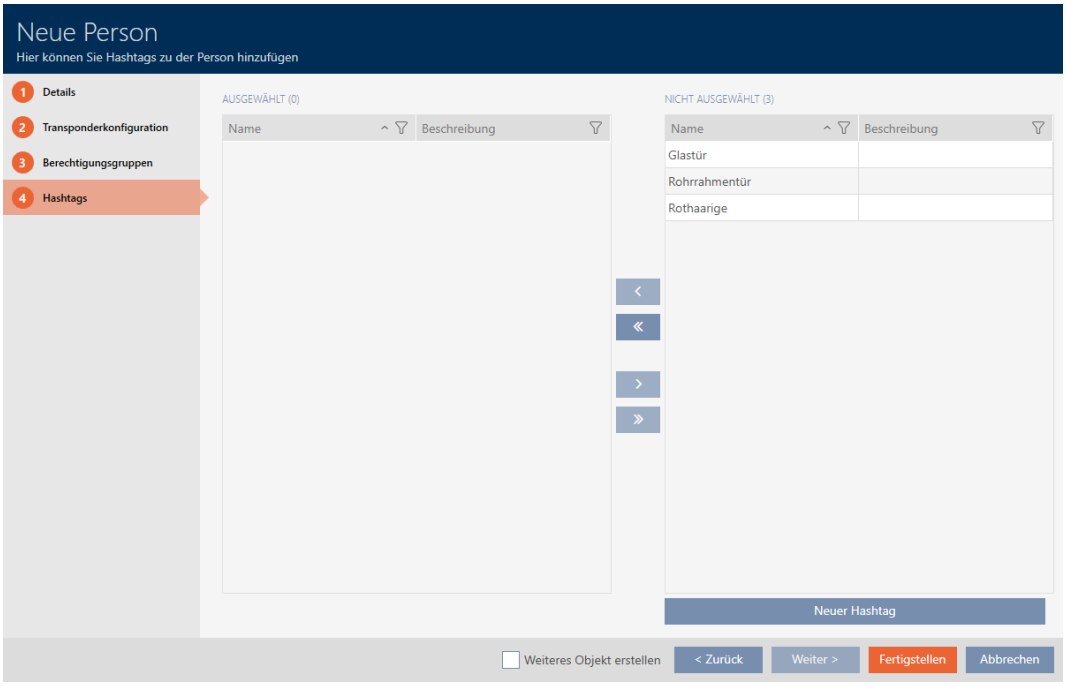


NOTE

Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

16. Use the Next > button to switch to the next tab or complete the entries with the Finish button.



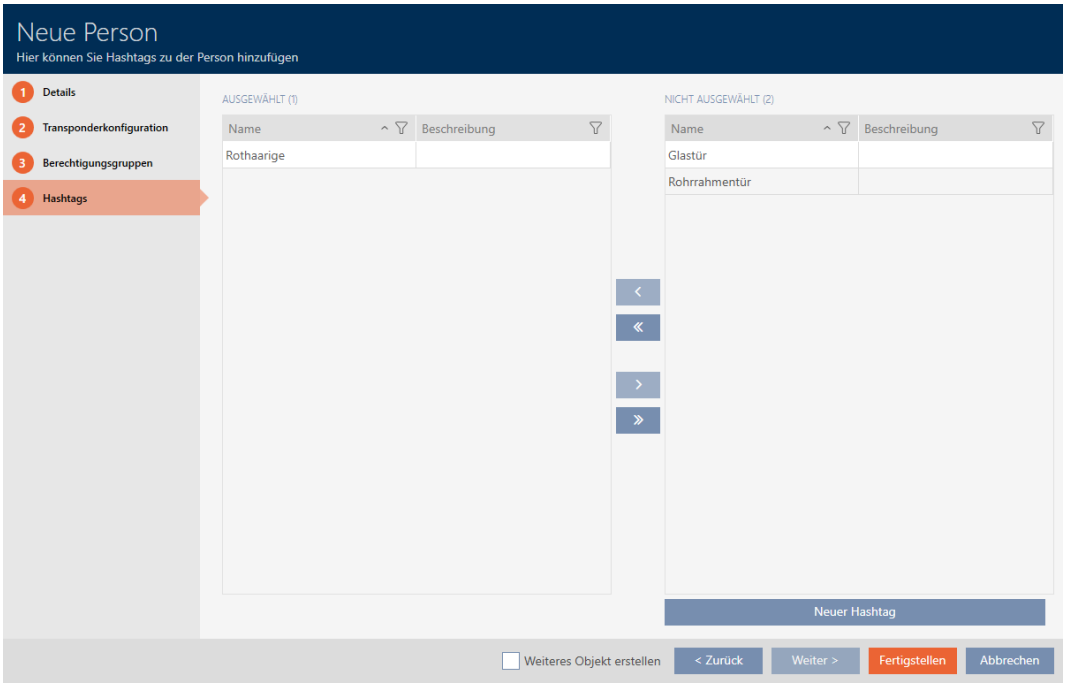
17. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
18. Select the required hashtags in the right column (Ctrl+click for single hashtags or Shift+click for multiple hashtags).
19. Use < to move only the selected hashtags or « to move all hashtags.

NOTE

Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

↳ The highlighted hashtags in the left-hand column are used for this identification medium.



20. Select the ☑ Create additional objects checkbox to leave the window with the same settings open for the next identification medium to be created.
21. Click on the Finish button to create the identification medium.
    ↳ The window for creating a new identification medium closes.

↳ Newly created identification medium is listed or displayed in the matrix.

15.1.2 Creating PIN code keypads

PIN code keypads allow your users to engage and disengage locking devices using a number code (PIN) (also see *Identification media, locking devices and the locking plan [▸ 360]*).

In the interests of best practice (see *Best practice: setting up the locking system [▸ 29]*), SimonsVoss recommends that you configure schedules/ time groups first:

- *Creating a schedule [▸ 45]* or *Create time group [▸ 49]* (see *Time groups and schedules [▸ 366]* for background information)

A PIN code keypad AX is created in this example. You can create a PIN code keypad 3068 in the same way, but you cannot specify the length of the PINs and the PINs in your AXM Lite (also see PIN Code G1 vs. PIN Code AX).

NOTE

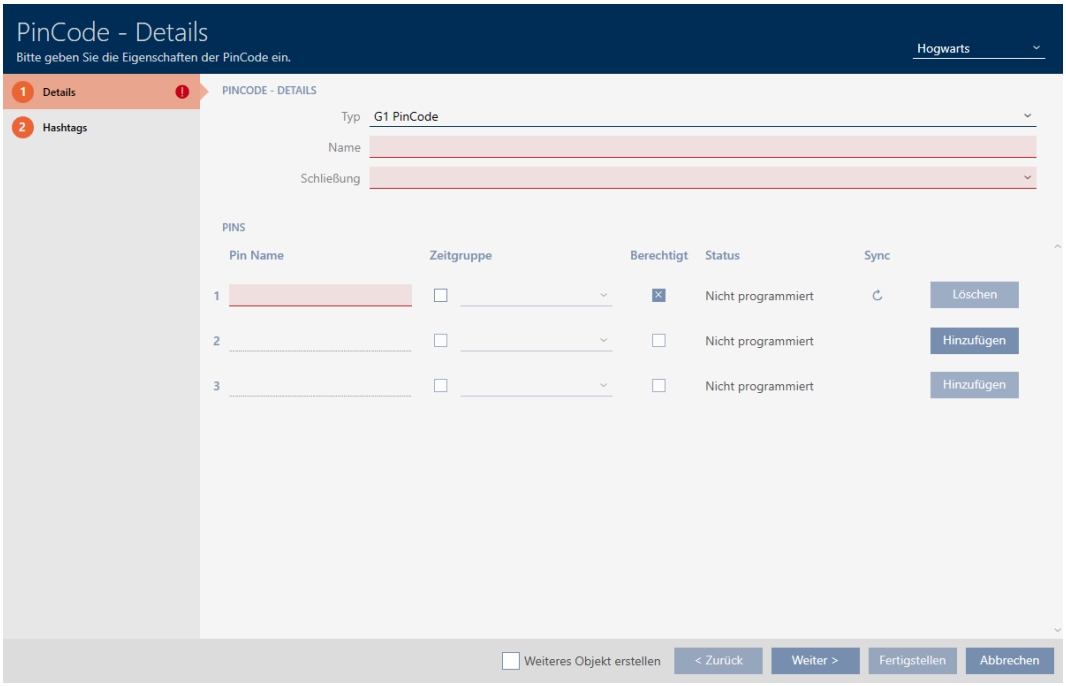
Authorisations set automatically

Your AXM Lite assumes that you also want to authorise newly created PINs. Newly created PINs therefore automatically receive authorisation for the assigned locking device.

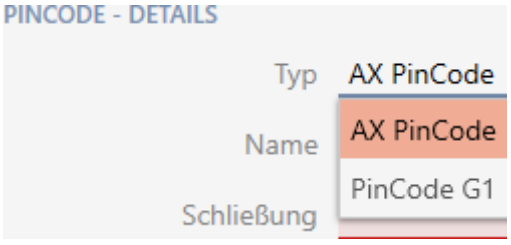
✓ AXM Lite open.

✓ Locking device has been created for the PIN code keypad (see *Creating a locking device [▸ 182]* in the AXM manual).

1. Click on the New PinCode button.
   ↳ The "PinCode - Details" window will open.

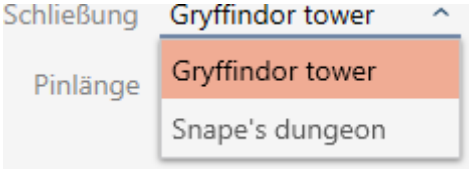


2. Select the PIN code keypad you wish to create from the ▼ **Type** drop-down menu.

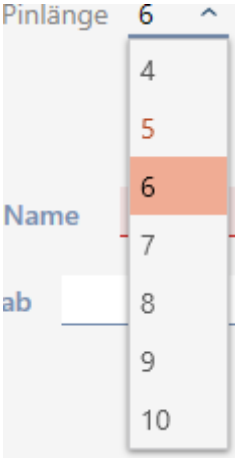


3. Enter a name for the PIN code keypad in the *Name* field.

4. Select the locking device on which you would like to use the PIN code keypad from the ▼ **Lock** drop-down menu.



5. If you are creating a PIN code keypad AX, select the length of the PINs from the ▼ **Pin length** drop-down menu.



6. Enter the name to be displayed in the matrix for this PIN in the *Pin name* field.
7. Enter a PIN.
   ↳ Authorisation is set automatically.

NOTE

Duplicate PINs not permitted for PIN code keypad AX

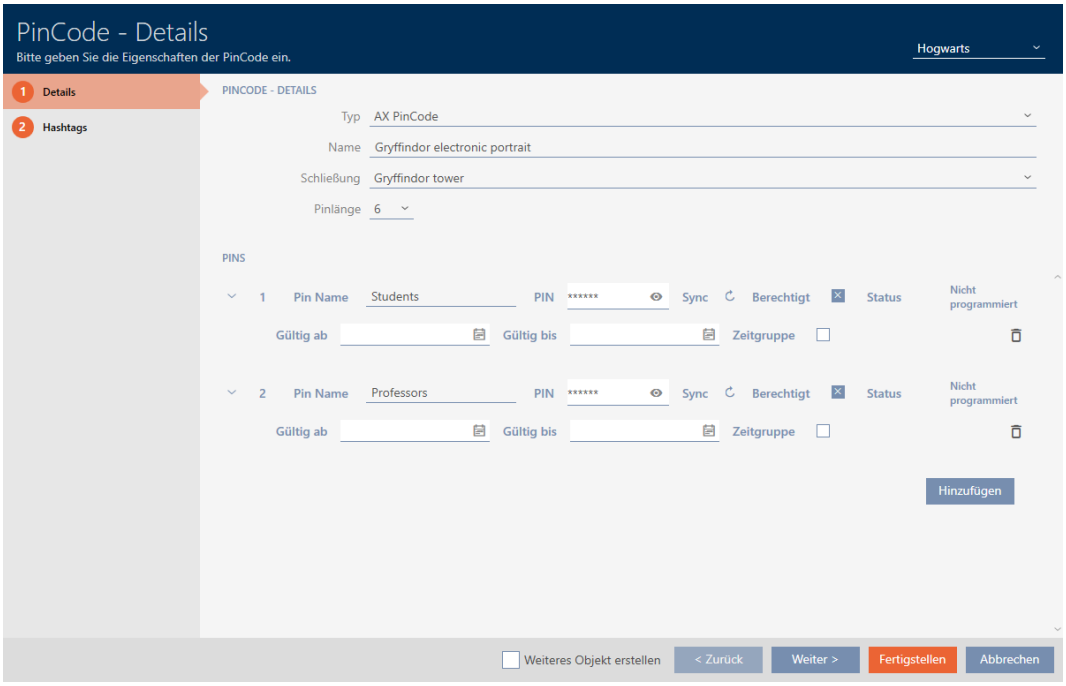
All PINs for a PIN code keypad must be different for reasons of security and traceability.

Your AXM Lite detects duplicate PINs and highlights them with *The pin is not unique* in red.

8. Disable the ☐ Authorised checkbox if you want to authorise the PIN at a later stage.
9. If you want to control an activation/expiry date or the authorisation in terms of time, use ⌄ to expand the PIN settings.
10. If necessary, enter the activation/expiry date in the *Valid from* or *Valid to* field.
    (PIN code keypad AX: possible to the exact day; PIN code keypad 3068: possible to the exact hour)

11. Select the ☑ Time group checkbox if required.
    ↳ A drop-down menu will appear.
12. Select the time group you want to use for this PIN from the ▼ **Time group** drop-down menu.

13. If necessary, click the Add button to create additional PINs.



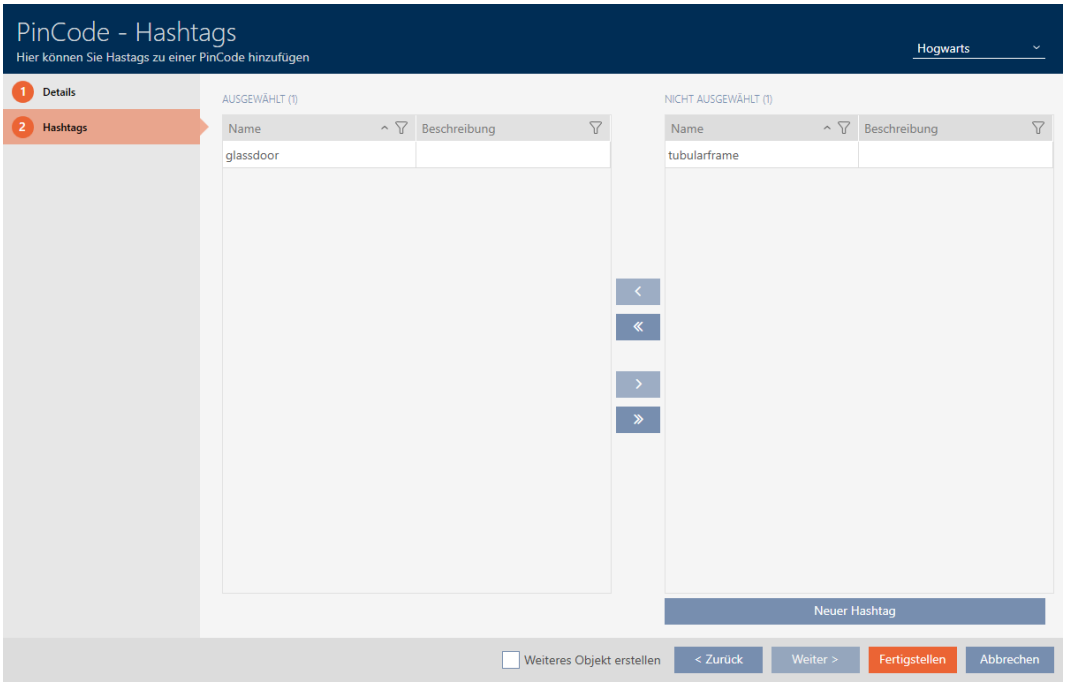
14. Use the Next > button to switch to the next tab or complete the entries with the Finish button.
15. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
16. Select the required hashtags in the right column (Ctrl+click for single hashtags or Shift+click for multiple hashtags).
17. Use < to move only the selected hashtags or « to move all hashtags.

NOTE

Double-clicking as an alternative to arrow keys

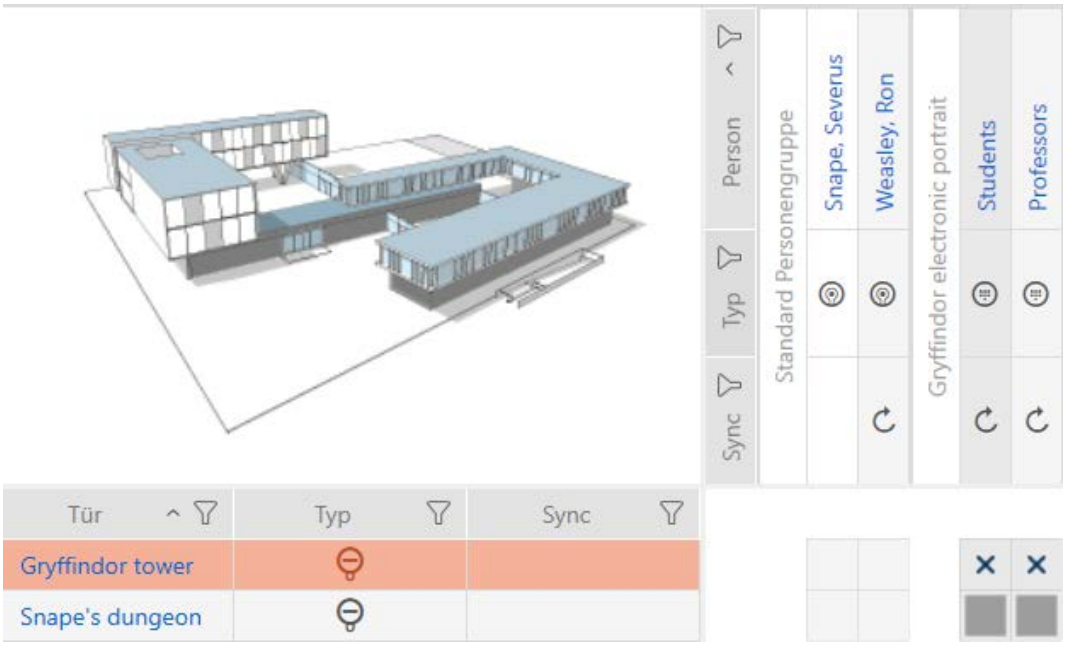
Double-clicking an entry in the list will also move this entry to the other column.

↳ The highlighted hashtags in the left-hand column are used for this PIN code.



18. Select the ☑ Create additional objects checkbox to leave the window with the same settings open for the next PIN code to be created.
19. Click the Finish button to create the PIN code.
    ↳ "PinCode - Details" window closes.

↳ Newly created PIN code is listed or displayed in the matrix.



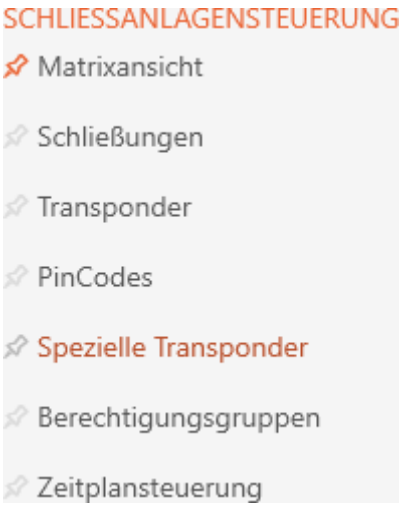
15.1.3 Creating special identification media

You can assign just one function to a specific identification medium, either Battery replacement or Lock Activation (see Special identification media and their functions). This identification medium can then no longer be used for other purposes in this project.

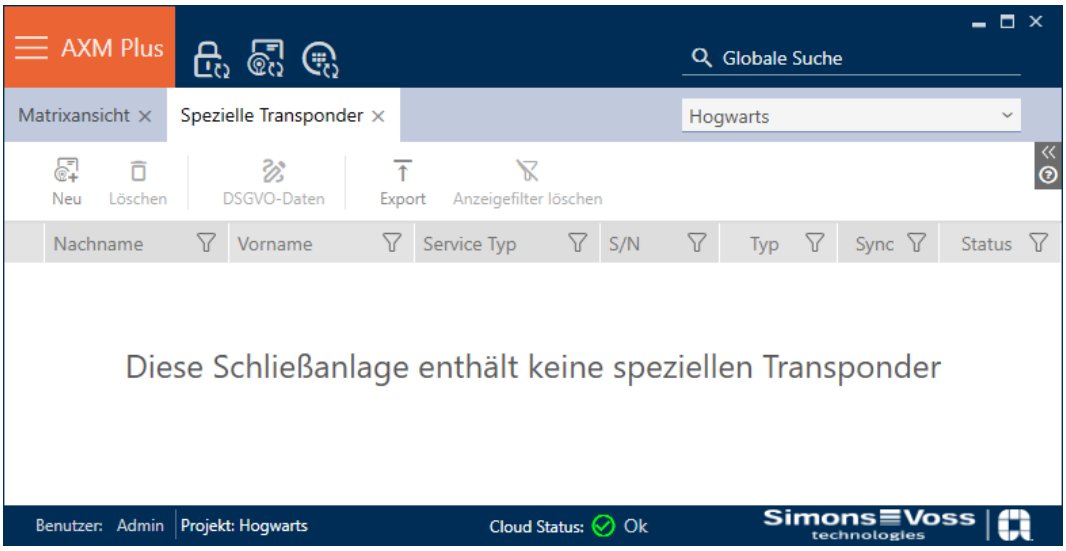
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

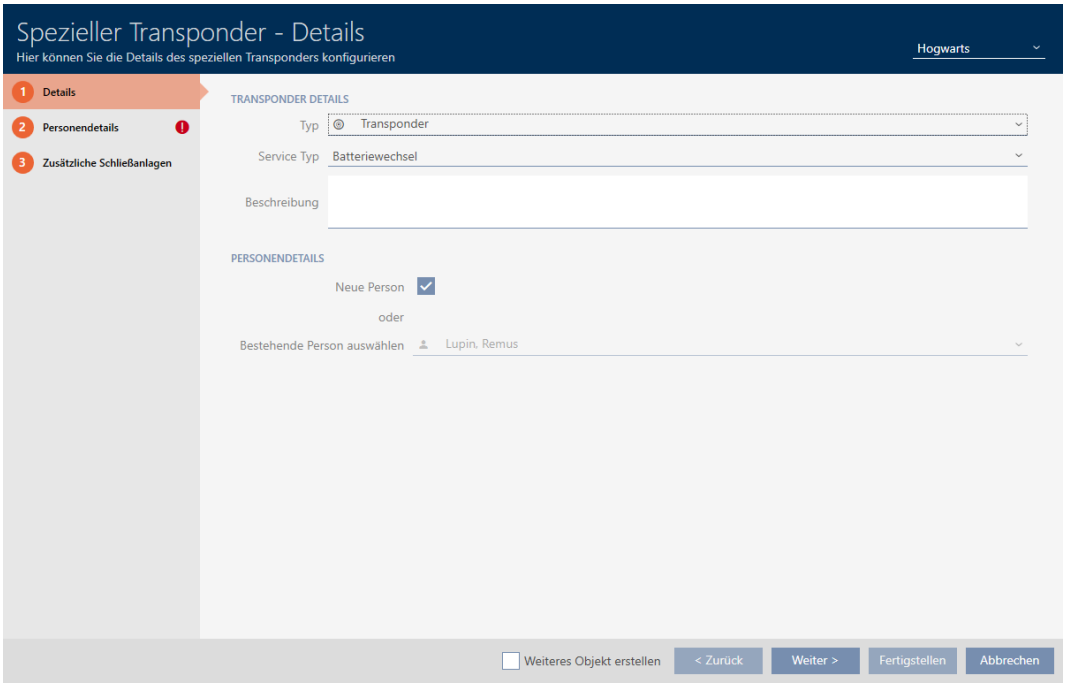
2. Select the Special Transponders entry in the | LOCKING SYSTEM CONTROL | group.



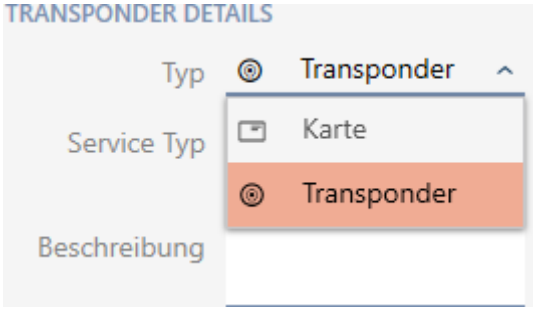
↳ The [Special Transponders] tab will open.



3. Click on the New button.
↳ The "Special Transponder" window will open.

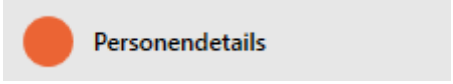


4. Select the type of identification medium you want to make a special identification medium from the drop-down ▼ **Type** menu.

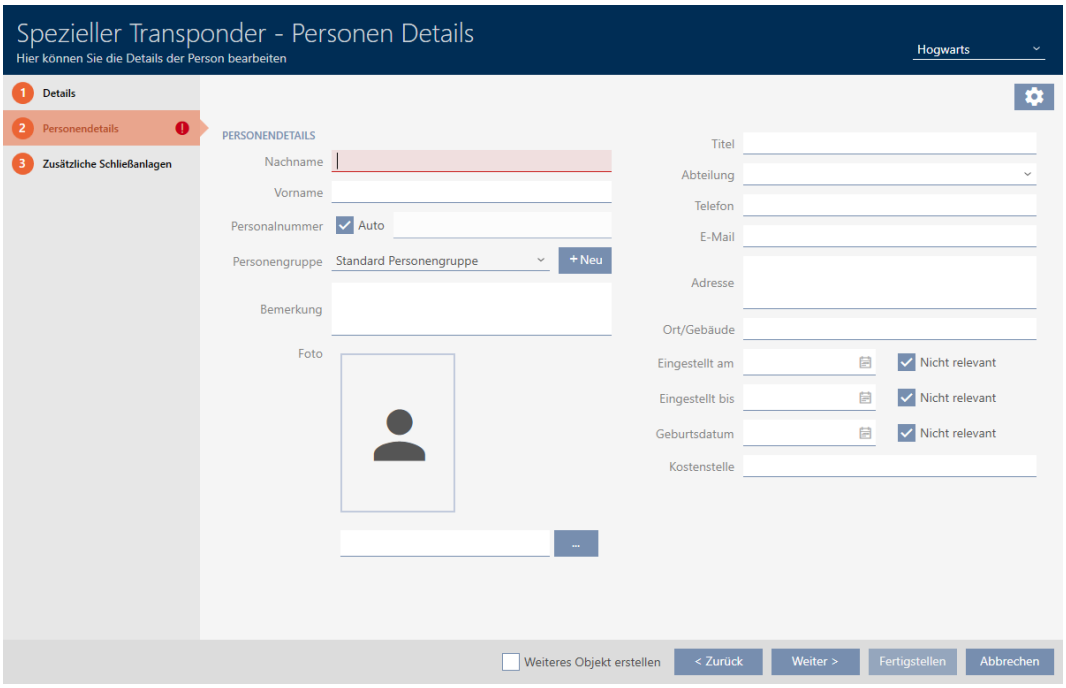


5. Then use the drop-down ▼ **Service Type** menu to select which function this identification medium should have ("Battery replacement" or "Lock Activation").

6. Enter a description if required.



7. Enter the surname and first name of the person who will receive the identification medium in the *Last name* and *First name* fields.
   ↳ The personnel number is generated automatically.



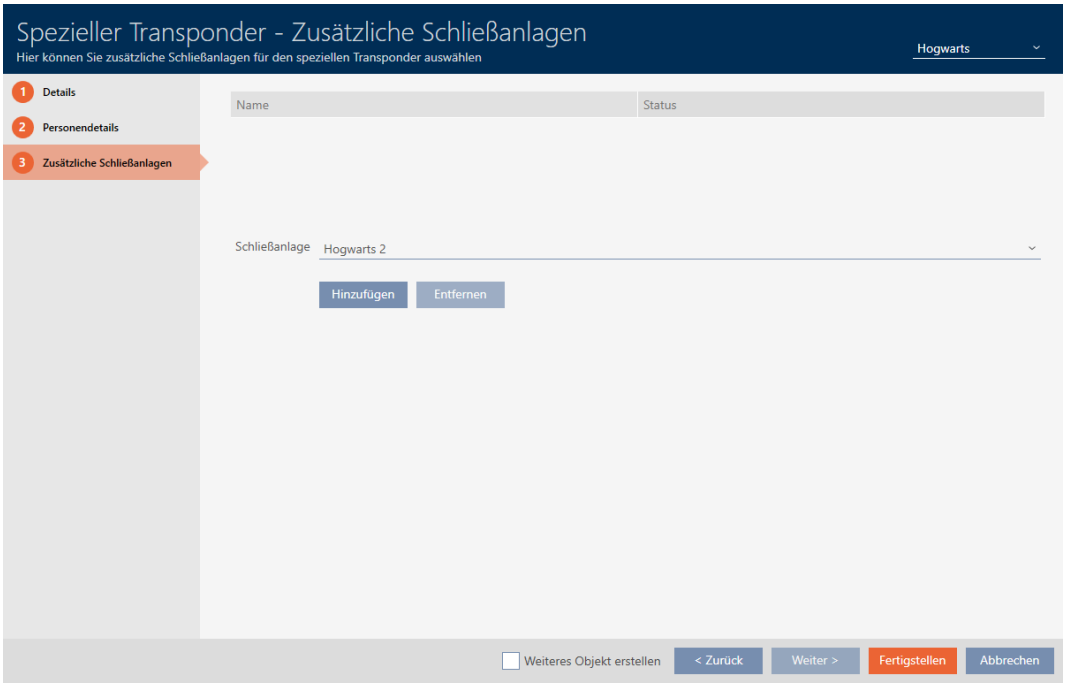
NOTE

Personnel number formula or manual entry

The AXM Lite generates personnel numbers based on the following formula: PN-1, PN-2, PN-X. The abbreviation *PN* can be changed if required (see *Changing automatic numbering [▸ 332]*).

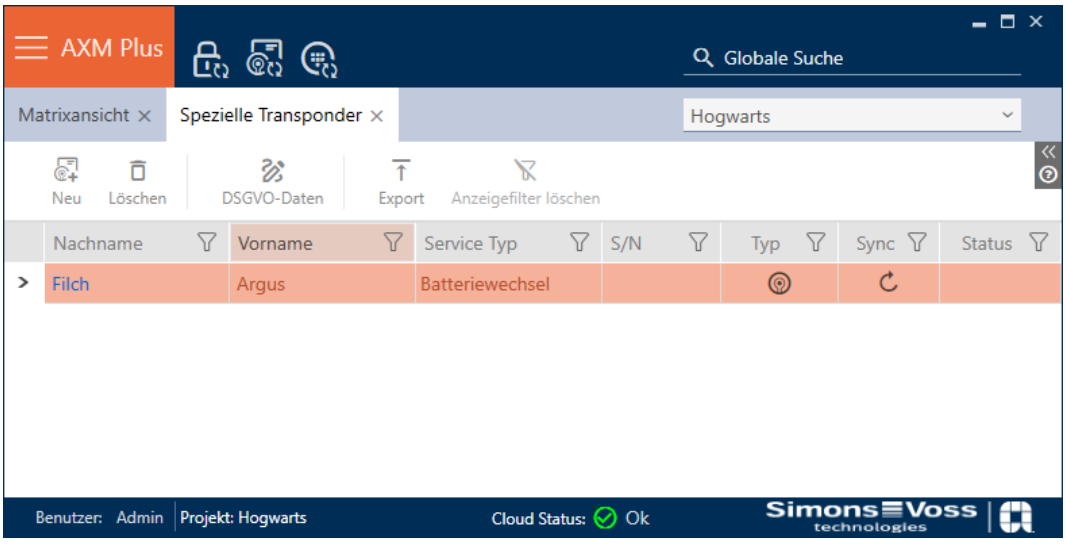
Alternatively, you can enter personnel numbers manually:

1. Activate the ☐ Auto check box.
   ↳ The *Personnel number* field is activated.
2. Enter the personnel number in the *Personnel number* field.



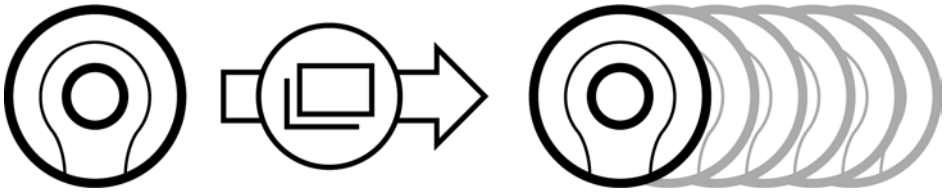
8. If you want to use this special identification medium in other locking systems, use the Add button to add other locking systems.
9. Click on the Finish button.
   ↳ "Special Transponders" window closes.

↳ Newly created identification medium with special function is now listed.



Identification media with special functions are not displayed in the matrix.

15.2 Duplicating an identification medium (including authorisations and settings)



Instead of creating a new identification medium, you can simply duplicate an existing identification medium. During this process, AXM Lite also applies the properties, which can be changed in the AXM Lite.

The following settings are duplicated:

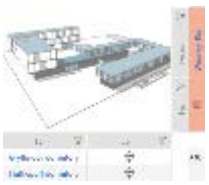
- Time group
- Person details (except for Personnel number. This is continued automatically with the adjustable abbreviation; also see *Changing automatic numbering [▸ 332]*)
- Transponder configuration
- Access levels
- Hashtags

The following settings are not duplicated:

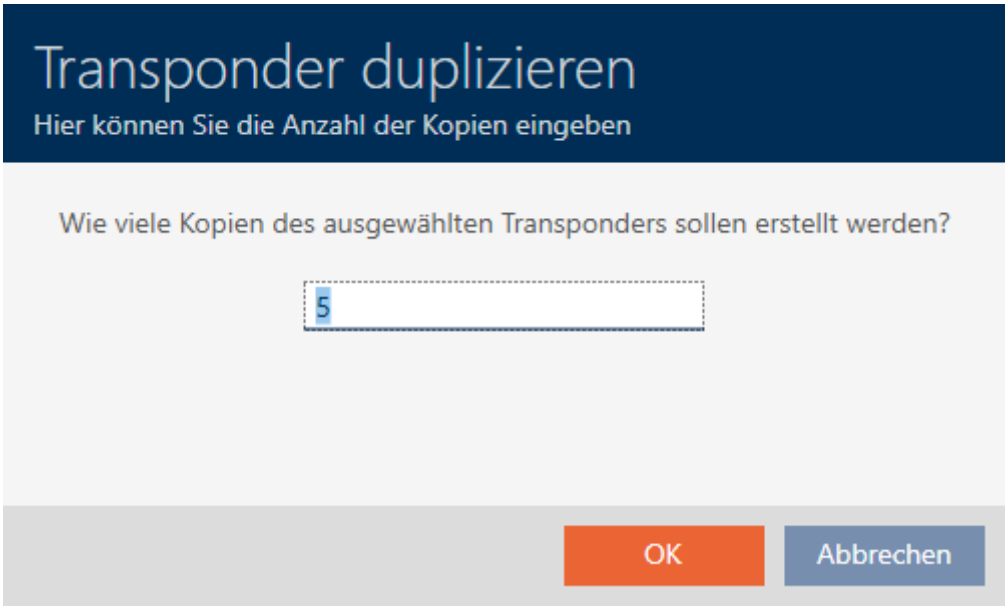
- Entries in the [Actions] tab
- Information that is stored on the hardware and imported during synchronisation:
  - Serial number
  - Firmware version
  - Battery status feedback
  - Personal audit trail

✓ AXM Lite open.
✓ Identification medium available.

1. Select the identification medium to be duplicated.

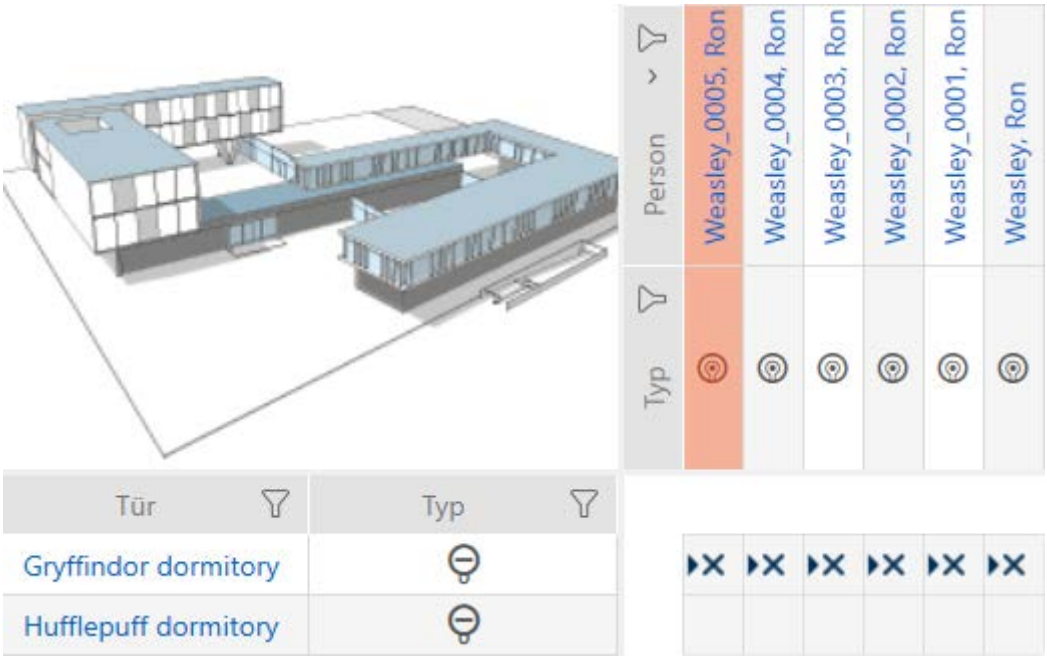


2. Click on the Duplicate button.
   ↳ The window for specifying copies will open.



3. Click on the OK button.

↳ The identification medium is duplicated.



15.3 Deleting an identification medium

15.3.1 Deleting a card/transponder

There are two ways to delete identification media:

1. Delete on the matrix screen (*Deleting individual identification media in the matrix [▸ 95]*)
2. Delete using the tab for identification media (*Deleting multiple identification media using the tab [▸ 96]*)

If you use the tab, you can delete several identification media at the same time.

NOTE

Deleted identification media in locking devices still known/authorised

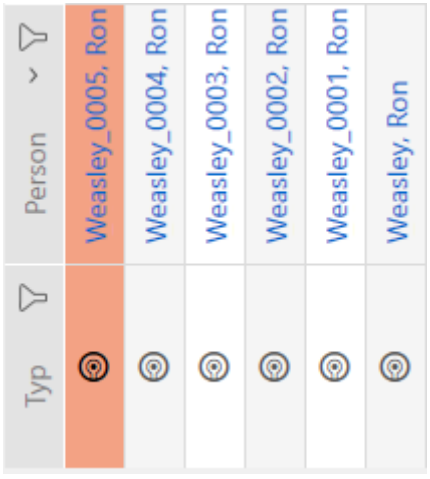
Deleting an identification medium only removes it from the database, but not from the locking devices. The locking devices will still recognise the identification medium (and possibly authorise it) until it is also deleted there (e.g. by synchronising).

- Use suitable measures (e.g. synchronisation) in your system to ensure that the identification medium is no longer recognised, including by locking devices.

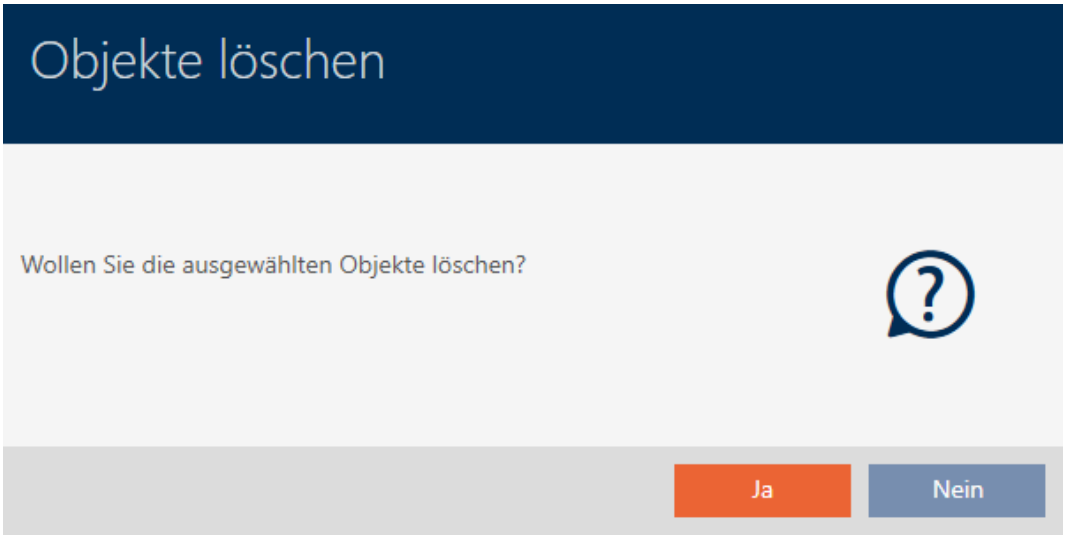
15.3.1.1 Deleting individual identification media in the matrix

✓ AXM Lite open.
✓ Matrix screen open.
✓ The identification medium to be deleted is unprogrammed or reset (see *Resetting cards/transponders [▸ 312]* about resetting).

1. Select the identification medium you wish to delete.

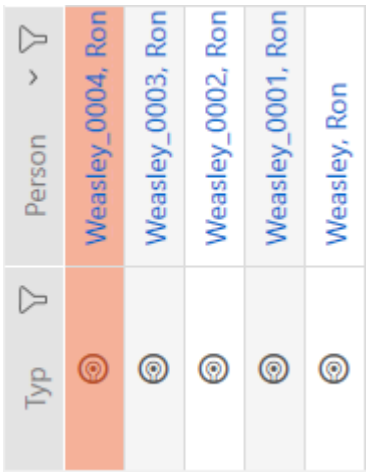


2. Click on the Delete button 🗑.
   ↳ Deletion query will open.



3. Click on the Yes button.
   ↳ Deletion query closes.

↳ Identification medium is deleted.



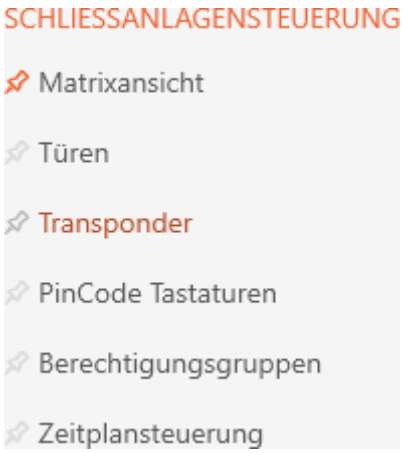
15.3.1.2 Deleting multiple identification media using the tab

✓ AXM Lite open.

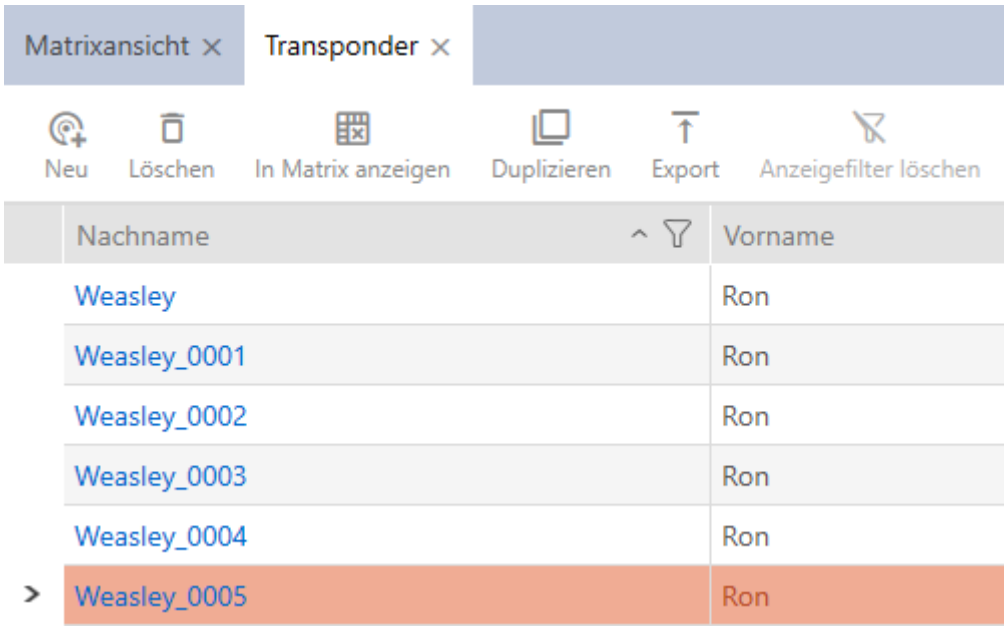
✓ Identification media to be deleted are unprogrammed or reset (see *Resetting cards/transponders [▸ 312]* about resetting).

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

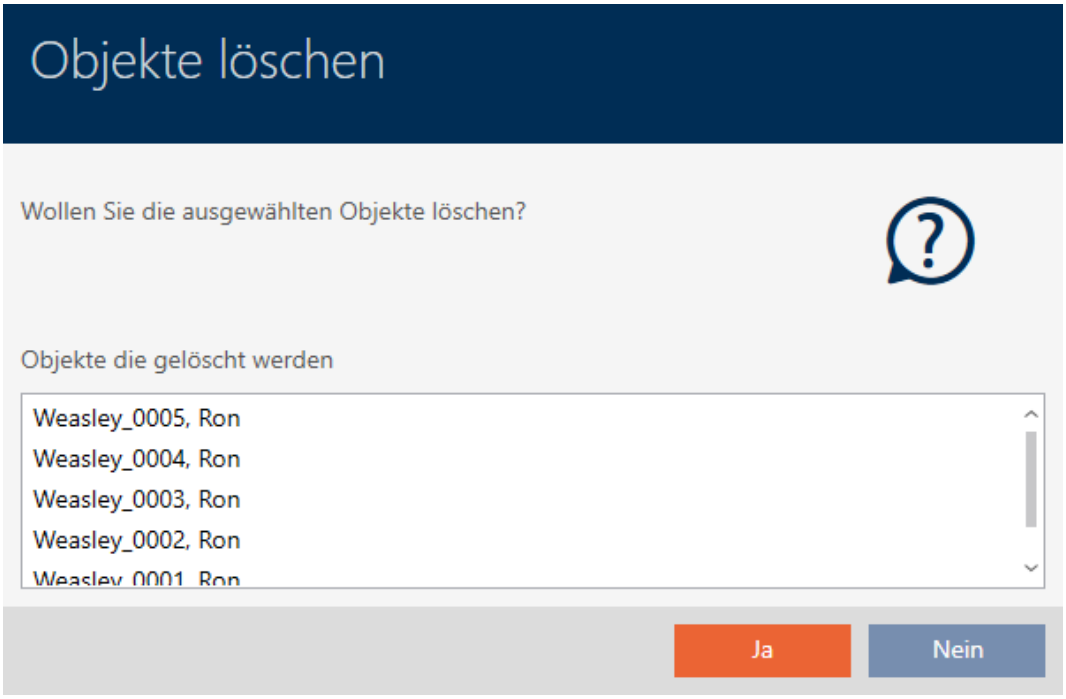
2. Select the Transponder entry in the | LOCKING SYSTEM CONTROL | group.



   ↳ The AXM bar will close.
   ↳ The [Transponder] tab will open.
3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Select all identification media that you wish to delete (Ctrl+click for single media or Shift+click for multiple media).

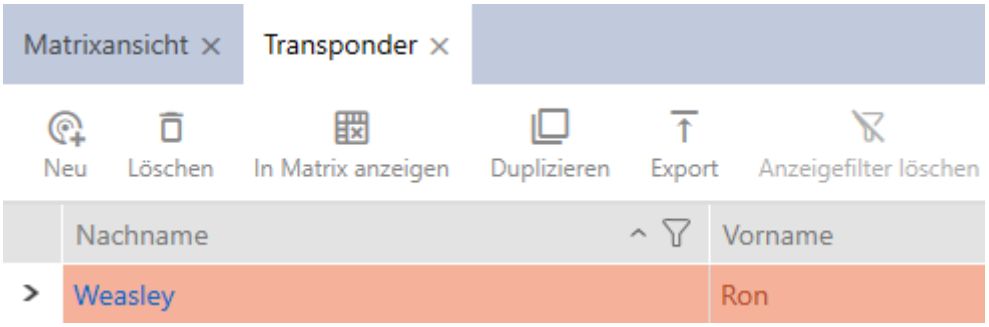


5. Click on the Delete button 🗑.
   ↳ Confirmation dialogue with a list of identification media to be deleted will open.



6. Click on the Yes button.
   ↳ Confirmation dialogue with list of identification media to be deleted closes.

↳ Identification media are now deleted.



NOTE

Deleted identification media in locking devices still known/authorised

Deleting an identification medium only removes it from the database, but not from the locking devices. The locking devices will still recognise the identification medium (and possibly authorise it) until it is also deleted there (e.g. by synchronising).

- Use suitable measures (e.g. synchronisation) in your system to ensure that the identification medium is no longer recognised, including by locking devices.

15.3.2 Deleting a PIN (PIN code keypad AX)

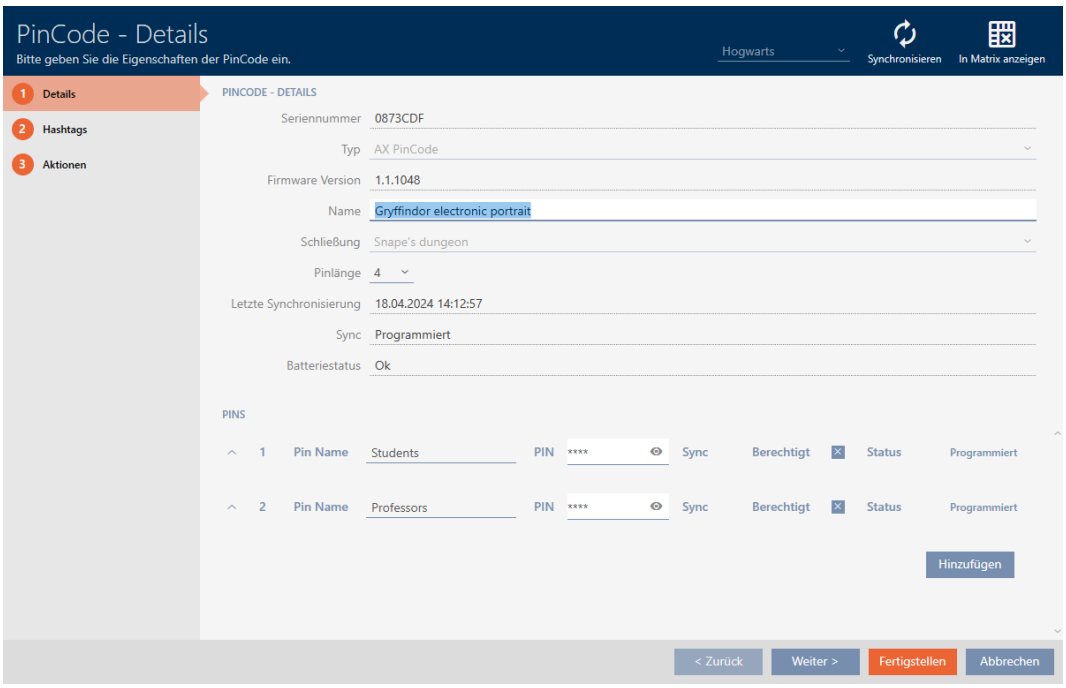
NOTE

Description only valid for PIN code keypad AX

The setting described here is only available for the PIN code keypad AX in yourAXM Lite. On the PIN code keypad 3068, you can use the Master PIN to change this setting directly on the PIN code keypad 3068.

✓ AXM Lite open.
✓ Matrix screen open.
✓ PIN code keypad AX created (see *Creating PIN code keypads [▸ 83]*).

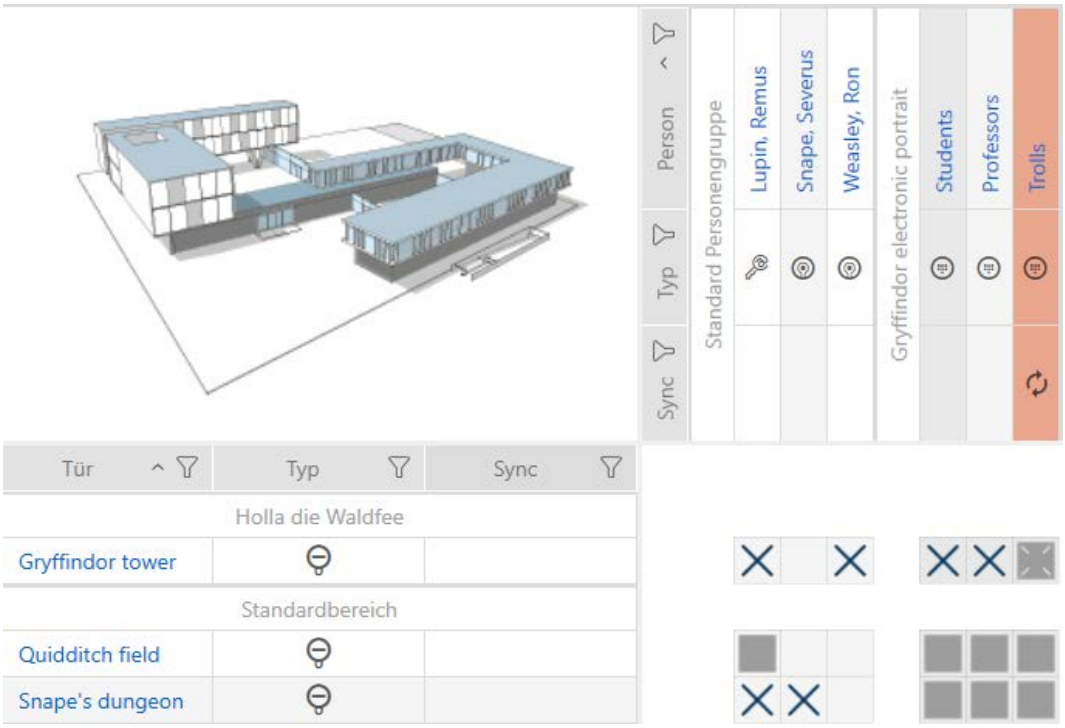
1. Click on any PIN to open details on your PIN code keypad AX.
   ↳ The "PinCode - Details" window will open.



2. Use the ⌄ to expand the settings for the PIN to be deleted.
3. Click on 🗑 to highlight the PIN to be deleted.
   ↳ *Status* field shows *Prepared to delete*.

4. Click on the Finish button.

↳ Deleted PIN is shown with greyed-out authorisation and programming requirement in the matrix.



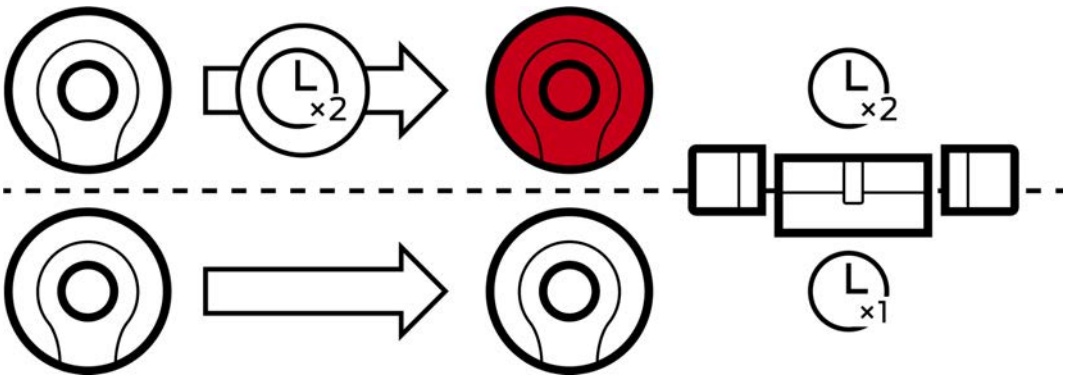
The deleted PIN will disappear after synchronisation.

15.4 Allowing an identification medium to open twice as long

Locking devices normally open for a pre-set interval in pulsed operation.

It is helpful if a locking device remains engaged open for a longer interval after actuation for some people.

The identification medium can therefore inform each locking device that it should engage for twice as long for the identification medium in question.

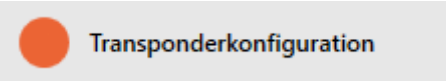


The maximum engagement interval remains 25 s:

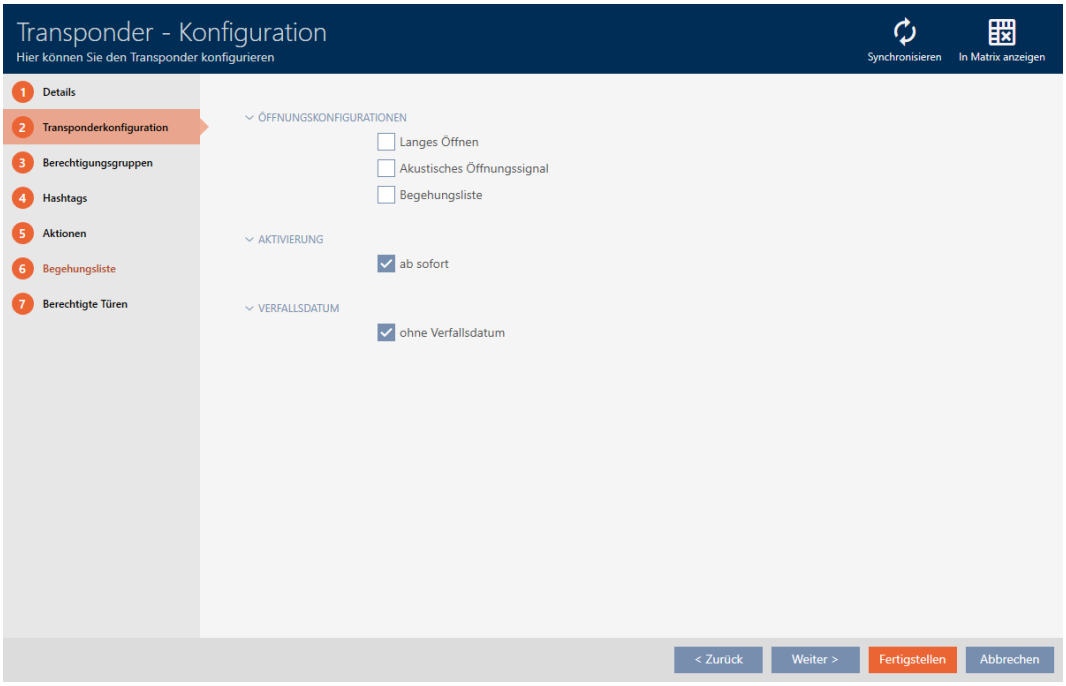
- 5 s changes to 10 s
- 10 s changes to 20 s
- But 20 s changes to 25 s

✓ AXM Lite open.
✓ Identification medium available.

1. Click on the identification medium which needs to open twice as long.
   ↳ The identification medium window will open.
2. Click on the Transponder configuration tab.



   ↳ Window switches to the "Transponder configuration" tab.



3. Activate the Long opening checkbox.
4. Click on the Finish button.
   ↳ The identification medium window closes.

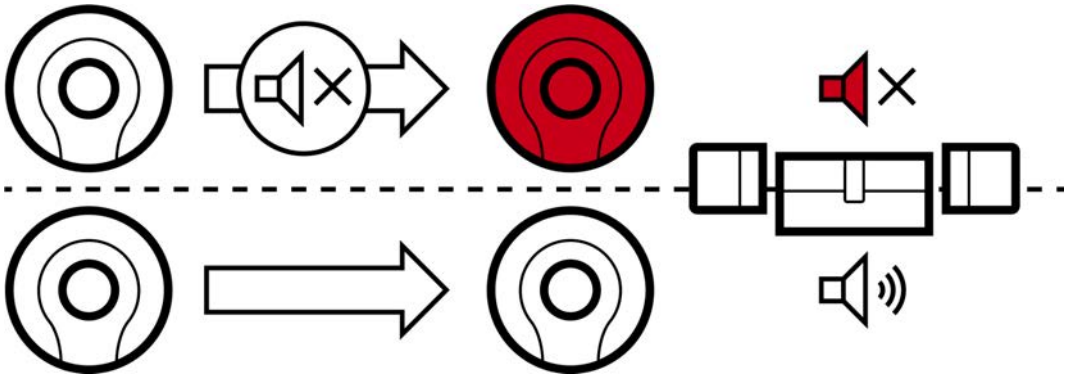
↳ All locking devices will now open twice as long for this identification medium.

15.5 Muting all locking devices for an identification medium

Locking devices normally emit a beep when an identification medium is used to engage the locking device.

This audible opening signal is not wanted in some situations. Example: A nurse should be able to enter a hospital room at night without waking the patient up with an audible opening signal.

The audible opening signal can therefore also be switched off for individual identification media. This setting is for the identification medium only.



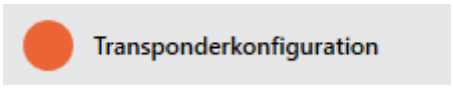
This means

- identification media for which ☐ Acoustic opening signal is deactivated will open all locking devices without emitting a beep.
- Other identification media will continue to open all locking devices with a beep sound as usual.

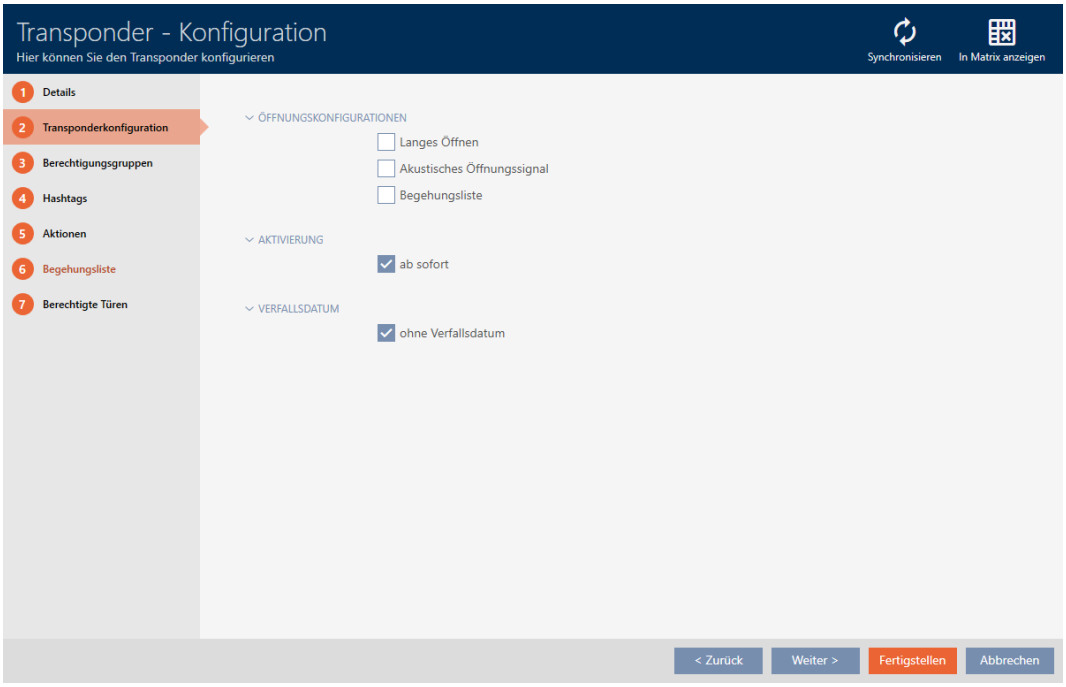
15.5.1 Muting all locking devices for a transponder or a card

✓ AXM Lite open.
✓ Identification medium available.

1. Click on the identification medium you wish to mute.
   ↳ The identification medium window will open.
2. Click on the Transponder configuration tab.



↳ Window switches to the "Transponder configuration" tab.



3. Activate the ☐ Acoustic opening signal checkbox.
4. Click on the Finish button.
   ↳ The identification medium window closes.

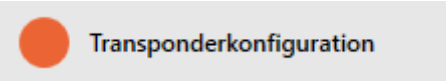
↳ All locking devices are now muted for this identification medium.

15.6 Allow accesses to be recorded by identification media (physical access list)

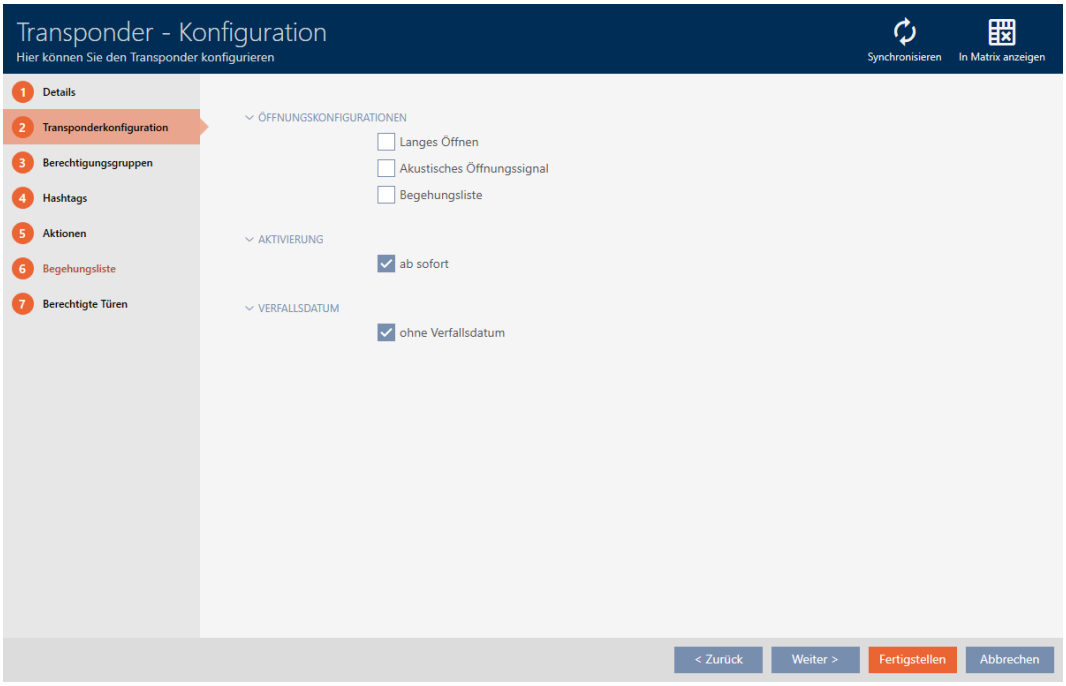
This is where you can switch on the physical access list. This means that your identification medium logs which locking devices it has activated (also see *Access and physical access lists [▸ 365]*).

✓ AXM Lite open.
✓ Identification medium available.

1. Click on the identification medium whose physical access list you wish to activate.
   ↳ The identification medium window will open.
2. Click on the Transponder configuration tab.



   ↳ Window switches to the "Transponder configuration" tab.



3. Activate the ☑ Personal audit trail checkbox.

4. Click on the Finish button.
   ↳ The identification medium window closes.

↳ Identification medium will now write which locking devices it has activated in the physical access list.

15.7 Restricting identification medium authorisations to specific times (time group)

You control an identification medium's authorisations with a time group. The time group is a time management component (see *Event management [▸ 366]*). See *Create time group [▸ 49]* and *Adding identification medium to time group [▸ 275]* to set up time management for identification media.

15.8 Activating or deactivating identification medium once at specific times (activation and expiry date)

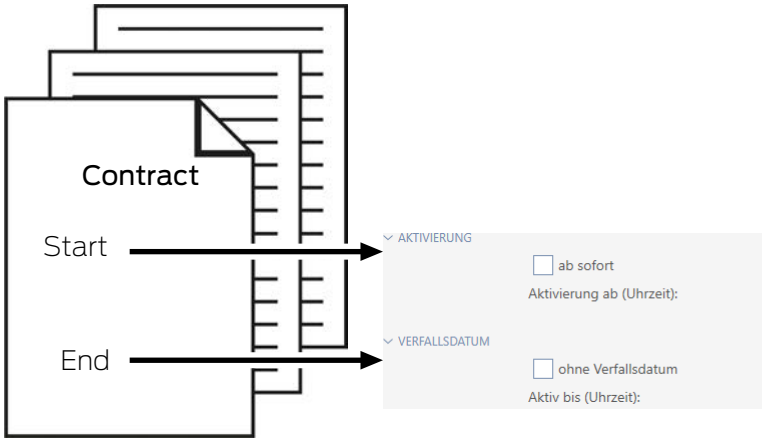
Your AXM Lite recognises two points in time for identification media:

- Activation date
- Expiry date

These dates are suitable if identification media are only to be used from a certain point in time and/or until a certain point in time. Alternatively, you can, of course, simply issue authorisations on the activation date and revoke them again on the expiry date. The key difference is that you will then need to synchronise all locking devices or identification media at these points in time.

You can save yourself the effort if you use an activation or expiry date. The identification medium will be automatically accepted on authorised locking devices at a certain point in time (activation date) or no longer accepted at a certain point in time (expiry date).

This function is suitable for temporary employment contracts, for example:



1. Conveniently synchronise the identification medium in advance.

2. Set the activation date to the start of the employment contract and the expiry date to the end of the employment contract.

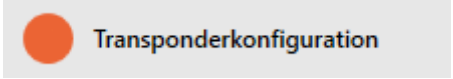
Both dates are normally set for the future. If you change these dates for an existing identification medium:

- Activation date in the past: identification medium is immediately active the next time it is synchronised.
- Expiry date in the past: identification medium is immediately deactivated the next time it is synchronised.

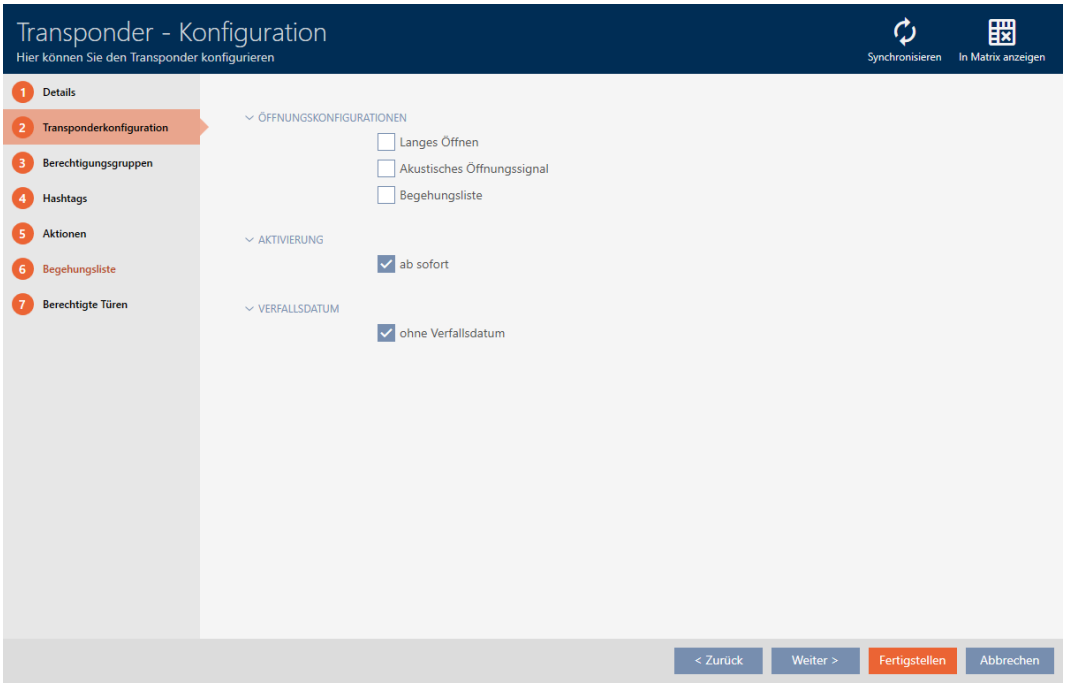
In this case, the AXM displays a warning, e.g.:

✓ AXM Lite open.
✓ Identification medium available.

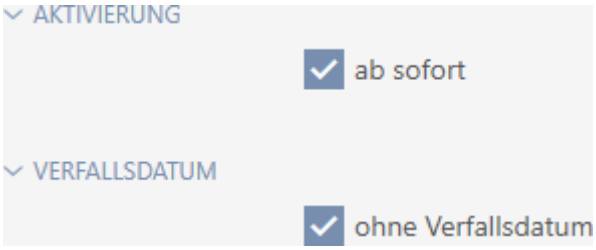
1. Click on the identification medium whose activation or expiry date you wish to set.
   ↳ The identification medium window will open.
2. Click on the Transponder configuration tab.



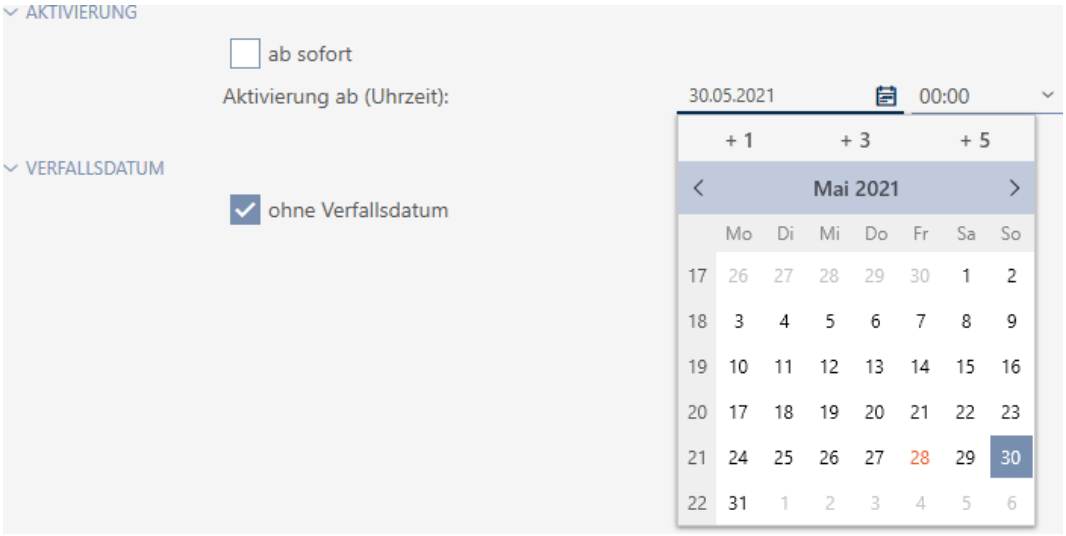
   ↳ Window switches to the "Transponder configuration" tab.



3. Open the "Activation" and "Expiry date" menus if necessary.



4. If you wish to set an activation date: Activate the ☐ from now check-box.
5. Set the activation date in the ▼ **Activation from (time):** drop-down menu or click on the icon to expand a calendar mask.



6. If you wish to set an expiration date: Activate the ☐ without expiry date checkbox.
7. Use the ▼ **Active until (time):** drop-down menu to set the expiration date or click on the icon to expand a calendar screen.

8. Click on the Finish button.
   ↳ The identification medium window closes.

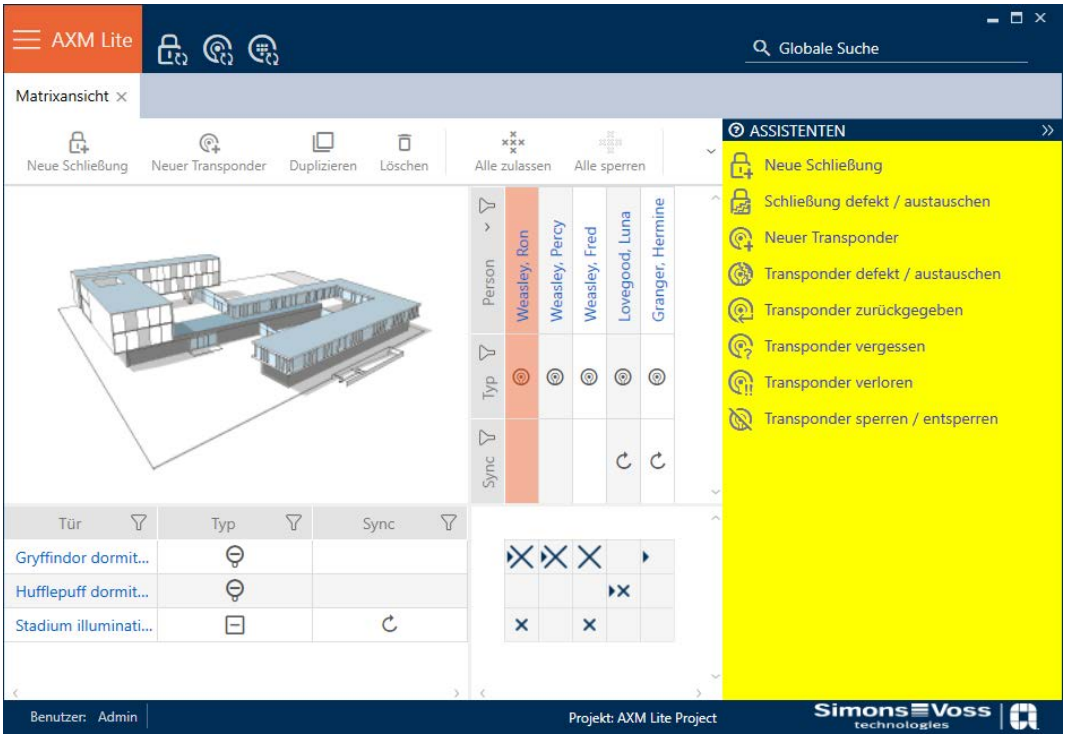
↳ Identification medium will become active or inactive at the specified times.

15.9 Handling defective identification media

Identification media can suffer from defects:

- Software defect
- Hardware defect

As a basic rule, all actions can be performed using the wizard section on the right-hand side:



If the identification medium has been lost or stolen, you must block it (see *Blocking and replacing lost/stolen card/transponder permanently [▸ 146]*).

The following overview will help you to decide on the correct course of action. It is helpful if you know how identification media and TID are linked (see *Identification media, locking devices and the locking plan [▸ 360]*).

Transponders/replacement transponders are required again immediately:

Suitable for:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
Identification media with undefined software status.	■ Identification media with external damage (e.g. scratched). ■ Identification media which needs to be replaced as a precaution (e.g. wet).	Identification media with permanent damage (e.g. burnt) for which a replacement is required.

Example situation:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
	Employee's transponder has fallen into the pool. Consequence: transponder works but at risk of failure due to exposure to water.	Employee's transponder has fallen into a camp fire. Consequence: transponder melted and permanently damaged.

Procedure:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
Repairing a card/transponder (resynchronising) [▸ 111] 1. Reset (= TID available in database again) 2. Resynchronise (= TID is immediately written back onto the same identification medium) The identification medium functions as before after it is repaired.	*Resetting and replacing a card/transponder [▸ 116]* 1. Reset (= TID flagged as defective in database and removed from original identification medium) 2. Synchronise replacement identification medium with new TID After the reset, the TID is no longer contained in the identification medium. The identification medium can therefore no longer be used. However, it can be re-synchronised. A new TID is written onto the identification medium.	*Deleting and replacing a card/transponder [▸ 119]* 1. Delete (= TID flagged as defective in database) and removed from project 2. Synchronise replacement identification medium with the new TID It is obviously not possible to reset a permanently damaged identification medium because it is no longer accessible. This means the TID remains in the identification medium. Deleting allows you to "clean up" your project. The TID marked as "defective" will remain permanently stored in the database regardless and will not be reassigned. You can also hide defective or disabled identification media as an alternative to deletion (see *Hiding deactivated and defective identification media [▸ 324]*).

Transponder/replacement transponder is not required:

Suitable for:

Taking out of use and leaving in project	Taking out of use and deleting from project
Permanently damaged identification media (e.g. burnt) for which no replacement is required (e.g. employee left company)	Permanently damaged identification media (e.g. burnt) for which no replacement is required (e.g. employee left company)

Example situation:

Taking out of use and leaving in project	Taking out of use and deleting from project
The employee's transponder fell into camp fire at the employees' farewell party. Consequence: transponder melted and permanently damaged; employee no longer on staff.	The employee's transponder fell into camp fire at the employees' farewell party. Consequence: transponder melted and permanently damaged; employee no longer on staff.

Procedure:

Taking out of use and leaving in project	Taking out of use and deleting from project
Take card/transponder out of use and leave in project [▸ 127] 1. Flag as taken out of operation (= TID flagged as defective in database) The permanently damaged identification medium retains its TID but the TID is flagged as "defective". New identification media cannot be created with this TID. This means that the same TID cannot brought into circulation twice.	*Taking a card/transponder out of use and deleting it from project [▸ 134]* 1. Delete (= TID flagged as defective in database) and removed from project Deleting allows you to "clean up" your project. The TID marked as "defective" will remain permanently stored in the database regardless and will not be reassigned. You can also hide defective or disabled identification media as an alternative to deletion (see *Hiding deactivated and defective identification media [▸ 324]*).

Handling a defective PIN code keypad

As with transponders and cards, you also have various options in the event of a defective PIN code keypad:

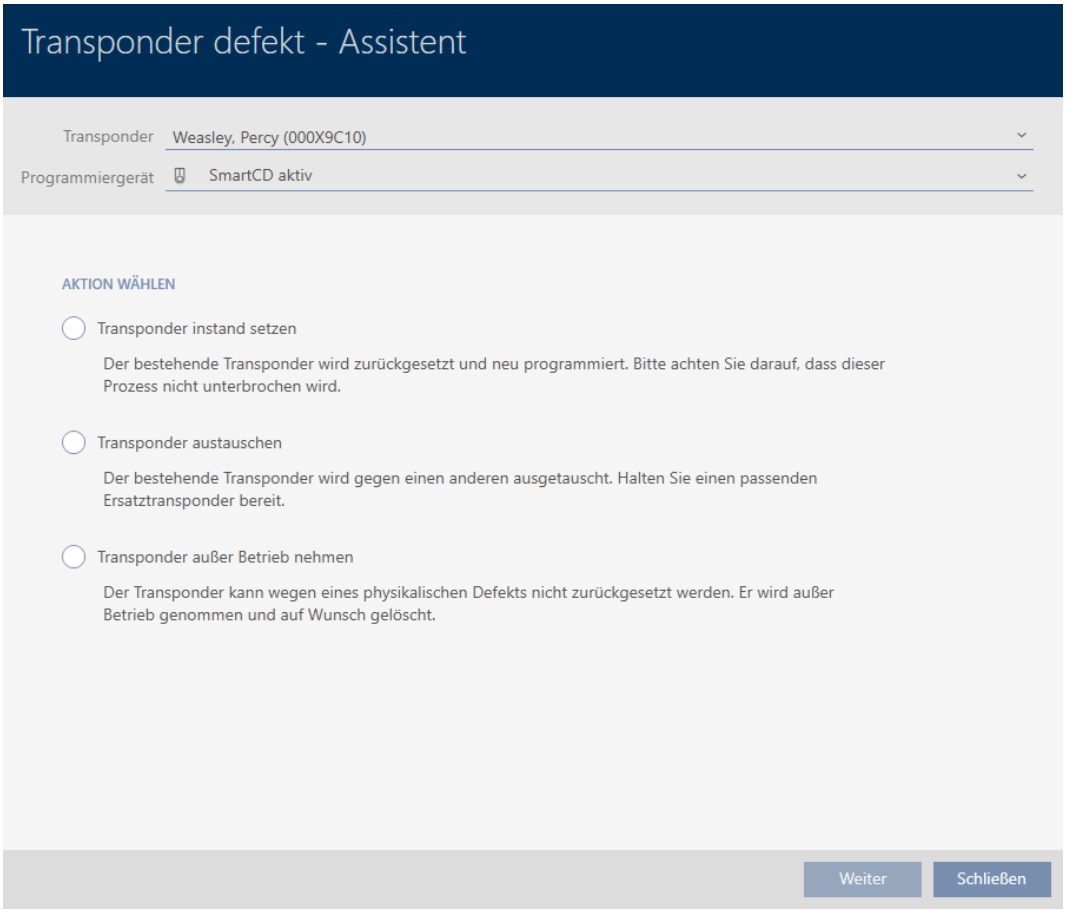
- Repair PinCode (see *Repairing a PIN code keypad (resynchronising) [▸ 112]*)
- Reset and PinCode (manual; not via wizard - see *Resetting and replacing a PIN code keypad [▸ 119]*)
- Delete and PinCode (see *Deleting and replacing a PIN code keypad [▸ 122]*)
- Decommission PinCode and leave in the project (see *Taking a PIN code keypad out of use and leaving it in project [▸ 130]*)
- Decommission PinCode and remove from project (see *Taking a PIN code keypad out of use and deleting it from project [▸ 136]*)

15.9.1 Repairing/resynchronising

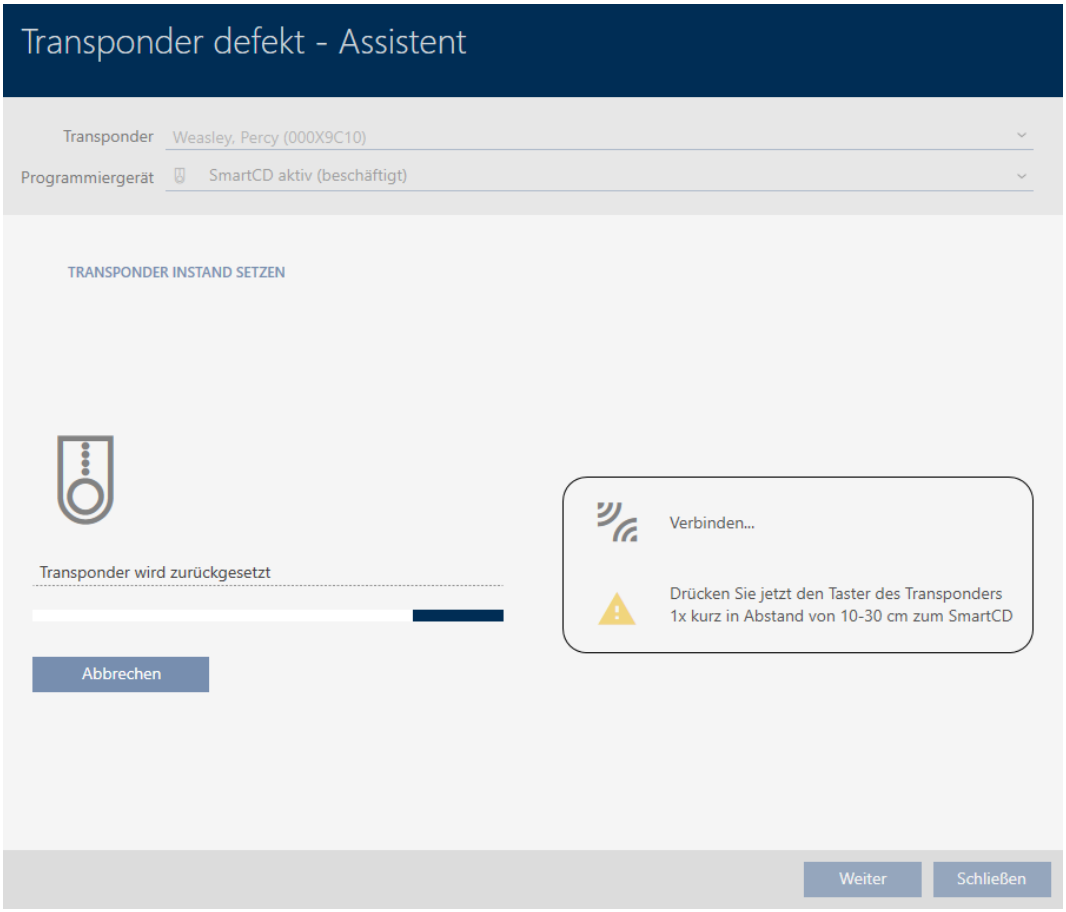
15.9.1.1 Repairing a card/transponder (resynchronising)

- ✓ AXM Lite open.
- ✓ Identification media list or matrix open.
- ✓ Identification medium at hand.
- ✓ Suitable programming device connected.

1. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag the defective identification medium.
3. Click the Transponder defective / replace button in the "Wizards" section.
   ↳ Wizard for handling a defective identification medium will open.

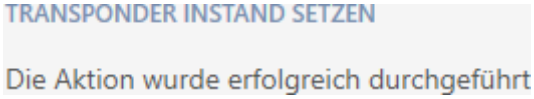


4. Select the option Repair transponder.
5. Click on the Next button.
   ↳ Identification medium is being reset.



↳ Identification medium is synchronised.

↳ Identification medium has been resynchronised with the same settings.



15.9.1.2 Repairing a PIN code keypad (resynchronising)

✓ AXM Lite open.

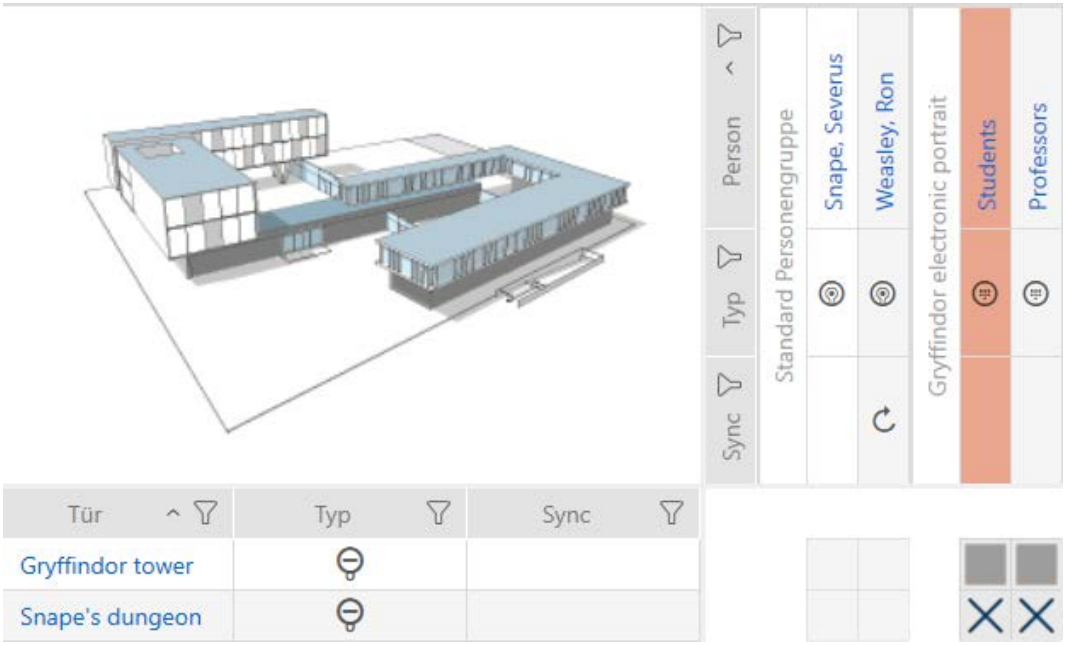
✓ List with PIN code keypads or matrix open.

✓ PIN code keypad at hand.

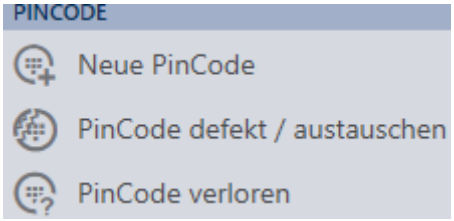
✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

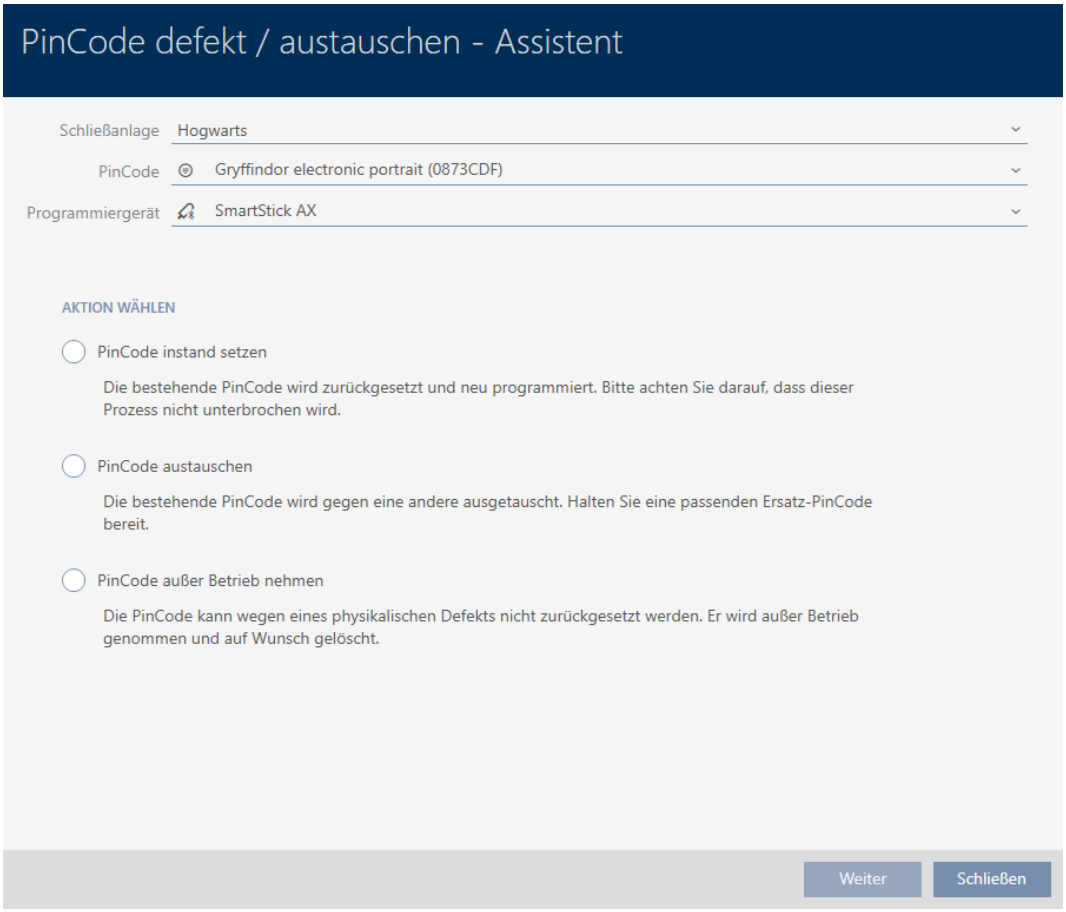
2. Flag a PIN associated with the defective PIN code keypad.



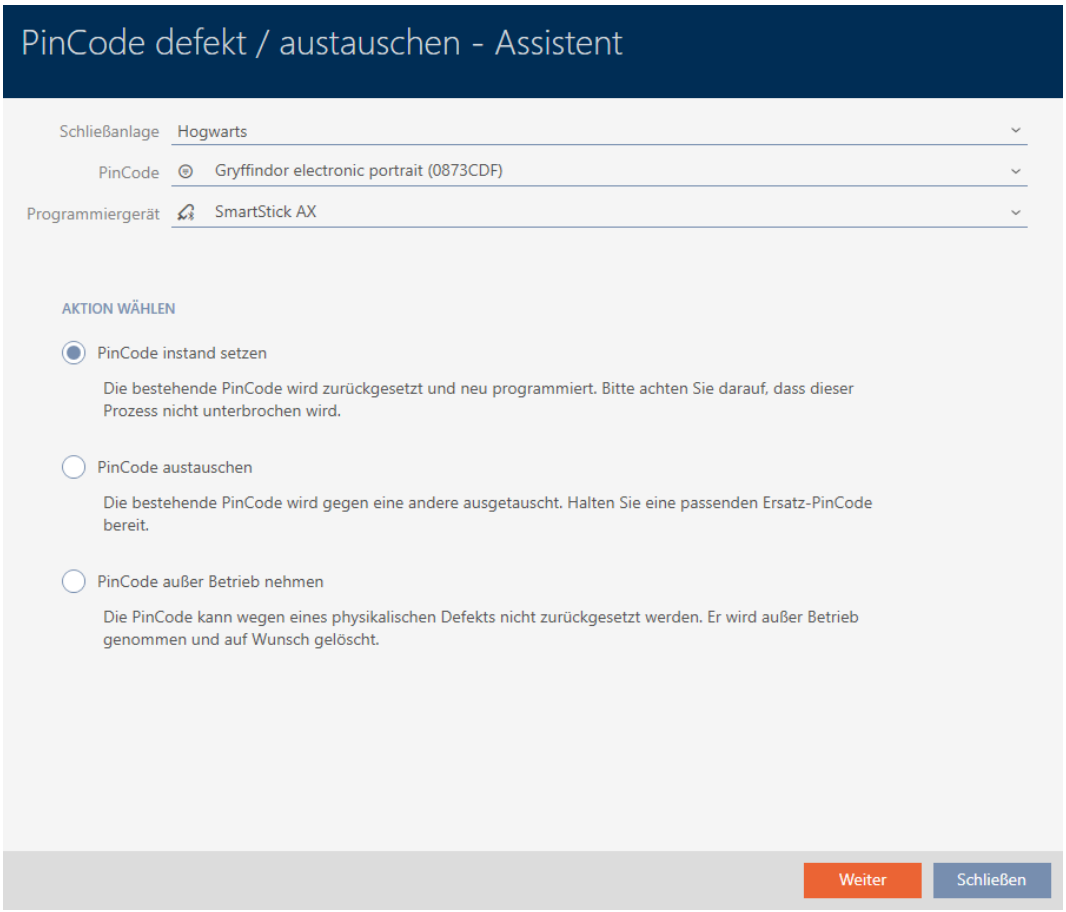
3. Click the PinCode defective / replace button in the "Wizards" section.



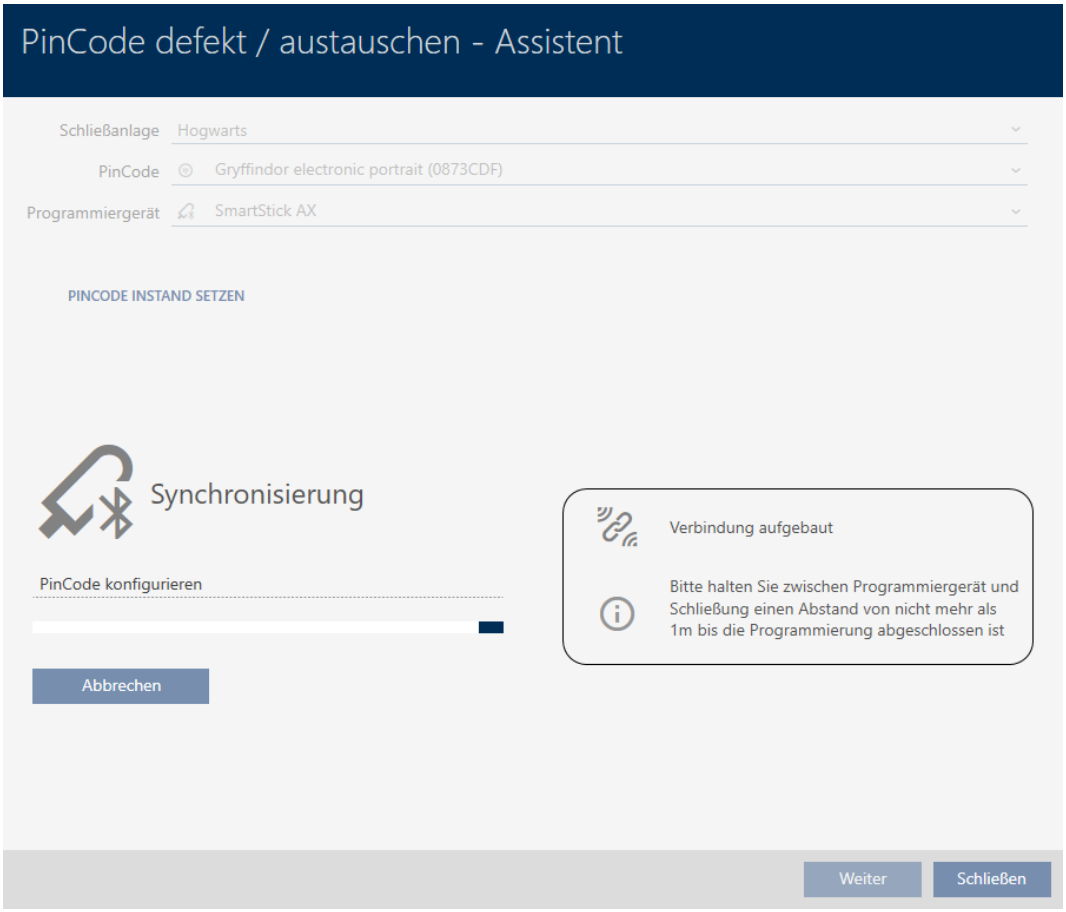
↳ Wizard to help with a faulty PIN code keypad will open.


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

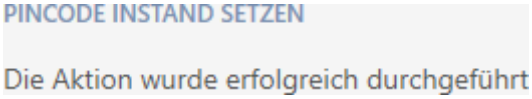
4. Select the option ◉ Repair PinCode.



5. Click on the Next button.
   ↳ PIN code keypad is reset.



6. Follow the instructions.
↳ PIN code keypad has been resynchronised with the same settings.

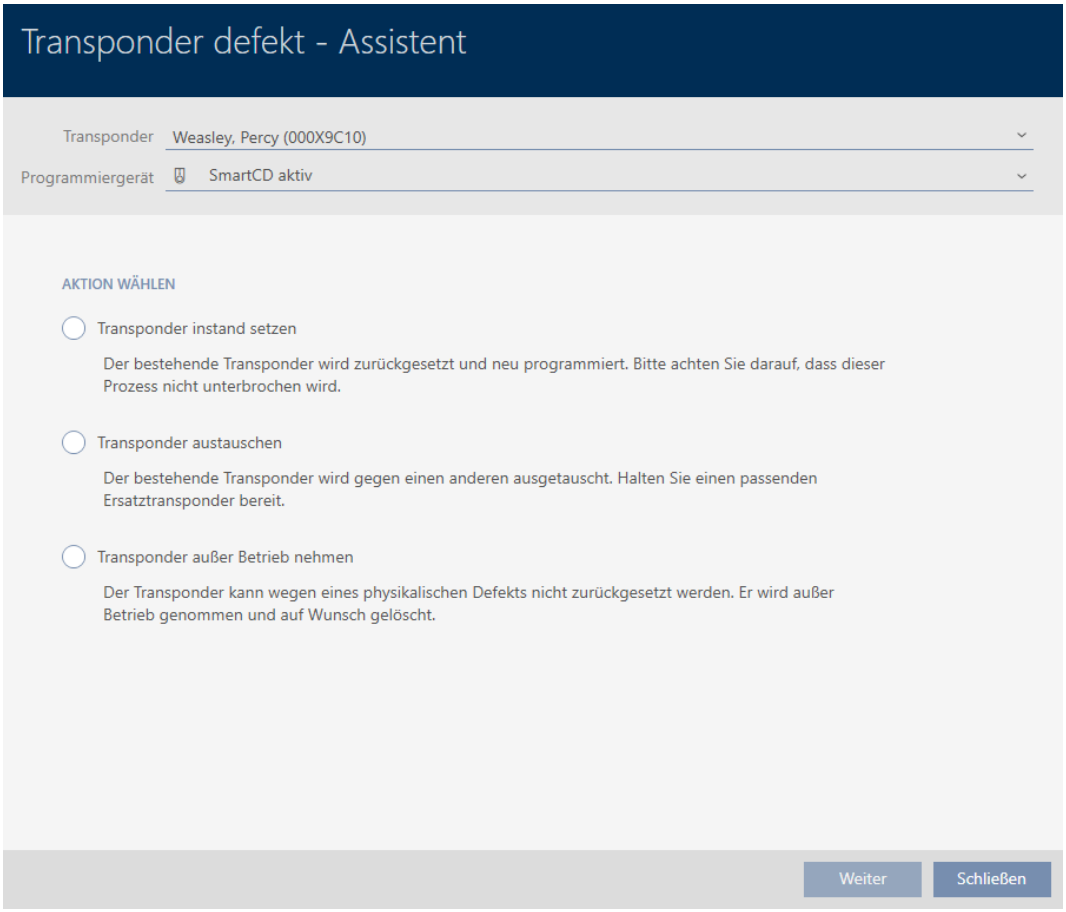


15.9.2 Resetting and replacing

15.9.2.1 Resetting and replacing a card/transponder

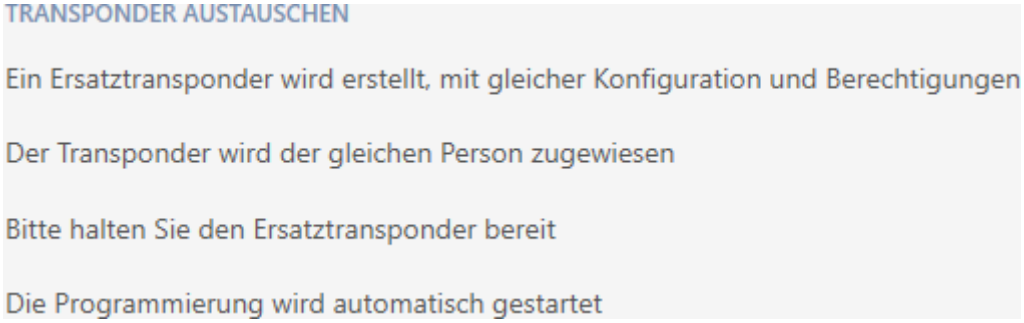
✓ AXM Lite open.
✓ Identification media list or matrix open.
✓ Identification medium at hand.
✓ Replacement identification medium at hand.
✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag the defective identification medium.
3. Click the Transponder defective / replace button in the "Wizards" section.
↳ Wizard for handling a defective identification medium will open.

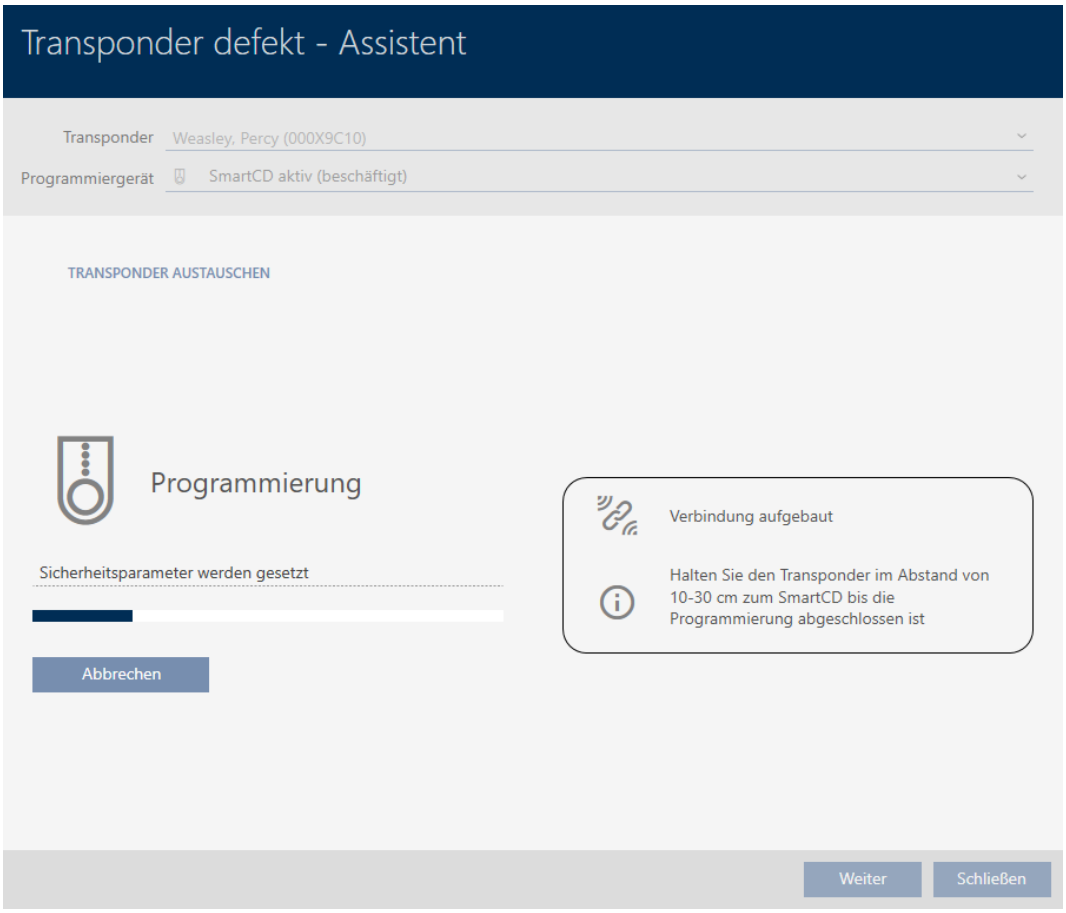


4. Select the option ◉ Replace transponder.
5. Click on the Next button.
   ↳ Reset query will open.

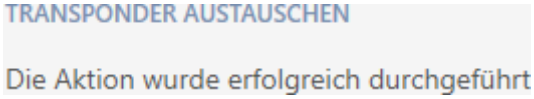
6. Click on the Yes button.
   ↳ Reset query will close.
   ↳ Identification medium is being reset.
   ↳ Wizard prepares programming for the replacement identification medium.



7. Click on the Next button.
   ↳ Replacement identification medium is being programmed.



↳ Replacement identification medium is now synchronised.



15.9.2.2 Resetting and replacing a PIN code keypad

There is no wizard for this procedure. Proceed as follows instead:

- ✓ AXM Lite open.
- ✓ List with PIN code keypads or matrix open.
- ✓ PIN code keypad at hand.
- ✓ Suitable programming device connected.
- ✓ Replacement PIN code keypad at hand.

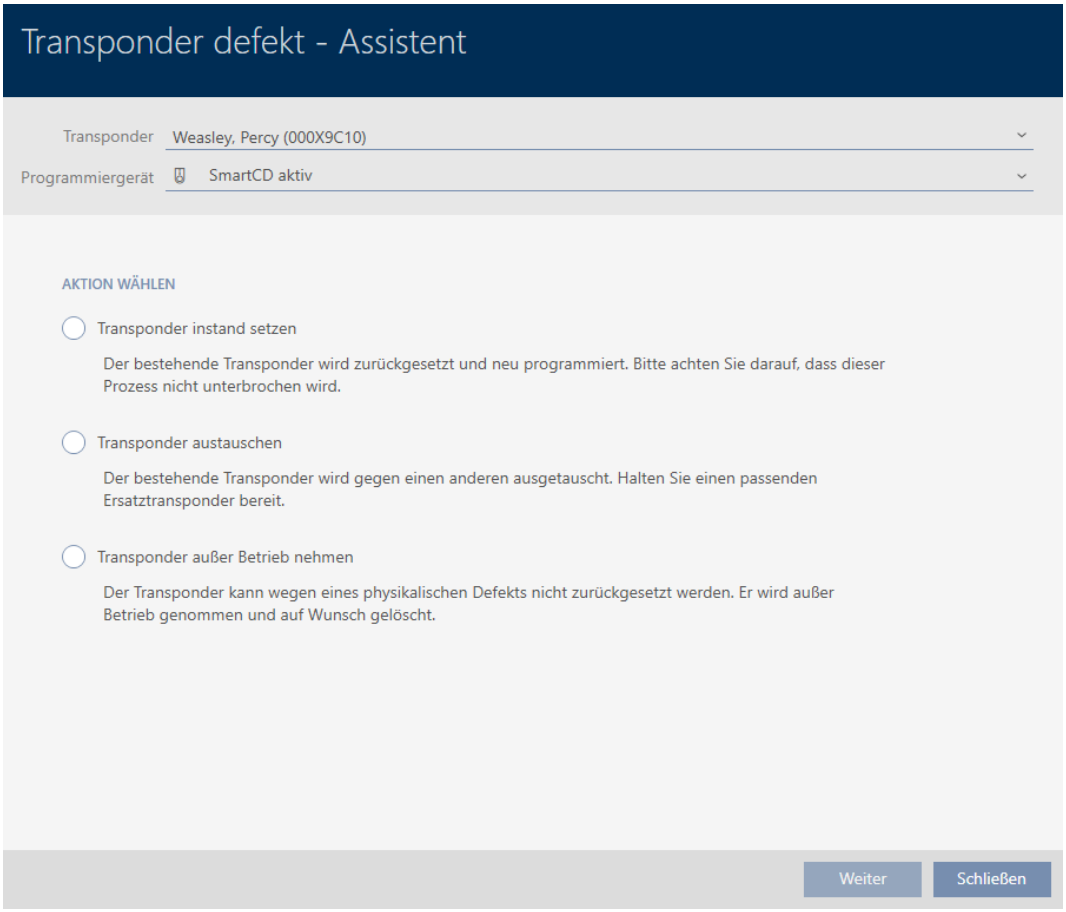
1. Reset the defective PIN code keypad (see *Resetting cards/transponders [▸ 312]*).
2. Create a new PIN code keypad (see *Creating PIN code keypads [▸ 83]*).
3. Synchronise the new PIN code keypad (see Synchronising a PIN code keypad).

15.9.3 Delete and replace

15.9.3.1 Deleting and replacing a card/transponder

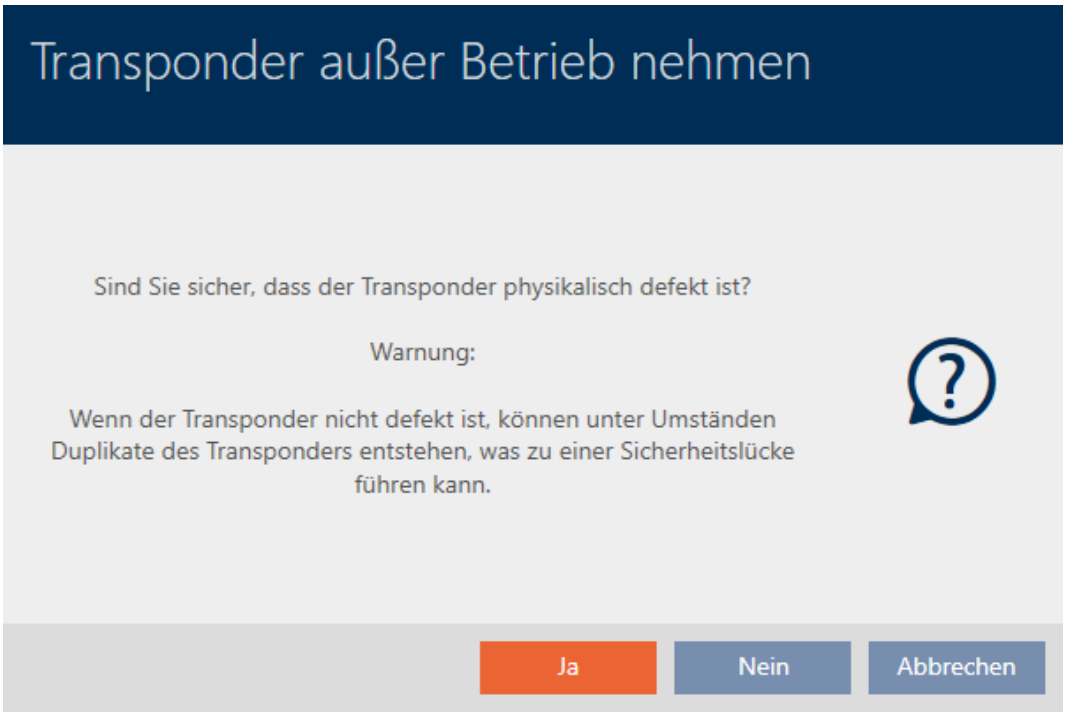
- ✓ AXM Lite open.
- ✓ Identification media list or matrix open.
- ✓ Identification medium at hand.
- ✓ Replacement identification medium at hand.
- ✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag the defective identification medium.
3. Click the Transponder defective / replace button in the "Wizards" section.
   ↳ Wizard for handling a defective identification medium will open.

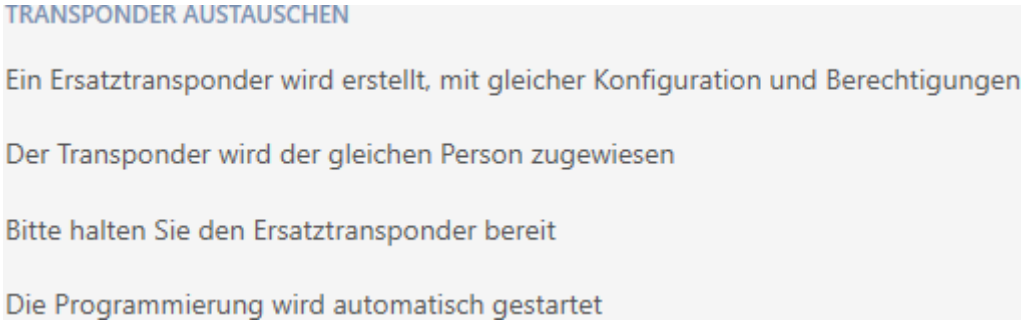


4. Select the option ◉ Replace transponder.
5. Click on the Next button.
   ↳ Reset query will open.

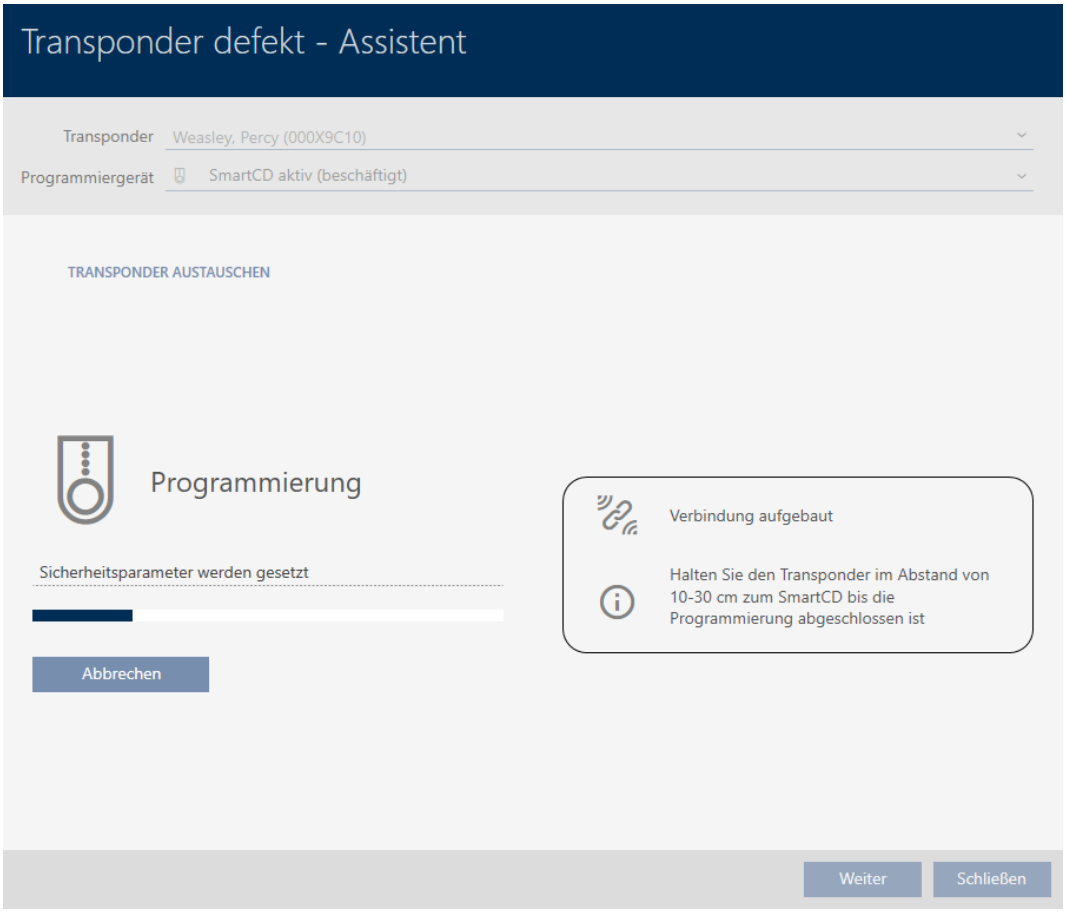
6. Click on the No button.
   ↳ Reset query will close.
   ↳ Message on checking the defect will open.



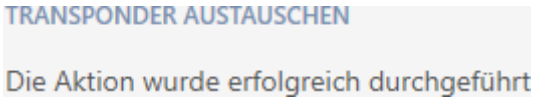
7. Click on the Yes button.
   ↳ Message on checking the defect closes.
   ↳ Wizard prepares programming for the replacement identification medium.



8. Click on the Next button.
   ↳ Replacement identification medium is synchronised.



↳ Replacement identification medium is now synchronised.



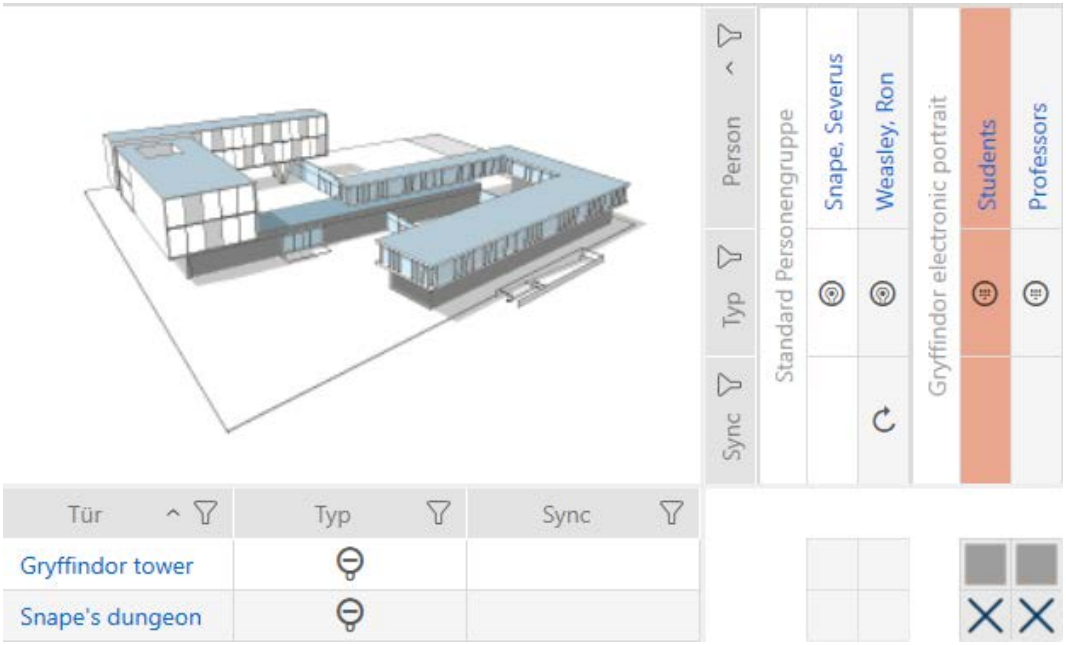
You can now reset the identification medium (see *Deleting an identification medium [▸ 94]*).

15.9.3.2 Deleting and replacing a PIN code keypad

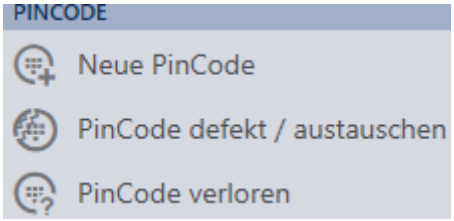
✓ AXM Lite open.
✓ List with PIN code keypads or matrix open.
✓ Replacement PIN code keypad at hand.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

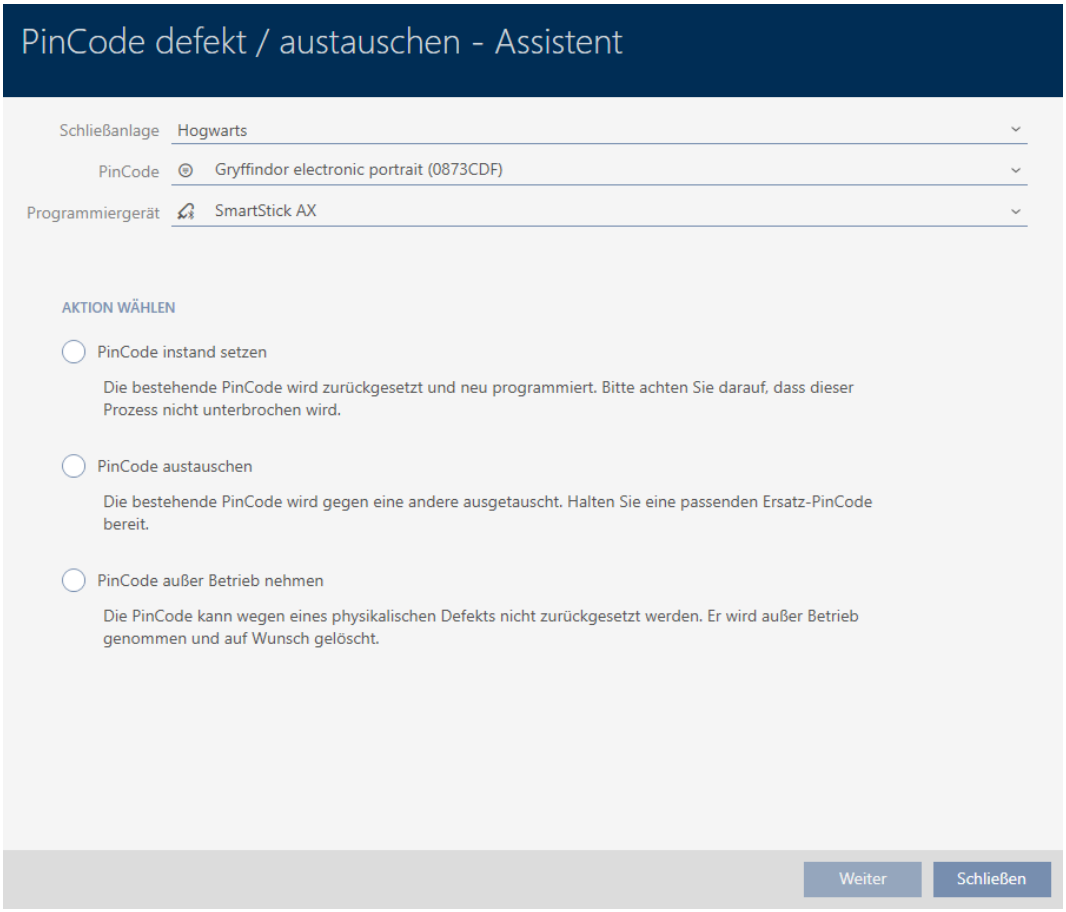
2. Flag a PIN associated with the defective PIN code keypad.



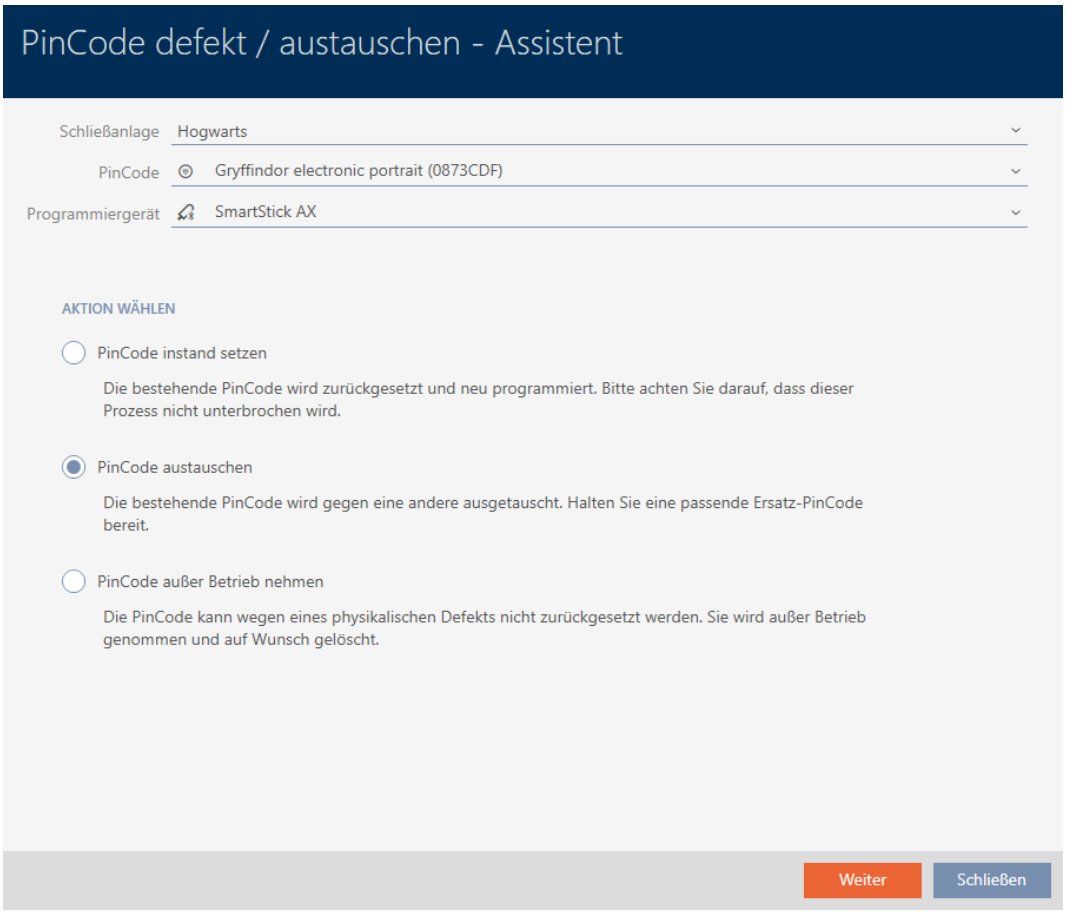
3. Click the PinCode defective / replace button in the "Wizards" section.



↳ Wizard to help with a faulty PIN code keypad will open.

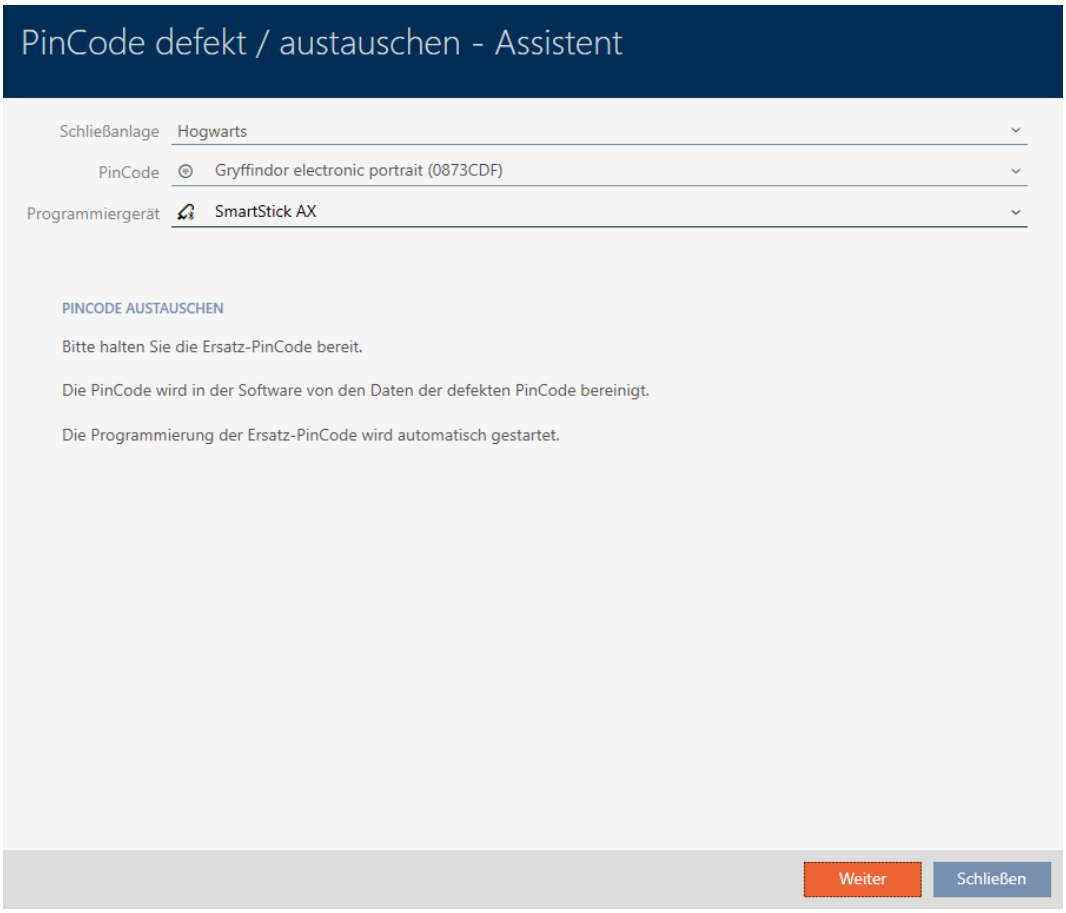

PinCode defekt / austauschen - Assistent
Schließanlage
Hogwarts
PinCode
Gryffindor electronic portrait (0873CDF)
Programmiergerät
SmartStick AX
AKTION WÄHLEN
PinCode instand setzen
Die bestehende PinCode wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen 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. Select the option ◉ PinCode.

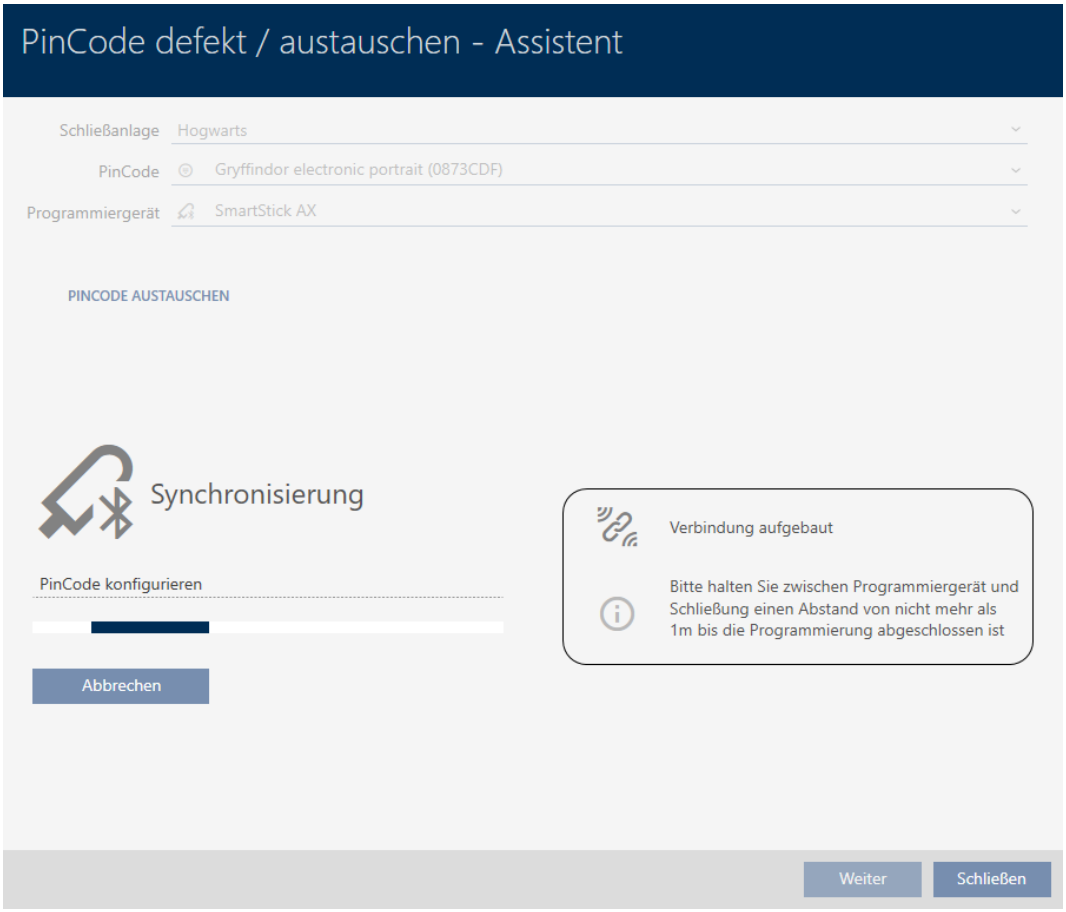


5. Click on the Next button.
   ↳ Confirmation dialogue will open.

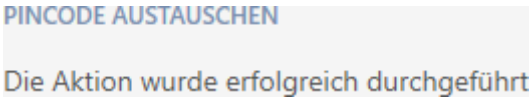
6. Click on the Yes button.
   ↳ Synchronisation of the replacement PIN code keypad is being prepared.



7. Click on the Next button.
   ↳ The replacement PIN code keypad is now synchronised.



↳ The PIN code keypad has been replaced.



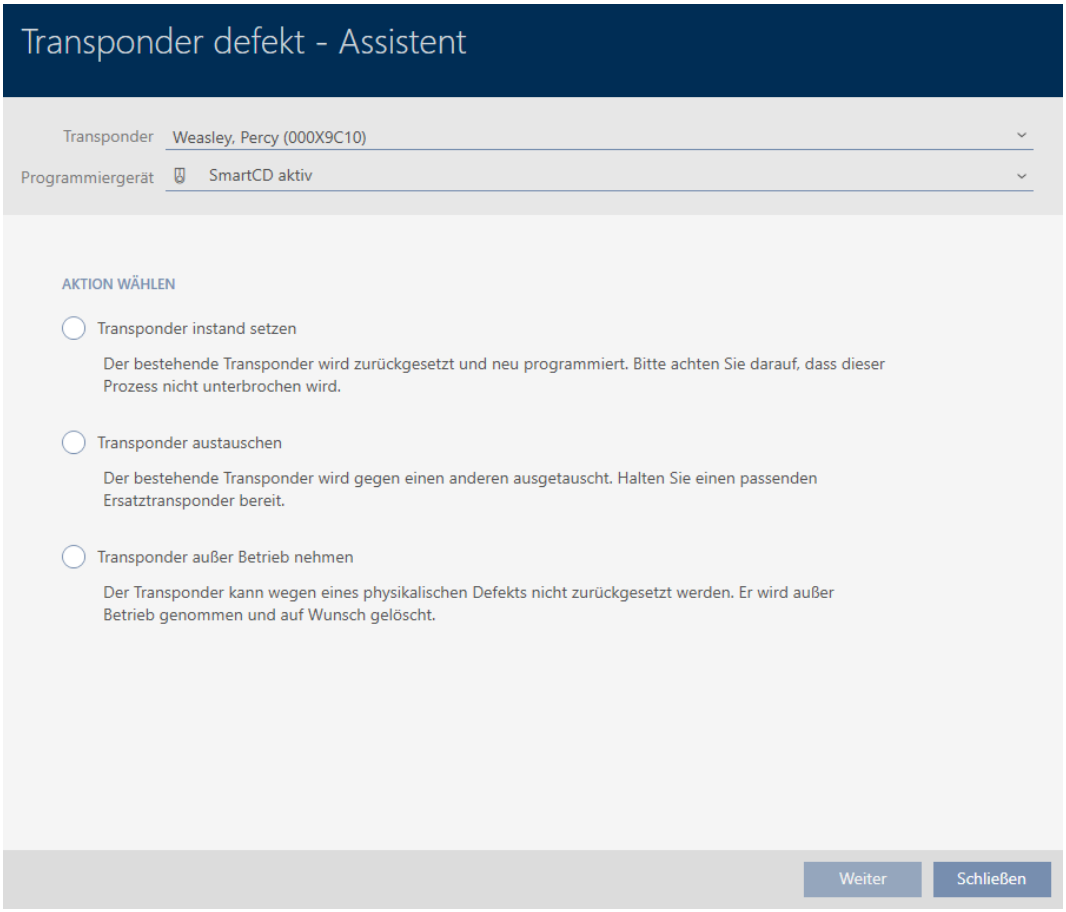
15.9.4 Take out of use and leave in project

15.9.4.1 Take card/transponder out of use and leave in project

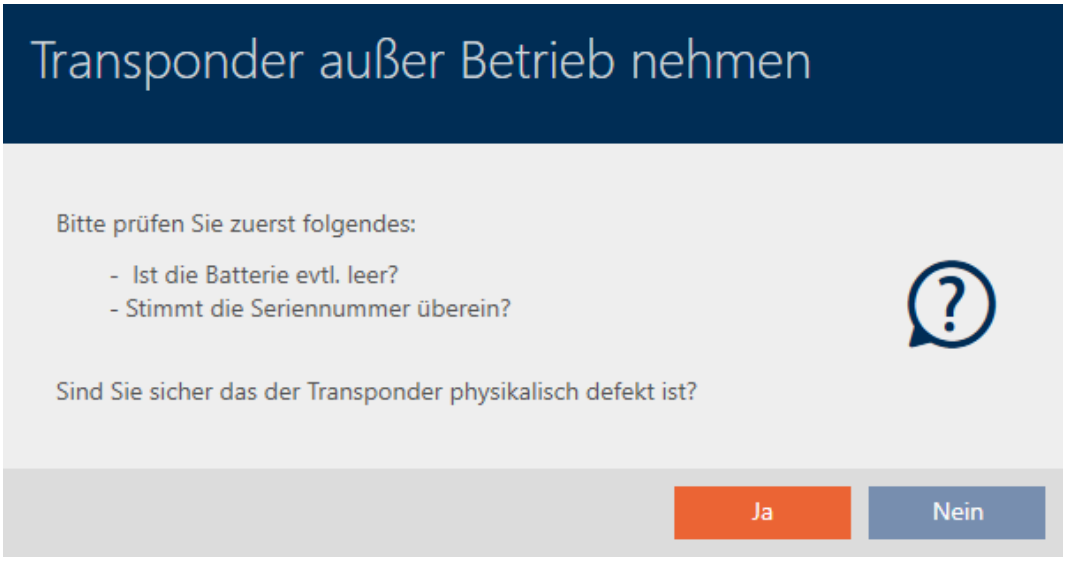
✓ AXM Lite open.

✓ Identification media list or matrix open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag the defective identification medium.
3. Click the Transponder defective / replace button in the "Wizards" section.
   ↳ Wizard for handling a defective identification medium will open.



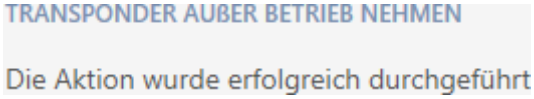
4. Select the option ◉ Decommission transponder.
5. Click on the Next button.
   ↳ A confirmation dialogue to take out of use will open.



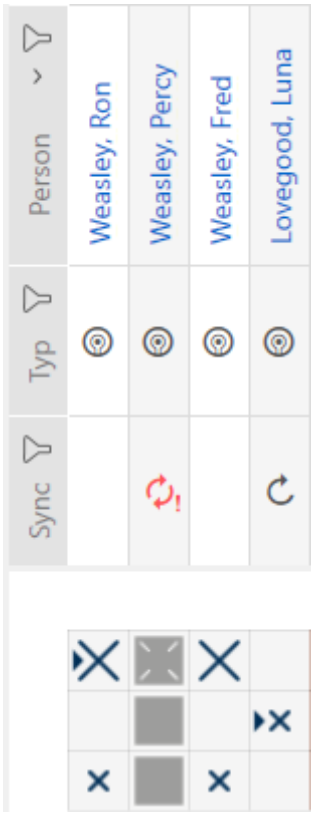
6. Click on the Yes button.
   ↳ Confirmation dialogue to take out of use closes.
   ↳ Confirmation dialogue for deleting the identification medium will open.

7. Click on the No button.
   ↳ Confirmation dialogue for deleting the identification medium closes.

↳ Identification medium has been taken out of operation.



Identification media that have been taken out of use but not deleted can be identified in the matrix:

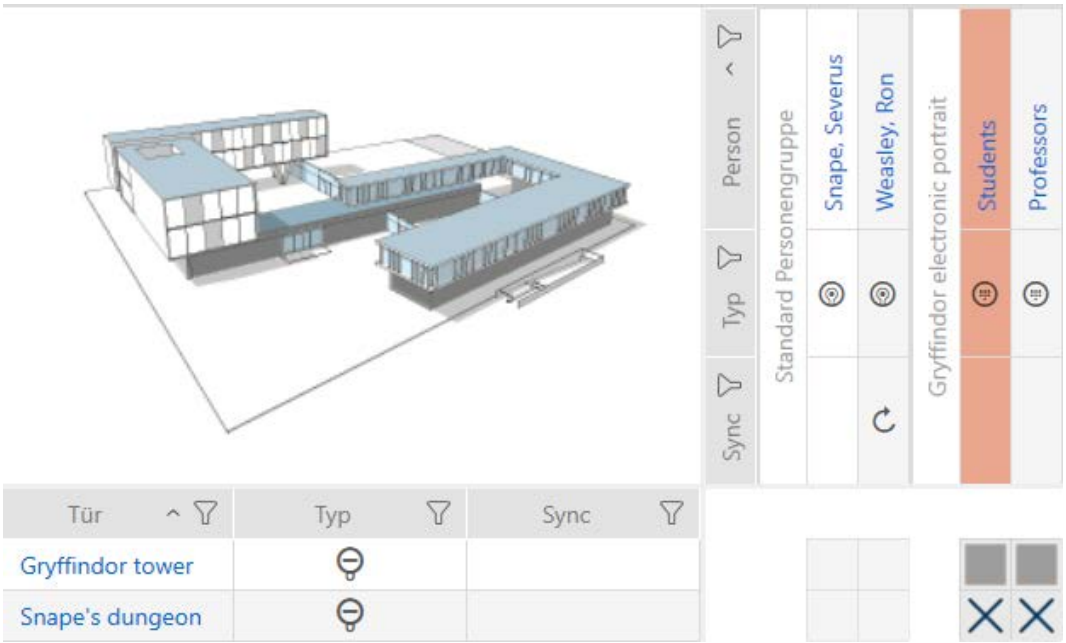


15.9.4.2 Taking a PIN code keypad out of use and leaving it in project

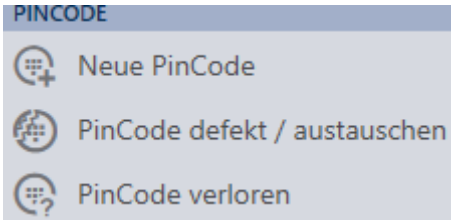
✓ AXM Lite open.

✓ List with PIN code keypads or matrix open.

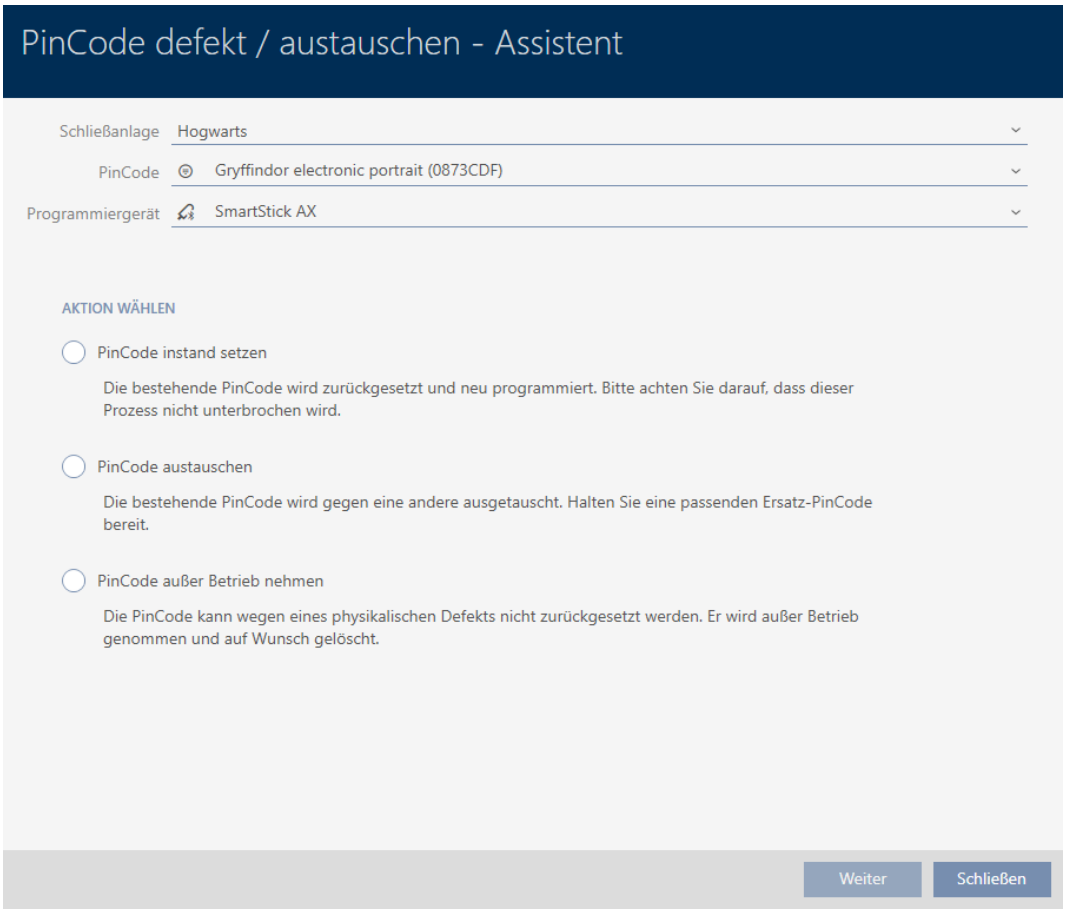
1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag a PIN associated with the defective PIN code keypad.



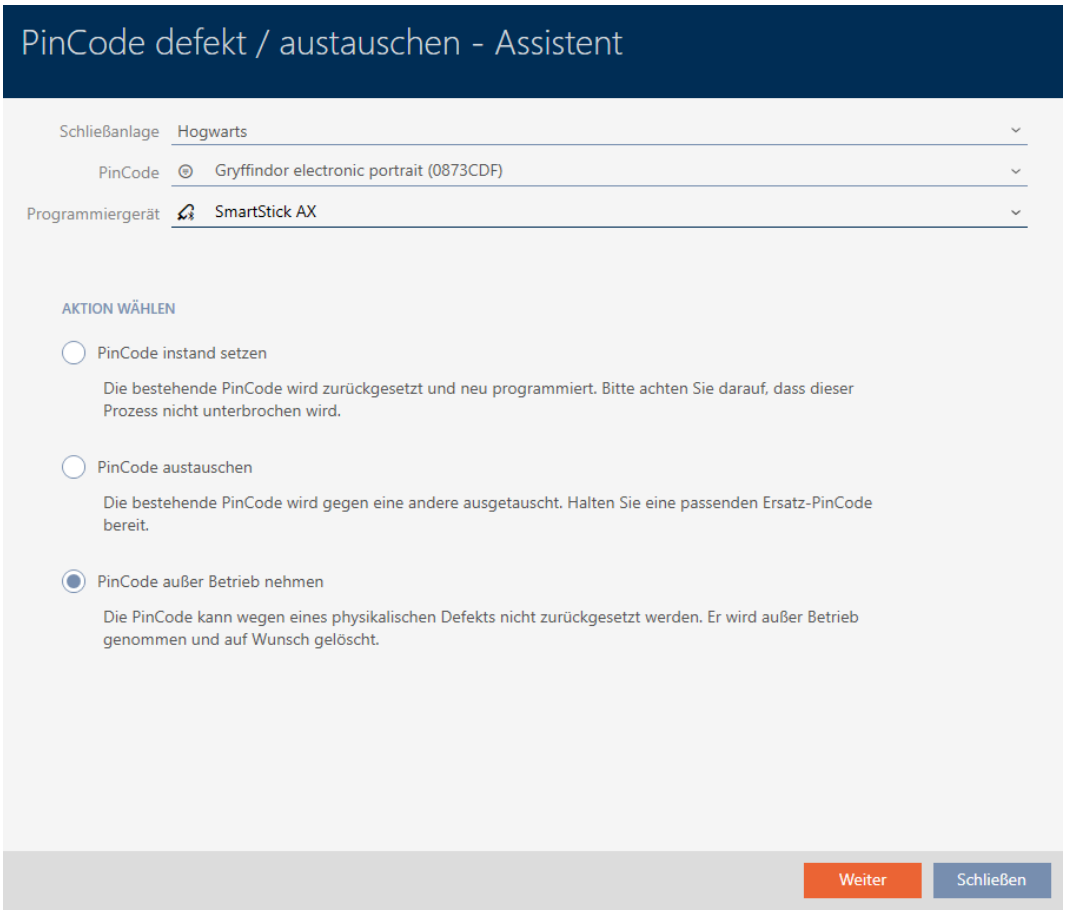
3. Click the PinCode defective / replace button in the "Wizards" section.



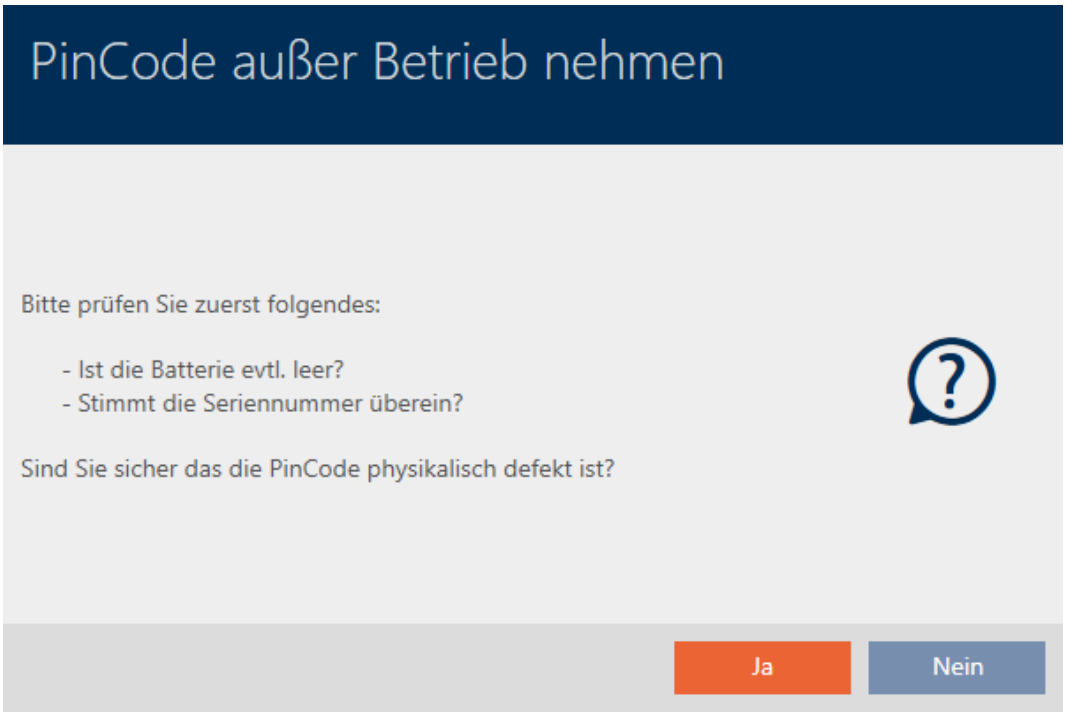
↳ Wizard to help with a faulty PIN code keypad will open.



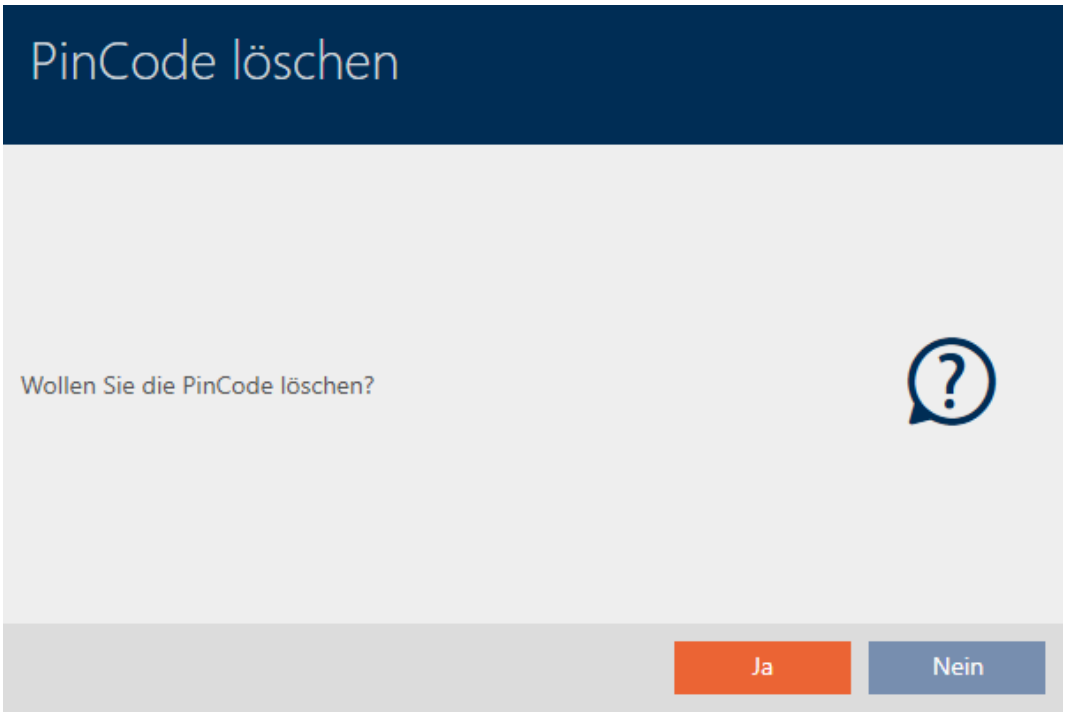
4. Select the option ◉ Decommission PinCode.



5. Click on the Next button.
   ↳ A confirmation dialogue to take out of use will open.

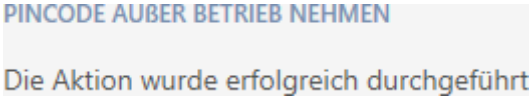


6. Click on the Yes button.
   ↳ Confirmation dialogue to take out of use closes.
   ↳ Confirmation dialogue to delete the PIN code keypad will open.

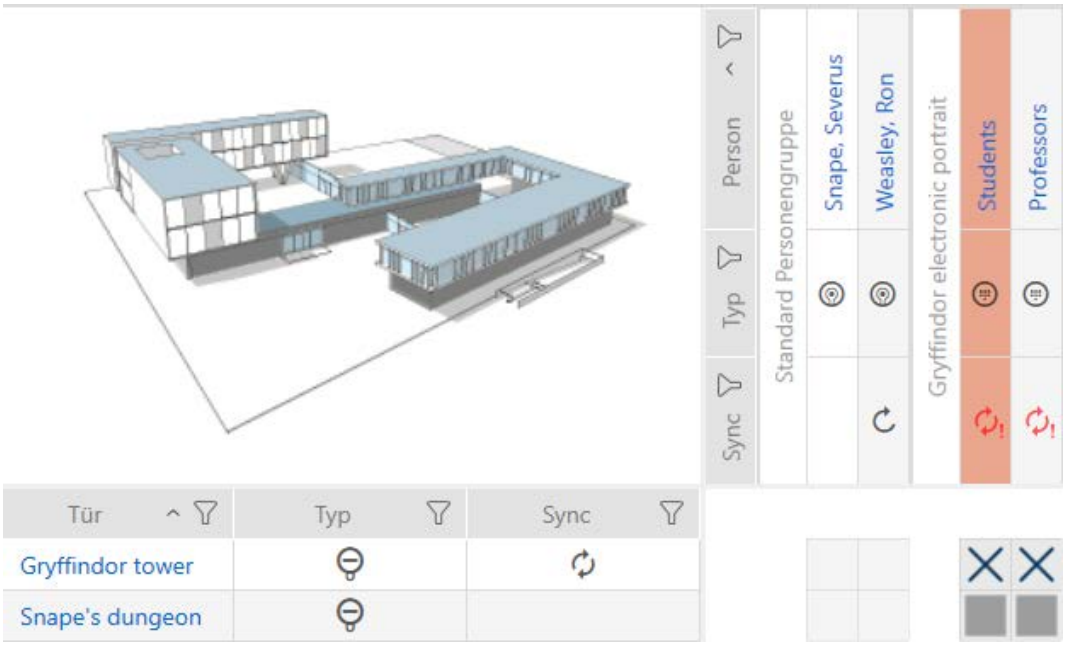


7. Click on the No button.
   ↳ Confirmation dialogue to delete the PIN code keypad closes.

↳ The PIN code keypad has been taken out of operation.



PIN code keypads that have been taken out of use but not deleted can be identified in the matrix:



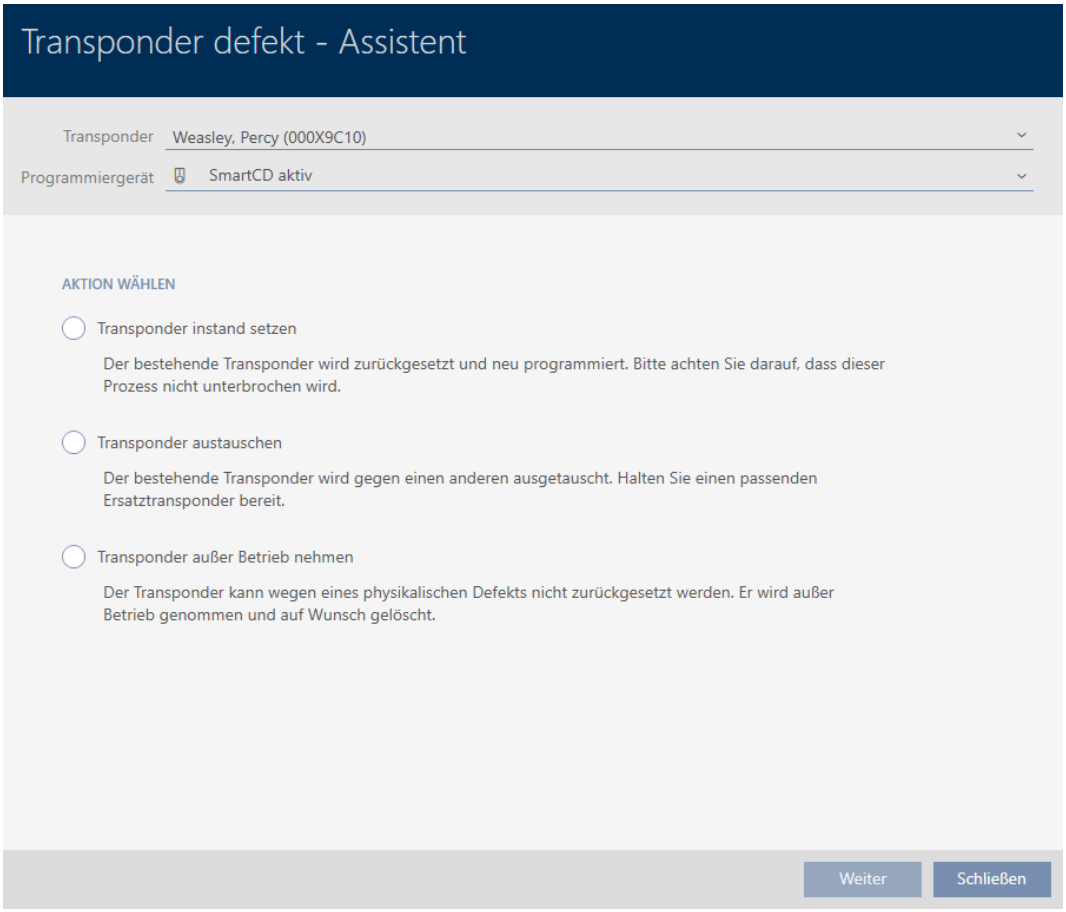
15.9.5 Taking out of use and deleting from the project

15.9.5.1 Taking a card/transponder out of use and deleting it from project

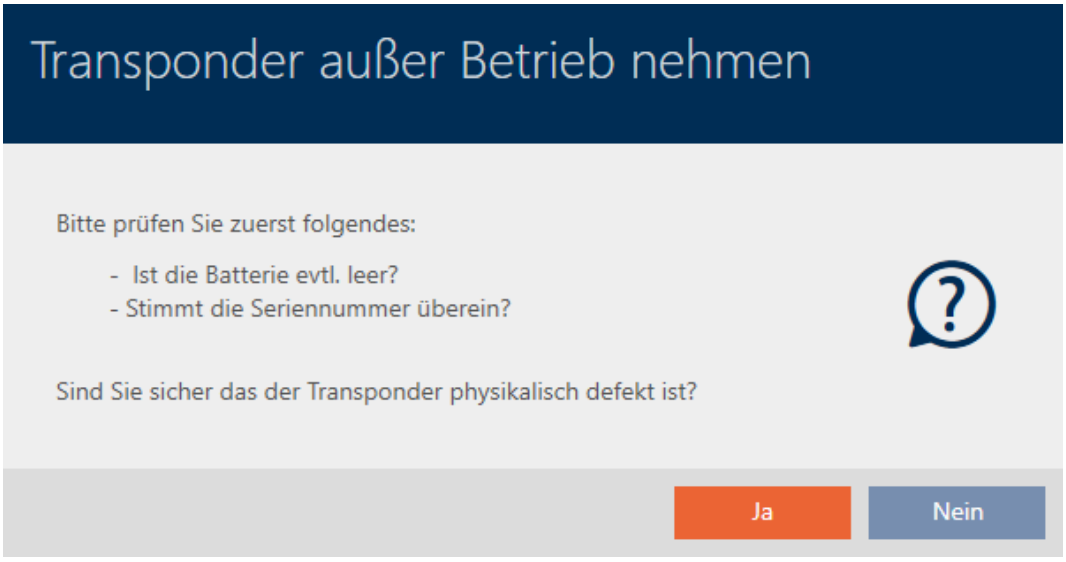
✓ AXM Lite open.

✓ Identification media list or matrix open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Flag the defective identification medium.
3. Click the Transponder defective / replace button in the "Wizards" section.
   ↳ Wizard for handling a defective identification medium will open.



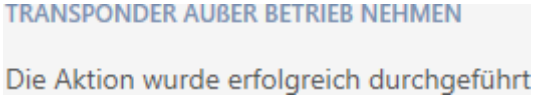
4. Select the option ◉ Decommission transponder.
5. Click on the Next button.
   ↳ A confirmation dialogue to take out of use will open.



6. Click on the Yes button.
   ↳ Confirmation dialogue to take out of use closes.
   ↳ Confirmation dialogue for deleting the identification medium will open.

7. Click on the Yes button.
   ↳ Confirmation dialogue to delete the identification medium closes.

↳ Identification medium is deleted without replacement.

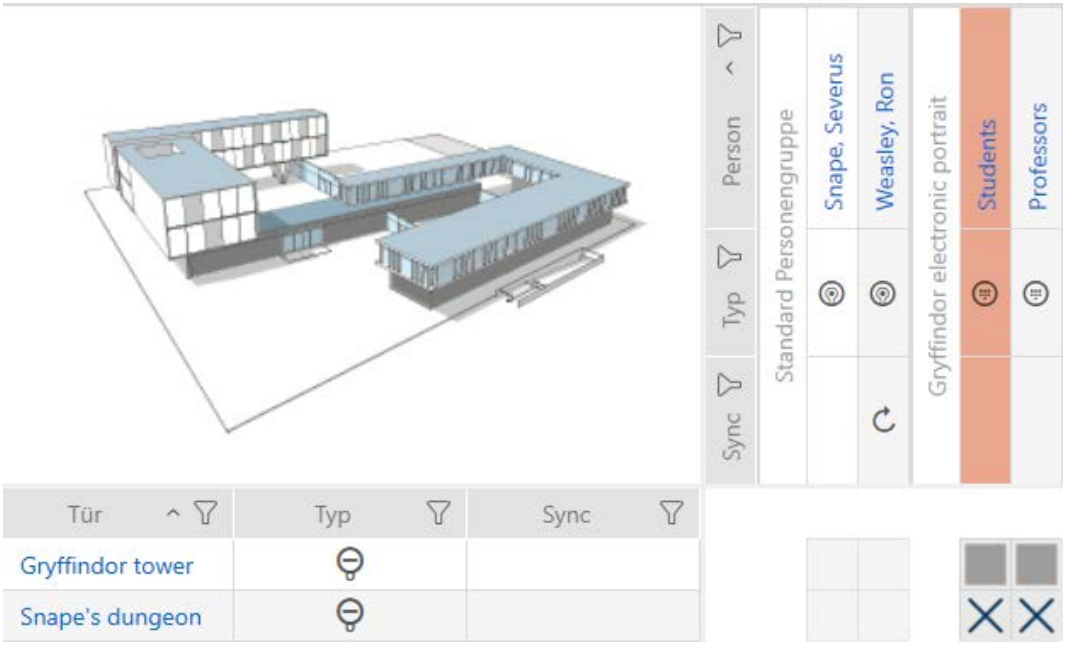


15.9.5.2 Taking a PIN code keypad out of use and deleting it from project

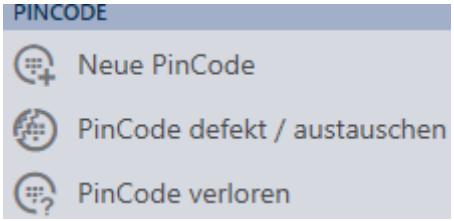
✓ AXM Lite open.
✓ List with PIN code keypads or matrix open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

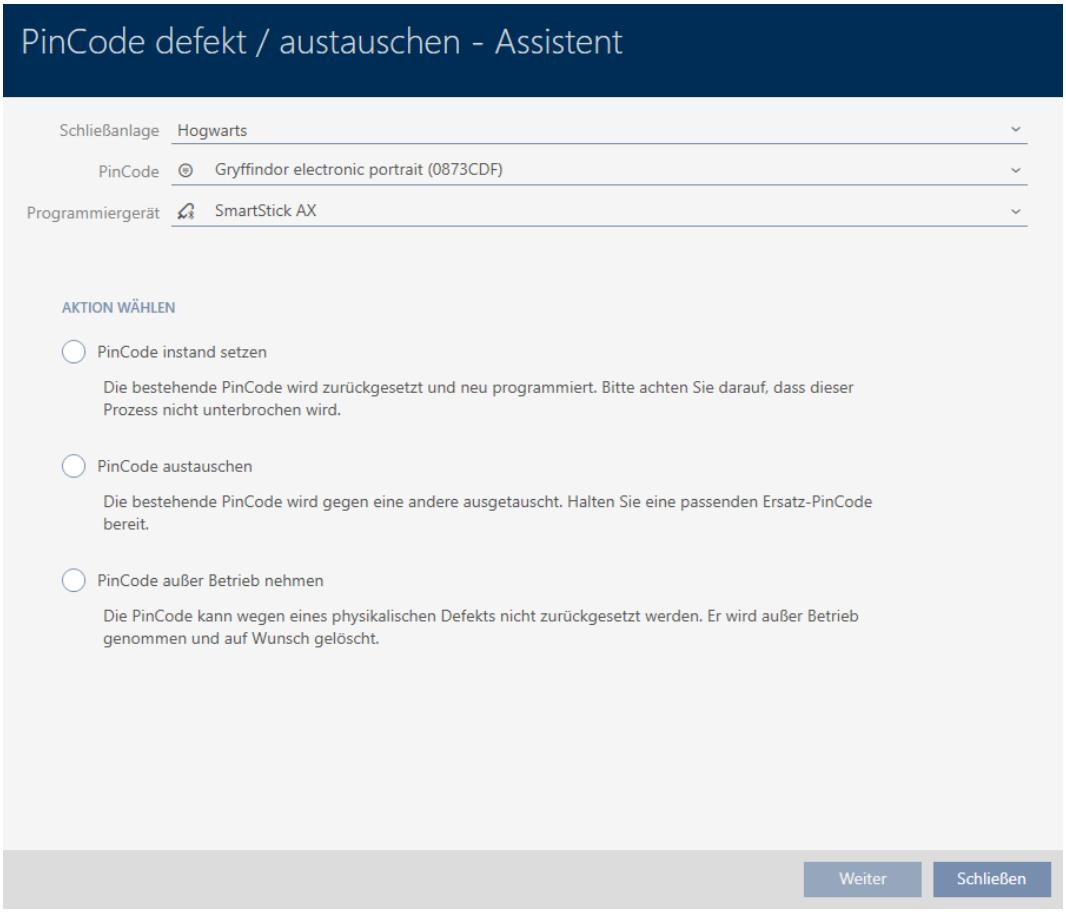
2. Flag a PIN associated with the defective PIN code keypad.



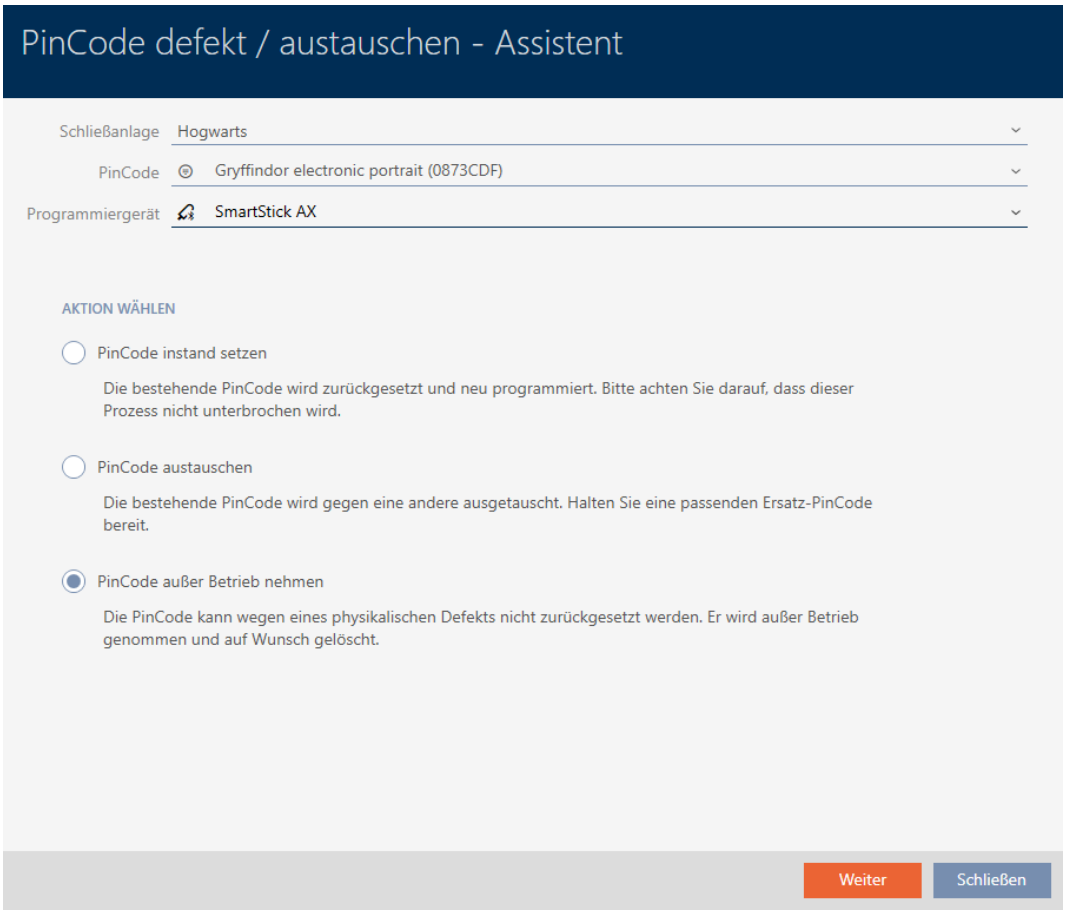
3. Click the PinCode defective / replace button in the "Wizards" section.



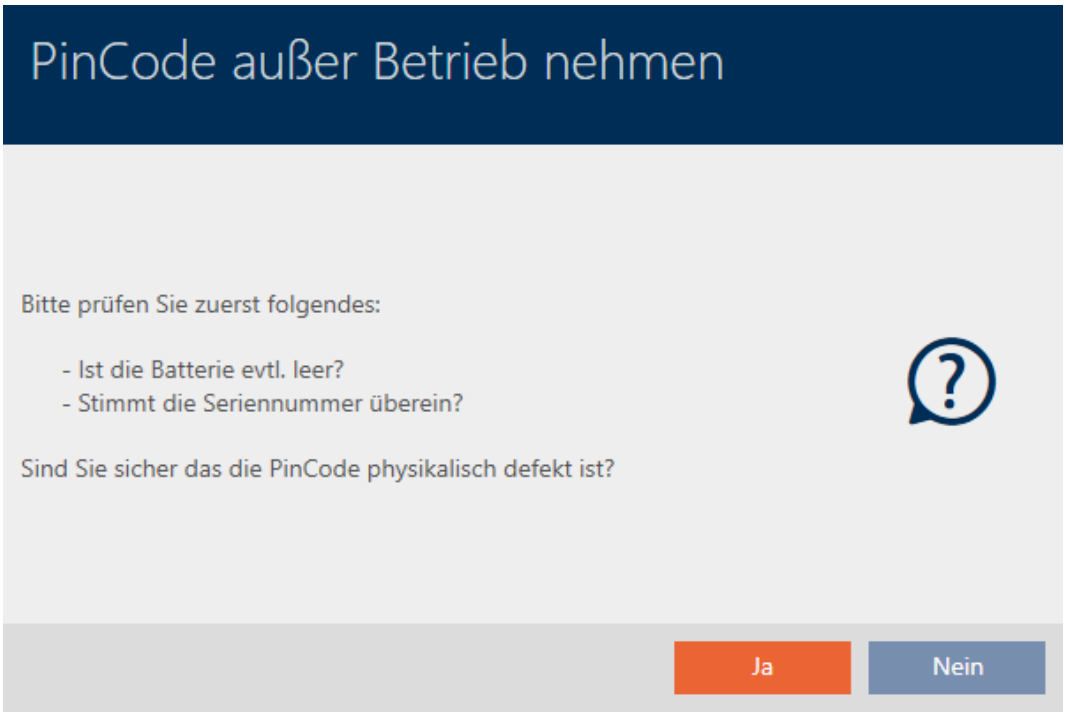
↳ Wizard to help with a faulty PIN code keypad will open.


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

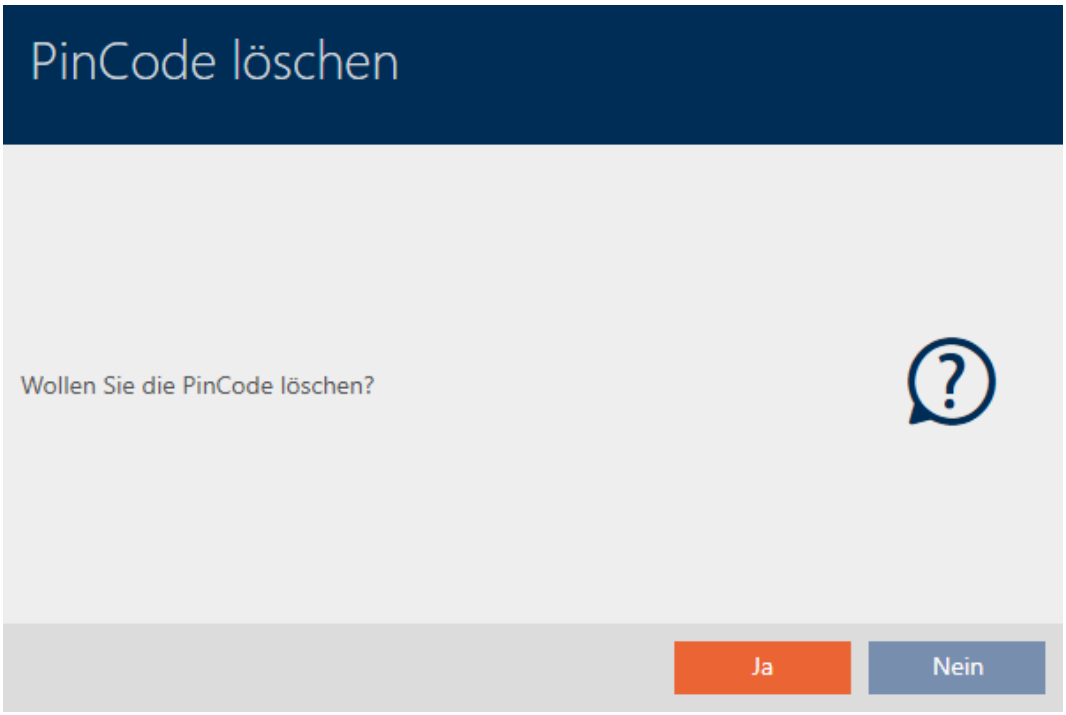
4. Select the option ◉ Decommission PinCode.



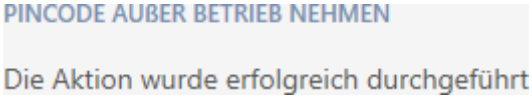
5. Click on the Next button.
   ↳ A confirmation dialogue to take out of use will open.



6. Click on the Yes button.
   ↳ Confirmation dialogue to take out of use closes.
   ↳ Confirmation dialogue to delete the PIN code keypad will open.



7. Click on the Yes button.
   ↳ Confirmation dialogue to delete the PIN code keypad closes.
8. The PIN code keypad has been taken out of use and deleted without replacement.



15.10 Duplicating forgotten identification medium temporarily

15.10.1 Duplicating a forgotten transponder or card temporarily

Identification media left elsewhere differ from defective or stolen/lost identification media:

- In contrast to defective identification media, identification media that the user has forgotten are fully functional.

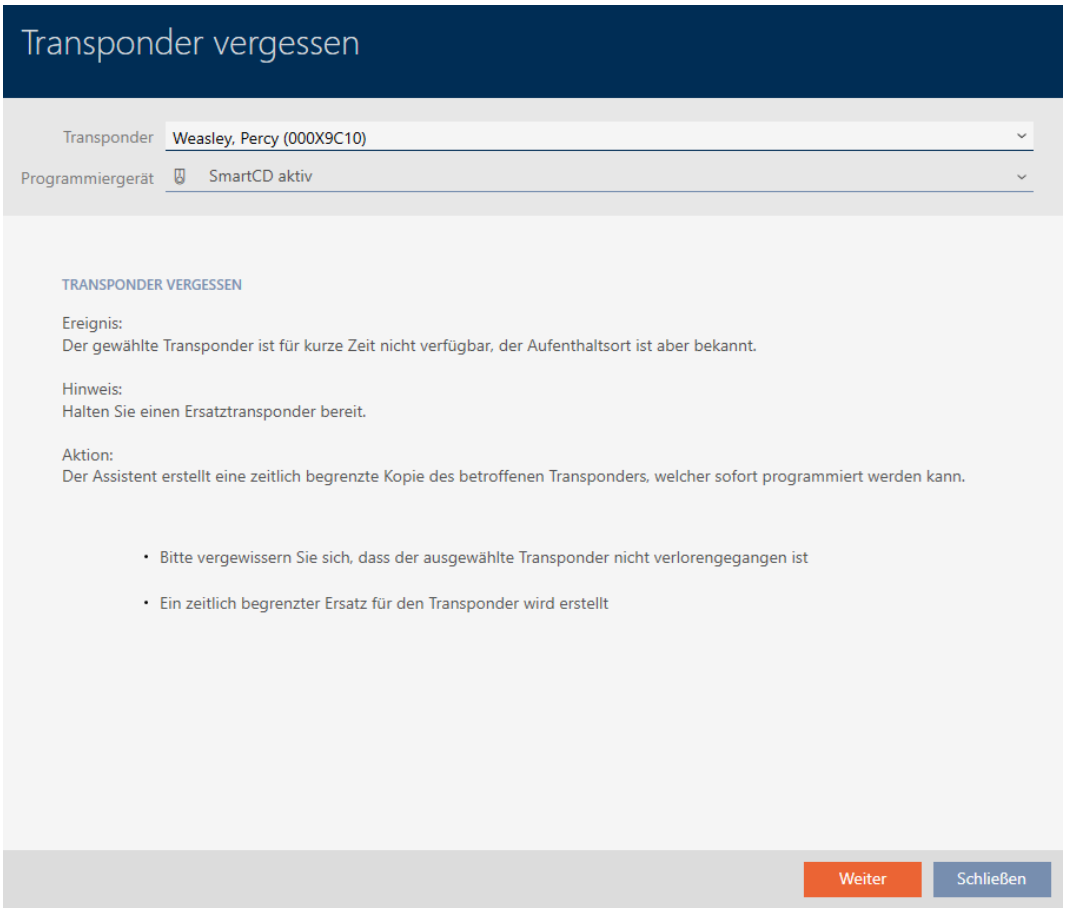
- In contrast to stolen/lost identification media, the identification medium is in a known/secure location.

Employees who have forgotten their identification medium can receive a copy with an expiry date. In this case, there is no need to reset or delete the identification medium as no unauthorised person has access to the forgotten identification medium.

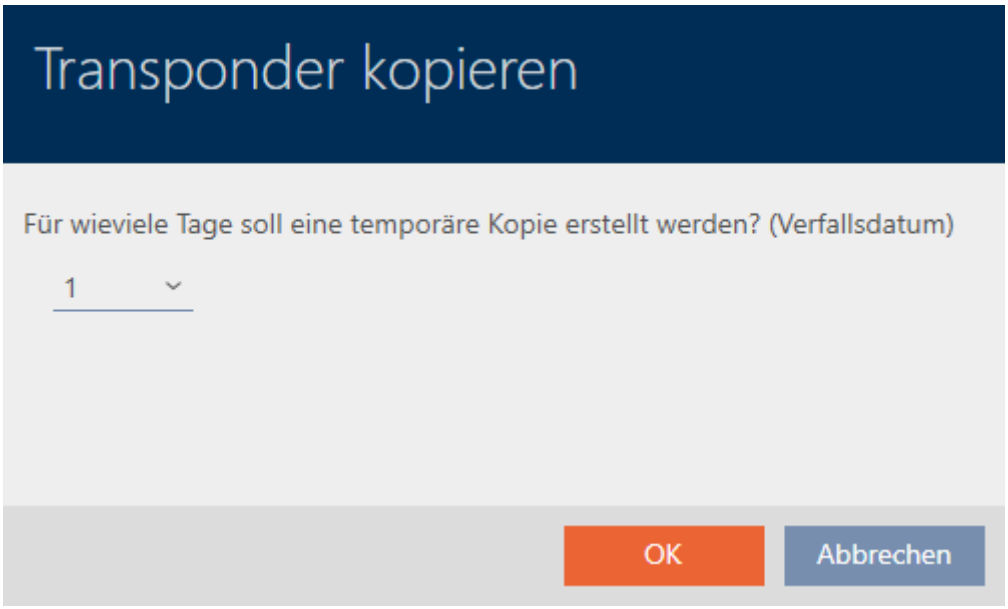
The duplicate receives a different TID and is thus a separate identification medium from a locking device perspective (see *Identification media, locking devices and the locking plan [▸ 360]* for information on the connection between TID and identification medium).

✓ AXM Lite open.
✓ Identification media list or matrix open.
✓ Identification medium available for temporary duplication for programming.
✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the forgotten identification medium.
3. Click the Forgot transponder button in the "Wizards" section.
   ↳ Wizard for forgotten identification media will open.

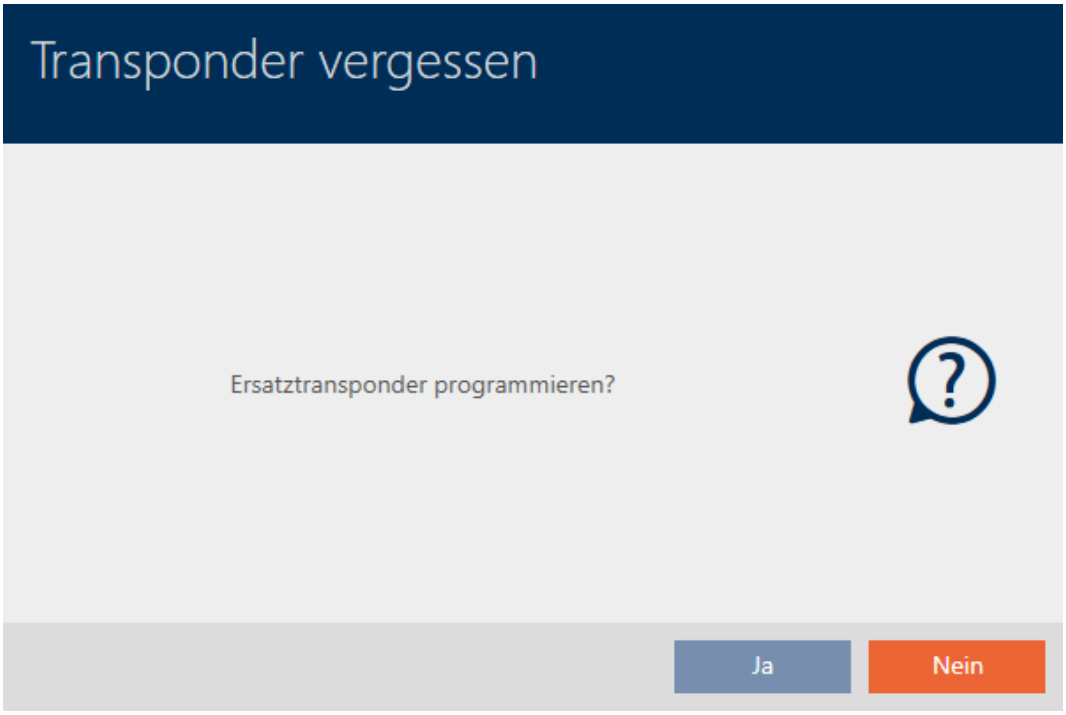


4. Click on the Next button.
   ↳ Confirmation dialogue for the duplicate's expiry date will open.

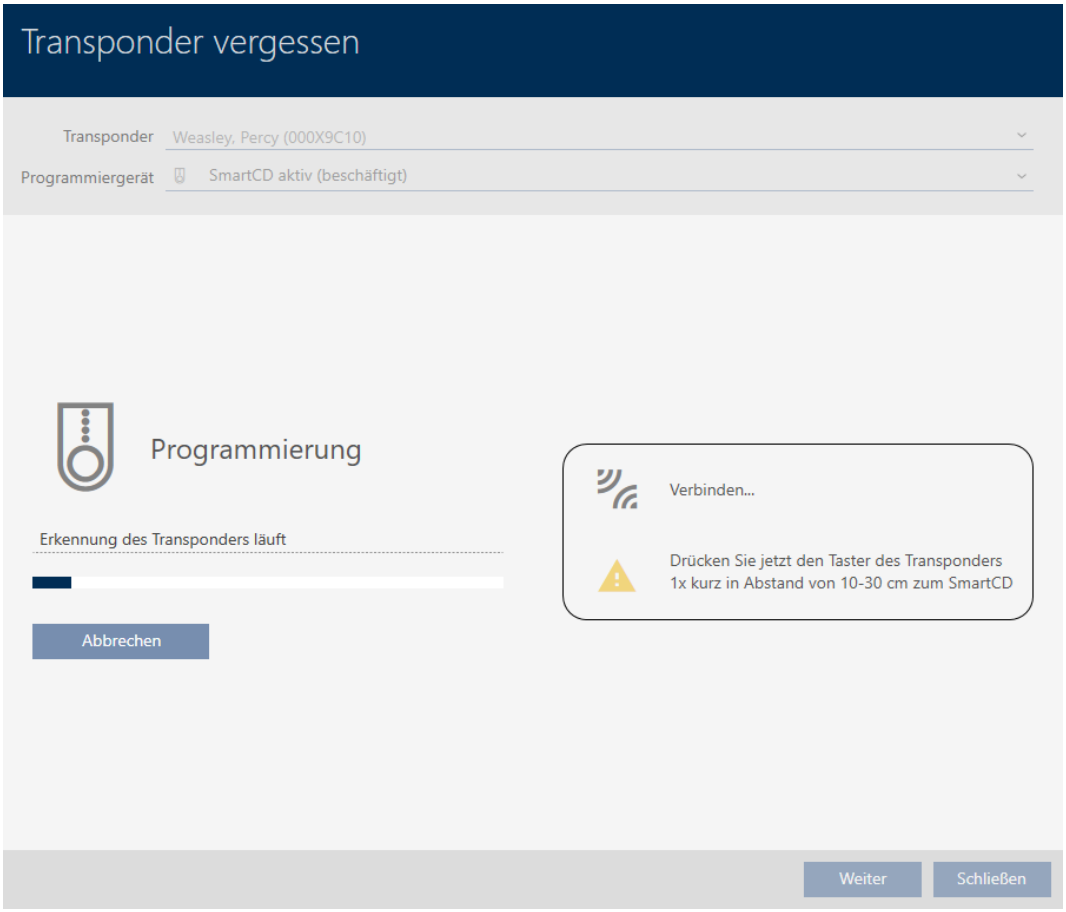


5. Specify how long the duplicate should be active for (max. 7 days).

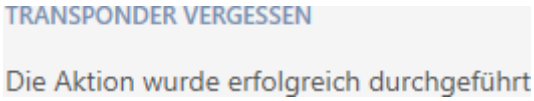
6. Click on the OK button.
   ↳ Confirmation dialogue for the duplicate's expiry date closes.
   ↳ Confirmation dialogue for immediate synchronisation will open.



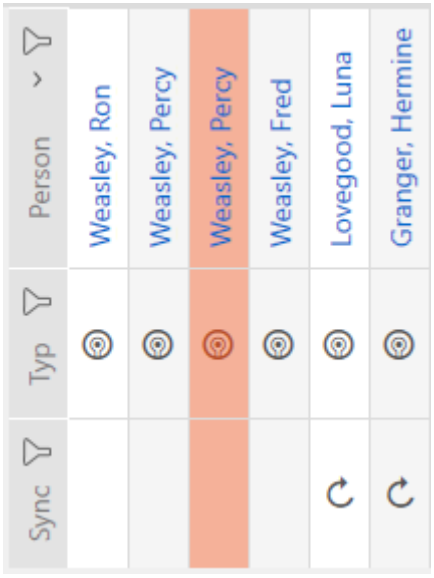
7. Click on the Yes button.
   ↳ Confirmation dialogue for immediate synchronisation closes.
   ↳ Duplicate is synchronised.



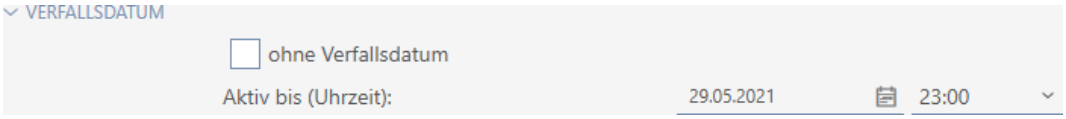
↳ Forgotten identification medium is now duplicated with expiry date.



Duplicated identification media are also displayed in the matrix:



You can view the expiry date in the duplicate's properties and extend it if necessary (see *Activating or deactivating identification medium once at specific times (activation and expiry date) [▸ 104]*):



In this example, the duplicate was created for one day at 23:00 hours on 28.05.2021. The duplicate's expiry date is therefore 23:00 hours on 29.05.2021.

If an identification medium is forgotten for a longer period of time (and thus may no longer have been left elsewhere but lost instead), it may be advisable to block the identification medium (see *Blocking and replacing lost/stolen card/transponder permanently [▸ 146]*).

15.11 Blocking lost/stolen identification media permanently

An identification medium that can no longer be found poses a security risk for your locking system. In contrast to a forgotten identification medium, the location is no longer known and unauthorised persons could gain access using this identification medium.

Block such an identification medium immediately (see *Blocking and replacing lost/stolen card/transponder permanently [▸ 146]*). You can also create a replacement identification medium with a different TID for the employee concerned, but with the same settings and authorisations. Your locking devices will recognise the replacement identification medium as a new identification medium (see *Identification media, locking devices and the locking plan [▸ 360]* for information on TIDs).

Lost and stolen PIN code keypads

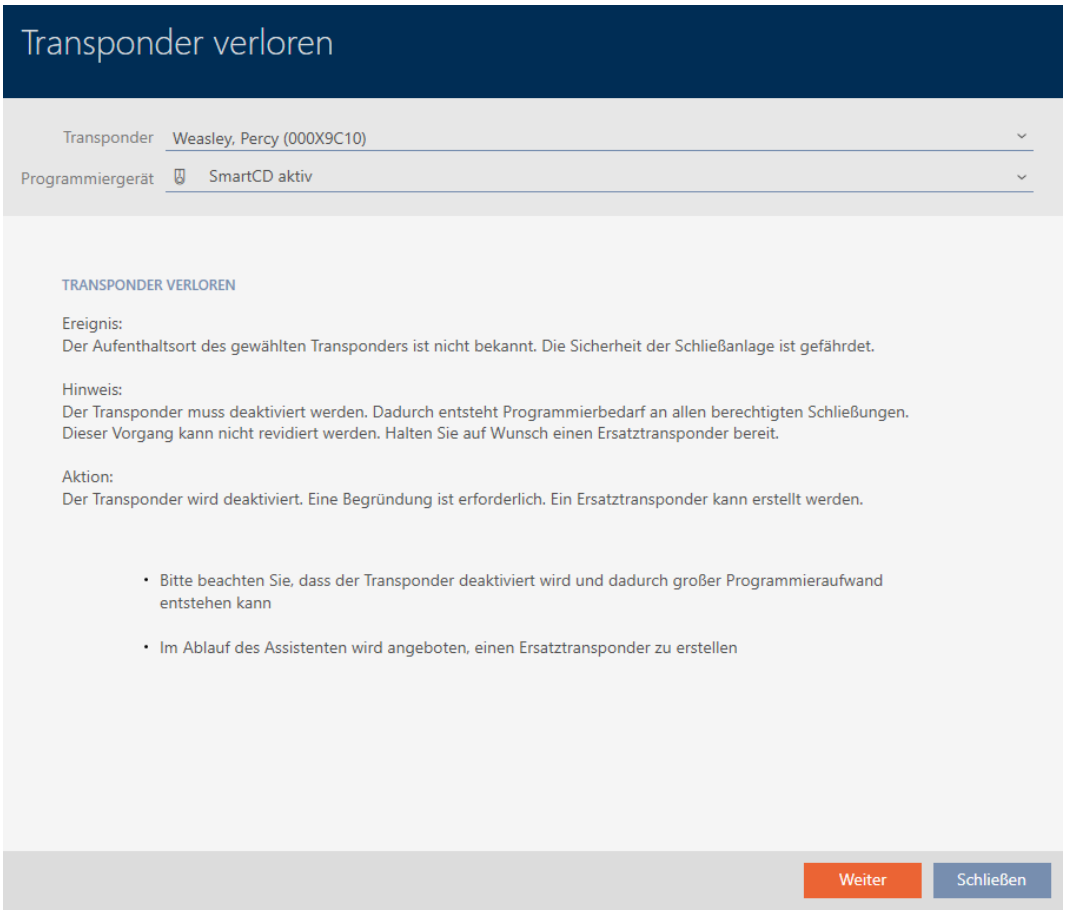
A PIN code keypad is fixed in place after installation and can no longer be lost. However, it can become lost on the way to its installation location and then stolen by force. For example, a thief could try different PINs in an unsecured area to find a valid PIN.

Since you cannot know which PIN the thief discovered by trial and error, you must always block the entire PIN keypad (see *Blocking a lost/stolen PIN code keypad permanently [▸ 151]*). If only one PIN is known and is therefore unsafe, you can change this PIN (see *Changing a PIN (PinCode AX) [▸ 180]*).

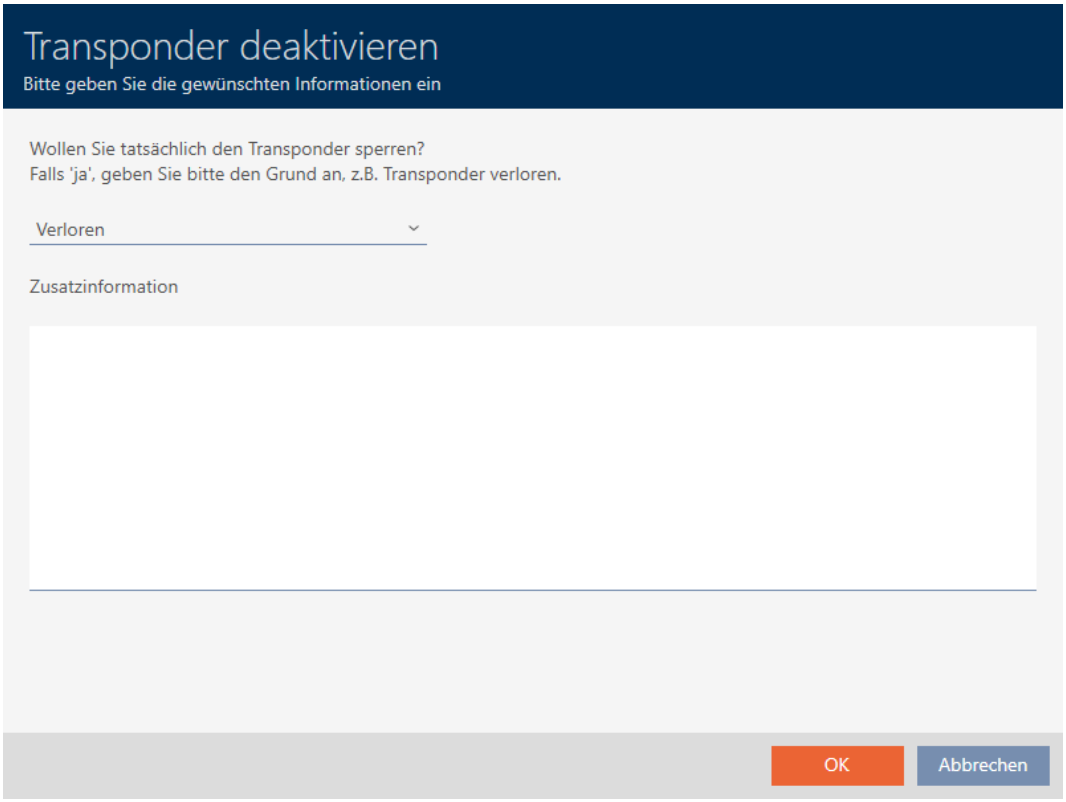
15.11.1 Blocking and replacing lost/stolen card/transponder permanently

- ✓ AXM Lite open.
- ✓ Identification media list or matrix open.
- ✓ Replacement identification medium at hand.
- ✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the identification medium that has been lost/stolen.
3. Click the ⓘ Transponder lost button in the "Wizards" section.
   ↳ Wizard for handling a lost identification medium will open.



4. Click on the Next button.
   ↳ The reason window will open.

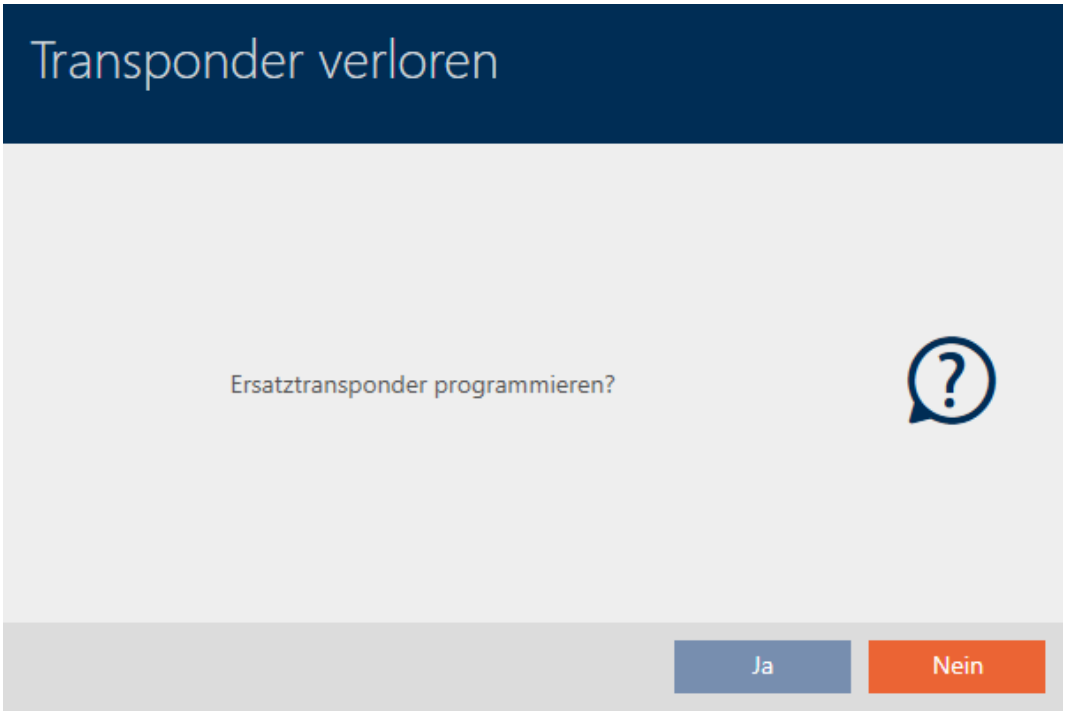


5. Enter the reason in the drop-down menu.

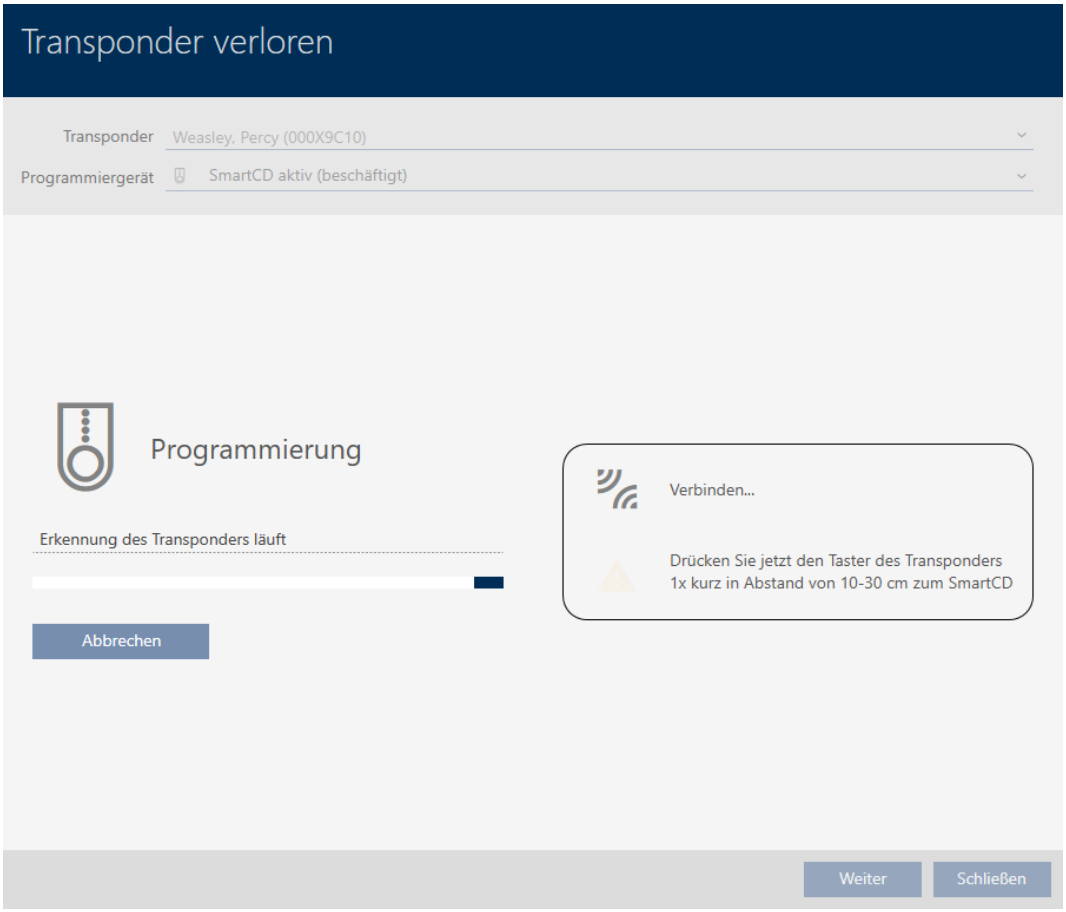
6. Click on the OK button.
   ↳ Confirmation dialogue for replacement identification medium will open.

7. Click on the Yes button.
   ↳ Confirmation dialogue for replacement identification medium closes.
   ↳ Replacement identification medium can already be seen in the matrix in the background.

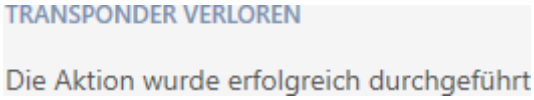
   ↳ Confirmation dialogue about synchronising the replacement identification medium will open.



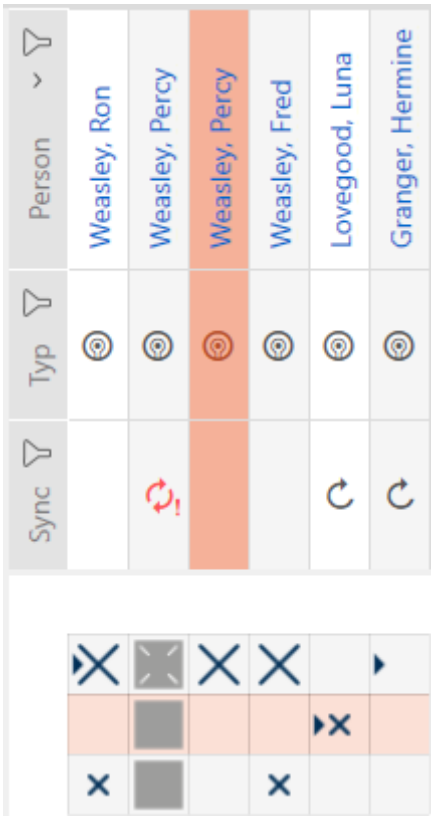
8. Click on the Yes button.
   ↳ Confirmation dialogue about synchronising the replacement identification medium closes.
   ↳ Synchronisation starts.



↳ Lost identification medium is blocked.
↳ Replacement identification medium is synchronised.



↳ Replacement identification medium is displayed in the matrix next to the lost identification medium.



IMPORTANT

Changes to the locking system only take effect after synchronisation

If you edit the locking system with the AXM Lite, the changes are initially only saved to your database.

Your actual components will not know about these changes until they are synchronised.

1. Regularly check the components in the matrix for synchronisation requirements (see *The AXM's structure [▸ 35]*).
2. In the event of critical incidents (e.g. identification medium lost), it is particularly important to synchronise immediately after responding to the incident (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*).

IMPORTANT

Block ID automatically written on replacement transponder

If you create a replacement transponder for a lost/stolen transponder, your AXM Lite automatically writes the block ID from the blocked transponder onto this replacement transponder.

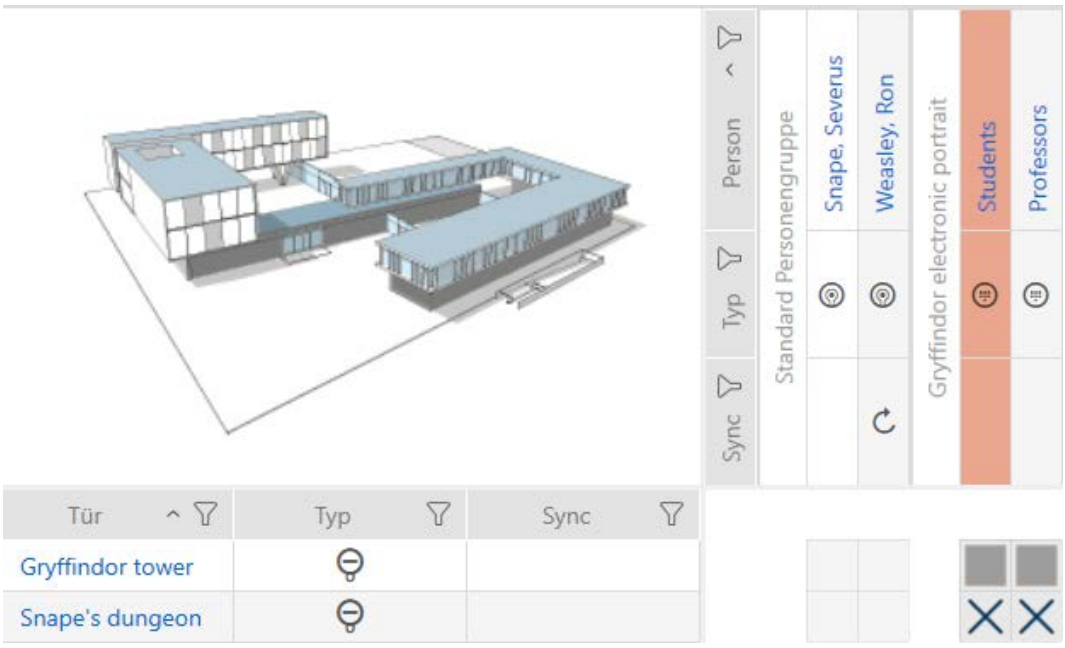
You can also use this replacement transponder to transfer the block ID to the locking devices without a virtual network. This means that you do not necessarily need to go to the locking device with a programming device, even if you use a Lite/Classic edition.

1. Present the replacement transponder to the locking devices.
2. Alternatively, synchronise the locking devices on site.

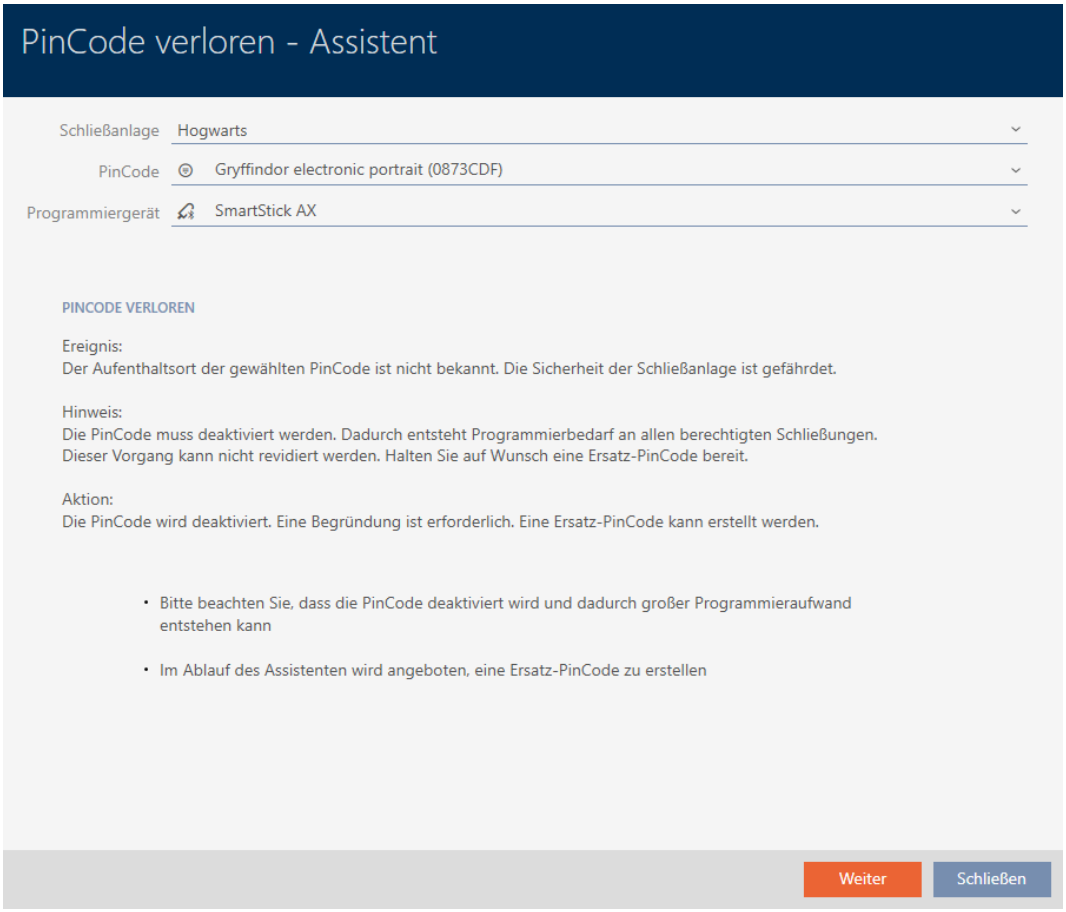
15.11.2 Blocking a lost/stolen PIN code keypad permanently

- ✓ AXM Lite open.
- ✓ List with PIN code keypads or matrix open.
- ✓ Suitable programming device connected to replace PIN code keypad.

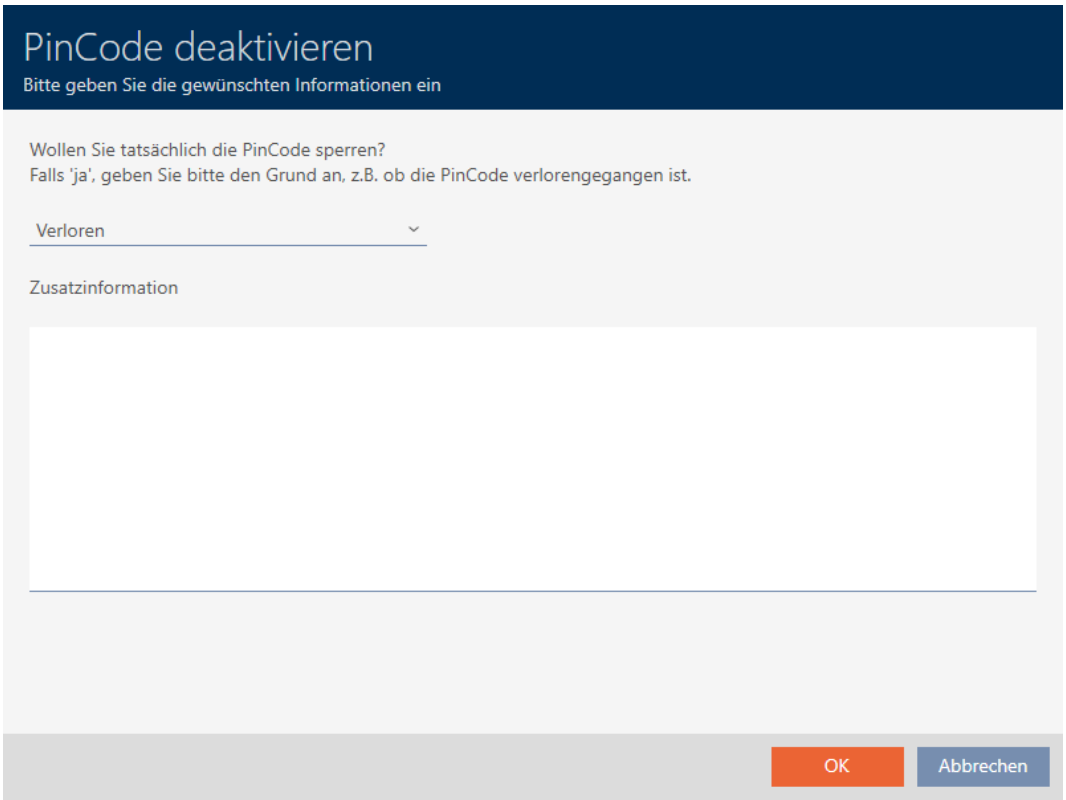
1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select a PIN associated with the lost PIN code keypad.



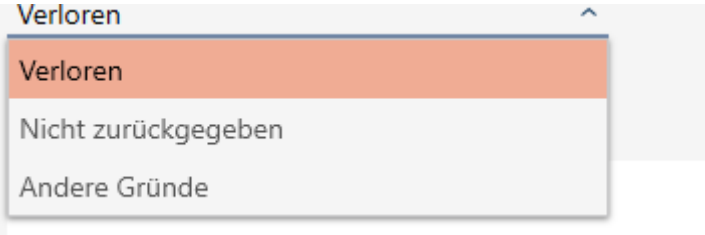
3. Click the PinCode lost button in the "Wizards" section.
   ↳ Wizard to help with a lost PIN code keypad will open.



4. Click on the Next button.
   ↳ The confirmation window will open.



5. If applicable, select a reason other than "Lost" from the drop-down menu.

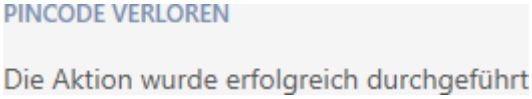


6. Enter any additional information in the *Additional information* field.
7. Click on the OK button.
   ↳ Confirmation window closes.
   ↳ AXM Lite offers to create a replacement PIN code keypad.

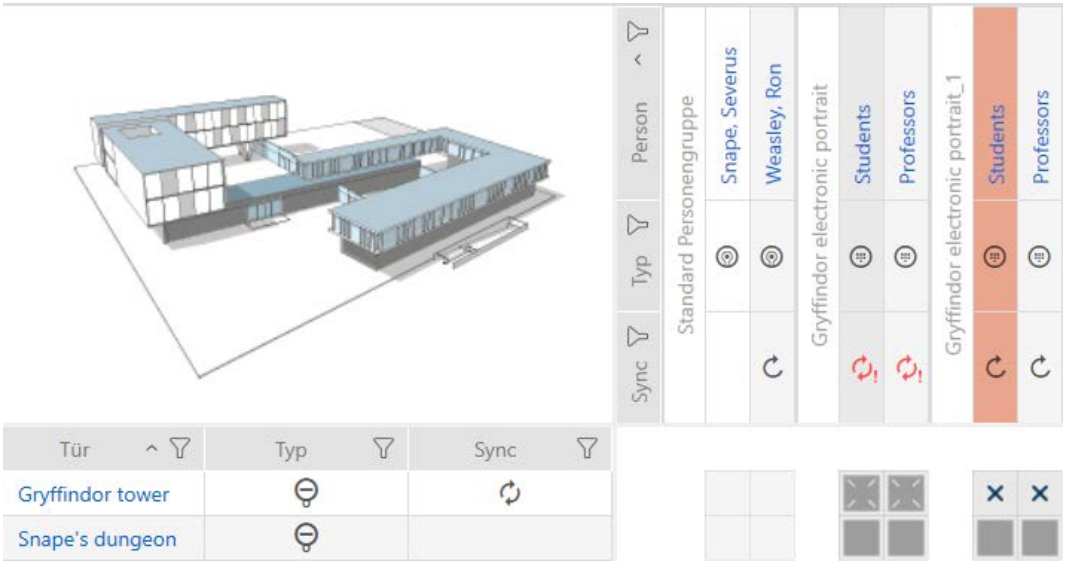
8. If you need a replacement, click the Yes button; otherwise, click the No button.
   (Example: Yes)
   ↳ AXM Lite creates a replacement PIN code keypad in the background.
   ↳ AXM Lite offers to synchronise the replacement PIN code keypad immediately.

9. Click on the Yes button.
   ↳ Synchronisation of the replacement PIN code keypad launches.
   ↳ AXM Lite offers to delete the lost PIN code keypad.

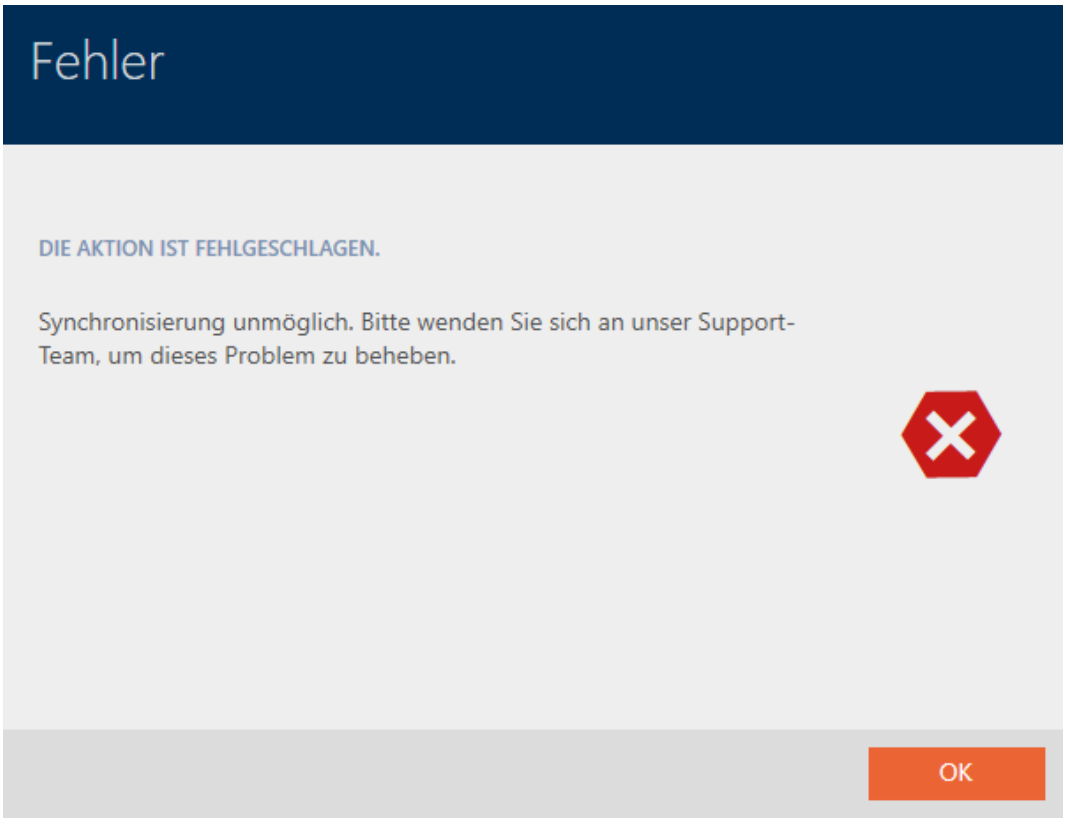
10. Click on the No button.
    ↳ The PIN code keypad has been blocked and a replacement PIN code keypad has been synchronised.



Both PIN code keypads are visible in the matrix.



You will need a different PIN code keypad for the replacement. If you try to use the same PIN code keypad, your AXM Lite will display an error message:



You can repair the PIN code keypad as an alternative; see *Repairing a PIN code keypad (resynchronising) [▸ 112]*.

15.12 Flag and reset returned identification medium (back to inventory)

An identification medium has been transferred to locking system management and should be withdrawn from circulation.

In contrast to reset and deletion, the physical identification medium is reset but remains in your locking system. AXM Lite enters a comment about the return in the identification medium's history instead.

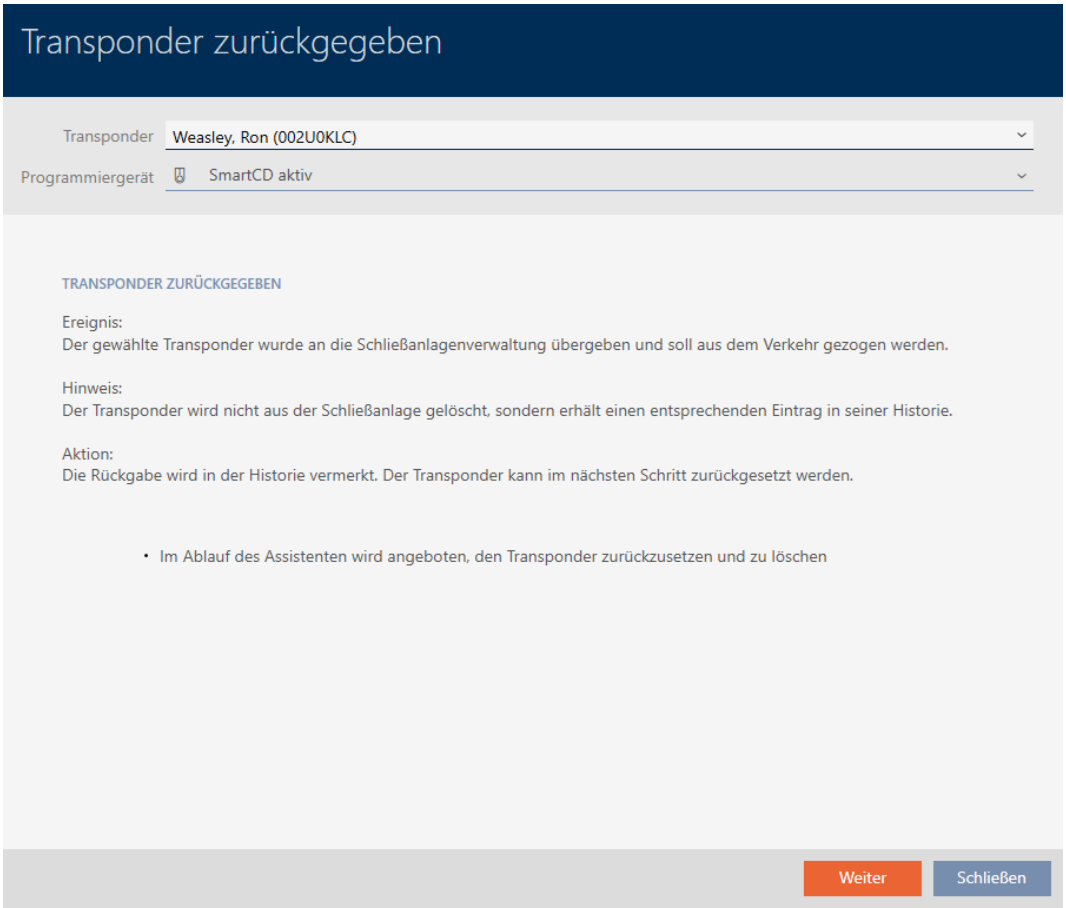
Obviously, you can also delete the identification medium from the locking system after resetting. However, the action list ("history") would be lost.

15.12.1 Flagging and resetting returned card/transponder (back to inventory)

Proceed as follows to withdraw a card or transponder without losing its action list:

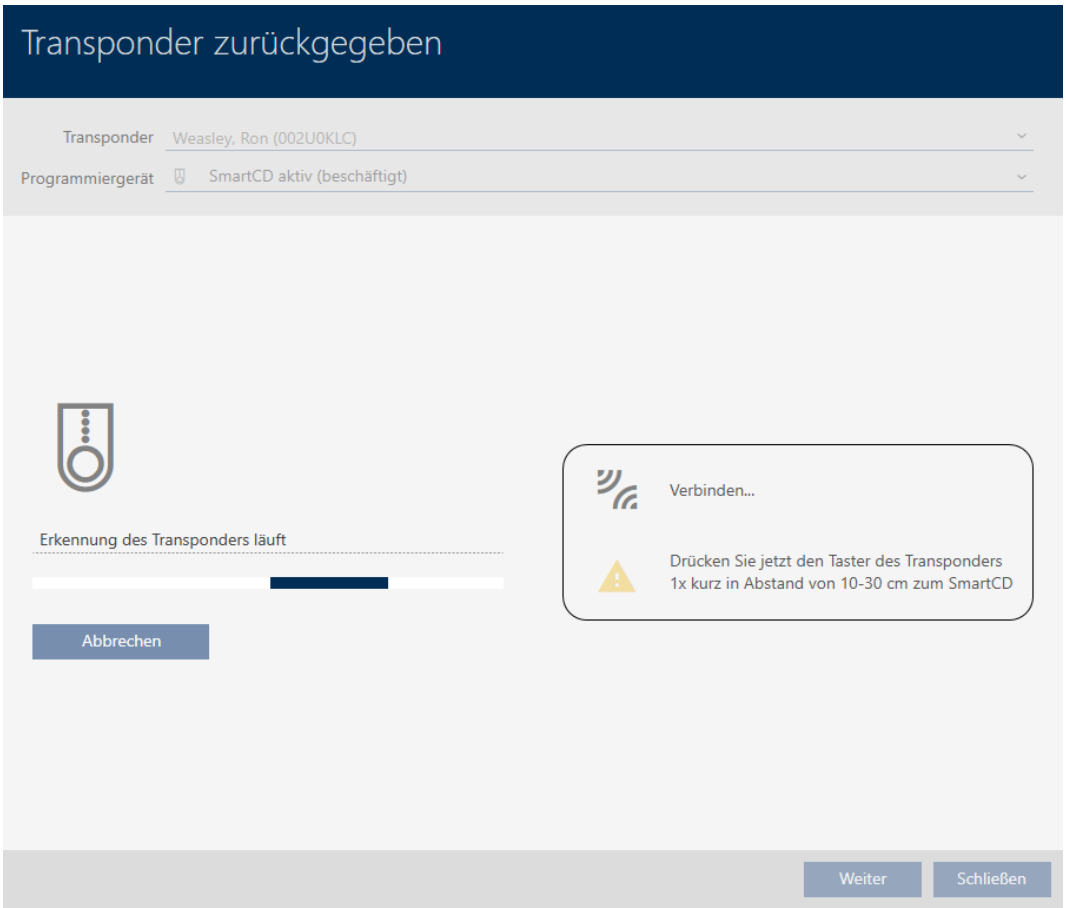
✓ AXM Lite open.
✓ Suitable programming device connected.

1. Click the Transponder returned button in the "Wizards" section.
   ↳ The wizard for ID media return will open.

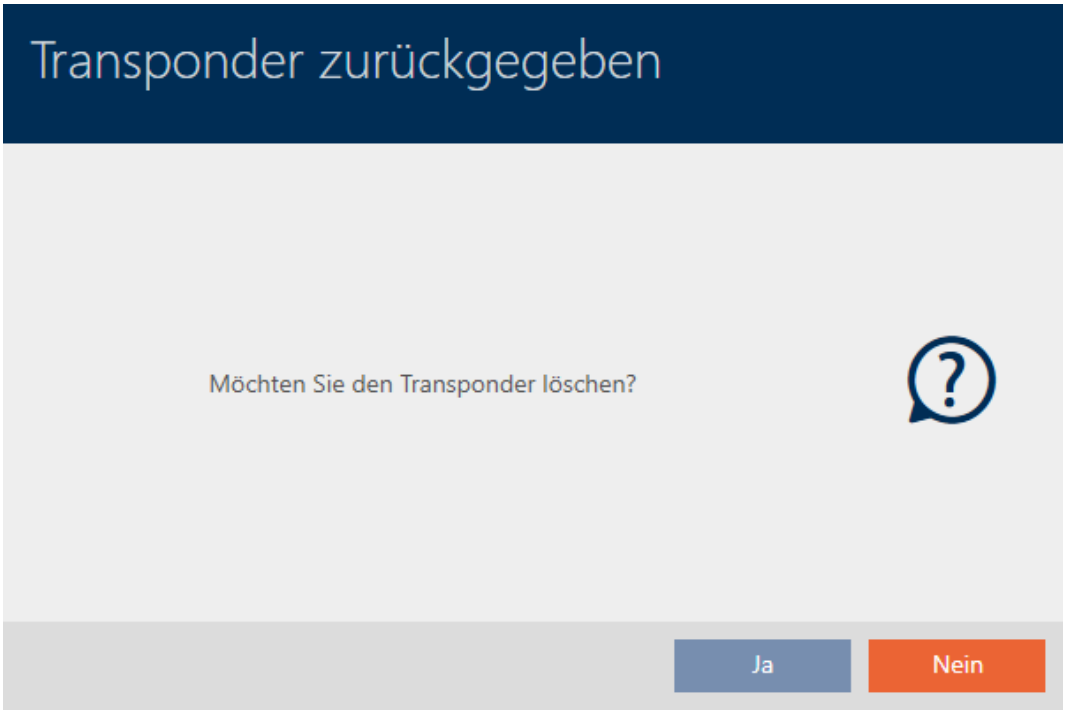


2. Click on the Next button.
   ↳ Confirmation dialogue about resetting the identification medium will open.

3. Click on the Yes button.
   ↳ Confirmation dialogue for resetting the identification medium closes.
   ↳ Identification medium is being reset.

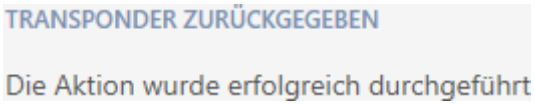


↳ Confirmation dialogue for deleting the identification medium will open.



4. Click on the No button.
   ↳ Confirmation dialogue for deleting the identification medium closes.

↳ Identification medium is reset, but not deleted.



The successful return is noted in the identification medium's action list (also see *Planning and logging card/transponder return [▸ 167]*).

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 Planning and tracking identification medium management tasks

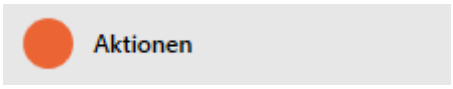
The central point for managing your identification medium is the "Transponder - Actions" tab . The following entries are displayed here collectively:

- Created
- Programming
- Issued
- Scheduled battery change
- Last battery change
- Planned return
- Handed back

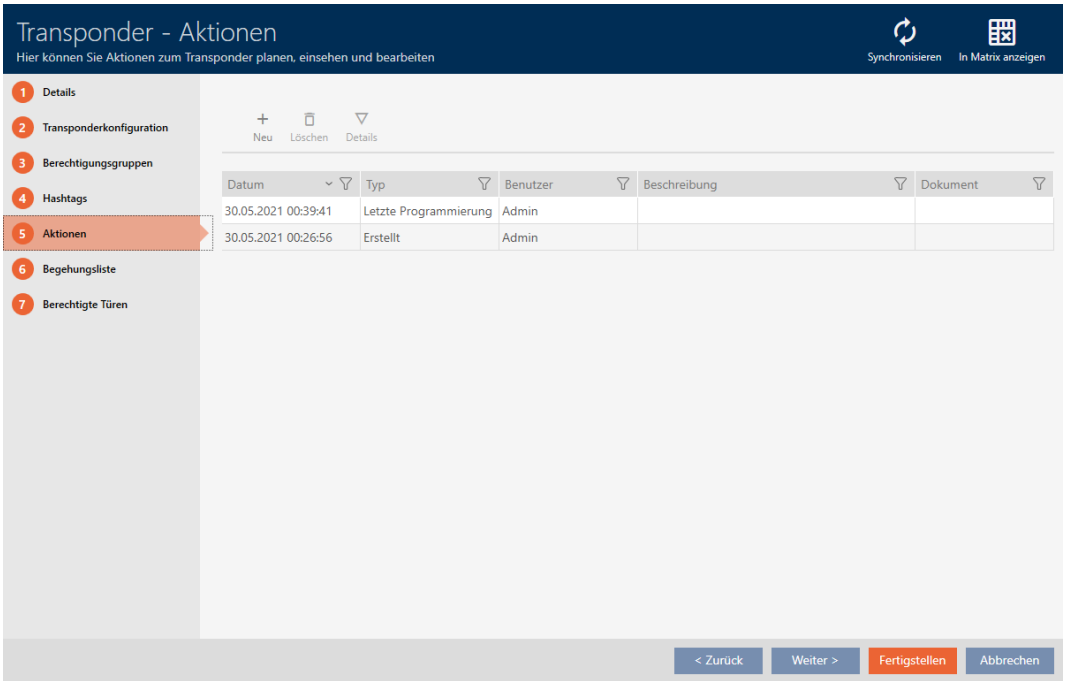
Not all entries are available for all types of identification medium. Since a PIN cannot be withdrawn like a transponder, for example, the entries "Planned return" and "Handed back" are not available for PIN code keypads.

✓ AXM Lite open.
✓ Identification media list or matrix open.
✓ Identification medium available.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the identification medium you wish to manage.
   ↳ The identification medium window will open.
3. Click on the Actions tab.



↳ Window switches to the "Actions" tab.



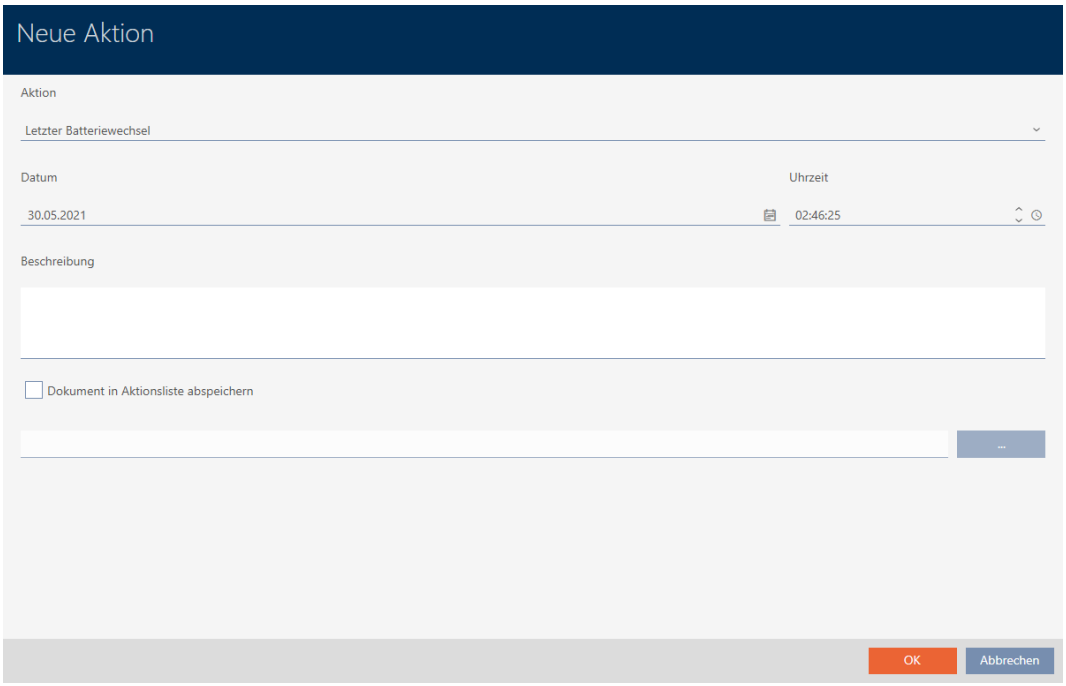
4. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

15.13.1 Noting the issue date

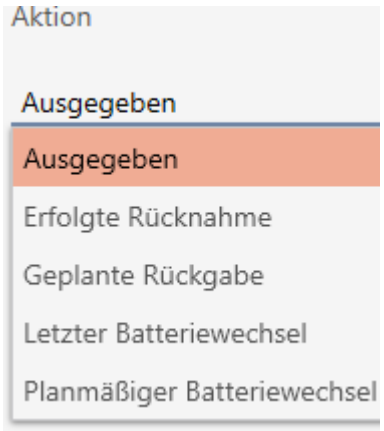
15.13.1.1 Note card/transponder issue date

AXM Lite does not know when you handed over the identification medium. You can thus enter this information manually for each identification medium.

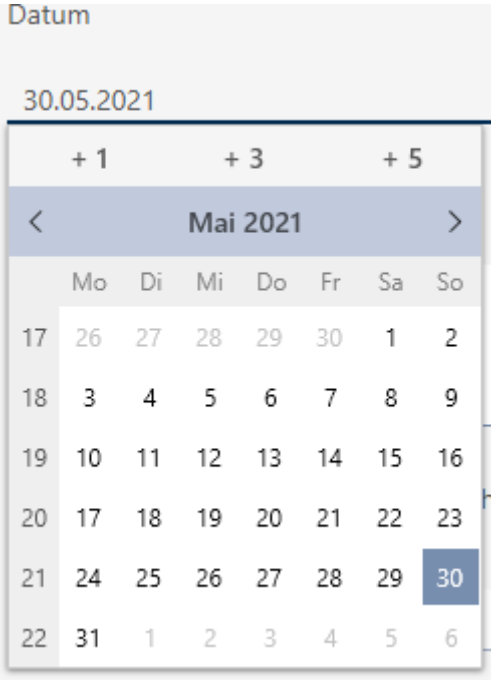
1. Click on the + New button.
   ↳ The window for a new action will open.



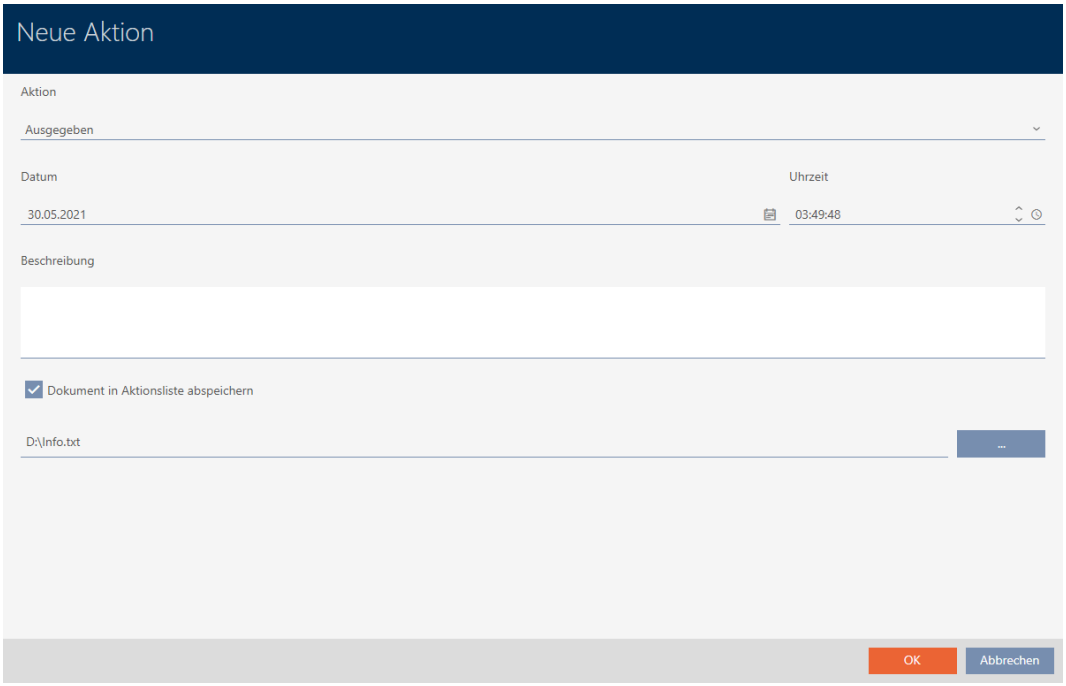
2. From the drop-down menu ▼ **Action**, select "Issued".



3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.
7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.



10. Click on the OK button.
    ↳ The window for the new action closes.

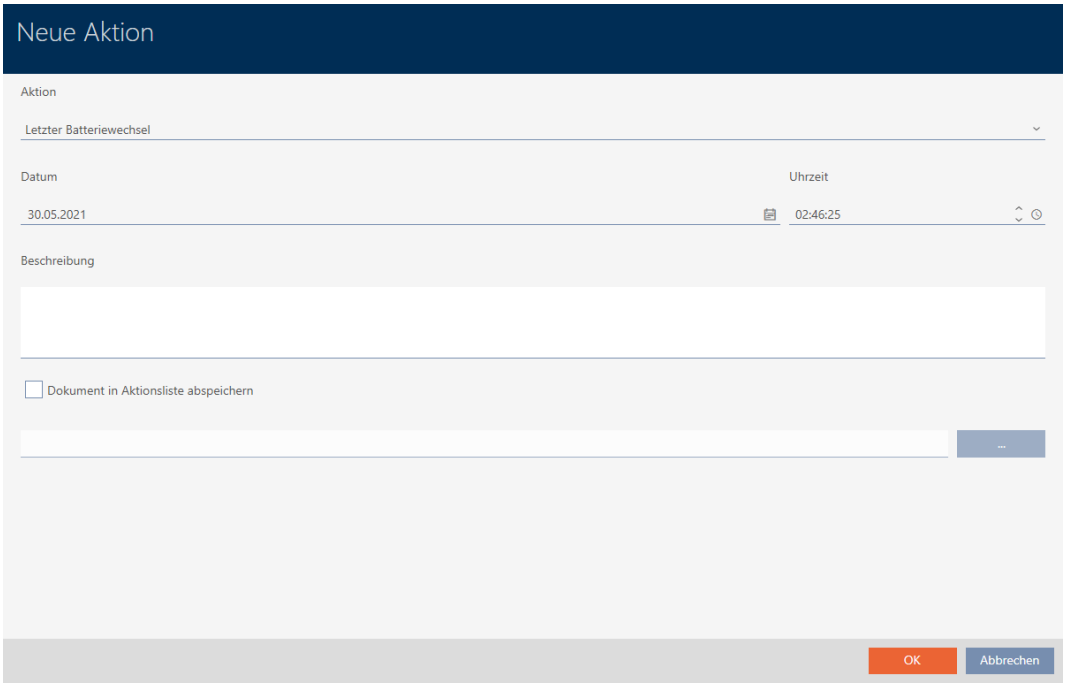
↳ Action is now created and listed.

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		

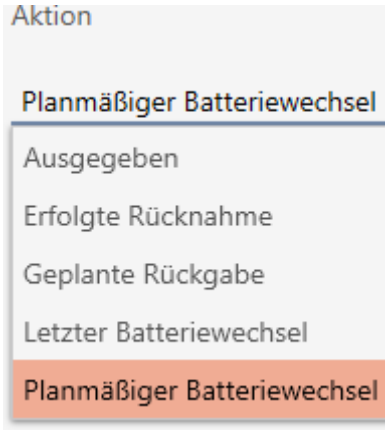
15.13.2 Planning and logging battery replacement

15.13.2.1 Planning and logging card/transponder battery changes

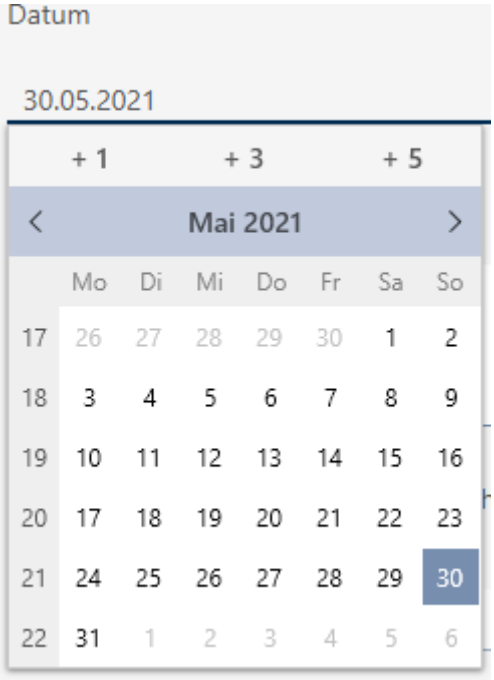
1. Click on the + New button.
    ↳ The window for a new action will open.



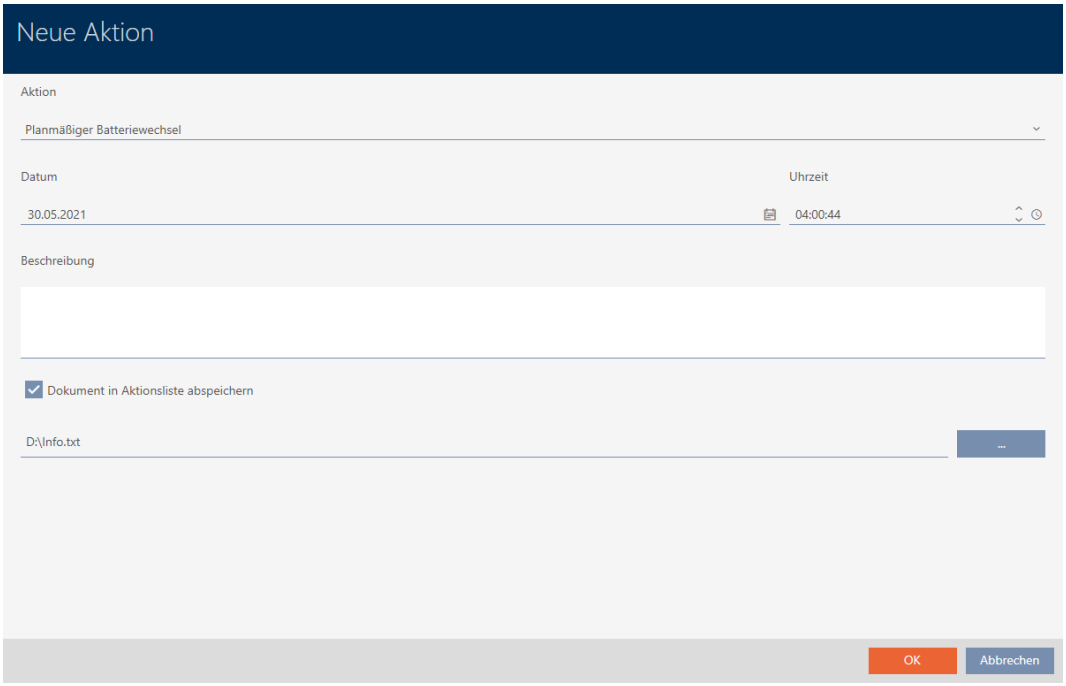
2. Select "Scheduled battery change" or "Last battery change" from the ▼ **Action** drop-down menu.



3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.
7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.



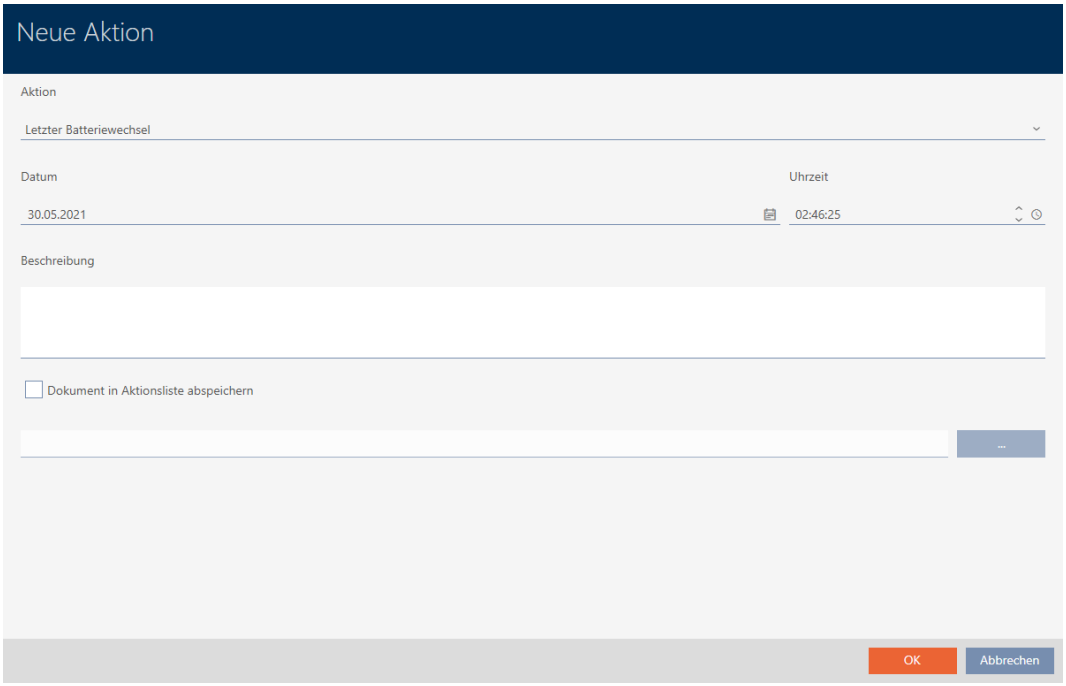
10. Click on the OK button.
    ↳ The window for the new action closes.

↳ Action is now created and listed.

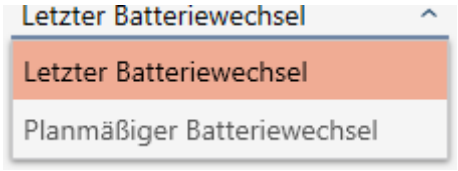
Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 04:00:44	Planmäßiger Batteriewec	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14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

15.13.2.2 Planning and logging PIN code keypad battery replacement

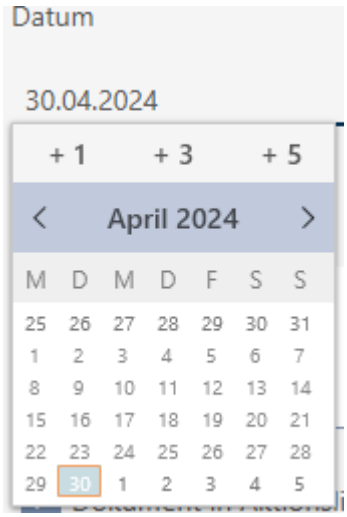
1. Click on the + New button.
    ↳ The window for a new action will open.



2. Select "Scheduled battery change" or "Last battery change" from the ▼ **Action** drop-down menu.

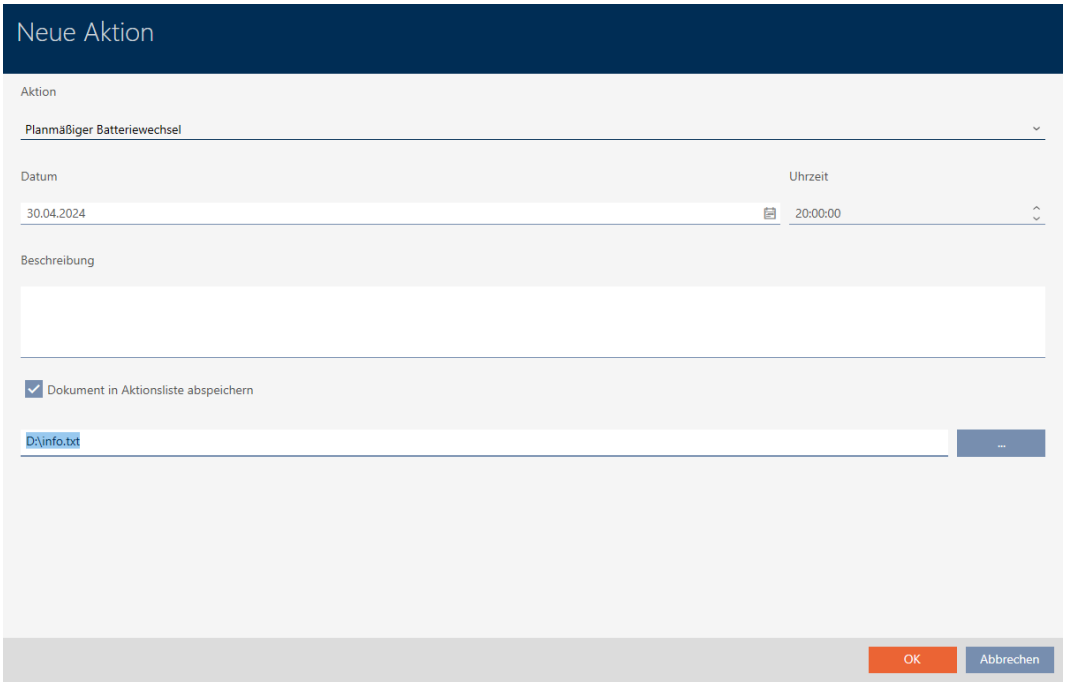


3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.

7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.



10. Click on the OK button.
    ↳ The window for the new action closes.

↳ Action is now created and listed.

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	

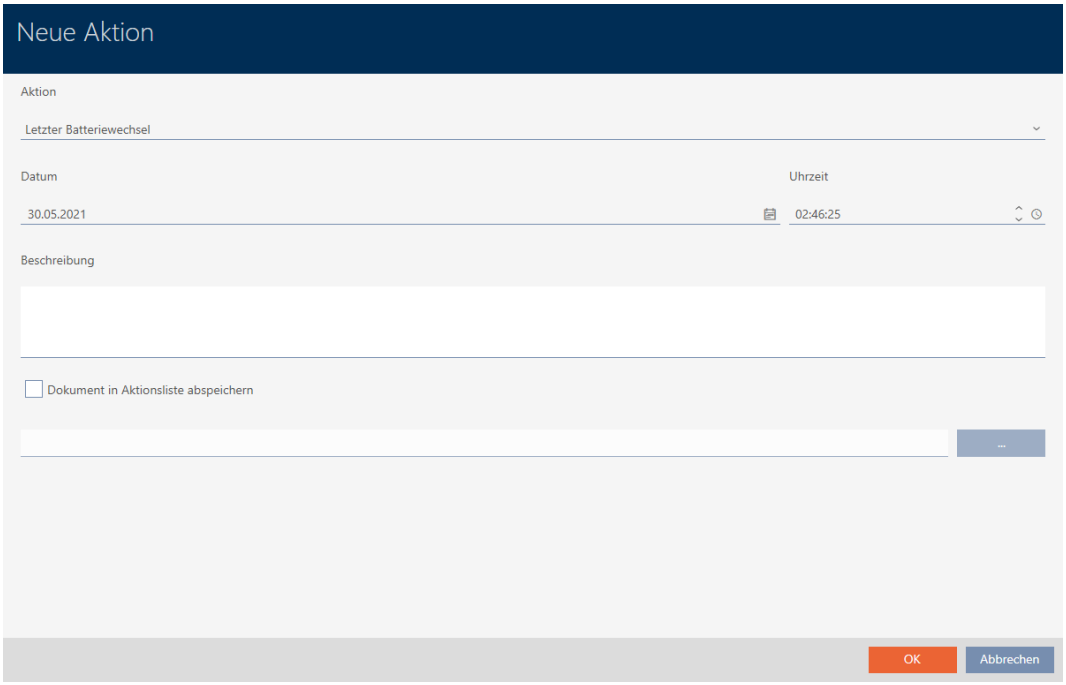
15.13.3 Planning and logging return

15.13.3.1 Planning and logging card/transponder return

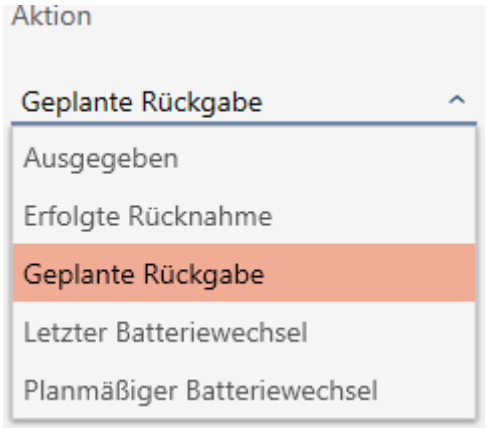
You can enter a suitable note in the action list to keep track of when which identification media need to be returned.

You can also enter when an identification medium was actually returned in the action list. However, you need to reset the identification medium manually in this case. The return wizard is ideal for returns instead of a manual reset: *Flagging and resetting returned card/transponder (back to inventory) [▸ 156]*. The entry in the action list is the same in the end, regardless of whether it is entered with or without a wizard.

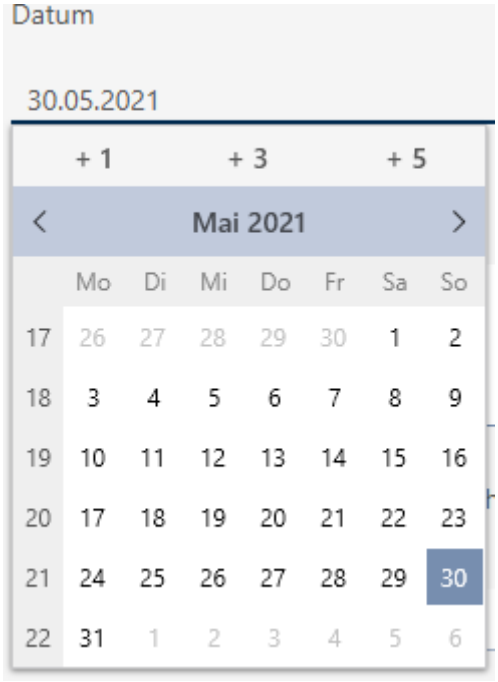
1. Click on the + New button.
   ↳ The window for a new action will open.



2. Select "Planned return" or "Handed back" from the ▼ **Action** drop-down menu.



3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.
7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.

10. Click on the OK button.
    ↳ The window for the new action closes.

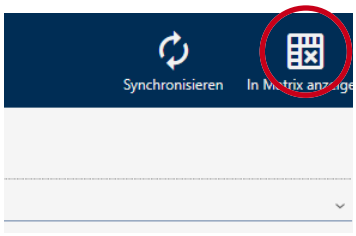
↳ Action is now created and listed.

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 Finding the identification medium or locking device again in the matrix

Various options are available to you to access the settings for your identification media and locking devices. Sometimes you need to quickly jump back to the entry in the matrix to make a final quick change to an authorisation, for example.

The settings window always provides you with the following button: Show in matrix



This button:

1. Always opens the matrix view.
2. Selects the identification medium or locking device entry.

This means you can immediately see which identification medium or locking device is meant.

15.15 Exporting identification media as a list

All identification media in your locking system can be exported as PDF files.

The PDF displays exactly the same identification media in exactly the same order as in AXM Lite.

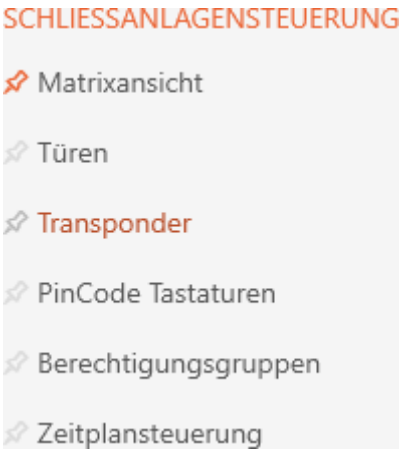
This means that you can sort and filter the display before exporting. It also allows you to sort and filter the exported list.

15.15.1 Export cards/transponders as a list

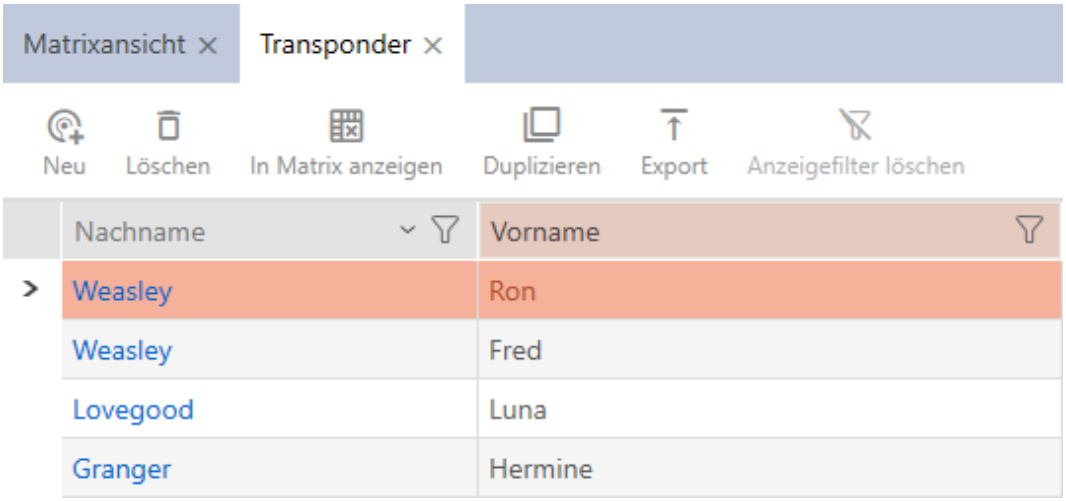
✓ AXM Lite open.
✓ Identification medium available.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Transponder entry in the | LOCKING SYSTEM CONTROL | group.



↳ The list with all identification media in the locking system will open.



3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Click on the Export button ⤒.
   ↳ The Explorer window will open.
5. Save the PDF file to a directory of your choice.

↳ Displayed identification media are exported as PDF files (DIN A4).

Alle Transponder für die Schließanlage 'Hogwarts' - gefiltert

Nachname	Vorname	S/N	Typ	Sync	Status	Zeitgruppe	Aktivierungs-datum / Verfallsdatum
Weasley	Ron		Transponder	Erstprogrammierung			
Weasley	Fred		Transponder	Erstprogrammierung			
Lovegood	Luna		Transponder	Erstprogrammierung			

Gedruckt am: 05.05.2021 1

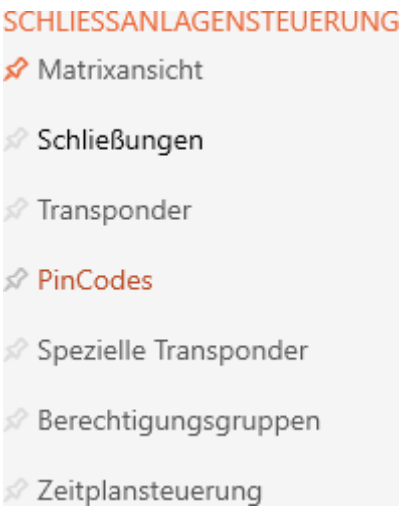
15.15.2 Exporting PINs and PIN code keypads as a list

✓ AXM Lite open.

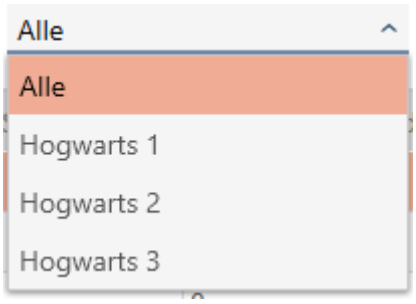
✓ PIN code keypad created (see *Creating PIN code keypads [▸ 83]*).

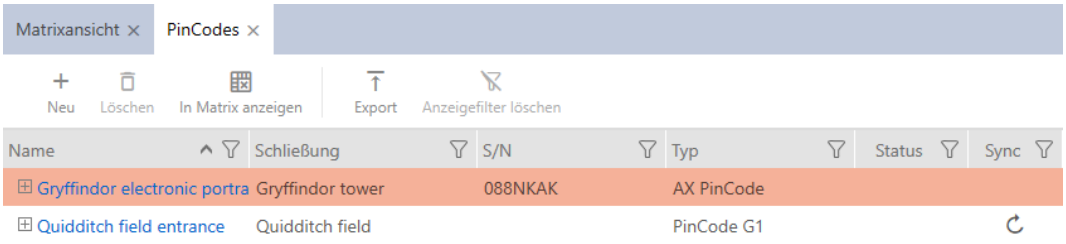
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the PinCodes entry in the | LOCKING SYSTEM CONTROL | group.



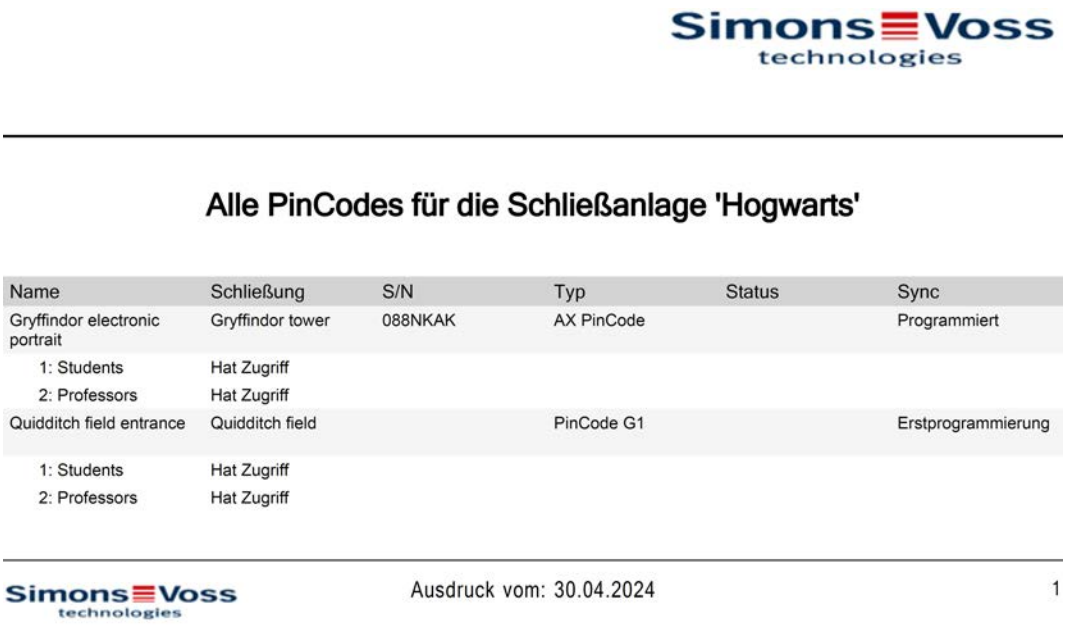
   ↳ The list with all PIN code keypads in the locking system will open.





3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Click on the Export ⤒ button.

↳ Displayed identification media are exported as PDF files (DIN A4).



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

15.16 Viewing an identification medium's serial number and/or TID

15.16.1 Viewing a card's/transponder's serial number and TID

Your cards and transponders have two numbers that are important:

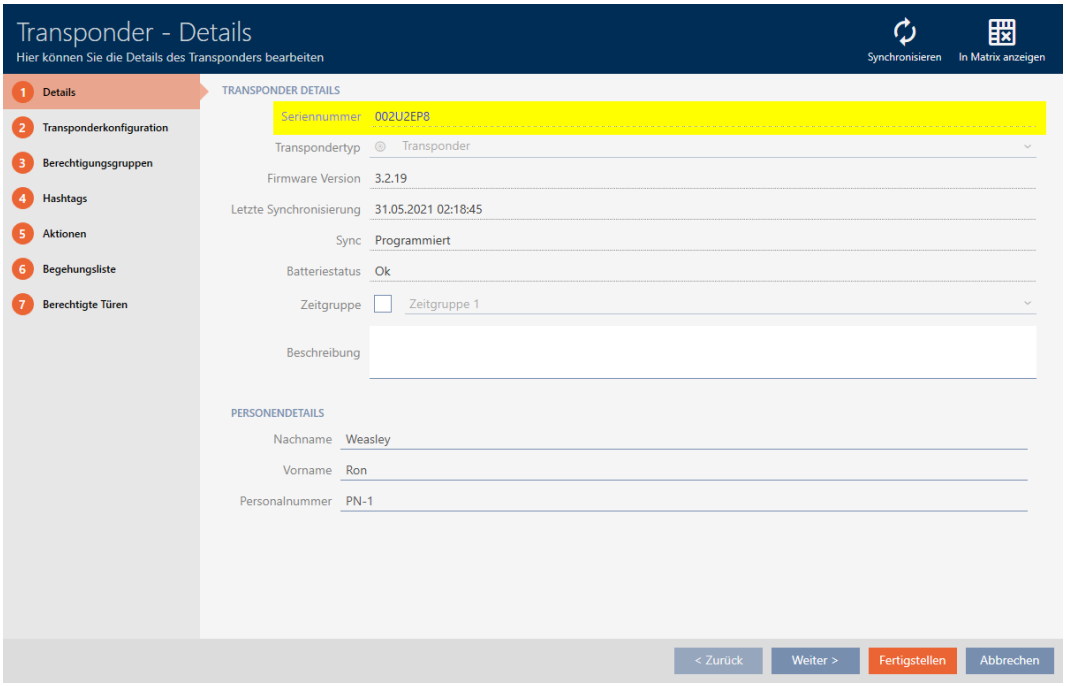
- Serial number (permanently stored in the identification medium and imported during synchronisation)
- TID (flexibly assigned by AXM Lite and written on the identification medium during synchronisation)

The serial number is a unique number for each identification medium while the TID is only unique in your locking system.

If you need the TID for support purposes, for example, you can view the TID for synchronised identification media in the synchronisation window:

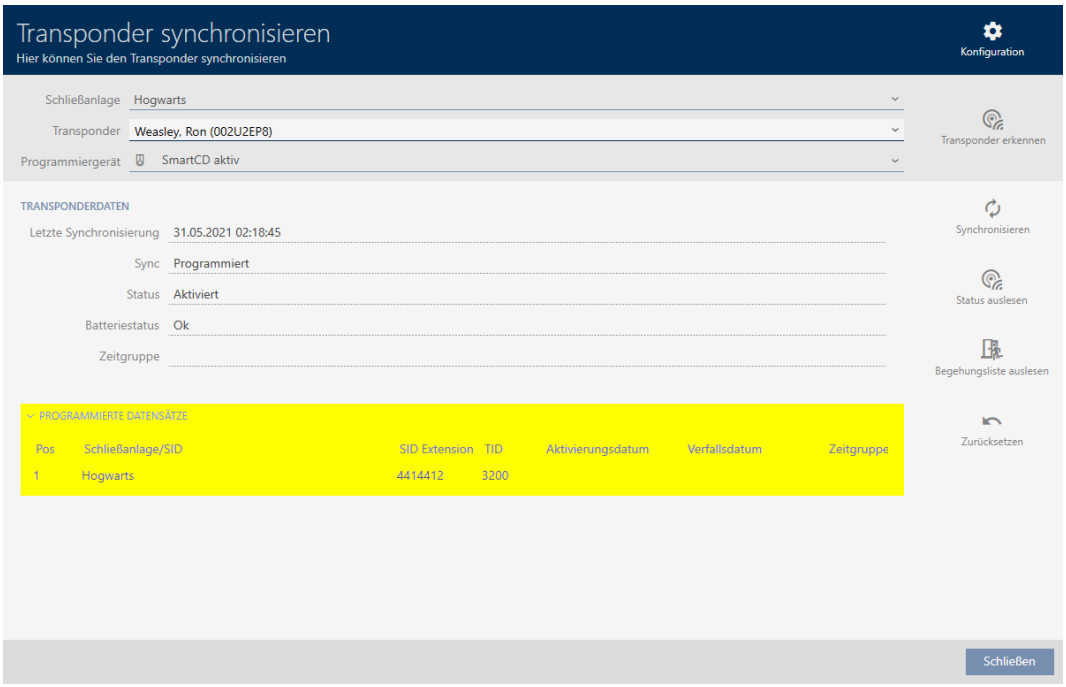
✓ AXM Lite open.
✓ Identification media list or matrix open.
✓ Identification medium synchronised.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the identification medium whose serial number and/or TID you wish to view.
   ↳ The identification medium window will open.
   ↳ Serial number is displayed.



3. Click on the ↻ Synchronisation button.
   ↳ Window switches to synchronisation.

4. Open up the "Programmed records" field.



↳ TIDs are displayed in table. If you use the identification medium in a number of locking systems, the TID used for each locking system is displayed.

15.16.2 Viewing a PIN code keypad's serial number

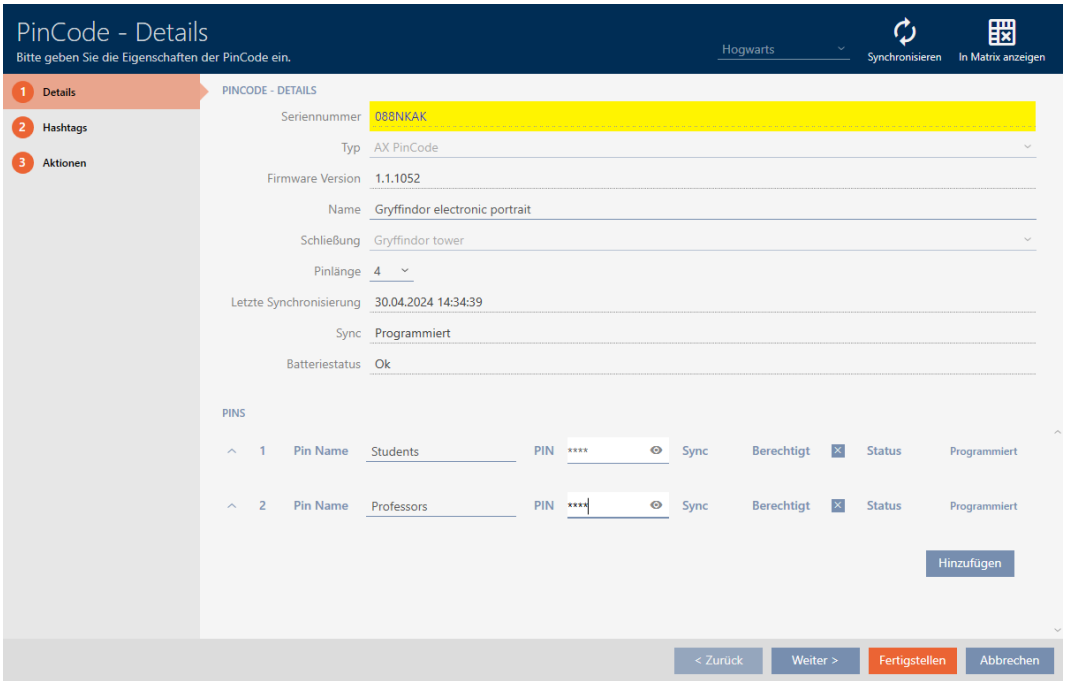
Your PIN code keypads do not have TIDs which are directly visible. You will find the serial number similar to that for cards and transponders in the details:

✓ AXM Lite open.
✓ PIN code keypad created and synchronised.
✓ List with PIN code keypads or matrix open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

2. Click on a PIN associated with the PIN code keypad whose serial number you want to view.

↳ The PIN code keypad window will open.
↳ Serial number is displayed.



15.17 Setting the PIN length (PinCode AX)

NOTE

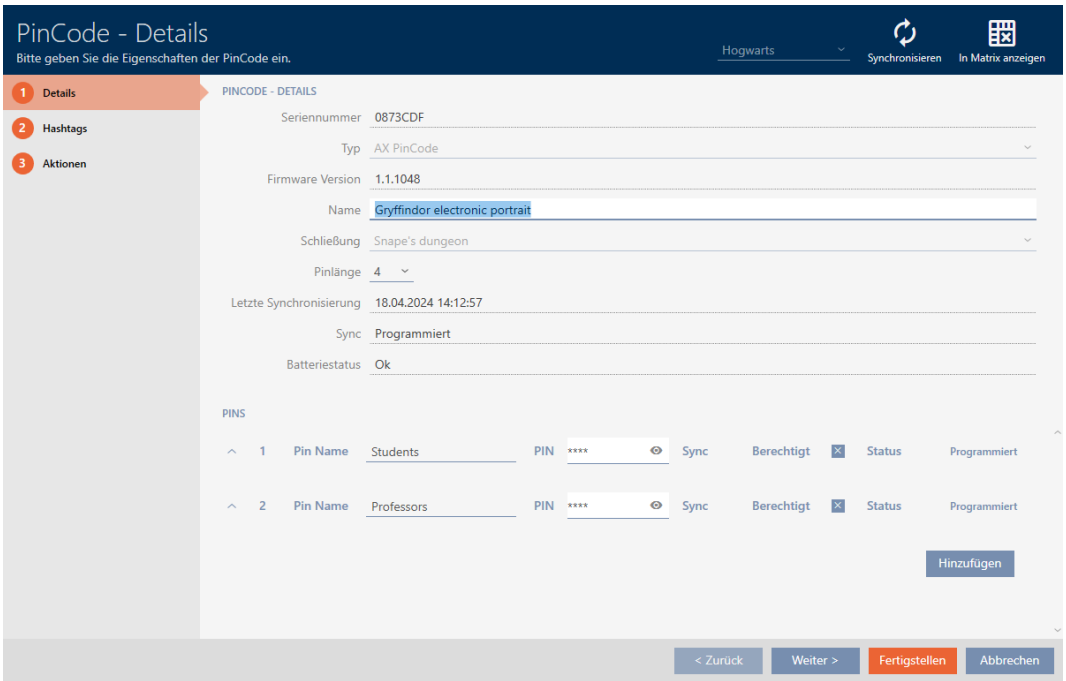
Description only valid for PIN code keypad AX

The setting described here is only available for the PIN code keypad AX in yourAXM Lite. On the PIN code keypad 3068, you can use the Master PIN to change this setting directly on the PIN code keypad 3068.

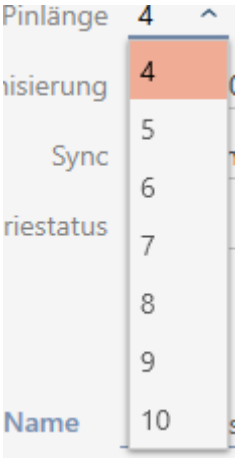
You always set the PIN length for the entire PIN code keypad AX, i.e. for all PINs simultaneously. For this reason, you must then reassign each PIN and synchronise the PIN code keypad AX.

✓ AXM Lite open.
✓ Matrix screen open.
✓ PIN code keypad AX created (see *Creating PIN code keypads [▸ 83]*).

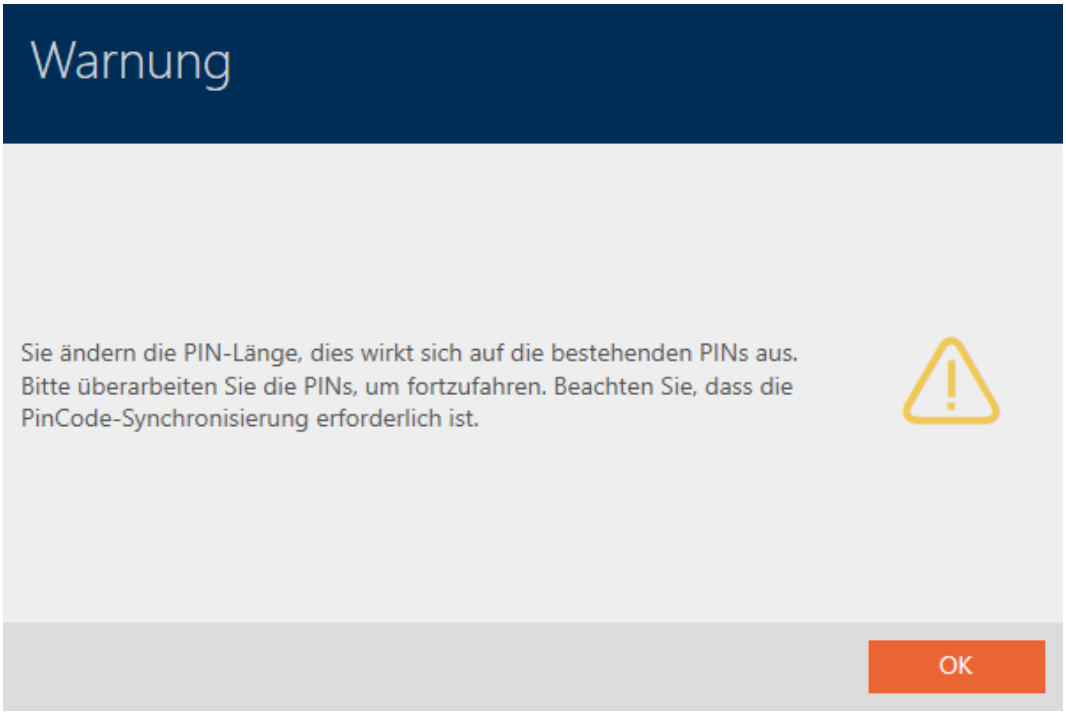
1. Click on any PIN to open details on your PIN code keypad AX.
   ↳ The "PinCode - Details" window will open.



2. Select the required PIN length from the ▼ **Pin length** drop-down menu.

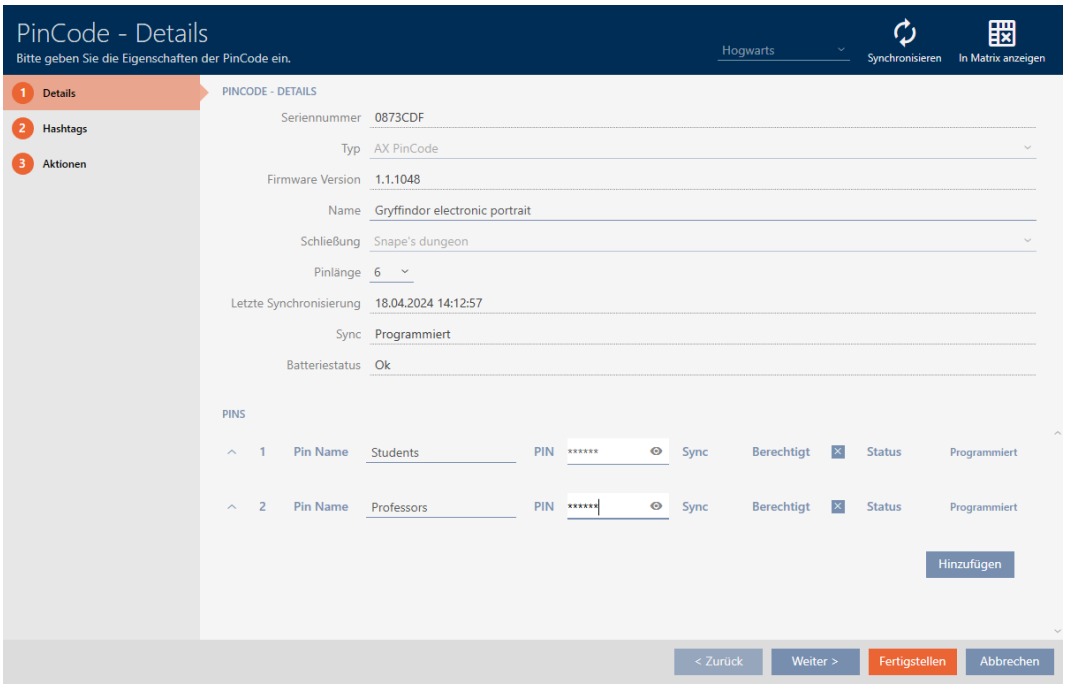


↳ Your AXM Lite will alert you to the upcoming workload.



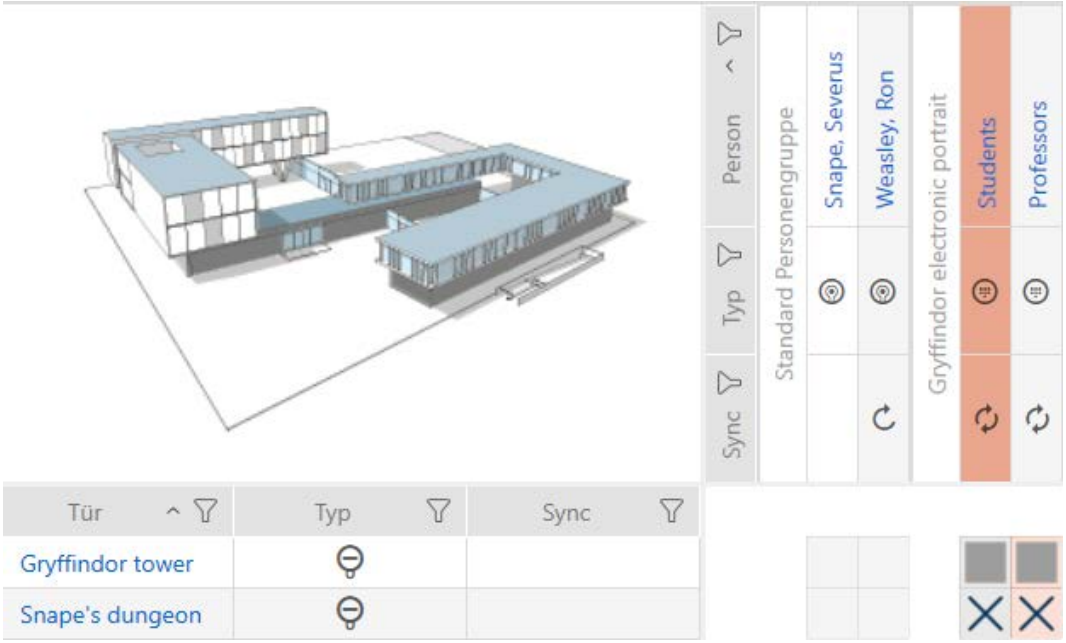
3. Click on the OK button.
   ↳ All PINs are red and must be reassigned.

4. Reassigning the PINs.



5. Click the Finish button.
   ↳ "PinCode - Details" window closes.

↳ The PIN length and PINs have been changed and the resulting programming requirement is displayed in the matrix.



15.18 Changing a PIN (PinCode AX)

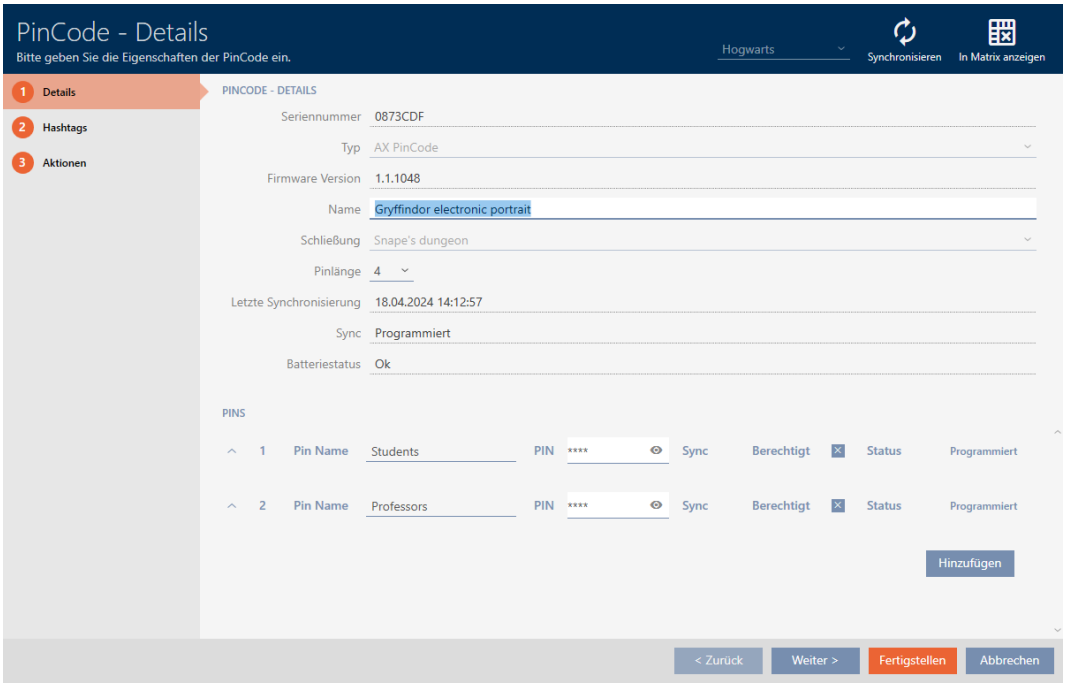
NOTE

Description only valid for PIN code keypad AX

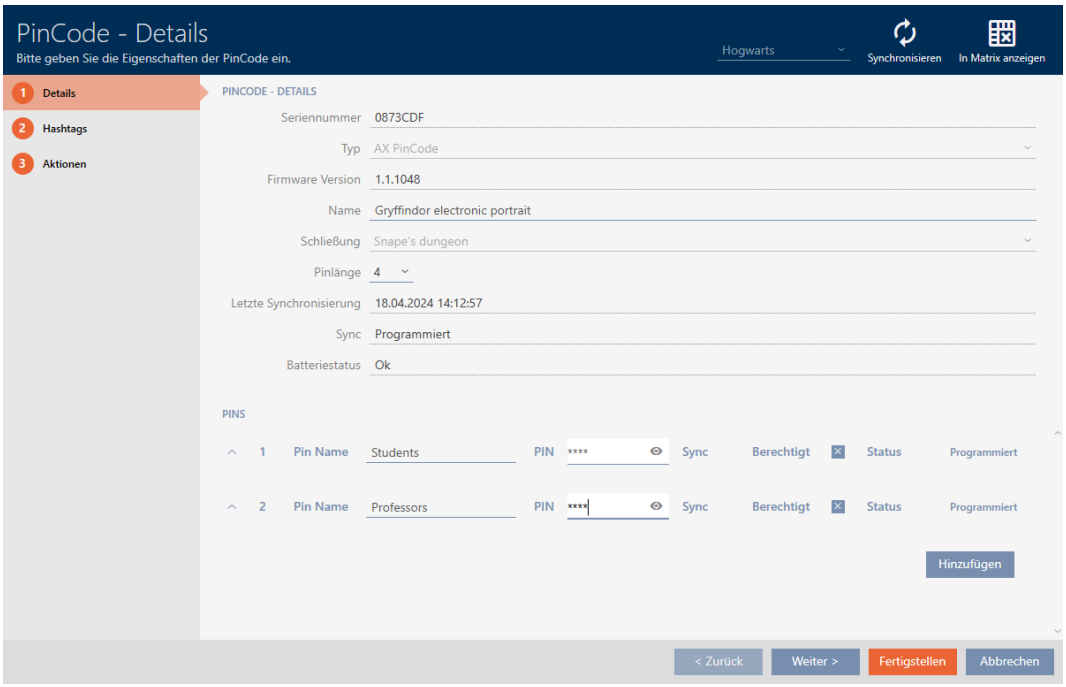
The setting described here is only available for the PIN code keypad AX in yourAXM Lite. On the PIN code keypad 3068, you can use the Master PIN to change this setting directly on the PIN code keypad 3068.

✓ AXM Lite open.
✓ Matrix screen open.
✓ PIN code keypad AX created (see *Creating PIN code keypads [▸ 83]*).

1. Click on any PIN to open details on your PIN code keypad AX.
   ↳ The "PinCode - Details" window will open.



2. Enter the new PIN in the appropriate *Pin name* field.



3. Click on the Finish button.

↳ PIN has been changed and the resulting programming requirement is displayed in the matrix.

16. Doors and locking devices

Any changes you make to the locking system will only take effect when synchronised (see *Synchronising the locking device (including reading access list) [▸ 291]*).

16.1 Creating a locking device

Depending on the type of locking device, locking devices can be:

- Engaged to open with an identification medium. The user can then open the door with the locking device (cylinder, SmartHandle).
- An identification medium can be used to unlock the device, i.e. the dead bolt retracts without user intervention. The user can then open the door (SmartLocker).
- Activated with an identification medium. The switch contact can then open a door (SmartRelay).

See *"Engaging", "opening", "locking", etc. [▸ 362]* for more information on this topic.

In line with best practice requirements (see *Best practice: setting up the locking system [▸ 29]*), SimonsVoss recommends that you first plan things out in preparation:

- *Access levels [▸ 261]* (see *Access levels [▸ 378]* for background information)
- *Creating a schedule [▸ 45]* or *Create time group [▸ 49]* (see *Time groups and schedules [▸ 366]* for background information)
- *Creating a time switchover [▸ 58]* (see *Time switchovers [▸ 370]* for background information)
- *Creating a location [▸ 69]* or *Creating a building and assigning it to a location [▸ 72]* (see *Buildings and locations [▸ 379]* for background information)
- *Creating a hashtag [▸ 74]* (see *Hashtags [▸ 380]* for background information)

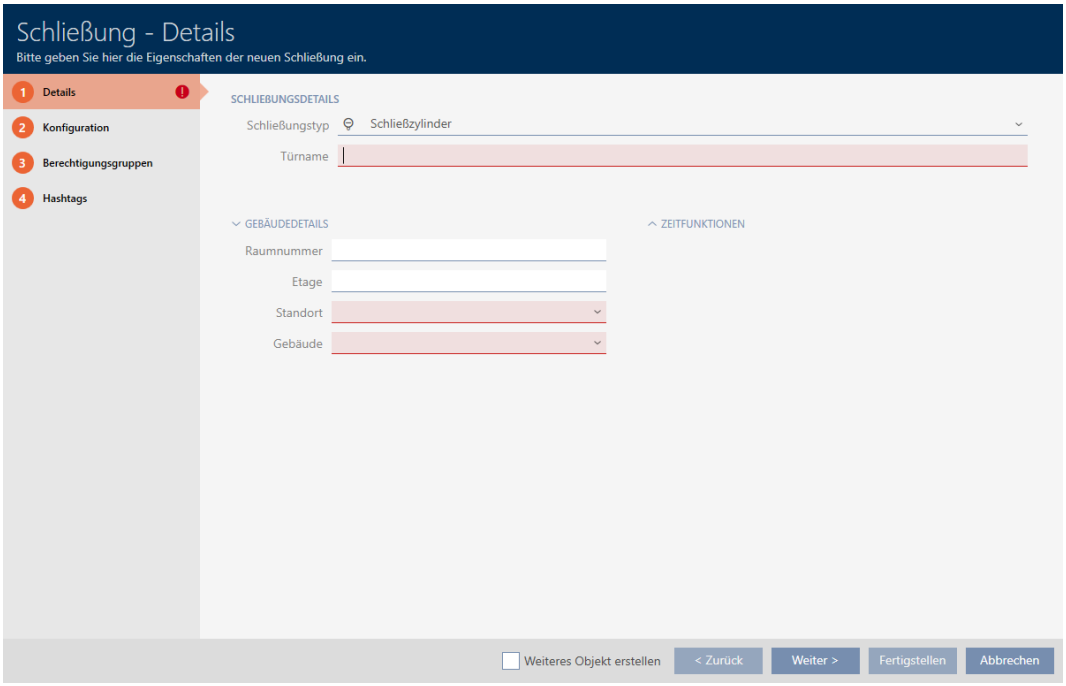
NOTE

Hidden settings

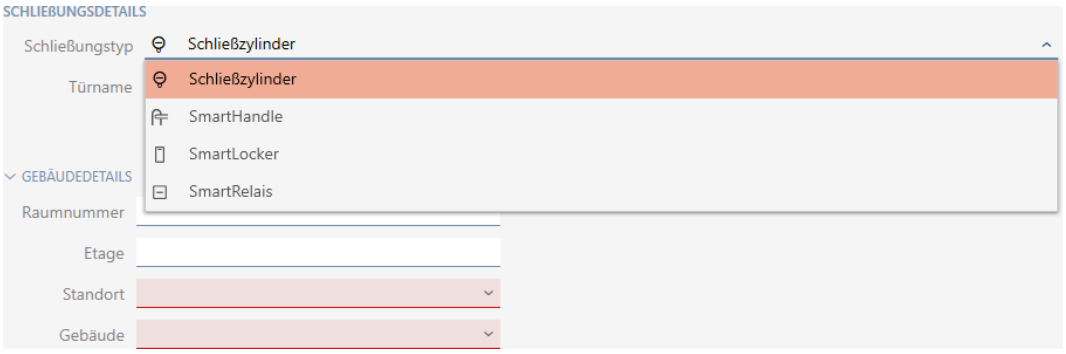
As soon as you have created the locking device and clicked on the Fertig-stellen button, AXM Lite knows your locking device type. It will then hide all non-relevant settings.

✓ AXM Lite open.

1. Click on the New lock button.
   ↳ The window for creating a new locking device will open.

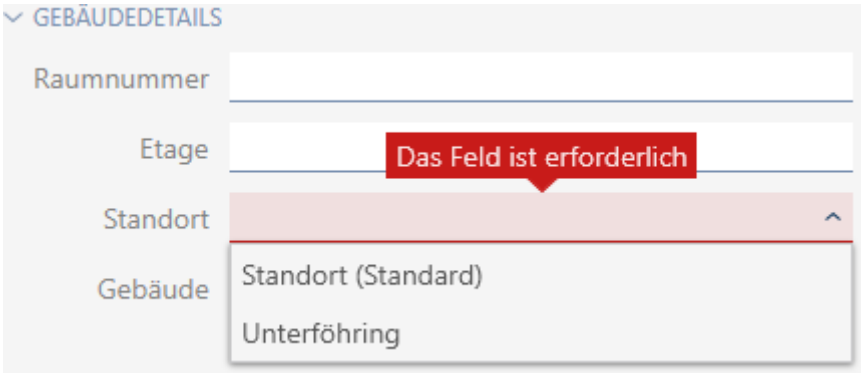


2. Select which locking devices you wish to create from the ▼ **Lock type** drop-down menu.



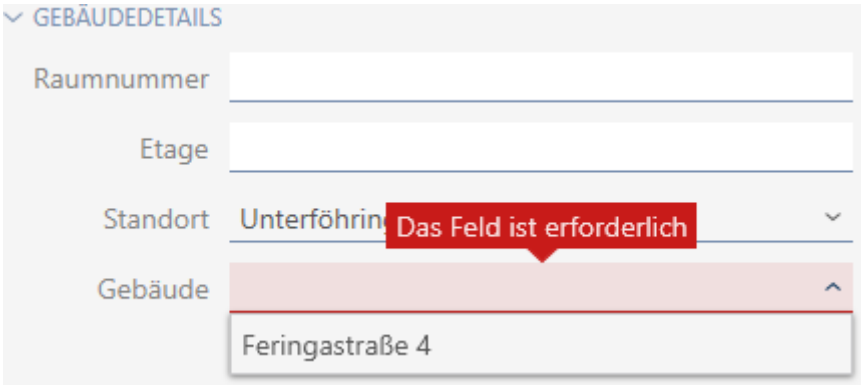
3. Enter the name of the door where your locking device will be installed in the *Door name* field.
4. If necessary, enter the number of the room where your locking device will be installed in the *Room number* field.
5. If necessary, enter the floor on which your locking device will be installed in the *Floor* field.

6. Select the location where your locking device will be installed from the ▼ **Location** drop-down menu.



   ↳ Selection in the ▼ **Building** drop-down menu is limited to the buildings in the selected location.

7. Select the building where your locking device is installed from the ▼ **Building**drop-down menu.



8. If you wish to use time functions: Expand the "Time functions" menu and make the settings (see *Limiting authorisations for locking devices to specific times (schedule) [▸ 220]* and *Engaging and disengaging locking devices automatically with time switchover [▸ 222]* for details).

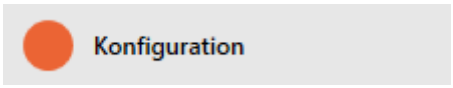
NOTE

Public holiday lists in locking device and locations

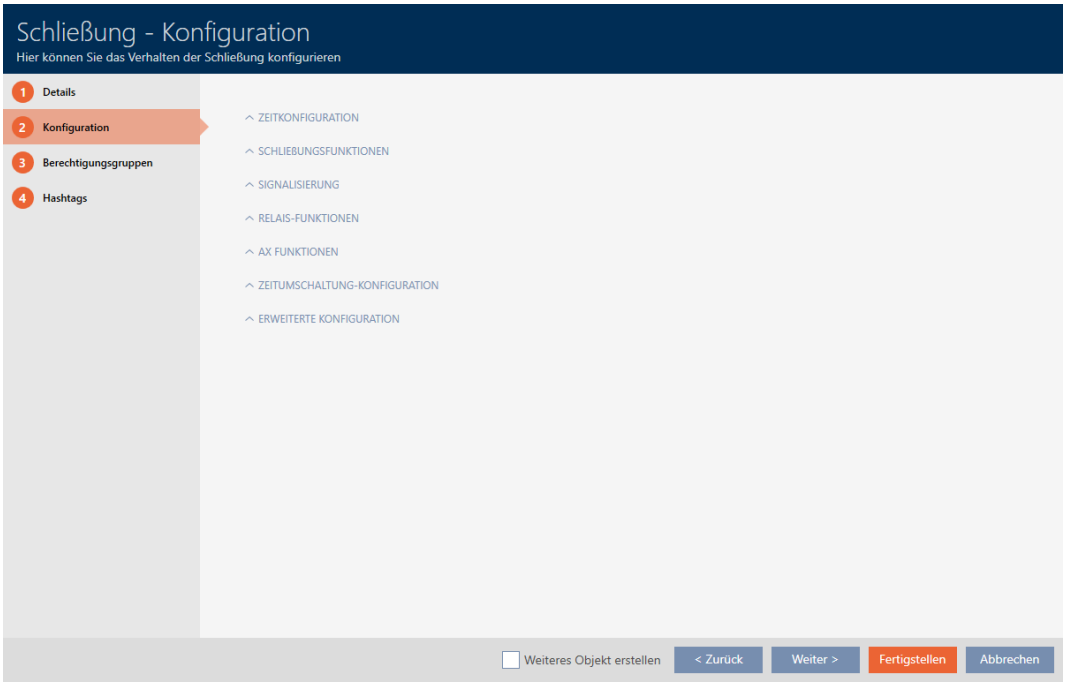
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

If a public holiday list is assigned to the location instead of the locking device, the public holiday list for the location is applied to the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

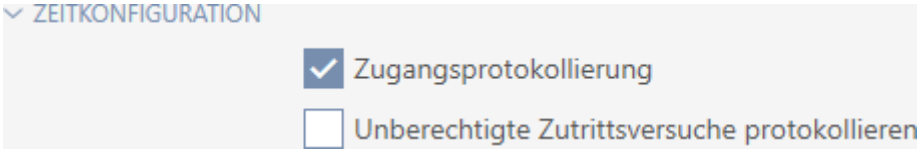
9. Click on the Configuration tab.



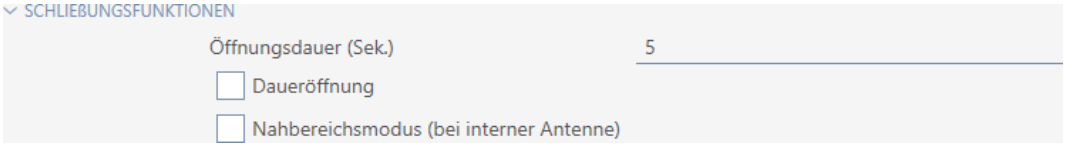
↳ Window switches to the "Configuration" tab.



10. If you want to log access attempts, expand the "Time configuration" menu and configure the settings (see *Have accesses logged by locking device (access list) [▸ 228]*).



11. If you want to change the opening time or use the close range mode, expand the "Lock functions" menu and configure the settings (see *Leaving the locking device open for longer, less time or permanently [▸ 229]* and *Limit locking device read range (close range mode) [▸ 231]*).

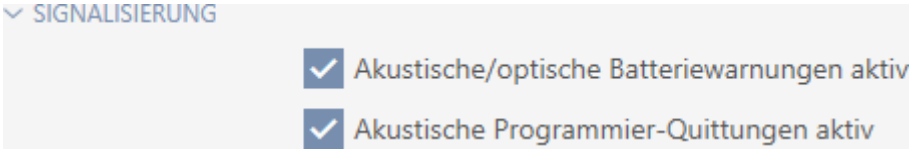


NOTE

Button control not adjustable

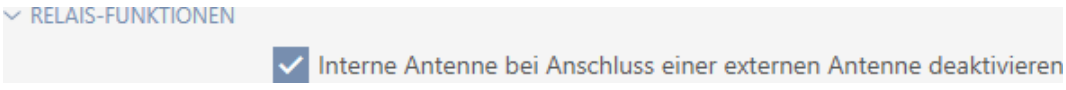
Some locking cylinders are equipped with a button on the inside thumbturn (TS option). If your AXM Lite detects such a locking cylinder, the ☑ Button control checkbox is displayed. However, this cannot be adjusted, i.e. you cannot disable the buttons.

12. If you want to change the battery warning signalling or programming acknowledgements, expand the "Feedback signals" menu and configure the settings (see *Muting a locking device (for battery warnings and programming) [▸ 233]*).



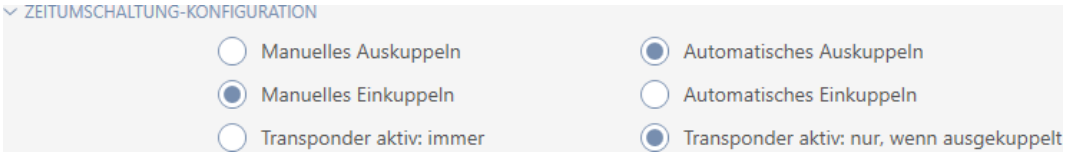
13. If you want to ignore the activation time window (see Activation date / expiry date), expand the "AX functions" menu and configure the settings (see *Ignoring activation and expiry date of identification media [▸ 234]*).

14. If you want to use the internal and external antenna together in a SmartRelay, expand the "Relay functions" menu and configure the settings (see *Using internal and external antenna simultaneously [▸ 243]*).

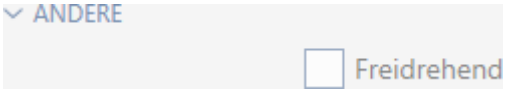


15. If you want to engage and disengage your locking device automatically, expand the "Time switching - Configuration" menu and configure the settings (see *Engaging and disengaging locking devices automatically*

with time switchover [▸ 222]).
The setting defined here applies only to this one locking device, not to the entire locking system.



16. If you want to use a freely rotating Digital Cylinder AX, expand the "Other" menu and select the ☑ Both sides free spinning checkbox.



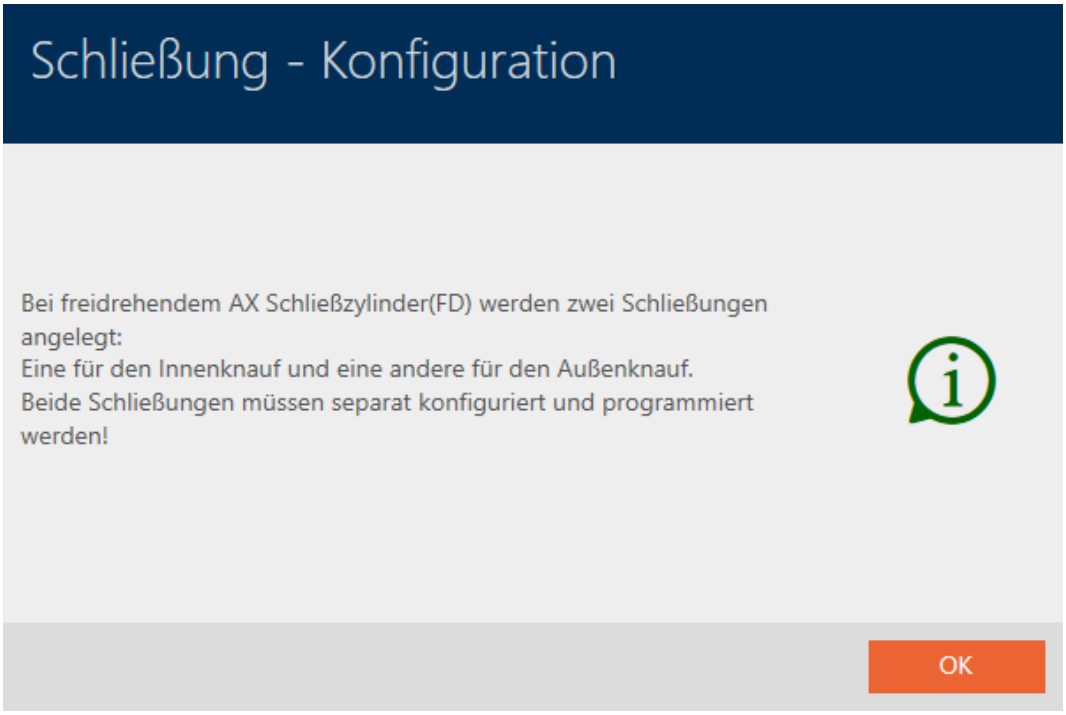
NOTE

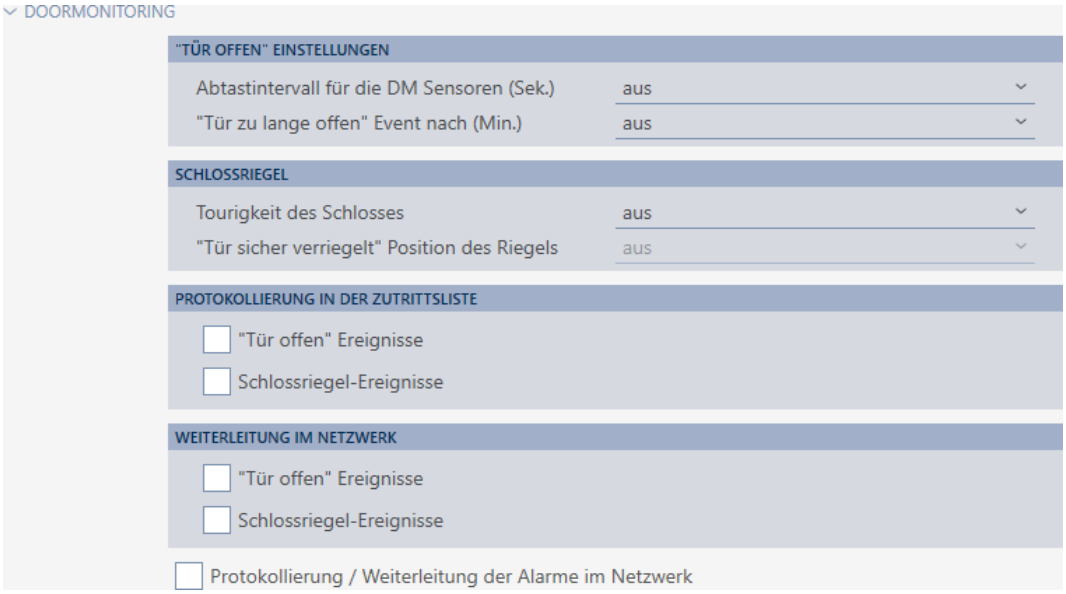
Both sides free spinning can only be selected for unprogrammed Digital Cylinder AX

Digital Cylinder AX which have already been configured cannot be reconfigured as freely rotating Digital Cylinder AX at a later stage.

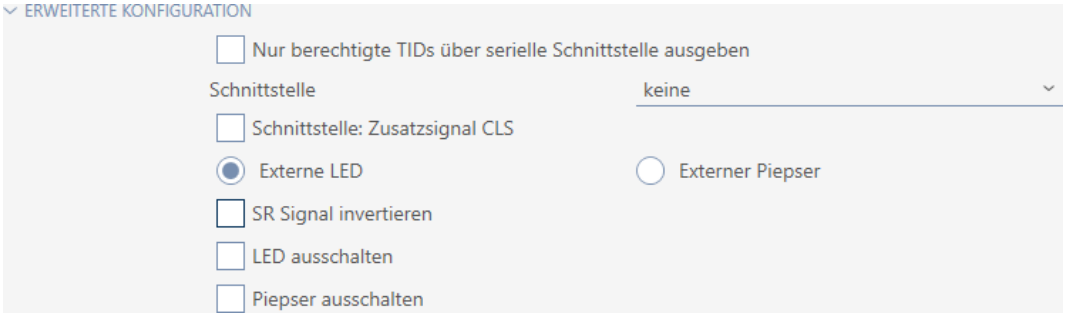
1. Duplicate the Digital Cylinder AX to get an unprogrammed copy with the same settings.
2. Select the checkbox in the ☑ Both sides free spinning section.
3. Reset the previous Digital Cylinder AX and synchronise the freely rotating copy.
4. Then delete the previous Digital Cylinder AX.

↳ AXM Lite creates a second Digital Cylinder AX and automatically selects the ☑ Close range mode checkbox for both. Both locking devices are independent of each other and must be synchronised separately.

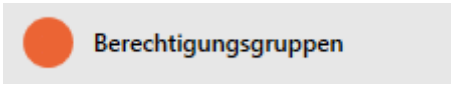




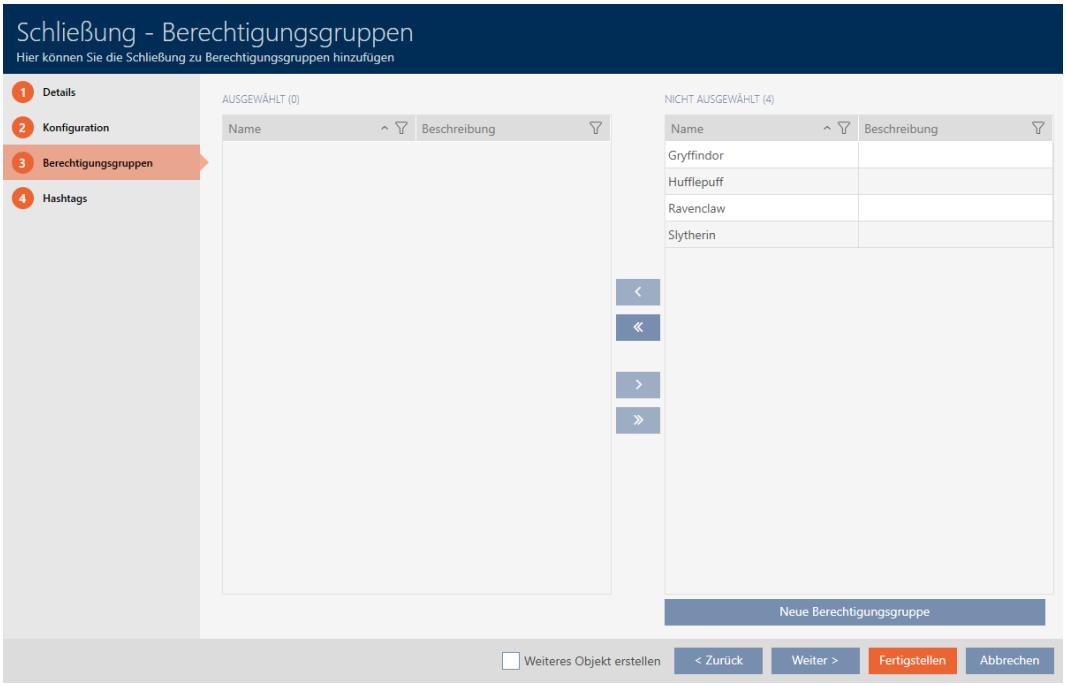
17. If you want to change the signalling on a SmartRelay or use the serial interface, expand the "Extended configuration" menu and configure the settings (see *Changing the SmartRelay settings [▸ 242]*).



18. Click on the Access levels tab.



↳ Window switches to the "Access levels" tab.



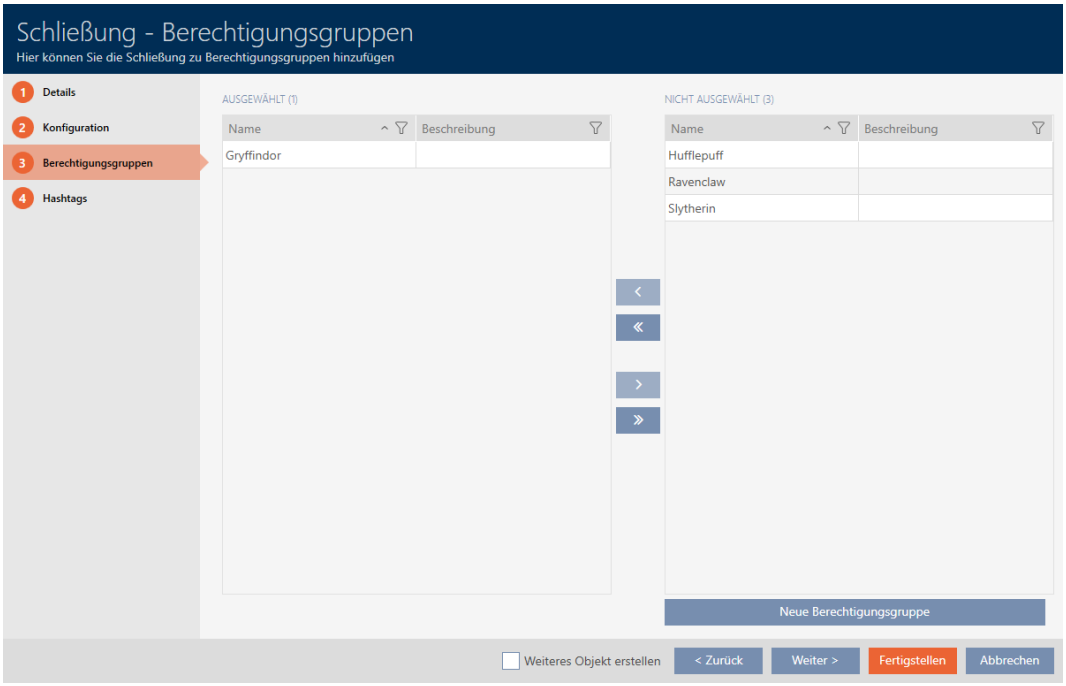
19. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
20. Select all access levels to which you wish to assign your locking device (Ctrl+click for individual groups or Shift+click for multiple groups).

NOTE

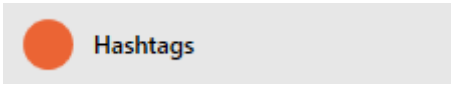
Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

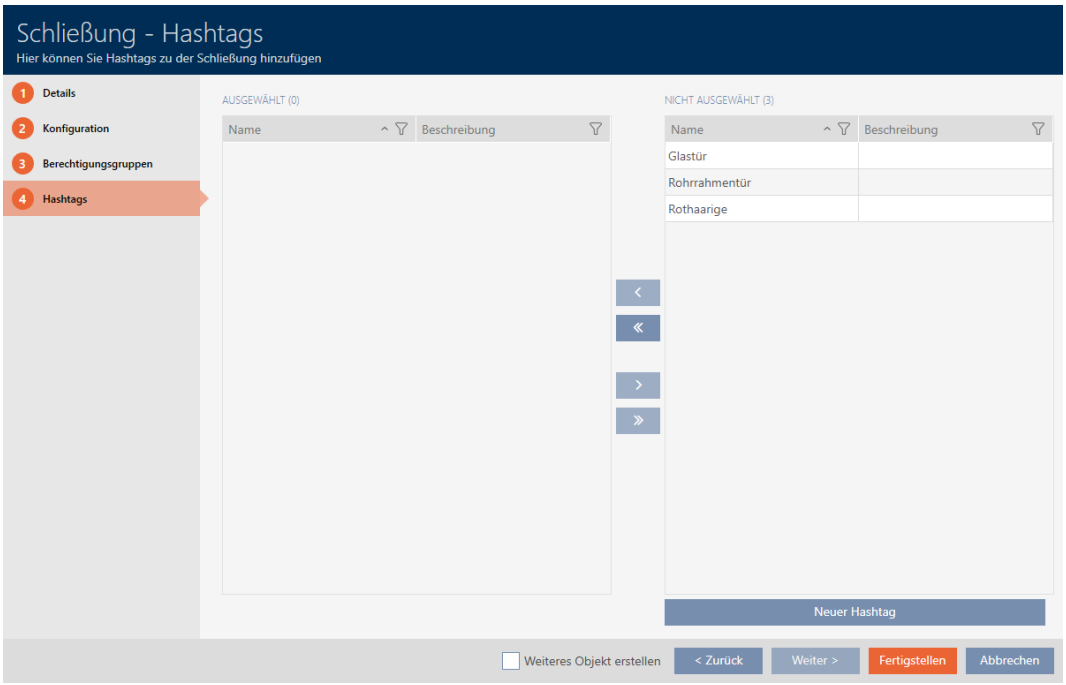
21. Use < to move the selected access levels only or << to move all displayed access levels.
    ↳ Your locking device is added to the access levels in the left-hand column.



22. Click on the Hashtags tab.



↳ Window switches to the "Hashtags" tab.



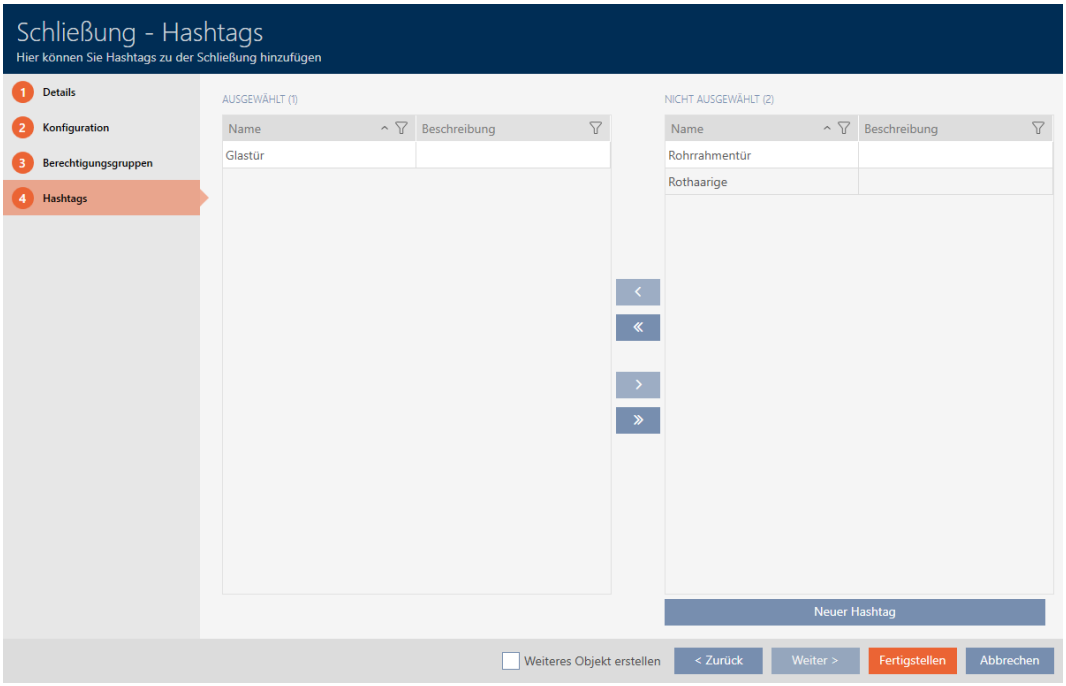
23. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
24. Select all hashtags that you wish to assign to your locking device (Ctrl+click for individual hashtags or Shift+click for multiple hashtags).

NOTE

Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

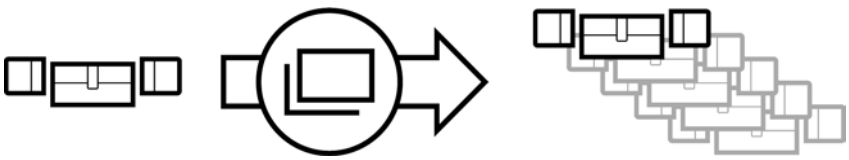
25. Use [<] to move only the selected hashtags or [<<] to move all the hashtags displayed.
    ↳ The hashtags in the left-hand column are added to your locking device.



26. Select the ☑ Create additional objects checkbox to leave the window with the same settings open for the next locking device to be created.
27. Click the Finish button to create the locking device.
    ↳ The window for creating a new locking device closes.

↳ Newly created locking device is listed or displayed in the matrix.

16.2 Duplicating the locking device (including authorisations and settings)



You can simply duplicate an existing locking device instead of creating a completely new one. During this process, AXM Lite also applies the properties, which can be changed in the AXM Lite.

The following settings are duplicated:

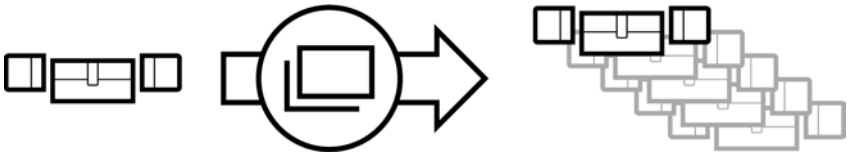
- Building details
- Door details (except door numbering, which is automatically continued with the adjustable abbreviation; also see *Changing automatic numbering [▸ 332]*)
- Time functions
- Configuration
- Access levels
- Hashtags

The following settings are not duplicated:

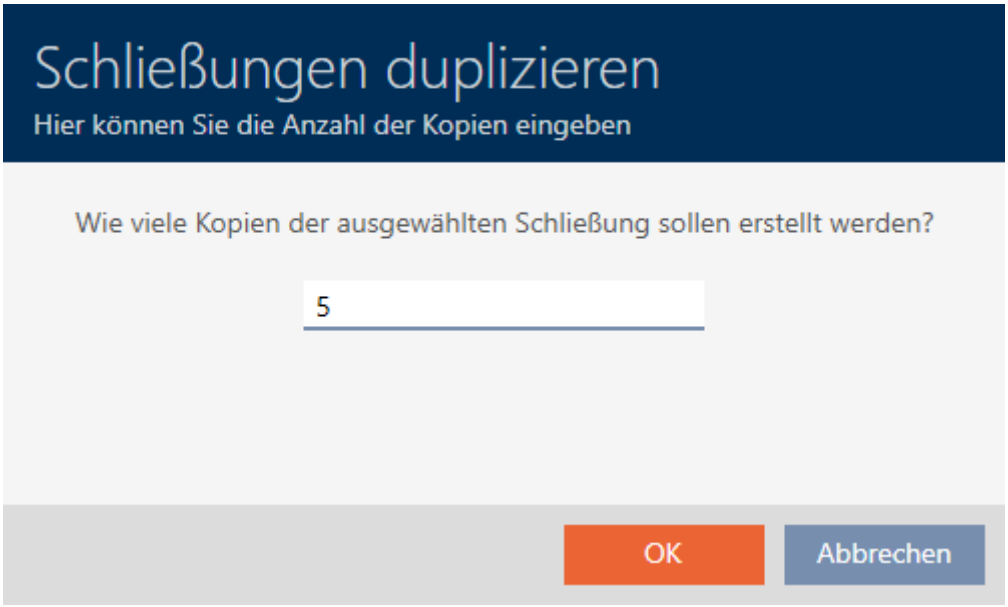
- Entries in the [Actions] tab
- Information that is stored on the hardware and imported during synchronisation:
  - Serial number
  - Firmware version
  - Battery status feedback
  - Access list
  - Assigned PIN code keypad

✓ AXM Lite open.
✓ Locking device available.

1. Select the locking device to be duplicated.



2. Click on the Duplicate button.
   ↳ The window for specifying copies will open.



3. Click on the OK button.

↳ Locking device is duplicated.

16.3 Delete locking device

There are two ways to delete locking devices:

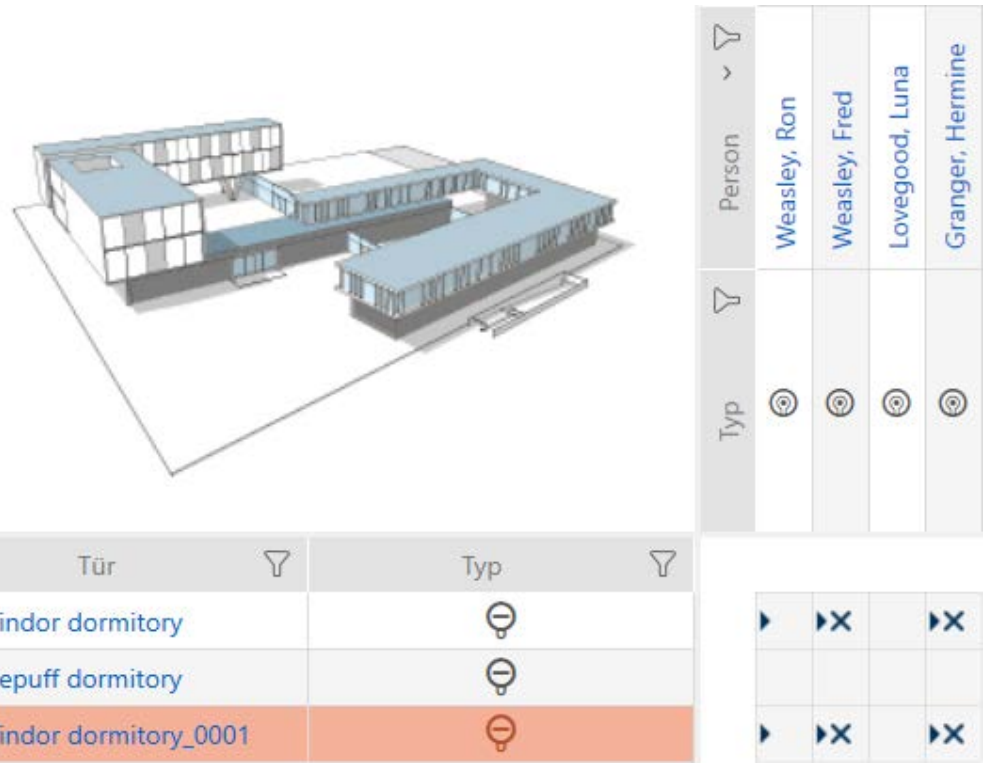
1. Delete on the matrix screen (*Deleting an individual locking device using the matrix [▸ 194]*)
2. Delete using the tab for locking devices (*Deleting several locking devices using the tab [▸ 195]*)

You can also delete several locking devices at the same time in this tab.

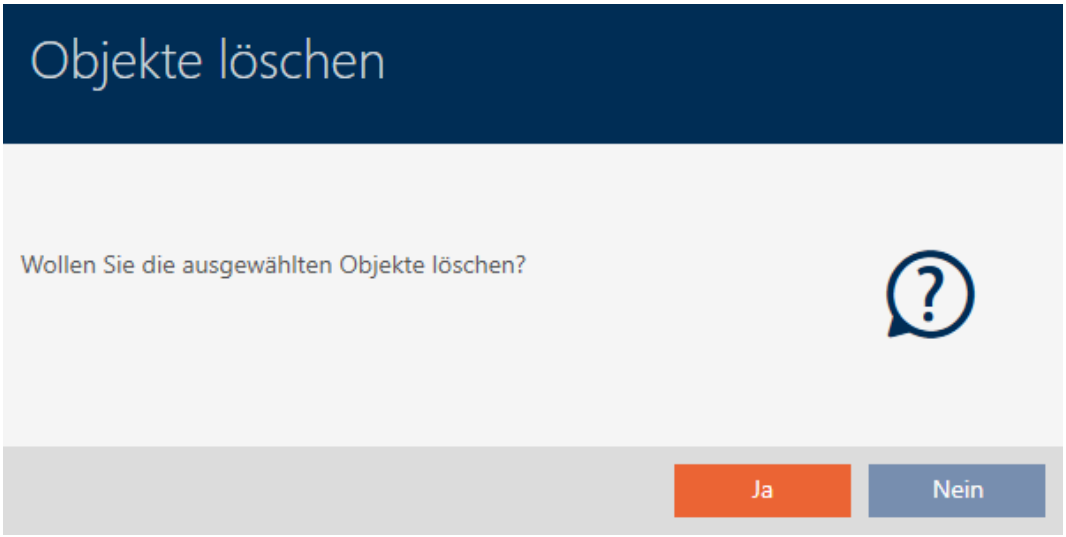
16.3.1 Deleting an individual locking device using the matrix

✓ AXM Lite open.
✓ Matrix screen open.

1. Select the locking device that you wish to delete.

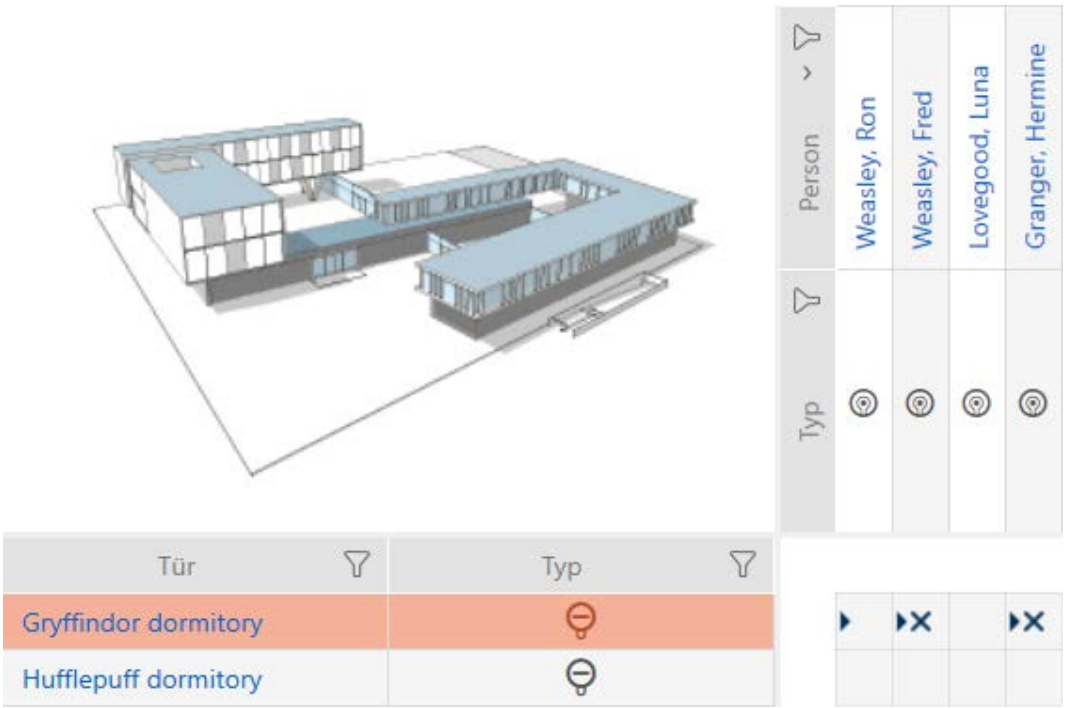


2. Click on the Delete button.
   ↳ Deletion query will open.



3. Click on the Yes button.
   ↳ Deletion query closes.

↳ Locking device has been deleted.

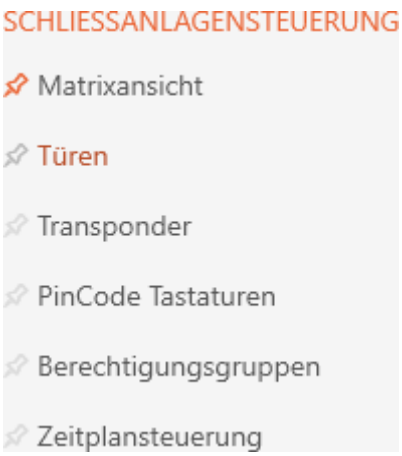


16.3.2 Deleting several locking devices using the tab

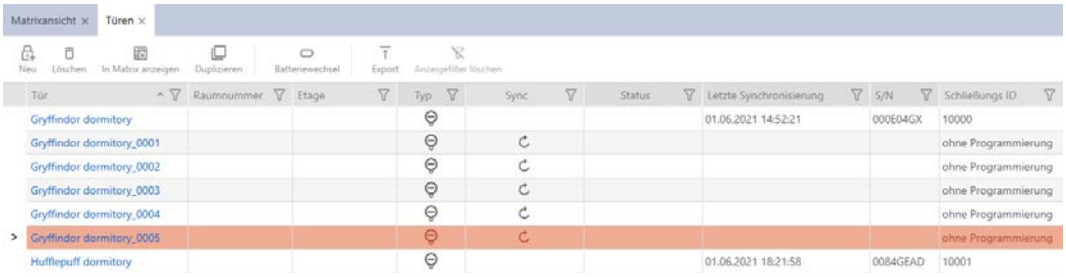
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

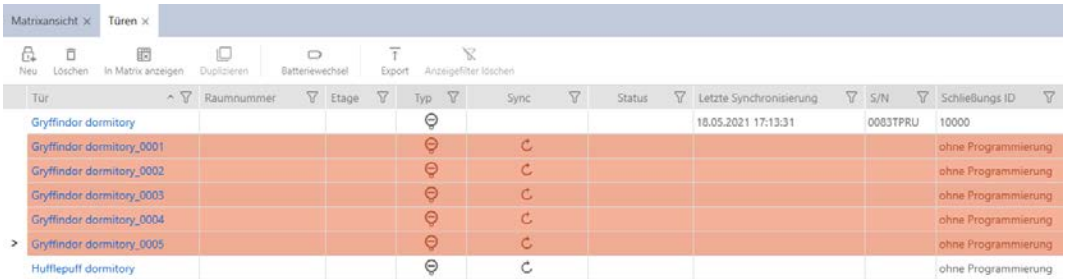
2. Select the Locks entry in the | LOCKING SYSTEM CONTROL | group.



↳ The AXM bar will close.
↳ The [Locks] tab will open.



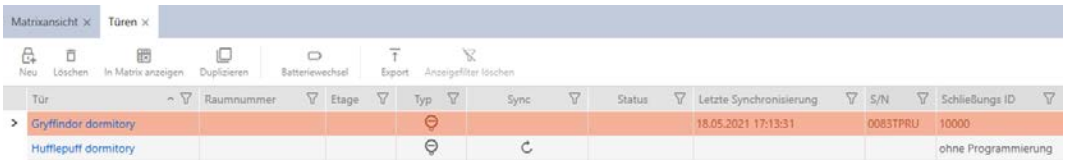
3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Select all locking devices that you wish to delete (Ctrl+click for single media or Shift+click for multiple media).



5. Click on the Delete button.
   ↳ Query with list of locking devices to be deleted will open.

6. Click on the Yes button.
   ↳ Query with list of locking devices to be deleted closes.

↳ Locking devices have been deleted.



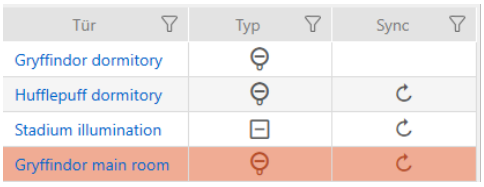
16.4 Changing locking device type at later stage

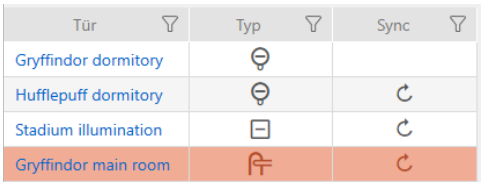
It sometimes becomes evident at a later stage that a different locking device type is more suitable for a particular place of use. It is possible that a cylinder should be replaced with a SmartHandle for convenience reasons, for example.

AXM Lite gives you the option of selecting a different locking device type at a later stage. The locking device remains in the database, including, most importantly, all authorisations and compatible settings.

- Settings that are provided for both the original and the new locking device type remain unchanged.
- Settings from the original locking device type that do not exist for the new locking device type expire.
- Settings that only exist for the new locking device type but not for the original locking device type are set to a default value.

	Original locking device type	New locking device type	Result
Setting A (e.g. *Open time (sec)*)	Adjustable	Adjustable	Is applied
Setting B (e.g. ☑ Invert SR signal)	Adjustable	Not adjustable	Expires
Setting C	Not adjustable	Adjustable	Set to default value

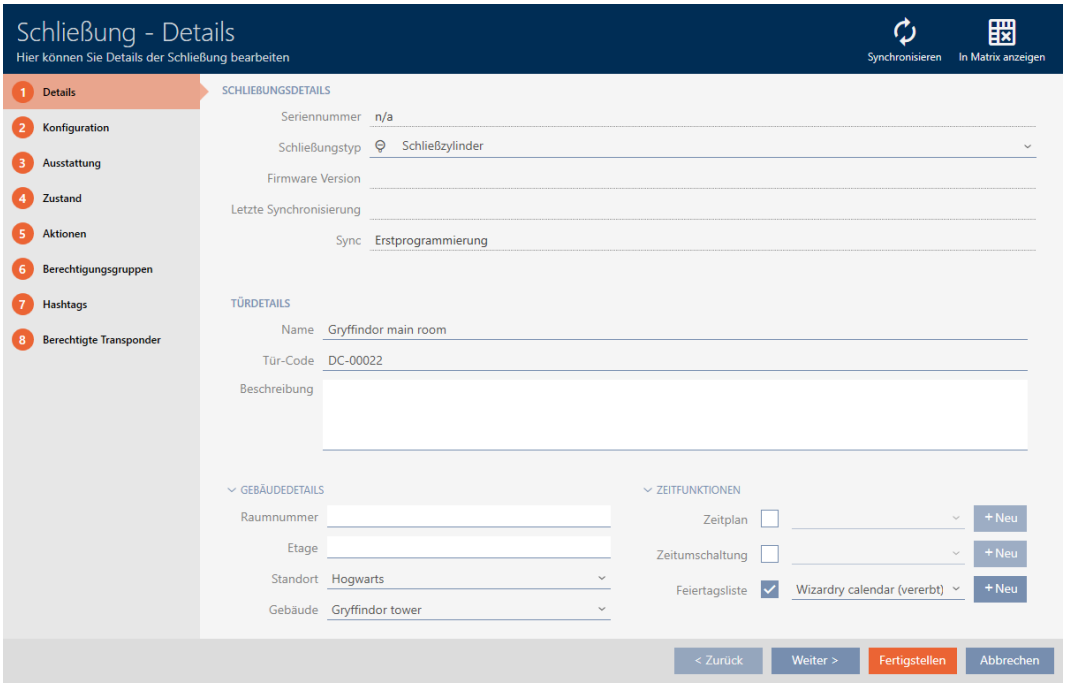




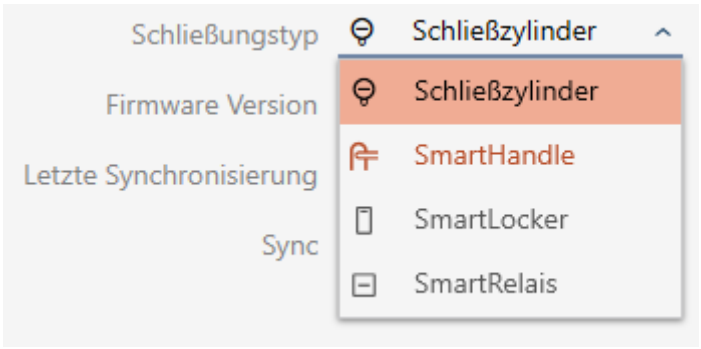
The locking device type can only be changed for non-synchronised locking devices.

✓ AXM Lite open.
✓ Locking device list or matrix view open.
✓ Locking device available.
✓ Locking device not synchronised (if necessary reset, see *Re-setting the locking device [▸ 300]*).

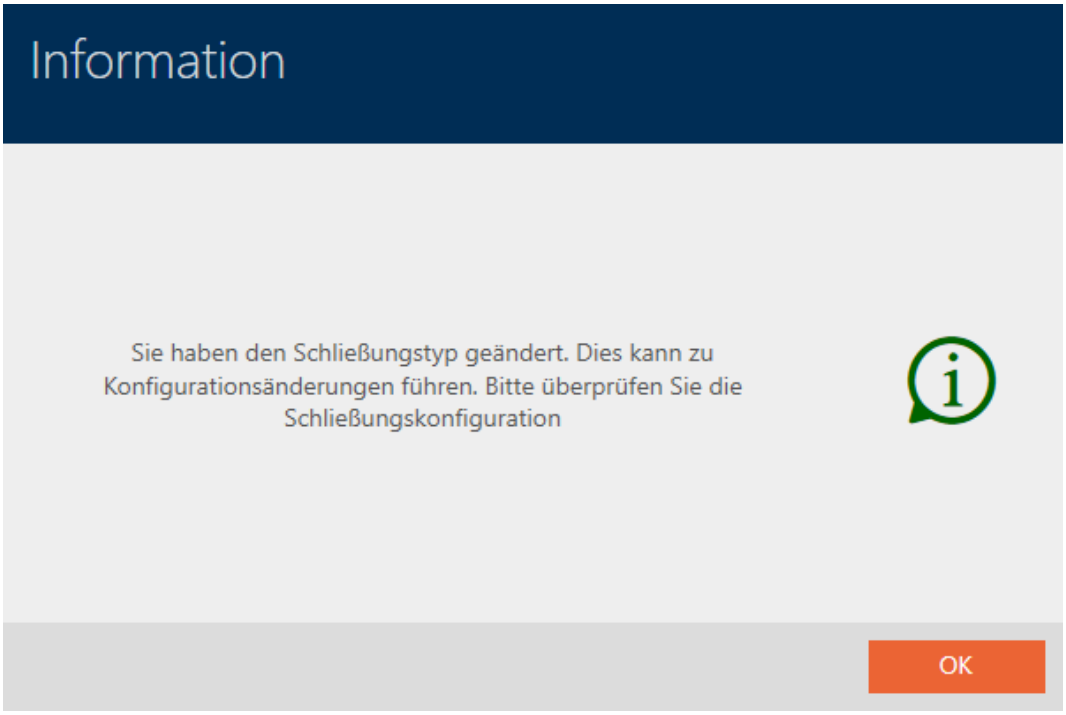
1. Click on the locking device whose type you wish to change.
   ↳ The locking device window will open.



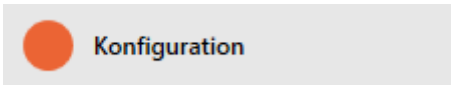
2. Select the new locking device type from the ▼ **Lock type** drop-down menu.



↳ Warning about the configuration change will open.



3. Click on the OK button.
   ↳ Warning about configuration change closes.
4. Click on the Configuration tab.



   ↳ Window switches to the "Configuration" tab.
5. Check and change the configuration if necessary.
6. Click on the Finish button.
   ↳ The locking device window closes.

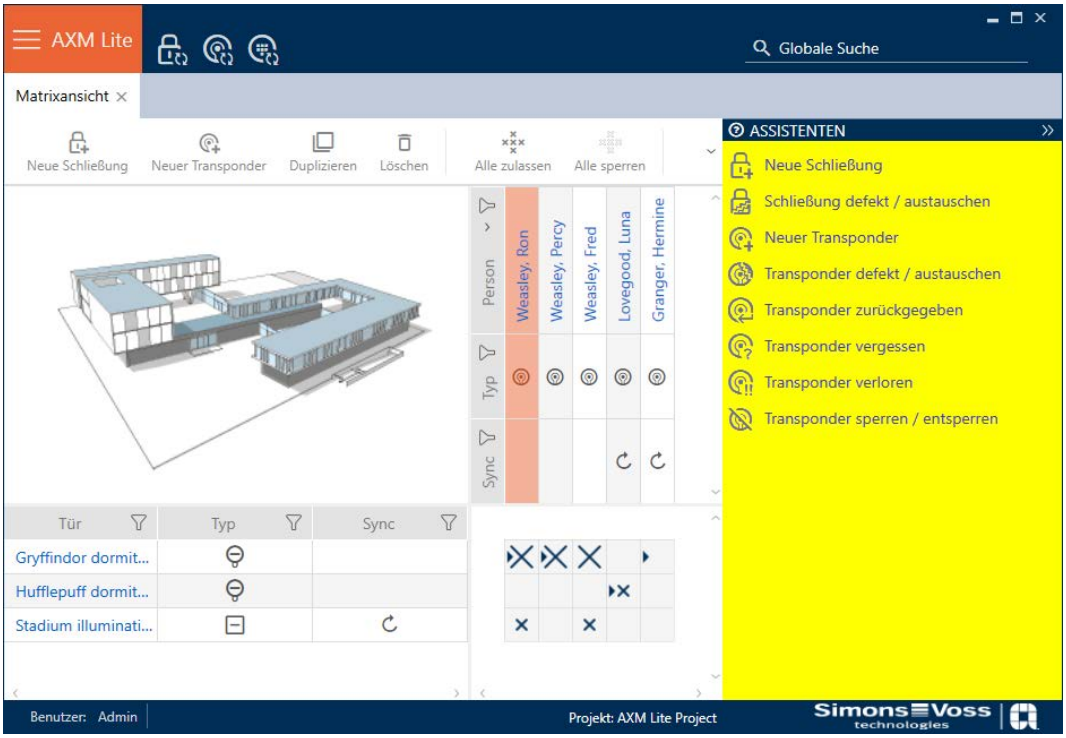
↳ Locking device type has been changed.

16.5 Handling defective locking devices

Defective locking devices cause problems. Reasons for failure may include:

- Software defects
- Hardware defects

As a basic rule, all actions can be performed using the wizard section on the right-hand side:



AXM Lite provides you with a wizard to repair defective locking devices.

The following overview will help you decide on the right course of action (information about the relationship between the locking device and the locking device ID stored internally in the project (= lock ID or LID): *Identification media, locking devices and the locking plan [▸ 360]*

Locking device is required again immediately:

Suitable for:

Repair	Resetting and replacing	Delete and replace
Locking devices with an undefined software status	■ Locking devices with external damage (e.g. scratched). ■ Locking devices that should be replaced as a precaution (e.g. if they get wet).	Locking devices permanently damaged (e.g. thumb-turn broken off) which require replacement.

Example situation:

Repair	Resetting and replacing	Delete and replace
	Bed pressed against thumb-turn, thumb-turn bent	Bed pushed against thumb-turn, thumb-turn broken off

Procedure:

Repair	Resetting and replacing	Delete and replace
Re-synchronise (repair) [▸ 203] 1. Reset (= LID available in database again) 2. Resynchronise (= LID is immediately written back onto the same locking device) The locking device works the same as before after repair.	*Resetting and replacing [▸ 205]* 1. Reset (= LID flagged as defective in database and removed from original locking device) 2. Synchronise replacement locking device with new LID The LID is no longer contained in the locking device due to the reset. The locking device can therefore no longer be used. However, it can be re-synchronised. A new LID is written onto the locking device during resynchronisation. The previous locking device remains in the database with its LID and is flagged as defective.	*Delete and replace [▸ 210]* 1. Synchronise replacement locking device with new LID 2. Delete defective locking device It is obviously no longer possible to reset a permanently damaged locking device. It is thus replaced by a replacement locking device with a new LID. The faulty locking device's LID can be used for another locking device in the future.

Locking device is not required again immediately:

Suitable for:

Reset	Purge (software reset)
■ Locking devices with external damage (e.g. scratched). ■ Locking devices that should be replaced as a precaution (e.g. if they get wet).	Locking devices with an undefined software status

Example situation:

Reset	Purge (software reset)
Bed pressed against thumb-turn, thumb-turn bent. Door must be repaired, therefore no immediate need for a locking cylinder.	Aborted programming

Procedure:

Reset	Purge (software reset)
Reset [▸ 214] Resetting removes the LID from the locking device. You can synchronise another locking device with this entry later, which will receive the same LID.	*Purge (only reset in database/software reset) [▸ 216]* The clean-up only affects the database in your AXM Lite. The actual locking device remains unaffected by this reset. Basically, you reset the locking device in the database without actually resetting the locking device itself. The LID is separated from the LID for the locking device previously used during the clean-up in the database (in current state). After cleaning up an entry, you can synchronise any locking device again with this entry at a later stage and it will receive the same LID. After the software reset, your AXM Lite is no longer aware that the LID has already been assigned. For this reason, make sure that you reset the locking device previously used for this entry (see *Re-setting the locking device [▸ 300]*). This deletes the LID from the old locking device and prevents the same LID from being in circulation twice.

NOTE

AX components: SmartCD.MP or SmartStick AX for initial synchronisation

A great deal of data is transferred during initial synchronisation of AX components. The carrier frequency and, consequently, the transmission speed is significantly higher with the SmartCD.MP or SmartStick AX.

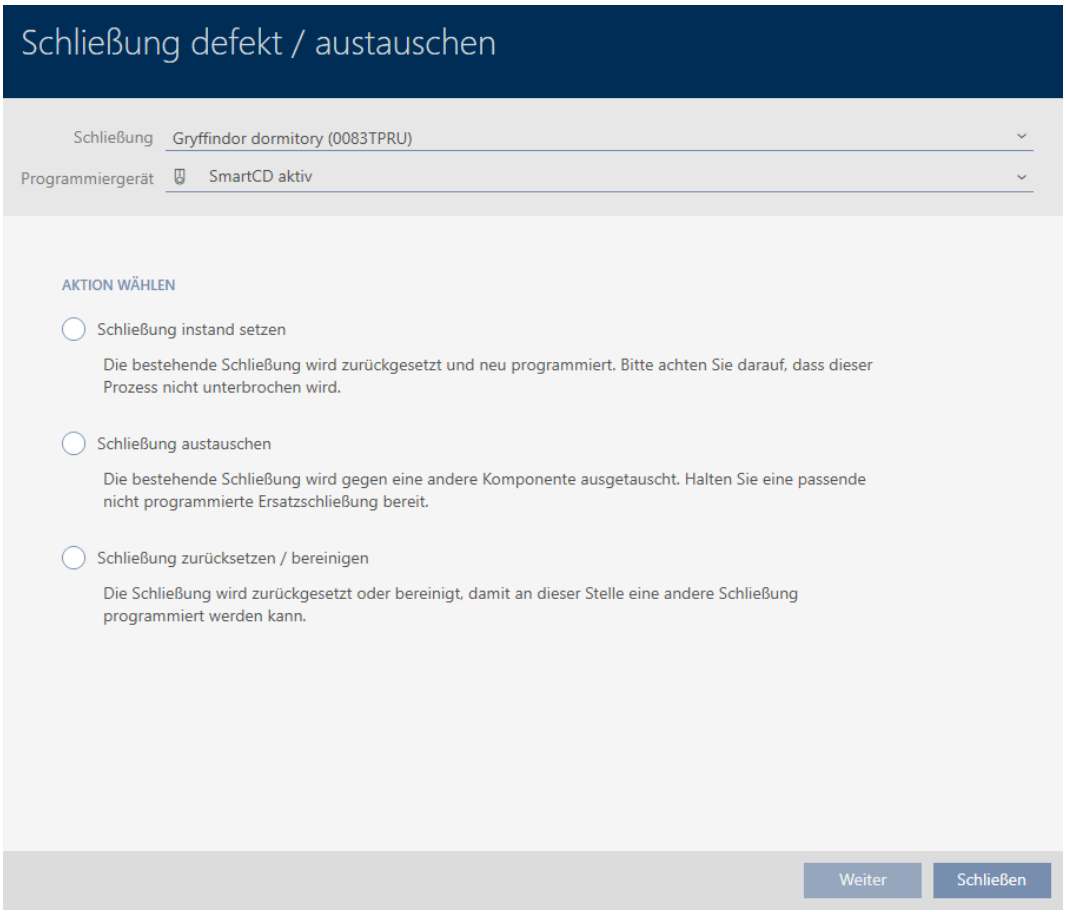
- It is especially important to use a SmartCD.MP or a SmartStick AX for initial synchronisation of AX components.

16.5.1 Re-synchronise (repair)

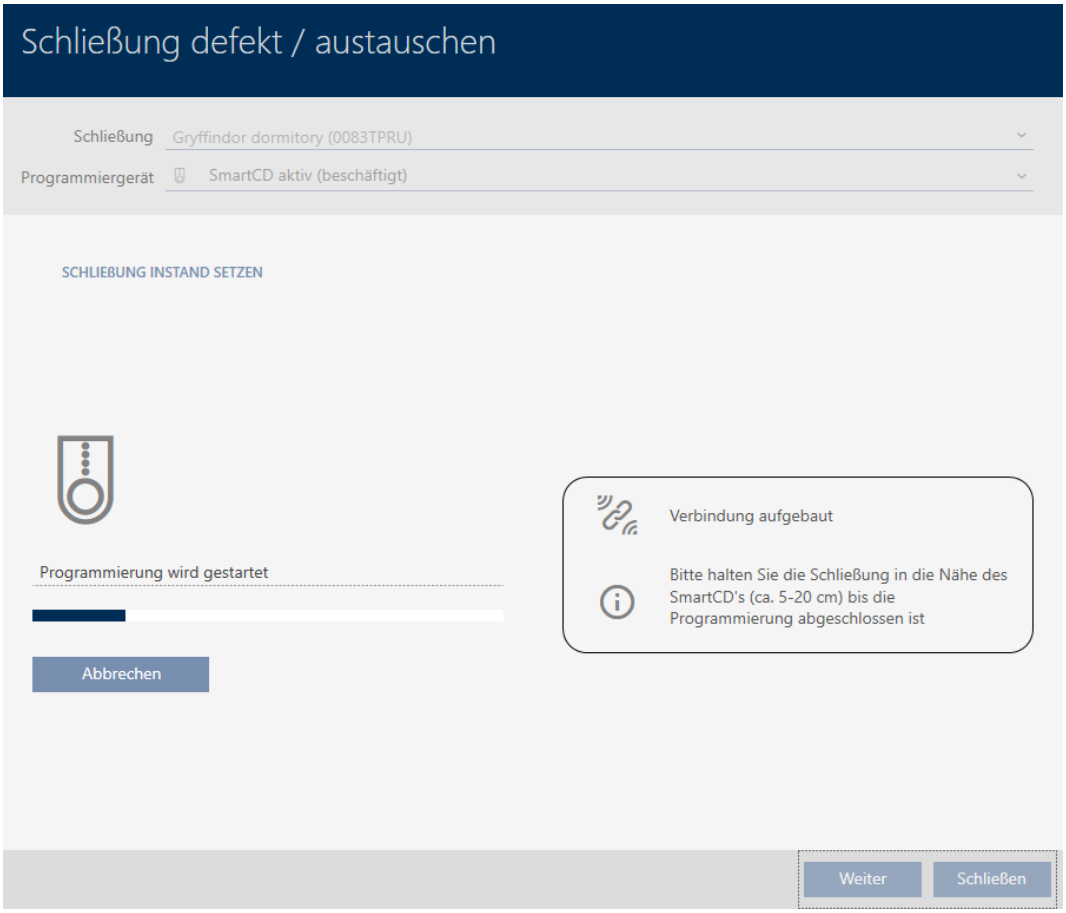
- ✓ AXM Lite open.
- ✓ Locking device list or matrix view open.
- ✓ Locking device present.
- ✓ Suitable programming device connected.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the faulty locking device.

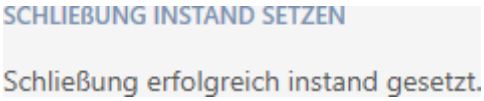
3. Click the Replace lock button in the "Wizards" section.
   ↳ Wizard for dealing with a faulty locking device will open.



4. Select the Repair lock option.
5. Click on the Next button.
   ↳ Locking device is being resynchronised.



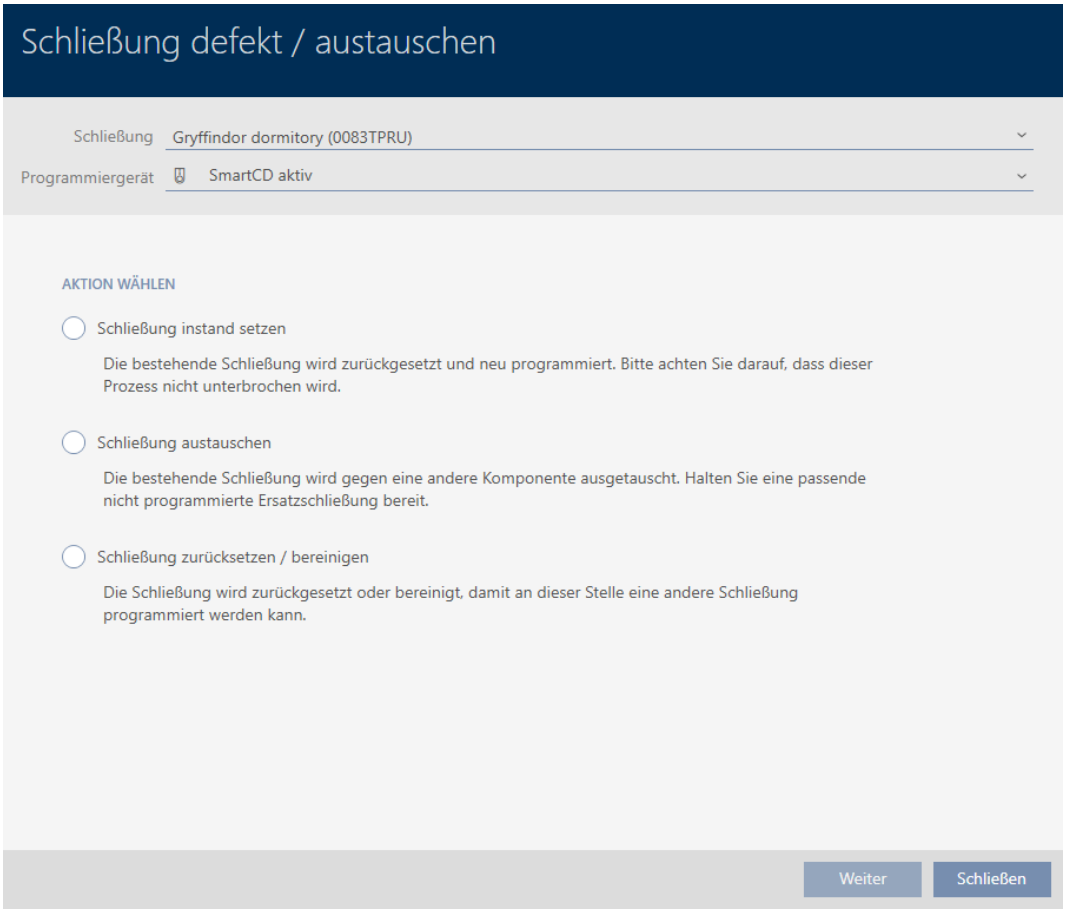
↳ Locking device is resynchronised.



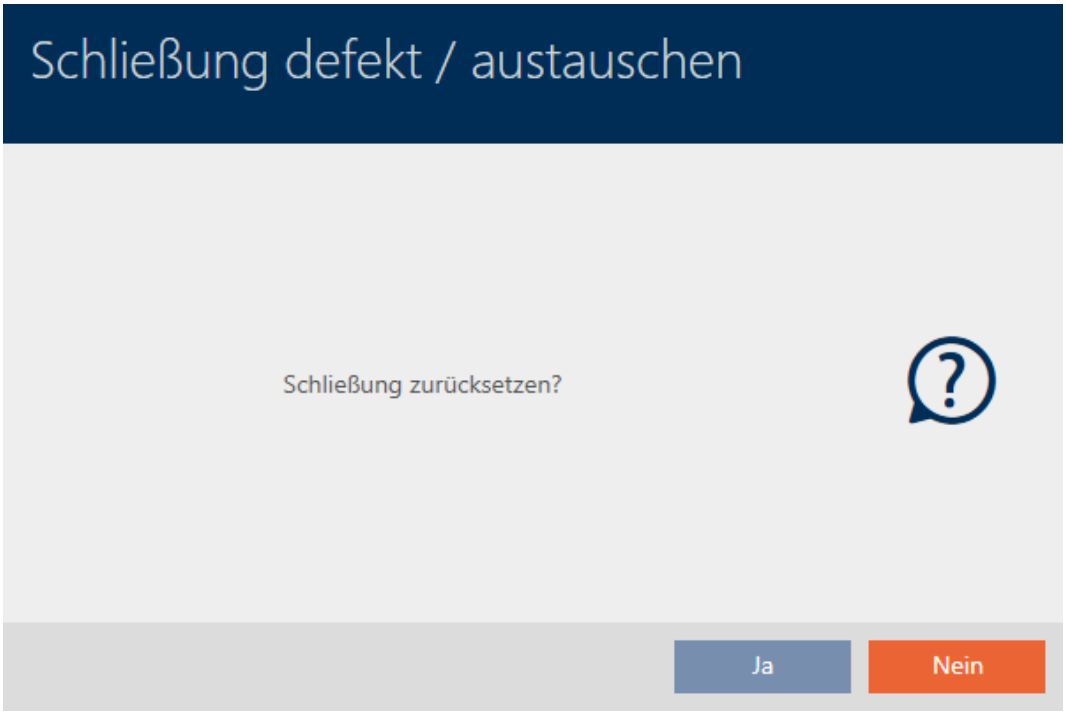
16.5.2 Resetting and replacing

✓ AXM Lite open.
✓ Locking device list or matrix view open.
✓ Locking device present.
✓ Suitable replacement locking device available.
✓ Suitable programming device connected.

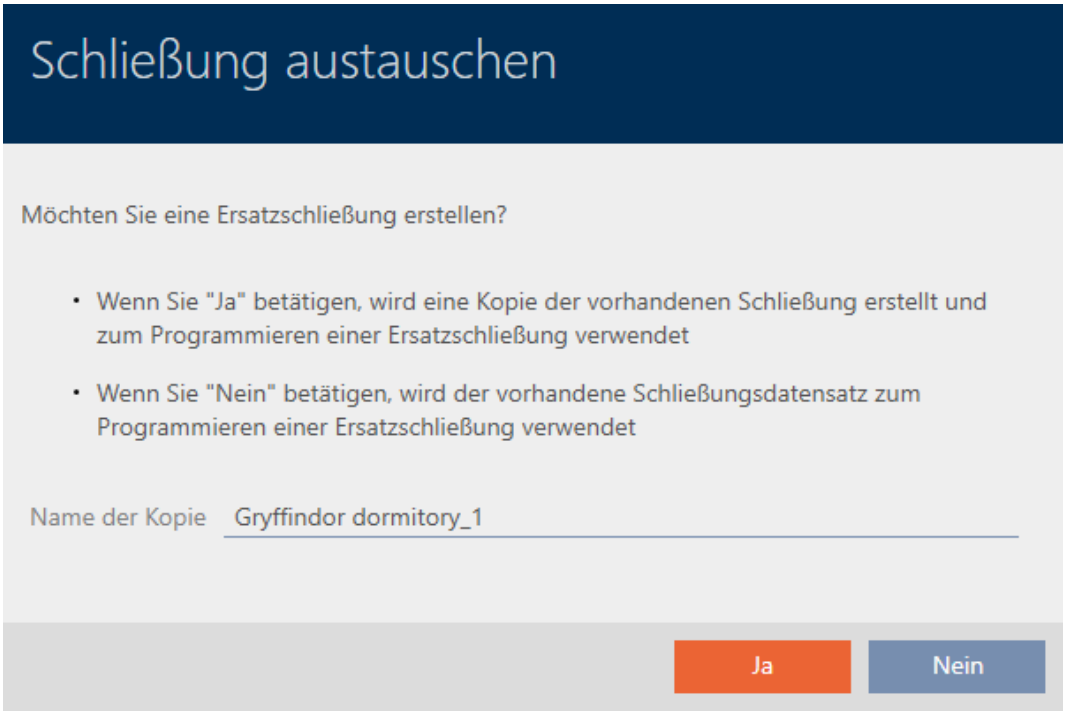
1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the faulty locking device.
3. Click the Replace lock button in the "Wizards" section.
   ↳ Wizard for dealing with a faulty locking device will open.



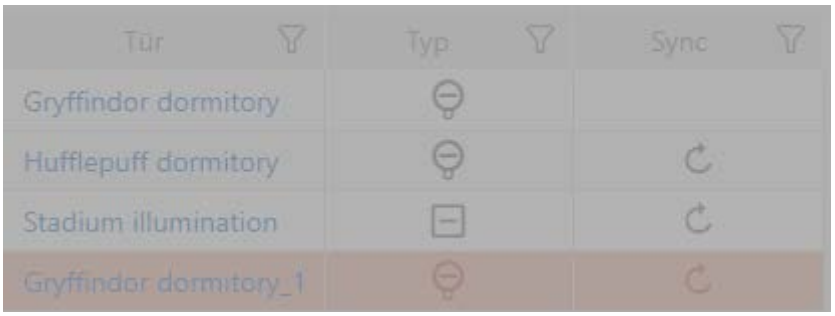
4. Select the ◉ Replace lock option.
5. Click on the Next button.
   ↳ Reset query will open.



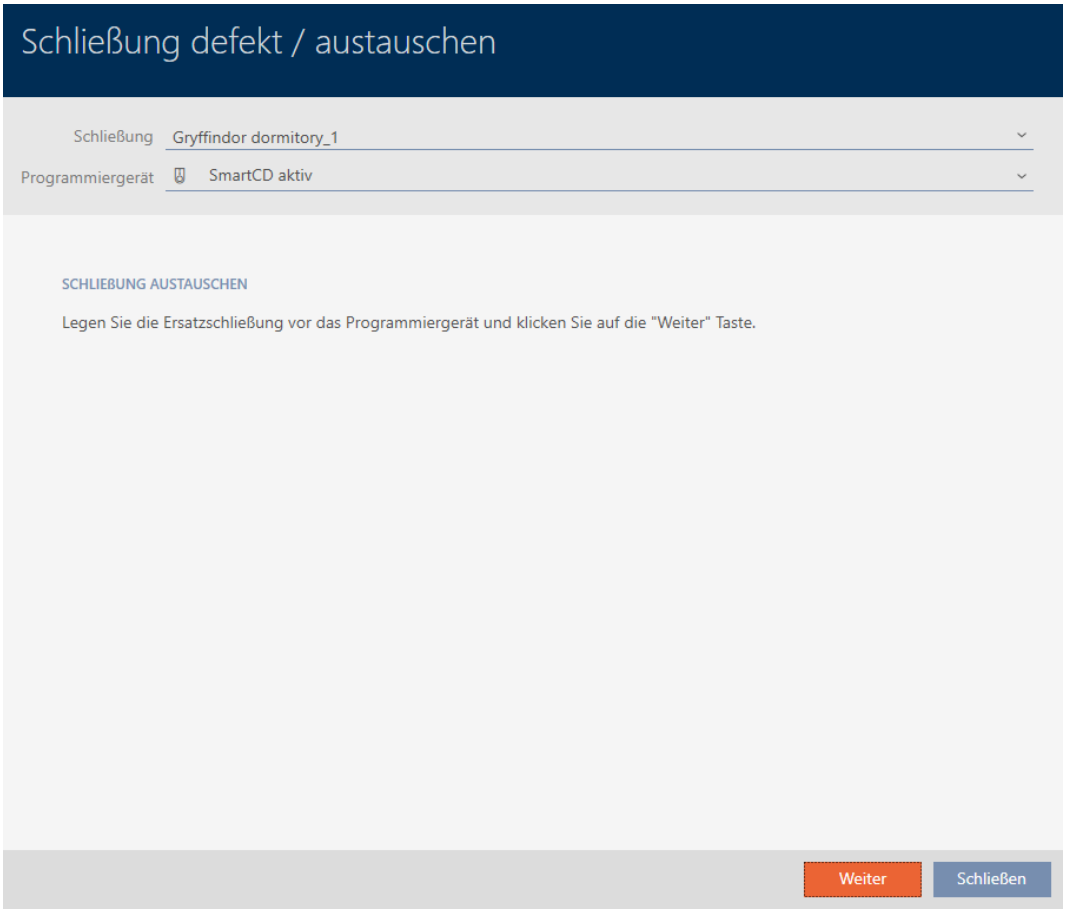
6. Click on the Yes button.
   ↳ Reset query will close.
   ↳ The locking device is reset.
   ↳ Confirmation dialogue for creating a replacement locking device will open.



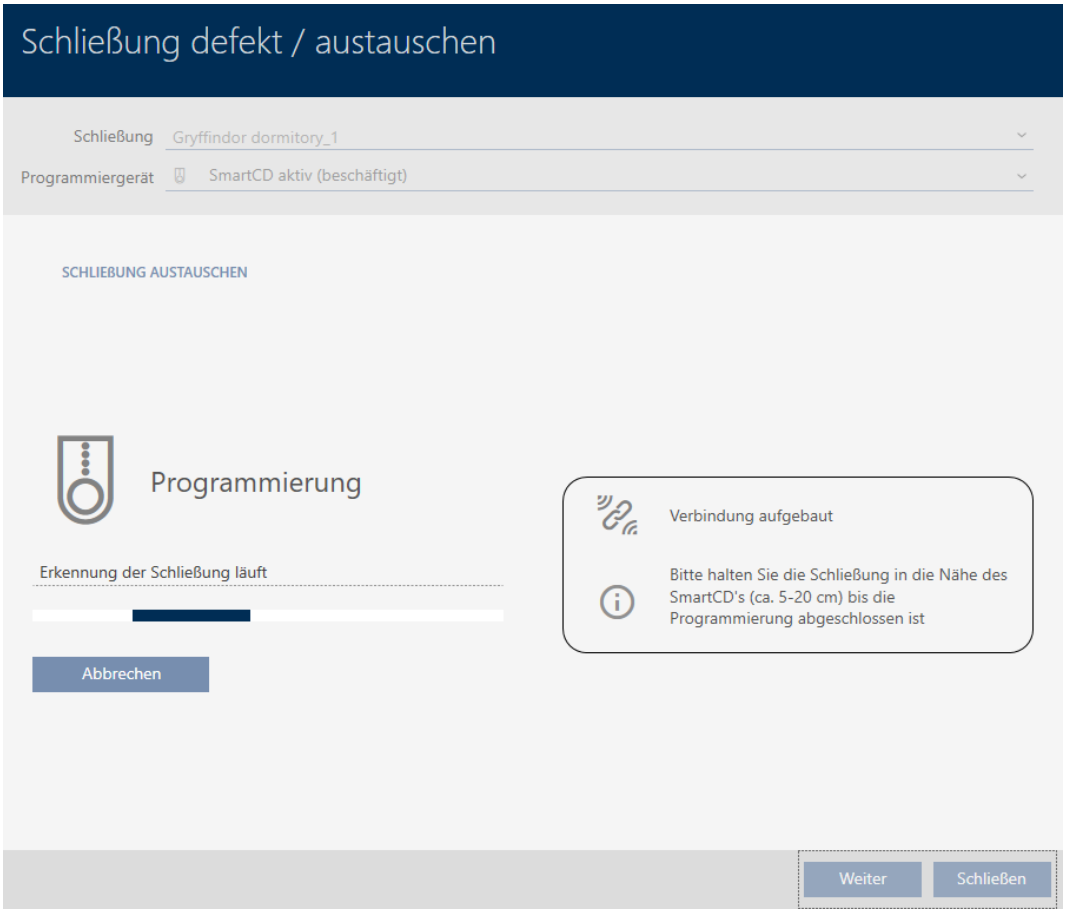
7. If necessary, change the entry in the *Copy name* field.
8. Click on the Yes button.
   ↳ Confirmation dialogue for creating a replacement locking device closes.
   ↳ Replacement locking device is already visible in the matrix in the background.



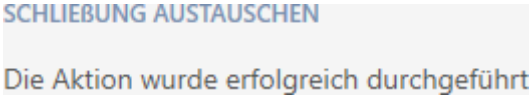
   ↳ Wizard prepares synchronisation for the replacement locking device.



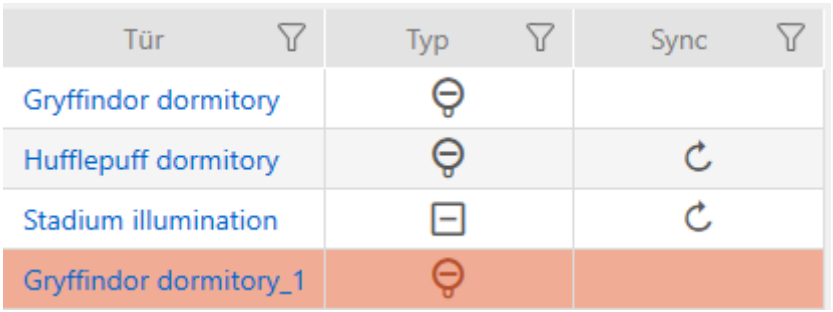
9. Click on the Next button.
   ↳ Replacement locking device is being synchronised.



↳ Replacement locking device is synchronised.



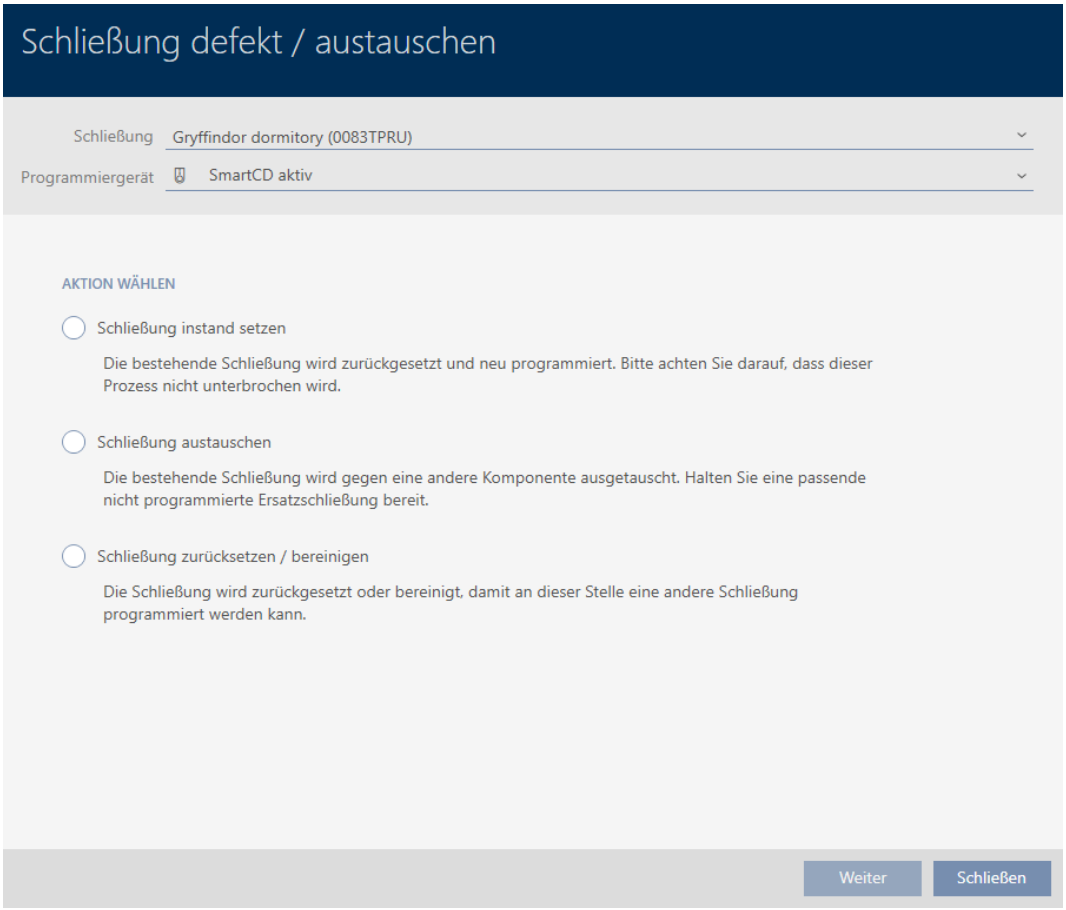
↳ Replacement locking device is displayed in the matrix.



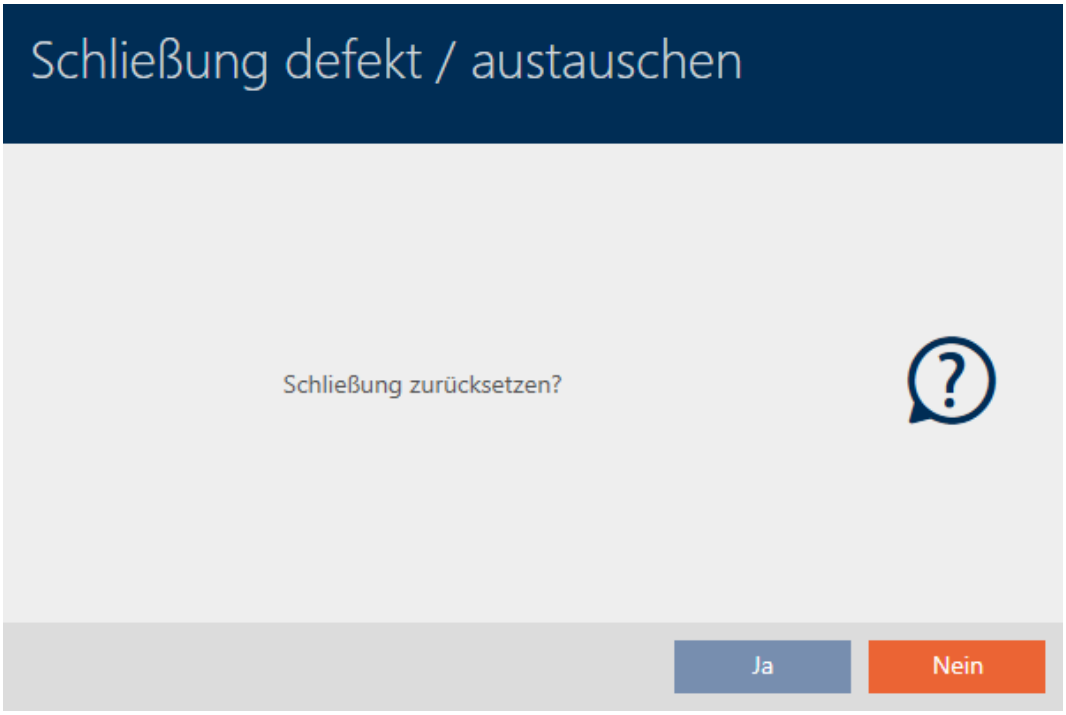
16.5.3 Delete and replace

- ✓ AXM Lite open.
- ✓ Locking device list or matrix view open.
- ✓ Suitable replacement locking device available.
- ✓ Suitable programming device connected.

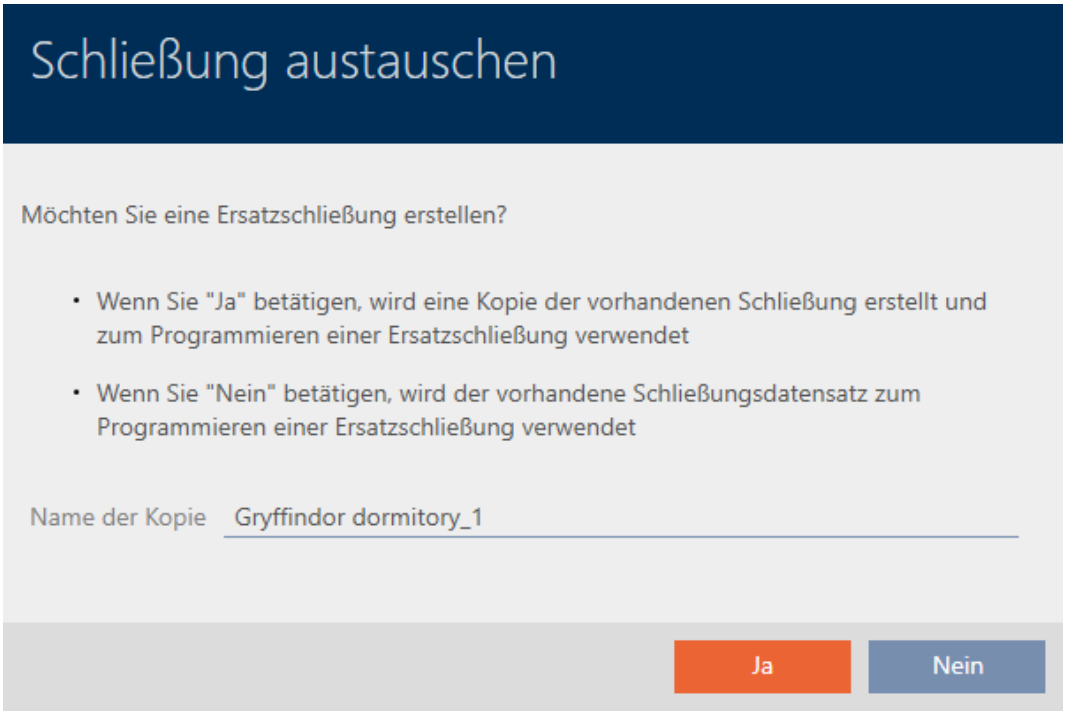
1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the faulty locking device.
3. Click the Replace lock button in the "Wizards" section.
   ↳ Wizard for dealing with a faulty locking device will open.



4. Select the Replace lock option.
5. Click on the Next button.
   ↳ Reset query will open.

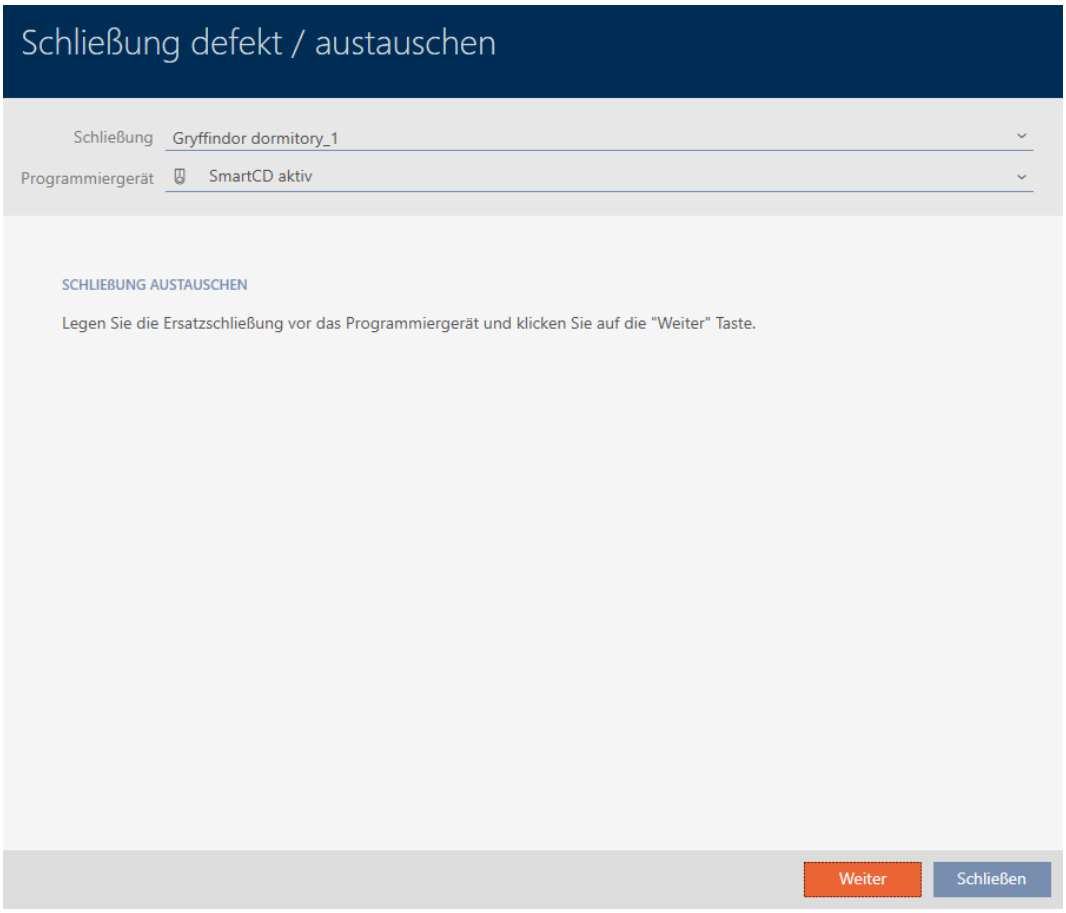


6. Click on the No button.
   ↳ Reset query will close.
   ↳ Confirmation dialogue for creating a replacement locking device will open.

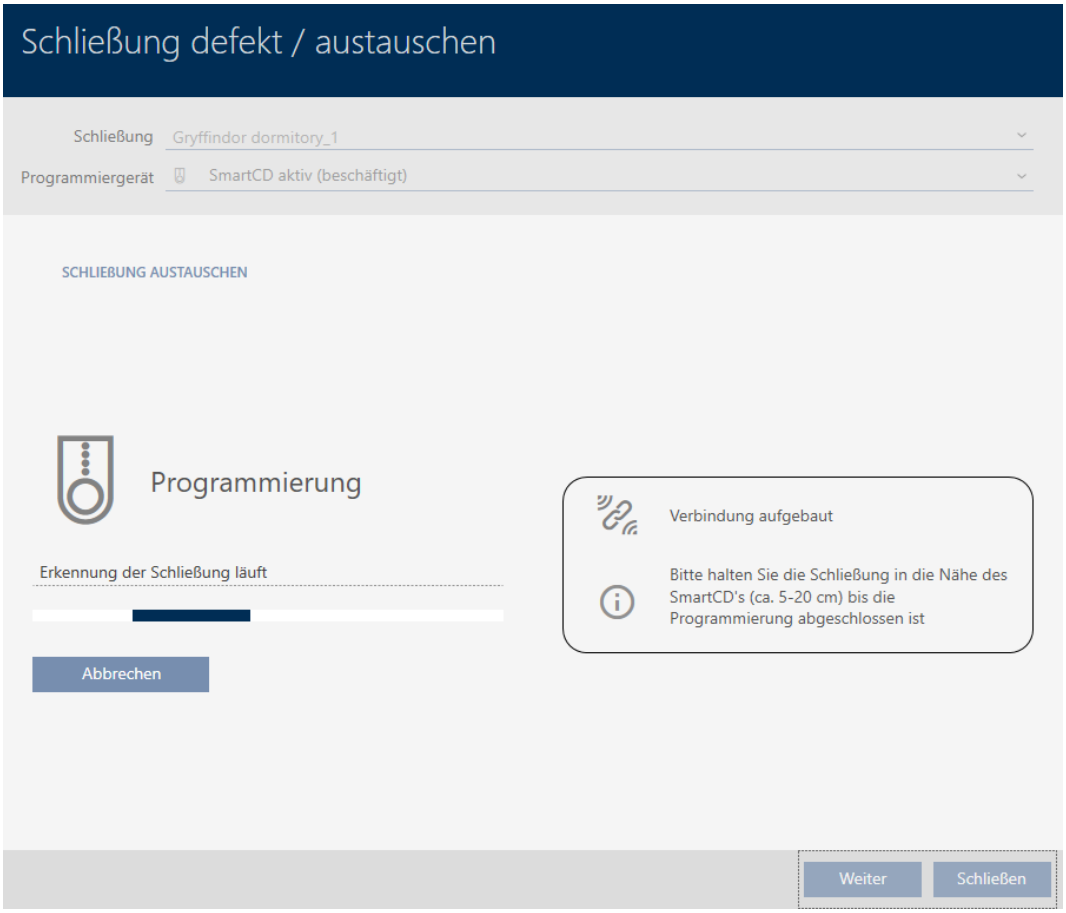


7. If necessary, change the entry in the *Copy name* field.
8. Click on the Yes button.
   ↳ Confirmation dialogue for creating a replacement locking device closes.

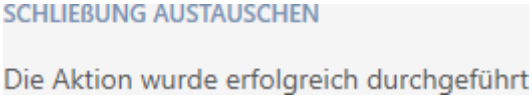
↳ Replacement locking device is already visible in the matrix in the background.
↳ Wizard prepares synchronisation for the replacement locking device.



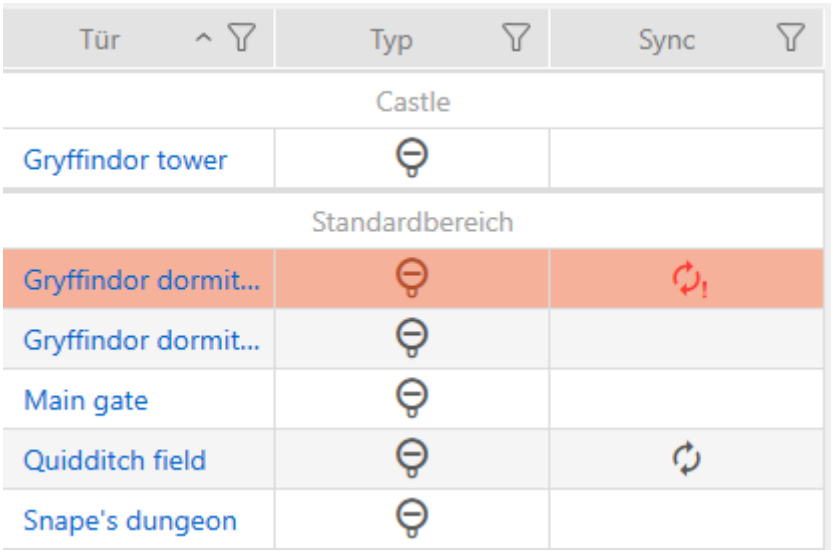
9. Click on the Next button.
↳ Replacement locking device is being synchronised.



↳ Replacement locking device is synchronised.

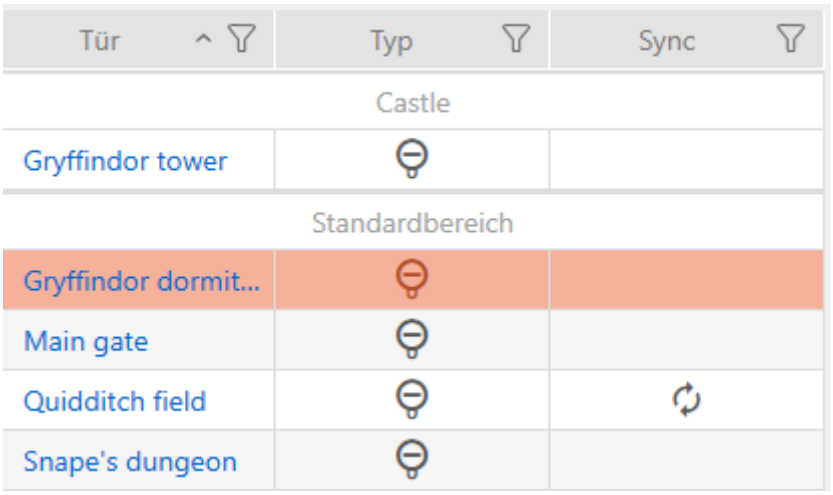


10. Click on the Close button.
    ↳ Wizard for dealing with a faulty locking device closes.
11. Select the defective original locking device.



12. Click on the Delete button.
    ↳ Defective locking device is deleted from the locking plan.

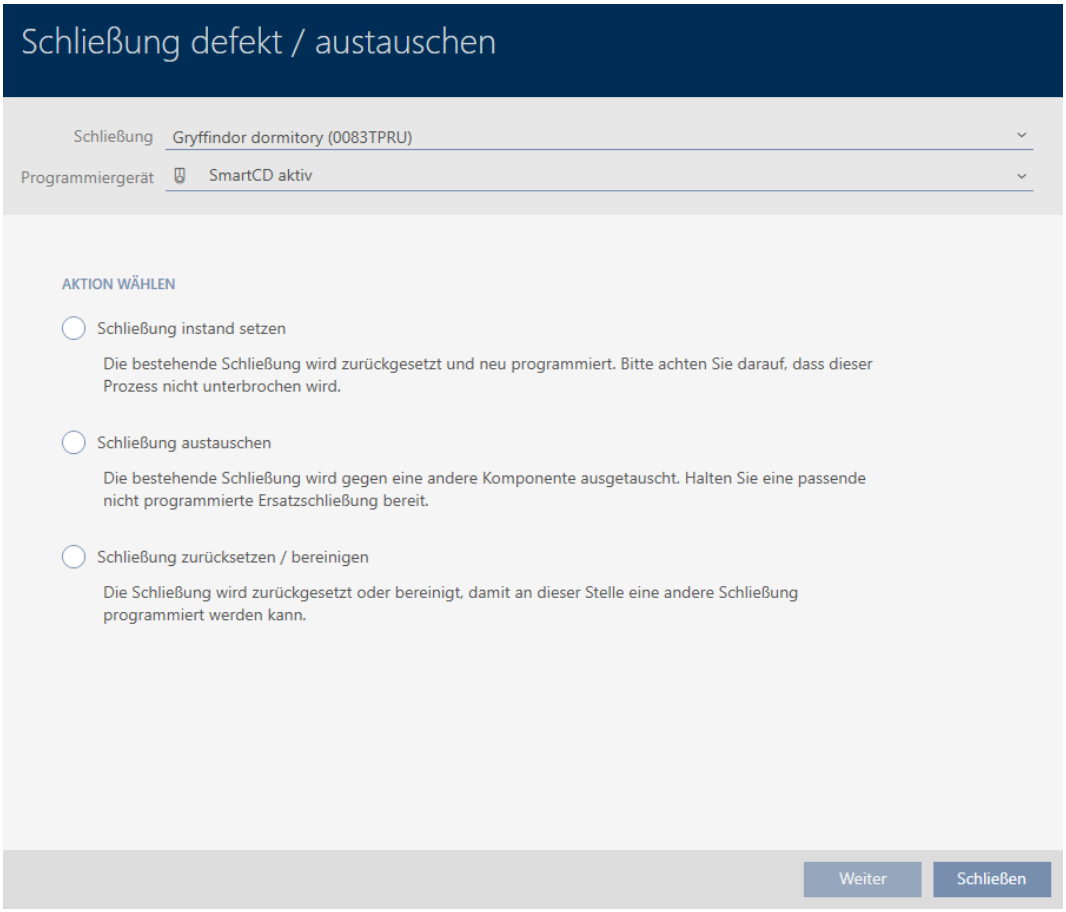
↳ Replacement locking device is displayed in the matrix.



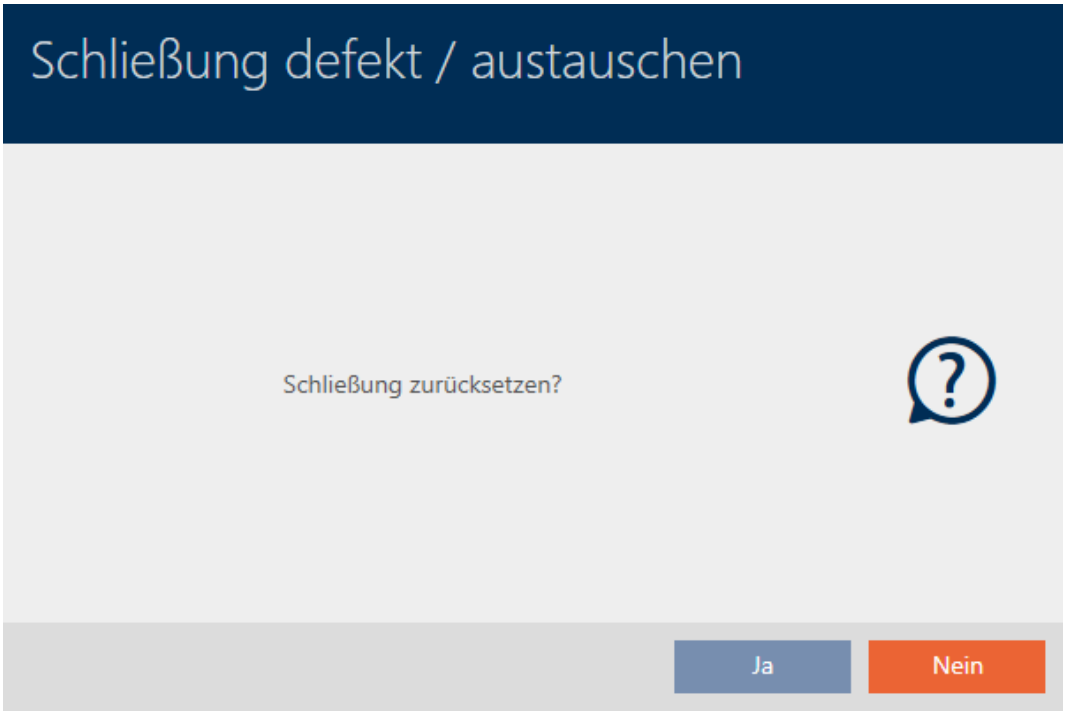
16.5.4 Reset

✓ AXM Lite open.
✓ Locking device list or matrix view open.
✓ Locking device present.
✓ Suitable programming device connected.

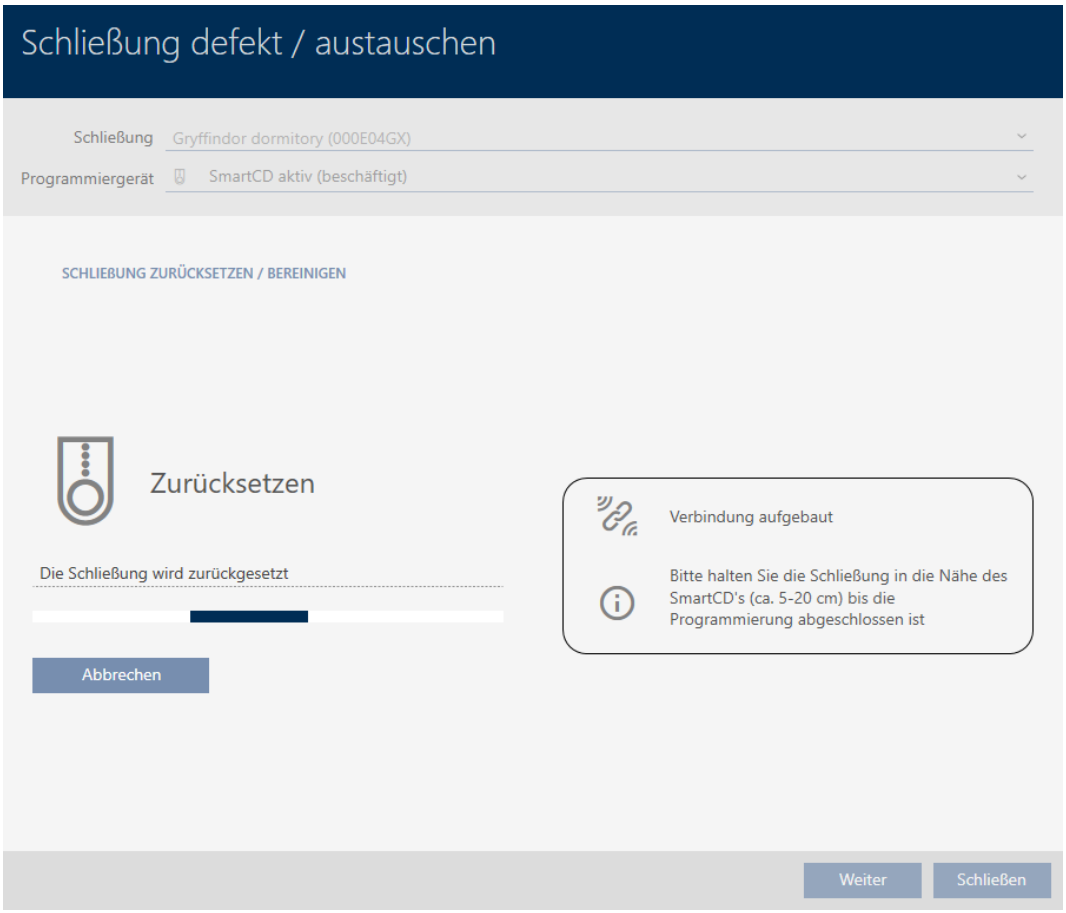
1. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the faulty locking device.
3. Click the Replace lock button in the "Wizards" section.
   ↳ Wizard for dealing with a faulty locking device will open.



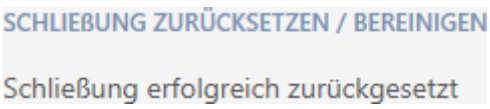
4. Select the ◉ Reset/purge lock option.
5. Click on the Next button.
   ↳ Reset query will open.



6. Click on the Yes button.
   ↳ Reset query will close.
   ↳ The locking device is reset.



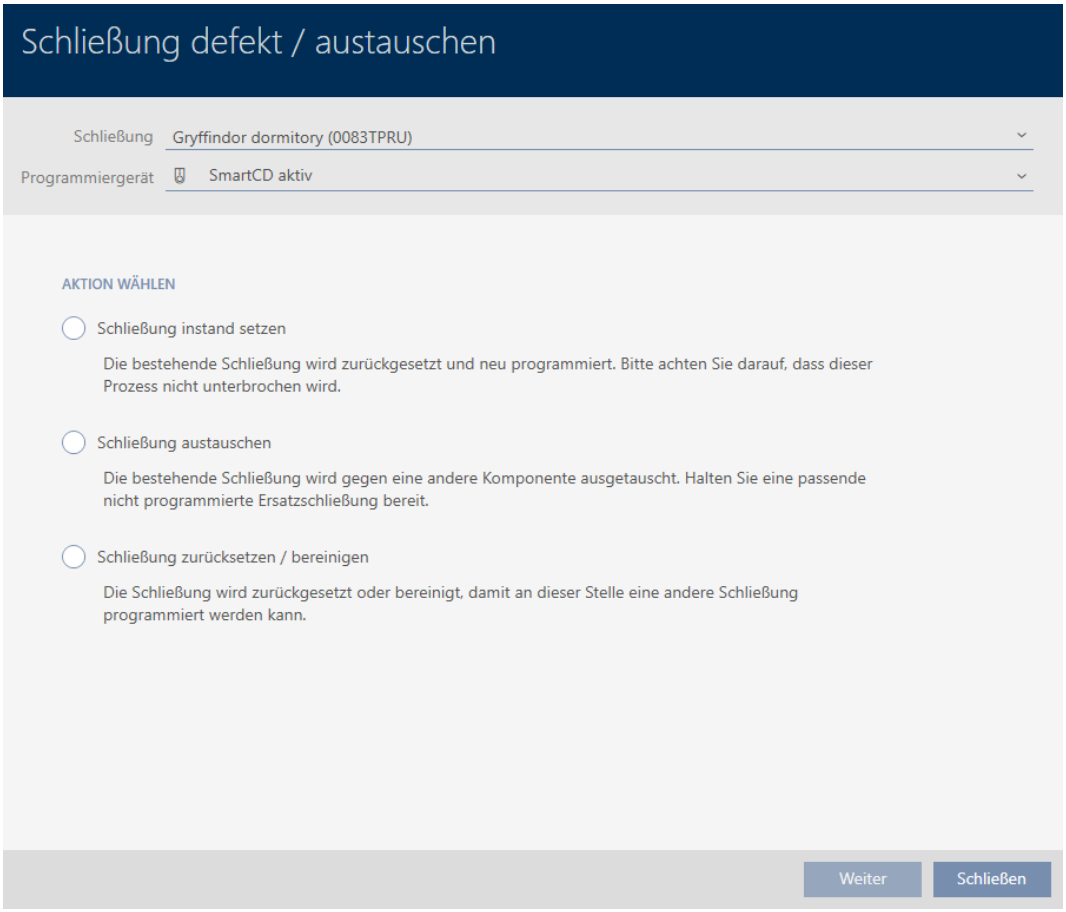
↳ Locking device is reset.



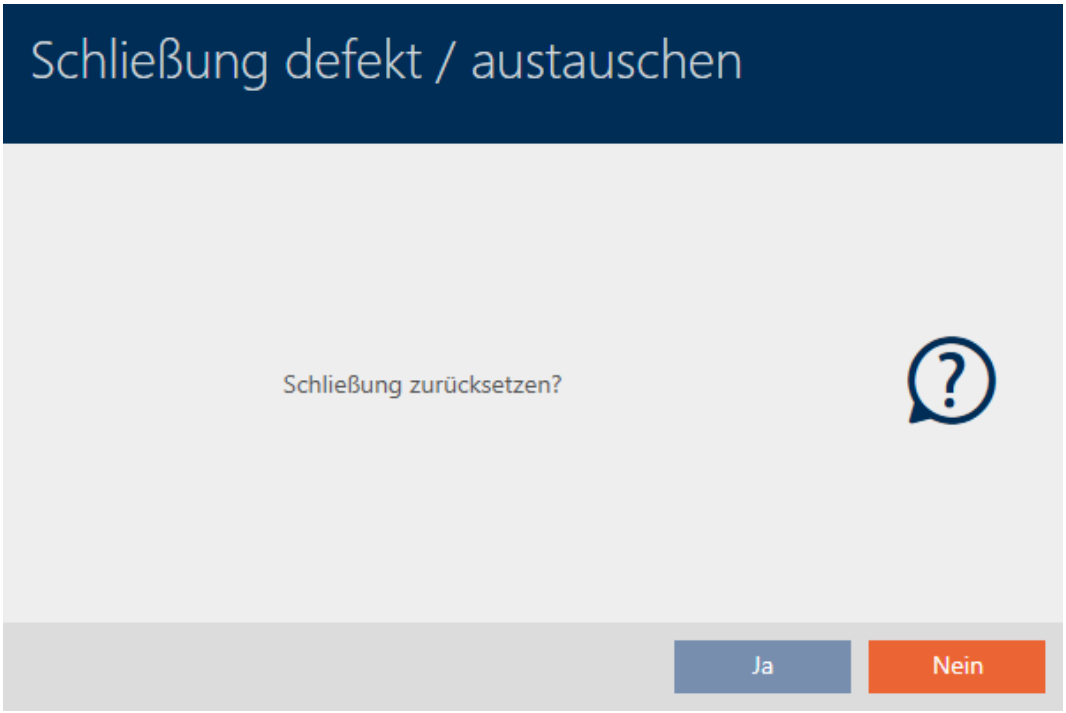
16.5.5 Purge (only reset in database/software reset)

✓ AXM Lite open.
✓ Locking device list or matrix view open.

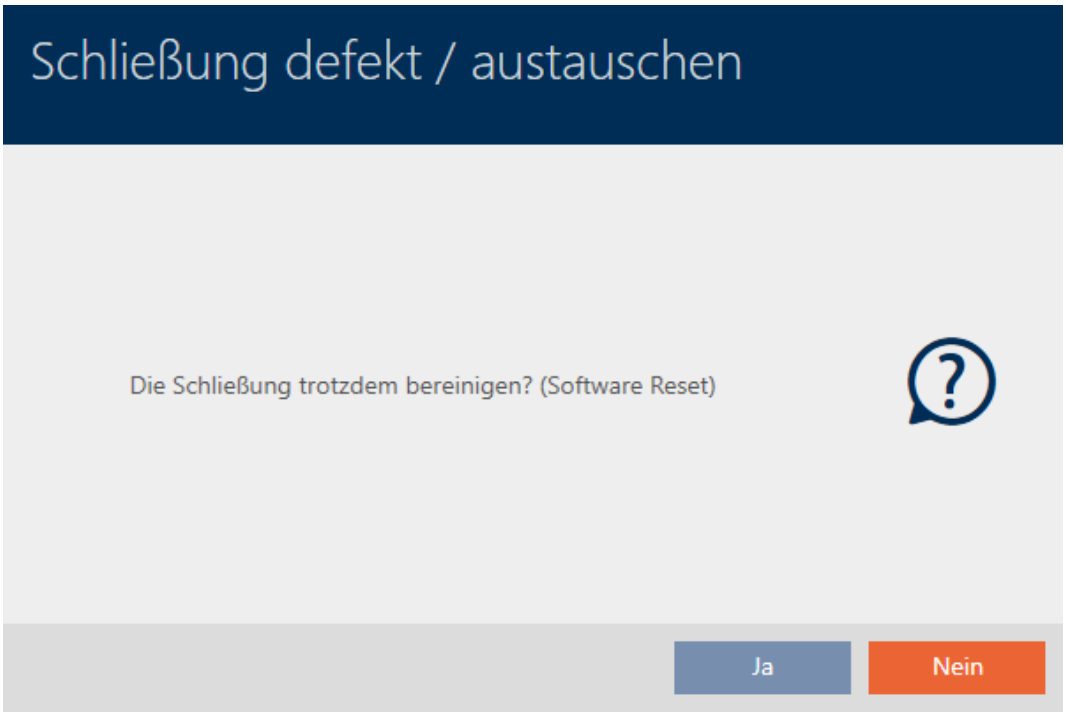
1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Select the faulty locking device.
3. Click the Replace lock button in the "Wizards" section.
   ↳ Wizard for dealing with a faulty locking device will open.



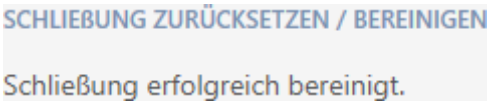
4. Select the ◉ Reset/purge lock option.
5. Click on the Next button.
   ↳ Reset query will open.



6. Click on the No button.
   ↳ Reset query will close.
   ↳ Query about purging will open.



7. Click on the Yes button.
   ↳ Locking device is reset in the database separately from the actual locking device.



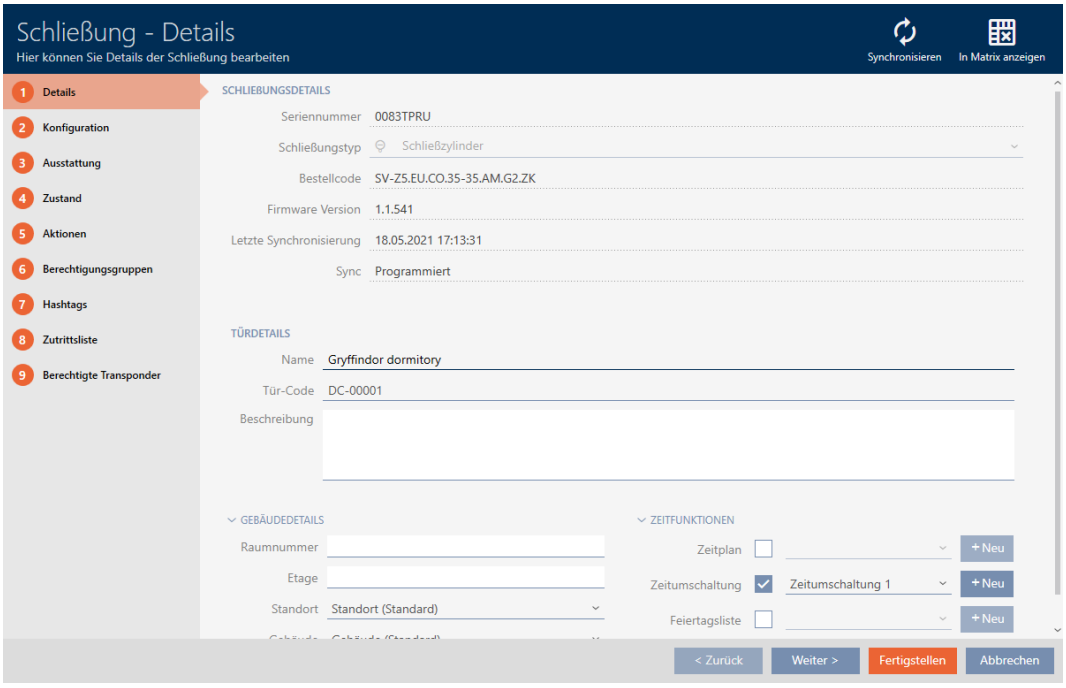
16.6 Assigning locking devices to buildings/locations

You must specify a location and a building the moment you create a locking device. Ideally, you should follow best practice (see *Best practice: setting up the locking system [▸ 29]*) and plan everything out in preparation before creating your locking devices (see *Organisational structure [▸ 44]*). This means that you only need to open windows once.

Obviously, you can also assign your locking devices to other buildings at a later date:

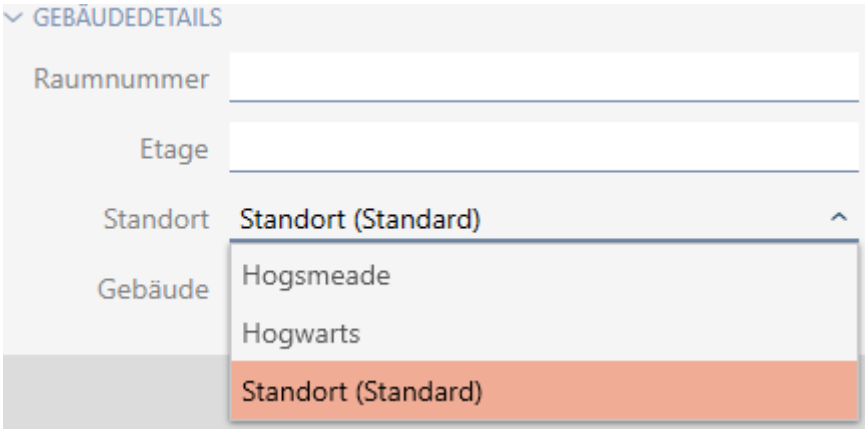
✓ AXM Lite open.
✓ At least one location created (see *Creating a location [▸ 69]*).
✓ At least one building created (see *Creating a building and assigning it to a location [▸ 72]*).

1. Click on the locking device you wish to assign to a location and a building.
   ↳ The locking device window will open.



2. Open the "Building details" menu if necessary.

3. Select the location where your locking device will be used from the ▼ **Location**drop-down menu.



   ↳ Building selection in the ▼ **Building** drop-down menu is restricted to the buildings at the selected location.
4. Select the building where your locking device will be used from the ▼ **Building** drop-down menu.
5. Click on the Finish button.
   ↳ The locking device window closes.

↳ Locking device is assigned to another building/location.

NOTE

Public holiday lists in locking device and locations

You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

If a public holiday list is assigned to the location instead of the locking device, the public holiday list for the location is applied to the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

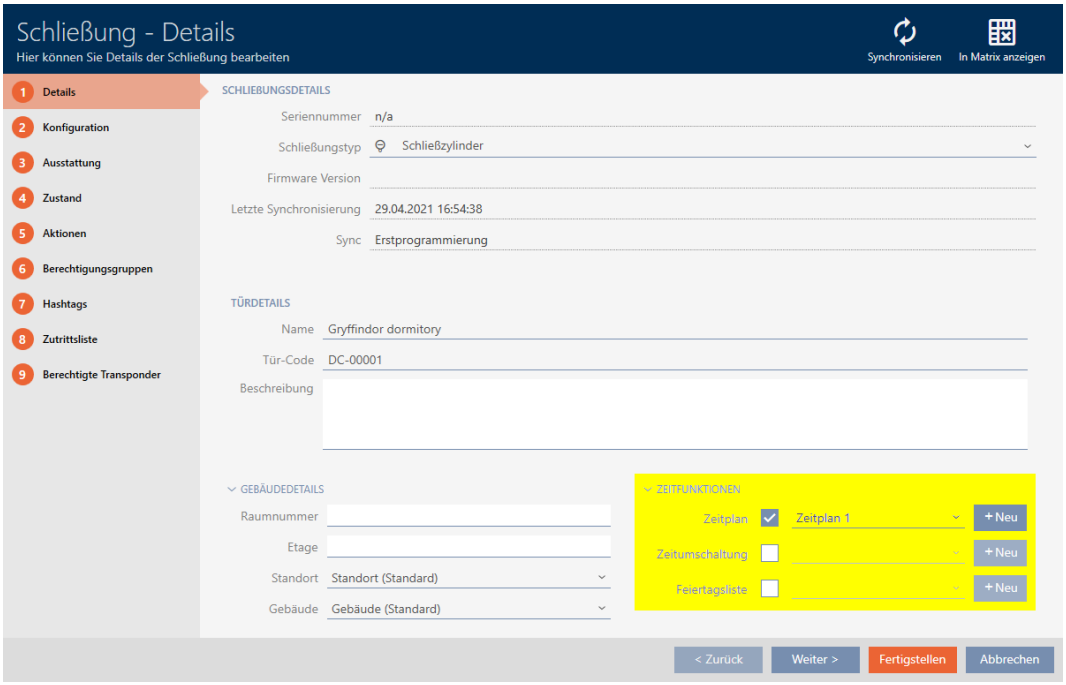
16.7 Limiting authorisations for locking devices to specific times (schedule)

You can limit authorisations to specific days and times with a schedule for your locking device (see *Event management [▸ 366]*).

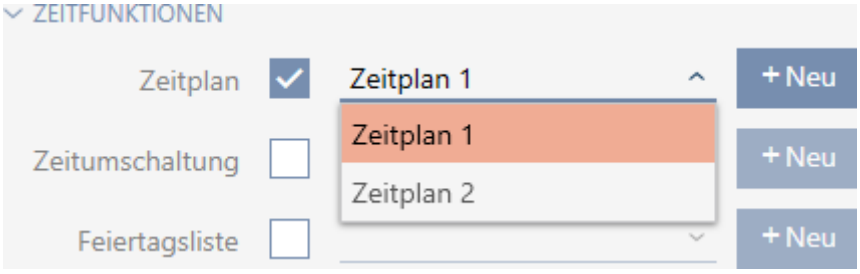
In this chapter you will learn how to add individual locking devices to a schedule using the locking device window. Multiple locking devices can be added more quickly in the schedule itself: *Adding locking devices to the schedule [▸ 272]*.

✓ AXM Lite open.
✓ Locking device created (see *Creating a locking device [▸ 182]*).
✓ Locking device equipped with .ZK option.
✓ Schedule created (see *Creating a schedule [▸ 45]*).

1. Click on the locking device you wish to add.
   ↳ The locking device window will open.

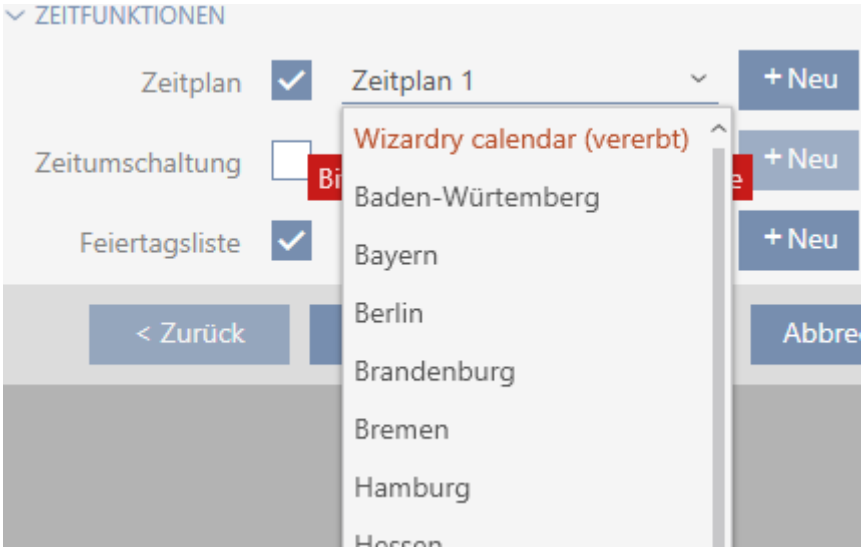


2. Open the "Time functions" menu if necessary.
3. Activate the ☑ Time schedule checkbox.
4. Select the schedule for your locking device from the ▼ **Time schedule** drop-down menu.



5. Activate the ☑ Holiday list checkbox.

6. Select the public holiday list for your locking device from the ▼ **Holiday list**drop-down menu.



NOTE

Public holiday lists in locking device and locations

You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

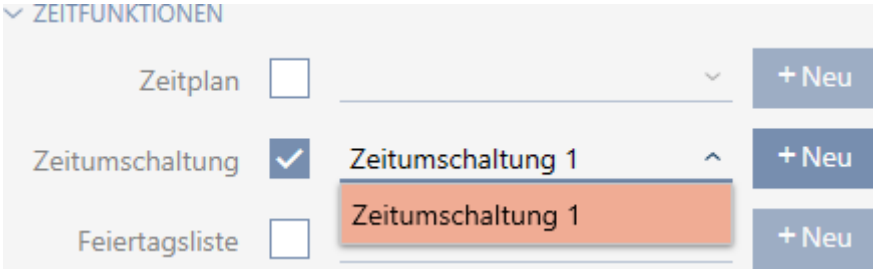
If a public holiday list is assigned to the location instead of the locking device, the public holiday list for the location is applied to the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

7. Click on the Finish button.
   ↳ The locking device window closes.

↳ Locking device is added to the schedule.

16.8 Engaging and disengaging locking devices automatically with time switchover

Ideally, you will have already created your time switchovers before creating the locking devices (see *Best practice: setting up the locking system [▸ 29]* and *Creating a time switchover [▸ 58]*). This allows you to set the time switchovers directly in the locking device properties when creating locking devices:

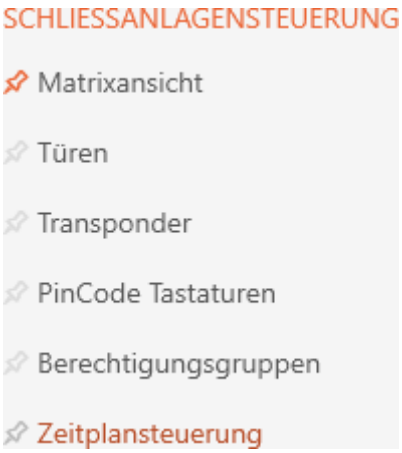


Obviously, you can also add your locking devices to the time switchovers at a later date:

✓ AXM Lite open.
✓ Locking device equipped with .ZK option.
✓ Time switchover created (see *Creating a time switchover [▸ 58]*).

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

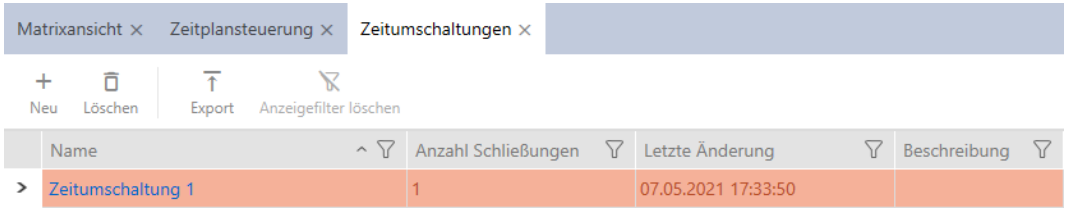
2. Select the Time schedule control entry in the | LOCKING SYSTEM CONTROL | group.



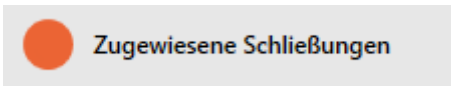
   ↳ The AXM bar will close.
   ↳ The [Time schedule control] tab will open.

3. Click on the Time switching button.

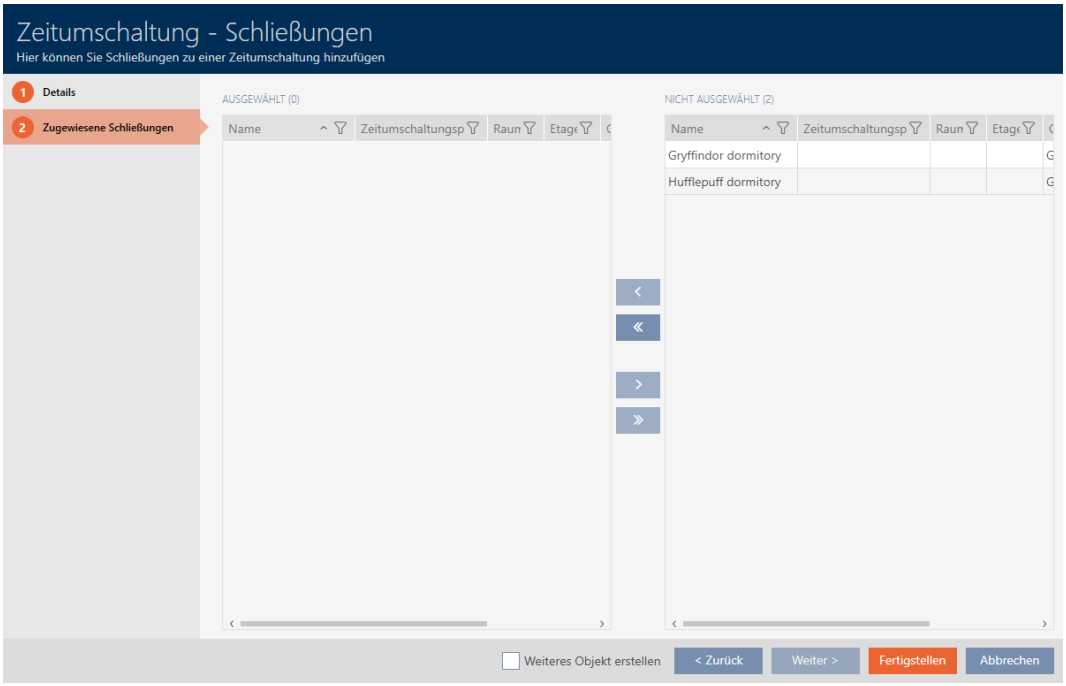
↳ The [Time switching] tab will open.



4. Click on the time switchover to which you wish to add your locking devices.
   ↳ The time switchover window will open.
5. Click on the Assigned locks tab.



↳ Window switches to the "Assigned locks" tab.



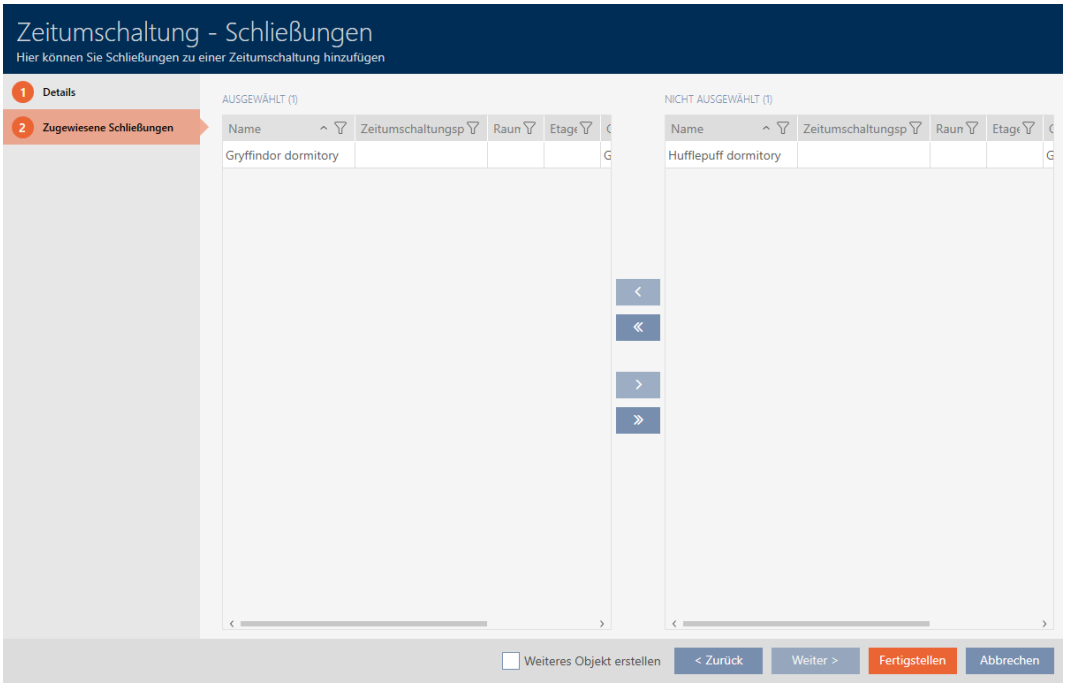
6. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
7. Select all locking devices that you wish to open and close with the schedule (Ctrl+click for single devices or Shift+click for multiple devices).

NOTE

Double-clicking as an alternative to arrow keys

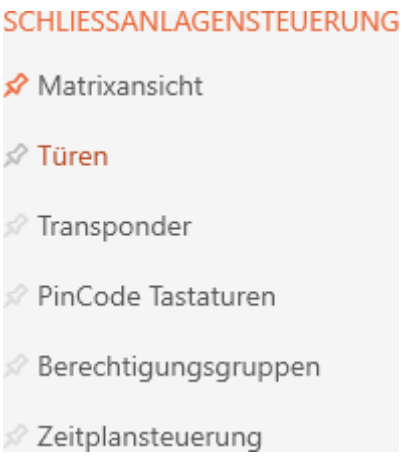
Double-clicking an entry in the list will also move this entry to the other column.

8. Use < to move only the selected locking devices or << to move all locking devices.
   ↳ The selected locking devices in the left-hand column will be added to the time switchover.



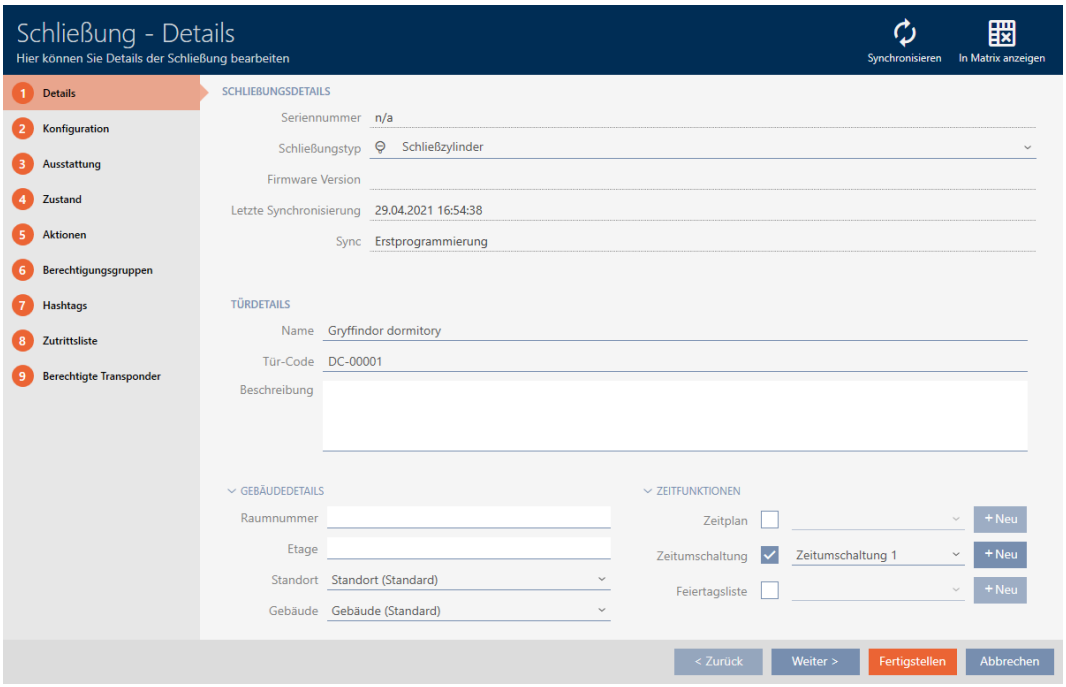
9. Click on the Finish button.
   ↳ The time switchover window closes.
10. Click the orange AXM button AXM.
    ↳ AXM bar opens.

11. Select the entry Locks in the group | LOCKING SYSTEM CONTROL |.

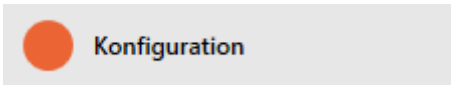


    ↳ The AXM bar will close.
    ↳ The [Locks] tab will open.

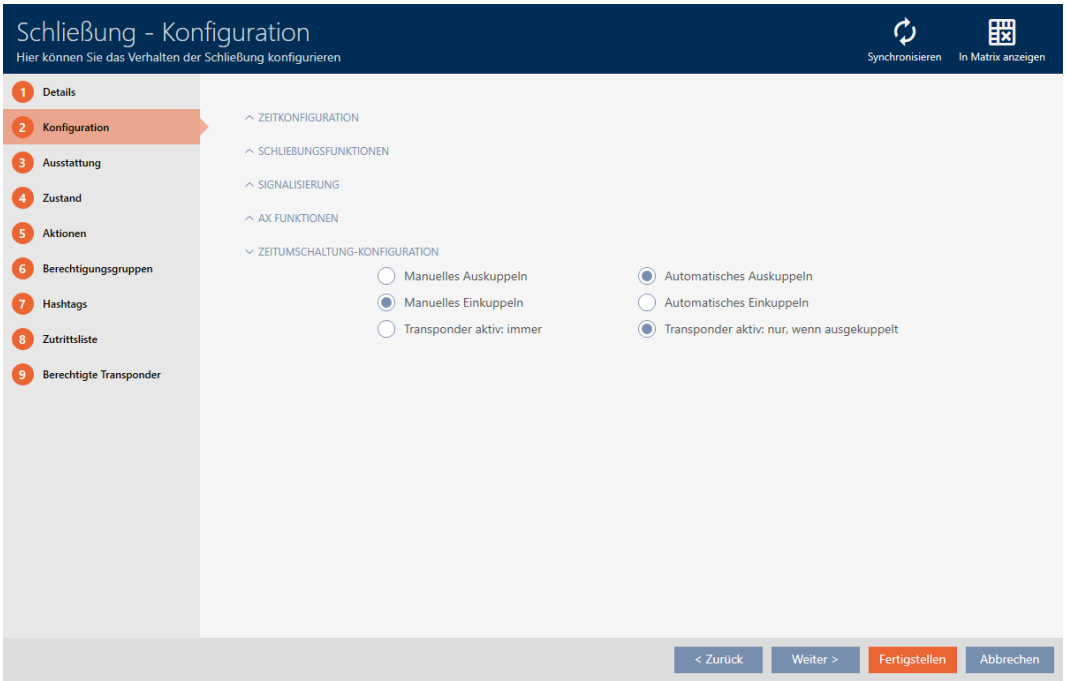
12. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
13. Click on the door to be controlled with the time switchover.
    ↳ The locking device window will open.



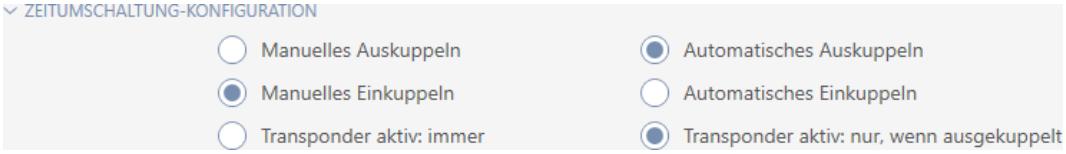
14. Click on the Configuration tab.



    ↳ Window switches to the "Configuration" tab.



15. Set the required behaviour in the "Time switching - Configuration" drop-down menu (see *Time switchovers [▸ 370]*).



16. Click on the Finish button.
    ↳ The locking device window closes.

↳ Time switchover is set up.

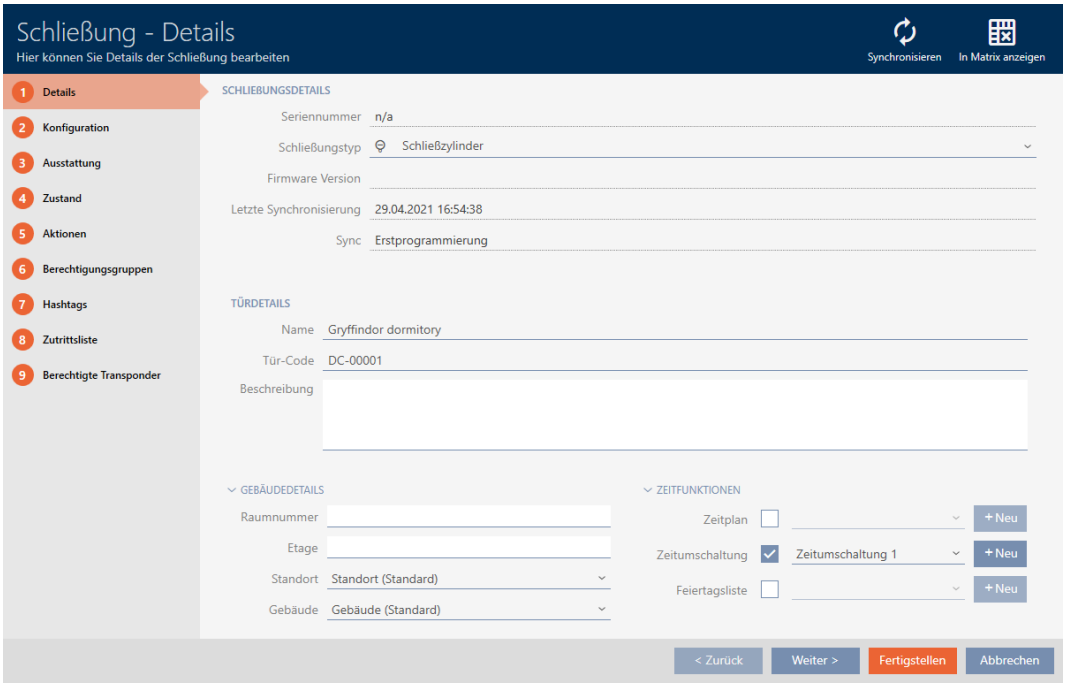
16.9 Have accesses logged by locking device (access list)

This is where you switch the access list on. Your locking device uses it to log which identification media have been activated (also see *Access and physical access lists [▸ 365]*).

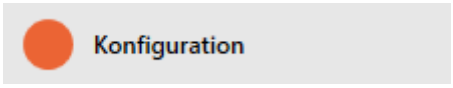
✓ AXM Lite open.

✓ Locking device equipped with .ZK option.

1. Click on the locking device that should log accesses.
    ↳ The locking device window will open.

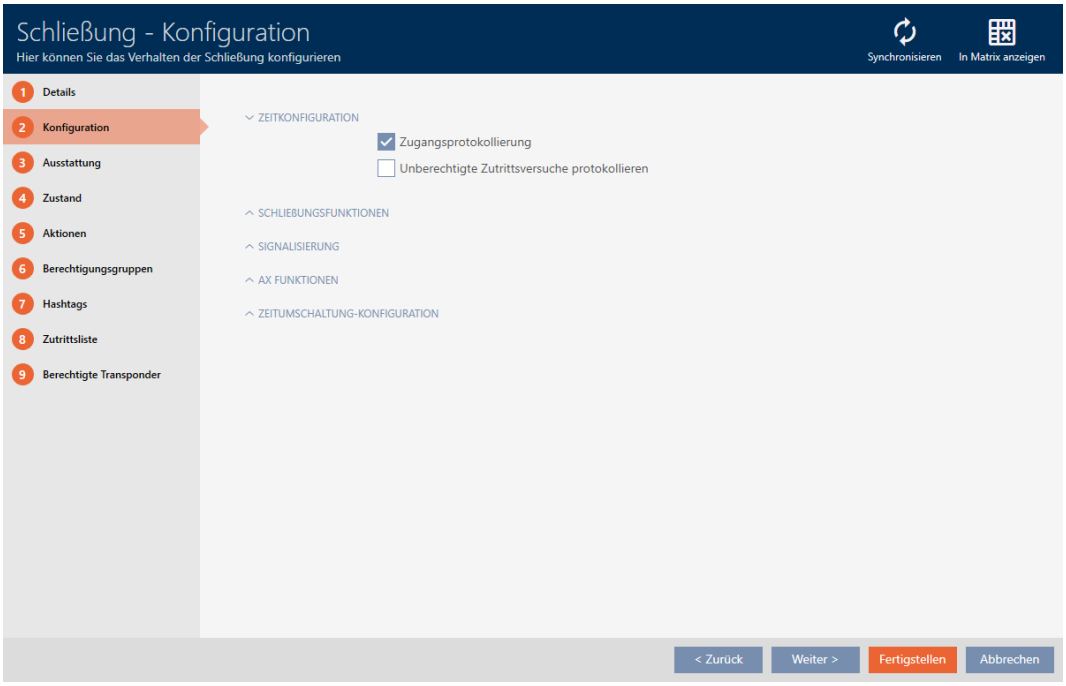


2. Click on the Configuration tab.



↳ Window switches to the "Configuration" tab.

3. Expand the "TIME CONFIGURATION" menu (only displayed for .ZK locking devices).



4. Activate the ☑ Access list checkbox (activated by default for .ZK locking devices).
5. Click on the Finish button.
   ↳ The locking device window closes.

↳ Access logging activated for this locking device.

The logged accesses are imported during synchronisation (see *Synchronising the locking device (including reading access list) [▸ 291]*).

The access list can then be opened in the locking device window using the [Access list] tab (see *Displaying and exporting a locking device's access list [▸ 296]*).

16.10 Leaving the locking device open for longer, less time or permanently

In the default factory setting, AXM Lite programmes your locking devices so that they engage for 5 seconds. However, other settings are also available:

- Pulse opening between 0 s and 25 s: The locking device remains engaged for this time interval after an identification medium has been activated. Then it disengages again automatically.
- Permanent opening: When an identification medium activates the locking device, it engages ready to open and remains engaged. The locking device does not disengage until an identification medium activates it again.

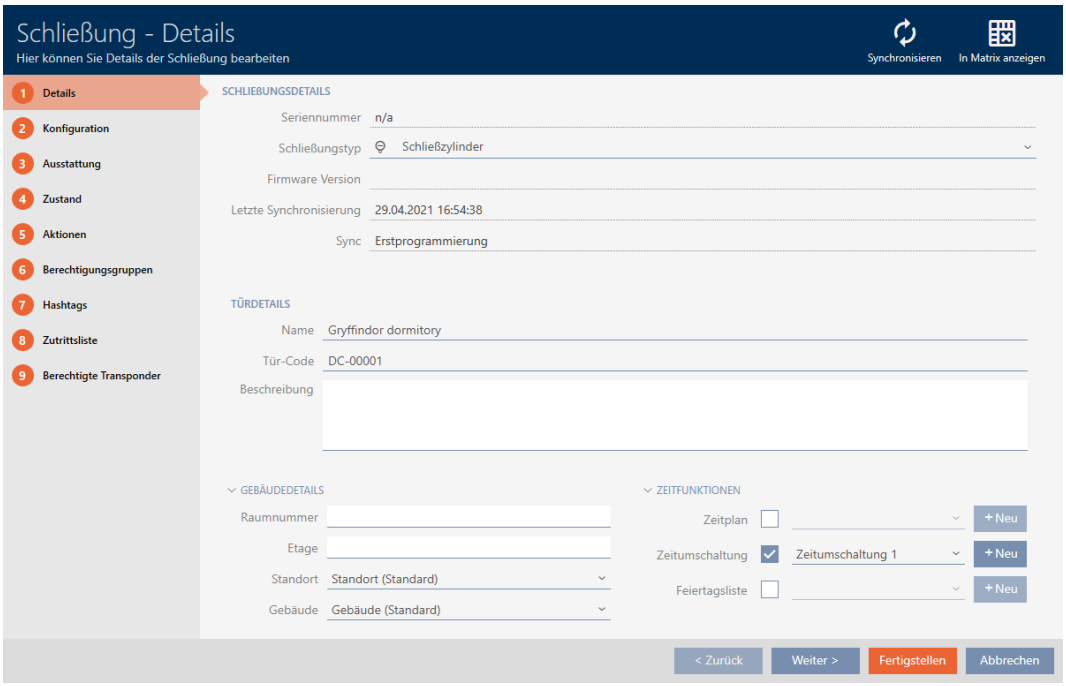
You can also work with settings that are not lock-related:

- *Allowing an identification medium to open twice as long [▸ 100]*
- *Engaging and disengaging locking devices automatically with time switchover [▸ 222]*

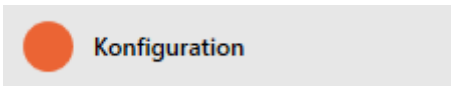
This section describes how to set the impulse interval or activate permanent opening:

✓ AXM Lite open.
✓ Locking device created.

1. Click on the locking device whose opening interval you wish to set.
   ↳ The locking device window will open.

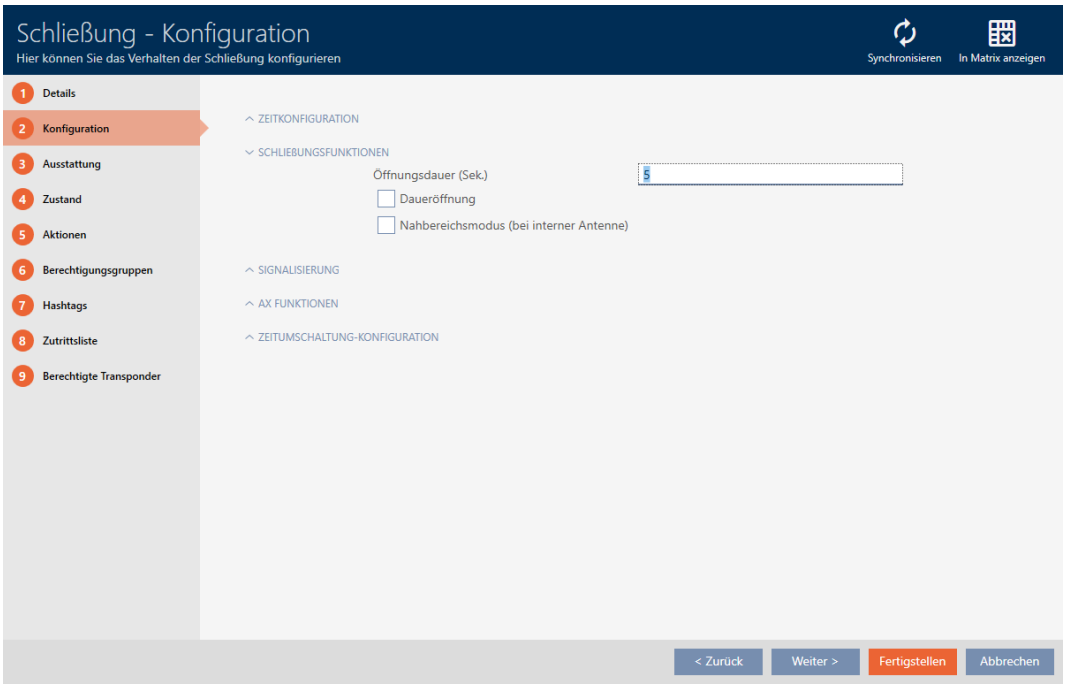


2. Click on the Configuration tab.



   ↳ Window switches to the "Configuration" tab.
3. Expand the "Lock functions" menu.

4. Enter the required engagement interval in the *Open time (sec)* field.



5. Alternatively, activate the ☑ Permanent open checkbox to configure permanent opening.
6. Click on the button Finish
   ↳ The locking device window closes.

↳ The locking device's opening interval is configured.

16.11 Limit locking device read range (close range mode)

Close range mode reduces the read range for locking devices. It is especially important for the freely rotating Digital Cylinder AX to be operated in close range mode. It is equipped with two electronic thumb-turns which would be activated at the same time if close range mode is not activated.

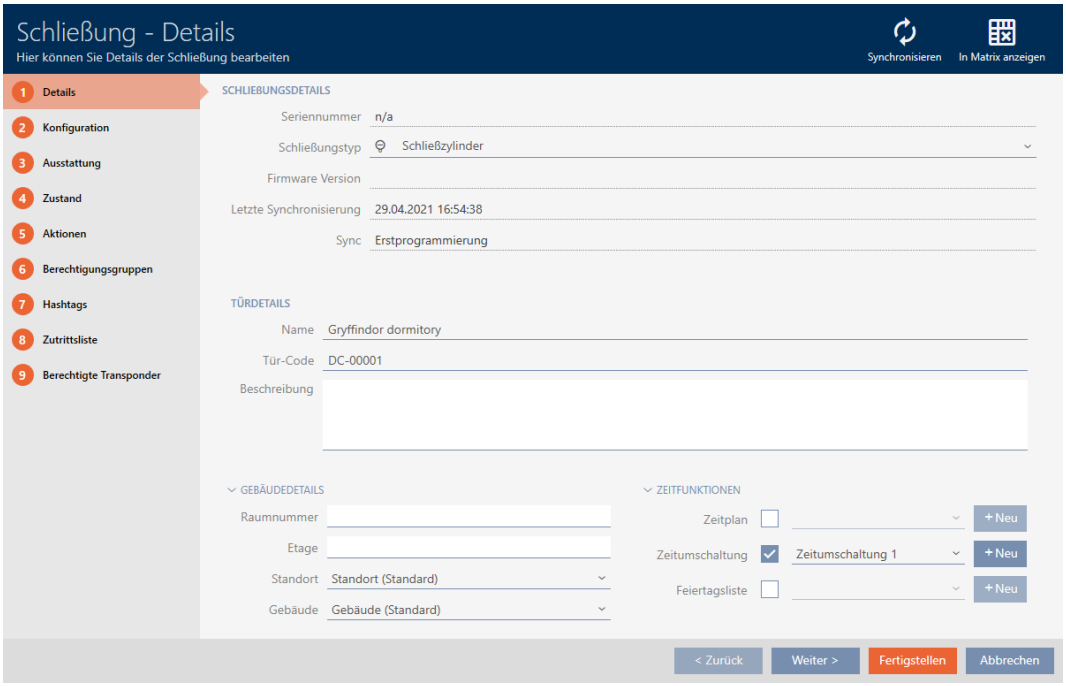
NOTE

Close range mode for freely rotating Digital Cylinder AX activated automatically

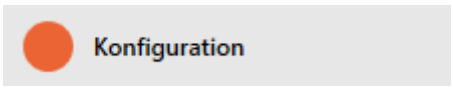
As soon as you activate the ☑ Freely rotating option on a Digital Cylinder AX, AXM Lite will automatically activate the ☑ Close range mode.

✓ AXM Lite open.

1. Click on the locking device whose read range needs to be limited.
   ↳ The locking device window will open.

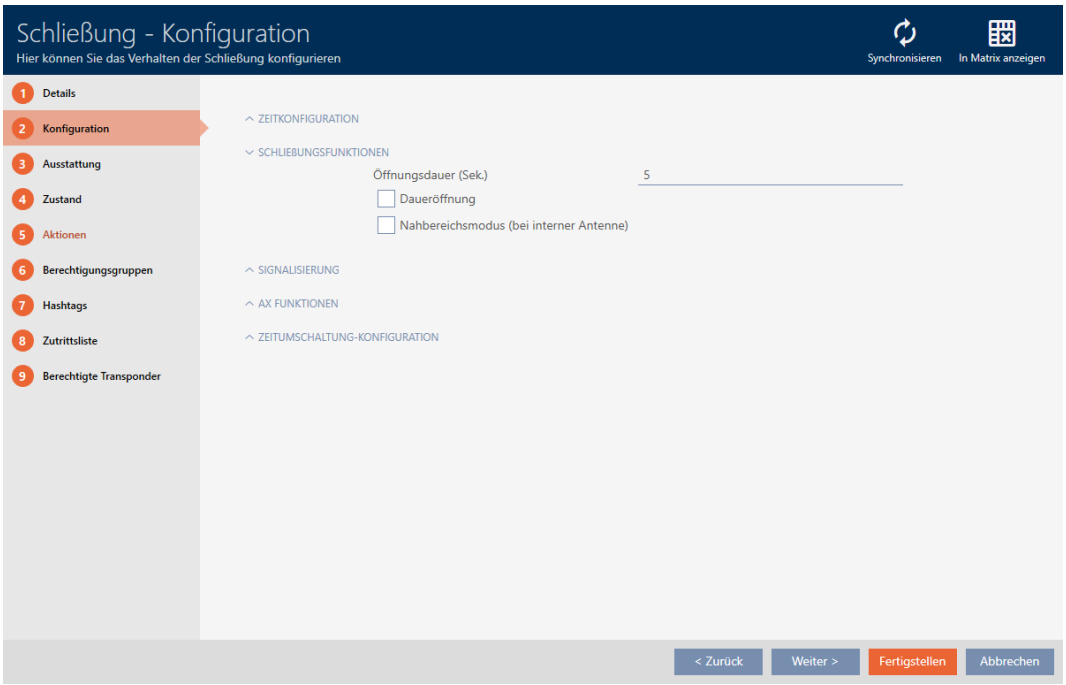


2. Click on the Configuration tab.



↳ Window switches to the [Configuration] tab.

3. Expand the "Lock functions" menu.



4. Activate the ☑ Close range mode check box (only displayed for suitable locking devices).

5. Click on the Finish button.
   ↳ The locking device window closes.

↳ Close range mode activated for this locking device.

16.12 Muting a locking device (for battery warnings and programming)

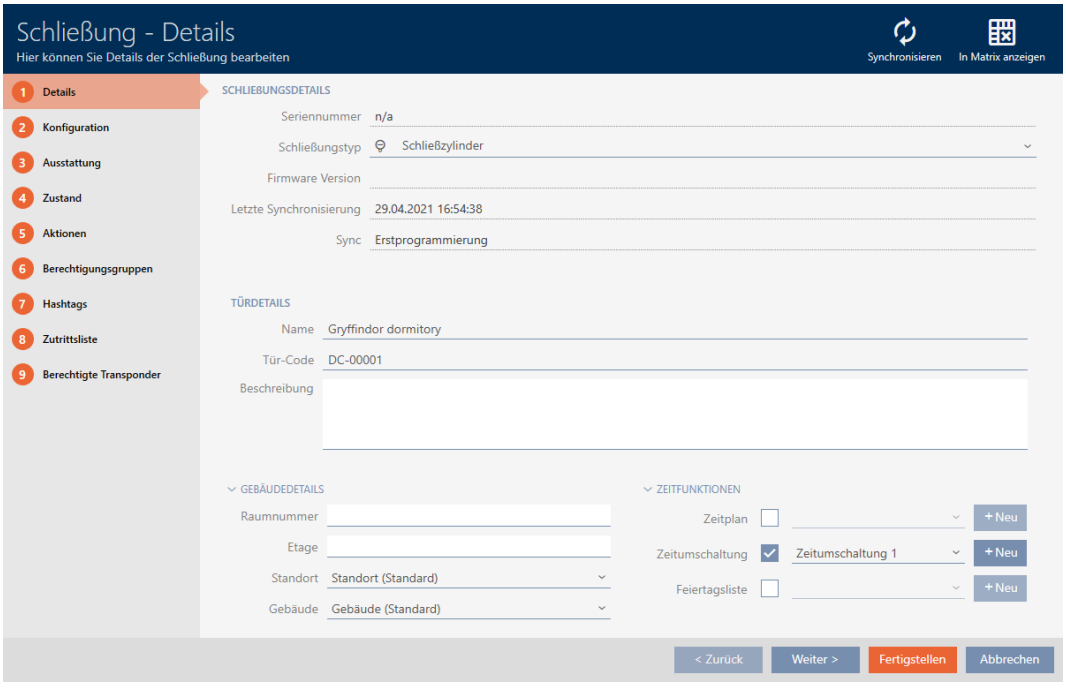
You can deactivate the following signals in the locking device properties:

- Audible and visual battery warnings
- Audible programming acknowledgements

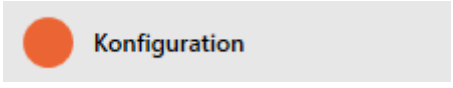
When an identification medium is activated, the locking device signals engaging as usual. You can also configured each identification medium except for PIN code keypads to prevent locking devices from signalling activation of this identification medium (see *Muting all locking devices for a transponder or a card [▸ 102]*).

✓ AXM Lite open.

1. Click on the locking device to be muted.
   ↳ The locking device window will open.

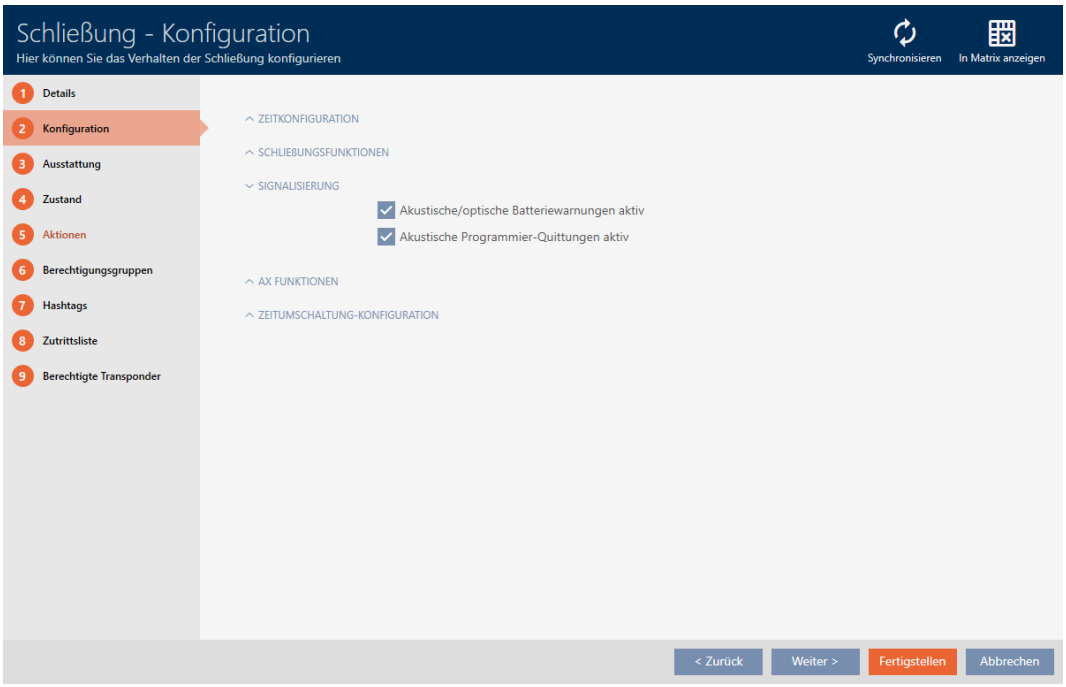


2. Click on the Configuration tab.

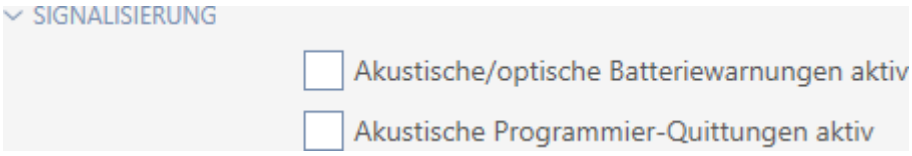


↳ Window switches to the [Configuration] tab.

3. Expand the "Feedback signals" menu.



4. Select the ☐ Acoustic/optical battery warnings active and ☐ Acoustic programming acknowledgments active checkboxes.



5. Click on the Finish button.
   ↳ The locking device window closes.

↳ Locking device will no longer signal any battery warnings or audible programming acknowledgements.

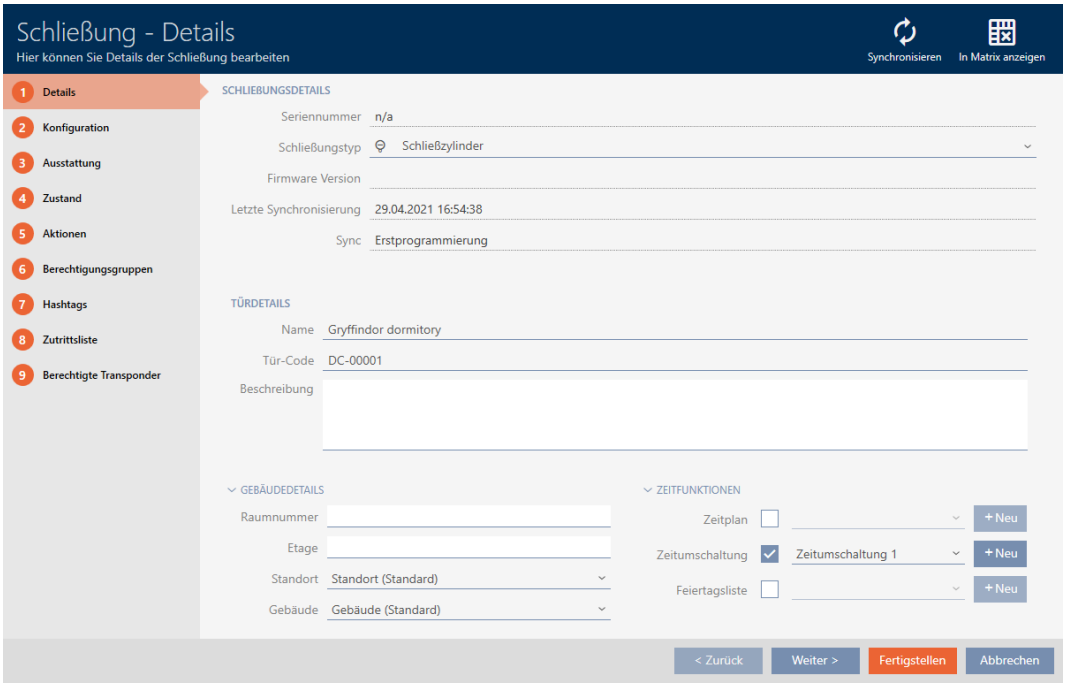
16.13 Ignoring activation and expiry date of identification media

You can enter your identification media's properties to specify that they are to be activated or deactivated on a specific date (see *Activating or deactivating identification medium once at specific times (activation and expiry date) [▸ 104]*).

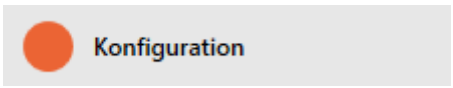
AX locking devices can ignore this activation and expiry date on request and still accept the identification media in question.

✓ AXM Lite open.
✓ AX-based locking device.

1. Click on the locking device to be muted.
   ↳ The locking device window will open.

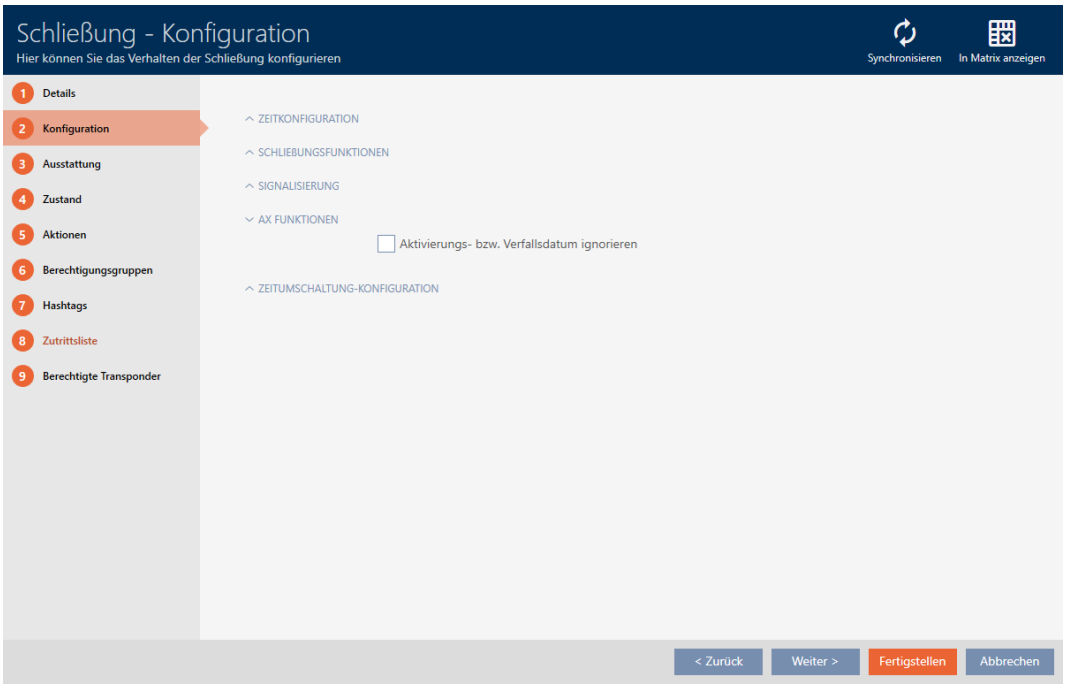


2. Click on the Configuration tab.

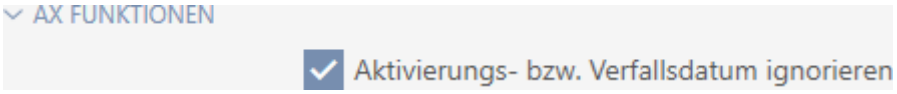


↳ Window switches to the [Configuration] tab.

3. Expand the "AX functions" menu.



4. Select the ☑ Ignore activation or expiry date checkbox.



5. Click on the Finish button.
   ↳ The locking device window closes.

↳ Locking device can also be operated with identification media that are not within their activation period.

16.14 Setting up door monitoring (DoorMonitoring)

You can use DoorMonitoring to monitor the status of your doors and locking devices (also see *DoorMonitoring [▸ 380]*).

NOTE

DoorMonitoring without direct networking (“WaveNet”) available to a limited extent

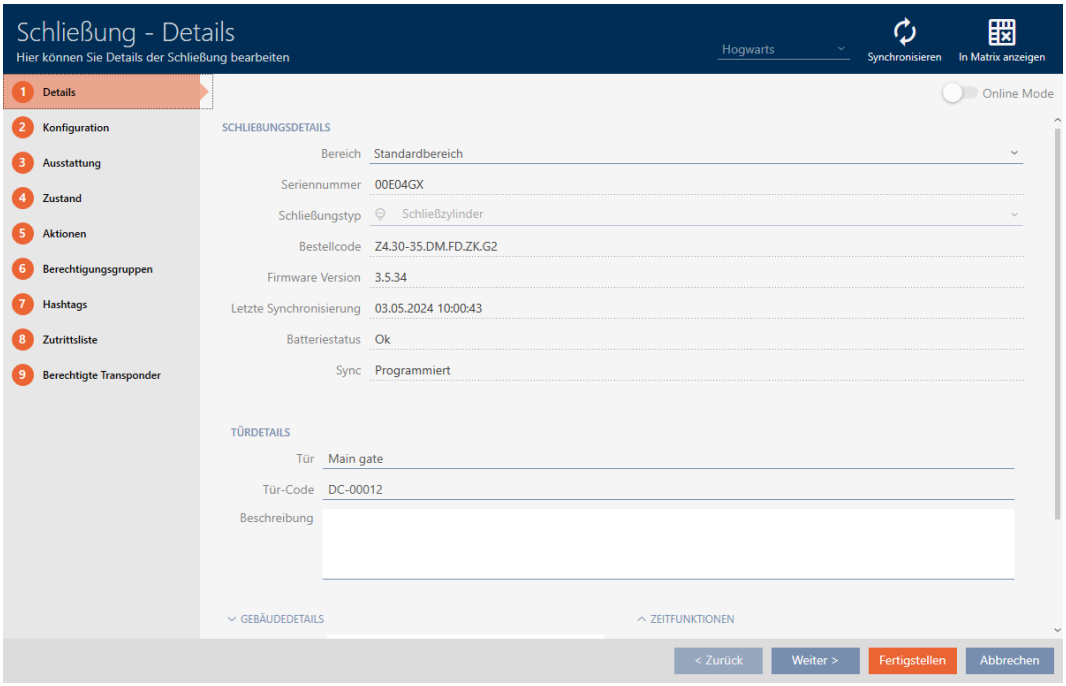
In a directly networked locking system, locking devices connected to the WaveNet can immediately transmit their DoorMonitoring events via the network. You can see these events in your locking plan software (e.g. AXM) in no time.

Locking devices without WaveNet also log their DoorMonitoring events and save them in the access list. You will only see these events after reading the access list in your locking plan software.

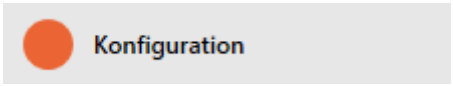
16.14.1 Setting up DoorMonitoring for locking cylinders

✓ AXM Lite open.
✓ Locking device is DoorMonitoring-capable (item code contains .DM).

1. Click on the locking device for which you wish to set up DoorMonitoring.
   ↳ The locking device window will open.

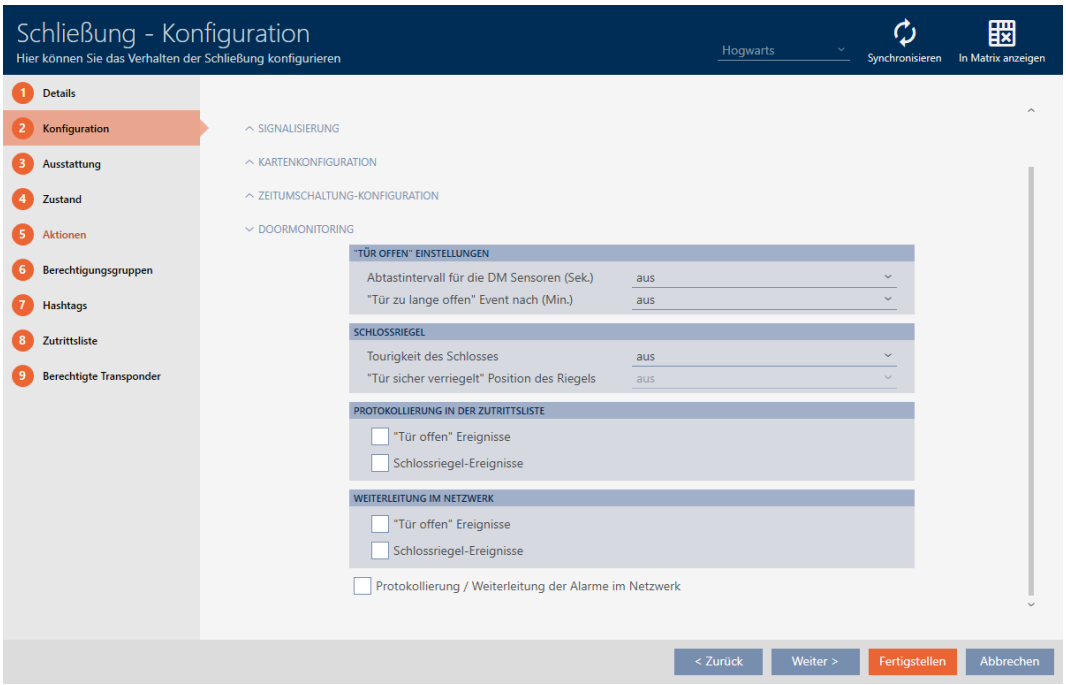


2. Click on the Configuration tab.



↳ Window switches to the [Configuration] tab.

3. Expand the "DoorMonitoring" menu.



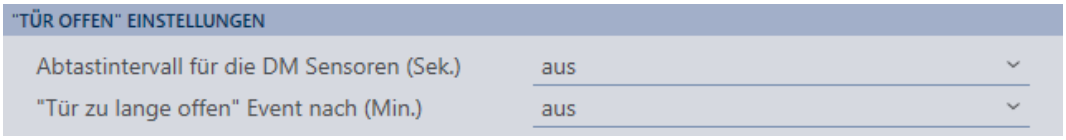
4. Configure the preferred settings.

5. Click the Finish button.
   ↳ The locking device window closes.

↳ DoorMonitoring is set up for this locking device.

You can select the following settings:

"Door open" settings

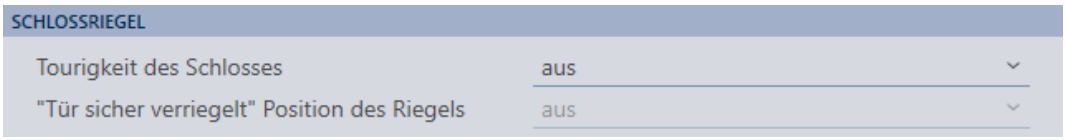


Your DoorMonitoring locking cylinders detect whether the door is open or closed with the help of a special fastening screw and a magnetic tab.

Setting	Explanation
Sampling interval for the DM sensors (sec.)	The frequency with which the locking cylinder checks whether the magnetic tab is in front of the fastening screw. In this case, the door is considered closed. Possible intervals are: ■ seconds ■ second ■ seconds ■ seconds ■ seconds ■ seconds ■ seconds More frequent checks lead to faster detection of an open door, but also increase power consumption.

Setting	Explanation
"Door open too long" event after (min.)	Safety-relevant doors such as fire doors must not be permanently open. This setting allows you to see if a door is open for longer than usual. This door could be wedged open, for example. After the set time has elapsed, the Door open too long event is triggered. Possible intervals: ■ minutes ■ minutes ■ minute ■ minutes ■ minutes ■ minutes

Lock bolt



Your DoorMonitoring locking cylinder uses a special sensor to detect how often the cam has been turned. With the aid of the following settings, the system then knows how far the dead bolt has been extended.

Setting	Explanation
Number of turns to lock	The number of turns required to fully extend the mortise lock dead bolt. Possible intervals are: ■ off ■ 1-turn ■ 2-turn ■ 3-turn ■ 4-turn

Setting	Explanation
“Door securely locked" position of dead bolt	In two- or multi-turn mortise locks, the door may be locked, but the dead bolt has not yet been extended far enough to rest securely in the door anchorage. In this case, the door is only considered Door is locked, but not Door is securely locked. This setting is used to specify how many turns are required until the dead bolt is extended far enough into the door and the locking device is considered secure. The available settings depend on what you have specified in Number of turns to lock: ▪ off ▪ ▪ ▪ ▪

Logging in the access list

You can also log DoorMonitoring events in your access list. This means that you can use DoorMonitoring to a limited extent, even without direct networking.

You can use these settings to specify which events are written into the access list for your DoorMonitoring locking device.

Setting	Explanation
"Door open" events	Select this checkbox to write "Door open" events into the access list for your locking device. This applies to these events: ■ Door is open ■ Door is closed ■ Door is open for a long time
Lock bolt events	Select this checkbox to write Lock bolt events into the access list for your locking device. This applies to these events: ■ Door is locked ■ Door is securely locked

Forward in network

DoorMonitoring works best with a directly networked system (WaveNet). In order to find the best setting for your particular circumstances, you can decide which events you wish to forward to your database via your WaveNet.

Additional forwarding means increased radio traffic and thus increased power consumption.

Setting	Explanation
"Door open" events	Select this checkbox to forward "Door open" events to the database. This applies to these events: ■ Door is open ■ Door is closed ■ Door is open for a long time If you select this checkbox, the events are also automatically saved in the access list.

Setting	Explanation
Lock bolt events	Select this checkbox to forward Lock bolt events to the database. This applies to these events: ■ Door is locked ■ Door is securely locked If you select this checkbox, the events are also automatically saved in the access list.
Event logging/forwarding of alarms in the network	Your DoorMonitoring locking device detects various alarm situations. You can forward these to your database. Examples of such situations are: ■ Door open too long ■ Tampering attempt (e.g. Fastening screw has been manipulated) ■ Door has been opened even though it is considered locked or securely locked

16.15 Changing the SmartRelay settings

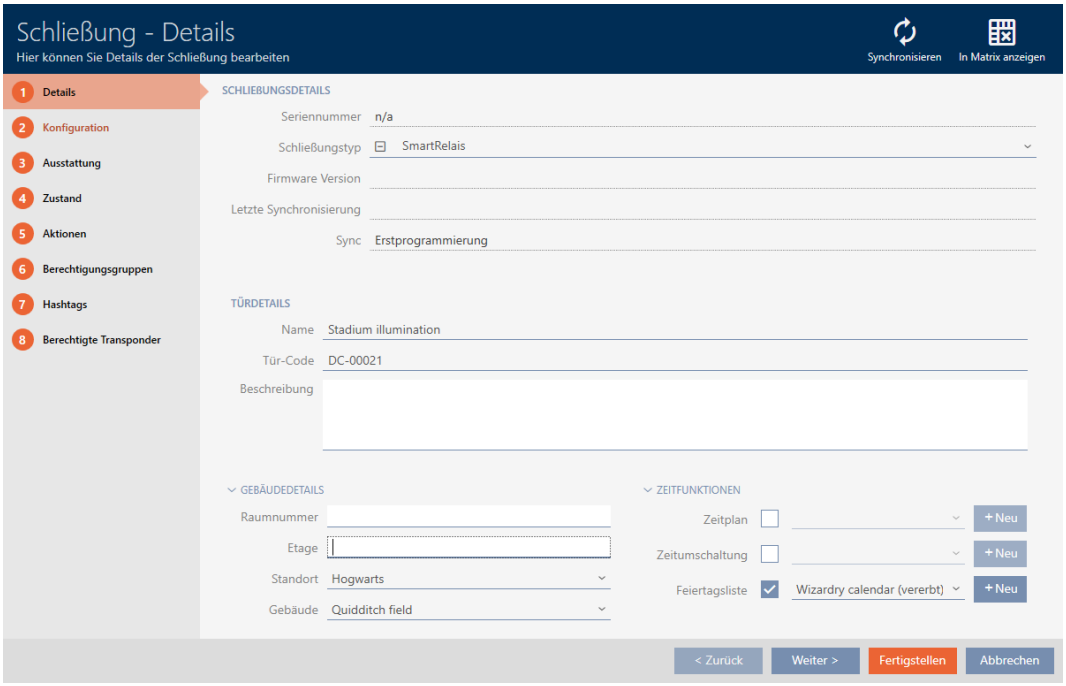
You will only see the settings for SmartRelay if you:

- Create a new locking device and have not yet clicked on Finish, or
- Have opened a "SmartRelays" locking device.

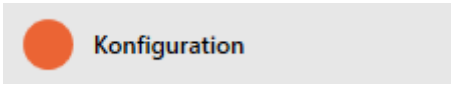
All SmartRelay settings are changed in the "Configuration" tab:

✓ AXM Lite open.
✓ Locking device list or matrix view open.

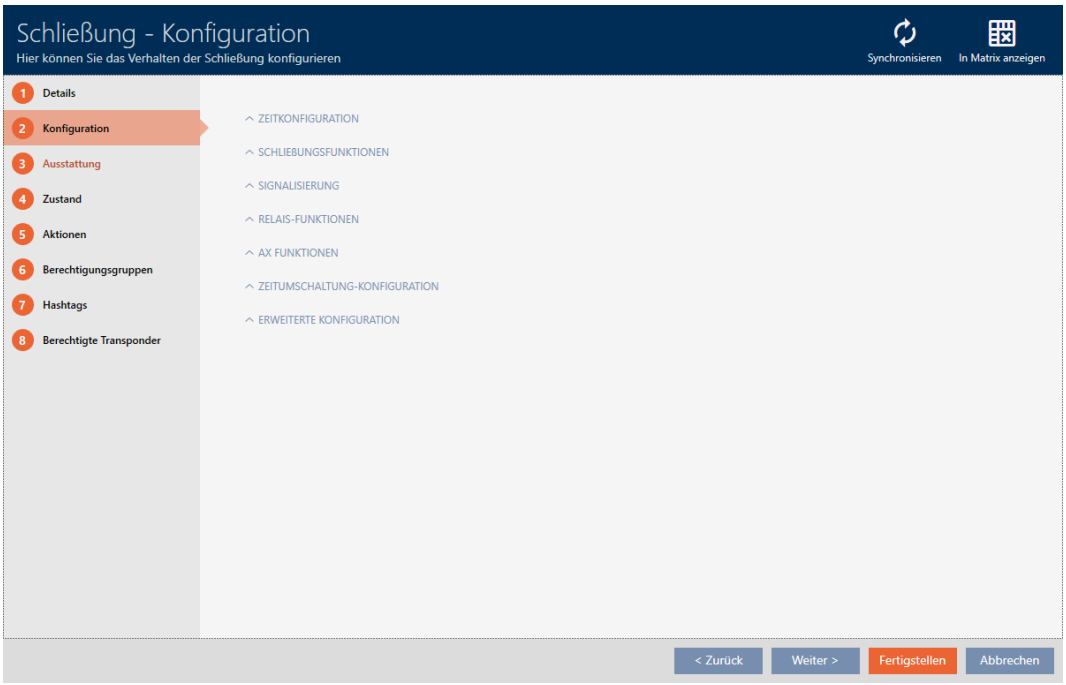
1. Click on the SmartRelay.
   ↳ The SmartRelay window will open.



2. Click on the Configuration tab.



↳ Window switches to the "Configuration" tab.



16.15.1 Using internal and external antenna simultaneously

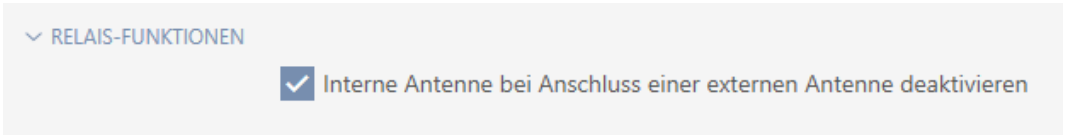
An external antenna is available for some SmartRelays (SREL.AV).

The internal antenna is normally deactivated as soon as SmartRelay detects an external antenna.

You can also use AXM Lite to configure the settings so that both antennas are used at the same time:

✓ "Configuration" tab open (see *Changing the SmartRelay settings [▸ 242]*).

1. Open the "Relay functions" menu if necessary.



2. Activate the ☐ Disable internal antenna when connecting an external antenna checkbox.
3. Click on the Finish button.
   ↳ The SmartRelay window closes.

↳ The SmartRelay's internal antenna will remain active even when an external antenna is connected.

16.15.2 Invert outputs

A relay has two states:

- Energised (coil energised)
- Not energised (idle state)

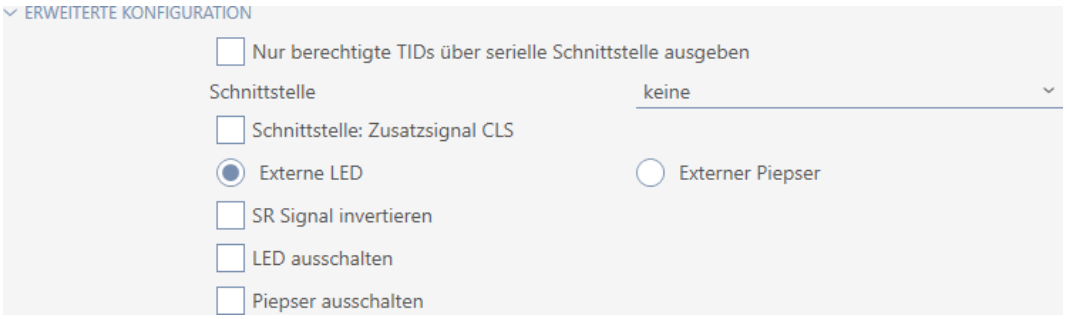
The relay is normally in the idle state and is energised when an identification medium is activated.

The ☑ Invert SR signal checkbox changes the SmartRelay's behaviour depending on the type of output (NO or changeover contact):

Changeover contact	NO contact
■ SREL ■ SREL.ADV ■ SREL.W ■ SREL.G2 ■ SREL.W.G2 ■ SREL 3 ■ SREL 3 Advanced ■ SREL AX Classic	SREL2.G2
☐ Invert SR signal ■ Identification medium activated: Relay energises, COM connected to NO ■ Identification medium not activated: Relay in idle state, COM connected to NC	☐ Invert SR signal ■ Identification medium activated: Relay energises, contacts connected ■ Identification medium not activated: Relay in idle state, contacts not connected
☑ Invert SR signal ■ Identification medium activated: Relay in idle state, COM connected to NC ■ Identification medium not activated: Relay energises, COM connected to NO	☑ Invert SR signal ■ Identification medium activated: Relay in idle state, contacts not connected ■ Identification medium not activated: Relay energises, contacts connected

✓ "Configuration" tab open (see *Changing the SmartRelay settings [▸ 242]*).

1. Open the "Extended configuration" menu if necessary.



2. Activate the ☑ Invert SR signal checkbox.

3. Click on the Finish button.
   ↳ The SmartRelay window closes.

↳ SmartRelay outputs are inverted.

16.15.3 Using the serial interface

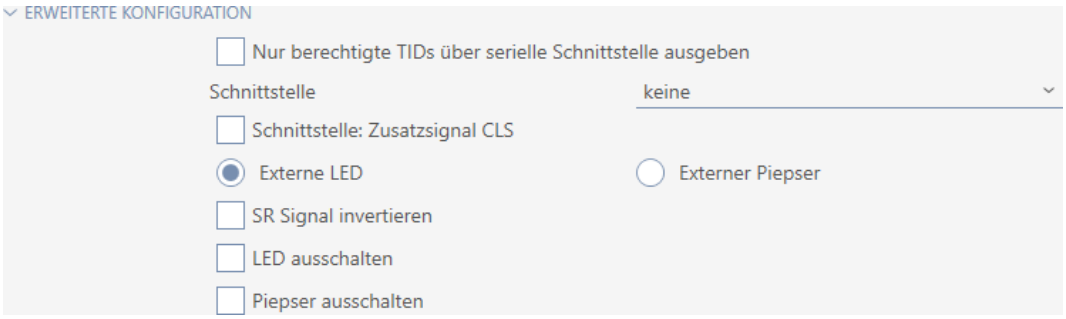
SmartRelays with a serial interface can transfer data from identification media to third-party systems. The following systems are available:

- "None"
- "Wiegand, 33 bit"
- "Wiegand, 26 bit"
- "Primion"
- "Siemens"
- "Kaba Benzing"
- "Gantner Legic"
- "Isgus"

To transfer data, configure the serial interface so that it is compatible with the required third-party system. You can find details on wiring in the manual for the SmartRelay in question.

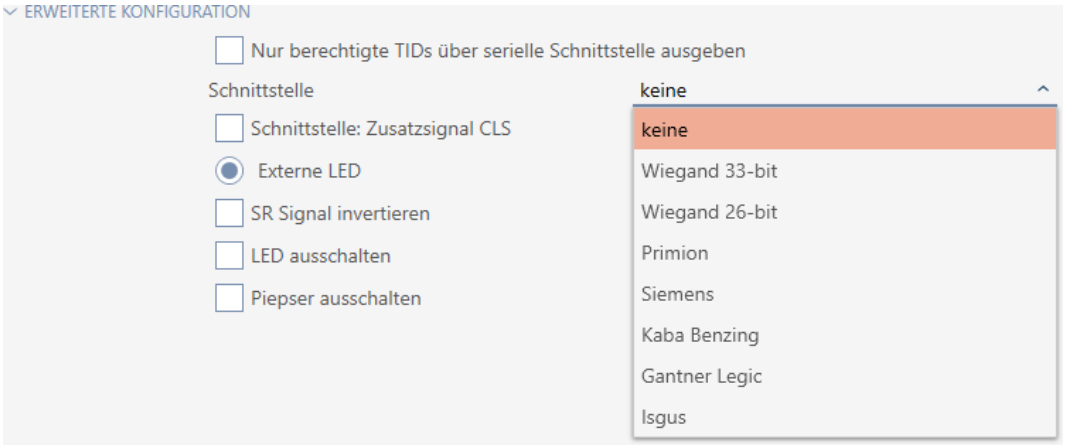
✓ "Configuration" tab open (see *Changing the SmartRelay settings [▸ 242]*).

1. Open the "Extended configuration" menu if necessary.



2. If you do not wish to transfer unauthorised identification media to the third-party system at all, select the ☑ Only issue authorised TIDs via serial interface checkbox.

3. Select the third-party system from the ▼ **Interface** drop-down menu: "Wiegand, 33 bit", "Wiegand, 26 bit", "Primion", "Siemens", "Kaba Benzing" "Gantner Legic" or "Isgus".



4. If you need a card load signal for your third-party system, select the ☑ Interface: Supplementary signal CLS checkbox.
5. Click the Finish button.
   ↳ The SmartRelay window closes.

↳ SmartRelay's serial connection is activated.

16.15.4 Changing the signalling

Different situations may require different signals.

You can configure signalling of your SmartRelay in AXM Lite to meet these different needs.

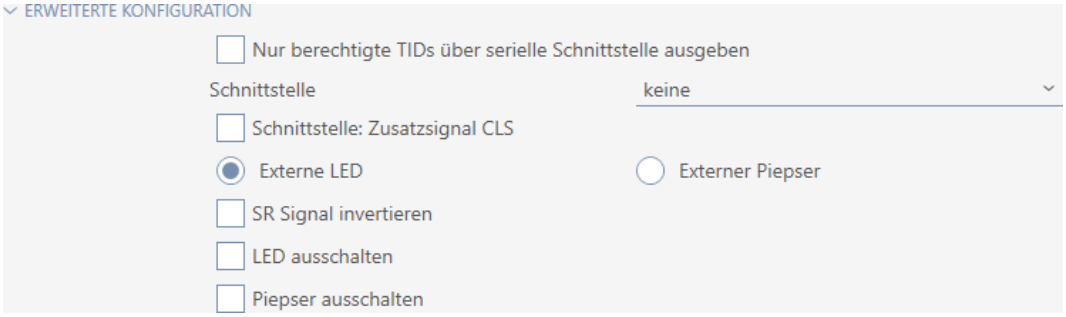
There is a connection for an external LED or an external beeper on the SREL.ADV and SREL2.G2. You can find details on connection in the manual for the SmartRelay concerned.

You can use the ◉ External LED or ◉ External beeper option to configure whether the connection switches permanently during opening or only when switching to ground.

◉ External LED	◉ External beeper
Connection permanently switches to ground during opening. The LED lights up as long as the SmartRelay is switched on.	Connection only switches when switching over. The beeper only beeps when the SmartRelay switches over. Continuous beeping would be annoying.

✓ "Configuration" tab open (see *Changing the SmartRelay settings [▸ 242]*).

1. Open the "Extended configuration" menu if necessary.



2. Choose between the ◉ External LED and ◉ External beeper options.
3. If necessary, use the ☑ Turn off LED or ☑ Turn off beeper checkboxes to switch off the LED or the beeper on your SmartRelay (also applies to external LEDs or external beepers).
4. Click on the Finish button.
   ↳ The SmartRelay window closes.

↳ The SmartRelay's signalling has been changed.

16.16 Planning and tracking locking device management tasks

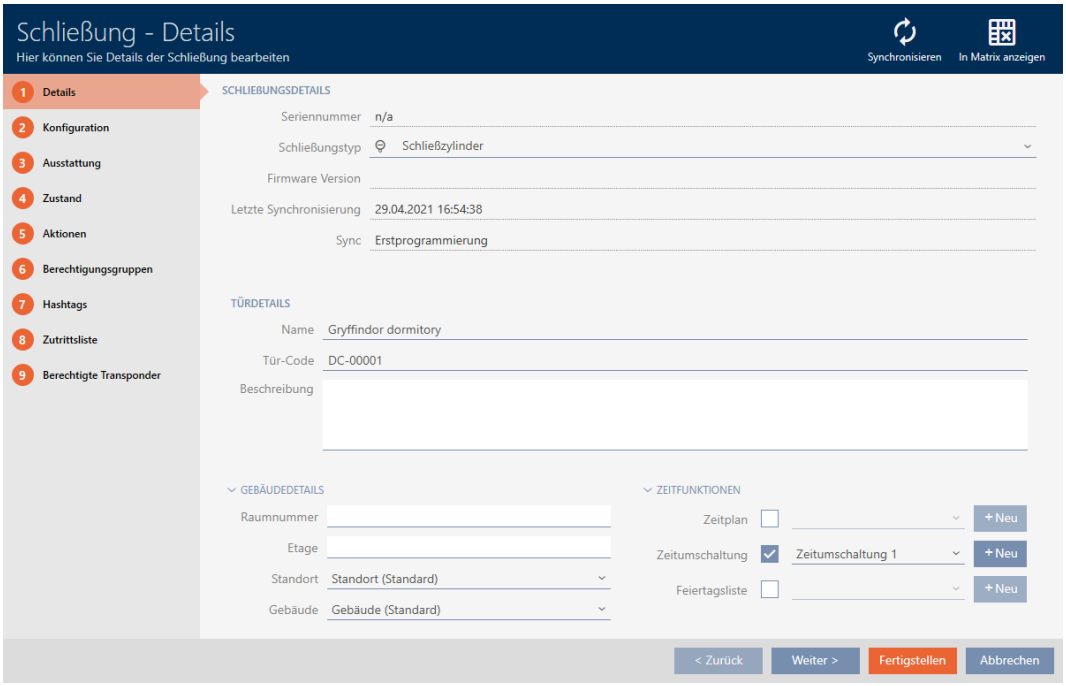
The central point of contact for managing your locking device is the "Actions"tab.

The following entries are displayed here collectively:

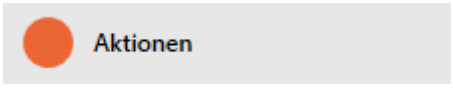
- Created
- Programming
- Installed
- Replaced
- Removed
- Scheduled battery change
- Last battery change

✓ AXM Lite open.
✓ Locking device has been created.

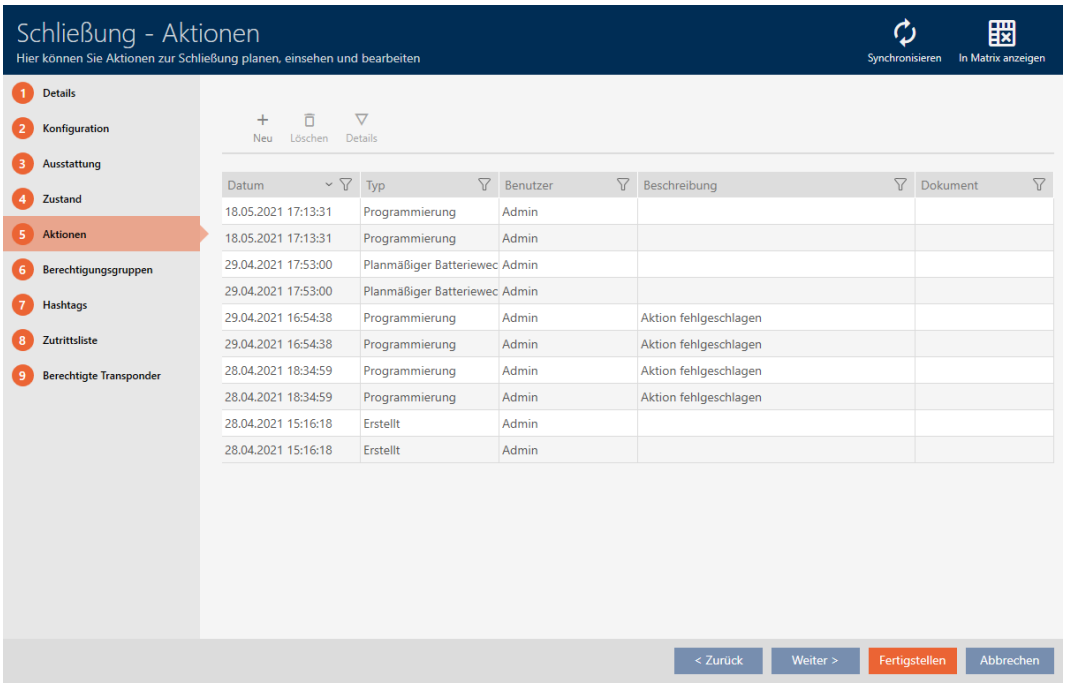
1. Click on the locking device you wish to manage.
   ↳ The locking device window will open.



2. Click on the Actions tab.



↳ Window switches to the "Actions" tab.

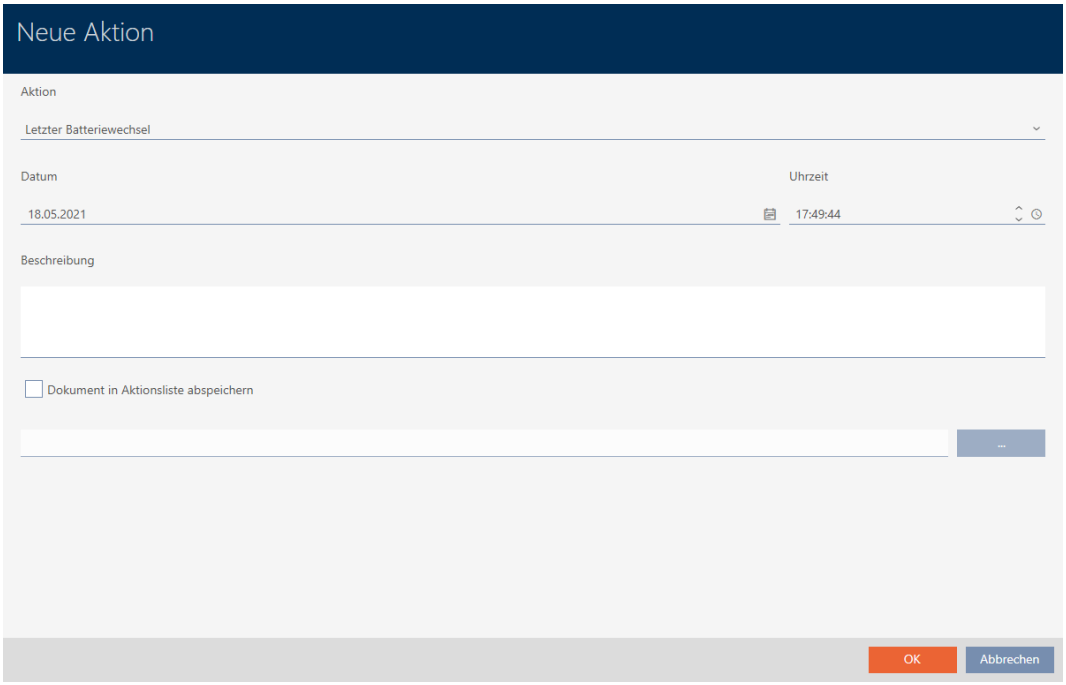


3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

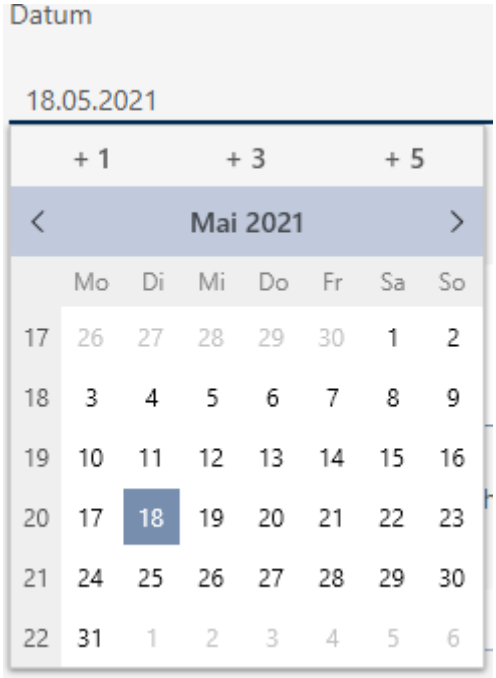
16.16.1 Note installation, replacement or removal date

✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks [▸ 248]*).

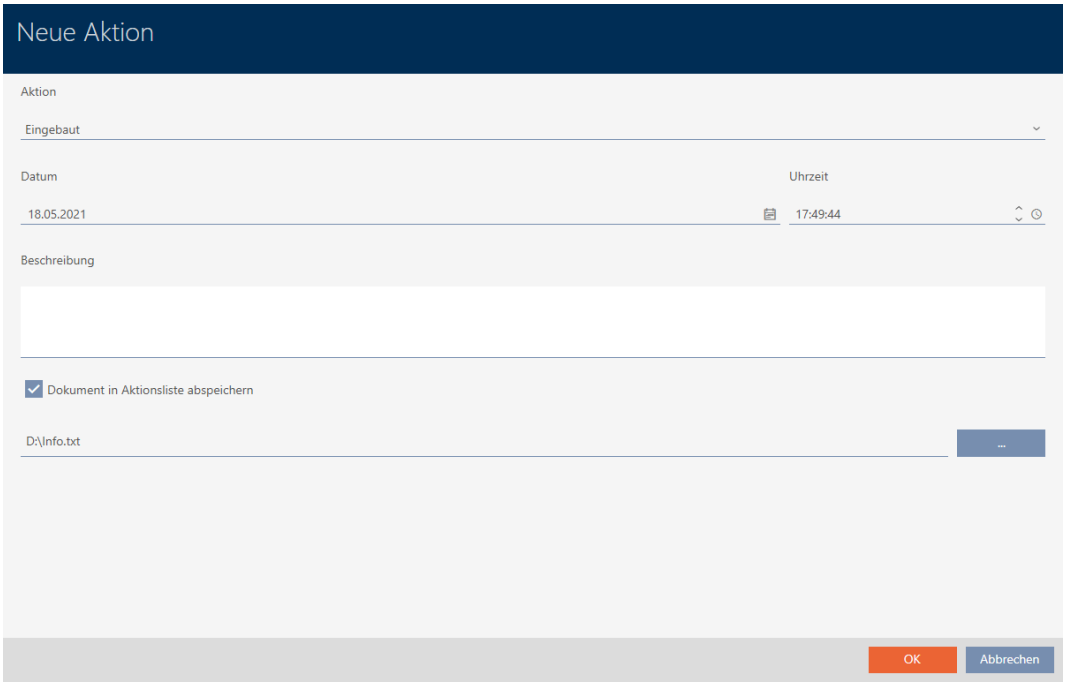
1. Click on the New + button.
   ↳ The window for a new action will open.



2. Select the "Installed", "Replaced" or "Removed" entry from the ▼ **Action** drop-down list.
3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.
7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.



10. Click on the OK button.
    ↳ The window for the new action closes.

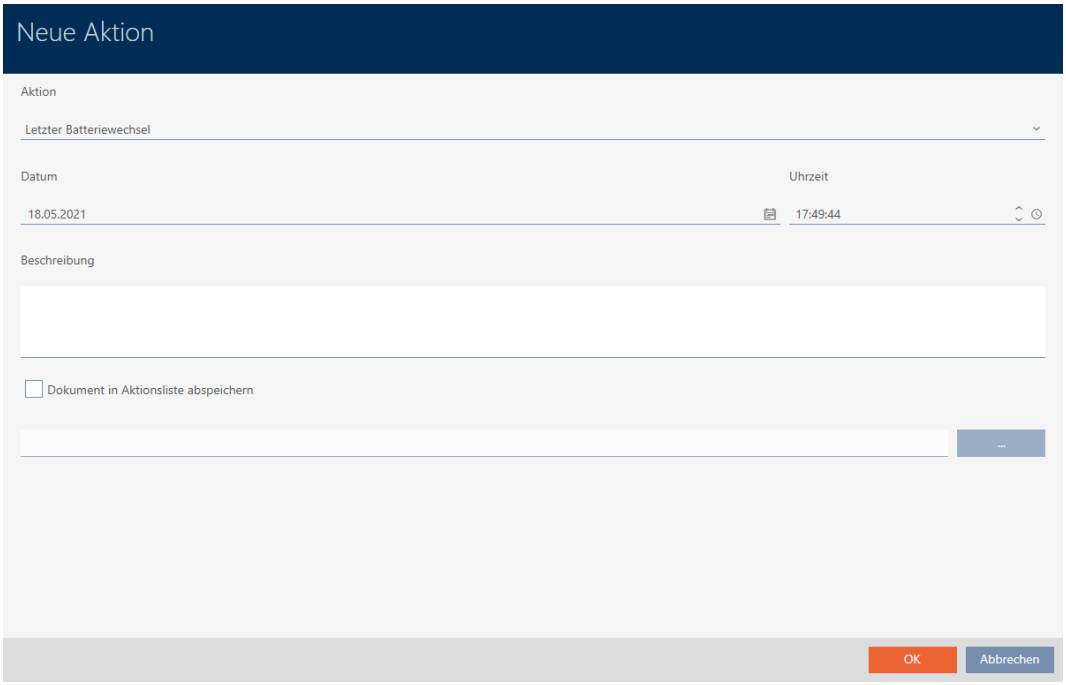
↳ Action is now created and listed.

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		

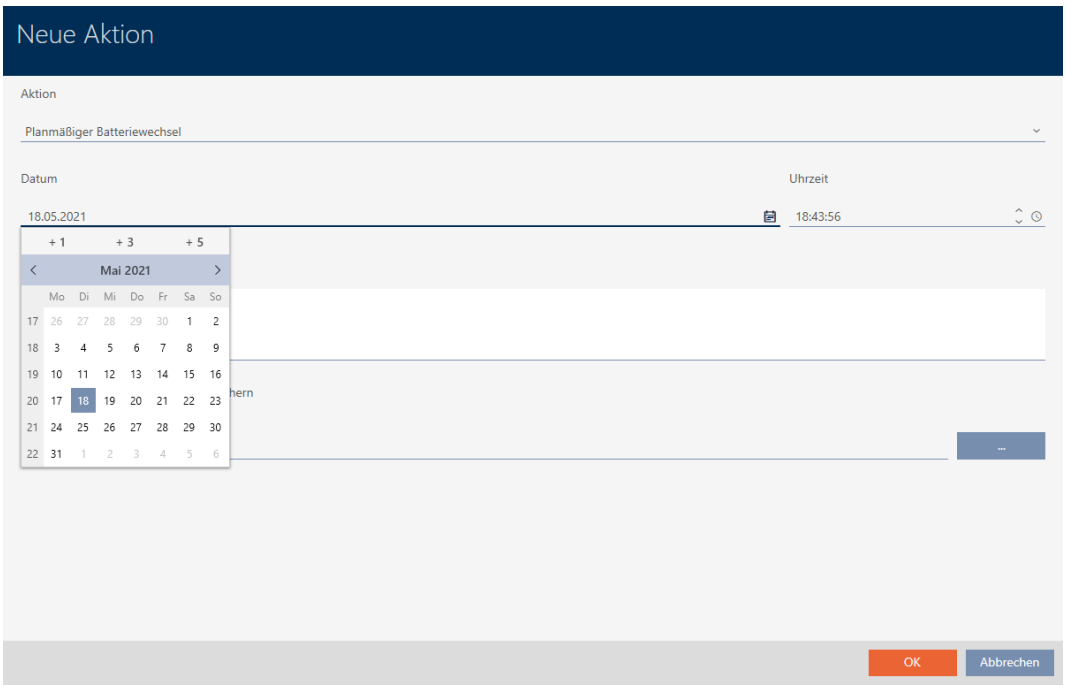
16.16.2 Planning and logging battery replacement

✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks [▸ 248]*).

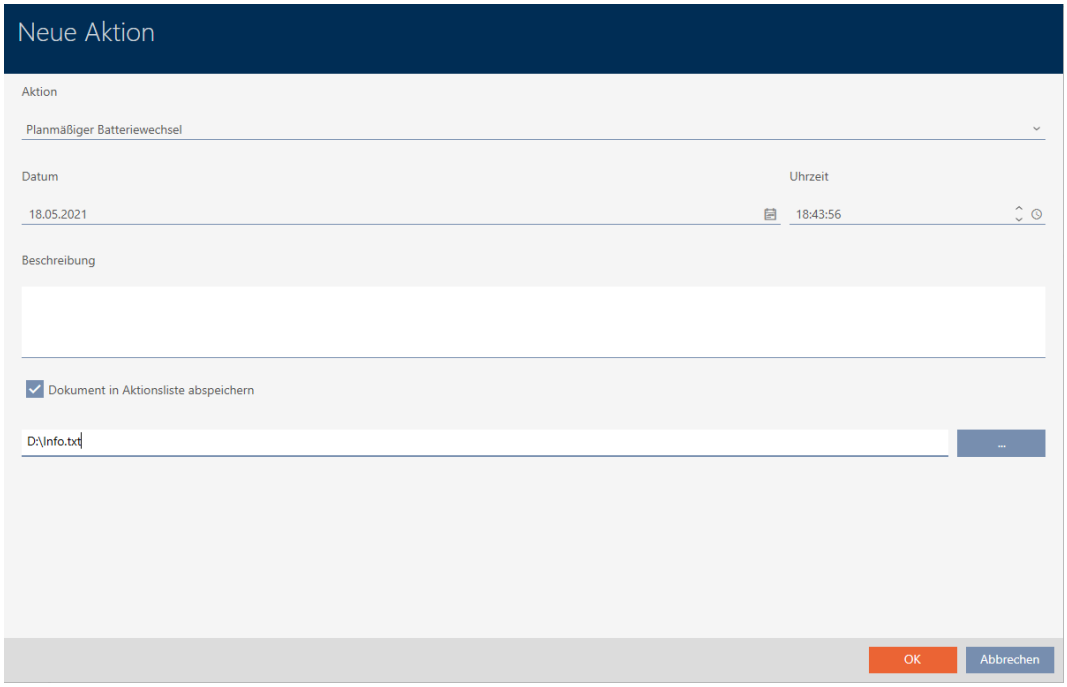
1. Click on the New + button.
   ↳ The window for a new action will open.



2. Select the "Scheduled battery change" or "Last battery change" entry from the ▼ **Action** drop-down list.
3. Enter a date in the *Date* field or click on the icon to expand a calendar screen.



4. Enter a time in the *Time* field.
5. Enter a description in the *Description* field.
6. If you wish to save a document for your action: Activate the ☑ Save document in action list checkbox.
7. If you wish to save a document for your action: Click on the ... button.
   ↳ The Explorer window will open.
8. Select your document.
9. Click on the Open button.
   ↳ Explorer window closes.



10. Click on the OK button.
    ↳ The window for the new action closes.

↳ Action is now created and listed.

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		

16.17 Exporting locking devices as a list

All locking devices in your locking system can be exported as PDFs.

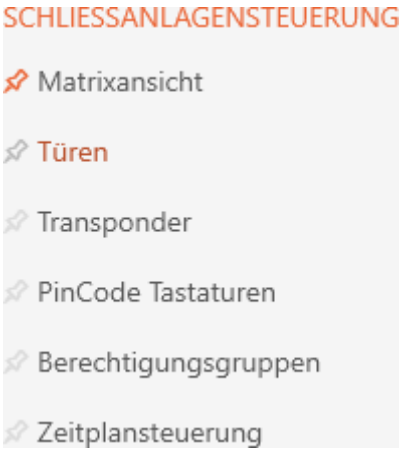
The PDF shows exactly the same locking devices in exactly the same order as in AXM Lite.

This means that you can sort and filter the display before exporting. It also allows you to sort and filter the exported list.

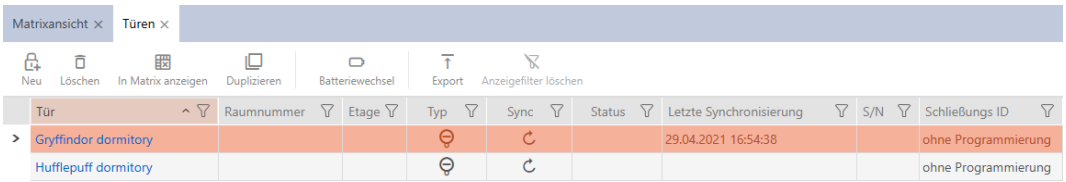
✓ AXM Lite open.
✓ Locking device has been created.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the entry Locks in the group | LOCKING SYSTEM CONTROL |.



   ↳ The list with all locking devices in the locking system will open.



3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Click on the Export ⤒ button.
   ↳ The Explorer window will open.
5. Save the PDF file to a file directory of your choice.

↳ Displayed identification media are exported as PDF files (DIN A4).

Alle Türen für die Schließanlage 'Hogwarts'

Tür	Raumnummer	Etage	Typ	Sync	Status	S/N
Gryffindor dormitory			Schließzylinder	Erstprogrammierung		
Hufflepuff dormitory			Schließzylinder	Erstprogrammierung		

17. Permissions

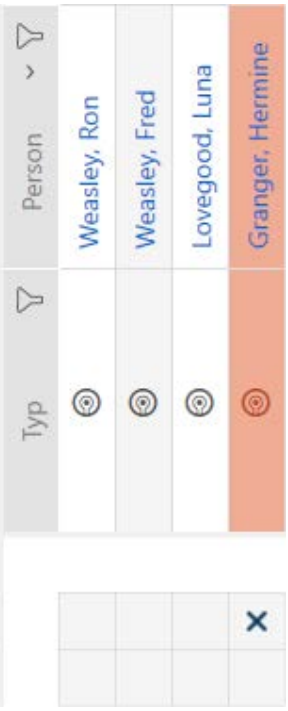
17.1 Changing individual authorisations (cross)

The quickest way to assign individual authorisations to individual doors is directly in the matrix.

✓ AXM Lite open.

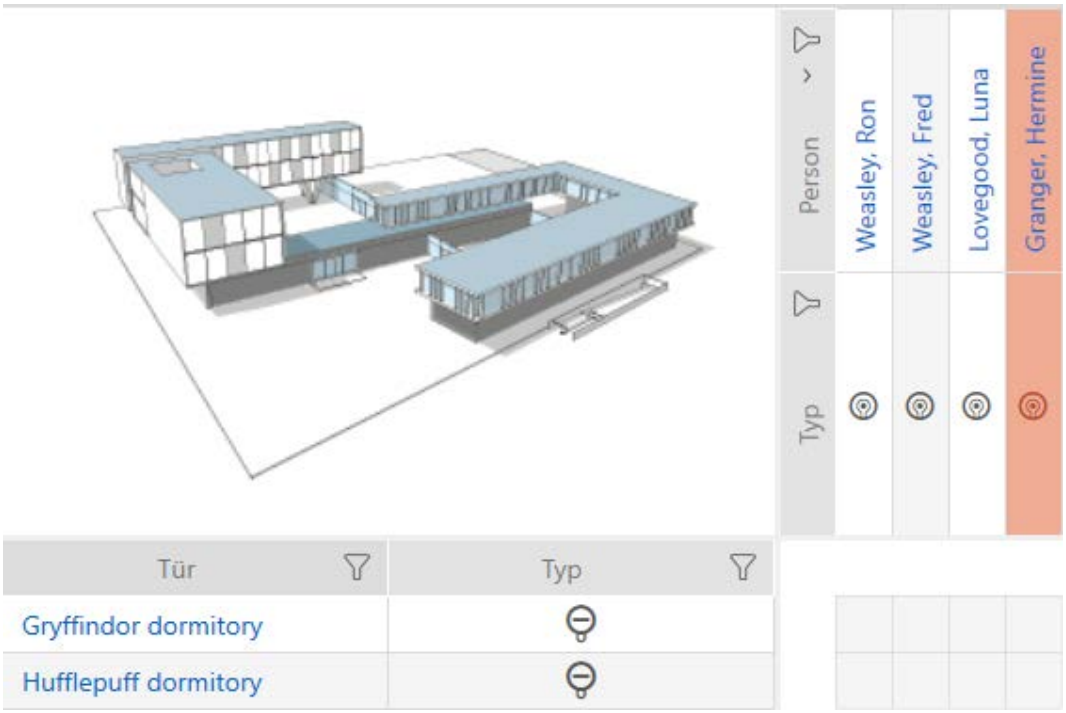
✓ Matrix screen open.

1. Click on a box in the matrix.
   ↳ Authorisation is issued for the identification medium concerned (column) on the locking device in question (row).



Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

2. Click on the same box again.
   ↳ Authorisation is withdrawn again.



↳ Individual authorisation has been issued or withdrawn.

NOTE

Modified authorisations only take effect after synchronisation

Modified authorisations are initially only stored in the database and do not affect the actual identification media and locking devices.

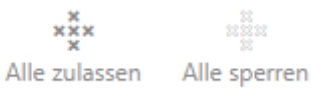
- Synchronise identification media and/or locking devices after you have changed authorisations.

The authorisation is issued by default after a single click. However, you can configure the type of click after which the authorisation is issued (see *Click to change authorisations [▸ 323]*):

- Single click of the mouse
- Double click
- Ctrl + single click

17.2 Changing many authorisations (on identification media and/or locking devices)

17.2.1 Allowing all or blocking all



Instead of individual authorisations, you can also:

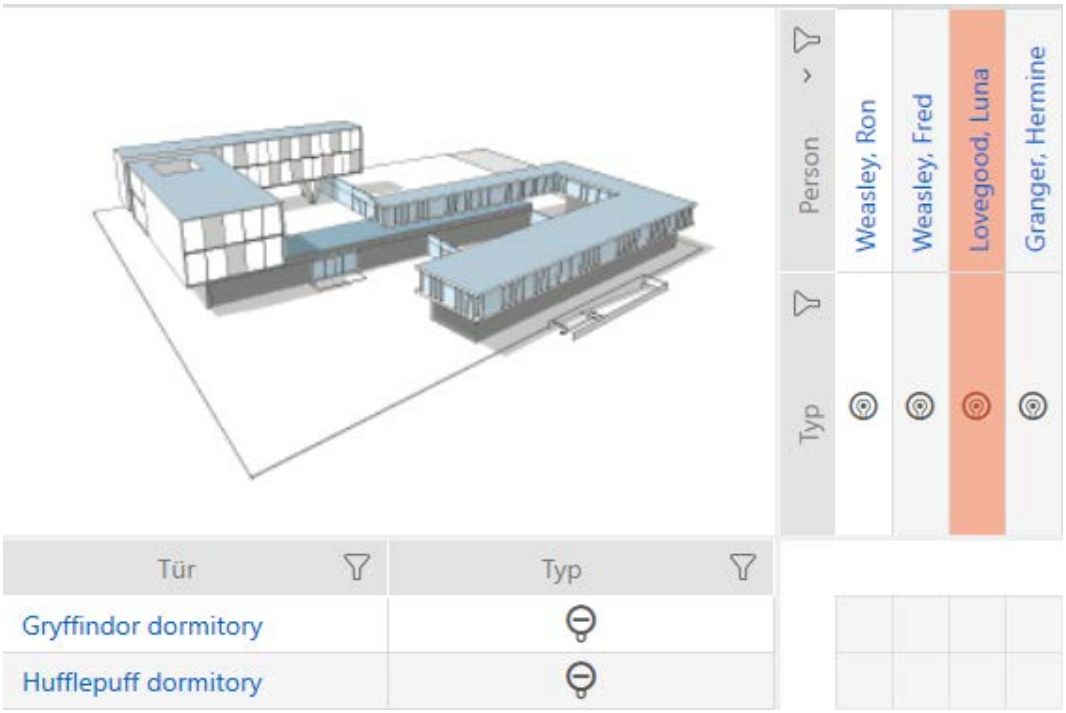
- Allow or block all currently displayed identification media on a locking device
- Allow or block identification media on all currently displayed locking devices

The Alle zulassen and Alle sperren functions are applied to the displayed identification media or locking devices. You can thus use filters to only allow specific identification media or locking devices.

This description refers to allowing all displayed identification media on a locking device. The following also work in the same way:

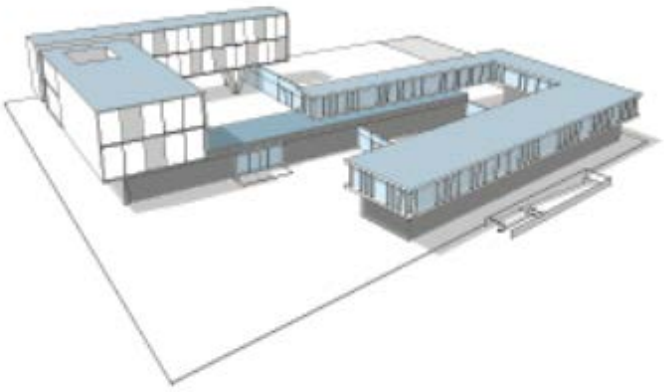
- Blocking all displayed identification media on a locking device
- Allowing identification media on all currently displayed locking devices
- Blocking an identification medium on all currently displayed locking devices

Initial situation:



- ✓ AXM Lite open.
- ✓ Matrix screen open
- ✓ Identification medium available.
- ✓ Locking device available.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).



Tür	Typ
Gryffindor dormitory	⊖
Hufflepuff dormitory	⊖

Person	Weasley, Ron	Weasley, Fred	Granger, Hermine
Typ	◎	◎	◎

2. Select the locking device on which you wish to authorise all identification media to be displayed.

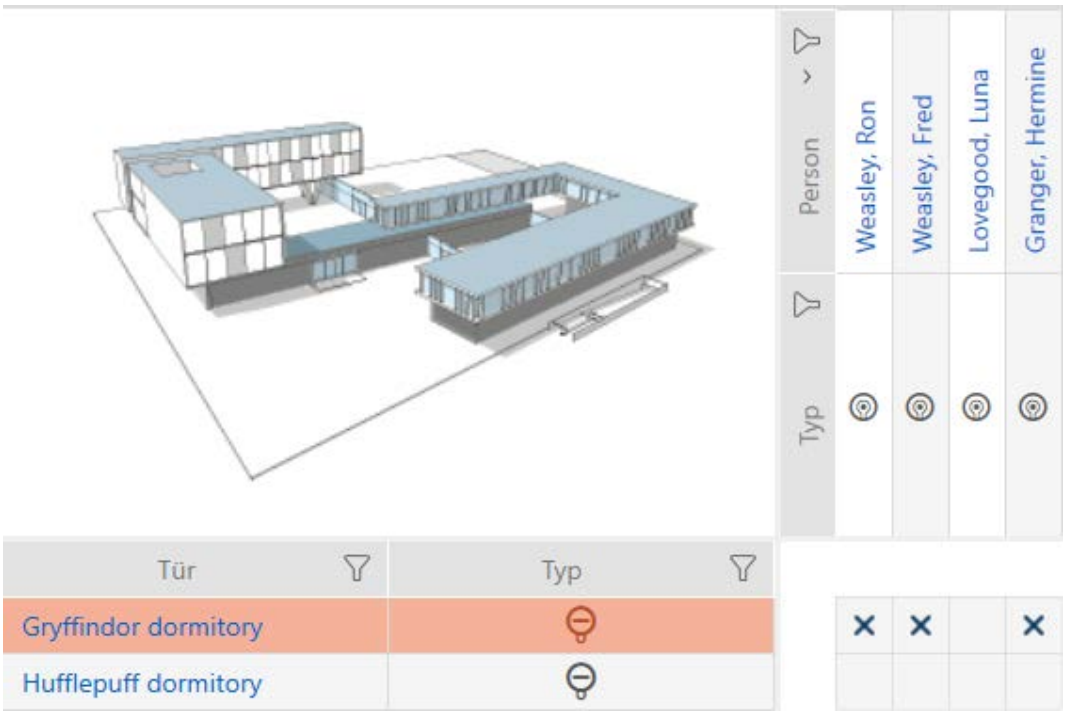
Tür	Typ	Person	Weasley, Ron	Weasley, Fred	Granger, Hermine
		Typ			
Gryffindor dormitory					
Hufflepuff dormitory					

3. Click on the Alle zulassen button.

↳ All displayed identification media are authorised for the selected locking device.

Tür	Typ	Person	Weasley, Ron	Weasley, Fred	Granger, Hermine
		Typ			
Gryffindor dormitory			✕	✕	✕
Hufflepuff dormitory					

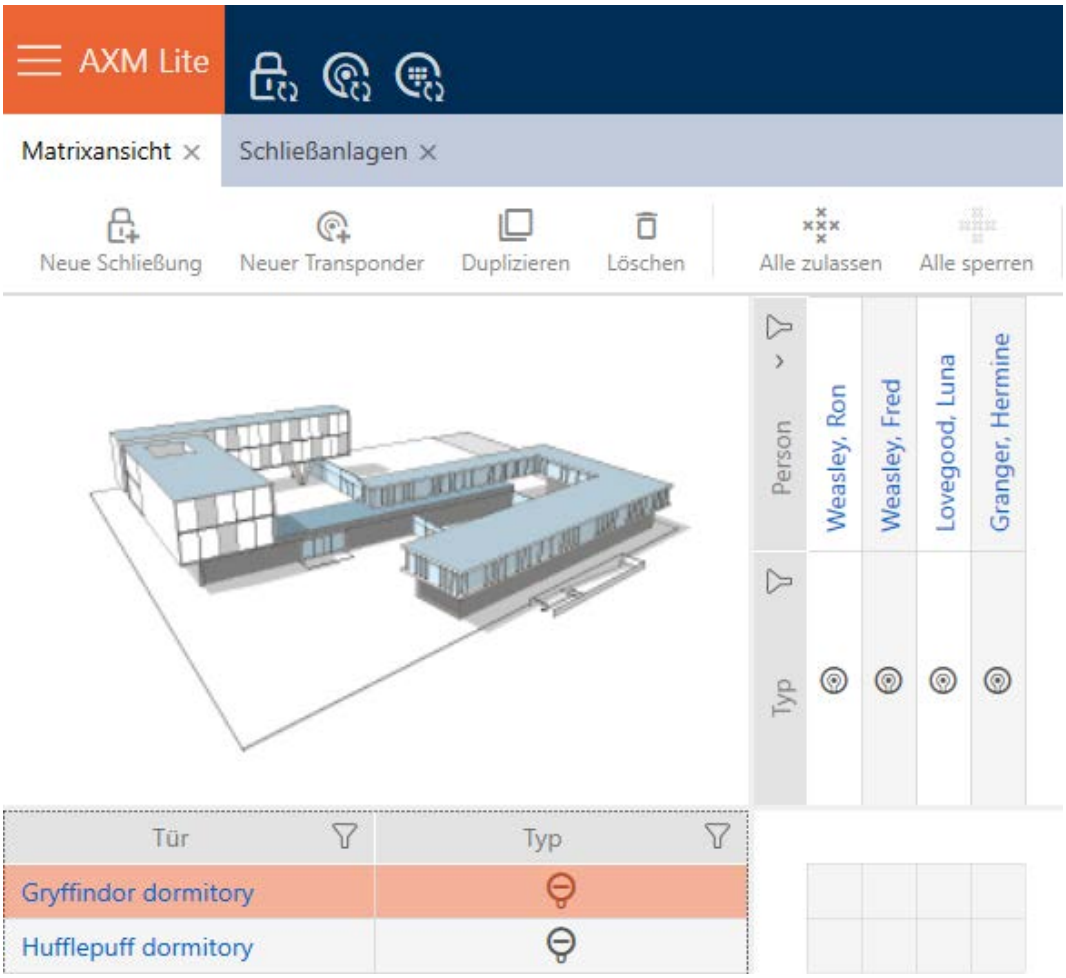
If you then use the button to remove the Anzeigefilter löschen filter again, you will find that the identification media that were filtered out were actually not permitted:



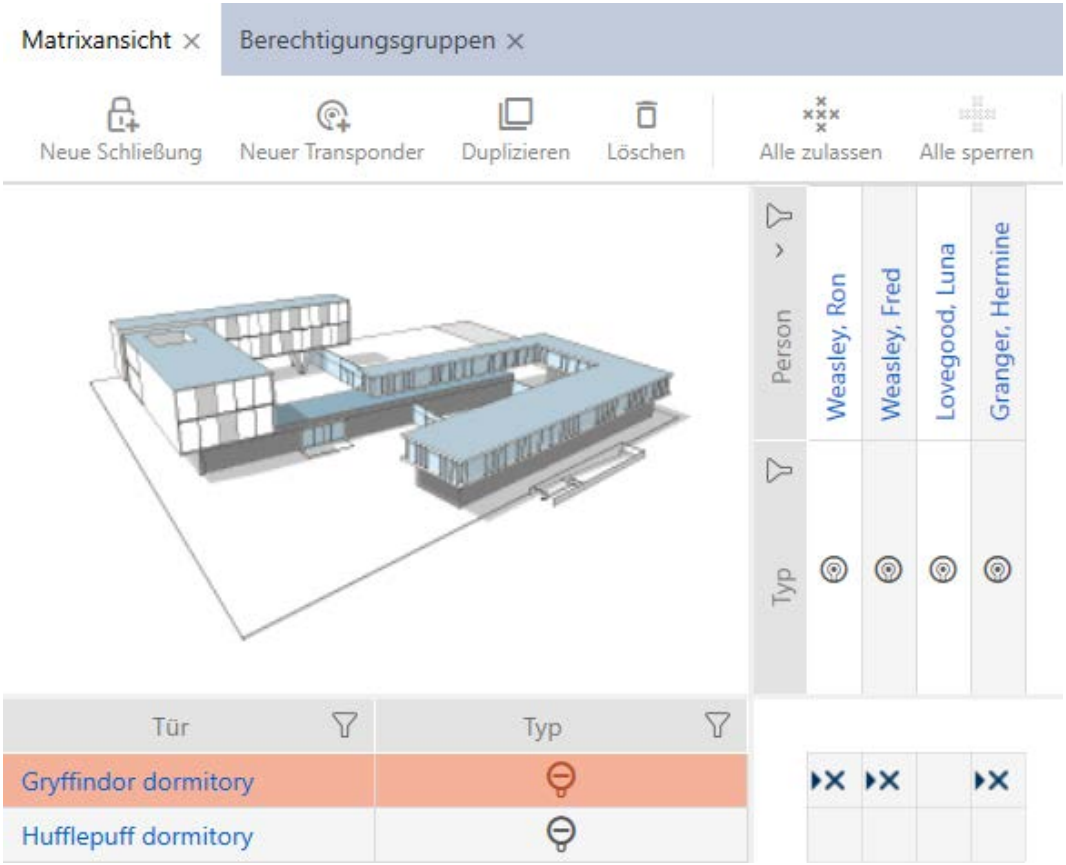
17.2.2 Access levels

Access levels are an easy way for you to set up authorisations for multiple doors and identification media at the same time (see *Access levels [▸ 378]*).

Matrix without authorisations

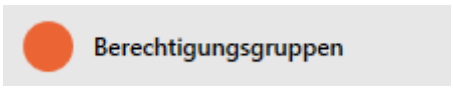


Matrix with access levels



17.2.2.1 Adding locking devices and identification media to access levels

Ideally, you will have already created your access levels before creating the locking devices (see *Best practice: setting up the locking system [▸ 29]* and *Creating access levels [▸ 44]*). This allows you to set access levels directly in locking device and identification medium properties when you create locking devices and identification media:



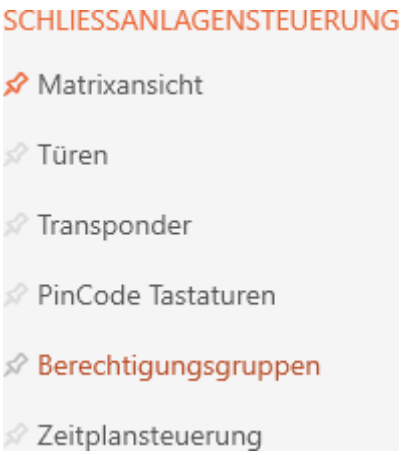
Obviously, you can also add your locking devices and identification media to the access levels at a later date:

✓ AXM Lite open.

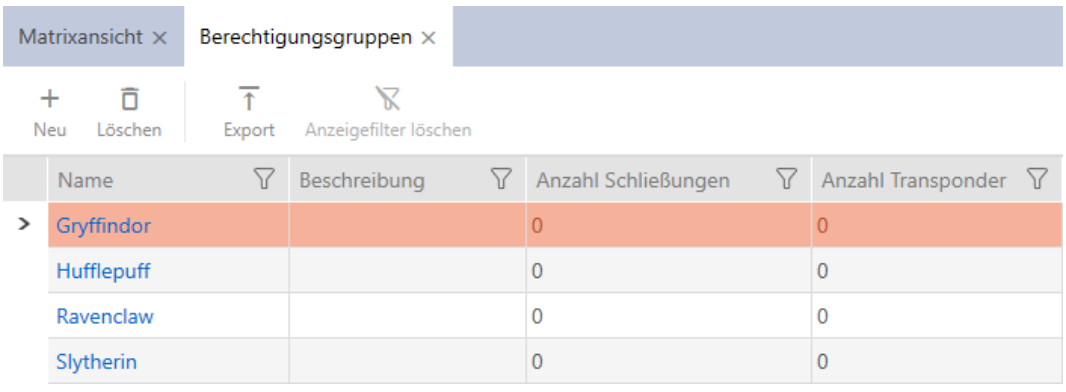
✓ Access level created (see *Creating access levels [▸ 44]*).

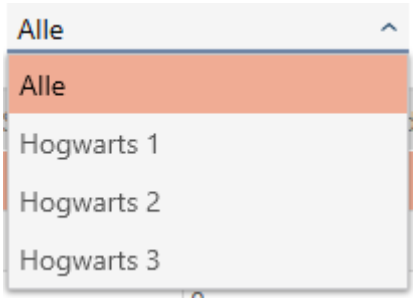
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Access levels entry in the | LOCKING SYSTEM CONTROL | group.

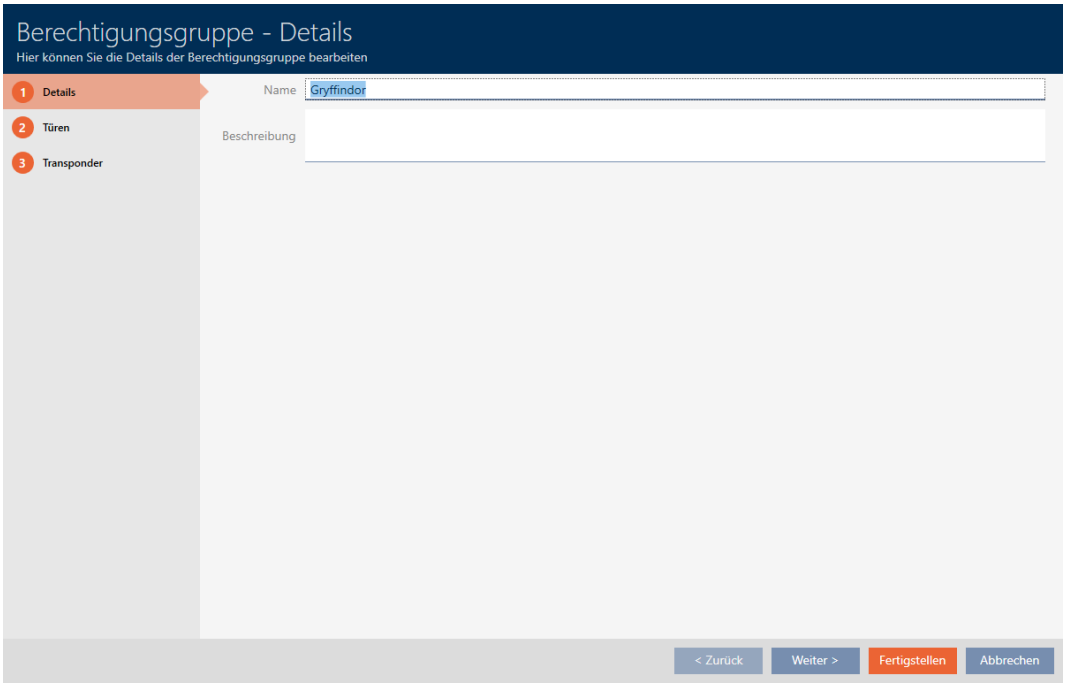


↳ The AXM bar will close.
↳ The [Access levels] tab will open.

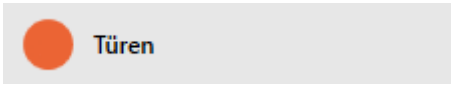




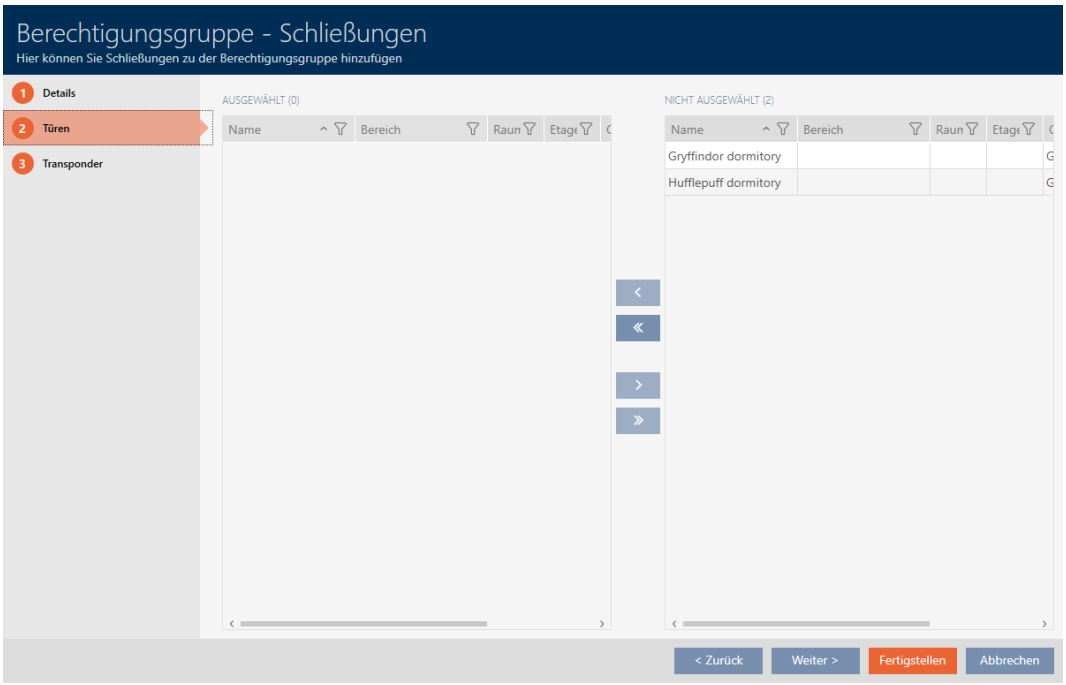
3. Click on the access level to which you wish to add locking devices and identification media.
↳ The access level window will open.



4. Click on the Locks tab.



↳ Window switches to the "Locks" tab.



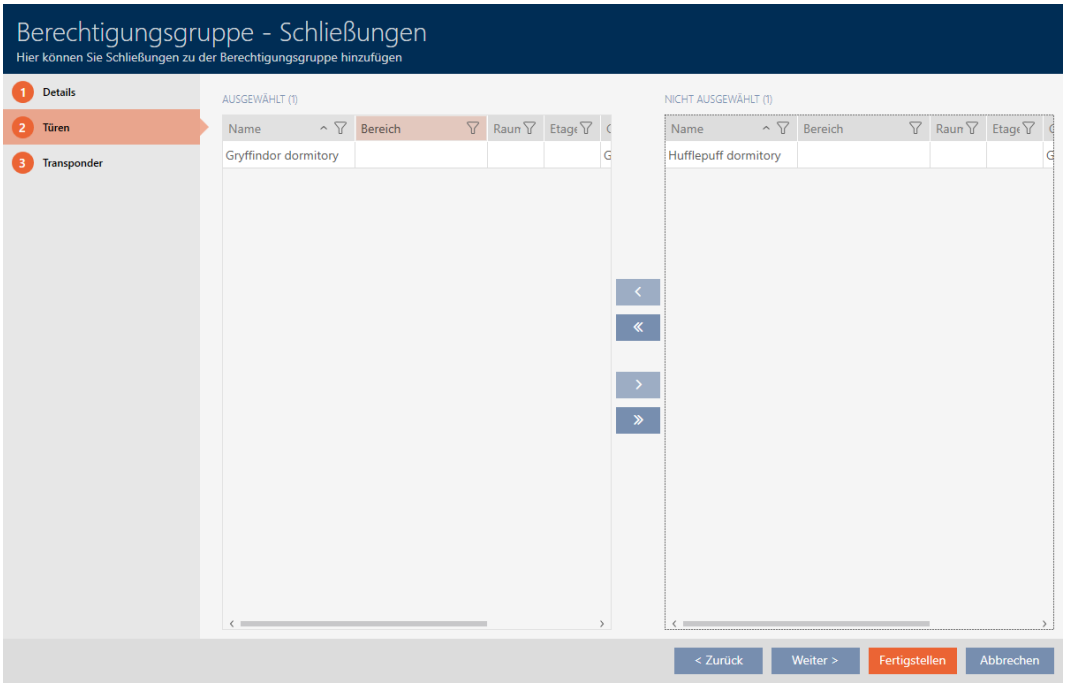
5. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
6. Select all locking devices that you wish to add to the access level (Ctrl+click for individual devices or Shift+click for multiple devices).

NOTE

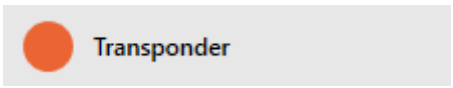
Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

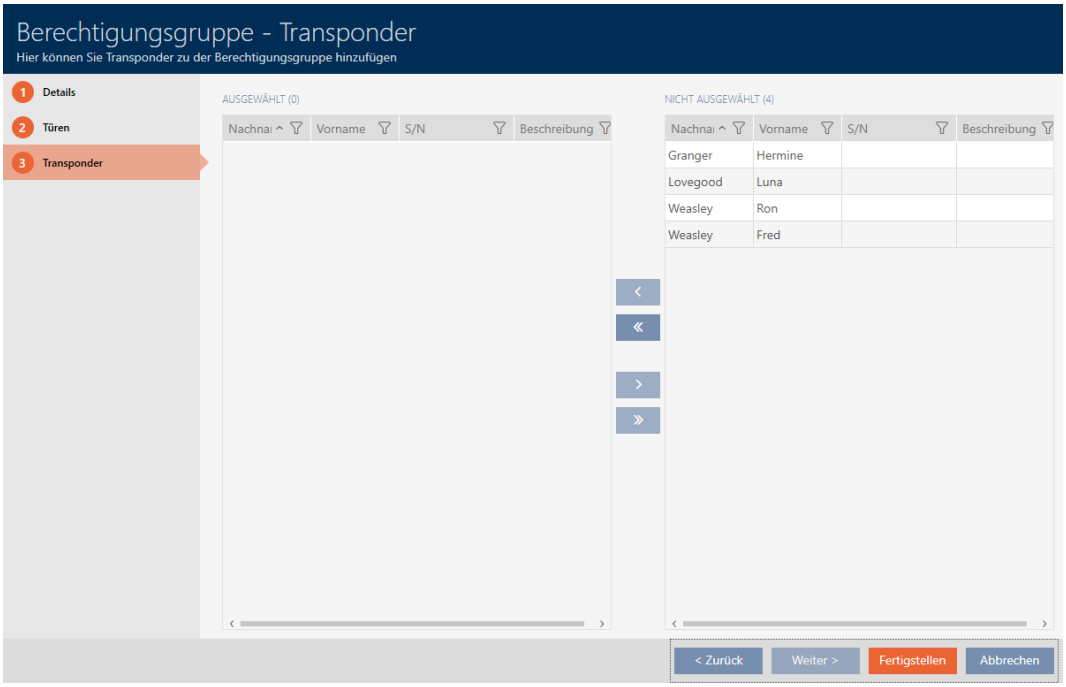
7. Use [<] to move only the selected locking devices or [<<] to move all locking devices.
   ↳ The selected locking device in the left-hand column is added to the access level.



8. Click on the Transponders tab.



   ↳ Window switches to the "Transponders" tab.



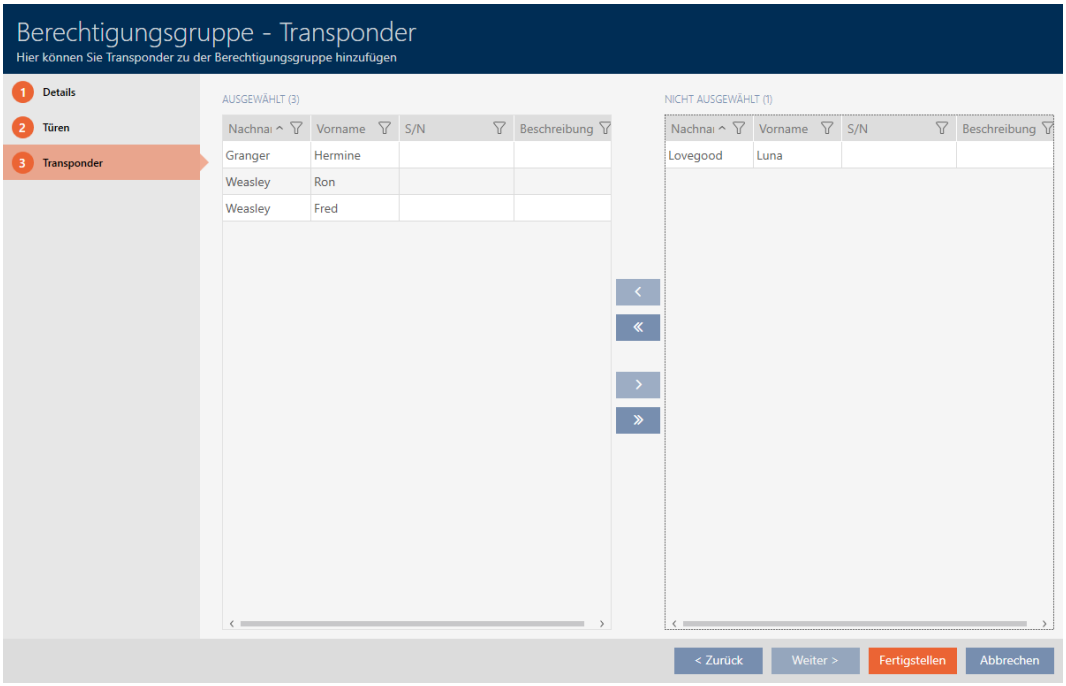
9. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
10. Select all identification media that you wish to add to the access level (Ctrl+click for individual media or Shift+click for multiple media).

NOTE

Double-clicking as an alternative to arrow keys

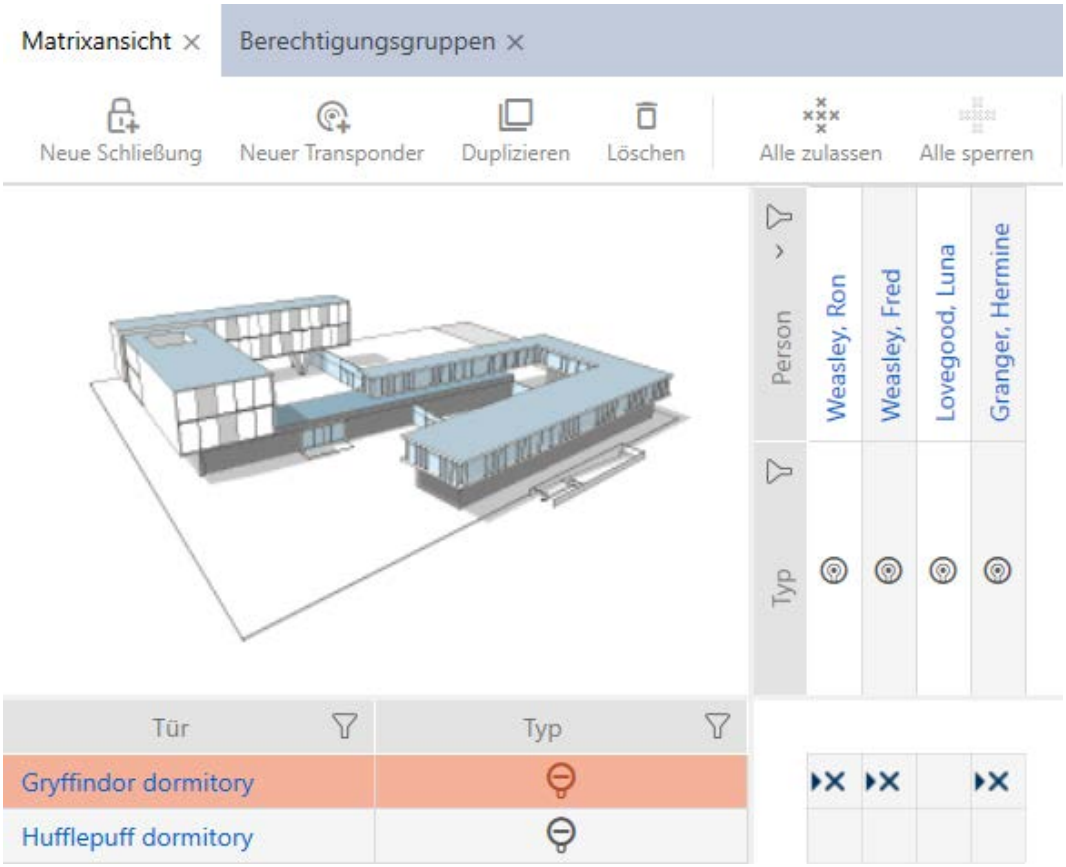
Double-clicking an entry in the list will also move this entry to the other column.

11. Use [<] to move only the selected identification media or [<<] to move all locking devices displayed.
    ↳ The selected identification media in the left-hand column are added to the access level.



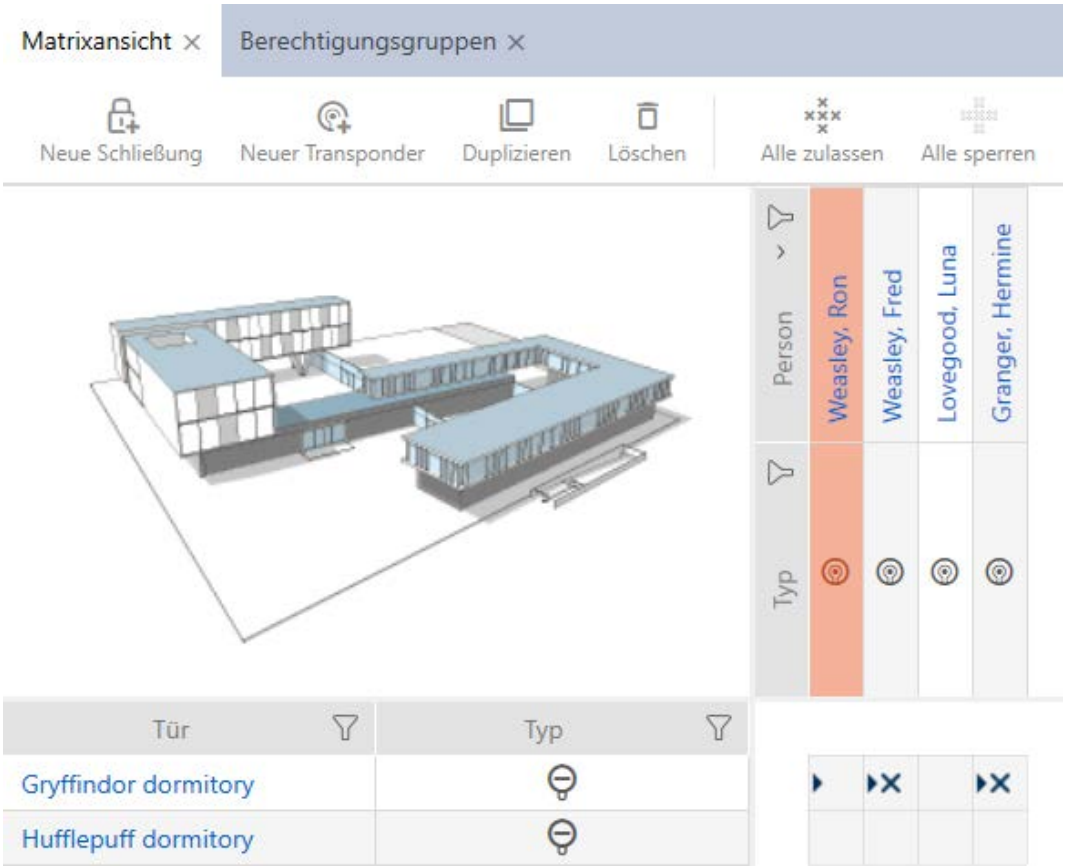
12. Click on the Finish button.
    ↳ The access level window closes.
    ↳ All identification media in this access level are authorised for all locking devices in this access level.
    ↳ Matrix view is visible again.
13. Click on the Refresh button.

↳ Matrix displays authorisations from your access level (identified by a small triangle next to the cross).



You can also overwrite individual authorisations from access levels manually. For example, it is possible to remove authorisation from an identification medium that would actually be authorised for a locking device.

Proceed as with the normal assignment of individual authorisations (see *Changing individual authorisations (cross) [▸ 256]*). In this case, it is only the cross that disappears, not the triangle:



The triangle continues to indicate that there is actually an authorisation from an access level here.

17.2.2.2 Exporting access levels as a list

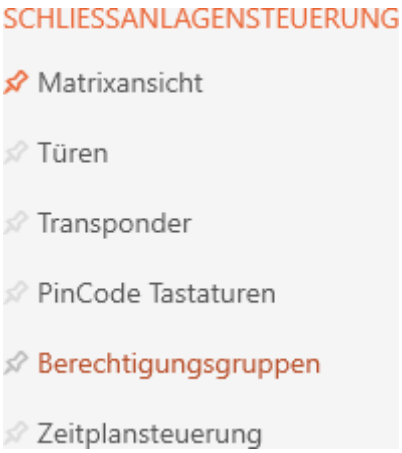
All access levels in your locking system can be exported as a PDF.

The PDF shows exactly the same access levels in exactly the same order as in AXM Lite.

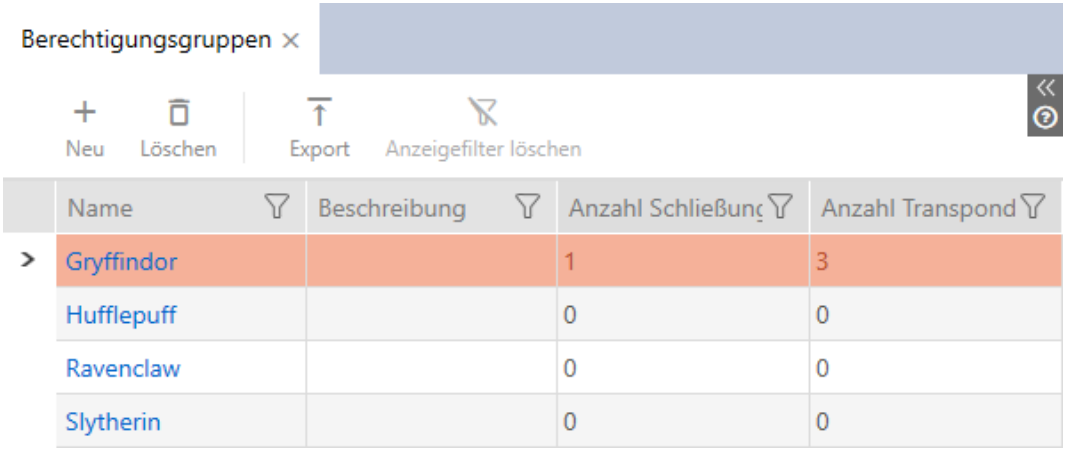
This means that you can sort and filter the display before exporting. It also allows you to sort and filter the exported list.

✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

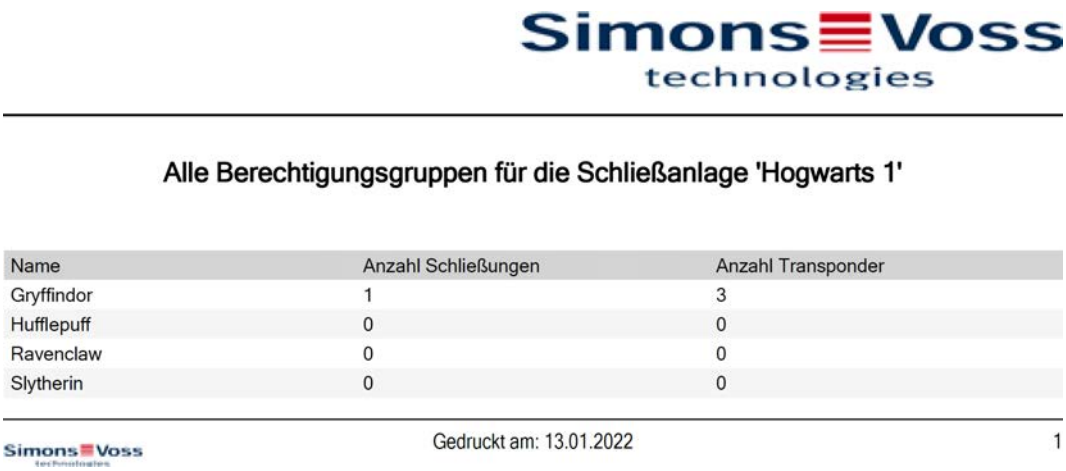


↳ The AXM bar will close.



2. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
3. Click on the Export ⤒ button.
   ↳ The Explorer window will open.
   ↳ Explorer window closes.

↳ The identification media displayed are exported as a PDF file (DIN A4).



17.2.3 Controlling authorisations in terms of time (schedules)

Time management in AXM Lite comprises:

- Time schedules for locking devices
- Time groups for transponders

You can find a detailed description and an example here: *Event management [▸ 366]*.

You can only create time groups using a schedule in AXM Lite. The first step after creating a concept is therefore a schedule:*Creating a schedule [▸ 45]*.

Schedules and time groups in multiple locking systems

Schedules and time groups created in a locking system can be configured throughout the project. You will also find them available for selection in other locking systems, provided that this locking system is in the same project. Changes to schedules and time groups therefore also apply equally to all locking systems within a project.

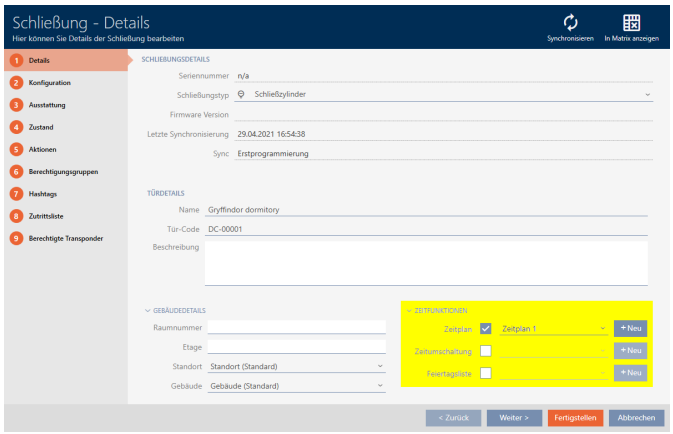
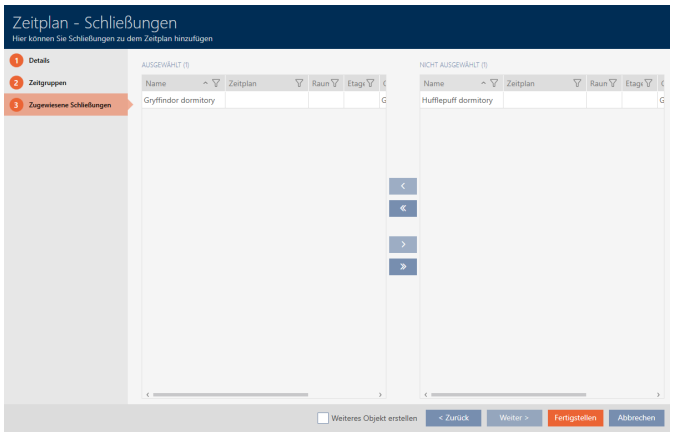
This does not affect locking systems in other projects. You cannot see or configure schedules and time groups from other projects.

17.2.3.1 Adding locking devices to the schedule

Ideally, you should create your schedules before the locking devices (see *Best practice: setting up the locking system [▸ 29]*). You can then add your locking devices to the schedule while you are creating each locking device (see *Creating a locking device [▸ 182]*).

Sometimes, however, you have already created locking devices and only later decide to control authorisations in terms of time, for example. In this case, you simply add the locking devices to your schedules at a later date.

There are two ways to do this:

Locking device window	Schedule window
	
■ Can be used directly when creating the locking device ■ Only one locking device possible per access point	■ Can be used directly when creating the schedule ■ Multiple locking operations possible per access point

In this section, you will learn how to add locking devices to a schedule in the time schedule window (see *Limiting authorisations for locking devices to specific times (schedule) [▸ 220]* for adding using the locking device properties).

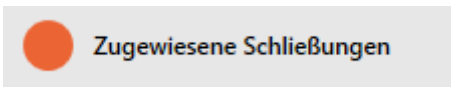
✓ AXM Lite open.

✓ Schedule created (see *Creating a schedule [▸ 45]*).

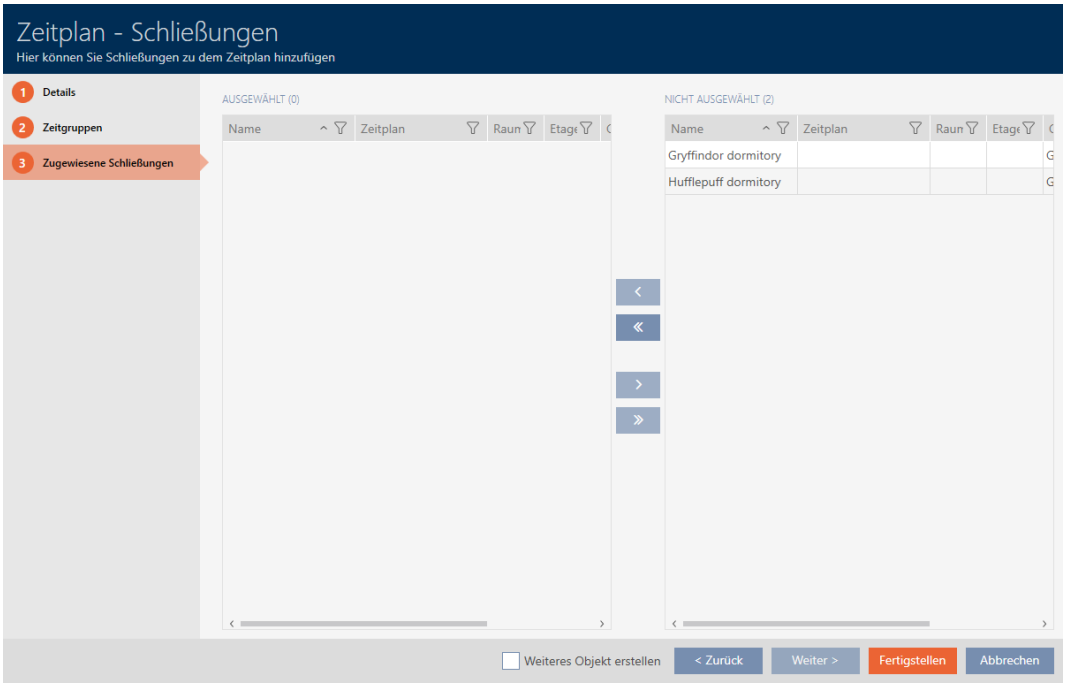
✓ Schedule window open (see *Creating a schedule [▸ 45]*).

✓ Locking device equipped with .ZK option.

1. Click on the Assigned locks tab.



↳ The schedule window changes to the "Assigned locks" tab.



2. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
3. Select all locking devices that you wish to assign (Ctrl+click for individual devices or Shift+click for multiple devices).

NOTE

Double-clicking as an alternative to arrow keys

Double-clicking an entry in the list will also move this entry to the other column.

4. Use [<] to move only the selected locking devices or [<<] to move all locking devices.

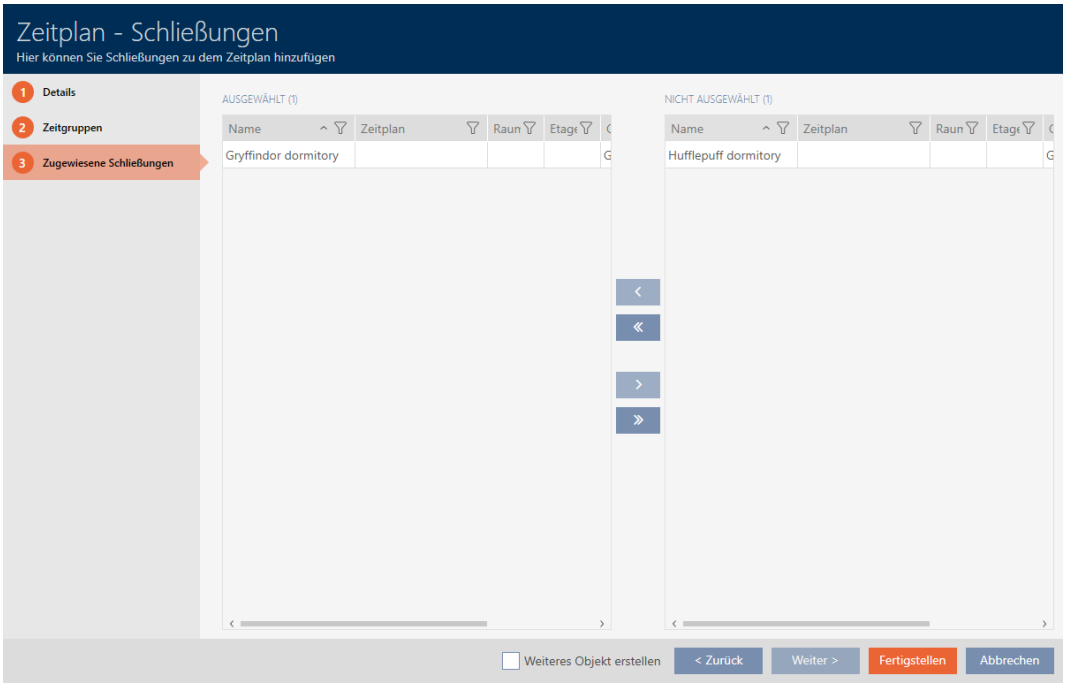
NOTE

Locking devices from other schedules

Locking devices from other schedules are also listed. They can also be moved from other schedules to the current schedule.

1. Filter/sort the displayed locking devices.
2. Check whether the selected locking devices are already being used in another schedule.

↳ The locking devices in the left-hand column are added to the schedule.



5. Click on the Finish button.
   ↳ Schedule window closes.

↳ Locking devices are now added to the schedule.

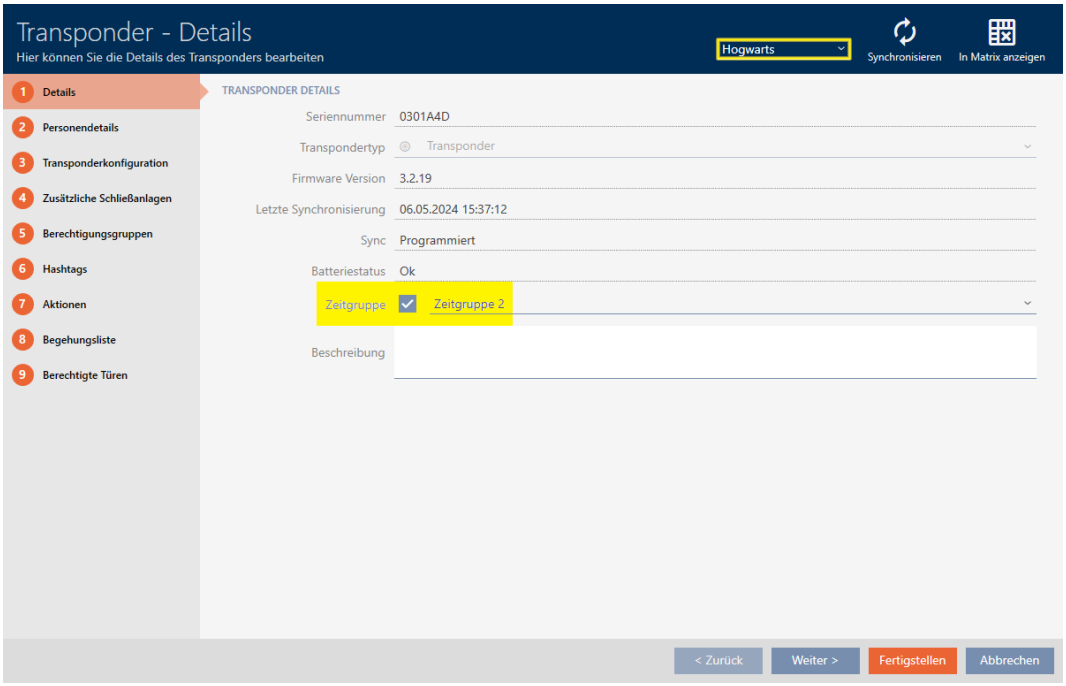
17.2.3.2 Adding identification medium to time group

Ideally, you should create your time groups before the locking devices (see *Best practice: setting up the locking system [▸ 29]*). You can then add your identification media to the time groups when you create them (see *Creating an identification medium [▸ 77]*).

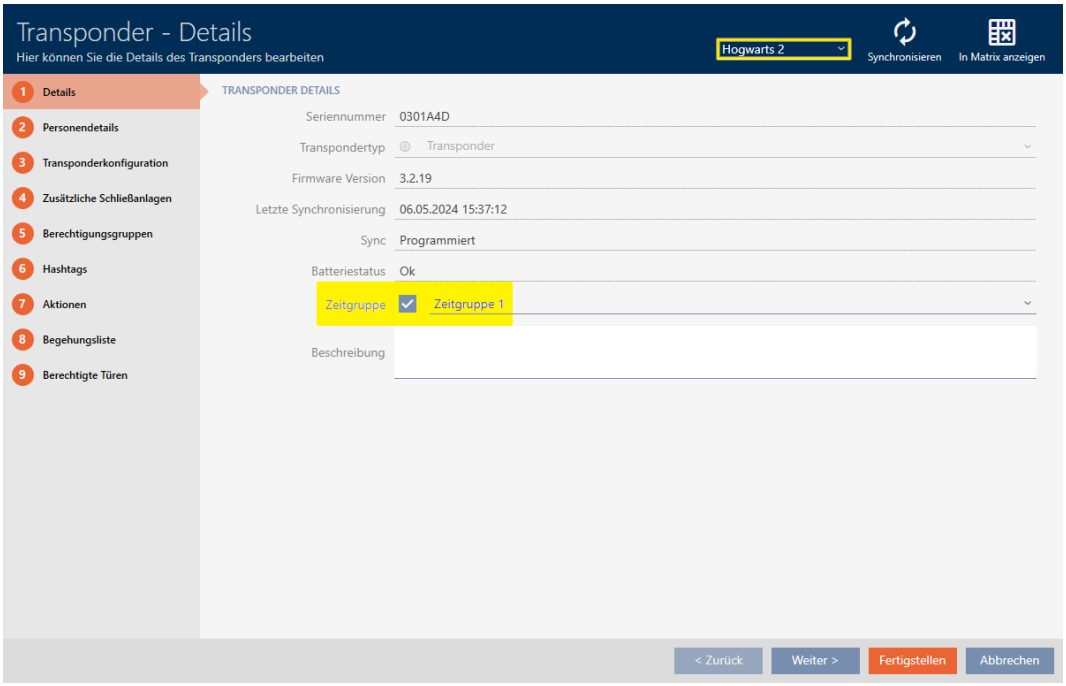
An identification medium can only be added to a time group in its properties.

Time groups with multiple locking systems

You can use identification media in multiple locking systems (see Reuse identification medium in the same project and Reusing identification medium in other projects/databases). The same identification medium may have a different time group in each locking system. You can therefore select the locking system in the identification medium details in the top right-hand corner and select the properties for this locking system.

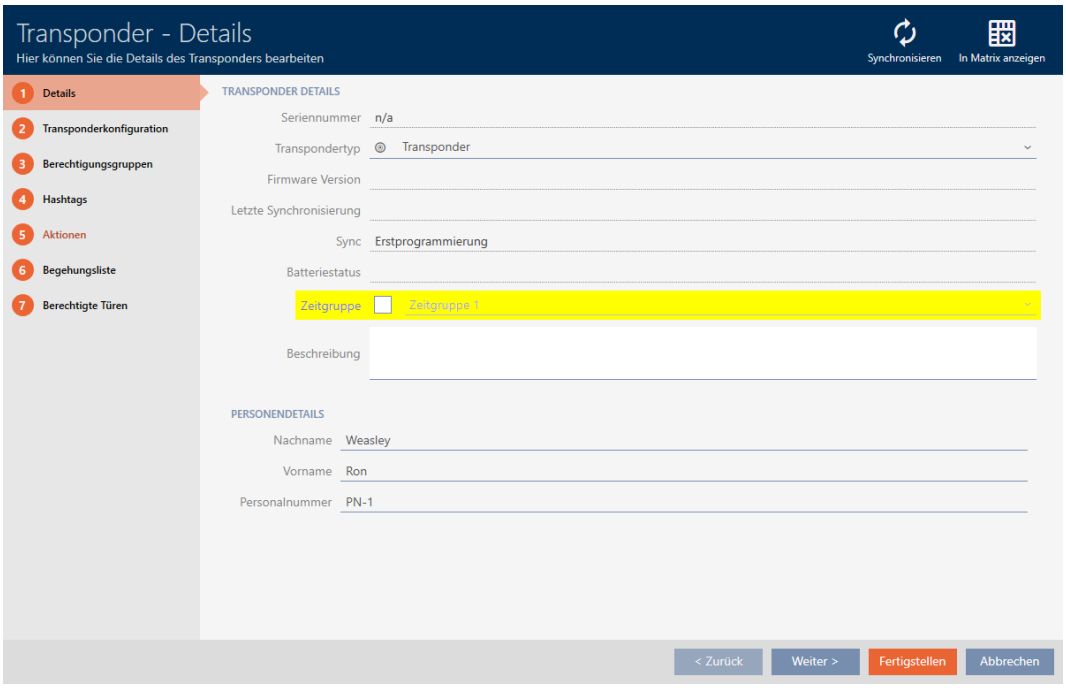


If you change the locking system in the drop-down menu, you can select a different time group for the identification medium in this different locking system.



PIN code keypads can only be used for one locking system. For this reason, you can select just one time group per PIN for PIN code keypads.

Add card/transponder to time group

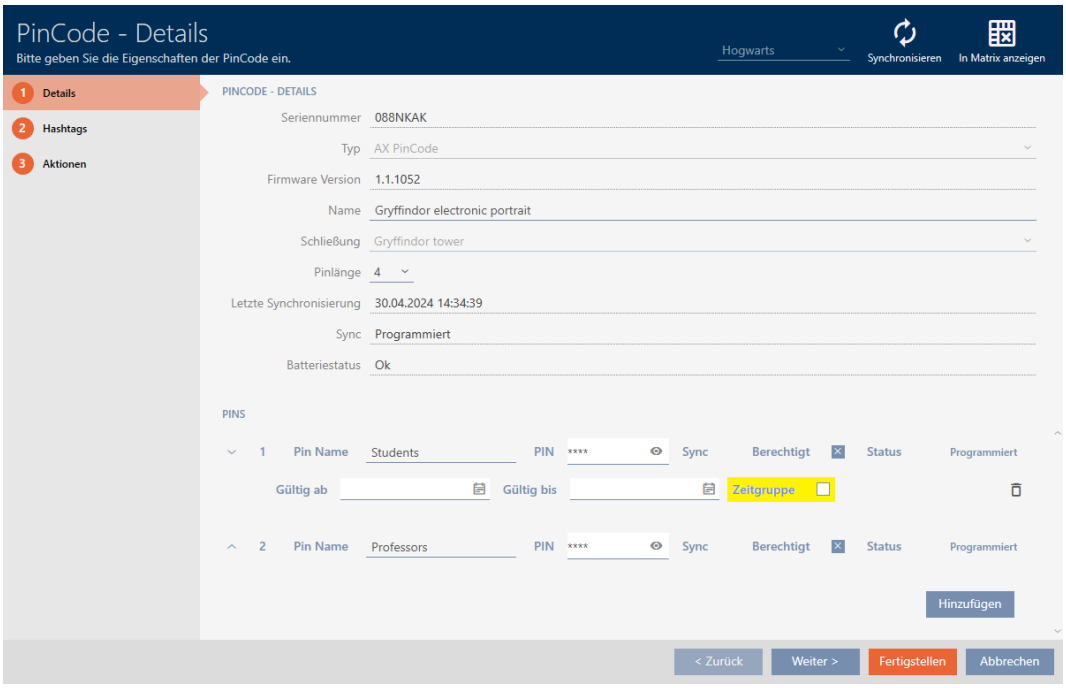


✓ AXM Lite open.

1. Click on the identification medium to be added to a time group.
   ↳ The identification medium window will open.
2. Select the ☑ Time group checkbox.
3. Select the time group from the ▼ **Time group** drop-down list (e.g. "Time group").
4. Click on the Finish button.
   ↳ The identification medium window closes.

↳ Identification medium has been added to the time group.

Adding PINs from a PIN code keypad to the time group



✓ AXM Lite open.

✓ PIN code keypad created with PINs (see *Creating PIN code keypads [▸ 83]*).

✓ Time groups created (see *Create time group [▸ 49]*).

1. Click on the PIN to be added to a time group.
   ↳ The window will open for the associated PIN code keypad.
2. Expand the PIN settings with the ⌄ button.
3. Select the ☑ Time group checkbox.
   ↳ A drop-down menu will appear.

4. Select the time group that you require.

5. Click on the Finish button.
   ↳ The window for the PIN code keypad closes.

↳ PIN has been added to the time group.

17.3 Meaning of the authorisation crosses in the matrix

Cross	Meaning
	Not authorised.
	Authorised in the database but not programmed yet.
	Authorised and programmed.
	Authorisation withdrawn, but authorisation removal not programmed yet.
	Authorised by an access level in the database, but not programmed yet.
	Authorised and programmed by an access level.
	Authorisation available and programmed by an access level; this authorisation has been removed manually. Authorisation removal not programmed yet.
	Authorisation by an access level available, but this authorisation was removed manually before programming.
	Authorised and programmed, but identification medium has been blocked (e.g. after theft).
	Not authorised; identification medium has been blocked (e.g. after theft). or: not possible, e.g. PIN code keypad has been assigned to another locking device.

18. Locking systems

18.1 Changing locking system password

IMPORTANT

Keep locking system password accessible and secure

The locking system password is the most important password of all. For security reasons, SimonsVoss is not able to reset any components without a locking system password or backup. There is no general master key.

It is no longer possible to program components if the locking system password is no longer known or can no longer be recovered from a backup. The components must be removed from locks and disposed of, which takes a great deal of effort.

1. Ensure that authorised persons can be view and/or access the locking system password at any time.
2. Take into account both foreseeable events (e.g. locking system administrator retires) and unforeseeable events (e.g. locking system administrator leaves post).

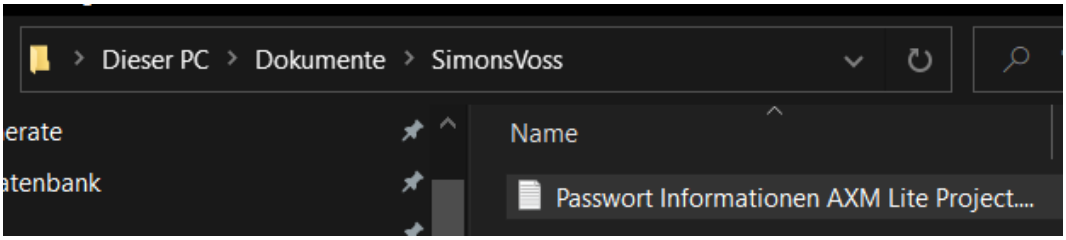
NOTE

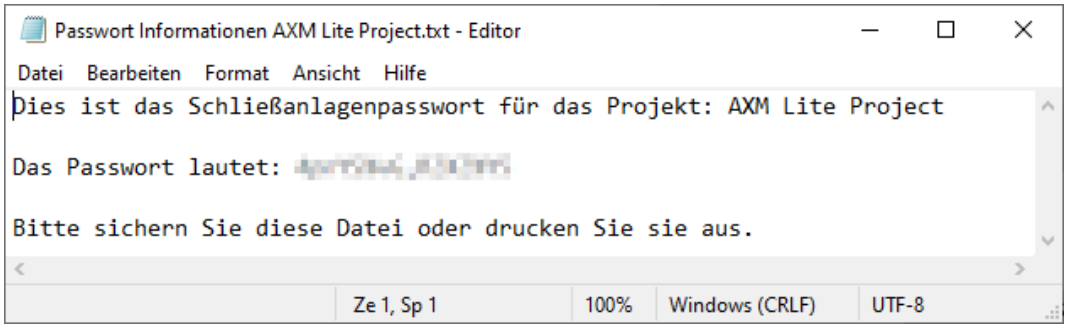
Programming required after changed locking system password

All data exchanged between locking devices and identification media is encrypted. The locking system password is required for this encryption. This means that a change in locking system password needs to be communicated to all locking devices and all identification media.

Changing the locking system password causes the greatest programming requirement of all possible changes in your database.

The locking system password generated when the project was created is saved in a text file (`Documents/SimonsVoss`).



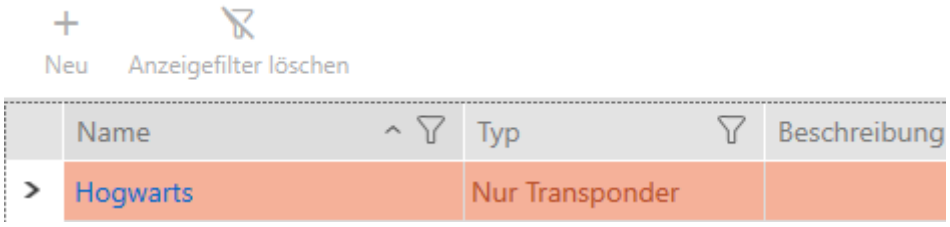


✓ Old locking system password is known.

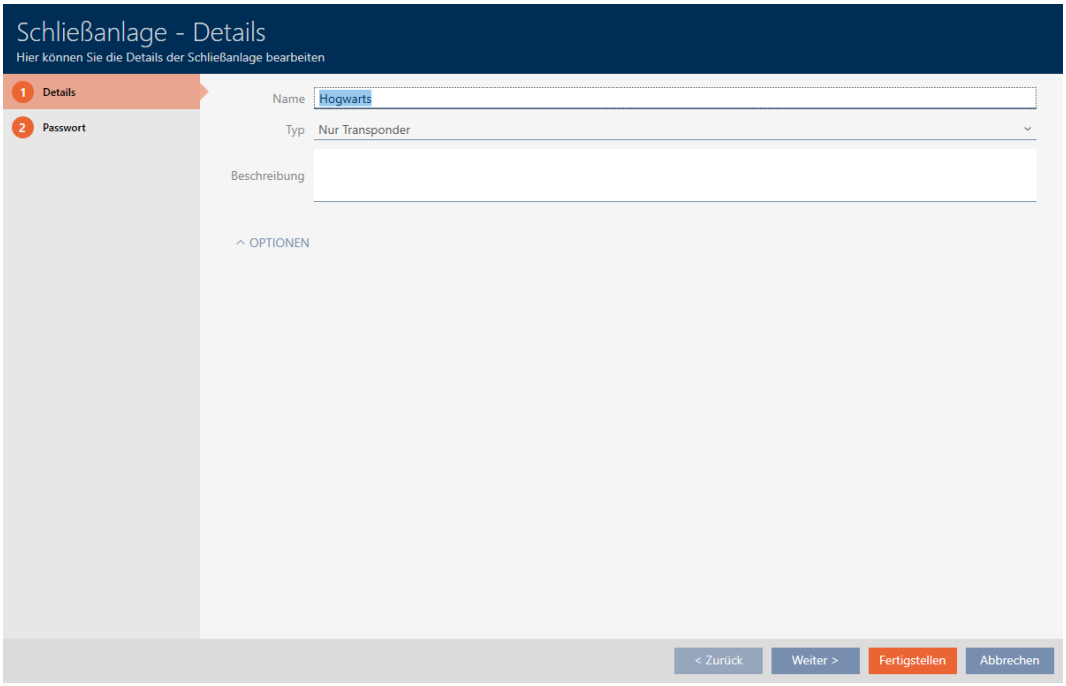
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

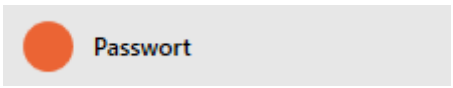
↳ The [Locking systems] tab with a list of all locking systems in the database will open.



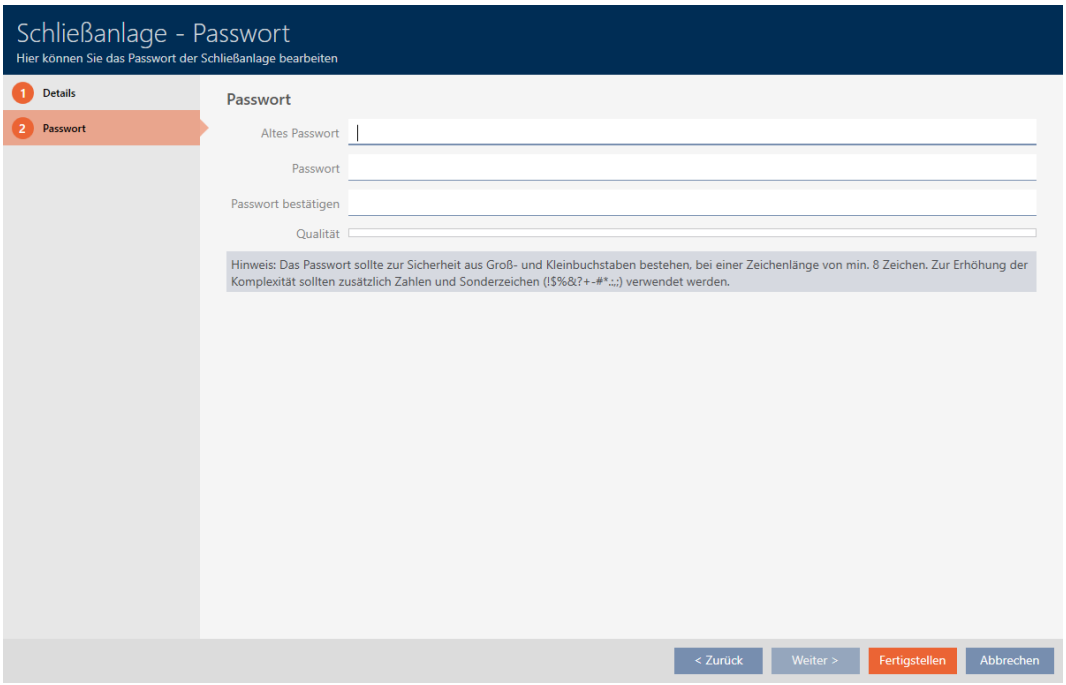
2. Click on the locking system whose password you wish to change.
   ↳ The locking system window will open.



3. Click on the Password tab.

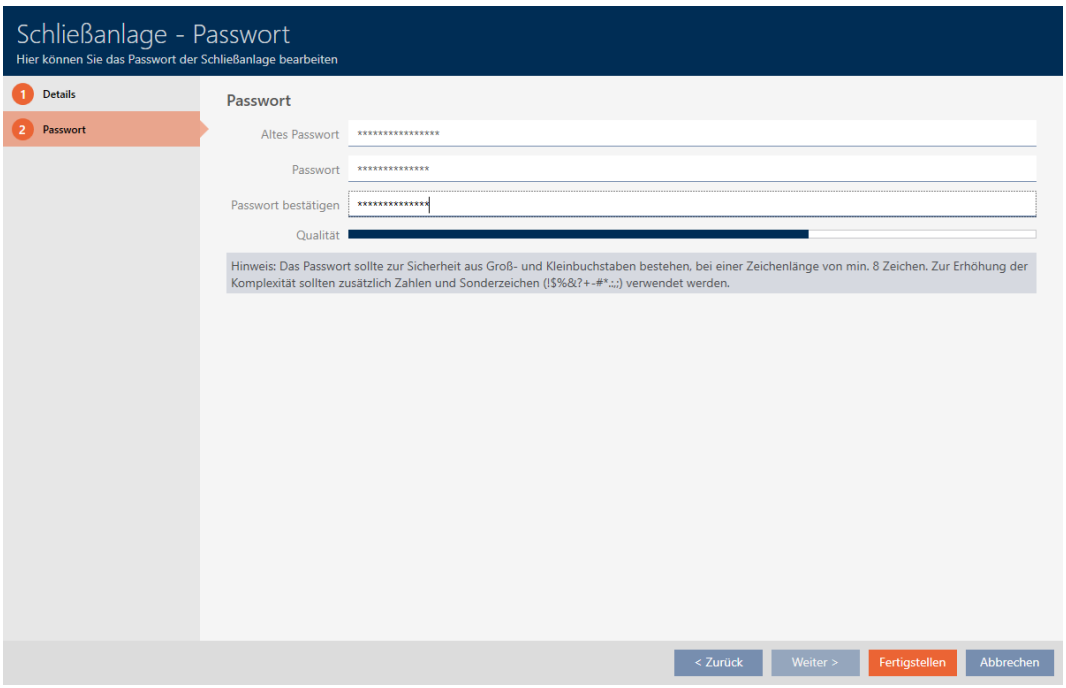


↳ Window switches to the "Password" tab.

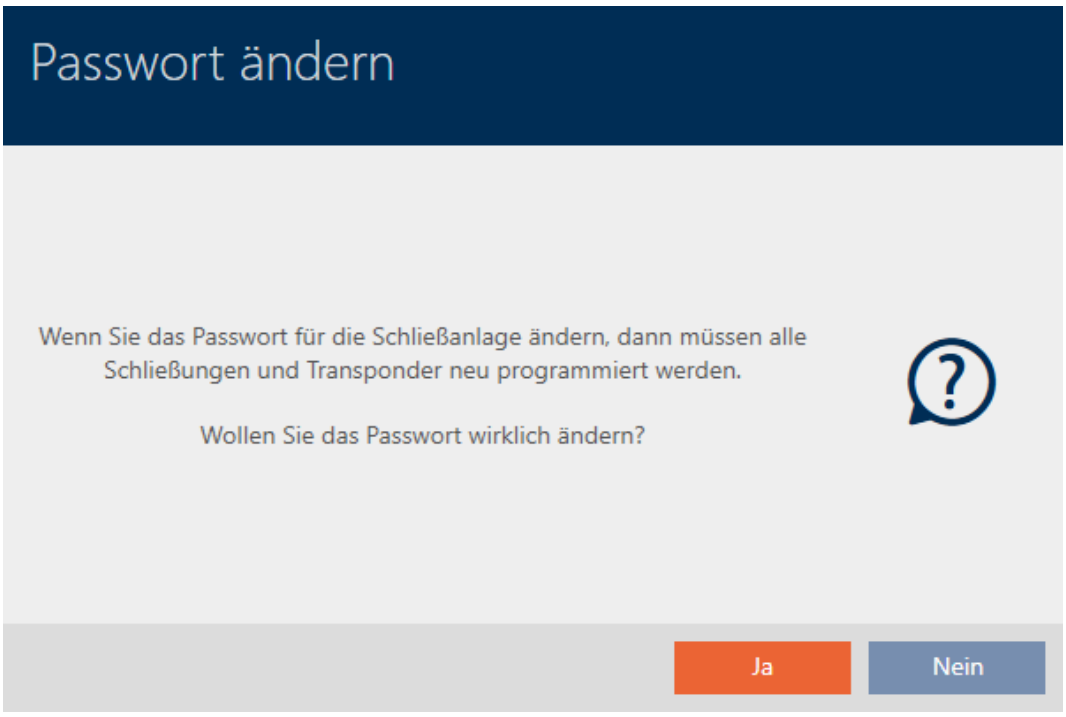


4. Enter the old locking system password in the *Old password* field.
5. Enter a new locking system password with at least 8 characters in the *Password* field.
   ↳ A coloured bar shows you how secure your password is.

6. Confirm the new locking system password in the *Confirm password* field.

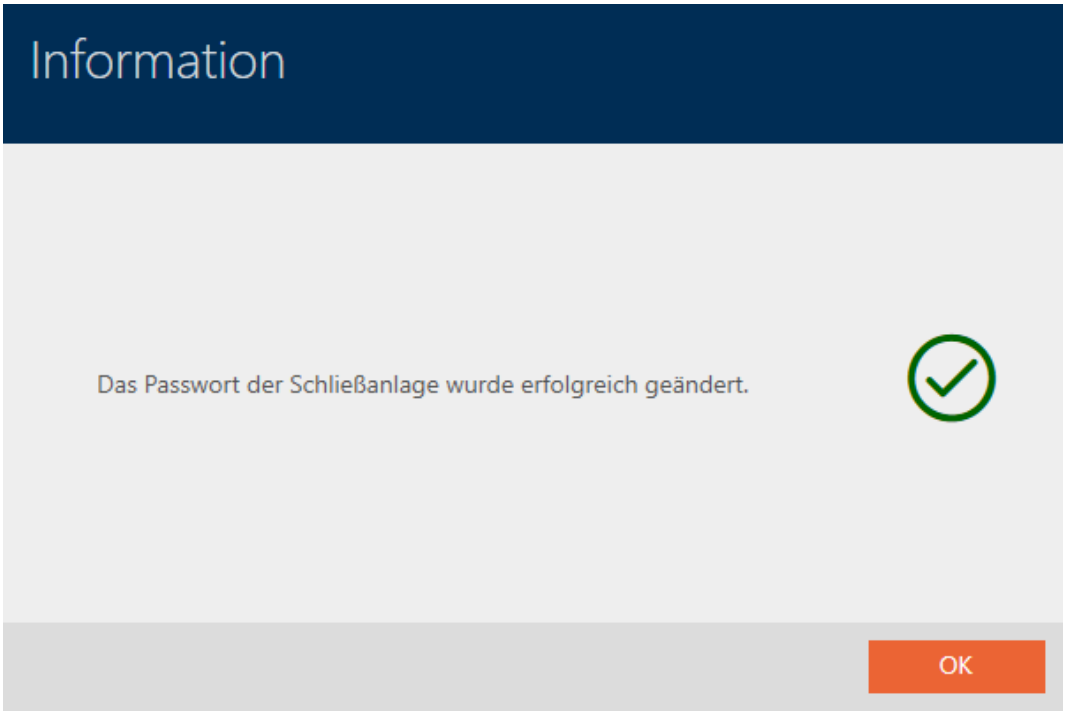


7. Click on the Finish button.
   ↳ Warning message appears about the expected scope of programming required.



8. Click on the Yes button.
   ↳ Warning message closes.

↳ Locking system password has been changed.



IMPORTANT

Documenting the changed locking system password

When a project is created, a locking system password is generated and saved in a text file. This text file is not updated if you change the locking system password.

- Enter the locking system password in the text file yourself or make sure that the new locking system password is documented in another way.

18.2 Using a common locking level

With a common locking level, you can use a transponder in multiple locking systems in the same project (e.g. for fire service transponders). See Detail function for the overarching locking levels for further information on common locking levels.

Setting up a common locking level consists of several parts:

1. Create a common locking level and assign it to this locking system (see *Creating a common locking level [▸ 285]*).

2. Create a transponder in one of the assigned locking systems (see *Creating transponders for common locking level [▸ 287]*).
   ↳ Transponders are automatically created in all locking systems that have been assigned to the common locking level.
3. Authorise the transponder in the assigned locking systems (see *Authorising a transponder with common locking level [▸ 288]*).

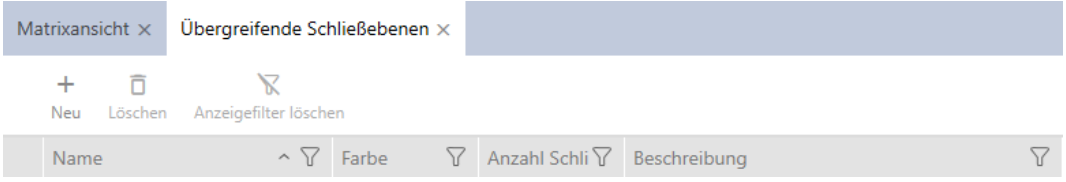
18.2.1 Creating a common locking level

✓ AXM Lite open.

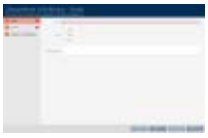
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Service Sets entry in the | SETTINGS | group.

   ↳ The [Service Sets] tab will open.



3. Click on the New button ✚.
   ↳ The "Master locking level" window will open.



4. Enter the name of your common locking level in the *Name* field.
5. Select the colour of your common locking level (Green, Blue or Red).
6. Enter a description if required.
7. Click the Next button.
   ↳ Window switches to the "Password" tab.

8. Enter the password for your common locking level in the field.
9. Re-enter the password in the *Confirm password* field.
   ↳ A coloured bar shows you how secure your password is.

10. Click the Next button.
    ↳ Window switches to the "Assigned Locking Systems" tab.
11. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
12. Select the required locking systems in the right-hand column (Ctrl+click for single systems or Shift+click for multiple systems).
13. Use to move only the selected locking systems or to move all displayed locking systems.
    ↳ The identification medium will be available later in the assigned locking systems.

14. Click the Finish button.
    ↳ Explorer window for saving the password as a PDF will open.

15. Save the PDF with the password in a location of your choice and keep the password in a safe place.
    ↳ Password is now saved as PDF.

    ↳ *Master locking level* window closes.

↳ Common locking level has been created and is [Service Sets] listed in the tab.

You can now use this common locking level to create transponders that will appear in all assigned locking systems (see *Creating transponders for common locking level [▸ 287]*).

18.2.2 Creating transponders for common locking level

✓ AXM Lite open.
✓ List with transponders or matrix screen opened.
✓ Common locking level created and locking system assigned (see *Creating a common locking level [▸ 285]*).

1. Switch to a locking system that you have assigned to the common locking level.
2. Click on the New transponder button.
    ↳ The window for creating an identification medium will open.

3. Select the ☑ Master locking level checkbox.
    ↳ Options for selecting the common locking level are displayed.
    ↳ Additional locking systems tab disappears.

4. Fill in the remaining options as for a normal transponder (see *Creating transponders and cards [▸ 77]*).

5. Click on the Finish button.
   ↳ The window for creating a new identification medium closes.

↳ The transponder is created in all assigned locking systems.

↳ Since it belongs to a common locking level, it is displayed in the locking level colour (red in the example).

Transponder in the first locking system:

Transponder in the second locking system:

You can now authorise the transponder created in multiple locking systems at the different locking devices in the locking systems (see *Authorising a transponder with common locking level [▸ 288]*).

After synchronisation is complete, the *Transponder* and *Colour* fields are displayed in the common locking level colour (example: red).

18.2.3 Authorising a transponder with common locking level

✓ AXM Lite open.

✓ Matrix screen open.

✓ Common locking level created (see *Creating a common locking level [▸ 285]*).

✓ Transponder created in common locking level (see *Creating transponders for common locking level [▸ 287]*).

1. Use the drop-down menu to switch from the common locking level to the locking system.

2. Assign all required authorisations in this locking system.

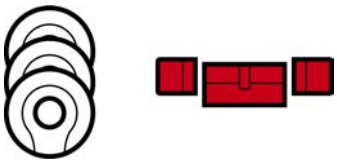
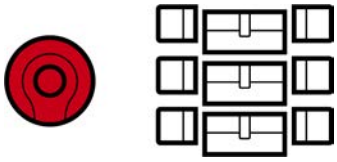
3. Use the drop-down menu to switch to the next locking system that you have assigned to the common locking level.
4. Assign all desired authorisations there as well.

5. Synchronise the locking devices and transponders as usual (see *Synchronising the locking device (including reading access list) [▸ 291]* and *Synchronising an identification medium [▸ 303]*).

↳ Thanks to the common locking level, the same transponder can operate locking devices from different locking systems.

19. Synchronisation: Comparison between locking plan and reality

Since the G2 protocol was introduced, it is up to you whether you synchronise the locking device or the identification medium for a new authorisation, for example.

Synchronising a locking device	Synchronising an identification medium
Synchronising the locking device (including reading access list) [▸ 291]	*Synchronise a card/transponder (including importing physical access list) [▸ 304]*
Useful if many identification media have been authorised for a locking device. In this case, only one locking device needs to be synchronised instead of many identification media. 	Useful if an identification medium has been authorised for many locking devices. In this case, only one identification medium needs to be synchronised instead of many locking devices. 

Other factors are important to consider when making this decision, such as:

- Available programming devices
- Locking device or identification medium on site
- Access list or physical access list imported

Synchronisation from the matrix

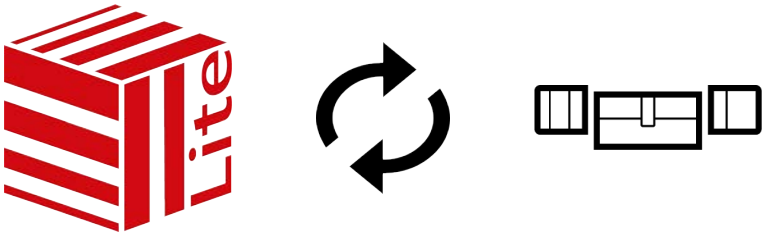
You can display the synchronisation requirement in the matrix. If you click directly on the ⟳ icon, you immediately start synchronising the entry concerned.

Initial or regular synchronisation

An initial synchronisation (symbol: ⟳) differs from other synchronisations (symbol: ⟳) due to the larger amount of data. In the case of AX locking devices, it is therefore preferable to use a SmartStick AX or a SmartCD.MP, especially for initial synchronisations.

SmartStick AX	SmartCD.MP

19.1 Synchronising the locking device (including reading access list)



Synchronisation is bidirectional:

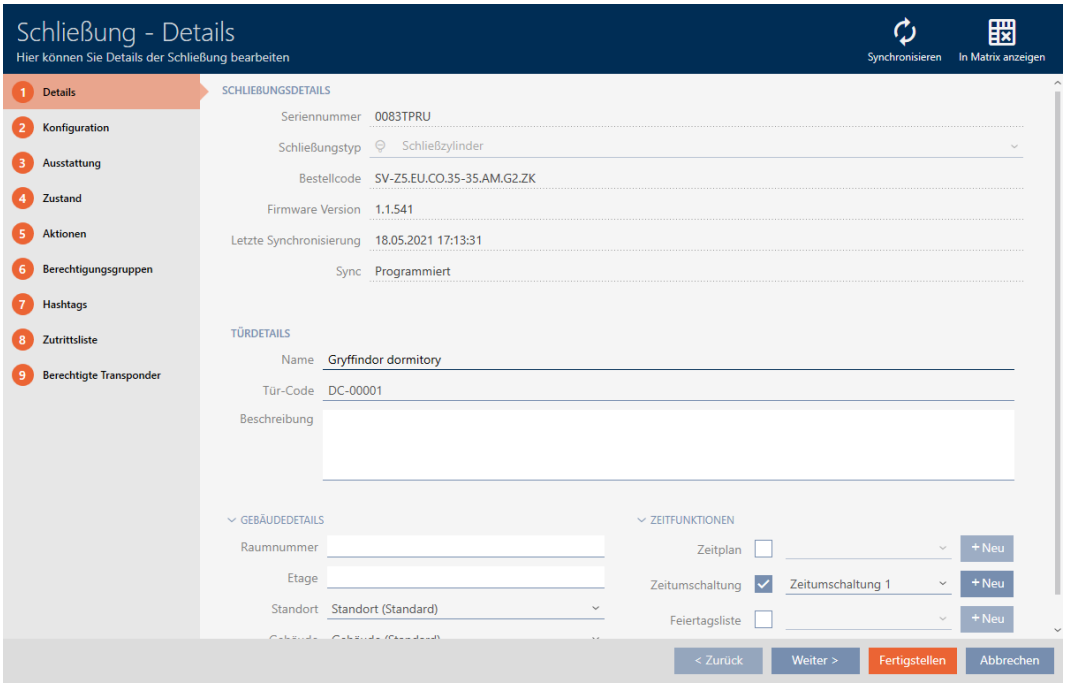
- Reading of data stored in the locking device (e.g. battery level)
- Writing of new data onto the locking device (e.g. authorisations)

Access lists can be imported separately (Read access list button). Access lists can also be easily read during synchronisation as an option (see *Reading access list/physical access list during synchronisation [▸ 327]*).

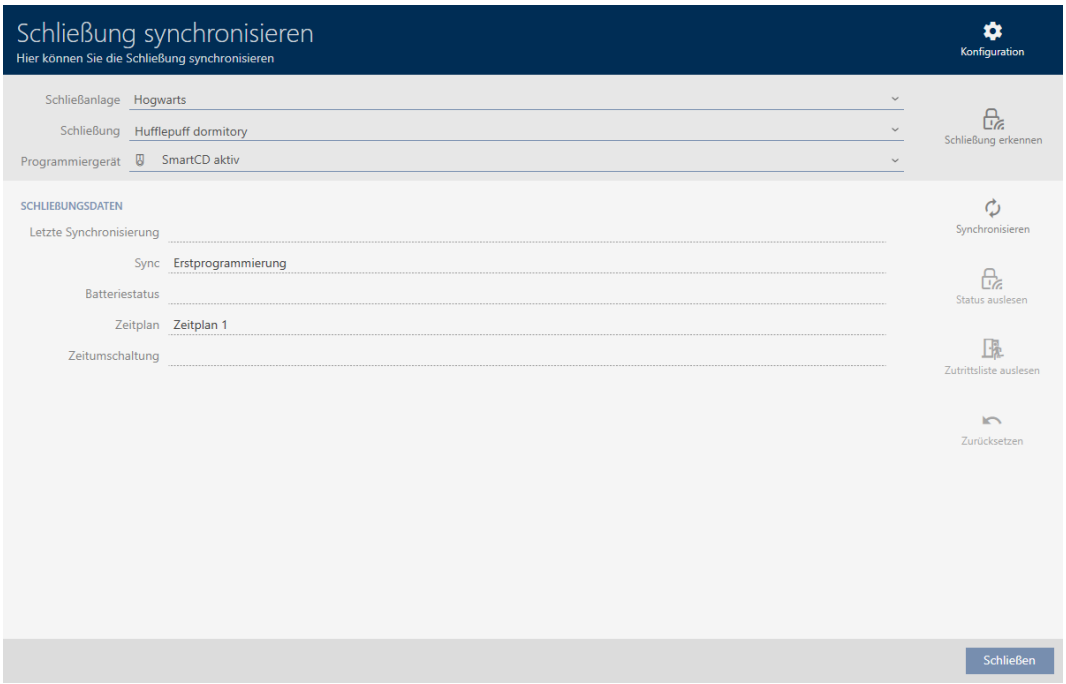
The imported data can then be displayed (see *Display locking device equipment and status [▸ 294]* or *Displaying and exporting a locking device's access list [▸ 296]*, for example).

✓ AXM Lite open.
✓ Locking device list or matrix view open.
✓ Suitable programming device connected.

1. Click on the locking device you wish to synchronise.
   ↳ The locking device window will open.



2. Click on the Synchronisation button .
   ↳ Synchronise window will open.



3. Select the programming device which you wish to use to synchronise from the ▼ **Programming device** drop-down menu.

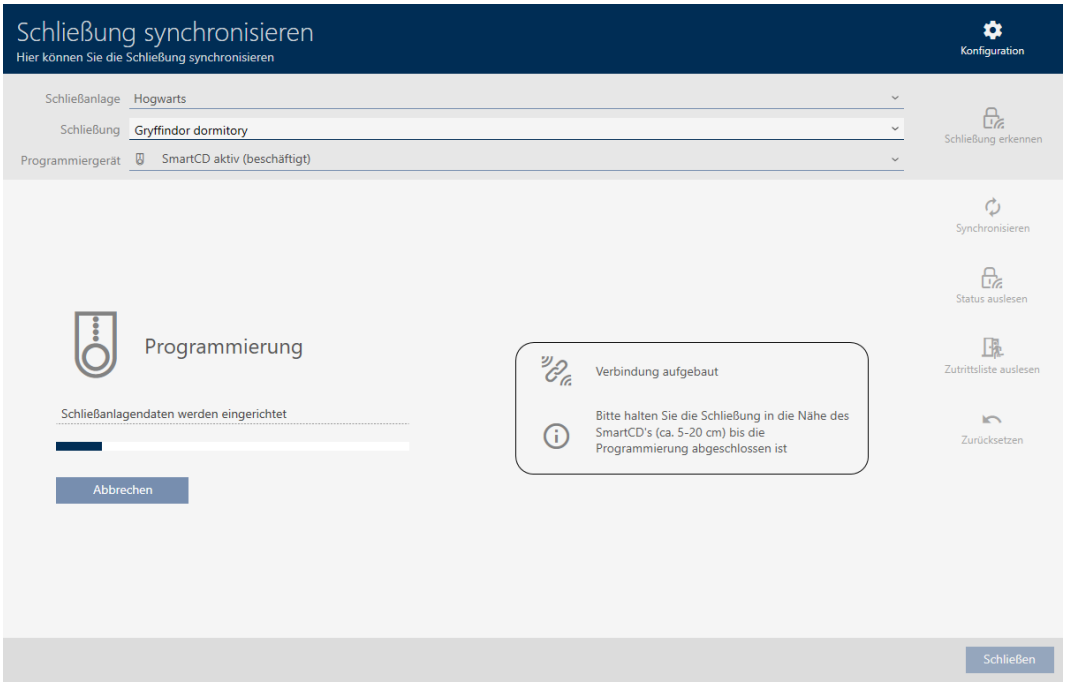
NOTE

AX components: SmartCD.MP or SmartStick AX for initial synchronisation

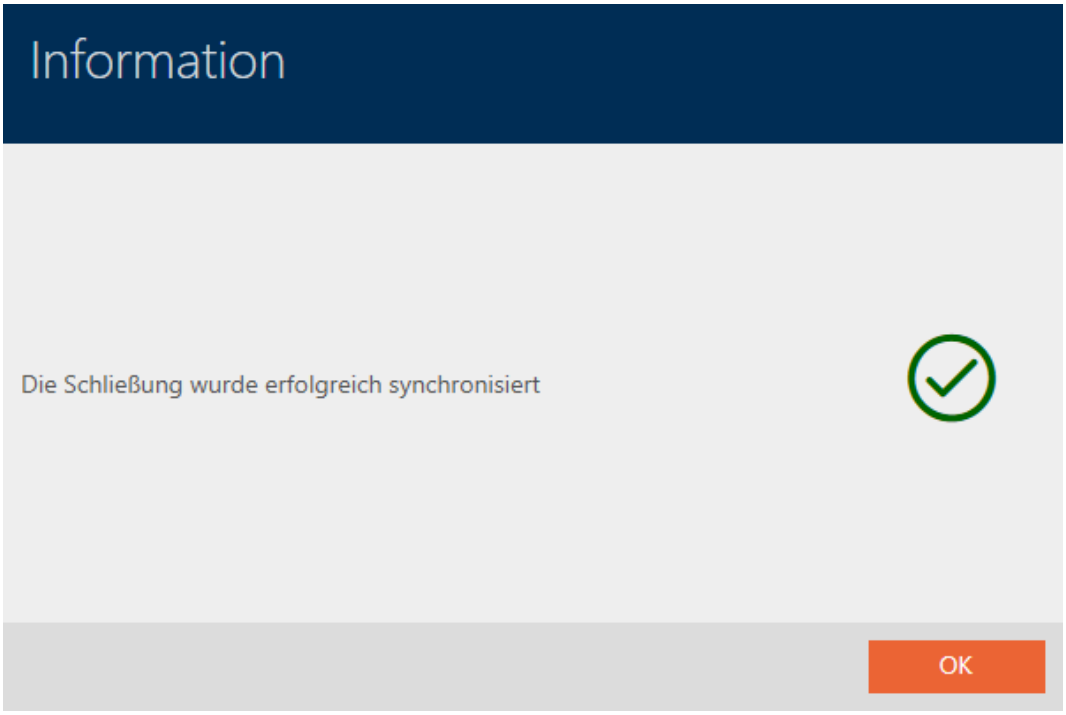
A great deal of data is transferred during initial synchronisation of AX components. The carrier frequency and, consequently, the transmission speed is significantly higher with the SmartCD.MP or SmartStick AX.

- It is especially important to use a SmartCD.MP or a SmartStick AX for initial synchronisation of AX components.

4. Click on the Synchronisation button.
   ↳ Locking device is being synchronised.



↳ Locking device is synchronised.



NOTE

First transponder activation rejected after initial programming of AX products

If a transponder is the first identification medium to be activated after initial programming, the transponder can be rejected once and synchronised with the locking device in the background. Transponders will then function as normal.

19.1.1 Display locking device equipment and status

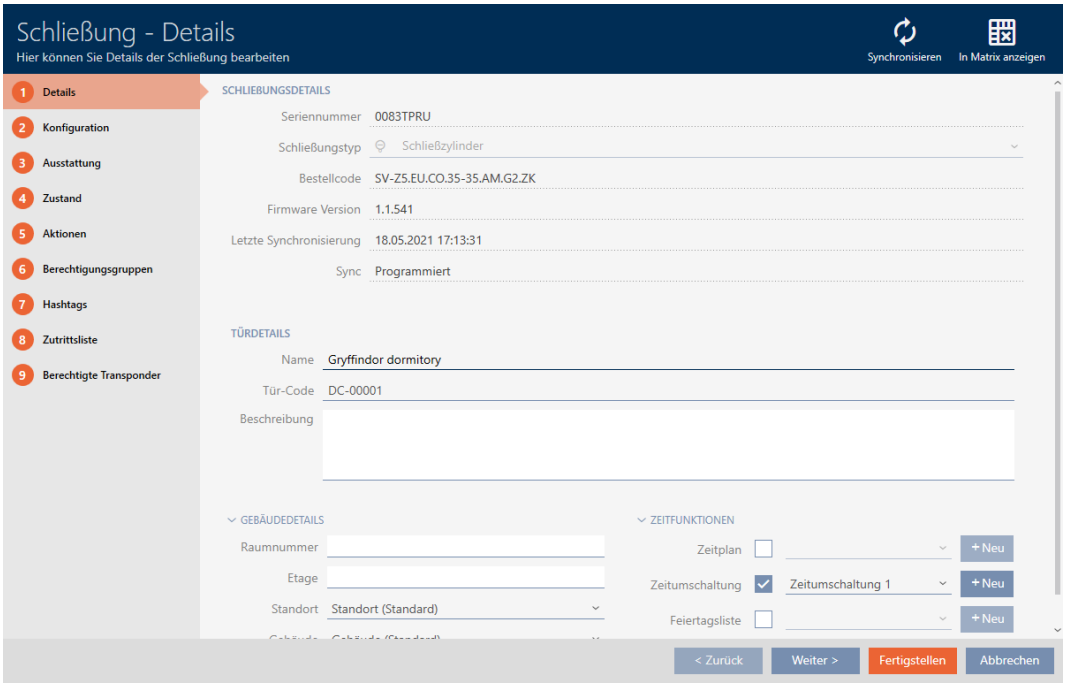
NOTE

Displayed status corresponds to the last synchronisation

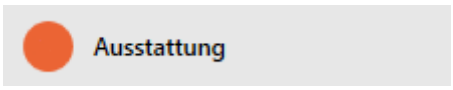
AXM Lite displays the status stored in the database at this point.

✓ AXM Lite open.
✓ Locking device synchronised at least once.

1. Click on the locking device whose status you wish to display.
   ↳ The locking device window will open.



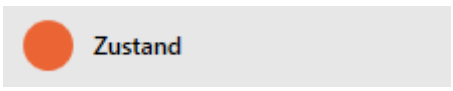
2. Click on the Features tab.



↳ Window switches to the "Features" tab.
↳ Imported equipment features are displayed (only for locking devices that have already been synchronised).

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. Click on the State tab.



↳ Window switches to the "State" tab.
↳ The imported status is displayed (only for locking devices that have already been synchronised).

19.1.2 Displaying and exporting a locking device's access list

The ZK function (access control) enables your locking devices to log which identification media have been activated (see *Have accesses logged by locking device (access list) [▸ 228]*). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation [▸ 327]* and *Synchronising the locking device (including reading access list) [▸ 291]*).

You can view and export the access list in the database.

NOTE

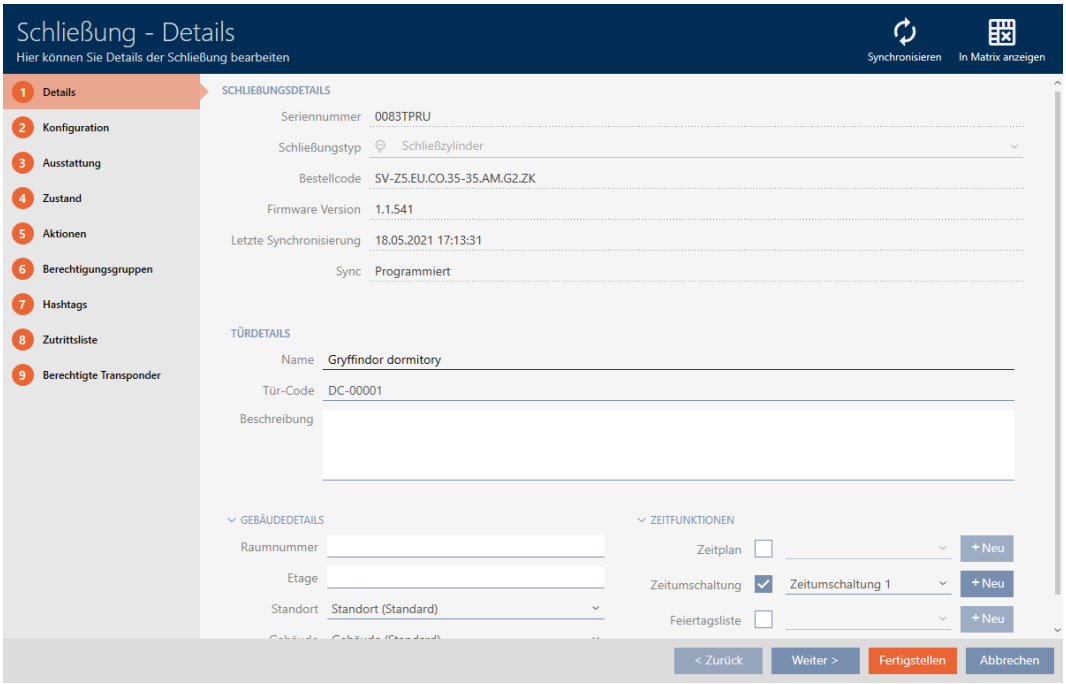
Displayed status corresponds to the last synchronisation

AXM Lite displays the status stored in the database at this point.

✓ AXM Lite open.

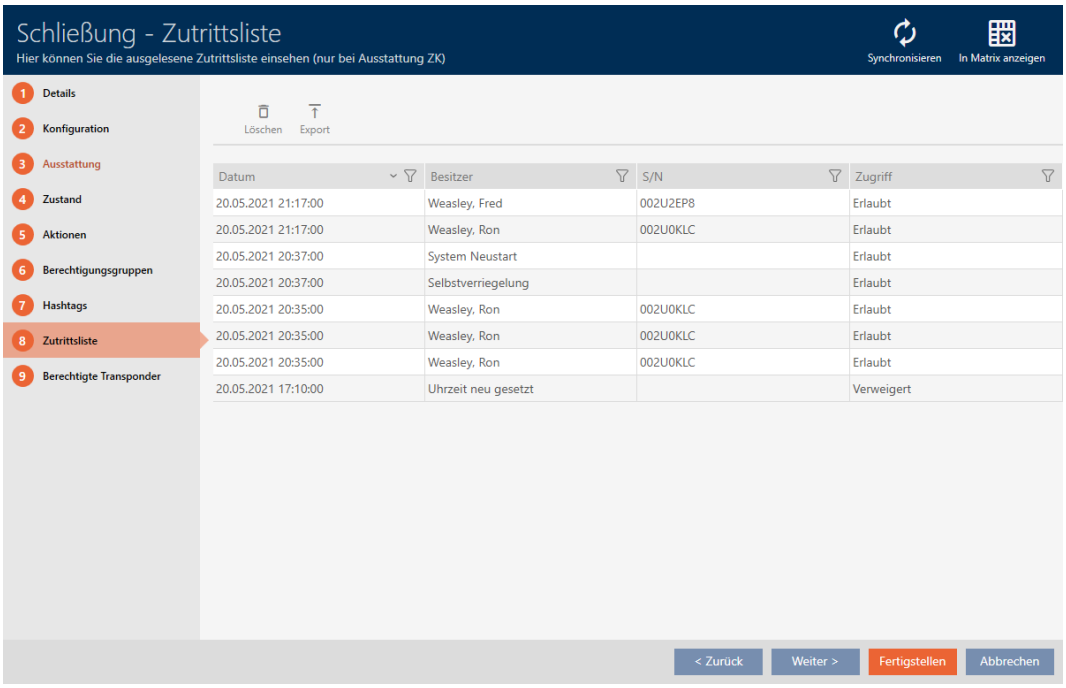
✓ Locking device synchronised at least once.

1. Click on the locking device whose access list you wish to display.
   ↳ The locking device window will open.



2. Click on the Access list tab.

↳ Window switches to the "Access list" tab.
↳ The imported access list is displayed (only for locking devices that have already been synchronised).



1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the Export ⤒ button.
   ↳ The Explorer window will open.
3. Save the exported access list to a file directory of your choice.
   ↳ Explorer window closes.

↳ The access list is exported.

Simons≡Voss technologies

Zutrittsliste für die Schließung 'Gryffindor dormitory'

Datum	Besitzer	S/N	Zugriff	Schließungskomponente
30.05.2021 04:57:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:55:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:54:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:53:00	##ServiceTId_IDS_AX_SETTIME		Verweigert	Master
30.05.2021 04:42:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:37:00	##ServiceTId_IDS_AX_SYSSTART		Erlaubt	Master
30.05.2021 04:37:00	##ServiceTId_IDS_TTL_SELF_CLOSE		Erlaubt	Master
21.05.2021 11:26:00	Weasley, Fred	002U2EP8	Erlaubt	Master
21.05.2021 11:26:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:26:00	Weasley, Fred	002U2EP8	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 21:17:00	Weasley, Fred	002U2EP8	Erlaubt	Master
20.05.2021 21:17:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:37:00	##ServiceTId_IDS_AX_SYSSTART		Erlaubt	Master
20.05.2021 20:37:00	##ServiceTId_IDS_TTL_SELF_CLOSE		Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 17:10:00	##ServiceTId_IDS_AX_SETTIME		Verweigert	Master
30.03.2019 00:45:00	##ServiceTId_IDS_DM_DOOR_CLOSED		Erlaubt	Master

Simons≡Voss technologies Gedruckt am: 03.12.2021 1

19.2 Identifying an unknown locking device

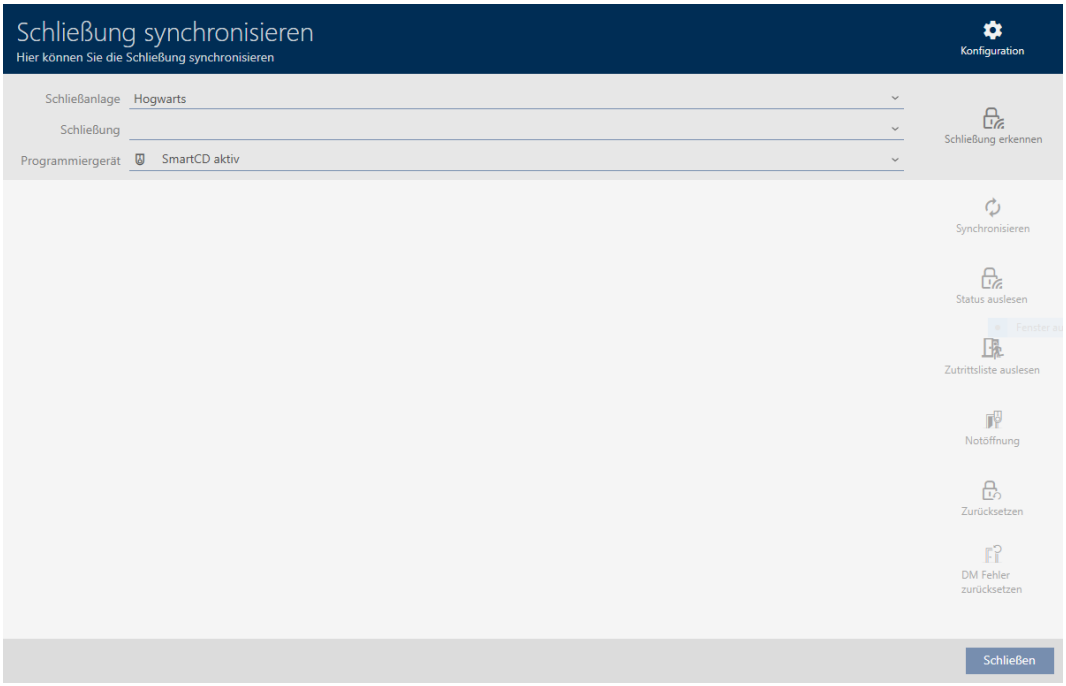
If you have an unknown locking device, you can use, for example, the synchronise symbol ( ) to identify it and reset if necessary (see *Re-setting the locking device [▸ 300]*).

✓ Suitable programming device connected.

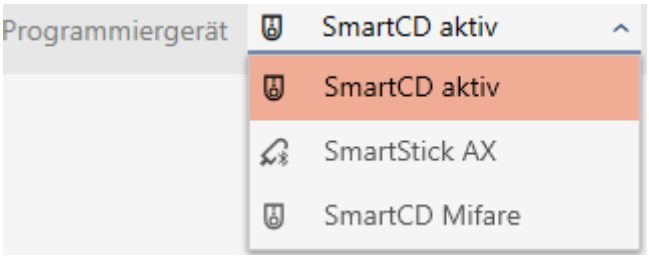
✓ AXM Lite open.

1. Click on the icon in the header.

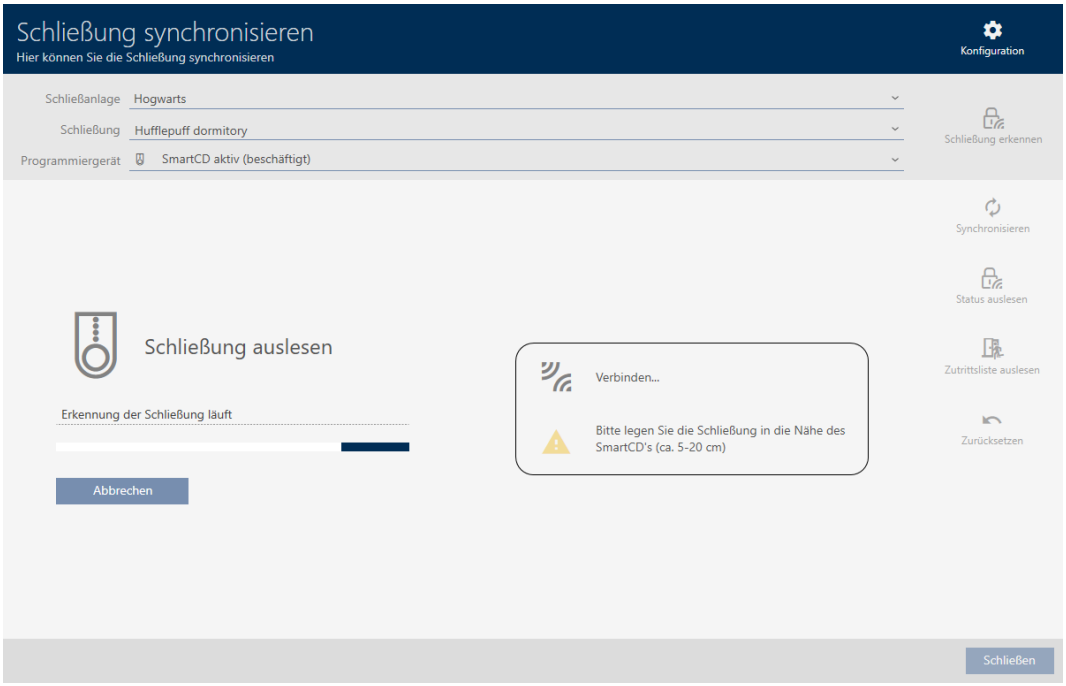
↳ The "Synchronise lock" window will open.



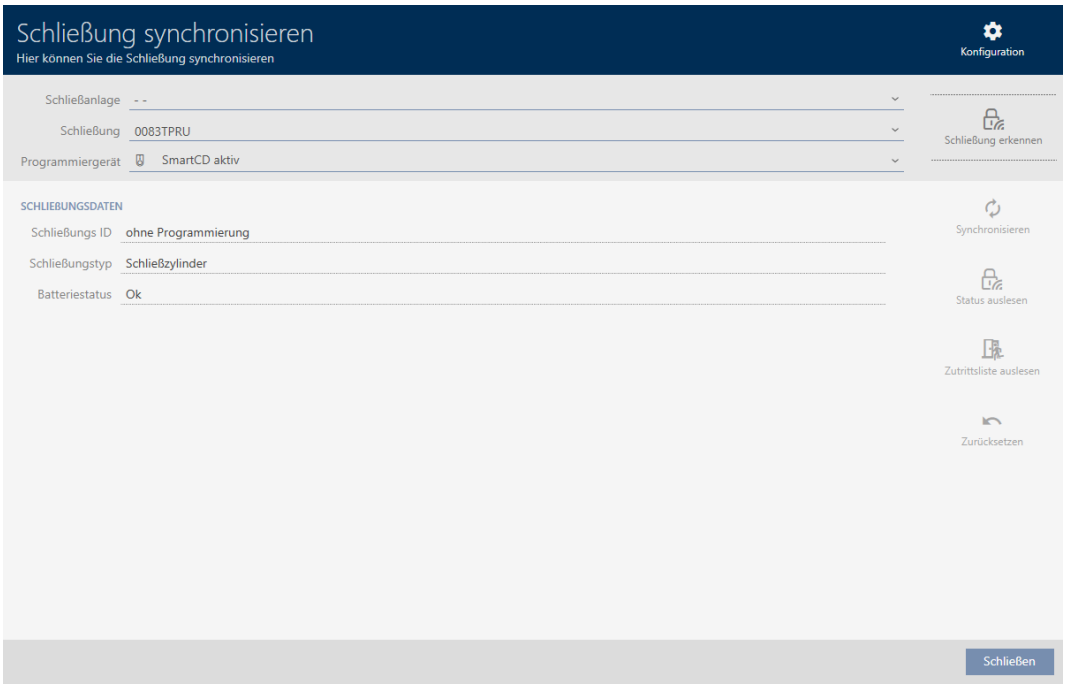
2. Select the programming device you wish to use to identify your locking device from the ▼ **Programming device** drop-down menu.



3. Click on the Detect lock button.
   ↳ Locking device is identified.



↳ Locking device information is displayed in the locking device window.



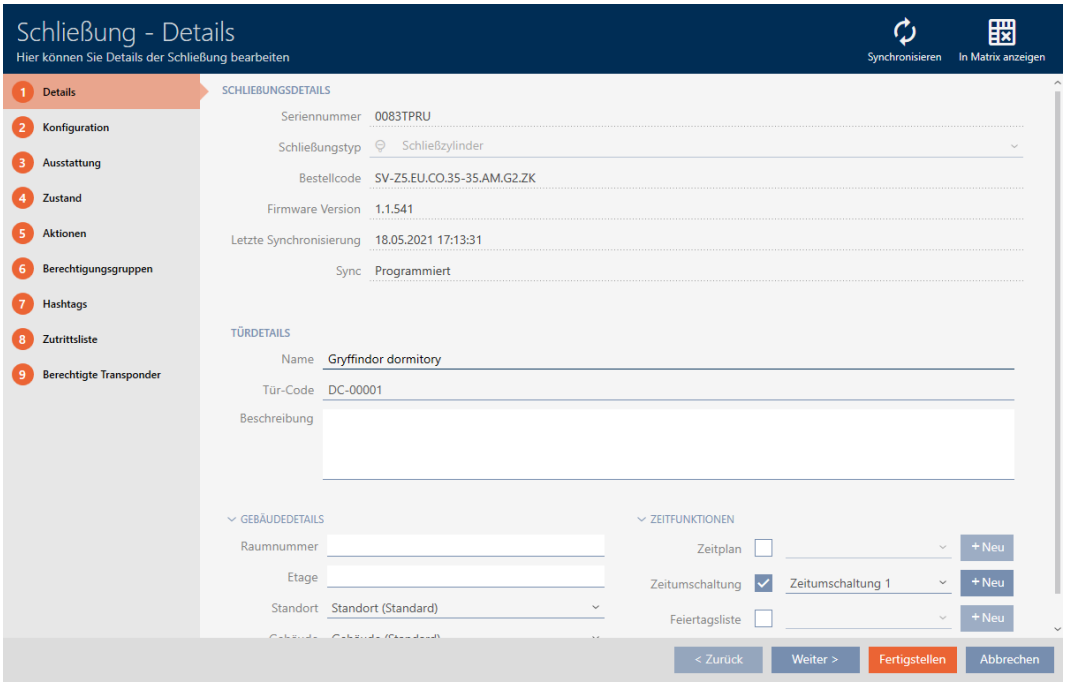
You can now reset the locking device, for example (see *Re-setting the locking device [▸ 300]*).

19.3 Re-setting the locking device

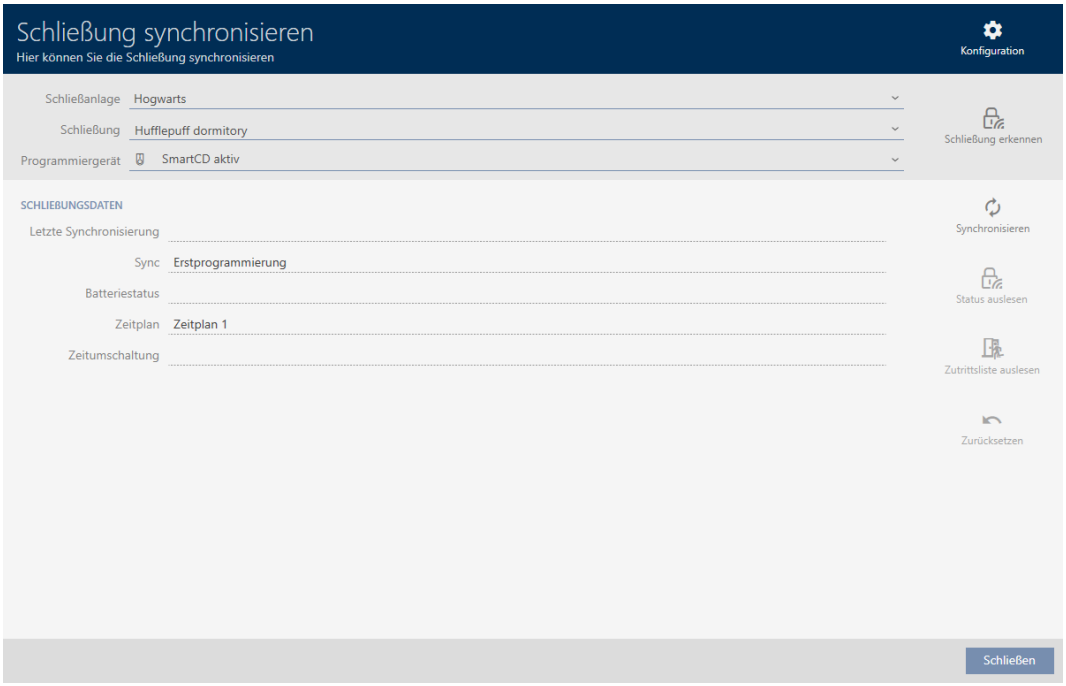
You must reset a component such as a locking cylinder before it can be used for another locking device or another locking system.

✓ Suitable programming device connected.
✓ AXM Lite open.
✓ Locking device list or matrix view open.

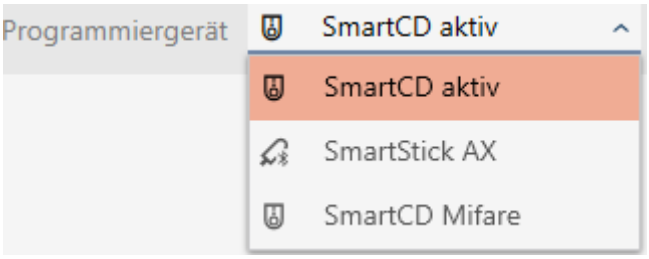
1. Click on the locking device you wish to reset.
   If you do not know the locking device, click on any locking device and identify the locking device (see *Identifying an unknown locking device [▸ 298]*). Then continue.
   ↳ The locking device window will open.



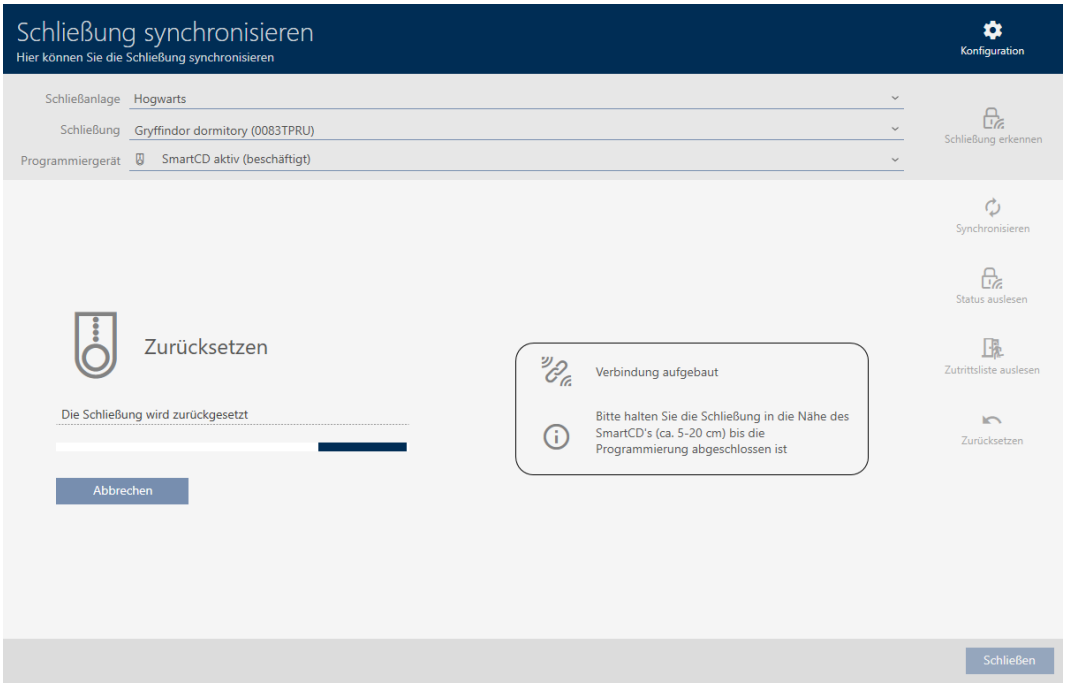
2. Click on the Synchronisation button .
   ↳ Synchronise window will open.



3. Select the programming device from the ▼ **Programming device** drop-down menu with which you wish to reset your locking device.



4. Click on the Reset button .
   ↳ The locking device is reset.



5. If necessary, accept the query asking whether the access lists should be imported again beforehand.

↳ Locking device is reset.

19.4 Synchronising an identification medium

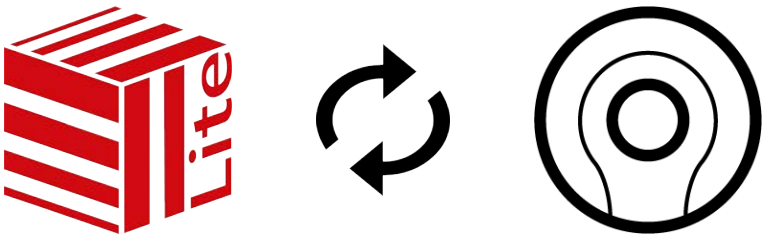
Synchronisation is bidirectional:

- Importing of data stored in the identification medium (e.g. battery level)
- Writing new data onto the identification medium (e.g. authorisations)

Physical access list can be imported separately (Read personal audit trail button). Physical access lists can also be imported easily during synchronisation as an option (see *Reading access list/physical access list during synchronisation [▸ 327]*).

The imported data can then be displayed (see *Displaying the identification medium battery status [▸ 306]* or *Displaying and exporting physical access lists for cards/transponders [▸ 307]*, for example).

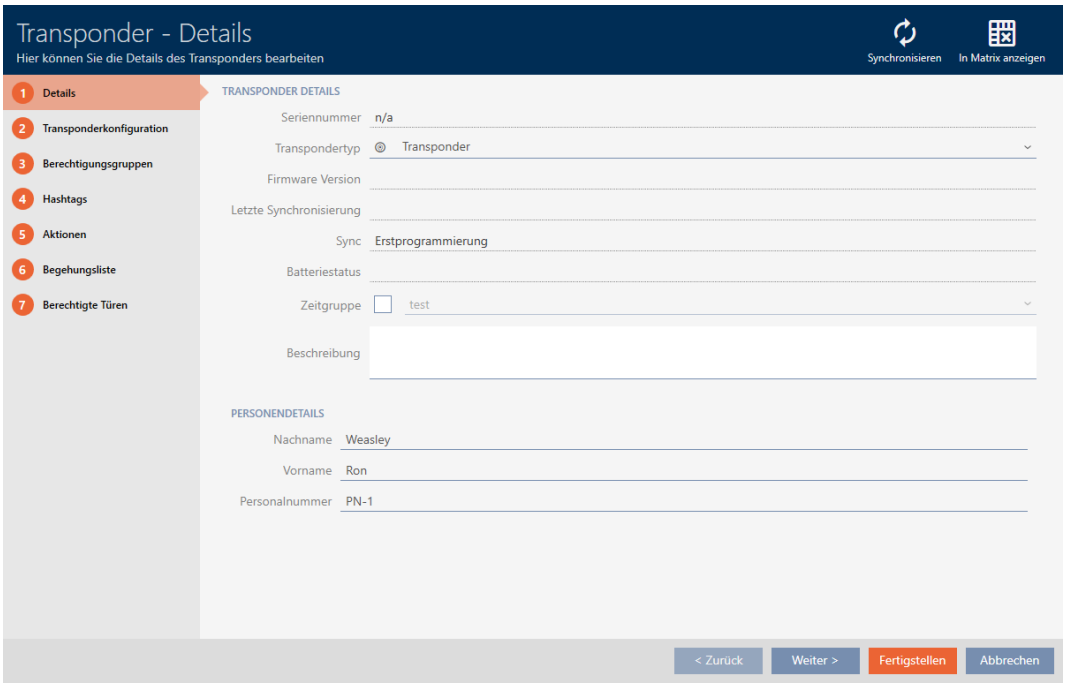
19.4.1 Synchronise a card/transponder (including importing physical access list)



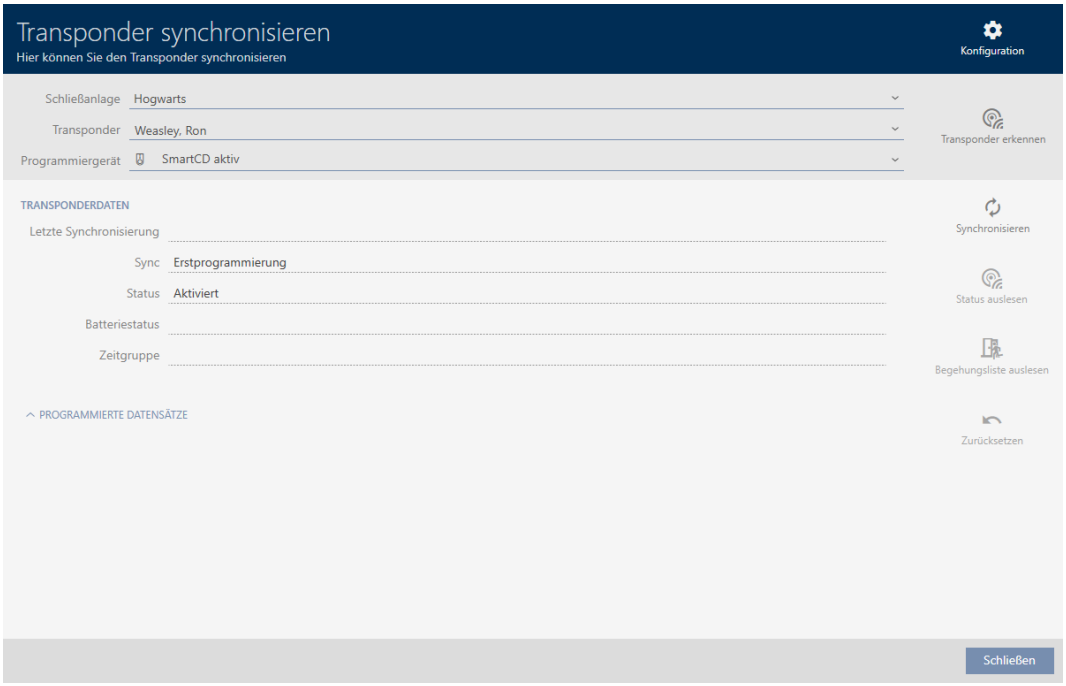
The following example shows how to synchronise a transponder.

✓ Suitable programming device connected.
✓ AXM Lite open.
✓ Identification media list or matrix view open.

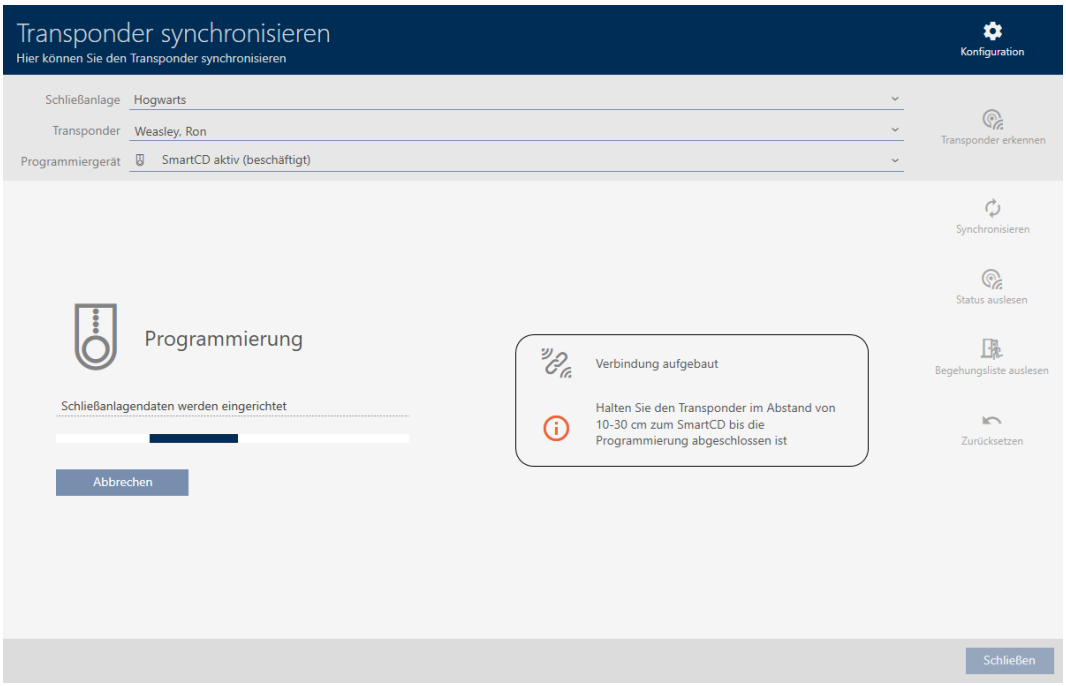
1. Click on the identification medium you wish to synchronise.
   ↳ The identification medium window will open.



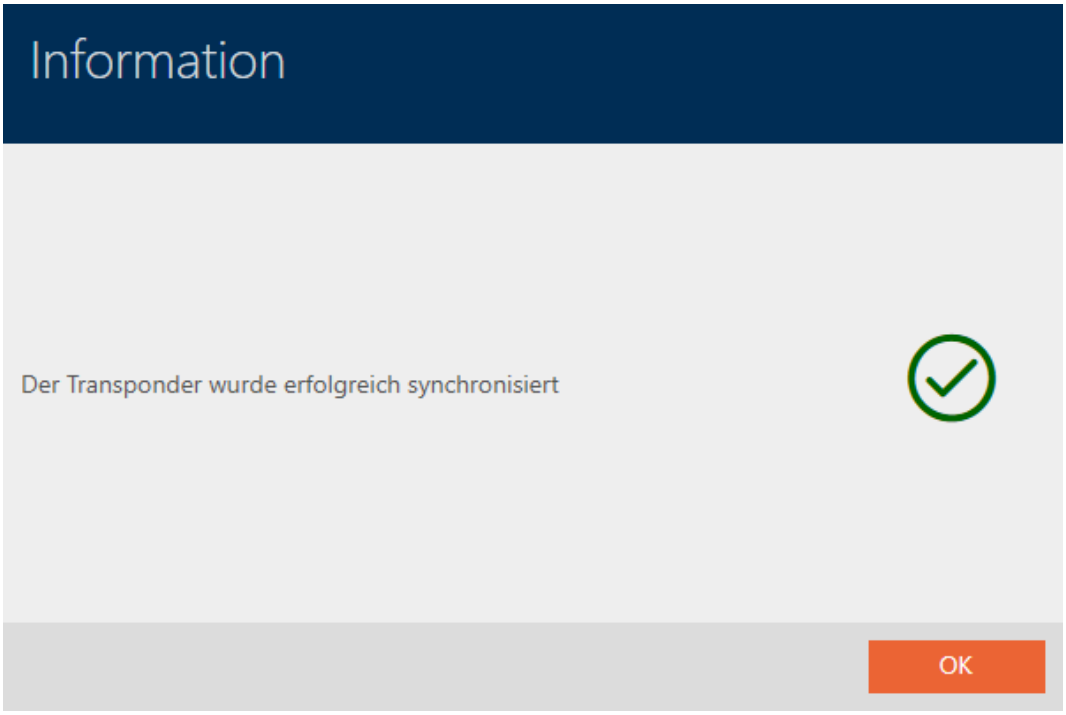
2. Click on the Synchronisation button .
   ↳ Synchronise window will open.



3. Click on the Synchronisation button .
   ↳ Identification medium is synchronised.



↳ ID medium is synchronised.



19.4.1.1 Displaying the identification medium battery status

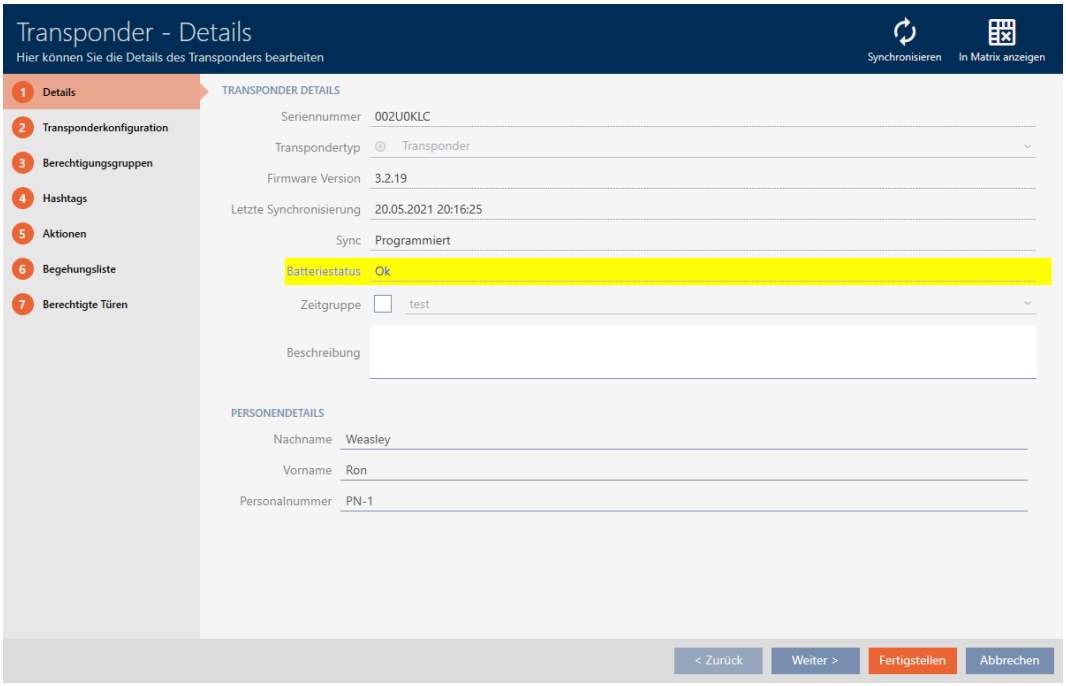
NOTE

Displayed status corresponds to the last synchronisation

AXM Lite displays the status stored in the database at this point.

✓ AXM Lite open.
✓ Identification medium synchronised at least once.

- Click on the identification medium whose status you wish to display.
  ↳ The identification medium window will open.



↳ Battery status is displayed.

19.4.1.2 Displaying and exporting physical access lists for cards/transponders

If required, your identification media can log which locking devices they were activated on (see *Allow accesses to be recorded by identification media (physical access list) [▸ 103]*). The entries saved in this physical access list are then transferred to the database during synchronisation, for example (see *Synchronise a card/transponder (including importing physical access list) [▸ 304]*).

You can view and export the physical access lists saved in the database.

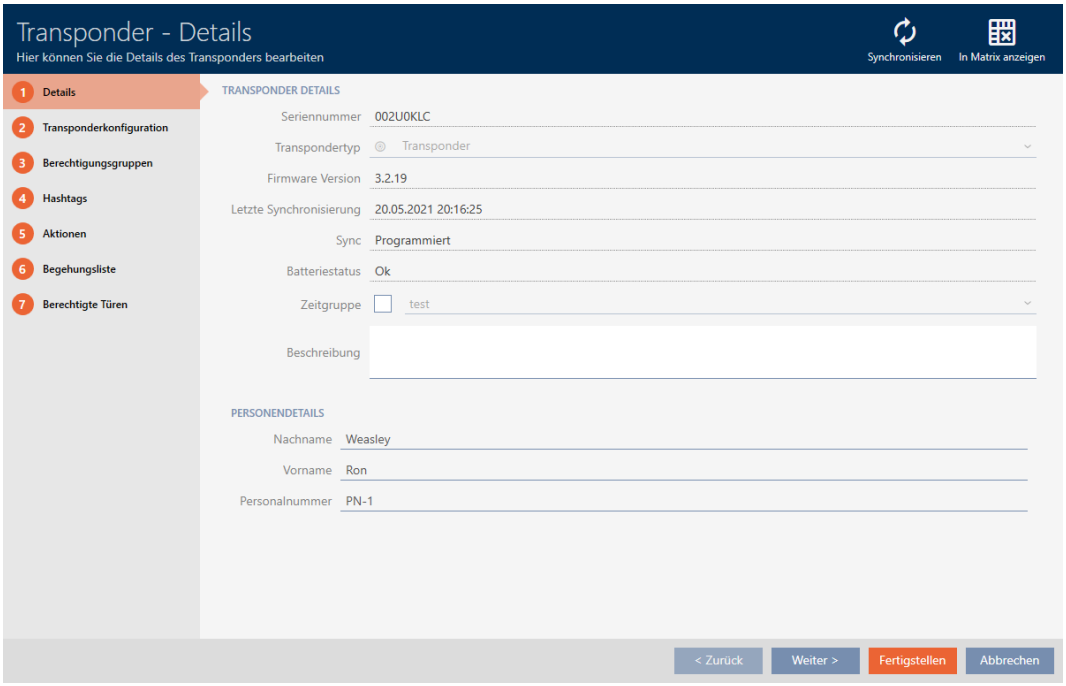
NOTE

Displayed status corresponds to the last synchronisation

AXM Lite displays the status stored in the database at this point.

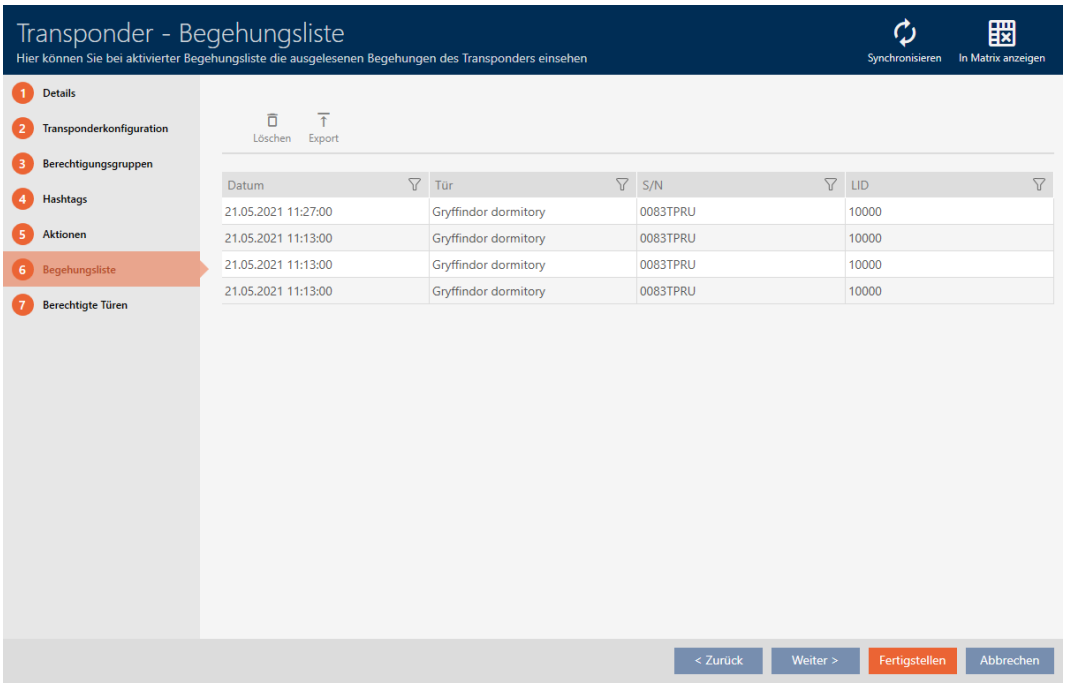
✓ AXM Lite open.
✓ Identification medium synchronised at least once.

1. Click on the identification medium whose physical access list you wish to display.
   ↳ The identification medium window will open.



2. Clicking on the Personal audit trail tab

↳ Window switches to the "Personal audit trail" tab.



3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Click on the Export ⤒ button.
   ↳ The Explorer window will open.

5. Save the exported physical access list to a file directory of your choice.
   ↳ Explorer window closes.

↳ Physical access list is exported.

Begehungsliste für den Transponder '002U0KLC'

Datum	Tür	S/N	LID
21.05.2021 11:27:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000

Gedruckt am: 21.05.2021 1

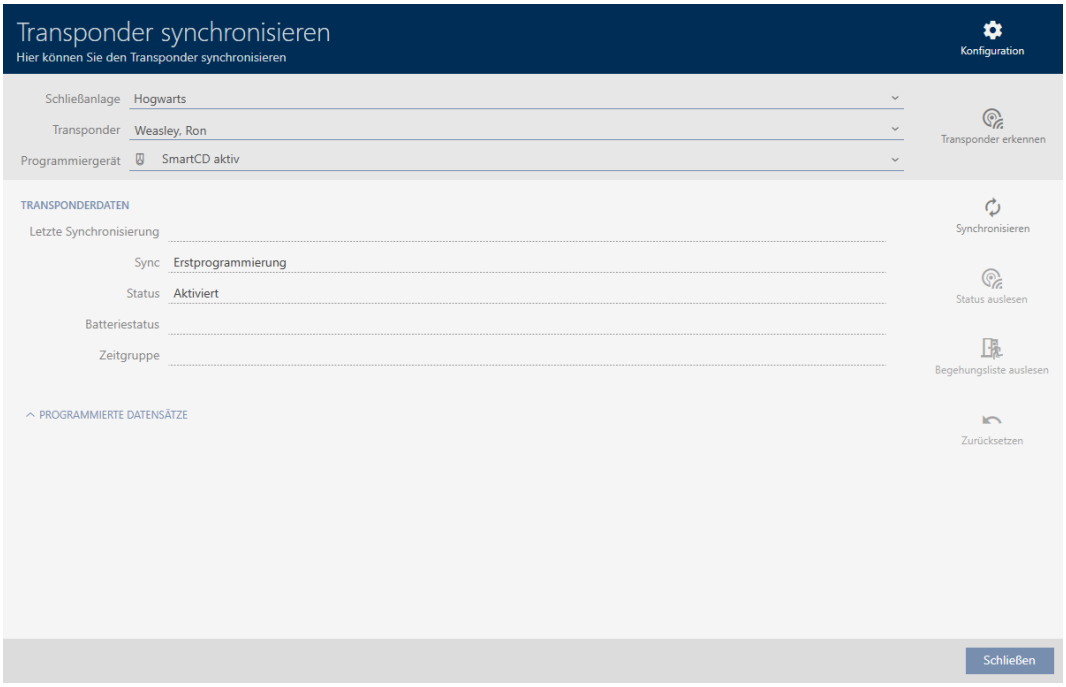
19.5 Identifying an unknown ID medium

19.5.1 Recognise unknown cards/transponders

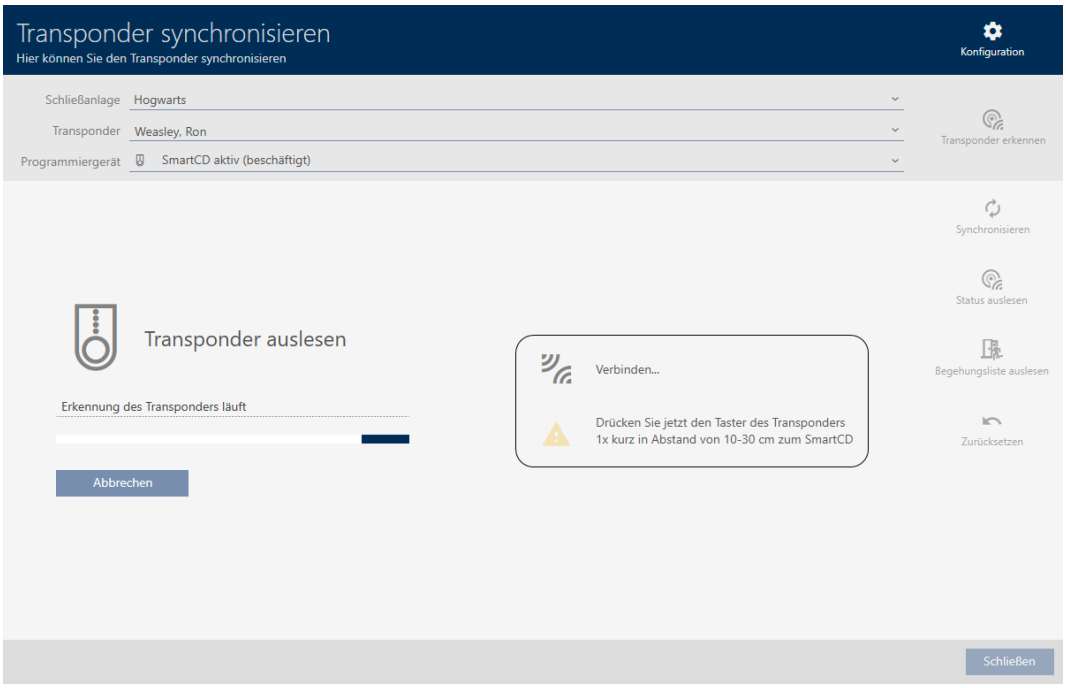
✓ Suitable programming device connected.
✓ AXM Lite open.

1. Click on the icon in the header.

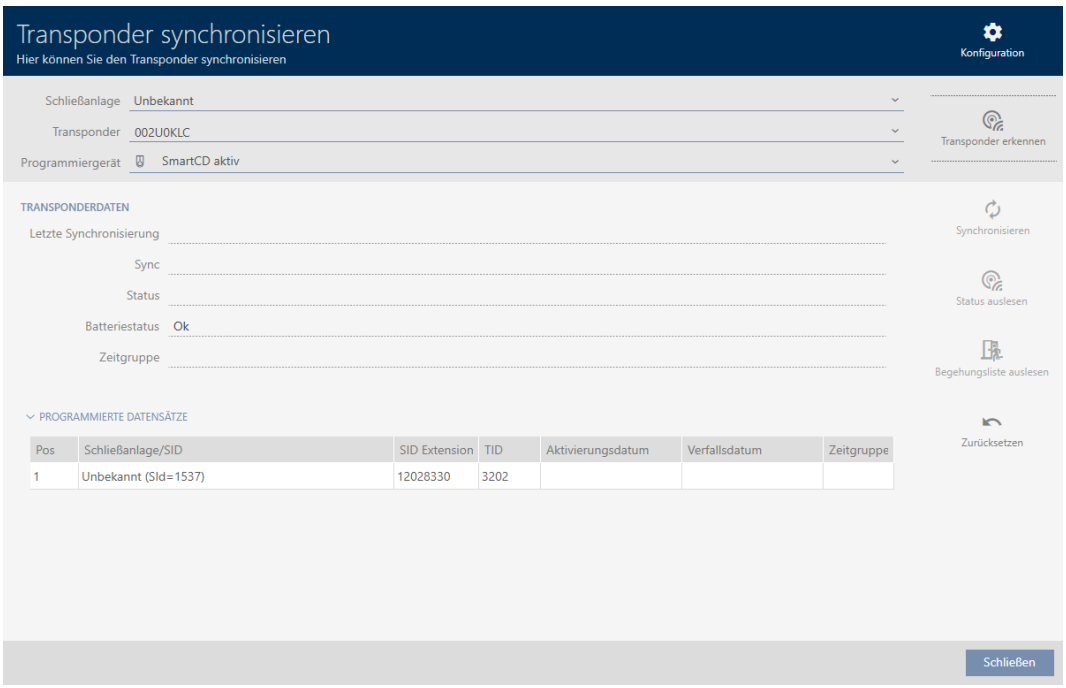
↳ The "Synchronise transponder" window will open.



2. Select the programming device which you wish to use to identify your identification medium from the ▼ **Programming device** drop-down menu.
3. Click on the Identify transponder button .
4. Follow the instructions as necessary.
   ↳ Identification medium is identified.



↳ Information about the identification medium is displayed in the window.



You can now reset the identification medium, for example (see *Resetting cards/transponders [▸ 312]*).

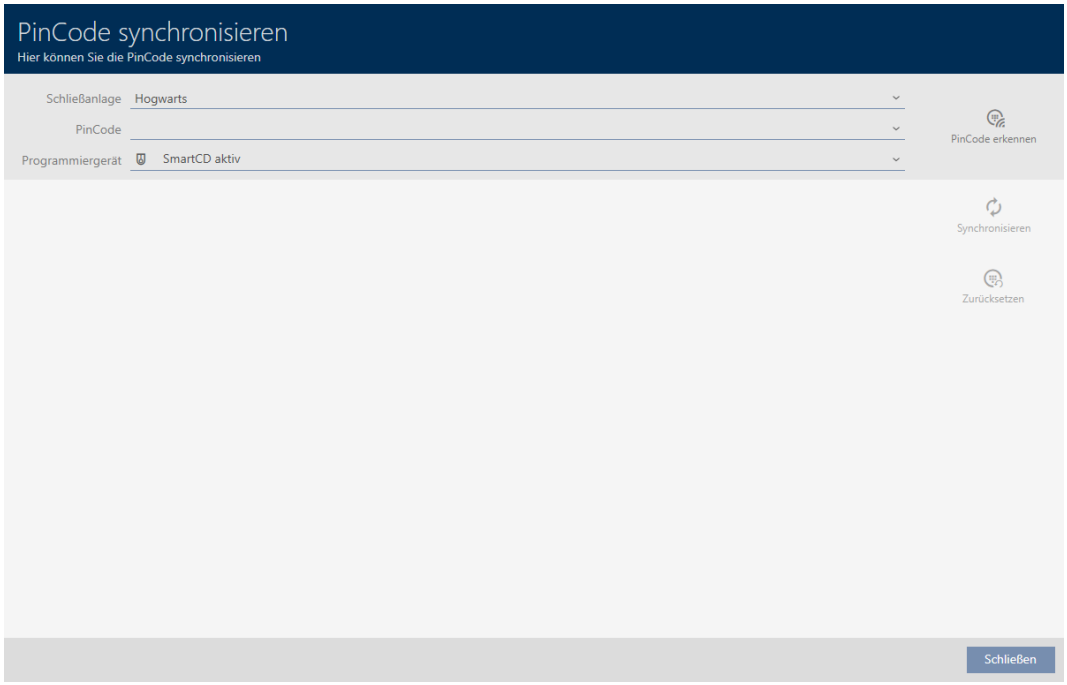
19.5.2 Identifying unknown PIN code keypad

✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)

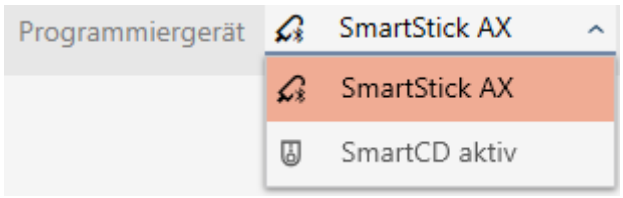
✓ AXM Lite open.

1. Click on the icon in the header.

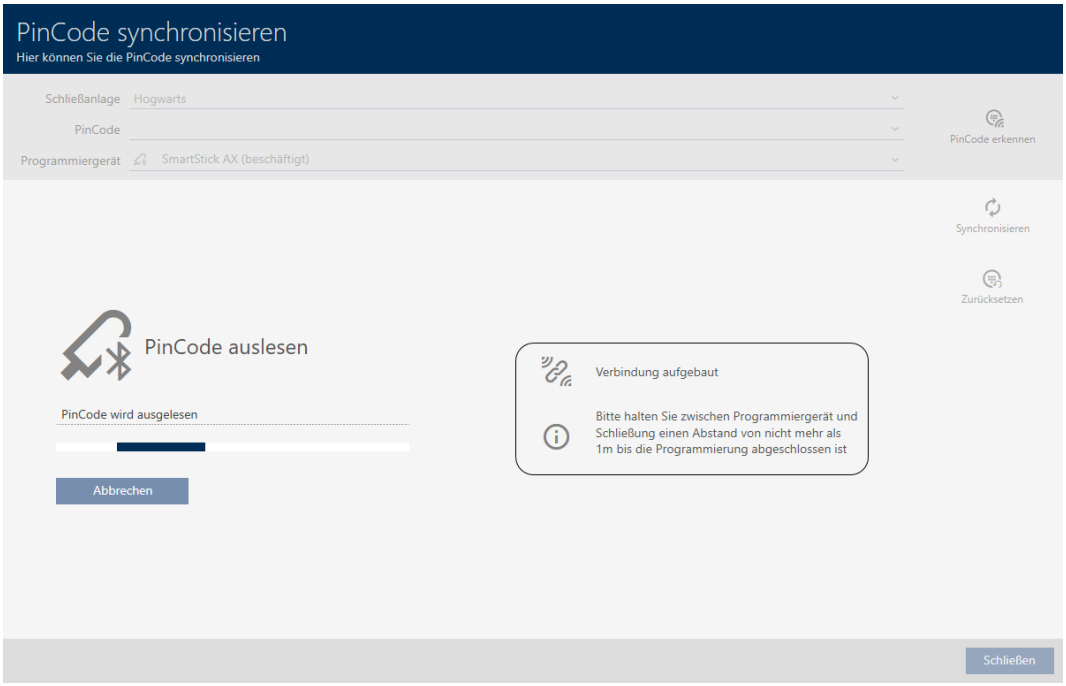
↳ The "Synchronise PinCode" window will open.



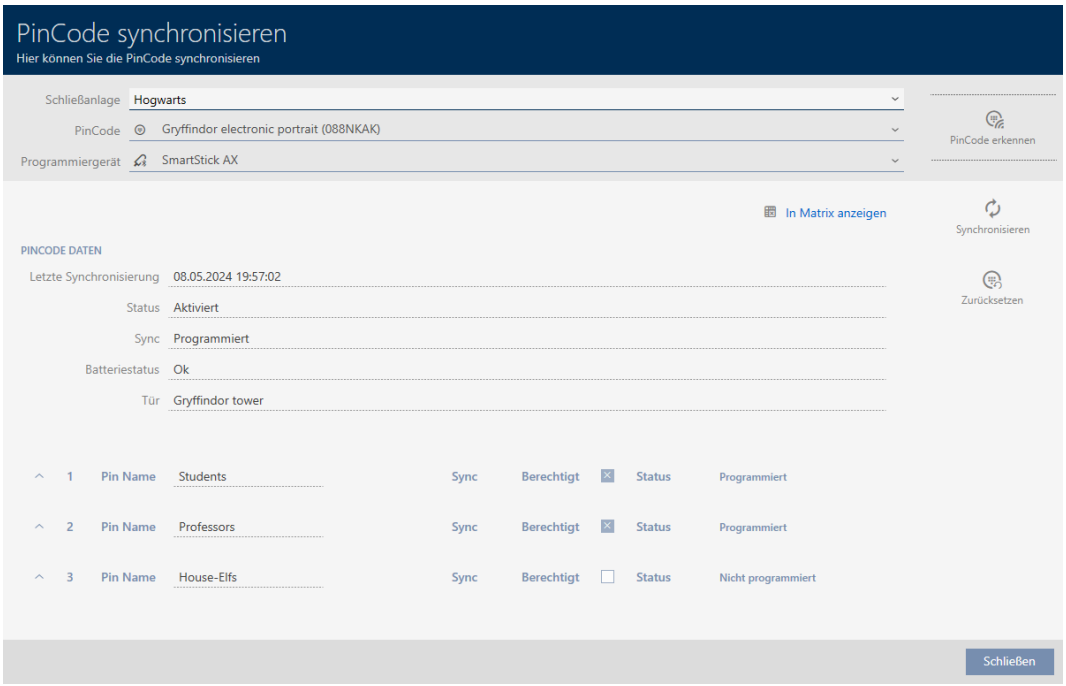
2. Select the programming device you wish to use to identify your PIN code keypad from the ▼ **Programming device** drop-down menu.



3. Click on the Detect PinCode button.
4. Follow the instructions as necessary.
   ↳ PIN code keypad is being read.



↳ Information about the PIN code keypad is displayed in the window.



You can now reset the PIN code keypad, for example (see *Resetting the PIN code keypad [▸ 316]*).

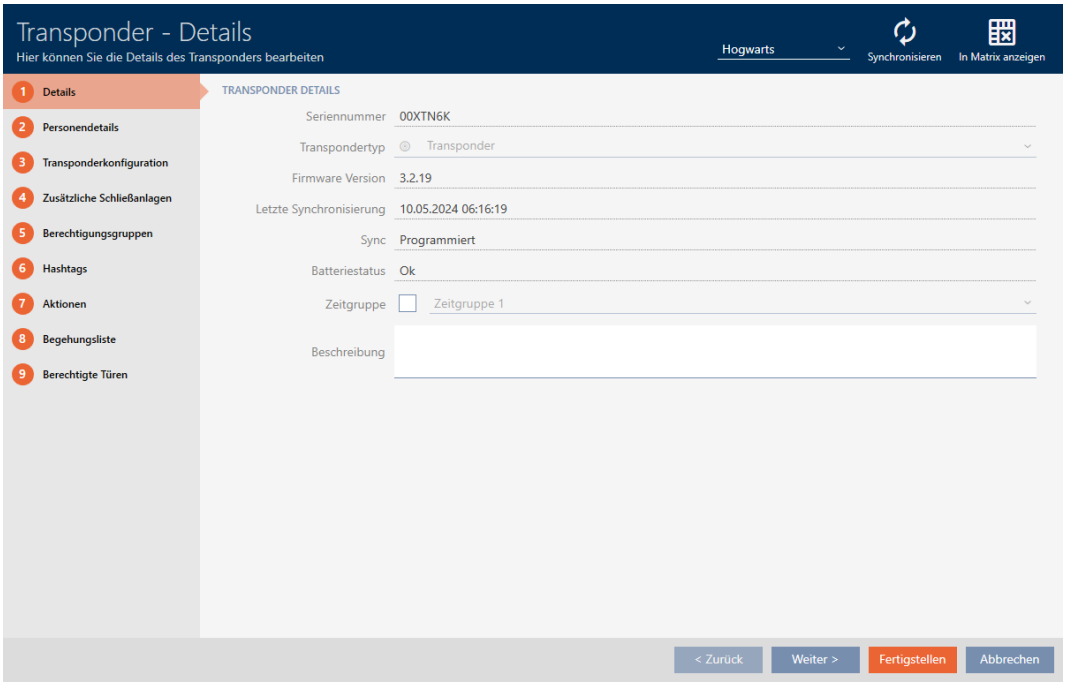
19.6 Resetting identification media

19.6.1 Resetting cards/transponders

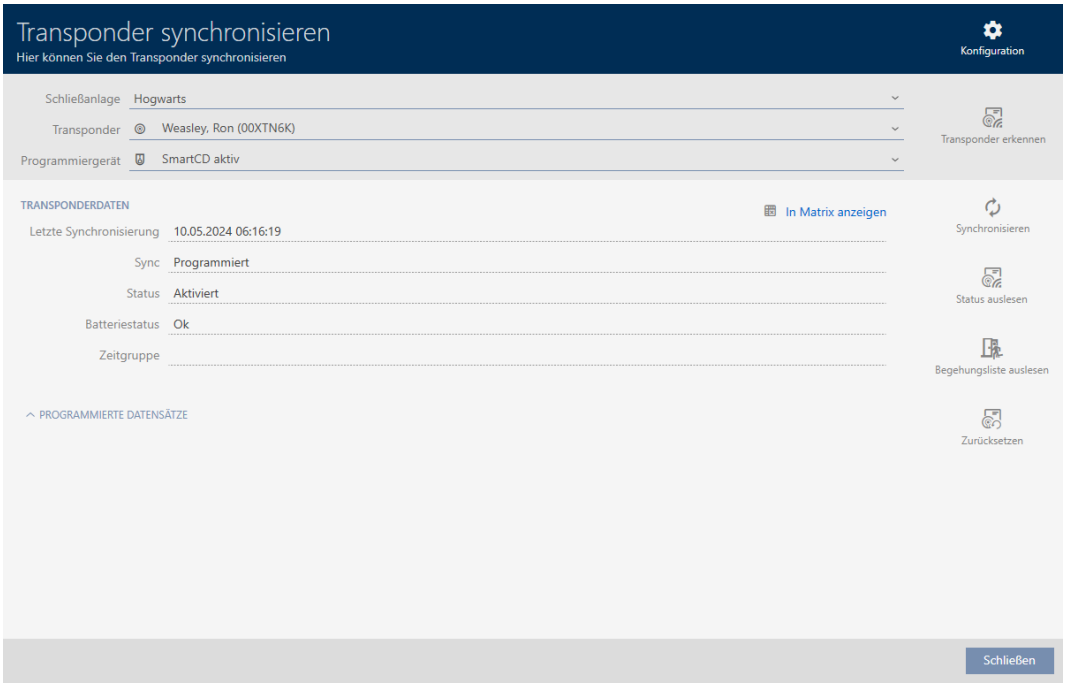
You must reset a component such as a transponder before it can be used again for an identification medium or another locking system.

- ✓ Suitable programming device connected.
- ✓ AXM Lite open.
- ✓ Identification media list or matrix view open.

1. Click on the identification medium you wish to reset.
   If the identification medium is not present in your locking system, identify the identification medium (see *Recognise unknown cards/ transponders [▸ 309]*). Then continue.
   ↳ The identification medium window will open.



2. Click on the Synchronisation button.
   ↳ Synchronise window will open.



3. Select the programming device you wish to use to reset your identification medium from the ▼ **Programming device** drop-down menu.
4. Click on the Reset button .
5. If necessary, select which of the existing data records you wish to reset.

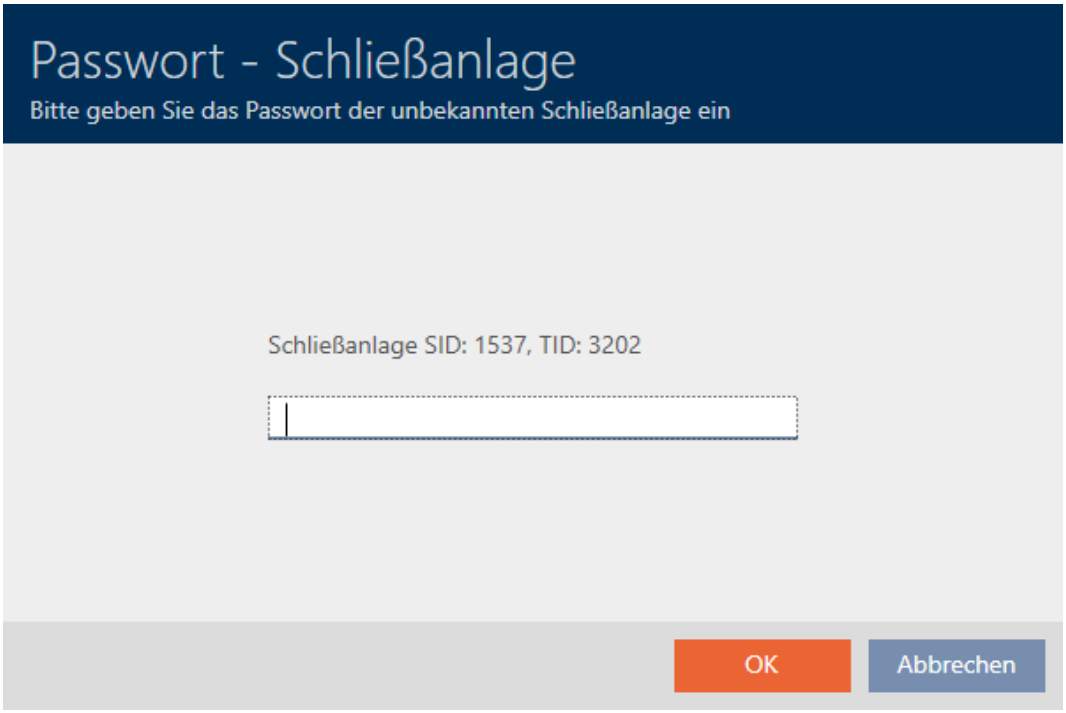
NOTE

Resetting data records from unknown locking systems

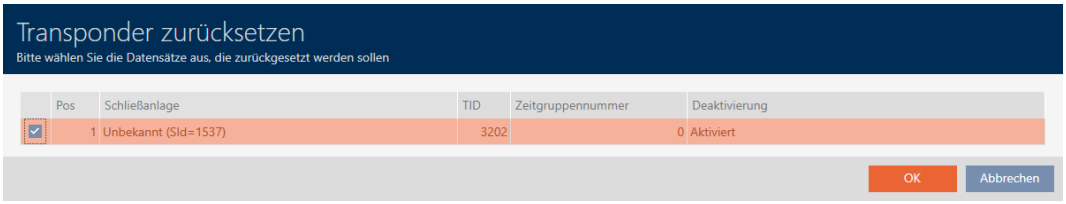
If a locking plan from a different project is stored on the identification medium, your AXM Lite does not recognise this locking system and indicates **Unknown**.

You can also select such data records using the checkbox in the "Pos" column. Since your AXM Lite does not know the locking system and thus doesn't know the locking system password either, you must enter the locking system password for the unknown locking system in this case.

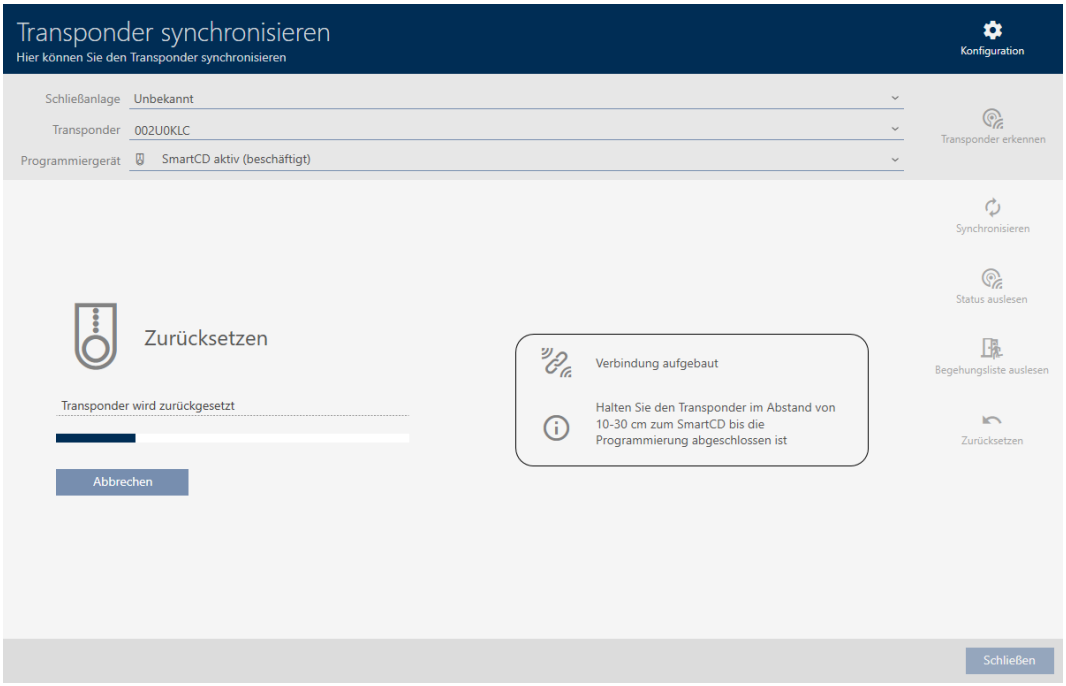
6. If necessary, enter the locking system password for the locking system to which this data record belongs.



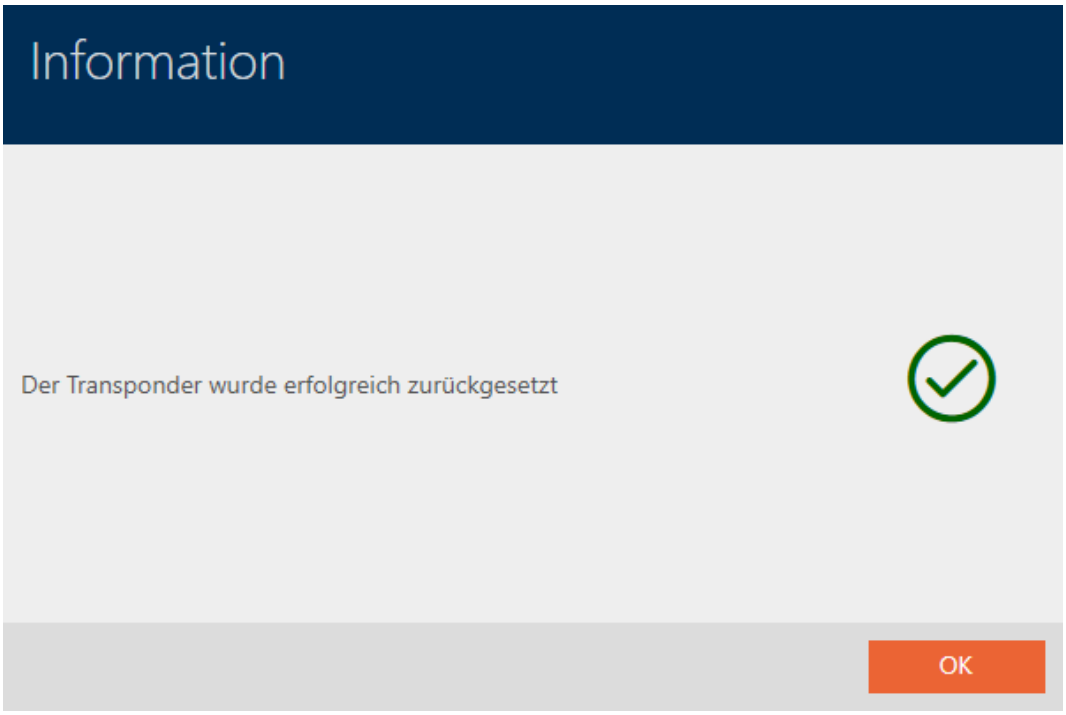
↳ The checkbox for the data record to be reset is activated.



7. Click on the OK button.
8. Follow any further instructions as necessary.
   ↳ Identification medium is being reset.



↳ Identification medium is reset.

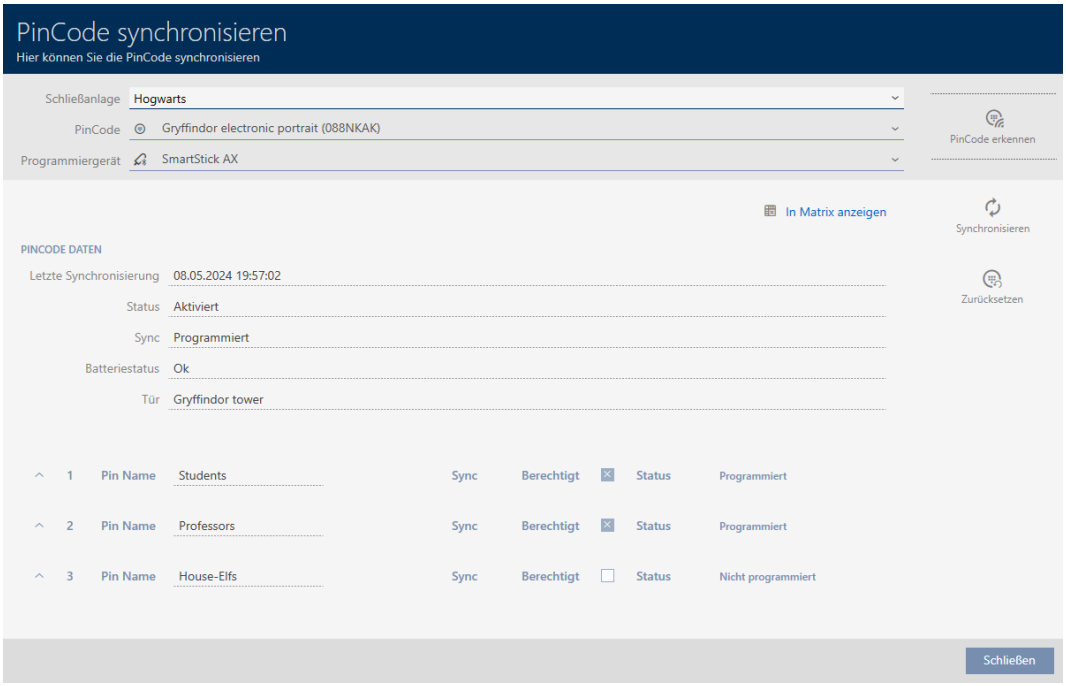


19.6.2 Resetting the PIN code keypad

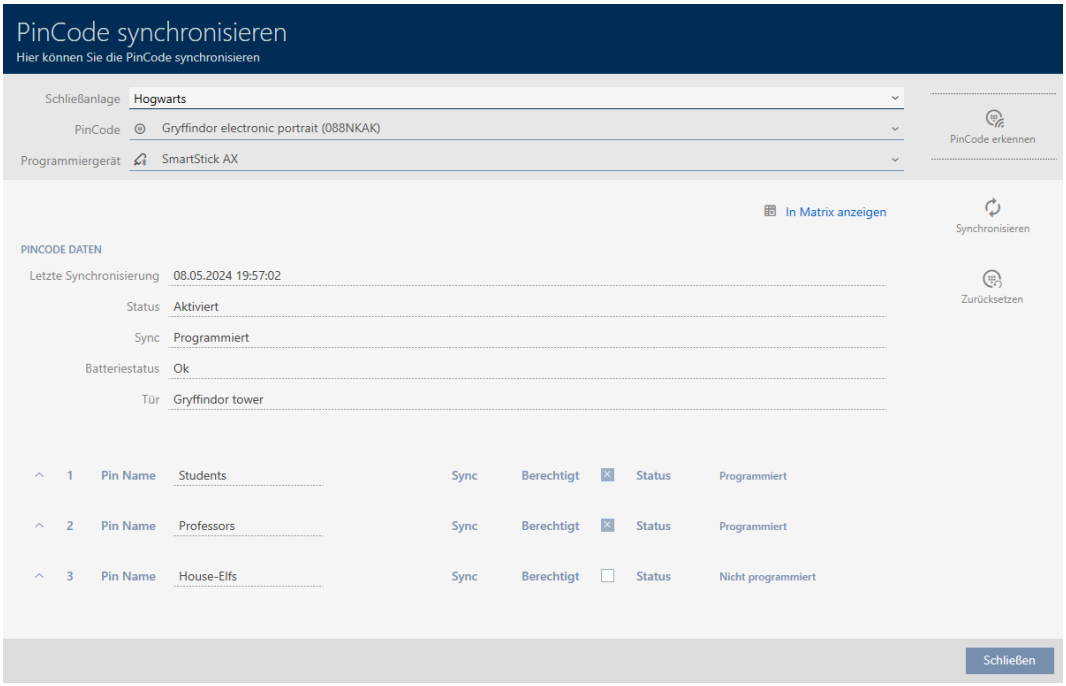
You must reset a component such as a PIN code keypad before it can be used again for an identification medium or another locking system.

- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)
- ✓ AXM Lite open.
- ✓ PIN code list or matrix screen open.

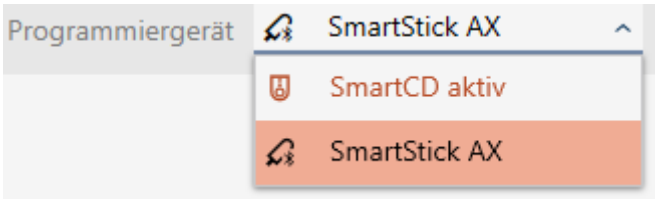
1. Click on the PIN code keypad you wish to reset.
   If the PIN code keypad is not present in your locking system, identify the PIN code keypad (see *Identifying unknown PIN code keypad [▸ 311]* in the AXM manual). Then continue.
   ↳ The PIN code keypad window will open.



2. Click on the Synchronisation button.
   ↳ Synchronise window will open.



3. Select the programming device from the ▼ **Programming device** drop-down menu with which you wish to reset your PIN code keypad.



4. Click on the Reset button .

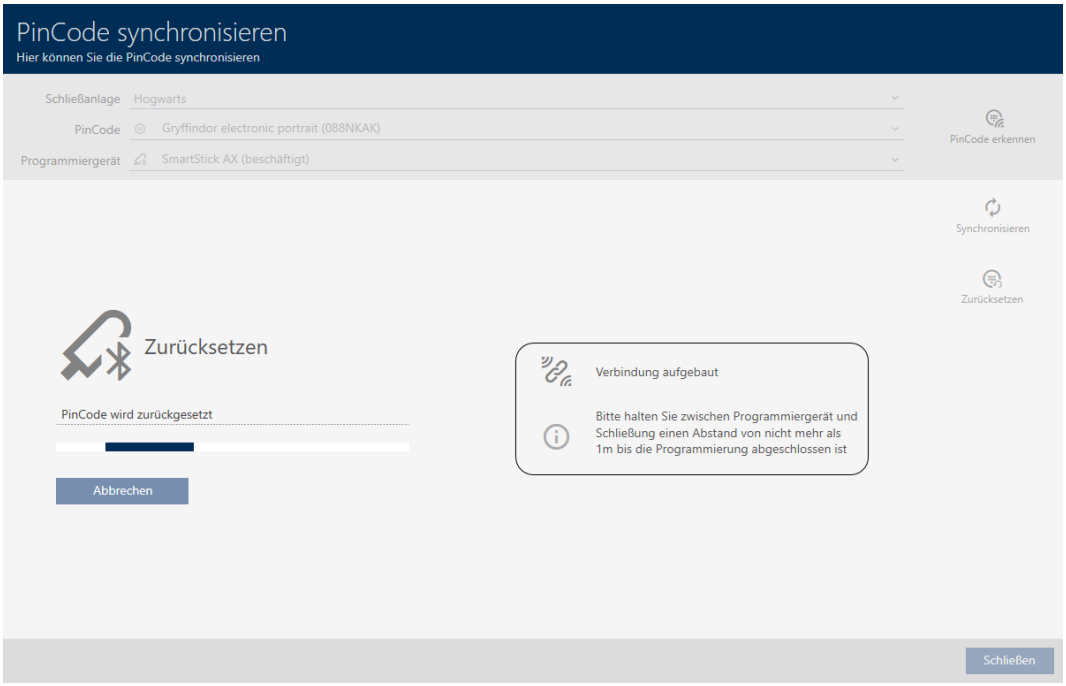
NOTE

Resetting PIN code keypads that do not form part of the project

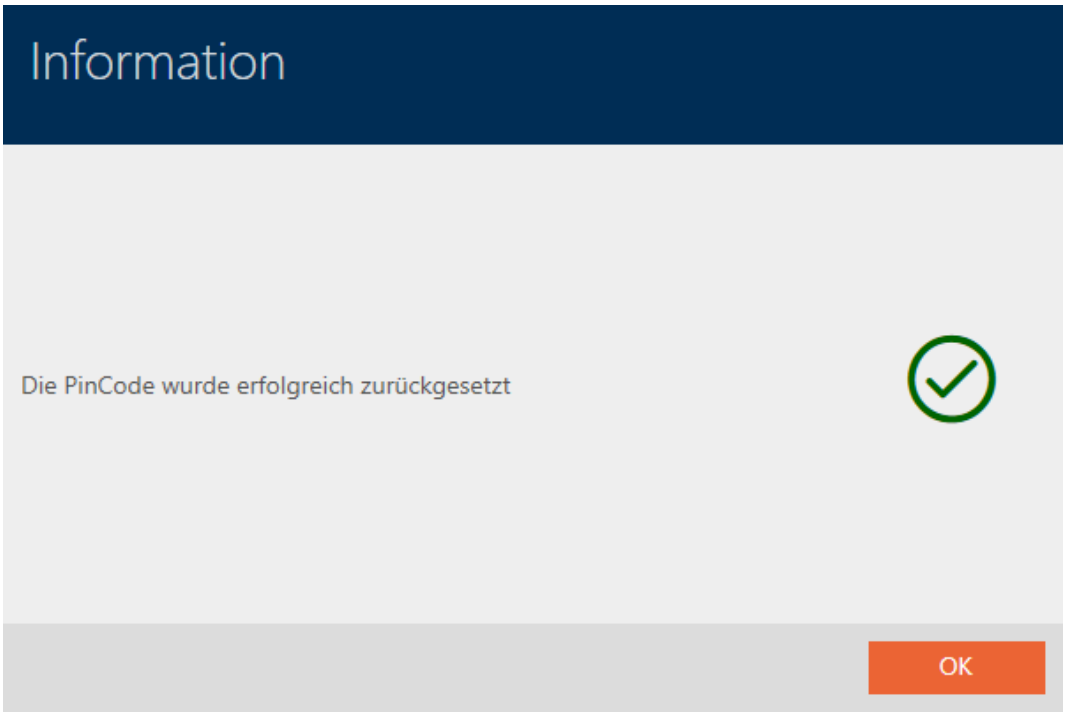
Your AXM Lite can also reset PIN code keypads that were not created in the same project. In this case, however, your AXM Lite does not know the locking system password used.

- In such instances, enter the locking system password when prompted.

5. If necessary, enter the locking system password for the locking system to which this PIN code keypad belongs.
6. Follow any further instructions as necessary.
   ↳ PIN code keypad is reset.



↳ PIN code keypad is reset.



19.7 Viewing connected/supported programming devices

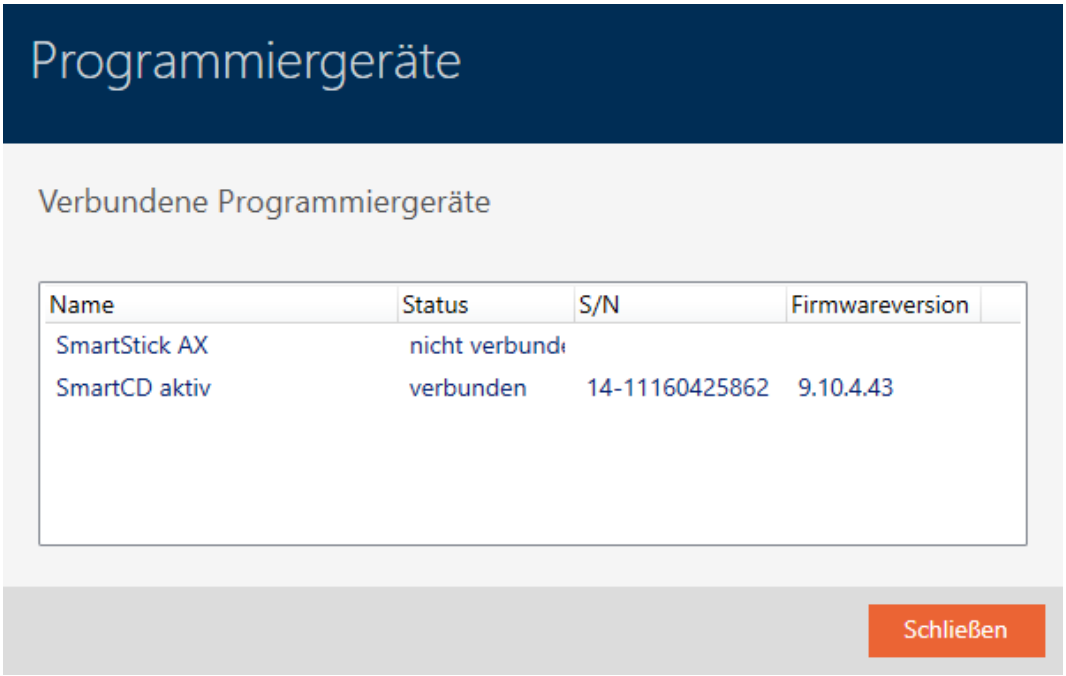
This window can be used to check whether a connected programming device is functional and identified.

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Programming devices entry in the | SETTINGS | group.

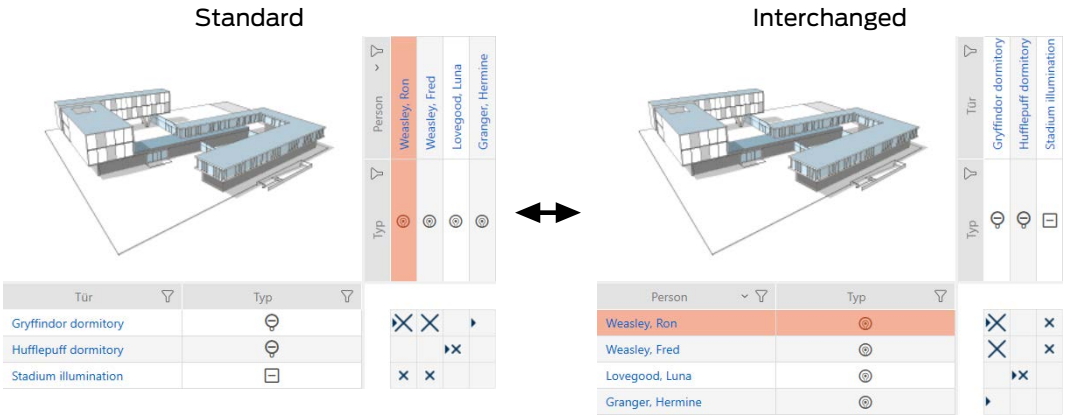
↳ Window with programming devices will open.



This window displays all supported programming devices. Other programming devices will be supported, depending on the edition of the AXM you are using (see *Range of functions for AXM Lite [▸ 16]*). In the status column, you will see if a programming device is connected and recognised by AXM Lite.

20. Your personalised AXM interface

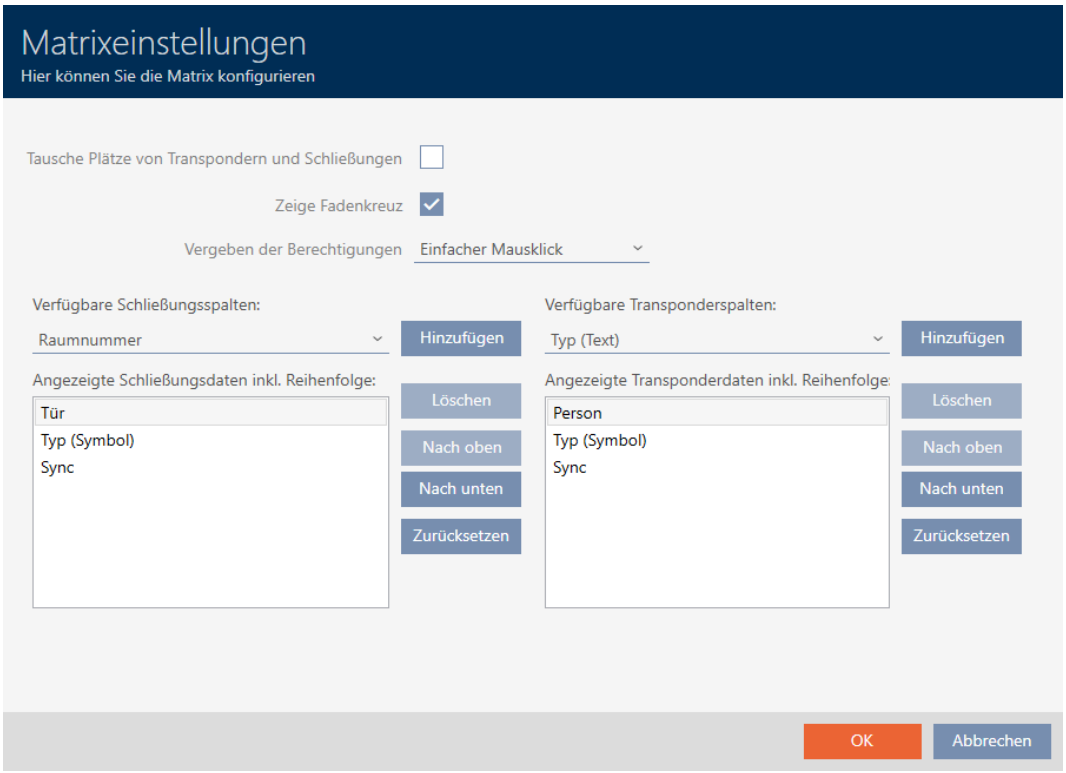
20.1 Interchanging (transposing) doors and persons in the matrix



In the standard view, the doors are displayed as rows and the persons as columns. You can also change this.

✓ Matrix screen open.

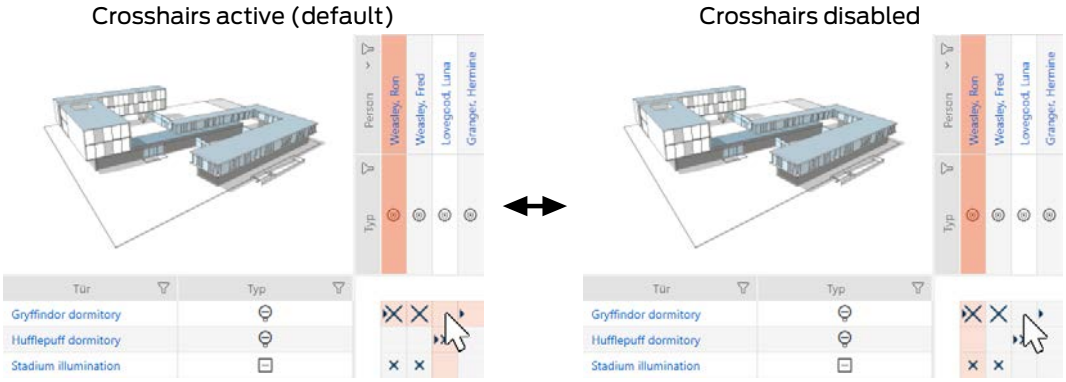
1. Click on the ⚙ Configuration button.
   ↳ The window with the AXM Lite matrix settings will open.



2. Activate the ☑ Swap places for transponders and locks check box.
3. Click on the OK button.
   ↳ The window with the AXM Lite matrix settings closes.

↳ Doors and persons are swapped in the matrix view.

20.2 Select columns and rows in the matrix (enable/disable crosshairs)

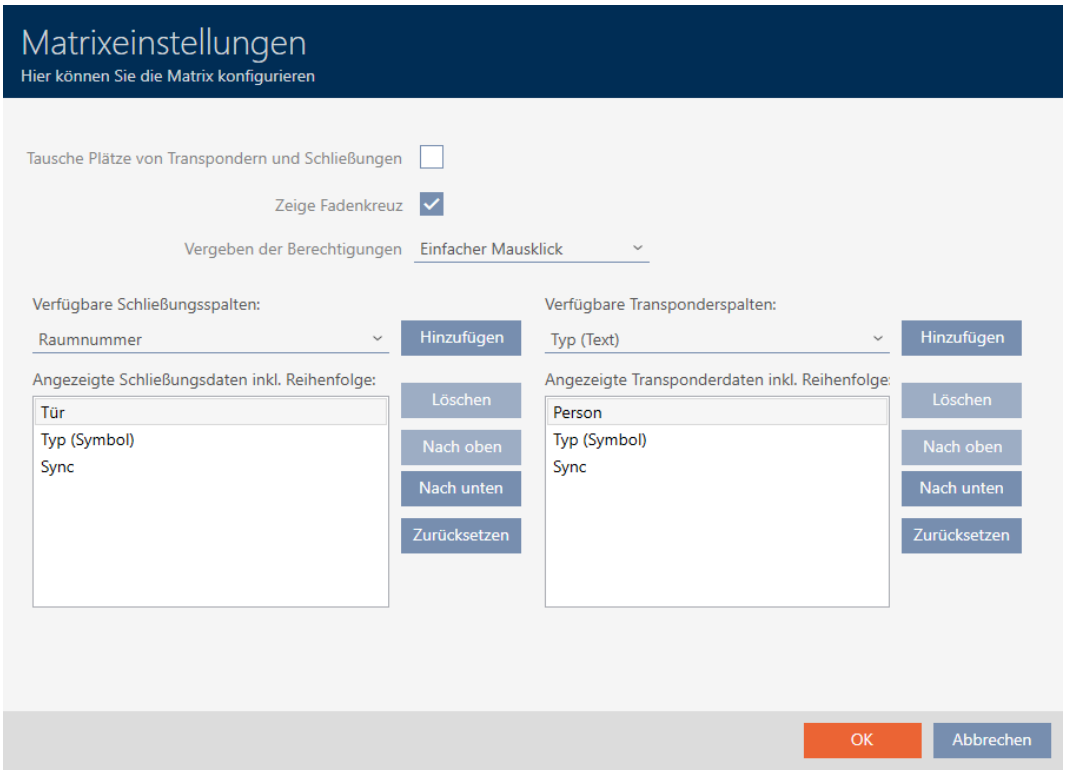


The box over which the mouse pointer is currently positioned belongs to a locking device or to your identification medium. The whole row and the whole column are highlighted in colour in the default setting. This allows you to find the locking device or identification medium you require quickly. This function is called crosshairs.

You can deactivate the crosshairs if you wish. In this case, the column or row to which the selected locking device or identification medium belongs is highlighted whether the mouse pointer is hovering over it or not.

✓ Matrix screen open.

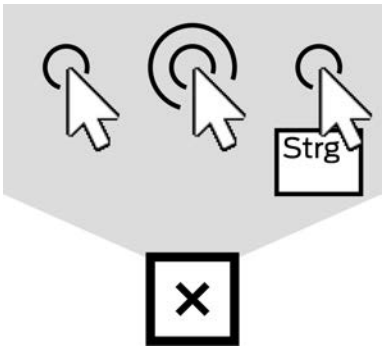
1. Click on the ⚙ Configuration button.
   ↳ The window with the AXM Lite matrix settings will open.



2. Activate or deactivate the ☑ Show crosshair check box.
3. Click on the OK button.
   ↳ The window with the AXM Lite matrix settings closes.

↳ Crosshairs are no longer displayed.

20.3 Click to change authorisations

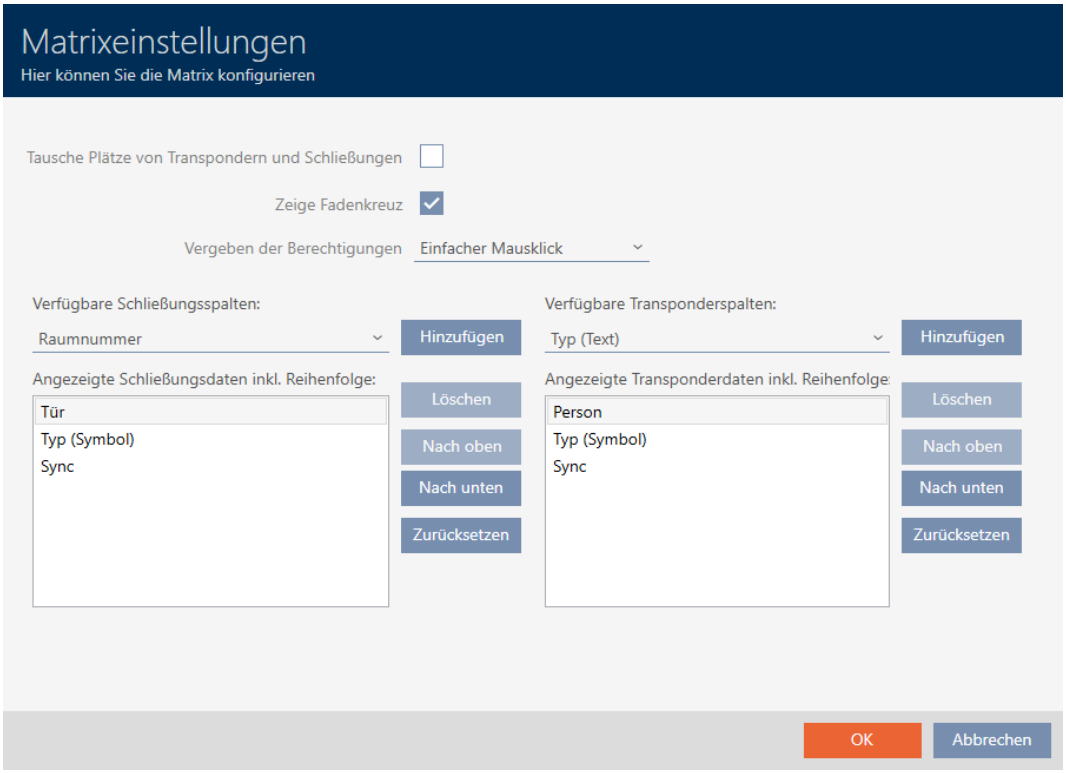


There are three ways to set an individual authorisation by clicking on the matrix:

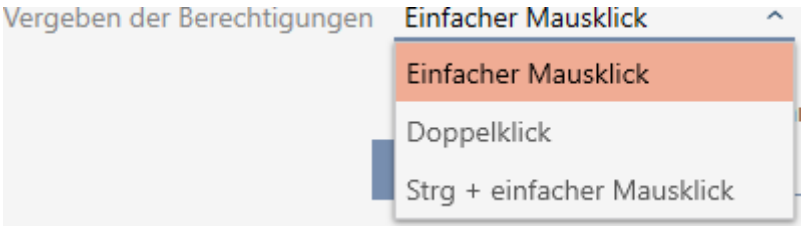
- Single click of the mouse (Standard)
- Double click
- Ctrl + single click

✓ Matrix screen open.

1. Click on the ⚙ Configuration button.
   ↳ The window with the AXM Lite matrix settings will open.



2. Choose between the "Single click of the mouse", "Double click" or "Ctrl + single click" entries from the ▼ **Issuing of authorisations** drop-down menu.



3. Click on the OK button.
   ↳ The window with the AXM Lite matrix settings closes.

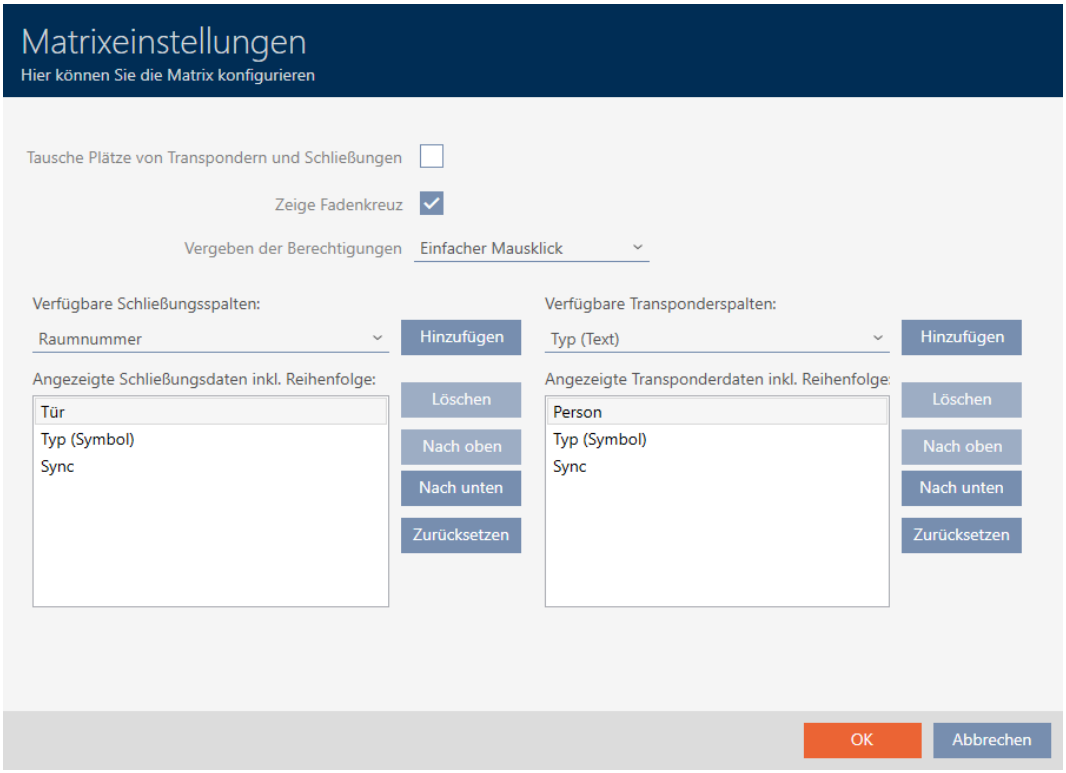
↳ Click for authorisations has been changed.

20.4 Hiding deactivated and defective identification media

This is where you have the option of “clearing up” your matrix and hiding all defective or deactivated identification media. You can recognise such identification media by the symbol and by the fact that they can no longer be synchronised.

✓ Matrix screen open.

1. Click on the Configuration button.
   ↳ The window with the AXM Lite matrix settings will open.

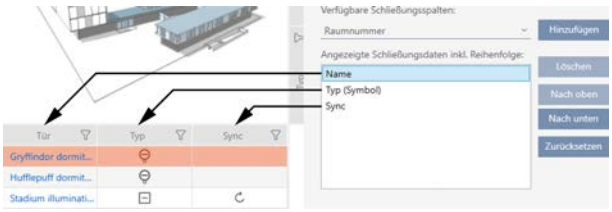


2. Disable the ☐ Show deactivated transponders checkbox.
3. Click on the OK button.
   ↳ The window with the AXM Lite matrix settings closes.

↳ Deactivated and defective identification media are now hidden.

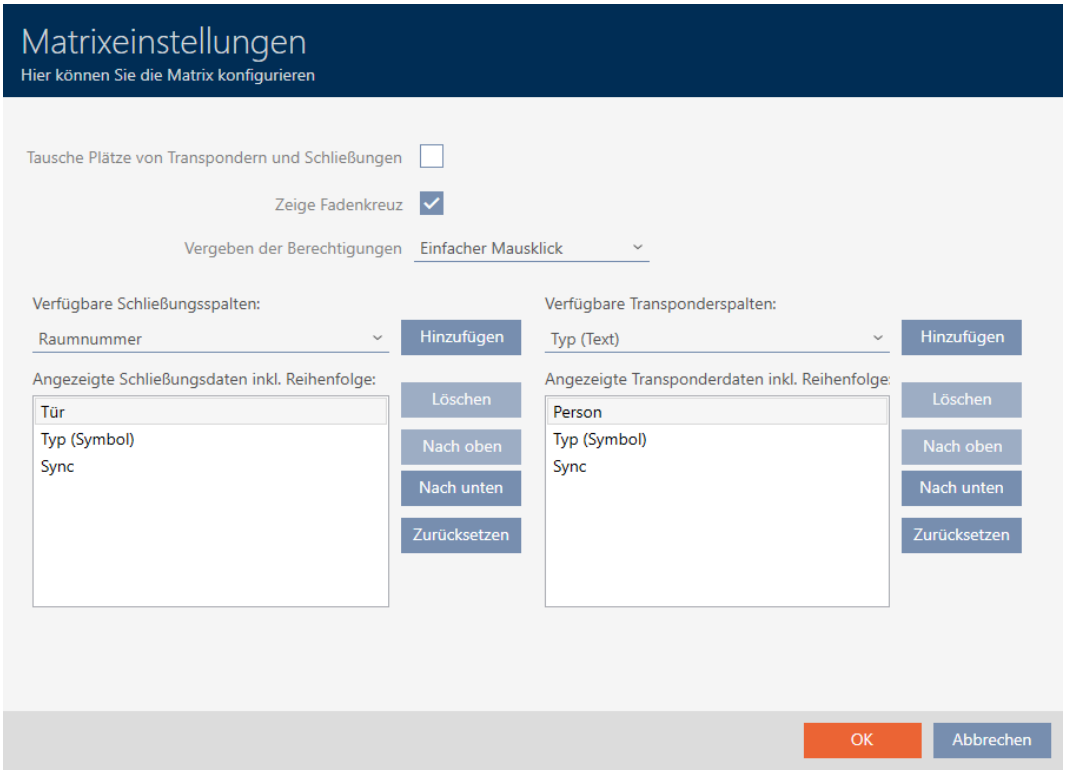
20.5 Showing or hiding rows/columns in the matrix

The following description applies to the columns displayed for locking devices. The identification media rows can be edited in the same way.

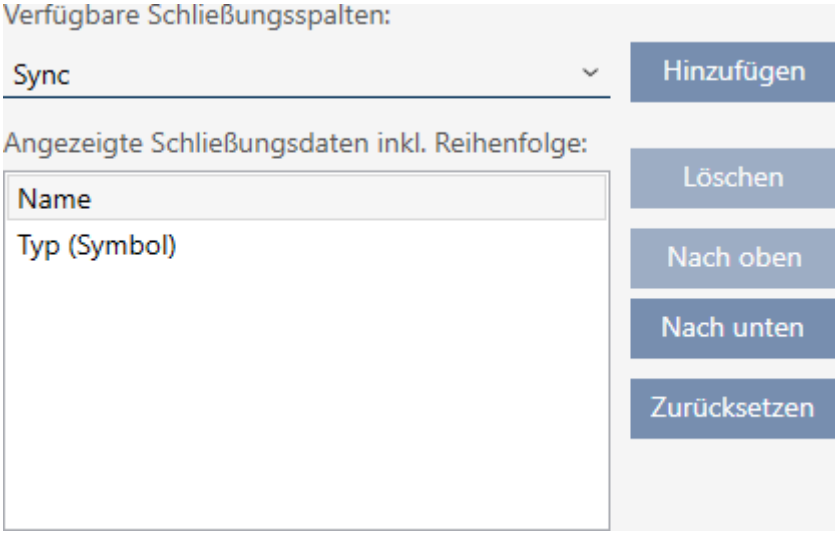


✓ Matrix screen open.

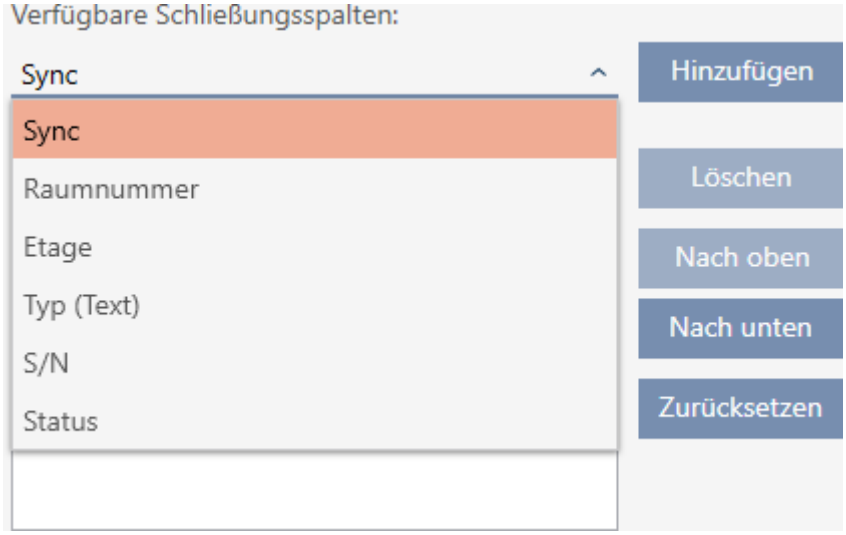
1. Click on the ⚙ Configuration button.
   ↳ The window with the AXM Lite matrix settings will open.



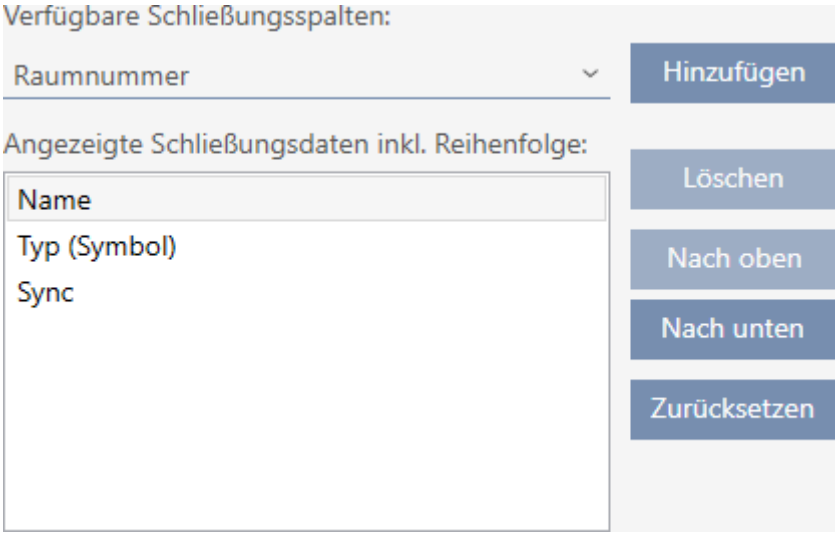
↳ The locking device columns currently displayed are listed.



2. Select the columns to be displayed in the matrix from the ▼ **Available lock columns:**drop-down menu.



3. Add and delete columns with the Add or Delete buttons.



4. Use the Up or Down buttons to change the order.
5. You can also use the Reset button to restore the default display.
6. Click on the OK button.
   ↳ The window with the AXM Lite matrix settings closes.

↳ Columns are changed as required.

20.6 Reading access list/physical access list during synchronisation

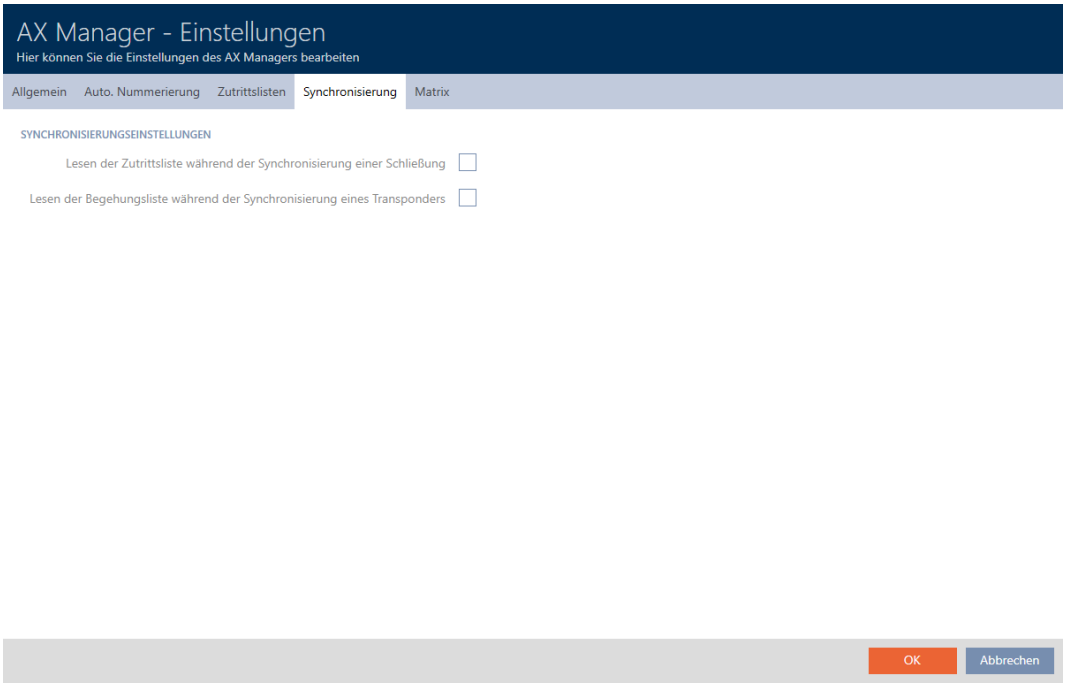
✓ AXM Lite open.

1. Click the orange AXM button ☰ AXM.
   ↳ AXM bar opens.

2. Select the AX Manager settings entry in the | SETTINGS | group.

↳ The AXM bar will close.
↳ The window with the AXM Lite settings will open.

3. Go to the [Synchronisation] tab.



4. Activate the ☑ Reading the access list during synchronisation of a lock or ☑ Reading the personal audit trail during transponder synchronisation checkboxes if required.

5. Click on the OK button.
   ↳ The window with the AXM Lite settings closes.

↳ The access list or physical access list will also be imported during synchronisation in the future.

20.7 Limiting the number of access list entries in the database

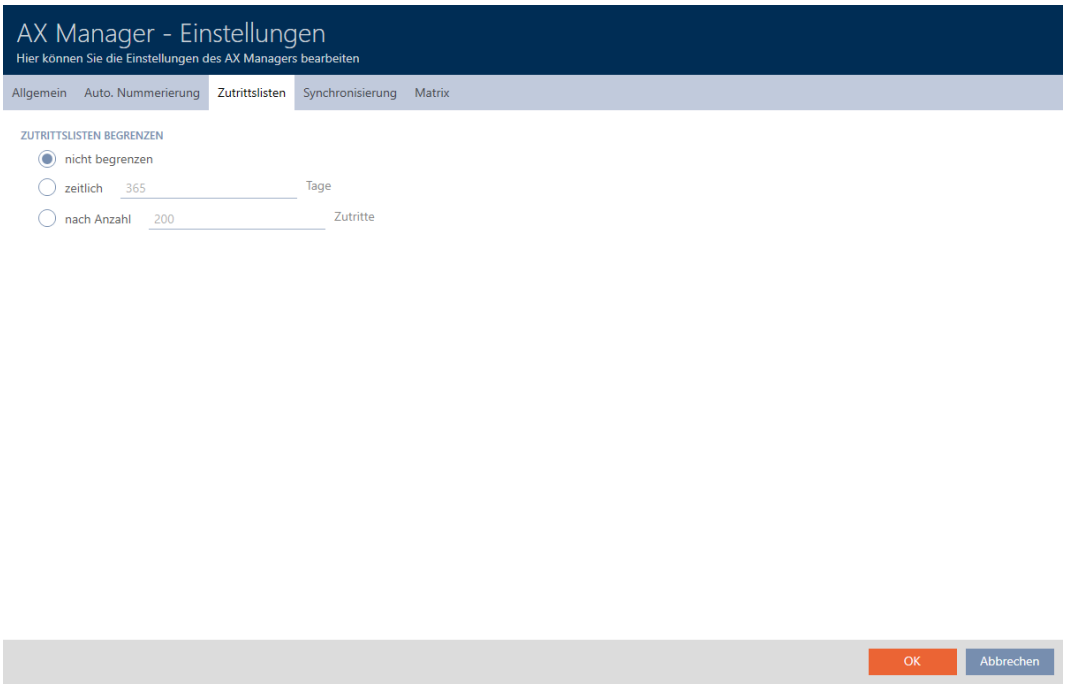
✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the AX Manager settings entry in the | SETTINGS | group.

   ↳ The AXM bar will close.
   ↳ The window with the AXM Lite settings will open.

3. Go to the [Access lists] tab.



4. Select one of the three options: ◉ Unlimited, ◉ temporally (max. 2000 days) or ◉ by number (max. 10,000 entries).
5. Click on the OK button.
   ↳ The window with the AXM Lite settings closes.

↳ Access list restriction is configured.

20.8 Pinning tabs

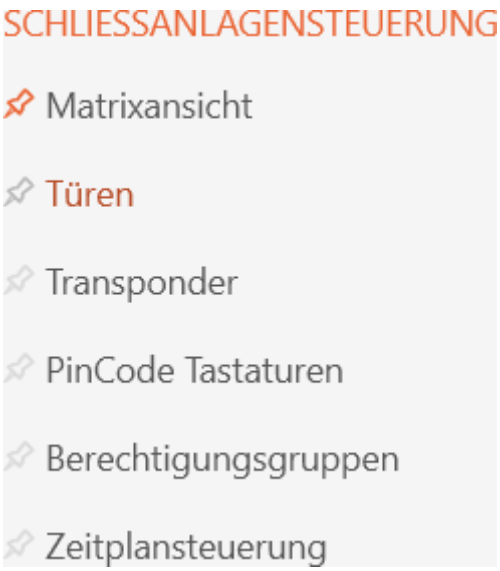
Experience has shown that you need some entries from the AXM bar more frequently.

You will see a grey pushpin next to some entries. You can use this pushpin to pin the entry in question and open it automatically the next time you start AXM Lite.

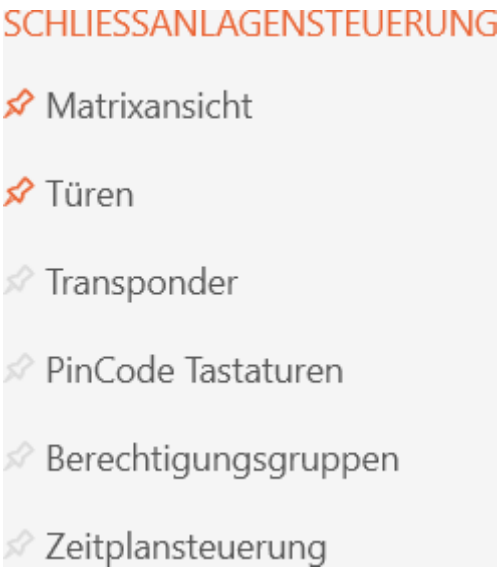
Start (Locks entry not pinned)	Start (Locks entry pinned)

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.
2. Click on the grey pushpin next to the entry you wish to pin.



↳ Pushpin turns orange.



↳ The pinned entry is automatically opened the next time the AXM Lite is started.

20.9 Changing automatic numbering

AXM Lite takes over the numbering of personnel and doors for you by default.

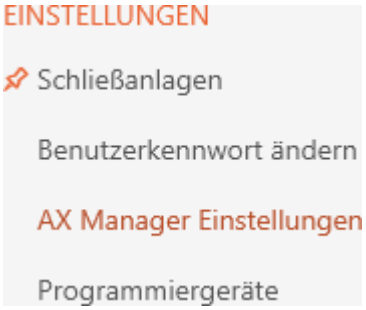
Personnel numbers	Door numbers
PN-1	**DC-**00001
PN-2	**DC-**00002
PN-X	**DC-**XXXXX

The abbreviations *PN-* (personnel number) and *DC-* (door code) can be changed in the AXM Lite properties:

✓ AXM Lite open.

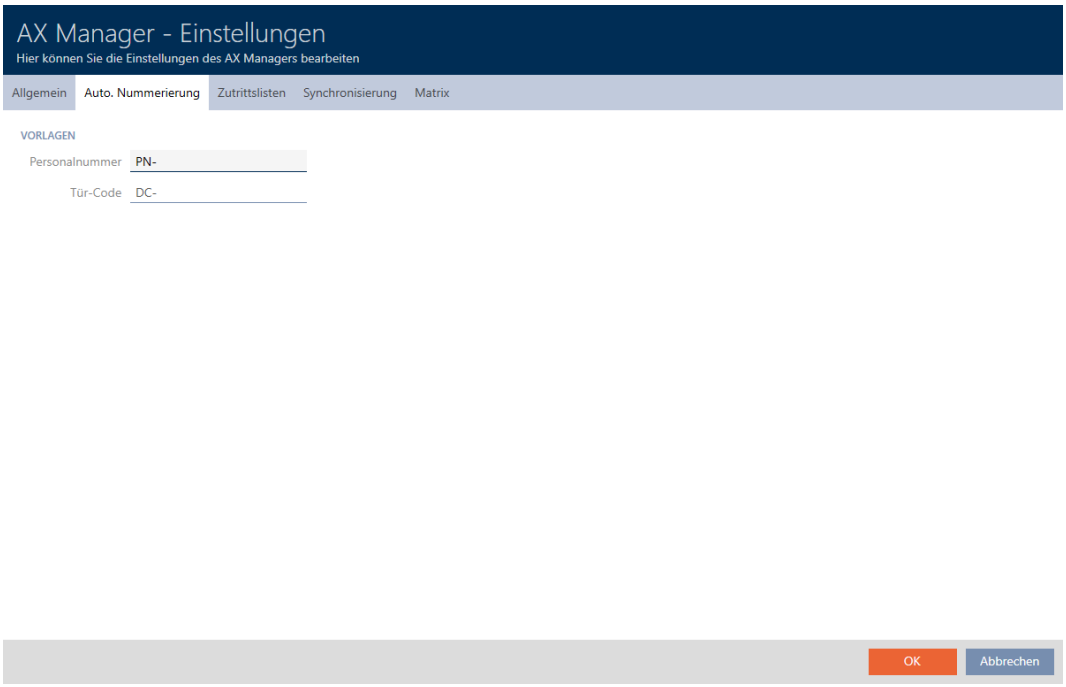
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the AX Manager settings entry in the | SETTINGS | group.



   ↳ The AXM bar will close.
   ↳ The window with the AXM Lite settings will open.

3. Go to the [Auto. Numbering] tab.



4. Enter the required abbreviations in the *Personnel number* or *Door code* fields.
5. Click on the OK button.
   ↳ The window with the AXM Lite settings closes.

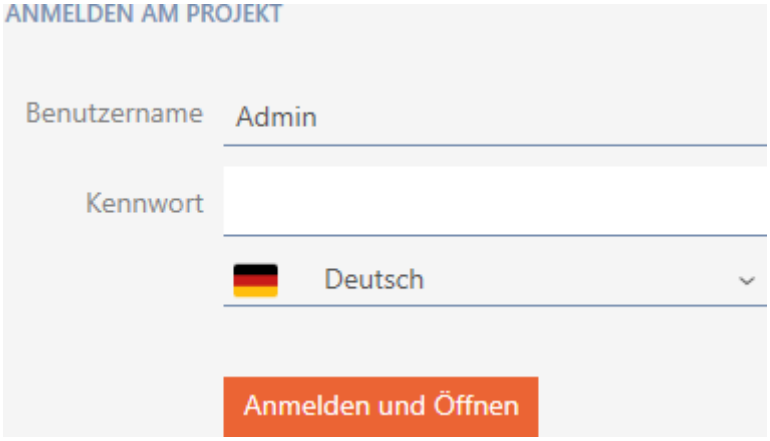
↳ Personnel numbers and door codes will be generated with the modified abbreviation in the future.

↳ Existing personnel numbers or door codes will remain unchanged.

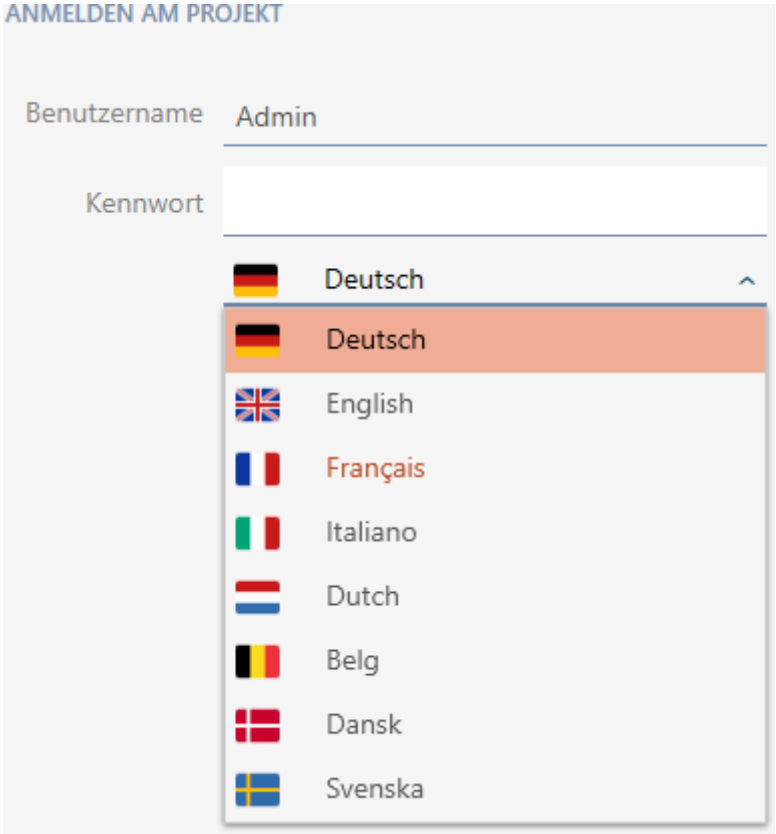
20.10 Changing the language

The AXM Lite is available in different languages. All available languages are automatically installed during installation.

When you launch the program for the first time, you will see a special window where you can set up your first project. The normal login window will then appear:



Select your preferred language in the *Password* field.



20.11 Preventing generated reports from opening automatically

By default, your reports created in AXM Lite open immediately so that you can read them.

However, this can disrupt your workflow in the case of many reports. This is why you can set whether reports should be opened automatically or not:

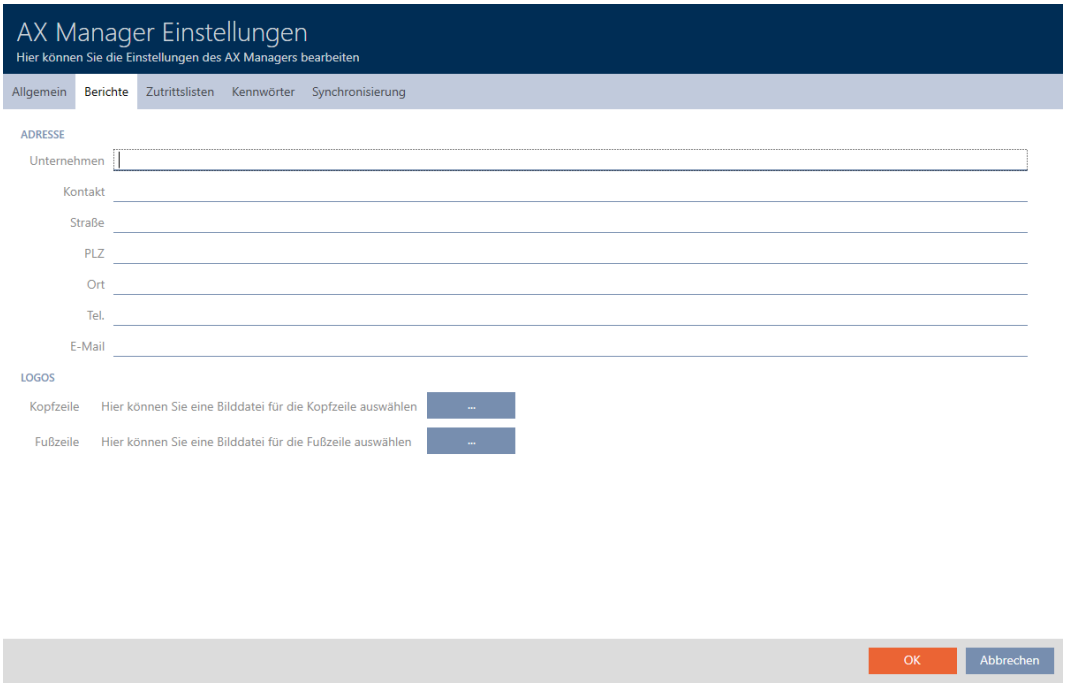
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

2. Select the AX Manager settings entry in the | SETTINGS | group.

   ↳ The AXM bar will close.
   ↳ The "AX Manager settings" window will open.

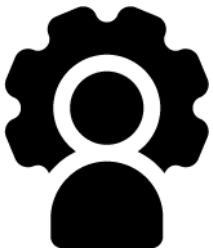
3. Change to the tab [Reports].



4. Disable the ☐ Open PDF documents after saving checkbox.
5. Click on the OK button.
   ↳ "AX Manager settings" window closes.

↳ In future, reports will now no longer open automatically after saving.

21. Administrative tasks



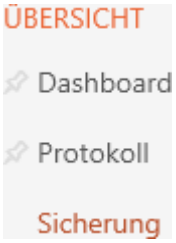
21.1 Creating a backup

Your database and thus your workload can be quickly restored if a backup is copied on a regular basis.

You can easily create the backup in AXM Lite itself:

On the login screen (Project backup button):

Alternatively: in the expandable AXM bar (Project backup button):

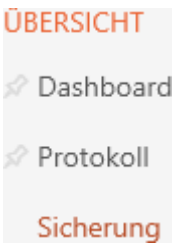


This section explains how to back up the database using the expandable AXM bar.

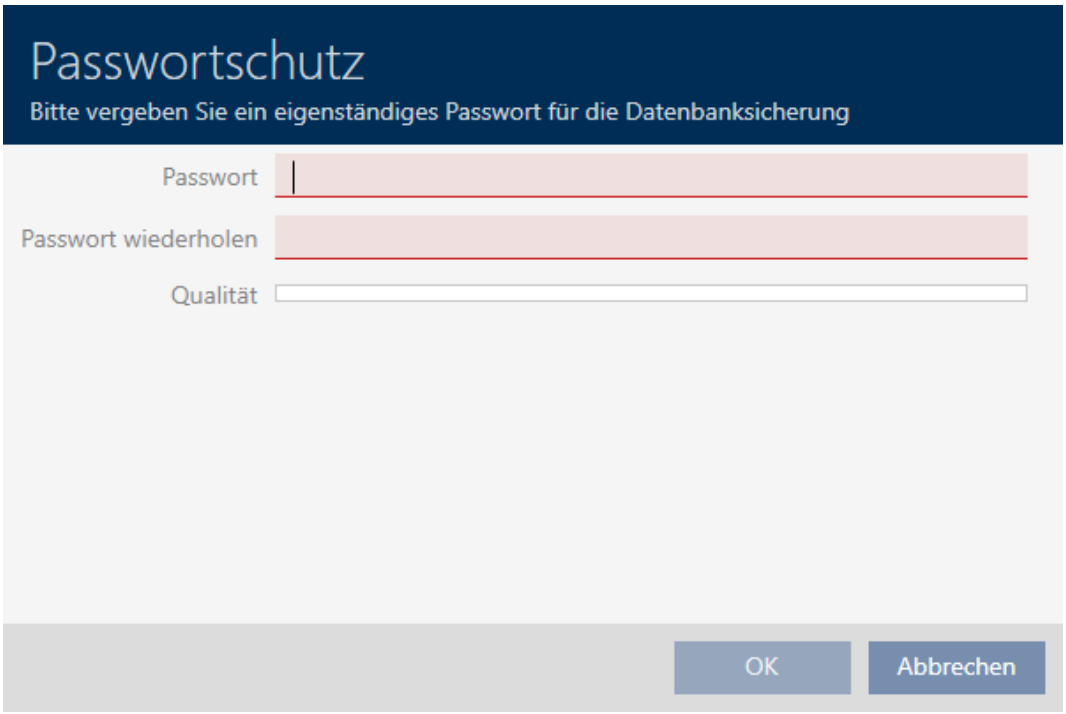
✓ AXM Lite open.

1. Click on the orange AXM icon AXM.
   ↳ AXM bar opens.

2. Click on the Project backup entry in the | OVERVIEW | group.

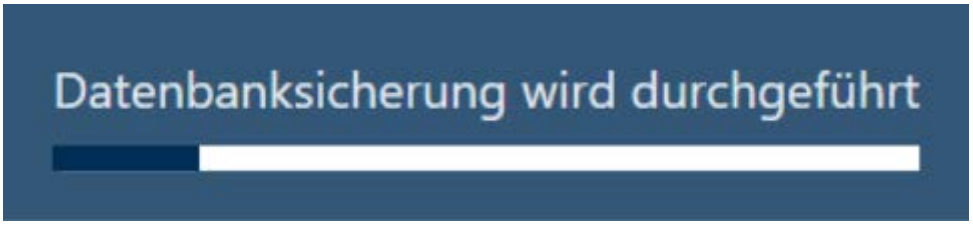


↳ The AXM bar will close.
↳ The window for assigning passwords will open.



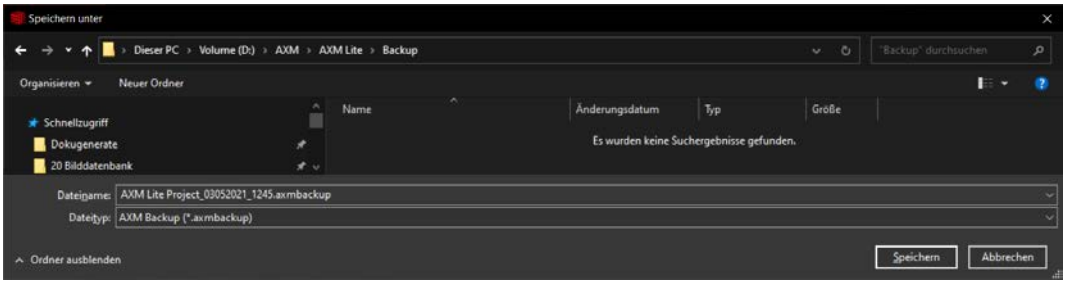
3. Enter a password in the *Password* field to protect this backup.
   ↳ A coloured bar shows you how secure your password is.

4. Repeat the entered password in the *Repeat password* field.
5. Click on the OK button.
   ↳ The window for assigning passwords closes.
   ↳ Backup is being created.



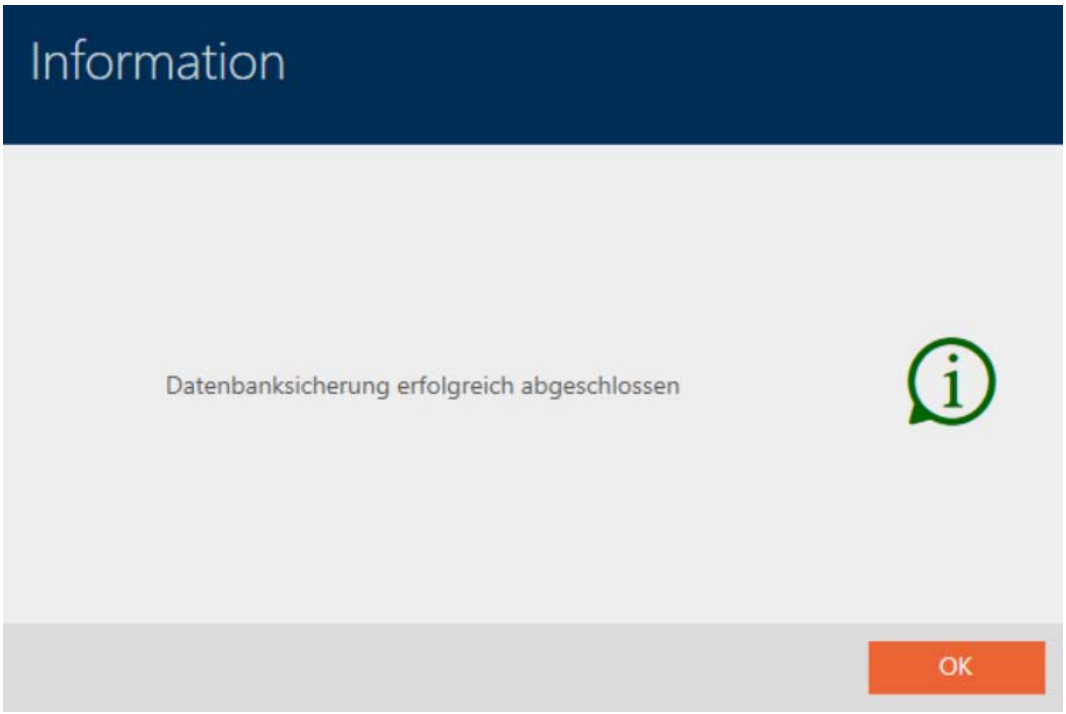
↳ The Explorer window will open.

6. Save the backup file (extension: .axmbackup) in a file directory of your choice.

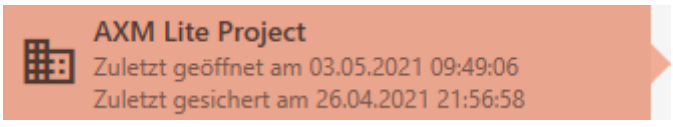


↳ Explorer window closes.

↳ Backup is complete.



You can also see when you last created a backup on the AXM Lite login screen:



21.2 Restoring the backup

If you restore a backup, restore the database to a previously backed-up state.

NOTE

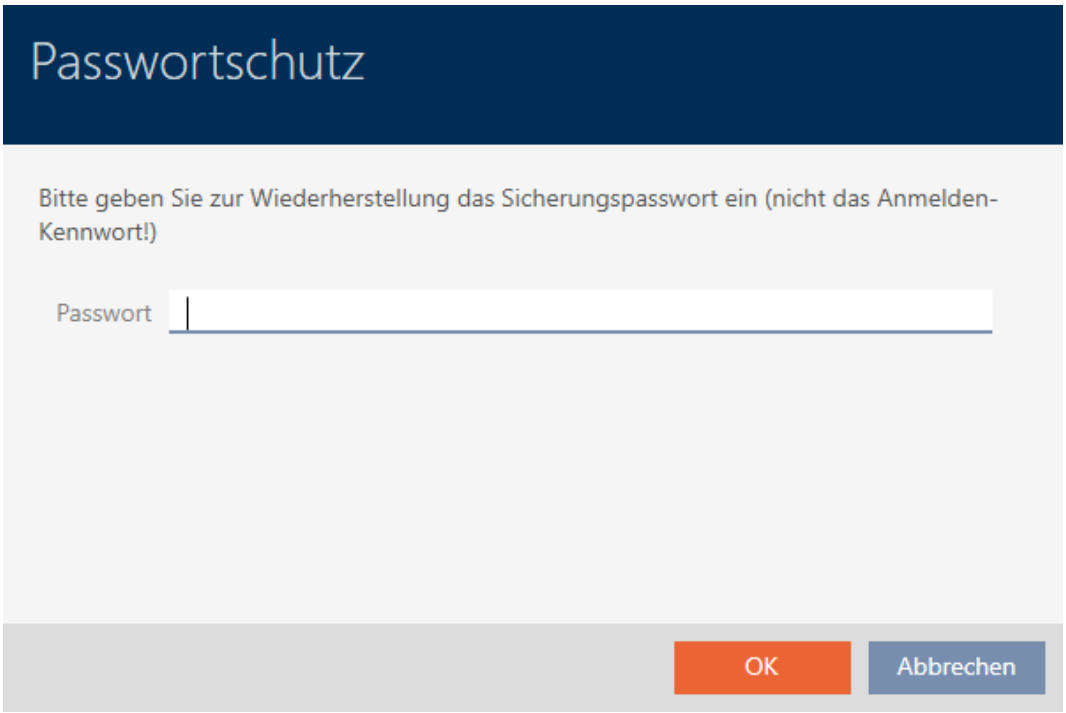
Backup has no influence on locking devices

The restore only applies to the database. It has no effect on existing identification media and locking devices.

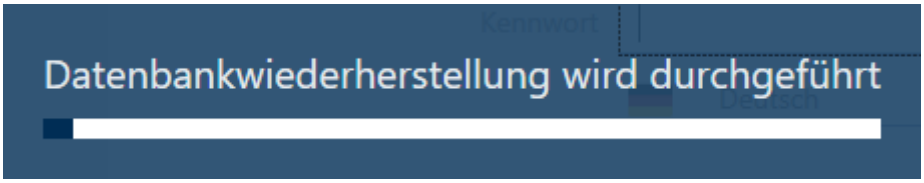
- Synchronise identification media and transponders if necessary (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*).

✓ Backup available (see *Creating a backup [▸ 336]*).

1. Click on the Restore. button on the login screen.
   ↳ The Explorer window will open.
2. Go to your backup.
3. Click on the Open button.
   ↳ Explorer window closes.
   ↳ Password prompt window will open.

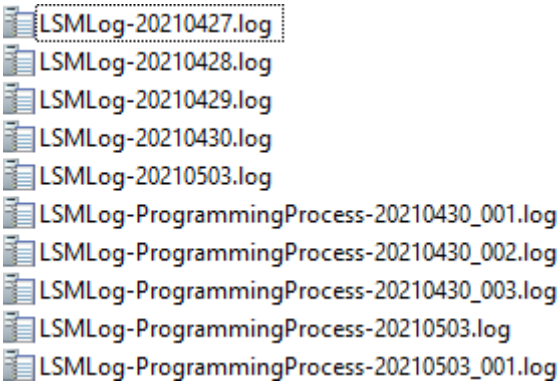


4. Enter the password you entered while creating the backup in the *Password* field.
5. Click on the OK button.
   ↳ Password prompt window closes.
   ↳ The database is restored.



21.3 Exporting error logs

Error logs help to resolve support cases more quickly and pinpoint any problems more quickly.



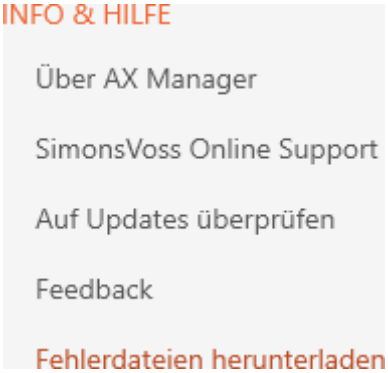
You can export error logs either on the login screen (Error Files button) or in the AXM bar (Download error files button).

The following description explains how to export the error logs using the AXM bar:

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Download error files entry in the | INFO & HELP | group.



↳ The Explorer window will open.

3. Save the error log (file extension: .zip) to a file directory of your choice.

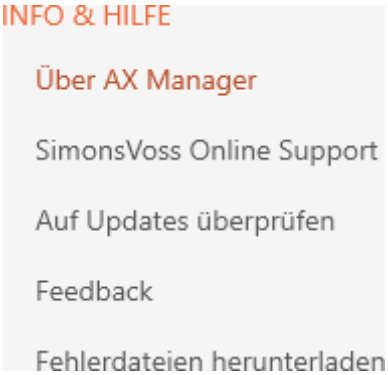
↳ The error log is now exported.

21.4 Displaying version number and licence key for the AXM installed

✓ AXM Lite open.

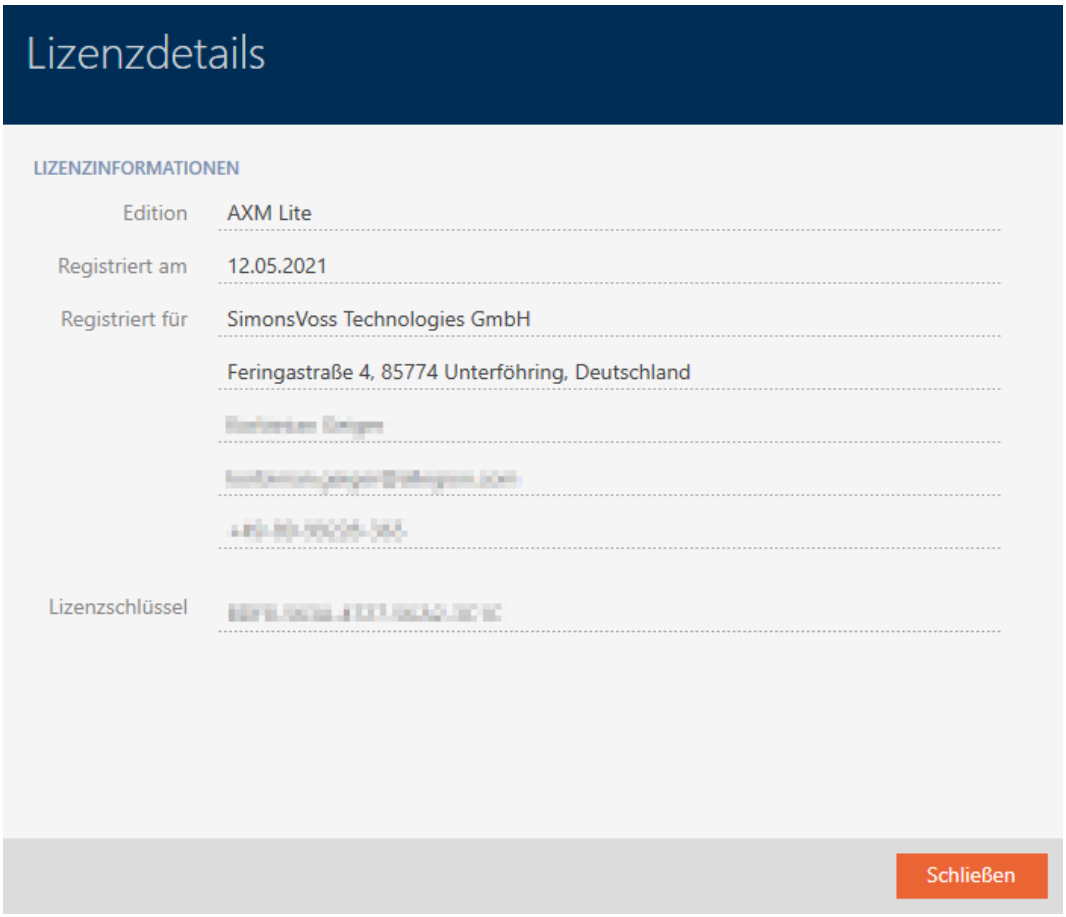
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the About AX Manager entry in the | INFO & HELP | group.



↳ The info window about AXM Lite will open.

3. Click on the Licence details button.
   ↳ The info window about AXM Lite closes.
   ↳ The licence info window will open.



4. Click on the Close button.
   ↳ The licence info window closes.

You can also register your AXM Lite here (see *Registration [▸ 31]*).

21.5 User management

21.5.1 Changing the user password

Your user password must meet the following requirements:

- Be at least 8 characters long
- Contain upper and lower case letters

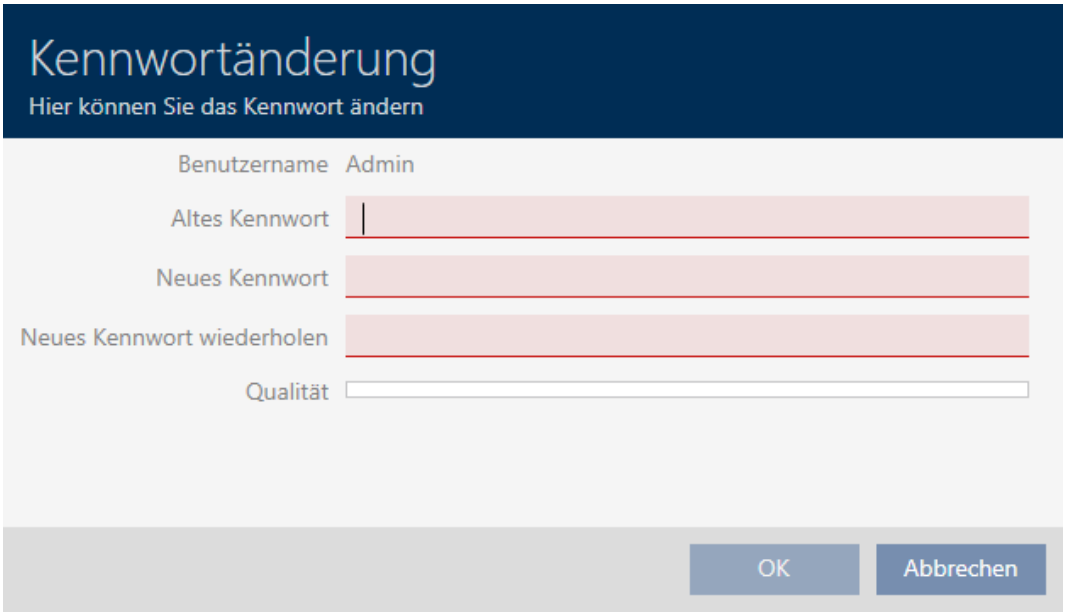
You can achieve even greater security if you also include numbers (1234...) and special characters (!$%&?...).

✓ AXM Lite open.

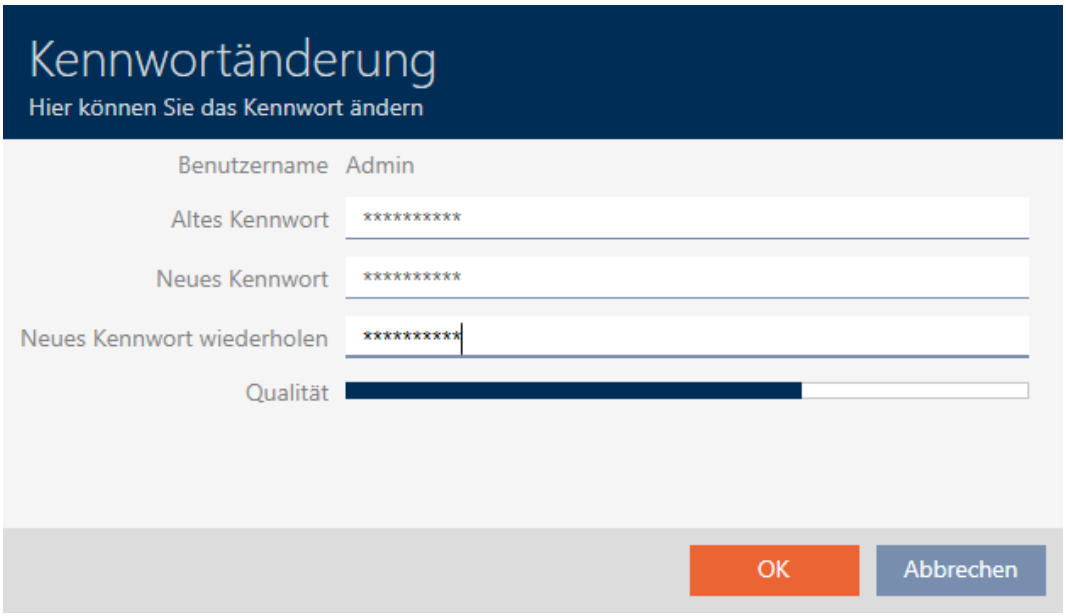
1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Change user password entry in the | SETTINGS | group.

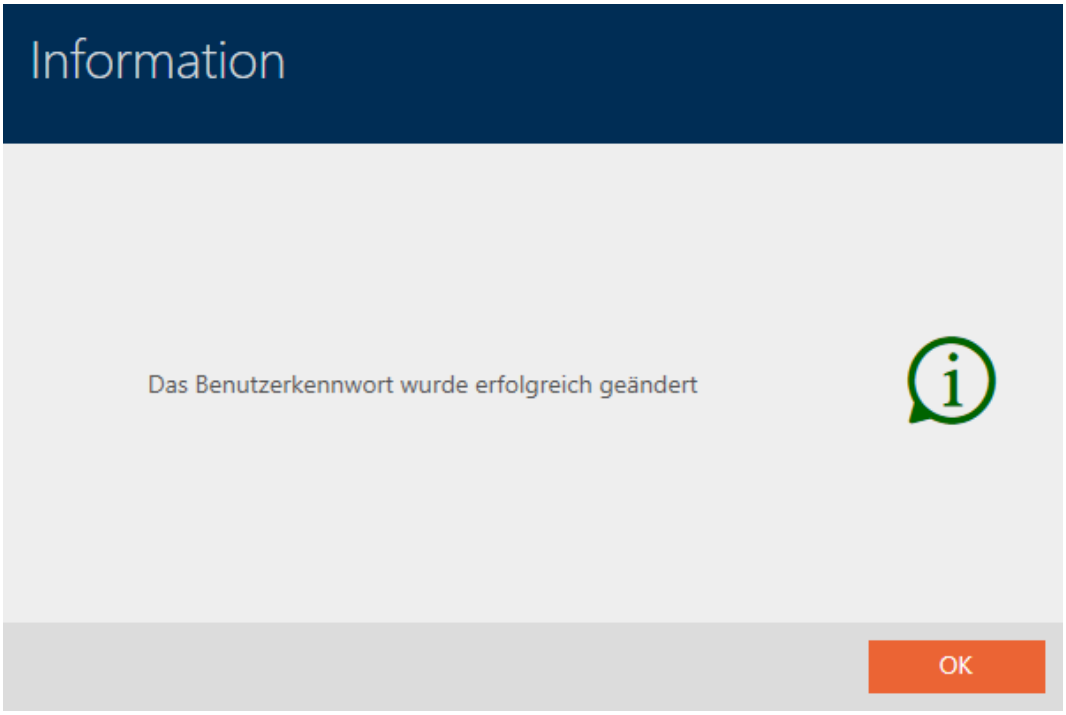
   ↳ The window for changing the user password will open.



3. Enter your current user password in the *Old password* field.
4. Enter your new password in the *New password* and *Repeat new password* fields.
   ↳ A coloured bar shows you how secure your password is.

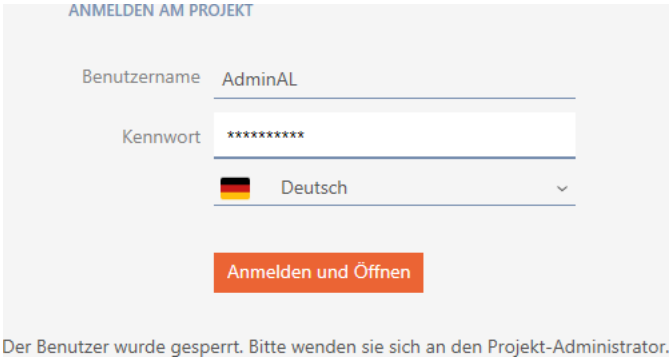


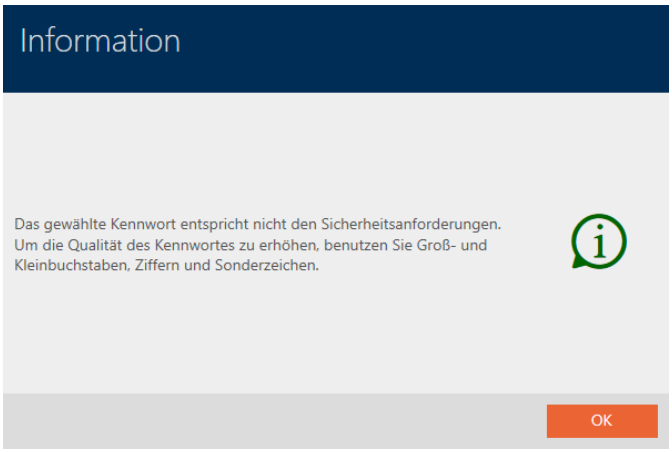
↳ The user password has now changed.



21.5.2 Increase password security

Passwords are a key component in your security concept. You can increase security using various settings:

☑ Password must be changed regularly	After the configured change interval has expired, the user must assign a new password. You can set the change interval yourself using *Prescribed change interval (in days)*.
☑ Lock the user after 3 incorrect password attempts	The new password must not be the same as any of the last ten passwords.
☑ Use password history of the last 10 passwords	If a user has entered the password incorrectly three times, they will no longer be able to log in until they have been unlocked.  You as *Admin* must delete and create a new *AdminAL* user in AXM Lite.

☑ High password security	AXM Lite automatically rejects trivial passwords such as “12345678”. 
☑ Lock AXM when idle after (in minutes)	If your AXM Lite does not detect any actions within the configured idle time, your AXM Lite is automatically blocked.

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the AX Manager settings entry in the | SETTINGS | group.

   ↳ The AXM bar will close.
   ↳ The window with the AXM Lite settings will open.
3. Go to the Passwords tab.
4. Select the required checkboxes.

5. Click on the OK button.
   ↳ The window with the AXM Lite settings closes.

↳ New password requirements are active.

22. Statistics and logs

22.1 Displaying and exporting a locking device's access list

The ZK function (access control) enables your locking devices to log which identification media have been activated (see *Have accesses logged by locking device (access list) [▸ 228]*). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation [▸ 327]* and *Synchronising the locking device (including reading access list) [▸ 291]*).

You can view and export the access list in the database.

NOTE

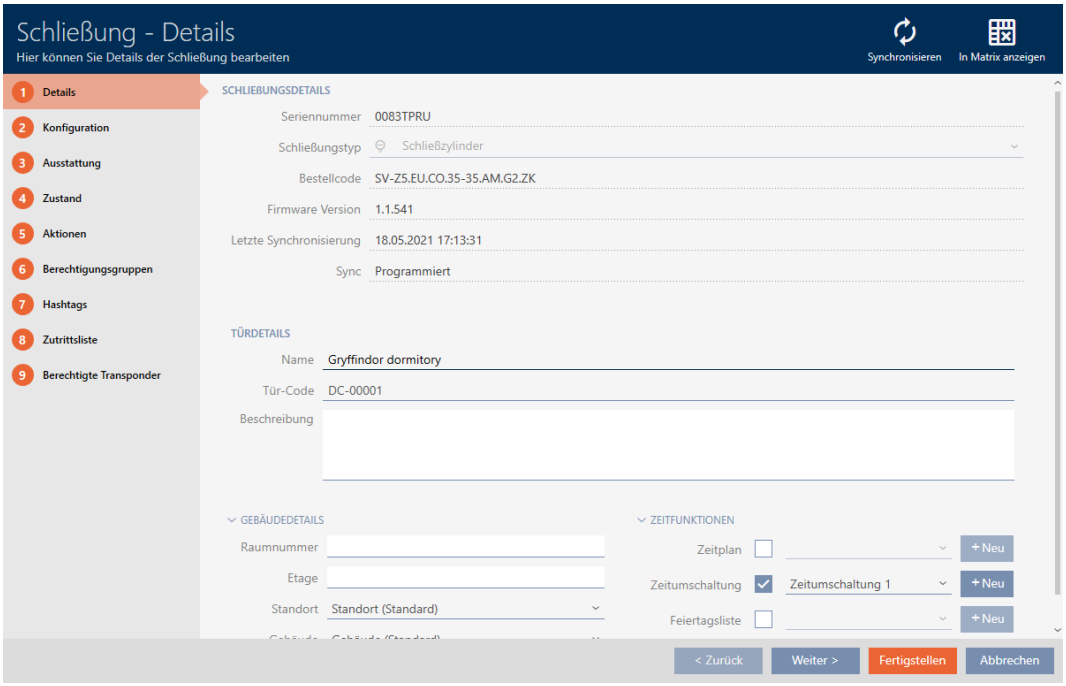
Displayed status corresponds to the last synchronisation

AXM Lite displays the status stored in the database at this point.

✓ AXM Lite open.

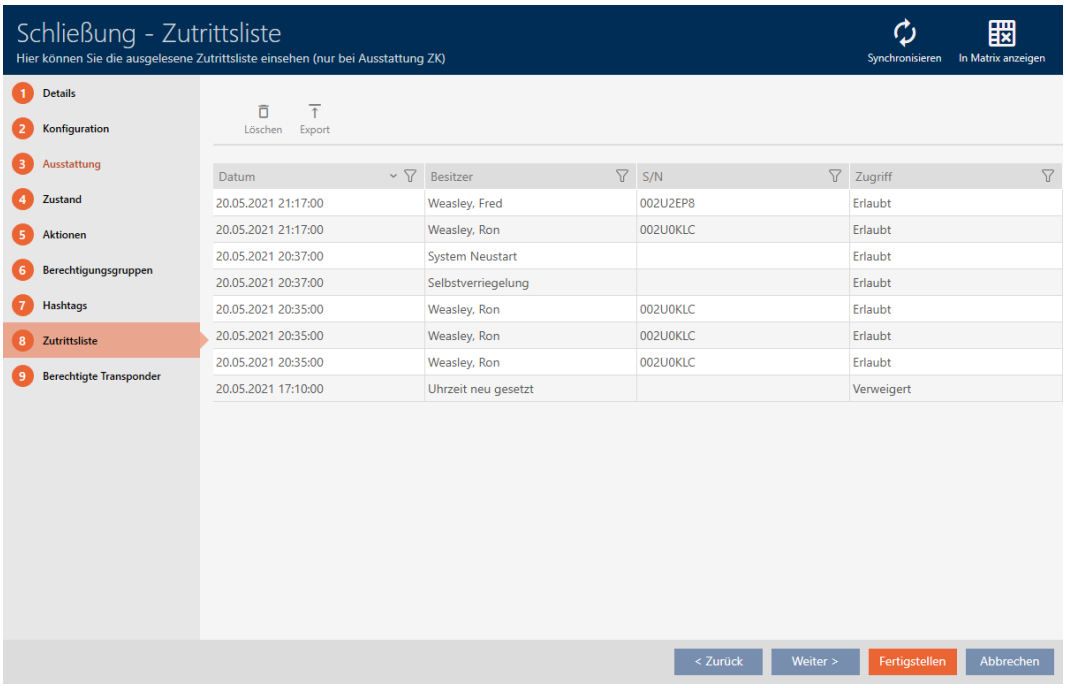
✓ Locking device synchronised at least once.

1. Click on the locking device whose access list you wish to display.
   ↳ The locking device window will open.



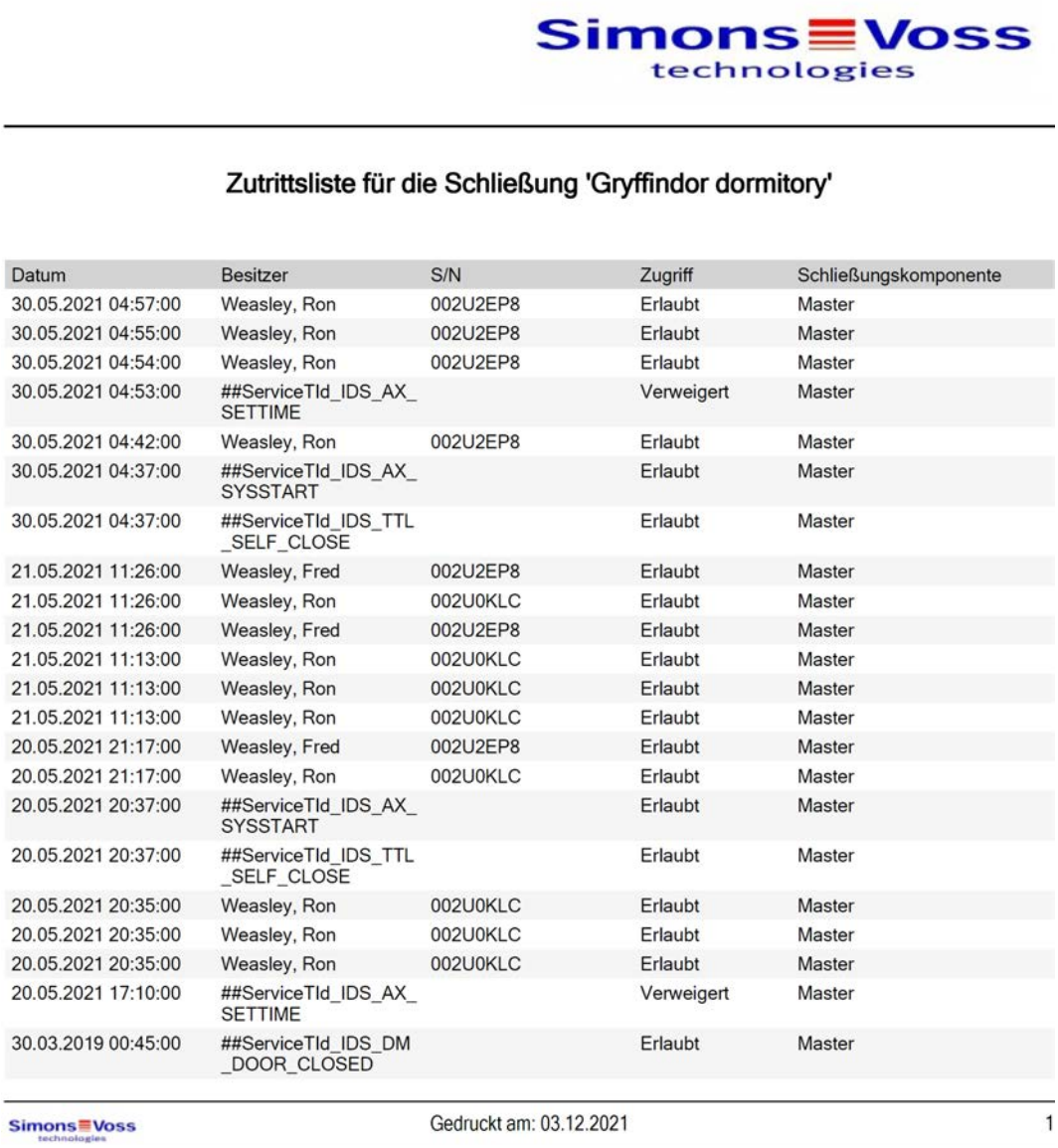
2. Click on the Access list tab.

↳ Window switches to the "Access list" tab.
↳ The imported access list is displayed (only for locking devices that have already been synchronised).



1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the Export ⤒ button.
   ↳ The Explorer window will open.
3. Save the exported access list to a file directory of your choice.
   ↳ Explorer window closes.

↳ The access list is exported.



Zutrittsliste für die Schließung 'Gryffindor dormitory'

Datum	Besitzer	S/N	Zugriff	Schließungskomponente
30.05.2021 04:57:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:55:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:54:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:53:00	##ServiceTId_IDS_AX_SETTIME		Verweigert	Master
30.05.2021 04:42:00	Weasley, Ron	002U2EP8	Erlaubt	Master
30.05.2021 04:37:00	##ServiceTId_IDS_AX_SYSSTART		Erlaubt	Master
30.05.2021 04:37:00	##ServiceTId_IDS_TTL_SELF_CLOSE		Erlaubt	Master
21.05.2021 11:26:00	Weasley, Fred	002U2EP8	Erlaubt	Master
21.05.2021 11:26:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:26:00	Weasley, Fred	002U2EP8	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
21.05.2021 11:13:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 21:17:00	Weasley, Fred	002U2EP8	Erlaubt	Master
20.05.2021 21:17:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:37:00	##ServiceTId_IDS_AX_SYSSTART		Erlaubt	Master
20.05.2021 20:37:00	##ServiceTId_IDS_TTL_SELF_CLOSE		Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 20:35:00	Weasley, Ron	002U0KLC	Erlaubt	Master
20.05.2021 17:10:00	##ServiceTId_IDS_AX_SETTIME		Verweigert	Master
30.03.2019 00:45:00	##ServiceTId_IDS_DM_DOOR_CLOSED		Erlaubt	Master

Gedruckt am: 03.12.2021 1

22.2 Displaying and exporting physical access lists for cards/ transponders

If required, your identification media can log which locking devices they were activated on (see *Allow accesses to be recorded by identification media (physical access list) [▸ 103]*). The entries saved in this physical access list are then transferred to the database during synchronisation, for example (see *Synchronise a card/transponder (including importing physical access list) [▸ 304]*).

You can view and export the physical access lists saved in the database.

NOTE

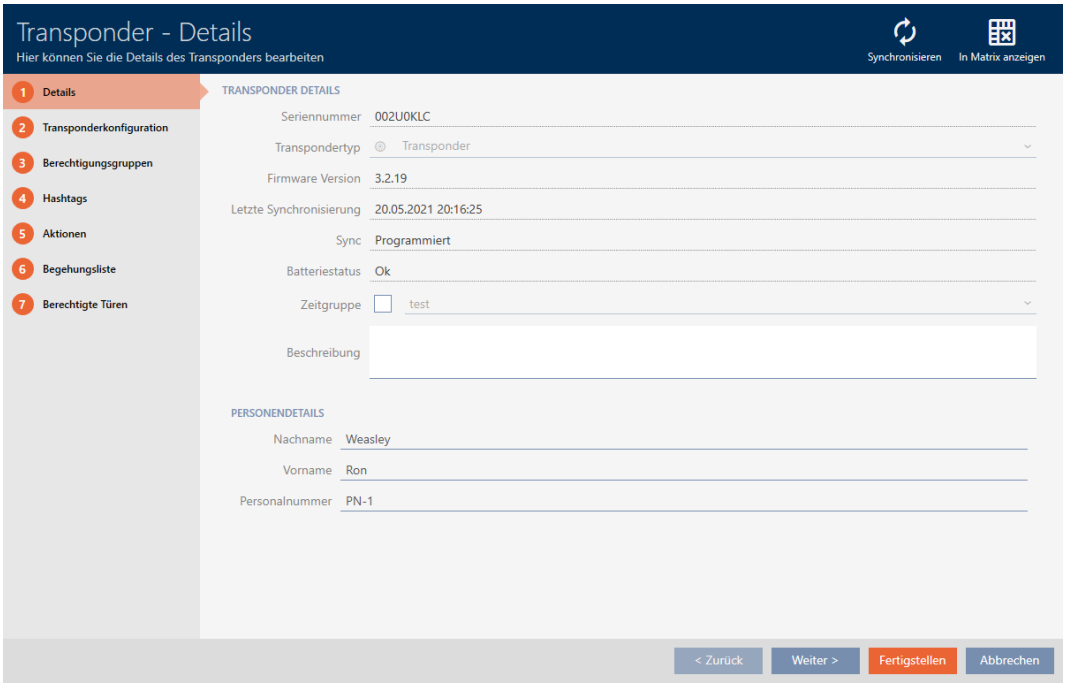
Displayed status corresponds to the last synchronisation

AXM Lite displays the status stored in the database at this point.

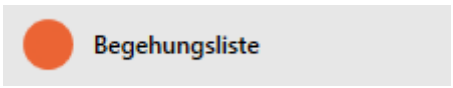
✓ AXM Lite open.

✓ Identification medium synchronised at least once.

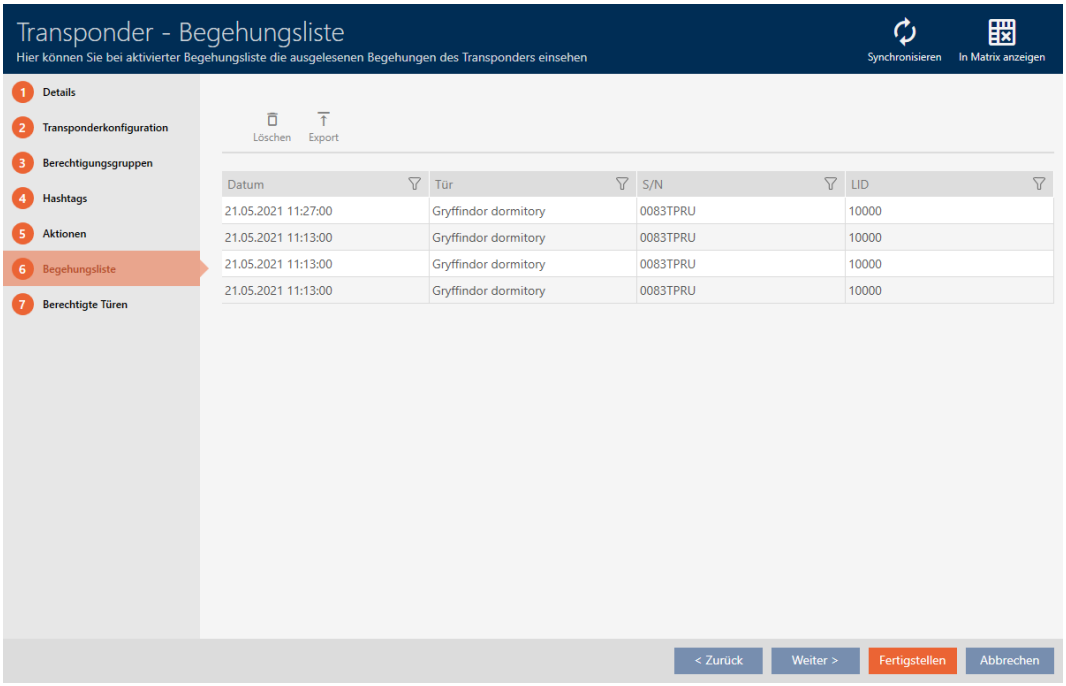
1. Click on the identification medium whose physical access list you wish to display.
   ↳ The identification medium window will open.



2. Clicking on the Personal audit trail tab

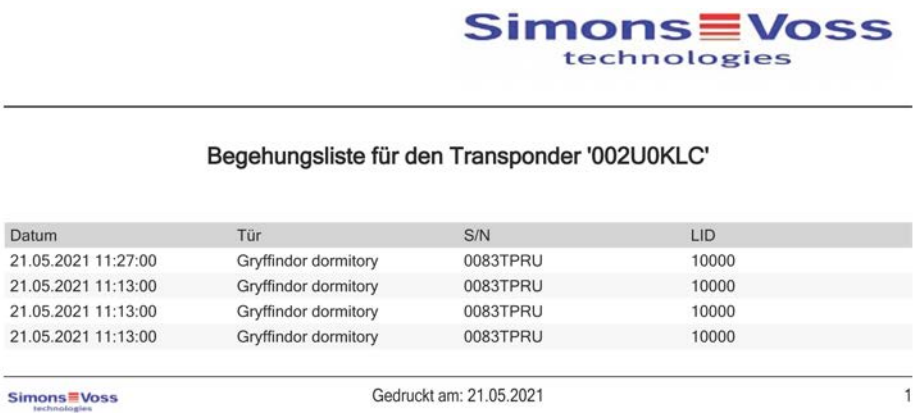


↳ Window switches to the "Personal audit trail" tab.



3. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
4. Click on the Export ⤒ button.
   ↳ The Explorer window will open.
5. Save the exported physical access list to a file directory of your choice.
   ↳ Explorer window closes.

↳ Physical access list is exported.



Begehungsliste für den Transponder '002U0KLC'

Datum	Tür	S/N	LID
21.05.2021 11:27:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000
21.05.2021 11:13:00	Gryffindor dormitory	0083TPRU	10000

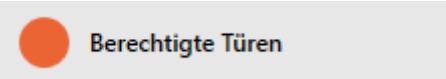
Gedruckt am: 21.05.2021 1

22.3 Display doors for which a specific identification medium is authorised

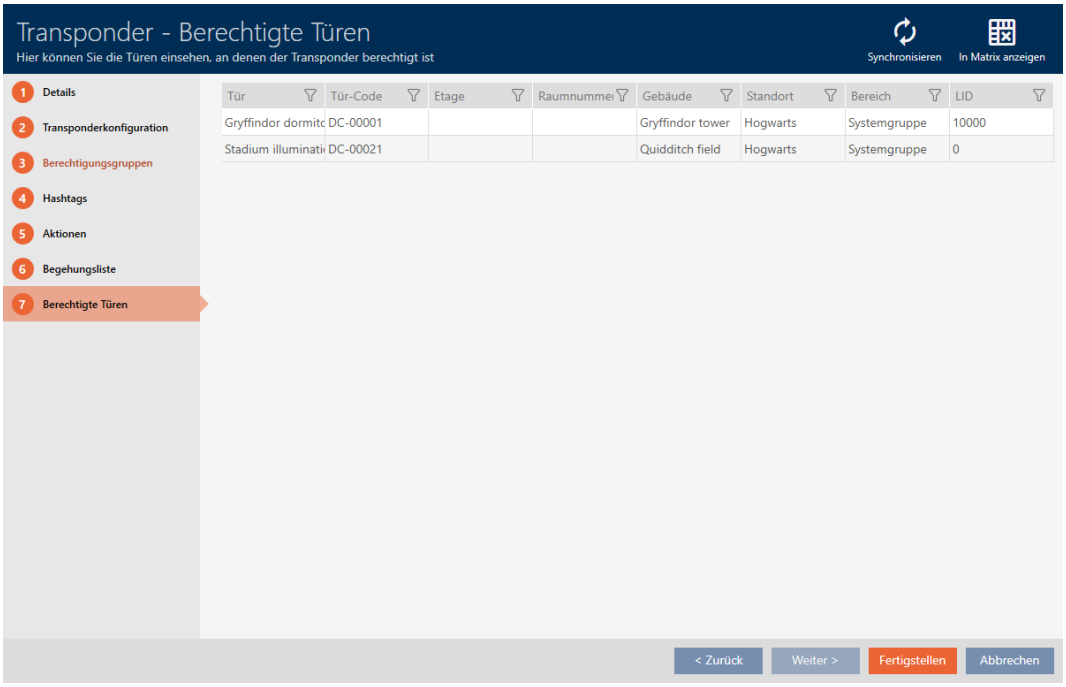
Alternatively, you can also display the identification media authorised for a door: *Displaying identification media which are authorised for a specific door [▸ 353]*

✓ AXM Lite open.
✓ Identification medium available.
✓ Locking device available.
✓ Identification media list or matrix open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the identification medium for which you wish to know the doors that it is authorised for.
   ↳ The identification medium window will open.
3. Click on the Authorised doors tab.



↳ Window switches to the "Authorised doors" tab.



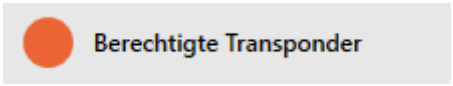
↳ Doors for which the identification medium is authorised are displayed.

22.4 Displaying identification media which are authorised for a specific door

Alternatively, you can also display the doors for which a specific identification medium is authorised: *Display doors for which a specific identification medium is authorised [▸ 352]*

✓ AXM Lite open.
✓ Identification medium available.
✓ Locking device available.
✓ Locking device list or matrix view open.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the locking device whose authorised identification media you wish to view.
   ↳ The locking device window will open.
3. Click on the Authorised transponders tab.



   ↳ Window switches to the "Authorised transponders" tab.

↳ Identification media that are authorised for the door are displayed.

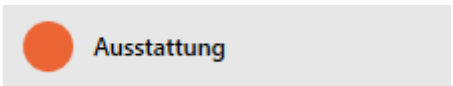
22.5 Displaying a locking device's equipment features

A locking device's equipment features are also imported during synchronisation. This allows AXM Lite to check whether the locking device is actually able to handle the required settings at all (e.g. whether an access control function is available).

You can display the imported equipment features in AXM Lite:

✓ AXM Lite open.
✓ Locking device available.
✓ Locking device list or matrix view open.
✓ Locking device synchronised.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the locking device whose equipment features you wish to display.
   ↳ The locking device window will open.
3. Click on the Features tab.



   ↳ Window switches to the "Features" tab.

↳ Equipment features are displayed.

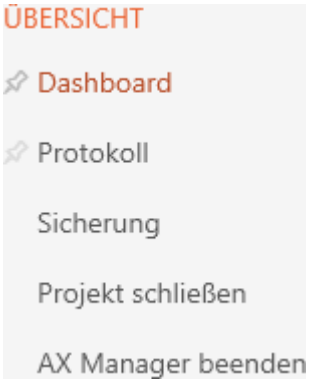
22.6 View statistics and warnings (dashboard)

AXM Lite comes with a new dashboard that gives you statistics on your database at a glance.

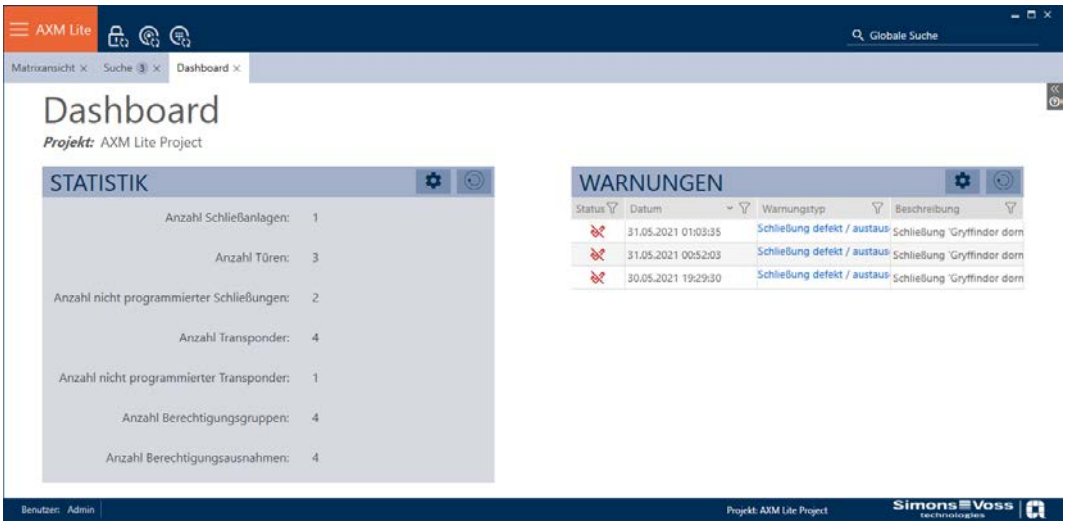
✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Dashboard entry in the | OVERVIEW | group.



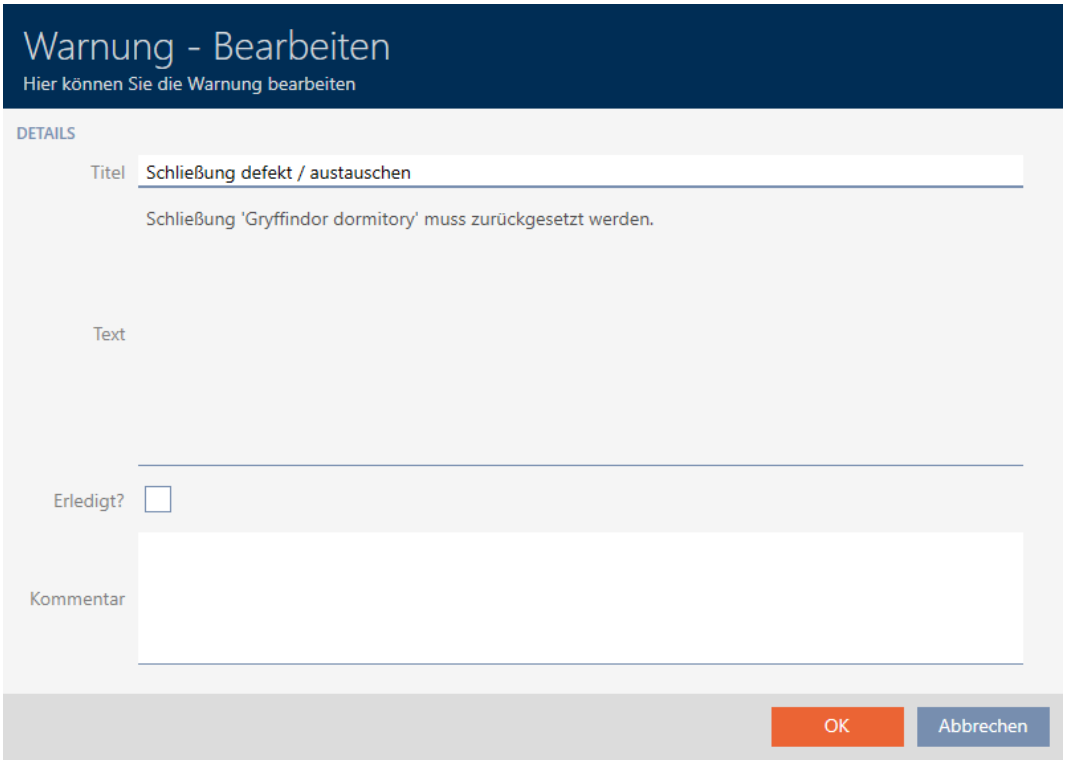
↳ The AXM bar will close.
↳ The [Dashboard] tab will open.



↳ Dashboard is displayed.

On the right-hand side you can see the statistics on your database and on the left-hand side you can see warnings:

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).
2. Click on the warning entry in the Warning column.
   ↳ Warning will open.



3. Change the *Title* and *Text* fields as required.
4. Deal with the warning if necessary. Then return to the warning and activate the ☑ Completed? checkbox.
5. Enter input into the *Comment* field.
6. Click on the OK button.
   ↳ Warning closes.

↳ Warning appears in the dashboard with a check mark as resolved.

22.7 Tracking activities in the database (log)

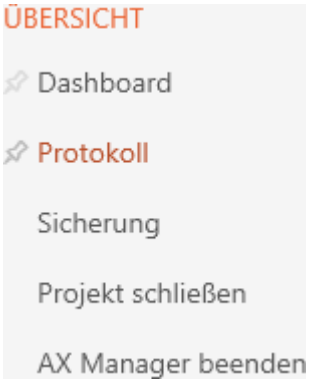
Every change and every setting in the database is logged in AXM Lite. This allows you to track who changed what in the database and when they made the changes.

The log archiving period can be adjusted (see *Setting the log archiving period [▸ 358]*).

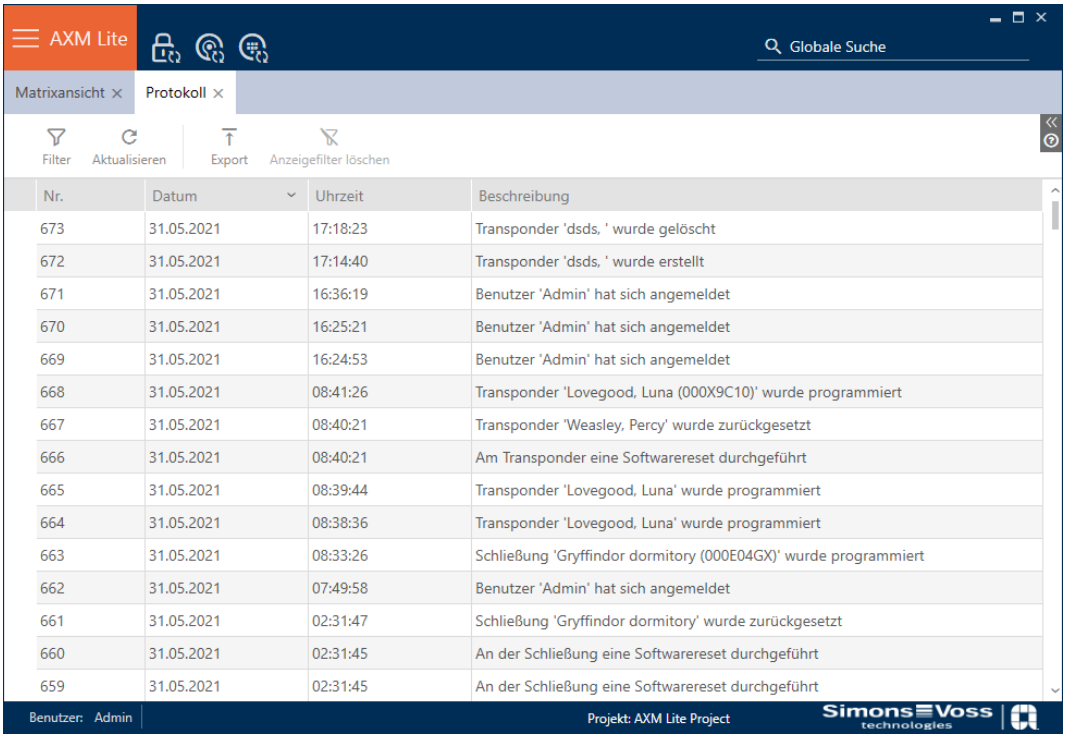
✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

2. Select the Protocol entry in the | OVERVIEW | group.



↳ The AXM bar will close.
↳ The [Protocol] tab will open.



3. Use to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 37]*).

↳ Log is displayed.

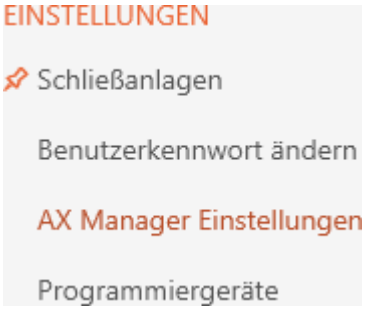
The Export button also allows you to export the log to provide a permanent backup.

22.7.1 Setting the log archiving period

✓ AXM Lite open.

1. Click the orange AXM button AXM.
   ↳ AXM bar opens.

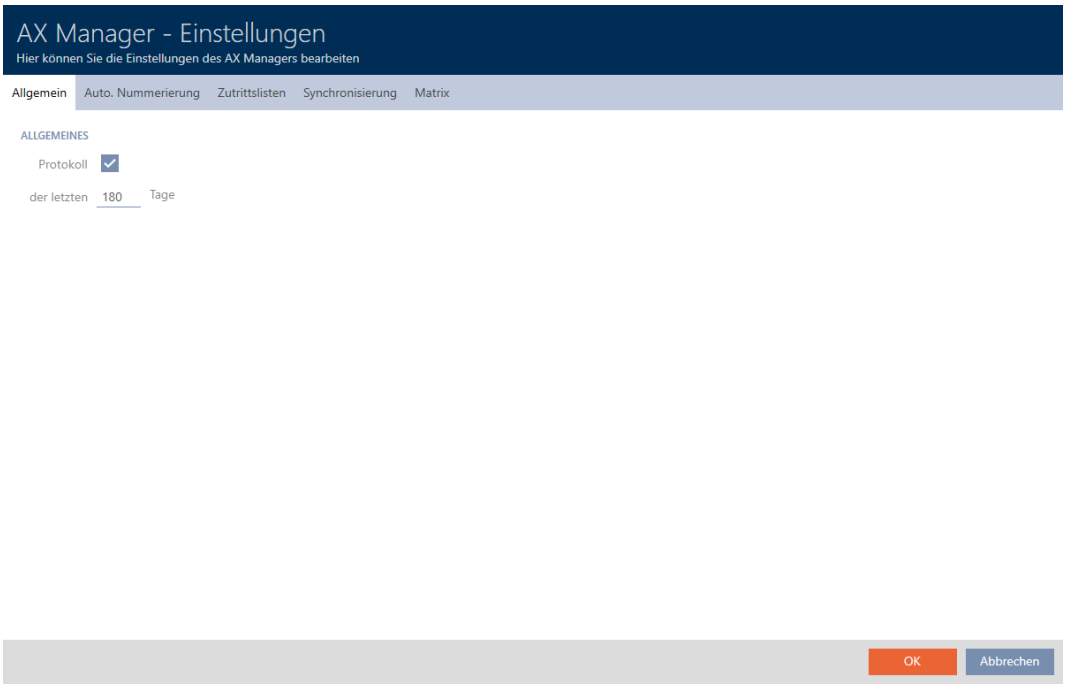
2. Select the AX Manager settings entry in the | SETTINGS | group.



↳ The AXM bar will close.

↳ The window with the AXM Lite settings will open.

3. Go to the [General] tab.



4. If you do not wish to log the changes to the database at all: Activate the ☐ Protocol checkbox.
5. Enter the required archiving period (max. 670 days).
6. Click on the OK button.
   ↳ The window with the AXM Lite settings closes.

↳ Protocol is limited to the required duration.

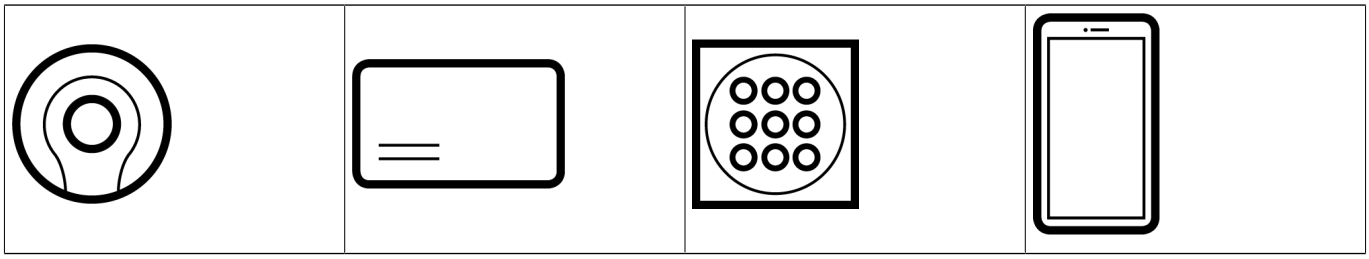
23. Background knowledge and explanations

23.1 Identification media, locking devices and the locking plan

Using identification media

The collective term identification medium refers to all components with which a person can identify themselves on a locking device. This primarily includes:

- Transponder
- Cards (smart card)
- Tags (smart tag)
- PIN code keypad



Identification media can communicate using the following technologies:

- Active technology (25 kHz)
- Passive technology (RFID, 13.56 MHz)
- Bluetooth Low Energy (BLE, 2.4 GHz)
- Active identification media (= transponders, PIN code keypad 3068) have a battery and can start communicating with a locking device themselves (actively).
- Passive identification media (= cards, tags) do not have a battery and must be powered by the locking device via an induction field. Only then can you communicate with the locking device.
- Identification media with BLE (= PIN code keypad AX and AX2Go) have a battery like active identification media, but communicate with the locking device via BLE.

Each technology offers advantages, depending on its specific use.

Your cards and transponders have two numbers that are important:

- Serial number (permanently stored in the identification medium and imported during synchronisation)
- TID (flexibly assigned by AXM Lite and written on the identification medium during synchronisation)

The serial number is a unique number for each identification medium while the TID is only unique in your locking system.

The database establishes a link between the imported serial number and the TID (transponder ID) during synchronisation. This means that AXM Lite knows which serial number and which TID belong together.

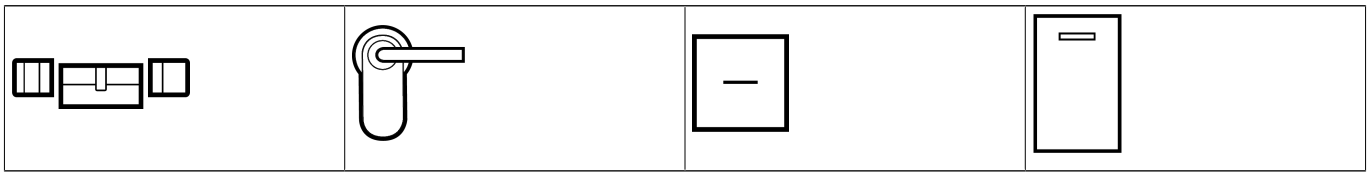
		TID
Seriennummer	002TU6TC	3203

However, this link is confined to AXM Lite and is not written onto identification media or locking devices. A locking device uses the TID (and not the serial number) to check whether an identification medium is authorised or not.

About locking devices

The collective term “locking devices” refers to all components which are “activated” with an identification medium. Locking devices are usually installed in or on a door (except SmartRelay). Locking devices primarily include:

- Locking cylinders
- SmartHandles
- SmartRelays
- SmartLocker



Locking devices can also communicate with identification media using different technologies:

- Active
- Passive
- BLE

It is important that the technologies used match. A passive locking device can normally only be opened with a passive identification medium, but not an active one.

Like an identification medium, each locking device has two important numbers:

S/N	Schließungs ID
000C1957	129
000DSP7E	128
000E04GX	10000
000DC331	10001

- Serial number (permanently stored in the locking device; imported during synchronisation)
- Lock ID (LID for short; flexibly assigned by AXM Lite and written onto the locking device during synchronisation)

The database establishes a link between the imported serial number and the LID in the database during synchronisation. This means that AXM Lite knows which serial number and which LID belong together. However, this link is confined to AXM Lite and is not written onto identification media or locking devices. A locking device uses the TID (and not the serial number) to check whether an identification medium is authorised or not.

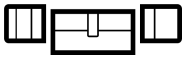
Normally, you don't need to concern yourself with the TID and LID as your AXM Lite does everything in the background.

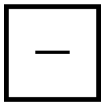
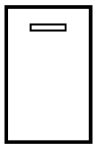
About the locking plan

Put very simply, the matrix is mapped and saved to the locking plan. Among other things, it contains the authorisations. Thanks to the locking plan, locking devices and identification media know who is authorised to use either.

23.2 “Engaging”, “opening”, “locking”, etc.

Different locking device types respond differently to an authorised identification medium due to their design:

Locking device	Response	User action
Locking cylinders 	Engage: The electronic thumb-turn connects to the cam mechanically.	Open: 1. Turn thumb-turn. 2. Take the door handle. 3. Pull open door with door handle.
SmartHandles	Engage: The handle on the electronic side connects to the spindle mechanically.	Open: 1. Press the handle. 2. Pull open door with door handle.

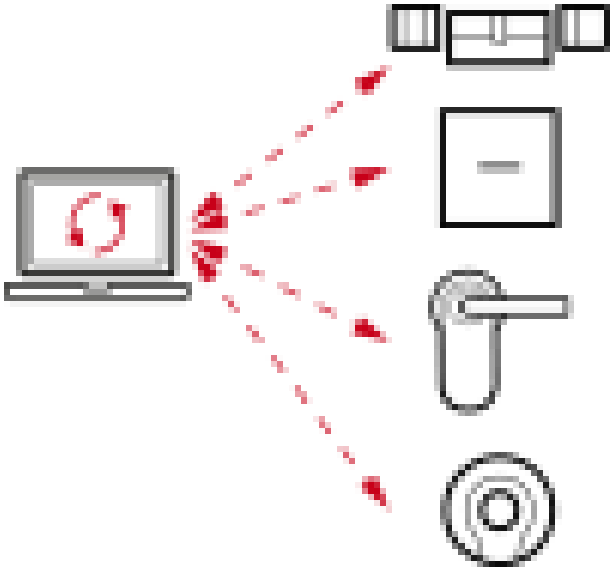
Locking device	Response	User action
SmartRelays 	Switching: The relay contact in SmartRelay switches. Depending on the SmartRelay, this is a make contact or a changeover contact. Connected electrical doors now open.	No further action required. The door is generally already open.
SmartLocker AX 	Retract dead bolt: The motor block in the SmartLocker retracts the dead bolt and releases the door.	Open: 1. Pull the door open.

As a general rule, the following applies: No locking device except SmartRelay is able to open, close or lock a door. Action is always required from the user (e.g. turning the thumb-turn and pulling the door open). Even SmartRelay requires a connected door control unit, a connected motor or similar.

Term	Meaning
Activate	An identification medium is activated on a locking device.
Engage	Locking cylinder and SmartHandle: The electronic thumb-turn or the electronic handle connect to the cam or spindle.
Open	A door is opened by the user (after a locking cylinder has been engaged, for example).
Close	A door is closed by the user and clicks shut. The mortise lock dead bolt has not extended yet.
Disengage	Locking cylinder and SmartHandle: The electronic thumb-turn or the electronic handle disengage from the cam or the spindle.
Switch	Only for SmartRelay: The relay switches and the relay contacts close or switch.

Term	Meaning
Lock	Only for locking cylinders: The locking cylinder is engaged and the thumb-turn is turned once. The mortise lock dead bolt extends.
Lock securely	Only for locking cylinders: The locking cylinder is engaged and the thumb-turn is turned twice. The mortise lock dead bolt extends fully.

23.3 Synchronisation of database and actual state



Everything you change in AXM Lite is stored in the database only (for the time being). There is no automatic connection between the database and your locking devices or identification media.

Changes only take effect after synchronisation (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*). You can see by the ⟳ symbol in the matrix that something has changed here since the last synchronisation and that a locking device or identification medium needs to be synchronised.

Data is transmitted in both directions during synchronisation:

- From the database to the locking device/identification medium, e.g. authorisation changes
- From the locking device/identification medium to the database, e.g. battery levels

IMPORTANT

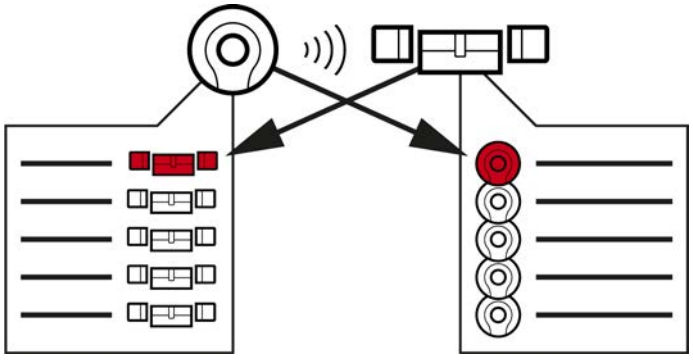
Changes to the locking system only take effect after synchronisation

If you edit the locking system with the AXM Lite, the changes are initially only saved to your database.

Your actual components will not know about these changes until they are synchronised.

1. Regularly check the components in the matrix for synchronisation requirements (see *The AXM's structure [▸ 35]*).
2. In the event of critical incidents (e.g. identification medium lost), it is particularly important to synchronise immediately after responding to the incident (see *Synchronisation: Comparison between locking plan and reality [▸ 290]*).

23.4 Access and physical access lists



Physical access list Access list

If an identification medium addresses a locking device, both can log this action (the access control function is a prerequisite for the locking device).

Card configuration with an AV template is required for cards.

- The locking device concerned is saved to a physical access list in the identification medium.
- The identification medium concerned is saved to an access list in the locking device.

Both lists can be read during synchronisation and imported into the database, for example:

- *Synchronising the locking device (including reading access list) [▸ 291]*
- *Synchronise a card/transponder (including importing physical access list) [▸ 304]*

You can then view both lists:

- *Displaying and exporting a locking device's access list [▸ 348]*

- *Displaying and exporting physical access lists for cards/transponders [▸ 350]*

23.5 Event management

The time management in System 3060 is very extensive and offers a wide range of setting options. There are basically two independent time functions:

- Restrict authorisations to specific times (*Time groups and schedules [▸ 366]*)
- Automatically engage locking devices (*Time switchovers [▸ 370]*)

NOTE

Summertime and wintertime

The time and switchover times in the device from which synchronisation takes place are used for all time-controlled functions and saved in the locking device.

- Before synchronising, check that the date and time are set correctly.

23.5.1 Time groups and schedules

Here you can see an example of how a schedule and time group work together:

Initial situation

For the sake of simplicity, let's say your sample company consists of three people:

1. Employee
2. Intern
3. Cleaner

Your example company also has two doors:

1. Main entrance
2. Laboratory

There are also the following important time periods in your sample company:

- Flexitime between 7:00 to 22:00 hours
- Core hours between 9:00 to 16:00 hours
- Cleaning time between 17:00 to 19:00 on Tuesdays and Thursdays

Considerations for time restriction to authorisations

As a responsible business owner, you consider the following:

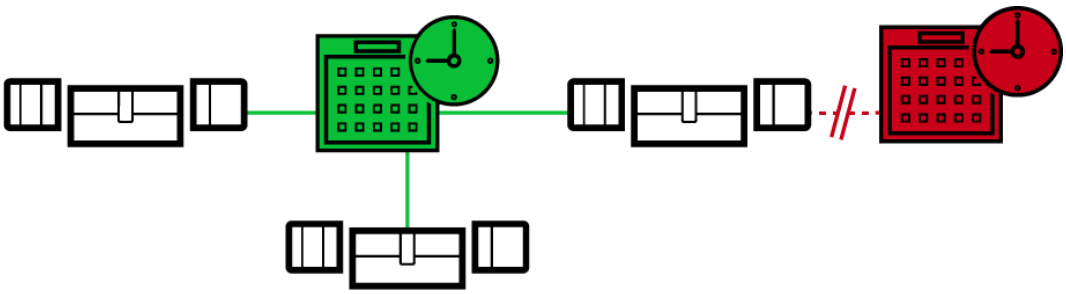
Considerations for:	Main entrance	Laboratory
Employee	Your employee may enter the building during the entire flexitime period and also between 7:00 to 22:00 hours on weekends.	Your employee may enter the laboratory during the entire flexitime and also between 7:00 to 22:00 hours on weekends.
Intern	Your intern shouldn't have to wait outside for your employee to come in when the weather is bad. Consequently, your intern may also enter the building during the entire flexitime between 7:00 to 22:00 hours on working days.	The laboratory is a dangerous workplace. To protect your intern, you want them only to be able to enter the laboratory under your employee's supervision. You therefore limit your intern's access to the laboratory to working days and to your employee's core working hours (9:00 to 16:00).
Cleaner	Your cleaner may enter the building during cleaning hours between 17:00 to 19:00 on Tuesdays and Thursdays.	The laboratory is dangerous and, consequently, only trained personnel may enter. Cleaning staff may possibly change and are therefore trained persons. As a result, you do not want your cleaner to enter the laboratory at all.

You can see that there are two doors where you wish to control authorisations with three different times. You will thus need:

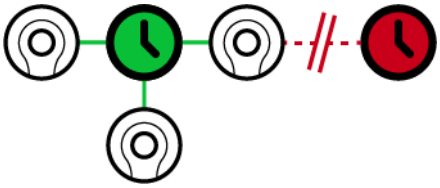
- Two schedules for doors or locking devices:
  - "Main entrance" schedule
  - "Laboratory" schedule
- Three time groups for the people in the company:
  - "Employee" time group
  - "Intern" time group
  - "Cleaner" time group

New schedule or new time group?

- There is one schedule per locking device, but any number of locking devices can be assigned per schedule.



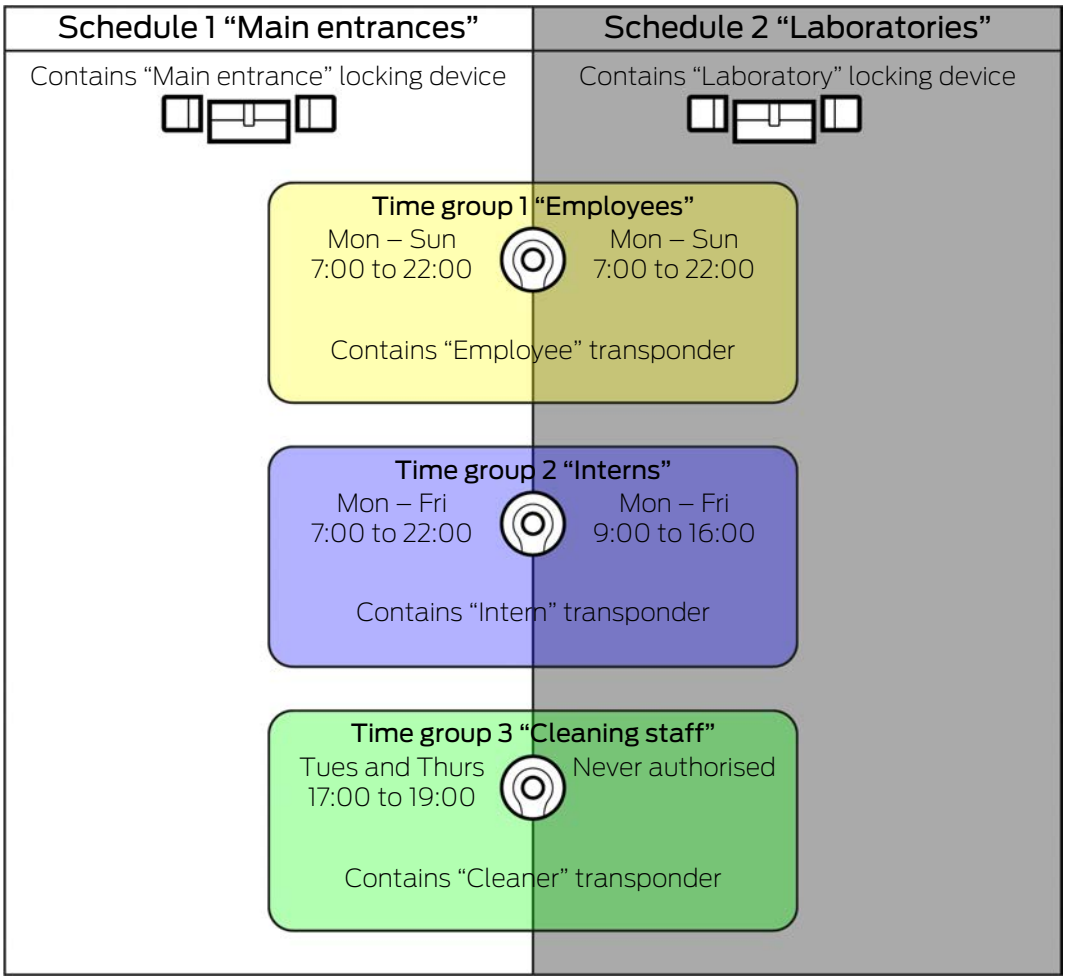
- One time group per identification medium, but any number of identification media can be assigned per time group.



- All time groups are visible/selectable in all schedules but are set individually for each schedule. If you create and set a new time group in one schedule, the time group will also appear in all other schedules. However, it is only available there and is set as “not authorised” by default for security reasons.

New schedule	New time group
If the same identification medium needs to be able to enter using two locking devices at different times. As you can only assign one time group to each identification medium, you assign a separate schedule to the locking devices in this case. Example: Although the intern’s transponder may open the main entrance between 7:00 to 22:00 hours, the same transponder may only open the laboratory between 9:00 to 16:00 hours.	If two identification media are to be able to enter using the same locking device at different times. As you can only assign one schedule per locking device, you assign a separate time group to the identification media in this case. Example: The employee may open the main entrance locking device between 7:00 to 22:00 hours daily, but the intern may only use the same locking device between 7:00 to 22:00 hours on working days.

Schematic diagram



	Main entrance	Laboratory
Employee	■ Your employee’s transponder: “Employees” time group ■ Main entrance locking device: “Main entrances” schedule ■ “Employees” time group authorised in “Main entrances” schedule between 7:00 to 22:00 daily Your employee can enter the main entrance between 7:00 to 22:00 hours daily.	■ Your employee’s transponder: “Employees” time group ■ Laboratory locking device: “Laboratories” schedule ■ “Employees” time group authorised in “Laboratories” schedule between 7:00 to 22:00 daily Your employee can enter the laboratory between 7:00 to 22:00 hours daily.

	Main entrance	Laboratory
Intern	▪ Your intern's transponder: "Interns" time group ▪ Main entrance locking device: "Main entrances" schedule ▪ "Interns" time group authorised in the "Main entrances" schedule between 7:00 to 22:00 on working days Your intern can enter the main entrance between 7:00 to 22:00 on working days.	▪ Your intern's transponder: "Interns" time group ▪ Laboratory locking device: "Laboratories" schedule ▪ "Interns" time group authorised in "Laboratories" schedule between 9:00 to 16:00 on working days Your intern can enter the laboratory between 9:00 to 16:00 on working days.
Cleaner	▪ Transponders for your cleaner: "Cleaning staff" time group ▪ Main entrance locking device: "Main entrances" schedule ▪ "Cleaning staff" time group authorised in the "Main entrances" schedule between 17:00 to 19:00 on working days Your cleaner can enter the main entrance between 17:00 to 19:00 on Tuesdays and Thursdays.	▪ Transponders for your cleaner: "Cleaning staff" time group ▪ Main entrance locking device: "Laboratories" schedule ▪ "Cleaning staff" time group never authorised in the "Laboratories" schedule Your cleaner can never enter the laboratory.

23.5.2 Time switchovers

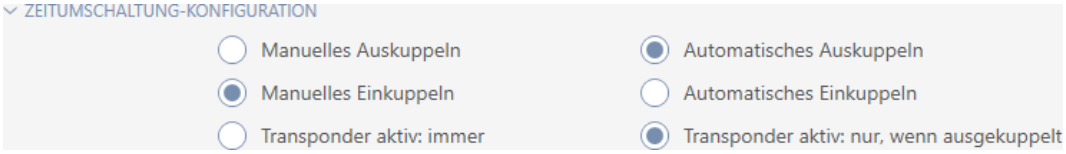
You can automatically engage and disengage your locking devices with time switchovers.

1. To do this, specify days and time intervals in a time switchover (see *Creating a time switchover [▸ 58]*).
2. Then add the locking devices you require to this time switchover (see *Engaging and disengaging locking devices automatically with time switchover [▸ 222]*).
3. Last of all, determine the required behaviour for each of the locking devices you require (see *Engaging and disengaging locking devices automatically with time switchover [▸ 222]*).

As a general rule, the following applies:

- Your locking devices behave as in office mode within a time interval.
- Your locking devices behave as in impulse opening mode outside a time interval.

The behaviour can be regulated even more precisely with the following options:



Manuelles Auskuppeln

Locking device disengages:

- Outside the time intervals and
- If authorised identification medium is activated

It remains disengaged. You can also engage the locking device outside the time intervals for the set impulse duration using an authorised identification medium (see *Leaving the locking device open for longer, less time or permanently [▸ 229]* for setting the impulse duration).

Automatisches Auskuppeln

Locking device disengages:

- Time interval ends

It remains disengaged. You can also engage the locking device outside the time intervals for the set impulse duration using an authorised identification medium (see *Leaving the locking device open for longer, less time or permanently [▸ 229]* for setting the impulse duration).

Manuelles Einkuppeln

Locking device engages:

- Within the time intervals and
- If authorised identification medium is activated

Example: Store in the shopping centre where the sliding door mustn't open automatically during the shopping centre's opening hours. The store owner could be delayed due to a traffic jam and the store would open with no-one in control.

Locking device remains engaged for the time interval.

You can also disengage the locking device during the time interval using an authorised identification medium (exception: ◉ Transponder aktiv: Nur, wenn ausgekuppelt option activated).

Locking device then remains disengaged until:

- You press an identification medium again during the same time interval: Locking device engages again, time switchover continues as usual.

- In the case of ◉ Manuelles Einkuppeln option: a new time interval starts and an identification medium is activated.
- In the case of ◉ Automatisches Einkuppeln option: a new time interval starts.

Automatisches Einkuppeln

Locking device engages:

- time interval starts

Locking device remains engaged for the time interval.

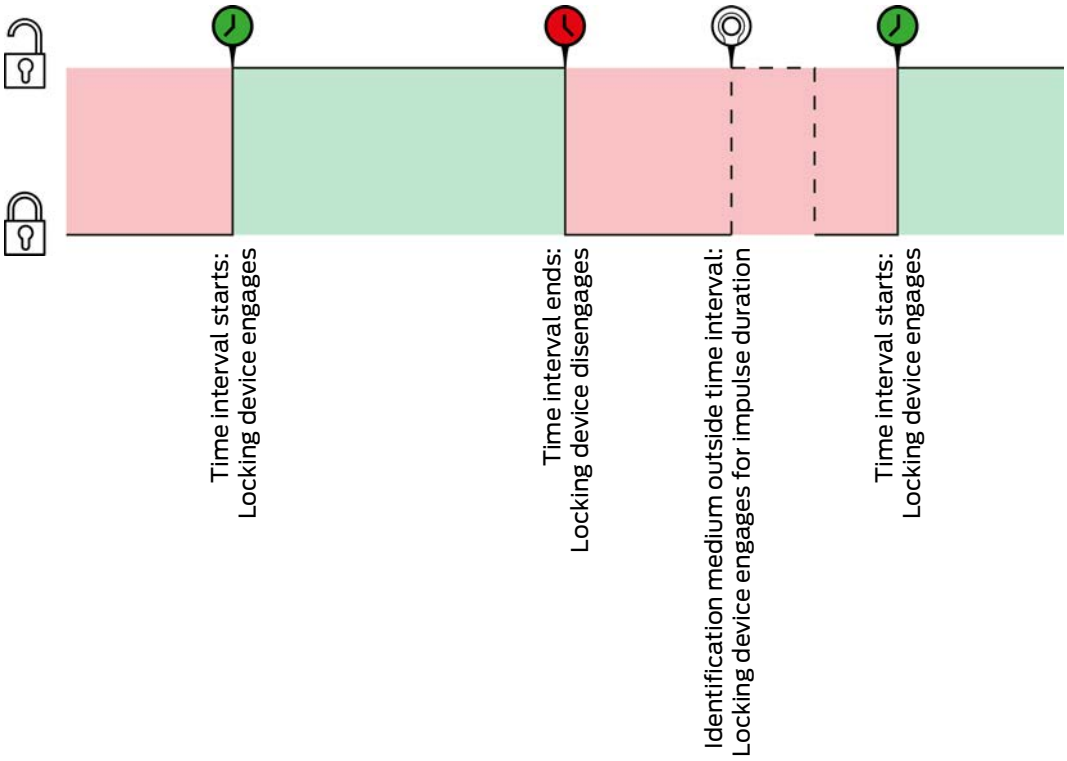
You can also disengage the locking device during the time interval using an authorised identification medium (exception: ◉ Transponder aktiv: Nur, wenn ausgekuppelt option activated).

Locking device then remains disengaged until:

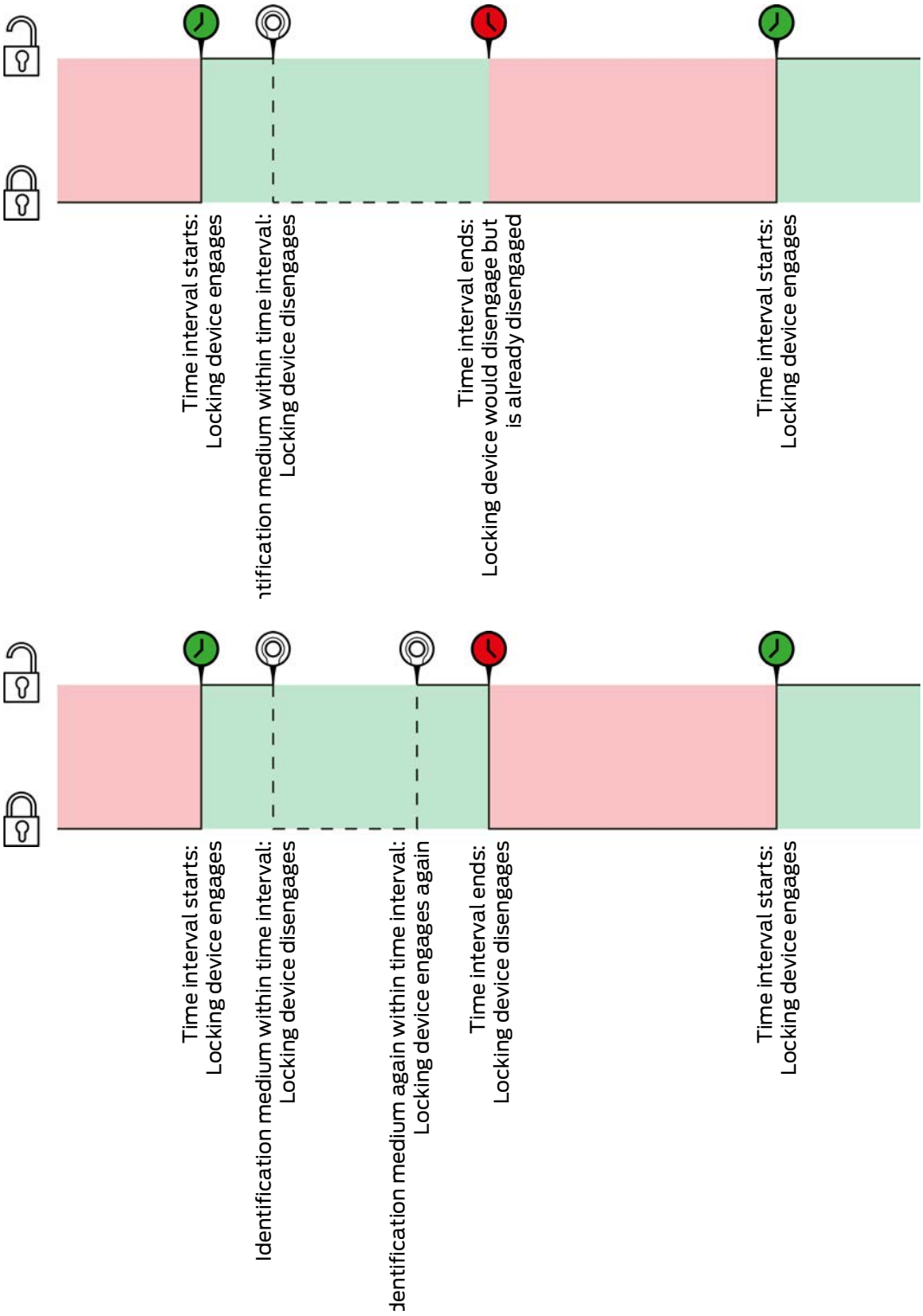
- You press an identification medium again during the same time interval: Locking device engages again, time switchover continues as usual.
- In the case of ◉ Manuelles Einkuppeln option: a new time interval starts and an identification medium is activated.
- In the case of ◉ Automatisches Einkuppeln option: a new time interval starts.

23.5.2.1 Examples

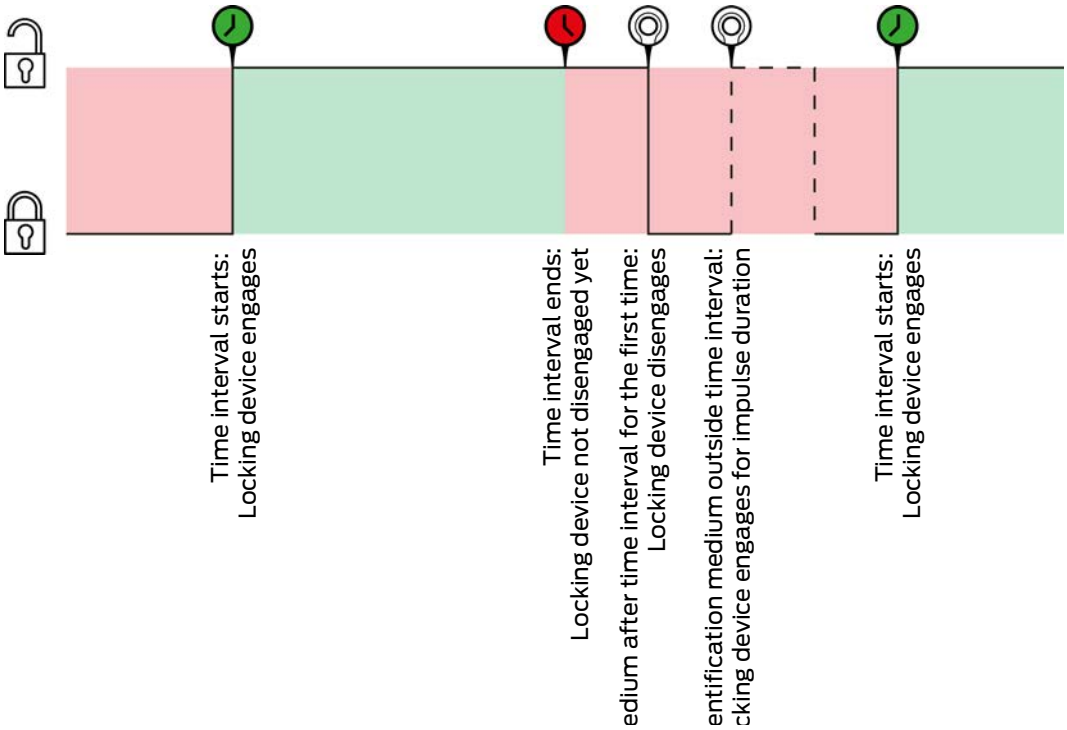
Automatisches Einkuppeln, Automatisches Auskuppeln



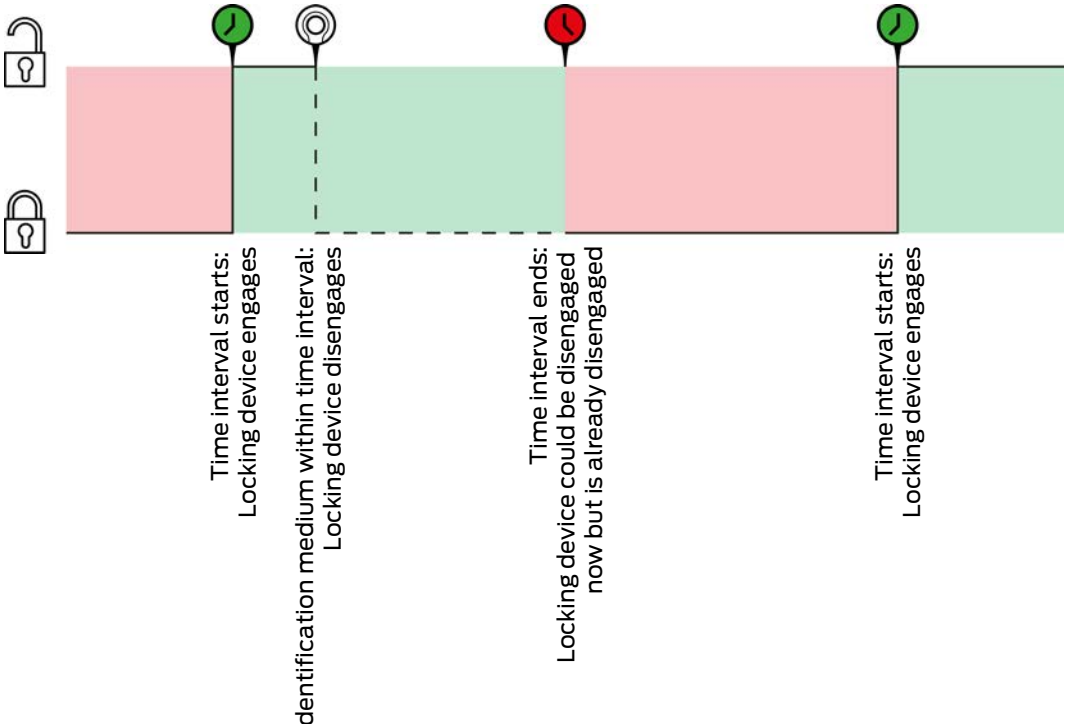
The ⊙ Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

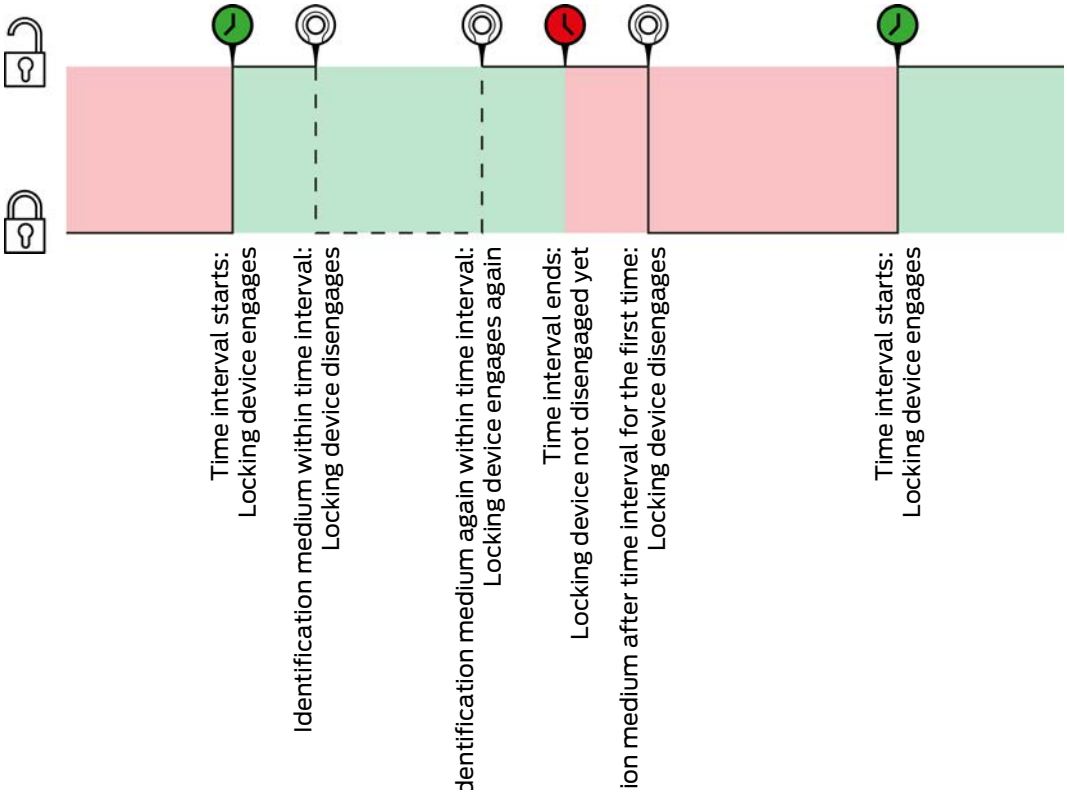


Automatisches Einkuppeln, Manuelles Auskuppeln

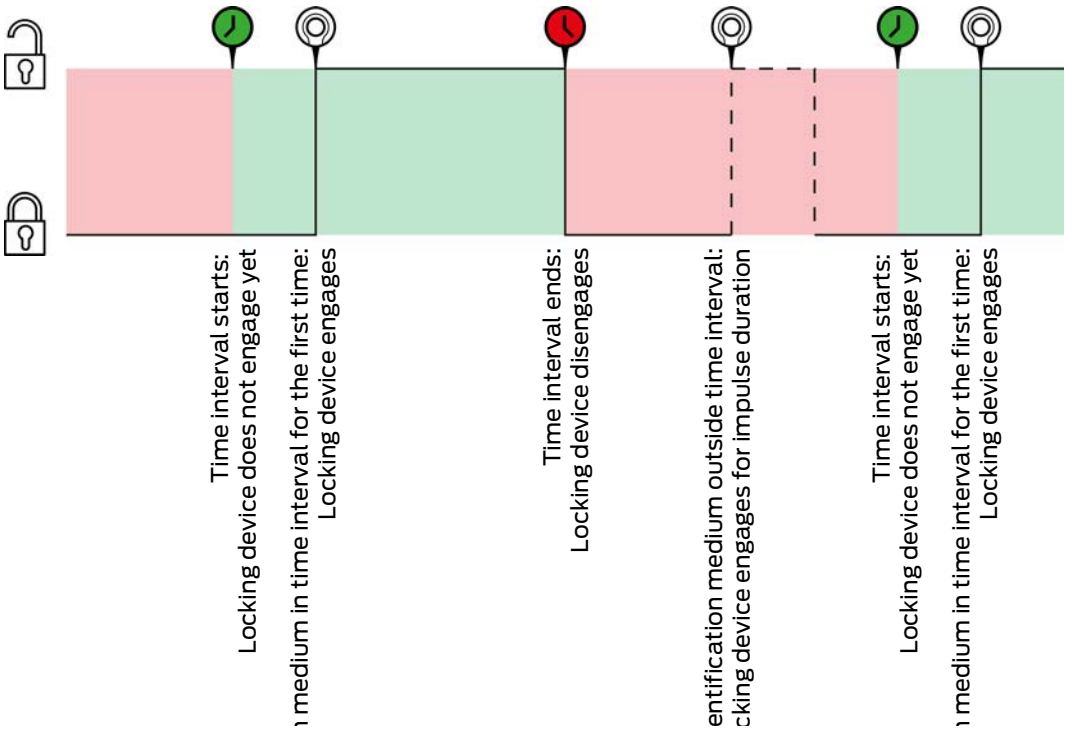


The Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

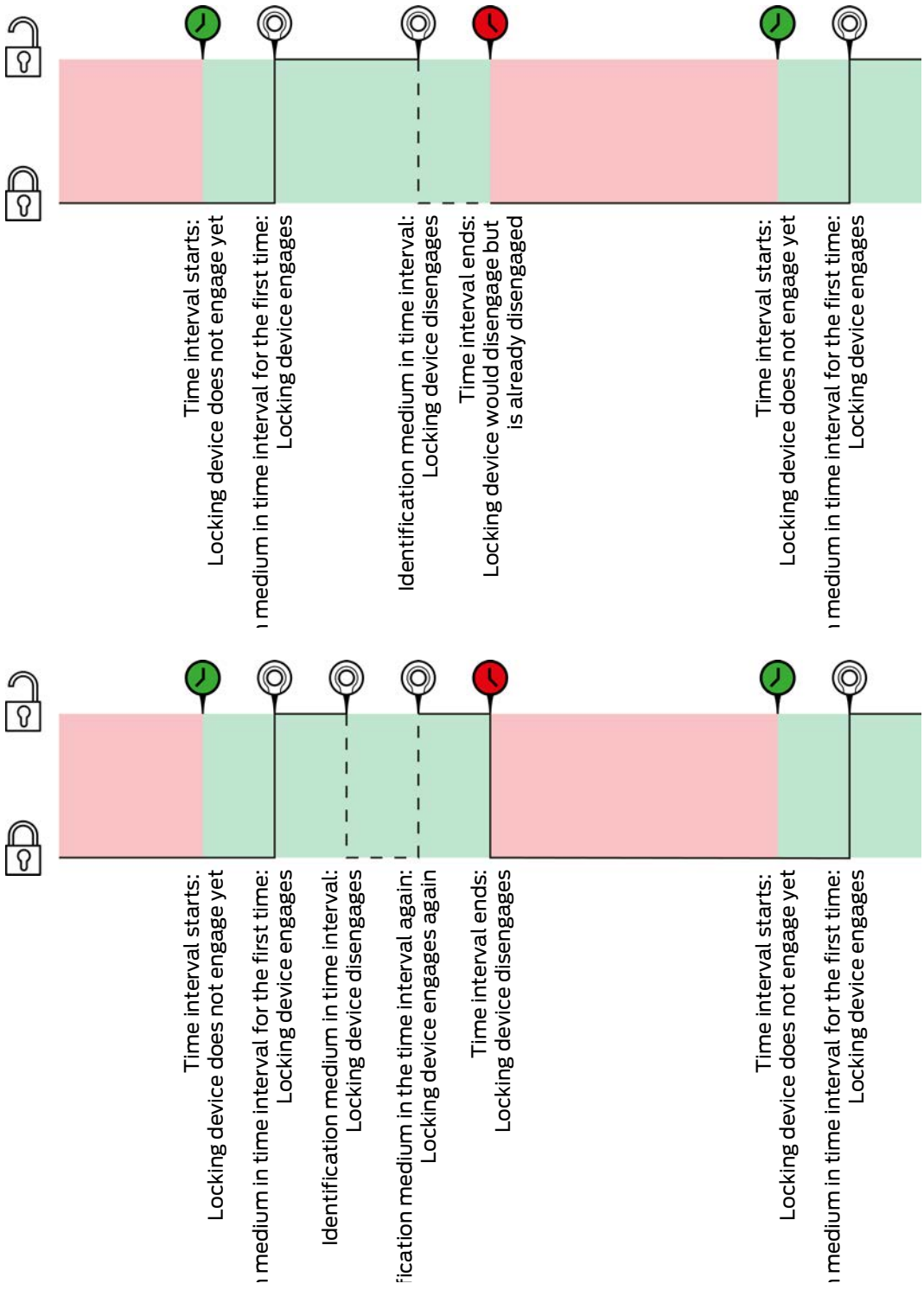




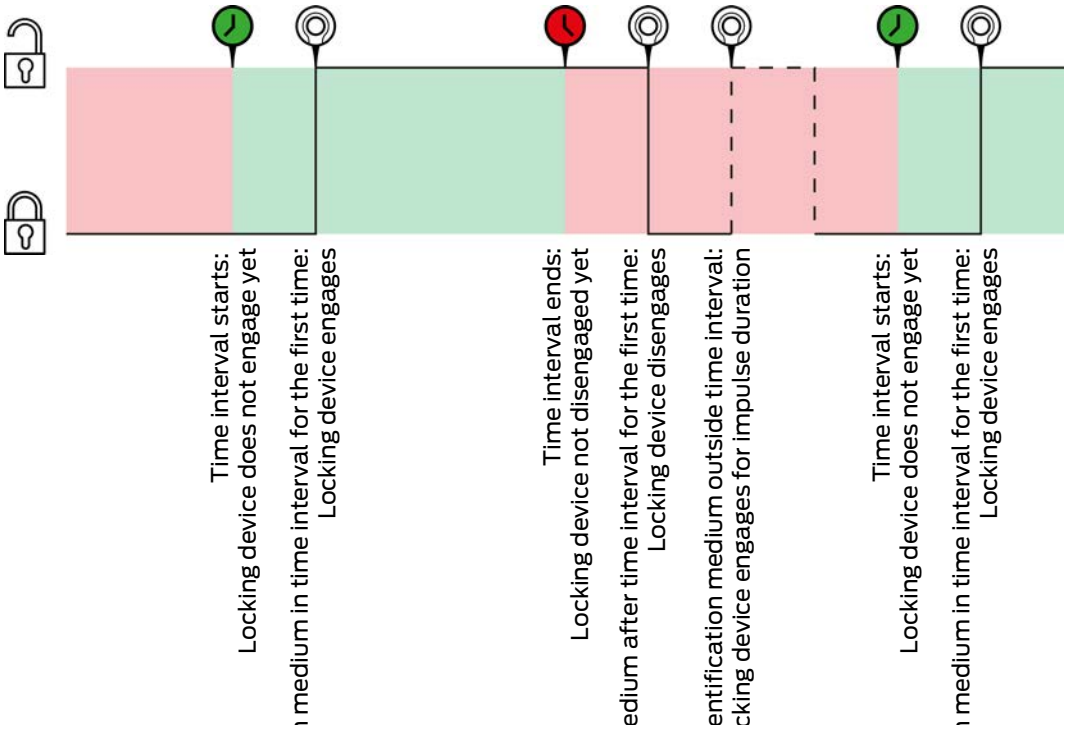
Manuelles Einkuppeln, Automatisches Auskuppeln



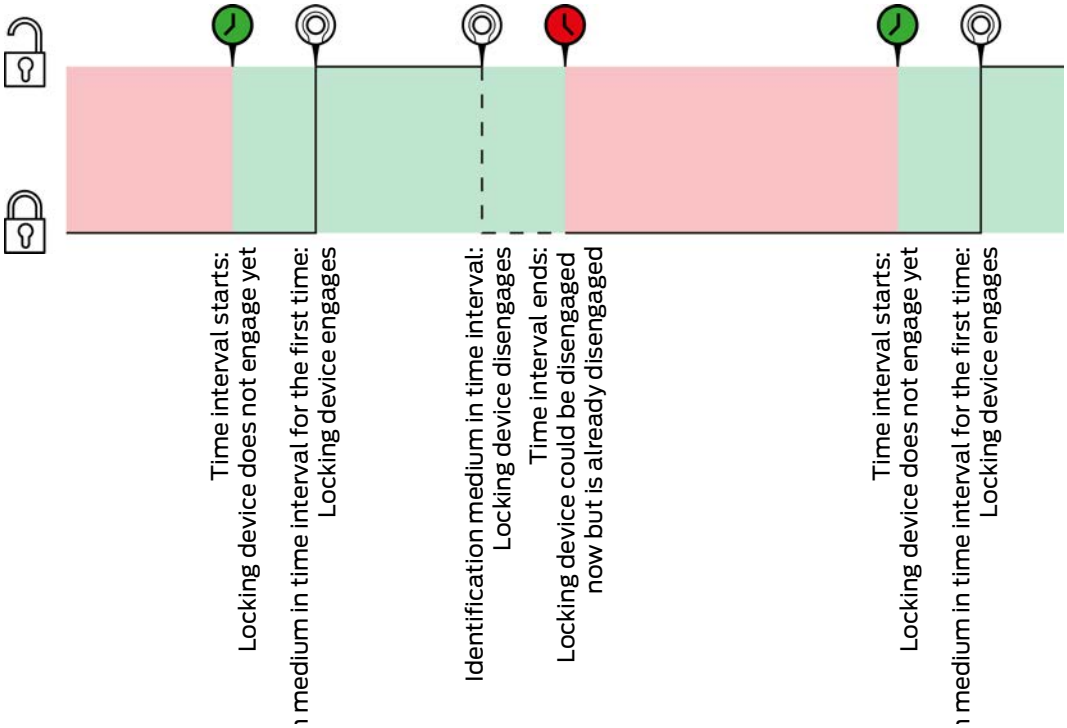
The ⊙ Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

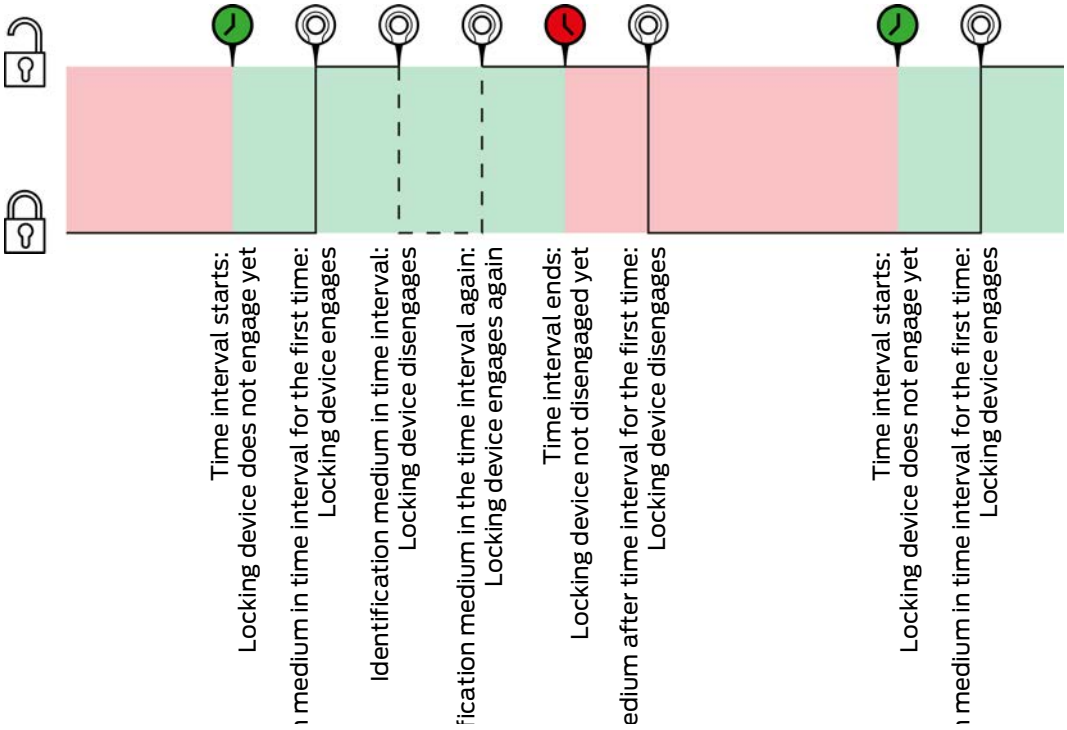

Time interval starts:
Locking device does not engage yet
medium in time interval for the first time:
Locking device engages
Identification medium in time interval:
Locking device disengages
Time interval ends:
Locking device would disengage but
is already disengaged
Time interval starts:
Locking device does not engage yet
medium in time interval for the first time:
Locking device engages
Time interval starts:
Locking device does not engage yet
medium in time interval for the first time:
Locking device engages
Identification medium in time interval:
Locking device disengages
fication medium in the time interval again:
Locking device engages again
Time interval ends:
Locking device disengages
Time interval starts:
Locking device does not engage yet
medium in time interval for the first time:
Locking device engages

Manuelles Einkuppeln, Manuelles Auskuppeln

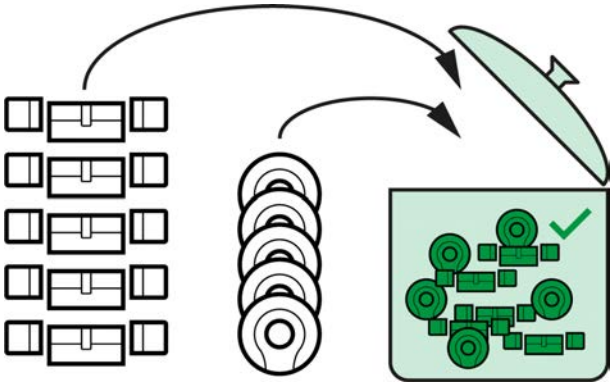


The ⊙ Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.





23.6 Access levels



Access levels are available for the first time with the introduction of AXM Lite.

The principle of an access level is very simple, similar to a melting pot. Within an access level, all locking devices are normally authorised on all identification media.

We say “normally” because you can also manually remove authorisations from individual identification media. This gives you full freedom to decide on authorisations, but you can do most of the work in an access level.

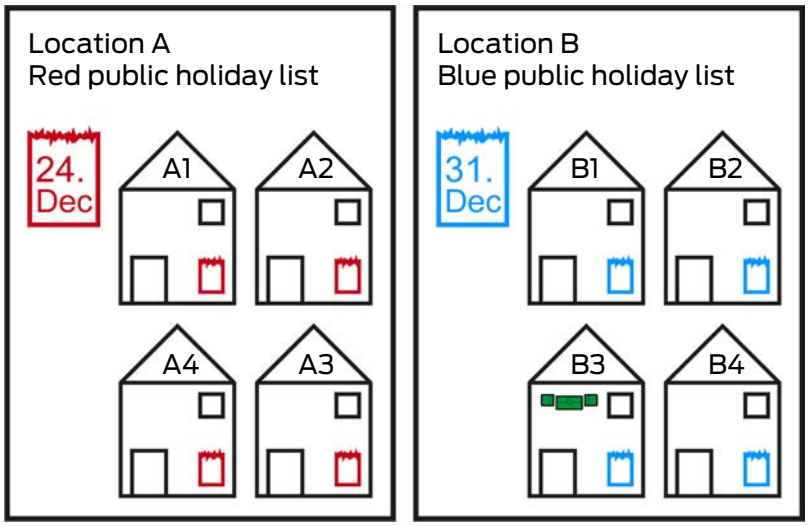
Identification media and locking devices can be assigned to a number of access levels.

Access levels are an organisational component. Ideally, you should set up your access levels before your locking devices and identification media (see *Best practice: setting up the locking system [▸ 29]* and *Creating access levels [▸ 44]*).

23.7 Passwords used

- User password: Protects your AXM Lite against unauthorised persons logging in and changing your locking system.
- Locking system password: Protects communication between the different components in your locking system (e.g. between a transponder and a locking cylinder).
- Backup passwords: Protects your AXM Lite against outdated locking system statuses being restored.

23.8 Buildings and locations



A location contains buildings and, optionally, a public holiday list.

A building always belongs to a location. Therefore, you must always have at least one location in your database. AXM Lite thus creates a standard location in new projects. You can delete it as soon as you have created your own locations.

Locations and buildings are particularly useful for organisation. For this reason, they should also be created before the locking devices in line with best practice (see *Best practice: setting up the locking system [▸ 29]*) (see *Creating a location [▸ 69]* and *Creating a building and assigning it to a location [▸ 72]*).

Public holiday lists and locations

As a rule, you only assign buildings to a location that are actually at the same location. It is therefore very likely that all these buildings will be subject to the same public holidays (e.g. all buildings at the Munich site: Bavarian public holidays apply to all buildings).

The public holiday lists are particularly interesting for time-controlled locking devices. Locking devices are conveniently always assigned to a building, which in turn is assigned to a location (mandatory information). Assigning a public holiday list to each locking device is a laborious task. Instead, you can assign the same public holiday list to all locking devices in buildings with the same location by simply assigning a public holiday list to the entire location.

The public holiday list assigned in this way applies to all locking devices at this location. In the example, the red public holiday list has been assigned to location A and the blue public holiday list to location B.

If other public holidays should apply to individual locking devices (for whatever reason), you can overwrite the location's public holiday list in the locking device properties (see *Limiting authorisations for locking devices to specific times (schedule) [▸ 220]*). In the example, a green public holiday list was assigned to a locking device in building B3 at location B. The blue public holiday list continues to apply to all other locking devices in building B3 and other buildings at location B.

23.9 Hashtags

Hashtags are an additional option for organising your locking system. Use any keyword for locking devices and identification media.

The installation situation, for example, would be good keyword: #glassdoor

23.10 DoorMonitoring

DoorMonitoring is an additional feature for recording door statuses and displaying them in your AXM Lite .

This requires locking devices with the associated sensors (=DoorMonitoring locking devices).

NOTE

DoorMonitoring without direct networking (“WaveNet”) available to a limited extent

In a directly networked locking system, locking devices connected to the WaveNet can immediately transmit their DoorMonitoring events via the network. You can see these events in your locking plan software (e.g. AXM) in no time.

Locking devices without WaveNet also log their DoorMonitoring events and save them in the access list. You will only see these events after reading the access list in your locking plan software.

For example, DoorMonitoring locking cylinders are fitted with a special sensor fastening screw.

23.10.1 Possible DoorMonitoring states of locking cylinders

- Door open/closed
- Door locked
- Door securely locked
- Door open for too long
- Forend screw manipulated

23.10.2 Possible DoorMonitoring states of SmartHandles

- Door open/closed
- Door open for too long
- Locked (only for self-locking mortise locks)
- Handle in use/not in use

23.10.3 Possible DoorMonitoring states of SmartRelais 3

- Input 1 active/inactive
- Input 2 active/inactive
- Input 3 active/inactive
- Sabotage detection

24. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

https://www.simons-voss.com/en/documents.html

Software and drivers

Software and drivers can be found on the website:

https://www.simons-voss.com/en/service/software-downloads.html

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

https://www.simons-voss.com/en/certificates.html

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

https://faq.simons-voss.com/otrs/public.pl

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany

This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2025, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

SimonsVoss technologies

Made in Germany

A BRAND OF ALLEGION