



## Contents

1.	General safety instructions .....	9
2.	Product-specific safety instructions .....	10
3.	Meaning of the text formatting .....	11
4.	Intended use.....	12
5.	General.....	13
6.	Information on data protection.....	14
6.1	IT basic protection .....	14
6.1.1	What protection requirements do the data processed in the system have? .....	14
6.1.2	What IT infrastructure requirements are recommended?.....	14
6.2	Encryption .....	14
6.2.1	Is the data in System 3060 encrypted?.....	14
6.2.2	What data is encrypted? .....	14
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? .....	15
6.3.3	How long is personal data stored in the software? .....	15
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?.....	16
6.3.7	Can personal data be deleted from the software? .....	16
7.	Range of functions for AXM Plus.....	17
8.	System requirements .....	19
8.1	AXM services and ports used .....	19
9.	Installation.....	20
9.1	Run AXM as the administrator (recommended).....	21
9.2	Updating AXM.....	23
10.	First steps after a new installation.....	25
10.1	Best practice: setting up the locking system .....	27
10.2	Best practice: set up AX2Go .....	28
10.3	Best practice: Database protection .....	28
11.	Registration .....	29
11.1	Registration as a trial version.....	29

11.2	Registration with licence.....	34
11.3	Updating your licence.....	39
<b>12.</b>	<b>The AXM's structure .....</b>	<b>41</b>
12.1	Sorting and filtering.....	44
12.2	Installation wizards.....	46
12.3	Multiple options, same result .....	46
12.4	Global search .....	47
12.5	Working with AXM more effectively.....	48
12.5.1	Tab operation .....	48
12.5.2	Hotkeys .....	48
12.5.3	Creating additional objects .....	49
<b>13.</b>	<b>Organisational structure .....</b>	<b>50</b>
13.1	Creating authorisation groups.....	50
13.2	Creating a person group.....	51
13.3	Creating a schedule.....	53
13.4	Create time group .....	56
13.5	Deleting a time group .....	61
13.6	Deleting schedules .....	64
13.7	Creating a time switchover.....	65
13.8	Creating and editing public holidays.....	69
13.9	Creating and editing public holiday lists .....	72
13.10	Creating a location.....	77
13.11	Creating a building and assigning it to a location.....	80
13.12	Creating an area.....	83
13.13	Creating a hashtag.....	85
<b>14.</b>	<b>Persons and identification media.....</b>	<b>88</b>
14.1	Creating an identification medium .....	88
14.1.1	Creating transponders and cards.....	89
14.1.2	Creating PIN code keypads .....	96
14.1.3	Creating special identification media.....	101
14.1.4	Creating an AX2Go key.....	106
14.2	Duplicating an identification medium (including authorisations and settings) .....	107
14.3	Deleting an identification medium.....	108
14.3.1	Deleting a card/transponder .....	108
14.3.2	Deleting a PIN (PIN code keypad AX).....	113
14.3.3	Blocking an AX2Go key.....	114
14.4	Allowing an identification medium to open twice as long.....	114

14.5	Muting all locking devices for an identification medium.....	116
14.5.1	Muting all locking devices for a transponder or a card.....	116
14.5.2	Muting all locking devices for an AX2Go key.....	117
14.6	Allow accesses to be recorded by identification media (physical access list) .....	118
14.7	Restricting identification medium authorisations to specific times (time group) .....	119
14.8	Activating or deactivating identification medium once at specific times (activation and expiry date) .....	119
14.9	Handling defective identification media.....	123
14.9.1	Repairing/resynchronising .....	126
14.9.2	Resetting and replacing.....	131
14.9.3	Delete and replace .....	134
14.9.4	Take out of use and leave in project.....	142
14.9.5	Taking out of use and deleting from the project .....	149
14.10	Duplicating forgotten identification medium temporarily .....	155
14.10.1	Duplicating a forgotten transponder or card temporarily.....	155
14.11	Blocking lost/stolen identification media permanently.....	160
14.11.1	Blocking and replacing lost/stolen card/transponder permanently.....	161
14.11.2	Blocking a lost/stolen PIN code keypad permanently .....	166
14.12	Flag and reset returned identification medium (back to inventory) .....	171
14.12.1	Flagging and resetting returned card/transponder (back to inventory).....	171
14.13	Planning and tracking identification medium management tasks.....	174
14.13.1	Noting the issue date .....	175
14.13.2	Planning and logging battery replacement.....	178
14.13.3	Planning and logging return.....	183
14.14	Finding the identification medium or locking device again in the matrix.....	186
14.15	Exporting identification media as a list.....	186
14.15.1	Exporting AX2Go keys/cards/transponders as a list.....	186
14.15.2	Exporting PINs and PIN code keypads as a list .....	188
14.16	Viewing an identification medium's serial number and/or TID .....	190
14.16.1	Viewing a card's/transponder's serial number and TID.....	190
14.16.2	Viewing a PIN code keypad's serial number .....	191
14.17	Assigning persons to person groups .....	193
14.17.1	Assigning individual persons/identification media to a person group (in transponder window) .....	194
14.17.2	Assign a number of persons/identification media to person group (in the person group window) .....	196
14.18	Use identification media in multiple locking systems .....	199
14.18.1	Reuse identification medium in the same project .....	202
14.18.2	Reusing identification medium in other projects/databases.....	208
14.19	Managing AX2Go keys .....	211
14.19.1	Assigning keys for AXM Plus and higher .....	211



14.19.2	Blocking an AX2Go key.....	217
14.19.3	Deleting AX2Go keys .....	221
14.20	Setting the PIN length (PinCode AX) .....	222
14.21	Changing a PIN (PinCode AX).....	225
<b>15.</b>	<b>Doors and locking devices .....</b>	<b>228</b>
15.1	Creating a locking device .....	228
15.2	Duplicating the locking device (including authorisations and settings) .....	238
15.3	Delete locking device.....	240
15.3.1	Deleting an individual locking device using the matrix .....	241
15.3.2	Deleting several locking devices using the tab .....	242
15.4	Changing locking device type at later stage .....	245
15.5	Handling defective locking devices .....	247
15.5.1	Re-synchronise (repair) .....	252
15.5.2	Resetting and replacing .....	254
15.5.3	Delete and replace .....	259
15.5.4	Reset .....	264
15.5.5	Purge (only reset in database/software reset) .....	266
15.6	Assigning locking devices to buildings/locations.....	268
15.7	Moving locking devices to areas.....	270
15.7.1	Assigning individual locking devices to a different area (in the locking device window).....	271
15.7.2	Assign multiple locking devices to another area (in the area window) .....	273
15.8	Limiting authorisations for locking devices to specific times (schedule).....	276
15.9	Engaging and disengaging locking devices automatically with time switchover .....	278
15.10	Have accesses logged by locking device (access list) .....	284
15.11	Leaving the locking device open for longer, less time or permanently .....	286
15.12	Limit locking device read range (close range mode) .....	288
15.13	Muting a locking device (for battery warnings and programming) .....	289
15.14	Activating and deactivating card readers.....	291
15.15	Ignoring activation and expiry date of identification media .....	293
15.16	Setting up door monitoring (DoorMonitoring) .....	294
15.16.1	Setting up DoorMonitoring for locking cylinders.....	295
15.17	Changing the SmartRelay settings.....	301
15.17.1	Using internal and external antenna simultaneously .....	302
15.17.2	Invert outputs.....	303
15.17.3	Using the serial interface .....	305
15.17.4	Changing the signalling .....	306
15.18	Planning and tracking locking device management tasks.....	307
15.18.1	Note installation, replacement or removal date .....	309

15.18.2	Planning and logging battery replacement.....	310
15.19	Displaying all locking devices in a project.....	312
15.20	Exporting locking devices as a list.....	314
<b>16.</b>	<b>Permissions .....</b>	<b>317</b>
16.1	Changing individual authorisations (cross).....	317
16.2	Changing many authorisations (on identification media and/or locking devices).....	318
16.2.1	Allowing all or blocking all.....	318
16.2.2	Authorisation groups.....	322
16.2.3	Controlling authorisations in terms of time (schedules).....	338
16.3	Meaning of the authorisation crosses in the matrix.....	348
<b>17.</b>	<b>Locking systems.....</b>	<b>349</b>
17.1	Create locking system.....	349
17.1.1	Adding a card configuration.....	354
17.2	Changing locking system password.....	383
17.3	Replacing the locking system.....	387
17.4	Enable cards or transponders.....	389
17.5	Using a common locking level.....	392
17.5.1	Creating a common locking level.....	392
17.5.2	Creating transponders for common locking level.....	395
17.5.3	Authorising a transponder with common locking level.....	396
<b>18.</b>	<b>Synchronisation: Comparison between locking plan and reality.....</b>	<b>398</b>
18.1	Synchronising the locking device (including reading access list).....	399
18.1.1	Display locking device equipment and status.....	402
18.1.2	Displaying and exporting a locking device's access list.....	404
18.2	Identifying an unknown locking device.....	406
18.3	Re-setting the locking device.....	408
18.4	Synchronising an identification medium.....	409
18.4.1	Synchronise a card/transponder (including importing physical access list) .....	410
18.4.2	Synchronising a PIN code keypad.....	415
18.4.3	Synchronising AX2Go key.....	418
18.5	Identifying an unknown ID medium.....	420
18.5.1	Recognise unknown cards/transponders.....	420
18.5.2	Identifying unknown PIN code keypad.....	422
18.6	Resetting identification media.....	424
18.6.1	Resetting cards/transponders.....	424
18.6.2	Resetting the PIN code keypad.....	428
18.7	Viewing connected/supported programming devices.....	430

18.8	Checking the connection between database and cloud.....	432
<b>19.</b>	<b>Your personalised AXM interface.....</b>	<b>433</b>
19.1	Interchanging (transposing) doors and persons in the matrix.....	433
19.2	Select columns and rows in the matrix (enable/disable crosshairs) .....	434
19.3	Click to change authorisations .....	435
19.4	Hiding deactivated and defective identification media .....	436
19.5	Showing or hiding rows/columns in the matrix.....	437
19.6	Reading access list/physical access list during synchronisation.....	439
19.7	Limiting the number of access list entries in the database .....	441
19.8	Pinning tabs.....	442
19.9	Changing automatic numbering .....	443
19.10	Changing the language.....	445
19.11	Personalising reports and exports .....	445
19.12	Preventing generated reports from opening automatically.....	448
19.13	Personalising properties for person details .....	449
19.13.1	Hide and show existing fields.....	450
19.13.2	Creating your own fields .....	455
<b>20.</b>	<b>Administrative tasks.....</b>	<b>465</b>
20.1	Creating a backup .....	465
20.2	Restoring the backup.....	468
20.3	Exporting error logs.....	469
20.4	Displaying version number and licence key for the AXM installed.....	470
20.5	User management.....	472
20.5.1	Changing the user password.....	472
20.5.2	Increase password security.....	474
20.5.3	Name person as an AXM user.....	478
20.5.4	Assign tasks/user roles to AXM users .....	480
20.6	AX2Go settings.....	487
<b>21.</b>	<b>Statistics and logs.....</b>	<b>491</b>
21.1	Displaying and exporting a locking device's access list.....	491
21.2	Displaying and exporting physical access lists for cards/transponders .....	493
21.3	Display doors for which a specific identification medium is authorised .....	495
21.4	Displaying identification media which are authorised for a specific door.....	496
21.5	Displaying a locking device's equipment features .....	497
21.6	View statistics and warnings (dashboard).....	498
21.7	Tracking activities in the database (log) .....	500

21.7.1	Setting the log archiving period .....	502
21.8	Reports .....	503
21.8.1	Displaying the report for identification media issue.....	504
21.8.2	Exporting the data protection report (GDPR) .....	507
<b>22.</b>	<b>Background knowledge and explanations .....</b>	<b>512</b>
22.1	Identification media, locking devices and the locking plan .....	512
22.1.1	PIN Code G1 vs. PIN Code AX .....	514
22.1.2	AX2Go.....	517
22.1.3	Special identification media and their functions.....	520
22.2	Locking systems.....	521
22.3	Common locking levels .....	523
22.4	“Engaging”, “opening”, “locking”, etc.....	524
22.5	Synchronisation of database and actual state.....	526
22.6	Access and physical access lists .....	527
22.7	Event management.....	528
22.7.1	Time groups and schedules.....	528
22.7.2	Time switchovers.....	532
22.7.3	Time budget (AX2Go and virtual network).....	540
22.8	Authorisation groups .....	543
22.9	Person groups .....	544
22.10	Passwords used.....	546
22.11	Buildings and locations .....	547
22.12	Areas.....	548
22.13	Hashtags.....	549
22.14	DoorMonitoring.....	549
22.14.1	Possible DoorMonitoring states of locking cylinders.....	550
22.14.2	Possible DoorMonitoring states of SmartHandles.....	550
22.14.3	Possible DoorMonitoring states of SmartRelais 3.....	550
22.15	Reports .....	551
22.15.1	Scaling image files.....	551
22.16	Cards and locking device IDs.....	552
22.16.1	Card templates .....	556
<b>23.</b>	<b>Help and other information .....</b>	<b>558</b>

## 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 Plus, 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* [▶ 41]).
  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* [▶ 398]).
-

### 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:

<b>Example</b>	button
<input checked="" type="checkbox"/> Example <input type="checkbox"/> Example	checkbox
<input checked="" type="radio"/> Example	Option
[Example]	Tab
"Example"	Name of a displayed window
Example	Upper programme bar
<b>Example</b>	Entry in the expanded upper programme bar
<b>Example</b>	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
<i>Example</i>	Field
<i>Example</i>	Name of a (Windows) service
<i>Example</i>	Commands (e.g. Windows CMD commands)
<b>Example</b>	Database entry
[Example]	MobileKey type selection

## 4. Intended use

The AX Manager Plus (AXM Plus) 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 assistants
- 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



Plus Edition

We are now advancing to the next level in locking system management with the Plus Edition. This edition features selected functions (compare with LSM Basic Online).

You have 64,000 locking devices and 64,000 identification media (transponders/cards) per locking system at your disposal.

## 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. The latest versions of our products offer you a higher level of security since they are always state-of-the-art. Multi-level encryption methods are used (AES, 3DES).

#### 6.2.2 What data is encrypted?

Within the system's own communication network, no personal data is processed. It is 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. Due to the end-to-end encryption type used, there is no need to also encrypt the transmission paths.

### 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 Plus



Projects/locking systems	Multiple projects with multiple locking systems
Users	Two users (Admin/AdminAL)
Number of locking devices	64,000 per locking system
Number of credentials	64,000 per locking system
Locking devices and identification media supported	<ul style="list-style-type: none"> <li>■ G2 components</li> <li>■ AX components</li> </ul>
	<ul style="list-style-type: none"> <li>■ Digital Cylinder AX</li> <li>■ Locking Cylinder 3061</li> <li>■ SmartHandle AX</li> <li>■ SmartHandle 3062</li> <li>■ SmartRelay 3063 (G2)</li> <li>■ SmartRelay 2 3063</li> <li>■ Padlock</li> <li>■ Padlock AX</li> <li>■ SmartLocker AX</li> <li>■ Furniture lock (G2)</li> <li>■ AX2Go</li> </ul>
Programming devices	<ul style="list-style-type: none"> <li>■ SmartCD.G2/SmartCD2.G2</li> <li>■ SmartCD.MP</li> <li>■ SmartStick AX</li> </ul>

<p>Web services</p>	<ul style="list-style-type: none"> <li>■ Registration</li> <li>■ AX2Go invites</li> <li>■ Cloud services (data transfer only with end-to-end encryption)</li> </ul>
---------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------

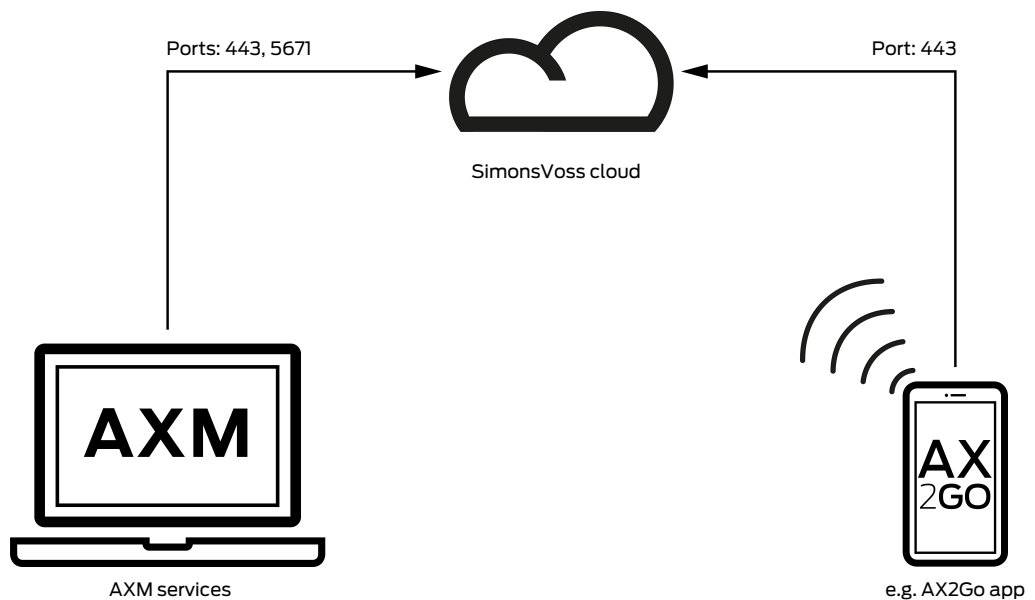
You can upgrade at any time if your version reaches its limits.

## 8. System requirements

### AXM Classic

Operating system	<ul style="list-style-type: none"> <li>■ Windows 10</li> <li>■ Windows 11</li> </ul>
CPU	2.66 GHz or faster (Intel, AMD) No support for ARM processors under System 3060
Main memory	4 GB or more
Free memory space	500 MB (physical); during installation approx. 1 GB
Display	<ul style="list-style-type: none"> <li>■ 13 inches (≈ 33 cm) or more</li> <li>■ 1280×1024 or more</li> </ul>
Supported MS SQL Edition	SQL Server Express Local DB

### 8.1 AXM services and ports used

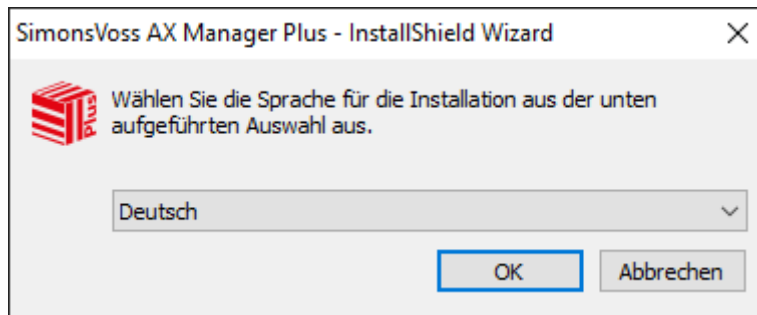


Port	Function
443	HTTPS data transfer
5671	Identification (if not available, fall back to port 443)



## 9. Installation

- ✓ System requirements fulfilled for the AXM Plus (see *System requirements* [▶ 19]).
- 1. Execute the set-up file.
  - ↳ The InstallShield wizard will open.



- 2. Select the language in which the is AXM Plus to be installed.
  - ↳ Set-up checks whether additional software needs to be installed.
- 3. Install the additional software displayed if required.
  - ↳ The AXM Plus set-up will open.



- 4. Follow the AXM Plus set-up.
  - ↳ AXM Plus is installed.

## 9.1 Run AXM as the administrator (recommended)

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

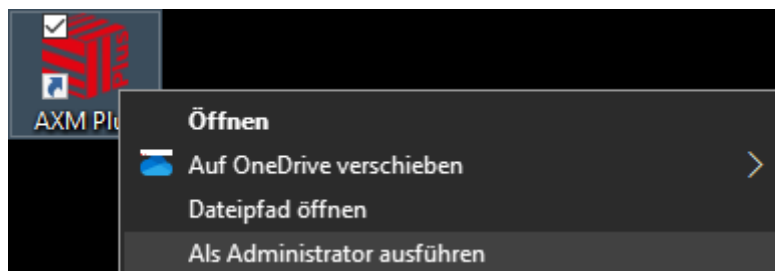
### Manual start as administrator

- ✓ AXM Plus installed.
- ✓ Administrator rights available.

1. Locate the shortcut or the AXM Plus 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 Plus 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 Plus as the administrator.

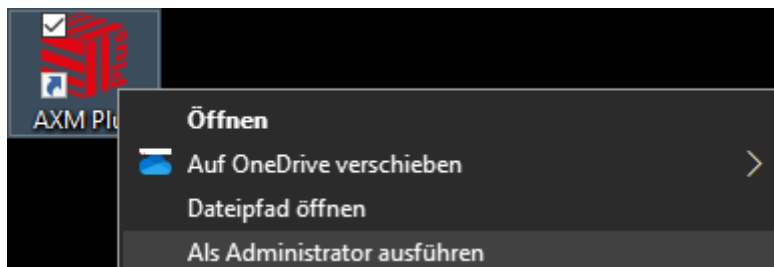
Consequently, SimonsVoss recommends that the properties of the link to AXM Plus be set so that the AXM Plus is always run as administrator using this shortcut.

- ✓ AXM Plus installed.
- ✓ Administrator rights available.

1. Locate the shortcut or the AXM Plus icon.

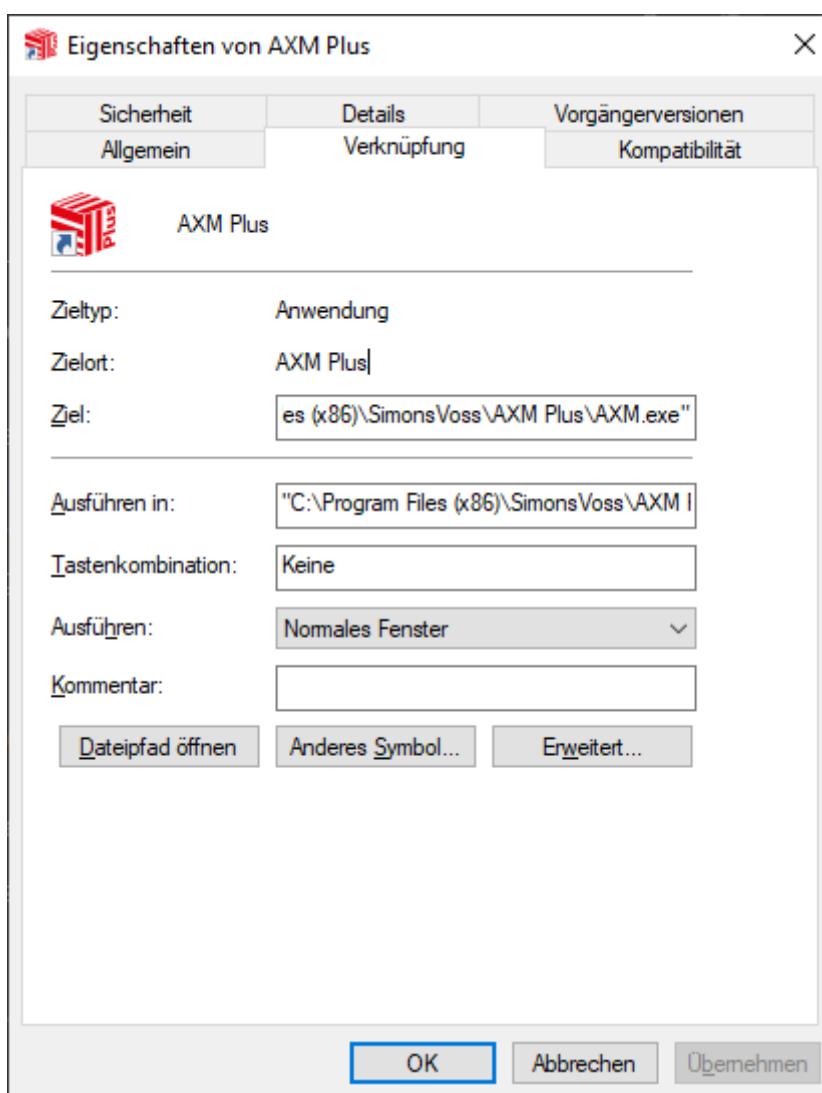


2. Right-click on the shortcut menu to open the context menu.
3. Click on the **Properties** entry with your name.



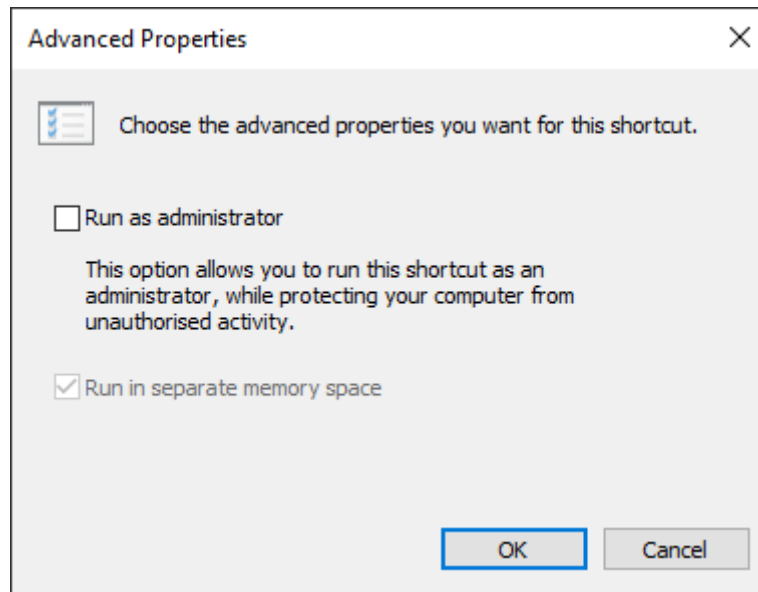
↳ The "AXM ... Properties" window will open.

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 Plus via this link in the future, AXM Plus will automatically run as the administrator.

## 9.2 Updating AXM

With the latest AXM Plus, you have the best software and hardware support. This is why your AXM Plus checks whether updates are available and also offer them for installation every time it launches. Back up your database (see *Creating a backup* [▶ 465]) before updating.

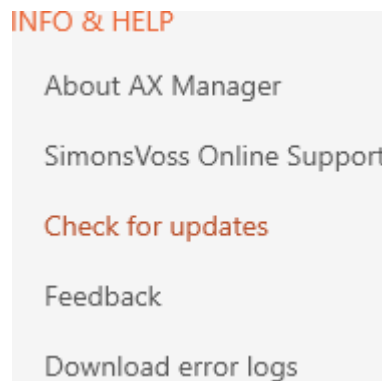
See *Displaying version number and licence key for the AXM installed* [▶ 470] to view the currently installed version of your AXM Plus instead.

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

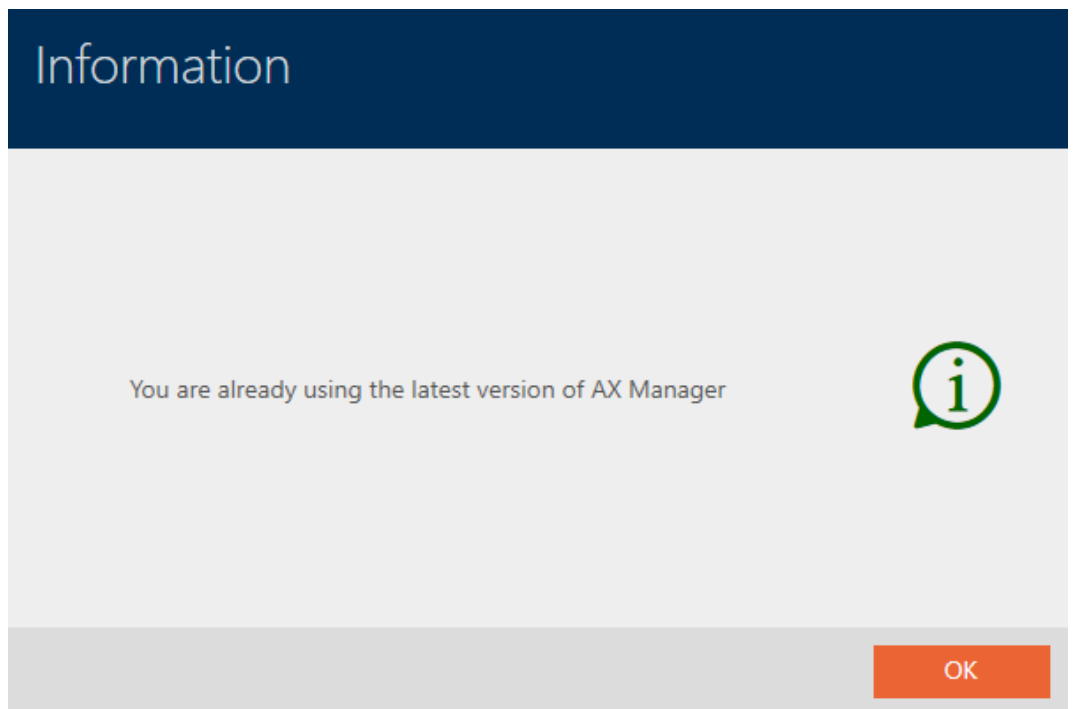
- ✓ Database backed up.
1. Click on the orange AXM icon **AXM**.
    - ↳ AXM bar opens.



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 Plus is up to date, you will see this window:





## 10. First steps after a new installation

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

Willkommen bei AXM Plus  
Zum Starten können Sie ein bestehendes Projekt laden oder ein neues Projekt erstellen

Neu Löschen Umbenennen

Ein neues Projekt anlegen

Projektname

Benutzername

Neues Kennwort

Kennwort wiederholen

Sie haben sich bisher noch nicht an diesem Projekt angemeldet.  
Deshalb müssen Sie zunächst ein Kennwort für den Admin-Benutzer festlegen.  
Das Kennwort muss mind. 8 Zeichen lang sein.

Qualität

Erstellen

2.0.24023.801 Abbrechen

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.

Quality

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 \[► 472\]](#)).

You can change the locking system password (see *Changing locking system password* [▶ 383]).

### 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 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 Plus for the first time

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

1. Add locking system
2. Add locking device
3. Add transponder



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

However, before setting up a large locking system, plan things out first in preparation (see *Best practice: setting up the locking system* [▶ 27]).

If you are working with a locking system for the first time, you will find explanations and background information here: *Background knowledge and explanations* [▶ 512].

## 10.1 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 as possible.

As a basic rule, the easiest way is to prepare the organisational structure first (see *Organisational structure* [▶ 50]).

Experience has shown that the following approach is best:

1. Create locations (see *Creating a location* [▶ 77]).
2. Create building (see *Creating a building and assigning it to a location* [▶ 80]).
3. Create areas (see *Creating an area* [▶ 83]).
4. Create the first schedule (see *Creating a schedule* [▶ 53]).
5. Create all required time groups (see *Create time group* [▶ 56]).
6. Create additional schedules, setting the time groups directly for each schedule while doing so.
7. Create authorisation groups (see *Authorisation groups* [▶ 322]).
8. Create person groups (see *Creating a person group* [▶ 51]).
9. If necessary, Configure cards in the locking system (see *Enable cards or transponders* [▶ 389]).
10. Create identification media and assign them directly to their authorisation groups and time groups when they are created (see *Creating transponders and cards* [▶ 89], *Creating a person group* [▶ 51] and *Restricting identification medium authorisations to specific times (time group)* [▶ 119]).
11. Create locking devices and assign them directly to authorisation groups, areas and schedules when they are created (see *Creating a locking device* [▶ 228], *Creating an area* [▶ 83] and *Limiting authorisations for locking devices to specific times (schedule)* [▶ 276]).
12. Synchronise locking devices (see *Synchronising the locking device (including reading access list)* [▶ 399]).
13. Synchronise identification media (see *Synchronise a card/transponder (including importing physical access list)* [▶ 410]).

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 authorisation groups directly in the window for the created identification medium

- Schedule and authorisation group directly in the window for the created locking device

Background knowledge for you to take into account for time management and authorisation groups:

- *Event management* [[▶ 528](#)]
- *Authorisation groups* [[▶ 543](#)]

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.

## 10.2 Best practice: set up AX2Go

The following concept has proven effective in the set-up and initial operation of AX2Go (mobile keys):

1. Install AXM Plus (see *Installation* [[▶ 20](#)]).
  2. Register AXM Plus (see *Registration* [[▶ 29](#)]).
  3. Set up your locking system with locking devices and transponders (see *Best practice: setting up the locking system* [[▶ 27](#)]).
  4. Configure your AX2Go settings (see *AX2Go settings* [[▶ 487](#)]).
- ↳ AX2Go is ready for use. You can now create and send invitations, for example (see *Managing AX2Go keys* [[▶ 211](#)]).

## 10.3 Best practice: Database protection

You can further enhance the security level of your AXM Plus 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.

## 11. Registration

### 11.1 Registration as a trial version

1. Launch AXM Plus.
  - ↳ Your AXM Plus will notify you that you still need to register it.



2. Click the `Start {0} day trial period` button.
  - ↳ Your AXM Plus will inform you that you also need a SimonsVoss ID during the trial period.




3. Click the `Next` button.
  - ↳ The registration form will open.

## Registrierung Ihres AX Managers

Bitte geben Sie Ihre Registrierungsdaten ein

Bitte füllen Sie dieses Formular vollständig aus und generieren Sie eine Lizenzanforderung.



Registrieren Sie eine neue Testlizenz

Edition AXM Plus ▼

Unternehmen

Adresse

PLZ  Ort

Land  ▼

Kontaktperson

E-Mail

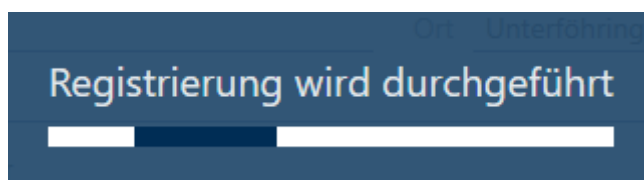
Tel.

Lizenzschlüssel XXXX-XXXX-XXXX-XXXX-XXXX

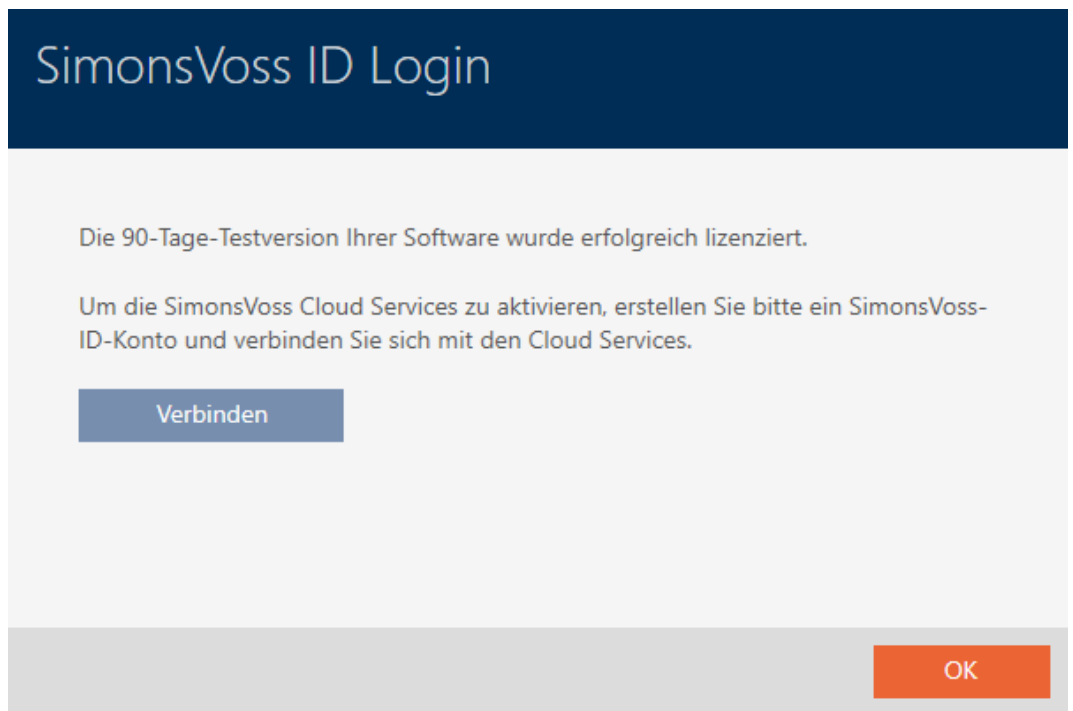
[Nutzungsbedingungen](#) akzeptieren

Registrieren
Abbrechen

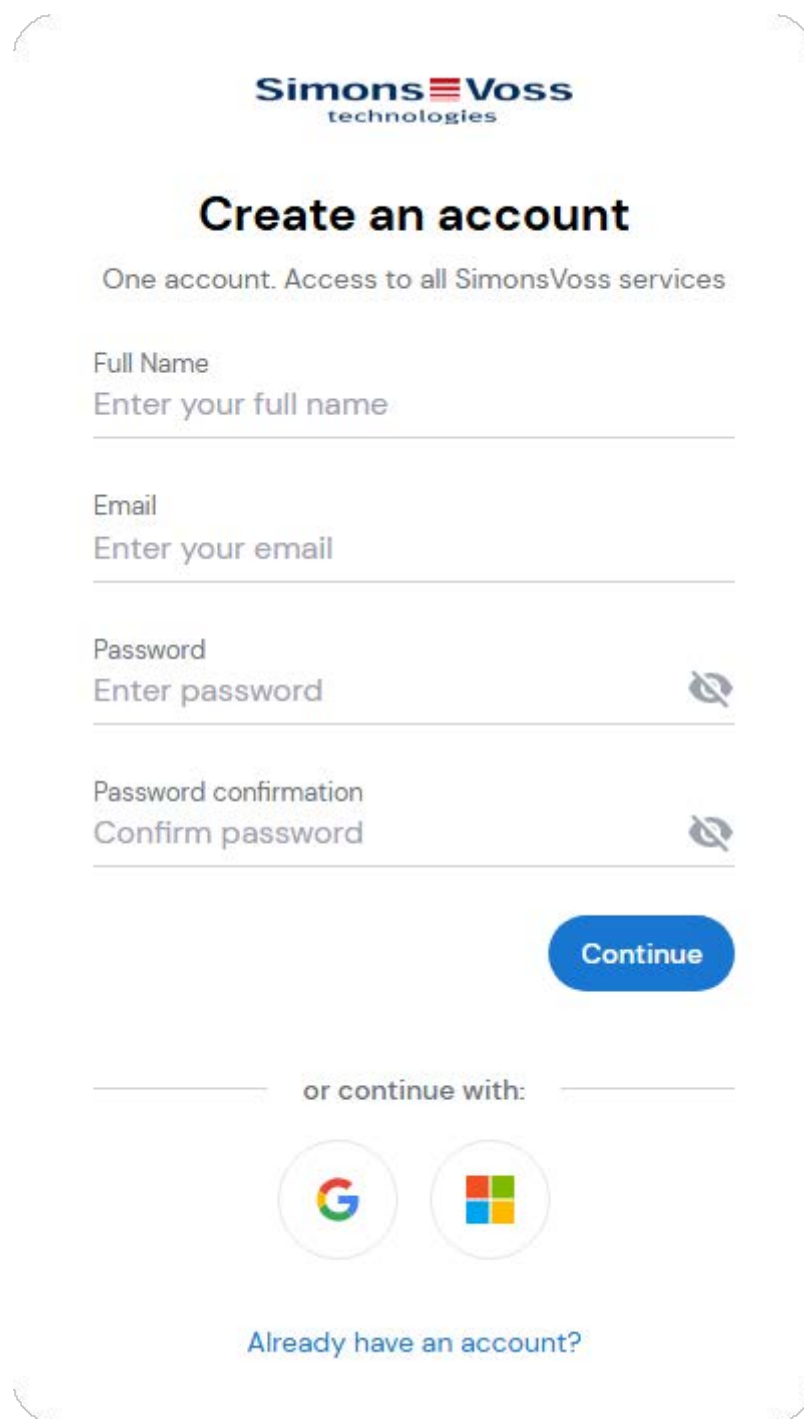
4. Fill in the registration form (the *Licence key* field is greyed out for trial registration).
5. Accept the terms of use.
6. Click the **Register** button.
  - ↳ Registration is in progress.



- ↳ Registration was successful.
- ↳ Your AXM Plus will prompt you to create a SimonsVoss ID.



7. Click the **Connect** button.
  - ↳ The website for creating a SimonsVoss ID will open.



The screenshot shows the 'Create an account' page for SimonsVoss technologies. At the top is the company logo. Below it is the heading 'Create an account' and a sub-heading 'One account. Access to all SimonsVoss services'. The form consists of four input fields: 'Full Name' with the placeholder 'Enter your full name', 'Email' with 'Enter your email', 'Password' with 'Enter password' and a toggle icon, and 'Password confirmation' with 'Confirm password' and a toggle icon. A blue 'Continue' button is positioned to the right of the password fields. Below the form, there is a section 'or continue with:' with two circular icons for Google and Microsoft. At the bottom, there is a link 'Already have an account?'.

8. Enter the required data or use your Google/Microsoft account. If you already have a SimonsVoss ID, you can use it and do not need to create a new one.
9. Press "Continue" to forward your details.
  - ↳ Registration request for a SimonsVoss ID has been sent.





## Registration confirmation

We sent a sign up link to you at

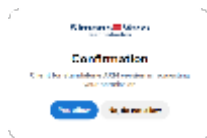
[\[Redacted Email Address\]](#)

If you do not receive a confirmation email, please check your spam folder. Also, please verify that you entered a valid email address in our sign-up form

[Resend email](#) | [Change email address](#)

10. Please check your email account and click on the confirmation link in the email from SimonsVoss.

↳ Website for linking your SimonsVoss ID to your AXM Plus will then open.



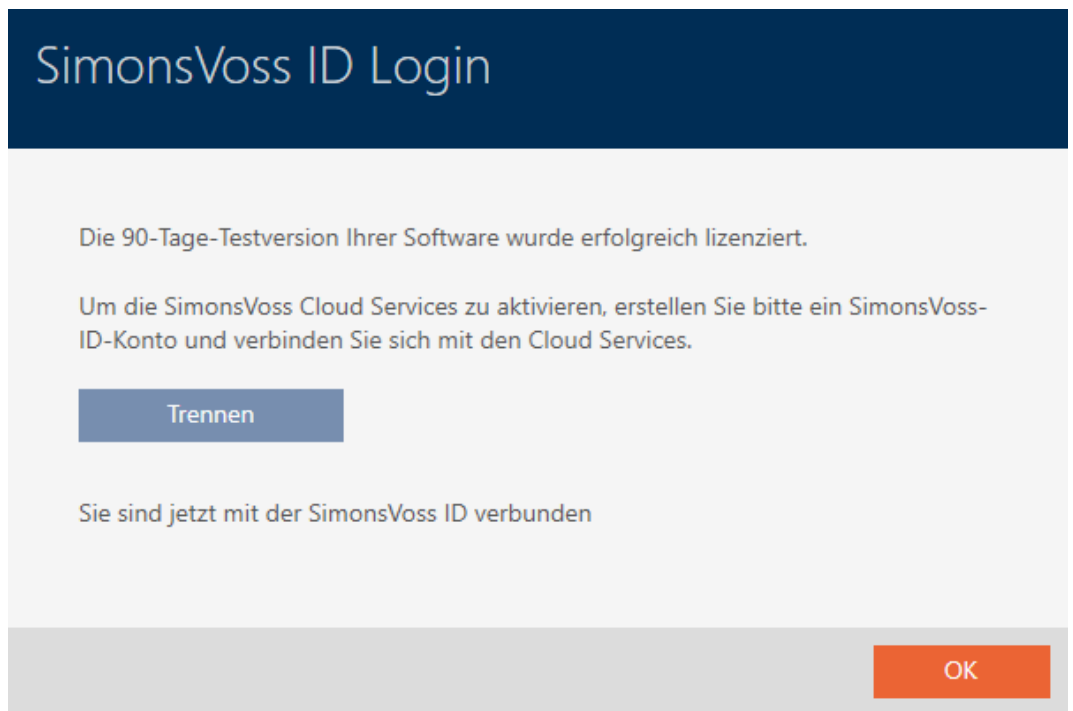
11. Click on “Yes, allow” to link your SimonsVoss ID and AXM Plus.

↳ Website and AXM Plus inform you that the link has been established.



## Success

You have successfully authorized the device.



12. Click on the **OK** button.

- ↳ Registration completed and valid for 90 days.
- ↳ AXM Plus will open a log-in window for you to log in.

## 11.2 Registration with licence

You need a licence key to register. You can obtain this key from one of our specialist retail partners.

1. Launch AXM Plus.
  - ↳ Your AXM Plus will notify you that you still need to register it.




2. Click the **Registering an existing licence** button.
  - ↳ The registration form will open.

## Registrierung Ihres AX Managers

Bitte geben Sie Ihre Registrierungsdaten ein

Bitte füllen Sie dieses Formular vollständig aus und generieren Sie eine Lizenzanforderung.



Verbinden Sie sich mit Ihrer SimonsVoss-ID mit der Cloud, um Ihre bestehende Lizenz zu registrieren

**Verbinden**

Registrieren Sie eine neue Lizenz

Edition AXM Plus

Unternehmen

Adresse

PLZ  Ort

Land ▼

Kontaktperson

E-Mail

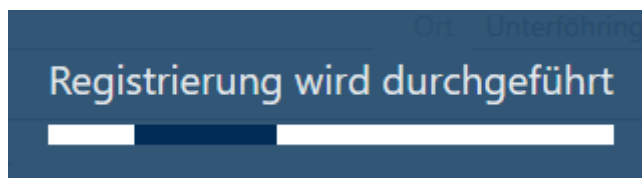
Tel.

Lizenzschlüssel

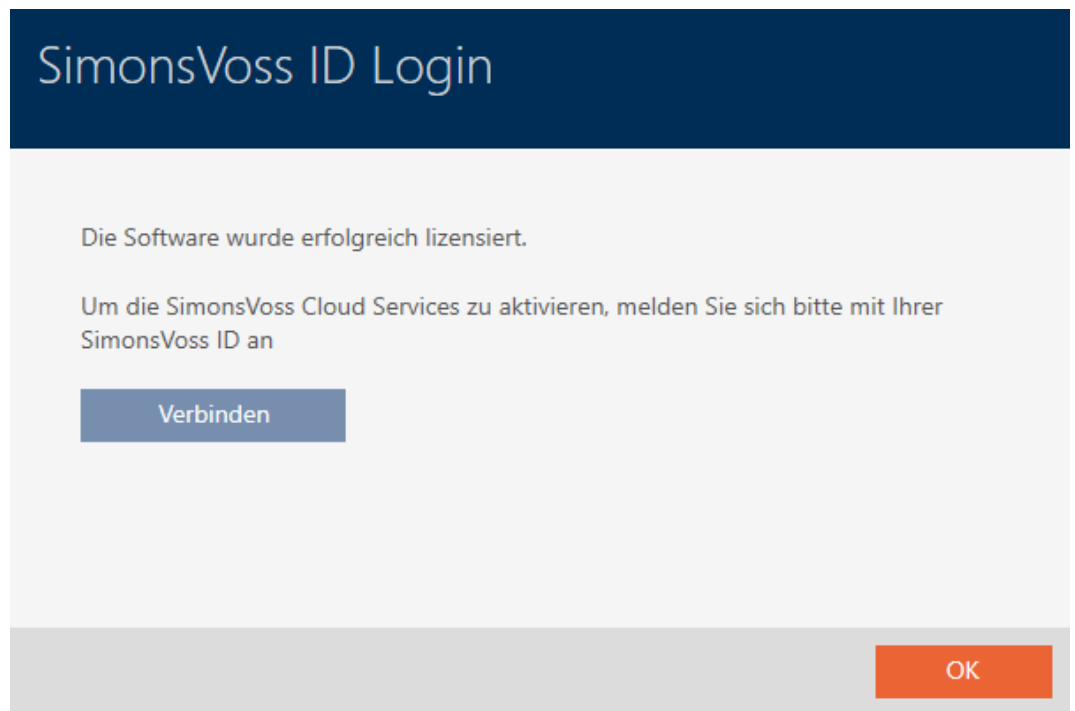
Nutzungsbedingungen akzeptieren

Lizenzdatei importieren
Registrieren
Starte 90-tägige Testphase
Abbrechen


3. Complete the registration form, including the *Licence key* field.  
If you have already registered the AXM Plus and linked it to your SimonsVoss ID, you can skip registration and connect directly to your SimonsVoss ID. The licence is then taken from the SimonsVoss ID.
4. Accept the terms of use.
5. Click the **Register** button.  
↳ Registration is in progress.



- ↳ Registration was successful.
- ↳ Your AXM Plus will prompt you to log in with your SimonsVoss ID.




6. Click the `Connect` button.
  - ↳ Website for login with a SimonsVoss ID will open.



## Sign in



Log in to continue using SimonsVoss services

Email  
Enter your email

Password  
Enter your password 

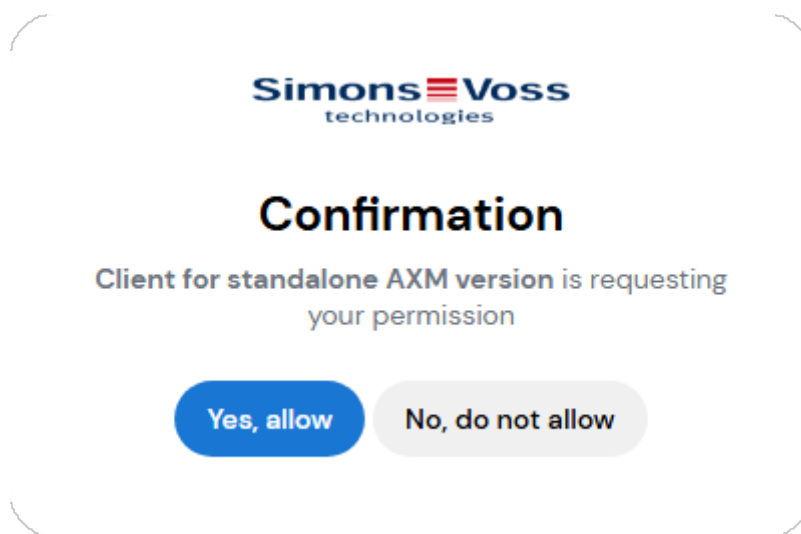
[Continue](#)

or continue with:

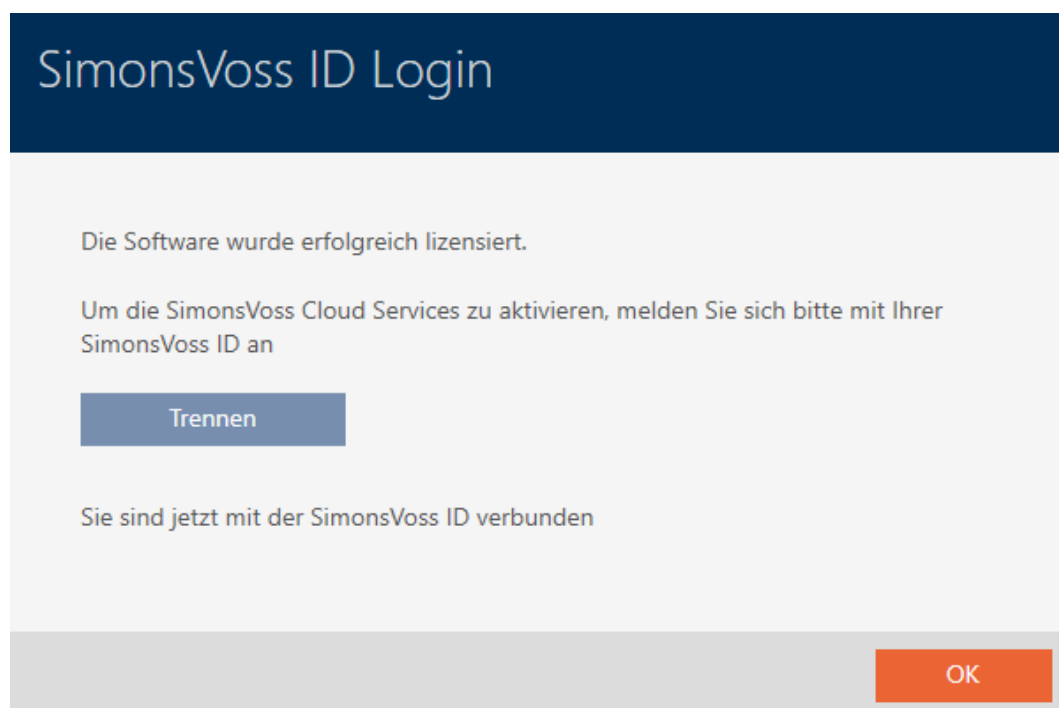
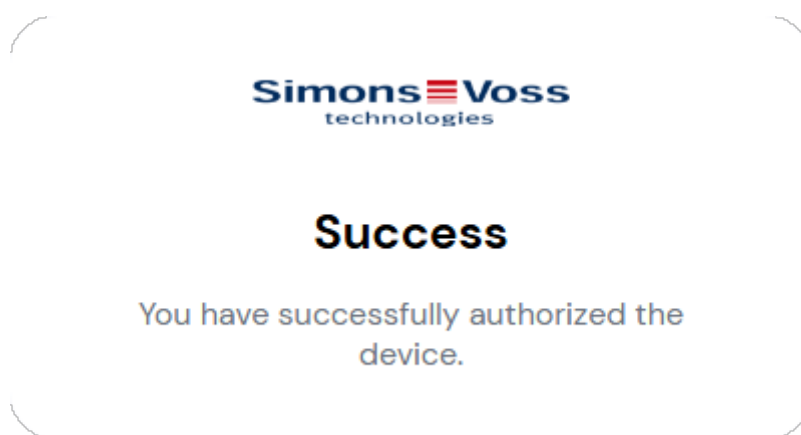
 

[Can't log in?](#) | [Create an account](#)

7. Enter the required data or use your Google/Microsoft account. If you already have a SimonsVoss ID, you can use it and do not need to create a new one.
8. Press "Continue" to forward your details.
  - ↳ Website for linking your SimonsVoss ID to your AXM Plus will then open.

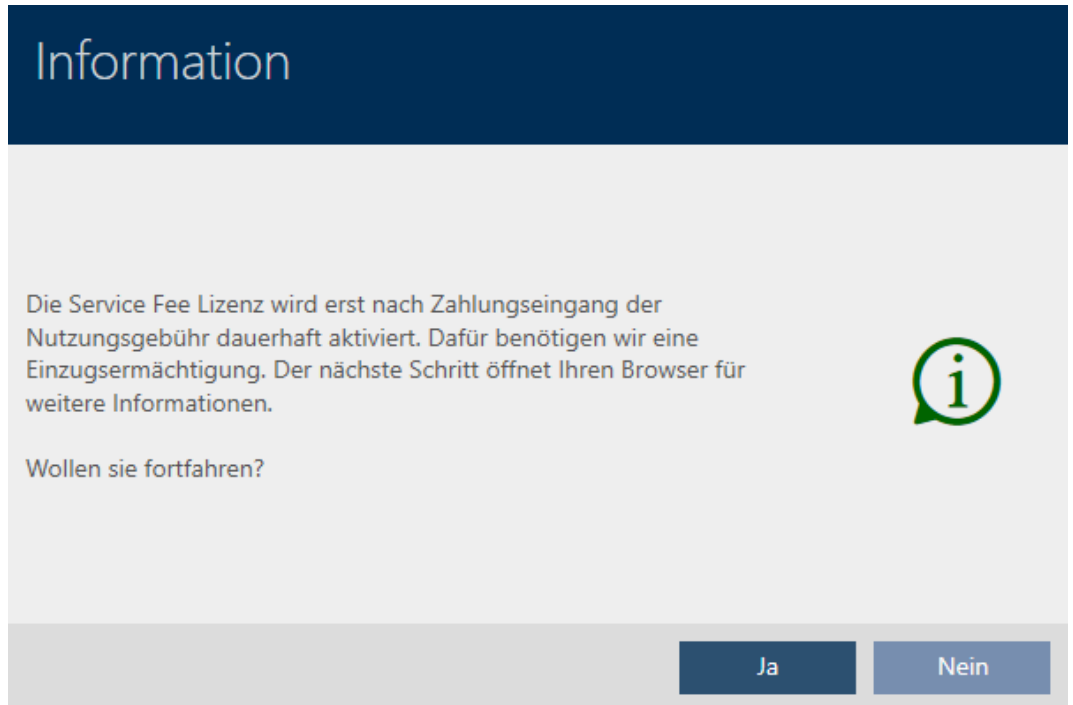


9. Click on "Yes, allow" to link your SimonsVoss ID and AXM Plus.  
↳ Website and AXM Plus inform you that the link has been established.



10. Click on the **OK** button.

↳ A notice about the service fee licence status will appear.



11. Click **Yes** to open the browser or click **No** to create a project.  
(Example: **Yes**)

↳ Website with further information opens.

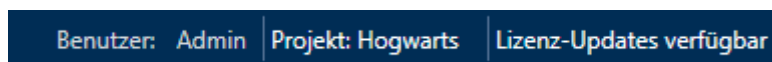
↳ Registration and link with SimonsVoss ID completed.

### 11.3 Updating your licence

Thanks to the connection with our licence service, the information on your software licence is always up to date.

As soon as changes are made (e.g. by extending the scope of services), the change is displayed in the AXM Plus footer when you start the application.

You can apply the changes by clicking on *Licence updates available*.



## Lizenzdetails

Edition	AXM Plus
Registriert am	15.10.2024
Ablaufdatum	15.10.2025
Registriert für	SimonsVoss Technologies GmbH
	<a href="#">Anbieter kontaktieren</a>
	<a href="#">Überprüfen</a>
	<a href="#">Lizenzschlüssel</a>
	<a href="#">Lizenz ändern</a>
AX2Go Lizenzen	1000
SmartSync Lizenzen	0
LockNode-Lizenzen	0
Lizenzschlüssel	<a href="#">Lizenzschlüssel</a>
Service Fee Lizenz	<input checked="" type="checkbox"/>
Gültig bis	12.09.2024
Zahlungseingang bestätigt	<input checked="" type="checkbox"/>

Nach Lizenz-Updates suchen
Lizenz ändern

Schließen

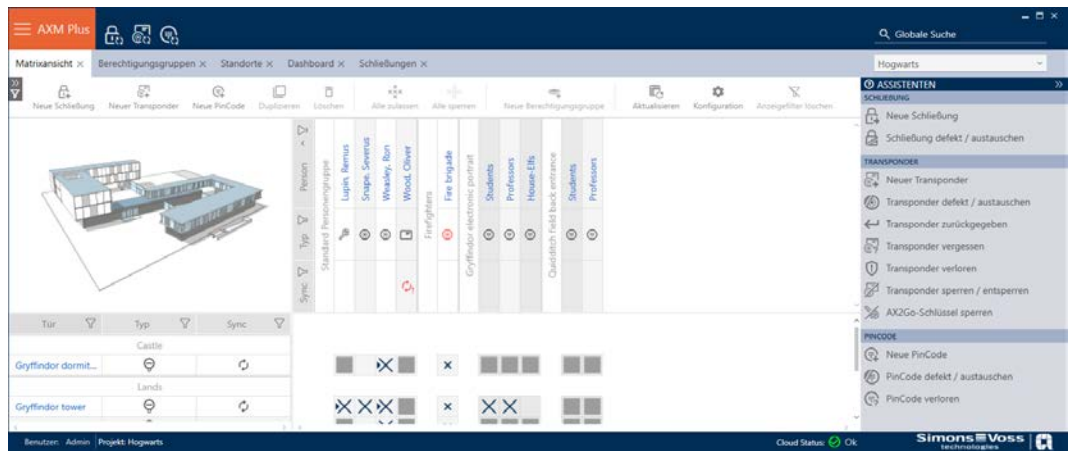
Scroll down in the window that opens and click on **Check for licence updates**.

Nach Lizenz-Updates suchen
Lizenz ändern

Die Lizenz wurde erfolgreich aktualisiert

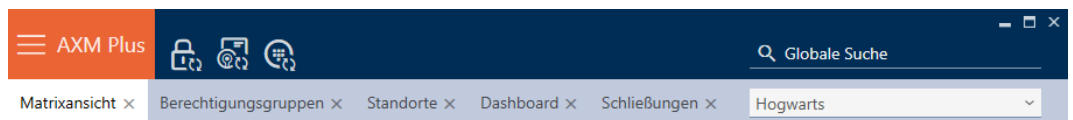


## 12. The AXM's structure



The AXM Plus 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 \[▶ 48\]](#)).

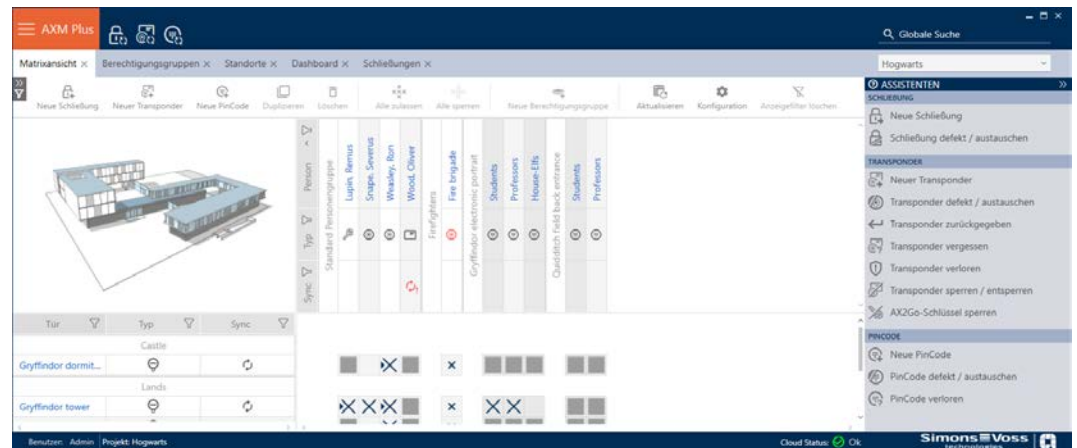
There are three buttons next to the AXM button to skip directly to synchronisation of locking devices and identification media.



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](#) [[▶ 47](#)]).



## Matrix section



The matrix section is the engine room behind your AXM Plus. 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](#) [[▶ 44](#)]).

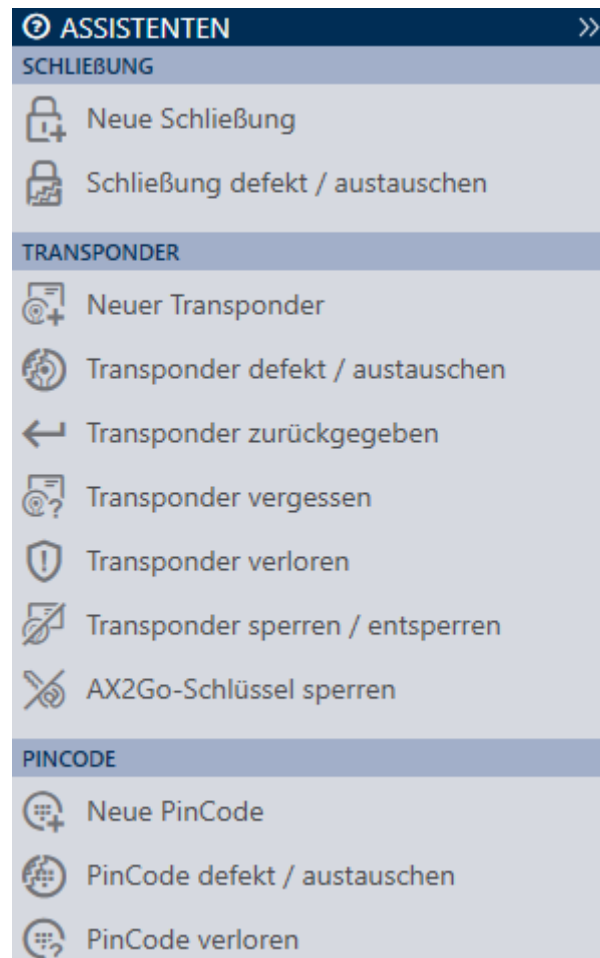
Each row normally represents a locking device and each column represents an identification medium. This identification medium's authorisation for this locking device is indicated where rows and columns meet (see [Permissions](#) [[▶ 317](#)]). There are basically two different main states:

- 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](#) [[▶ 398](#)]). 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:

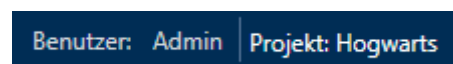
## Wizard menu



There is a wizard menu on the right side of your AXM Plus. 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 Plus is the dashboard (see [View statistics and warnings \(dashboard\) \[▶ 498\]](#)). 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)* [[▶ 500](#)]).

The log can also be accessed via the AXM bar.

## 12.1 Sorting and filtering


Large lists and tables can become confusing.

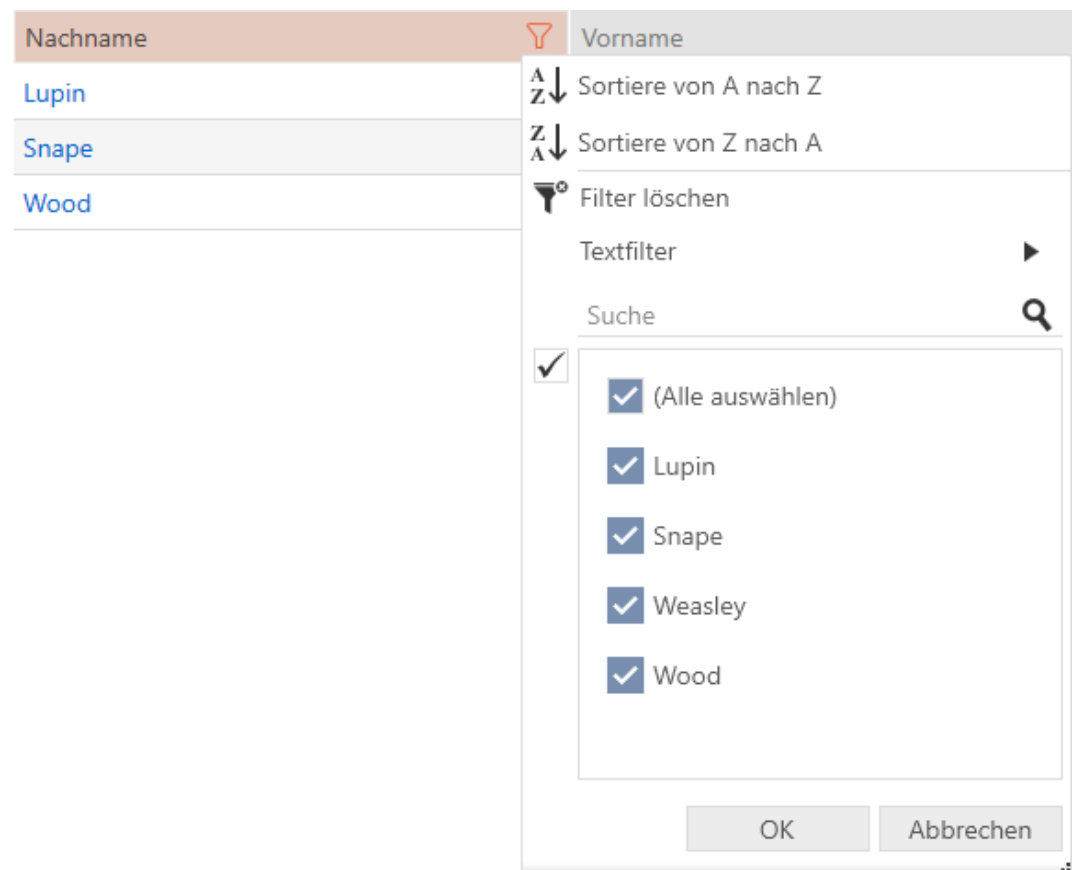
The AXM Plus provides you with sorting and filtering functions to simplify things.

### Sorting

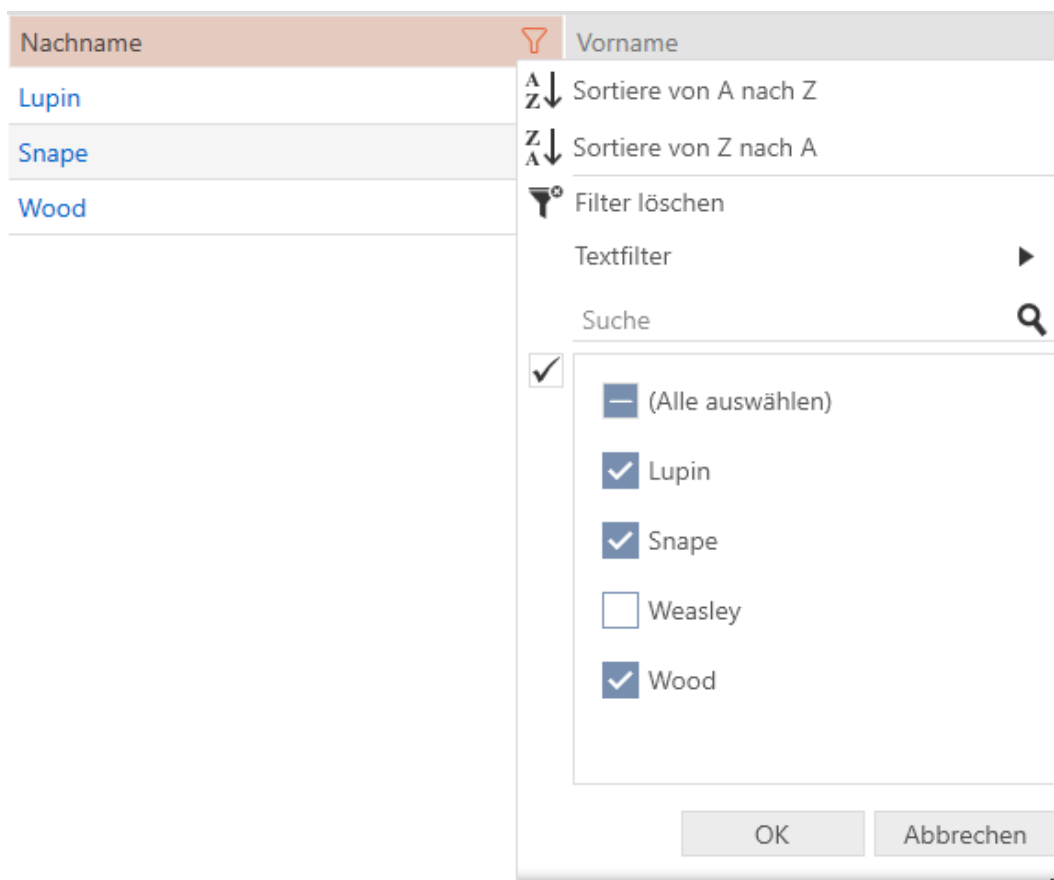
1. Click on one of the column or row headings.
  - ↳ Entries will then be sorted by this column/row.
2. Click on the same heading again.
  - ↳ The sort order is reversed.

### Filtering

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



2. Adjust the filters.

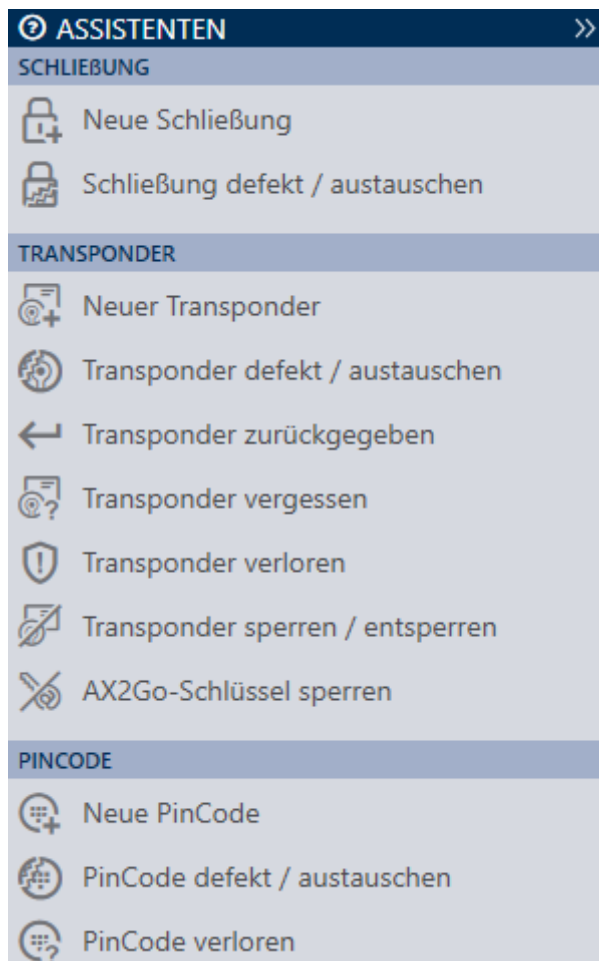


3. Click on the **OK** button.

- ↳ The filter menu will close.
- ↳ Entries will now be filtered when displayed.

Nach	Vorn:	S/N	Typ	Sync	Status	Zeitg	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L					
Snape	Severus	0301A4D				Zeitgrupp	
Wood	Oliver						

## 12.2 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.

## 12.3 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.

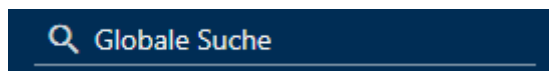
For example, you can delete an entry in the matrix in two ways:



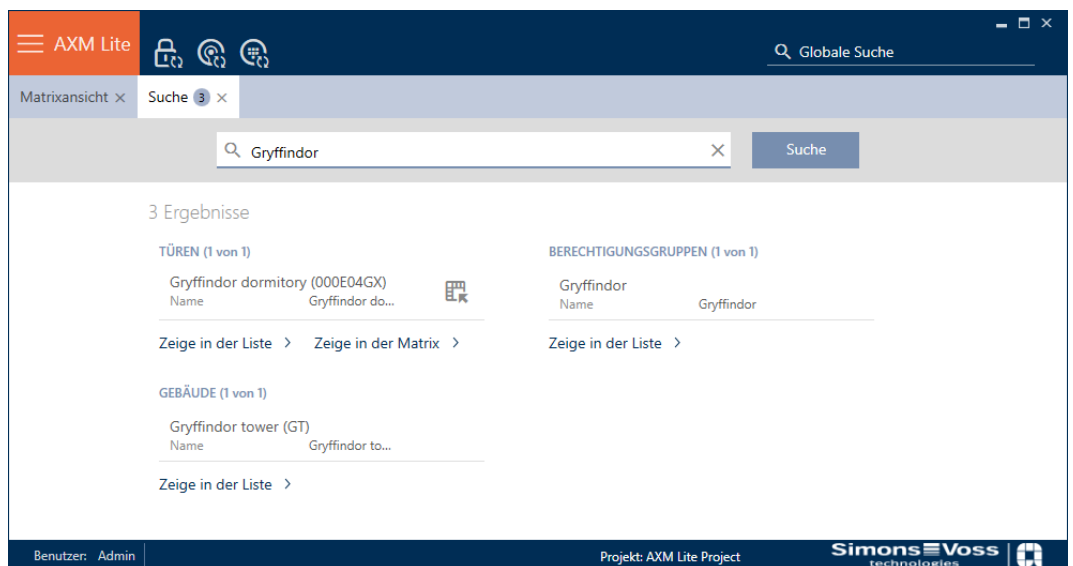
1. Using the matrix bar: **Löschen**
2. Using the context menu: **Löschen**

Both ways delete the entry.

## 12.4 Global search

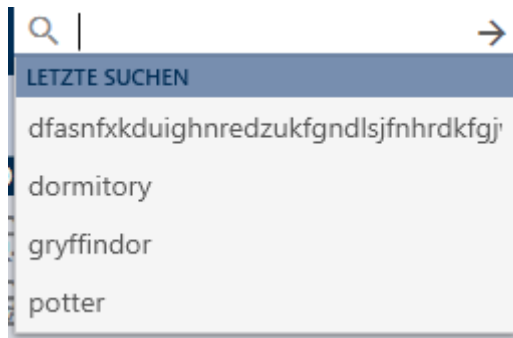


The global search in AXM Plus searches all entries and lists them in an overview:



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



## 12.5 Working with AXM more effectively

### 12.5.1 Tab operation

AXM Plus 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.

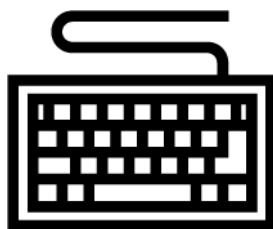
Frequently used tabs can also be opened automatically when the program is launched (see *Pinning tabs* [▶ 442]).

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 Plus is greyed out when opened.

### 12.5.2 Hotkeys



Key shortcut	Response
Tab	Skips to next input field.
Shift + Tab	Skips to the previous input field.
Ctrl + tab	Skips to next tab.



Key shortcut	Response
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)

### 12.5.3 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 Plus 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.

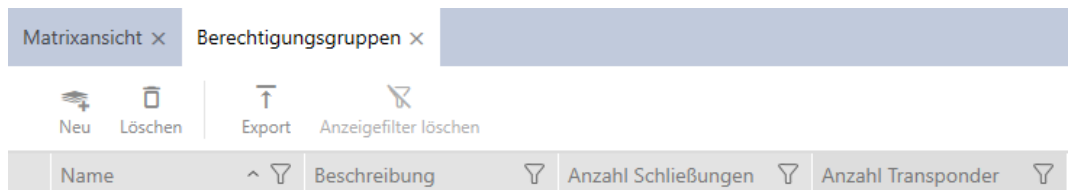
## 13. Organisational structure


### 13.1 Creating authorisation groups

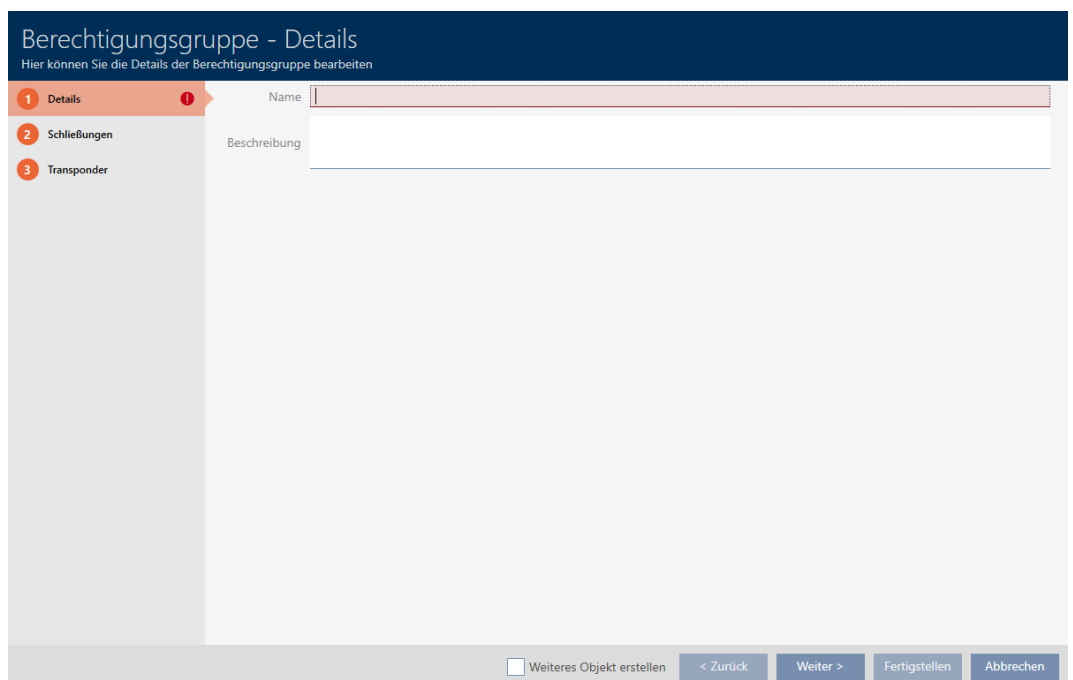
1. Click the orange AXM button .
  - ↳ AXM bar opens.



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 authorisation group will open.



4. Enter a name for your authorisation group in the *Name* field.
5. Enter a description in the *Description* field.
6. Click on the **Finish** button.
  - ↳ The window for the new authorisation group will close.
- ↳ The new authorisation group is listed.

Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder
Gryffindor		0	0

### 13.2 Creating a person group

Person groups are a very useful structure for your locking system (also see *Person groups* [▶ 544]).

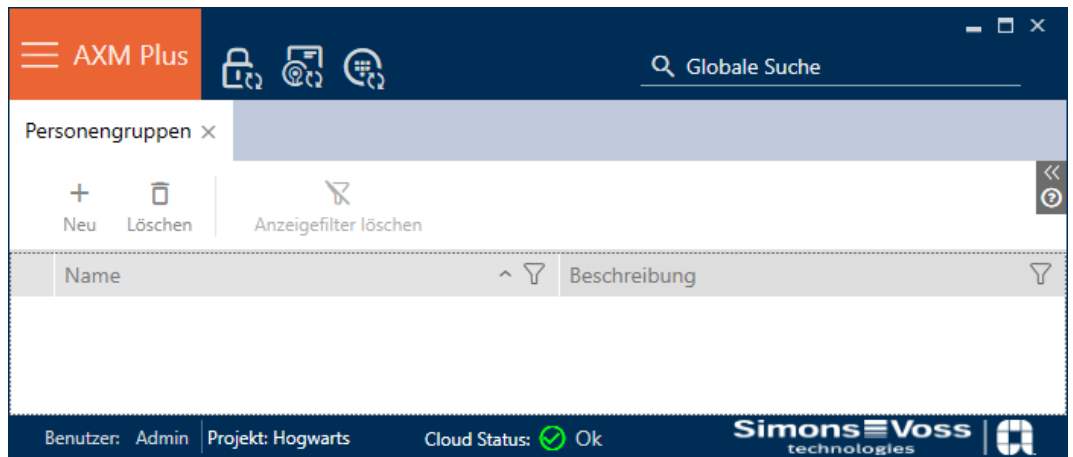
1. Click the orange AXM button .
  - ↳ AXM bar opens.



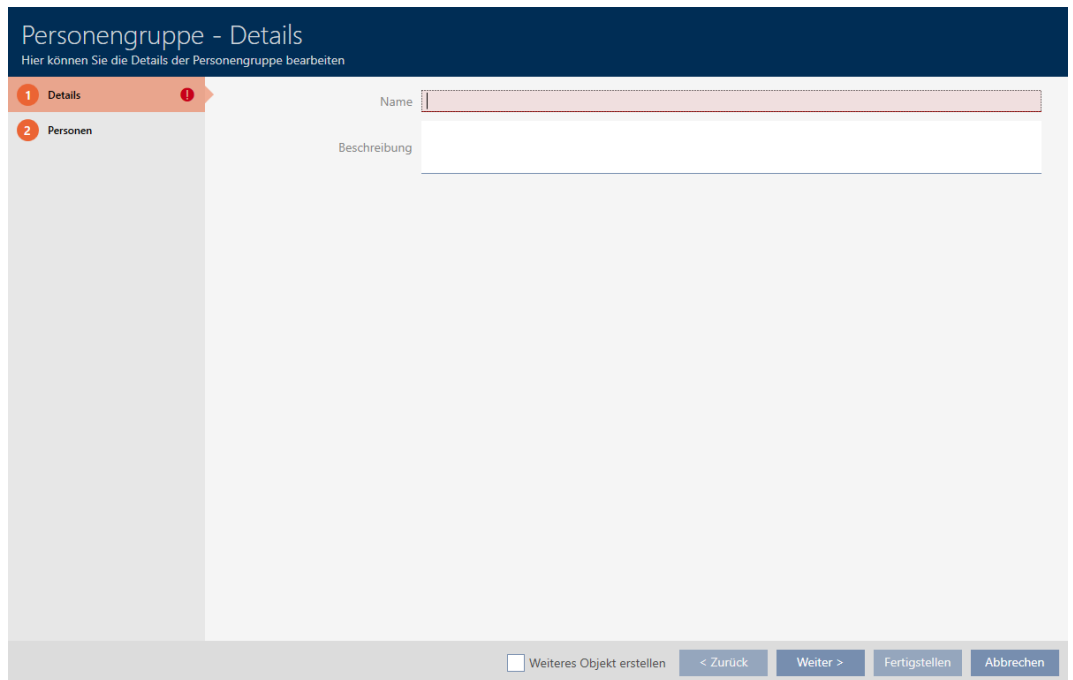
2. Select the **Person groups** entry in the | LOCKING SYSTEM CONTROL | group.



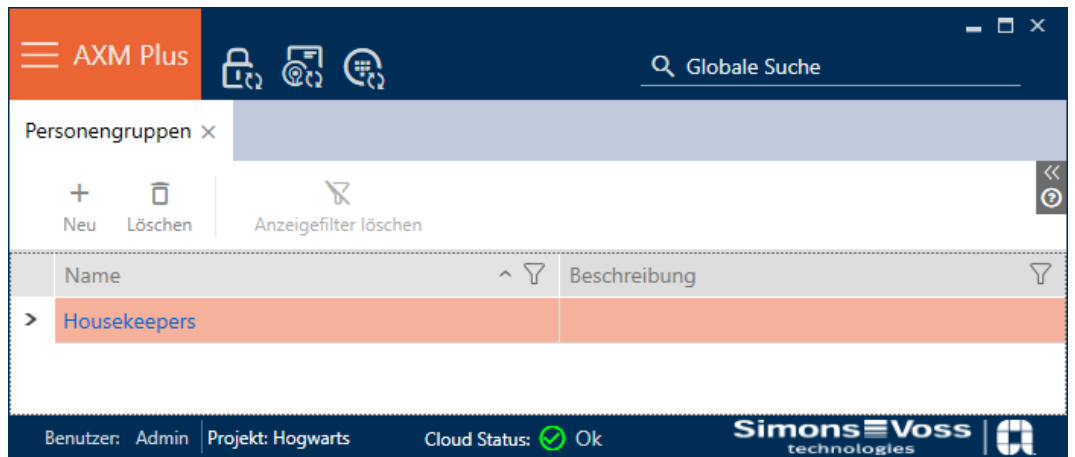
- ↳ The [Person groups] tab will open.




3. Click on the **New** **+** button.
  - ↳ The "Person group" window will open.



4. Enter the name of your person group in the *Name* field.
5. Enter a description of your person group in the *Description* field if required.
6. Click on the **Finish** button.
  - ↳ "Person group" window closes.
  - ↳ Newly created person group is now listed.

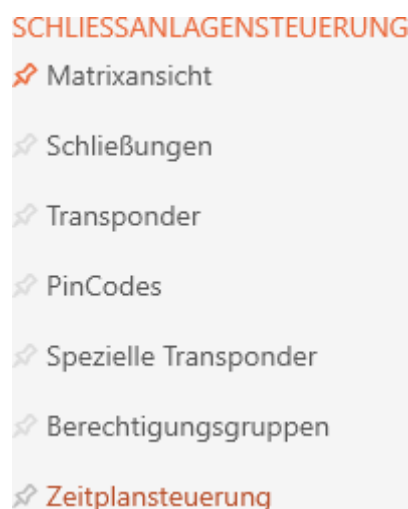


### 13.3 Creating a schedule


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

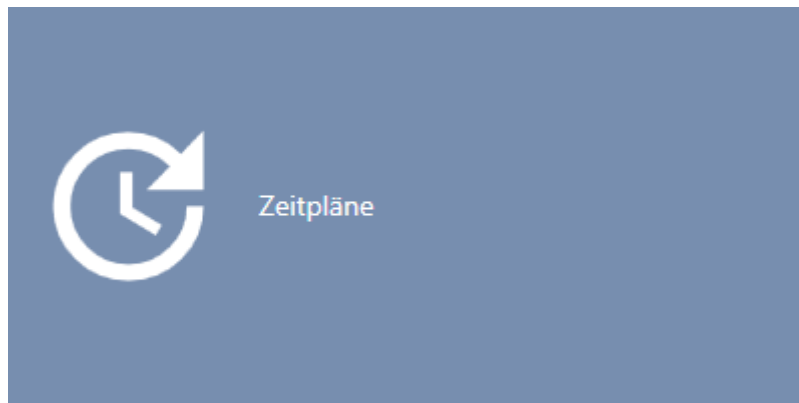


2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

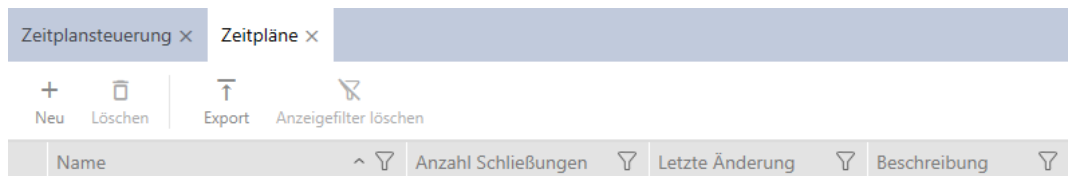


- ↳ The AXM bar will close.
- ↳ The [Time schedule control] tab will open.

3. Click on the **Time schedules**  button.

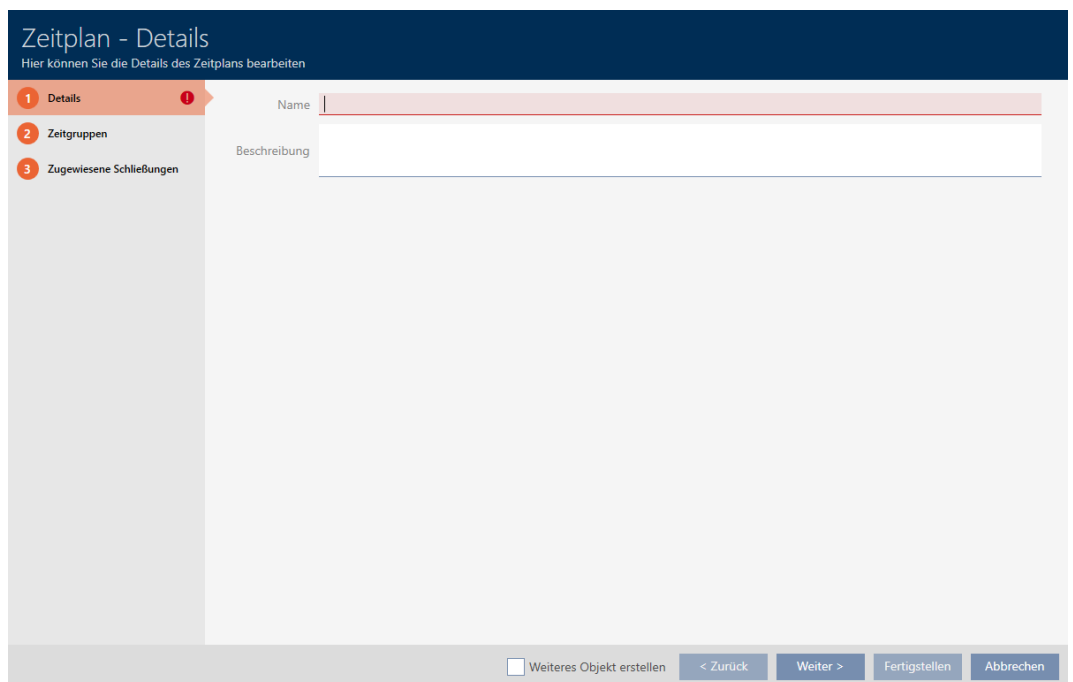


↳ The [Time schedules] tab will open.



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.

Zeitplan - Details  
Hier können Sie die Details des Zeitplans bearbeiten

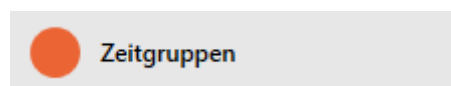
1 Details  
2 Zeitgruppen  
3 Zugewiesene Schließungen

Name

Beschreibung

Weiteres Objekt erstellen

7. Click on the  Time groups tab.



↳ Window switches to the "Time groups" tab.

Zeitplan - Zeitgruppen  
Hier können Sie die Zeitgruppen für Transponder konfigurieren

1 Details  
2 Zeitgruppen  
3 Zugewiesene Schließungen

Name

Modus  Berechtigt  Nicht berechtigt  Zeiten beschränken

Für PinCode Tastatur

ZEITEN

	Von	Bis	Tage
<input type="checkbox"/>	00:00	24:00	<input type="checkbox"/> Mo <input type="checkbox"/> Di <input type="checkbox"/> Mi <input type="checkbox"/> Do <input type="checkbox"/> Fr <input type="checkbox"/> Sa <input type="checkbox"/> So <input type="checkbox"/> Sonntag

Weiteres Objekt erstellen



**NOTE**

**First time group created automatically**

You need at least one time group for AXM Plus time management. AXM Plus 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 [▶ 56]*).  
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 [▶ 341]* and *Adding locking devices to the schedule [▶ 338]* if required.
  - ↳ Schedule has been created and is listed.

Zeitplansteuerung ×		Zeitpläne ×	
Name	Anzahl Schließungen	Letzte Änderung	Beschreibung
> Zeitplan 1	1	06.05.2021 11:53:10	


**13.4 Create time group**

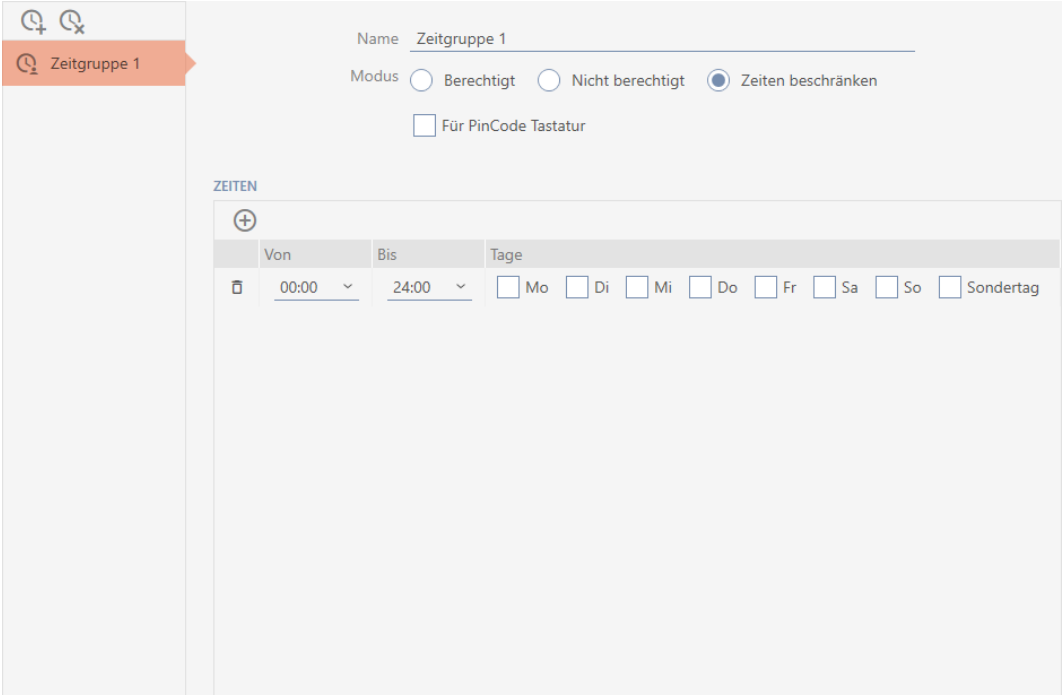
As a general rule, the following applies: All settings in a time group apply to each schedule.

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

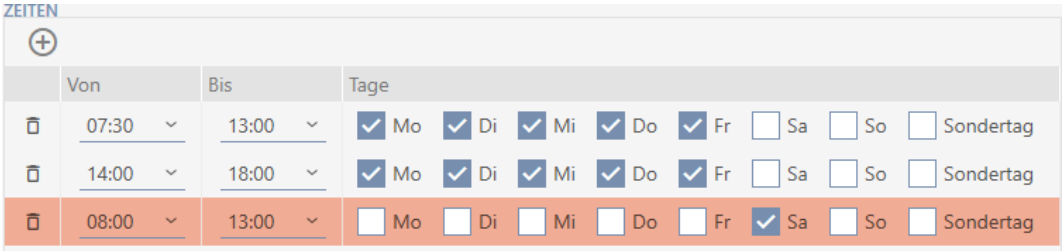
<p><input checked="" type="radio"/> Authorised</p>	<p>All identification media in this time group are authorised for all locking devices in this schedule as specified in the matrix or authorisation groups.</p> <p><input checked="" type="radio"/> Authorised corresponds to a time limit that permits use between 0–24 hours every day (i.e. it is effectively not a limit at all); see screenshot:</p> <div style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <p><b>ZEITEN</b></p> <p>+ Von 00:00 Bis 24:00 Tage <input checked="" type="checkbox"/> Mo <input checked="" type="checkbox"/> Di <input checked="" type="checkbox"/> Mi <input checked="" type="checkbox"/> Do <input checked="" type="checkbox"/> Fr <input checked="" type="checkbox"/> Sa <input checked="" type="checkbox"/> So <input checked="" type="checkbox"/> Sondertag</p> </div> <p>If you try to save this time limit in this way, the AXM Plus automatically changes the mode to <input checked="" type="radio"/> Berechtig.</p>
----------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------



<p><input checked="" type="radio"/> Not authorised</p>	<p>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.</p> <p><input checked="" type="radio"/> Not authorised corresponds to a time limit that does not allow use on any day (i.e. effectively restricted at all times); see screenshot:</p> 
<p><input checked="" type="radio"/> Limit times</p>	<p>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.</p>



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




	Von	Bis	Tage
<input type="checkbox"/>	07:30	13:00	<input checked="" type="checkbox"/> Mo <input checked="" type="checkbox"/> Di <input checked="" type="checkbox"/> Mi <input checked="" type="checkbox"/> Do <input checked="" type="checkbox"/> Fr <input type="checkbox"/> Sa <input type="checkbox"/> So <input type="checkbox"/> Sondertag
<input type="checkbox"/>	14:00	18:00	<input checked="" type="checkbox"/> Mo <input checked="" type="checkbox"/> Di <input checked="" type="checkbox"/> Mi <input checked="" type="checkbox"/> Do <input checked="" type="checkbox"/> Fr <input type="checkbox"/> Sa <input type="checkbox"/> So <input type="checkbox"/> Sondertag
<input type="checkbox"/>	08:00	13:00	<input type="checkbox"/> Mo <input type="checkbox"/> Di <input type="checkbox"/> Mi <input type="checkbox"/> Do <input type="checkbox"/> Fr <input checked="" type="checkbox"/> Sa <input type="checkbox"/> So <input type="checkbox"/> Sondertag

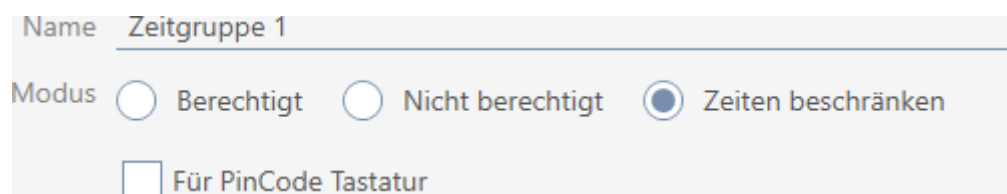
- Different time intervals for the same days (e.g. a store has its lunch break between 13:00 and 14:00)
- Different time intervals for different days (e.g. a store is only open in the morning on Saturdays)

More information; see *Time groups and schedules* [▶ 528].

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* [▶ 69]).

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

- ✓ Schedule created (see *Creating a schedule* [▶ 53]).
  - ✓ Schedule window open (see *Creating a schedule* [▶ 53]).
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.



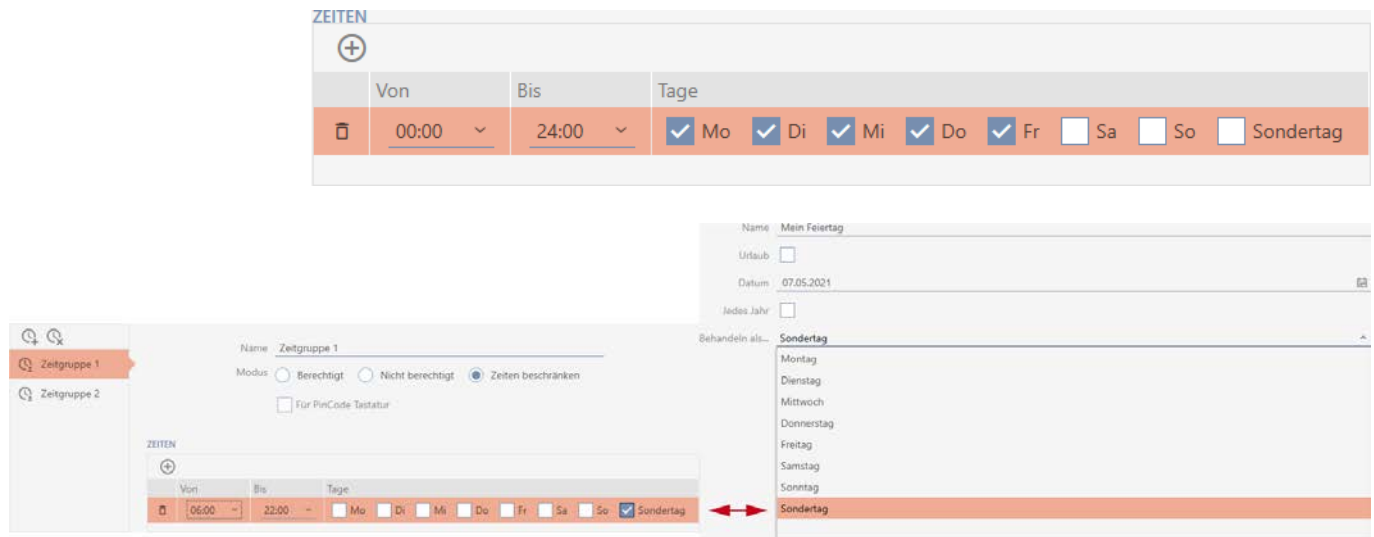
#### NOTE

##### Time groups for PIN code keypads

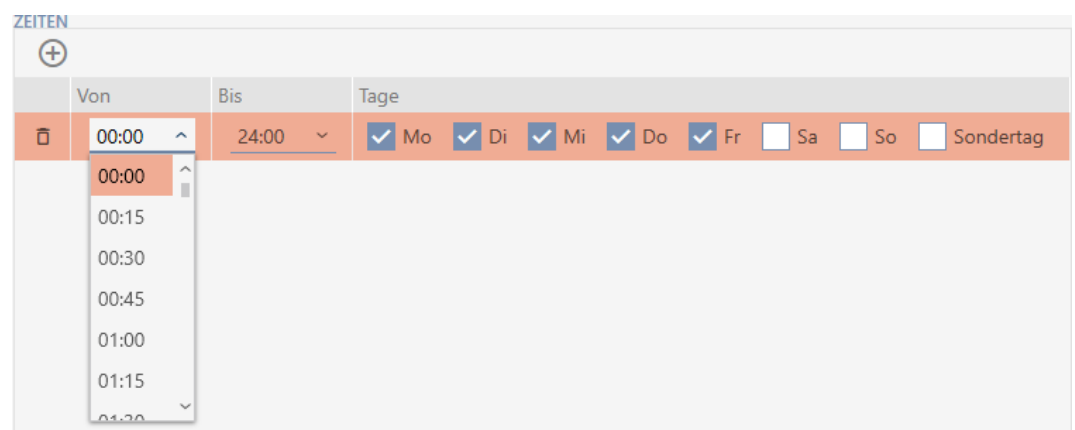
PIN code keypads use the G1 protocol. This is why PIN code keypads require their own time groups. These time groups can also only be used for PIN code keypads.

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.

### 13.5 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.

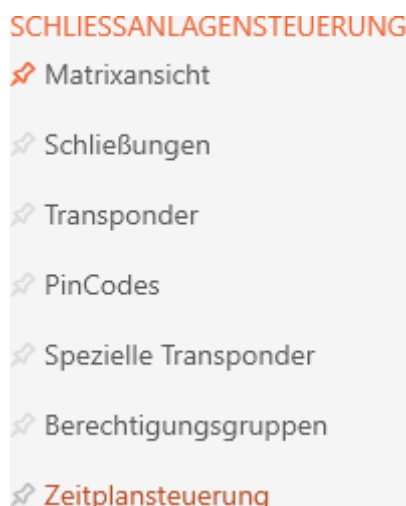
All identification media that were previously assigned to the deleted time group are then no longer assigned to a time group and must be added to one on an individual basis where necessary (see *Adding identification medium to time group* [▶ 341]).

- 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.


1. Click on the orange AXM icon .  
↳ 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.

Zeitplansteuerung x		Zeitpläne x	
Name	Anzahl Schließungen	Letzte Änderung	Beschreibung
> Zeitplan 1	1	06.05.2021 11:53:10	

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

### Zeitplan - Details

Hier können Sie die Details des Zeitplans bearbeiten

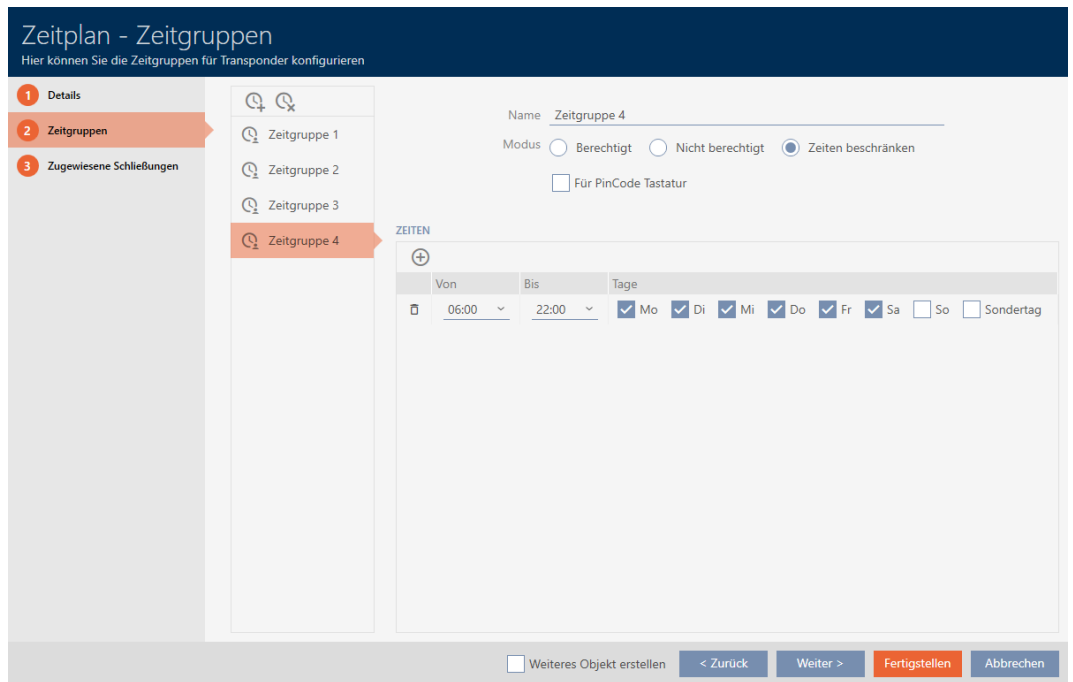
- 1 Details
- 2 Zeitgruppen
- 3 Zugeordnete Schließungen


Name

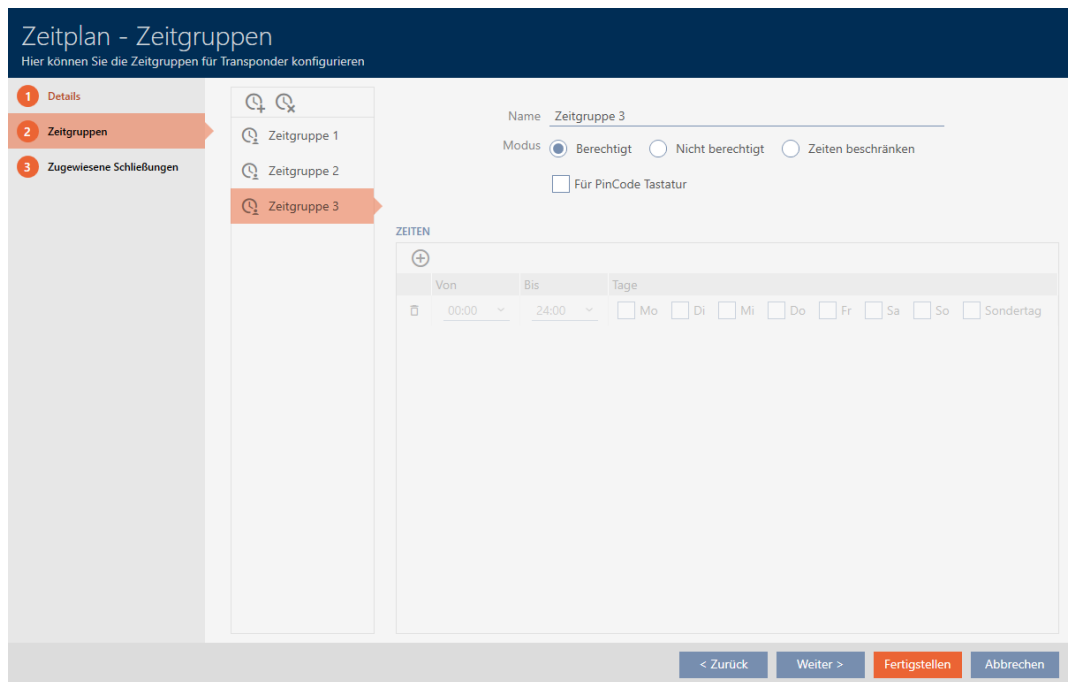
Beschreibung

Weiteres Objekt erstellen
< Zurück
Weiter >
Fertigstellen
Abbrechen

- 5. Click on the 2 **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.



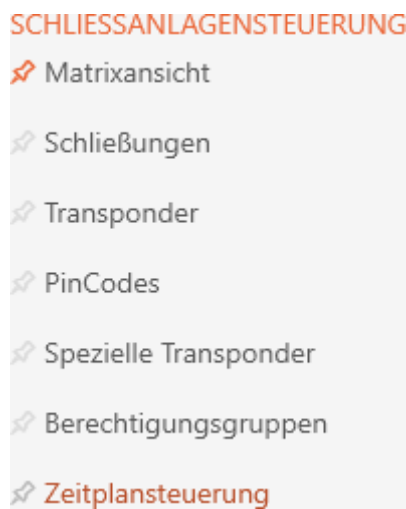
### 13.6 Deleting schedules

- ✓ Schedules are no longer assigned to a locking device (see *Adding locking devices to the schedule* [▶ 338] for instructions on how to edit assigned locking devices).


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

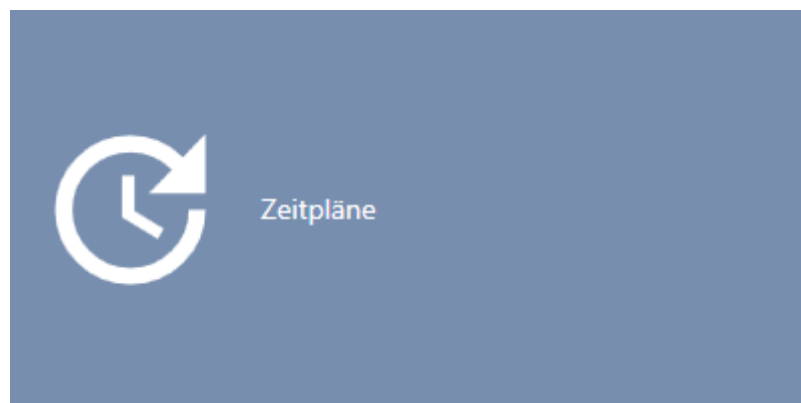


2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.



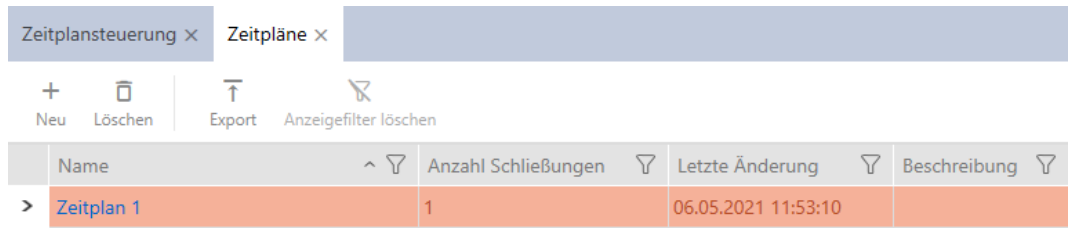
- ↳ The AXM bar will close.
- ↳ The [Time schedule control] tab will open.

3. Click on the **Time schedules**  button.





↳ The [Time schedules] tab will open.

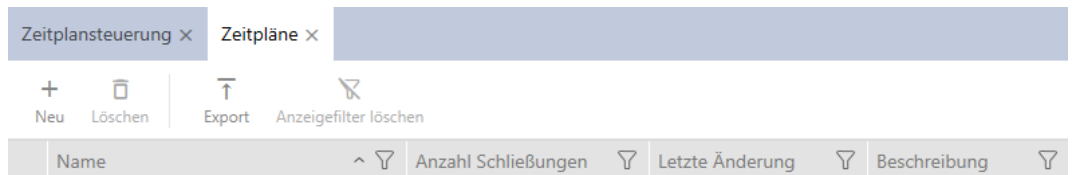


4. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

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.



### 13.7 Creating a time switchover

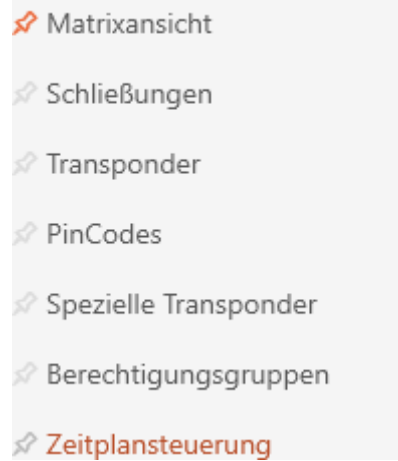
1. Click the orange AXM button .

↳ AXM bar opens.



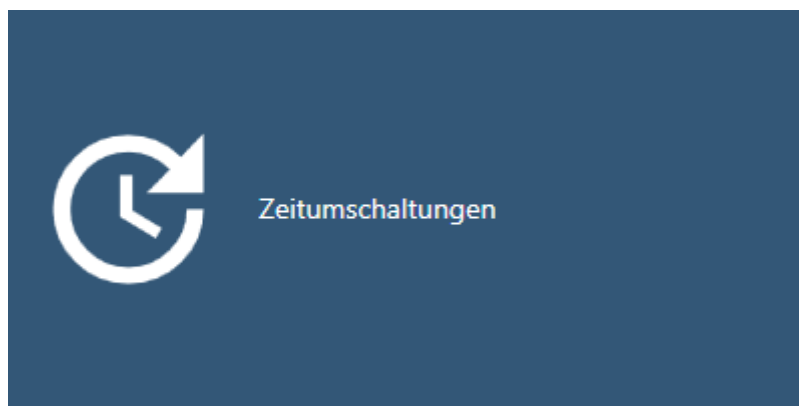
2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

**SCHLISSANLAGENSTEUERUNG**

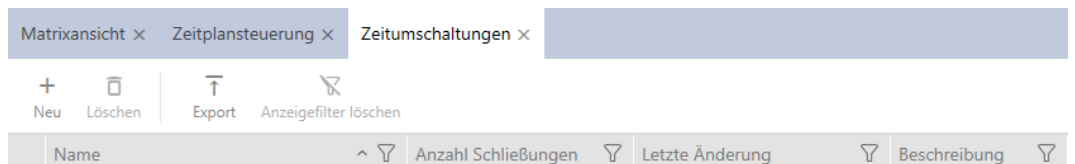



- ↳ The AXM bar will close.
- ↳ The [Time schedule control] tab will open.

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.

**Zeitumschaltung - Details**  
Hier können Sie die Details der Zeitumschaltung bearbeiten

1 Details

2 Zugeordnete Schließungen

Name

Beschreibung

ZEITEN

+

Von	Bis	Tage

Weiteres Objekt erstellen   < Zurück   Weiter >   Fertigstellen   Abbrechen

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

**Zeitumschaltung - Details**  
Hier können Sie die Details der Zeitumschaltung bearbeiten

1 Details

2 Zugeordnete Schließungen

Name

Beschreibung

ZEITEN

+

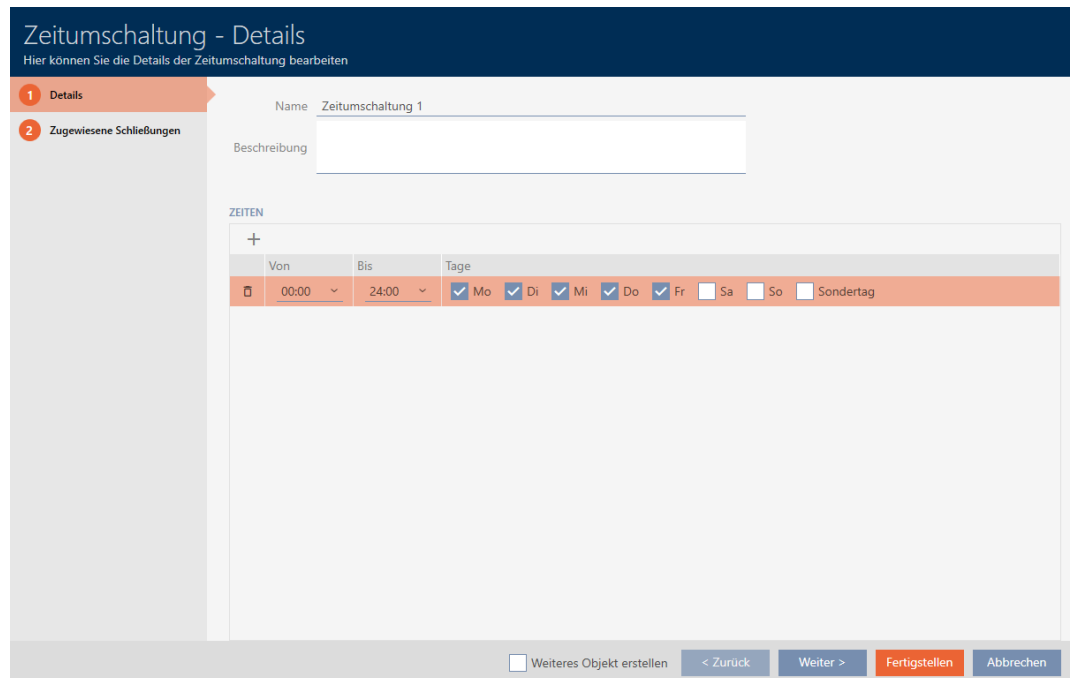
Von	Bis	Tage

Weiteres Objekt erstellen   < Zurück   Weiter >   Fertigstellen   Abbrechen

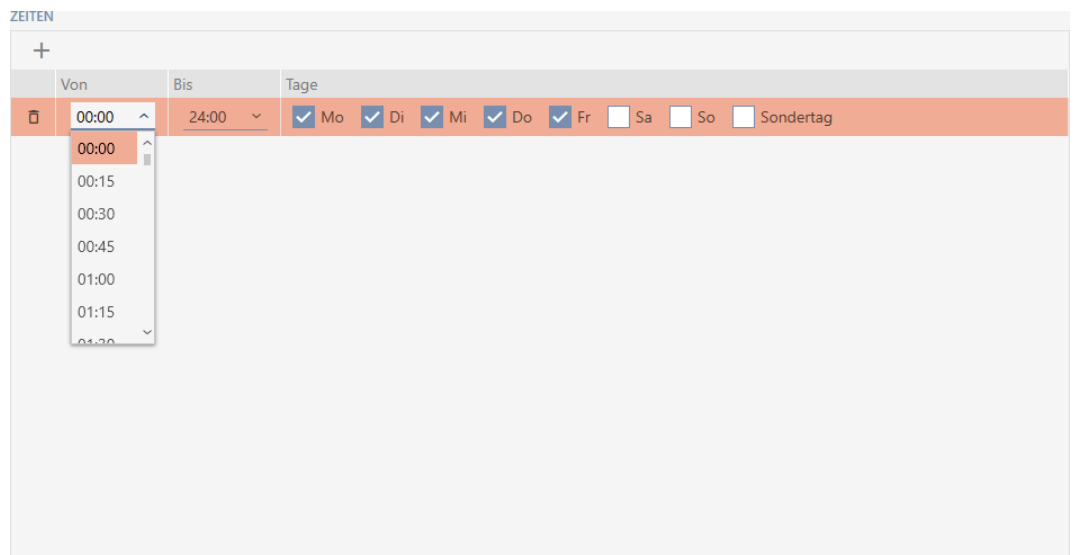
6. Enter a description in the *Description* field if required.

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 dis-engaging locking devices automatically with time switchover* [▶ 278] if required.

Name	Anzahl Schließungen	Letzte Änderung	Beschreibung
> Zeitmuschaltung 1	1	07.05.2021 17:33:50	

### 13.8 Creating and editing public holidays



#### NOTE

#### Public holidays available in all locking systems








The list of public holidays is the same for all locking systems within a project. Public holidays created here are therefore also available in all other locking systems.


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

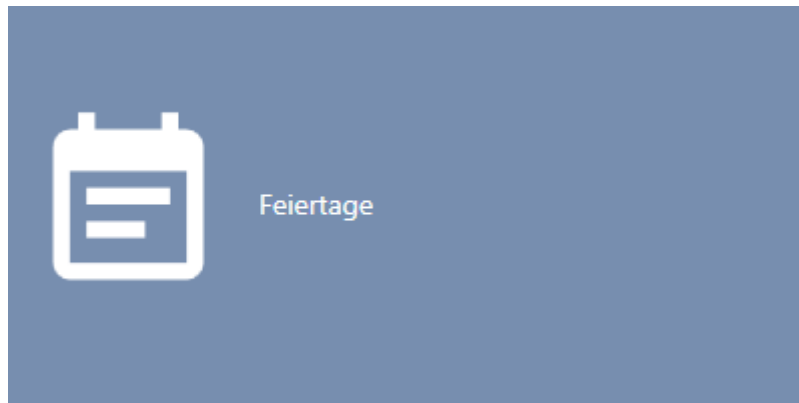


2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

#### SCHLISSANLAGENSTEUERUNG





-  Matrixansicht
-  Schließungen
-  Transponder
-  PinCodes
-  Spezielle Transponder
-  Berechtigungsgruppen
-  **Zeitplansteuerung**

- ↳ 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.

Matrixansicht x Zeitplansteuerung x **Feiertage** x

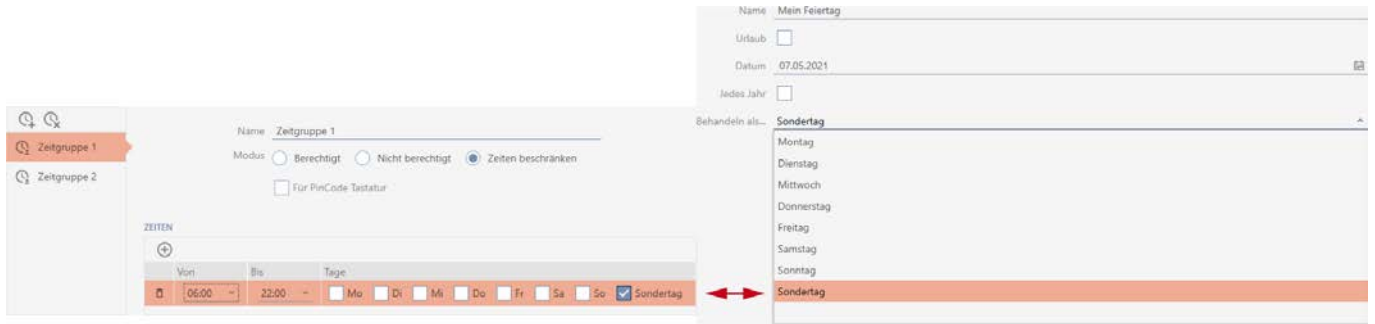




  
 Neu Löschen Export Anzeigefilter löschen

	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 Betttag	17.11.2021		Nein	Sonntag
	Christi Himmelfahrt	13.05.2021		Nein	Sonntag
	Erntedanktag	04.10.2021		Nein	Sonntag
	Fastnacht	16.02.2021		Nein	Sonntag
	Festa Nazionale	25.04.2021		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.


- 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").



- Click on the **Finish** button.
  - ↳ The window for creating a public holiday will close.
  - ↳ The public holiday has been created and is listed.

Heilige Drei Könige	06.01.2021	Nein	Sonntag
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
Reformationstag	11.10.2021	Nein	Sonntag

### 13.9 Creating and editing public holiday lists

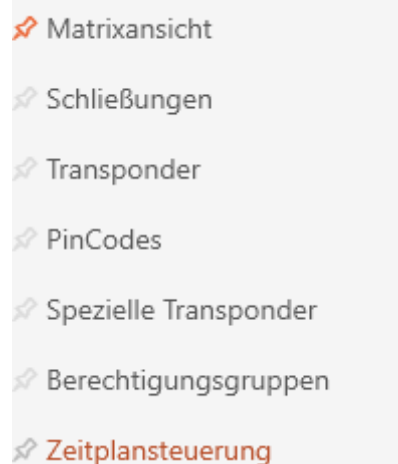
- Click the orange AXM button .
  - ↳ AXM bar opens.






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

**SCHLISSANLAGENSTEUERUNG**





- ↳ 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.

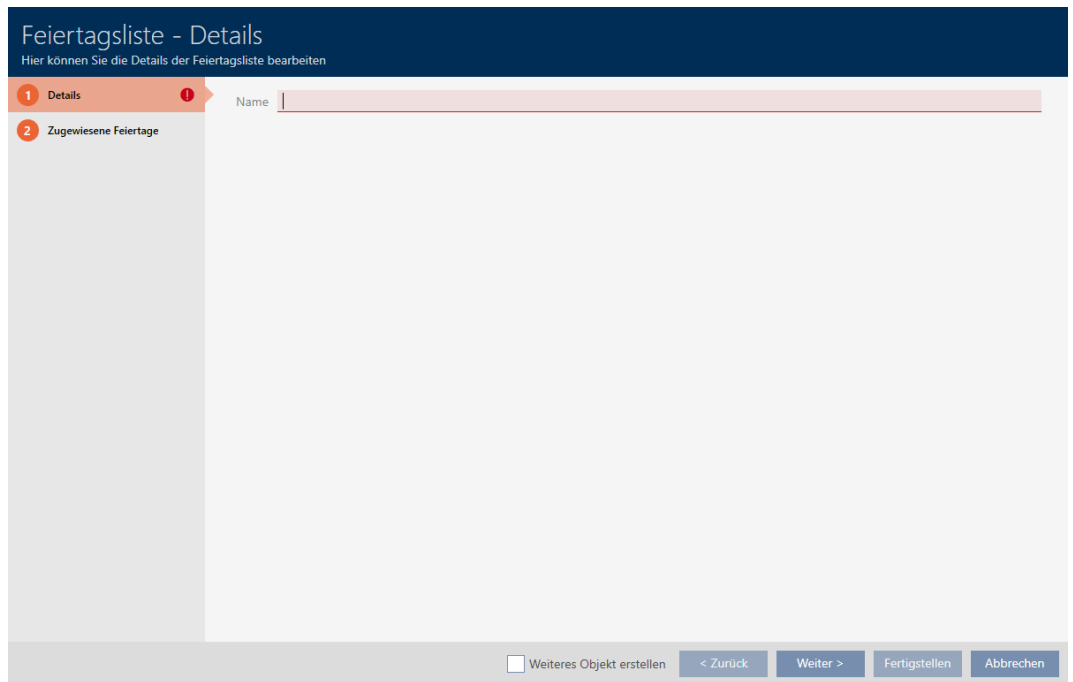
Matrixansicht × Zeitplansteuerung × Feiertagslisten × Feiertage ×

+ Neu     Löschen    ↑ Export     Anzeigefilter löschen

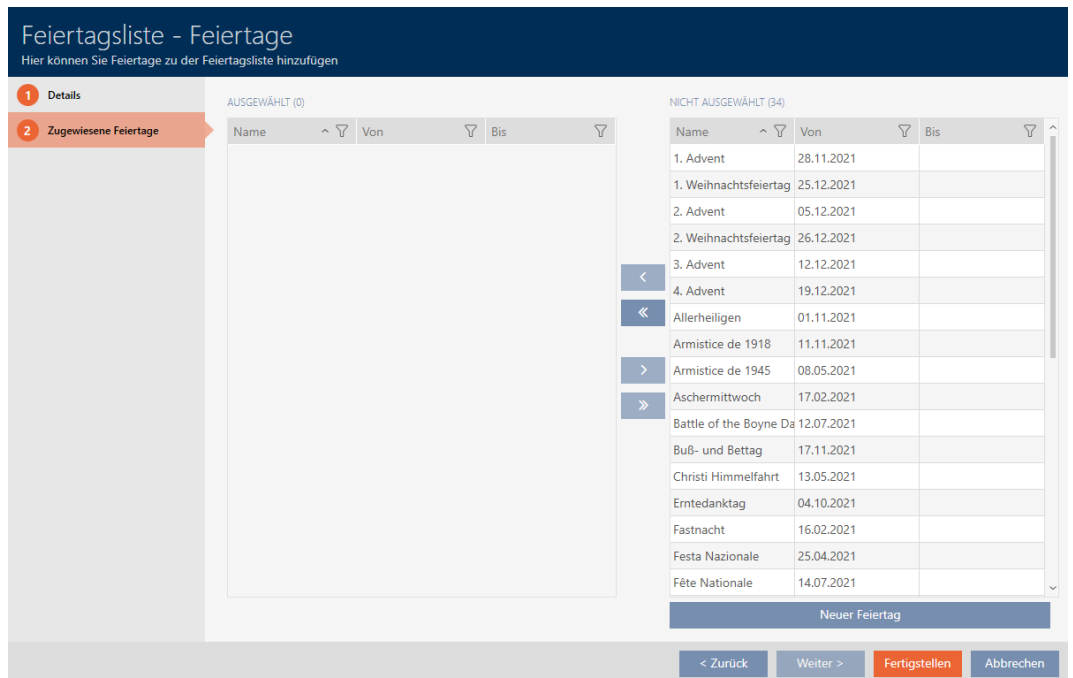
	Name 	Letzte Änderung 
>	Baden-Württemberg	26.04.2021 23:56:58
	Bayern	26.04.2021 23:56:58
	Berlin	26.04.2021 23:56:58
	Brandenburg	26.04.2021 23:56:58
	Bremen	26.04.2021 23:56:58
	Hamburg	26.04.2021 23:56:58
	Hessen	26.04.2021 23:56:58
	Mecklenburg-Vorpommern	26.04.2021 23:56:58
	Niedersachsen	26.04.2021 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* [▶ 44]).
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.

**Feiertagsliste - Feiertage**  
 Hier können Sie Feiertage zu der Feiertagsliste hinzufügen

**1 Details**

**2 Zugewiesene Feiertage**

AUSGEWÄHLT (4)				NICHT AUSGEWÄHLT (31)			
Name	Von	Bis		Name	Von	Bis	
1. Advent	28.11.2021			1. Weihnachtsfeiertag	25.12.2021		
2. Advent	05.12.2021			2. Weihnachtsfeiertag	26.12.2021		
3. Advent	12.12.2021			Allerheiligen	01.11.2021		
4. Advent	19.12.2021			Armistice de 1918	11.11.2021		
				Armistice de 1945	08.05.2021		
				Aschermittwoch	17.02.2021		
				Battle of the Boyne Da	12.07.2021		
				Buß- und Betttag	17.11.2021		
				Christi Himmelfahrt	13.05.2021		
				Erntedanktag	04.10.2021		
				Fastnacht	16.02.2021		
				Festa Nazionale	25.04.2021		
				Fête Nationale	14.07.2021		
				Fronleichnam	03.06.2021		
				Heilige Drei Könige	06.01.2021		
				Heiliger Abend	24.12.2021		
				Karfreitag	02.04.2021		

Neuer Feiertag

< Zurück   Weiter >   Fertigstellen   Abbrechen

- 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.

Matrixansicht ×		Zeitplansteuerung ×		Feiertagslisten ×		Feiertage ×	
+		☐		↑		✕	
Neu		Löschen		Export		Anzeigefilter löschen	
Name	^	☐	Letzte Änderung		☐		
Baden-Württemberg			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)* [[▶ 276](#)].

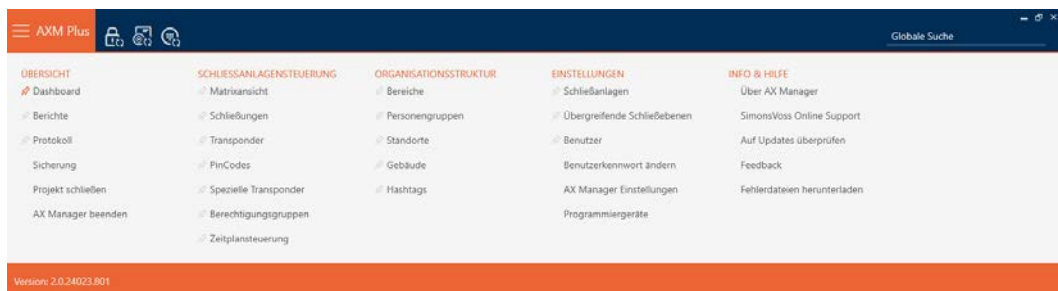
### 13.10 Creating a location



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

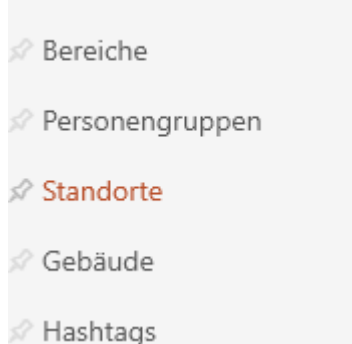
1. Click on the orange AXM icon .

↳ AXM bar opens.

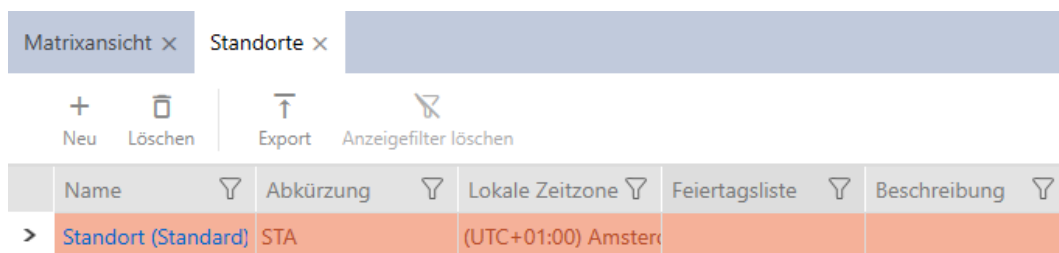


2. Select the **Locations** entry in the | ORGANISATIONAL STRUCTURE | group.

### ORGANISATIONSTRUKTUR



↳ 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* [▶ 72]).



### 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. Select the Use as default check box if you would like to preselect this location for new locking devices/doors.
10. Click on the **Finish** button.
  - ↳ The window for creating a new location closes.
  - ↳ The newly created location is listed.

Matrixansicht ×		Standorte ×				
+ Neu		🗑️ Löschen		↑ Export		🗖️ Anzeigefilter löschen
Name	Abkürzung	Lokale Zeitzone	Feiertagsliste	Beschreibung		
> Hogsmeade	HM	(UTC+01:00) Amster				
Standort (Standard)	STA	(UTC+01:00) Amster				

### 13.11 Creating a building and assigning it to a location



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

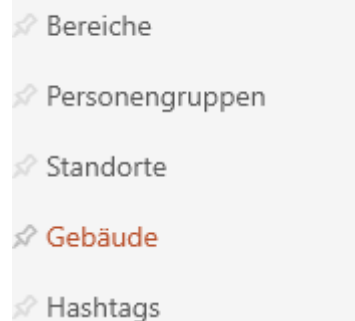
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.



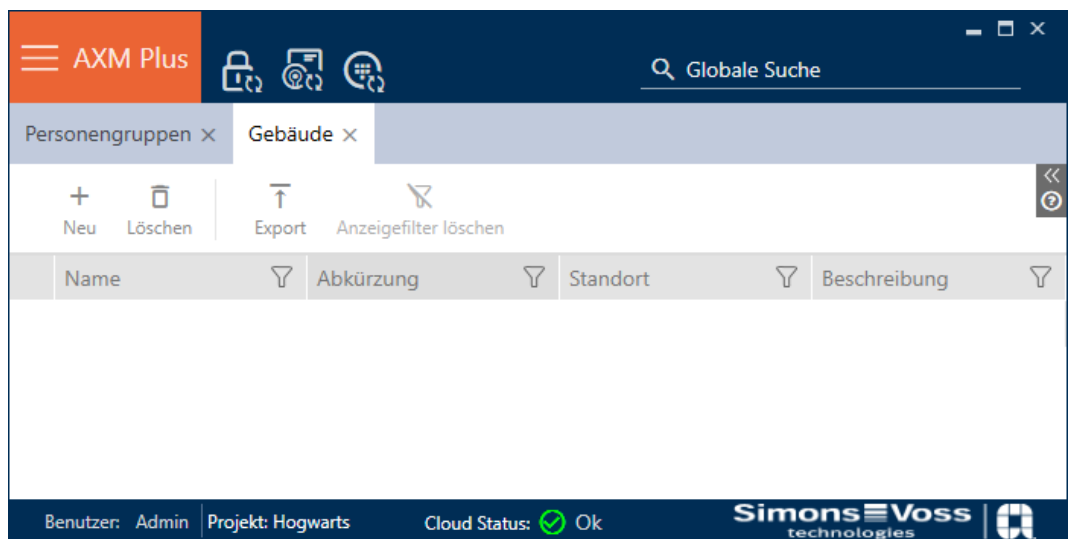


2. Select the **Building** entry in the | ORGANISATIONAL STRUCTURE | group.

**ORGANISATIONSTRUKTUR**



↳ The [Building] tab will open.



3. Click on the **New** + button.

↳ The window for creating a new building will open.

Gebäude - Details  
Hier können Sie die Details des Gebäudes bearbeiten

1 Details

Name

Abkürzung

Standort Hogsmeade

Beschreibung

Als Standard verwenden

Weiteres Objekt erstellen Fertigstellen Abbrechen

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.

Gebäude - Details  
Hier können Sie die Details des Gebäudes bearbeiten

1 Details

Name

Abkürzung

Standort Hogsmeade

Beschreibung

Als Standard verwenden


Weiteres Objekt erstellen Fertigstellen Abbrechen

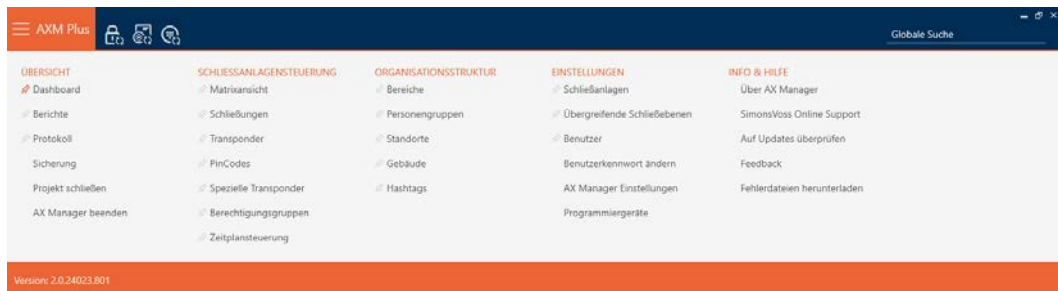
7. Enter a description of your building in the *Description* field if required.
8. Click on the **Finish** button.
  - ↳ Window for creating a new building closes.
  - ↳ The newly created building is listed.

Matrixansicht x Gebäude x			
Name	Abkürzung	Standort	Beschreibung
Gebäude (Standard)	GEB	Standort (Standard)	
Gryffindor tower	GT	Hogwarts	

### 13.12 Creating an area

Areas are a very useful structure for your locking system (also see *Areas* [▶ 548]).

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




2. Select the **Area** entry in the | LOCKING SYSTEM CONTROL | group.



↳ The [Areas] tab will open.

Bereiche x		
Name	Zeitplan	Beschreibung

3. Click on the **New**  button.
  - ↳ The "Area" window will open.

4. Enter a name for your area in the *Name* field.
5. Select a schedule that you wish to use for the locking devices in this area from the ▼ **Time schedule** drop-down menu if required.



## NOTE

### Available schedules

Obviously, schedules that you wish to use for an area need to be available. If there are no schedules in your locking system, the ▼ **Time schedule** drop-down menu is greyed out.

- ❑ Create at least one schedule beforehand (see *Creating a schedule* [▶ 53]) in such a case.

6. Enter a description of your area in the *Description* field if necessary.
7. Click on the **Finish** button.
  - ↳ "Area" window closes.
  - ↳ The newly created area is listed.

Bereiche x

+ Neu    - Löschen    Anzeigefilter löschen

Name	Zeitplan	Beschreibung
> Castle	5th grade schedule	



**NOTE**

**Schedules in locking devices and areas**


You can assign schedules both to a locking device and to the locking device area. In this case, the schedule is used in the locking device and the schedule for the area is ignored.

If a schedule is assigned to an area instead of the locking device, the schedule for the area is adopted for the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

13.13 Creating a hashtag



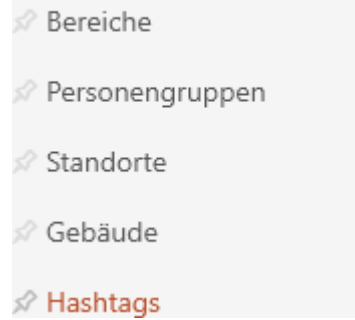
Hashtags can be used as keywords for persons and/or doors (see *Hashtags* [▶ 549]).

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

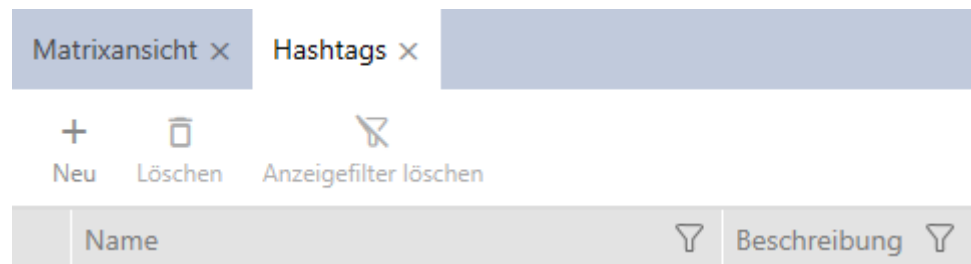


2. Select the **Hashtags** entry in the | ORGANISATIONAL STRUCTURE | group.

**ORGANISATIONSTRUKTUR**

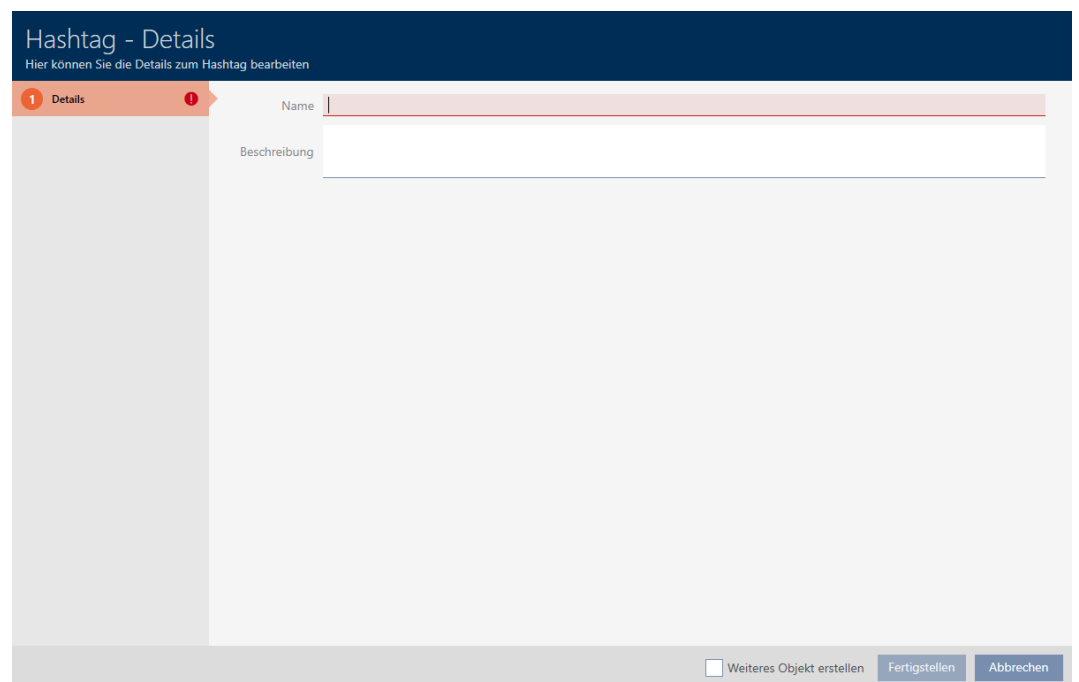


↳ The [Hashtags] tab will open.



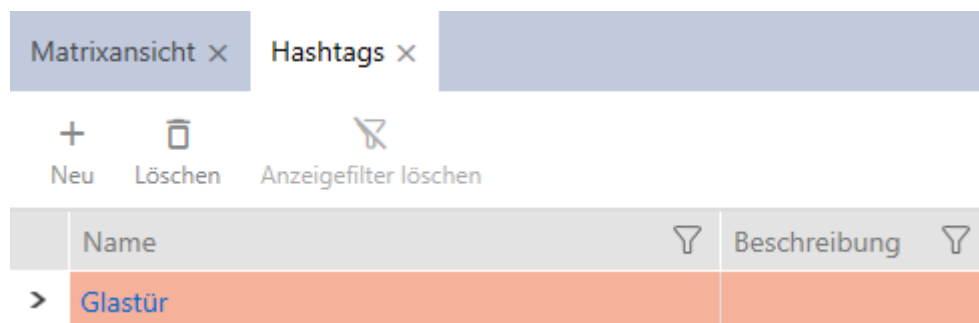
3. Click on the **New +** button.

↳ 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.



## 14. 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)* [▶ 410]).

### 14.1 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* [▶ 512]).

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

- Transponder
- Cards
- PIN code keypad AX
- PIN code keypad 3068 with G1 protocol
- AX2Go key

These identification media differ from one another:

	Cards/transponders	PIN code keypad AX PIN code keypad 3068 with G1 protocol	AX2Go key
Operable locking devices	All locking devices that have the required interface (active/passive).	Only the locking device assigned in AXM Plus.	All locking devices that feature the required interface and firmware (BLE 1.1.1148 and higher).
Available settings	All	<ul style="list-style-type: none"> <li>■ Time groups</li> <li>■ Activation and expiry date</li> </ul>	<ul style="list-style-type: none"> <li>■ <input checked="" type="checkbox"/> Long opening</li> <li>■ <input checked="" type="checkbox"/> Acoustic opening signal</li> <li>■ <input checked="" type="checkbox"/> from now</li> <li>■ <input checked="" type="checkbox"/> without expiry date</li> </ul>
Service Sets	For transponders	No	No
Creation procedure	See <i>Creating transponders and cards</i> [▶ 89].	See <i>Creating PIN code keypads</i> [▶ 96].	See <i>Assigning keys for AXM Plus and higher</i> [▶ 211].



Further information on the different identification media and their differences can be found in Section *Identification media, locking devices and the locking plan* [▶ 512].

### 14.1.1 Creating transponders and cards



#### NOTE

#### Activating cards or transponders for a locking system

The only credential types available are those that have been activated in your locking system.

- If necessary, activate cards or transponders in the locking system properties (see *Enable cards or transponders* [▶ 389]).

In the interests of best practice (see *Best practice: setting up the locking system* [▶ 27]), SimonsVoss recommends that you configure authorisation groups, person groups and schedules/time groups:

- *Authorisation groups* [▶ 322] (see *Authorisation groups* [▶ 543] for background information )
- *Creating a person group* [▶ 51] (see *Person groups* [▶ 544] for background information )
- *Creating a schedule* [▶ 53] or *Create time group* [▶ 56] (see *Time groups and schedules* [▶ 528] for background information )

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

Transponder/Personen - Details

Bitte konfigurieren Sie hier die Details des Transponders und der zugehörigen Person.

- 1 Details
- 2 Personendetails !
- 3 Transponderkonfiguration
- 4 Zusätzliche Schließanlagen
- 5 Berechtigungsgruppen
- 6 Hashtags

TRANSPONDER DETAILS

Typ ⊙ Transponder

Beschreibung

Zeitgruppe  Zeitgruppe 1

PERSONENDETAILS

Neue Person

oder

Bestehende Person auswählen DirektClassic, Dieter22

Weiteres Objekt erstellen
< Zurück
Weiter >
Fertigstellen
Abbrechen

2. Select the identification medium you wish to create from the ▼ **Type** drop-down menu.
3. Enter a description if required.
4. If the identification medium is to feature time-controlled authorisations: select the  Time group checkbox.
5. Select the time group from the ▼ **Time group** drop-down list (e.g. "Time group").
6. Activate the  New person check box.
  - ↳ AXM Plus will automatically create a new person for the new identification medium. Deactivate this check box to select an existing person (e.g. for a second identification medium or a replacement identification medium).
  - ↳ The "Person details" tab is shown.
7. Click on the  **Person details** tab.

8. 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 Plus 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* [▶ 443]).

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.
- 
9. If you wish to assign this person to a person group: Select the person group to which this person belongs from the ▼ **Person group** drop-down menu.

10. Give further details about the person if required.  
↳ You can then simply select the information you enter in the *Department* field from a list for other persons.
11. If you want to edit the *Set on*, *Quitting date* or *Date of birth* fields: Deactivate the relevant  Not relevant check box.

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

13. If locking devices need to open twice as long for this identification medium (doubling to max. 25 s): select the  Long opening checkbox.
14. If you don't wish locking devices for this identification medium to beep: disable the  No acoustic opening signal checkbox.
15. 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.
16. Select one of the three options in the "Dynamic time window" area (see *Time budget (AX2Go and virtual network)* [▶ 540]):
- Do not change time window on the gateway option: Does not use time budgets.
  - until a particular time of (next) day option: Authorisations for this identification medium expire at a specific time and can only be renewed at the gateway.
  - Number of hours from the last full hour of the booking option: Authorisations for this identification medium expire after the specified number of hours, but can be extended or renewed at any time at the gateway.



## NOTE

### Gateway to renew time budgets

If you select the  Number of hours from the last full hour of the booking or  until a particular time of (next) day option, your users will need a gateway to reload their time budgets.

17. If you do not want the transponder to be usable immediately: disable the  from now checkbox. Then enter an activation date.
18. 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.
19. Use the **Additional locking systems** button to switch to the next tab or complete the entries with the **Finish** button.
20. If you wish to use the identification medium in other locking systems in this project: Use the **Add** button to add further locking systems (see *Use identification media in multiple locking systems* [▶ 199]).



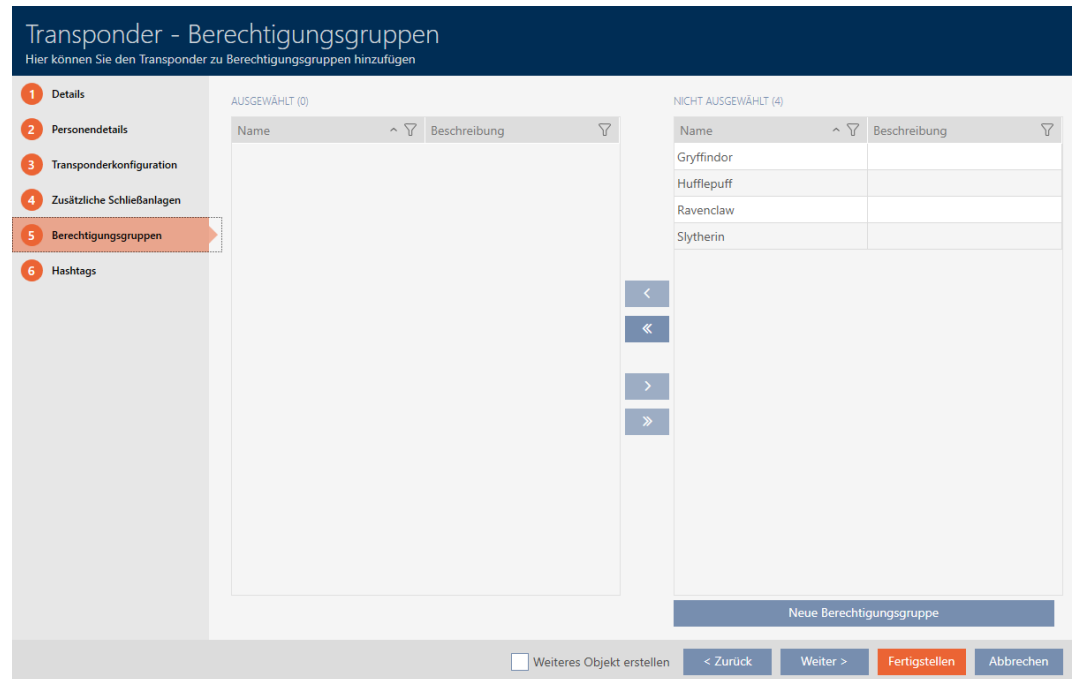
#### NOTE




##### Limitations for Transponder - Additional locking systems

Depending on the type of identification medium, different volumes of memory space are available for additional locking devices (e.g.: G2 transponders can store four G2 locking systems). The locking system also needs to support the identification medium (e.g.: transponders cannot be used in card-only locking systems).

1. Make sure that there is sufficient memory space on your identification medium.
2. Make sure that the required locking system supports your identification medium. Upgrade the locking system if necessary (see *Enable cards or transponders* [▶ 389]).
3. Ensure that the locking system memory spaces do not overlap in the case of cards.

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



22. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
23. Select the required authorisation groups in the right column (Ctrl+click for single groups or Shift+click for multiple groups).
24. Use  to move the selected authorisation groups only or  to move all displayed authorisation groups.
- ↳ The identification medium is assigned to the highlighted authorisation groups.

**Transponder - Berechtigungsgruppen**  
Hier können Sie den Transponder zu Berechtigungsgruppen hinzufügen

- 1 Details
- 2 Personendetails
- 3 Transponderkonfiguration
- 4 Zusätzliche Schließanlagen
- 5 Berechtigungsgruppen
- 6 Hashtags

AUSGEWÄHLT (1)		NICHT AUSGEWÄHLT (3)	
Name	Beschreibung	Name	Beschreibung
Gryffindor		Hufflepuff	
		Ravenclaw	
		Slytherin	

Weiteres Objekt erstellen
 < Zurück
Weiter >
Fertigstellen
Abbrechen



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

**Neue Person**  
Hier können Sie Hashtags zu der Person hinzufügen

- 1 Details
- 2 Personendetails
- 3 Transponderkonfiguration
- 4 Zusätzliche Schließanlagen
- 5 Berechtigungsgruppen
- 6 Hashtags

AUSGEWÄHLT (0)		NICHT AUSGEWÄHLT (3)	
Name	Beschreibung	Name	Beschreibung
		Glastür	
		Rohrrahmentür	
		Rothaarige	

Weiteres Objekt erstellen
 < Zurück
Weiter >
Fertigstellen
Abbrechen

26. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

- 27. Select the required hashtags in the right column (Ctrl+click for single hashtags or Shift+click for multiple hashtags).
- 28. Use **←** to move only the selected hashtags or **⇐** to move all hashtags.

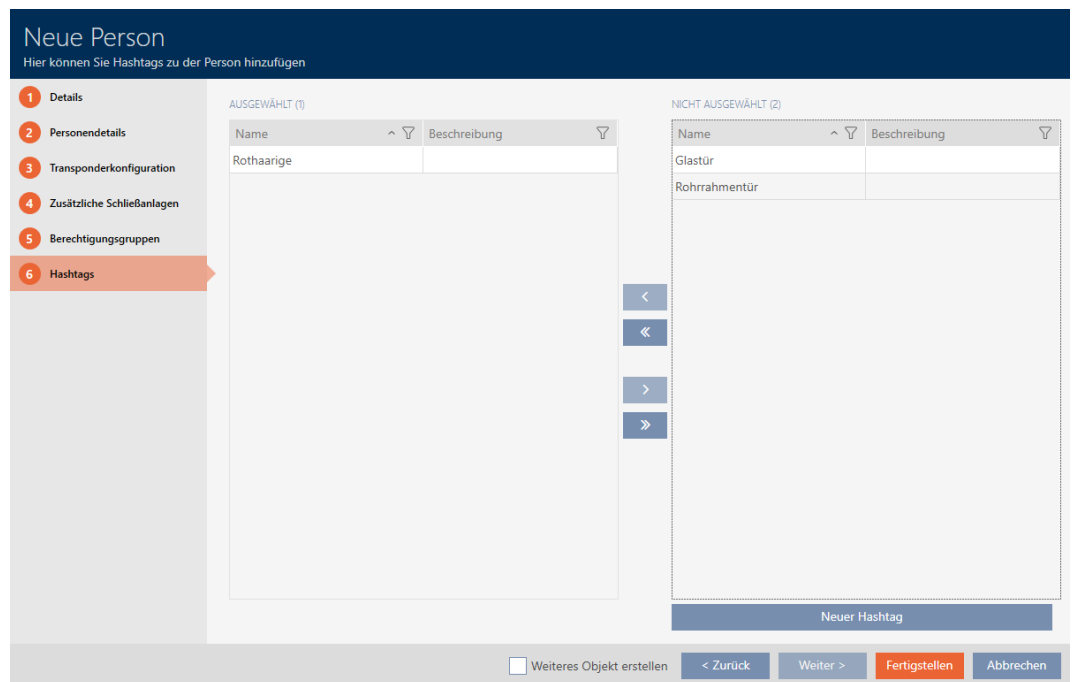


**NOTE**

**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.



- 29. Select the  Create additional objects checkbox to leave the window with the same settings open for the next identification medium to be created.
- 30. 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.

**14.1.2 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* [▶ 512]).



In the interests of best practice (see *Best practice: setting up the locking system* [▶ 27]), SimonsVoss recommends that you configure schedules/ time groups first:

- *Creating a schedule* [▶ 53] or *Create time group* [▶ 56] (see *Time groups and schedules* [▶ 528] 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 Plus (also see *PIN Code G1 vs. PIN Code AX* [▶ 514]).




**NOTE**

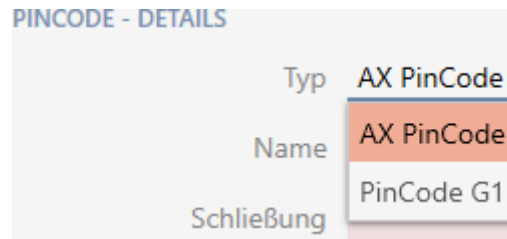
**Authorisations set automatically**

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

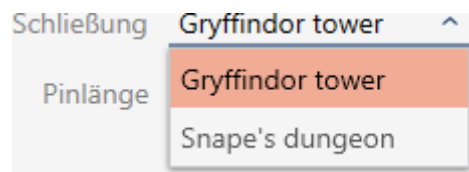
- ✓ Locking device has been created for the PIN code keypad (see *Creating a locking device* [▶ 228] in the AXM manual).

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

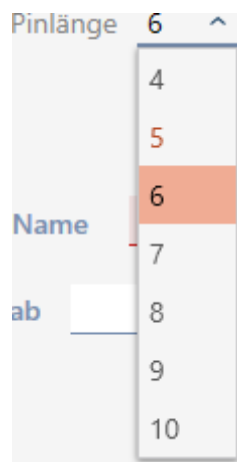
2. Select the PIN code keypad you wish to create from the ▼ **Type** drop-down menu.



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 Plus 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* [▶ 44]).

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.

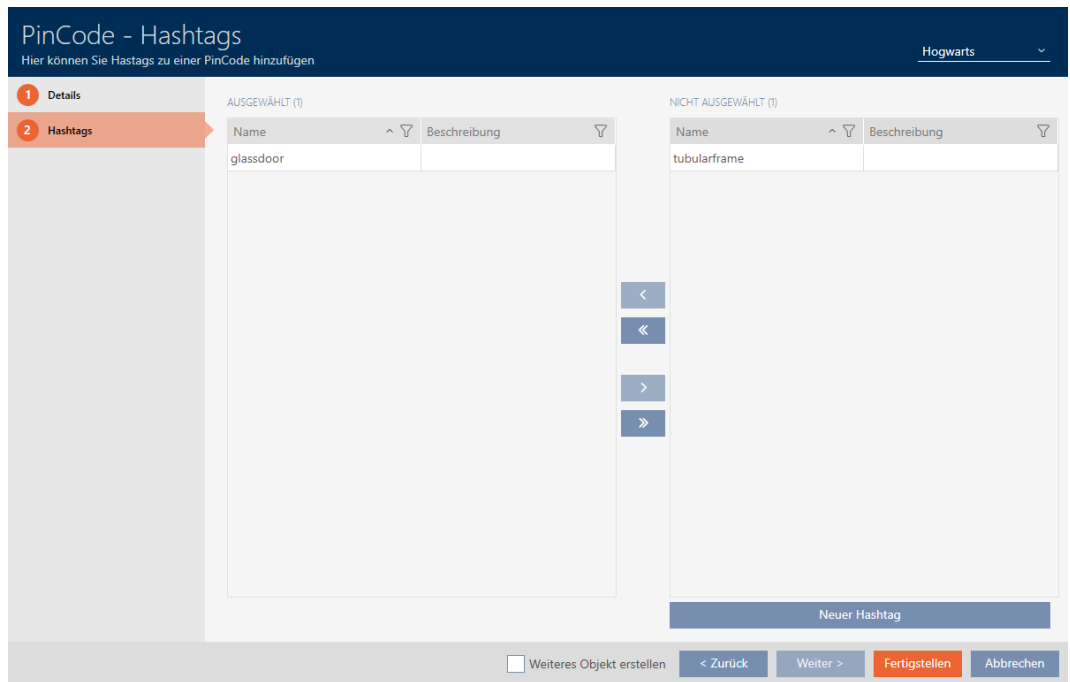


**NOTE**

**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.

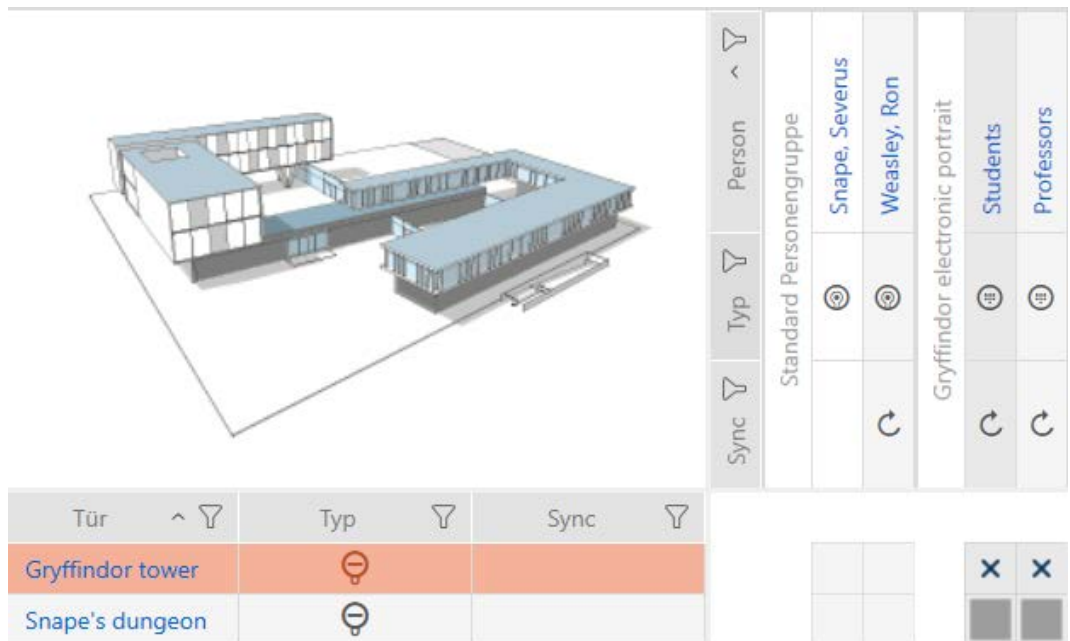


18. Select the  Create additional objects checkbox to leave the window with the same settings open for the next PIN code to be created.

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.



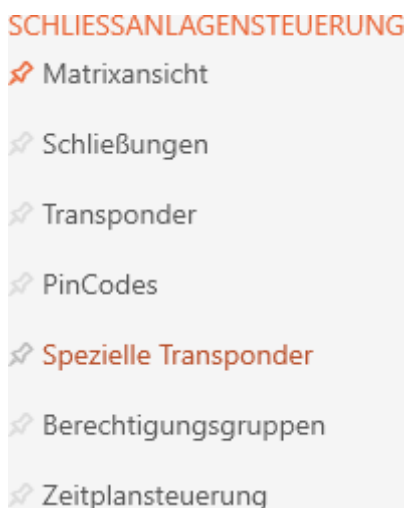
### 14.1.3 Creating special identification media

You can assign just one function to a specific identification medium, either Battery replacement or Lock Activation (see *Special identification media and their functions* [▶ 520]). This identification medium can then no longer be used for other purposes in this project.

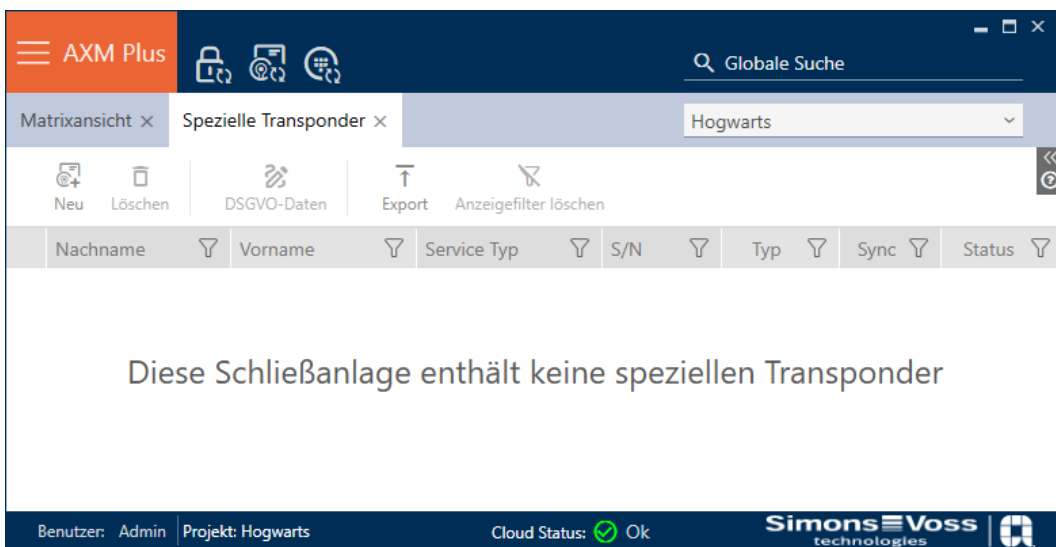
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.



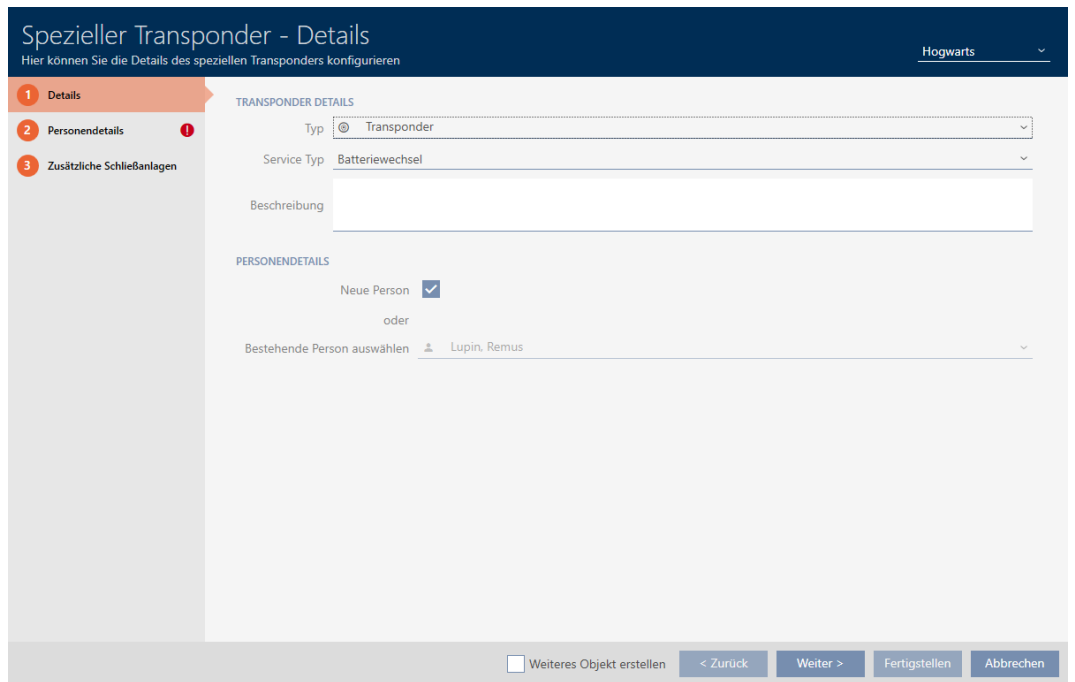
2. Select the **Special Transponders** entry in the | LOCKING SYSTEM CONTROL | group.
  - ↳ The [Special Transponders] tab will open.



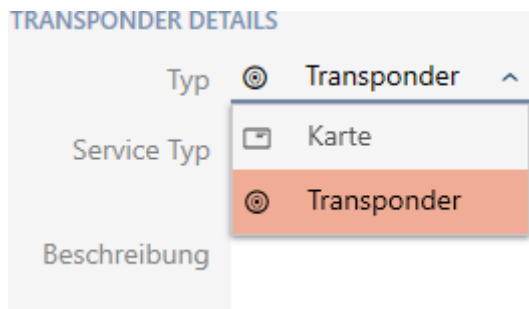
↳ The [Special Transponders] tab will open.



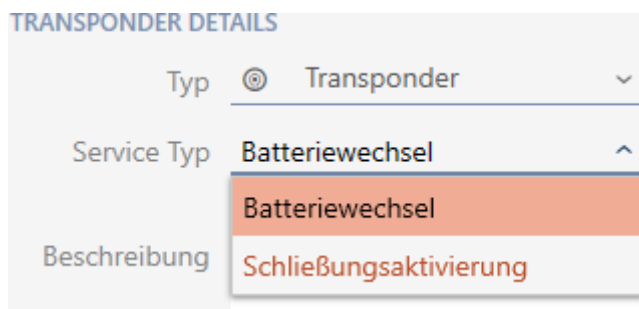
3. Click on the **New** button .
  - ↳ The "Special Transponder" window will open.



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

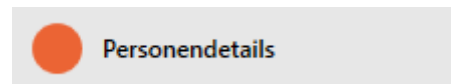


5. Then use the drop-down ▼ **Service Type** menu to select which function this identification medium should have ("Battery replacement" or "Lock Activation").



6. Enter a description if required.

7. Activate the  New person check box.
  - ↳ AXM Plus will automatically create a new person for the new identification medium. Deactivate this check box to select an existing person (e.g. for a second identification medium or a replacement identification medium).
  - ↳ The "Person details" tab is shown.
8. Click on the  Person details tab.



9. 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**

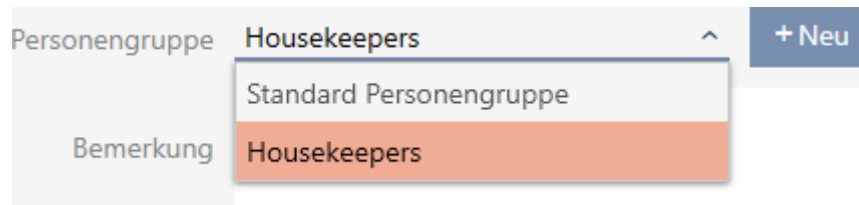
The AXM Plus generates personnel numbers based on the following formula: PN-1, PN-2, PN-X. The abbreviation *PN* can be changed if required (see *Changing automatic numbering* [▶ 443]).

Alternatively, you can enter personnel numbers manually:

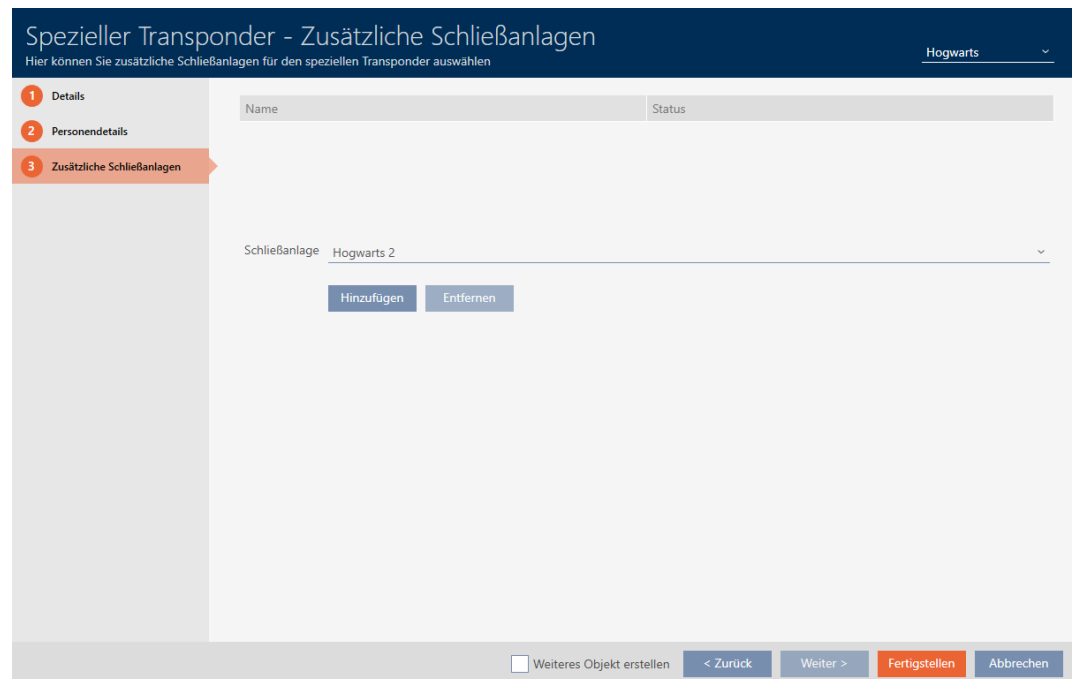
1. Activate the  Auto check box.
  - ↳ The *Personnel number* field is activated.
2. Enter the personnel number in the *Personnel number* field.



- If you wish to assign this person to a person group: Select the person group to which this person belongs from the ▼ **Person group** drop-down menu.



- Give further details about the person if required.
  - ↳ You can then simply select the information you enter in the *Department* field from a list for other persons.
- If you want to edit the *Set on*, *Quitting date* or *Date of birth* fields: Deactivate the relevant  Not relevant check box.
- Use the **Additional locking systems** button to switch to the next tab or complete the entries with the **Finish** button.



- If you want to use this special identification medium in other locking systems, use the **Add** button to add other locking systems.



**NOTE**

**Limitations for Transponder - Additional locking systems**

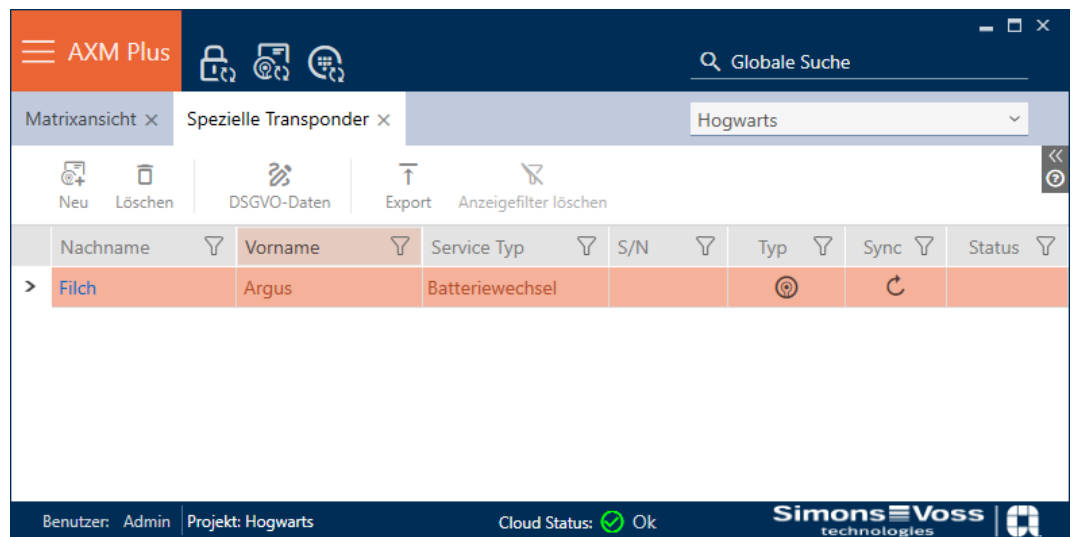
Depending on the type of identification medium, different volumes of memory space are available for additional locking devices (e.g.: G2 transponders can store four G2 locking systems). The locking system also needs to support the identification medium (e.g.: transponders cannot be used in card-only locking systems).

1. Make sure that there is sufficient memory space on your identification medium.
2. Make sure that the required locking system supports your identification medium. Upgrade the locking system if necessary (see *Enable cards or transponders* [▶ 389]).
3. Ensure that the locking system memory spaces do not overlap in the case of cards.

15. Click on the **Finish** button.

↳ "Special Transponders" window closes.

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

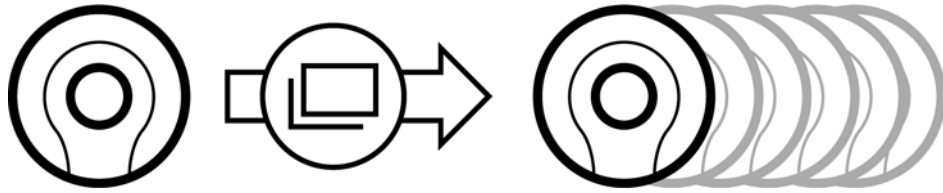


Identification media with special functions are not displayed in the matrix.

**14.1.4 Creating an AX2Go key**

See *Assigning keys for AXM Plus and higher* [▶ 211].

## 14.2 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 Plus also applies the properties, which can be changed in the AXM Plus.

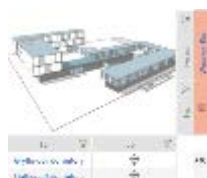
The following settings are duplicated:


- Transponder type
- Time group
- Person details (except for Personnel number. This is continued automatically with the adjustable abbreviation; also see *Changing automatic numbering* [▶ 443])
- Person group
- Transponder configuration
- Transponder - Additional locking systems
- Access levels
- Hashtags

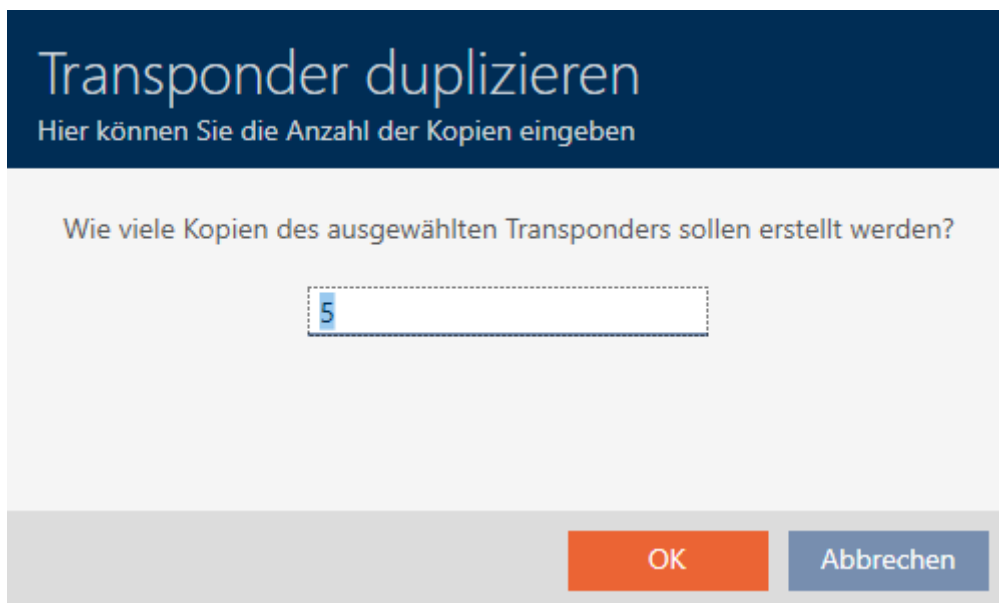
The following settings are not duplicated:

- 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
- ✓ Identification medium available.

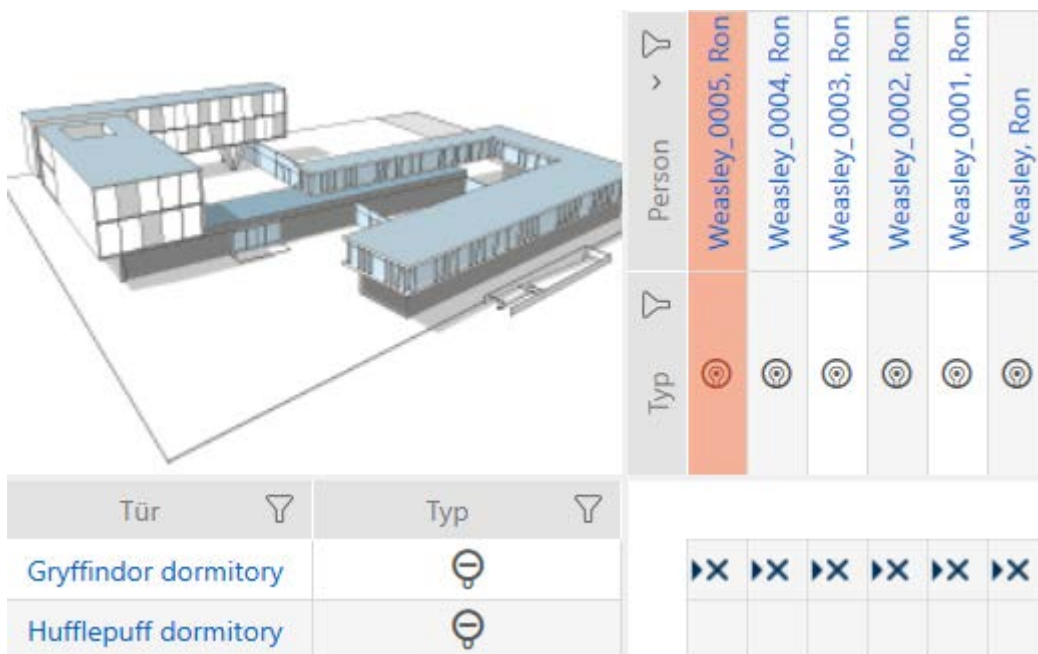
1. Select the identification medium to be duplicated.



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



- Click on the OK button.
  - The identification medium is duplicated.



### 14.3 Deleting an identification medium

#### 14.3.1 Deleting a card/transponder

There are two ways to delete identification media:

- Delete on the matrix screen (*Deleting individual identification media in the matrix* [[▶ 109](#)])

2. Delete using the tab for identification media (*Deleting multiple identification media using the tab* [▶ 110])

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.

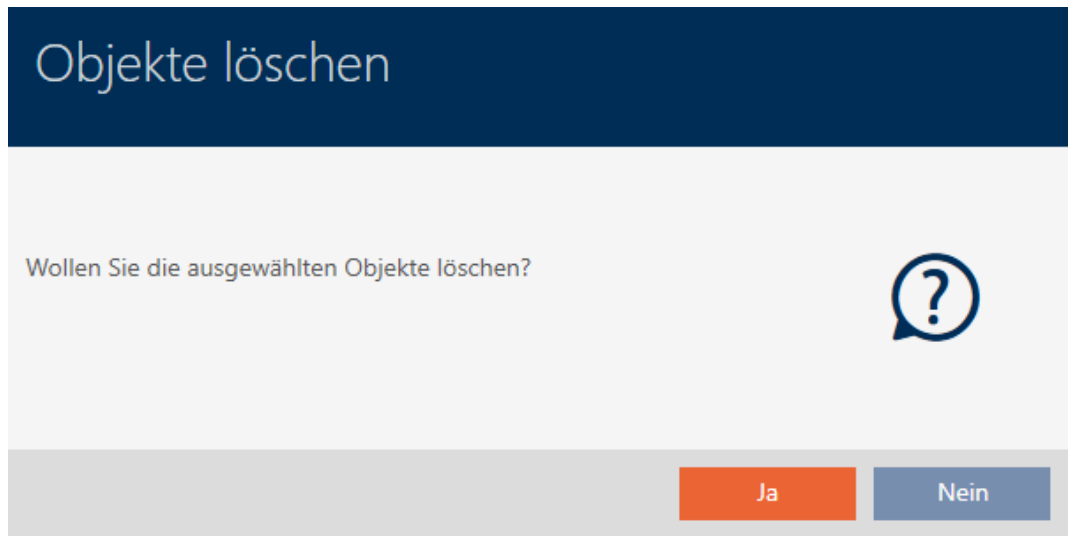
14.3.1.1 Deleting individual identification media in the matrix

- ✓ Matrix screen open.
- ✓ The identification medium to be deleted is unprogrammed or reset (see *Resetting cards/transponders* [▶ 424] about resetting).

1. Select the identification medium you wish to delete.

Person	Typ
Weasley_0005, Ron	
Weasley_0004, Ron	
Weasley_0003, Ron	
Weasley_0002, Ron	
Weasley_0001, Ron	
Weasley, Ron	

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



3. Click on the **Yes** button.
  - ↳ Deletion query closes.
  - ↳ Identification medium is deleted.

Person	Typ
Weasley_0004, Ron	
Weasley_0003, Ron	
Weasley_0002, Ron	
Weasley_0001, Ron	
Weasley, Ron	

### 14.3.1.2 Deleting multiple identification media using the tab

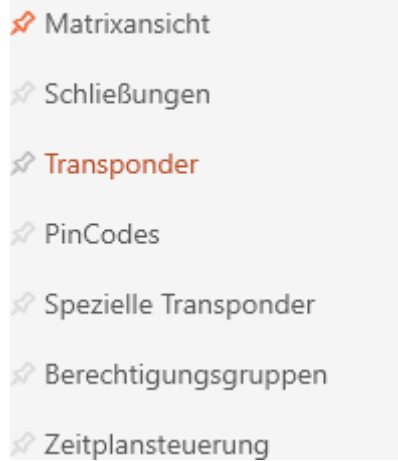
- ✓ Identification media to be deleted are unprogrammed or reset (see *Resetting cards/transponders* [▶ 424] about resetting).

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




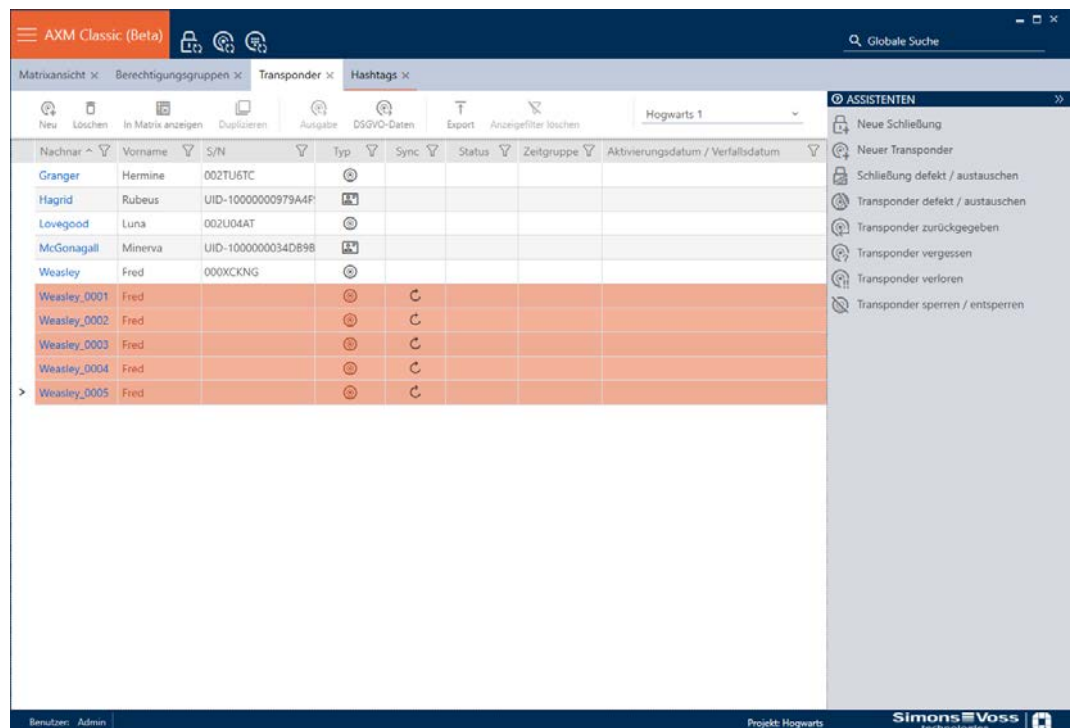
2. Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.


**SCHLISSANLAGENSTEUERUNG**

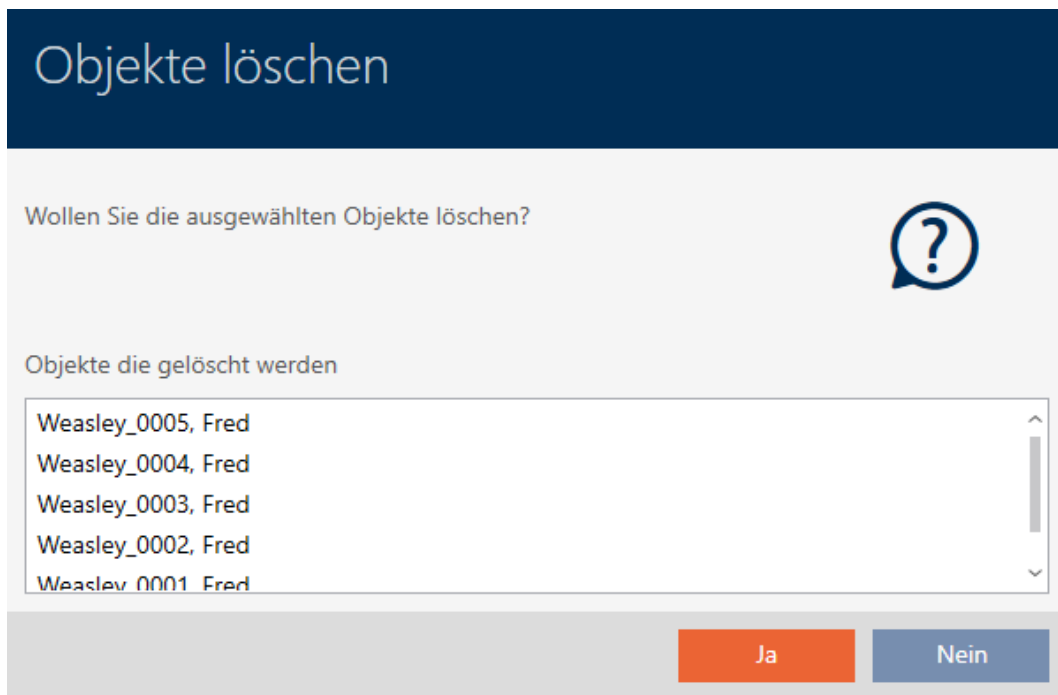


- ↳ The AXM bar will close.
- ↳ The [Transponder] tab will open.

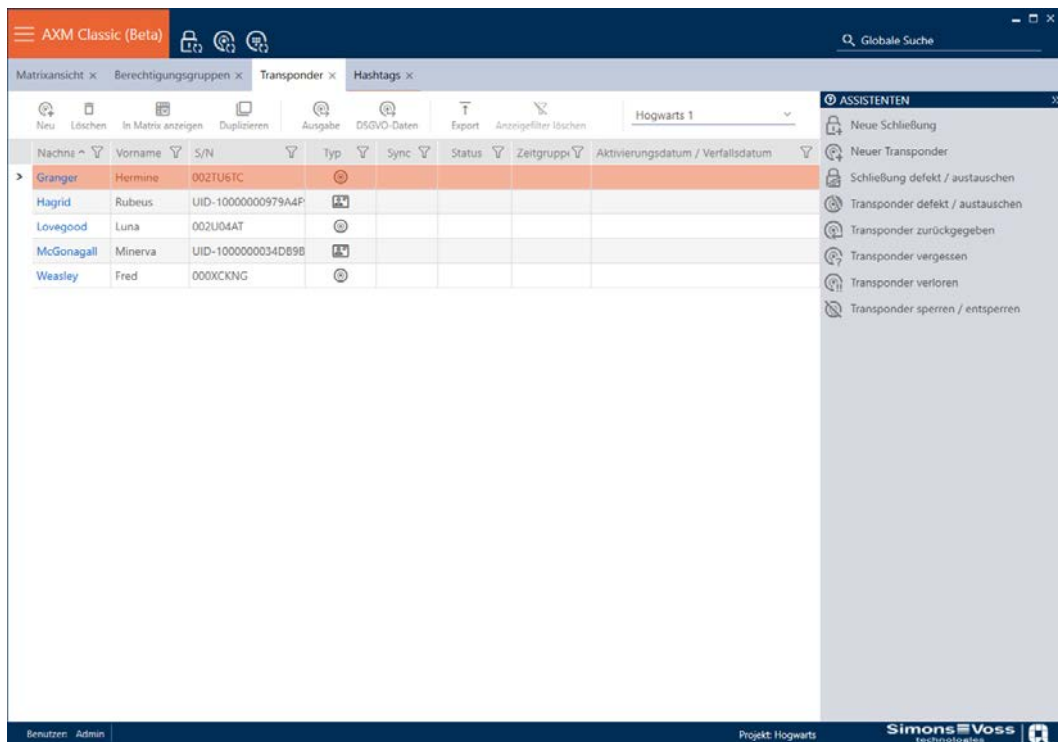
3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
4. Select all identification media that you wish to delete (Ctrl+click for single media or Shift+click for multiple media).



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.

**14.3.2 Deleting a PIN (PIN code keypad AX)**

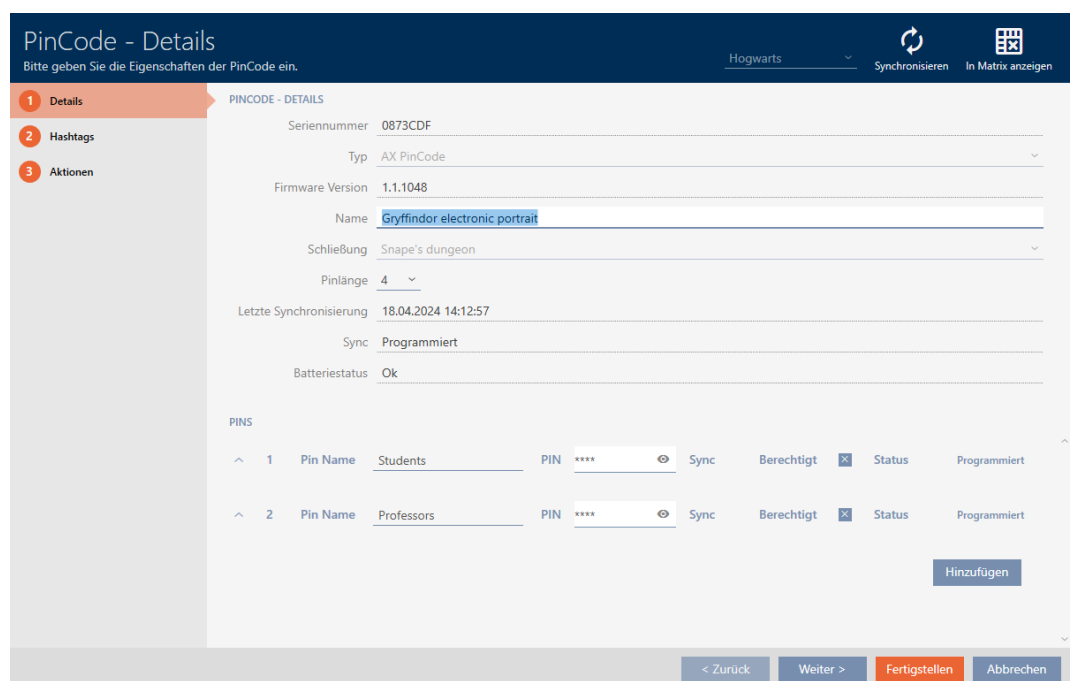


**NOTE**

**Description only valid for PIN code keypad AX**

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

- ✓ Matrix screen open.
  - ✓ PIN code keypad AX created (see *Creating PIN code keypads [▶ 96]*).
1. Click on any PIN to open details on your PIN code keypad AX.
    - ↳ The "PinCode - Details" window will open.

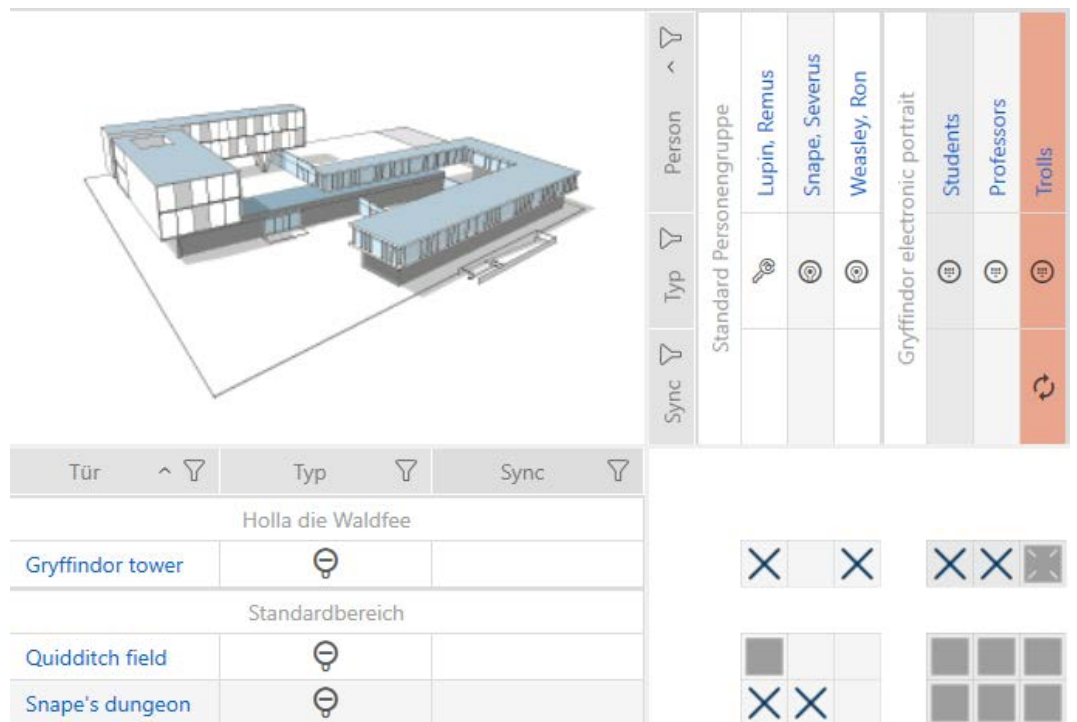


2. Use the ▼ to expand the settings for the PIN to be deleted.

- Click on  to highlight the PIN to be deleted.  
 ↳ Status field shows *Prepared to delete*.



- 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.

### 14.3.3 Blocking an AX2Go key

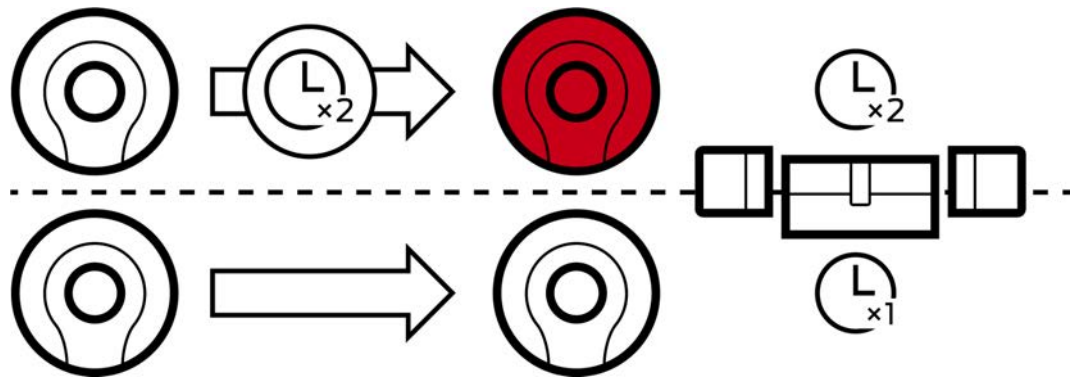
See *Blocking an AX2Go key* [▶ 217].

### 14.4 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.

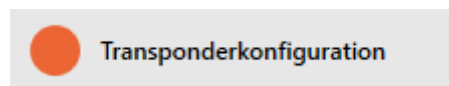
The identification medium can therefore inform each locking device that it should engage for twice as long for the identification medium in question.



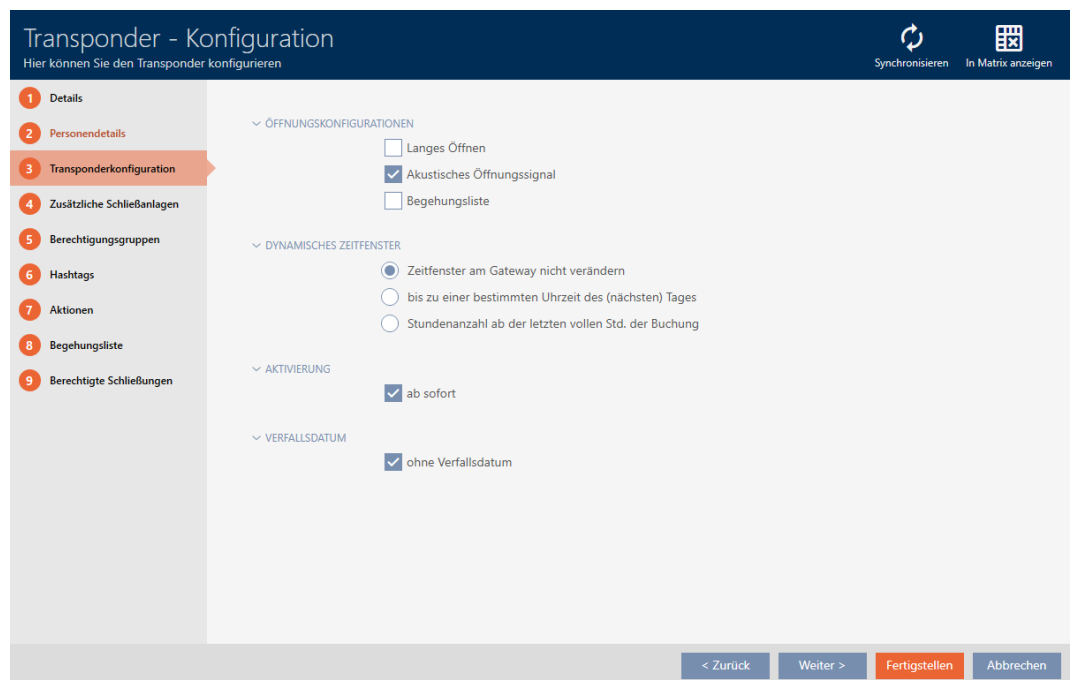
The maximum engagement interval remains 25 s:

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

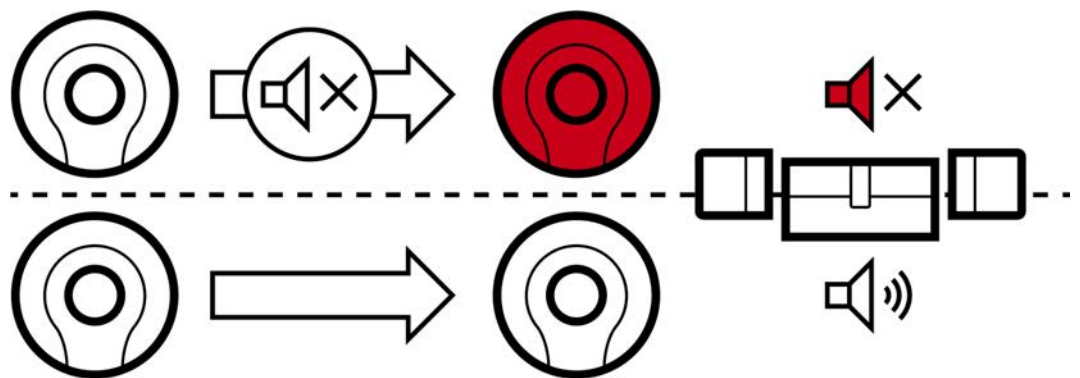
4. Click on the **Finish** button.
  - ↳ The identification medium window closes.
  - ↳ All locking devices will now open twice as long for this identification medium.

### 14.5 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.

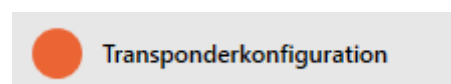


This means

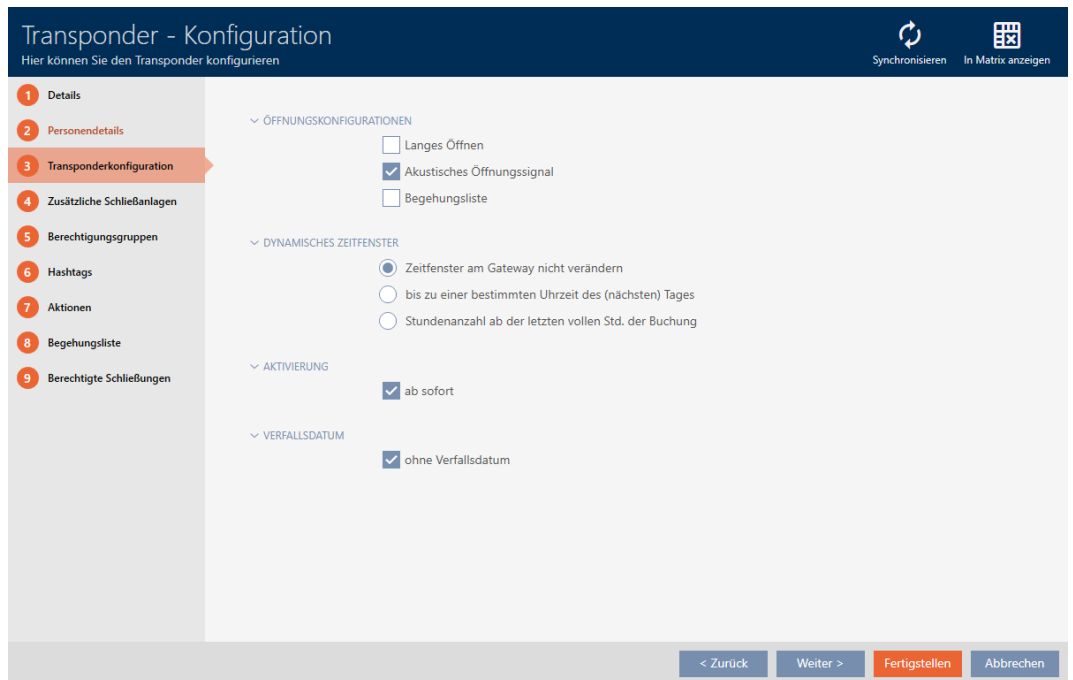
- identification media for which  Acoustic opening signal is deactivated will open all locking devices without emitting a beep.
- Other identification media will continue to open all locking devices with a beep sound as usual.

#### 14.5.1 Muting all locking devices for a transponder or a card

- ✓ 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.



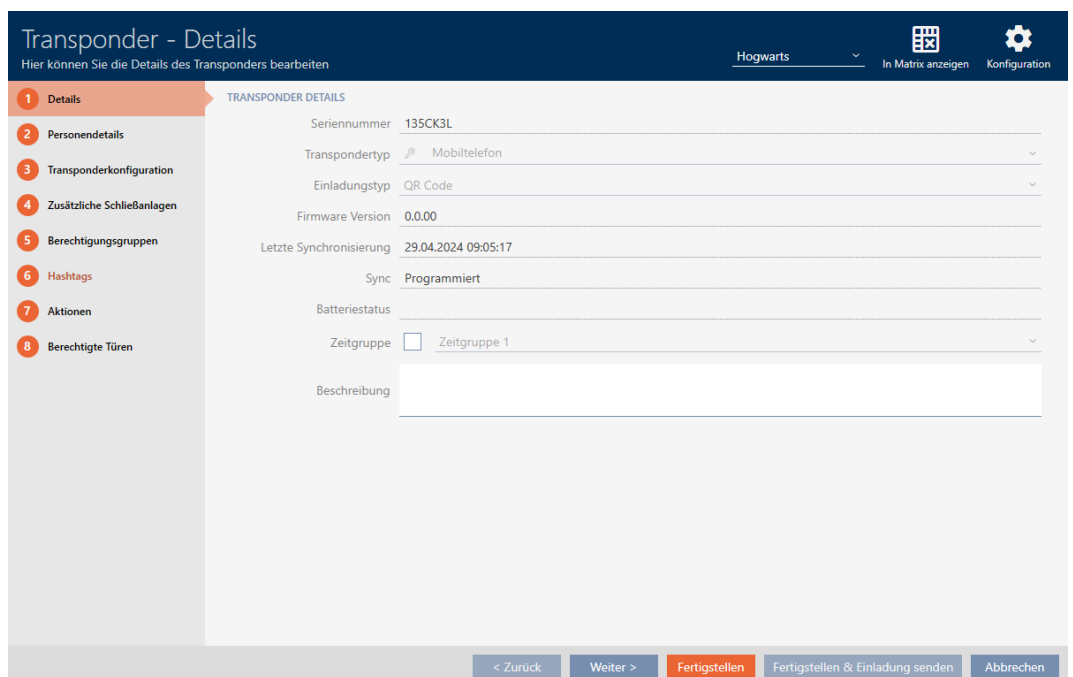
- ↳ Window switches to the "Transponder configuration" tab.



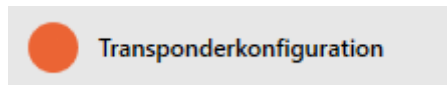
3. Activate the  Acoustic opening signal checkbox.
4. Click on the **Finish** button.
  - ↳ The identification medium window closes.
  - ↳ All locking devices are now muted for this identification medium.

### 14.5.2 Muting all locking devices for an AX2Go key

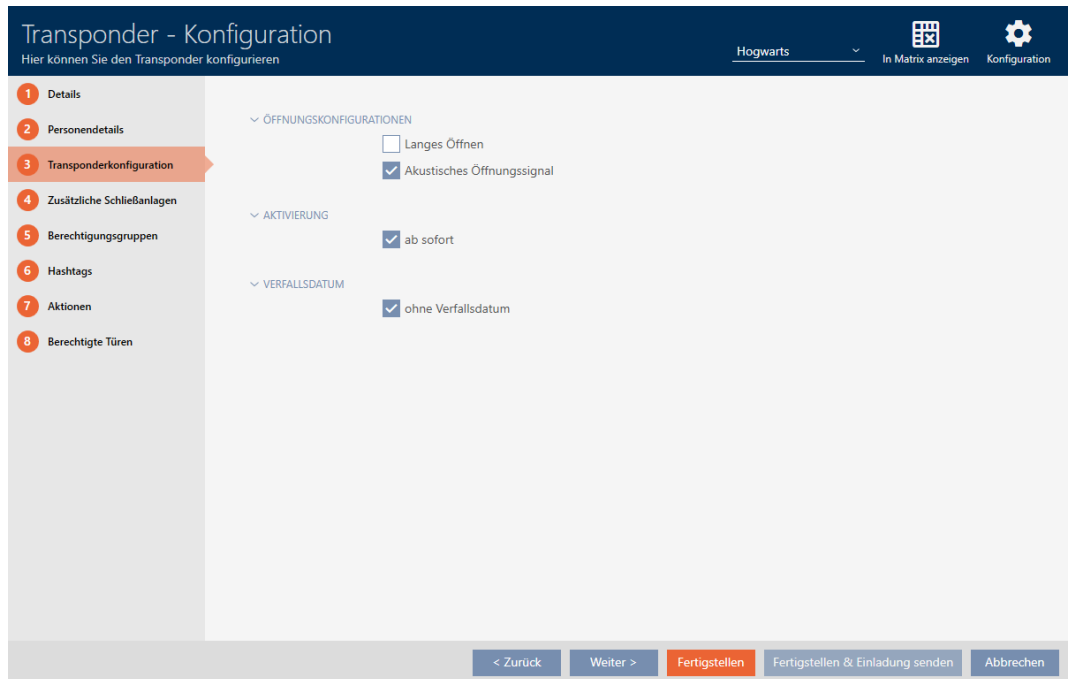
- ✓ AX2Go key at hand.
1. Click on the AX2Go key you wish to mute.
    - ↳ The AX2Go key window will open.



- Click on the **Transponder configuration** tab.



↳ Window switches to the "Transponder configuration" tab.



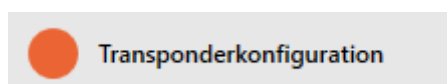
- Disable the  Acoustic opening signal check box.
- Click on the **Finish** button.
  - ↳ The AX2Go key window closes.
  - ↳ All locking devices are now muted for this AX2Go key.

### 14.6 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* [▶ 527]).

✓ Identification medium available.

- Click on the identification medium whose physical access list you wish to activate.
  - ↳ The identification medium window will open.
- 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.

### 14.7 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* [▶ 528]). See *Create time group* [▶ 56] and *Adding identification medium to time group* [▶ 341] to set up time management for identification media.

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

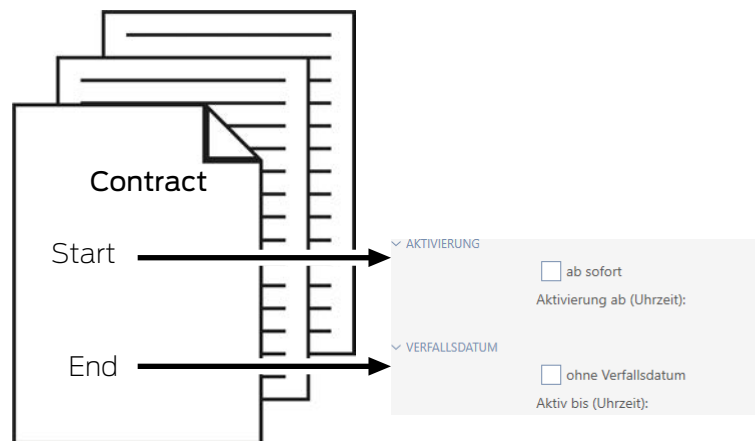
Your AXM Plus recognises two points in time for identification media:

- 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.

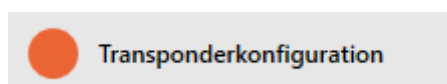
In this case, the AXM displays a warning, e.g.:



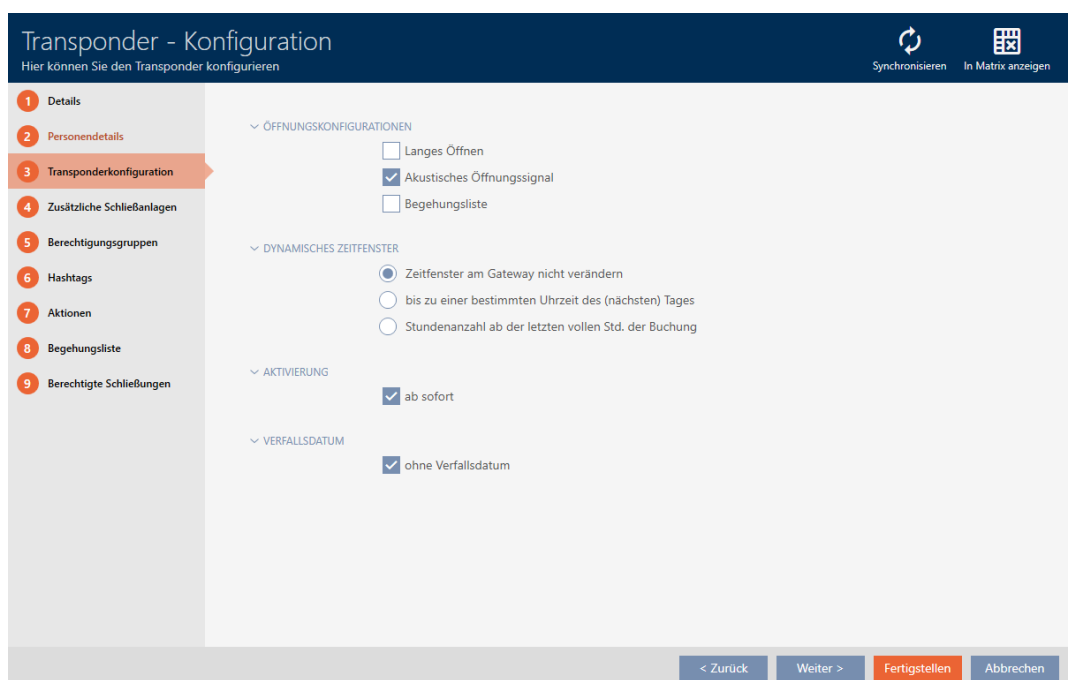


✓ Identification medium available.

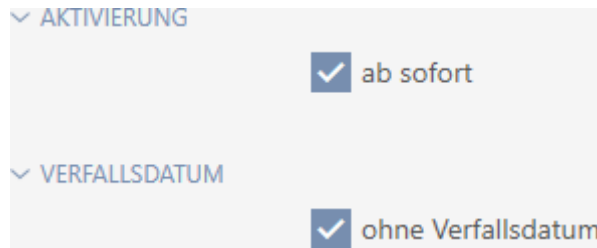
1. Click on the identification medium whose activation or expiry date you wish to set.
  - ↳ The identification medium window will open.
2. Click on the **Transponderkonfiguration** tab.



↳ Window switches to the "Transponder configuration" tab.

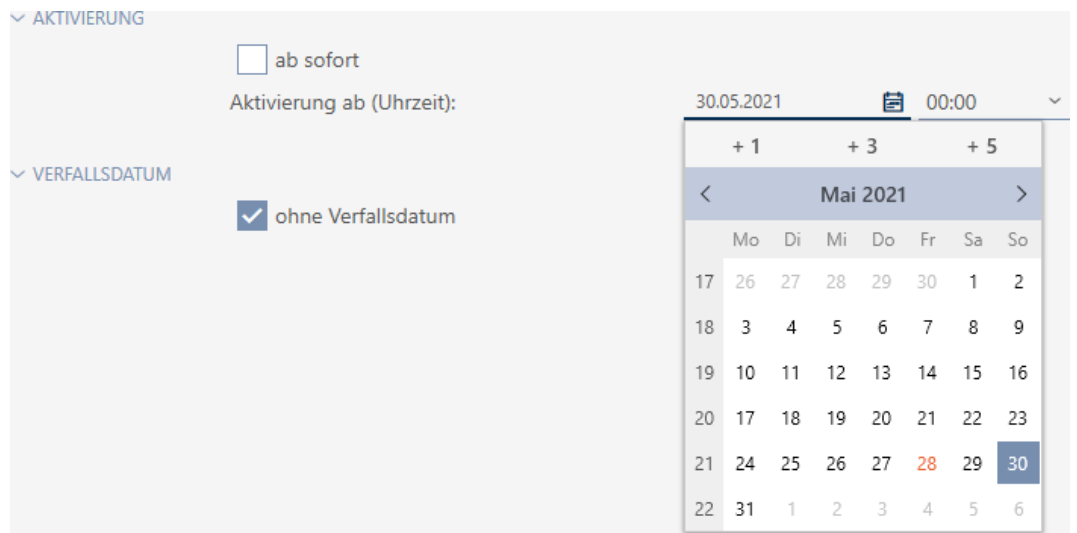


3. Open the "Activation" and "Expiry date" menus if necessary.



4. If you wish to set an activation date: Activate the  from now checkbox.

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.



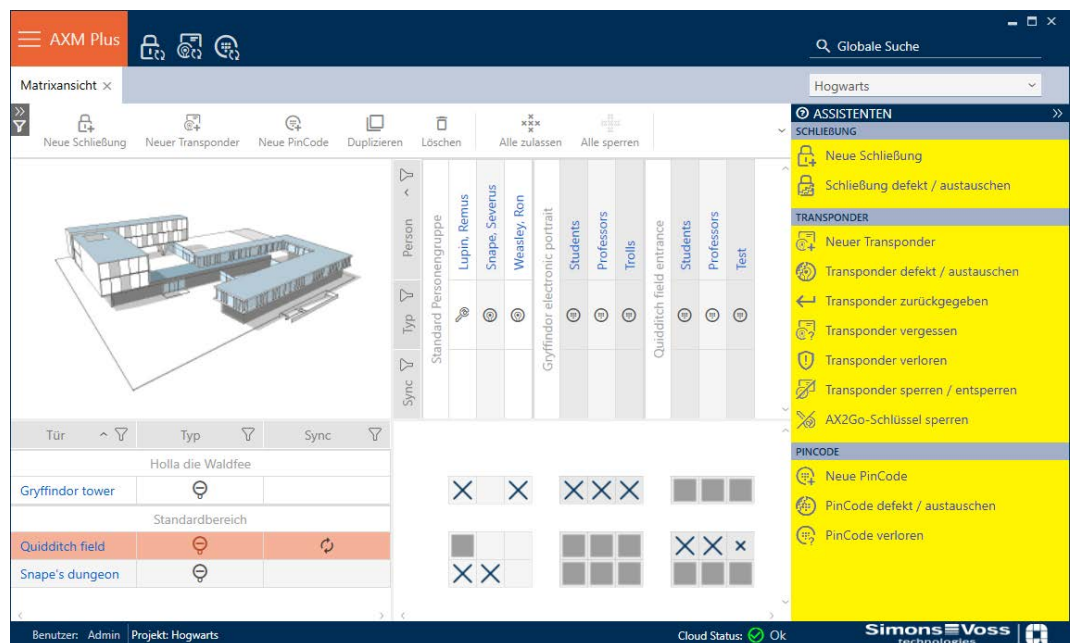
8. Click on the **Finish** button.
  - ↳ The identification medium window closes.
  - ↳ Identification medium will become active or inactive at the specified times.

### 14.9 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* [▶ 161]).

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* [▶ 512]).

**Transponders/replacement transponders are required again immediately:**

Suitable for:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
Identification media with undefined software status.	<ul style="list-style-type: none"> <li>■ Identification media with external damage (e.g. scratched).</li> <li>■ Identification media which needs to be replaced as a precaution (e.g. wet).</li> </ul>	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
	<p>Employee's transponder has fallen into the pool.</p> <p>Consequence: transponder works but at risk of failure due to exposure to water.</p>	<p>Employee's transponder has fallen into a camp fire.</p> <p>Consequence: transponder melted and permanently damaged.</p>

Procedure:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
<p><i>Repairing a card/transponder (resynchronising) [▶ 126]</i></p> <ol style="list-style-type: none"> <li>1. Reset (= TID available in database again)</li> <li>2. Resynchronise (= TID is immediately written back onto the same identification medium)</li> </ol> <p>The identification medium functions as before after it is repaired.</p>	<p><i>Resetting and replacing a card/transponder [▶ 131]</i></p> <ol style="list-style-type: none"> <li>1. Reset (= TID flagged as defective in database and removed from original identification medium)</li> <li>2. Synchronise replacement identification medium with new TID</li> </ol> <p>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.</p>	<p><i>Deleting and replacing a card/transponder [▶ 134]</i></p> <ol style="list-style-type: none"> <li>1. Delete (= TID flagged as defective in database) and removed from project</li> <li>2. Synchronise replacement identification medium with the new TID</li> </ol> <p>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.</p> <p>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 re-assigned.</p> <p>You can also hide defective or disabled identification media as an alternative to deletion (see <i>Hiding deactivated and defective identification media [▶ 436]</i>).</p>

**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
<p>The employee's transponder fell into camp fire at the employees' farewell party.</p> <p>Consequence: transponder melted and permanently damaged; employee no longer on staff.</p>	<p>The employee's transponder fell into camp fire at the employees' farewell party.</p> <p>Consequence: transponder melted and permanently damaged; employee no longer on staff.</p>

Procedure:

Taking out of use and leaving in project	Taking out of use and deleting from project
<p><i>Take card/transponder out of use and leave in project [▶ 142]</i></p> <p>1. Flag as taken out of operation (= TID flagged as defective in database)</p> <p>The permanently damaged identification medium retains its TID but the TID is flagged as "defective". New identification media cannot be created with this TID.</p> <p>This means that the same TID cannot be brought into circulation twice.</p>	<p><i>Taking a card/transponder out of use and deleting it from project [▶ 149]</i></p> <p>1. Delete (= TID flagged as defective in database) and removed from project</p> <p>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.</p> <p>You can also hide defective or disabled identification media as an alternative to deletion (see <i>Hiding deactivated and defective identification media [▶ 436]</i>).</p>

**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:

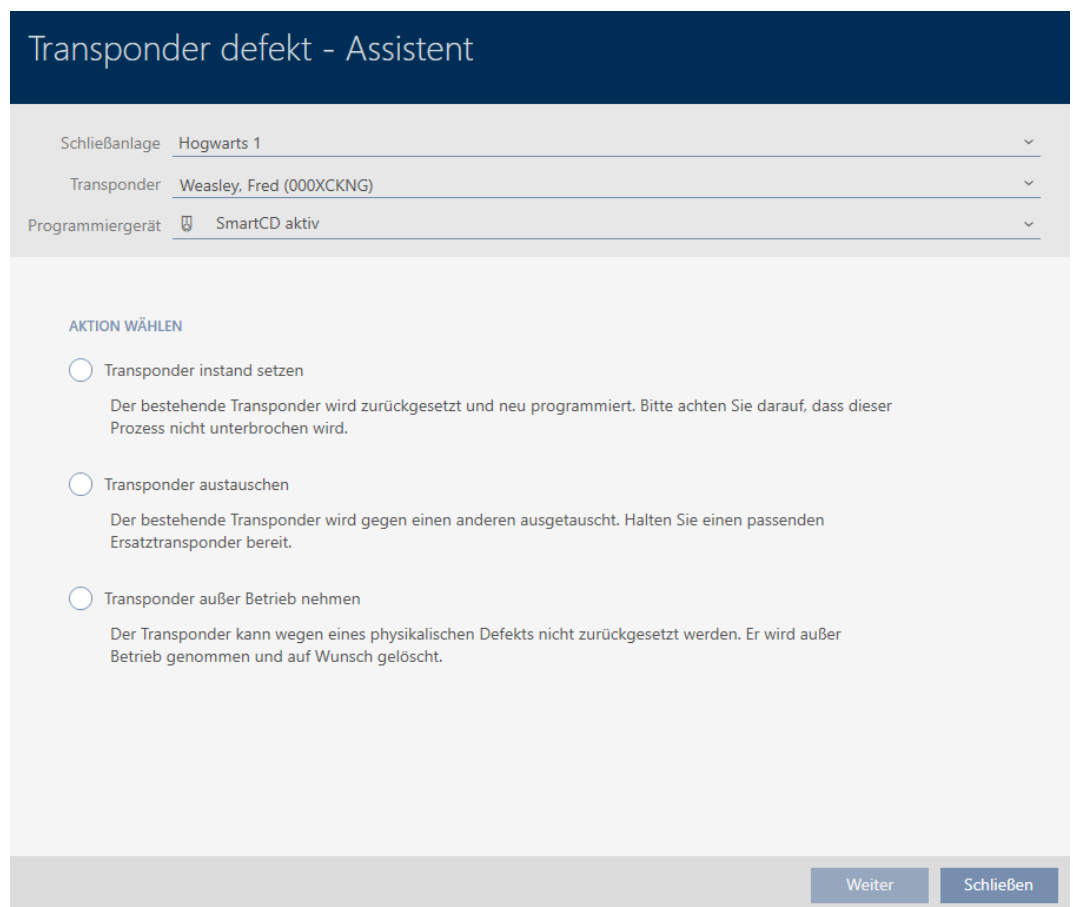
- Repair PinCode (see *Repairing a PIN code keypad (resynchronising) [▶ 127]*)
- Reset and PinCode (manual; not via wizard - see *Resetting and replacing a PIN code keypad [▶ 134]*)
- Delete and PinCode (see *Deleting and replacing a PIN code keypad [▶ 137]*)

- Decommission PinCode and leave in the project (see *Taking a PIN code keypad out of use and leaving it in project [▶ 145]*)
- Decommission PinCode and remove from project (see *Taking a PIN code keypad out of use and deleting it from project [▶ 151]*)

### 14.9.1 Repairing/resynchronising

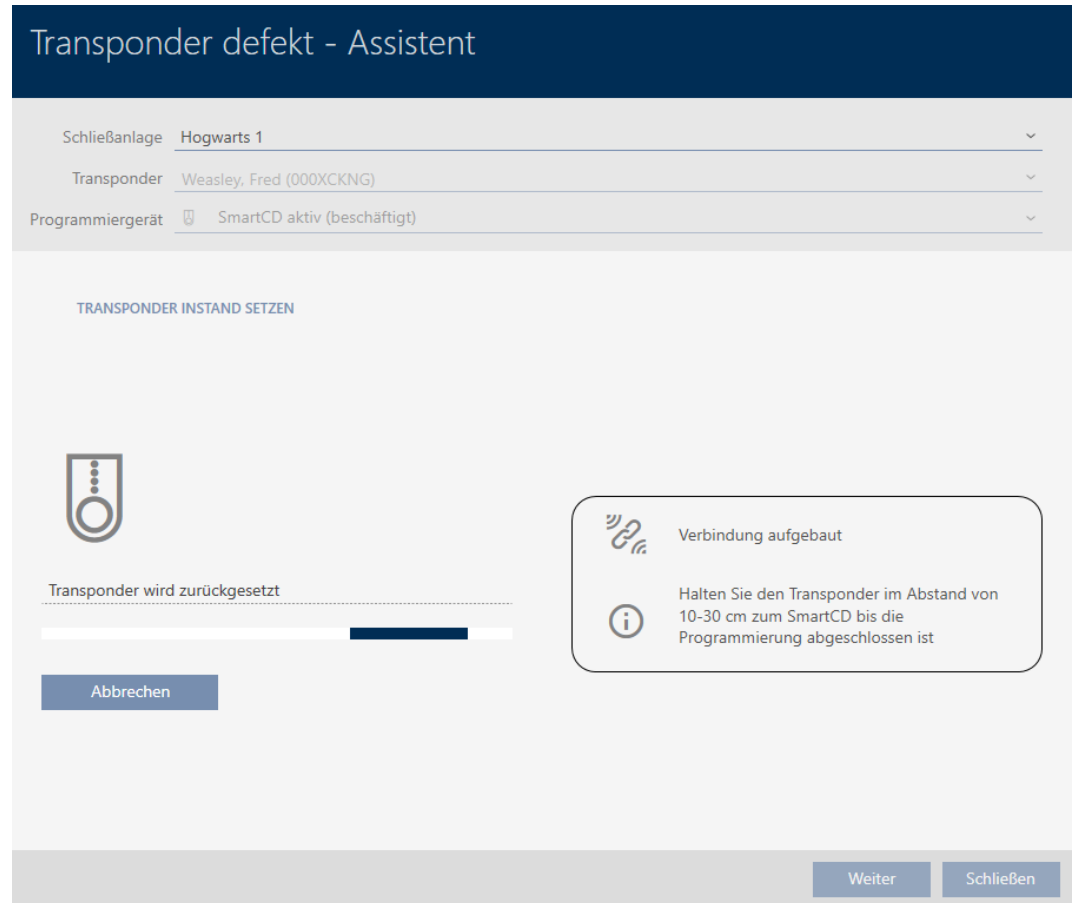
#### 14.9.1.1 Repairing a card/transponder (resynchronising)

- ✓ 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 [▶ 44]*).
  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.

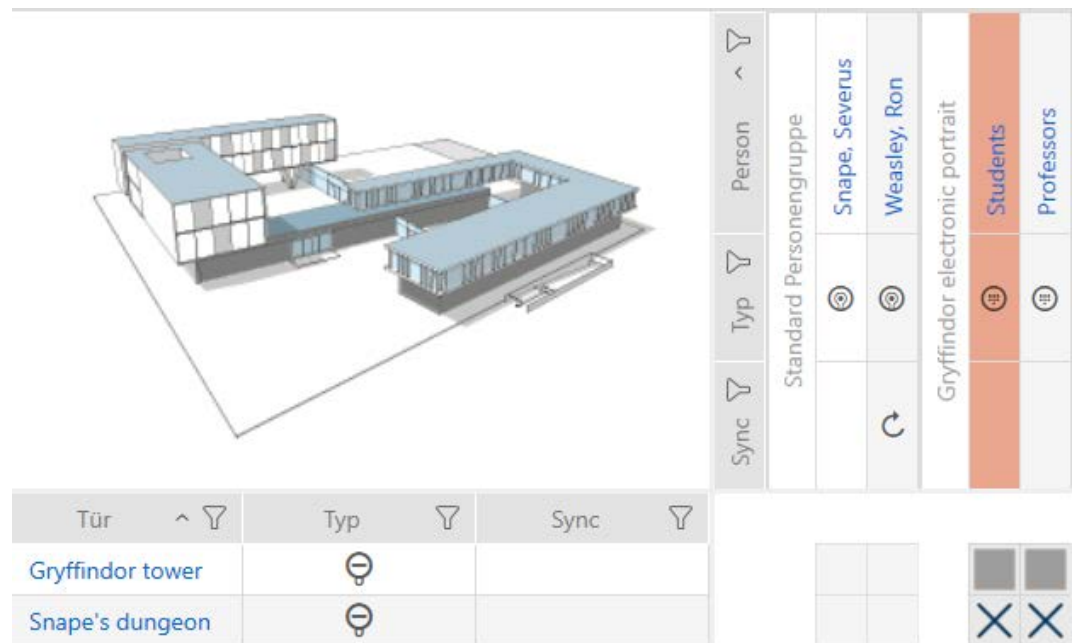
**TRANSPONDER INSTAND SETZEN**  
 Die Aktion wurde erfolgreich durchgeführt


#### 14.9.1.2 Repairing a PIN code keypad (resynchronising)

- ✓ 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* [▶ 44]).

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.

### PinCode defekt / austauschen - Assistent

Schließanlage	Hogwarts	▼
PinCode	<input checked="" type="radio"/> Gryffindor electronic portrait (0873CDF)	▼
Programmiergerät	 SmartStick AX	▼

**AKTION WÄHLEN**

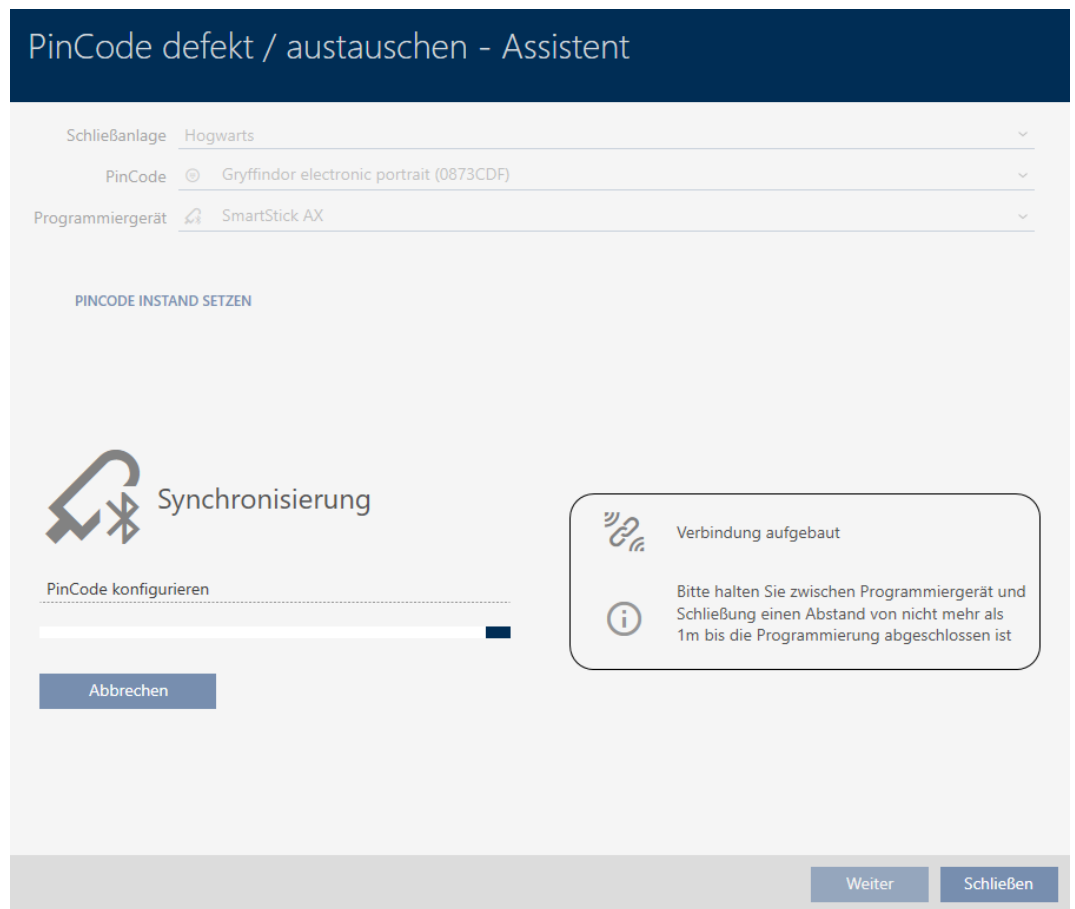
PinCode instand setzen  
Die bestehende PinCode wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

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.

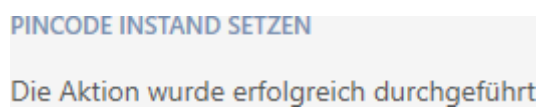
**Weiter** **Schließen**

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.

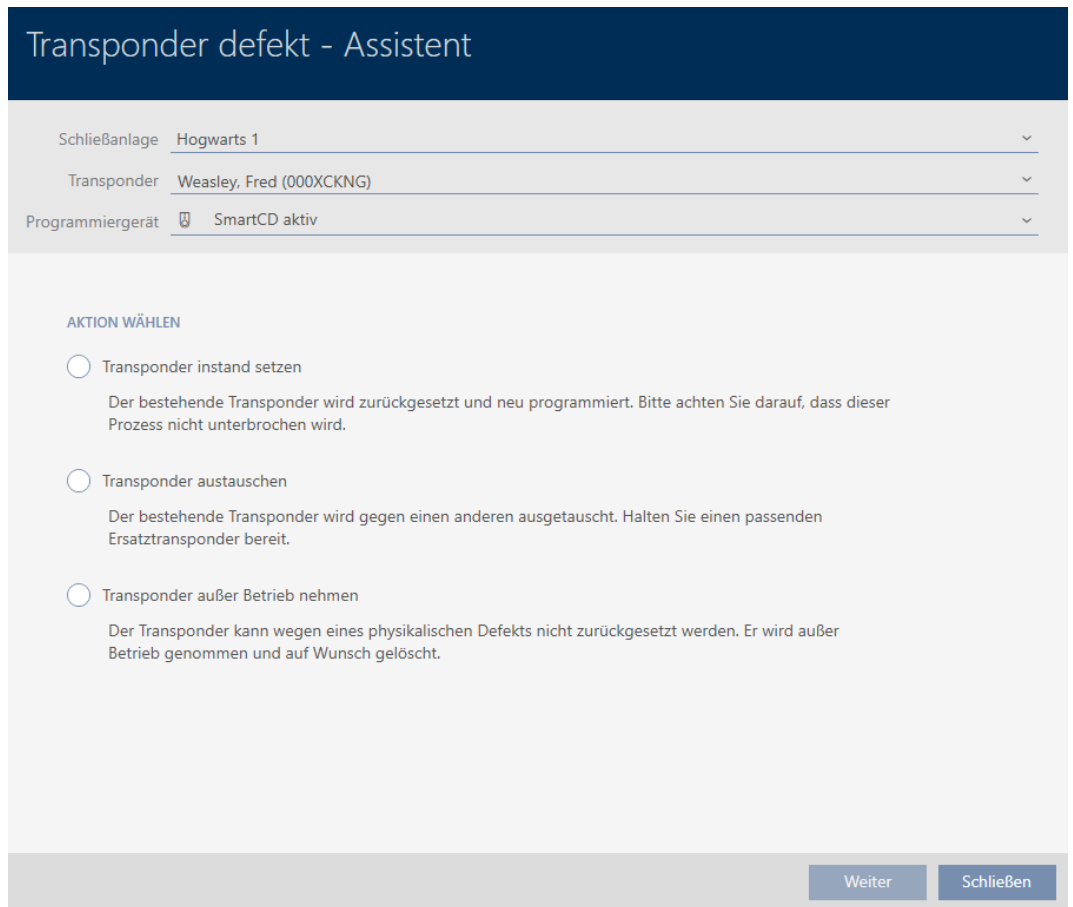


### 14.9.2 Resetting and replacing

#### 14.9.2.1 Resetting and replacing a card/transponder

- ✓ 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* [▶ 44]).
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.

**TRANSPONDER AUSTAUSCHEN**

Bitte halten Sie den Ersatztransponder bereit.

Der Transponder wird in der Software von den Daten des defekten Transponders bereinigt.


Die Programmierung des Ersatztransponders wird automatisch gestartet.

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

**Transponder defekt - Assistent**

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Fred (000XCKNG)	▼
Programmiergerät	SmartCD aktiv (beschäftigt)	▼


TRANSPONDER AUSTAUSCHEN




Programmierung

Schließanlagendaten werden eingerichtet

Abbrechen

 Verbindung aufgebaut

 Halten Sie den Transponder im Abstand von 10-30 cm zum SmartCD bis die Programmierung abgeschlossen ist

Weiter

Schließen

- ↳ Replacement identification medium is now synchronised.

**TRANSPONDER AUSTAUSCHEN**

Die Aktion wurde erfolgreich durchgeführt



#### 14.9.2.2 Resetting and replacing a PIN code keypad

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

- ✓ 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* [▶ 424]).
  2. Create a new PIN code keypad (see *Creating PIN code keypads* [▶ 96]).
  3. Synchronise the new PIN code keypad (see *Synchronising a PIN code keypad* [▶ 415]).

#### 14.9.3 Delete and replace

##### 14.9.3.1 Deleting and replacing a card/transponder

- ✓ 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* [▶ 44]).
  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.

## Transponder defekt - Assistent

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Fred (000XCKNG)	▼
Programmiergerät	SmartCD aktiv	▼

**AKTION WÄHLEN**

Transponder instand setzen  
Der bestehende Transponder wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Transponder austauschen  
Der bestehende Transponder wird gegen einen anderen ausgetauscht. Halten Sie einen passenden Ersatztransponder bereit.

Transponder außer Betrieb nehmen  
Der Transponder kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Er wird außer Betrieb genommen und auf Wunsch gelöscht.

Weiter Schließen

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

## Transponder zurücksetzen

Wollen Sie den alten Transponder zurücksetzen?



Ja Nein

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.

#### TRANSPONDER AUSTAUSCHEN

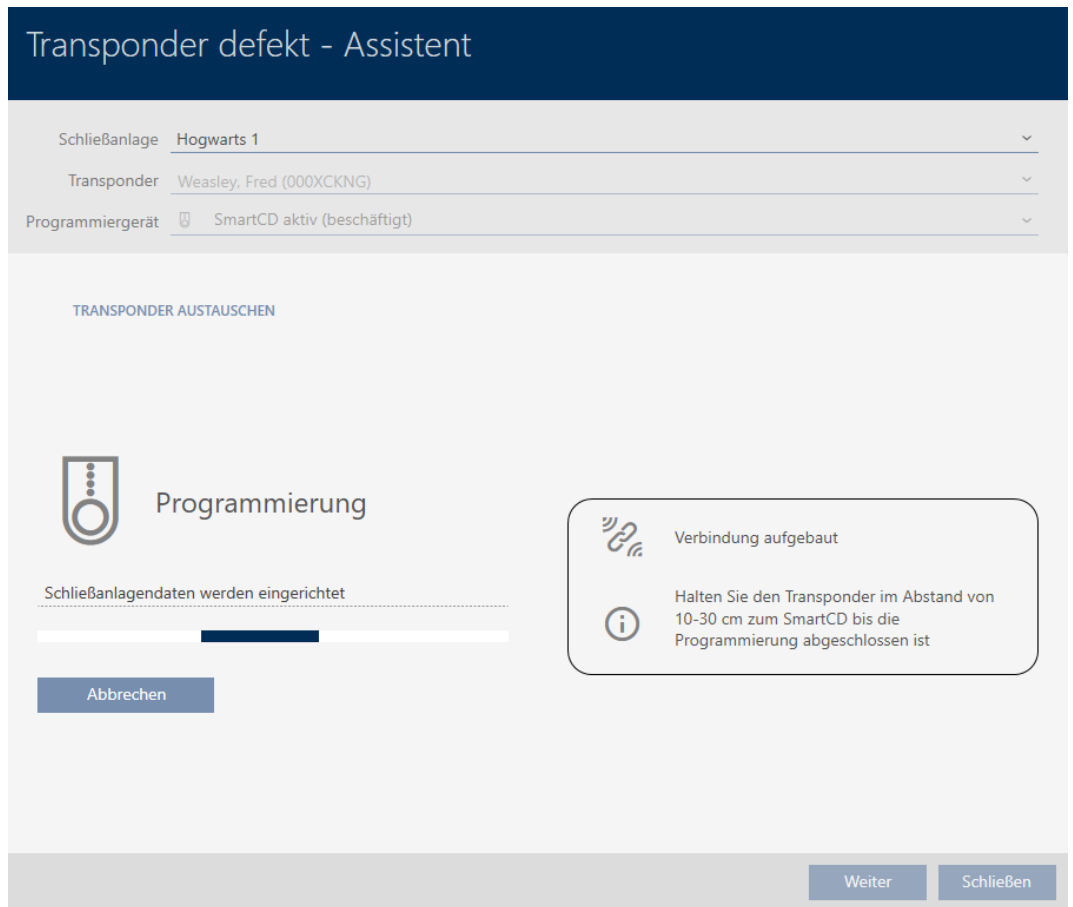
Bitte halten Sie den Ersatztransponder bereit.

Der Transponder wird in der Software von den Daten des defekten Transponders bereinigt.

Die Programmierung des Ersatztransponders wird automatisch gestartet.

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





↳ Replacement identification medium is now synchronised.

**TRANSPONDER AUSTAUSCHEN**  
 Die Aktion wurde erfolgreich durchgeführt

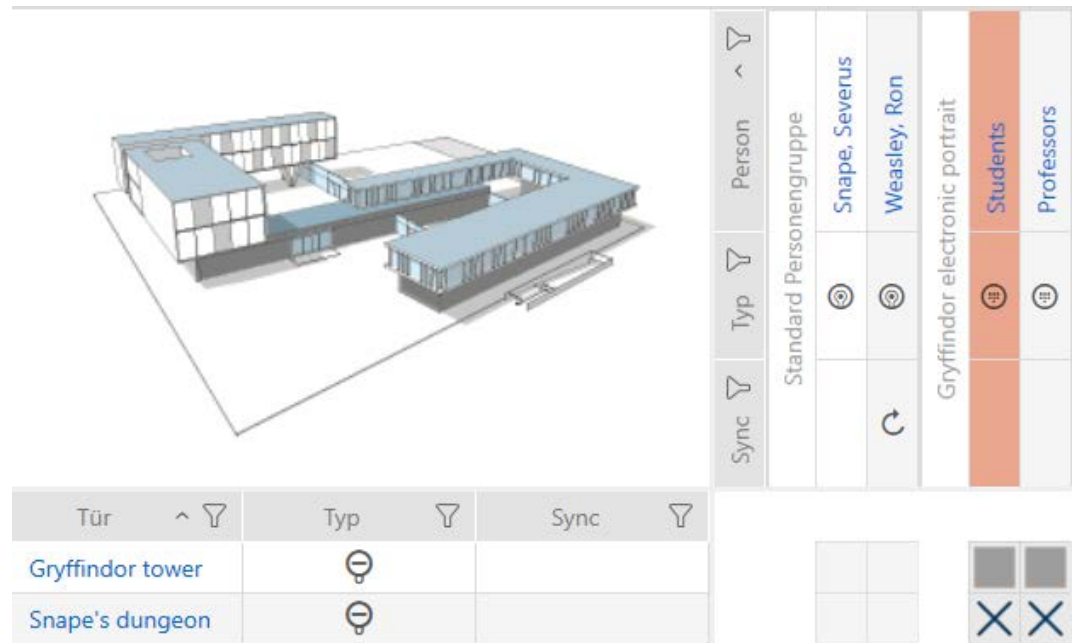
You can now reset the identification medium (see *Deleting an identification medium* [▶ 108]).


### 14.9.3.2 Deleting and replacing a PIN code keypad

- ✓ 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* [▶ 44]).

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.

## PinCode defekt / austauschen - Assistent

Schließenanlage	Hogwarts	▼
PinCode	<input checked="" type="radio"/> 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 passende Ersatz-PinCode bereit.

PinCode außer Betrieb nehmen  
Die PinCode kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Sie wird außer Betrieb genommen und auf Wunsch gelöscht.

Weiter Schließen

5. Click on the **Next** button.

↳ Confirmation dialogue will open.

## PinCode austauschen

Sind Sie sicher, dass die PinCode physikalisch defekt ist?

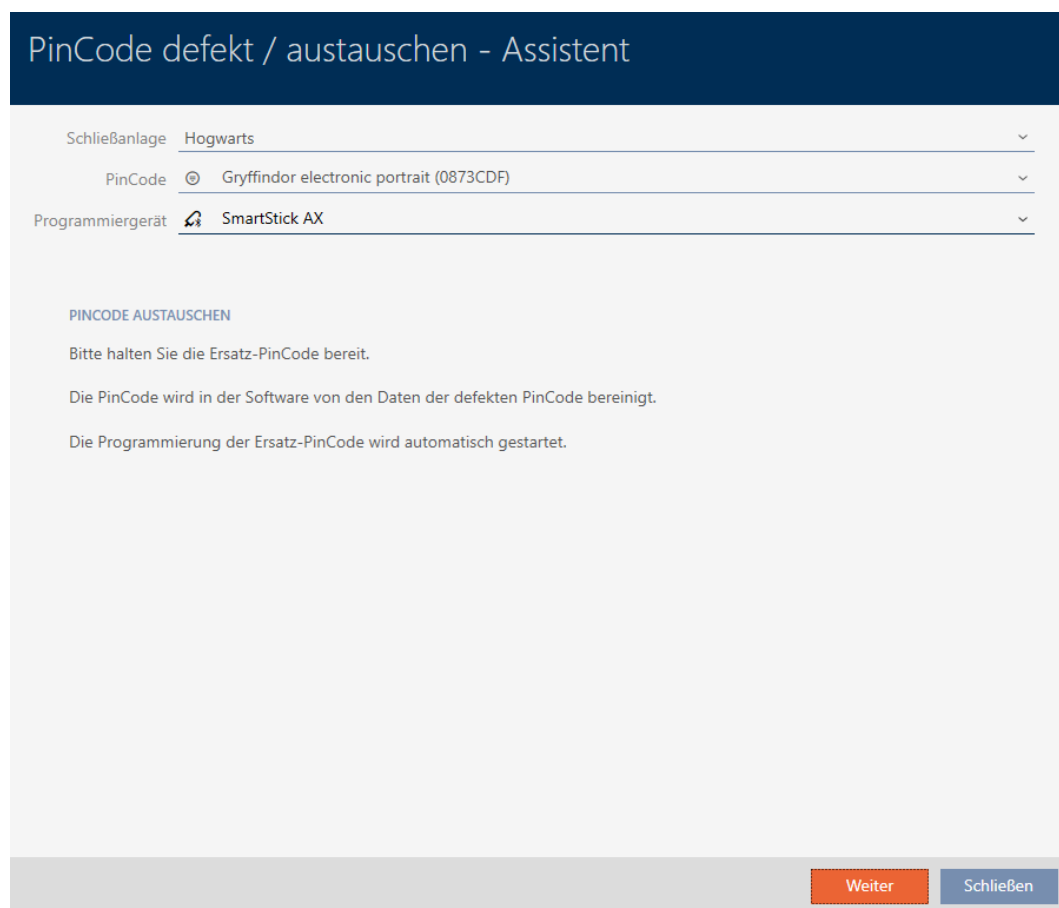
Warnung:

Wenn die PinCode nicht defekt ist, können unter Umständen Duplikate der PinCode entstehen, was zu einer Sicherheitslücke führen kann.

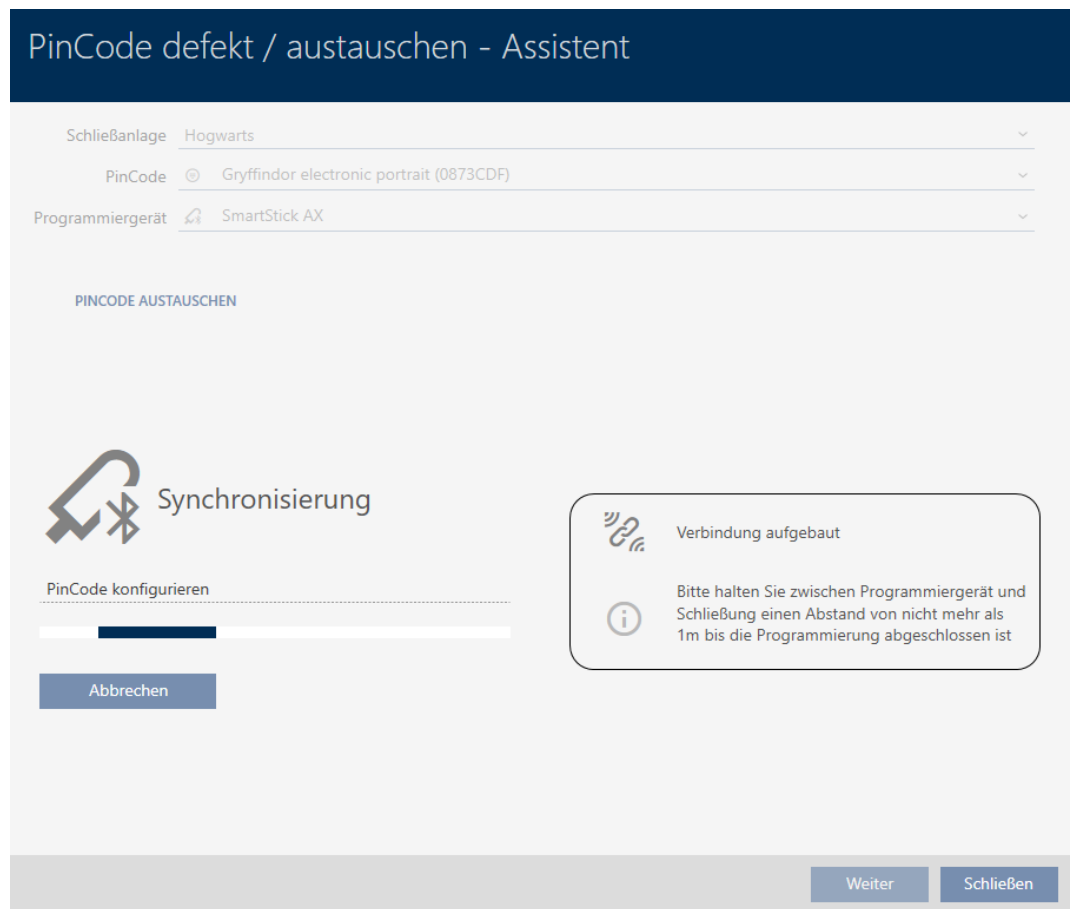


Ja Nein Abbrechen

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.

**PINCODE AUSTAUSCHEN**  
 Die Aktion wurde erfolgreich durchgeführt

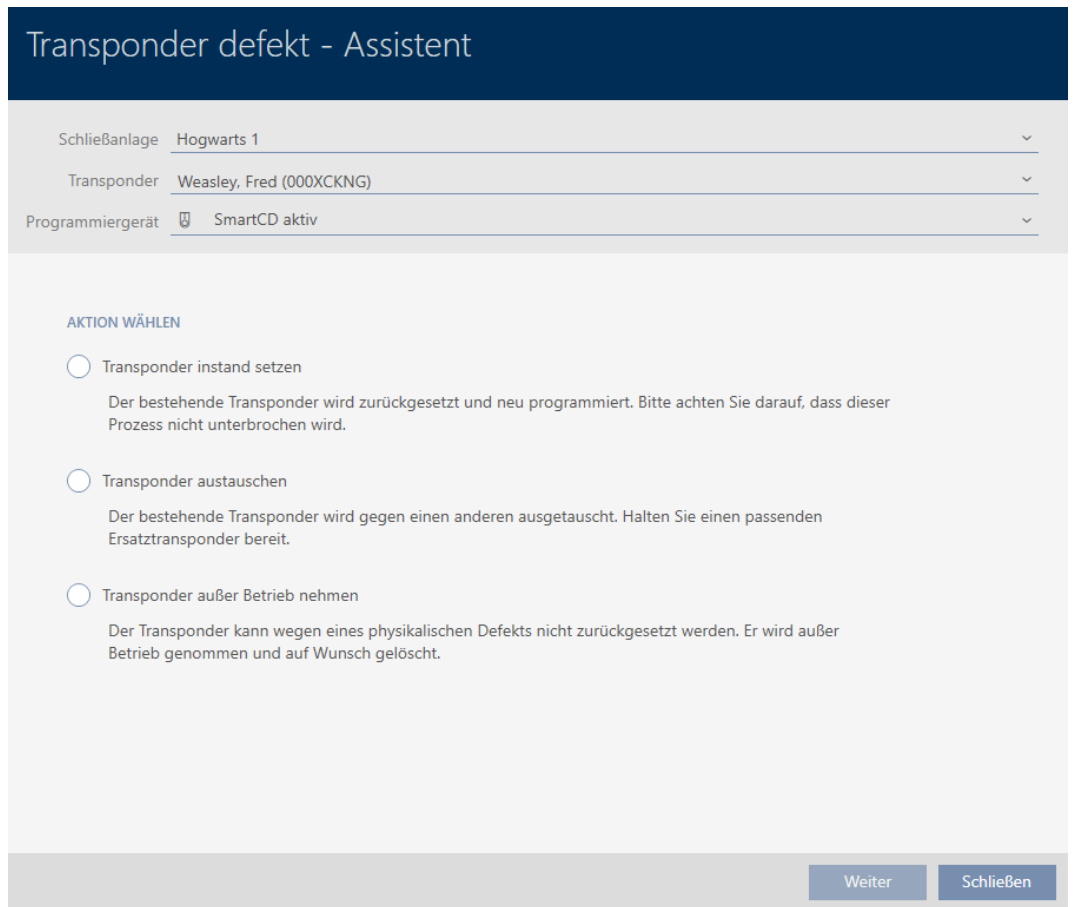
#### 14.9.4 Take out of use and leave in project

##### 14.9.4.1 Take card/transponder out of use and leave in project

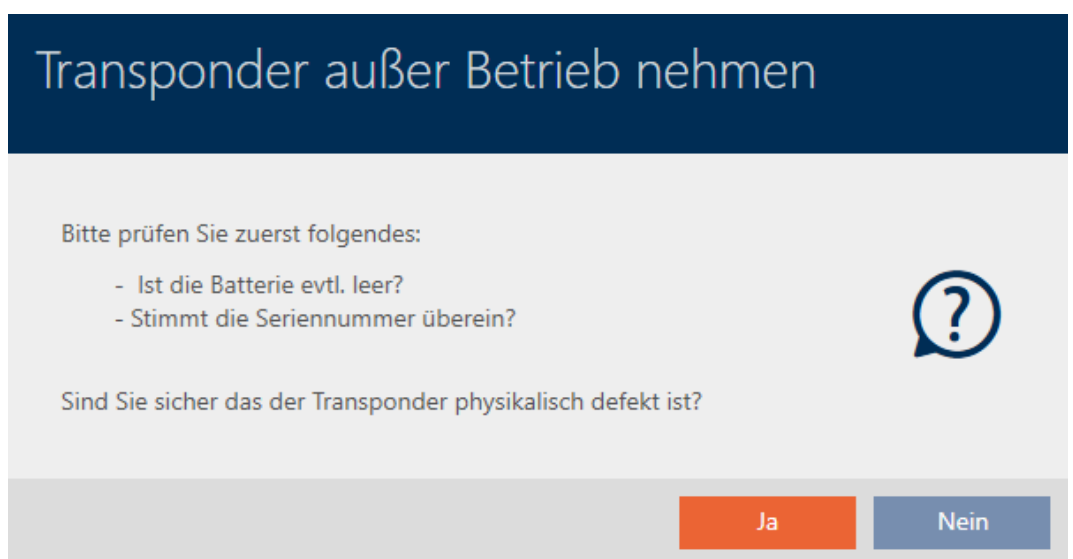
✓ Identification media list or matrix open.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
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.

#### TRANSPONDER AUßER BETRIEB NEHMEN

Die Aktion wurde erfolgreich durchgeführt

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



Sync	Typ	Person
	🎯	Weasley, Ron
🔄	🎯	Weasley, Percy
	🎯	Weasley, Fred
🔄	🎯	Lovegood, Luna

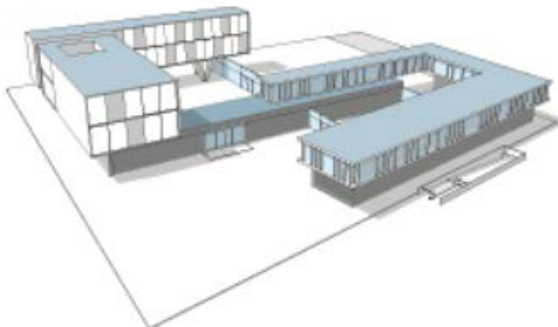
  

✕	☐	✕	
	☐		➡✕
✕	☐	✕	

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

✓ List with PIN code keypads or matrix open.

1. Use 🎯 to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
2. Flag a PIN associated with the defective PIN code keypad.




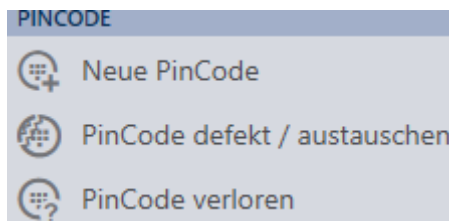
Sync	Typ	Person
		Standard Personengruppe
	🎯	Snape, Severus
🔄	🎯	Weasley, Ron
		Gryffindor electronic portrait
	🎯	Students
	🎯	Professors

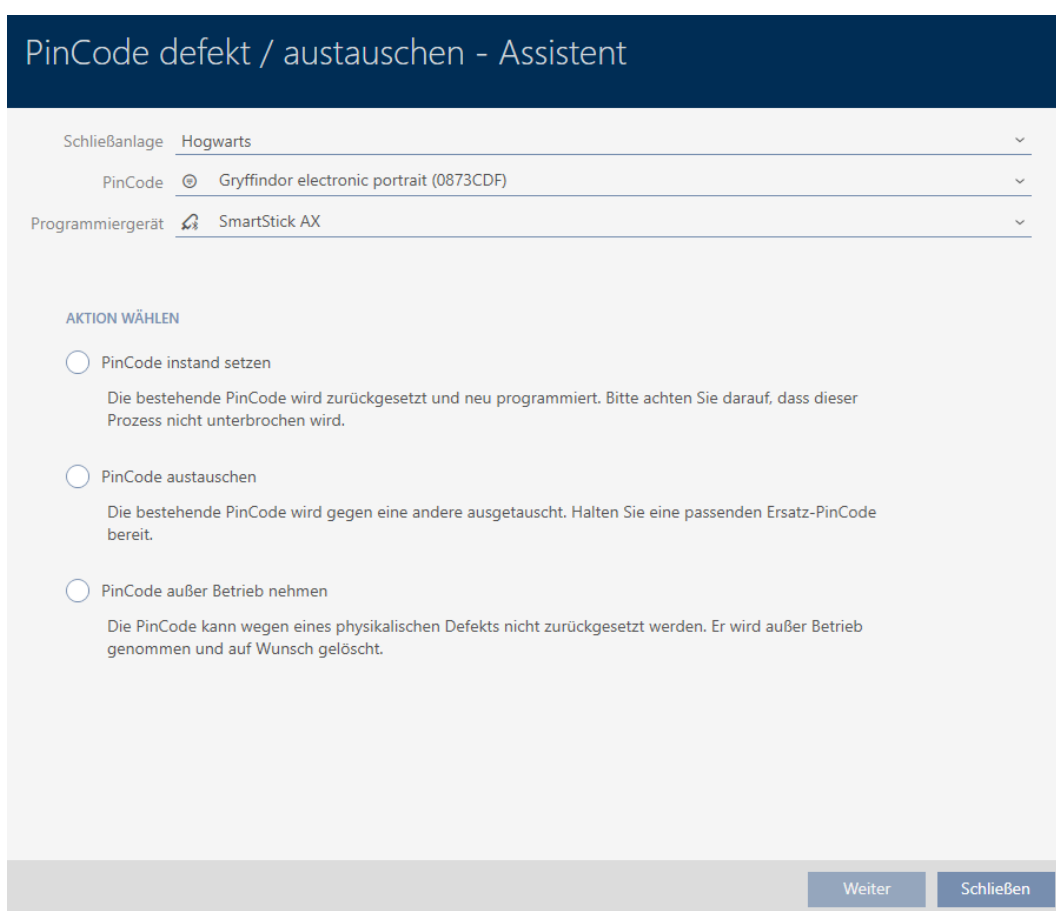
Tür	Typ	Sync
Gryffindor tower	🎯	
Snape's dungeon	🎯	


✕	✕

- 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.

## PinCode defekt / austauschen - Assistent

Schließenanlage 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

5. Click on the **Next** button.

↳ A confirmation dialogue to take out of use will open.

## PinCode außer Betrieb nehmen

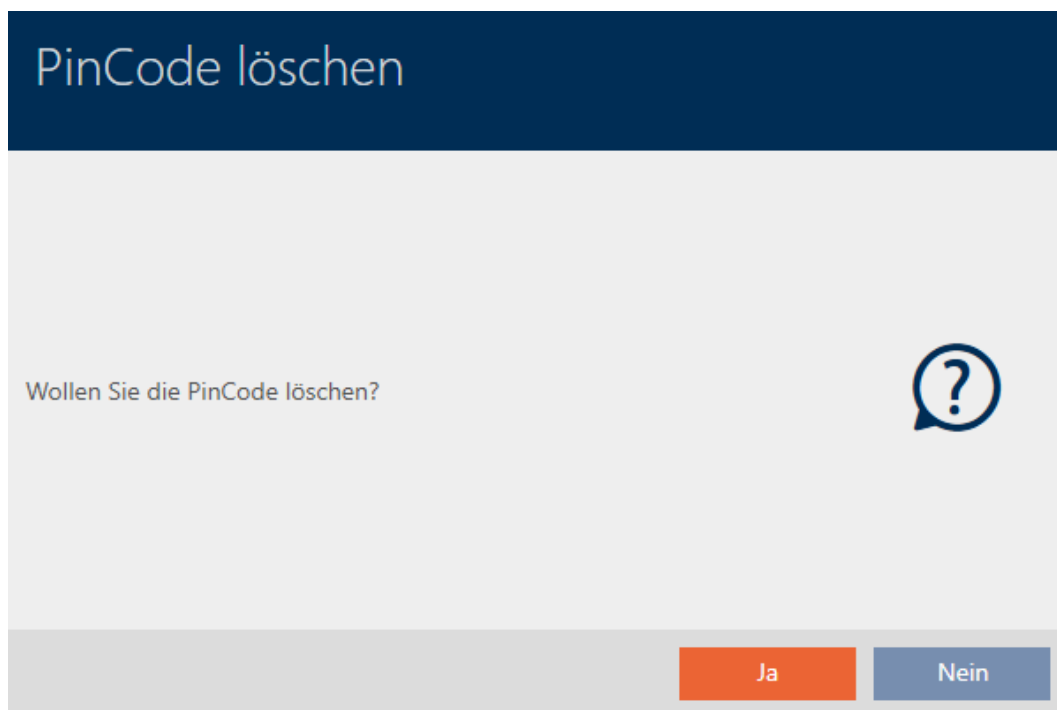
Bitte prüfen Sie zuerst folgendes:

- Ist die Batterie evtl. leer?
- Stimmt die Seriennummer überein?

Sind Sie sicher das die PinCode physikalisch defekt ist?

Ja Nein

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

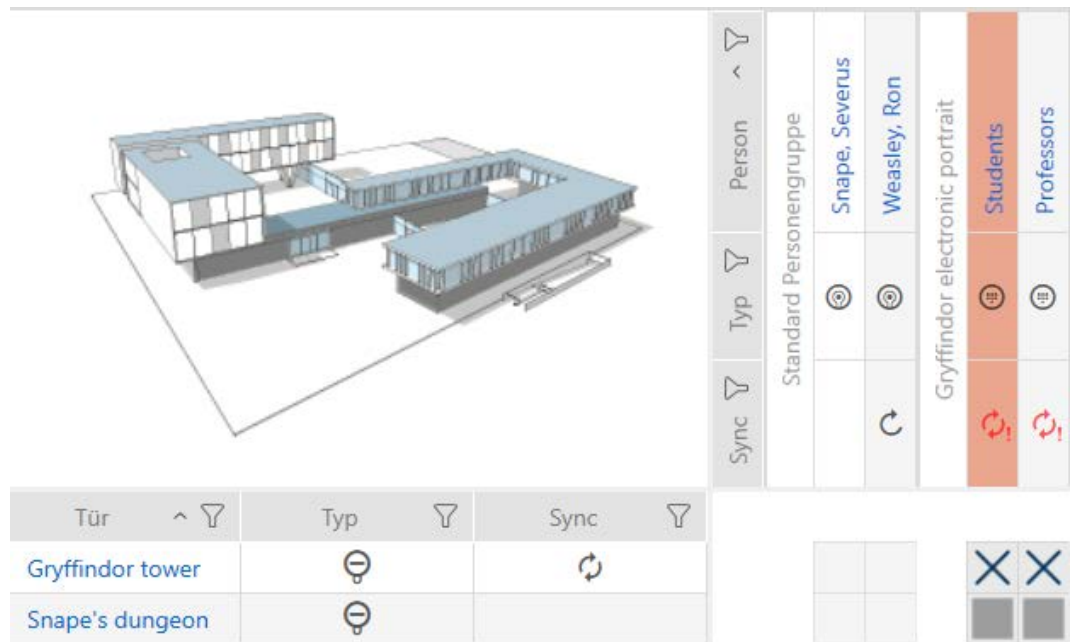


7. Click on the **No** button.
  - ↳ Confirmation dialogue to delete the PIN code keypad closes.
  - ↳ The PIN code keypad has been taken out of operation.

#### PINCODE AUßER BETRIEB NEHMEN

Die Aktion wurde erfolgreich durchgeführt

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



### 14.9.5 Taking out of use and deleting from the project

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

✓ Identification media list or matrix open.

1. Use ☿ to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
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.

## Transponder defekt - Assistent

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Fred (000XCKNG)	▼
Programmiergerät	SmartCD aktiv	▼

**AKTION WÄHLEN**

Transponder instand setzen  
Der bestehende Transponder wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Transponder austauschen  
Der bestehende Transponder wird gegen einen anderen ausgetauscht. Halten Sie einen passenden Ersatztransponder bereit.

Transponder außer Betrieb nehmen  
Der Transponder kann wegen eines physikalischen Defekts nicht zurückgesetzt werden. Er wird außer Betrieb genommen und auf Wunsch gelöscht.

Weiter Schließen

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

## Transponder außer Betrieb nehmen

Bitte prüfen Sie zuerst folgendes:

- Ist die Batterie evtl. leer?
- Stimmt die Seriennummer überein?

Sind Sie sicher das der Transponder physikalisch defekt ist?

Ja Nein

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.

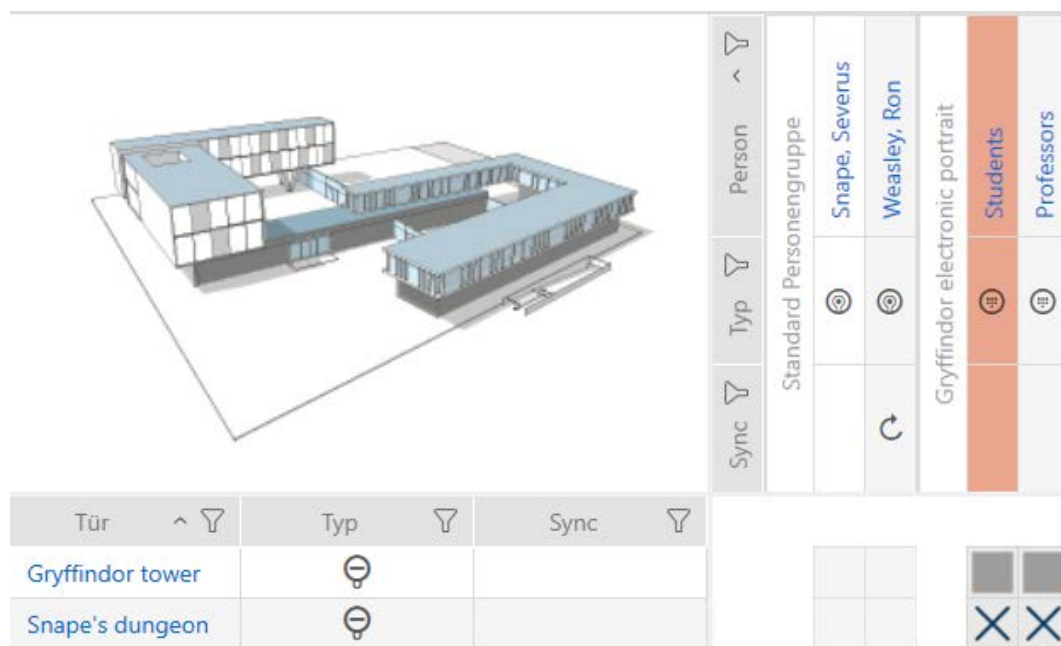
**TRANSPONDER AUßER BETRIEB NEHMEN**

Die Aktion wurde erfolgreich durchgeführt

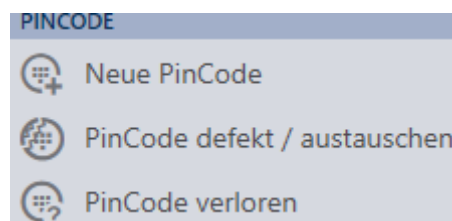
#### 14.9.5.2 Taking a PIN code keypad out of use and deleting it from project

- ✓ List with PIN code keypads or matrix open.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

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.

## PinCode defekt / austauschen - Assistent

Schließenanlage	Hogwarts	▼
PinCode	<input checked="" type="radio"/> 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

5. Click on the **Next** button.

↳ A confirmation dialogue to take out of use will open.

## PinCode außer Betrieb nehmen

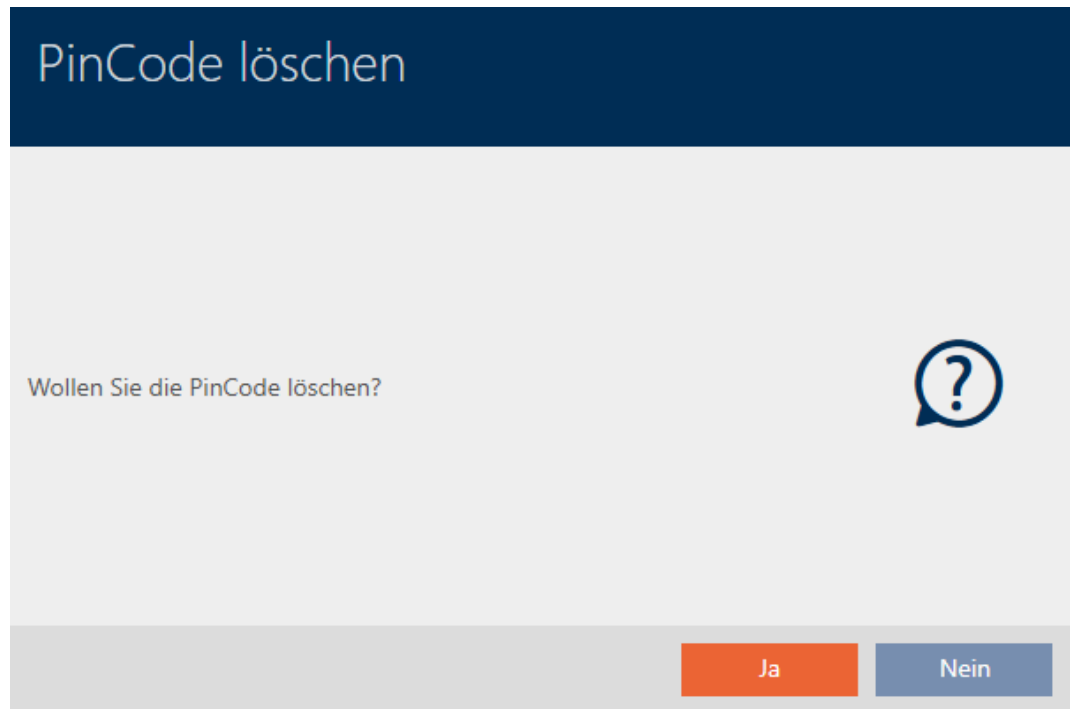
Bitte prüfen Sie zuerst folgendes:

- Ist die Batterie evtl. leer?
- Stimmt die Seriennummer überein?

Sind Sie sicher das die PinCode physikalisch defekt ist?

Ja
Nein

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.

**PINCODE AUßER BETRIEB NEHMEN**  
Die Aktion wurde erfolgreich durchgeführt

## 14.10 Duplicating forgotten identification medium temporarily



### 14.10.1 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* [▶ 512] for information on the connection between TID and identification medium).

- ✓ 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* [▶ 44]).
  2. Select the forgotten identification medium.
  3. Click the  **Forgot transponder** button in the "Wizards" section.
    - ↳ Wizard for forgotten identification media will open.

## Transponder vergessen

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Percy (000XCKNG)	▼
Programmiergerät	 SmartCD aktiv	▼

**TRANSPONDER VERGESSEN**

**Ereignis:**  
Der gewählte Transponder ist für kurze Zeit nicht verfügbar, der Aufenthaltsort ist aber bekannt.

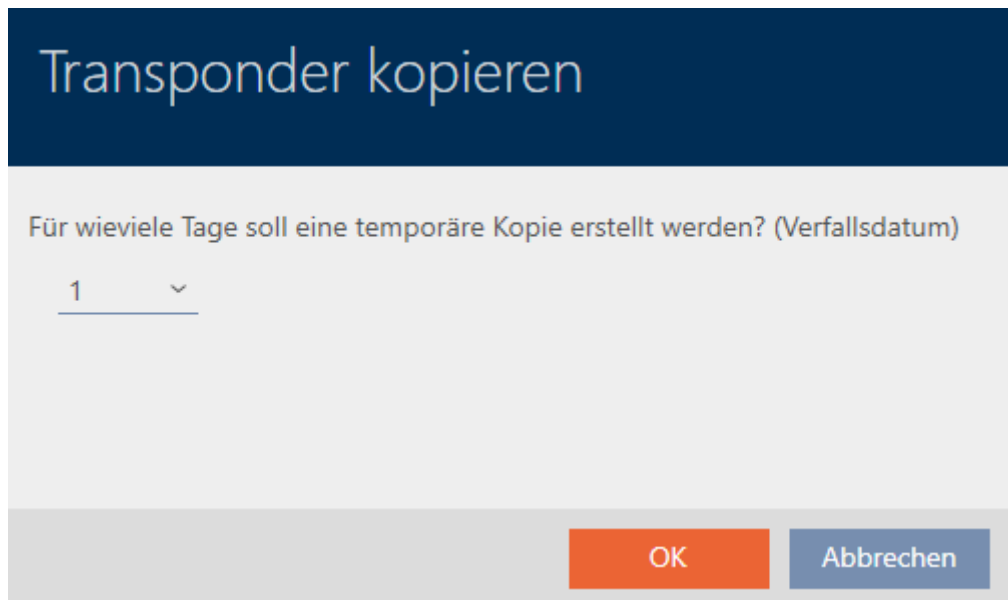
**Hinweis:**  
Halten Sie einen Ersatztransponder bereit.

**Aktion:**  
Der Assistent erstellt eine zeitlich begrenzte Kopie des betroffenen Transponders, welcher sofort programmiert werden kann.

- Bitte vergewissern Sie sich, dass der ausgewählte Transponder nicht verlorengegangen ist
- Ein zeitlich begrenzter Ersatz für den Transponder wird erstellt

Weiter
Schließen

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



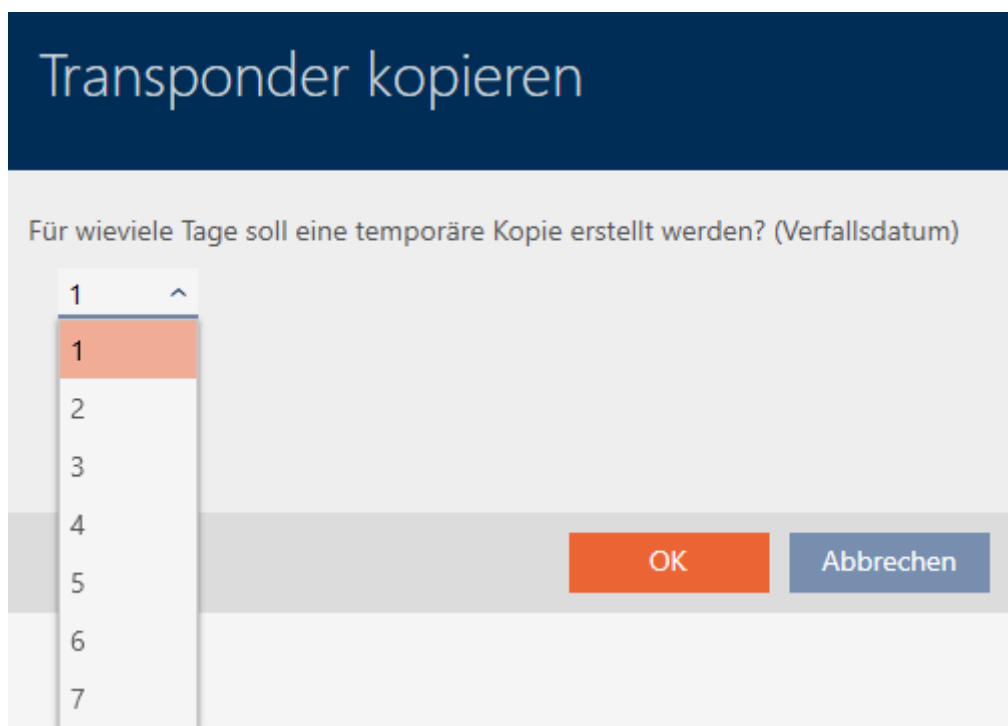
Transponder kopieren

Für wieviele Tage soll eine temporäre Kopie erstellt werden? (Verfallsdatum)

1

OK Abbrechen

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



Transponder kopieren

Für wieviele Tage soll eine temporäre Kopie erstellt werden? (Verfallsdatum)

1

1

2

3

4

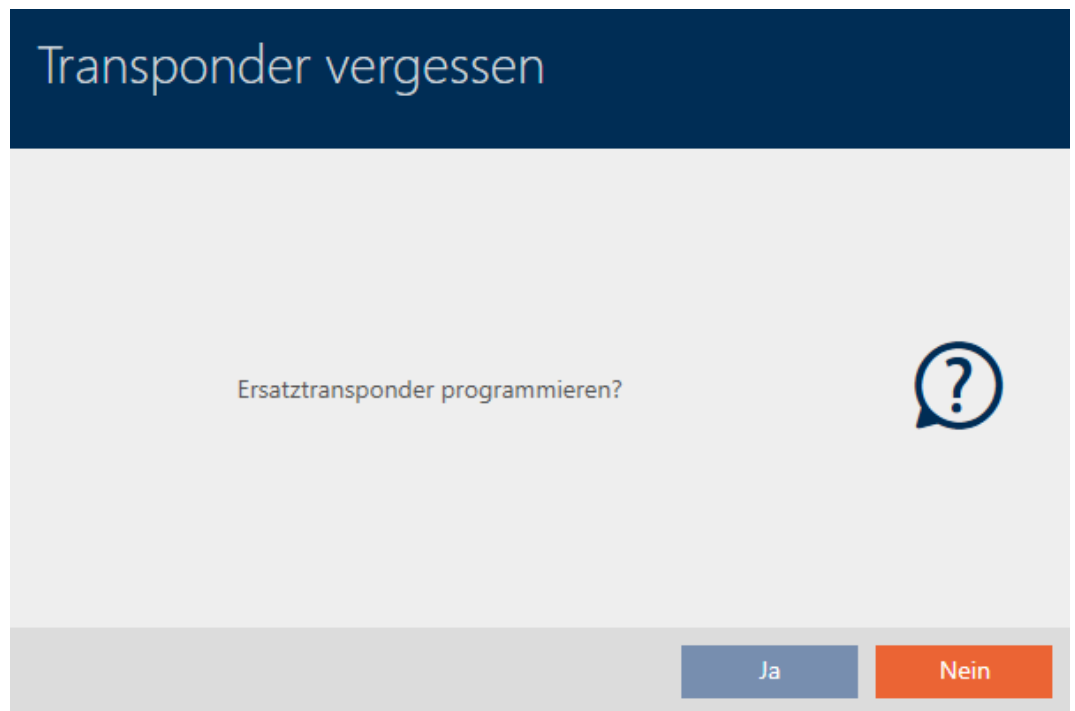
5

6

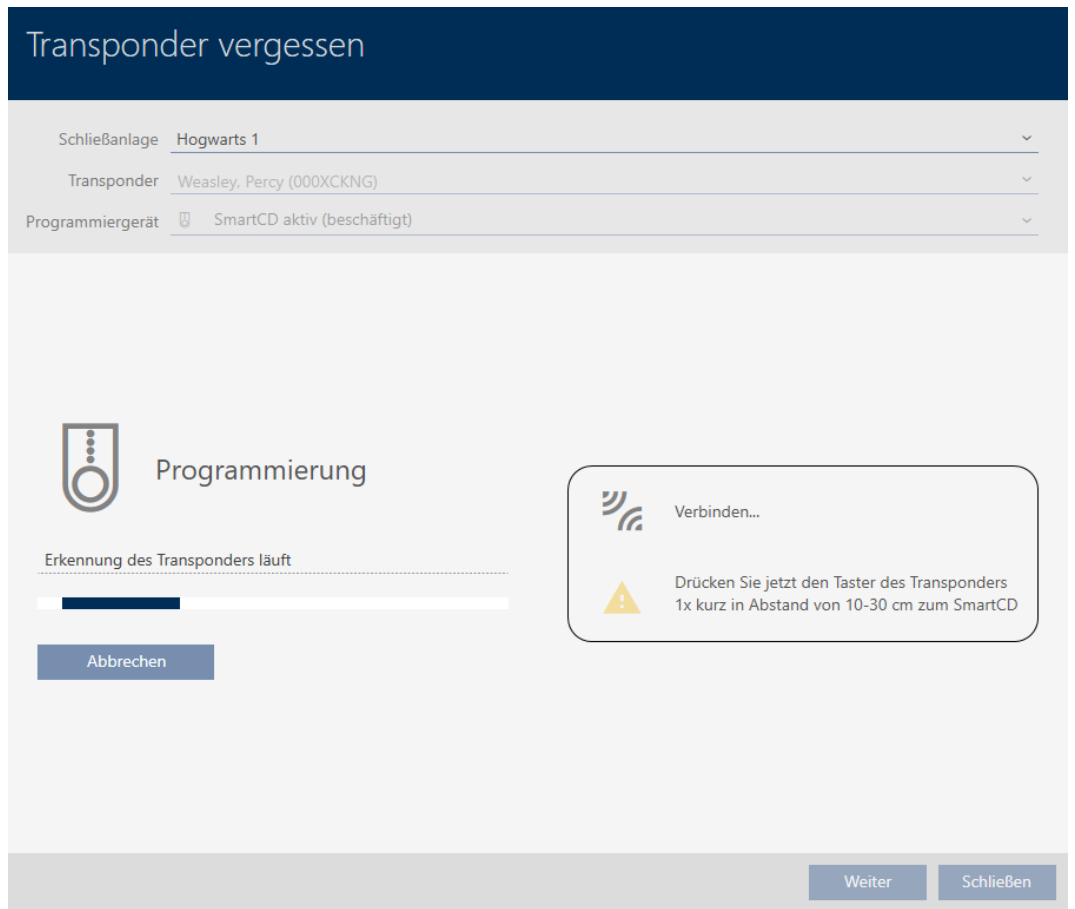
7

OK Abbrechen

- 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.

**TRANSPONDER VERGESSEN**  
 Die Aktion wurde erfolgreich durchgeführt

Duplicated identification media are also displayed in the matrix:

Sync	Typ	Person
	👤	Weasley, Ron
	👤	Weasley, Percy
	👤	Weasley, Percy
	👤	Weasley, Fred
	👤	Lovegood, Luna
↻	👤	Granger, Hermine

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)* [▶ 119]):

▼ VERFALLSDATUM

ohne Verfallsdatum

Aktiv bis (Uhrzeit): 29.05.2021 23:00 ▼

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* [▶ 161]).

#### 14.11 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* [▶ 161]). 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* [▶ 512] 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* [▶ 166]). If only one PIN is known and is therefore unsafe, you can change this PIN (see *Changing a PIN (PinCode AX)* [▶ 225]).

#### 14.11.1 Blocking and replacing lost/stolen card/transponder permanently

- ✓ 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* [▶ 44]).
  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.

**Transponder verloren**

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Percy (000XCKNG)	▼
Programmiergerät	 SmartCD aktiv	▼

**TRANSPONDER VERLOREN**

**Ereignis:**  
Der Aufenthaltsort des gewählten Transponders ist nicht bekannt. Die Sicherheit der Schließanlage ist gefährdet.

**Hinweis:**  
Der Transponder muss deaktiviert werden. Dadurch entsteht Programmierbedarf an allen berechtigten Schließungen. Dieser Vorgang kann nicht revidiert werden. Halten Sie auf Wunsch einen Ersatztransponder bereit.

**Aktion:**  
Der Transponder wird deaktiviert. Eine Begründung ist erforderlich. Ein Ersatztransponder kann erstellt werden.

- Bitte beachten Sie, dass der Transponder deaktiviert wird und dadurch großer Programmieraufwand entstehen kann
- Im Ablauf des Assistenten wird angeboten, einen Ersatztransponder zu erstellen

Weiter
Schließen

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

The screenshot shows a dialog box titled "Transponder deaktivieren" with the subtitle "Bitte geben Sie die gewünschten Informationen ein". The main text asks: "Wollen Sie tatsächlich den Transponder sperren? Falls 'ja', geben Sie bitte den Grund an, z.B. Transponder verloren." Below this is a drop-down menu currently showing "Verloren". Underneath the menu is a section labeled "Zusatzinformation" with a large empty text area. At the bottom right, there are two buttons: "OK" (orange) and "Abbrechen" (blue).

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

A close-up of the drop-down menu from the previous screenshot. The menu is open, showing the current selection "Verloren" at the top, which is highlighted with an orange background. Below it are two other options: "Nicht zurückgegeben" and "Andere Gründe".

6. Click on the **OK** button.

- ↳ Confirmation dialogue for replacement identification medium will open.



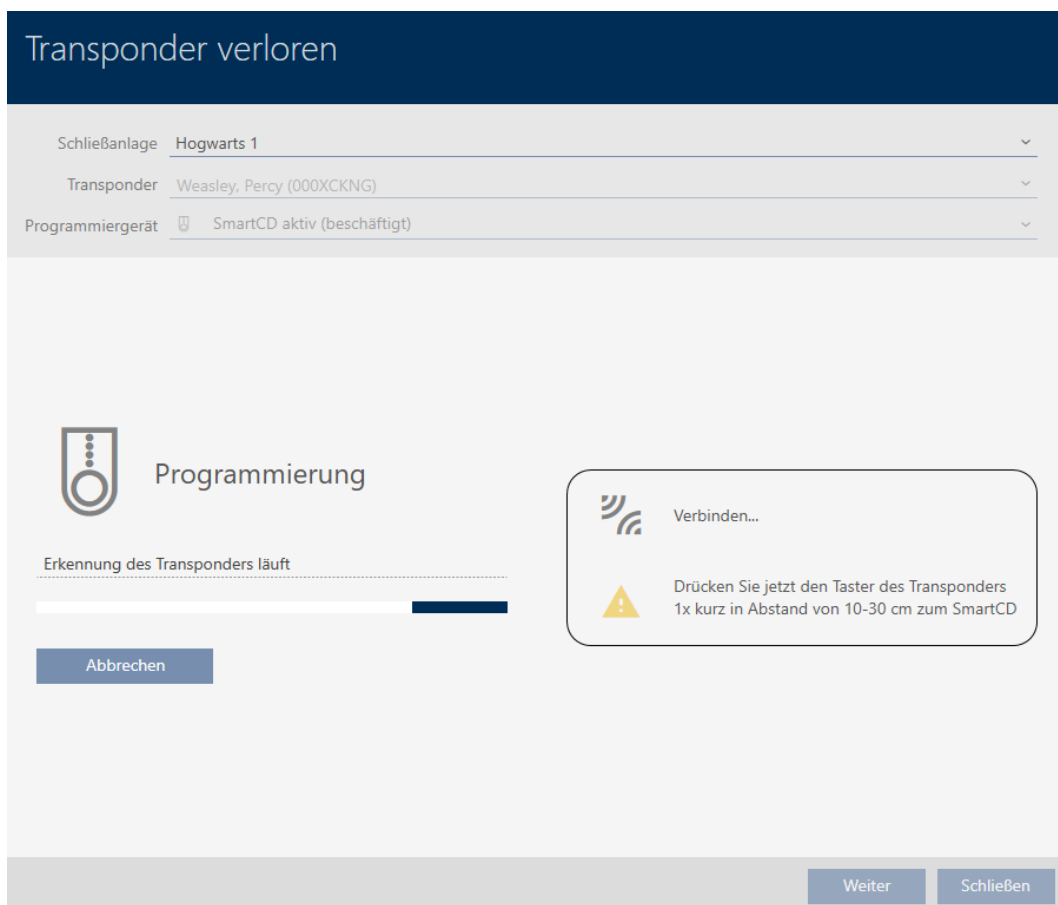
7. Click on the **Yes** button.
  - ↳ Confirmation dialogue for replacement identification medium closes.
  - ↳ Replacement identification medium can already be seen in the matrix in the background.

Sync	Typ	Person
	☺	Weasley, Ron
↻	☺	Weasley, Percy
↻	☺	Weasley, Percy
	☺	Weasley, Fred
	☺	Lovegood, Luna
	☺	Granger, Hermine

- ↳ 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.

**TRANSPONDER VERLOREN**  
 Die Aktion wurde erfolgreich durchgeführt

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

Person	Typ	Sync
Weasley, Ron		
Weasley, Percy		
Weasley, Percy		
Weasley, Fred		
Lovegood, Luna		
Granger, Hermine		


**IMPORTANT**

**Changes to the locking system only take effect after synchronisation**

If you edit the locking system with the AXM Plus, 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* [▶ 41]).
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* [▶ 398]).

**IMPORTANT**


**Block ID automatically written on replacement transponder**

If you create a replacement transponder for a lost/stolen transponder, your AXM Plus 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.

**14.11.2 Blocking a lost/stolen PIN code keypad permanently**

- ✓ 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* [▶ 44]).
  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.

### PinCode verloren - Assistent

Schließanlage	Hogwarts	▼
PinCode	Ⓢ Gryffindor electronic portrait (0873CDF)	▼
Programmiergerät	🔌 SmartStick AX	▼

**PINCODE VERLOREN**

**Ereignis:**  
Der Aufenthaltsort der gewählten PinCode ist nicht bekannt. Die Sicherheit der Schließanlage ist gefährdet.

**Hinweis:**  
Die PinCode muss deaktiviert werden. Dadurch entsteht Programmierbedarf an allen berechtigten Schließungen. Dieser Vorgang kann nicht revidiert werden. Halten Sie auf Wunsch eine Ersatz-PinCode bereit.

**Aktion:**  
Die PinCode wird deaktiviert. Eine Begründung ist erforderlich. Eine Ersatz-PinCode kann erstellt werden.

- Bitte beachten Sie, dass die PinCode deaktiviert wird und dadurch großer Programmieraufwand entstehen kann
- Im Ablauf des Assistenten wird angeboten, eine Ersatz-PinCode zu erstellen

Weiter
Schließen

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

### PinCode deaktivieren

Bitte geben Sie die gewünschten Informationen ein

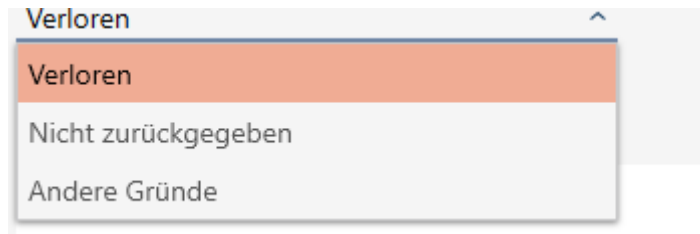
Wollen Sie tatsächlich die PinCode sperren?  
Falls 'ja', geben Sie bitte den Grund an, z.B. ob die PinCode verlorengegangen ist.

Verloren ▼

Zusatzinformation

OK
Abbrechen

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 Plus offers to create a replacement PIN code keypad.

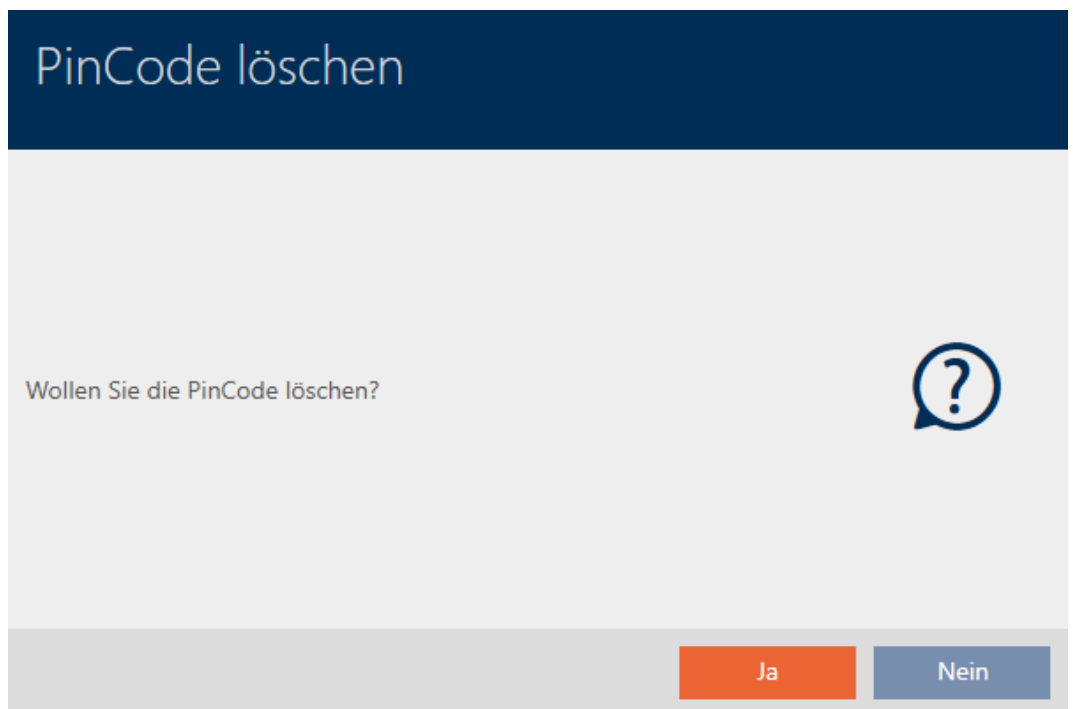


8. If you need a replacement, click the **Yes** button; otherwise, click the **No** button.  
(Example: Yes)
  - ↳ AXM Plus creates a replacement PIN code keypad in the background.
  - ↳ AXM Plus offers to synchronise the replacement PIN code keypad immediately.





9. Click on the **Yes** button.
- ↳ Synchronisation of the replacement PIN code keypad launches.
  - ↳ AXM Plus 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.

**PINCODE VERLOREN**  
 Die Aktion wurde erfolgreich durchgeführt

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 Plus will display an error message:



You can repair the PIN code keypad as an alternative; see *Repairing a PIN code keypad (resynchronising)* [▶ 127].

## 14.12 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 Plus 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.

### PIN code keypad PINs cannot be withdrawn


PIN code keypad PINs are not physical and therefore cannot be withdrawn. You have the option to change the PIN instead (see *Changing a PIN (PinCode AX)* [▶ 225]).

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

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

- ✓ Suitable programming device connected.
- 1. Click the  **Transponder returned** button in the "Wizards" section.
  - ↳ The wizard for ID media return will open.

## Transponder zurückgegeben

Schließanlage	Hogwarts 1	▼
Transponder	Weasley, Percy (000XCKNG)	▼
Programmiergerät	 SmartCD aktiv	▼

**TRANSPONDER ZURÜCKGEBEN**

**Ereignis:**  
Der gewählte Transponder wurde an die Schließanlagenverwaltung übergeben und soll aus dem Verkehr gezogen werden.

**Hinweis:**  
Der Transponder wird nicht aus der Schließanlage gelöscht, sondern erhält einen entsprechenden Eintrag in seiner Historie.

**Aktion:**  
Die Rückgabe wird in der Historie vermerkt. Der Transponder kann im nächsten Schritt zurückgesetzt werden.

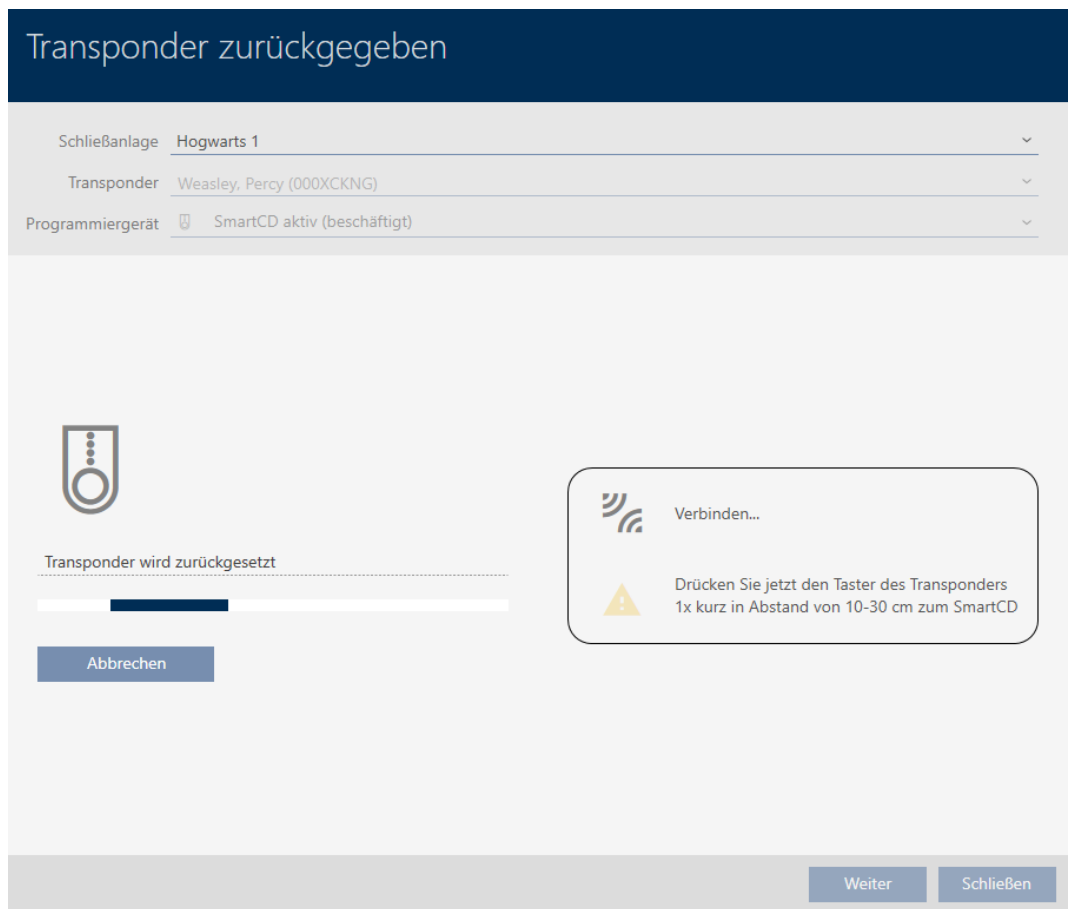
- Im Ablauf des Assistenten wird angeboten, den Transponder zurückzusetzen und zu löschen

Weiter Schließen

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.

**TRANSPONDER ZURÜCKGEGEBEN**  
 Die Aktion wurde erfolgreich durchgeführt

The successful return is noted in the identification medium's action list (also see *Planning and logging card/transponder return [▶ 183]*).


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	

### 14.13 Planning and tracking identification medium management tasks

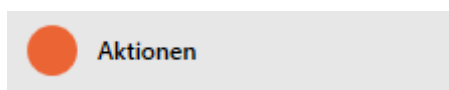
The central point for managing your identification medium is the "Transponder - Actions" tab . The following entries are displayed here collectively:

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

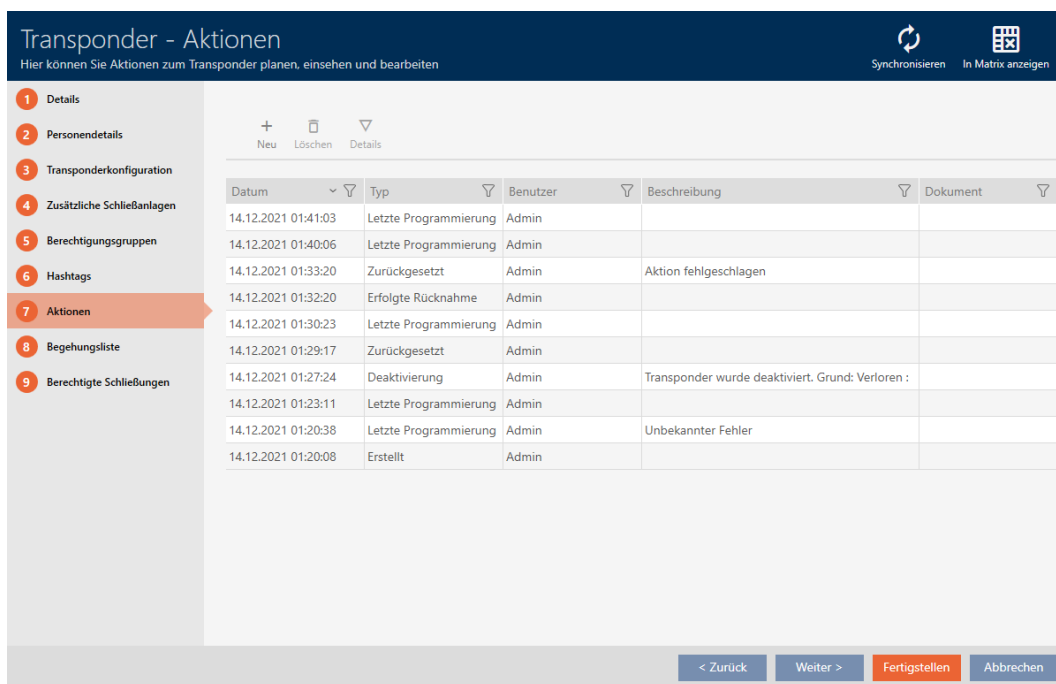
Not all entries are available for all types of identification medium. Since a PIN cannot be withdrawn like a transponder, for example, the entries "Planned return" and "Handed back" are not available for PIN code keypads.

- ✓ Identification media list or matrix open.
  - ✓ Identification medium available.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering [▶ 44]*).
  2. Click on the identification medium you wish to manage.
    - ↳ The identification medium window will open.

3. Click on the  **Aktionen** tab.



↳ Window switches to the "Actions" tab.



4. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

### 14.13.1 Noting the issue date

#### 14.13.1.1 Note card/transponder issue date

AXM Plus 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.

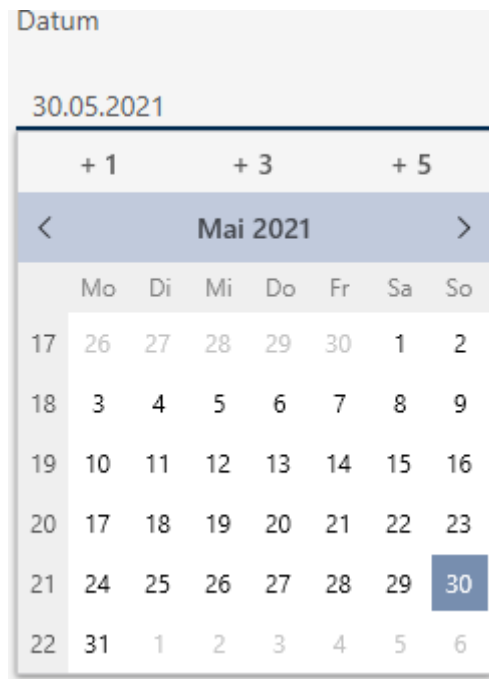
↳ The window for a new action will open.


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

- 
- Aktion
  - Ausgegeben
  - Ausgegeben
  - Erfolgte Rücknahme
  - Geplante Rückgabe
  - Letzter Batteriewechsel
  - Planmäßiger Batteriewechsel



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.
  - ↳ Explorer window closes.

9. Click on the **OK** button.
  - ↳ The window for the new action closes.
  - ↳ Action is now created and listed.

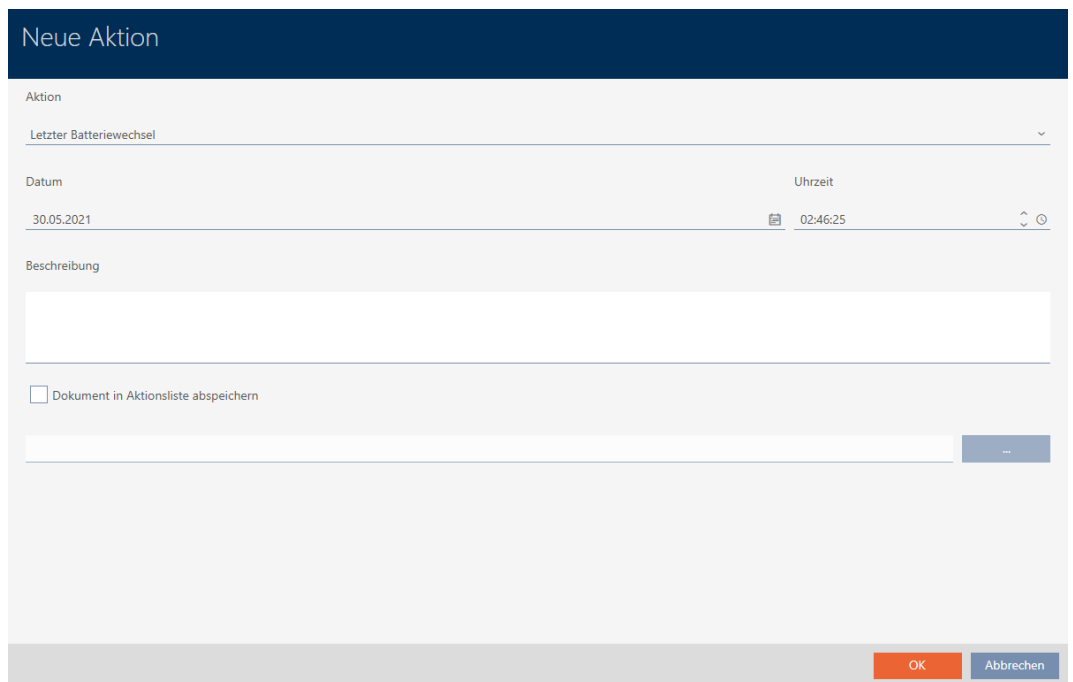
Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 03:49:48	Ausgegeben	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14	Letzte Programmierung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

You can generate a suitable report with signature fields (see *Displaying the report for identification media issue* [▶ 504]) to prepare the transfer of the identification medium.

### 14.13.2 Planning and logging battery replacement

#### 14.13.2.1 Planning and logging card/transponder battery changes

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



Neue Aktion

Aktion  
Letzter Batteriewechsel

Datum  
30.05.2021

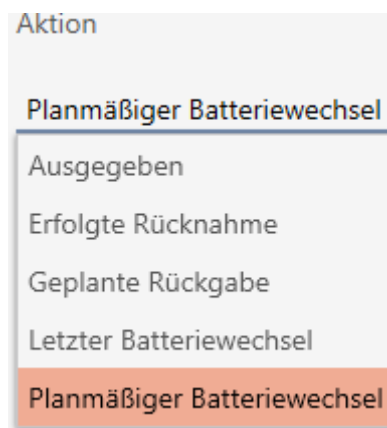
Uhrzeit  
02:46:25

Beschreibung

Dokument in Aktionsliste abspeichern

OK Abbrechen

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



Aktion

Planmäßiger Batteriewechsel

Ausgegeben

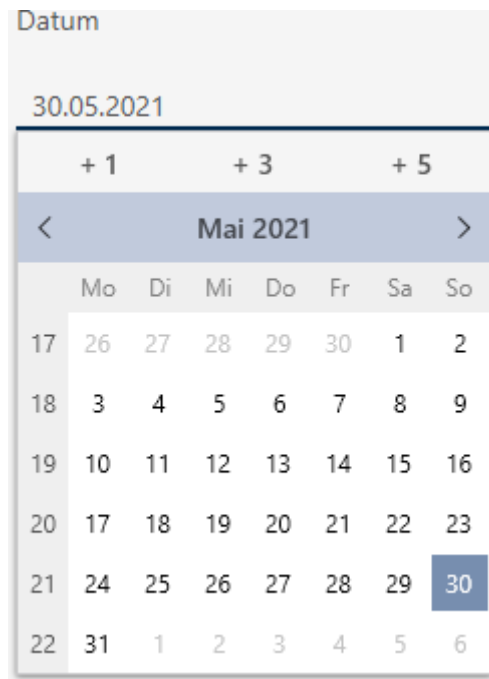
Erfolgte Rücknahme


Geplante Rückgabe

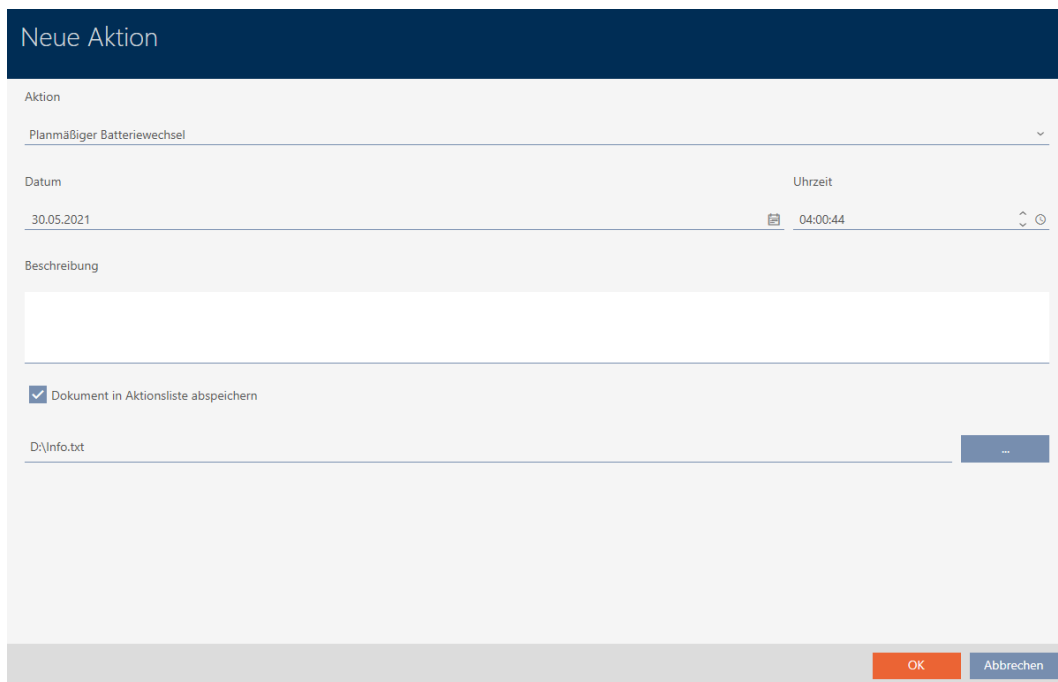
Letzter Batteriewechsel

Planmäßiger Batteriewechsel

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.
  - ↳ Explorer window closes.



9. 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		

### 14.13.2.2 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.
  - ↳ Explorer window closes.

Neue Aktion

Aktion

Planmäßiger Batteriewechsel ▼

---

Datum Uhrzeit

30.04.2024 📅 20:00:00 ⌵

Beschreibung

Dokument in Aktionsliste abspeichern

D:\info.txt ...

OK
Abbrechen

9. 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 Batteriewe	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	

### 14.13.3 Planning and logging return

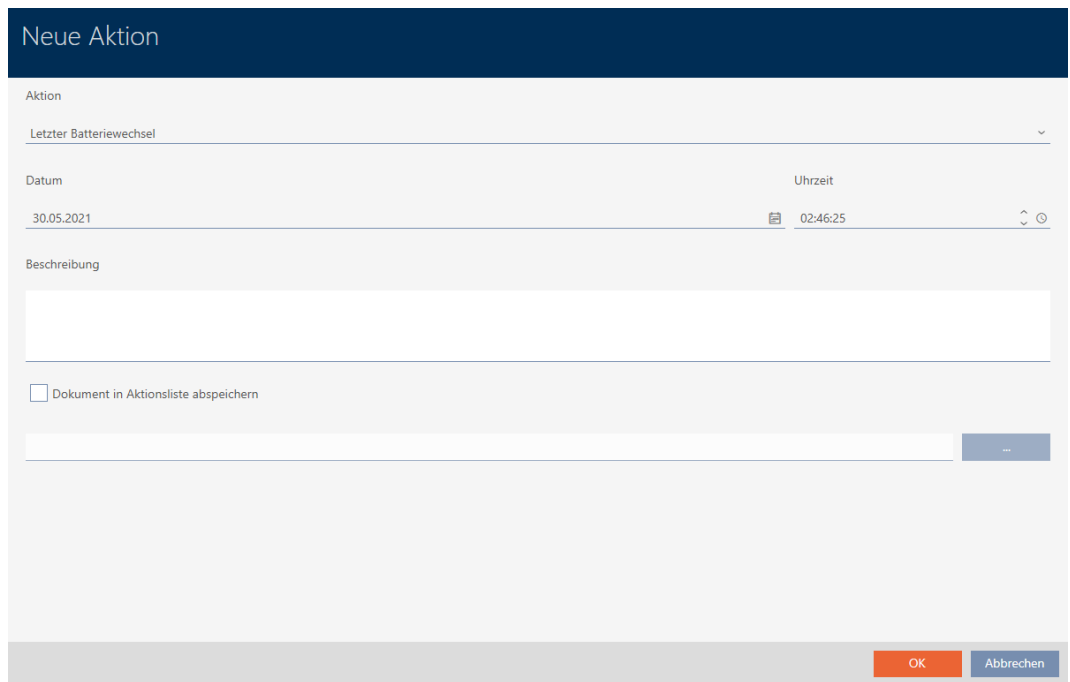
#### 14.13.3.1 Planning and logging card/transponder return

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

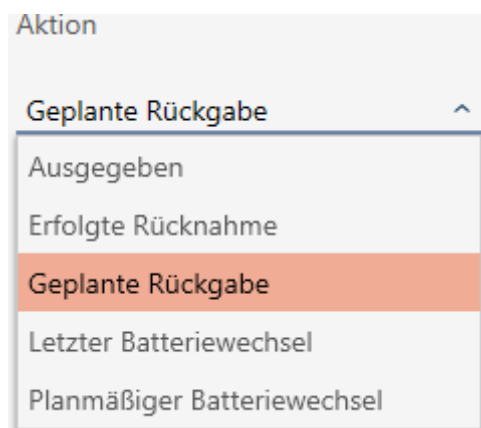
You can also enter when an identification medium was actually returned in the action list. However, you need to reset the identification medium manually in this case. The return wizard is ideal for returns instead of a

manual reset: *Flagging and resetting returned card/transponder (back to inventory)* [▶ 171]. 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.

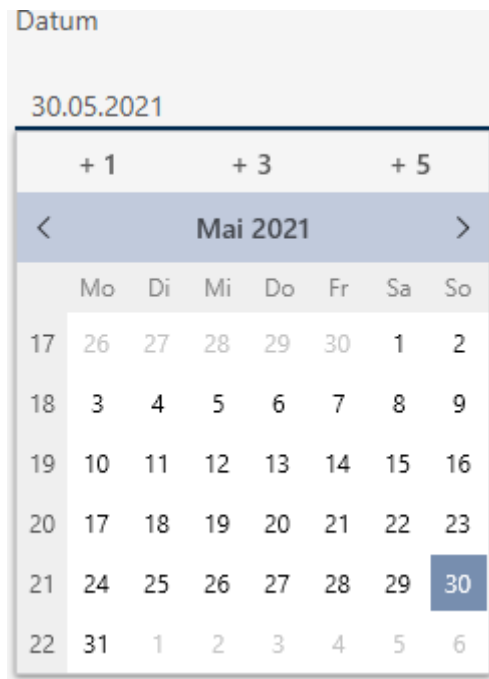



2. Select "Planned return" or "Handed back" from the ▼ **Action** drop-down menu.

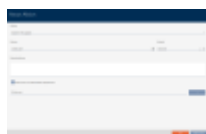





3. Enter a date in the *Date* field or click on the  icon to expand a calendar screen.



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.
  - ↳ Explorer window closes.




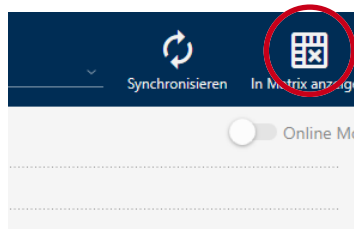
9. Click on the  button.
  - ↳ The window for the new action closes.
- ↳ Action is now created and listed.

Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 03:05:41	Gep plante 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		

### 14.14 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.

### 14.15 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 Plus.

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

#### 14.15.1 Exporting AX2Go keys/cards/transponders as a list

✓ Identification medium available.

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



- Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.

**SCHLISSANLAGENSTEUERUNG**

- Matrixansicht
- Schließungen
- Transponder**
- PinCodes
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung

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

- Select the locking system whose identification media you would like to export on the right (alternatively: "All").



Matrixansicht x Transponder x

Neu Löschen In Matrix anzeigen Duplizieren Ausgabe DSGVO-Daten Export Anzeigefilter löschen Importieren

Nach	Vorn:	S/N	Typ	Sync	Status	Zeitg	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L	🔑				
Snape	Severus	0301A4D	🔒			Zeitgrupp	
Weasley	Ron	00XTN6K	🔒				
Wood	Oliver		📄	↻			

- Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
- Click on the **Export** button .
  - ↳ The Explorer window will open.
- 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	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L	Mobiltelefon	Programmiert			
Snape	Severus	0301A4D	Transponder	Programmiert		Zeitgruppe 2	
Wood	Oliver		Karte	Erstprogrammierung			

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

#### 14.15.2 Exporting PINs and PIN code keypads as a list

✓ PIN code keypad created (see *Creating PIN code keypads* [▶ 96]).

1. Click the orange AXM button .

↳ AXM bar opens.



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

#### SCHLISSANLAGENSTEUERUNG

- Matrixansicht
- Schließungen
- Transponder
- PinCodes**
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung

- ↳ The list with all PIN code keypads in the locking system will open.
- 3. Select the locking system whose identification media you would like to export on the right (alternatively: "All").

The screenshot shows a dropdown menu with 'Hogwarts' selected. Below it is a table with columns: Name, Schließung, S/N, Typ, Status, and Sync. The table contains two entries: 'Gryffindor electronic portra' and 'Quidditch field entrance'.

Name	Schließung	S/N	Typ	Status	Sync
Gryffindor electronic portra	Gryffindor tower	088NKAK	AX PinCode		
Quidditch field entrance	Quidditch field		PinCode G1		

- 4. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
- 5. 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				

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

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


### 14.16.1 Viewing a card's/transponder's serial number and TID

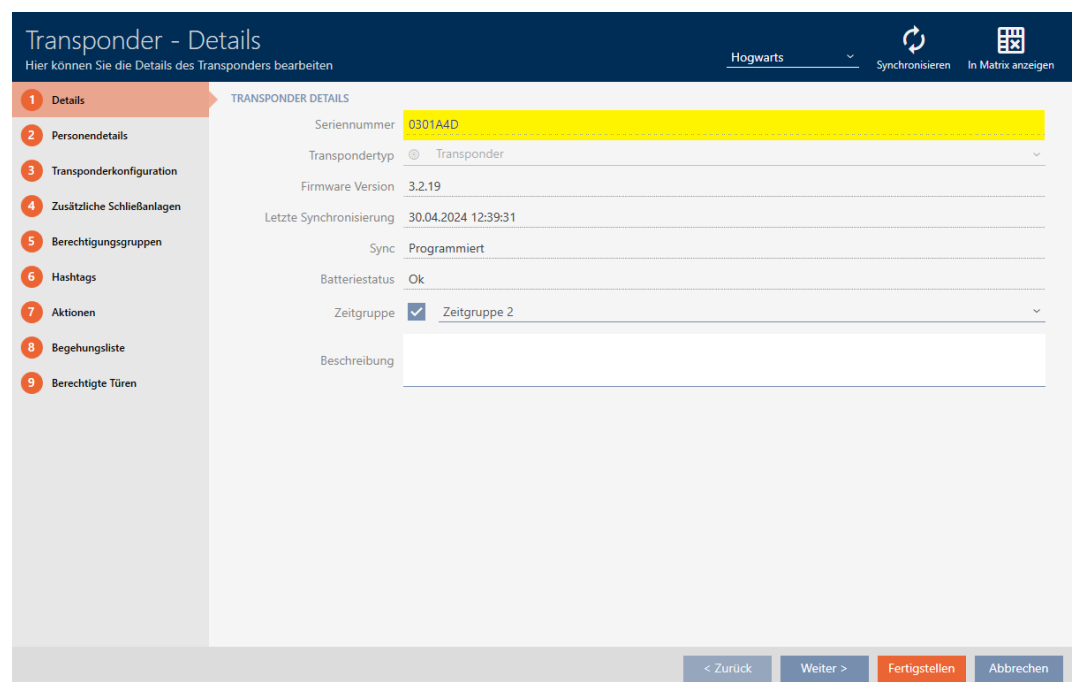
Your cards and transponders have two numbers that are important:


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

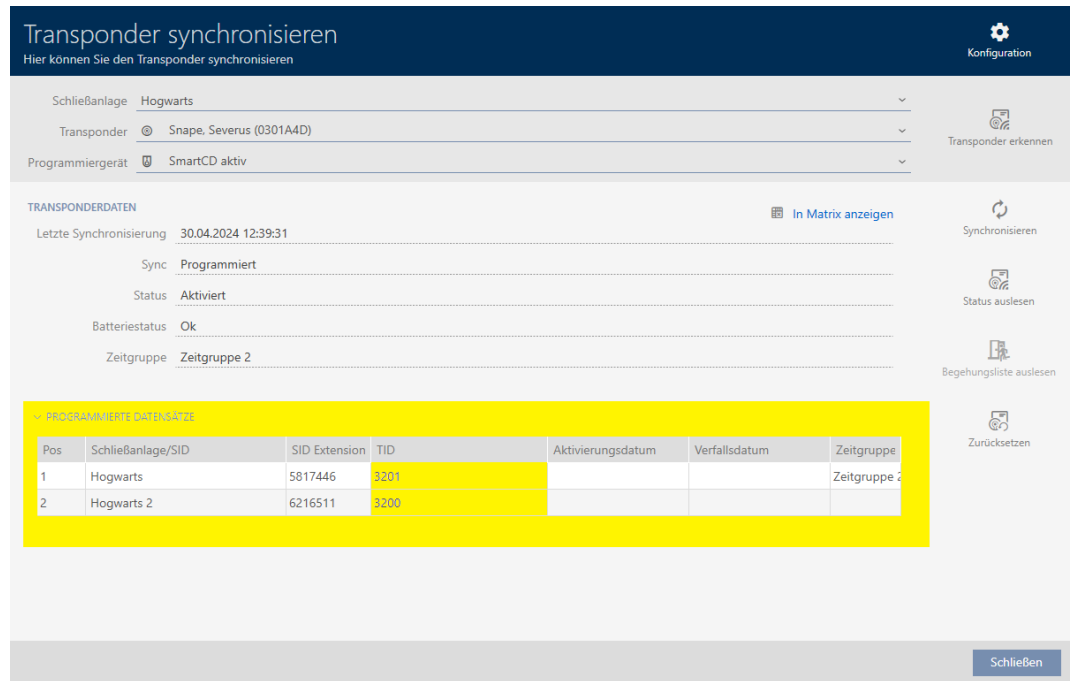
If you need the TID for support purposes, for example, you can view the TID for synchronised identification media in the synchronisation window:

- ✓ Identification media list or matrix open.
  - ✓ Identification medium synchronised.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
  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.



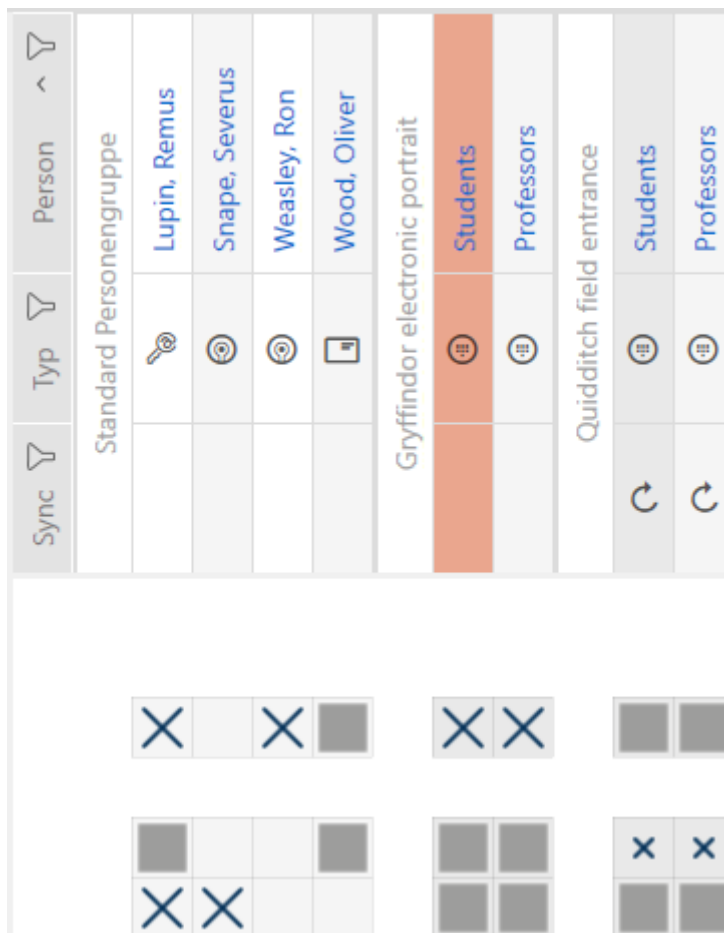
↳ TIDs are displayed in table. If you use the identification medium in a number of locking systems, the TID used for each locking system is displayed.

### 14.16.2 Viewing a PIN code keypad's serial number

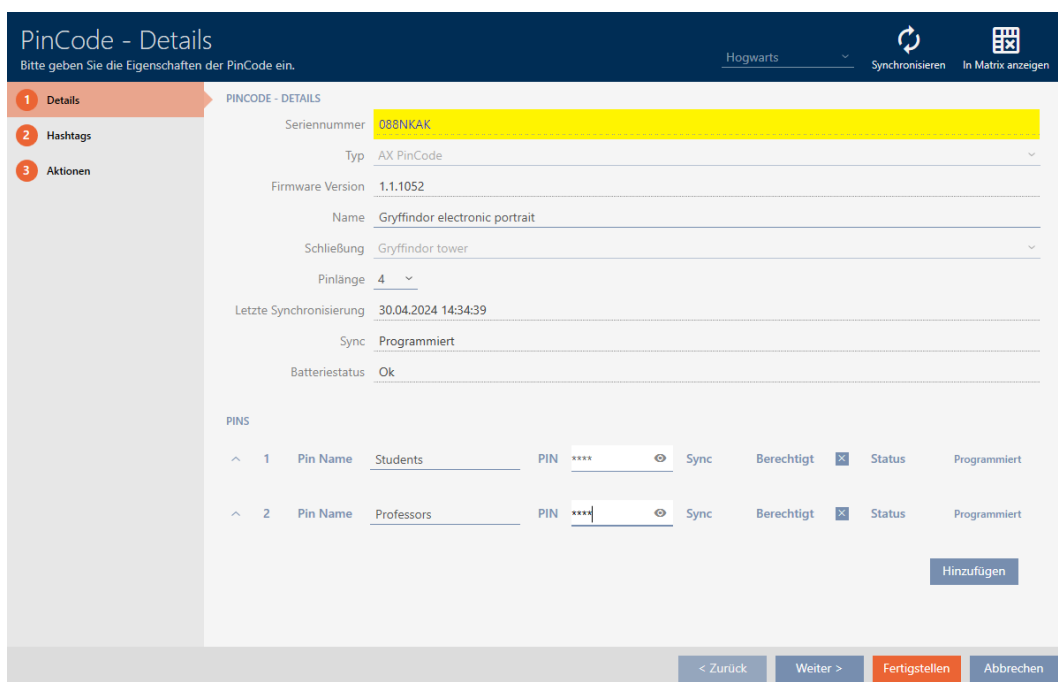
Your PIN code keypads do not have TIDs which are directly visible. You will find the serial number similar to that for cards and transponders in the details:

- ✓ 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* [▶ 44]).

- 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.





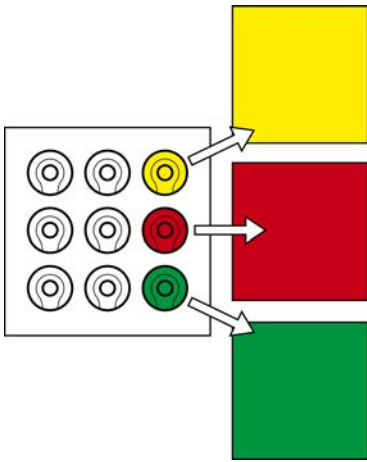
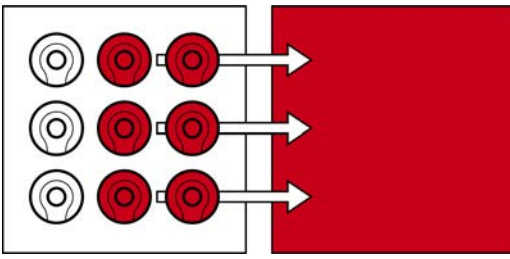
### 14.17 Assigning persons to person groups

Identification media are linked to people. As a rule, you will also create a person who owns a identification medium when you create it.

PIN code keypads are an exception here. They are designed to be used by a number of people and therefore cannot be assigned to a group of people. However, you can assign the PINs to a time group instead (see *Adding PINs from a PIN code keypad to the time group* [▶ 344]).

You need to specify a person group as soon as you add a person. Ideally, you should follow best practice (see *Best practice: setting up the locking system* [▶ 27]) and plan everything out ready before creating your persons (see *Organisational structure* [▶ 50]). This means that you only need to open windows once.

Obviously, you can also move your persons to another person group at a later point in time.

Moving Individual persons	Moving multiple locking devices
<p><i>Assigning individual persons/identification media to a person group (in transponder window) [▶ 194]</i></p> <p>Suitable for moving few people into many different person groups:</p> 	<p><i>Assign a number of persons/identification media to person group (in the person group window) [▶ 196]</i></p> <p>Suitable for moving a number of persons into a few different person groups:</p> 



**NOTE**

**Maximum one area per locking device**

A locking device can only belong to one single area. There are no overlapping areas in the AXM Plus . If you assign a different area to a locking device, this locking device may be automatically removed from its existing area.

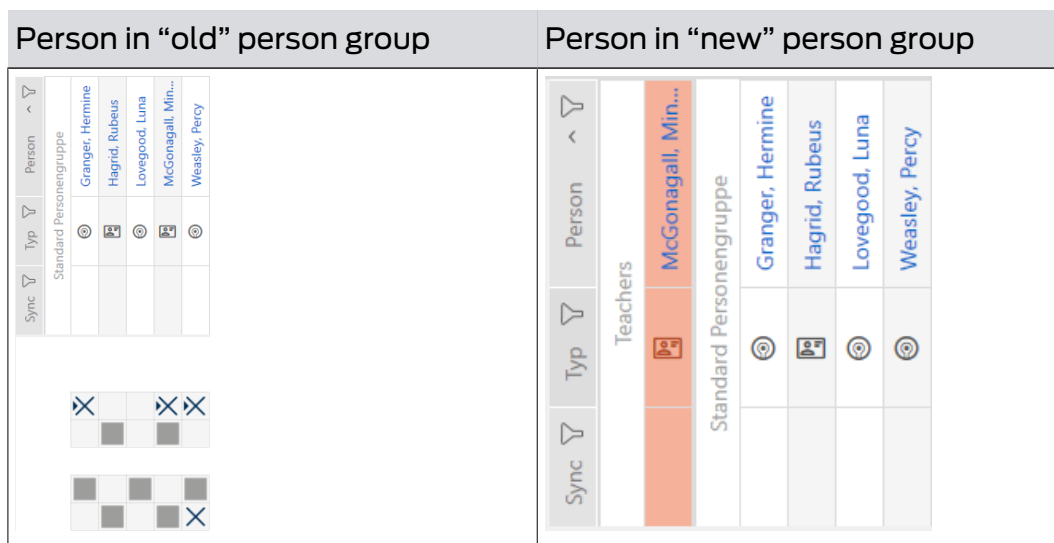
- You can use the Area - Details column in the "Area - Details" window to check whether a locking device has already been assigned to an area.

**Person groups have no influence on authorisations**

Authorisations are not directly linked to person groups. If a person is moved to a different person group, the change does not affect authorisations initially. However, person groups are a useful tool for changing authorisations more quickly.

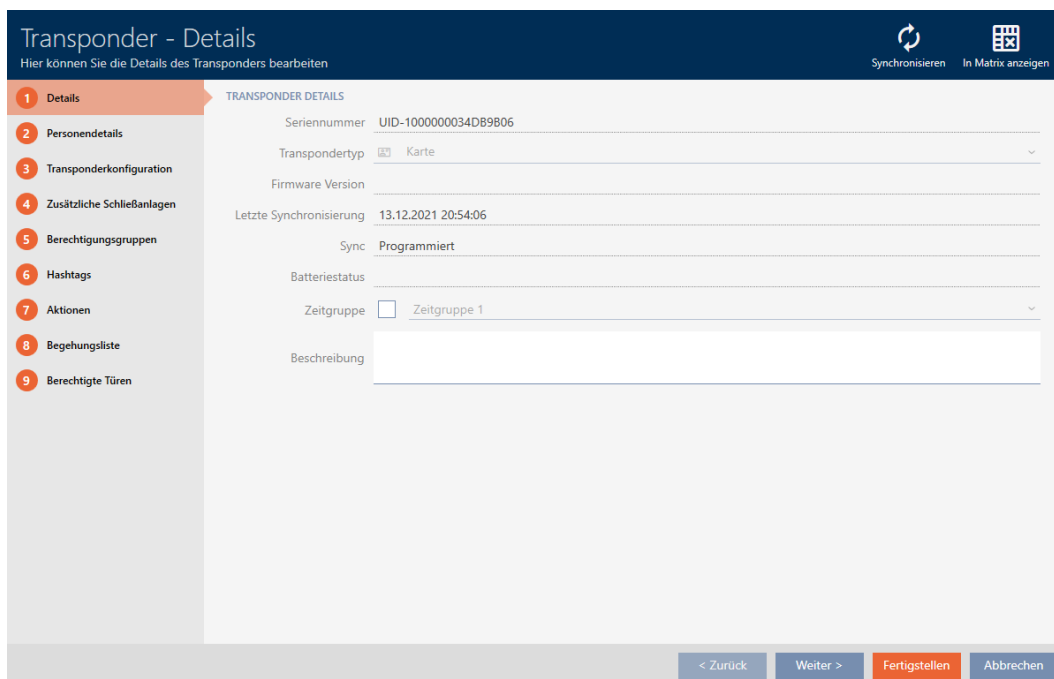
- Use person groups to add people to authorisation groups more quickly (see *Adding areas and person groups to authorisation groups* [▶ 331]).

**14.17.1 Assigning individual persons/identification media to a person group (in transponder window)**

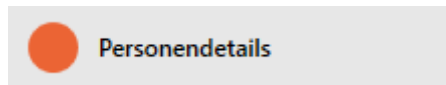


- ✓ At least one person group created (see *Creating a person group* [▶ 51]).

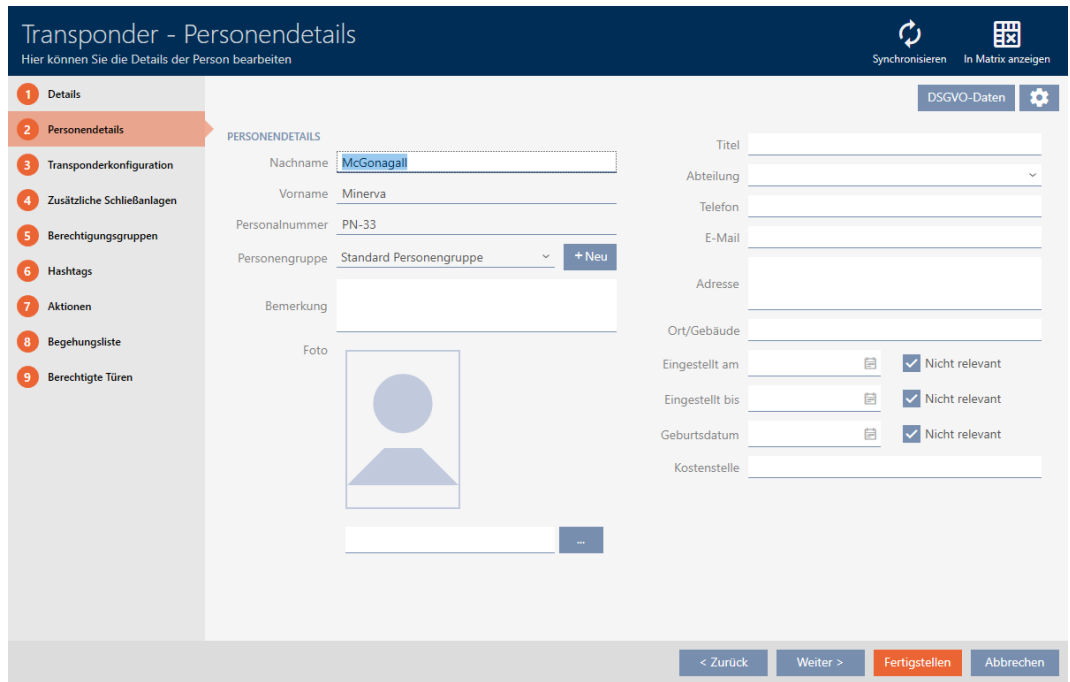
1. Click on the identification medium of the person you wish to assign to a new person group.
  - ↳ The identification medium window will open.



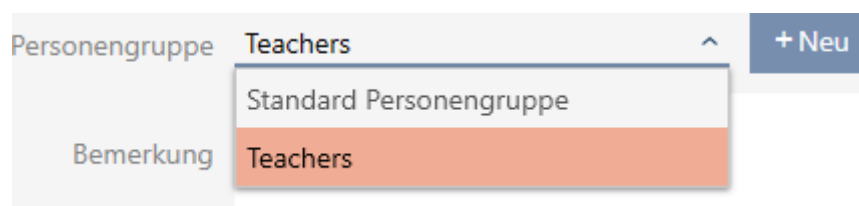
2. Click on the **Person details** tab.



↳ The "Person details" tab is shown.








3. Select the person group to which the person should belong in the future from the **Person group** drop-down menu.



















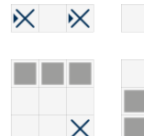















4. Click on the **Finish** button.

↳ The identification medium window closes.


↳ Person belongs to a new person group.

Sync	Typ	Person
	Teachers	
		McGonagall, Min...
	Standard Personengruppe	
		Granger, Hermine
		Hagrid, Rubeus
		Lovegood, Luna
		Weasley, Percy

14.17.2 Assign a number of persons/identification media to person group (in the person group window)

Persons in "old" person group	Persons in "new" person group																																													
<table border="1"> <thead> <tr> <th>Sync</th> <th>Typ</th> <th>Person</th> </tr> </thead> <tbody> <tr> <td></td> <td>Standard Personengruppe</td> <td></td> </tr> <tr> <td></td> <td></td> <td>Granger, Hermine</td> </tr> <tr> <td></td> <td></td> <td>Hagrid, Rubeus</td> </tr> <tr> <td></td> <td></td> <td>Lovegood, Luna</td> </tr> <tr> <td></td> <td></td> <td>McGonagall, Min...</td> </tr> <tr> <td></td> <td></td> <td>Weasley, Percy</td> </tr> </tbody> </table> 	Sync	Typ	Person		Standard Personengruppe				Granger, Hermine			Hagrid, Rubeus			Lovegood, Luna			McGonagall, Min...			Weasley, Percy	<table border="1"> <thead> <tr> <th>Sync</th> <th>Typ</th> <th>Person</th> </tr> </thead> <tbody> <tr> <td></td> <td>Pupils</td> <td></td> </tr> <tr> <td></td> <td></td> <td>Granger, Hermine</td> </tr> <tr> <td></td> <td></td> <td>Lovegood, Luna</td> </tr> <tr> <td></td> <td></td> <td>Weasley, Percy</td> </tr> <tr> <td></td> <td>Standard Personengruppe</td> <td></td> </tr> <tr> <td></td> <td></td> <td>Hagrid, Rubeus</td> </tr> <tr> <td></td> <td></td> <td>McGonagall, Min...</td> </tr> </tbody> </table> 	Sync	Typ	Person		Pupils				Granger, Hermine			Lovegood, Luna			Weasley, Percy		Standard Personengruppe				Hagrid, Rubeus			McGonagall, Min...
Sync	Typ	Person																																												
	Standard Personengruppe																																													
		Granger, Hermine																																												
		Hagrid, Rubeus																																												
		Lovegood, Luna																																												
		McGonagall, Min...																																												
		Weasley, Percy																																												
Sync	Typ	Person																																												
	Pupils																																													
		Granger, Hermine																																												
		Lovegood, Luna																																												
		Weasley, Percy																																												
	Standard Personengruppe																																													
		Hagrid, Rubeus																																												
		McGonagall, Min...																																												

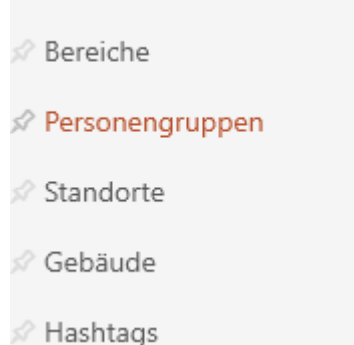
✓ At least one person group created (see *Creating a person group* [▶ 51]).

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

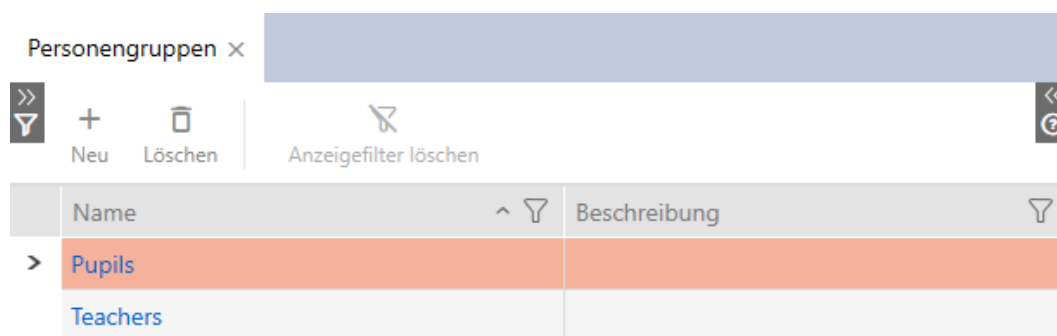


2. Select the **Person groups** entry in the | ORGANISATIONAL STRUCTURE | group.

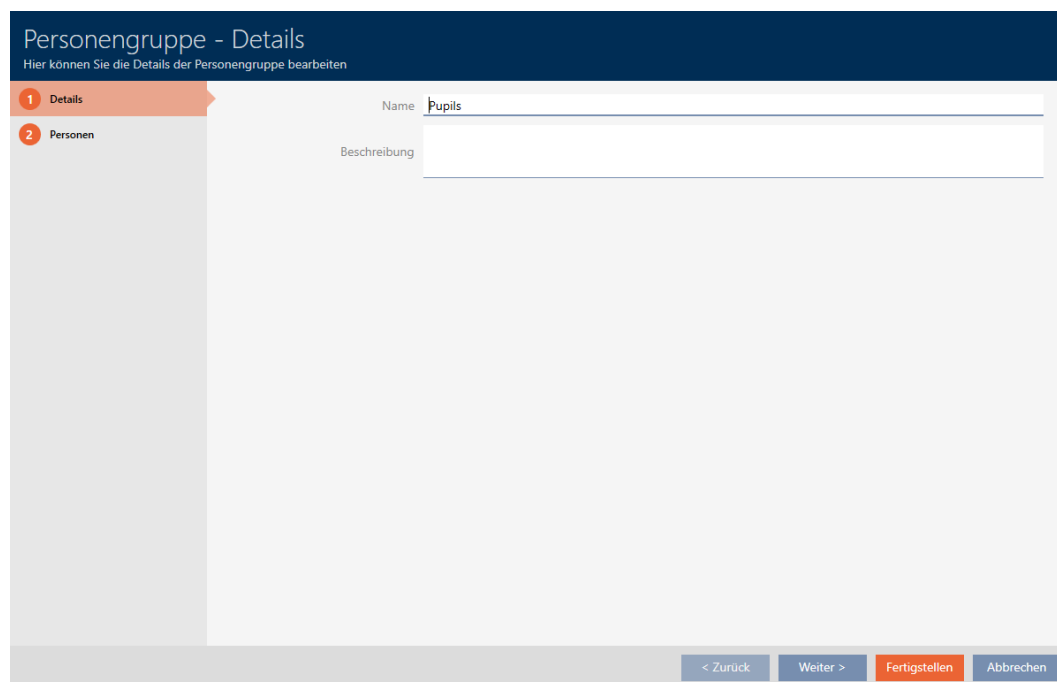
**ORGANISATIONSTRUKTUR**



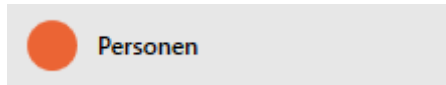
- ↳ The AXM bar will close.
- ↳ The [Person groups] tab will open.



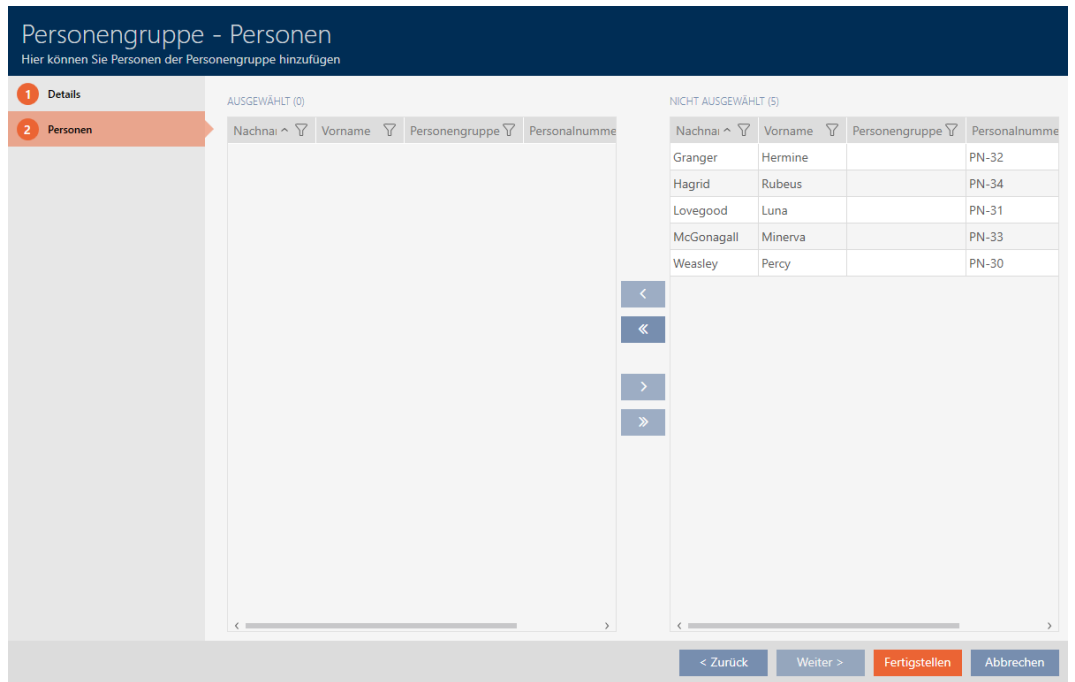
3. Click on the person group to which you want to assign the persons.
  - ↳ The "Person group" window will open.




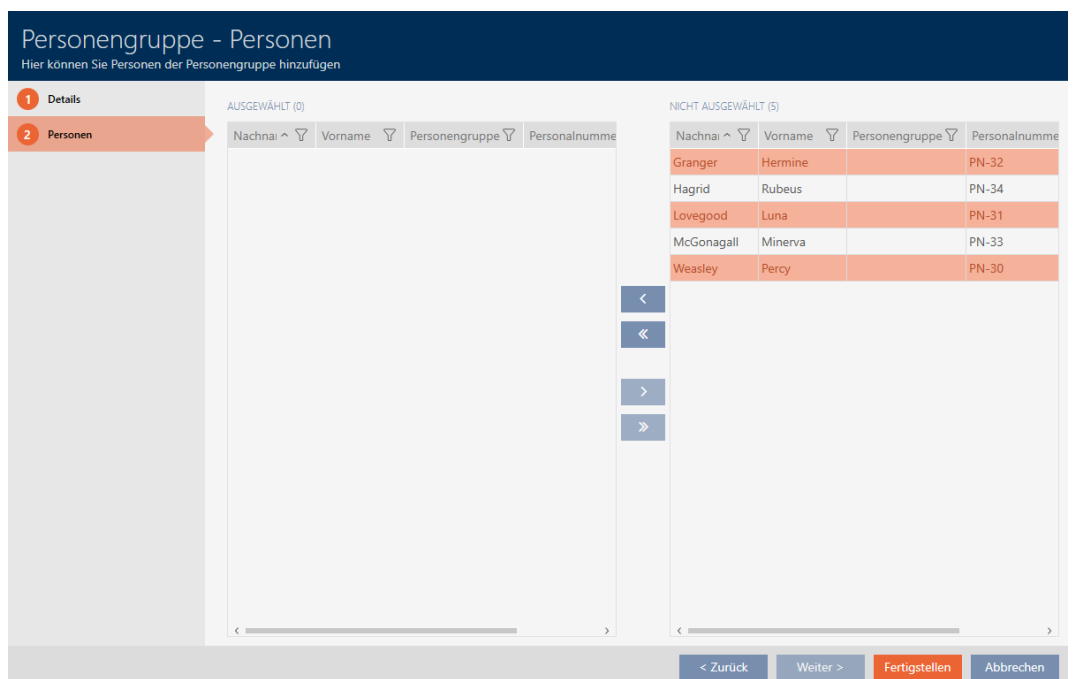
4. Click on the  **Persons** tab.





↳ Window switches to the  **Persons** tab.



- Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
- Highlight all persons you want to add to the area (Ctrl + mouse click for a single person or shift + mouse click for multiple persons).



- Use  to move the selected persons only or use  to move all displayed authorisation persons.








**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 persons in the left column are added to the person group.
- Click on the **Finish** button.
    - ↳ "Person group" window closes.
    - ↳ Persons are assigned to the new person group.
  - ↳ Matrix displays structure with new person groups.

Sync	Typ	Person
		Pupils
		Granger, Hermine
		Lovegood, Luna
		Weasley, Percy
		Standard Personengruppe
		Hagrid, Rubeus
		McGonagall, Min...

**14.18 Use identification media in multiple locking systems**

In certain cases, it a good idea to use multiple locking systems (see *Locking systems* [[▶ 521](#)]).

In such a case, it is practical if selected users can use the same identification medium in multiple locking systems.

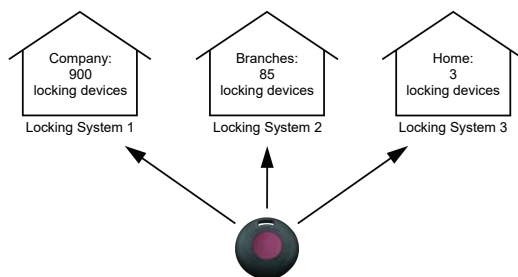
Usage in multiple locking systems differs from the common locking level:

Use in multiple locking systems	Common locking levels
<ul style="list-style-type: none"> <li>■ Multiple independent locking systems are stored on identification media</li> <li>■ Can come from different projects and databases</li> <li>■ Number of possible locking systems limited in the identification medium</li> <li>■ TID in each of these locking systems independent of TIDs in other locking systems</li> </ul>	<ul style="list-style-type: none"> <li>■ Common locking level is created and locking systems assigned</li> <li>■ Transponder is created in one of these locking systems. AXM Plus automatically creates the transponder in the other assigned locking systems as well</li> <li>■ Number of locking systems assigned in this way not limited</li> <li>■ Authorisations are configured in assigned locking systems</li> </ul> <p>See <i>Using a common locking level</i> [<a href="#">▶ 392</a>] to set up an common locking level.</p>

You will find further information on the common locking level here: *Common locking levels* [[▶ 523](#)].

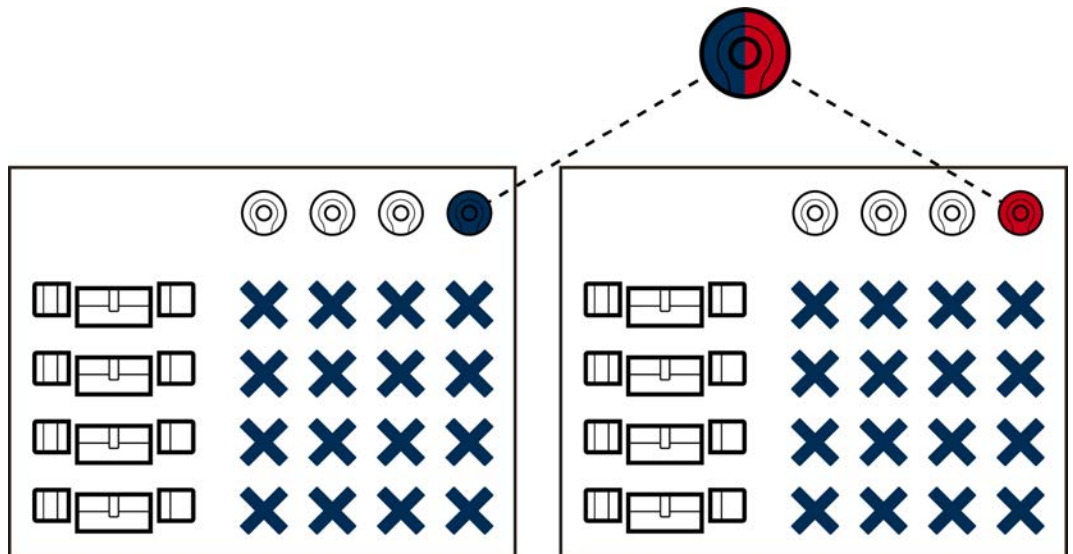
A PIN code keypad is permanently assigned to just one locking device and is not mobile. Use in multiple locking systems or in common locking levels is therefore not a good idea and not possible for PIN code keypads.

Example: a caretaker needs to be granted access to doors in different locking systems.



He does not need to carry multiple identification media around. Instead, you can add the caretaker's identification medium to each locking system, but then synchronise the same transponder.





- G2 transponders can store up to five locking systems (3 G2 locking systems and 2 G1 locking systems).
- Cards can also store multiple locking systems, depending on the available memory and card configuration (see *Card templates* [▶ 556]). You no longer make card configurations in AXM Plus across projects, but across different locking systems instead (see *Enable cards or transponders* [▶ 389]). This has two advantages:
  - Multiple locking systems on a single card are not a problem – treat an existing locking system as an external application and select free sectors or app IDs for the additional locking system (*MIFARE Classic (card already used)* [▶ 362] or *MIFARE DESFire (card already in use)* [▶ 376]).

Name: SectList Wert: 2,3,4,5 Beschreibung: Sector List	Name: SectList Wert: 6,7,8,9 Beschreibung: Sector List
--------------------------------------------------------------	--------------------------------------------------------------

- You can even use different card configurations in your locking systems provided you use the same card type (Classic/DESFire).

Kartentyp: Mifare Classic	Parameter:
Konfiguration: MC1200L	Name: SectList
Speicherbedarf: 192 Bytes	Wert: 2,3,4,5
Schließungs-IDs: 128 - 1327 im Kartenprofil	Beschreibung: Sector List
Begehungen im Protokoll: --	Name: TransportSectorTrailer
Virtuelles Netzwerk: --	Wert: *****
	Beschreibung: Transport Settings

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC3800L	Name: SectList
Speicherbedarf	528 Bytes	Wert: 6,7,8,9,10,11,12,13,14,15,17
Schließungs-IDs	128 - 3927 im Kartenprofil	<input type="button" value="Bearbeiten"/>
Begehungen im Protokoll	--	Beschreibung: Sector List
Virtuelles Netzwerk	--	Name: TransportSectorTrailer
		Wert: *****
		<input type="button" value="Bearbeiten"/>
		Beschreibung: Transport Settings

Transponders are easier to operate than cards in multiple locking systems since you do not need to take sectors or app IDs into account in this case.

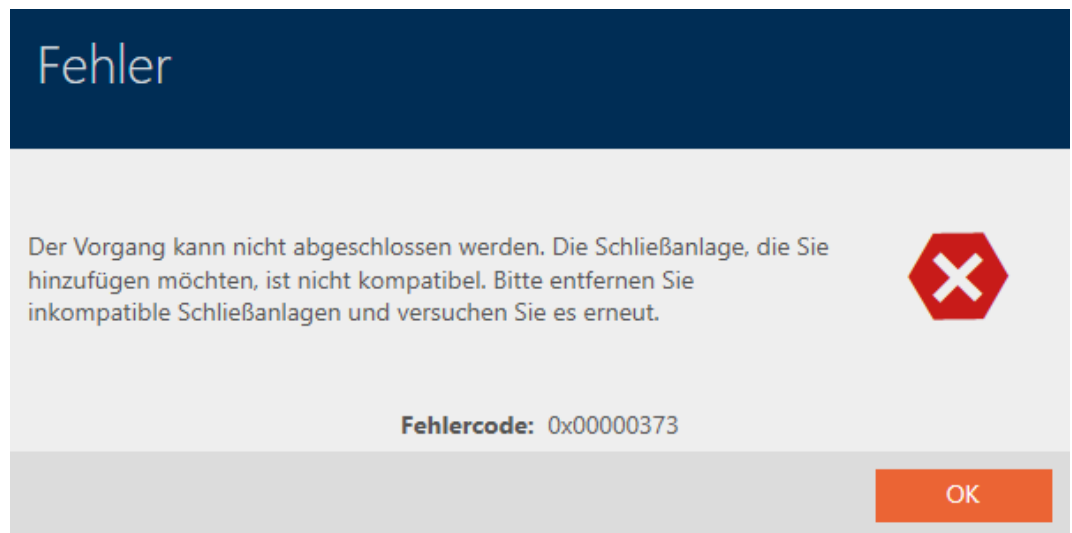
There are two ways to reuse an identification medium:

- *Reuse identification medium in the same project [▶ 202]*
- *Reusing identification medium in other projects/databases [▶ 208]*


### 14.18.1 Reuse identification medium in the same project

With AXM Plus, you can simply use the same identification medium for several locking systems.

If you are working with cards, AXM Plus will even check whether the set card configurations are compatible with one another or whether, for example, the sectors would overlap:

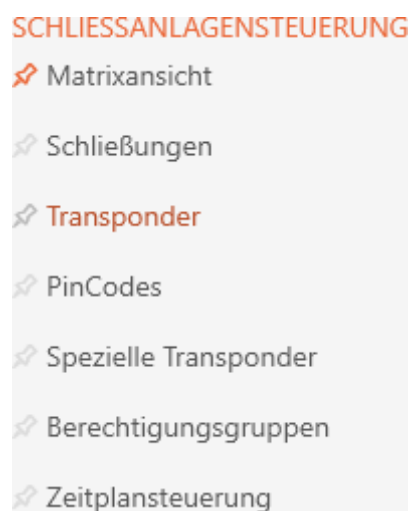



✓ At least two locking systems created in the same project (see *Create locking system [▶ 349]*).

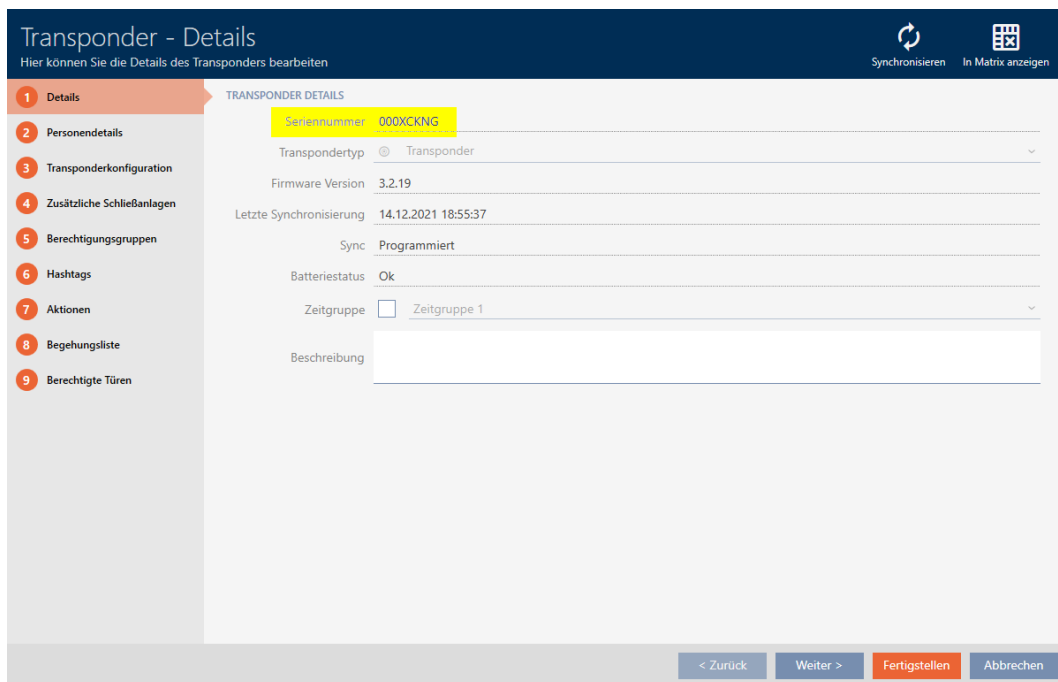
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.



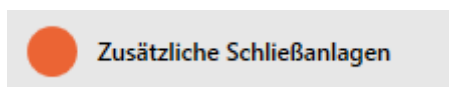
2. Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.



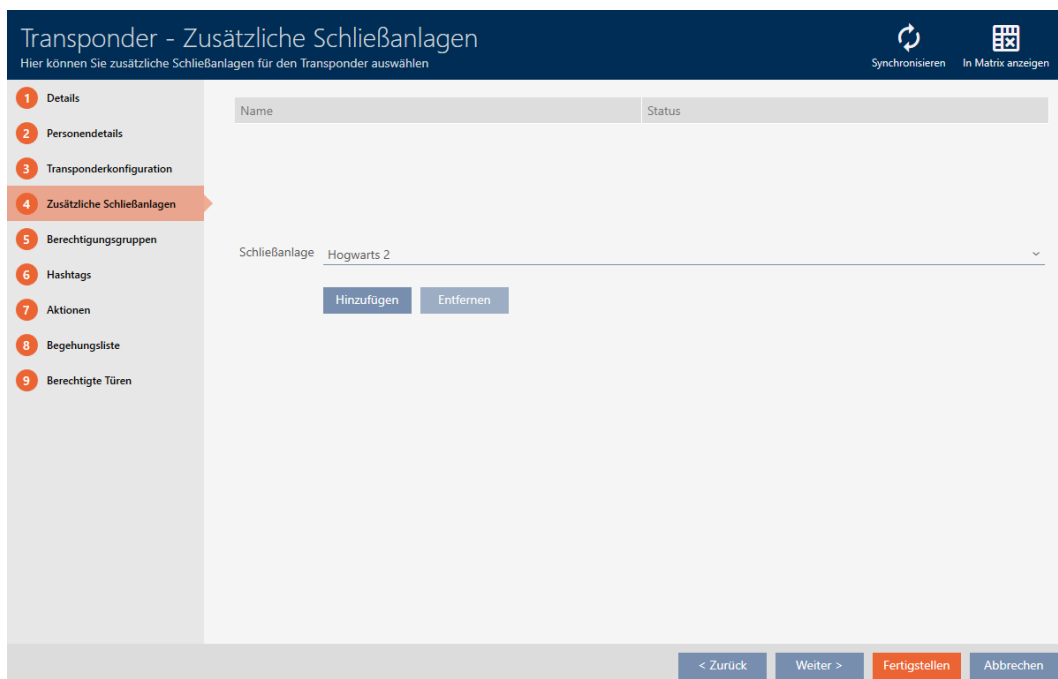
- ↳ The AXM bar will close.
  - ↳ The [Transponder] tab will open.
3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
  4. Click on the identification medium you would like to use in another locking system.
    - ↳ The identification medium window will open.



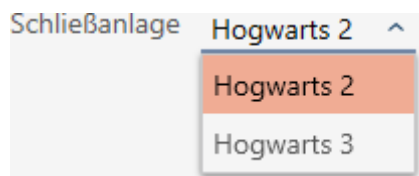
5. Click on the **Zusätzliche Schließanlagen** tab.



↳ Window switches to the "Additional locking systems" tab.



6. Select the locking system in which you would like to reuse the identification medium from the ▼ Locking system drop-down menu.



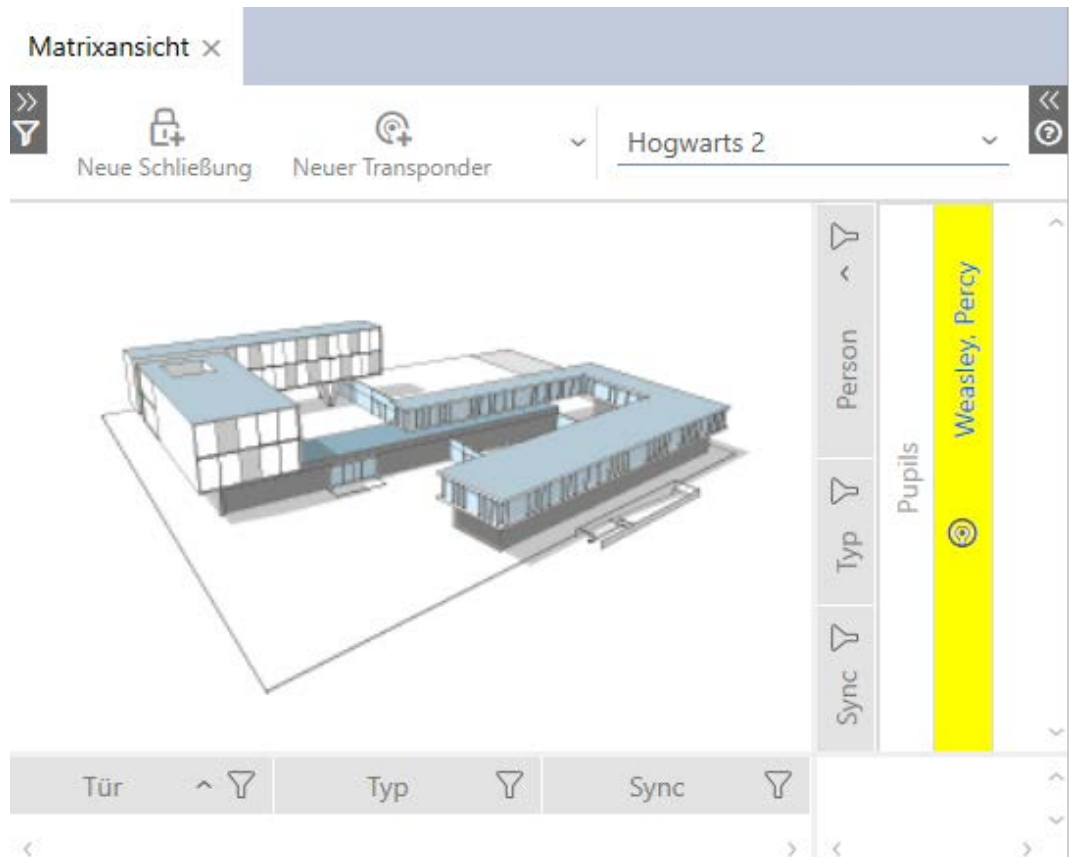
7. Click on the **Add** button.
  - ↳ The selected locking system is listed in the table.

Name	Status
Hogwarts 2	

Schließanlage **Hogwarts 3** ▼

**Hinzufügen** **Entfernen**

8. Click on the **Finish** button.
  - ↳ Your AXM Plus will check whether the locking systems are compatible.
  - ↳ The identification medium window closes.
  - ↳ Reused identification media are automatically added to the other locking systems.

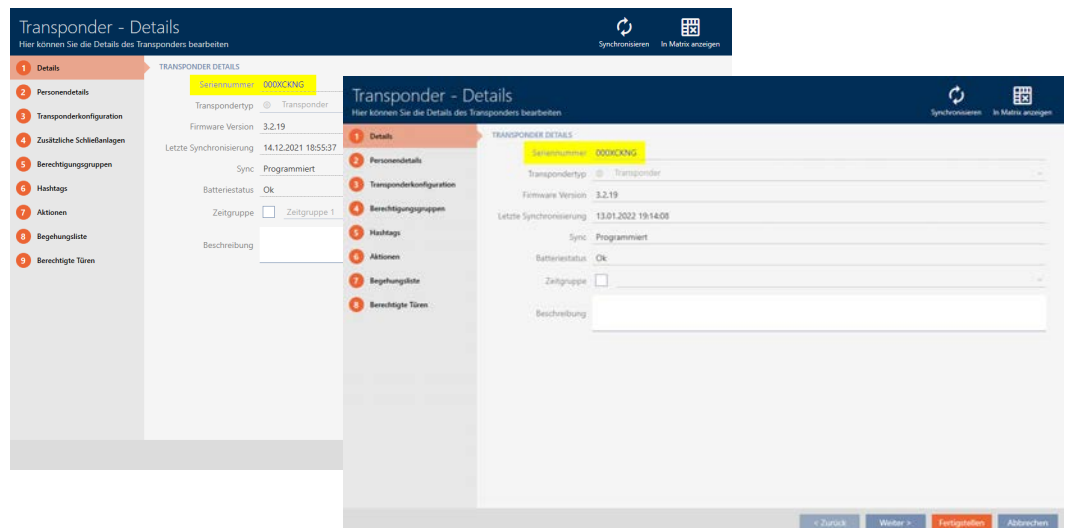


9. Synchronise the identification medium (see *Synchronise a card/transponder (including importing physical access list)* [▶ 410]).

↳ All locking systems in which the identification medium is used are automatically synchronised.

### Recognition by the serial number

Both identification media have the same entry in the *Serial number* field in the "Transponder" window.



One look at the programmed transponder tells you that it really is the same transponder:



(It's required that the transponder's enclosure is the same as delivered from the factory.)

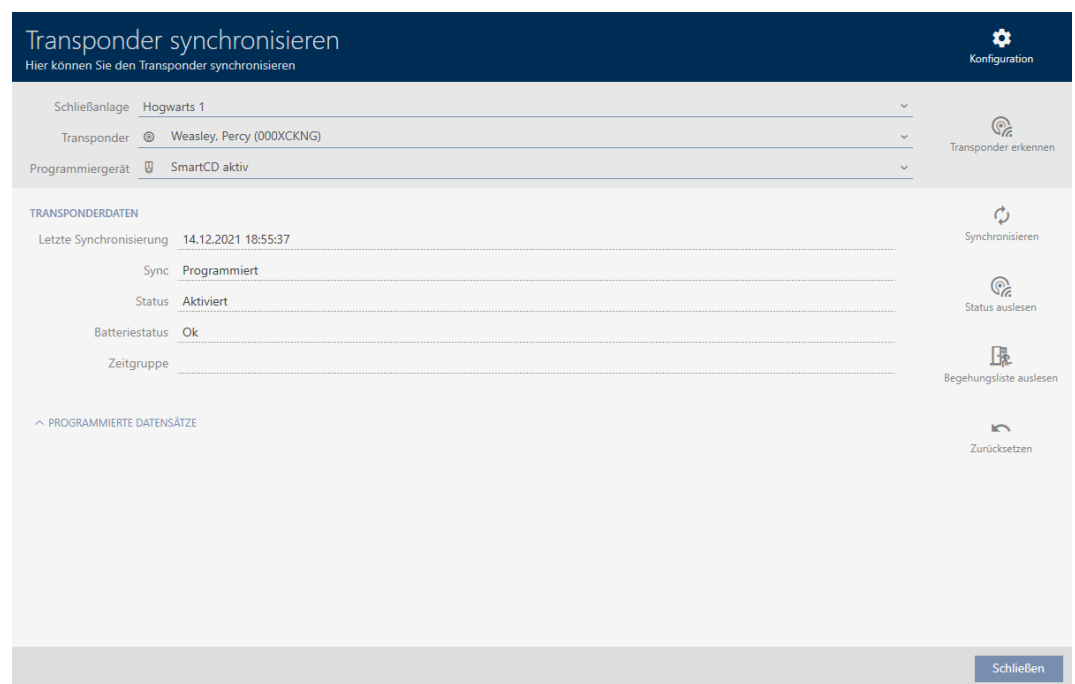
### Recognition by the programmed data sets

You can also recognise use in other locking systems by the programmed data records:

✓ "Transponder" open.

1. Click on the **Synchronisation**  button.

↳ The "Synchronise transponder" window will open.



2. Expand the "Programmed records" area.

↳ You can see the locking system you added earlier in the programmed data sets.

**Transponder synchronisieren**  
Hier können Sie den Transponder synchronisieren

Schließanlage: Hogwarts 1  
Transponder: Weasley, Percy (000XCKNG)  
Programmiergerät: SmartCD aktiv

**TRANSPONDERDATEN**

Letzte Synchronisierung: 14.01.2022 10:50:07  
Sync: Programmiert  
Status: Aktiviert  
Batteriestatus: Ok  
Zeitgruppe:

**PROGRAMMIERTE DATENLISTE**

Pos	Schließanlage/SID	SID Extension	TID	Aktivierungsdatum	Verfallsdatum	Zeitgruppe
1	Hogwarts 1	6644767	3201			
2	Hogwarts 2	6131048	3202			

Schließen

### 14.18.2 Reusing identification medium in other projects/databases

#### Using the same identification medium in different projects/databases

You are not only able to use the same identification medium within a project (see *Reuse identification medium in the same project* [▶ 202]).

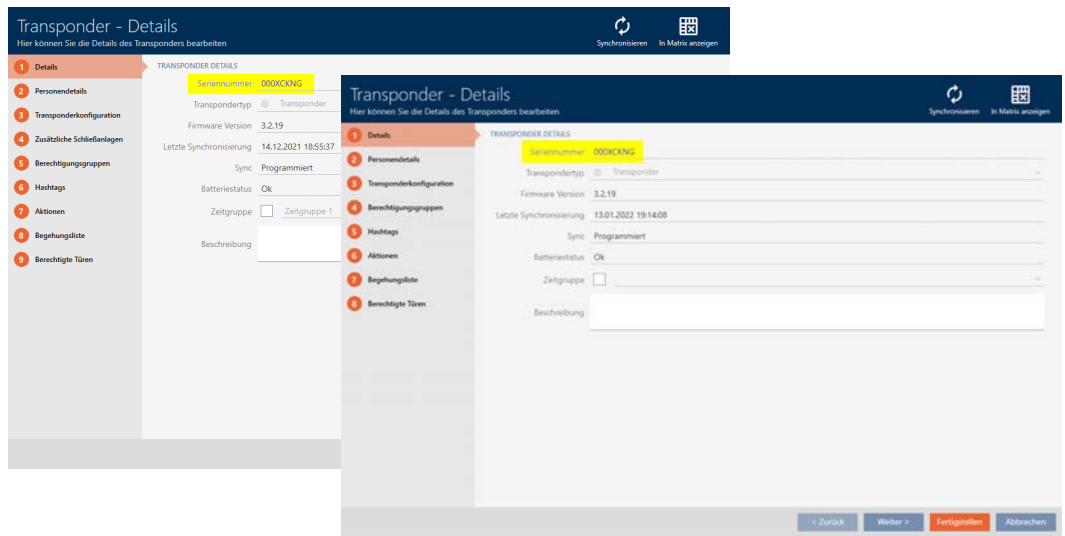
You also have the option of using the same identification medium not only in different locking systems, but also in different databases:

- Use in different AXM projects (projects have their own database)
  - Use in an AXM and an LSM locking system
1. Synchronise the identification medium in your project (see *Synchronise a card/transponder (including importing physical access list)* [▶ 410]).
  2. Synchronise the same identification medium in another project or in another database.
- ↳ Identification medium is used in several locking systems which are separate from one another.

#### Recognition by the serial number

Although they are in different projects, both identification media have the same entry in the *Serial number* field in the "Transponder" window.






A look at the programmed transponder tells you that it really is the same transponder:

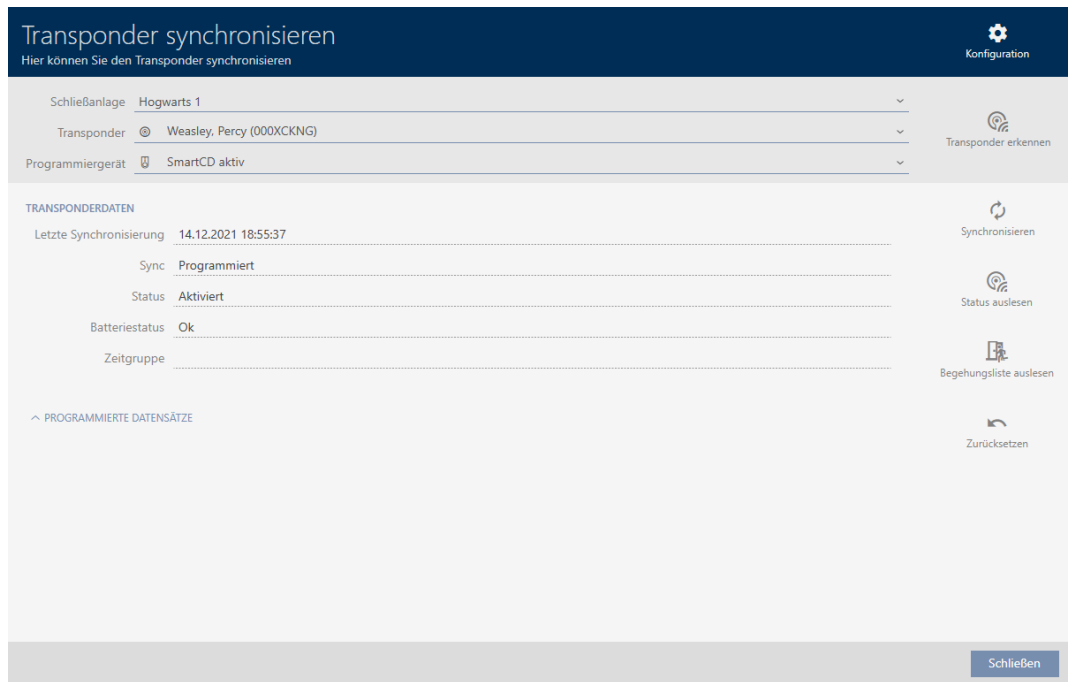


(It's required that the transponder's enclosure is the same as delivered from the factory.)

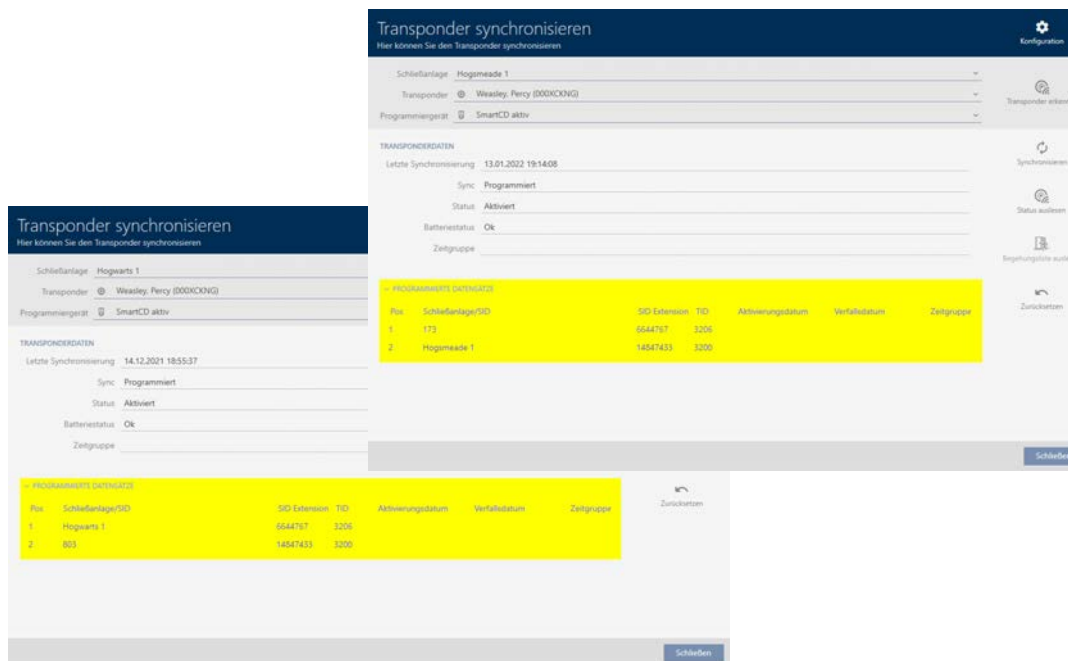
### Recognition by the programmed data sets

You can also identify use in other databases by the programmed data sets:

- ✓ "Transponder" open.
- 1. Click on the **Synchronisation**  button.
  - ↳ The "Synchronise transponder" window will open.



2. Synchronise the transponder (see *Synchronise a card/transponder (including importing physical access list)* [▶ 410]).
3. Expand the "Programmed records" area.
  - ↳ Depending on which locking system you are in, you will see a second locking system in the programmed data sets. However, you will only see the locking system ID unlike when you reuse it in the same project (see *Reuse identification medium in the same project* [▶ 202]). The locking system ID is also stored in the identification medium and is therefore known. However, the locking system's name is saved in another database and therefore cannot be displayed.



## 14.19 Managing AX2Go keys

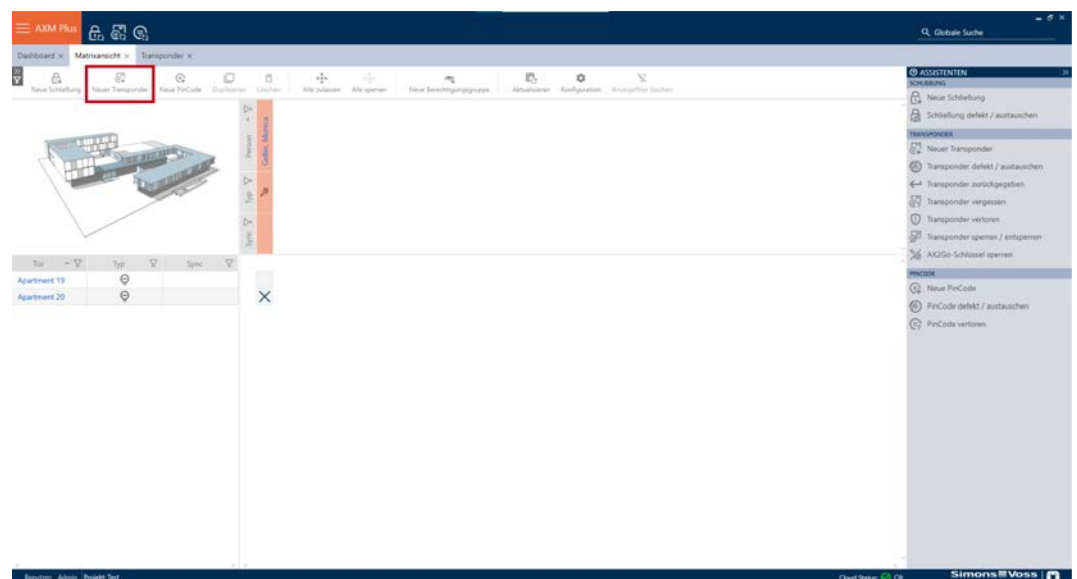
### 14.19.1 Assigning keys for AXM Plus and higher

In the interests of best practice (see *Best practice: setting up the locking system* [▶ 27]), SimonsVoss recommends that you configure authorisation groups, person groups and schedules/time groups:

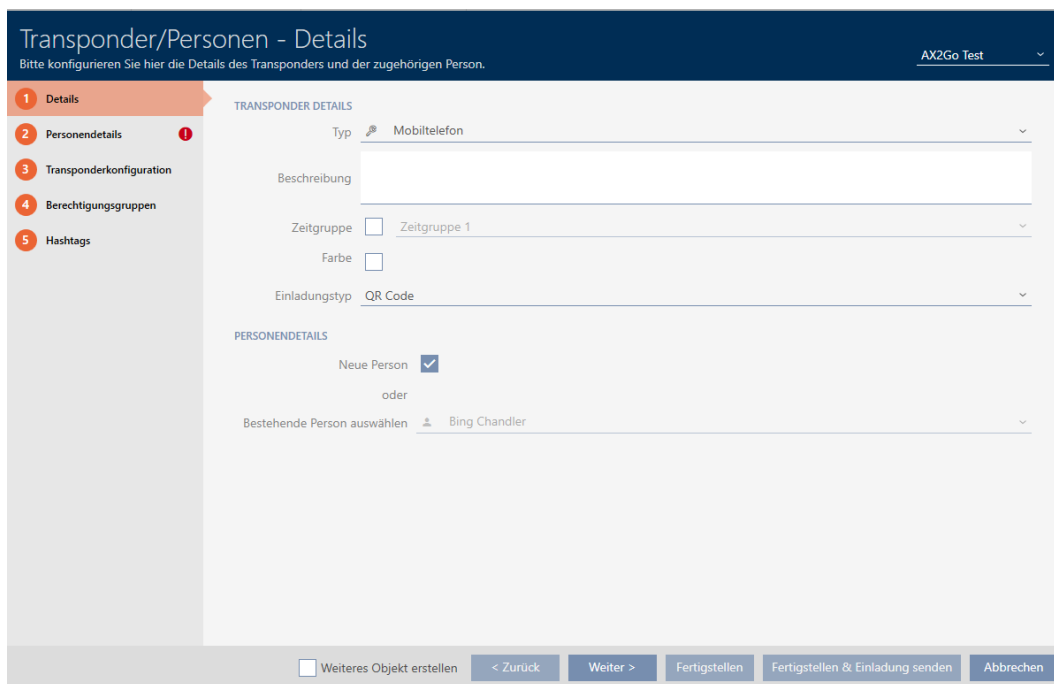
- *Authorisation groups* [▶ 322] (see *Authorisation groups* [▶ 543] for background information )
- *Creating a person group* [▶ 51] (see *Person groups* [▶ 544] for background information )
- *Creating a schedule* [▶ 53] or *Create time group* [▶ 56] (see *Time groups and schedules* [▶ 528] for background information )

As a locking system administrator, you can also send mobile keys to users, which are saved as access authorisations in the AX2Go app. Creating keys for AX2Go works in the same way as creating transponders.

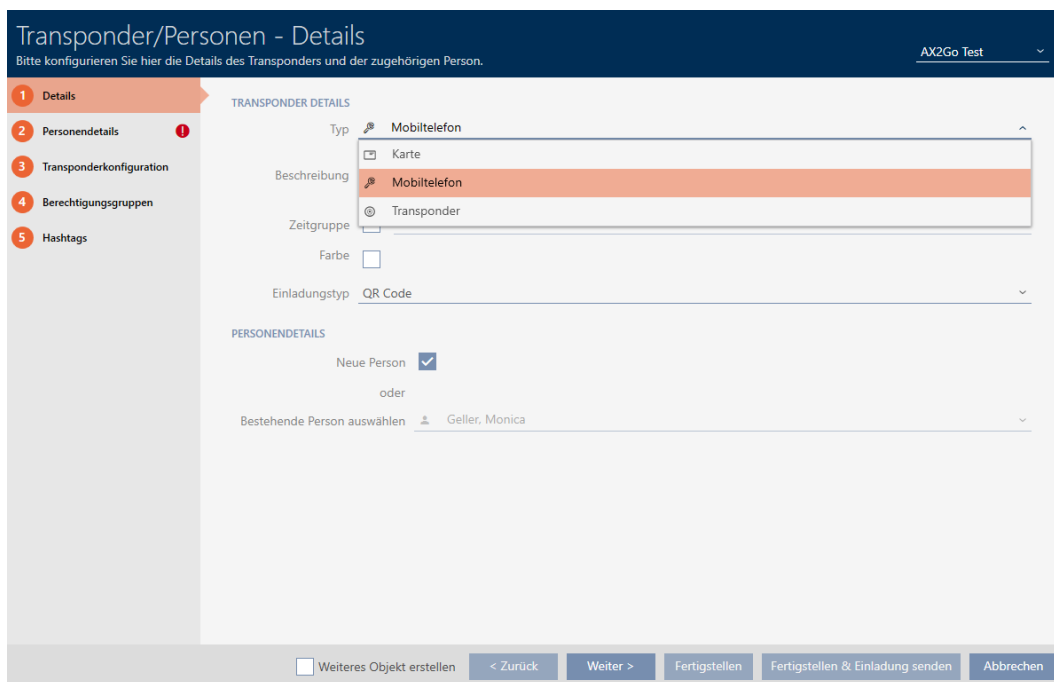
1. Click the  **New transponder** button in the matrix view of your locking system.



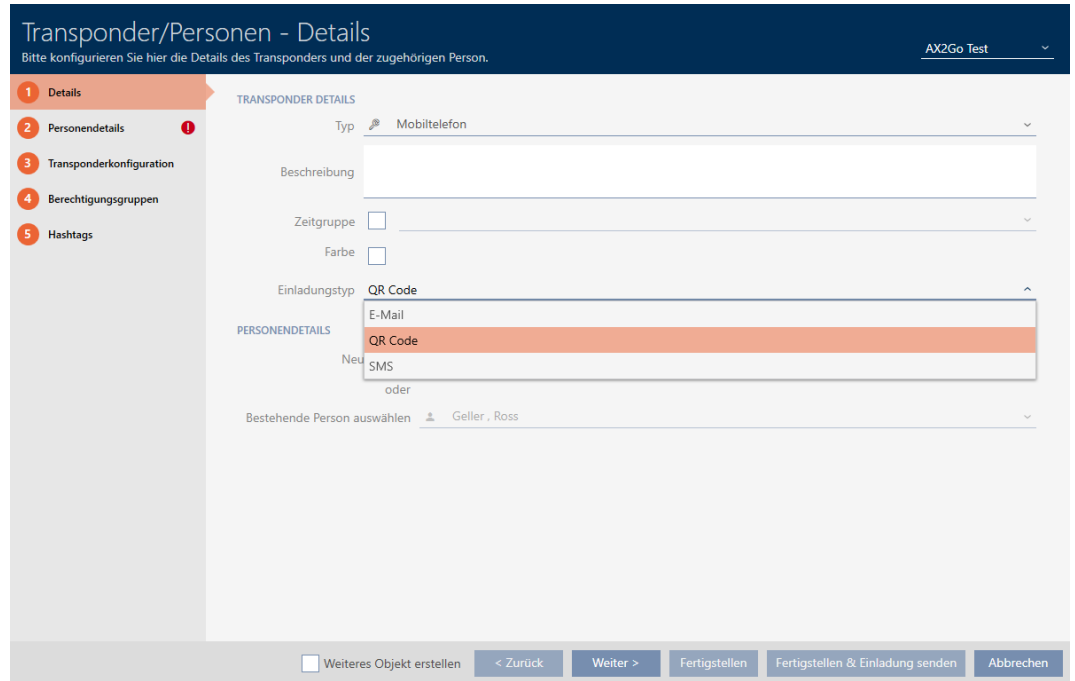
- ↳ A screen will open where you can configure the key and user settings.



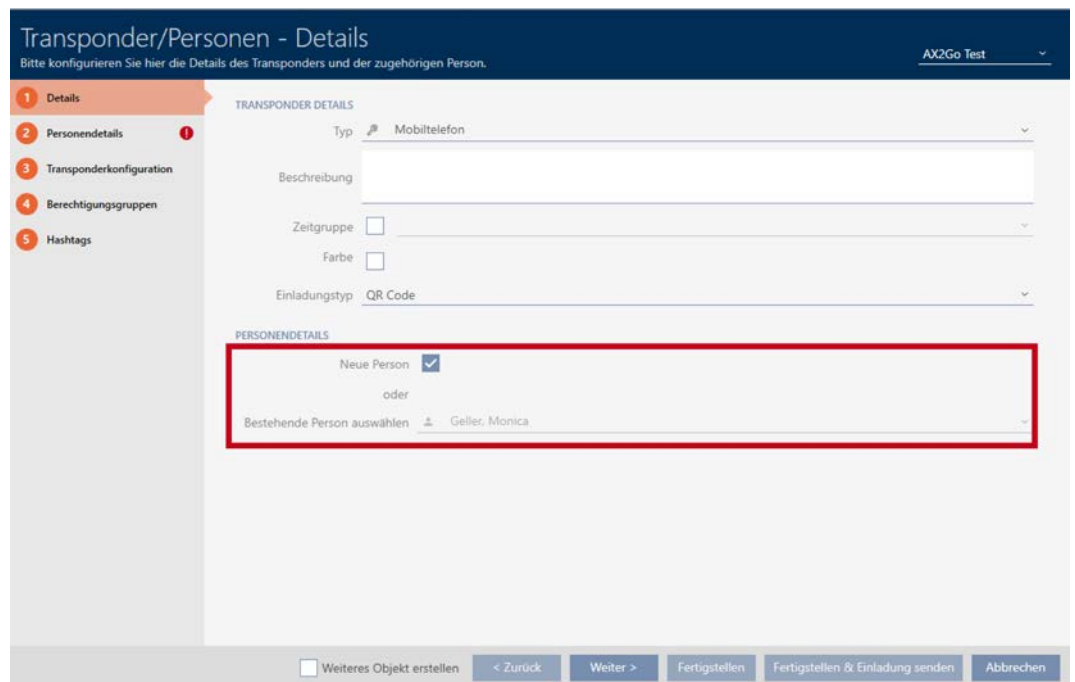
2. Selecting "Smartphone" as a transponder type



3. Select the option that you require from ▼ Invitation type.  
You can choose between "Email", "QR Code" and SMS here.



4. To create a new person, select the  New person box in the **Person details** section.  
Alternatively, you can also choose from the list of existing persons if you want to assign a second key to a person. Then click on **Next >**.



- Fill in the mandatory fields marked in red in the **Person details** tab. All other details are optional. Then click on **Next >**.



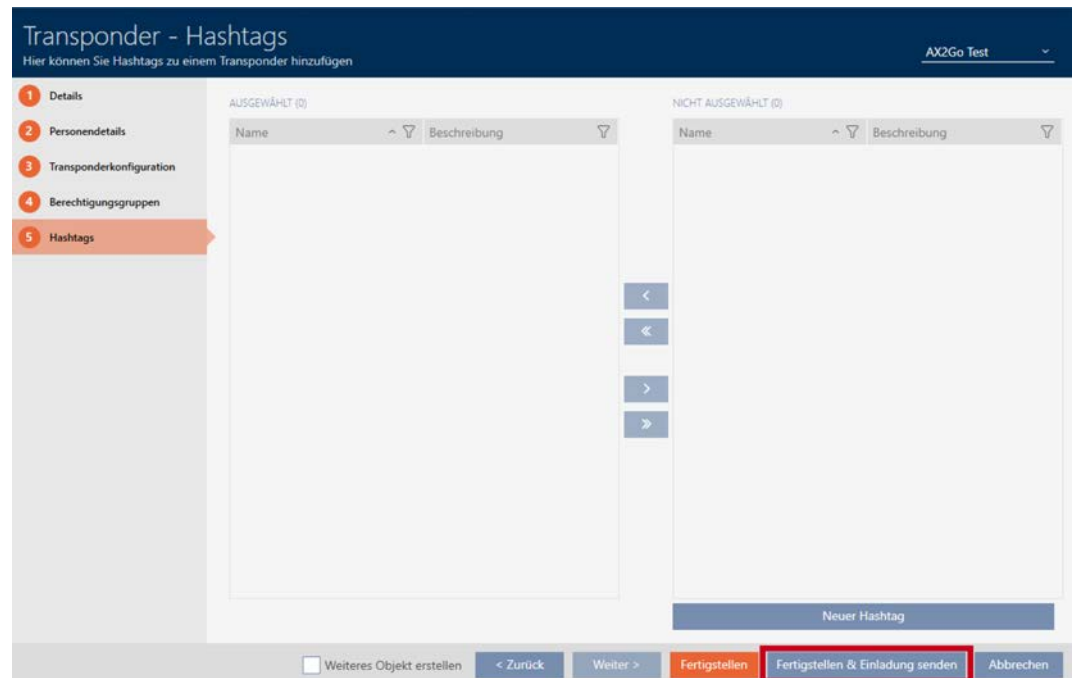
**NOTE**

**Mandatory information, depending on the type of invitation**

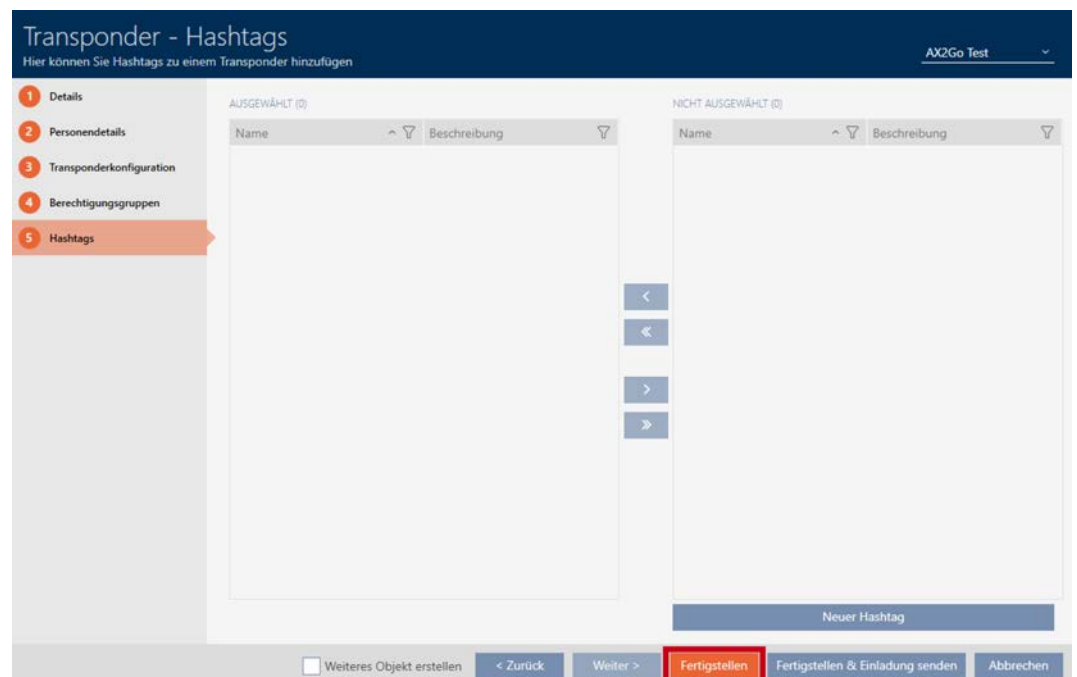
Note that the mandatory fields to be completed vary depending on the type of invitation selected.

- You **can** configure further settings in the **Transponder configuration**, **Access levels** and **Hashtags** tabs. See *Creating transponders and cards* [▶ 89], *Creating a hashtag* [▶ 85] and *Authorisation groups* [▶ 322] for more information.

- Once you have made all the settings that are relevant to you, you can complete the configuration and send an invitation immediately. To do so, click on the **Finish & Send an Invite** button.



- Optionally**, you can complete the configuration with the **Finish** button and send the invitation at a later time in the transponder settings.

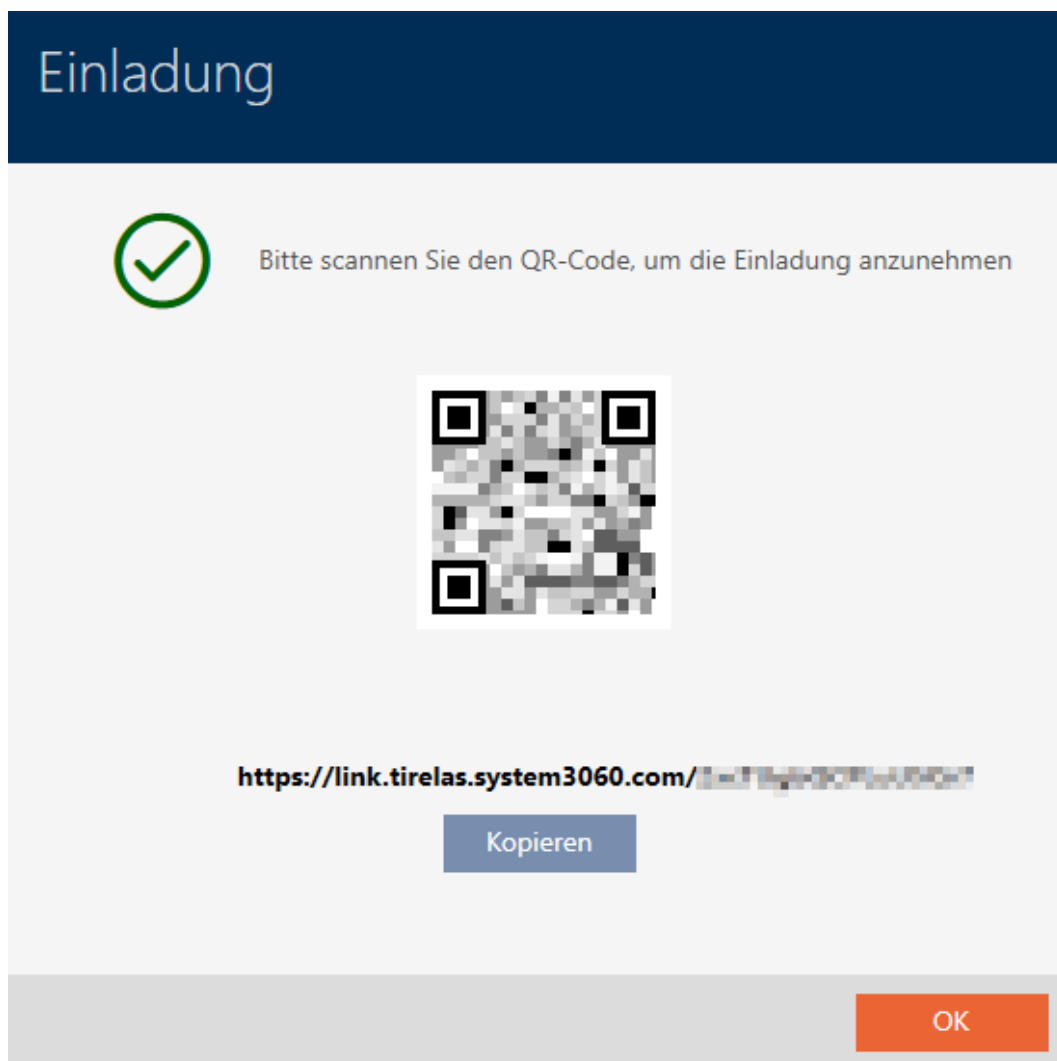


- Click on the relevant user.
  - ↳ The transponder details will open. A message will also appear stating that no invitation has been registered for this user yet.

 Es wurde keine Einladung registriert.

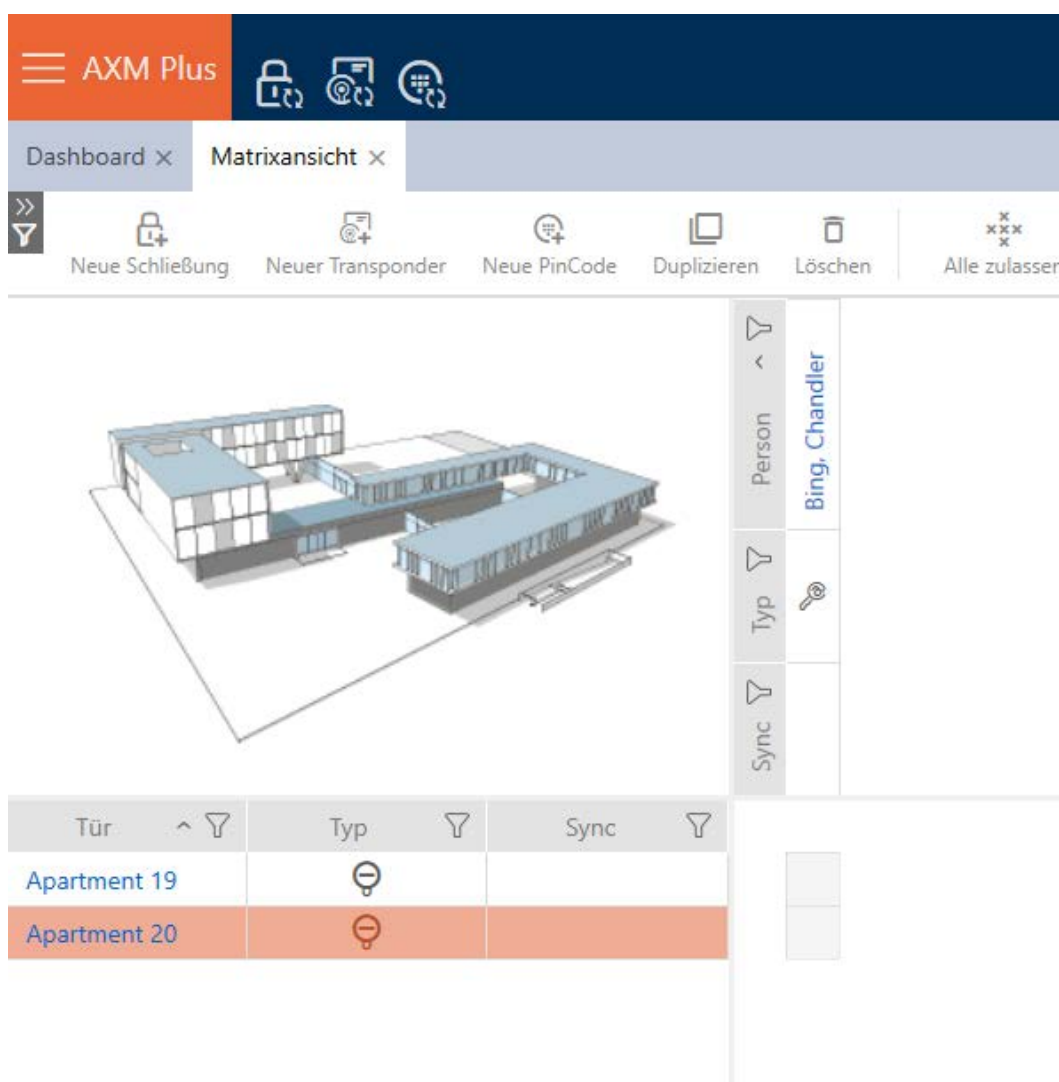
10. Click the **Finish & Send an Invite** button to send the invitation.

↳ With **▼ Invitation type**, another window will appear, e.g. with a QR code and a link.



↳ You have successfully sent the invitation and created an AX2Go key.

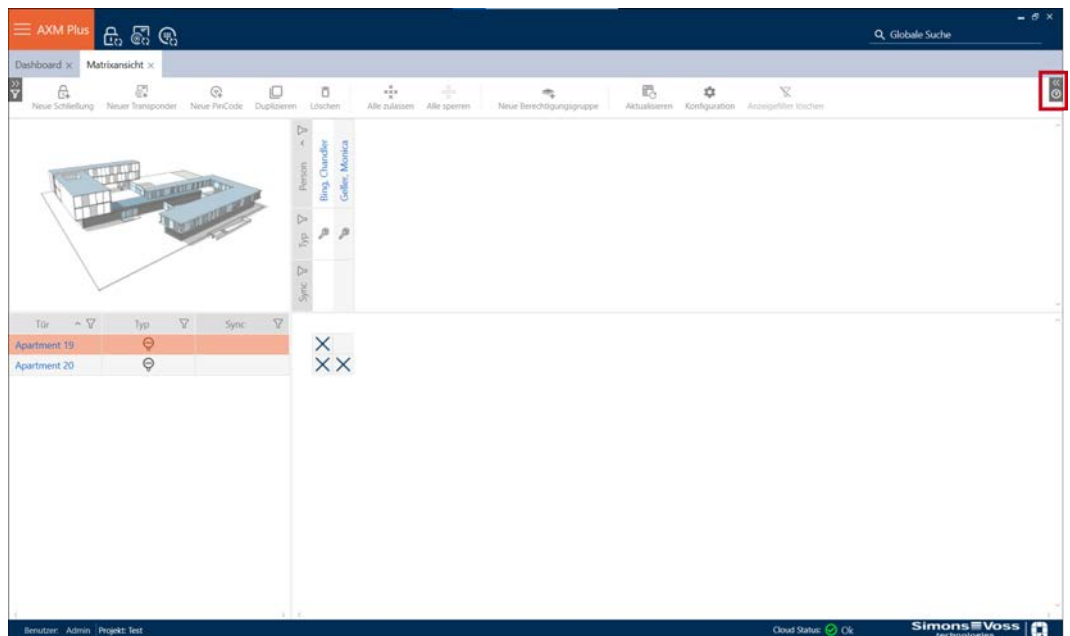




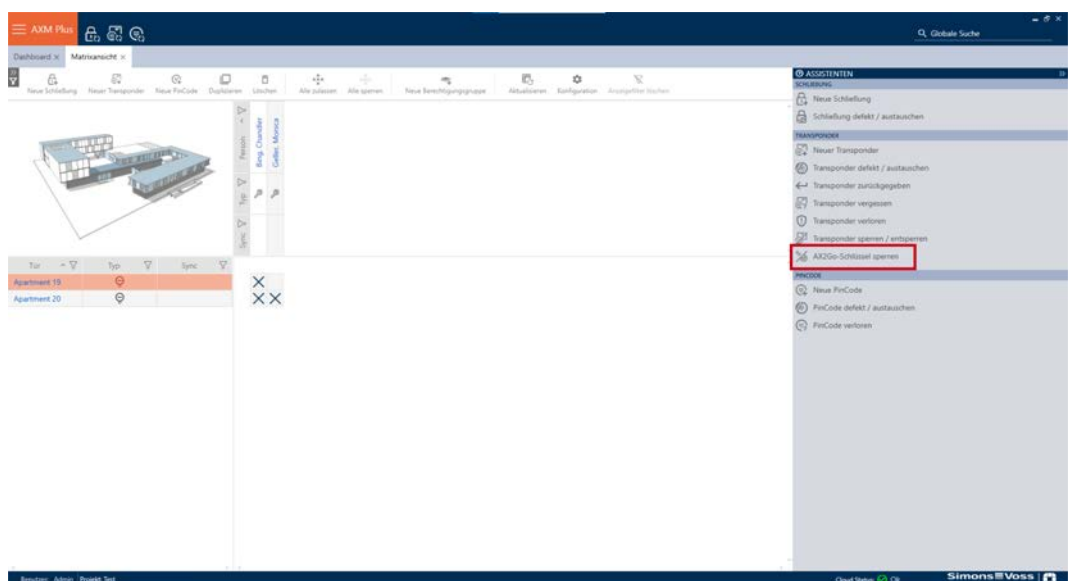
### 14.19.2 Blocking an AX2Go key

The locking system administrator can also withdraw assigned keys, thus blocking them.

1. Open the Wizards on the right-hand side of your matrix screen.



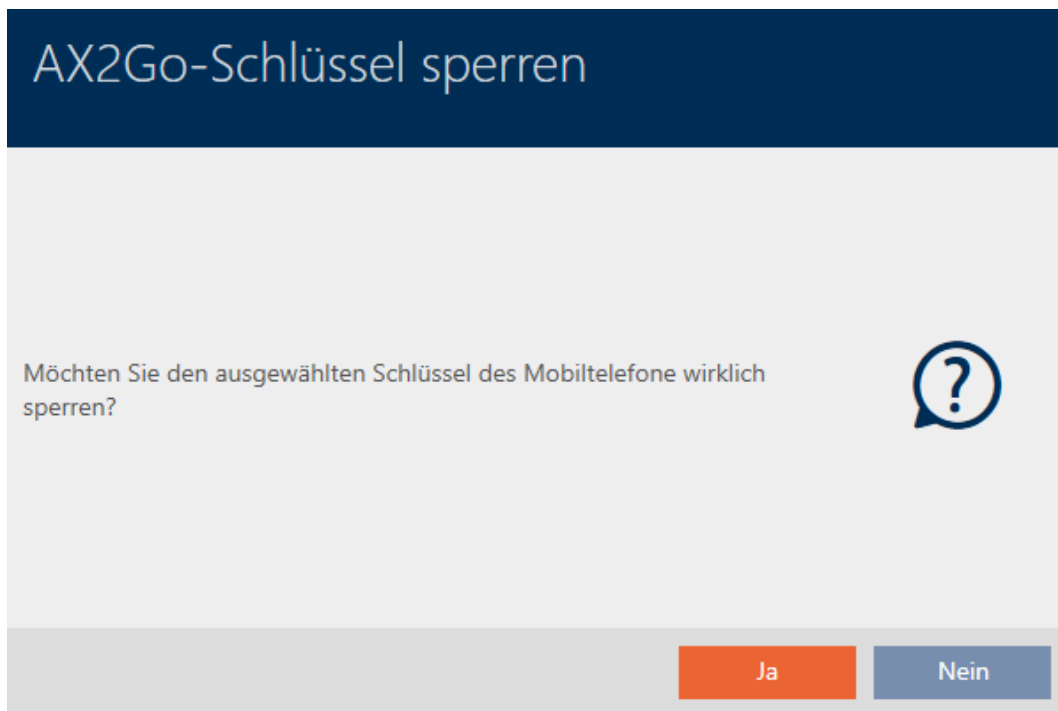
2. Click on the point  Revoke AX2Go Key.



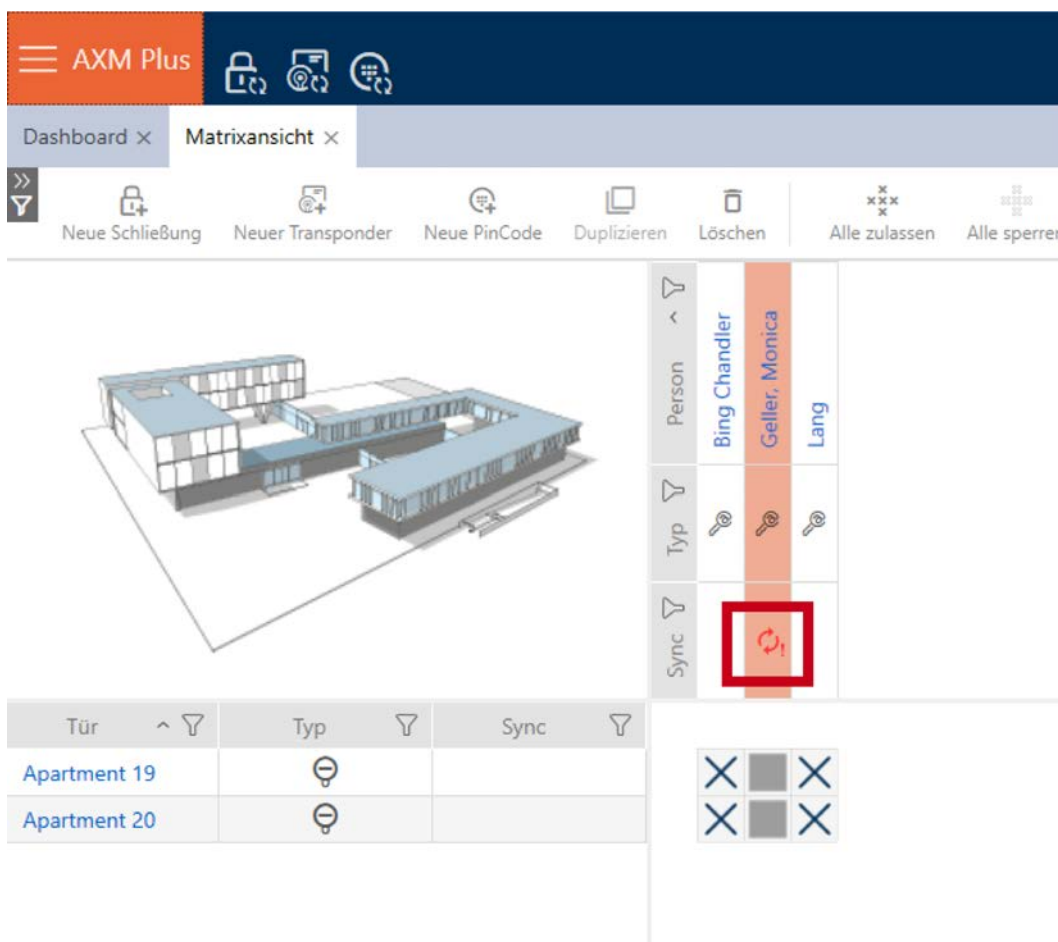
- Under Transponder, select the person whose AX2Go key you want to block and click on **Next**.

The screenshot shows a software window titled "AX2Go-Schlüssel widerrufen - Assistent". At the top, there is a dark blue header with the title. Below the header, there are two dropdown menus. The first is labeled "Schließanlage" and has "AX2Go Test" selected. The second is labeled "Transponder" and has a list of two options: "Bing, Chandler (135CKA5)" and "Geller, Monica (135CK9K)". Below the dropdowns, there is a section titled "AX2GO-SCHLÜSSEL WIDERRUFEN". Under this title, there are two sections: "Ereignis:" followed by the text "Der ausgewählte Schlüssel des Mobiltelefons soll widerrufen werden." and "Aktion:" followed by the text "Der aktuelle Schlüssel des Mobiltelefons wird dauerhaft gesperrt." At the bottom right of the window, there are two buttons: "Weiter" and "Schließen".

- A window will appear asking you whether you are sure you want to block the key. Click on **Yes**.



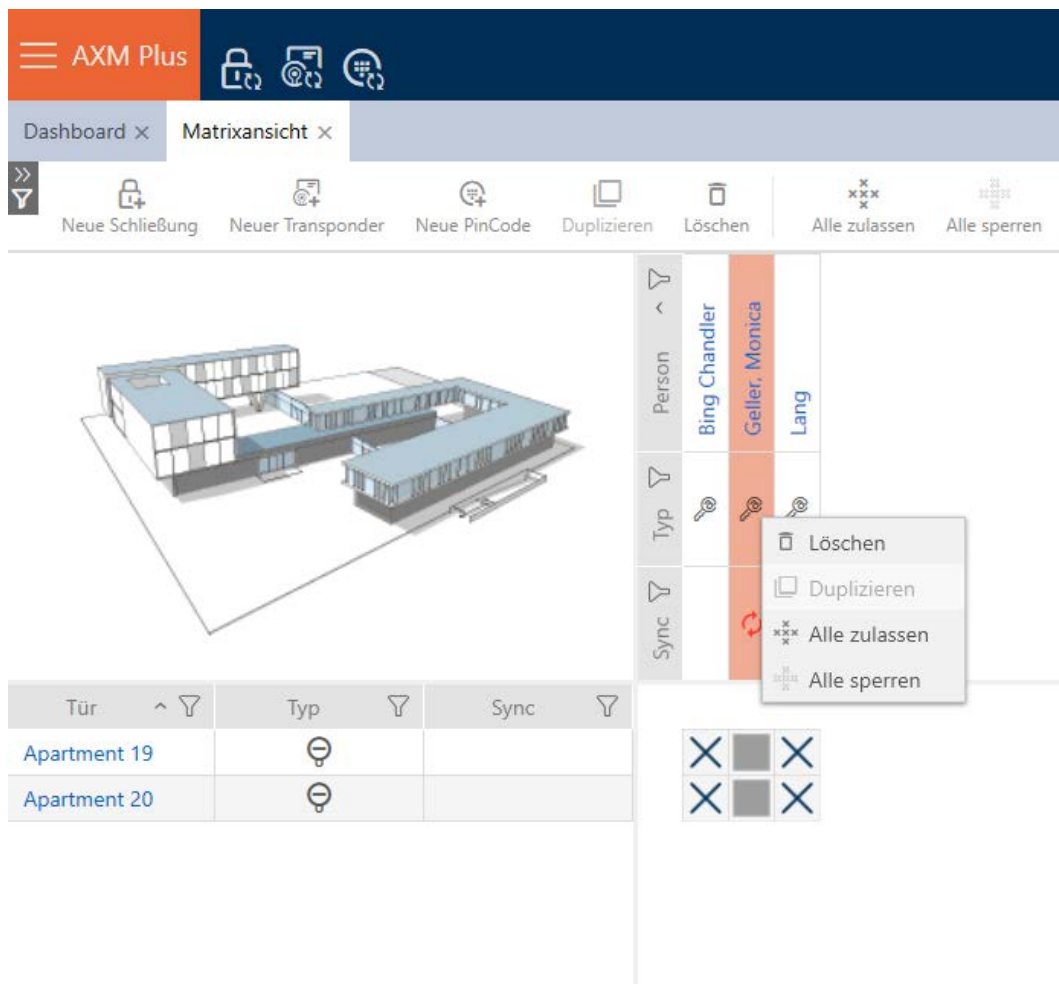
↳ The AX2Go key you selected has been blocked successfully.



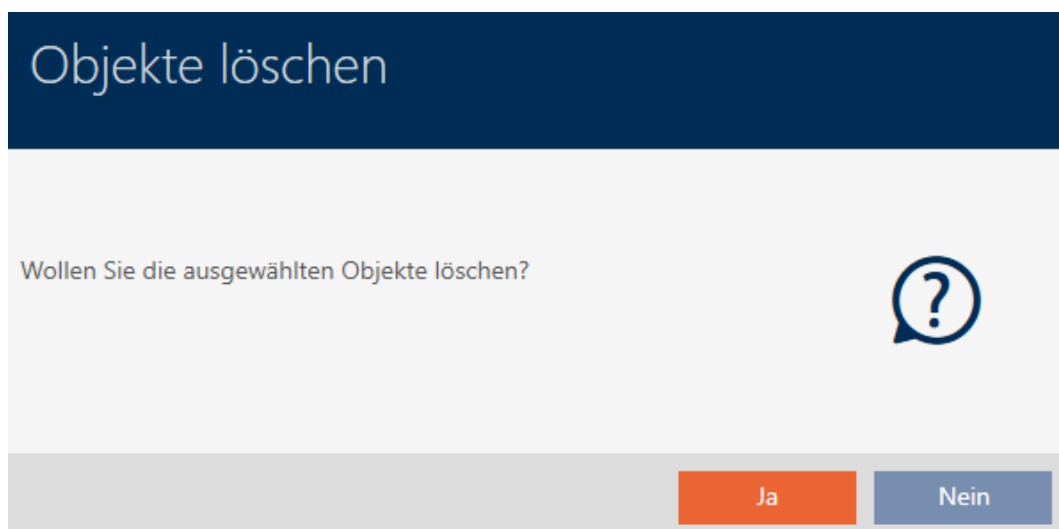
### 14.19.3 Deleting AX2Go keys

After blocking the key, you can also delete it and thus remove it completely. Proceed as follows to remove the AX2Go key from the matrix view:

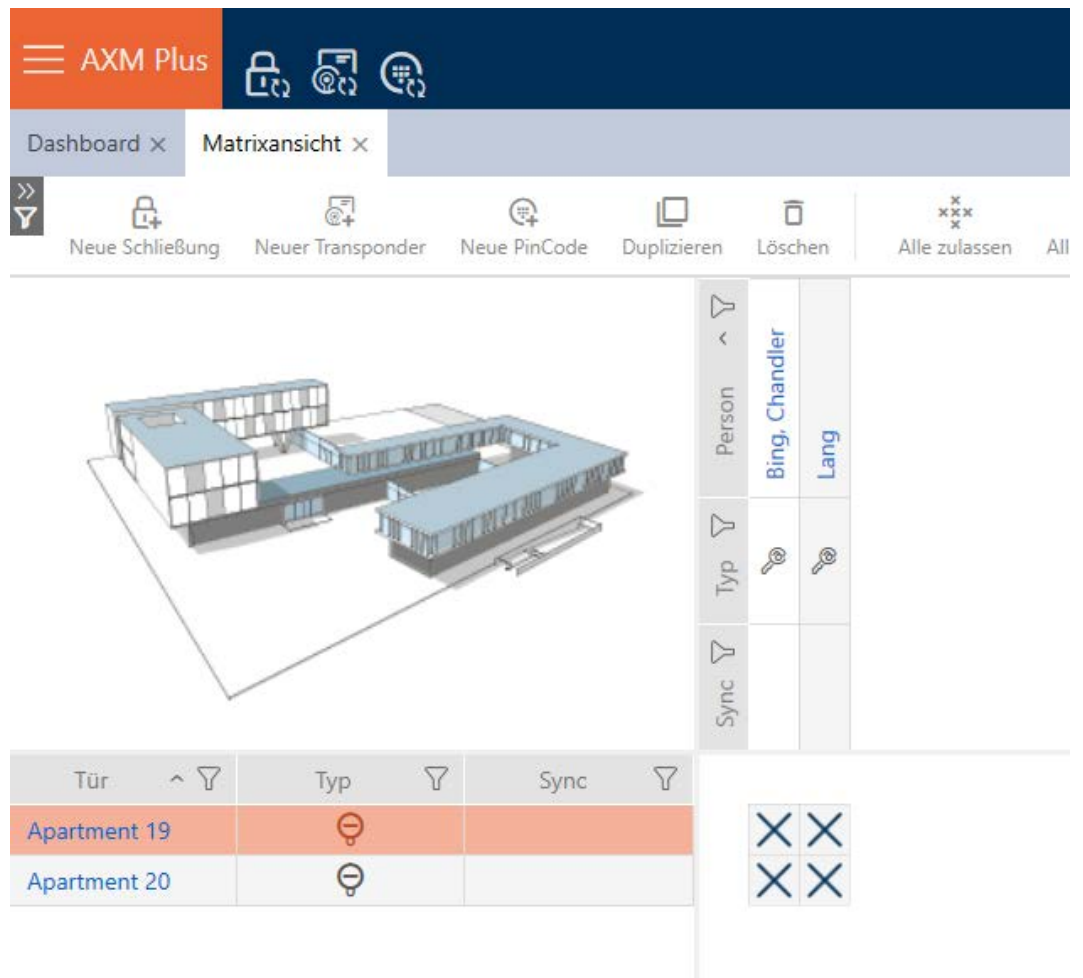
1. Right-click on the key and click on **Delete**.



- ↳ A screen will open asking you whether you are sure you wish to delete the object.



2. Click on the **Yes** button.
  - ↳ You have successfully deleted the selected key. It is no longer visible in the matrix view.



## 14.20 Setting the PIN length (PinCode AX)



### NOTE

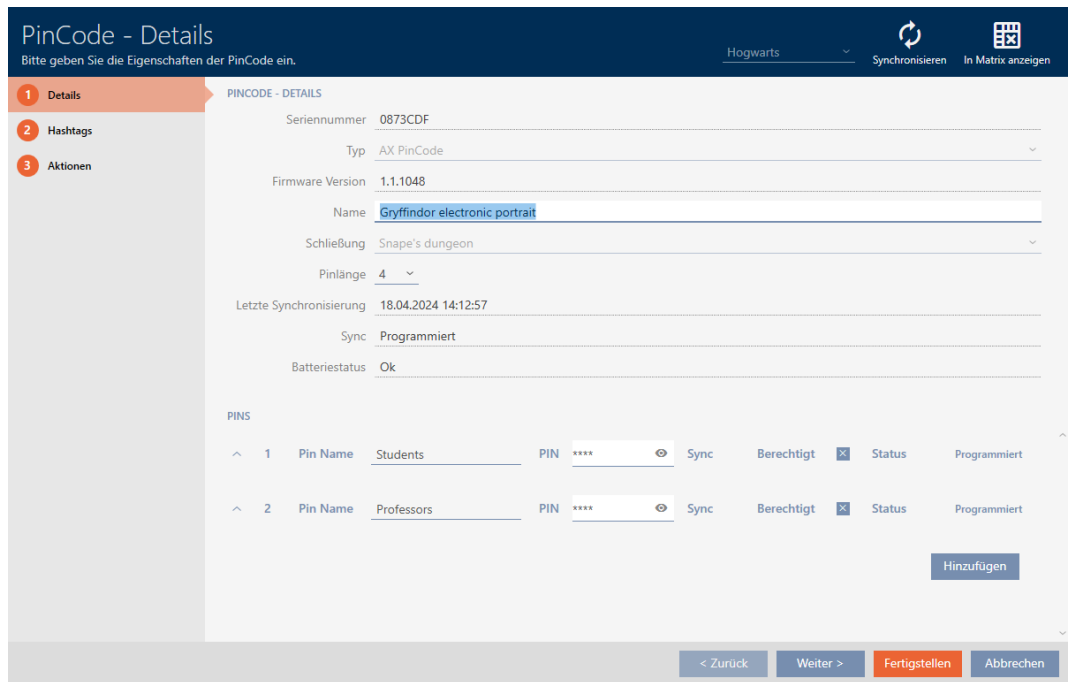
#### Description only valid for PIN code keypad AX

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

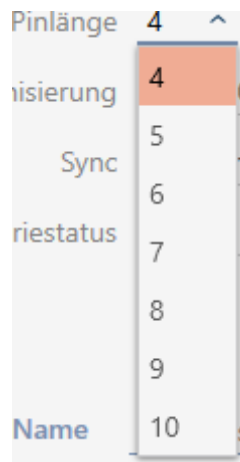
You always set the PIN length for the entire PIN code keypad AX, i.e. for all PINs simultaneously. For this reason, you must then reassign each PIN and synchronise the PIN code keypad AX.

- ✓ Matrix screen open.
- ✓ PIN code keypad AX created (see *Creating PIN code keypads* [▶ 96]).

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



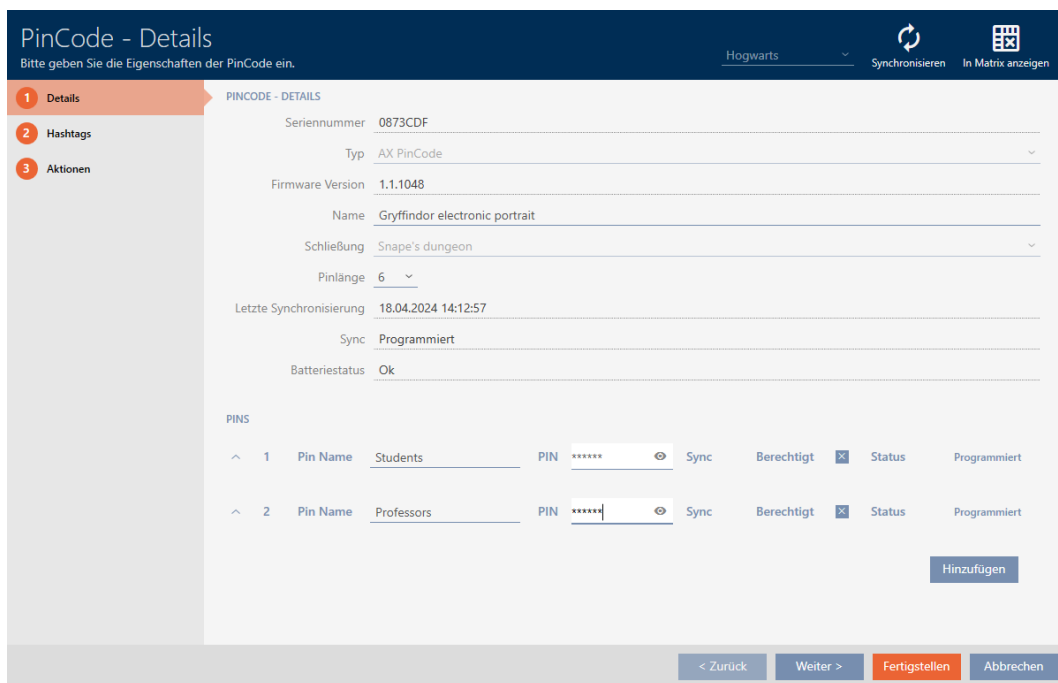
2. Select the required PIN length from the ▼ Pin length drop-down menu.



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

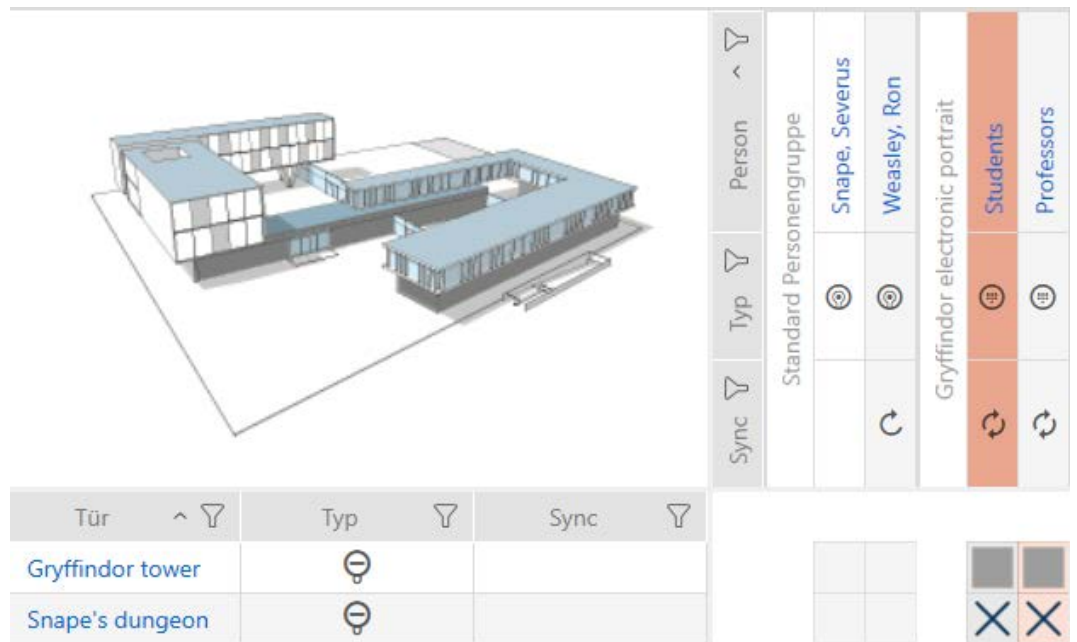


3. Click on the **OK** button.
  - ↳ All PINs are red and must be reassigned.
4. Reassigning the PINs.



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.





### 14.21 Changing a PIN (PinCode AX)

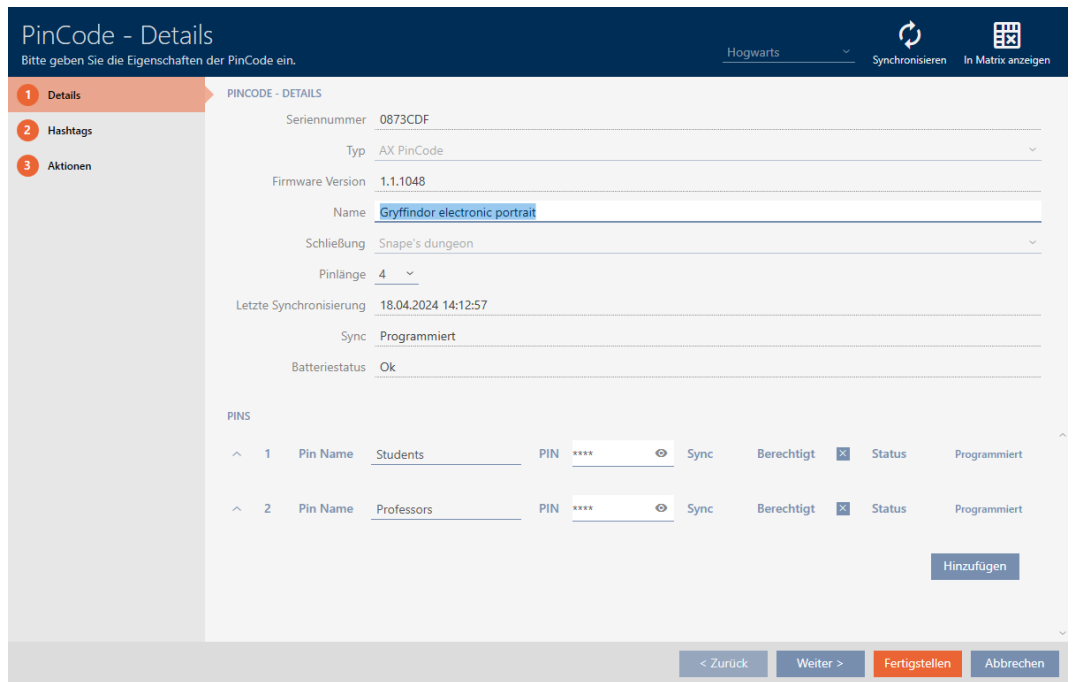


#### NOTE

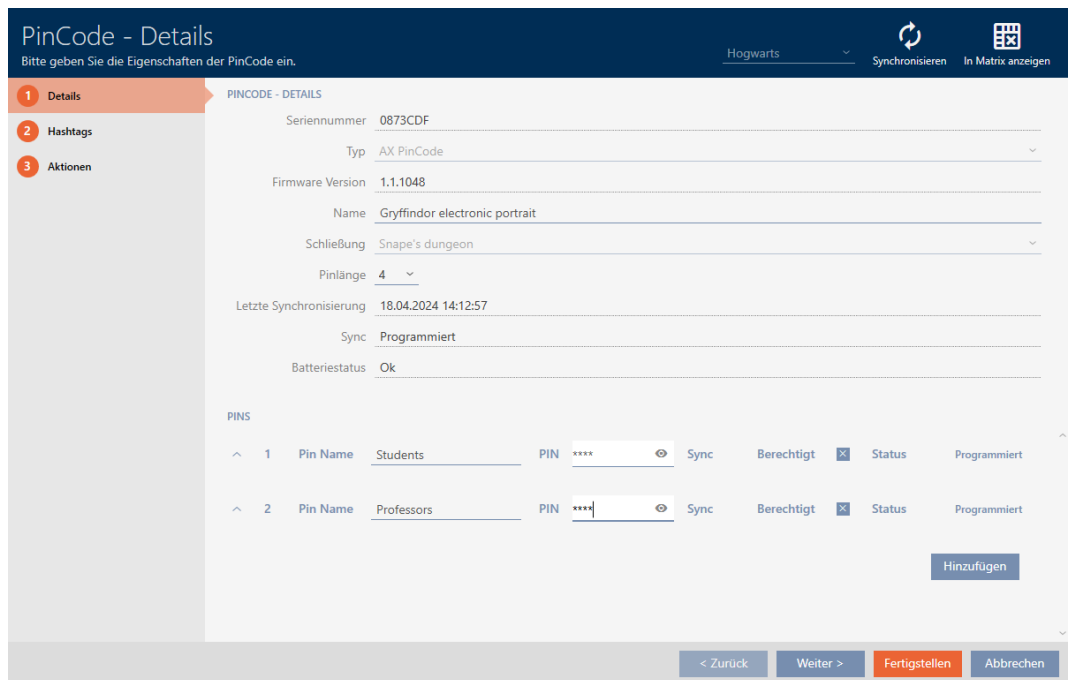
#### Description only valid for PIN code keypad AX

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

- ✓ Matrix screen open.
  - ✓ PIN code keypad AX created (see *Creating PIN code keypads* [▶ 96]).
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.



Tür	Typ	Sync
Gryffindor tower	☹	
Snape's dungeon	☹	

Person	Typ	Sync
Standard Personengruppe		
Snape, Severus	☹	
Weasley, Ron	☹	
Gryffindor electronic portrait		
Students	☹	↻
Professors	☹	

		✕	✕

## 15. 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)* [▶ 399]).

### 15.1 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.* [▶ 524] for more information on this topic.

In line with best practice requirements (see *Best practice: setting up the locking system* [▶ 27]), SimonsVoss recommends that you first plan things out in preparation:

- *Authorisation groups* [▶ 322] (see *Authorisation groups* [▶ 543] for background information )
- *Creating an area* [▶ 83] (see *Areas* [▶ 548] for background information )
- *Creating a schedule* [▶ 53] or *Create time group* [▶ 56] (see *Time groups and schedules* [▶ 528] for background information )
- *Creating a time switchover* [▶ 65] (see *Time switchovers* [▶ 532] for background information )
- *Creating a location* [▶ 77] or *Creating a building and assigning it to a location* [▶ 80] (see *Buildings and locations* [▶ 547] for background information )
- *Creating a hashtag* [▶ 85] (see *Hashtags* [▶ 549] for background information )

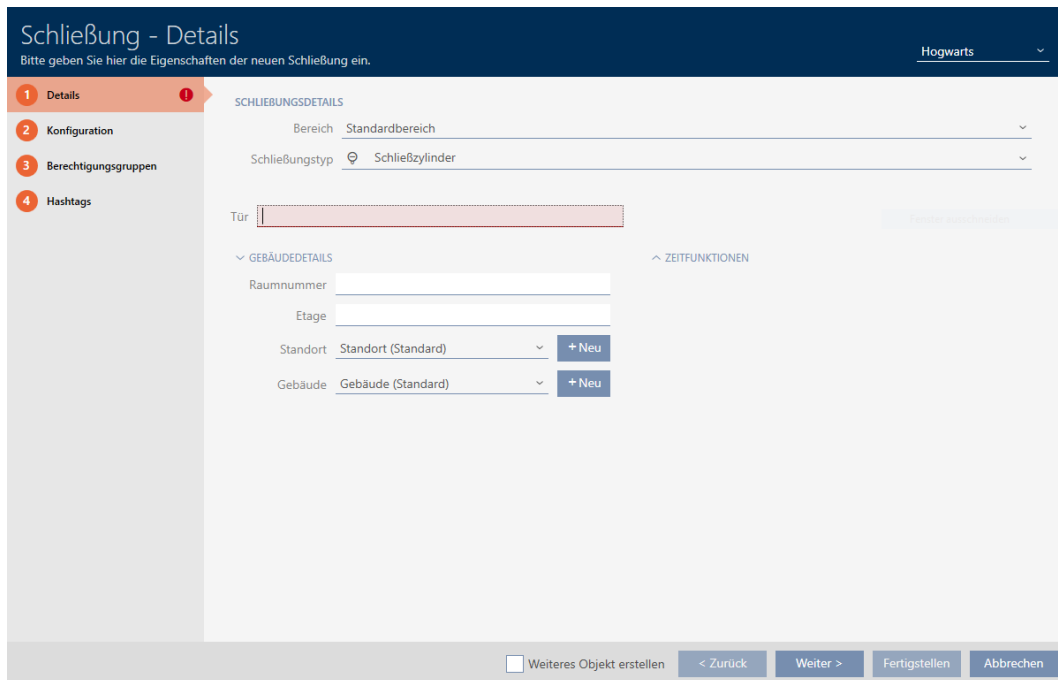


#### NOTE

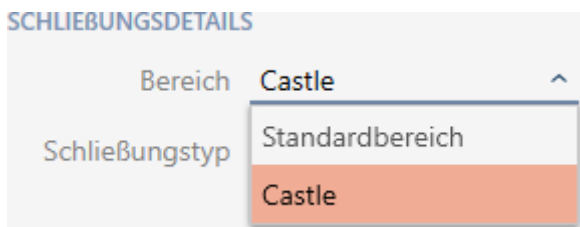
##### Hidden settings

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

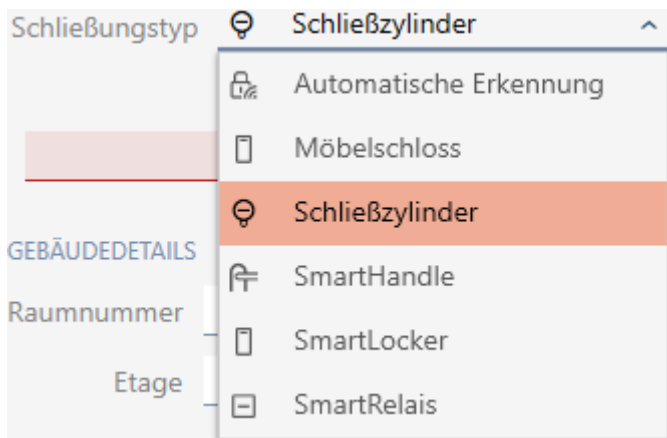
1. Click on the **New lock** button .  
 ↳ The window for creating a new locking device will open.



2. Select the area to which your locking device belongs from the ▼ **Area** drop-down menu.



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





**NOTE**

**Recognising a locking device automatically**

You may not know which entry to select from the ▼ **Lock type** drop-down list yet. AXM Plus also provides you with the "Automatic detection" entry.

AXM Plus does not save the detected locking device type until you actually program the locking device. The options in the "Configuration" tab are also extended or hidden to match the locking device type at this time.

4. Name your locking device in the *Door* field.
5. If necessary, enter the number of the room where your locking device will be installed in the *Room number* field.
6. If necessary, enter the floor on which your locking device will be installed in the *Floor* field.
7. Select the location where your locking device will be installed from the ▼ **Location** drop-down menu.

▼ GEBÄUDEDETAILS

Raumnummer

Etage  **Das Feld ist erforderlich**

Standort  ^

Gebäude  Standort (Standard)  
Unterföhring

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

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

▼ GEBÄUDEDETAILS

Raumnummer

Etage

Standort  Unterföhring **Das Feld ist erforderlich** v

Gebäude  ^  
FeringasträÙe 4

9. 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)* [▶ 276] and *Engaging and disengaging locking devices automatically with time switchover* [▶ 278] for details).

▼ ZEITFUNKTIONEN		
Zeitplan	<input type="checkbox"/>	+ Neu
Zeitumschaltung	<input type="checkbox"/>	+ Neu
Feiertagsliste	<input type="checkbox"/>	+ Neu



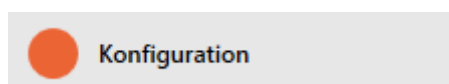
#### NOTE

##### Public holiday lists in locking device and locations

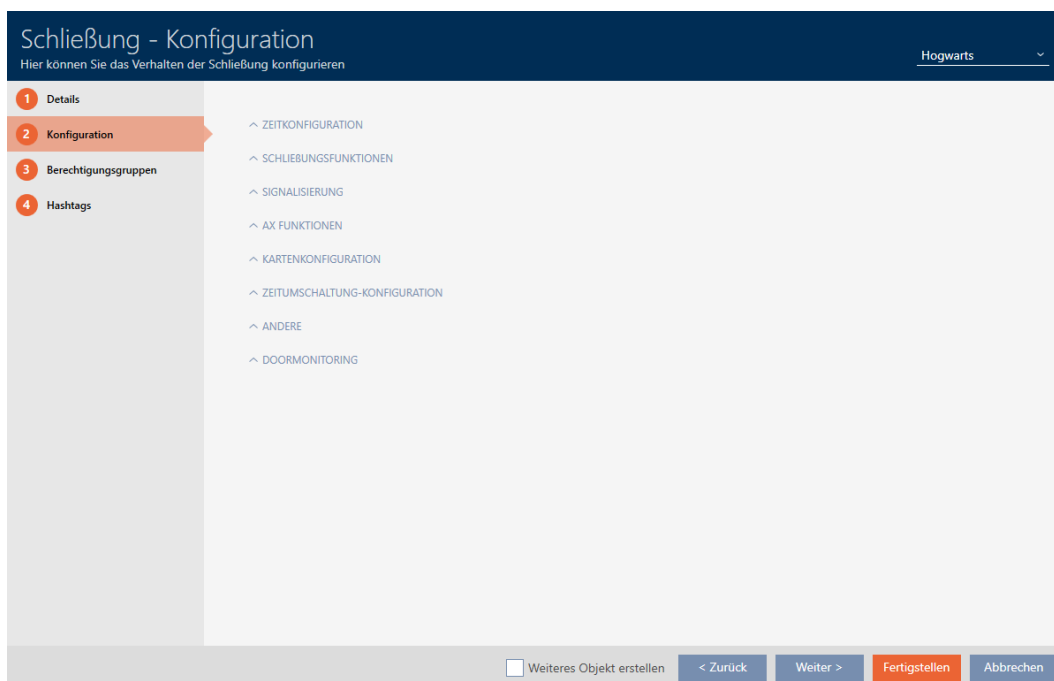
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

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.

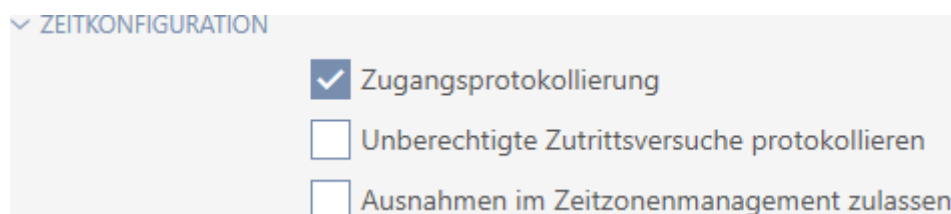
10. Click on the  Configuration tab.



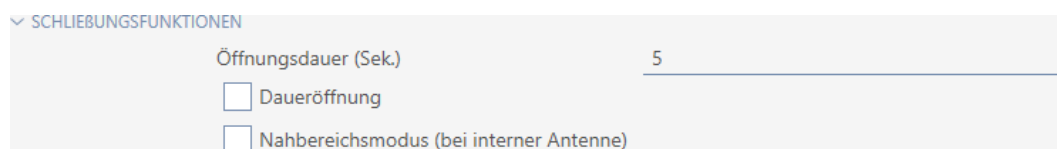
- ↳ Window switches to the "Configuration" tab.



11. 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)* [▶ 284]).



12. 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* [▶ 286] and *Limit locking device read range (close range mode)* [▶ 288]).



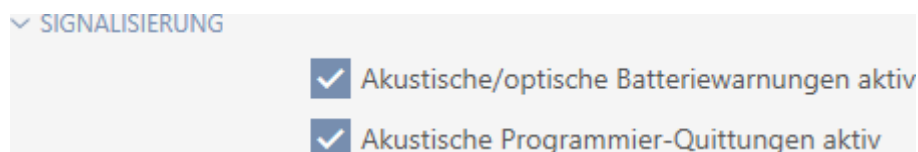
**NOTE**

**Button control not adjustable**

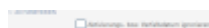
Some locking cylinders are equipped with a button on the inside thumb-turn (TS option). If your AXM Plus detects such a locking cylinder, the  Button control checkbox is displayed. However, this cannot be adjusted, i.e. you cannot disable the buttons.



13. 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)* [▶ 289]).



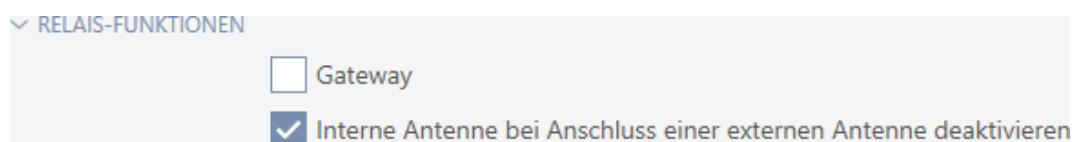
14. If you want to ignore the activation time window (see Activation date / expiry date), expand the "AX functions" menu and configure the settings (see *Ignoring activation and expiry date of identification media* [▶ 293]).



15. If you wish to activate/deactivate the card reader for the locking device: Expand the "Card configuration" menu and make the settings (see *Activating and deactivating card readers* [▶ 291]).

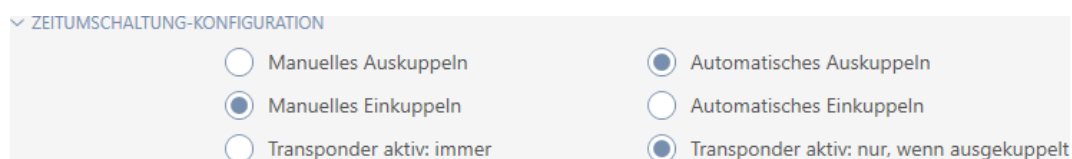


16. If you want to use the internal and external antenna together in a SmartRelay, expand the "Relay functions" menu and configure the settings (see *Using internal and external antenna simultaneously* [▶ 302]).

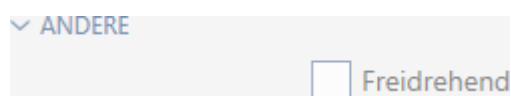


17. If you want to engage and disengage your locking device automatically, expand the "Time switching - Configuration" menu and configure the settings (see *Engaging and disengaging locking devices automatically with time switchover* [▶ 278]).

The setting defined here applies only to this one locking device, not to the entire locking system.



18. 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 Plus 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.

## Schließung - Konfiguration

Bei freidrehendem AX Schließzylinder(FD) werden zwei Schließungen angelegt:  
Eine für den Innenknäuf und eine andere für den Außenknäuf.  
Beide Schließungen müssen separat konfiguriert und programmiert werden!



OK

19. If you want to activate door monitoring for a suitable locking device, expand the "DoorMonitoring" menu and configure the settings (see *Setting up door monitoring (DoorMonitoring)* [▶ 294]).

▼ DOORMONITORING

"TÜR OFFEN" EINSTELLUNGEN	
Abtastintervall für die DM Sensoren (Sek.)	aus
"Tür zu lange offen" Event nach (Min.)	aus

SCHLOSSRIEGEL	
Tourigkeit des Schlosses	aus
"Tür sicher verriegelt" Position des Riegels	aus

PROTOKOLLIERUNG IN DER ZUTRITTSLISTE

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

WEITERLEITUNG IM NETZWERK

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Protokollierung / Weiterleitung der Alarme im Netzwerk

20. 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* [▶ 301]).

▼ ERWEITERTE KONFIGURATION

Nur berechtigte TIDs über serielle Schnittstelle ausgeben

Schnittstelle keine

Schnittstelle: Zusatzsignal CLS

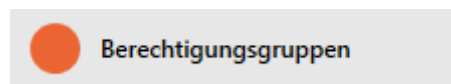
Externe LED  Externer Piepser

SR Signal invertieren

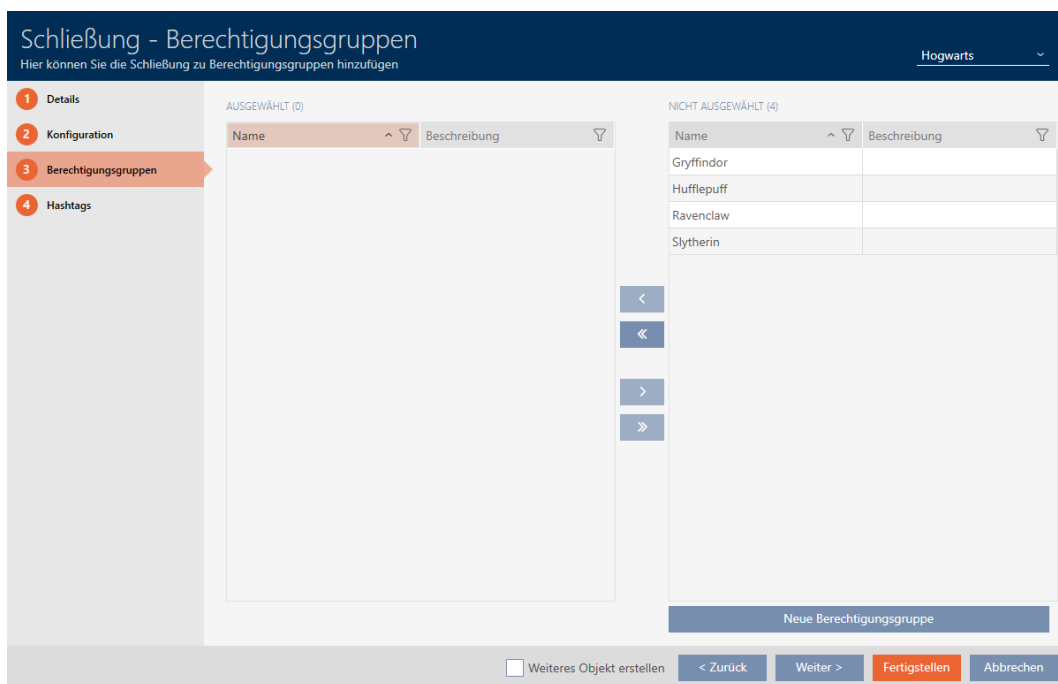
LED ausschalten


Piepser ausschalten

21. Click on the **Access levels** tab.



↳ Window switches to the "Access levels" tab.





22. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
23. Select all authorisation groups to which you wish to assign your locking device (Ctrl+click for individual groups or Shift+click for multiple groups).

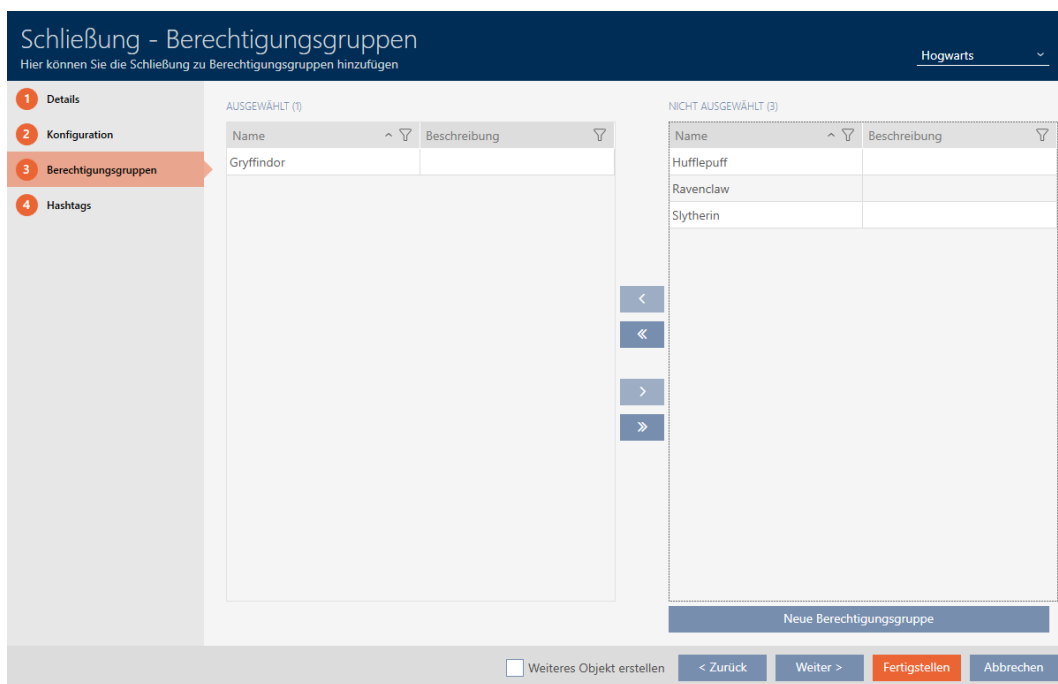


**NOTE**

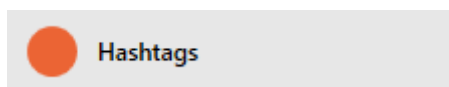
**Double-clicking as an alternative to arrow keys**

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

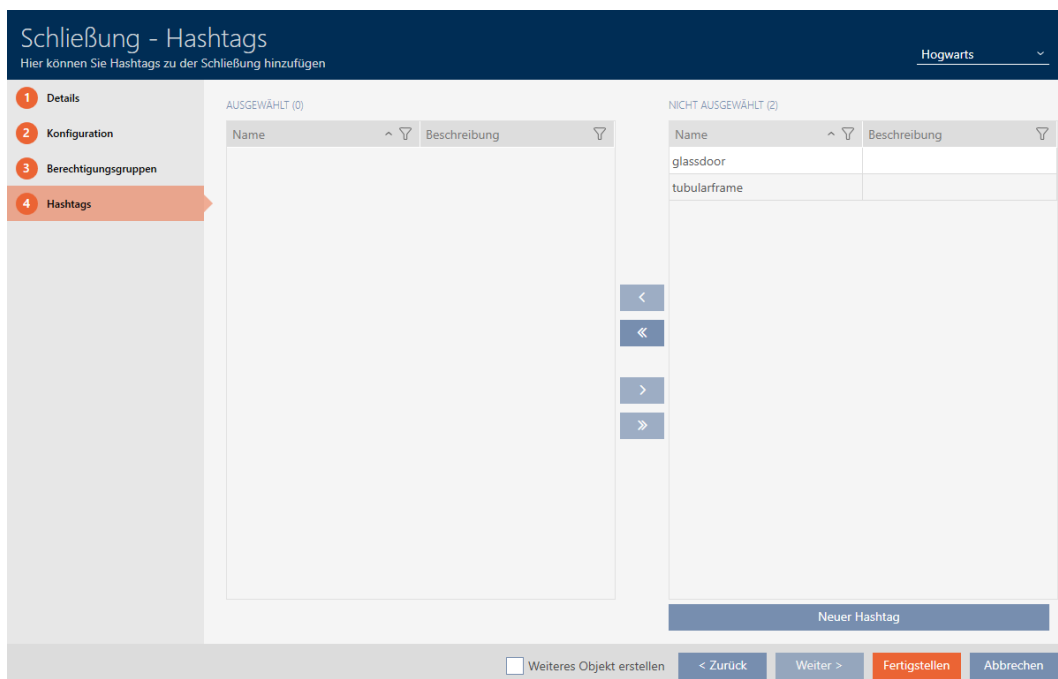
24. Use  to move the selected authorisation groups only or  to move all displayed authorisation groups.
  - ↳ Your locking device is added to the authorisation groups in the left-hand column.




25. Click on the  Hashtags tab.



↳ Window switches to the "Hashtags" tab.



26. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

27. Select all hashtags that you wish to assign to your locking device (Ctrl+click for individual hashtags or Shift+click for multiple hashtags).



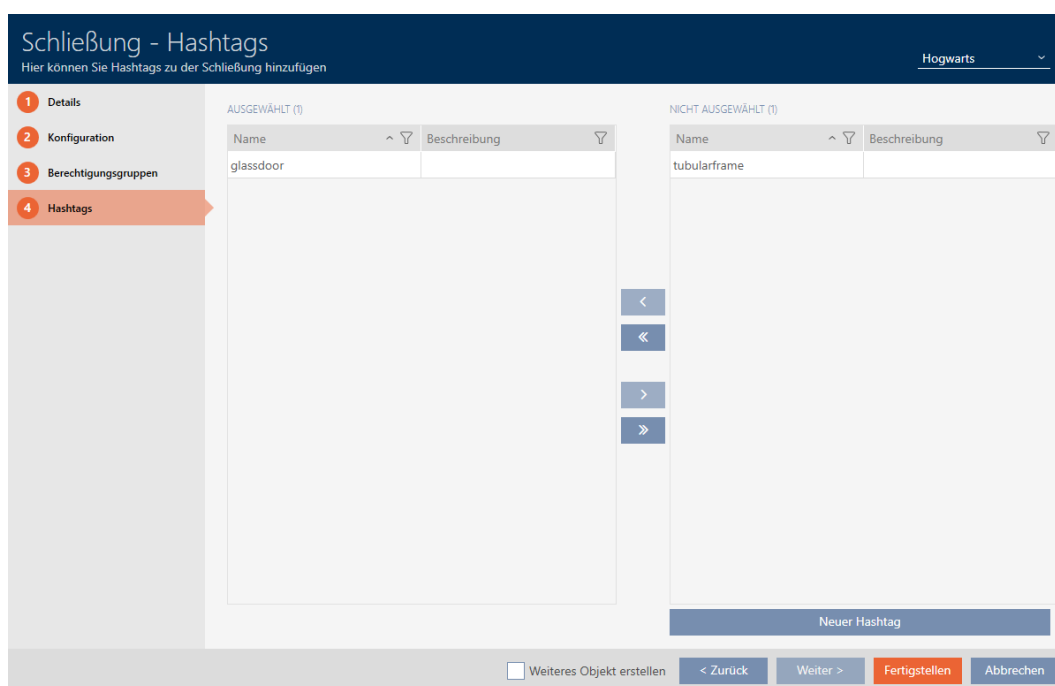
**NOTE**

**Double-clicking as an alternative to arrow keys**

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

28. 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.



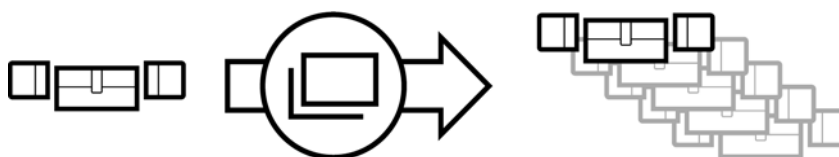
29. Select the  Create additional objects checkbox to leave the window with the same settings open for the next locking device to be created.

30. 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.

**15.2 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 Plus also applies the properties, which can be changed in the AXM Plus.

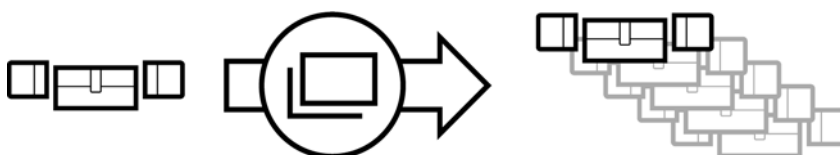
The following settings are duplicated:


- Building details
- Door details (except door numbering, which is automatically continued with the adjustable abbreviation; also see *Changing automatic numbering* [▶ 443])
- Time functions
- Configuration
- Access levels
- Hashtags

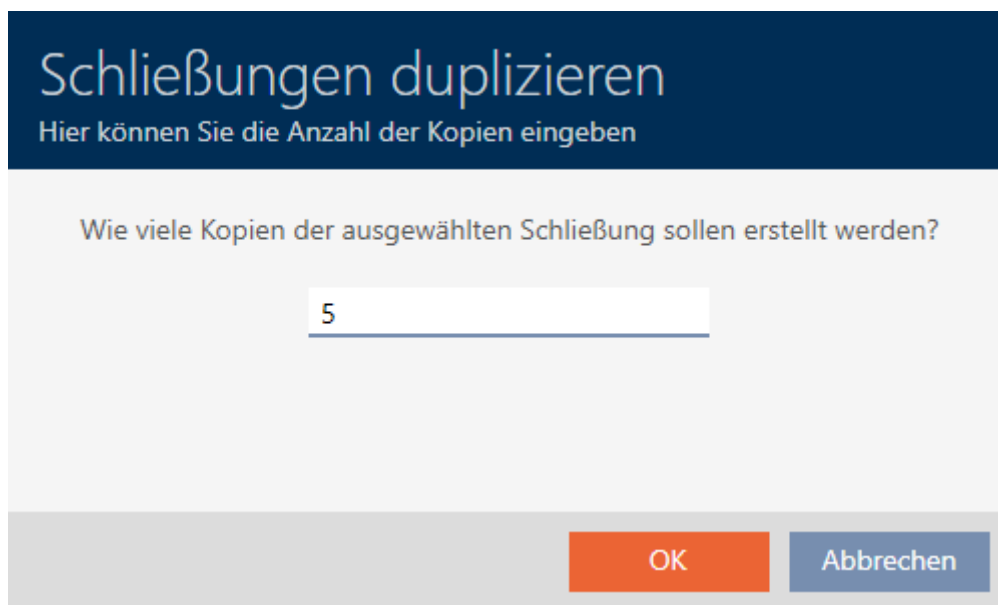
The following settings are not duplicated:

- 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
- ✓ 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.

Person	Typ
Weasley, Ron	☉
Weasley, Fred	☉
Lovegood, Luna	☉
Granger, Hermine	☉

Tür	Typ
Gryffindor dormitory	☉
Hufflepuff dormitory	☉
Gryffindor dormitory_0001	☉
Gryffindor dormitory_0002	☉
Gryffindor dormitory_0003	☉
Gryffindor dormitory_0004	☉
Gryffindor dormitory_0005	☉

▶	▶ X	▶ X
▶	▶ X	▶ X
▶	▶ X	▶ X
▶	▶ X	▶ X
▶	▶ X	▶ X
▶	▶ X	▶ X

### 15.3 Delete locking device

There are two ways to delete locking devices:



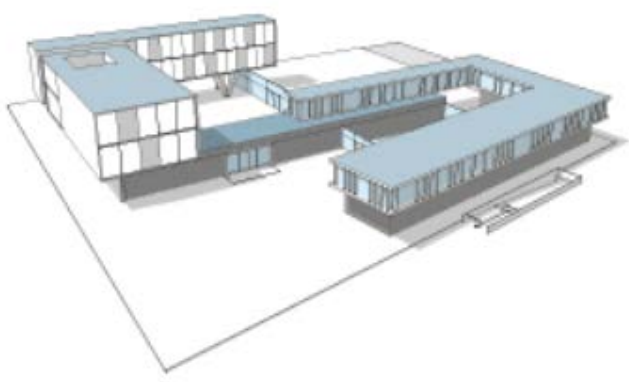
1. Delete on the matrix screen (*Deleting an individual locking device using the matrix [▶ 241]*)
2. Delete using the tab for locking devices (*Deleting several locking devices using the tab [▶ 242]*)

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

### 15.3.1 Deleting an individual locking device using the matrix

✓ Matrix screen open.


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

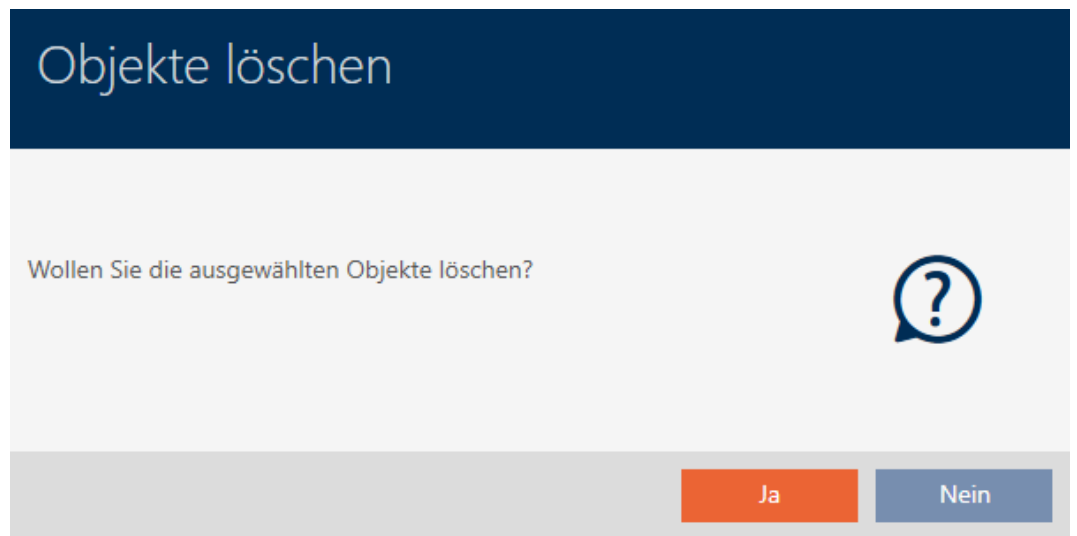


Person	Typ
Weasley, Ron	☹
Weasley, Fred	☹
Lovegood, Luna	☹
Granger, Hermine	☹

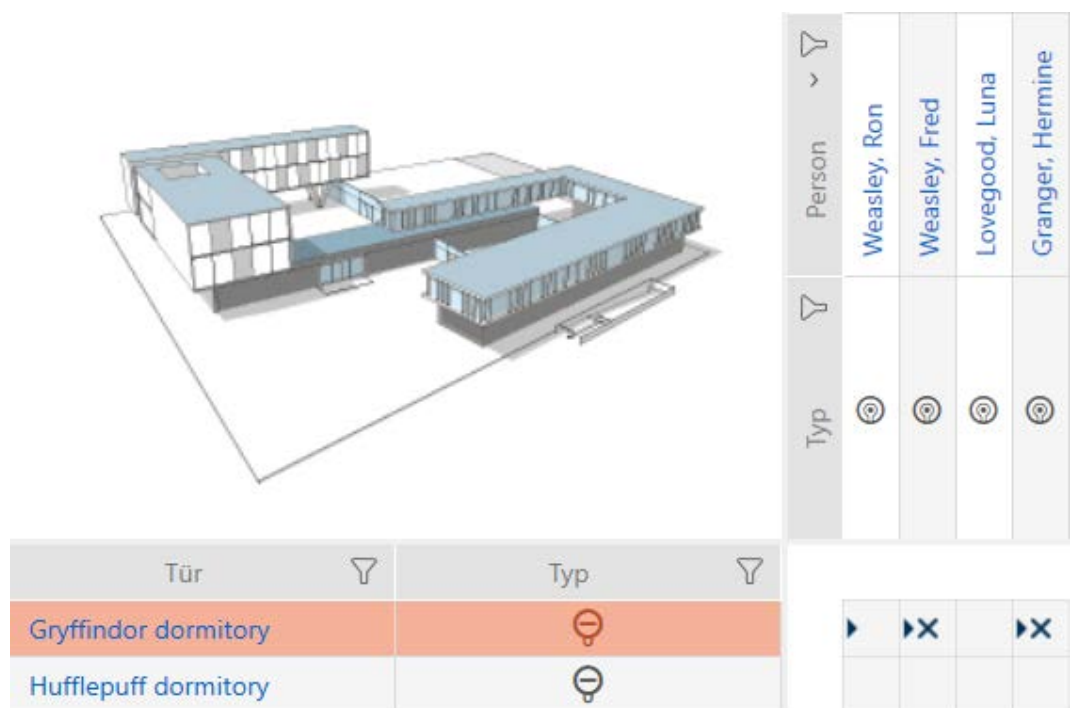
Tür	Typ
Gryffindor dormitory	☹
Hufflepuff dormitory	☹
Gryffindor dormitory_0001	☹

▶	▶X	▶X
▶	▶X	▶X


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



3. Click on the **Yes** button.
  - ↳ Deletion query closes.
  - ↳ Locking device has been deleted.



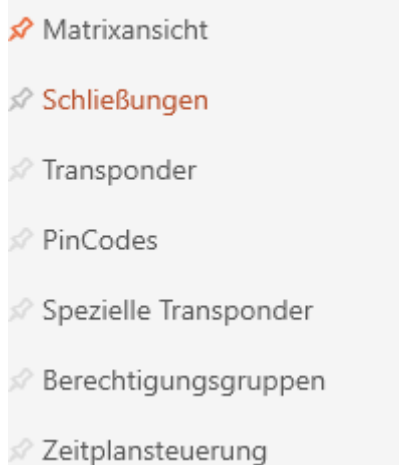
### 15.3.2 Deleting several locking devices using the tab

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



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

SCHLISSANLAGENSTEUERUNG




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

Tür	Raumnummer	Etage	Typ	Sync	Status	Letzte Synchronisierung	S/N	Schließungs ID
Gryffindor dormitory			⊕	↻		13.12.2021 20:32:04	0084GEAD	129
Gryffindor dormitory_0001			⊕	↻				ohne Programmierung
Gryffindor dormitory_0002			⊕	↻				ohne Programmierung
Gryffindor dormitory_0003			⊕	↻				ohne Programmierung
Gryffindor dormitory_0004			⊕	↻				ohne Programmierung
Gryffindor dormitory_0005			⊕	↻				ohne Programmierung
Hagrid's hut			⊕			13.12.2021 20:31:29	000D5P7E	128
Hufflepuff tower			⊕			13.12.2021 20:33:19	000E04GX	10000
Stadium illumination			⊕			13.12.2021 20:34:32	000EN84L	10001

3. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

- Select all locking devices that you wish to delete (Ctrl+click for single media or Shift+click for multiple media).

Tür	Raumnummer	Etage	Typ	Sync	Status	Letzte Synchronisierung	S/N	Schließungs ID
Gryffindor dormitory			🔒	↻		13.12.2021 20:32:04	0084GEAD	129
Gryffindor dormitory_0001			🔒	↻				ohne Programmierung
Gryffindor dormitory_0002			🔒	↻				ohne Programmierung
Gryffindor dormitory_0003			🔒	↻				ohne Programmierung
Gryffindor dormitory_0004			🔒	↻				ohne Programmierung
Gryffindor dormitory_0005			🔒	↻				ohne Programmierung
Hagrid's hut			🔒			13.12.2021 20:31:29	000D5P7E	128
Hufflepuff tower			🔒			13.12.2021 20:33:19	000E04GX	10000
Stadium illumination			🔒			13.12.2021 20:34:32	000EN84L	10001

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

- Click on the Yes button.
  - Query with list of locking devices to be deleted closes.
  - Locking devices have been deleted.

Tür	Raumnummer	Etage	Typ	Sync	Status	Letzte Synchronisierung	S/N	Schließungs ID
Gryffindor dormitory			🔒	↻		13.12.2021 20:32:04	0084GEAD	129
Hagrid's hut			🔒			13.12.2021 20:31:29	000D5P7E	128
Hufflepuff tower			🔒			13.12.2021 20:33:19	000E04GX	10000
Stadium illumination			🔒			13.12.2021 20:34:32	000EN84L	10001

### 15.4 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 Plus 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. <i>Open time (sec)</i> )	Adjustable	Adjustable	Is applied
Setting B (e.g. <input checked="" type="checkbox"/> <i>Invert SR signal</i> )	Adjustable	Not adjustable	Expires
Setting C	Not adjustable	Adjustable	Set to default value

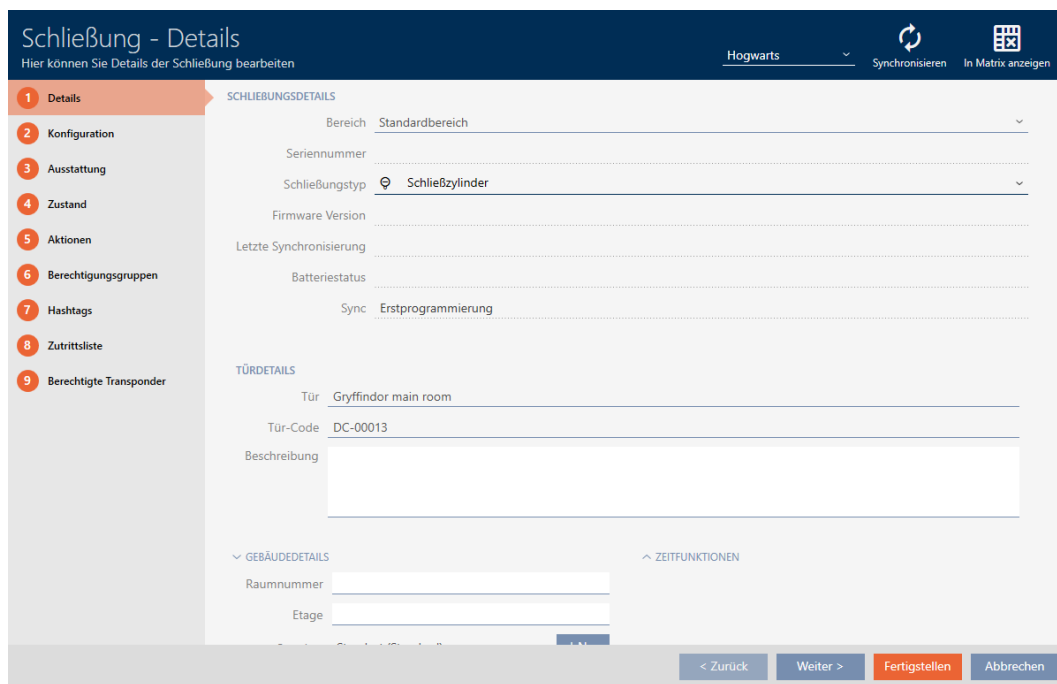
Tür	Typ	Sync
Castle		
Gryffindor tower	🔑	
Standardbereich		
Gryffindor dormit...	🔑	
Gryffindor main ro...	🔑	↻
Main gate	🔑	
Quidditch field	🔑	↻
Snape's dungeon	🔑	

Tür	Typ	Sync
Castle		
Gryffindor tower	🔑	
Standardbereich		
Gryffindor dormit...	🔑	
Gryffindor main ro...	🔑	↻
Main gate	🔑	
Quidditch field	🔑	↻
Snape's dungeon	🔑	

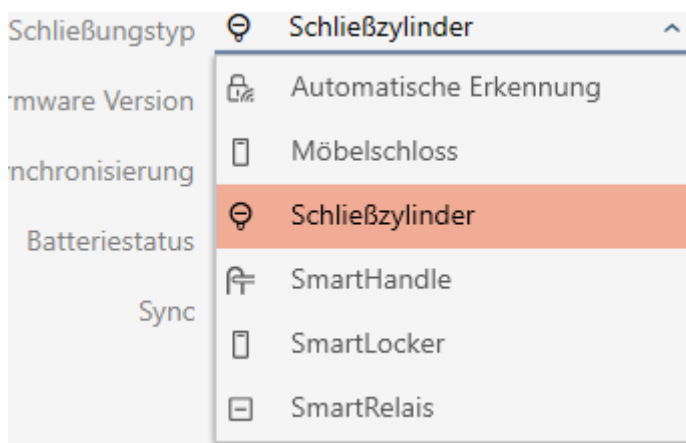
The locking device type can only be changed for non-synchronised locking devices.

- ✓ Locking device list or matrix view open.
- ✓ Locking device available.
- ✓ Locking device not synchronised (if necessary reset, see *Re-setting the locking device* [▶ 408]).

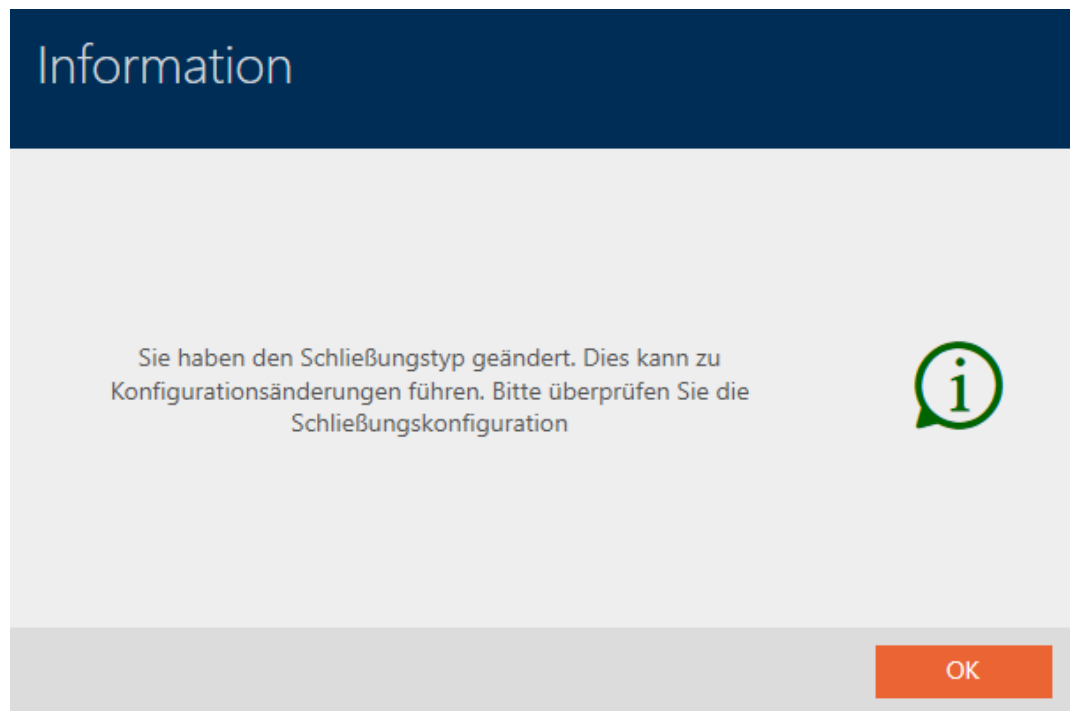
1. Click on the locking device whose type you wish to change.
  - ↳ The locking device window will open.



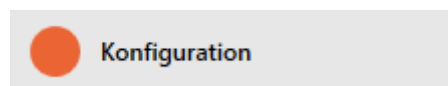
2. Select the new locking device type from the ▼ Lock type drop-down menu.



- ↳ Warning about the configuration change will open.



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



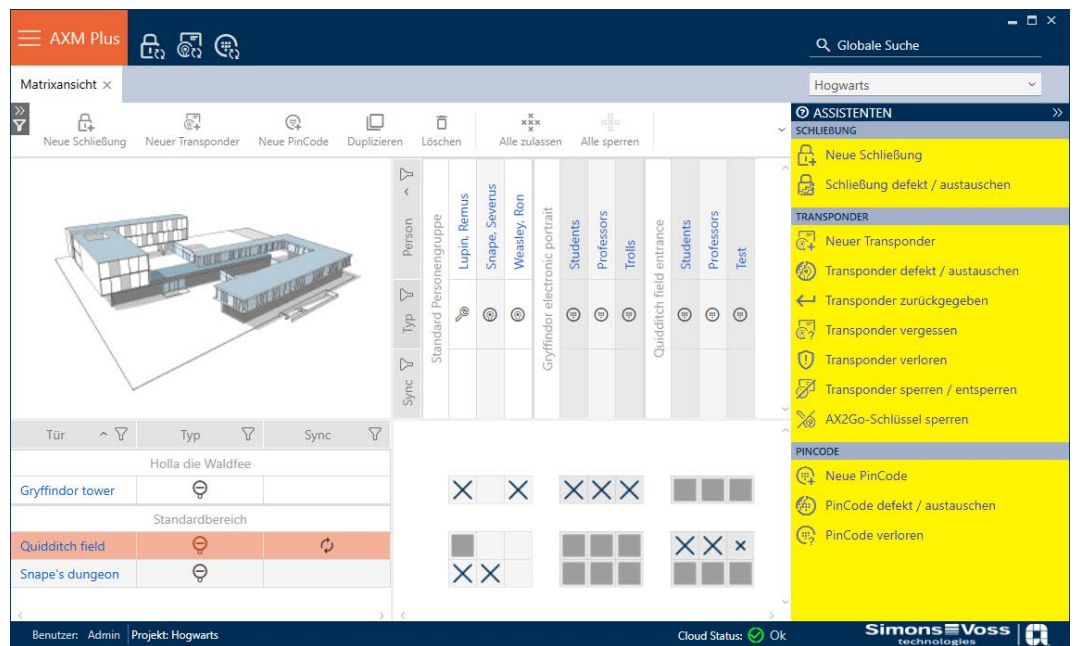
- ↳ Window switches to the "Configuration" tab.
5. Check and change the configuration if necessary.
6. Click on the **Finish** button.
  - ↳ The locking device window closes.
- ↳ Locking device type has been changed.

## 15.5 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 Plus 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 [► 512]*



Locking device is required again immediately:

### Schließung defekt / austauschen - Assistent

Schließanlage ▼ **Hogwarts**

Schließung ▼ **Gryffindor dormitory (00AXNNH)**

Programmiergerät ▼ **SmartCD aktiv**

**AKTION WÄHLEN**

**Schließung, instand setzen**

Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

**Schließung austauschen**

Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.

**Schließung zurücksetzen / bereinigen**

Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter
Schließen

Suitable for:

Repair	Resetting and replacing	Delete and replace
Locking devices with an un-defined software status	<ul style="list-style-type: none"> <li>■ Locking devices with external damage (e.g. scratched).</li> <li>■ Locking devices that should be replaced as a precaution (e.g. if they get wet).</li> </ul>	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
<p><i>Re-synchronise (repair)</i> [▶ 252]</p> <ol style="list-style-type: none"> <li>Reset (= LID available in database again)</li> <li>Resynchronise (= LID is immediately written back onto the same locking device)</li> </ol> <p>The locking device works the same as before after repair.</p>	<p><i>Resetting and replacing</i> [▶ 254]</p> <ol style="list-style-type: none"> <li>Reset (= LID flagged as defective in database and removed from original locking device)</li> <li>Synchronise replacement locking device with new LID</li> </ol> <p>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.</p> <p>The previous locking device remains in the database with its LID and is flagged as defective.</p>	<p><i>Delete and replace</i> [▶ 259]</p> <ol style="list-style-type: none"> <li>Synchronise replacement locking device with new LID</li> <li>Delete defective locking device</li> </ol> <p>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.</p>

Locking device is not required again immediately:

### Schließung defekt / austauschen - Assistent

Schließanlage ▼ **Hogwarts**

---

Schließung ▼ Gryffindor dormitory (00AXNNH)

---

Programmiergerät ▼ SmartCD aktiv

---

**AKTION WÄHLEN**

Schließung instand setzen  
 Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
 Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.

Schließung zurücksetzen / bereinigen  
 Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter
Schließen

Suitable for:

Reset	Purge (software reset)
<ul style="list-style-type: none"> <li><span style="color: red;">■</span> Locking devices with external damage (e.g. scratched).</li> <li><span style="color: red;">■</span> Locking devices that should be replaced as a precaution (e.g. if they get wet).</li> </ul>	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)
<p><i>Reset [▶ 264]</i></p> <p>Resetting removes the LID from the locking device.</p> <p>You can synchronise another locking device with this entry later, which will receive the same LID.</p>	<p><i>Purge (only reset in database/software reset) [▶ 266]</i></p> <p>The clean-up only affects the database in your AXM Plus. 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.</p> <p>The LID is separated from the LID for the locking device previously used during the clean-up in the database (in current state).</p> <p>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 Plus 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 <i>Re-setting the locking device [▶ 408]</i>). This deletes the LID from the old locking device and prevents the same LID from being in circulation twice.</p>




**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.

**15.5.1 Re-synchronise (repair)**


- ✓ 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 [▶ 44]*).
  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.

### Schließung defekt / austauschen - Assistent

Schließanlage **Hogwarts** ▾

Schließung **Gryffindor dormitory (00AXNNH)** ▾

Programmiergerät  SmartCD aktiv ▾

**AKTION WÄHLEN**

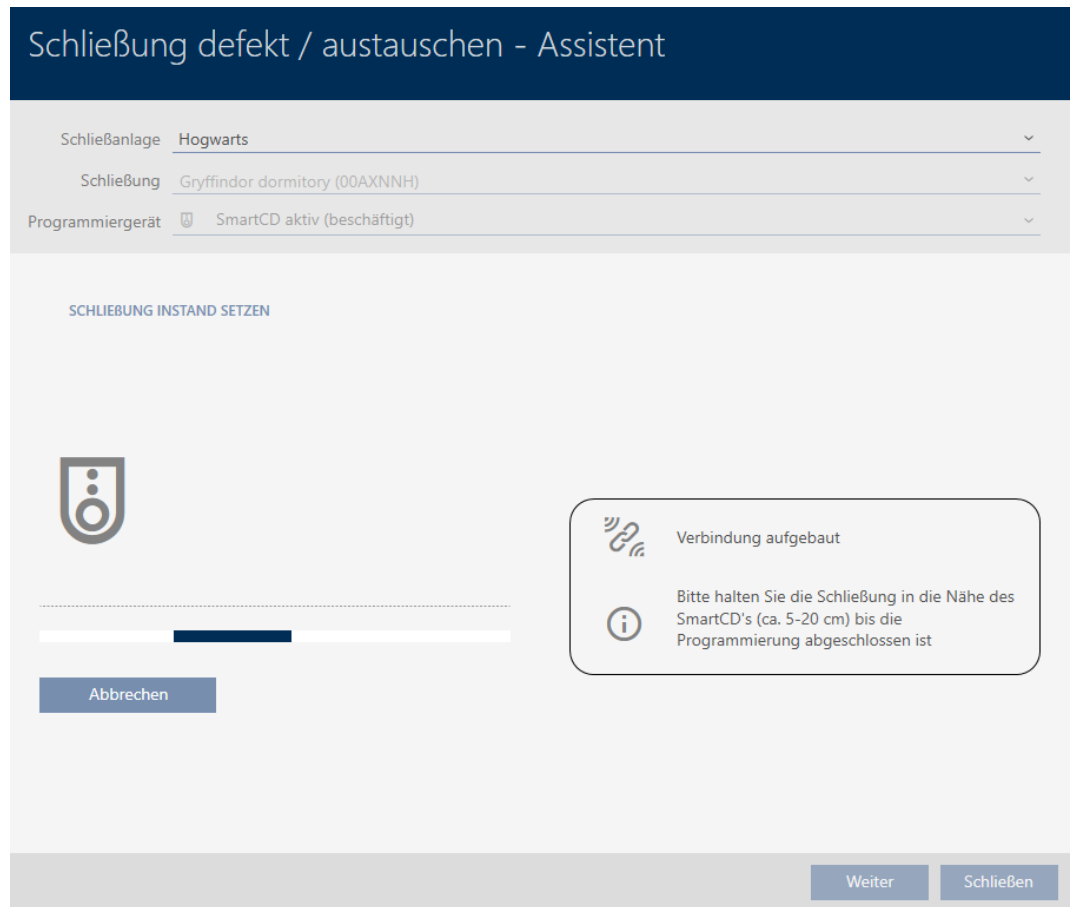
Schließung instand setzen  
Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.

Schließung zurücksetzen / bereinigen  
Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

**Weiter** **Schließen**



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



↳ Locking device is resynchronised.

**SCHLIEßUNG INSTAND SETZEN**  
 Schließung erfolgreich instand gesetzt.

### 15.5.2 Resetting and replacing

- ✓ 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* [▶ 44]).
  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.

## Schließung defekt / austauschen - Assistent

Schließanlage **Hogwarts** ▾

Schließung **Gryffindor dormitory (00AXNNH)** ▾

Programmiergerät **SmartCD aktiv** ▾

**AKTION WÄHLEN**

Schließung instand setzen  
Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.


Schließung zurücksetzen / bereinigen  
Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter Schließen

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

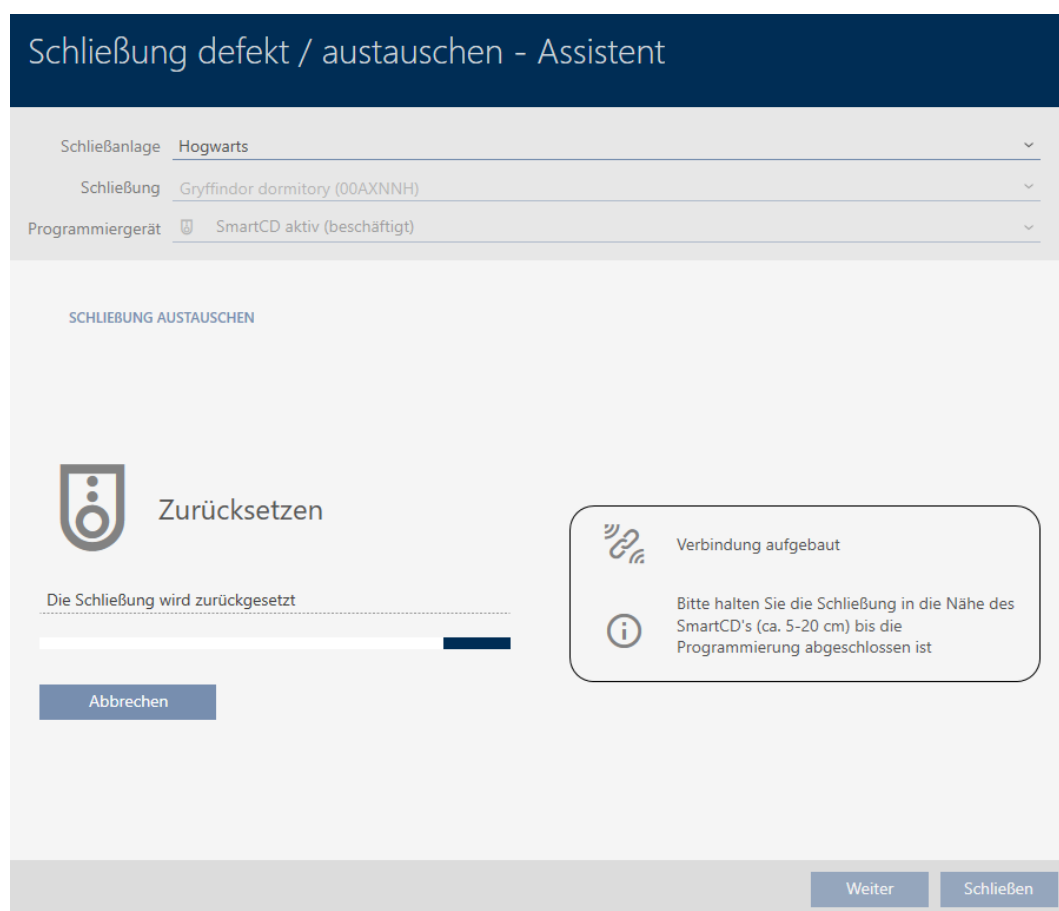
## Schließung defekt / austauschen

Schließung zurücksetzen?



Ja Nein

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.



## Schließung austauschen

Möchten Sie eine Ersatzschließung erstellen?

- Wenn Sie "Ja" betätigen, wird eine Kopie der vorhandenen Schließung erstellt und zum Programmieren einer Ersatzschließung verwendet
- Wenn Sie "Nein" betätigen, wird der vorhandene Schließungsdatensatz zum Programmieren einer Ersatzschließung verwendet


Name der Kopie Gryffindor dormitory\_1

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.

Tür	Typ	Sync
Castle		
Gryffindor tower	🔒	
Standardbereich		
Gryffindor dormit..	🔒	↻
Gryffindor dormit..	🔒	↻

- ↳ Wizard prepares synchronisation for the replacement locking device.

## Schließung defekt / austauschen - Assistent

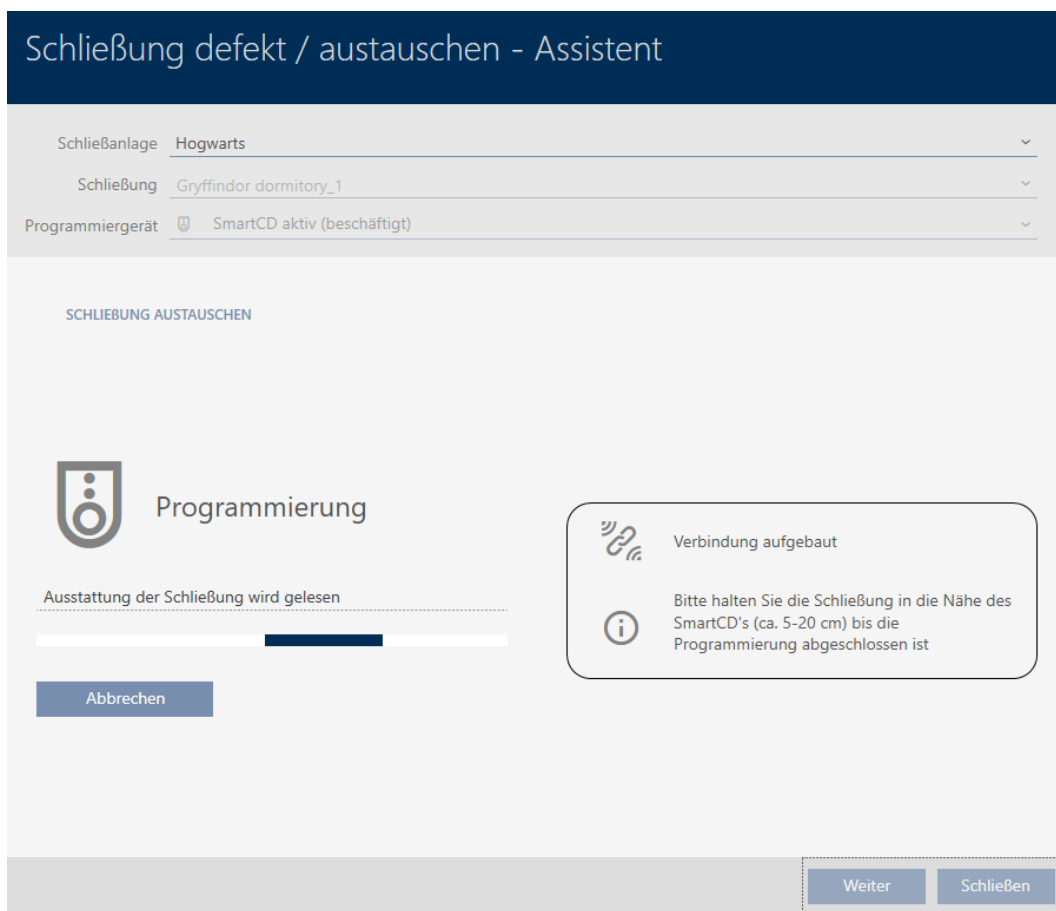
Schließanlage	Hogwarts	▼
Schließung	Gryffindor dormitory_1	▼
Programmiergerät	 SmartCD aktiv	▼

**SCHLIEBUNG AUSTAUSCHEN**

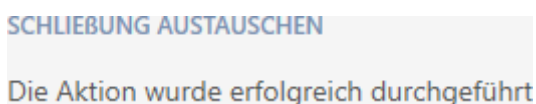
Legen Sie die Ersatzschließung vor das Programmiergerät und klicken Sie auf die "Weiter" Taste.

[Weiter](#) [Schließen](#)

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.

Tür	Typ	Sync
Gryffindor dormitory	⊖	
Hufflepuff dormitory	⊖	↻
Stadium illumination	⊖	↻
Gryffindor dormitory_1	⊖	


### 15.5.3 Delete and replace

- ✓ 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* [▶ 44]).

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.

### Schließung defekt / austauschen - Assistent

Schließanlage	Hogwarts	▼
Schließung	Gryffindor dormitory (00AXNNH)	▼
Programmiergerät	 SmartCD aktiv	▼

**AKTION WÄHLEN**

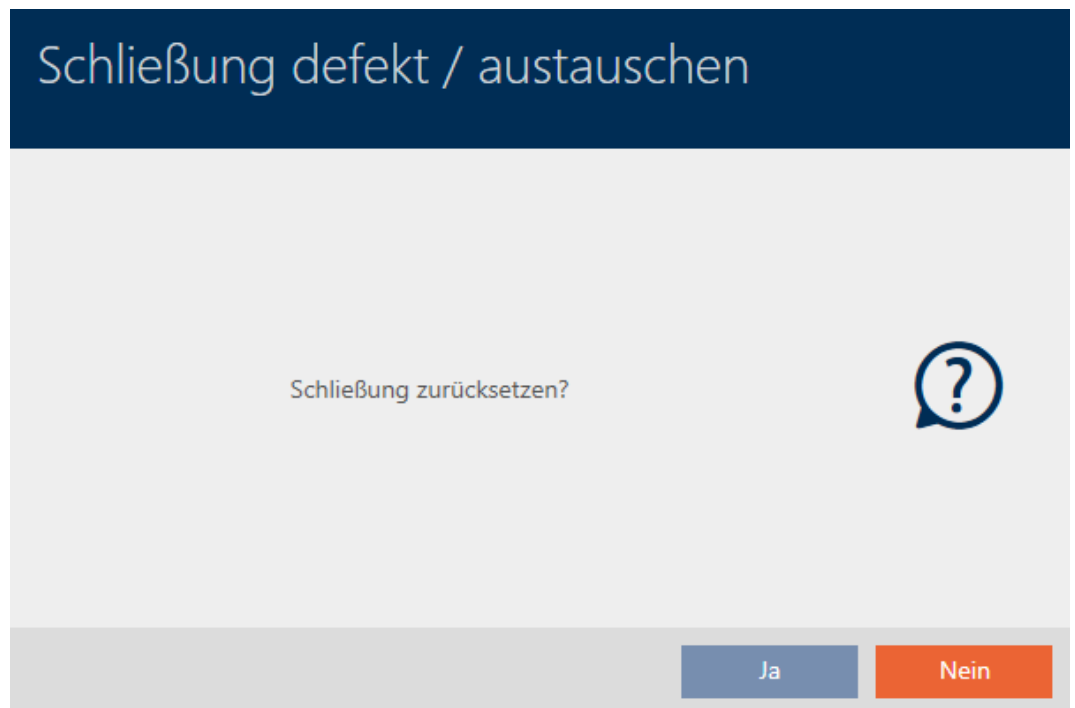
Schließung instand setzen  
Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.

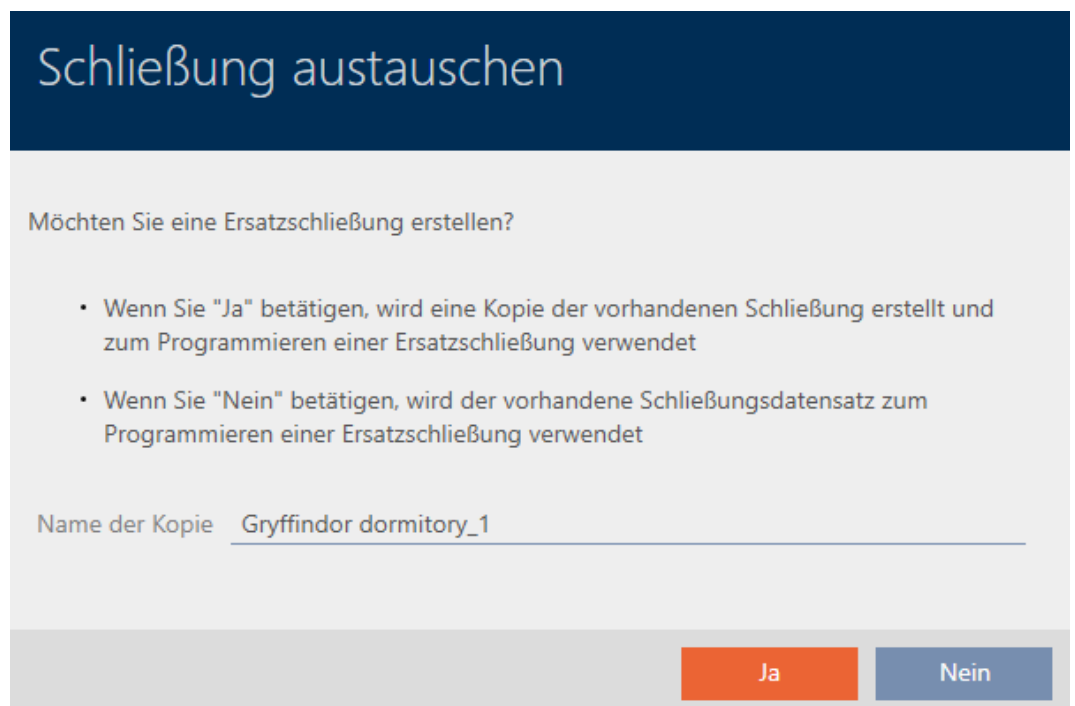
Schließung zurücksetzen / bereinigen  
Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter Schließen

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.

Tür	Typ	Sync
Castle		
Gryffindor tower	🔒	
Standardbereich		
Gryffindor dormit...	🔒	🔄
Gryffindor dormit...	🔒	🔄
Main gate	🔒	
Quidditch field	🔒	🔄
Snape's dungeon	🔒	

- ↳ Wizard prepares synchronisation for the replacement locking device.

### Schließung defekt / austauschen - Assistent

Schließanlage	Hogwarts	▼
Schließung	Gryffindor dormitory_1	▼
Programmiergerät	🔒 SmartCD aktiv	▼

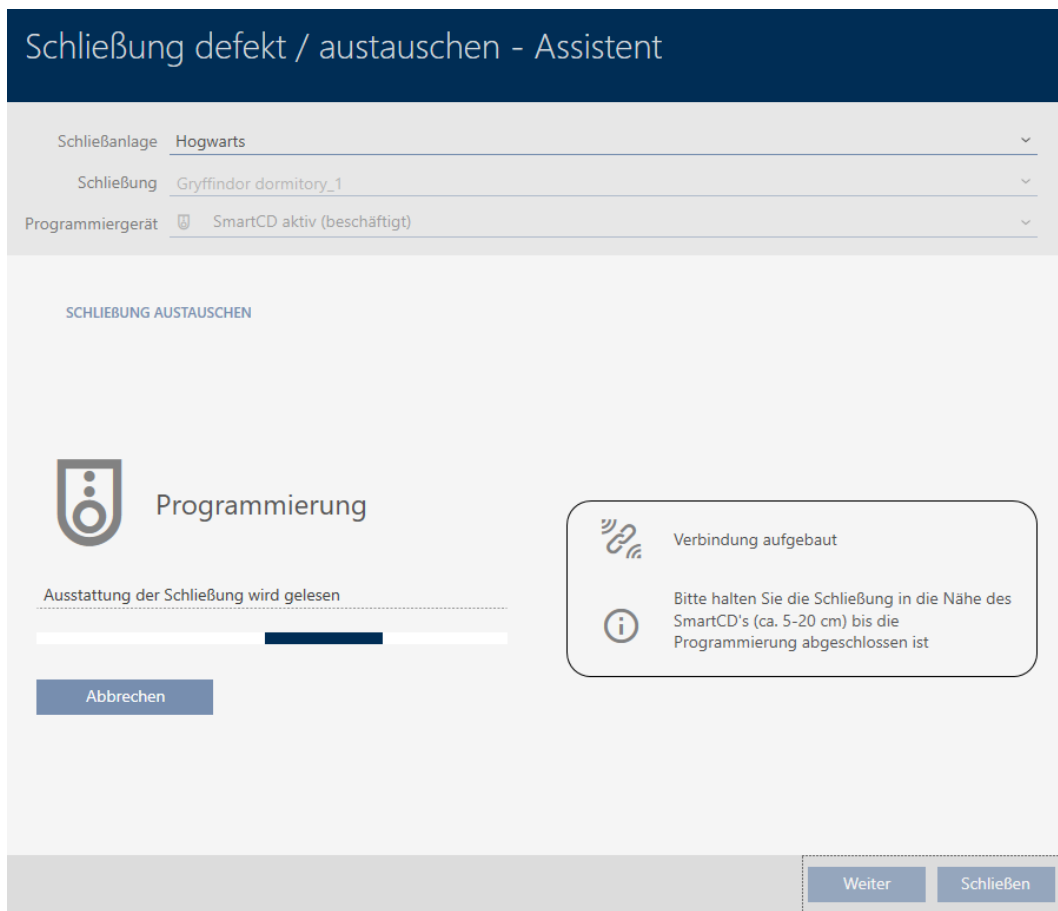
**SCHLIEßUNG AUSTAUSCHEN**

Legen Sie die Ersatzschließung vor das Programmiergerät und klicken Sie auf die "Weiter" Taste.

Weiter
Schließen

- Click on the **Next** button.

- ↳ Replacement locking device is being synchronised.



↳ Replacement locking device is synchronised.

**SCHLIEBUNG AUSTAUSCHEN**  
 Die Aktion wurde erfolgreich durchgeführt







10. Click on the **Close** button.

↳ Wizard for dealing with a faulty locking device closes.



11. Select the defective original locking device.

Tür	Typ	Sync
Castle		
Gryffindor tower		
Standardbereich		
Gryffindor dormit...		
Gryffindor dormit...		
Main gate		
Quidditch field		
Snape's dungeon		

12. Click on the **Delete** button .
  - ↳ Defective locking device is deleted from the locking plan.
  - ↳ Replacement locking device is displayed in the matrix.

Tür	^	▼	Typ	▼	Sync	▼
Castle						
Gryffindor tower						
Standardbereich						
Gryffindor dormit...						
Main gate						
Quidditch field						
Snape's dungeon						

#### 15.5.4 Reset

- ✓ 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* [▶ 44]).
  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.



## Schließung defekt / austauschen - Assistent

Schließanlage **Hogwarts** ▾

Schließung **Gryffindor dormitory (00AXNNH)** ▾

Programmiergerät **SmartCD aktiv** ▾

**AKTION WÄHLEN**

Schließung instand setzen  
Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.


Schließung zurücksetzen / bereinigen  
Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter Schließen

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

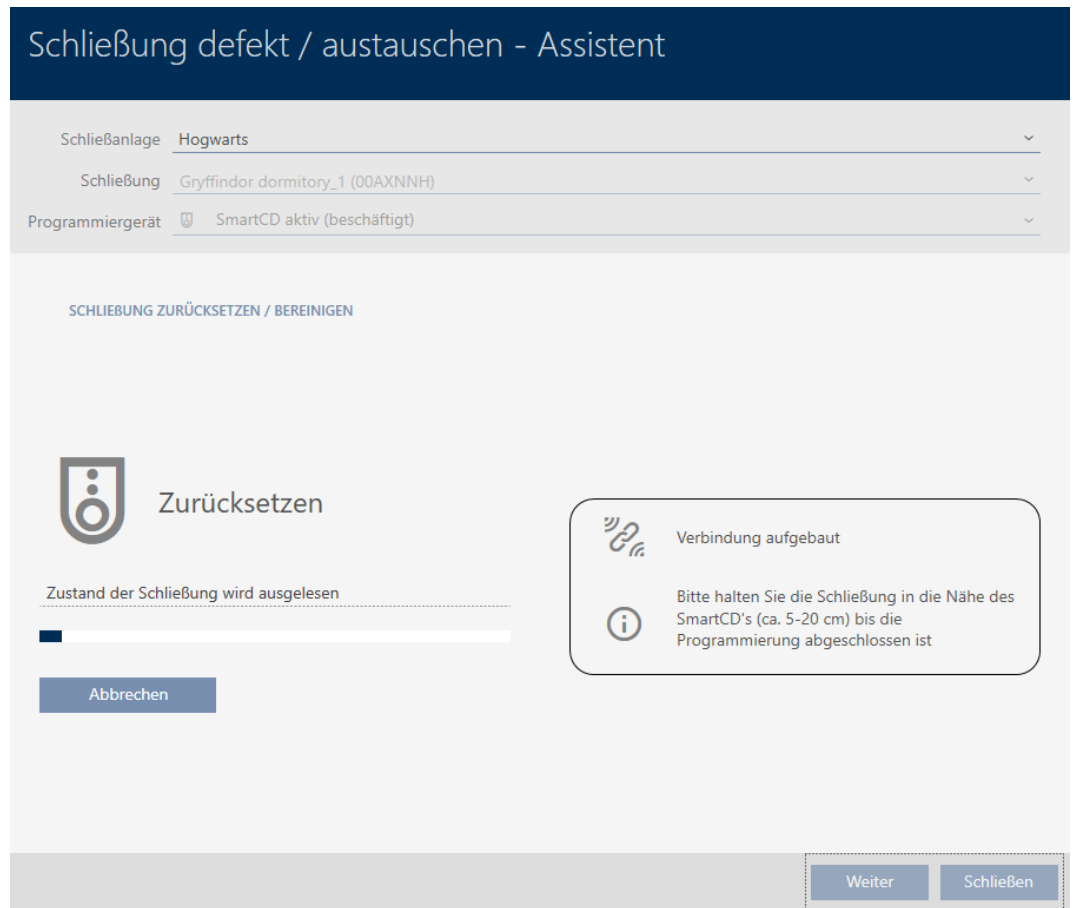
## Schließung defekt / austauschen

Schließung zurücksetzen?



Ja Nein



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



- ↳ Locking device is reset.

SCHLIEBUNG ZURÜCKSETZEN / BEREINIGEN  
 Schließung erfolgreich zurückgesetzt

### 15.5.5 Purge (only reset in database/software reset)

- ✓ Locking device list or matrix view open.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
  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.

## Schließung defekt / austauschen - Assistent

Schließanlage **Hogwarts** ▾

Schließung **Gryffindor dormitory (00AXNNH)** ▾

Programmiergerät **SmartCD aktiv** ▾

**AKTION WÄHLEN**

Schließung instand setzen  
Die bestehende Schließung wird zurückgesetzt und neu programmiert. Bitte achten Sie darauf, dass dieser Prozess nicht unterbrochen wird.

Schließung austauschen  
Die bestehende Schließung wird gegen eine andere Komponente ausgetauscht. Halten Sie eine passende nicht programmierte Ersatzschließung bereit.


Schließung zurücksetzen / bereinigen  
Die Schließung wird zurückgesetzt oder bereinigt, damit an dieser Stelle eine andere Schließung programmiert werden kann.

Weiter Schließen

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

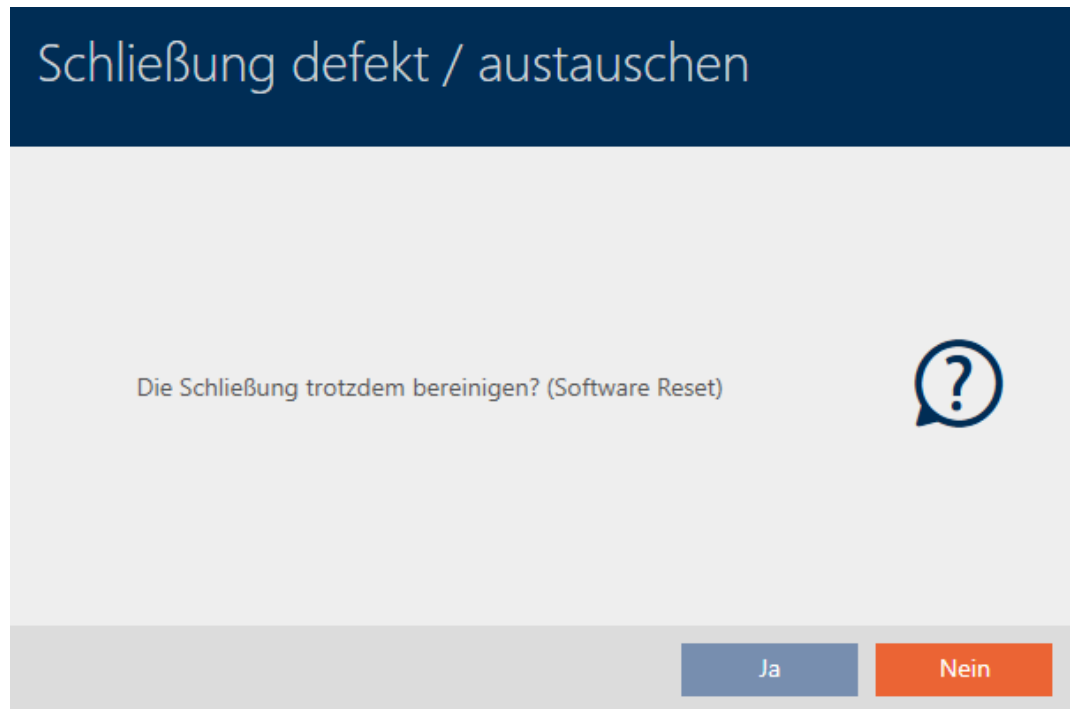
## Schließung defekt / austauschen

Schließung zurücksetzen?



Ja Nein

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.

#### SCHLIEßUNG ZURÜCKSETZEN / BEREINIGEN

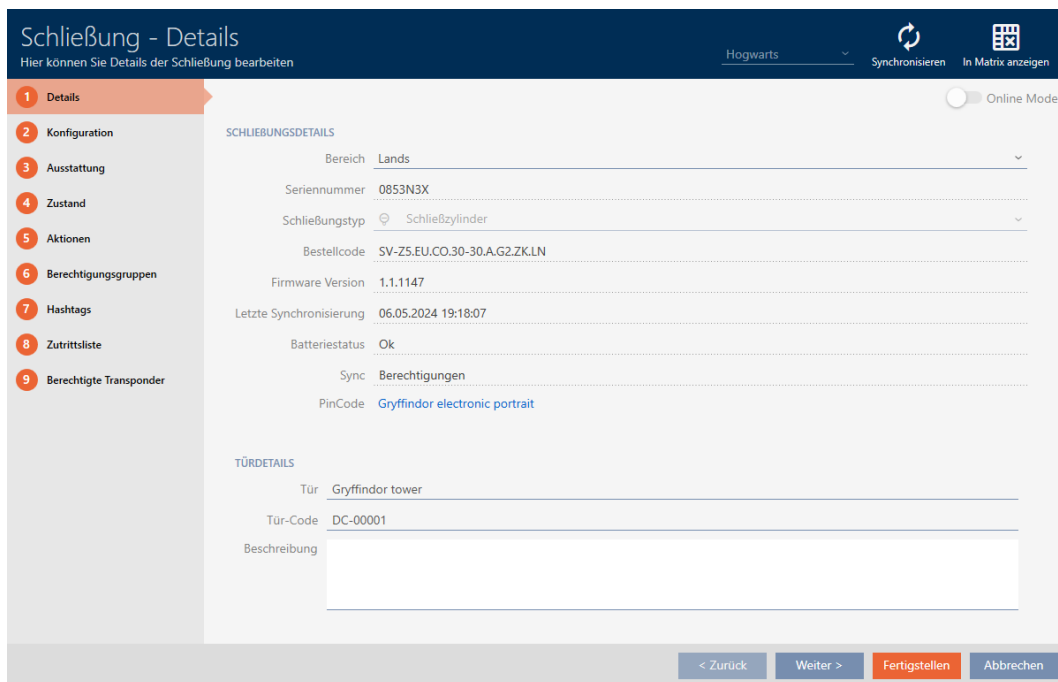
Schließung erfolgreich bereinigt.

## 15.6 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* [▶ 27]) and plan everything out in preparation before creating your locking devices (see *Organisational structure* [▶ 50]). 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:

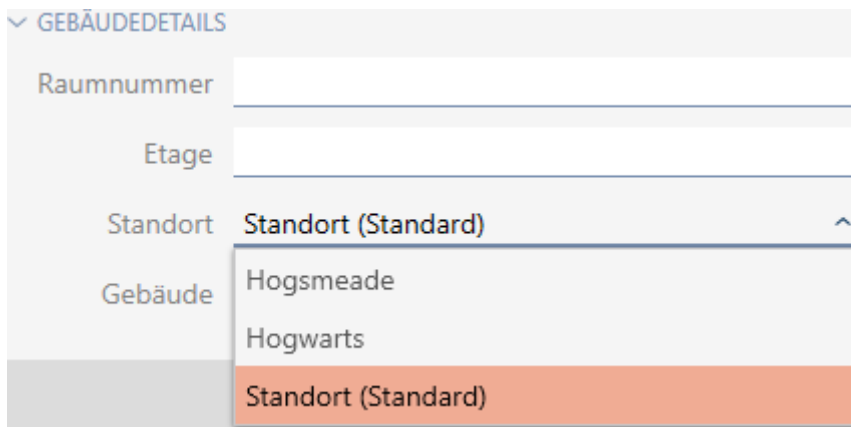
- ✓ At least one location created (see *Creating a location* [▶ 77]).
  - ✓ At least one building created (see *Creating a building and assigning it to a location* [▶ 80]).
1. Click on the locking device you wish to assign to a location and a building.
    - ↳ The locking device window will open.



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



3. Select the location where your locking device will be used from the ▼ Locationdrop-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**

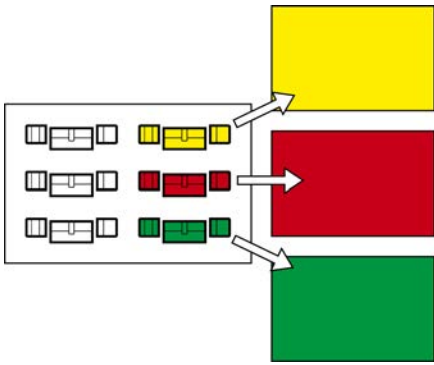
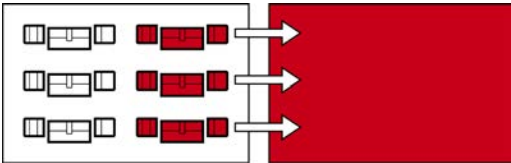
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

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.

**15.7 Moving locking devices to areas**

As soon as you create a locking device, you must specify an area. Ideally, you should follow best practice (see *Best practice: setting up the locking system* [▶ 27]) and plan everything out in advance before creating your locking devices (see *Organisational structure* [▶ 50]). This means that you only need to open windows once.

Obviously, you can also move your locking devices to another area at a later date.

Moving individual locking devices	Moving multiple locking devices
<p><i>Assigning individual locking devices to a different area (in the locking device window) [▶ 271]</i></p> <p>Suitable for moving a few locking devices into many different areas:</p> 	<p><i>Assign multiple locking devices to another area (in the area window) [▶ 273]</i></p> <p>Suitable for moving multiple locking devices into a few different areas:</p> 



**NOTE**

**Maximum one area per locking device**

A locking device can only belong to one single area. There are no overlapping areas in the AXM Plus . If you assign a different area to a locking device, this locking device may be automatically removed from its existing area.

- You can use the Area - Details column in the "Area - Details" window to check whether a locking device has already been assigned to an area.

**Areas have no influence on authorisations**

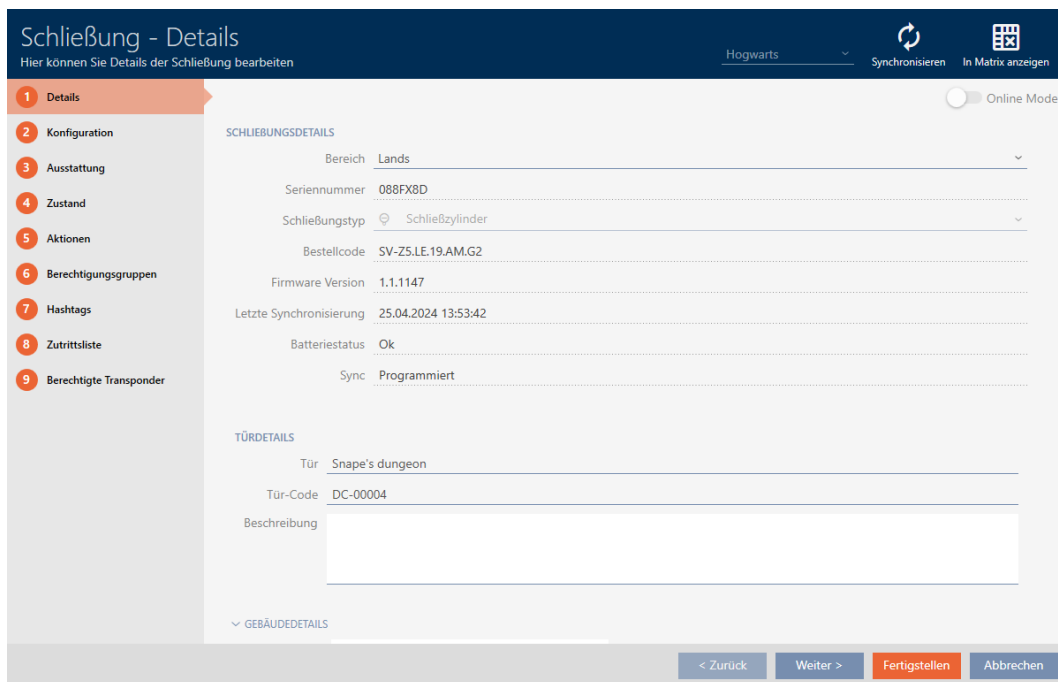
Authorisations are not directly linked to areas. Consequently, if a locking device is moved to a different area, the change does not affect authorisations initially. However, areas are a useful tool for changing authorisations more quickly.

- Use areas to add locking devices to authorisation groups more quickly (see *Adding areas and person groups to authorisation groups* [▶ 331]).

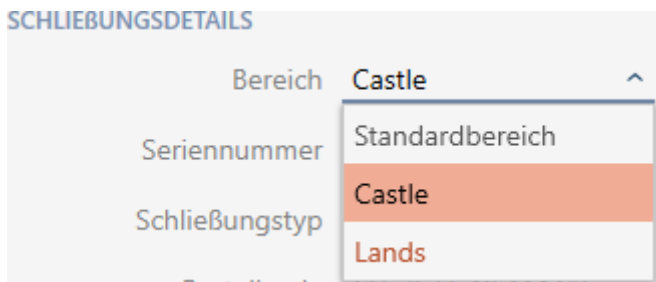
**15.7.1 Assigning individual locking devices to a different area (in the locking device window)**

Locking device in the “old” area				Locking device in the “new” area			
Tür	^	Typ	Sync	Tür	^	Typ	Sync
Castle				Castle			
Gryffindor dormit...		🔒		Gryffindor dormit...		🔒	
Gryffindor tower		🔒		Gryffindor tower		🔒	
Lands				Lands			
Main gate		🔒		Main gate		🔒	
Quidditch field		🔒	🔄	Quidditch field		🔒	🔄
Snape's dungeon		🔒		Snape's dungeon		🔒	

- ✓ At least one area created (see *Creating an area* [▶ 83]).
1. Click on the locking device you wish to move to another area.
    - ↳ The locking device window will open.



2. In the ▼ Area drop-down menu, select the area to which you wish to move the locking device.



3. Click on the **Finish** button.
  - ↳ The locking device window closes.
  - ↳ The locking device is in the new area.

Tür	Typ	Sync
Castle		
Gryffindor dormit...	🔒	
Gryffindor tower	🔒	
Snape's dungeon	🔒	
Lands		
Main gate	🔒	
Quidditch field	🔒	🔄





**NOTE**

**Schedules in locking devices and areas**

You can assign schedules both to a locking device and to the locking device area. In this case, the schedule is used in the locking device and the schedule for the area is ignored.

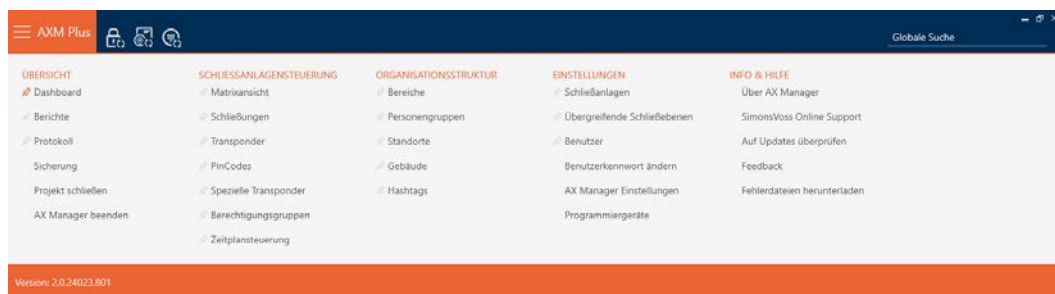
If a schedule is assigned to an area instead of the locking device, the schedule for the area is adopted for the locking device. The suffix "(inherited)" in the locking device window indicates that this is the case.

**15.7.2 Assign multiple locking devices to another area (in the area window)**

Locking device in the "old" area	Locking device in the "new" area

✓ At least one area created (see *Creating an area* [▶ 83]).

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

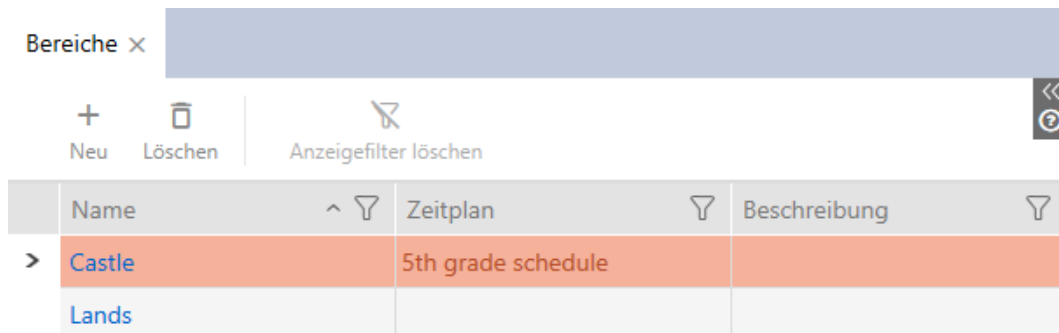


2. Select the **Areas** entry in the | ORGANISATIONAL STRUCTURE | group.

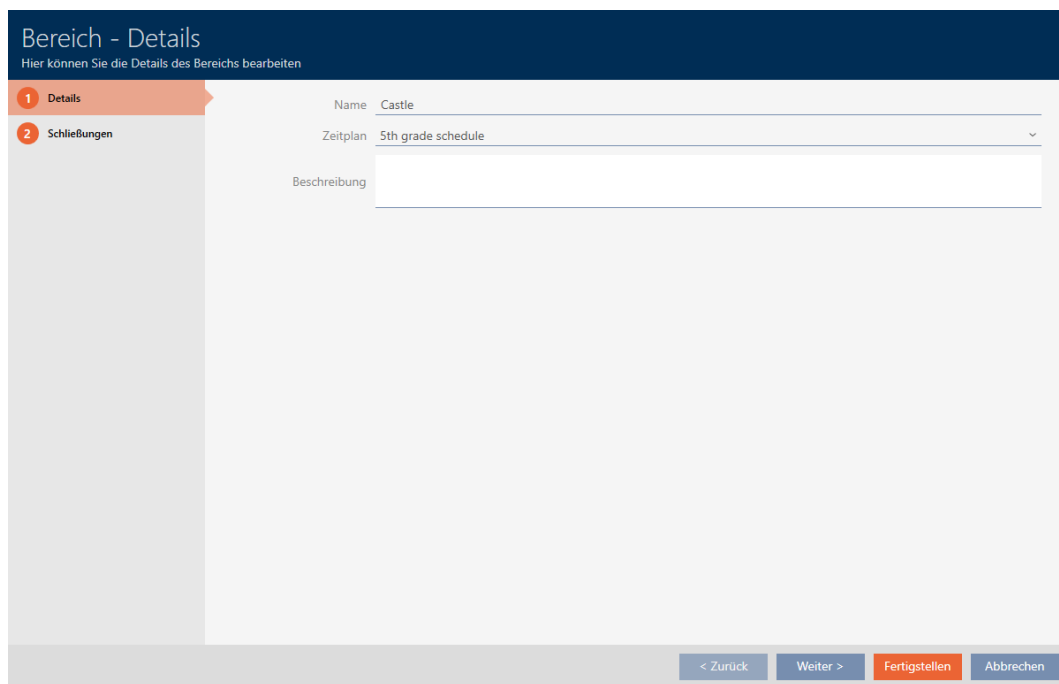
**ORGANISATIONSTRUKTUR**

- Bereiche
- Personengruppen
- Standorte
- Gebäude
- Hashtags

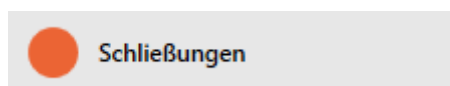
- ↳ The AXM bar will close.
- ↳ The [Areas] tab will open.



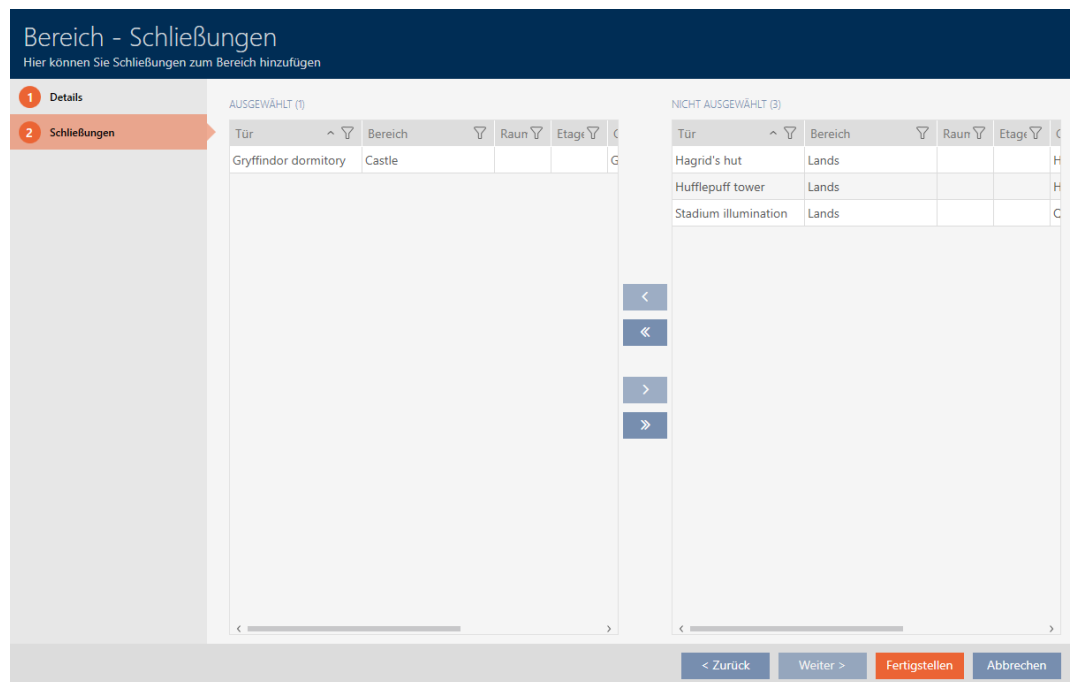
3. Click on the area to which you wish to move the locking devices.
  - ↳ The "Area" window will open.






4. Click on the **Schließungen** tab.



- ↳ Window switches to the "Locks" tab.



5. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
6. Select all locking devices that you wish to add (Ctrl + mouse click for individual devices or Shift + mouse click for multiple devices).
7. Use  to move only the selected locking devices or  to move all locking devices.

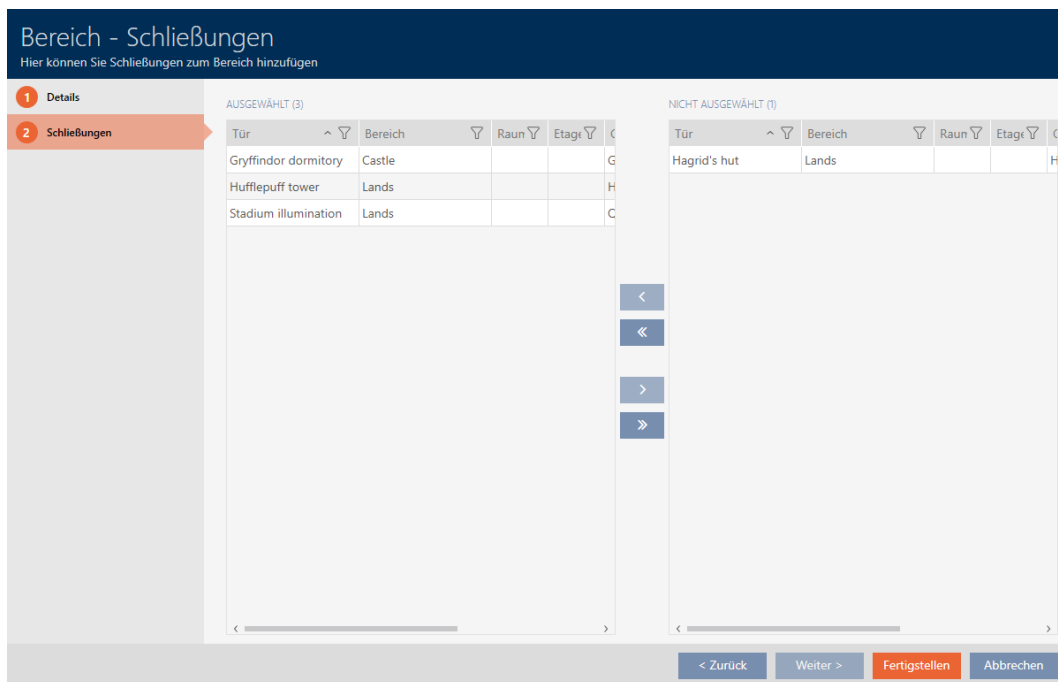


**NOTE**

**Double-clicking as an alternative to arrow keys**

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

- ↳ The highlighted locking device in the left-hand column is added to the area.



8. Click on the **Finish** button.
  - ↳ "Area" window closes.
  - ↳ Locking devices have been moved to the new area.
  - ↳ Matrix displays structure with new areas.

Tür	Typ	Sync
Castle		
Gryffindor dormit...	🔒	🔄
Hufflepuff tower	🔒	
Stadium illuminati...	🔒	
Lands		
Hagrid's hut	🔒	

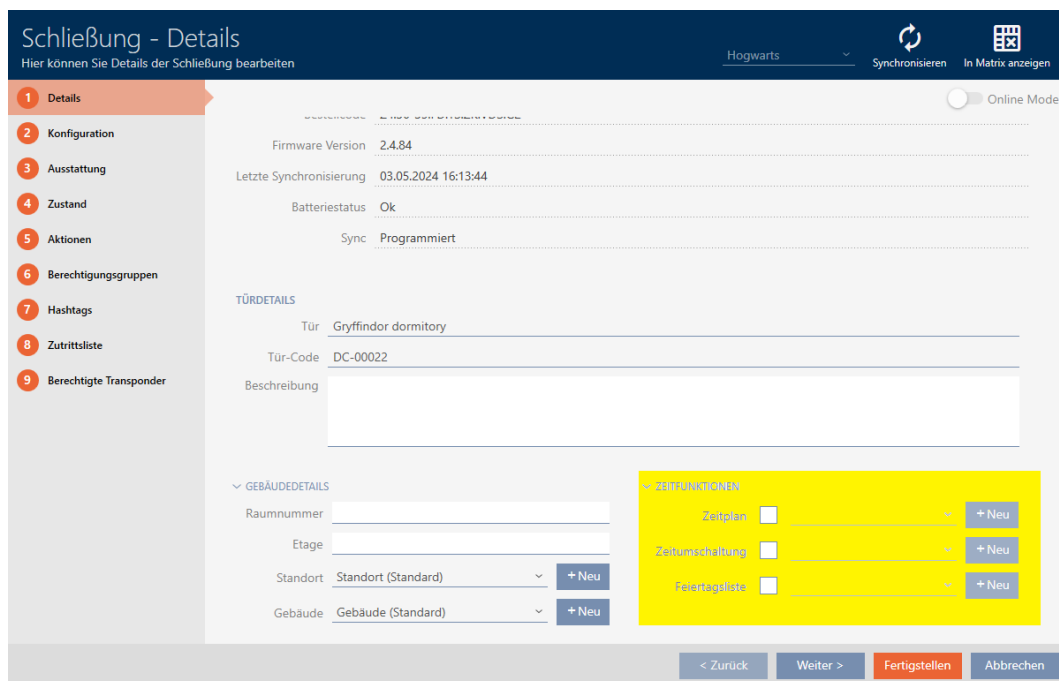
### 15.8 Limiting authorisations for locking devices to specific times (schedule)

You can limit authorisations to specific days and times with a schedule for your locking device (see *Event management* [▶ 528]).

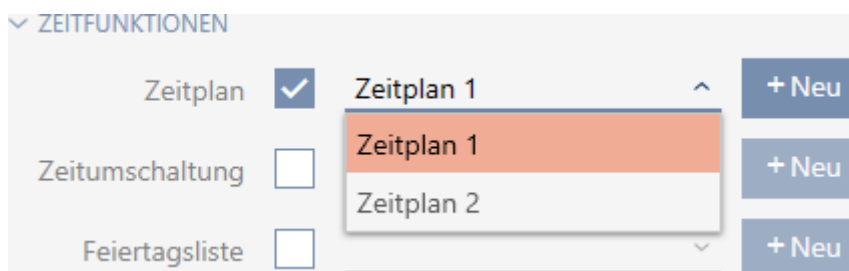
In this chapter you will learn how to add individual locking devices to a schedule using the locking device window. Multiple locking devices can be added more quickly in the schedule itself: *Adding locking devices to the schedule* [▶ 338].

- ✓ Locking device created (see *Creating a locking device* [▶ 228]).
- ✓ Locking device equipped with .ZK option.
- ✓ Schedule created (see *Creating a schedule* [▶ 53]).

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

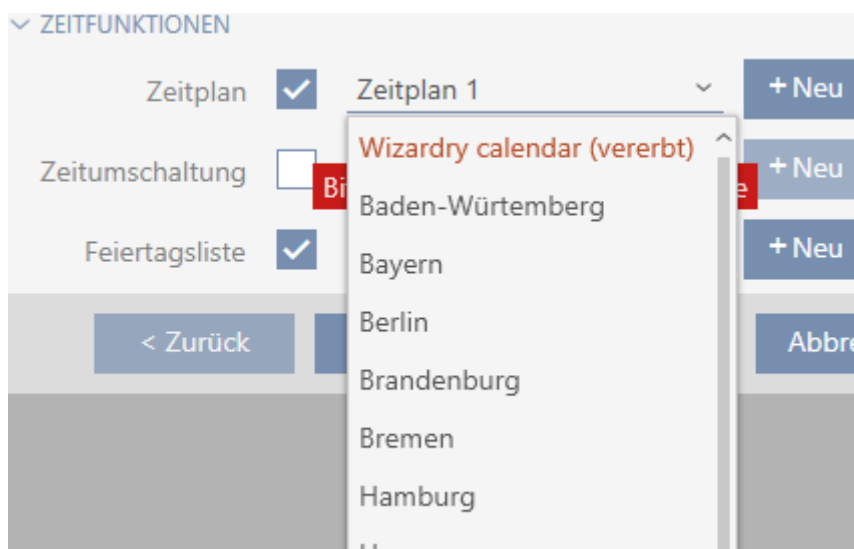


2. Open the "Time functions" menu if necessary.
3. Activate the  Time schedule checkbox.
4. Select the schedule for your locking device from the ▼ Time schedule drop-down menu.



5. Activate the  Holiday list checkbox.

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



#### NOTE

##### Public holiday lists in locking device and locations

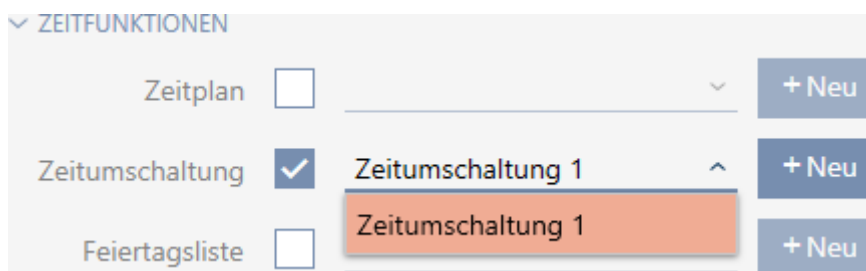
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

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.


### 15.9 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* [▶ 27] and *Creating a time switchover* [▶ 65]). This allows you to set the time switchovers directly in the locking device properties when creating locking devices:



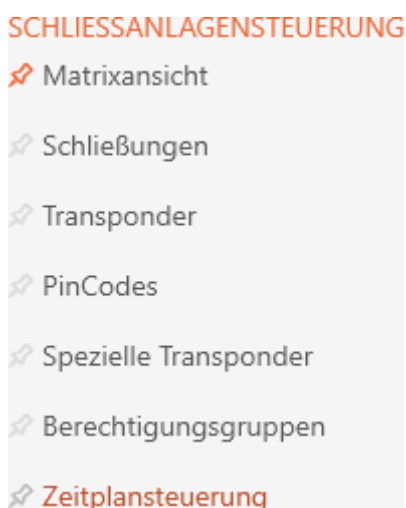
Obviously, you can also add your locking devices to the time switchovers at a later date:

- ✓ Locking device equipped with .ZK option.
- ✓ Time switchover created (see *Creating a time switchover* [▶ 65]).

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

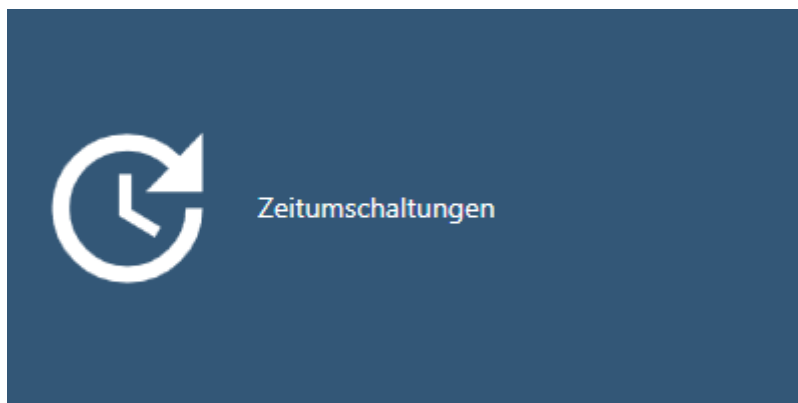


2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.



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

3. Click on the **Time switching**  button.



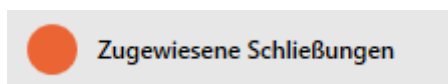
↳ The [Time switching] tab will open.

Matrixansicht × Zeitplansteuerung × Zeitumschaltungen ×				
+ Neu		🗑️ Löschen	📄 Export	🗑️ Anzeigefilter löschen
Name	^	Anzahl Schließungen	Letzte Änderung	Beschreibung
> Zeitumschaltung 1		1	07.05.2021 17:33:50	

4. Click on the time switchover to which you wish to add your locking devices.

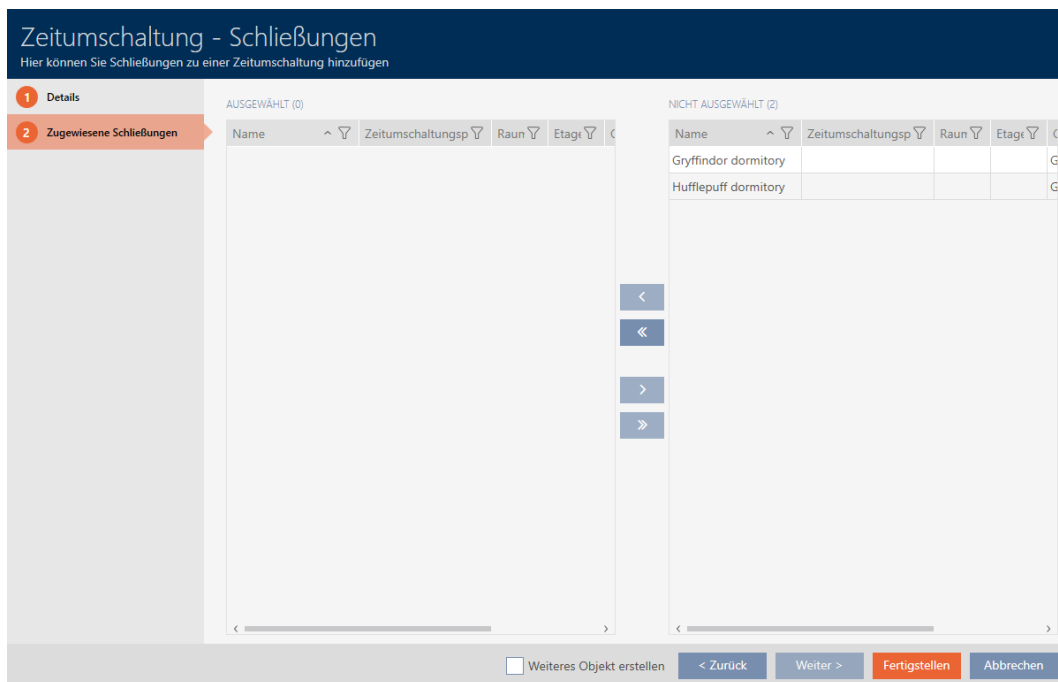
↳ The time switchover window will open.


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* [▶ 44]).
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).

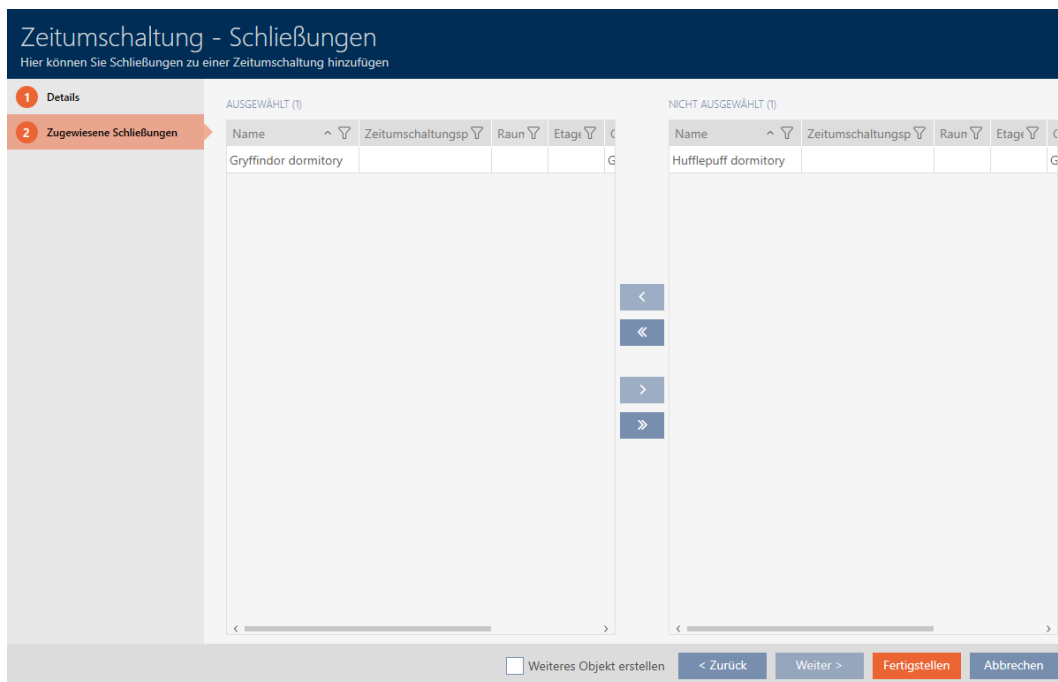


**NOTE**


**Double-clicking as an alternative to arrow keys**

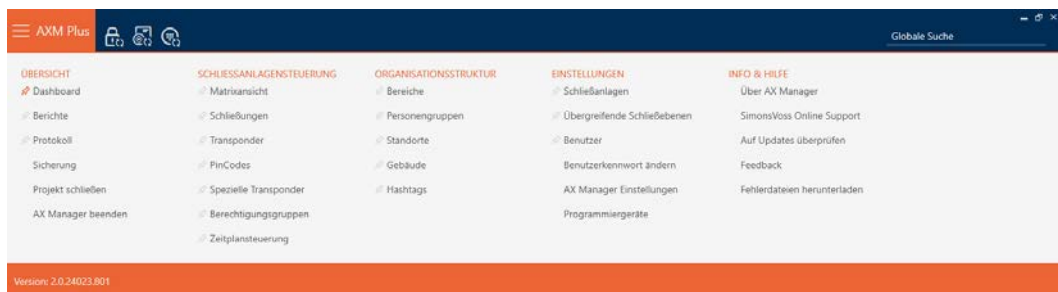
Double-clicking an entry in the list will also move this entry to the other column.

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.

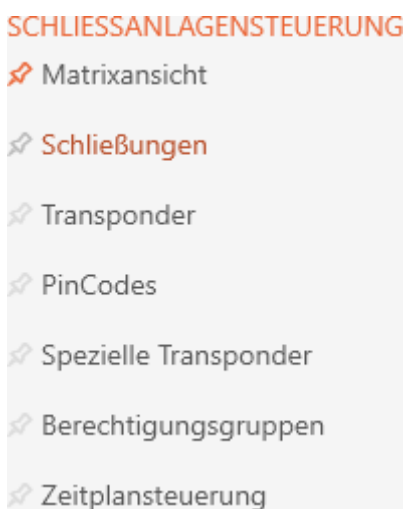



9. Click on the **Finish** button.  
 ↳ The time switchover window closes.

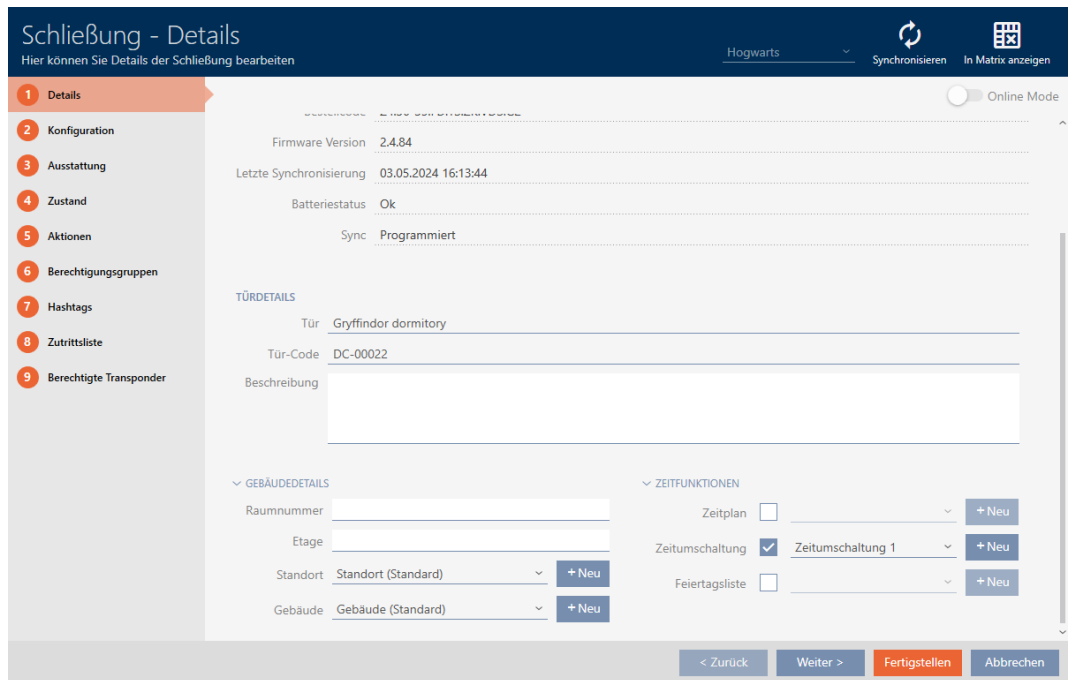
10. Click the orange AXM button .  
 ↳ AXM bar opens.



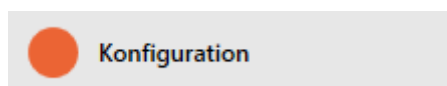
11. Select the entry **Locks** in the group | LOCKING SYSTEM CONTROL |.



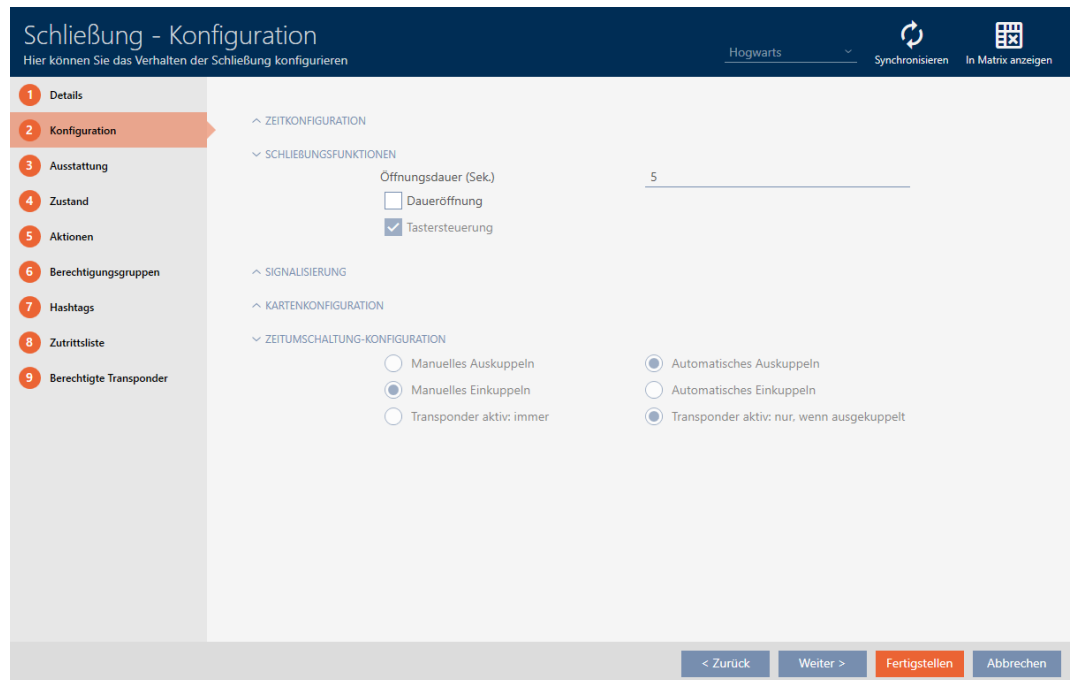
- ↳ The AXM bar will close.
  - ↳ The [Locks] tab will open.
12. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
13. Click on the door to be controlled with the time switchover.
- ↳ The locking device window will open.



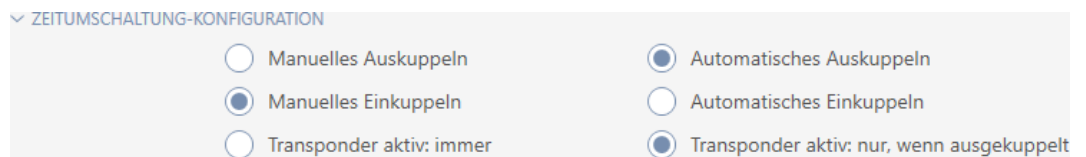
14. Click on the  Configuration tab.



- ↳ Window switches to the "Configuration" tab.



15. Set the required behaviour in the "Time switching - Configuration" drop-down menu (see *Time switchovers* [▶ 532]).



16. Click on the **Finish** button.

↳ The locking device window closes.

↳ Time switchover is set up.

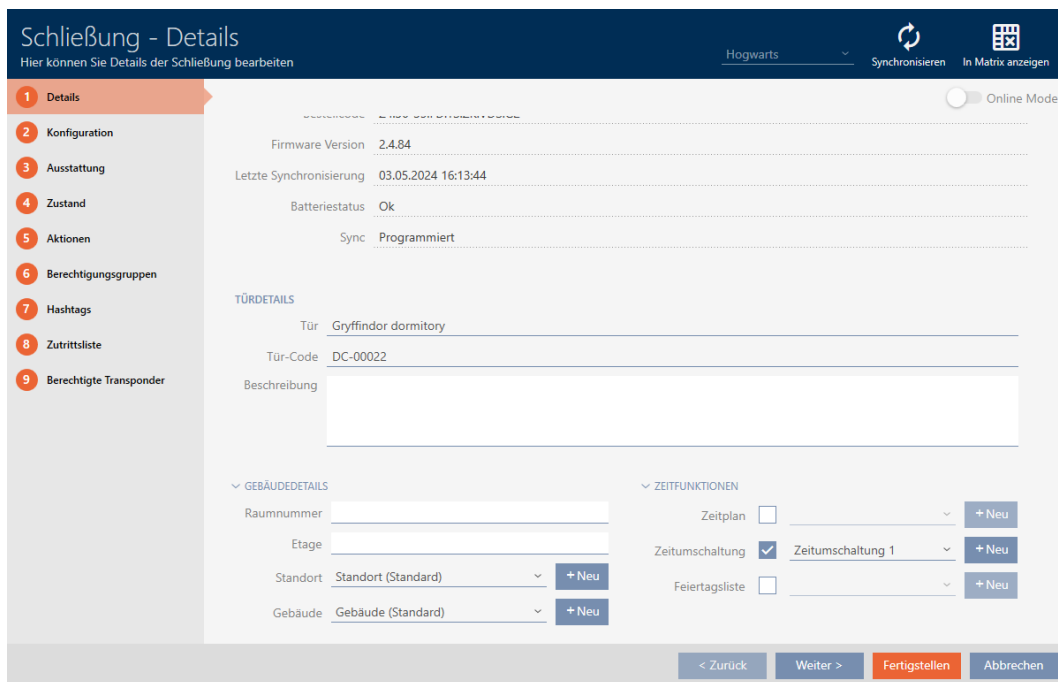
### 15.10 Have accesses logged by locking device (access list)

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* [▶ 527]).

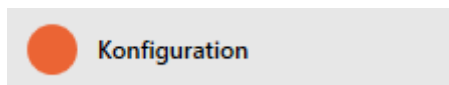
✓ Locking device equipped with .ZK option.

1. Click on the locking device that should log accesses.

↳ The locking device window will open.

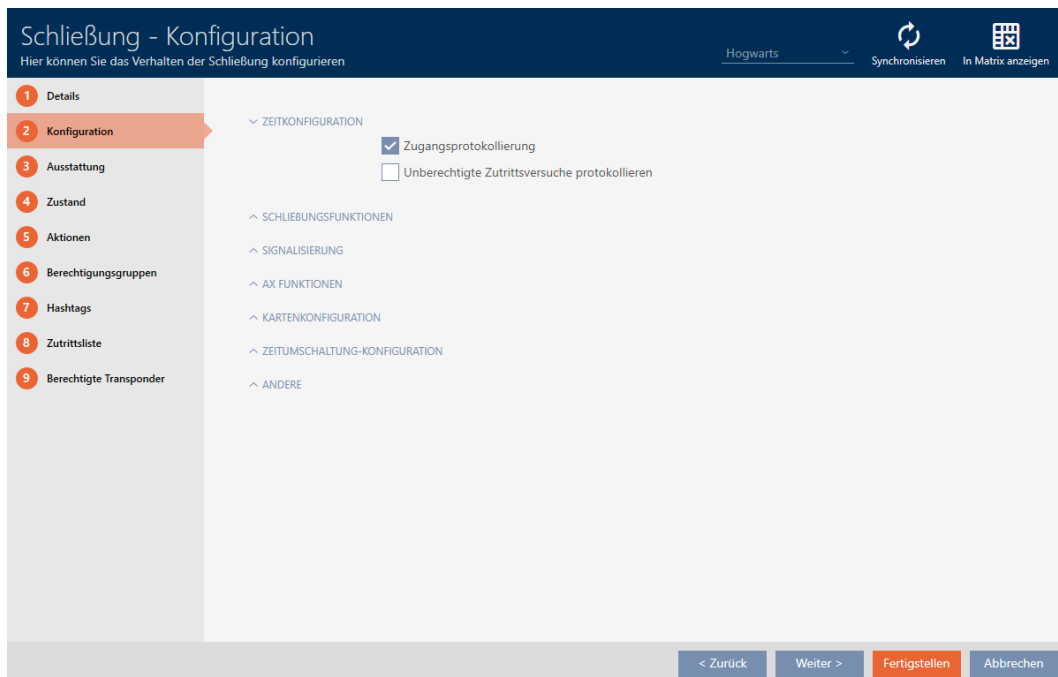


2. Click on the  Configuration tab.



↳ 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)* [▶ 399]).

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* [▶ 404]).

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

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

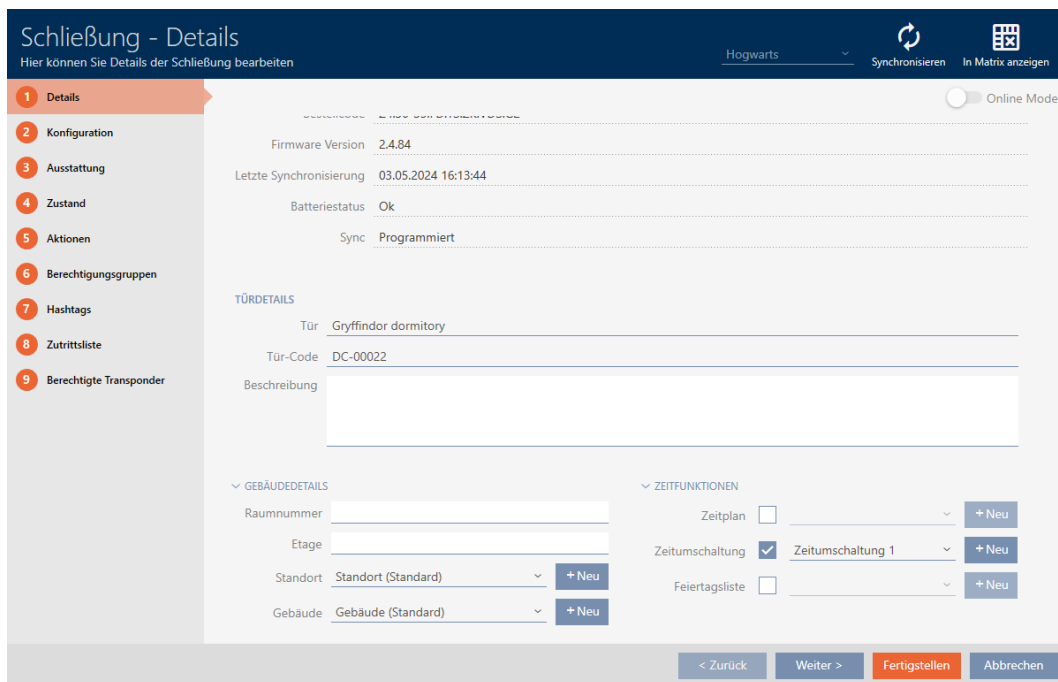
- Pulse opening between 0 s and 25 s: The locking device remains engaged for this time interval after an identification medium has been activated. Then it disengages again automatically.
- Permanent opening: When an identification medium activates the locking device, it engages ready to open and remains 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:

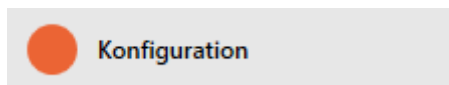
- *Allowing an identification medium to open twice as long* [▶ 114]
- *Engaging and disengaging locking devices automatically with time switchover* [▶ 278]

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

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



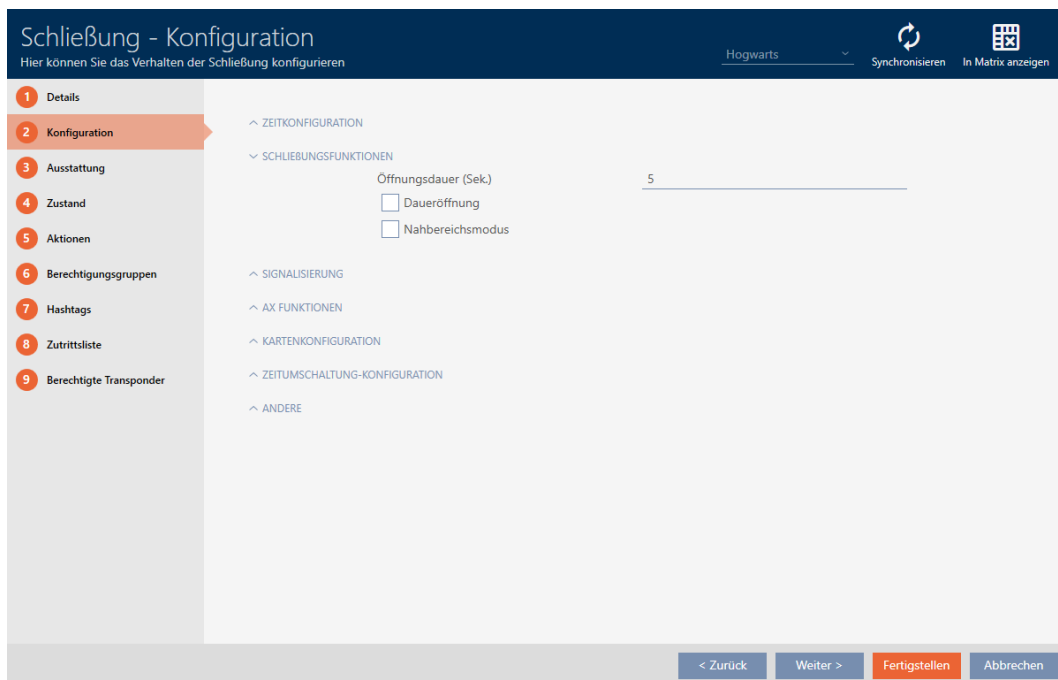
2. Click on the  Configuration tab.



↳ 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.

## 15.12 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.



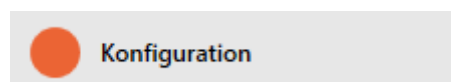
### NOTE

#### 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 Plus will automatically activate the  Close range mode.

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

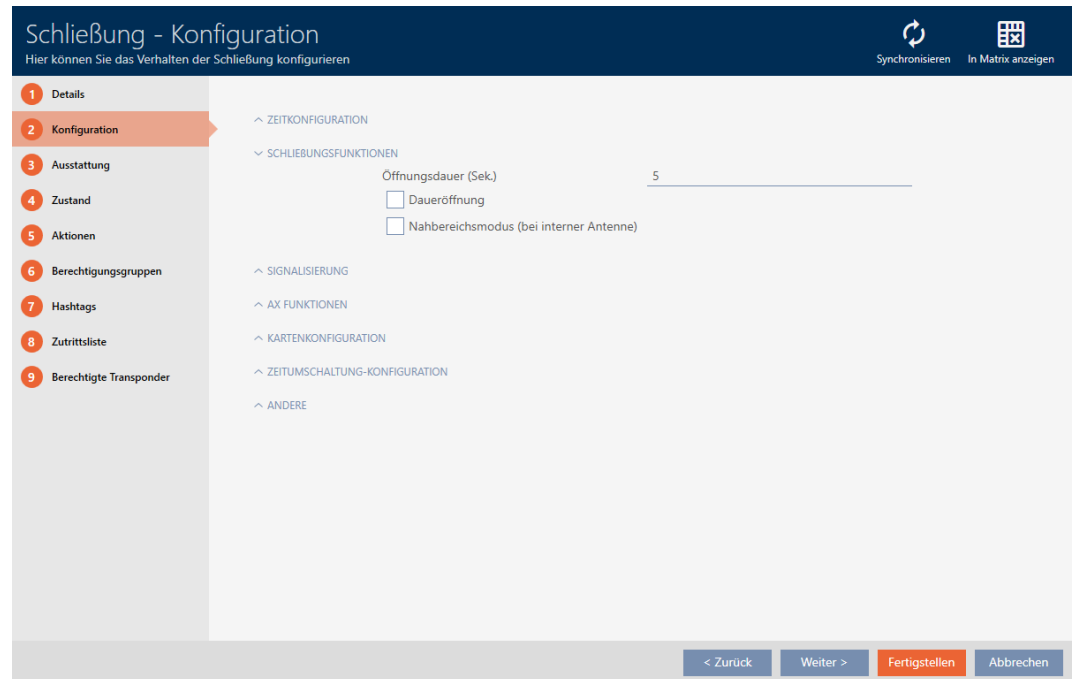
2. Click on the **Konfiguration** tab.



- ↳ Window switches to the [Configuration] tab.



- Expand the "Lock functions" menu.



- Activate the  Close range mode check box (only displayed for suitable locking devices).
- Click on the **Finish** button.
  - ↳ The locking device window closes.
  - ↳ Close range mode activated for this locking device.

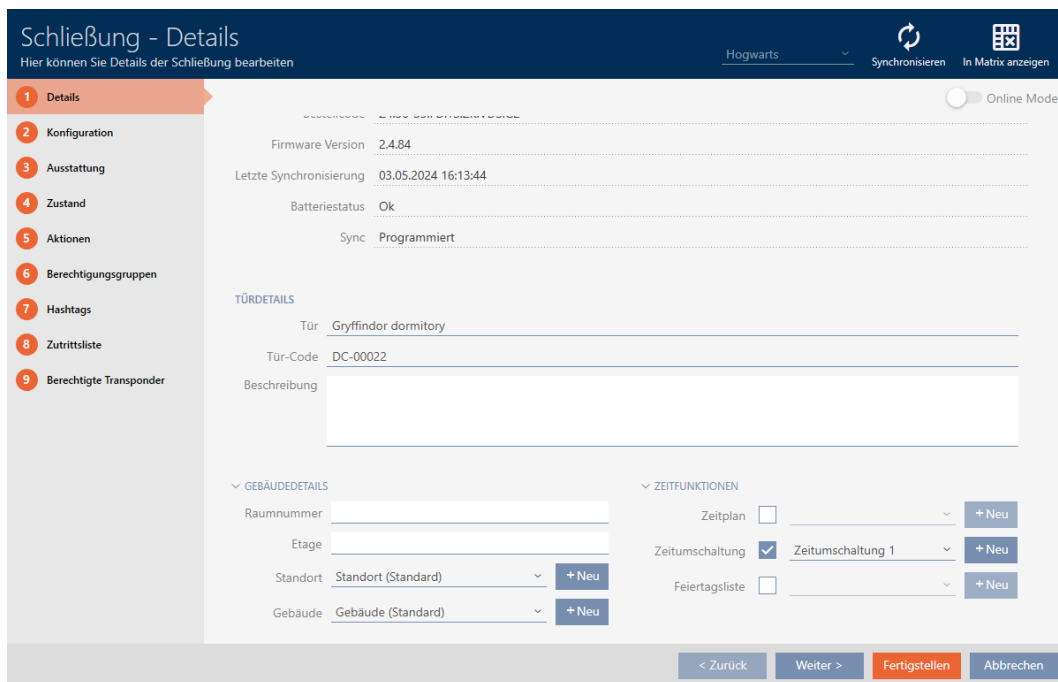
### 15.13 Muting a locking device (for battery warnings and programming)

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

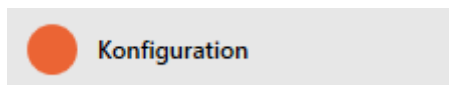
- Audible and visual battery warnings
- Audible programming acknowledgements

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* [▶ 116]).

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

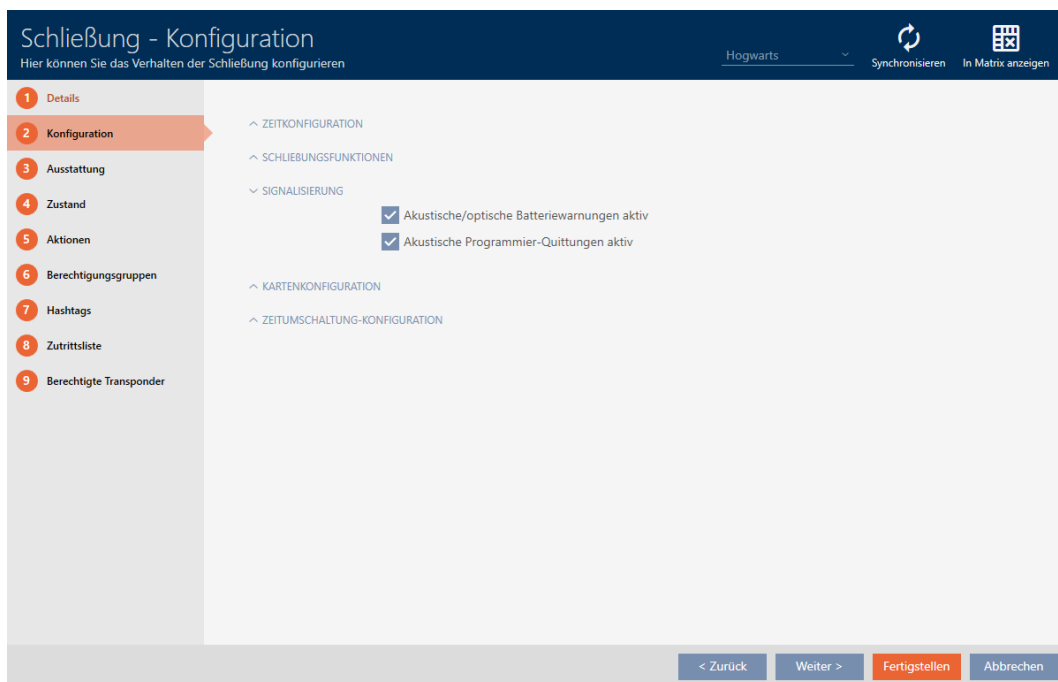


2. Click on the  Configuration tab.

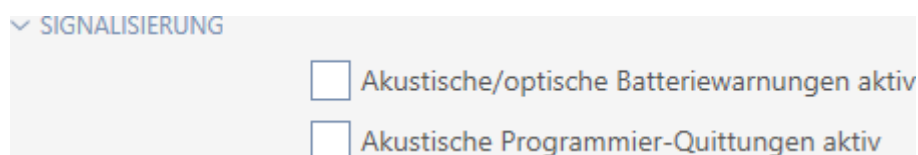


↳ Window switches to the [Configuration] tab.

3. Expand the "Feedback signals" menu.



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



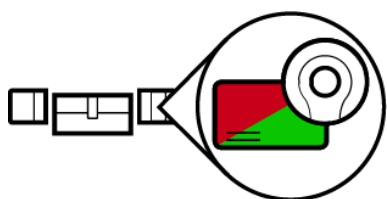
5. Click on the **Finish** button.
  - ↳ The locking device window closes.
  - ↳ Locking device will no longer signal any battery warnings or audible programming acknowledgements.

### 15.14 Activating and deactivating card readers

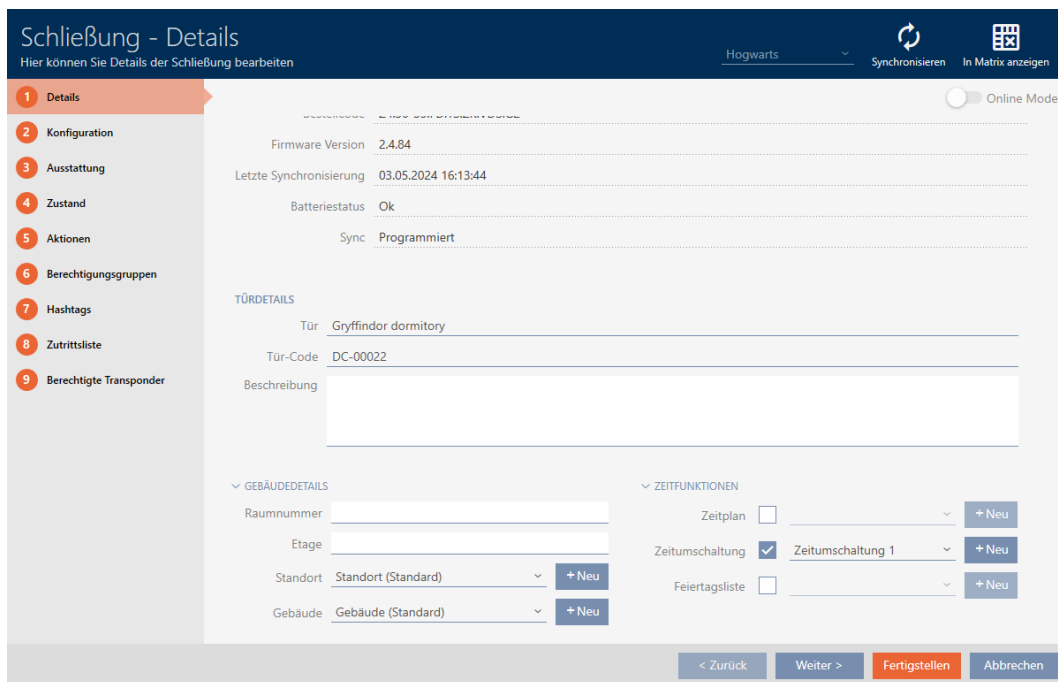
In the default setting, AXM Plus automatically activates the card reader on your locking devices under certain conditions:

- Locking device is in a passive or hybrid locking system  
The card reader is only used if cards can also be used in the locking system. Only transponders are used in an active locking system.
- Locking device has a built-in card reader.  
No card reader can be activated for locking devices without a card reader.

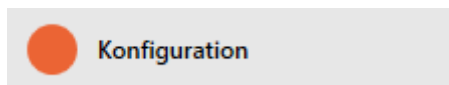
In the case of hybrid locking devices in hybrid locking systems, the locking device might not need to be operated with a card at all. In this case, you can deactivate the card reader with your AXM Plus . This saves power and extends battery life.



- ✓ Locking device created.
1. Click on the locking device whose card reader you wish to activate/deactivate.
    - ↳ The locking device window will open.

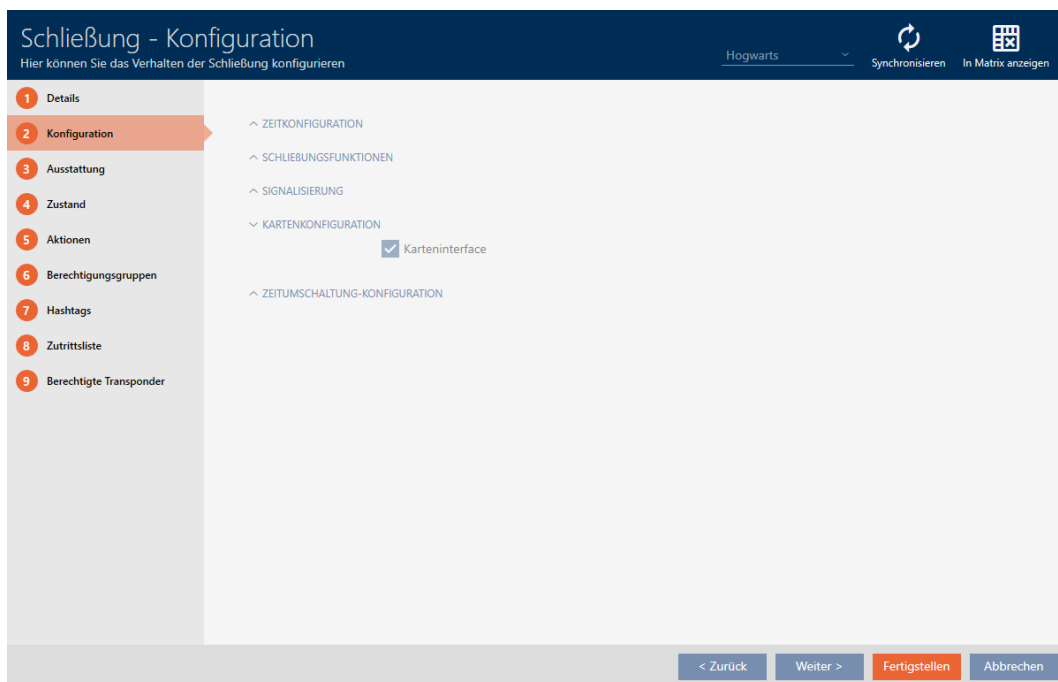


2. Click on the  Configuration tab.



↳ Window switches to the "Configuration" tab.

3. Expand the "Card configuration" menu.



4. Activate or deactivate the  Card interface check box.

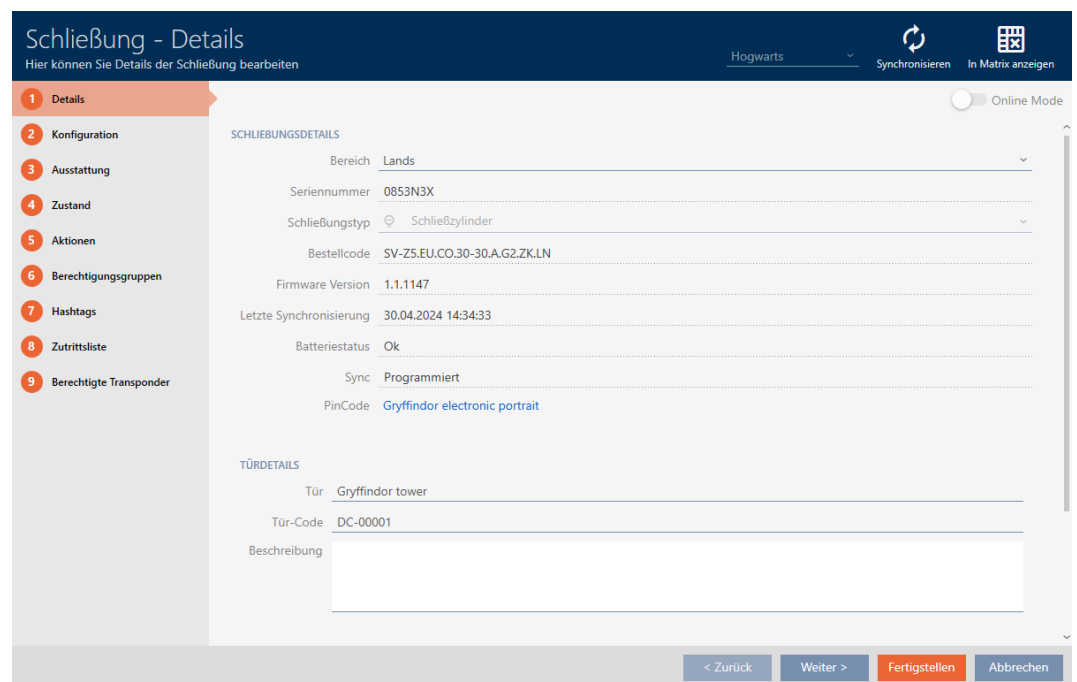
5. Click on the **Finish** button.
  - ↳ The locking device window closes.
  - ↳ Locking device card reader is activated/deactivated.

### 15.15 Ignoring activation and expiry date of identification media

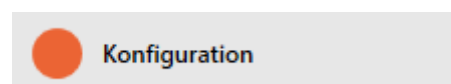
You can enter your identification media's properties to specify that they are to be activated or deactivated on a specific date (see *Activating or deactivating identification medium once at specific times (activation and expiry date)* [▶ 119]).

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

- ✓ AX-based locking device.
1. Click on the locking device to be muted.
    - ↳ The locking device window will open.

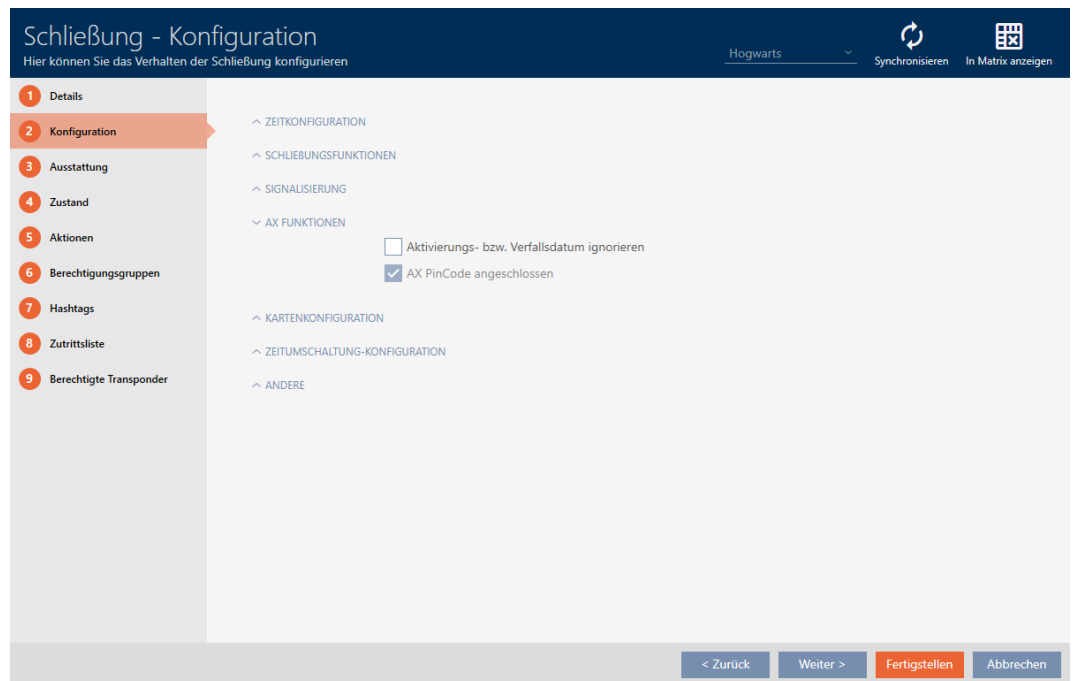


2. Click on the **Konfiguration** tab.

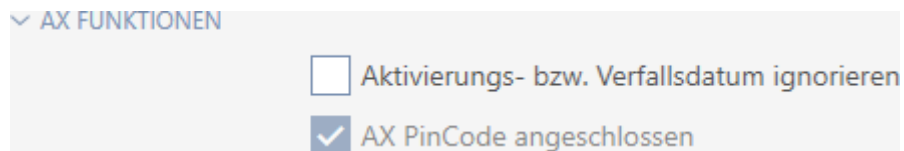


- ↳ Window switches to the [Configuration] tab.

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.

### 15.16 Setting up door monitoring (DoorMonitoring)

You can use DoorMonitoring to monitor the status of your doors and locking devices (also see *DoorMonitoring* [▶ 549]).

**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.

**15.16.1 Setting up DoorMonitoring for locking cylinders**

- ✓ 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.

Schließung - Details  
Hier können Sie Details der Schließung bearbeiten

Hogwarts Synchronisieren In Matrix anzeigen

1 Details Online Mode

2 Konfiguration SCHLIEßUNGSDetails

3 Ausstattung

4 Zustand

5 Aktionen

6 Berechtigungsgruppen

7 Hashtags

8 Zutrittsliste

9 Berechtigte Transponder

Bereich Standardbereich

Seriennummer 00E04GX

Schließungstyp Schließzylinder

Bestellcode Z4.30-35.DM.FD.ZK.G2

Firmware Version 3.5.34

Letzte Synchronisierung 03.05.2024 10:00:43

Batteriestatus Ok

Sync Programmiert

TÜRDETAILS

Tür Main gate

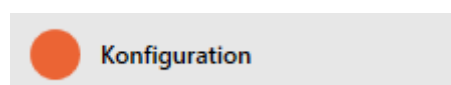
Tür-Code DC-00012

Beschreibung

GEBÄUDEDETAILS ZEITFUNKTIONEN

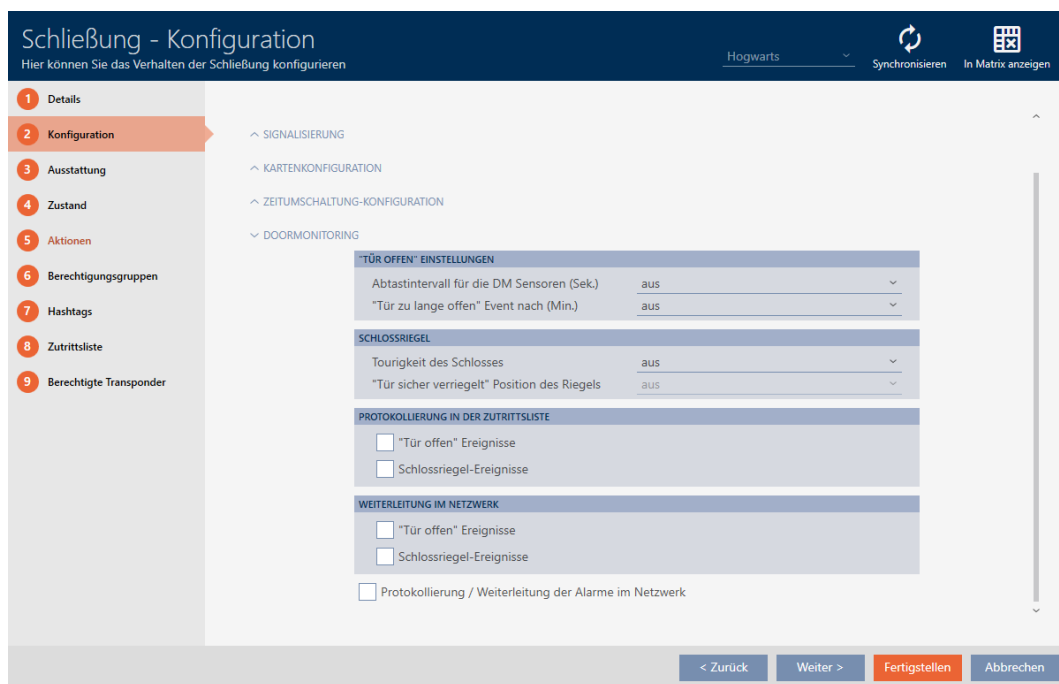
< Zurück Weiter > Fertigstellen Abbrechen

2. Click on the **Konfiguration** 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

"TÜR OFFEN" EINSTELLUNGEN	
Abtastintervall für die DM Sensoren (Sek.)	aus
"Tür zu lange offen" Event nach (Min.)	aus

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
<p>Sampling interval for the DM sensors (sec.)</p>	<p>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.</p> <p>Possible intervals are:</p> <ul style="list-style-type: none"> <li>■ seconds</li> <li>■ second</li> <li>■ seconds</li> <li>■ seconds</li> <li>■ seconds</li> <li>■ seconds</li> <li>■ seconds</li> </ul> <p>More frequent checks lead to faster detection of an open door, but also increase power consumption.</p>
<p>"Door open too long" event after (min.)</p>	<p>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.</p> <p>After the set time has elapsed, the Door open too long event is triggered.</p> <p>Possible intervals:</p> <ul style="list-style-type: none"> <li>■ minutes</li> <li>■ minutes</li> <li>■ minute</li> <li>■ minutes</li> <li>■ minutes</li> <li>■ minutes</li> </ul>

Lock bolt

SCHLOSSRIEGEL		
Tourigkeit des Schlosses	aus	▼
"Tür sicher verriegelt" Position des Riegels	aus	▼

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	<p>The number of turns required to fully extend the mortise lock dead bolt.</p> <p>Possible intervals are:</p> <ul style="list-style-type: none"> <li>■ off</li> <li>■ 1-turn</li> <li>■ 2-turn</li> <li>■ 3-turn</li> <li>■ 4-turn</li> </ul>

Setting	Explanation
<p>“Door securely locked” position of dead bolt</p>	<p>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.</p> <p>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.</p> <p>The available settings depend on what you have specified in Number of turns to lock:</p> <ul style="list-style-type: none"> <li>■ off</li> <li>■</li> <li>■</li> <li>■</li> <li>■</li> </ul>

### Logging in the access list

**PROTOKOLLIERUNG IN DER ZUTRITTSLISTE**

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

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	<p>Select this checkbox to write "Door open" events into the access list for your locking device.</p> <p>This applies to these events:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Door is open</li> <li><input checked="" type="checkbox"/> Door is closed</li> <li><input checked="" type="checkbox"/> Door is open for a long time</li> </ul>
Lock bolt events	<p>Select this checkbox to write Lock bolt events into the access list for your locking device.</p> <p>This applies to these events:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Door is locked</li> <li><input checked="" type="checkbox"/> Door is securely locked</li> </ul>

### Forward in network

**WEITERLEITUNG IM NETZWERK**

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Protokollierung / Weiterleitung der Alarme im Netzwerk

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	<p>Select this checkbox to forward "Door open" events to the database.</p> <p>This applies to these events:</p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Door is open</li> <li><input checked="" type="checkbox"/> Door is closed</li> <li><input checked="" type="checkbox"/> Door is open for a long time</li> </ul> <p>If you select this checkbox, the events are also automatically saved in the access list.</p>

Setting	Explanation
Lock bolt events	<p>Select this checkbox to forward Lock bolt events to the database.</p> <p>This applies to these events:</p> <ul style="list-style-type: none"> <li>■ Door is locked</li> <li>■ Door is securely locked</li> </ul> <p>If you select this checkbox, the events are also automatically saved in the access list.</p>
Event logging/forwarding of alarms in the network	<p>Your DoorMonitoring locking device detects various alarm situations. You can forward these to your database.</p> <p>Examples of such situations are:</p> <ul style="list-style-type: none"> <li>■ Door open too long</li> <li>■ Tampering attempt (e.g. Fastening screw has been manipulated)</li> <li>■ Door has been opened even though it is considered locked or securely locked</li> </ul>

### 15.17 Changing the SmartRelay settings

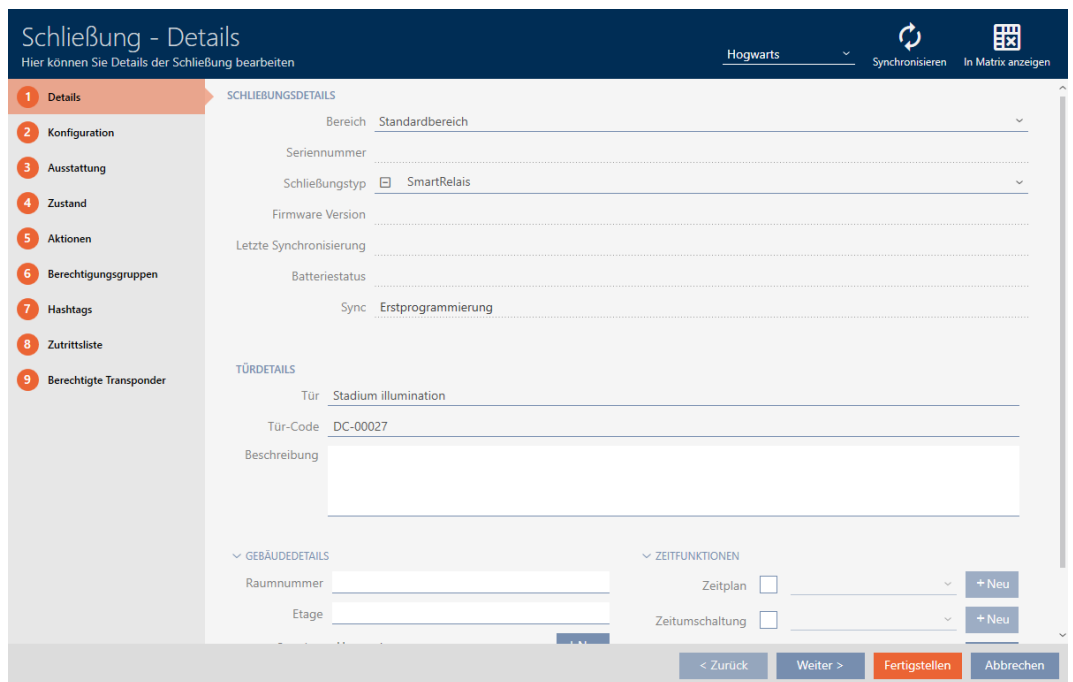
You will only see the settings for SmartRelay if you:

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

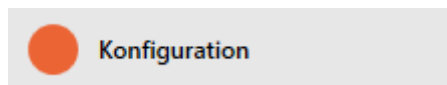
All SmartRelay settings are changed in the "Configuration" tab:

- ✓ Locking device list or matrix view open.

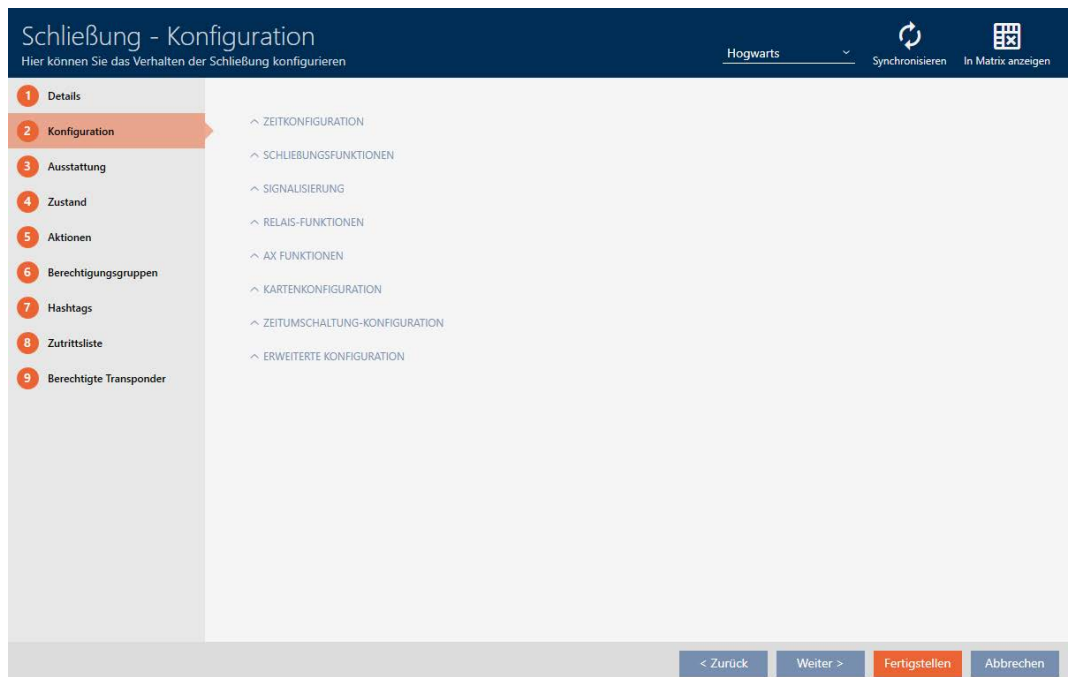
1. Click on the SmartRelay.
  - ↳ The SmartRelay window will open.



2. Click on the  Configuration tab.



↳ Window switches to the "Configuration" tab.



### 15.17.1 Using internal and external antenna simultaneously

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

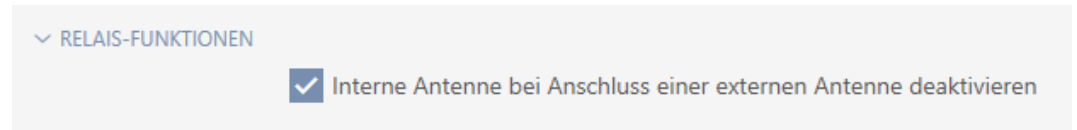


The internal antenna is normally deactivated as soon as SmartRelay detects an external antenna.

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

✓ "Configuration" tab open (see *Changing the SmartRelay settings* [▶ 301]).

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.

### 15.17.2 Invert outputs

A relay has two states:

■ Energised (coil energised)

■ Not energised (idle state)

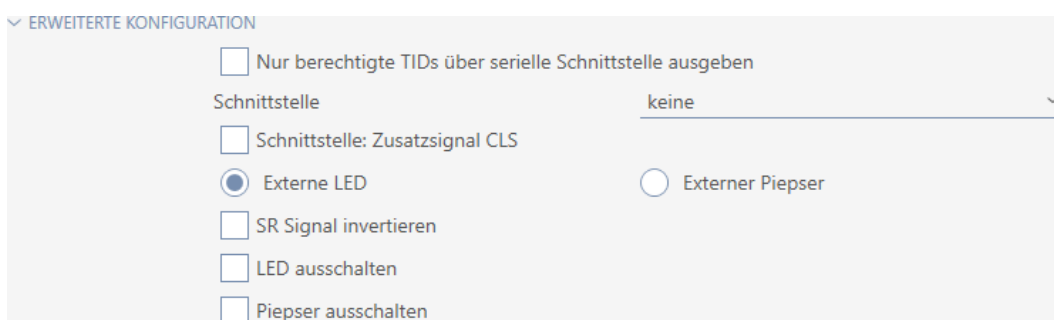
The relay is normally in the idle state and is energised when an identification medium is activated.

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

Changeover contact	NO contact
<ul style="list-style-type: none"> <li>■ SREL</li> <li>■ SREL.ADV</li> <li>■ SREL.W</li> <li>■ SREL.G2</li> <li>■ SREL.W.G2</li> <li>■ SREL 3</li> <li>■ SREL 3 Advanced</li> <li>■ SREL AX Classic</li> </ul>	SREL2.G2
<input type="checkbox"/> Invert SR signal <ul style="list-style-type: none"> <li>■ Identification medium activated: Relay energises, COM connected to NO</li> <li>■ Identification medium not activated: Relay in idle state, COM connected to NC</li> </ul>	<input type="checkbox"/> Invert SR signal <ul style="list-style-type: none"> <li>■ Identification medium activated: Relay energises, contacts connected</li> <li>■ Identification medium not activated: Relay in idle state, contacts not connected</li> </ul>
<input checked="" type="checkbox"/> Invert SR signal <ul style="list-style-type: none"> <li>■ Identification medium activated: Relay in idle state, COM connected to NC</li> <li>■ Identification medium not activated: Relay energises, COM connected to NO</li> </ul>	<input checked="" type="checkbox"/> Invert SR signal <ul style="list-style-type: none"> <li>■ Identification medium activated: Relay in idle state, contacts not connected</li> <li>■ Identification medium not activated: Relay energises, contacts connected</li> </ul>

✓ "Configuration" tab open (see *Changing the SmartRelay settings* [[▶ 301](#)]).

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.

### 15.17.3 Using the serial interface

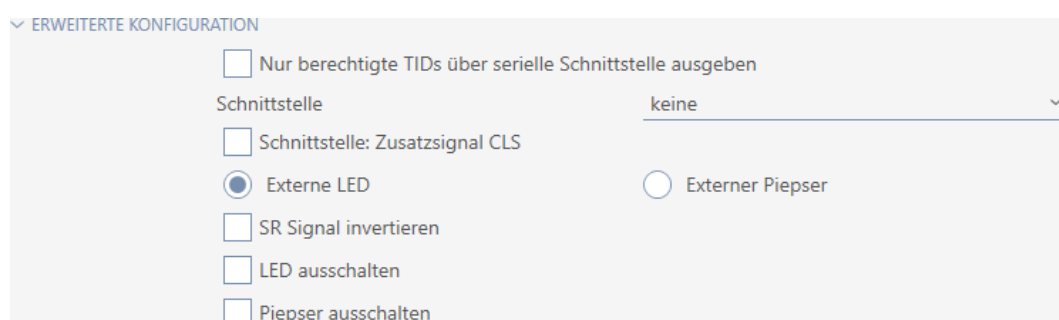
SmartRelays with a serial interface can transfer data from identification media to third-party systems. The following systems are available:

- ❑ "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* [▶ 301]).

1. Open the "Extended configuration" menu if necessary.

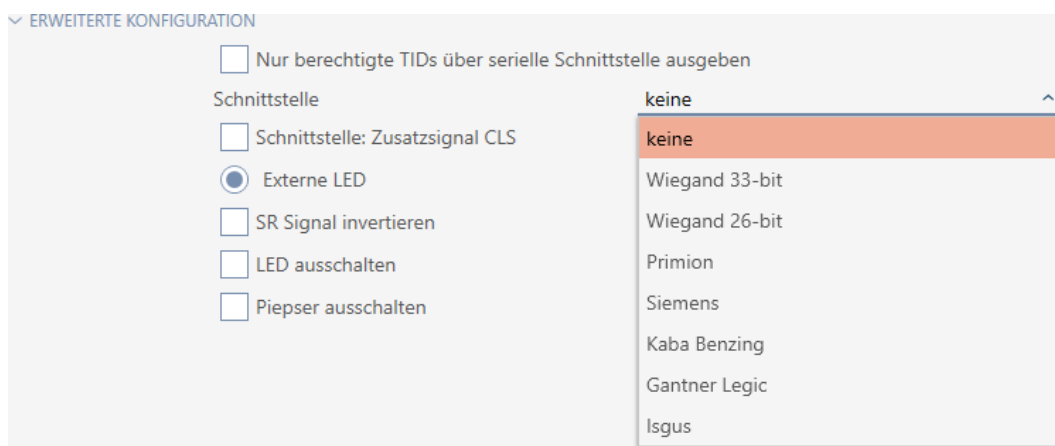


ERWEITERTE KONFIGURATION

- Nur berechtigte TIDs über serielle Schnittstelle ausgeben
- Schnittstelle: keine
- Schnittstelle: Zusatzsignal CLS
- Externe LED  Externer Piepser
- SR Signal invertieren
- LED ausschalten
- Piepser ausschalten

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.

#### 15.17.4 Changing the signalling

Different situations may require different signals.

You can configure signalling of your SmartRelay in AXM Plus to meet these different needs.

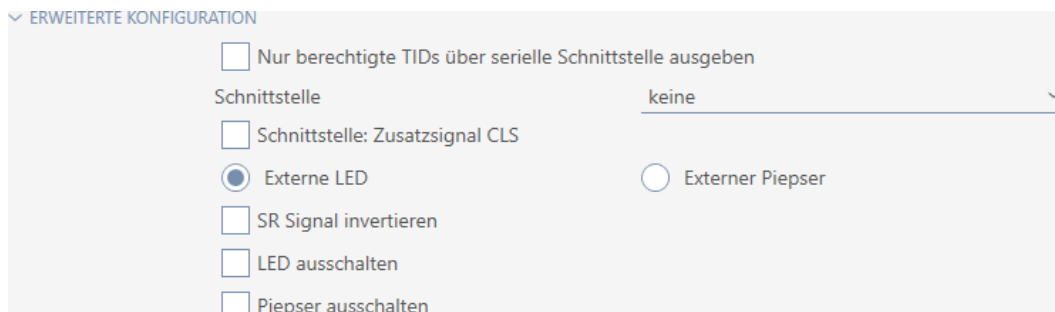
There is a connection for an external LED or an external beeper on the SREL.ADV and SREL2.G2. You can find details on connection in the manual for the SmartRelay concerned.

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.

<input checked="" type="radio"/> External LED	<input checked="" type="radio"/> 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* [▶301]).

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.

### 15.18 Planning and tracking locking device management tasks

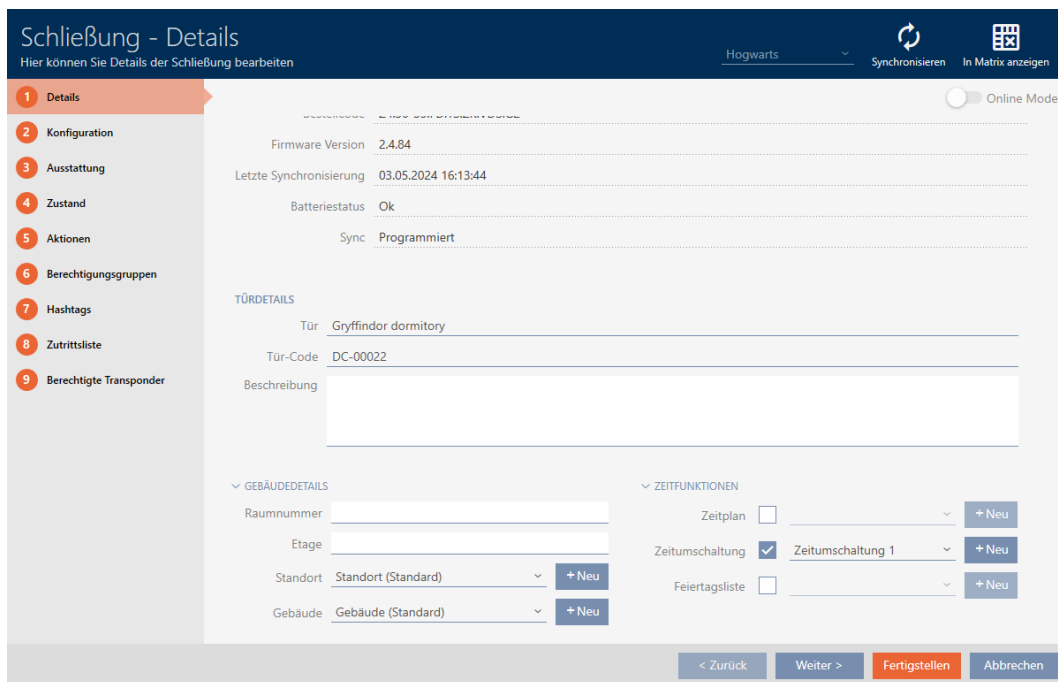
The central point of contact for managing your locking device is the "Actions" tab.

The following entries are displayed here collectively:

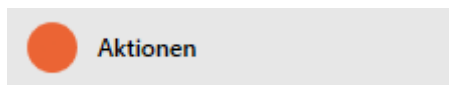
- Created
- Programming
- Installed
- Replaced
- Removed
- Scheduled battery change
- Last battery change

- ✓ Locking device has been created.

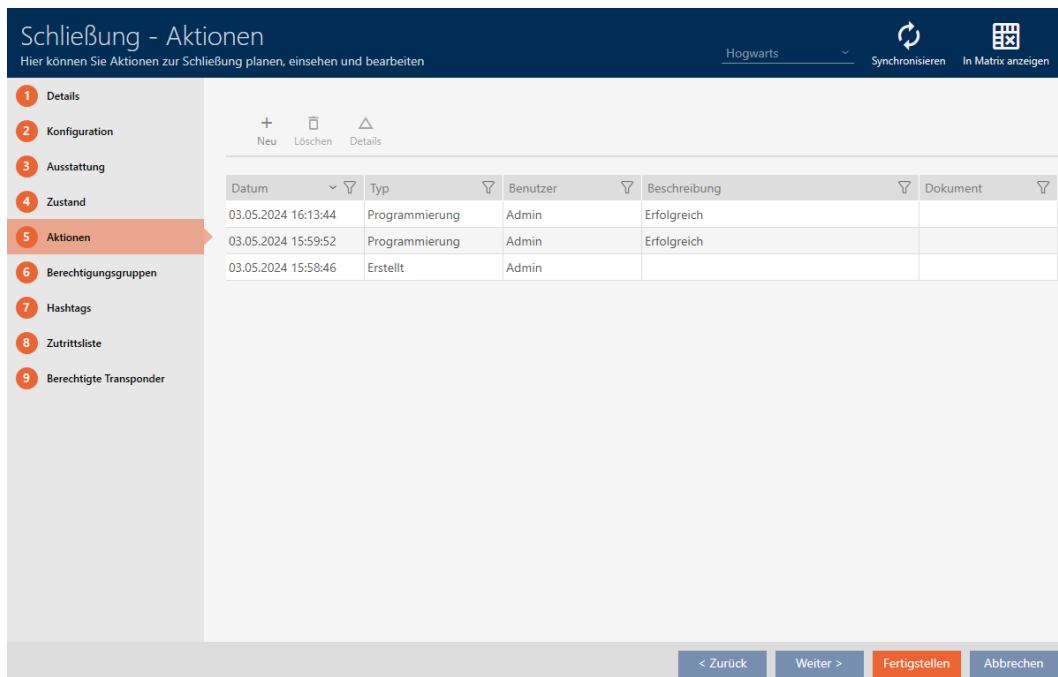
1. Click on the locking device you wish to manage.
  - ↳ The locking device window will open.




2. Click on the  Actions tab.



↳ Window switches to the "Actions" tab.

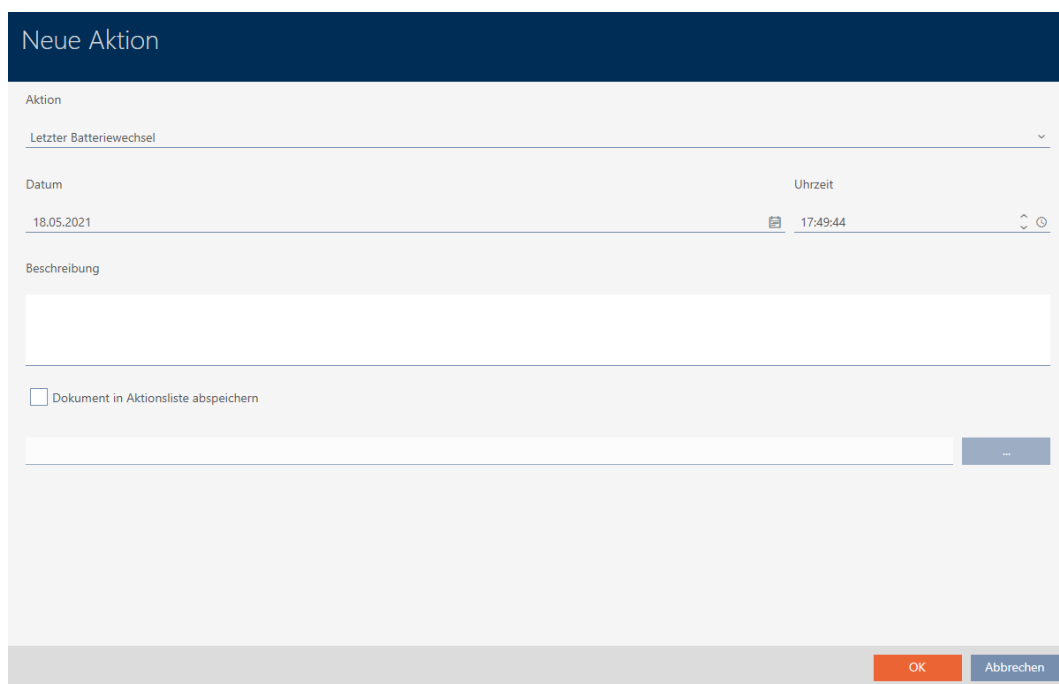


3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

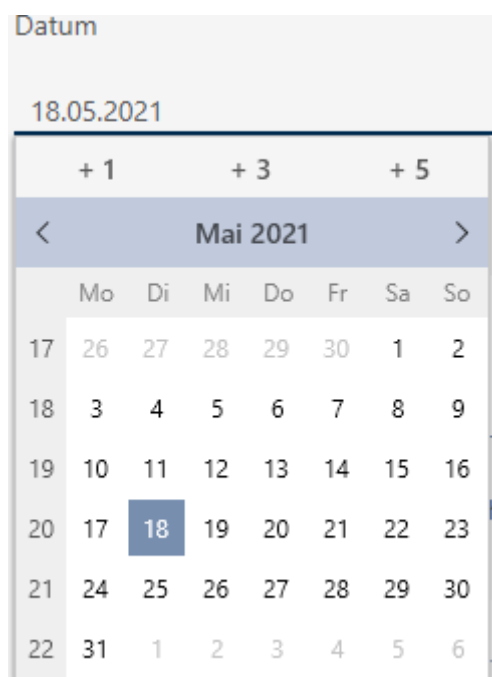
15.18.1 Note installation, replacement or removal date


✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks [▶ 307]*).


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.
  - ↳ Explorer window closes.

9. Click on the  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		

### 15.18.2 Planning and logging battery replacement

- ✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks* [▶ 307]).
1. Click on the  button.
    - ↳ The window for a new action will open.

**Neue Aktion**

Aktion  
 Letzter Batteriewechsel

Datum  
 18.05.2021

Uhrzeit  
 17:49:44

Beschreibung

Dokument in Aktionsliste abspeichern

OK Abbrechen

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.

**Neue Aktion**

Aktion  
 Planmäßiger Batteriewechsel


Datum  
 18.05.2021

Uhrzeit  
 18:43:56

Mai 2021						
Mo	Di	Mi	Do	Fr	Sa	So
17	26	27	28	29	30	1 2
18	3	4	5	6	7	8 9
19	10	11	12	13	14	15 16
20	17	18	19	20	21	22 23
21	24	25	26	27	28	29 30
22	31	1	2	3	4	5 6

OK Abbrechen

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.
  - ↳ Explorer window closes.

**Neue Aktion**

Aktion

Planmäßiger Batteriewechsel ▼

---

Datum Uhrzeit


18.05.2021 📅 18:43:56 ↕ ⌚

---

Beschreibung


---

Dokument in Aktionsliste abspeichern

D:\info.txt 


---

OK
Abbrechen

9. Click on the  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		

### 15.19 Displaying all locking devices in a project

- ✓ At least one locking device created (see *Creating a locking device* [[▶ 228](#)]).
1. Click on the orange AXM icon .
    - ↳ AXM bar opens.





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

**SCHLISSANLAGENSTEUERUNG**

- Matrixansicht
- Schließungen**
- Transponder
- PinCodes
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung

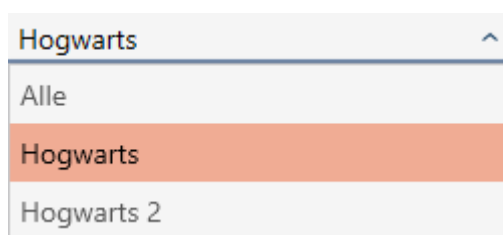
- ↳ The AXM bar will close.
- ↳ The [Locks] tab will open.

Schließungen x

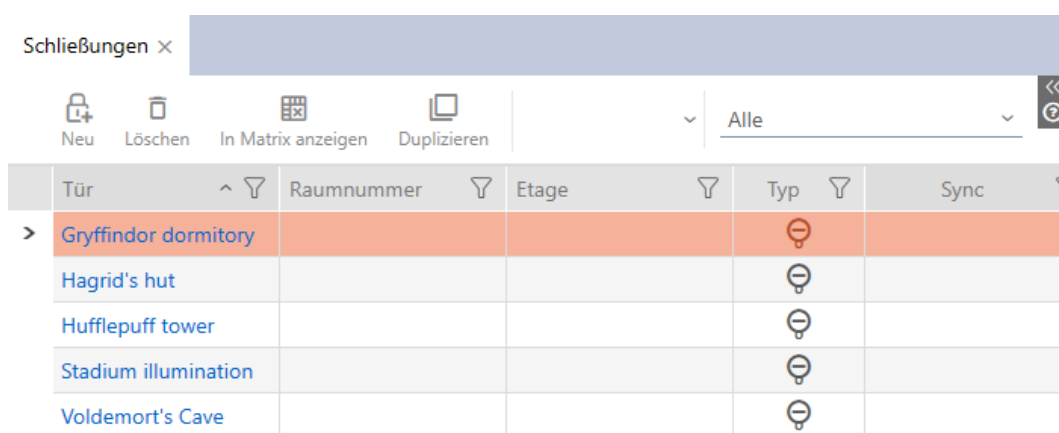
Neu Löschen In Matrix anzeigen Duplizieren | Hogwarts 1

Tür	Raumnummer	Etage	Typ	Sync
> Gryffindor dormitory			🔦	
Hagrid's hut			🔦	
Hufflepuff tower			🔦	
Stadium illumination			🔦	

3. Select the "All" entry for the locking system from the drop-down menu.



↳ All locking devices in all locking systems in the same project are displayed.



You can also export the locking devices displayed as a list (see *Exporting locking devices as a list* [▶ 314]).

## 15.20 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 Plus.

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

✓ Locking device has been created.

1. Click the orange AXM button .

↳ AXM bar opens.



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

**SCHLIESSANLAGENSTEUERUNG**

- Matrixansicht
- Schließungen**
- Transponder
- PinCodes
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung

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

3. Replace if necessary using the drop-down menu for another locking system or select the "All" entry to display the locking devices in all locking systems.

Tür	Raumnummer	Etage	Typ	Sync	Status	Letzte Synchronisierung	S/N	Schließungs ID
> Gryffindor dormi...			🔒			14.12.2021 15:56:38	0084GEAD	129
Hagrid's hut			🔒			13.12.2021 20:31:29	000DSP7E	128
Hufflepuff tower			🔒			13.12.2021 20:33:19	000E04GX	10000
Stadium illumina...			🔒	↻		13.12.2021 20:34:32		ohne Programmierung

4. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

5. Click on the **Export** button.

↳ The Explorer window will open.

6. Save the PDF file to a file directory of your choice.

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



**Alle Schließungen für die Schließanlage 'Hogwarts 1'**

Tür	Raumnummer	Etage	Typ	Sync	Status	S/N
Gryffindor dormitory			Schließzylinder	Programmiert		0084GEAD
Hagrid's hut			Schließzylinder	Programmiert		000DSP7E
Hufflepuff tower			Schließzylinder	Programmiert		000E04GX
Stadium illumination			Schließzylinder	Erstprogrammierung		

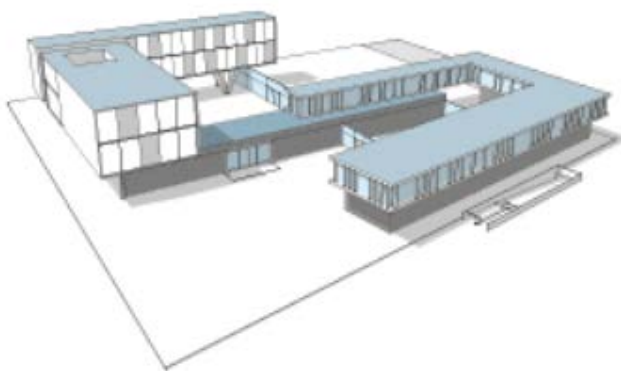
You have the option to personalise reports (see *Personalising reports and exports* [[▶ 445](#)]).

## 16. Permissions

### 16.1 Changing individual authorisations (cross)

The quickest way to assign individual authorisations to individual doors is directly in the matrix.

- ✓ 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).



Person	Weasley, Ron	Weasley, Fred	Lovegood, Luna	Granger, Hermine
Typ	⊕	⊕	⊕	⊕

Tür	Typ
Gryffindor dormitory	⊕
Hufflepuff dormitory	⊕

			X

- 2. Click on the same box again.
  - ↳ Authorisation is withdrawn again.

Tür	Typ	Person
Gryffindor dormitory	⊖	Weasley, Ron
Hufflepuff dormitory	⊖	Weasley, Fred
	⊖	Lovegood, Luna
	⊖	Granger, Hermine

↳ 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* [▶ 435]):

- Single click of the mouse
- Double click
- Ctrl + single click



**16.2 Changing many authorisations (on identification media and/or locking devices)**

**16.2.1 Allowing all or blocking all**



Instead of individual authorisations, you can also:

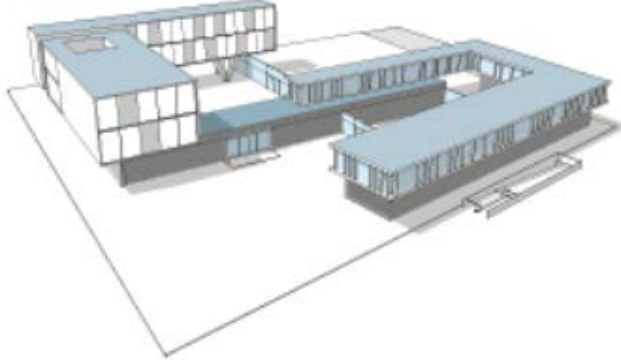
- Allow or block all currently displayed identification media on a locking device
- Allow or block identification media on all currently displayed locking devices





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:

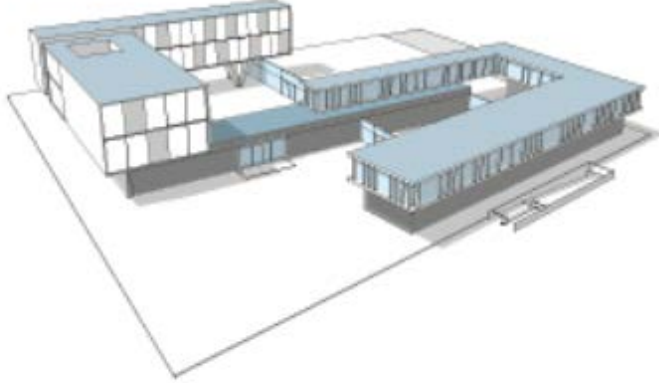







Person	Weasley, Ron	Weasley, Fred	Lovegood, Luna	Granger, Hermine
Typ				

Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	





- ✓ Matrix screen open
- ✓ Identification medium available.
- ✓ Locking device available.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).



	Person	▼	Weasley, Ron	Weasley, Fred	Granger, Hermine
	Typ				

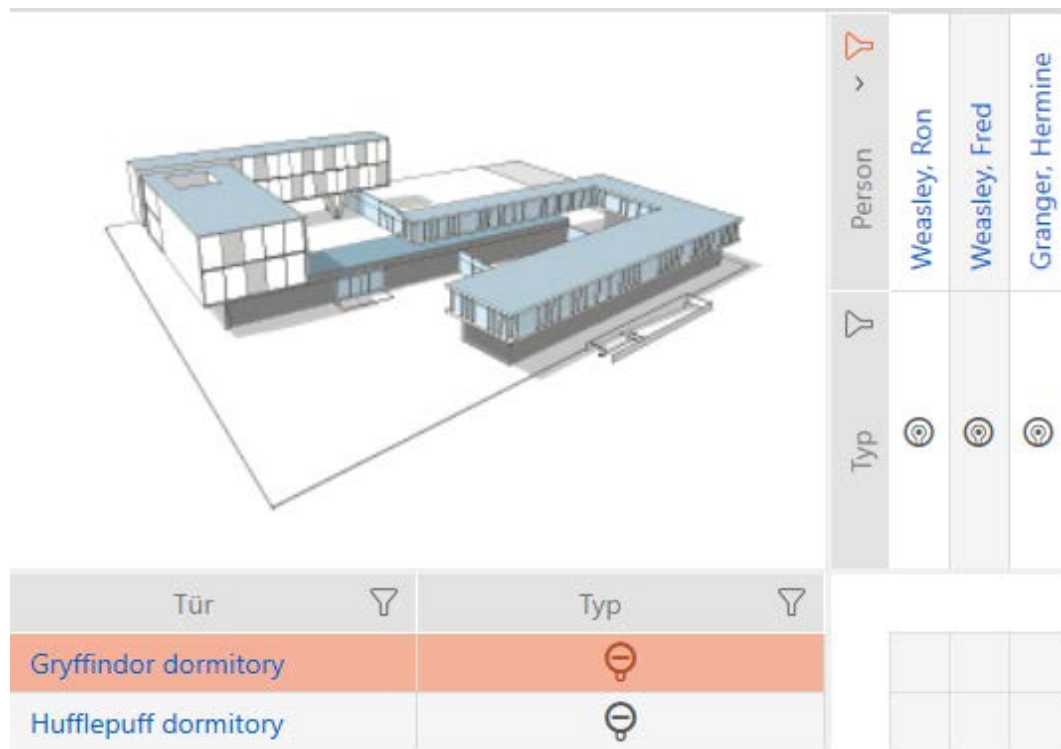
  

Tür		Typ	
Gryffindor dormitory			
Hufflepuff dormitory			

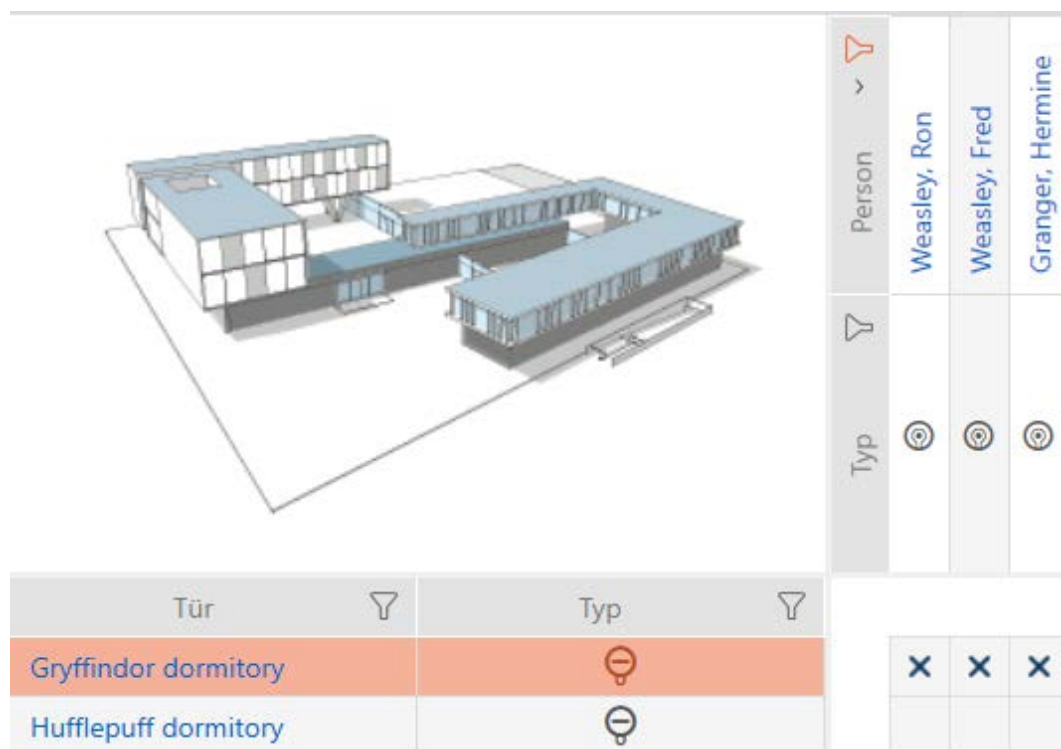



- Select the locking device on which you wish to authorise all identification media to be displayed.

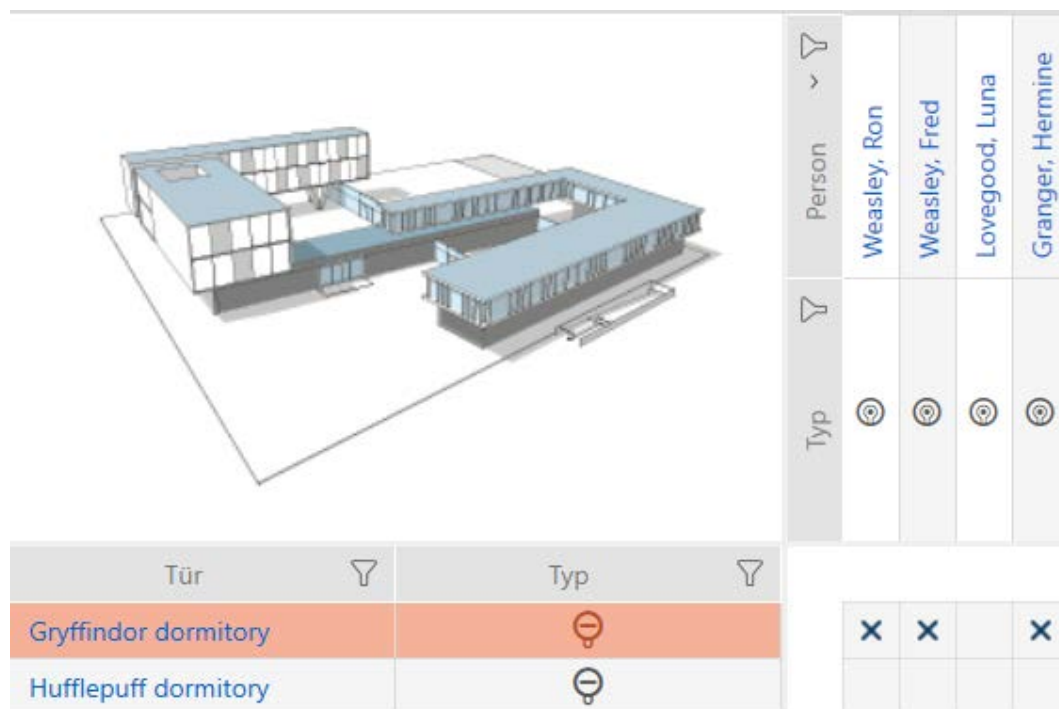


- Click on the **Alle zulassen**  button.

→ All displayed identification media are authorised for the selected locking device.



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:



### 16.2.2 Authorisation groups

Authorisation groups are an easy way for you to set up authorisations for multiple doors and identification media at the same time (see *Authorisation groups* [▶ 543]).

Matrix without authorisations

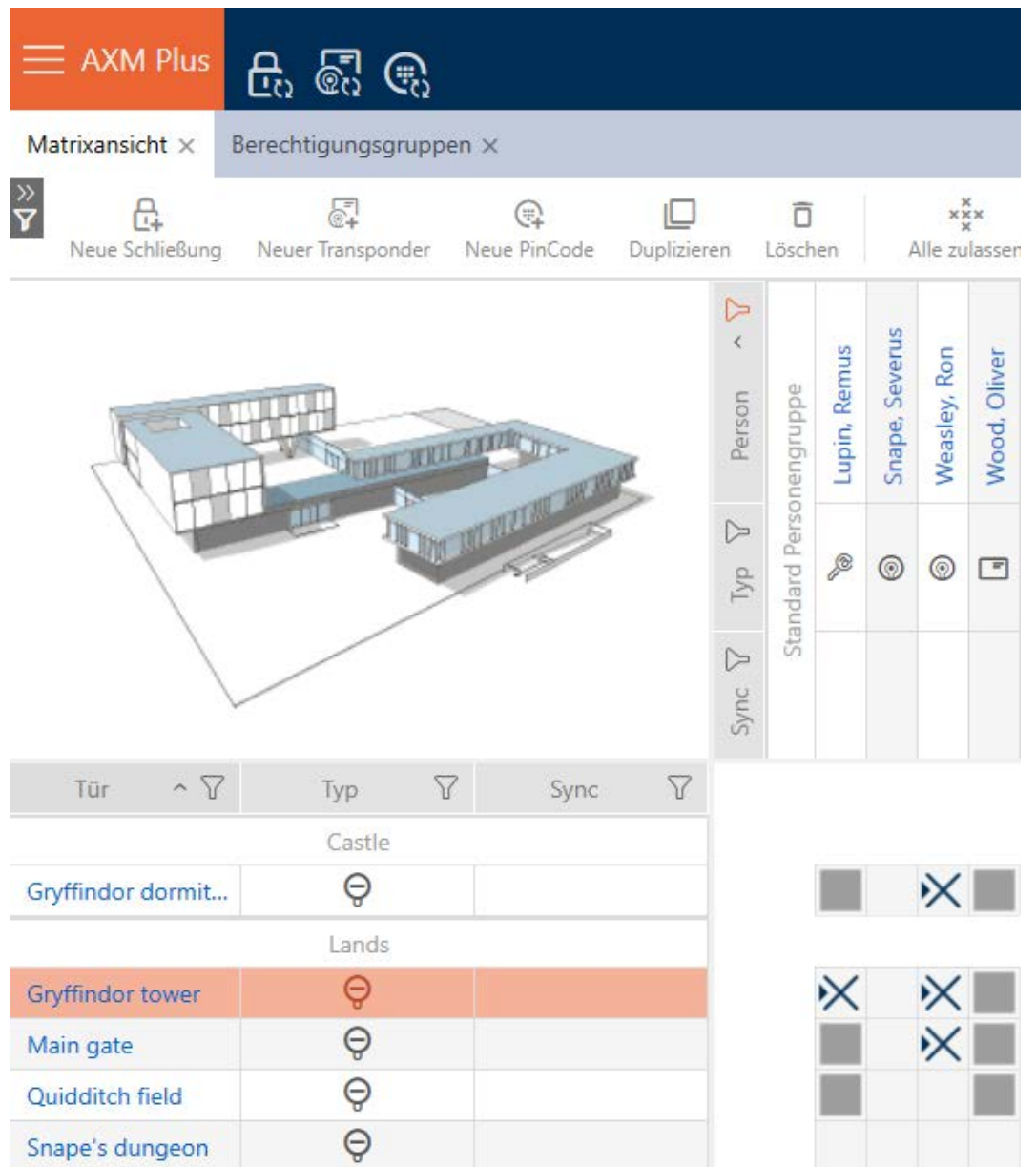
The screenshot shows the AXM Plus software interface. At the top, there is a navigation bar with the 'AXM Plus' logo and several icons. Below this is a 'Matrixansicht' header. A toolbar contains icons for 'Neue Schließung', 'Neuer Transponder', 'Neue PinCode', 'Duplizieren', 'Löschen', and 'Alle zulassen'. The main area features a 3D architectural rendering of a building complex. To the right of the 3D view is a table with columns for 'Person', 'Typ', and 'Sync'. Below the 3D view is another table with columns for 'Tür', 'Typ', and 'Sync'. The 'Quidditch field' row in the bottom table is highlighted in orange.

Person	Typ	Sync
Standard Personengruppe		
Lupin, Remus	🔍	
Snape, Severus	🎯	
Weasley, Ron	🎯	
Wood, Oliver	📄	

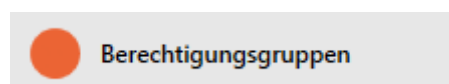
  

Tür	Typ	Sync
Castle		
Gryffindor dormit...	🚫	
Lands		
Gryffindor tower	🚫	
Main gate	🚫	
Quidditch field	🚫	
Snape's dungeon	🚫	

Matrix with authorisation group




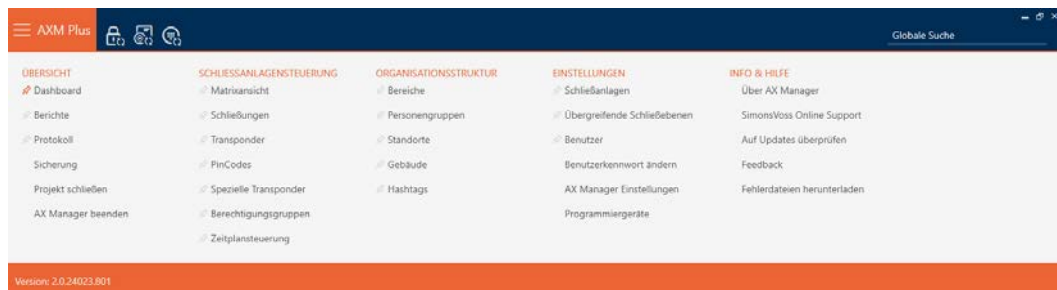
16.2.2.1 Adding locking devices and identification media to authorisation groups  
 Ideally, you will have already created your authorisation groups before creating the locking devices (see *Best practice: setting up the locking system* [▶ 27] and *Creating authorisation groups* [▶ 50]). This allows you to set authorisation groups 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 authorisation groups at a later date:

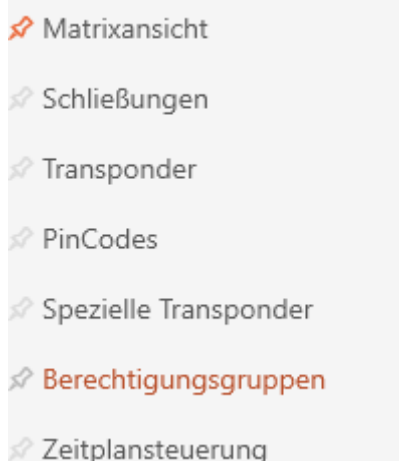
✓ Authorisation group created (see *Creating authorisation groups* [▶ 50]).

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



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

**SCHLISSANLAGENSTEUERUNG**



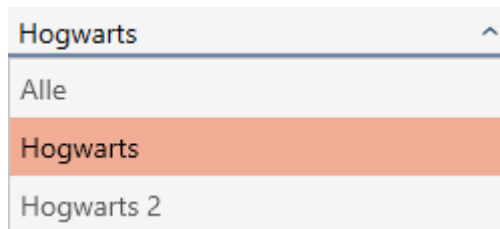
- ↳ The AXM bar will close.
- ↳ The [Access levels] tab will open.

Matrixansicht × Berechtigungsgruppen ×

Neu Löschen Export Anzeigefilter löschen

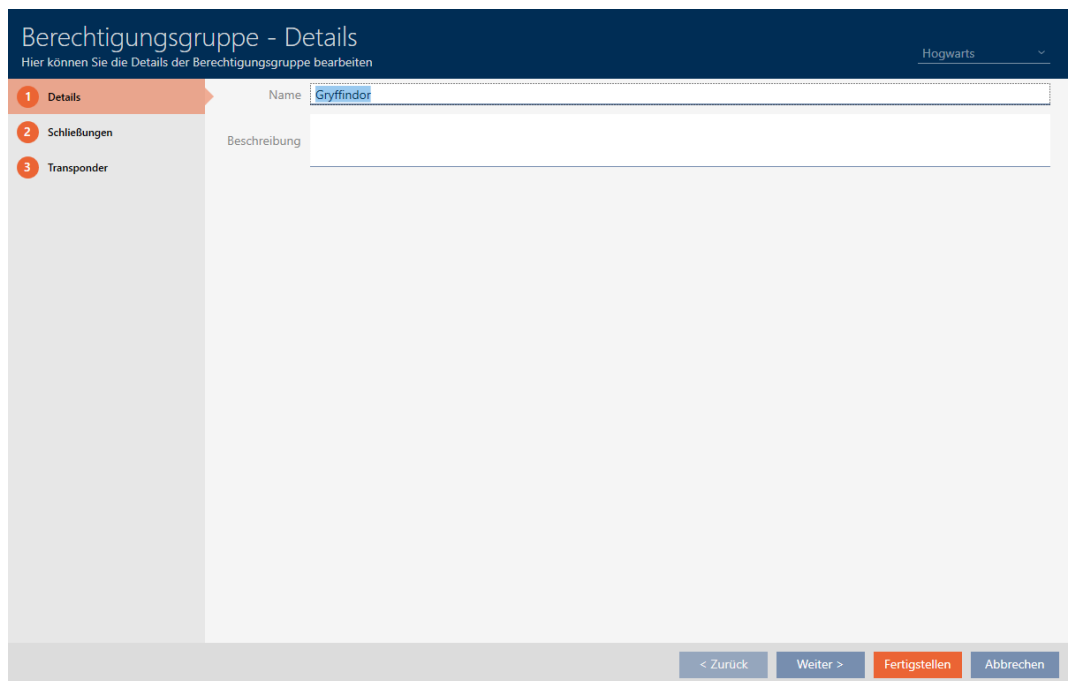
Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder
> Gryffindor		0	0
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

3. Select another locking system in the drop-down menu or select the "All" drop-down entry to display the authorisation groups in all locking systems.

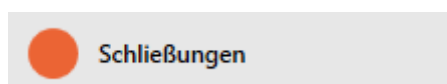


4. Click on the authorisation group to which you wish to add locking devices and identification media.

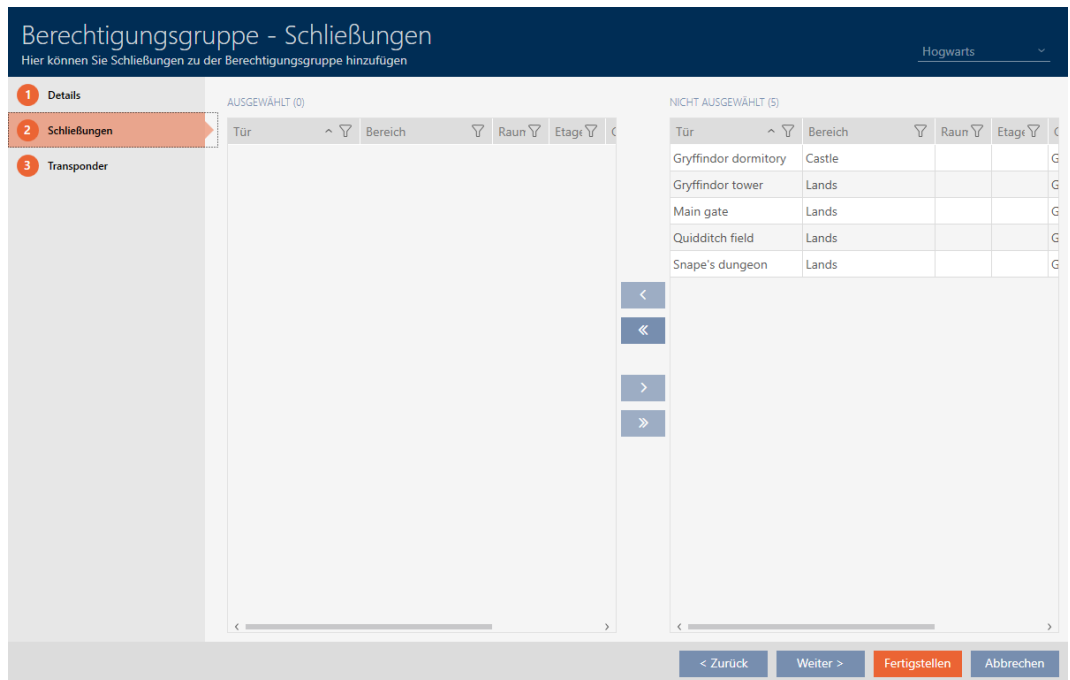
↳ The authorisation group window will open.




5. Click on the **Schließungen** tab.



↳ Window switches to the "Locks" tab.





6. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
7. Select all locking devices that you wish to add to the authorisation group (Ctrl+click for individual devices or Shift+click for multiple devices).

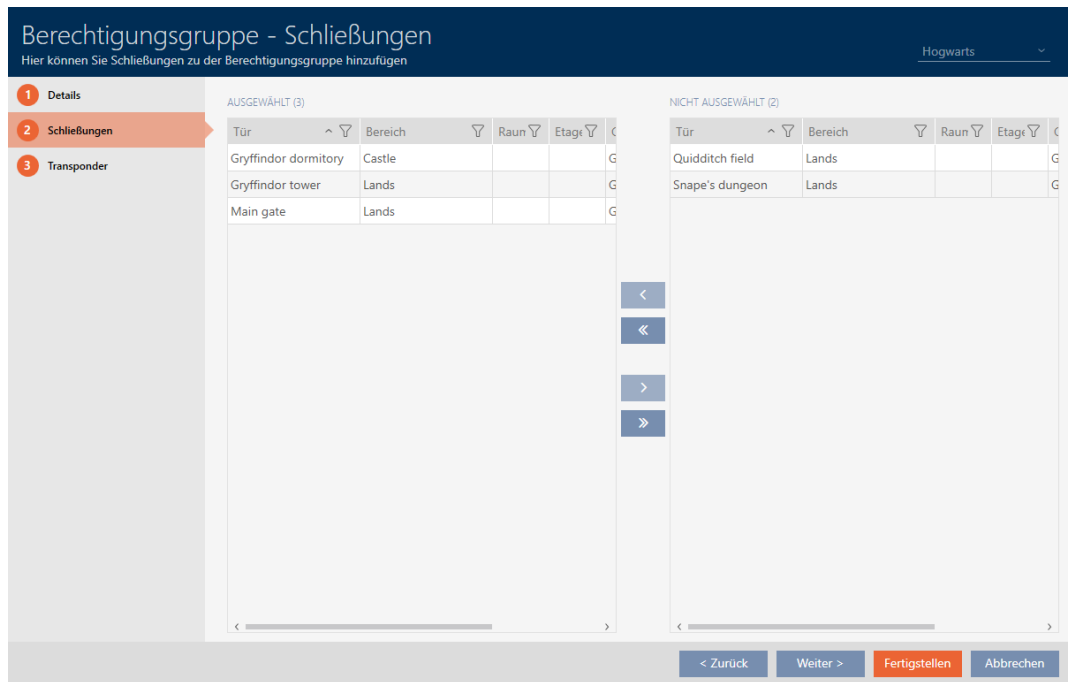


**NOTE**

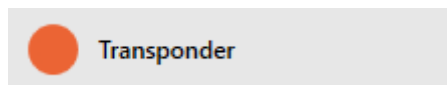
**Double-clicking as an alternative to arrow keys**

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

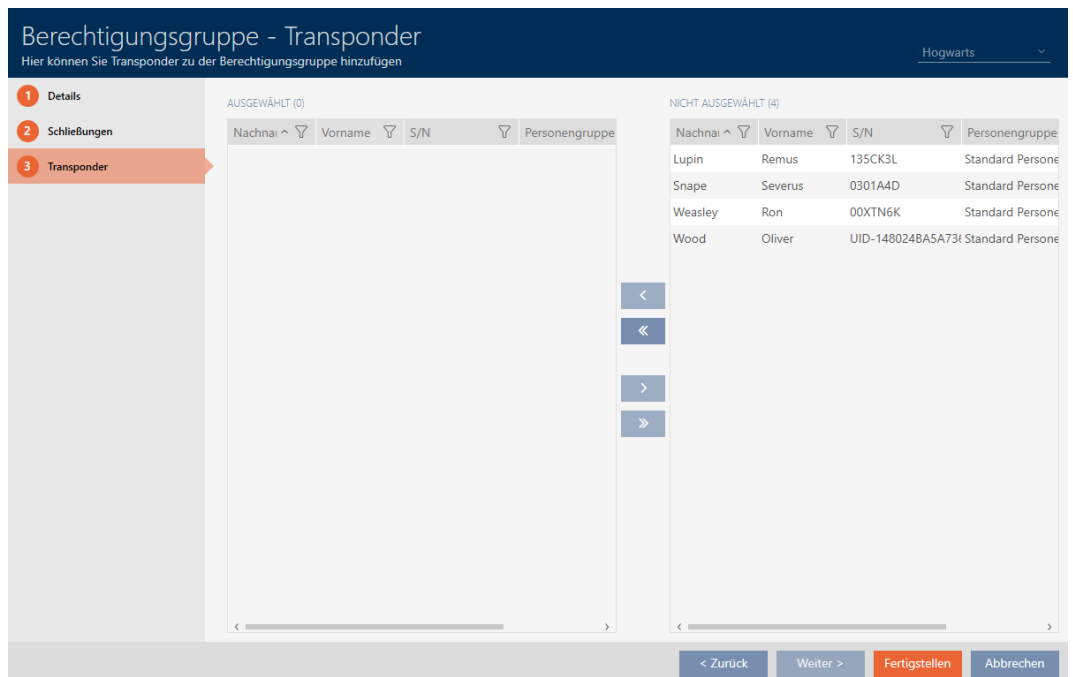
8. Use  to move only the selected locking devices or  to move all locking devices.
  - ↳ The selected locking device in the left-hand column is added to the authorisation group.



9. Click on the  Transponders tab.



↳ Window switches to the "Transponders" tab.



10. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).

11. Select all identification media that you wish to add to the authorisation group (Ctrl+click for individual media or Shift+click for multiple media).





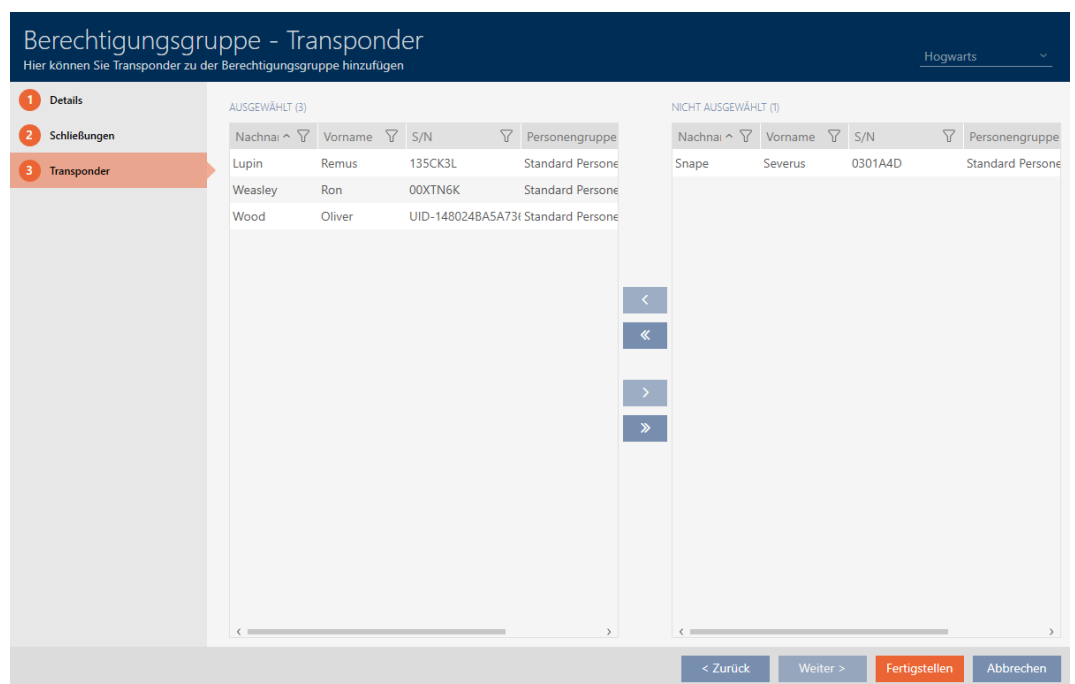



**NOTE**

**Double-clicking as an alternative to arrow keys**

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

12. 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 authorisation group.



13. Click on the **Finish** button.
  - ↳ The authorisation group window closes.
  - ↳ All identification media in this authorisation group are authorised for all locking devices in this authorisation group.
  - ↳ Matrix view is visible again.
14. Click on the **Refresh**  button.
  - ↳ Matrix displays authorisations from your authorisation group (identified by a small triangle next to the cross).

The screenshot shows the AXM Plus interface with a 3D model of a building and a permissions matrix. The matrix is organized as follows:

Tür	Typ	Sync
Castle		
Gryffindor dormit...	⊖	
Lands		
Gryffindor tower	⊖	
Main gate	⊖	
Quidditch field	⊖	
Snape's dungeon	⊖	

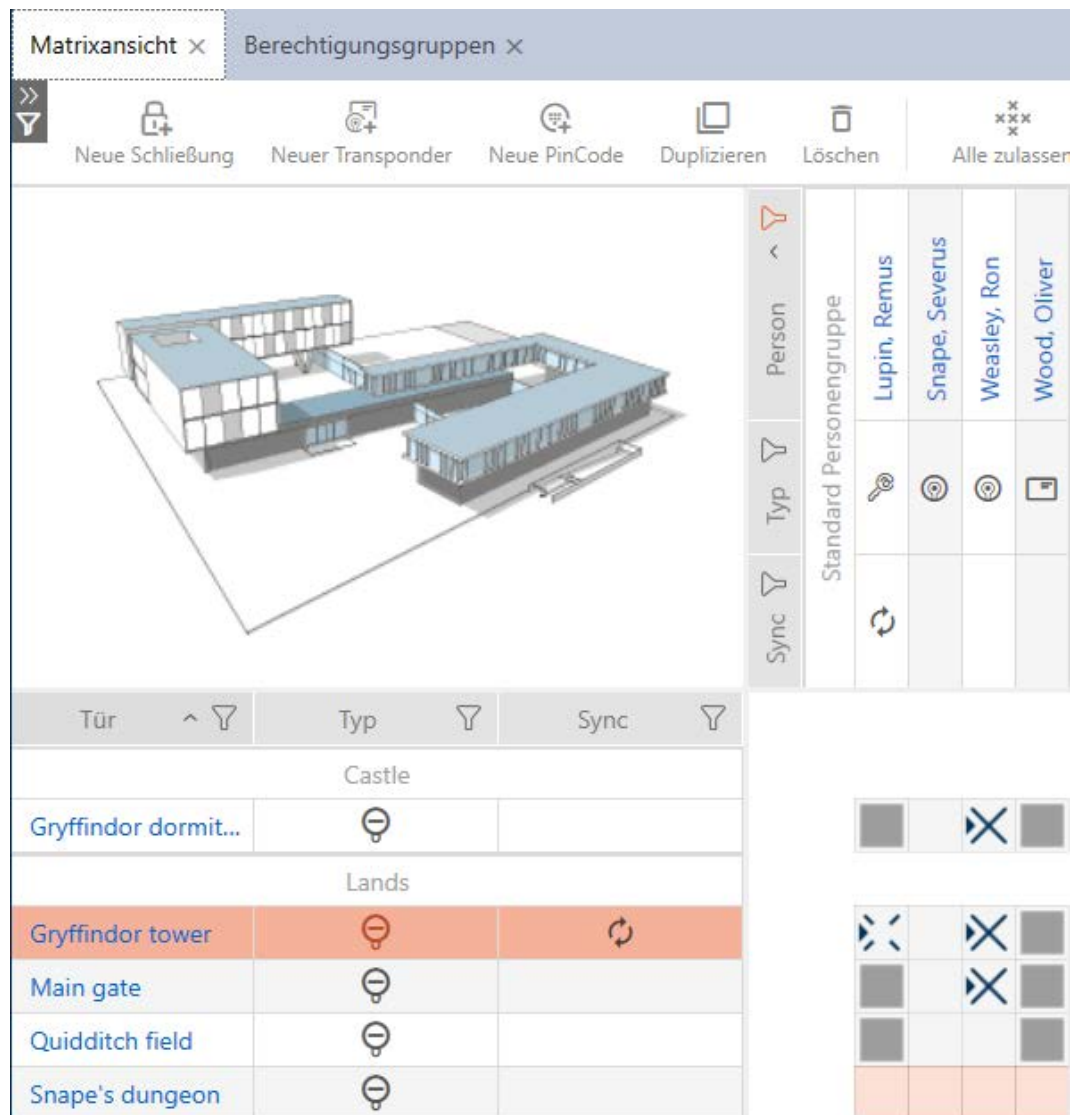
  

Person	Typ	Sync
Lupin, Remus	🔑	
Snape, Severus	⊖	
Weasley, Ron	⊖	
Wood, Oliver	📄	

Below the matrix, there are two 2x2 grids of controls. The top grid shows a grey square, a blue 'X' in a square, and another grey square. The bottom grid shows a blue 'X' in a square, a blue 'X' in a square, a grey square, a grey square, a blue 'X' in a square, and a grey square.

You can also overwrite individual authorisations from authorisation groups 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)* [▶ 317]). In this case, it is only the cross that disappears, not the triangle:

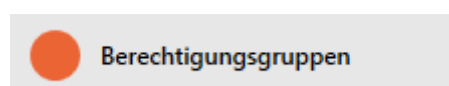


The triangle continues to indicate that there is actually an authorisation from an authorisation group here.

### 16.2.2.2 Adding areas and person groups to authorisation groups


This section explains how to add multiple locking devices to authorisation groups quickly using areas. The process for person groups/identification media is similar.

Ideally, you will have already created your authorisation groups before creating the locking devices (see *Best practice: setting up the locking system* [▶ 27] and *Creating authorisation groups* [▶ 50]). This allows you to set authorisation groups directly in locking device and identification medium properties when you create locking devices and identification media:



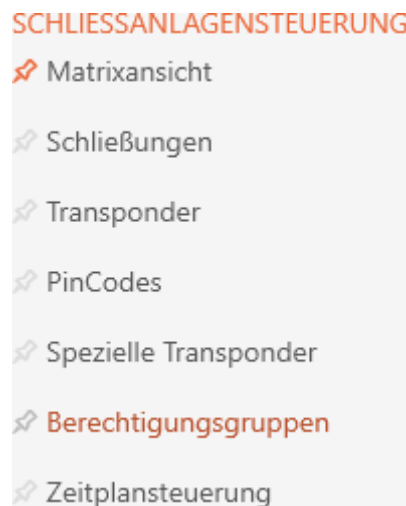
You can use areas to quickly add several locking devices to authorisation groups:

- ✓ Authorisation group created (see *Creating authorisation groups [▶ 50]*).
- ✓ At least one area created (see *Creating an area [▶ 83]*).
- ✓ At least one locking device has been assigned to the area (see *Moving locking devices to areas [▶ 270]*).

1. Click the orange AXM button .
  - ↳ 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.

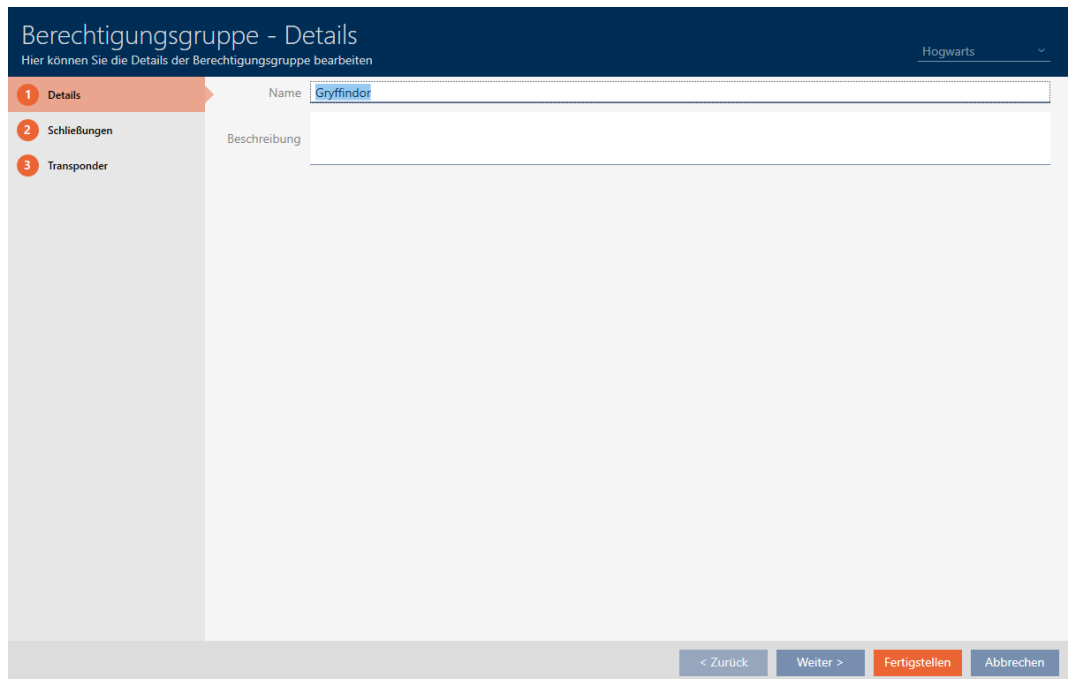
Matrixansicht x		Berechtigungsgruppen x			
Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder		
> Gryffindor		0	0		
Hufflepuff		0	0		
Ravenclaw		0	0		
Slytherin		0	0		

3. Select another locking system in the drop-down menu or select the "All" drop-down entry to display the authorisation groups in all locking systems.

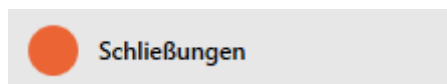


4. Click on the authorisation group to which you wish to add locking devices and identification media.

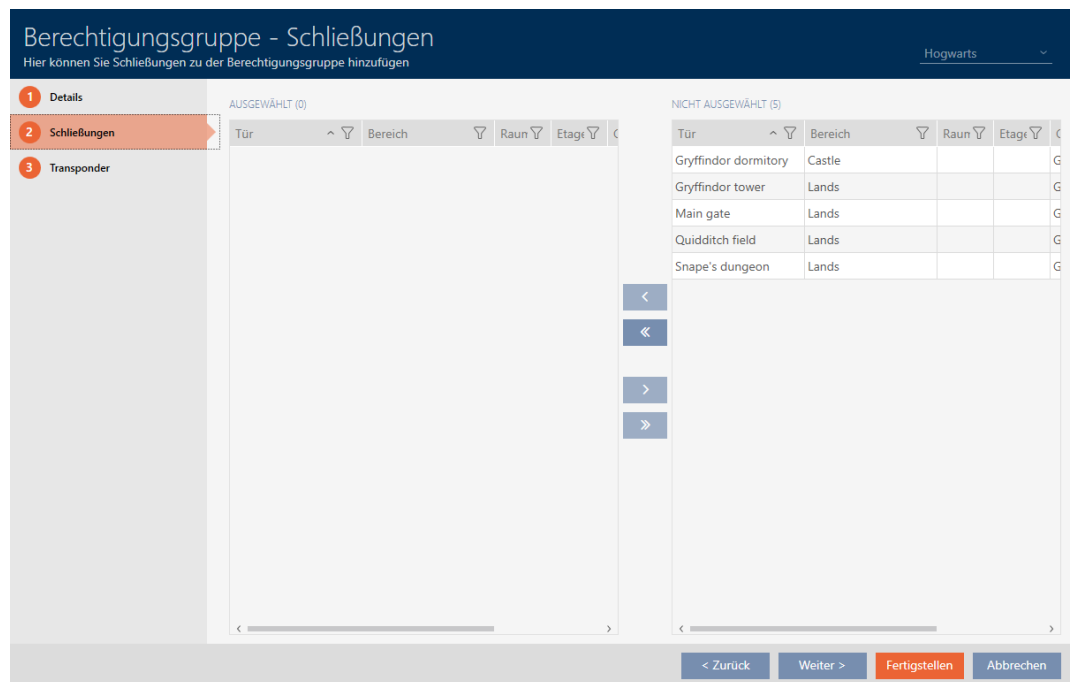
↳ The authorisation group window will open.



5. Click on the **Schließungen** tab.



↳ Window switches to the "Locks" tab.



6. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).



**NOTE**

**Areas as a filter criterion**

Areas can be used as filter criterion, thus simplifying selection of your locking devices.

1. Click the filter icon in the *Area* column.
2. Select one or more areas.



7. Select all locking devices that you wish to add to the authorisation group (Ctrl+click for individual devices or Shift+click for multiple devices).

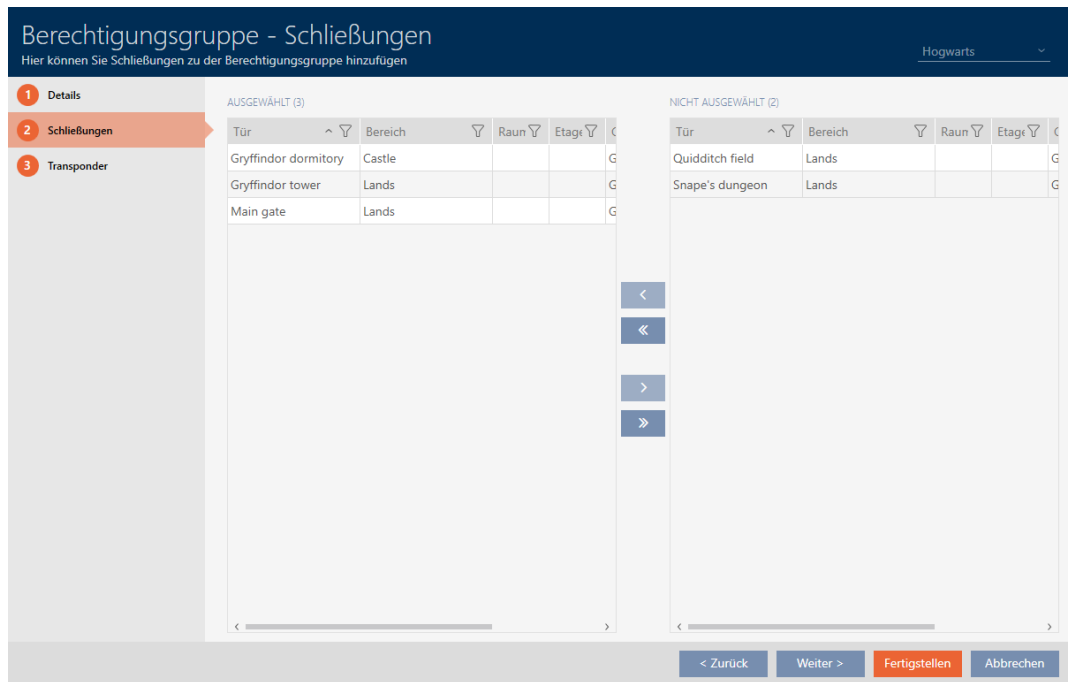



**NOTE**

**Double-clicking as an alternative to arrow keys**

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


8. 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 authorisation group.



9. Click on the **Finish** button.
  - ↳ The authorisation group window closes.
  - ↳ All identification media in this authorisation group are authorised for all locking devices in this authorisation group.
  - ↳ Matrix view is visible again.
10. Click on the **Refresh**  button.
  - ↳ Matrix displays authorisations from your authorisation group (identified by a small triangle next to the cross).

### 16.2.2.3 Show all authorisation groups in a project

- ✓ At least one authorisation group created (see *Creating authorisation groups* [▶ 50]).

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



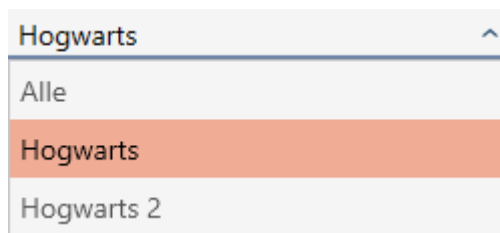
2. Select the **Access levels** entry in the | LOCKING SYSTEM CONTROL | group.
  - ↳ The AXM bar will close.
  - ↳ The [Access levels] tab will open.

Matrixansicht x Berechtigungsgruppen x

Neu Löschen Export Anzeigefilter löschen

Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder
> Gryffindor		3	3
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

3. Select the "All" entry for the locking system from the drop-down menu.



↳ All authorisation groups in all locking systems in the same project are displayed.

Matrixansicht x Berechtigungsgruppen x

Neu Löschen Export Anzeigefilter löschen

Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder
> Deatheaters		0	0
Gryffindor		3	3
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

You can also export the authorisation groups displayed as a list (see *Exporting authorisation groups as a list* [▶ 336]).

#### 16.2.2.4 Exporting authorisation groups as a list


All authorisation groups in your locking system can be exported as a PDF.

The PDF shows exactly the same authorisation groups in exactly the same order as in AXM Plus.

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

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

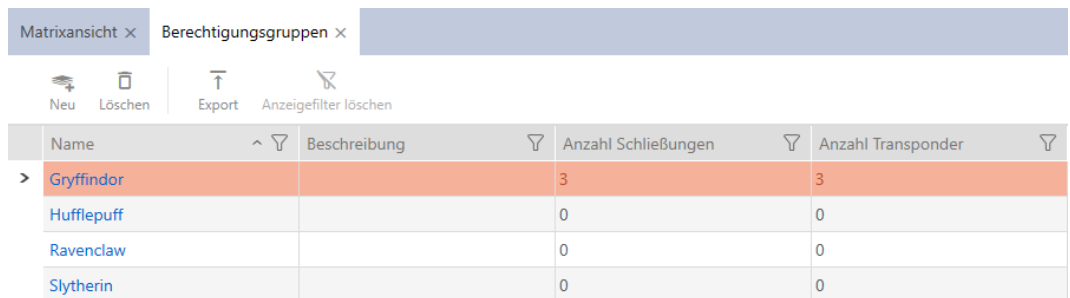
✓ At least one authorisation group created (see *Creating authorisation groups* [▶ 50]).

1. Click on the orange AXM icon .
  - ↳ 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. Select a specific locking system or all locking systems with the authorisation groups to be exported from the drop-down menu.



4. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
5. Click on the **Export** button.
  - ↳ The Explorer window will open.
6. Save the PDF file to a directory of your choice.
  - ↳ Explorer window closes.
- ↳ The identification media displayed are exported as a PDF file (DIN A4).



**Alle Berechtigungsgruppen für die Schließanlage 'Hogwarts 1'**

Name	Anzahl Schließungen	Anzahl Transponder
Gryffindor	1	3
Hufflepuff	0	0
Ravenclaw	0	0
Slytherin	0	0

### 16.2.3 Controlling authorisations in terms of time (schedules)

Time management in AXM Plus comprises:

- Time schedules for locking devices
- Time groups for transponders

You can find a detailed description and an example here: *Event management* [▶ 528].

You can only create time groups using a schedule in AXM Plus. The first step after creating a concept is therefore a schedule: *Creating a schedule* [▶ 53].

#### 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.

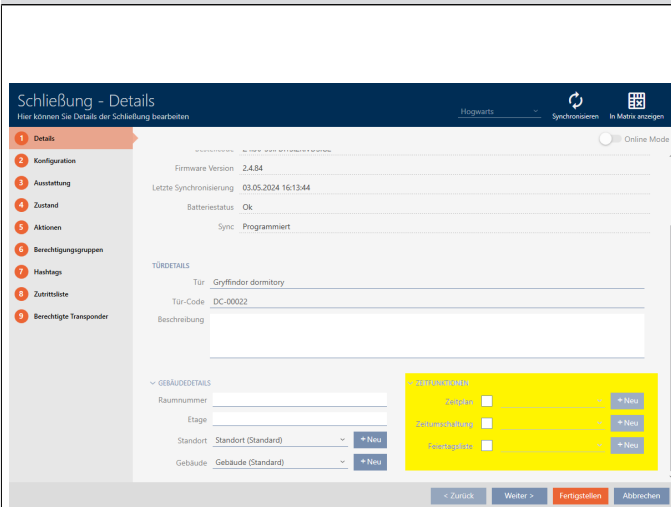
#### 16.2.3.1 Adding locking devices to the schedule

Ideally, you should create your schedules before the locking devices (see *Best practice: setting up the locking system* [▶ 27]). You can then add your locking devices to the schedule while you are creating each locking device (see *Creating a locking device* [▶ 228]).

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.

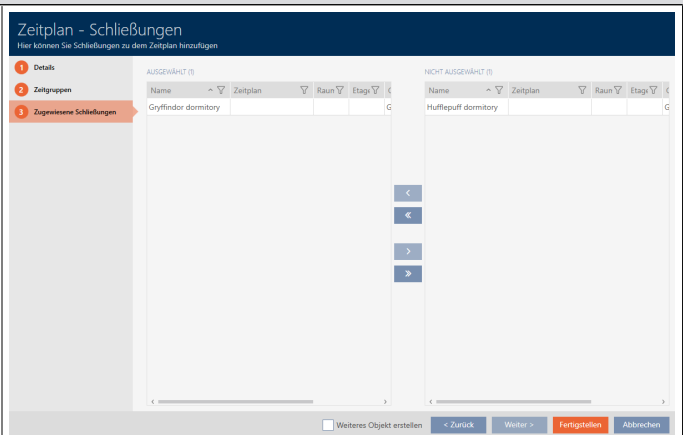
There are two ways to do this:

Locking device window



- Can be used directly when creating the locking device
- Only one locking device possible per access point

Schedule window

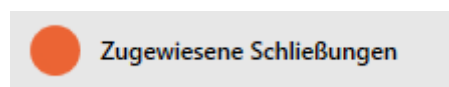


- Can be used directly when creating the schedule
- Multiple locking operations possible per access point
- Ranges can be used as filter criteria (see *Add area, including locking devices, to a schedule* [▶ 345]).

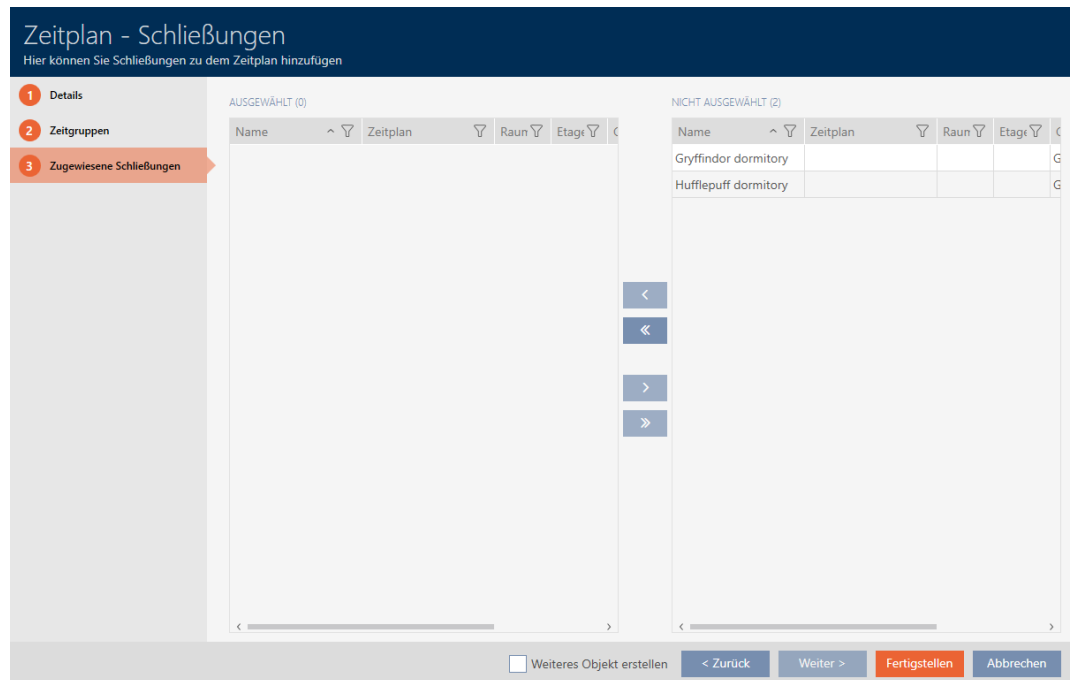
In this section, you will learn how to add locking devices to a schedule in the time schedule window (see *Limiting authorisations for locking devices to specific times (schedule)* [▶ 276] for adding using the locking device properties).


- ✓ Schedule created (see *Creating a schedule* [▶ 53]).
- ✓ Schedule window open (see *Creating a schedule* [▶ 53]).
- ✓ 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* [▶ 44]).
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.



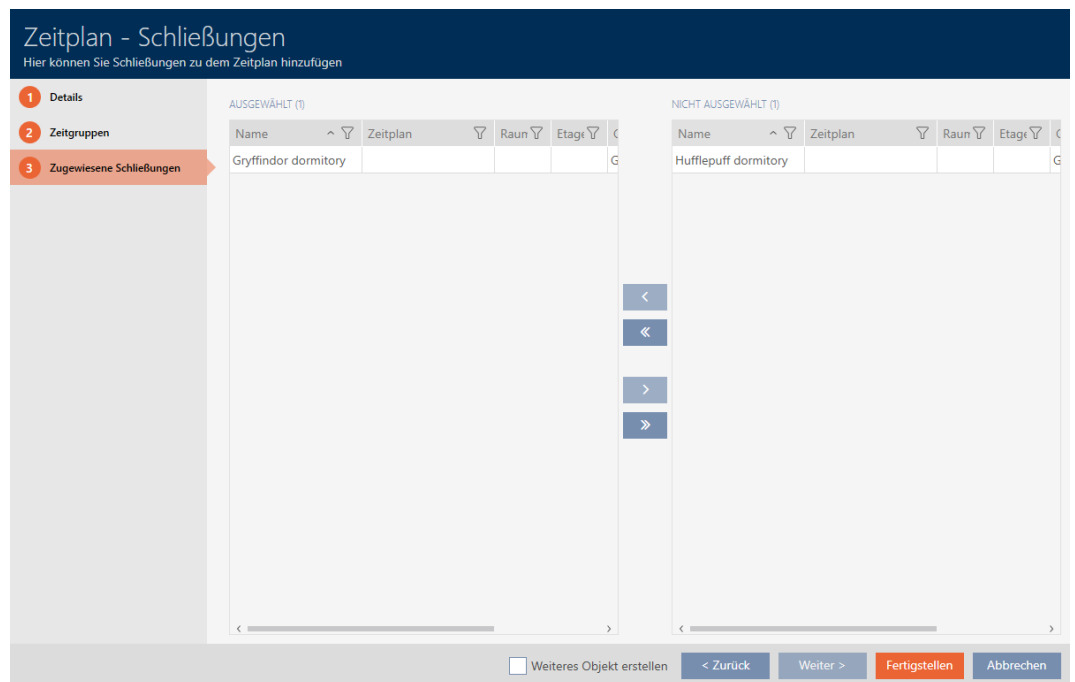
**NOTE**

**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.

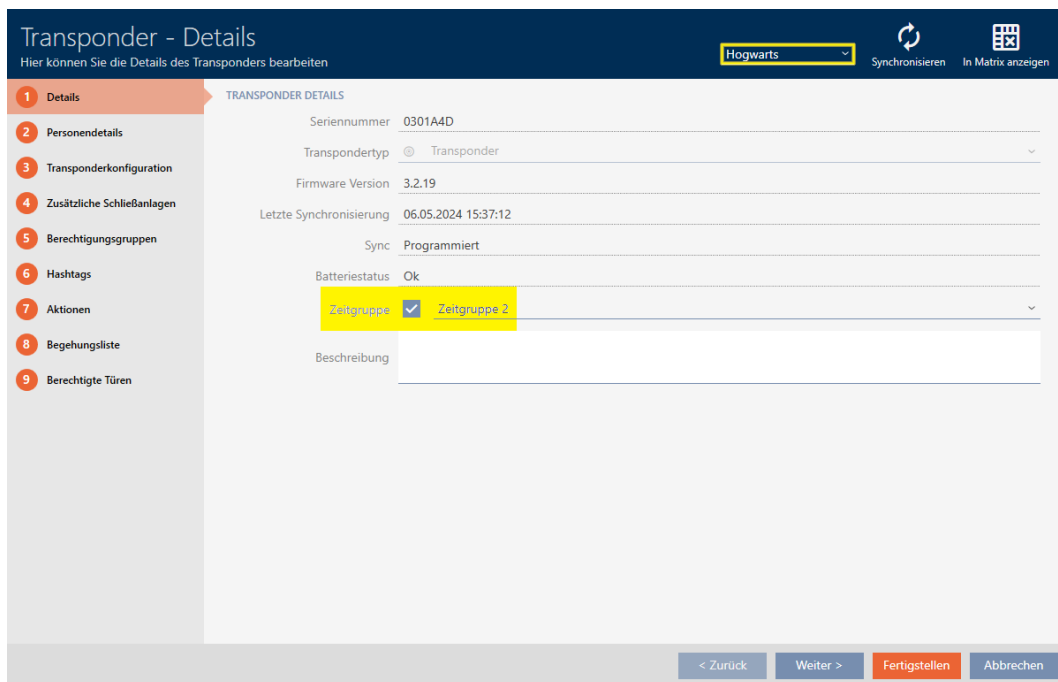
### 16.2.3.2 Adding identification medium to time group

Ideally, you should create your time groups before the locking devices (see *Best practice: setting up the locking system* [▶ 27]). You can then add your identification media to the time groups when you create them (see *Creating an identification medium* [▶ 88]).

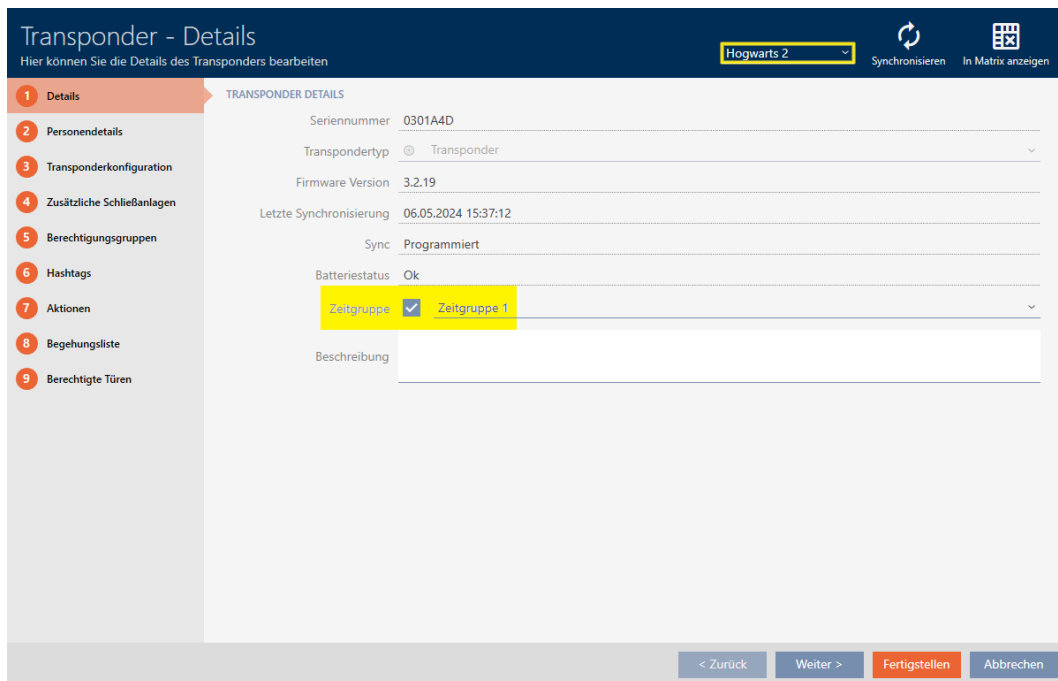
An identification medium can only be added to a time group in its properties.

#### Time groups with multiple locking systems

You can use identification media in multiple locking systems (see *Reuse identification medium in the same project* [▶ 202] and *Reusing identification medium in other projects/databases* [▶ 208]). 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/AX2Go key to time group

Transponder - Details  
Hier können Sie die Details des Transponders bearbeiten

Hogwarts Synchronisieren In Matrix anzeigen

1 Details  
2 Personendetails  
3 Transponderkonfiguration  
4 Zusätzliche Schließanlagen  
5 Berechtigungsgruppen  
6 Hashtags  
7 Aktionen  
8 Begehungsliste  
9 Berechtigte Türen

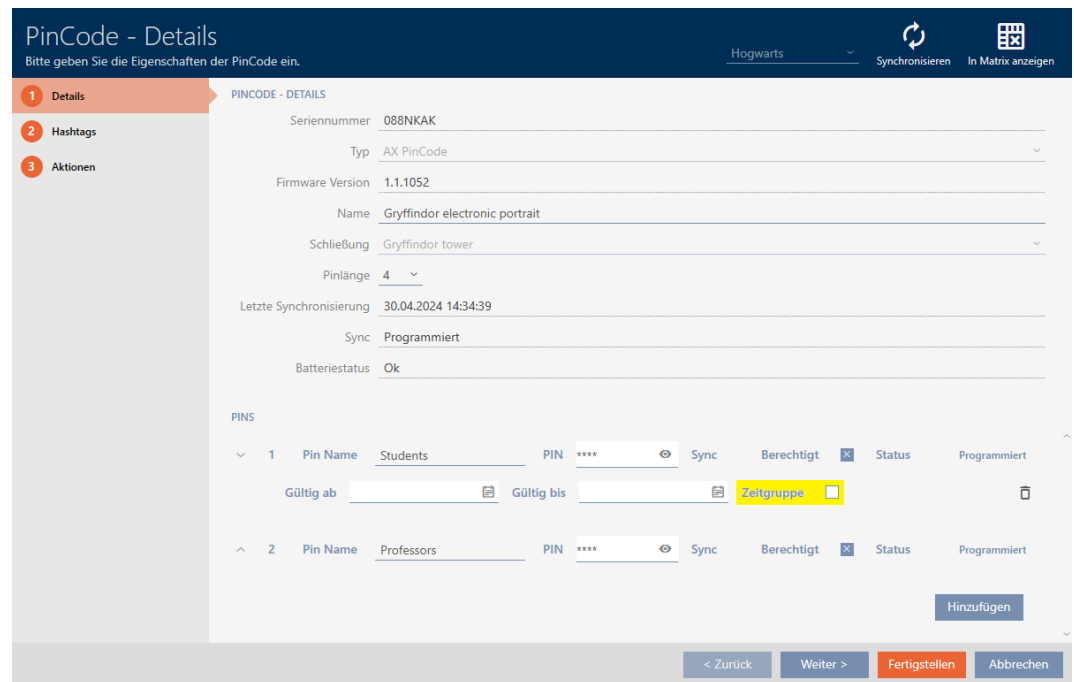
TRANSPONDER DETAILS

Seriennummer 00XTN6K  
Transpondertyp Transponder  
Firmware Version 3.2.19  
Letzte Synchronisierung 25.04.2024 14:52:24  
Sync Programmiert  
Batteriestatus Ok  
Zeitgruppe  Zeitgruppe 1  
Beschreibung

< Zurück Weiter > Fertigstellen Abbrechen

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.

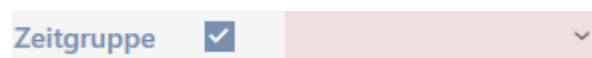
Adding PINs from a PIN code keypad to the time group



✓ PIN code keypad created with PINs (see *Creating PIN code keypads* [[▶ 96](#)]).

✓ Time groups created (see *Create time group* [[▶ 56](#)]).

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.






### 16.2.3.3 Add area, including locking devices, to a schedule

Ideally, you should create your schedules before the locking devices (see *Best practice: setting up the locking system* [▶ 27]). You can then add your locking devices to the schedule while you are creating each locking device (see *Creating a locking device* [▶ 228]).

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.

In this section, you will learn how to add an entire area, including locking devices, to a schedule in the schedule window (see *Limiting authorisations for locking devices to specific times (schedule)* [▶ 276] for adding individual locking devices using the locking device properties).

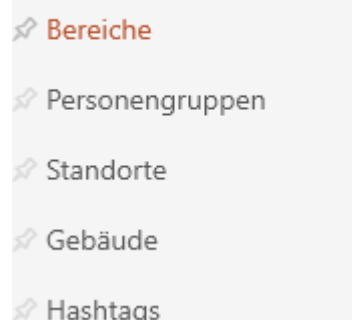
- ✓ Schedule created (see *Creating a schedule* [▶ 53]).
- ✓ Area created (see *Creating an area* [▶ 83]).
- ✓ Locking devices in the area (see *Moving locking devices to areas* [▶ 270]).
- ✓ Locking device equipped with .ZK option.

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



2. Select the **Area** entry in the | LOCKING SYSTEM CONTROL | group.

#### ORGANISATIONSTRUKTUR



- ↳ The [Areas] tab will open.

Name	Zeitplan	Beschreibung
Castle		
Lands		

3. Select the locking system with the area you want to assign to a time group in the top right-hand corner (alternatively: "All").
4. Click on the area you want to assign to a time group.
  - ↳ The "Area" window will open.

**Bereich - Details**  
Hier können Sie die Details des Bereichs bearbeiten

1 Details

2 Schließungen

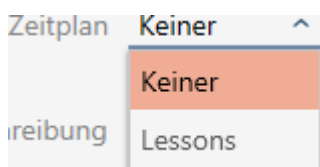
Name:

Zeitplan:

Beschreibung:

< Zurück   Weiter >   Fertigstellen   Abbrechen

5. Select the required schedule from the ▼ Time schedule drop-down menu.



6. Click on the **Finish** button.
  - ↳ "Area" window closes.
  - ↳ Area, including locking devices, added to the schedule.

Matrixansicht × Bereiche ×		
Name	Zeitplan	Beschreibung
> Castle	Lessons	
Lands		

Locking devices within an area with a schedule can also be assigned a different schedule or no schedule at all. To do so, select another schedule from the ▼ **Time schedule** drop-down menu.

### Behaviour of inherited schedules

You can recognise inherited schedules by the suffix ("inherited").

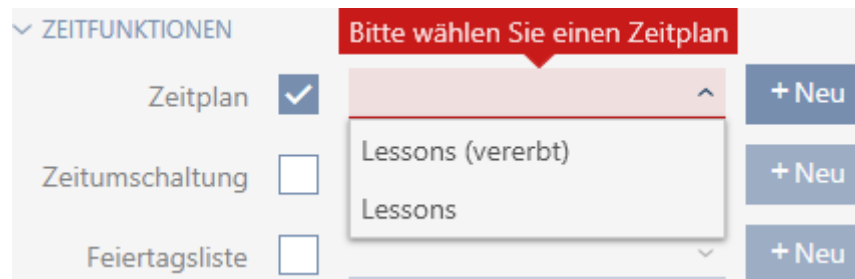
- Newly created locking devices inherit the schedule if they are assigned to an area with a schedule during their creation.
- Locking devices that have already been created but never synchronised inherit the schedule if they are assigned to an area with a schedule.
- Locking devices with inherited schedules adopt the area's schedule, even if it is changed in the area
  - If the schedule is removed from the area, locking devices that have inherited it will also no longer have the schedule.
  - If you assign a different schedule to the area, the schedule also changes for the locking devices that inherit the schedule.
- Locking devices that have already been synchronised with an inherited schedule inherit the schedule of the new area if a new area with a schedule is assigned to them.
- Locking devices that have already been synchronised with an inherited schedule will no longer have the schedule if they are assigned a new area without a schedule.
- Locking devices that have already been synchronised in an area without a schedule inherit the schedule if a schedule is assigned to their area.
- Locking devices with a manually assigned schedule retain this schedule, even if they are assigned to an area with a schedule.

### Inheriting a schedule from existing and synchronised locking devices

In some cases, locking devices do not automatically inherit the schedule for security reasons. You can still configure this "inherit" relationship for the schedule manually:

1. Select the  Time schedule checkbox in the details for the locking devices concerned.

2. Then select the entry with the suffix "inherited".



3. Click on the **Finish** button.

↳ Locking device inherits the area's schedule.

### 16.3 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 authorisation group in the database, but not programmed yet.
	Authorised and programmed by an authorisation group.
	Authorisation available and programmed by an authorisation group; this authorisation has been removed manually. Authorisation removal not programmed yet.
	Authorisation by an authorisation group 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.

## 17. Locking systems

### 17.1 Create locking system

With AXM Plus, you have the freedom to use multiple locking systems (see *Locking systems* [▶ 521] for background information on locking systems).

You have probably already created your first locking system with the wizard after starting your project (see *First steps after a new installation* [▶ 25]). You can create additional locking systems in the [Locking systems] tab:


#### 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.

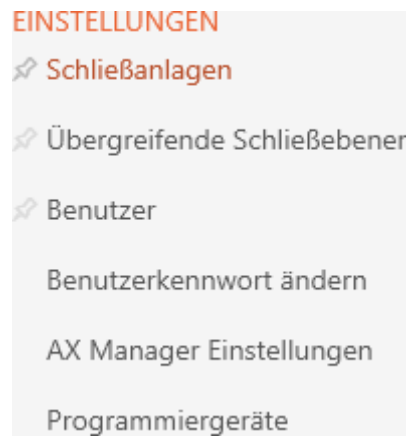
It is no longer possible to program components if the locking system password is no longer known or can no longer be recovered from a backup. The components must be removed from locks and disposed of, which takes a great deal of effort.

1. Ensure that authorised persons can 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).

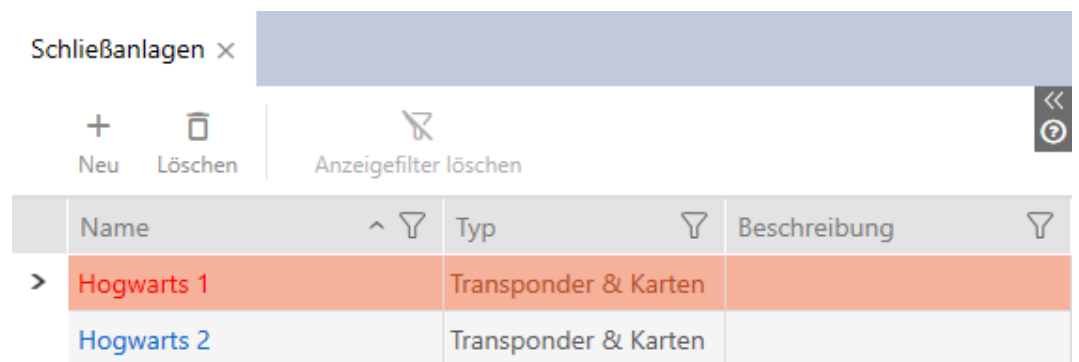
1. Click on the orange AXM icon .   
↳ AXM bar opens.



- Select the **Locking systems** entry in the | SETTINGS | group.

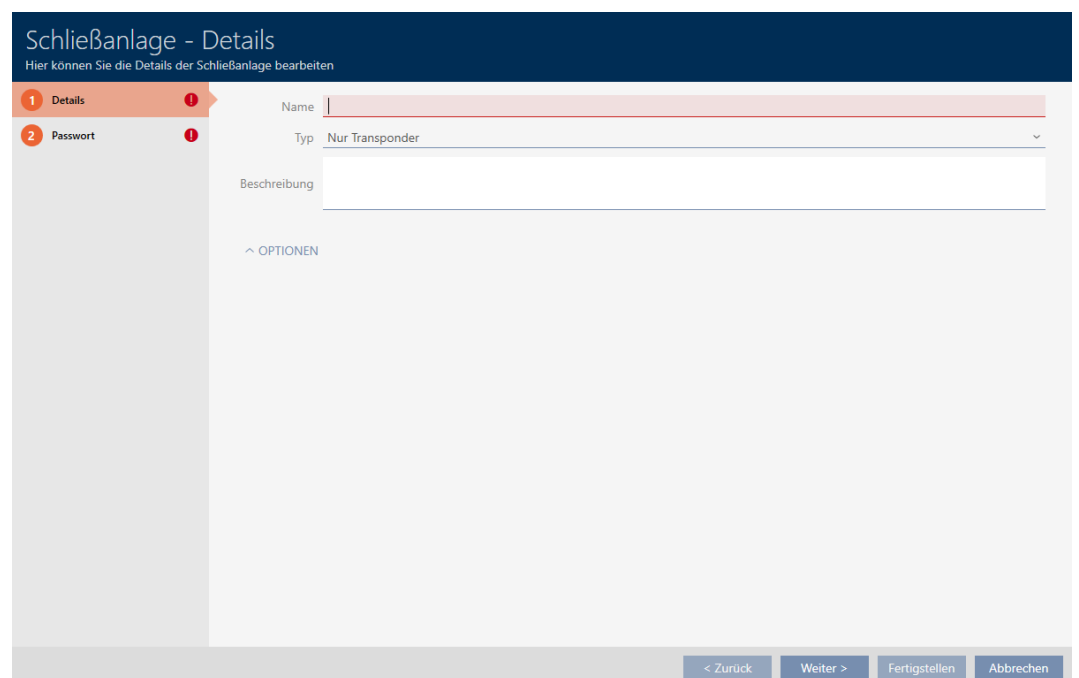


- ↳ The [Locking systems] tab with a list of all locking systems in the database will open.

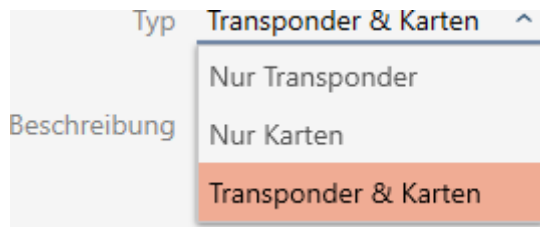


- Click on the **New** button **+**.

- ↳ The Locking system window will open.



4. Enter a name for your locking system in the *Name* field.
5. Select which identification media your locking system should support ("Transponders only", "Cards only" or "Transponders & cards") from the ▼ **Type** drop-down menu.




#### NOTE

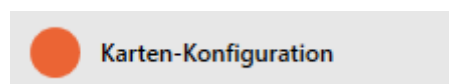
##### Do not activate cards as a “precaution”


Cards (or RFID inlays, tags, etc.) have limited storage space. For this reason, only a limited number of locking device IDs from your locking system can be used with cards (see *Cards and locking device IDs* [▶ 552]). You can find the exact number in Section *Card templates* [▶ 556] – the locking device IDs 0 to 127 are reserved for internal purposes.

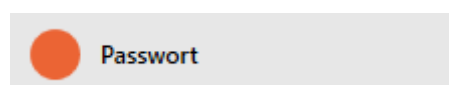
Example: MC1000L\_AV uses locking device IDs 0-1127. You can create 64,000 locking devices and use them for transponders, but only 1,000 of them can be used for your cards (namely those with a locking device ID between 128 and 1127).

1. Select "Transponder" if you do not expect cards or similar RFID identification media to be used.
2. Activate cards later if required (see *Enable cards or transponders* [▶ 389]).

↳ The  **Card configurations** tab is displayed for "Cards only" or "Transponders & cards".



6. Enter a description in the *Description* field if required.
7. Click on the  **Password** tab



↳ Window switches to the "Password" tab.

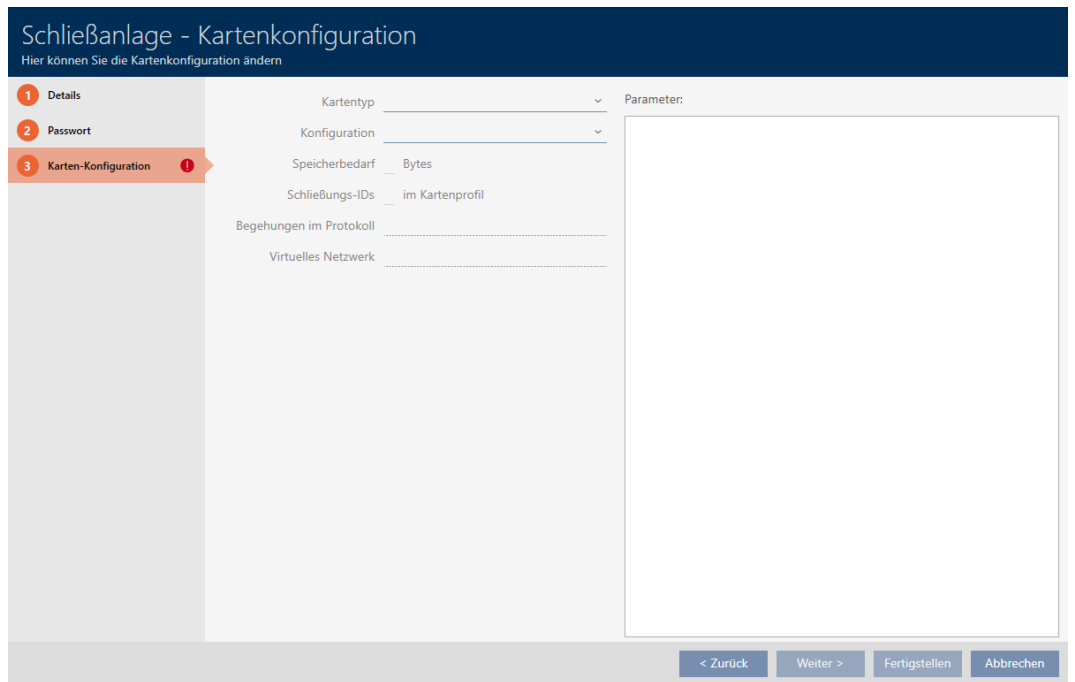
8. Enter the locking system password for your new locking system in the *Password* field.
9. Re-enter the locking system password in the *Confirm password* field.
  - ↳ A coloured bar shows you how secure your password is.

Quality



- ↳ If your locking system is "Transponders only" and you do not want to use a common locking level, you are now finished.
10. Use the **Card configurations** button to switch to the next tab or complete the entries with the **Finish** button.
    - ↳ Window switches to the "Card configurations" tab.

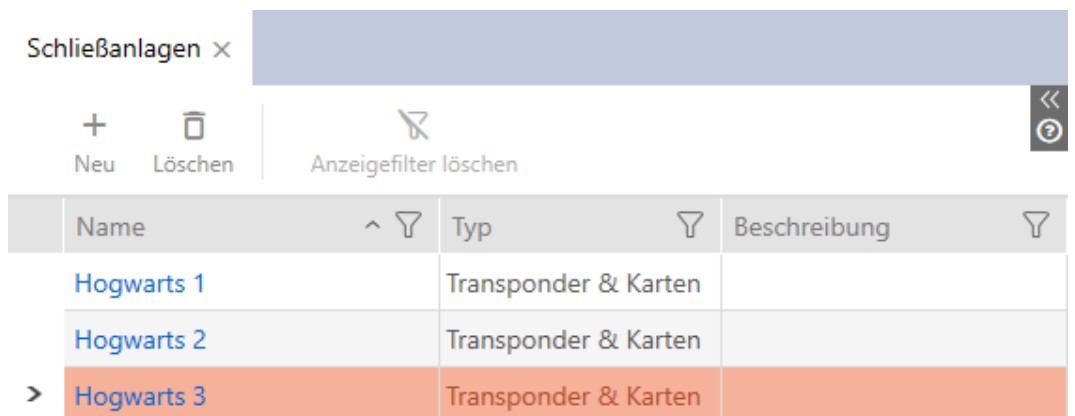




11. Enter your card configuration here (see *Adding a card configuration* [▶ 354] for card configuration).
12. Click the **Finish** or **Next >** button to assign the locking system to a common locking level.



13. Click on the **Finish** button.
  - ↳ Window "Locking system" closes.
  - ↳ New locking system is listed.

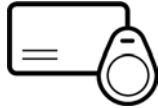


You can find information on your locking system's structure sequence here:  
*Best practice: setting up the locking system* [▶ 27].

17.1.1 Adding a card configuration

The following sections describe how to determine a card configuration for your locking system and how to configure it in your AXM Plus .

Available RFID identification media



The description refers to “cards”. However, the procedure is similar for all supported RFID identification media; for example:

- Cards
- Smart tags
- RFID inlays



**NOTE**

**Card analysis by SimonsVoss**



Analysing your cards and finding the right card configuration for trouble-free operation can be challenging, especially when it comes to cards already in use.

That's why SimonsVoss offers you to help.

1. If you decide to have SimonsVoss check your cards, please contact one of our sales representatives in your region.
2. If you want to determine the card configuration yourself: Read through the following sections carefully.

**Basis: MIFARE DESFire and MIFARE Classic**

MIFARE DESFire and MIFARE Classic encryption technologies are the most important for RFID identification media:

MIFARE Classic	MIFARE DESFire
<ul style="list-style-type: none"> <li>■ Easy protection</li> <li>■ Inexpensive identification media</li> <li>■ Limited performance</li> <li>■ Memory as numbers/letter sequence</li> </ul> 	<ul style="list-style-type: none"> <li>■ Effective protection</li> <li>■ High-performance identification media</li> <li>■ Memory as a file system</li> <li>■ More flexible handling</li> </ul> 

MIFARE Classic	MIFARE DESFire
MIFARE Classic encryption is now considered non-secure. SimonsVoss therefore recommends using MIFARE DESFire only.	

MIFARE Classic	MIFARE DESFire																									
<ul style="list-style-type: none"> <li>■ Data stored in sectors</li> <li>■ Addressing with sectors in sector list</li> <li>■ Sector protection using the last block in sector</li> <li>■ MIFARE Classic encryption hacked and now insecure</li> </ul>	<ul style="list-style-type: none"> <li>■ Data saved in files</li> <li>■ Addressing with application ID</li> <li>■ File backed up by file read key</li> <li>■ Locking system data must be stored in an application file. Read access is required to the file.</li> <li>■ Encryption with AES (128 bit)</li> </ul>																									
<p>Distribution of the memory:</p> <table border="1" style="margin-left: 20px;"> <tr> <td>MAD information</td> <td>MAD information</td> <td>MAD information</td> <td>16B Safe Block</td> <td>Sector 0</td> </tr> <tr> <td>16B Block data</td> <td>16B Block data</td> <td>16B Block data</td> <td>16B Safe Block</td> <td>Sector 1</td> </tr> <tr> <td>16B Block data</td> <td>16B Block data</td> <td>16B Block data</td> <td>16B Safe Block</td> <td>Sector 2</td> </tr> <tr> <td>16B Block data</td> <td>16B Block data</td> <td>16B Block data</td> <td>16B Safe Block</td> <td>...</td> </tr> <tr> <td>16B Block data</td> <td>16B Block data</td> <td>16B Block data</td> <td>16B Safe Block</td> <td>Sector X</td> </tr> </table>	MAD information	MAD information	MAD information	16B Safe Block	Sector 0	16B Block data	16B Block data	16B Block data	16B Safe Block	Sector 1	16B Block data	16B Block data	16B Block data	16B Safe Block	Sector 2	16B Block data	16B Block data	16B Block data	16B Safe Block	...	16B Block data	16B Block data	16B Block data	16B Safe Block	Sector X	<p>Distribution of the memory:</p> <div style="margin-left: 20px;"> <div style="border: 1px solid black; padding: 5px; margin-bottom: 10px;"> <p>Application X</p> <div style="background-color: #f08080; width: 100px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: #ffff00; width: 100px; height: 15px;"></div> </div> <div style="border: 1px solid black; padding: 5px;"> <p>Application Y</p> <div style="background-color: #90ee90; width: 100px; height: 15px; margin-bottom: 5px;"></div> <div style="background-color: #add8e6; width: 100px; height: 15px;"></div> </div> </div>
MAD information	MAD information	MAD information	16B Safe Block	Sector 0																						
16B Block data	16B Block data	16B Block data	16B Safe Block	Sector 1																						
16B Block data	16B Block data	16B Block data	16B Safe Block	Sector 2																						
16B Block data	16B Block data	16B Block data	16B Safe Block	...																						
16B Block data	16B Block data	16B Block data	16B Safe Block	Sector X																						

## Determine the values to be entered in advance

Schließenanlage - Kartenkonfiguration  
Hier können Sie die Kartenkonfiguration ändern

1 Details  
2 Passwort  
3 Karten-Konfiguration

Kartentyp  
Konfiguration  
Speicherbedarf Bytes  
Schließungs-IDs im Kartenprofil  
Begehungen im Protokoll  
Virtuelles Netzwerk

Parameter:

< Zurück Weiter > Fertigstellen Abbrechen

You need to determine the values before entering them. An NFC-compatible smartphone is ideal for reading your cards. The examples show Android with NXP's TagInfo app (<https://play.google.com/store/apps/details?id=com.NXP.taginfo>). The required report is the "full report".



Make a note of the values determined. You proceed with this in a different way, depending on the situation:

- *MIFARE Classic (new/empty card)* [▶ 357]
- *MIFARE Classic (card already used)* [▶ 362]
- *MIFARE DESFire (new/empty card)* [▶ 370]
- *MIFARE DESFire (card already in use)* [▶ 376]

You can then enter the values for the card configuration.

### Entering the card configuration

- ✓ "Locking system - Card configuration" tab open (see *Create locking system* [▶ 349] or *Enable cards or transponders* [▶ 389])
- 1. Select your card type from the ▼ **Card type** drop-down menu.
- 2. Select the configuration you require from the ▼ **Configuration** drop-down menu.
- 3. Enter the remaining previously determined parameters in the section on the right.
- 4. Click on the **Finish** button.
- ↳ The card configuration is set.

#### 17.1.1.1 MIFARE Classic (new/empty card)

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1000L_AV	Name: SectList
Speicherbedarf	528 Bytes	Wert: 2,3,4,5,6,7,8,9,10,11,12
Schließungs-IDs	128 - 1127 im Kartenprofil	<input type="button" value="Bearbeiten"/>
Begehungen im Protokoll	19	Beschreibung: Sector List
Virtuelles Netzwerk	OK	Name: TransportSectorTrailer
		Wert: *****
		<input type="button" value="Bearbeiten"/>
		Beschreibung: Transport Settings

The following parameters are determined during configuration:

- ❑ ▼ **Card type:** MIFARE Classic or DESFire
- ❑ ▼ **Configuration:** Card template (see *Card templates* [▶ 556])

The card template decides on:

- ❑ *Memory requirements:* must be available in free memory space on the card.
- ❑ *Lock IDs:* shows the number of possible locking device IDs for this card. AXM Plus automatically assigns lock IDs with LID 0-127 reserved for internal functions.  
See *Cards and locking device IDs* [▶ 552] for background information.
- ❑ *Physical accesses in the log:* shows the number of entries that can be written on this card's physical access list. For AV templates only (**A**udit trail & **V**irtual network).
- ❑ *Virtual Network:* indicates whether a virtual network is possible. AV templates only.

The following is also determined for MIFARE Classic:

- *SectList*: List of sectors where the data from your locking system is stored.
  - *TransportSectorTrailer*: Encryption of your locking system data on the card
  - ✓ Card type: MIFARE Classic
1. Read the card or consult the data sheet.
    - ↳ Full report is displayed.
  2. Determine the available memory space or sectors (*EXTRA # Memory size* section).

```
-- EXTRA -----
# Memory size:
1 kB
* 16 sectors, with 4 blocks per sector
* 64 blocks, with 16 bytes per block
```

- ↳ Card contains 16 sectors.
- ↳ Sector 0 is internal for MIFARE Classic and sector 1 should not be used, so there are 14 sectors available.



**NOTE**

**Sector structure, card-specific**

The sector structure may differ for your card. Cards with a larger memory in particular may have more master sectors (e.g. often sector 16) and have different sector sizes, i.e. more storage space per sector.

Even on new cards, the manufacturer may have blocked sectors and these must first be unblocked.

Example: MIFARE Classic EV1 4k: 4kB memory, divided into Sectors 0-31 with 4 blocks each and Sectors 32-39 with 16 blocks each. Sector 16 is another master sector here.

1. Read the report carefully to determine master sectors and sector size.
2. If you decide to have SimonsVoss check your cards, please contact one of our sales representatives in your region.

- ↳ Each sector consists of three writeable blocks and one block for encryption: 3\*16 bytes = 48 bytes per sector.



↳ Available sectors can be identified in the report by three blocks marked [rwi]: *read/write/increment* – the fourth block is for encryption.

```
Sector 1 (0x01)
[04] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[05] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[06] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[07] wxx FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
      Factory default key          Factory default key (readable)
```

↳ Internal card sectors can be identified in the report by the fact that not all three blocks are marked with [rwi]:

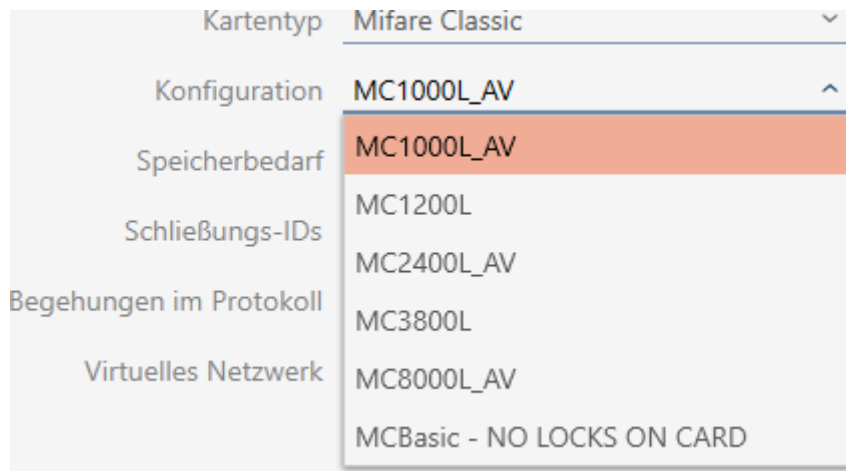
```
Sector 0 (0x00)
[00] r- 50 07 32 57 32 88 04 00 46 8F 74 D0 65 40 23 11 |P.2W2...F.t.e@#.|
[01] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[02] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[03] wxx FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
      Factory default key          Factory default key (readable)
```

3. Calculate the available storage space: Bytes per sector \* available sectors (example: 48 bytes \* 14 sectors = 672 bytes).
4. From the drop-down menu ▼ **Card type**, select "MIFARE Classic".



5. Consider whether you need a physical access list or a virtual network for your cards.
  - ↳ If you do: You need an AV template (= "Audit trail and "Virtual network").

- Determine the largest card configuration that fits into the available memory (see *Card templates* [▶ 556] – example for AV: MC1000L\_AV with 528 bytes).



- Select the configuration you just specified from the ▼ **Configuration** drop-down menu (example: MC1000L\_AV).
  - ↳ *Memory requirements* shows the memory requirement on the card.
  - ↳ *Lock IDs* shows the number of possible locking device IDs for this card (AXM Plus automatically assigns lock IDs with LID 0-127 being reserved for internal functions). See *Cards and locking device IDs* [▶ 552] for background information.
  - ↳ *Physical accesses in the log* shows the number of possible entries in the physical access list (for AV templates only).



- ↳ The number of entries for locking devices in the matrix is limited to the number of possible locking device IDs. Locking devices can also consume more than one entry, e.g. freely rotating Digital Cylinder AX.
- ↳ The physical access list is overwritten on a rolling basis, so it is not limited.
- ↳ A virtual network is possible.



8. Calculate the number of sectors actually needed: *Memory requirements* / bytes per sector (example: 528 bytes / 48 bytes = 11 sectors). Round off the result to the next integer if necessary.
9. Click the **Edit** button in the *SectList* field.
  - ↳ The "Enter parameter value" window will open.

## Parameterwert eingeben

Hier können Sie einen neuen Wert für den Parameter eingeben

Neuer Wert

OK
Abbrechen

10. Enter as many free sectors as you need in the *New value* field (example: 2,3,4,5,6,7,8,9,10,11,12). Do not use sectors that are not writeable or used as a master sector (example: Sector 0 is not writeable and Sector 1 is a master sector).  
Numbers separated by commas, without spaces.



### NOTE

#### Saved storage space thanks to own sector list

Obviously, you can also use the default sector list. However, it may even be the case that not all sectors from this list are used because the card configuration also fits into fewer sectors.

- Enter your own sector list.
  - ↳ This allows you to save sectors on your cards that you might want to use for other applications in the future.

11. Click on the **OK** button.
  - ↳ "Enter parameter value" window closes.
12. Leave the *TransportSectorTrailer* field unchanged.
  - ↳ TransportSectorTrailer is an integral part of card encryption. Your AXM Plus will automatically generate this entry for you.

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1000L_AV	Name: SectList
Speicherbedarf	528 Bytes	Wert: 2,3,4,5,6,7,8,9,10,11,12
Schließungs-IDs	128 - 1127 im Kartenprofil	<input type="button" value="Bearbeiten"/>
Begehungen im Protokoll	19	Beschreibung: Sector List
Virtuelles Netzwerk	OK	Name: TransportSectorTrailer
		Wert: *****
		<input type="button" value="Bearbeiten"/>
		Beschreibung: Transport Settings

13. Click on the **Finish** button.

↳ Window "Locking system" closes.

↳ Card configuration saved.

### 17.1.1.2 MIFARE Classic (card already used)

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1200L	Name: SectList
Speicherbedarf	192 Bytes	Wert: 7,8,9,10
Schließungs-IDs	128 - 1327 im Kartenprofil	<input type="button" value="Bearbeiten"/>
Begehungen im Protokoll	--	Beschreibung: Sector List
Virtuelles Netzwerk	--	Name: TransportSectorTrailer
		Wert: *****
		<input type="button" value="Bearbeiten"/>
		Beschreibung: Transport Settings

❑ ▼ **Card type:** MIFARE Classic or DESFire

❑ ▼ **Configuration:** Card template (see *Card templates* [▶ 556])

The card template decides on:

❑ *Memory requirements:* must be available in free memory space on the card.

❑ *Lock IDs:* shows the number of possible locking device IDs for this card. AXM Plus automatically assigns lock IDs with LID 0-127 reserved for internal functions.

See *Cards and locking device IDs* [▶ 552] for background information.

❑ *Physical accesses in the log:* shows the number of entries that can be written on this card's physical access list. For AV templates only (Audit trail & Virtual network).

❑ *Virtual Network:* indicates whether a virtual network is possible. AV templates only.

The following is also determined for MIFARE Classic:

❑ *SectList:* List of sectors where the data from your locking system is stored.

- ❑ *TransportSectorTrailer*: Encryption of your locking system data on the card
- ✓ Card type: MIFARE Classic
- 1. Read the card or consult the data sheet.
  - ↳ Full report is displayed.
- 2. Determine the available memory space or sectors (*EXTRA # Memory size* section).

```
-- EXTRA -----
# Memory size:
1 kB
* 16 sectors, with 4 blocks per sector
* 64 blocks, with 16 bytes per block
```

- ↳ Card contains 16 sectors.
- ↳ Sector 0 is internal for MIFARE Classic and sector 1 should not be used, so there are 14 sectors available.



**NOTE**

**Sector structure, card-specific**

The sector structure may differ for your card. Cards with a larger memory in particular may have more master sectors (e.g. often sector 16) and different sector sizes, i.e. more storage space per sector.

Even on new cards, the manufacturer may have blocked sectors and these must first be unblocked.

In some cases, third-party applications also block all sectors, although they do not even use all sectors.

Example: MIFARE Classic EV1 4k: 4kB memory, divided into Sectors 0-31 with 4 blocks each and Sectors 32-39 with 16 blocks each. Sector 16 is another master sector here.

1. Read the report carefully to determine master sectors and sector size.
2. If you decide to have SimonsVoss check your cards, please contact one of our sales representatives in your region.
3. If necessary, unlock blocked unused sectors with the *TransportSectorTrailer*.

- ↳ Each sector consists of three writeable blocks and one block for encryption: 3\*16 bytes = 48 bytes per sector.



- ↳ Available sectors can be identified in the report by three blocks marked [rwi]: *read/write/increment* – the fourth block is for encryption.

```
Sector 1 (0x01)
[04] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[05] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[06] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[07] wxx FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
      Factory default key          Factory default key (readable)
```

- ↳ Internal card sectors can be identified in the report by the fact that not all three blocks are marked with [rwi]:

```
Sector 0 (0x00)
[00] r- 50 07 32 57 32 88 04 00 46 8F 74 D0 65 40 23 11 |P.2W2...F.t.e@#.|
[01] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[02] rwi 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 |.....|
[03] wxx FF:FF:FF:FF:FF:FF FF:07:80 69 FF:FF:FF:FF:FF:FF
      Factory default key          Factory default key (readable)
```

- ↳ Sectors that have already been used can be recognised by the fact that the data can no longer be read in plain text:

```

Sector 2 (0x02)
[08] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[09] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0A] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0B] ???  XX:XX:XX:XX:XX:XX  --:--:--  --  XX:XX:XX:XX:XX:XX
                (unknown key)                (unknown key)

Sector 3 (0x03)
[0C] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0D] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0E] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[0F] ???  XX:XX:XX:XX:XX:XX  --:--:--  --  XX:XX:XX:XX:XX:XX
                (unknown key)                (unknown key)

Sector 4 (0x04)
[10] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[11] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[12] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[13] ???  XX:XX:XX:XX:XX:XX  --:--:--  --  XX:XX:XX:XX:XX:XX
                (unknown key)                (unknown key)

Sector 5 (0x05)
[14] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[15] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[16] ???  -- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --
[17] ???  XX:XX:XX:XX:XX:XX  --:--:--  --  XX:XX:XX:XX:XX:XX
                (unknown key)                (unknown key)
    
```

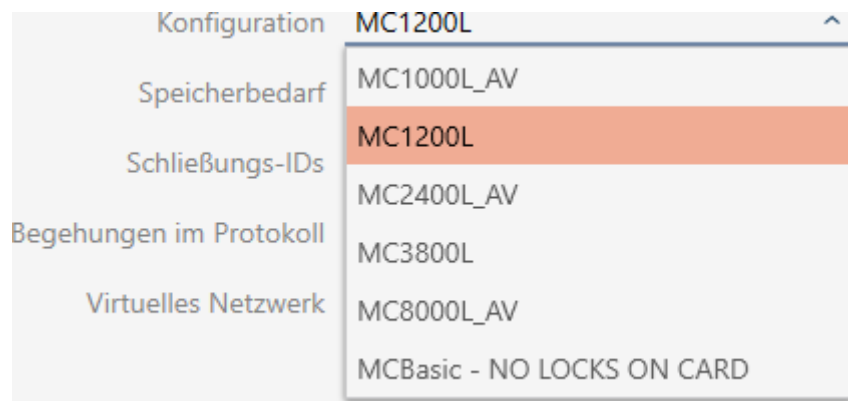
- ↳ Sectors 2, 3, 4 and 5 have already been written on (e.g. by another application) and are not available for the locking system.
- ↳ Sectors 0 and 1 cannot be used either. As a result, the sectors available are: 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15 (= 10 sectors available for the locking system).

3. Calculate the available storage space: Bytes per sector \* available sectors (example: 48 bytes \* 10 sectors = 480 bytes).

4. From the drop-down menu ▼ **Card type**, select "MIFARE Classic".



5. Consider whether you need a physical access list or a virtual network for your cards.
  - ↳ If you do: You need an AV template (= "Audit trail and "Virtual network").
6. Determine the largest card configuration that fits into the available memory (see *Card templates* [▶ 556] – example: MC1200L with 192 bytes).
7. Select the configuration you just specified from the ▼ Configuration drop-down menu (example: MC1200L).

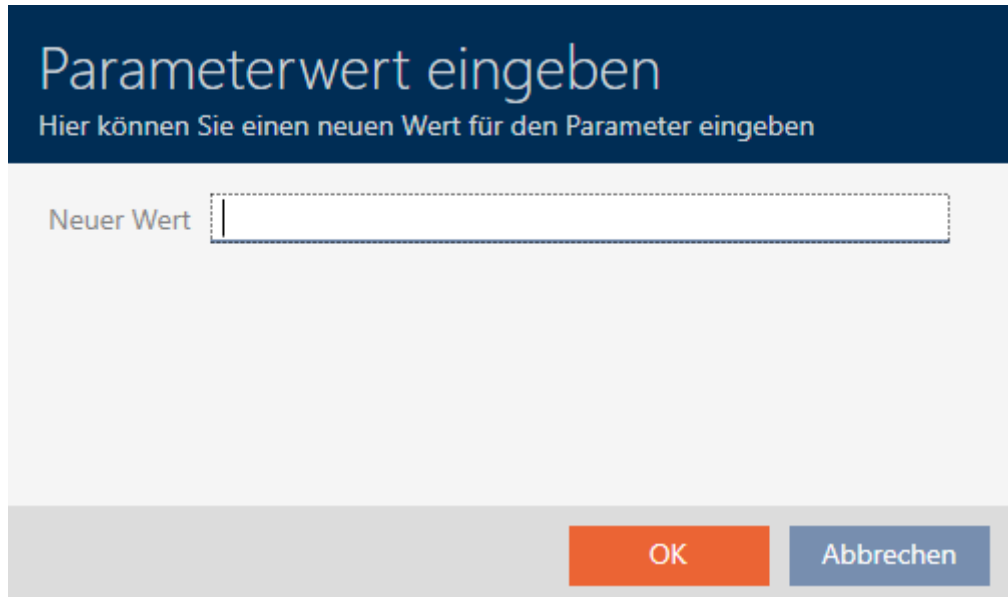


- ↳ *Memory requirements* shows the memory requirement on the card.
- ↳ *Lock IDs* shows the number of possible locking device IDs for this card (AXM Plus automatically assigns lock IDs with LID 0-127 being reserved for internal functions). See *Cards and locking device IDs* [▶ 552] for background information.

Kartentyp	Mifare Classic
Konfiguration	MC1200L
Speicherbedarf	192 Bytes
Schließungs-IDs	128 - 1327 im Kartenprofil
Begehungen im Protokoll	--
Virtuelles Netzwerk	--

- ↳ The number of entries for locking devices in the matrix is limited to the number of possible locking device IDs. Locking devices can also consume more than one entry, e.g. freely rotating Digital Cylinder AX.
  - ↳ Physical access list not available (it is not an AV template).
  - ↳ Virtual network not possible.
8. Calculate the number of sectors actually needed: *Memory requirements*/ bytes per sector (example: 192 bytes / 48 bytes = 4 sectors). Round off the result to the next integer if necessary.

- Click the **Edit** button in the *SectList* field.
  - ↳ The "Enter parameter value" window will open.



- Enter as many free sectors as you need in the *New value* field (example: 7,8,9,10). Do not use sectors that are not writeable or used as a master sector (example: Sector 0 is not writeable and Sector 1 is a master sector).  
Numbers separated by commas, without spaces.



#### NOTE

##### Saved storage space thanks to own sector list

Obviously, you can also use the default sector list. However, it may even be the case that not all sectors from this list are used because the card configuration also fits into fewer sectors.

- Enter your own sector list.
  - ↳ This allows you to save sectors on your cards that you might want to use for other applications in the future.



#### NOTE

##### Sectors do not need to be contiguous

The sector list does not have to be contiguous. If sectors in the middle of the sector list are used for other purposes, this is not a problem for AXM Plus.

- Click on the **OK** button.
  - ↳ "Enter parameter value" window closes.

12. Leave the *TransportSectorTrailer* field unchanged.

- ↳ TransportSectorTrailer is an integral part of card encryption. Your AXM Plus will automatically generate this entry for you.

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1200L	Name: SectList
Speicherbedarf	192 Bytes	Wert: 7,8,9,10
Schließungs-IDs	128 - 1327 im Kartenprofil	<input type="button" value="Bearbeiten"/>
Begehungen im Protokoll	--	Beschreibung: Sector List
Virtuelles Netzwerk	--	Name: TransportSectorTrailer
		Wert: *****
		<input type="button" value="Bearbeiten"/>
		Beschreibung: Transport Settings

13. Click on the **Finish** button.

- ↳ Window "Locking system" closes.
- ↳ Card configuration saved.

AXM Plus only writes on the sectors specified in the sector list. All other sectors remain unchanged.

Other applications (e.g. canteen billing) simply continue to write on their "own" sectors. They work – completely separately from your AXM Plus as before.

### Unlocking blocked sectors with the TransportSectorTrailer



In exceptional cases, another application may block sectors, but may not actually use them. In this case, you can use your AXM Plus to unlock these sectors and use them for your locking system.



**NOTE****Malfunctions in other applications and/or your locking system**

Data in sectors used by a specific application may only be modified by the application in question.

For example, if your locking system changes the data in a sector used by your canteen system, then the canteen system will most likely no longer be able to process data. Conversely, the canteen system can also render your locking system data unusable.

1. Before unlocking "third-party" sectors, ensure that they are not really used.
2. Consult the third-party application operator or the owner of the sectors.
3. If you decide to have SimonsVoss check your cards, please contact one of our sales representatives in your region.

1. Click the **Edit** button in the TransportSectorTrailer section.  
↳ The "Enter parameter value" window will open.

Parameterwert eingeben  
Hier können Sie einen neuen Wert für den Parameter eingeben

Neues Passwort

Bestätigung

OK Abbrechen

2. Enter the TransportSectorTrailer into the *New password* field that the other application uses.
3. Repeat the entry in the *Confirmation* field.
4. Click on the **OK** button.  
↳ "Enter parameter value" window closes.  
↳ AXM Plus unlocks blocked sectors and uses them for the locking system.

17.1.1.3 MIFARE DESFire (new/empty card)

Kartentyp	Mifare Desfire	Parameter
Konfiguration	MD4000L_AV	Name Appld
Speicherbedarf	1600 Bytes	Wert 1
Schließungs-IDs	128 - 4127 im Kartenprofil	Bearbeiten
Begehungen im Protokoll	100	Beschreibung Application Id
Virtuelles Netzwerk	OK	Name CryptoMode
		Wert AES
		Bearbeiten
		Beschreibung Cryptography: AES or 3DES
		Name PiccCryptoMode
		Wert AES
		Bearbeiten
		Beschreibung Cryptography: AES or 3DES
		Name PiccMasterKey
		Wert *****
		Bearbeiten
		Beschreibung Card Master Key

- ❑ ▼ Card type: MIFARE Classic or DESFire
- ❑ ▼ Configuration: Card template (see *Card templates* [▶ 556])
 

The card template decides on:

  - ❑ *Memory requirements*: must be available in free memory space on the card.
  - ❑ *Lock IDs*: shows the number of possible locking device IDs for this card. AXM Plus automatically assigns lock IDs with LID 0-127 reserved for internal functions.  
See *Cards and locking device IDs* [▶ 552] for background information.
  - ❑ *Physical accesses in the log*: shows the number of entries that can be written on this card's physical access list. For AV templates only (Audit trail & Virtual network).
  - ❑ *Virtual Network*: indicates whether a virtual network is possible. AV templates only.

The following are also determined for MIFARE DESFire:

- ❑ *App ID*: App ID where your locking system data is stored.
- ❑ *CryptoMode*: encryption process for your locking system data (encryption of your app ID's content – recommended: AES)
- ❑ *PiccCryptoMode*: General encryption method (encryption of the entire card – recommended: AES)
- ❑ *PiccMasterKey*: key that protects the card from full formatting.

- ✓ Card type: MIFARE DESFire
- 1. Read the card or consult the data sheet.
  - ↳ Full report is displayed.
- 2. Locate the available storage space (Section # *Memory information*).

# Memory information:

Size: 2 kB

Available: 2.3 kB

↳ Only app ID 0 is used for new/empty cards:

Application ID 0x000000 (PICC)

\* Default master key

\* Key configuration:

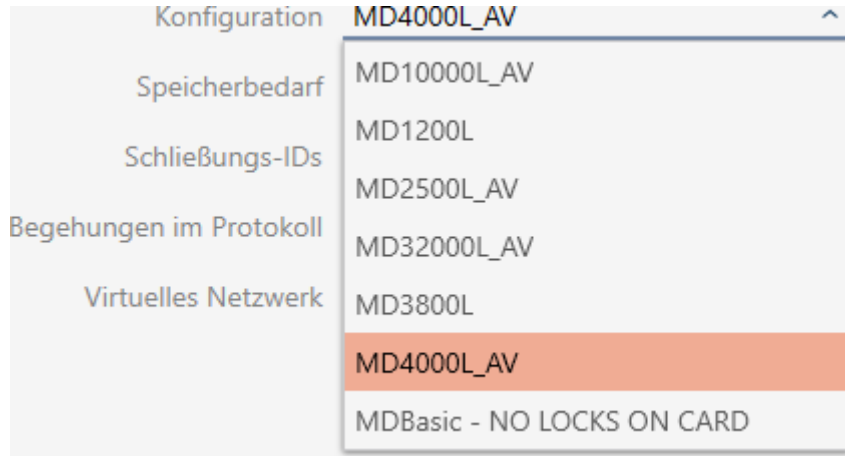
- 1 (3)DES key
- Master key changeable
- Master key required for:
  - ~ directory list access: no
  - ~ create/delete files: no
- Configuration changeable

- 3. From the drop-down menu ▼ **Card type**, select "MIFARE DESFire".



- 4. Consider whether you need a physical access list or a virtual network for your cards.
  - ↳ If you do: You need an AV template (= "Audit trail and "Virtual network").
- 5. Determine the largest card configuration that fits into the available memory (see *Card templates* [▶ 556] – example for AV: MD4000L\_AV with 1600 bytes).

6. Select the configuration you just specified from the ▼ Configuration drop-down menu (example: MD4000L\_AV).



- ↳ *Memory requirements* shows the memory requirement on the card.
- ↳ *Lock IDs* shows the number of possible locking device IDs for this card (AXM Plus automatically assigns lock IDs with LID 0-127 being reserved for internal functions). See *Cards and locking device IDs* [▶ 552] for background information.
- ↳ *Physical accesses in the log* shows the number of possible entries in the physical access list (for AV templates only).

Kartentyp	Mifare Desfire
Konfiguration	MD4000L_AV
Speicherbedarf	1600 Bytes
Schließungs-IDs	128 - 4127 im Kartenprofil
Begehungen im Protokoll	100
Virtuelles Netzwerk	OK

- ↳ The number of entries for locking devices in the matrix is limited to the number of possible locking device IDs. Locking devices can also consume more than one entry, e.g. freely rotating Digital Cylinder AX.
- ↳ The physical access list is overwritten on a rolling basis, so it is not limited.
- ↳ A virtual network is possible.

7. Click the **Edit** button next to the app ID for the parameters.

Name:	AppId
Wert:	1
<input type="button" value="Bearbeiten"/>	
Beschreibung: Application Id	

↳ The "Enter parameter value" window will open.

## Parameterwert eingeben

Hier können Sie einen neuen Wert für den Parameter eingeben

Neuer Wert

8. Enter an app ID in the *New value* field (decimal system) or leave the value at the default value 1.

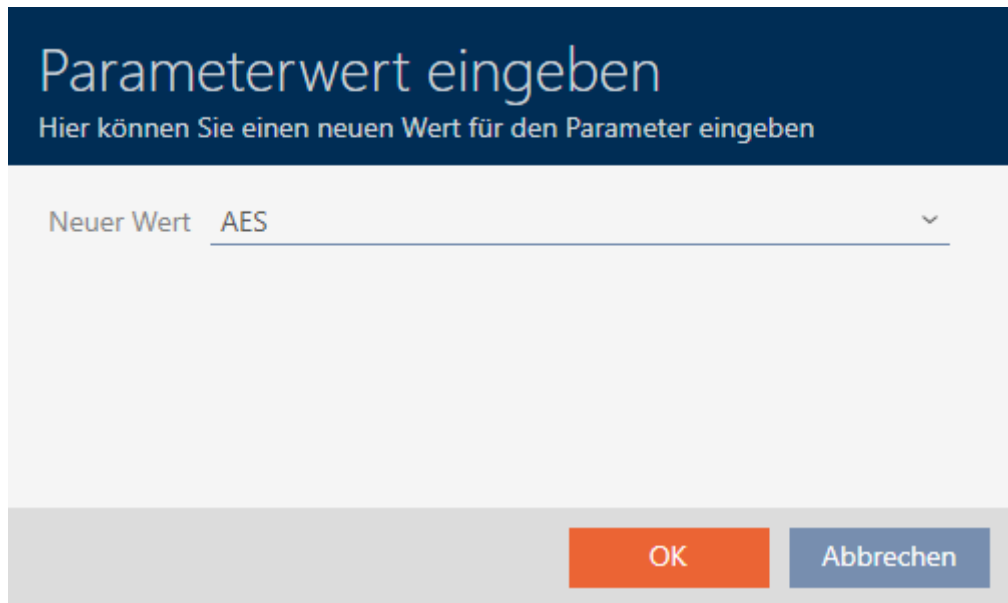
9. Click on the **OK** button.

↳ "Enter parameter value" window closes.

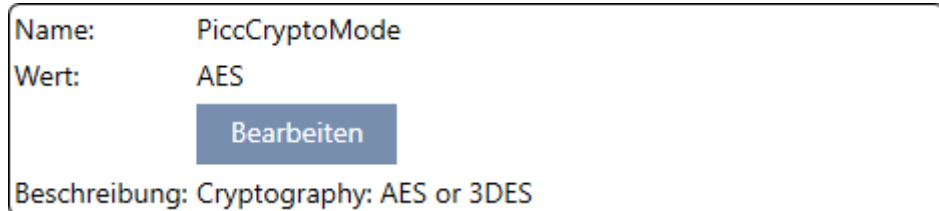
10. Click the **Edit** button next to CryptoMode for the parameters.

Name:	CryptoMode
Wert:	AES
<input type="button" value="Bearbeiten"/>	
Beschreibung: Cryptography: AES or 3DES	

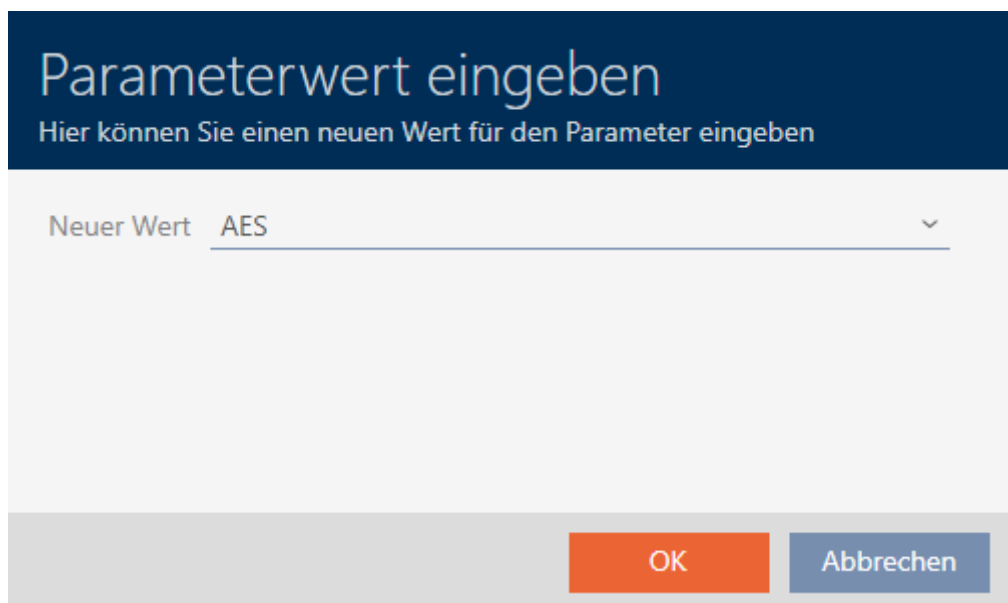
↳ The "Enter parameter value" window will open.



11. Select the AES entry from the ▼ **New value** drop-down menu.
12. Click on the **OK** button.
  - ↳ "Enter parameter value" window closes.
13. Click the **Edit** button next to PiccCryptoMode for the parameters.



- ↳ The "Enter parameter value" window will open.



14. Select the AES entry from the ▼ **New value** drop-down menu.

- 15. Click on the **OK** button.
  - ↳ "Enter parameter value" window closes.
- 16. Only edit the PiccMasterKey if the manufacturer has not set the PiccMasterKey to a default value.

**Name:** PiccMasterKey

**Wert:** \*\*\*\*\*

**Bearbeiten**

**Beschreibung:** Card Master Key

- ↳ Your AXM Plus will determine the right PiccMasterKey itself. If you specify a PiccMasterKey, AXM Plus will only use this one and will not determine one.

Kartentyp	Parameter
Mifare Desfire	<div style="border: 1px solid black; padding: 5px;"> <p><b>Name</b> Appld</p> <p><b>Wert</b> 1</p> <p style="text-align: center;"><b>Bearbeiten</b></p> <p><b>Beschreibung</b> Application Id</p> </div>
Konfiguration MD4000L_AV	<div style="border: 1px solid black; padding: 5px;"> <p><b>Name</b> CryptoMode</p> <p><b>Wert</b> AES</p> <p style="text-align: center;"><b>Bearbeiten</b></p> <p><b>Beschreibung</b> Cryptography: AES or 3DES</p> </div>
Speicherbedarf 1600 Bytes	<div style="border: 1px solid black; padding: 5px;"> <p><b>Name</b> PiccCryptoMode</p> <p><b>Wert</b> AES</p> <p style="text-align: center;"><b>Bearbeiten</b></p> <p><b>Beschreibung</b> Cryptography: AES or 3DES</p> </div>
Schließungs-IDs 128 - 4127 im Kartenprofil	<div style="border: 1px solid black; padding: 5px;"> <p><b>Name</b> PiccMasterKey</p> <p><b>Wert</b> *****</p> <p style="text-align: center;"><b>Bearbeiten</b></p> <p><b>Beschreibung</b> Card Master Key</p> </div>
Begehungen im Protokoll 100	
Virtuelles Netzwerk OK	

- 17. Click on the **Finish** button.
  - ↳ Window "Locking system" closes.
  - ↳ Card configuration saved.



**NOTE**

**PiccMasterKey identical throughout the locking system**

The same PiccMasterKey must be used for all cards within a locking system.

17.1.1.4 MIFARE DESFire (card already in use)

Kartentyp	Mifare Desfire	Parameter
Konfiguration	MD4000L_AV	
Speicherbedarf	1600 Bytes	Name Appld Wert 2 <input type="button" value="Bearbeiten"/> Beschreibung Application Id
Schließungs-IDs	128 - 4127 im Kartenprofil	Name CryptoMode Wert AES <input type="button" value="Bearbeiten"/> Beschreibung Cryptography: AES or 3DES
Begehungen im Protokoll	100	Name PiccCryptoMode Wert AES <input type="button" value="Bearbeiten"/> Beschreibung Cryptography: AES or 3DES
Virtuelles Netzwerk	OK	Name PiccMasterKey Wert ***** <input type="button" value="Bearbeiten"/> Beschreibung Card Master Key

- ❑ ▼ Card type: MIFARE Classic or DESFire
- ❑ ▼ Configuration: Card template (see *Card templates* [▶ 556])
 

The card template decides on:

  - ❑ *Memory requirements*: must be available in free memory space on the card.
  - ❑ *Lock IDs*: shows the number of possible locking device IDs for this card. AXM Plus automatically assigns lock IDs with LID 0-127 reserved for internal functions.  
See *Cards and locking device IDs* [▶ 552] for background information.
  - ❑ *Physical accesses in the log*: shows the number of entries that can be written on this card's physical access list. For AV templates only (Audit trail & Virtual network).
  - ❑ *Virtual Network*: indicates whether a virtual network is possible. AV templates only.

The following are also determined for MIFARE DESFire:

- ❑ *App ID*: App ID where your locking system data is stored.
- ❑ *CryptoMode*: encryption process for your locking system data (encryption of your app ID's content – recommended: AES)
- ❑ *PiccCryptoMode*: General encryption method (encryption of the entire card – recommended: AES)
- ❑ *PiccMasterKey*: key that protects the card from full formatting.



✓ Card type: MIFARE DESFire

1. Read the card or consult the data sheet.

↳ Full report is displayed.

2. Locate the available storage space (Section # *Memory information*).

# Memory information:

Size: 2 kB

Available: 1.9 kB

↳ Full storage space is no longer available on this card. This suggests that at least one other application is active and uses storage space.

3. Use the full report to determine the app IDs of the existing applications:

-----  
Application ID 0x000000 (PICC)

\* Key configuration:

- 1 (3)DES key
- Master key changeable
- Master key required for:
  - ~ directory list access: no
  - ~ create/delete files: yes
- Configuration changeable

Application ID 0x010000

\* Key configuration:

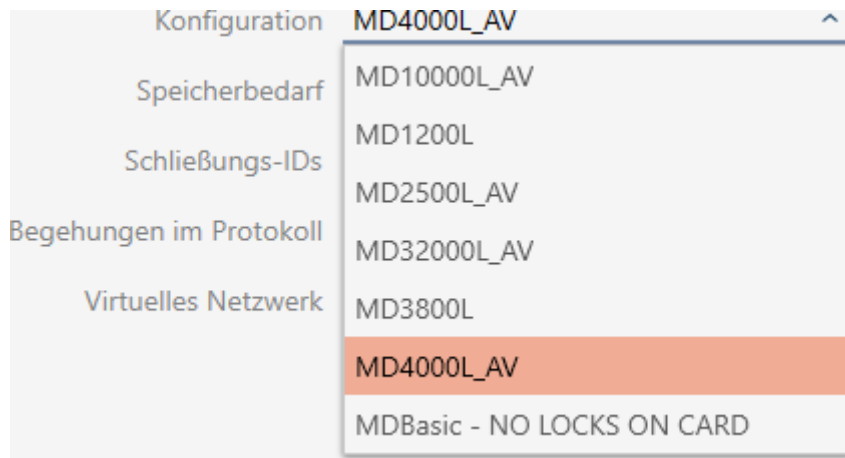
- 2 AES keys
- Master key changeable
- Master key required for:
  - ~ directory list access: no
  - ~ create/delete files: yes
- Configuration changeable
- Master key required for changing a key
- Key versions:
  - ~ Master key: 0
  - ~ Key #1: 0
- File ID 0x00: Standard data, 192 bytes
  - ~ Communication: encrypted
  - ~ Read key: key #1
  - ~ Write key: key #1
  - ~ Read/Write key: key #1
  - ~ Change key: master key
  - ~ (No access)

↳ App ID 0 is assigned in the factory, the app ID 1 is a third-party application with a 192 byte memory.

4. From the drop-down menu ▼ **Card type**, select "MIFARE DESFire".



5. Consider whether you need a physical access list or a virtual network for your cards.
  - ↳ If you do: You need an AV template (= "Audit trail and "Virtual network").
6. Determine the largest card configuration that fits into the available memory (see *Card templates* [▶ 556] – example for AV: MD4000L\_AV with 1600 bytes).
7. Select the configuration you just specified from the ▼ Configuration drop-down menu (example: MD4000L\_AV).



- ↳ *Memory requirements* shows the memory requirement on the card.
- ↳ *Lock IDs* shows the number of possible locking device IDs for this card (AXM Plus automatically assigns lock IDs with LID 0-127 being reserved for internal functions). See *Cards and locking device IDs* [▶ 552] for background information.
- ↳ *Physical accesses in the log* shows the number of possible entries in the physical access list (for AV templates only).



- ↳ The number of entries for locking devices in the matrix is limited to the number of possible locking device IDs. Locking devices can also consume more than one entry, e.g. freely rotating Digital Cylinder AX.
- ↳ The physical access list is overwritten on a rolling basis, so it is not limited.

↳ A virtual network is possible.

8. Click the **Edit** button next to the app ID for the parameters.

Name:	AppId
Wert:	1
<input type="button" value="Bearbeiten"/>	
Beschreibung: Application Id	

↳ The "Enter parameter value" window will open.

## Parameterwert eingeben

Hier können Sie einen neuen Wert für den Parameter eingeben

Neuer Wert

9. Enter an unused app ID as a decimal value (in the example, 0 and 1 are assigned – 2 is thus possible) in the *New value* field.



**NOTE**

**Number of applications for DESFire EV1 and EV2**

MIFARE DESFire EV1 supports a maximum of 28 applications (0-27). The highest app ID is therefore App ID 27.

MIFARE DESFire EV2 has no limits in this respect.

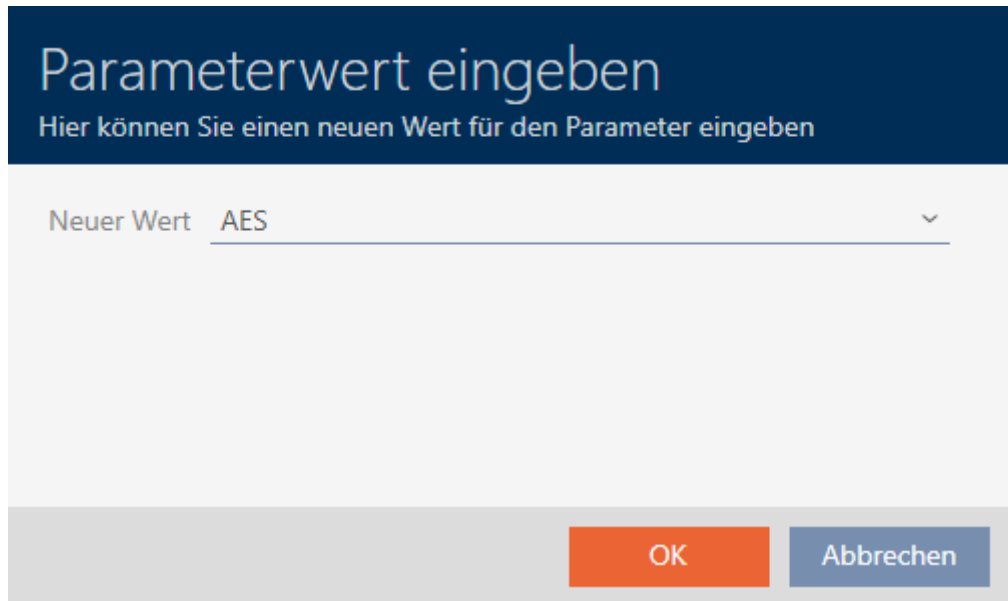
10. Click on the **OK** button.

↳ "Enter parameter value" window closes.

11. Click the **Edit** button next to CryptoMode for the parameters.

Name:	CryptoMode
Wert:	AES
<input type="button" value="Bearbeiten"/>	
Beschreibung: Cryptography: AES or 3DES	

↳ The "Enter parameter value" window will open.

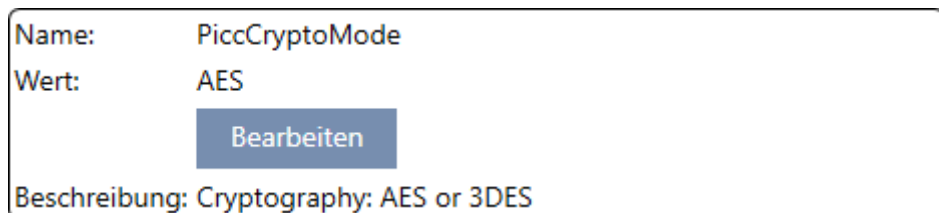


12. Select the AES entry from the ▼ **New value** drop-down menu.

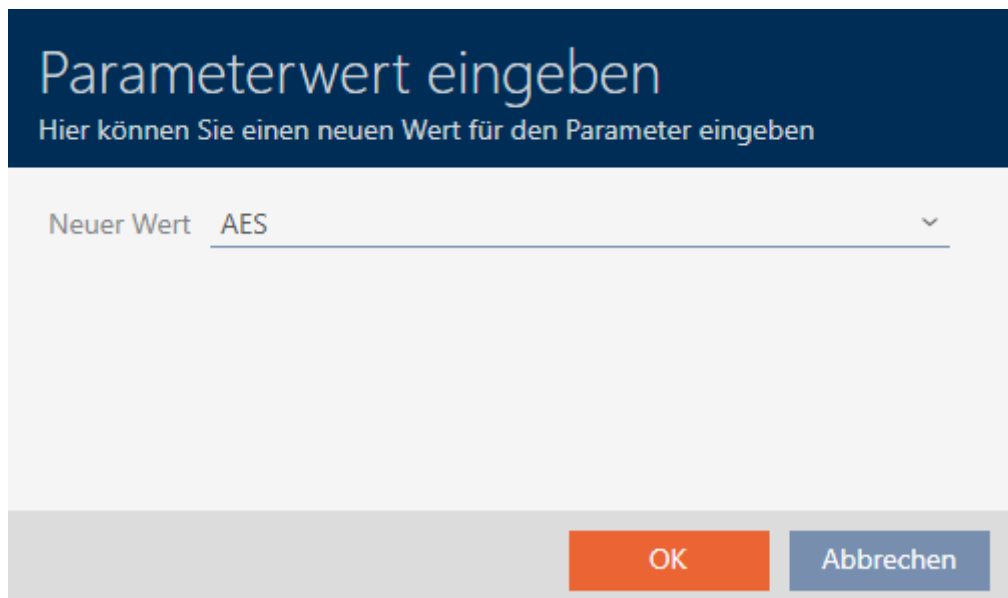
13. Click on the **OK** button.

↳ "Enter parameter value" window closes.

14. Click the **Edit** button next to PiccCryptoMode for the parameters.



↳ The "Enter parameter value" window will open.



- 15. Select the AES entry from the ▼ New value drop-down menu.
- 16. Click on the OK button.
  - ↳ "Enter parameter value" window closes.
- 17. Only edit the PiccMasterKey if the manufacturer has not set the PiccMasterKey to a default value.

Name: PiccMasterKey

Wert: \*\*\*\*\*

Beschreibung: Card Master Key

- ↳ Your AXM Plus will determine the right PiccMasterKey itself. If you specify a PiccMasterKey, AXM Plus will only use this one and will not determine one.

<p>Kartentyp Mifare Desfire</p> <p>Konfiguration MD4000L_AV</p> <p>Speicherbedarf 1600 Bytes</p> <p>Schließungs-IDs 128 - 4127 im Kartenprofil</p> <p>Begehungen im Protokoll 100</p> <p>Virtuelles Netzwerk OK</p>	<p>Parameter</p> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;"> <p>Name Appld</p> <p>Wert 2</p> <p style="text-align: center;"><input type="button" value="Bearbeiten"/></p> <p>Beschreibung Application Id</p> </div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;"> <p>Name CryptoMode</p> <p>Wert AES</p> <p style="text-align: center;"><input type="button" value="Bearbeiten"/></p> <p>Beschreibung Cryptography: AES or 3DES</p> </div> <div style="border: 1px solid gray; padding: 2px; margin-bottom: 2px;"> <p>Name PiccCryptoMode</p> <p>Wert AES</p> <p style="text-align: center;"><input type="button" value="Bearbeiten"/></p> <p>Beschreibung Cryptography: AES or 3DES</p> </div> <div style="border: 1px solid gray; padding: 2px;"> <p>Name PiccMasterKey</p> <p>Wert *****</p> <p style="text-align: center;"><input type="button" value="Bearbeiten"/></p> <p>Beschreibung Card Master Key</p> </div>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

- 18. Click on the Finish button.
  - ↳ Window "Locking system" closes.
  - ↳ Card configuration saved.



**NOTE**

**PiccMasterKey identical throughout the locking system**

The same PiccMasterKey must be used for all cards within a locking system.

The following phenomena may also occur with the DESFire cards used:

- Third-party applications change the PiccMasterKey (contact the operator of the third-party application)

- Card manufacturers change the PiccMasterKey (read data sheet)
- Predefined cards: Organisations write “empty” app IDs on cards centrally (contact Central Organisation Management).

## 17.2 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 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.

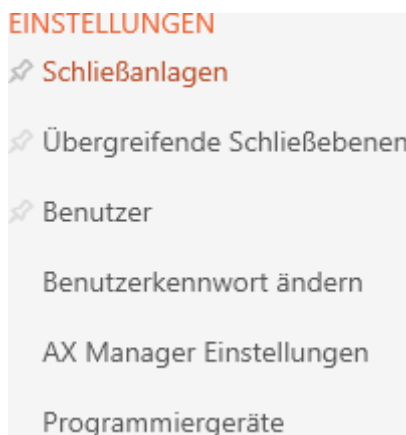
Changing the locking system password causes the greatest programming requirement of all possible changes in your database.

- ✓ Old locking system password is known.

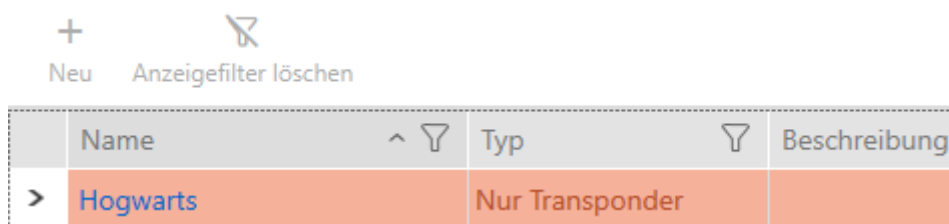
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.



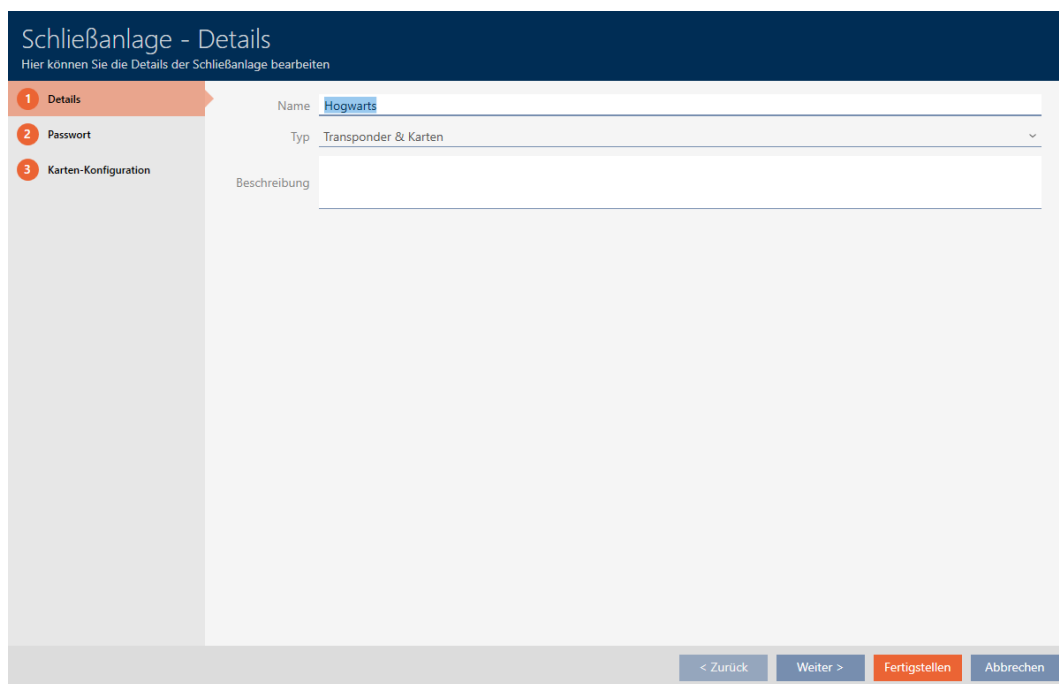
- Select the **Locking systems** entry in the | SETTINGS | group.



- ↳ The [Locking systems] tab with a list of all locking systems in the database will open.



- Click on the locking system whose password you wish to change.
  - ↳ The locking system window will open.





4. Click on the **Password** tab.



↳ Window switches to the "Password" tab.

5. Enter the old locking system password in the *Old password* field.

6. Enter a new locking system password with at least 8 characters in the *Password* field.

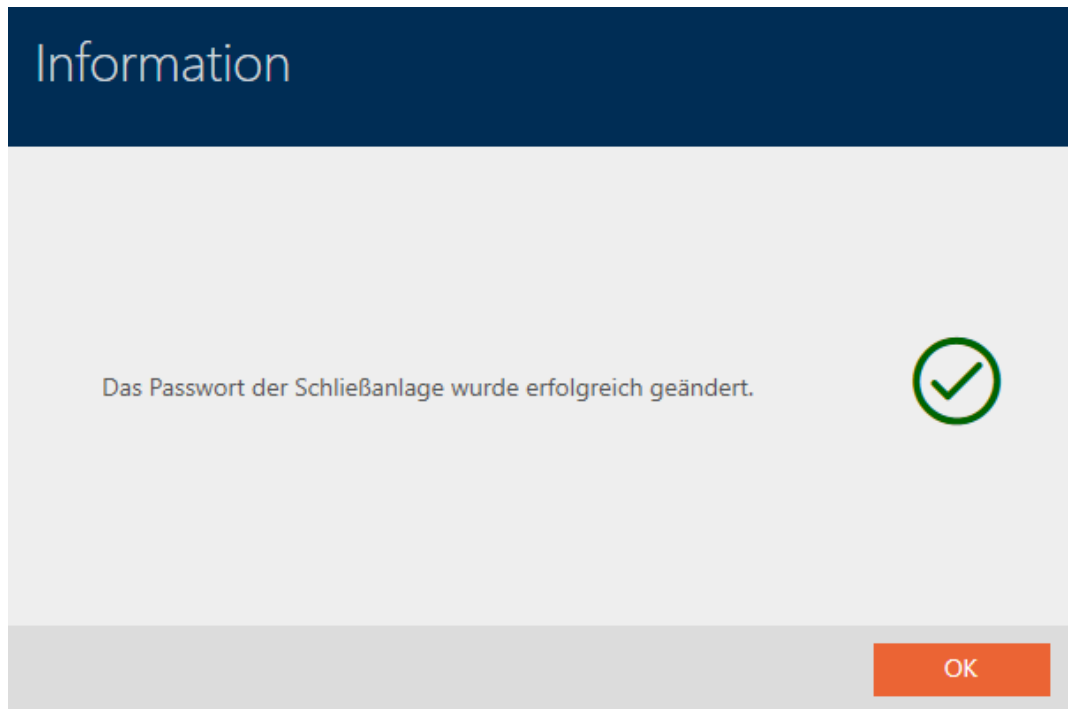
↳ A coloured bar shows you how secure your password is.



7. Confirm the new locking system password in the *Confirm password* field.

8. Click on the **Finish** button.
  - ↳ Warning message appears about the expected scope of programming required.

9. Click on the **Yes** button.
  - ↳ Warning message closes.
  - ↳ Locking system password has been changed.



### 17.3 Replacing the locking system

Working with multiple locking systems can offer you advantages (see *Locking systems* [▶ 521]). Your AXM Plus provides you with an uncluttered interface and therefore normally only shows you the entries that belong to the selected locking system.

However, in some tabs, you can decide for yourself which entries you want to see:

- Only the entries for a specific locking system (e.g. all identification media of a company with its own locking system)
- All entries from all locking systems (e.g. all identification media in a building with multiple companies, each with its own locking system)

Simply open the drop-down menu in the corresponding tabs and select one or all locking systems. As an example, you can see some tabs where you can change the locking system.

[Matrix view]

Matrixansicht x Hogwarts

Neue Schließung
Neuer Transponder
Neue PinCode
Duplizieren
Löschen

Person

Standard Personengruppe

Lupin, Remus

Snape, Severus

Weasley, Ron

Wood, Oliver

Gryffindor electronic portrait

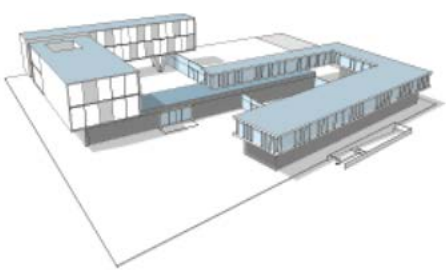
Students

Professors

Quidditch field entrance

Students

Professors



Tür	Typ	Sync
Castle		
Gryffindor dormit...	🔒	
Lands		
Gryffindor tower	🔒	
Main gate	🔒	
Quidditch field	🔒	
Snape's dungeon	🔒	

X	X	X

X	X	X

X	X	X

[Locks]

Schließungen x Hogwarts

Neu
Löschen
In Matrix anzeigen
Duplizieren
Batteriewechsel
Export

Tür	Raumnummer	Etage	Typ	Status
> Gryffindor dormitory			🔒	
Gryffindor tower			🔒	
Main gate			🔒	
Quidditch field			🔒	
Snape's dungeon			🔒	

[Transponder]

Transponder x Hogwarts

Neu
Löschen
In Matrix anzeigen
Duplizieren
Ausgabe
DSGVO-Daten
Export
Anzeigefilter löschen
Importieren

Nachname	Vorname	S/N	Typ	Sync	Status	Zeitgruppe
> Lupin	Remus	135CK3L	🔑			
Snape	Severus	0301A4D	🔒			Zeitgruppe 2
Weasley	Ron	00XTN6K	🔒			
Wood	Oliver	UID-148024BA5A7369	🔒			

[PinCodes]

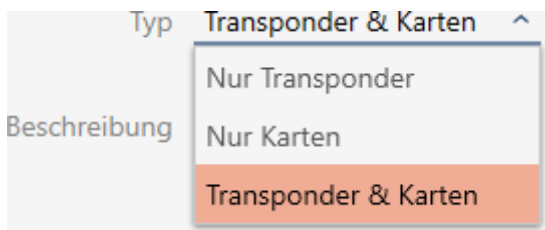
Name	Schließung	S/N	Typ
Gryffindor electronic portrait	Gryffindor tower	088NKAK	AX PinCode
Quidditch field entrance	Quidditch field		PinCode G1

[Access levels]

Name	Beschreibung	Anzahl Schließungen	
Gryffindor		3	3
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

17.4 Enable cards or transponders

When you created your locking system, you decided in the ▼ **Type** drop-down menu which type of identification media should be used in your locking system:



Circumstances may have changed in the meantime and you would now like to use cards in your locking system, for example. You thus switch your locking system from active (= transponder only) to hybrid (= transponder + cards). This is not a problem with AXM Plus as you can simply activate additional cards or transponders here.


Please note that you can only address a limited number of locking devices with cards when cards are enabled at a later date (see *Cards and locking device IDs* [▶ 552]).

You will not have this problem with transponders enabled at a later date.

**Enabling cards**

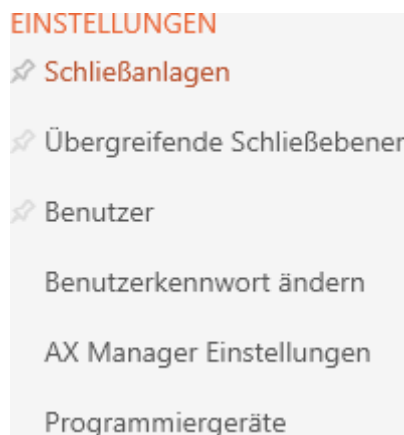
The following example describes how you can also use cards in an exclusively transponder-based locking system. When we say cards, we are also referring to other RFID identification media, such as smart tags or RFID inlays. The MC1000L\_AV template is used in the example.

✓ At least one locking system created (see *Create locking system* [▶ 349]).

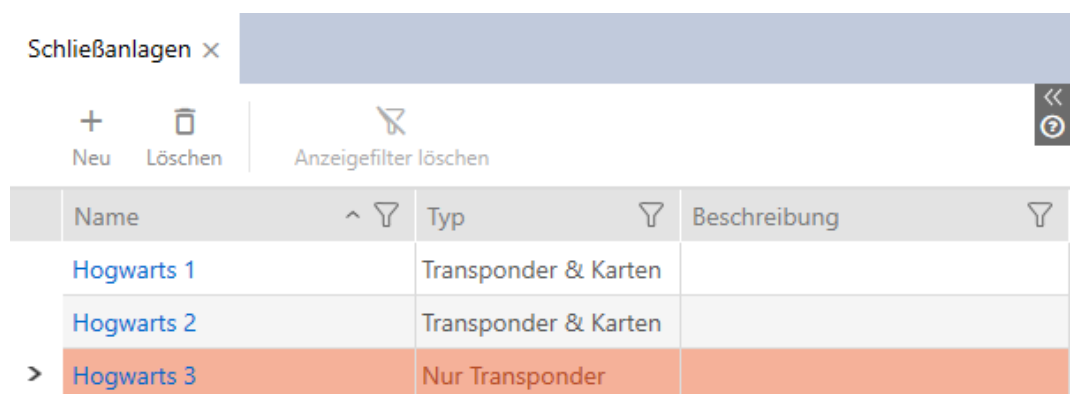
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.




2. Select the **Locking systems** entry in the | SETTINGS | group.



↳ The [Locking systems] tab with a list of all locking systems in the database will open.

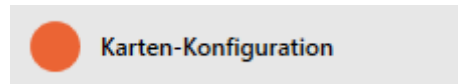


3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
4. Select the locking system in which you'd like to enable cards or transponders.
  - ↳ The Locking system window will open.

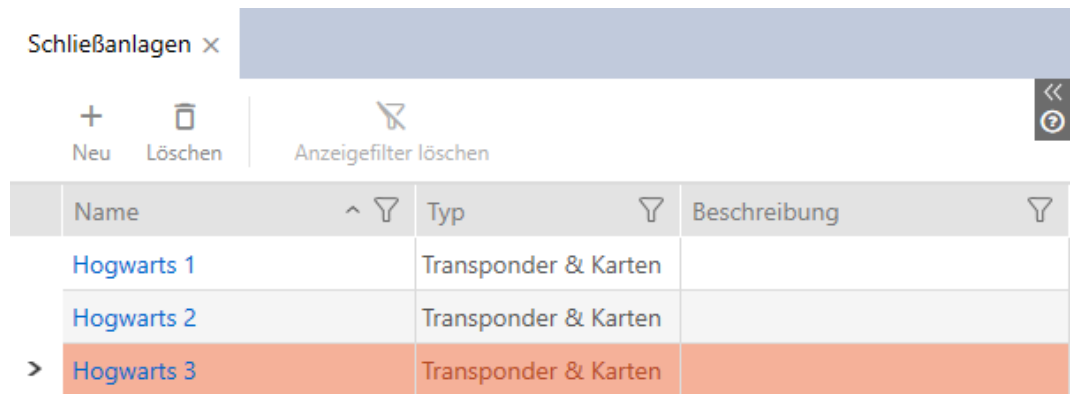
5. Select your locking system type from the ▼ **Type** drop-down menu: "Transponders only", "Transponders & cards" or "Cards only".

↳ A warning window will open.

6. Click on the **Yes** button.
  - ↳ Warning window closes.
  - ↳ The **Card configurations** tab will appear if required.



7. If you have switched to a "Transponders & cards" or "Cards only" type, enter the card configuration (see *Adding a card configuration* [▶ 354]).
8. Click on the **Finish** button.
  - ↳ Window "Locking system" closes.
- ↳ Locking system is now listed with a new locking system type.



### 17.5 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* [▶ 392]).
2. Create a transponder in one of the assigned locking systems (see *Creating transponders for common locking level* [▶ 395]).
  - ↳ 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* [▶ 396]).

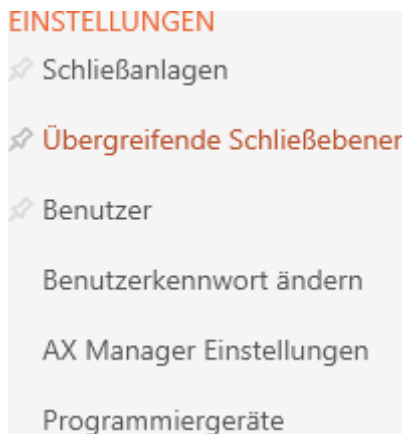
#### 17.5.1 Creating a common locking level

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





2. Select the **Service Sets** entry in the | SETTINGS | group.

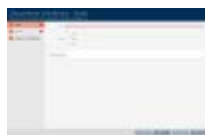


↳ The [Service Sets] tab will open.



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* [▶ 44]).
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.



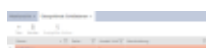
14. Click the **Finish** button.
  - ↳ Explorer window for saving the password as a PDF will open.



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* [▶ 395]).

### 17.5.2 Creating transponders for common locking level




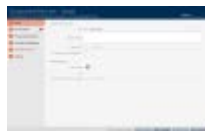
#### NOTE

#### Activating cards or transponders for a locking system

The only credential types available are those that have been activated in your locking system.

- If necessary, activate cards or transponders in the locking system properties (see *Enable cards or transponders* [▶ 389]).

- ✓ List with transponders or matrix screen opened.
  - ✓ Common locking level created and locking system assigned (see *Creating a common locking level* [▶ 392]).
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* [▶ 89]).
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:



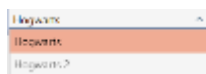
You can now authorise the transponder created in multiple locking systems at the different locking devices in the locking systems (see *Authorising a transponder with common locking level* [▶ 396]).

After synchronisation is complete, the *Transponder* and *Colour* fields are displayed in the common locking level colour (example: red).



### 17.5.3 Authorising a transponder with common locking level

- ✓ Matrix screen open.
  - ✓ Common locking level created (see *Creating a common locking level* [▶ 392]).
  - ✓ Transponder created in common locking level (see *Creating transponders for common locking level* [▶ 395]).
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.

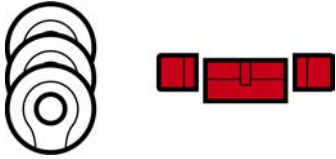
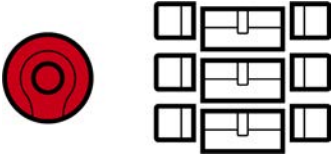
4. Assign all desired authorisations there as well.



5. Synchronise the locking devices and transponders as usual (see *Synchronising the locking device (including reading access list)* [▶ 399] and *Synchronising an identification medium* [▶ 409]).
  - ↳ Thanks to the common locking level, the same transponder can operate locking devices from different locking systems.

## 18. 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
<p><i>Synchronising the locking device (including reading access list) [▶ 399]</i></p>	<p><i>Synchronise a card/transponder (including importing physical access list) [▶ 410]</i></p>
<p>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.</p> 	<p>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.</p> 



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

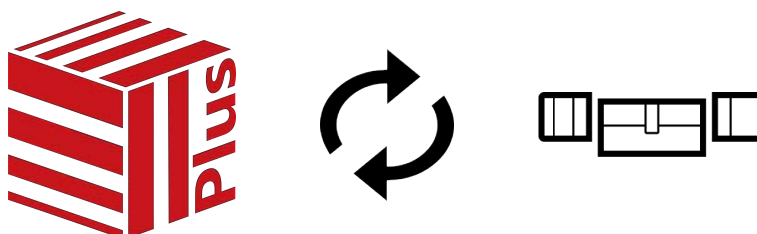
You can display the synchronisation requirement in the matrix. If you click directly on the  icon, you immediately start synchronising the entry concerned.

### 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.




### 18.1 Synchronising the locking device (including reading access list)



Synchronisation is bidirectional:

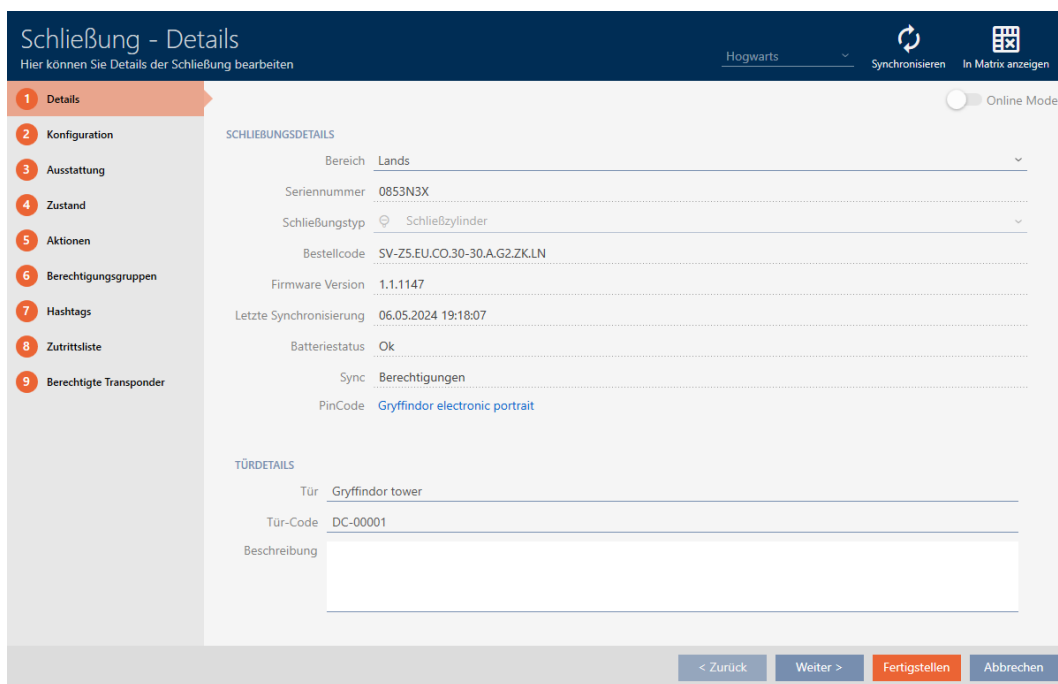
- Reading of data stored in the locking device (e.g. battery level)
- Writing of new data onto the locking device (e.g. authorisations)


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* [[▶ 439](#)]).

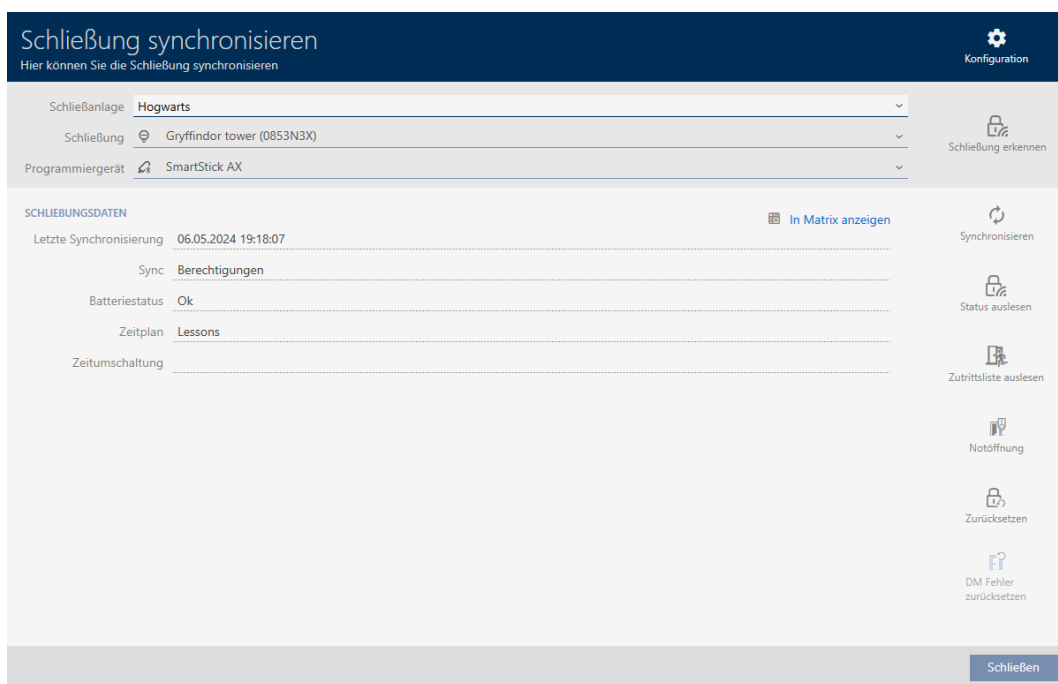
The imported data can then be displayed (see *Display locking device equipment and status* [[▶ 402](#)] or *Displaying and exporting a locking device's access list* [[▶ 404](#)], for example).

- ✓ 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.






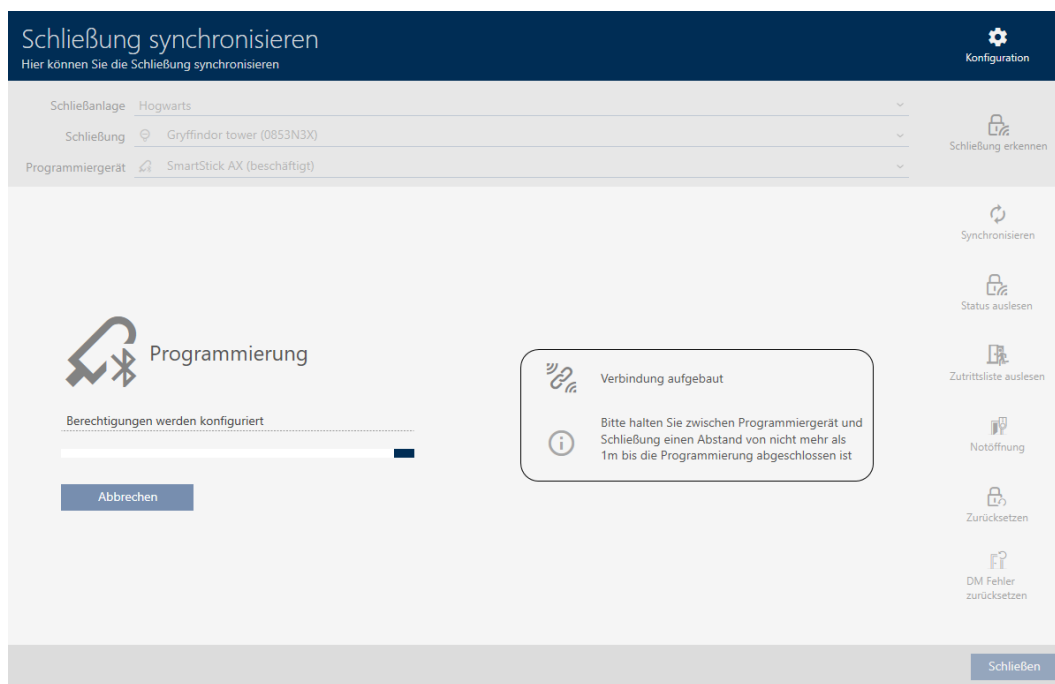
**NOTE**

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

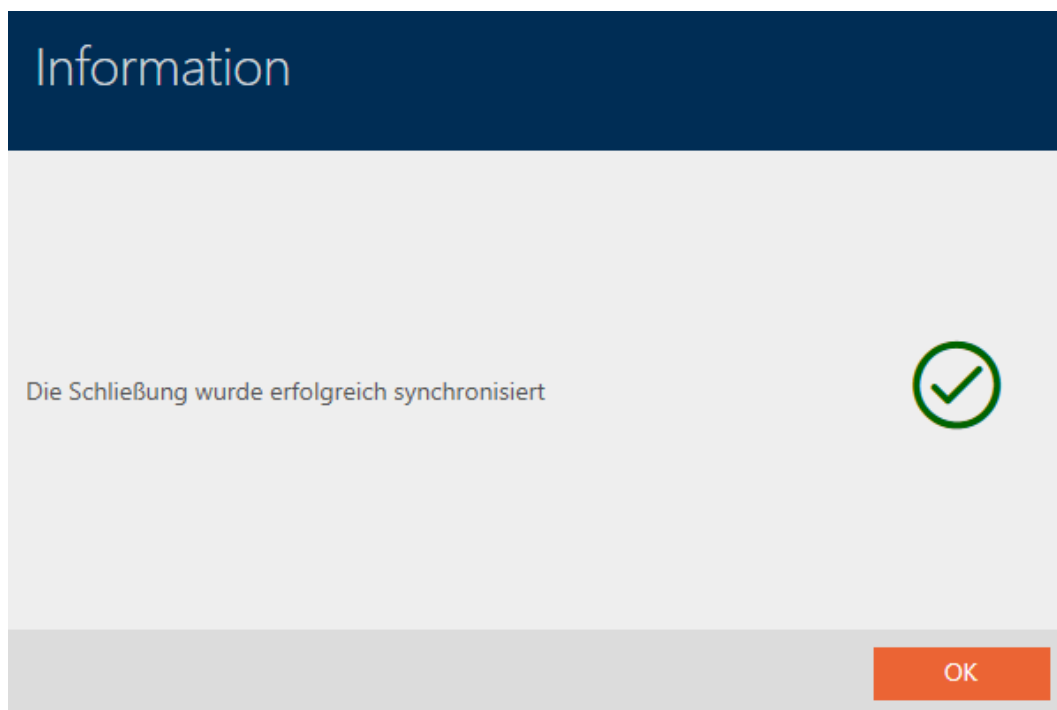
A great deal of data is transferred during initial synchronisation of AX components. The carrier frequency and, consequently, the transmission speed is significantly higher with the SmartCD.MP or SmartStick AX.

- 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.

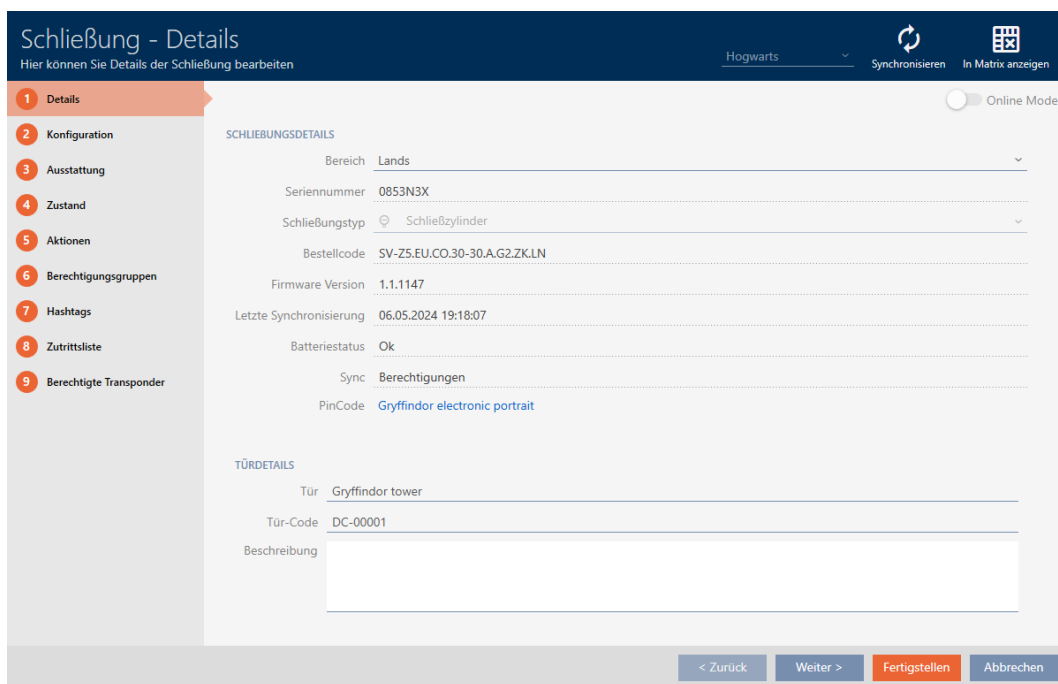
**NOTE****First transponder activation rejected after initial programming of AX products**

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.

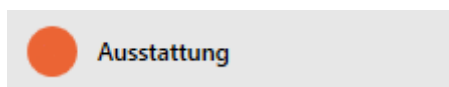
**18.1.1 Display locking device equipment and status****NOTE****Displayed status corresponds to the last synchronisation**

AXM Plus displays the status stored in the database at this point.

- ✓ Locking device synchronised at least once.
- 1. Click on the locking device whose status you wish to display.
  - ↳ The locking device window will open.



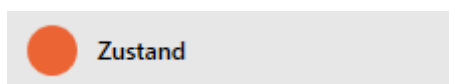
2. Click on the **Features** tab.



- ↳ 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 / Zeitonensteuerung
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).



### 18.1.2 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)* [▶ 284]). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation* [▶ 439] and *Synchronising the locking device (including reading access list)* [▶ 399]).

You can view and export the access list in the database.



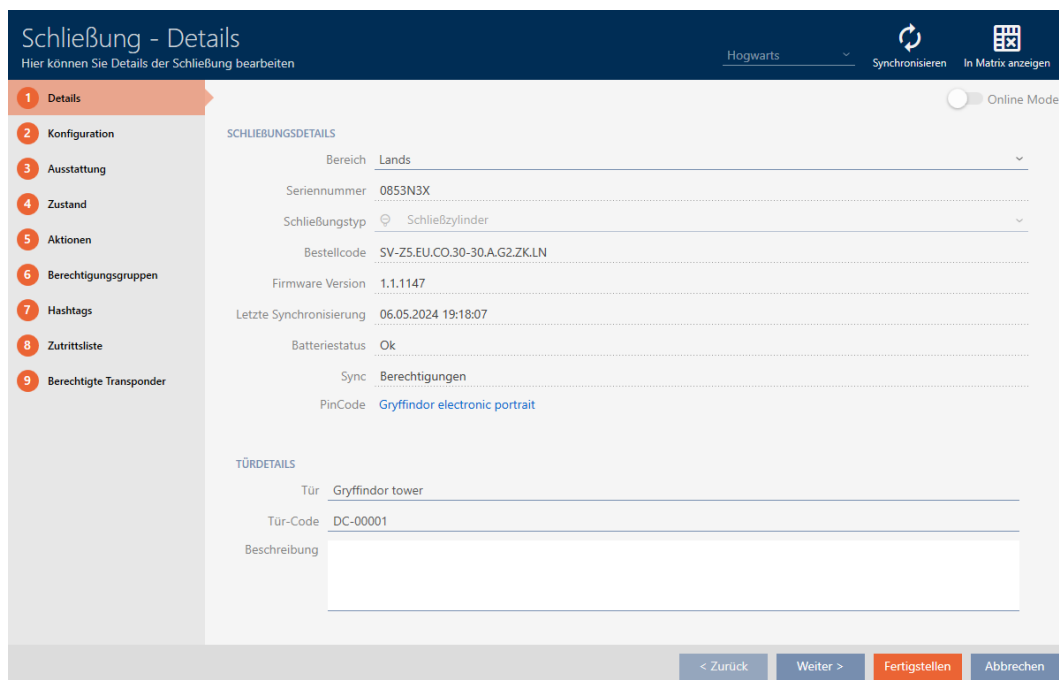
#### NOTE

#### Displayed status corresponds to the last synchronisation

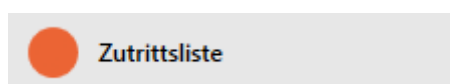
AXM Plus displays the status stored in the database at this point.

✓ 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 **Zutrittsliste** 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* [▶ 44]).
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
14.12.2021 17:52:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 17:51:00	McGonagall, Minerva	UID-1000000034DB9B06	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
13.12.2021 20:32:00	##ServiceTId_IDS_AX_SETTIME		Erlaubt	Master

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

### 18.2 Identifying an unknown locking device

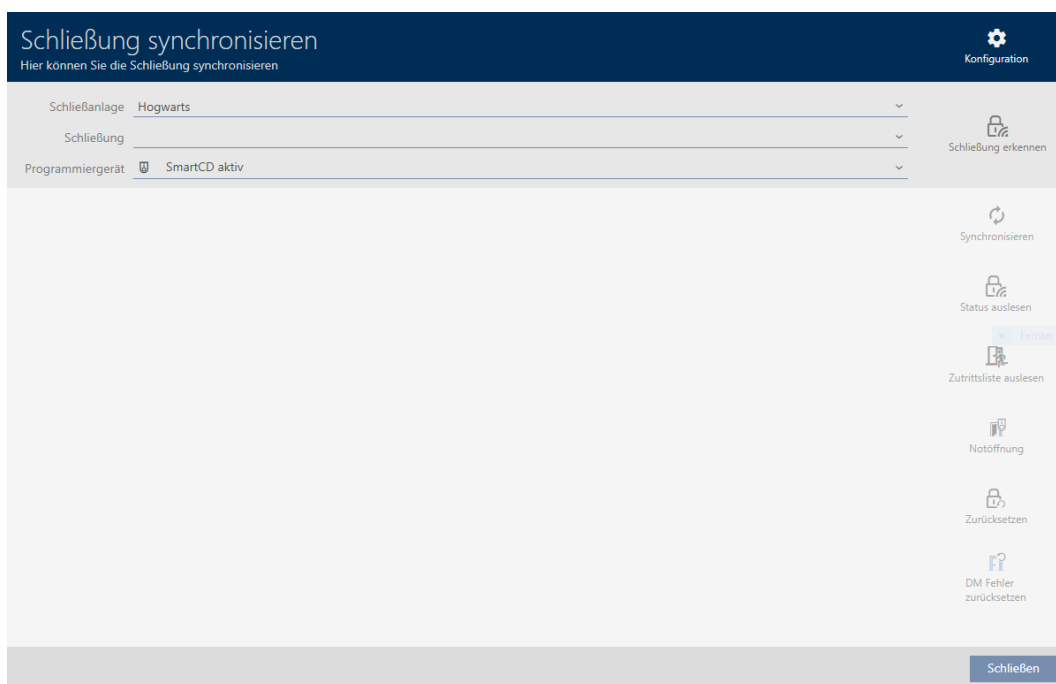
If you have an unknown locking device, you can use, for example, the synchronise symbol (🔑) to identify it and reset if necessary (see *Re-setting the locking device* [▶ 408]).

✓ Suitable programming device connected.

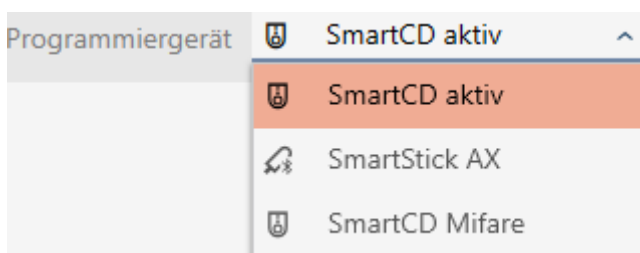
1. Click on the 🔑 icon in the header.




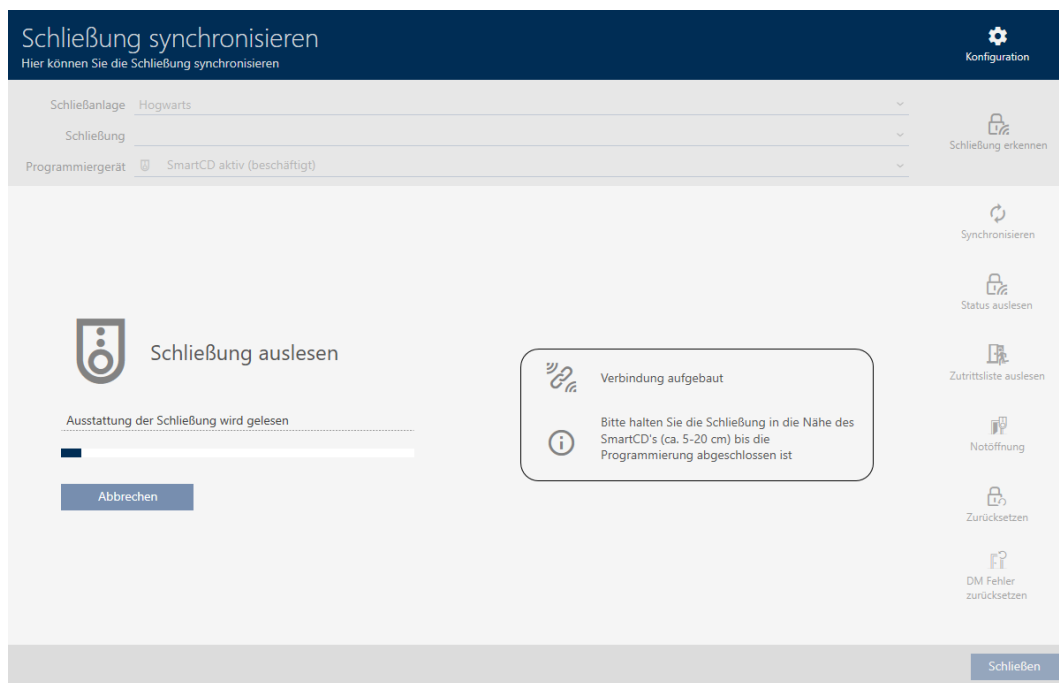
↳ The "Synchronise lock" window will open.



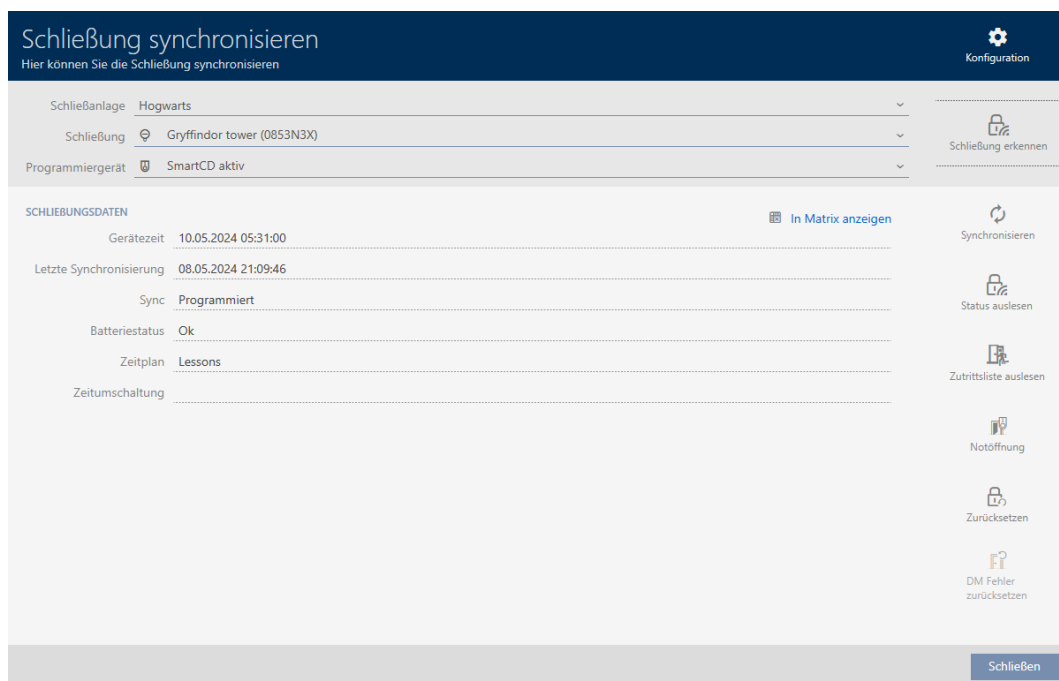
2. Select the programming device you wish to use to identify your locking device from the ▼ Programming device drop-down menu.



3. Click on the Detect lock button 
  - ↳ Locking device is identified.



- ↳ Locking device information is displayed in the locking device window.

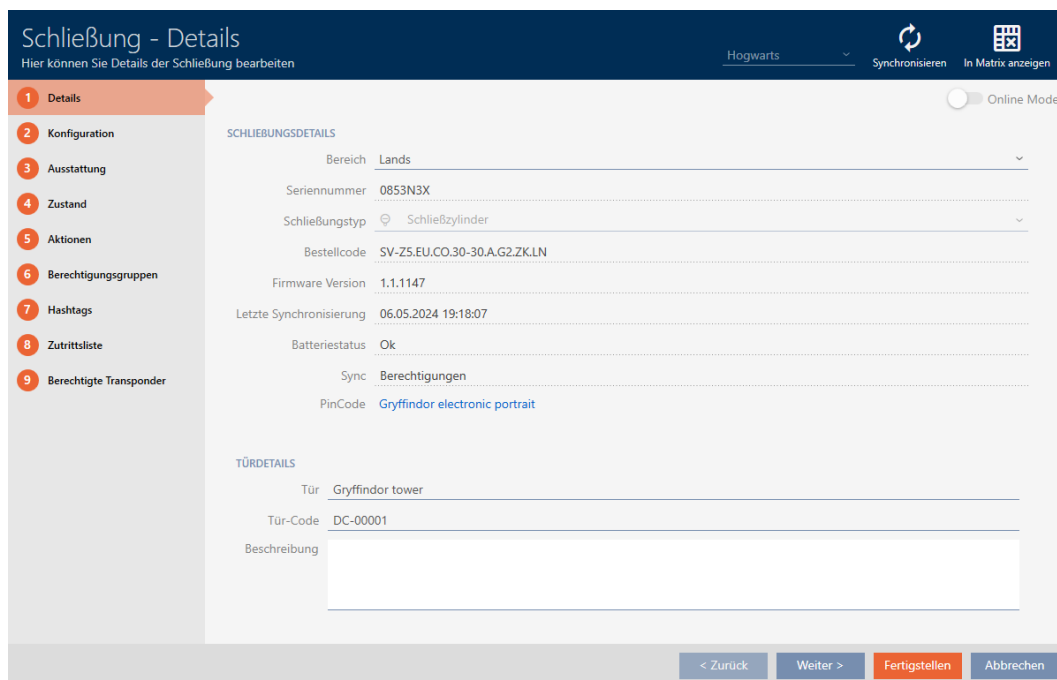



You can now reset the locking device, for example (see *Re-setting the locking device* [▶ 408]).

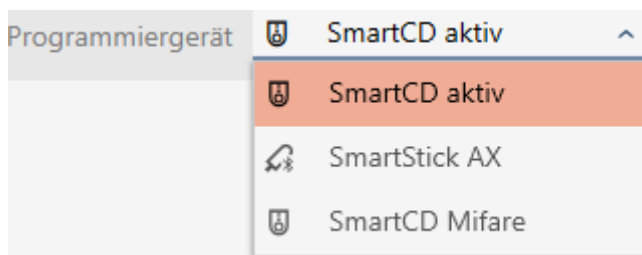
### 18.3 Re-setting the locking device


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.
  - ✓ 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* [▶ 406]). Then continue.  
↳ The locking device window will open.

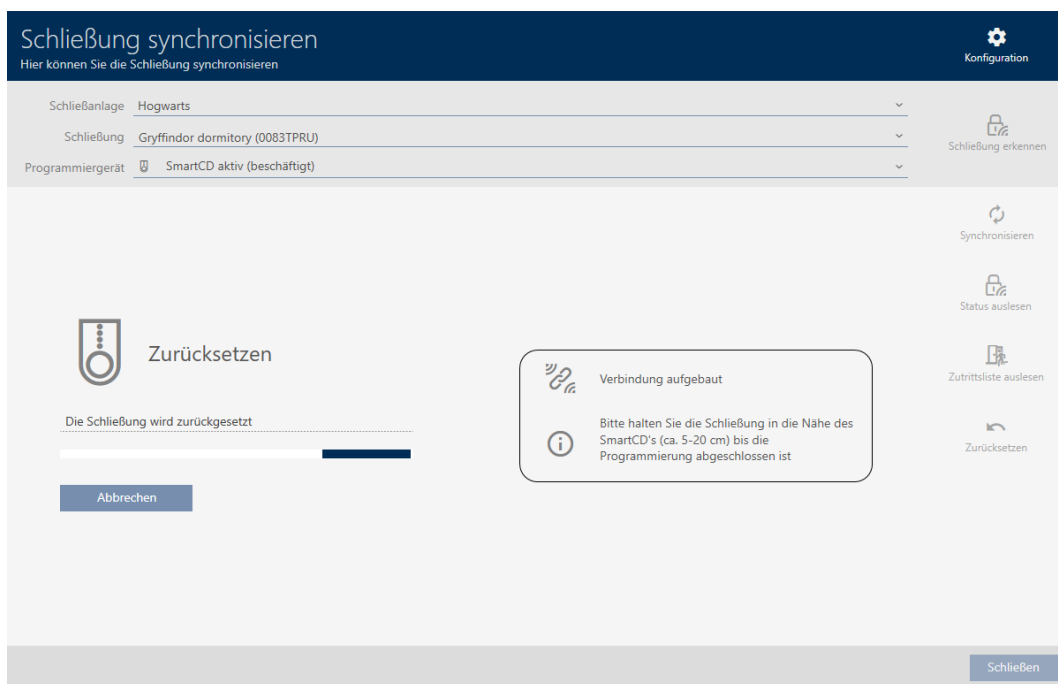


2. Click on the **Synchronisation** button .  
↳ Synchronise window will open.
3. Select the programming device from the **▼ Programming device** drop-down menu with which you wish to reset your locking device.



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.



#### 18.4 Synchronising an identification medium

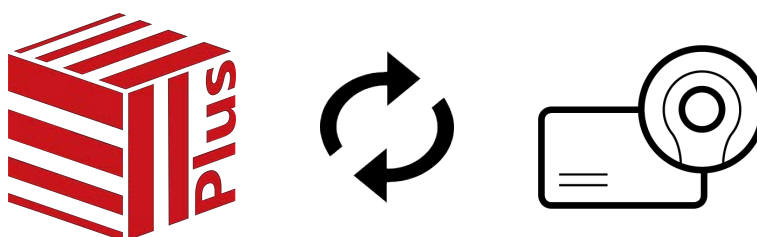
Synchronisation is bidirectional:

- 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* [▶ 439]).

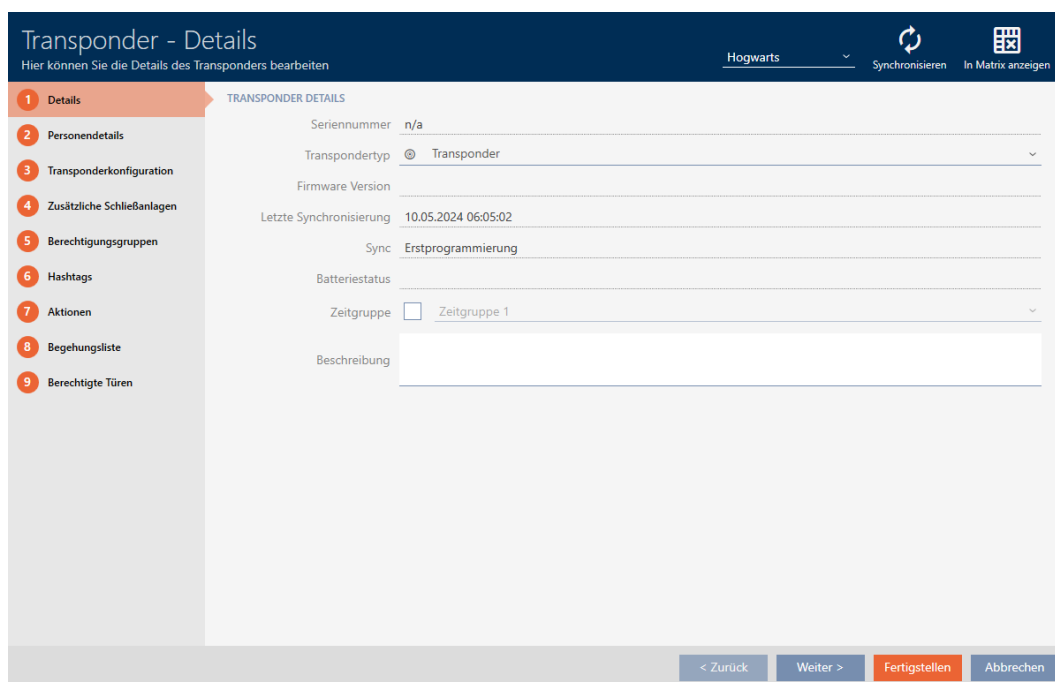
The imported data can then be displayed (see *Displaying the identification medium battery status* [▶ 412] or *Displaying and exporting physical access lists for cards/transponders* [▶ 413], for example).

### 18.4.1 Synchronise a card/transponder (including importing physical access list)

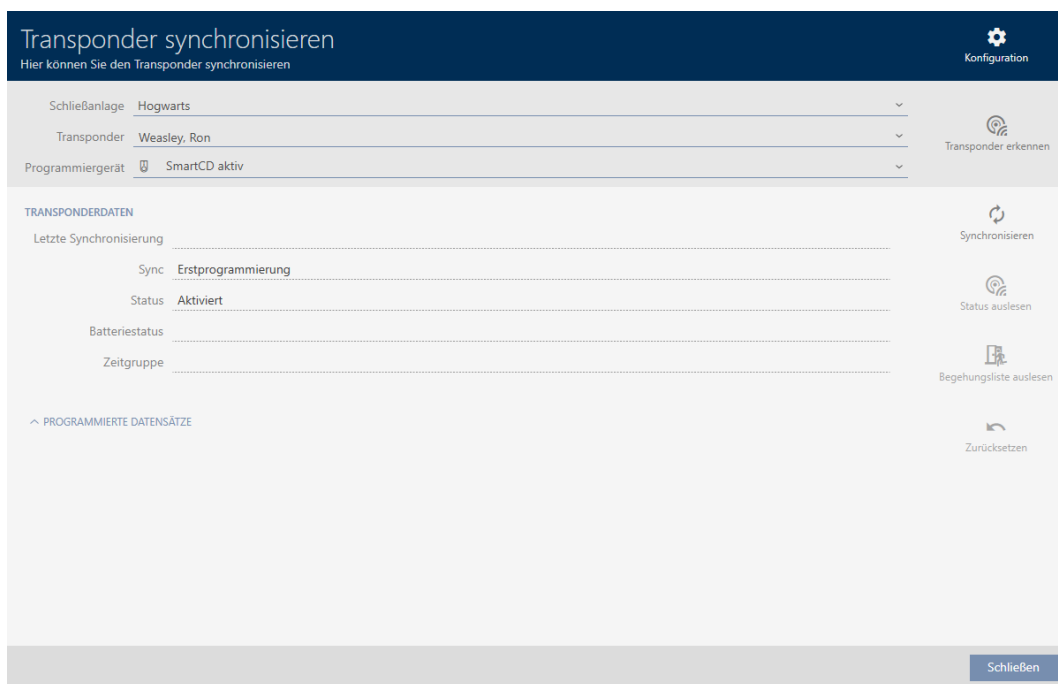


The following example shows how to synchronise a transponder.

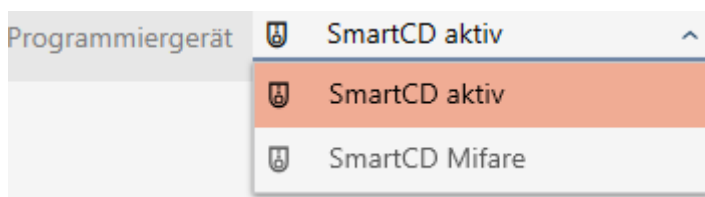
- ✓ Suitable programming device connected.
  - ✓ Identification media list or matrix view open.
1. Click on the identification medium you wish to synchronise.
    - ↳ The identification medium window will open.




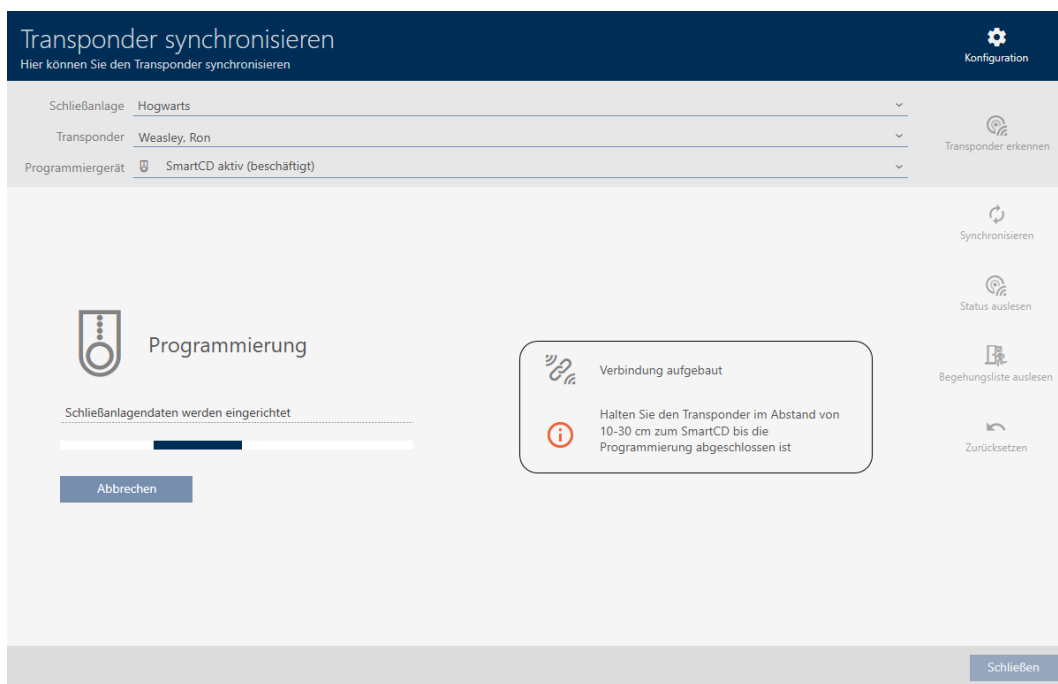
2. Click on the **Synchronisation** button .
  - ↳ Synchronise window will open.



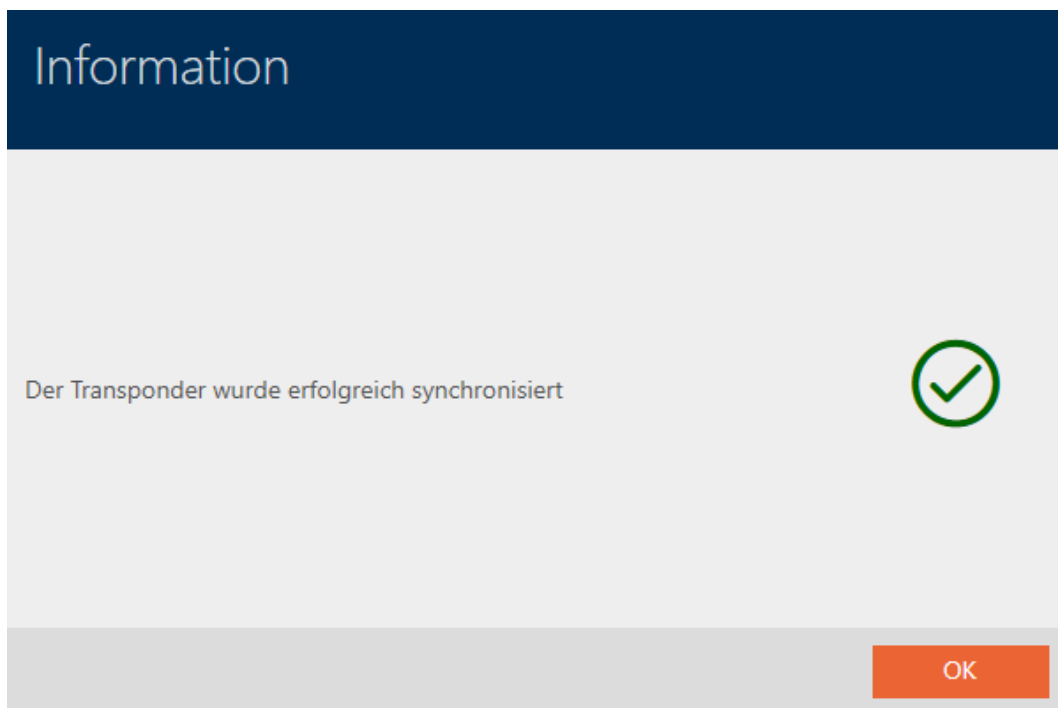
3. Select the programming device which you wish to use to synchronise from the ▼ Programming device drop-down menu.



4. Click on the **Synchronisation** button .
  - ↳ Identification medium is synchronised.



↳ ID medium is synchronised.



18.4.1.1 Displaying the identification medium battery status



**NOTE**

**Displayed status corresponds to the last synchronisation**  
AXM Plus displays the status stored in the database at this point.

- ✓ 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.

#### 18.4.1.2 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)* [▶ 118]). 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)* [▶ 410]).

You can view and export the physical access lists saved in the database.

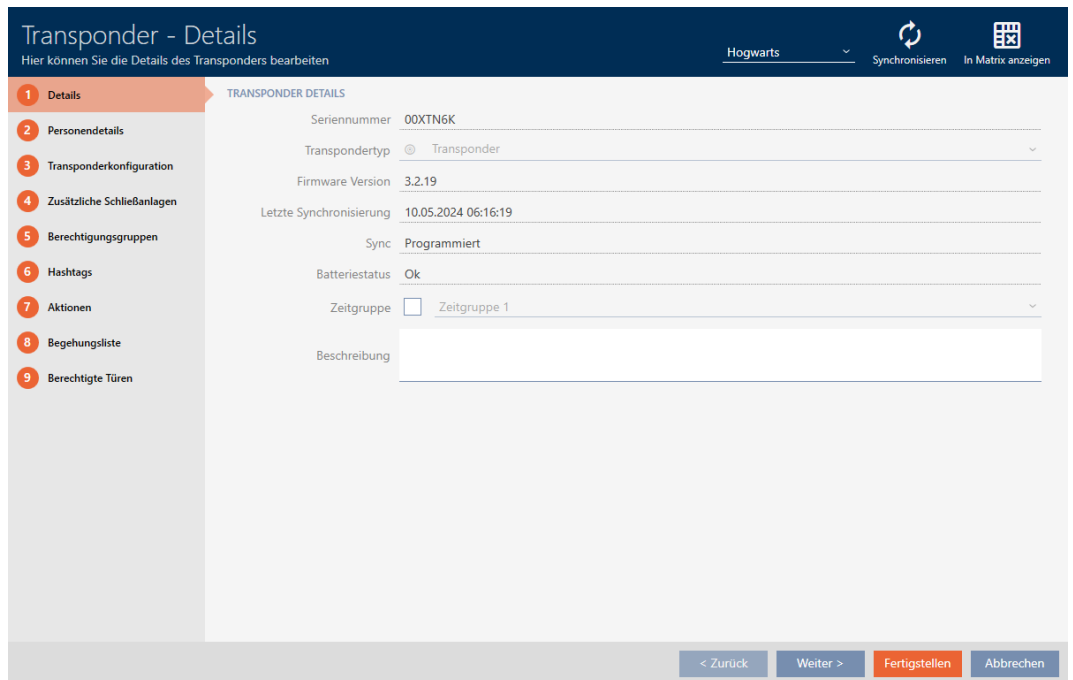


### NOTE

#### Displayed status corresponds to the last synchronisation

AXM Plus displays the status stored in the database at this point.

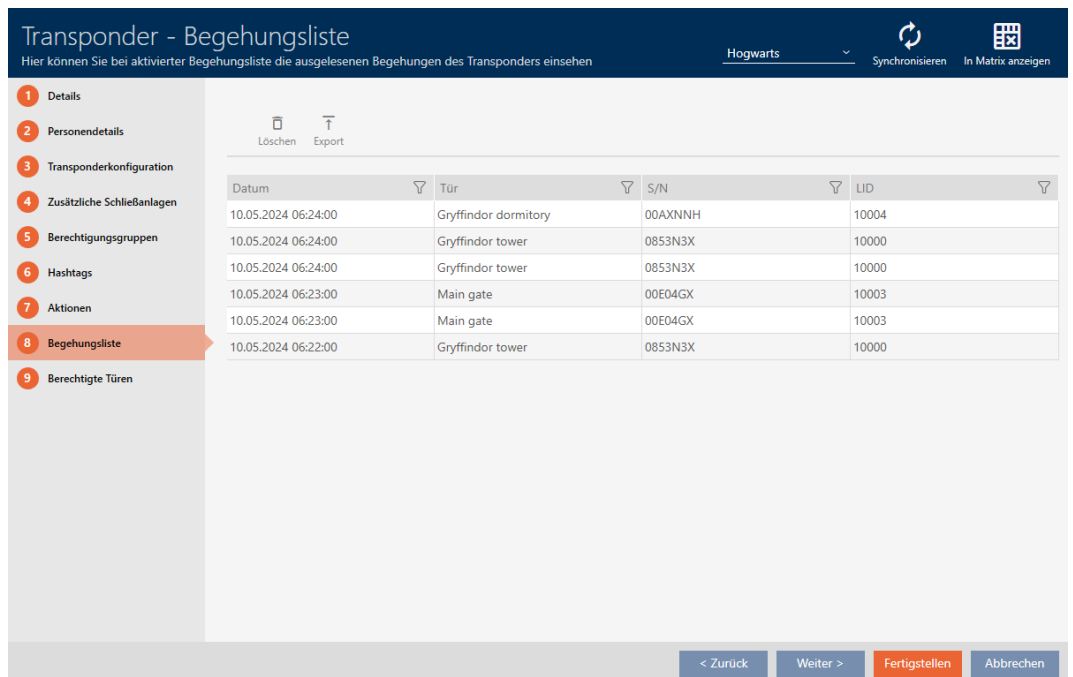
- ✓ Identification medium synchronised at least once.
- 1. Click on the identification medium whose physical access list you wish to display.
  - ↳ The identification medium window will open.



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* [▶ 44]).

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 Weasley '00XTN6K'**

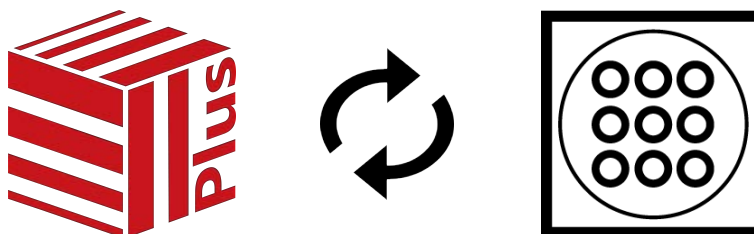
Datum	Tür	S/N	LID
10.05.2024 06:24:00	Gryffindor dormitory	00AXNNH	10004
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:22:00	Gryffindor tower	0853N3X	10000



Ausdruck vom: 10.05.2024

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

18.4.2 Synchronising a PIN code keypad



Changes to a PIN code keypad can also entail programming requirements for the assigned locking device (see *PIN Code G1 vs. PIN Code AX* [▶ 514]). In this case, synchronise the locking device instead (see *Synchronising the locking device (including reading access list)* [▶ 399]).

Synchronisation between the two PIN code keypads is different. Your AXM Plus will assist you with instructions during synchronisation.




**NOTE**

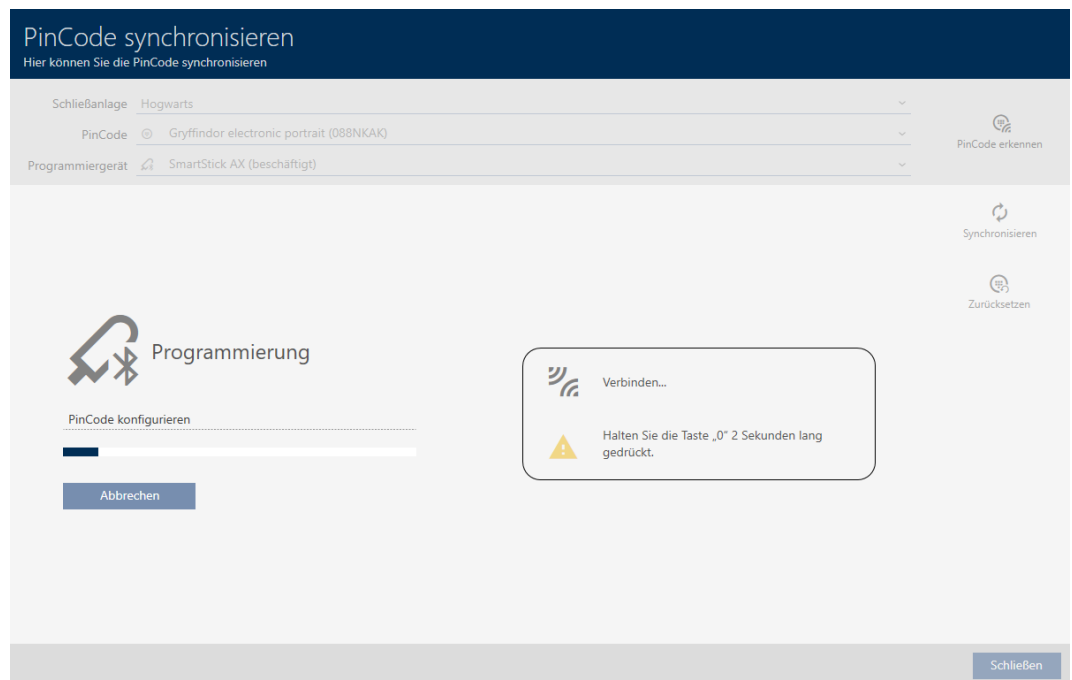
**PIN code keypad 3068 synchronisation requires a master PIN and user PINs**

In PIN code keypad 3068, the user PINs are linked to a G1 ID. The G1 IDs cannot be accessed and synchronised without user PINs being configured.

1. Change the factory default master PIN (see the PIN code keypad 3068 manual).
2. Assign at least one user PIN.

In the following example, a PIN code keypad AX is synchronised.

- ✓ PIN code keypad AX created and assigned (see *Creating PIN code keypads [▶ 96]*).
  - ✓ Programming requirement for PIN code keypad AX, e.g. due to a change in authorisation.
  - ✓ Suitable programming device connected (SmartStick AX).
  - ✓ Matrix screen open.
1. Click the synchronise icon  for any PIN associated with the PIN code keypad AX concerned.
    - ↳ The "Synchronise PinCode" window opens and synchronisation starts.

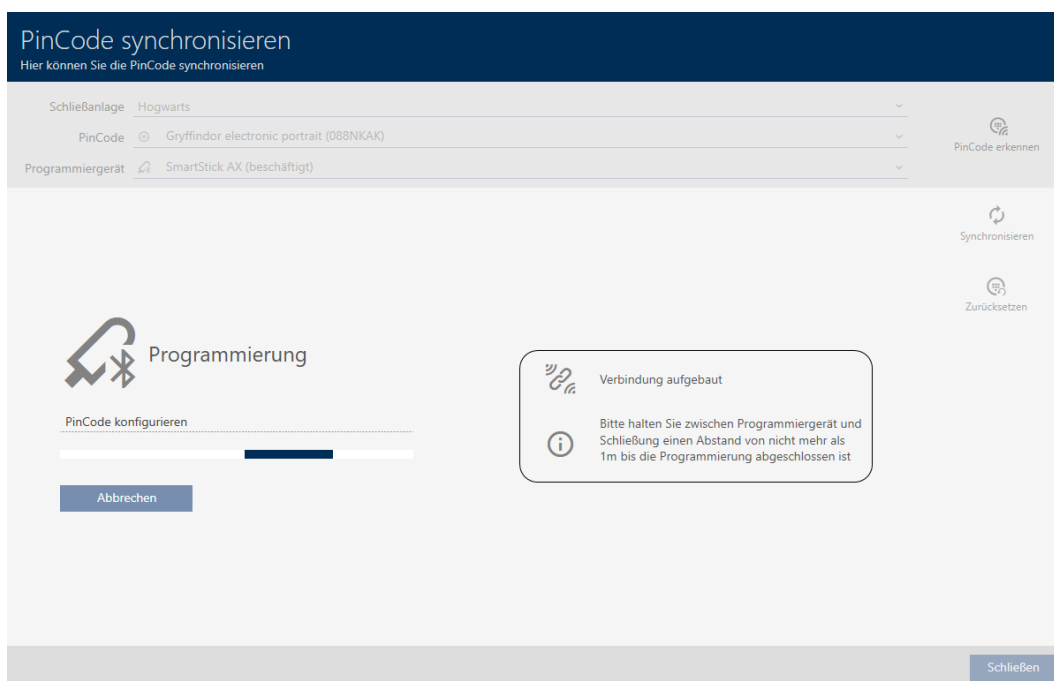




- Press and hold the “0” button on the PIN code keypad AX for at least two seconds.



- Position the SmartStick AX close to the PIN code keypad AX (max. 1 m).
  - ↳ LED flickers green and PIN code keypad AX beeps.
  - ↳ BLE interface has been wakened.
  - ↳ PIN code keypad AX is synchronised.



- ↳ PIN code keypad AX is synchronised.

**NOTE****PIN code keypad AX in programming mode after synchronisation**

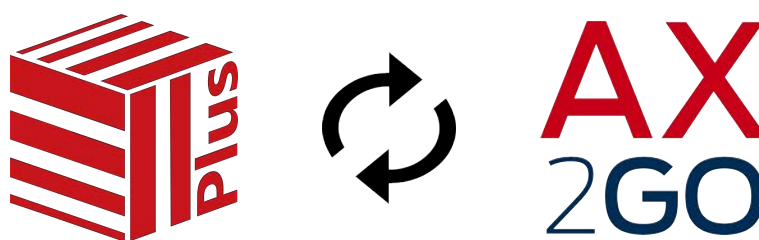
After synchronisation is complete, the PIN code keypad AX will not function for about 30 seconds as it is still in programming mode.

**Information**

Die PinCode wurde erfolgreich synchronisiert



OK

**18.4.3 Synchronising AX2Go key**

After AX2Go is set up for the first time, changes are transmitted conveniently via the SimonsVoss Cloud (see *Synchronisation of AX2Go keys via the cloud* [▶ 518] for more information).

The following example describes the synchronisation process when an AX2Go key is authorised for a locking device for the first time.

In the initial situation, no AX2Go key has been authorised on the locking device yet:

The screenshot displays the AXM Plus software interface. At the top left is a 3D perspective view of a building. Below it is a table with columns 'Tür', 'Typ', and 'Sync'. The table lists doors under 'Castle' and 'Lands' categories. 'Snape's dungeon' is highlighted in orange. To the right is a 'Person' selection table with columns for 'Standard Personengruppe' and 'Gryffindor electronic portrait'. Below these is a matrix screen with a grid of cells, some containing 'X' marks and others containing icons.

Tür	Typ	Sync
Castle		
Gryffindor dormit...	🔑	
Lands		
Gryffindor tower	🔑	
Main gate	🔑	
Quidditch field	🔑	
Snape's dungeon	🔑	

Person	Typ	Sync
Standard Personengruppe		
Lupin, Remus	🔑	
Snape, Severus	🔑	
Weasley, Ron	🔑	
Wood, Oliver	🔑	
Gryffindor electronic portrait		
Students	🔑	
Professors	🔑	
Quidditch field entrance		
Students	🔄	
Professors	🔄	

- ✓ Valid  Service fee licence (see *Registration with licence* [▶ 34]).
- ✓ Connection between SimonsVoss ID and AXM Plus (see *Registration with licence* [▶ 34]).
- ✓ Matrix screen open.
- Authorise the AX2Go key for all required locking devices.
  - ↳ Programming requirements for locking device and AX2Go arise.
  - ↳ AX2Go key is automatically synchronised via the cloud.
  - ↳ Programming requirement disappears.

Tür	Typ	Sync
Castle		
Gryffindor dormit...	🔑	
Lands		
Gryffindor tower	🔑	
Main gate	🔑	
Quidditch field	🔑	
Snape's dungeon	🔑	

Person	Typ	Sync
Standard Personengruppe		
Lupin, Remus	🔑	
Snape, Severus	🔑	
Weasley, Ron	🔑	
Wood, Oliver	🔑	
Gryffindor electronic portrait		
Students	🔑	
Professors	🔑	
Quidditch field entrance		
Students	🔑	↻
Professors	🔑	↻

↳ AX2Go key is authorised for locking device.

If the authorisation change is not transferred, restart the AXM service and then reconnect your AXM Plus to your SimonsVoss ID (see *Checking the connection between database and cloud* [▶ 432]).

### 18.5 Identifying an unknown ID medium

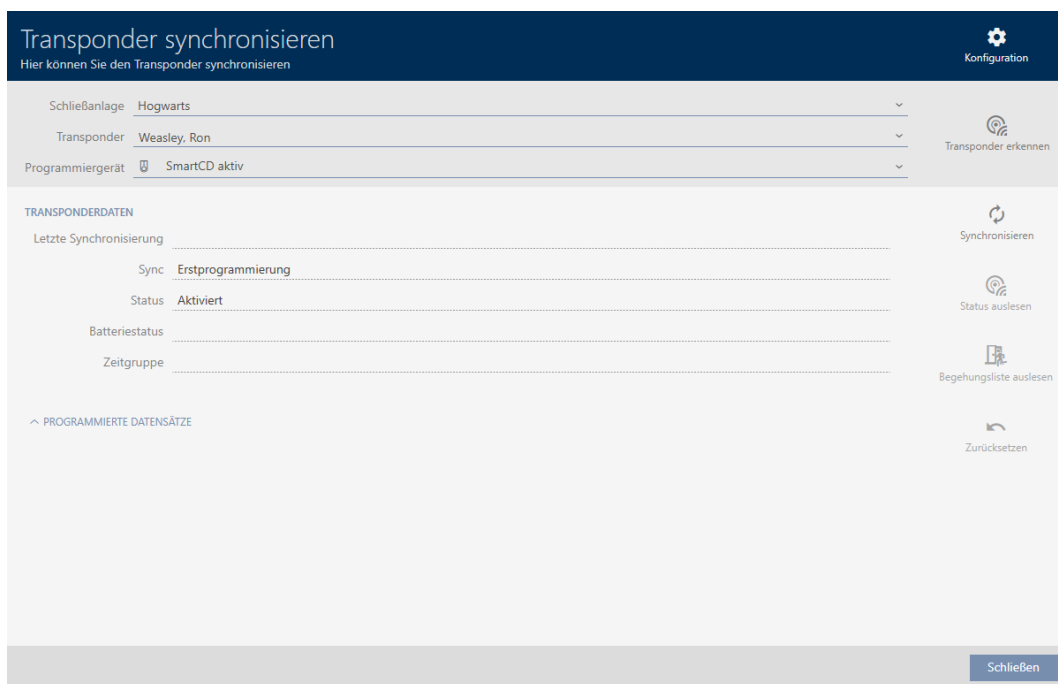
#### 18.5.1 Recognise unknown cards/transponders


✓ Suitable programming device connected.

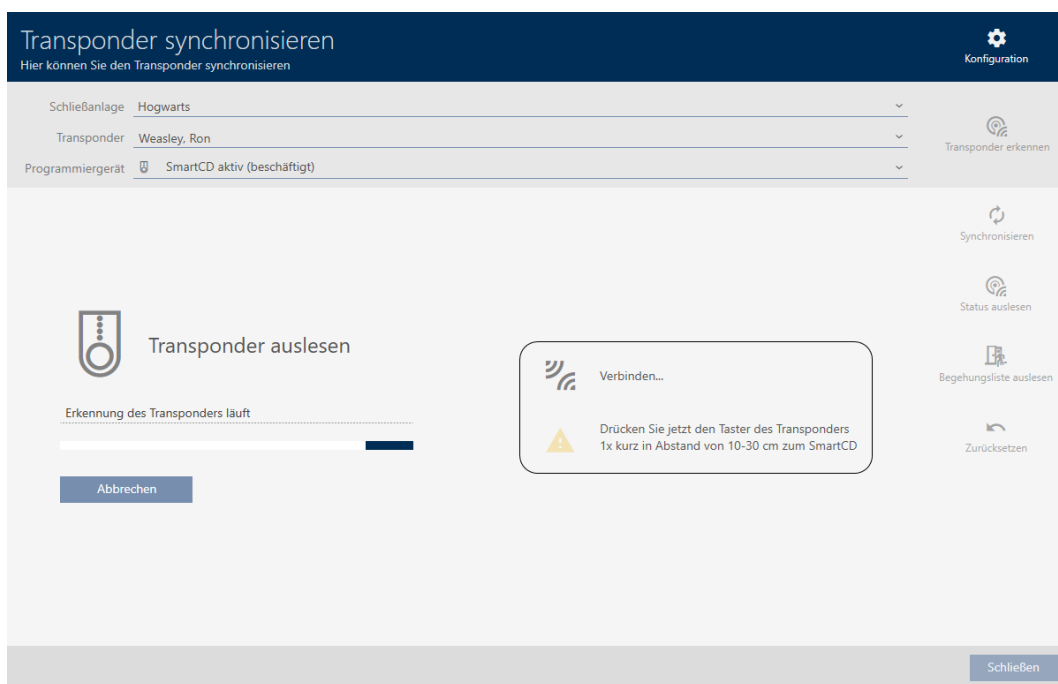
1. Click on the icon in the header.



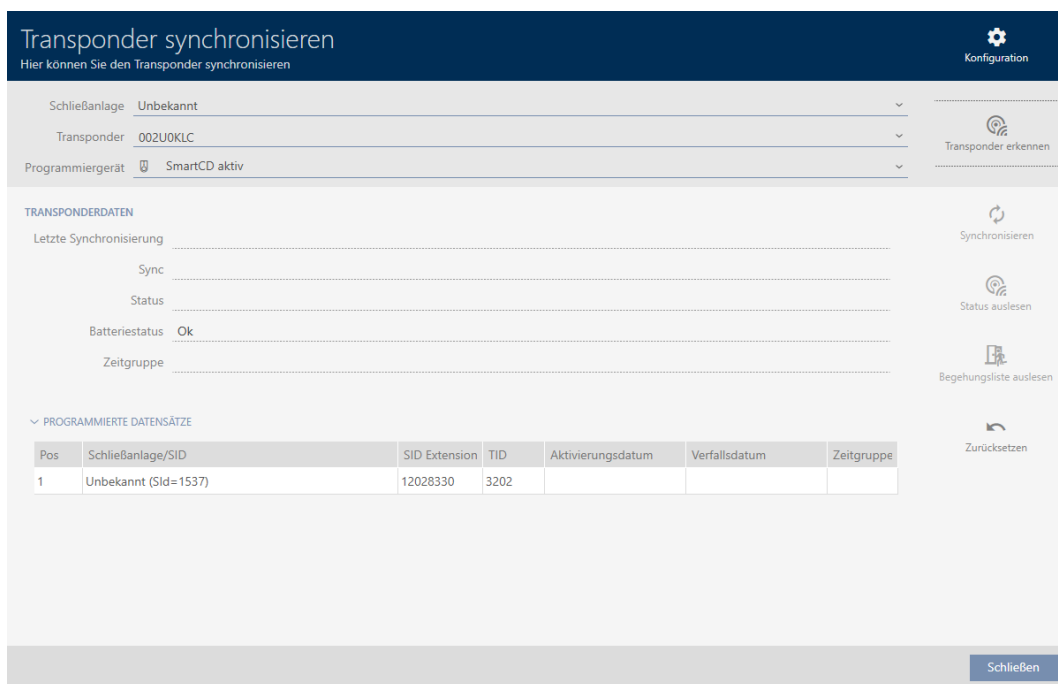
↳ The "Synchronise transponder" window will open.



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* [▶ 424]).

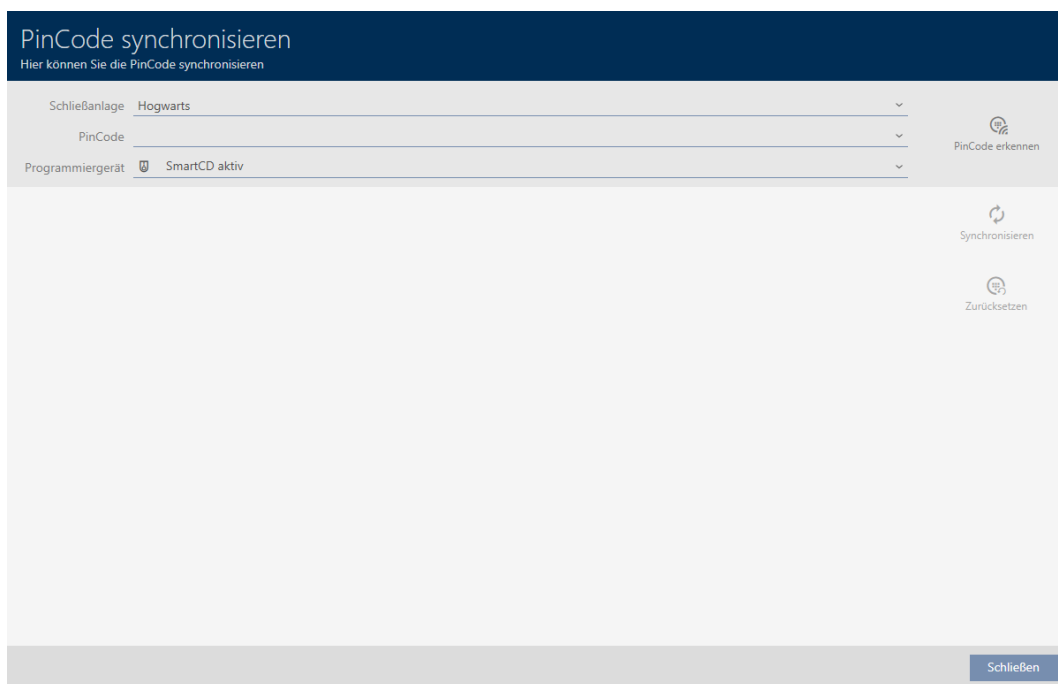
### 18.5.2 Identifying unknown PIN code keypad

- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)

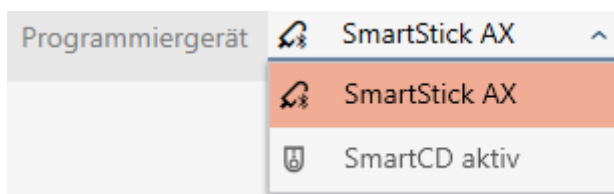
1. Click on the  icon in the header.




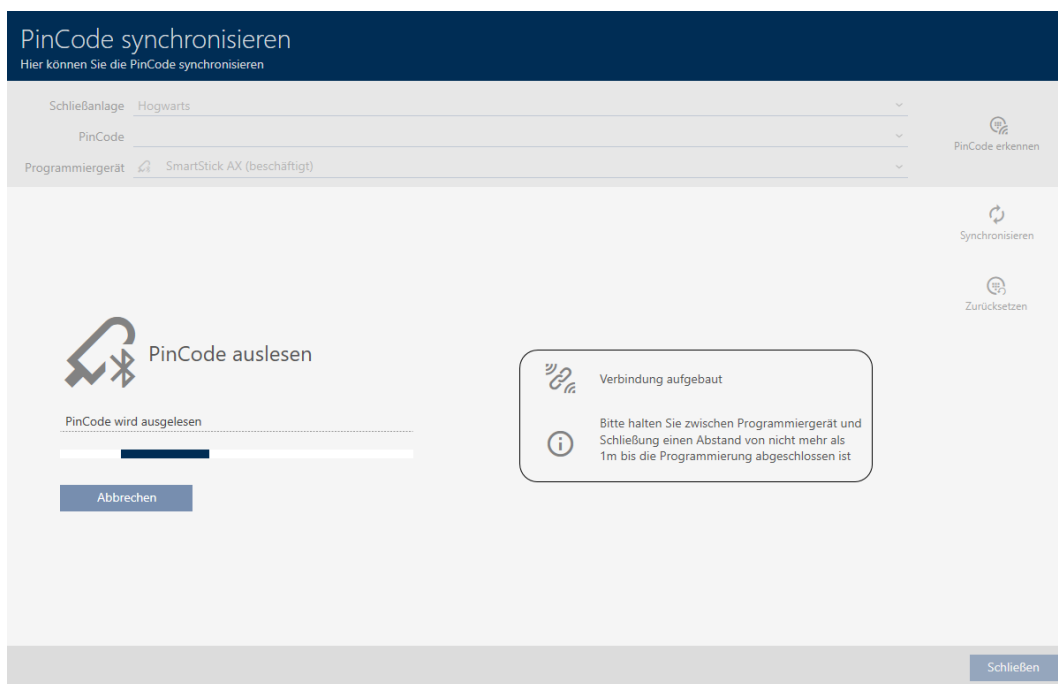
↳ The "Synchronise PinCode" window will open.



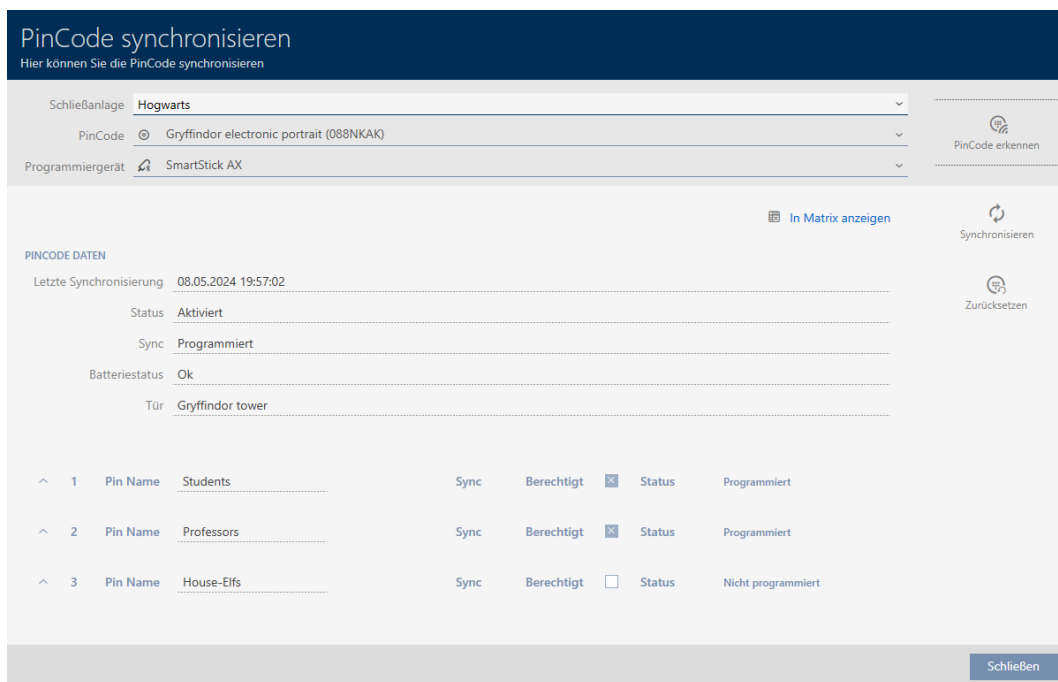
2. Select the programming device you wish to use to identify your PIN code keypad from the ▼ **Programming device** drop-down menu.



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* [▶ 428]).

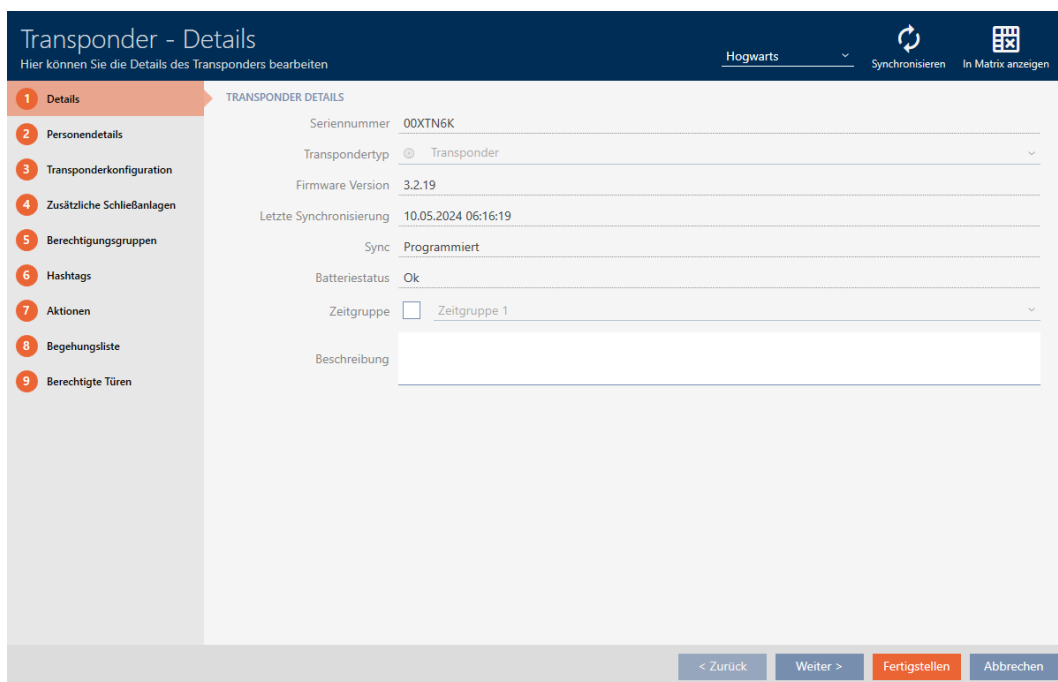
## 18.6 Resetting identification media


### 18.6.1 Resetting cards/transponders

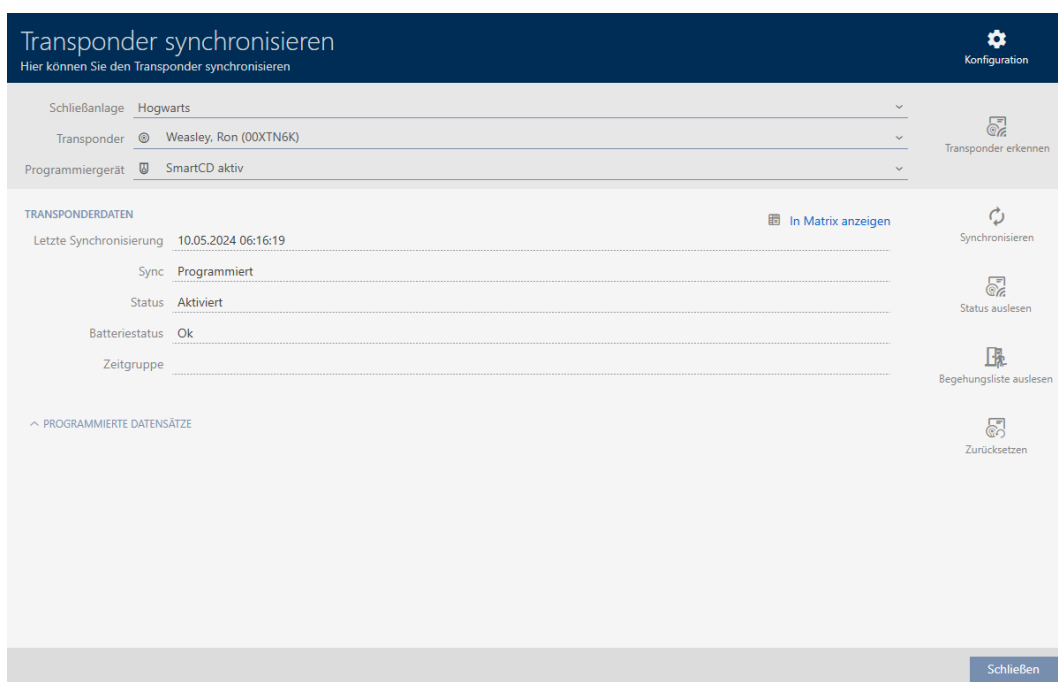
You must reset a component such as a transponder before it can be used again for an identification medium or another locking system.




- ✓ Suitable programming device connected.
  - ✓ 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* [▶ 420]). 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.

	Pos	Schließanlage	TID	Zeitgruppennummer	Deaktivierung
<input type="checkbox"/>	1	SID: 8974	3200	0	
<input checked="" type="checkbox"/>	2	Hogwarts	3209	0	



**NOTE**

**Resetting data records from unknown locking systems**

If a locking plan from a different project is stored on the identification medium, your AXM Plus 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 Plus 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.

Passwort - Schließanlage

Bitte geben Sie das Passwort der unbekanntten Schließanlage ein

Schließanlage SID: 8974, TID: 3200

OK

Abbrechen

↳ The checkbox for the data record to be reset is activated.

	Pos	Schließanlage	TID	Zeitgruppennummer	Deaktivierung
<input checked="" type="checkbox"/>	1	SID: 8974	3200		0
<input checked="" type="checkbox"/>	2	Hogwarts	3209		0

7. Click on the **OK** button.
8. Follow any further instructions as necessary.
  - ↳ Identification medium is being reset.

Transponder synchronisieren ⚙️ Konfiguration

Hier können Sie den Transponder synchronisieren

Schließanlage Hogwarts

Transponder Weasley, Ron (00XTN6K)

Programmiergerät SmartCD aktiv (beschäftigt)

Transponder erkennen

Synchronisieren

Status auslesen

Begehungliste auslesen

Zurücksetzen

## Zurücksetzen

Transponder wird zurückgesetzt

Abbrechen

Verbindung aufgebaut

Halten Sie den Transponder im Abstand von 10-30 cm zum SmartCD bis die Programmierung abgeschlossen ist

Schließen

- ↳ Identification medium is reset.

# Information

Der Transponder wurde erfolgreich zurückgesetzt

OK

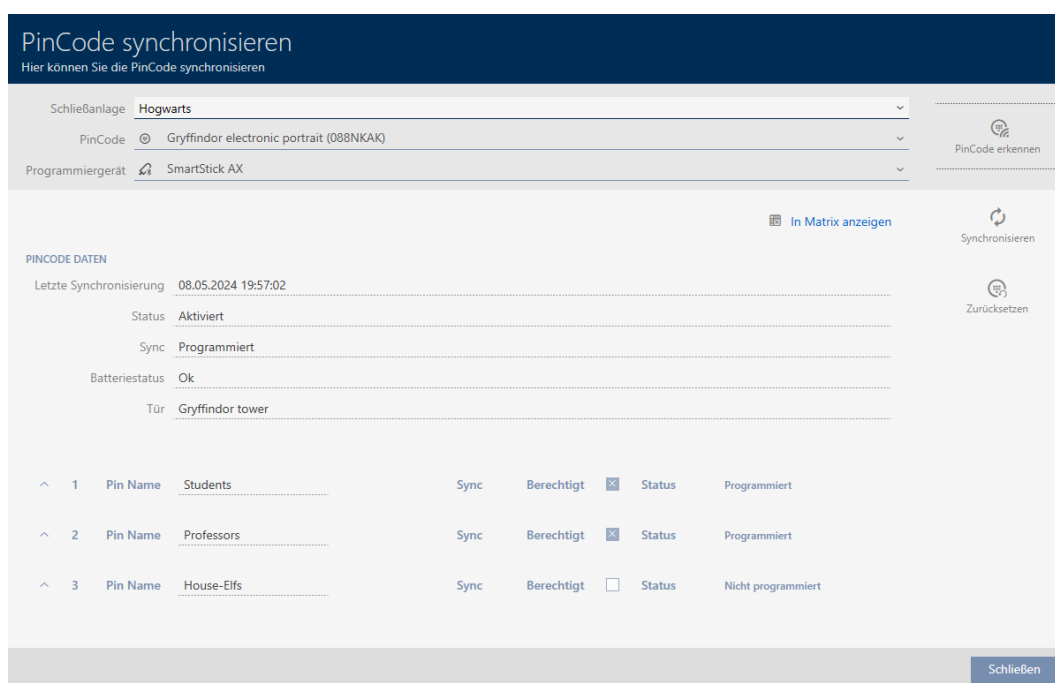
### 18.6.2 Resetting the PIN code keypad

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)
- ✓ PIN code list or matrix screen open.

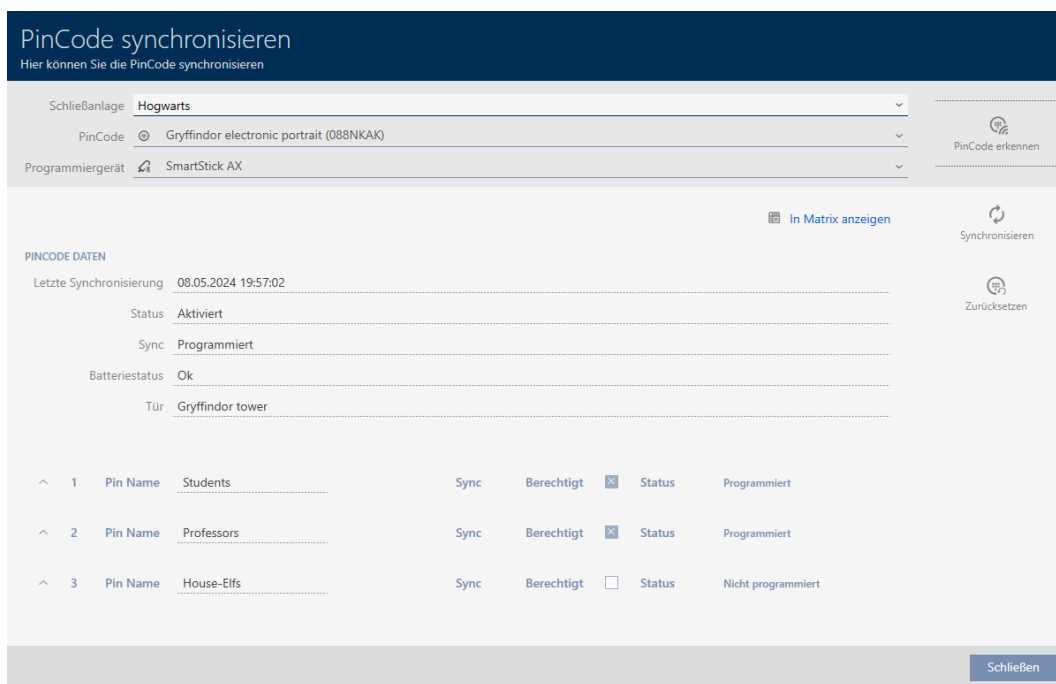
1. Click on the PIN code keypad you wish to reset.  
If the PIN code keypad is not present in your locking system, identify the PIN code keypad (see *Identifying unknown PIN code keypad* [▶ 422] in the AXM manual). Then continue.

↳ The PIN code keypad window will open.

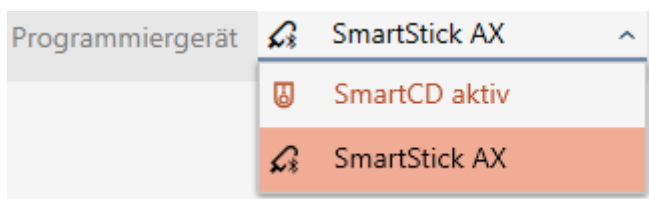


2. Click on the **Synchronisation**  button.

↳ 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**

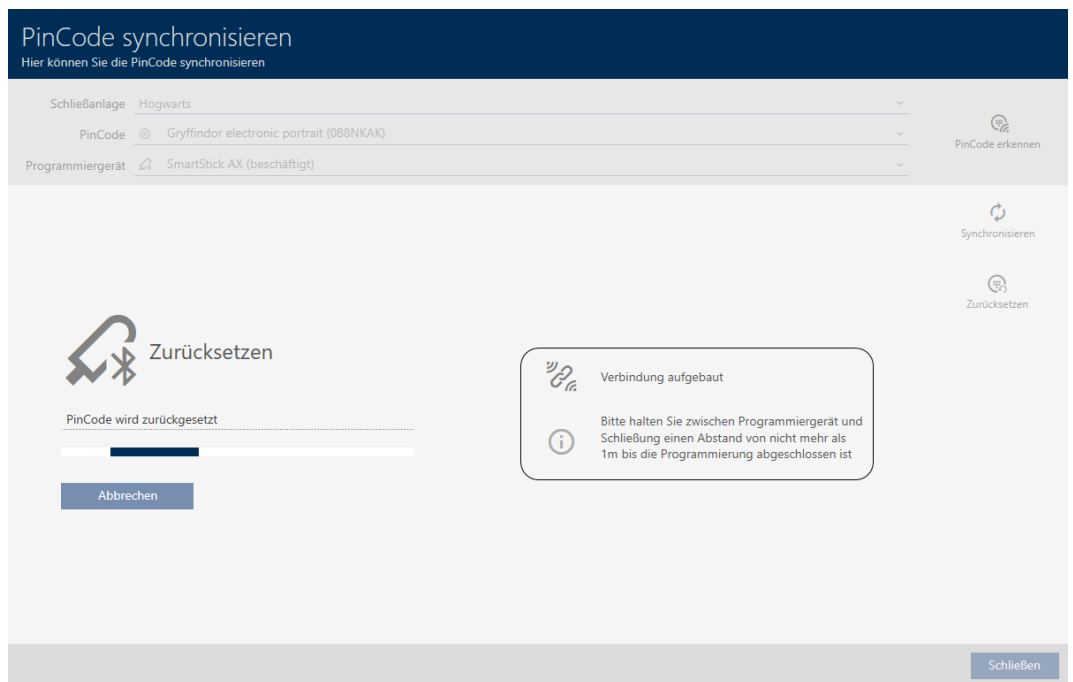
Your AXM Plus can also reset PIN code keypads that were not created in the same project. In this case, however, your AXM Plus does not know the locking system password used.

■ In such instances, enter the locking system password when prompted.

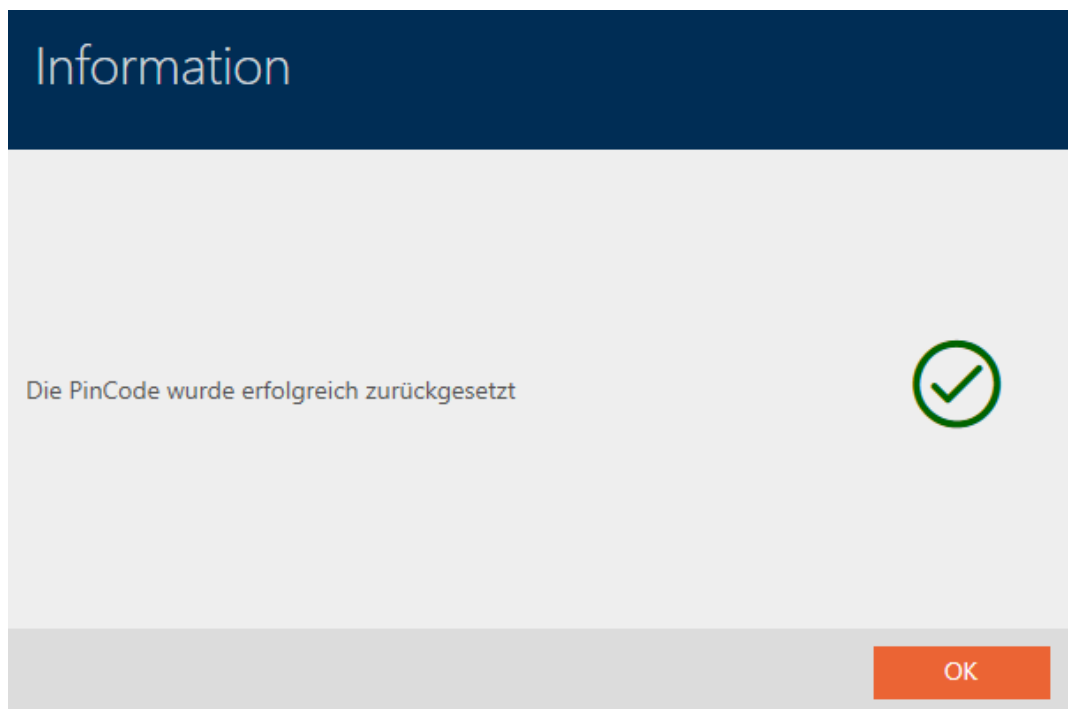
5. If necessary, enter the locking system password for the locking system to which this PIN code keypad belongs.

6. Follow any further instructions as necessary.

↳ PIN code keypad is reset.




↳ PIN code keypad is reset.



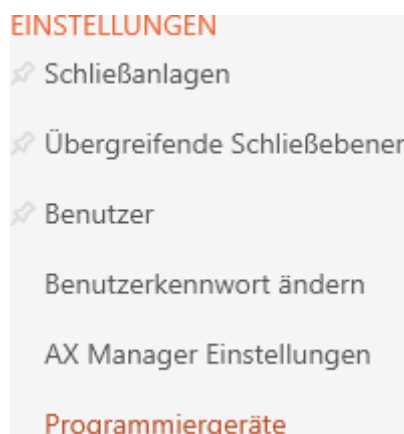
### 18.7 Viewing connected/supported programming devices

This window can be used to check whether a connected programming device is functional and identified.

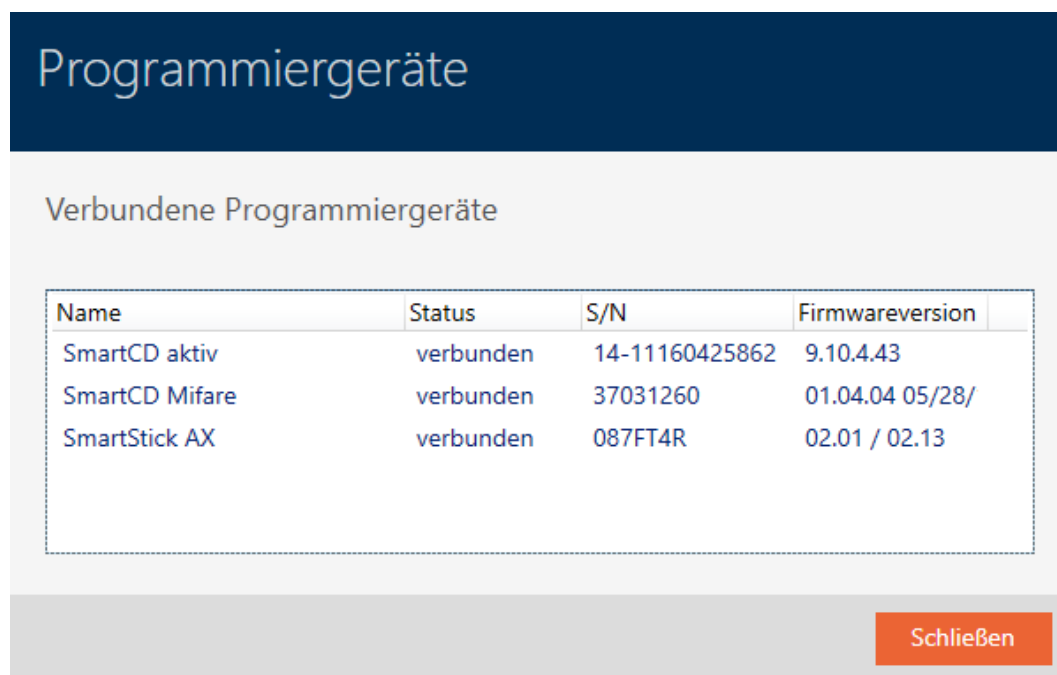
1. Click the orange AXM button .
  - ↳ AXM bar opens.



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). In the status column, you will see if a programming device is connected and recognised by AXM Plus.

## 18.8 Checking the connection between database and cloud

Certain cloud-based functions only work if your AXM Plus's database, the AXM service and the SimonsVoss cloud are connected.

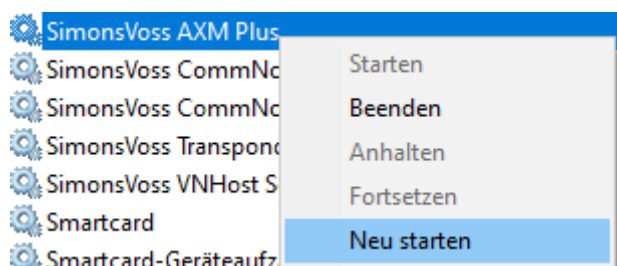
You can easily check this connection in the lower bar of your AXM Plus:



The entry **Cloud State:** indicates either *OK* or *Error*.

In the event of *Error*, you can re-establish the connection by restarting the AXM service and linking your AXM Plus to your SimonsVoss ID again:

- ✓ Administrator rights available.
  - ✓ AXM not opened.
1. Open the Windows window "Services" with administrator rights.
  2. Restart the *SimonsVoss AXM Plus* service.
  3. Right-click on the service to open the context menu and restart the service.



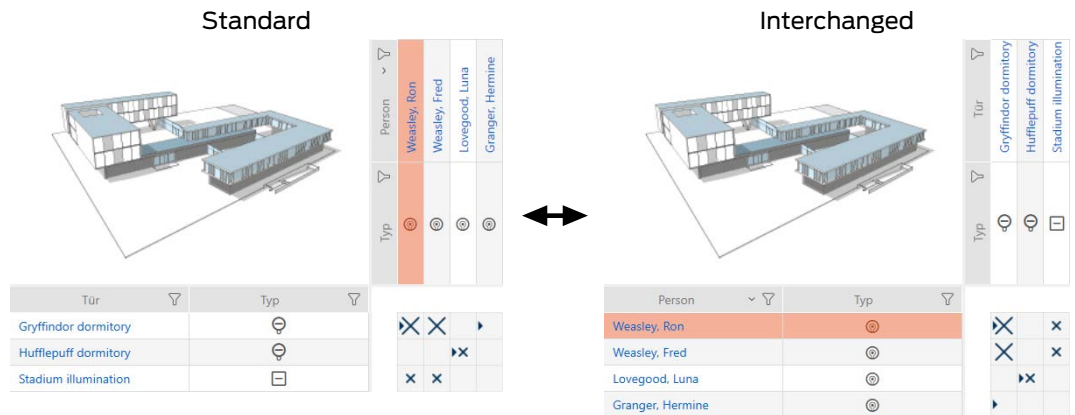
↳ *SimonsVoss AXM Plus* restarts.

4. Launch the AXM Plus and log on to the project.
5. Reconnect your SimonsVoss ID to your AXM Plus again (as described in [Registration \[▶ 29\]](#)).
6. Then check the entry again using **Cloud State:**.



## 19. Your personalised AXM interface

### 19.1 Interchanging (transposing) doors and persons in the matrix

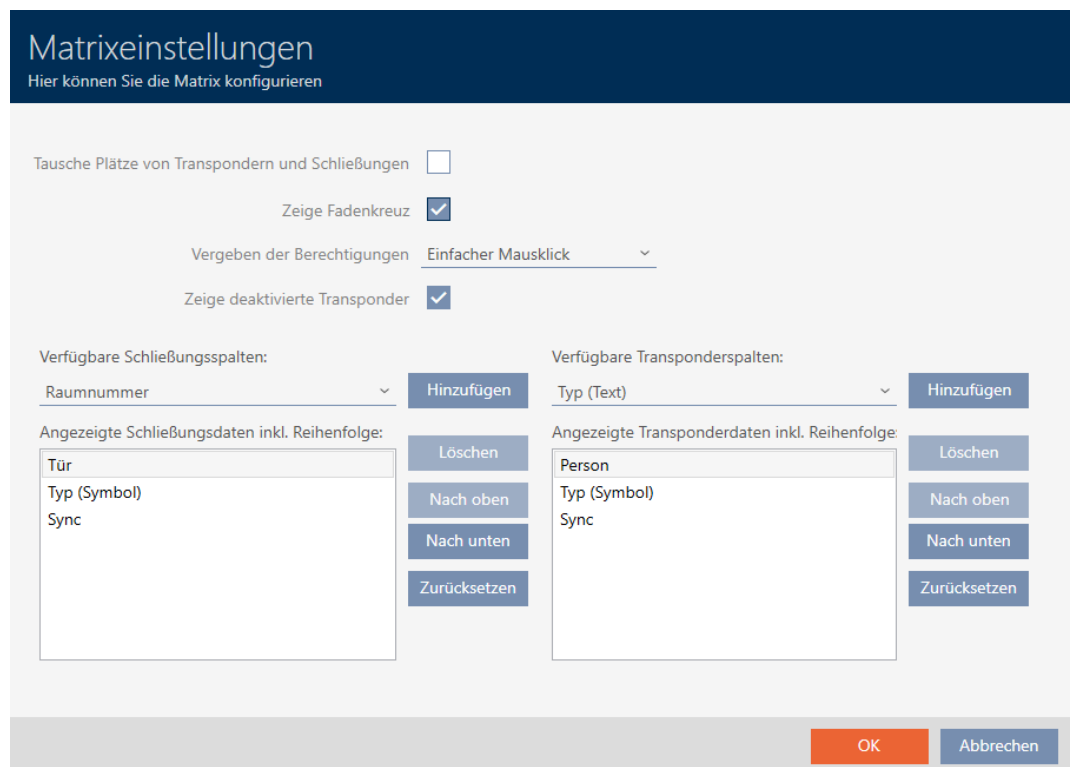


In the standard view, the doors are displayed as rows and the persons as columns. You can also change this.

✓ Matrix screen open.

1. Click on the  Configuration button.

↳ The window with the AXM Plus matrix settings will open.



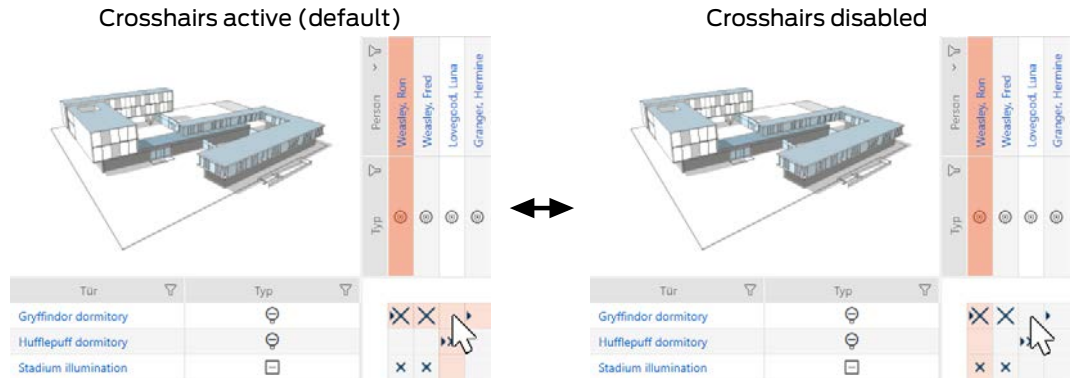
2. Activate the  Swap places for transponders and locks check box.

3. Click on the **OK** button.

↳ The window with the AXM Plus matrix settings closes.

↳ Doors and persons are swapped in the matrix view.

### 19.2 Select columns and rows in the matrix (enable/disable crosshairs)



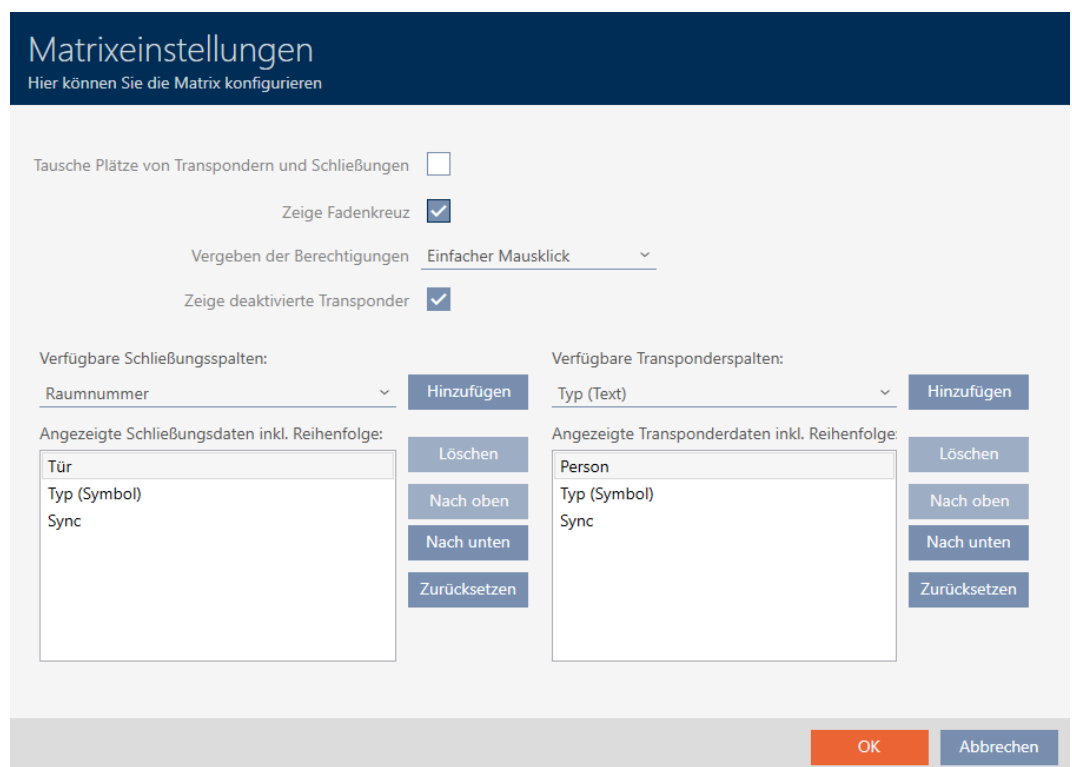
The box over which the mouse pointer is currently positioned belongs to a locking device or to your identification medium. The whole row and the whole column are highlighted in colour in the default setting. This allows you to find the locking device or identification medium you require quickly. This 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.

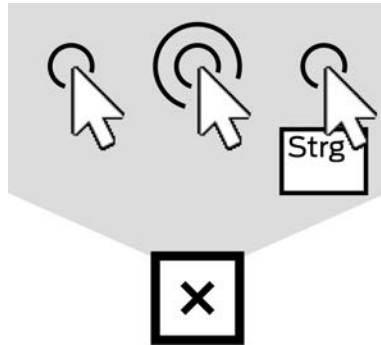
1. Click on the  Configuration button.

↳ The window with the AXM Plus matrix settings will open.




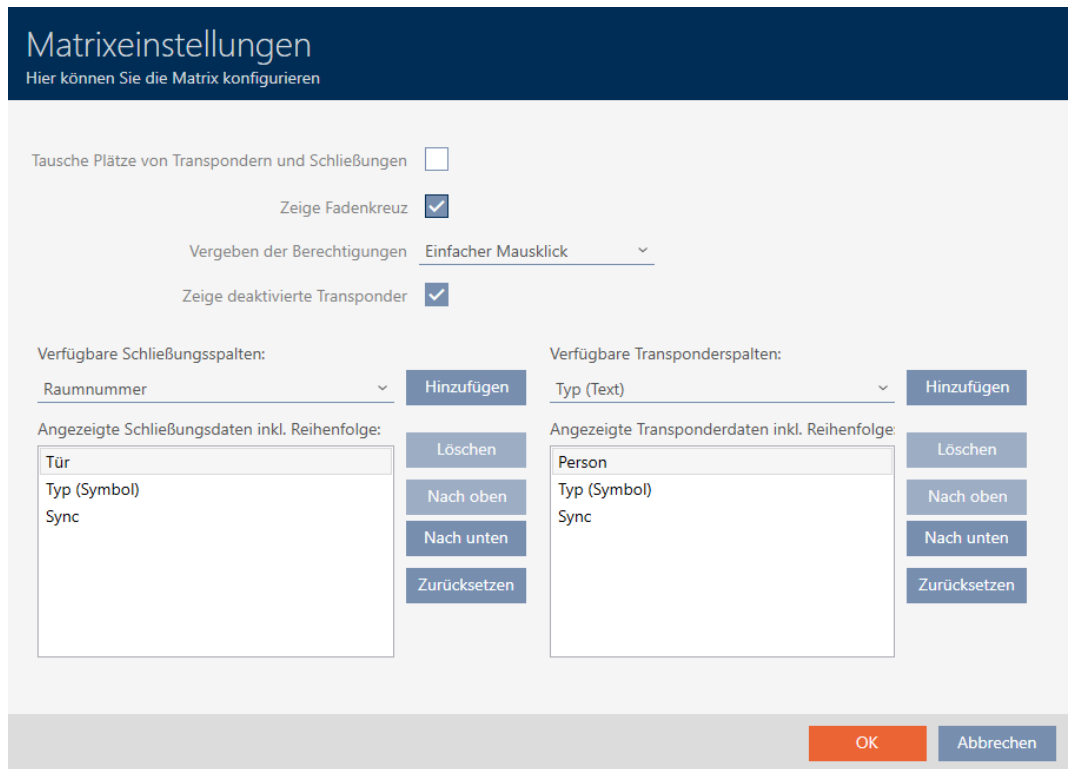
2. Activate or deactivate the  Show crosshair check box.
3. Click on the **OK** button.
  - ↳ The window with the AXM Plus matrix settings closes.
  - ↳ Crosshairs are no longer displayed.

### 19.3 Click to change authorisations

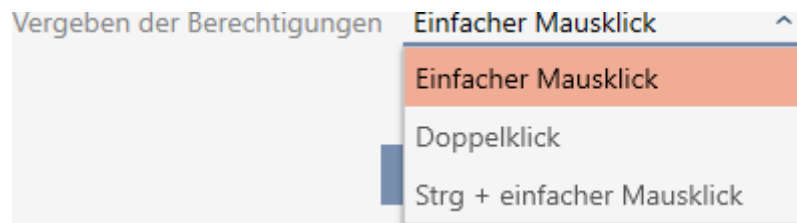


There are three ways to set an individual authorisation by clicking on the matrix:

- 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 Plus matrix settings will open.

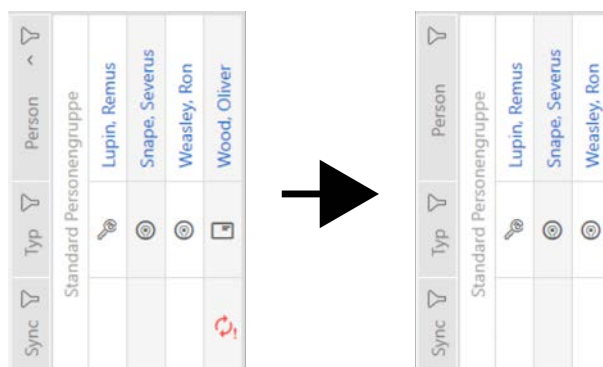



2. Choose between the "Single click of the mouse", "Double click" or "Ctrl + single click" entries from the ▼ Issuing of authorisations drop-down menu.




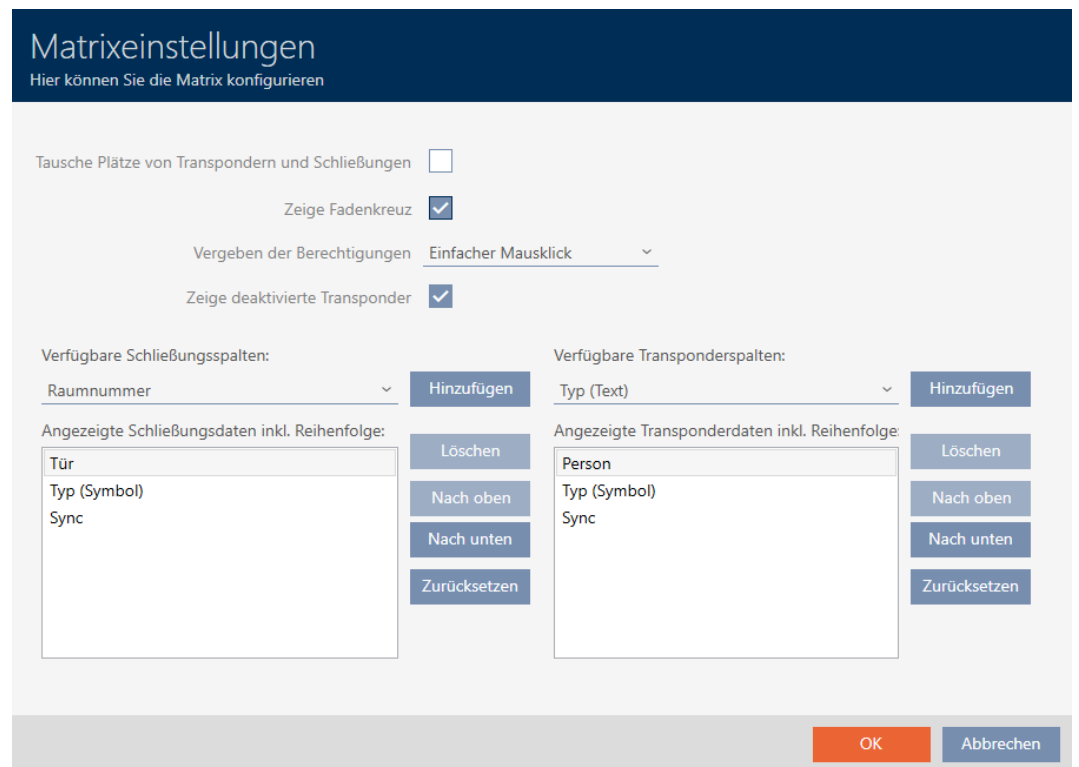
3. Click on the **OK** button.
  - ↳ The window with the AXM Plus matrix settings closes.
  - ↳ Click for authorisations has been changed.

#### 19.4 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.

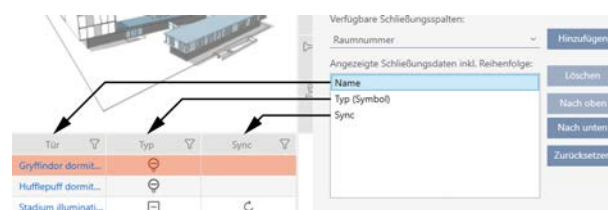
- ✓ Matrix screen open.
- 1. Click on the  Configuration button.
  - ↳ The window with the AXM Plus matrix settings will open.




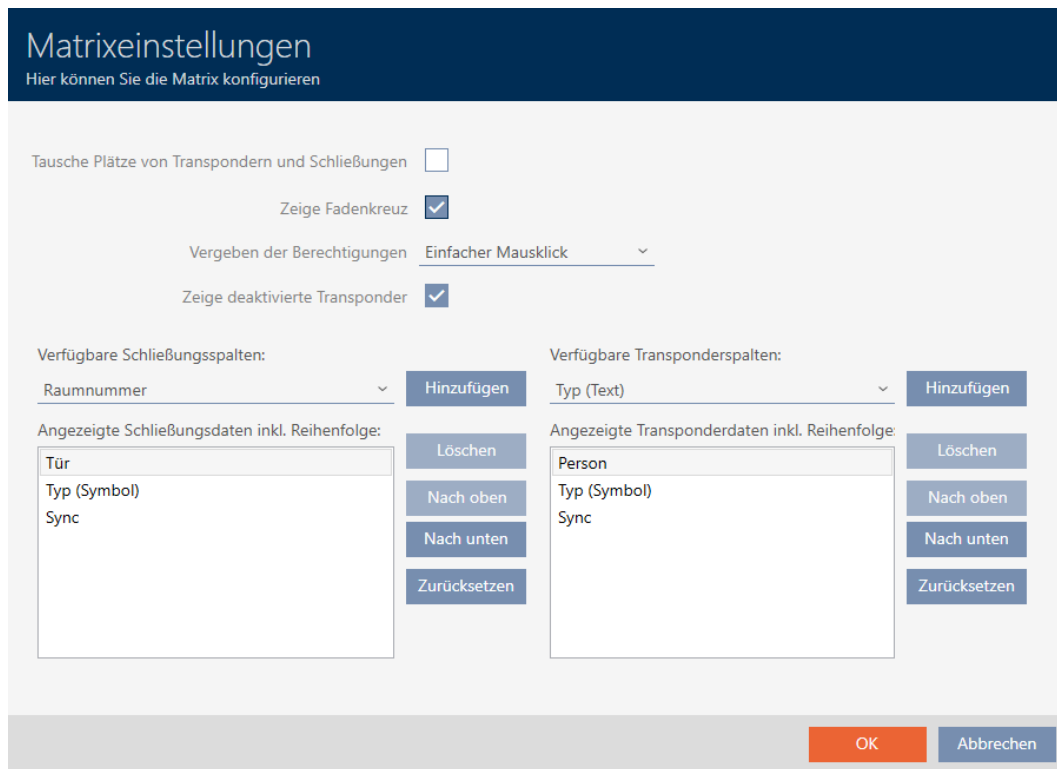
- 2. Disable the  Show deactivated transponders checkbox.
- 3. Click on the **OK** button.
  - ↳ The window with the AXM Plus matrix settings closes.
  - ↳ Deactivated and defective identification media are now hidden.

### 19.5 Showing or hiding rows/columns in the matrix

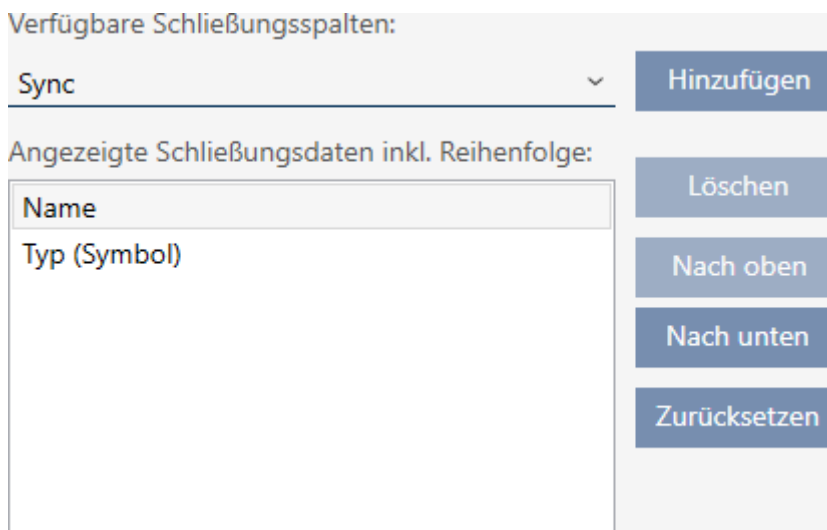
The following description applies to the columns displayed for locking devices. The identification media rows can be edited in the same way.



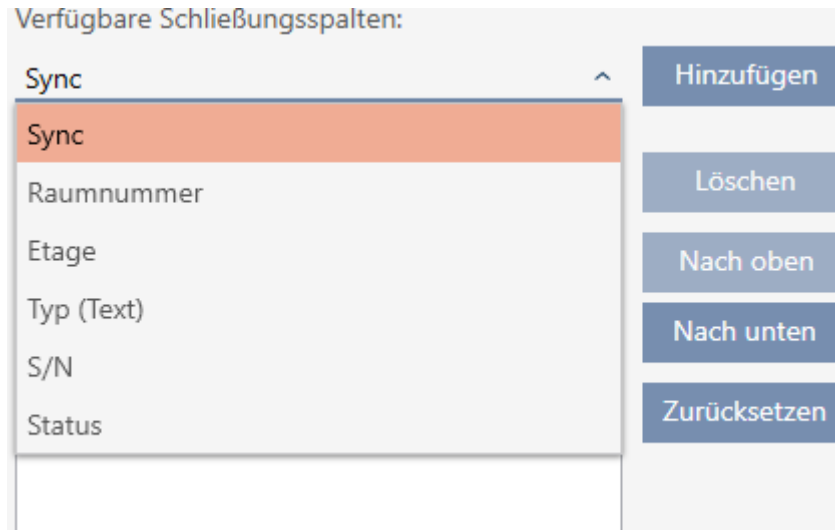
- ✓ Matrix screen open.
- 1. Click on the  Configuration button.
  - ↳ The window with the AXM Plus matrix settings will open.



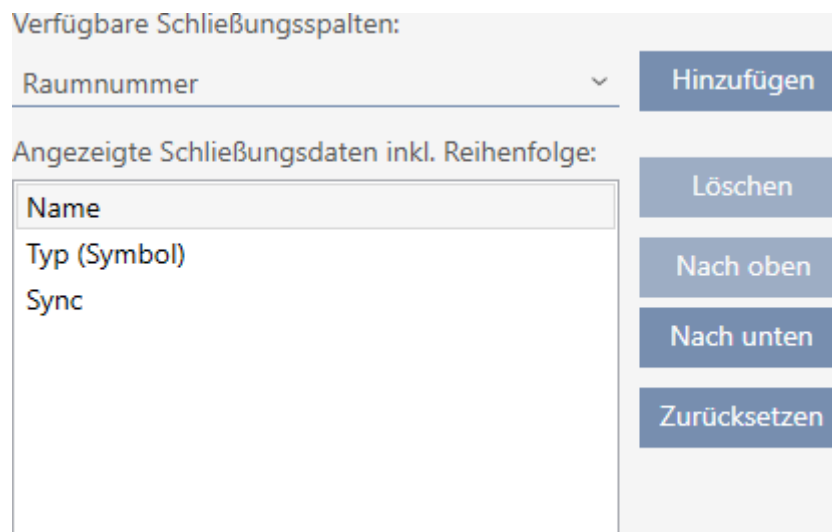
- ↳ The locking device columns currently displayed are listed.



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.



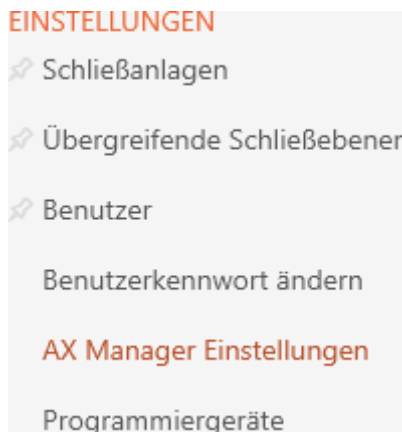
4. Use the Up or Down buttons to change the order.
5. You can also use the Reset button to restore the default display.
6. Click on the OK button.
  - ↳ The window with the AXM Plus matrix settings closes.
  - ↳ Columns are changed as required.

### 19.6 Reading access list/physical access list during synchronisation

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

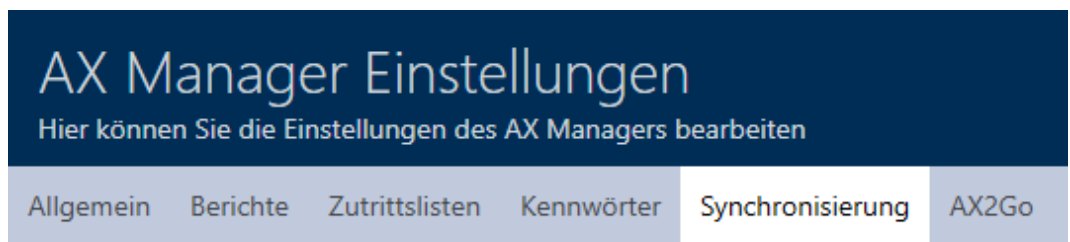


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The window with the AXM Plus settings will open.

3. Go to the [Synchronisation] tab.



SYNCHRONISIERUNGSEINSTELLUNGEN

Lesen der Zutrittsliste während der Synchronisierung einer Schließung

Lesen der Begehungsliste während der Synchronisierung eines Transponders

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 Plus settings closes.

↳ The access list or physical access list will also be imported during synchronisation in the future.

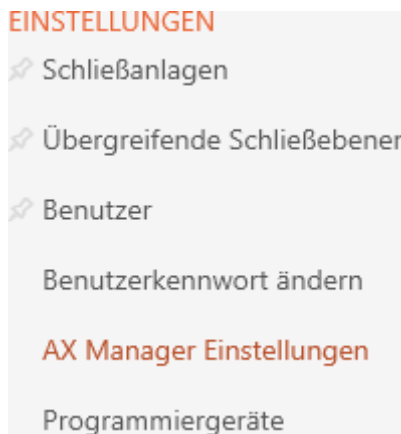


### 19.7 Limiting the number of access list entries in the database

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



2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
  - ↳ The window with the AXM Plus 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).

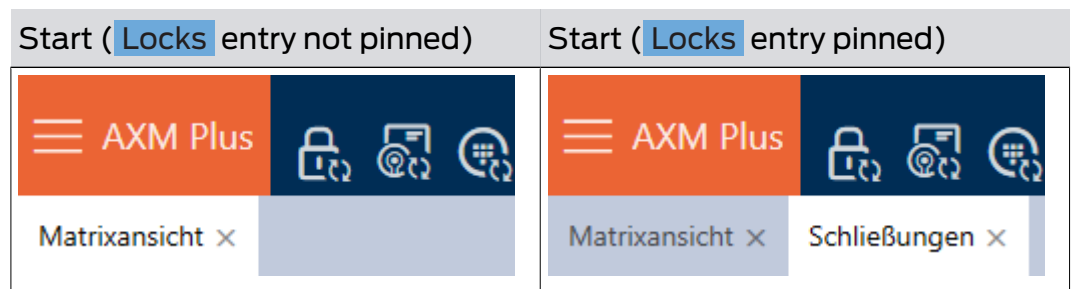
5. Click on the **OK** button.
  - ↳ The window with the AXM Plus settings closes.
  - ↳ Access list restriction is configured.

### 19.8 Pinning tabs

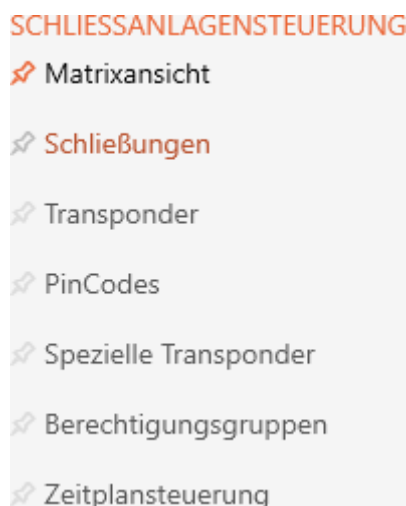
Experience has shown that you need some entries from the AXM bar more frequently.



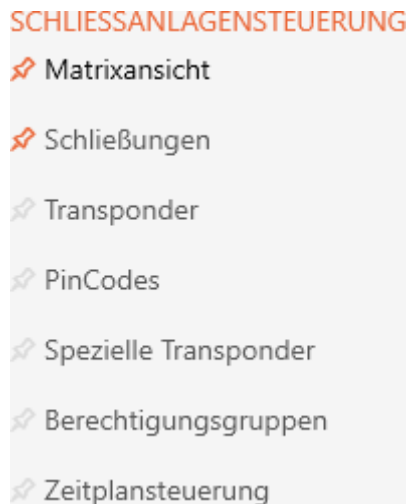
You will see a grey pushpin next to some entries. You can use this pushpin to pin the entry in question and open it automatically the next time you start AXM Plus.



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 Plus is started.

### 19.9 Changing automatic numbering

AXM Plus takes over the numbering of personnel and doors for you by default.

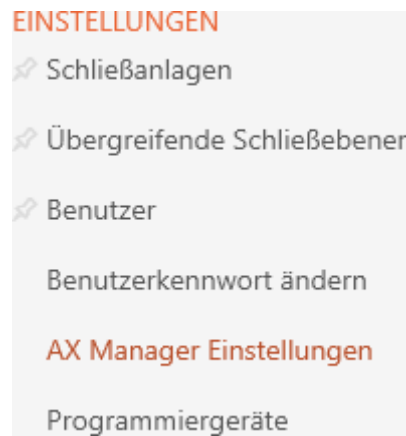
Personnel numbers	Door numbers
<p><b>PERSONENDETAILS</b></p> <p>Nachname <u>Weasley</u></p> <p>Vorname <u>Ron</u></p> <p>Personalnummer <u>PN-1</u></p>	<p><b>TÜRDETAILS</b></p> <p>Name <u>Gryffindor dormitory</u></p> <p>Tür-Code <u>DC-00001</u></p>
PN-1	DC-00001
PN-2	DC-00002
PN-X	DC-XXXXX

The abbreviations *PN-* (personnel number) and *DC-* (door code) can be changed in the AXM Plus properties:

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



2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The window with the AXM Plus settings will open.

3. Go to the [General] tab.

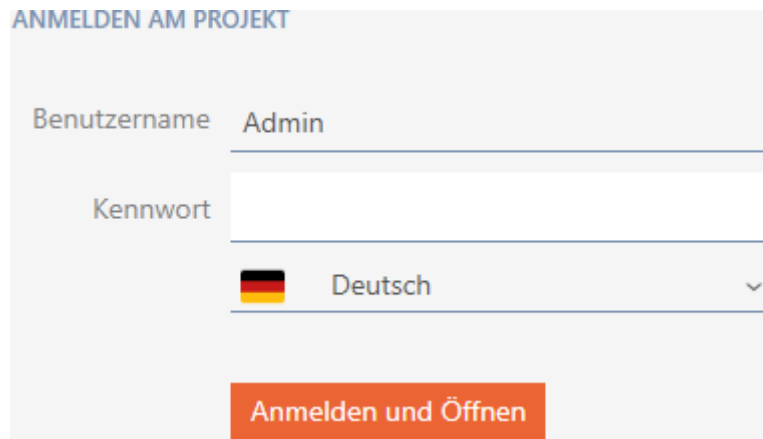


4. Enter the required abbreviations in the *Personnel number* or *Door code* fields.
5. Click on the **OK** button.
  - ↳ The window with the AXM Plus settings closes.
  - ↳ Personnel numbers and door codes will be generated with the modified abbreviation in the future.
  - ↳ Existing personnel numbers or door codes will remain unchanged.

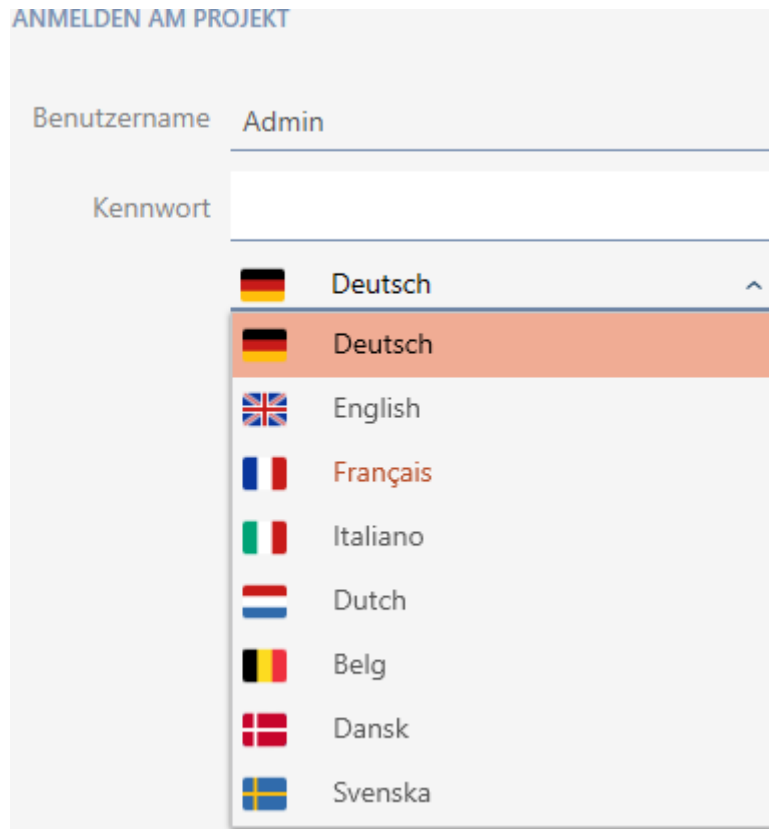
### 19.10 Changing the language

The AXM Plus 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.




### 19.11 Personalising reports and exports

AXM Plus allows you to personalise your reports and exports:

- Logo for header

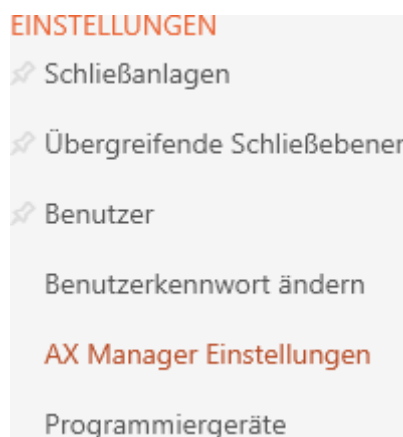
- Permitted formats: .bmp, .jpg, .png
- Automatic scaling (frame format: 25:10.5; also see *Scaling image files* [▶ 551])
- Information for the header
  - Company
  - Street
  - Town/city, postcode
  - Telephone
  - Email
  - Contact
- Logo for footer (frame format: 3:1; also see *Scaling image files* [▶ 551])
  - Permitted formats: .bmp, .jpg, .png

This information is used universally for all reports to ensure a uniform appearance.

1. Click on the orange AXM icon .
  - ↳ 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 "[Reports]" tab.

4. Fill in the fields in the "Address" section.
  - ↳ Uncompleted fields are hidden in the report.
5. Click on the  button in the "Logos" section.
  - ↳ The Explorer window will open.
6. Select a suitable image file for the header or footer.
  - ↳ Explorer window closes.
  - ↳ Selected image files are displayed in the "Logos" section.

LOGOS




7. Click on the  button.
  - ↳ "AX Manager settings" window closes.
- ↳ Reports will now be issued with your own information and logos in the future.



### 19.12 Preventing generated reports from opening automatically

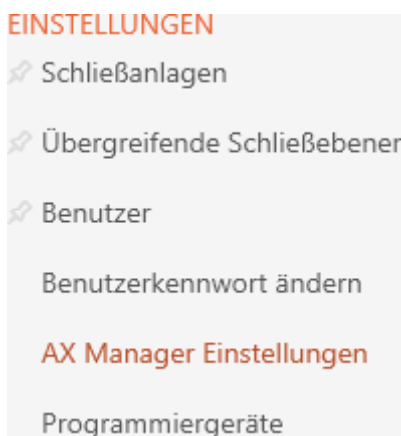
By default, your reports created in AXM Plus open immediately so that you can read them.

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:

1. Click on the orange AXM icon .
  - ↳ 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].

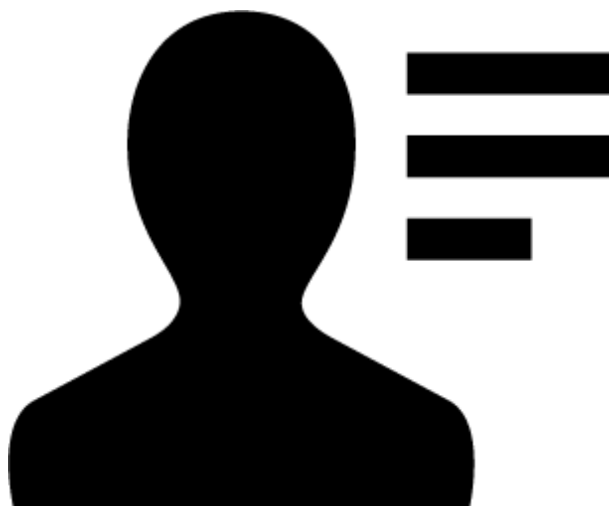
4. Disable the  Open PDF documents after saving checkbox.

5. Click on the **OK** button.

↳ "AX Manager settings" window closes.

↳ In future, reports will now no longer open automatically after saving.

### 19.13 Personalising properties for person details



The default properties that AXM Plus provides for persons and locking devices may not be suitable for your application.

For example, you might like an office number instead of the standard *Title* field.

In this case, AXM Plus gives you the freedom to decide for yourself which properties you want to work with:

- Hide properties you don't need easily. You can unhide the properties again later at any time (see *Hide and show existing fields* [▶ 450]).  
In the example, you hide the default *Title* field.
- Create your own properties (see *Creating your own fields* [▶ 455]).  
In the example, you create an own field called office number.



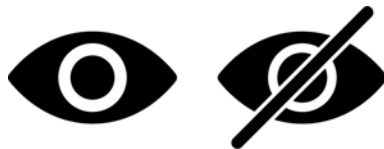
**NOTE**

**Accidental editing of properties set across the project**

Property personalisation applies to all locking systems within the same project. For example, a property that you delete within a locking system is also deleted in all other locking systems.

- Before editing, consider whether you'd also like to edit the properties in all other locking systems.

19.13.1 Hide and show existing fields



AXM Plus contains the following fields by default:

**Person details**

<input checked="" type="checkbox"/> Titel	<input checked="" type="checkbox"/> Eingestellt bis	<input checked="" type="checkbox"/> Abteilung
<input checked="" type="checkbox"/> Adresse	<input checked="" type="checkbox"/> Geburtstag	<input checked="" type="checkbox"/> E-Mail
<input checked="" type="checkbox"/> Ort/Gebäude	<input checked="" type="checkbox"/> Kostenstelle	<input checked="" type="checkbox"/> Telefon
<input checked="" type="checkbox"/> Eingestellt am	<input checked="" type="checkbox"/> Foto	

You can hide the following fields and unhide them again:

- Title
- Address
- Location/Building
- Set on
- Quitting date
- Date of birth

- Cost Centre
- Photo
- Department

The following fields are fixed:

- E-Mail
- Telephone



**NOTE**


**Hiding does not delete content**

If you merely hide a field, the field's content is retained in the database. The content is restored as soon as the field is displayed again.

Fields with content that are hidden will continue to be used for reports. This ensures that absolutely all stored data is exported in the GDPR report (see *Exporting the data protection report (GDPR)* [▶ 507]), for example.

1. Do not use the hide function if you actually want to delete data.
2. Delete the content of the individual field or the entire person or their identification medium instead (see *Deleting a card/transponder* [▶ 108]).

✓ Identification medium available.

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



- Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.

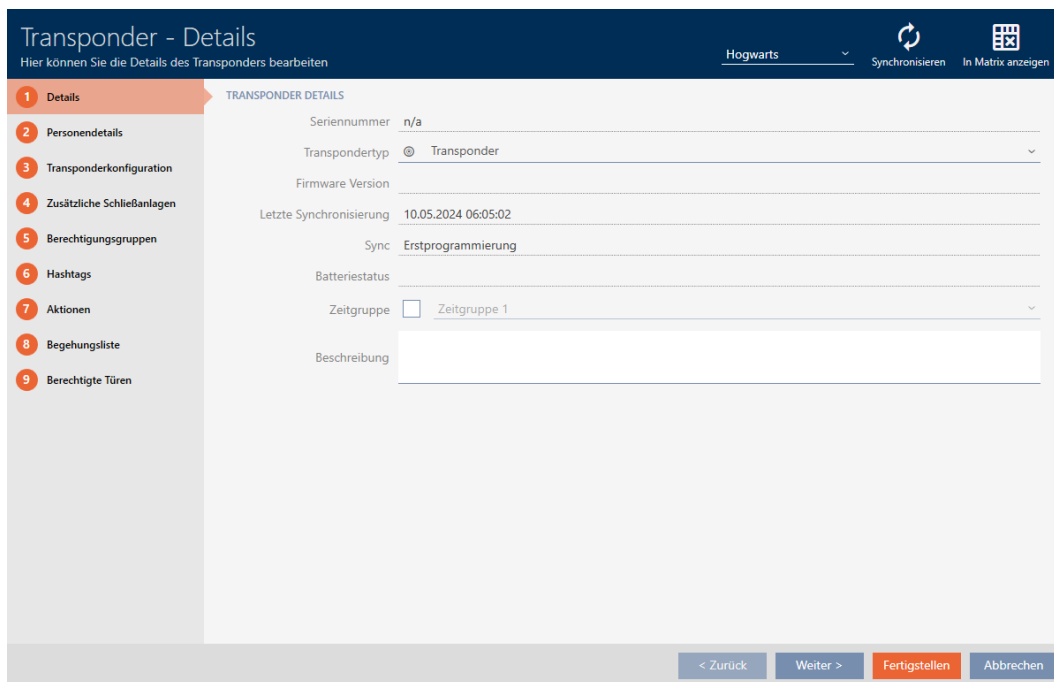
**SCHLISSANLAGENSTEUERUNG**

- Matrixansicht
- Schließungen
- Transponder**
- PinCodes
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung

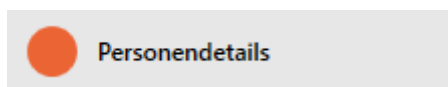
- ↳ The AXM bar will close.
- ↳ The window with identification media opens.

Nach	Vorn:	S/N	Typ	Sync	Status	Zeitg	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L					
Snape	Severus	0301A4D				Zeitgruppe	
> Weasley	Ron	00XTN6K					
Wood	Oliver	UID-148024BA5A7369					

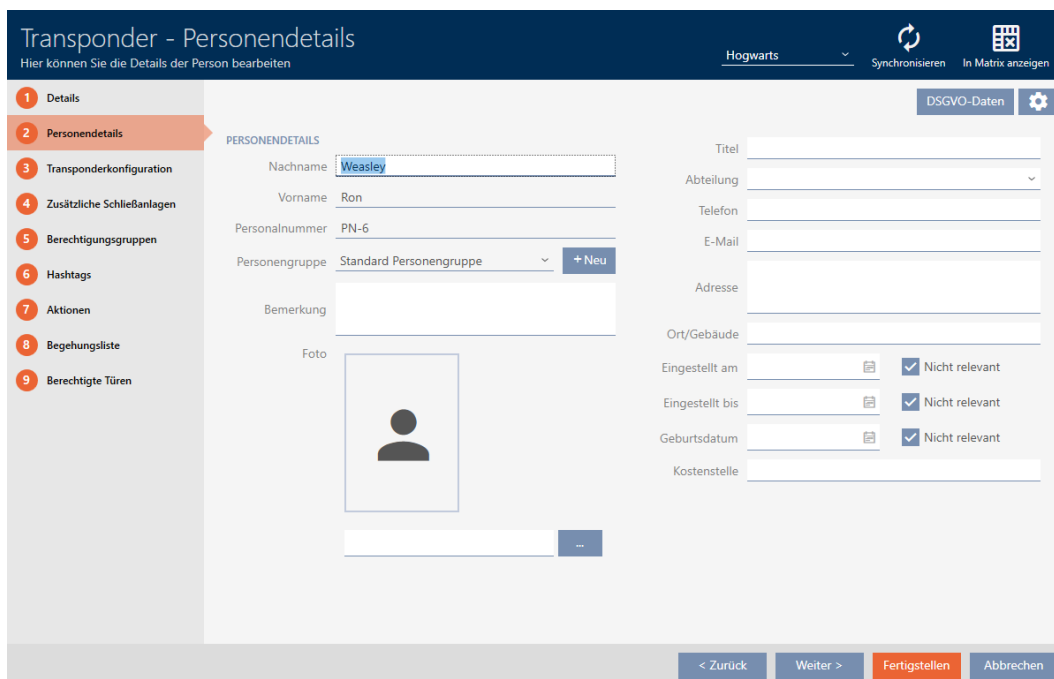
- Click on any non-blocked/deactivated identification medium.
  - ↳ The identification medium window will open.



4. Click on the  Person details tab.



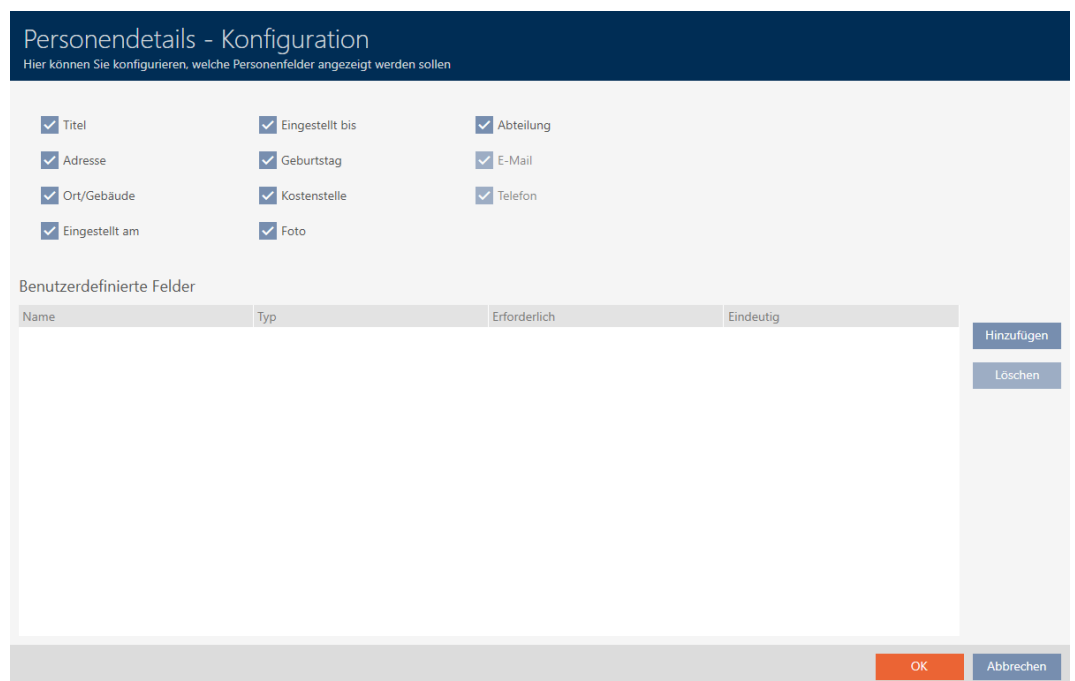
↳ Window switches to the "Person details" tab.



5. Click on the  configuration button.



6. The "Configuration" window will open.



7. Select or deactivate the required fields (example: disable the  Title checkbox).

8. Click on the **OK** button.

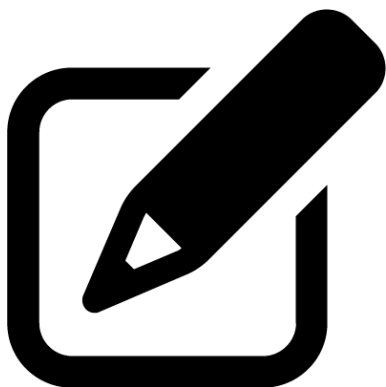
9. "Configuration" window closes.

↳ The identification medium window shows the changed fields in the "Person details" tab (example: the *Title* field is missing).

10. Click on the **Finish** button.

↳ Fields are shown or hidden in all locking systems in the same project.

### 19.13.2 Creating your own fields




Benutzerdefinierte Felder			
Name	Typ	Erforderlich	Eindeutig
<input type="button" value="Hinzufügen"/>			
<input type="button" value="Löschen"/>			

In some cases, you may need different or additional fields to those provided by your AXM Plus. Additional fields for person properties are also exported in the GDPR report (see *Exporting the data protection report (GDPR)* [▶ 507]).

For this reason, you can also create your own fields (see *Subsequently modified user-defined fields* [▶ 461] for more information on the properties of your own fields):








✓ Identification medium available.

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









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

**SCHLISSANLAGENSTEUERUNG**

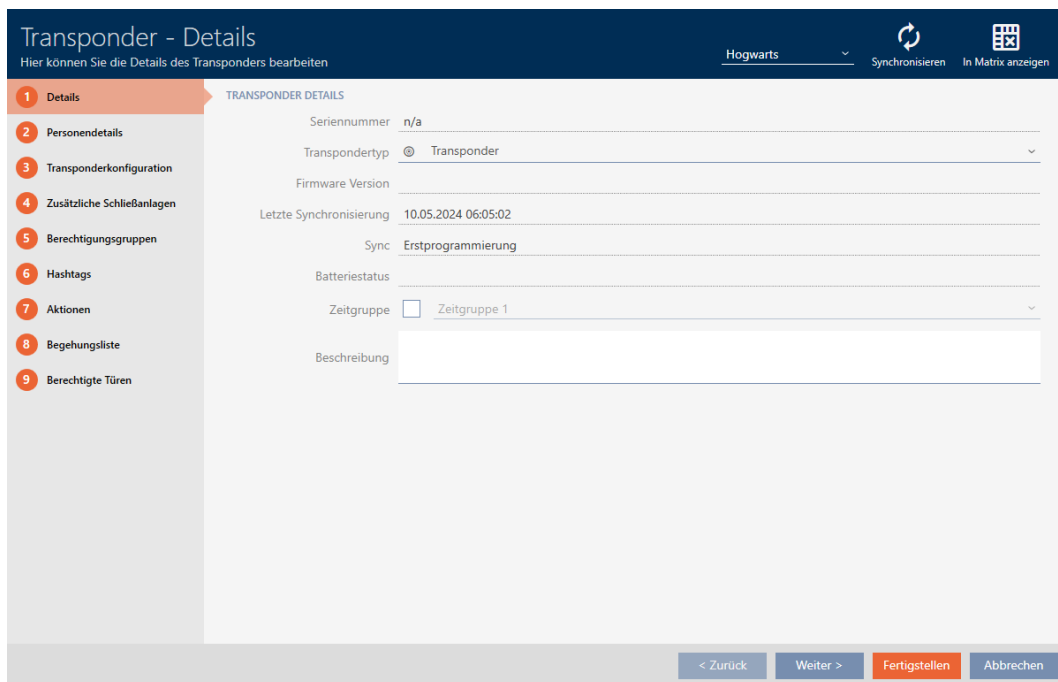
-  Matrixansicht
-  Schließungen
-  **Transponder**
-  PinCodes
-  Spezielle Transponder
-  Berechtigungsgruppen
-  Zeitplansteuerung

- ↳ The AXM bar will close.
- ↳ The window with identification media opens.

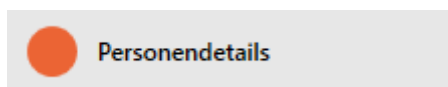
Nach	Vorn	S/N	Typ	Sync	Status	Zeitg	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L					
Snape	Severus	0301A4D				Zeitgrupp	
> Weasley	Ron	00XTN6K					
Wood	Oliver	UID-148024BA5A7369					

3. Click on any identification medium.
  - ↳ The identification medium window will open.

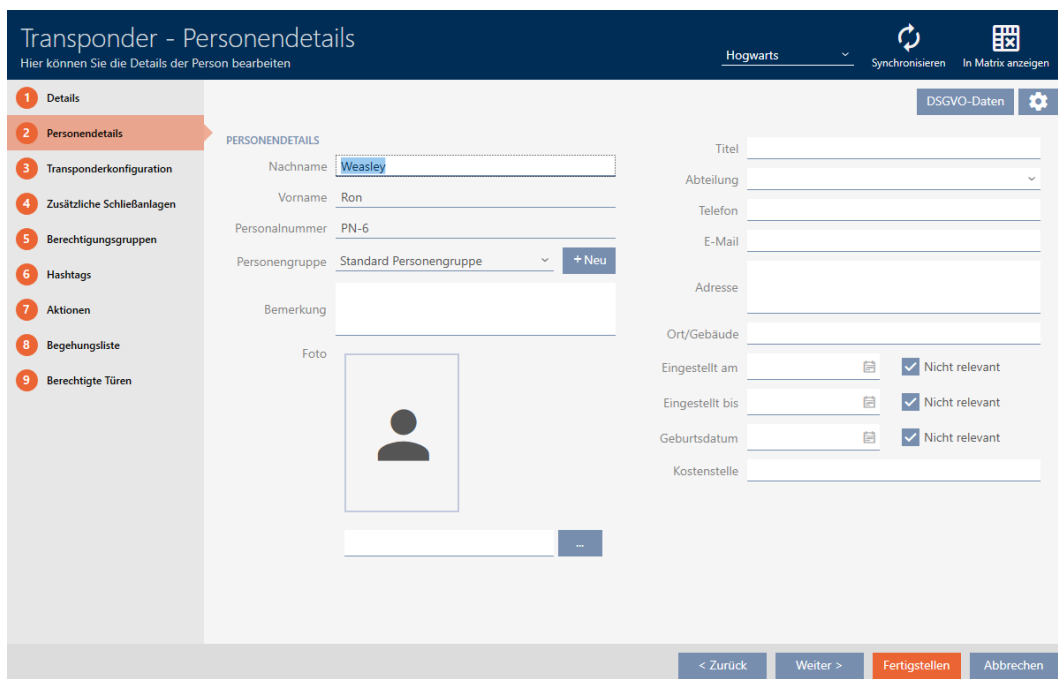




4. Click on the  Person details tab.



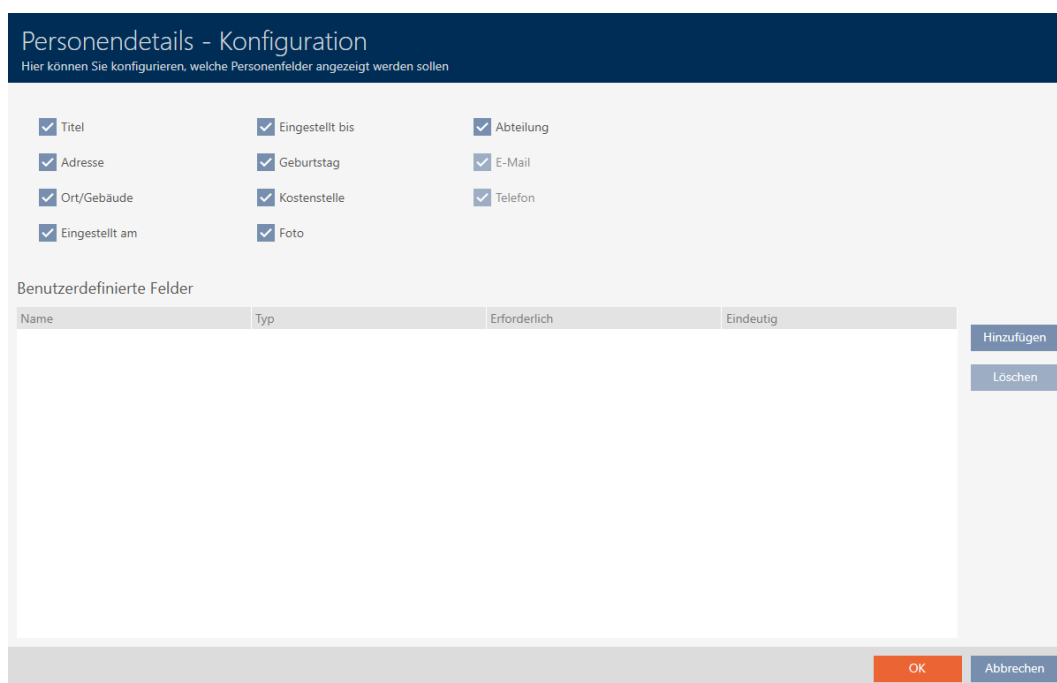
↳ Window switches to the "Person details" tab.



5. Click on the  configuration button.

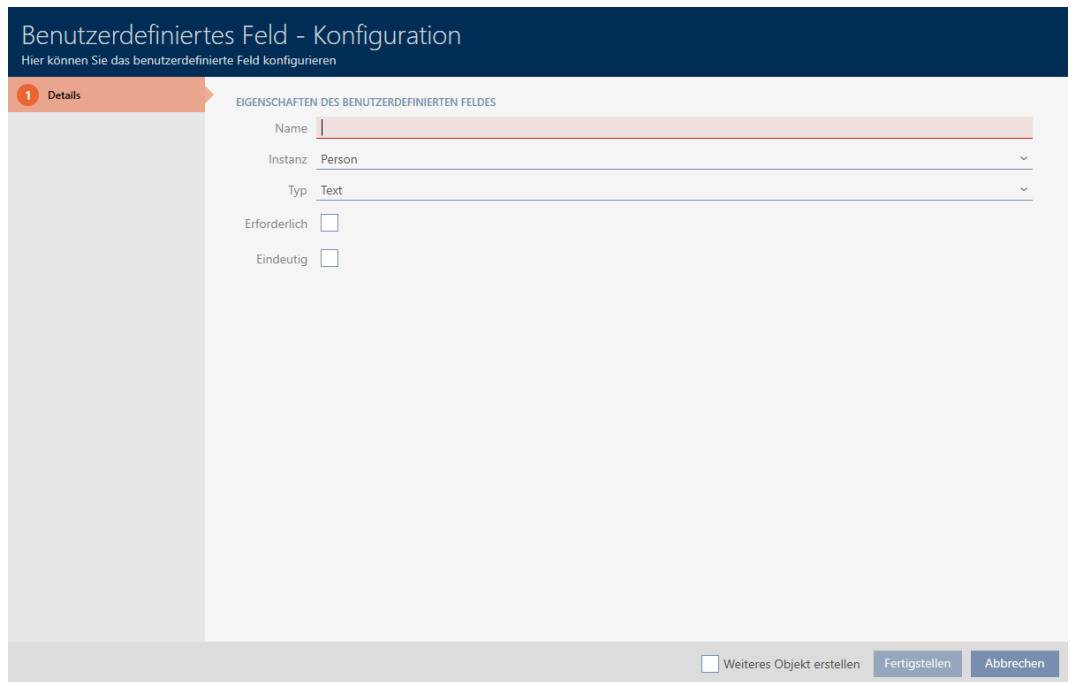


6. The "Configuration" window will open.



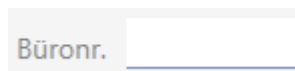
7. Click on the **Add** button.

↳ The "Configuration" window will open.



8. Enter the name of your user-defined field in the *Name* field (example: *office no.*).

↳ This name will be displayed in front of the input field later.



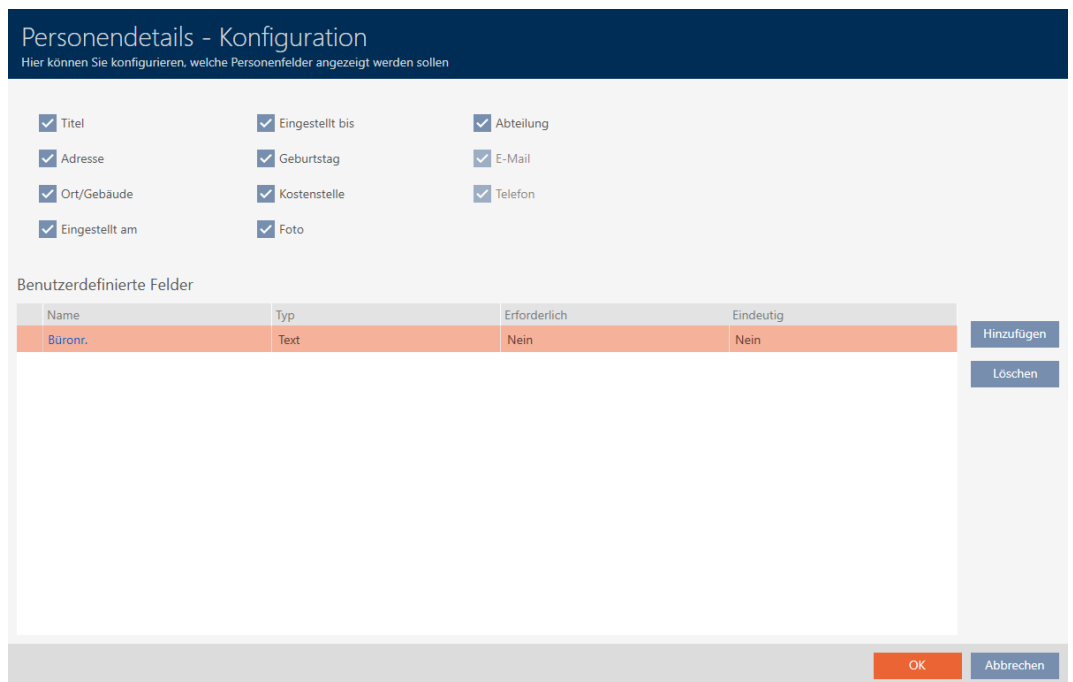
9. If an entry in your field needs to be mandatory: activate the  Required check box (example: office no. is not mandatory – not every employee has an office with a number).

10. If an entry in your field must not be reused for the same field for another person: activate the  Unique check box (example: office no. is not clear – a number of employees work in the same office – therefore do not activate the check box).

11. Click on the **Finish** button.

↳ "Configuration" window closes.

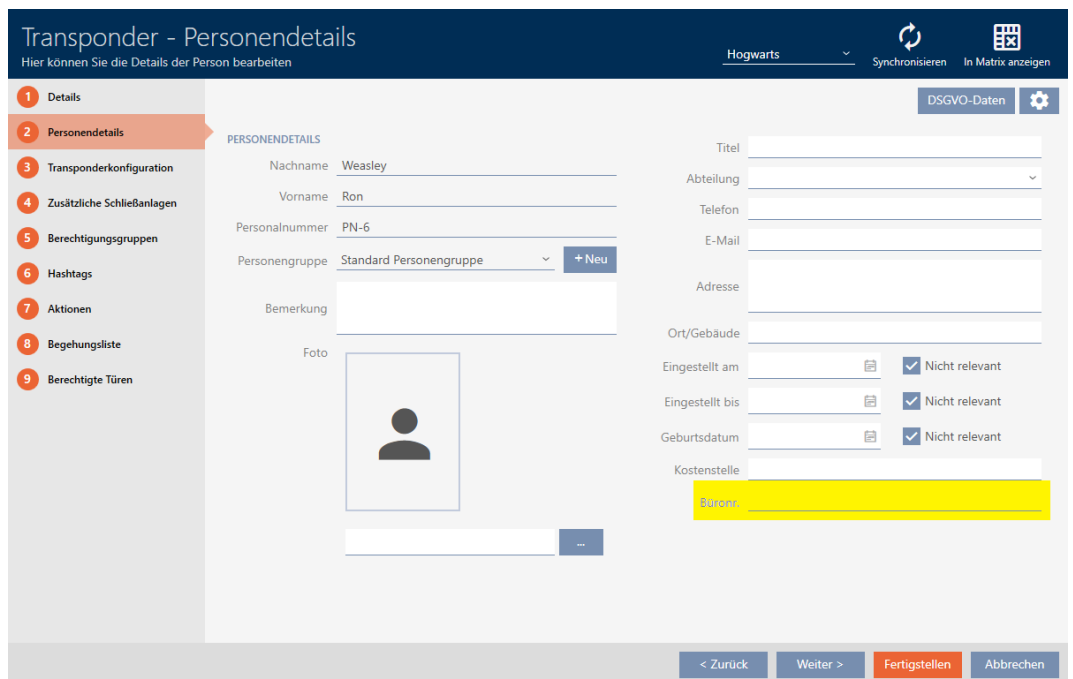
↳ Your new user-defined field is now listed.



12. Click on the **OK** button.

13. "Configuration" window closes.

- ↳ The identification medium window displays your new user-defined field in the "Person details" tab (example: The *office no.* field is displayed).



14. Click on the **Finish** button.

- ↳ Your new user-defined field is available in all locking systems belonging to the same project.

**NOTE****AXM Plus's behaviour with user-defined fields created or modified at a later date**

User-defined fields can be created at any time and changed at a later date. Example: you create a required field even though some people already exist in the locking system.

This results in this newly created required field being empty for existing persons, even though it is marked as  Required.

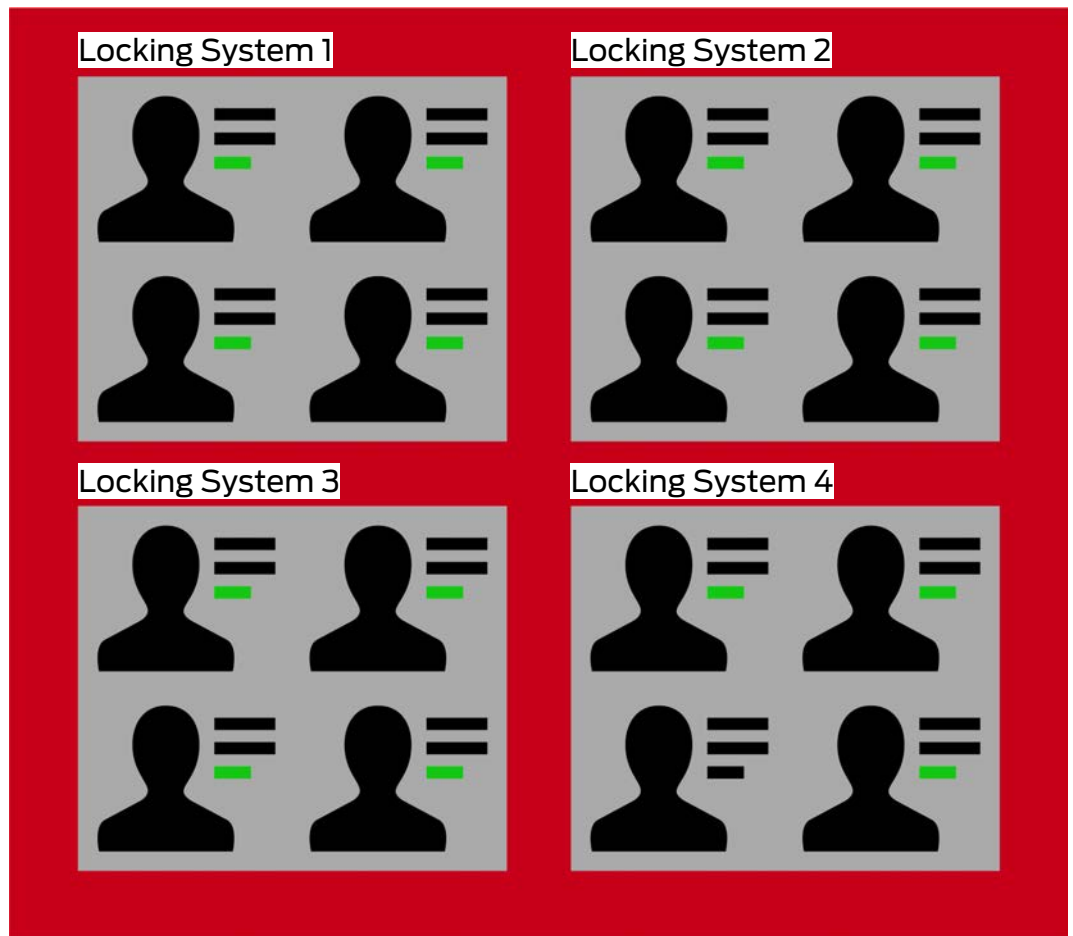
- Find out how AXM Plus responds in such cases (see *Subsequently modified user-defined fields* [[▶ 461](#)]).

#### 19.13.2.1 Subsequently modified user-defined fields

Your AXM Plus allows you to create custom fields at any time (see *Creating your own fields* [[▶ 455](#)]).

User-defined fields always apply throughout the entire project – i.e. they apply to all properties concerned in all locking systems of a project. In the diagram shown as an example, the green user-defined field has been newly created and applies to all persons concerned.

## Project





Example: You create a custom field for "Person details". In the future, this field will thus be available:

- For all persons
- In all locking systems
- Within your project.


User-defined fields can have two important properties:  Required and  Unique.

The following examples and explanations deals with user-defined properties for persons.

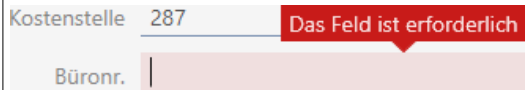
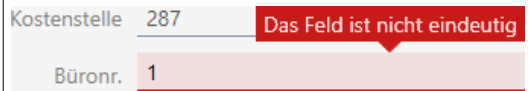
User-defined properties for new persons

Required	Unique
<p>If a field marked as required yet not completed is displayed, the <b>Finish</b> button is greyed out.</p> <p>You can only complete the input once you have completed the field.</p> <p>Required fields that are not entered are highlighted in red. In the example, office no. has been marked as <input checked="" type="checkbox"/> Required:</p> 	<p>If a field is shown as uniquely marked, the AXM Plus will first accept each entry. However, as soon as the entries are saved with the <b>Finish</b> button, AXM Plus checks whether the same entry already exists in the same field for another object. If this is the case, the <b>Finish</b> button is greyed out.</p> <p>You can only complete the entry after you have entered no value or a unique value. In the example, office no. has been marked as <input checked="" type="checkbox"/> Unique:</p> 

New user-defined properties for existing persons

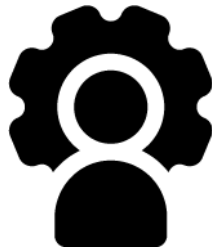
Required	Unique
<p>Persons who have already been created do not have an office number yet. As soon as you open such a person, the newly available field is highlighted in red:</p>  <p>You can only complete the input once you have completed the field.</p> <p>Empty values are therefore possible for newly created required fields.</p>	<p>No problem. A field that is newly created cannot be filled with duplicate values. All newly entered values are checked before saving.</p>

Modified user-defined properties for existing persons

Required	Unique
<p>Fields which become required at a later point in time are treated as newly created required fields:</p> <p>Persons who have already been created do not have an office number yet. As soon as you open such a person, the newly available field is highlighted in red:</p>  <p>You can only complete the input once you have completed the field. Empty values are therefore possible for fields which become required at a later point in time.</p>	<p>Fields that are made unique at a later point in time are treated as newly created unique fields:</p> <p>Persons who have already been created can have the same entry several times in the same field – a unique input was not required before now. As soon as you open a person and click on the <b>Finish</b> button, AXM Plus checks whether all unique fields are completed with unique values. If they are not, the fields concerned are highlighted in red:</p>  <p>You can only complete the entry after you have entered no value or a unique value.</p>



## 20. Administrative tasks

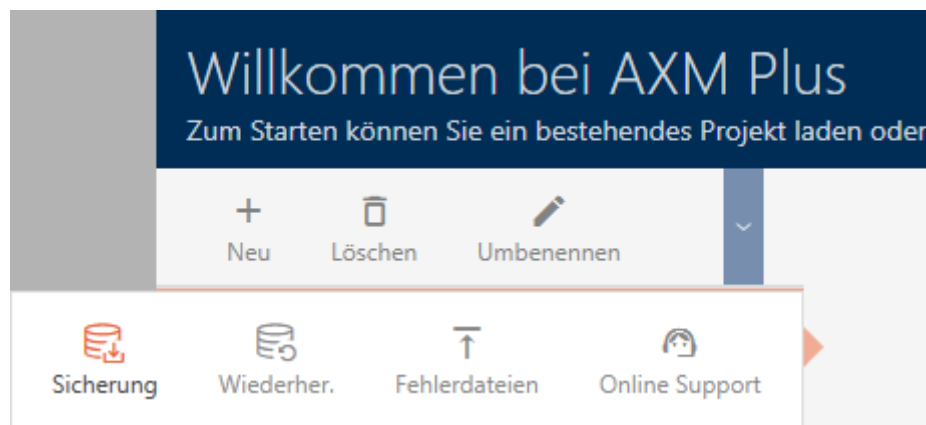


### 20.1 Creating a backup

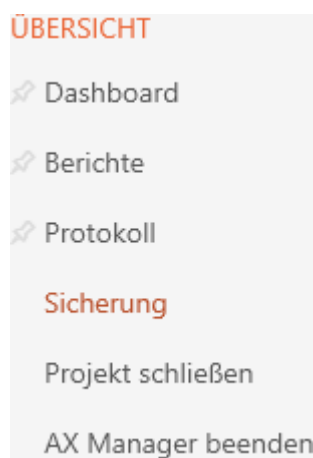
Your database and thus your workload can be quickly restored if a backup is copied on a regular basis.

You can easily create the backup in AXM Plus itself:


On the login screen ( **Project backup** button  ):



Alternatively: in the expandable AXM bar ( **Project backup** button ):

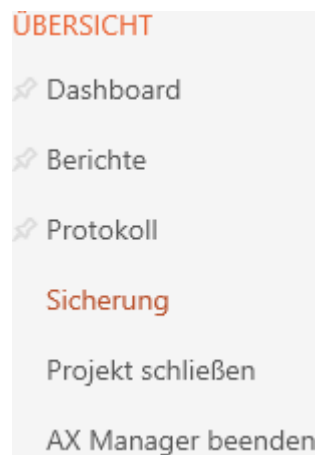


This section explains how to back up the database using the expandable AXM bar.

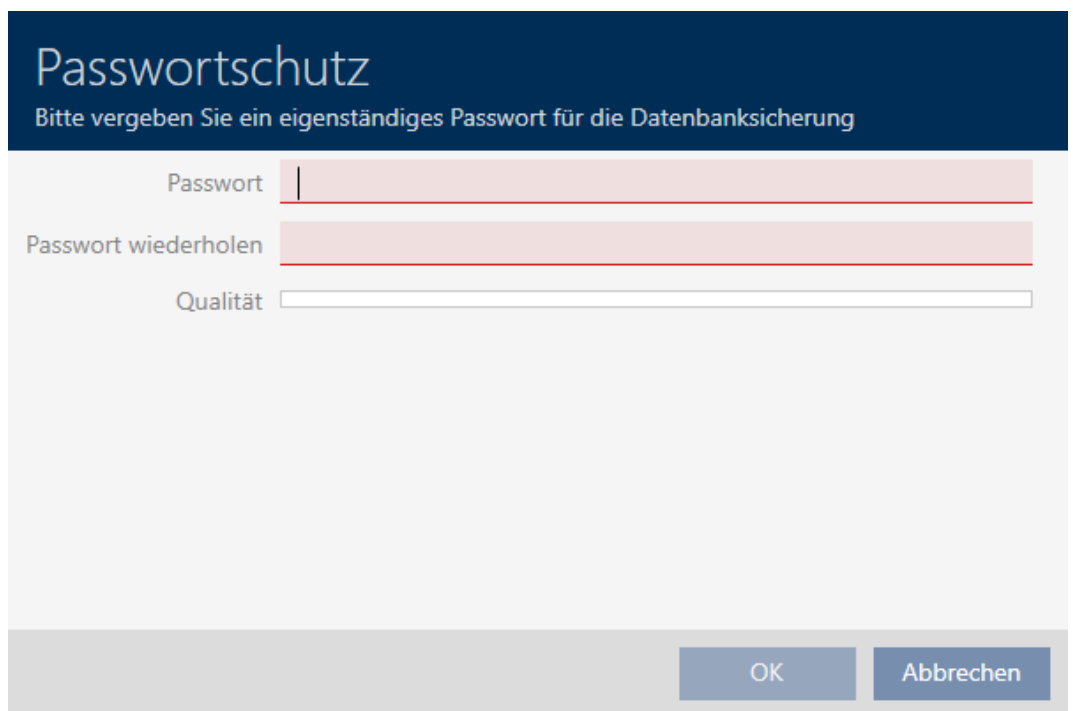
1. Click on the orange AXM icon .
  - ↳ AXM bar opens.



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.

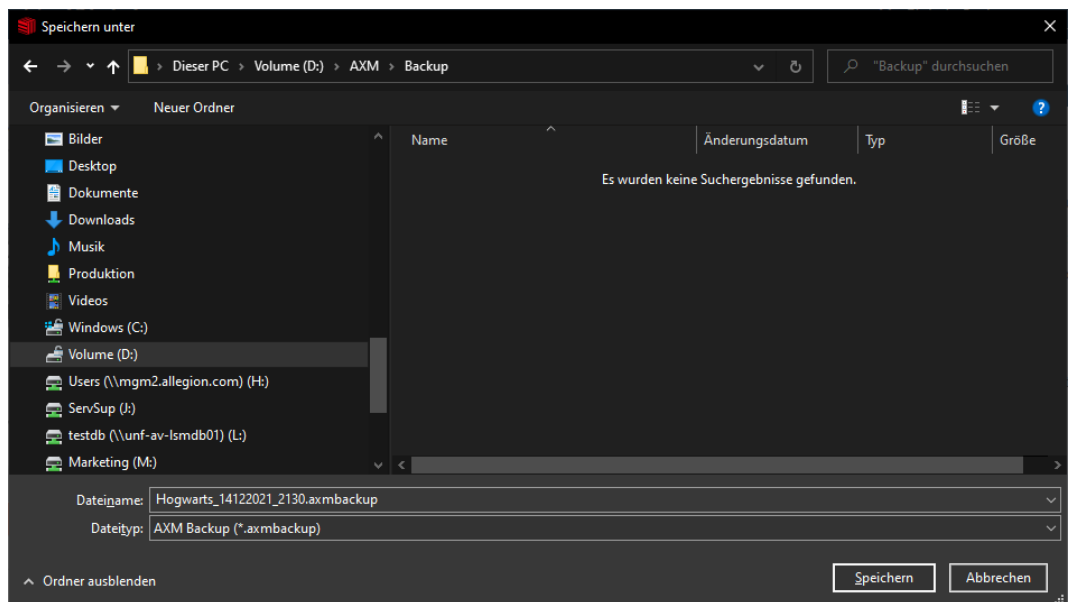
- ↳ A coloured bar shows you how secure your password is.

Quality 

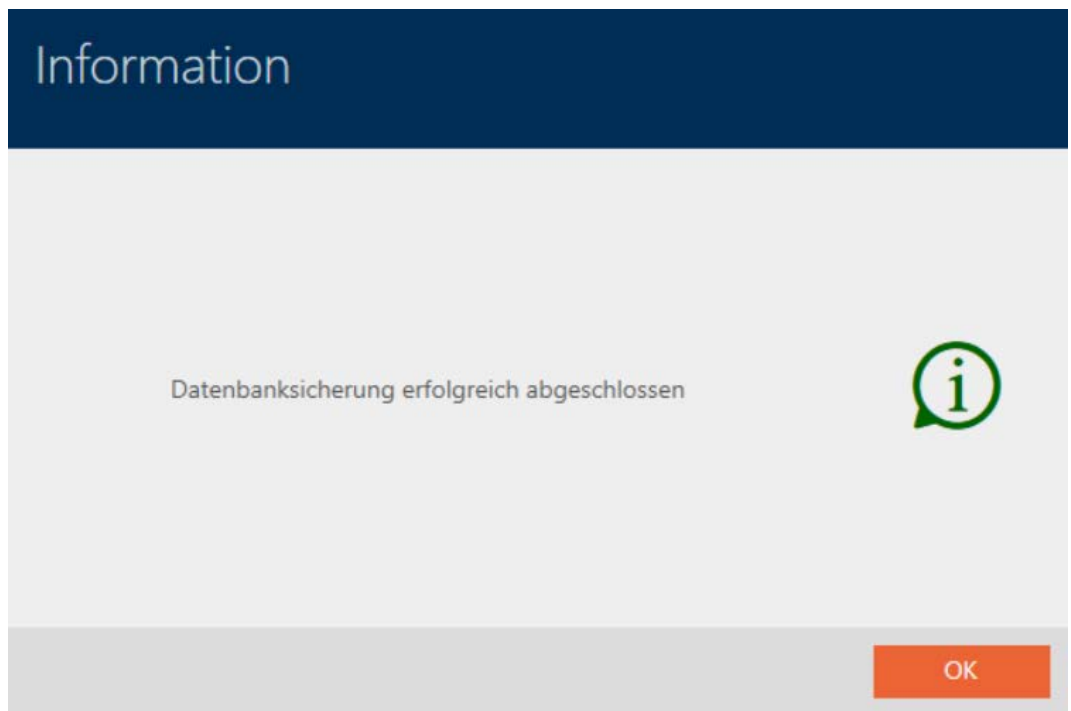
4. Repeat the entered password in the *Repeat password* field.
5. Click on the **OK** button.
  - ↳ The window for assigning passwords closes.
  - ↳ Backup is being created.



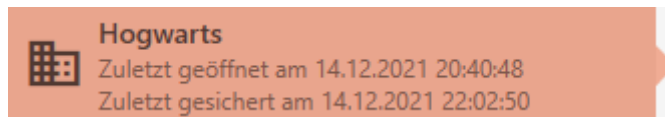
- ↳ The Explorer window will open.
6. Save the backup file (extension: .axmbackup) in a file directory of your choice.



- ↳ Explorer window closes.
- ↳ Backup is complete.



You can also see when you last created a backup on the AXM Plus login screen:



## 20.2 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* [▶ 398]).

- ✓ Backup available (see *Creating a backup* [▶ 465]).
1. Click on the **Restore**  button on the login screen.
    - ↳ The Explorer window will open.
  2. Go to your backup.
    - ↳ Explorer window closes.
    - ↳ Password prompt window will open.



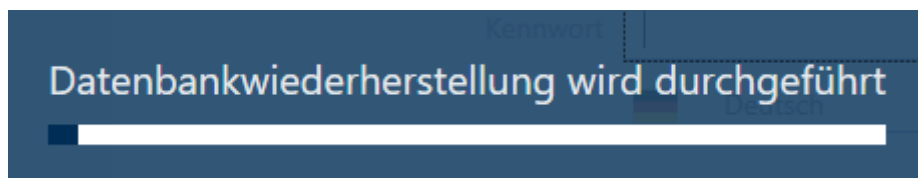
Passwortschutz

Bitte geben Sie zur Wiederherstellung das Sicherungspasswort ein (nicht das Anmelden-Kennwort!)

Passwort






OK Abbrechen


3. Enter the password you entered while creating the backup in the *Password* field.
4. Click on the **OK** button.
  - ↳ Password prompt window closes.
  - ↳ The database is restored.




### 20.3 Exporting error logs

Error logs help to resolve support cases more quickly and pinpoint any problems more quickly.

-  AXMLog-Plus-20240516.log
-  AXMLog-Plus-20240517.log
-  AXMLog-Plus-20240527.log
-  AXMLog-Plus-20240528.log
-  AXMLog-Plus-20240529.log

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:

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




2. Select the **Download error files** entry in the | INFO & HELP | group.



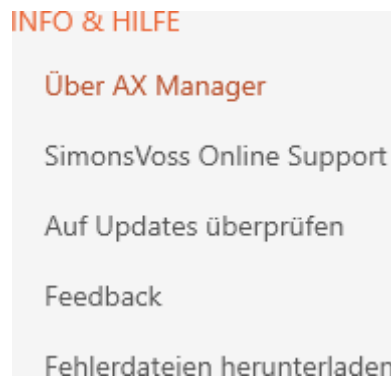
- ↳ The Explorer window will open.
3. Save the error log (file extension: .zip) to a file directory of your choice.  
 ↳ The error log is now exported.

## 20.4 Displaying version number and licence key for the AXM installed

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



2. Select the **About AX Manager** entry in the | INFO & HELP | group.



- ↳ The info window about AXM Plus will open.



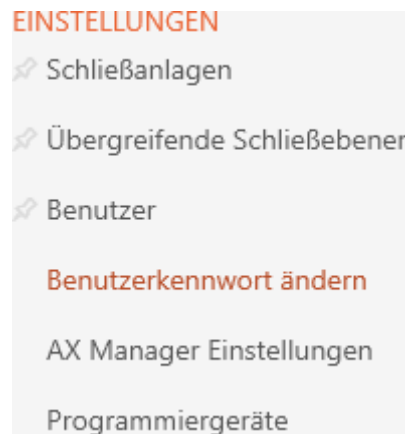
3. Click on the **Licence details** button.
  - ↳ The info window about AXM Plus closes.
  - ↳ The licence info window will open.



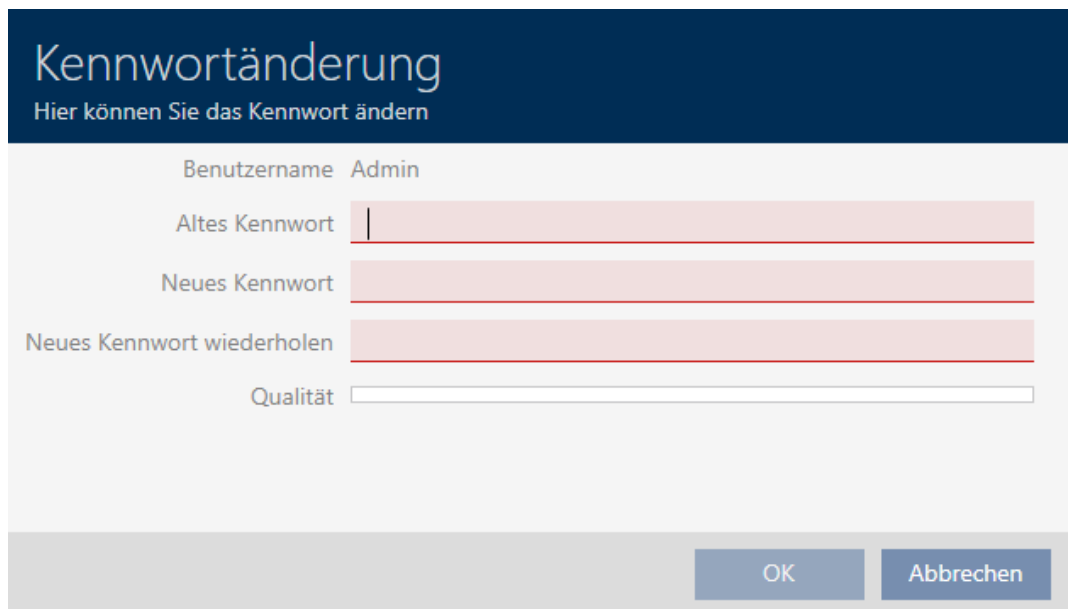




2. Select the **Change user password** entry in the | SETTINGS | group.



↳ 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.

## Kennwortänderung

Hier können Sie das Kennwort ändern

Benutzername Admin

Altes Kennwort

Neues Kennwort

Neues Kennwort wiederholen

Qualität

↳ The user password has now changed.

## Information

Das Benutzerkennwort wurde erfolgreich geändert



### 20.5.2 Increase password security

Passwords are a key component in your security concept. You can increase security using various settings:

SICHERHEIT BENUTZERKENNWORT

Kennwort muss regelmäßig geändert werden


Vorgeschriebenes Änderungsintervall (in Tagen)

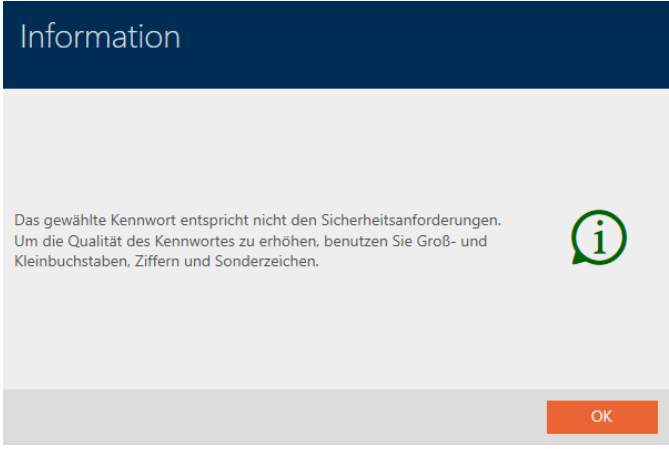
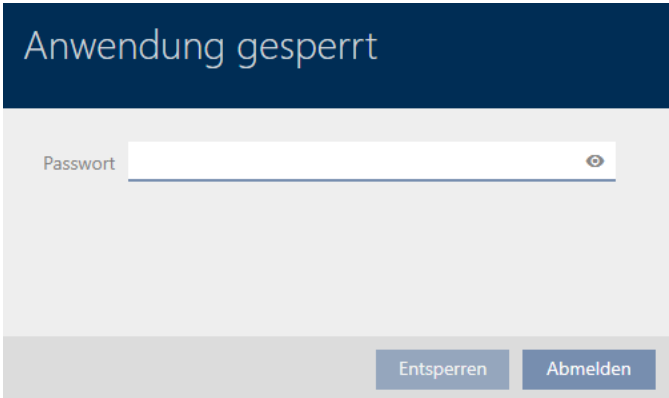
Kennworthistorie der letzten 10 Kennwörter verwenden


Den Benutzer nach 3malig falsch eingegebenem Kennwort sperren

Hohe Kennwortsicherheit

Sperrmechanismus bei Leerlauf (in Minuten)

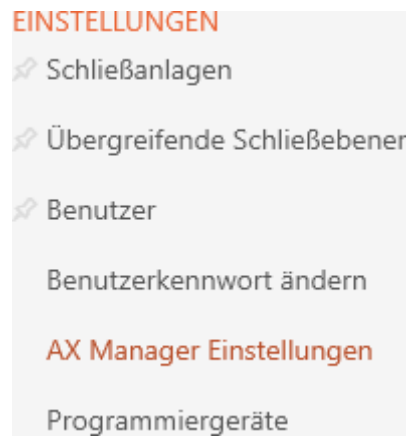
<p><input checked="" type="checkbox"/> Password must be changed regularly</p>	<p>After the configured change interval has expired, the user must assign a new password. You can set the change interval yourself using <i>Prescribed change interval (in days)</i>.</p>
<p><input checked="" type="checkbox"/> Lock the user after 3 incorrect password attempts</p>	<p>The new password must not be the same as any of the last ten passwords.</p>
<p><input checked="" type="checkbox"/> Use password history of the last 10 passwords</p>	<p>If a user has entered the password incorrectly three times, they will no longer be able to log in until they have been unlocked.</p> <div data-bbox="802 1184 1474 1480" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <p style="text-align: center; margin: 0;"><b>ANMELDEN AM PROJEKT</b></p> <p>Benutzername <input type="text" value="AdminAL"/></p> <p>Kennwort <input type="password" value="*****"/></p> <p style="text-align: right;"> Deutsch <span style="font-size: 0.8em;">v</span></p> <p style="text-align: center; margin-top: 10px;"><span style="background-color: #e67e22; color: white; padding: 5px 15px; border-radius: 3px;">Anmelden und Öffnen</span></p> </div> <p>Der Benutzer wurde gesperrt. Bitte wenden sie sich an den Projekt-Administrator.</p> <p>You as <i>Admin</i> must delete and create a new <i>AdminAL</i> user in AXM Plus.</p>

<p><input checked="" type="checkbox"/> High password security</p>	<p>AXM Plus automatically rejects trivial passwords such as “12345678”.</p> 
<p><input checked="" type="checkbox"/> Lock AXM when idle after (in minutes)</p>	<p>If your AXM Plus does not detect any actions within the configured idle time, your AXM Plus is automatically blocked.</p> 

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

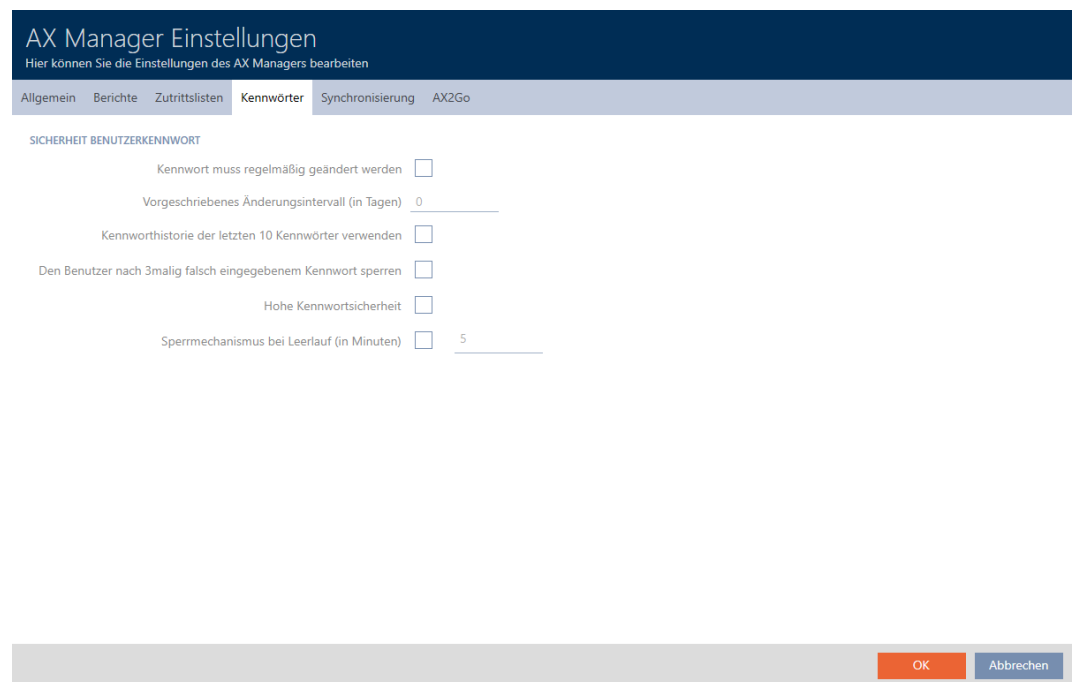


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The window with the AXM Plus 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 Plus settings closes.
  - ↳ New password requirements are active.

### 20.5.3 Name person as an AXM user

Matrixansicht x Benutzer x		
Neu                  Löschen	Aktivieren                  Deaktivieren	
Anzeigefilter löschen		
Name	Aktiviert	Zugewiesene Person
> Admin	Ja	Lupin, Remus
AdminAL	Ja	

You can name people in your project as AXM users to keep track of AXM Plus users. A person can be assigned to several users. The contact details for this person are taken directly from the database and automatically displayed for the user concerned.

#### Difference between Admin and AdminAL

There are only two user types in AXM Plus: Admin and AdminAL.

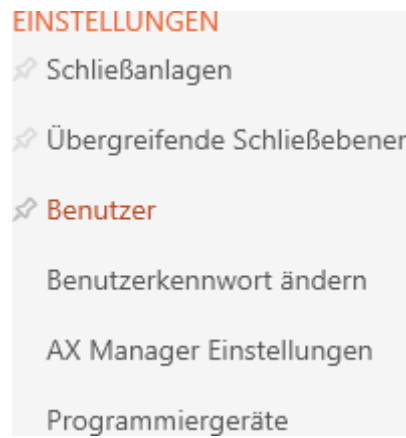
- **Admin** is the default user.
- **AdminAL** means AdminAccessList and is a strictly limited user. An AdminAL can mainly read access lists without having full access to the locking system. This allows other persons to read access lists without being able to manipulate the locking system themselves.

✓ At least one identification medium or at least one person is created.

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



2. Select the **Users** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The [Users] tab will open.

The screenshot shows the 'Benutzer' (Users) management interface. At the top, there are tabs for 'Matrixansicht' and 'Benutzer'. Below the tabs are action buttons: '+ Neu', 'Löschen', 'Aktivieren', 'Deaktivieren', and 'Anzeigefilter löschen'. The main area contains a table with the following data:

Name	Aktiviert	Zugewiesene Person
Admin	Ja	
AdminAL	Ja	

3. Click on the user to whom you wish to assign a person in the locking system.

- ↳ The "Users" window will open.

The screenshot shows the 'Benutzer - Details' (User Details) form. The title is 'Benutzer - Details' and the subtitle is 'Hier können Sie die Details für den Benutzer bearbeiten'. On the left, there is a sidebar with a list of tabs: '1 Details' (selected), '2 Projektrollen', '3 Schließanlagenrollen', '4 Bereichsrollen', '5 Personengruppenrollen', and '6 Übergr. Schließebene Rollen'. The main form area contains the following fields:

- Benutzername: Admin
- E-Mail:
- Zugewiesene Person:

At the bottom right, there are four buttons: '< Zurück', 'Weiter >', 'Fertigstellen', and 'Abbrechen'.

4. Select the person in your project that you wish to assign to the user from the ▼ Assigned person drop-down menu.



↳ The "Person information" section is automatically completed with the information stored for this person (*Name, Department, Tel.* and *E-Mail*).

5. Click on the **Finish** button.

↳ "Users" window closes.

↳ Assigned person is displayed next to the user.



#### 20.5.4 Assign tasks/user roles to AXM users

User roles are permissions for specific task fields. You can use the user roles to set which user is permitted to do what to your locking system. You can thus increase security in your locking system.

Only give each user the rights that they need to perform the designated tasks. Someone who only reads access lists, for example, does not need the locking system  Administration of access lists role. After all, they only need to read access lists and do not decide who is allowed to read access lists.

There are the following user roles in your AXM Plus:

Only the  Access lists and  Administration of access lists user roles can be changed in the "Locking system roles" in AXM Plus.



Project roles

<p>Protocol</p>	<p>Allows the database log to be read and exported. Example: <i>Tracking activities in the database (log)</i> [▶ 500]</p>
<p>Time schedule control</p>	<p>Allows schedules to be edited. Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Creating a schedule</i> [▶ 53]</li> <li>■ <i>Create time group</i> [▶ 56]</li> <li>■ <i>Deleting schedules</i> [▶ 64]</li> </ul>
<p>Site/Building management</p>	<p>Allows the corresponding organisational structures to be edited. Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Creating a location</i> [▶ 77]</li> <li>■ <i>Creating a building and assigning it to a location</i> [▶ 80]</li> </ul>
<p>Using SmartSync</p>	<p>Allows the use of SmartSync.</p>
<p>Hashtags</p>	<p>Allows hashtags to be edited. Example: <i>Creating a hashtag</i> [▶ 85]</p>
<p>User administration</p>	<p>Allows persons to be assigned to users and user roles to be edited. Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Name person as an AXM user</i> [▶ 478]</li> <li>■ <i>Assign tasks/user roles to AXM users</i> [▶ 480]</li> </ul>
<p>AX Manager settings</p>	<p>Allows your AXM Plus settings to be edited. Example: <i>Your personalised AXM interface</i> [▶ 433]</p>

Locking system roles

<p>Locking systems</p>	<p>Allows locking system details to be edited.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Create locking system [▶ 349]</i></li> <li>■ <i>Changing locking system password [▶ 383]</i></li> <li>■ <i>Enable cards or transponders [▶ 389]</i></li> </ul>
<p>Accesses</p>	<p>Allows access rights to be read and changed.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Changing individual authorisations (cross) [▶ 317]</i></li> <li>■ <i>Changing many authorisations (on identification media and/or locking devices) [▶ 318]</i></li> </ul>
<p>Personnel administration</p>	<p>Allows personal data to be edited.</p> <p>Example: <i>Persons and identification media [▶ 88]</i></p>
<p>Reporting</p>	<p>Allows reports to be exported.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Exporting the data protection report (GDPR) [▶ 507]</i></li> <li>■ <i>Displaying the report for identification media issue [▶ 504]</i></li> </ul>
<p>Administration of access lists</p>	<p>Allows the Access lists and Administration of access lists user roles to be changed. Anyone who does not have these user roles cannot read access lists themselves or allow others to.</p>

<p>Access lists</p>	<p>Allows access lists and physical access lists to be read.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Synchronising the locking device (including reading access list) [▶ 399]</i></li> <li>■ <i>Synchronise a card/transponder (including importing physical access list) [▶ 410]</i></li> </ul>
---------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Area roles**

<p>Read out locks</p>	<p>Allows locking devices to be read in general.</p> <p>Example: <i>Synchronising the locking device (including reading access list) [▶ 399]</i></p>
<p>Program locks</p>	<p>Allows locking devices to be synchronised.</p> <p>Example: <i>Synchronising the locking device (including reading access list) [▶ 399]</i></p>
<p>View/edit locks and areas</p>	<p>Allows locking devices and areas to be edited.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Creating a locking device [▶ 228]</i></li> <li>■ <i>Moving locking devices to areas [▶ 270]</i></li> <li>■ <i>Creating an area [▶ 83]</i></li> </ul>

**Person group roles**

<p>Read Transponders</p>	<p>Allows identification media to be read in general.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Recognise unknown cards/transponders [▶ 420]</i></li> <li>■ <i>Displaying the identification medium battery status [▶ 412]</i></li> </ul>
--------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------


<p>Program Transponders</p>	<p>Allows identification media to be programmed. Example: <i>Synchronise a card/transponder (including importing physical access list)</i> [▶ 410]</p>
<p>View/edit transponders and groups</p>	<p>Allows identification media and person groups to be viewed and edited. Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Duplicating an identification medium (including authorisations and settings)</i> [▶ 107]</li> <li>■ <i>Restricting identification medium authorisations to specific times (time group)</i> [▶ 119]</li> <li>■ <i>Assigning persons to person groups</i> [▶ 193]</li> </ul>

### Service Set roles

<p>Service Set Management</p>	<p>Allows you to set up and change common locking levels Examples:</p> <ul style="list-style-type: none"> <li>■ <i>Using a common locking level</i> [▶ 392]</li> </ul>
-------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

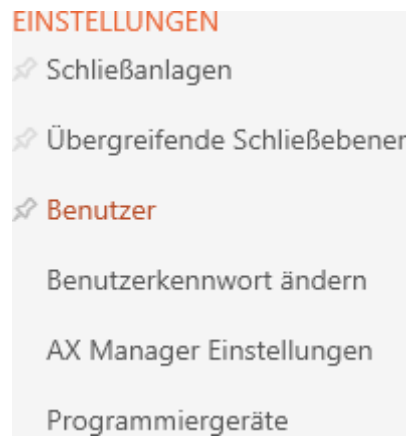
You can assign user roles in user management. In the example, AdminAL should no longer be able to decide whether other users are allowed to read access lists. As a result, we will deactivate the  Access lists user role for them.

- ✓ At least one identification medium or at least one person is created.

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



2. Select the **Users** entry in the | SETTINGS | group.



↳ The AXM bar will close.

↳ The [Users] tab will open.

Matrixansicht × Benutzer ×		
Name	Aktiviert	Zugewiesene Person
> Admin	Ja	
AdminAL	Ja	

3. Click the user whose user roles you want to edit (example: AdminAL).

↳ The "Users" window will open.

### Benutzer - Details

Hier können Sie die Details für den Benutzer bearbeiten

- 1 Details
- 2 Projektrollen
- 3 Schließenlagenrollen
- 4 Bereichsrollen
- 5 Personengruppenrollen
- 6 Übergr. Schließebene Rollen

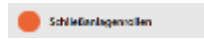
Benutzername

E-Mail

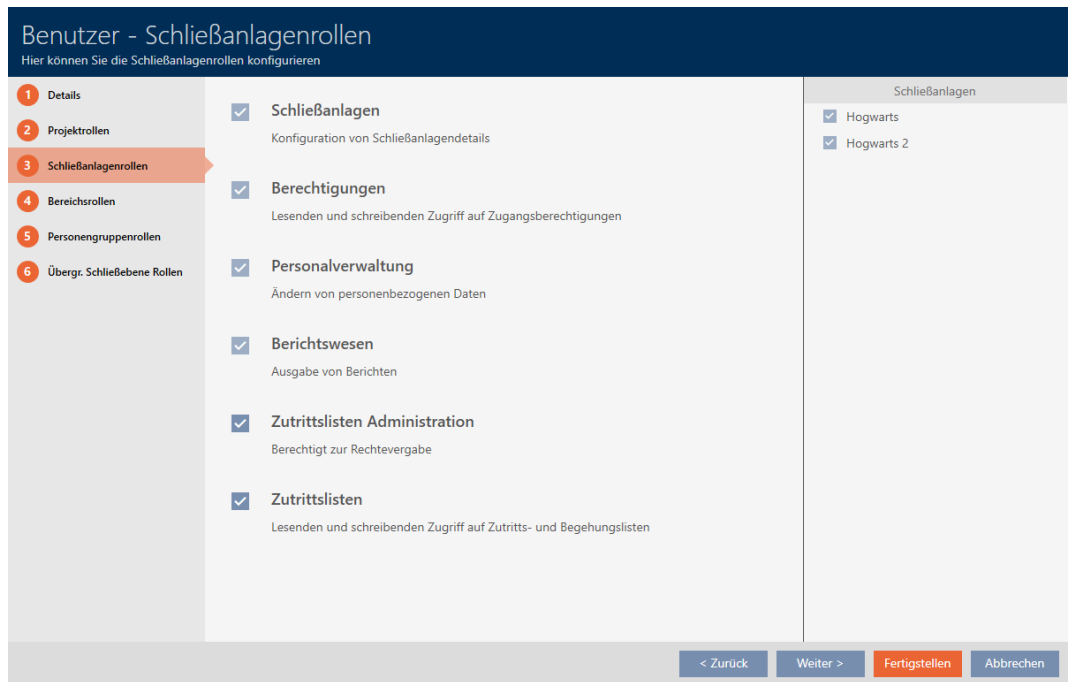
Zugewiesene Person

< Zurück
Weiter >
Fertigstellen
Abbrechen

- Click on the tab with the role that you want to change (example: **Locking system roles** tab).



↳ Window switches to the "Locking system roles" tab.



- Select or deactivate the required user roles (example: disable the  Administration of access lists checkbox).
- Use the **Next >** button to switch to the next tab or complete the entries with the **Finish** button.
  - ↳ "Users" window closes.
  - ↳ New user roles have been assigned (example: AdminAL can no longer change the  Access lists and  Administration of access lists checkboxes).



**NOTE**

**“Locking out” own user**

Users can also restrict their own user roles. Depending on which user roles are affected, these users can no longer restore them themselves.

Example: if you lock the Access lists and Access lists user roles yourself, you do not have the rights to change access list user roles. You have locked yourself out of these user roles.

AXM Plus prevents all users from locking themselves out of a user role simultaneously. If this is the case, the corresponding checkbox is greyed out.

1. Check carefully which user roles you activate or deactivate.
2. In such a case, ask another authorised user to assign the desired user role to you again.

## 20.6 AX2Go settings

AX2Go can be custom-adjusted to your personal needs.

**AX Manager Einstellungen**  
Hier können Sie die Einstellungen des AX Managers bearbeiten

Allgemein | Berichte | Zutrittslisten | Kennwörter | Synchronisierung | **AX2Go**

Ablauf der Einladung (in Stunden)

Hinweis: Mit dieser Einstellung bestimmen Sie die Gültigkeitsdauer einer versendeten Einladung. Nach Ablauf der Zeitspanne kann der Schlüssel nicht mehr in eine AX2Go App geladen werden. Ein hoher Wert erhöht den Komfort, kann aber ein Sicherheitsrisiko bedeuten.

Offline Zeitbudget (in Tagen)

Hinweis: Es werden keine Schließenlagendaten in der Cloud gespeichert, daher ist es notwendig, dass zur Synchronisierung sowohl der AXM Plus Dienst, als auch die AX2Go Applikationen aktiv und erreichbar (Online) sind. Hier stellen Sie die Gültigkeit eines Schlüssels ein, wenn eine der beiden Seiten nicht erreichbar (Offline) sind. Ein hoher Wert erhöht den Komfort, kann aber ein Sicherheitsrisiko bedeuten.

Schlüsselname

Kontaktperson

Unternehmen

Adresse

E-Mail

Tel.

OK Abbrechen

The following settings are available to you:

Setting	Meaning
Invite expiration (in hours)	The longer an invitation is valid, the more time users need to import it into their AX2Go app. Invitations that are valid for longer are more convenient but riskier. The maximum value is 120 hours (= 5 days).

Setting	Meaning
Offline time budget (in days)	<p>This setting determines how long the AX2Go will work on the mobile device if no connection can be established between AX2Go and your AXM Plus's AXM service. A longer offline time budget is more convenient but riskier.</p> <p>The maximum value is 30 days.</p> <p>Note: no locking system data is stored in the cloud. For synchronisation, the AX2Go must therefore be able to communicate to the cloud and from there to the AXM service. This means that both must be active and accessible (online).</p> <p>You can check the connection between the AXM service and the cloud: <i>Checking the connection between database and cloud</i> [▶ 432].</p>



#### NOTE

##### Differences in time budgets in AX2Go and the virtual network

AX2Go: the AXM service fully reloads the time budget as soon as the AX2Go has connected to it.

Main purpose: prevent a AX2Go permission from being used permanently using flight mode.

Virtual network: the gateway reloads the time budget as configured as soon as the identification medium is activated on it.

Main purpose: to fetch identification media to the gateway to transfer data regularly.


- See *Time budget (AX2Go and virtual network)* [▶ 540] for more information on time budgets.

Please also specify a suitable contact person for your internal support here (e.g. locking system administrator). This information is displayed in the mobile keys in the AX2Go app.

- Key name (e.g. locking system or company name)
- Contact person
- Company
- Address
- Email
- Phone number

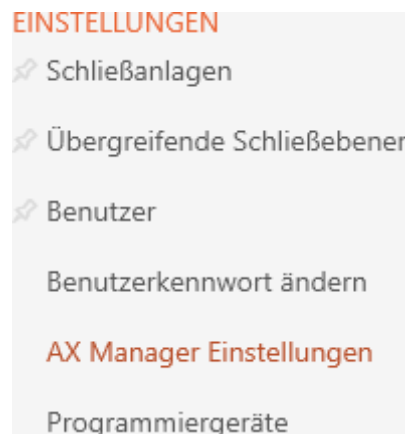


### Changing the AX2Go settings

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



2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
  - ↳ The window with the AXM Plus settings will open.
3. Go to the "AX2Go" tab.

4. Specify the required settings.

### AX Manager Einstellungen

Hier können Sie die Einstellungen des AX Managers bearbeiten

Allgemein
Berichte
Zutrittslisten
Kennwörter
Synchronisierung
AX2Go

Ablauf der Einladung (in Stunden)

Hinweis: Mit dieser Einstellung bestimmen Sie die Gültigkeitsdauer einer versendeten Einladung. Nach Ablauf der Zeitspanne kann der Schlüssel nicht mehr in eine AX2Go App geladen werden. Ein hoher Wert erhöht den Komfort, kann aber ein Sicherheitsrisiko bedeuten.

Offline Zeitbudget (in Tagen)

Hinweis: Es werden keine Schließenlagendaten in der Cloud gespeichert, daher ist es notwendig, dass zur Synchronisierung sowohl der AXM Plus Dienst, als auch die AX2Go Applikationen aktiv und erreichbar (Online) sind. Hier stellen Sie die Gültigkeit eines Schlüssels ein, wenn eine der beiden Seiten nicht erreichbar (Offline) sind. Ein hoher Wert erhöht den Komfort, kann aber ein Sicherheitsrisiko bedeuten.

Schlüsselname

Kontaktperson

Unternehmen

Adresse

E-Mail

Tel.

Hinweis: Der Schlüsselname wird auch in der AX2Go App angezeigt und dient der Identifizierung des jeweiligen Projekts. Die Kontaktinformationen werden als Hilfekontakt in den Schlüsseldetails angezeigt.

OK
Abbrechen

5. Click on the **OK** button.

- ↳ The window with the AXM Plus settings closes.
- ↳ Settings for your AX2Go are fixed and used on new AX2Go keys. Existing AX2Go keys receive the update twice daily with the AXM service or after a change to the AX2Go key.

## 21. Statistics and logs



### 21.1 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)* [▶ 284]). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation* [▶ 439] and *Synchronising the locking device (including reading access list)* [▶ 399]).

You can view and export the access list in the database.



#### NOTE

#### Displayed status corresponds to the last synchronisation

AXM Plus displays the status stored in the database at this point.

✓ 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.

Schließung - Details Hogwarts Synchronisieren In Matrix anzeigen

Hier können Sie Details der Schließung bearbeiten

- 1 Details
- 2 Konfiguration
- 3 Ausstattung
- 4 Zustand
- 5 Aktionen
- 6 Berechtigungsgruppen
- 7 Hashtags
- 8 Zutrittsliste
- 9 Berechtigte Transponder

SCHLIEBUNGSDetails

Bereich Lands

Seriennummer 0853NSX

Schließungstyp Schließzylinder

Bestellcode SV-Z5.EU.CO.30-30.A.G2.ZK.LN

Firmware Version 1.1.1147

Letzte Synchronisierung 06.05.2024 19:18:07

Batteriestatus Ok

Sync Berechtigungen

PinCode Griffindor electronic portrait

TÜRDetails

Tür Griffindor tower

Tür-Code DC-00001

Beschreibung

< Zurück
Weiter >
Fertigstellen
Abbrechen

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).

Schließung - Zutrittsliste

Hier können Sie die ausgelesene Zutrittsliste einsehen (nur bei Ausstattung ZK)

Hogwarts Synchronisieren In Matrix anzeigen

1 Details  
 2 Konfiguration  
 3 Ausstattung  
 4 Zustand  
 5 Aktionen  
 6 Berechtigungsgruppen  
 7 Hashtags  
 8 **Zutrittsliste**  
 9 Berechtigte Transponder

Löschen Export

Datum	Besitzer	S/N	Zugriff
08.05.2024 21:32:00	Snape, Severus	0301A4D	Erlaubt
08.05.2024 21:31:00	Snape, Severus	0301A4D	Erlaubt
08.05.2024 14:49:00	Sabotage		Erlaubt
25.04.2024 14:20:00	Unknown, Unknown	135CK3L	Erlaubt
25.04.2024 14:20:00	Unknown, Unknown	135CK3L	Erlaubt
25.04.2024 14:14:00	Unknown, Unknown	135CK3L	Erlaubt
25.04.2024 13:55:00	Gryffindor electronic portrait, Students	0873CDF	Erlaubt
25.04.2024 13:54:00	Gryffindor electronic portrait, Students	Removed	Erlaubt
25.04.2024 13:27:00	Unknown, Unknown	135CK3L	Erlaubt
25.04.2024 11:16:00	Unknown, Unknown	135CK3L	Erlaubt
25.04.2024 09:06:00	Gryffindor electronic portrait, Students	0873CDF	Erlaubt
25.04.2024 09:06:00	Gryffindor electronic portrait, Students	0873CDF	Erlaubt

< Zurück Weiter > Fertigstellen Abbrechen

1. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
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
14.12.2021 17:52:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 17:51:00	McGonagall, Minerva	UID-1000000034DB9B06	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
14.12.2021 01:40:00	Weasley, Percy	000XCKNG	Erlaubt	Master
13.12.2021 20:32:00	##ServiceTId_IDS_AX_SETTIME		Erlaubt	Master

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

## 21.2 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)* [▶ 118]). 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)* [▶ 410]).

You can view and export the physical access lists saved in the database.

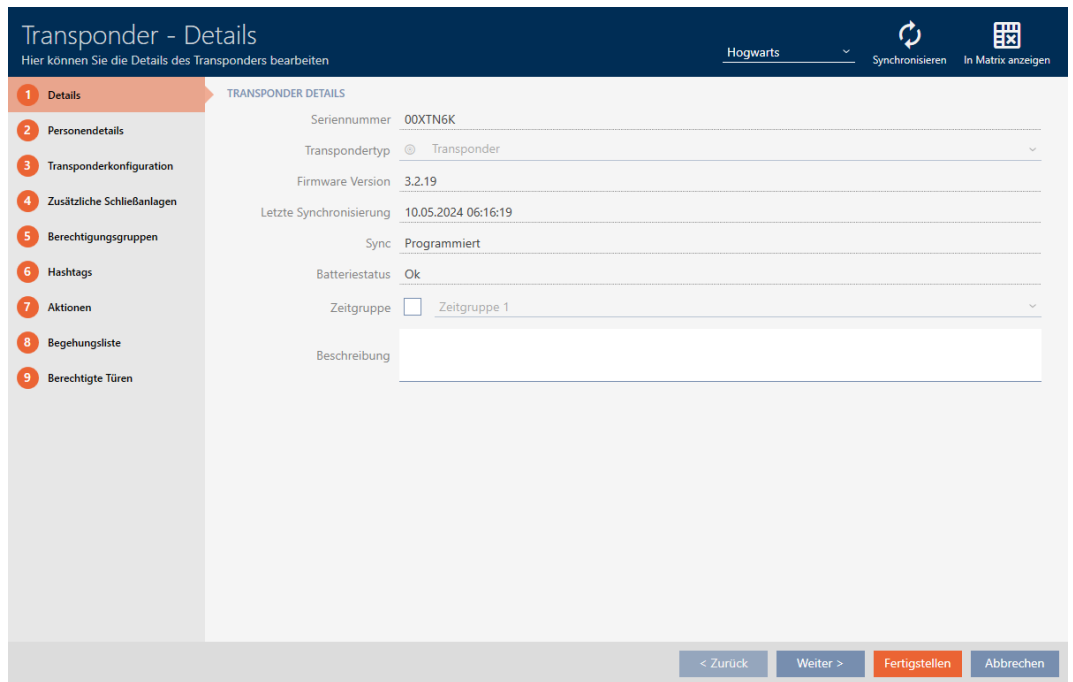


### NOTE

#### Displayed status corresponds to the last synchronisation

AXM Plus displays the status stored in the database at this point.

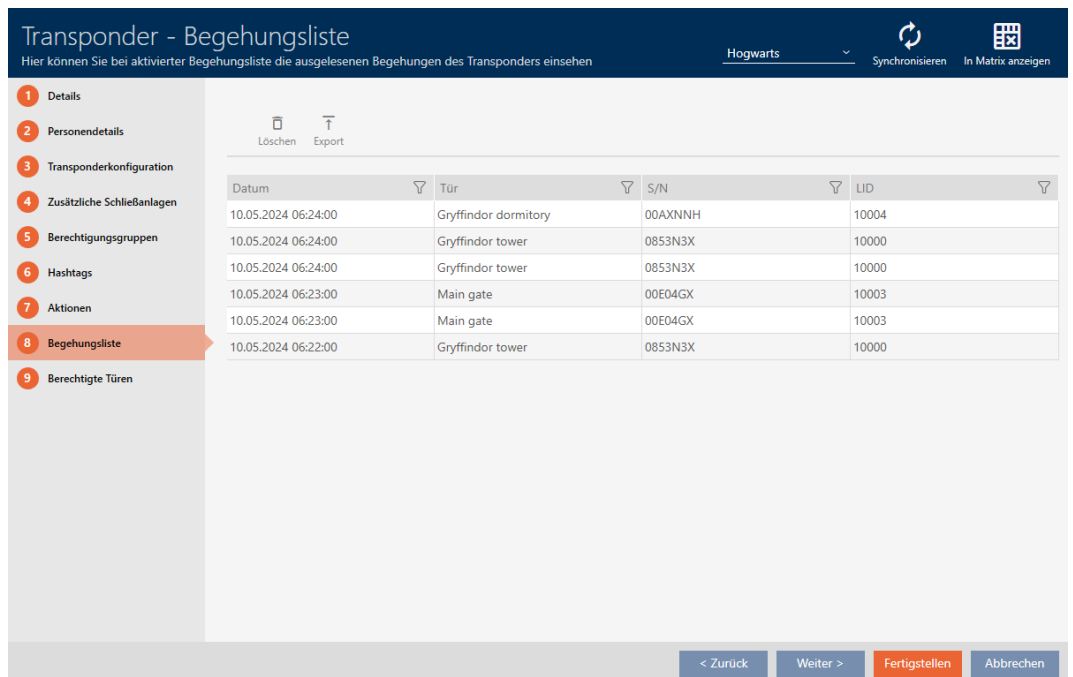
- ✓ Identification medium synchronised at least once.
- 1. Click on the identification medium whose physical access list you wish to display.
  - ↳ The identification medium window will open.




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* [▶ 44]).

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 Weasley '00XTN6K'

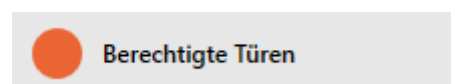
Datum	Tür	S/N	LID
10.05.2024 06:24:00	Gryffindor dormitory	00AXNNH	10004
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:22:00	Gryffindor tower	0853N3X	10000

You have the option to personalise reports (see *Personalising reports and exports* [▶ 445]).

### 21.3 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* [▶ 496]

- ✓ 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* [▶ 44]).
  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.

Transponder - Berechtigte Türen

Hier können Sie die Türen einsehen, an denen der Transponder berechtigt ist

Hogwarts In Matrix anzeigen Konfiguration



Tür	Tür-Code	Etage	Raumnummer	Gebäude	Standort	Bereich	LID
Gryffindor tower	DC-00001			Gebäude (Standard)	Standort (Standard)	Lands	10000
Main gate	DC-00012			Gebäude (Standard)	Standort (Standard)	Lands	10003
Gryffindor dormitc	DC-00022			Gebäude (Standard)	Standort (Standard)	Castle	10004
Snape's dungeon	DC-00032			Quidditch field	Hogwarts	Systemgruppe	128

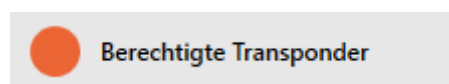
< Zurück Weiter > Fertigstellen Fertigstellen & Einladung senden Abbrechen

↳ Doors for which the identification medium is authorised are displayed.

### 21.4 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* [▶ 495]

- ✓ 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* [▶ 44]).
  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.





S/N	Besitzer	Schließanlage	TID
00XTN6K	Weasley, Ron	Hogwarts	3209
135CK3L	Lupin, Remus	Hogwarts	3210
0301A4D	Snape, Severus	Hogwarts	3201

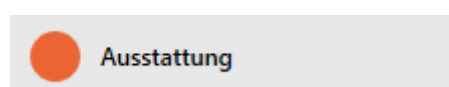
↳ Identification media that are authorised for the door are displayed.

## 21.5 Displaying a locking device's equipment features

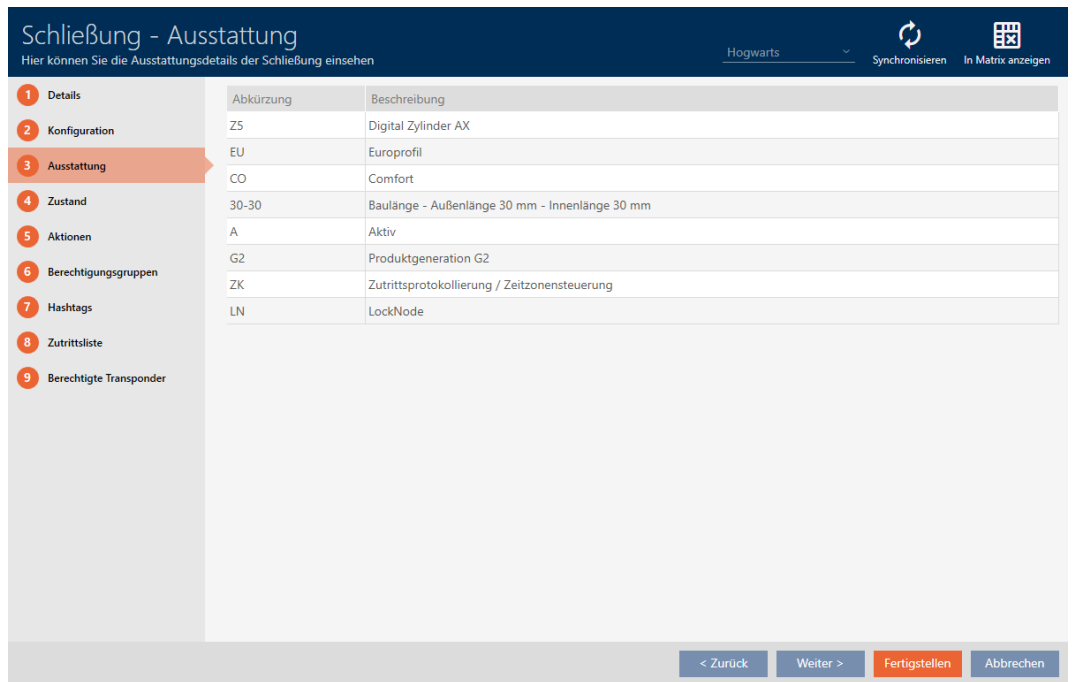
A locking device's equipment features are also imported during synchronisation. This allows AXM Plus to check whether the locking device is actually able to handle the required settings at all (e.g. whether an access control function is available).

You can display the imported equipment features in AXM Plus:

- ✓ 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* [▶ 44]).
  2. Click on the locking device whose equipment features you wish to display.
    - ↳ The locking device window will open.
  3. Click on the  **Ausstattung** tab.



↳ Window switches to the "Features" tab.



↳ Equipment features are displayed.

## 21.6 View statistics and warnings (dashboard)

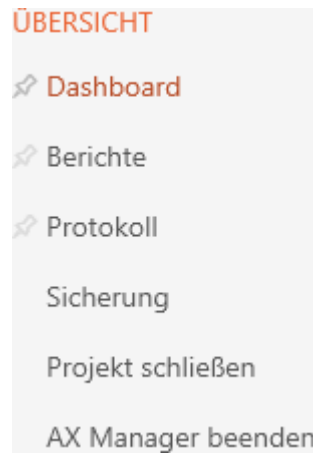
AXM Plus comes with a new dashboard that gives you statistics on your database at a glance.

1. Click the orange AXM button .

↳ AXM bar opens.



- Select the **Dashboard** entry in the | OVERVIEW | group.



- ↳ The AXM bar will close.
- ↳ The [Dashboard] tab will open.

## Dashboard

Widgets konfigurieren

Projekt: Hogwarts

STATISTIK	
Anzahl Schließanlagen:	2
Anzahl Türen:	4
Anzahl nicht programmierter Schließungen:	0
Anzahl Transponder:	13
Anzahl nicht programmierter Transponder:	1
Anzahl Berechtigungsgruppen:	6
Anzahl Berechtigungsausnahmen:	1
Anzahl Personengruppen:	2
Anzahl Bereiche:	1

WARNUNGEN			
Status	Datum	Warnungstyp	Beschreibung
	14.12.2021 15:51:00	Schließung defekt / aust	Schließung 'Gryffind
	27.10.2021 12:34:49	Schließung defekt / aust	Schließung 'Main Ent
	27.10.2021 12:32:40	Schließung defekt / aust	Schließung 'Main Ent
	27.10.2021 12:30:59	Schließung defekt / aust	Schließung 'Main Ent

- ↳ 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:


- Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
- Click on the warning entry in the Warning column.
  - ↳ Warning will open.

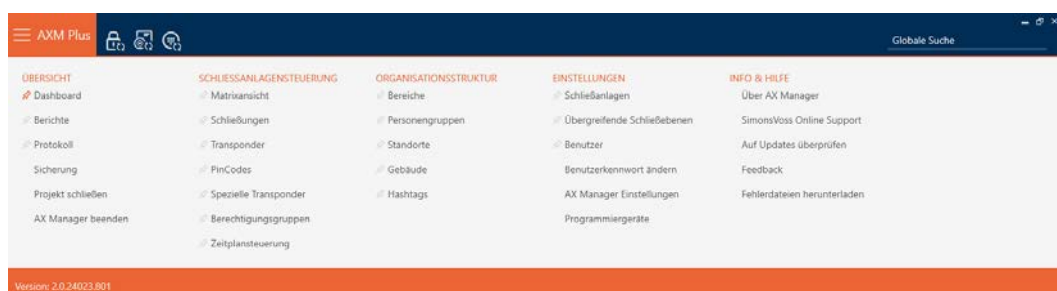
3. Change the *Title* and *Text* fields as required.
4. Deal with the warning if necessary. Then return to the warning and activate the  Completed? checkbox.
5. Enter input into the *Comment* field.
6. Click on the **OK** button.
  - ↳ Warning closes.
  - ↳ Warning appears in the dashboard with a check mark as resolved.

## 21.7 Tracking activities in the database (log)

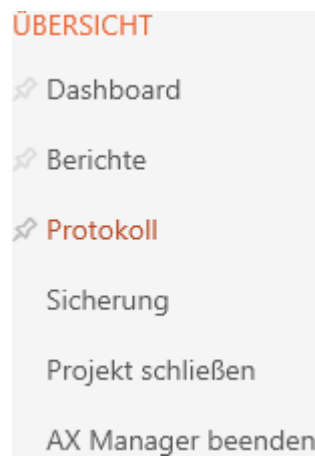
Every change and every setting in the database is logged in AXM Plus. This allows you to track who changed what in the database and when they made the changes.

The log archiving period can be adjusted (see *Setting the log archiving period* [▶ 502]).

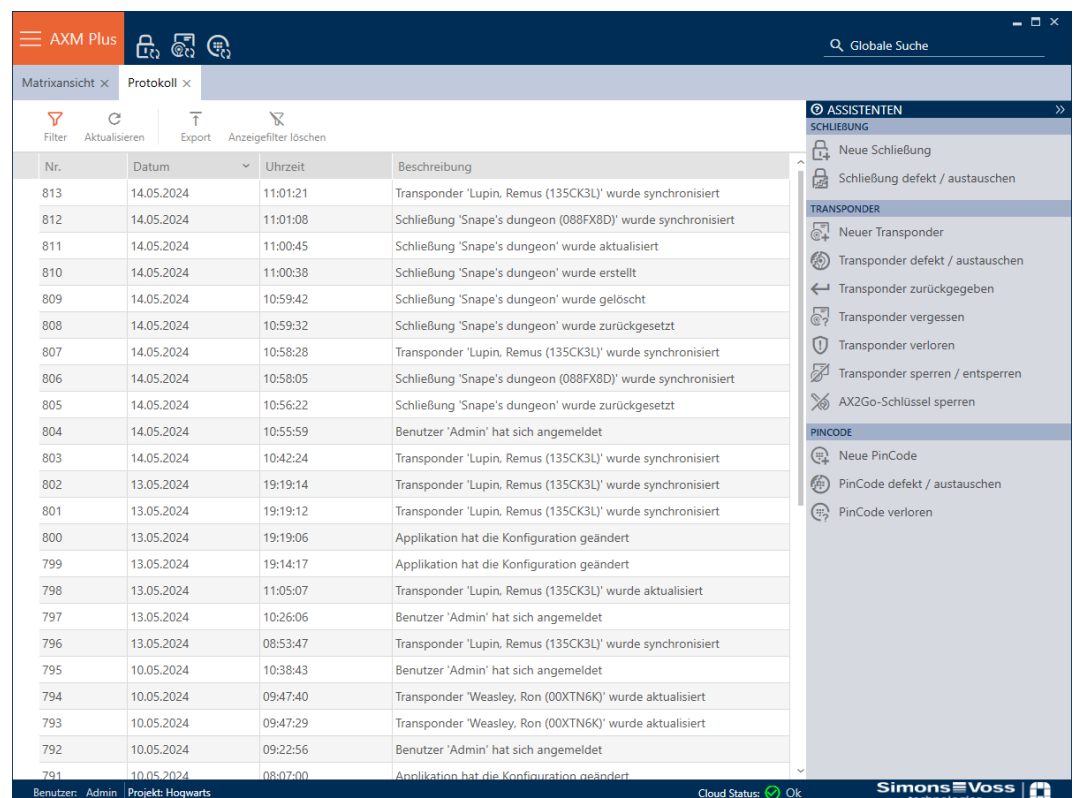
1. Click the orange AXM button .
  - ↳ AXM bar opens.



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* [▶ 44]).

↳ Log is displayed.

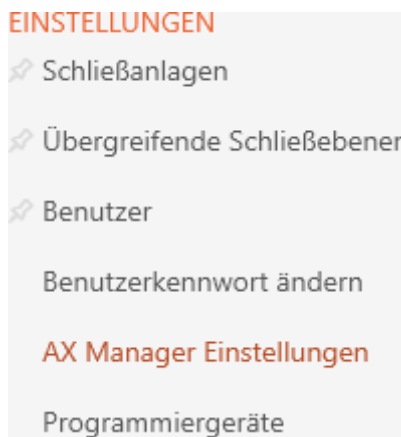
The **Export** button also allows you to export the log to provide a permanent backup.

### 21.7.1 Setting the log archiving period

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

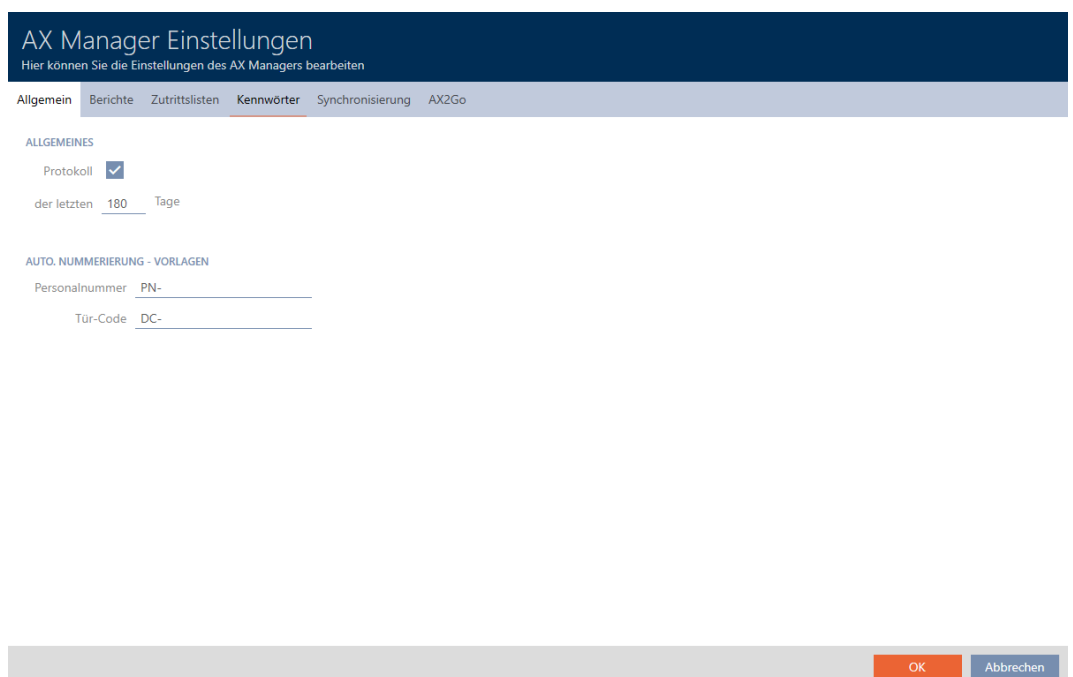


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The window with the AXM Plus settings will open.

3. Go to the [General] tab.

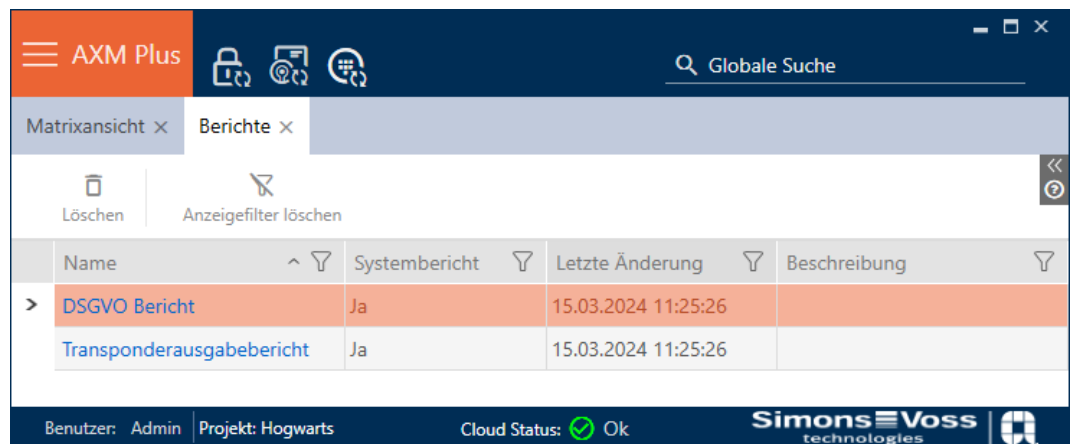
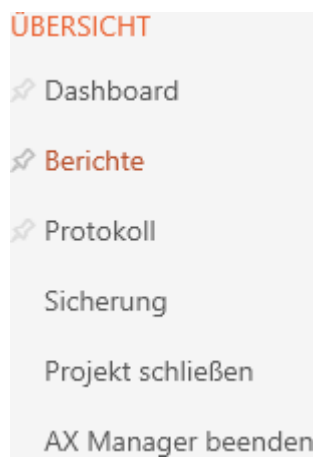


4. If you do not wish to log the changes to the database at all: Activate the  Protocol checkbox.
5. Enter the required archiving period (max. 670 days).
6. Click on the **OK** button.
  - ↳ The window with the AXM Plus settings closes.
  - ↳ Protocol is limited to the required duration.

## 21.8 Reports

Reports are a useful tool that allow you to keep an eye on your locking system at all times.

Some of these reports (namely the system reports) can be found in the [Reports] tab:




However, you cannot display the reports in this tab. You have the option of entering your own values in the *Description* and *Name* fields instead. Entries in the *Name* field are included as headings in the report concerned.

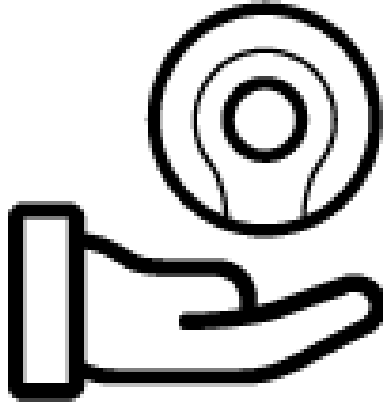
You can display the actual reports at the useful points in AXM Plus .

Example: you can find the data protection report in several places.

- With the **GDPR data** button in the "Person details" tab in the identification media window.

- With the **GDPR data**  button in the [Transponders] tab.

### 21.8.1 Displaying the report for identification media issue



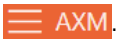
You can use this report to prove that someone has received a specific identification medium and instruction from you.

You can thus only export this report specifically for one selected identification medium at a time.

You as a locking system operator can thus record the TID and protect yourself. Signature fields are provided on the report for this purpose.


The report contains the following data:

- Name of the person who received the identification medium
- The issued identification medium's serial number
- The locking system administrator's telephone number (source: AX Manager settings; see *Personalising reports and exports* [[▶ 445](#)])
- The locking system administrator's email address (source: AX Manager settings, see *Personalising reports and exports* [[▶ 445](#)])
- The locking system administrator's address
- Date when the report was created
- Optional: scheduled return date
- Optional: authorisations (including areas)










1. Click on the orange AXM icon .   
↳ 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. Make changes if necessary in the drop-down menu which contains the desired identification medium in the top right-hand corner of the locking system.
4. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 44]).
5. Select the identification medium you wish to display.
  - ↳ The highlighted row is shown in orange.

Transponder x Hogwarts


Nachname	Vorname	S/N	Typ	Sync	Status	Zeitgruppe	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L					
Snape	Severus	0301A4D				Zeitgruppe 2	
> Weasley	Ron	00XTN6K					
Wood	Oliver	UID-148024BA5A7369					

6. Click on the **Issue Transponder** button .
  - ↳ The "Transponder handover" window will open.

## Transponderausgabe

Bitte geben Sie die gewünschten Informationen ein


Rückgabedatum angeben

geplantes Rückgabedatum  

mit Berechtigungen

in die Aktionsliste eintragen

Bericht in der Aktionsliste abspeichern

- If you want to include a possibly predetermined return date, select the  Specify return date checkbox and select the return date by clicking on the  calendar.
- If you also want to include any existing authorisations, select the  With authorisations checkbox.
- If you also want to enter the issuing of the identification medium in its action list, select the  Enter in the Actions list checkbox and use the  Save report in the Actions list checkbox to also save the corresponding medium in the action list if necessary (also see *Planning and tracking identification medium management tasks* [▶ 174] for the action list).
- Click on the  button.
  - ↳ "Transponder handover" window closes.
  - ↳ The Explorer window will open.
- Save the PDF file to a directory of your choice.
  - ↳ Issue report for the selected identification medium is exported as a PDF file (DIN A4).

## Transponderausgabe

Weasley, Ron / 6

Ich bestätige hiermit, dass ich heute den Transponder mit der nachfolgend aufgeführten Seriennummer erhalten habe und die üblichen Sicherheitsvorkehrungen beim Benutzen und Aufbewahren beachten werde.

Seriennummer: 00XTN6K

\* Bei Verlust des Transponders ist die zuständige Schließanlagenverwaltung sofort zu informieren.  
 \* Eine Weitergabe an Dritte ist unzulässig.  
 \* Der Transponder ist beim Austritt des Mitarbeiters wieder an die Schließanlagenverwaltung zurückzugeben.

Eintragungen im obigen Textfeld beruhen auf betrieblichen Vereinbarungen/Vorgaben der Betreibergesellschaft. Die SimonsVoss Technologies GmbH übernimmt keine Gewähr für diese Angaben

14.05.2024 \_\_\_\_\_

Weasley, Ron

zurückgenommen: \_\_\_\_\_

You have the option to personalise reports (see *Personalising reports and exports* [[▶ 445](#)]).

You can also enter the issue date directly in the action list for the identification medium concerned (see *Note card/transponder issue date* [[▶ 175](#)]).

### 21.8.2 Exporting the data protection report (GDPR)



The data protection report (=GDPR report) informs you which personal data relating to a person is stored in AXM Plus. You can export this report to multiple people at the same time. A separate PDF file is exported for each person.

The report can be confirmed with the existing signature field.

It consists of the following sections:

Person details

**Personendetails**

<b>Titel</b>	Junior Assistant
<b>Vorname</b>	Percy
<b>Nachname</b>	Weasley
<b>Personalnummer</b>	PN-30
<b>Abteilung</b>	Department of International Magical Cooperation
<b>Telefon</b>	+44 020 3492 32113 85
<b>E-Mail</b>	pweasley@ministryofmagic.com
<b>Adresse</b>	Whitehall London, England Great Britain
<b>Ort/Debäude</b>	Ministry
<b>Eingestellt am</b>	03.02.2010 00:00:00
<b>Eingestellt bis</b>	11.02.2022 00:00:00
<b>Geburtsdatum</b>	07.06.2000 00:00:00
<b>Kostenstelle</b>	57324

This section contains the stored personal data.

- First name
- Last name
- Personnel number
- Telephone
- E-Mail
- Address

Entries that are empty in AXM Plus are automatically hidden in the report.

**Person History**

**Personenhistorie**

Personalnummer	Datum	Vorname	Nachname
PN-30	14 Dezember 2021 1:20	Fred	Weasley
PN-30	14 Dezember 2021 1:32	Percy	Weasley

This section logs the changes to the following data:

- First name
- Last name
- Personnel number

Protocol

Protokoll

Nr.	Datum	Uhrzeit	Beschreibung
1661	14 Dezember 2021	18:55:18	Transponder 'Weasley, Percy (000XCKNG)' wurde aktualisiert
1662	14 Dezember 2021	18:55:37	Transponder 'Weasley, Percy (000XCKNG)' wurde synchronisiert
1663	14 Dezember 2021	19:27:05	Transponder 'Weasley, Percy (000XCKNG)' wurde Zugriffsliste wurden synchronisiert
1672	03 Januar 2022	18:40:47	Transponder 'Weasley, Percy (000XCKNG)' wurde aktualisiert


This section is a change log. All entries in the database relating to this person or their identification medium are displayed here (also see *Tracking activities in the database (log)* [▶ 500]).



**NOTE**

**Exporting user-defined fields**

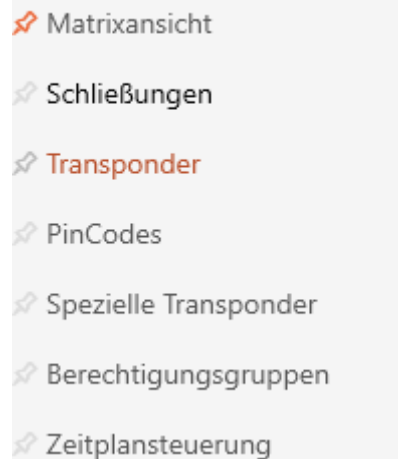
You can also create user-defined fields for Person details (see *Personalising properties for person details* [▶ 449]). These are then exported too.

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



- Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.

**SCHLISSANLAGENSTEUERUNG**



- ↳ The AXM bar will close.
- ↳ The [Transponder] tab will open.

- Make changes if necessary in the drop-down menu which contains the desired identification medium in the top right-hand corner of the locking system.
- Highlight one or more identification media whose data protection reports you wish to export.
  - ↳ Highlighted rows are shown in orange.

Transponder x Hogwarts

Neu Löschen In Matrix anzeigen Duplizieren Ausgabe DSGVO-Daten Export Anzeigefilter löschen Importieren

Nachname	Vorname	S/N	Typ	Sync	Status	Zeitgruppe	Aktivierungsdatum / Verfallsdatum
Lupin	Remus	135CK3L					
Snape	Severus	0301A4D				Zeitgruppe 2	
> Weasley	Ron	00XTN6K					
Wood	Oliver	UID-148024BA5A7369					

- Click on the **GDPR data** button .
  - ↳ The Explorer window will open.
- Save the report to a directory of your choice.
  - ↳ Data protection report is exported as a PDF (DIN A4).
  - ↳ If you have highlighted multiple identification media, the Explorer window will open again immediately and you can save the next report.

### DSGVO-Bericht

#### Personendetails

Vorname	Ron
Nachname	Weasley
Personalnummer	PN-6
Abteilung	Pupils
Telefon	08932168
E-Mail	ron.weasley@hogwarts.co.uk
Adresse	The Burrow Devon
Ort/Gebäude	Gryffindor rooms
Kostenstelle	310
Büronr.	23523

#### Personenhistorie

Personalnummer	Datum	Vorname	Nachname
PN-6	10.05.2024 07:37	Ron	Weasley

#### Protokoll

Nr.	Datum	Uhrzeit	Beschreibung
775	10.05.2024	04:06	Transponder 'Weasley, Ron' wurde zurückgesetzt
776	10.05.2024	04:08	Transponder 'Weasley, Ron (00XTN6K)' wurde synchronisiert
777	10.05.2024	04:15	Transponder 'Weasley, Ron (00XTN6K)' wurde aktualisiert

14.05.2024 \_\_\_\_\_

You have the option to personalise reports (see *Personalising reports and exports* [[▶ 445](#)]).

See *Information on data protection* [[▶ 14](#)] for further general information on data protection in System 3060.

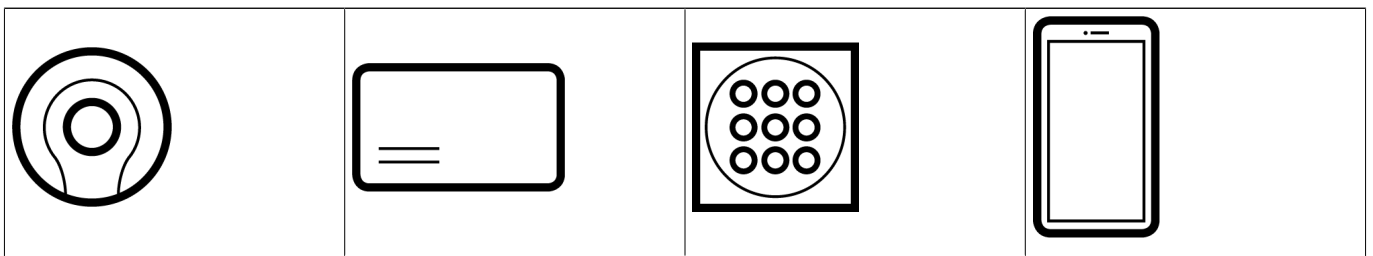
## 22. Background knowledge and explanations

### 22.1 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
- AX2Go app on smartphone



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 Plus 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 Plus knows which serial number and which TID belong together.

	TID
Seriennummer 002TU6TC	3203

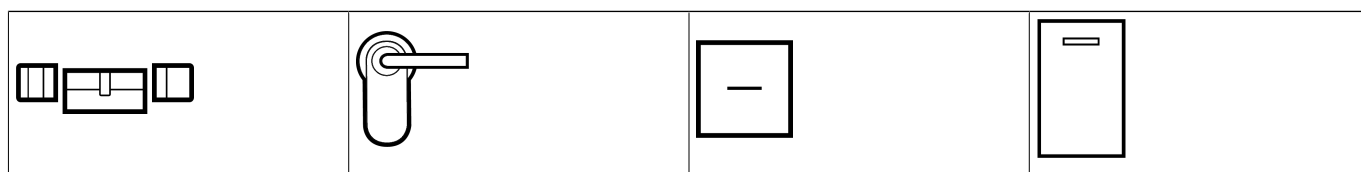
However, this link is confined to AXM Plus and is not written onto identification media or locking devices. A locking device uses the TID (and not the serial number) to check whether an identification medium is authorised or not.

Passive identification media have physical limitations when put to use (see [Cards and locking device IDs \[► 552\]](#)).

### 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 Plus 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 Plus knows which serial number and which LID belong together. However, this link is confined to AXM Plus 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.

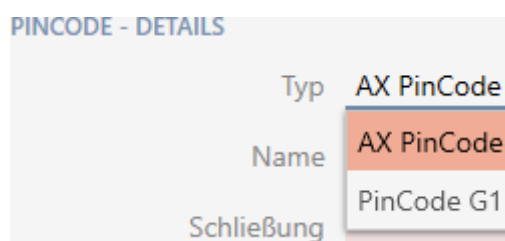
Normally, you don't need to concern yourself with the TID and LID as your AXM Plus does everything in the background.

### 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.

#### 22.1.1 PIN Code G1 vs. PIN Code AX

The AXM Plus offers you two different PIN code keypads:



- PIN code keypad 3068
- PIN code keypad AX

These two PIN code keypads are almost identical on the outside. You can recognise the PIN code keypad AX by a Bluetooth symbol:



However, the programming and the interface used are different:

	PIN code keypad AX	PIN code keypad 3068
Interface	<ul style="list-style-type: none"> <li>❑ BLE (Bluetooth low energy)</li> </ul>	<ul style="list-style-type: none"> <li>❑ Active (= 25 kHz) with G1 protocol</li> </ul>
Read range	<ul style="list-style-type: none"> <li>❑ Good range for AX locking devices</li> </ul>	<ul style="list-style-type: none"> <li>❑ Good range for non-AX locking devices</li> <li>❑ Shorter range of AX locking devices</li> </ul>
PIN assignment	<ul style="list-style-type: none"> <li>❑ Programming of PINs directly in the AXM Plus</li> <li>❑ Log in to the AXM Plus as authorisation for programming</li> </ul>	<ul style="list-style-type: none"> <li>❑ Programming of PINs directly on the PIN code keypad 3068</li> <li>❑ Segmentation into one Master PIN and up to three User PINs</li> <li>❑ Master PIN as authorisation for programming</li> </ul>

	PIN code keypad AX	PIN code keypad 3068
Synchronization	<p>Your AXM Plus will help you synchronise with instructions. The process in brief:</p> <ol style="list-style-type: none"> <li>1. Start synchronisation.</li> <li>2. Press and hold 0 for at least two seconds to enter programming mode.</li> <li>3. Wait until synchronisation is complete.</li> </ol>	<p>Your AXM Plus will help you synchronise with instructions. The process in brief:</p> <ol style="list-style-type: none"> <li>1. Create Master PIN on the PIN code keypad 3068.</li> <li>2. Create User PINs with Master PIN on the PIN code keypad 3068.</li> <li>3. Start synchronisation. Enter 00 and master PIN on PIN code keypad 3068.</li> <li>4. Continue with synchronisation in AXM Plus.</li> <li>5. Enter the corresponding PIN code keypad 3068 on the keypad on User PIN (e.g. 1 for the first User PIN).</li> <li>6. Wait until synchronisation is complete.</li> </ol>

**Behaviour during initial synchronisation, additional PINs and authorisation changes**

A significant difference between the PIN code keypad AX and the PIN code keypad 3068 is also the behaviour during the first synchronisation and in the event of authorisation changes.

This difference is due to the different communication between the two PIN code keypads and the locking device:

- PIN code keypad AX: uses a permanently assigned BLE channel to send information to the locking device.  
Such information could be, for example, “Entered PIN authorised”.
- PIN code keypad 3068: uses the G1 protocol and a separate G1 ID for each PIN.

	PIN code keypad AX	PIN code keypad 3068
First synchronisation	<p>The permanently assigned BLE channel must be set up for both the PIN code keypad AX and the locking device. This is performed in the background when assigning a PIN code keypad AX.</p> <p>This is why a programming requirement arises <b>on the PIN code keypad and on the locking device</b> after assignment of PIN code keypad AX.</p>	<p>The PIN code keypad 3068 receives one G1 ID per PIN and the locking device receives a locking plan with information on whether this G1 ID is authorised.</p> <p>This is why a programming requirement arises <b>on the PIN code keypad and on the locking device</b> after assignment of PIN code keypad 3068.</p>
Additional PINs	<p>New PINs are saved in the PIN code keypad AX. The previously configured BLE channel that will still be used for commands to the locking device.</p> <p>The new PINs are communicated to the PIN code keypad AX, which is why <b>programming is only required on the PIN code keypad.</b></p>	<p>New PINs are saved in the PIN code keypad 3068 with one G1 ID per PIN. This G1 ID is then saved as authorised in the locking plan.</p> <p>The new G1 IDs are communicated to the PIN code keypad 3068 and the changed locking plan is saved in the locking device. This means that <b>programming is required on the PIN code keypad and locking device.</b></p>
Changes to authorisations	<p>The PIN code keypad AX continues to use the channel previously configured for commands to the locking device. For this reason, AXM Plus only needs to inform the PIN code keypad AX when it should send information such as “Entered PIN authorised” to the locking device. <b>Programming is only required on the PIN code keypad.</b></p>	<p>The PIN code keypad 3068 retains the G1 ID unchanged. The changed authorisation is saved in the locking device’s locking plan.</p> <p>This means that <b>programming is only required on the locking device.</b></p>

### 22.1.2 AX2Go

#### 22.1.2.1 General information

AX2Go is a mobile key for opening SimonsVoss digital locking components using Bluetooth Low Energy (BLE). Bluetooth Low Energy is a wireless standard that is used to establish a Bluetooth connection, including when transmission power and power consumption are low.

If locking authorisations are stored in the app, the smartphone can be used like an access card or transponder. It's this easy: unlock your smartphone, touch the locking device with it and open the door. The AX2Go app runs in the background and does not need to be launched to open the door.

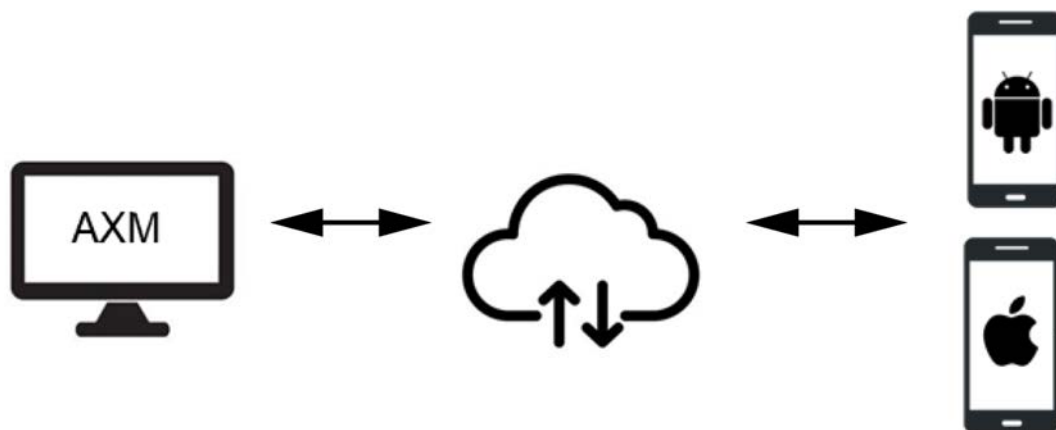
### Functions

- Up to 5 different locking systems (AX2Go key) on one smartphone
- Transfer key authorisations via **email**, **SMS** or **QR** code from **AX Manager** (management software)
- Easy to set up, meaning the app is ready to use in less than a minute
- Clearly visible access status and quick solution assistance
- No registration or verification required

#### 22.1.2.2 Synchronisation of AX2Go keys via the cloud

You distribute changes such as authorisations, time, etc. to your AX2Go users conveniently via a cloud connection.

The SimonsVoss cloud **transfers** data from your AXM Plus to the AX2Go **without** data being **stored** in the SimonsVoss cloud (tunnel; no dormant customer data).



The AX2Go uses a direct connection via Bluetooth Low Energy (=BLE channel). The locking device firmware must be version 1.1.1148 or higher to use this BLE channel. You can update the firmware yourself with a simplified patch tool provided for this purpose (except for directly networked locking devices = WaveNet).

### Data transfer

A AX2Go key is basically a virtual G2 transponder on a smartphone. As with a normal G2 identification medium, you can also choose in this case whether you would prefer to synchronise the locking device or the AX2Go

key. Thanks to the cloud connection, however, your AXM Plus is virtually directly connected to the AX2Go keys and transfers authorisation changes, for example, almost immediately using a service running in the background.

Less prioritised data (e.g. changes to the locking system administrator's contact details) are also transferred automatically via the cloud, but not immediately:

- During the AXM service's next push cycle (twice daily) or
- Together with higher-priority data (e.g. an authorisation change)

As AXM Plus - similar to LSM Basic Online - is a local installation, the AXM service only runs when you have started the computer. The AXM Plus itself does not need to be open for this service.

#### Prerequisites for using the cloud services

- Connection between your AXM Plus and your SimonsVoss ID (see *Checking the connection between database and cloud* [▶ 432])
- Valid registration with Service fee licence (see *Registration* [▶ 29])

#### 22.1.2.3 Time budget in AX2Go

A smartphone could be set to flight mode and thus the connection to the AXM service could be intentionally interrupted. In this case, an authorisation change (in particular also blocking the AX2Go key) would never reach the AX2Go.

"Offline time budget (in days)" forces all AX2Go users to allow a connection between the AX2Go and AXM service on a regular basis. The smartphone user does not need to take action themselves. This prevents flight mode from being misused and inadvertently use a permission permanently.

This Offline time budget (in days) differs from the time budget in a virtual network (see *Time budget (AX2Go and virtual network)* [▶ 540] for details).

#### 22.1.2.4 Security

##### Can data be manipulated or copied?

No. In addition to the components already mentioned, we also use random number series (what are known as counters), which are attached to each data package once during each transfer. Subsequent transmission with manipulated or copied data will feature the wrong counter and the data is unusable.

Each component represents a high level of security and thus protects our data reliably, sustainably and redundantly.

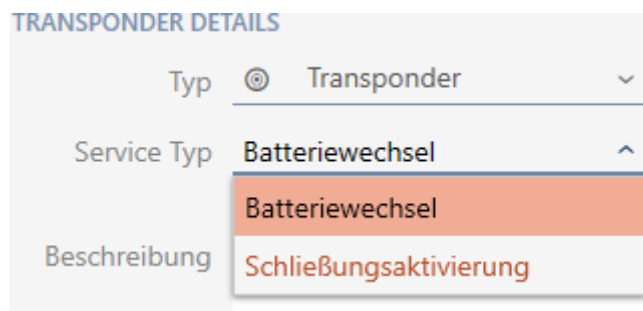
**How do I make sure that the person I invited actually gets the AX2Go key? What happens if the email is intercepted or forwarded unnoticed?**

To eliminate the risk of intercepted emails, it is advisable to send the invitation link from the AXM administration software via an end-to-end encrypted communication channel such as an encrypted email. To do this, select the invitation type "QR Code" and copy the generated dynamic link into your email program.

You can also send the invitation without authorisations for the time being and only add them at a later stage (when you know that the right user has received the invitation) via group or individual authorisations.

**22.1.3 Special identification media and their functions**

There are identification media with special functions in System 3060. These identification media only have one special function, i.e. a battery replacement transponder cannot simultaneously become an activation transponder, for example.





Battery replacement	Lock Activation
<p>G2 locking devices switch to freeze mode when the battery level is very low. Once in freeze mode, locking devices no longer react to authorised transponders.</p> <p>You can temporarily cancel freeze mode on G2 locking devices with a Battery replacement identification medium.</p> <p>You can then engage the locking device with a second, authorised identification medium to open the door and replace the batteries.</p> <p>This does not affect AX locking devices as the batteries can also be accessed and replaced when completely discharged.</p>	<p>You can reactivate a disabled locking device with a Lock Activation identification medium.</p> <p>You can then engage the locking device with a second authorised identification medium.</p>

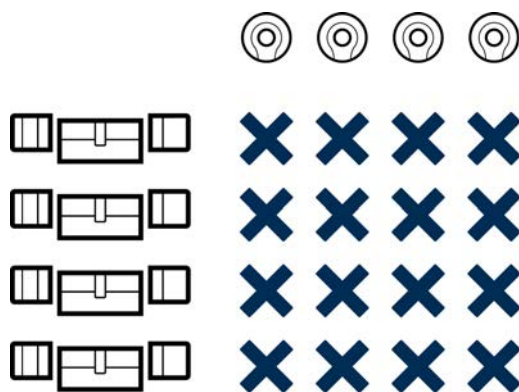
## 22.2 Locking systems

A locking system is a contiguous structure consisting of:

- Locking plan
- Organisational components

### Locking plan

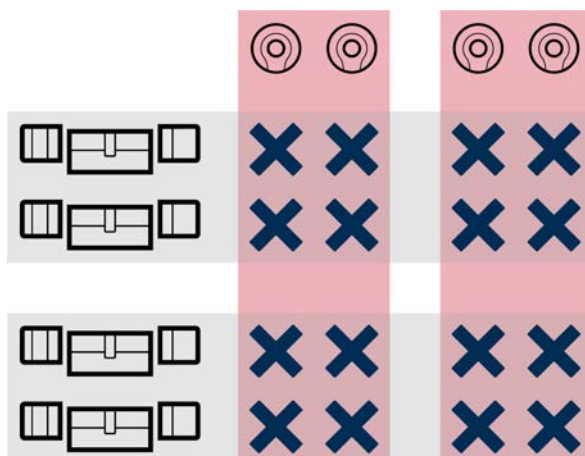
Locking devices, identification media and authorisations are saved in the locking plan (also see *Identification media, locking devices and the locking plan* [▶ 512]).



The locking plan becomes a locking system with further organisational components:

- Areas [▶ 548]

- [Person groups \[▶ 544\]](#)
- [Authorisation groups \[▶ 543\]](#)
- [Time groups and schedules \[▶ 528\]](#)
- [Time switchovers \[▶ 532\]](#)
- [Hashtags \[▶ 549\]](#)



### A number of locking systems in the same project

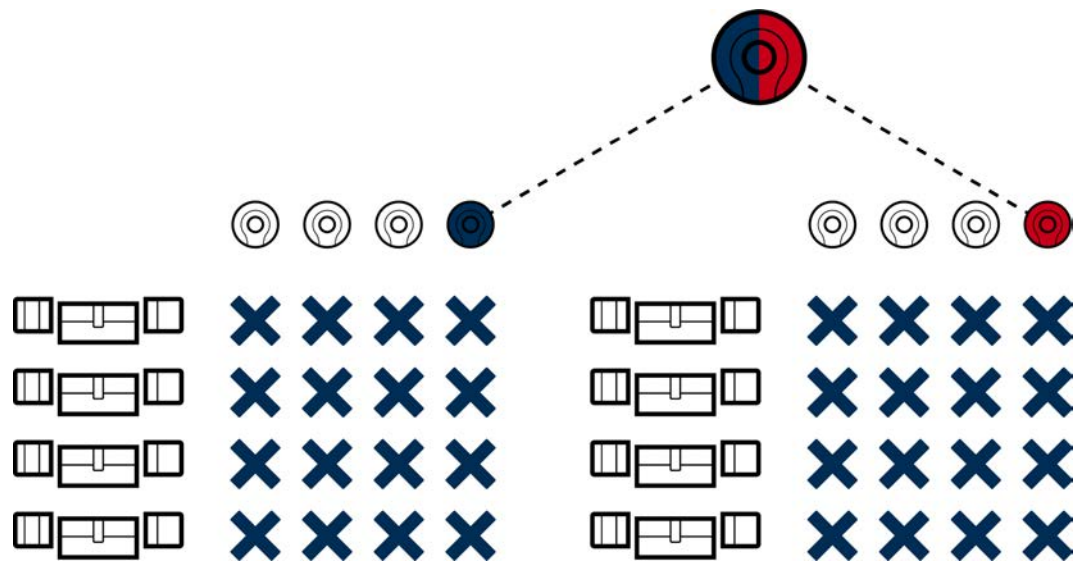
At times it may make sense to work with more than one locking system. You might wish to manage two companies in the same building in your AXM Plus and want a stricter separation on an organisational level.

In this case, you can set up an own locking system for the second company. This will give you better separation between the two companies.

You can even use the same identification medium in several locking systems (see [Use identification media in multiple locking systems \[▶ 199\]](#)).

As a basic rule, several locking systems are possible depending on the identification medium. The locking systems are completely independent of each other and do not have an influence on one another.

One transponder to rule them all:



### 22.3 Common locking levels

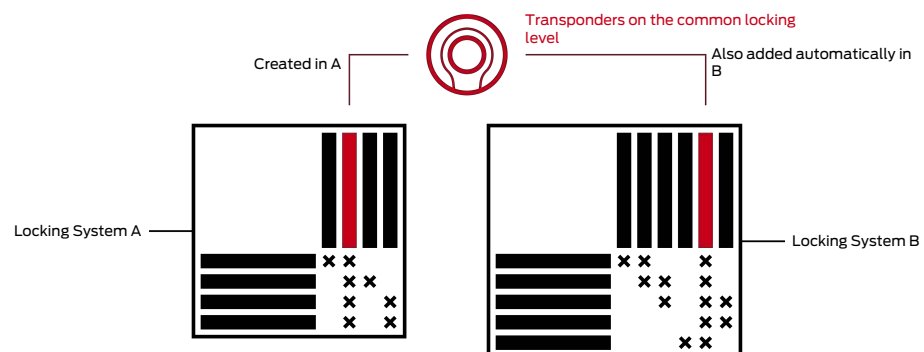
Common locking levels allow you to authorise identification media on locking devices from many different locking systems.

#### Advantage

For example, you may have an industrial site that consists of multiple parts with many buildings. A fire service key tube with a fire service transponder needs to be left at the main gate for the fire service. You also want to manage the individual parts with your own locking system. If you then have too many locking systems, you will no longer be able to write them all on the fire service transponder.

The concept of the common locking levels helps you in such a case.

#### Function



First, create your locking systems with identification media and locking devices as usual.

Then create a common locking level, e.g. a red one. You then assign locking systems to this common locking level.

You create a transponder in one of these locking systems and activate the common locking level for this transponder. This means that the AXM Plus creates the transponder in all locking systems that you have assigned to this common locking level.

You then assign your authorisations within the locking system concerned as usual.

### Requirements and notes

- Multiple colours are available for the common locking levels: Red, Blue and Green.

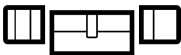
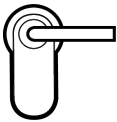
SimonsVoss recommends using the red common locking level for emergency purposes only (fire service, rescue services, etc.).

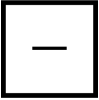
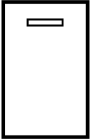
Transponders on the red common locking level are also able to operate disabled locking devices.

- You can choose the password for the common locking level freely; it does not need to be identical to the locking system passwords.
- Passive identification media (e.g. cards) cannot be used in a common locking level.

## 22.4 “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.

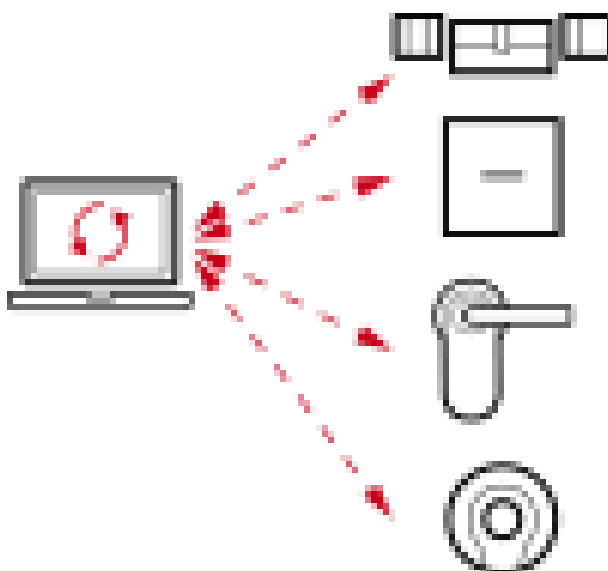
Locking device	Response	User action
SmartRelays 	Switching: The relay contact in SmartRelay switches. Depending on the SmartRelay, this is a make contact or a changeover contact. Connected electrical doors now open.	No further action required. The door is generally already open.
SmartLocker AX 	Retract 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.

### 22.5 Synchronisation of database and actual state



Everything you change in AXM Plus 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* [▶ 398]). 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**

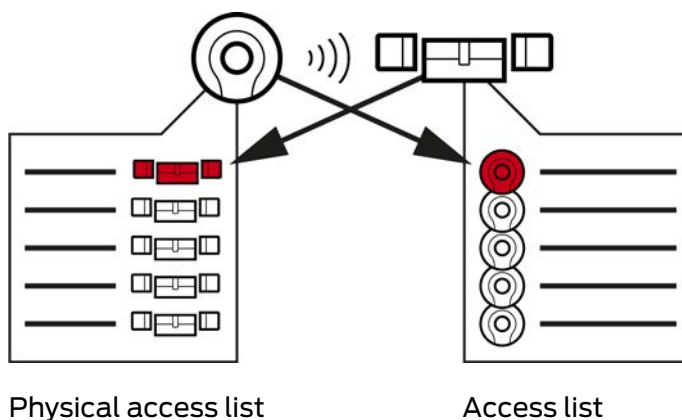
If you edit the locking system with the AXM Plus, the changes are initially only saved to your database.

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* [▶ 41]).
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* [▶ 398]).

The AX2Go is a special case due to the cloud connection; see *Synchronisation of AX2Go keys via the cloud* [▶ 518].

## 22.6 Access and physical access lists



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)* [▶ 399]
- *Synchronise a card/transponder (including importing physical access list)* [▶ 410]

You can then view both lists:

- [Displaying and exporting a locking device's access list \[▶ 491\]](#)
- [Displaying and exporting physical access lists for cards/transponders \[▶ 493\]](#)

## 22.7 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* [▶ 528])
- Automatically engage locking devices (*Time switchovers* [▶ 532])



### 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.

### 22.7.1 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:

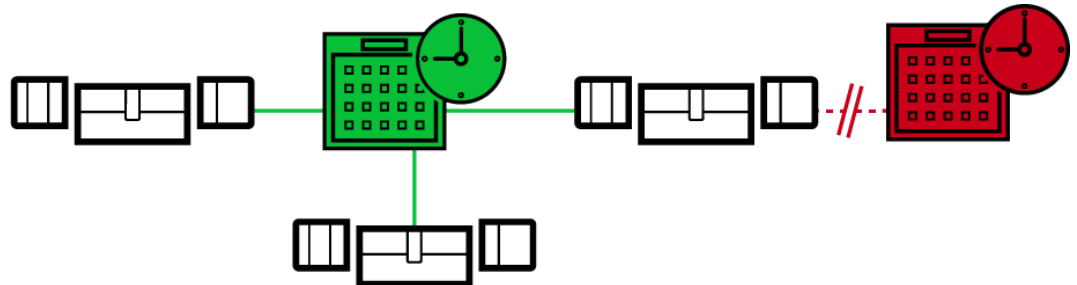
Considerations for:	Main entrance	Laboratory
<b>Employee</b>	Your employee may enter the building during the entire flexitime period and also between 7:00 to 22:00 hours on weekends.	Your employee may enter the laboratory during the entire flexitime and also between 7:00 to 22:00 hours on weekends.
<b>Intern</b>	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).
<b>Cleaner</b>	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:

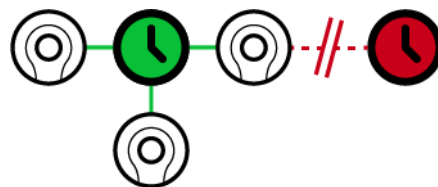
- Two schedules for doors or locking devices:
  - "Main entrance" schedule
  - "Laboratory" schedule
- Three time groups for the people in the company:
  - "Employee" time group
  - "Intern" time group
  - "Cleaner" time group

**New schedule or new time group?**

- There is one schedule per locking device, but any number of locking devices can be assigned per schedule.



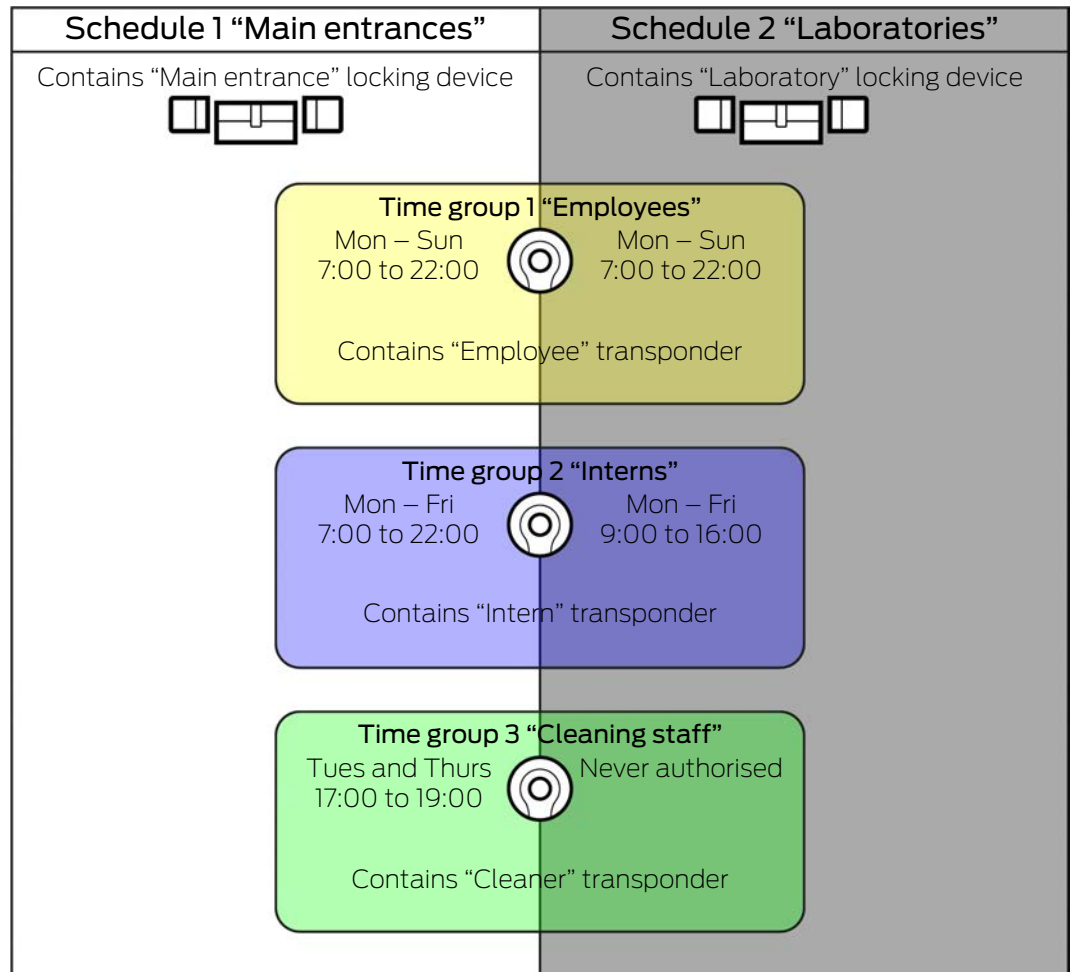
- One time group per identification medium, but any number of identification media can be assigned per time group.



- 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
<p>If the same identification medium needs to be able to enter using two locking devices at different times.</p> <p>As you can only assign one time group to each identification medium, you assign a separate schedule to the locking devices in this case.</p> <p>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.</p>	<p>If two identification media are to be able to enter using the same locking device at different times.</p> <p>As you can only assign one schedule per locking device, you assign a separate time group to the identification media in this case.</p> <p>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.</p>

Schematic diagram



	Main entrance	Laboratory
Employee	<ul style="list-style-type: none"> <li>❑ Your employee's transponder: "Employees" time group</li> <li>❑ Main entrance locking device: "Main entrances" schedule</li> <li>❑ "Employees" time group authorised in "Main entrances" schedule between 7:00 to 22:00 daily</li> </ul> <p>Your employee can enter the main entrance between 7:00 to 22:00 hours daily.</p>	<ul style="list-style-type: none"> <li>❑ Your employee's transponder: "Employees" time group</li> <li>❑ Laboratory locking device: "Laboratories" schedule</li> <li>❑ "Employees" time group authorised in "Laboratories" schedule between 7:00 to 22:00 daily</li> </ul> <p>Your employee can enter the laboratory between 7:00 to 22:00 hours daily.</p>

	Main entrance	Laboratory
Intern	<ul style="list-style-type: none"> <li>■ Your intern's transponder: "Interns" time group</li> <li>■ Main entrance locking device: "Main entrances" schedule</li> <li>■ "Interns" time group authorised in the "Main entrances" schedule between 7:00 to 22:00 on working days</li> </ul> <p>Your intern can enter the main entrance between 7:00 to 22:00 on working days.</p>	<ul style="list-style-type: none"> <li>■ Your intern's transponder: "Interns" time group</li> <li>■ Laboratory locking device: "Laboratories" schedule</li> <li>■ "Interns" time group authorised in "Laboratories" schedule between 9:00 to 16:00 on working days</li> </ul> <p>Your intern can enter the laboratory between 9:00 to 16:00 on working days.</p>
Cleaner	<ul style="list-style-type: none"> <li>■ Transponders for your cleaner: "Cleaning staff" time group</li> <li>■ Main entrance locking device: "Main entrances" schedule</li> <li>■ "Cleaning staff" time group authorised in the "Main entrances" schedule between 17:00 to 19:00 on working days</li> </ul> <p>Your cleaner can enter the main entrance between 17:00 to 19:00 on Tuesdays and Thursdays.</p>	<ul style="list-style-type: none"> <li>■ Transponders for your cleaner: "Cleaning staff" time group</li> <li>■ Main entrance locking device: "Laboratories" schedule</li> <li>■ "Cleaning staff" time group never authorised in the "Laboratories" schedule</li> </ul> <p>Your cleaner can never enter the laboratory.</p>

### 22.7.2 Time switchovers

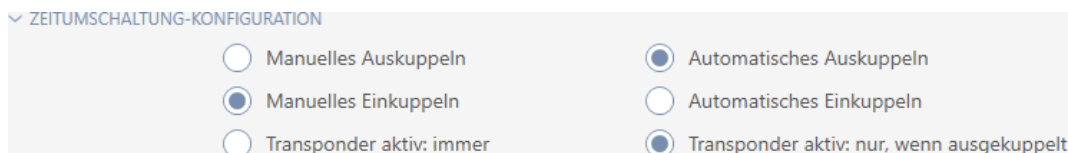
You can automatically engage and disengage your locking devices with time switchovers.

1. To do this, specify days and time intervals in a time switchover (see *Creating a time switchover* [▶ 65]).
2. Then add the locking devices you require to this time switchover (see *Engaging and disengaging locking devices automatically with time switchover* [▶ 278]).
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* [▶ 278]).

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* [▶ 286] 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* [▶ 286] 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.

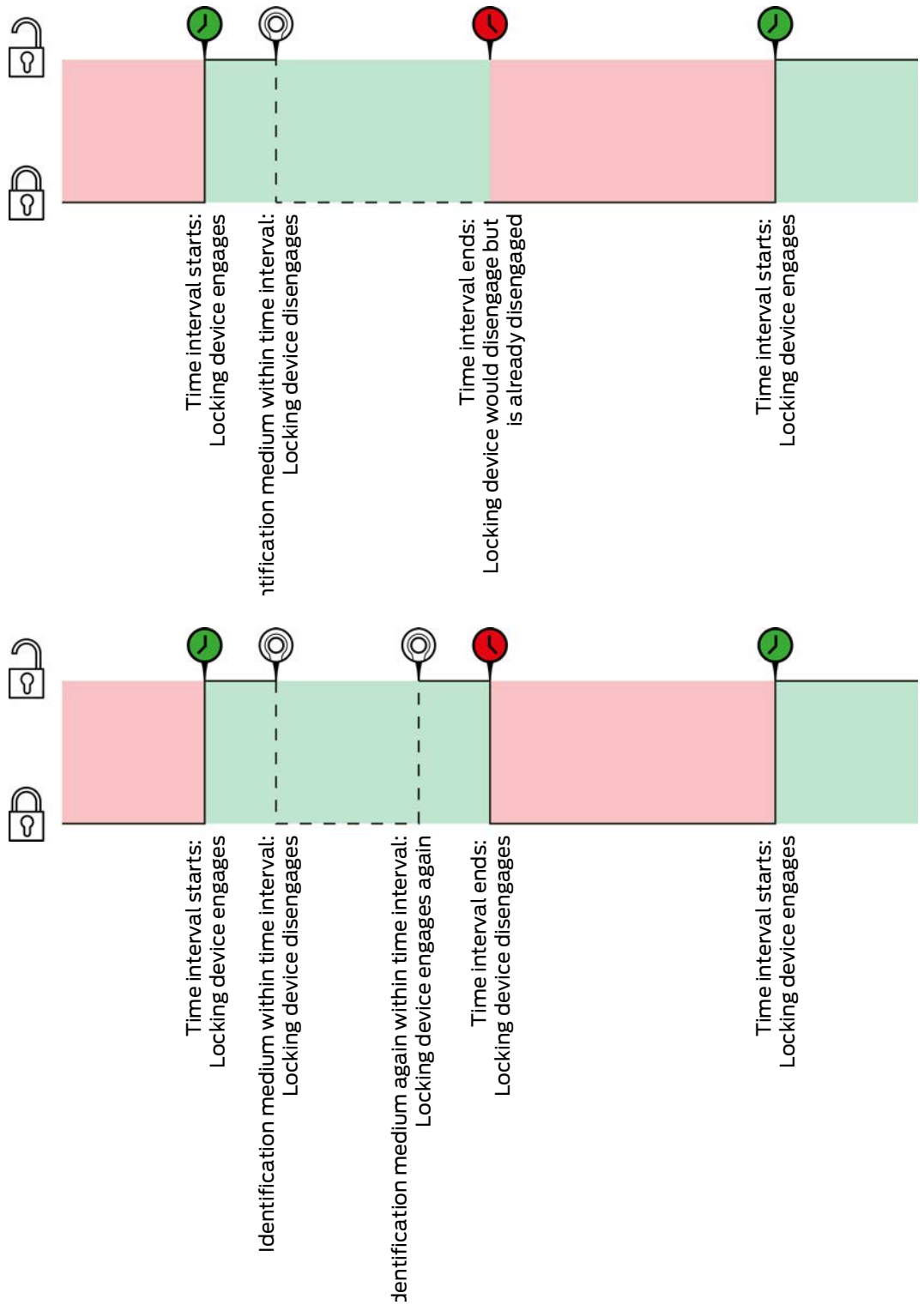
You can also disengage the locking device during the time interval using an authorised identification medium (exception:  Transponder aktiv: Nur, wenn ausgekuppelt option activated).

Locking device then remains disengaged until:

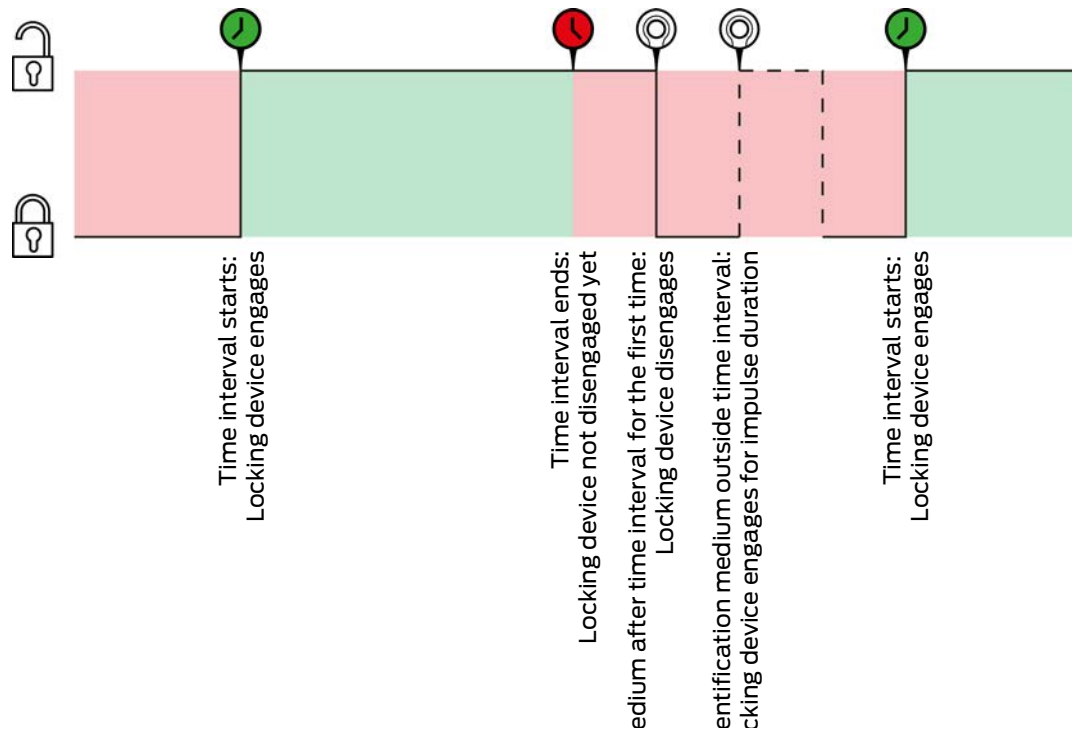
- You press an identification medium again during the same time interval: Locking device engages again, time switchover continues as usual.




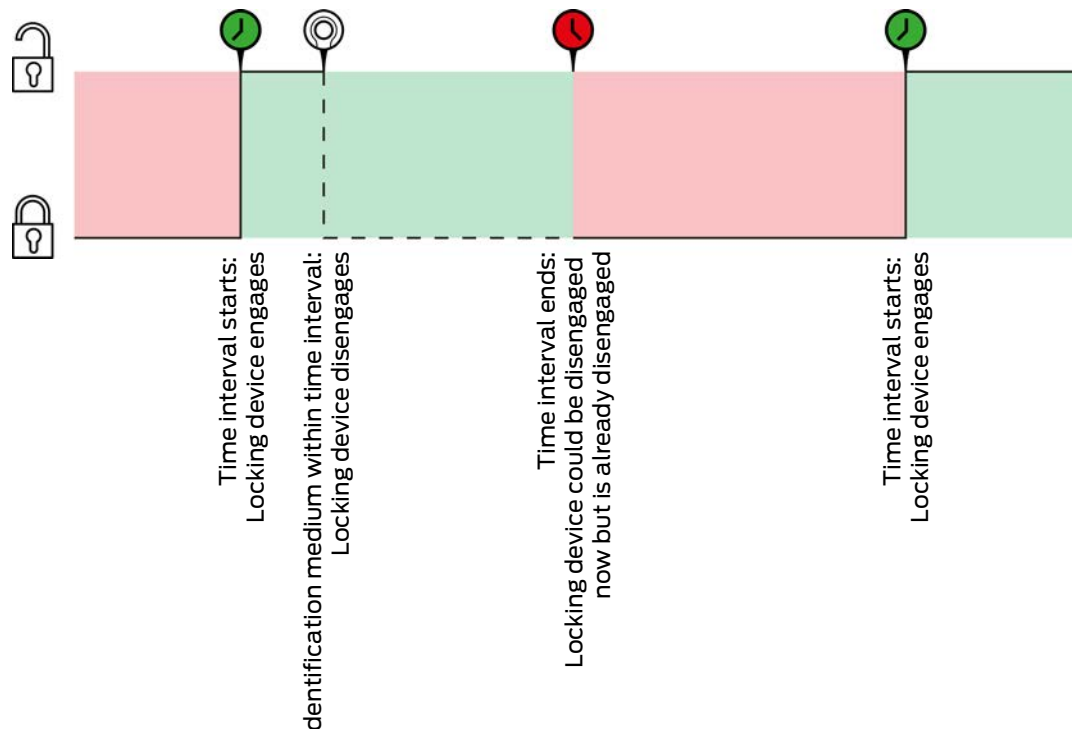
The  Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.



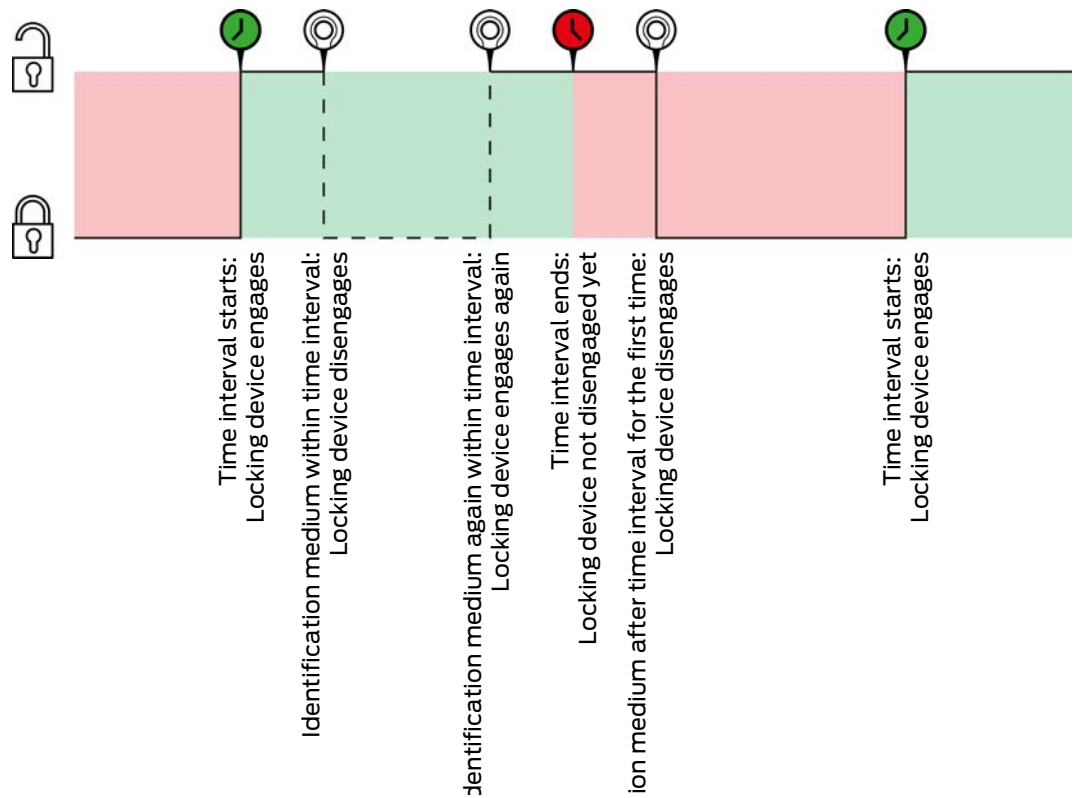
Automatisches Einkuppeln, Manuelles Auskuppeln



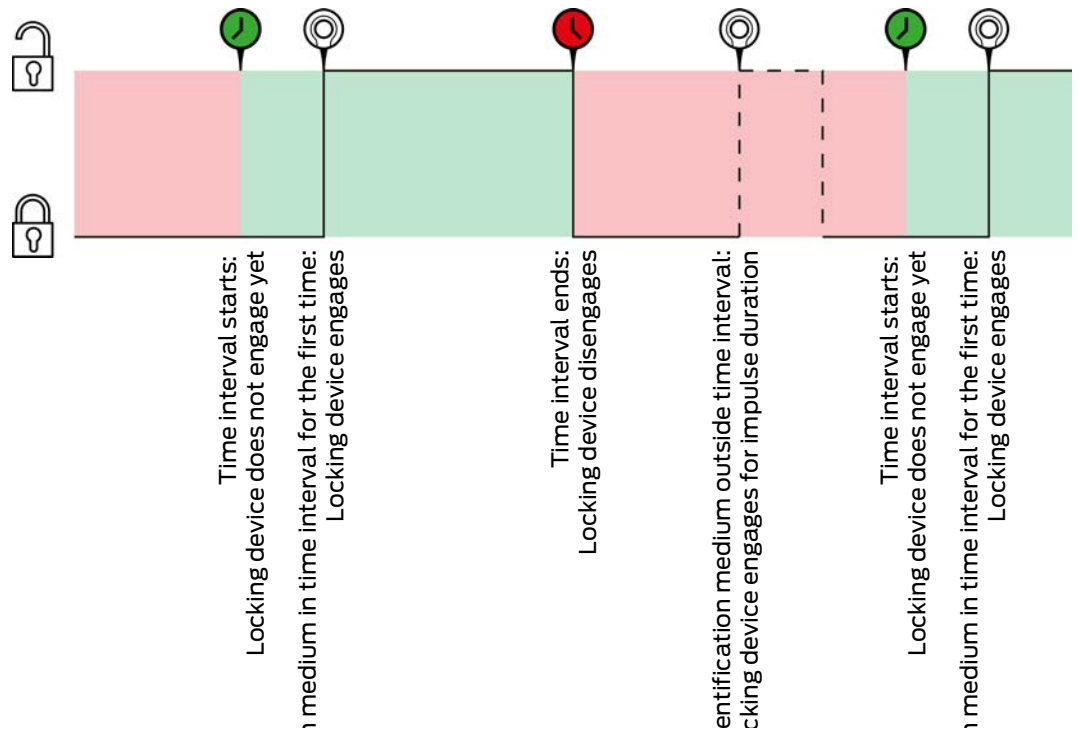
The  Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.




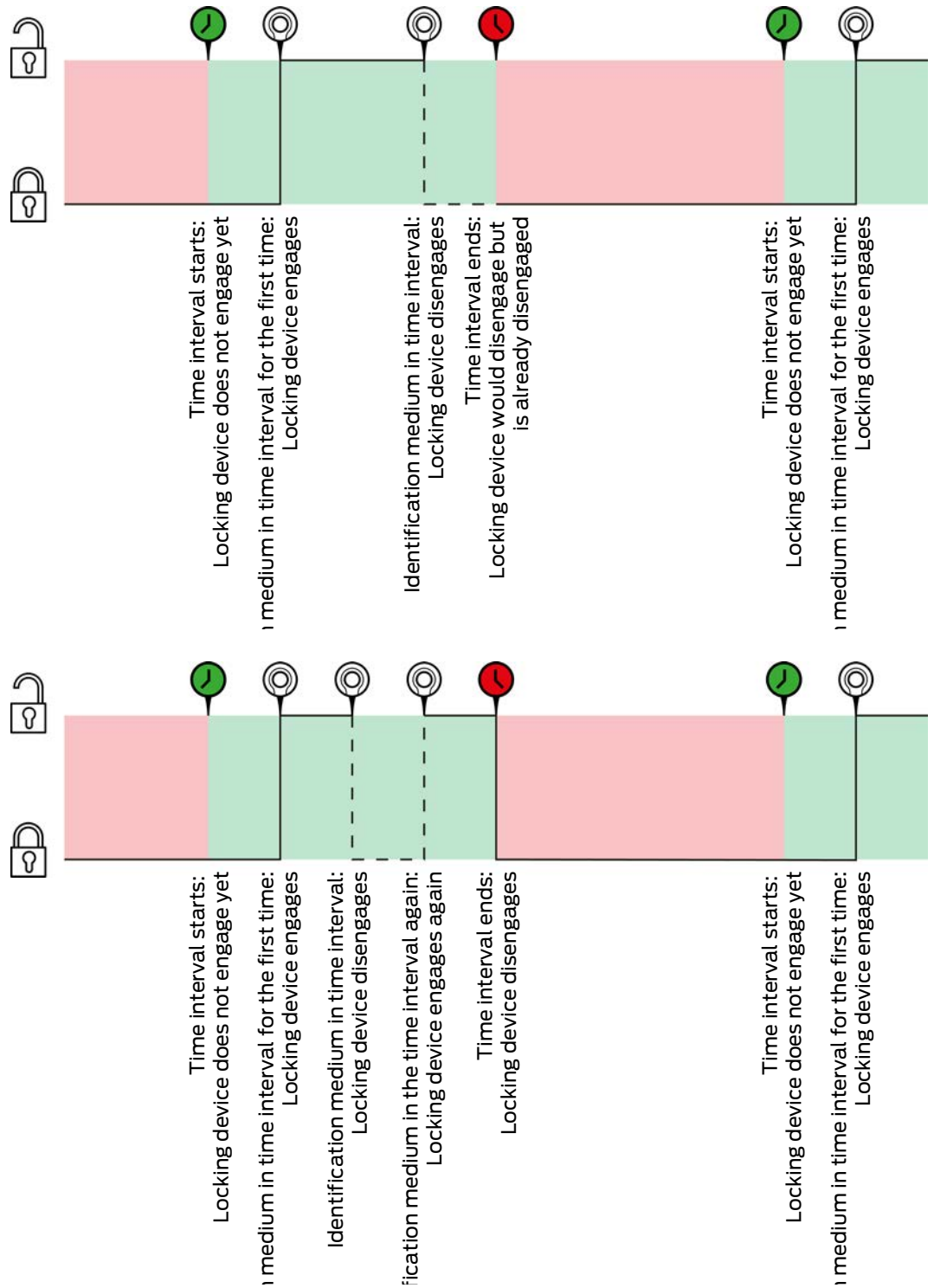




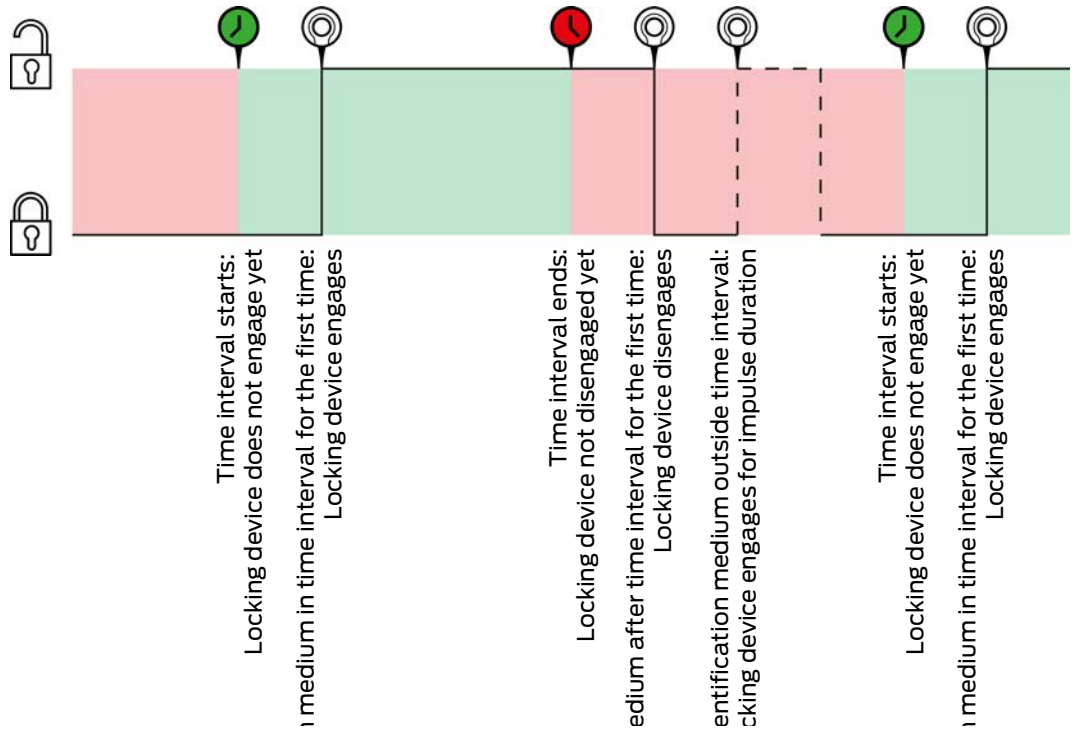
Manuelles Einkuppeln, Automatisches Auskuppeln



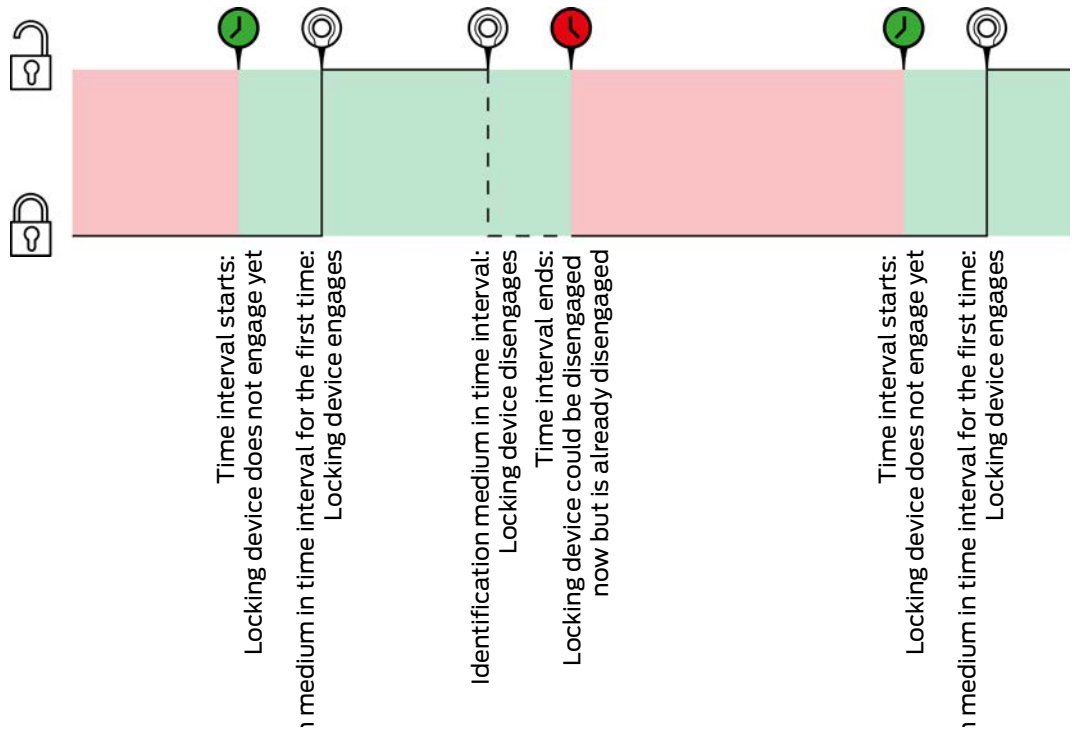
The  Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

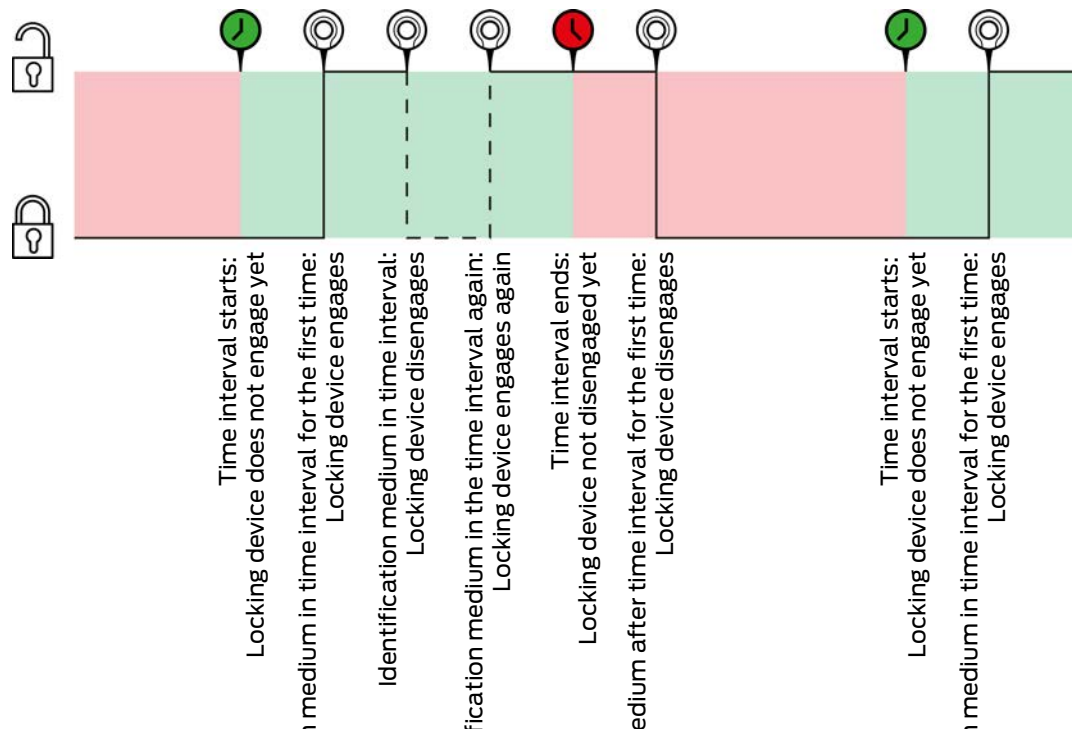


Manuelles Einkuppeln, Manuelles Auskuppeln



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.





### 22.7.3 Time budget (AX2Go and virtual network)

The term “time budget” occurs in two different contexts:

- AX2Go: Offline time budget (in days)
- Virtual network: Dynamic time window

Both means that an identification medium can only be used for a limited time before the time budget needs to be topped up again. When reloading, the system checks whether authorisation changes have been made or whether the identification medium has even been blocked.

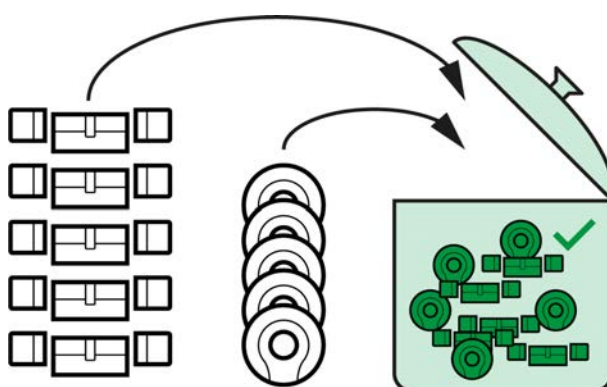
	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Adjustability	<ul style="list-style-type: none"> <li>■ Max. 30 days since last top-up</li> <li>■ Adjustable to the exact day</li> </ul>	<ul style="list-style-type: none"> <li>■ Max. 120 hours (=5 days) or</li> <li>■ Up to a given time after top-up (e.g. until 8 p.m. after top-up)</li> <li>■ Adjustable to the exact hour</li> </ul>
Top-up of	<p>AXM service.</p> <p>As soon as the AX2Go and the AXM service both access the cloud and thus see each other, the time budget is fully topped up again.</p>	<p>Virtual network gateways</p>

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Top-up frequency	<p>With a few exceptions, the smartphone with the AX2Go is permanently connected to the Internet and thus to the cloud. This means that the time budget is fully topped up each time the AXM service connects to the cloud.</p> <p>The AXM service connects to the cloud immediately in the event of important changes (e.g. changes to authorisations); otherwise, it connects about twice a day.</p>	<p>The time budget is topped up whenever the identification medium is presented to the gateway and it has not been blocked.</p>
Purpose	<p>A smartphone could be set to flight mode and thus the connection to the AXM service could be intentionally interrupted. In this case, an authorisation change would never reach the AX2Go.</p> <p>“Offline time budget (in days)” forces all AX2Go users to allow a connection between the AX2Go and AXM service on a regular basis. This prevents flight mode from being misused and inadvertently use a permission permanently.</p>	<p>In the virtual network, “Dynamic time window” performs two tasks:</p> <ol style="list-style-type: none"> <li>1. Forcing identification media to go to gateway</li> <li>2. Time limitation of authorisation in the event of lost identification media</li> </ol> <p>In the virtual network, data is transported from the gateway to the locking devices and back again using identification media. The more often the identification media are presented to the gateway, the more effectively data exchange works. With a limited time budget, you can ensure that all users go to the gateway on a regular basis.</p> <p>Moreover, a stolen identification medium cannot be used for longer than the configured time budget after it is blocked. It is irrelevant whether the block was applied to the locking devices. The stolen identification medium’s time budget can no longer be renewed and thus expires.</p>

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
<p>Example (normal operation)</p>	<p>Example: time budget set to 30 days.</p> <p>A user's AX2Go connects to the AXM service via the cloud. Since the user is still authorised, the time budget is renewed to the full 30 days.</p> <p>The locking system administrator closes their laptop and goes on vacation for three weeks.</p> <p>However, since the user's AX2Go has a time budget of 30 days, the AX2Go can be used without problems during the locking system administrator's entire vacation leave.</p> <p>After the locking system administrator returns, they restart their laptop. The AXM service connects to the cloud and the user's time budget is renewed.</p> <p>The user's AX2Go functions uninterrupted at all times.</p>	<p>Example: 8-hour time budget configured.</p> <p>A user presents their identification medium on the gateway. The gateway connects to the database and determines that the identification medium has not been blocked and renews the time budget.</p> <p>The user can then use their identification medium for 8 hours.</p> <p>They then activate their identification medium again at the gateway and receive a new time budget.</p>

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Example (problem)	<p>Example: time budget set to 7 days.</p> <p>An authorisation is withdrawn from a AX2Go user. However, since the user knows that this authorisation is to be revoked and they want to operate the locking device at a later stage without being detected, they activate flight mode to prevent authorisation from being revoked.</p> <p>The AX2Go can no longer establish a connection to the cloud, so the time budget of the user concerned is no longer renewed.</p> <p>After the 7 days have elapsed, the user can no longer operate a locking device with their AX2Go and is forced to allow an online connection. This means that the revoked authorisation also reaches its AX2Go.</p>	<p>Example: 8-hour time budget configured.</p> <p>An identification medium is reported as stolen and is subsequently blocked by the locking system administrator. Over time, the block IDs are distributed to the locking devices in the virtual network. However, some remote locking devices have not yet received a block ID eight hours after the block.</p> <p>However, the stolen identification medium can no longer be used on these locking devices. The time budget has expired and will no longer be renewed due to the block.</p>

## 22.8 Authorisation groups



Authorisation groups are available for the first time with the introduction of AXM Plus.

The principle of an authorisation group is very simple, similar to a melting pot. Within an authorisation group, all locking devices are normally authorised on all identification media.

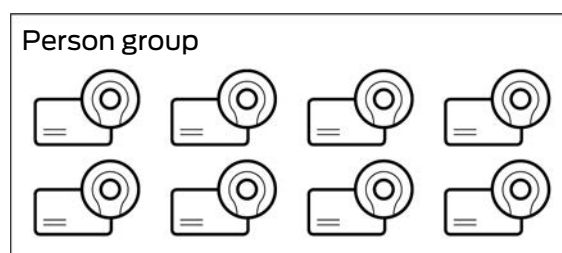
We say “normally” because you can also manually remove authorisations from individual identification media. This gives you full freedom to decide on authorisations, but you can do most of the work in an authorisation group.

Identification media and locking devices can be assigned to a number of authorisation groups.

Authorisation groups are an organisational component. Ideally, you should set up your authorisation groups before your locking devices and identification media (see *Best practice: setting up the locking system* [▶ 27] and *Creating authorisation groups* [▶ 50]).

## 22.9 Person groups

Person groups are an organizational unit. You can also use a group of persons (or their identification media) that belong together in AXM Plus .



Departments are the typical example of where person groups are used. It is highly probable that all employees within a department will receive the same authorisations (e.g. every mechanic should be able to operate all locking devices in the workshop). Instead of assigning the necessary authorisations to each identification medium individually: Bring the identification media together into a person group and authorise the entire person group at the same time.

Person groups also offer other advantages:

- Filtering by identification media which are part of a person group
- Authorising entire person groups (see *Adding areas and person groups to authorisation groups* [▶ 331])
- Matrix structure
- Moving identification media to another person group at a later date (see *Assigning persons to person groups* [▶ 193])

Person groups are an organisational component. Ideally, you should set up your person groups before the identification media (see *Best practice: setting up the locking system* [▶ 27] and *Creating a person group* [▶ 51]).



**NOTE****Maximum one person group per identification medium**

An identification medium can only belong to one single person group. Persons belonging to several departments do not exist in AXM Plus. If you assign a different person group to an identification medium, this identification medium is automatically removed from their previous person group.

- You can use the Person group column in the "Person group" window to check whether an identification medium has already been assigned to a person group.

**Matrix without person groups**

Person	Typ	Sync
Standard Personengruppe		
Granger, Hermine		
Hagrid, Rubeus		
Lovegood, Luna		
McGonagall, Min...		
Weasley, Percy		


Matrix with person groups

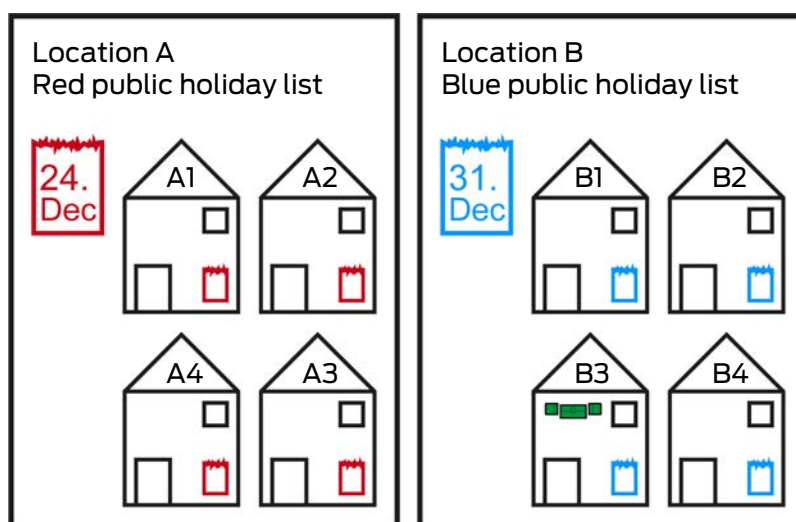
Sync	Typ	Person
	Grangers	
		Granger, Hermine
	Weasleys	
		Weasley, Percy
	Standard Personengruppe	
		Hagrid, Rubeus
		Lovegood, Luna
		McGonagall, Min...


22.10 Passwords used

- User password: Protects your AXM Plus 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 Plus against outdated locking system statuses being restored.

## 22.11 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 Plus 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* [▶ 27]) (see *Creating a location* [▶ 77] and *Creating a building and assigning it to a location* [▶ 80]).

### 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).

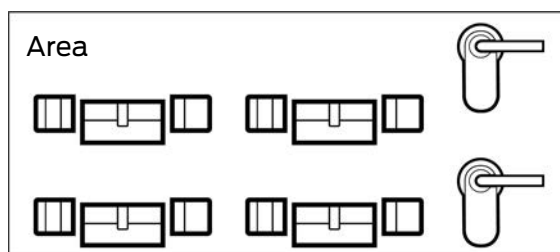
The public holiday lists are particularly interesting for time-controlled locking devices. Locking devices are conveniently always assigned to a building, which in turn is assigned to a location (mandatory information). Assigning a public holiday list to each locking device is a laborious task. Instead, 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)* [▶ 276]). 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.

## 22.12 Areas

Areas are an organisational unit for your locking devices. You can also use an area to combine locking devices which belong together in AXM Plus.



Rooms and spaces such as an entrance area are a typical example of where areas are used. An entrance area can contain a number of doors and locking devices. In this case, it would be practical if you did not have to “touch” each of these locking devices when working on your locking system. The use of areas allows you to do just that and provides additional comfort functions:

- Authorising several locking devices at once
- Filtering by locking devices which form part of an area
- Matrix structure
- Authorisations for entire areas (see *Adding areas and person groups to authorisation groups* [▶ 331])
- Moving a locking device to another area at a later date (see *Moving locking devices to areas* [▶ 270])
- Assigning a schedule to an entire area instead of individual locking devices (see *Add area, including locking devices, to a schedule* [▶ 345])

Areas are an organisational component. Ideally, you should set up your areas before the identification media (see *Best practice: setting up the locking system* [▶ 27] and *Creating an area* [▶ 83]).

**NOTE****Maximum one area per locking device**

A locking device can only belong to one single area. There are no overlapping areas in the AXM Plus. If you assign a different area to a locking device, this locking device may be automatically removed from its existing area.

- You can use the Area - Details column in the "Area - Details" window to check whether a locking device has already been assigned to an area.

**Matrix without areas**

Tür	Typ	Sync
Gryffindor dormit...	⊖	
Hagrid's hut	⊖	
Hufflepuff tower	⊖	
Stadium illuminati...	⊖	

**Matrix with areas**

Tür	Typ	Sync
Castle		
Gryffindor dormit...	⊖	
Hufflepuff tower	⊖	
Lands		
Hagrid's hut	⊖	
Stadium illuminati...	⊖	

**22.13 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

**22.14 DoorMonitoring**

DoorMonitoring is an additional feature for recording door statuses and displaying them in your AXM Plus.

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.

**22.14.1 Possible DoorMonitoring states of locking cylinders**

- Door open/closed
- Door locked
- Door securely locked
- Door open for too long
- Forend screw manipulated

**22.14.2 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

**22.14.3 Possible DoorMonitoring states of SmartRelais 3**

- Input 1 active/inactive
- Input 2 active/inactive
- Input 3 active/inactive
- Sabotage detection

## 22.15 Reports

### 22.15.1 Scaling image files

AXM Plus allows you to personalise your reports with your own image files in the header and footer (see *Personalising reports and exports* [▶ 445]).

You can insert your own logo here, for example.

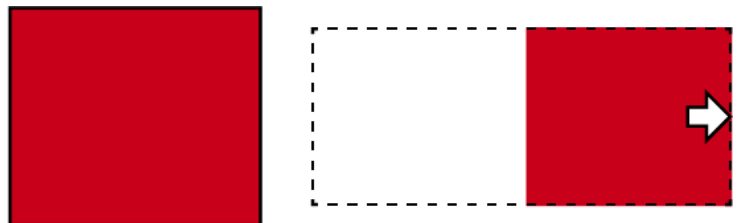
You can freely select the image file. A specific box is provided for your image files in exported reports. AXM Plus automatically scales your images to fit into the box:

#### Image too narrow and too low



The image is enlarged in proportion and aligned to the right in the box.

#### Image too high



The image is made smaller in proportion and aligned to the right in the box.

#### Image too wide



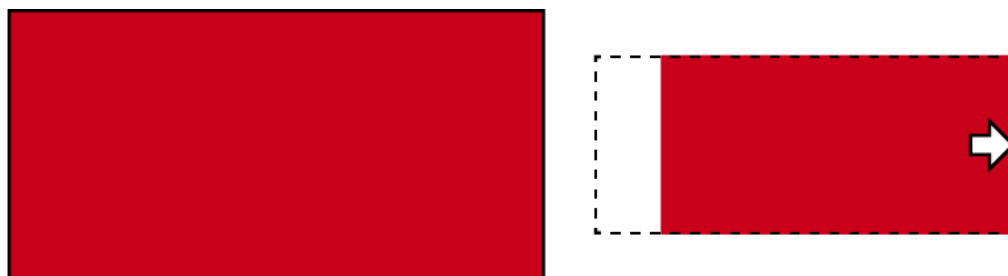
The image is made smaller in proportion and aligned with the bottom of the box.

### Image too high and much too wide



The image is made smaller in proportion and aligned with the bottom of the box.

### Image too wide and much too high



The image is made smaller in proportion and aligned to the right in the box.

## 22.16 Cards and locking device IDs

“Cards” in this document refer to all types of passive identification media.

Cards offer advantages such as:

- No need for battery replacement
- Printable

Cards also have drawbacks, however:

- Short range (a few millimetres)
- Less memory space

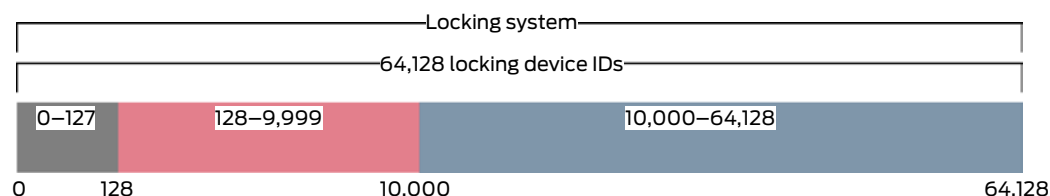
It is especially important to take the small memory space into account.

### Distribution of locking device IDs in AXM Plus

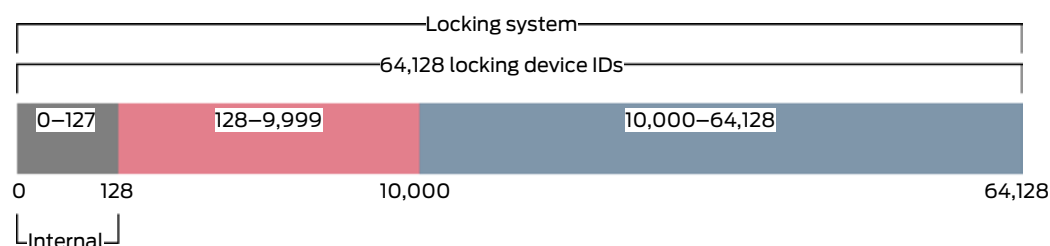
As a basic rule, each row in the column with locking devices receives its own LID (lock ID). A locking device can also use several locking device IDs – for example, if there are two separate reader thumb-turns on the free-turning Digital Cylinder AX. In this case, a locking device ID is used for each reader thumb-turn.

There are 64,128 locking device IDs (0 to 64,128) in an active locking system.

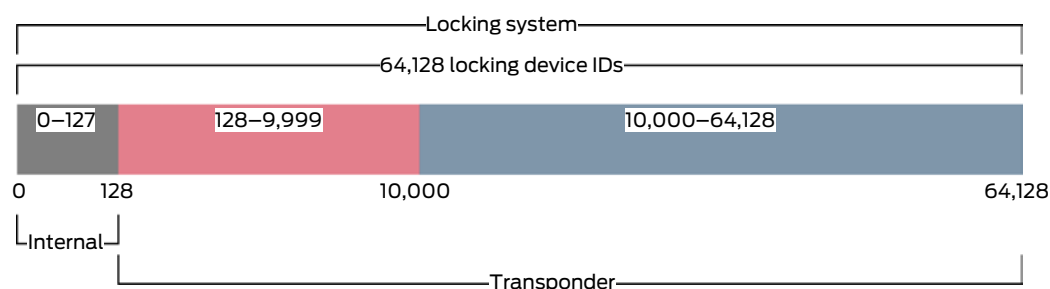




The first 128 locking device IDs (0 to 127) are reserved for internal purposes and cannot be used.



You can use the locking device IDs 128 to 64,128 with a transponder. You can manage 64,000 locking devices in just one locking system with a single transponder.



This is different for cards. Standard cards have far less memory space than a transponder. You must take this into account when configuring the card (see *Card templates* [▶ 556] and *Adding a card configuration* [▶ 354]). What's more, the size of your cards also plays a role in the number of locking devices that you can actually manage with your cards.

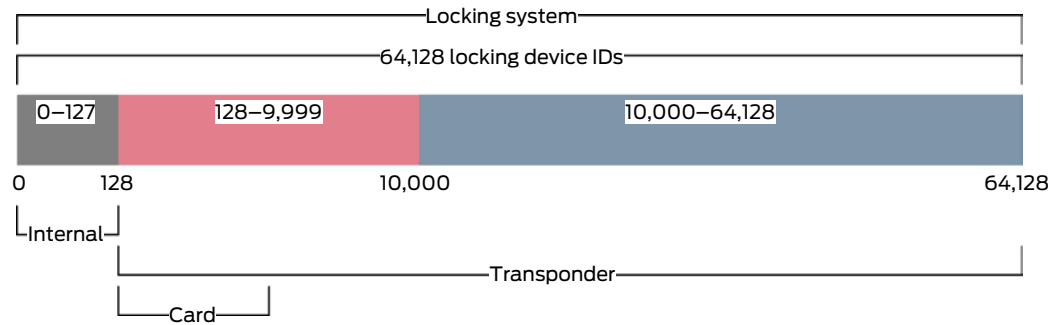
Cards can only be used in conjunction with a card template. Card templates differ in a number of characteristics but the most important ones are quite clear:

- Memory requirements
- Locking device ID section

Memory requirements and the locking device ID section are interlinked: The more locking device IDs you write on the card, the greater the memory you require is. Example: The MC8000L\_AV template can manage eight times more locking devices, but it also requires four times as much memory on the card:

MC1000L_AV	MC8000L_AV
Kartentyp <u>Mifare Classic</u>	Kartentyp <u>Mifare Classic</u>
Konfiguration <u>MC1000L_AV</u>	Konfiguration <u>MC8000L_AV</u>
Speicherbedarf <u>528 Bytes</u>	Speicherbedarf <u>2048 Bytes</u>
Schließungs-IDs <u>128 - 1127 im Kartenprofil</u>	Schließungs-IDs <u>128 - 8127 im Kartenprofil</u>
Begehungen im Protokoll <u>19</u>	Begehungen im Protokoll <u>125</u>
Virtuelles Netzwerk <u>OK</u>	Virtuelles Netzwerk <u>OK</u>
<ul style="list-style-type: none"> <li>■ 528 bytes</li> <li>■ Locking device IDs 128 to 1127 (= 1000 entries)</li> </ul>	<ul style="list-style-type: none"> <li>■ 2048 bytes</li> <li>■ Locking device IDs 128 to 8127 (= 8000 entries)</li> </ul>

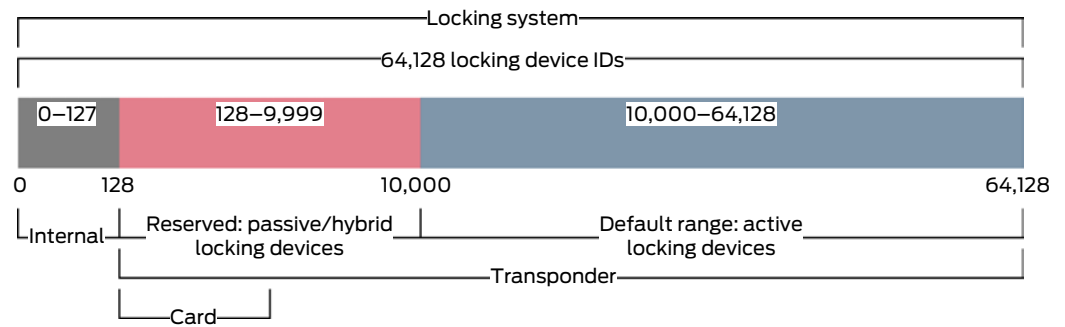
It is evident that cards in the entire range for locking device IDs can only address the lower locking device IDs in the lower section.



These low locking device IDs are therefore particularly “useful”. Active locking devices are not suitable in the lower range – they cannot communicate with cards anyway, so it makes no sense if they are assigned the “useful” low locking device IDs.



Your AXM Plus allows for this. Active locking devices are generally only created with locking device ID 10,000 and onwards. Locking device IDs 128 to 9,999 are thus reserved for passive and hybrid locking devices – regardless of whether you even use cards or not.



In large locking systems, it is of course possible that the separate ranges become too small. In such cases, AXM Plus will take number outside the designated range:

“Too many” passive/hybrid locking devices	“Too many” active locking devices
<p>If you assign passive or hybrid locking devices to all locking device IDs from 128 to 9999, the “reserved” range is allocated. Newly created locking devices are then treated equally and receive the next higher free locking device ID – regardless of whether they are active or passive.</p> <p>As soon as a locking device ID is free in the lower range once more (e.g. locking device reset; see <a href="#">Reset [▶ 264]</a>), it is exclusively assigned a passive or hybrid locking device again.</p>	<p>If all locking device IDs from 10,000 to 64,128 are issued, AXM Plus will also assign active locking devices to these useful locking device IDs in the lower range.</p> <p>As soon as a locking device ID is free in the upper range once more (e.g. locking device reset; see <a href="#">Reset [▶ 264]</a>), it is exclusively assigned an active locking device again.</p>

### Locking device IDs in the [Locks] tab

You can also see the distribution in the "Lock ID" column in the [Locks] tab.

In this example, the first two locking devices are hybrid locking devices and assigned a locking device ID in the useful range (128 and 129). The last two locking devices are active locking devices and are therefore assigned a locking device ID numbered 10,000 and upwards (10,000 and 10,001).

Schließungen x										
Hogwarts 1										
Tür	^	▼	Raumnummer	Etage	Typ	Sync	Status	Letzte Synchronisierung	S/N	Schließungs ID
>	Gryffindor dormitory				🔑			12.01.2022 16:36:15	000C1957	129
	Hagrid's hut				🔑			14.12.2021 16:57:42	000D5P7E	128
	Hufflepuff tower				🔑			14.12.2021 16:58:30	000E04GX	10000
	Stadium illumination				🔑			14.12.2021 18:52:36	000EN84L	10001

### Your benefit with the locking device IDs concept

You can also decide to use cards at a later stage (see *Enable cards or transponders* [▶ 389]). All locking devices that you can address with the cards are located in the lower range of locking device IDs. The active locking devices that you would not be able to address with your cards anyway are outside the range of most card templates.

This means that active locking devices do not unnecessarily occupy any memory space on the cards. This means that you can actually use all locking device IDs that will fit onto your card with passive or hybrid locking devices.

#### 22.16.1 Card templates

Configuration	G1/G2	Lock IDs	Number of locking devices	Physical accesses in the log	Sectors	Memory requirements (Bytes)	Virtual Network
MCBasic	G1	-	-	-	2-15	48	-
MC1200L	G2	128-1327	1200	-	2-15	192	-
MC3800L	G2	128-3927	3800	-	2-15	528	-
MC1000L_AV	G2	128-1127	1000	19	2-15	528	√
MC_2400L_AV	G2	128-2527	2400	70	2-15 + 31-39	900	√
MC8000L_AV	G2	128-8127	8000	125	2-15 + 31-39	2048	√
MBasic	G1	-	-	-	2-15	48	-
M1200L	G2	128-1327	1200	-	2-15	192	-
M3800L	G2	128-3927	3800	-	2-15	528	-
M1000L_AV	G2	128-1127	1000	16	2-15	528	√
M4000L_AV	G2	128-4127	4000	100	2-15 + 31-39	1600	√
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	√
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	√
MDBasic	G1	-	-	-	2-15	48	-

Configuration	G1/G2	Lock IDs	Number of locking devices	Physical accesses in the log	Sectors	Memory requirements (Bytes)	Virtual Network
MD1200L	G2	128-1327	1200	-	2-15	192	-
MD3800L	G2	128-3927	3800	-	n.a. (DES-Fire)	528	-
MD2500L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	√
MD4000L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	√
MD10000L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	√
MD32000L_AV	G2	128-32127	32000	470	n.a. (DES-Fire)	7000	√
MD2400L_AV	G2	128-2527	2400	34	n.a. (DES-Fire)	830	√
MD3650L_AV	G2	128-3777	3650	2	n.a. (DES-Fire)	830	√

## 23. 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](mailto: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](http://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.

© 2024, 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**