

AXM MANAGER

The next dimension of Locking System Management

AXM Plus

Manual

03.06.2026

Contents

1.	General safety instructions	10
2.	Product-specific safety instructions	11
3.	Meaning of the text formatting	12
4.	Intended use.....	13
5.	General.....	14
6.	Information on data protection.....	15
6.1	IT basic protection	15
6.1.1	What protection requirements do the data processed in the system have?	15
6.1.2	What IT infrastructure requirements are recommended?	15
6.2	Licensing	15
6.2.1	What data is collected for licensing?	15
6.3	System-wide measures and methods in detail	15
6.3.1	Is the data in System 3060 encrypted?	15
6.3.2	What data is encrypted?	16
6.3.3	Are the transmission channels also encrypted?	16
6.3.4	How secure is end-to-end encryption?	16
6.3.5	Can key copies of identification media be created without being detected?	16
6.3.6	Can an opening signal be intercepted and repeated (replay attack)?.....	16
6.4	Communication via cloud services (e.g. AX2Go)	17
6.4.1	Will my data be stored in the cloud?	17
6.4.2	Is the pseudonymised data protected from third-party access during trans- mission?.....	17
6.4.3	How is authentication handled with SimonsVoss Cloud Services?	17
6.4.4	Where is the pseudonymised data stored on the smartphone?	17
6.5	Working in compliance with data protection regulations (GDPR).....	17
6.5.1	What personal data is stored in the software?	17
6.5.2	For what purpose is personal data stored in the software?	18
6.5.3	How long is personal data stored in the software?	18
6.5.4	Can the right to read access lists be additionally secured?	18
6.5.5	Is personal data in the software protected against access by third parties?	18
6.5.6	Can the stored data be made available as a copy?	19
6.5.7	Can personal data be deleted from the software?	19
7.	Range of functions for AXM Plus.....	20
8.	System requirements	22
8.1	AXM services and ports used	23

9. Release notes	24
9.1 Version 2.0.24303.0902	24
9.2 Version 2.0.24346.0501	24
9.3 Version 2.0.25083.0801	24
9.4 Version 2.0.25105.0001	25
9.5 Version 2.0.25105.0001 (HotFix)	25
9.6 Version 2.0.25225.0801	26
10. Installation	27
10.1 Run AXM as the administrator (recommended)	28
10.2 Updating AXM	30
10.3 Using a web proxy	31
11. First steps after a new installation	35
11.1 Best practice: setting up the locking system	37
11.2 Best practice: set up AX2Go	38
11.3 Best practice: Database protection	38
12. Registration	39
12.1 Registration as a trial version	39
12.2 Registration with licence	44
12.3 Updating your licence	49
13. The AXM's structure	51
13.1 Sorting and filtering	54
13.2 Installation wizards	56
13.3 Multiple options, same result	56
13.4 Global search	57
13.5 Working with AXM more effectively	58
13.5.1 Tab operation	58
13.5.2 Hotkeys	58
13.5.3 Creating additional objects	59
14. Organisational structure	60
14.1 Creating access levels	60
14.2 Creating a person group	61
14.3 Creating a schedule	63
14.4 Create time group	66
14.5 Deleting a time group	71
14.6 Deleting schedules	74

14.7	Creating a time switchover	75
14.8	Creating and editing public holidays.....	79
14.9	Creating and editing public holiday lists	82
14.10	Creating a location.....	87
14.11	Creating a building and assigning it to a location.....	90
14.12	Creating an area.....	93
14.13	Creating a hashtag.....	95
15.	Persons and identification media.....	98
15.1	Creating an identification medium	98
15.1.1	Creating transponders and cards.....	99
15.1.2	Creating PIN code keypads	106
15.1.3	Creating special identification media.....	111
15.1.4	Creating an AX2Go key.....	116
15.1.5	Import identification media.....	117
15.2	Duplicating an identification medium (including authorisations and settings)	122
15.3	Deleting an identification medium.....	124
15.3.1	Deleting a card/transponder	124
15.3.2	Deleting a PIN (PIN code keypad AX).....	128
15.3.3	Blocking an AX2Go key.....	130
15.4	Allowing an identification medium to open twice as long.....	130
15.5	Muting all locking devices for an identification medium.....	131
15.5.1	Muting all locking devices for a transponder or a card	132
15.5.2	Muting all locking devices for an AX2Go key	133
15.6	Allow accesses to be recorded by identification media (physical access list)	134
15.7	Restricting identification medium authorisations to specific times (time group)	135
15.8	Activating or deactivating identification medium once at specific times (activation and expiry date)	135
15.9	Handling defective identification media	139
15.9.1	Repairing/resynchronising	142
15.9.2	Resetting and replacing	147
15.9.3	Delete and replace	150
15.9.4	Take out of use and leave in project.....	158
15.9.5	Taking out of use and deleting from the project	165
15.10	Duplicating forgotten identification medium temporarily	171
15.10.1	Duplicating a forgotten transponder or card temporarily.....	171
15.11	Blocking lost/stolen identification media permanently.....	176
15.11.1	Blocking and replacing lost/stolen card/transponder permanently.....	177
15.11.2	Blocking a lost/stolen PIN code keypad permanently	182
15.12	Flag and reset returned identification medium (back to inventory)	187

15.12.1	Flagging and resetting returned card/transponder (back to inventory).....	187
15.13	Planning and tracking identification medium management tasks.....	190
15.13.1	Noting the issue date	191
15.13.2	Planning and logging battery replacement.....	194
15.13.3	Planning and logging return.....	199
15.14	Finding the identification medium or locking device again in the matrix.....	202
15.15	Exporting identification media as a list.....	202
15.15.1	Exporting AX2Go keys/cards/transponders as a list.....	202
15.15.2	Exporting PINs and PIN code keypads as a list	204
15.16	Viewing an identification medium's serial number and/or TID	206
15.16.1	Viewing a card's/transponder's serial number and TID.....	206
15.16.2	Viewing a PIN code keypad's serial number	207
15.17	Assigning persons to person groups	209
15.17.1	Assigning individual persons/identification media to a person group (in transponder window)	210
15.17.2	Assign a number of persons/identification media to person group (in the person group window)	212
15.18	Use identification media in multiple locking systems	215
15.18.1	Reuse identification medium in the same project	218
15.18.2	Reusing identification medium in other projects/databases.....	224
15.19	Managing AX2Go keys	227
15.19.1	Assigning keys for AXM Plus and higher	227
15.19.2	Revoking an AX2Go key	233
15.19.3	Deleting AX2Go keys	237
15.20	Setting the PIN length (PinCode AX)	238
15.21	Changing a PIN (PinCode AX).....	241
15.22	Set up a dynamic time window (time budget)	243
16.	Doors and locking devices	245
16.1	Creating a locking device	245
16.1.1	Importing locking devices.....	255
16.2	Duplicating the locking device (including authorisations and settings)	261
16.3	Delete locking device.....	263
16.3.1	Deleting an individual locking device using the matrix	264
16.3.2	Deleting several locking devices using the tab.....	265
16.4	Changing locking device type at later stage	268
16.5	Handling defective locking devices	270
16.5.1	Re-synchronise (repair)	275
16.5.2	Resetting and replacing.....	277
16.5.3	Delete and replace	282
16.5.4	Reset	287

16.5.5	Purge (only reset in database/software reset)	289
16.6	Assigning locking devices to buildings/locations.....	291
16.7	Moving locking devices to areas.....	293
16.7.1	Assigning individual locking devices to a different area (in the locking device window)	294
16.7.2	Assign multiple locking devices to another area (in the area window)	296
16.8	Limiting authorisations for locking devices to specific times (schedule)	299
16.9	Engaging and disengaging locking devices automatically with time switchover	301
16.10	Have accesses logged by locking device (access list)	307
16.11	Leaving the locking device open for longer, less time or permanently	309
16.12	Limit locking device read range (close range mode)	311
16.13	Muting a locking device (for battery warnings and programming)	312
16.14	Activating and deactivating card readers.....	314
16.15	Ignoring activation and expiry date of identification media	316
16.16	Changing the SmartRelay settings.....	317
16.16.1	Using internal and external antenna simultaneously	318
16.16.2	Invert outputs.....	319
16.16.3	Using the serial interface	321
16.16.4	Changing the signalling	322
16.16.5	Connect SmartRelay to network.....	323
16.17	Planning and tracking locking device management tasks.....	325
16.17.1	Note installation, replacement or removal date	326
16.17.2	Planning and logging battery replacement.....	328
16.18	Displaying all locking devices in a project.....	330
16.19	Exporting locking devices as a list.....	332
17.	Permissions	335
17.1	Changing individual authorisations (cross)	335
17.2	Changing many authorisations (on identification media and/or locking devices) ...	336
17.2.1	Allowing all or blocking all	336
17.2.2	Access levels	340
17.2.3	Controlling authorisations in terms of time (schedules).....	356
17.3	Meaning of the authorisation crosses in the matrix	366
18.	Locking systems.....	367
18.1	Create locking system.....	367
18.1.1	Adding a card configuration.....	372
18.2	Changing locking system password.....	401
18.3	Replacing the locking system.....	405
18.4	Enable cards or transponders	407

18.5	Using a common locking level	410
18.5.1	Creating a common locking level.....	410
18.5.2	Creating transponders for common locking level.....	413
18.5.3	Authorising a transponder with common locking level.....	414
19.	Synchronisation: Comparison between locking plan and reality.....	416
19.1	Synchronising the locking device (including reading access list).....	417
19.1.1	Display locking device equipment and status	420
19.1.2	Displaying and exporting a locking device's access list	422
19.2	Identifying an unknown locking device	424
19.3	Re-setting the locking device	426
19.4	Synchronising an identification medium.....	427
19.4.1	Synchronise a card/transponder (including importing physical access list)	428
19.4.2	Synchronising a PIN code keypad.....	433
19.4.3	Synchronising AX2Go key	437
19.5	Identifying an unknown ID medium.....	438
19.5.1	Recognise unknown cards/transponders.....	438
19.5.2	Identifying unknown PIN code keypad	440
19.6	Resetting identification media.....	442
19.6.1	Resetting cards/transponders.....	442
19.6.2	Resetting the PIN code keypad.....	446
19.7	Viewing connected/supported programming devices	448
19.8	Checking the connection between database and cloud.....	450
20.	Networking.....	451
20.1	CommNode set up	451
20.2	Virtual network	451
20.2.1	Configure of VNHost.....	452
20.2.2	Add Gateways	453
20.2.3	Checking virtual network	454
20.2.4	Overview of blocked IDs (VN block list)	456
20.2.5	Set up a dynamic time window (time budget)	462
20.3	WaveNet.....	463
20.3.1	Specify WaveNet channel, address and password	463
20.3.2	Add RouterNodes	465
20.3.3	Add Lock Nodes.....	468
20.3.4	Repair RouterNode or LockNode	471
20.3.5	Replace RouterNode or change IP address.....	472
20.3.6	Test RouterNode or LockNode	475
20.3.7	Reset (remove) RouterNode or LockNode	476
20.3.8	Execute tasks via WaveNet on multiple locking devices (collective orders)	478

21. Your personalised AXM interface.....	481
21.1 Interchanging (transposing) doors and persons in the matrix.....	481
21.2 Select columns and rows in the matrix (enable/disable crosshairs)	482
21.3 Click to change authorisations	483
21.4 Hiding deactivated and defective identification media	484
21.5 Showing or hiding rows/columns in the matrix.....	485
21.6 Reading access list/physical access list during synchronisation.....	487
21.7 Limiting the number of access list entries in the database	489
21.8 Pinning tabs.....	490
21.9 Changing automatic numbering	491
21.10 Changing the language.....	493
21.11 Personalising reports and exports	493
21.12 Preventing generated reports from opening automatically.....	496
21.13 Personalising properties for person details	497
21.13.1 Hide and show existing fields.....	498
21.13.2 Creating your own fields	503
22. Administrative tasks.....	513
22.1 Creating a backup	513
22.2 Restoring the backup.....	516
22.3 Migrate project (transfer).....	517
22.4 Exporting error logs.....	527
22.5 Displaying version number and licence key for the AXM installed.....	527
22.6 User management.....	529
22.6.1 Changing the user password.....	529
22.6.2 Increase password security.....	531
22.6.3 Name person as an AXM user.....	535
22.6.4 Assign tasks/user roles to AXM users	537
22.7 AX2Go settings	544
23. Statistics and logs.....	548
23.1 Displaying and exporting a locking device's access list.....	548
23.2 Displaying and exporting physical access lists for cards/transponders	550
23.3 Display doors for which a specific identification medium is authorised	552
23.4 Displaying identification media which are authorised for a specific door	553
23.5 Displaying a locking device's equipment features	554
23.6 View statistics and warnings (dashboard).....	555
23.7 Tracking activities in the database (log)	557

23.7.1	Setting the log archiving period	559
23.8	Reports and exports.....	560
23.8.1	Displaying the report for identification media issue.....	561
23.8.2	Exporting the data protection report (GDPR)	564
23.8.3	Export identification media and locking devices as a list.....	568
23.8.4	Create database report.....	569
24.	Background knowledge and explanations.....	571
24.1	Identification media, locking devices and the locking plan	571
24.1.1	PIN Code G1 vs. PIN Code AX	573
24.1.2	AX2Go.....	576
24.1.3	Special identification media and their functions.....	579
24.2	Locking systems.....	580
24.3	Common locking levels	582
24.4	“Engaging”, “opening”, “locking”, etc.....	583
24.5	Synchronisation of database and actual state.....	585
24.6	Access and physical access lists	586
24.7	Event management.....	587
24.7.1	Time groups and schedules.....	587
24.7.2	Time switchovers	591
24.7.3	Time budget (AX2Go and virtual network).....	599
24.8	Access levels	602
24.9	Person groups	603
24.10	Passwords used.....	605
24.11	Buildings and locations	606
24.12	Areas.....	607
24.13	Hashtags.....	608
24.14	Networking.....	608
24.14.1	Virtual network	608
24.14.2	WaveNet.....	618
24.14.3	CommNode and VNHost.....	621
24.15	Reports	623
24.15.1	Scaling image files.....	623
24.16	Cards and locking device IDs	624
24.16.1	Card templates	628
25.	Help and other information	630

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

Installation and initial operation require specialist knowledge.

- Only trained specialist personnel may install and put the product into operation.

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* [► 51]).
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* [► 416]).

3. Meaning of the text formatting

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

Example	button
☒ Example ☐ Example	checkbox
☒ Example	Option
[Example]	Tab
"Example"	Name of a displayed window
Example	Upper programme bar
Example	Entry in the expanded upper programme bar
Example	Context menu entry
▼ Example	Name of a drop-down menu
"Example"	Selection option in a drop-down menu
"Example"	Area
<i>Example</i>	Field
<i>Example</i>	Name of a (Windows) service
<i>Example</i>	Commands (e.g. Windows CMD commands)
Example	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 Licensing

6.2.1 What data is collected for licensing?

Our licensing model is based on device-based registration. We collect certain system data to ensure compliance with the licence terms, with the data depending on the software used and the registration method chosen. The following information is transmitted in encrypted form when registering offline by email using RGO and LIC files:

- Name of the device
- Serial number for the hard disk partition concerned (usually C partition)
- Mac address
- SID (Security Identifier) for the Windows installation

A new registration request is required if any of these parameters change.

6.3 System-wide measures and methods in detail

6.3.1 Is the data in System 3060 encrypted?

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

**NOTE****Locking system password as part of the security concept**

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

6.3.2 What data is encrypted?

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

6.3.3 Are the transmission channels also encrypted?

Thanks to consistent end-to-end encryption, our secure communication is independent of the transmission method. Intercepted data cannot be read without the appropriate secret key.

6.3.4 How secure is end-to-end encryption?

The German Federal Office for Information Security (BSI) states that only end-to-end encryption offers complete protection.

(Source https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Verschluesst-kommunizieren/verschluesst-kommunizieren_node.html)

6.3.5 Can key copies of identification media be created without being detected?

No. During initial programming, each identification medium is assigned a component-specific password in the system, which can only be used with this credential and the individual PHI (Physical Hardware Identifier). If the same data is stored on a different credential, this alters the calculated result during decryption, and the authenticity of the copied credential cannot be verified.

6.3.6 Can an opening signal be intercepted and repeated (replay attack)?

For each communication between components, an elaborately calculated random number is generated. A replay of the same message fails because the random number has already been used.

6.4 Communication via cloud services (e.g. AX2Go)

6.4.1 Will my data be stored in the cloud?

No. All current applications and extensions that need to use cloud services to function do not store any data in the cloud. Our cloud services consist purely of data in transit. Data can only be sent if the other end (secure endpoint, e.g., client to smartphone) is accessible.

All restricted-access locking system data, including personal data, is stored exclusively in the database and on the operator's secure network.

6.4.2 Is the pseudonymised data protected from third-party access during transmission?

Yes. In addition to the measures previously described (*System-wide measures and methods in detail [▶ 15]*), we use HTTPS transport encryption (TLS 1.2/1.3) in cloud communication between two secure endpoints (security block, secure element).

6.4.3 How is authentication handled with SimonsVoss Cloud Services?

To obtain secure access to our cloud services, the administrator must log in to their SV-ID account. In order to clearly prove the identity of the user, we use effective 2-factor authentication.

6.4.4 Where is the pseudonymised data stored on the smartphone?

In a smartphone, we use the Secure Element for the secure storage of all system data. The Secure Element also stores sensitive data, such as that relating to bank cards.

6.5 Working in compliance with data protection regulations (GDPR)

6.5.1 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.

6.5.2 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).

6.5.3 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.

6.5.4 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.

6.5.5 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.

6.5.6 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).

6.5.7 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	■ G2 components ■ AX components
	■ Digital Cylinder AX ■ Locking Cylinder 3061 ■ SmartHandle AX ■ SmartHandle 3062 ■ SmartRelay 3063 (G2) ■ SmartRelay 2 3063 ■ Padlock ■ Padlock AX ■ SmartLocker AX ■ Furniture lock (G2) ■ AX2Go
Programming devices	■ SmartCD.G2/SmartCD2.G2 ■ SmartCD.MP ■ SmartStick AX
Web services	■ Registration ■ AX2Go invites ■ Cloud services (data transfer only with end-to-end encryption)
Basic functions WaveNet and VN (optional)	Network programming of locking devices and identification media (only for active services)

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

Functions

- Microsoft SQL Server 2019 Express LocalDB (small local SQL server)

- Matrix view
- Transponder and locking device lists with import function
- User control: Comprehensive filtering and sorting functions, global search, hashtags
- Building structure (location, building, floor, room number)
- Authorisation groups (unlike LSM, doors and persons can be authorised in more than one group)
- Schedule control with time switching, time groups and schedules (hardware side 100+1 time groups available)
- Special transponders (battery replacement and locking device activation)
- PIN code keypads (G1 and AX)
- G2 and AX locking devices incl. SmartHandle AX Advanced and SmartRelay AX Classic
- SmartStick AX, SmartCD2.G2 and SmartCD.MP
- ...

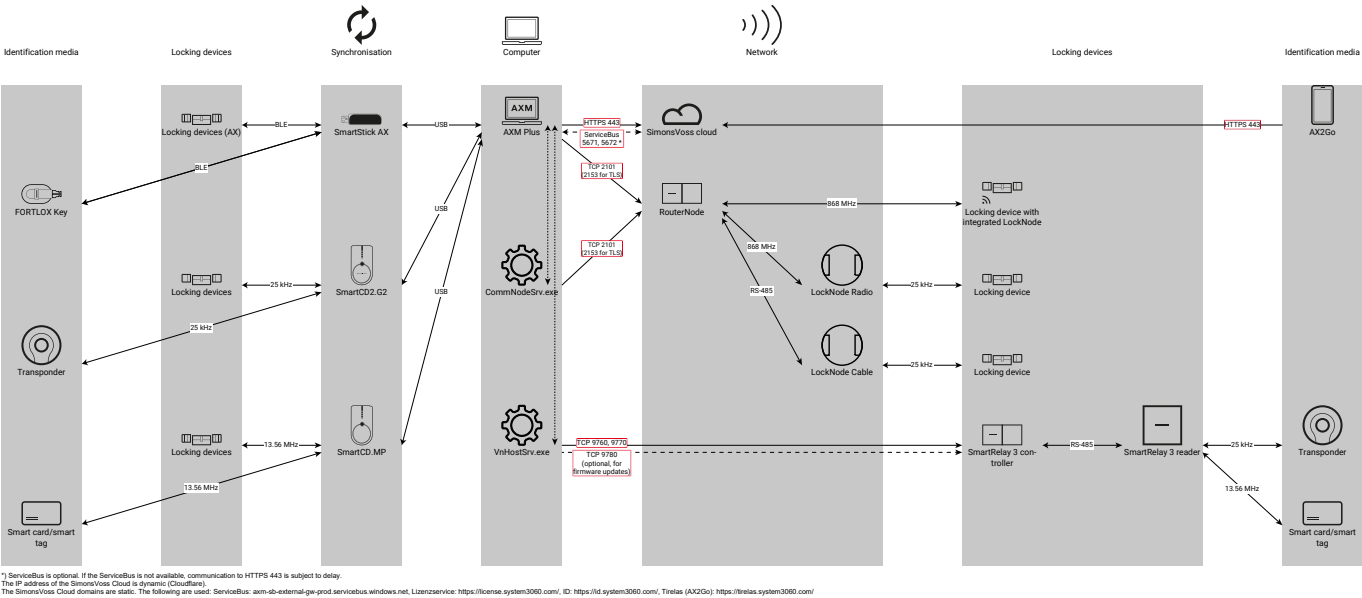
8. System requirements

AXM Plus

Operating system	■ MS Windows 11 64 Bit (Pro)
CPU	■ Supports only Intel and comparable AMD processors No support for ARM processors in System 3060 ■ Minimum: Intel® Core™ i5 (11th generation) Recommended: Intel® Core™ i7 (11th generation) or higher
Main memory	16 GB or greater
Memory	■ 500 MB free memory (physical), approx. 1 GB during installation ■ 256 GB SSD or greater
Display	■ 13 inches ($\approx$ 33 cm) or greater ■ 1920×1080 or greater
Supported MS SQL Edition	MS SQL Server Express LocalDB (installed and configured automatically)

Administrator rights are not necessary for normal locking system management using your AXM Plus. Administrator rights are required to install and restart services.

8.1 AXM services and ports used



9. Release notes

9.1 Version 2.0.24303.0902

Released on 30.11.2024

Improvements

- 1. End of the public preview and general availability

9.2 Version 2.0.24346.0501

Released 12/11/2024

New functions

- First version with VNHost- & WaveNet support (see *Networking* [[▶ 451](#)])
- AX2Go Resolving out-of-sync issues
- AX2Go Project migration (see *Migrate project (transfer)* [[▶ 517](#)])

New hardware support

- SmartRelais 3 Advanced
- SmartRelay AX Classic

Known restrictions

- Option to change columns in matrix deactivated

9.3 Version 2.0.25083.0801

Released on 24/03/2025

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

Improvements

- 1. Optimised recovery process for backups in the event of e.g. system crash, reconnect process with decision support for the administrator (rectification of the so-called out-of-sync, database and cloud no longer synchronised)
- 2. Hand-over function, planned migration process of AXM installations and projects to a new system, pausing the cloud state and reconnecting without restrictions or losses

3. Support for new AX hardware

- SREL AX Classic, door opener incl. BLE for AX2Go
- SREL 3 as door opener (offline)

Bugfixes

1. The setup problem has been fixed if ASP.Net x64 is already installed
2. Fixed problem with programming requirements and updating the access status
3. Fixed application error due to missing locking system
4. Fixed a problem when editing "Special transponders"
5. Fixed a problem when resetting the PinCode AX
6. Fixed incorrect calculation of free AX2Go floating licences
7. Fixed problem when working with the cloud directly after installation/registration
8. Fixed a problem when disconnecting the cloud after a long period of inactivity

9.4 Version 2.0.25105.0001

Released on 08/04/2025

Component	File	Version
GUI Version	AXM.exe	2.0.25063.0102
Platform Version	Axm.Server.Api.exe	2.0.25098.0902
VNService		2.0.25041.0901
CommNode		2.0.25041.0901
SVDriver	AXWDrv.dll	7.63.0
SVDriver for AX2Go	AXWDrv_V3.dll	8.24.0.3

Hotfixes

1. AX2Go performance
2. Small authorisation crosses after update with 2.0.25083.0801

9.5 Version 2.0.25105.0001 (HotFix)

Released 15/04/2025

Bug fixes

- AX2Go Scaling disabled during synchronisation
- The issue was resolved when all permissions were displayed in a reduced font

9.6 Version 2.0.25225.0801

Released 13/08/2025

New functions

- Beta support for FORTLOX Cylinder and FORTLOX Key
- Extended WaveNet functionality:
 - Test function shows battery status, signal quality and firmware version (see [Test RouterNode or LockNode \[▶ 475\]](#))
 - Search for router (CENTRAL NODE) via Hostname (see [Add RouterNodes \[▶ 465\]](#))
 - Replacement of router (CENTRAL NODE) via IP (see [Replace RouterNode or change IP address \[▶ 472\]](#))

Bug fixes

- Troubleshooting Digital Cylinder AX FD thumb-turn detection
- RouterNode freeze when resetting
- Wrong time stamp in physical access lists
- Empty matrix after backup import
- Various UI display problems and programming errors

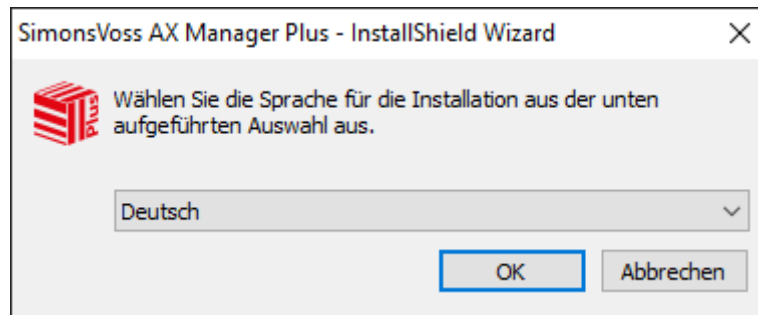
Known restrictions

- AX2Go in rare cases, cannot be opened despite authorisation (workaround: reassign authorisation)
- AX2Go request cannot be confirmed (workaround: reinstall app)
- IP change SmartRelais 3 Advanced via TCP not possible
- VNHost: No matrix updates - deactivated TID

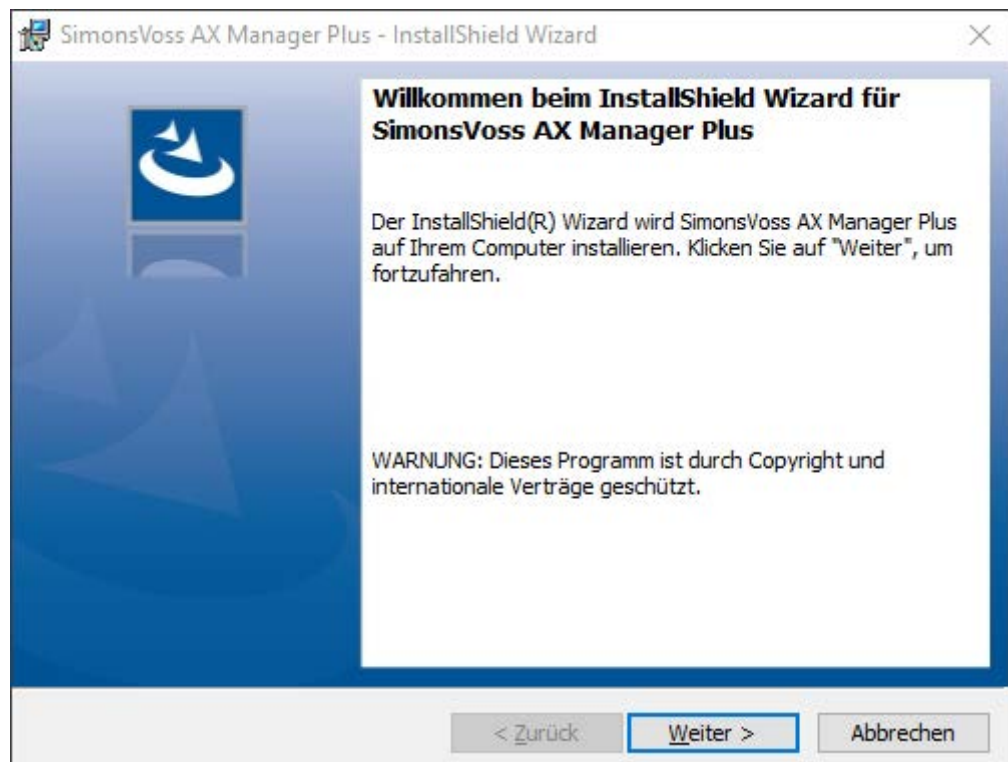
10. Installation

- ✓ System requirements fulfilled for the AXM Plus (see *System requirements* [▶ 22]).

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.

10.1 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:

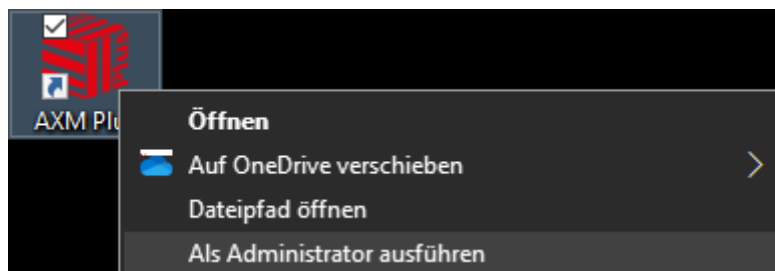
Manual start as administrator

- ✓ 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.

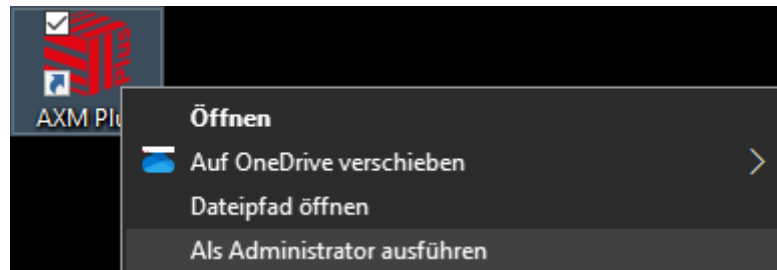
Consequently, SimonsVoss recommends that the properties of the link to AXM Plus be set so that the AXM Plus is always run as administrator using this shortcut.

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

1. Locate the shortcut or the AXM Plus icon.

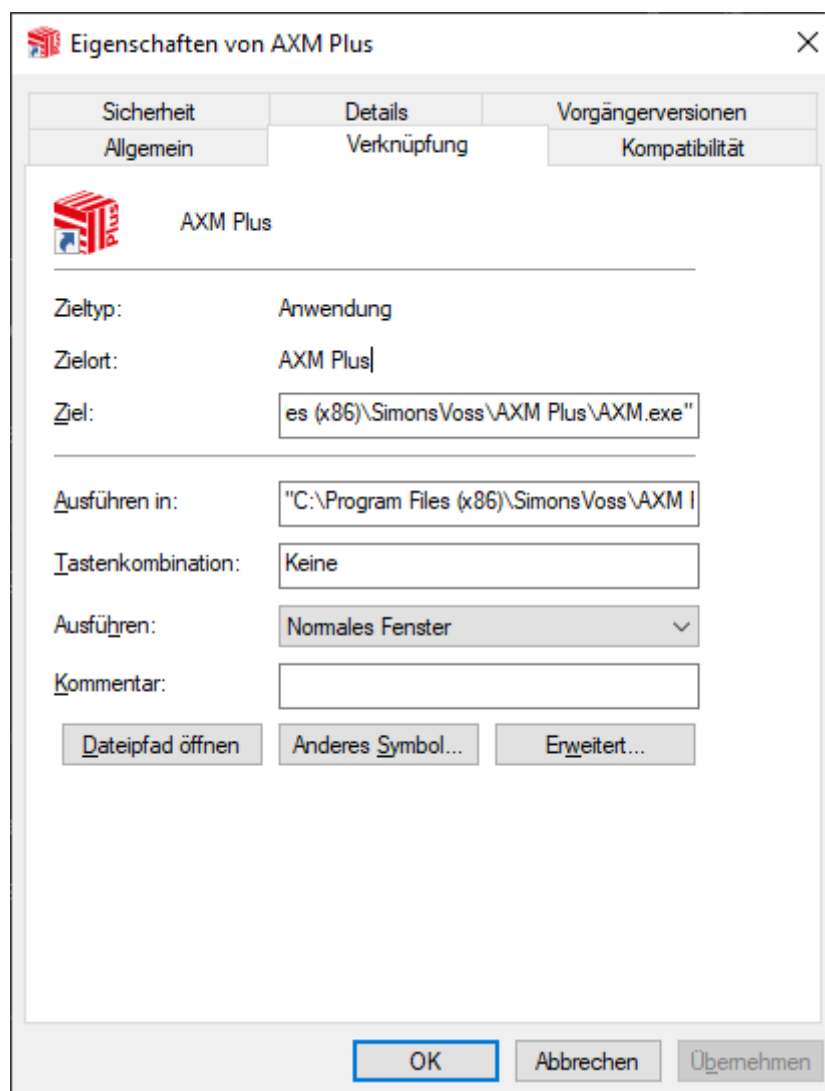


2. Right-click on the shortcut menu to open the context menu.
3. Click on the **Properties** entry with your name.



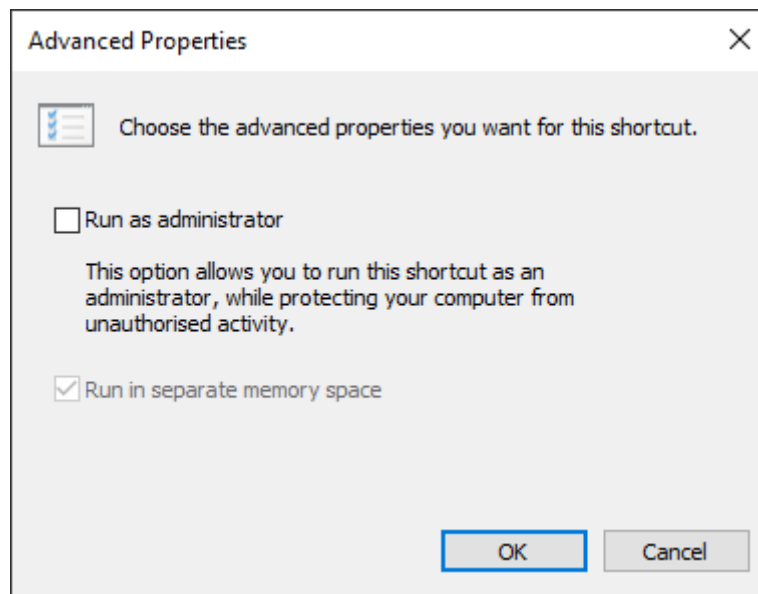
→ The "AXM ... Properties" window will open.

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.

10.2 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](#) [▶ 513]) before updating.

See [Displaying version number and licence key for the AXM installed](#) [▶ 527] 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 bar opens.



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

INFO & HELP

About AX Manager

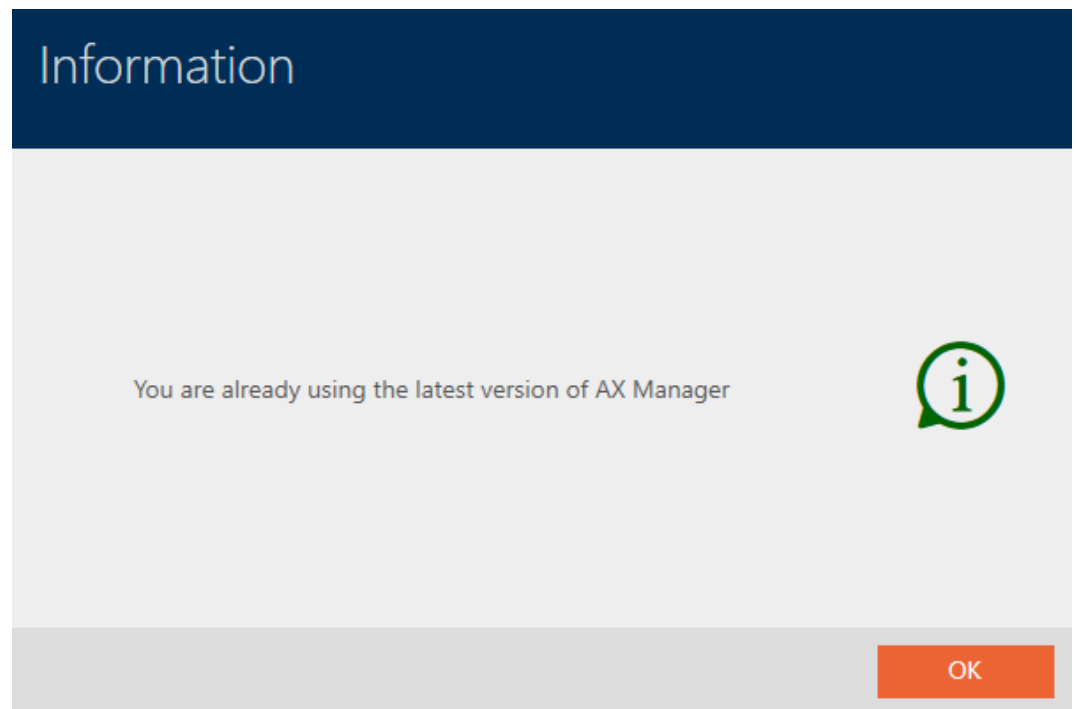
SimonsVoss Online Support

Check for updates

Feedback

Download error logs

- ➔ 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:



10.3 Using a web proxy

All AXM versions must connect to the SimonsVoss servers to activate their licence. If you have configured a web proxy in your network that restricts access, you need to enter this web proxy. Simply entering the web proxy in the Windows front-end is not enough.

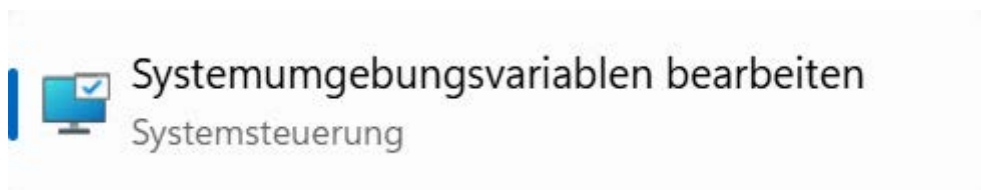
Background: the AXM uses a background system service written in .NET. This service reads the web proxy configuration from the system environment variables.

The following system environment variables must be configured on the AXM device:

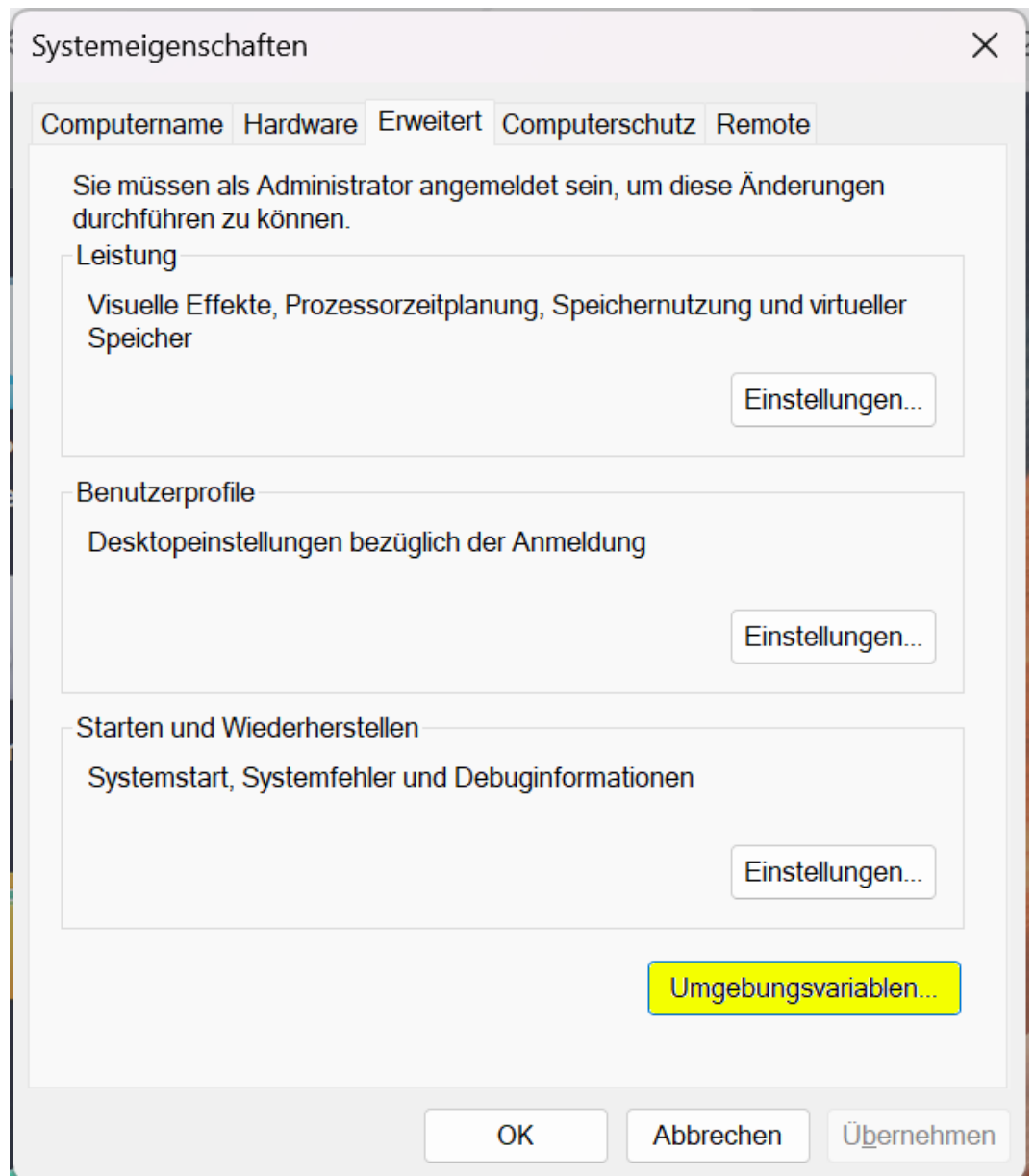
HTTP_PROXY	http://<proxyaddress>:<proxypor- t>
HTTPS_PROXY	https://<proxyaddress>:<proxy- port>
NO_PROXY	localhost,127.0.0.1

✓ Administrator rights available.

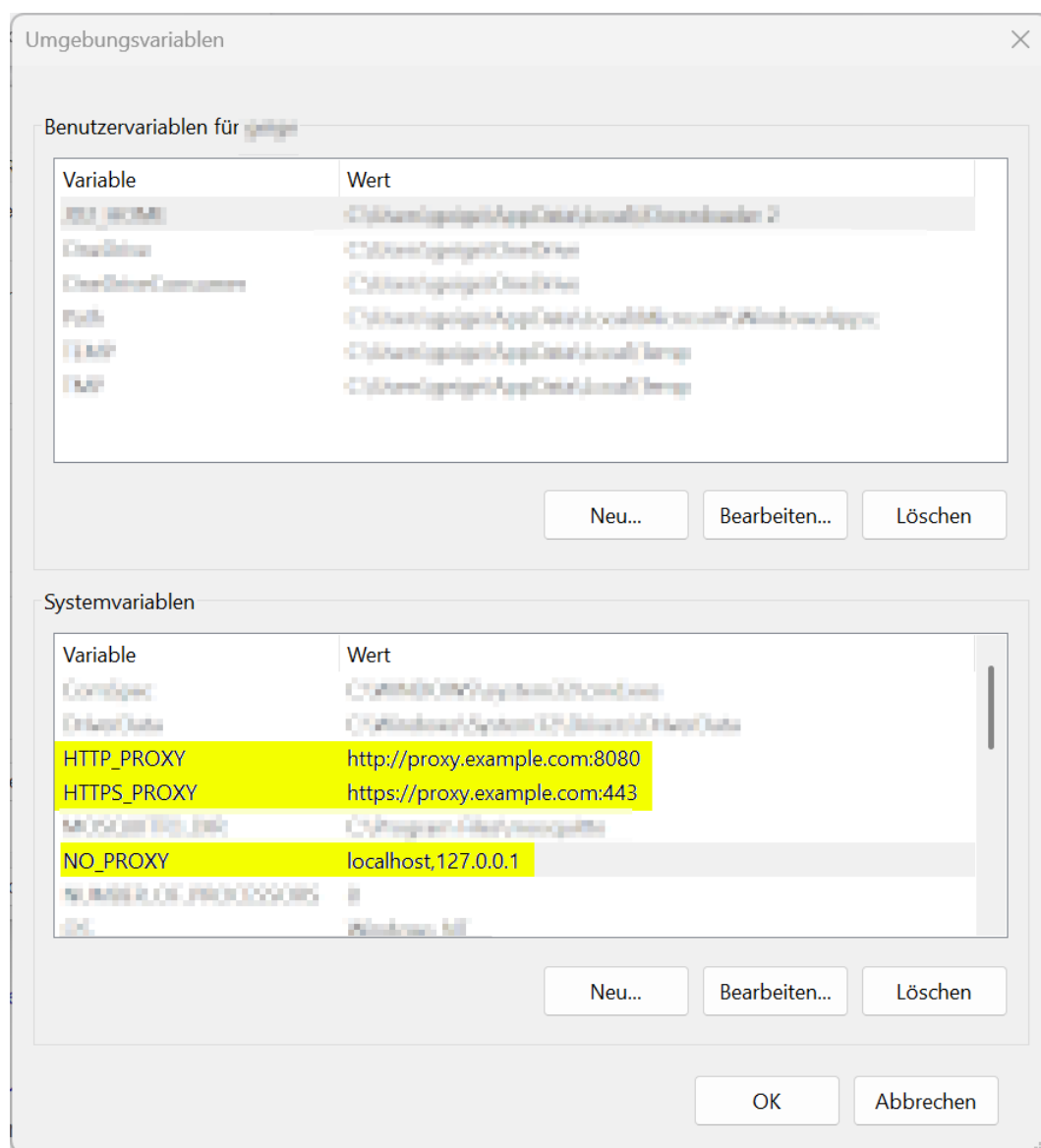
1. Access the system environment variables by opening the start menu, for example, and searching for “system environment variables”.



2. Click on the "Environment variables" button.



3. Create the required system environment variables.



4. Click on the “OK” button to save the system environment variables.
5. Then restart the computer so that the changed system environment variables can take effect.

11. First steps after a new installation

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

The screenshot shows the 'Willkommen bei AXM Plus' (Welcome to AXM Plus) interface. At the top, a dark blue header contains the title and a subtitle: 'Zum Starten können Sie ein bestehendes Projekt laden oder ein neues Projekt erstellen'. Below the header is a navigation bar with three icons: a plus sign for 'Neu' (New), a trash can for 'Löschen' (Delete), and a pencil for 'Umbenennen' (Rename). The main content area is titled 'Ein neues Projekt anlegen' (Create a new project). It contains four input fields: 'Projektname' (Project name), 'Benutzername' (Username) with the value 'Admin', 'Neues Kennwort' (New password), and 'Kennwort wiederholen' (Repeat password). Below these fields is a message: '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.' (You have not yet logged in to this project. Therefore, you must first set a password for the Admin user. The password must be at least 8 characters long). Below the message is a 'Qualität' (Quality) bar. At the bottom right is a blue 'Erstellen' (Create) button. At the bottom left is the version number '2.0.24023.801' and at the bottom right is a blue 'Abbrechen' (Cancel) button.

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 \[► 529\]](#)).

You can change the locking system password (see [Changing locking system password \[► 401\]](#)).

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 \[► 37\]](#)).

If you are working with a locking system for the first time, you will find explanations and background information here: [Background knowledge and explanations \[► 57\]](#).

11.1 Best practice: setting up the locking system

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

As a basic rule, the easiest way is to prepare the organisational structure first (see *Organisational structure* [▶ 60]).

Experience has shown that the following approach is best:

1. If necessary, set the time budget for virtual network (see *Set up a dynamic time window (time budget)* [▶ 243]).
2. Create locations (see *Creating a location* [▶ 87]).
3. Create building (see *Creating a building and assigning it to a location* [▶ 90]).
4. Create areas (see *Creating an area* [▶ 93]).
5. Create the first schedule (see *Creating a schedule* [▶ 63]).
6. Create all required time groups (see *Create time group* [▶ 66]).
7. Create additional schedules, setting the time groups directly for each schedule while doing so.
8. Create authorisation groups (see *Access levels* [▶ 340]).
9. Create person groups (see *Creating a person group* [▶ 61]).
10. If necessary, Configure cards in the locking system (see *Enable cards or transponders* [▶ 407]).
11. Create identification media and assign them directly to their access levels and time groups when they are created (see *Creating transponders and cards* [▶ 99], *Creating a person group* [▶ 61] and *Restricting identification medium authorisations to specific times (time group)* [▶ 135]).
12. Create locking devices and assign them directly to access levels, areas and schedules when they are created (see *Creating a locking device* [▶ 245], *Creating an area* [▶ 93] and *Limiting authorisations for locking devices to specific times (schedule)* [▶ 299]).
13. Synchronise locking devices (see *Synchronising the locking device (including reading access list)* [▶ 417]).
14. Synchronise identification media (see *Synchronise a card/transponder (including importing physical access list)* [▶ 428]).

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* [[▶ 587](#)]
- *Access levels* [[▶ 602](#)]

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

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

11.2 Best practice: 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* [[▶ 27](#)]).
 2. Register AXM Plus (see *Registration* [[▶ 39](#)]).
 3. Set up your locking system with locking devices and transponders (see *Best practice: setting up the locking system* [[▶ 37](#)]).
 4. Configure your AX2Go settings (see *AX2Go settings* [[▶ 544](#)]).
- ➔ AX2Go is ready for use. You can now create and send invitations, for example (see *Managing AX2Go keys* [[▶ 227](#)]).

11.3 Best practice: Database protection

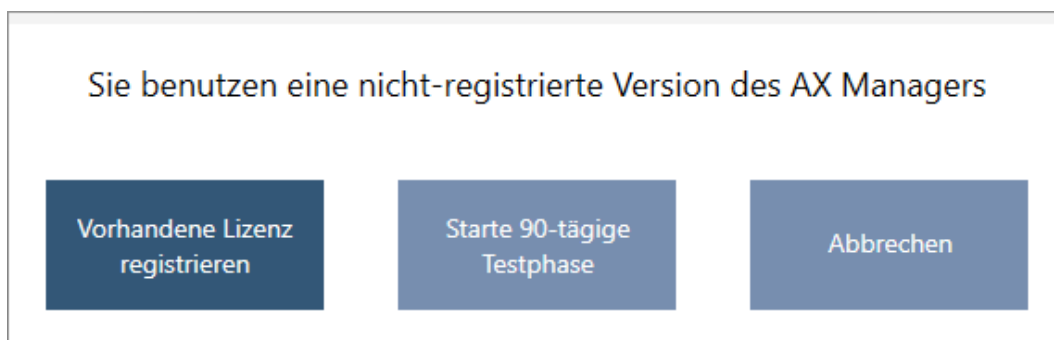
You can further enhance the security level of your AXM Plus by protecting access to your SQL database.

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.

12. Registration

12.1 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

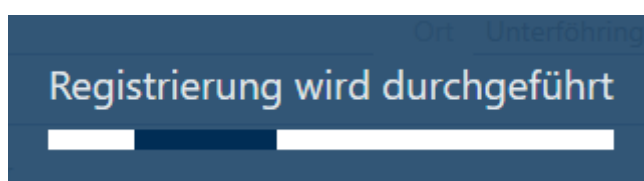
Tel.

Lizenzschlüssel XXXX-XXXX-XXXX-XXXX-XXXX

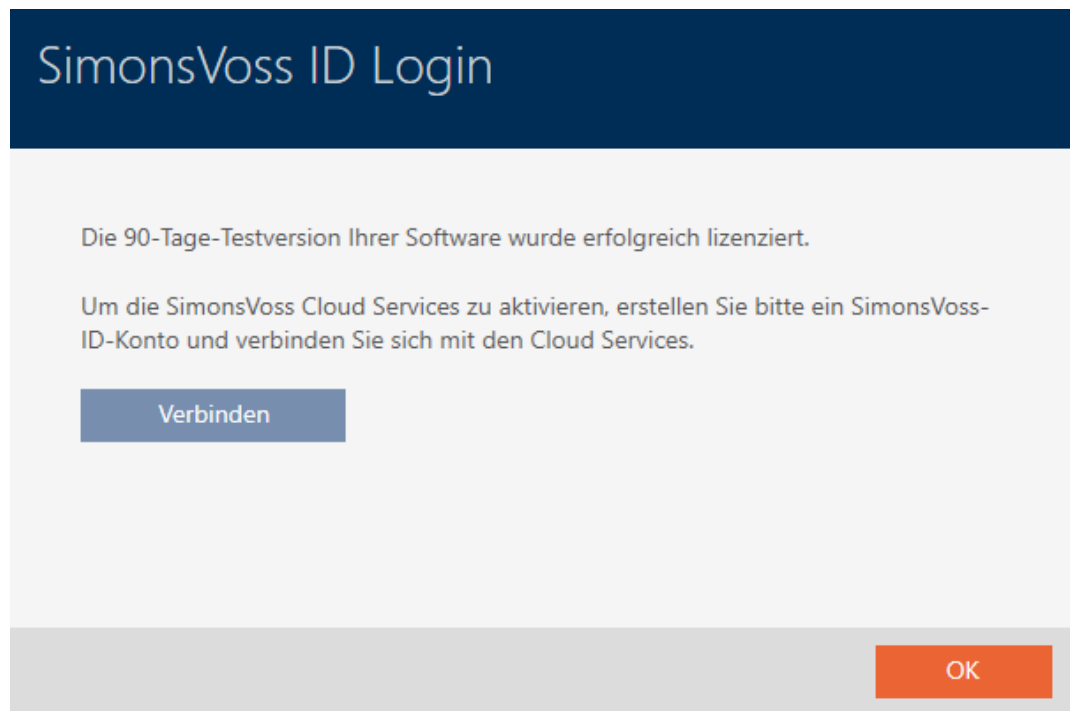
☐ [Nutzungsbedingungen](#) akzeptieren

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.



Create an account

One account. Access to all SimonsVoss services

Full Name
Enter your full name

Email
Enter your email

Password
Enter password

Password confirmation
Confirm password

Continue

or continue with:

[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

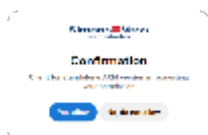
[Redacted email address]

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.



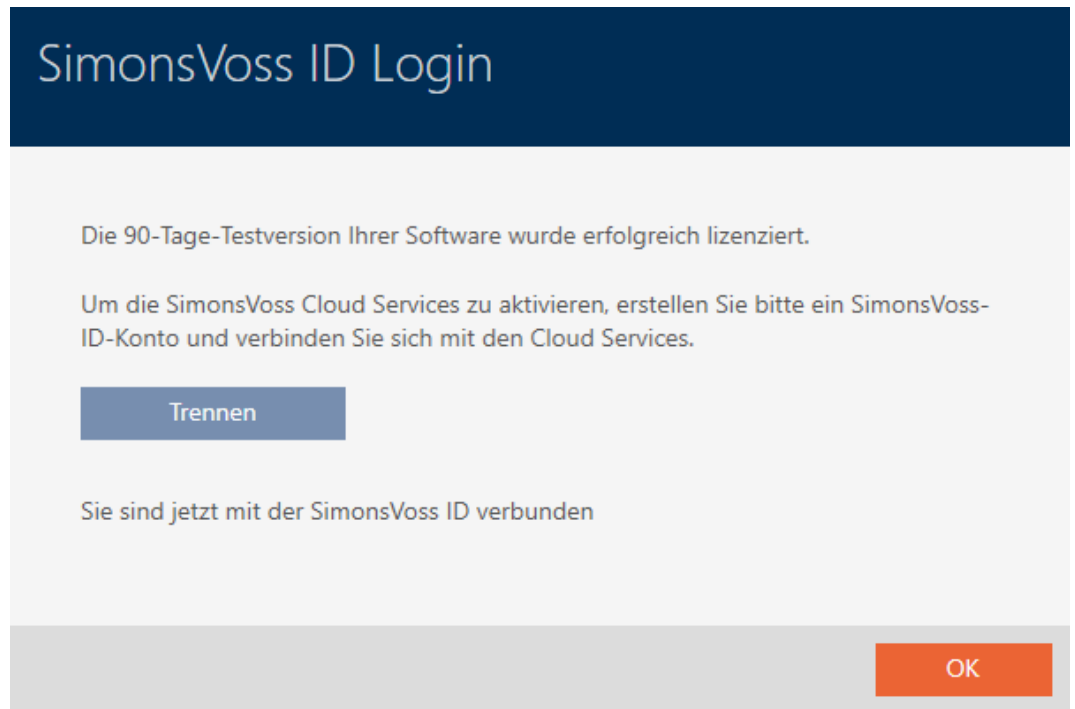
11. Click on “Yes, allow” to link your SimonsVoss ID and AXM Plus.

↳ 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.

12.2 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

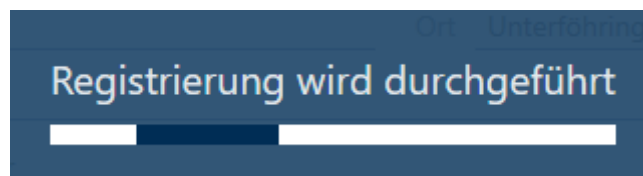
Lizenzdatei importieren

Registrieren

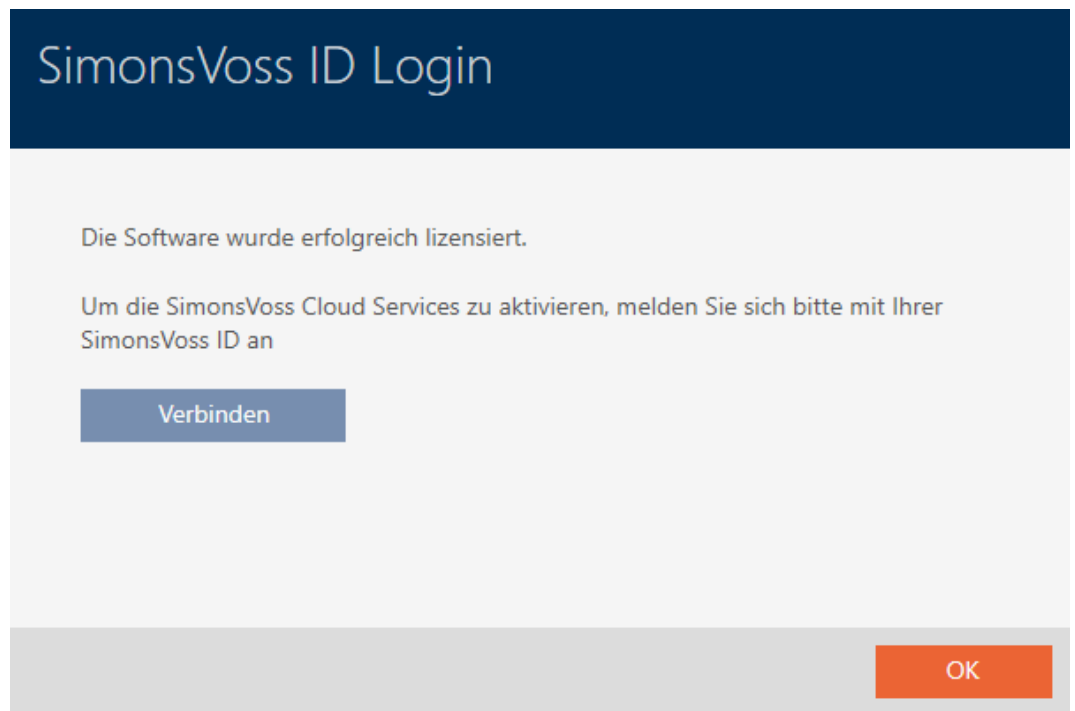
Starte 90-tägige Testphase

Abbrechen

- 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.
- Accept the terms of use.
- 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

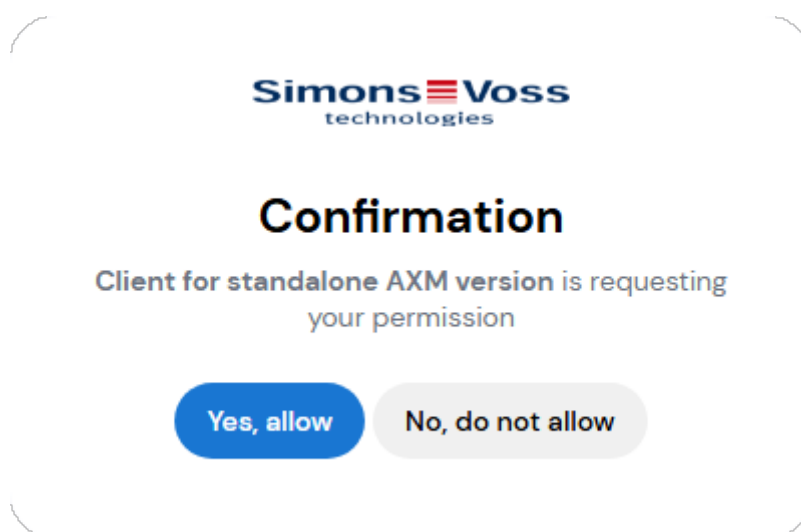
Continue

or continue with:

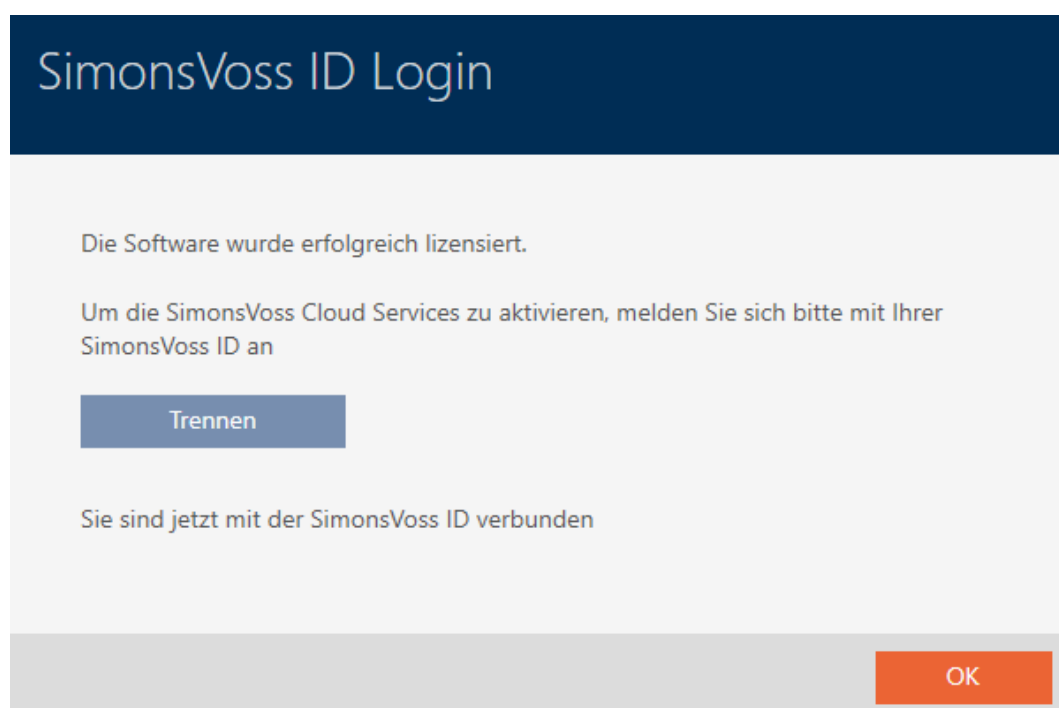
 

[Can't log in?](#) | [Create an account](#)

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.

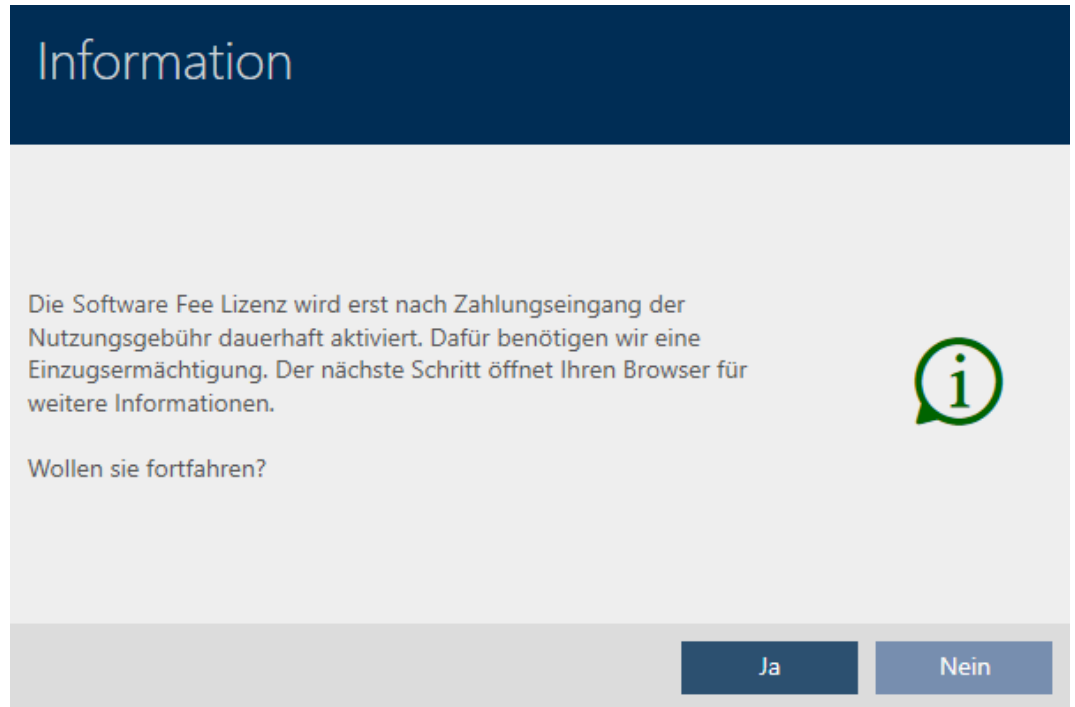


9. Click on “Yes, allow” to link your SimonsVoss ID and AXM Plus.
↳ Website and AXM Plus inform you that the link has been established.



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

→ A notice about the software 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.

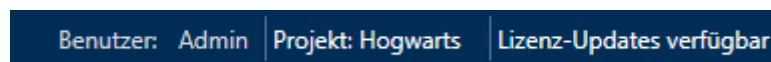
→ Registration and link with SimonsVoss ID completed.

12.3 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
AX2Go Lizenzen	1000
SmartSync Lizenzen	0
LockNode-Lizenzen	0
Lizenzschlüssel	
Service Fee Lizenz	☒
Gültig bis	12.09.2024
Zahlungseingang bestätigt	☒

Nach Lizenz-Updates suchen

Lizenz ändern

Schließen

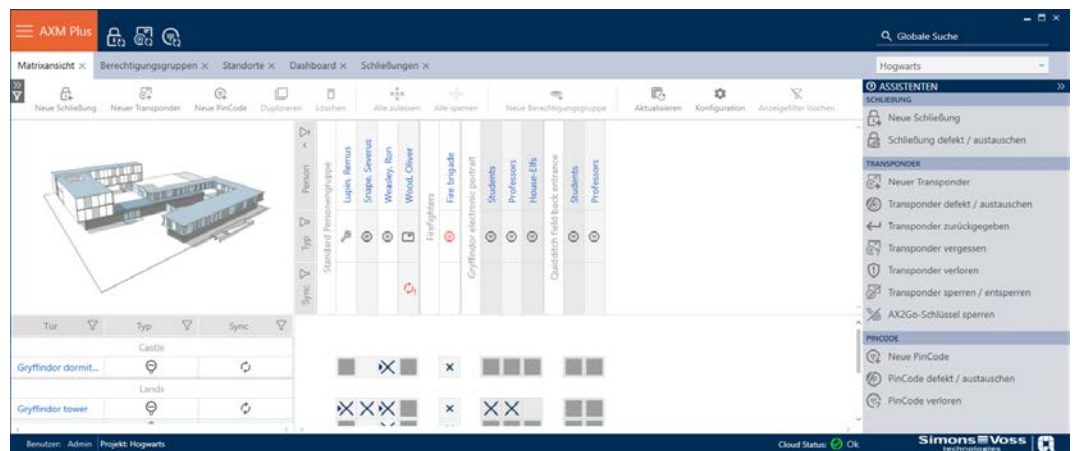
Scroll down in the window that opens and click on **Check for licence updates**.

Nach Lizenz-Updates suchen

Lizenz ändern

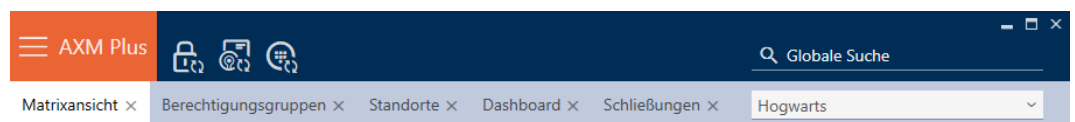
Die Lizenz wurde erfolgreich aktualisiert

13. 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](#) [▶ 58]).

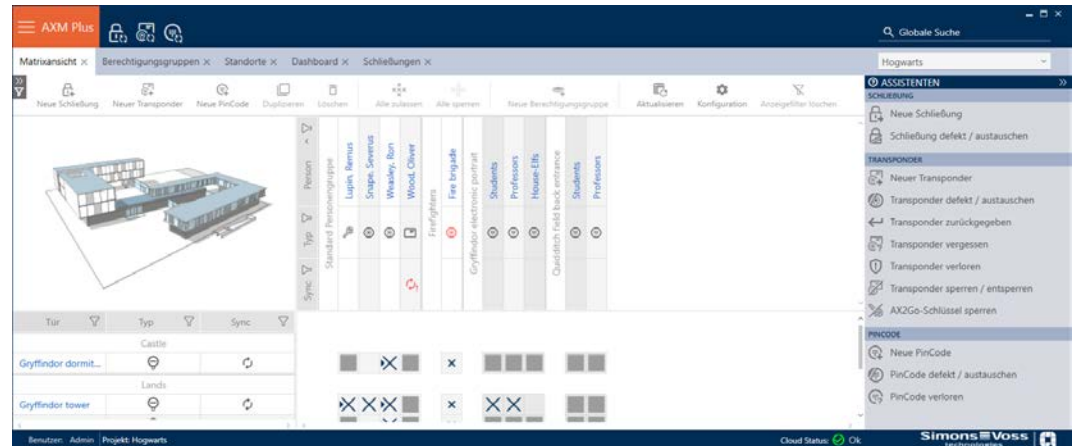
There are three buttons next to the AXM button to skip directly to synchronisation of locking devices and identification media.



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](#) [[▶ 57](#)]).

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](#) [[▶ 54](#)]).

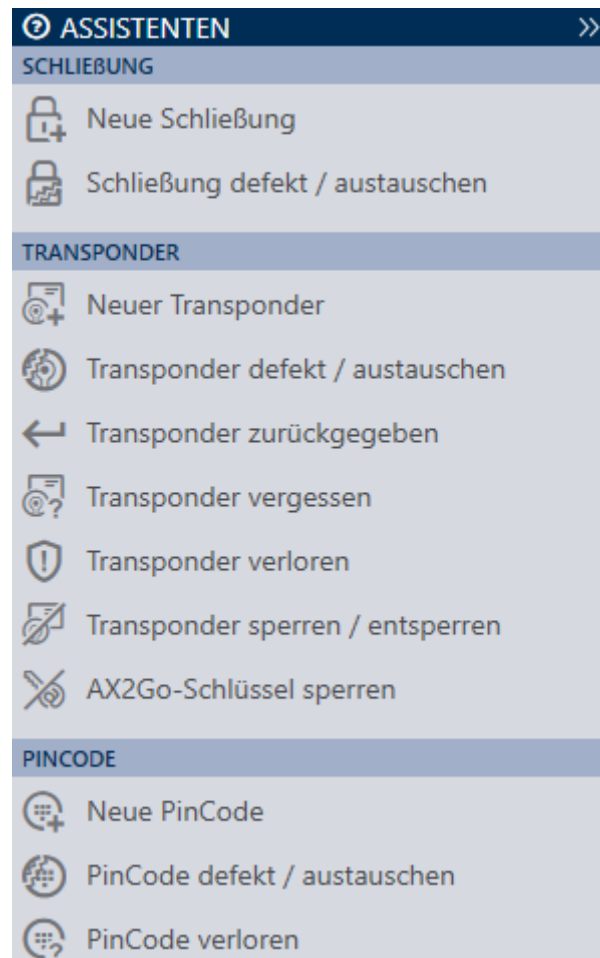
Each row normally represents a locking device and each column represents an identification medium. This identification medium's authorisation for this locking device is indicated where rows and columns meet (see [Permissions](#) [[▶ 335](#)]). There are basically two different main states:

- 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](#) [[▶ 416](#)]). 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:

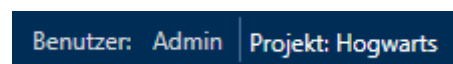
Wizard menu



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 \(dashboard\) \[► 555\]](#)). 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 \(log\)](#) [▶ 557]).

The log can also be accessed via the AXM bar.

13.1 Sorting and filtering

Large lists and tables can become confusing.

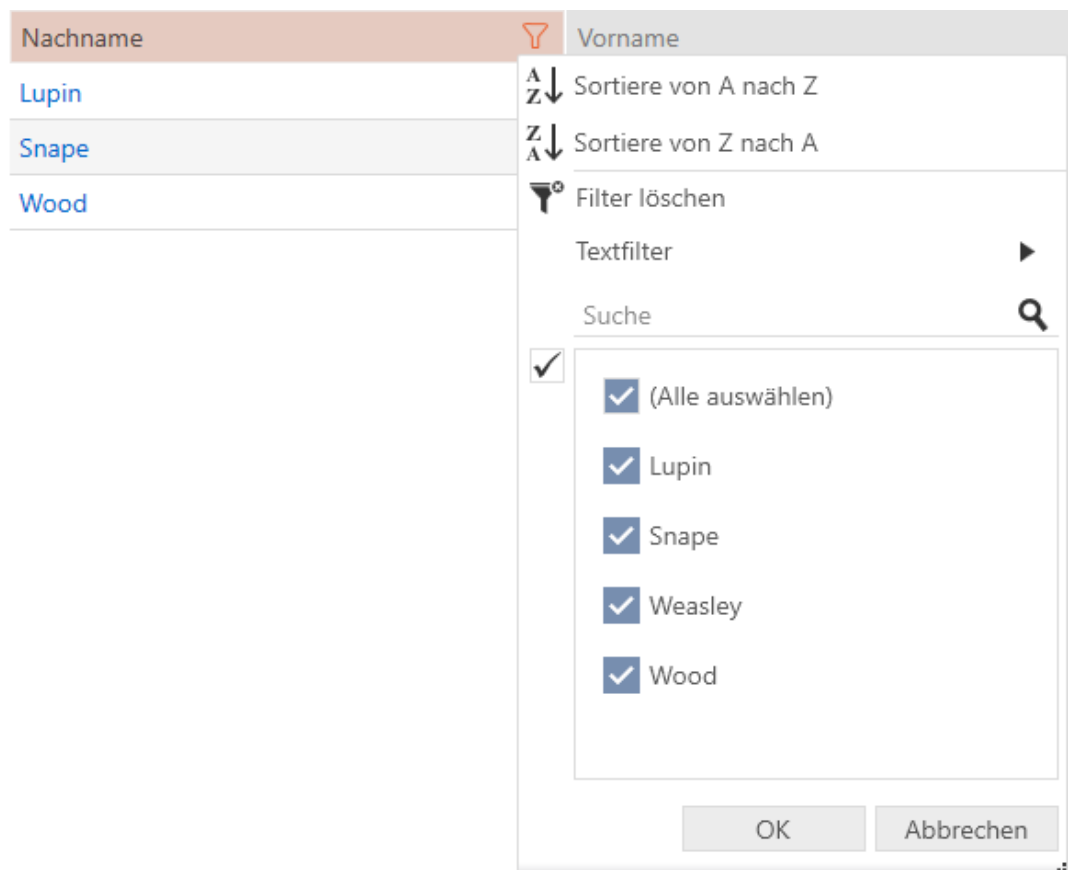
The AXM Plus provides you with sorting and filtering functions to simplify things.

Sorting

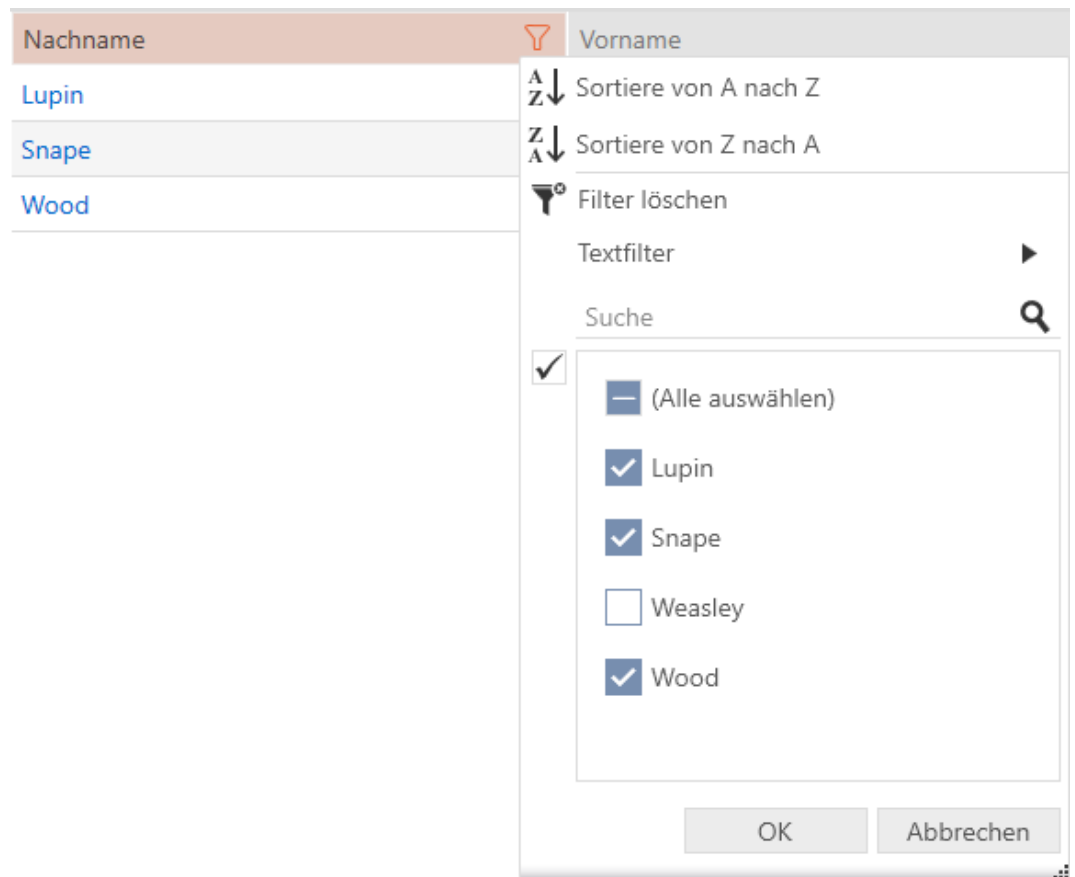
1. Click on one of the column or row headings.
 - ↳ Entries will then be sorted by this column/row.
2. Click on the same heading again.
 - ↳ The sort order is reversed.

Filtering

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



2. Adjust the filters.

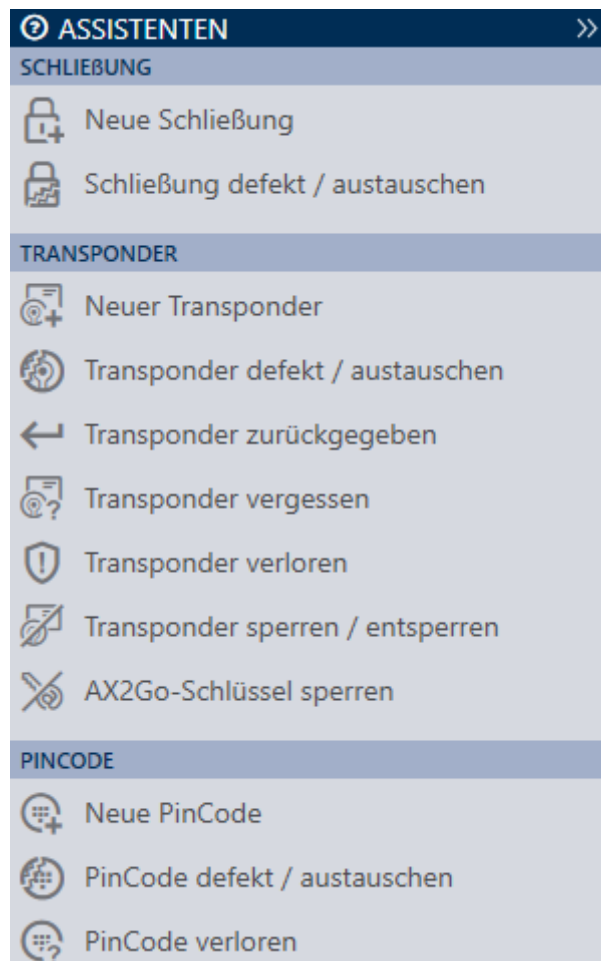


3. Click on the **OK** button.

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

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

13.2 Installation wizards



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

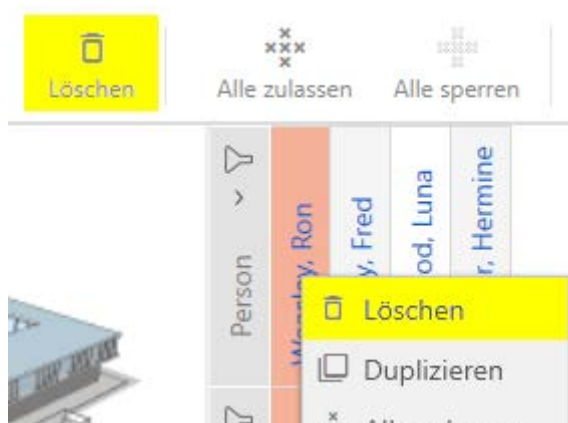
If you need more space, you can use **>>** to hide the wizard menu and **<<** to show it.

13.3 Multiple options, same result

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

There are often several ways to achieve the same result.

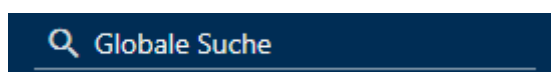
For example, you can delete an entry in the matrix in two ways:



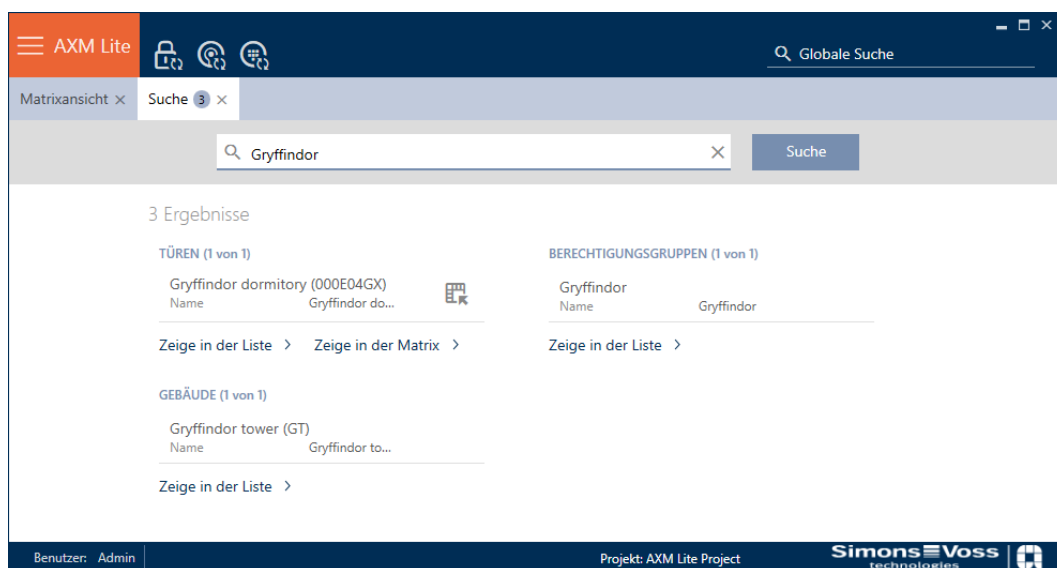
1. Using the matrix bar: **Löschen**
2. Using the context menu: **Löschen**

Both ways delete the entry.

13.4 Global search

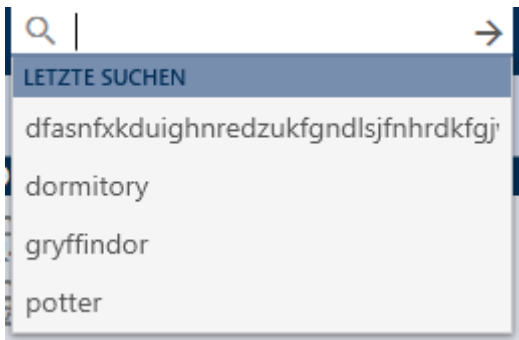


The global search in AXM Plus searches all entries and lists them in an overview:



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:



13.5 Working with AXM more effectively

13.5.1 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.

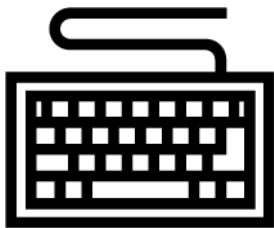
Frequently used tabs can also be opened automatically when the program is launched (see *Pinning tabs* [▶ 490]).

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.

13.5.2 Hotkeys



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

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)

13.5.3 Creating additional objects

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

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

This is where AXM 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.

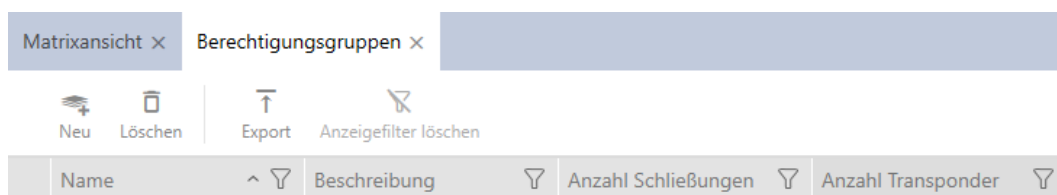
14. Organisational structure

14.1 Creating access levels

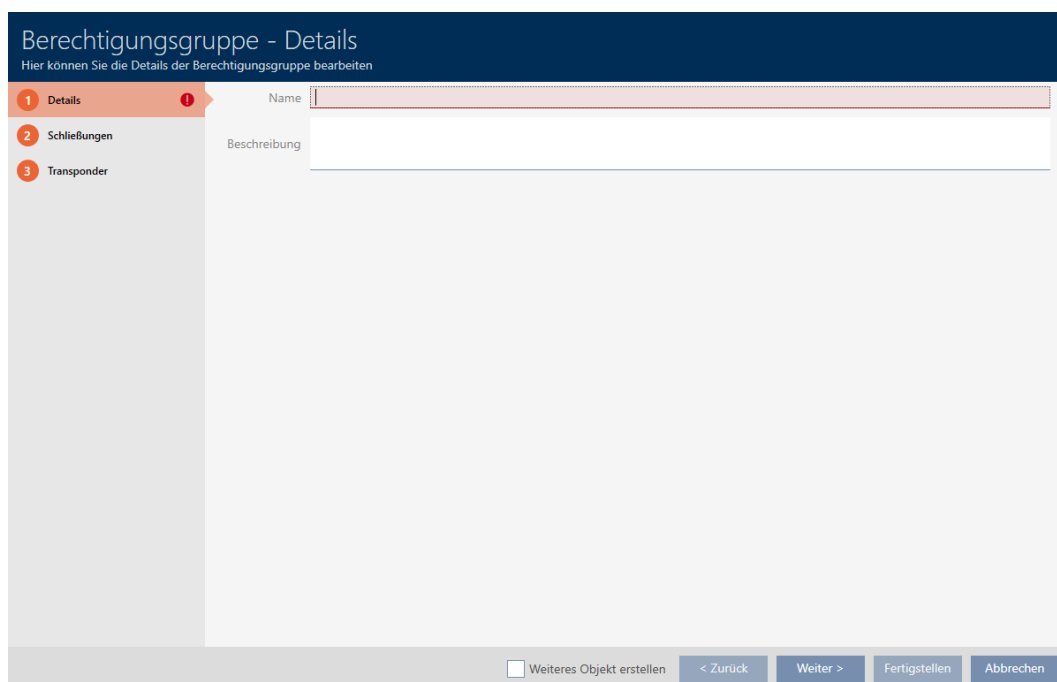
1. Click the orange AXM button .
 - ↳ AXM bar opens.



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 access level will open.



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

Matrixansicht x		Berechtigungsgruppen x		Hogwarts	
Neu		Löschen		Export	
				Anzeigefilter löschen	
Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder		
> Gryffindor		0	0		

14.2 Creating a person group

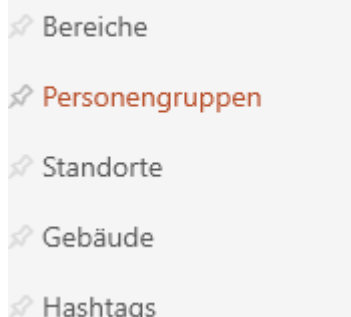
Person groups are a very useful structure for your locking system (also see *Person groups* [▶ 603]).

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

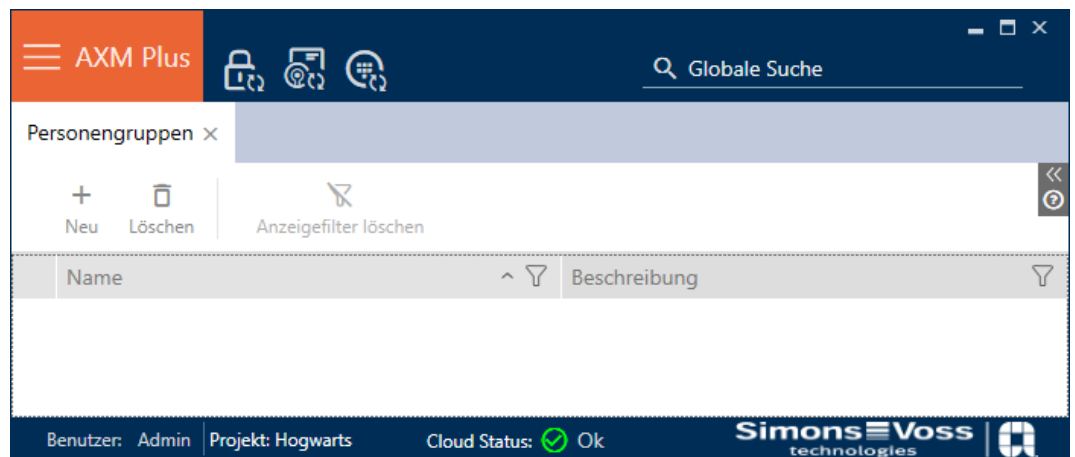


2. Select the **Person groups** entry in the | LOCKING SYSTEM CONTROL | group.

ORGANISATIONSTRUKTUR

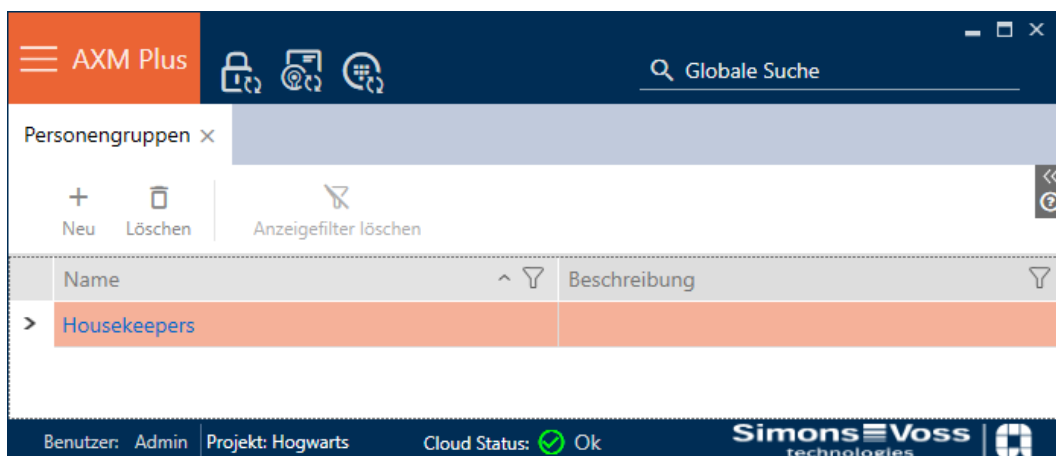


- ↳ The [Person groups] tab will open.



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.



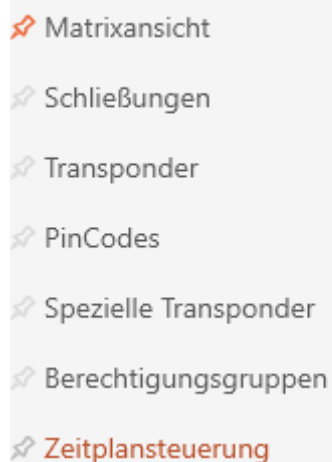
14.3 Creating a schedule

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



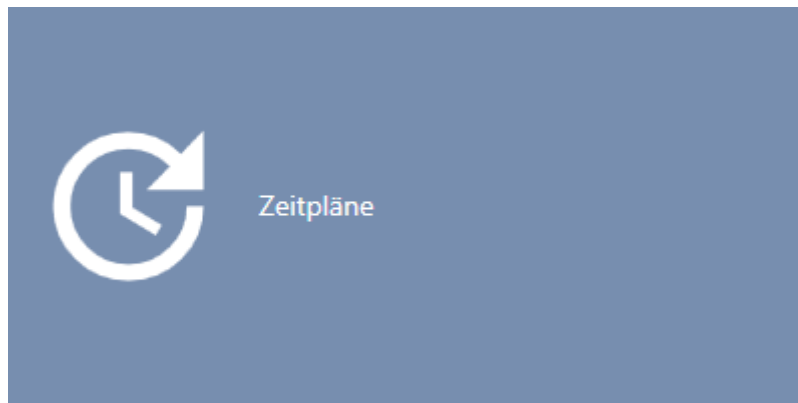
2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLIESSANLAGENSTEUERUNG

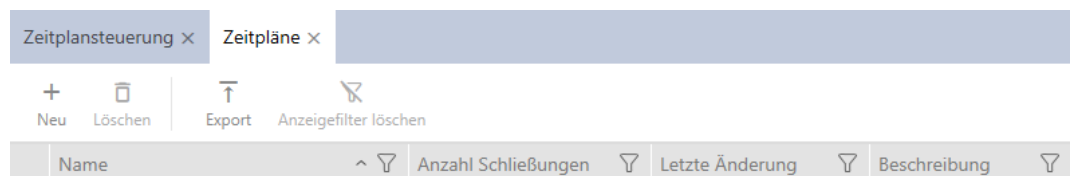


- ➞ The AXM bar will close.
- ➞ The [Time schedule control] tab will open.

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

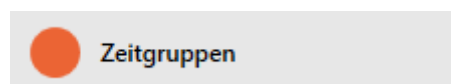
3 Zugewiesene Schließungen

Name Zeitplan 1

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 Zeitgruppe 1

Modus ☐ Berechtigt ☐ Nicht berechtigt ☒ Zeiten beschränken

☐ Für PinCode Tastatur

ZEITEN

	Von	Bis	Tage
☐	00:00	24:00	☐ Mo ☐ Di ☐ Mi ☐ Do ☐ Fr ☐ Sa ☐ So ☐ Sonderstag

☐ Weiteres Objekt erstellen

Not authorised	No identification media in this time group are authorised for any of the locking devices in this schedule, even if they were authorised in the matrix. Not authorised corresponds to a time limit that does not allow use on any day (i.e. effectively restricted at all times); see screenshot: ZEITEN <table><tr><th>Von</th><th>Bis</th><th>Tage</th></tr><tr><td> 00:00 </td><td> 24:00 </td><td> Mo Di Mi Do Fr Sa So Sonntag </td></tr></table>	Von	Bis	Tage	00:00	24:00	Mo Di Mi Do Fr Sa So Sonntag
Von	Bis	Tage					
00:00	24:00	Mo Di Mi Do Fr Sa So Sonntag					
Limit times	All identification media in this time group are authorised for all locking devices in this schedule as specified in the matrix or authorisation groups if one of the configured time intervals applies.						

Zeitgruppe 1

Name

Zeitgruppe 1

Modus

☐ Berechtigt

☐ Nicht berechtigt

☒ Zeiten beschränken

☐ Für PinCode Tastatur

ZEITEN

Von	Bis	Tage
00:00	24:00	☐ Mo ☐ Di ☐ Mi ☐ Do ☐ Fr ☐ Sa ☐ So ☐ Sondertag

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

ZEITEN

	Von	Bis	Tage
	07:30	13:00	☒ Mo ☒ Di ☒ Mi ☒ Do ☒ Fr ☐ Sa ☐ So ☐ Sondertag
	14:00	18:00	☒ Mo ☒ Di ☒ Mi ☒ Do ☒ Fr ☐ Sa ☐ So ☐ Sondertag
	08:00	13:00	☐ Mo ☐ Di ☐ Mi ☐ Do ☐ Fr ☒ Sa ☐ So ☐ Sondertag

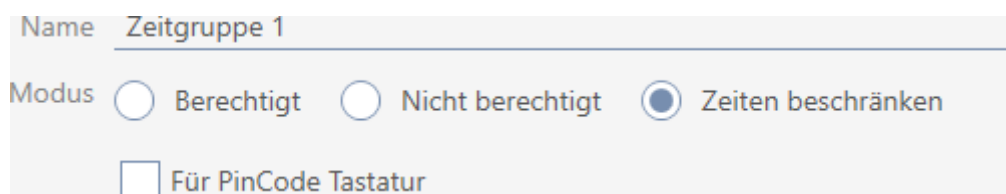
- Different time intervals for the same days (e.g. a store has its lunch break between 13:00 and 14:00)
- Different time intervals for different days (e.g. a store is only open in the morning on Saturdays)

More information; see *Time groups and schedules* [► 587].

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* [► 79]).

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

- ✓ Schedule created (see *Creating a schedule* [► 63]).
 - ✓ Schedule window open (see *Creating a schedule* [► 63]).
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 keypad 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).

ZEITEN

	Von	Bis	Tage
	00:00	24:00	☒ Mo ☒ Di ☒ Mi ☒ Do ☒ Fr ☐ Sa ☐ So ☐ Sondertag

ZEITGRUPPE 1

Name: Zeitgruppe 1

Modus: ☐ Berechtigt ☐ Nicht berechtigt ☒ Zeiten beschränken

☐ Für PinCode Testatur

ZEITEN

	Von	Bis	Tage
	06:00	22:00	☐ Mo ☐ Di ☐ Mi ☐ Do ☐ Fr ☐ Sa ☐ So ☒ Sondertag

Behandeln als...

Name: Mein Feiertag

Urlaub: ☐

Datum: 07.05.2021

Jedes Jahr: ☐

Sondertag

Montag

Dienstag

Mittwoch

Donnerstag

Freitag

Samstag

Sonntag

Sondertag

6. Set the time for the selected days.

ZEITEN

	Von	Bis	Tage
	00:00	24:00	☒ Mo ☒ Di ☒ Mi ☒ Do ☒ Fr ☐ Sa ☐ So ☐ Sondertag

00:00

00:15

00:30

00:45

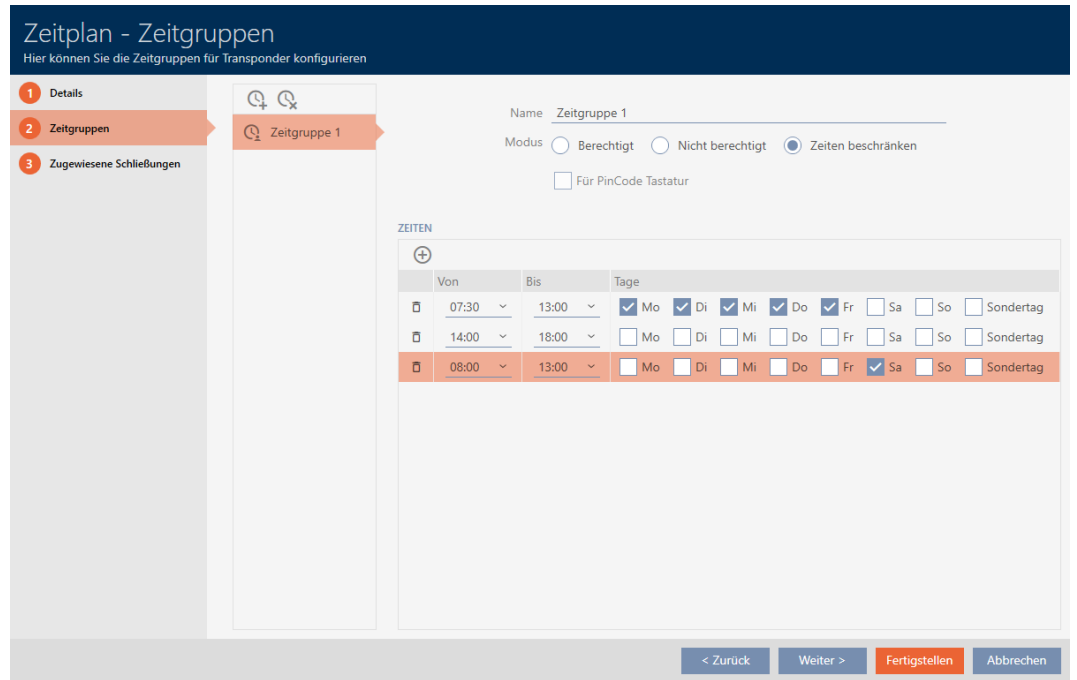
01:00

01:15

01:30

→ First time interval defined.

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



8. Click on the **Finish** button or create additional time groups with the  button if required.
- ➔ Time group is created and configured for the currently selected schedule.



NOTE

Configure new time groups for other schedules

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

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

14.5 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* [▶ 359]).

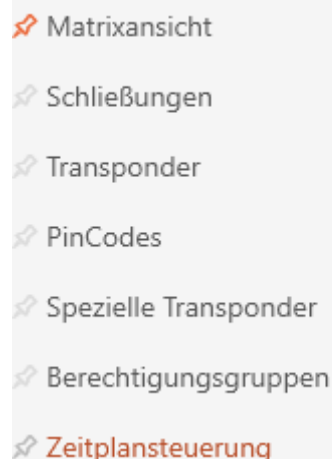
- If you do not wish to use a time group for just one schedule, set the time group to  Authorised mode.
- ➔ Identification media in this time group can open the locking devices for which they are authorised at any time.

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



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

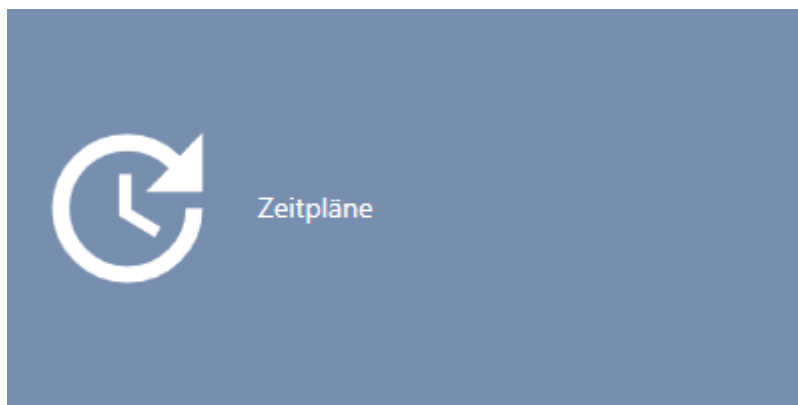
SCHLISSANLAGENSTEUERUNG



- ➔ 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					
 Neu		 Löschen		 Export		 Anzeigefilter löschen	
	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 Zugewiesene Schließungen

Name

Zeitplan 1

Beschreibung

☐ Weiteres Objekt erstellen

< Zurück

Weiter >

Fertigstellen

Abbrechen

5. 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

Zeitgruppe 1
Zeitgruppe 2
Zeitgruppe 3
Zeitgruppe 4

Name: Zeitgruppe 4
Modus: ☐ Berechtigt ☐ Nicht berechtigt ☒ Zeiten beschränken
☐ Für PinCode Tastatur

ZEITEN

Von	Bis	Tage
06:00	22:00	☒ Mo ☒ Di ☒ Mi ☒ Do ☒ Fr ☒ Sa ☐ So ☐ Sondertag

☐ Weiteres Objekt erstellen

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.

Zeitplan - Zeitgruppen
Hier können Sie die Zeitgruppen für Transponder konfigurieren

1 Details
2 Zeitgruppen
3 Zugewiesene Schließungen

Zeitgruppe 1
Zeitgruppe 2
Zeitgruppe 3

Name: Zeitgruppe 3
Modus: ☒ Berechtigt ☐ Nicht berechtigt ☐ Zeiten beschränken
☐ Für PinCode Tastatur

ZEITEN

Von	Bis	Tage
00:00	24:00	☐ Mo ☐ Di ☐ Mi ☐ Do ☐ Fr ☐ Sa ☐ So ☐ Sondertag

14.6 Deleting schedules

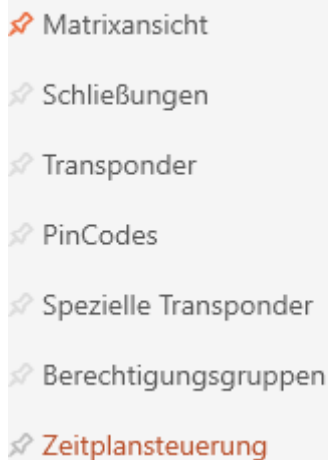
- ✓ Schedules are no longer assigned to a locking device (see [Adding locking devices to the schedule \[▶ 356\]](#) for instructions on how to edit assigned locking devices).

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



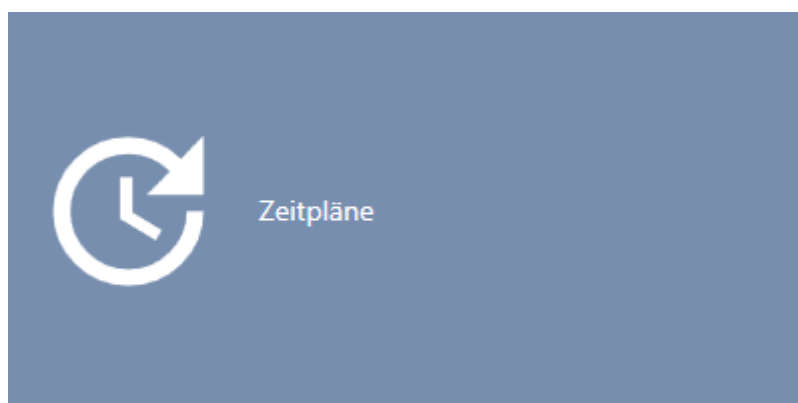
2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLISSANLAGENSTEUERUNG



- ↳ 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			
+ Neu		🗑️ Löschen		⬆️ Export	
				🗑️ Anzeigefilter löschen	
	Name		Anzahl Schließungen	Letzte Änderung	Beschreibung
>	Zeitplan 1		1	06.05.2021 11:53:10	

4. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
 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.

Zeitplansteuerung x		Zeitpläne x			
+ Neu		🗑️ Löschen		⬆️ Export	
				🗑️ Anzeigefilter löschen	
	Name		Anzahl Schließungen	Letzte Änderung	Beschreibung

14.7 Creating a time switchover

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



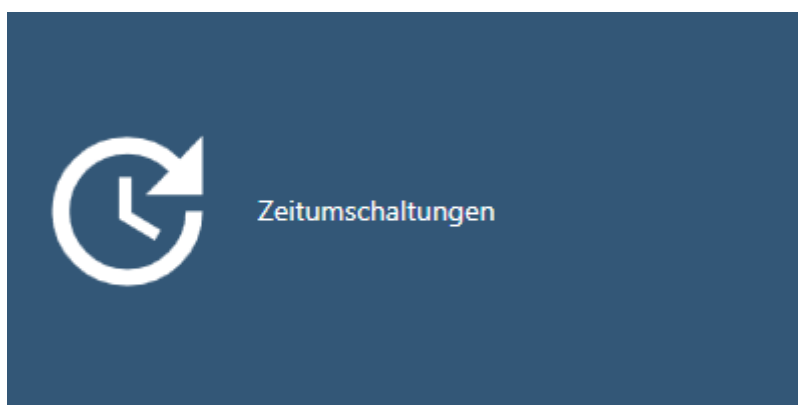
2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLIESSANLAGENSTEUERUNG

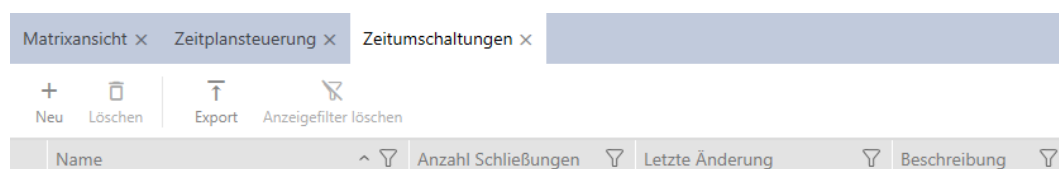
- Matrixansicht
- Schließungen
- Transponder
- PinCodes
- Spezielle Transponder
- Berechtigungsgruppen
- Zeitplansteuerung**

- ↳ 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 Zugewiesene 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 Zugewiesene 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* [► 301] if required.

Matrixansicht x Zeitplansteuerung x Zeitempfehlungen x				
+ Neu ✖ Löschen ↑ Export 🗑️ Anzeigefilter löschen				
Name	Anzahl Schließungen	Letzte Änderung	Beschreibung	
> Zeitempfehlung 1	1	07.05.2021 17:33:50		

14.8 Creating and editing public holidays



NOTE

Public holidays available in all locking systems

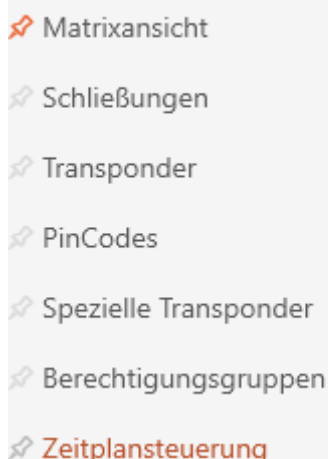
The list of public holidays is the same for all locking systems within a project. Public holidays created here are therefore also available in all other locking systems.

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

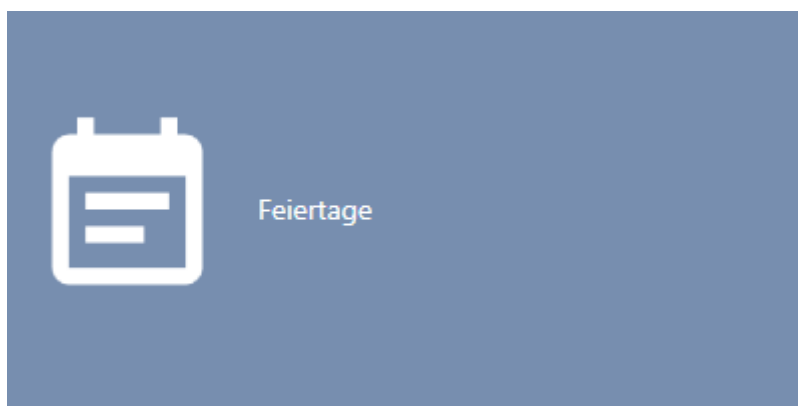


- Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLIESSANLAGENSTEUERUNG



- ↳ 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 ×		Zeitplansteuerung ×		Feiertage ×					
+ 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 Bettag	17.11.2021		Nein	Sonntag				
	Christi Himmelfahrt	13.05.2021		Nein	Sonntag				
	Erntedanktag	04.10.2021		Nein	Sonntag				
	Fastnacht	16.02.2021		Nein	Sonntag				
	Erste Mai	21.05.2021		Nein	Sonntag				

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

Feiertag - Details
Hier können Sie die Details des Feiertags bearbeiten

1 Details

Name

Urlaub ☐

Datum 

Jedes Jahr ☐

Behandeln als... Sonntag ▼

☐ Weiteres Objekt erstellen **Fertigstellen** **Abbrechen**

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.

Feiertag - Details
Hier können Sie die Details des Feiertags bearbeiten

1 Details

Name Mein Feiertag

Urlaub ☐

Datum  Das Feld ist erforderlich

Jedes Jahr ☐

Behandeln als... ▼

+ 1 + 3 + 5

< 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

☐ Weiteres Objekt erstellen **Fertigstellen** **Abbrechen**

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

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

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

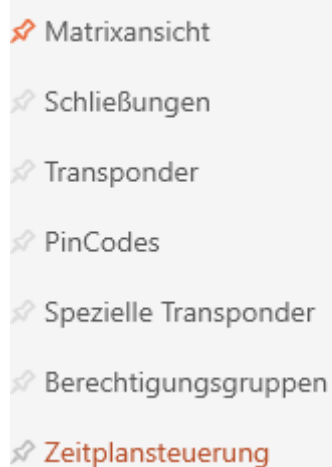
14.9 Creating and editing public holiday lists

1. Click the orange AXM button  **AXM**.
 - 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.

Feiertagsliste - Details

Hier können Sie die Details der Feiertagsliste bearbeiten

1 Details
2 Zugewiesene Feiertage

Name

☐ Weiteres Objekt erstellen
< Zurück
Weiter >
Fertigstellen
Abbrechen

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.

Feiertagsliste - Feiertage

Hier können Sie Feiertage zu der Feiertagsliste hinzufügen

1 Details
2 Zugewiesene Feiertage

AUSGEWÄHLT (0)

Name	Von	Bis

NICHT AUSGEWÄHLT (34)

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	
4. Advent	19.12.2021	
Allerheiligen	01.11.2021	
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	

Neuer Feiertag

< Zurück
Weiter >
Fertigstellen
Abbrechen

7. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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.

1 Details

2 Zugewiesene Feiertage

Feiertagsliste - Feiertage

Hier können Sie Feiertage zu der Feiertagsliste hinzufügen

AUSGEWÄHLT (4)

Name	Von	Bis
1. Advent	28.11.2021	
2. Advent	05.12.2021	
3. Advent	12.12.2021	
4. Advent	19.12.2021	

NICHT AUSGEWÄHLT (31)

Name	Von	Bis
1. Weihnachtsfeiertag	25.12.2021	
2. Weihnachtsfeiertag	26.12.2021	
Allerheiligen	01.11.2021	
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)* [▶ 299].

14.10 Creating a location



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

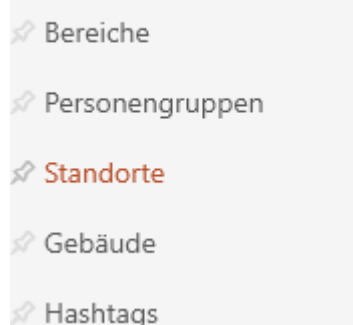
1. Click on the orange AXM icon  AXM.

↳ AXM bar opens.

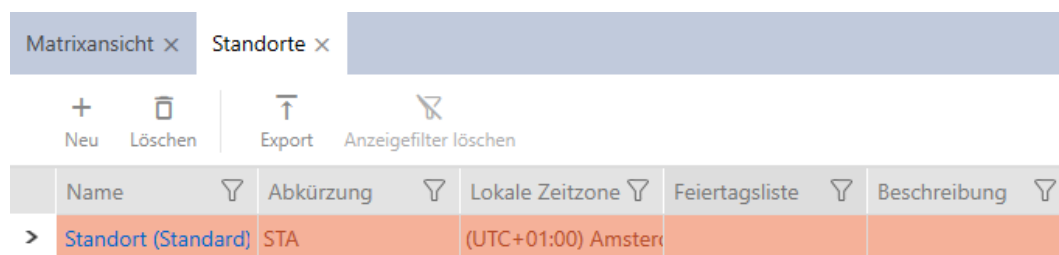


2. Select the **Locations** entry in the | ORGANISATIONAL STRUCTURE | group.

ORGANISATIONSTRUKTUR



↳ The [Locations] tab will open.



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

↳ The window for creating a new location will open.

Standort - Details
Hier können Sie die Details des Standorts bearbeiten

1 Details

Name

Abkürzung

Lokale Zeitzone (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Feiertagsliste **+ Neu**

Beschreibung

Als Standard verwenden ☐

☐ Weiteres Objekt erstellen **Fertigstellen** **Abbrechen**

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* [► 82]).

Standort - Details
Hier können Sie die Details des Standorts bearbeiten

1 Details

2 Zugeordnete Gebäude

Name

Abkürzung

Lokale Zeitzone (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna

Feiertagsliste **+ Neu**

Beschreibung

Als Standard verwenden ☐

☐ Bayern
☐ Berlin
☐ Brandenburg
☐ Bremen
☐ Hamburg
☐ Hessen
☐ Mecklenburg-Vorpommern
☐ Meine Feiertage
☐ Niedersachsen
☐ Nordrhein-Westfalen

< Zurück **Weiter >** **Fertigstellen** **Abbrechen**

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

14.11 Creating a building and assigning it to a location



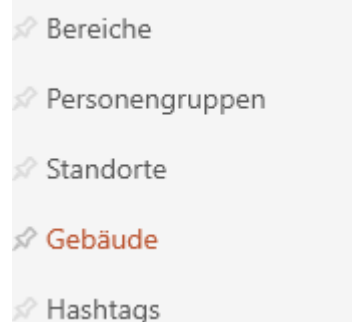
There must be at least one building in the database. AXM Plus therefore creates a default building for you. Obviously, you can create additional buildings.

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

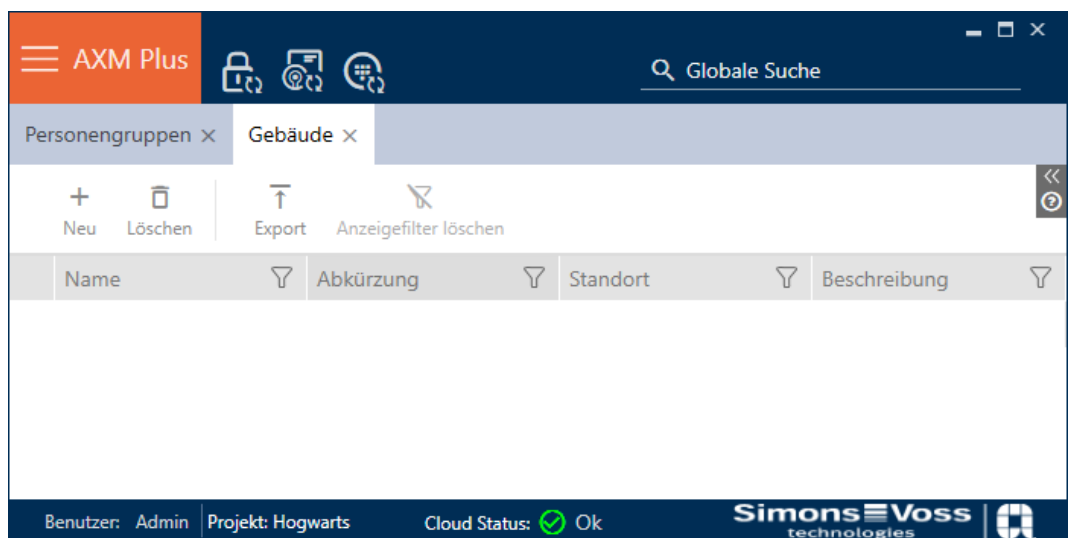


2. Select the **Building** entry in the | ORGANISATIONAL STRUCTURE | group.

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 × Gebäude ×			
+ Neu		↑ Export	
🗑️ Löschen		🗑️ Anzeigefilter löschen	
Name	Abkürzung	Standort	Beschreibung
Gebäude (Standard)	GEB	Standort (Standard)	
> Gryffindor tower	GT	Hogwarts	

14.12 Creating an area

Areas are a very useful structure for your locking system (also see [Areas](#) [▶ 607]).

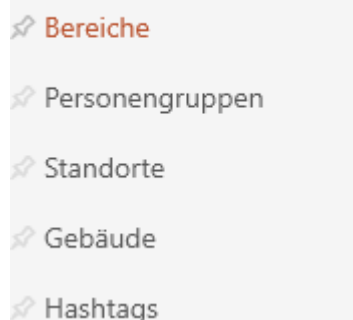
1. Click the orange AXM button .

↳ AXM bar opens.



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

ORGANISATIONSTRUKTUR



- ↳ The [Areas] tab will open.

Bereiche ×			
+ Neu		🗑️ Löschen	
		🗑️ Anzeigefilter löschen	
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* [▶ 63]) 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 ×

+ 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.

14.13 Creating a hashtag



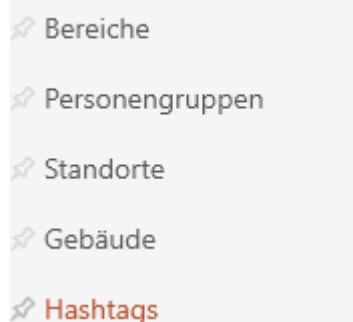
Hashtags can be used as keywords for persons and/or doors (see *Hashtags* [▶ 608]).

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

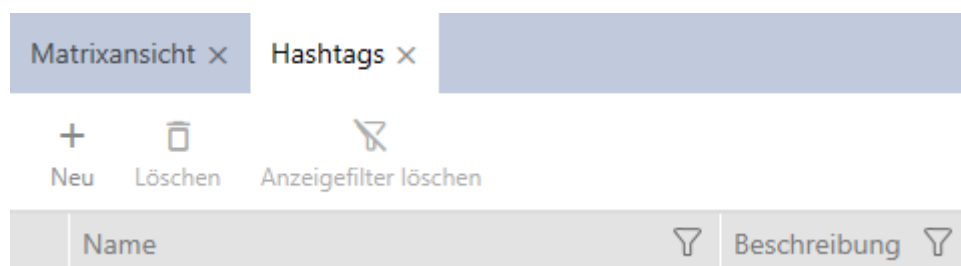


2. Select the **Hashtags** entry in the | ORGANISATIONAL STRUCTURE | group.

ORGANISATIONSTRUKTUR



- The [Hashtags] tab will open.



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

- The window for creating a new hashtag will open.

A screenshot of the 'Hashtag - Details' form. The form has a dark blue header with the title 'Hashtag - Details' and a subtitle 'Hier können Sie die Details zum Hashtag bearbeiten'. Below the header is a sidebar with a 'Details' tab. The main area contains two input fields: 'Name' and 'Beschreibung'. At the bottom right, there are three buttons: 'Weiteres Objekt erstellen' (disabled), 'Fertigstellen', and 'Abbrechen'.

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.

Matrixansicht ×		Hashtags ×	
+		Anzeige	
Neu		Löschen	
		Anzeigefilter löschen	
	Name		Beschreibung
>	Glastür		

15. Persons and identification media

Any changes you make to the locking system will only take effect when synchronised (see *Synchronise a card/transponder (including importing physical access list)* [► 428]).

15.1 Creating an identification medium

Your users can use identification media to engage and disengage locking devices (also see *Identification media, locking devices and the locking plan* [► 571]).

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	■ Time groups ■ Activation and expiry date	■ ☒ Long opening ■ ☒ Acoustic opening signal ■ ☒ from now ■ ☒ without expiry date
Service Sets	For transponders	No	No
Creation procedure	See <i>Creating transponders and cards</i> [► 99].	See <i>Creating PIN code keypads</i> [► 106].	See <i>Assigning keys for AXM Plus and higher</i> [► 227].

Further information on the different identification media and their differences can be found in Section *Identification media, locking devices and the locking plan* [▶ 571].

15.1.1 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* [▶ 407]).

In the interests of best practice (see *Best practice: setting up the locking system* [▶ 37]), SimonsVoss recommends that you configure access levels, person groups and schedules/time groups:

- *Access levels* [▶ 340] (see *Access levels* [▶ 602] for background information)
- *Creating a person group* [▶ 61] (see *Person groups* [▶ 603] for background information)
- *Creating a schedule* [▶ 63] or *Create time group* [▶ 66] (see *Time groups and schedules* [▶ 587] 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

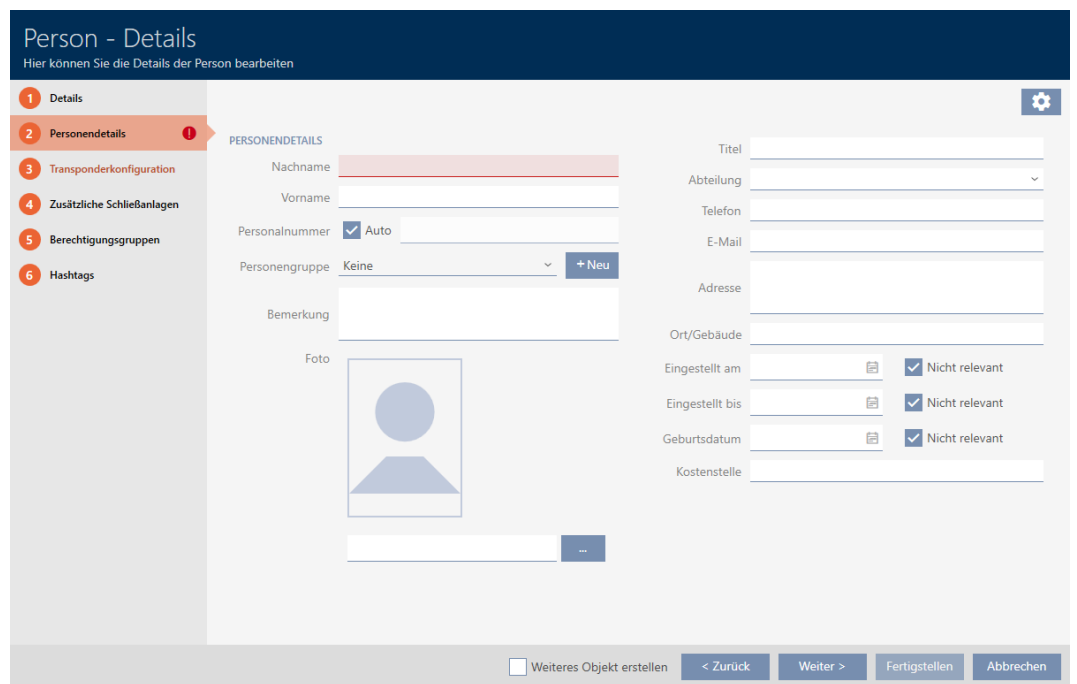
Neue Person ☒

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 \[► 491\]](#)).

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 *Hiring date*, *Exit 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 \(AX2Go and virtual network\) \[► 599\]](#)):
- ☒ 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* [► 215]).



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* [► 407]).
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.

Transponder - Berechtigungsgruppen

Hier können Sie den Transponder zu Berechtigungsgruppen hinzufügen

1 Details

2 Personendetails

3 Transponderkonfiguration

4 Zusätzliche Schließenlagen

5 Berechtigungsgruppen

6 Hashtags

AUSGEWÄHLT (0)

Name	Beschreibung
------	--------------

NICHT AUSGEWÄHLT (4)

Name	Beschreibung
Gryffindor	
Hufflepuff	
Ravenclaw	
Slytherin	

Neue Berechtigungsgruppe

☐ Weiteres Objekt erstellen

< Zurück

Weiter >

Fertigstellen

Abbrechen

22. Use  to sort/filter the displayed entries if required (see [Sorting and filtering \[► 54\]](#)).
23. Select the required access levels in the right column (Ctrl+click for single groups or Shift+click for multiple groups).
24. Use  to move the selected access levels only or  to move all displayed access levels.
 - ➔ The identification medium is assigned to the highlighted access levels.

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)

Name	Beschreibung
Gryffindor	

NICHT AUSGEWÄHLT (3)

Name	Beschreibung
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)

Name	Beschreibung
------	--------------

NICHT AUSGEWÄHLT (3)

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* [▶ 54]).

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.

15.1.2 Creating PIN code keypads

PIN code keypads allow your users to engage and disengage locking devices using a number code (PIN) (also see *Identification media, locking devices and the locking plan* [► 571]).

In the interests of best practice (see *Best practice: setting up the locking system* [▶ 37]), SimonsVoss recommends that you configure schedules/ time groups first:

- *Creating a schedule* [▶ 63] or *Create time group* [▶ 66] (see *Time groups and schedules* [▶ 587] 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* [▶ 573]).



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* [▶ 245] in the AXM manual).

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

PinCode - Details
Bitte geben Sie die Eigenschaften der PinCode ein.

Hogwarts

1 Details **2 Hashtags**

PINCODE - DETAILS

Typ: G1 PinCode

Name: _____

Schließung: _____

PINs	Pin Name	Zeitgruppe	Berechtigt	Status	Sync	
1	_____	_____	☒	Nicht programmiert		Löschen
2	_____	_____	☐	Nicht programmiert		Hinzufügen
3	_____	_____	☐	Nicht programmiert		Hinzufügen

☐ Weiteres Objekt erstellen < Zurück Weiter > Fertigstellen Abbrechen

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

PINCODE - DETAILS

Typ	AX PinCode
Name	AX PinCode
Schließung	PinCode G1

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.

Schließung	Gryffindor tower
Pinlänge	Gryffindor tower
	Snape's dungeon

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

Pinlänge	6
	4
	5
	6
Name	
ab	
	7
	8
	9
	10

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* [▶ 54]).

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.

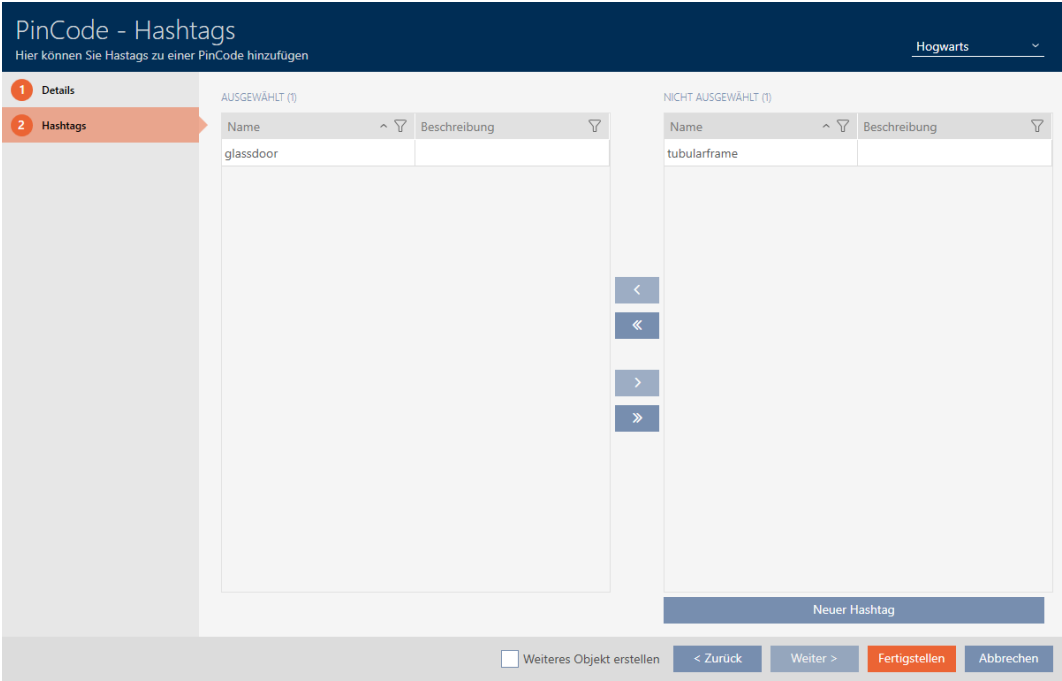


NOTE

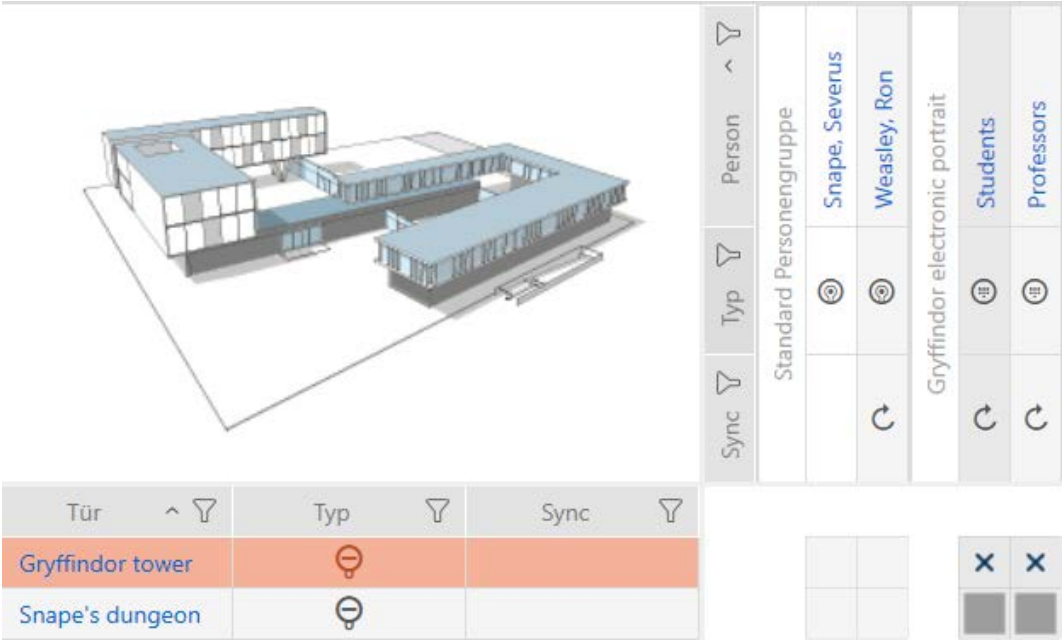
Double-clicking as an alternative to arrow keys

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 Keypad - Details" window closes.
 - ➔ Newly created PIN code is listed or displayed in the matrix.



15.1.3 Creating special identification media

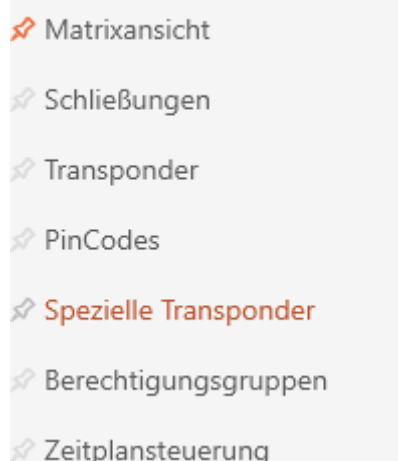
You can assign just one function to a specific identification medium, either Battery replacement or Lock Activation (see *Special identification media and their functions* [▶ 579]). This identification medium can then no longer be used for other purposes in this project.

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

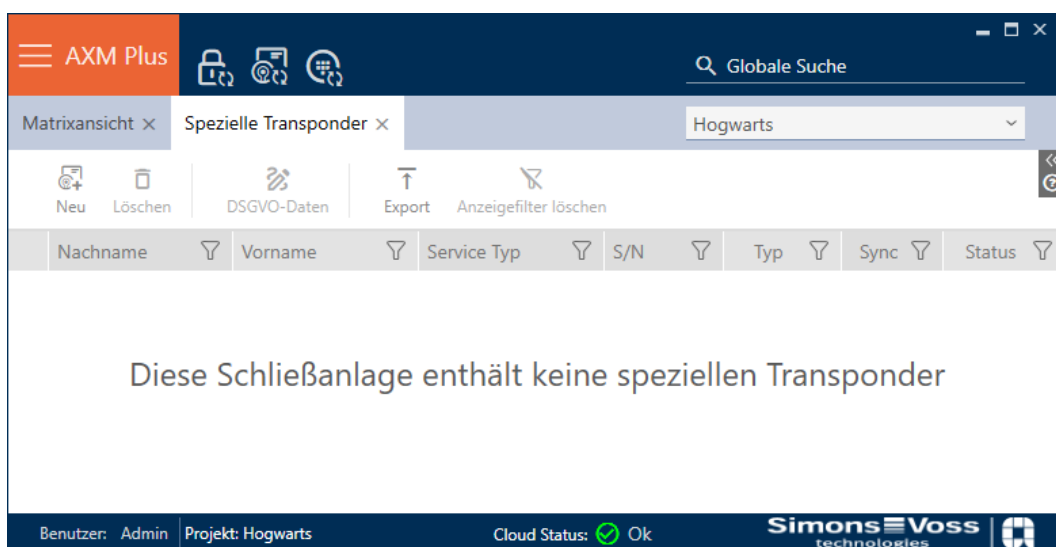


2. Select the **Special Transponders** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLIESANLAGENSTEUERUNG



- ↳ The [Special Transponders] tab will open.



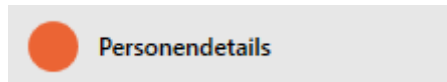
3. Click on the **New** button .
↳ The "Special Transponder" window will open.

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.

Spezieller Transponder - Personen Details

Hier können Sie die Details der Person bearbeiten

Hogwarts

1 Details

2 Personendetails

3 Zusätzliche Schließanlagen

PERSONENDETAILS

Nachname

Vorname

Personalnummer ☒ Auto

Personengruppe Standard Personengruppe + Neu

Bemerkung

Foto

Titel

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

Eingestellt am ☒ Nicht relevant

Eingestellt bis ☒ Nicht relevant

Geburtsdatum ☒ Nicht relevant

Kostenstelle

☐ Weiteres Objekt erstellen

< Zurück Weiter > Fertigstellen Abbrechen



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 \[▶ 491\]](#)).

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.

10. 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.

Personengruppe: Housekeepers

Bemerkung: Standard Personengruppe, Housekeepers

+ Neu

11. 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.
12. If you want to edit the *Hiring date*, *Exit date* or *Date of birth* fields: Deactivate the relevant ☐ Not relevant check box.
13. Use the **Additional locking systems** button to switch to the next tab or complete the entries with the **Finish** button.

Spezieller Transponder - Zusätzliche Schließanlagen

Hier können Sie zusätzliche Schließanlagen für den speziellen Transponder auswählen

Hogwarts

1 Details

2 Personendetails

3 Zusätzliche Schließanlagen

Name

Status

Schließanlage: Hogwarts 2

Hinzufügen Entfernen

☐ Weiteres Objekt erstellen

< Zurück Weiter > Fertigstellen Abbrechen

14. 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 \[► 407\]](#)).
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.

Nachname	Vorname	Service Typ	S/N	Typ	Sync	Status
Filch	Argus	Batteriewechsel				

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

15.1.4 Creating an AX2Go key

See [Assigning keys for AXM Plus and higher \[► 227\]](#).

15.1.5 Import identification media

The import function can be used to create multiple identification media/ persons simultaneously. To do this, you need an import file in CSV or XLSX format. The columns in this file are subsequently assigned to a field in the AXM Plus. A new identification medium (and person) is created with each line, with the fields populated with the contents of the assigned columns.

Ideally, your import file is encoded in **Unicode (UTF-8)** format.

There is a similar function for doors and locking devices: *Importing locking devices* [[▶ 255](#)]

Example file

An example file could look like this:

	A	B	C	D	E	F	G	H
1	Personalnummer	Nachname	Vorname	Abteilung	Gebäude	E-Mail	Eintrittsdatum	Austrittsdatum
2	1	Kühn	Wolfgang	Rezeption	Besuchergebäude	Kühn.Wolfgang@demo-company.de	01.11.2005	
3	2	Müller	Noah	Versand	Halle A	Müller.Noah@demo-company.de	07.09.2022	
4	3	Hausmann	Paul	Lager	Halle A	Hausmann.Paul@demo-company.de	19.01.2010	
5	4	Schäfer	Sarah	Reinigung	Halle A	Schäfer.Sarah@demo-company.de	18.04.2015	
6	5	Weber	Laura	Prozesse	Halle B	Weber.Laura@demo-company.de	04.04.2020	
7	6	Vogel	Dieter	Reinigung	Halle B	Vogel.Dieter@demo-company.de	05.07.2023	01.06.2030
8	7	Bach	Tanja	Produktion	Halle B	Bach.Tanja@demo-company.de	06.05.2019	01.10.2027
9	8	Schmidt	Anke	Produktion	Halle B	Schmidt.Anke@demo-company.de	01.01.2026	
10	9	Bergmann	Gisela	Vorstand	Besuchergebäude	Bergmann.Gisela@demo-company.de	01.05.2021	

- ✓ Selection values (e.g. "Person group"), which appear in the import file, have already been created (see e.g. *Creating a person group* [[▶ 61](#)]).

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



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

SCHLIESSANLAGENSTEUERUNG

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

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

3. Click on the **Import** button.

→ The "Import - Persons" window will open.

Import - Personen
Hier können Sie Personen importieren

Importdatei auswählen

Durchsuchen

Encoding: Unicode (UTF-8)

Trennzeichen: ;

Zeilen überspringen: 0

Import Optionen

Standard-AXM-Optionen für neue Personen

Schließanlage: AXM Plus

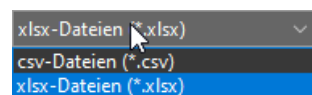
Personengruppe: [Automatisch generiert]

Transponder Typ: Transponder

Spaltenzuordnung

Importieren Abbrechen

4. Click the **Browse** button and navigate to your import file. You may need to set the file type to see your import file.



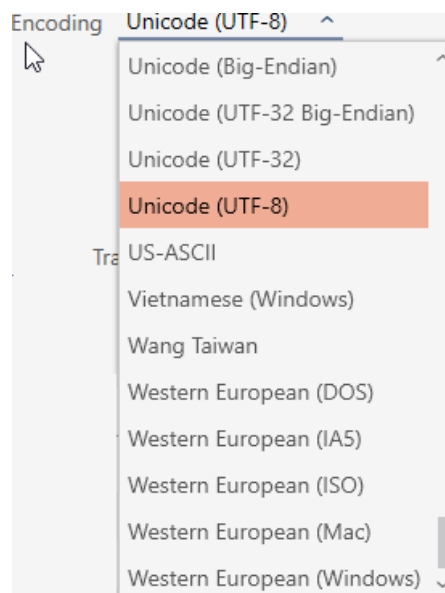
→ Area "Column mapping" is loading.

Spaltenzuordnung

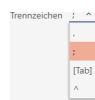
☐	Nein ▾	Nein ▾	Nein ▾	Nein ▾	Nein ▾	Nein ▾	Nein ▾	Nein
☐	1	Kühn	Wolfgang	Rezeption	Besuchergebäude	Kühn.Wolfgang@demo-con	01.11.2005 00:00:00	
☐	2	Müller	Noah	Versand	Halle A	Müller.Noah@demo-comp	07.09.2022 00:00:00	
☐	3	Hausmann	Paul	Lager	Halle A	Hausmann.Paul@demo-con	19.01.2010 00:00:00	
☐	4	Schäfer	Sarah	Reinigung	Halle A	Schäfer.Sarah@demo-comp	18.04.2015 00:00:00	
☐	5	Weber	Laura	Prozesse	Halle B	Weber.Laura@demo-comp	04.04.2020 00:00:00	
☐	6	Vogel	Dieter	Reinigung	Halle B	Vogel.Dieter@demo-comp	05.07.2023 00:00:00	01.06.2030 00:00:00
☐	7	Bach	Tanja	Produktion	Halle B	Bach.Tanja@demo-compa	06.05.2019 00:00:00	01.10.2027 00:00:00
☐	8	Schmidt	Anke	Produktion	Halle B	Schmidt.Anke@demo-comp	01.01.2026 00:00:00	
☐	9	Bergmann	Gisela	Vorstand	Besuchergebäude	Bergmann.Gisela@demo-cc	01.05.2021 00:00:00	

Importieren Abbrechen

5. Select the encoding for your import file from the dropdown menu; ▼ **Encoding** (recommendation: import the file in **Unicode (UTF-8)** format).



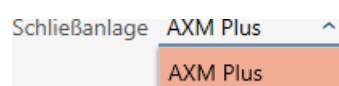
6. Select the delimiter for your import file from the dropdown menu ▼ **Delimiter** (in the example: ;).



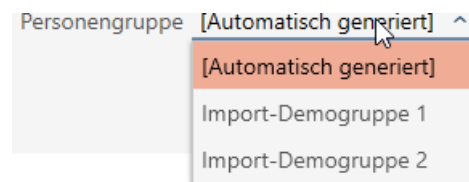
7. In field *Skip rows*, give the number of import file lines that should be skipped (for example, column headings, in the example: 1).

Zeilen überspringen 1

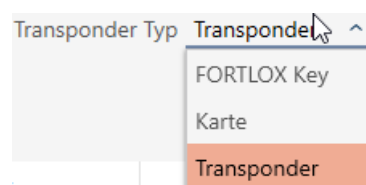
8. Open the dropdown menu ▼ **Locking system** and select the target locking system .



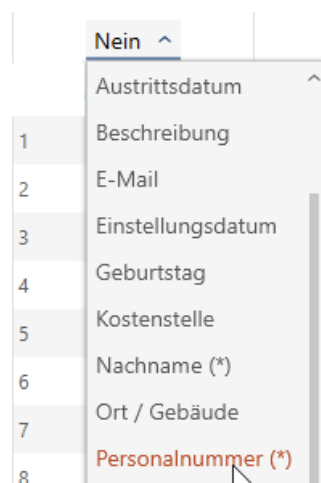
9. Open the dropdown menu ▼ **Person group** and select the target group of people to whom you want to import your identification media.



10. Open the dropdown menu ▼ **Transponder type** and select the type of identification medium you want to create with the import.



11. Each column has a drop-down menu above it. Use this drop-down menu to select the field in the identity media details into which you want to import the entry in this column. If you select the entry "None", the column will be ignored and not imported.
The entries "Last name (*)" and "Personnel number (*)" must be selected as these fields are mandatory (*) fields.



NOTE

Values to be imported must be selected before importing

Fields such as "Person group" are selectable values. Only existing values may be selected for import; new values cannot be created.

If a selection value is not available, the field is skipped during import.

- Create all required values before importing.

- Columns are assigned to the fields as per the identification media details.

Spaltenzuordnung

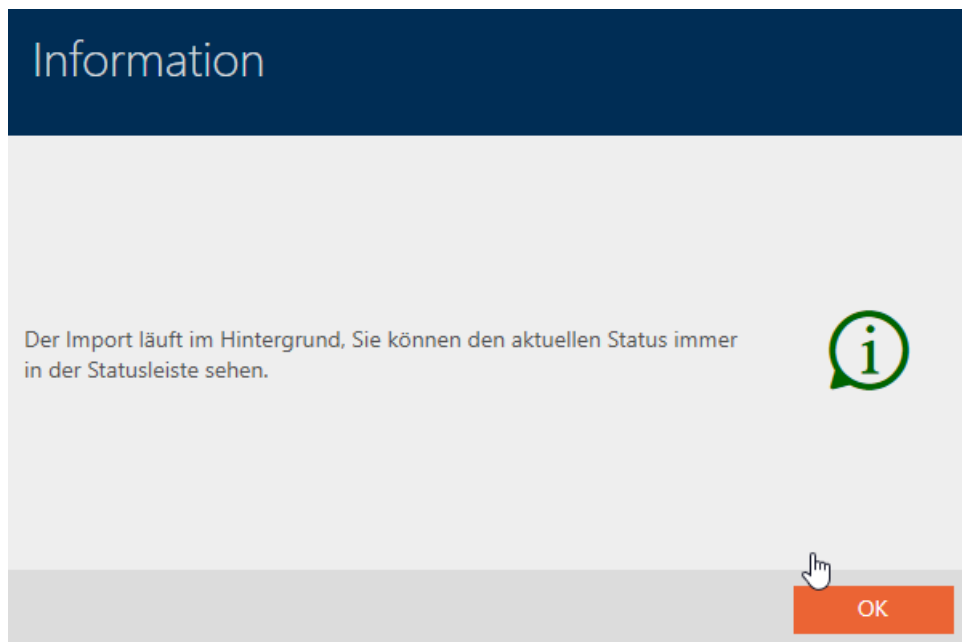
☐	Personalnummer ▾	Nachname (*) ▾	Vorname ▾	Abteilung ▾	Ort / Gebäude ▾	E-Mail ▾	Einstellungsdatum ▾	Austrittsdat
☐	1	Kühn	Wolfgang	Rezeption	Besuchergebäude	Kühn.Wolfgang@demo-cor	01.11.2005 00:00:00	
☐	2	Müller	Noah	Versand	Halle A	Müller.Noah@demo-comp	07.09.2022 00:00:00	
☐	3	Hausmann	Paul	Lager	Halle A	Hausmann.Paul@demo-cor	19.01.2010 00:00:00	
☐	4	Schäfer	Sarah	Reinigung	Halle A	Schäfer.Sarah@demo-comp	18.04.2015 00:00:00	
☐	5	Weber	Laura	Prozesse	Halle B	Weber.Laura@demo-comp	04.04.2020 00:00:00	
☐	6	Vogel	Dieter	Reinigung	Halle B	Vogel.Dieter@demo-comp	05.07.2023 00:00:00	01.06.2030 00:00:00
☐	7	Bach	Tanja	Produktion	Halle B	Bach.Tanja@demo-company	06.05.2019 00:00:00	01.10.2027 00:00:00
☐	8	Schmidt	Anke	Produktion	Halle B	Schmidt.Anke@demo-comp	01.01.2026 00:00:00	
☐	9	Bergmann	Gisela	Vorstand	Besuchergebäude	Bergmann.Gisela@demo-cc	01.05.2021 00:00:00	

12. Mark all the lines you want to import.

☒	Personalnummer ▾	Nachname (*) ▾	Vorname ▾	Abteilung ▾	Ort / Gebäude ▾	E-Mail ▾	Einstellungsdatum ▾	Austrittsdat
☒	1	Kühn	Wolfgang	Rezeption	Besuchergebäude	Kühn.Wolfgang@demo-cor	01.11.2005 00:00:00	
☒	2	Müller	Noah	Versand	Halle A	Müller.Noah@demo-comp	07.09.2022 00:00:00	
☒	3	Hausmann	Paul	Lager	Halle A	Hausmann.Paul@demo-cor	19.01.2010 00:00:00	
☒	4	Schäfer	Sarah	Reinigung	Halle A	Schäfer.Sarah@demo-comp	18.04.2015 00:00:00	
☒	5	Weber	Laura	Prozesse	Halle B	Weber.Laura@demo-comp	04.04.2020 00:00:00	
☒	6	Vogel	Dieter	Reinigung	Halle B	Vogel.Dieter@demo-comp	05.07.2023 00:00:00	01.06.2030 00:00:00
☒	7	Bach	Tanja	Produktion	Halle B	Bach.Tanja@demo-company	06.05.2019 00:00:00	01.10.2027 00:00:00
☒	8	Schmidt	Anke	Produktion	Halle B	Schmidt.Anke@demo-comp	01.01.2026 00:00:00	
☒	9	Bergmann	Gisela	Vorstand	Besuchergebäude	Bergmann.Gisela@demo-cc	01.05.2021 00:00:00	

13. Click the **Import** button.

- Import begins.



- Once the import is concluded, the imported identification media/persons can be viewed in the list of identification media:

Nachname	Vorname	S/N	Typ	Sync	Status
Bach	Tanja		⊙	↻	
Bergmann	Gisela		⊙	↻	
Hausmann	Paul		⊙	↻	
Kühn	Wolfgang		⊙	↻	
Müller	Noah		⊙	↻	
Nachname	Vorname		⊙	↻	
Schmidt	Anke		⊙	↻	
Schäfer	Sarah		⊙	↻	
Vogel	Dieter		⊙	↻	
Weber	Laura		⊙	↻	

The details you have entered, including the automatically generated person group, can be viewed in the person details of the imported persons:

DSGVO-Daten ⚙️

PERSONENDETAILS

Nachname

Vorname

Personalnummer

Personengruppe + Neu

Bemerkung

Foto 

Titel

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

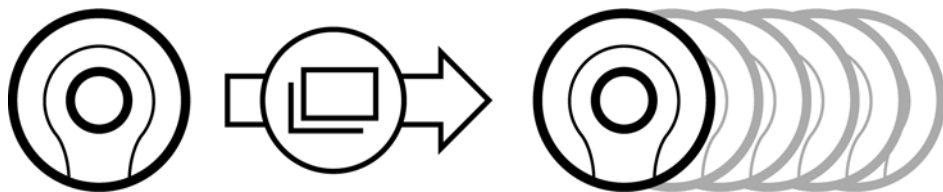
Eingestellt am ☐ Nicht relevant

Eingestellt bis ☐ Nicht relevant

Geburtsdatum ☒ Nicht relevant

Kostenstelle

15.2 Duplicating an identification medium (including authorisations and settings)



Instead of creating a new identification medium, you can simply duplicate an existing identification medium. During this process, AXM 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 \[► 491\]](#))

- 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.



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

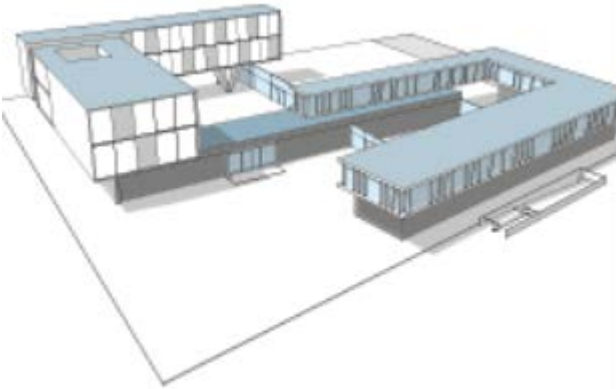
Transponder duplizieren

Hier können Sie die Anzahl der Kopien eingeben

Wie viele Kopien des ausgewählten Transponders sollen erstellt werden?

OKAbbrechen

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



Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

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

✕

✕

✕

✕

✕

✕

15.3 Deleting an identification medium

15.3.1 Deleting a card/transponder

There are two ways to delete identification media:

- 1. Delete on the matrix screen (*Deleting individual identification media in the matrix [▶ 125]*)
- 2. Delete using the tab for identification media (*Deleting multiple identification media using the tab [▶ 126]*)

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



NOTE

Deleted identification media in locking devices still known/authorised

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

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

15.3.1.1 Deleting individual identification media in the matrix

- ✓ Matrix screen open.
- ✓ The identification medium to be deleted is unprogrammed or reset (see *Resetting cards/transponders* [▶ 442] about resetting).

1. Select the identification medium you wish to delete.

Typ	Person
	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.

Objekte löschen

Wollen Sie die ausgewählten Objekte löschen?



Ja
Nein

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	

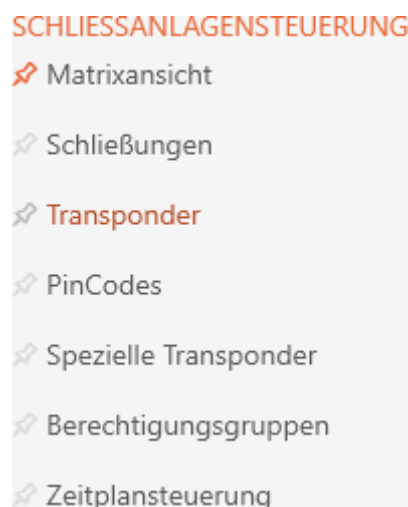
15.3.1.2 Deleting multiple identification media using the tab

- ✓ Identification media to be deleted are unprogrammed or reset (see [Resetting cards/transponders \[► 442\]](#) about resetting).

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

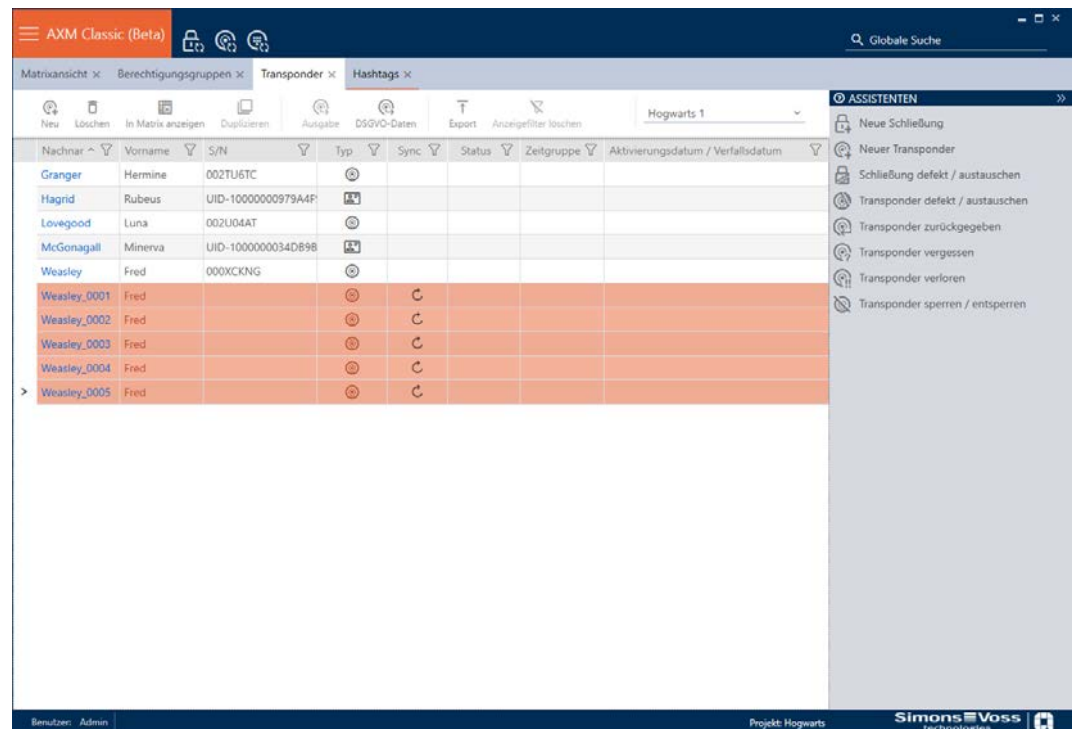


2. Select the **Transponder** entry in the | LOCKING SYSTEM CONTROL | group.

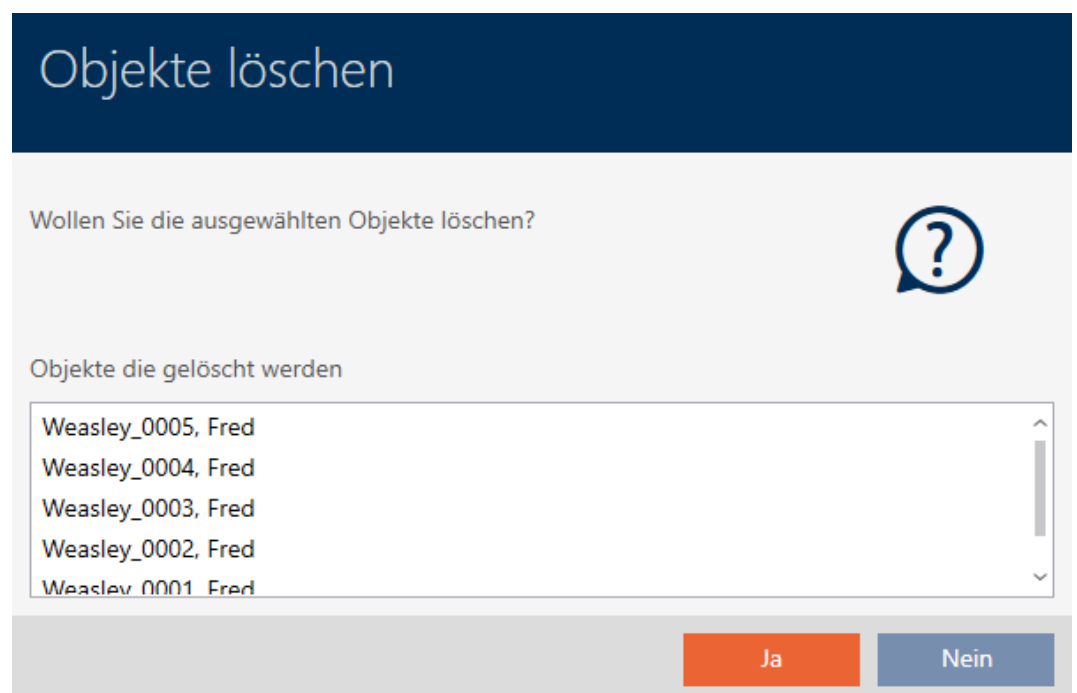


- ↳ The AXM bar will close.
- ↳ The [Transponder] tab will open.

3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
4. Select all identification media that you wish to delete (Ctrl+click for single media or Shift+click for multiple media).



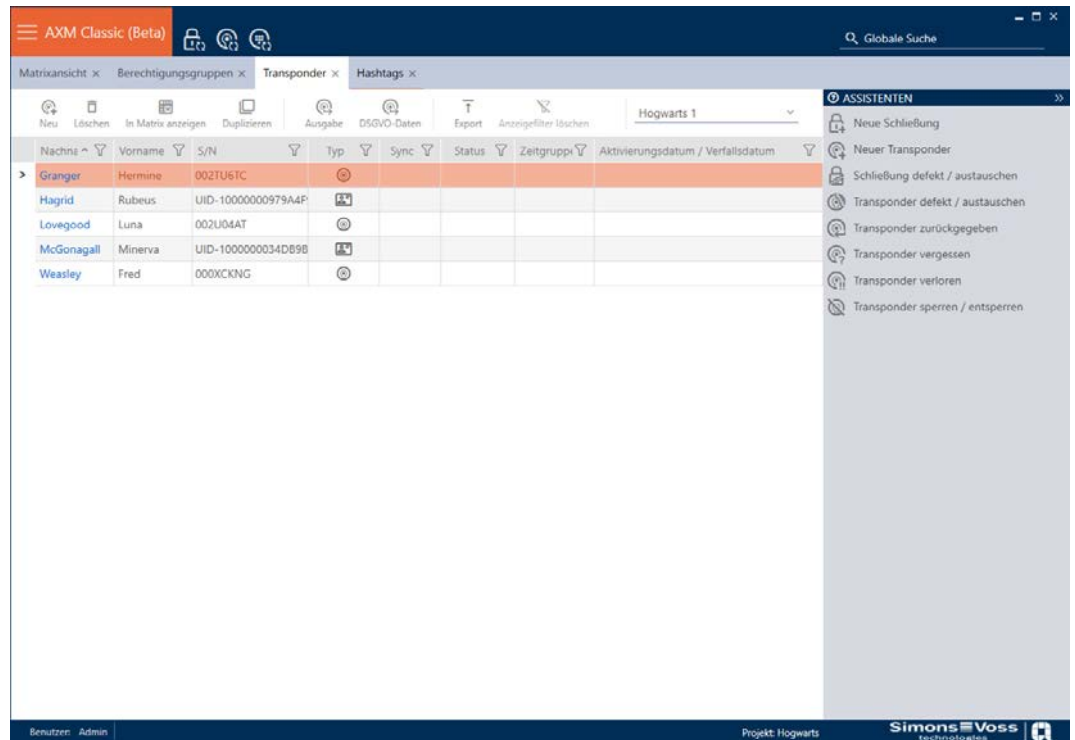
5. Click on the **Delete** button .
 - ➔ Confirmation dialogue with a list of identification media to be deleted will open.



6. Click on the **Yes** button.

↳ Confirmation dialogue with list of identification media to be deleted closes.

↳ Identification media are now deleted.



NOTE

Deleted identification media in locking devices still known/authorised

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

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

15.3.2 Deleting a PIN (PIN code keypad AX)



NOTE

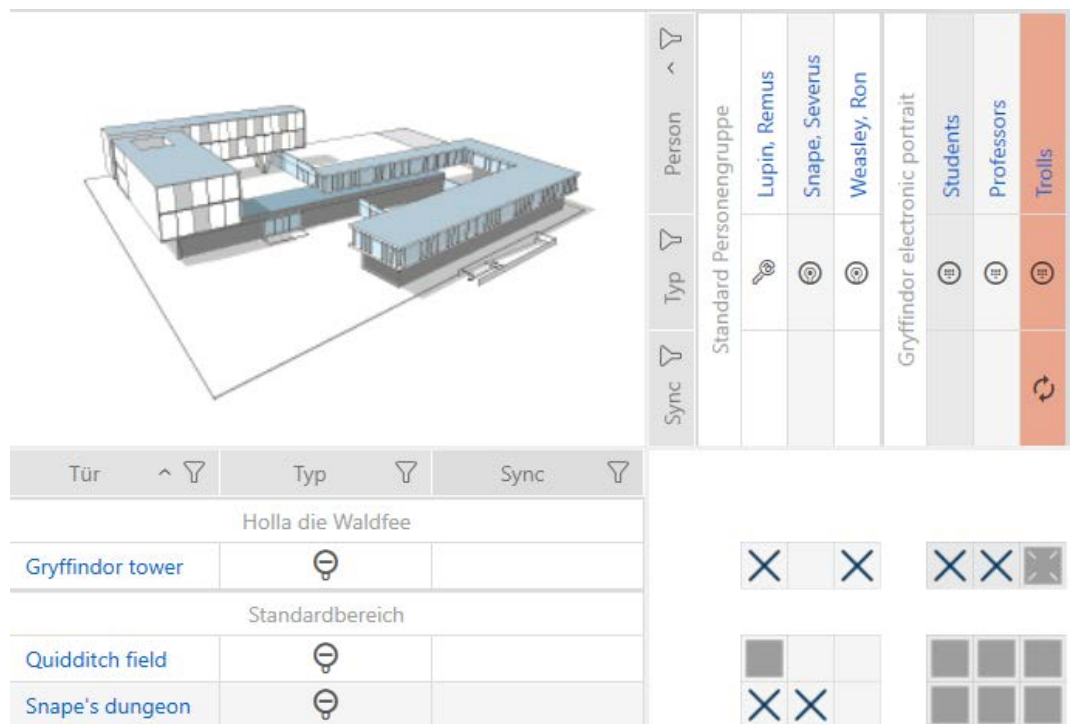
Description only valid for PIN code keypad AX

The setting described here is only available for the PIN code keypad AX in 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* [▶ 106]).
1. Click on any PIN to open details on your PIN code keypad AX.
 - ↳ The "PinCode Keypad - Details" window will open.

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

4. Click on the **Finish** button.
 - ↳ Deleted PIN is shown with greyed-out authorisation and programming requirement in the matrix.



The deleted PIN will disappear after synchronisation.

15.3.3 Blocking an AX2Go key

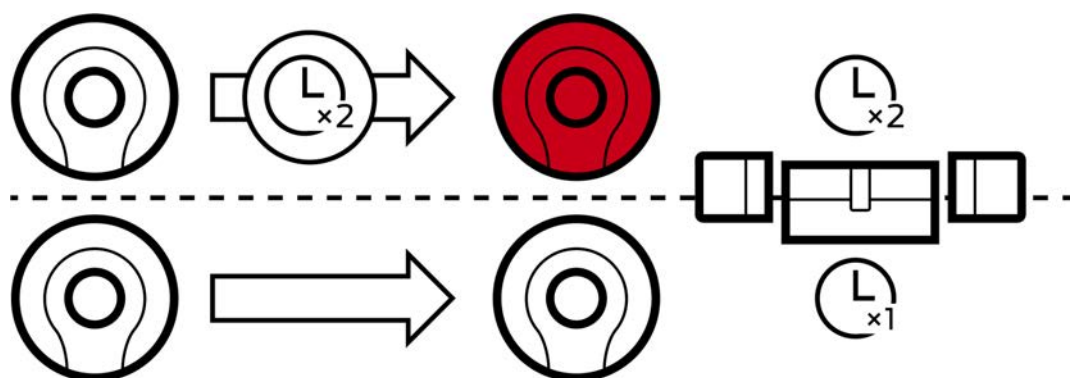
See [Revoking an AX2Go key \[233\]](#).

15.4 Allowing an identification medium to open twice as long

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

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

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



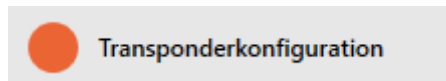
The maximum engagement interval remains 25 s:

- 5 s changes to 10 s
- 10 s changes to 20 s

❑ But 20 s changes to 25 s

✓ 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.

A screenshot of the "Transponder - Konfiguration" web interface. The title bar is dark blue with "Transponder - Konfiguration" and "Hier können Sie den Transponder konfigurieren". On the right are "Synchronisieren" and "In Matrix anzeigen" buttons. A left sidebar contains a list of steps: 1 Details, 2 Personendetails, 3 Transponderkonfiguration (highlighted), 4 Zusätzliche Schließanlagen, 5 Berechtigungsgruppen, 6 Hashtags, 7 Aktionen, 8 Begehungsliste, and 9 Berechtigte Schließungen. The main area is titled "ÖFFNUNGSKONFIGURATIONEN" and contains three sections: "ÖFFNUNGSKONFIGURATIONEN" with checkboxes for "Langes Öffnen" (unchecked), "Akustisches Öffnungssignal" (checked), and "Begehungsliste" (unchecked); "DYNAMISCHES ZEITFENSTER" with radio buttons for "Zeitfenster am Gateway nicht verändern" (selected), "bis zu einer bestimmten Uhrzeit des (nächsten) Tages", and "Stundenanzahl ab der letzten vollen Std. der Buchung"; and "AKTIVIERUNG" with a checked checkbox for "ab sofort". Below is a "VERFALLSDATUM" section with a checked checkbox for "ohne Verfallsdatum". At the bottom are buttons: "< Zurück", "Weiter >", "Fertigstellen" (highlighted in orange), and "Abbrechen".

3. Activate the ☐ Long opening checkbox.

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

↳ The identification medium window closes.

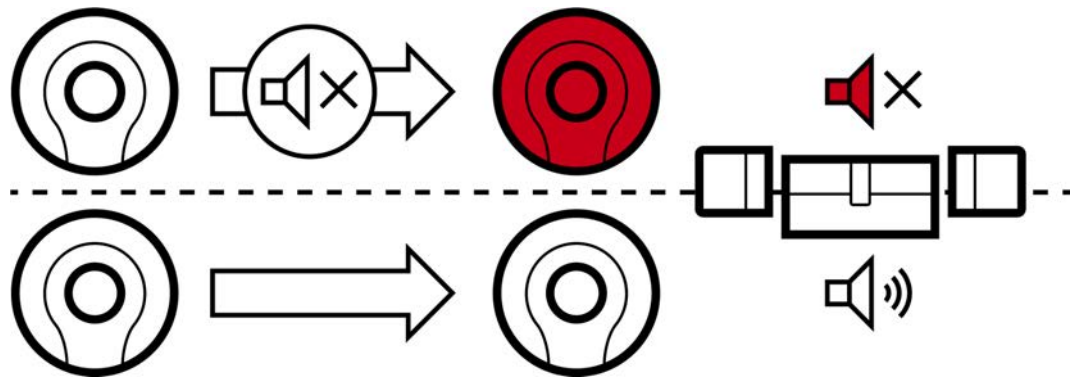
↳ All locking devices will now open twice as long for this identification medium.

15.5 Muting all locking devices for an identification medium

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

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

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



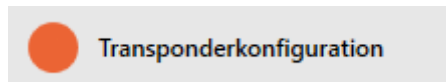
This means

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

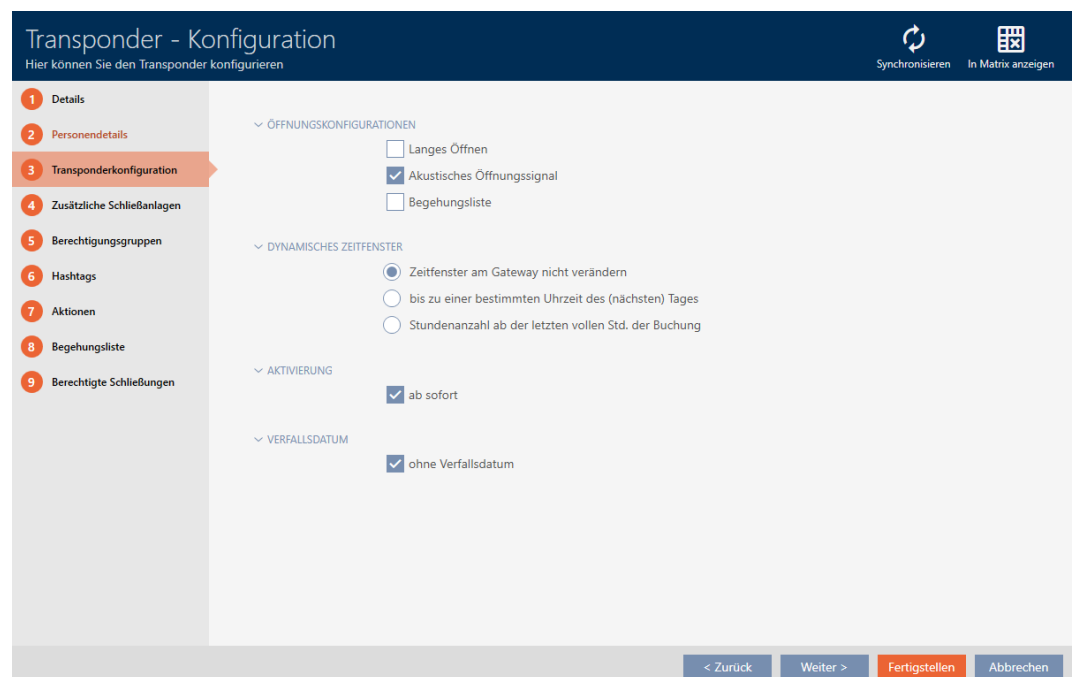
15.5.1 Muting all locking devices for a transponder or a card

✓ Identification medium available.

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



↳ Window switches to the "Transponder configuration" tab.

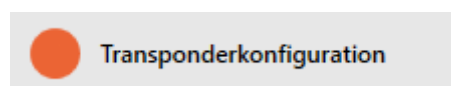


3. Activate the ☐ Acoustic opening signal checkbox.
4. Click on the **Finish** button.
 - ↳ The identification medium window closes.
 - ↳ All locking devices are now muted for this identification medium.

15.5.2 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.

2. Click on the **Transponderkonfiguration** tab.



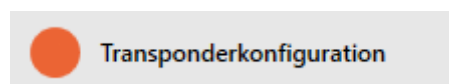
- ↳ Window switches to the "Transponder configuration" tab.

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

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

This is where you can switch on the physical access list. This means that your identification medium logs which locking devices it has activated (also see [Access and physical access lists \[► 586\]](#)).

- ✓ Identification medium available.
1. Click on the identification medium whose physical access list you wish to activate.
 - ↳ The identification medium window will open.
 2. Click on the **Transponderkonfiguration** tab.



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

3. Activate the ☒ Personal audit trail checkbox.
4. Click on the **Finish** button.
 - ➞ The identification medium window closes.
 - ➞ Identification medium will now write which locking devices it has activated in the physical access list.

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

You control an identification medium's authorisations with a time group. The time group is a time management component (see [Event management \[► 587\]](#)). See [Create time group \[► 66\]](#) and [Adding identification medium to time group \[► 359\]](#) to set up time management for identification media.

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

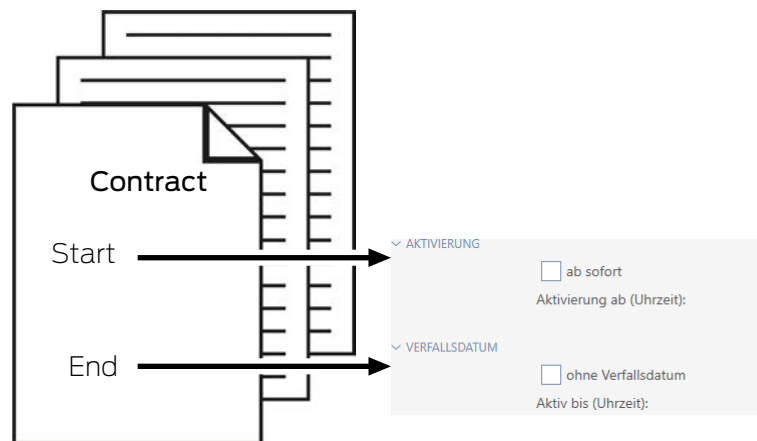
Your AXM Plus recognises two points in time for identification media:

- 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.:

Warnung

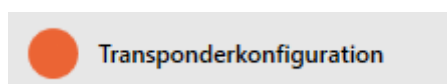
Das Verfallsdatum liegt in der Vergangenheit
Möchten Sie den Vorgang fortsetzen?



JaNein

✓ 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.

Transponder - Konfiguration

Hier können Sie den Transponder konfigurieren

1 Details

2 Personendetails

3 **Transponderkonfiguration**

4 Zusätzliche Schließanlagen

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungsliste

9 Berechtigte Schließungen

ÖFFNUNGSKONFIGURATIONEN

☐ Langes Öffnen

☒ Akustisches Öffnungssignal

☐ Begehungsliste

DYNAMISCHES ZEITFENSTER

☒ Zeitfenster am Gateway nicht verändern

☐ bis zu einer bestimmten Uhrzeit des (nächsten) Tages

☐ Stundenzahl ab der letzten vollen Std. der Buchung

AKTIVIERUNG

☒ ab sofort

VERFALLSDATUM

☒ ohne Verfallsdatum

< Zurück

Weiter >

Fertigstellen

Abbrechen

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

▼ AKTIVIERUNG

☒ ab sofort

▼ VERFALLSDATUM

☒ ohne Verfallsdatum

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

▼ AKTIVIERUNG

☐ ab sofort

Aktivierung ab (Uhrzeit):

▼ VERFALLSDATUM

☒ ohne Verfallsdatum

30.05.2021  00:00 ▼

+ 1 + 3 + 5

< 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

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

▼ VERFALLSDATUM

☐ ohne Verfallsdatum

Aktiv bis (Uhrzeit):

29.05.2021  00:00 ▼

+ 1 + 3 + 5

< 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

8. Click on the **Finish** button.

↳ The identification medium window closes.

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

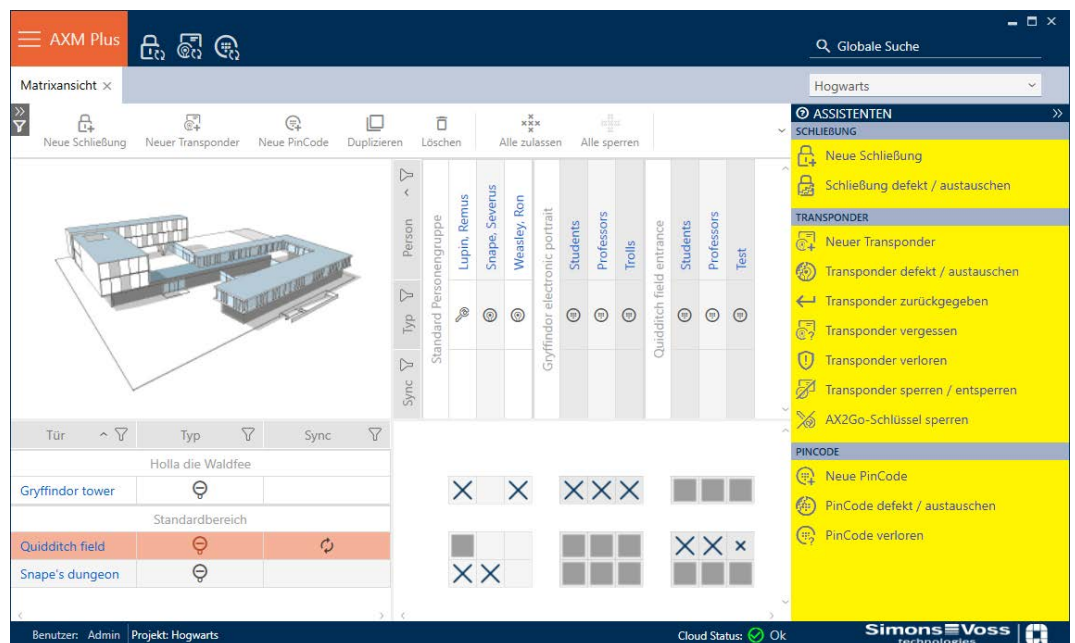
15.9 Handling defective identification media

Identification media can suffer from defects:

■ Software defect

■ Hardware defect

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



If the identification medium has been lost or stolen, you must block it (see *Blocking and replacing lost/stolen card/transponder permanently* [▶ 177]).

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* [▶ 571]).

Transponders/replacement transponders are required again immediately:

Suitable for:

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

Example situation:

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

Procedure:

Re-synchronise (repair)	Resetting and replacing	Delete and replace
<i>Repairing a card/transponder (resynchronising) [► 142]</i> - Reset (= TID available in database again) - Resynchronise (= TID is immediately written back onto the same identification medium) The identification medium functions as before after it is repaired.	<i>Resetting and replacing a card/transponder [► 147]</i> - Reset (= TID flagged as defective in database and removed from original identification medium) - Synchronise replacement identification medium with new TID After the reset, the TID is no longer contained in the identification medium. The identification medium can therefore no longer be used. However, it can be re-synchronised. A new TID is written onto the identification medium.	<i>Deleting and replacing a card/transponder [► 150]</i> - Delete (= TID flagged as defective in database) and removed from project - Synchronise replacement identification medium with the new TID It is obviously not possible to reset a permanently damaged identification medium because it is no longer accessible. This means the TID remains in the identification medium. Deleting allows you to "clean up" your project. The TID marked as "defective" will remain permanently stored in the database regardless and will not be re-assigned. You can also hide defective or disabled identification media as an alternative to deletion (see <i>Hiding deactivated and defective identification media [► 484]</i>).

Transponder/replacement transponder is not required:

Suitable for:

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

Example situation:

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

Procedure:

Taking out of use and leaving in project	Taking out of use and deleting from project
<i>Take card/transponder out of use and leave in project [► 158]</i> Flag as taken out of operation (= TID flagged as defective in database) The permanently damaged identification medium retains its TID but the TID is flagged as "defective". New identification media cannot be created with this TID. This means that the same TID cannot be brought into circulation twice.	<i>Taking a card/transponder out of use and deleting it from project [► 165]</i> Delete (= TID flagged as defective in database) and removed from project Deleting allows you to "clean up" your project. The TID marked as "defective" will remain permanently stored in the database regardless and will not be reassigned. You can also hide defective or disabled identification media as an alternative to deletion (see <i>Hiding deactivated and defective identification media [► 484]</i>).

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 keypad (see *Repairing a PIN code keypad (resynchronising) [► 143]*)
- Reset and Replace PinCode keypad (manual; not via wizard - see *Resetting and replacing a PIN code keypad [► 150]*)
- Delete and Replace PinCode keypad (see *Deleting and replacing a PIN code keypad [► 153]*)

- Decommission PinCode keypad and leave in the project (see *Taking a PIN code keypad out of use and leaving it in project* [► 161])
- Decommission PinCode keypad and remove from project (see *Taking a PIN code keypad out of use and deleting it from project* [► 167])

15.9.1 Repairing/resynchronising

15.9.1.1 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* [► 54]).
 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  Repair transponder.

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

→ Identification medium is being reset.

Transponder defekt - Assistent

Schließanlage

Hogwarts 1

Transponder

Weasley, Fred (000XCKNG)

Programmiergerät

SmartCD aktiv (beschäftigt)

TRANSPONDER INSTAND SETZEN



Transponder wird zurückgesetzt

Abbrechen



Verbindung aufgebaut



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

Weiter

Schließen

→ Identification medium is synchronised.

→ Identification medium has been resynchronised with the same settings.

TRANSPONDER INSTAND SETZEN

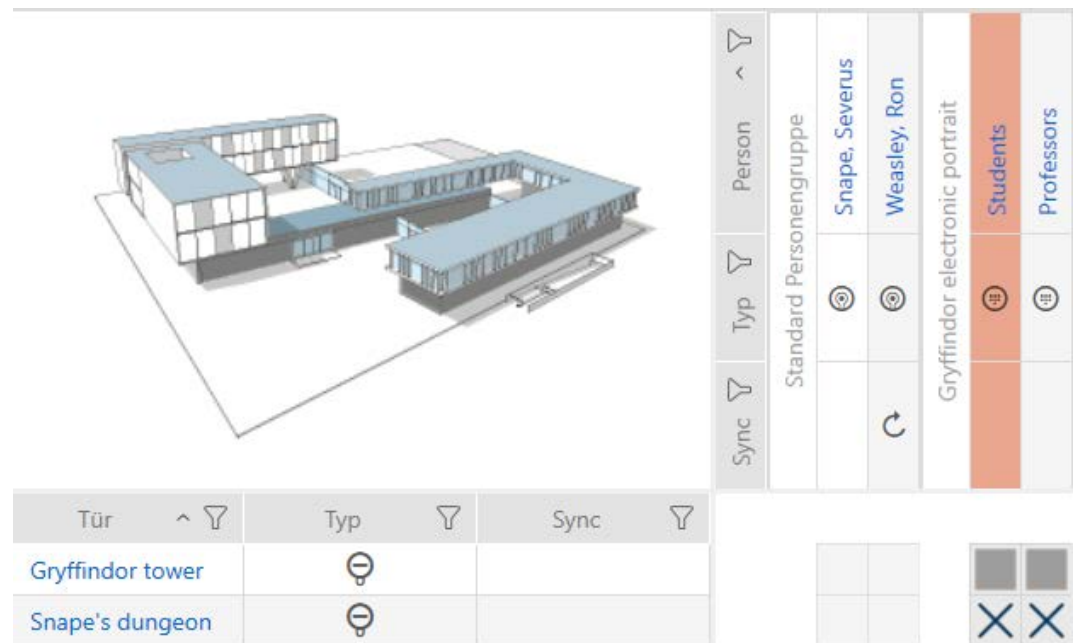
Die Aktion wurde erfolgreich durchgeführt

15.9.1.2 Repairing a PIN code keypad (resynchronising)

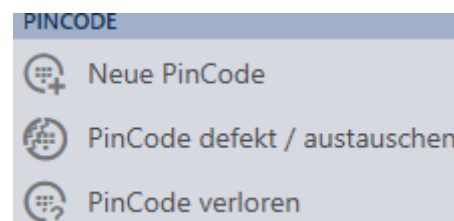
- ✓ List with PIN code keypads or matrix open.
- ✓ PIN code keypad at hand.
- ✓ Suitable programming device connected.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

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



- Click the  PinCode Keypad 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 keypad.

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.

WeiterSchließen

5. Click on the **Next** button.
- ➞ PIN code keypad is reset.

PinCode defekt / austauschen - Assistent

Schließanlage
Hogwarts
▼

PinCode
🔒 Gryffindor electronic portrait (0873CDF)
▼

Programmiergerät
🔌 SmartStick AX
▼

PINCODE INSTAND SETZEN



Synchronisierung

PinCode konfigurieren

Abbrechen


Verbindung aufgebaut



Bitte halten Sie zwischen Programmiergerät und Schließung einen Abstand von nicht mehr als 1m bis die Programmierung abgeschlossen ist

Weiter

Schließen

6. Follow the instructions.

➞ PIN code keypad has been resynchronised with the same settings.

PINCODE INSTAND SETZEN

Die Aktion wurde erfolgreich durchgeführt

15.9.2 Resetting and replacing

15.9.2.1 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* [▶ 54]).
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 **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

15.9.2.2 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* [► 442]).
 2. Create a new PIN code keypad (see *Creating PIN code keypads* [► 106]).
 3. Synchronise the new PIN code keypad (see *Synchronising a PIN code keypad* [► 433]).

15.9.3 Delete and replace

15.9.3.1 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* [► 54]).
 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.

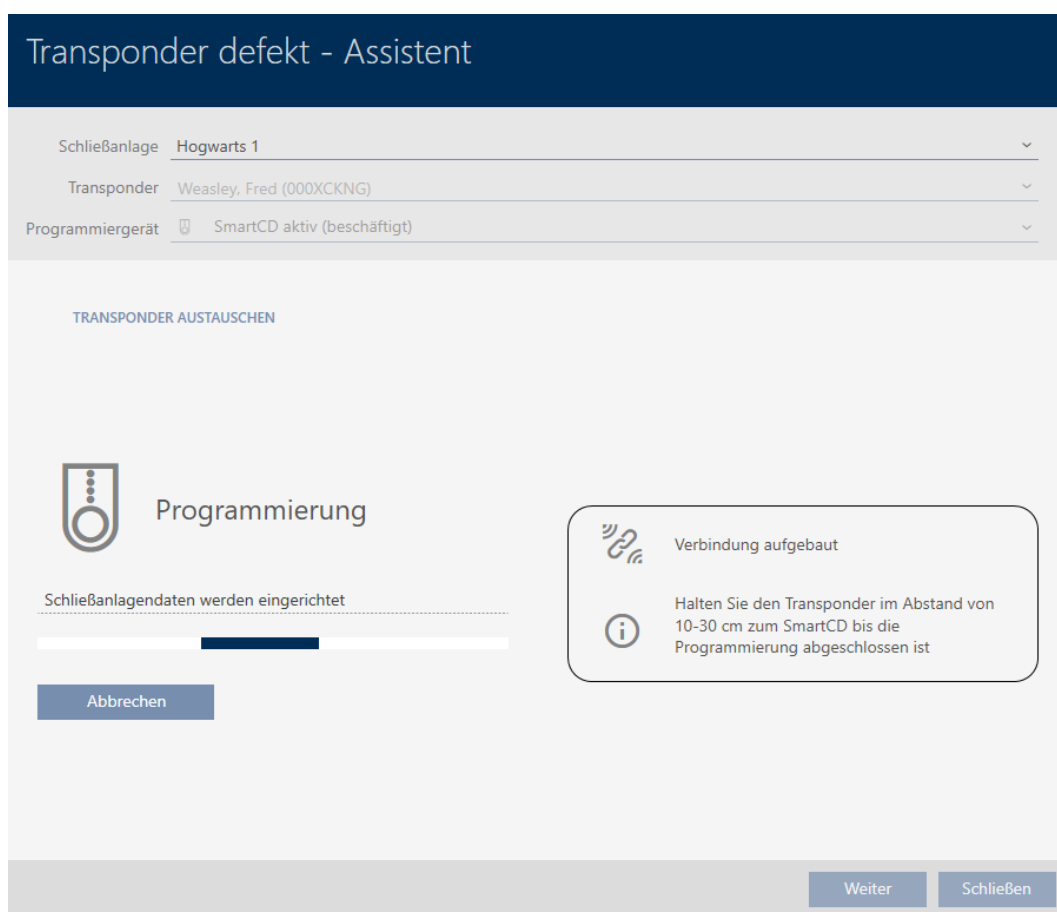
TRANSPONDER AUSTAUSCHEN

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

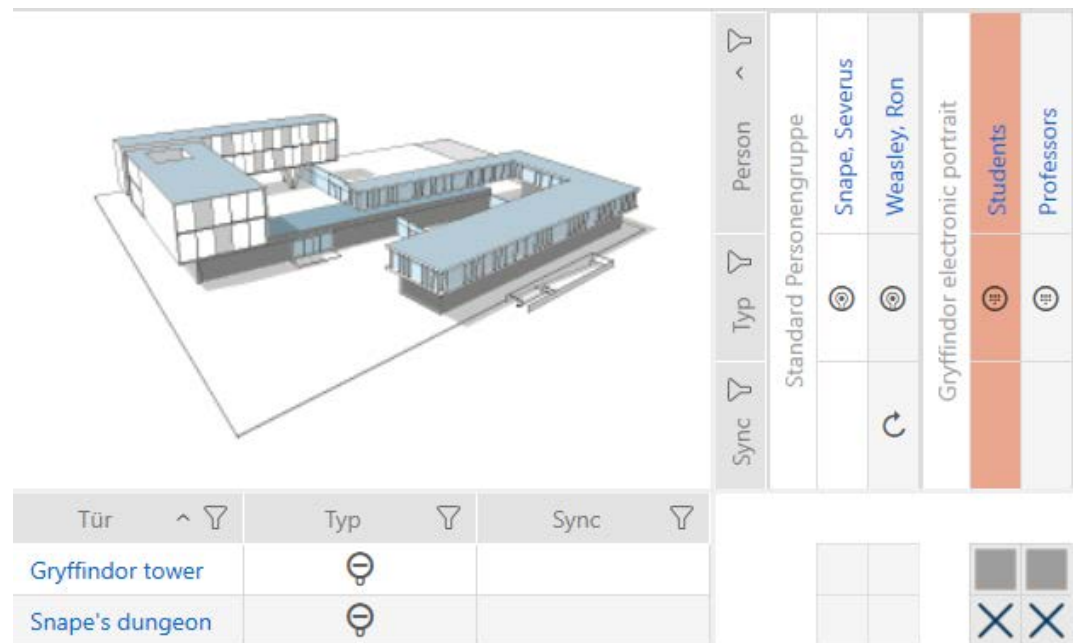
You can now reset the identification medium (see *Deleting an identification medium* [▶ 124]).

15.9.3.2 Deleting and replacing a PIN code keypad

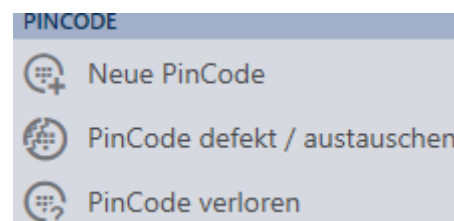
- ✓ List with PIN code keypads or matrix open.
- ✓ Replacement PIN code keypad at hand.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

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



- Click the  PinCode Keypad 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  Replace PinCode keypad.

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 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.

WeiterSchließen

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.



JaNeinAbbrechen

6. Click on the **Yes** button.

→ Synchronisation of the replacement PIN code keypad is being prepared.

PinCode defekt / austauschen - Assistent

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

PINCODE AUSTAUSCHEN

Bitte halten Sie die Ersatz-PinCode bereit.

Die PinCode wird in der Software von den Daten der defekten PinCode bereinigt.

Die Programmierung der Ersatz-PinCode wird automatisch gestartet.

WeiterSchließen

7. Click on the **Next** button.

→ The replacement PIN code keypad is now synchronised.

PinCode defekt / austauschen - Assistent

Schließanlage

Hogwarts

PinCode

Gryffindor electronic portrait (0873CDF)

Programmiergerät

SmartStick AX

PINCODE AUSTAUSCHEN



Synchronisierung

PinCode konfigurieren

Abbrechen



Verbindung aufgebaut



Bitte halten Sie zwischen Programmiergerät und Schließung einen Abstand von nicht mehr als 1m bis die Programmierung abgeschlossen ist

Weiter

Schließen

→ The PIN code keypad has been replaced.

PINCODE AUSTAUSCHEN
Die Aktion wurde erfolgreich durchgeführt

15.9.4 Take out of use and leave in project

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

✓ Identification media list or matrix open.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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 **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

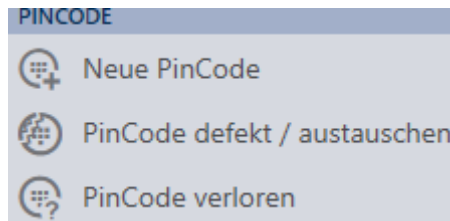
Identification media that have been taken out of use but not deleted can be identified in the matrix:

Sync	Type	Person
		Weasley, Ron
		Weasley, Percy
		Weasley, Fred
		Lovegood, Luna

15.9.4.2 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* [► 54]).
- 2. Flag a PIN associated with the defective PIN code keypad.

3. Click the  PinCode Keypad 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 keypad.

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.

WeiterSchließen

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?

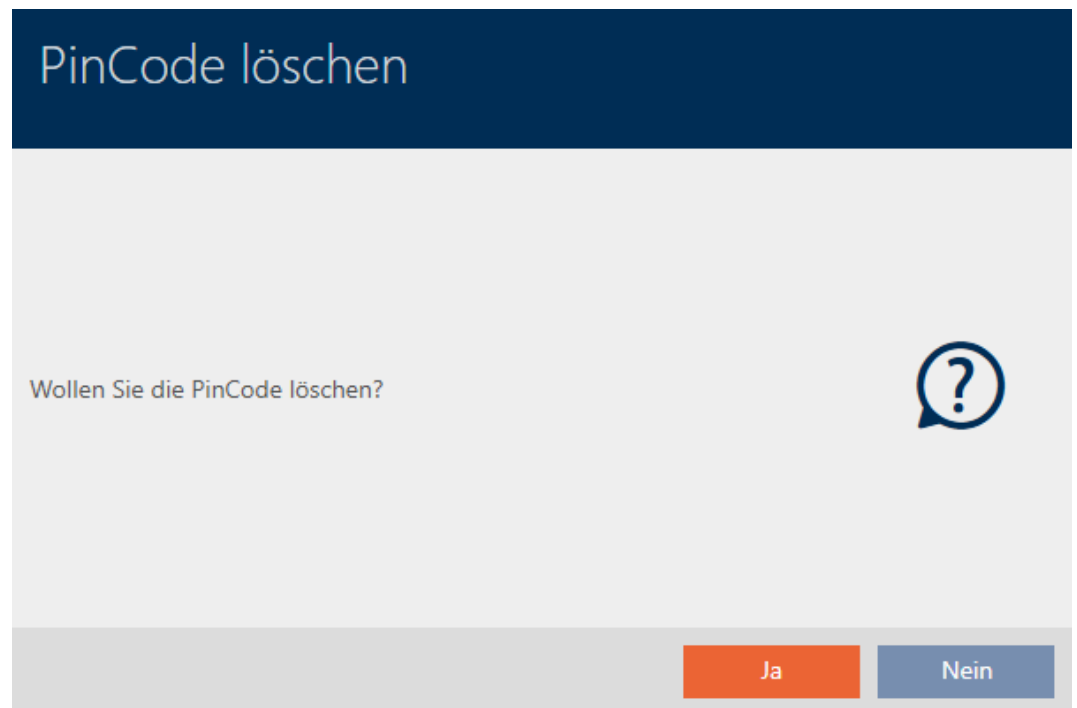
Sind Sie sicher das die PinCode physikalisch defekt ist?

JaNein

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.

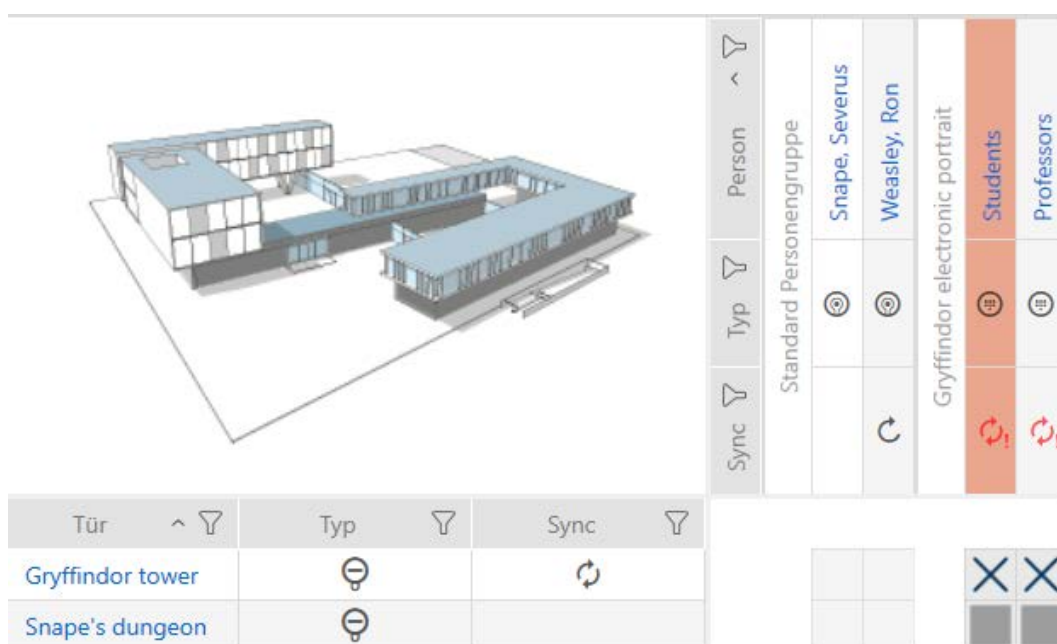
↳ Confirmation dialogue to delete the PIN code keypad closes.

↳ 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:



15.9.5 Taking out of use and deleting from the project

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

✓ Identification media list or matrix open.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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

- Select the option ☒ Decommission transponder.
- 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

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



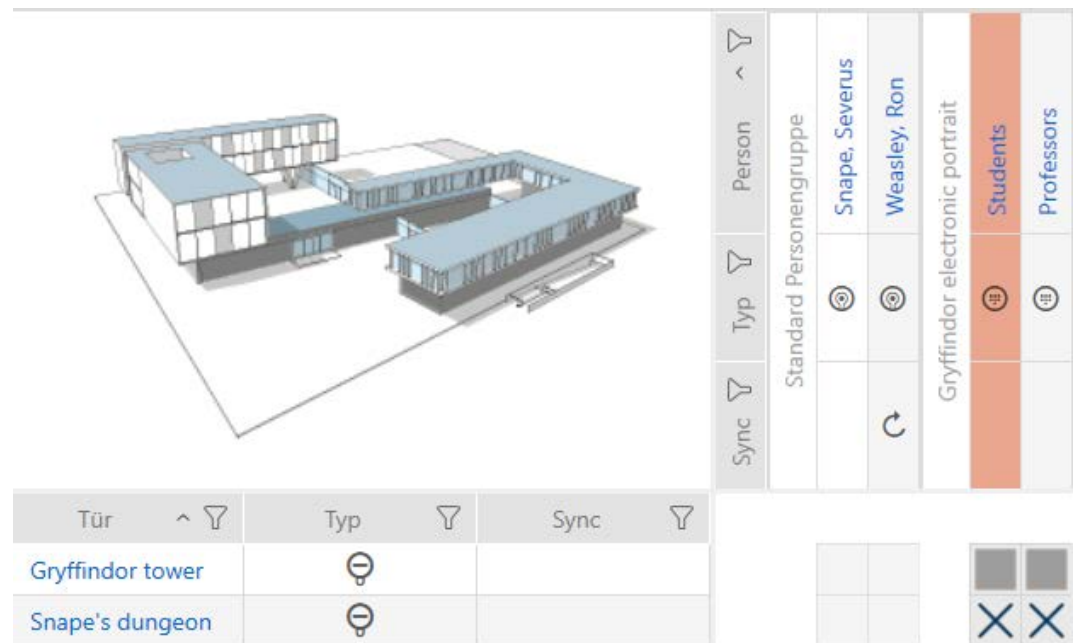
7. Click on the **Yes** button.
 - ↳ Confirmation dialogue to delete the identification medium closes.
 - ↳ Identification medium is deleted without replacement.

TRANSPONDER AUßER BETRIEB NEHMEN
Die Aktion wurde erfolgreich durchgeführt

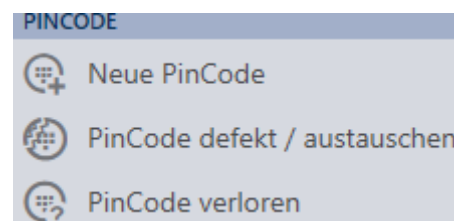
15.9.5.2 Taking a PIN code keypad out of use and deleting it from project

- ✓ List with PIN code keypads or matrix open.
- 1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

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



- Click the  PinCode Keypad 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 keypad.

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.

WeiterSchließen

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

PinCode außer Betrieb nehmen

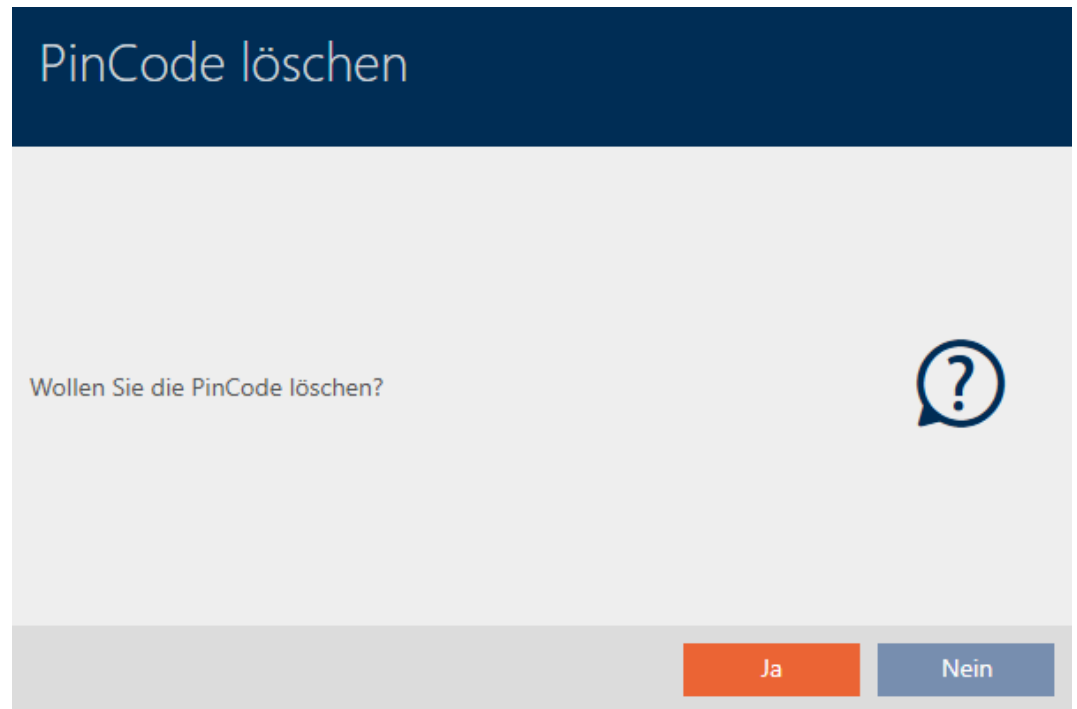
Bitte prüfen Sie zuerst folgendes:

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

Sind Sie sicher das die PinCode physikalisch defekt ist?

JaNein

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

15.10 Duplicating forgotten identification medium temporarily



15.10.1 Duplicating a forgotten transponder or card temporarily

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

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

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

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

The duplicate receives a different TID and is thus a separate identification medium from a locking device perspective (see *Identification media, locking devices and the locking plan* [▶ 571] 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* [▶ 54]).
 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.

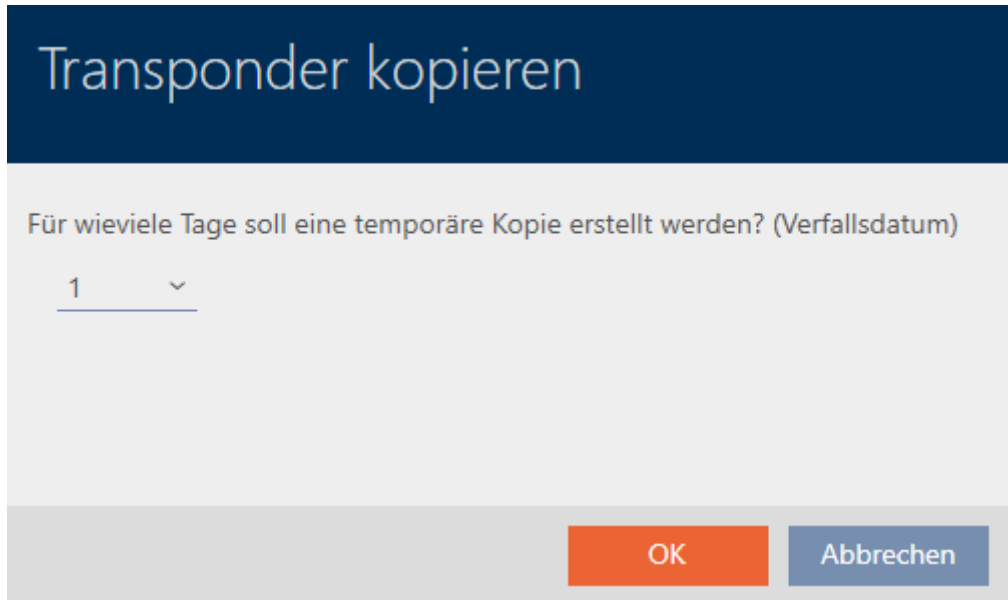
Aktion:
Der Assistent erstellt eine zeitlich begrenzte Kopie des betroffenen Transponders, welcher sofort programmiert werden kann.

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

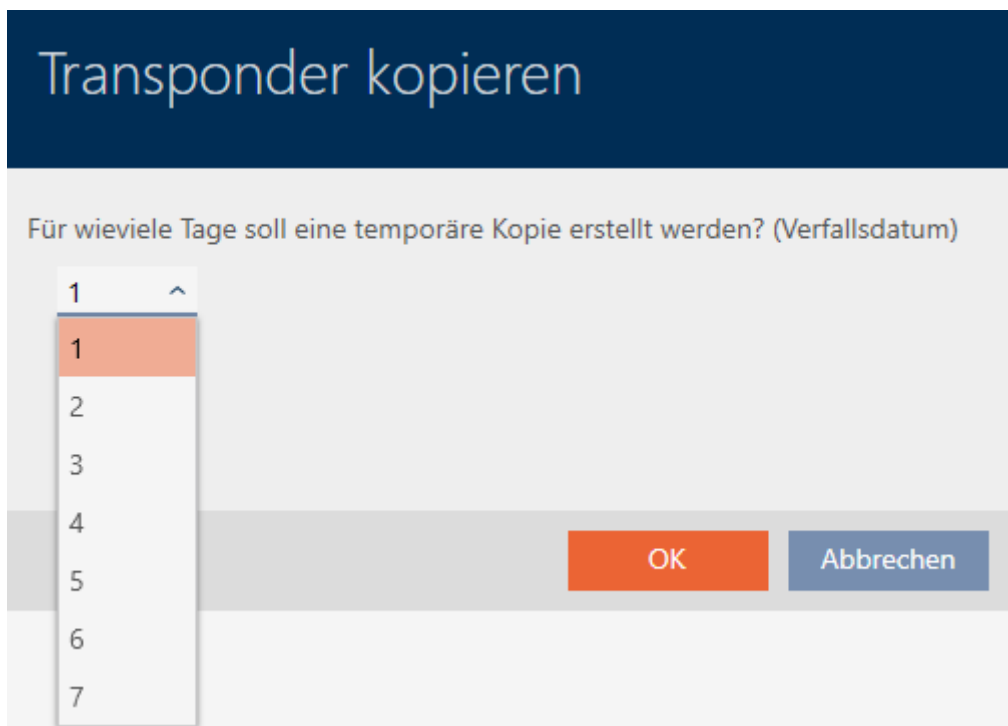
WeiterSchließen

4. Click on the **Next** button.

→ Confirmation dialogue for the duplicate's expiry date will open.



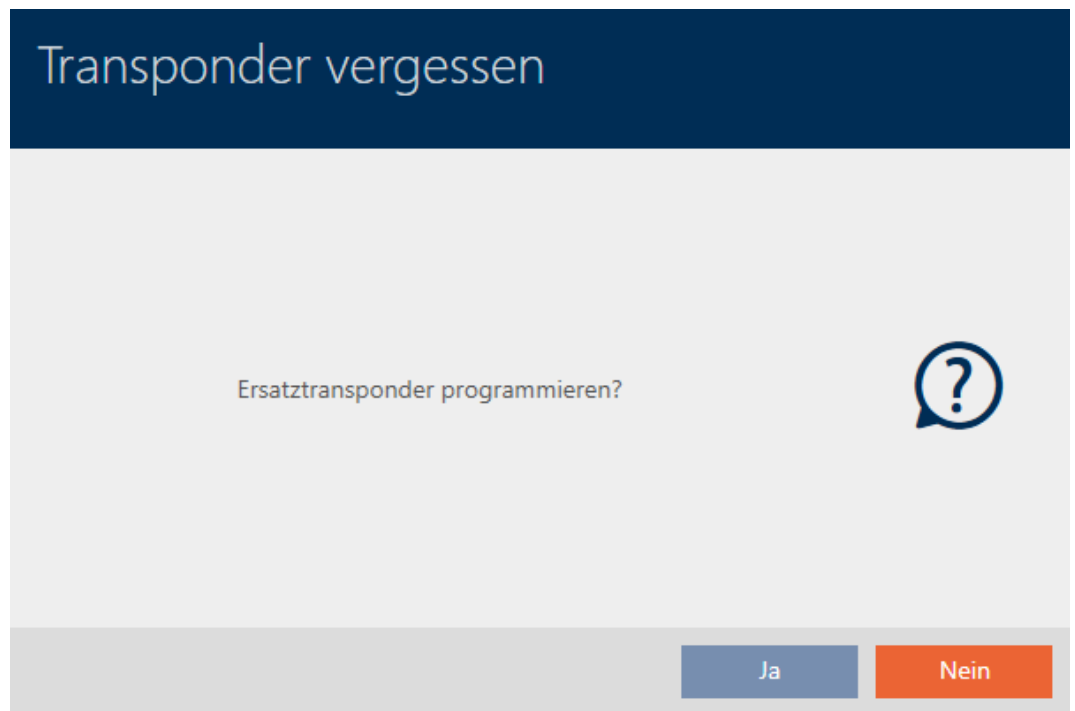
5. Specify how long the duplicate should be active for (max. 7 days).



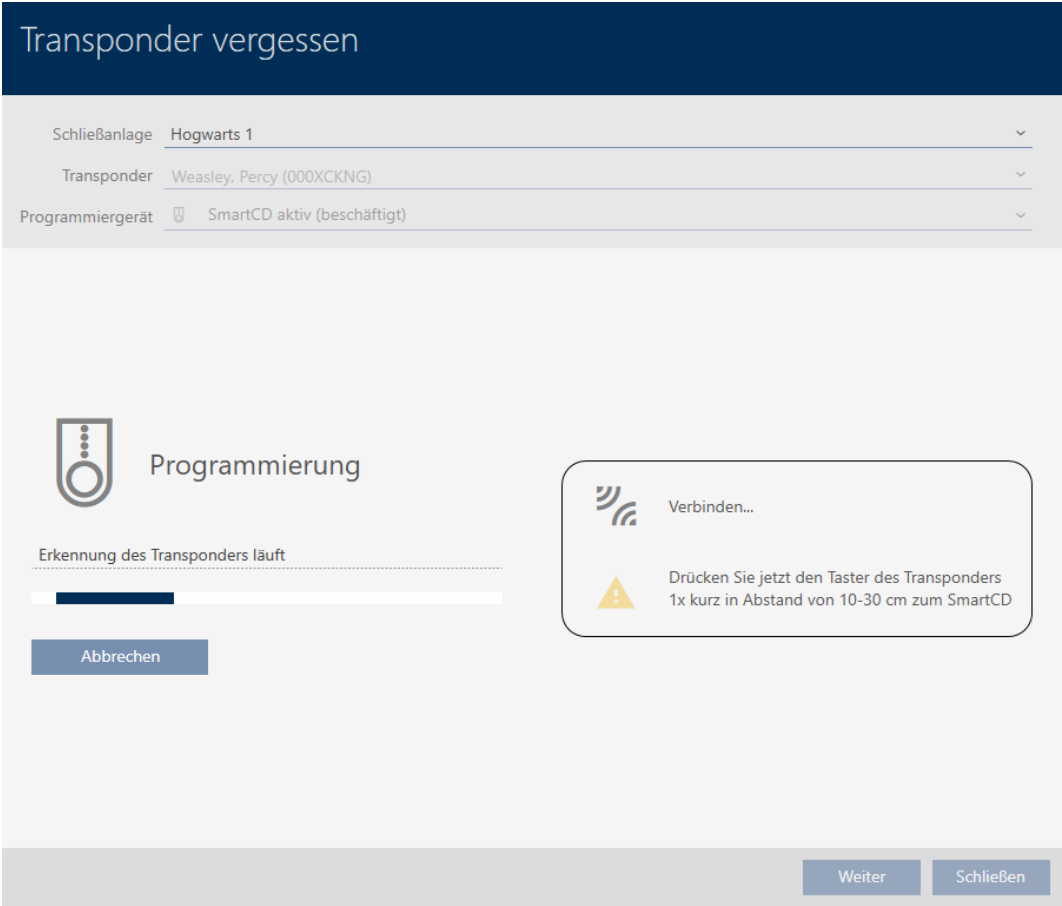
6. Click on the **OK** button.

→ Confirmation dialogue for the duplicate's expiry date closes.

→ Confirmation dialogue for immediate synchronisation will open.



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



↳ Forgotten identification medium is now duplicated with expiry date.

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)* [► 135]):

▼ 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* [► 177]).

15.11 Blocking lost/stolen identification media permanently



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

Block such an identification medium immediately (see *Blocking and replacing lost/stolen card/transponder permanently* [► 177]). 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* [► 571] 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* [▶ 182]). If only one PIN is known and is therefore unsafe, you can change this PIN (see *Changing a PIN (PinCode AX)* [▶ 241]).

15.11.1 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* [▶ 54]).
 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 web-based dialog box titled "Transponder deaktivieren" (Deactivate Transponder). Below the title, it says "Bitte geben Sie die gewünschten Informationen ein" (Please enter the desired information). The main content area contains the question "Wollen Sie tatsächlich den Transponder sperren?" (Do you really want to lock the transponder?) followed by the instruction "Falls 'ja', geben Sie bitte den Grund an, z.B. Transponder verloren." (If 'yes', please give the reason, e.g., transponder lost). There is a dropdown menu with "Verloren" (Lost) selected. Below this is a text input field labeled "Zusatzinformation" (Additional information). At the bottom right, there are two buttons: "OK" (orange) and "Abbrechen" (blue).

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

This is a close-up of the dropdown menu. The menu is open, showing three options: "Verloren" (Lost), "Nicht zurückgegeben" (Not returned), and "Andere Gründe" (Other reasons). The "Verloren" option is highlighted with an orange background. The dropdown is titled "Verloren" with an upward arrow icon.

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

- ➔ Confirmation dialogue for replacement identification medium will open.



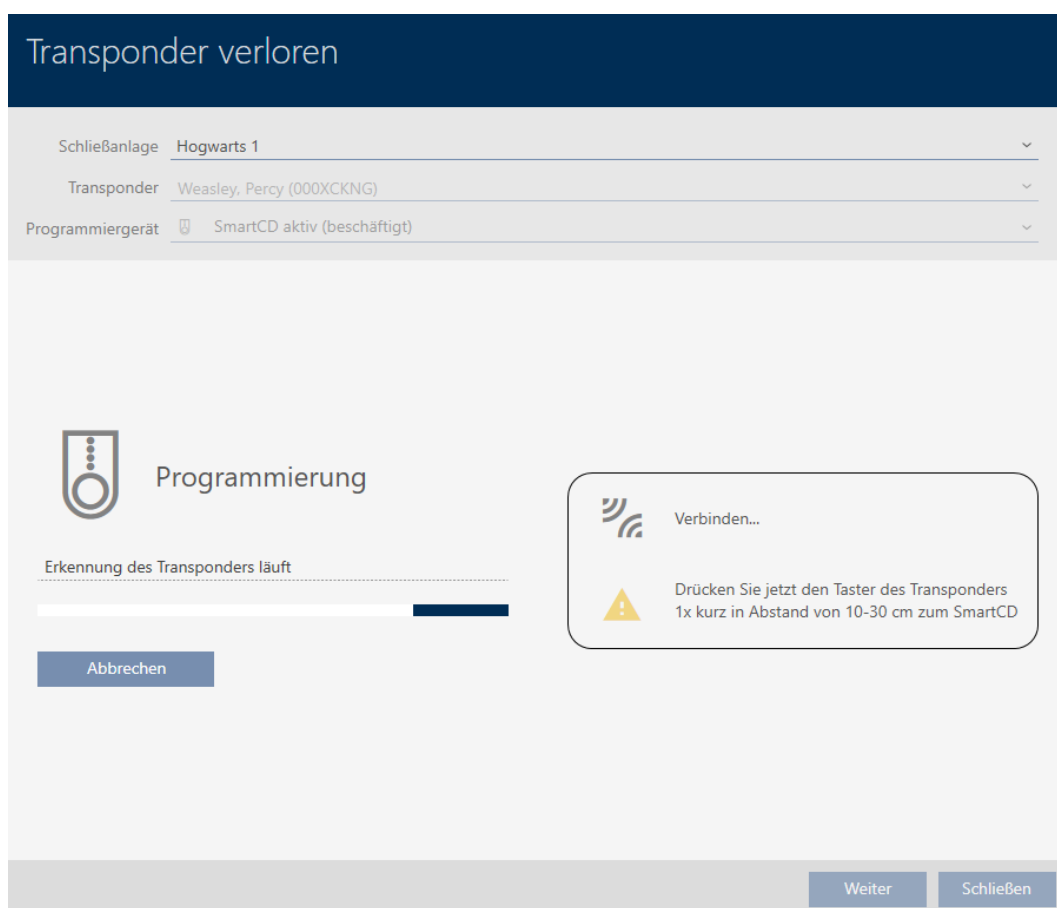
7. Click on the **Yes** button.
 - ↳ Confirmation dialogue for replacement identification medium closes.
 - ↳ Replacement identification medium can already be seen in the matrix in the background.

Sync	Typ	Person
	☺	Weasley, Ron
↻	☺	Weasley, Percy
C	☺	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* [► 51]).
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* [► 416]).

IMPORTANT

Block ID automatically written on replacement transponder

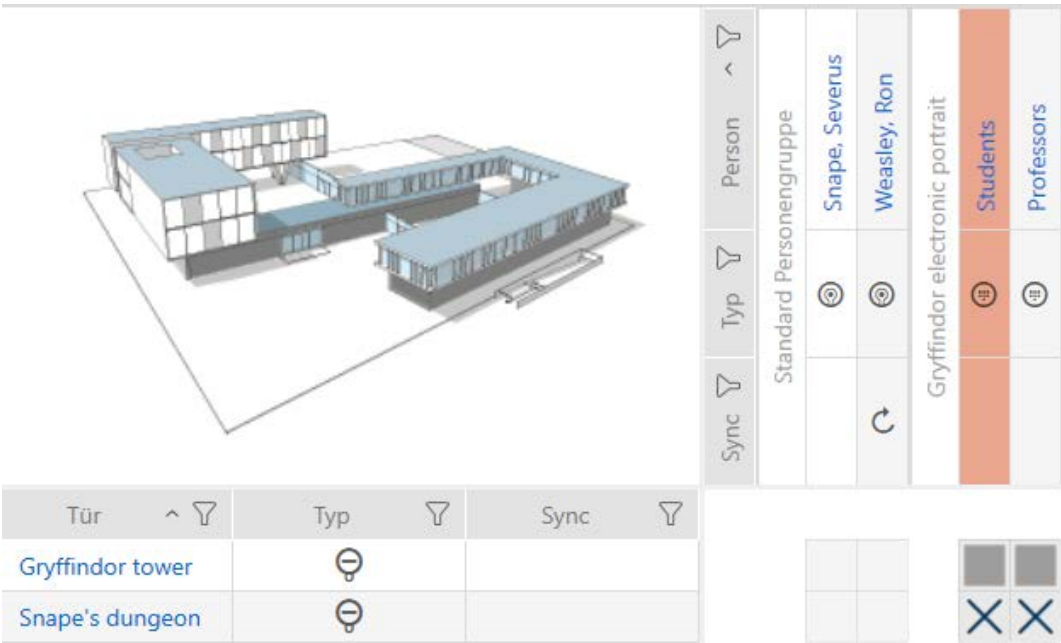
If you create a replacement transponder for a lost/stolen transponder, your AXM Plus automatically writes the block ID from the blocked transponder onto this replacement transponder.

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.

15.11.2 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* [▶ 54]).
 2. Select a PIN associated with the lost PIN code keypad.



3. Click the  PinCode Keypad 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**

4. Click on the **Next** button.

➞ The confirmation window will open.

PinCode deaktivieren

Bitte geben Sie die gewünschten Informationen ein

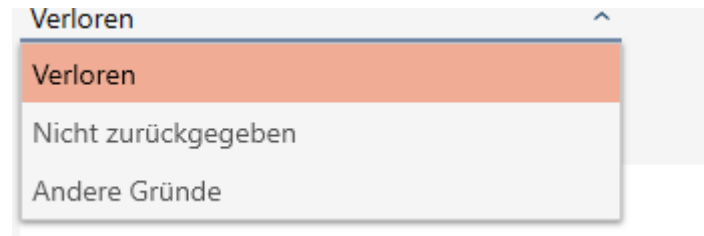
Wollen Sie tatsächlich die PinCode sperren?
Falls 'ja', geben Sie bitte den Grund an, z.B. ob die PinCode verlorengegangen ist.

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.

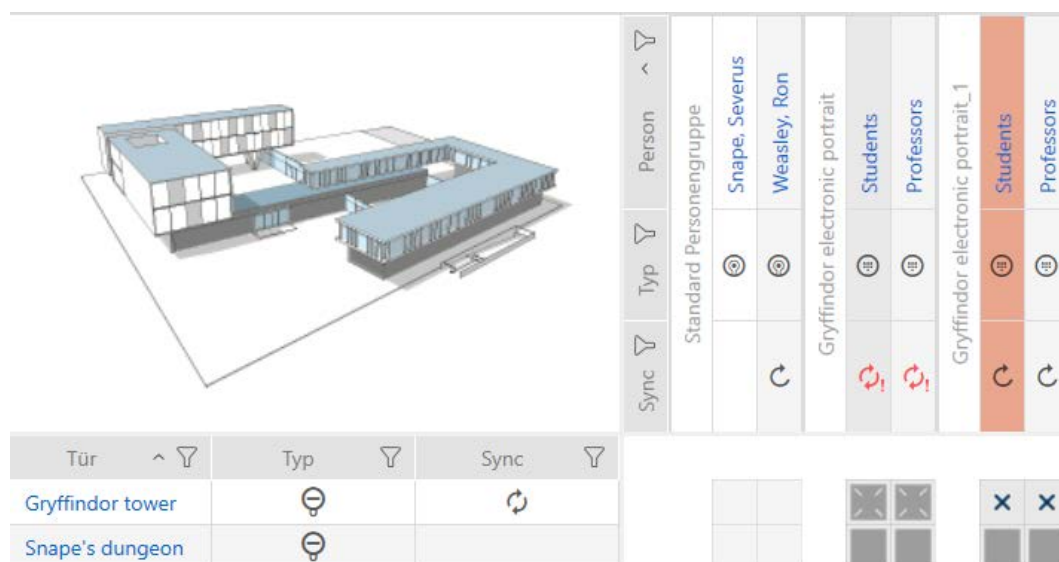


10. Click on the **No** button.
- ↳ The PIN code keypad has been blocked and a replacement PIN code keypad has been synchronised.

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:

Fehler

DIE AKTION IST FEHLGESCHLAGEN.

Synchronisierung unmöglich. Bitte wenden Sie sich an unser Support-Team, um dieses Problem zu beheben.



OK

You can repair the PIN code keypad as an alternative; see [Repairing a PIN code keypad \(resynchronising\)](#) [► 143].

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

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

In contrast to reset and deletion, the physical identification medium is reset but remains in your locking system. AXM 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 \(PinCode AX\)](#) [► 241]).

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

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

- ✓ 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 ZURÜCKGEGEBEN

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

WeiterSchließen

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.

Transponder zurückgeben

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



Transponder wird zurückgesetzt

Abbrechen



Verbinden...



Drücken Sie jetzt den Taster des Transponders
1x kurz in Abstand von 10-30 cm zum SmartCD

Weiter

Schließen

→ Confirmation dialogue for deleting the identification medium will open.

Transponder zurückgeben

Möchten Sie den Transponder löschen?



Ja

Nein

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* [► 199]).

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

15.13 Planning and tracking identification medium management tasks

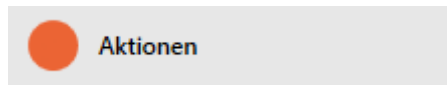
The central point for managing your identification medium is the "Transponder - Actions" tab. The following entries are displayed here collectively:

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

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

- ✓ Identification media list or matrix open.
 - ✓ Identification medium available.
1. Use ▼ to sort/filter the displayed entries if required (see *Sorting and filtering* [► 54]).
 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.

Transponder - Aktionen
Hier können Sie Aktionen zum Transponder planen, einsehen und bearbeiten

Synchronisieren In Matrix anzeigen

1 Details
2 Personendetails
3 Transponderkonfiguration
4 Zusätzliche Schließanlagen
5 Berechtigungsgruppen
6 Hashtags
7 **Aktionen**
8 Begehungliste
9 Berechtigte Schließungen

+ Neu - Löschen ▾ Details

Datum	Typ	Benutzer	Beschreibung	Dokument
14.12.2021 01:41:03	Letzte Programmierung	Admin		
14.12.2021 01:40:06	Letzte Programmierung	Admin		
14.12.2021 01:33:20	Zurückgesetzt	Admin	Aktion fehlgeschlagen	
14.12.2021 01:32:20	Erfolgte Rücknahme	Admin		
14.12.2021 01:30:23	Letzte Programmierung	Admin		
14.12.2021 01:29:17	Zurückgesetzt	Admin		
14.12.2021 01:27:24	Deaktivierung	Admin	Transponder wurde deaktiviert. Grund: Verloren :	
14.12.2021 01:23:11	Letzte Programmierung	Admin		
14.12.2021 01:20:38	Letzte Programmierung	Admin	Unbekannter Fehler	
14.12.2021 01:20:08	Erstellt	Admin		

< Zurück Weiter > Fertigstellen Abbrechen

4. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [► 54]).

15.13.1 Noting the issue date

15.13.1.1 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.

Neue Aktion

Aktion
Letzter Batteriewechsel

Datum
30.05.2021

Uhrzeit
02:46:25

Beschreibung

☐ Dokument in Aktionsliste abspeichern

OK Abbrechen

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

Aktion

Ausgegeben

Ausgegeben

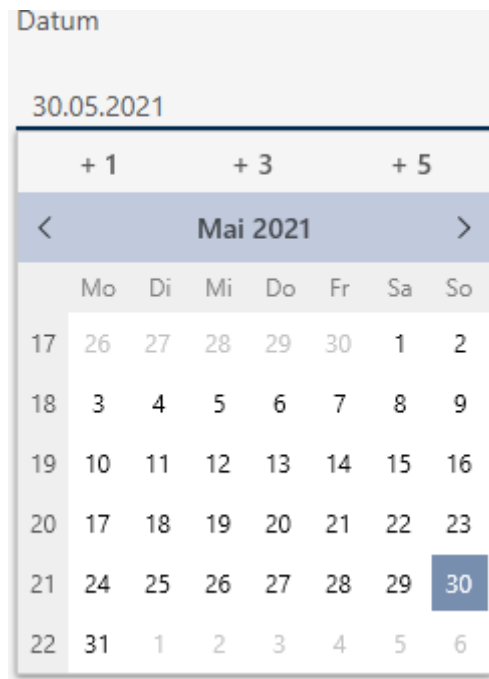
Erfolgte Rücknahme

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.

Neue Aktion

Aktion

Ausgegeben

Datum

30.05.2021

Uhrzeit

03:49:48

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
30.05.2021 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* [▶ 561]) to prepare the transfer of the identification medium.

15.13.2 Planning and logging battery replacement

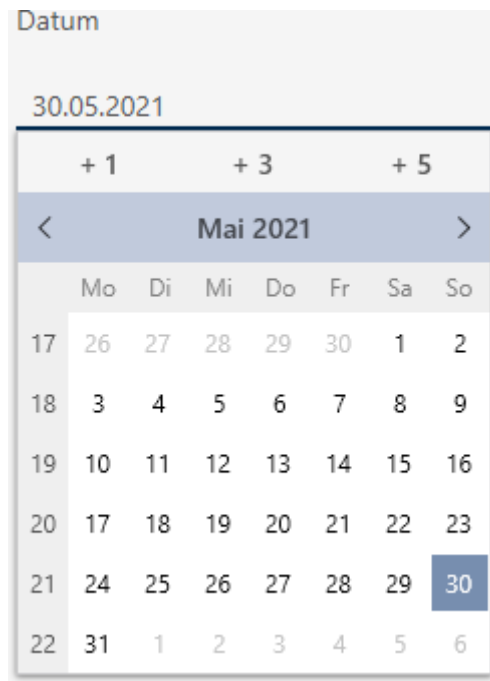
15.13.2.1 Planning and logging card/transponder battery changes

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

→ The window for a new action will open.

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

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



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

Neue Aktion

Aktion

Planmäßiger Batteriewechsel

Datum

30.05.2021

Uhrzeit

04:00:44

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

15.13.2.2 Planning and logging PIN code keypad battery replacement

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

→ The window for a new action will open.

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.

Letzter Batteriewechsel

Letzter Batteriewechsel

Planmäßiger Batteriewechsel

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

Datum

30.04.2024

+1

+3

+5

<

April 2024

>

M	D	M	D	F	S	S
25	26	27	28	29	30	31
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	1	2	3	4	5

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

30.04.2024

Uhrzeit

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 Batteriewechsel	Admin		D:\info.txt
30.04.2024 14:34:39	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:34:03	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:31:23	Zurückgesetzt	Admin	ErrorCode = NoError	
30.04.2024 14:30:50	Letzte Programmierung	Admin	ErrorCode = NoError	
30.04.2024 14:30:36	Letzte Programmierung	Admin	ErrorCode = WrongDevice	
30.04.2024 14:30:24	Zurückgesetzt	Admin	ErrorCode = NoError	
30.04.2024 14:29:59	Letzte Programmierung	Admin	ErrorCode = NoError	

15.13.3 Planning and logging return

15.13.3.1 Planning and logging card/transponder return

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

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

manual reset: *Flagging and resetting returned card/transponder (back to inventory)* [► 187]. The entry in the action list is the same in the end, regardless of whether it is entered with or without a wizard.

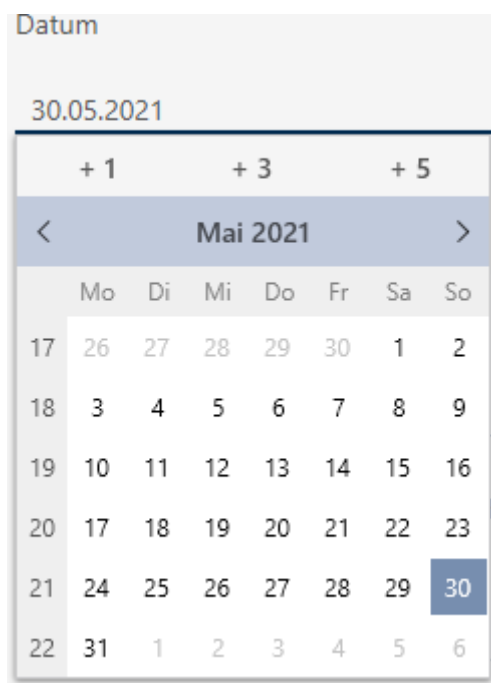
1. Click on the **+** **New** button.
↳ The window for a new action will open.

The screenshot shows the 'Neue Aktion' (New Action) form. At the top, there is a dark blue header with the title 'Neue Aktion'. Below the header, the form is divided into several sections. The first section is 'Aktion' (Action), which contains a dropdown menu currently showing 'Letzter Batteriewechsel'. The second section is 'Datum' (Date), with a text input field showing '30.05.2021'. The third section is 'Uhrzeit' (Time), with a text input field showing '02:46:25'. The fourth section is 'Beschreibung' (Description), with a large text area. Below the description, there is a checkbox labeled 'Dokument in Aktionsliste abspeichern' (Save document in action list). At the bottom right of the form, there are two buttons: 'OK' (orange) and 'Abbrechen' (blue).

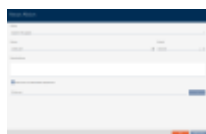
2. Select "Planned return" or "Handed back" from the ▼ **Action** drop-down menu.

The screenshot shows the 'Aktion' (Action) dropdown menu. The menu is open, showing a list of actions. The first item is 'Geplante Rückgabe' (Planned return), which is highlighted in orange. Below it are 'Ausgegeben' (Issued), 'Erfolgte Rücknahme' (Successful return), 'Letzter Batteriewechsel' (Last battery change), and 'Planmäßiger Batteriewechsel' (Regular battery change). The dropdown menu has a small upward arrow icon at the top right.

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.

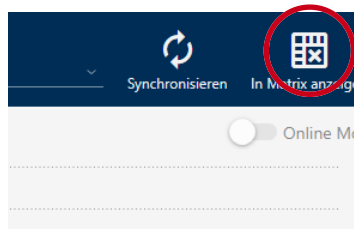
Datum	Typ	Benutzer	Beschreibung	Dokument
30.05.2021 03:05:41	Geplante Rückgabe	Admin		txt
30.05.2021 00:00:49	Letzte Programmierung	Admin		
29.05.2021 00:08:58	Zurückgesetzt	Admin		
29.05.2021 00:08:42	Erfolgte Rücknahme	Admin		
20.05.2021 20:40:08	Letzte Programmierung	Admin		
20.05.2021 20:39:14	Letzte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

15.14 Finding the identification medium or locking device again in the matrix

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

The settings window always provides you with the following button: 

Show in matrix



This button:

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

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

15.15 Exporting identification media as a list

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

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

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

15.15.1 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.

SCHLIESSANLAGENSTEUERUNG

- 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").

Hogwarts	^
Alle	
Hogwarts	
Hogwarts 2	

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
Weasley	Ron	00XTN6K
Wood	Oliver	

- Use  to sort/filter the displayed entries if required (see [Sorting and filtering \[▶ 54\]](#)).
- 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	Aktivierungs- datum / 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* [▶ 493]).

15.15.2 Exporting PINs and PIN code keypads as a list

✓ PIN code keypad created (see *Creating PIN code keypads* [▶ 106]).

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



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

SCHLIESSANLAGENSTEUERUNG

 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").

Hogwarts

Alle

Hogwarts

Hogwarts 2

Matrixansicht x

PinCodes x

+

Neu

🗑

Löschen

📄

In Matrix anzeigen

↑

Export

🗑

Anzeigefilter löschen

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* [▶ 54]).
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* [▶ 493]).

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

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

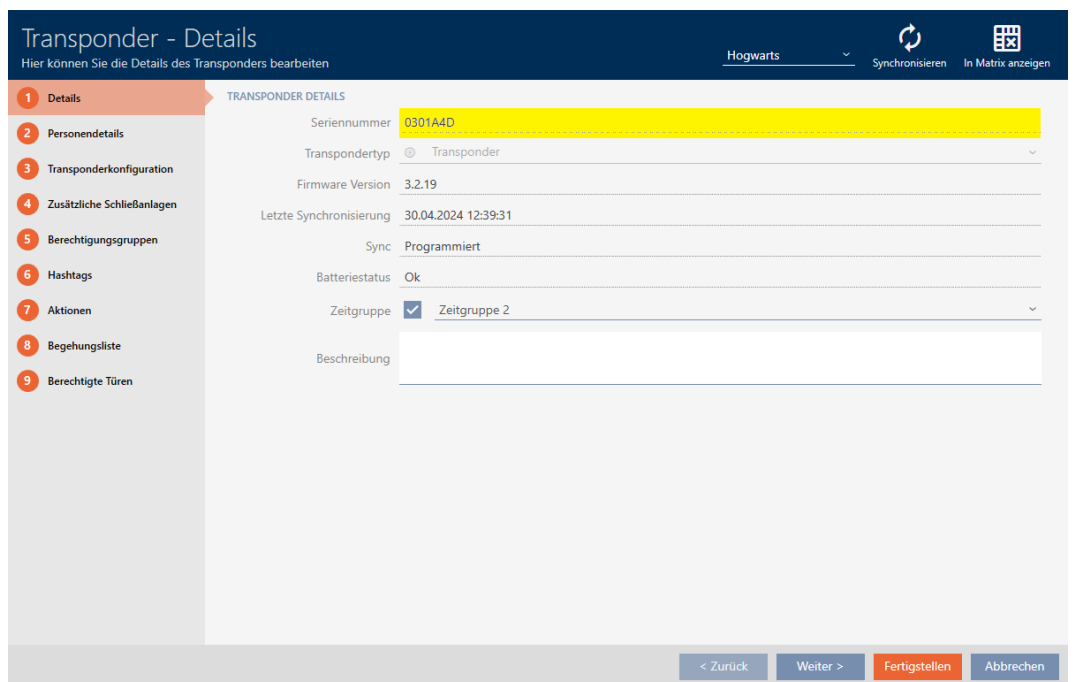
Your cards and transponders have two numbers that are important:

- Serial number (permanently stored in the identification medium and imported during synchronisation)
- TID (flexibly assigned by AXM 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* [▶ 54]).
 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.

Transponder synchronisieren
Hier können Sie den Transponder synchronisieren

Schließanlage: Hogwarts
Transponder: Snape, Severus (0301A4D)
Programmiergerät: SmartCD aktiv

TRANSPONDERDATEN
 Letzte Synchronisierung: 30.04.2024 12:39:31
 Sync: Programmiert
 Status: Aktiviert
 Batteriestatus: Ok
 Zeitgruppe: Zeitgruppe 2

PROGRAMMIERTE DATENSÄTZE

Pos	Schließanlage/SID	SID Extension	TID	Aktivierungsdatum	Verfallsdatum	Zeitgruppe
1	Hogwarts	5817446	3201			Zeitgruppe 2
2	Hogwarts 2	6216511	3200			

Schließen

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

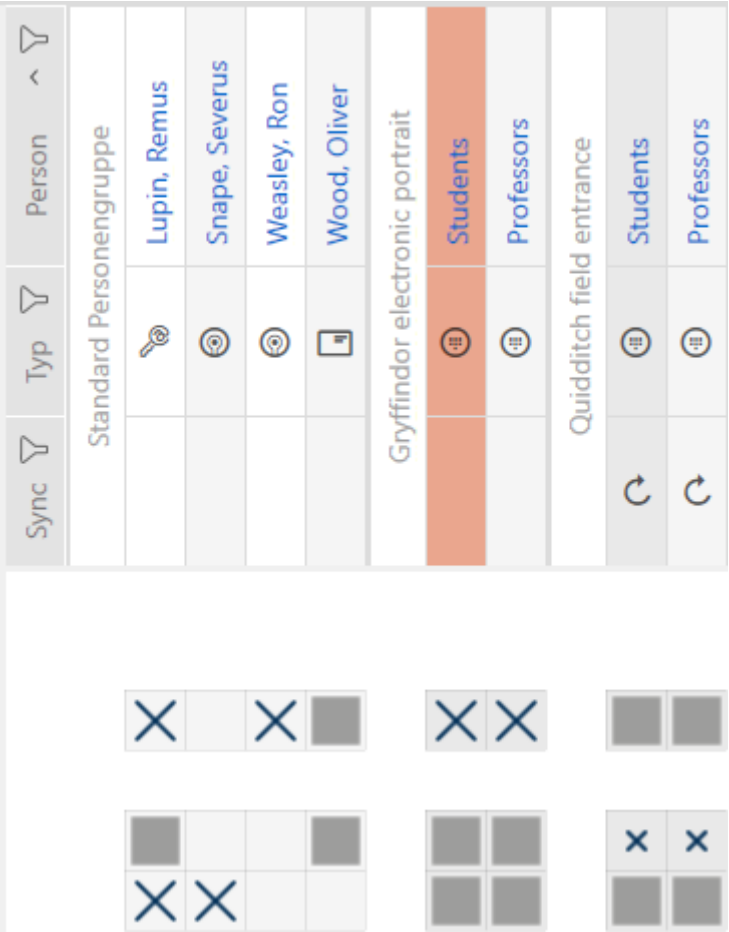
15.16.2 Viewing a PIN code keypad's serial number

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

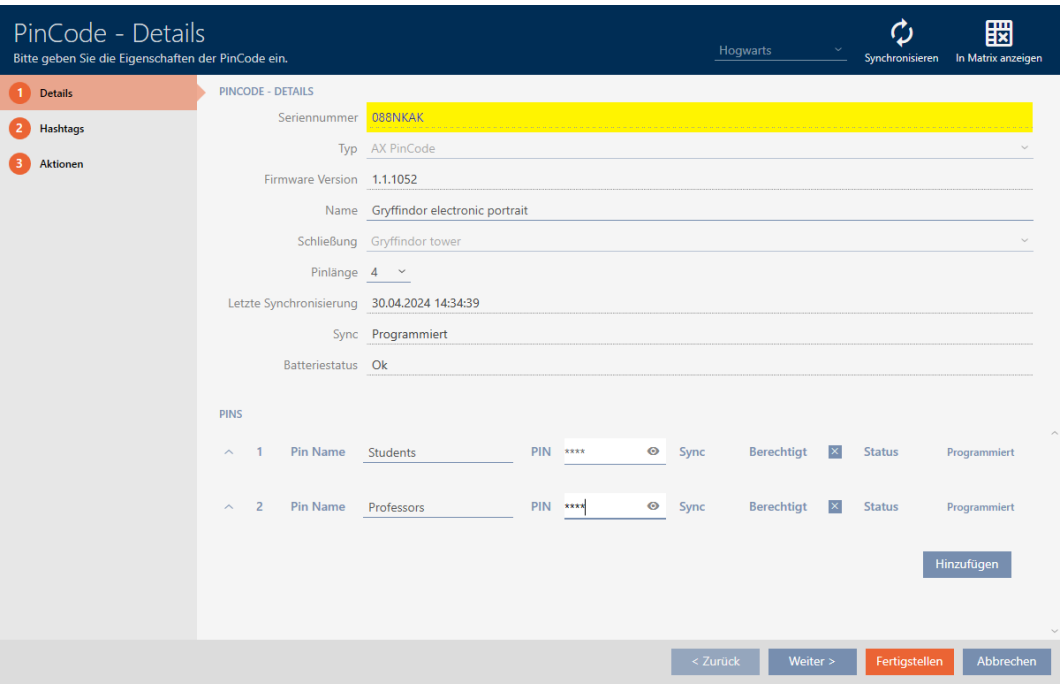
- ✓ PIN code keypad created and synchronised.
- ✓ List with PIN code keypads or matrix open.

1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

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



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



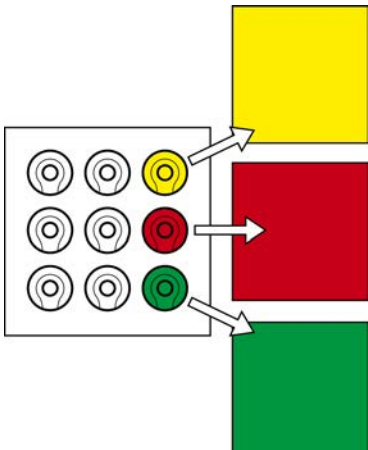
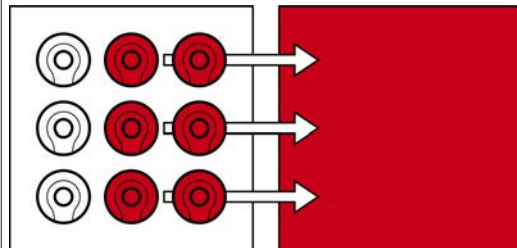
15.17 Assigning persons to person groups

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 \[▶ 362\]](#)).

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 \[▶ 37\]](#)) and plan everything out ready before creating your persons (see [Organisational structure \[▶ 60\]](#)). 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
<i>Assigning individual persons/identification media to a person group (in transponder window) [▶ 210]</i> Suitable for moving few people into many different person groups: 	<i>Assign a number of persons/identification media to person group (in the person group window) [▶ 212]</i> Suitable for moving a number of persons into a few different person groups: 



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 access levels more quickly (see *Adding areas and person groups to access levels* [▶ 349]).

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

Person in "old" person group	Person in "new" person group
Person Standard Personengruppe Granger, Hermine Hagrid, Rubeus Lovegood, Luna McGonagall, Min... Weasley, Percy Typ Standard Personengruppe Granger, Hermine Hagrid, Rubeus Lovegood, Luna McGonagall, Min... Weasley, Percy Sync Standard Personengruppe Granger, Hermine Hagrid, Rubeus Lovegood, Luna McGonagall, Min... Weasley, Percy	Person Teachers McGonagall, Min... Granger, Hermine Hagrid, Rubeus Lovegood, Luna Weasley, Percy Typ Teachers McGonagall, Min... Granger, Hermine Hagrid, Rubeus Lovegood, Luna Weasley, Percy Sync Teachers McGonagall, Min... Granger, Hermine Hagrid, Rubeus Lovegood, Luna Weasley, Percy

- ✓ At least one person group created (see *Creating a person group* [▶ 61]).

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

Transponder - Details

Hier können Sie die Details des Transponders bearbeiten

Synchronisieren

In Matrix anzeigen

1 Details

2 Personendetails

3 Transponderkonfiguration

4 Zusätzliche Schließanlagen

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungliste

9 Berechtigte Türen

TRANSPONDER DETAILS

Seriennummer

UID-1000000034DB9806

Transpondertyp

Karte

Firmware Version

Letzte Synchronisierung

13.12.2021 20:54:06

Sync

Programmiert

Batteriestatus

Zeitgruppe

Zeitgruppe 1

Beschreibung

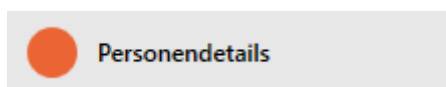
< Zurück

Weiter >

Fertigstellen

Abbrechen

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



- ↳ The "Person details" tab is shown.

The screenshot shows the "Transponder - Personendetails" form. On the left is a sidebar with a list of tabs: 1 Details, 2 Personendetails (highlighted), 3 Transponderkonfiguration, 4 Zusätzliche Schließanlagen, 5 Berechtigungsgruppen, 6 Hashtags, 7 Aktionen, 8 Begehungliste, and 9 Berechtigte Türen. The main area is titled "PERSONENDETAILS" and contains fields for Nachname (McGonagall), Vorname (Minerva), Personalnummer (PN-33), Personengruppe (Standard Personengruppe), Bemerkung, and Foto. On the right, there are fields for Titel, Abteilung, Telefon, E-Mail, Adresse, Ort/Gebäude, and a section for "Einstellt am", "Einstellt bis", and "Geburtsdatum" with checkboxes for "Nicht relevant". At the bottom right, there is a "Kostenstelle" field. The bottom of the form has navigation buttons: "< Zurück", "Weiter >", "Fertigstellen", and "Abbrechen".

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

A close-up of the "Personengruppe" dropdown menu. The current selection is "Teachers". The dropdown list is open, showing "Standard Personengruppe" and "Teachers" (highlighted in orange). There is a "+ Neu" button to the right of the dropdown.

4. Click on the **Finish** button.
- ↳ The identification medium window closes.
- ↳ Person belongs to a new person group.

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

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

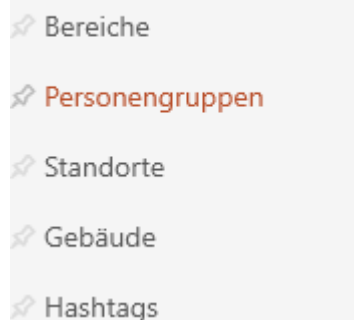
Persons in “old” person group				Persons in “new” person group			
Sync	Typ	Person	Standard Personengruppe	Sync	Typ	Person	Standard Personengruppe
			Granger, Hermine				Granger, Hermine
			Hagrid, Rubens				Hagrid, Rubens
			Lovegood, Luna				Lovegood, Luna
			McGonagall, Min...				McGonagall, Min...
			Weasley, Percy				Weasley, Percy

- ✓ At least one person group created (see *Creating a person group* [► 61]).
- 1. Click on the orange AXM icon .
- ↳ AXM bar opens.

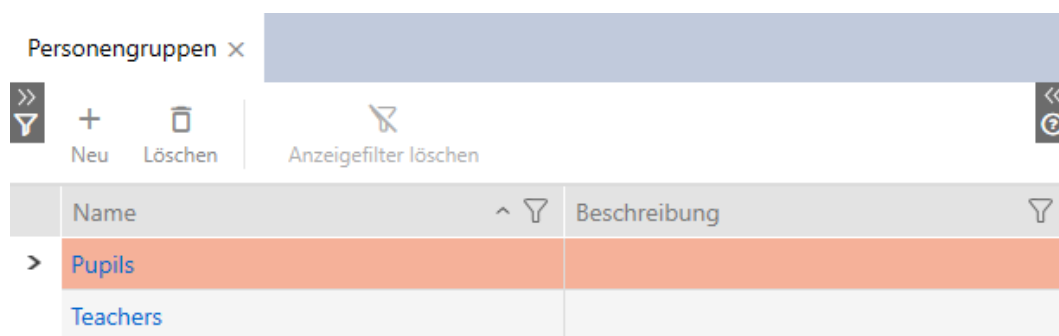


2. Select the **Person groups** entry in the | ORGANISATIONAL STRUCTURE | group.

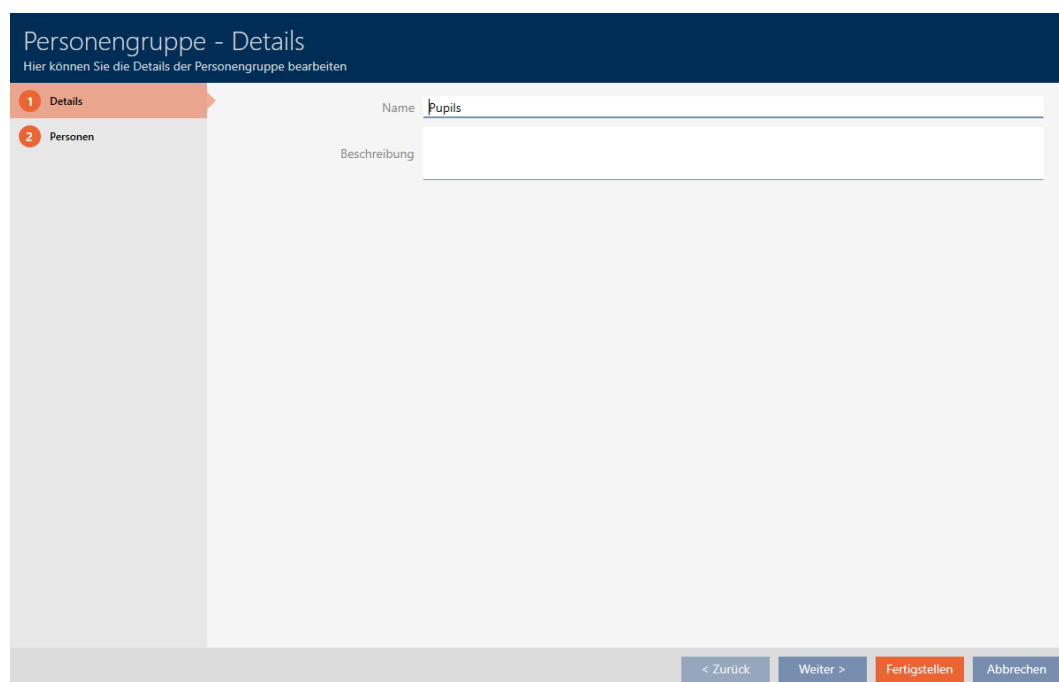
ORGANISATIONSTRUKTUR



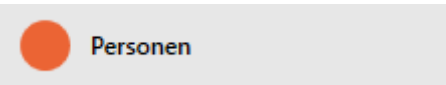
- ↳ The AXM bar will close.
- ↳ The [Person groups] tab will open.



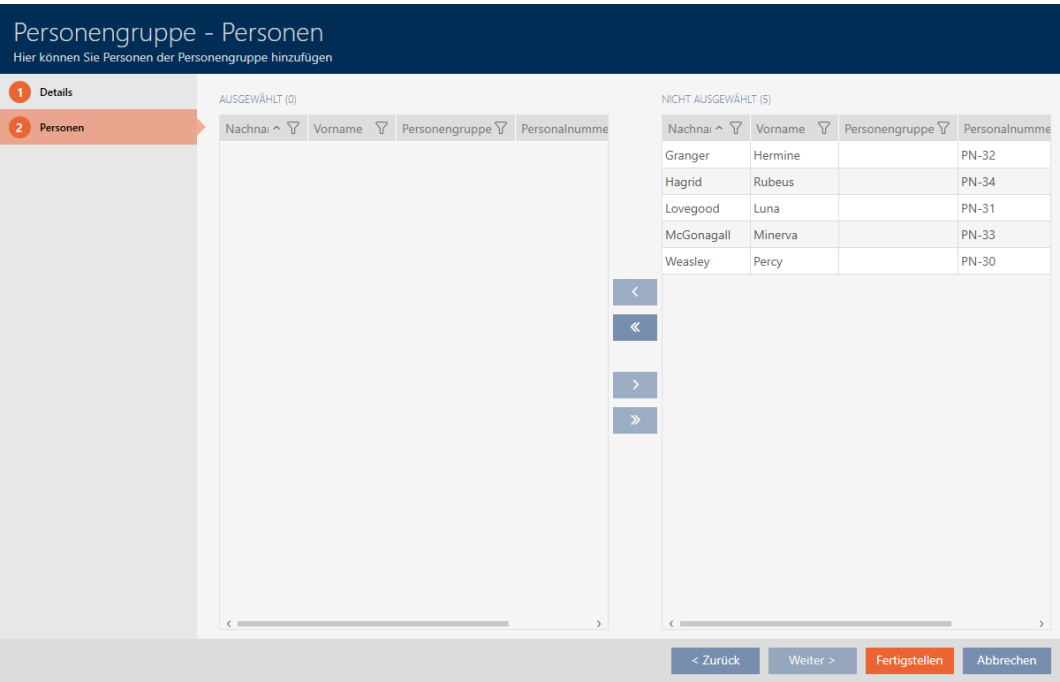
3. Click on the person group to which you want to assign the persons.
- ↳ The "Person group" window will open.



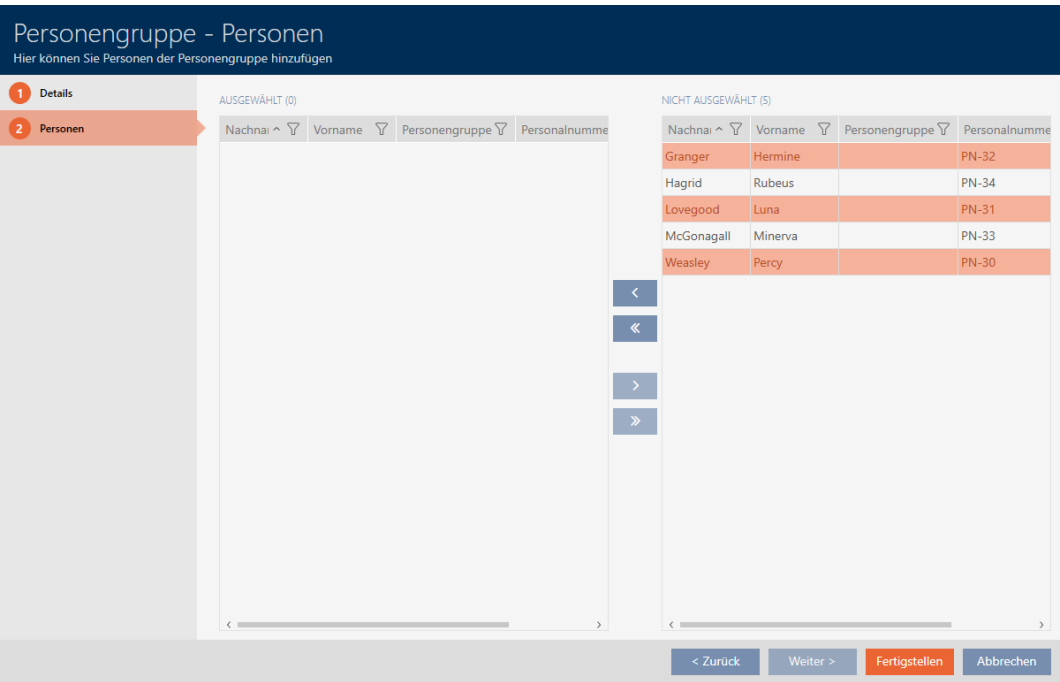
4. Click on the  **Persons** tab.



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



- 5. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
- 6. Highlight all persons you want to add to the area (Ctrl + mouse click for a single person or shift + mouse click for multiple persons).



7. 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.
- 8. 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	Type	Person
		Pupils
		Granger, Hermine
		Lovegood, Luna
		Weasley, Percy
		Standard Personengruppe
		Hagrid, Rubeus
		McGonagall, Min...







































15.18 Use identification media in multiple locking systems

In certain cases, it a good idea to use multiple locking systems (see *Locking systems* [▶ 580]).

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

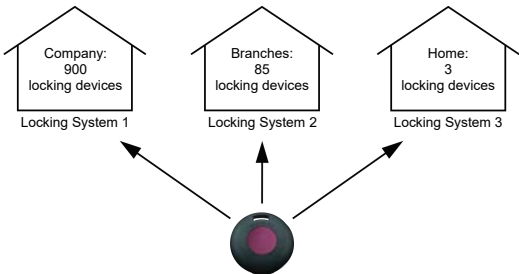
Usage in multiple locking systems differs from the common locking level:

Use in multiple locking systems	Common locking levels
■ Multiple independent locking systems are stored on identification media ■ Can come from different projects and databases ■ Number of possible locking systems limited in the identification medium ■ TID in each of these locking systems independent of TIDs in other locking systems	■ Common locking level is created and locking systems assigned ■ Transponder is created in one of these locking systems. AXM Plus automatically creates the transponder in the other assigned locking systems as well ■ Number of locking systems assigned in this way not limited ■ Authorisations are configured in assigned locking systems See <i>Using a common locking level</i> [▶ 410] to set up an common locking level.

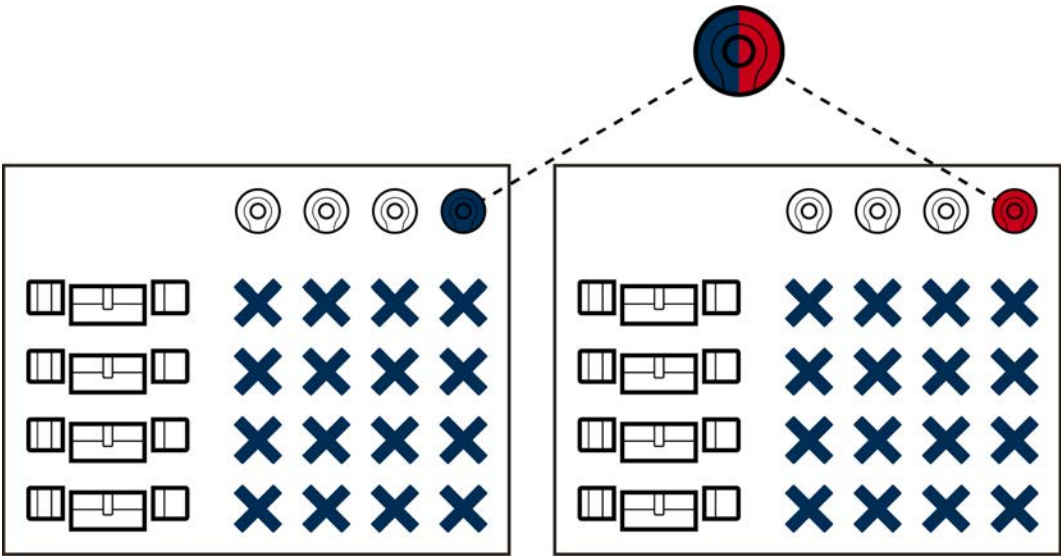
You will find further information on the common locking level here:
Common locking levels [▶ 582].

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 \[▶ 628\]](#)). You no longer make card configurations in AXM Plus across projects, but across different locking systems instead (see [Enable cards or transponders \[▶ 407\]](#)). 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) [▶ 380]* or *MIFARE DESFire (card already in use) [▶ 394]*).

Name: SectList

Wert: 2.3.4.5

Bearbeiten

Beschreibung: Sector List

Name: SectList

Wert: 6.7.8.9

Bearbeiten

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

Konfiguration: MC1200L

Speicherbedarf: 192 Bytes

Schließungs-IDs: 128 - 1327 im Kartenprofil

Begehungen im Protokoll: --

Virtuelles Netzwerk: --

Parameter:

Name: SectList

Wert: 2.3.4.5

Bearbeiten

Beschreibung: Sector List

Name: TransportSectorTrailer

Wert: *****

Bearbeiten

Beschreibung: Transport Settings

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC3800L	
Speicherbedarf	528 Bytes	
Schließungs-IDs	128 - 3927 im Kartenprofil	
Begehungen im Protokoll	--	
Virtuelles Netzwerk	--	

Name:	SectList
Wert:	6,7,8,9,10,11,12,13,14,15,17
Bearbeiten	
Beschreibung: Sector List	

Name:	TransportSectorTrailer
Wert:	*****
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.

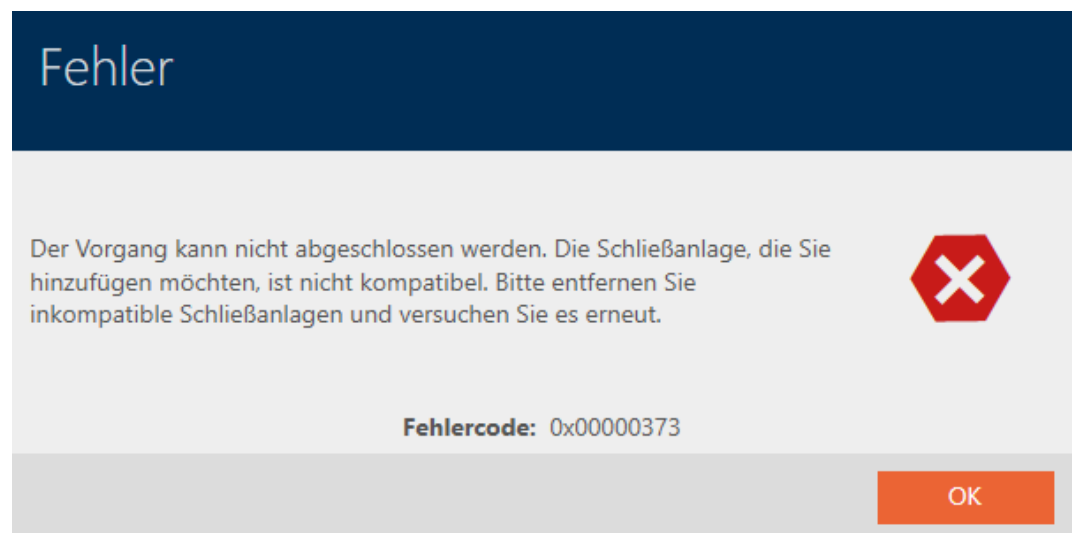
There are two ways to reuse an identification medium:

- *Reuse identification medium in the same project [▶ 218]*
- *Reusing identification medium in other projects/databases [▶ 224]*

15.18.1 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:



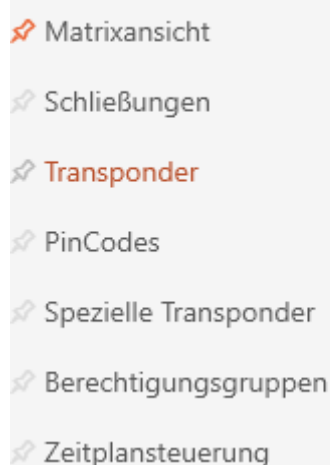
- ✓ At least two locking systems created in the same project (see *Create locking system* [▶ 367]).

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



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

SCHLIESSANLAGENSTEUERUNG



- ↳ The AXM bar will close.
 - ↳ The [Transponder] tab will open.
3. Use  to sort/filter the displayed entries if required (see [Sorting and filtering](#) [▶ 54]).
4. Click on the identification medium you would like to use in another locking system.
 - ↳ The identification medium window will open.

Transponder - Details

Hier können Sie die Details des Transponders bearbeiten

Synchronisieren In Matrix anzeigen

1 Details

2 Personendetails

3 Transponderkonfiguration

4 **Zusätzliche Schließanlagen**

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungliste

9 Berechtigte Türen

TRANSPONDER DETAILS

Seriennummer **000XCKNG**

Transpondertyp ⊙ Transponder

Firmware Version 3.2.19

Letzte Synchronisierung 14.12.2021 18:55:37

Sync Programmiert

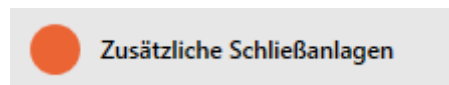
Batteriestatus Ok

Zeitgruppe ☐ Zeitgruppe 1

Beschreibung

[< Zurück](#)
[Weiter >](#)
[Fertigstellen](#)
[Abbrechen](#)

5. Click on the **Additional locking systems** tab.



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

Transponder - Zusätzliche Schließanlagen

Hier können Sie zusätzliche Schließanlagen für den Transponder auswählen

Synchronisieren In Matrix anzeigen

1 Details

2 Personendetails

3 Transponderkonfiguration

4 **Zusätzliche Schließanlagen**

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungliste

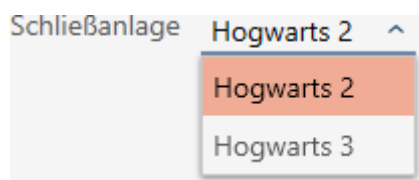
9 Berechtigte Türen

Name	Status
Schließanlage: Hogwarts 2	

[Hinzufügen](#)
[Entfernen](#)

[< Zurück](#)
[Weiter >](#)
[Fertigstellen](#)
[Abbrechen](#)

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.

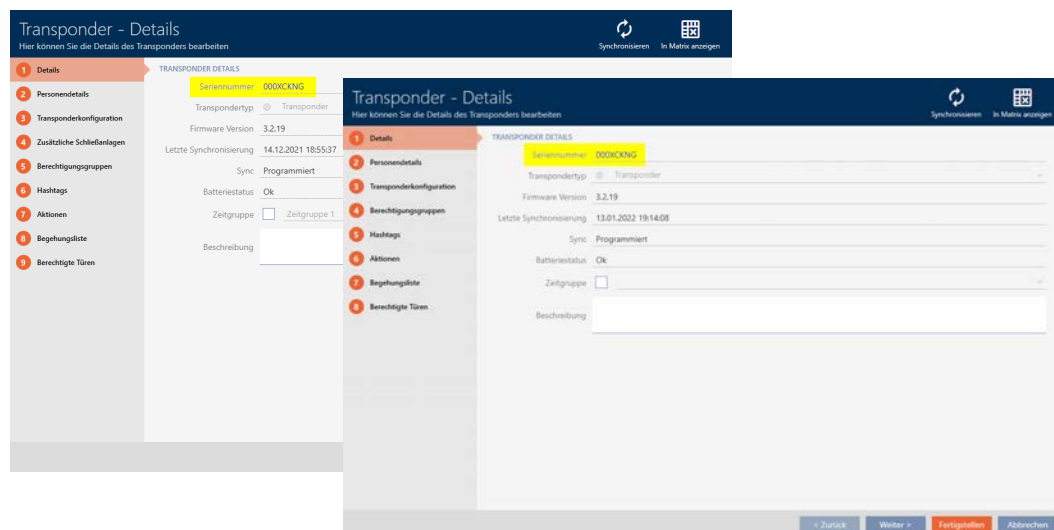


9. Synchronise the identification medium (see *Synchronise a card/transponder (including importing physical access list)* [► 428]).

➔ 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.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage	Hogwarts 1	▼	Transponder erkennen Synchronisieren Status auslesen Begehungliste auslesen Zurücksetzen
Transponder	⊙ Weasley, Percy (000XCKNG)	▼	
Programmiergerät	🔑 SmartCD aktiv	▼	

TRANSPONDERDATEN

Letzte Synchronisierung

14.12.2021 18:55:37

Sync

Programmiert

Status

Aktiviert

Batteriestatus

Ok

Zeitgruppe

PROGRAMMIERTE DATENSÄTZE

Schließen

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

Konfiguration

Schließanlage

Hogwarts 1

Transponder

Ⓢ Weasley, Percy (000XCKNG)

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

14.01.2022 10:50:07

Sync

Programmiert

Status

Aktiviert

Batteriestatus

Ok

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

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

Schließen

15.18.2 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* [► 218]).

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

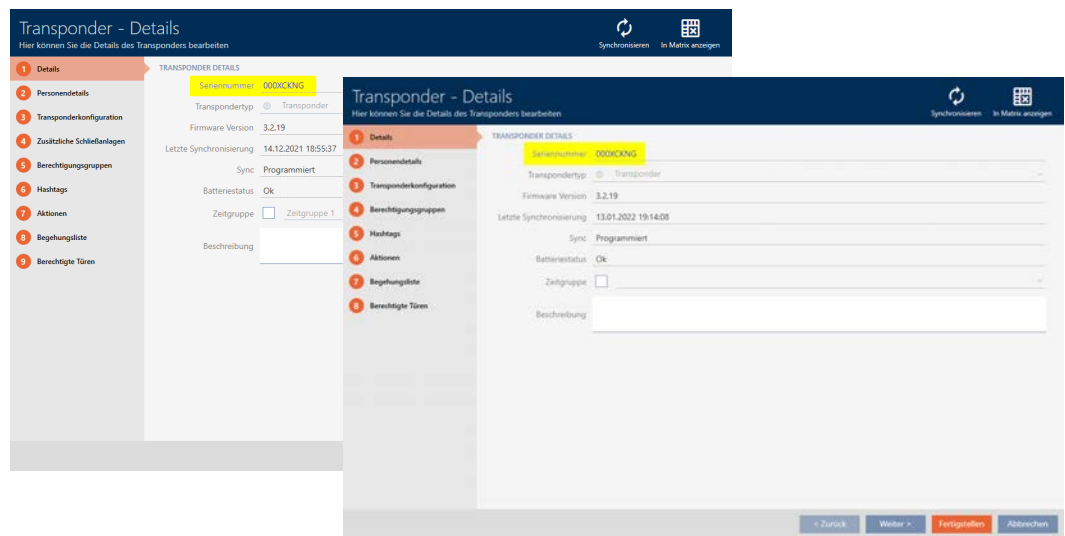
- Use in different AXM projects (projects have their own database)
- Use in an AXM and an LSM locking system

1. Synchronise the identification medium in your project (see *Synchronise a card/transponder (including importing physical access list)* [► 428]).
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.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts 1

Transponder

Weasley, Percy (000XCKNG)

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

14.12.2021 18:55:37

Sync

Programmiert

Status

Aktiviert

Batteriestatus

Ok

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

Schließen

- Synchronise the transponder (see *Synchronise a card/transponder (including importing physical access list)* [► 428]).
 - 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* [► 218]). 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 data-base and therefore cannot be displayed.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts 1

Transponder

Weasley, Percy (000XCKNG)

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

13.01.2022 19:14:08

Sync

Programmiert

Status

Aktiviert

Batteriestatus

Ok

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

Nr.	Schließanlage/ID	SD Extension	TID	Aktivierungsdatum	Verfallsdatum	Zeitgruppe
1.	773	6644767	3206			
2.	Hogwarts 1	14547433	3206			

Schließen

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts 1

Transponder

Weasley, Percy (000XCKNG)

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

14.12.2021 18:55:37

Sync

Programmiert

Status

Aktiviert

Batteriestatus

Ok

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

Nr.	Schließanlage/ID	SD Extension	TID	Aktivierungsdatum	Verfallsdatum	Zeitgruppe
1.	Hogwarts 1	6644767	3206			
2.	803	14547433	3206			

Schließen

15.19 Managing AX2Go keys

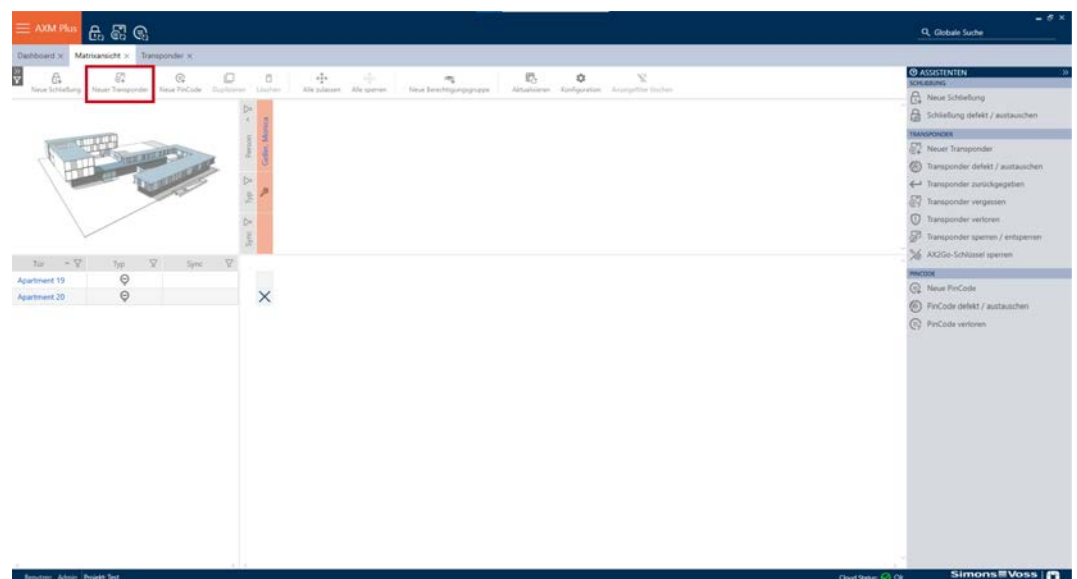
15.19.1 Assigning keys for AXM Plus and higher

In the interests of best practice (see *Best practice: setting up the locking system* [▶ 37]), SimonsVoss recommends that you configure access levels, person groups and schedules/time groups:

- *Access levels* [▶ 340] (see *Access levels* [▶ 602] for background information)
- *Creating a person group* [▶ 61] (see *Person groups* [▶ 603] for background information)
- *Creating a schedule* [▶ 63] or *Create time group* [▶ 66] (see *Time groups and schedules* [▶ 587] 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.

Transponder/Personen - Details

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

AX2Go Test

- 1 Details
- 2 Personendetails
- 3 Transponderkonfiguration
- 4 Berechtigungsgruppen
- 5 Hashtags

TRANSPONDER DETAILS

Typ: Mobiltelefon

Beschreibung:

Zeitgruppe: ☐ Zeitgruppe 1

Farbe: ☐

Einladungstyp: QR Code

PERSONENDETAILS

Neue Person: ☒

oder

Bestehende Person auswählen: Bing Chandler

☐ Weiteres Objekt erstellen

< Zurück Weiter > Fertigstellen Fertigstellen & Einladung senden Abbrechen

2. Selecting "Smartphone" as a transponder type

Transponder/Personen - Details

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

AX2Go Test

- 1 Details
- 2 Personendetails
- 3 Transponderkonfiguration
- 4 Berechtigungsgruppen
- 5 Hashtags

TRANSPONDER DETAILS

Typ: ☐ Karte ☒ Mobiltelefon ☐ Transponder

Beschreibung:

Zeitgruppe: ☐

Farbe: ☐

Einladungstyp: QR Code

PERSONENDETAILS

Neue Person: ☒

oder

Bestehende Person auswählen: Geller, Monica

☐ Weiteres Objekt erstellen

< Zurück Weiter > Fertigstellen Fertigstellen & Einladung senden Abbrechen

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

The screenshot shows the 'Transponder/Personen - Details' form. The left sidebar contains a navigation menu with five items: 1. Details, 2. Personendetails (highlighted with a red circle and a red exclamation mark), 3. Transponderkonfiguration, 4. Berechtigungsgruppen, and 5. Hashtags. The main content area is titled 'TRANSPONDER DETAILS' and contains the following fields: 'Typ' (set to 'Mobiltelefon'), 'Beschreibung' (empty text field), 'Zeitgruppe' (checkbox), 'Farbe' (checkbox), and 'Einladungstyp' (dropdown menu). The 'Einladungstyp' dropdown is open, showing three options: 'QR Code' (highlighted in orange), 'E-Mail', and 'SMS'. Below the dropdown, there is a 'Neu' button and an 'oder' label. At the bottom of the form, there is a 'Bestehende Person auswählen' dropdown menu showing 'Geller, Ross'. The bottom of the form has a row of buttons: 'Weiteres Objekt erstellen' (checkbox), '< Zurück', 'Weiter >', 'Fertigstellen', 'Fertigstellen & Einladung senden', and 'Abbrechen'.

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 >**.

The screenshot shows the 'Transponder/Personen - Details' form. The left sidebar is the same as in the previous screenshot. The main content area is titled 'TRANSPONDER DETAILS' and contains the same fields as before. The 'Einladungstyp' dropdown is now set to 'QR Code'. Below the dropdown, there is a 'Neue Person' checkbox (checked) and an 'oder' label. Below the 'oder' label, there is a 'Bestehende Person auswählen' dropdown menu showing 'Geller, Monica'. The bottom of the form has the same row of buttons as in the previous screenshot.

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



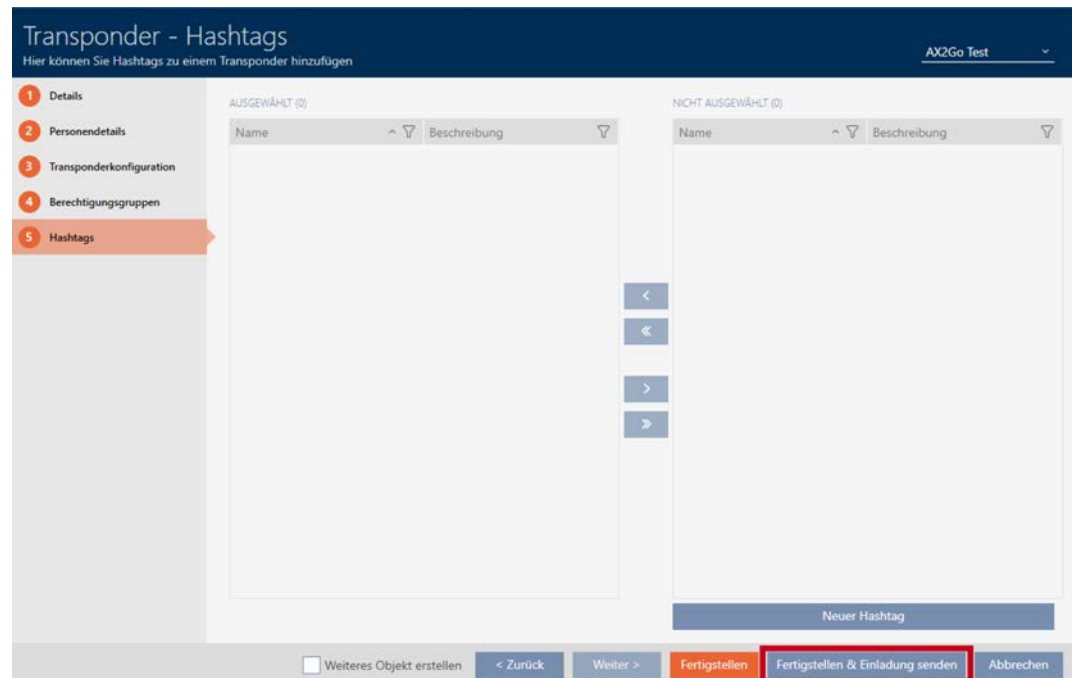
NOTE

Mandatory information, depending on the type of invitation

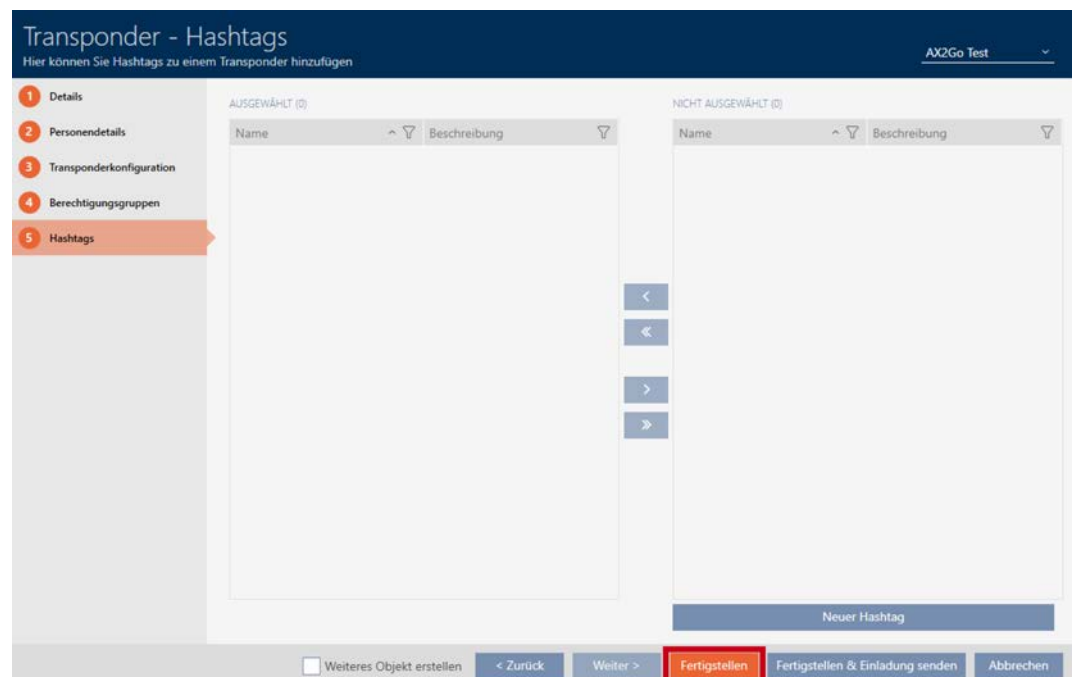
Note that the mandatory fields to be completed vary depending on the type of invitation selected.

6. You **can** configure further settings in the **Transponder configuration**, **Access levels** and **Hashtags** tabs.
See *Creating transponders and cards* [▶ 99], *Creating a hashtag* [▶ 95] and *Access levels* [▶ 340] for more information.

7. 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.



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



9. 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.

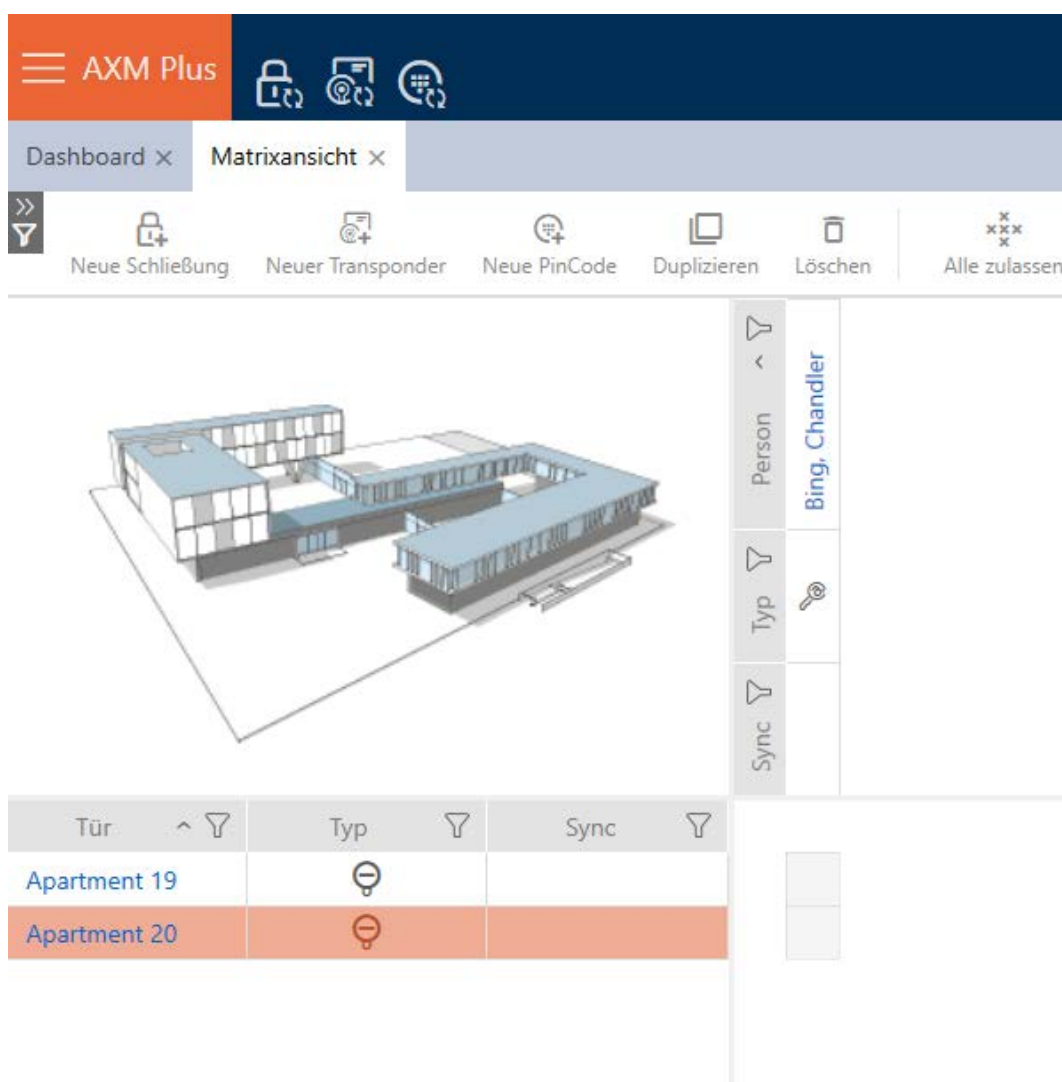
 Es wurde keine Einladung registriert.

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.



15.19.2 Revoking an AX2Go key

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

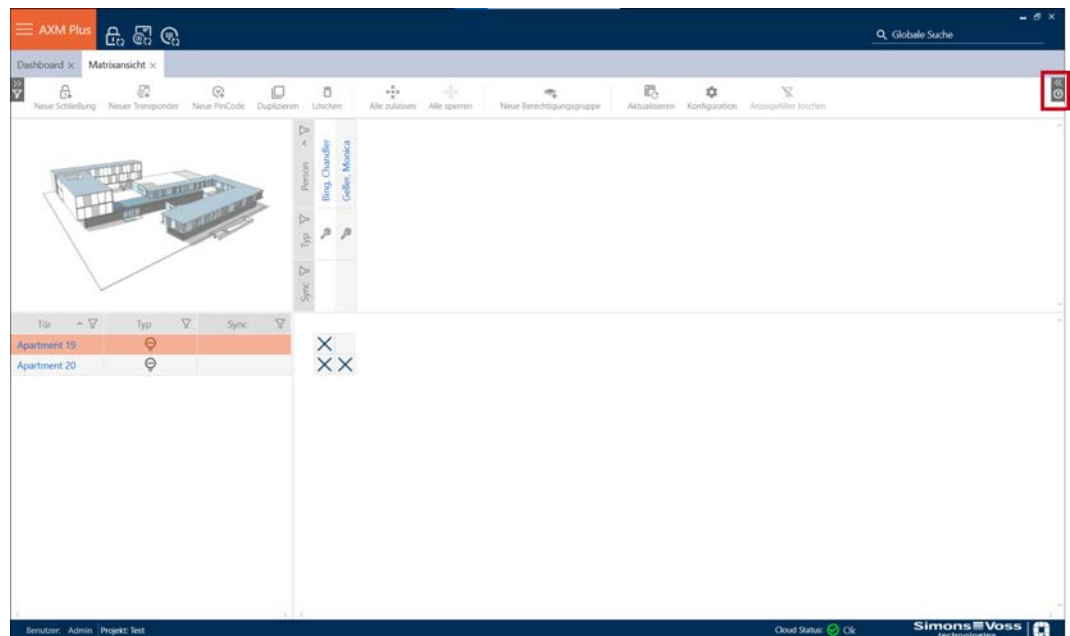


NOTE

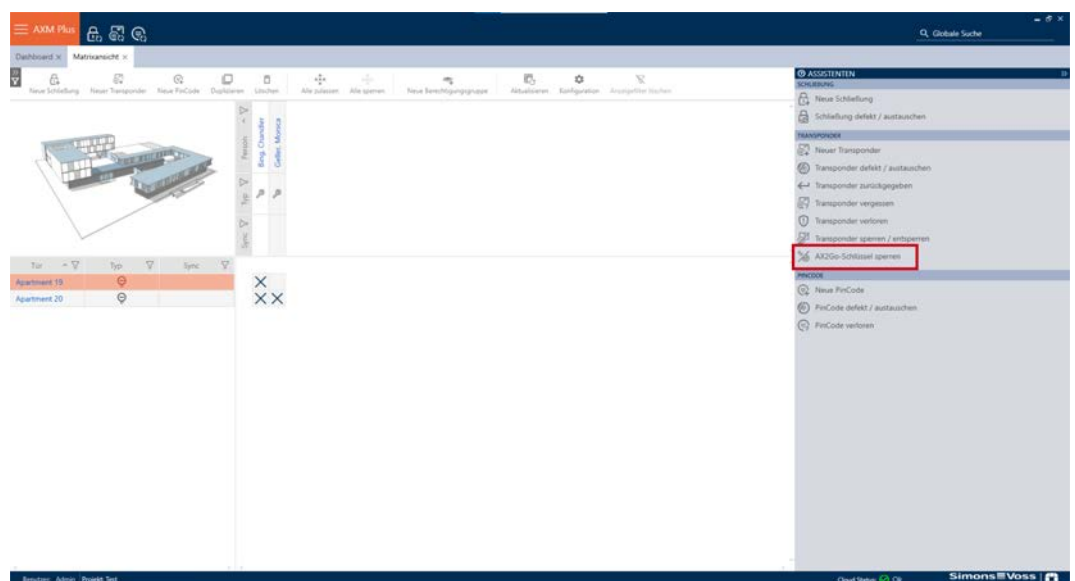
Revoking can't be undone

You can't undo the revoking of an AX2Go key.

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



2. Click on the point  Revoke AX2Go Key.



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

AX2Go-Schlüssel widerrufen - Assistent

Schließanlage: AX2Go Test

Transponder:

- Bing, Chandler (135CKA5)
- Geller, Monica (135CK9K)

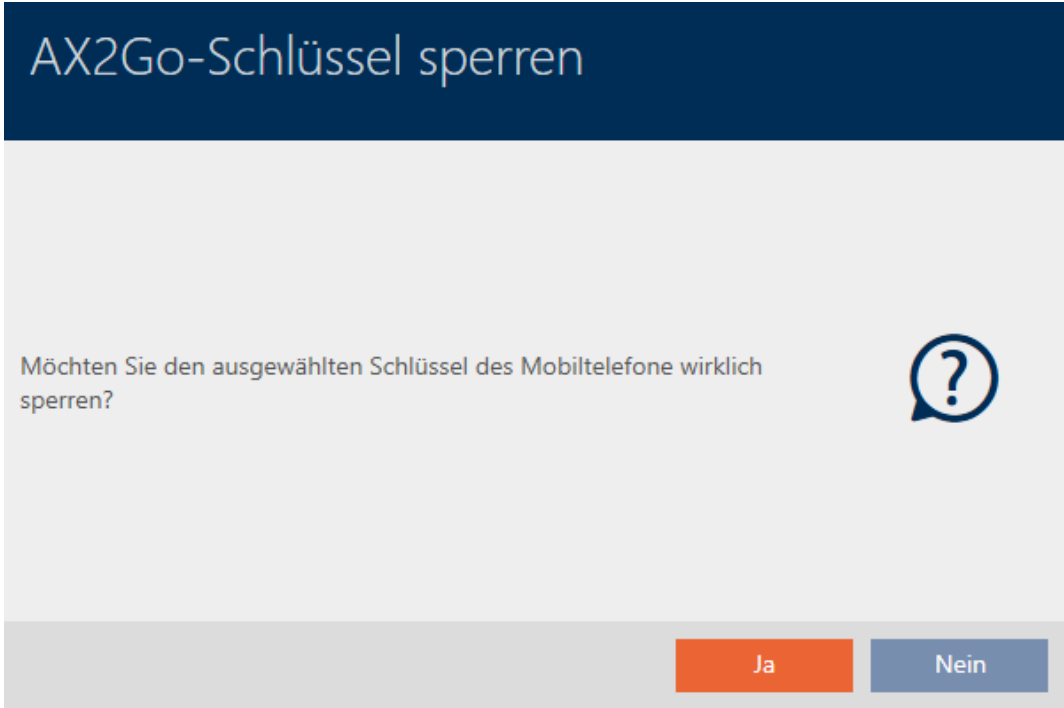
AX2GO-SCHLÜSSEL WIDERRUFEN

Ereignis:
Der ausgewählte Schlüssel des Mobiltelefons soll widerrufen werden.

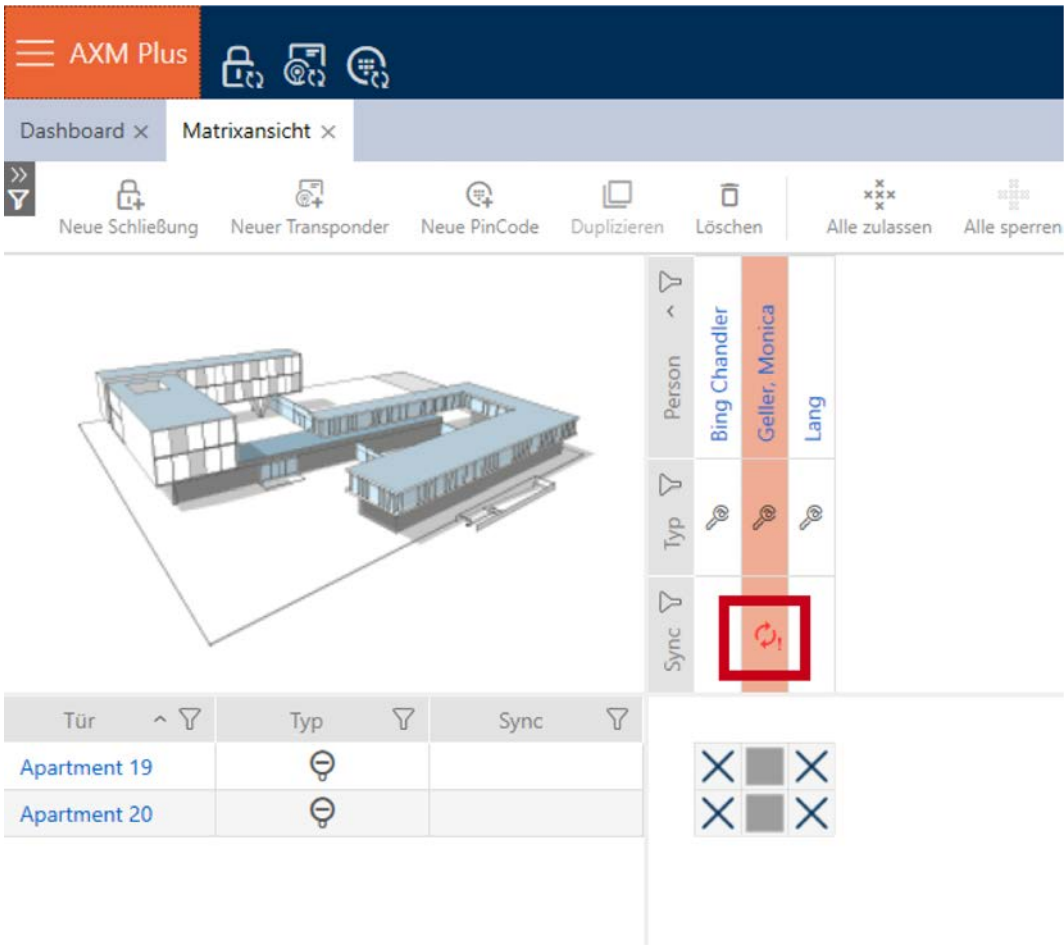
Aktion:
Der aktuelle Schlüssel des Mobiltelefons wird dauerhaft gesperrt.

Weiter Schließen

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



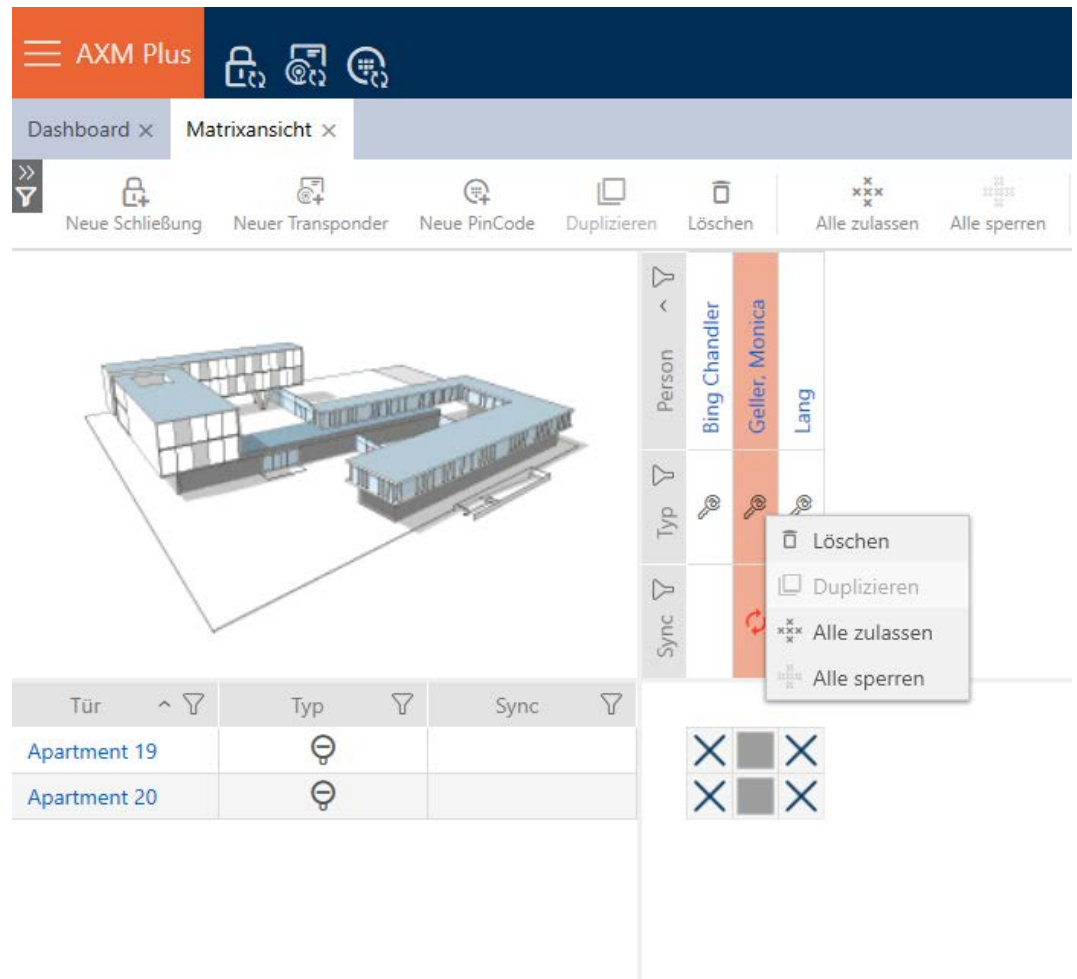
→ The AX2Go key you selected has been blocked successfully.



15.19.3 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.

Objekte löschen

Wollen Sie die ausgewählten Objekte löschen?

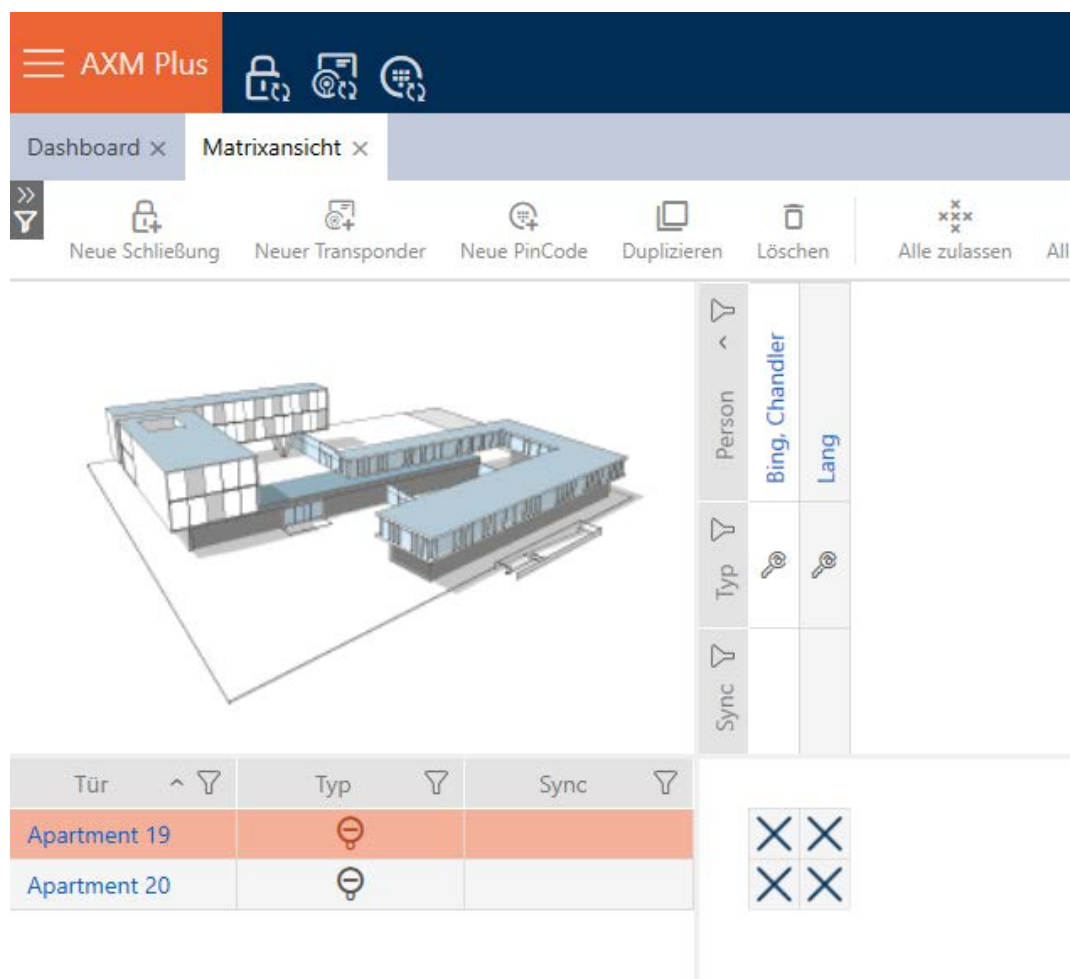


Ja

Nein

2. Click on the **Yes** button.

→ You have successfully deleted the selected key. It is no longer visible in the matrix view.



15.20 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 \[▶ 106\]](#)).

1. Click on any PIN to open details on your PIN code keypad AX.

→ The "PinCode Keypad - Details" window will open.

PinCode - Details

Bitte geben Sie die Eigenschaften der PinCode ein.

Hogwarts Synchronisieren In Matrix anzeigen

1 Details 2 Hashtags 3 Aktionen

PINCODE - DETAILS

Seriennummer 0873CDF

Typ AX PinCode

Firmware Version 1.1.1048

Name Gryffindor electronic portrait

Schließung Snape's dungeon

Pinlänge 4

Letzte Synchronisierung 18.04.2024 14:12:57

Sync Programmiert

Batteriestatus Ok

PINS

	Pin Name	PIN	Sync	Berechtigt	Status	Programmirt
1	Students	****	Sync	Berechtigt	Status	Programmiert
2	Professors	****	Sync	Berechtigt	Status	Programmiert

Hinzufügen

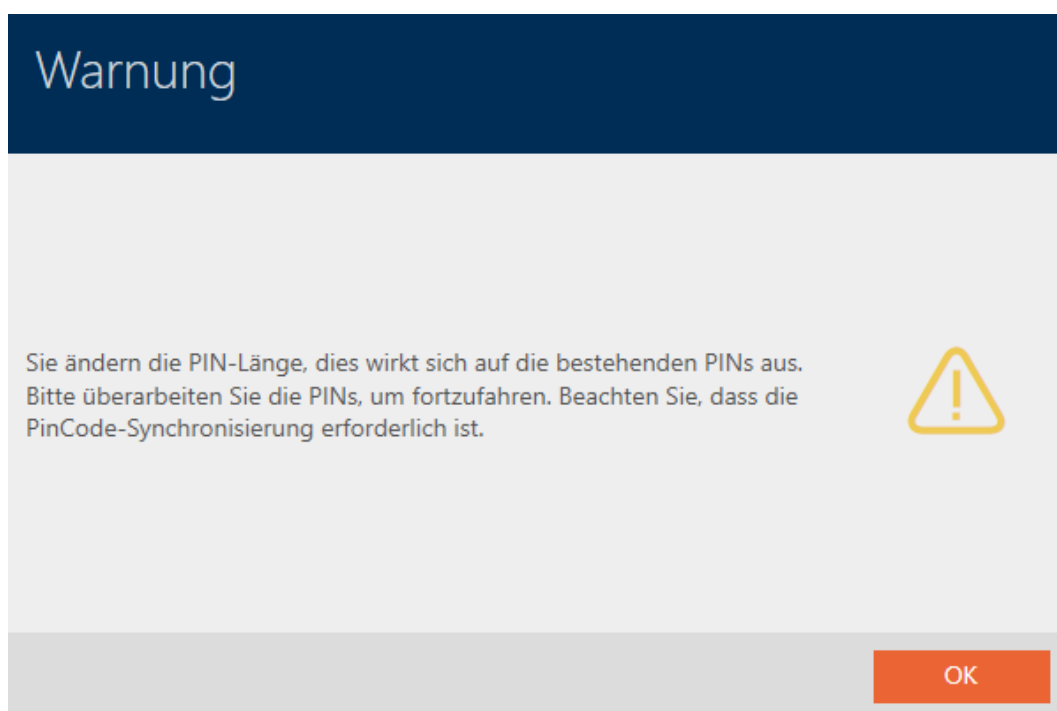
< Zurück Weiter > Fertigstellen Abbrechen

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

Pinlänge 4

4 5 6 7 8 9 10

→ 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.

PinCode - Details
Bitte geben Sie die Eigenschaften der PinCode ein.

Hogwarts Synchronisieren In Matrix anzeigen

1 Details PINCODE - DETAILS
2 Hashtags
3 Aktionen

Seriennummer 0873CDF
Typ AX PinCode
Firmware Version 1.1.1048
Name Gryffindor electronic portrait
Schließung Snape's dungeon
Pinlänge 6
Letzte Synchronisierung 18.04.2024 14:12:57
Sync Programmiert
Batteriestatus Ok

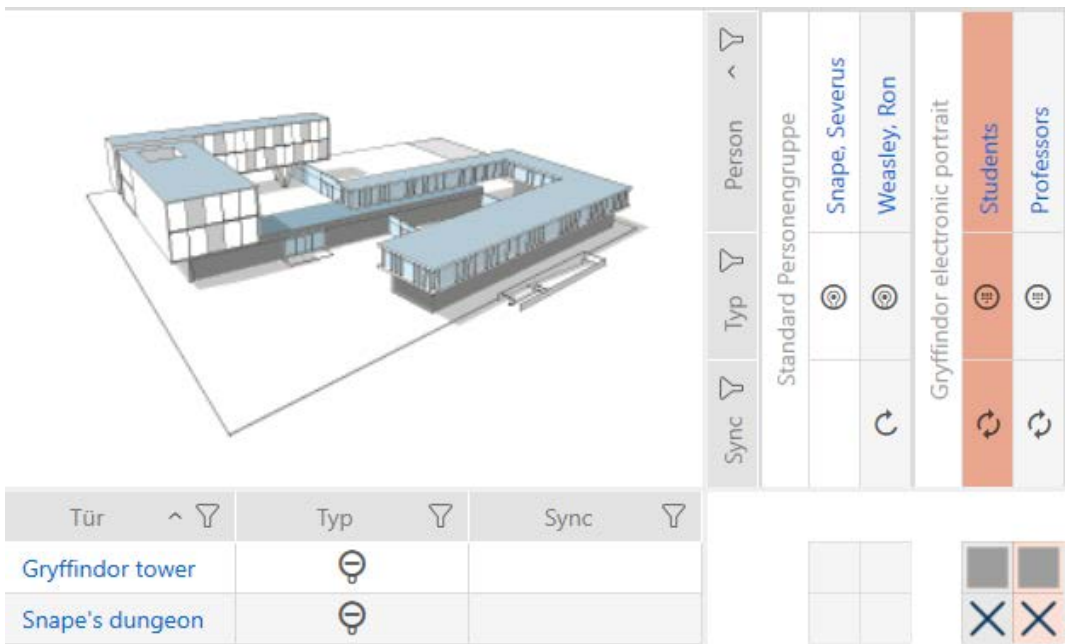
PINS

	Pin Name	PIN	Sync	Berechtigt	Status	Programmiert
1	Students	*****	Sync	Berechtigt	Status	Programmiert
2	Professors	*****	Sync	Berechtigt	Status	Programmiert

Hinzufügen

< Zurück Weiter > Fertigstellen Abbrechen

5. Click the **Finish** button.
 - ➔ "PinCode Keypad - Details" window closes.
 - ➔ The PIN length and PINs have been changed and the resulting programming requirement is displayed in the matrix.



15.21 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 yourAXM 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* [▶ 106]).
1. Click on any PIN to open details on your PIN code keypad AX.
 - ➔ The "PinCode Keypad - Details" window will open.

PinCode - Details
Bitte geben Sie die Eigenschaften der PinCode ein.

Hogwarts Synchronisieren In Matrix anzeigen

1 Details
2 Hashtags
3 Aktionen

PINCODE - DETAILS

Seriennummer 0873CDF
Typ AX PinCode
Firmware Version 1.1.1048
Name Gryffindor electronic portrait
Schließung Snape's dungeon
Pinlänge 4
Letzte Synchronisierung 18.04.2024 14:12:57
Sync Programmiert
Batteriestatus Ok

PINS

1	Pin Name	Students	PIN	****	Sync	Berechtigt	Status	Programmiert
2	Pin Name	Professors	PIN	****	Sync	Berechtigt	Status	Programmiert

Hinzufügen

< Zurück Weiter > Fertigstellen Abbrechen

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

PinCode - Details
Bitte geben Sie die Eigenschaften der PinCode ein.

Hogwarts Synchronisieren In Matrix anzeigen

1 Details
2 Hashtags
3 Aktionen

PINCODE - DETAILS

Seriennummer 0873CDF
Typ AX PinCode
Firmware Version 1.1.1048
Name Gryffindor electronic portrait
Schließung Snape's dungeon
Pinlänge 4
Letzte Synchronisierung 18.04.2024 14:12:57
Sync Programmiert
Batteriestatus Ok

PINS

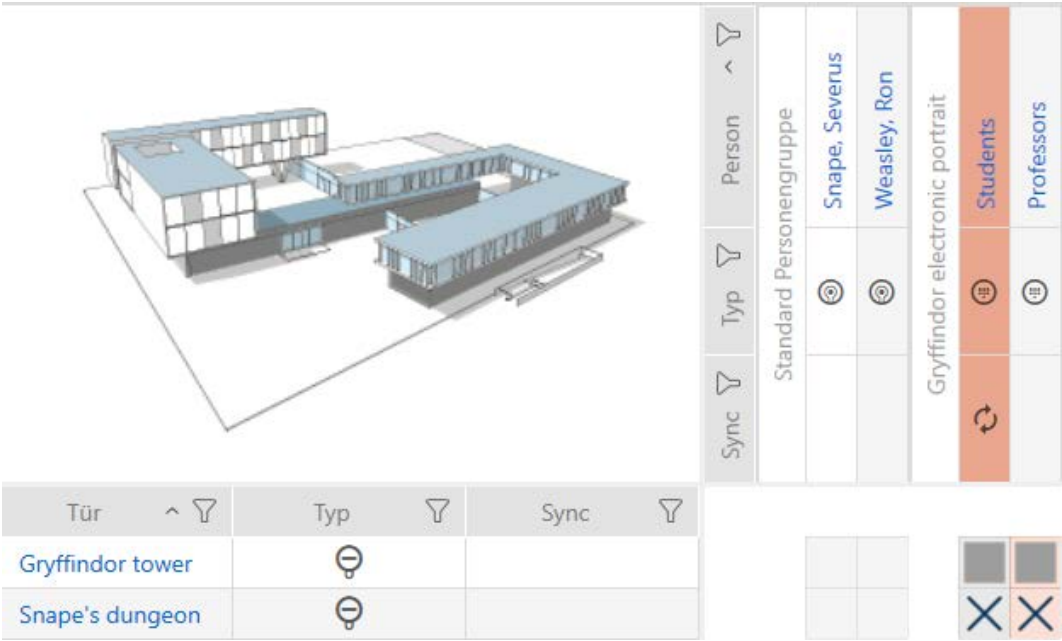
1	Pin Name	Students	PIN	****	Sync	Berechtigt	Status	Programmiert
2	Pin Name	Professors	PIN	****	Sync	Berechtigt	Status	Programmiert

Hinzufügen

< Zurück Weiter > Fertigstellen Abbrechen

3. Click on the **Finish** button.

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



15.22 Set up a dynamic time window (time budget)

The dynamic time window (= "time budget") ensures that the identification media in your locking system are regularly activated via the gateway (for further information, see *Virtual network* [▶ 608]).

The dynamic time window in the virtual network differs from the Offline time budget (in days) of the AX2Go, see *Time budget (AX2Go and virtual network)* [▶ 599]. For the configuration of Offline time budget (in days) for AX2Go see *AX2Go settings* [▶ 544].

You have three options to choose from:



☒ Do not change time window on the gateway	The use of this identification medium is not restricted by a time budget. It can be used permanently on authorised locking devices.
☒ until a particular time of (next) day	After activation at the gateway, this identification medium may be utilised to operate authorised locking devices until the designated time (e.g. 12 noon).

⦿ Number of hours from the last full hour of the booking	After activation at the gateway, this identification medium may be utilised to operate authorised locking devices until the set number of hours has elapsed.
---	---

This setting is customised for each transponder. It is important to select the correct tab "Transponder configuration" setting:

You can also set a dynamic time window (see [Create locking system \[▶ 367\]](#)) within the lock system details. This only applies to newly created identification media (default settings) and does not affect the time window of existing identification media.

If you want to change the time window for existing identification media retrospectively, you need to adjust the settings for each medium individually. It is therefore advisable to set the time budget at the time of installing a locking system (*Best practice: setting up the locking system [▶ 37]*).

16. Doors and locking devices

Any changes you make to the locking system will only take effect when synchronised (see *Synchronising the locking device (including reading access list)* [► 417]).

16.1 Creating a locking device

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

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

See *“Engaging”, “opening”, “locking”, etc.* [► 583] for more information on this topic.

In line with best practice requirements (see *Best practice: setting up the locking system* [► 37]), SimonsVoss recommends that you first plan things out in preparation:

- *Access levels* [► 340] (see *Access levels* [► 602] for background information)
- *Creating an area* [► 93] (see *Areas* [► 607] for background information)
- *Creating a schedule* [► 63] or *Create time group* [► 66] (see *Time groups and schedules* [► 587] for background information)
- *Creating a time switchover* [► 75] (see *Time switchovers* [► 591] for background information)
- *Creating a location* [► 87] or *Creating a building and assigning it to a location* [► 90] (see *Buildings and locations* [► 606] for background information)
- *Creating a hashtag* [► 95] (see *Hashtags* [► 608] for background information)

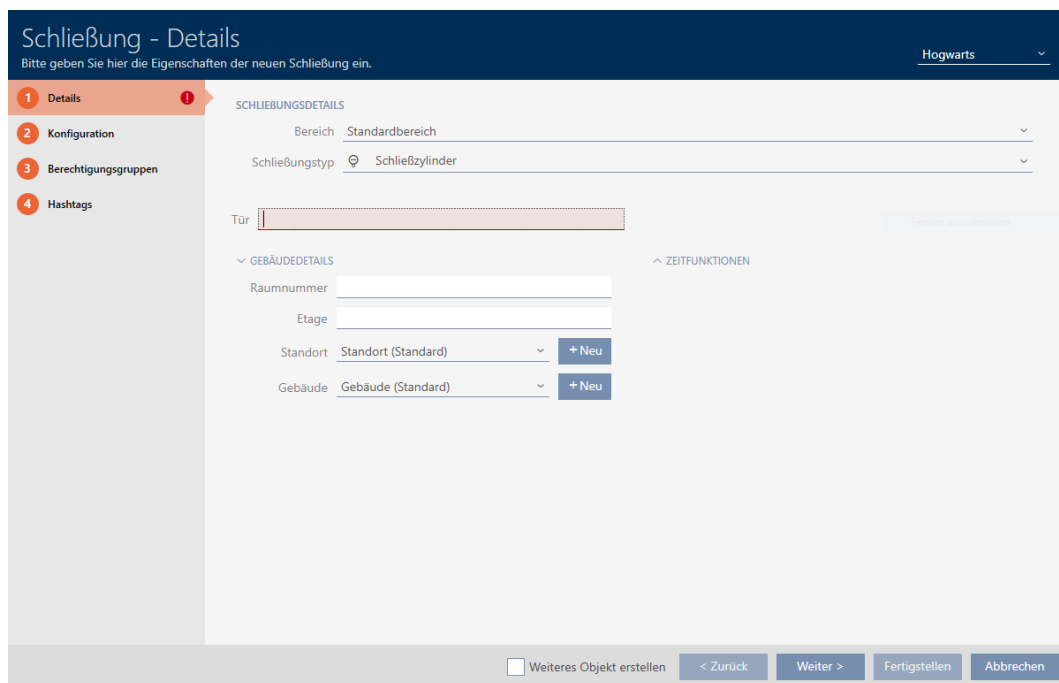


NOTE

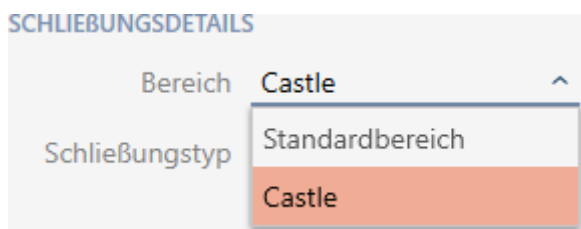
Hidden settings

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.

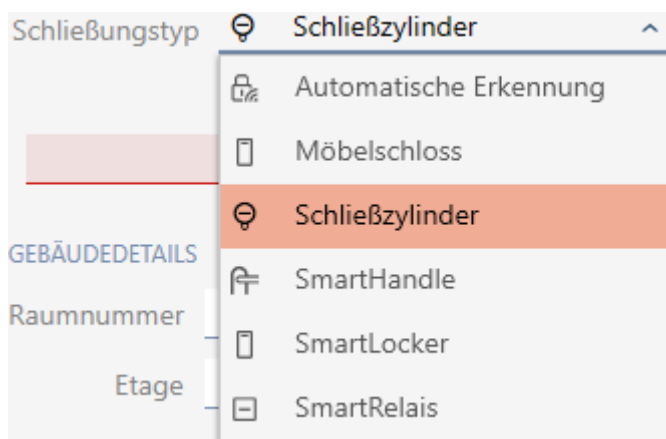
- Click on the **New lock** button .
 ↳ The window for creating a new locking device will open.



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



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

▼ GEBÄUDEDDETAILS

Raumnummer

Etage

Standort

Gebäude

Das Feld ist erforderlich

- 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.

▼ GEBÄUDEDDETAILS

Raumnummer

Etage

Standort

Gebäude

Das Feld ist erforderlich

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)* [► 299] and *Engaging and disengaging locking devices automatically with time switchover* [► 301] for details).

▼ ZEITFUNKTIONEN

Zeitplan	☐	_____ ▼	+ Neu
Zeitumschaltung	☐	_____ ▼	+ Neu
Feiertagsliste	☐	_____ ▼	+ Neu



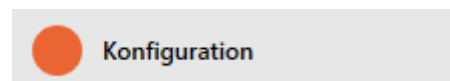
NOTE

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.

Schließung - Konfiguration

Hier können Sie das Verhalten der Schließung konfigurieren

Hogwarts

1 Details

2 Konfiguration

3 Berechtigungsgruppen

4 Hashtags

^ ZEITKONFIGURATION

^ SCHLIEBUNGSFUNKTIONEN

^ SIGNALISIERUNG

^ AX FUNKTIONEN

^ KARTENKONFIGURATION

^ ZEITUMSCHALTUNG-KONFIGURATION

^ ANDERE

^ DOORMONITORING

☐ Weiteres Objekt erstellen

< Zurück

Weiter >

Fertigstellen

Abbrechen

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)* [▶ 307]).

^ ZEITKONFIGURATION

☒ Zugangsprotokollierung
 ☐ Unberechtigte Zutrittsversuche protokollieren
 ☐ Ausnahmen im Zeitonenmanagement zulassen

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* [▶ 309] and *Limit locking device read range (close range mode)* [▶ 311]).

^ SCHLIEBUNGSFUNKTIONEN

Öffnungsdauer (Sek.)

5

☐ Daueröffnung

☐ Nahbereichsmodus (bei interner Antenne)

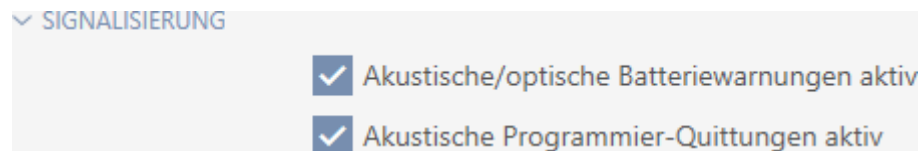


NOTE

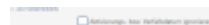
Button control not adjustable

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)* [► 312]).



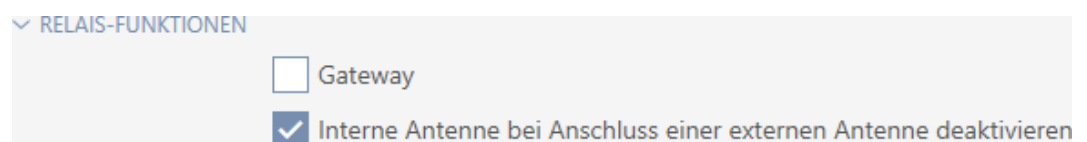
14. If you want to ignore the activation time window (see Activation date / expiry date), expand the "AX functions" menu and configure the settings (see *Ignoring activation and expiry date of identification media* [► 316]).



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* [► 314]).

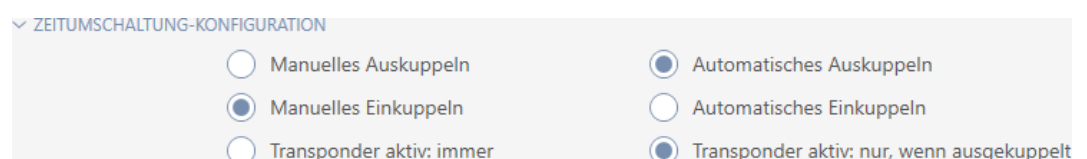


16. If you want to use the internal and external antenna together in a SmartRelay, expand the "Relay functions" menu and configure the settings (see *Using internal and external antenna simultaneously* [► 318]).



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* [► 301]).

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.

▼ ANDERE

☐ Freidrehend



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 Innenknauf und eine andere für den Außenknauf.
Beide Schließungen müssen separat konfiguriert und programmiert werden!



OK

19. 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 \[▶ 317\]](#)).

☐ Nur berechnete TIDs über serielle Schnittstelle ausgeben

Schnittstelle keine

☐ Schnittstelle: Zusatzsignal CLS

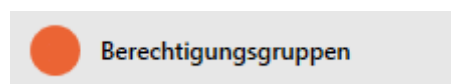
☒ Externe LED ☐ Externer Piepser

☐ SR Signal invertieren

☐ LED ausschalten

☐ Piepser ausschalten

20. Click on the  Access levels tab.



➡ Window switches to the "Access levels" tab.

Schließung - Berechtigungsgruppen

Hier können Sie die Schließung zu Berechtigungsgruppen hinzufügen

- Details
- Konfiguration
- Berechtigungsgruppen**
- Hashtags

AUSGEWÄHLT (0)

Name	Beschreibung
------	--------------

NICHT AUSGEWÄHLT (4)

Name	Beschreibung
Gryffindor	
Hufflepuff	
Ravenclaw	
Slytherin	

Neue Berechtigungsgruppe

☐ Weiteres Objekt erstellen < Zurück Weiter > Fertigstellen Abbrechen

21. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [► 54]).

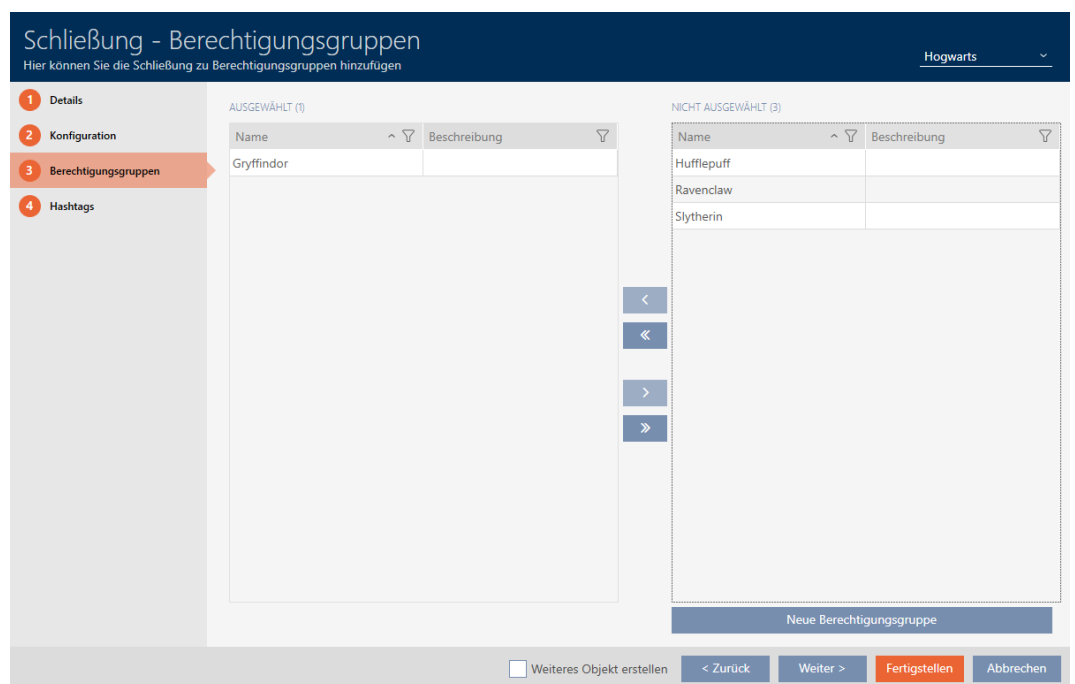
22. Select all access levels to which you wish to assign your locking device (Ctrl+click for individual groups or Shift+click for multiple groups).

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

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

23. Use  to move the selected access levels only or  to move all displayed access levels.

→ Your locking device is added to the access levels in the left-hand column.



Schließung - Berechtigungsgruppen
Hier können Sie die Schließung zu Berechtigungsgruppen hinzufügen

Hogwarts

1 Details
2 Konfiguration
3 Berechtigungsgruppen
4 Hashtags

AUSGEWÄHLT (1)

Name	Beschreibung
Gryffindor	

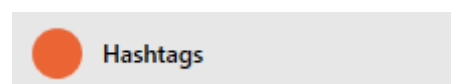
NICHT AUSGEWÄHLT (3)

Name	Beschreibung
Hufflepuff	
Ravenclaw	
Slytherin	

Neue Berechtigungsgruppe

☐ Weiteres Objekt erstellen < Zurück Weiter > Fertigstellen Abbrechen

24. Click on the  Hashtags tab.



→ Window switches to the "Hashtags" tab.

25. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

26. 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.

27. 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.

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

29. Click the **Finish** button to create the locking device.

→ The window for creating a new locking device closes.

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

16.1.1 Importing locking devices

The import function allows the simultaneous creation of multiple locking devices/doors. To do this, you need an import file in CSV or XLSX format. The columns in this file are subsequently assigned to a field in the AXM Plus. A new locking device (and a new door) are created with each new line, and the fields are populated with the contents of their assigned columns.

Ideally, your import file is encoded in **Unicode (UTF-8)** format.

There is a similar function for identification media and persons: [Import identification media](#) [▶ 117]

Example file

An example file could look like this:

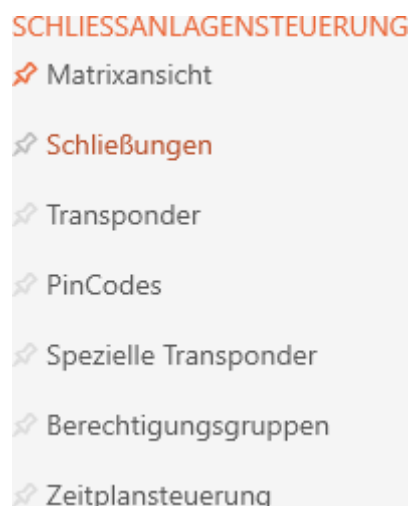
	A	B	C	D	E
1	Türnummer	Bezeichnung	Etage	Beschreibung	Gebäude
2	1	Besuchereingang	EG	Rezeption	Besuchergebäude
3	2	Wareneingang	EG	Versand	Halle A
4	3	Notausgang	EG	Lager	Halle A
5	4	Haupteingang	EG	Reinigung	Halle A
6	5	Nebeneingang	EG	Prozesse	Halle B
7	6	Südausgang	OG	Reinigung	Halle B
8	7	Außenmittelsbereich	OG	Produktion	Halle B
9	8	Parkplatz	EG	Produktion	Halle B
10	9	Garage	UG	Vorstand	Besuchergebäude

- ✓ Selection values (e.g. "Building"), which appear in the import file, have already been created (see e.g. *Creating a building and assigning it to a location* [▶ 90]).

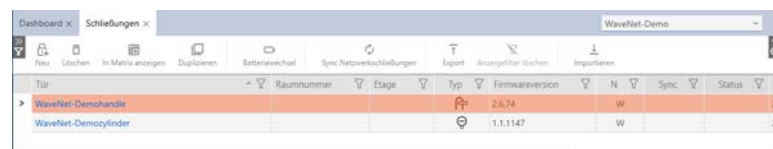
1. Click the orange AXM button .
 - ↳ AXM bar opens.



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



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



3. Click on the **Import** button.
 - ↳ The window will open.

Import - Türen

Hier können Sie Türen importieren

Importdatei auswählen

Durchsuchen

EncodingUnicode (UTF-8)

Trennzeichen:

Zeilen überspringen0

Import Optionen

Standard-AXM-Optionen für neue Türen

SchließanlageWaveNet-Demo

BereichAutomatisch generiert

SchließungstypAutomatische Erkennung

Spaltenzuordnung

Importieren

Abbrechen

4. Click the **Browse** button and navigate to your import file. You may need to set the file type to see your import file.

xlsx-Dateien (*.xlsx)

csv-Dateien (*.csv)

xlsx-Dateien (*.xlsx)

➡ Area "Column mapping" is loading.

Import - Türen

Hier können Sie Türen importieren

Importdatei auswählen

Durchsuchen

EncodingUnicode (UTF-8)

Trennzeichen:

Zeilen überspringen1

Import Optionen

Standard-AXM-Optionen für neue Türen

SchließanlageWaveNet-Demo

BereichAutomatisch generiert

SchließungstypAutomatische Erkennung

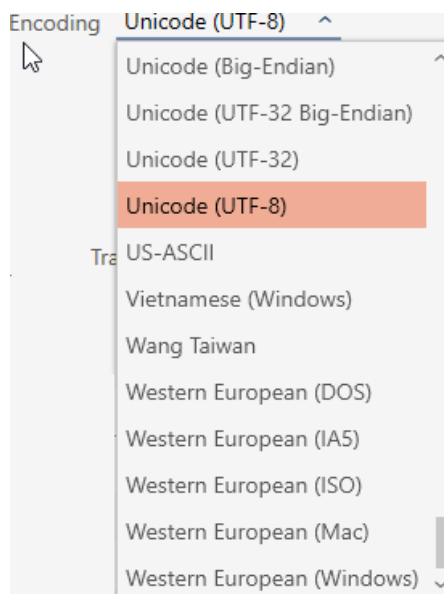
Spaltenzuordnung

☐	nein	nein	nein	nein	nein	nein	nein	nein
☐	1	Besuchereingang	EG	Rezeption	Besuchergebäude			
☐	2	Warenausgang	EG	Versand	Halle A			
☐	3	Notausgang	EG	Lager	Halle A			
☐	4	Haupteingang	EG	Reinigung	Halle A			
☐	5	Nebeneingang	EG	Prozesse	Halle B			
☐	6	Südausgang	OG	Reinigung	Halle B			
☐	7	Aufenthaltsbereich	OG	Produktion	Halle B			
☐	8	Parkplatz	EG	Produktion	Halle B			
☐	9	Garage	UG	Vorstand	Besuchergebäude			

Importieren

Abbrechen

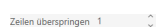
5. Select the encoding for your import file from the dropdown menu; ▼ **Encoding** (recommendation: import the file in **Unicode (UTF-8)** format).



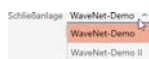
6. Select the delimiter for your import file from the dropdown menu ▼ **Delimiter** (in the example: ;).



7. In field *Skip rows*, give the number of import file lines that should be skipped (for example, column headings, in the example: 1).



8. Open the dropdown menu ▼ **Locking system** and select the target locking system .



9. Use this drop-down menu ▼ **Areato** to select the field in the locking devices details into which you want to import the entry in this column.



10. Use the drop-down menu ▼ **Lock type** to select the type of locking device for the imported locking devices.



11. Each column has a drop-down menu above it. Use this drop-down menu to select the field in the locking device details into which you want to import the entry in this column. If you select the entry "None", the column will be ignored and not imported. The entries "Door code (*)" and "Door name (*)" must be selected as these fields are mandatory (*) fields.



NOTE

Values to be imported must be selected before importing

Fields such as "Location" or "Building" are selection values. Only existing values may be selected for import; new values cannot be created.

If a selection value is not available, the field is skipped during import.

- Create all required values before importing.

↳ Columns are assigned to the fields in the locking device details.

Import - Türen

Hier können Sie Türen importieren

Importdatei auswählen

Q:\Produktmarketing\40 Technische Redaktion'

Durchsuchen

Encoding

Unicode (UTF-8)

Trennzeichen

:

Zeilen überspringen

1

Import Optionen

Standard-AXM-Optionen für neue Türen

Schließanlage

WaveNet-Demo

Bereich

Außentüren

Schließungstyp

Automatische Erkennung

Spaltenzuordnung

☐	Türcode (*)	Türname (*)	Etage	nein	Gebäude	nein	nein	nein
☐	1	Besuchereingang	EG	Rezeption	Besuchergebäude			
☐	2	Warenausgang	EG	Versand	Halle A			
☐	3	Notausgang	EG	Lager	Halle A			
☐	4	Haupteingang	EG	Reinigung	Halle A			
☐	5	Nebeneingang	EG	Prozesse	Halle B			
☐	6	Südausgang	OG	Reinigung	Halle B			
☐	7	Aufenthaltsbereich	OG	Produktion	Halle B			
☐	8	Parkplatz	EG	Produktion	Halle B			
☐	9	Garage	UG	Vorstand	Besuchergebäude			

Importieren

Abbrechen

12. Mark all the lines you want to import.

Import - Türen

Hier können Sie Türen importieren

Importdatei auswählen

Q:\Produktmarketing\40 Technische Redaktion'

Durchsuchen

Encoding

Unicode (UTF-8)

Trennzeichen

:

Zeilen überspringen

1

Import Optionen

Standard-AXM-Optionen für neue Türen

Schließanlage

WaveNet-Demo

Bereich

Außentüren

Schließungstyp

Automatische Erkennung

Spaltenzuordnung

☒	Türcode (*)	Türname (*)	Etage	nein	Gebäude	nein	nein	nein
☒	1	Besuchereingang	EG	Rezeption	Besuchergebäude			
☒	2	Warenausgang	EG	Versand	Halle A			
☒	3	Notausgang	EG	Lager	Halle A			
☒	4	Haupteingang	EG	Reinigung	Halle A			
☒	5	Nebeneingang	EG	Prozesse	Halle B			
☒	6	Südausgang	OG	Reinigung	Halle B			
☒	7	Aufenthaltsbereich	OG	Produktion	Halle B			
☒	8	Parkplatz	EG	Produktion	Halle B			
☒	9	Garage	UG	Vorstand	Besuchergebäude			

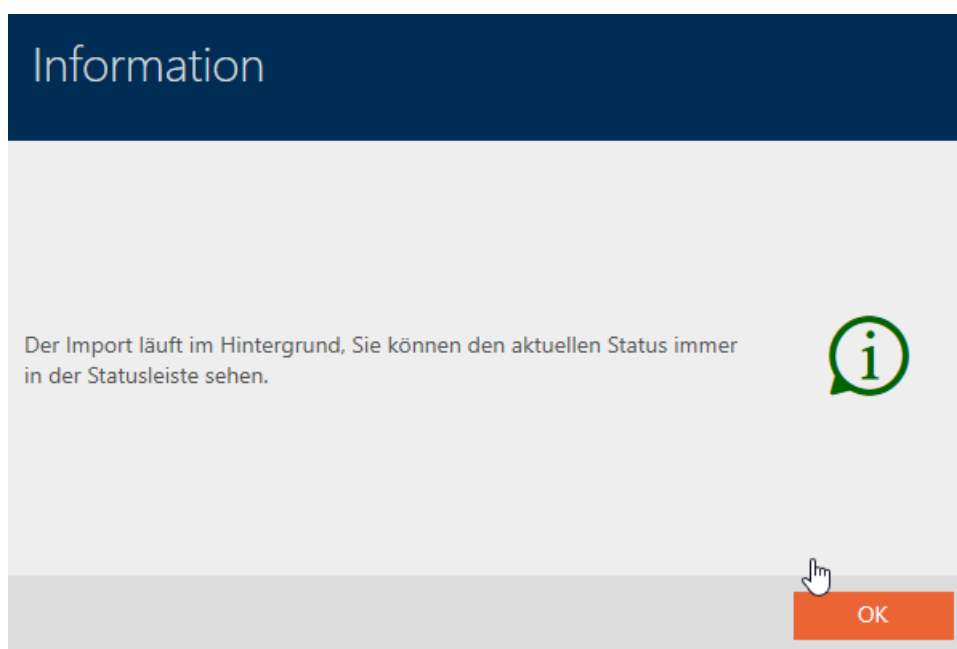
Importieren

Abbrechen

13. Click the

Import

 button.
➡ Import begins.



➡ Once the import is complete, the imported locking devices/doors can be seen in the list of locking devices:

Dashboard x

Schließungen x

WaveNet-Demo

Neu

Löschen

In Matrix anzeigen

Duplizieren

Batteriewechsel

Sync Netzwerkverschließungen

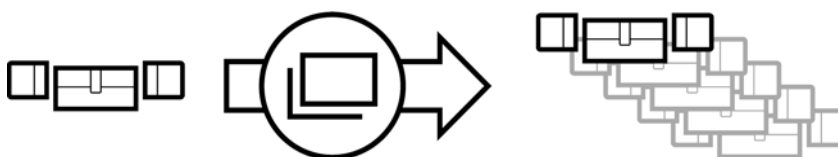
Export

Anzeigefilter löschen

Importieren

Tür	Raumnummer	Etage	Typ	Firmwareversion	N	Sync	Status
Aufenthaltsbereich		OG					
Besuchereingang		EG					
Garage		UG					
Haupteingang		EG					
Nebeneingang		EG					
Notausgang		EG					
Parkplatz		EG					
Südausgang		OG					
Warenausgang		EG					
WaveNet-Demohandle				2.6.74	W		
WaveNet-Demozylinder				1.1.1147	W		

16.2 Duplicating the locking device (including authorisations and settings)



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

The following settings are duplicated:

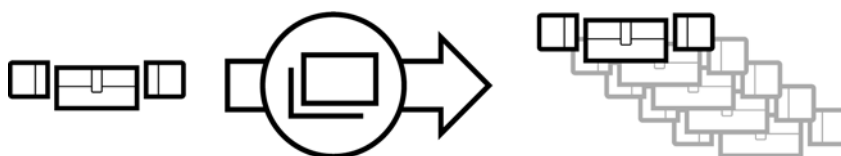
- ## ■ Building details

- ❑ Door details (except door numbering, which is automatically continued with the adjustable abbreviation; also see *Changing automatic numbering* [▶ 491])
- ❑ 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.

Schließungen duplizieren

Hier können Sie die Anzahl der Kopien eingeben

Wie viele Kopien der ausgewählten Schließung sollen erstellt werden?

5

OK

Abbrechen

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

16.3 Delete locking device

There are two ways to delete locking devices:

- 1. Delete on the matrix screen (*Deleting an individual locking device using the matrix [▶ 264]*)
- 2. Delete using the tab for locking devices (*Deleting several locking devices using the tab [▶ 265]*)

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

16.3.1 Deleting an individual locking device using the matrix

- ✓ Matrix screen open.
- 1. Select the locking device that you wish to delete.

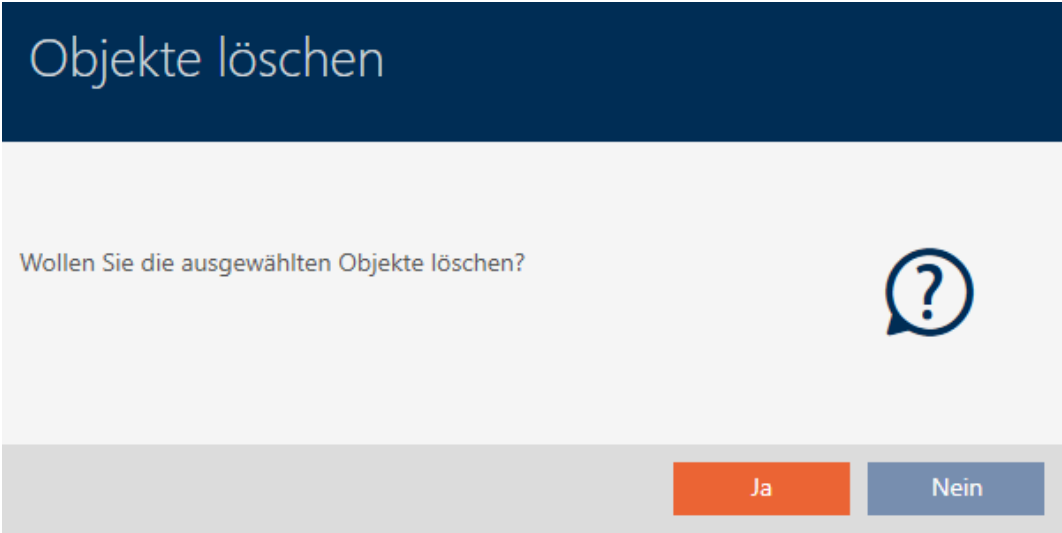


Tür	Typ
Gryffindor dormitory	🔒
Hufflepuff dormitory	🔒
Gryffindor dormitory_0001	🔒

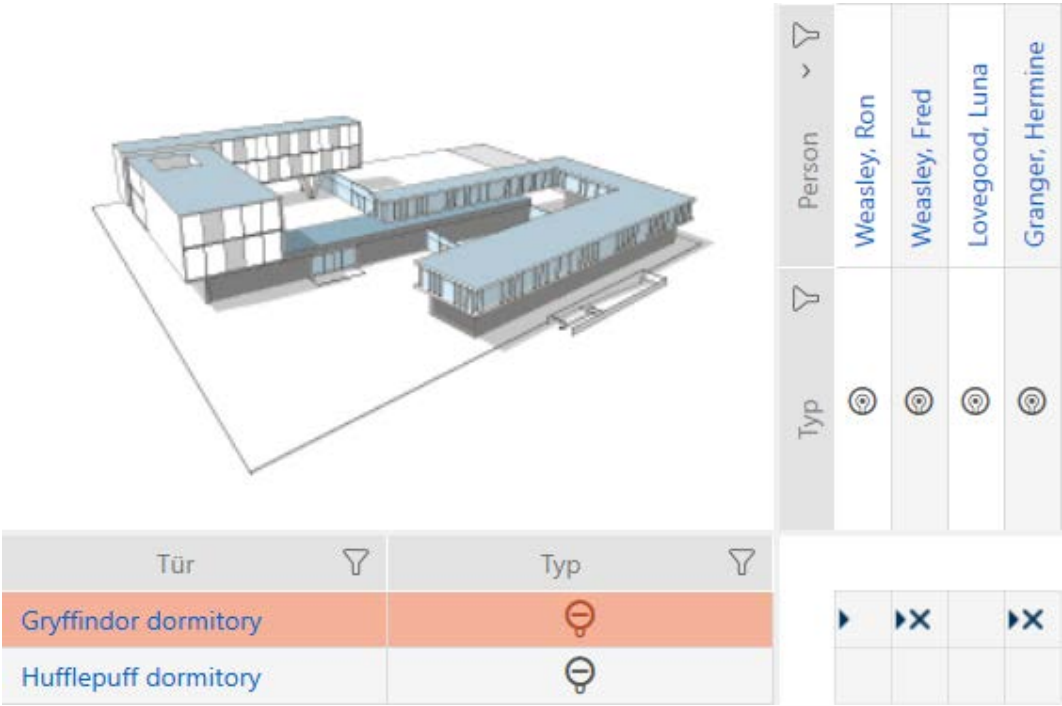
Person
Weasley, Ron
Weasley, Fred
Lovegood, Luna
Granger, Hermine

▶	▶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.



16.3.2 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.

SCHLIESSANLAGENSTEUERUNG

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

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

Matrixansicht x Schließungen x									
Neu Löschen In Matrix anzeigen Duplizieren Batteriewechsel Export Anzeigefehler löschen									
Hogwarts 1									
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* [▶ 54]).

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

Matrixansicht x Schließungen x									
Neu Löschen In Matrix anzeigen Duplizieren Batteriewechsel Export Anzeigefilter löschen Hogwarts 1									
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	

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

Objekte löschen

Wollen Sie die ausgewählten Objekte löschen?



Objekte die gelöscht werden

Gryffindor dormitory_0005
Gryffindor dormitory_0004
Gryffindor dormitory_0003
Gryffindor dormitory_0002
Gryffindor dormitory_0001

Ja

Nein

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

Matrixansicht x Schließungen x									
Neu Löschen In Matrix anzeigen Duplizieren Batteriewechsel Export Anzeigefilter löschen Hogwarts 1									
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	

16.4 Changing locking device type at later stage

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

AXM 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. ☒ Invert SR signal)	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.

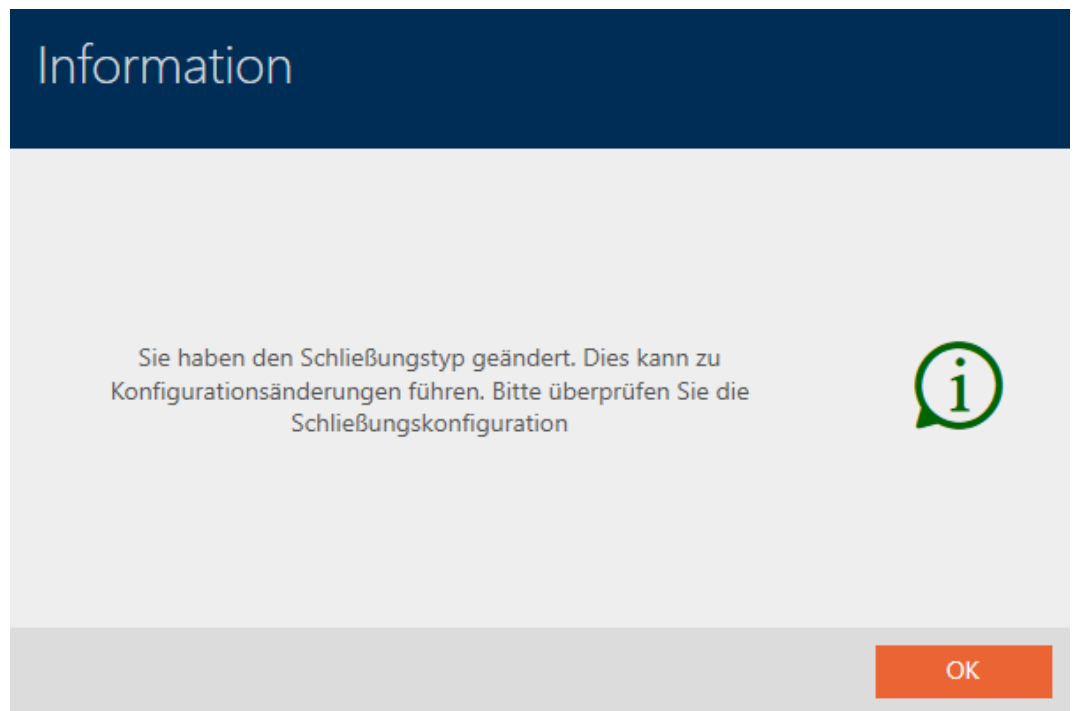
- ✓ Locking device list or matrix view open.
- ✓ Locking device available.
- ✓ Locking device not synchronised (if necessary reset, see *Re-setting the locking device* [► 426]).

1. Click on the locking device whose type you wish to change.

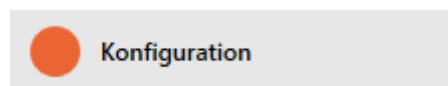
→ The locking device window will open.

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

→ Warning about the configuration change will open.



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



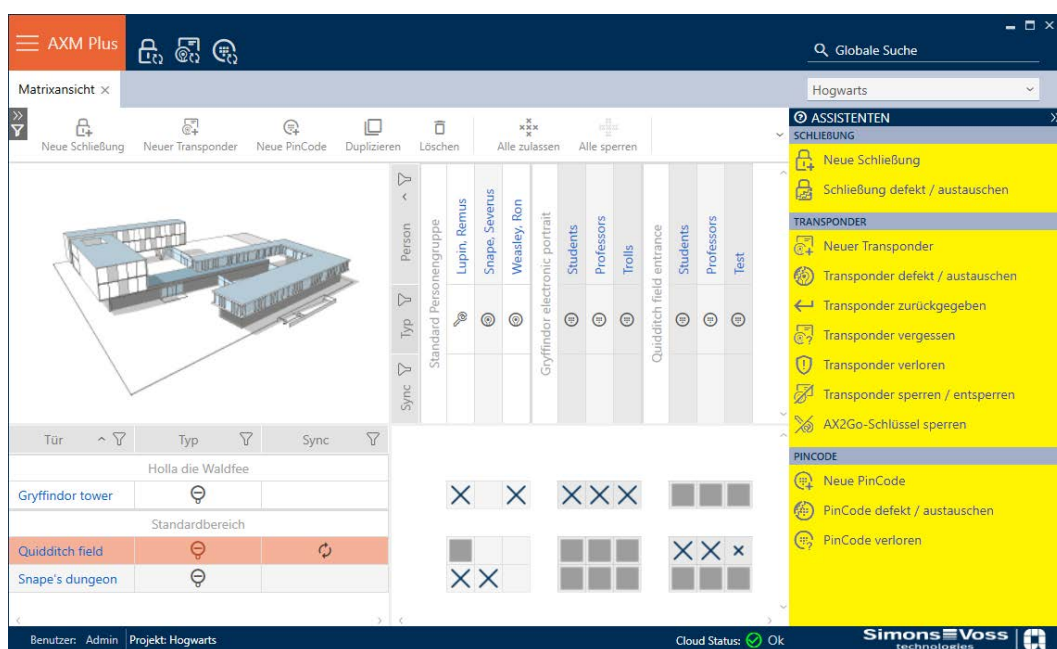
- ↳ Window switches to the "Configuration" tab.
5. Check and change the configuration if necessary.
6. Click on the **Finish** button.
 - ↳ The locking device window closes.
- ↳ Locking device type has been changed.

16.5 Handling defective locking devices

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

- Software defects
- Hardware defects

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



AXM 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 [► 571]

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	■ Locking devices with external damage (e.g. scratched). ■ Locking devices that should be replaced as a precaution (e.g. if they get wet).	Locking devices permanently damaged (e.g. thumb-turn broken off) which require replacement.

Example situation:

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

Procedure:

Repair	Resetting and replacing	Delete and replace
<i>Re-synchronise (repair)</i> [▶ 275] 1. Reset (= LID available in database again) 2. Resynchronise (= LID is immediately written back onto the same locking device) The locking device works the same as before after repair.	<i>Resetting and replacing</i> [▶ 277] 1. Reset (= LID flagged as defective in database and removed from original locking device) 2. Synchronise replacement locking device with new LID The LID is no longer contained in the locking device due to the reset. The locking device can therefore no longer be used. However, it can be re-synchronised. A new LID is written onto the locking device during resynchronisation. The previous locking device remains in the database with its LID and is flagged as defective.	<i>Delete and replace</i> [▶ 282] 1. Synchronise replacement locking device with new LID 2. Delete defective locking device It is obviously no longer possible to reset a permanently damaged locking device. It is thus replaced by a replacement locking device with a new LID. The faulty locking device's LID can be used for another locking device in the future.

Locking device is not required again immediately:

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

Example situation:

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

Procedure:

Reset	Purge (software reset)
<i>Reset [▶ 287]</i> Resetting removes the LID from the locking device. You can synchronise another locking device with this entry later, which will receive the same LID.	<i>Purge (only reset in database/software reset) [▶ 289]</i> 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. The LID is separated from the LID for the locking device previously used during the clean-up in the database (in current state). After cleaning up an entry, you can synchronise any locking device again with this entry at a later stage and it will receive the same LID. After the software reset, your AXM 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</i> [▶ 426]). This deletes the LID from the old locking device and prevents the same LID from being in circulation twice.



NOTE

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

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

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

16.5.1 Re-synchronise (repair)

- ✓ 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* [▶ 54]).
 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.

Schließung defekt / austauschen - Assistent

Schließanlage
Hogwarts

Schließung
Gryffindor dormitory (00AXNNH)

Programmiergerät
SmartCD aktiv (beschäftigt)

SCHLIEßUNG INSTAND SETZEN



Verbindung aufgebaut

Bitte halten Sie die Schließung in die Nähe des SmartCD's (ca. 5-20 cm) bis die Programmierung abgeschlossen ist

Abbrechen

Weiter
Schließen

➔ Locking device is resynchronised.

SCHLIEßUNG INSTAND SETZEN

Schließung erfolgreich instand gesetzt.

16.5.2 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* [▶ 54]).
 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.

Schließung defekt / austauschen - Assistent

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

SCHLIEßUNG AUSTAUSCHEN



Zurücksetzen

Die Schließung wird zurückgesetzt

Abbrechen



Verbindung aufgebaut



Bitte halten Sie die Schließung in die Nähe des SmartCD's (ca. 5-20 cm) bis die Programmierung abgeschlossen ist

Weiter

Schließen

- ↳ 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	▼

SCHLIEßUNG 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.

Schließung defekt / austauschen - Assistent

Schließanlage Hogwarts ▼

Schließung Gryffindor dormitory_1 ▼

Programmiergerät SmartCD aktiv (beschäftigt) ▼

SCHLIEßUNG AUSTAUSCHEN

Programmierung

Ausstattung der Schließung wird gelesen

Abbrechen

Verbindung aufgebaut

Bitte halten Sie die Schließung in die Nähe des SmartCD's (ca. 5-20 cm) bis die Programmierung abgeschlossen ist

Weiter Schließen

➞ Replacement locking device is synchronised.

SCHLIEßUNG AUSTAUSCHEN

Die Aktion wurde erfolgreich durchgeführt

➞ Replacement locking device is displayed in the matrix.

Tür ▼	Typ ▼	Sync ▼
Gryffindor dormitory		
Hufflepuff dormitory		
Stadium illumination		
Gryffindor dormitory_1		

16.5.3 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* [▶ 54]).

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 **No** button.
 - ↳ Reset query will close.
 - ↳ 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

Ja Nein

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.

WeiterSchließen

9. Click on the **Next** button.

- Replacement locking device is being synchronised.

Schließung defekt / austauschen - Assistent

Schließanlage: Hogwarts ▾

Schließung: Gryffindor dormitory_1 ▾

Programmiergerät: SmartCD aktiv (beschäftigt) ▾

SCHLIEßUNG AUSTAUSCHEN

Programmierung

Ausstattung der Schließung wird gelesen

Abbrechen

Verbindung aufgebaut

Bitte halten Sie die Schließung in die Nähe des SmartCD's (ca. 5-20 cm) bis die Programmierung abgeschlossen ist

Weiter Schließen

➞ Replacement locking device is synchronised.

SCHLIEßUNG 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			

16.5.4 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* [▶ 54]).
 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.

Schließung defekt / austauschen - Assistent

Schließanlage
Hogwarts
▼

Schließung
Gryffindor dormitory_1 (00AXNNH)
▼

Programmiergerät
SmartCD aktiv (beschäftigt)
▼

SCHLIEßUNG ZURÜCKSETZEN / BEREINIGEN

Zurücksetzen

Zustand der Schließung wird ausgelesen

Abbrechen

Verbindung aufgebaut

Bitte halten Sie die Schließung in die Nähe des SmartCD's (ca. 5-20 cm) bis die Programmierung abgeschlossen ist

Weiter

Schließen

- ↳ Locking device is reset.

SCHLIEßUNG ZURÜCKSETZEN / BEREINIGEN

Schließung erfolgreich zurückgesetzt

16.5.5 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* [▶ 54]).
 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.

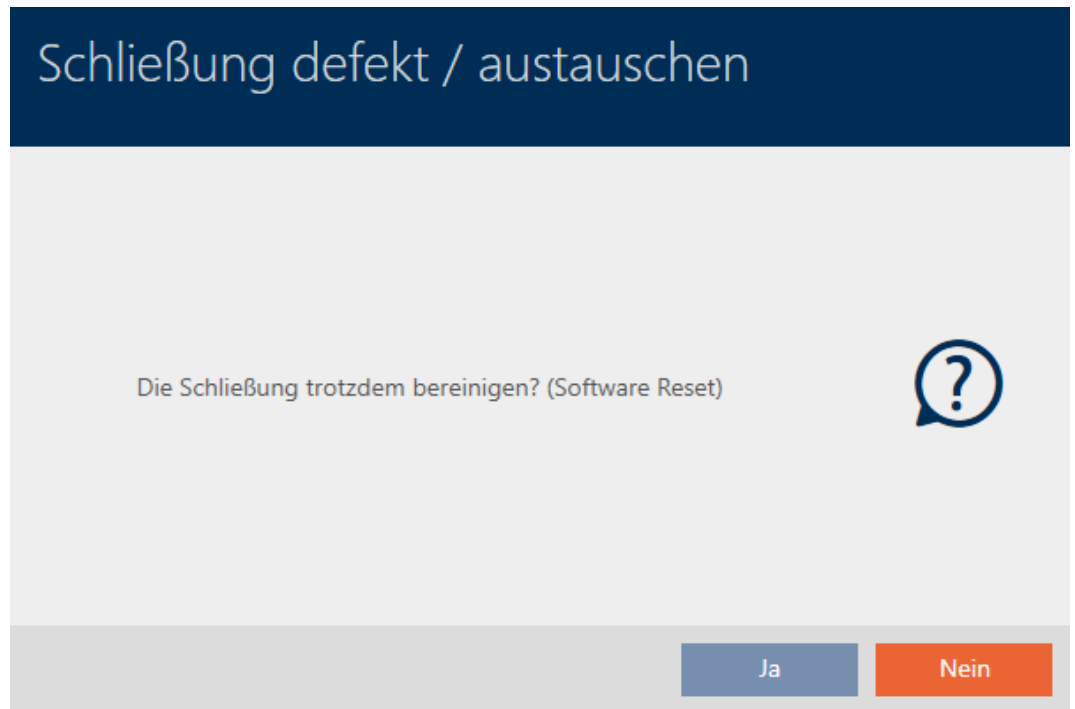
Schließung defekt / austauschen

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.

16.6 Assigning locking devices to buildings/locations

You must specify a location and a building the moment you create a locking device. Ideally, you should follow best practice (see *Best practice: setting up the locking system* [▶ 37]) and plan everything out in preparation before creating your locking devices (see *Organisational structure* [▶ 60]). 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* [▶ 87]).
 - ✓ At least one building created (see *Creating a building and assigning it to a location* [▶ 90]).
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

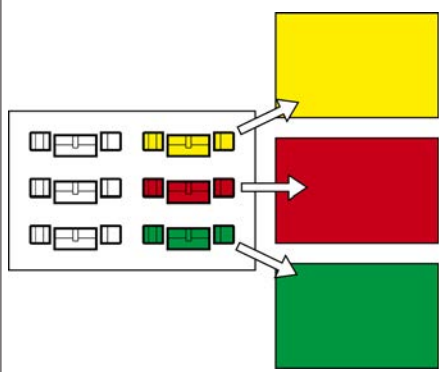
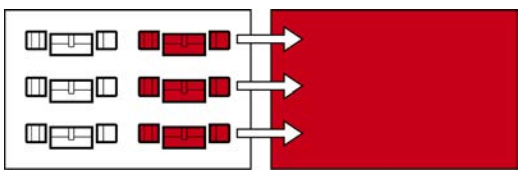
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

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.

16.7 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* [▶ 37]) and plan everything out in advance before creating your locking devices (see *Organisational structure* [▶ 60]). 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
<i>Assigning individual locking devices to a different area (in the locking device window) [▶ 294]</i> Suitable for moving a few locking devices into many different areas: 	<i>Assign multiple locking devices to another area (in the area window) [▶ 296]</i> Suitable for moving multiple locking devices into a few different areas: 

**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 access levels more quickly (see *Adding areas and person groups to access levels* [▶ 349]).

16.7.1 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* [▶ 93]).
1. Click on the locking device you wish to move to another area.
 - ➡ The locking device window will open.

Schließung - Details

Hier können Sie Details der Schließung bearbeiten

Hogwarts

Synchronisieren

In Matrix anzeigen

Online Mode

1 Details

2 Konfiguration

3 Ausstattung

4 Zustand

5 Aktionen

6 Berechtigungsgruppen

7 Hashtags

8 Zutrittsliste

9 Berechtigte Transponder

SCHLIEßUNGSDetails

Bereich

Lands

Seriennummer

088FX8D

Schließungstyp

Schließzylinder

Bestellcode

SV-Z5.LE.19.AM.G2

Firmware Version

1.1.1147

Letzte Synchronisierung

25.04.2024 13:53:42

Batteriestatus

Ok

Sync

Programmiert

TÜRDetails

Tür

Snape's dungeon

Tür-Code

DC-00004

Beschreibung

GEBÄUDEDetails

< Zurück

Weiter >

Fertigstellen

Abbrechen

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

SCHLIEßUNGSDetails

Bereich

Castle

Standardbereich

Castle

Lands

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.

16.7.2 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* [▶ 93]).

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

Bereiche x

+

Neu

🗑️

Löschen

🗑️

Anzeigefilter löschen

⏪

?

	Name	Zeitplan	Beschreibung
>	Castle	5th grade schedule	
	Lands		

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

Bereich - Details

Hier können Sie die Details des Bereichs bearbeiten

1 Details

2 Schließungen

Name

Castle

Zeitplan

5th grade schedule

Beschreibung

< Zurück

Weiter >

Fertigstellen

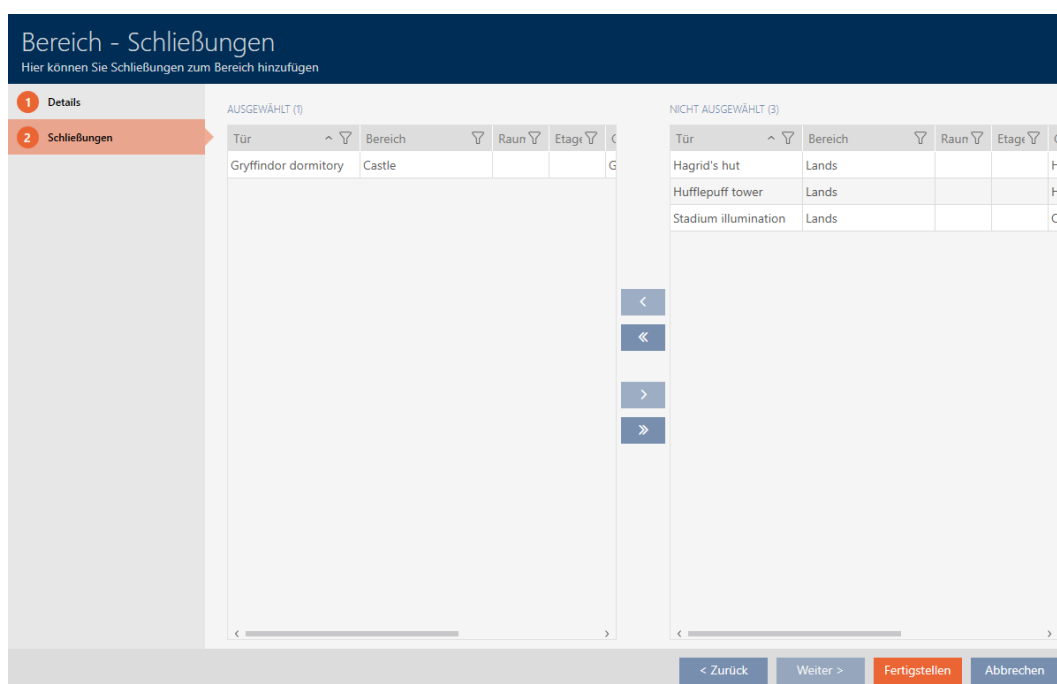
Abbrechen

4. Click on the  Locks tab.



Schließungen

- Window switches to the "Locks" tab.



5. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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.

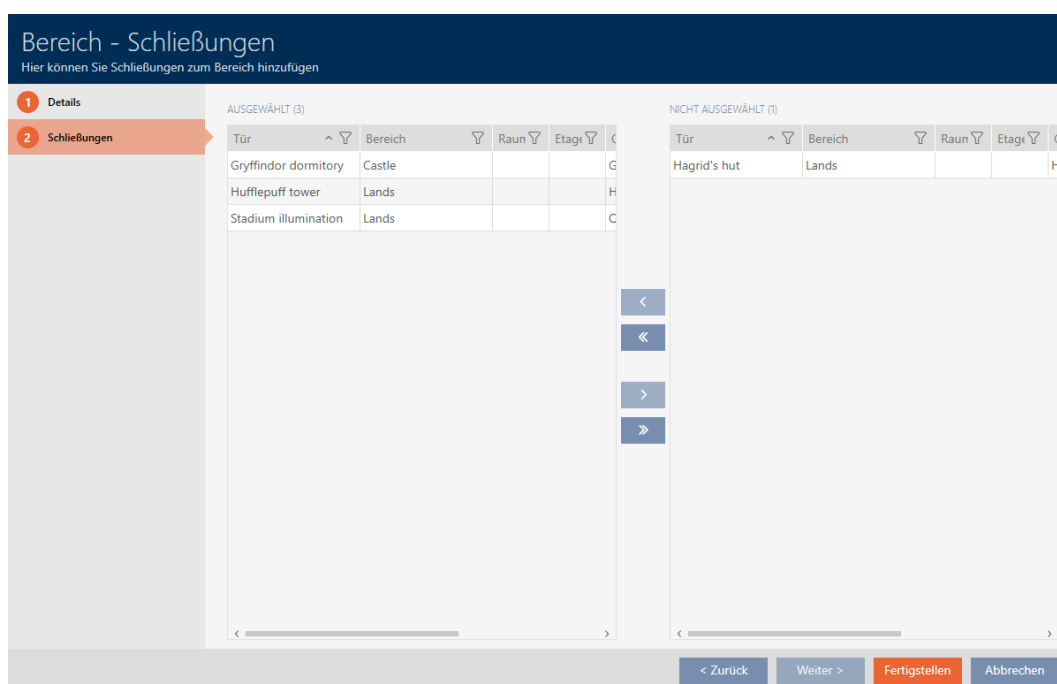


NOTE

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		

16.8 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* [► 587]).

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* [► 356].

- ✓ Locking device created (see [Creating a locking device \[▶ 245\]](#)).
- ✓ Locking device equipped with .ZK option.
- ✓ Schedule created (see [Creating a schedule \[▶ 63\]](#)).

1. Click on the locking device you wish to add.

↳ The locking device window will open.

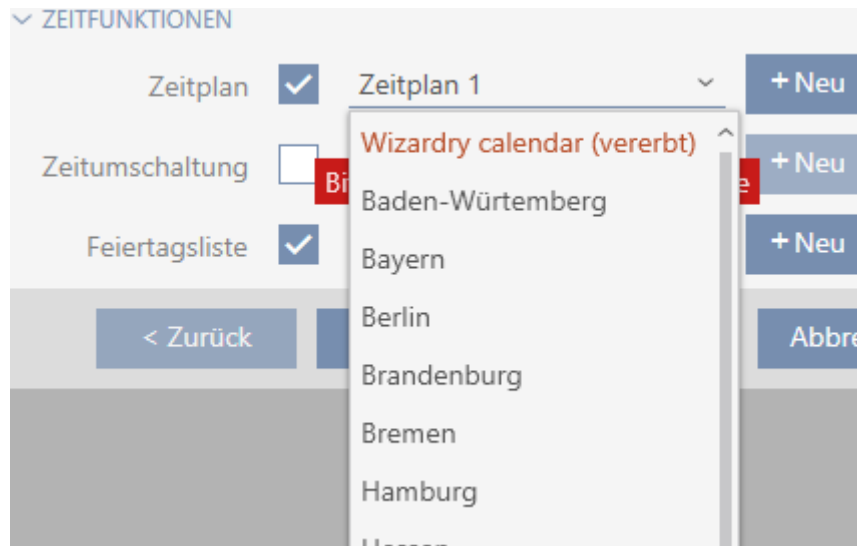
2. Open the "Time functions" menu if necessary.

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

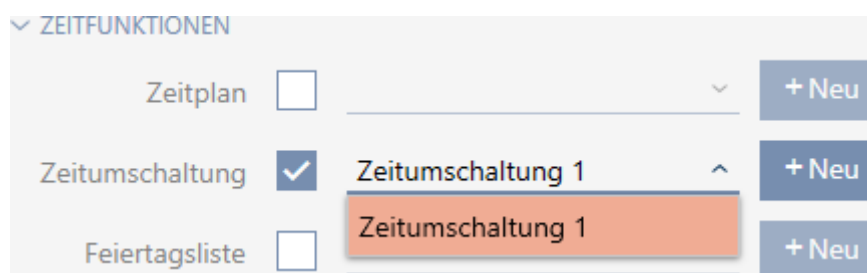
You can assign public holiday lists to both a locking device and the locking device's location. In this case, the public holiday list is used in the locking device and the public holiday list in the location is ignored.

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.

16.9 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* [▶ 37] and *Creating a time switchover* [▶ 75]). This allows you to set the time switchovers directly in the locking device properties when creating locking devices:



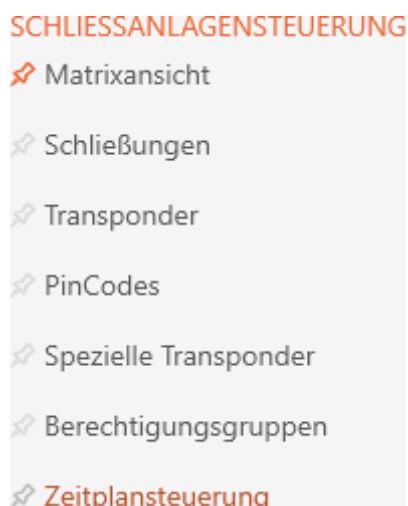
Obviously, you can also add your locking devices to the time switchovers at a later date:

- ✓ Locking device equipped with .ZK option.
- ✓ Time switchover created (see [Creating a time switchover \[► 75\]](#)).

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

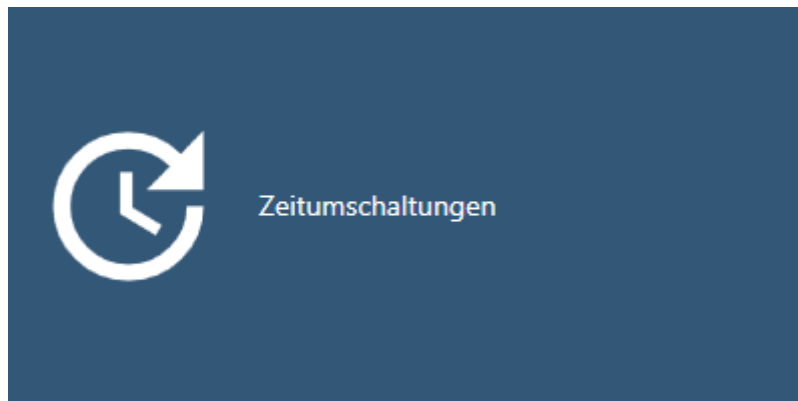


2. Select the **Time schedule control** entry in the | LOCKING SYSTEM CONTROL | group.



- ↳ 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

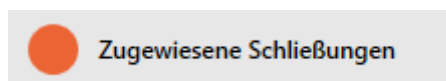
Anzeigefilter löschen

	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* [▶ 54]).
7. Select all locking devices that you wish to open and close with the schedule (Ctrl+click for single devices or Shift+click for multiple devices).

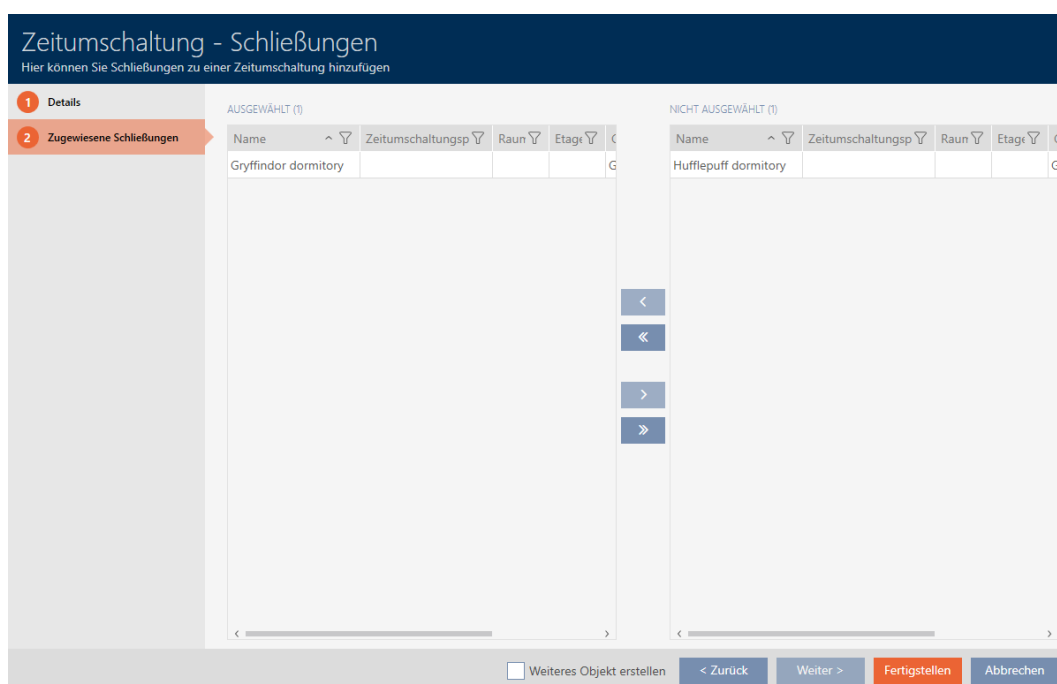


NOTE

Double-clicking as an alternative to arrow keys

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

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



9. Click on the **Finish** button.

→ The time switchover window closes.

10. Click the orange AXM button **AXM**.

→ AXM bar opens.



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

SCHLIESSANLAGENSTEUERUNG

Matrixansicht

Schließungen

Transponder

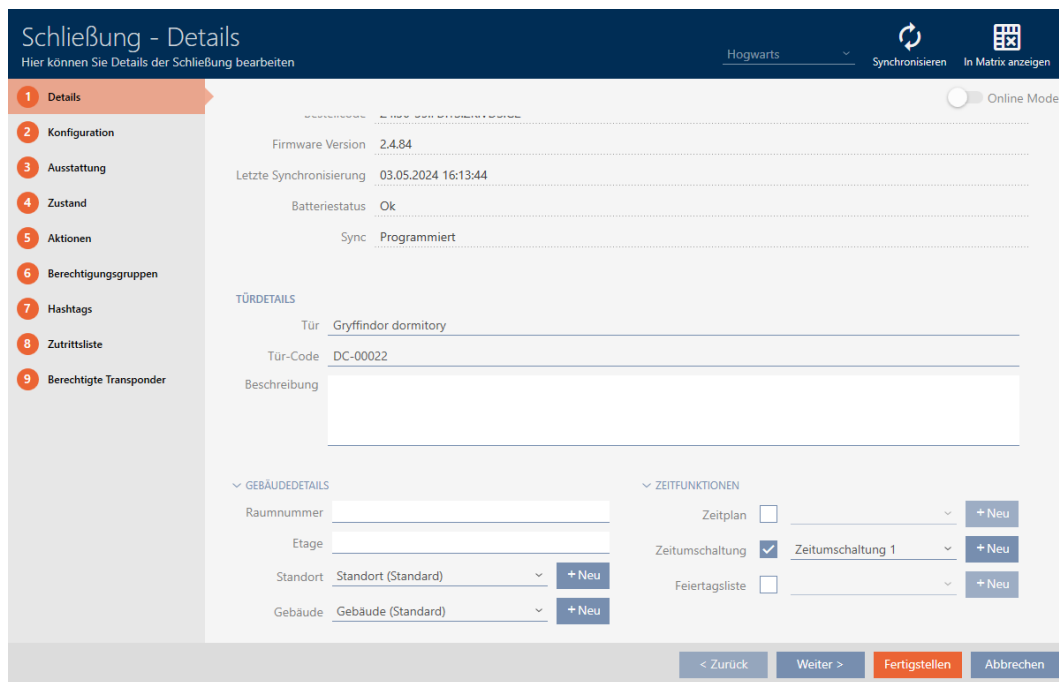
PinCodes

Spezielle Transponder

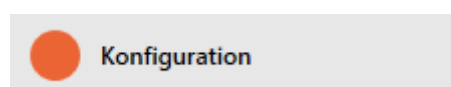
Berechtigungsgruppen

Zeitplansteuerung

- ↳ The AXM bar will close.
 - ↳ The [Locks] tab will open.
12. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
13. Click on the door to be controlled with the time switchover.
- ↳ The locking device window will open.



14. Click on the  **Konfiguration** tab.



- ↳ Window switches to the "Configuration" tab.

15. Set the required behaviour in the "Time switching - Configuration" drop-down menu (see *Time switchovers* [► 591]).

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

➞ The locking device window closes.

➞ Time switchover is set up.

16.10 Have accesses logged by locking device (access list)

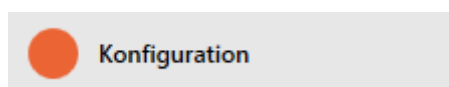
This is where you switch the access list on. Your locking device uses it to log which identification media have been activated (also see *Access and physical access lists* [► 586]).

✓ 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  Audit trail 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)* [► 417]).

The access list can then be opened in the locking device window using the [Audit trail] tab (see *Displaying and exporting a locking device's access list* [► 422]).

16.11 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:

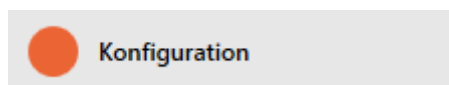
- *Allowing an identification medium to open twice as long* [► 130]
- *Engaging and disengaging locking devices automatically with time switchover* [► 301]

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.

16.12 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.



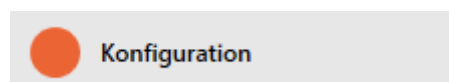
NOTE

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.

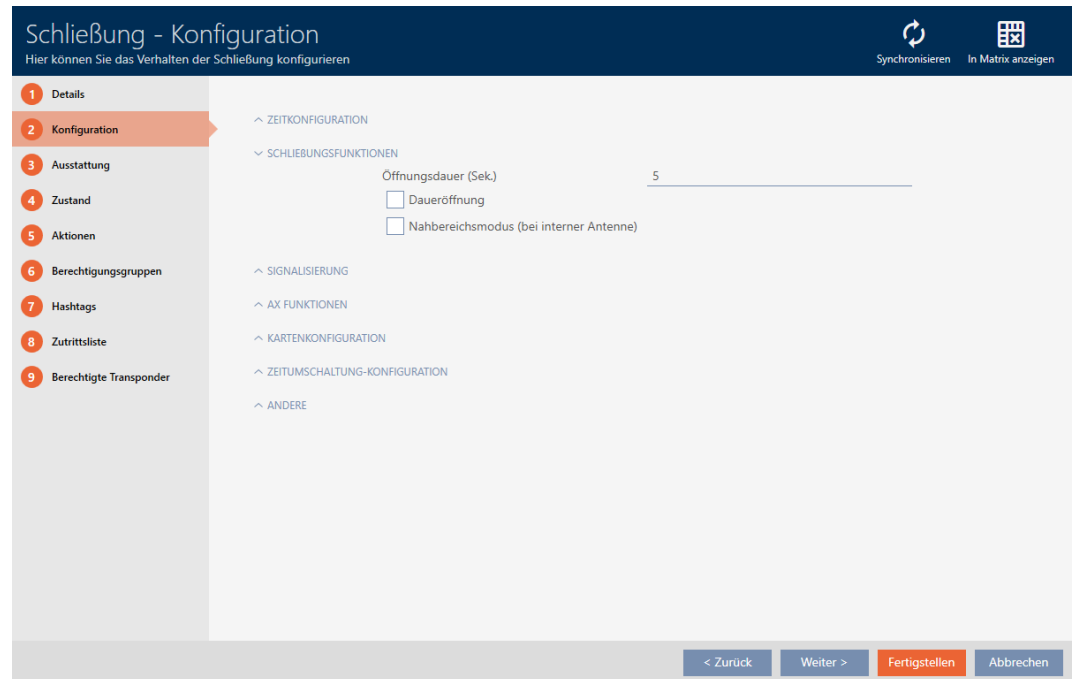
1. Click on the locking device whose read range needs to be limited.
 - ↳ The locking device window will open.

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



- ↳ Window switches to the [Configuration] tab.

3. Expand the "Lock functions" menu.



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

5. Click on the **Finish** button.

↳ The locking device window closes.

↳ Close range mode activated for this locking device.

16.13 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* [▶ 132]).

1. Click on the locking device to be muted.

↳ The locking device window will open.

Schließung - Details
Hier können Sie Details der Schließung bearbeiten

Hogwarts Synchronisieren In Matrix anzeigen Online Mode

1 Details
2 Konfiguration
3 Ausstattung
4 Zustand
5 Aktionen
6 Berechtigungsgruppen
7 Hashtags
8 Zutrittsliste
9 Berechtigte Transponder

Firmware Version 2.4.84
Letzte Synchronisierung 03.05.2024 16:13:44
Batteriestatus Ok
Sync Programmiert

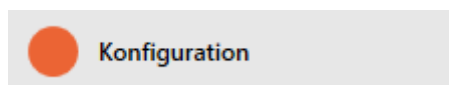
TÜRDETAILS
Tür Gryffindor dormitory
Tür-Code DC-00022
Beschreibung

GEBÄUDEDETAILS
Raumnummer
Etage
Standort Standort (Standard) + Neu
Gebäude Gebäude (Standard) + Neu

ZEITFUNKTIONEN
Zeitplan ☐ + Neu
Zeitumschaltung ☒ Zeitumschaltung 1 + Neu
Feiertagsliste ☐ + Neu

< Zurück Weiter > Fertigstellen Abbrechen

2. Click on the  Configuration tab.



↳ Window switches to the [Configuration] tab.

3. Expand the "Feedback signals" menu.

Schließung - Konfiguration
Hier können Sie das Verhalten der Schließung konfigurieren

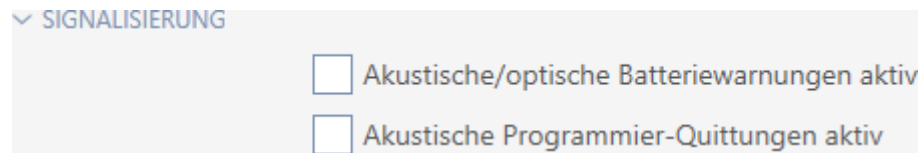
Hogwarts Synchronisieren In Matrix anzeigen

1 Details
2 Konfiguration
3 Ausstattung
4 Zustand
5 Aktionen
6 Berechtigungsgruppen
7 Hashtags
8 Zutrittsliste
9 Berechtigte Transponder

^ ZEITKONFIGURATION
^ SCHLIEßUNGSFUNKTIONEN
^ SIGNALISIERUNG
✓ Akustische/optische Batteriewarnungen aktiv
✓ Akustische Programmier-Quittungen aktiv
^ KARTENKONFIGURATION
^ ZEITUMSCHALTUNG-KONFIGURATION

< Zurück Weiter > Fertigstellen Abbrechen

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



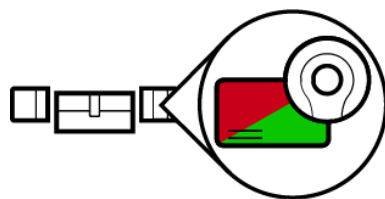
5. Click on the **Finish** button.
 - ↳ The locking device window closes.
 - ↳ Locking device will no longer signal any battery warnings or audible programming acknowledgements.

16.14 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.

Schließung - Details
Hier können Sie Details der Schließung bearbeiten

Hogwarts Synchronisieren In Matrix anzeigen

Online Mode

1 Details
2 Konfiguration
3 Ausstattung
4 Zustand
5 Aktionen
6 Berechtigungsgruppen
7 Hashtags
8 Zutrittsliste
9 Berechtigte Transponder

Firmware Version 2.4.84
Letzte Synchronisierung 03.05.2024 16:13:44
Batteriestatus Ok
Sync Programmiert

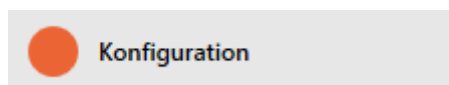
TÜRDETAILS
Tür Gryffindor dormitory
Tür-Code DC-00022
Beschreibung

~ GEBÄUDEDETAILS
Raumnummer
Etage
Standort Standort (Standard) + Neu
Gebäude Gebäude (Standard) + Neu

~ ZEITFUNKTIONEN
Zeitplan ☐ + Neu
Zeitumschaltung ☒ Zeitumschaltung 1 + Neu
Feiertagsliste ☐ + Neu

< Zurück Weiter > Fertigstellen Abbrechen

2. Click on the  Configuration tab.



↳ Window switches to the "Configuration" tab.

3. Expand the "Card configuration" menu.

Schließung - Konfiguration
Hier können Sie das Verhalten der Schließung konfigurieren

Hogwarts Synchronisieren In Matrix anzeigen

1 Details
2 Konfiguration
3 Ausstattung
4 Zustand
5 Aktionen
6 Berechtigungsgruppen
7 Hashtags
8 Zutrittsliste
9 Berechtigte Transponder

^ ZEITKONFIGURATION
^ SCHLIEBUNGSFUNKTIONEN
^ SIGNALISIERUNG
~ KARTENKONFIGURATION
 ☒ Karteninterface
^ ZEITUMSCHALTUNG-KONFIGURATION

< Zurück Weiter > Fertigstellen Abbrechen

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.

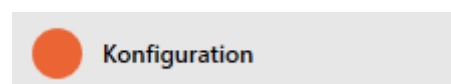
16.15 Ignoring activation and expiry date of identification media

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)* [▶ 135]).

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

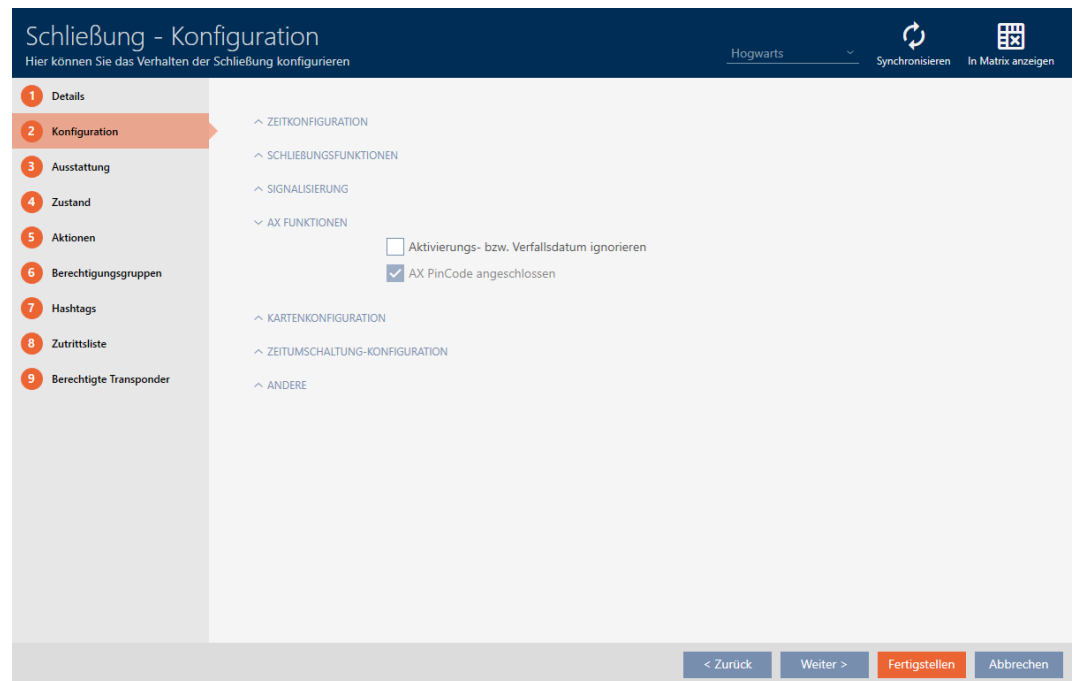
- ✓ AX-based locking device.
1. Click on the locking device to be muted.
 - ↳ The locking device window will open.

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

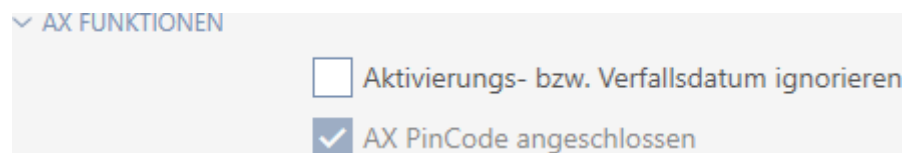


- ↳ Window switches to the [Configuration] tab.

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.

16.16 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.

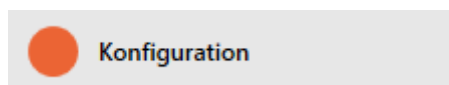
All SmartRelay settings are changed in the "Configuration" tab:

- ✓ 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.

16.16.1 Using internal and external antenna simultaneously

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

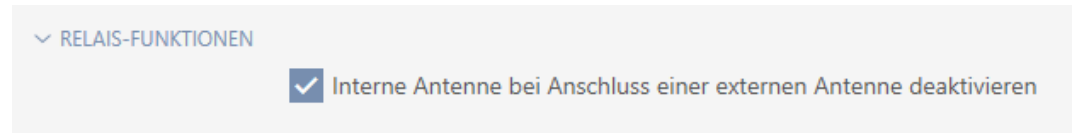


The internal antenna is normally deactivated as soon as SmartRelay detects an external antenna.

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* [▶ 317]).

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



2. Activate the ☐ Disable internal antenna when connecting an external antenna checkbox.

3. Click on the **Finish** button.

➡ The SmartRelay window closes.

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

16.16.2 Invert outputs

A relay has two states:

■ Energised (coil energised)

■ Not energised (idle state)

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

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

Changeover contact	NO contact
■ SREL ■ SREL.ADV ■ SREL.W ■ SREL.G2 ■ SREL.W.G2 ■ SREL 3 ■ SREL 3 Advanced ■ SREL AX Classic	SREL2.G2
☐ Invert SR signal ■ Identification medium activated: Relay energises, COM connected to NO ■ Identification medium not activated: Relay in idle state, COM connected to NC	☐ Invert SR signal ■ Identification medium activated: Relay energises, contacts connected ■ Identification medium not activated: Relay in idle state, contacts not connected
☒ Invert SR signal ■ Identification medium activated: Relay in idle state, COM connected to NC ■ Identification medium not activated: Relay energises, COM connected to NO	☒ Invert SR signal ■ Identification medium activated: Relay in idle state, contacts not connected ■ Identification medium not activated: Relay energises, contacts connected

✓ "Configuration" tab open (see *Changing the SmartRelay settings* [▶ 317]).

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. Activate the ☒ Invert SR signal checkbox.

3. Click on the **Finish** button.
 - ↳ The SmartRelay window closes.
 - ↳ SmartRelay outputs are inverted.

16.16.3 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](#) [▶ 317]).

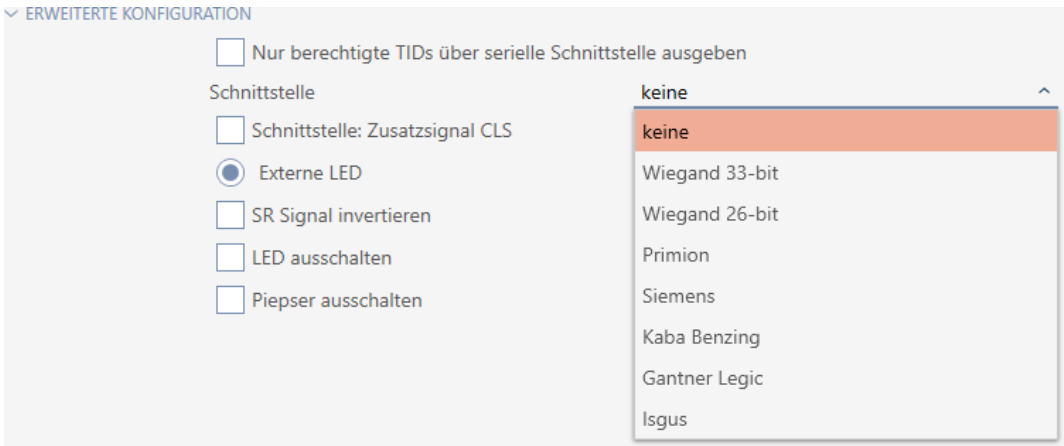
1. Open the "Extended configuration" menu if necessary.

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.

16.16.4 Changing the signalling

Different situations may require different signals.

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

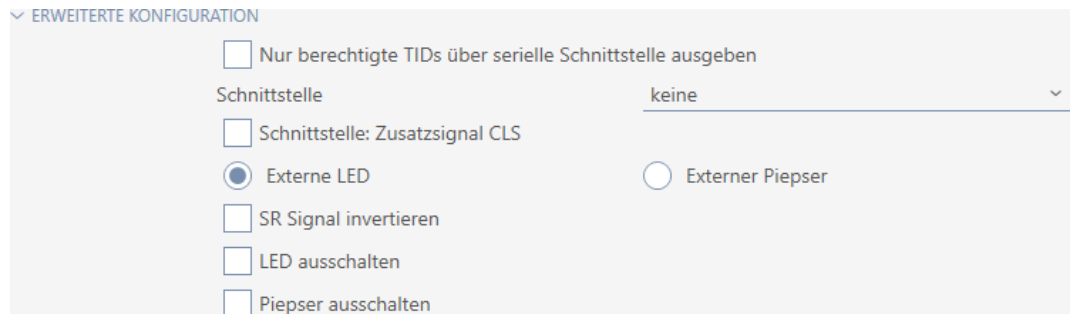
There is a connection for an external LED or an external beeper on the SREL.ADV and SREL2.G2. You can find details on connection in the manual for the SmartRelay concerned.

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.

☒ External LED	☒ External beeper
Connection permanently switches to ground during opening. The LED lights up as long as the SmartRelay is switched on.	Connection only switches when switching over. The beeper only beeps when the SmartRelay switches over. Continuous beeping would be annoying.

- ✓ "Configuration" tab open (see [Changing the SmartRelay settings](#) [[▶ 317](#)]).

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



2. Choose between the ☒ External LED and ☐ External beeper options.
3. If necessary, use the ☒ Turn off LED or ☒ Turn off beeper checkboxes to switch off the LED or the beeper on your SmartRelay (also applies to external LEDs or external beepers).
4. Click on the **Finish** button.
 - ➔ The SmartRelay window closes.
 - ➔ The SmartRelay's signalling has been changed.

16.16.5 Connect SmartRelay to network



NOTE

SmartRelay with current IP settings before changing IP settings

The AXM Plus cannot change IP settings that are already stored in the SmartRelay.

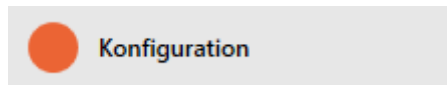
- Reset the SmartRelay before changing the IP settings (see [Reset](#) [[▶ 287](#)]).

You may also communicate via the network using network-compatible SmartRelay (e.g., SmartRelais 3 Advanced). The necessary settings for this are IP Settings.

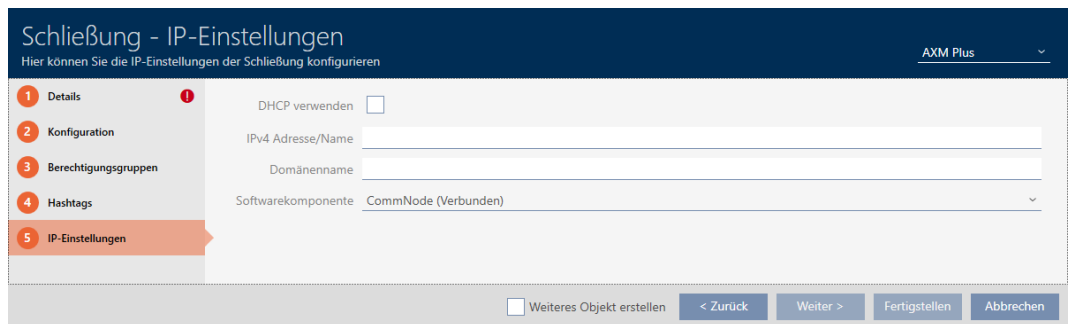
- ✓ CommNode installed (see [CommNode set up](#) [[▶ 451](#)]).
- ✓ Locking device list or matrix view open.
- ✓ The planned IP settings are known (by the IT department or network administrator): free static IPv4 address, domain name if applicable, or alternatively, operation using a DHCP server.

1. Click on the SmartRelay you want to connect to the network.
 - ➔ The locking device window will open.

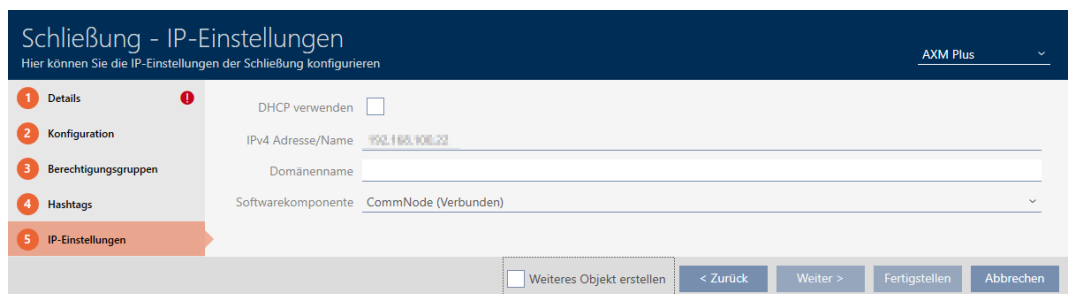
2. Click the tab  IP Settings.



→ Window switches to the "IP Settings" tab.



3. Enter the IP settings provided by the IT department (static IPv4 Address/Name and, if necessary Domain Name *or* activate the checkbox ☒ Use DHCP).



4. Click the **Finish** button.
 → The locking device window closes.
5. Click the button  **Synchronisation** and synchronise the locking device (for details see *Synchronising the locking device (including reading access list)* [▶ 417]).



NOTE

Synchronisation via USB

The IP settings you have entered have not yet been saved in the SmartRelay. Therefore, the SmartRelay is not (yet) accessible via the network.

- Synchronise new IP settings for the SmartRelay via the USB port.

→ You can then access and synchronise the SmartRelay via the network.

16.17 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.

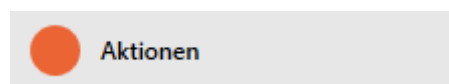
1. Click on the locking device you wish to manage.
 - ➞ The locking device window will open.

The screenshot shows the 'Schließung - Details' window. The sidebar on the left has a list of tabs: 1 Details (highlighted), 2 Konfiguration, 3 Ausstattung, 4 Zustand, 5 Aktionen, 6 Berechtigungsgruppen, 7 Hashtags, 8 Zutrittsliste, and 9 Berechtigte Transponder. The main area displays the following information:

- Firmware Version:** 2.4.84
- Letzte Synchronisierung:** 03.05.2024 16:13:44
- Batteriestatus:** Ok
- Sync:** Programmiert
- TÜRDETAILS:**
 - Tür:** Gryffindor dormitory
 - Tür-Code:** DC-00022
 - Beschreibung:** (empty text box)
- GEBÄUDEDETAILS:**
 - Raumnummer:** (empty text box)
 - Etage:** (empty text box)
 - Standort:** Standort (Standard) + Neu
 - Gebäude:** Gebäude (Standard) + Neu
- ZEITFUNKTIONEN:**
 - Zeitplan:** (checkbox) + Neu
 - Zeitmumschaltung:** (checked) Zeitmumschaltung 1 + Neu
 - Feiertagsliste:** (checkbox) + Neu

At the bottom, there are four buttons: < Zurück, Weiter >, Fertigstellen, and Abbrechen.

2. Click on the **Aktionen** tab.



- ➞ Window switches to the "Actions" tab.

Schließung - Aktionen
Hier können Sie Aktionen zur Schließung planen, einsehen und bearbeiten

Hogwarts ↕ Synchronisieren 📅 In Matrix anzeigen

1 Details
2 Konfiguration
3 Ausstattung
4 Zustand
5 **Aktionen**
6 Berechtigungsgruppen
7 Hashtags
8 Zutrittsliste
9 Berechtigte Transponder

+ Neu 🗑️ Löschen 🔍 Details

Datum	Typ	Benutzer	Beschreibung	Dokument
03.05.2024 16:13:44	Programmierung	Admin	Erfolgreich	
03.05.2024 15:59:52	Programmierung	Admin	Erfolgreich	
03.05.2024 15:58:46	Erstellt	Admin		

< Zurück Weiter > Fertigstellen Abbrechen

3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

16.17.1 Note installation, replacement or removal date

✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks* [▶ 325]).

1. Click on the **New**  button.

➞ The window for a new action will open.

Neue Aktion

Aktion

Letzter Batteriewechsel ↕

Datum Uhrzeit

18.05.2021 📅 17:49:44 ⌚

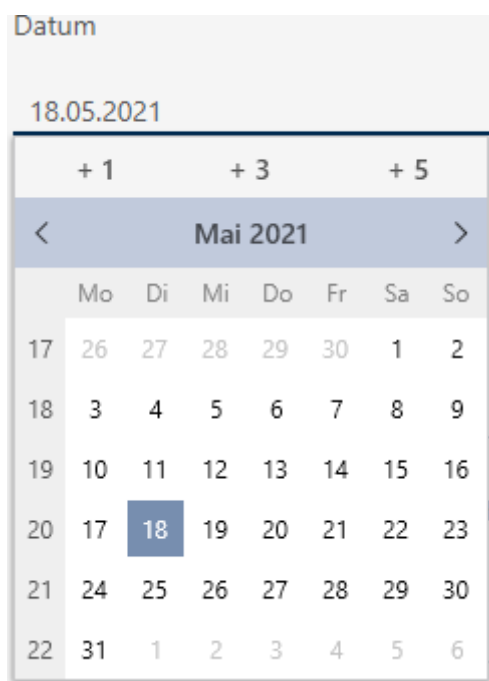
Beschreibung

☐ Dokument in Aktionsliste abspeichern

...

OK Abbrechen

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.

Neue Aktion

Aktion

Eingebaut

Datum

18.05.2021

Uhrzeit

17:49:44

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
18.05.2021 17:49:44	Eingebaut	Admin		txt
18.05.2021 17:13:31	Programmierung	Admin		
29.04.2021 17:53:00	Planmäßiger Batteriewec	Admin		
29.04.2021 16:54:38	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 18:34:59	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 15:16:18	Erstellt	Admin		

16.17.2 Planning and logging battery replacement

✓ The locking device window shows the "Actions" tab (see *Planning and tracking locking device management tasks* [▶ 325]).

1. Click on the **New** **+** 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

+ 1

+ 3

+ 5

<

Mai 2021

>

Mo	Di	Mi	Do	Fr	Sa	So
17	26	27	28	29	30	1
18	3	4	5	6	7	8
19	10	11	12	13	14	15
20	17	18	19	20	21	22
21	24	25	26	27	28	29
22	31	1	2	3	4	5

☐ Dokument in Aktionsliste abspeichern

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

18.05.2021

Uhrzeit

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.

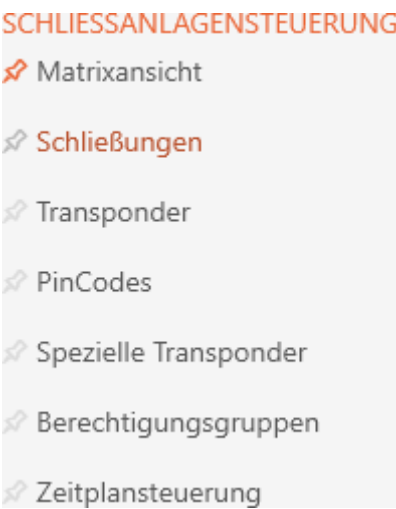
Datum	Typ	Benutzer	Beschreibung	Dokument
18.05.2021 18:43:56	Planmäßiger Batteriewec	Admin		txt
18.05.2021 17:49:44	Eingebaut	Admin		txt
18.05.2021 17:13:31	Programmierung	Admin		
29.04.2021 17:53:00	Planmäßiger Batteriewec	Admin		
29.04.2021 16:54:38	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 18:34:59	Programmierung	Admin	Aktion fehlgeschlagen	
28.04.2021 15:16:18	Erstellt	Admin		

16.18 Displaying all locking devices in a project

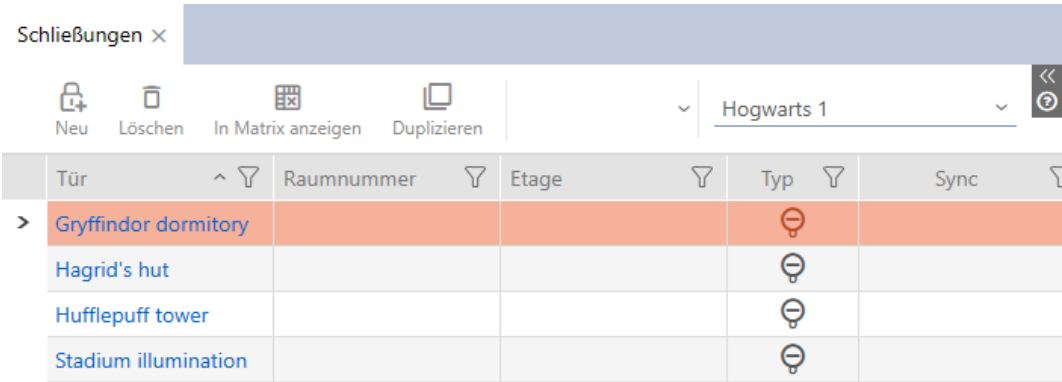
- ✓ At least one locking device created (see *Creating a locking device* [▶ 245]).
1. Click on the orange AXM icon .
 ↳ AXM bar opens.



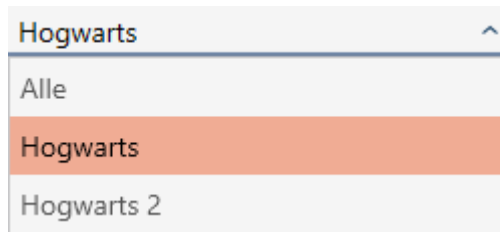
2. Select the entry **Locks** in the group | LOCKING SYSTEM CONTROL |.



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



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.

Schließungen x

Neu Löschen In Matrix anzeigen Duplizieren

Alle

	Tür	Raumnummer	Etage	Typ	Sync
>	Gryffindor dormitory			🔒	
	Hagrid's hut			🔒	
	Hufflepuff tower			🔒	
	Stadium illumination			🔒	
	Voldemort's Cave			🔒	

You can also export the locking devices displayed as a list (see [Exporting locking devices as a list](#) [▶ 332]).

16.19 Exporting locking devices as a list

All locking devices in your locking system can be exported as PDFs.

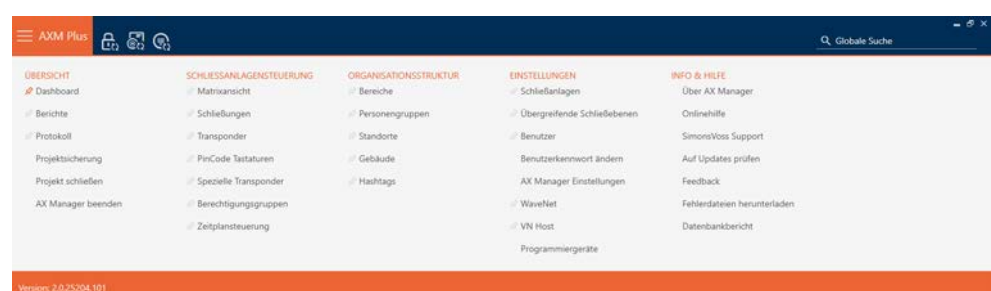
The PDF shows exactly the same locking devices in exactly the same order as in AXM Plus.

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.

Matrixansicht x		Schließungen x									
Neu		Löschen		In Matrix anzeigen		Duplizieren		Batteriewechsel		Export	
Anzeigefilter löschen										Hogwarts 1	
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* [▶ 54]).
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).

Simons Voss
technologies

Alle Schließungen für die Schließanlage 'Hogwarts 1'

Tür	Raumnummer	Etage	Typ	Sync	Status	S/N
Gryffindor dormitory			Schließzylinder	Programmiert		0084GEAD
Hagrid's hut			Schließzylinder	Programmiert		000DSP7E
Hufflepuff tower			Schließzylinder	Programmiert		000E04GX
Stadium illumination			Schließzylinder	Erstprogrammierung		

You have the option to personalise reports (see *Personalising reports and exports* [► 493]).

17. Permissions

17.1 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).

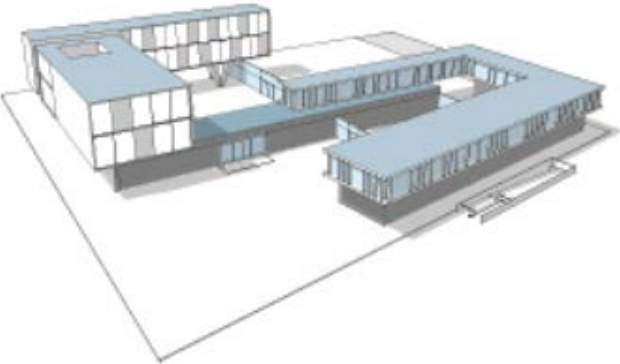


Tür	Typ
Gryffindor dormitory	⊖
Hufflepuff dormitory	⊖

Person	Typ
Weasley, Ron	⊖
Weasley, Fred	⊖
Lovegood, Luna	⊖
Granger, Hermione	⊖

			✕

- 2. Click on the same box again.
 - ➔ Authorisation is withdrawn again.



Tür	Person	Typ
Gryffindor dormitory	Weasley, Ron	⊖
Hufflepuff dormitory	Weasley, Fred	⊖
	Lovegood, Luna	⊖
	Granger, Hermine	⊖

Tür	Typ
Gryffindor dormitory	⊖
Hufflepuff dormitory	⊖

➡ 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.

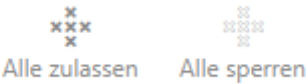
- Synchronise identification media and/or locking devices after you have changed authorisations.

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 \[▶ 483\]](#)):

- Single click of the mouse
- Double click
- Ctrl + single click

17.2 Changing many authorisations (on identification media and/or locking devices)

17.2.1 Allowing all or blocking all



Instead of individual authorisations, you can also:

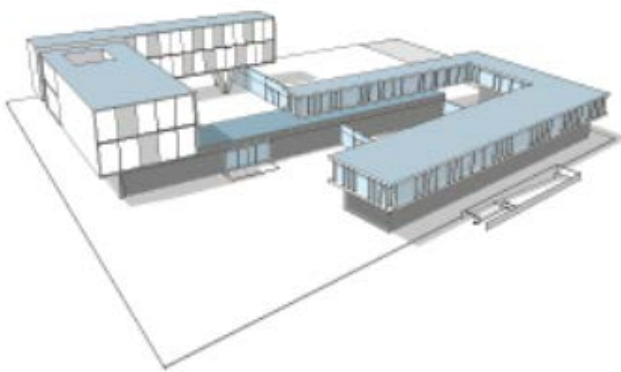
- Allow or block all currently displayed identification media on a locking device
- Allow or block identification media on all currently displayed locking devices

The **Alle zulassen**  and **Alle sperren**  functions are applied to the displayed identification media or locking devices. You can thus use filters to only allow specific identification media or locking devices.

This description refers to allowing all displayed identification media on a locking device. The following also work in the same way:

- Blocking all displayed identification media on a locking device
- Allowing identification media on all currently displayed locking devices
- Blocking an identification medium on all currently displayed locking devices

Initial situation:



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

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* [▶ 54]).

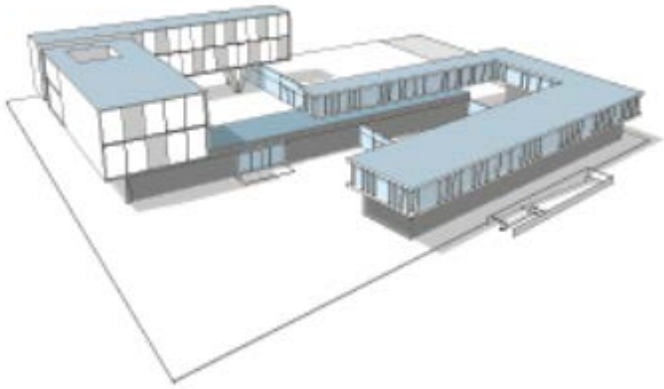


Person	Person	Person
	Weasley, Ron	Weasley, Fred
		Granger, Hermine

Typ	Typ	Typ
		

Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

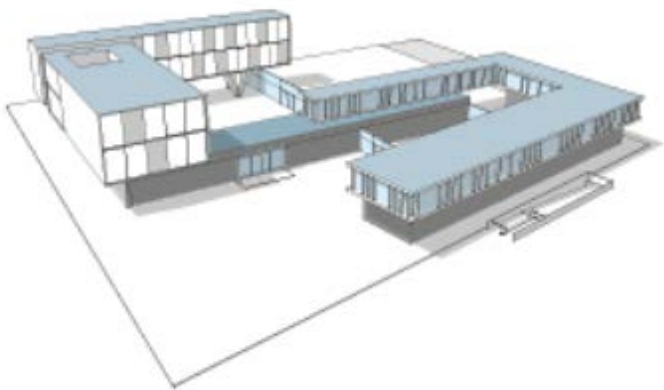
2. Select the locking device on which you wish to authorise all identification media to be displayed.



Person	Weasley, Ron	Weasley, Fred	Granger, Hermine
Typ			

Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

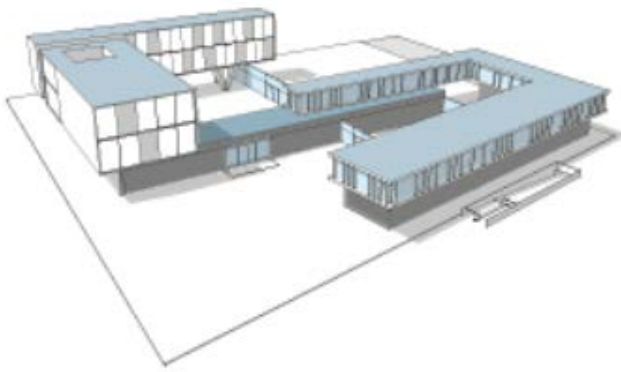
3. Click on the **Alle zulassen**  button.
- ➔ All displayed identification media are authorised for the selected locking device.



Person	Weasley, Ron	Weasley, Fred	Granger, Hermine
Typ			

Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

If you then use the button to remove the **Anzeigefilter löschen** filter again, you will find that the identification media that were filtered out were actually not permitted:



Tür	Typ
Gryffindor dormitory	
Hufflepuff dormitory	

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

17.2.2 Access levels

Access levels are an easy way for you to set up authorisations for multiple doors and identification media at the same time (see [Access levels](#) [[▶ 602](#)]).

Matrix without authorisations

AXM Plus



Matrixansicht ×





Neue Schließung



Neuer Transponder



Neue PinCode



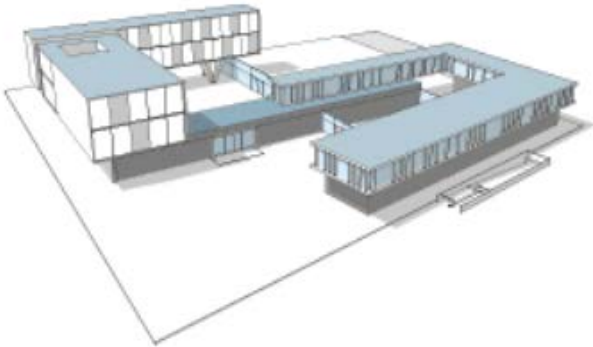
Duplizieren



Löschen



Alle zulassen





Person



Type

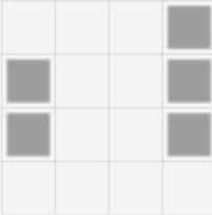


Sync

Standard Personengruppe			
	Lupin, Remus		
	Snape, Severus		
	Weasley, Ron		
	Wood, Oliver		

Tür	^	Type	Sync
Castle			
Gryffindor dormit...			
Lands			
Gryffindor tower			
Main gate			
Quidditch field			
Snape's dungeon			





Matrix with access levels

AXM Plus

Matrixansicht

Berechtigungsgruppen

Neue Schließung

Neuer Transponder

Neue PinCode

Duplizieren

Löschen

Alle zulassen

Person

Typ

Sync

Standard Personenengruppe

Lupin, Remus

Snape, Severus

Weasley, Ron

Wood, Oliver

Tür

^

Typ

Sync

Castle

Gryffindor dormit...

Lands

Gryffindor tower

Main gate

Quidditch field

Snape's dungeon

×

×

×

×

17.2.2.1 Adding locking devices and identification media to access levels

Ideally, you will have already created your access levels before creating the locking devices (see *Best practice: setting up the locking system* [▶ 37] and *Creating access levels* [▶ 60]). This allows you to set access levels directly in locking device and identification medium properties when you create locking devices and identification media:

Berechtigungsgruppen

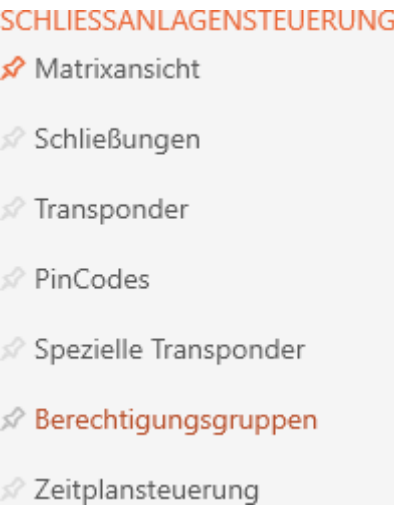
Obviously, you can also add your locking devices and identification media to the access levels at a later date:

✓ Access level created (see *Creating access levels* [▶ 60]).

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



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



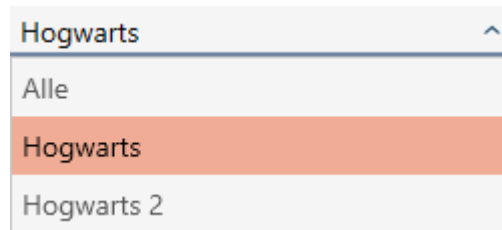
- ↳ The AXM bar will close.
- ↳ The [Access levels] tab will open.

Matrixansicht x Berechtigungsgruppen x

Neu Löschen Export Anzeigefilter löschen

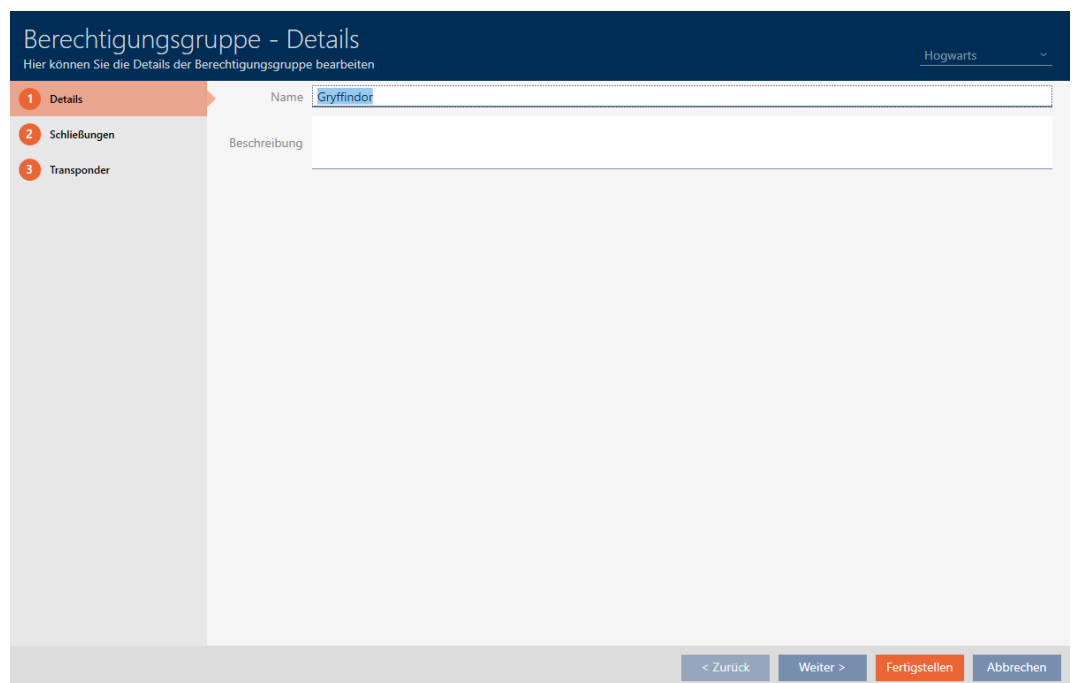
Name	Beschreibung	Anzahl Schließungen	Anzahl Transponder
> Gryffindor		0	0
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

3. Select another locking system in the drop-down menu or select the "All" drop-down entry to display the access levels in all locking systems.

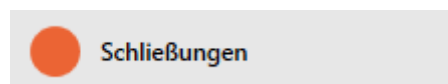


4. Click on the access level to which you wish to add locking devices and identification media.

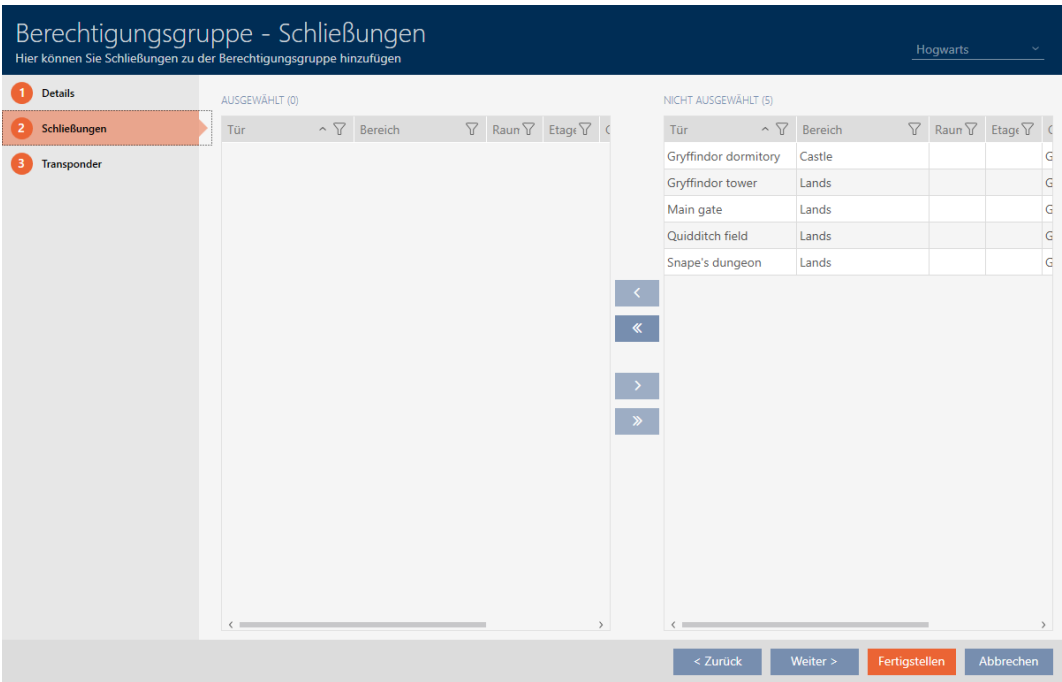
→ The access level window will open.



5. Click on the  Locks tab.



→ Window switches to the "Locks" tab.



- 6. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
- 7. Select all locking devices that you wish to add to the access level (Ctrl+click for individual devices or Shift+click for multiple devices).

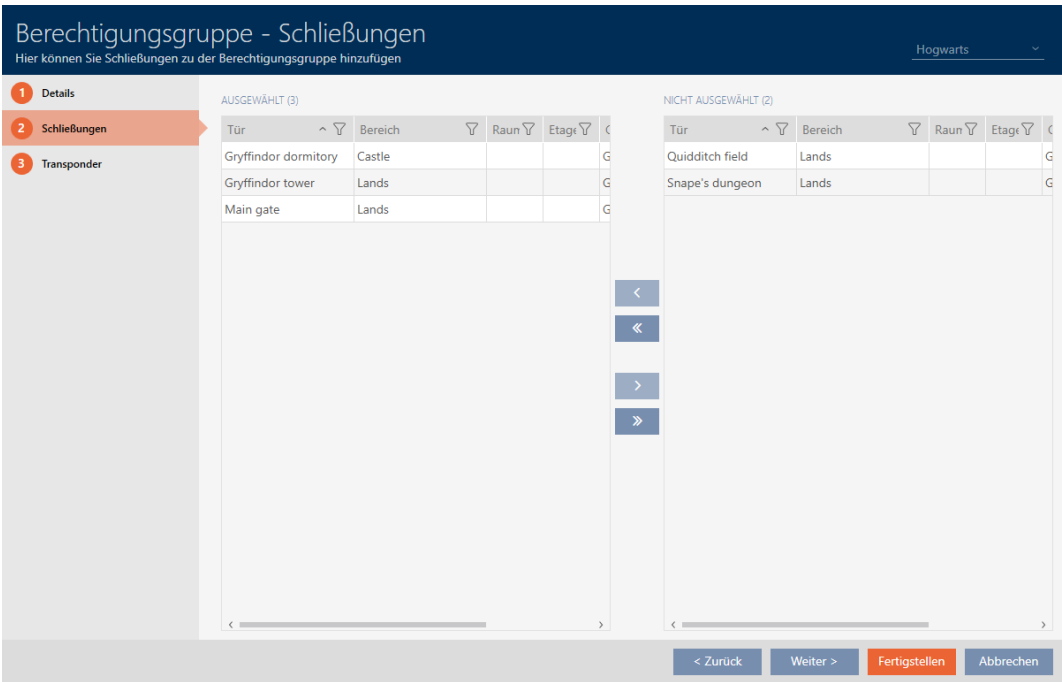


NOTE

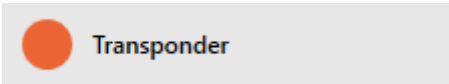
Double-clicking as an alternative to arrow keys

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

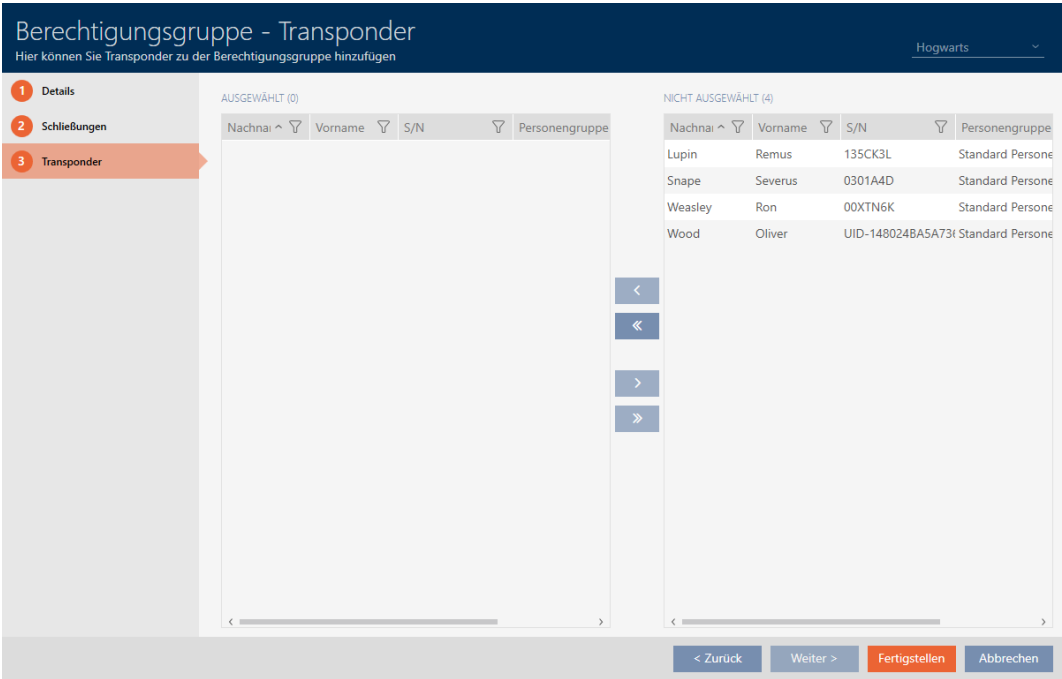
- 8. Use  to move only the selected locking devices or  to move all locking devices.
 - ➔ The selected locking device in the left-hand column is added to the access level.



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* [▶ 54]).
11. Select all identification media that you wish to add to the access level (Ctrl+click for individual media or Shift+click for multiple media).

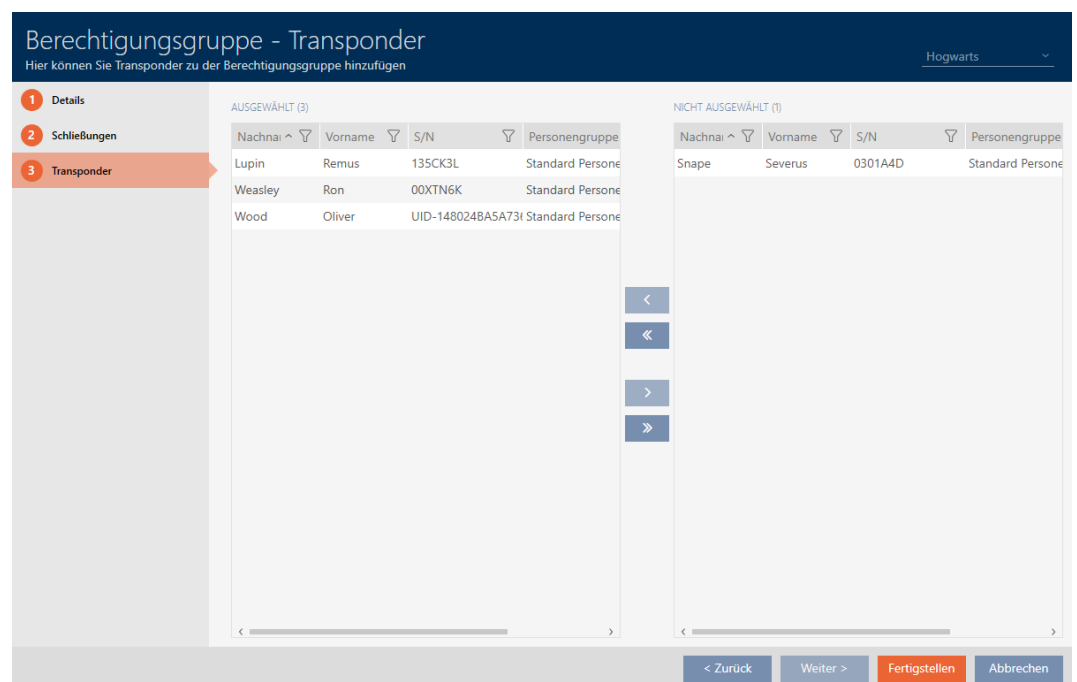


NOTE

Double-clicking as an alternative to arrow keys

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

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 access level.



13. Click on the **Finish** button.
 - ↳ The access level window closes.
 - ↳ All identification media in this access level are authorised for all locking devices in this access level.
 - ↳ Matrix view is visible again.
14. Click on the **Refresh**  button.
 - ↳ Matrix displays authorisations from your access level (identified by a small triangle next to the cross).

AXM Plus



Matrixansicht ×

Berechtigungsgruppen ×

>>

 Neue Schließung

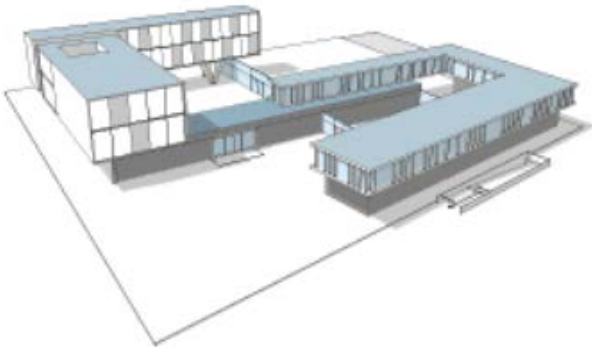
 Neuer Transponder

 Neue PinCode

 Duplizieren

 Löschen

 Alle zulassen



Person

Standard Personengruppe

Lupin, Remus

Snape, Severus

Weasley, Ron

Wood, Oliver

Typ









Sync

Tür ^

Typ

Sync

Castle

Gryffindor dormit...

Lands

Gryffindor tower

Main gate

Quidditch field

Snape's dungeon











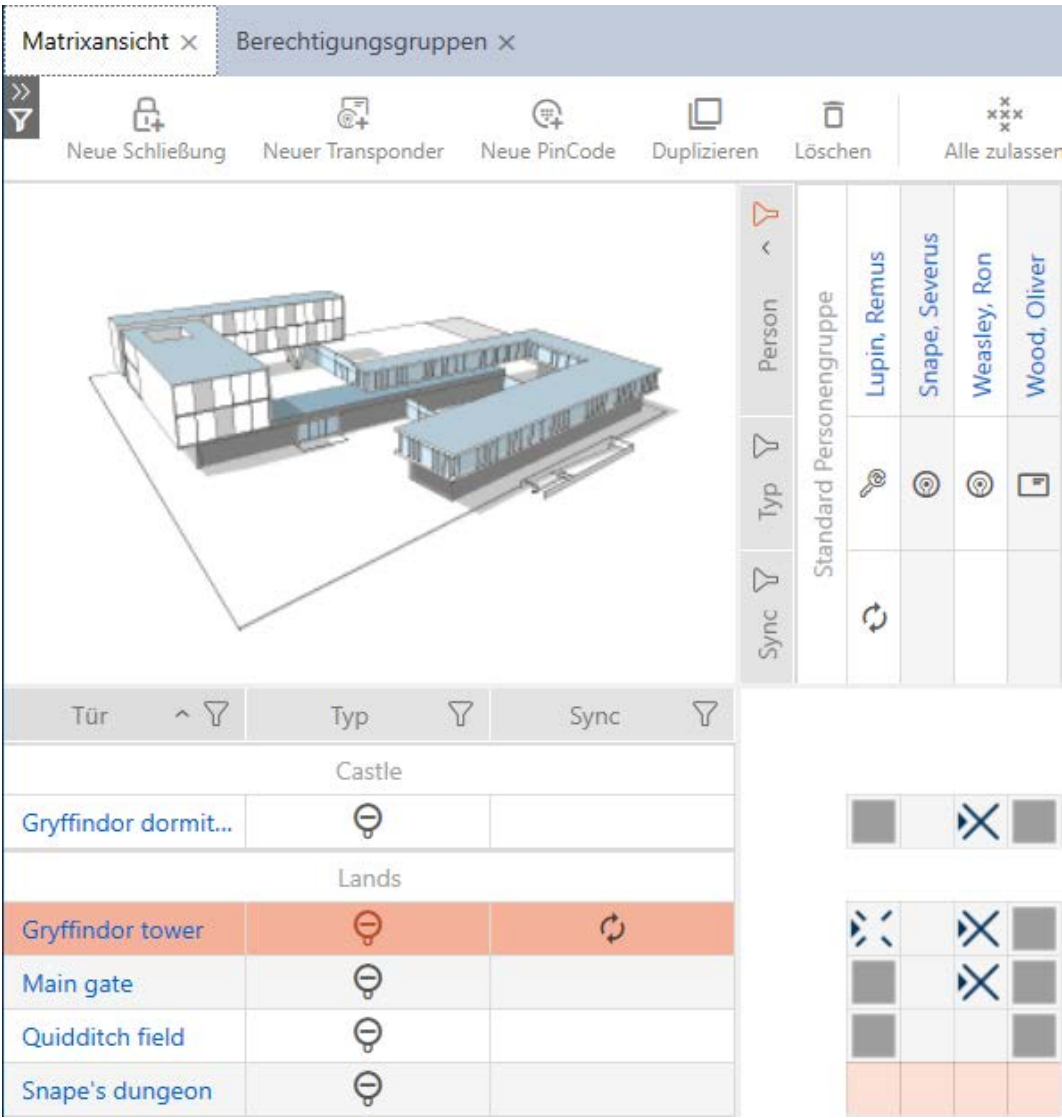






You can also overwrite individual authorisations from access levels manually. For example, it is possible to remove authorisation from an identification medium that would actually be authorised for a locking device.

Proceed as with the normal assignment of individual authorisations (see *Changing individual authorisations (cross)* [▶ 335]). In this case, it is only the cross that disappears, not the triangle:

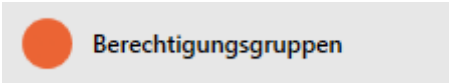


The triangle continues to indicate that there is actually an authorisation from an access level here.

17.2.2.2 Adding areas and person groups to access levels

This section explains how to add multiple locking devices to access levels quickly using areas. The process for person groups/identification media is similar.

Ideally, you will have already created your access levels before creating the locking devices (see *Best practice: setting up the locking system* [▶ 37] and *Creating access levels* [▶ 60]). This allows you to set access levels directly in locking device and identification medium properties when you create locking devices and identification media:



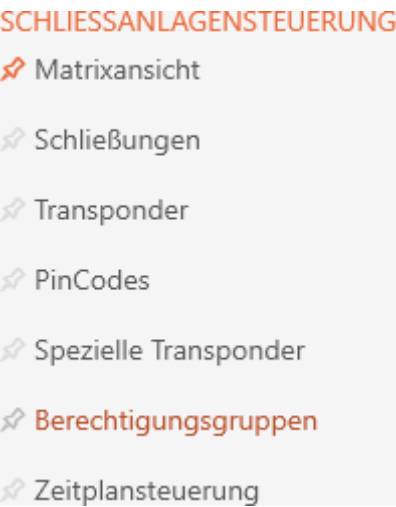
You can use areas to quickly add several locking devices to access levels:

- ✓ Access levels created (see *Creating access levels* [▶ 60]).
- ✓ At least one area created (see *Creating an area* [▶ 93]).
- ✓ At least one locking device has been assigned to the area (see *Moving locking devices to areas* [▶ 293]).

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.

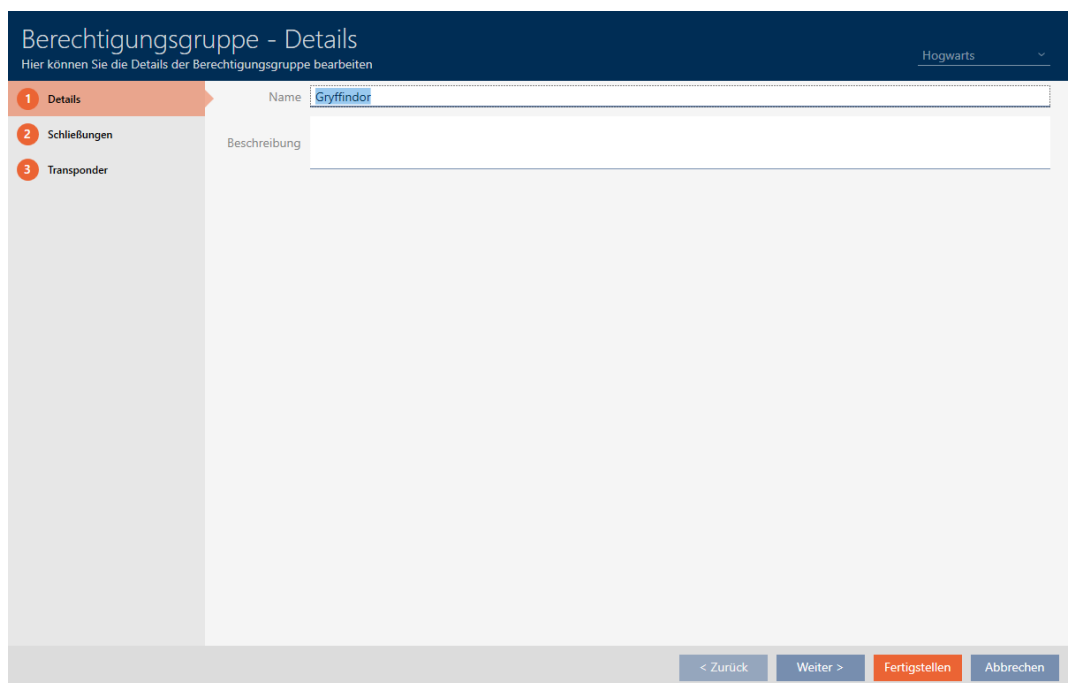
Matrixansicht ×		Berechtigungsgruppen ×			
 Neu		 Löschen		 Export	
				 Anzeigefilter löschen	
Name	^ v	Beschreibung	v	Anzahl Schließungen	v
> Gryffindor				0	0
Hufflepuff				0	0
Ravenclaw				0	0
Slytherin				0	0

3. Select another locking system in the drop-down menu or select the "All" drop-down entry to display the access levels in all locking systems.

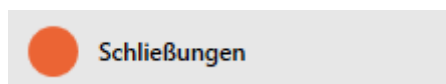


4. Click on the access level to which you wish to add locking devices and identification media.

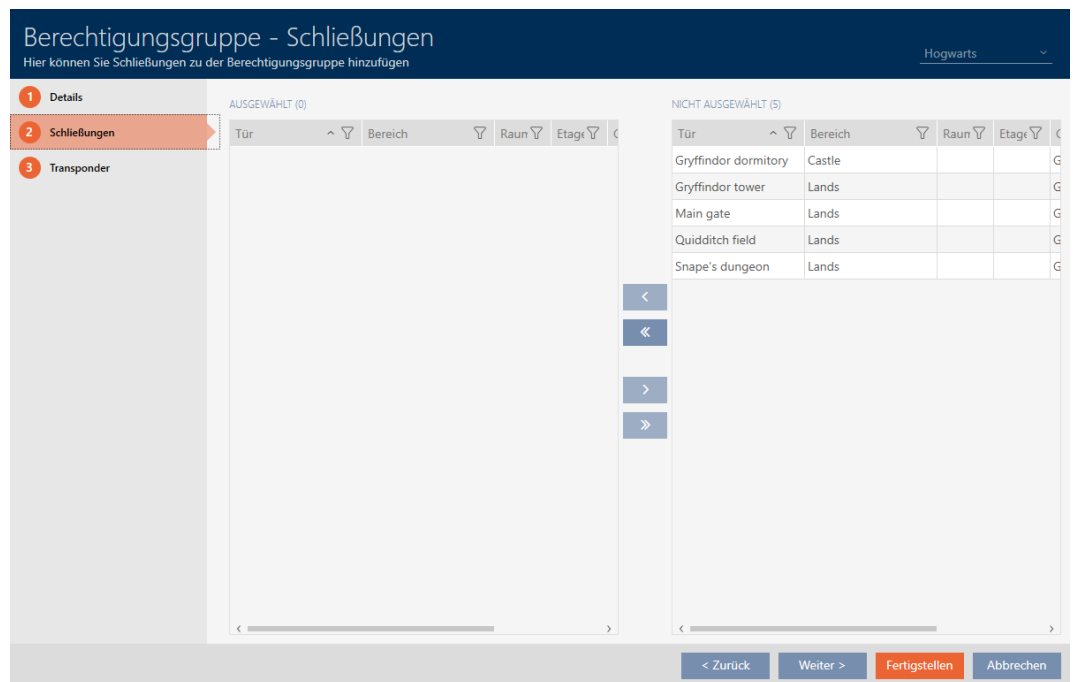
→ The access level window will open.



5. Click on the **Locks** tab.



→ Window switches to the "Locks" tab.



6. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).



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 access level (Ctrl+click for individual devices or Shift+click for multiple devices).

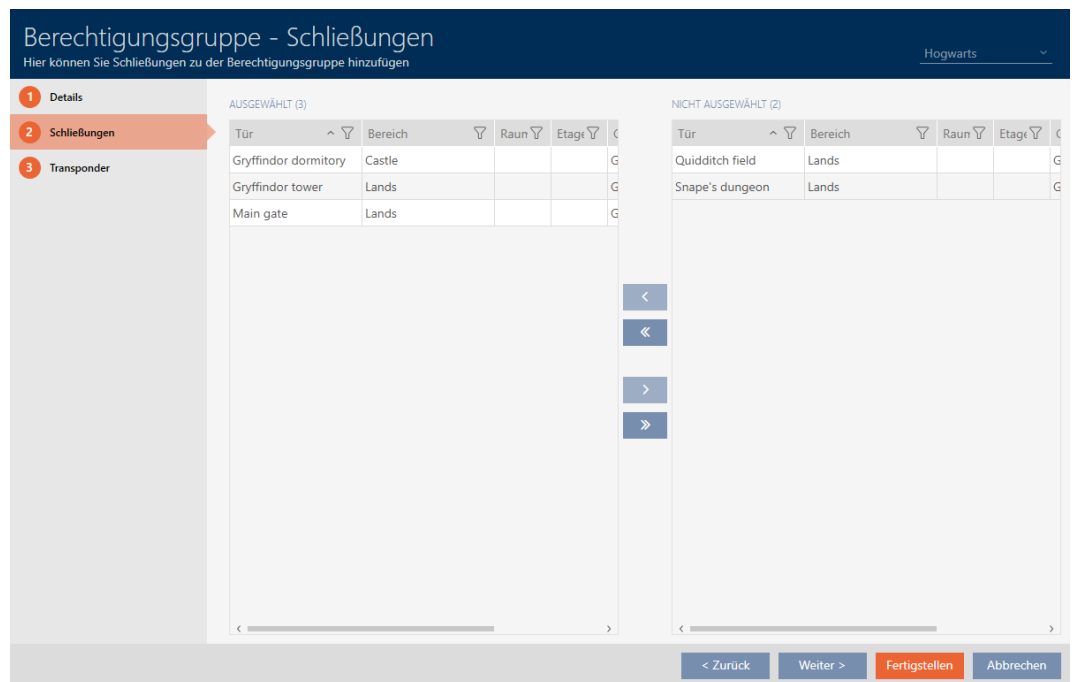


NOTE

Double-clicking as an alternative to arrow keys

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

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 access level.



9. Click on the **Finish** button.

- ↳ The access level window closes.
- ↳ All identification media in this access level are authorised for all locking devices in this access level.
- ↳ Matrix view is visible again.

10. Click on the **Refresh** button.

- ↳ Matrix displays authorisations from your access levels (identified by a small triangle next to the cross).

17.2.2.3 Show all access levels in a project

- ✓ At least one access level created (see *Creating access levels* [▶ 60]).

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.

Hogwarts
Alle
Hogwarts
Hogwarts 2

→ All access levels 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 access levels displayed as a list (see [Exporting access levels as a list](#) [▶ 354]).

17.2.2.4 Exporting access levels as a list

All access levels in your locking system can be exported as a PDF.

The PDF shows exactly the same access levels in exactly the same order as in AXM 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](#) [▶ 493]).

✓ At least one access level created (see [Creating access levels](#) [▶ 60]).

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 access levels to be exported from the drop-down menu.

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	

4. Use  to sort/filter the displayed entries if required (see [Sorting and filtering \[p. 54\]](#)).
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

17.2.3 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* [► 587].

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* [► 63].

Schedules and time groups in multiple locking systems

Schedules and time groups created in a locking system can be configured throughout the project. You will also find them available for selection in other locking systems, provided that this locking system is in the same project. Changes to schedules and time groups therefore also apply equally to all locking systems within a project.

This does not affect locking systems in other projects. You cannot see or configure schedules and time groups from other projects.

17.2.3.1 Adding locking devices to the schedule

Ideally, you should create your schedules before the locking devices (see *Best practice: setting up the locking system* [► 37]). You can then add your locking devices to the schedule while you are creating each locking device (see *Creating a locking device* [► 245]).

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

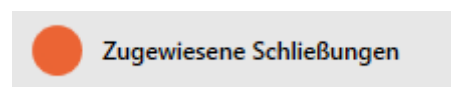
Schedule window

- 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* [▶ 363]).

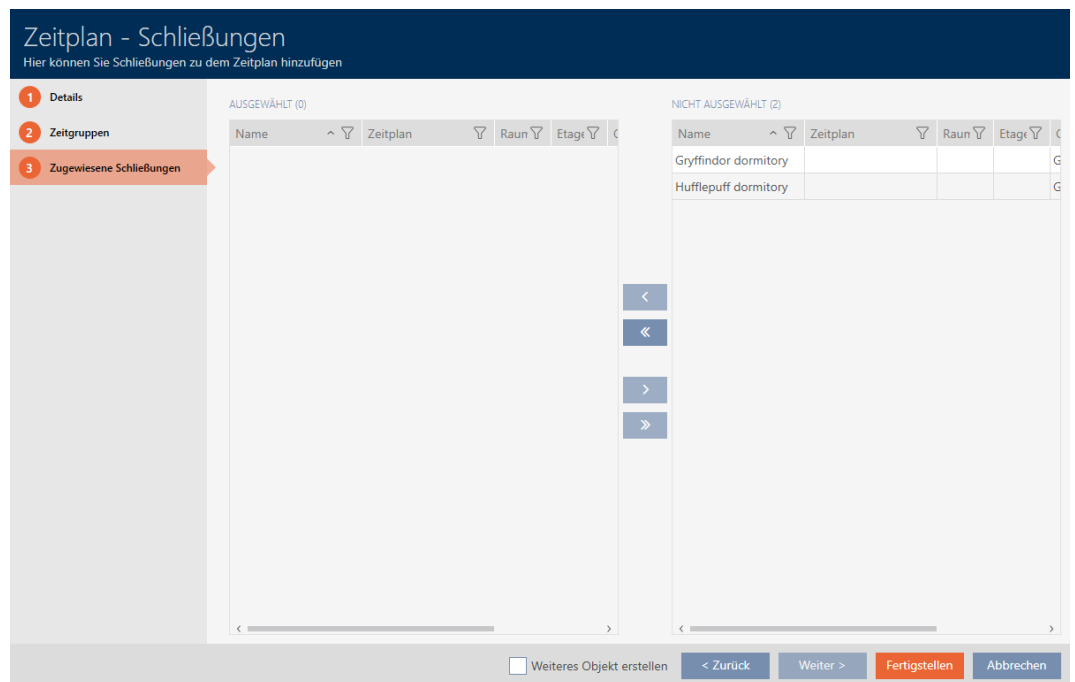
In this section, you will learn how to add locking devices to a schedule in the time schedule window (see *Limiting authorisations for locking devices to specific times (schedule)* [▶ 299] for adding using the locking device properties).

- ✓ Schedule created (see *Creating a schedule* [▶ 63]).
- ✓ Schedule window open (see *Creating a schedule* [▶ 63]).
- ✓ 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* [▶ 54]).
3. Select all locking devices that you wish to assign (Ctrl+click for individual devices or Shift+click for multiple devices).



NOTE

Double-clicking as an alternative to arrow keys

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

4. Use  to move only the selected locking devices or  to move all locking devices.



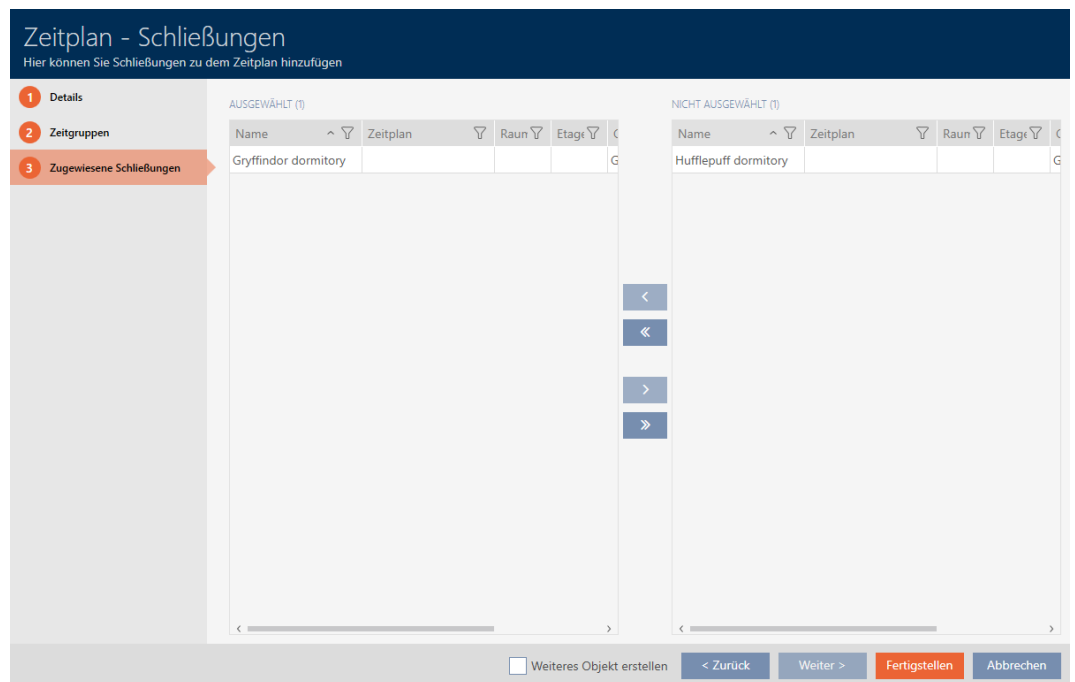
NOTE

Locking devices from other schedules

Locking devices from other schedules are also listed. They can also be moved from other schedules to the current schedule.

1. Filter/sort the displayed locking devices.
2. Check whether the selected locking devices are already being used in another schedule.

➞ The locking devices in the left-hand column are added to the schedule.



5. Click on the **Finish** button.

↳ Schedule window closes.

↳ Locking devices are now added to the schedule.

17.2.3.2 Adding identification medium to time group

Ideally, you should create your time groups before the locking devices (see *Best practice: setting up the locking system* [► 37]). You can then add your identification media to the time groups when you create them (see *Creating an identification medium* [► 98]).

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* [► 218] and *Reusing identification medium in other projects/databases* [► 224]). 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.

The screenshot shows the 'Transponder - Details' page in a web application. The left sidebar contains a list of menu items: 1 Details, 2 Personendetails, 3 Transponderkonfiguration, 4 Zusätzliche Schließanlagen, 5 Berechtigungsgruppen, 6 Hashtags, 7 Aktionen, 8 Begehungsliste, and 9 Berechtigte Türen. The main content area is titled 'TRANSPONDER DETAILS' and contains the following fields: Seriennummer (0301A4D), Transpondertyp (Transponder), Firmware Version (3.2.19), Letzte Synchronisierung (06.05.2024 15:37:12), Sync (Programmiert), Batteriestatus (Ok), Zeitgruppe (Zeitgruppe 2), and Beschreibung. The 'Zeitgruppe' dropdown menu is highlighted in yellow. At the top right, there is a dropdown menu set to 'Hogwarts', a 'Synchronisieren' button, and an 'In Matrix anzeigen' button. At the bottom right, there are four buttons: '< Zurück', 'Weiter >', 'Fertigstellen', and 'Abbrechen'.

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.

The screenshot shows the 'Transponder - Details' page in a web application, similar to the previous one but with the dropdown menu set to 'Hogwarts 2'. The 'Zeitgruppe' dropdown menu is now set to 'Zeitgruppe 1' and is highlighted in yellow. All other fields and the sidebar remain the same. The bottom right buttons are also the same: '< Zurück', 'Weiter >', 'Fertigstellen', and 'Abbrechen'.

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* [[▶ 106](#)]).

✓ Time groups created (see *Create time group* [[▶ 66](#)]).

1. Click on the PIN to be added to a time group.
↳ The window will open for the associated PIN code keypad.
2. Expand the PIN settings with the ▼ button.
3. Select the ☒ Time group checkbox.
↳ A drop-down menu will appear.

4. Select the time group that you require.

5. Click on the **Finish** button.
↳ The window for the PIN code keypad closes.
↳ PIN has been added to the time group.

17.2.3.3 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* [► 37]). You can then add your locking devices to the schedule while you are creating each locking device (see *Creating a locking device* [► 245]).

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)* [► 299] for adding individual locking devices using the locking device properties).

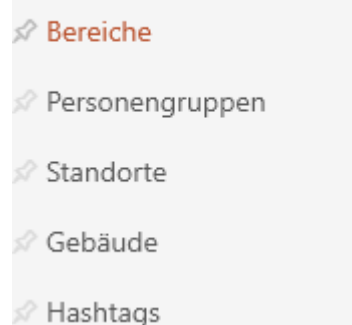
- ✓ Schedule created (see *Creating a schedule* [► 63]).
- ✓ Area created (see *Creating an area* [► 93]).
- ✓ Locking devices in the area (see *Moving locking devices to areas* [► 293]).
- ✓ Locking device equipped with .ZK option.

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



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

ORGANISATIONSSTRUKTUR



- ↳ The [Areas] tab will open.

Matrixansicht x Bereiche x

+ Neu - Löschen Anzeigefilter löschen

	Name ^ v	Zeitplan v	Beschreibung v
>	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.

Zeitplan Keiner ^

Keiner

Lessons

reibung

6. Click on the **Finish** button.
 ↳ "Area" window closes.
 ↳ Area, including locking devices, added to the schedule.

Matrixansicht ×	Bereiche ×	
+	🗑️	🗑️
Neu	Löschen	Anzeigefilter löschen
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").

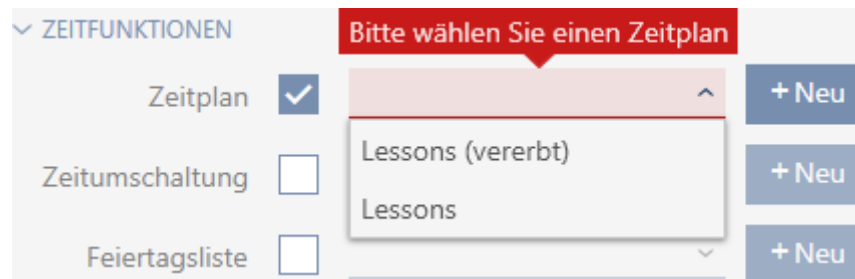
- ❑ Newly created locking devices inherit the schedule if they are assigned to an area with a schedule during their creation.
- ❑ Locking devices that have already been created but never synchronised inherit the schedule if they are assigned to an area with a schedule.
- ❑ Locking devices with inherited 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.

17.3 Meaning of the authorisation crosses in the matrix

Cross	Meaning
	Not authorised.
	Authorised in the database but not programmed yet.
	Authorised and programmed.
	Authorisation withdrawn, but authorisation removal not programmed yet.
	Authorised by an access level in the database, but not programmed yet.
	Authorised and programmed by an access level.
	Authorisation available and programmed by an access level; this authorisation has been removed manually. Authorisation removal not programmed yet.
	Authorisation by an access level available, but this authorisation was removed manually before programming.
	Authorised and programmed, but identification medium has been blocked (e.g. after theft).
	Not authorised; identification medium has been blocked (e.g. after theft). or: not possible, e.g. PIN code keypad has been assigned to another locking device.

18. Locking systems

18.1 Create locking system

With AXM Plus, you have the freedom to use multiple locking systems (see [Locking systems \[► 580\]](#) 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 \[► 35\]](#)). 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.

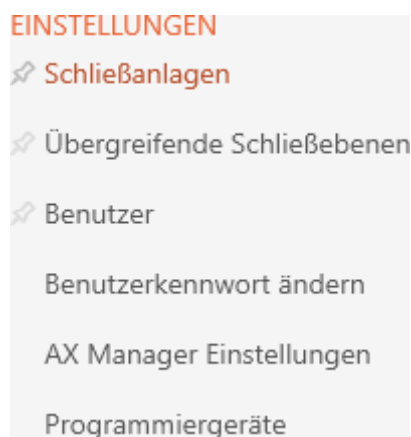
It is no longer possible to program components if the locking system password is no longer known or can no longer be recovered from a backup. The components must be removed from locks and disposed of, which takes a great deal of effort.

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).

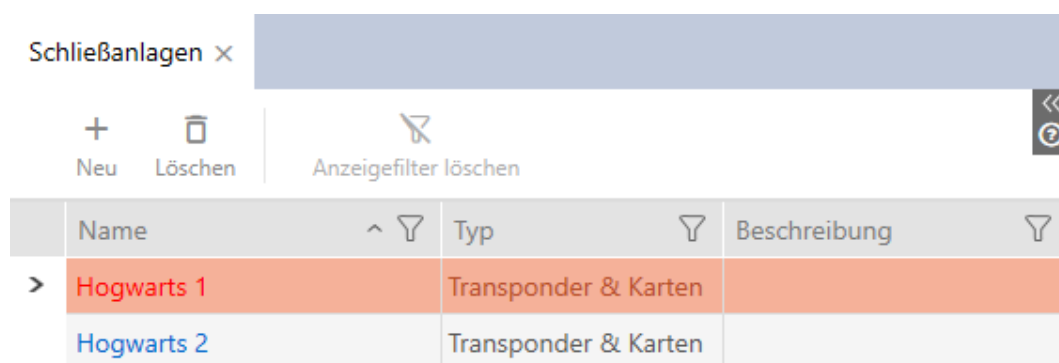
1. Click on the orange AXM icon  AXM.
→ AXM bar opens.



2. Select the **Locking systems** entry in the | SETTINGS | group.

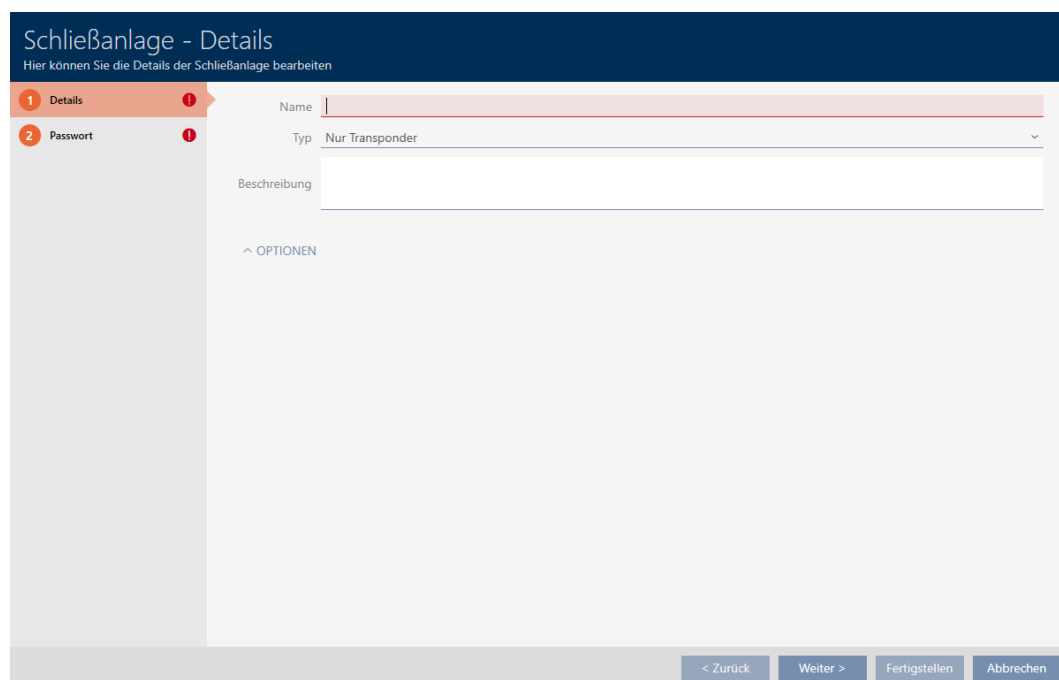


- The [Locking systems] tab with a list of all locking systems in the database will open.

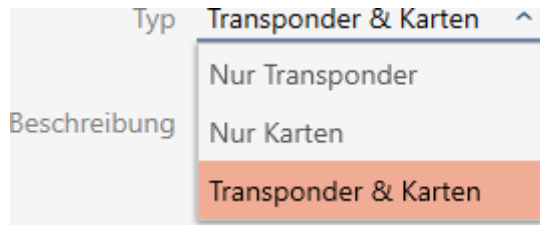


3. Click on the button **New** +.

- 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

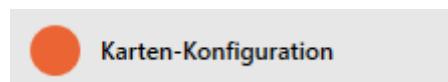
Do not activate cards as a “precaution”

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 \[► 624\]](#)). You can find the exact number in Section [Card templates \[► 628\]](#) – 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 \[► 407\]](#)).

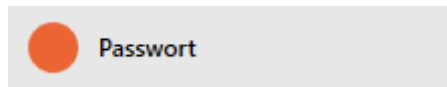
→ The **Card configurations** tab is displayed for "Cards only" or "Transponders & cards".



6. Enter a description in the *Description* field if required.
7. If you want to use a virtual network with a time budget for this locking system: expand the area "Dynamic time window" and select one of the three options.



8. Click on the tab **Password**



→ Window switches to the "Password" tab.

9. Enter the locking system password for your new locking system in the *Password* field.
10. Re-enter the locking system password in the *Confirm password* field.
- A coloured bar shows you how secure your password is.



- If your locking system is "Transponders only" and you do not want to use a common locking level, you are now finished.
11. 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.

12. Enter your card configuration here (see *Adding a card configuration* [► 372] for card configuration).

13. Click the **Finish** or **Next >** button to assign the locking system to a common locking level.



14. Click on the **Finish** button.

→ Window "Locking system" closes.

→ New locking system is listed.

Schließanlagen x

+ Neu
 Löschen
 Anzeigefilter löschen

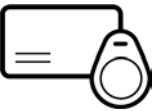
	Name ^ ∩	Typ ∩	Beschreibung ∩
	Hogwarts 1	Transponder & Karten	
	Hogwarts 2	Transponder & Karten	
>	Hogwarts 3	Transponder & Karten	

You can find information on your locking system's structure sequence here:
Best practice: setting up the locking system [► 37].

18.1.1 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.

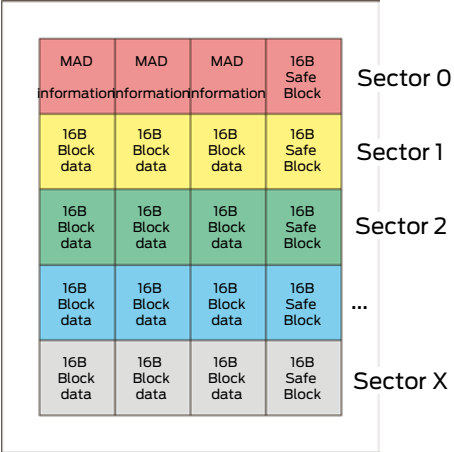
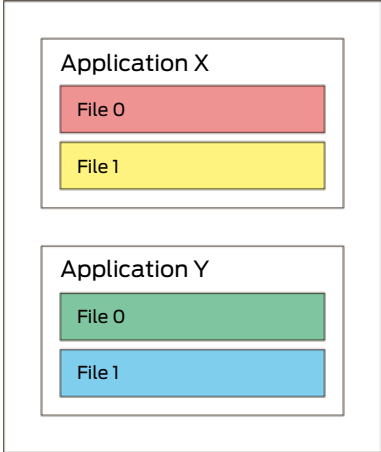
1. If you decide to have SimonsVoss check your cards, please contact one of our sales representatives in your region.
2. If you want to determine the card configuration yourself: Read through the following sections carefully.

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
▣ Easy protection ▣ Inexpensive identification media ▣ Limited performance ▣ Memory as numbers/letter sequence 	▣ Effective protection ▣ High-performance identification media ▣ Memory as a file system ▣ More flexible handling 

MIFARE Classic	MIFARE DESFire
MIFARE Classic encryption is now considered non-secure. SimonsVoss therefore recommends using MIFARE DESFire only.	

MIFARE Classic	MIFARE DESFire
❑ Data stored in sectors ❑ Addressing with sectors in sector list ❑ Sector protection using the last block in sector ❑ MIFARE Classic encryption hacked and now insecure	❑ Data saved in files ❑ Addressing with application ID ❑ File backed up by file read key ❑ Locking system data must be stored in an application file. Read access is required to the file. ❑ Encryption with AES (128 bit)
Distribution of the memory: 	Distribution of the memory: 

Determine the values to be entered in advance

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) [▶ 375]*
- *MIFARE Classic (card already used) [▶ 380]*
- *MIFARE DESFire (new/empty card) [▶ 388]*
- *MIFARE DESFire (card already in use) [▶ 394]*

You can then enter the values for the card configuration.

Entering the card configuration

- ✓ "Locking system - Card configuration" tab open (see [Create locking system \[▶ 367\]](#) or [Enable cards or transponders \[▶ 407\]](#))
- 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.

18.1.1.1 MIFARE Classic (new/empty card)

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1000L_AV	
Speicherbedarf	528 Bytes	
Schließungs-IDs	128 - 1127 im Kartenprofil	
Begehungen im Protokoll	19	
Virtuelles Netzwerk	OK	

Name: SectList
Wert: 2,3,4,5,6,7,8,9,10,11,12
Bearbeiten

Beschreibung: Sector List

Name: TransportSectorTrailer
Wert: *****
Bearbeiten

Beschreibung: Transport Settings

The following parameters are determined during configuration:

- ❑ ▼ **Card type:** MIFARE Classic or DESFire
- ❑ ▼ **Configuration:** Card template (see [Card templates \[▶ 628\]](#))

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 \[▶ 624\]](#) 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 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: $3 \times 16 \text{ bytes} = 48 \text{ bytes per sector}$.



- 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)
```

- Calculate the available storage space: Bytes per sector * available sectors (example: 48 bytes * 14 sectors = 672 bytes).
- From the drop-down menu ▼ **Card type**, select "MIFARE Classic".



- 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* [▶ 628] – example for AV: MC1000L_AV with 528 bytes).

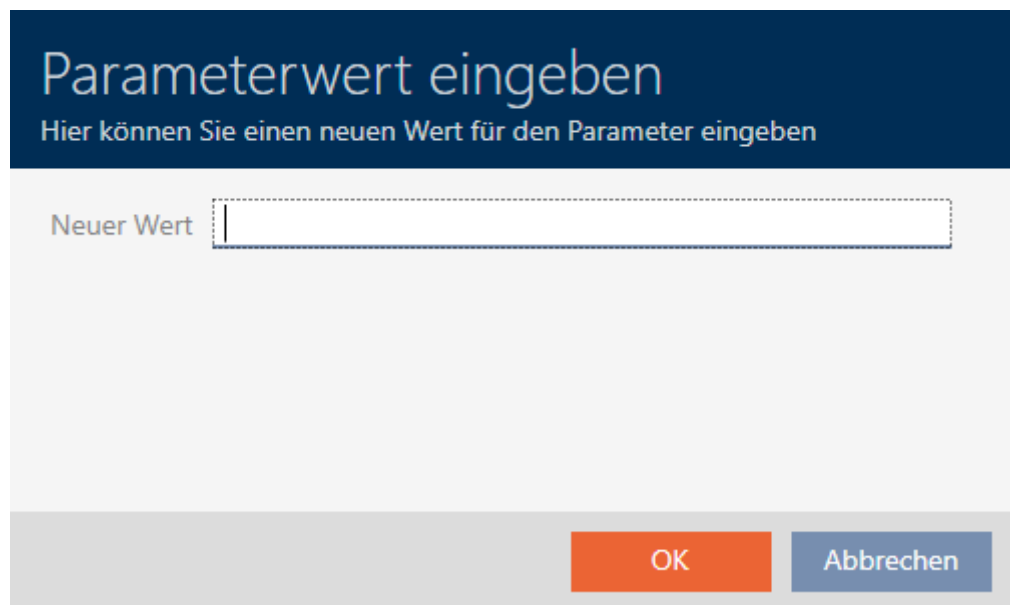
Kartentyp	Mifare Classic
Konfiguration	MC1000L_AV
Speicherbedarf	MC1000L_AV
Schließungs-IDs	MC1200L
Begehungen im Protokoll	MC2400L_AV
Virtuelles Netzwerk	MC3800L
	MC8000L_AV
	MCBasic - NO LOCKS ON CARD

7. 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* [▶ 624] 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 Classic
Konfiguration	MC1000L_AV
Speicherbedarf	528 Bytes
Schließungs-IDs	128 - 1127 im Kartenprofil
Begehungen im Protokoll	19
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.

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.



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	
Speicherbedarf	528 Bytes	
Schließungs-IDs	128 - 1127 im Kartenprofil	
Begehungen im Protokoll	19	
Virtuelles Netzwerk	OK	

Name:	SectList
Wert:	2,3,4,5,6,7,8,9,10,11,12
Bearbeiten	
Beschreibung: Sector List	

Name:	TransportSectorTrailer
Wert:	*****
Bearbeiten	
Beschreibung: Transport Settings	

13. Click on the **Finish** button.

↳ Window "Locking system" closes.

↳ Card configuration saved.

18.1.1.2 MIFARE Classic (card already used)

Kartentyp	Mifare Classic	Parameter:
Konfiguration	MC1200L	
Speicherbedarf	192 Bytes	
Schließungs-IDs	128 - 1327 im Kartenprofil	
Begehungen im Protokoll	--	
Virtuelles Netzwerk	--	

Name:	SectList
Wert:	7,8,9,10
Bearbeiten	
Beschreibung: Sector List	

Name:	TransportSectorTrailer
Wert:	*****
Bearbeiten	
Beschreibung: Transport Settings	

❑ ▼ **Card type:** MIFARE Classic or DESFire

❑ ▼ **Configuration:** Card template (see [Card templates](#) [▶ 628])

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](#) [▶ 624] 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: $3 \times 16 \text{ bytes} = 48 \text{ bytes per sector}$.



- 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)

```

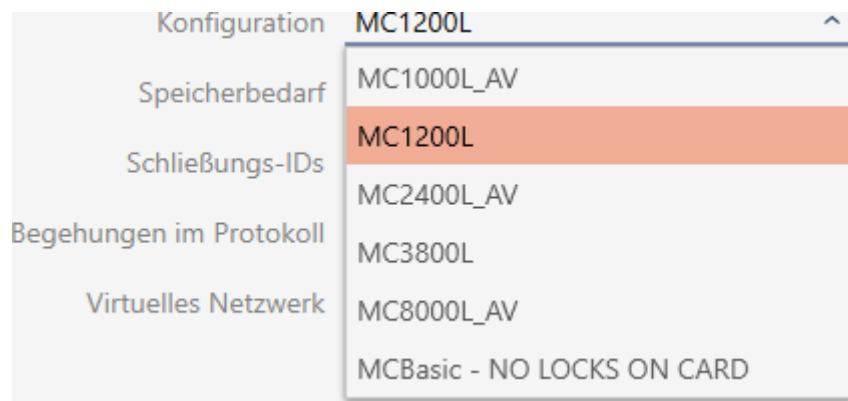
- ↳ Sectors 2, 3, 4 and 5 have already been written on (e.g. by another application) and are not available for the locking system.
- ↳ Sectors 0 and 1 cannot be used either. As a result, the sectors available are: 6, 7, 8, 9, 10, 11, 12, 13, 14 and 15 (= 10 sectors available for the locking system).

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 \[► 628\]](#) – example: MC1200L with 192 bytes).
7. Select the configuration you just specified from the ▼ Configuration drop-down menu (example: MC1200L).

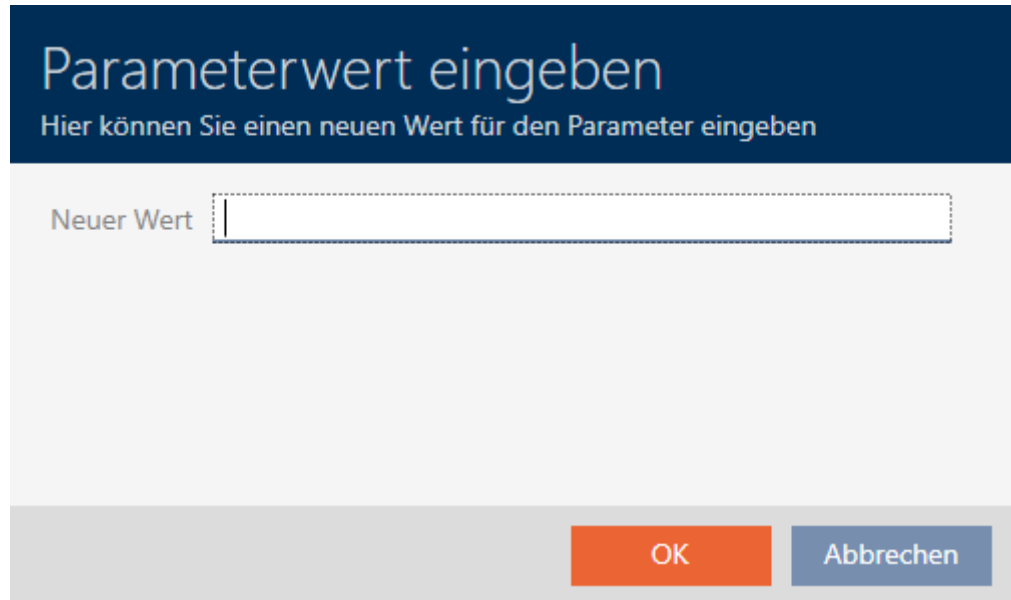


- ↳ *Memory requirements* shows the memory requirement on the card.
- ↳ *Lock IDs* shows the number of possible locking device IDs for this card (AXM Plus automatically assigns lock IDs with LID 0-127 being reserved for internal functions). See [Cards and locking device IDs \[► 624\]](#) for background 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.

9. Click the **Edit** button in the *SectList* field.
→ The "Enter parameter value" window will open.



10. 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.

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	MC1200L	
Speicherbedarf	192 Bytes	
Schließungs-IDs	128 - 1327 im Kartenprofil	
Begehungen im Protokoll	--	
Virtuelles Netzwerk	--	

Name:	SectList
Wert:	7,8,9,10
Bearbeiten	
Beschreibung: Sector List	

Name:	TransportSectorTrailer
Wert:	*****
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.

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.

18.1.1.3 MIFARE DESFire (new/empty card)

Kartentyp	Mifare Desfire	Parameter
Konfiguration	MD4000L_AV	Name: Appld Wert: 1 Bearbeiten Beschreibung: Application Id
Speicherbedarf	1600 Bytes	Name: CryptoMode Wert: AES Bearbeiten Beschreibung: Cryptography: AES or 3DES
Schließungs-IDs	128 - 4127 im Kartenprofil	Name: PiccCryptoMode Wert: AES Bearbeiten Beschreibung: Cryptography: AES or 3DES
Begehungen im Protokoll	100	Name: PiccMasterKey Wert: ***** Bearbeiten Beschreibung: Card Master Key
Virtuelles Netzwerk	OK	

❑ ▼ Card type: MIFARE Classic or DESFire

❑ ▼ Configuration: Card template (see [Card templates \[▶ 628\]](#))

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 \[▶ 624\]](#) 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".

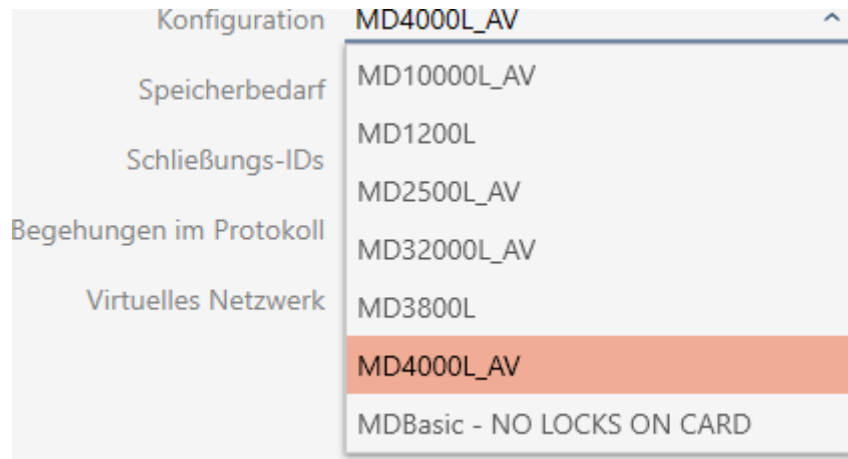


4. Consider whether you need a physical access list or a virtual network for your cards.

↳ 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](#) [▶ 628] – 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 \[► 624\]](#) 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:	Appld
Wert:	1
	Bearbeiten
Beschreibung: Application Id	

→ The "Enter parameter value" window will open.

Parameterwert eingeben

Hier können Sie einen neuen Wert für den Parameter eingeben

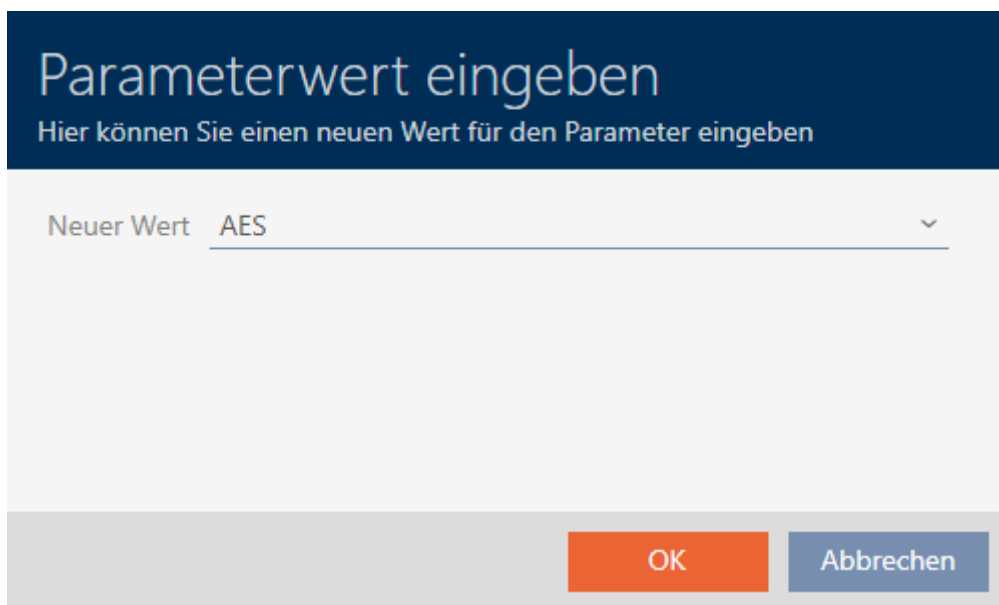
Neuer Wert

OK **Abbrechen**

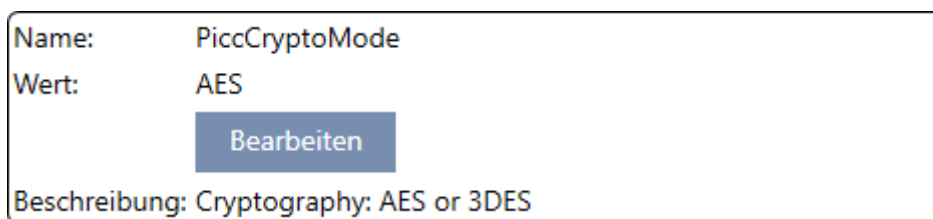
8. Enter an app ID in the *New value* field (decimal system) or leave the value at the default value 1.
9. Click on the **OK** button.
- "Enter parameter value" window closes.
10. Click the **Edit** button next to CryptoMode for the parameters.

Name:	CryptoMode
Wert:	AES
	Bearbeiten
Beschreibung: Cryptography: AES or 3DES	

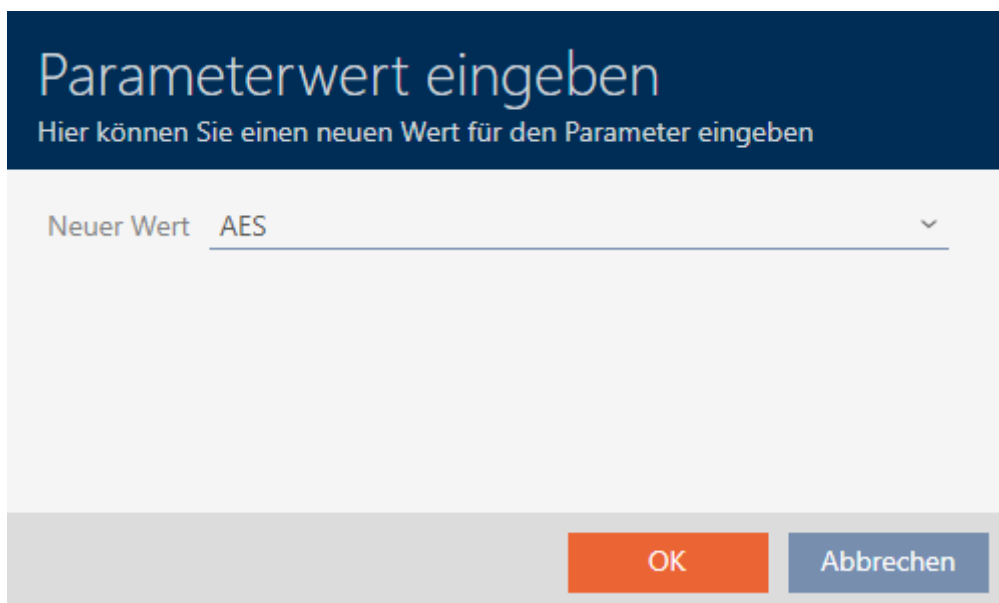
→ The "Enter parameter value" window will open.



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	Mifare Desfire	Parameter
Konfiguration	MD4000L_AV	
Speicherbedarf	1600 Bytes	
Schließungs-IDs	128 - 4127 im Kartenprofil	
Begehungen im Protokoll	100	
Virtuelles Netzwerk	OK	

Name	Appld
Wert	1
Bearbeiten	
Beschreibung Application Id	
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	

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.

18.1.1.4 MIFARE DESFire (card already in use)

Kartentyp	Mifare Desfire	Parameter
Konfiguration	MD4000L_AV	
Speicherbedarf	1600 Bytes	
Schließungs-IDs	128 - 4127 im Kartenprofil	
Begehungen im Protokoll	100	
Virtuelles Netzwerk	OK	
		Name Appld Wert 2 Bearbeiten Beschreibung Application Id
		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 \[▶ 628\]](#))

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 \[▶ 624\]](#) 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:

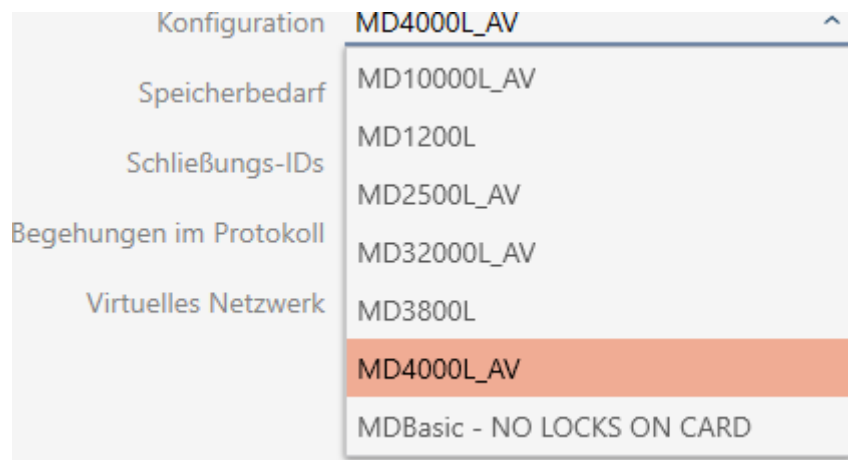
- 2 AES keys
- Master key changeable
- Master key required for:
 - ~ directory list access: no
 - ~ create/delete files: yes
- Configuration changeable
- Master key required for changing a key
- Key versions:
 - ~ Master key: 0
 - ~ Key #1: 0
- File ID 0x00: Standard data, 192 bytes
 - ~ Communication: 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 \[► 628\]](#) – 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 \[► 624\]](#) 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.

8. Click the **Edit** button next to the app ID for the parameters.

Name:	AppId
Wert:	1
	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

OK **Abbrechen**

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.

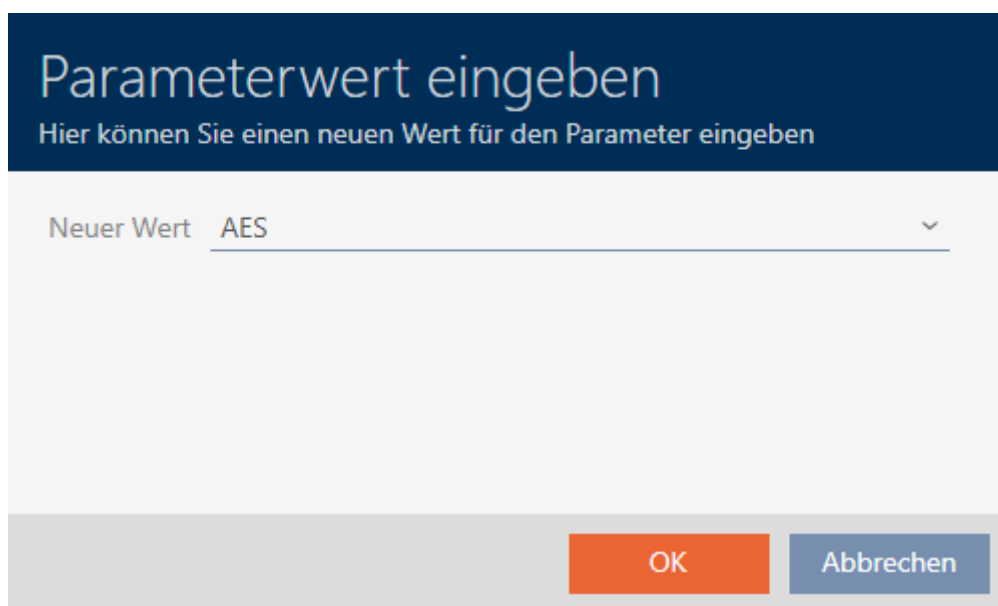
10. Click on the **OK** button.

↳ "Enter parameter value" window closes.

11. Click the **Edit** button next to CryptoMode for the parameters.

Name:	CryptoMode
Wert:	AES
	Bearbeiten
Beschreibung: Cryptography: AES or 3DES	

→ The "Enter parameter value" window will open.

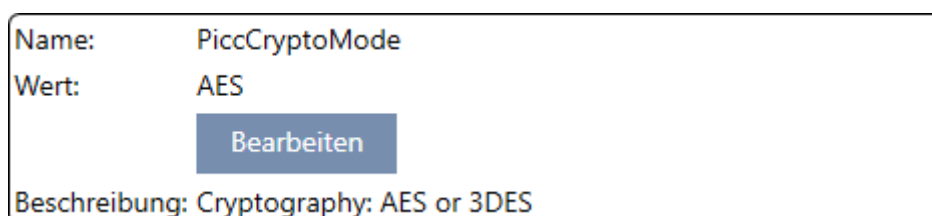


12. Select the AES entry from the ▼ **New value** drop-down menu.

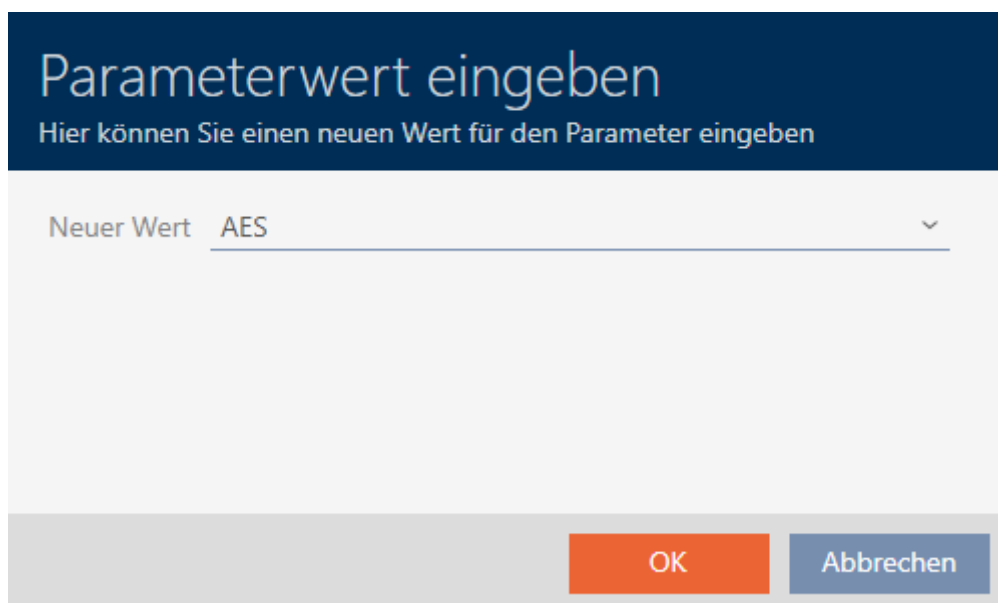
13. Click on the **OK** button.

→ "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:	*****
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	Mifare Desfire	Parameter								
Konfiguration	MD4000L_AV	<table border="1"> <tr> <td>Name</td> <td>Appld</td> </tr> <tr> <td>Wert</td> <td>2</td> </tr> <tr> <td colspan="2" style="text-align: center;"> Bearbeiten </td> </tr> <tr> <td colspan="2">Beschreibung Application Id</td> </tr> </table>	Name	Appld	Wert	2	Bearbeiten		Beschreibung Application Id	
Name	Appld									
Wert	2									
Bearbeiten										
Beschreibung Application Id										
Speicherbedarf	1600 Bytes	<table border="1"> <tr> <td>Name</td> <td>CryptoMode</td> </tr> <tr> <td>Wert</td> <td>AES</td> </tr> <tr> <td colspan="2" style="text-align: center;"> Bearbeiten </td> </tr> <tr> <td colspan="2">Beschreibung Cryptography: AES or 3DES</td> </tr> </table>	Name	CryptoMode	Wert	AES	Bearbeiten		Beschreibung Cryptography: AES or 3DES	
Name	CryptoMode									
Wert	AES									
Bearbeiten										
Beschreibung Cryptography: AES or 3DES										
Schließungs-IDs	128 - 4127 im Kartenprofil	<table border="1"> <tr> <td>Name</td> <td>PiccCryptoMode</td> </tr> <tr> <td>Wert</td> <td>AES</td> </tr> <tr> <td colspan="2" style="text-align: center;"> Bearbeiten </td> </tr> <tr> <td colspan="2">Beschreibung Cryptography: AES or 3DES</td> </tr> </table>	Name	PiccCryptoMode	Wert	AES	Bearbeiten		Beschreibung Cryptography: AES or 3DES	
Name	PiccCryptoMode									
Wert	AES									
Bearbeiten										
Beschreibung Cryptography: AES or 3DES										
Begehungen im Protokoll	100	<table border="1"> <tr> <td>Name</td> <td>PiccMasterKey</td> </tr> <tr> <td>Wert</td> <td>*****</td> </tr> <tr> <td colspan="2" style="text-align: center;"> Bearbeiten </td> </tr> <tr> <td colspan="2">Beschreibung Card Master Key</td> </tr> </table>	Name	PiccMasterKey	Wert	*****	Bearbeiten		Beschreibung Card Master Key	
Name	PiccMasterKey									
Wert	*****									
Bearbeiten										
Beschreibung Card Master Key										
Virtuelles Netzwerk	OK									

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).

18.2 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.



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.

+

Neu

✕

Anzeigefilter löschen

	Name	^	⌵	Typ	⌵	Beschreibung
>	Hogwarts			Nur Transponder		

3. Click on the locking system whose password you wish to change.

→ The locking system window will open.

Schließanlage - Details

Hier können Sie die Details der Schließanlage bearbeiten

1 Details

2 Passwort

3 Karten-Konfiguration

Name

Hogwarts

Typ

Transponder & Karten

Beschreibung

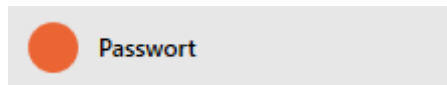
< Zurück

Weiter >

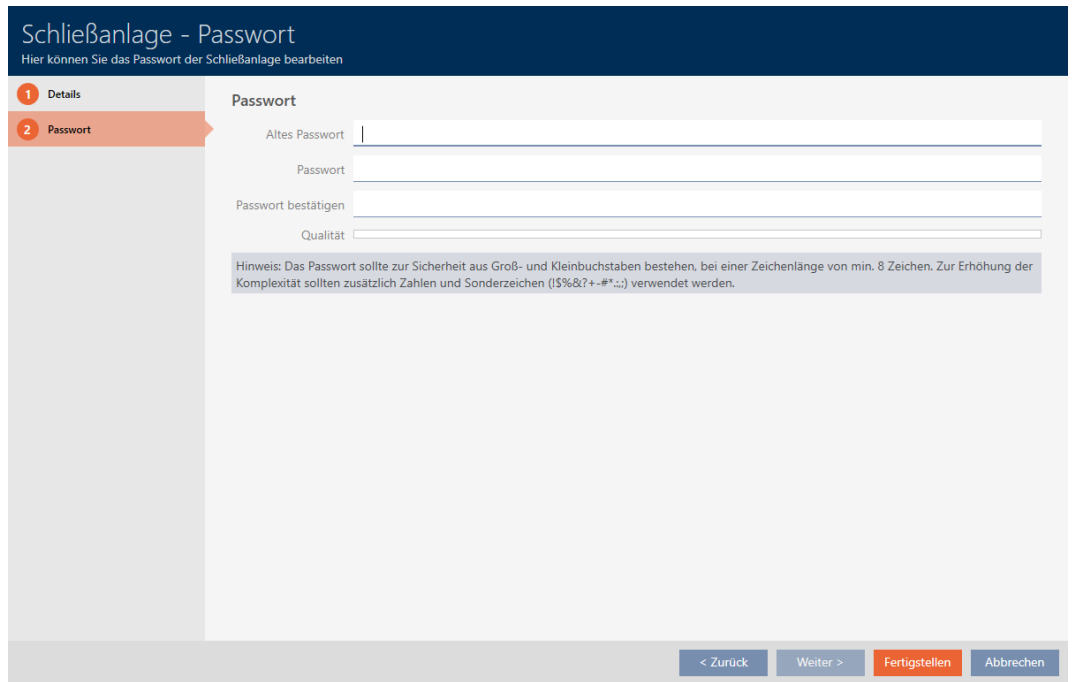
Fertigstellen

Abbrechen

4. Click on the  Password tab.



→ Window switches to the "Password" tab.

A screenshot of a web form titled "Schließanlage - Passwort". The subtitle reads "Hier können Sie das Passwort der Schließanlage bearbeiten". On the left, there is a sidebar with two tabs: "1 Details" and "2 Passwort", with "2 Passwort" being the active tab. The main content area is titled "Passwort" and contains four input fields: "Altes Passwort", "Passwort", "Passwort bestätigen", and "Qualität". Below these fields is a grey box with a warning message in German: "Hinweis: Das Passwort sollte zur Sicherheit aus Groß- und Kleinbuchstaben bestehen, bei einer Zeichenlänge von min. 8 Zeichen. Zur Erhöhung der Komplexität sollten zusätzlich Zahlen und Sonderzeichen (!\$%&?+-#*~) verwendet werden." At the bottom right, there are four buttons: "< Zurück", "Weiter >", "Fertigstellen" (highlighted in orange), and "Abbrechen".

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.

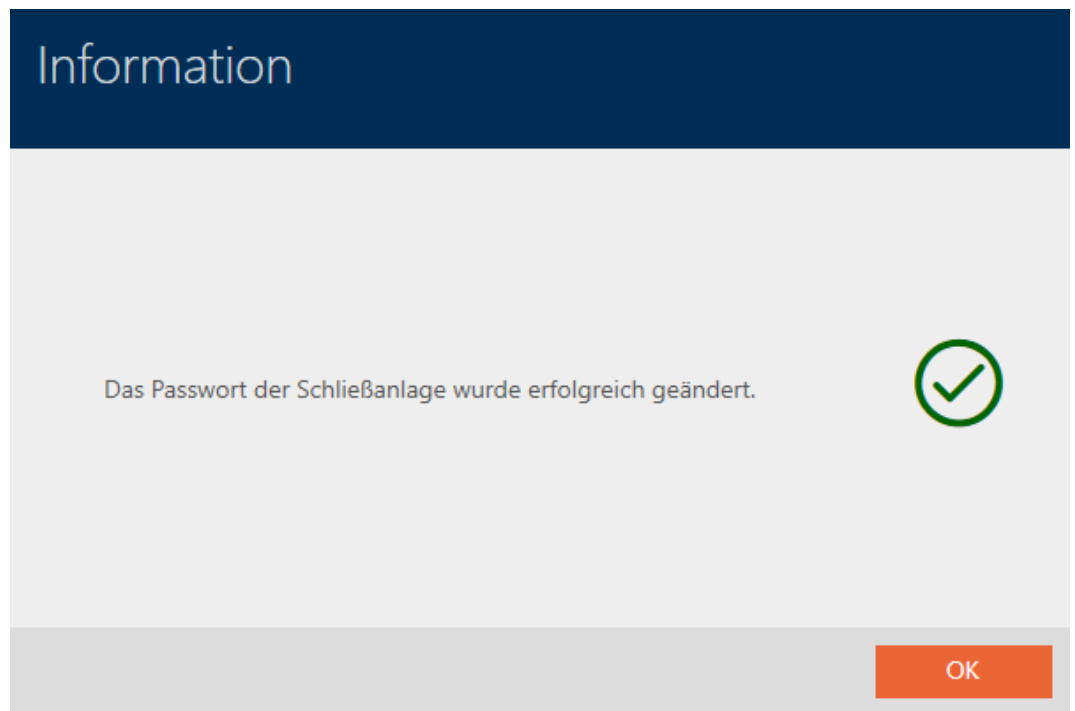
→ A coloured bar shows you how secure your password is.



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.



18.3 Replacing the locking system

Working with multiple locking systems can offer you advantages (see *Locking systems* [▶ 580]). 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

Neue Schließung

Neuer Transponder

Neue PinCode

Duplizieren

Löschen

Hogwarts

Hogwarts

Hogwarts 2

Person

Typ

Sync

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

[Locks]

Schließungen

Neu

Löschen

In Matrix anzeigen

Duplizieren

Batteriewechsel

Export

Hogwarts

Alle

Hogwarts

Hogwarts 2

Tür

Raumnummer

Etage

Typ

Status

Gryffindor dormitory

Gryffindor tower

Main gate

Quidditch field

Snape's dungeon

[Transponder]

Transponder

Neu

Löschen

In Matrix anzeigen

Duplizieren

Ausgabe

DSGVO-Daten

Export

Anzeigefilter löschen

Importieren

Hogwarts

Alle

Hogwarts

Hogwarts 2

Nachname

Vorname

S/N

Typ

Sync

Status

Zeitgruppe

Lupin

Remus

135CK3L

Snape

Severus

0301A4D

Weasley

Ron

00XTN6K

Wood

Oliver

UID-148024BA5A7369

[PinCode Keypads]

PinCodes ×

Neu Löschen In Matrix anzeigen Export Anzeigefilter löschen

Hogwarts
Alle
Hogwarts
Hogwarts 2

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

[Access levels]

Berechtigungsgruppen ×

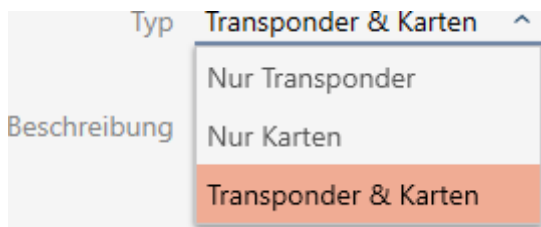
Neu Löschen Export Anzeigefilter löschen

Hogwarts
Alle
Hogwarts
Hogwarts 2

Name	Beschreibung	Anzahl Schließungen	Anzahl Karten
Gryffindor		3	3
Hufflepuff		0	0
Ravenclaw		0	0
Slytherin		0	0

18.4 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](#) [▶ 624]).

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.

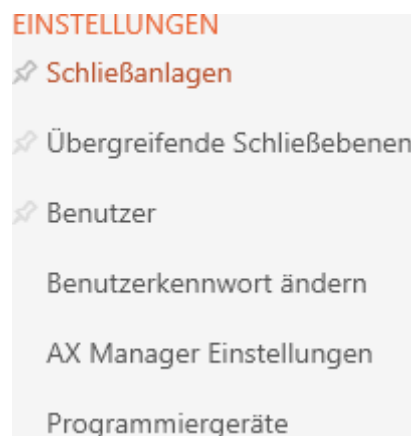
✓ At least one locking system created (see *Create locking system* [▶ 367]).

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.

Schließanlagen ×

+ Neu Löschen Anzeigefilter löschen

	Name ^	Typ	Beschreibung
	Hogwarts 1	Transponder & Karten	
	Hogwarts 2	Transponder & Karten	
>	Hogwarts 3	Nur Transponder	

3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

4. Select the locking system in which you'd like to enable cards or transponders.

↳ The Locking system window will open.

Schließanlage - Details

Hier können Sie die Details der Schließanlage bearbeiten

1 Details
2 Passwort

Name

Typ

Beschreibung

^ OPTIONEN

< Zurück
Weiter >
Fertigstellen
Abbrechen

5. Select your locking system type from the ▼ **Type** drop-down menu:
"Transponders only", "Transponders & cards" or "Cards only".

Typ **Transponder & Karten** ^

Beschreibung

Nur Transponder
Nur Karten
Transponder & Karten

→ A warning window will open.

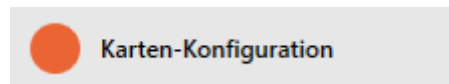
Warnung

Die Änderung des Schließagentyps kann umfangreichen Programmierbedarf erzeugen!

Wollen Sie den Typ wirklich ändern?

Ja
Nein

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 \[▶ 372\]](#)).
8. Click on the **Finish** button.
 - ↳ Window "Locking system" closes.
- ↳ Locking system is now listed with a new locking system type.

Schließanlagen x

+	🗑️	🗑️	⏮
Neu	Löschen	Anzeigefilter löschen	?

	Name	Typ	Beschreibung
	Hogwarts 1	Transponder & Karten	
	Hogwarts 2	Transponder & Karten	
>	Hogwarts 3	Transponder & Karten	

18.5 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:

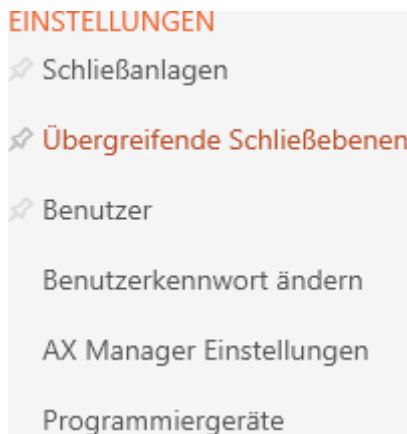
1. Create a common locking level and assign it to this locking system (see [Creating a common locking level \[▶ 410\]](#)).
2. Create a transponder in one of the assigned locking systems (see [Creating transponders for common locking level \[▶ 413\]](#)).
 - ↳ Transponders are automatically created in 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 \[▶ 414\]](#)).

18.5.1 Creating a common locking level

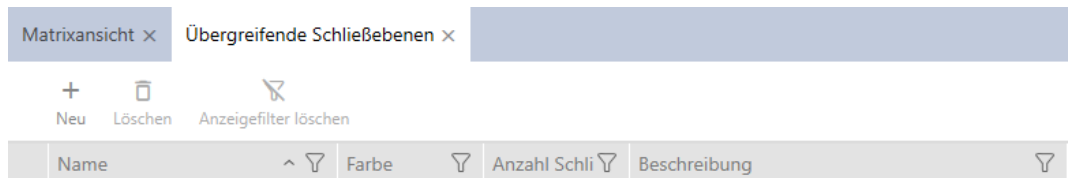
1. Click the orange AXM button .
 - ↳ AXM bar opens.



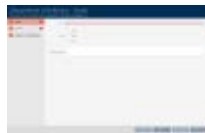
2. Select the **Service Sets** entry in the | SETTINGS | group.



- 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 \[► 54\]](#)).
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* [▶ 413]).

18.5.2 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* [▶ 407]).

- ✓ List with transponders or matrix screen opened.
 - ✓ Common locking level created and locking system assigned (see *Creating a common locking level* [▶ 410]).
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* [▶ 99]).
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 \[► 414\]](#)).

After synchronisation is complete, the *Transponder* and *Colour* fields are displayed in the common locking level colour (example: red).



18.5.3 Authorising a transponder with common locking level

- ✓ Matrix screen open.
 - ✓ Common locking level created (see [Creating a common locking level \[► 410\]](#)).
 - ✓ Transponder created in common locking level (see [Creating transponders for common locking level \[► 413\]](#)).
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.

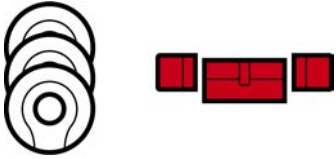
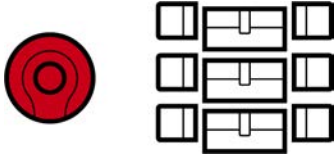
4. Assign all desired authorisations there as well.



5. Synchronise the locking devices and transponders as usual (see *Synchronising the locking device (including reading access list)* [▶ 417] and *Synchronising an identification medium* [▶ 427]).
- ↳ Thanks to the common locking level, the same transponder can operate locking devices from different locking systems.

19. Synchronisation: Comparison between locking plan and reality

Since the G2 protocol was introduced, it is up to you whether you synchronise the locking device or the identification medium for a new authorisation, for example.

Synchronising a locking device	Synchronising an identification medium
<i>Synchronising the locking device (including reading access list) [► 417]</i>	<i>Synchronise a card/transponder (including importing physical access list) [► 428]</i>
Useful if many identification media have been authorised for a locking device. In this case, only one locking device needs to be synchronised instead of many identification media. 	Useful if an identification medium has been authorised for many locking devices. In this case, only one identification medium needs to be synchronised instead of many locking devices. 

Other factors are important to consider when making this decision, such as:

- Available programming devices
- Locking device or identification medium on site
- Access list or physical access list imported

Synchronisation from the matrix

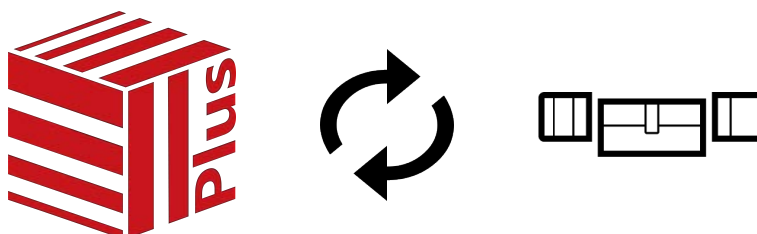
You can display the synchronisation requirement in the matrix. If you click directly on the  icon, you immediately start synchronising the entry concerned.

Initial or regular synchronisation

An initial synchronisation (symbol: ) differs from other synchronisations (symbol: ) due to the larger amount of data. In the case of AX locking devices, it is therefore preferable to use a SmartStick AX or a SmartCD.MP, especially for initial synchronisations.



19.1 Synchronising the locking device (including reading access list)



Synchronisation is bidirectional:

- Reading of data stored in the locking device (e.g. battery level)
- Writing of new data onto the locking device (e.g. authorisations)

Access lists can be imported separately ([Read audit trail](#)  button).
Access lists can also be easily read during synchronisation as an option
(see [Reading access list/physical access list during synchronisation](#)
[\[▶ 487\]](#)).

The imported data can then be displayed (see [Display locking device equipment and status](#) [\[▶ 420\]](#) or [Displaying and exporting a locking device's access list](#) [\[▶ 422\]](#), 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.



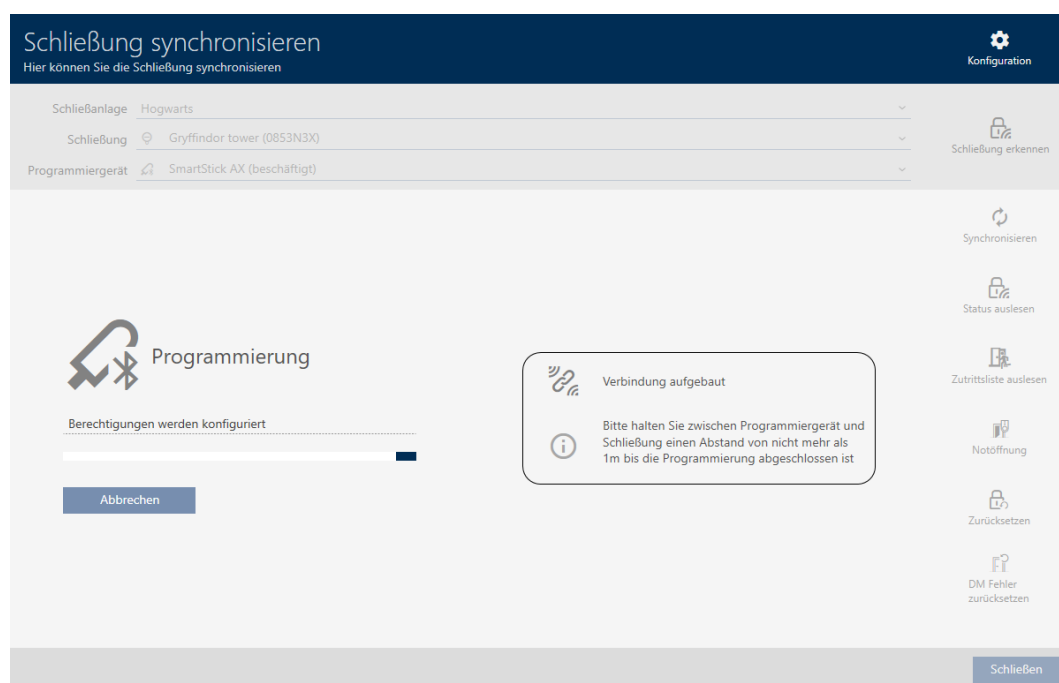
NOTE

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.

- Click on the **Synchronisation** button .
 Locking device is being synchronised.



- 
- Locking device is synchronised.

Information

Die Schließung wurde erfolgreich synchronisiert



OK



NOTE

First transponder activation rejected after initial programming of AX products

If a transponder is the first identification medium to be activated after initial programming, the transponder can be rejected once and synchronised with the locking device in the background. Transponders will then function as normal.

19.1.1 Display locking device equipment and status



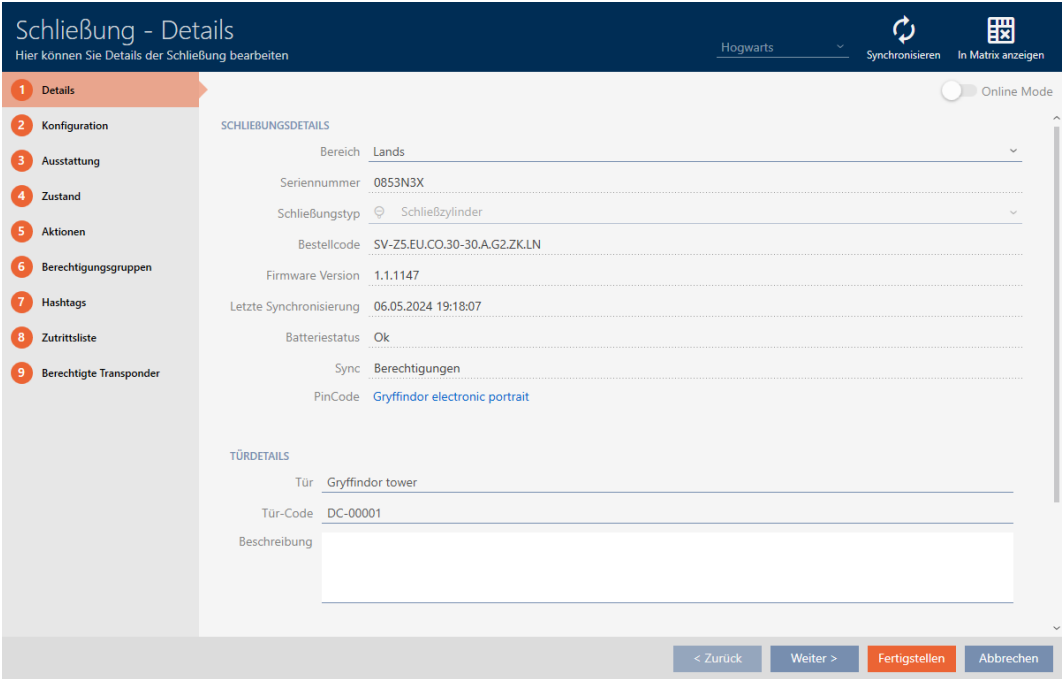
NOTE

Displayed status corresponds to the last synchronisation

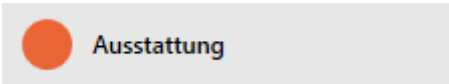
AXM Plus displays the status stored in the database at this point.

✓ Locking device synchronised at least once.

1. Click on the locking device whose status you wish to display.
→ The locking device window will open.



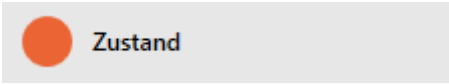
2. Click on the  **Ausstattung** tab.



- ↳ 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 / Zeitzonesteuerung
LN	LockNode

3. Click on the  **Zustand** tab.



- ↳ Window switches to the "State" tab.
- ↳ The imported status is displayed (only for locking devices that have already been synchronised).

Zustand beim letzten Auslesen: 18.05.2021 17:11:28

Batteriezustand: Ok

☐ Notfreischaltung ☐ Deaktiviert ☐ Eingekuppelt

19.1.2 Displaying and exporting a locking device's access list

The ZK function (access control) enables your locking devices to log which identification media have been activated (see *Have accesses logged by locking device (access list)* [▶ 307]). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation* [▶ 487] and *Synchronising the locking device (including reading access list)* [▶ 417]).

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
Hier können Sie Details der Schließung bearbeiten

Hogwarts Synchronisieren In Matrix anzeigen Online Mode

1 Details

SCHLIEßUNGSDetails

Bereich: Lands

Seriennummer: 0853N3X

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: Gryffindor electronic portrait

TÜRDETAILS

Tür: Gryffindor tower

Tür-Code: DC-00001

Beschreibung:

< Zurück Weiter > Fertigstellen Abbrechen

2. Click on the **Audit trail** tab.

Zutrittsliste

- Window switches to the "Audit trail" 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

- Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
- Click on the **Export**  button.
 - The Explorer window will open.
- 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* [▶ 493]).

19.2 Identifying an unknown locking device

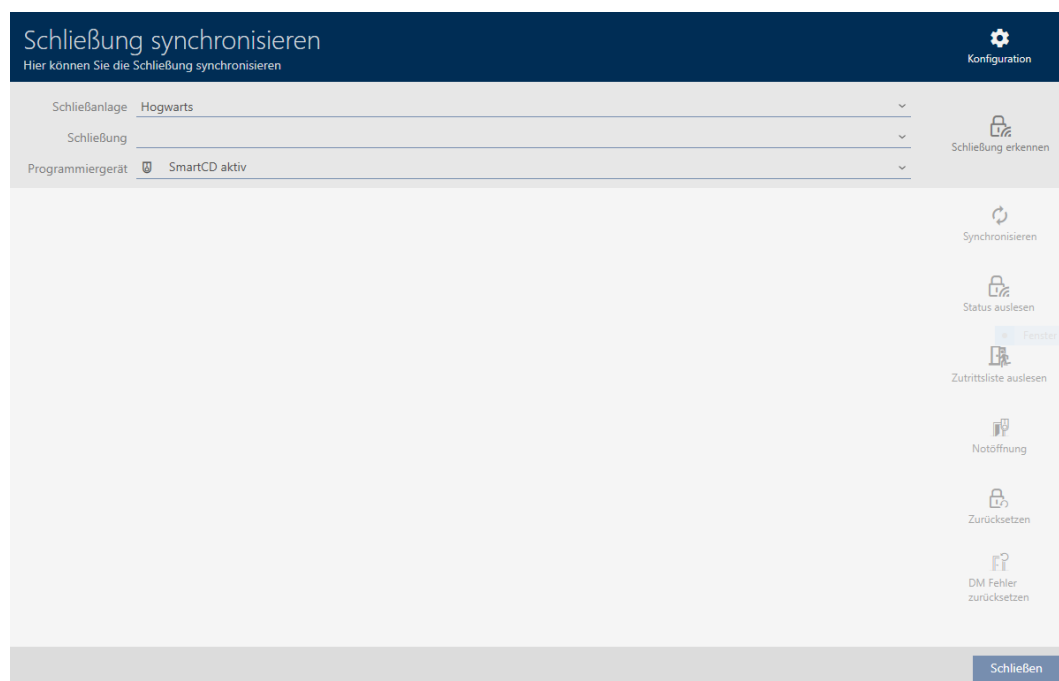
If you have an unknown locking device, you can use, for example, the synchronise symbol (🔑) to identify it and reset if necessary (see *Re-setting the locking device* [▶ 426]).

✓ Suitable programming device connected.

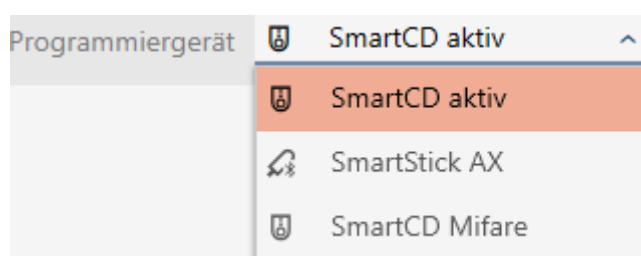
1. Click on the 🔑 icon in the header.



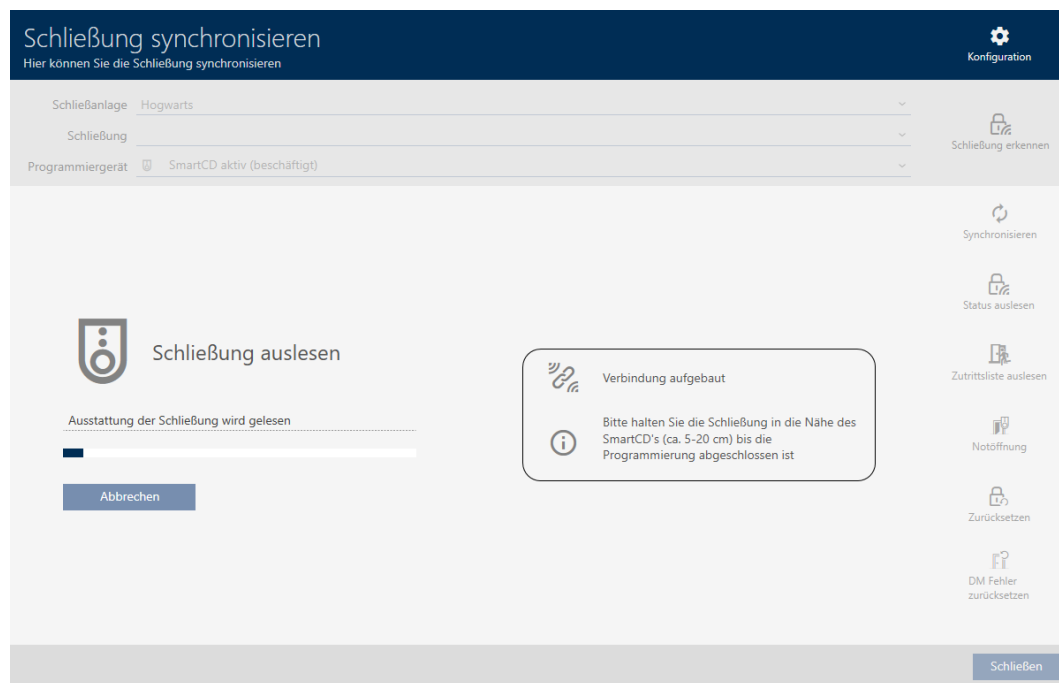
→ The "Synchronise lock" window will open.



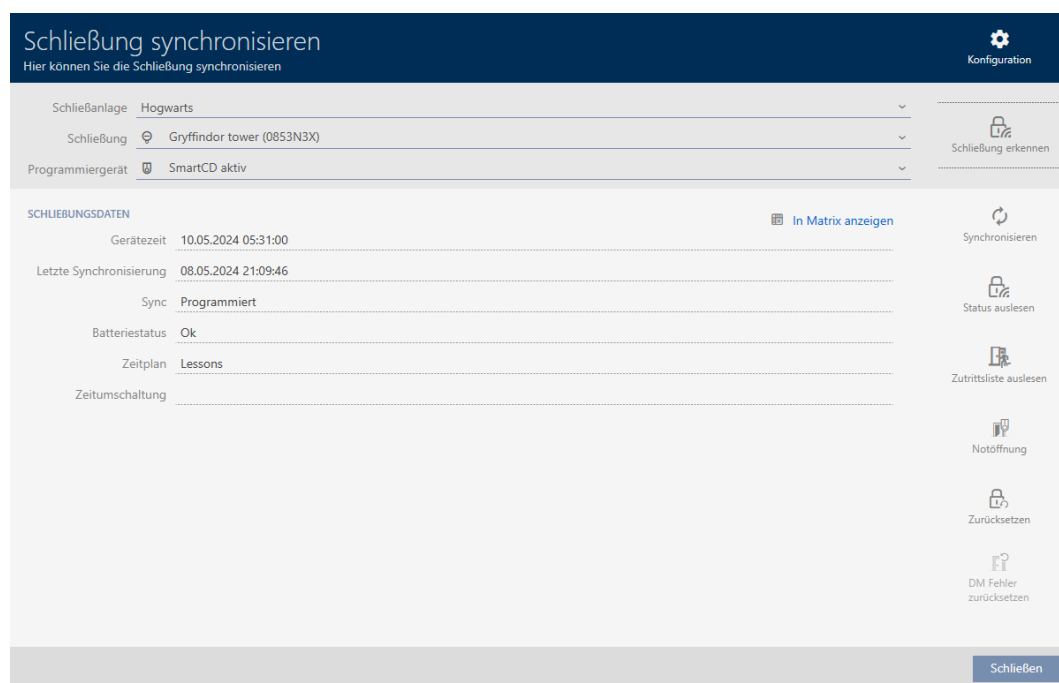
2. Select the programming device you wish to use to identify your locking device from the ▼ Programming device drop-down menu.



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* [▶ 426]).

19.3 Re-setting the locking device

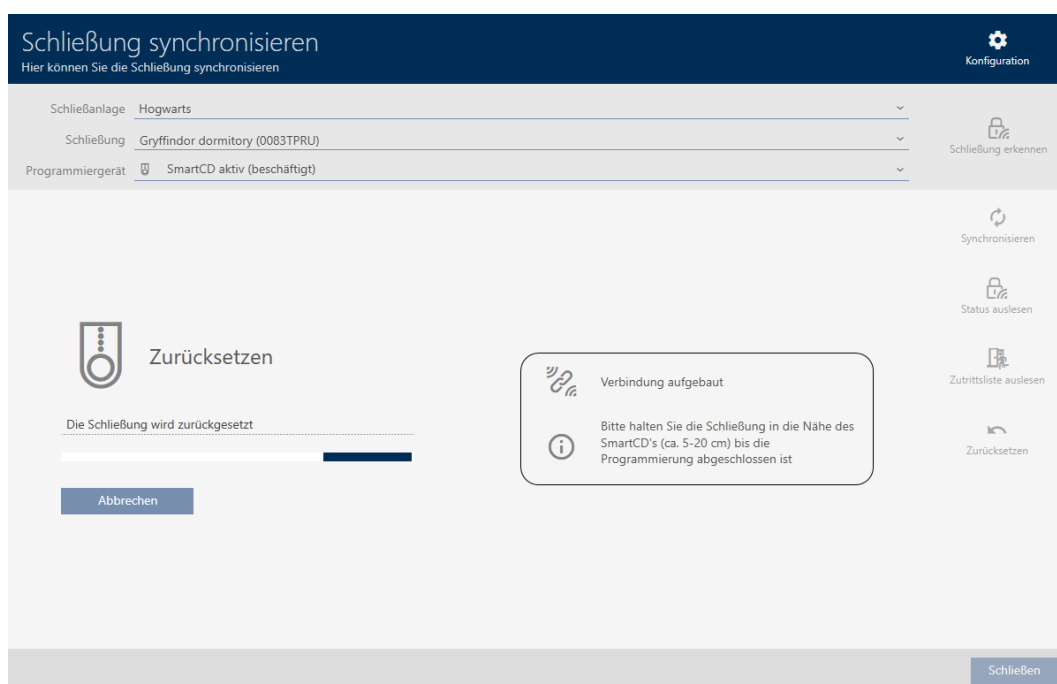
You must reset a component such as a locking cylinder before it can be used for another locking device or another locking system.

- ✓ Suitable programming device connected.
- ✓ 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* [▶ 424]). Then continue.
→ The locking device window will open.

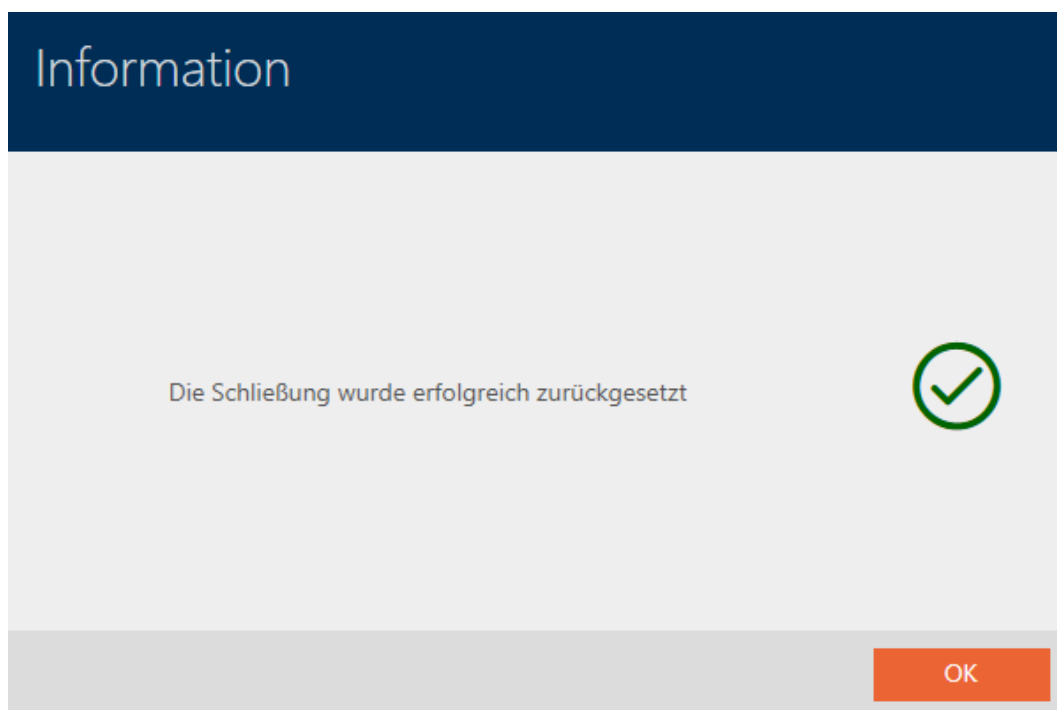
2. Click on the **Synchronisation** button .
→ Synchronise window will open.
3. Select the programming device from the ▼ **Programming device** drop-down menu with which you wish to reset your locking device.

4. Click on the **Reset** button .
→ The locking device is reset.



5. If necessary, accept the query asking whether the access lists should be imported again beforehand.

→ Locking device is reset.



19.4 Synchronising an identification medium

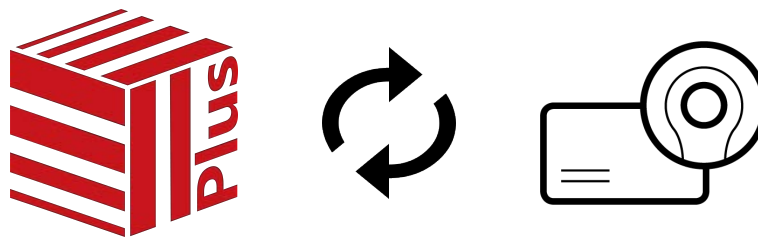
Synchronisation is bidirectional:

- Importing of data stored in the identification medium (e.g. battery level)
- Writing new data onto the identification medium (e.g. authorisations)

Physical access list can be imported separately ([Read personal audit trail](#) button). Physical access lists can also be imported easily during synchronisation as an option (see [Reading access list/physical access list during synchronisation](#) [▶ 487]).

The imported data can then be displayed (see [Displaying the identification medium battery status](#) [▶ 430] or [Displaying and exporting physical access lists for cards/transponders](#) [▶ 431], for example).

19.4.1 Synchronise a card/transponder (including importing physical access list)



The following example shows how to synchronise a transponder.

- ✓ Suitable programming device connected.
 - ✓ Identification media list or matrix view open.
1. Click on the identification medium you wish to synchronise.
 - ➔ The identification medium window will open.

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

n/a

Transpondertyp

⊗ Transponder

Firmware Version

Letzte Synchronisierung

10.05.2024 06:05:02

Sync

Erstprogrammierung

Batteriestatus

Zeitgruppe

☐ Zeitgruppe 1

Beschreibung

< Zurück

Weiter >

Fertigstellen

Abbrechen

2. Click on the [Synchronisation](#) button .
 - ➔ Synchronise window will open.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts

Transponder

Weasley, Ron

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

Sync

Erstprogrammierung

Status

Aktiviert

Batteriestatus

Zeitgruppe

Synchronisieren

Status auslesen

Begehungliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

Schließen

3. Select the programming device which you wish to use to synchronise from the ▼ Programming device drop-down menu.

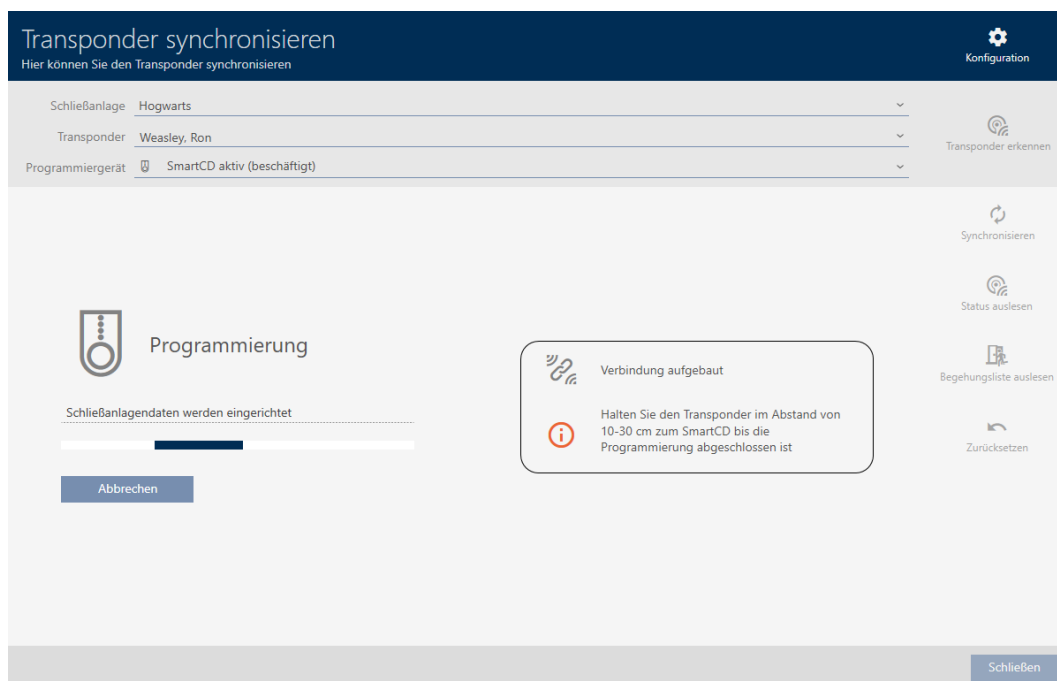
Programmiergerät

SmartCD aktiv

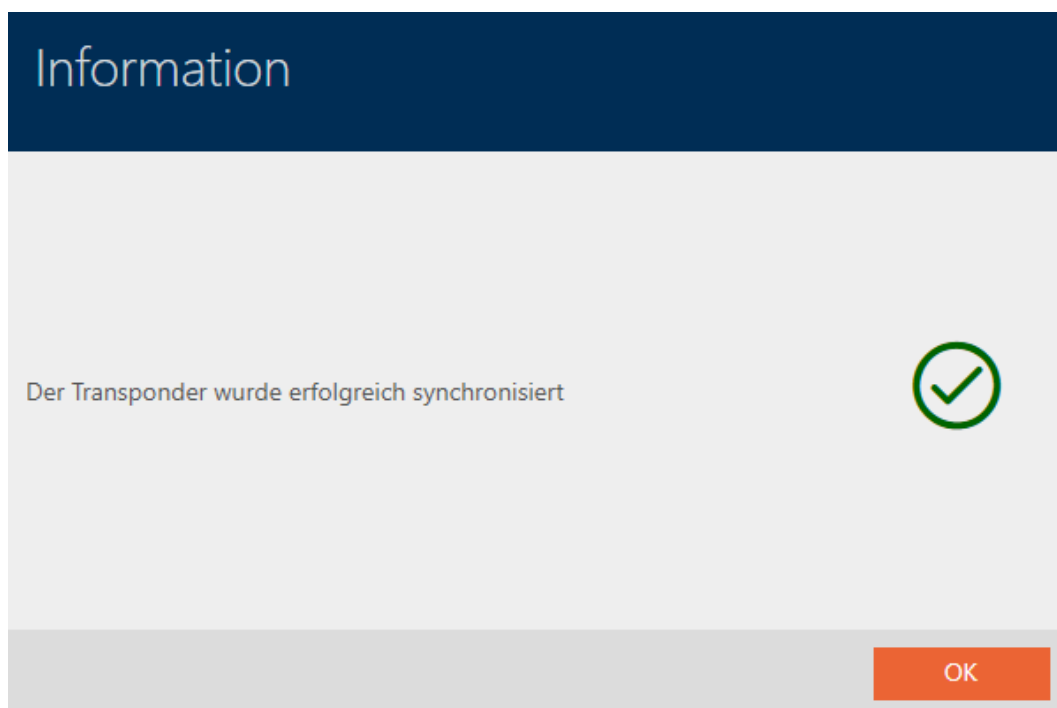
SmartCD aktiv

SmartCD Mifare

4. Click on the **Synchronisation** button .
 ↳ Identification medium is synchronised.



→ ID medium is synchronised.



19.4.1.1 Displaying the identification medium battery status



NOTE

Displayed status corresponds to the last synchronisation

AXM 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.

19.4.1.2 Displaying and exporting physical access lists for cards/transponders

If required, your identification media can log which locking devices they were activated on (see *Allow accesses to be recorded by identification media (physical access list)* [▶ 134]). 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)* [▶ 428]).

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.

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

10.05.2024 06:16:19

Sync

Programmiert

Batteriestatus

Ok

Zeitgruppe

Zeitgruppe 1

Beschreibung

< Zurück

Weiter >

Fertigstellen

Abbrechen

2. Clicking on the **Personal audit trail** tab

Begehungsliste

➡ Window switches to the "Personal audit trail" tab.

Transponder - Begehungsliste

Hier können Sie bei aktivierter Begehungsliste die ausgelesenen Begehungen des Transponders einsehen

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

Löschen

Export

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

< Zurück

Weiter >

Fertigstellen

Abbrechen

3. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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'

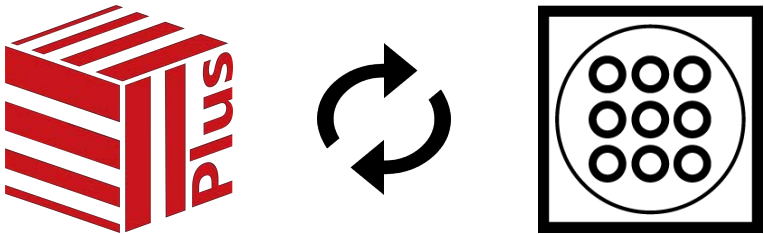
Datum	Tür	S/N	LID
10.05.2024 06:24:00	Gryffindor dormitory	00AXNNH	10004
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:24:00	Gryffindor tower	0853N3X	10000
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:23:00	Main gate	00E04GX	10003
10.05.2024 06:22:00	Gryffindor tower	0853N3X	10000



Ausdruck vom: 10.05.2024

You have the option to personalise reports (see *Personalising reports and exports* [▶ 493]).

19.4.2 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* [▶ 573]). In this case, synchronise the locking device instead (see *Synchronising the locking device (including reading access list)* [▶ 417]).

Synchronisation between the two PIN code keypads is different. Your AXM Plus will assist you with instructions during synchronisation.



NOTE

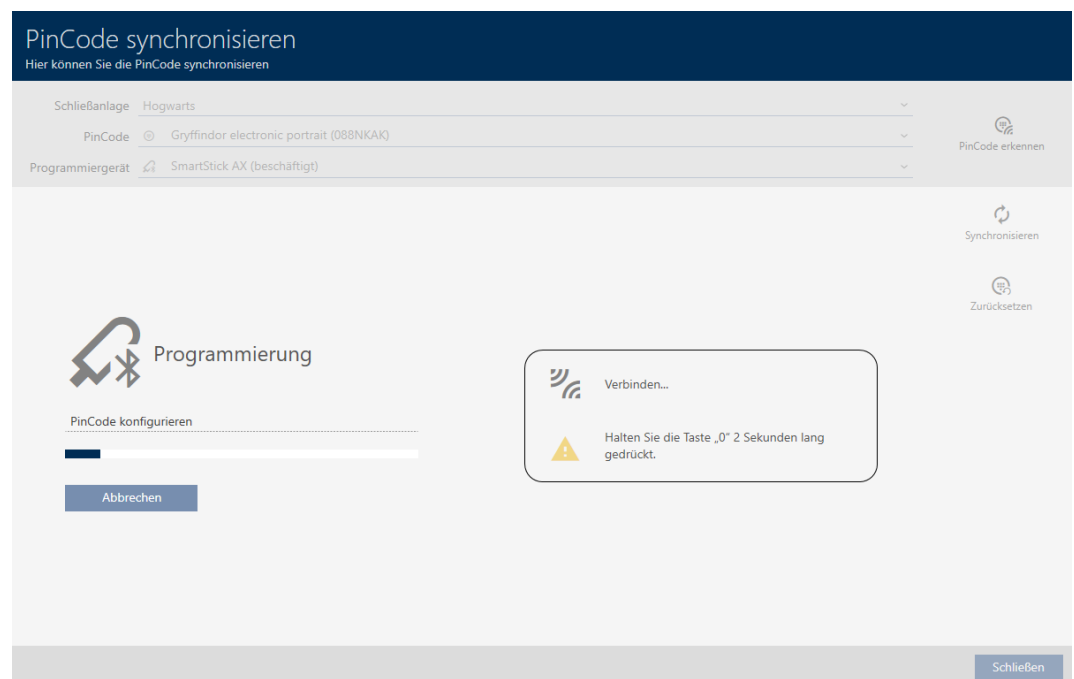
PIN code keypad 3068 synchronisation requires a master PIN and user PINs

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.

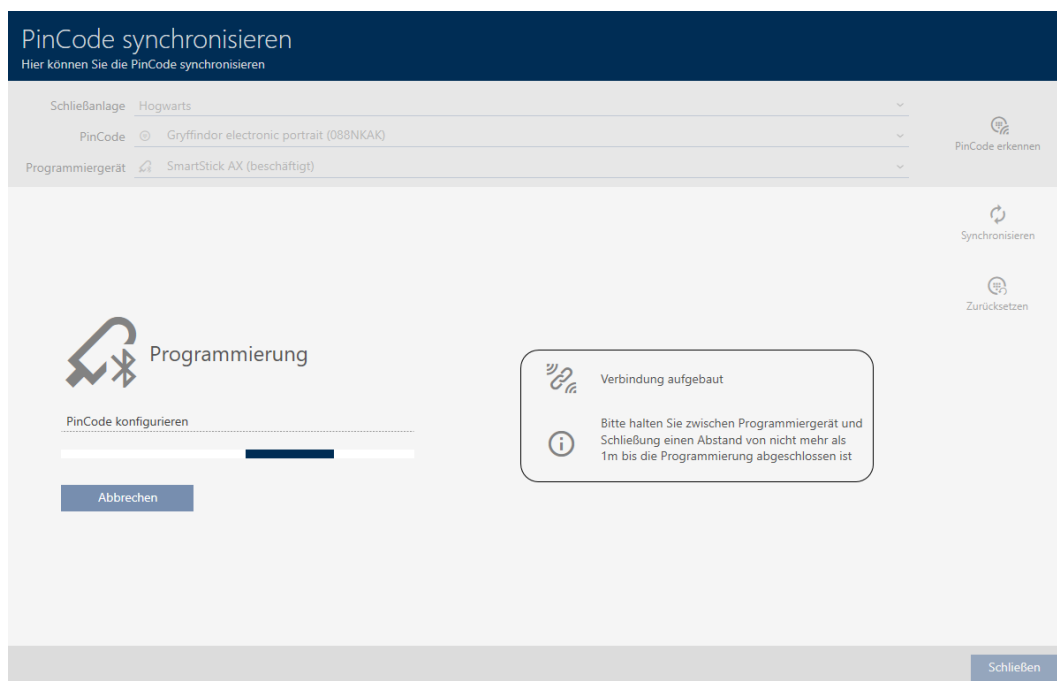
- ✓ PIN code keypad AX created and assigned (see [Creating PIN code keypads \[► 106\]](#)).
 - ✓ Programming requirement for PIN code keypad AX, e.g. due to a change in authorisation.
 - ✓ Suitable programming device connected (SmartStick AX).
 - ✓ Matrix screen open.
1. Click the synchronise icon for any PIN associated with the PIN code keypad AX concerned.
 - ➔ The "Synchronise PinCode keypad" window opens and synchronisation starts.



2. Press and hold the “0” button on the PIN code keypad AX for at least two seconds.



3. 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 awakened.
 - ↳ 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.

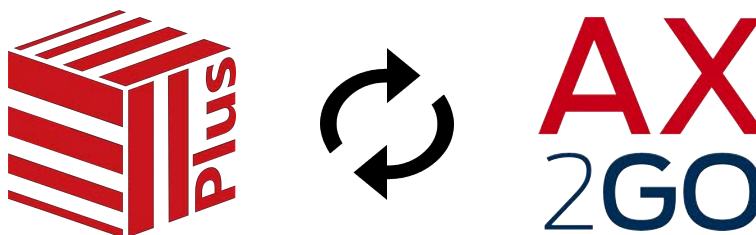
Information

Die PinCode wurde erfolgreich synchronisiert



OK

19.4.3 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* [▶ 577] for more information).

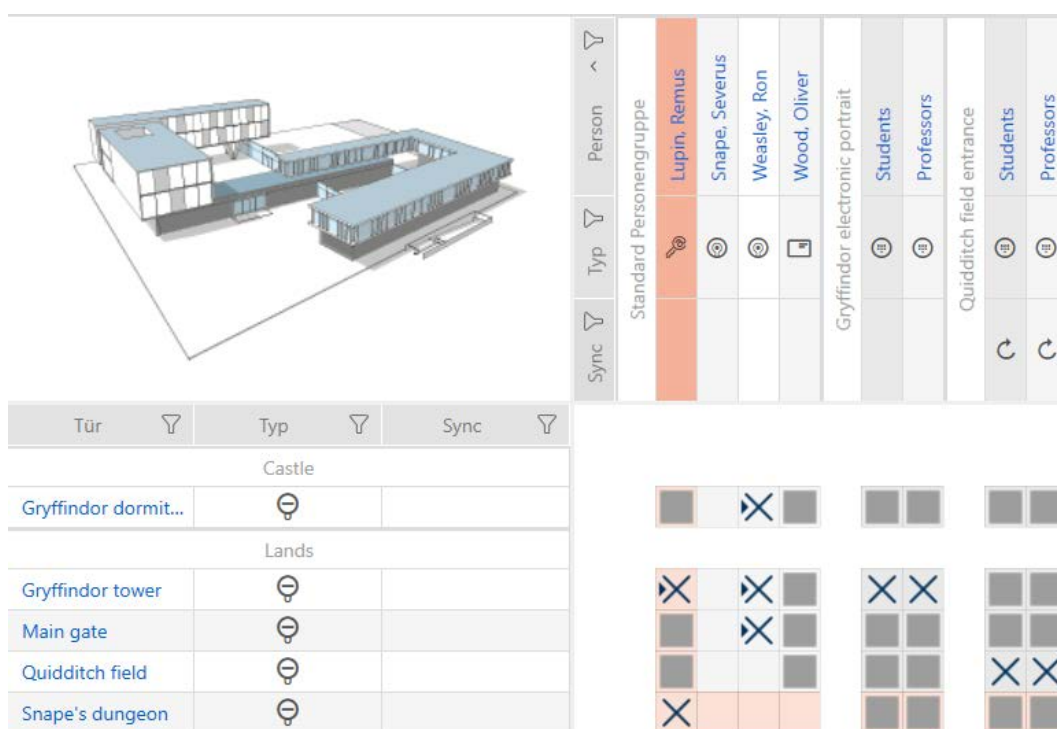
The following example describes the synchronisation process when an AX2Go key is authorised for a locking device for the first time.

In the initial situation, no AX2Go key has been authorised on the locking device yet:

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	🔑	
Gryffindor electronic portrait		
Students	🔑	
Professors	🔑	
Quidditch field entrance		
Students	🔑	
Professors	🔑	

- ✓ Valid ☒ Software Fee licence (see *Registration with licence* [▶ 44]).
- ✓ Connection between SimonsVoss ID and AXM Plus (see *Registration with licence* [▶ 44]).
- ✓ 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.



➔ 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](#) [▶ 450]).

19.5 Identifying an unknown ID medium

19.5.1 Recognise unknown cards/transponders

✓ Suitable programming device connected.

1. Click on the  icon in the header.



➔ The "Synchronise transponder" window will open.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts

Transponder

Weasley, Ron

Programmiergerät

SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung

Sync

Erstprogrammierung

Status

Aktiviert

Batteriestatus

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

PROGRAMMIERTE DATENSÄTZE

Schließen

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.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts

Transponder

Weasley, Ron

Programmiergerät

SmartCD aktiv (beschäftigt)

Transponder erkennen



Transponder auslesen

Erkennung des Transponders läuft

Abbrechen



Verbinden...



Drücken Sie jetzt den Taster des Transponders
1x kurz in Abstand von 10-30 cm zum SmartCD

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

Schließen

- ➔ Information about the identification medium is displayed in the window.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren



Konfiguration

Schließanlage

Unbekannt

Transponder

002U0KLC

Programmiergerät

SmartCD aktiv



Transponder erkennen



Synchronisieren



Status auslesen



Begehungliste auslesen



Zurücksetzen

TRANSPONDERDATEN

Letzte Synchronisierung

Sync

Status

Batteriestatus

Zeitgruppe

Ok

PROGRAMMIERTE DATENSÄTZE

Pos	Schließanlage/SID	SID Extension	TID	Aktivierungsdatum	Verfallsdatum	Zeitgruppe
1	Unbekannt (Sid=1537)	12028330	3202			

Schließen

You can now reset the identification medium, for example (see [Resetting cards/transponders](#) [▶ 442]).

19.5.2 Identifying unknown PIN code keypad

- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)

1. Click on the  icon in the header.



- The "Synchronise PinCode keypad" 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 keypad** button .
4. Follow the instructions as necessary.
 - ➔ PIN code keypad is being read.

PinCode synchronisieren

Hier können Sie die PinCode synchronisieren

Schließanlage

Hogwarts

PinCode

Programmiergerät

SmartStick AX (beschäftigt)

PinCode erkennen

Synchronisieren

Zurücksetzen

PinCode auslesen

PinCode wird ausgelesen

Abbrechen

Verbindung aufgebaut

Bitte halten Sie zwischen Programmiergerät und Schließung einen Abstand von nicht mehr als 1m bis die Programmierung abgeschlossen ist

Schließen

→ Information about the PIN code keypad is displayed in the window.

PinCode synchronisieren

Hier können Sie die PinCode synchronisieren

Schließanlage

Hogwarts

PinCode

Gryffindor electronic portrait (088NKAK)

Programmiergerät

SmartStick AX

PinCode erkennen

Synchronisieren

Zurücksetzen

In Matrix anzeigen

PINCODE DATEN

Letzte Synchronisierung

08.05.2024 19:57:02

Status

Aktiviert

Sync

Programmiert

Batteriestatus

Ok

Tür

Gryffindor tower

1	Pin Name	Students	Sync	Berechtigt	☒	Status	Programmiert
2	Pin Name	Professors	Sync	Berechtigt	☒	Status	Programmiert
3	Pin Name	House-Elfs	Sync	Berechtigt	☐	Status	Nicht programmiert

Schließen

You can now reset the PIN code keypad, for example (see *Resetting the PIN code keypad* [▶ 446]).

19.6 Resetting identification media

19.6.1 Resetting cards/transponders

You must reset a component such as a transponder before it can be used again for an identification medium or another locking system.

- ✓ Suitable programming device connected.
- ✓ 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* [▶ 438]). Then continue.
→ The identification medium window will open.

Transponder - Details

Hier können Sie die Details des Transponders bearbeiten

- 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 10.05.2024 06:16:19

Sync Programmiert

Batteriestatus Ok

Zeitgruppe ☐ Zeitgruppe 1

Beschreibung

< Zurück
Weiter >
Fertigstellen
Abbrechen

2. Click on the **Synchronisation** button.
→ Synchronise window will open.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage Hogwarts

Transponder Weasley, Ron (00XTN6K)

Programmiergerät SmartCD aktiv

Transponder erkennen

TRANSPONDERDATEN

Letzte Synchronisierung 10.05.2024 06:16:19 In Matrix anzeigen

Sync Programmiert

Status Aktiviert

Batteriestatus Ok

Zeitgruppe

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

^ PROGRAMMIERTE DATENSÄTZE

Schließen

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
☐	1	SID: 8974	3200	0	
☒	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 unbekannten 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
☒	1	SID: 8974	3200	0	
☒	2	Hogwarts	3209	0	

7. Click on the **OK** button.
8. Follow any further instructions as necessary.
 - ➔ Identification medium is being reset.

Transponder synchronisieren

Hier können Sie den Transponder synchronisieren

Konfiguration

Schließanlage

Hogwarts

Transponder

Weasley, Ron (00XTN6Q)

Programmiergerät

SmartCD aktiv (beschäftigt)

Transponder erkennen

Zurücksetzen

Transponder wird zurückgesetzt

Abbrechen

Verbindung aufgebaut

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

Synchronisieren

Status auslesen

Begehungsliste auslesen

Zurücksetzen

Schließen

- ➔ Identification medium is reset.

Information

Der Transponder wurde erfolgreich zurückgesetzt

OK

19.6.2 Resetting the PIN code keypad

You must reset a component such as a PIN code keypad before it can be used again for an identification medium or another locking system.

- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)
- ✓ 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* [▶ 440] in the AXM manual). Then continue.

→ The PIN code keypad window will open.

PinCode synchronisieren

Hier können Sie die PinCode synchronisieren

Schließanlage

Hogwarts

PinCode

Gryffindor electronic portrait (088NKAK)

Programmiergerät

SmartStick AX

PinCode erkennen

In Matrix anzeigen

Synchronisieren

Zurücksetzen

PINCODE DATEN

Letzte Synchronisierung	08.05.2024 19:57:02				
Status	Aktiviert				
Sync	Programmiert				
Batteriestatus	Ok				
Tür	Gryffindor tower				

1	Pin Name	Students	Sync	Berechtigt	☒	Status	Programmiert
2	Pin Name	Professors	Sync	Berechtigt	☒	Status	Programmiert
3	Pin Name	House-Elfs	Sync	Berechtigt	☐	Status	Nicht programmiert

Schließen

2. Click on the **Synchronisation** button.

→ Synchronise window will open.

PinCode synchronisieren
Hier können Sie die PinCode synchronisieren

Schließanlage: **Hogwarts**

PinCode: **Gryffindor electronic portrait (088NKAX)**

Programmiergerät: **SmartStick AX**

[In Matrix anzeigen](#) [Synchronisieren](#) [Zurücksetzen](#)

PINCODE DATEN

Letzte Synchronisierung: **08.05.2024 19:57:02**

Status: **Aktiviert**

Sync: **Programmiert**

Batteriestatus: **Ok**

Tür: **Gryffindor tower**

	Pin Name	Sync	Berechtigt	Status
1	Students	Sync	Berechtigt	Programmiert
2	Professors	Sync	Berechtigt	Programmiert
3	House-Elfs	Sync	Berechtigt	Nicht programmiert

[Schließen](#)

3. Select the programming device from the ▼ **Programming device** drop-down menu with which you wish to reset your PIN code keypad.

Programmiergerät: **SmartStick AX**

SmartCD aktiv

SmartStick AX

4. Click on the **Reset** button .



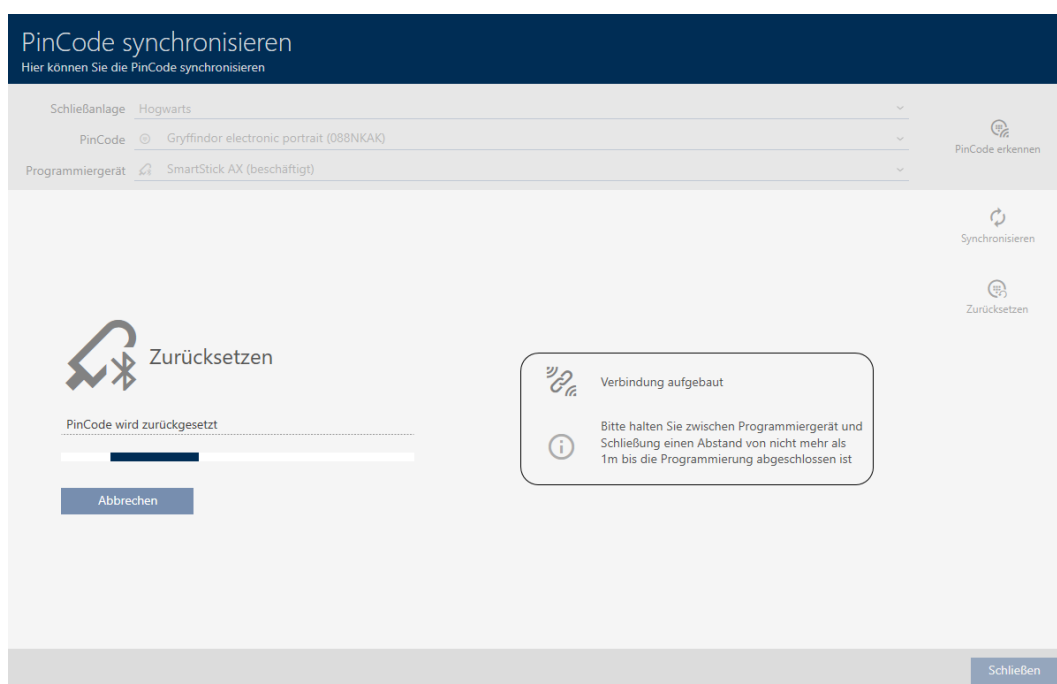
NOTE

Resetting PIN code keypads that do not form part of the project

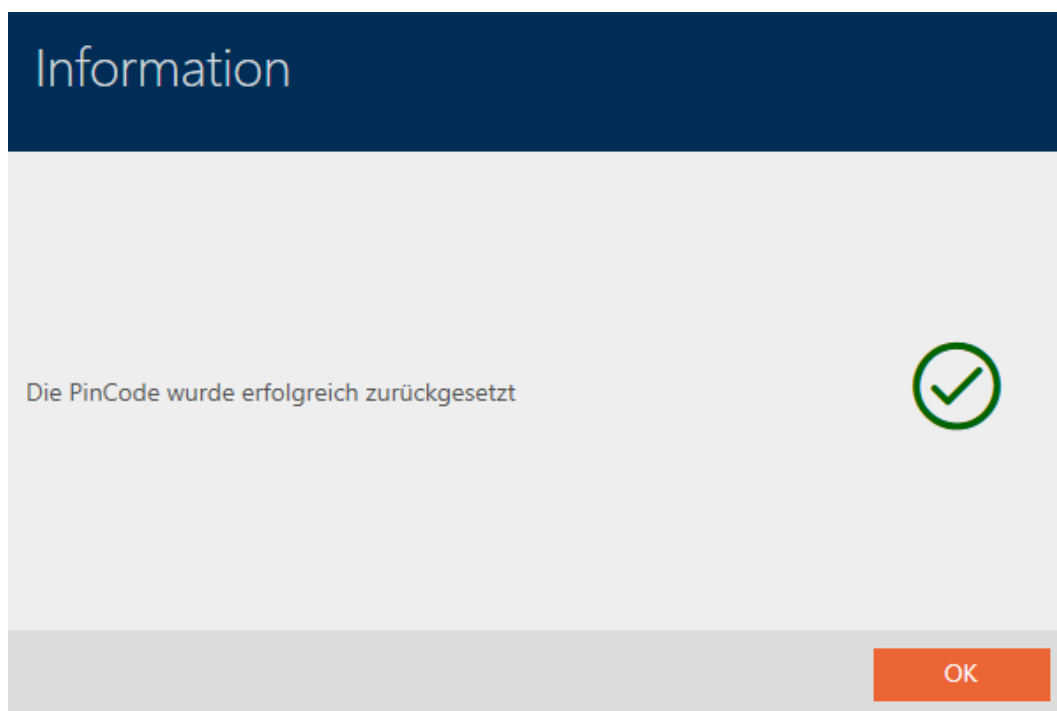
Your AXM Plus can also reset PIN code keypads that were not created in the same project. In this case, however, your AXM Plus does not know the locking system password used.

- 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.



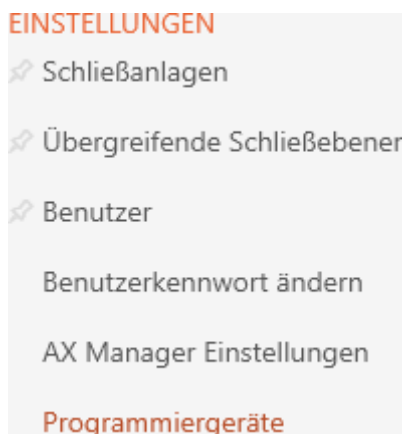
19.7 Viewing connected/supported programming devices

This window can be used to check whether a connected programming device is functional and identified.

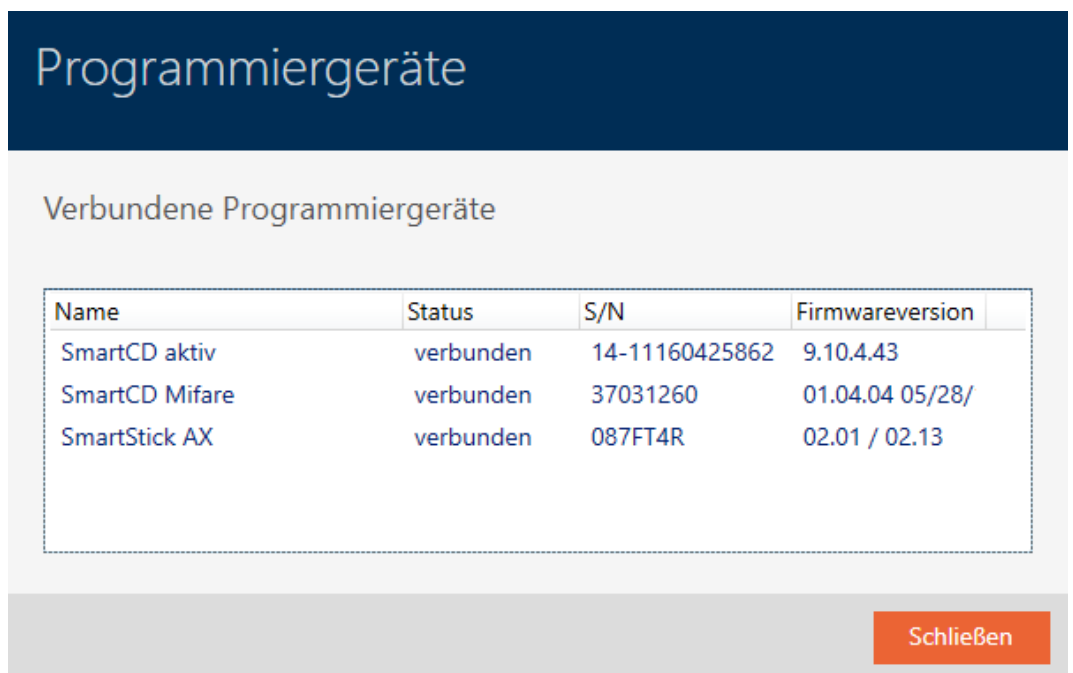
1. Click the orange AXM button .
 - AXM bar opens.



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.

19.8 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.

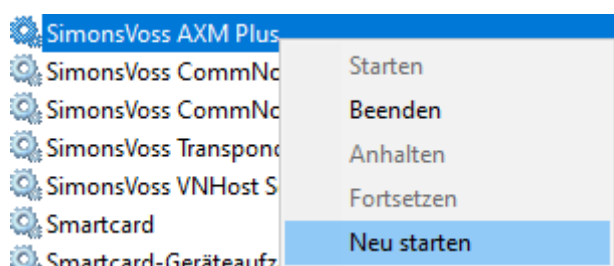
You can easily check this connection in the lower bar of your AXM Plus:



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 \[▶ 39\]](#)).
6. Then check the entry again using **Cloud State:**.

20. Networking

20.1 CommNode set up

The CommNode is required as soon as you start working with networked locking devices. For more information, see *CommNode and VNHost* [▶ 621].

- ✓ AXM Plus is installed (see *Installation* [▶ 27]).
- ✓ At least one project is available (see *First steps after a new installation* [▶ 35]).

1. Open the Windows application "CommNode".



- ↳ The browser opens to the CommNode configuration page.



2. Click the **Verbinden** button.

- ↳ A message appears in the browser indicating that CommNode has been successfully connected.

CommNode

CommNode-Host ist mit der Plattform verbunden

Then proceed with setting up your network:

- Virtual network: *Virtual network* [▶ 451]
- WaveNet: *WaveNet* [▶ 463]

20.2 Virtual network

To operate your virtual network, you need the *VNHost service* [▶ 452] and *gateways* [▶ 453].

Enhance the security of your virtual network with a dynamic time window (optional, see *Set up a dynamic time window (time budget)* [▶ 462]).

Further information on function and configuration can be found here, together with examples of usage: [Virtual network \[▶ 608\]](#).

20.2.1 Configure of VNHost

The VNHost required for the virtual network is automatically installed together with your AXM Plus. It is responsible for the communication between the gateways and the database.

- ✓ AXM Plus is installed (see [Installation \[▶ 27\]](#)).
- ✓ At least one project is available (see [First steps after a new installation \[▶ 35\]](#)).

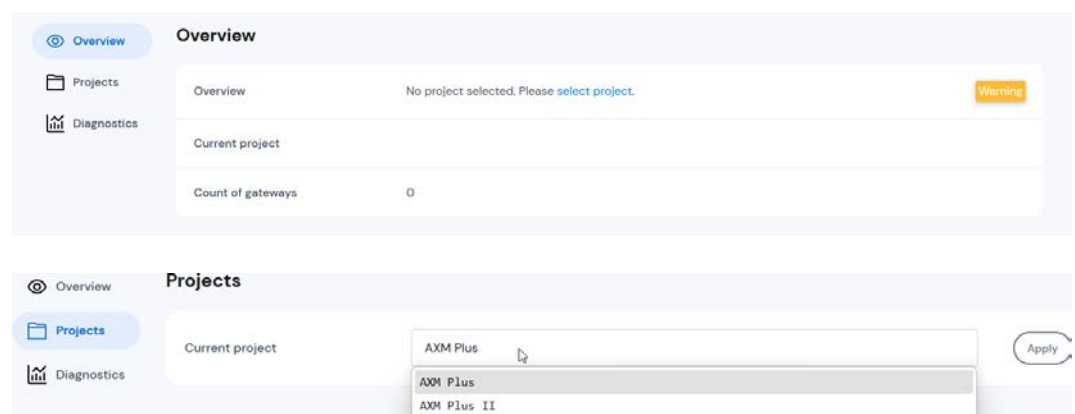
1. Open Windows services "VNHost".



→ The browser opens with the VNHost configuration page.

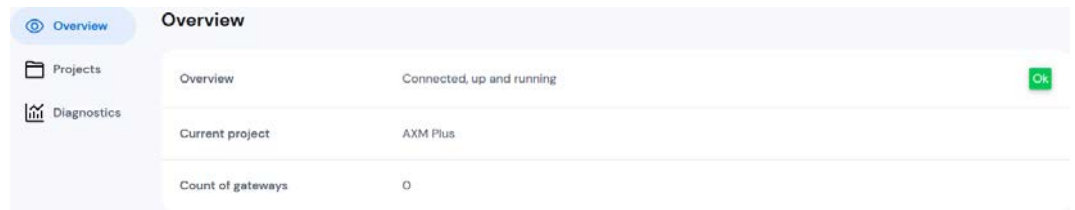


2. Click the **Connect** button.
3. If you have more than one project in your AXM Plus, switch to the Projects tab and select the project with which you want to use the virtual network.



4. Confirm the selection with the **Apply** button.

→ VNHost is configured.



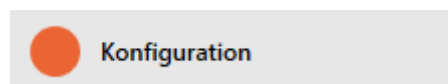
You may now add gateways that will be utilised in the virtual network. (see [Add Gateways \[▶ 453\]](#)).

20.2.2 Add Gateways

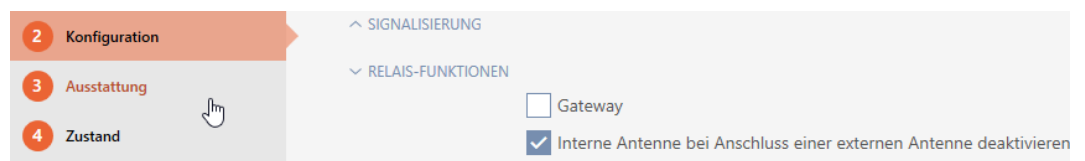
The gateways recognise identification media such as transponders and query the VNHost for current information stored in the database. (see [Virtual network \[▶ 608\]](#)).

- ✓ Locking device list or matrix view open.
- ✓ VNHost is configured for the current project (see [Configure of VNHost \[▶ 452\]](#)).
- ✓ At least one SmartRelais 3 Advanced is networked (see [Connect SmartRelay to network \[▶ 323\]](#)).

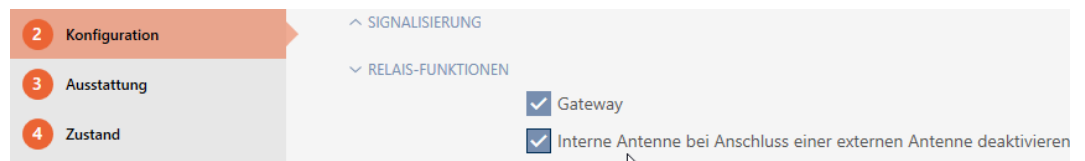
1. Click on the SmartRelay that is to be utilised as a gateway.
2. Click on the **Configuration** tab.



→ Window switches to the "Configuration" tab.



3. Expand the "Relay functions" menu.
4. Select the ☒ Gateway checkbox.



5. Click the **Finish** button.
- The locking device window closes.

- Click the button  **Synchronisation** and synchronise the locking device (for details see *Synchronising the locking device (including reading access list)* [▶ 417]).

➔ Gateway is installed.

Then check the virtual network (see *Checking virtual network* [▶ 454]) to see if your new Gateway is displayed.

20.2.3 Checking virtual network

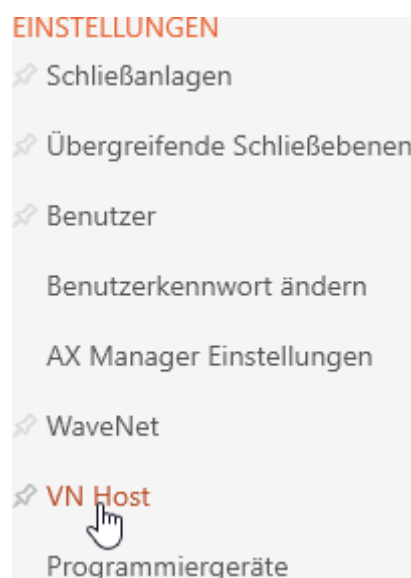
This chapter contains information on how to verify the VNHost. The transmission of blocked IDs to locking devices etc. can be checked with VN Block List (see *Overview of blocked IDs (VN block list)* [▶ 456]).

Check in the AXM Plus

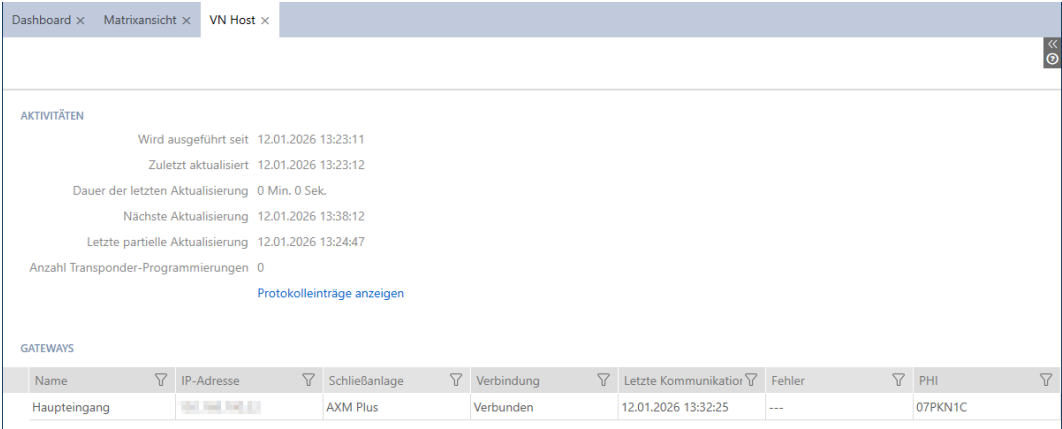
- Click the orange AXM button  **AXM**.
- ➔ AXM bar opens.



- Select the **VN Host** entry in the | SETTINGS | group.



➔ The [VN Host] tab will open.



The tab [VN Host] displays the following information:

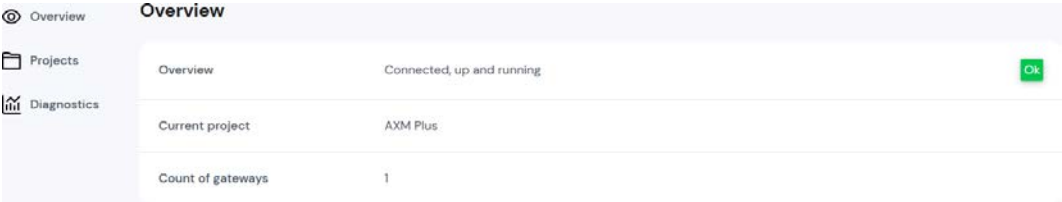
Activities	- Executed since - Last updated - Duration of the last update - Next update - Last partial update - Number of transponder programmings
Gateways	Here you will find a list of gateways connected to your virtual network. You can add more Gateways at any time (see Add Gateways [453]). If you cannot see the newly added Gateways yet, you will need to re-start the Windows service <i>SimonsVoss VNHost</i>.

Check in the web app

- Open Windows services "VNHost".



→ The browser opens with the VNHost configuration page.



The overview shows the following information:

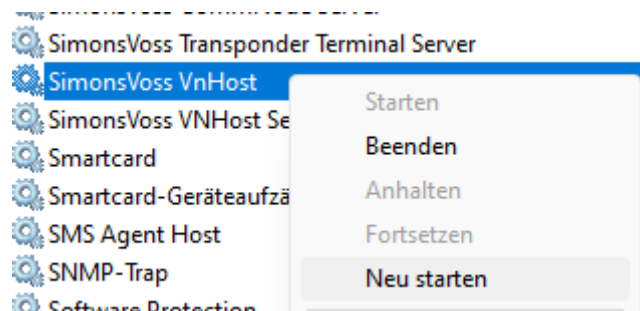
- Service status
- Project to which the VNHost is currently connected
- Number of gateways

If you have recently installed a gateway that is not yet displayed, do the following:

1. Open Windows services.



2. Right-click on the service *SimonsVoss VNHost* to open the context menu and restart the service.



3. Reload the browser page (Ctrl+F5).

20.2.4 Overview of blocked IDs (VN block list)

This window lists the locking devices that have not yet been affected by the blocking of an authorised transponder.

If you create a substitute transponder during the blocking process, the blocked transponder's block ID is automatically assigned to the substitute.

In the following example, a transponder is blocked and a substitute transponder is created.

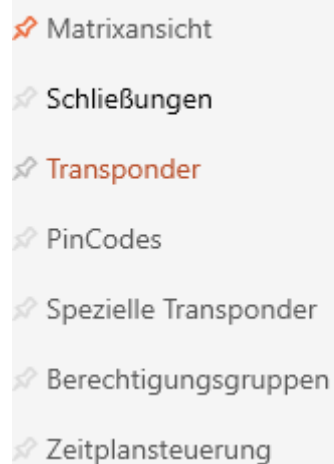
- ✓ Virtual network is installed (see [CommNode set up \[▶ 451\]](#), [Configure of VNHost \[▶ 452\]](#) and [Add Gateways \[▶ 453\]](#)).

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



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

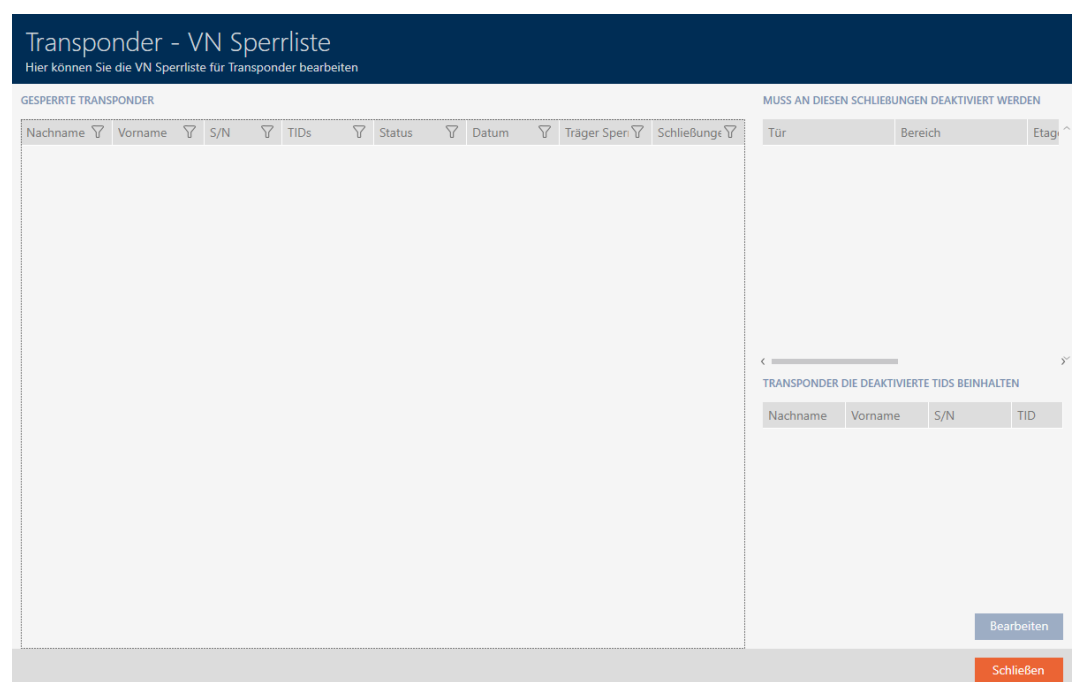
SCHLIESSANLAGENSTEUERUNG



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

3. Click on the **VN Block List** button.

- ↳ The "Transponder - VN Block list" window opens.



There are currently no entries in this window because you have not yet blocked any transponders. The Window consists of several parts:

Blocked transponders

GESPERRTE TRANSPONDER

Nachname	Vorname	S/N	TIDs	Status	Datum	Träger Speri	Schließung
----------	---------	-----	------	--------	-------	--------------	------------

This list shows all the identification media that you have blocked, for example, in response to a loss. (see *Blocking and replacing lost/stolen card/transponder permanently* [▶ 177]).

Should be deactivated in locks

MUSS AN DIESEN SCHLIEßUNGEN DEAKTIVIERT WERDEN		
Tür	Bereich	Etag

This list shows all the locking devices for which the selected blocked identification medium was previously authorised. These locking devices must be informed of the blocking of the identification medium. Locking devices for which the identification medium is not authorised are not displayed, as this medium cannot be used to grant access. The entry is removed from the list when:

1. An identification medium has retrieved the blocked ID from the gateway **and**
2. transferred it to the locking device **and**
3. has returned the locking device confirmation (= has received blocked ID) to the gateway.

Further information and an example of the procedure can be found here: *Example: loss of transponder* [▶ 616]

Transponders containing deactivated TIDs

TRANSPONDER DIE DEAKTIVIERTE TIDS BEINHALTEN

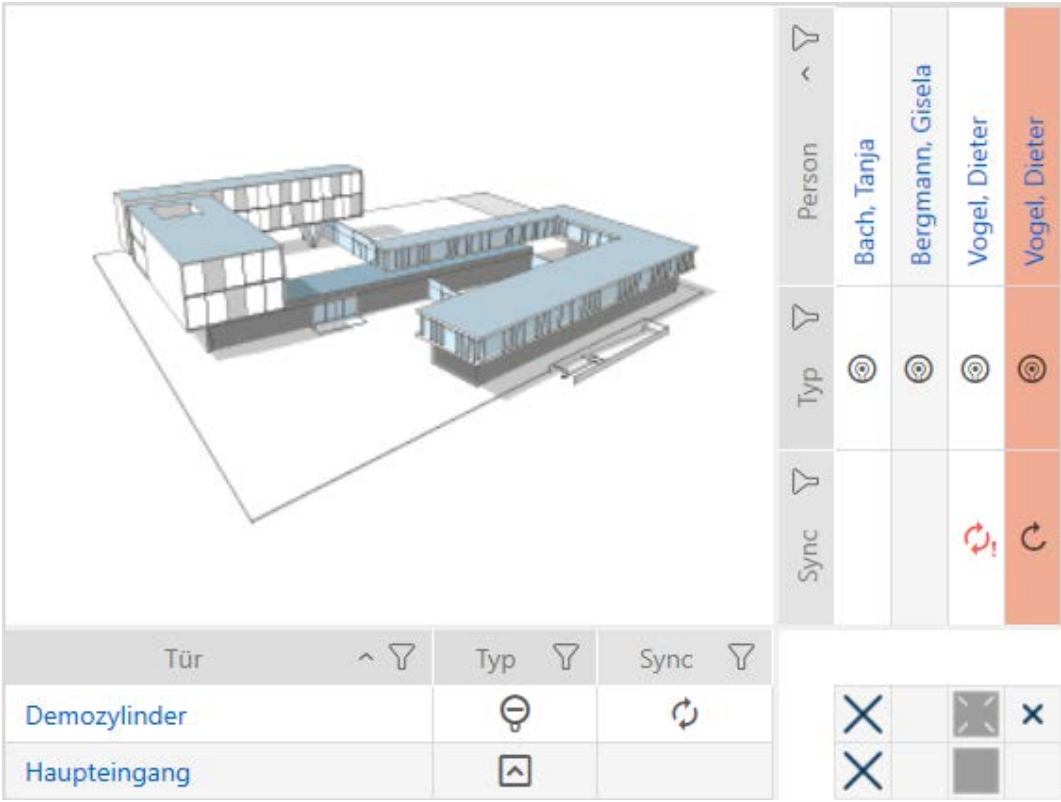
Nachname	Vorname	S/N	TID
----------	---------	-----	-----

The blocked ID is transferred via other identification media **of the same type**. In normal cases, two blocked IDs (cards: one blocked ID) are randomly selected from the list "Blocked transponders" and written to the identification media at the gateway. There are two exceptions:

- Substitute transponders: These automatically incorporate the blocked ID of the blocked transponder. As the communication distances are likely to be similar, the affected locking devices are updated promptly.
- Manual assignment: With the button **Edit**, you can explicitly assign the marked blocked ID to specific identification media.

Example: Blocking transponders and creating substitute transponders

1. Block a transponder and create a substitute transponder (see *Blocking and replacing lost/stolen card/transponder permanently* [► 177]).
 - ➔ Blocked transponders and substitute transponders are visible in the matrix.



The screenshot displays the AXM Plus software interface. On the left, there is a 3D isometric view of a building complex. To the right of the building view is a table with four columns: 'Person', 'Typ', and 'Sync'. The 'Person' column lists names: 'Bach, Tanja', 'Bergmann, Gisela', 'Vogel, Dieter', and 'Vogel, Dieter'. The 'Typ' column contains icons representing different transponder types. The 'Sync' column contains icons representing synchronization status. Below the building view is a table with three columns: 'Tür', 'Typ', and 'Sync'. The 'Tür' column lists door names: 'Demozylinder' and 'Haupteingang'. The 'Typ' column contains icons representing different door types. The 'Sync' column contains icons representing synchronization status. To the right of the bottom table is a small grid of icons, including a large 'X', a small 'X', and a square icon.

Person	Typ	Sync
Bach, Tanja	⊙	
Bergmann, Gisela	⊙	
Vogel, Dieter	⊙	↻
Vogel, Dieter	⊙	↻

Tür	Typ	Sync
Demozylinder	⊙	↻
Haupteingang	⊙	

2. Go back to the tab [Transponder].
3. Click on the **VN Block List** button.
 - ➔ The "Transponder - VN Block list" window opens.

Transponder - VN Sperrliste

Hier können Sie die VN Sperrliste für Transponder bearbeiten

Nachname	Vorname	S/N	TIDs	Status	Datum	Träger Sper	Schließung
Vogel	Dieter	03UEP47	3208	Deaktiviert	15.01.2026	1	1

MUSS AN DIESEN SCHLIEßUNGEN DEAKTIVIERT WERDEN

Tür	Bereich	Etag
Demozylinder		

TRANSPONDER DIE DEAKTIVIERTE TIDS BEINHALTEN

Nachnam	Vorname	S/N	TID
Vogel	Dieter		1 von 2

[Bearbeiten](#) [Schließen](#)

- The transponder that has just been blocked is now in the list "Blocked transponders".
 - Since the blocked transponder was authorised for storage, this locking device is included in the list "Should be deactivated in locks".
 - A substitute transponder was created and the blocked transponder's ID was automatically assigned to it. Hence, the substitute transponder is included in the list "Transponders containing deactivated TIDs".
4. Click the button **Edit**.
- "Transponders that are to contain deactivated TIDs" opens.

Transponder die deaktivierte TIDs beinhalten sollen

Hier können sie die deaktivierten TIDs zu Transpondern hinzufügen

Ausgewählter Transponder: Vogel, Dieter - Seriennummer: 03UEP47 - TID: 3208

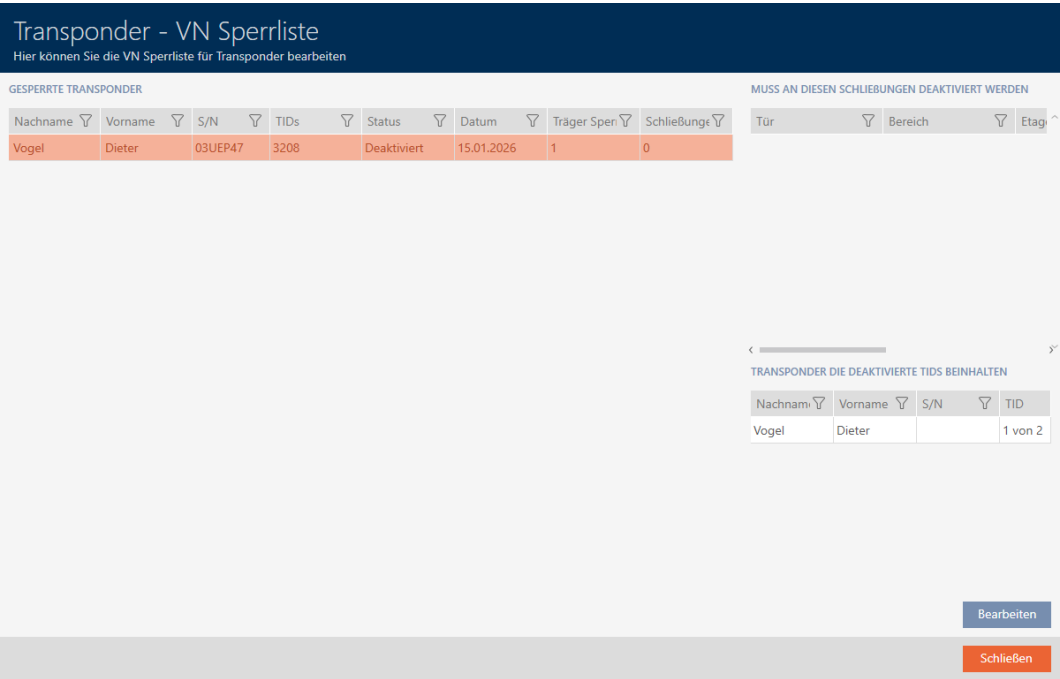
Nachname	Vorname	S/N	TIDs
Vogel	Dieter		1 von 2

Nachname	Vorname	S/N	TID
Bach	Tanja	01X4CDH	0 von 2
Bergmann	Gisela	01X14GT	0 von 2

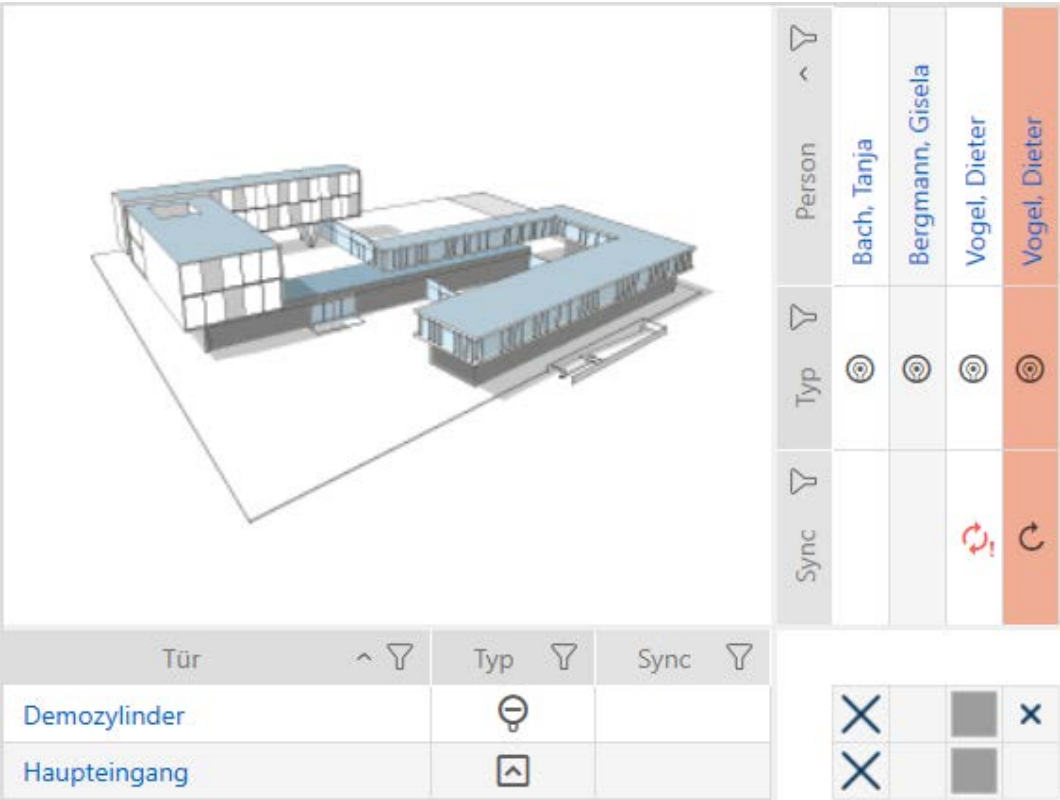
[OK](#) [Abbrechen](#)

5. Optional: You can assign the blocked ID to another transponder in the right-hand column.

Once the blocked transponder's ID has been transferred to the affected locking device, it will no longer be displayed in the list "Should be deactivated in locks":



Additionally, the locking device is no longer programmed into the matrix, and the authorisation check mark for the blocked transponder is removed:



20.2.5 Set up a dynamic time window (time budget)

The dynamic time window (= "time budget") ensures that the identification media in your locking system are regularly activated via the gateway (for further information, see *Virtual network* [▶ 608]).

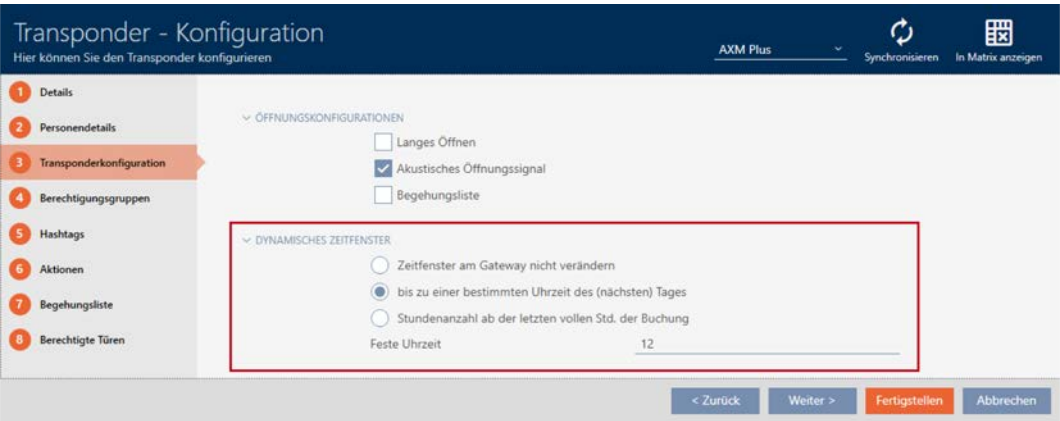
The dynamic time window in the virtual network differs from the Offline time budget (in days) of the AX2Go, see *Time budget (AX2Go and virtual network)* [▶ 599]. For the configuration of Offline time budget (in days) for AX2Go see *AX2Go settings* [▶ 544].

You have three options to choose from:



☒ Do not change time window on the gateway	The use of this identification medium is not restricted by a time budget. It can be used permanently on authorised locking devices.
☒ until a particular time of (next) day	After activation at the gateway, this identification medium may be utilised to operate authorised locking devices until the designated time (e.g. 12 noon).
☒ Number of hours from the last full hour of the booking	After activation at the gateway, this identification medium may be utilised to operate authorised locking devices until the set number of hours has elapsed.

This setting is customised for each transponder. It is important to select the correct tab "Transponder configuration" setting:



You can also set a dynamic time window (see [Create locking system \[▶ 367\]](#)) within the lock system details. This only applies to newly created identification media (default settings) and does not affect the time window of existing identification media.

If you want to change the time window for existing identification media retrospectively, you need to adjust the settings for each medium individually. It is therefore advisable to set the time budget at the time of installing a locking system ([Best practice: setting up the locking system \[▶ 37\]](#)).

20.3 WaveNet

WaveNet is a wireless network that enables users to remotely access and programme locking devices. The prerequisites for this are RouterNodes and networked locking devices (= equipped with a LockNode).

Configuring WaveNet involves the following steps:

1. [CommNode set up \[▶ 451\]](#)

The CommNode stores information about the network structure, allowing it to recognise how to reach each locking device.

2. First, specify the wireless channel and a password to protect your WaveNet (see [Specify WaveNet channel, address and password \[▶ 463\]](#)).

3. RouterNodes are required to access the locking devices: [Add Router-Nodes \[▶ 465\]](#)

4. The RouterNodes can then be used to search for networked locking devices and add them to the WaveNet.: [Add Lock Nodes \[▶ 468\]](#)

You will subsequently recognise connected locking devices by their AXM Plus entry in the relevant column "N".

Tür	Raumnummer	Etage	Typ	Firmwareversion	N	Sync	Status	Letzte Synchronisierung	S/N	Schließungs-ID
WaveNet-Demohandie				2.6.74	W			25.11.2025 20:44:50	0064301	10000
> WaveNet-Demozylinder				1.1.1147	W			25.11.2025 19:58:35	0841405	128

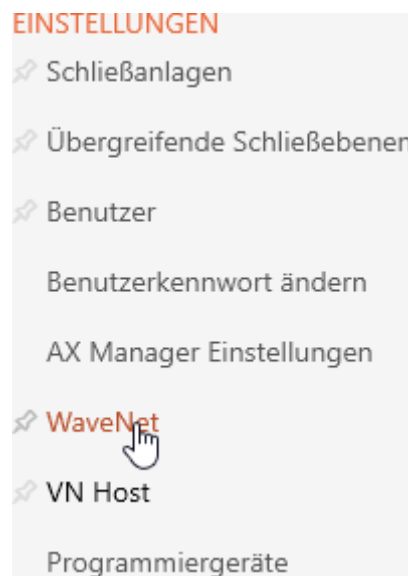
20.3.1 Specify WaveNet channel, address and password

- ✓ AXM Plus is installed (see [Installation \[▶ 27\]](#)).
- ✓ At least one project is available (see [First steps after a new installation \[▶ 35\]](#)).
- ✓ ConfigNode is configured (see [CommNode set up \[▶ 451\]](#)).

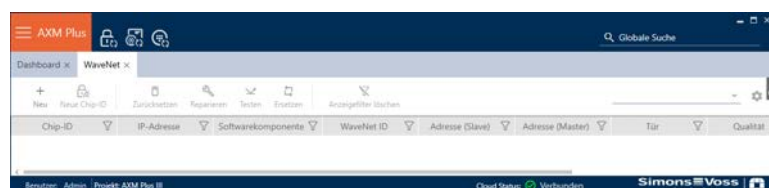
1. Click on the orange AXM icon  AXM.
 ↳ AXM bar opens.



2. Click on the **WaveNet** entry in the | SETTINGS | group.

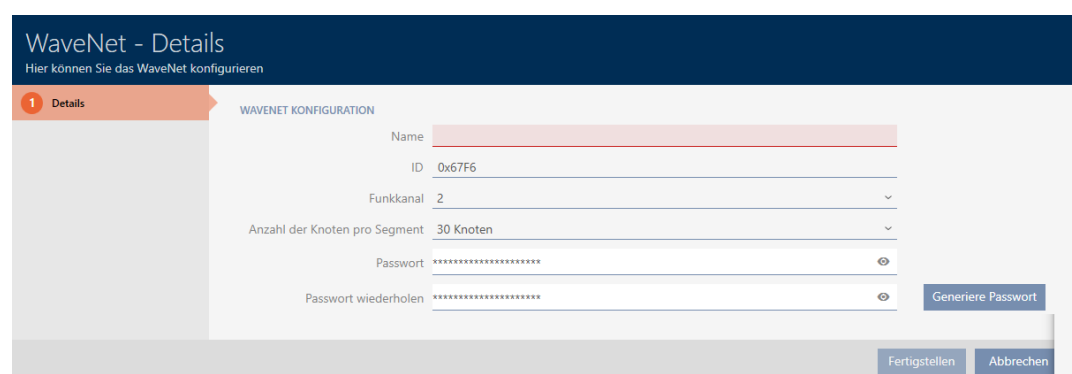


- The AXM bar will close.
- The [WaveNet] tab will open.

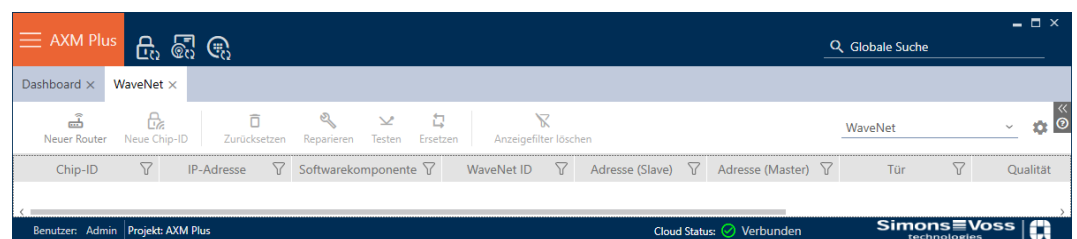


3. Click on the **+** **New** button.

- The "WaveNet - Details" window will open.



4. Enter a name for your WaveNet in the *Name* field.
5. The ID is automatically randomly generated. As necessary, you can also enter your own ID in the field *ID*.
The ID and password make your WaveNet unique and prevent accidental reprogramming.
6. Select the desired channel from the dropdown menu ▼ **Radio channel** (details on channels and frequencies can be found in the WaveNet manual).
7. Select the number of Lock Nodes from the drop-down menu ▼ **Number of nodes per segment** that you want to use per RouterNode.
With 30 nodes per RouterNode, you can use a maximum of 1790 RouterNodes (equivalent to the 11_5-bit mask). With 254 nodes per RouterNode, you can use a maximum of 249 RouterNodes (equivalent to the 8_8-bit mask). For further details on addressing, see the WaveNet manual.
8. Enter a secure password in the *Password* and *Repeat password* fields.
9. Click on the **Finish** button.
↳ Windows Explorer opens, allowing the WaveNet password to be saved as a PDF.
10. Save the PDF with the WaveNet password in a suitable location.
↳ Window "WaveNet - Details" closes.
↳ WaveNet is installed.



- The button **+ New** is not displayed because you have just created the WaveNet.
- The button **New Router** is displayed. Add individual RouterNodes (see [Add RouterNodes](#) [▶ 465]).

20.3.2 Add RouterNodes

You can add the RouterNodes either via the IP address or via the host name.

- First, you must first determine the IP address. Details can be found in the manual of the respective RouterNode. Alternatively, you can find the IP address via a DHCP server if one is available.
- The host name can be found on the back of your RouterNode.

- ❑ You must change the factory password before adding the RouterNode (see the manual of the respective RouterNode).

Further details on the assignment of IP addresses and host names can be found in the WaveNet manual and the respective RouterNode manual.

- ✓ WaveNet is configured (see *Specify WaveNet channel, address and password* [▶ 463]).
- ✓ Tab ▼ **WaveNet** opens.
- ✓ RouterNode is connected to the same network and ready for operation.
- ✓ The factory password of the RouterNode has been changed.

1. Click on the  **New Router** button.
 ↳ The "Search for router" window will open.

2. Please ensure that entry "Software component" is selected in section "CommNode".
3. Enter the IP address or hostname of your RouterNode in field *IP-adresse/Hostname*.



NOTE

Search without specifying IP address/hostname

A search by IP address or host name without further conditions will find all RouterNodes that can be reached in the network. This enables you to simultaneously add multiple RouterNodes.

4. Click the button **Search**.
 ↳ The window displays a list of available RouterNode (column "Unconfigured routers found").

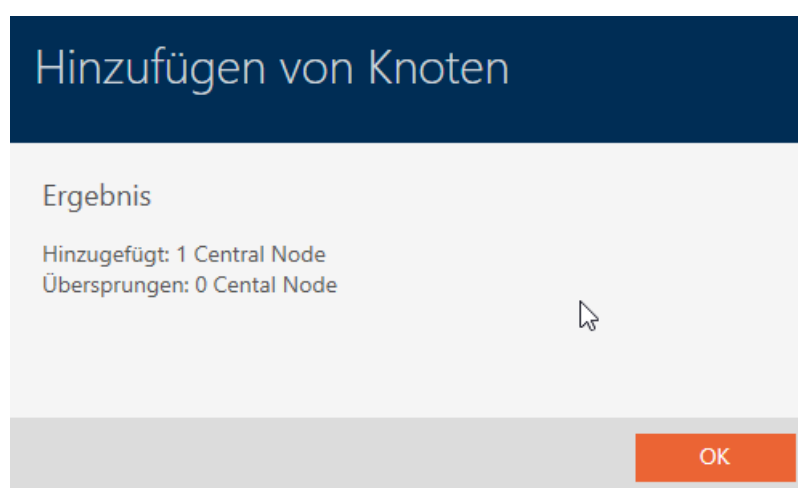
Gefundene unkonfigurierte Router		Gefundene konfigurierte Router					
☐	Name	Produkt	IP-Adresse	MAC Adresse	Softwarekomponent	WaveNet ID	
☐			192.168.1.1		CommNode (Verbunden)	Nicht konfiguriert	

5. Mark the RouterNode you want to add.

Gefundene unkonfigurierte Router		Gefundene konfigurierte Router					
☒	Name	Produkt	IP-Adresse	MAC Adresse	Softwarekomponent	WaveNet ID	
☒			192.168.1.1		CommNode (Verbunden)	Nicht konfiguriert	

6. Click the **Add Selected Routers** button.

→ RouterNodes are added.



7. Click on the **OK** button.

→ Window "Search for router" closes.

→ List of available RouterNode.

Dashboard x		WaveNet x									
Neuer Router	Neuer Chip-ID	Zurücksetzen	Regenerieren	Testen	Ersetzen	Anzeige für Wachen	WaveNet				
Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion	
890018C1A	192.168.1.1	CommNode	0x67F6	0x0006	0x0021				Central Node	40.11.0.0	

With the help of the RouterNode, you may now search for the Lock Nodes in your locking devices (see *Add Lock Nodes* [▶ 468]).

20.3.3 Add Lock Nodes

- ✓ At least one RouterNode has been added to the WaveNet (see *Add RouterNodes* [▶ 465]).
- ✓ RouterNode is connected to the same network and ready for operation.
- ✓ Integrated Lock Nodes (LN.I) must be installed in a locking device in order to be supplied with power.
- ✓ Tab ▼ **WaveNet** opens.

1. Mark the RouterNode with which you want to search for the LockNode.



2. Click on the  **New Chip-ID** button.
 - ➔ The "Search for nodes" window will open.

The screenshot shows the 'Knoten suchen' window. It has a search bar with the text 'Suche nach Chip-IDs in 192.168.1.100' and a 'Suche' button. Below the search bar is a 'Chip-ID' input field and a 'Quick Scan' checkbox which is checked. At the bottom, there are two tabs: 'Gefundene unkonfigurierte Knoten' and 'Gefundene konfigurierte Knoten'. The 'Gefundene konfigurierte Knoten' tab is active, showing a table with columns for Chip-ID, WaveNet ID, Produkt, and Qualität. At the bottom right, there are buttons for 'Gefundene Knoten hinzufügen' and 'Abbrechen'.

3. Enter the chip ID of the Lock Nodes to be added in the field *Chip-ID*.
The chip ID can be found on the LockNode itself or on the stickers supplied with it.



NOTE

Search without specifying chip ID

Searching for a chip ID without further conditions will find all the Lock Nodes that the RouterNode can access. Thus, multiple Lock Nodes can be added simultaneously.

4. Click the button **Search**.
 - ➔ Search for LockNode in progress.

Knoten suchen

Suche nach Chip-IDs in 192.168.1.1

Suche

Chip-ID 5D

Quick Scan ☒

Gefundene unkonfigurierte Knoten

Gefundene konfigurierte Knoten

Chip-ID	WaveNet ID	Produkt	Qualität

Gefundene Knoten hinzufügen

Abbrechen

→ Detected LockNode displayed.

Gefundene unkonfigurierte Knoten

Gefundene konfigurierte Knoten

Chip-ID	WaveNet ID	Produkt	Qualität
☐ 000		LockNode	-34 dB

5. Mark the LockNode you want to add.

Gefundene unkonfigurierte Knoten

Gefundene konfigurierte Knoten

Chip-ID	WaveNet ID	Produkt	Qualität
☒ 0005		LockNode	-35 dB

6. Click the **Add Selected Nodes** button.

→ LockNode is added.

Hinzufügen von Knoten

Bitte warten

Stop



- Click on the **OK** button.
 - Window "Search for nodes" closes.
 - LockNode displayed in the list.

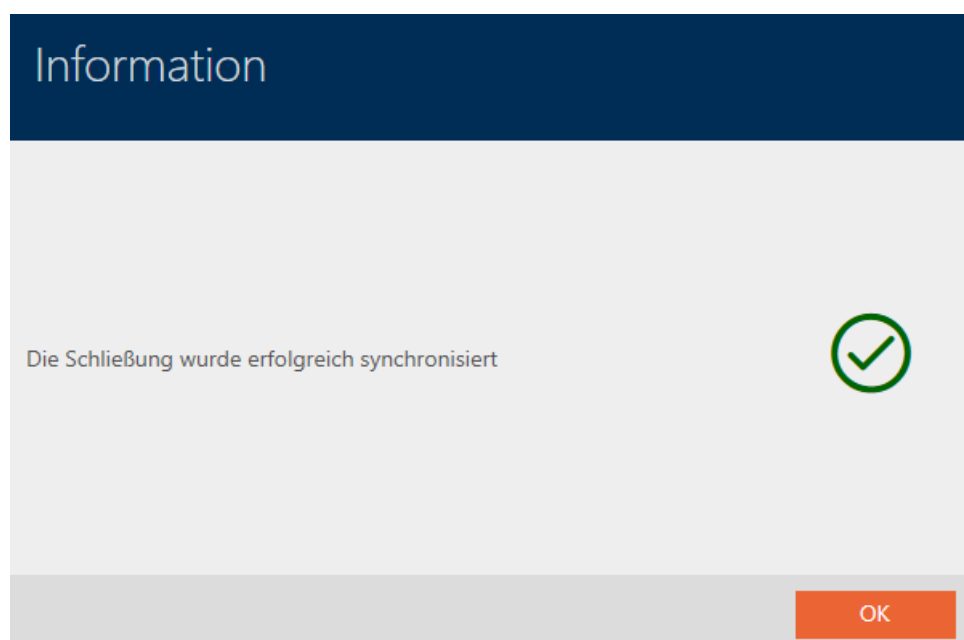
Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tur	Qualität	Zustand	Typ	Firmwareversion
B90036#	192.168.178.19	CommNode	0x67f6	0x0006	0x0021				Central Node	40.11.0.0
0005'x018			0x67f6	0x0026		WaveNet-Demozyklus	-35 dB		LockNode	33.7.17.7

LockNode in unprogrammed locking device

The column does not contain entries for Lock Nodes whose locking devices have not yet been synchronised *Door*.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
090008A1	192.168.1.30/28	CommNode	0x67F6	0x0006	0x0021				CentralNode	40.11.0.0
00020A78			0x67F6	0x0027			-35 dB		LockNode	32.15.16.3

In this case, it is necessary to synchronise the locking device so that AXM can "recognise" and display it. (see *Synchronising the locking device (including reading access list)* [► 417]).



After synchronising, the locking device is displayed together with the LockNode:

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
890068C4	192.168.100.29	CommNode	0x6776	0x0006	0x0021				Central Node	40.11.0.0
0002AA79			0x6776	0x0027		WaveNet-Demohandie	-35 dB		LockNode	32.15.16.3

20.3.3.1 Adding Lock Nodes to unprogrammed locking devices

20.3.4 Repair RouterNode or LockNode

With the function  **Repair**, you can fix errors in the configuration of the WaveNet components.

✓ Tab **WaveNet** opens.

1. Mark the RouterNode or LockNode that you want to repair.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
890068C4	192.168.100.29	CommNode	0x6776	0x0006	0x0021				Central Node	40.11.0.0
0002AA79			0x6776	0x0027		WaveNet-Demohandie	-37 dB		LockNode	32.15.16.3
0005...			0x6776	0x0026		WaveNet-Demohandie	-51 dB		LockNode	33.7.17.0

2. Click on the  **Repair** button.

→ The "Repair node" window will open.



3. Click the **Yes** button.

→ RouterNode or LockNode repaired.



→ RouterNode or LockNode repaired.



If repair is not possible, you can replace the component:

- RouterNodes: *Replace RouterNode or change IP address* [▶ 472]
- Lock Nodes: *Reset (remove) RouterNode or LockNode* [▶ 476] and *Add Lock Nodes* [▶ 468] (Lock Nodes are not directly replaceable)

20.3.5 Replace RouterNode or change IP address

If a RouterNode cannot be repaired (see *Repair RouterNode or LockNode* [▶ 471]), you can replace a RouterNode with a new one. Possible reasons for replacement:

- Replacement with newer model
- Substitute
- Theft
- Defects

Alternatively, you may also use the function if the IP address of the RouterNode has changed but the same RouterNode continues to be utilised.



NOTE

Replace not available for Lock Nodes

Lock Nodes cannot be replaced in the AXM Plus.

1. Remove affected Lock Nodes (see *Reset (remove) RouterNode or LockNode* [▶ 476]).
2. Subsequently, add the new LockNode (see *Add Lock Nodes* [▶ 468]).

- ✓ The substitute RouterNode is ready for operation and connected to the same network.
- ✓ Tab ▼ **WaveNet** opens.

1. Mark the RouterNode you wish to delete.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
890000000000	192.168.1.100	CommNode	0x67F6	0x0006	0x0021				Central Node	40.11.0.0
0002A0000000			0x67F6	0x0027		WaveNet-Demohandlie	-36 dB		LockNode	32.15.16.3
000500000000			0x67F6	0x0026		WaveNet-Demozyklinder	-51 dB		LockNode	33.7.17.0

2. Click on the  **Replace** button.
 ↳ The "Replace Router" window will open.

Router ersetzen

Neue IP-Adresse

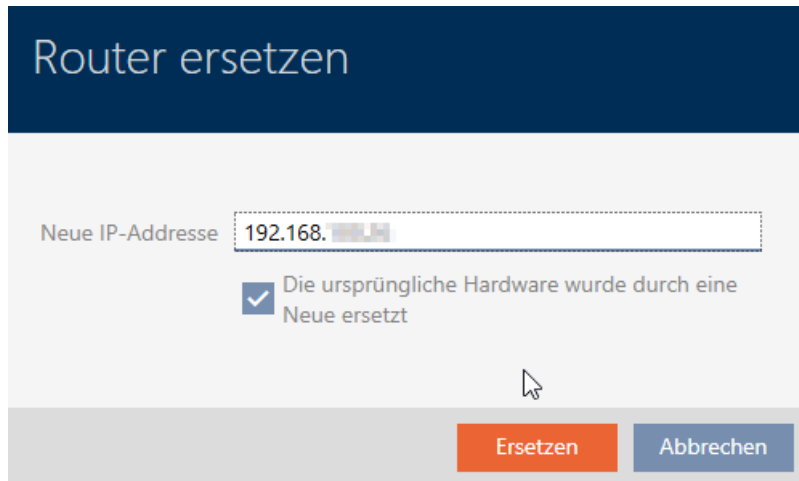
☐ Die ursprüngliche Hardware wurde durch eine Neue ersetzt

Ersetzen

Abbrechen

3. Enter the IP address of the substitute RouterNode in the field *New IP Address*.

4. If you replace the RouterNode with a new RouterNode, then activate the checkbox ☒ The original hardware was replaced with the new one. If the same RouterNode is reused and only the IP address has changed, then deactivate the checkbox ☐ The original hardware was replaced with the new one.



The screenshot shows a dialog box titled "Router ersetzen" (Replace Router). It has a dark blue header bar with the title in white. Below the header, there is a light gray area containing a text input field labeled "Neue IP-Adresse" (New IP address) with the value "192.168.1.1" and a small icon of a router. Below the input field, there is a checkbox labeled "Die ursprüngliche Hardware wurde durch eine Neue ersetzt" (The original hardware was replaced by a new one), which is currently checked. At the bottom of the dialog, there are two buttons: "Ersetzen" (Replace) in an orange box and "Abbrechen" (Cancel) in a blue box. A mouse cursor is pointing at the "Ersetzen" button.

5. Click the **Replace** button.
↳ RouterNode is replaced.



The screenshot shows the same "Router ersetzen" dialog box, but now it is in a waiting state. The central area of the dialog is white and contains a dark blue box with the text "Bitte warten" (Please wait) and a progress bar below it. The progress bar is partially filled with a dark blue bar. At the bottom right of the dialog, there is a single button labeled "OK" in a blue box. A mouse cursor is pointing at the "OK" button.



→ The substitute RouterNode is listed instead of the original RouterNode.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
E1 8900	192.168.1.10	CommNode	0x67f6	0x0006	0x0021				Central Node	40.11.0.0
0002A4			0x67f6	0x0027		WaveNet-Demohandie	-36 dB		LockNode	32.15.16.3
0005D0			0x67f6	0x0026		WaveNet-Demozylinder	-51 dB		LockNode	33.7.17.0

20.3.6 Test RouterNode or LockNode

You can use the function **Test** to test if your WaveNet components are accessible and functioning.

✓ Tab **WaveNet** opens.

1. Mark the RouterNode or LockNode that you want to test.

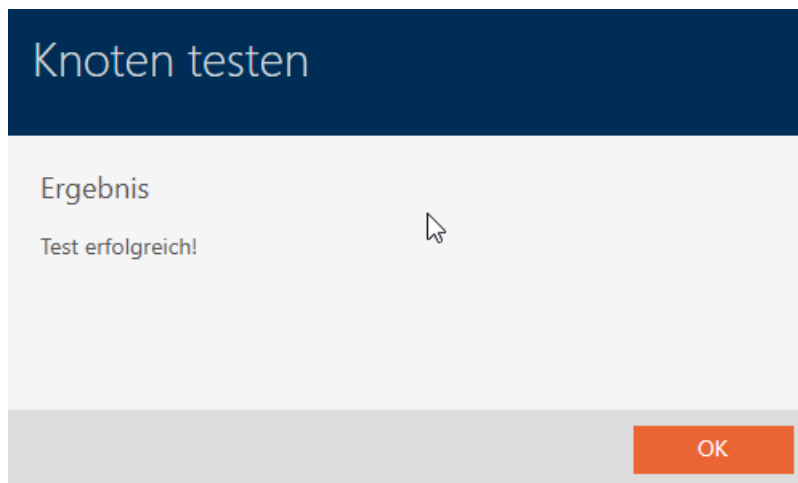
Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
E1 8900	192.168.1.10	CommNode	0x67f6	0x0006	0x0021				Central Node	40.11.0.0
0002A4			0x67f6	0x0027		WaveNet-Demohandie	-37 dB		LockNode	32.15.16.3
0005D0			0x67f6	0x0026		WaveNet-Demozylinder	-51 dB		LockNode	33.7.17.0

2. Click on the **Test** button.

→ RouterNode or LockNode is tested.



→ RouterNode or LockNode has been tested and the test result is displayed.



If the test is not successful, you can try to repair the RouterNode or LockNode (see [Repair RouterNode or LockNode](#) [▶ 471]).

20.3.7 Reset (remove) RouterNode or LockNode



NOTE

Reset Lock Nodes before Router Nodes

Lock Nodes can only be accessed via the associated RouterNode. Therefore, you may only reset a RouterNode when no LockNode is assigned to that RouterNode.

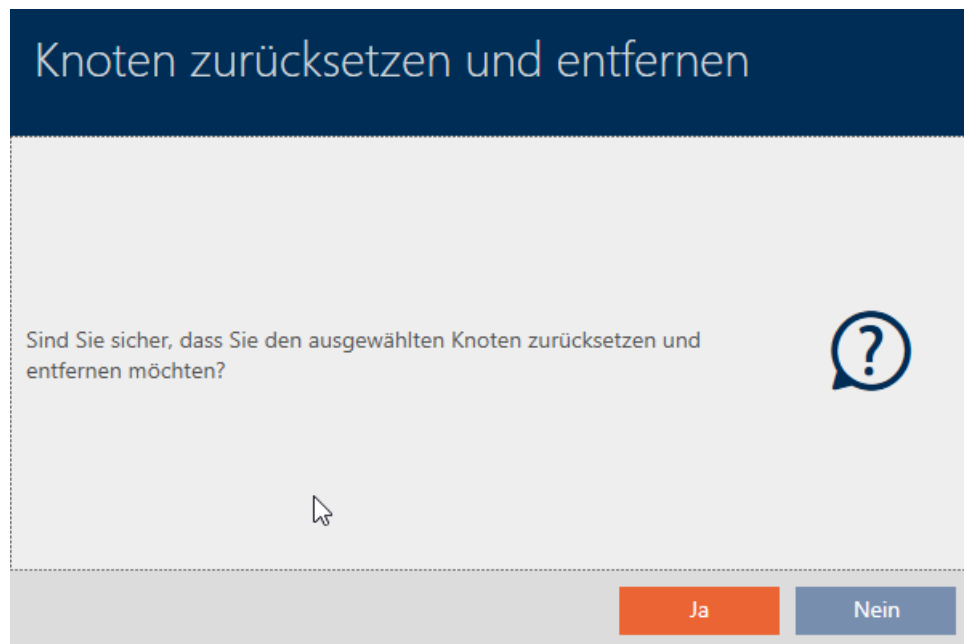
1. First reset all Lock Nodes that belong to a RouterNode.
2. Then reset the RouterNode.

✓ Tab ▼ **WaveNet** opens.

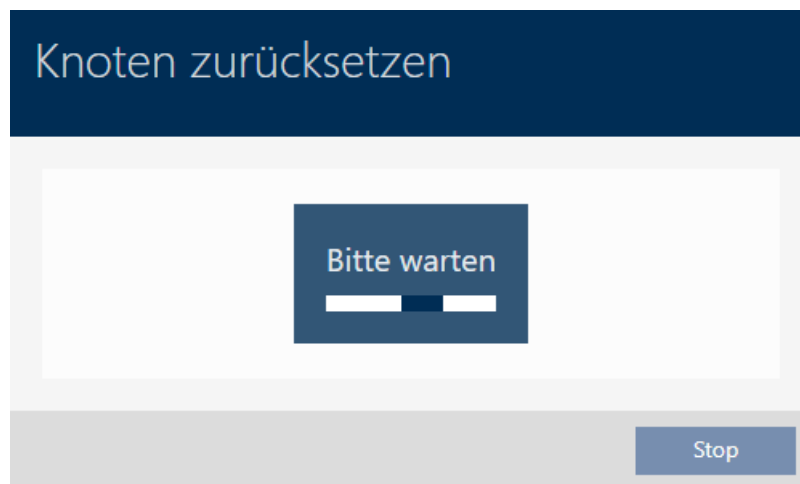
1. Mark the RouterNode or LockNode that you want to reset.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
890018C	192.168.1.1	CommNode	0x67F6	0x0006	0x0021				Central Node	40.11.0.0
0002AA7F			0x67F6	0x0027		WaveNet-Demoschleife	-35 dB		LockNode	32.15.16.3
0005C488			0x67F6	0x0026		WaveNet-Demoschleife	-54 dB		LockNode	33.7.17.0

2. Click on the  **Reset** button.
 ↳ The "Reset and remove nodes" window will open.



3. Click on the **Yes** button.
↳ RouterNode or LockNode is reset.



- ↳ RouterNode or LockNode is no longer listed.

Chip-ID	IP-Adresse	Softwarekomponente	WaveNet ID	Adresse (Slave)	Adresse (Master)	Tür	Qualität	Zustand	Typ	Firmwareversion
890018C4	192.168.1.100	CommNode	0x67F6	0x0006	0x0021	WaveNet-Demozylinder	-54 dB		Central Node	40.11.0.0
0005100E			0x67F6	0x0026					LockNode	33.7.17.0

Reset Lock Nodes whose RouterNode is no longer available

Normally, you first reset all Lock Nodes before resetting the RouterNode. In some cases, however, it can happen that the RouterNode is no longer available due to a defect and a LockNode has only been removed but not reset. The LockNode can then no longer be reached.

In this case, you can still reset the LockNode by installing it in a programmed locking device of another locking system. The locking device then beeps/ flashes four times and the LockNode is reset.

20.3.8 Execute tasks via WaveNet on multiple locking devices (collective orders)

With the Sync Network Locks function, you may perform a task sequentially on several networked locking devices. It is no longer necessary to start the task for each locking device.

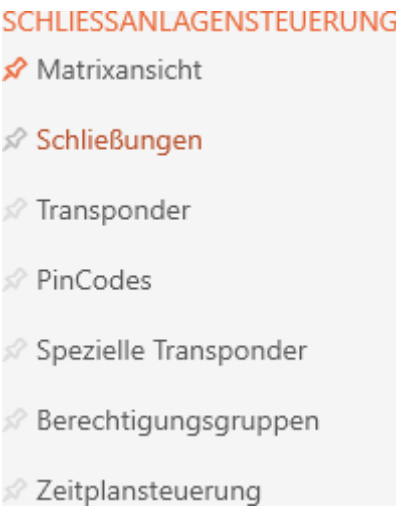
In the example, the access list should be read at two networked locking devices:

- ✓ At least one locking device created (see *Creating a locking device* [▶ 245]).
- ✓ Locking device networked (see *Add Lock Nodes* [▶ 468]).

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



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



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

A screenshot of the 'Schließungen' (Locks) tab in the software interface. The interface shows a table with columns: Tür, Raumnummer, Etage, Typ, Firmwareversion, N, Sync, Status, and Le. The table contains several rows of lock data. The first row is highlighted in orange. The table data is as follows:

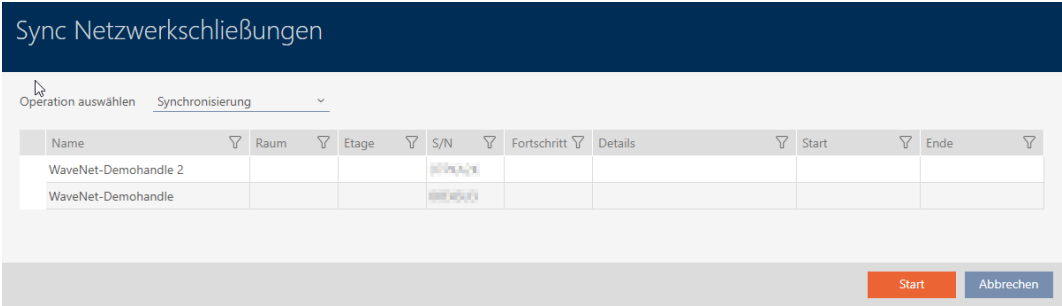
Tür	Raumnummer	Etage	Typ	Firmwareversion	N	Sync	Status	Le
Aufenthaltsbereich		OG	🔒			🔄		
Besuchereingang		EG	🔒			🔄		
Garage		UG	🔒			🔄		
Haupteingang		EG	🔒			🔄		
Nebeneingang		EG	🔒			🔄		
Notausgang		EG	🔒			🔄		
Parkplatz		EG	🔒			🔄		
Südausgang		OG	🔒			🔄		
Warenausgang		EG	🔒			🔄		
WaveNet-Demohandle			🔑	2.6.74	W			25
WaveNet-Demohandle 2			🔑	1.1.304	W			20
WaveNet-Demozylinder			🔑	1.1.1147	W		⚠️	20

3. Mark the locking devices on which you want to perform the task.

A screenshot of the 'Schließungen' (Locks) tab in the software interface, showing the same table as before. In this screenshot, the rows for 'WaveNet-Demohandle' and 'WaveNet-Demohandle 2' are highlighted in orange, indicating they are selected. The table data is as follows:

Tür	Raumnummer	Etage	Typ	Firmwareversion	N	Sync	Status	Le
Aufenthaltsbereich		OG	🔒			🔄		
Besuchereingang		EG	🔒			🔄		
Garage		UG	🔒			🔄		
Haupteingang		EG	🔒			🔄		
Nebeneingang		EG	🔒			🔄		
Notausgang		EG	🔒			🔄		
Parkplatz		EG	🔒			🔄		
Südausgang		OG	🔒			🔄		
Warenausgang		EG	🔒			🔄		
WaveNet-Demohandle			🔑	2.6.74	W			25
WaveNet-Demohandle 2			🔑	1.1.304	W			20
WaveNet-Demozylinder			🔑	1.1.1147	W		⚠️	20

4. Click on the **Sync Network Locks** button.
→ The "Sync Network Locks" window will open.



5. Select the task you wish to perform from the drop-down menu ▼ **Select operation** (example: Read audit trail).

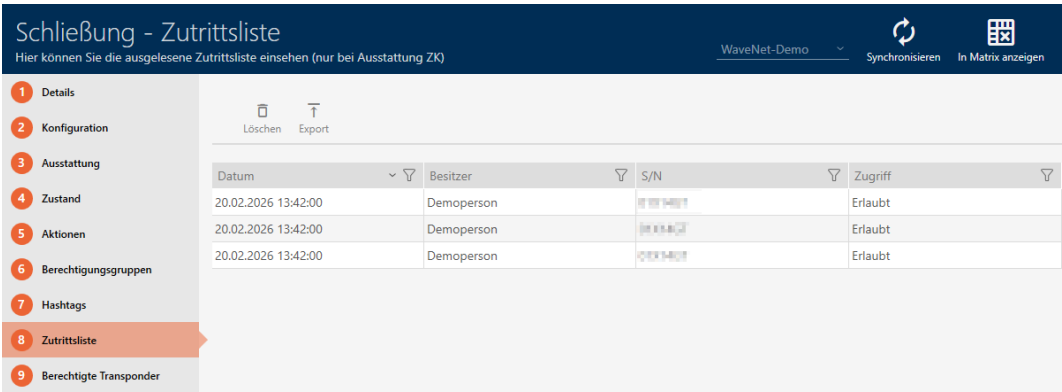
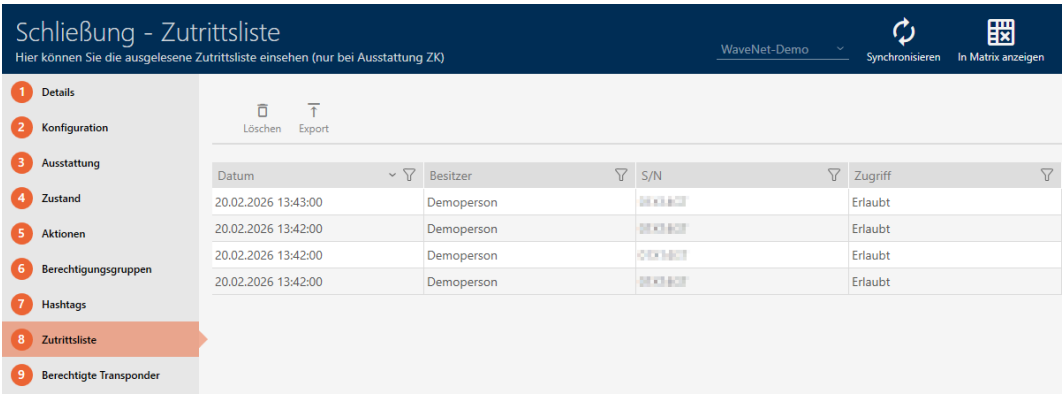


6. Click the **Start** button.
→ Your AXM Plus completes the tasks consecutively.

Name	Raum	Etage	S/N	Fortschritt	Details	Start	Ende
WaveNet-Demohandle 2					Erledigt	20.02.2026 13:53:16	20.02.2026 13:53:36
WaveNet-Demohandle					Zutrittsliste wird ausgelesen	20.02.2026 13:53:36	

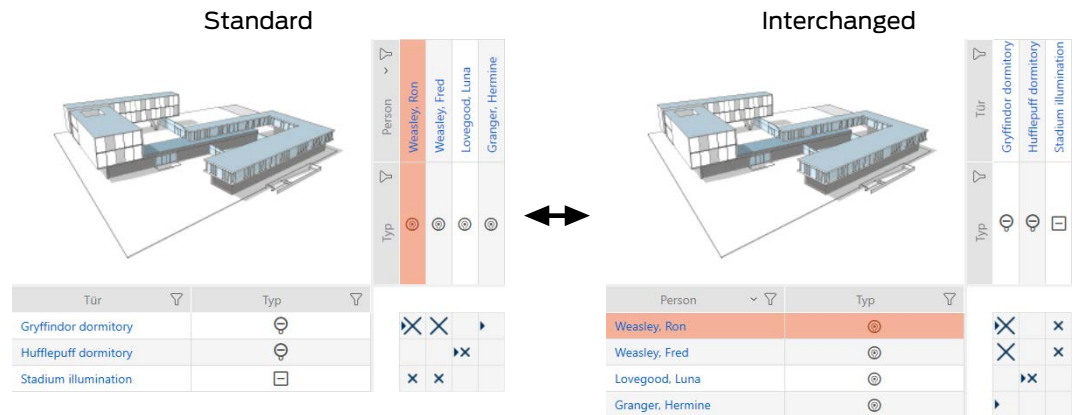
→ All tasks completed (example: access lists for both locking devices have been read).

Name	Raum	Etage	S/N	Fortschritt	Details	Start	Ende
WaveNet-Demohandle 2					Erledigt	20.02.2026 13:53:16	20.02.2026 13:53:36
WaveNet-Demohandle					Erledigt	20.02.2026 13:53:36	20.02.2026 13:53:45



21. Your personalised AXM interface

21.1 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.

Matrizeinstellungen

Hier können Sie die Matrix konfigurieren

Tausche Plätze von Transpondern und Schließungen ☐

Zeige Fadenkreuz ☒

Vergeben der Berechtigungen Einfacher Mausklick

Zeige deaktivierte Transponder ☒

Verfügbare Schließungsspalten:

Raumnummer

Hinzufügen

Verfügbare Transponderspalten:

Typ (Text)

Hinzufügen

Angezeigte Schließungsdaten inkl. Reihenfolge:

Tür

Typ (Symbol)

Sync

Löschen

Nach oben

Nach unten

Zurücksetzen

Angezeigte Transponderdaten inkl. Reihenfolge:

Person

Typ (Symbol)

Sync

Löschen

Nach oben

Nach unten

Zurücksetzen

OK

Abbrechen

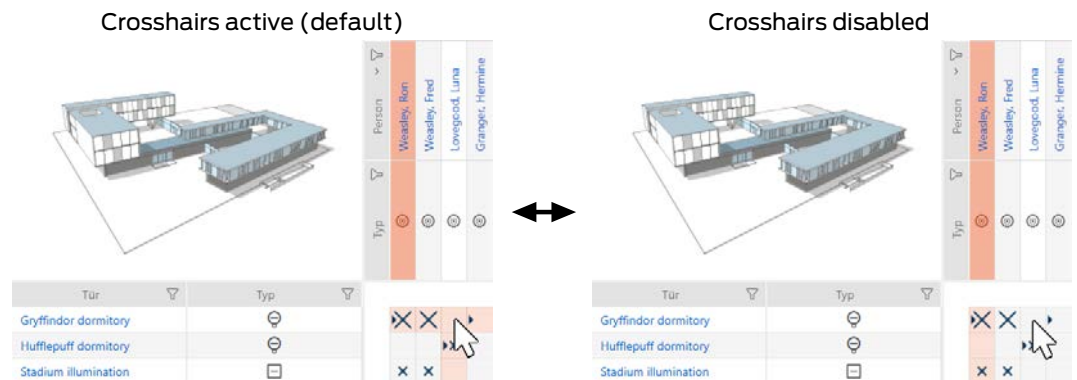
2. Activate the ☒ Swap places for transponders and locks check box.

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

→ The window with the AXM Plus matrix settings closes.

→ Doors and persons are swapped in the matrix view.

21.2 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.

Matrizeinstellungen

Hier können Sie die Matrix konfigurieren

Tausche Plätze von Transpondern und Schließungen
☐

Zeige Fadenkreuz
☒

Vergeben der Berechtigungen
Einfacher Mausklick

Zeige deaktivierte Transponder
☒

Verfügbare Schließungsspalten:

Raumnummer

Hinzufügen

Angezeigte Schließungsdaten inkl. Reihenfolge:

Tür
Typ (Symbol)
Sync

Löschen
Nach oben
Nach unten
Zurücksetzen

Verfügbare Transponderspalten:

Typ (Text)

Hinzufügen

Angezeigte Transponderdaten inkl. Reihenfolge:

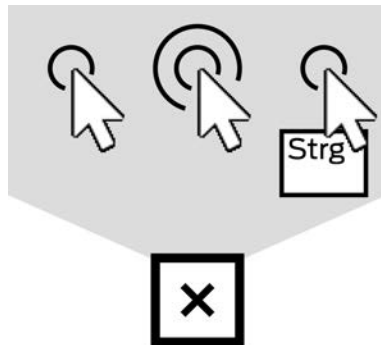
Person
Typ (Symbol)
Sync

Löschen
Nach oben
Nach unten
Zurücksetzen

OK
Abbrechen

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.

21.3 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.

Matrizeinstellungen

Hier können Sie die Matrix konfigurieren

Tausche Plätze von Transpondern und Schließungen ☐

Zeige Fadenkreuz ☒

Vergeben der Berechtigungen Einfacher Mausklick

Zeige deaktivierte Transponder ☒

Verfügbare Schließungsspalten:

Raumnummer

Hinzufügen

Angezeigte Schließungsdaten inkl. Reihenfolge:

Tür
Typ (Symbol)
Sync

Löschen

Nach oben

Nach unten

Zurücksetzen

Verfügbare Transponderspalten:

Typ (Text)

Hinzufügen

Angezeigte Transponderdaten inkl. Reihenfolge:

Person
Typ (Symbol)
Sync

Löschen

Nach oben

Nach unten

Zurücksetzen

OK Abbrechen

- Choose between the "Single click of the mouse", "Double click" or "Ctrl + single click" entries from the ▼ Issuing of authorisations drop-down menu.

Vergeben der Berechtigungen Einfacher Mausklick

Einfacher Mausklick

Doppelklick

Strg + einfacher Mausklick

- Click on the **OK** button.
 - The window with the AXM Plus matrix settings closes.
 - Click for authorisations has been changed.

21.4 Hiding deactivated and defective identification media

Sync	Typ	Person
	Standard Personengruppe	
	Lupin, Remus	
	Snape, Severus	
	Weasley, Ron	
	Wood, Oliver	

➔

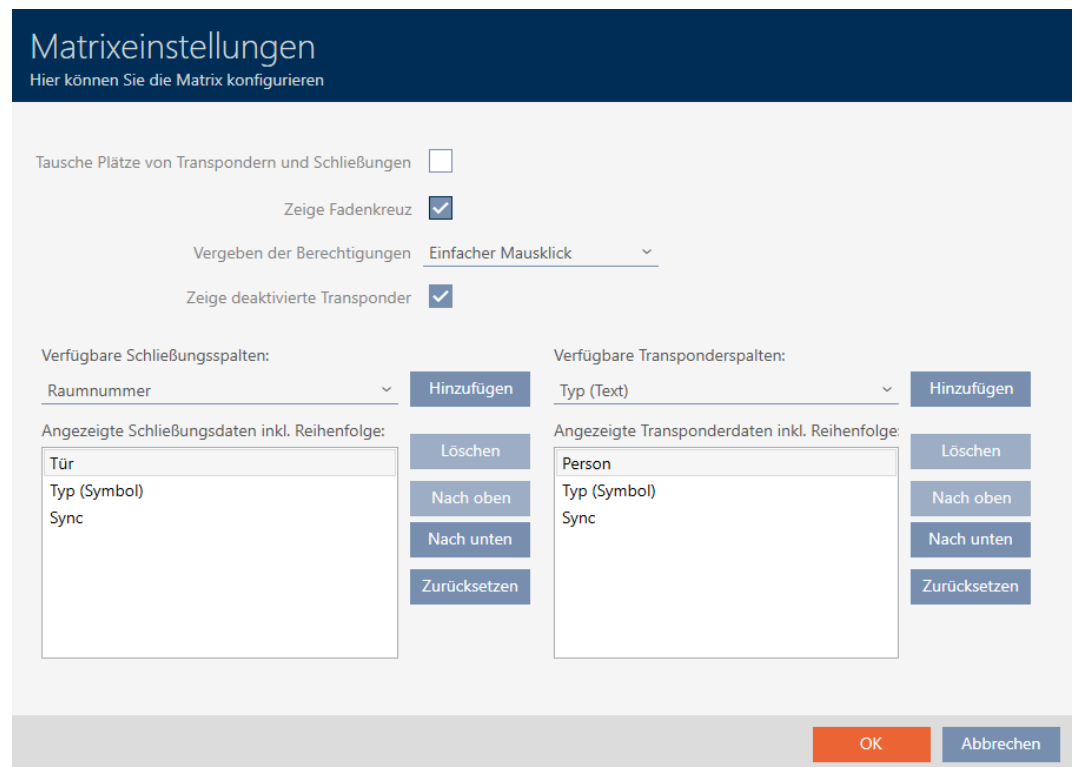
Sync	Typ	Person
	Standard Personengruppe	
	Lupin, Remus	
	Snape, Severus	
	Weasley, Ron	

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.

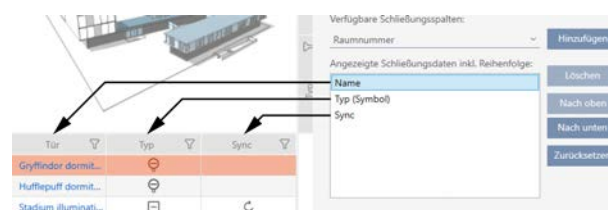
3. Click on the **OK** button.

➔ The window with the AXM Plus matrix settings closes.

➔ Deactivated and defective identification media are now hidden.

21.5 Showing or hiding rows/columns in the matrix

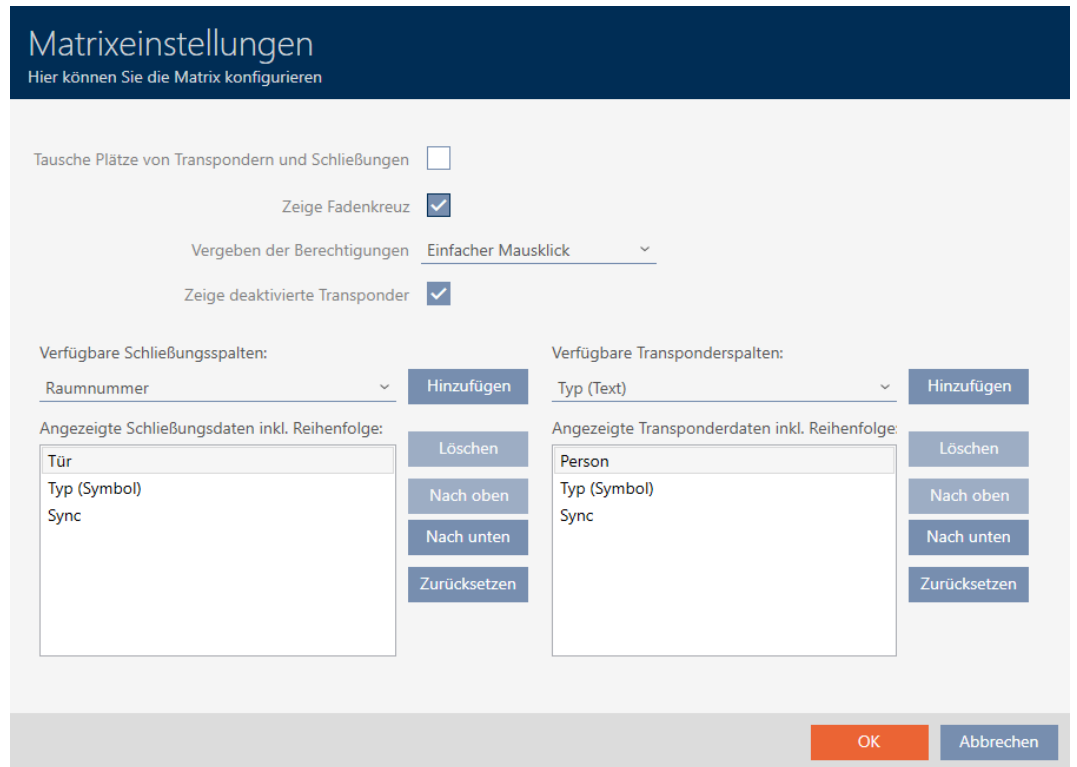
The following description applies to the columns displayed for locking devices. The identification media rows can be edited in the same way.



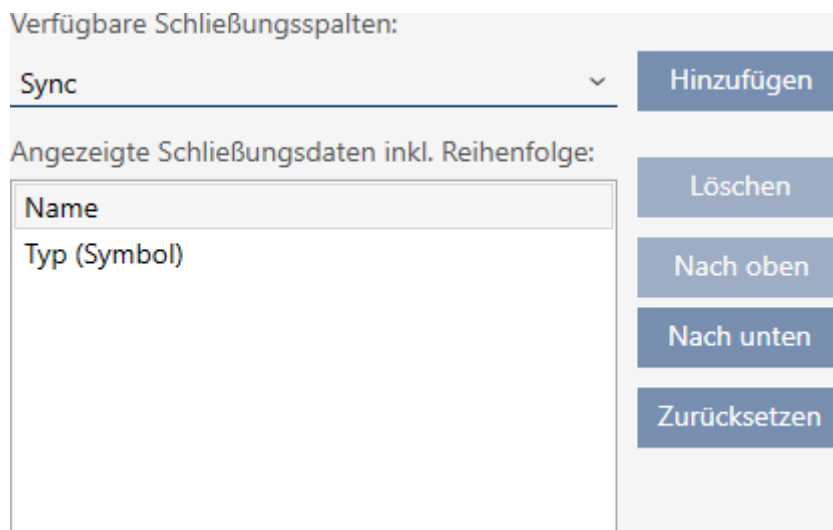
✓ Matrix screen open.

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.

Verfügbare Schließungsspalten:

Sync	Hinzufügen
Sync	Löschen
Raumnummer	Nach oben
Etage	Nach unten
Typ (Text)	Zurücksetzen
S/N	
Status	

3. Add and delete columns with the Add or Delete buttons.

Verfügbare Schließungsspalten:

Raumnummer	Hinzufügen
------------	------------

Angezeigte Schließungsdaten inkl. Reihenfolge:

Name	Löschen
Typ (Symbol)	Nach oben
Sync	Nach unten
	Zurücksetzen

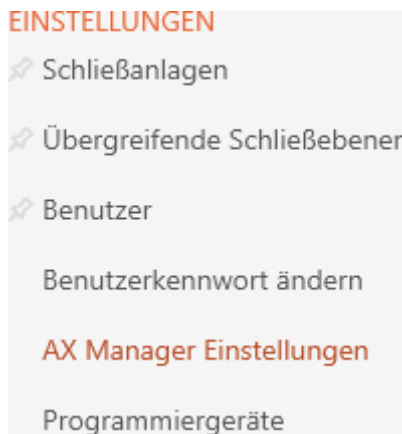
4. Use the Up or Down buttons to change the order.
5. You can also use the Reset button to restore the default display.
6. Click on the OK button.
 - The window with the AXM Plus matrix settings closes.
 - Columns are changed as required.

21.6 Reading access list/physical access list during synchronisation

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

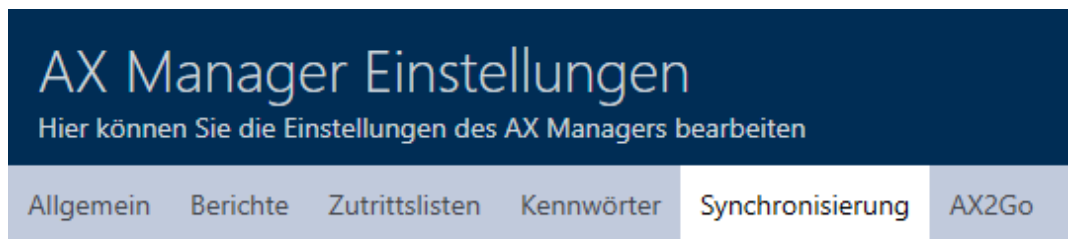


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- 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 ☐

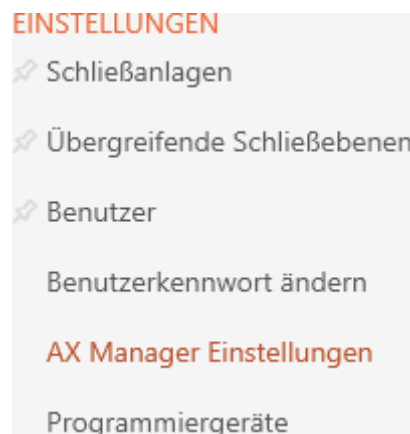
4. Activate the ☒ Reading the audit trail during synchronisation of a lock or ☒ Reading the personal audit trail during transponder synchronisation checkboxes if required.
5. Click on the **OK** button.
 - The window with the AXM Plus settings closes.
 - The access list or physical access list will also be imported during synchronisation in the future.

21.7 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 [Audit trails] tab.



4. Select one of the three options: ☒ Unlimited, ☐ temporally (max. 2000 days) or ☐ by number (max. 10,000 entries).

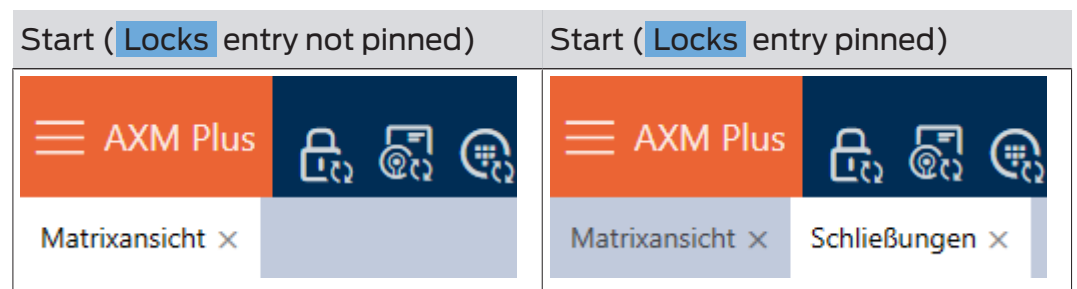
5. Click on the **OK** button.
 - ↳ The window with the AXM Plus settings closes.
 - ↳ Access list restriction is configured.

21.8 Pinning tabs

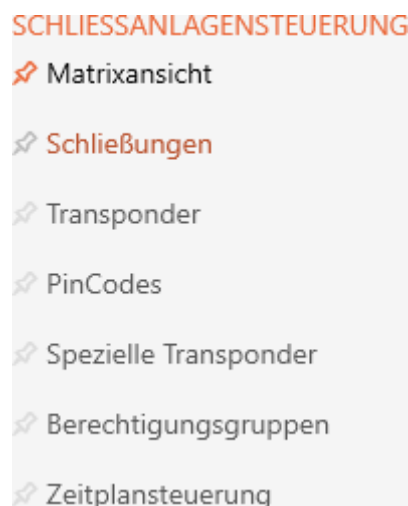
Experience has shown that you need some entries from the AXM bar more frequently.



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.

SCHLIESSANLAGENSTEUERUNG

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

→ The pinned entry is automatically opened the next time the AXM Plus is started.

21.9 Changing automatic numbering

AXM Plus takes over the numbering of personnel and doors for you by default.

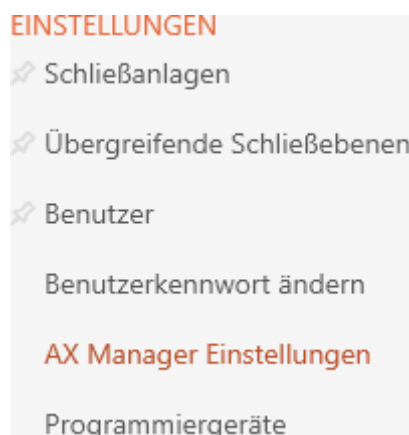
Personnel numbers	Door numbers
PERSONENDETAILS Nachname Weasley Vorname Ron Personalnummer PN-1	TÜRDETAILS Name Gryffindor dormitory Tür-Code DC-00001
PN-1	DC-00001
PN-2	DC-00002
PN-X	DC-XXXXX

The abbreviations *PN*- (personnel number) and *DC*- (door code) can be changed in the AXM Plus properties:

- 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.

21.10 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:

ANMELDEN AM PROJEKT

Benutzername	Admin
Kennwort	
	 Deutsch
<button>Anmelden und Öffnen</button>	

Select your preferred language in the *Password* field.

ANMELDEN AM PROJEKT

Benutzername	Admin
Kennwort	
	 Deutsch
	 Deutsch  English  Français  Italiano  Dutch  Belg  Dansk  Svenska

21.11 Personalising reports and exports

AXM Plus allows you to personalise your reports and exports:

-  Logo for header

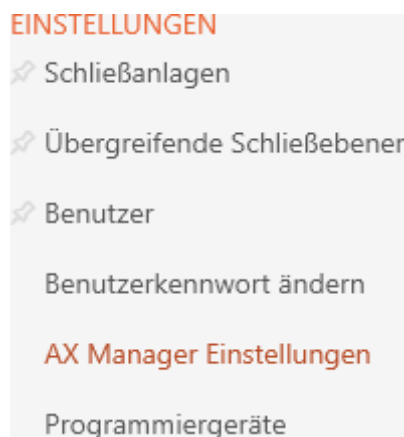
- Permitted formats: .bmp, .jpg, .png
- Automatic scaling (frame format: 25:10.5; also see *Scaling image files* [▶ 623])
- Information for the header
 - Company
 - Street
 - Town/city, postcode
 - Telephone
 - Email
 - Contact
- Logo for footer (frame format: 3:1; also see *Scaling image files* [▶ 623])
 - 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.

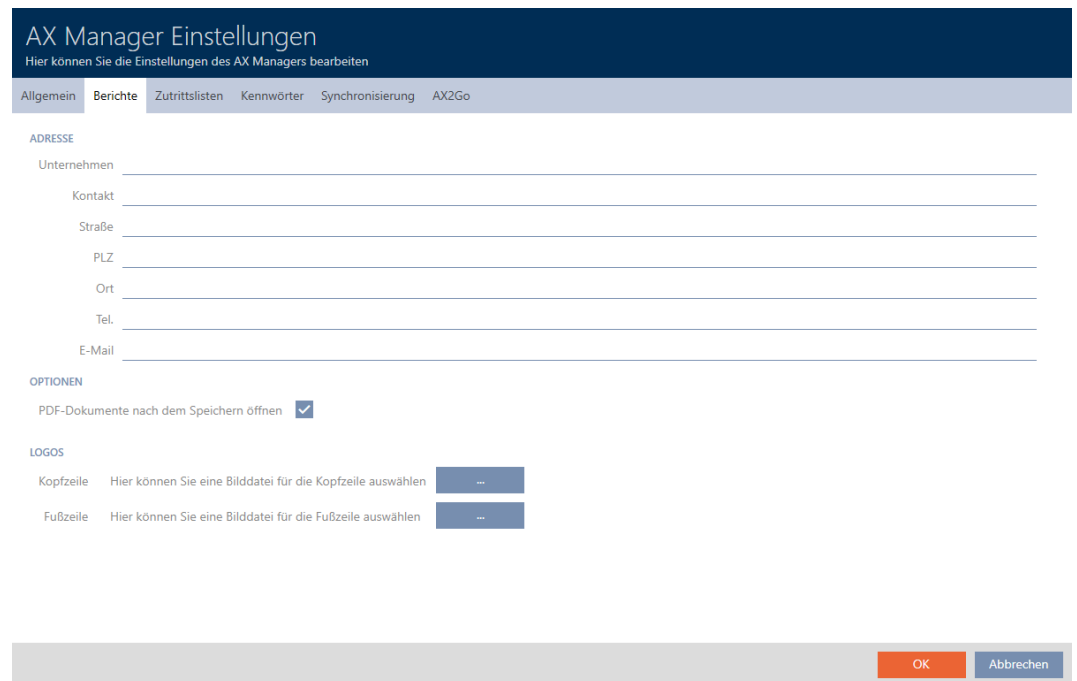


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ 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.

SimonsVoss Technologies GmbH
Feringastrasse 4
85774 Unterföhring
Tel.: 089 99 228 333
E-Mail: support-simonsvoss@allegion.com
Kontakt: Support

SimonsVoss
technologies

CS/IT/IT-Bericht

Ausdruck vom: 04 Januar 2022 14:59

1/2

SimonsVoss
technologies

21.12 Preventing generated reports from opening automatically

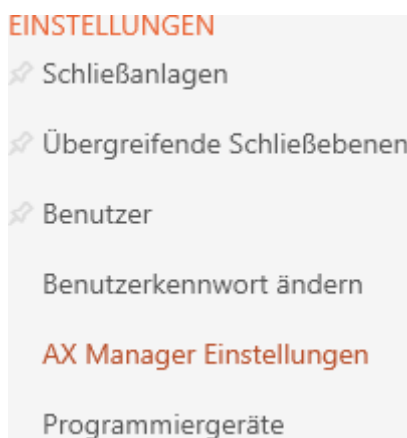
By default, your reports created in AXM Plus open immediately so that you can read them.

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.

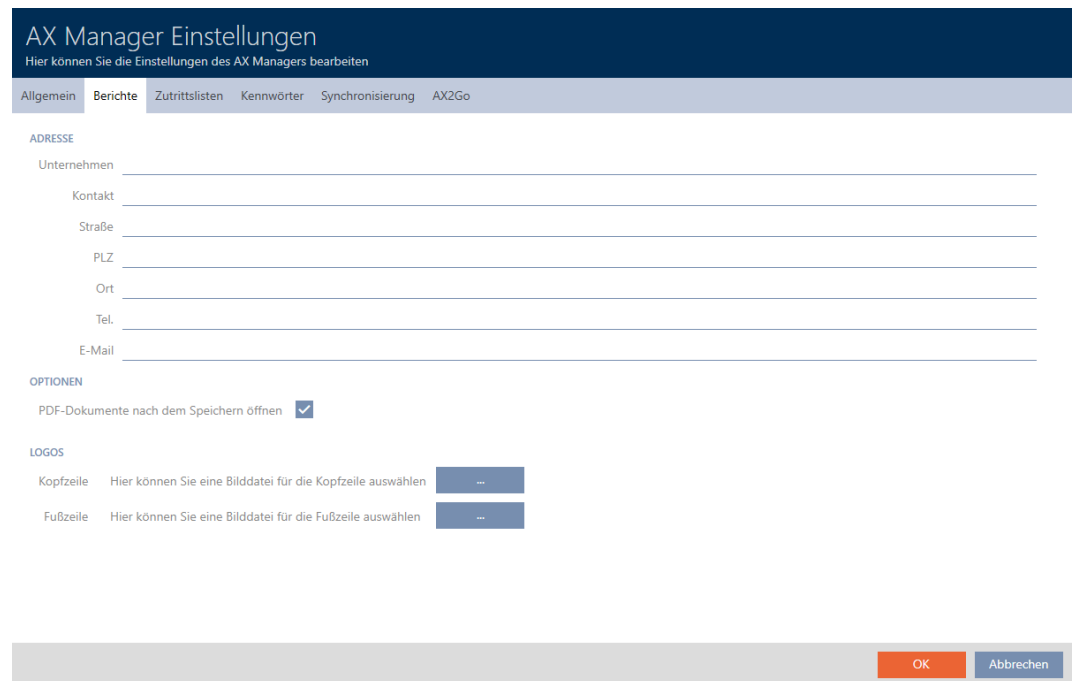


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ➔ The AXM bar will close.
- ➔ The "AX Manager settings" window will open.

3. Change to the tab [Reports].



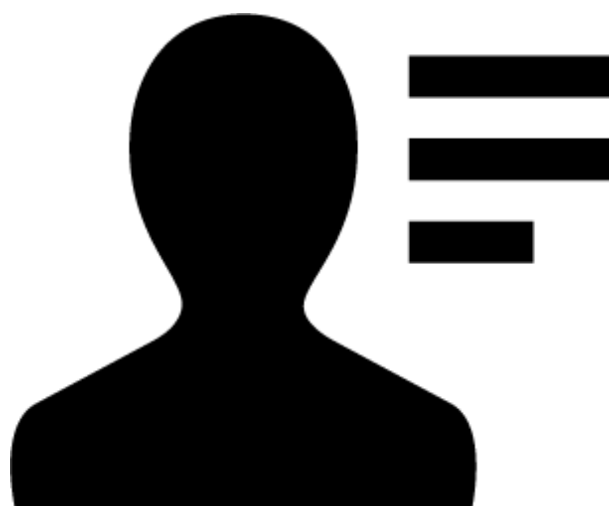
4. Disable the ☐ Open PDF documents after saving checkbox.

5. Click on the button.

↳ "AX Manager settings" window closes.

↳ In future, reports will now no longer open automatically after saving.

21.13 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](#) [► 498]).
In the example, you hide the default *Title* field.
- Create your own properties (see [Creating your own fields](#) [► 503]).
In the example, you create an own field called office number.



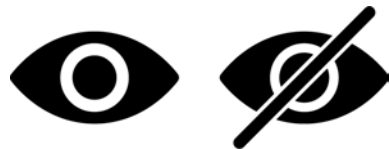
NOTE

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.

21.13.1 Hide and show existing fields



AXM Plus contains the following fields by default:

Person details

☒ Titel	☒ Eingestellt bis	☒ Abteilung
☒ Adresse	☒ Geburtstag	☒ E-Mail
☒ Ort/Gebäude	☒ Kostenstelle	☒ Telefon
☒ Eingestellt am	☒ Foto	

You can hide the following fields and unhide them again:

- Title
- Address
- Location/Building
- Hiring date
- Exit 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)* [► 564]), 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* [► 124]).

✓ Identification medium available.

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



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

SCHLIESSANLAGENSTEUERUNG

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

→ The AXM bar will close.

→ The window with identification media opens.

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				Zeitgruppe	
> Weasley	Ron	00XTN6K					
Wood	Oliver	UID-148024BA5A7369					

- Click on any non-blocked/deactivated identification medium.
 - The identification medium window will open.

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

n/a

Transpondertyp

⊗ Transponder

Firmware Version

Letzte Synchronisierung

10.05.2024 06:05:02

Sync

Erstprogrammierung

Batteriestatus

Zeitgruppe

☐ Zeitgruppe 1

Beschreibung

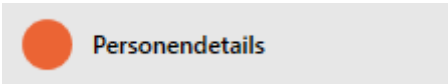
< Zurück

Weiter >

Fertigstellen

Abbrechen

4. Click on the  Person details tab.



➞ Window switches to the "Person details" tab.

Transponder - Personendetails

Hier können Sie die Details der Person bearbeiten

Hogwarts

Synchronisieren

In Matrix anzeigen

DSGVO-Daten

1 Details

2 Personendetails

3 Transponderkonfiguration

4 Zusätzliche Schließanlagen

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungsliste

9 Berechtigte Türen

PERSONENDETAILS

Nachname

Weasley

Vorname

Ron

Personalnummer

PN-6

Personengruppe

Standard Personengruppe

+ Neu

Bemerkung

Foto

Titel

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

Eingestellt am

☒ Nicht relevant

Eingestellt bis

☒ Nicht relevant

Geburtsdatum

☒ Nicht relevant

Kostenstelle

< Zurück

Weiter >

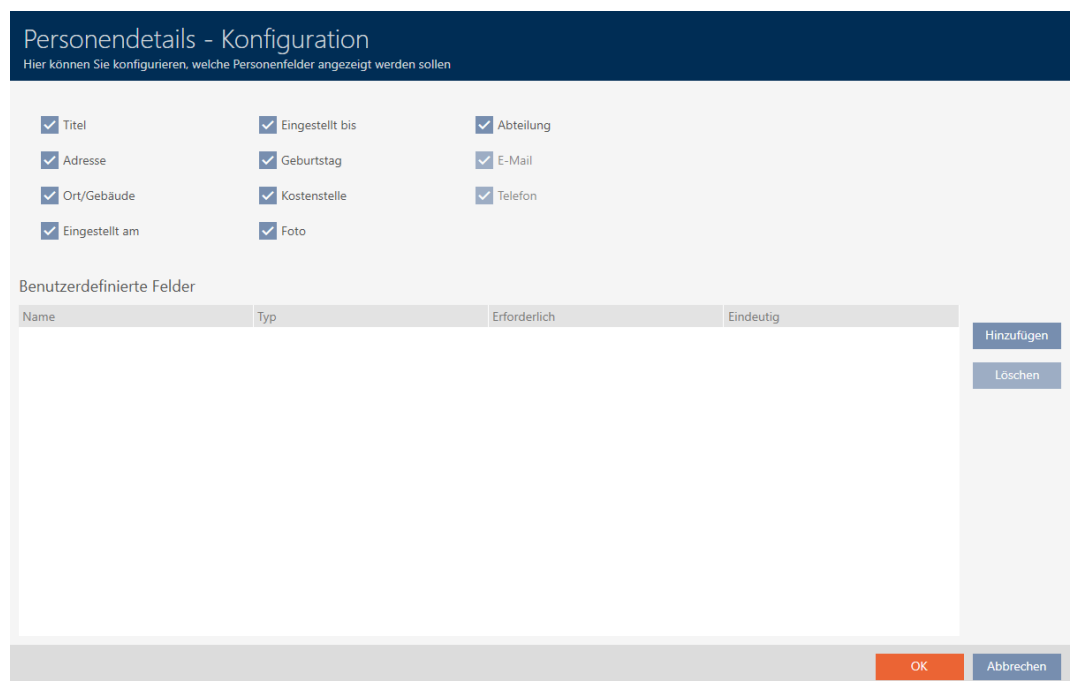
Fertigstellen

Abbrechen

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).

Transponder - Personendetails

Hier können Sie die Details der Person bearbeiten

Hogwarts

Synchronisieren

In Matrix anzeigen

DSGVO-Daten

1 Details

2 Personendetails

3 Transponderkonfiguration

4 Zusätzliche Schließanlagen

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungliste

9 Berechtigte Türen

PERSONENDETAILS

Nachname Weasley

Vorname Ron

Personalnummer PN-6

Personengruppe Standard Personengruppe + Neu

Bemerkung

Foto

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

Eingestellt am ☒ Nicht relevant

Eingestellt bis ☒ Nicht relevant

Geburtsdatum ☒ Nicht relevant

Kostenstelle

< Zurück

Weiter >

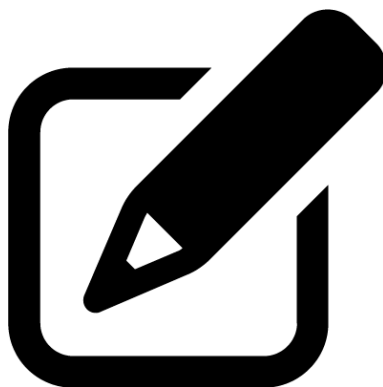
Fertigstellen

Abbrechen

10. Click on the **Finish** button.

→ Fields are shown or hidden in all locking systems in the same project.

21.13.2 Creating your own fields



Benutzerdefinierte Felder				
Name	Typ	Erforderlich	Eindeutig	
				Hinzufügen
				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)* [▶ 564]).

For this reason, you can also create your own fields (see *Subsequently modified user-defined fields* [▶ 509] 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.

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	UID-148024BA5A7369					

3. Click on any identification medium.

↳ The identification medium window will open.

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

n/a

Transpondertyp

⊗ Transponder

Firmware Version

Letzte Synchronisierung

10.05.2024 06:05:02

Sync

Erstprogrammierung

Batteriestatus

Zeitgruppe

☐ Zeitgruppe 1

Beschreibung

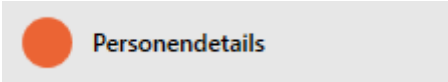
< Zurück

Weiter >

Fertigstellen

Abbrechen

4. Click on the  Person details tab.



↳ Window switches to the "Person details" tab.

Transponder - Personendetails

Hier können Sie die Details der Person bearbeiten

Hogwarts

Synchronisieren

In Matrix anzeigen

DSGVO-Daten

⚙

1 Details

2 Personendetails

3 Transponderkonfiguration

4 Zusätzliche Schließanlagen

5 Berechtigungsgruppen

6 Hashtags

7 Aktionen

8 Begehungsliste

9 Berechtigte Türen

PERSONENDETAILS

Nachname

Weasley

Vorname

Ron

Personalnummer

PN-6

Personengruppe

Standard Personengruppe

+ Neu

Bemerkung

Foto

Titel

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

Eingestellt am

☒ Nicht relevant

Eingestellt bis

☒ Nicht relevant

Geburtsdatum

☒ Nicht relevant

Kostenstelle

< Zurück

Weiter >

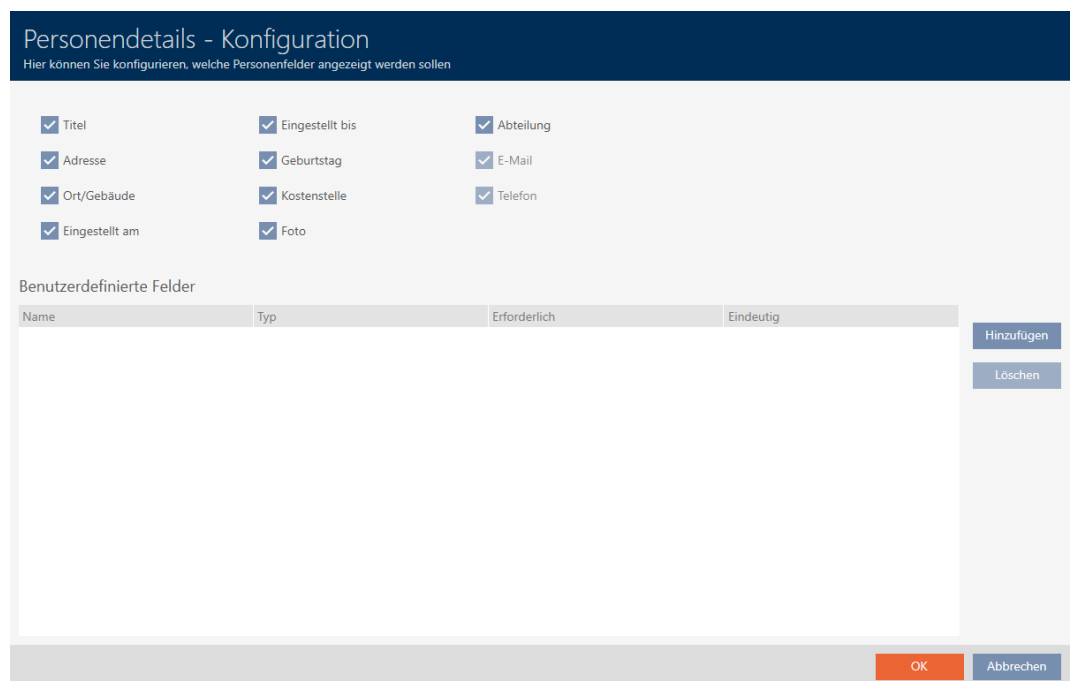
Fertigstellen

Abbrechen

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.

Personendetails - Konfiguration

Hier können Sie konfigurieren, welche Personenfelder angezeigt werden sollen

☒ Titel
 ☒ Eingestellt bis
 ☒ Abteilung

☒ Adresse
 ☒ Geburtstag
 ☒ E-Mail

☒ Ort/Gebäude
 ☒ Kostenstelle
 ☒ Telefon

☒ Eingestellt am
 ☒ Foto

Benutzerdefinierte Felder

Name	Typ	Erforderlich	Eindeutig
Büro nr.	Text	Nein	Nein

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).

Transponder - Personendetails

Hier können Sie die Details der Person bearbeiten

Hogwarts
Synchronisieren
In Matrix anzeigen

- Details
- Personendetails**
- Transponderkonfiguration
- Zusätzliche Schließanlagen
- Berechtigungsgruppen
- Hashtags
- Aktionen
- Begehungliste
- Berechtigte Türen

PERSONENDETAILS

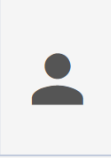
Nachname

Vorname

Personalnummer

Personengruppe

Bemerkung

Foto 

Titel

Abteilung

Telefon

E-Mail

Adresse

Ort/Gebäude

Eingestellt am ☒ Nicht relevant

Eingestellt bis ☒ Nicht relevant

Geburtsdatum ☒ Nicht relevant

Kostenstelle

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.

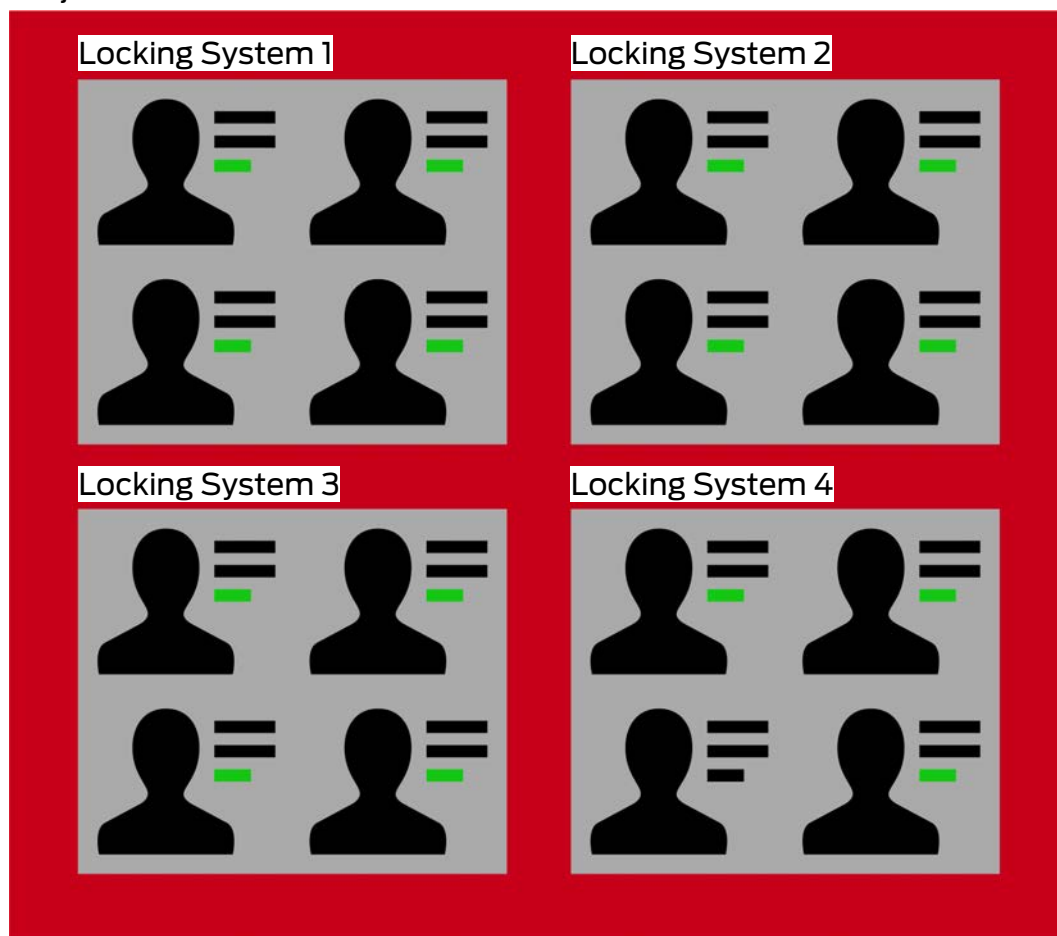
- Find out how AXM Plus responds in such cases (see *Subsequently modified user-defined fields* [▶ 509]).

21.13.2.1 Subsequently modified user-defined fields

Your AXM Plus allows you to create custom fields at any time (see *Creating your own fields* [▶ 503]).

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
If a field marked as required yet not completed is displayed, the Finish button is greyed out. You can only complete the input once you have completed the field. Required fields that are not entered are highlighted in red. In the example, office no. has been marked as ☒ Required: Kostenstelle287 Das Feld ist erforderlich Büronr.	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 Finish button, AXM Plus checks whether the same entry already exists in the same field for another object. If this is the case, the Finish button is greyed out. 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 ☒ Unique: Kostenstelle287 Das Feld ist nicht eindeutig Büronr.1

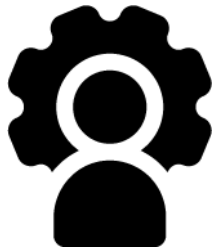
New user-defined properties for existing persons

Required	Unique
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: Kostenstelle287 Das Feld ist erforderlich Büronr. You can only complete the input once you have completed the field. Empty values are therefore possible for newly created required fields.	No problem. A field that is newly created cannot be filled with duplicate values. All newly entered values are checked before saving.

Modified user-defined properties for existing persons

Required	Unique
Fields which become required at a later point in time are treated as newly created required fields: 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: Kostenstelle287 Das Feld ist erforderlich Büronr. 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.	Fields that are made unique at a later point in time are treated as newly created unique fields: 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 Finish button, AXM Plus checks whether all unique fields are completed with unique values. If they are not, the fields concerned are highlighted in red: Kostenstelle287 Das Feld ist nicht eindeutig Büronr.1 You can only complete the entry after you have entered no value or a unique value.

22. Administrative tasks



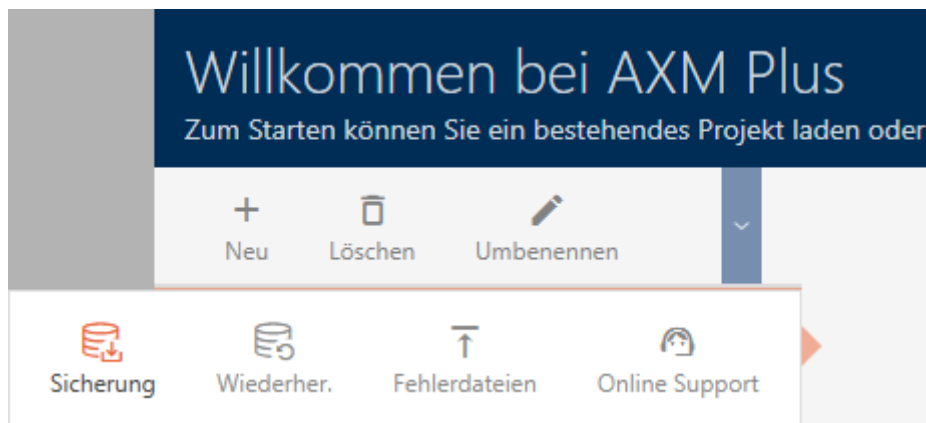
22.1 Creating a backup

Your database and thus your workload can be quickly restored if a backup is copied on a regular basis.

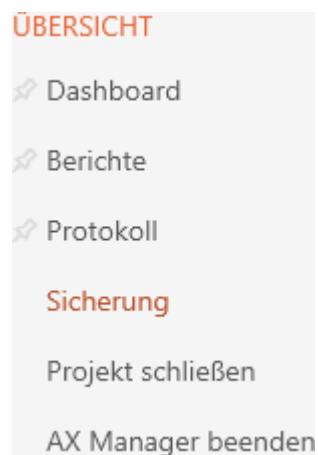
Our backup function uses AES 256 encryption.

You can easily create the backup in AXM Plus itself:

On the login mask (button **Project backup** 



Alternatively: in the expandable AXM bar (**Project backup** button):

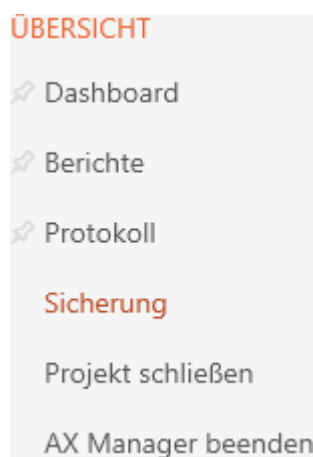


This section explains how to back up the database using the expandable AXM bar.

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.

Passwortschutz

Bitte vergeben Sie ein eigenständiges Passwort für die Datenbanksicherung

Passwort

Passwort wiederholen

Qualität

OK

Abbrechen

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.

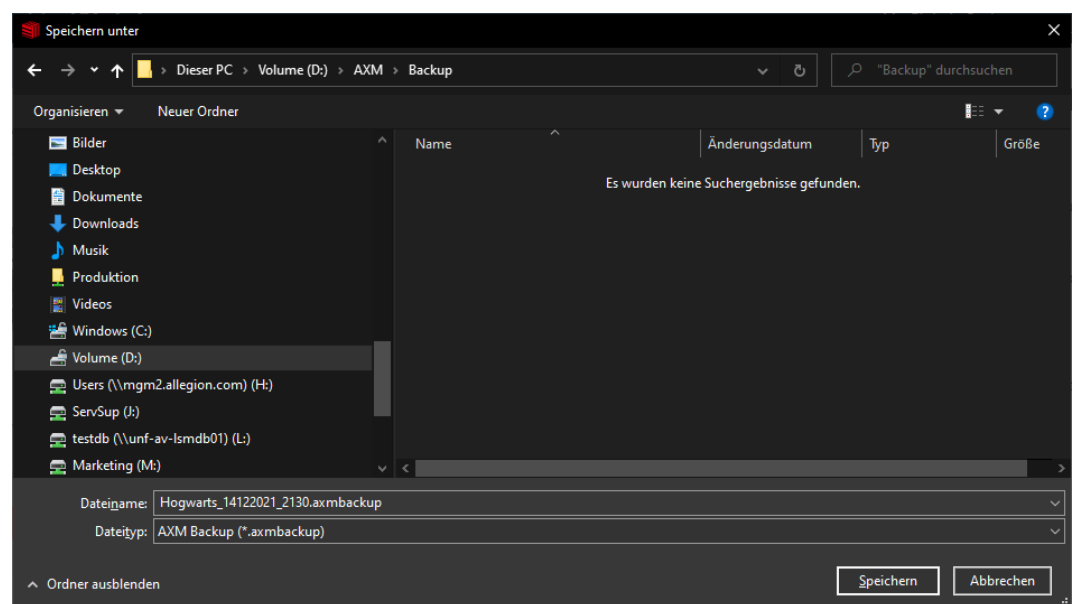
↳ The window for assigning passwords closes.

↳ Backup is being created.



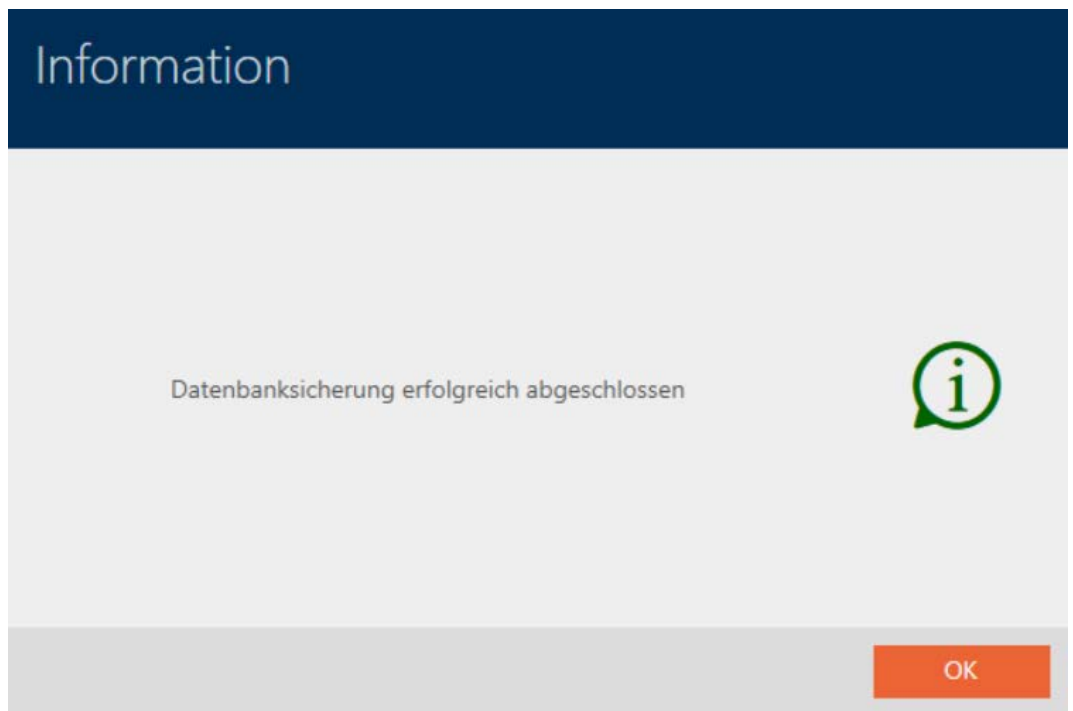
↳ The Explorer window will open.

6. Save the backup file (extension: .axmbackup) in a file directory of your choice.

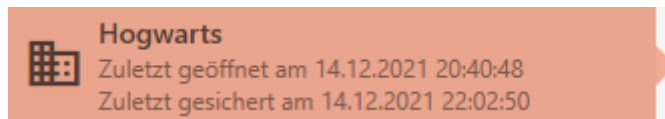


↳ Explorer window closes.

↳ Backup is complete.



You can also see when you last created a backup on the AXM Plus login mask:



22.2 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

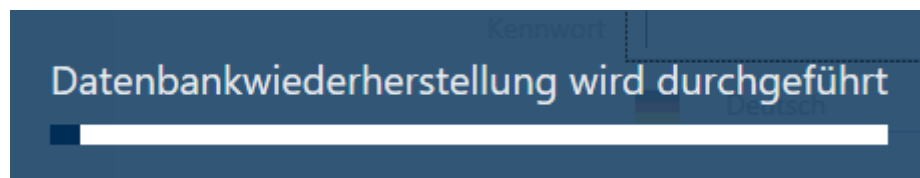
The restore only applies to the database. It has no effect on existing identification media and locking devices.

- Synchronise identification media and transponders if necessary (see *Synchronisation: Comparison between locking plan and reality* [► 416]).

✓ Backup available (see *Creating a backup* [► 513]).

1. Click on the **Restore project**  button on the login screen.
 - ↳ The Explorer window will open.
2. Go to your backup.
 - ↳ Explorer window closes.
 - ↳ Password prompt window will open.

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.



22.3 Migrate project (transfer)

Images: Q:\Produktmarketing\40 Technische Redaktion\20 Bilddatenbank\Software\AXM\Plus\AXM Plus with Netzwerk\Migration

Information from test spec.: Prerequisite: SimonsVoss ID connected to the cloud. Set the option to check cloud status

Registration must be performed via the SV-ID. Thus, it is possible to create a connection to the cloud (see description). Otherwise, the cloud will not know when it is allowed to “continue”.

Information from the procedure: Registration via the SV-ID is more straightforward. After recovery, CommNode and VNHost must be paired again on the new computer

In cloud applications (e.g. AX2Go), the cloud must be at the same level as the project in your AXM Plus. In some cases, you may wish to transfer your AXM Plus data using a backup, for example:

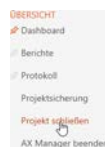
- Migrating to a new computer
- Transfer to another person after configuration

During a normal backup, the project would be paused, and the cloud would continue to run, resulting in error Resolve Out-Of-Sync. In this case, use the  **Project Migration**. It differs from the normal  **Project backup**:

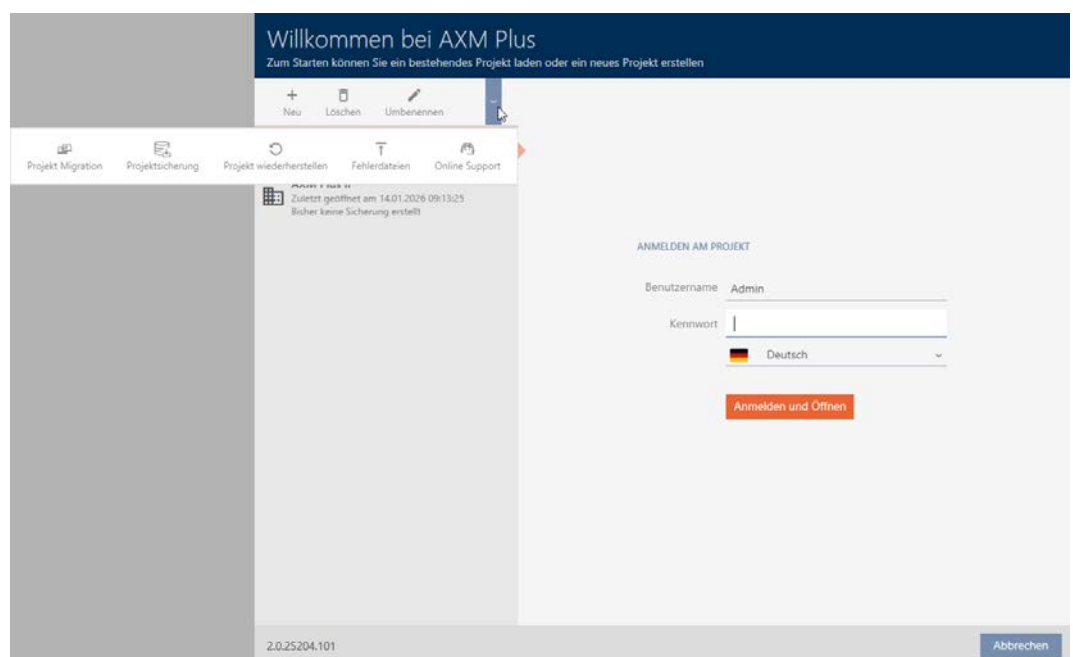
- As long as cloud services are active, there will be a pause until the project has been restored on the target computer, registered and connected to the SV-ID.
- After saving the backup file, the project is removed from the project overview and may not be edited until it has been restored.

Create migration file

- ✓ AXM registered and connected with SV-ID (see [Registration with licence](#) [▶ 44]).
 - ✓ At least one project has been created that is to be migrated (see [First steps after a new installation](#) [▶ 35]).
1. Close currently open projects, as necessary, (expand the AXM toolbar and select the entry | OVERVIEW | in the group **Close project**).



- ➔ The window for logging on to a project is visible.
2. Select the project to be migrated and expand the project options.



3. Click on the  Project Migration button.
 - ↳ The information window for the migration process opens.



Projekt Migration

Sie werden eine Migrationssicherungsdatei erstellen. Während dieses Vorgangs werden alle Projektaktivitäten gestoppt. Sobald die Sicherung erfolgreich erstellt wurde, wird das Originalprojekt gelöscht. Anschließend können Sie es auf dem Zielcomputer wiederherstellen.

PROJEKTANMELDUNG

Benutzername Admin

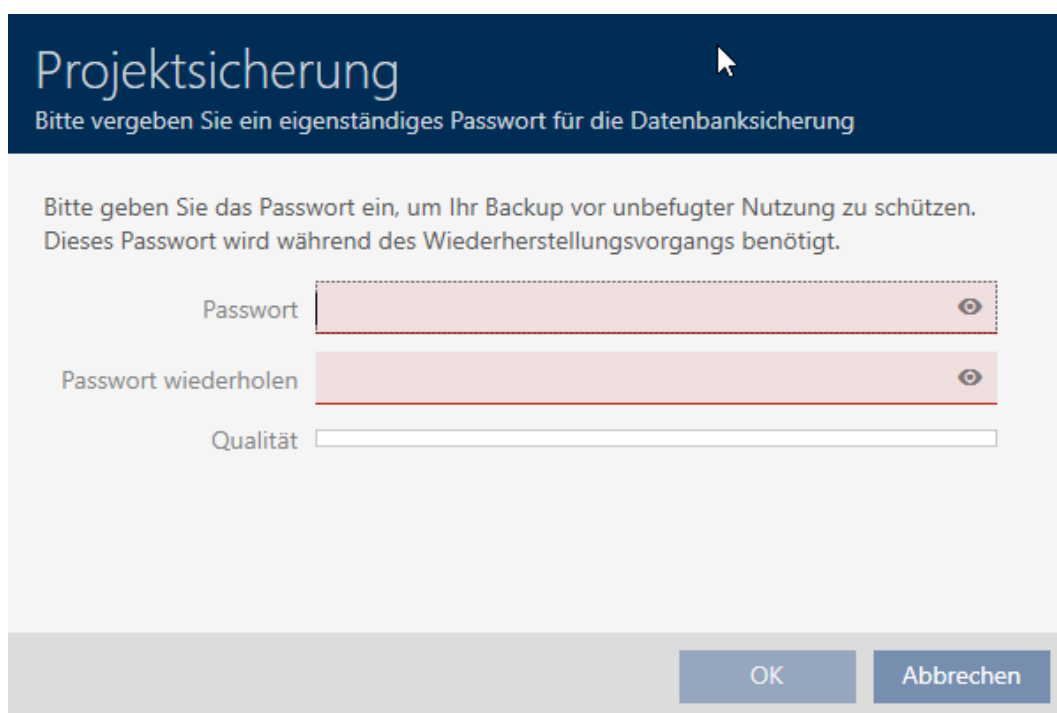
Kennwort

Anmelden Abbrechen

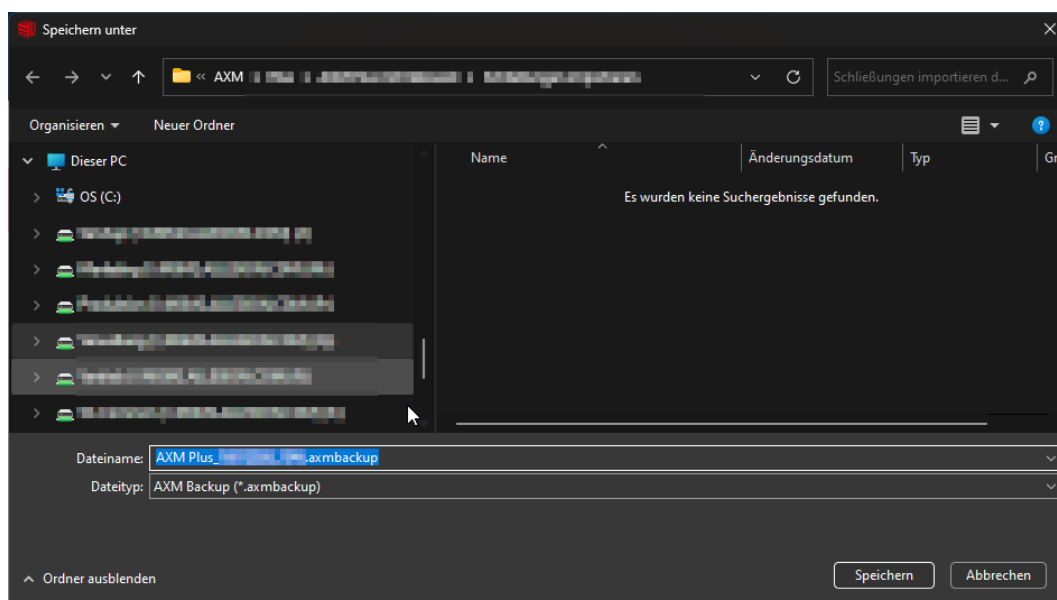
4. Enter the login details you would normally use to log in to this project in fields *User name* and *Password*.
5. Click the button **Login**.
 - ↳ Project migration is being prepared.



- ↳ Window "Project Backup" is displayed.



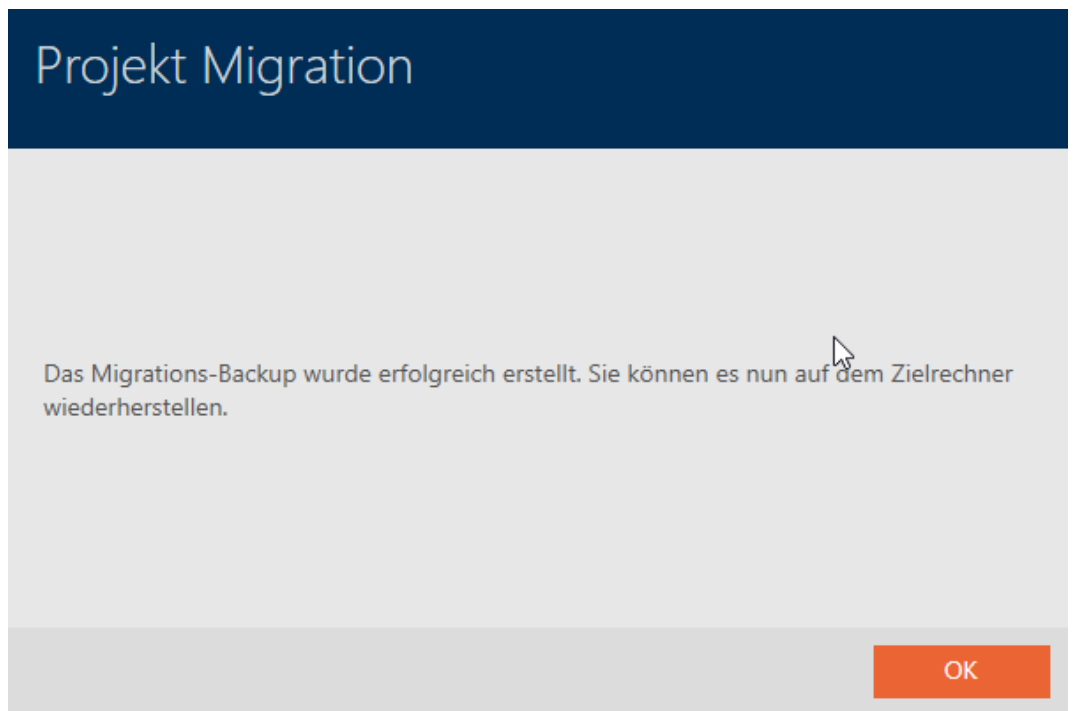
6. Enter a password in the fields *Password* and *Repeat password* to protect the project backup.
7. Click on the **OK** button.
 - ↳ Window "Project Backup" closes.
 - ↳ Windows Explorer opens.



8. Save the migration file (*.axmbackup) to a suitable location.
 - ↳ Migration file is being saved.



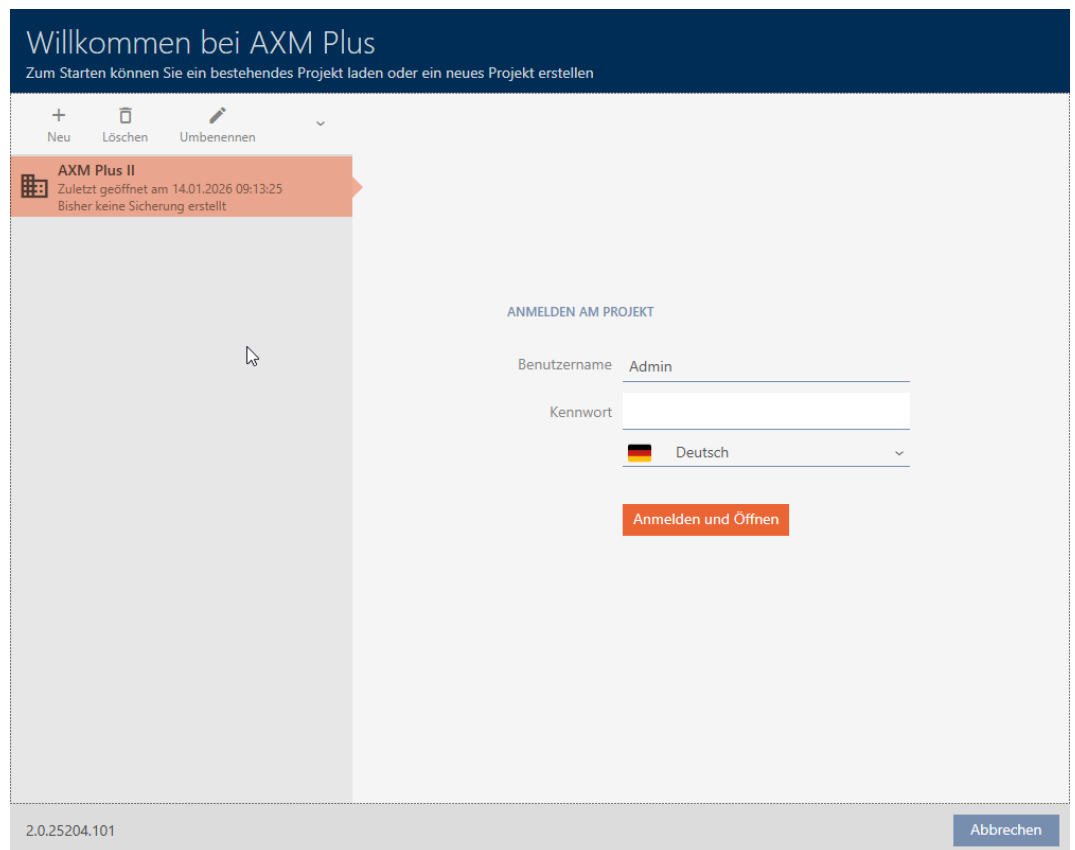
➞ Migration file saved successfully.



9. Click on the **OK** button.

➞ AXM Plus returns to the project login.

➞ The project to be migrated is no longer displayed.

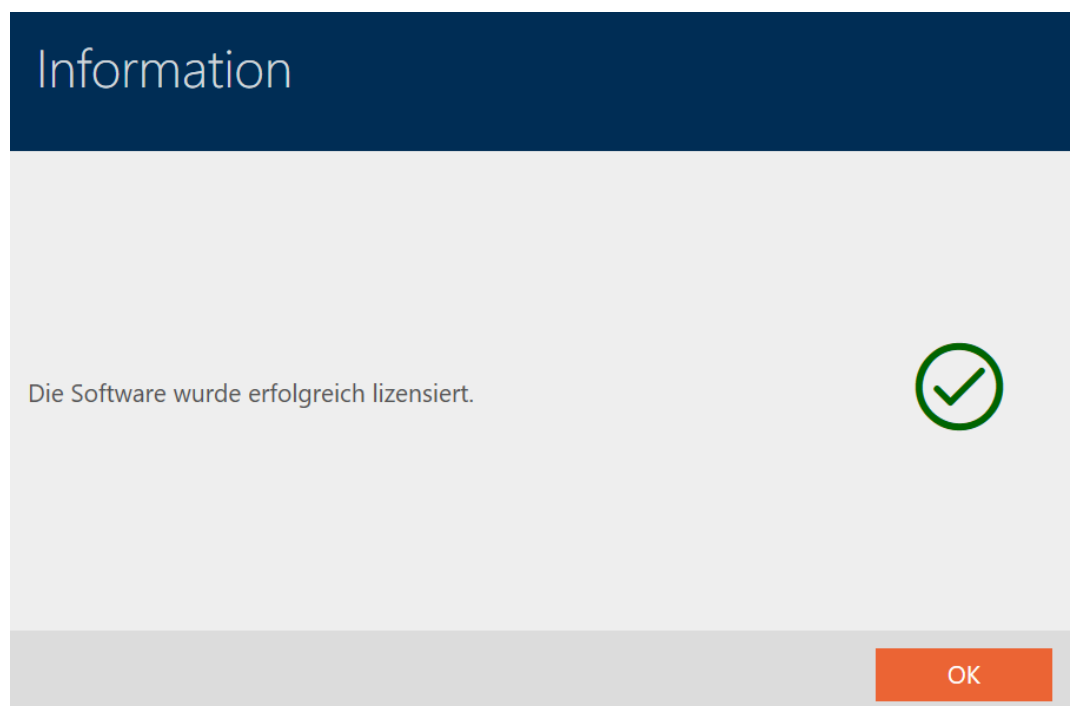
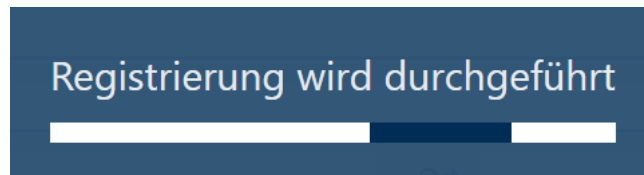


Import migration file and restore project

The transfer to the target computer consists of several parts:

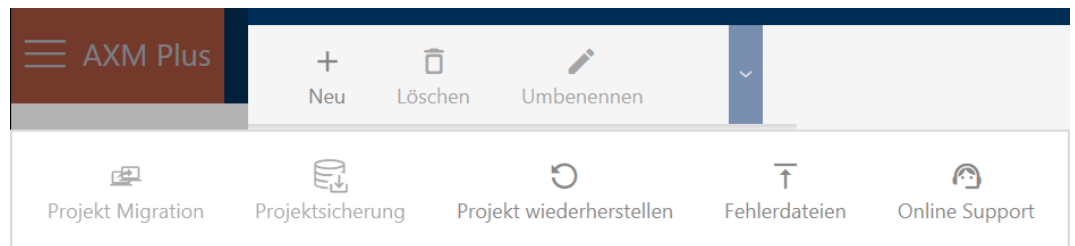
1. AXM Plus install and register.
 2. Import migration file.
 3. Re-link services (e.g. CommNode) (see *CommNode set up* [▶ 451] and *Configure of VNHost* [▶ 452]).
- ✓ Migration file created.
 - ✓ AXM Plus is installed (see *Installation* [▶ 27]).
1. Open the AXM Plus.

2. Register the AXM Plus with the same SV-ID (details see [Registration \[▶ 39\]](#)).

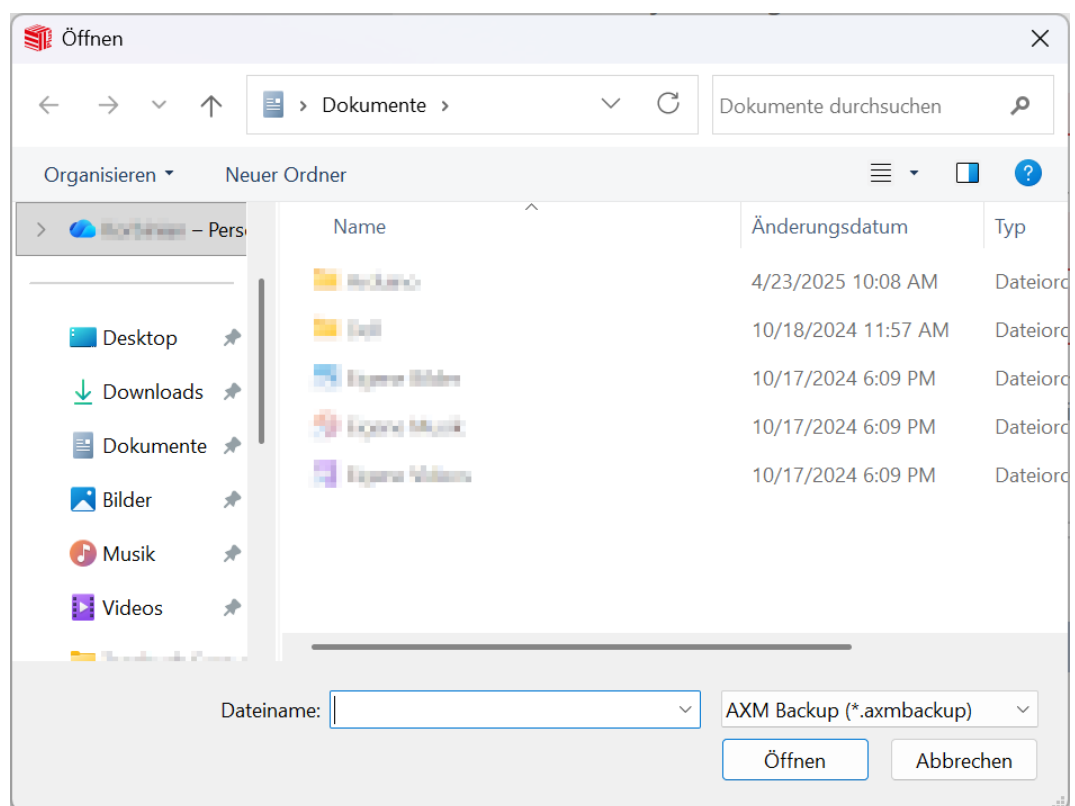


3. Click on the **OK** button.

4. Expand Project Options.



5. Click on the **Restore project** button on the login mask.
→ The Explorer window will open.



6. Select the previously created migration file (*.axmbakup).

AXM Plus_16110101_16110101.axmbakup

- The "Project Restore" window will open.

Projekt Wiederherstellung

Bitte geben Sie zur Wiederherstellung das Sicherungspasswort ein (nicht das Anmelden-Kennwort!)

Passwort

7. Enter the password you entered while creating the backup in field *Password*.
8. Click on the button.
 - ➔ The "Project Migration" window will open.

Projekt Migration

Die Datenbankwiederherstellung wurde erfolgreich abgeschlossen

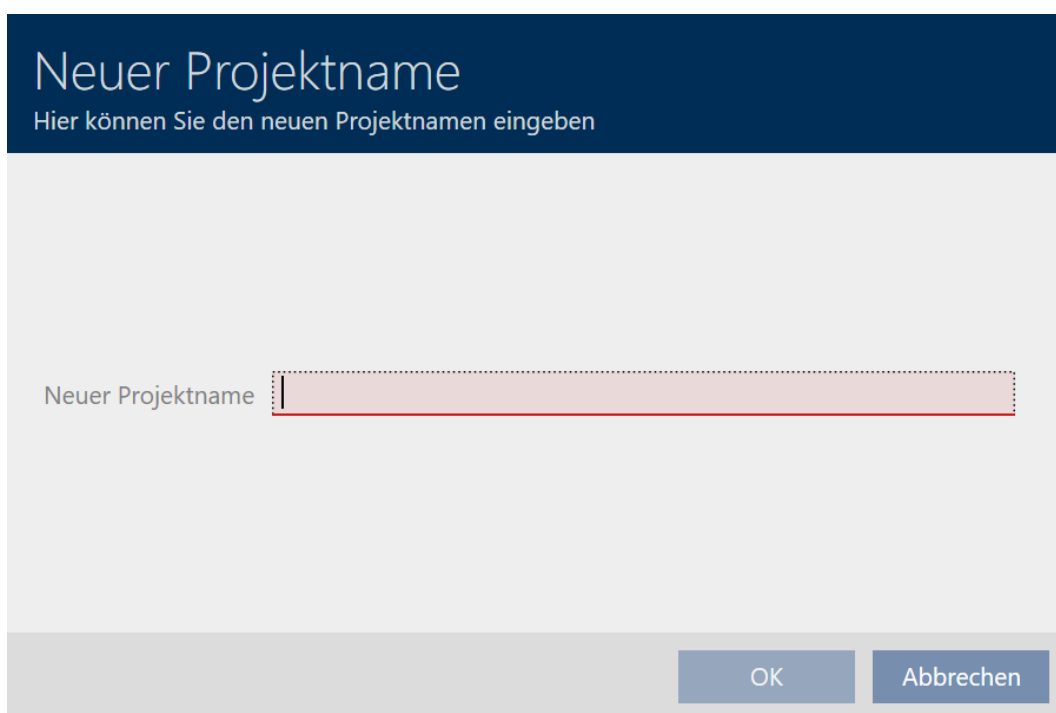
Bitte geben Sie die Projekt-Anmeldedaten ein, um die Cloud-Dienste weiterhin nutzen zu können.

PROJEKTANMELDUNG

Benutzername

Kennwort

9. Enter the login details in the fields *User name* and *Password* that you used to sign in to this project before the migration.
10. Click the button .
 - ➔ The "New project name" window will open.



The screenshot shows a dialog box titled "Neuer Projektname" (New Project Name) with a subtitle "Hier können Sie den neuen Projektnamen eingeben" (Here you can enter the new project name). The dialog has a light gray background. In the center, there is a text input field with a red border and a red dashed outline. To the left of the input field is the label "Neuer Projektname". At the bottom right of the dialog, there are two buttons: "OK" and "Abbrechen" (Cancel).

11. Enter the name you want to use to display the migrated project in field *New project name*.

The name does not have to be identical to the pre-migration name.

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

➡ Database backup completed successfully.



The screenshot shows a dialog box titled "Projekt Migration" (Project Migration) with a subtitle "Die Datenbankwiederherstellung wurde erfolgreich abgeschlossen" (The database restoration was successfully completed). The dialog has a light gray background. At the bottom right of the dialog, there is a single button labeled "OK".

When your project uses networking, proceed with linking the necessary services (see *CommNode set up* [▶ 451] and *Configure of VNHost* [▶ 452]).

22.4 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**

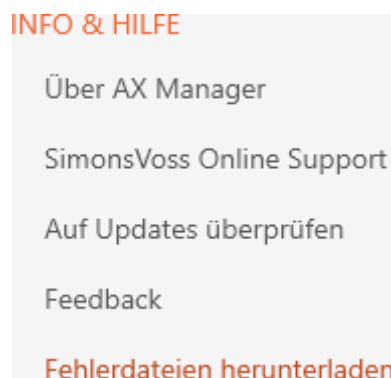
You can export error logs either on the login screen (**Error Files**  button) or in the AXM bar (**Download error files** button).

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.



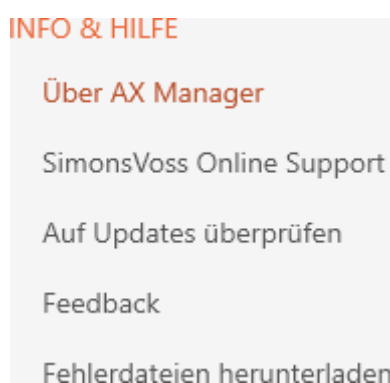
-  The Explorer window will open.
3. Save the error log (file extension: .zip) to a file directory of your choice.
-  The error log is now exported.

22.5 Displaying version number and licence key for the AXM installed

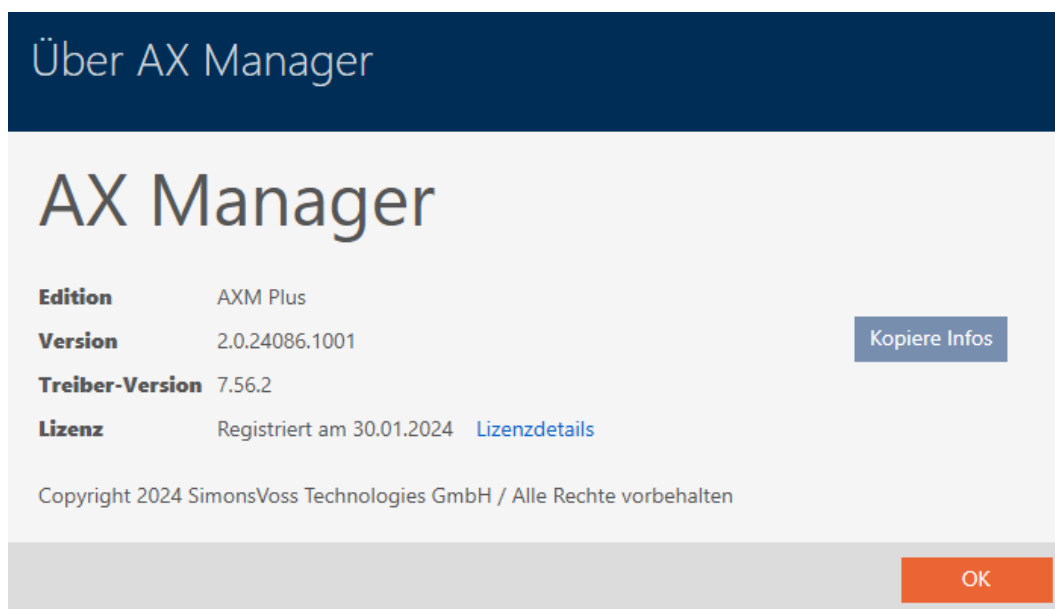
1. Click the orange AXM button .
 AXM bar opens.



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.

Lizenzdetails

LIZENZINFORMATIONEN

Kommissionsnummer	XXXXXXXXXX
Lizenz Typ	Perpetual
Edition	AXM Plus
Registriert am	30.01.2024
Ablaufdatum	29.01.2025
Registriert für	SimonsVoss Technologies GmbH
	Jörg SimonsVoss, Geschäftsführer
	Strombergstr. 10
	42699 Solingen
	Telefon: +49 212 3456789
	E-Mail: j.s@simonsvoss.de
AX2Go Lizenzen	1000
SmartSync Lizenzen	0
LockNode-Lizenzen	0
Lizenzschlüssel	XXXX-XXXX-XXXX-XXXX
Service Fee Lizenz	☒
Gültig bis	12.09.2024
Zahlungseingang bestätigt	☒

Nach Lizenz-Updates suchen
Lizenz ändern

Schließen

4. Click on the **Close** button.

→ The licence info window closes.

You can also register your AXM Plus here (see [Registration](#) [▶ 39]).

22.6 User management

22.6.1 Changing the user password

Your user password must meet the following requirements:

- Be at least 8 characters long
- Contain upper and lower case letters

You can achieve even greater security if you also include numbers (1234...) and special characters (!\$%&?...).

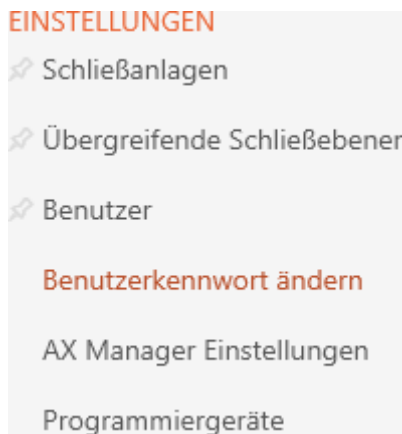
It goes without saying that each user can only change their own user password. Administrators can improve security with increased requirements for user passwords (see [Increase password security](#) [▶ 531]).

1. Click the orange AXM button .

→ AXM bar opens.



2. Select the **Change user password** entry in the | SETTINGS | group.



→ The window for changing the user password will open.

Kennwortänderung

Hier können Sie das Kennwort ändern

Benutzername

Admin

Altes Kennwort

Neues Kennwort

Neues Kennwort wiederholen

Qualität

OK

Abbrechen

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

OK Abbrechen

→ The user password has now changed.

Information

Das Benutzerkennwort wurde erfolgreich geändert



OK

22.6.2 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)

0

Kennworthistorie der letzten 10 Kennwörter verwenden

☐

Den Benutzer nach 3malig falsch eingegebenem Kennwort sperren

☐

Hohe Kennwortsicherheit

☐

Sperrmechanismus bei Leerlauf (in Minuten)

5

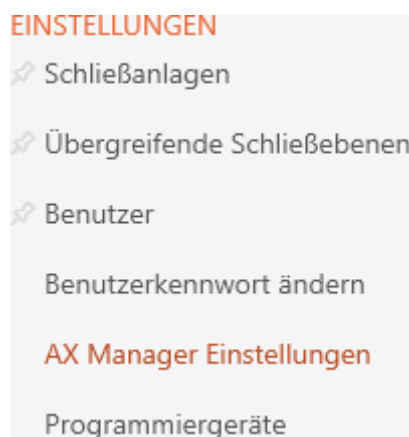
☒ Password must be changed regularly	After the configured change interval has expired, the user must assign a new password. You can set the change interval yourself using <i>Prescribed change interval (in days)</i> .
☒ Lock the user after 3 incorrect password attempts	The new password must not be the same as any of the last ten passwords.
☒ Use password history of the last 10 passwords	If a user has entered the password incorrectly three times, they will no longer be able to log in until they have been unlocked. ANMELDEN AM PROJEKT Benutzername AdminAL Kennwort *****  Deutsch ▼ Anmelden und Öffnen Der Benutzer wurde gesperrt. Bitte wenden sie sich an den Projekt-Administrator. You as <i>Admin</i> must delete and create a new <i>AdminAL</i> user in AXM Plus.

☒ High password security	AXM Plus automatically rejects trivial passwords such as "12345678". Information Das gewählte Kennwort entspricht nicht den Sicherheitsanforderungen. Um die Qualität des Kennwortes zu erhöhen, benutzen Sie Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.  OK
☒ Lock AXM when idle after (in minutes)	If your AXM Plus does not detect any actions within the configured idle time, your AXM Plus is automatically blocked. Anwendung gesperrt Passwort Entsperren Abmelden

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.

22.6.3 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.

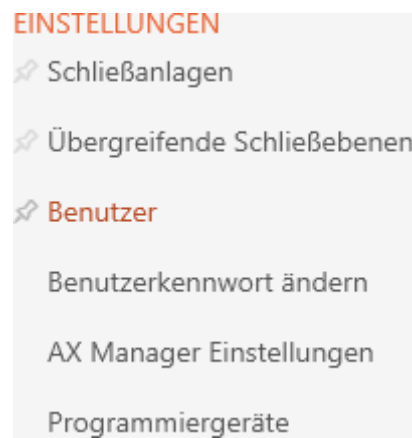
- **Admin** is the default user.
- **AdminAL** means AdminAccessList and is a strictly limited user. An AdminAL can mainly read access lists without having full access to the locking system. This allows other persons to read access lists without being able to manipulate the locking system themselves.

✓ 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.

Matrixansicht x	Benutzer x			
+	🗑️	👤	👤x	🗑️
Neu	Löschen	Aktivieren	Deaktivieren	Anzeigefilter löschen
	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.

Benutzer - Details

Hier können Sie die Details für den Benutzer bearbeiten

1 Details
2 Projektrollen
3 Schließenlagenrollen
4 Bereichsrollen
5 Personengruppenrollen
6 Überg: Schließebene Rollen

Benutzername Admin
E-Mail
Zugewiesene Person

< Zurück
Weiter >
Fertigstellen
Abbrechen

4. Select the person in your project that you wish to assign to the user from the ▼ Assigned person drop-down menu.

Zugewiesene Person Lupin, Remus ^

PERSONENINFORMATION

Name Lupin, Remus

Abteilung Teacher

Tel. 089 32 16

E-Mail remus.lupin@hogwarts.co.uk

Filch, Argus

Lupin, Remus

Snape, Severus

Weasley, Ron

Wood, Oliver

- ↳ 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.

Matrixansicht x Benutzer x			
+ Neu 🗑️ Löschen 👤 Aktivieren 🚫 Deaktivieren 🗑️ Anzeigefilter löschen			
Name	Aktiviert	Zugewiesene Person	
> Admin	Ja	Lupin, Remus	
AdminAL	Ja		

22.6.4 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 audit trails 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 audit trails user roles can be changed in the "Locking system roles" in AXM Plus.

Project roles

Protocol	Allows the database log to be read and exported. Example: <i>Tracking activities in the database (log)</i> [► 557]
Time schedule control	Allows schedules to be edited. Examples: ■ <i>Creating a schedule</i> [► 63] ■ <i>Create time group</i> [► 66] ■ <i>Deleting schedules</i> [► 74]
Site/Building management	Allows the corresponding organisational structures to be edited. Examples: ■ <i>Creating a location</i> [► 87] ■ <i>Creating a building and assigning it to a location</i> [► 90]
Using SmartSync	Allows the use of SmartSync.
Hashtags	Allows hashtags to be edited. Example: <i>Creating a hashtag</i> [► 95]
User administration	Allows persons to be assigned to users and user roles to be edited. Examples: ■ <i>Name person as an AXM user</i> [► 535] ■ <i>Assign tasks/user roles to AXM users</i> [► 537]
AX Manager settings	Allows your AXM Plus settings to be edited. Example: <i>Your personalised AXM interface</i> [► 481]

Locking system roles

Locking systems	Allows locking system details to be edited. Examples: ■ <i>Create locking system</i> [► 367] ■ <i>Changing locking system password</i> [► 401] ■ <i>Enable cards or transponders</i> [► 407]
Accesses	Allows access rights to be read and changed. Examples: ■ <i>Changing individual authorisations (cross)</i> [► 335] ■ <i>Changing many authorisations (on identification media and/or locking devices)</i> [► 336]
Personnel administration	Allows personal data to be edited. Example: <i>Persons and identification media</i> [► 98]
Reporting	Allows reports to be exported. Examples: ■ <i>Exporting the data protection report (GDPR)</i> [► 564] ■ <i>Displaying the report for identification media issue</i> [► 561]
Administration of audit trails	Allows the Audit trails and Administration of audit trails user roles to be changed. Anyone who does not have these user roles cannot read access lists themselves or allow others to.

Audit trails	Allows access lists and physical access lists to be read. Examples: ■ <i>Synchronising the locking device (including reading access list) [► 417]</i> ■ <i>Synchronise a card/transponder (including importing physical access list) [► 428]</i>
--------------	---

Area roles

Read out locks	Allows locking devices to be read in general. Example: <i>Synchronising the locking device (including reading access list) [► 417]</i>
Program locks	Allows locking devices to be synchronised. Example: <i>Synchronising the locking device (including reading access list) [► 417]</i>
View/edit locks and areas	Allows locking devices and areas to be edited. Examples: ■ <i>Creating a locking device [► 245]</i> ■ <i>Moving locking devices to areas [► 293]</i> ■ <i>Creating an area [► 93]</i>

Person group roles

Read Transponders	Allows identification media to be read in general. Examples: ■ <i>Recognise unknown cards/transponders [► 438]</i> ■ <i>Displaying the identification medium battery status [► 430]</i>
-------------------	--

Program Transponders	Allows identification media to be programmed. Example: <i>Synchronise a card/transponder (including importing physical access list)</i> [► 428]
View/edit transponders and groups	Allows identification media and person groups to be viewed and edited. Examples: ■ <i>Duplicating an identification medium (including authorisations and settings)</i> [► 122] ■ <i>Restricting identification medium authorisations to specific times (time group)</i> [► 135] ■ <i>Assigning persons to person groups</i> [► 209]

Service Set roles

Service Set Management	Allows you to set up and change common locking levels Examples: ■ <i>Using a common locking level</i> [► 410]
------------------------	---

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.

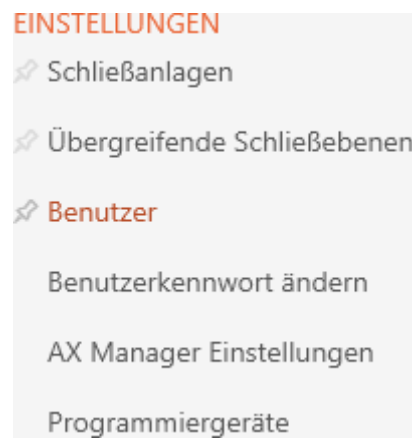
✓ At least one identification medium or at least one person is created.

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 x Benutzer x			
+ Neu 🗑️ Löschen 👤 Aktivieren 👤 Deaktivieren 🗑️ Anzeigefilter löschen			
	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

Admin

E-Mail

Zugewiesene Person

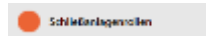
< Zurück

Weiter >

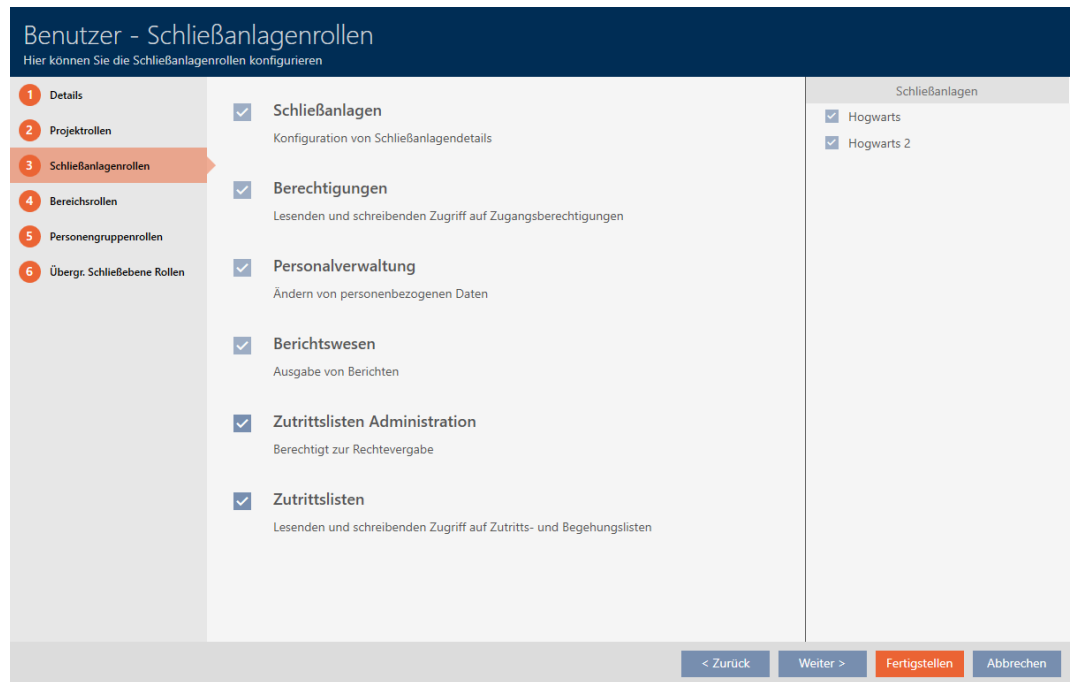
Fertigstellen

Abbrechen

4. 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.



5. Select or deactivate the required user roles (example: disable the  Administration of audit trails checkbox).
6. 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  Audit trails and  Administration of audit trails 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 Audit trails 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.

22.7 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.

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)	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. The maximum value is 30 days. 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). You can check the connection between the AXM service and the cloud: <i>Checking the connection between database and cloud</i> [► 450].



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)* [► 599] 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.

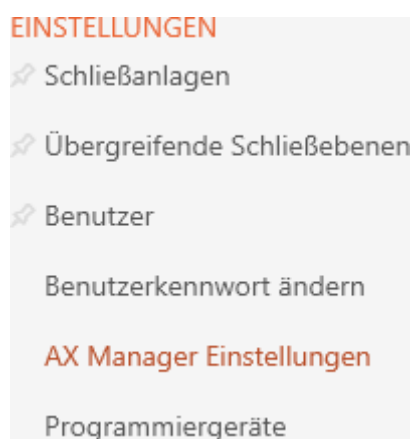
- Key name (e.g. locking system or company name)
- Contact person
- Company
- Address
- Email
- Phone number

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
- Kenntnisse
- 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 Schließanlagen 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 Hilfefunktion in den Schlüsseldetails angezeigt.

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.

23. Statistics and logs



23.1 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)* [▶ 307]). The logged access events can then be imported during synchronisation and written into the database (see *Reading access list/physical access list during synchronisation* [▶ 487] and *Synchronising the locking device (including reading access list)* [▶ 417]).

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.

- Click on the  Audit trail tab.



- ↳ Window switches to the "Audit trail" 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	Snap, Severus	0301A4D	Erlaubt
08.05.2024 21:31:00	Snap, 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

- Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
- Click on the **Export**  button.
 - ↳ The Explorer window will open.
- 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* [▶ 493]).

23.2 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)* [▶ 134]). 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)* [▶ 428]).

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.

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

10.05.2024 06:16:19

Sync

Programmiert

Batteriestatus

Ok

Zeitgruppe

Zeitgruppe 1

Beschreibung

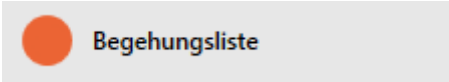
< Zurück

Weiter >

Fertigstellen

Abbrechen

2. Clicking on the **Personal audit trail** tab



➞ Window switches to the "Personal audit trail" tab.

Transponder - Begehungsliste

Hier können Sie bei aktivierter Begehungsliste die ausgelesenen Begehungen des Transponders einsehen

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

Löschen

Export

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

< Zurück

Weiter >

Fertigstellen

Abbrechen

3. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
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

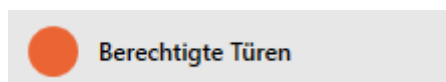
1

You have the option to personalise reports (see [Personalising reports and exports](#) [► 493]).

23.3 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](#) [► 553]

- ✓ 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](#) [► 54]).
 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 dormitory	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

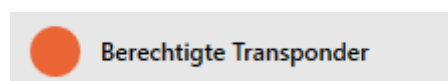
→ Doors for which the identification medium is authorised are displayed.

23.4 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* [► 552]

- ✓ 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* [► 54]).
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

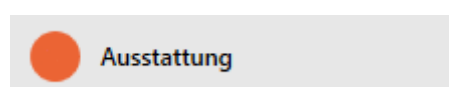
➞ Identification media that are authorised for the door are displayed.

23.5 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* [▶ 54]).
 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.

Schließung - Ausstattung
Hier können Sie die Ausstattungsdetails der Schließung einsehen

Hogwarts ↕ Synchronisieren 📊 In Matrix anzeigen

Abkürzung	Beschreibung
ZS	Digital Zylinder AX
EU	Europrofil
CO	Comfort
30-30	Baulänge - Außenlänge 30 mm - Innenlänge 30 mm
A	Aktiv
G2	Produktgeneration G2
ZK	Zutrittsprotokollierung / Zeitzonesteuerung
LN	LockNode

< Zurück Weiter > Fertigstellen Abbrechen

➞ Equipment features are displayed.

23.6 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 .

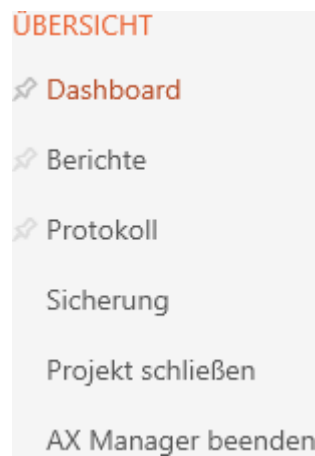
➞ AXM bar opens.

AXM Plus  Globale Suche

ÜBERSICHT	SCHLÜSSANLAGENSTEUERUNG	ORGANISATIONSSTRUKTUR	EINSTELLUNGEN	INFO & HILFE
Dashboard	Matrixansicht	Bereiche	Schließanlagen	Über AX Manager
Berichte	Schließungen	Personengruppen	Übergreifende Schließebenen	Onlinehilfe
Protokoll	Transponder	Standorte	Benutzer	SimonsVoss Support
Projektsicherung	PinCode Tastaturen	Gebäude	Benutzerkennwort ändern	Auf Updates prüfen
Projekt schließen	Spezielle Transponder	Hashtags	AX Manager Einstellungen	Feedback
AX Manager beenden	Berechtigungsguppen		WaveNet	Fehlerrückmeldung
	Zeitplansteuerung		VN Host	Datenbankbericht
			Programmiergeräte	

Version: 2.0.25.04.101

2. 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:

1. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).
2. Click on the warning entry in the Warning column.
 - ↳ Warning will open.

Warnung - Bearbeiten

Hier können Sie die Warnung bearbeiten

DETAILS

Titel Schließung defekt / austauschen
 Schließung 'Gryffindor dormitory' muss zurückgesetzt werden.

Text

Erledigt? ☐

Kommentar

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.

23.7 Tracking activities in the database (log)

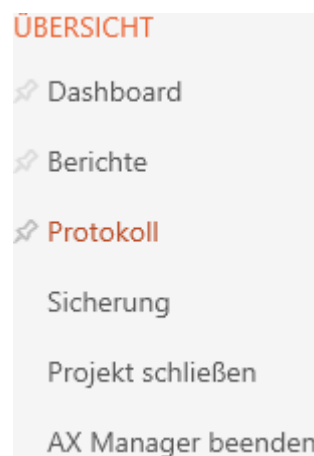
Every change and every setting in the database is logged in AXM Plus. This allows you to track who changed what in the database and when they made the changes.

The log archiving period can be adjusted (see [Setting the log archiving period](#) [▶ 559]).

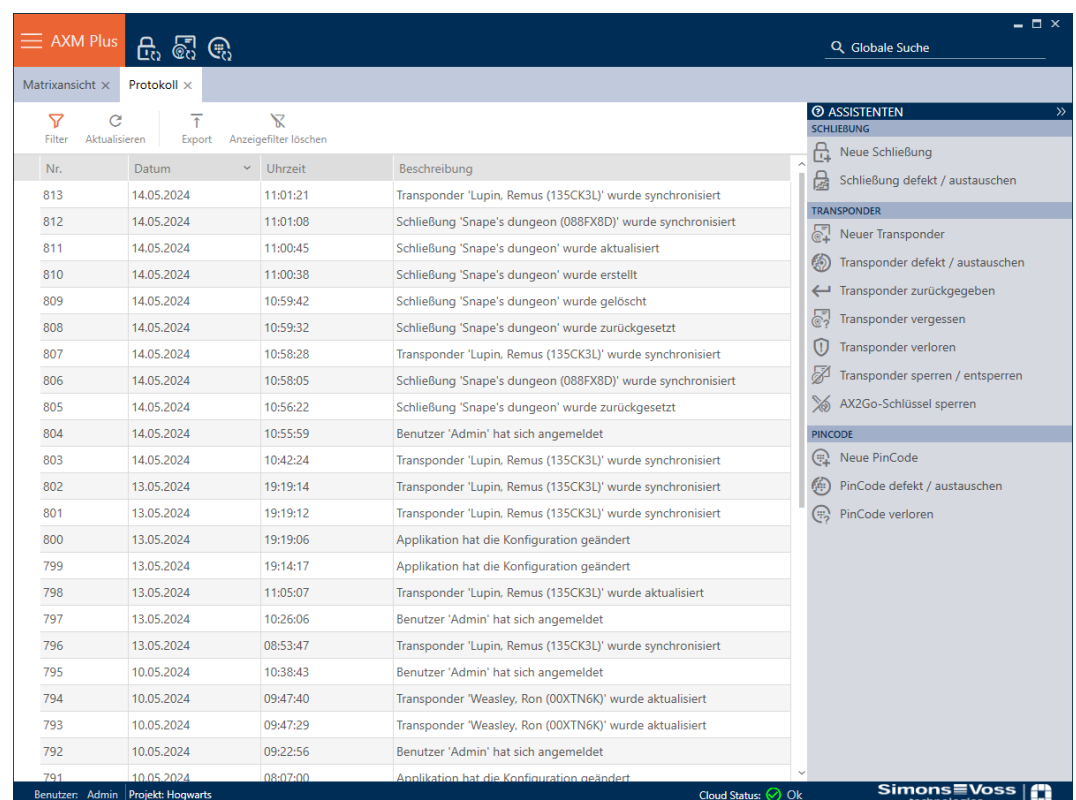
1. Click the orange AXM button .
 - ➔ AXM bar opens.



- Select the **Protocol** entry in the | OVERVIEW | group.



- The AXM bar will close.
- The [Protocol] tab will open.



- Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 54]).

- Log is displayed.

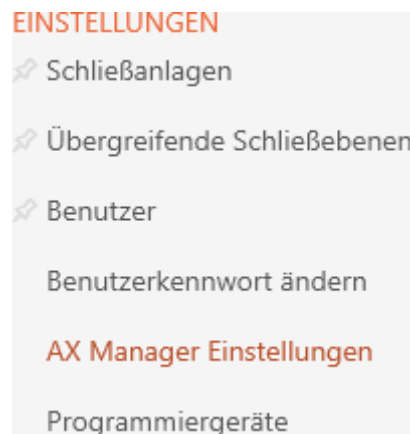
The **Export**  button also allows you to export the log to provide a permanent backup.

23.7.1 Setting the log archiving period

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

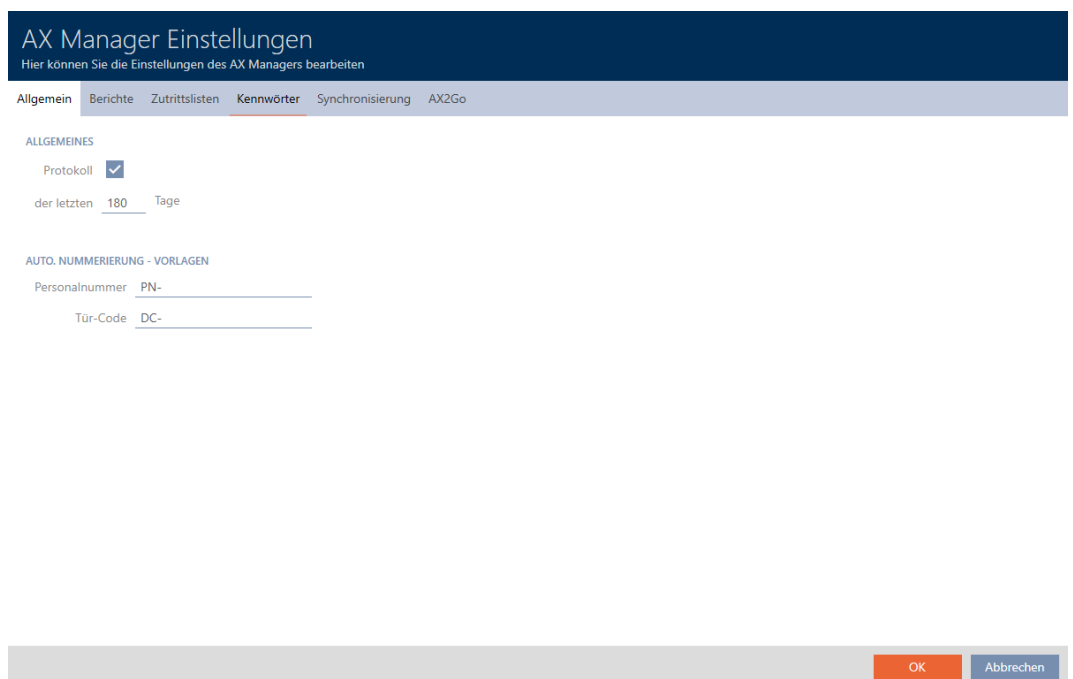


2. Select the **AX Manager settings** entry in the | SETTINGS | group.



- ↳ The AXM bar will close.
- ↳ The window with the AXM Plus settings will open.

3. Go to the [General] tab.

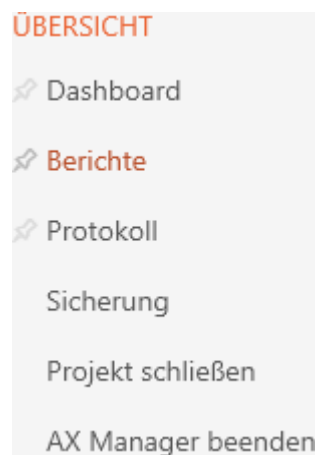


4. If you do not wish to log the changes to the database at all: Activate the ☐ Protocol checkbox.
5. Enter the required archiving period (max. 670 days).
6. Click on the **OK** button.
 - ↳ The window with the AXM Plus settings closes.
 - ↳ Protocol is limited to the required duration.

23.8 Reports and exports

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:



☰ AXM Plus

Globale Suche

Matrixansicht x

Berichte x

Löschen

Anzeigefilter löschen

	Name	Systembericht	Letzte Änderung	Beschreibung
>	DSGVO Bericht	Ja	15.03.2024 11:25:26	
	Transponderausgabebericht	Ja	15.03.2024 11:25:26	

Benutzer: Admin

Projekt: Hogwarts

Cloud Status: Ok

SimonsVoss

technologies

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.

23.8.1 Displaying the report for identification media issue



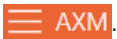
You can use this report to prove that someone has received a specific identification medium and instruction from you.

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* [► 493])
- The locking system administrator's email address (source: AX Manager settings, see *Personalising reports and exports* [► 493])
- 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 \[▶ 54\]](#)).
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					
Snap	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 ☐

OK

Abbrechen

7. 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.
8. If you also want to include any existing authorisations, select the ☒ With authorisations checkbox.
9. 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* [▶ 190] for the action list).
10. Click on the button.
 - ↳ "Transponder handover" window closes.
 - ↳ The Explorer window will open.
11. 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](#) [▶ 493]).

You can also enter the issue date directly in the action list for the identification medium concerned (see [Note card/transponder issue date](#) [▶ 191]).

23.8.2 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

Titel	Junior Assistant
Vorname	Percy
Nachname	Weasley
Personalnummer	PN-30
Abteilung	Department of International Magical Cooperation
Telefon	+44 020 3492 32113 85
E-Mail	pweasley@ministryofmagic.com
Adresse	Whitehall London, England Great Britain
Ort/Debäude	Ministry
Eingestellt am	03.02.2010 00:00:00
Eingestellt bis	11.02.2022 00:00:00
Geburtsdatum	07.06.2000 00:00:00
Kostenstelle	57324

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)* [► 557]).



NOTE

Exporting user-defined fields

You can also create user-defined fields for Person details (see *Personalising properties for person details* [► 497]). These are then exported too.

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



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

SCHLIESSANLAGENSTEUERUNG

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

- ➞ 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. 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	🔑	🔄	⚠️				

5. Click on the **GDPR data** button .
 - ➞ The Explorer window will open.
6. 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 \[► 493\]](#)).

See [Information on data protection \[► 15\]](#) for further general information on data protection in System 3060.

23.8.3 Export identification media and locking devices as a list

You have the option of exporting all identification media and all locking devices as lists.

You can find the corresponding buttons in tab [Transponders] (see *Exporting identification media as a list* [► 202]) and in tab [Locks] (see *Exporting locking devices as a list* [► 332]).

23.8.4 Create database report

The Database report supports you in the following cases, for example:

- Support
- Maintenance
- Battery replacement
- Locking device replacement

It provides comprehensive information on:

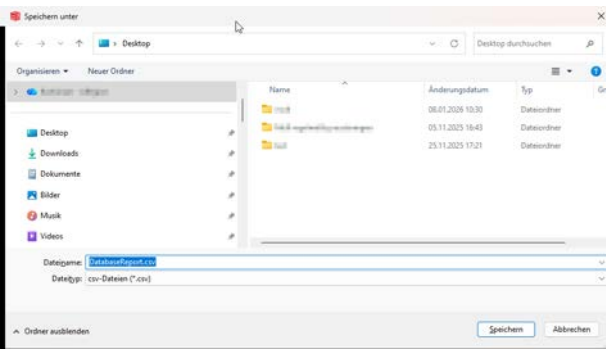
- Database version
- Registration and Licencing
- Users
- Locking systems
- Locking devices
- Identification media
- PIN code keypad
- Networking

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



2. Select the **Database report** entry in the | INFO & HELP | group.
↳ Windows Explorer opens.

3. Save the database report to a location of your choice.



→ Creating database report.

Example of a database report:

	A	B	C	D	E	F
1	Versions					
2	ClientVersion	2.0.25204.101				
3	PlatformVersion	2.0.25218.901				
4	DatabaseVersion	15.0.2000.5				
5						
6	Registration					
7	CommissionNumber					
8	LicenseType	Standard				
9	SoftwareEdition	Plus				
10	StartDate	16.01.2026				
11	ExpirationDate	16.01.2027				
12	MobileCredentials	10				
13	SmartSyncLicenses	5				
14	WaveNet	128				
15	LicenseKey					
16	Subscription.Enabled	True				
17	Subscription.ExpiryDate	21.11.2027				
18						
19	Users					
20	Name					
21	Admin					
22						
23	Systems					
24	Name	Type	CardTemplate	CardConfiguration		
25	WaveNet-Demo	OnlyTransponder				
26	WaveNet-Demo II	OnlyTransponder				
27						
28	Locks					
29	Door	DoorCode	SerialNumber	Phi	EquipmentCode	FirmwareVersion
30	WaveNet-Demozylinder	DC-0001			SV-ZS-EU-CO-35-AM-62-ZK	1.1.1147
31	WaveNet-Demohandle	DC-0003			SHB508C051AA11G2ZK	5.6.74
32	Besuchereingang		1			
33	Wareneingang		2			
34	Notausgang		3			
35	Haupteingang		4			
36	Nebeneingang		5			
37	SÄVidusgang		6			
38	Aufenthaltbereich		7			
39	Parkplatz		8			
40	Garage		9			
41						
42	Transponders					
43	SerialNumber	Type	Firmware			
44						
45	PinCodeKey pads					
46	Name	SerialNumber	Type	Door	FirmwareVersion	
47						
48	Network					
49	Door	ChipId	Type	Firmware	MasterAddress	SlaveAddress
50						
51	WaveNet-Demohandle	0001111111	CentralNode	40.11.0.0	33	6
52	WaveNet-Demozylinder	0001111111	LockNode	32.15.16.3	0	39
53			LockNode	33.7.17.0	0	38

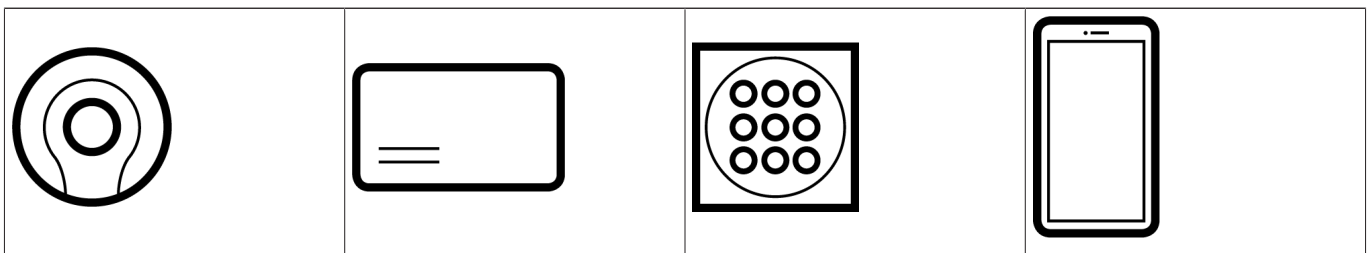
24. Background knowledge and explanations

24.1 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.

Seriennummer		TID
002TU6TC		3203

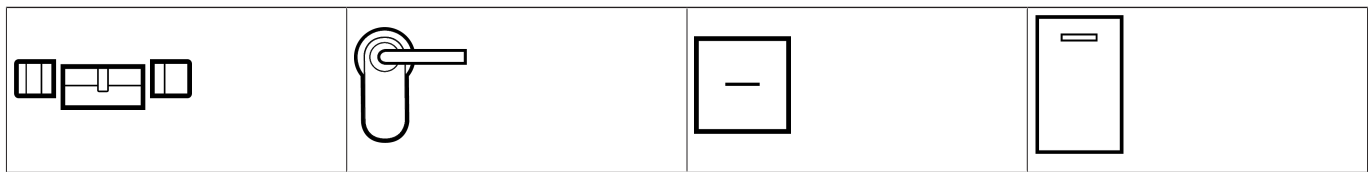
However, this link is confined to AXM Plus and is not written onto identification media or locking devices. A locking device uses the TID (and not the serial number) to check whether an identification medium is authorised or not.

Passive identification media have physical limitations when put to use (see [Cards and locking device IDs \[► 624\]](#)).

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.

24.1.1 PIN Code G1 vs. PIN Code AX

The AXM Plus offers you two different PIN code keypads:

PINCODE - DETAILS	
Typ	AX PinCode
Name	AX PinCode
Schließung	PinCode G1

- 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	❑ BLE (Bluetooth low energy)	❑ Active (= 25 kHz) with G1 protocol
Read range	❑ Good range for AX locking devices	❑ Good range for non-AX locking devices ❑ Shorter range of AX locking devices
PIN assignment	❑ Programming of PINs directly in the AXM Plus ❑ Log in to the AXM Plus as authorisation for programming	❑ Programming of PINs directly on the PIN code keypad 3068 ❑ Segmentation into one Master PIN and up to three User PINs ❑ Master PIN as authorisation for programming

PIN code keypad AX		PIN code keypad 3068
Synchronization	Your AXM Plus will help you synchronise with instructions. The process in brief: 1. Start synchronisation. 2. Press and hold 0 for at least two seconds to enter programming mode. 3. Wait until synchronisation is complete.	Your AXM Plus will help you synchronise with instructions. The process in brief: 1. Create Master PIN on the PIN code keypad 3068. 2. Create User PINs with Master PIN on the PIN code keypad 3068. 3. Start synchronisation. Enter 00 and master PIN on PIN code keypad 3068. 4. Continue with synchronisation in AXM Plus. 5. Enter the corresponding PIN code keypad 3068 on the keypad on User PIN (e.g. 1 for the first User PIN). 6. Wait until synchronisation is complete.

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	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. This is why a programming requirement arises on the PIN code keypad and on the locking device after assignment of PIN code keypad AX.	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. This is why a programming requirement arises on the PIN code keypad and on the locking device after assignment of PIN code keypad 3068.
Additional PINs	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. The new PINs are communicated to the PIN code keypad AX, which is why programming is only required on the PIN code keypad.	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. 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 programming is required on the PIN code keypad and locking device.
Changes to authorisations	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. Programming is only required on the PIN code keypad.	The PIN code keypad 3068 retains the G1 ID unchanged. The changed authorisation is saved in the locking device’s locking plan. This means that programming is only required on the locking device.

24.1.2 AX2Go

24.1.2.1 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.

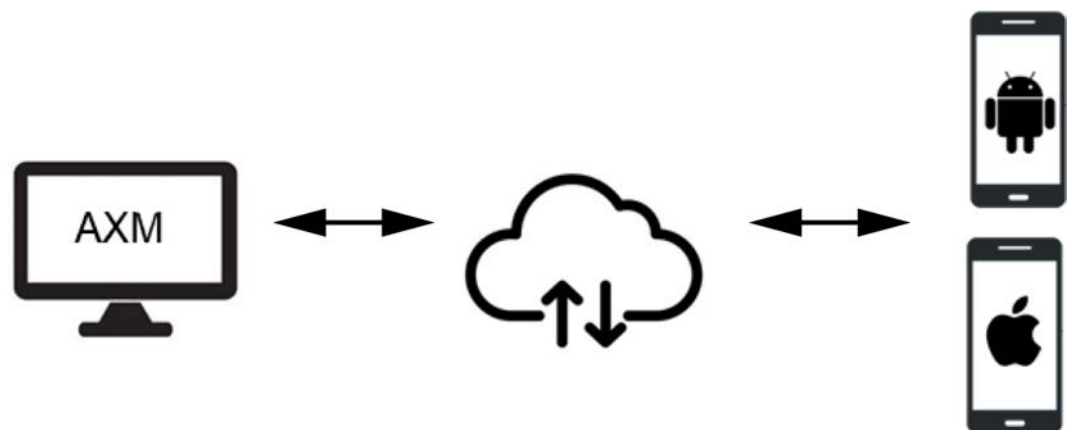
Functions

- 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

24.1.2.2 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 \[► 450\]](#))
- Valid registration with Software Fee licence (see [Registration \[► 39\]](#))

24.1.2.3 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 \(AX2Go and virtual network\) \[► 599\]](#) for details).

24.1.2.4 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.

24.1.2.5 Transferred data

- Authorisations
- Time budget renewal

From iOS 1.1.6/Android 1.3.32

- Physical access list on the smartphones concerned (AX2Go users)
- Battery warnings for AX locking devices

24.1.3 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.

TRANSPONDER DETAILS		
Typ	⊙	Transponder
Service Typ		Batteriewechsel
Beschreibung		Batteriewechsel Schließungsaktivierung

Battery replacement	Lock Activation
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. You can temporarily cancel freeze mode on G2 locking devices with a Battery replacement identification medium. You can then engage the locking device with a second, authorised identification medium to open the door and replace the batteries. This does not affect AX locking devices as the batteries can also be accessed and replaced when completely discharged.	You can reactivate a disabled locking device with a Lock Activation identification medium. You can then engage the locking device with a second authorised identification medium.

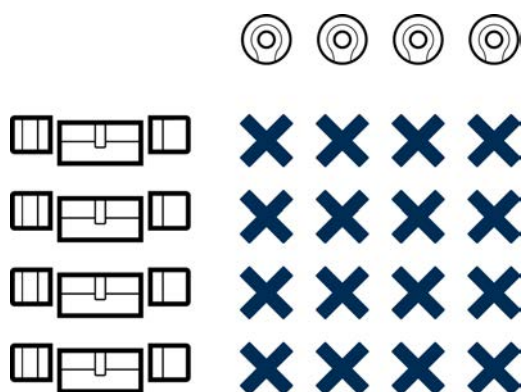
24.2 Locking systems

A locking system is a contiguous structure consisting of:

- Locking plan
- Organisational components

Locking plan

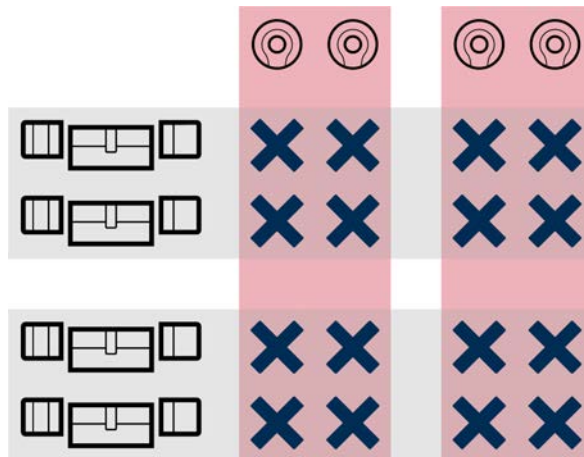
Locking devices, identification media and authorisations are saved in the locking plan (also see *Identification media, locking devices and the locking plan* [▶ 571]).



The locking plan becomes a locking system with further organisational components:

- Areas [▶ 607]

- [Person groups](#) [[▶ 603](#)]
- [Access levels](#) [[▶ 602](#)]
- [Time groups and schedules](#) [[▶ 587](#)]
- [Time switchovers](#) [[▶ 591](#)]
- [Hashtags](#) [[▶ 608](#)]



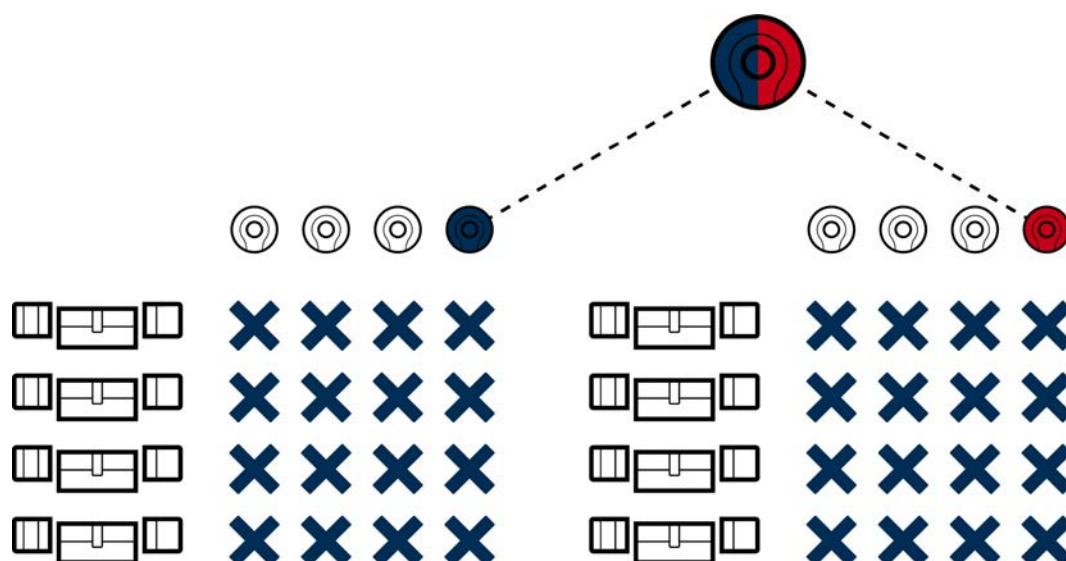
A number of locking systems in the same project

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](#) [[▶ 215](#)]). 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:



24.3 Common locking levels

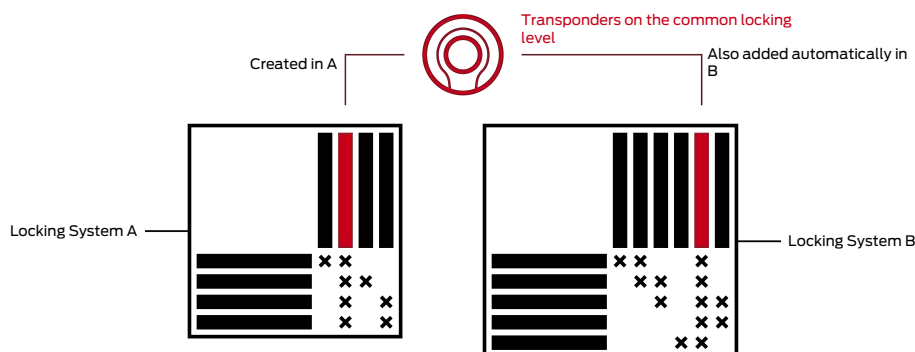
Common locking levels allow you to authorise identification media on locking devices from many different locking systems.

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.

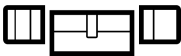
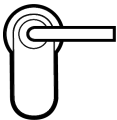
SimonsVoss recommends using the red common locking level for emergency purposes only (fire service, rescue services, etc.).

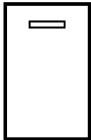
Transponders on the red common locking level are also able to operate disabled locking devices.

- 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.

24.4 “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.

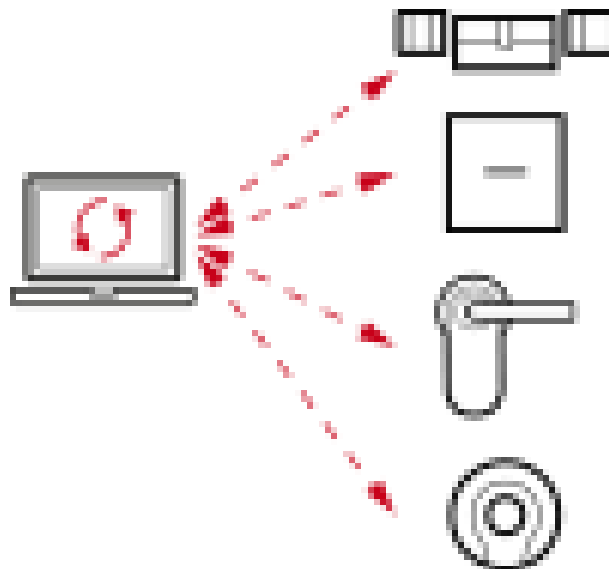
Locking device	Response	User action
SmartRelays 	Switching: The relay contact in SmartRelay switches. Depending on the SmartRelay, this is a make contact or a changeover contact. Connected electrical doors now open.	No further action required. The door is generally already open.
SmartLocker AX 	Retract 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.

24.5 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* [► 416]). 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

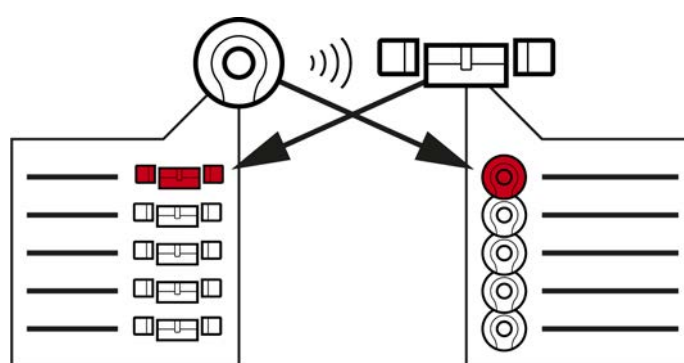
IMPORTANT**Changes to the locking system only take effect after synchronisation**

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* [► 51]).
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* [► 416]).

The AX2Go is a special case due to the cloud connection; see *Synchronisation of AX2Go keys via the cloud* [► 577].

24.6 Access and physical access lists**Physical access list****Access list**

If an identification medium addresses a locking device, both can log this action (the access control function is a prerequisite for the locking device).

Card configuration with an AV template is required for cards.

- The locking device concerned is saved to a physical access list in the identification medium.
- The identification medium concerned is saved to an access list in the locking device.

Both lists can be read during synchronisation and imported into the database, for example:

- *Synchronising the locking device (including reading access list)* [► 417]
- *Synchronise a card/transponder (including importing physical access list)* [► 428]

You can then view both lists:

- *Displaying and exporting a locking device's access list [► 548]*
- *Displaying and exporting physical access lists for cards/transponders [► 550]*

24.7 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 [► 587]*)
- Automatically engage locking devices (*Time switchovers [► 591]*)



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.

24.7.1 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:

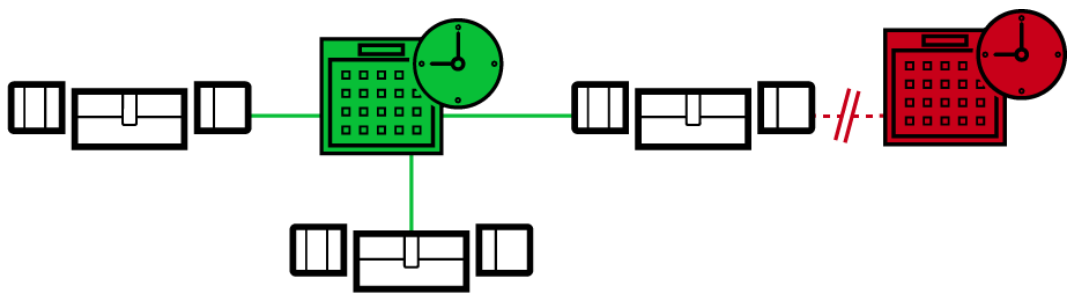
Considerations for:	Main entrance	Laboratory
Employee	Your employee may enter the building during the entire flexitime period and also between 7:00 to 22:00 hours on weekends.	Your employee may enter the laboratory during the entire flexitime and also between 7:00 to 22:00 hours on weekends.
Intern	Your intern shouldn't have to wait outside for your employee to come in when the weather is bad. Consequently, your intern may also enter the building during the entire flexitime between 7:00 to 22:00 hours on working days.	The laboratory is a dangerous workplace. To protect your intern, you want them only to be able to enter the laboratory under your employee's supervision. You therefore limit your intern's access to the laboratory to working days and to your employee's core working hours (9:00 to 16:00).
Cleaner	Your cleaner may enter the building during cleaning hours between 17:00 to 19:00 on Tuesdays and Thursdays.	The laboratory is dangerous and, consequently, only trained personnel may enter. Cleaning staff may possibly change and are therefore trained persons. As a result, you do not want your cleaner to enter the laboratory at all.

You can see that there are two doors where you wish to control authorisations with three different times. You will thus need:

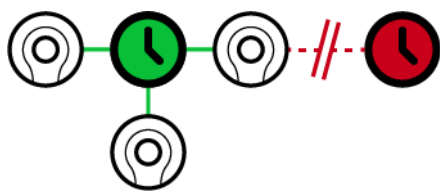
- Two schedules for doors or locking devices:
 - "Main entrance" schedule
 - "Laboratory" schedule
- Three time groups for the people in the company:
 - "Employee" time group
 - "Intern" time group
 - "Cleaner" time group

New schedule or new time group?

- There is one schedule per locking device, but any number of locking devices can be assigned per schedule.



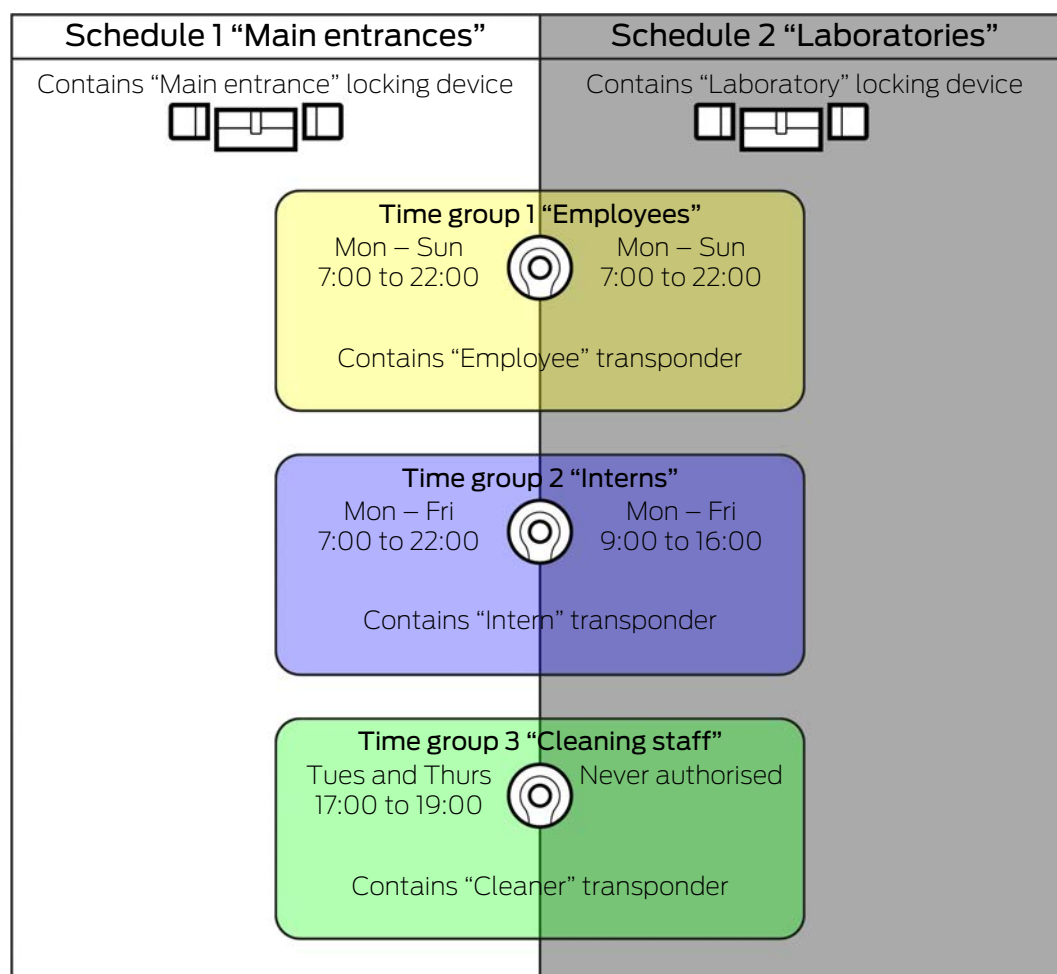
- One time group per identification medium, but any number of identification media can be assigned per time group.



- All time groups are visible/selectable in all schedules but are set individually for each schedule. If you create and set a new time group in one schedule, the time group will also appear in all other schedules. However, it is only available there and is set as “not authorised” by default for security reasons.

New schedule	New time group
If the same identification medium needs to be able to enter using two locking devices at different times. As you can only assign one time group to each identification medium, you assign a separate schedule to the locking devices in this case. Example: Although the intern’s transponder may open the main entrance between 7:00 to 22:00 hours, the same transponder may only open the laboratory between 9:00 to 16:00 hours.	If two identification media are to be able to enter using the same locking device at different times. As you can only assign one schedule per locking device, you assign a separate time group to the identification media in this case. Example: The employee may open the main entrance locking device between 7:00 to 22:00 hours daily, but the intern may only use the same locking device between 7:00 to 22:00 hours on working days.

Schematic diagram



	Main entrance	Laboratory
Employee	❑ Your employee's transponder: "Employees" time group ❑ Main entrance locking device: "Main entrances" schedule ❑ "Employees" time group authorised in "Main entrances" schedule between 7:00 to 22:00 daily Your employee can enter the main entrance between 7:00 to 22:00 hours daily.	❑ Your employee's transponder: "Employees" time group ❑ Laboratory locking device: "Laboratories" schedule ❑ "Employees" time group authorised in "Laboratories" schedule between 7:00 to 22:00 daily Your employee can enter the laboratory between 7:00 to 22:00 hours daily.

	Main entrance	Laboratory
Intern	■ Your intern's transponder: "Interns" time group ■ Main entrance locking device: "Main entrances" schedule ■ "Interns" time group authorised in the "Main entrances" schedule between 7:00 to 22:00 on working days Your intern can enter the main entrance between 7:00 to 22:00 on working days.	■ Your intern's transponder: "Interns" time group ■ Laboratory locking device: "Laboratories" schedule ■ "Interns" time group authorised in "Laboratories" schedule between 9:00 to 16:00 on working days Your intern can enter the laboratory between 9:00 to 16:00 on working days.
Cleaner	■ Transponders for your cleaner: "Cleaning staff" time group ■ Main entrance locking device: "Main entrances" schedule ■ "Cleaning staff" time group authorised in the "Main entrances" schedule between 17:00 to 19:00 on working days Your cleaner can enter the main entrance between 17:00 to 19:00 on Tuesdays and Thursdays.	■ Transponders for your cleaner: "Cleaning staff" time group ■ Main entrance locking device: "Laboratories" schedule ■ "Cleaning staff" time group never authorised in the "Laboratories" schedule Your cleaner can never enter the laboratory.

24.7.2 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* [► 75]).
2. Then add the locking devices you require to this time switchover (see *Engaging and disengaging locking devices automatically with time switchover* [► 301]).
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* [► 301]).

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:

ZEITUMSCHALTUNG-KONFIGURATION

☐ Manuelles Auskuppeln	☒ Automatisches Auskuppeln
☒ Manuelles Einkuppeln	☐ Automatisches Einkuppeln
☐ Transponder aktiv: immer	☒ Transponder aktiv: nur, wenn ausgekuppelt

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* [▶ 309] 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* [▶ 309] for setting the impulse duration).

Manuelles Einkuppeln

Locking device engages:

- ▣ Within the time intervals and
- ▣ If authorised identification medium is activated

Example: Store in the shopping centre where the sliding door mustn't open automatically during the shopping centre's opening hours. The store owner could be delayed due to a traffic jam and the store would open with no-one in control.

Locking device remains engaged for the time interval.

You can also disengage the locking device during the time interval using an authorised identification medium (exception:  Transponder aktiv: Nur, wenn ausgekuppelt option activated).

Locking device then remains disengaged until:

- ▣ You press an identification medium again during the same time interval: Locking device engages again, time switchover continues as usual.

- In the case of  Manuelles Einkuppeln option: a new time interval starts and an identification medium is activated.
- In the case of  Automatisches Einkuppeln option: a new time interval starts.

Automatisches Einkuppeln

Locking device engages:

- time interval starts

Locking device remains engaged for the time interval.

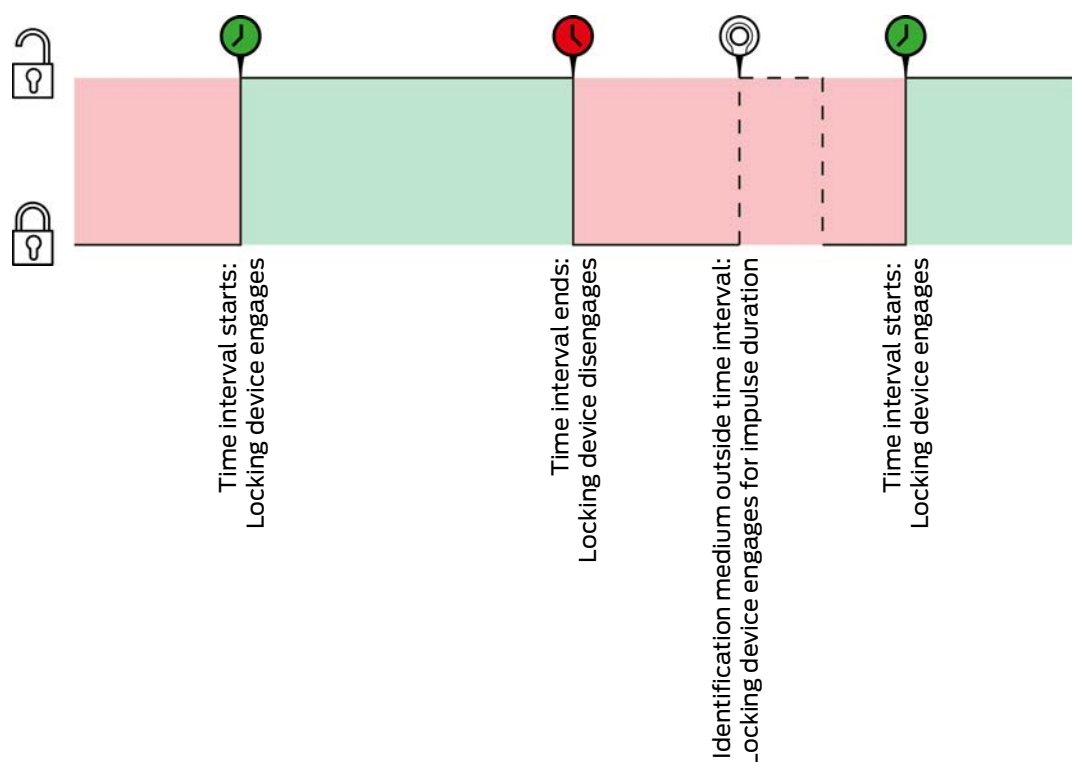
You can also disengage the locking device during the time interval using an authorised identification medium (exception:  Transponder aktiv: Nur, wenn ausgekuppelt option activated).

Locking device then remains disengaged until:

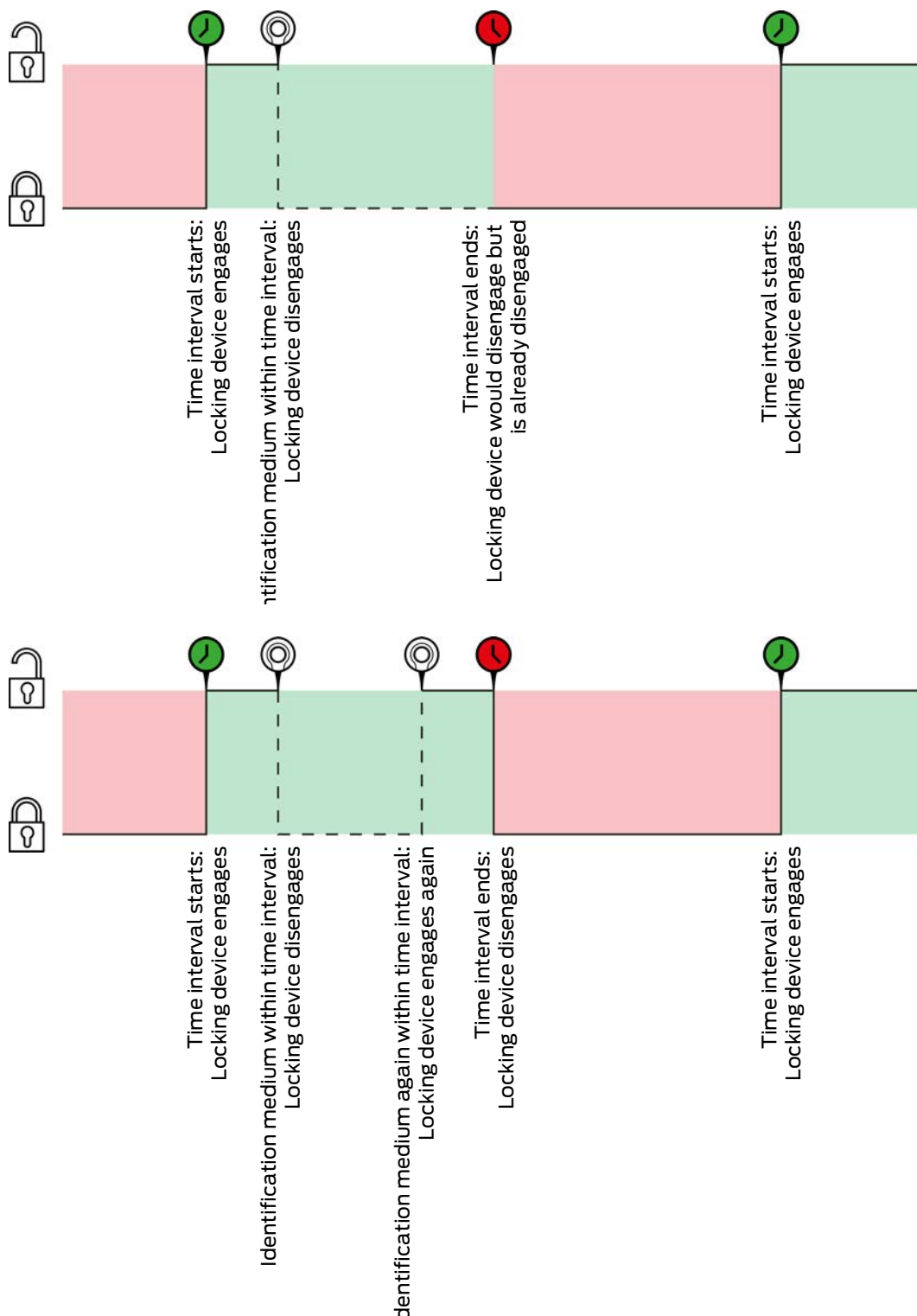
- You press an identification medium again during the same time interval: Locking device engages again, time switchover continues as usual.
- In the case of  Manuelles Einkuppeln option: a new time interval starts and an identification medium is activated.
- In the case of  Automatisches Einkuppeln option: a new time interval starts.

24.7.2.1 Examples

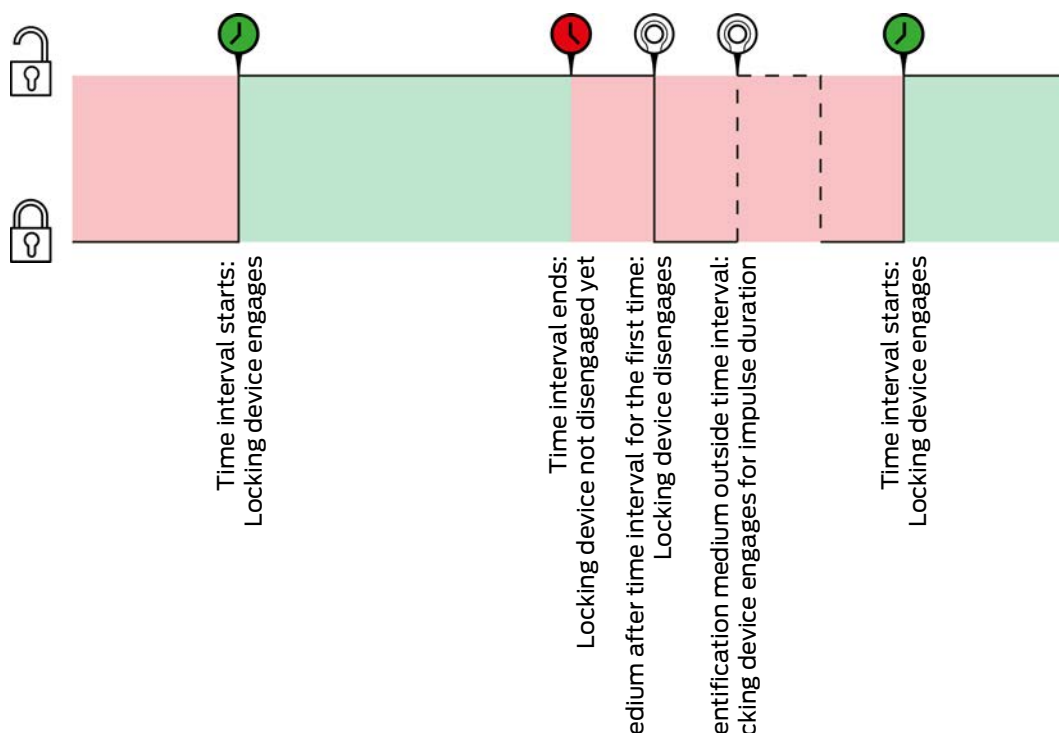
Automatisches Einkuppeln, Automatisches Auskuppeln



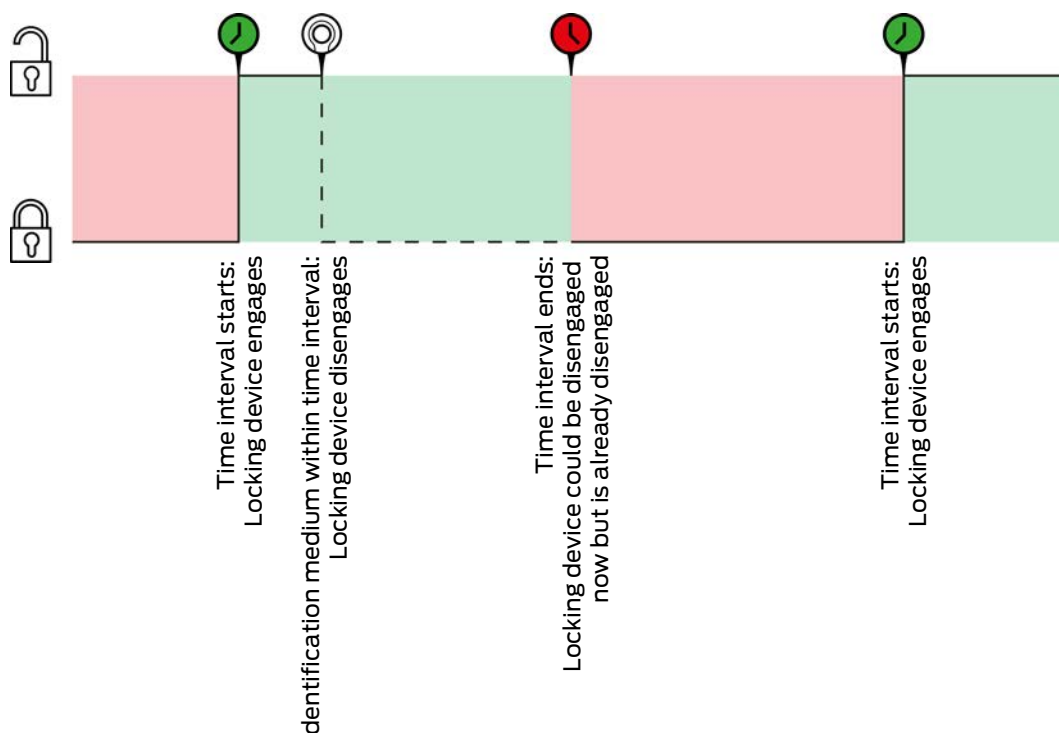
The  Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

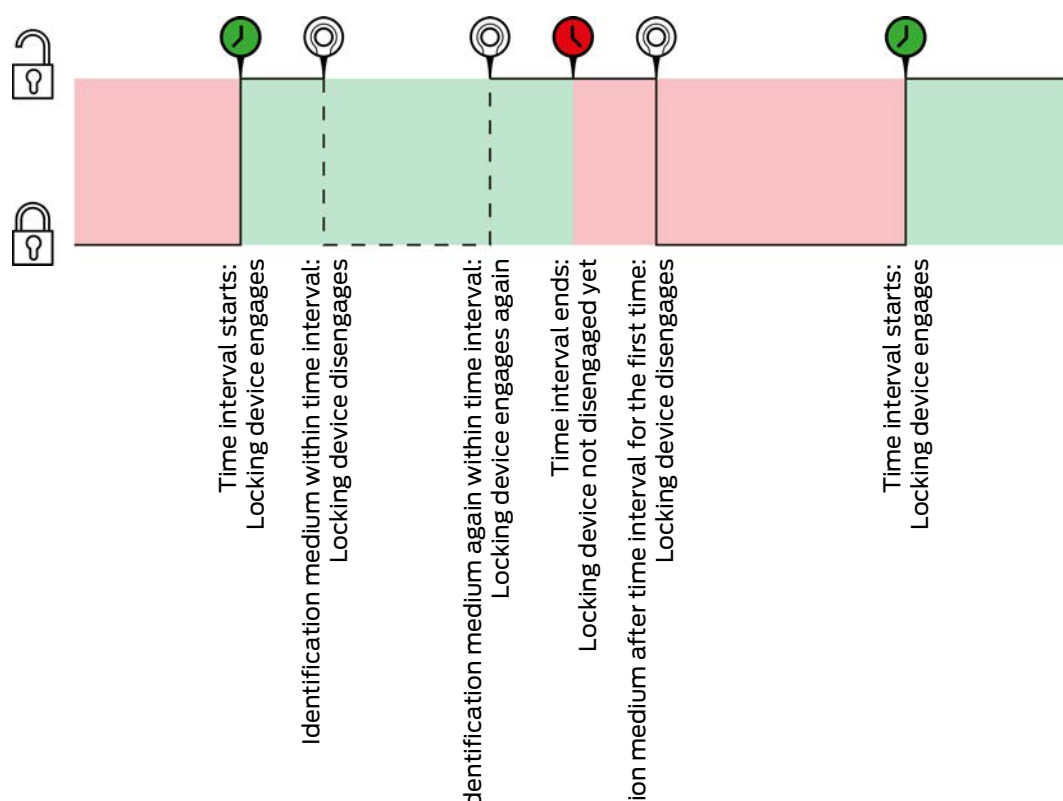


Automatisches Einkuppeln, Manuelles Auskuppeln

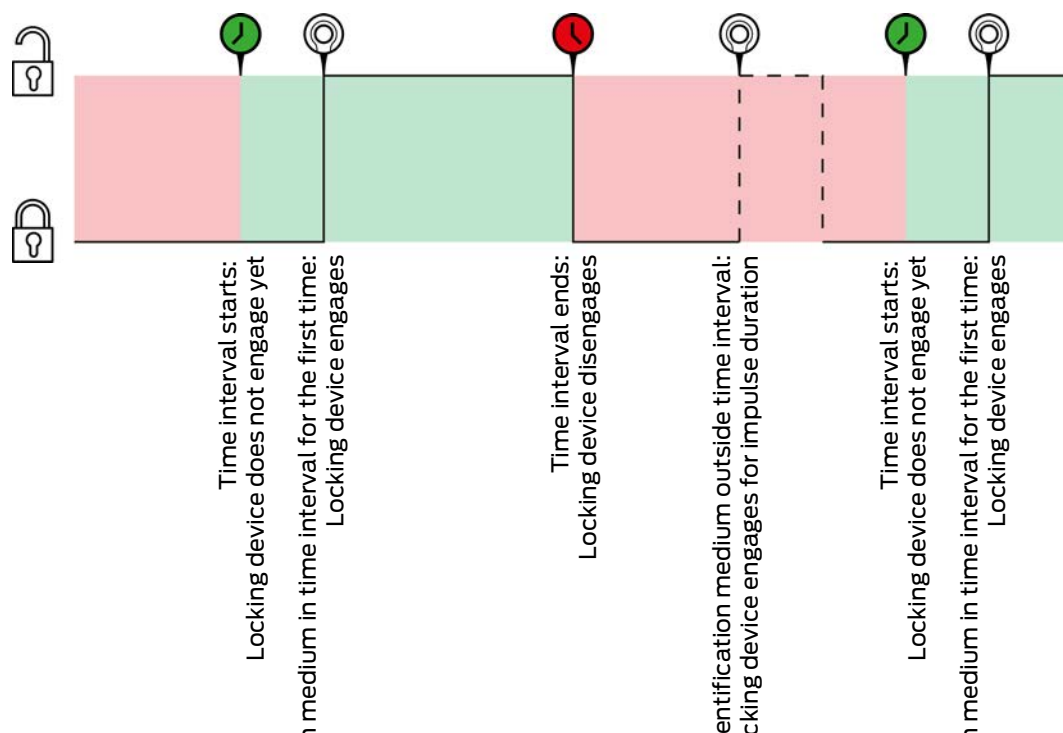


The  Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

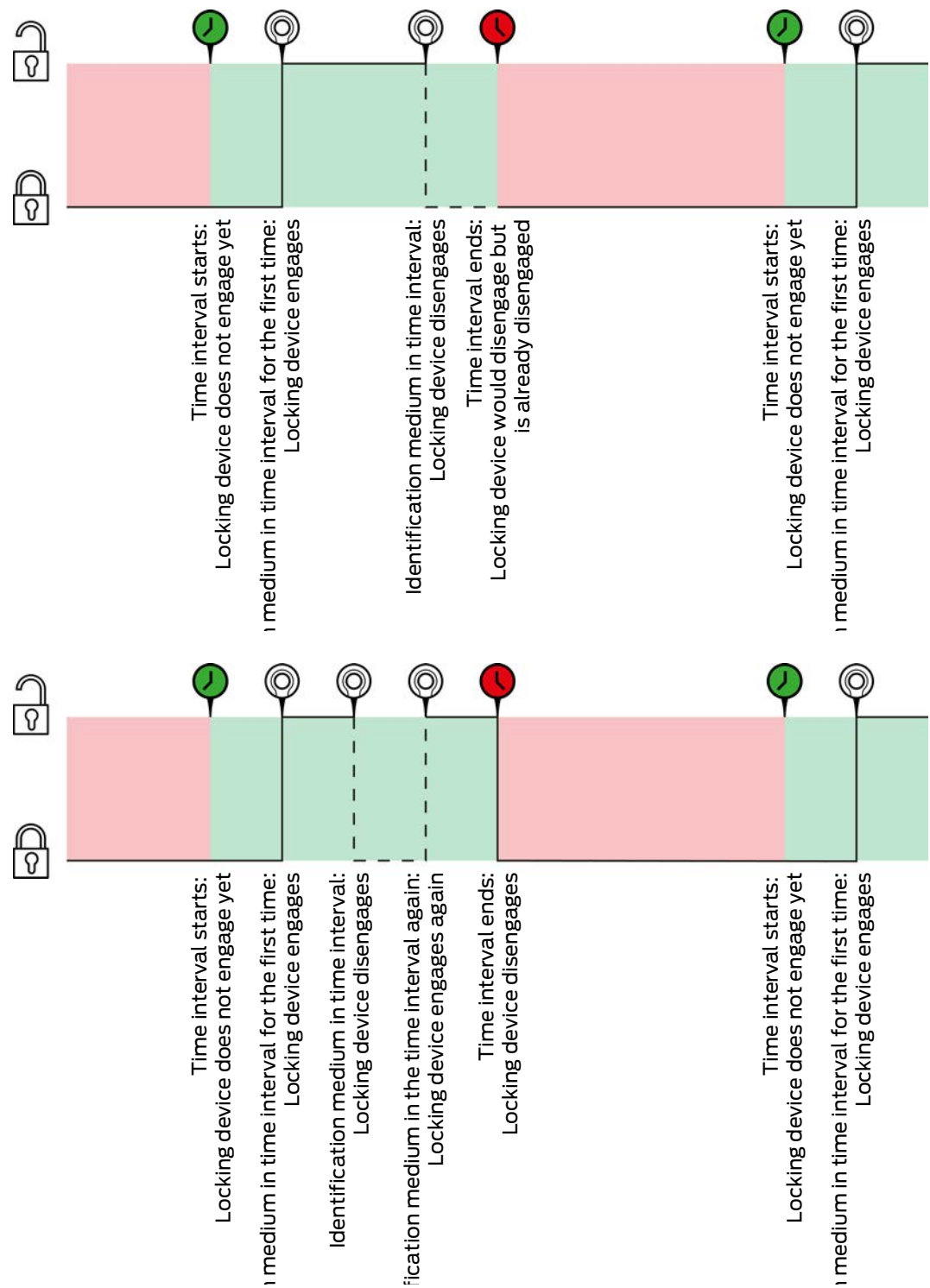




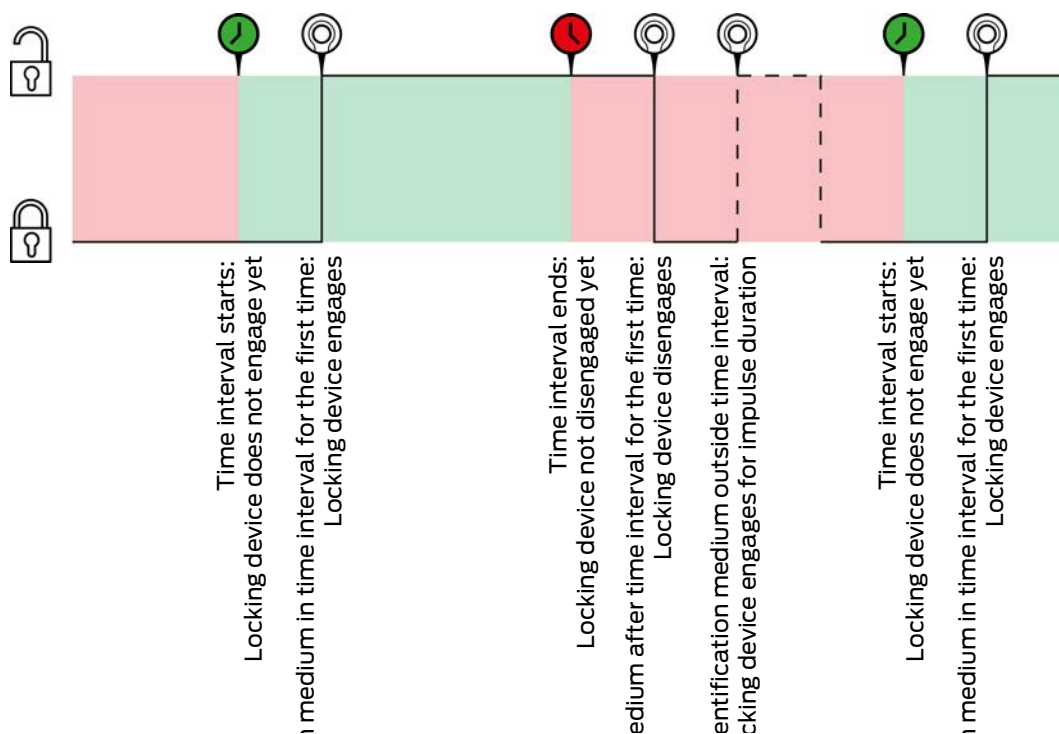
Manuelles Einkuppeln, Automatisches Auskuppeln



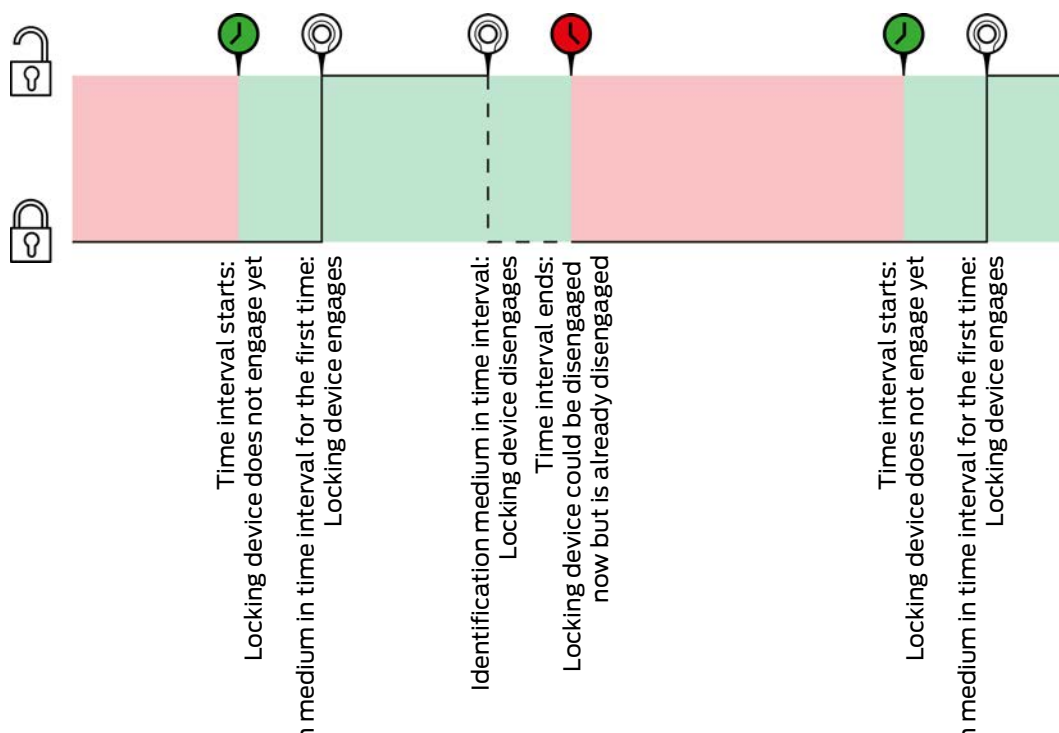
The Transponder aktiv: immer option must be selected for the two following examples as, otherwise, the identification medium cannot be activated within the time interval.

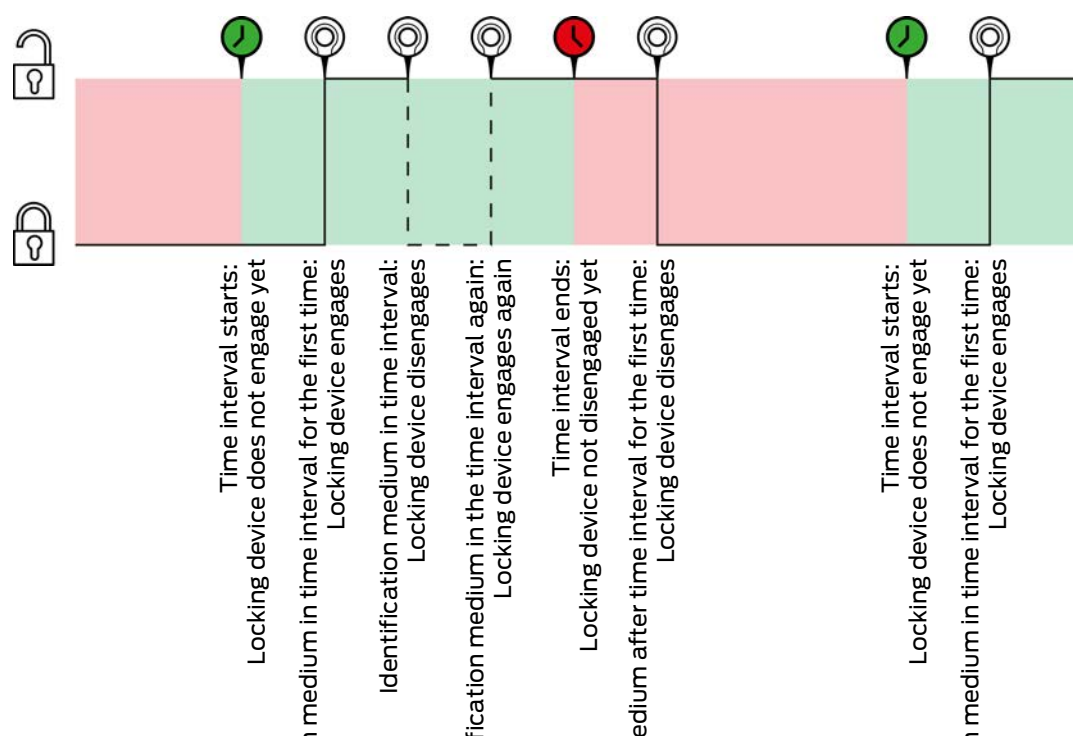


Manuelles Einkuppeln, Manuelles Auskuppeln



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.





24.7.3 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 topping up, the system checks whether authorisation changes have been made or whether the identification medium has even been blocked.

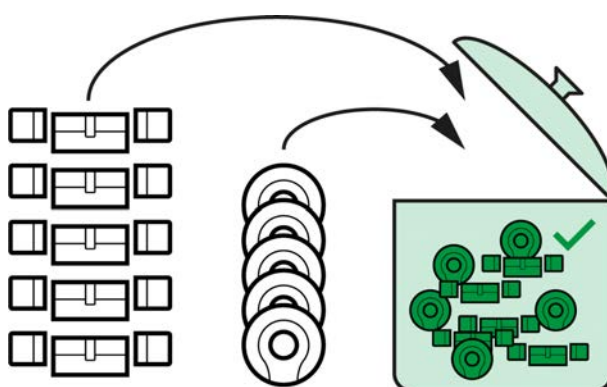
	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Adjustability	■ Max. 30 days since last top-up ■ Adjustable to the exact day	■ Max. 255 hours (approx. 10 days) or ■ up to a given time from topping up (e.g., from topping up until 8 p.m.) ■ Adjustable to the exact hour
Topping up through	AXM service. 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.	Virtual network gateways

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Top-up frequency	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. 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.	The time budget is topped up again once the identification medium is activated at the gateway, provided it has not been blocked.
Intended purpose	A smartphone could be set to flight mode and thus the connection to the AXM service could be intentionally interrupted. In this case, a change in authorisation 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. This prevents flight mode from being misused and inadvertently use a permission permanently.	In the virtual network, “Dynamic time window” performs two tasks: 1. Forcing identification media to go to gateway 2. Time limitation of authorisation in the event of lost identification media 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. After deactivation (for example, following its loss), a stolen identification medium may not be utilised beyond the set time limit. Wholly independent of whether the deactivation was carried out at the locking device. The stolen identification medium’s time budget can no longer be renewed and thus expires.

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Example (normal operation)	Example: time budget set to 30 days. A user's AX2Go is connected to the AXM service via the cloud. Since the user is still authorised, the time budget is renewed to the full 30 days. The locking system administrator closes their laptop and goes on vacation for three weeks. 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. After the locking system administrator returns, they restart their laptop. The AXM service connects to the cloud and the user's time budget is topped up. The user's AX2Go functions uninterrupted at all times.	Example: Budgeted time set at 10 hours. 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. The user may subsequently use their identification medium for 10 hours. They then activate their identification medium again at the gateway and receive a new time budget.

	AX2GO: Offline time budget (in days)	Virtual network: Dynamic time window
Example (problem)	Example: time budget set to 7 days. 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. The AX2Go can no longer establish a connection to the cloud, so the time budget of the user concerned is no longer renewed. 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.	Example: Budgeted time set at 10 hours. An identification medium is reported as stolen and is subsequently deactivated by the locking system administrator. Over time, the blocked IDs are distributed to the locking devices in the virtual network. However, some more remote locking devices have still not received a blocked ID ten hours later. However, the stolen identification medium can no longer be used on these locking devices. The time budget has expired and there will be no renewal due to deactivation.

24.8 Access levels



Access levels are available for the first time with the introduction of AXM Plus.

The principle of an access level is very simple, similar to a melting pot. Within an access level, all locking devices are normally authorised on all identification media.

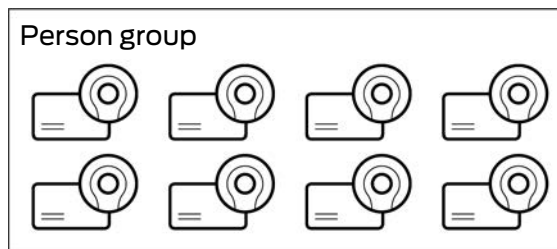
We say “normally” because you can also manually remove authorisations from individual identification media. This gives you full freedom to decide on authorisations, but you can do most of the work in an access level.

Identification media and locking devices can be assigned to a number of access levels.

Access levels are an organisational component. Ideally, you should set up your access levels before your locking devices and identification media (see *Best practice: setting up the locking system* [▶ 37] and *Creating access levels* [▶ 60]).

24.9 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 access levels* [▶ 349])
- Matrix structure
- Moving identification media to another person group at a later date (see *Assigning persons to person groups* [▶ 209])

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* [▶ 37] and *Creating a person group* [▶ 61]).

**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

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

✕			✕	✕

				✕

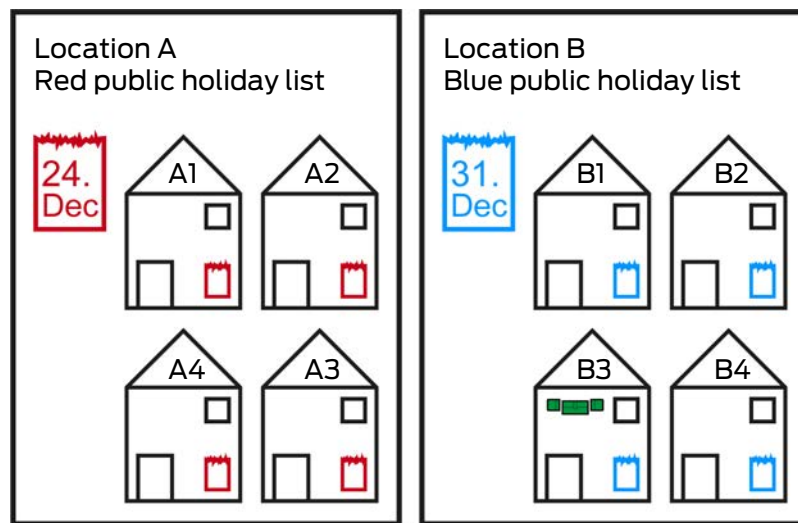
Matrix with person groups

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

24.10 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.

24.11 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* [► 37]) (see *Creating a location* [► 87] and *Creating a building and assigning it to a location* [► 90]).

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).

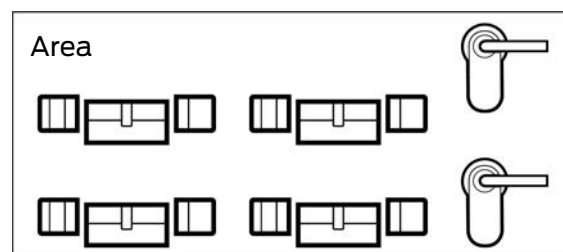
The public holiday lists are particularly interesting for time-controlled locking devices. Locking devices are conveniently always assigned to a building, which in turn is assigned to a location (mandatory information). Assigning a public holiday list to each locking device is a laborious task. Instead, 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)* [► 299]). 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.

24.12 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 access levels* [► 349])
- Moving a locking device to another area at a later date (see *Moving locking devices to areas* [► 293])
- Assigning a schedule to an entire area instead of individual locking devices (see *Add area, including locking devices, to a schedule* [► 363])

Areas are an organisational component. Ideally, you should set up your areas before the identification media (see *Best practice: setting up the locking system* [► 37] and *Creating an area* [► 93]).

**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...		⊖	

24.13 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

24.14 Networking**24.14.1 Virtual network**

The virtual network is an alternative to a direct wireless connection of your locking devices to the WaveNet (see *WaveNet* [▶ 618]).

Benefits of the virtual network

Instead of using the programming device to go to locking devices or identification media, you can use the virtual network to carry out the following tasks and others from a convenient location:

- Writing authorisation changes on identification media (*Example: authorisation change [▶ 611]*)
- Blocking of identification media transferred to your locking devices (*Example: loss of transponder [▶ 616]*)

Identification media as data carriers instead of radio

Normally, people enter a building at a few centrally located entrances. For example, a sliding entrance door. The identification media of these persons are therefore very often used at the entry terminal at this entrance door.

There is also usually still some free memory space on the identification media.

You can take advantage of these characteristics with the virtual network. To do so, connect the locking device at the entrance door directly to the database of your AXM Plus. This entry terminal thus becomes a  Gateway.

When you block an identification medium, a blocked ID is created and stored in the database.

A person now wishes to enter the building and therefore activates their identification medium at your gateway. At this point, the gateway checks if the database has any info that must be available around the building and locates the blocked ID. The gateway writes the blocked ID to the identification medium.

The person who has entered the building will open multiple doors during the course of the day and thus operate their identification medium with the blocked ID at different locking devices. The identification medium transmits the blocked ID to each of these locking devices and in return receives confirmation that the blocked ID has also been delivered.

The next time the person operates their identification medium on the gateway, the gateway reads the confirmations and saves the information that the blocked ID has also been delivered to the locking devices concerned.

All types of virtual networks require an AV card template when using cards (AV = audit trail/virtual network).

Information transmitted in the virtual network

- Blocked IDs

(Maximum of two per identification medium. When there are more blocking IDs in the database, a random selection will take place.)

If you create a substitute transponder, the blocked ID of the blocked transponder is automatically assigned to it.

- Blocking confirmations

(A blocking confirmation serves as validation that a locking device has received a blocked ID.)

- Locking device battery levels

- Card's physical access list (function not supported by transponder)

- Assigning/changing time groups

- Assigning/changing time budgets

Authorisation changes are not transferred; instead, they are changed directly on the identification media concerned by the gateway.

Dynamic time window (time budget)

The more frequently identification media are used at the gateways, the more effectively the virtual network works. The entrance sliding door might need to remain open permanently during opening hours. From a user perspective, there is therefore no compelling reason anymore for users to present their identification media at the gateway. The door is already open.

You can limit the validity of identification media so that they have to present them. After this time has elapsed, validity at the gateway must be renewed. The duration may be specified, either by the hour (e.g., 8 hours from topping up) or until a fixed time (for example, after charging until 5:00 p.m.).

The advantages of a dynamic time window are:

- Persons with identification media are forced to go to the gateway at regular intervals. This improves the virtual network's function.

- Blocked identification media will, of course, not receive a new time budget.

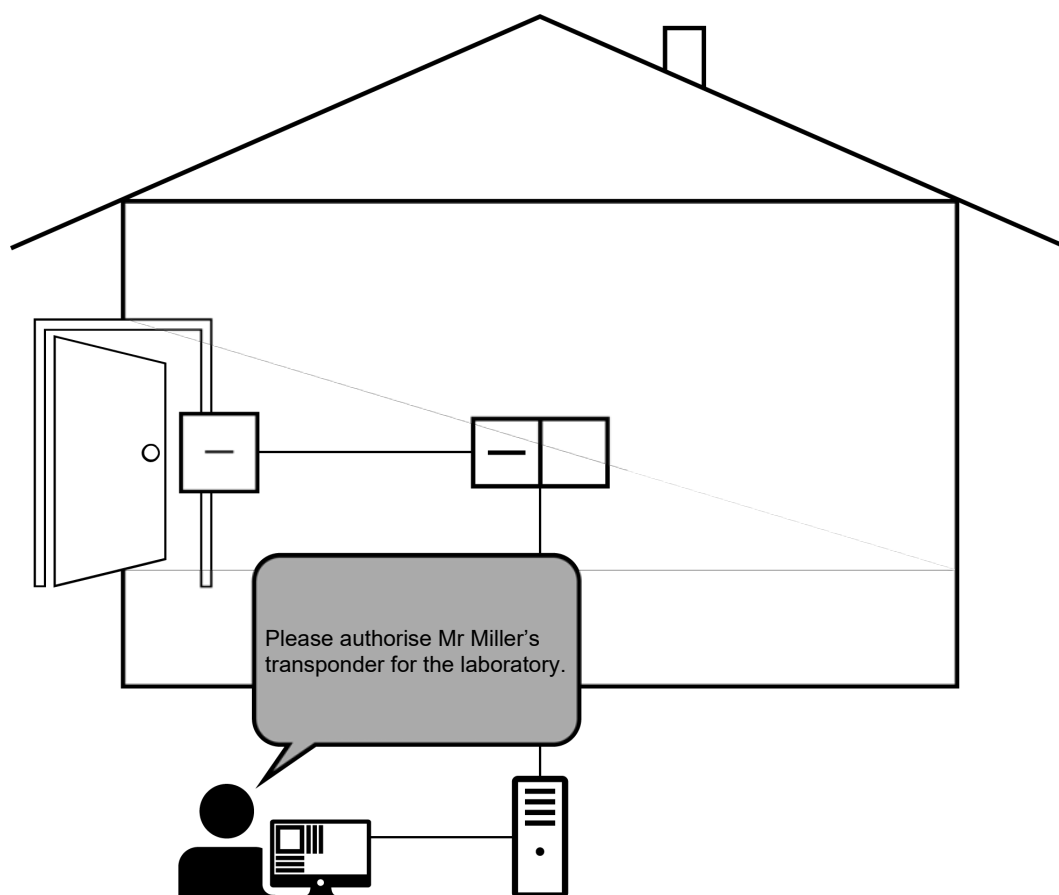
This means that stolen and blocked identification media can no longer be used after the time budget has expired, even if the thief deliberately does not go to the gateway.

If you do not introduce the time budget in your virtual network until a later date, you can also write this change directly to the identification media using the virtual network. You do not need to explicitly program each identification medium individually. The prerequisite is that all identification media go to the gateway; otherwise, the change cannot be written onto the identification media.

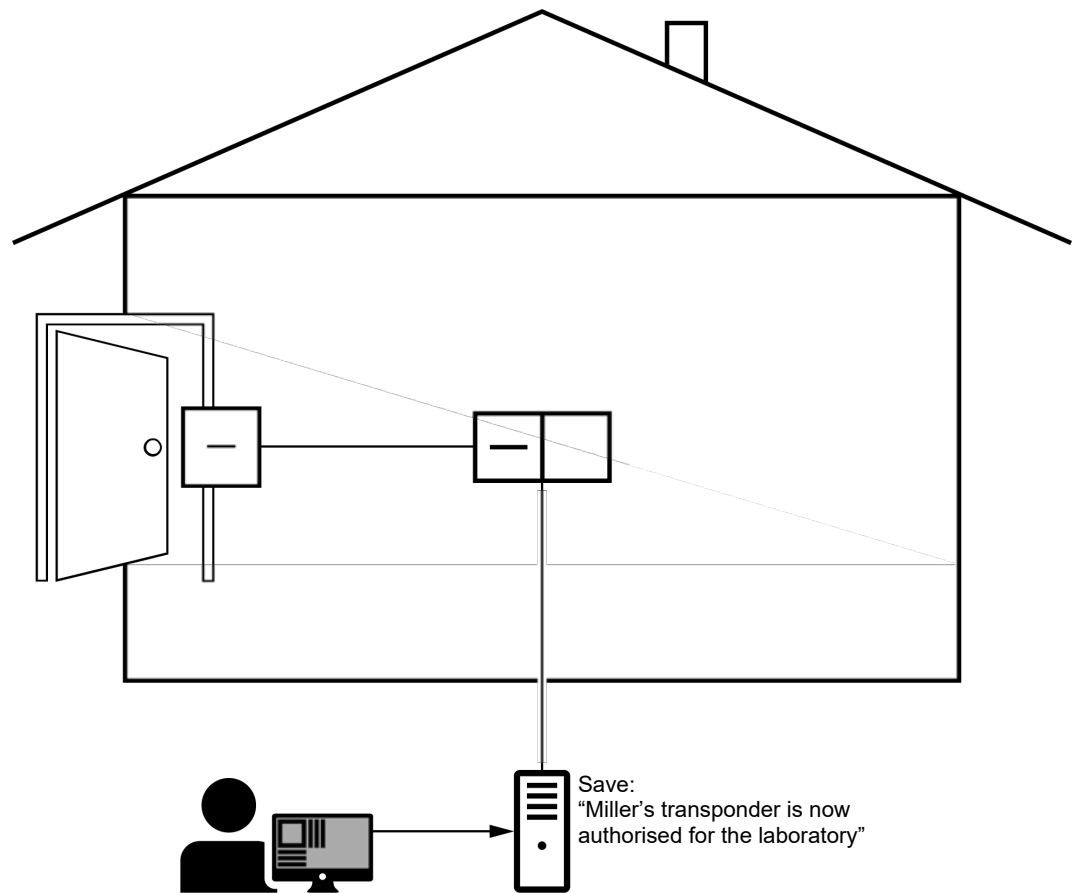
24.14.1.1 Example: authorisation change

Mr Miller has been promoted and will continue to work in the laboratory in the future. In our scenario, Mr Miller will pass by the entrance door, where the gateway will write his new authorisation to his transponder.

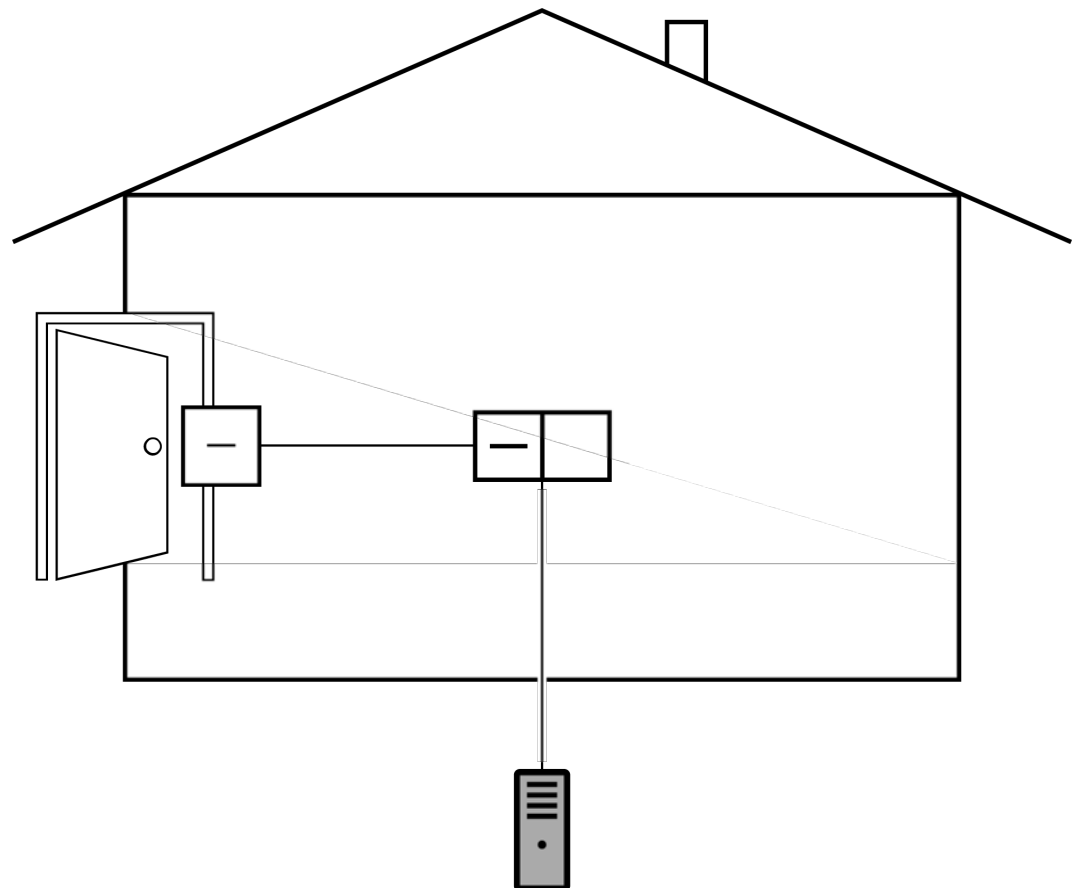
This means that Mr Miller can then also enter the laboratory.



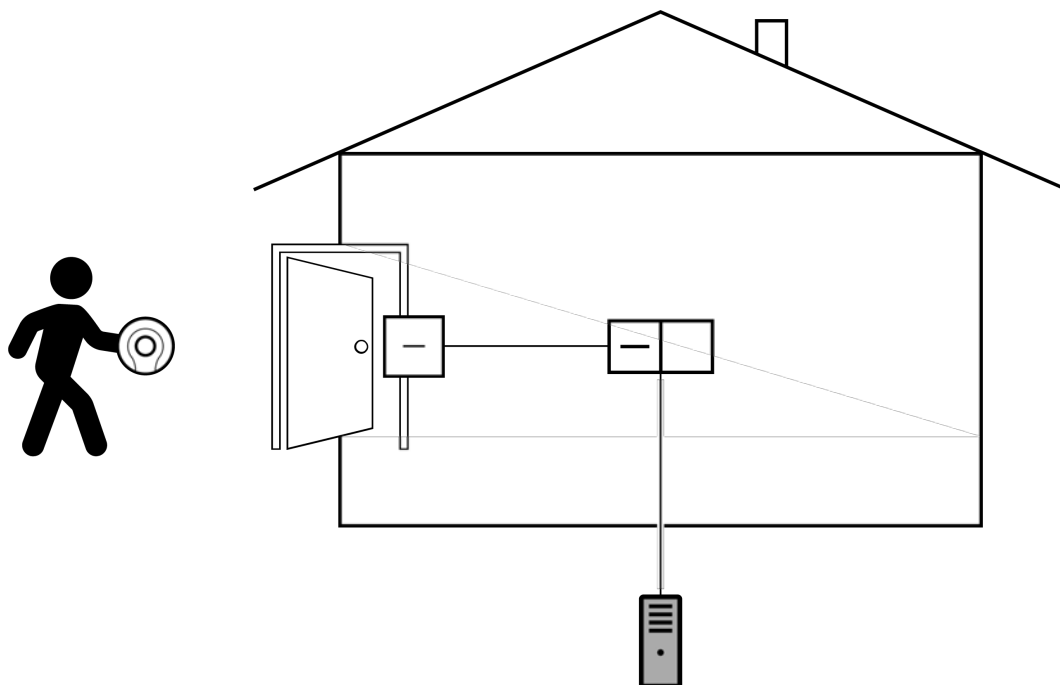
The locking system administrator has been informed of Miller's promotion and issues him with authorisation for the laboratory.



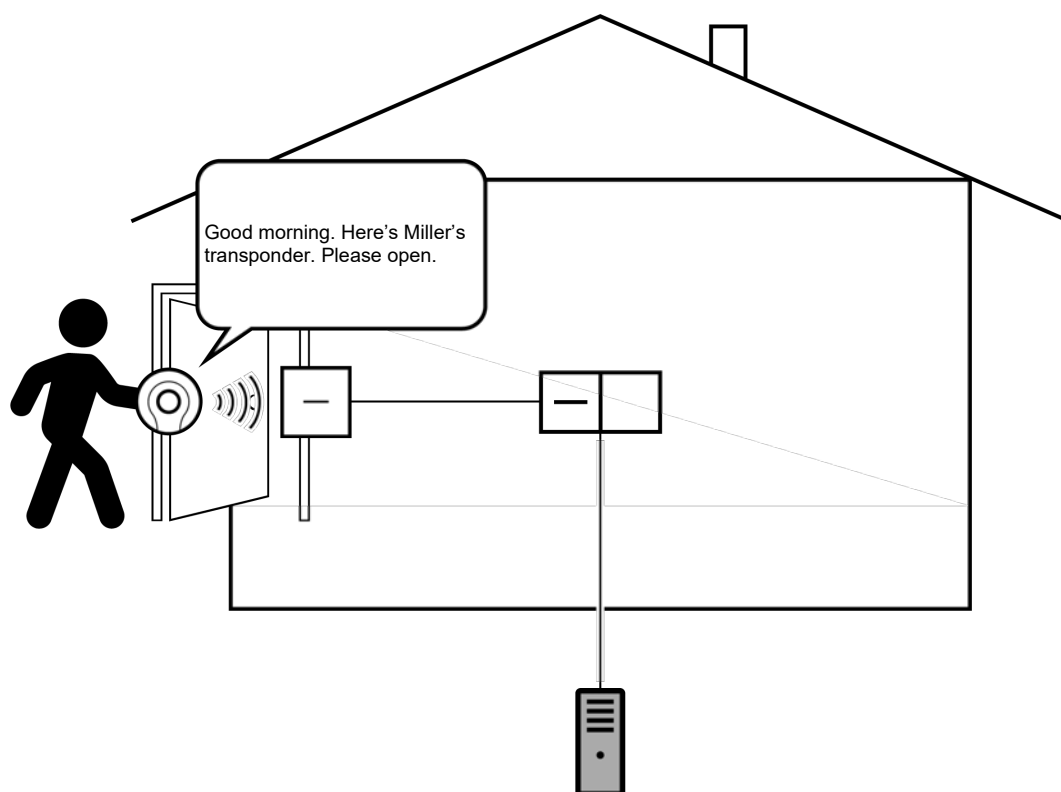
The AXM Plus saves the new authorisation for "Miller" in the database.



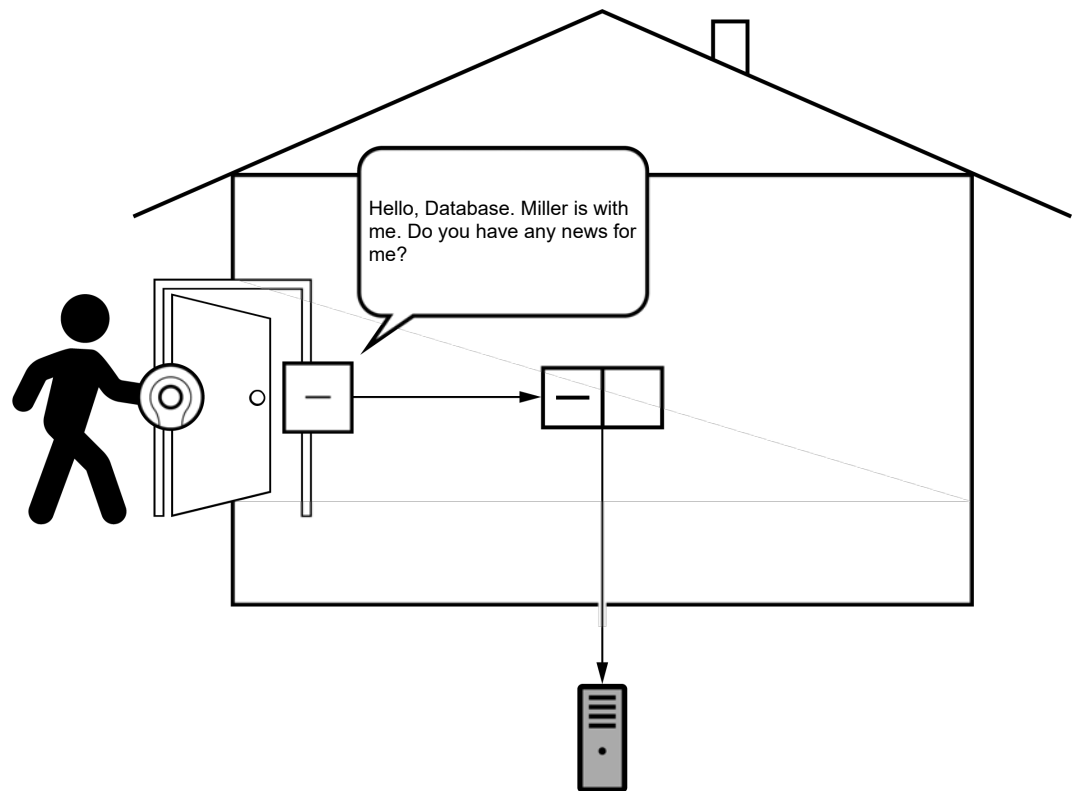
The locking system administrator shuts off his computer and leaves the building. The new authorisation for “Miller” remains saved in the database.



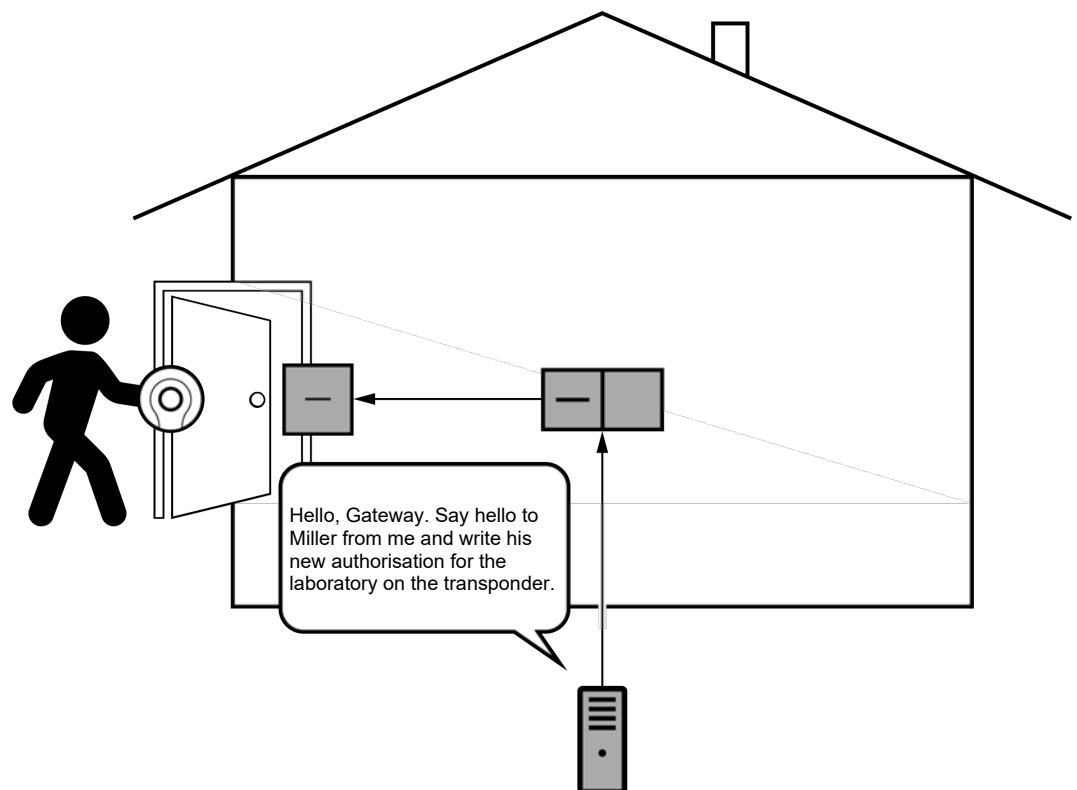
Mr Miller comes to the building with his transponder and wants to enter through the entrance door.



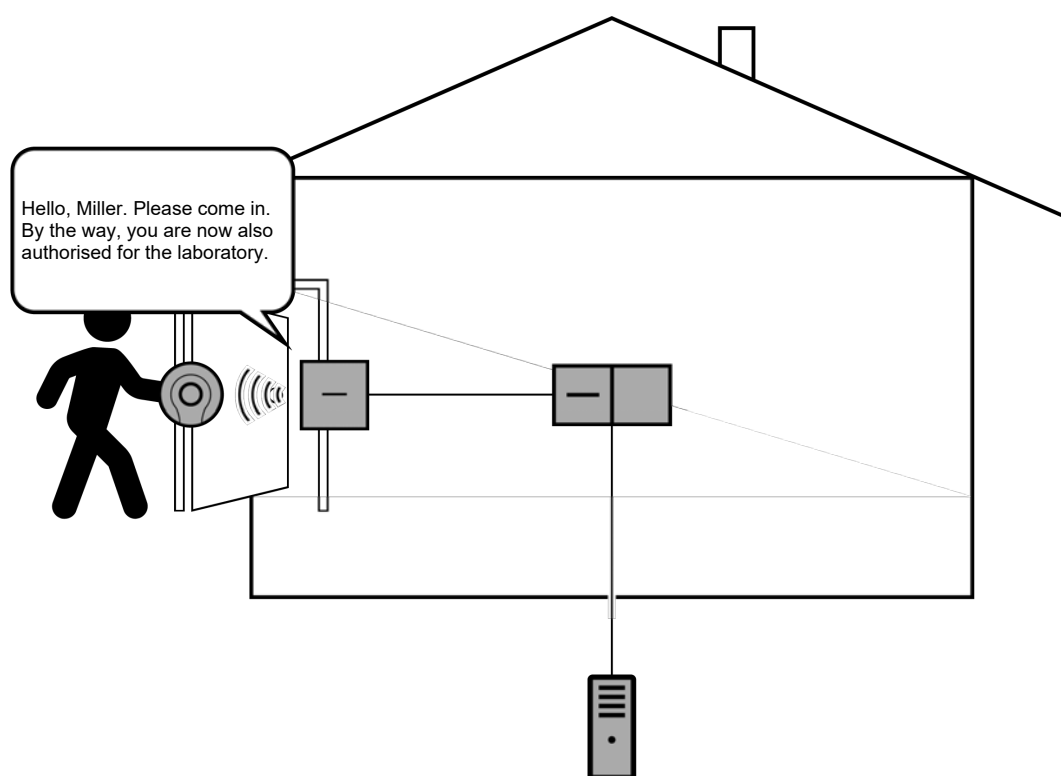
Mr Miller presents his transponder at the entrance door to access the building. The transponder communicates with the gateway.



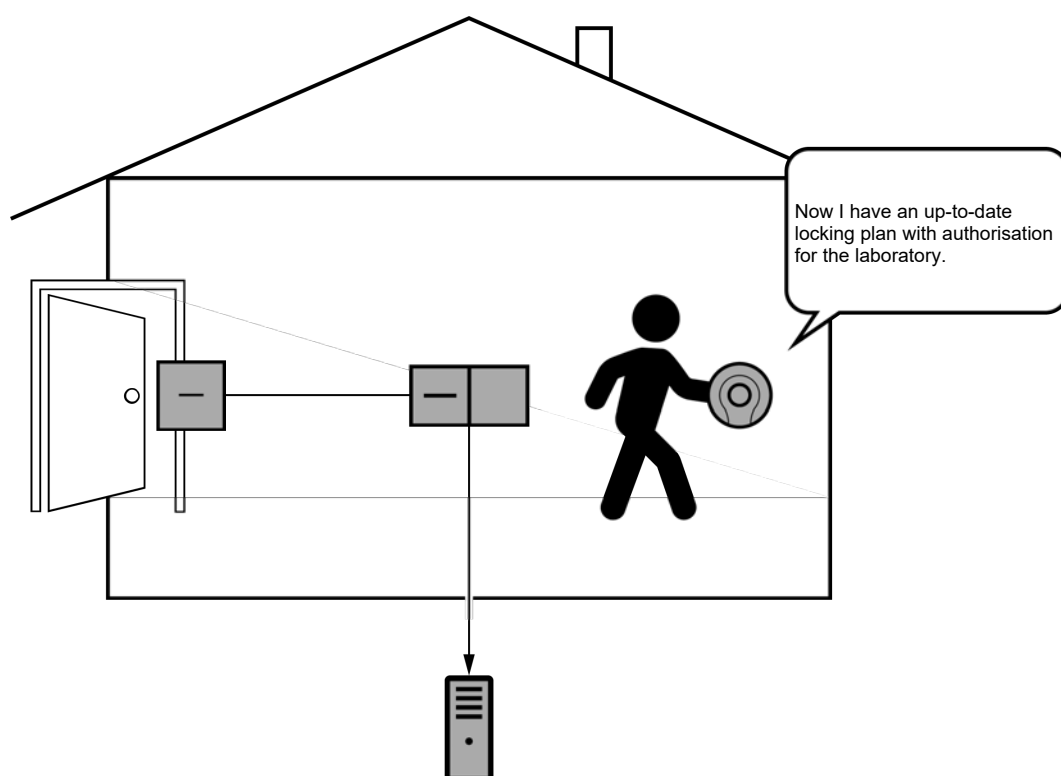
The gateway reports to the database that Mr Miller is currently on site and asks whether any information needs to be transferred.



The database informs the gateway that there is a new authorisation for "Miller".



The gateway opens the door and gives Mr Miller's transponder an up-to-date locking plan with authorisation for the laboratory.



Thanks to the new locking plan and the G2 protocol, Mr Miller's transponder can now also open the locking device in the laboratory.

Mr Miller can enter the laboratory without the locking system administrator needing to take the programming device to Mr Miller's transponder or to the laboratory locking device.

24.14.1.2 Example: loss of transponder

In this example, we see the lost transponder belonging to Mr. Maier is blocked in a partially networked system, and the blocking is confirmed by the locking devices.

Synopsis of the example

1. The admin blocks the lost transponder.
2. The AXM Plus stores a blocked ID in the database.
3. Another person (Ms. Schneider) enters the building through the entrance door.
4. The gateway checks if the database contains current information for Ms Schneider's transponder.
5. The database informs the gateway that a blocked ID exists for 'Maier'.
6. The gateway transfers the blocked ID for "Maier" to Ms. Schneider's transponder.
7. Ms Schneider's transponder transmits the locked ID for "Maier" to a SmartHandle AX where it is activated.
8. The SmartHandle AX confirms to the transponder that it has blocked "Maier".
9. Ms. Schneider's transponder transmits the blocked ID for "Maier" to other locking devices and also receives confirmations.
10. Ms. Schneider leaves the building through another door. Your transponder informs the gateway that the blocking for "Maier" has arrived at SmartHandle AX and at the locking cylinder.
11. The gateway transfers this information to the database.
12. The admin sees that "Maier" has been blocked on SmartHandle AX and on the other locking devices.

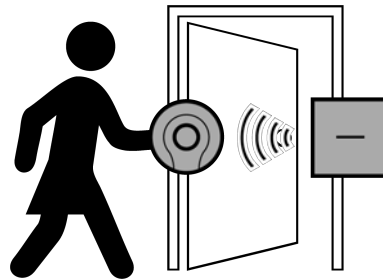
1. Part: Blocking in AXM Plus, transmission to gateways and networked locking devices

The admin has learned of the loss and blocks the transponder in the AXM Plus. A blocked ID is created in the database for the "Maier transponder".

The AXM Plus saves a blocked ID for "Maier" in the database. As the system is partially networked, the transponder is immediately blocked at critical external doors (that are networked via WaveNet or Ethernet).

Even after the admin computer has been shut down, the blocking information remains in the database.

Part 2: Transmission to transponders and propagation within the building

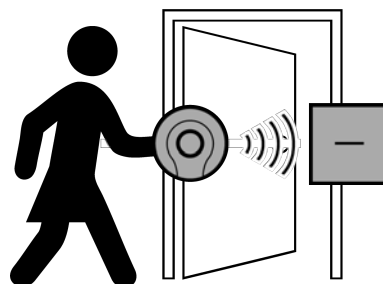


Later, when Ms. Schneider opens an outside door with her transponder SmartRelais 3 Advanced, her transponder also receives the information that Mr. Maier's old transponder is now blocked throughout the entire locking system.

Ms Schneider continues to her department and presents her transponder to open the door. In doing so, she informs the installed SmartHandle AX that "Maier" is blocked. The SmartHandle AX stores the confirmation that it has received the information on the transponder. During the course of the day, Ms. Schneider passes by other doors. They also receive the information about the blocking and confirm it.

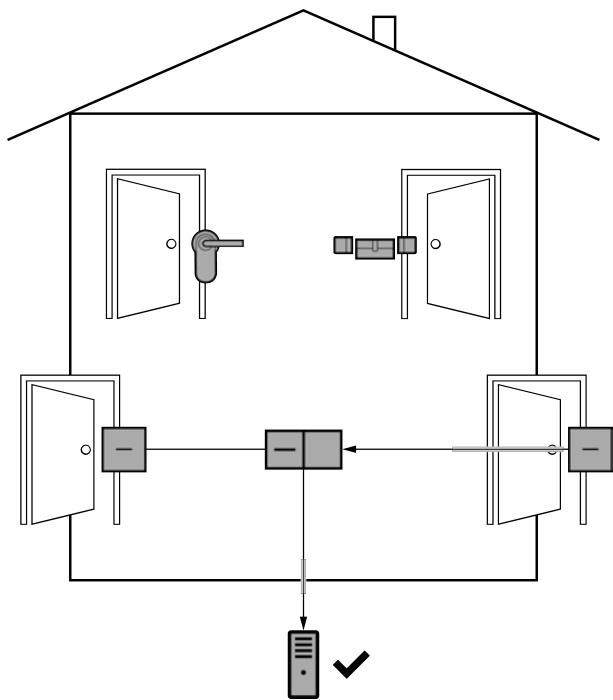
Part 3: Returning the blocked IDs back to the database

At the end of the day, Ms Schneider leaves the building and swipes her transponder at another gateway to access the underground car park. The transponder communicates with the gateway once again and informs that the blocking of "Maier" has now been received by the SmartHandle AX and the locking cylinder.



The gateway notifies the database that the Schneider transponder was just there and to which locking devices the blocked ID was transmitted.

The next time the AXM Plus is opened, the administrator can see which locking devices have already been notified about the blocking and which doors must still be notified.



Additional information

Naturally, the locking system administrator also has a transponder that can carry blocked IDs. The administrator no longer needs to bring a laptop or programming device to the not-blocked locking devices; they can conveniently use their personal transponder, just like Ms Schneider. As the blocked IDs are transferred to the locking devices regardless of authorisations, this method is effective even if the transponder does not have authorisation for the specific door.

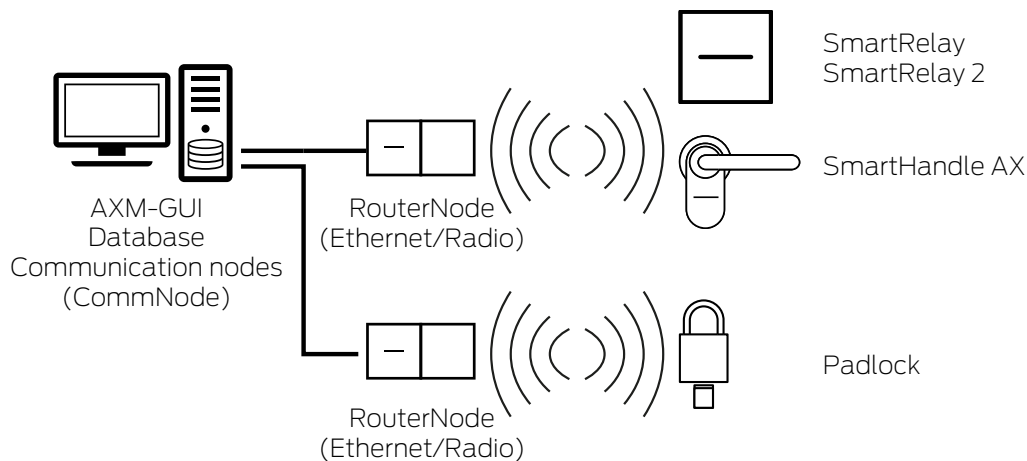
24.14.2 WaveNet

You can network SimonsVoss locks (Locking cylinders, SmartHandles, SmartRelay and SmartLocker AX) in several ways and manage them centrally. WaveNet is the most advanced and convenient way to manage and monitor large locking systems with many locking devices.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Functional principle	Data transmission with networked WaveNet devices.	Data transmission via identification media (except programming data).	Data transmission with programming devices.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Extension	WaveNet devices are linked via various transmission media. All types of data are transmitted using these transmission media.	In the virtual network, specific data is transferred to the identification media via a gateway. When you activate this identification media on a virtual network locking device, the data is transferred to the locking device.	Locking devices that are not networked can only exchange data with the programming device. You must go to the locking devices with the programming device.
Programming effort	Low.	Low.	The expenditure depends on the complexity of the locking system. ■ Small locking system: low complexity. ■ Medium locking system: medium complexity. ■ Large locking system: high complexity.
Transmission speed of the data exchange	Immediate. Data exchange with different transmission media.	Speed between gateway and locking devices highly dependent on the intensity of use of the locking devices. Identification media are data transmission media - no data transmission without identification.	Slow.
Central activation/deactivation of locking devices	Possible.	Not possible.	Not possible.
Activation/deactivation centrally traceable	Possible.	Not possible.	Not possible.
Remote opening	Possible.	Not possible.	Not possible.

	WaveNet (online)	Virtual networking (virtual)	No networking (offline)
Event management	Possible.	Not possible.	Not possible.
Access lists centrally retrievable	Possible.	Not possible (except SREL 3).	Not possible.



WaveNet is a proprietary network that you may install and use in building automation with just a few cables. If you want to retrofit WaveNet, you can also use existing building networks such as a LAN. This is why WaveNet is not only suitable for equipping new buildings with a locking system (e.g. for room units with flexible use). WaveNet is particularly suitable for managing and controlling your existing SimonsVoss 3060 locking system online in existing buildings.

As an alternative to full networking, you can freely combine different networking types. For example, you can connect the doors of the outer shell (i.e. the building envelope) and critical locking devices (e.g. on server room doors) to your WaveNet, as well as all other locking devices.



NOTE

WaveNet training and planning

WaveNet is a comprehensive solution that can be very well tailored to your requirements. If you want to fully exploit the potential of your WaveNet, you can attend a SimonsVoss Technologies GmbH WaveNet training course. You can also plan your WaveNet project together with a SimonsVoss technician and benefit from their many years of experience.

24.14.3 CommNode and VNHost

Your AXM Plus includes two different services that are automatically installed. Web apps for configuring these two services can be opened via the Start menu:



	CommNode	VNHost
Intended purpose	The CommNode connects your networked locking devices to the database of your AXM Plus. Example: You start the AXM Plus synchronisation of a locking device via the network. The programming task is sent from the AXM Plus to the CommNode. The latter is aware of how the relevant locking device can be accessed via the network and sends the programming command to the locking device via the appropriate RouterNode. You need the CommNode, for example, for: ■ Programming your locking devices via WaveNet ■ Retrieving battery levels or access lists via WaveNet ■ Virtual network (to connect your gateways to the database)	The VNHost permits your gateways to query your database for information regarding the current identification medium. AXM Plus. You need the VNHost for the virtual network. Once a gateway has recognised an identification medium, it must be able to query the database to determine if information is available for this identification medium. Such information may include a blocked ID, for example. For more information on the features of the virtual network see Virtual network [► 608].

	CommNode	VNHost
Number of projects	The CommNode is used in all projects at the same time. It only needs to be connected to your AXM Plus database (see <i>CommNode set up</i> [► 451]).	The VNHost can only be assigned to one project. If there is more than one project in the database, one of them must be selected and connected to VNHost during setup (see <i>Configure of VNHost</i> [► 452]).

24.15 Reports

24.15.1 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* [► 493]).

You can insert your own logo here, for example.

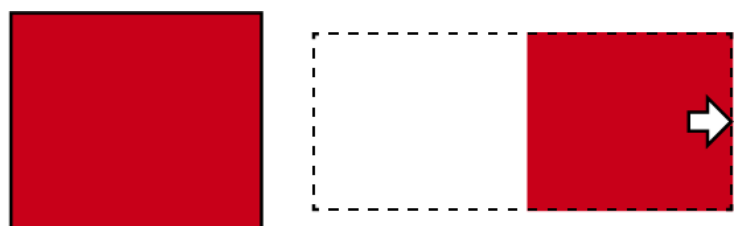
You can freely select the image file. A specific box is provided for your image files in exported reports. AXM Plus automatically scales your images to fit into the box:

Image too narrow and too low



The image is enlarged in proportion and aligned to the right in the box.

Image too high



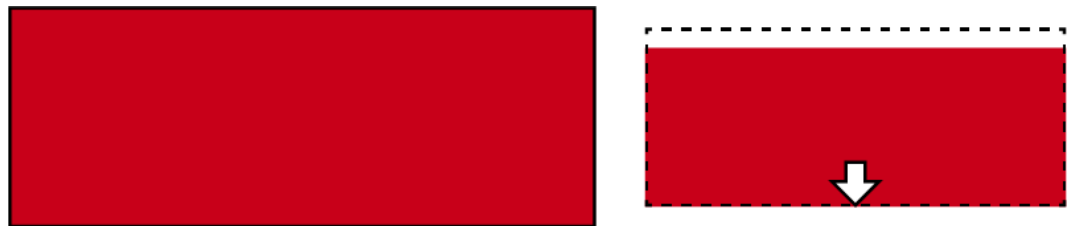
The image is made smaller in proportion and aligned to the right in the box.

Image too wide



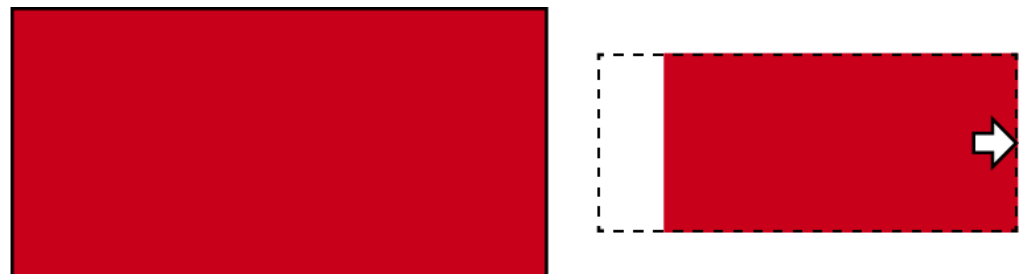
The image is made smaller in proportion and aligned with the bottom of the box.

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.

24.16 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:

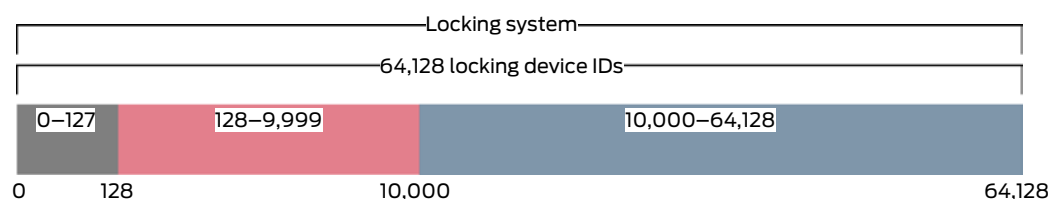
- Short range (a few millimetres)
- Less memory space

It is especially important to take the small memory space into account.

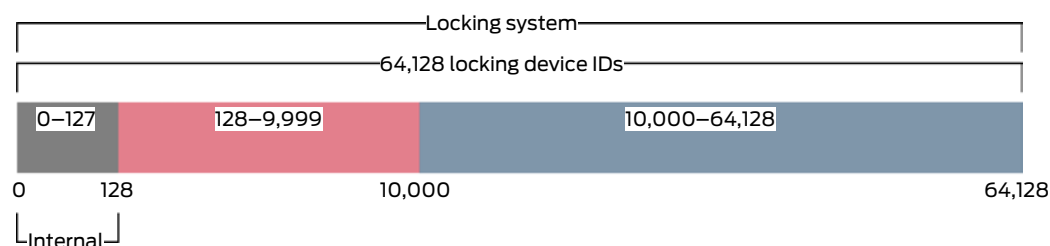
Distribution of locking device IDs in AXM Plus

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.

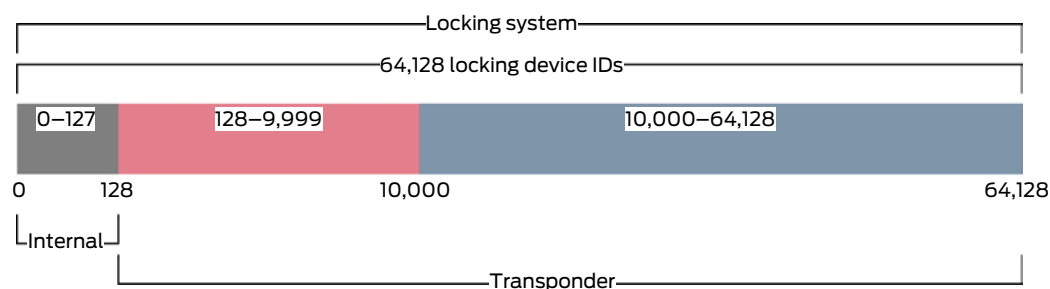
There are 64,128 locking device IDs (0 to 64,128) in an active locking system.



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 \[► 628\]](#) and [Adding a card configuration \[► 372\]](#)). 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.

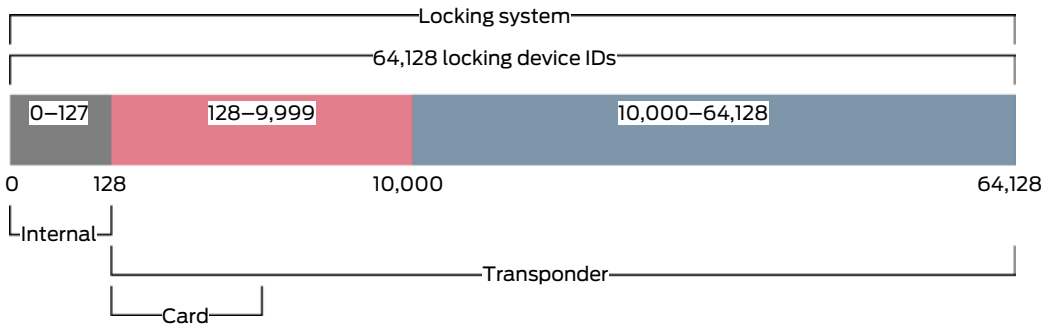
Cards can only be used in conjunction with a card template. Card templates differ in a number of characteristics but the most important ones are quite clear:

- ❑ 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
KartentypMifare Classic KonfigurationMC1000L_AV Speicherbedarf528 Bytes Schließungs-IDs128 - 1127 im Kartenprofil Begehungen im Protokoll19 Virtuelles NetzwerkOK ❑ 528 bytes ❑ Locking device IDs 128 to 1127 (= 1000 entries)	KartentypMifare Classic KonfigurationMC8000L_AV Speicherbedarf2048 Bytes Schließungs-IDs128 - 8127 im Kartenprofil Begehungen im Protokoll125 Virtuelles NetzwerkOK ❑ 2048 bytes ❑ Locking device IDs 128 to 8127 (= 8000 entries)

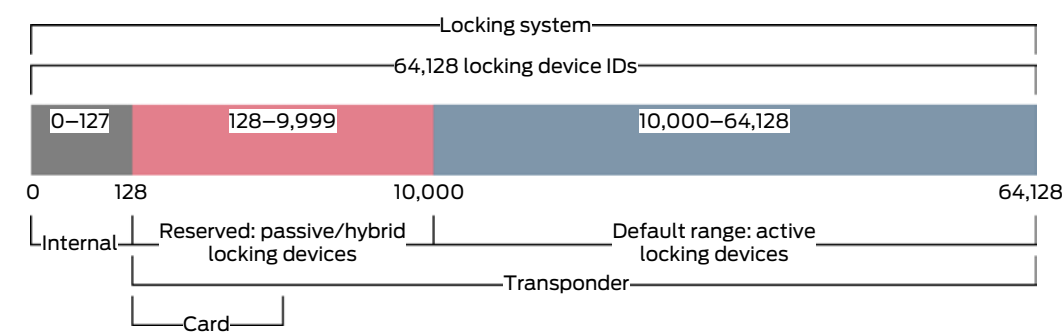
It is evident that cards in the entire range for locking device IDs can only address the lower locking device IDs in the lower section.



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
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. As soon as a locking device ID is free in the lower range once more (e.g. locking device reset; see Reset [▶ 287]), it is exclusively assigned a passive or hybrid locking device again.	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. As soon as a locking device ID is free in the upper range once more (e.g. locking device reset; see Reset [▶ 287]), it is exclusively assigned an active locking device again.

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

 Neu

 Löschen

 In Matrix anzeigen

 Duplizieren

 Batteriewechsel

 Export

 Anzeigefilter löschen

Hogwarts 1

Tür	^ v	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	000DSP7E	128
Hufflepuff tower				🔒			14.12.2021 16:58:30	000E04GX	10000
Stadium illumination				🔒			14.12.2021 18:52:36	000ENB4L	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](#) [▶ 407]). 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.

24.16.1 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	✓

Configuration	G1/G2	Lock IDs	Number of locking devices	Physical accesses in the log	Sectors	Memory requirements (Bytes)	Virtual Network
M8000L_AV	G2	128-8127	8000	124	2-15 + 31-39	2048	✓
M10000L_AV	G2	128-10127	10000	225	2-15 + 31-39	3048	✓
MDBasic	G1	-	-	-	2-15	48	-
MD1200L	G2	128-1327	1200	-	2-15	192	-
MD3800L	G2	128-3927	3800	-	n.a. (DES-Fire)	528	-
MD2500L_AV	G2	128-2627	2500	58	n.a. (DES-Fire)	1024	✓
MD4000L_AV	G2	128-4127	4000	100	n.a. (DES-Fire)	1600	✓
MD10000L_AV	G2	128-10127	10000	225	n.a. (DES-Fire)	3048	✓
MD32000L_AV	G2	128-32127	32000	470	n.a. (DES-Fire)	7000	✓
MD2400L_AV	G2	128-2527	2400	34	n.a. (DES-Fire)	830	✓
MD3650L_AV	G2	128-3777	3650	2	n.a. (DES-Fire)	830	✓

25. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

Software and drivers

Software and drivers can be found on the website:

<https://www.simons-voss.com/en/service/software-downloads.html>

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

<https://faq.simons-voss.com/otrs/public.pl>

Address

SimonsVoss Technologies GmbH
Muenchner Str. 16
D-85774 Unterfoehring
Germany



This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 2026, 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

