

AXM MANAGER

The next dimension of Locking System Management

AXM Lite
Short manual

Manual

12.07.2024

Simons Voss
technologies

Contents

1.	First steps after a new installation.....	4
2.	The AXM's structure	7
2.1	Sorting and filtering.....	9
3.	Organisational structure	12
3.1	Creating authorisation groups.....	12
4.	Persons and identification media.....	13
4.1	Creating an identification medium	13
4.1.1	Creating transponders and cards.....	13
4.1.2	Creating PIN code keypads	15
4.1.3	Creating special identification media.....	20
4.2	Deleting an identification medium.....	24
4.2.1	Deleting a PIN (PIN code keypad AX).....	24
4.3	Muting all locking devices for an identification medium.....	26
4.4	Duplicating forgotten identification medium temporarily	26
4.5	Blocking lost/stolen identification media permanently.....	26
4.5.1	Blocking and replacing lost/stolen card/transponder permanently.....	27
4.5.2	Blocking a lost/stolen PIN code keypad permanently	30
4.6	Flag and reset returned identification medium (back to inventory).....	35
4.7	Exporting identification media as a list.....	35
4.7.1	Exporting PINs and PIN code keypads as a list	35
4.8	Viewing an identification medium's serial number and/or TID	36
4.8.1	Viewing a PIN code keypad's serial number	36
4.9	Setting the PIN length (PinCode AX)	38
4.10	Changing a PIN (PinCode AX).....	41
5.	Doors and locking devices	44
5.1	Creating a locking device	44
5.2	Setting up door monitoring (DoorMonitoring)	49
5.2.1	Setting up DoorMonitoring for locking cylinders.....	50
6.	Permissions	57
6.1	Changing individual authorisations (cross)	57
6.2	Changing many authorisations (on identification media and/or locking devices).....	58
6.2.1	Allowing all or blocking all	58
6.2.2	Authorisation groups	59
6.3	Meaning of the authorisation crosses in the matrix	61
7.	Synchronisation: Comparison between locking plan and reality.....	63

7.1	Synchronising the locking device (including reading access list).....	64
7.2	Re-setting the locking device	66
7.3	Synchronising an identification medium.....	67
7.3.1	Synchronise a card/transponder (including importing physical access list)	67
7.4	Identifying an unknown ID medium.....	68
7.4.1	Identifying unknown PIN code keypad	68
7.5	Resetting identification media.....	70
7.5.1	Resetting cards/transponders.....	70
7.5.2	Resetting the PIN code keypad.....	73

1. First steps after a new installation

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

Willkommen bei AXM Lite (Beta)
Zum Starten melden Sie sich an ihrem Projekt an

Sicherung Wiederher. Fehlerdateien

Ein neues Projekt anlegen

Projektname

Benutzername

Neues Kennwort

Kennwort wiederholen

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

Qualität

Erstellen

Abbrechen

You will see the following input fields:

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

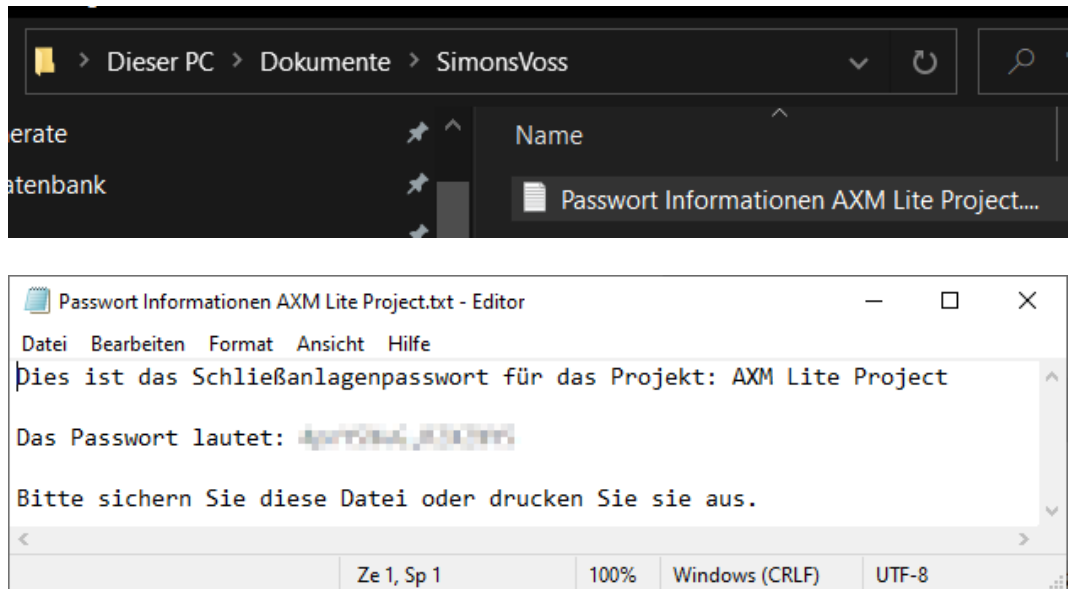
1. Enter a project name in the *Project name* field.
2. Enter a password of at least 8 characters in the *New password* field to protect your project.
 - ↳ A coloured bar shows you how secure your password is.

Quality

3. Repeat the password entered in the *Repeat password* field.
4. Click on the **Create** button.
 - ↳ The new project is protected.

You can change the user password you have just created if required (see Changing the user password).

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



You can change the locking system password (see Changing locking system password).

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 Classic for the first time

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

1. Add locking device
2. Add transponder

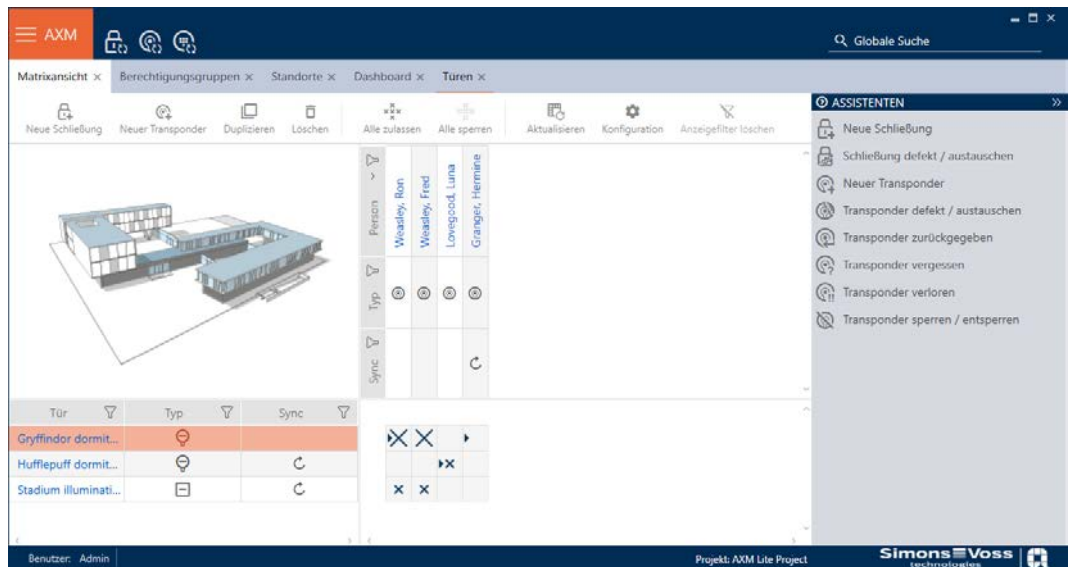


These wizards allow you to start building your locking system directly and familiarise yourself with the AXM Classic interface.

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

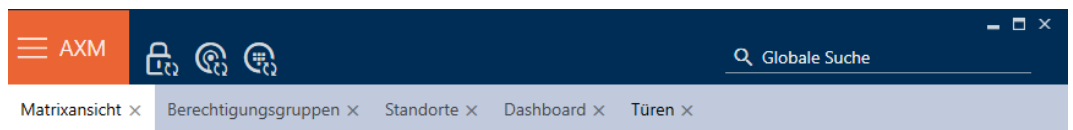
If you are working with a locking system for the first time, you will find explanations and background information here: [Background knowledge and explanations](#).

2. The AXM's structure



The AXM Classic 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).

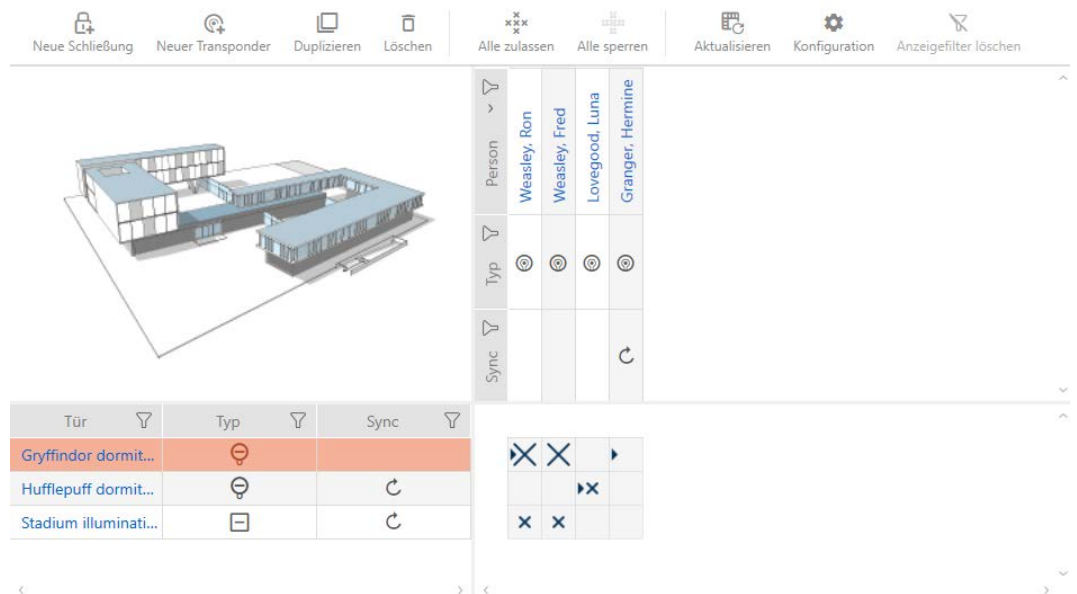
There are three buttons next to the AXM button to skip directly to synchronisation of locking devices and identification media.



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).



Matrix section



The matrix section is the engine room behind your AXM Classic. 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 \[▶ 9\]](#)).

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 \[▶ 57\]](#)). There are basically two different main states:

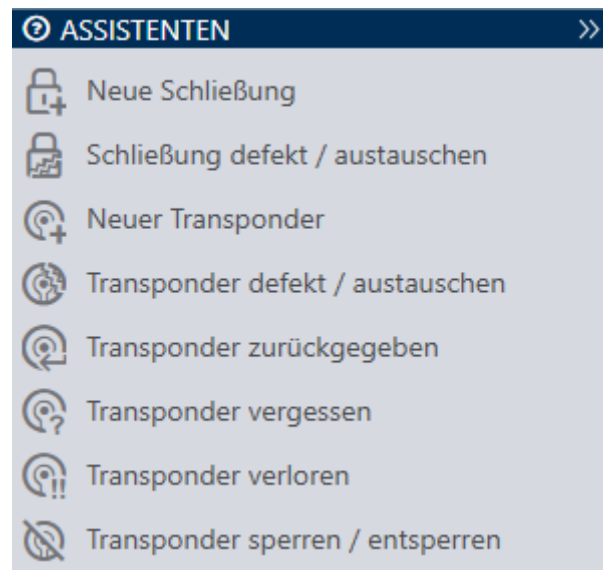
- Authorisation set (cross)
- No authorisation set (no cross)

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 \[▶ 63\]](#)). 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:



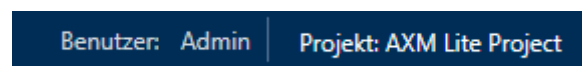
Wizard menu



There is a wizard menu on the right side of your AXM Classic. 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 Classic is the dashboard (see View statistics and warnings (dashboard)). 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)).

The log can also be accessed via the AXM bar.

2.1 Sorting and filtering


Large lists and tables can become confusing.

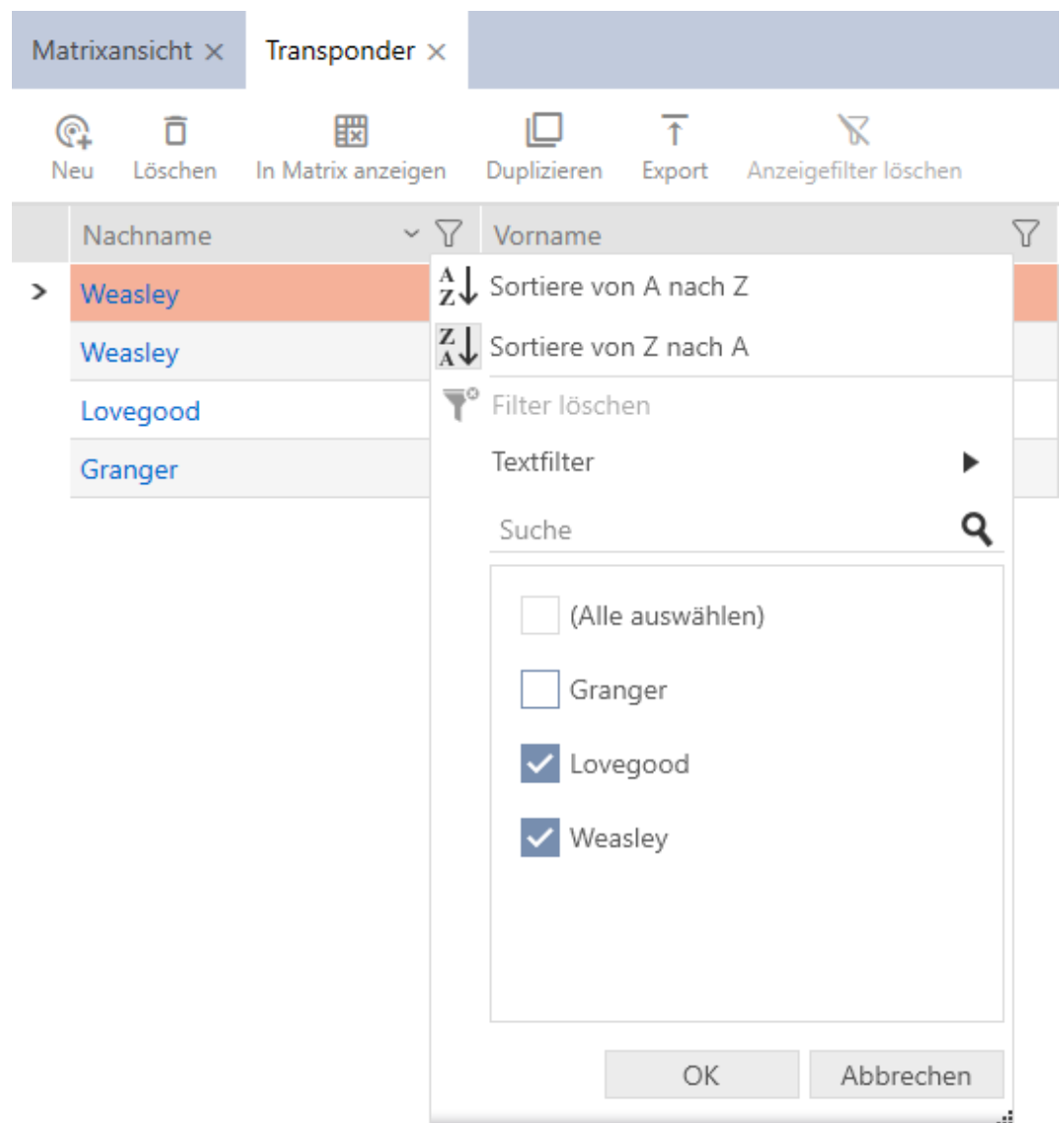
The AXM Classic provides you with sorting and filtering functions to simplify things.

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.




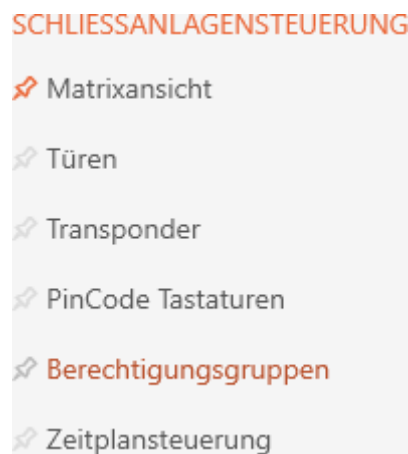
3. Click on the **OK** button.
 - ↳ The filter menu will close.

↳ Entries will now be filtered when displayed.

3. Organisational structure

3.1 Creating authorisation groups

1. Click the orange AXM button  AXM.
 - ↳ AXM bar opens.
2. Select the **Access levels** entry in the | LOCKING SYSTEM CONTROL | group.



- ↳ The AXM bar will close.
 - ↳ The [Access levels] tab will open.
3. Click on the **New +** button.
 - ↳ The window for a new authorisation group will open.
4. Enter a name for your authorisation group in the *Name* field.
5. Enter a description in the *Description* field.
6. Click on the **Finish** button.
 - ↳ The window for the new authorisation group will close.
 - ↳ The new authorisation group is listed.

4. 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)* [▶ 67]).

4.1 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).

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

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


These identification media differ from one another:

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

4.1.1 Creating transponders and cards

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

- *Authorisation groups* [▶ 59] (see Authorisation groups for background information)
- Creating a schedule or Create time group (see Time groups and schedules for background information)

1. Click on the **New transponder**  button.
 - ↳ The window for creating an identification medium will open.
2. Enter a description if required.
3. If the identification medium is to feature time-controlled authorisations: select the Time group checkbox.
4. Select the time group from the ▼ **Time group** drop-down list (e.g. "Time group").
5. Enter the surname and first name of the person who will receive the identification medium in the *Last name* and *First name* fields.
 - ↳ The surname and first name will be displayed in the matrix at a later point in time.

↳ The personnel number is generated automatically.






NOTE

Personnel number formula or manual entry

The AXM Classic 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).

Alternatively, you can enter personnel numbers manually:




1. Activate the Auto check box.
 - ↳ The *Personnel number* field is activated.
 2. Enter the personnel number in the *Personnel number* field.
-
6. Use the **Next >** button to switch to the next tab or complete the entries with the **Finish** button.
 7. If locking devices need to open twice as long for this identification medium (doubling to max. 25 s): select the Long opening checkbox.
 8. If you don't wish locking devices for this identification medium to beep: disable the No acoustic opening signal checkbox.
 9. If you need to save the locking devices on which the identification medium was used on the identification medium: select the Personal audit trail checkbox.
 10. If you do not want the transponder to be usable immediately: disable the from now checkbox. Then enter an activation date.
 11. If the transponder is only to be used for a limited period of time, disable the without expiry date checkbox. Then enter an expiry date.
 12. Use the **Next >** button to switch to the next tab or complete the entries with the **Finish** button.
 13. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 9]).
 14. Select the required authorisation groups in the right column (Ctrl+click for single groups or Shift+click for multiple groups).
 15. Use  to move the selected authorisation groups only or  to move all displayed authorisation groups.
 - ↳ The identification medium is assigned to the highlighted authorisation groups.



NOTE

Double-clicking as an alternative to arrow keys

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

16. Use the **Next >** button to switch to the next tab or complete the entries with the **Finish** button.
17. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [[▶ 9](#)]).
18. Select the required hashtags in the right column (Ctrl+click for single hashtags or Shift+click for multiple hashtags).
19. Use  to move only the selected hashtags or  to move all hashtags.



NOTE

Double-clicking as an alternative to arrow keys

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

- ↳ The highlighted hashtags in the left-hand column are used for this identification medium.
20. Select the Create additional objects checkbox to leave the window with the same settings open for the next identification medium to be created.
 21. Click on the **Finish** button to create the identification medium.
 - ↳ The window for creating a new identification medium closes.
 - ↳ Newly created identification medium is listed or displayed in the matrix.

4.1.2 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).

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

- Creating a schedule or Create time group (see Time groups and schedules 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 Classic (also see PIN Code G1 vs. PIN Code AX).




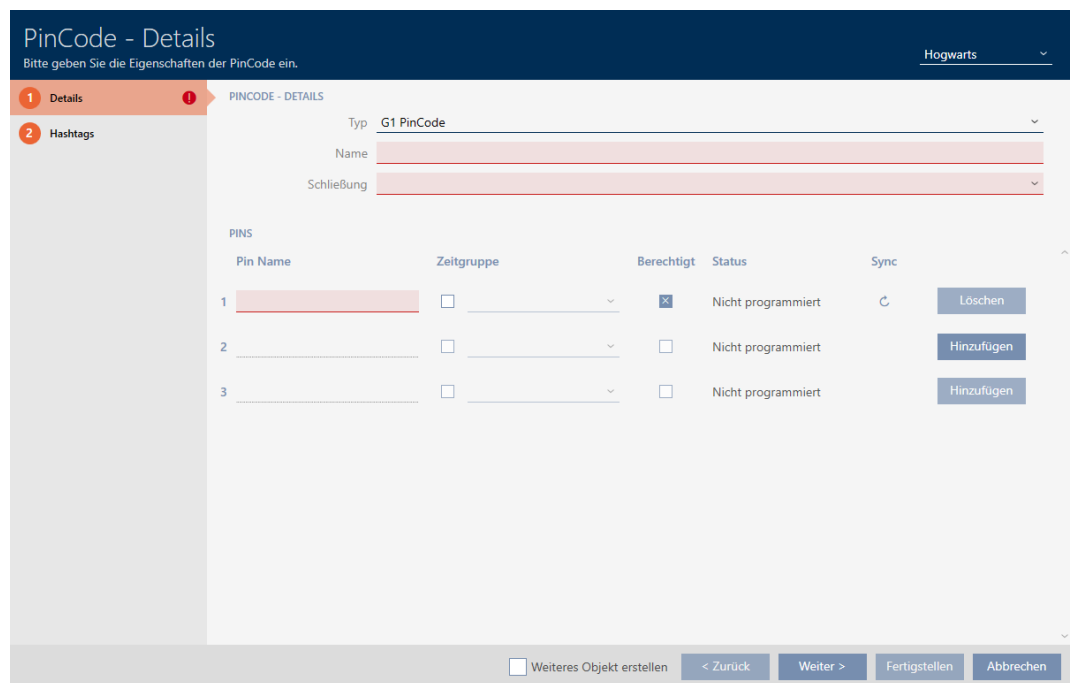
NOTE

Authorisations set automatically

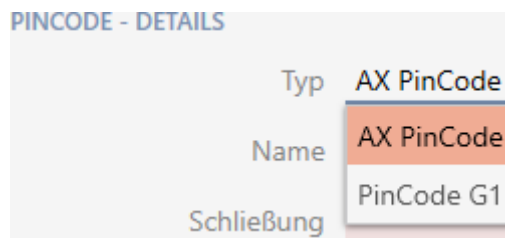
Your AXM Classic assumes that you also want to authorise newly created PINs. Newly created PINs therefore automatically receive authorisation for the assigned locking device.

✓ Locking device has been created for the PIN code keypad (see *Creating a locking device* [▶ 44] in the AXM manual).

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

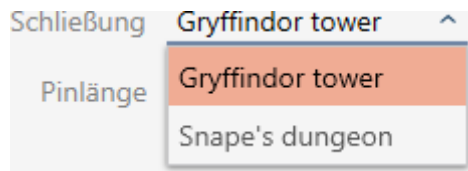


2. Select the PIN code keypad you wish to create from the ▼ **Type** drop-down menu.

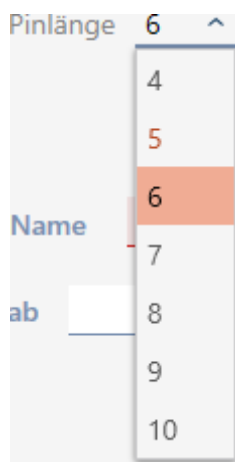


3. Enter a name for the PIN code keypad in the *Name* field.

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



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



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



NOTE

Duplicate PINs not permitted for PIN code keypad AX

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

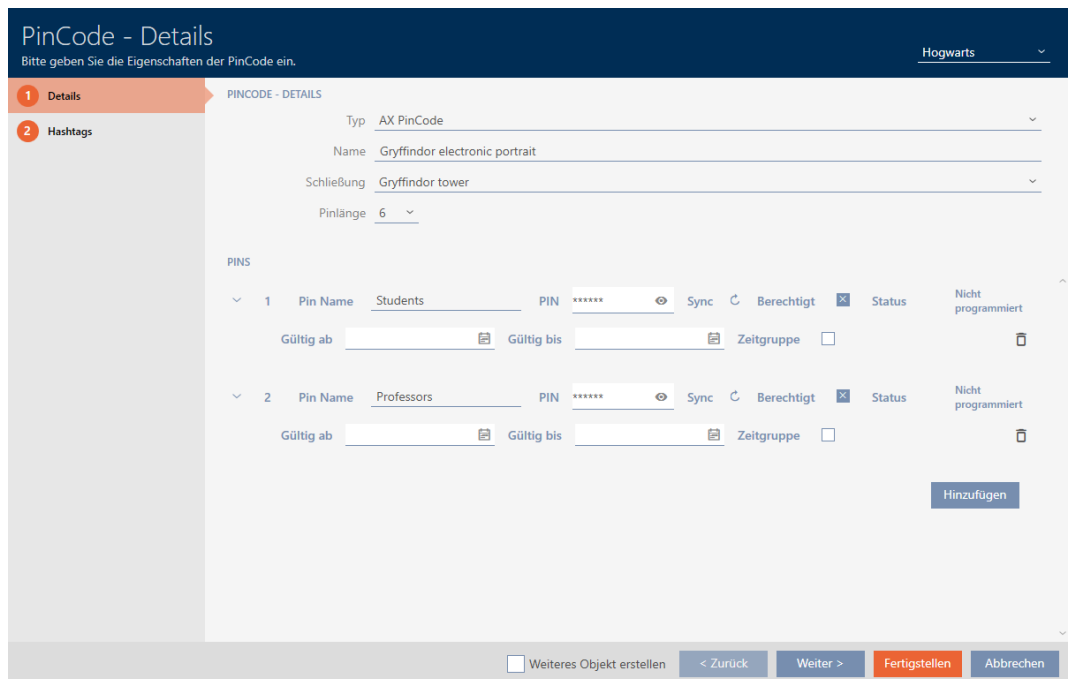
Your AXM Classic detects duplicate PINs and highlights them with *The pin is not unique* in red.

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* [▶ 9]).
16. Select the required hashtags in the right column (Ctrl+click for single hashtags or Shift+click for multiple hashtags).
17. Use to move only the selected hashtags or to move all hashtags.

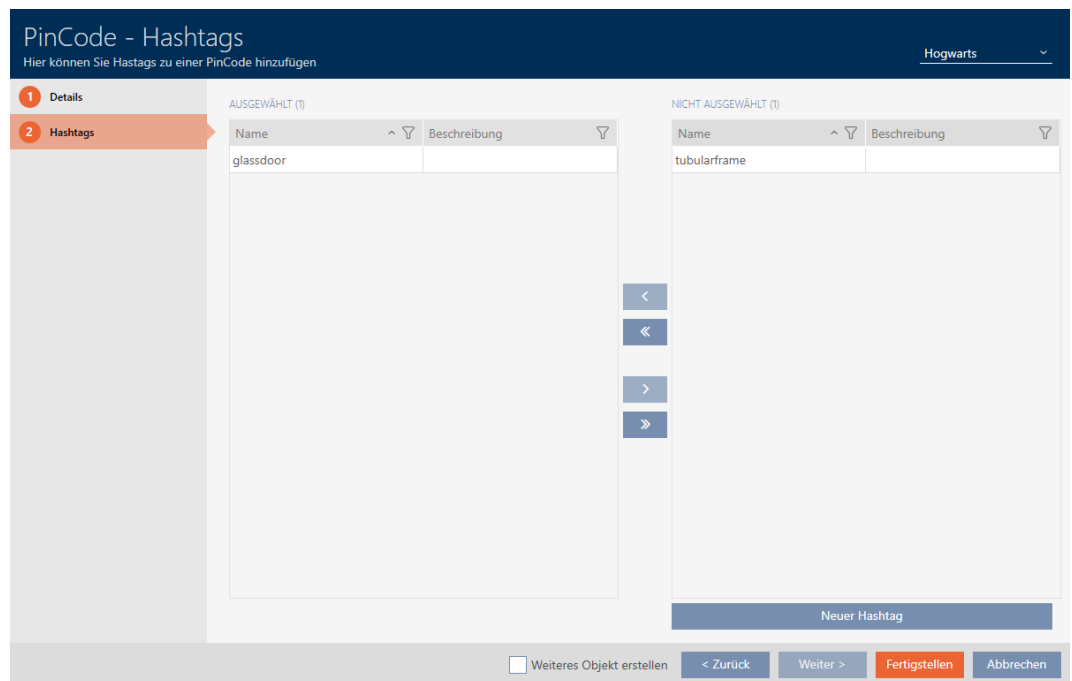


NOTE

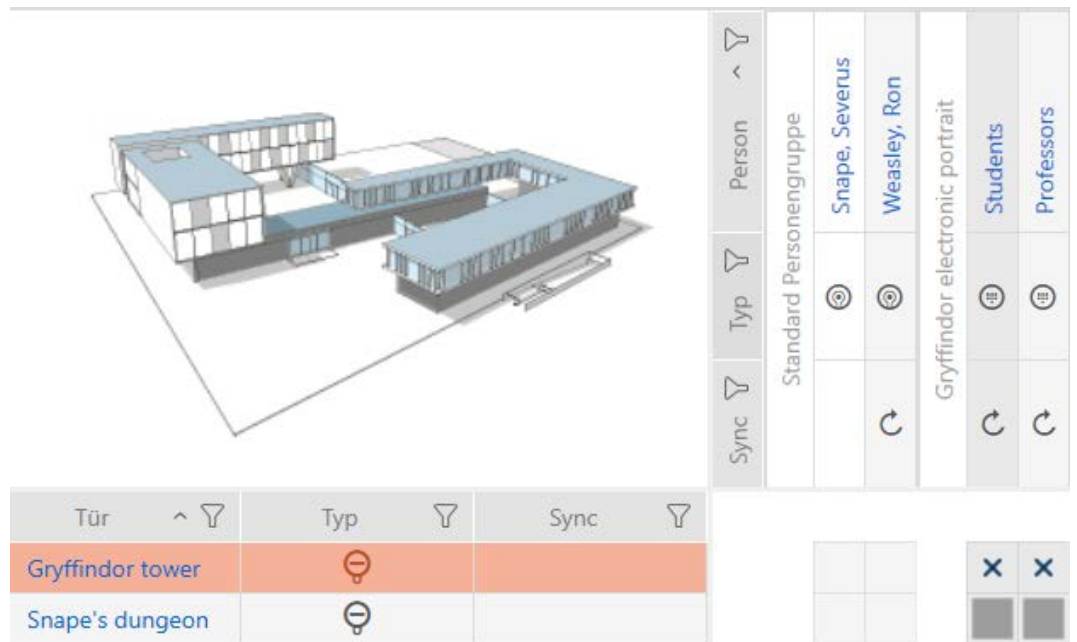
Double-clicking as an alternative to arrow keys

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

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




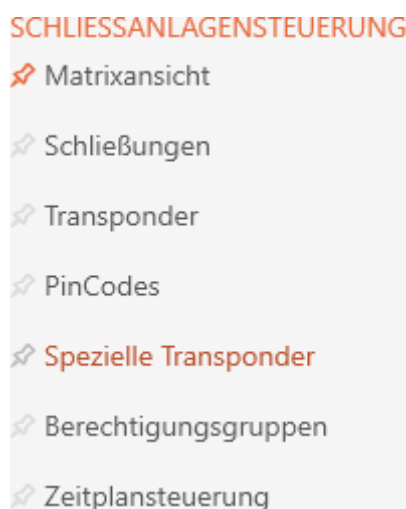
18. Select the Create additional objects checkbox to leave the window with the same settings open for the next PIN code to be created.
19. Click the **Finish** button to create the PIN code.
 - ↳ "PinCode - Details" window closes.
 - ↳ Newly created PIN code is listed or displayed in the matrix.



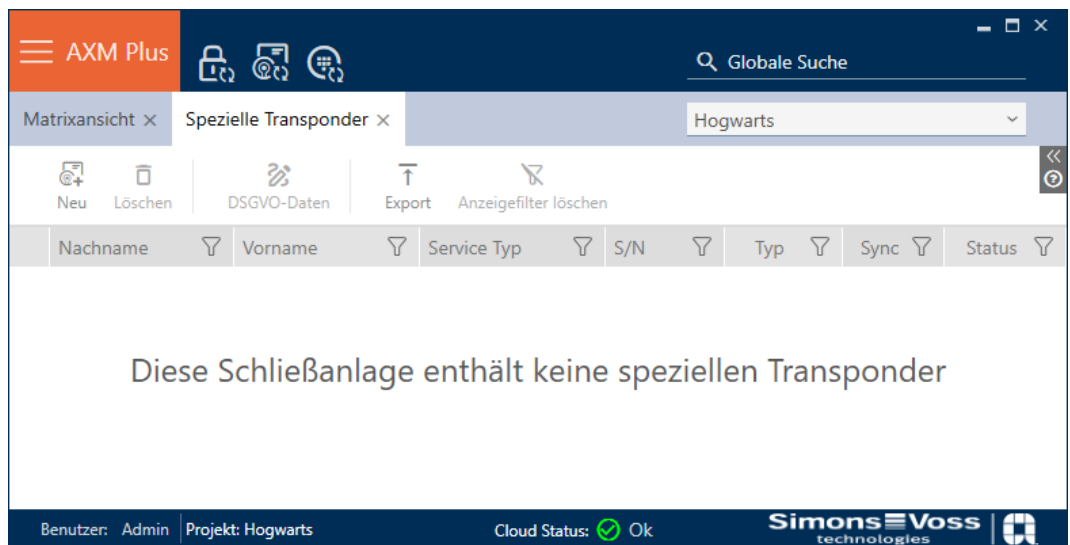
4.1.3 Creating special identification media


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

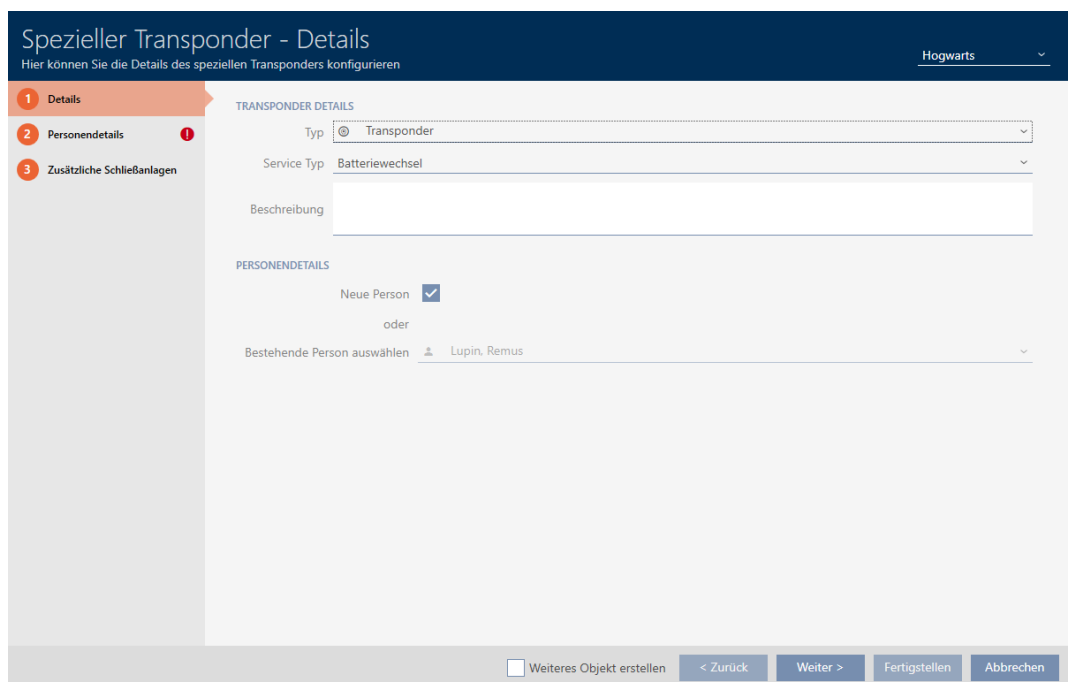
1. Click on the orange AXM icon .
 - ↳ AXM bar opens.
2. Select the **Special Transponders** entry in the | LOCKING SYSTEM CONTROL | group.



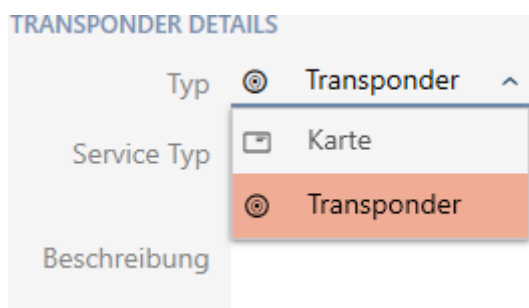
↳ The [Special Transponders] tab will open.



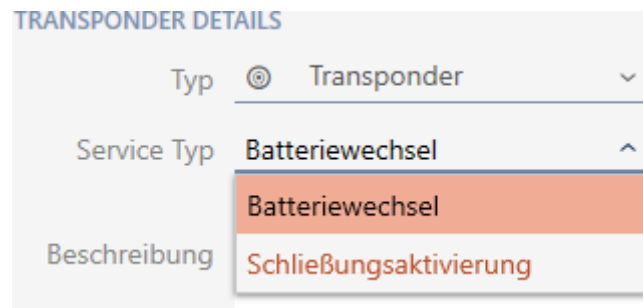
3. Click on the **New** button .
 - ↳ The "Special Transponder" window will open.



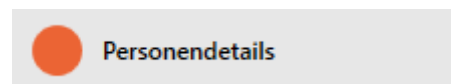
4. Select the type of identification medium you want to make a special identification medium from the drop-down **Type** menu.



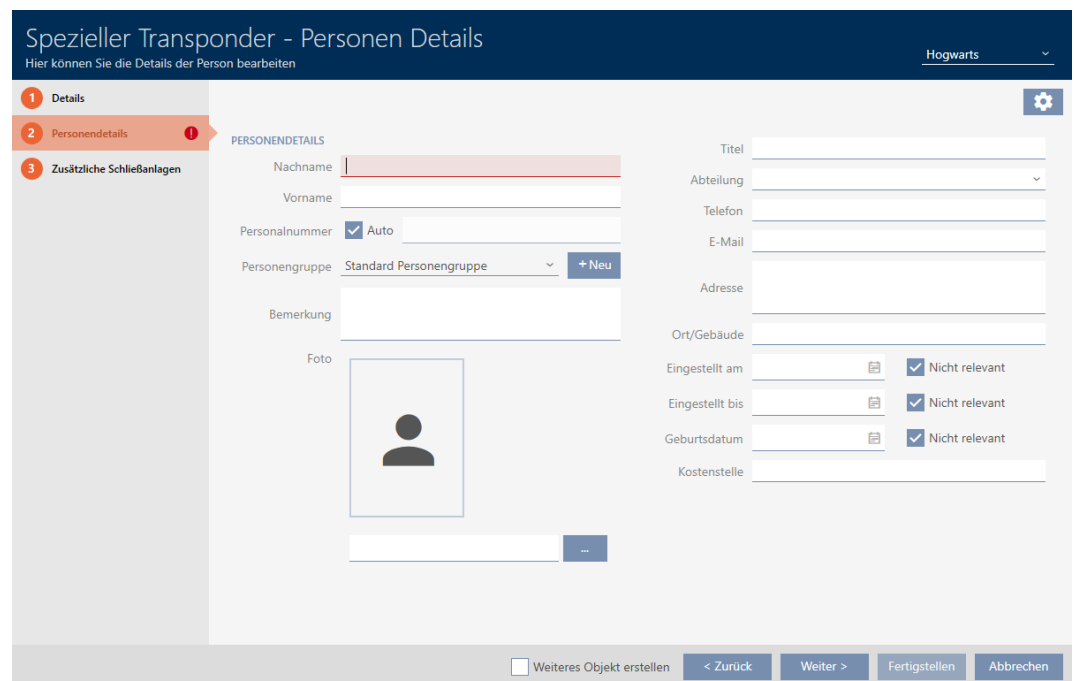
- Then use the drop-down ▼ **Service Type** menu to select which function this identification medium should have ("Battery replacement" or "Lock Activation").



- Enter a description if required.



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





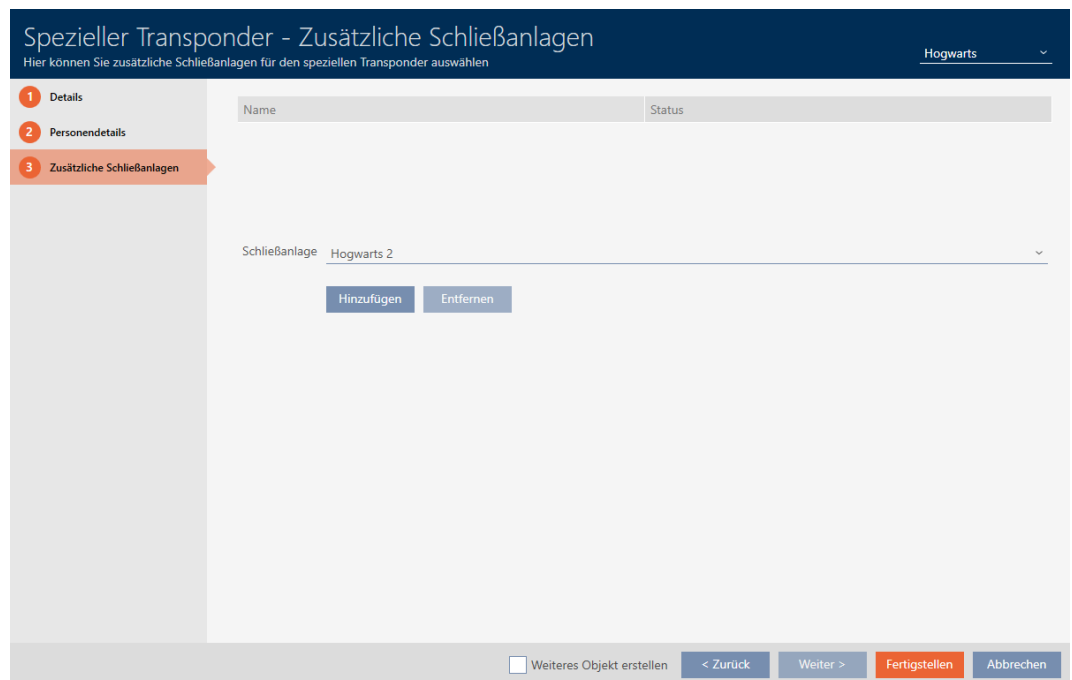
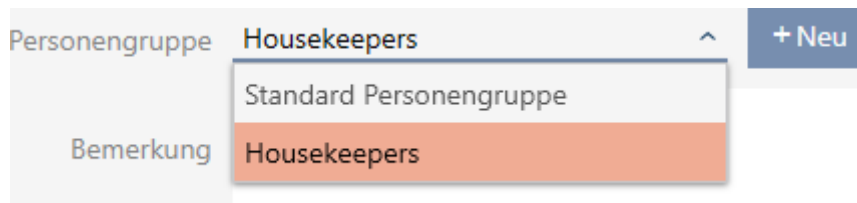
NOTE

Personnel number formula or manual entry

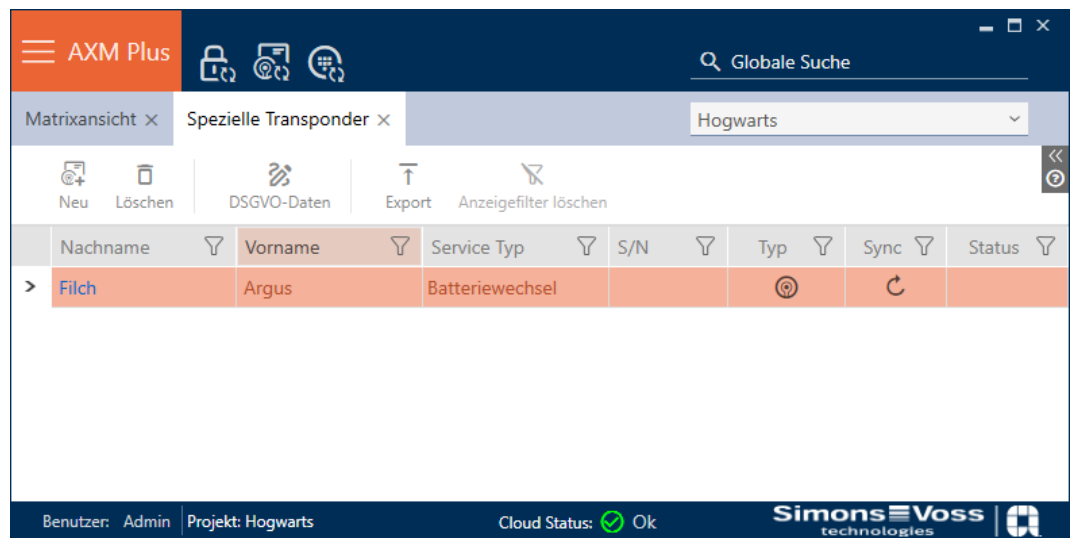
The AXM Classic generates personnel numbers based on the following formula: PN-1, PN-2, PN-X. The abbreviation *PN* can be changed if required (see Changing automatic numbering).

Alternatively, you can enter personnel numbers manually:

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



8. If you want to use this special identification medium in other locking systems, use the **Add** button to add other locking systems.
9. Click on the **Finish** button.
 ↳ "Special Transponders" window closes.
 ↳ Newly created identification medium with special function is now listed.



The screenshot shows the AXM Plus software interface. At the top, there is a navigation bar with 'AXM Plus' and a search bar labeled 'Globale Suche'. Below this, there are tabs for 'Matrixansicht' and 'Spezielle Transponder'. A dropdown menu shows 'Hogwarts'. The main area contains a table with the following columns: Nachname, Vorname, Service Typ, S/N, Typ, Sync, and Status. A single row is visible with the following data: Nachname: Filch, Vorname: Argus, Service Typ: Batteriewechsel, S/N: (empty), Typ: (empty), Sync: (empty), Status: (empty). The bottom status bar shows 'Benutzer: Admin', 'Projekt: Hogwarts', 'Cloud Status: Ok', and the Simons & Voss Technologies logo.

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

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

4.2 Deleting an identification medium

4.2.1 Deleting a PIN (PIN code keypad AX)

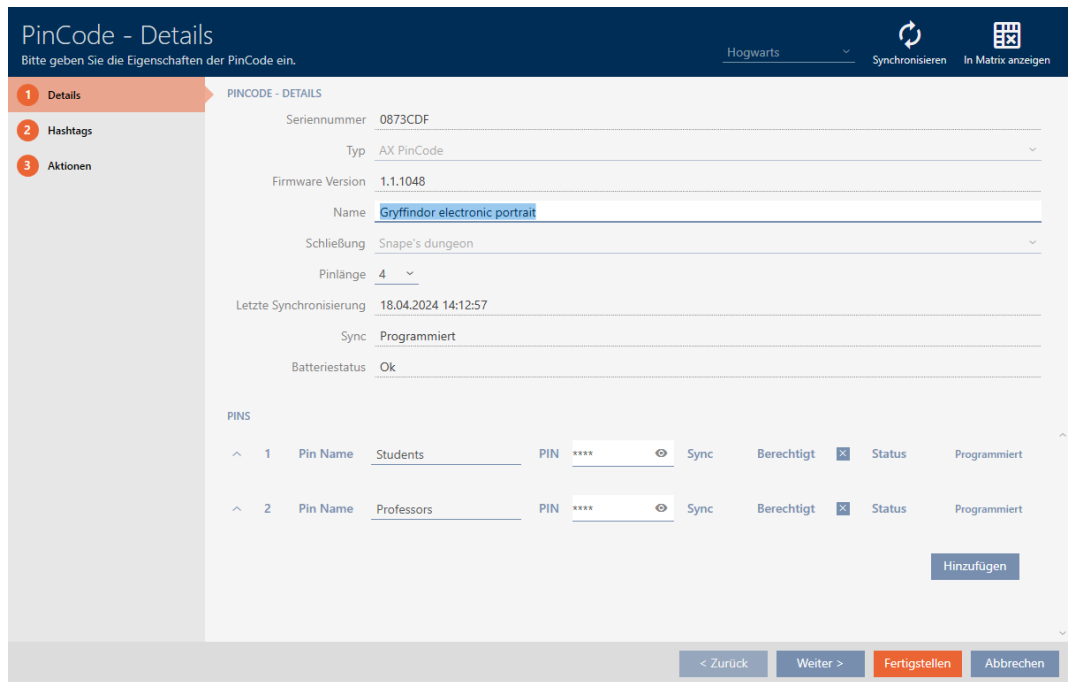


NOTE

Description only valid for PIN code keypad AX

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

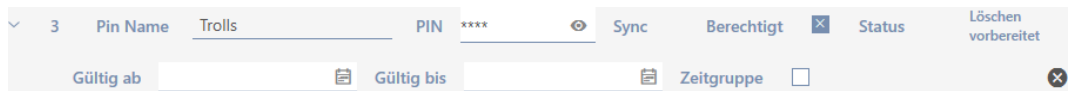
- ✓ Matrix screen open.
 - ✓ PIN code keypad AX created (see *Creating PIN code keypads* [▶ 15]).
1. Click on any PIN to open details on your PIN code keypad AX.
 - ↳ The "PinCode - Details" window will open.



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

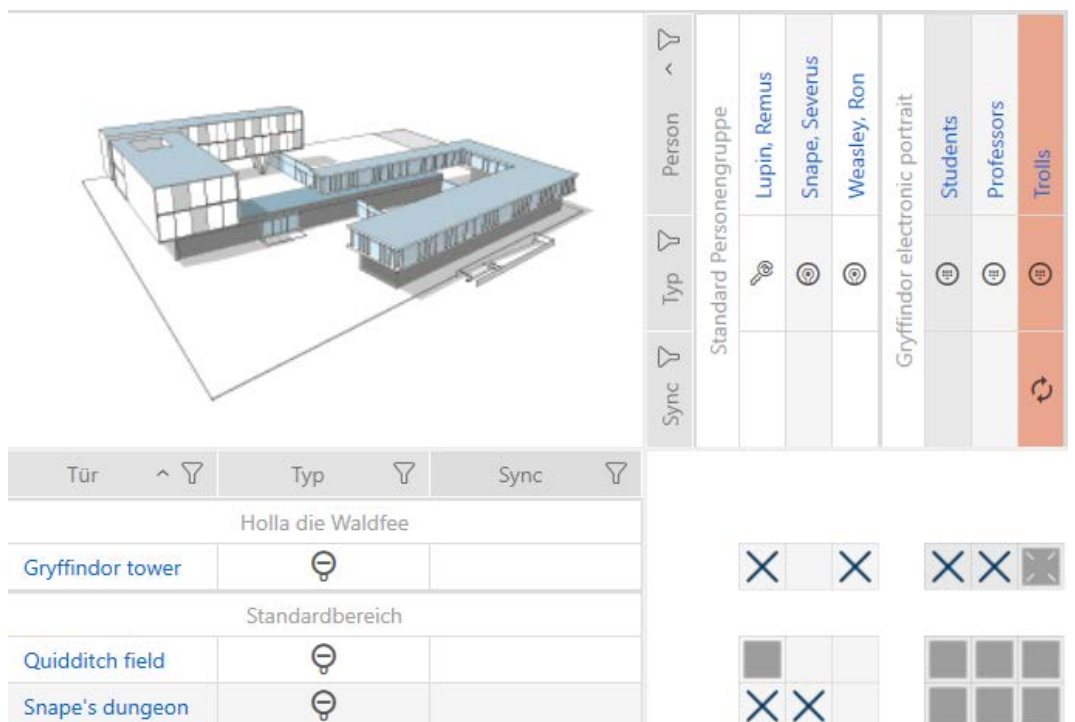
3. Click on  to highlight the PIN to be deleted.

↳ *Status* field shows *Prepared to delete*.



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

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



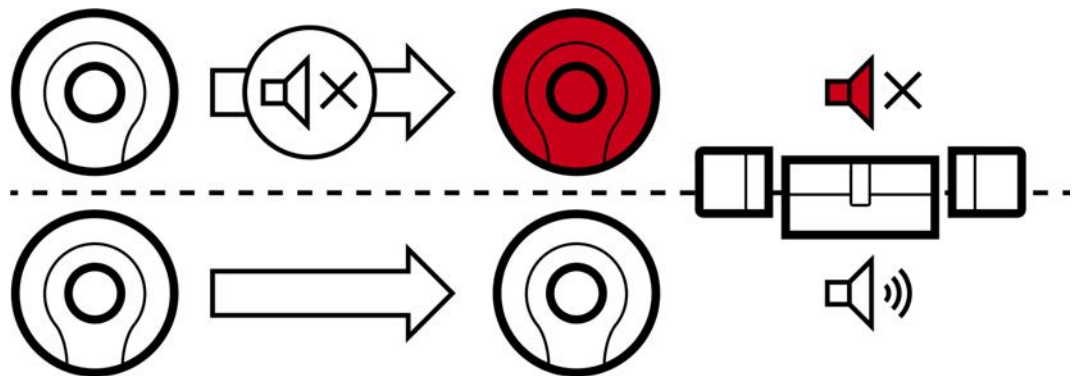
The deleted PIN will disappear after synchronisation.

4.3 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.

4.4 Duplicating forgotten identification medium temporarily



4.5 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* [▶ 27]). 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 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* [▶ 30]). If only one PIN is known and is therefore unsafe, you can change this PIN (see *Changing a PIN (PinCode AX)* [▶ 41]).

4.5.1 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* [▶ 9]).
 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

Transponder	Weasley, Percy (000X9C10)	▼
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.
5. Enter the reason in the drop-down menu.
6. Click on the **OK** button.
 - ↳ Confirmation dialogue for replacement identification medium will open.
7. Click on the **Yes** button.
 - ↳ Confirmation dialogue for replacement identification medium closes.
 - ↳ Replacement identification medium can already be seen in the matrix in the background.

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

- ↳ Confirmation dialogue about synchronising the replacement identification medium will open.
- 8. Click on the **Yes** button.
- ↳ Confirmation dialogue about synchronising the replacement identification medium closes.
- ↳ Synchronisation starts.
- ↳ Lost identification medium is blocked.
- ↳ Replacement identification medium is synchronised.
- ↳ Replacement identification medium is displayed in the matrix next to the lost identification medium.

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

✕	⊠	✕	✕		▶
	⊠			▶ ✕	
✕	⊠		✕		

IMPORTANT


Block ID automatically written on replacement transponder

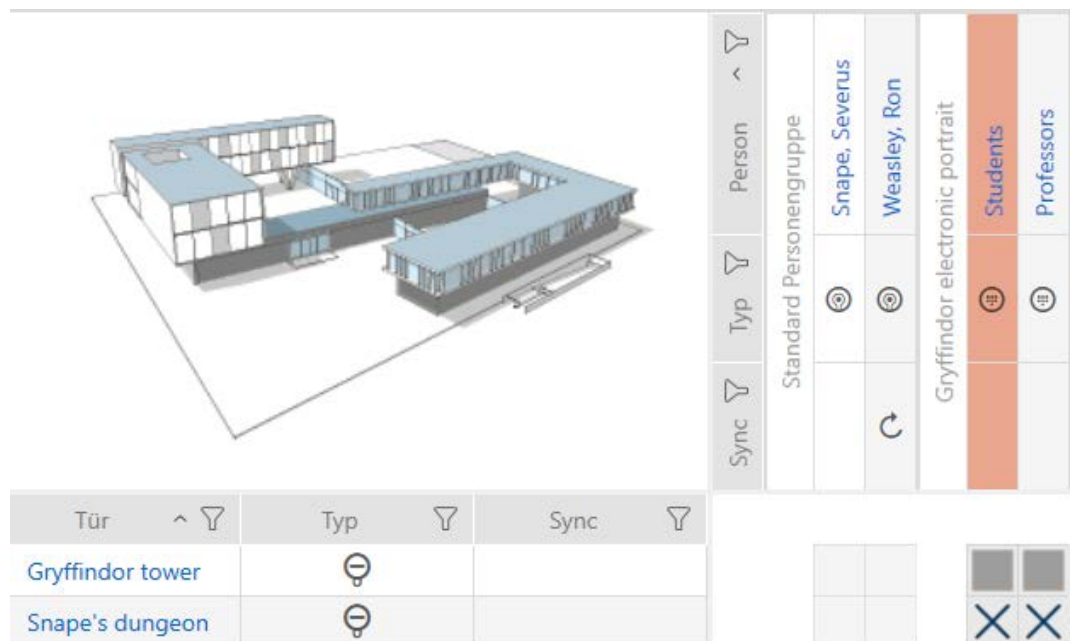
If you create a replacement transponder for a lost/stolen transponder, your AXM Classic automatically writes the block ID from the blocked transponder onto this replacement transponder.


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.

4.5.2 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* [[▶ 9](#)]).
 2. Select a PIN associated with the lost PIN code keypad.



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

PinCode verloren - Assistent

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

PINCODE VERLOREN

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

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

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

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

Weiter
Schließen

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

PinCode deaktivieren

Bitte geben Sie die gewünschten Informationen ein

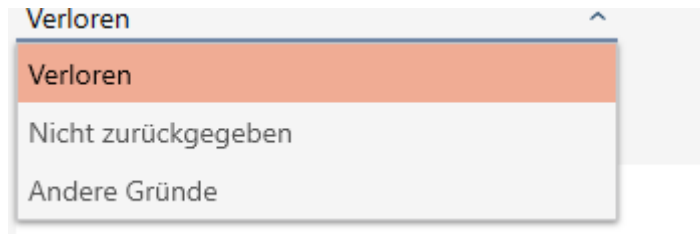
Wollen Sie tatsächlich die PinCode sperren?
Falls 'ja', geben Sie bitte den Grund an, z.B. ob die PinCode verlorengegangen ist.

Verloren ▼

Zusatzinformation

OK
Abbrechen

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



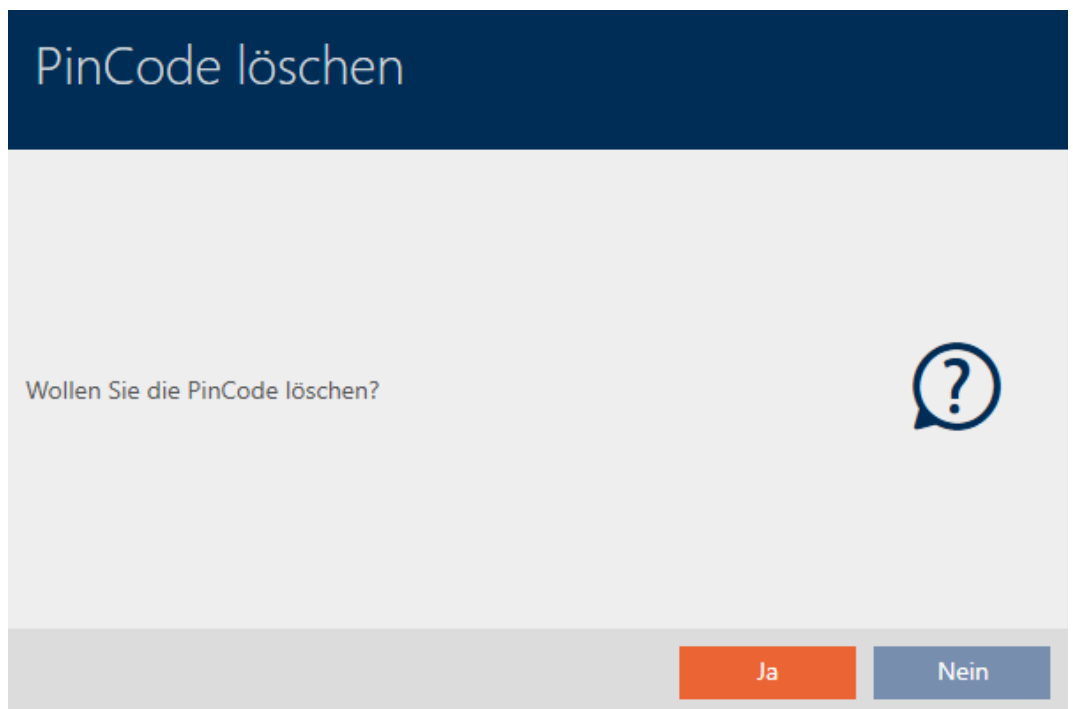
6. Enter any additional information in the *Additional information* field.
7. Click on the **OK** button.
 - ↳ Confirmation window closes.
 - ↳ AXM Classic offers to create a replacement PIN code keypad.



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



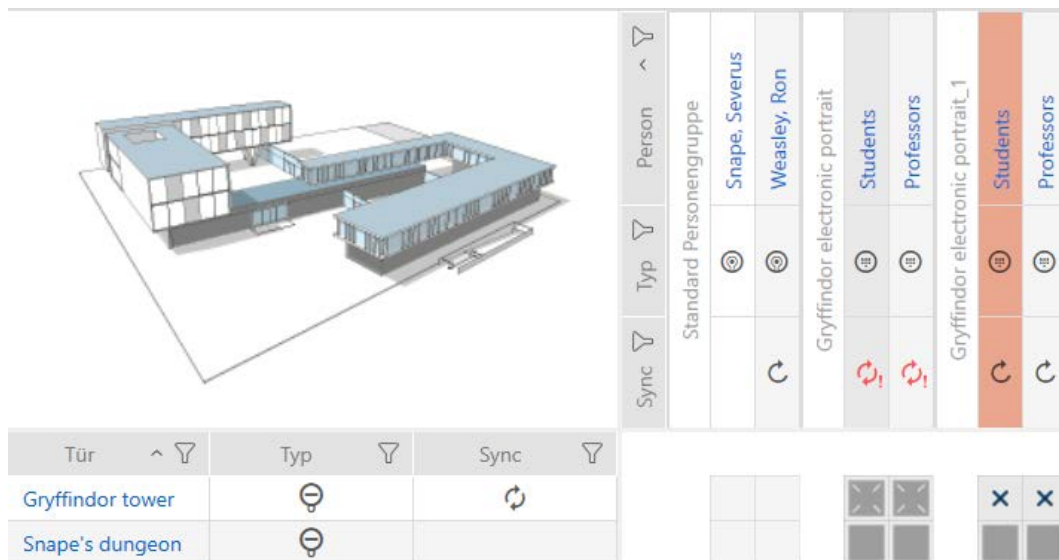
9. Click on the **Yes** button.
- ↳ Synchronisation of the replacement PIN code keypad launches.
 - ↳ AXM Classic offers to delete the lost PIN code keypad.



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 Classic will display an error message:



You can repair the PIN code keypad as an alternative; see Repairing a PIN code keypad (resynchronising).

4.6 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 Classic 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.

4.7 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 Classic.








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

4.7.1 Exporting PINs and PIN code keypads as a list

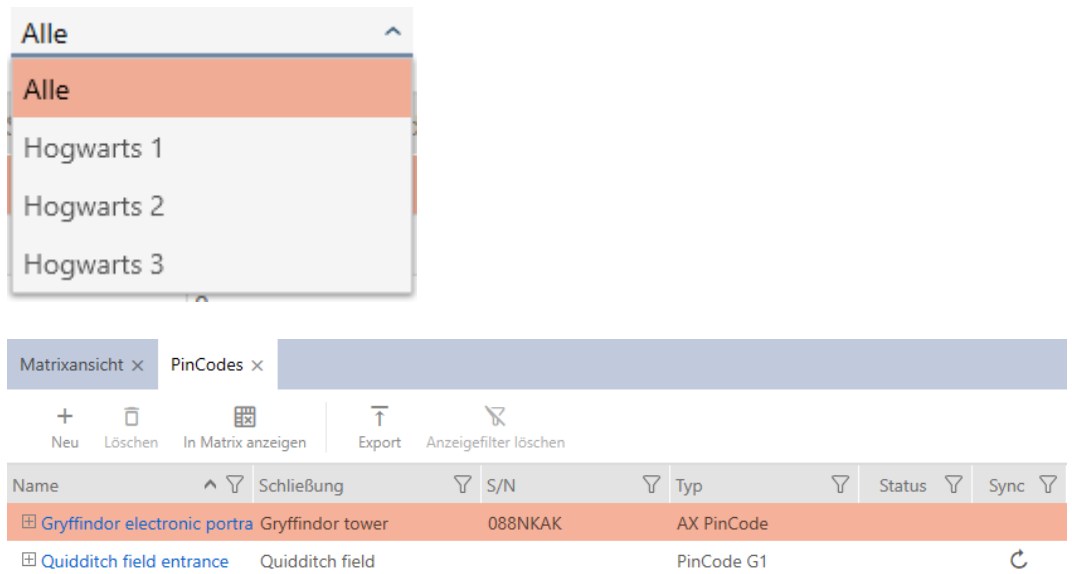
✓ PIN code keypad created (see *Creating PIN code keypads* [▶ 15]).

1. Click the orange AXM button  AXM.
↳ AXM bar opens.
2. Select the **PIN code keypads** entry in the | LOCKING SYSTEM CONTROL | group.

SCHLISSANLAGENSTEUERUNG

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

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



3. Use to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 9]).

4. Click on the **Export** button.

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



Alle PinCodes für die Schließanlage 'Hogwarts'


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














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


4.8.1 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:

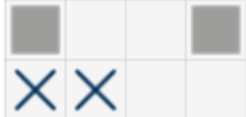
- ✓ PIN code keypad created and synchronised.
 - ✓ List with PIN code keypads or matrix open.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [[9](#)]).
 2. Click on a PIN associated with the PIN code keypad whose serial number you want to view.


Sync	Typ	Person
	Standard Personengruppe	
		Lupin, Remus
		Snape, Severus
		Weasley, Ron
		Wood, Oliver
	Gryffindor electronic portrait	
		Students
		Professors
	Quidditch field entrance	
		Students
		Professors






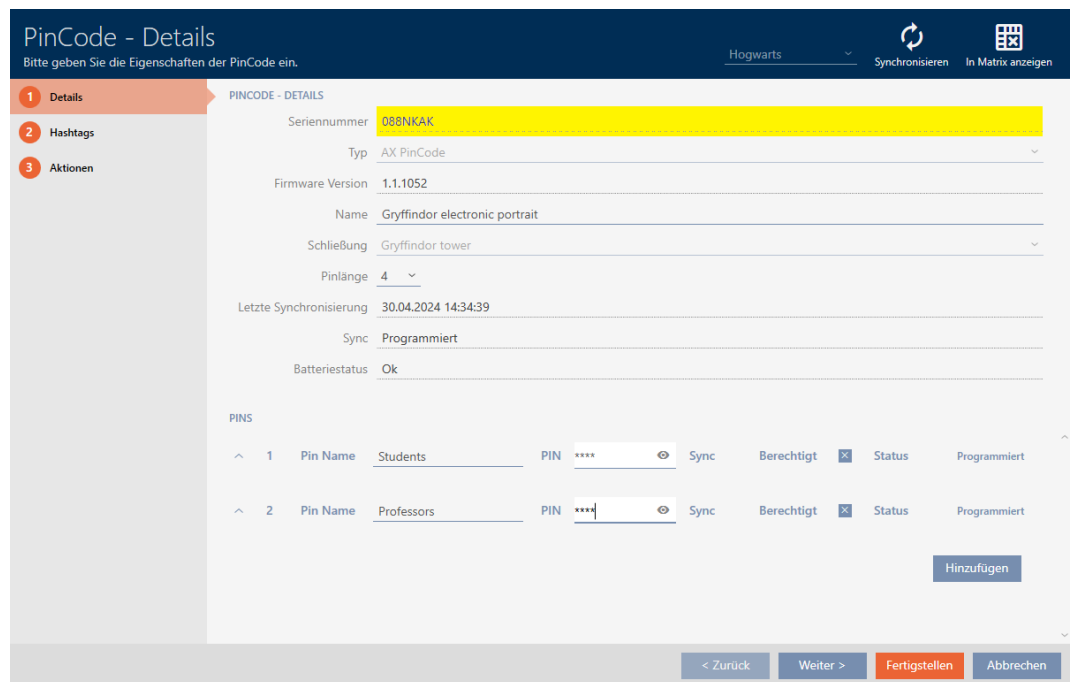








- ↳ The PIN code keypad window will open.
- ↳ Serial number is displayed.



4.9 Setting the PIN length (PinCode AX)



NOTE

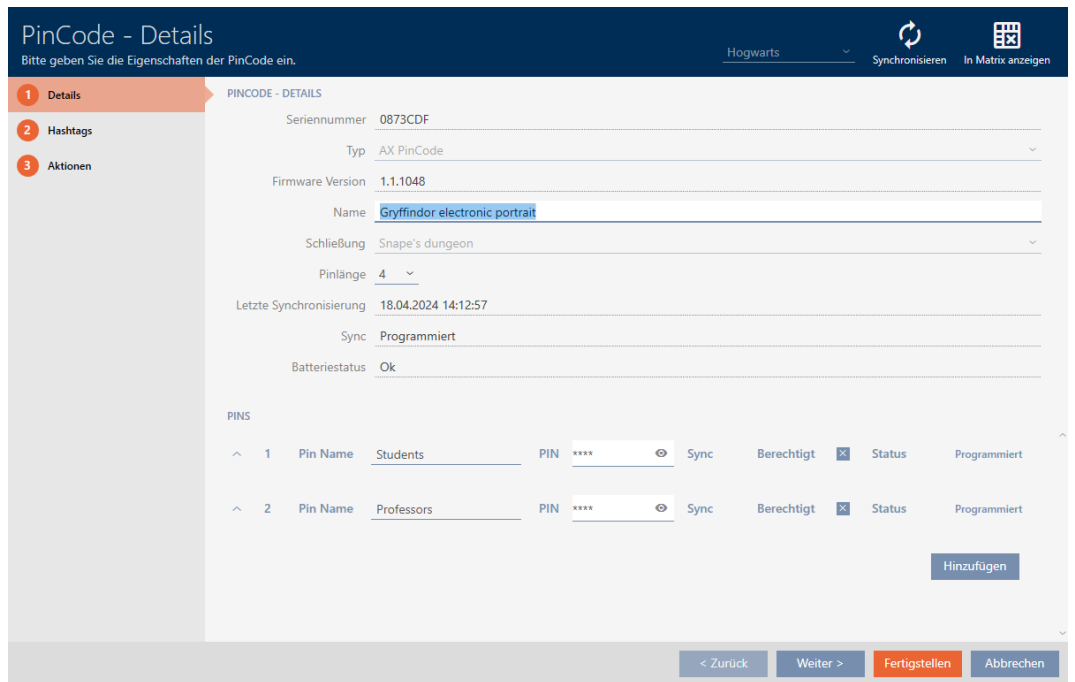
Description only valid for PIN code keypad AX

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

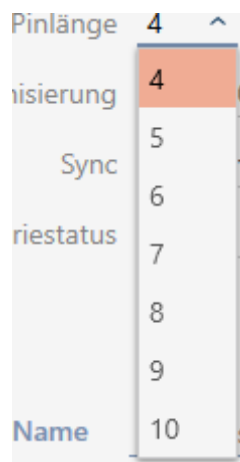
You always set the PIN length for the entire PIN code keypad AX, i.e. for all PINs simultaneously. For this reason, you must then reassign each PIN and synchronise the PIN code keypad AX.

- ✓ Matrix screen open.
- ✓ PIN code keypad AX created (see *Creating PIN code keypads* [▶ 15]).

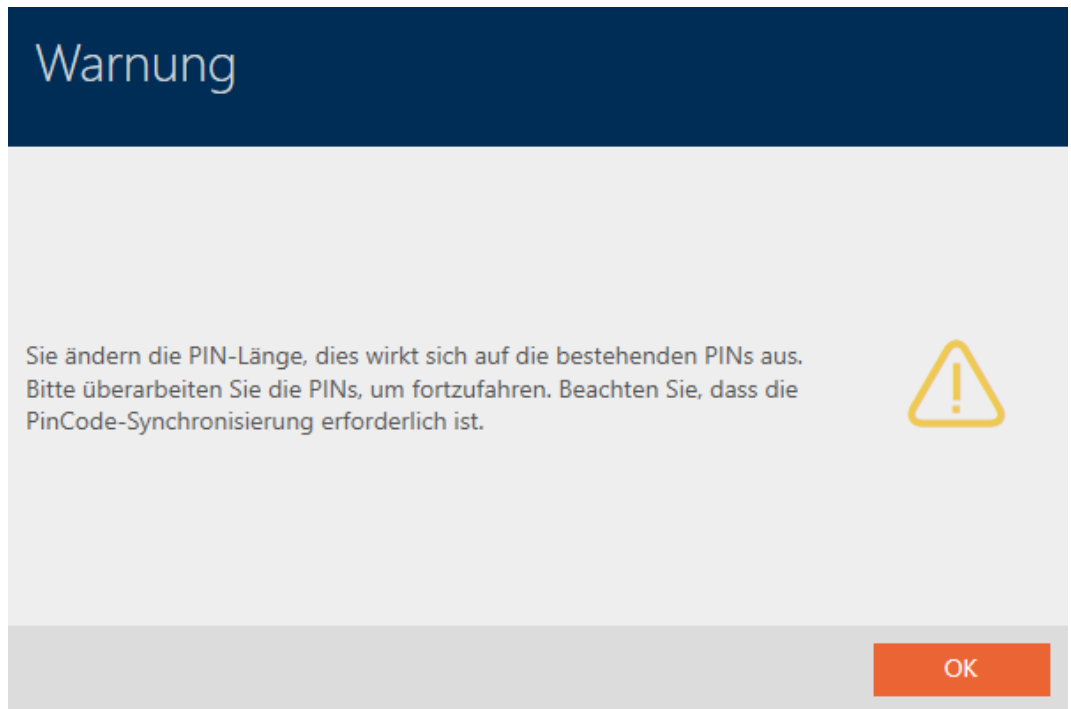
1. Click on any PIN to open details on your PIN code keypad AX.
 - ↳ The "PinCode - Details" window will open.



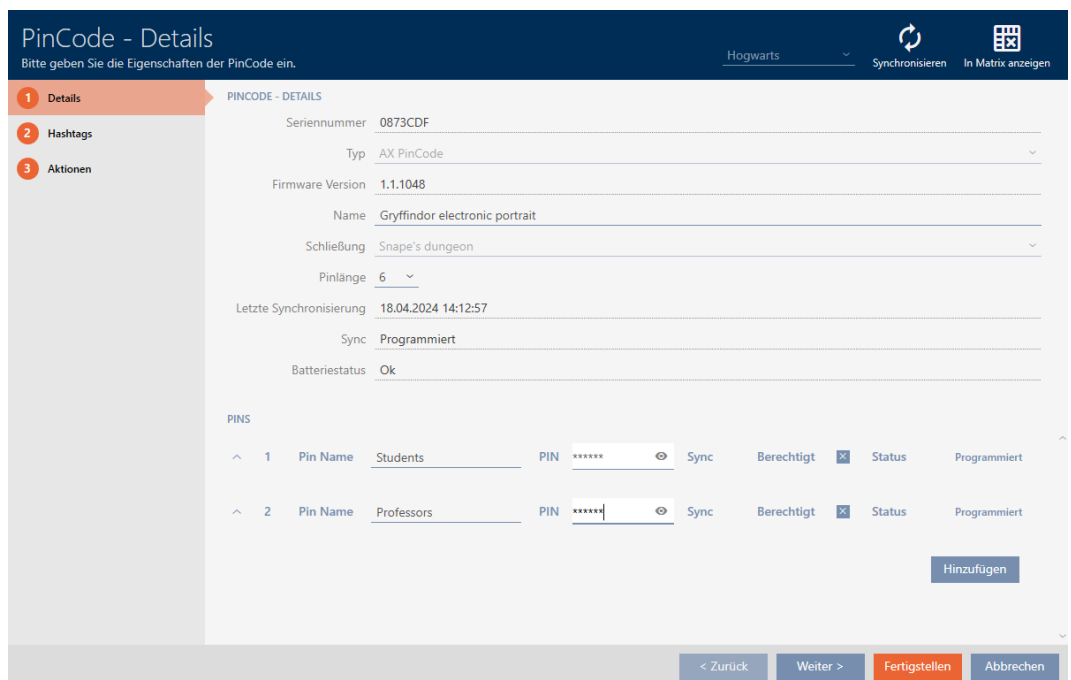
2. Select the required PIN length from the ▼ Pin length drop-down menu.



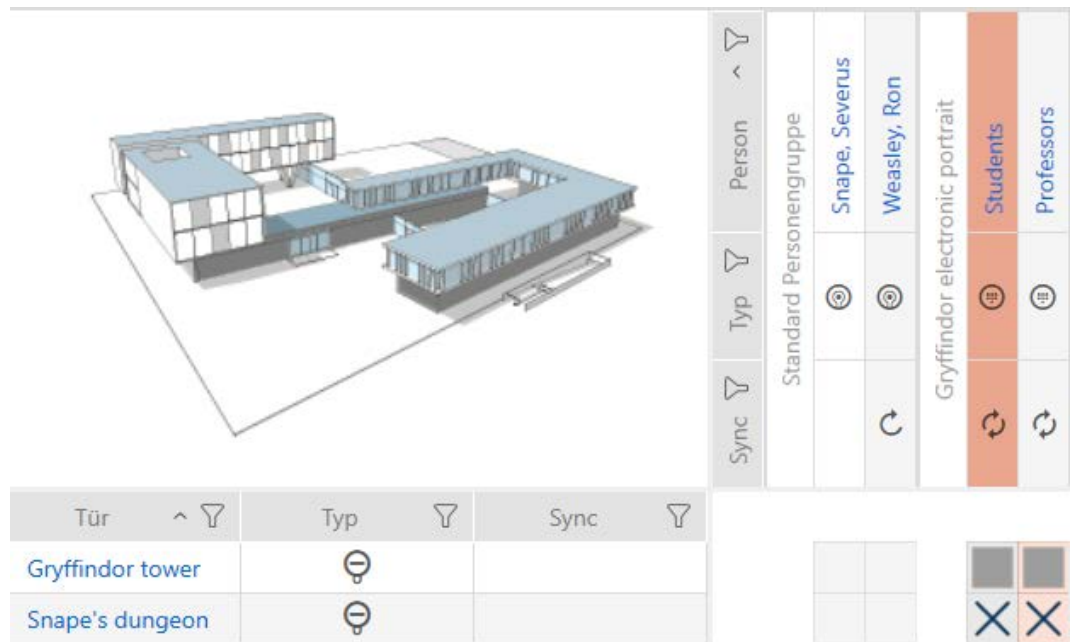
↳ Your AXM Classic will alert you to the upcoming workload.



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



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



4.10 Changing a PIN (PinCode AX)

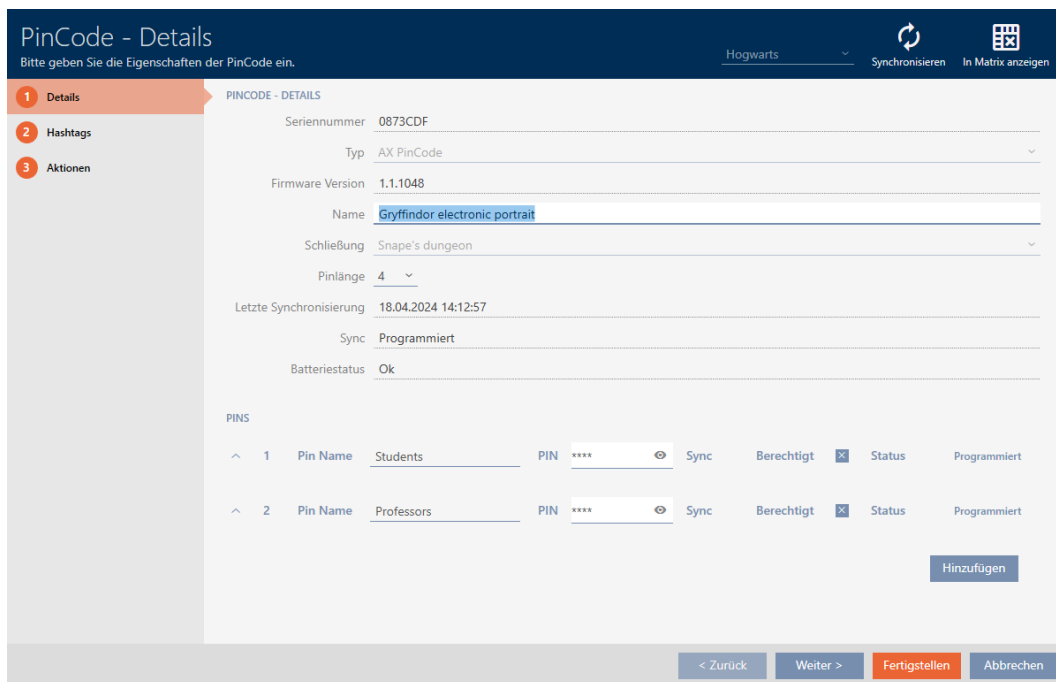


NOTE

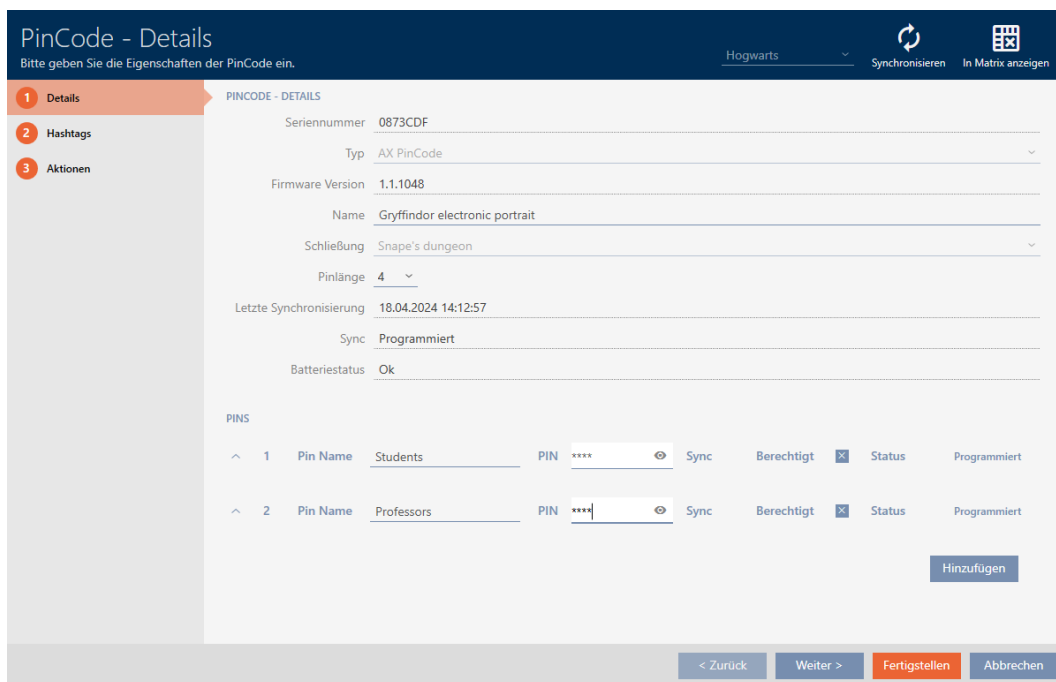
Description only valid for PIN code keypad AX

The setting described here is only available for the PIN code keypad AX in your AXM Classic. 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* [▶ 15]).
1. Click on any PIN to open details on your PIN code keypad AX.
 - ↳ The "PinCode - Details" window will open.




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



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

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



Tür	Typ	Sync
Gryffindor tower	☹	
Snape's dungeon	☹	

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

		☒	☒
		✕	✕

5. 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)* [▶ 64]).

5.1 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. for more information on this topic.

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

- *Authorisation groups* [▶ 59] (see Authorisation groups for background information)
- Creating a schedule or Create time group (see Time groups and schedules for background information)
- Creating a time switchover (see Time switchovers for background information)
- Creating a location or Creating a building and assigning it to a location (see Buildings and locations for background information)
- Creating a hashtag (see Hashtags for background information)



NOTE

Hidden settings

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

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

Schließung - Details
Bitte geben Sie hier die Eigenschaften der neuen Schließung ein.

1 Details
2 Konfiguration
3 Berechtigungsgruppen
4 Hashtags

SCHLIEßUNGSDetails

Schließungstyp Schließzylinder

Türname

^ GEBÄUDEDETAILS ^ ZEITFUNKTIONEN

Raumnummer

Etage

Standort

Gebäude

Weiteres Objekt erstellen < Zurück Weiter > Fertigstellen Abbrechen

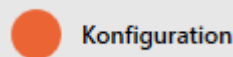
2. Select which locking devices you wish to create from the ▼ **Lock type** drop-down menu.
3. Enter the name of the door where your locking device will be installed in the *Door name* field.
4. If necessary, enter the number of the room where your locking device will be installed in the *Room number* field.
5. If necessary, enter the floor on which your locking device will be installed in the *Floor* field.
6. Select the location where your locking device will be installed from the ▼ **Location** drop-down menu.
 - ↳ Selection in the ▼ **Building** drop-down menu is limited to the buildings in the selected location.
7. Select the building where your locking device is installed from the ▼ **Building** drop-down menu.
8. If you wish to use time functions: Expand the "Time functions" menu and make the settings (see Limiting authorisations for locking devices to specific times (schedule) and Engaging and disengaging locking devices automatically with time switchover for details).

**NOTE****Public holiday lists in locking device and locations**

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

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

9. Click on the  Configuration tab.



↳ Window switches to the "Configuration" tab.

10. If you want to log access attempts, expand the "Time configuration" menu and configure the settings (see Have accesses logged by locking device (access list)).
11. If you want to change the opening time or use the close range mode, expand the "Lock functions" menu and configure the settings (see Leaving the locking device open for longer, less time or permanently and Limit locking device read range (close range mode)).

**NOTE****Button control not adjustable**

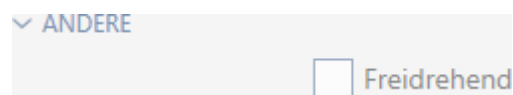
Some locking cylinders are equipped with a button on the inside thumb-turn (TS option). If your AXM Classic detects such a locking cylinder, the Button control checkbox is displayed. However, this cannot be adjusted, i.e. you cannot disable the buttons.

12. If you want to change the battery warning signalling or programming acknowledgements, expand the "Feedback signals" menu and configure the settings (see Muting a locking device (for battery warnings and programming)).
13. If you want to ignore the activation time window (see Activation date / expiry date), expand the "AX functions" menu and configure the settings (see Ignoring activation and expiry date of identification media).
14. If you want to use the internal and external antenna together in a SmartRelay, expand the "Relay functions" menu and configure the settings (see Using internal and external antenna simultaneously).

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

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

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



NOTE

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


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

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

↳ AXM Classic 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

▼ DOORMONITORING

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

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

PROTOKOLLIERUNG IN DER ZUTRITTSLISTE	
<input type="checkbox"/> "Tür offen" Ereignisse	
<input type="checkbox"/> Schlossriegel-Ereignisse	

WEITERLEITUNG IM NETZWERK	
<input type="checkbox"/> "Tür offen" Ereignisse	
<input type="checkbox"/> Schlossriegel-Ereignisse	
<input type="checkbox"/> Protokollierung / Weiterleitung der Alarme im Netzwerk	

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

18. Click on the Access levels tab.

Berechtigungsgruppen

↳ Window switches to the "Access levels" tab.

19. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 9]).



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



NOTE

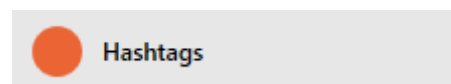
Double-clicking as an alternative to arrow keys

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


21. Use  to move the selected authorisation groups only or  to move all displayed authorisation groups.

↳ Your locking device is added to the authorisation groups in the left-hand column.

22. Click on the  Hashtags tab.



↳ Window switches to the "Hashtags" tab.

23. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [▶ 9]).

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



NOTE

Double-clicking as an alternative to arrow keys

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

25. Use  to move only the selected hashtags or  to move all the hashtags displayed.

↳ The hashtags in the left-hand column are added to your locking device.

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

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

↳ The window for creating a new locking device closes.

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

5.2 Setting up door monitoring (DoorMonitoring)

You can use DoorMonitoring to monitor the status of your doors and locking devices (also see DoorMonitoring).

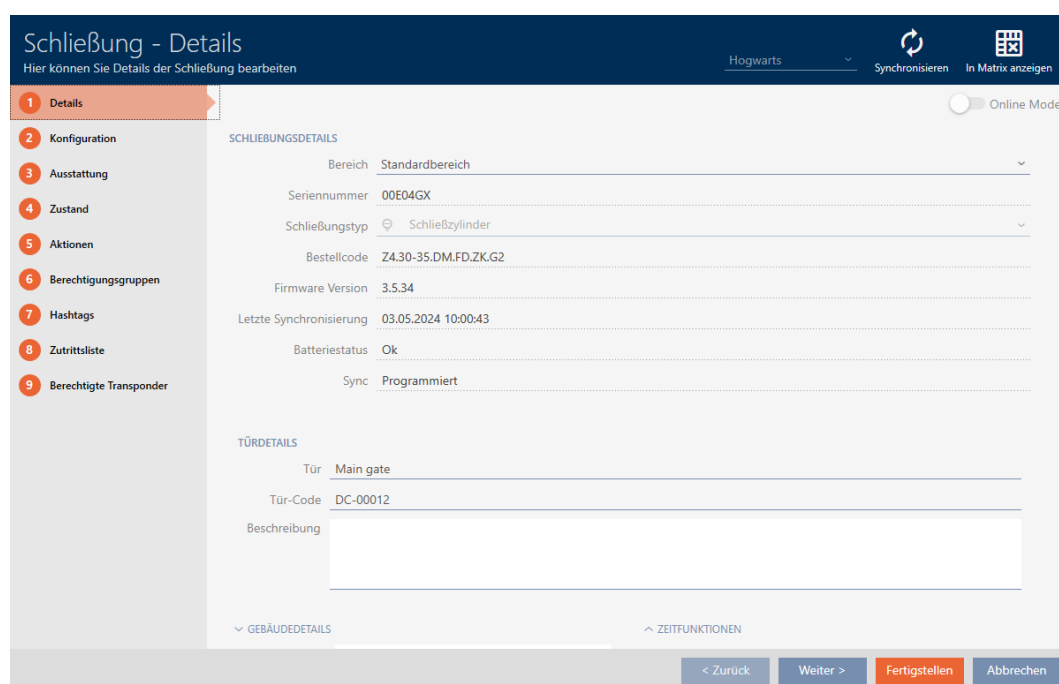
**NOTE****DoorMonitoring without direct networking (“WaveNet”) available to a limited extent**

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

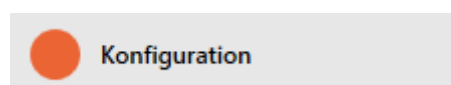
Locking devices without WaveNet also log their DoorMonitoring events and save them in the access list. You will only see these events after reading the access list in your locking plan software.

5.2.1 Setting up DoorMonitoring for locking cylinders

- ✓ Locking device is DoorMonitoring-capable (item code contains .DM).
- 1. Click on the locking device for which you wish to set up DoorMonitoring.

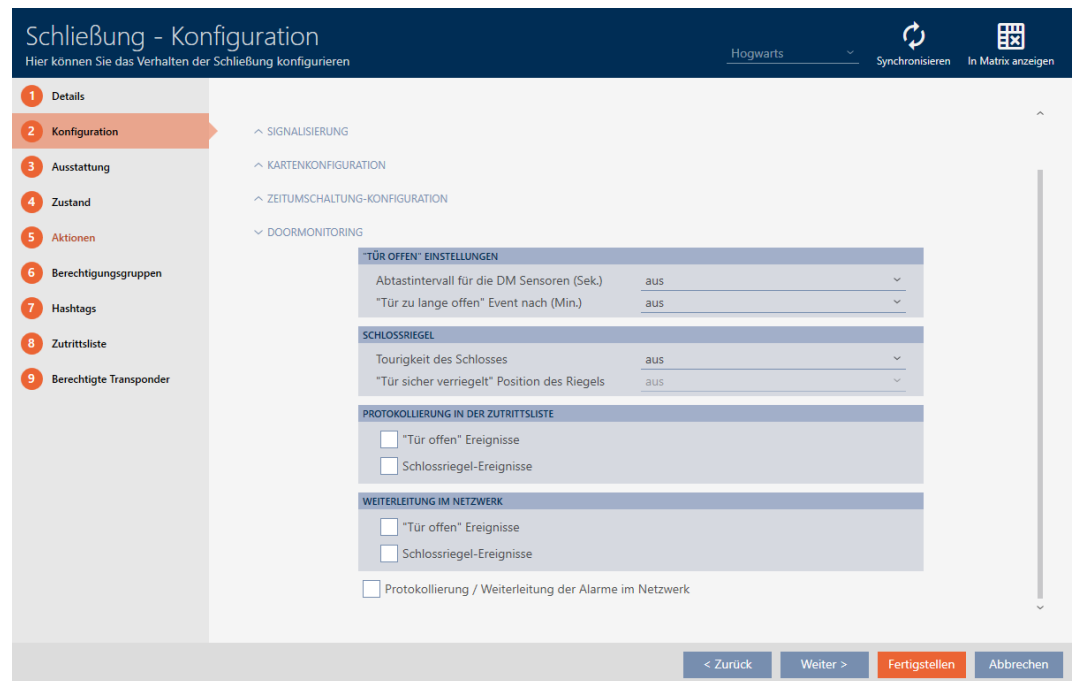


- 2. Click on the **Konfiguration** tab.



- ↳ Window switches to the [Configuration] tab.

3. Expand the "DoorMonitoring" menu.



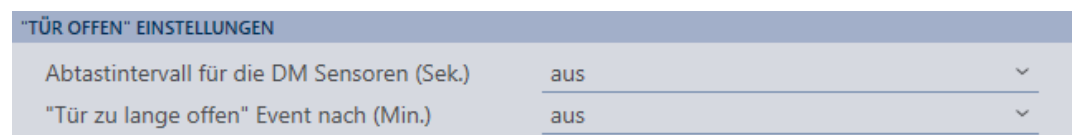
4. Configure the preferred settings.

5. Click the **Finish** button.

↳ DoorMonitoring is set up for this locking device.

You can select the following settings:

"Door open" settings



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

Setting	Explanation
<p>Sampling interval for the DM sensors (sec.)</p>	<p>The frequency with which the locking cylinder checks whether the magnetic tab is in front of the fastening screw. In this case, the door is considered closed.</p> <p>Possible intervals are:</p> <ul style="list-style-type: none"> ■ 0.5 seconds ■ 1.0 second ■ 2.0 seconds ■ 3.0 seconds ■ 4.0 seconds ■ 5.0 seconds ■ 10.0 seconds <p>More frequent checks lead to faster detection of an open door, but also increase power consumption.</p>
<p>"Door open too long" event after (min.)</p>	<p>Safety-relevant doors such as fire doors must not be permanently open. This setting allows you to see if a door is open for longer than usual. This door could be wedged open, for example.</p> <p>After the set time has elapsed, the Door open too long event is triggered.</p> <p>Possible intervals:</p> <ul style="list-style-type: none"> ■ 0.2 minutes ■ 0.5 minutes ■ 1.0 minute ■ 2.0 minutes ■ 5.0 minutes ■ 8.0 minutes

Lock bolt

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

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

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

Setting	Explanation
<p>“Door securely locked” position of dead bolt</p>	<p>In two- or multi-turn mortise locks, the door may be locked, but the dead bolt has not yet been extended far enough to rest securely in the door anchorage. In this case, the door is only considered Door is locked, but not Door is securely locked.</p> <p>This setting is used to specify how many turns are required until the dead bolt is extended far enough into the door and the locking device is considered secure.</p> <p>The available settings depend on what you have specified in Number of turns to lock:</p> <ul style="list-style-type: none"> ■ off ■ 1 ■ 2 ■ 3 ■ 4

Logging in the access list

PROTOKOLLIERUNG IN DER ZUTRITTSLISTE

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

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

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

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

Forward in network

WEITERLEITUNG IM NETZWERK

"Tür offen" Ereignisse

Schlossriegel-Ereignisse

Protokollierung / Weiterleitung der Alarme im Netzwerk

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

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

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

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

6. Permissions

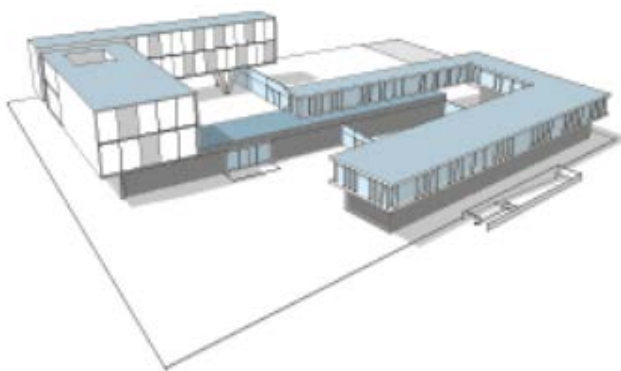
6.1 Changing individual authorisations (cross)

The quickest way to assign individual authorisations to individual doors is directly in the matrix.

✓ Matrix screen open.

1. Click on a box in the matrix.

↳ Authorisation is issued for the identification medium concerned (column) on the locking device in question (row).



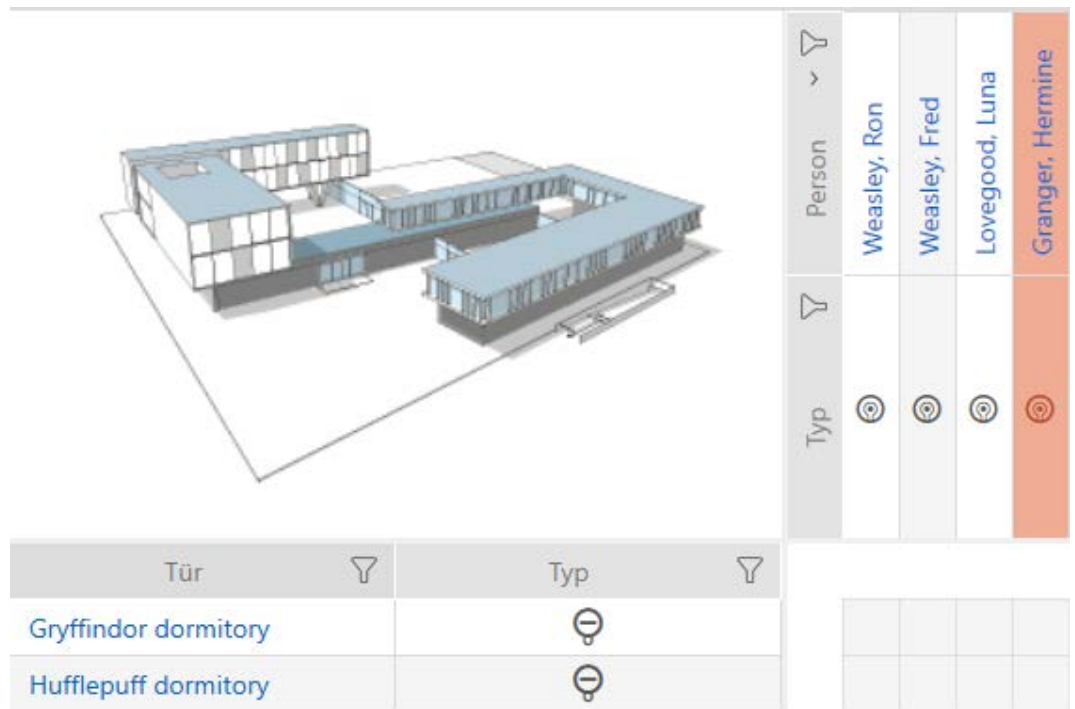
Person	Weasley, Ron	Weasley, Fred	Lovegood, Luna	Granger, Hermine
Typ	⊕	⊕	⊕	⊕

Tür	Typ
Gryffindor dormitory	⊕
Hufflepuff dormitory	⊕

				X

2. Click on the same box again.

↳ Authorisation is withdrawn again.



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):

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



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

6.2.1 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:

- ✓ Matrix screen open
 - ✓ Identification medium available.
 - ✓ Locking device available.
1. Use  to sort/filter the displayed entries if required (see *Sorting and filtering* [[▶ 9](#)]).
 2. Select the locking device on which you wish to authorise all identification media to be displayed.
 3. Click on the **Alle zulassen**  button.
- ↳ All displayed identification media are authorised for the selected locking device.

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

6.2.2 Authorisation groups

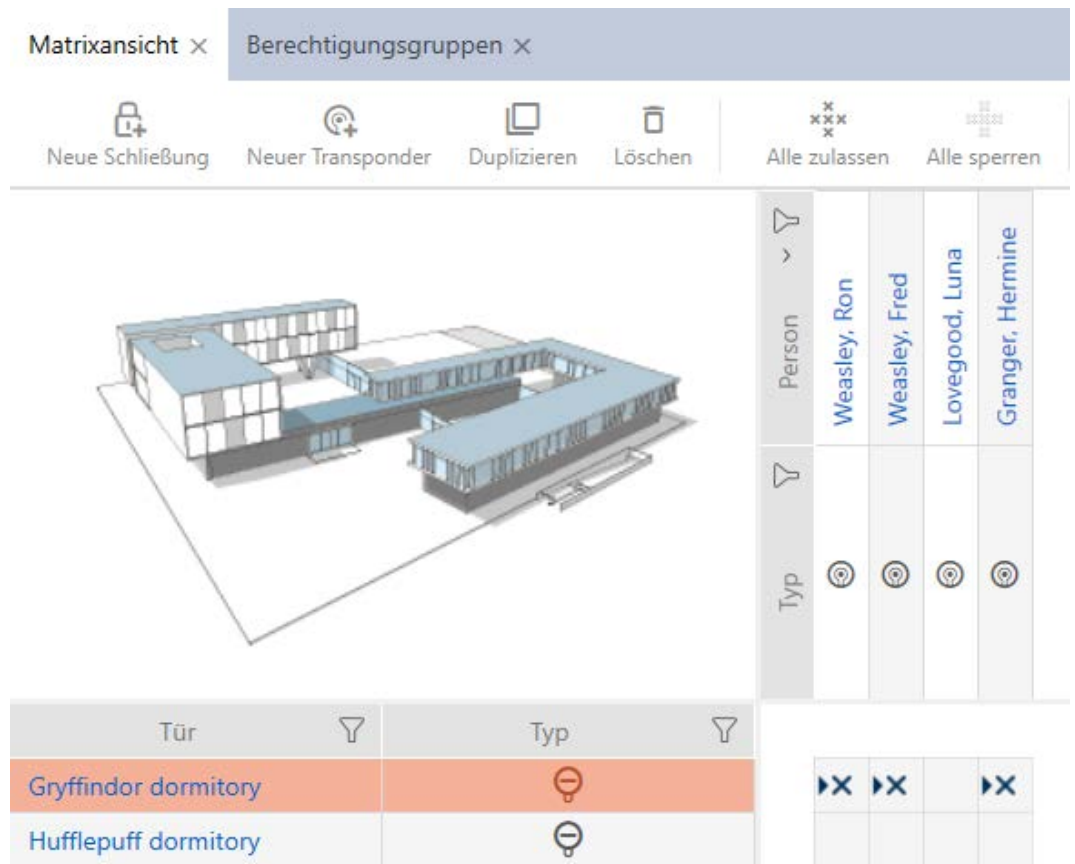
Authorisation groups are an easy way for you to set up authorisations for multiple doors and identification media at the same time (see *Authorisation groups*).

Matrix without authorisations

The screenshot displays the AXM Lite software interface for managing lock systems. At the top, there is a navigation bar with the 'AXM Lite' logo and icons for lock management. Below this is a sub-header indicating the current view is 'Matrixansicht' (Matrix view) for 'Schließanlagen' (Lock systems). A toolbar provides various actions: 'Neue Schließung' (New lock), 'Neuer Transponder' (New transponder), 'Duplizieren' (Duplicate), 'Löschen' (Delete), 'Alle zulassen' (Allow all), and 'Alle sperren' (Deny all). The main interface shows a 3D architectural rendering of a building complex. To the right of the rendering is a table with columns for 'Person' and 'Typ'. The 'Person' column lists names like 'Weasley, Ron', 'Weasley, Fred', 'Lovegood, Luna', and 'Granger, Hermine'. The 'Typ' column contains lock type icons. Below the main view, a detailed table shows the 'Typ' column expanded, listing 'Gryffindor dormitory' and 'Hufflepuff dormitory' with their respective lock type icons.




Tür	Typ
Gryffindor dormitory	[Lock Type Icon]
Hufflepuff dormitory	[Lock Type Icon]

Matrix with authorisation group



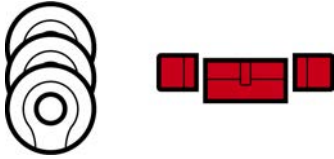
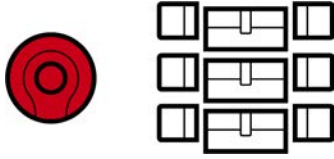
6.3 Meaning of the authorisation crosses in the matrix

Cross	Meaning
	Not authorised.
	Authorised in the database but not programmed yet.
	Authorised and programmed.
	Authorisation withdrawn, but authorisation removal not programmed yet.
	Authorised by an authorisation group in the database, but not programmed yet.
	Authorised and programmed by an authorisation group.
	Authorisation available and programmed by an authorisation group; this authorisation has been removed manually. Authorisation removal not programmed yet.

Cross	Meaning
	<p>Authorisation by an authorisation group available, but this authorisation was removed manually before programming.</p>
	<p>Authorised and programmed, but identification medium has been blocked (e.g. after theft).</p>
	<p>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.</p>

7. 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) [▶ 64]</i>	<i>Synchronise a card/transponder (including importing physical access list) [▶ 67]</i>
<p>Useful if many identification media have been authorised for a locking device. In this case, only one locking device needs to be synchronised instead of many identification media.</p> 	<p>Useful if an identification medium has been authorised for many locking devices. In this case, only one identification medium needs to be synchronised instead of many locking devices.</p> 



Other factors are important to consider when making this decision, such as:

- Available programming devices
- Locking device or identification medium on site
- Access list or physical access list imported

Synchronisation from the matrix

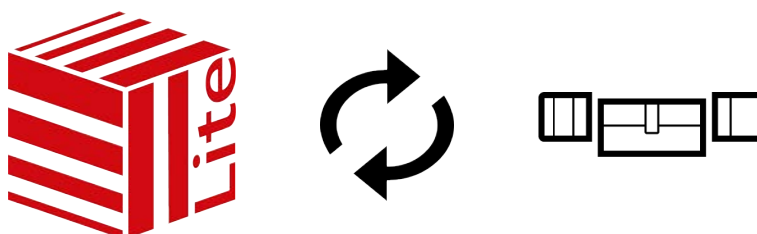
You can display the synchronisation requirement in the matrix. If you click directly on the  icon, you immediately start synchronising the entry concerned.

Initial or regular synchronisation

An initial synchronisation (symbol: ) differs from other synchronisations (symbol: ) due to the larger amount of data. In the case of AX locking devices, it is therefore preferable to use a SmartStick AX or a SmartCD.MP, especially for initial synchronisations.




7.1 Synchronising the locking device (including reading access list)




Synchronisation is bidirectional:

- Reading of data stored in the locking device (e.g. battery level)
- Writing of new data onto the locking device (e.g. authorisations)

Access lists can be imported separately (**Read access list**  button). Access lists can also be easily read during synchronisation as an option (see Reading access list/physical access list during synchronisation).

The imported data can then be displayed (see Display locking device equipment and status or Displaying and exporting a locking device's access list, for example).

- ✓ Suitable programming device connected.
1. Click on the locking device you wish to synchronise.
 - ↳ The locking device window will open.
 2. Click on the **Synchronisation** button .
 - ↳ Synchronise window will open.
 3. Select the programming device which you wish to use to synchronise from the ▼ **Programming device** drop-down menu.




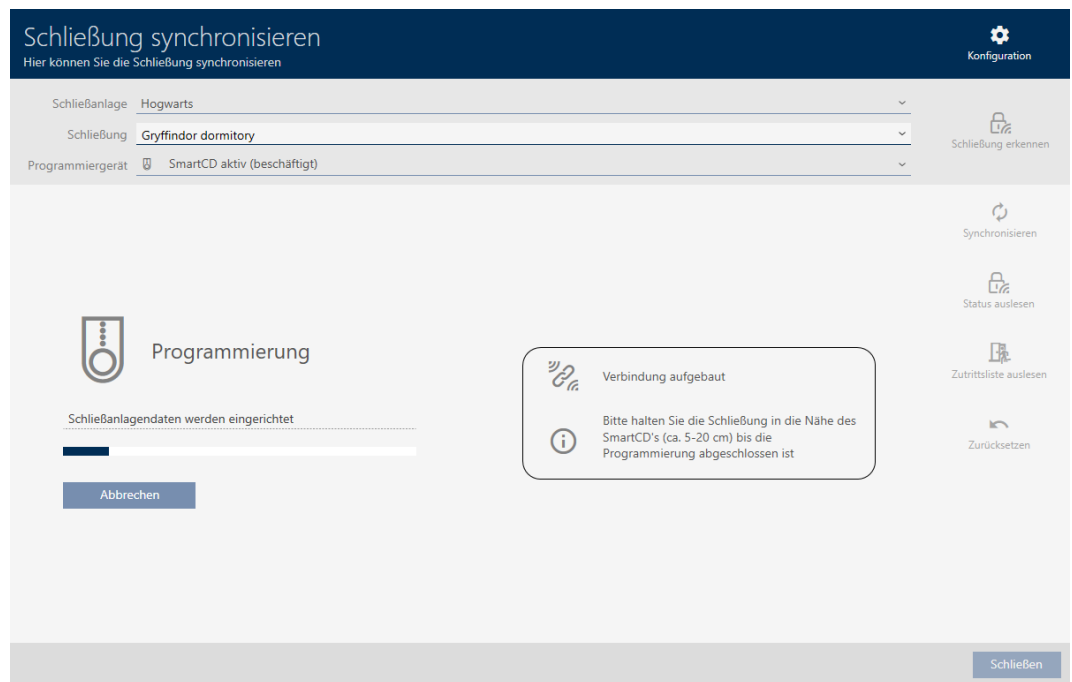
NOTE

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

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

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

4. Click on the **Synchronisation** button .
 - ↳ Locking device is being synchronised.



- ↳ Locking device is synchronised.




NOTE

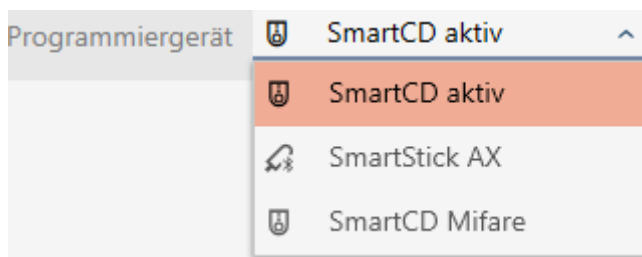
First transponder activation rejected after initial programming of AX products


If a transponder is the first identification medium to be activated after initial programming, the transponder can be rejected once and synchronised with the locking device in the background. Transponders will then function as normal.

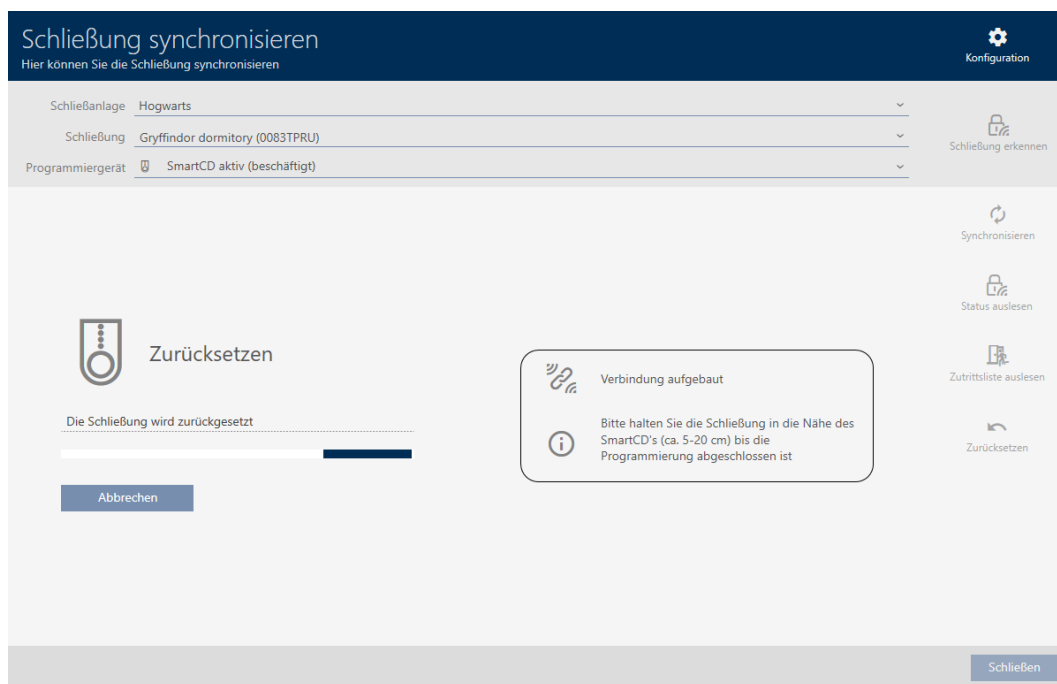
7.2 Re-setting the locking device

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.
- 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). 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.

7.3 Synchronising an identification medium

Synchronisation is bidirectional:

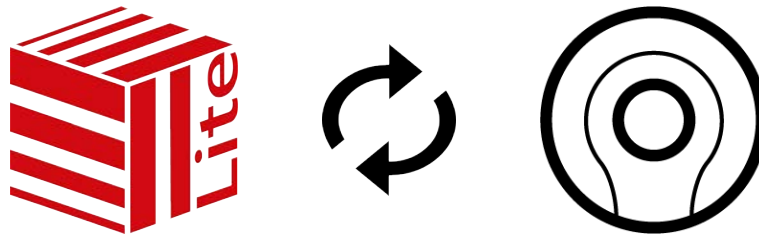
■ Importing of data stored in the identification medium (e.g. battery level)

■ 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).

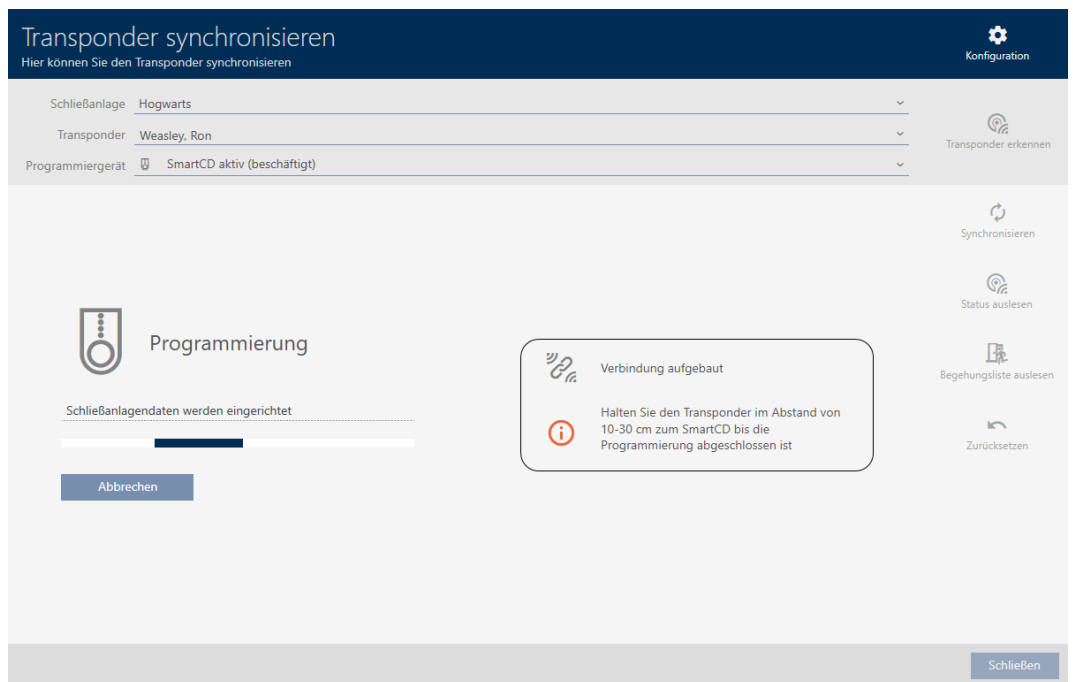
The imported data can then be displayed (see Displaying the identification medium battery status or Displaying and exporting physical access lists for cards/transponders, for example).

7.3.1 Synchronise a card/transponder (including importing physical access list)



The following example shows how to synchronise a transponder.

- ✓ Suitable programming device connected.
 - ✓ Identification media list or matrix view open.
1. Click on the identification medium you wish to synchronise.
 - ↳ The identification medium window will open.
 2. Click on the **Synchronisation** button 
 - ↳ Synchronise window will open.
 3. Click on the **Synchronisation** button 
 - ↳ Identification medium is synchronised.



↳ ID medium is synchronised.

7.4 Identifying an unknown ID medium

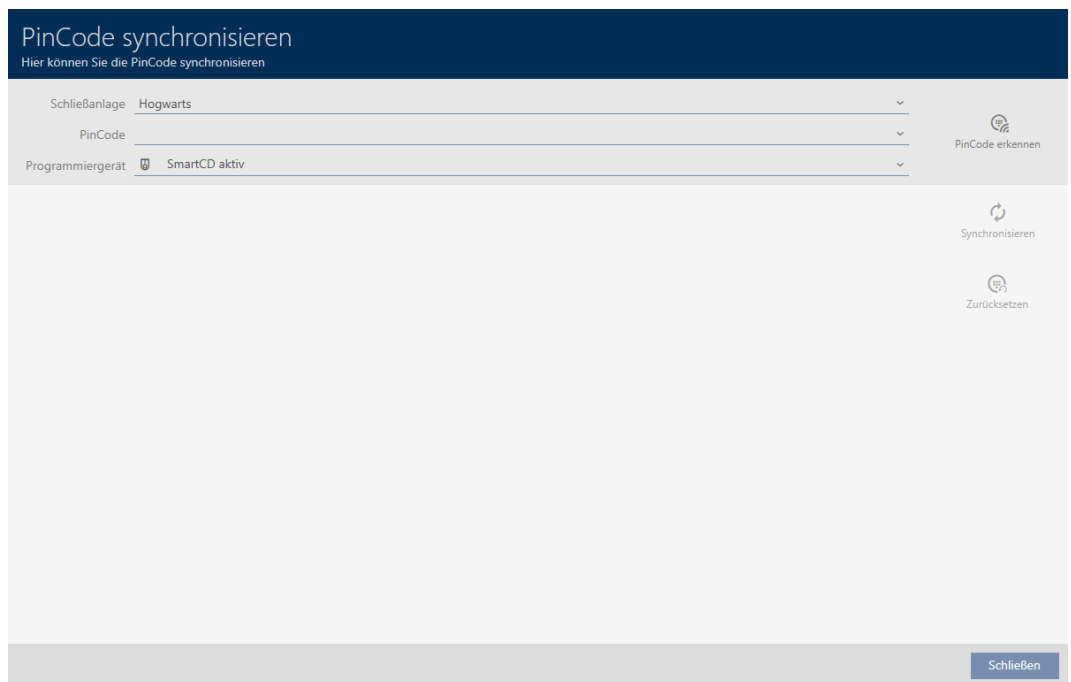
7.4.1 Identifying unknown PIN code keypad

- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)

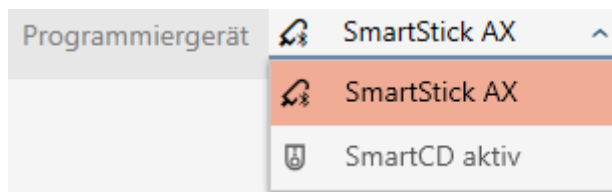
1. Click on the  icon in the header.




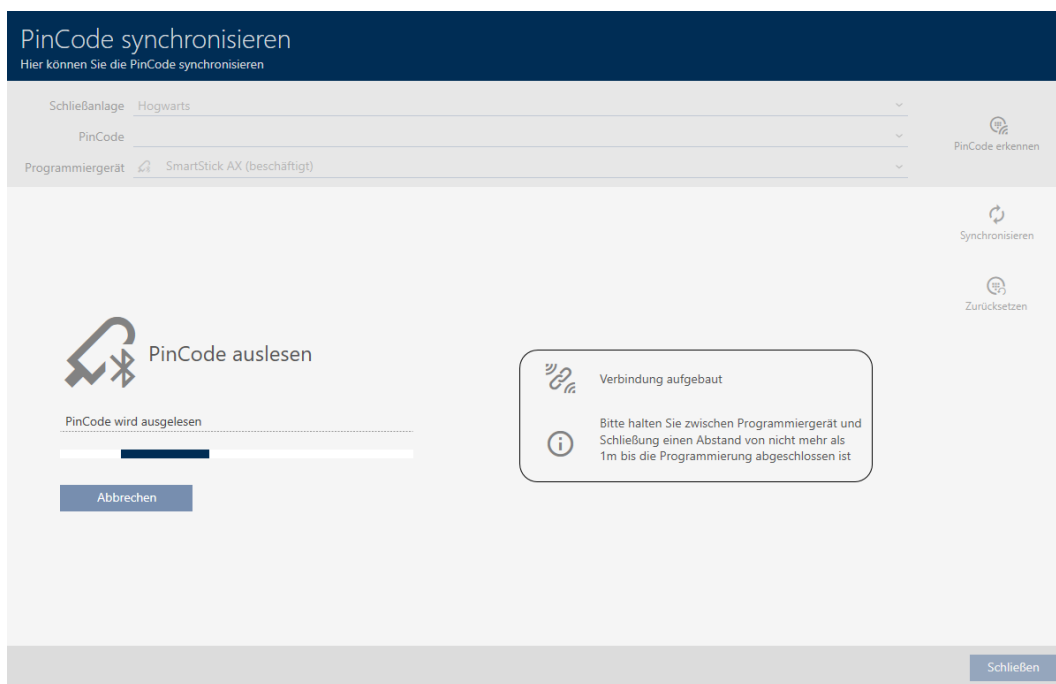
↳ The "Synchronise PinCode" window will open.



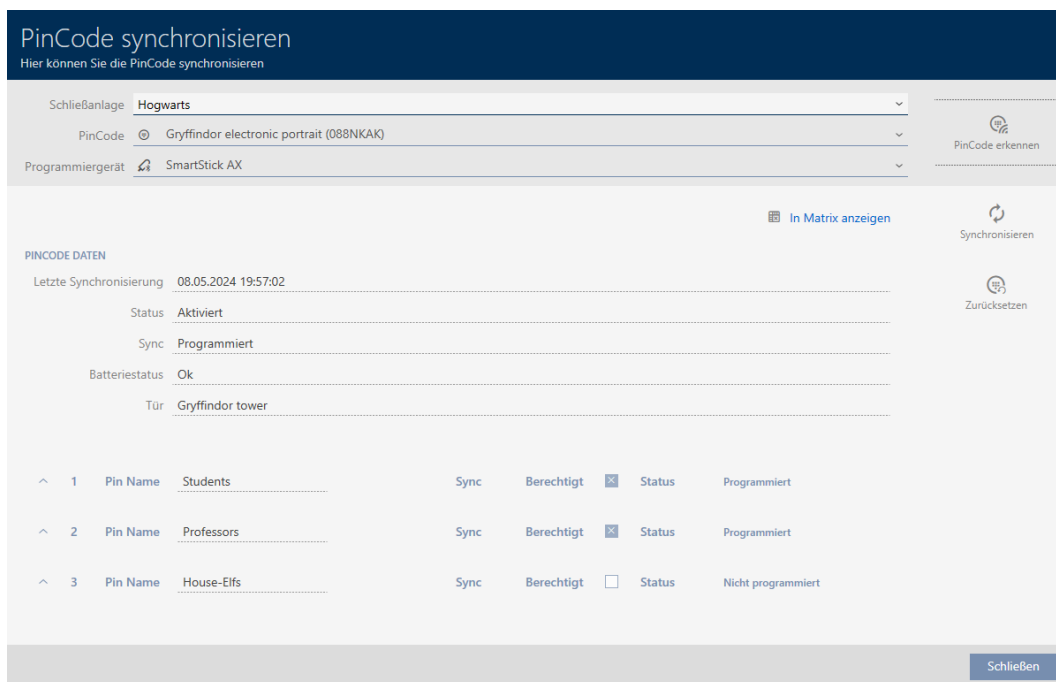
2. Select the programming device you wish to use to identify your PIN code keypad from the ▼ **Programming device** drop-down menu.



3. Click on the **Detect PinCode** button .
4. Follow the instructions as necessary.
 - ↳ PIN code keypad is being read.



↳ Information about the PIN code keypad is displayed in the window.



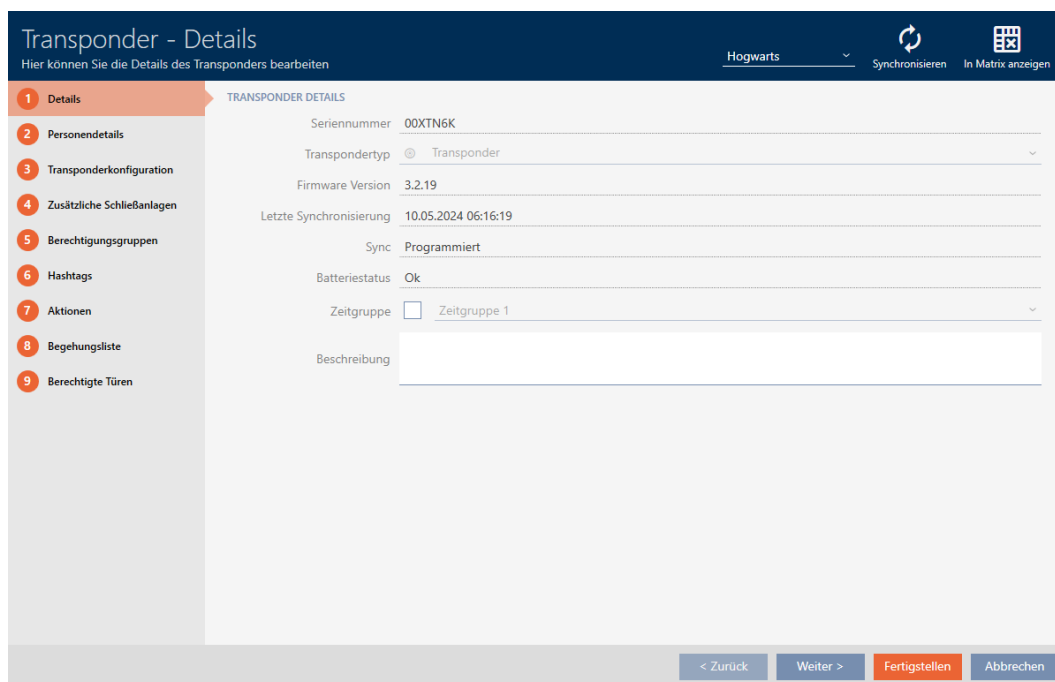
You can now reset the PIN code keypad, for example (see *Resetting the PIN code keypad* [▶ 73]).


7.5 Resetting identification media

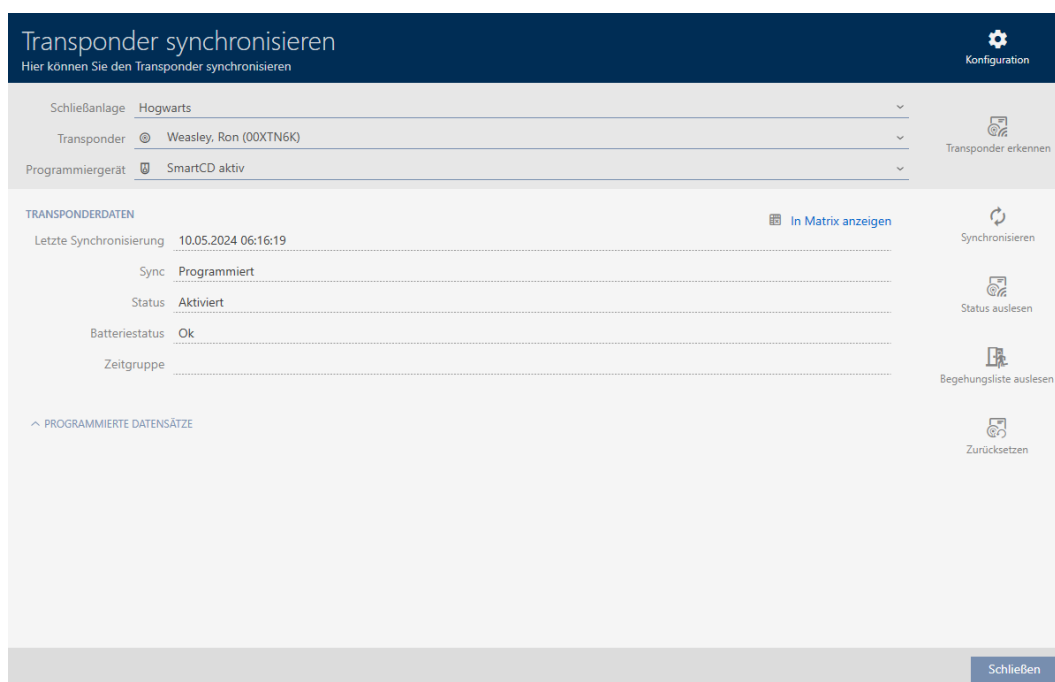
7.5.1 Resetting cards/transponders


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). Then continue.
 - ↳ The identification medium window will open.



2. Click on the **Synchronisation**  button.
 - ↳ Synchronise window will open.



3. Select the programming device you wish to use to reset your identification medium from the ▼ **Programming device** drop-down menu.
4. Click on the **Reset** button .
5. If necessary, select which of the existing data records you wish to reset.

Transponder zurücksetzen
Bitte wählen Sie die Datensätze aus, die zurückgesetzt werden sollen

Pos	Schließanlage	TID	Zeitgruppennummer	Deaktivierung
<input type="checkbox"/>	1 Unbekannt (Sid=1537)	3202		0 Aktiviert

OK **Abbrechen**



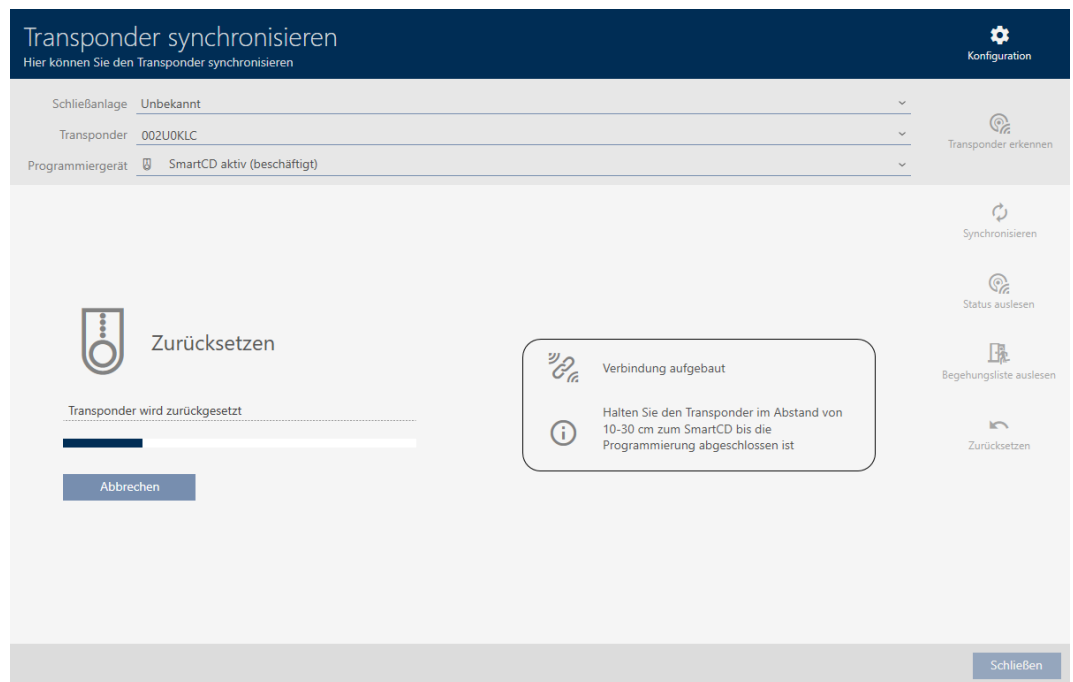
NOTE

Resetting data records from unknown locking systems

If a locking plan from a different project is stored on the identification medium, your AXM Classic 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 Classic does not know the locking system and thus doesn't know the locking system password either, you must enter the locking system password for the unknown locking system in this case.

6. If necessary, enter the locking system password for the locking system to which this data record belongs.
 - ↳ The checkbox for the data record to be reset is activated.
7. Click on the **OK** button.
8. Follow any further instructions as necessary.
 - ↳ Identification medium is being reset.



↳ Identification medium is reset.

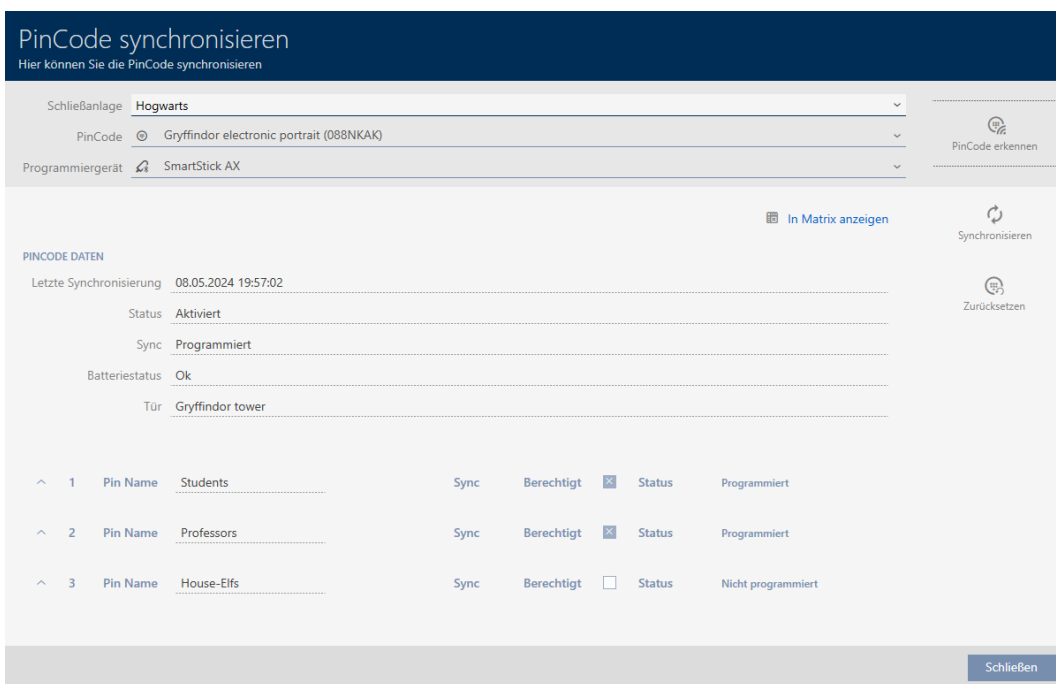
7.5.2 Resetting the PIN code keypad


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.

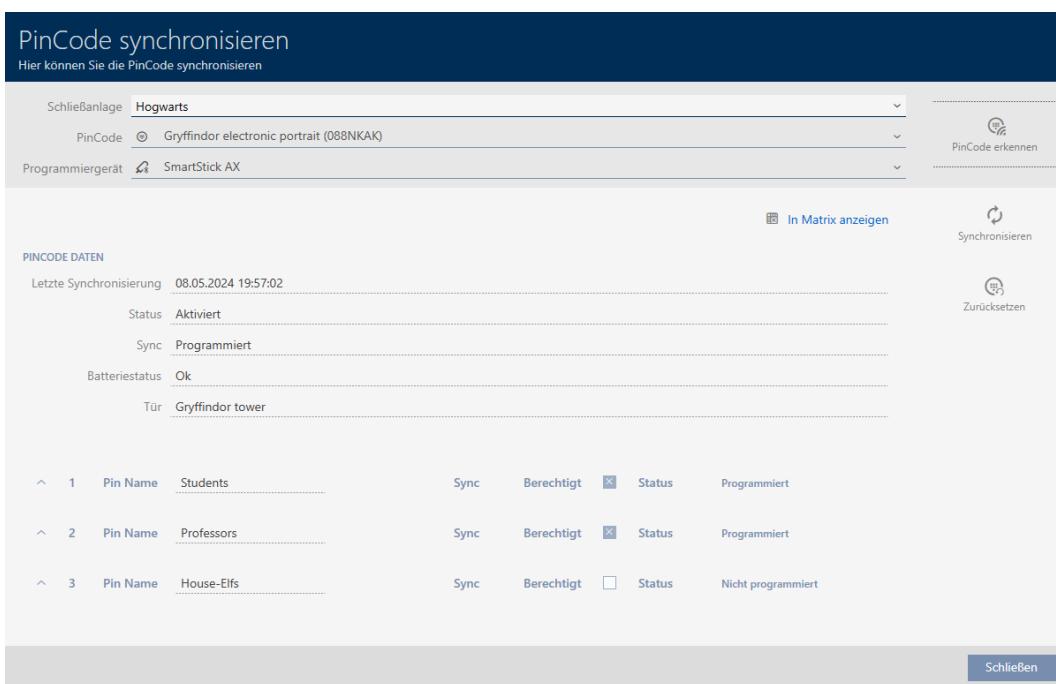
- ✓ Suitable programming device connected (SmartStick AX for PIN code keypad AX, SmartCD2.G2 for PIN code keypad 3068)
- ✓ PIN code list or matrix screen open.

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* [▶ 68] in the AXM manual). Then continue.

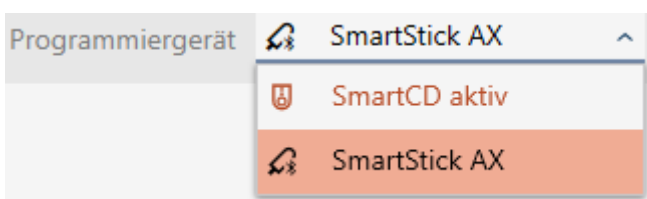
↳ The PIN code keypad window will open.



- Click on the **Synchronisation**  button.
↳ Synchronise window will open.



- Select the programming device from the **▼ Programming device** drop-down menu with which you wish to reset your PIN code keypad.



4. Click on the **Reset** button .



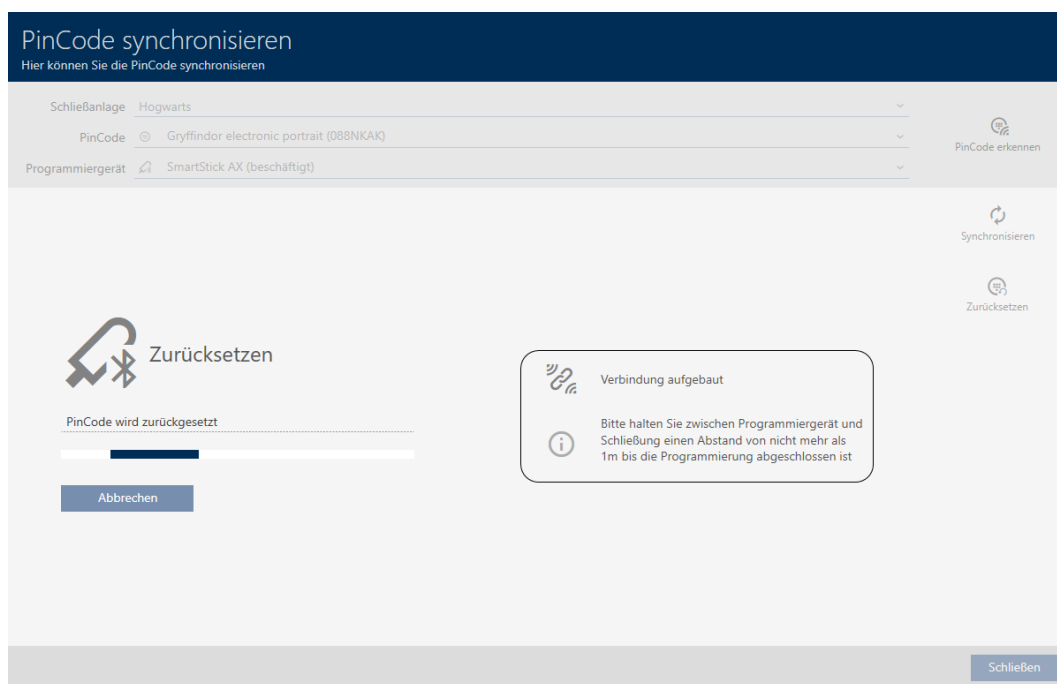
NOTE

Resetting PIN code keypads that do not form part of the project

Your AXM Classic can also reset PIN code keypads that were not created in the same project. In this case, however, your AXM Classic 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.

Information

Die PinCode wurde erfolgreich zurückgesetzt



OK



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.

© 2024, SimonsVoss Technologies GmbH, Unterföhring

All rights are reserved. Text, images and diagrams are protected under copyright law.

The content of this document must not be copied, distributed or modified. More information about this product can be found on the SimonsVoss website. Subject to technical changes.

SimonsVoss and MobileKey are registered brands belonging to SimonsVoss Technologies GmbH.

SimonsVoss
technologies

Made in Germany

A BRAND OF


ALLEGION™