AX MANAGER

The next dimension of Locking System Management

AXM Lite
Short manual

Manual

15.06.2023

SimonsVoss technologies

ALLEGION

Contents

1 First steps after a new installation

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

You will see the following input fields:

- Project name
- Username
- New password
- Repeat password

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

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

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

The first locking system password is generated automatically and saved in a text file (`Documents/SimonsVoss`).
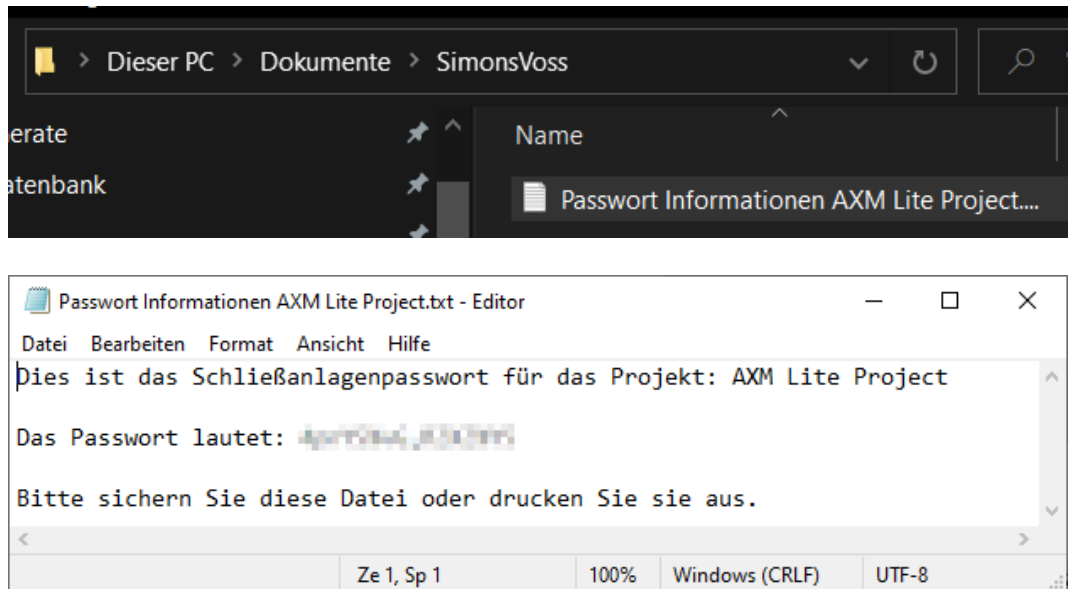
You can change the locking system password (see Changing locking system password).

<div style="background:yellow">

IMPORTANT

</div>

Keep locking system password accessible and secure

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

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

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

Launching AXM Classic for the first time

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

1. Add locking device
2. Add transponder

Kein Transponder vorhanden	Keine Schließung vorhanden
Es sind noch keine Transponder vorhanden. Wollen Sie jetzt einen anlegen?	Es ist noch keine Schließung vorhanden. Wollen Sie jetzt eine anlegen?
Ja Nein	Ja Nein

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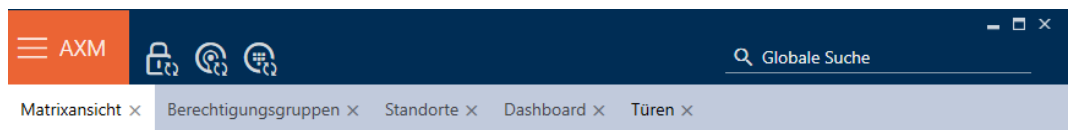
If you are working with a locking system for the first time, you will find explanations and background information here: Background knowledge and explanations.

2 The AXM's structure
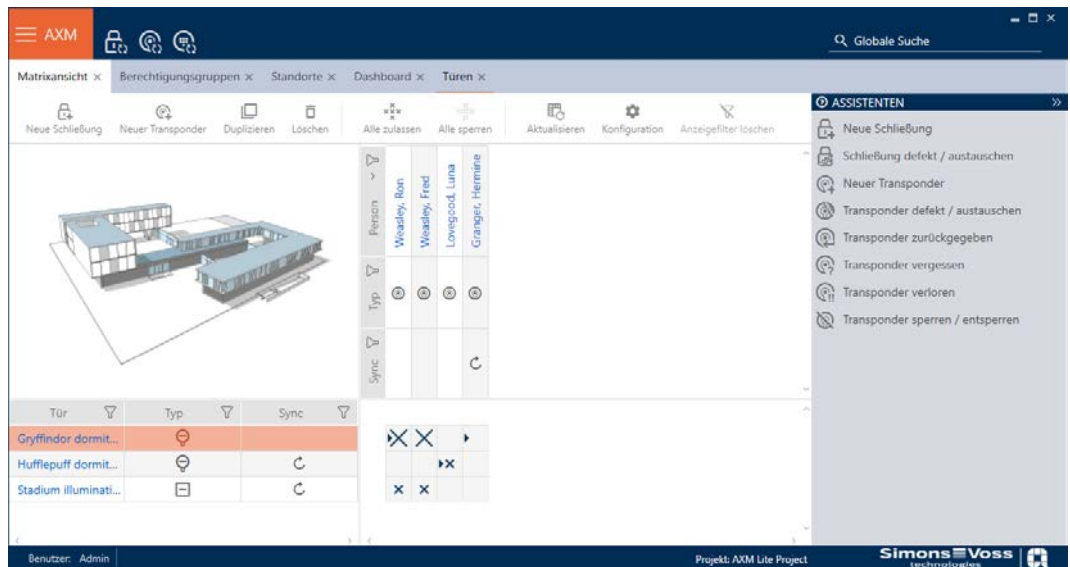
The AXM Classic interface consists primarily of four large sections:

AXM bar and tabs

Use the orange AXM button ☰ AXM 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
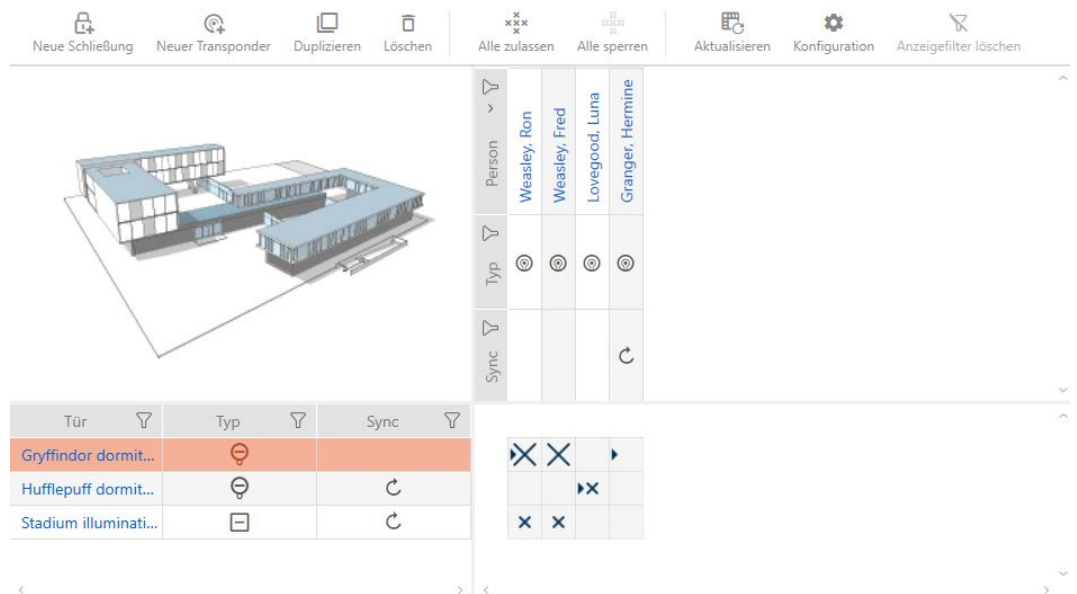
The matrix section is the engine room behind your AXM Classic. This is where you can see all locking devices and identification media. You can use the filter function to hide entries and thus gain an overview (see *Sorting and filtering [▶ 8]*).

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 [▶ 23]*). 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. If you see the synchronise icon ♻ here, you need to synchronise (see *Synchronisation: Comparison between locking plan and reality [▶ 29]*). 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:
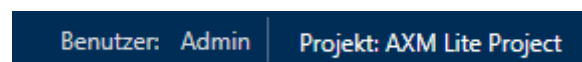
Wizard menu
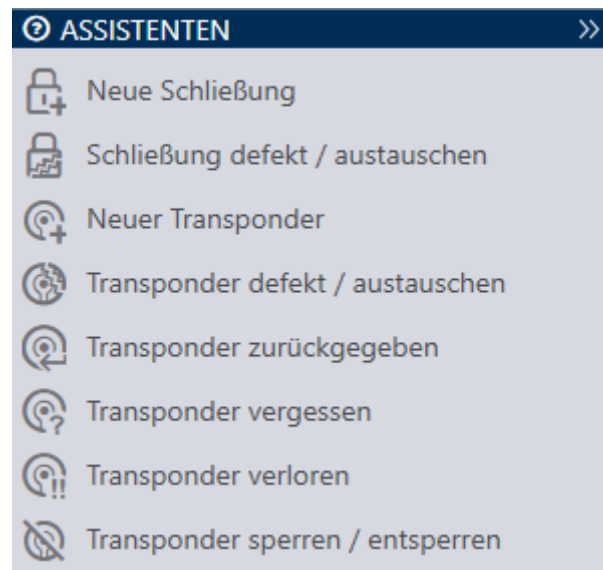
There is a wizard menu on the right side of your AXM Classic. This is where you will find wizards to assist you in situations that occur frequently (e.g. lost identification media).

If you need more space, you can use Assistenten wegklappen: >> [offen] to hide the wizard menu and Assistenten ausklappen: << [offen] 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.
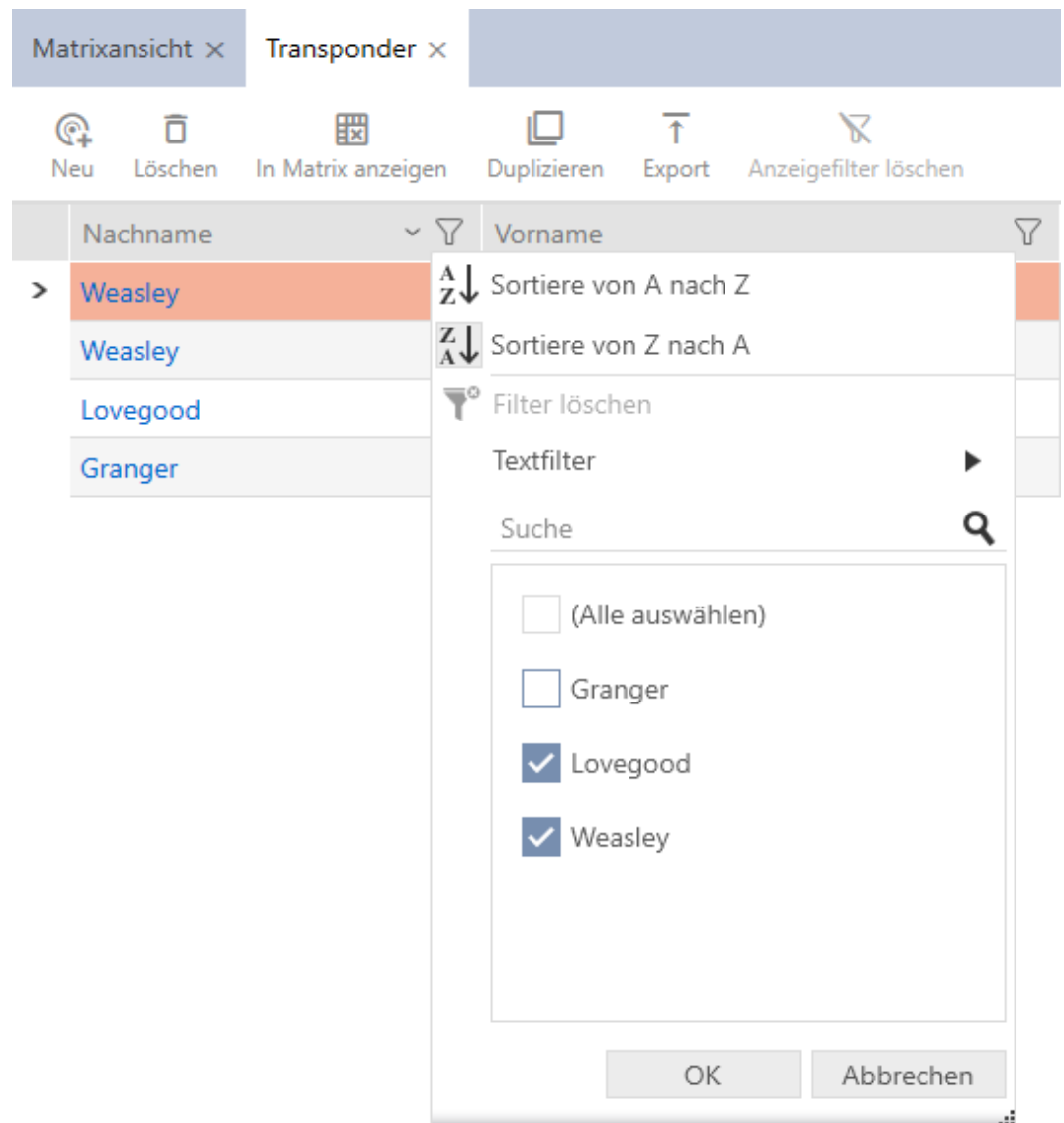
3. Click on the OK button.
   ↳ The filter menu will close.

↳ Entries will now be filtered when displayed.

3 Organisational structure

3.1 Creating authorisation groups

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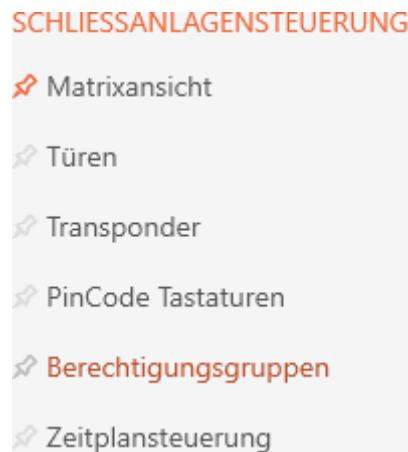   ↳ AXM bar opens.
2. Select the Access Levels entry in the | LOCKING SYSTEM CONTROL | group.

SCHLIESSANLAGENSTEUERUNG

📌 Matrixansicht

🔖 Türen

🔖 Transponder

🔖 PinCode Tastaturen

📌 Berechtigungsgruppen

🔖 Zeitplansteuerung

   ↳ 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 an identification medium (including importing physical access list) [▸ 32]*).

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).

NOTE

Activating the PIN code keypad

AXM Classic also supports the PIN code keypad but it is not displayed for your locking system by default.

▪▪ Activate the PIN code keypad for your locking system manually if required (see Enabling PIN code keypads).

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 [▸ 25]* (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 needs time-controlled authorisations: Activate the ☑ Time group check box.
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): Activate the ☑ Long opening check box.
8. If locking devices should not beep for this identification medium: Activate the ☐ No acoustic opening signal check box.
9. If the locking devices on which the identification medium was used need to be saved on the identification medium: Activate the ☑ Audit trail check box.
10. If the transponder is not to be used immediately: Activate the ☐ as of now check box. Then enter an activation date.
11. If the transponder is only to be used for a limited period: Activate the ☐ Without expiration date check box. Then enter an expiration 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 [▸ 8]*).
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 [▶ 8]*).

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. Activate the ☑ Create additional objects check box to exit 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.

4.2 Blocking and replacing 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. 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).

✓ 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 [▶ 8]*).

2. Select the identification medium that has been lost/stolen.

3. Click the �e Transponder lost button in the "Wizards" section.

↳ Wizard for handling a lost identification medium will open.

4. Click on the Continue button.
   ↳ The reason window will open.
5. Enter the reason in the drop-down menu.
6. Click on the OK button.
   ↳ Query about replacement identification medium will open.
7. Click on the Yes button.
   ↳ Query about replacement identification medium closes.
   ↳ Replacement identification medium can already be seen in the matrix in the background.

↳ Query about synchronising the replacement identification medium will open.

8. Click on the Yes button.

↳ Query about synchronising the replacement identification medium closes.

↳ Synchronisation starts.

↳ Lost identification medium is blocked.

↳ Replacement identification medium is synchronised.

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

IMPORTANT

Blocking IDs not transmitted to locking devices in Lite edition

In the Lite edition locking devices cannot be updated with blocking IDs.

⠒ Synchronize affected locking devices manually.

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) [▸ 29]*).

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).

▪ 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 [▸ 25]* (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 `Schließungseigenschaften: Fertiigstellen [offen]` 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.

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 ▼ **Buildings** drop-down menu is limited to the buildings in the selected location.

7. Select the building where your locking device is installed from the ▼ **Buildings**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.
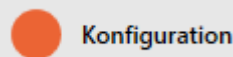
↳   Window switches to the Configuration tab.

10. If you wish to log access attempts: Expand the "Time configuration" menu and make the settings (see Have accesses logged by locking device (access list)).

11. If you wish to change the opening interval or use close range mode: Expand the "Lock functions" menu and make the settings (see Leaving the locking device open for longer, less time or permanently and Limit locking device read range (close range mode)).

12. If you wish to change the signalling of battery warnings or programming acknowledgements: Expand the "Feedback signals" menu and make the settings (see Muting a locking device (for battery warnings and programming)).

13. If you wish to ignore the activation time slot (see Activation date / expiry date): Expand the "AX functions" menu and make the settings (see Ignoring activation and expiry date of identification media).

14. If you wish to use the internal and external antenna together with a SmartRelay: Expand the "Relay functions" menu and make the settings (see Using internal and external antenna simultaneously).

15. If you wish to engage and disengage your locking device automatically: Expand the "Time switching - Configuration" menu and make the settings (see Engaging and disengaging locking devices automatically with time switchover).

16. If you wish to change the signalling for a SmartRelay or use the serial interface: Expand the "Extended configuration" menu and make the settings (see Changing the SmartRelay settings).

17. Click on the Access levels tab.

🔴 Berechtigungsgruppen

   ↳ Window switches to the Access levels tab.

18. Use 🔽 to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 8]*).

19. 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.

---

20. 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.

21. Click on the Hashtags tab.

🔴 Hashtags

   ↳ Window switches to the Hashtags tab.

22. Use 🔽 to sort/filter the displayed entries if required (see *Sorting and filtering [▸ 8]*).

23. 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.

---

24. 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.

25. Activate the ☑ Create additional objects check box to leave the window with the same settings open for the next locking device to be created.

26. 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.

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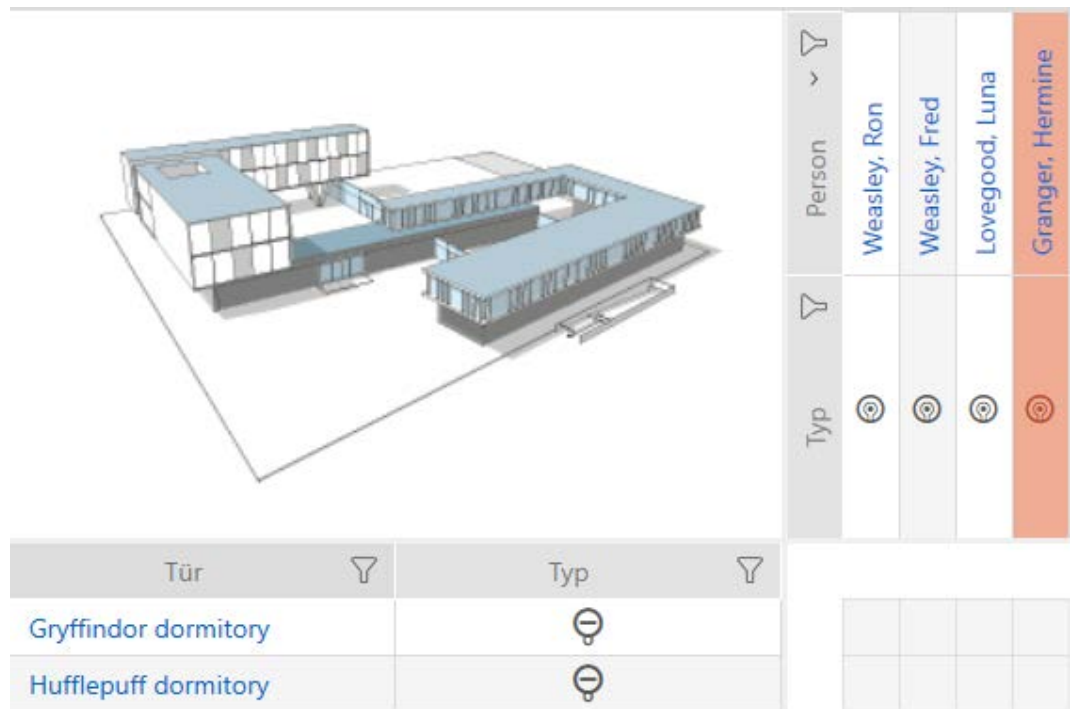   ↳ Authorisation is issued for the identification medium concerned (column) on the locking device in question (row).

2. Click on the same box again.
   ↳ Authorisation is withdrawn again.

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):

⠿ 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

Alle zulassen   Alle sperren

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 Matrixansicht: Alle zulassen [offen] ✛ and Matrixansicht: Alle sperren [offen] ✛ 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

✓ Locking device available.

1. Use ▽ to sort/filter the displayed entries if required (see *Sorting and filtering [▶ 8]*).

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

3. Click on the Matrixansicht: Alle zulassen [offen] ✛ button.

↳ All displayed identification media are authorised for the selected locking device.

If you then use the button to remove the Matrixansciht: Anzeigefilter löschen [offen] filter again, you will find that the identification media that were filtered out were actually not permitted:
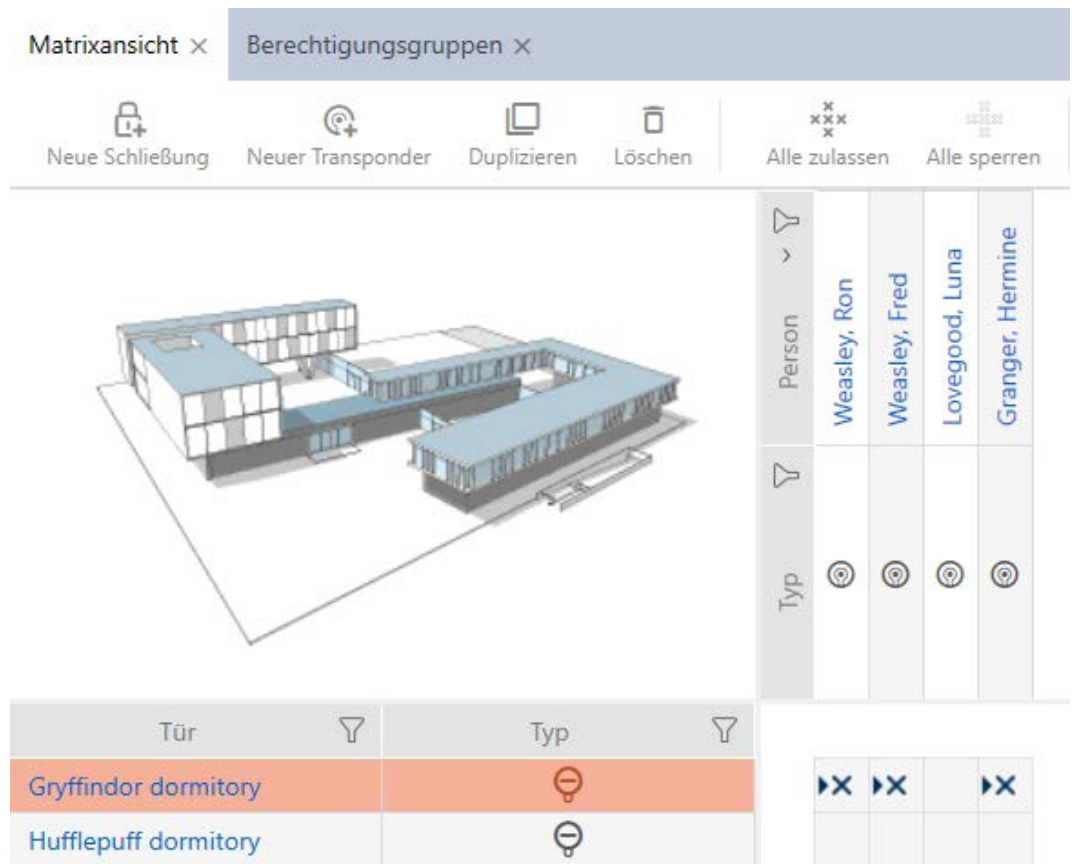
6.2.2 Authorisation groups

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

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
▸	Authorisation by an authorisation group available, but this authorisation was removed manually before programming.
	Authorised and programmed, but identification medium has been blocked (e.g. after theft).
	Not authorised; identification medium has been blocked (e.g. after theft).

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
Synchronising the locking device (including reading access list) [▶ 29]	*Synchronise an identification medium (including importing physical access list) [▶ 32]*
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.

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 e.g. Displaying and exporting a locking device's access list or Display locking device equipment and status).

✓ 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.
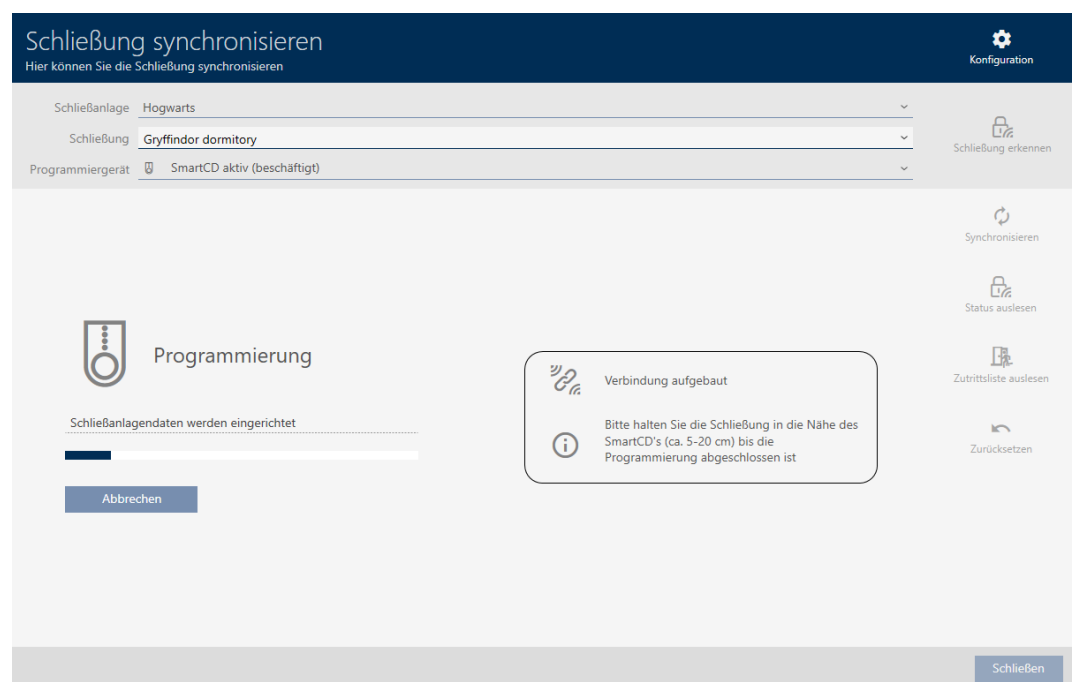
↳ Locking device is synchronised.

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 is 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.

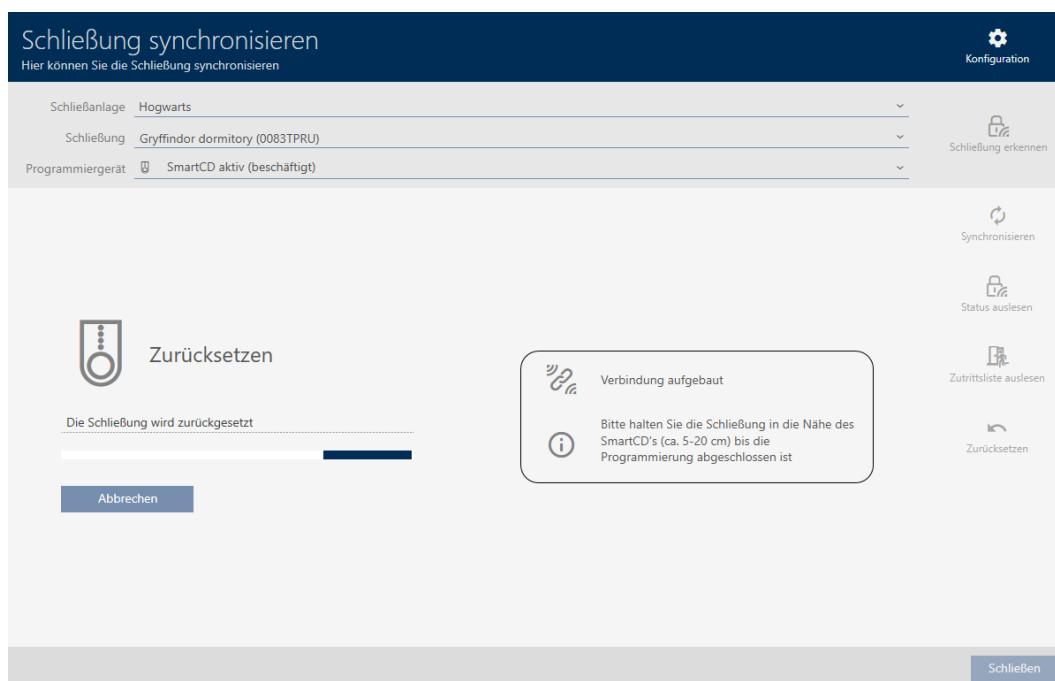2. Select the programming device from the ▼ **Programming device** drop-down menu with which you wish to reset your locking device.

3. Click on the Synchronisation: 🔄 button.
   ↳ Synchronise window will open.

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 Synchronise an identification medium (including importing physical access list)

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 🔲 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 e.g. Displaying and exporting the physical access list of an identification medium or Displaying the transponder battery status).

✓ Suitable programming device connected.

1. Click on the identification medium you wish to synchronise.
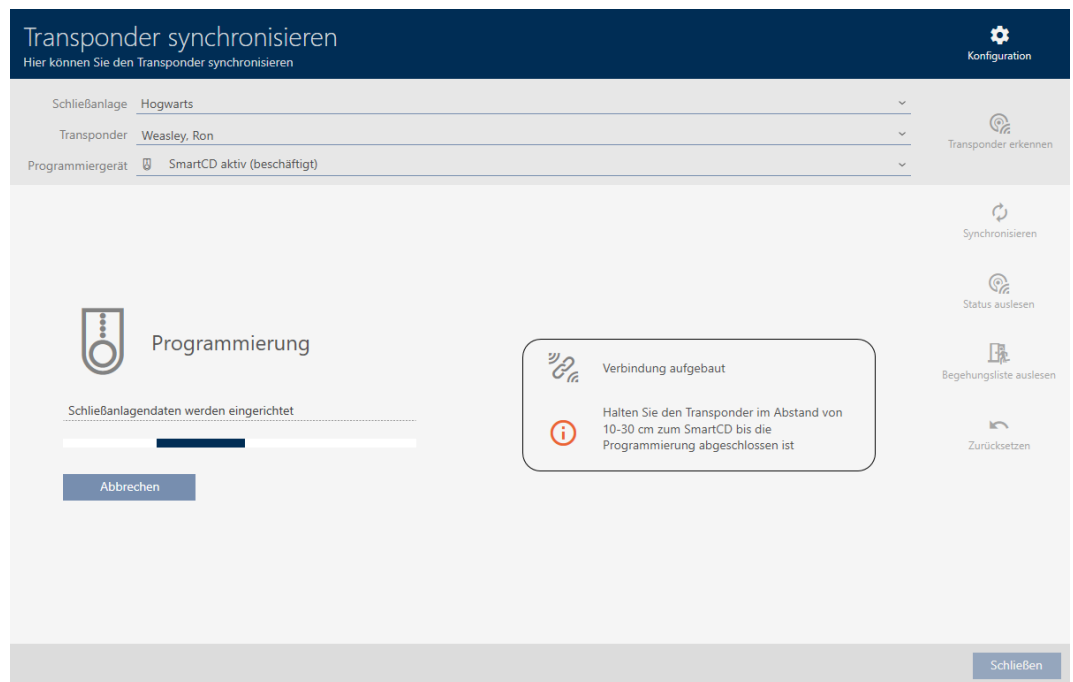   ↳ The identification medium window will open.
2. Click on the Synchronisation: ↻ button.
   ↳ Synchronise window will open.
3. Select the programming device which you wish to use to synchronise from the ▼ **Programming device** drop-down menu.
4. Click on the Synchronisation: ↻ button.
   ↳ Identification medium is synchronised.

↳ ID medium is synchronised.
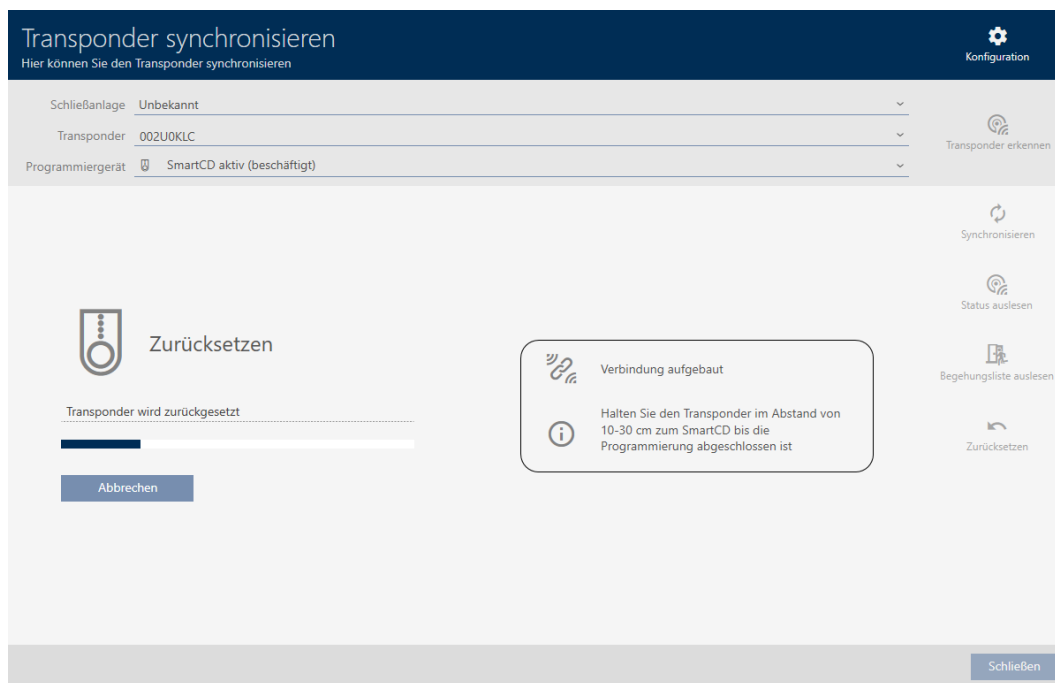
7.4 Resetting the identification medium

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.

1. Click on the identification medium you wish to reset.
   If the identification medium is not available in your locking system: Click on any identification medium and identify the identification medium (see Identifying an unknown ID medium). 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 identifica-tion 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.

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.

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.

SimonsVoss
technologies

Made in Germany

A BRAND OF
ALLEGION