



MobileKey

Manual

22.01.2024

Simons  Voss
technologies

Contents

1.	Introduction	4
1.1	System requirements.....	5
1.1.1	Locking system management.....	5
1.1.2	Programming.....	6
2.	General safety instructions	8
3.	Product-specific safety instructions	11
4.	Meaning of the text formatting	12
5.	The matrix	13
6.	Basic functions	17
6.1	Creating a lock.....	17
6.2	Add key.....	18
6.3	Add PIN code keypad.....	19
6.4	Issue authorisation and save.....	21
6.5	Assign time plan.....	21
6.6	Programming components.....	25
6.6.1	IMPORTANT: Programming on a Windows device.....	26
6.6.2	IMPORTANT: Programming on an Android device.....	26
6.6.3	IMPORTANT: Programming on a macOS device.....	26
6.7	Resetting components.....	27
6.8	Forced component deletion.....	27
6.9	Exporting the component list.....	28
6.10	Read access event log.....	31
6.11	Changing the colour scheme.....	33
7.	MobileKey online upgrade	35
7.1	SmartBridges.....	36
7.1.1	Setting up SmartBridges.....	36
7.1.2	Setting up SmartBridges.....	37
7.1.3	Deleting SmartBridge.....	39
7.2	Creating a lock with online upgrade.....	40
7.3	Deleting a lock with online upgrade.....	42
7.4	Adding a PIN code keypad with online upgrade.....	42
7.5	Deleting a PIN code keypad with online upgrade.....	43
7.6	Configure network.....	44
7.7	Programming of components with online upgrade.....	44

7.8	Disconnecting components with online upgrade.....	46
7.9	Carrying out remote opening.....	46
7.10	Key4Friends.....	47
7.10.1	Sharing keys.....	49
7.10.2	Managing keys.....	50
7.11	DoorMonitoring locking device - displayed locking statuses.....	51
8.	Event management	54
8.1	Creating rules.....	55
8.2	Important information	57
9.	Settings.....	58
10.	Fault rectification	60
10.1	Key lost, damaged or stolen	60
10.2	Defective lock.....	62
10.3	Reset or re-use deleted components	63
10.4	Read components	63
10.5	SmartBridge does not work	64
10.6	PIN code keypad with online upgrade does not work.....	66
10.7	Lock with online upgrade does not work.....	66
10.8	Network error.....	66
10.9	Manual resetting of LockNodes	66
11.	Maintenance, cleaning and disinfection	68
12.	MobileKey apps.....	69
13.	Tips & Tricks	70
13.1	Link to the web app.....	70
13.2	Using keys without the USB config device.....	70
13.3	Setting the language	70
14.	Help and other information	72

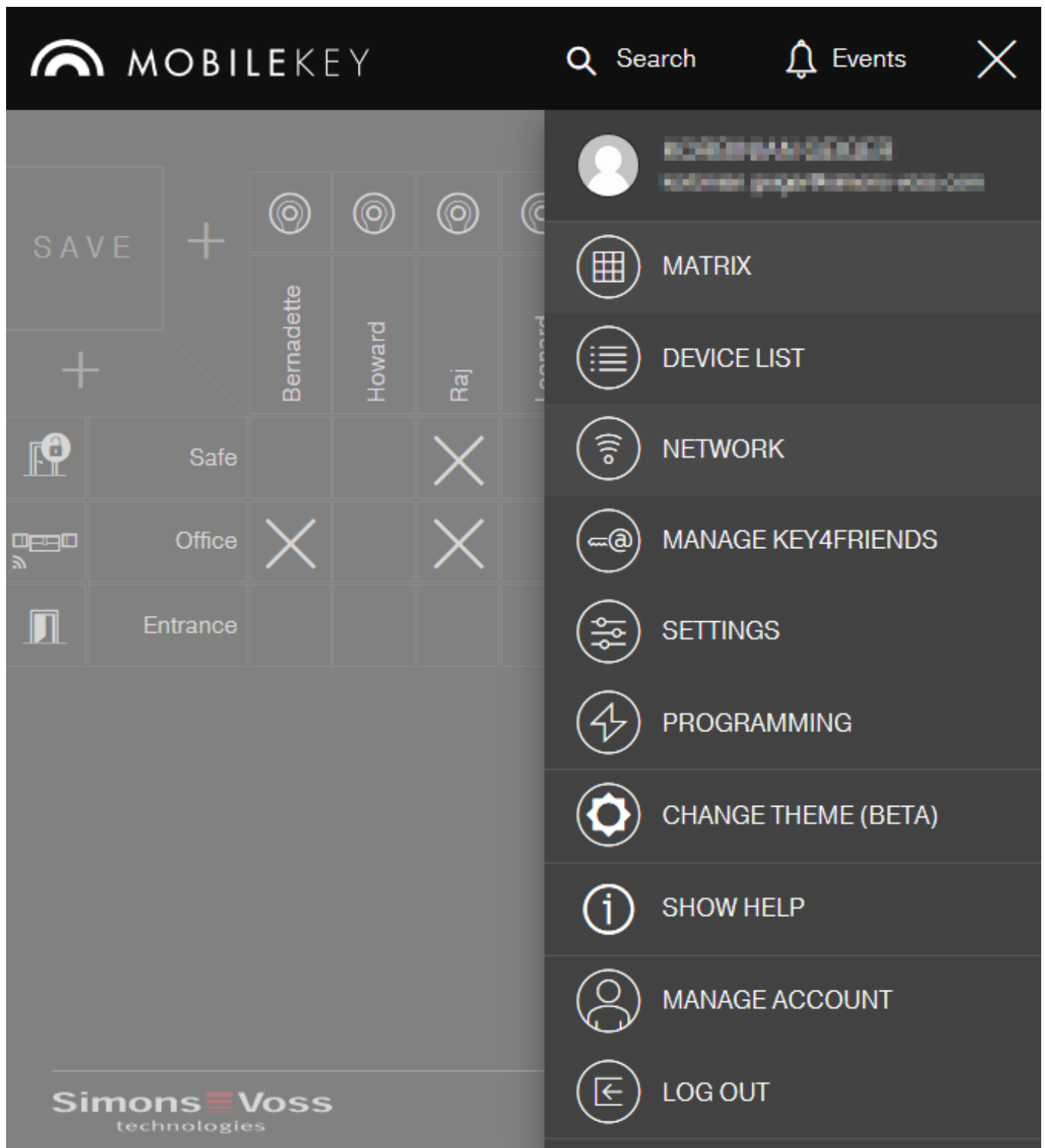
1. Introduction

MobileKey is a separate product category for small locking systems. You can administer up to 100 keys (*transponders*) and 20 locking devices (*locking cylinders and SmartRelays*).



NOTE

The locking plan is managed using the MobileKey web application only. You can access the application at www.my-mobilekey.com. Just click on "Login web app" to access the application directly. Here, you simply create a free user account to work with MobileKey.



1.1 System requirements

1.1.1 Locking system management

The locking plan can be **displayed and edited** using any standard browser, irrespective of the platform. Basically, no special hardware is required, although the terminal device should support the latest version of one of the following browsers:

- Microsoft Internet Explorer
- Mozilla Firefox
- Google Chrome
- Apple Safari
- Opera

You also need to have a permanent internet connection at all times. A high-speed Internet access is required to work without interruption.

1.1.2 Programming

You can programme the MobileKey locking components with the USB config device with the following devices:

■ Windows device

- Operating system: Windows Server 7, 8 or 10.
- Hardware: USB port to connect the USB config device.
*No special hardware configurations are required for programming.
The operating system must be stable and run free of errors.*
- The current version of Microsoft .NET Framework (at least Version 3.5) must be installed on the computer.

Follow the instructions on programming app installation to programme the MobileKey locking components.

■ Android device

- You need to install the programming app from the Google Play Store to use the MobileKey app.
Changes to the locking plan are made in the browser, such as the MobileKey web app.
- The USB config device can be connected directly to the Android device or using an OTG cable available separately.
The Android device must support the OTG function in such a case. If you are not sure whether your Android device supports OTG or not, you can use a suitable app from Google Play to check this function. Search for "OTG check", for example.
Important: Such apps have nothing to do with SimonsVoss Technologies GmbH. We therefore accept no liability for any damages or problems caused by such apps.

Use the MobileKey web app to launch the MobileKey app to programme the MobileKey locking components.

❑ macOS device

- ❑ Operating system: OS X 10.11 El Capitan or higher
- ❑ Hardware: USB port to connect the USB config device.

*No special hardware configurations are required for programming.
The operating system must be stable and run free of errors.*

❑ Optional: Online via SmartBridge

Locking devices can also be programmed online with a USB config device. See *Programming of components with online upgrade [▶ 44]*. In this particular case, only the transponders need to be programmed with the aid of the USB config device.

Tip:

*If there should be no Windows or Android devices available for programming new keys, it is recommended to programme additional transponders as a reserve. These can then be assigned to networked online locks at a later stage. See *Using keys without the USB config device [▶ 70]* for more information.*

2. General safety instructions

Signal word: Possible immediate effects of non-compliance

WARNING: Death or serious injury (possible, but unlikely)

CAUTION: Minor injury

IMPORTANT: Property damage or malfunction

NOTE: Low or none



WARNING

Blocked access

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

Blocked access through manipulation of the product

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

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

Do not swallow battery. Danger of burns from hazardous substances

This product contains lithium button cell batteries. Swallowing the button cell battery, in can result in severe internal burns leading to death in as little as two hours.

1. Keep new and used batteries away from children.
2. If the battery compartment does not close securely, cease using the product and keep it away from children.
3. If you think batteries have been swallowed or are in any part of the body, seek medical attention immediately.

Risk of explosion due to incorrect battery type

Inserting the wrong type of battery can cause an explosion.

- ❑ Only use the batteries specified in the technical data.



CAUTION

Fire hazard posed by batteries

The batteries used may pose a fire or burn hazard if handled incorrectly.

1. Do not try to charge, open, heat or burn the batteries.
2. Do not short-circuit the batteries.

IMPORTANT**Damage resulting from electrostatic discharge (ESD)**

This product contains electronic components that may be damaged by electrostatic discharges.

1. Use ESD-compliant working materials (e.g. Grounding strap).
2. Ground yourself before carrying out any work that could bring you into contact with the electronics. For this purpose, touch earthed metallic surfaces (e.g. door frames, water pipes or heating valves).

Damage resulting from liquids

This product contains electronic and/or mechanic components that may be damaged by liquids of any kind.

- ❑ Keep liquids away from the electronics.

Damage resulting from aggressive cleaning agents

The surface of this product may be damaged as a result of the use of unsuitable cleaning agents.

- ❑ Only use cleaning agents that are suitable for plastic or metal surfaces.

Damage as a result of mechanical impact

This product contains electronic components that may be damaged by mechanical impacts of any kind.

1. Avoid touching the electronics.
2. Avoid other mechanical influences on the electronics.

Damage as a result of overcurrent or overvoltage

This product contains electronic components that may be damaged by excessive current or voltage.

- ❑ Do not exceed the maximum permissible voltages and/or currents.

Damage due to polarity reversal

This product contains electronic components that may be damaged by reverse polarity of the power source.

- ❑ Do not reverse the polarity of the voltage source (batteries or mains adapters).

Operational malfunction due to radio interference

This product may be affected by electromagnetic or magnetic interference.

- ❑ Do not mount or place the product directly next to devices that could cause electromagnetic or magnetic interference (switching power supplies!).

Communication interference due to metallic surfaces

This product communicates wirelessly. Metallic surfaces can greatly reduce the range of the product.

- ❑ Do not mount or place the product on or near metallic surfaces.

**NOTE****Intended use**

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

- ❑ Do not use SimonsVoss products for any other purposes.

Malfunctions due to poor contact or different discharge

Contact surfaces that are too small/contaminated or different discharged batteries can lead to malfunctions.

1. Only use batteries that are approved by SimonsVoss.
2. Do not touch the contacts of the new batteries with your hands.
3. Use clean and grease-free gloves.
4. Always replace all batteries at the same time.

Different times for G2 locks

The internal time unit of the G2 locks has a technical tolerance of up to ± 15 minutes per year.

Qualifications required

The installation and commissioning requires specialized knowledge.

- ❑ Only trained personnel may install and commission the product.

Incorrect installation

SimonsVoss Technologies GmbH accepts no liability for damage caused to doors or components due to incorrect fitting or installation.

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

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

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

3. Product-specific safety instructions

**NOTE**




All options in the online extension require a correctly configured MobileKey radio network. You can only perform any of the online functions if a stable Internet connection and power supply are guaranteed.

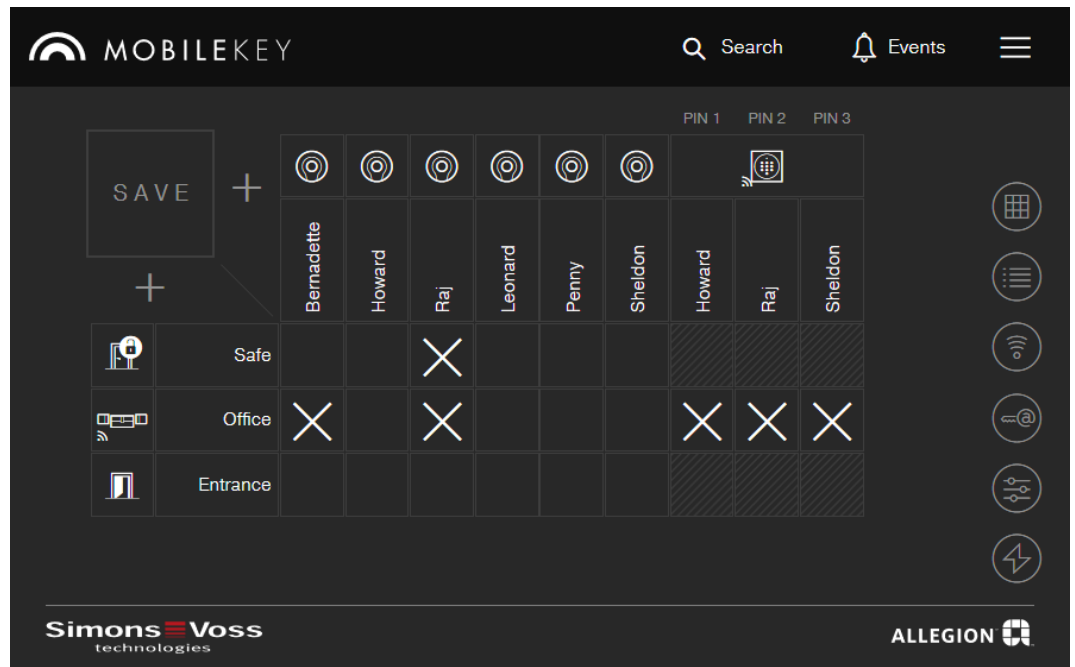
4. Meaning of the text formatting

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

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



5. The matrix

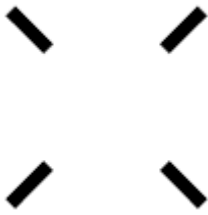
The matrix provides a clearly arranged view of the entire locking system. This view is thus the centre point for all functions. All keys (e.g. transponders) are displayed horizontally and all locking devices (e.g. locking cylinders) vertically. Important menus can be called via the interfaces  Search ,  Events and .



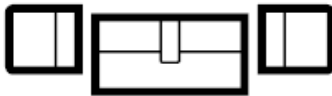


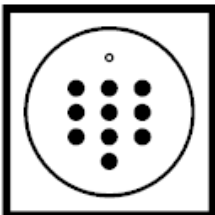
Different systems are used to keep the matrix as straightforward as possible.

Authorisations

Icon	Description
	Authorisation cross: New Authorisation has been configured, but not programmed yet.
	Authorisation cross: Set The authorisation has been set and is active.

Icon	Description
	<p>Authorisation cross: Remove</p> <p>Authorisation has been configured, but not programmed yet.</p>
	<p>Authorisation cross: No authorisation</p> <p>If none of the previous three crosses are displayed, there is currently no authorisation at this position.</p>



Locking devices & keys


















Icon	Description
	<p>Locking device: Locking device</p> <p>This component is either a locking device or a locking cylinder.</p> <p><i>An additional radio symbol in the lower left corner indicates that an online extension is available.</i></p>
	<p>Locking device: SmartRelay</p> <p>This component is a SmartRelay.</p> <p><i>An additional radio symbol in the lower left corner indicates that an online extension is available.</i></p>
	<p>Key: Transponder</p> <p>This component is a transponder.</p>
	<p>Key: PIN code keypad</p> <p>This component is a PIN code keypad.</p> <p><i>An additional radio symbol in the lower left corner indicates that an online extension is available.</i></p>

Search function

Call of further functions

You can also call up other functions from the matrix view.

Icon	Description
	<p>Search</p> <p>Click on the Search to call up a search function. It finds:</p> <ul style="list-style-type: none">■ Locks (lock cylinder or SmartRelay, see <i>Creating a lock</i> [▶ 17])■ Key (transponder, see <i>Add key</i> [▶ 18])■ Key4Friends (see <i>Key4Friends</i> [▶ 47]) <p>You can then access and edit the entries found.</p>
	<p>Events</p> <p>You can set whether you want to be notified of certain events. If a notification exists for you, this is displayed here (see <i>Event management</i> [▶ 54]).</p>

Icon	Description
	<p>Menu</p> <p>You can access all MobileKey functions here (see <i>Basic functions</i> [▶ 17] and <i>MobileKey online upgrade</i> [▶ 35]):</p> <ul style="list-style-type: none">  Matrix  Components  Network  Manage Key4Friends  Settings  Programming  Change theme  View Help  Manage account  Log off <p>Using a quick launch bar on the right side of the matrix view, you can also access the following functions without a menu to save time:</p> <ul style="list-style-type: none">  Matrix  Components  Network  Manage Key4Friends  Settings  Programming

6. Basic functions

A setup wizard will appear the first time that you log on to a MobileKey account, making it easy to configure. This wizard will help you to add locking devices and keys quickly and conveniently.

6.1 Creating a lock

The screenshot shows the 'CREATE LOCK' screen in the MobileKey app. The screen is dark-themed and contains the following elements:

- TYPE:** CYLINDER (with a lock icon and navigation arrows).
- Name *:** An input field for naming the lock.
- MODE:** Two radio button options: 'Opening duration in seconds' (selected) and 'Permanently open'.
- Opening duration in seconds:** A slider control with the value '5'.
- ONLINE EXTENSION:** A toggle switch set to 'OFF'.
- Bottom buttons:** 'Create another', 'Save', and 'Cancel'.

✓ Matrix screen open

1. Click on the Add lock icon (beneath the **SAVE** button).
2. Select the lock type, e.g. "CYLINDER" for a normal locking cylinder.
3. Assign a name, e.g. front door.
4. Select one of the options: Opening duration in seconds or Per-
manently open.
 - ↳ If you have selected Permantently open the lock will remain engaged ready for use until it is actuated again with a key or by remote opening.



CAUTION

Security risk with permanent opening

A door which is permanently open may pose a security risk. SimonsVoss Technologies GmbH therefore recommends limiting the opening time interval.

5. If you want to create another lock, select the checkbox Create another.
 - ↳ With this checkbox you stay in this view after saving and can immediately create another lock.
6. Click on the button **SAVE**.
 - ↳ The lock is created.



NOTE

Extended network settings are shown first if at least one SmartBridge has been added and configured. Further online options, such as the interval for "Door left open", are visible once the DM locking devices have been programmed for the first time.

In the case of **SmartRelay 2**, it is possible **to invert the output (relay contact)**, but you need to add and programme a SmartRelay first. The "OUTPUT CONFIGURATION" setting will then be visible with the "Invert output" option in the SmartRelay properties. If you activate this option, the SmartRelay needs to be reprogrammed.

6.2 Add key


CREATE KEY

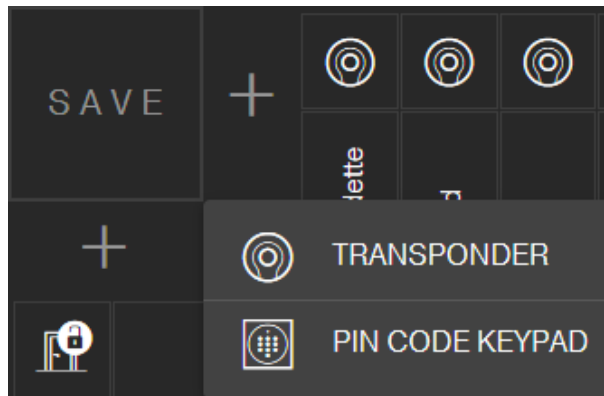
TYPE
TRANSPONDER

Name *

VALIDITY ▾

Create another **Save** **Cancel**

- ✓ Matrix screen open
- 1. Click on the Add Key icon  (next to the **SAVE** button).
 - ↳ The context menu opens.



- 2. Select the key type **TRANSPONDER**.
- 3. Assign a name, e.g. "John Smith".
- 4. Specify the validity if necessary.
 - ↳ "Valid from": From this date, the key is authorised in the locking system.
 - ↳ "Valid to": From this date, the key is no longer authorised in the locking system.
- 5. If you want to create another key (transponder), select the checkbox Create another.
- 6. Click on the button **SAVE**.
 - ↳ The key is added.



NOTE

Assignment of keys (transponders) with component list

Many successively programmed transponders are difficult to assign. You do not need to mark these transponders. A unique ID is engraved on each transponder. This ID is assigned to the name you specify. You can see this assignment in the component list (see [Exporting the component list](#) [[▶ 28](#)]).

6.3 Add PIN code keypad

This chapter describes how to set up a PIN code keypad without online upgrade. If you have a PIN code keypad with online upgrade, please proceed as described in chapter [Adding a PIN code keypad with online upgrade](#) [[▶ 42](#)].

- ✓ PIN code keypad already configured; see supplied quick guide (*master pin and at least one user pin must be configured!*)
 - ✓ Lock created for PIN code keypad (see [Creating a lock \[▶ 17\]](#) or [Creating a lock with online upgrade \[▶ 40\]](#))
 - ✓ Matrix screen open
1. Click on the Add Key icon (next to the **SAVE** button).
 2. Select the type **PIN CODE KEYPAD**.
 3. Specify the lock on which the PinCode keypad is operated.
 4. Assign a name for PIN 1 (*corresponds to user PIN 1*), e.g. "Hans Müller". The white checkbox for PIN 1 is already active.
 5. If you want to use a second and third PIN, select the checkboxes. Then proceed in the same way as for PIN 1.
 6. If you want to create another PinCode Keypad, select the checkbox **Create another**.
 - ↳ With this checkbox you remain in this view after saving and can immediately create another PIN code keypad.

7. Click on the button **SAVE**.
↳ The PIN code keypad is created.




**NOTE**

Up to 3 user PINs can be configured directly on the PIN code keypad. These user PINs must be activated in the web app when the PIN code keypad is assigned to a locking device.

Individual user PINs for an existing PIN code keypad can be changed by clicking on the corresponding button in the matrix and selecting **EDIT**.

6.4 Issue authorisation and save

Authorisations can be issued or withdrawn on the matrix screen.

- Authorising key at locking device: Click on the empty field at the intersection point between the key and locking device to add a cross. The cross is displayed reduced in size until the new authorisation has been programmed: . Once programming is successfully complete, the cross fills the entire matrix square: .
- Revoking a key's authorisation for a locking device: Click on the empty field at the intersection point between the key and locking device to remove the authorisation cross. The cross is not shown completely until the new change has been programmed: . The authorisation cross will not disappear completely until programming is successfully complete.

**NOTE**

Changes are shown with yellow borders and are not yet saved. These changes are not saved during programming.

- Accept the changes before programming by clicking the button **SAVE**.

All component changes and authorisations must be programmed (see *Programming components* [▶ 25]) before they actually come into effect.

6.5 Assign time plan

This additional function is optional, so you don't necessarily need to use it.

There are basically two types of time plans:

- Weekly: Individual time intervals can be assigned to each day of the week.

EXAMPLE: The housekeeper only has access on certain days and at certain times – e.g. Mondays 8 a.m. to noon and Thursdays 1 p.m. to 3.30 p.m.

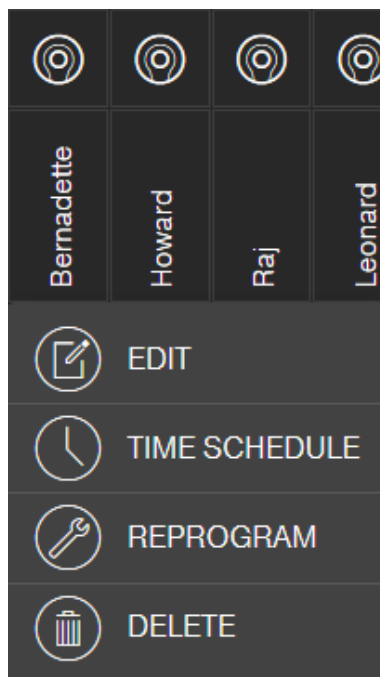
- Daily: A general time zone plan can be created for an entire week.

EXAMPLE: Employee John Dorian is authorised to activate locking devices between 7 a.m. and 7 p.m. from Mon to Fri.

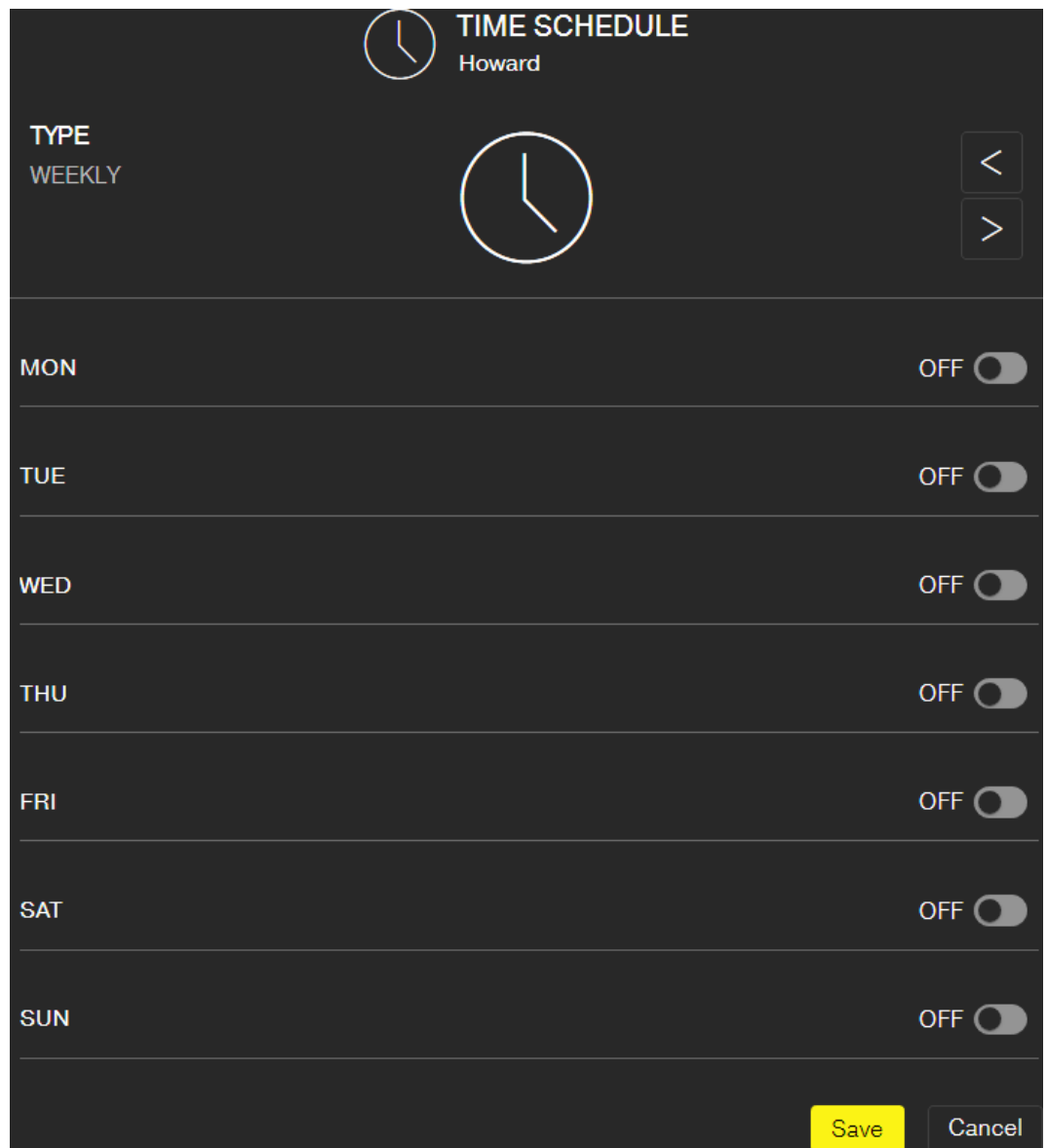
Proceed as follows to assign a time plan to a key:

- ✓ Matrix screen open

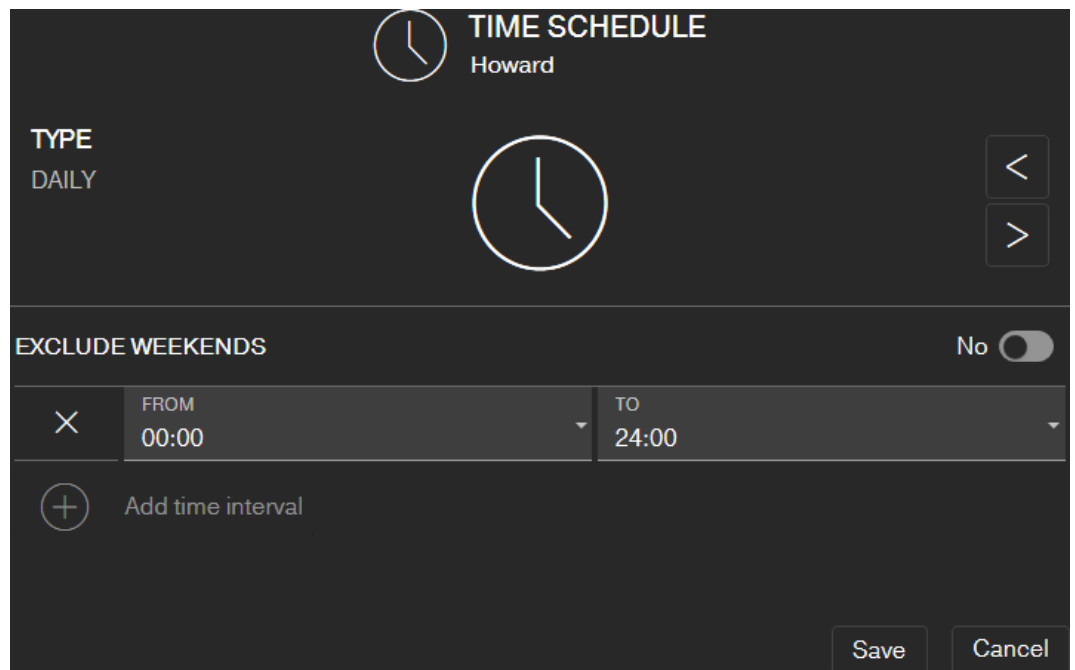
1. Click on the required key on the matrix screen.
 - ↳ The context menu opens.



2. Click on the button **TIME SCHEDULE**.
3. Select the time schedule type.
 - ↳ Weekly: Select day and "Create time interval". Several time intervals can be selected on different days.



- ↳ Daily: Click on "exclude weekends" if the schedule is to apply from Monday to Friday only. Then a "Create time interval". Several time intervals can be added.



TIME SCHEDULE
Howard

TYPE
DAILY

EXCLUDE WEEKENDS No

FROM 00:00 TO 24:00

+ Add time interval

Save Cancel

4. Click on the button **SAVE**.
 - ↳ Key is saved.
 - ↳ Matrix screen is displayed.
 - ↳ Key is assigned to the time schedule.



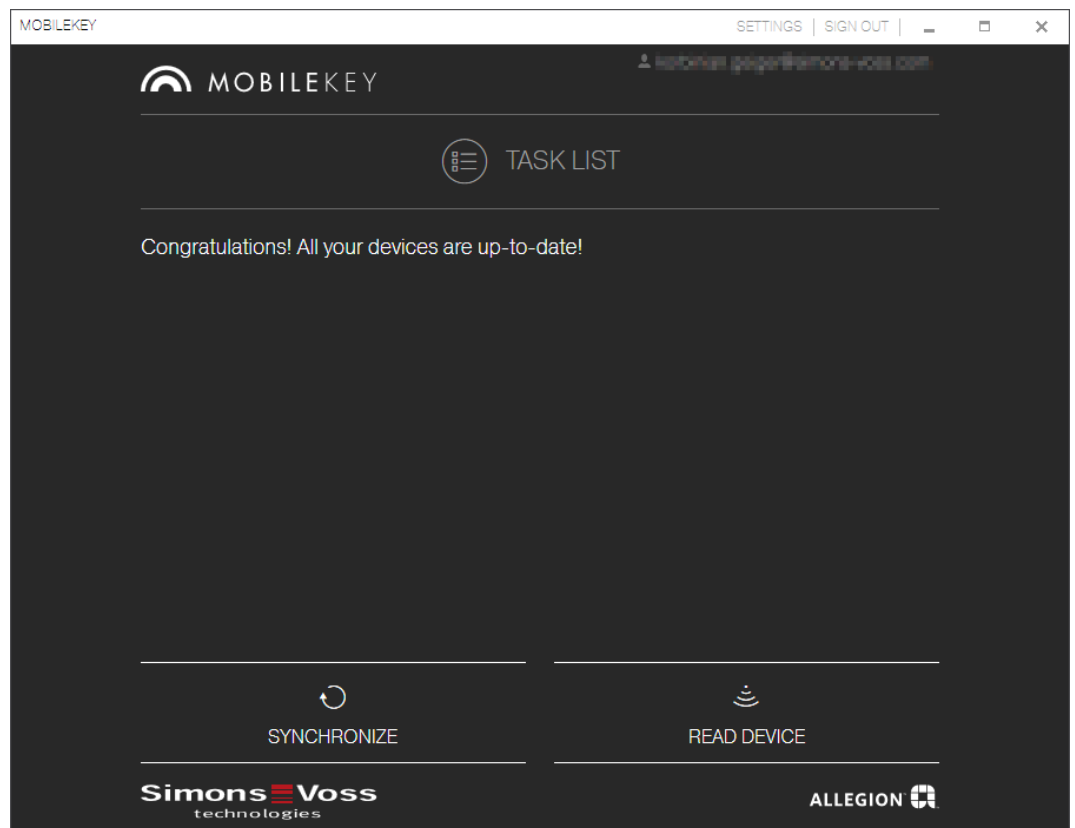
NOTE

Time intervals around midnight

If a time interval exceeds midnight, it cannot be programmed with a day. You must split such a time interval into two days:

1. Create a time interval from "time before midnight" to "midnight".
2. Create a second time interval from "Midnight" to "Time after midnight".

6.6 Programming components



NOTE



Programme each lock or Online PIN Code Keypad before installing it.

Proceed as follows to launch the programming app from the MobileKey web app and thus complete the individual programming tasks:

- ✓ Programming tasks pending (shown on respective components in matrix)
- 1. Click on the menu button .
 - ↳ Menu opens.
- 2. Click on the button PROGRAMMING .
 - ↳ The programming app launches.
- 3. Log on if required.
 - ↳ Task list shows components requiring programming.
- 4. Execute all pending tasks.
- 5. Click on the first component to start programming it.
- 6. Then follow the instructions in the programming app.

6.6.1 IMPORTANT: Programming on a Windows device

You must download and install the programming app once. Then log in. The USB config device must be connected to the computer's USB port to programme.

The installation is indicated as soon as you click on the menu  and  PROGRAMMING . The download of the installation file starts after clicking on Install / Repair . Install the programming app (administrator rights required).

Take hardware requirements into account: [Programming \[▶ 6\]](#)

6.6.2 IMPORTANT: Programming on an Android device

Download the free MobileKey app from the [Google Play Store](#) and connect the programming stick to the Android device. You may need a separately available USB-On-The-Go cable (OTG):



Launch the app one time to enter your user name and password.

Take hardware requirements into account: [Programming \[▶ 6\]](#)


6.6.3 IMPORTANT: Programming on a macOS device

You need to install a service one time for programming in macOS. A prompt will appear if the service has not yet been installed or has not been launched. You must not quit the browser when the service is running. Devices with an activated online extension do not need to be programmed. There are two options for programming keys and locks without an online extension in macOS.

Take hardware requirements into account: [Programming \[▶ 6\]](#)



Programming in the menu

The first option is to programme using the context menu. This method is suitable if few keys or locks have been changed.

1. Click on the components which need to be programmed.
 - ↳ Menu opens.
2. Click on the button  PROGRAMMING .
 - ↳ Programming window opens.
3. Follow the instructions on the screen.
 - ↳ Programming is complete.


Programming with programming list

The second option is to programme using the programming list. This method is suitable if many keys or locks have been changed in the matrix.

- ✓ Matrix screen open
- 1. Click on the menu button 
 - ↳ Menu opens.
- 2. Click on the button  PROGRAMMING.
 - ↳ Programming list opens.
- 3. Click on a component in the list which needs to be programmed.
- 4. Follow the instructions on the screen.
 - ↳ Component is programmed.
- 5. Click on the next component in the list to programme it.
 - ↳ Programming is complete.

6.7 Resetting components

Components can be easily reset. After a reset, they are in storage mode and can be used in another system.

- 1. Click on the component you require.
 - ↳ Menu opens.
- 2. Click the **DELETE** button.
- 3. Click on the button  PROGRAMMING.
 - ↳ The programming app launches.
- 4. Complete all tasks.
 - ↳ Component has been deleted from locking plan after successful programming.

6.8 Forced component deletion

If a defective component cannot be reset without any difficulty (see *Resetting components* [▶ 27]), it is possible to delete it from the locking plan. A repeated deletion of the component leads to a forced deletion of the component.

- ✓ Component already deleted.
- ✓ Component programmed previously.
- 1. Click on the component again.
- 2. Click the button **FORCE DELETE** and confirm the input.



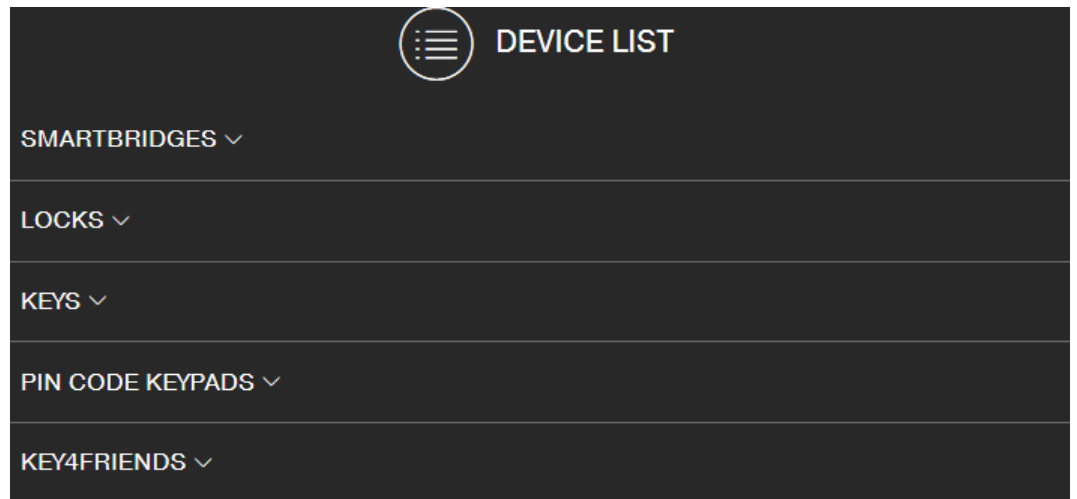
NOTE

Forced deletion disables a (still) programmed component, so it can no longer be used. You should only use this procedure on defective components!

- You can reset the components using the programming app (see *Reset or re-use deleted components* [▶ 63]).

6.9 Exporting the component list

You can see what is available in your MobileKey locking plan via the  menu  Devices :



You can see the components by opening the drop-down menus:

- ▼ SMARTBRIDGES
- ▼ LOCKS
- ▼ KEYS
- ▼ PIN CODE KEYPADS
- ▼ KEY4FRIENDS

Use the  **Generate PDF** button to create a PDF with detailed information:




Location and account

Information	Meaning
Location	Location of the components (Here the location specification in the settings is used, see <i>Settings</i> [▶ 58]).

Information	Meaning
Account	Account to which the components belong.

SMARTBRIDGES




SMARTBRIDGES

Office Type: Standart		Firmware: -- MobileKeyID: 0255803366670747	Status: IN USE Code: MK.SMARTBRIDGE.ER
Garage Type: Standart		Firmware: -- MobileKeyID: 3981205053636715	Status: IN USE Code: MK.SMARTBRIDGE.ER
Apartment Type: Standart		Firmware: -- MobileKeyID: 2906415534063641	Status: IN USE Code: MK.SMARTBRIDGE.ER

Information	Meaning
Type	Standard entry without any further meaning.
Firmware	Firmware version of SmartBridge.
MobileKeyID	MobileKey ID of SmartBridge.
Status	Possible statuses:

LOCKS

LIST OF LOCKS







Safe Type: Cylinder		Firmware: 3.5.37 ChipID: 000259CD	Status: IN USE Code: MK.Z4.30-35.DM.FD.FH.ZK.G2
Office Type: Cylinder		Firmware: 2.4.00 ChipID: 00023890	Status: IN USE Code: MK.Z4.30-30.FD.FH.LN.ZK.G2
Entrance Type: Cylinder		Firmware: 3.0.38 ChipID: 00031400	Status: IN USE Code: MK.Z4.30-35.DM.FD.FH.ZK.G2

Information	Meaning
Type	Indicates whether the device is a cylinder or a SmartRelay.
Firmware	Firmware of the lock used. If the lock is not programmed, then -- is displayed.
ChipID	Chip ID of the network node used (LockNode). If the lock is not programmed, then -- is displayed.

Information	Meaning
Status	Possible statuses:
Code	<p>Article number of the cylinder. You can re-order the same cylinder with this article number. In the event of technical problems, you can send this article number to support for identification.</p> <p>If the lock is not programmed, then -- is displayed.</p>

KEYS


LIST OF KEYS

Bernadette Type: Transponder		Firmware: 3.2.19 Serial number: 2U43M2	Status: IN USE Code: MK.TRA2.G2
Howard Type: Transponder		Firmware: 3.2.17 Serial number: 1UHL3L	Status: IN USE Code: MK.TRA2.G2
Raj Type: Transponder		Firmware: 3.2.19 Serial number: 2U03MM	Status: IN USE Code: MK.TRA2.G2
Leonard Type: Transponder		Firmware: 3.2.19 Serial number: 2U4P7M	Status: IN USE Code: MK.TRA2.G2
Penny Type: Transponder		Firmware: 3.2.19 Serial number: 0XK3C4	Status: IN USE Code: MK.TRA2.G2
Sheldon Type: Transponder		Firmware: 2.3.5 Serial number: 06137T	Status: IN USE Code: MK.TRA2.G2

Information	Meaning
Type	Standard entry without any further meaning.
Firmware	Firmware of the transponder.
Serial number	Transponder serial number. You will also find this serial number engraved on the back of the transponder. Use this serial number to clearly assign physical transponders to the transponders in the locking plan.
Status	Possible statuses:
Code	Article number of the transponder. In the event of technical problems, you can send this article number to support for identification.

PIN CODE KEYPADS

PIN CODE KEYPADS

PinCode Office		Firmware: --	Status: NEW
Type: PIN Keypad		ChipID: 00040CA2	Code: MK.PINCODE.ONLINE

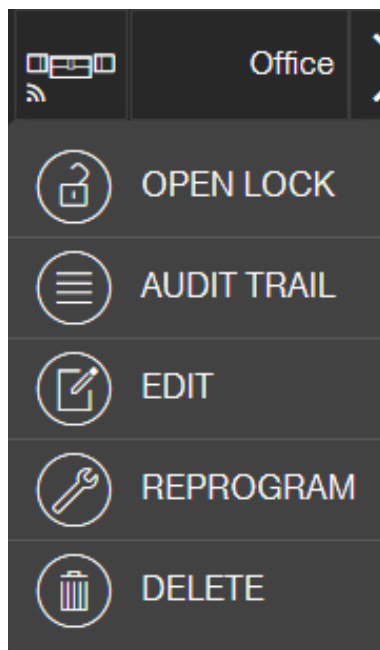
Information	Meaning
Type	Standard entry without any further meaning.
Firmware	Firmware of the PIN code keypad used. If the PIN code keypad is not programmed, then -- is displayed.
ChipID	Chip ID of the network node used (LockNode). If no LockNode is present, then -- is displayed.
Status	Possible statuses:
Code	Article number of the PIN code keypad. You can reorder the same PIN code keypad with this article number. In the event of technical problems, you can send this article number to support for identification.

Alternatively, you can also read out the components (see [Read components \[▶ 63\]](#)).

6.10 Read access event log

All access events with a key are logged in the locking device. MobileKey locks log up to 500 accesses. If further accesses take place afterwards, the oldest accesses are overwritten. Proceed as follows to display the access protocol:

- ✓ Matrix screen open
- 1. Click on the required ready programmed lock to read its log.
 - ↳ Menu opens.





2. Click on the button **AUDIT TRAIL**.
3. Click on the button **READ AUDIT TRAIL**.

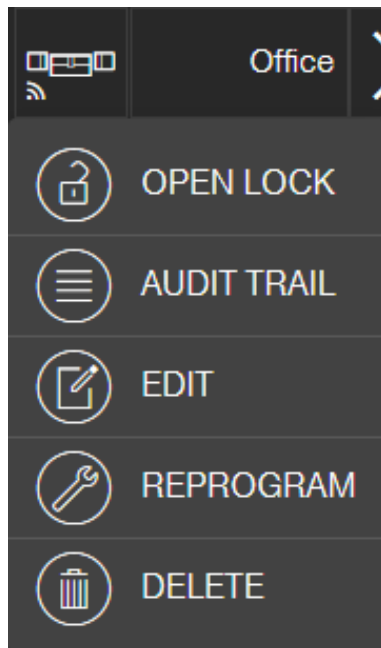


NOTE

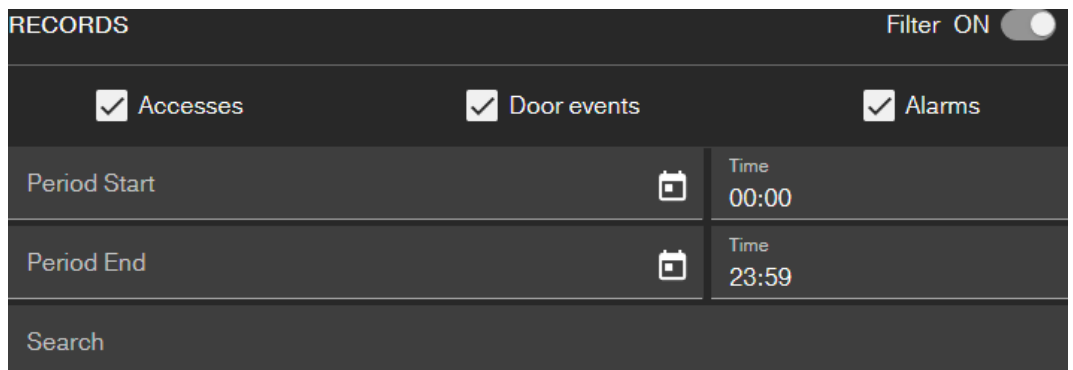
Reading out locks with online upgrade

Locks with online upgrade are automatically read out via the SmartBridge. You do not need to read these locks with the programming app and the USB config device.

- ↳ The "Read access log" command is sent to the programming app as a task.
4. Click on the menu button .
- ↳ Menu opens.
5. Click on the button  **PROGRAMMING**.
- ↳ The programming app launches.
6. Execute the programming task.
7. Open the matrix.
8. Click on the required lock to read its log.
- ↳ Menu opens.



9. Click on the button **AUDIT TRAIL**.
 - ↳ Access event log is displayed.
10. If necessary, filter the entries.

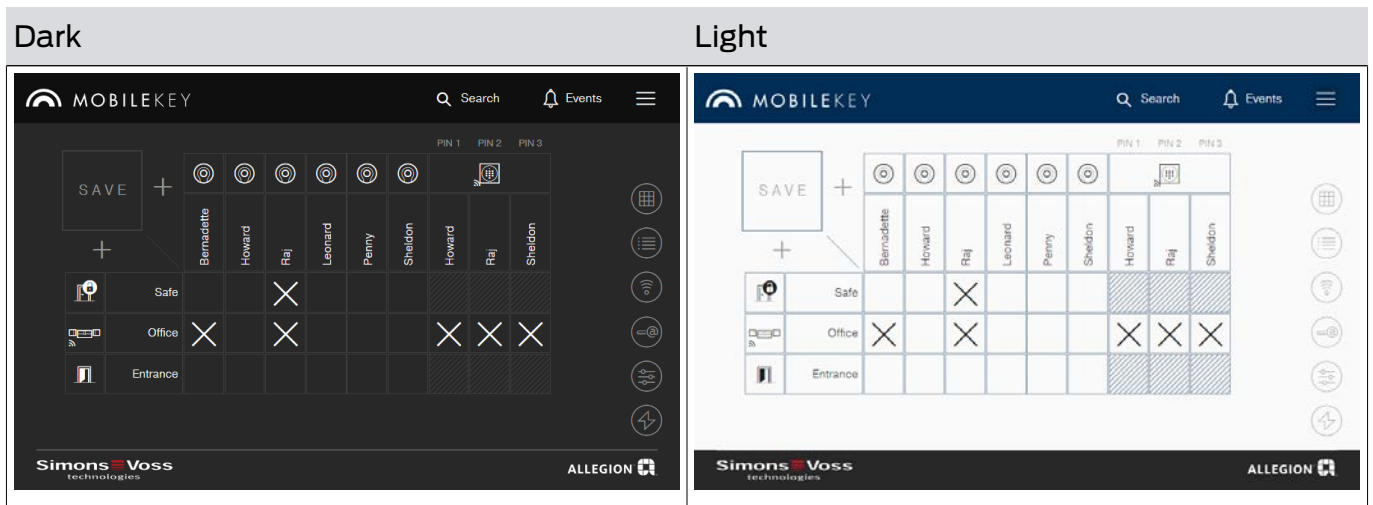


- ↳ Filtered access log is displayed.



6.11 Changing the colour scheme

Two colour schemes are available:

Dark	Light
Light font and symbols on dark grey background (default after login or page refresh)	Dark font and symbols on white background



You can switch between the themes according to your personal preference:

1. Click on the menu button .
 - ↳ Menu opens.
2. Click on the button  **Change theme** .
 - ↳ The theme is changed.

7. MobileKey online upgrade

You can network locks and PinCode keypads with online upgrade via a SmartBridge (which serves as an access point) to communicate directly with the Web App. You benefit from the following advantages:

- Program locks and PinCode keypads with online upgrade platform-independent.
- Track door statuses (open, closed, locked) in real time.
- Read lock access lists from anywhere in the world.
- Share your keys with friends with Key4Friends.
- Open and close your locks remotely.

Components for online upgrade

Special components are required to use these functions:

- SmartBridge: as an access point, SmartBridge is permanently connected to the Internet.
- Lock with online upgrade All MobileKey locking devices can be equipped with a special network node (*SmartRelay with suitable circuit board*) to retrofit online functions. This where we refer to what are known as LockNodes.

Locking devices with a "DoorMonitoring configuration" also feature sophisticated sensor technology. These locking devices can determine door statuses (open, closed, locked) and inform the web app.

- PIN code keypad with online upgrade: This PIN code keyboard is connected to the SmartBridge via a network node (LockNode).

Note on network dependency and offline fallback level

MobileKey is a web-based solution for managing a locking plan with locks and keys, which works independently after programming (offline).

The described online extension depends on a permanent and reliable internet connection to our server. It offers the following functions, for example:

- Remote opening
- Key4Friends
- Online PinCode-keypad
- Immediate sending of notifications

Remote openings enable persons without their own physical identification medium to gain direct access to networked locks. In contrast, Key4Friends temporarily authorise persons without their own physical identification medium to gain independent access. Such persons are for example:

- Friends (as the name suggests)
- Service provider
- Neighbours
- Suppliers



NOTE

Offline fallback level for networked locks

All functions of the online extension (including Key4Friends) are designed only as an extension and not as a replacement for the offline functions. They are not a replacement for persons with permanent authorizations or as exclusive access authorization at security-critical doors and access points.

- Therefore, when extending our standard system online (offline), especially when using it with Key4Friends or remote opening, always provide one or more offline backups (PinCode keypad (offline), transponder).
- ↳ These physical identification media communicate directly with the locks. They ensure access to the corresponding doors and access points at all times and independently of the network.

7.1 SmartBridges

At least one SmartBridge must be operated as an access point. This connected to the Internet and thus guarantees connection to the server and web app.



NOTE

Extended network settings (*e.g. when a locking device is added*) are not shown until at least one SmartBridge has been added.

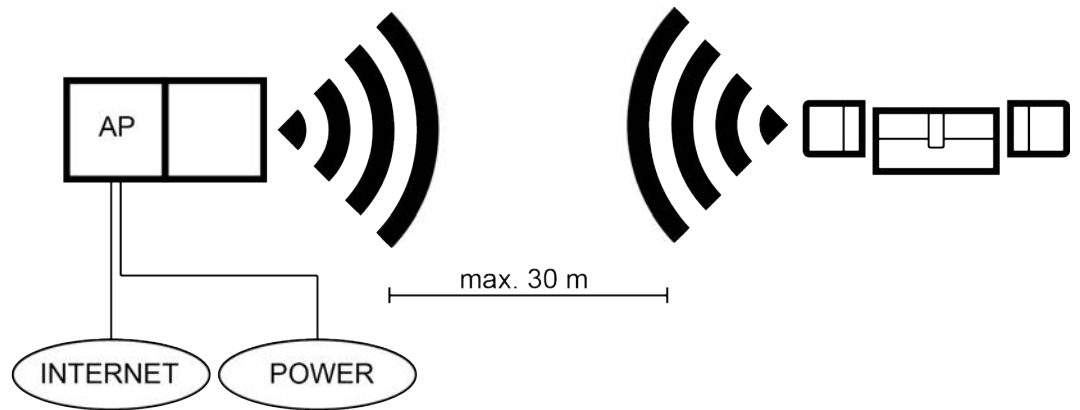
Note that a maximum of 10 SmartBridges can be used with MobileKey.

7.1.1 Setting up SmartBridges

SmartBridges can be operated in different ways depending on their use and configuration. The key scenarios are shown below.

7.1.1.1 A SmartBridge

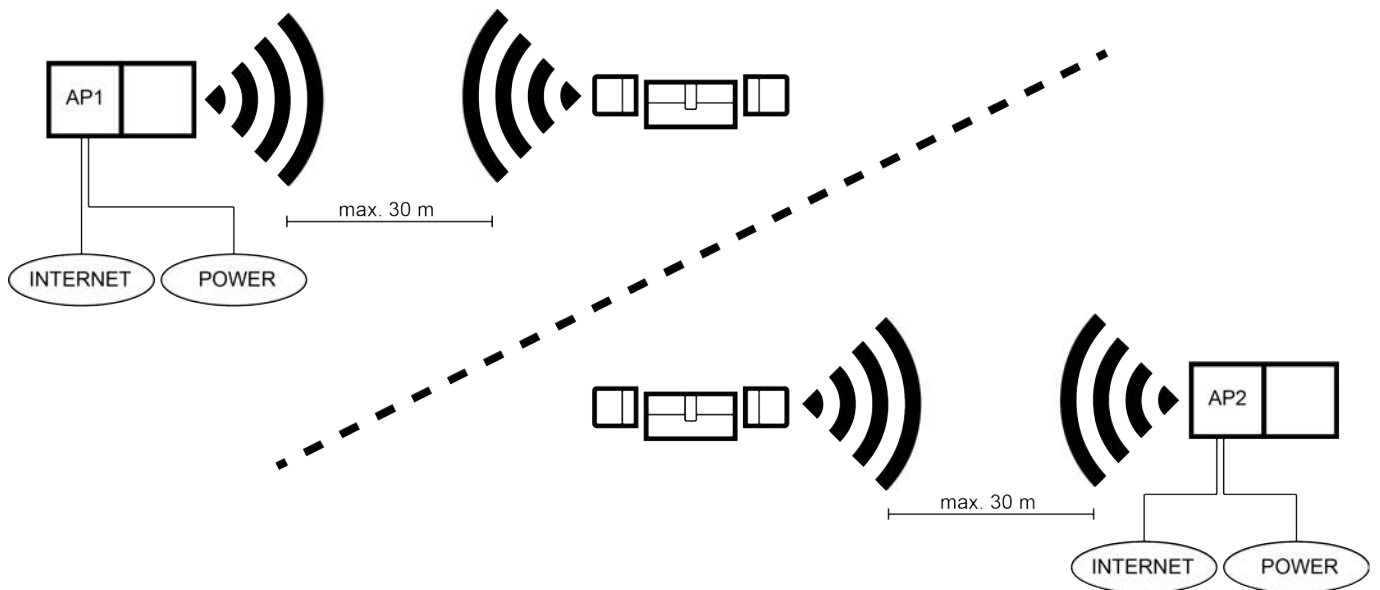
The simplest use for MobileKey ONLINE is as a SmartBridge configured as an access point.



7.1.1.2 Two or more SmartBridges

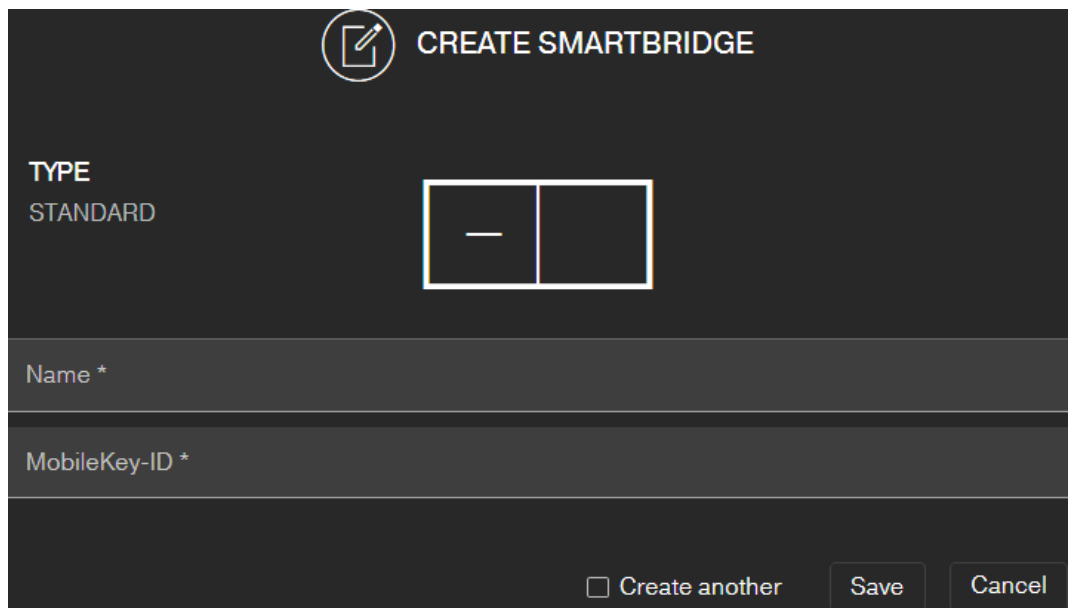
MobileKey ONLINE can manage a number of access points. This allows several locations or very distant locking devices to be covered with the MobileKey ONLINE network.

MobileKey ONLINE automatically determines which particular locking device is addressed by which particular access point based on the signal strength. You can trace the communication path in the "NETWORK" menu by activating the "Show Uplink" option.



7.1.2 Setting up SmartBridges

This how you add a new SmartBridge to the web app:






CREATE SMARTBRIDGE

TYPE
STANDARD

Name *

MobileKey-ID *

Create another Save Cancel

1. Click on the menu button .
↳ Menu opens.
2. Click on the button  NETWORK.
↳ The network view opens.
3. Add a new SmartBridge using the  button on SmartBridges.
↳ Dialogue for adding a new SmartBridge starts.
4. Assign a unique name (e.g. "SmartBridge Office 2").
5. Enter the MobileKey ID (see packaging or back of the SmartBridge, format XXXX-XXXX-XXXX-XXXX).
6. If you want to create another PIN code keypad, select the checkbox Create another.
↳ With this checkbox you remain in this view after saving and can immediately create another SmartBridge
7. Click on the button SAVE.
↳ SmartBridge is created.



NOTE

SmartBridge connection to server

Your SmartBridge connects to the server approximately every 15 seconds. If you start the network configuration immediately after setting up the SmartBridge, the server cannot yet identify the SmartBridge and the network configuration fails.

- After setting up the SmartBridge, wait about twenty seconds before starting the network configuration.

Changing the default password

Unauthorised access with standard access data

The standard access data can be viewed freely. Unauthorised persons cannot change the access authorisations, but they can change the network configuration. You will then no longer be able to reach the device via the network and will have to reset it.

Some browsers do not transmit spaces at the beginning of the password.

1. Change the default password.
2. Do not start or end the password with spaces.

Change the default password of your SmartBridge:

1. Use the OAM tool to determine the IP address of your SmartBridge.
2. Call up the web interface of your SmartBridge with a browser (user name: SimonsVoss, password: SimonsVoss).
3. Assign a new password.

For detailed information about the OAM tool and your SmartBridge, please refer to the OAM Tool Manual, the quick guide for your SmartBridge and the SmartBridge manual.




7.1.3 Deleting SmartBridge



NOTE

The LockNodes in locking devices can only be reset via the connected SmartBridge. If locking devices are not flagged for deletion, they will retain their configuration. However, the locking devices can now only be accessed via a new SmartBridge or the programming device.

This is how you delete your SmartBridge in the web app:

- ✓ Connected locks have status "ONLINE".
1. Click on the menu button .
 - ↳ Menu opens.
 2. Click on the button  NETWORK.
 3. Click on the SmartBridge to be deleted.
 4. Click the **DELETE** button.
 - ↳ The SmartBridge is flagged for deletion.
 5. Start the network configuration by clicking the  **START CONFIGURATION** button.
 6. The programming procedure (in this case, resetting the SmartBridge) is performed. The SmartBridge can then be re-integrated in any MobileKey locking system.

7.2 Creating a lock with online upgrade




NOTE

Locking devices which have already been installed and programmed without an online function can also be integrated into MobileKey ONLINE retroactively. To do so, you merely need to replace the thumb-turn cover (*inside thumb-turn cover on FD locking devices, outer thumb-turn cover on CO locking devices or added circuit board in SmartRelay*) with an online thumb-turn cover containing a LockNode. Information on the exchange can be found in the LockNode's quick guide. The new chipID for the LockNode can then be added to the locking device in the web app.

The screenshot shows the 'CREATE LOCK' interface in a dark theme. At the top, there is a pencil icon and the text 'CREATE LOCK'. Below this, the 'TYPE' is set to 'CYLINDER', accompanied by a diagram of a cylinder lock and left/right navigation arrows. A 'Name *' input field is present. The 'MODE' section includes a slider for 'Opening duration in seconds' set to 5, and a radio button for 'Permanently open'. The 'ONLINE EXTENSION' section has a toggle switch set to 'ON'. Below this is a 'Chip-ID *' input field. At the bottom, there is a checkbox for 'Fast communication' and three buttons: 'Create another', 'Save' (highlighted in yellow), and 'Cancel'.

This how you add a new online locking device:

- ✓ SmartBridge added (See *Setting up SmartBridges* [▶ 37]).
 - ✓ Matrix screen open
1. Click on the Add lock icon  (beneath the **SAVE** button).
 2. Select the lock type, e.g. "CYLINDER" for a normal locking cylinder.
 3. Assign a name, e.g. front door.

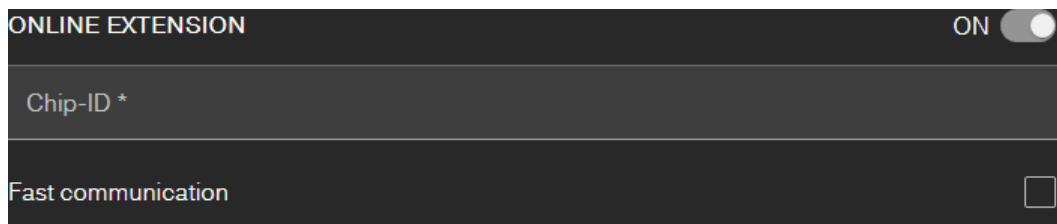


CAUTION

Security risk with permanent opening

A door which is permanently open may pose a security risk. SimonsVoss Technologies GmbH therefore recommends limiting the opening time interval.

4. Select one of the options: Opening duration in seconds or Permanently open.
 - ↳ If you have selected Permanently open the lock will remain engaged ready for use until it is actuated again with a key or by remote opening.
5. Activate the online upgrade.



6. Enter the Chip-ID (see packaging or inside of the thumb-turn, format XXXXXXXX).



NOTE



Low battery life

If you activate the Fast communication, the locking device checks more frequently whether an action should be performed. This reduces the response time, but it also shortens the battery life by up to 30%.


7. Optionally select the checkbox Fast communication.
8. If you want to add another lock with online upgrade, activate the checkbox Create another.
 - ↳ With this checkbox you stay in this view after saving and can immediately add another lock with online upgrade.
9. Click on the button **SAVE**.
 - ↳ Lock with online function (LockNode) added.

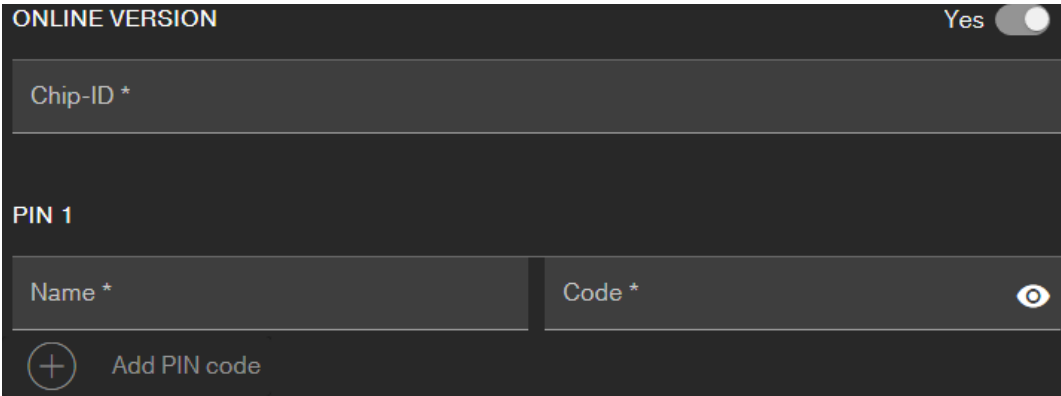
7.3 Deleting a lock with online upgrade

This is how you delete an existing online locking device via the SmartBridge:



- ✓ SmartBridge added (see [Setting up SmartBridges \[▶ 37\]](#))
 - ✓ Network set up and functioning
 - ✓ The online status of the lock that you wish to delete "ONLINE"
1. Click on the menu button 
 - ↳ Menu opens.
 2. Click on the button  NETWORK.
 3. Click on the lock you wish to delete in the "NETWORK" menu.
 4. Click the **DELETE** button.
 - ↳ The locking device is flagged for deletion.
 5. Use the "START CONFIGURATION" button to launch the network configuration.
 - ↳ Programming process is implemented (*in this case: reset*).
 - ↳ The lock can then be re-incorporated into the MobileKey locking system.
- ↳ Lock is deleted.

7.4 Adding a PIN code keypad with online upgrade

- ✓ Online PIN code keypad already configured (see supplied quick guide).
 - ✓ Lock for online PIN code keypad already added (see [Creating a lock with online upgrade \[▶ 40\]](#)).
 - ✓ Matrix screen open
1. Click on the Add Key icon  (next to the **SAVE** button).
 2. Enter a name for the PIN code keypad, e.g. "Office door".
 3. Open the dropdown menu ▼ **Lock**.
 4. Specify the lock on which the online PIN code keypad is operated.
 5. Activate the online upgrade.



6. Enter the chip ID (See packaging or back side, format: XXXXXXXX).

7. Enter a name for the first PIN, e.g. "Hans Müller".
8. Enter a PIN (you can see the PIN in plain text with the Visible button )
9. If necessary, create up to two further PINs ( Create PinCode keypad button).
10. If you want to create further PIN code keyboards with online upgrade, activate the Create another.
 - ↳ With this checkbox you stay in this view after saving and can immediately create another PIN code keypad with online upgrade.
11. Click on the button **SAVE**.
 - ↳ Online PIN code keypad is added.



NOTE




If you subsequently wish to edit the user PINs, click on the entry in the matrix and select the **EDIT** button from the menu.

IMPORTANT

Blocking after incorrect inputs



If a user PIN is entered incorrectly seven times, the SmartBridge continues to reset reception, but the system blocks processing of entered user PINs for three minutes. A relevant notification is displayed in the messages on the web app.

7.5 Deleting a PIN code keypad with online upgrade

- ✓ SmartBridge added (See *Setting up SmartBridges* [▶ 37]).
 - ✓ Network set up and functioning (see *Configure network* [▶ 44]).
 - ✓ The online status of the online PIN code keypad you wish to delete "ONLINE".
1. Click on the menu button 
 - ↳ Menu opens.
 2. Click on the button  **NETWORK**.
 3. In the NETWORK menu, click the online PIN code keypad you wish to delete.
 4. Click the **DELETE** button.
 - ↳ The online PIN code keypad is flagged for deletion.
 5. Start the network configuration by clicking the  **START CONFIGURATION** button.
 - ↳ Programming process is implemented (*in this case: reset*).

- ↳ The online PIN code keypad can then be re-integrated into any MobileKey locking system after it has been reset to the delivery status (see supplied quick guide).
- ↳ Online PIN code keypad is deleted.

7.6 Configure network

- ✓ At least one SmartBridge has been added.
 - ✓ SmartBridge connected to Internet and ready for operation.
 - ✓ At least one lock with online chip ID added.
 - ✓ The distance between SmartBridge and locking devices is less than 30 m. *All components should be within the SmartBridge radio range at all times!*
1. Click on the menu button .
 - ↳ Menu opens.
 2. Click on the button  NETWORK.
 3. Click on the button **START CONFIGURATION**.
 - ↳ The MobileKey network is configured fully automatically.
- ↳ The status of SmartBridges and locking devices must be set to "ON-LINE" when configuration is complete.

Go through the following check list if the automatic configuration was not successful: [Lock with online upgrade does not work \[▶ 66\]](#).

7.7 Programming of components with online upgrade

Programming online locks or online PIN code keypad is also possible via SmartBridge. Keys or transponders must be programmed using the USB config device since they do not have a network node (LockNode).



NOTE

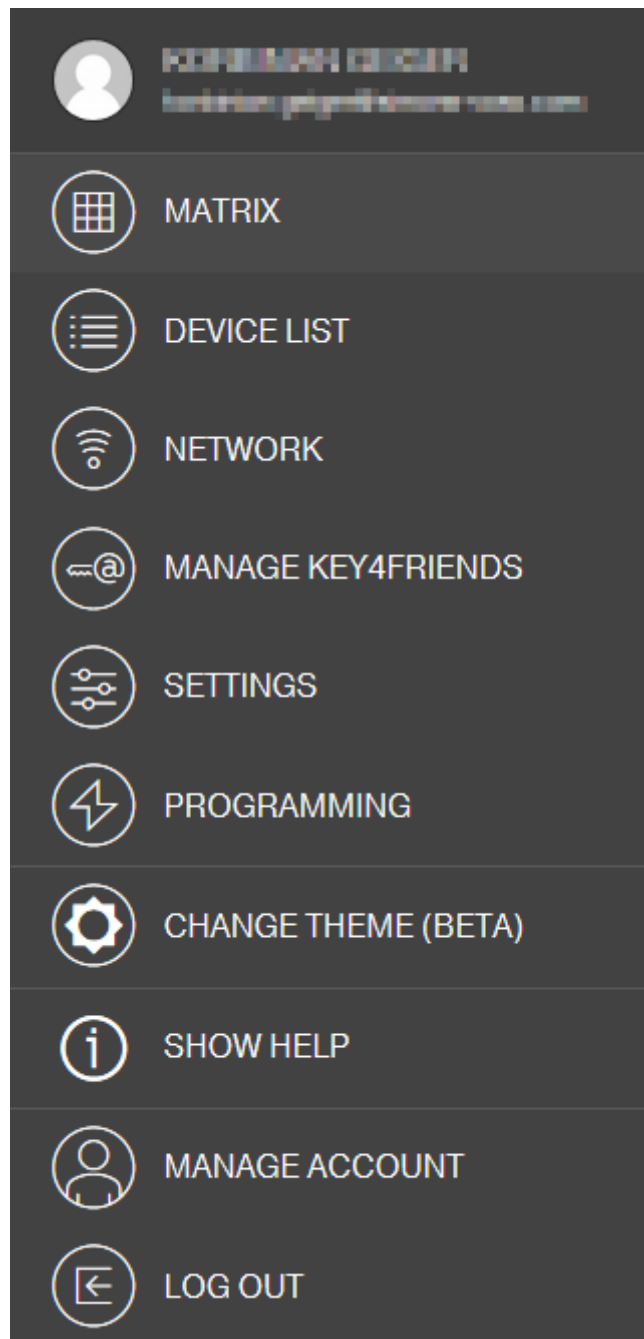
Programme each lock or Online PIN Code Keypad before installing it.

The access list stored in the locking device is reprogrammed every time that the device is reprogrammed. Only accesses already imported into the web app are conserved.

This how you complete programming using the SmartBridge:

- ✓ Chip ID of the lock or online PIN code keypad specified when creating the lock.
 - ✓ SmartBridge successfully configured (see [Configure network \[▶ 44\]](#)).
 - ✓ Matrix screen open
1. Add a component.

2. Assign authorisations if necessary (if you want to change authorisations).
3. Click on the menu button (☰).
 - ↳ Menu opens.
 - ↳ Programming process starts via SmartBridge.





4. Click on the button **NETWORK**.
 - ↳ Network overview opens.
5. Click on the button **START CONFIGURATION**.
 - ↳ Configuration with new component starts.

- ↳ Completion of the configuration is signalled by a fast tone that repeats itself three times (*beep-beep-beep*).
- ↳ The programming process which then starts automatically is displayed via the lower message bar.
- ↳ Programming completed.

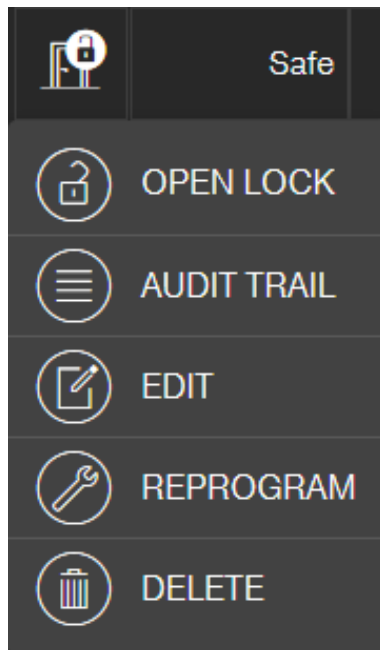
7.8 Disconnecting components with online upgrade


Online components can be removed from the system again if required. Warning messages are activated if components are physically removed – when they are taken outside the MobileKey radio range, for example. You should therefore always de-register the components concerned in the system. The de-registration process resets the LockNode. The lock or the online PIN code keypad retains the configuration and can then only be accessed via the USB config device until a new online setup is performed.

- ✓ At least one online lock or online PIN code keypad has been created.
 - ✓ At least one SmartBridge is created.
1. Click on the menu button .
 - ↳ The context menu opens.
 2. Click on the button  NETWORK.
 3. Click on the lock to be disconnected or on the Online PIN code keypad to be disconnected.
 - ↳ Menu opens.
 4. Click on the button EDIT.
 - ↳ The editing menu of the lock or the PIN code keypad opens.
 5. Deactivate the checkbox ONLINE VERSION.
 6. Click on the button SAVE.
 7. To start the online configuration with the button START CONFIGURATION.

7.9 Carrying out remote opening

- ✓ Locking system configured correctly.
 - ✓ SmartBridge connected to the Internet.
 - ✓ Remotely opening lock with online extension.
 - ✓ Remote lock properly configured (see *Creating a lock with online upgrade* [▶ 40]).
 - ✓ Matrix screen open
1. Click on the locking device you wish to open remotely.
 - ↳ Context menu opens.



2. Click on the button  OPEN LOCK .
 - ↳ The command is sent directly to the locking device via the SmartBridge. If you send this command to an open lock in permanent open mode, the lock will be closed.
 - ↳ Lock is opened/closed.

7.10 Key4Friends

Key4Friends allows users to share keys using smartphones. Keys can be shared with friends very easily using Key4Friends.

Your friend receives an email informing them that you wish to share a key with them. The email describes exactly how this shared key can be used with the help of the Key4Friends app.

Your friend installs the Key4Friends app and uses their email address and telephone number to register quickly and easily. This unique combination is the only way to ensure that your key can only be used by your friend's telephone.

**NOTE****Offline fallback level for networked locks**

All functions of the online extension (including Key4Friends) are designed only as an extension and not as a replacement for the offline functions. They are not a replacement for persons with permanent authorizations or as exclusive access authorization at security-critical doors and access points.

- Therefore, when extending our standard system online (offline), especially when using it with Key4Friends or remote opening, always provide one or more offline backups (PinCode keypad (offline), transponder).
- ↳ These physical identification media communicate directly with the locks. They ensure access to the corresponding doors and access points at all times and independently of the network.

7.10.1 Sharing keys

CREATE KEY4FRIENDS

TYPE
KEY4FRIENDS

Name *




E-MAIL SETTINGS

Email *

Language
English



VALIDITY ▾

LOCKS

	Safe	<input type="checkbox"/>
	Office	<input type="checkbox"/>
	Entrance	<input type="checkbox"/>

Create another **Save** **Cancel**

The e-mail contains the name specified in the settings (see [Settings](#) [▶ 58]).

- ✓ The locking system is configured correctly.
 - ✓ Matrix screen open
1. Click on the menu button .
 - ↳ Menu opens.
 2. Click on the button **MANAGE KEY4FRIENDS** .
 - ↳ Component overview opens.
 3. Click on the button  **NEW KEY4FRIENDS** .
 4. Enter the name and e-mail address of the recipient.

5. Select the language of the e-mail (Danish, Dutch, English, French, German, Italian or Swedish) from the ▼ **Language** .
6. If necessary, restrict the validity of the key.
7. Select all locks where the key is to be valid.

**NOTE****Key4Friends only with online upgrade**

The Key4Friends app sends a remote opening command via the Smart-Bridge (cf. *Carrying out remote opening* [▶ 46]) and works only with online upgrade. Therefore you can only mark locks with online upgrade here.

8. Optionally select the checkbox **Create another**.
 - ↳ With this checkbox you stay in this view after saving and can immediately add another lock with online upgrade.
9. Click on the button **SAVE**.
 - ↳ Your friend will then receive an email. The email describes exactly how they can use the key.

*All settings and details for shared keys can be changed or revoked at any time; see *Managing keys* [▶ 50].*


**NOTE**

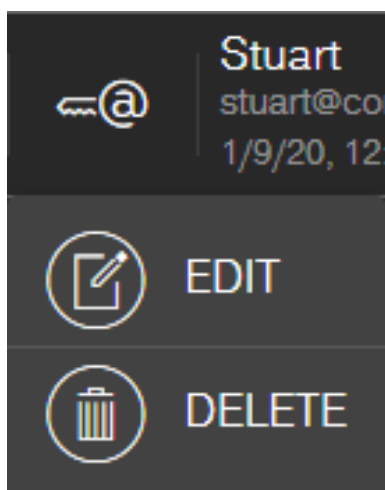
The time window for shared keys is limited to six months.

- If you want to give friends permanent access, use transponders or a PIN code keypad.

7.10.2 Managing keys

You can click on each shared key to edit or revoke it.

- ✓ Locking system configured correctly.
 - ✓ Matrix screen open
1. Click on the menu button 
 - ↳ Menu opens.
 2. Click on the button **MANAGE KEY4FRIENDS**.
 - ↳ Component overview opens. In the section KEY4FRIENDS you see all Key4Friends.
 3. Click on the Key4Friend you want to edit or delete.
 - ↳ Context menu opens.




4.  EDIT or  DELETE Sie den Key4Friend.



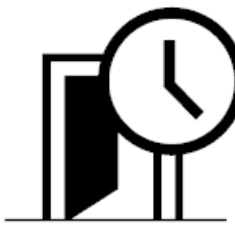
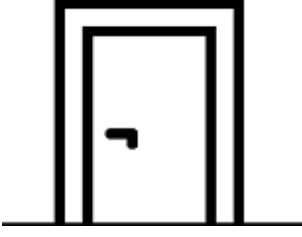
EDIT	DELETE
<p>With this you edit the properties of the Key4Friend:</p> <ul style="list-style-type: none"> ■ Name ■ Validity ■ Locks that are valid for the Key4Friend 	<p>This will delete the Key4Friend. No more locks can be opened with this Key4Friend.</p>

7.11 DoorMonitoring locking device - displayed locking statuses

Locking devices with a DoorMonitoring option use a special fastening screw to communicate door statuses. These locking devices are ready designed for use with MobileKey ONLINE as they already feature what is known as a LockNode.

The following door states of the DoorMonitoring lock are displayed (partly combined) via a corresponding icon in the matrix of the web app:

Icon	Description
	<p>Door open.</p>

Icon	Description
	<p>Door closed but not locked.</p>
	<p>Door securely closed and locking device locked.</p>
	<p>Door open too long.</p> <p>Set the time after initial programming (see <i>Programming of components with online upgrade</i> [▶ 44]) in the lock settings (see <i>Creating a lock with online upgrade</i> [▶ 40]):</p> <ul style="list-style-type: none"> ■ Never ■ 30 seconds ■ One minute ■ Two minutes ■ Five minutes
	<p>Door closed. Locking status not monitored.</p>

In addition, further warnings can be displayed for your DoorMonitoring lock.



NOTE

If there has been a break-in or deliberate manipulation of the DoorMonitoring locking device, the corresponding door must be checked immediately. Look for any damage to the door or locking device. The locking device must then be reset. See *Programming of components with online upgrade* [▶ 44]

**CAUTION****Dead bolt not monitored**

If the permanent opening mode is set, the status of the lock is not monitored!

- ❑ Do not use the permanently open mode if you also want to monitor the dead bolt.

The access list stored in the locking device is reprogrammed every time that the device is reprogrammed. Only accesses already imported into the web app are conserved.


Please note that your MobileKey network must be configured correctly. The SmartBridge and DoorMonitoring lock must both always be "ONLINE". *See [Lock with online upgrade does not work](#) [▶ 66] for further help.*

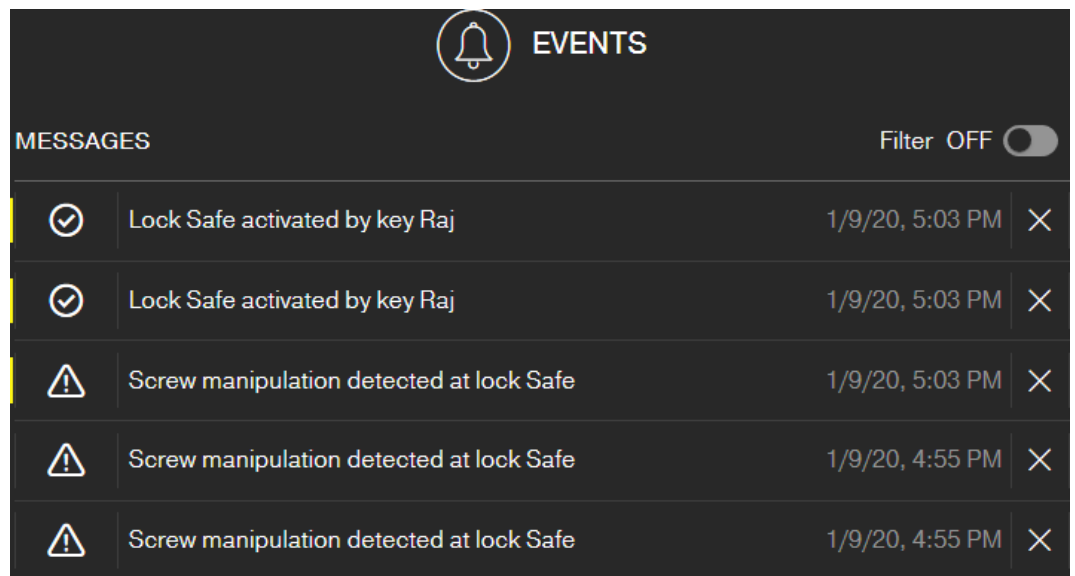
8. Event management

Use MobileKey event management to be notified of certain events that you have defined:

Event type	Meaning
Access	Select keys, locks and a period. If one of these keys is used at one of these locks within the period, you will receive a notification.
DoorMonitoring	Select DoorMonitoring events, locks and a time period. If one of these DoorMonitoring events (see <i>Door-Monitoring locking device - displayed locking statuses [▶ 51]</i>) occurs at one of these locks within the time period, you will receive a notification.
Alarm	Select which problems you want to be notified about: <ul style="list-style-type: none"> ■ Low battery ■ Network error ■ Break-in ■ Hardware problem

You will receive these notifications through various channels:

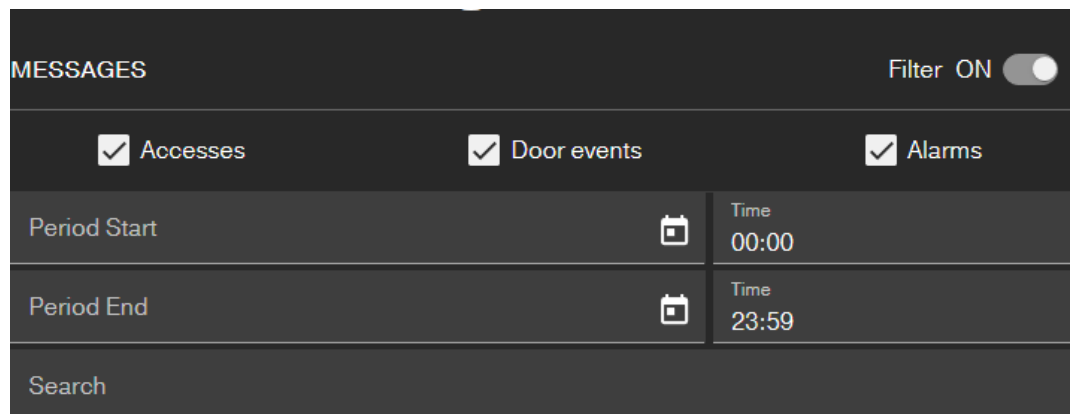
- E-mail transmission to several addresses
- Push notifications to your smartphone (only when MobileKey app is running)
- MobileKey web app (click on the button  Events)



This symbol also shows you if there are new events that you have not yet seen.




Filter

You can filter the events displayed. To do this, activate the filter and set it as needed.



8.1 Creating rules

Create individual events:

- ✓ Matrix screen open
1. Click on the button  Events .
↳ The event overview opens.
 2. Click on the button  Manage rules .
↳ Rule administration opens.
 3. Click on the button  Add event rule .

4. Follow the instructions of the wizard.

↳ The rule is created. You will receive a notification when the event you specified occurs.

Overview of the available event types

Access

Trigger	Description
Remote opening	A notification is sent for all remote opening events.
Key4Friends	A notification is forwarded for one opening event or all opening events actuated with Key4Friends.
Transponders/PINs	A notification is sent for one or all opening events actuated with a key (transponder) or PIN code.

DoorMonitoring

Trigger	Description
Door open	A notification is sent as soon as the door is physically opened.
Door closed	A notification is sent as soon as the door is physically closed.
Door open too long	A notification is sent as soon as the door is physically open for too long.
Door closed after being open too long	A notification is sent as soon as the door is closed again after being physically open for too long.
Door unlocked	A notification is sent as soon as the door is unlocked.
Door locked	A notification is sent as soon as the door is properly locked.

Alarm

Trigger	Description
Low battery	A notification is sent as soon as the battery level in a locking device is low.
Network error	A notification is sent as soon as a network error occurs.
Break-in	A notification is sent as soon as a DoorMonitoring locking device detects an attempted break-in.

Trigger	Description
Hardware error	A notification is sent as soon as a hardware error is detected.

8.2 Important information



NOTE

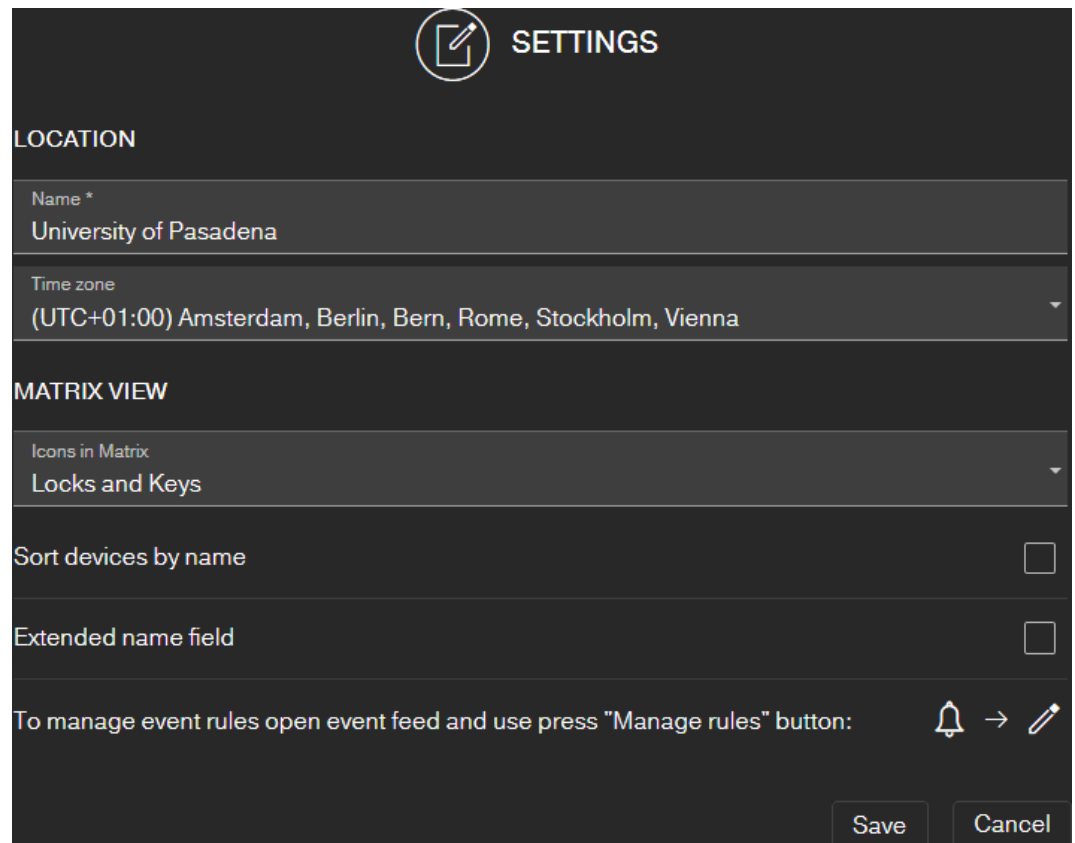
All events are transmitted via the SmartBridge. You will not receive any notifications about events if the Internet connection is malfunctioning or the power supply has been interrupted. All events which occur during the time period when the SmartBridge is not properly online.

An "ALARM" type notification is recommended in any case. This is how you can configure this event: *Creating rules* [[▶ 55](#)]

Notifications of events are reported in real time only if the locking devices have been networked with SmartBridge. Alarms are also recorded for non-networked locking devices when a programming task is carried out on the locking device concerned. All events and alarms can be displayed, filtered and reset under "EVENT FEED".

9. Settings

Call up the settings via the menu button  and the  **SETTINGS** button:



Location of the locking system

Enter the *name of the location* (e.g. Office) and the time zone of the location.

The location specification is also used in the exported component list (see [Exporting the component list \[▶ 28\]](#)).

Matrix view

Adjust the display of your matrix here:

setting	Effect
Icons in the matrix	Choose between the following display options: <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Locks and keys (standard) <input type="checkbox"/> Locks only <input type="checkbox"/> All hidden

setting	Effect
Sort devices by name	<p>If the <input checked="" type="checkbox"/> Sort devices by name checkbox is activated, the entries in the matrix are sorted alphabetically.</p> <p>If the <input type="checkbox"/> Sort devices by name checkbox is not selected, the entries in the matrix are displayed in the order in which they were created.</p>
Extended name field	<p>For a better overview, only 16 characters of component names are displayed in the matrix.</p> <p>If the <input checked="" type="checkbox"/> Extended name field checkbox is activated, then 22 characters of the component names are displayed in the matrix.</p>

10. Fault rectification

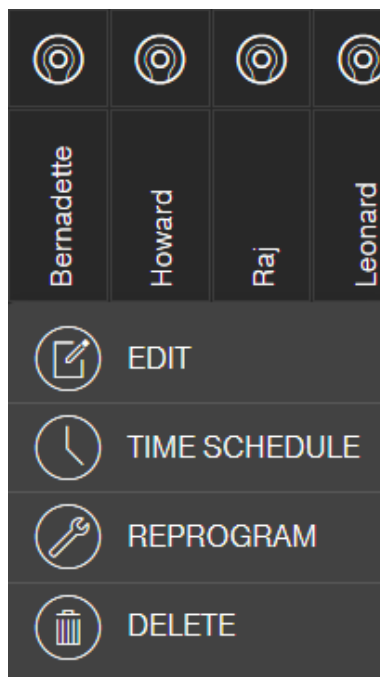
Help for possible day-to-day problems are shown below.


10.1 Key lost, damaged or stolen

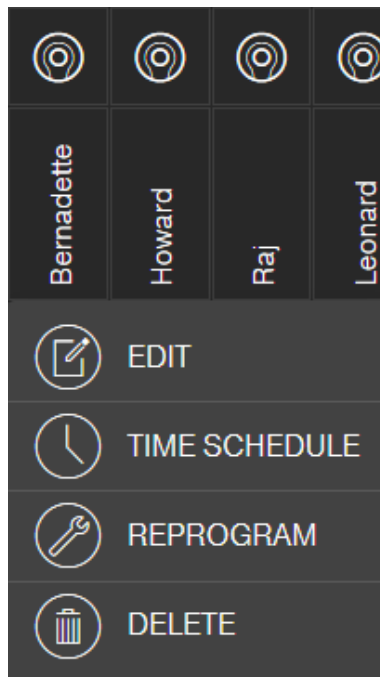
Keys or transponders may get lost, stolen or damaged at some point. Whatever the case, the old key needs to be deleted in the locking plan and a replacement key needs to be created. The deleted key's authorisations must be removed from all locking devices for security reasons. You can do this by programming all locks.

This is how you replace a key that no longer exists or is defective:

- ✓ Matrix screen open
- 1. Search for the key concerned in the locking plan.
- 2. Click on the key in the locking plan.
 - ↳ The context menu opens.



- 3. Click the  DELETE button.
 - ↳ Key is now flagged for reset.
 - ↳ Task will be completed in the programming app at a later stage.
- 4. Click on the key concerned in the locking plan.
 - ↳ The context menu opens.



5. Click on the "FORCE DELETE" button.
 - ↳ Key is deleted in the locking plan.
 - ↳ Key is not yet deactivated in the lock.
 6. If necessary, create a new key (see [Add key \[▶ 18\]](#)).
 7. Assign any necessary authorisations (see [Issue authorisation and save \[▶ 21\]](#)).
 8. Click on the button **SAVE**.
 - ↳ Changes are saved (locks with online extension are automatically programmed when a network connection is established).
 9. Click on the menu button .
 - ↳ Menu opens.
 10. Click on the button **PROGRAMMING**.
 - ↳ The programming app launches.
 11. Carry out all tasks.
 - ↳ The following programming tasks can be expected: Removing authorisations for the deleted key from all locking devices and authorise a new key for the locking devices if required.
- ↳ Programming is performed.



CAUTION

Unauthorised access after theft

A stolen key is authorised at the locking system until the key is deleted and the locks are reprogrammed.

- Re-programme all authorised keys immediately if a key is lost.

10.2 Defective lock

Locking devices or locking cylinders may present a defect. First, change the batteries of the lock (see the quick guide supplied). Then try to program the lock again.

If the locking device still doesn't work correctly, it needs to be replaced.

You can also simply replace the lock if you want to use a lock with different properties.

Proceed as follows to replace a locking device:

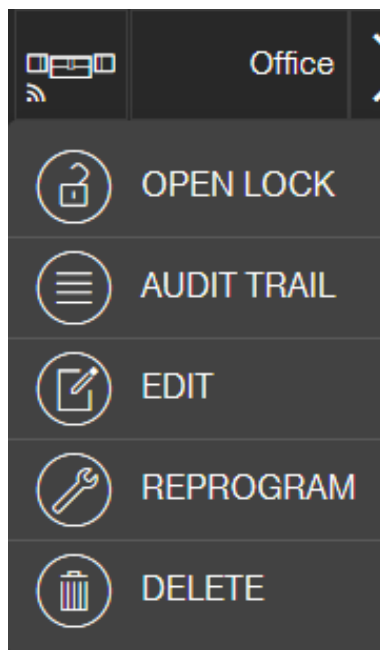
✓ Matrix screen open

1. Remove the locking device concerned from the door.

It may be difficult to remove a lock from a locked door. If necessary, ask the dealer who installed the SimonsVoss products for advice.

2. Click on the lock concerned in the locking plan.

↳ The context menu opens.



3. Click the  DELETE button.

↳ The lock is flagged for reset.

↳ Task will be completed in the programming app at a later stage.



4. If the locking device is defective: Click on the lock.

↳ The context menu opens.

5. Click the button  "FORCE DELETE".



↳ Lock is permanently deleted in the locking plan.

6. Create a new lock (see [Creating a lock \[▶ 17\]](#) oder [Creating a lock with online upgrade \[▶ 40\]](#)).

7. Assign the necessary authorisations (see *Issue authorisation and save* [[▶ 21](#)]).
8. Click on the button **SAVE**.
9. Click on the menu button 
 - ↳ Menu opens.
10. Click on the button  **PROGRAMMING**.
 - ↳ The programming app launches.
11. Carry out all tasks.
 - ↳ Programming is performed.

10.3 Reset or re-use deleted components

If you delete a SimonsVoss component, such as a key or locking device, from the locking system without resetting it correctly beforehand, you can still continue to use it:




- ✓ Matrix screen open
1. Add the component concerned (e.g. key or transponder) to the locking plan again.
 2. Click on the menu button 
 - ↳ Menu opens.
 3. Click on the button  **PROGRAMMING**.
 - ↳ The programming app launches.
 4. Complete all tasks.
 - ↳ The initial attempt to re-programme is acknowledged with an error message.
 5. Carry out the task again.
 - ↳ Component is now reprogrammed.

Always reset the components correctly to prevent this problem.

10.4 Read components

You can read all MobileKey components to see what their purpose is. This might be important if you find a key, such as a transponder, to which you are unable to assign to a user, for example.


How to read out MobileKey components:

1. Click on the menu button 
 - ↳ Menu opens.
2. Click on the button  **PROGRAMMING**.
 - ↳ The programming app launches.
3. Click on the button  **READ DEVICE**.



NOTE

Reading in macOS/Android

The programming interface opens directly in the application itself instead of a programming app. There is no  **READ DEVICE** button. Click on the wireless icon button.

4. Select the component that you wish to read.

↳ Feedback message shows, for example, the name of the key (John Smith) or whether a non-programme MobileKey component is in storage mode.

Alternatively, you can also read out the component list (see *Exporting the component list* [▶ 28]).

10.5 SmartBridge does not work

Go through the following check list if the automatic configuration was not successful due to a problem with SmartBridge:

- ❑ Check the **power supply**.
 - ❑ Is the SmartBridge LED flashing?
- ❑ Check the **LAN connection**.
- ❑ Check the **Internet access**.
 - ❑ Are the **ports 1883 and 8883** (TCP/IP) of the firewall open?

If necessary, add appropriate exceptions or forwarding in your router to allow the SmartBridge to communicate externally on ports 1883 and 8883. Look for *port sharing*, *port forwarding*, *special applications*, or the like.



NOTE

Port sharing device dependent

Usually routers automatically recognise that the SmartBridge wants to communicate via port 8883 and releases the port.



- ❑ In exceptional cases or in higher-security networks, you must release the port manually (see the following examples).

Special Applications List

Name	Status	Trigger Port	Trigger Protocol	Open Protocol	Open Port	Options
TCP	On	1883	TCP/UDP	TCP/UDP	1883	Edit Delete
TCP2	On	8883	TCP/UDP	TCP/UDP	8883	Edit Delete

Add

Freigaben

Status	Bezeichnung	Protokoll	IP-Adresse im Internet	Port extern vergeben	
●	MobileKey	TCP	IPv4	8883 (8883)	 

Neue Freigabe

- ❑ Is the DHCP server configured in such a way that a device is able to register on the network?

You can also reach the SmartBridge via a Windows PC using the **SimonsVoss OAM tool**. The OAM Tool allows you make additional settings to SmartBridge, such as assigning a fixed IP address or configuring the integrated DHCP server settings. You can find the OAM tool in the software downloads on the SimonsVoss homepage (www.simons-voss.com).

Detailed information on the OAM tool can be found in the OAM tool manual.



NOTE

Using fixed IP addresses

DHCP is activated by default. The IP address is assigned automatically. Alternatively, you can also assign a fixed IP address.

- ❑ If you use a fixed IP address, enter a DNS (Domain Name Service) via the OAM tool.
- ❑ Check whether the **chip IDs and MobileKey IDs** have been entered correctly.
- ❑ Is the **distance** between the SmartBridge and lock more than 1.5 m and less than about 30 m?
 - ❑ Test the set-up if there is a clear linear distance of 3 m without any obstacles.
 - ❑ Environmental influences, walls, objects and many other factors have a considerable effect on signal quality. Network coverage up to about 30 m cannot be guaranteed. If necessary, place additional SmartBridges.



NOTE

Resetting the SmartBridge

The SmartBridge can be reset to the factory settings by means of a hardware reset (see the supplied quick guide or manual).

10.6 PIN code keypad with online upgrade does not work

If you have a problem with the online PIN code keypad, go through the following checklist.

1. Check the **battery level**. Perform a battery test (see the quick guide provided).
2. Check that the **chip IDs** have been entered correctly.
3. Check whether the lock is correctly assigned to the Online PIN code keypad (see *Adding a PIN code keypad with online upgrade* [▶ 42]).

10.7 Lock with online upgrade does not work

Go through the following checklist if the automatic configuration was not successful due to **problems with online locks**:

1. Check that the different locks **chip IDs** have all been entered correctly.
2. Check that the **network thumbturn cap (LockNode) is installed correctly**. See also the supplied quick guide.
 - ↳ After the network thumbturn cap has been installed correctly, you will hear four short beeps.
3. When retrofitting or replacing network thumbturn caps, check the correct assignment of the locks!

10.8 Network error

Check that your Internet connection is stable if several network errors occur within 24 hours.



NOTE

Many standard Internet routers obtain a new IP address at specific intervals, which may lead to a brief interruption in the Internet connection. An error message will be generated (*mainly at night*) if this process is longer than 30 seconds.

10.9 Manual resetting of LockNodes

A programmed online locking device consists of two separately programmed components: the locking device and the LockNode. Both components are matched to one another and cannot be used in another locking system when programmed. Always use the web app to reset the LockNode; see *Disconnecting components with online upgrade* [▶ 46].

If this step is not possible, the LockNode configuration can only be reset with the help of a locking device which does not form part of the locking system. Fit the LockNode temporarily to an unknown locking device for this purpose. The system signals that the LockNode is reset after a few seconds:

- Locking cylinder: Audible signal (4 beeps)
- SmartRelay: Optical signalling by LED. (Ensure the power supply is correct)

The LockNode can be connected to any SmartBridge again once it has been reset.

11. Maintenance, cleaning and disinfection

IMPORTANT

Damage to surfaces

The use of unsuitable or aggressive disinfectants can damage MobileKey components.

1. Keep oil, paint, grease or acid away from your MobileKey components.
2. Only use disinfectants that are expressly intended for disinfecting sensitive metallic surfaces or plastics.



CAUTION

Battery replacement

Empty batteries always must be replaced by new ones approved for use by SimonsVoss (see the respective quick guide). Always dispose of old batteries in the proper manner.

12. MobileKey apps

The MobileKey app is available from iOS and Android app stores and supports the following functions:

- Overview of door statuses (if DM cylinder is used).
- Remote opening.
- Sending of Key4Friends authorisations.
- Reading and display of the access list.
- Reception of push messages from event management.
- Use of touch ID for security-related actions (remote opening, Key4Friends, deactivating push messages).
- Programming of keys and locking devices using the USB config device.
Only available with Android devices with OTG function and OTG cable.

13. Tips & Tricks

13.1 Link to the web app

A direct link to the MobileKey web app can be established on all devices. The web app can be launched particularly quickly and conveniently on your desktop or home screen, even on smartphones and tablet PCs. Try it out!

13.2 Using keys without the USB config device

All keys (transponders) must be programmed using the USB config device at the moment. This makes things particularly difficult when there is no access to a Windows or Android device. You will find below a way in which you can assign pre-programmed keys with any supported end device without needing to use a USB config device:

- ✓ Locks with ONLINE extension.
 - ✓ Locks with "ONLINE" status.
 - ✓ Matrix screen open
1. First of all, create a number of keys, such as Key Extra1, Extra2, Extra3 and so on.
 - ↳ These keys are not assigned authorisations to begin with.
 2. Programme all keys once with the USB config device and make them with a name if required.
 - ↳ A key can obviously also be read at a later point in time.
 3. Instead of adding a new key and programming it with the USB config device, simply change the properties of a key that you added previously, such as "Extra1".
 4. Click on the key you have already created, e.g. "Extra1" and select **EDIT**.
 5. Change the name.
 6. Optionally enter data for "Valid from" and "Valid to".
 7. Click on the **SAVE** button and return to the matrix.
 - ↳ Key is saved.
 8. Authorise the key for all required locking devices.
 9. Click on the button **SAVE**.
 - ↳ Programming takes place online via the SmartBridge.
 - ↳ Keys are authorised on selected locks.

13.3 Setting the language



You can very easily set the language for the web app. The following are available:

- 🇬🇧 English
- 🇩🇰 Danish

- German
- French
- Italian
- Dutch
- Swedish

Procedure:

✓ Matrix screen open

1. Click on the menu symbol .
↳ Menu on the right launches.
2. Click on the button  **MANAGE ACCOUNT**.
↳ The account overview opens
3. In the upper area of the account overview, click on the button **LANGUAGES**.
↳ Selection menu for languages is opened.
4. Select the language that you require.
↳ Language is set.

Return to the matrix with the button **HOME**.

14. Help and other information

Information material/documents

You will find detailed information on operation and configuration and other documents on the website:

<https://www.simons-voss.com/en/documents.html>

Software and drivers

Software and drivers can be found on the website:

<https://www.simons-voss.com/en/service/software-downloads.html>

Declarations of conformity

You will find declarations of conformity and other certificates on the website:

<https://www.simons-voss.com/en/certificates.html>

Technical support

Our technical support will be happy to help you (landline, costs depend on provider):

+49 (0) 89 / 99 228 333

Email

You may prefer to send us an email.

support-simonsvoss@allegion.com

FAQs

You will find information and help in the FAQ section:

<https://faq.simons-voss.com/otrs/public.pl>

Address

SimonsVoss Technologies GmbH
Feringastr. 4
D-85774 Unterfoehring
Germany



This is SimonsVoss

SimonsVoss, the pioneer in remote-controlled, cable-free locking technology provides system solutions with a wide range of products for SOHOs, SMEs, major companies and public institutions. SimonsVoss locking systems combine intelligent functionality, high quality and award-winning design Made in Germany.

As an innovative system provider, SimonsVoss focuses on scalable systems, high security, reliable components, powerful software and simple operation. As such, SimonsVoss is regarded as a technology leader in digital locking systems.

Our commercial success lies in the courage to innovate, sustainable thinking and action, and heartfelt appreciation of employees and partners.

SimonsVoss is a company in the ALLEGION Group, a globally active network in the security sector. Allegion is represented in around 130 countries worldwide (www.allegion.com).

Made in Germany

SimonsVoss is truly committed to Germany as a manufacturing location: all products are developed and produced exclusively in Germany.

© 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