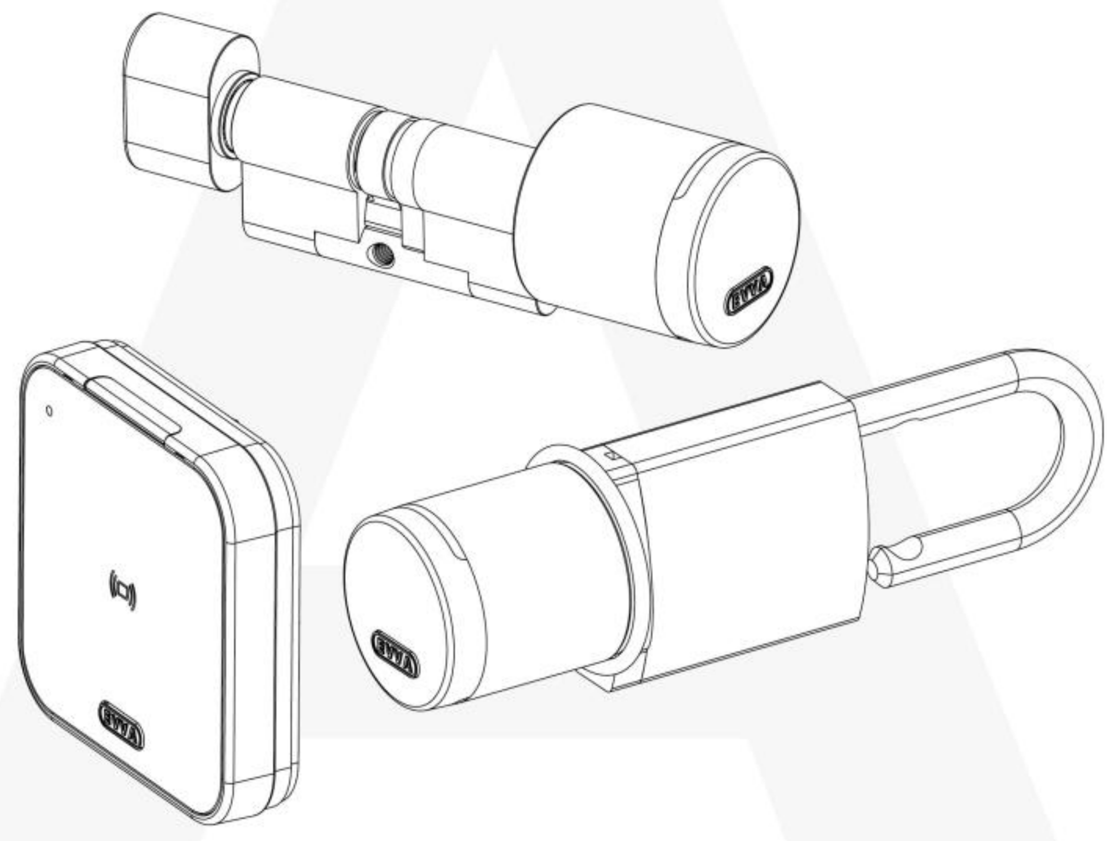


AirKey

System manual 2.7

1 Table of contents

2 Introduction, overview

This access control system manual contains information on installation, operation, and the controls of the electronic access control system, consisting of the AirKey Online Administration, app, cylinders, wall readers, padlocks, and media for the access control system.

The products and/or "AirKey Online Administration" user software described in the access control system manual must exclusively be operated by personnel that are adequately qualified for the corresponding task. Qualified personnel are able to identify risks when handling products / systems and prevent potential hazards on the basis of their expertise.

2.1 General legal notes

- EVVA concludes the contract on the use of AirKey exclusively on the basis of its General Terms and Conditions of Business (EVVA GTC) as well as its General Licensing Conditions (EULA) with regards to the software for the product.
- We explicitly notify clients that the use of the access control system subject to this contract may trigger legal approval, reporting or registration obligations, in particular with regard to data protection (e.g. a comprehensive information system), as well as grant the right of co-determination to staff in the event of use on corporate premises. Customers, clients, and end users shall be responsible for product use in compliance with legal stipulations.
- The aforementioned information must be observed and passed on to operators and users as per the defined manufacturer product liability according to product liability legislation. Non-compliance releases EVVA from any liability.
- Not suitable in environments with children under 36 months due to a risk of suffocation caused by small parts that may be swallowed.
- Any use deemed as non-compliant with the contract or as unintended use, any repair work or modifications that have not been explicitly approved by EVVA as well as all types of incorrect servicing may cause malfunctions and are prohibited. Any modifications that have not been explicitly approved by EVVA render claims to liability, warranty as well as any separate guarantee claims void.
- Architects and advisory institutions are obliged to request all necessary product information from EVVA and consider all such information to comply with obligations regarding information and instructions under the Product Liability Act. Specialist retailers and installers must comply with the information in EVVA documentation, and they must pass on such information to customers, if applicable.
- Please observe the corresponding international and national specifications in the corresponding legislation, directives, standards, and guidelines, particularly regarding the requirements for escape routes and emergency exits, during project management and installation of the locking components.

2.2 EVVA support

AirKey is a sophisticated and tested access control system. However, should you still require support, please do not hesitate to contact your EVVA partner.

A list of certified EVVA Partners is available on our homepage at https://www.evva.com/uk-en/handlersuche/.

Select the "Electronic system partner" filter option to exclusively filter for EVVA partners that offer electronic EVVA access control systems and can fall back on qualified specialist expertise in this area.

Use the EVVA online form for certain types of support requests. We currently provide the online form for the following situations:

- You have exceeded the maximum attempts to enter credit codes.
- Unable to add credit.
- AirKey Online Administration login page not available.
- Login unavailable. Forgot username and/or e-mail address.
- You have activated two-factor authentication and do not have access to your telephone number.

Click the following link to access the online form: https://www.evva.com/en/airkey/support/.

For general information on AirKey visit our homepage at https://www.evva.com/en/airkey/website/.

2.3 Signs and symbols

Throughout the system manual, sequences of commands, individual commands or buttons are illustrated as follows.

Example: Main menu ***Media & persons*** → ***Create person*** or buttons, such as ***Save***.

⚠	Warning, risk of material damage in the event of non-compliance with the corresponding safety measures.
❗	Notices and additional information
💡	Hints and recommendations
✖	Error messages
Option	Options

2.4 Tips for optimal navigation in this document

This document also contains many internal links that lead to other chapters or passages in the text. The quickest and most convenient way to get back to the original position or forward again under Windows is to use these key combinations:

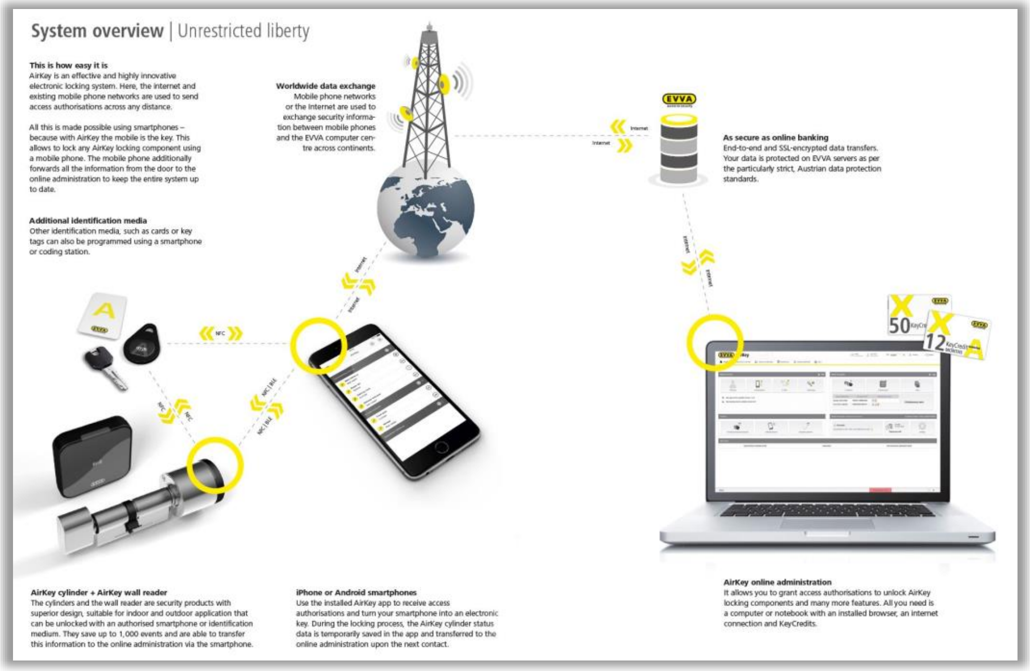
Alt + ◀	(Alt + cursor arrow to the left)	= navigate back
Alt + ▶	(Alt + cursor arrow to the right)	= navigate forward

These keyboard shortcuts work in many PDF viewers as well as in Microsoft Word, for example.

To try out the keyboard shortcuts, click this link and navigate back with Alt + ◀.

3 System architecture

The following figure provides an overview of AirKey locking components and their communication methods. This is followed by descriptions of the individual components.



System overview | Unrestricted liberty

This is how easy it is
AirKey is an effective and highly innovative electronic locking system. Here, the internet and existing mobile phone networks are used to send access authorisations across any distance.

All this is made possible using smartphones – because with AirKey the mobile is the key. This allows to lock any AirKey locking component using a mobile phone. The mobile phone additionally forwards all the information from the door to the online administration to keep the entire system up to date.

Additional identification media
Other identification media, such as cards or key tags can also be programmed using a smartphone or coding station.

Worldwide data exchange
Mobile phone networks or the Internet are used to exchange security information between mobile phones and the EVVA computer centre across continents.

As secure as online banking
End-to-end and SSL-encrypted data transfers. Your data is protected on EVVA servers as per the particularly strict, Austrian data protection standards.

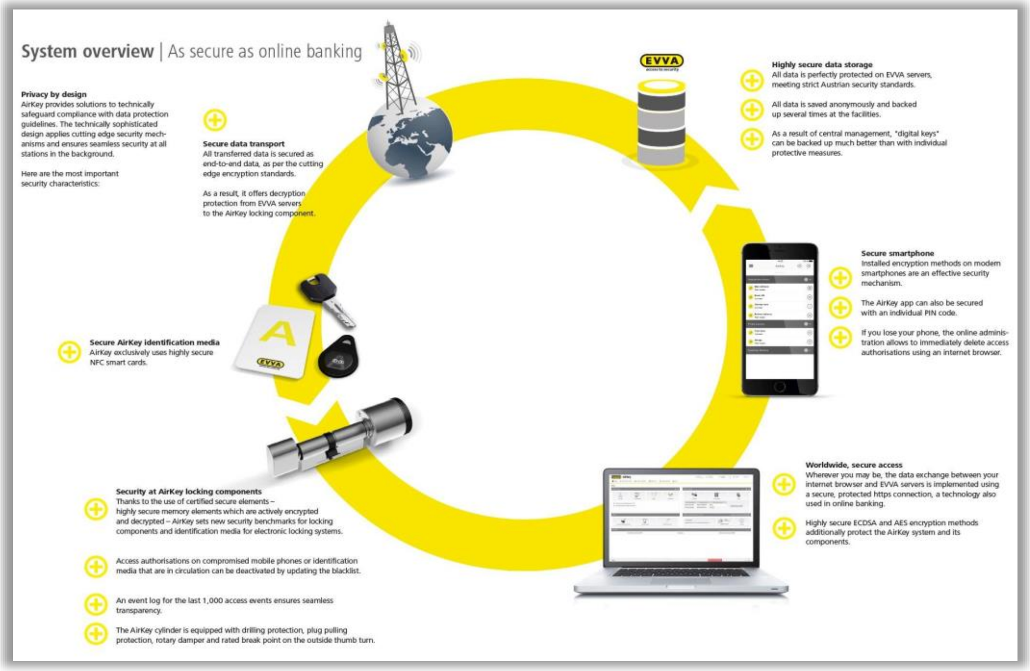
AirKey cylinder + AirKey wall reader
The cylinders and the wall reader are security products with superior design, suitable for indoor and outdoor application that can be unlocked with an authorised smartphone or identification medium. They save up to 1,000 events and are able to transfer this information to the online administration via the smartphone.

iPhone or Android smartphones
Use the installed AirKey app to receive access authorisations and turn your smartphone into an electronic key. During the locking process, the AirKey cylinder status data is temporarily saved in the app and transferred to the online administration upon the next contact.

AirKey online administration
It allows you to grant access authorisations to unlock AirKey locking components and many more features. All you need is a computer or notebook with an installed browser, an internet connection and KeyCredits.

Figure 1: System architecture

All transferred data is secured as end-to-end data according to the most recent encryption standards, encrypted from EVVA servers to locking components.



System overview | As secure as online banking

Privacy by design
AirKey provides solutions to technically safeguard compliance with data protection guidelines. The technically sophisticated design applies cutting edge security mechanisms and ensures seamless security at all stations in the background.

Here are the most important security characteristics:

Secure data transport
All transferred data is secured as end-to-end data, as per the cutting edge encryption standards.

As a result, it offers decryption protection from EVVA servers to the AirKey locking component.

Highly secure data storage
All data is perfectly protected on EVVA servers, meeting strict Austrian security standards.

All data is saved anonymously and backed up several times at the facilities.

As a result of central management, "digital keys" can be backed up much better than with individual protective measures.

Secure smartphone
Installed encryption methods on modern smartphones are an effective security mechanism.

The AirKey app can also be secured with an individual PIN code.

If you lose your phone, the online administration allows to immediately delete access authorisations using an internet browser.

Worldwide, secure access
Wherever you may be, the data exchange between your internet browser and EVVA servers is implemented using a secure, protected https connection, a technology also used in online banking.

Highly secure ECDSA and AES encryption methods additionally protect the AirKey system and its components.

Secure AirKey identification media
AirKey exclusively uses highly secure NFC smart cards.

Security at AirKey locking components
Thanks to the use of certified secure elements – highly secure memory elements which are actively encrypted and decrypted – AirKey sets new security benchmarks for locking components and identification media for electronic locking systems.

Access authorisations on compromised mobile phones or identification media that are in circulation can be deactivated by updating the blacklist.

An event log for the last 1,000 access events ensures seamless transparency.

The AirKey cylinder is equipped with drilling protection, plug pulling protection, rotary damper and rated break point on the outside thumb turn.

Figure 2: System overview – seamless security

3.1 Locking components

Locking components (AirKey cylinders and wall readers) control access at the doors. Depending on the authorisation, the locking component enables or denies access.

3.1.1 AirKey cylinders

AirKey cylinders are battery-operated locking components. They are certified for indoor and outdoor use. Depending on the specific requirements, AirKey cylinders may also be suitable for use in areas that are critical to security. AirKey cylinders boast mechanical protection from vandalism and manipulation. AirKey cylinders are suitable for installation in fire doors and emergency exit doors*, providing they have been installed as per the standards.

AirKey cylinders are available as half cylinders or double cylinders. Double cylinders are available as one-sided or double-sided access models. One-sided access models merely feature electric authorisation components on the outside, whereas users must provide authorisation on both sides with the double-sided access model. The electronic thumb turn on the identification side rotates freely unless authorisation is provided. The black plastic cap of the AirKey cylinder is the reader unit.

If users hold an authorised medium against the thumb turn, the cylinder engages briefly to allow to turn the electronic thumb turn and operate the lock. In this context, also observe the information on operating locking components.

Note that when the door is closed, it is not automatically locked. The door must be locked manually or alternatively using an additional device.

Please check if the AirKey cylinder you selected is suitable for your application. The AirKey cylinder is available in various designs and configurations for this purpose.

The required data sheets as well as the product catalogue are available on our homepage in the download section: https://www.evva.com/en/downloads/.

AirKey cylinders feature visual and acoustic signals. Please refer to the Locking components signals section for descriptions of the individual signals.

Follow the assembly manual enclosed with the packaging during assembly of the AirKey cylinder or the online assembly video clip at https://www.evva.com/en/airkey/website/.

* The FAP anti-panic function may be required for use in emergency exit and panic doors, depending on the mortise lock. For this purpose, please observe the corresponding information and certificates from lock manufacturers as well as the product code in the order.

3.1.2 AirKey hybrid cylinder

The AirKey hybrid cylinder has the same characteristics as the AirKey cylinder. It can therefore be used both indoors and outdoors as well as in safety-relevant areas.

Compared to the AirKey double cylinder with one-sided access, the AirKey hybrid cylinder has a key module on the inside instead of the mechanical knob. This means that access from the outside is via an electronic authorisation check and access from the inside via a mechanical key.

! Note that when the door is closed, it is not automatically locked. The door must be locked manually or alternatively using an additional device.

Please check whether the AirKey hybrid cylinder is suitable for your intended application.

The required data sheet as well as the product catalogue is available on our homepage in the download section: https://www.evva.com/en/downloads/.

The AirKey hybrid cylinder has an optical and an acoustic signal. The explanation of the various signals can be found under Locking components signals.

Follow the assembly manual enclosed with the packaging during assembly of the AirKey hybrid cylinder.

3.1.3 AirKey lever cylinder

The AirKey lever cylinder is a battery-operated locking component for use in lockers, showcases, various containers, up to letterboxes both indoors and outdoors.

Access is via an electronic authorisation check on the outside. There is a lever on the inside which locks the unit. Both unlocking and locking can only take place by manually turning the AirKey lever cylinder after a successful authorisation check. Unlike the AirKey cylinder and hybrid cylinder, the electronic knob on the identification side does not rotate freely without authorisation.

Please check whether the AirKey lever cylinder is suitable for your intended application. The AirKey lever cylinder is available in different designs and configurations.

The required data sheets as well as the product catalogue are available on our homepage in the download section: https://www.evva.com/en/downloads/.

The AirKey lever cylinder has an optical and an acoustic signal. The explanation of the various signals can be found under Locking components signals.

Follow the assembly manual enclosed with the packaging during assembly of the AirKey lever cylinder.

3.1.4 AirKey padlock

The AirKey padlock is a battery-operated locking component for use in barrier systems, roller shutters, depots, and archive containers both indoors and outdoors.

Access is via an electronic authorisation check on the underside. A hardened steel shackle is used for locking. Both unlocking and locking can only take place by manually turning the electronic knob of the AirKey padlock after a successful authorisation check.

Please check whether the AirKey padlock is suitable for your intended application. The AirKey padlock is available in different designs and configurations.

The required data sheet as well as the product catalogue is available on our homepage in the download section: https://www.evva.com/en/downloads/.

The AirKey padlock has an optical and an acoustic signal. The explanation of the various signals can be found under Locking components signals.

Follow the assembly manual enclosed with the packaging during assembly of the AirKey padlock.

Assembly tools for the AirKey cylinder, hybrid cylinder, lever cylinder, and padlock

AirKey cylinders, hybrid cylinders, lever cylinders and padlocks are protected against manipulation with a special mechanism. The electronic thumb turn can be removed with special tools only. The required assembly tools for assembly, disassembly, and those to change the batteries are not enclosed with the AirKey cylinder as standard and for this reason, they must be ordered separately.

The order code can be found in the AirKey product catalogue on our homepage in the download area https://www.evva.com/en/downloads/.

3.1.5 AirKey wall readers

AirKey wall readers are suitable for indoors and outdoors, surface-mounted, or flush installation and for areas critical to security.

Please use the dedicated seal enclosed with the product for use outdoors or in areas that are exposed to water as well as in the event of surface-mounted installation. Observe the information in the assembly manual.

AirKey wall readers are connected to the AirKey control unit using CAT5 cables (max. 100 m, loop max. = 2 Ohm) to supply them with power. The AirKey control unit is supplied with power by the mains adapter and in the event of a power cut it features a data buffer for a maximum of 72 h, providing the AirKey control unit had previously been in operation for a minimum of six hours.

Please note that one AirKey control unit each is required to operate one AirKey wall reader.

AirKey wall reader and control unit combinations can be used to operate electronic locking elements, such as motorised cylinders, sliding and swinging doors, etc.

It is also possible to connect an external enable element (button) to the control unit. Press it and the door opens as it would when accessing the door using the reader unit. However, opening the door using the external release element will NOT be logged. For security reasons please note that it is consequently possible to access AirKey systems with third-party systems without creating an entry in the event log.

Please check carefully to make sure the AirKey product you selected is suitable for your intended application / assembly situation. We have made the required data sheet, the product catalogue or assembly manual available in the download section of our homepage: https://www.evva.com/en/downloads/.

3.2 AirKey app

EVVA provides the AirKey app in the Google Play Store or Apple App Store free of charge.

The AirKey app is required to operate locking components with your smartphone. You can also use your smartphone to add or update locking components and media to your access control system. Most AirKey app features require an active Internet connection. However, locking components can also be operated offline.

Internet connections may incur extra charges. For this purpose, please note your provider agreement.

3.3 Smartphones

Smartphones must meet the following minimum requirements for use in access control systems:

- Smartphone featuring NFC or Bluetooth 4.0 (Bluetooth Low Energy/BLE)
- Operating system:
  - Android™ from 5.0 (NFC functionality available only)
  - Android™ from 6.0 (NFC and Bluetooth)
  - Apple™ from iOS 10 (Bluetooth functionality available only)
- AirKey app from Google Play Store or Apple App Store
- Android smartphones require "Access telephone status and identity" authorisation and location services must have been enabled.

List of smartphones compatible with the AirKey system

Please note that the smartphones' compatibility depends on many factors and not every smartphone that meets the minimum requirements can guarantee compatibility. For this reason, EVVA comprehensively tests smartphones. For a permanently up-to-date list of tested smartphone models suitable for use with AirKey go to the list of compatible smartphones.

Enabling **access to "Telephone status and identity"** is necessary to uniquely identify smartphones when adding them to a new access control system.

Access to the **location is necessary because Android 6+ demands the activation of location services to be able to scan for Bluetooth components!** If you would like to use Bluetooth functions in the AirKey app, you must activate the location services as well as authorise the app to access this data in the device settings. If you REFUSE to activate location services, you can establish a connection to the components (media and locking components) using NFC.

With **Apple devices** (iOS operating system) there is no option to deactivate the "Access telephone status and identity" authorisation. iOS can also search for Bluetooth components without having been granted access to location services.

3.4 AirKey media

As media currently available are tested smartphone models as well as cards, key fobs, combi keys and wristbands in various configurations, for example in combination with *Mifare DESFire EV1* technology.

The required data sheets as well as the product catalogue are available on our homepage in the download section: https://www.evva.com/en/downloads/.

Media, such as cards, key fobs, combi keys or wristbands are supplied in factory state. You must add media to your access control system before being able to use them.

3.5 AirKey Online Administration

The AirKey Online Administration is EVVA's online software solution to manage access control systems. The electronic access control system is compatible with all common Internet browsers and operating systems and does not require local software installations or dedicated IT infrastructure. EVVA is responsible for live operation and maintenance of AirKey servers.

3.5.1 System requirements

- Operating systems: Windows 10 (or higher), MacOS 10.15 (or higher), Linux
- Currently compatible with the following browsers: Chrome, Firefox, Edge, Safari
- JavaScript activated in browser
- Internet connection (1 MBit/s or faster)
- Optionally: USB port 2.0 for coding station
- Internet port 443 must be available.

! You require a valid e-mail address to register an AirKey access control system.

3.6 EVVA KeyCredits

KeyCredits are required to operate access control systems, for instance to assign or change access authorisations. KeyCredits are available either as quantity credit (defined number of enabled changes to authorisations within an unrestricted period of time) or as time credit (unrestricted number of enabled changes to authorisations within a defined period of time). The matching KeyCredit package for every application is available from specialist EVVA retailers, tailored to the size and dynamic characteristics of your access control system. Please refer to the AirKey product catalogue for more detailed information under https://www.evva.com/en/downloads/.

3.7 Coding station

Add or update locking components and media to your access control system using the optionally available coding station or a smartphone with maintenance authorisation. The coding station can be activated using an own application. The coding station application brings the advantage that it is compatible with current browsers and the coding station remains available for updates of locking components and media after the browser has been closed or users have logged off from the AirKey Online Administration.

The application supports the following browsers: Chrome, Firefox, and Edge.

System requirements:

- USB port
- Java 7 or higher
- Coding station driver

Please refer to Installing coding stations for more information.

3.8 Emergency power device

All locking components feature an interface at the front of the locking component, below the EVVA logo. Slightly press towards the inside on the left-hand side of the logo (near the "E") and fold out on the right-hand side (near the "A") to access it. The installed interface is intended for emergency power supply only and it is not required as part of normal operation.

The emergency power device supplies locking components with power to enable operation if the batteries have gone flat. For this purpose, connect the emergency power device connection cable to the corresponding interface and then switch it on. No other interactions with the emergency power device are required. A medium with valid authorisation is still required to operate the locking component.

In this process, please note that this must be a permanent authorisation without a restricted validity period. Please refer to Emergency media for more information. Immediately replace batteries after having used the emergency power device to operate locking components and subsequently update locking components to also enable access with additional media. Please refer to Replacing batteries and using the emergency power device for more information.

Please note that the AirKey wall reader cannot be supplied with power using the emergency power device, it is supplied with power using an external power supply in combination with the AirKey control unit.

4 Commissioning

This section describes the first steps to commission the access control system.

Visit our homepage at https://www.evva.com/en/airkey/website/ for a screencast describing the first steps and commissioning of the access control systems.

EVVA offers the following materials to support locking component assembly:

- **Assembly manual**:
  EVVA provides non-verbal assembly manuals to support locking component assembly. They are enclosed with the packaging of the corresponding product or available from our homepage at https://www.evva.com/en/downloads/.
- **Videos**:
  We have provided assembly video clips on our homepage at https://www.evva.com/en/airkey/website/.

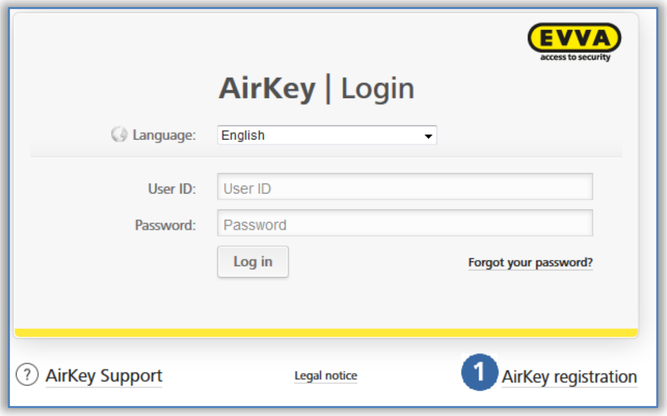
4.1 Installing the AirKey app

- Download the AirKey app from the Google Play Store or Apple App Store.
- Follow the AirKey app installation instructions on your smartphone.

4.2 Registering to the AirKey Online Administration

Register with EVVA using a valid e-mail address to be able to use the AirKey Online Administration.

- Open the following page in your browser: https://airkey.evva.com.
  The AirKey Online Administration login page opens.
- Select your preferred ***language***.
- Click the ***AirKey registration*** ❶ link.



AirKey | Login

Language: English

User ID: User ID

Password: Password

Log in

Forgot your password?

AirKey Support

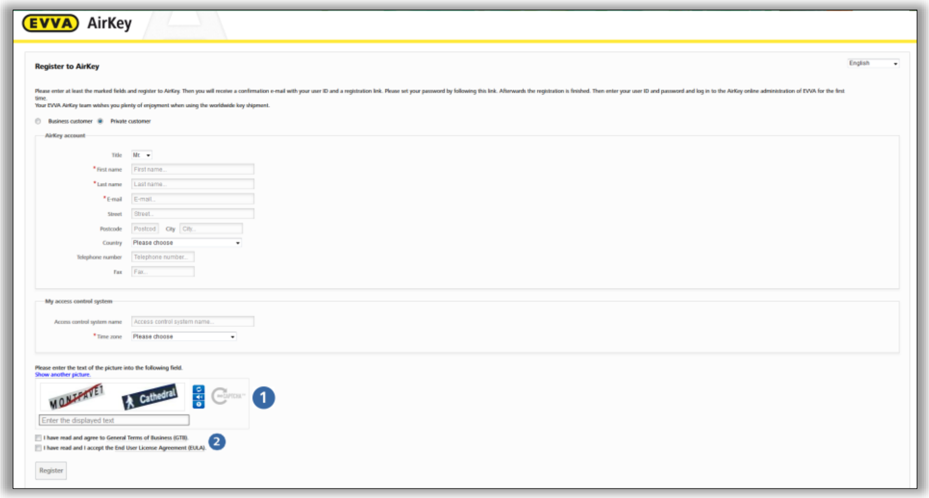
Legal notice

1 AirKey registration

Figure 3: "AirKey registration"link

Complete the fields in the registration screen and register to AirKey.

- Select ***Business customer*** or ***Private customer***.
- Complete the fields in the form.
  Fields highlighted by * are mandatory fields.
- Solve the Captcha ❶.
- Activate the checkbox using the General Terms and Conditions of Business (EVVA GTC) link and the checkbox at the General Licensing Conditions (EULA) ❷ link. The system automatically opens the two corresponding PDF documents. You can also access the documents at https://www.evva.com/en/airkey/impressum/.



Register to AirKey

Please enter at least the marked fields and register to AirKey. Then you will receive a confirmation e-mail with your user ID and a registration link. Please set your password by following this link. Afterwards the registration is finished. Then enter your user ID and password and log in to the AirKey online administration of EVVA for the first time.
Your EVVA AirKey team wishes you plenty of enjoyment when using the worldwide key shipment.

○ Business customer ● Private customer

AirKey account

Title: Mr
*First name: First name...
*Last name: Last name...
*E-mail: E-mail...
Street: Street...
Postcode: Postcod City: City...
Country: Please choose
Telephone number: Telephone number...
Fax: Fax...

My access control system

Access control system name: Access control system name...
*Time zone: Please choose

Please enter the text of the picture into the following field.
Show another picture.

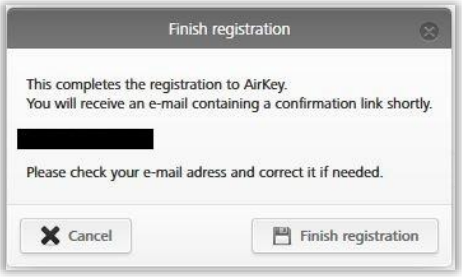
Enter the displayed text

□ I have read and agree to General Terms of Business (GTB).
□ I have read and I accept the End User License Agreement (EULA).

Figure 4: Registering to AirKey

If necessary, you can retrospectively change your customer data at any time. For this purpose, click ***Access control system*** → ***Customer data*** in the main menu of the AirKey Online Administration.

- Click ***Register***. The "Finish registration" application window opens.
- Once again check the e-mail address you entered as we will send a confirmation containing a registration link to this address.
- Click ***Cancel*** to cancel the process and correct your input if the e-mail address shown was incorrect.
- Click ***Finish registration*** if the e-mail address is correct and complete the process.



Finish registration

This completes the registration to AirKey.
You will receive an e-mail containing a confirmation link shortly.

[redacted]

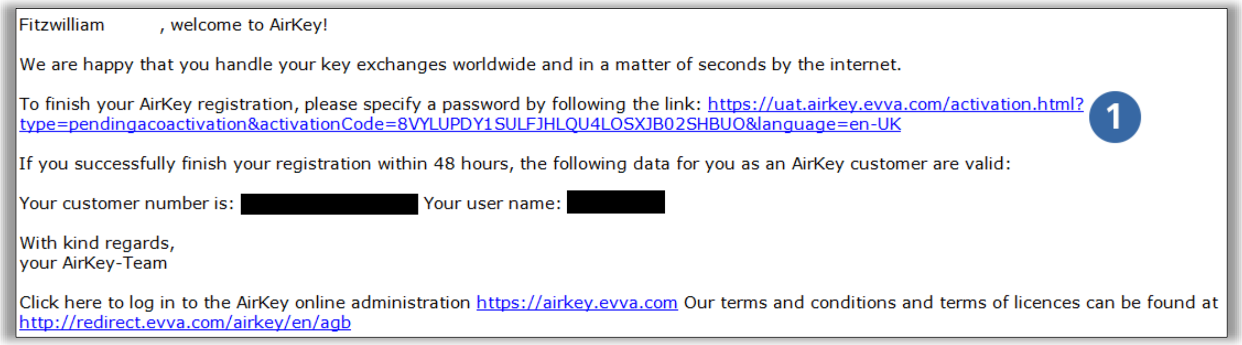
Please check your e-mail adress and correct it if needed.

Figure 5: Finishing registration

The access control system automatically generates one user ID and one registration link and sends it to the e-mail address you stated as part of a registration e-mail.

- Open your e-mail client. It will contain an e-mail from *EVVA AirKey* with the subject line "EVVA AirKey registration".
- Open the e-mail and click the registration link. ❶

Keep this e-mail safe. If you need support, you require the unique user ID and your customer number in the e-mail.



Fitzwilliam , welcome to AirKey!

We are happy that you handle your key exchanges worldwide and in a matter of seconds by the internet.

To finish your AirKey registration, please specify a password by following the link: https://uat.airkey.evva.com/activation.html?type=pendingacoactivation&activationCode=8VYLUPDY1SULFJHLQU4LOSXJB02SHBUO&language=en-UK

If you successfully finish your registration within 48 hours, the following data for you as an AirKey customer are valid:

Your customer number is: [redacted] Your user name: [redacted]

With kind regards,
your AirKey-Team

Click here to log in to the AirKey online administration https://airkey.evva.com Our terms and conditions and terms of licences can be found at http://redirect.evva.com/airkey/en/agb

Figure 6: "EVVA AirKey registration" e-mail

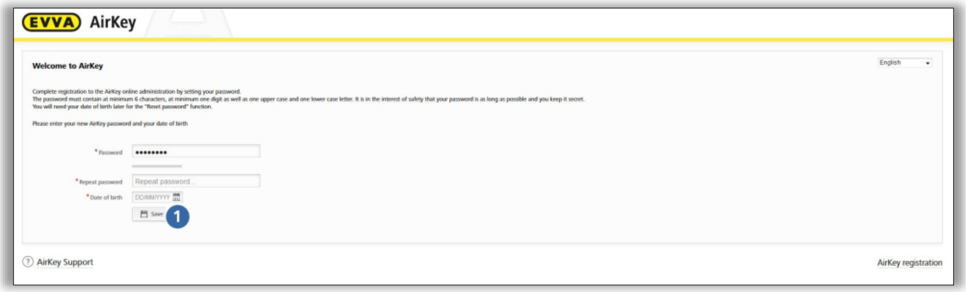
The registration link in the e-mail is valid for 48 hours only.

An error message indicating an invalid registration link will appear if the registration link has expired or if it is invalid. In this case, you must re-register.

The Welcome window opens after having clicked the registration link. This is where you complete registration.

- Enter a personal password for the AirKey Online Administration.
  The password must contain at least 6 characters and one numeral, as well as an upper-case and a lower-case letter. An error message is output if your password does not meet the specifications.
- Re-enter your password.
- Enter your date of birth. It is used as a security question to confirm your identity if you have forgotten your password.

We recommend you make your AirKey password as long as possible and do not disclose it.



Welcome to AirKey

Complete registration to the AirKey online administration by setting your password.
The password must contain at minimum 6 characters, at minimum one digit as well as one upper case and one lower case letter. It is in the interest of safety that your password is as long as possible and you keep it secret.
You will need your date of birth later for the "Reset password" function.

Please enter your new AirKey password and your date of birth

* Password: ••••••••
* Repeat password: Repeat password...
* Date of birth: DD/MM/YYYY

Figure 7: Specifying an AirKey password to complete registration

- Click ***Save*** ❶ to finish registration once you have completed the mandatory fields and both AirKey passwords match.

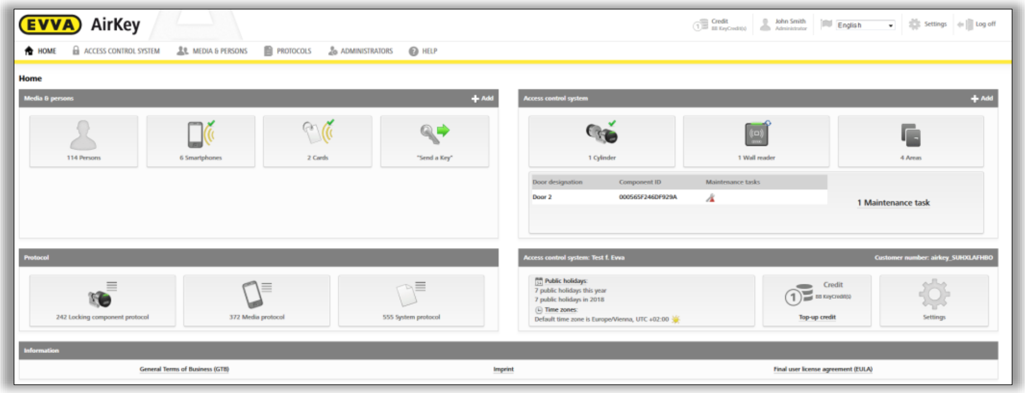
You have now completed the registration process and your access control system has been activated successfully.

You can now log on at any time on the AirKey Online Administration login page. All you need is the user ID from the registration e-mail and the previously defined AirKey password.

4.3 Login

You must log in to configure and manage the access control system.

- Open the following page in your browser https://airkey.evva.com.
  The AirKey Online Administration login page opens.
- Select your preferred ***language***. You can change the language in the right-hand menu bar at any time within the active session.
- Enter your user ID from the registration e-mail and the defined password and confirm with ***Log in***. The access control system home screen appears.



Door designation	Component ID	Maintenance tasks
Door 2	000565F246DF929A	⚠

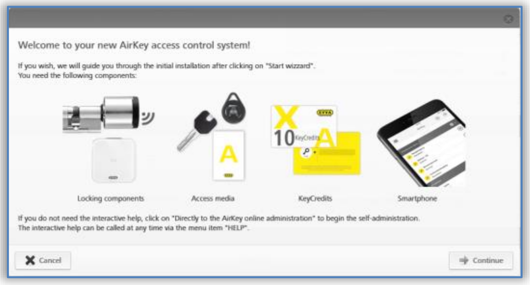
Public holidays:
7 public holidays this year
7 public holidays in 2018
Time zones:
Default time zone is Europe/Vienna, UTC +02:00

Figure 8: Access control system – home screen

The home screen provides an overview of all data relevant to the system. Browse to any functions and settings from this screen.

4.4 Interactive help

AirKey Online Administration starts the interactive help file after having logged in for the first time to give you a tour of the program and explain the most important functions.



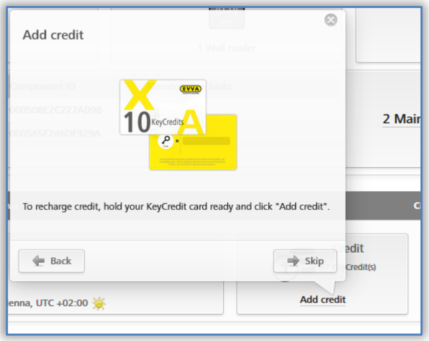
Welcome to your new AirKey access control system!

If you wish, we will guide you through the initial installation after clicking on "Start wizzard".
You need the following components:

If you do not need the interactive help, click on "Directly to the AirKey online administration" to begin the self-administration.
The interactive help can be called at any time via the menu item "HELP".

Figure 9: Interactive help

The example here is the "Add credit" function. The interactive help file will demonstrate which buttons to click and it will notify you of any information you need to enter in the fields. You can browse forwards and backwards within the interactive help file.



Add credit

To recharge credit, hold your KeyCredit card ready and click "Add credit".

Figure 10: Interactive help – topping up credit

You can also close the interactive help file and get to know the AirKey Online Administration using the system manual.

If you have closed and would like to re-open the interactive help, select ***Help* → *Interactive help*** in the main menu. Consequently, you can restart the interactive help as many times as you need, at any time.

4.5 Installing coding stations

Option

AirKey coding stations are optional components used to add or update locking components and media in access control systems.

To use a coding station in the AirKey system, it is necessary to install a coding station application.

There are two ways to use the coding station:

- in the browser, via the AirKey Online Administration.
- without a browser, via the command line

4.5.1 Using the coding station via the AirKey Online Administration

The coding station application brings the advantage that it is compatible with current browsers and the coding station remains available for updates of locking components and media after the browser has been closed or users have logged off from the AirKey Online Administration.

Adding and removing locking components to an access control system as well as the firmware update of locking components or the Keyring update of access media is only possible after logging in to the AirKey Online Administration. Updates of media and locking components are also possible after logging out of the AirKey Online Administration or when the browser has been closed.

The following browsers support communication between the AirKey Online Administration and the coding station application: Chrome, Firefox, and Edge.

Downloading and running the coding station application is browser / operating system specific. The illustration in your browser may differ from the depiction herein (Firefox).

Register and log in to the AirKey Online Administration (see chapter Registering to the AirKey Online Administration).

- Connect the coding station to a USB port on your computer.
- Click the ✚ icon in the bottom right ❶ of the AirKey Online Administration.

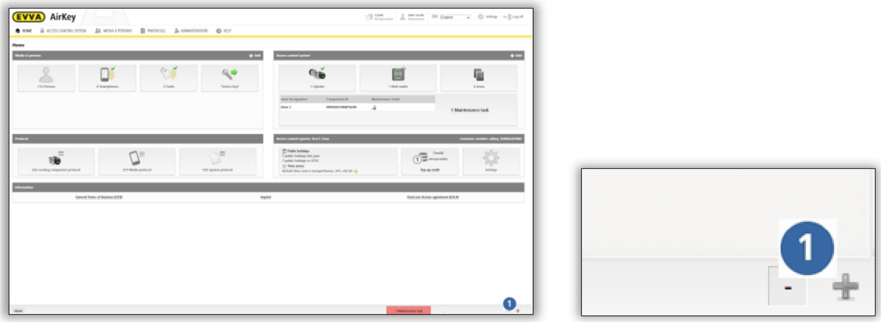
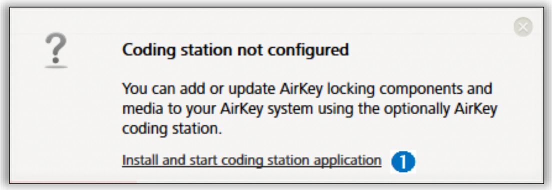


Figure 11: Coding station – installing the application

- Subsequently click the "Install and start AirKey coding station application" ❶ link to install the coding station application.



Coding station not configured

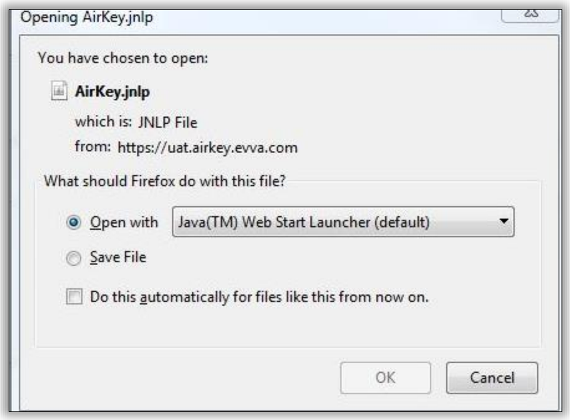
You can add or update AirKey locking components and media to your AirKey system using the optionally AirKey coding station.

Install and start coding station application ❶

Figure 12: Installing and starting coding station application

After having clicked the link, you have 60 seconds to open the AirKey.jnlp file (see continue step). If the system times out, you must repeat the installation from this step. Alternatively, you can also save the AirKey.jnlp file and manually open it.

- The AirKey.jnlp file download dialogue appears. Open the file using the "Java(TM) Web Start Launcher".



Opening AirKey.jnlp

You have chosen to open:

AirKey.jnlp

which is: JNLP File

from: https://uat.airkey.evva.com

What should Firefox do with this file?

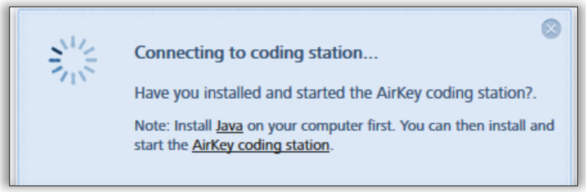
● Open with Java(TM) Web Start Launcher (default)

○ Save File

□ Do this automatically for files like this from now on.

Figure 13: Opening the AirKey.jnlp file

- A connection to the coding station is established after having opened the file.



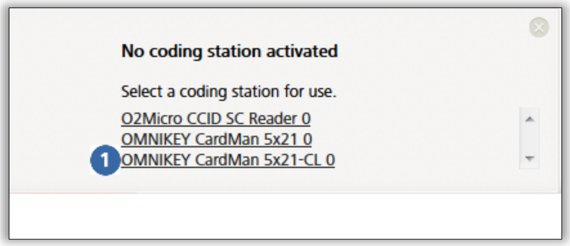
Connecting to coding station...

Have you installed and started the AirKey coding station?.

Note: Install Java on your computer first. You can then install and start the AirKey coding station.

Figure 14: Establishing a connection to the coding station

- Select the available coding station (e.g. "OMNIKEY CardMan 5x21-CL 0" ❶) from the list.



No coding station activated

Select a coding station for use.

O2Micro CCID SC Reader 0

OMNIKEY CardMan 5x21 0

OMNIKEY CardMan 5x21-CL 0

Figure 15: Selecting coding stations

- An AirKey icon Ⓐ appears in the taskbar in the bottom left – the coding station has been installed successfully and is active.

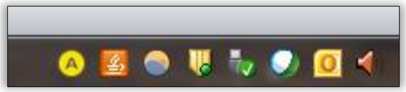


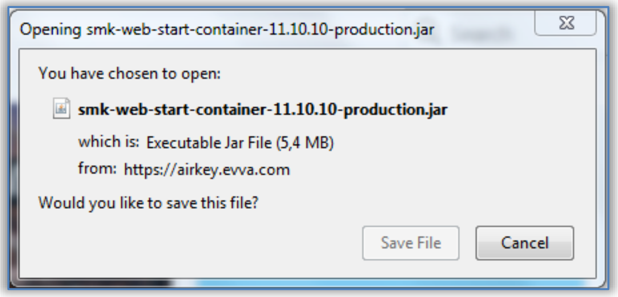
Figure 16: AirKey icon in the taskbar

4.5.2 Using the coding station via the command line

The coding station application can also be installed and configured without AirKey Online Administration, for example via the command line. (This option requires advanced IT know-ledge, especially working via the command line.)

Via the command line, the coding station can only be used to update access media and locking components. A firmware update of the locking components is only possible via browser or with a smartphone with maintenance authorisation.

- Save the coding station application via the link https://airkey.evva.com/smkrest/jnlp/newest-jar-file/ in the desired directory.



Opening smk-web-start-container-11.10.10-production.jar

You have chosen to open:

smk-web-start-container-11.10.10-production.jar

which is: Executable Jar File (5,4 MB)

from: https://airkey.evva.com

Would you like to save this file?

Figure 17: Download coding station application

- Open the command line and navigate to the directory where the coding station application was previously stored.
- Start the coding station application with the following command:

  `java -jar <filename>`

  (e.g. `web-start-container-customer-15.10.0-8.jar`)

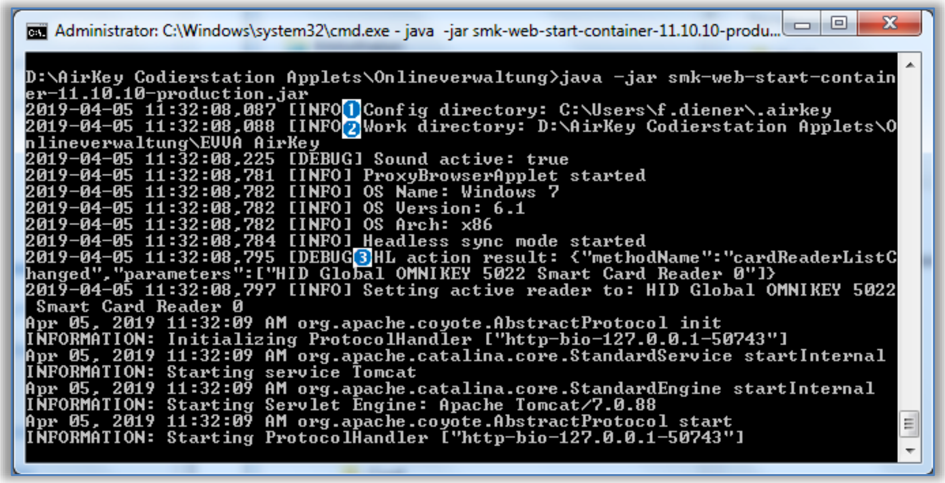
In addition, you can specify the following optional parameters:

- **`-reader "<name of the coding station>"`**: With this parameter, a specific coding station (e.g. "HID Global OMNIKEY 5022 Smart Card Reader 0") can be used. In this case, the configuration file `config_customer.json` is ignored.
- **`-port <VALUE [1024-65535]>`**: If this parameter is not specified, the port 50743 is used by default. Port 50743 is also used if the coding station is used via the AirKey Online Administration in the browser. If you want to use several coding stations in parallel on one computer, you must specify a separate port for each coding station. With the parameter "**`-port 0`**", a random port is used.
- **`-configDir <VALUE>`**: The configuration file `config_customer.json` is saved in the specified folder (default value for Windows: `%USERPROFILE%\.airkey`). This is automatically generated the first time the coding station application is started and saves the last settings used.
- **`-workDir <VALUE>`**: For example, the log file `logs\application.log` is created in the specified folder when the coding station application is started. All actions that were performed with the coding station application are logged in this file. If you use several coding stations in parallel, it makes sense to use a separate folder for each coding station.
- **`-notify <filename>`**: Defines an executable file / script that can forward the lockingSystemID as a hex string (argument1) or as a long-int (argument2) of an successfully updated access medium to a third party system. This parameter is mainly relevant for the integration of AirKey into third party

systems and the use of the AirKey Cloud Interface. There, the lockingSystemId of the access medium can then be evaluated and further processed. For example, to find out the person to whom the access medium belongs. Details about the AirKey Cloud Interface can be found in the chapter AirKey Cloud Interface (API).

- **`-version`**: Displays the version of the coding station application.
- **`-help`**: Opens the help and describes all possible parameters.

> The AirKey icon Ⓐ appears in the task bar at the bottom right. Information about the configuration directory ❶, the working directory ❷ and the available coding stations ❸ are displayed in the command line.



Administrator: C:\Windows\system32\cmd.exe - java -jar smk-web-start-container-11.10.10-produ...

```
D:\AirKey Codierstation Applets\Onlineverwaltung>java -jar smk-web-start-contain
er-11.10.10-production.jar
2019-04-05 11:32:08,087 [INFO①Config directory: C:\Users\f.diener\.airkey
2019-04-05 11:32:08,088 [INFO②Work directory: D:\AirKey Codierstation Applets\O
nlineverwaltung\EVVA AirKey
2019-04-05 11:32:08,225 [DEBUG] Sound active: true
2019-04-05 11:32:08,781 [INFO] ProxyBrowserApplet started
2019-04-05 11:32:08,782 [INFO] OS Name: Windows 7
2019-04-05 11:32:08,782 [INFO] OS Version: 6.1
2019-04-05 11:32:08,782 [INFO] OS Arch: x86
2019-04-05 11:32:08,784 [INFO] Headless sync mode started
2019-04-05 11:32:08,795 [DEBUG③HL action result: {"methodName":"cardReaderListC
hanged","parameters":["HID Global OMNIKEY 5022 Smart Card Reader 0"]}
2019-04-05 11:32:08,797 [INFO] Setting active reader to: HID Global OMNIKEY 5022
 Smart Card Reader 0
Apr 05, 2019 11:32:09 AM org.apache.coyote.AbstractProtocol init
INFORMATION: Initializing ProtocolHandler ["http-bio-127.0.0.1-50743"]
Apr 05, 2019 11:32:09 AM org.apache.catalina.core.StandardService startInternal
INFORMATION: Starting service Tomcat
Apr 05, 2019 11:32:09 AM org.apache.catalina.core.StandardEngine startInternal
INFORMATION: Starting Servlet Engine: Apache Tomcat/7.0.88
Apr 05, 2019 11:32:09 AM org.apache.coyote.AbstractProtocol start
INFORMATION: Starting ProtocolHandler ["http-bio-127.0.0.1-50743"]
```

Figure 18: Starting coding station application via command line

4.5.3 Configuring the coding station application

Right-click the AirKey icon Ⓐ to open the corresponding context menu.

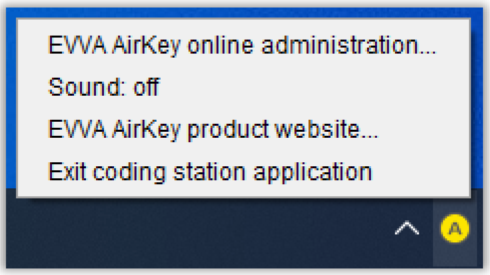

EVVA AirKey online administration...
Sound: off
EVVA AirKey product website...
Exit coding station application
A

Figure 19: Configuring the coding station application

List of corresponding menu items:

> ***EVVA AirKey Online Administration*** – AirKey Online Administration login page link

> ***Sound: on*** – a sound is indicated when updating components using a coding station. Audible feedback signals are recommended if the coding station is used without AirKey Online Administration. With click on ***Sound: on*** it will change to ***Sound: off***.

> ***Sound: off*** – no sound will be emitted. With click on ***Sound: off*** it will change to ***Sound: on***.

- ***EVVA AirKey product website*** – link to AirKey product website
- ***Exit coding station application*** – quits the coding station application.

4.5.4 Solutions for possible problems with the coding station

The LED indicates the coding station is ready for operation once it has been connected. Disconnect and reconnect if the coding station does not indicate it is ready for operation. If necessary, re-install the coding station drivers.

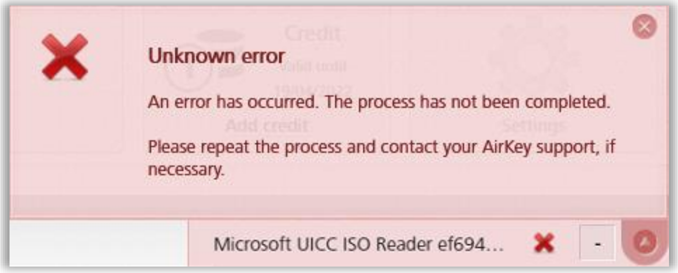
The coding station application is automatically quit upon shutting down the computer. Create an application shortcut to the AirKey.jnlp-File and save it in the auto start folder.

The coding station application ends after starting

By default, the coding station application uses port 50743 for communication with the browser. If this port is used by another program, the coding station application cannot be started. On Windows 10 or later, this port can be used by Hyper-V. You can prevent Hyper-V from using this port as follows:

- Deactivate Hyper-V:
  ```
  C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V
  ```
- Restart the computer.
- Add an exception for port 50743:
  ```
  C:\> netsh int ipv4 add excludedportrange protocol=tcp startport=50743
       numberofports=1
  ```
- Reactivate Hyper-V:
  ```
  C:\> dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All
  ```
- Restart the computer.

The Microsoft UICC card reader is selected as the coding station



Unknown error

An error has occurred. The process has not been completed.

Please repeat the process and contact your AirKey support, if necessary.

Figure 20: Microsoft UICC card reader in AirKey Online Administration

As a solution, this card reader can be deactivated in the Windows Device Manager:
Device Manager → Software devices → Microsoft UICC ISO Reader → Disable device

The connection to the coding station cannot be established via the AirKey Online Administration (https proxy)

Both the AirKey Online Administration and the coding station application communicate in encrypted form with the AirKey system via port 443. However, in networks that use an https proxy, it may be necessary to define an exception for "airkey.evva.com" and subdomains because the coding station application uses "certificate pinning" to check the server certificate and therefore does not allow https proxies.

The connection to the coding station cannot be established via the AirKey Online Administration (DNS rebinding protection)

The AirKey Online Administration communicates locally between the browser and the coding station application. Actions such as placing locking components or access media on the coding station are then displayed in the AirKey Online Administration.

The browser connects to the coding station application via "components.airkey.evva.com" (port 50743). This URL is resolved by the DNS server as 127.0.0.1.

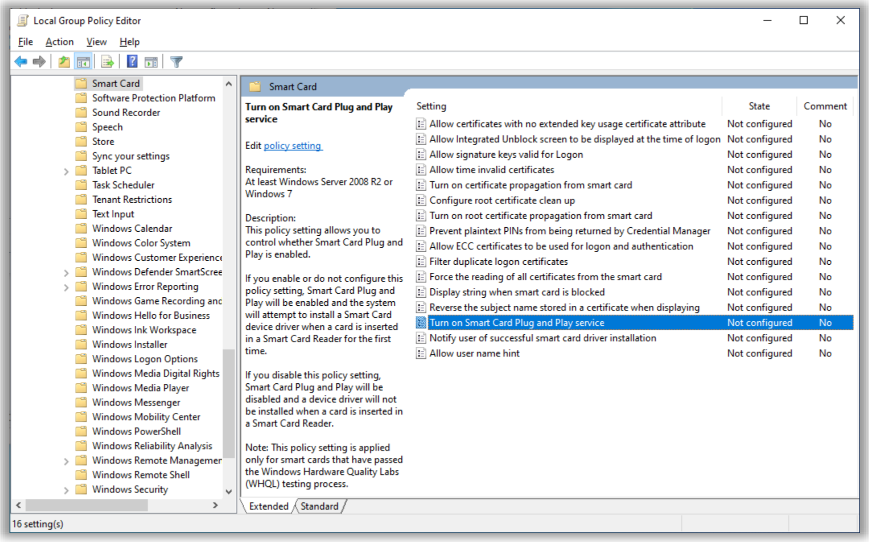
Therefore, it may be necessary to add exceptions for "components.airkey.evva.com" and subdomains of "airkey.evva.com" when DNS rebind protection is active.

Windows searches the driver for the coding station repeatedly

When you place a locking component or an access medium on the coding station, Windows tries to find and install a driver for the coding station. This can affect the communication with the coding station and lead to malfunctions.

As a solution, the Windows smart card plug and play service can be disabled:

- Windows key + R
- Type "gpedit.msc" and confirm with ***Enter***.
- Program "Local Group Policy Editor" → Computer Configuration → Administrative Templates → Windows Components → Smart Card
- Double-click the line with the entry "Turn on Smart Card Plug and Play service" on the right-hand side.



Turn on Smart Card Plug and Play service

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:
This policy setting allows you to control whether Smart Card Plug and Play is enabled.

If you enable or do not configure this policy setting, Smart Card Plug and Play will be enabled and the system will attempt to install a Smart Card device driver when a card is inserted in a Smart Card Reader for the first time.

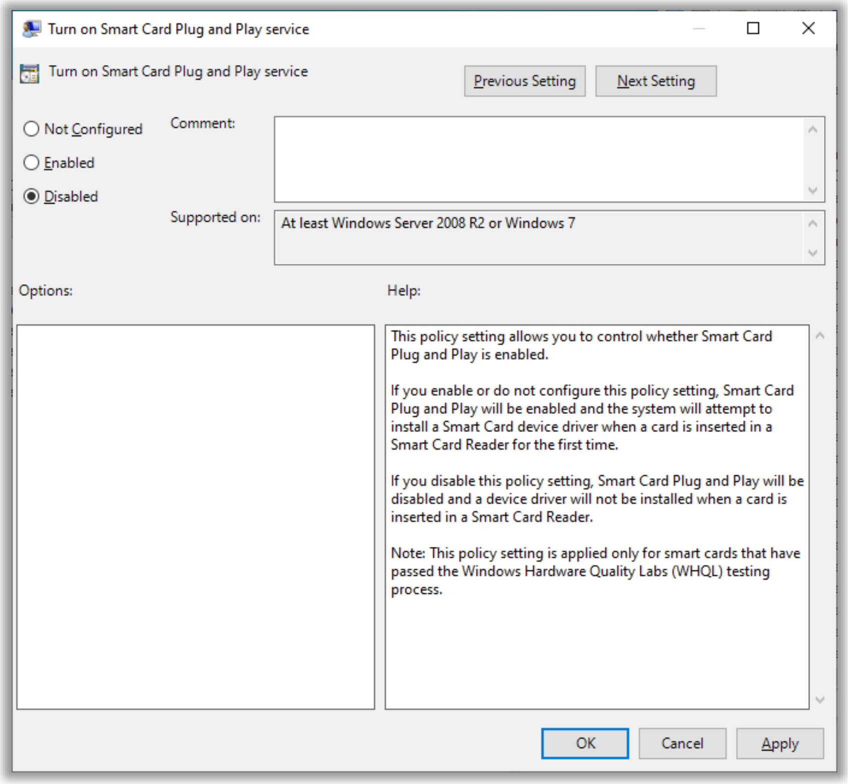
If you disable this policy setting, Smart Card Plug and Play will be disabled and a device driver will not be installed when a card is inserted in a Smart Card Reader.

Note: This policy setting is applied only for smart cards that have passed the Windows Hardware Quality Labs (WHQL) testing process.

Setting	State	Comment
Allow certificates with no extended key usage certificate attribute	Not configured	No
Allow Integrated Unblock screen to be displayed at the time of logon	Not configured	No
Allow signature keys valid for Logon	Not configured	No
Allow time invalid certificates	Not configured	No
Turn on certificate propagation from smart card	Not configured	No
Configure root certificate clean up	Not configured	No
Turn on root certificate propagation from smart card	Not configured	No
Prevent plaintext PINs from being returned by Credential Manager	Not configured	No
Allow ECC certificates to be used for logon and authentication	Not configured	No
Filter duplicate logon certificates	Not configured	No
Force the reading of all certificates from the smart card	Not configured	No
Display string when smart card is blocked	Not configured	No
Reverse the subject name stored in a certificate when displaying	Not configured	No
Turn on Smart Card Plug and Play service	Not configured	No
Notify user of successful smart card driver installation	Not configured	No
Allow user name hint	Not configured	No

Figure 21: Local Group Policy Editor

- Select radio button ***Disabled***.
- Confirm with ***OK***.


Turn on Smart Card Plug and Play service
Turn on Smart Card Plug and Play service
Previous Setting
Next Setting
Comment:
Supported on:
Options:
Help:
OK
Cancel
Apply

○ Not Configured
○ Enabled
● Disabled

Supported on: At least Windows Server 2008 R2 or Windows 7

This policy setting allows you to control whether Smart Card Plug and Play is enabled.

If you enable or do not configure this policy setting, Smart Card Plug and Play will be enabled and the system will attempt to install a Smart Card device driver when a card is inserted in a Smart Card Reader for the first time.

If you disable this policy setting, Smart Card Plug and Play will be disabled and a device driver will not be installed when a card is inserted in a Smart Card Reader.

Note: This policy setting is applied only for smart cards that have passed the Windows Hardware Quality Labs (WHQL) testing process.

Figure 22: Smart Card Plug and Play service

No coding station can be selected with MacOS 11.x or higher

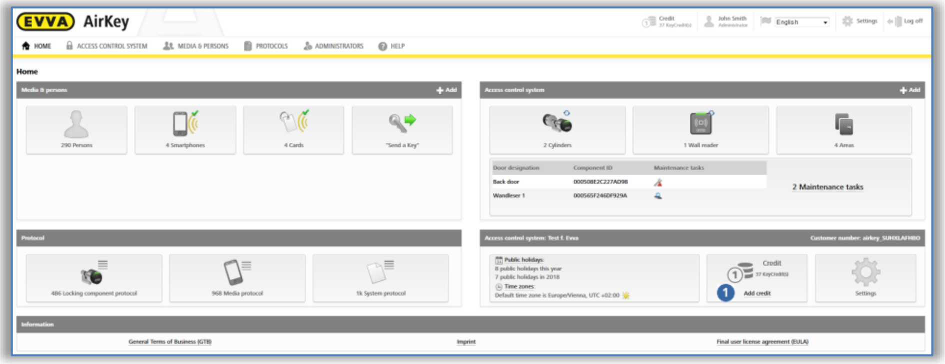
Since MacOS Big Sur (11.x) it is no longer possible on a Mac to select a connected coding station via the AirKey Online Administration. The coding station application can be started successfully, but no coding station is displayed in the AirKey Online Administration.

As a solution, the coding station can be started via the command line (see chapter Using the coding station via the command line). However, a prerequisite for this is that the Java version JDK17 (Oracle JDK17 or OpenJDK17) or higher is installed.

4.6 Add credit

For this purpose, a KeyCredit card is required featuring a scratch field on the rear that conceals a credit code.

- On the ***Home*** screen, select the ***Add credit*** button. ❶
- Alternatively click ***Credit*** in the header.

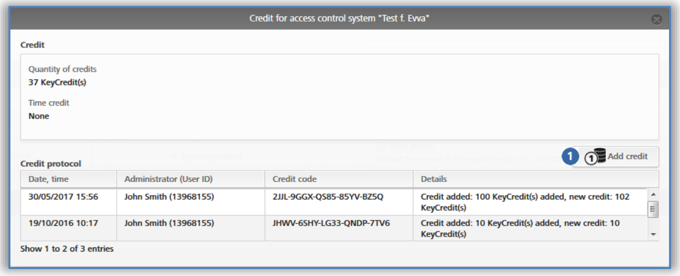


Door designation	Component ID	Maintenance tasks
Back door	000508E2C227AD98	
Wandleser 1	000565F246DF929A	

Public holidays:
8 public holidays this year
7 public holidays in 2018
Time zones:
Default time zone is Europe/Vienna, UTC +02:00

Figure 23: Credit

- The screen shows an overview of your current credit and any previous top ups.
- Click the ***Add credit*** ❶ button.



Credit

Quantity of credits
37 KeyCredit(s)

Time credit
None

Credit protocol

Date, time	Administrator (User ID)	Credit code	Details
30/05/2017 15:56	John Smith (13968155)	2JJL-9GGX-QS85-85YV-BZ5Q	Credit added: 100 KeyCredit(s) added, new credit: 102 KeyCredit(s)
19/10/2016 10:17	John Smith (13968155)	JHWV-6SHY-LG33-QNDP-7TV6	Credit added: 10 KeyCredit(s) added, new credit: 10 KeyCredit(s)

Show 1 to 2 of 3 entries

Figure 24: Add credit

- Enter the code you uncovered by scratching the KeyCredit-Card in the "Add credit" application window.

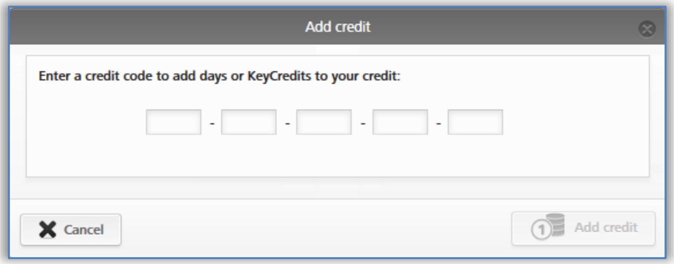
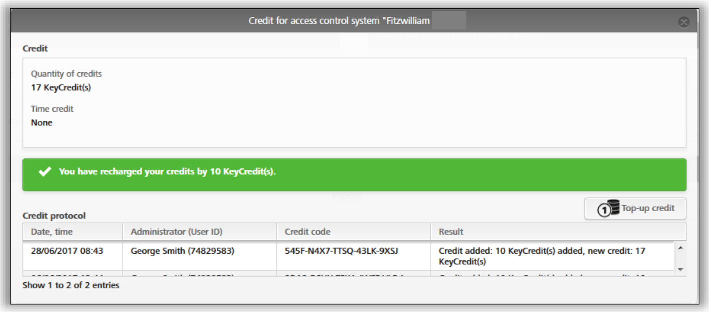

Add credit
Enter a credit code to add days or KeyCredits to your credit:
- - - -
Cancel
Add credit

Figure 25: Entering credit codes

- Click ***Add credit***.

If you entered the code correctly, the system confirms your input and adds the credit.



Credit for access control system "Fitzwilliam [redacted]

Credit

Quantity of credits
17 KeyCredit(s)

Time credit
None

✓ You have recharged your credits by 10 KeyCredit(s).

Credit protocol

Date, time	Administrator (User ID)	Credit code	Result
28/06/2017 08:43	George Smith (74829583)	545F-N4X7-TTSQ-43LK-9XSJ	Credit added: 10 KeyCredit(s) added, new credit: 17 KeyCredit(s)

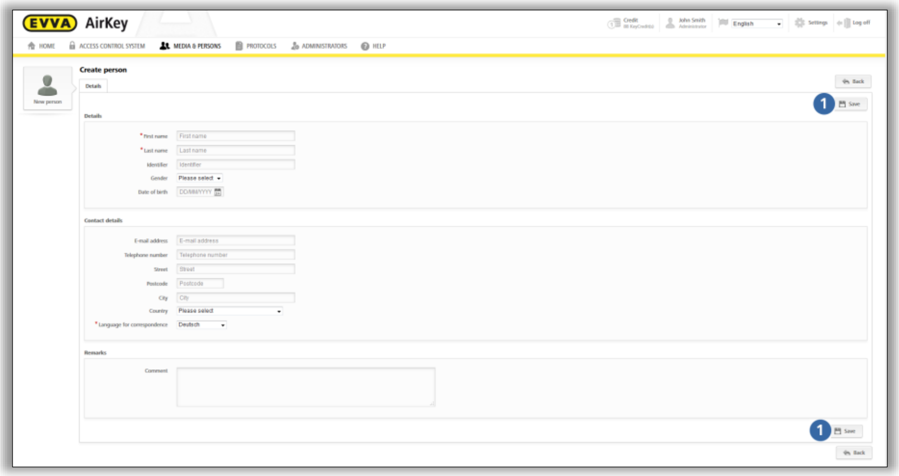
Show 1 to 2 of 2 entries

Figure 26: Add credit

4.7 Creating persons

Each person designated to be granted authorisation to the access control system must be created beforehand.

- On the ***Home*** screen, in the grey bar of the ***Media & persons*** section, click ***Add*** → ***Create person***.
- Alternatively, go to the ***Home*** screen and select the ***Persons*** → ***Create person*** tile.
- You can also select ***Media & persons*** → ***Create person*** in the main menu.
- Or select the **"*Send a Key*"** button and click ***Create new***. This function allows creating persons using smartphones.
- Complete the fields in the form. Fields highlighted by * are mandatory fields.
- Click ***Save*** ❶.



Create person

Details

*First name	First name
*Last name	Last name
Identifier	Identifier
Gender	Please select
Date of birth	DD/MM/YYYY

Contact details

E-mail address	E-mail address
Telephone number	Telephone number
Street	Street
Postcode	Postcode
City	City
Country	Please select
*Language for correspondence	Deutsch

Remarks

Comment

Figure 27: Creating persons

The first name / last name / ID fields result in a unique combination within the access control system.

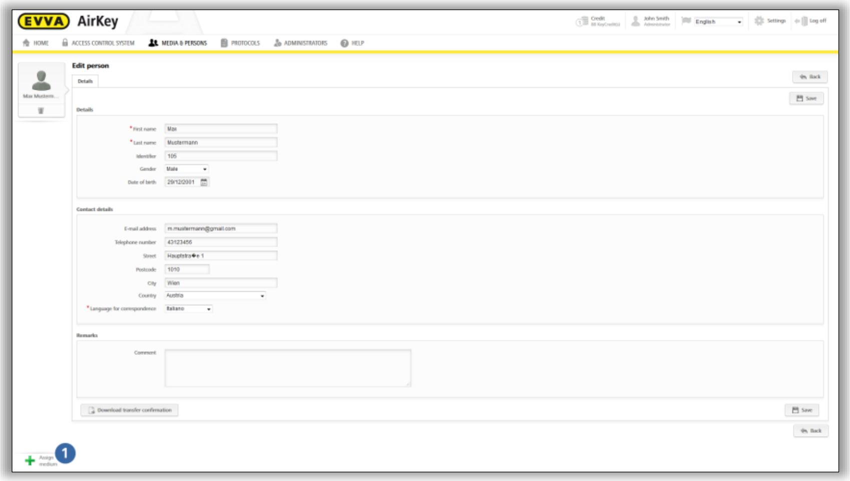
If you additionally use the "ID" field, enter a value that ensures the combination of first name and last name is unique (e.g. the staff number). This makes sense (most of all) in situations where there are persons with the same first and last names.

The characters in the "First name", "Last name", "E-mail address", "Telephone number", "Streen", and "City" fields are restricted to a maximum of 50. A maximum of 10 characters can be used for the "Postal code" field. The character limit for texts in the "Comment" field is 500 characters.

If the combination you entered already exists, the system will report "Person already exists".

- Check or correct your input.
- Click ***Save***.

Once you have successfully created a person, the system shows a confirmation and a new button appears below the name, ***Assign medium*** ❶.



Edit person

Details

*First name: Max
*Last name: Mustermann
Identifier: 105
Gender: Male
Date of birth: 29/12/2001

Contact details

E-mail address: m.mustermann@gmail.com
Telephone number: 43123456
Street: Hauptstra�e 1
Postcode: 1010
City: Wien
Country: Austria
*Language for correspondence: Italiano

Remarks

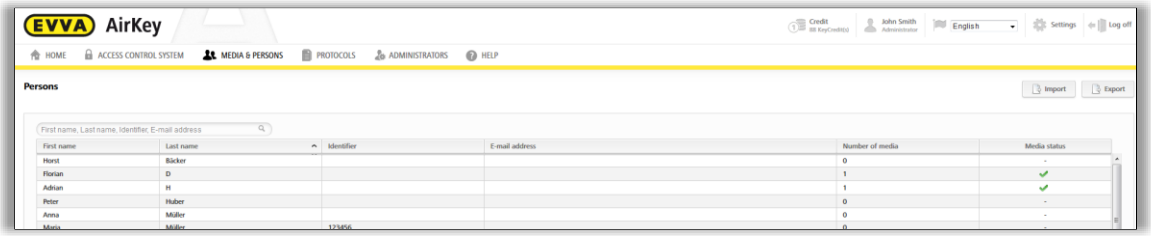
Comment:

Figure 28: Assigning media

You have now created the person in the access control system and the user appears on the person list.

4.7.1 Importing personal data

You can also create persons for AirKey in external files. For this purpose, you require a corresponding CSV file to import into the AirKey Online Administration.

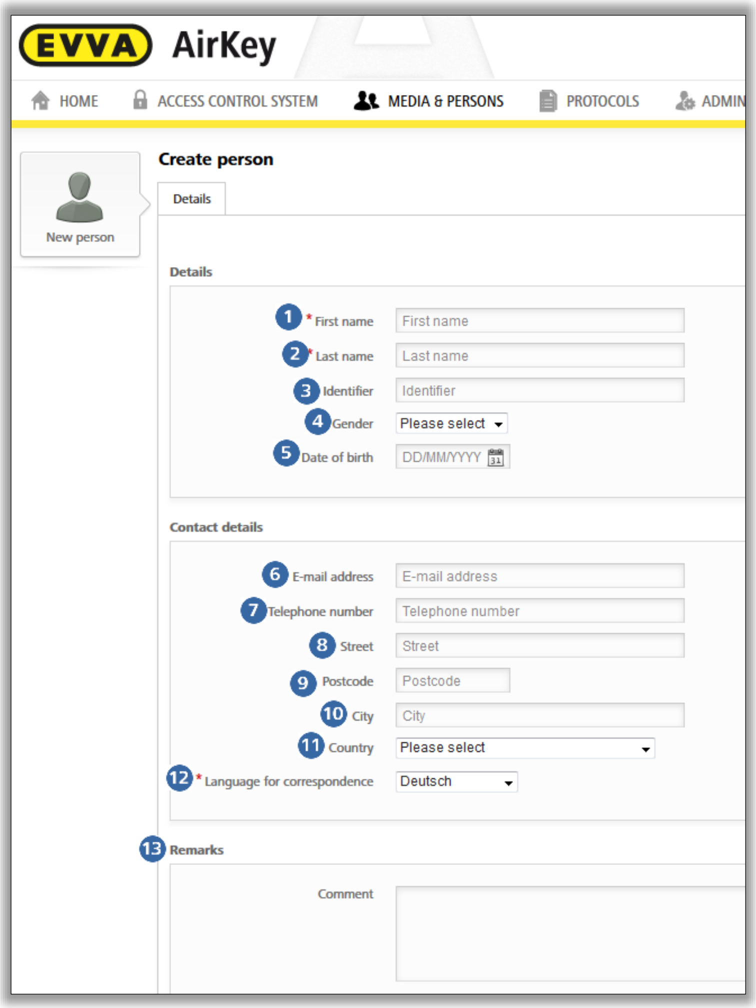


Persons

First name	Last name	Identifier	E-mail address	Number of media	Media status
Horst	Bäcker			0	-
Florian	D			1	✓
Adrian	H			1	✓
Peter	Huber			0	-
Anna	Müller			0	-
Maria	Müller	123456		0	-

Figure 29: Importing person lists

The parameters of the personal data table are identical to the ***Creating persons*** section in the AirKey Online Administration i.e., column A is the first name ❶, column B is the last name ❷, column C is the ID ❸, etc. The CSV file is imported into the AirKey Online Administration in this sequence.



Create person

Details

❶ * First name: First name
❷ * Last name: Last name
❸ Identifier: Identifier
❹ Gender: Please select
❺ Date of birth: DD/MM/YYYY

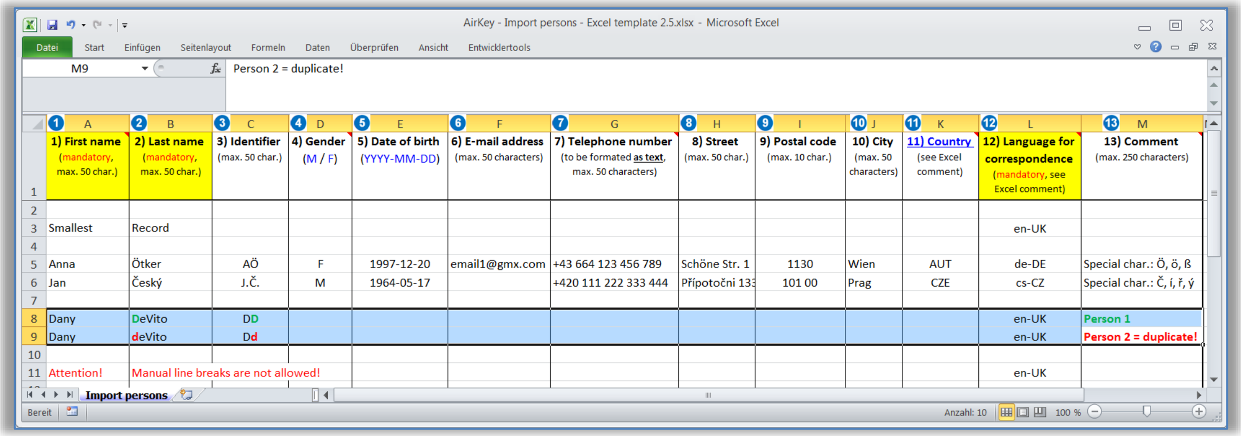
Contact details

❻ E-mail address: E-mail address
❼ Telephone number: Telephone number
❽ Street: Street
❾ Postcode: Postcode
❿ City: City
⓫ Country: Please select
⓬ * Language for correspondence: Deutsch

⓭ **Remarks**

Comment:

Figure 30: Importing persons – persons list



M9 | Person 2 = duplicate!

	❶ A	❷ B	❸ C	❹ D	❺ E	❻ F	❼ G	❽ H	❾ I	❿ J	⓫ K	⓬ L	⓭ M
1	**1) First name** (mandatory, max. 50 char.)	**2) Last name** (mandatory, max. 50 char.)	**3) Identifier** (max. 50 char.)	**4) Gender** (M / F)	**5) Date of birth** (YYYY-MM-DD)	**6) E-mail address** (max. 50 characters)	**7) Telephone number** (to be formated as text, max. 50 characters)	**8) Street** (max. 50 char.)	**9) Postal code** (max. 10 char.)	**10) City** (max. 50 characters)	**11) Country** (see Excel comment)	**12) Language for correspondence** (mandatory, see Excel comment)	**13) Comment** (max. 250 characters)
2													
3	Smallest	Record										en-UK	
4													
5	Anna	Ötker	AÖ	F	1997-12-20	email1@gmx.com	+43 664 123 456 789	Schöne Str. 1	1130	Wien	AUT	de-DE	Special char.: Ö, ö, ß
6	Jan	Český	J.Č.	M	1964-05-17		+420 111 222 333 444	Připotočni 133	101 00	Prag	CZE	cs-CZ	Special char.: Č, í, ř, ý
7													
8	Dany	DeVito	DD									en-UK	**Person 1**
9	Dany	deVito	Dd									en-UK	**Person 2 = duplicate!**
10													
11	Attention!	Manual line breaks are not allowed!										en-UK	

Figure 31: Importing persons – fields on the persons list

CSV file properties with personal data for import:

- The first row is always ignored. For this reason, we recommend you enter the field names in this row to make identification of the remaining data easier. You can also leave the first row empty. However, it must not contain personal data because that would then not be imported.
- Empty rows or rows featuring spaces and tab stops (blanks) only are also ignored. Consequently, you can leave any number of blanks if you would like to add more transparency to your CSV file.
- Each file must feature all 13 fields (attributes) shown in Figure 30.
- Fields are each separated by a semicolon.
- There are a mere three mandatory fields: first name (field 1), last name (field 2) and language for correspondence (field 12).
- If the remaining fields do not feature data, they must still be available as empty fields (;;).
- The gender (field 4) must exclusively contain **M** (for *male*) or **F** (for *female*) or be left empty. This applies to all languages and M and F must be used in capital letters only.
- Enter the date of birth (field 5) in **YYYY-MM-DD** format (e.g. 1997-12-20).
- The e-mail address (field 6) must contain the **@** character including other characters or be empty.
- The country for the address (field 10) must contain the 3-digit ISO 3166-1 code (ALPHA-3 column) of the corresponding country or be left empty. Enter the code in capitals only. Examples: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL, etc.
- The field to specify the language for correspondence (field 12) is a mandatory field and must feature the ISO code for the language. Keep to the exact spelling with upper/lower-case letters. Only the following codes are accepted: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- A person to be imported is shown as a person that is already available (⚠ icon) if the first name + last name + ID (fields 1-3) combination already exists in the AirKey Online Administration, even if the remaining fields (fields 4-13) are different. These persons are not imported. Please note that the names are case insensitive (e.g. "Danny;**D**eVito;D**D**" and "Danny;**d**eVito;D**d**" are considered the same person and only the first person will be imported).
- Persons are interpreted as duplicates within the CSV file if the combination of first name + last name + ID (fields 1-3) already exists once, even if the remaining fields (fields 4-13) are different. In this case, merely the first row is shown with a certain combination before it is imported. Any further duplicates are ignored and not shown in the table of persons to be imported.
- A CSV file may contain the data of max. 10,000 persons. If you want to import more persons, create several CSV files that you can import separately.
- Faulty rows in the CSV file are highlighted by the ✖ icon and added to the tool tip that describes all errors prior to import. These rows are not imported.

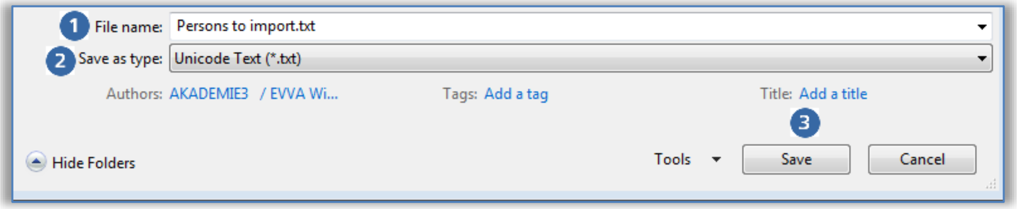
- All correct rows are highlighted by the ✓ icon before they are imported, regardless of any potentially faulty rows.

The character encoding of the CSV file must be UTF-8 so that language-specific letters (Ä, ß, ç, Ñ, č, etc.) are displayed correctly. The process to create a CSV file in UTF-8 format is explained in detail further down.

Creating a CSV file in UTF-8 format

The following description refers to Windows 10™ using Microsoft Excel™ auxiliary programs that are already available in Windows 10™. The process to create CSV files in UTF-8 format is similar for other Windows versions or operating systems. Required steps:

- An Excel file featuring the data of persons you would like to import is assumed as the initial basis for this description.
- Make sure that the seventh column (Telephone number) has been formatted as text in the Excel sheet. If this column were formatted as digits, leading characters, such as "+" and "0" (zero) would be lost during the conversion. However, spaces within the telephone number are permitted as they boost the legibility in the AirKey Online Administration.
- Use the Excel search function to verify the sheet does not contain the following characters:
    - " (double, straight quotation marks)
    - ; (semicolon = separator in the CSV file for importing to AirKey Online Administration)
- Excel is unable to directly save the data in UTF-8 format. Consequently, it is possible to initially save it in Unicode format.
- For this purpose, open the ***File*** → ***Save as*** menu item in Excel (or press the F12 key).
- Enter the desired file name in the following "Save as" dialogue window ❶.
- In the ***File type*** ❷ drop-down menu select ***Unicode Text (*.txt)*** format.
- Click ***Save*** ❸.



1 File name: Persons to import.txt

2 Save as type: Unicode Text (*.txt)

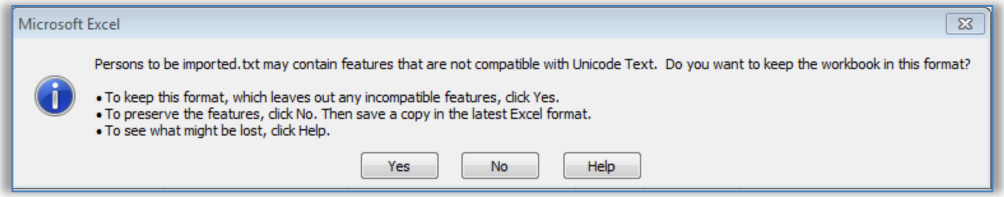
Authors: AKADEMIE3 / EVVA Wi...

Tags: Add a tag

Title: Add a title

Figure 32: Excel – Save as – "Unicode Text (*.txt)"

- Then confirm the subsequent Excel prompt referring to "Unicode Text" with ***Yes***.



Microsoft Excel

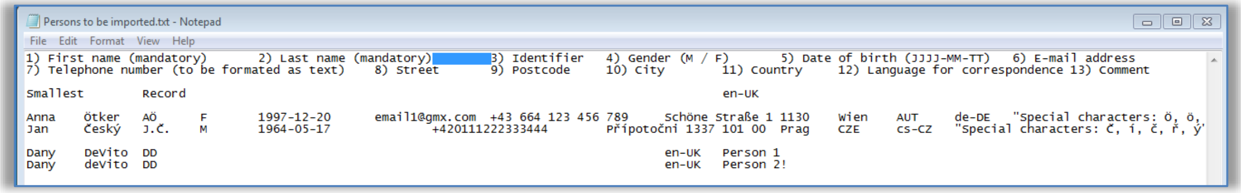
Persons to be imported.txt may contain features that are not compatible with Unicode Text. Do you want to keep the workbook in this format?

- To keep this format, which leaves out any incompatible features, click Yes.
- To preserve the features, click No. Then save a copy in the latest Excel format.
- To see what might be lost, click Help.

Figure 33: Excel – Save as "Unicode Text (*.txt)"

> Open the file you created (*.txt) using a text editor. As standard, Windows™ uses the ***Editor*** program.

> Tab is the separator in the Unicode text file. All tabs must be replaced by semicolons (;). For this purpose, initially highlight a tab between two fields and copy it.



Persons to be imported.txt - Notepad
File Edit Format View Help

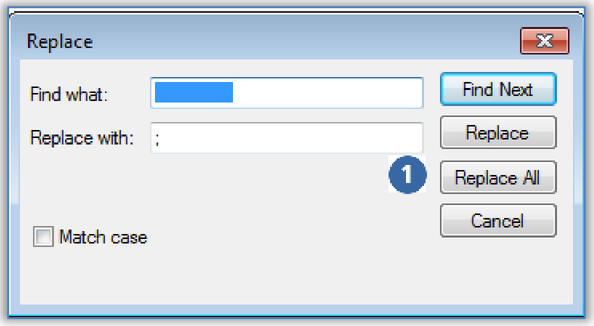
```
1) First name (mandatory)      2) Last name (mandatory)        3) Identifier    4) Gender (M / F)       5) Date of birth (JJJJ-MM-TT)    6) E-mail address
7) Telephone number (to be formated as text)     8) Street        9) Postcode      10) City         11) Country      12) Language for correspondence 13) Comment

Smallest        Record                                                                             en-UK

Anna    Ötker   AÖ      F       1997-12-20      email1@gmx.com  +43 664 123 456 789     Schöne Straße 1 1130    Wien    AUT     de-DE   "Special characters: Ö, ö,
Jan     Český   J.Č.    M       1964-05-17              +420111222333444        Přípotočni 1337 101 00  Prag    CZE     cs-CZ   "Special characters: Č, í, č, ř, ý'

Dany    DeVito  DD                                                                         en-UK   Person 1
Dany    deVito  DD                                                                         en-UK   Person 2!
```

Figure 34: Text file in "Editor" – highlight a tab and copy it to clipboard

> Confirm the subsequent Excel question regarding "Unicode Text" with ***Yes***.

> In ***Editor*** open the ***Edit*** → ***Replace*** menu item to open the "Replace" dialogue window.

- Insert the tab character from the clipboard in the ***Search*** field because it is not possible to directly input it here.
- Enter a semicolon (;) in the ***Replace*** field.
- Click ***Replace all*** ❶.



Replace

Find what:

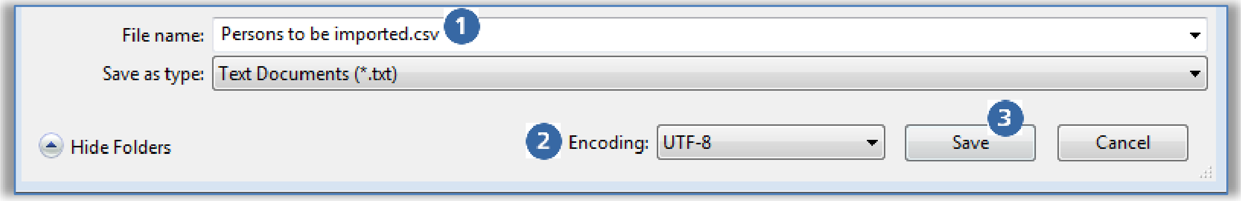
Replace with: ;

□ Match case

Figure 35: "Editor" – replacing all tabs with semicolons

> Close the "Replace" dialogue window and in ***Editor*** open the ***Edit*** → ***Save as*** menu item to open the "Save as" dialogue window.

- Manually change the file suffix from .txt to .csv in the ***File name*** ❶ field. It will be more complicated to rename the file suffix at a later stage!
- In the drop-down list select ***Encoding*** ❷ and ***UTF-8*** format.
- Click ***Save*** ❸.



File name: Persons to be imported.csv 1

Save as type: Text Documents (*.txt)

2 Encoding: UTF-8

Figure 36: "Editor" – Save as – Manually enter .csv file suffix and select UTF-8 encoding

- This process creates a CSV file that can then be imported to AirKey Online Administration.

You can directly open the CSV file using Excel. Do NOT make any changes to the CSV file in Excel as the file would then not be saved in UTF-8 format!

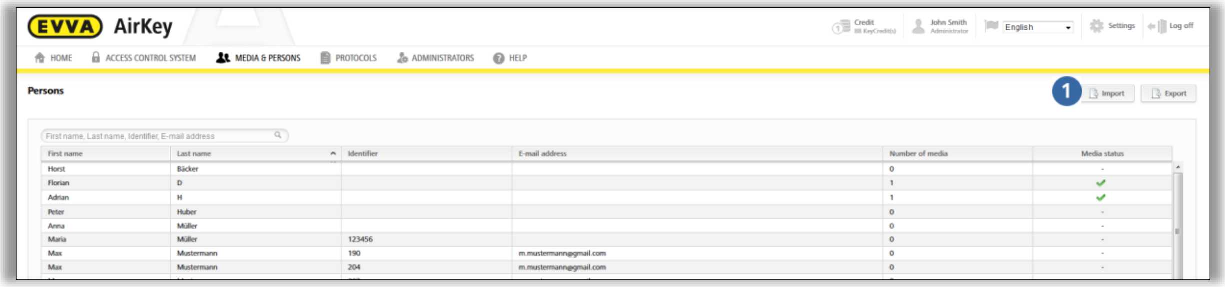
For instance, open the file in the ***Editor*** and subsequently save it there after having executed any minor, retrospective changes to the personal data.

If there are comprehensive changes to the personal data we recommend to make these in the original Excel file before repeating the entire process to create a CSV file in UTF-8 format.

Importing the CSV file to the AirKey Online Administration in UTF-8 format

Proceed as follows to import a CSV file with personal data:

- On the ***Home*** screen, select the ***Persons*** tile.
- Alternatively select ***Media & persons*** → ***Persons*** in the main menu.
- Click ***Import*** ❶ on the right.

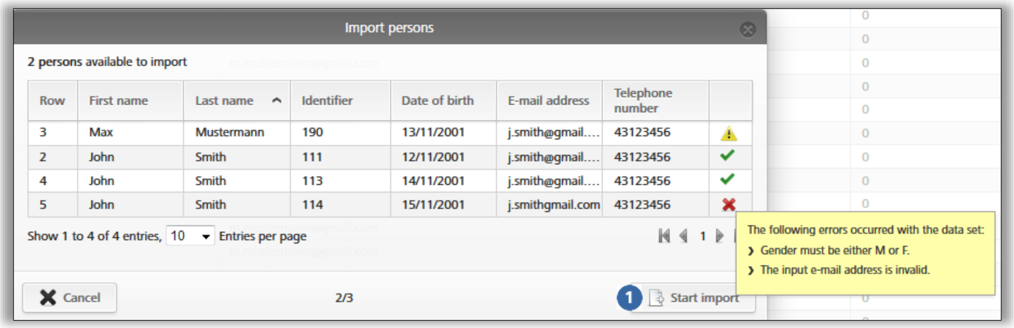


Persons

First name	Last name	Identifier	E-mail address	Number of media	Media status
Horst	Bäcker			0	-
Florian	D			1	✓
Adrian	H			1	✓
Peter	Huber			0	-
Anna	Müller			0	-
Maria	Müller	123456		0	-
Max	Mustermann	190	m.mustermann@gmail.com	0	-
Max	Mustermann	204	m.mustermann@gmail.com	0	-

Figure 37: Importing persons

- Click ***Select file***.
- Select the corresponding CSV file you would like to import.
- You are provided with an overview of the persons to import.
- Click ***Start import*** ❶.



Import persons

2 persons available to import

Row	First name	Last name	Identifier	Date of birth	E-mail address	Telephone number	
3	Max	Mustermann	190	13/11/2001	j.smith@gmail.…	43123456	⚠
2	John	Smith	111	12/11/2001	j.smith@gmail.…	43123456	✓
4	John	Smith	113	14/11/2001	j.smith@gmail.…	43123456	✓
5	John	Smith	114	15/11/2001	j.smithgmail.com	43123456	✗

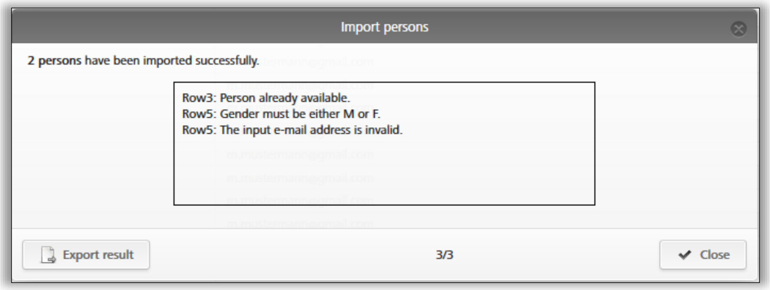
Show 1 to 4 of 4 entries, 10 Entries per page

The following errors occurred with the data set:

- Gender must be either M or F.
- The input e-mail address is invalid.

Figure 38: Importing persons

- A report is output listing the number of successfully imported persons and faulty rows.
- Click ***Close***.



Import persons

2 persons have been imported successfully.

Row3: Person already available.
Row5: Gender must be either M or F.
Row5: The input e-mail address is invalid.

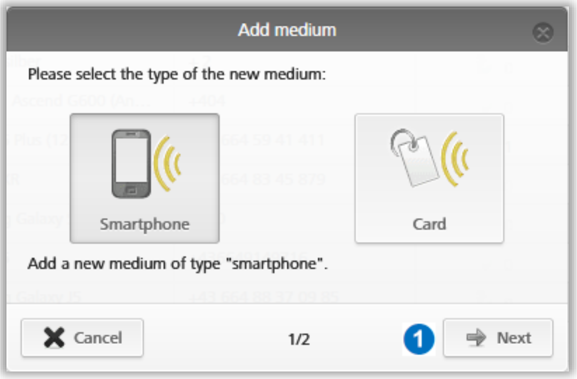
Figure 39: Importing persons – result

- The AirKey Online Administration automatically forwards you to the overview list of persons.
- Assign the desired access authorisations to the corresponding persons individually using the familiar process described in Assigning media to persons. Consequently, identical access authorisations can be quickly and easily duplicated. Please refer to Duplicating media for more information.

4.8 Creating smartphones

You must create or add smartphones to your access control system before you can manage them as part of your access control system.

- On the ***Home*** screen, in the grey bar of the ***Media and persons*** section, click ***Add*** → ***Add medium***.
- Alternatively, on the ***Home*** screen, select the ***Smartphones*** → ***Add medium*** tile.
- You can also select ***Media & persons*** → ***Add medium*** in the main menu.



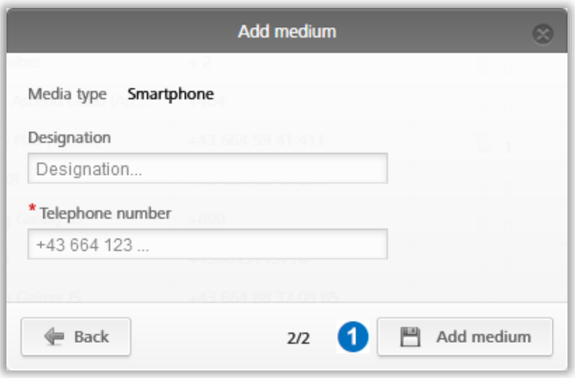
Add medium

Please select the type of the new medium:

Add a new medium of type "smartphone".

Figure 40: New smartphone or card media

- Select ***Smartphone*** as the new medium and click ***Next*** ❶.
- Enter unique information (e.g. smartphone type) in the "Designation" field.
- Enter the phone number of the smartphone. The phone number must begin with **+** and country code, and may contain a maximum of 50 characters (+, 0-9, and spaces).
- Click ***Add medium*** ❶.



Add medium

Media type Smartphone

Designation

Designation...

* Telephone number

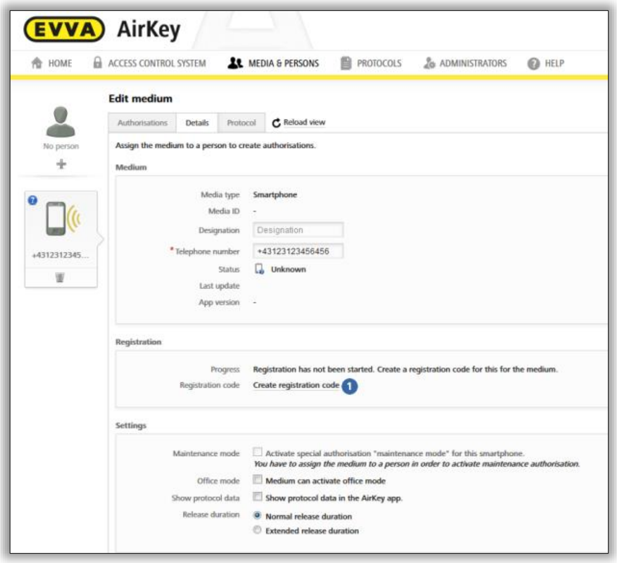
+43 664 123 ...

Figure 41: Adding new media

An error message will appear if the telephone number is invalid or the telephone number has already been created.

Now you are in the details section of this smartphones.

- Click ***Create registration code*** ❶ if you have not yet created a registration code.



Edit medium

Assign the medium to a person to create authorisations.

Medium

Media type	Smartphone
Media ID	-
Designation	Designation
* Telephone number	+43123123456456
Status	Unknown
Last update	
App version	-

Registration

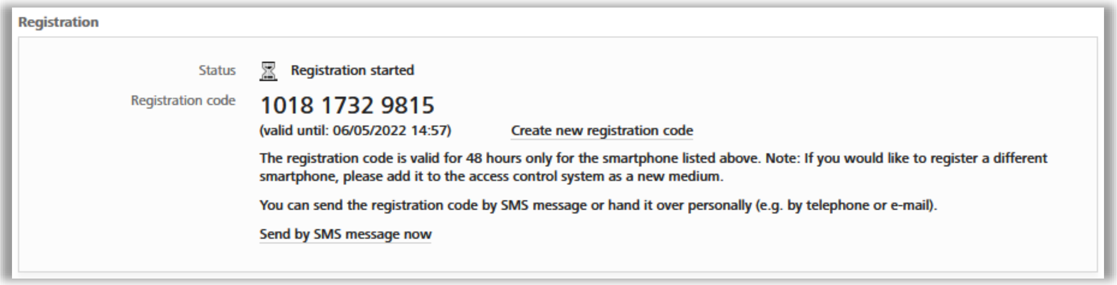
Progress	Registration has not been started. Create a registration code for this for the medium.
Registration code	Create registration code

Settings

Maintenance mode	□ Activate special authorisation "maintenance mode" for this smartphone. *You have to assign the medium to a person in order to activate maintenance authorisation.*
Office mode	□ Medium can activate office mode
Show protocol data	□ Show protocol data in the AirKey app.
Release duration	● Normal release duration ○ Extended release duration

Figure 42: Creating registration codes

The ***Registration*** section shows a valid registration code and its expiry date. You can also send it by text message (SMS). For this purpose, you must merely click the corresponding link. Then the exact date and time appears when the registration code was sent by text message (SMS).

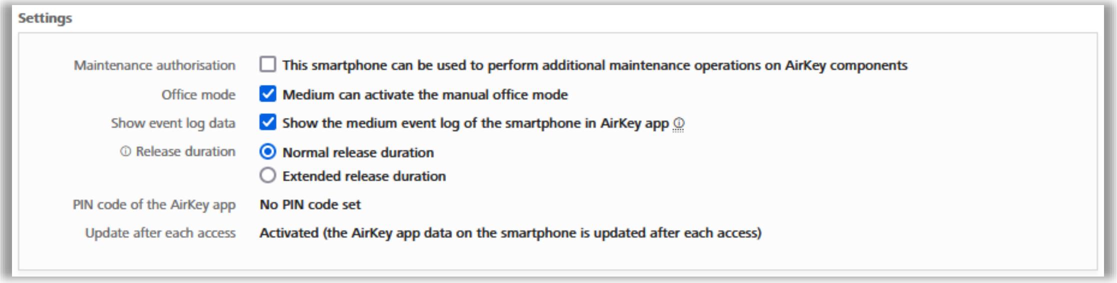


Registration

Status	Registration started
Registration code	1018 1732 9815 (valid until: 06/05/2022 14:57) Create new registration code The registration code is valid for 48 hours only for the smartphone listed above. Note: If you would like to register a different smartphone, please add it to the access control system as a new medium. You can send the registration code by SMS message or hand it over personally (e.g. by telephone or e-mail). Send by SMS message now

Figure 43: Registration code

Specify the following parameters in the ***Settings*** section in the smartphone's details section:



Settings

Maintenance authorisation	□ This smartphone can be used to perform additional maintenance operations on AirKey components
Office mode	☑ Medium can activate the manual office mode
Show event log data	☑ Show the medium event log of the smartphone in AirKey app ⓘ
ⓘ Release duration	● Normal release duration ○ Extended release duration
PIN code of the AirKey app	No PIN code set
Update after each access	Activated (the AirKey app data on the smartphone is updated after each access)

Figure 44: Editing media – settings

> **Maintenance authorisation:** This special authorisation can exclusively be activated on smartphones that have already been assigned to a person. Smartphones with this function are granted to unlock locking components in factory state and add or delete media as well as locking components to access control systems. The maintenance

authorisation additionally allows updates of the locking component firmware and of the media Keyring.

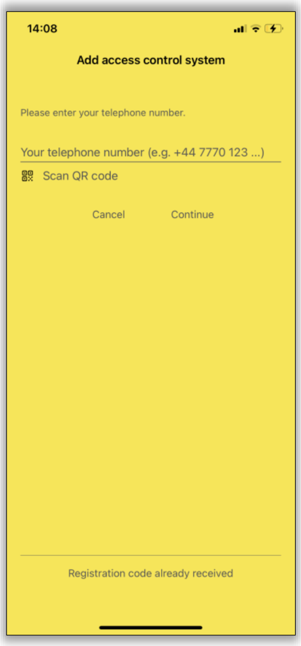
- **This medium can activate the manual office mode:** select this option and the access medium can set the automatic office mode status at the locking component. However, the medium must have been assigned a valid authorisation for the corresponding locking components.
- **Show the medium event log of the smartphone in AirKey app:** This option shows persons their own access events and any other event log data relevant to the media in the AirKey app.
- **Release duration:** Specifies how long the locking component is unlocked when using this smartphone. The length of the normal or enhanced release duration is specified in the locking components (from 1-250 seconds).
- **PIN code of the AirKey app:** Shows the status of whether PIN code protection is on or off in the AirKey app of this smartphone. If it is active and the person has forgotten their PIN code, you can reset it here.
- **Update after each access:** Specifies the status whether the AirKey app data of this smartphone is automatically updated after each access process. Details about the activation of this function can be found in the chapter General.

4.9 Registering smartphones

You can register smartphones once you have created them in the access control system and you know the registration code.

- Start the AirKey app on your smartphone.
- Accept the license agreement and any queries about access to certain services of the smartphone.
- If the smartphone has not been connected to an access control system, the dialogue for entering the registration code is displayed automatically.

For iOS smartphones, tap ***Registration code already received*** to skip entering the phone number and go to entering the registration code.



14:08

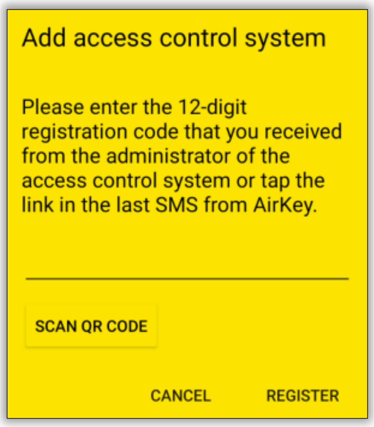
Add access control system

Please enter your telephone number.

Your telephone number (e.g. +44 7770 123 ...)

Figure 45: AirKey app – adding an access control system (iOS)

> Enter the registration code you received from the access control system administrator.



Add access control system

Please enter the 12-digit registration code that you received from the administrator of the access control system or tap the link in the last SMS from AirKey.

Figure 46: AirKey app – adding access control systems (Android)

> Tap ***Register*** to confirm.

You can also register a single smartphone in several access control systems. Select ***Settings*** → ***Add access control system*** in the AirKey app main menu to re-open the registration dialogue. Please refer to Using smartphones in several systems for more information.

An error message appears if the registration code is invalid or has expired. In this event, please contact the access control system administrator from whom you received the registration code.

The ***Scan QR code*** button is only required in conjunction with a smartphone replacement. Details about the smartphone replacement can be found in the chapter Smartphone replacement.

If users delete the AirKey app or app data, there is the option to once again assign authorisations that had already been granted to the smartphone without using additional credits. However, this exclusively applies to the same device and your access control system. This option does not apply to a different device. Details about the simple device replacement can be found in the chapter Smartphone replacement.

- On the ***Home*** screen select the ***Smartphones*** tile.
- You can also select ***Media & persons*** → ***Media*** in (the upper left corner of) the header.
- Select the affected smartphone from the overview list.
- Click ***Create new registration code*** and send the registration code to the person wanting to register a smartphone to the access control system.
- Enter the registration code in the AirKey app and the smartphone is registered to the access control system.

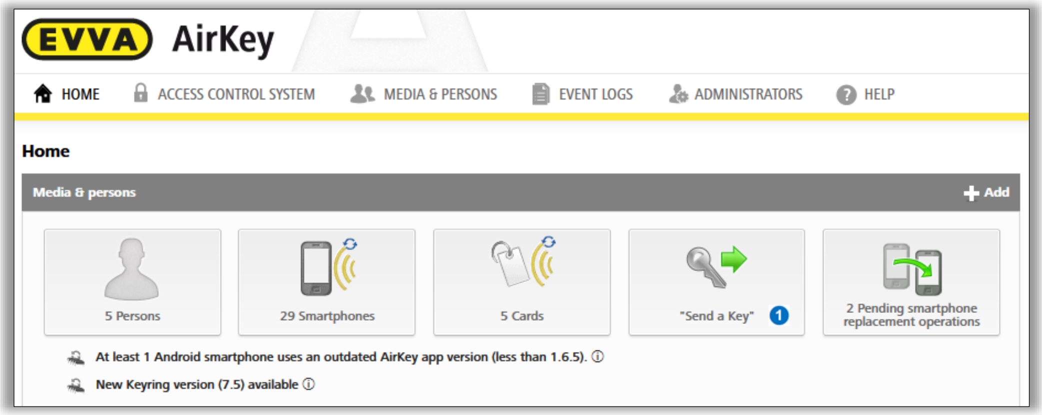
If your smartphone had previously been registered to an access control system and it had not been correctly removed from this system when the app data was deleted and you then register your smartphone to a different access control system, a message appears indicating the smartphone had already been registered to an access control system. You can register the smartphone as usual if you ignore the message. The smartphone is created as a new medium and any previous data is rendered unusable.

EVVA recommends assigning a PIN code. It serves as an additional level of security. You can subsequently activate or deactivate the PIN code protection. Please refer to Activating PIN code for more information.

4.9.1 "Send a Key" function

To all persons owning a smartphone you can also send "keys" using the "Send a Key" function. This function is useful to administrators and saves smartphone owners from manually entering the registration code for a new access control system.

- Click the "***Send a Key***" button.

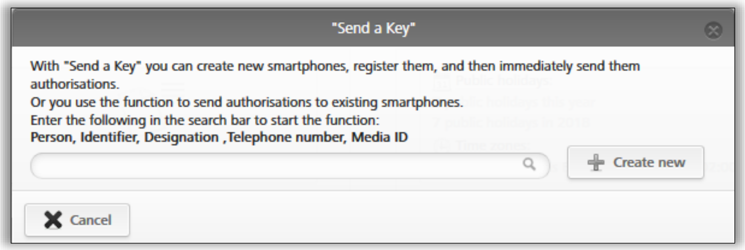


At least 1 Android smartphone uses an outdated AirKey app version (less than 1.6.5). ⓘ

New Keyring version (7.5) available ⓘ

Figure 47: "Send a Key"

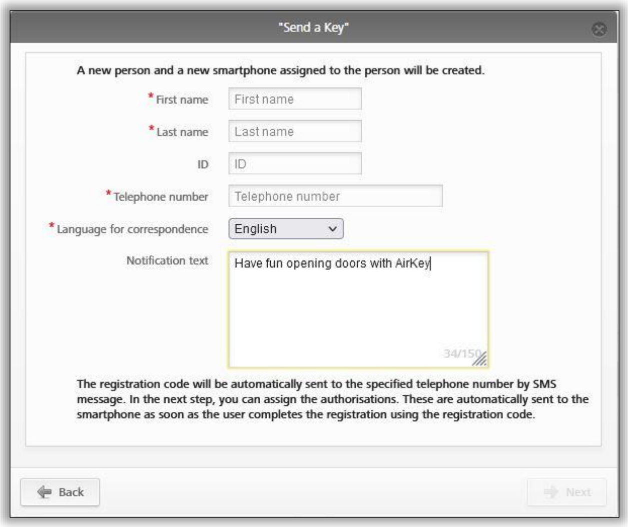
> Enter a person's name, code, etc. in the search field. If you are aware of the fact the user has not yet been created, select ***Create new***.



With "Send a Key" you can create new smartphones, register them, and then immediately send them authorisations.
Or you use the function to send authorisations to existing smartphones.
Enter the following in the search bar to start the function:
Person, Identifier, Designation ,Telephone number, Media ID

Figure 48: "Send a Key" – search field

> Click ***Continue*** once you have completed all mandatory fields. A text message is immediately sent to the corresponding user containing a link to the AirKey app to register for an access control system. If you have selected an own text for the "Send a Key" SMS in the general settings, you can also adjust or personalise the text of the SMS here. (Details about the general settings can be found in chapter General.)



A new person and a new smartphone assigned to the person will be created.

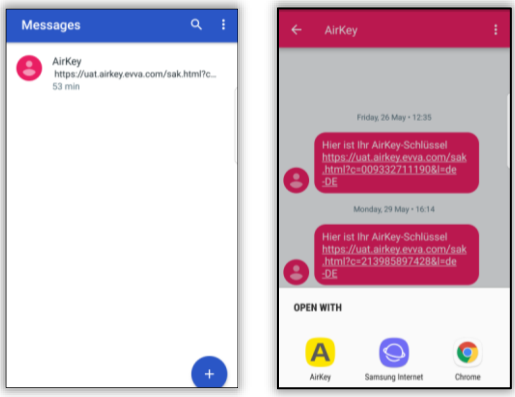
* First name	First name
* Last name	Last name
ID	ID
* Telephone number	Telephone number
* Language for correspondence	English
Notification text	Have fun opening doors with AirKey 34/150

The registration code will be automatically sent to the specified telephone number by SMS message. In the next step, you can assign the authorisations. These are automatically sent to the smartphone as soon as the user completes the registration using the registration code.

Figure 49: "Send a Key" – creating persons

AirKey system manual version 2.7 | 06/03/2024 | Subject to technical changes and misprints

Depending on the smartphone’s network availability it may take some time until it receives the Registration code text message (SMS).



AirKey
https://uat.airkey.evva.com/sak.html?c...
53 min

Friday, 26 May • 12:35

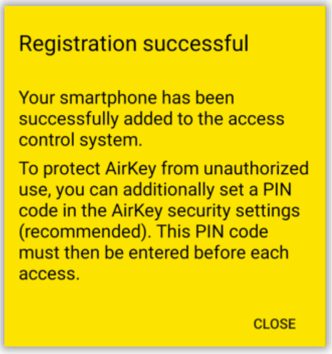
Hier ist Ihr AirKey-Schlüssel https://uat.airkey.evva.com/sak.html?c=009332711190&l=de-DE

Monday, 29 May • 16:14

Hier ist Ihr AirKey-Schlüssel https://uat.airkey.evva.com/sak.html?c=213985897428&l=de-DE

Figure 50: Text message (SMS) with link – shown here on a Samsung Galaxy S7 Edge

- After opening the link from the SMS with AirKey, the registration is automatically started and executed.



Registration successful

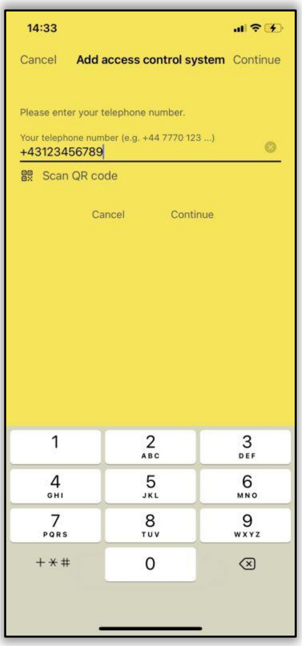
Your smartphone has been successfully added to the access control system.

To protect AirKey from unauthorized use, you can additionally set a PIN code in the AirKey security settings (recommended). This PIN code must then be entered before each access.

Figure 51: Registration successful

Proceed as follows if you have not yet installed the AirKey app on the smartphone:

- Tap the link in the text message (SMS) and install the app on the smartphone.
- Start the AirKey app.
- On Android smartphones the registration is started and executed automatically. On iOS smartphones, enter your phone number and confirm with ***Continue***. (The ***Scan QR code*** button is only required in conjunction with a smartphone replacement. Details about the smartphone replacement can be found in the chapter Smartphone replacement.)



14:33

Cancel **Add access control system** Continue

Please enter your telephone number.

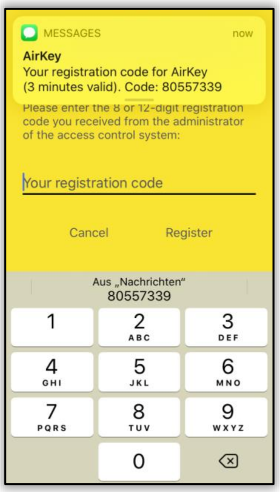
Your telephone number (e.g. +44 7770 123 ...)
+43123456789

Scan QR code

Cancel Continue

Figure 52: Enter phone number (iOS)

- You will receive another SMS. Stay in the AirKey app and select the eight-digit registration code that will be displayed above the keyboard.



MESSAGES now

AirKey
Your registration code for AirKey (3 minutes valid). Code: 80557339

Please enter the 8 or 12-digit registration code you received from the administrator of the access control system:

Your registration code

Cancel Register

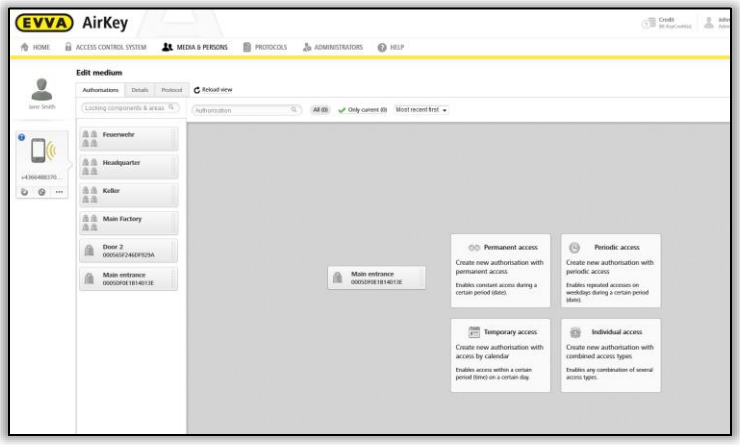
Aus „Nachrichten“
80557339

Figure 53: Registration code (iOS)

If the eight-digit registration code is not displayed as a suggestion, or you have closed the AirKey app in the meantime, you must copy the eight-digit registration code from the SMS and paste it within the AirKey app.

- Finish the registration with ***Register***.

In the AirKey Online Administration you are taken to the ***Edit medium*** authorisation view to create the desired authorisations. Drag and drop the corresponding locking component to which you would like to grant the access authorisation to the desired access type (permanent access, temporary access, periodic access, individual access) – see also Assigning authorisations.



Permanent access

Create new authorisation with permanent access

Enables constant access during a certain period (date).

Periodic access

Create new authorisation with periodic access

Enables repeated accesses on weekdays during a certain period (date).

Temporary access

Create new authorisation with access by calendar

Enables access within a certain period (time) on a certain day.

Individual access

Create new authorisation with combined access types

Enables any combination of several access types.

Figure 54: Access types

4.10 Installing locking components

4.10.1 AirKey cylinders, hybrid cylinders, lever cylinders, and padlocks

Follow the assembly manual enclosed with the packaging during assembly of the AirKey cylinder, hybrid cylinder, lever cylinder, and padlock or the online assembly video clip at https://www.evva.com/en/airkey/website/.

Make sure both sides of a double-sided AirKey cylinder have been configured within the access control system to prevent locking users in or out.

4.10.2 AirKey wall readers

Please note the assembly manual enclosed in the packaging to assemble the AirKey wall reader. Our homepage additionally provides a drilling template or the assembly video at https://www.evva.com/en/airkey/website/.

One control unit is required per wall reader. The control unit must be installed indoors, in a secure area. Check the cabling on the wall reader and control unit.

Locking components are always supplied in factory state.

- Media in factory state can unlock locking components in factory state.
- Smartphones with installed AirKey app and enabled maintenance authorisation can unlock locking components in factory state
- Unlocking attempts are not recorded in factory state.
- Locking authorisations have only been assigned after having added the locking component to a access control system.
- Observe the notes in the assembly manual during assembly. Open the

door and secure it against accidentally slamming shut during assembly and disassembly of the locking components.

4.11 Adding locking components

Add locking components to the access control system using smartphones featuring maintenance authorisation or an optionally available coding station. Locking components must be in factory state.

You must meet the following requirements to add locking components using your smartphone:

- The AirKey app has been installed.
- An active Internet connection is available.
- The smartphone has been registered within the access control system.
- The smartphone has been assigned to a person.
- The maintenance authorisation has been assigned to the smartphone.

4.11.1 Adding locking components using a smartphone

- Start the AirKey app.
- Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** ❶ icon.
- Establishing a connection using **Bluetooth** (for **Android** smartphones): open the context menu of the locking component in factory state which you would like to add to the access control system (⋮) and then select ***Connect*** ❷.
- Establishing a connection using **Bluetooth** (for **iPhones**): swipe the "In factory state" designation of the locking component in factory state which you would like to add to your access control system towards the left and then select ***Connect*** ❸.

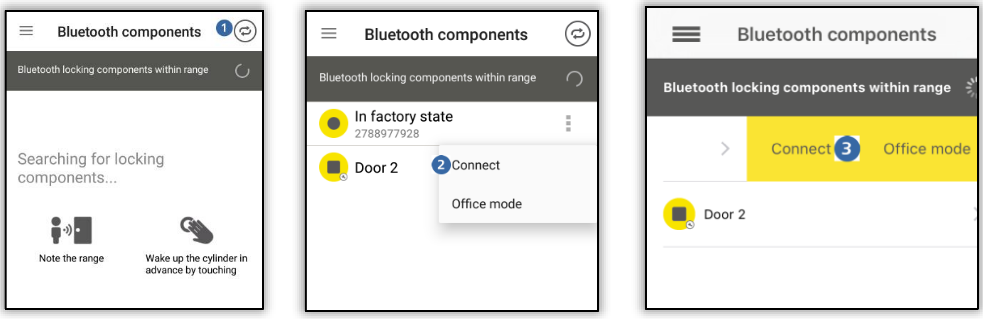
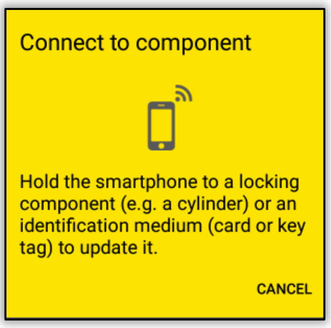

Bluetooth components
1
Bluetooth locking components within range
Searching for locking components...
Note the range
Wake up the cylinder in advance by touching
Bluetooth components
Bluetooth locking components within range
In factory state
2788977928
Door 2
2
Connect
Office mode
Bluetooth components
Bluetooth locking components within range
Connect
3
Office mode
Door 2

Figure 55: AirKey app – connecting to component (using NFC for Android smartphones / using Bluetooth for Android smartphones / using Bluetooth for iPhones)

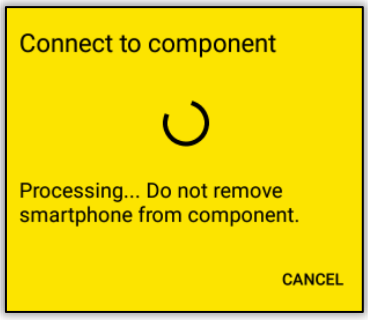


Connect to component

Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

Figure 56: AirKey app – connecting to component

- Hold the smartphone to the locking component in factory state or select the corresponding locking component from the displayed component list within range. The smartphone establishes a connection to the locking component. Do not remove the smartphone from the locking component while it is establishing the connection.

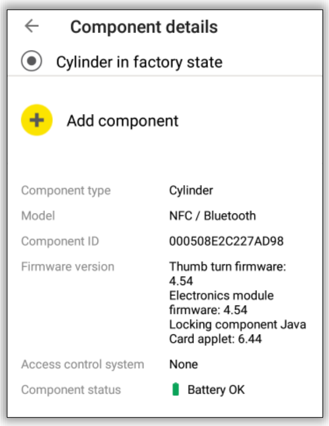


Connect to component

Processing... Do not remove smartphone from component.

Figure 57: AirKey app – connecting

- Now you see information about the locking component.



Component details

◉ Cylinder in factory state

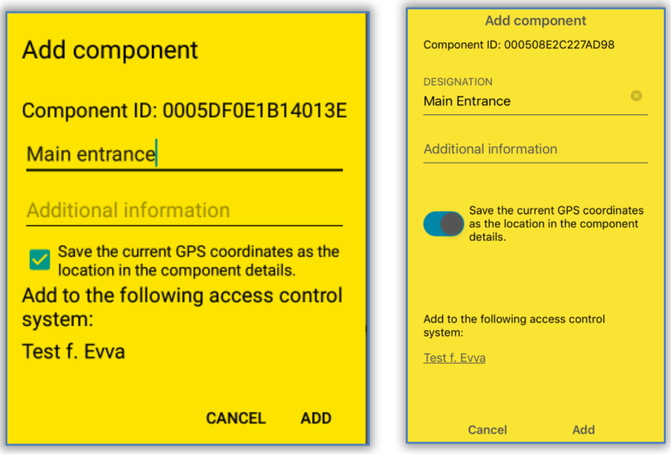
Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Access control system	None
Component status	Battery OK

Figure 58: Adding components

- Tap ***Add component***.
- Enter a unique designation for the locking component.

Make sure both sides of a double-sided cylinder have been configured within the access control system. Assign a clear designation to each of the sides on cylinders with double-sided access. Create an area that features both sides of the cylinder and assign an area authorisation to obtain the same authorisation for both sides.

> Select the access control system to which you would like to add the locking component if the smartphone with active maintenance authorisation is registered in several access control systems.



Add component

Component ID: 0005DF0E1B14013E

Main entrance

Additional information

☑ Save the current GPS coordinates as the location in the component details.

Add to the following access control system:

Test f. Evva

CANCEL ADD

Add component

Component ID: 000508E2C227AD98

DESIGNATION

Main Entrance

Additional information

Save the current GPS coordinates as the location in the component details.

Add to the following access control system:

Test f. Evva

Cancel Add

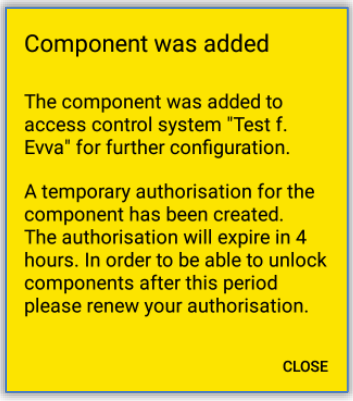
Figure 59: AirKey app – adding locking components Android/iPhone

> Tap ***Add***.

> Now once again hold the smartphone to the locking component to complete the process. Bluetooth connection will be established automatically.

The system checks the data and updates the locking component. In this process, do not remove the smartphone from the locking component.

> A confirmation prompt completes the process. The locking component is now available for management in the AirKey Online Administration.



Component was added

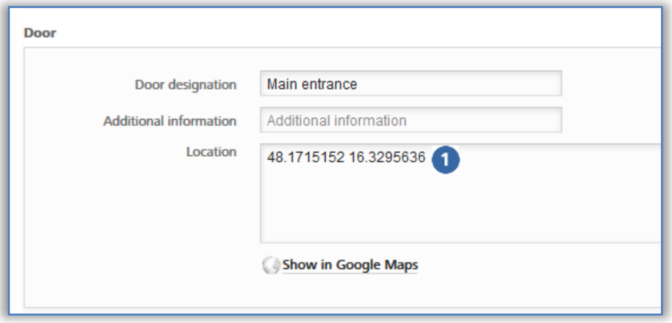
The component was added to access control system "Test f. Evva" for further configuration.

A temporary authorisation for the component has been created. The authorisation will expire in 4 hours. In order to be able to unlock components after this period please renew your authorisation.

CLOSE

Figure 60: AirKey app – locking component added

The locking component appears in the locking components overview list in the AirKey Online Administration. If the GPS coordinates ❶ were determined when the locking component was added, they are available in the locking component's section of the AirKey Online Administration in the ***Details*** tab in the "Door" section.



Door

Door designation: Main entrance

Additional information: Additional information

Location: 48.1715152 16.3295636 ❶

Figure 61: GPS coordinates in the locking component details

Alternatively enter the address in the "Location" field where the locking component is located.

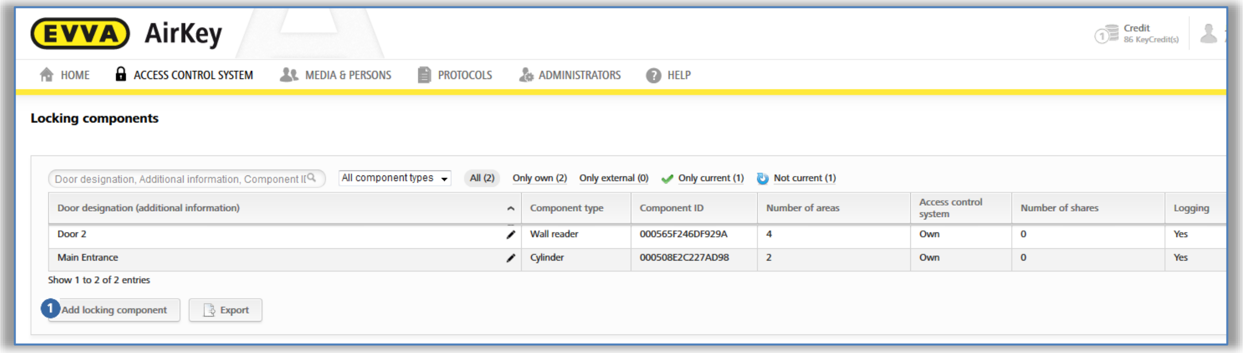
⚠ The locking component is now no longer in factory state. Media in factory state or smartphones in maintenance authorisation are consequently no longer authorised. The smartphone that added the locking component is automatically authorised for a period of four hours. Please change the corresponding authorisation or assign additional media with a valid authorisation to continue to have access to this locking component.

4.11.2 Adding locking components using coding stations

Option

Proceed as follows to add locking components using coding stations:

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.
- Click the Add locking component button ❶.
- Alternatively, select ***Access control system*** → Add locking components in the main menu.



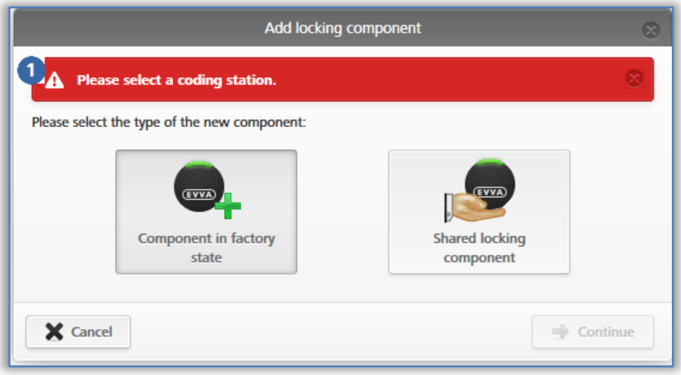
Locking components

Door designation (additional information)	Component type	Component ID	Number of areas	Access control system	Number of shares	Logging
Door 2	Wall reader	000565F246DF929A	4	Own	0	Yes
Main Entrance	Cylinder	000508E2C227AD98	2	Own	0	Yes

Show 1 to 2 of 2 entries

Figure 62: Adding locking components

- Connect the coding station to the computer otherwise the system notice appears. ❶

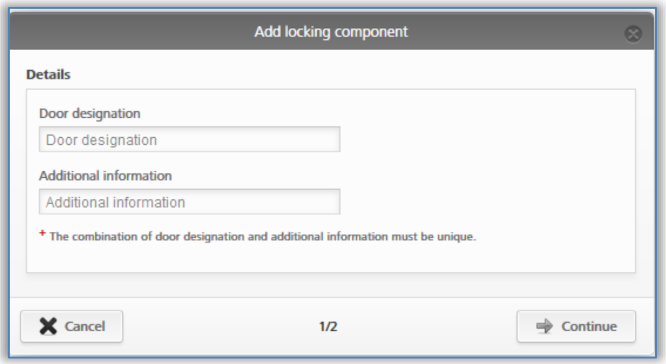

Add locking component

1 Please select a coding station.

Please select the type of the new component:

Figure 63: Adding locking components / no coding station

- Select ***Component in factory state.***
- Click ***Continue****.*
- Enter the door designation in the following dialogue window and click ***Continue****.*


Add locking component

Details

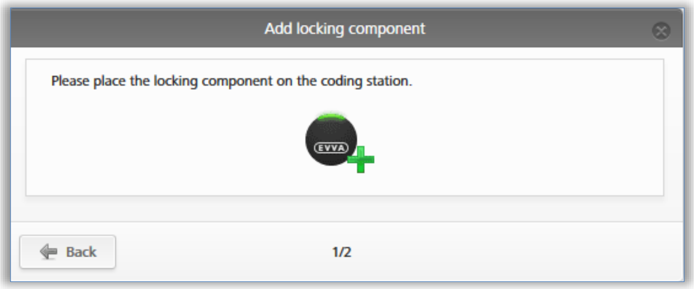
Door designation: Door designation

Additional information: Additional information

* The combination of door designation and additional information must be unique.

Figure 64: Adding locking components – assigning names

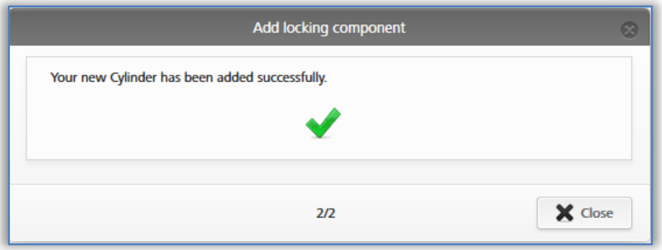
- Follow the on-screen instructions and place the locking component on the coding station.


Add locking component

Please place the locking component on the coding station.

Figure 65: Adding locking components

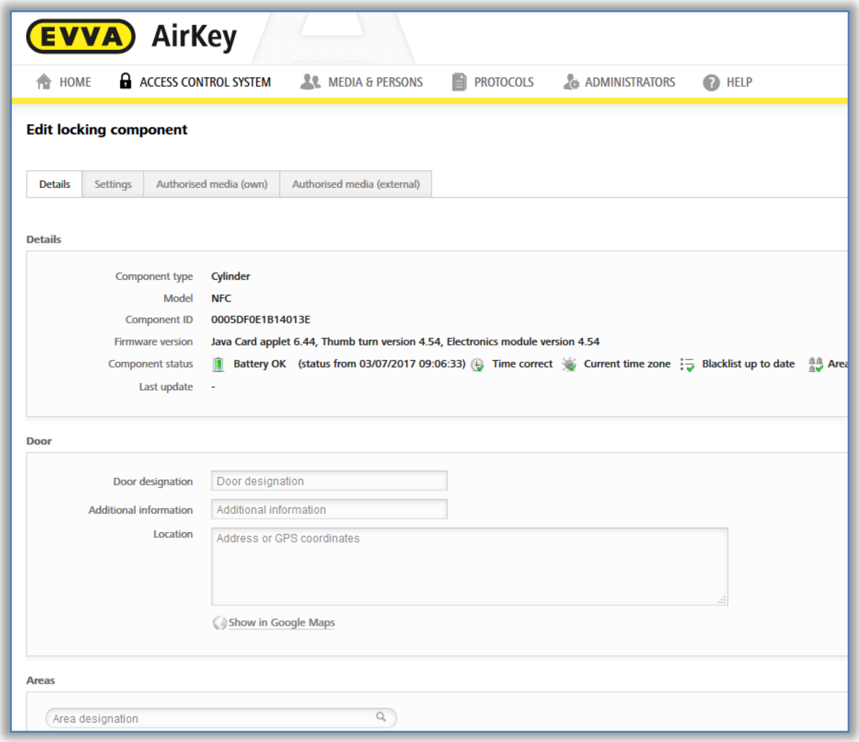
- A confirmation prompt appears and the locking component is added to the access control system.



Your new Cylinder has been added successfully.

Figure 66: Adding locking components – confirmation

After having confirmed the prompt, you are forwarded to the detailed locking component view.



Edit locking component

Details

Component type	Cylinder
Model	NFC
Component ID	0005DF0E1B14013E
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status	Battery OK (status from 03/07/2017 09:06:33) Time correct Current time zone Blacklist up to date Area
Last update	-

Door

Door designation	Door designation
Additional information	Additional information
Location	Address or GPS coordinates

Areas

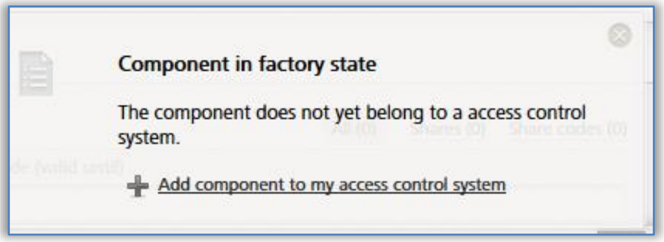
Area designation

Figure 67: Locking component details

⚠ The locking component is now no longer in factory state. Media in factory state or smartphones with maintenance authorisation are consequently no longer authorised to unlock the locking component. Add a medium or smartphone to the access control system and assign valid authorisations to said locking components to continue to be able to unlock them.

❗ The default time zone and data protection settings are automatically configured for the added locking component according to the specified settings. Refer to Default values (for all recently added locking components) for more information on these settings.

Alternatively, you can also just place a locking component in factory state on the coding station. An information window appears in the bottom right, enabling you to also add the locking component to the access control system using the ***Add component to my access control system*** link.



Component in factory state

The component does not yet belong to a access control system.

Add component to my access control system

Figure 68: Adding components to my access control system

4.12 Adding cards, key fobs, combi keys, and wristbands using a smartphone

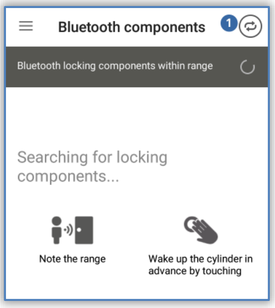
Access media in factory state are added to access control systems using smartphones with maintenance authorisation or an optionally available coding station.

> Start the AirKey app.

When using smartphones to add combi keys to the access control system you must hold the combi key side featuring the RFID icon to the smartphone. Most models require the combi key to be held directly on the smartphone.

This action is available using an Android smartphone that is compatible with NFC. Please refer to the Encoding media section for details on adding media using Bluetooth with an Android smartphone or an iPhone.

> Tap the ***Connect to component*** ❶ icon.



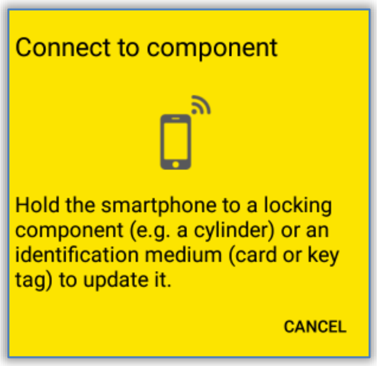
Bluetooth components

Bluetooth locking components within range

Searching for locking components...

Figure 69: AirKey app – connecting to component

> Hold the smartphone to the medium in factory state.
A connection to the medium will be established.

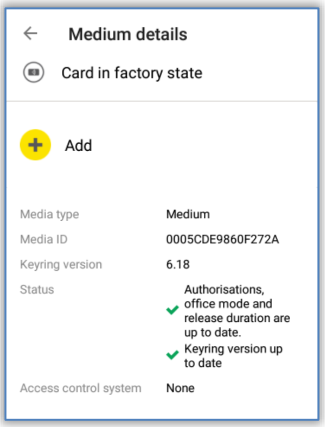


Connect to component

Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

Figure 70: AirKey app – connecting

- Do not remove the medium from the smartphone while it is establishing the connection. Now you see information about the medium.



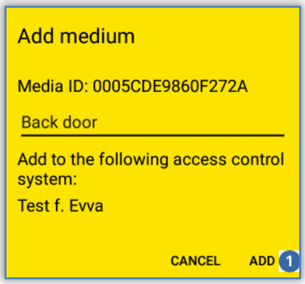
Medium details

Card in factory state

Media type	Medium
Media ID	0005CDE9860F272A
Keyring version	6.18
Status	✓ Authorisations, office mode and release duration are up to date. ✓ Keyring version up to date
Access control system	None

Figure 71: Medium details

- Tap ***Add***.
- Enter a designation for the medium.



Add medium

Media ID: 0005CDE9860F272A

Back door

Add to the following access control system:

Test f. Evva

Figure 72: Adding media – specifying designations

- Select the access control system to which you would like to add the medium if the smartphone has been registered in several access control systems.
- Tap ***Add*** ❶.
- Now once again hold the smartphone to the medium to complete the process.

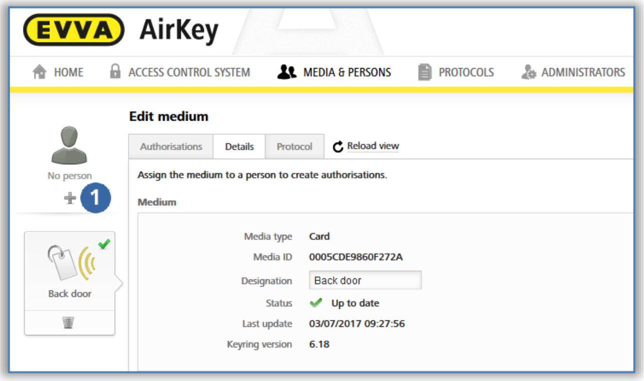
- A confirmation prompt completes the process. The medium is now available for management in the AirKey Online Administration – and it must now be assigned to a person.

This process is identical for cards, key fobs, combi keys, and wristbands. All three elements are grouped in "Card".

4.13 Assigning persons to media

As part of the continue step, you must assign the medium to a person within the AirKey Online Administration to be able to assign authorisations. This is the only way to link persons to access events.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium that has not been assigned to a person yet in the media list.
- Continue to the ***No person*** button click the **+** icon ❶



Edit medium

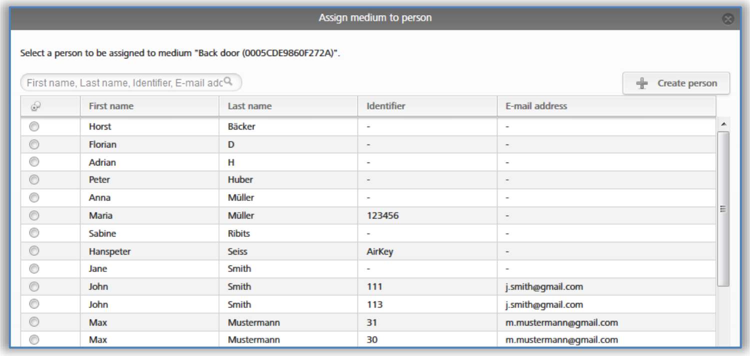
Assign the medium to a person to create authorisations.

Medium

Media type	Card
Media ID	0005CDE9860F272A
Designation	Back door
Status	✓ Up to date
Last update	03/07/2017 09:27:56
Keyring version	6.18

Figure 73: Assigning persons

- Select the person from the persons list you would like to assign this medium to.



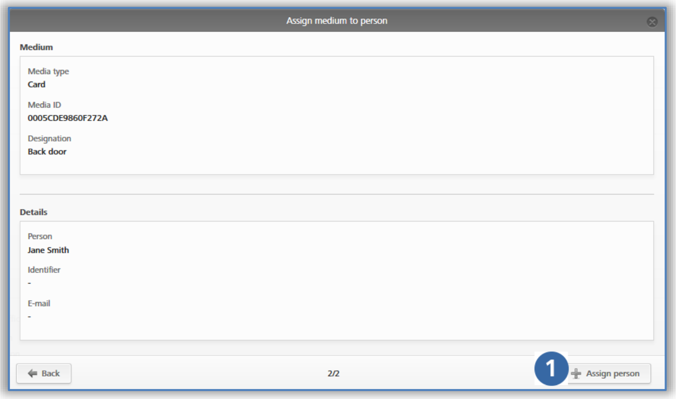
Select a person to be assigned to medium "Back door (0005CDE9860F272A)".

	First name	Last name	Identifier	E-mail address
○	Horst	Bäcker	-	-
○	Florian	D	-	-
○	Adrian	H	-	-
○	Peter	Huber	-	-
○	Anna	Müller	-	-
○	Maria	Müller	123456	-
○	Sabine	Ribits	-	-
○	Hanspeter	Seiss	AirKey	-
○	Jane	Smith	-	-
○	John	Smith	111	j.smith@gmail.com
○	John	Smith	113	j.smith@gmail.com
○	Max	Mustermann	31	m.mustermann@gmail.com
○	Max	Mustermann	30	m.mustermann@gmail.com

Figure 74: Assigning persons to media

- If a certain user has not been created yet, use the ***Create person*** button to open a second dialogue window, "Assign medium to person".

- Select ***Assign person*** ❶ to confirm you would like to assign the selected person to the medium.



Assign medium to person

Medium

Media type
Card

Media ID
0005CDE9860F272A

Designation
Back door

Details

Person
Jane Smith

Identifier
-

E-mail
-

Figure 75: Confirming persons

- Please refer to Assigning authorisations for more information.

Alternatively, you can also assign media to persons using the medium. Please refer to Assigning media to persons for more information.

4.14 Assigning authorisations

Please note that you can only assign authorisations once a medium has been assigned to a person.

- Select ***Media & persons*** → ***Media*** in the main menu.
- Select the desired medium from the overview list.
- If the medium has been assigned to a person, an overview of authorisations for this medium appears.
- As soon as you drag and drop the corresponding locking component to the grey area, available access types appear in the four areas with dotted edges.

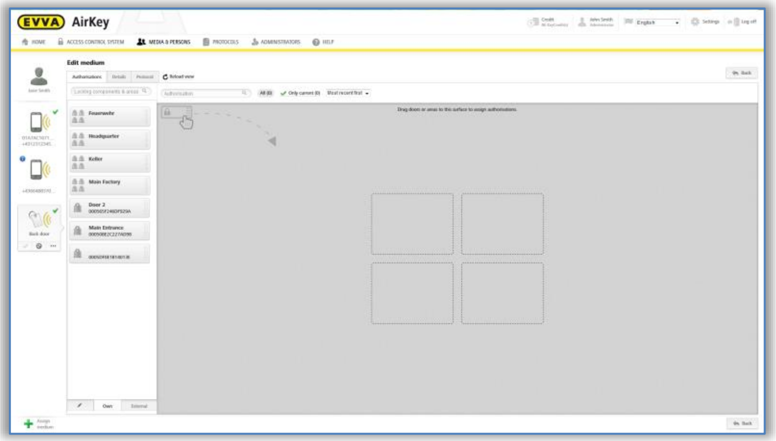


Figure 76: Assigning authorisations

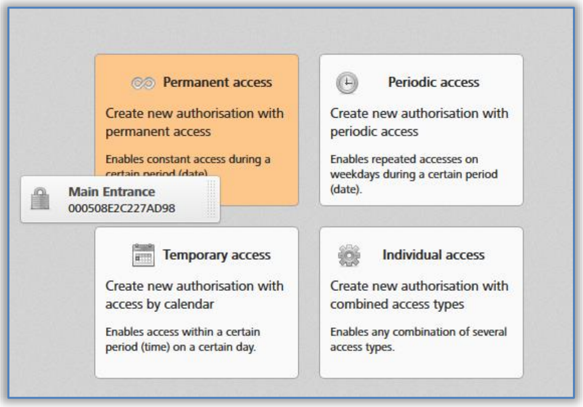
- Drag and drop the selected door / selected area to the corresponding field to select the desired access type.

Four access types are available:

- Permanent access
- Periodic access
- Temporary access
- Individual access

4.14.1 Permanent access

Permanent access indicates access is granted at any time. Specify a start and end date to restrict the authorisation.



Permanent access

Create new authorisation with permanent access

Enables constant access during a certain period (date).

Main Entrance
000508E2C227AD98

Periodic access

Create new authorisation with periodic access

Enables repeated accesses on weekdays during a certain period (date).

Temporary access

Create new authorisation with access by calendar

Enables access within a certain period (time) on a certain day.

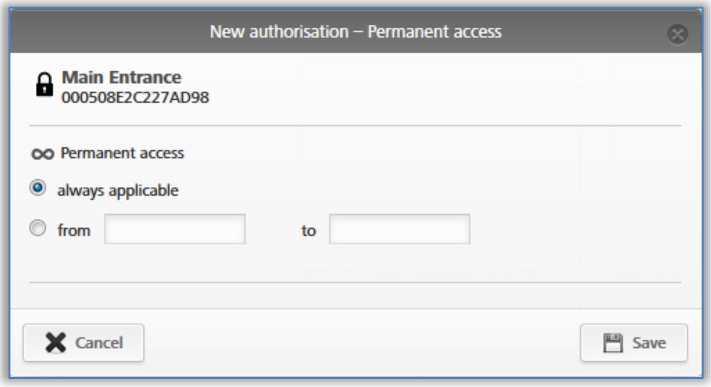
Individual access

Create new authorisation with combined access types

Enables any combination of several access types.

Figure 77: Assigning permanent access authorisations

- Specify the period of permanent access. You can choose between unrestricted, permanent access or permanent access with a specified start and end date.



New authorisation – Permanent access

Main Entrance
000508E2C227AD98

Permanent access

● always applicable

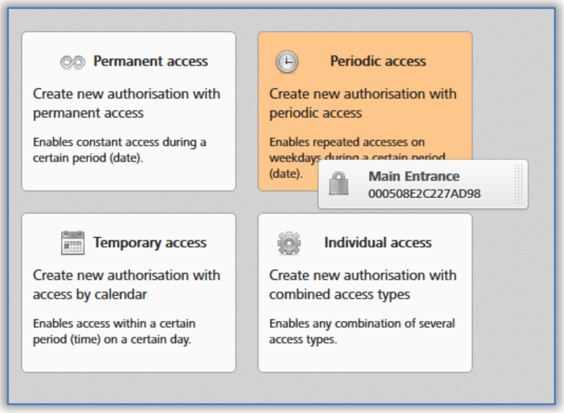
○ from ______ to ______

Figure 78: Assigning permanent access authorisations

- Click ***Save***.

4.14.2 Periodic access

Assign periodic access for recurring access at certain times. For instance, recurring access events could be a series of weekly appointments.



Permanent access
Create new authorisation with permanent access
Enables constant access during a certain period (date).

Periodic access
Create new authorisation with periodic access
Enables repeated accesses on weekdays during a certain period (date).

Main Entrance
000508E2C227AD98

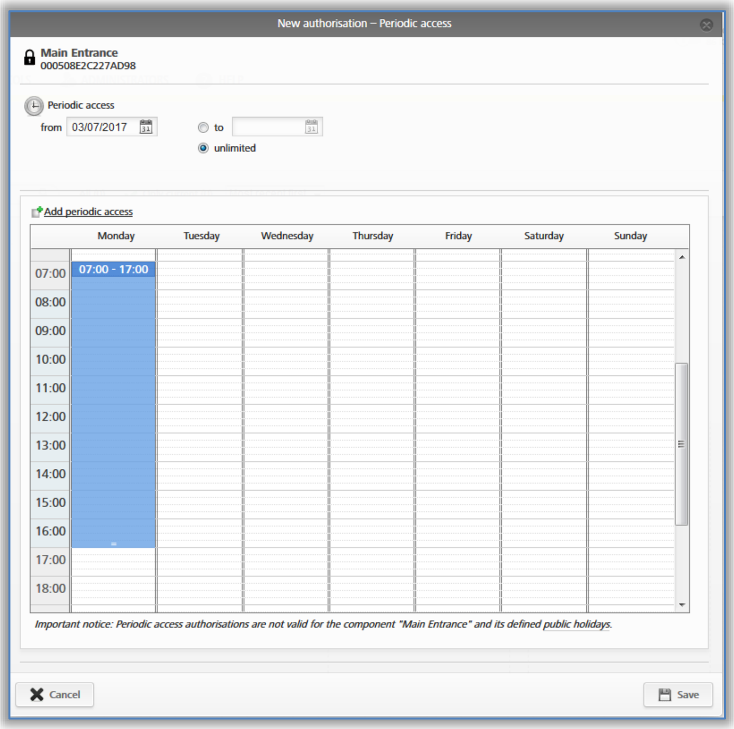
Temporary access
Create new authorisation with access by calendar
Enables access within a certain period (time) on a certain day.

Individual access
Create new authorisation with combined access types
Enables any combination of several access types.

Figure 79: Assigning periodic access

The system shows a weekly calendar allowing you to define up to four periods for each day of the week.

> Specify the period of periodic access.



New authorisation – Periodic access

Main Entrance
000508E2C227AD98

Periodic access
from 03/07/2017 ○ to
● unlimited

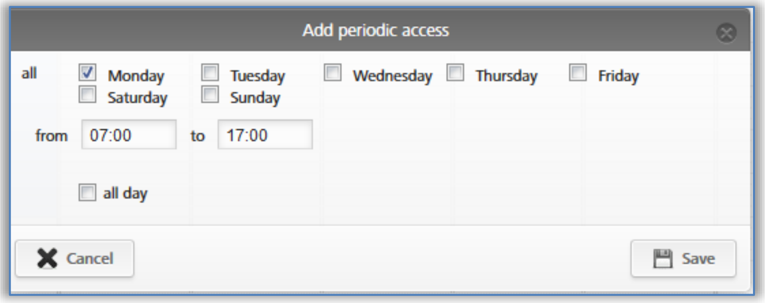
Add periodic access

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
07:00	07:00 - 17:00						
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							

Important notice: Periodic access authorisations are not valid for the component "Main Entrance" and its defined public holidays.

Figure 80: Assigning periodic access

> Directly highlight the period in the calendar or click ***Add periodic access***.



all ☑ Monday ☐ Tuesday ☐ Wednesday ☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

from 07:00 to 17:00

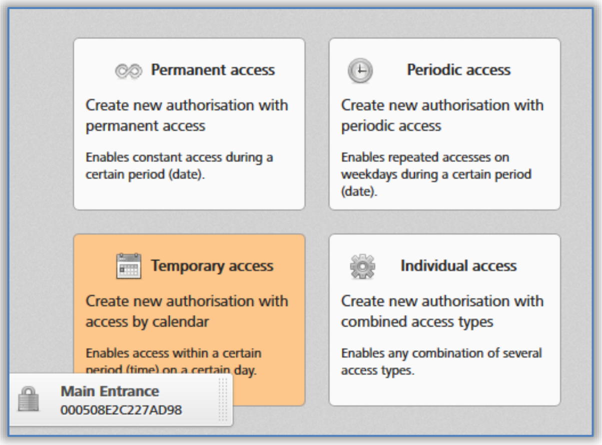
☐ all day

Figure 81: Adding periodic access

> Enter the desired period and click ***Save***.
> Also click ***Save*** in the "New authorisation – Periodic access" window.

4.14.3 Temporary access

Assign single access authorisations, if access must be restricted to a certain day and a certain period.



Permanent access
Create new authorisation with permanent access
Enables constant access during a certain period (date).

Periodic access
Create new authorisation with periodic access
Enables repeated accesses on weekdays during a certain period (date).

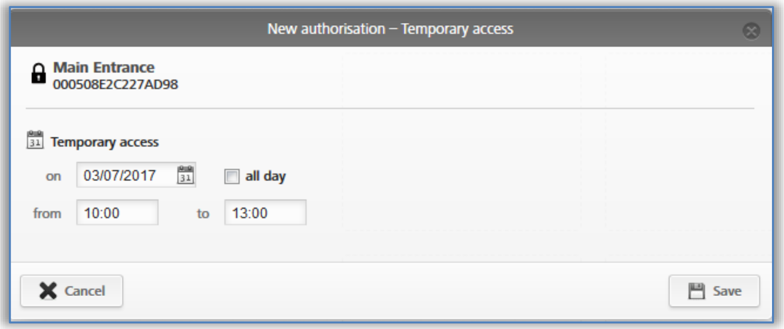
Temporary access
Create new authorisation with access by calendar
Enables access within a certain period (time) on a certain day.

Individual access
Create new authorisation with combined access types
Enables any combination of several access types.

Main Entrance
000508E2C227AD98

Figure 82: Assigning temporary access authorisations

> Enter the desired period and click ***Save***.



Main Entrance
000508E2C227AD98

Temporary access

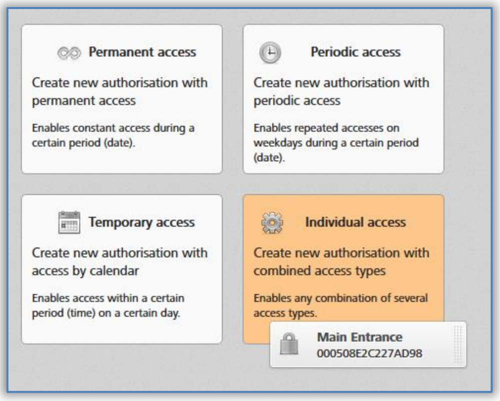
on 03/07/2017 ☐ all day

from 10:00 to 13:00

Figure 83: Assigning temporary access authorisations

4.14.4 Individual access

Assign individual access authorisations if you require a combination of permanent access, single access, and periodic access.



Permanent access
Create new authorisation with permanent access
Enables constant access during a certain period (date).

Periodic access
Create new authorisation with periodic access
Enables repeated accesses on weekdays during a certain period (date).

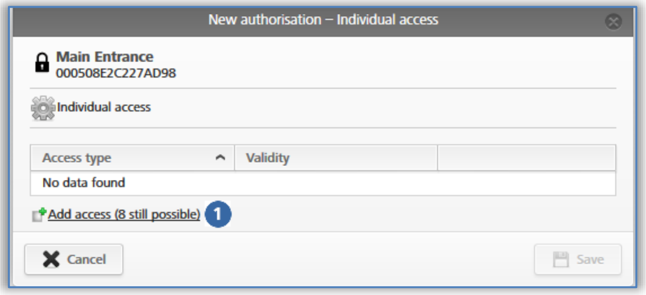
Temporary access
Create new authorisation with access by calendar
Enables access within a certain period (time) on a certain day.

Individual access
Create new authorisation with combined access types
Enables any combination of several access types.

Main Entrance
000508E2C227AD98

Figure 84: Assigning individual access

- The "New authorisation – Individual access" dialogue window shows any individual access authorisations you have already assigned.
- Click an entry in a row to change the authorisation.
- Alternatively click ***Add access*** ❶ for a new entry.



New authorisation – Individual access

Main Entrance
000508E2C227AD98

Individual access

Access type	Validity	
No data found		

Add access (8 still possible) 1

Figure 85: New authorisation – individual access

Select ***permanent access***, ***periodic access*** or ***temporary access*** and define the specifications in each case. The parameters correspond to the access authorisations that have been described above.

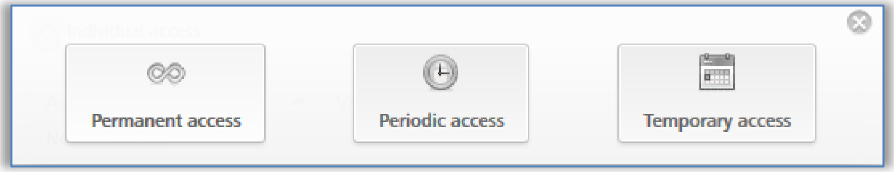


Figure 86: New authorisation – individual access

- Click ***Save*** once you have configured all authorisations for individual access.

> - Permanent access and periodic access periods must not overlap.
> - It is possible to define a maximum of one individual access period per day.

- If individual access and periodic access periods overlap, both access types are valid.
- You can configure a maximum of eight individual authorisations.

4.15 Creating authorisations

After having created the access authorisations for a medium, you must complete the process with ***Create authorisation*** and update the corresponding medium.

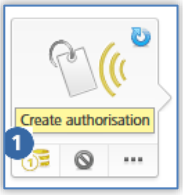


Figure 87: Creating authorisations

Changing an existing authorisation or creating new authorisations changes the icon of the corresponding medium. You can now create the authorisation, providing you have sufficient credit.

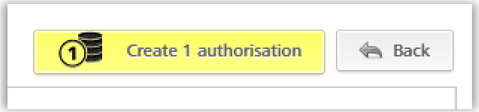


Figure 88: Creating new or changed authorisations

- Click on the yellow button ***Create 1 authorisation*** or the ❶ icon of the medium to create the authorisation and debit a KeyCredit.

A corresponding message appears if you do not have sufficient credit at this point in the process. You can immediately top-up your credit using a link in this message. Topping up your credit using this message will automatically create the authorisation and deduct one KeyCredit from your account.

You must now update media, such as cards, key fobs, combi keys or wristbands using a smartphone or coding station for the authorisations to be activated on the medium. Authorisations to smartphones are sent by push messages (notifications).

In the last chapter you learned to set up the access control system correctly. The processes described herein illustrate the first steps and enable management of your access control system. Please refer to the following sections for a more detailed description of individual AirKey Online Administration functions and the AirKey app.

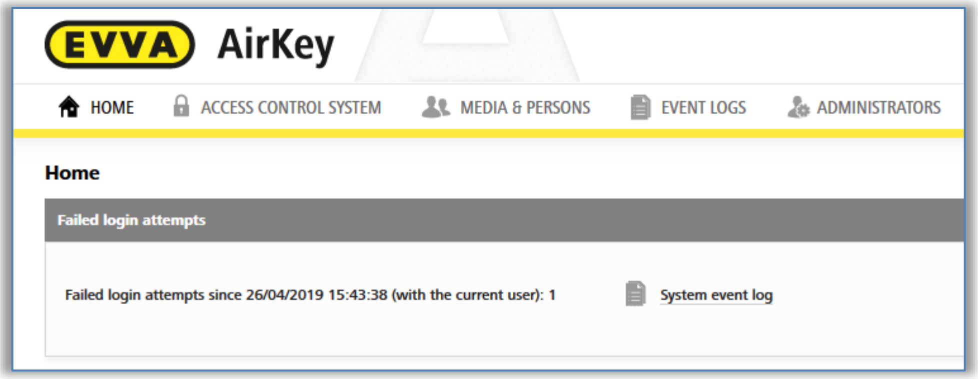
5 AirKey Online Administration

5.1 AirKey login

The login is required to configure or manage the AirKey access control system. In the AirKey Online Administration settings, a two-factor authentication can be optionally activated for the login. The activation is described in the chapter Access control system settings.

Activate the two-factor authentication to increase the security of your AirKey access control system.

Failed login attempts are displayed on the start page and logged in the system event log. The display on the start page only appears if there has been at least one failed login attempt since the last successful login.



Home

Failed login attempts

Failed login attempts since 26/04/2019 15:43:38 (with the current user): 1

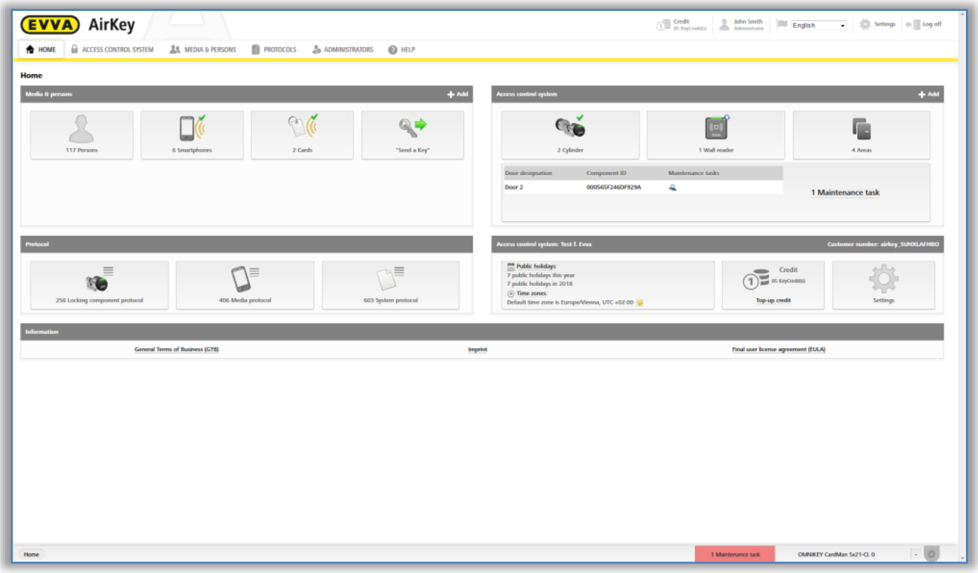
System event log

Figure 89: Failed login attempts

5.1.1 AirKey login without two-factor authentication

- Open the following page in your browser: https://airkey.evva.com.
  The AirKey Online Administration login page opens.
- Enter the user ID you received in the "EVVA AirKey registration" e-mail.
- Enter your personal AirKey password and confirm with ***Log in***.

Once you have logged on, the system opens the ***Home*** screen. It provides an overview of your AirKey access control system.



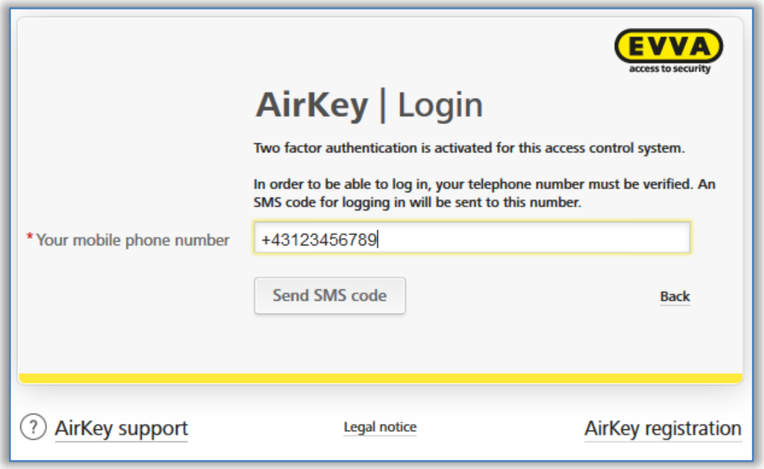
Door designation	Component ID	Maintenance tasks
Door 2	000565F246DF929A	

Public holidays:
7 public holidays this year
7 public holidays in 2018
Time zones:
Default time zone is Europe/Vienna, UTC +02:00

Figure 90: AirKey Online Administration – home screen

5.1.2 AirKey login with two-factor authentication

- Open the following page in your browser: https://airkey.evva.com. The AirKey Online Administration login page opens.
- Enter the user ID you received in the "EVVA AirKey registration" e-mail.
- Enter your personal AirKey password and confirm with ***Log in***.
- If no phone number has been verified for the administrator, a prompt appears to enter a phone number for verification.
- Enter the phone number of the smartphone to be used for two-factor authentication and confirm with ***Send SMS code***. The phone number must begin with **+** and country code, and may contain a maximum of 50 characters (+, 0-9, and spaces).



Two factor authentication is activated for this access control system.

In order to be able to log in, your telephone number must be verified. An SMS code for logging in will be sent to this number.

* Your mobile phone number: +43123456789

Figure 91: Verify mobile phone number on login

- An SMS with an SMS code is sent to the entered telephone number.
- Enter this SMS code in the dialogue within the AirKey Online Administration and confirm with ***Log in***.

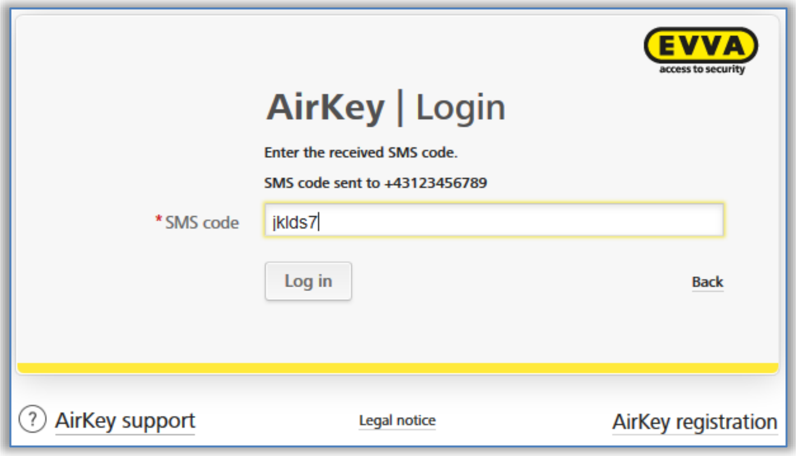


Figure 92: Enter SMS code for login

> The telephone number is now verified for two-factor authentication and the start page of your AirKey access control system is displayed.

! If the phone number has already been verified, it does not need to be re-entered after entering the user ID and password. In this case, an SMS code is immediately sent to the verified phone number.

! The SMS code is valid for 5 minutes. If the 5 minutes are exceeded, the login process must be repeated.

! Without access to the verified telephone number no login to the AirKey Online Administration can take place. If you want to change the phone number, you must change the phone number in the details of the administrator (see Editing administrators). However, this requires the currently verified phone number. If the telephone number is no longer available, please contact EVVA support.

5.1.3 Have you forgotten your password?

You can individually reset your password should it be unavailable.
Click ***Forgot your password?*** ❶

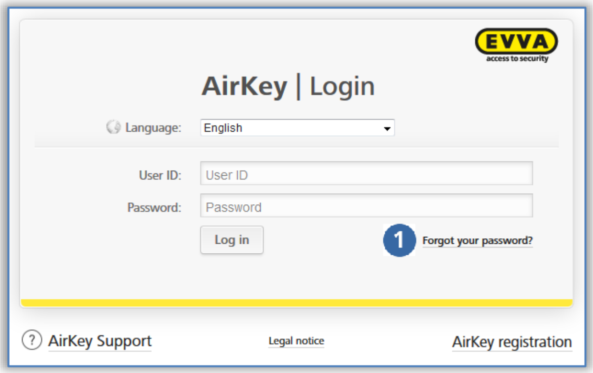
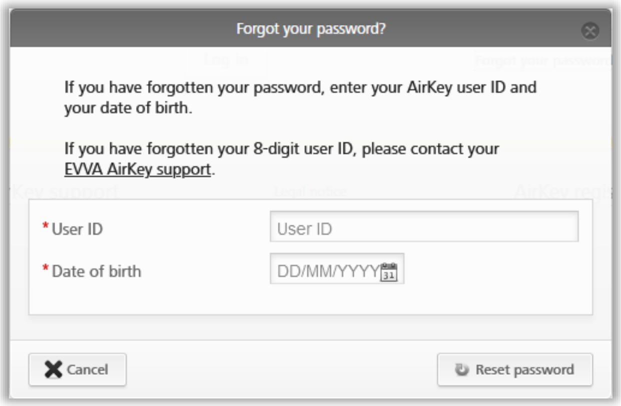


Figure 93: AirKey Online Administration login page

AirKey system manual version 2.7 | 06/03/2024 | Subject to technical changes and misprints

- Enter your username and the date of birth you entered upon registration in the "Forgot your password?" dialogue window and click ***Reset password***.



Forgot your password?

If you have forgotten your password, enter your AirKey user ID and your date of birth.

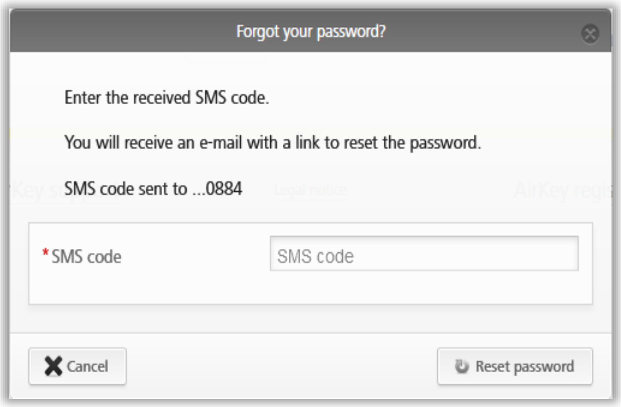
If you have forgotten your 8-digit user ID, please contact your EVVA AirKey support.

*User ID: User ID

*Date of birth: DD/MM/YYYY

Figure 94: Forgot your password?

- If two-factor authentication is activated, you will receive an SMS code to your verified smartphone, which must be entered in the following dialogue and confirmed with ***Reset password***. (This step does not apply if the two-factor authentication is not activated or the phone number is not yet verified.)



Forgot your password?

Enter the received SMS code.

You will receive an e-mail with a link to reset the password.

SMS code sent to ...0884

*SMS code: SMS code

Figure 95: SMS code reset password

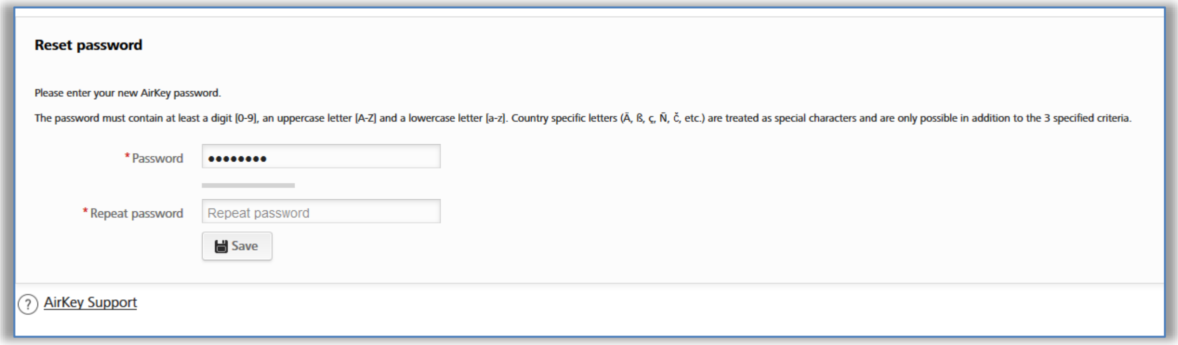
The SMS code is valid for 5 minutes. If the 5 minutes are exceeded, the process must be repeated.

Without access to the verified phone number, the process cannot be completed. If the telephone number is no longer available, please contact EVVA support.

You will receive an automated e-mail from *EVVA AirKey* with the following subject line: "EVVA AirKey Online Administration – reset your password".

- Open the e-mail from *EVVA AirKey*.
- In the e-mail, click the link to reset your password. The "Reset password" website opens.
- Enter your new password and re-enter your new password to confirm the process.

- Click ***Save***.



Reset password

Please enter your new AirKey password.

The password must contain at least a digit [0-9], an uppercase letter [A-Z] and a lowercase letter [a-z]. Country specific letters (Ā, ß, ç, Ñ, č, etc.) are treated as special characters and are only possible in addition to the 3 specified criteria.

* Password	••••••••
* Repeat password	Repeat password

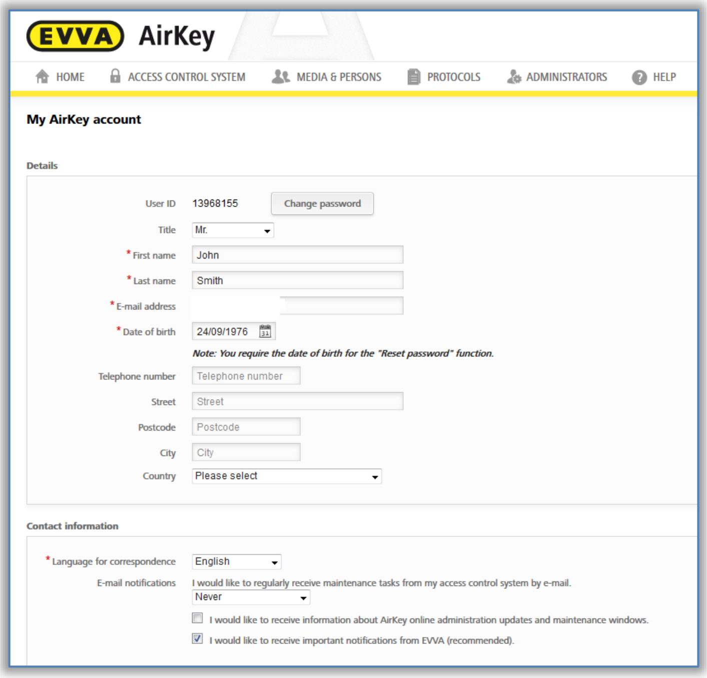
Figure 96: Resetting the AirKey password

The AirKey Online Administration login page opens.

- Perform the login as described in AirKey login without two-factor authentication or AirKey login with two-factor authentication, with the new password.

If your input is correct, the AirKey Online Administration ***Home*** screen opens. The top right shows the name of the user that has logged in.

If required, you can also change your password in the AirKey Online Administration. For this purpose, click the administrator's name in the right-hand AirKey Online Administration header and use the ***Change password*** function.



My AirKey account

Details

User ID	13968155
Title	Mr.
* First name	John
* Last name	Smith
* E-mail address	
* Date of birth	24/09/1976
	Note: You require the date of birth for the "Reset password" function.
Telephone number	Telephone number
Street	Street
Postcode	Postcode
City	City
Country	Please select

Contact information

* Language for correspondence	English
E-mail notifications	I would like to regularly receive maintenance tasks from my access control system by e-mail. Never
	□ I would like to receive information about AirKey online administration updates and maintenance windows.
	☑ I would like to receive important notifications from EVVA (recommended).

Figure 97: My AirKey account

5.2 AirKey logout

Click ***Log out*** ❶ to quit the AirKey Online Administration.

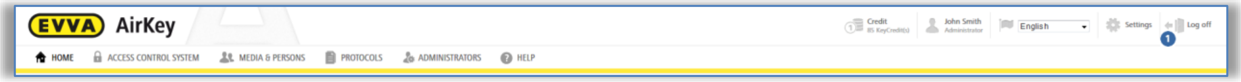


Figure 98: Logging out

Despite having integrated an automatic logout feature after 30 minutes we highly recommend administrators always log out after having completed any due tasks in the AirKey Online Administration using the ***Log out*** button.

5.3 Administrators

There are two roles for administrators to manage the AirKey system: system administrators and sub-administrators.

System administrators have all rights to manage the entire AirKey access control system and can also create, edit and delete other administrators.

Sub-administrators have limited rights and are used especially for personal and authorisation management. In addition, sub-administrators can also be restricted to specific areas and locking components of the AirKey access control system. This means that they can only create and edit access authorisations for locking components and areas for which they are authorised.

There must be a minimum of one system administrator per access control system.

Please refer to the ***Administrators*** ❶ main menu for the administrator management functions.

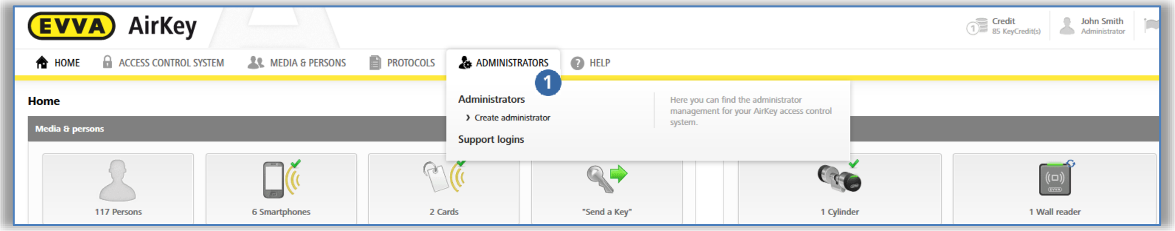
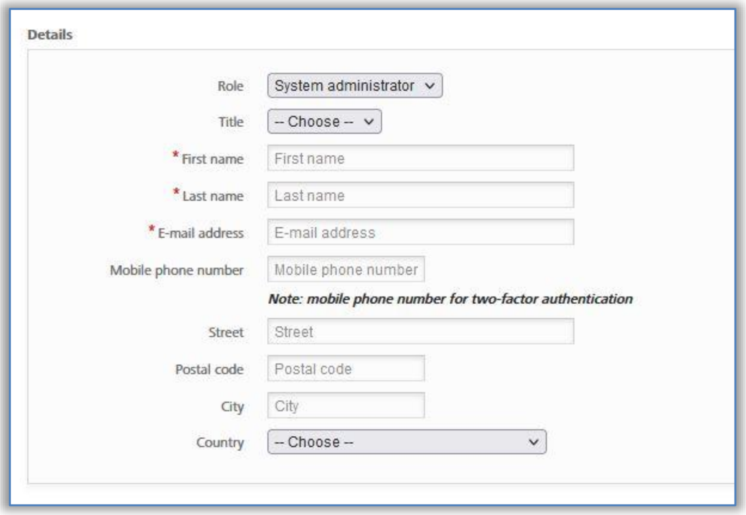


Figure 99: Administrators main menu

5.3.1 Creating administrators

Administrators can exclusively be created by other administrators.

- In the main menu select ***Administrators*** → ***Create administrator***.
- Select whether the role is that of a **system administrator** or **sub-administrator**.

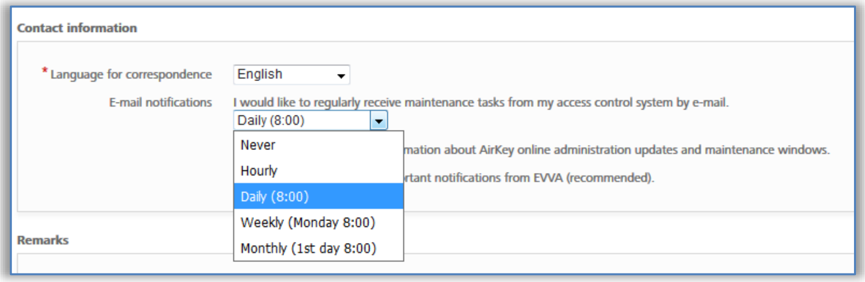


Details

Role	System administrator
Title	-- Choose --
* First name	First name
* Last name	Last name
* E-mail address	E-mail address
Mobile phone number	Mobile phone number *Note: mobile phone number for two-factor authentication*
Street	Street
Postal code	Postal code
City	City
Country	-- Choose --

Figure 100: Details of an administrator

- Complete the fields in the form. Fields highlighted by * are mandatory fields.
- In the "Contact information" field, you can also specify whether the administrator should receive e-mail notifications about certain events, such as open maintenance tasks, upcoming maintenance windows or other important information. E-mail notifications are sent in the selected language for correspondence.



Contact information

* Language for correspondence	English
E-mail notifications	I would like to regularly receive maintenance tasks from my access control system by e-mail. Daily (8:00)

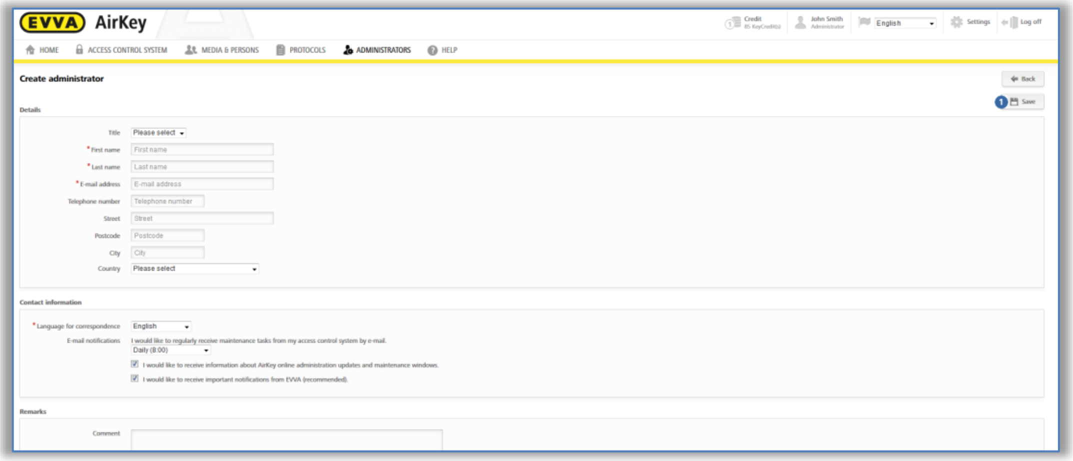
...mation about AirKey online administration updates and maintenance windows.

...rtant notifications from EVVA (recommended).

Remarks

Figure 101: Contact information

- Click ***Save*** ❶.



Create administrator

Details

Title	Please select
* First name	First name
* Last name	Last name
* E-mail address	E-mail address
Telephone number	Telephone number
Street	Street
Postcode	Postcode
City	City
Country	Please select

Contact information

* Language for correspondence	English
E-mail notifications	I would like to regularly receive maintenance tasks from my access control system by e-mail. Daily (8:00) ☑ I would like to receive information about AirKey online administration updates and maintenance windows. ☑ I would like to receive important notifications from EVVA (recommended).

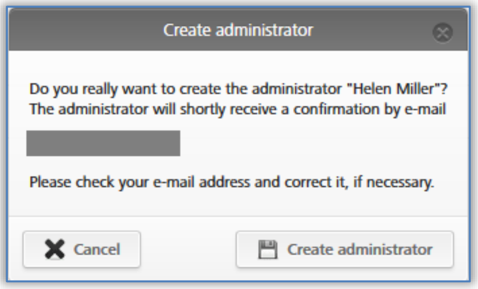
Remarks

Comment	

Figure 102: Creating administrators

Check the e-mail address to which the activation link is sent before you save.

- > Click ***Create administrator*** to confirm the security prompt and complete the process.



Create administrator

Do you really want to create the administrator "Helen Miller"? The administrator will shortly receive a confirmation by e-mail

[redacted]

Please check your e-mail address and correct it, if necessary.

Figure 103: Creating administrators

The system reports "The administrator has been saved" once you have created an administrator.

Now the administrator you created receives an e-mail from *EVVA AirKey* with an activation link. You can only manage the rights for **sub-administrators** after creating the administrator successfully. Details about the rights management of sub-administrators can be found in the chapter Editing administrators.

The data is deleted and the activation link is rendered invalid, if it is not activated within 48 hours.

The administrator you created must complete registration as described below:

- > Open the e-mail with the subject line "EVVA AirKey registration".
- > Click the activation link. The "Welcome to AirKey" website opens.
- > Enter your personal password, re-enter the password and specify your date of birth.
- > Click ***Save***.

This completes the process to create administrators. The system then opens the AirKey Online Administration login page for administrators to log in.

5.3.2 Editing administrators

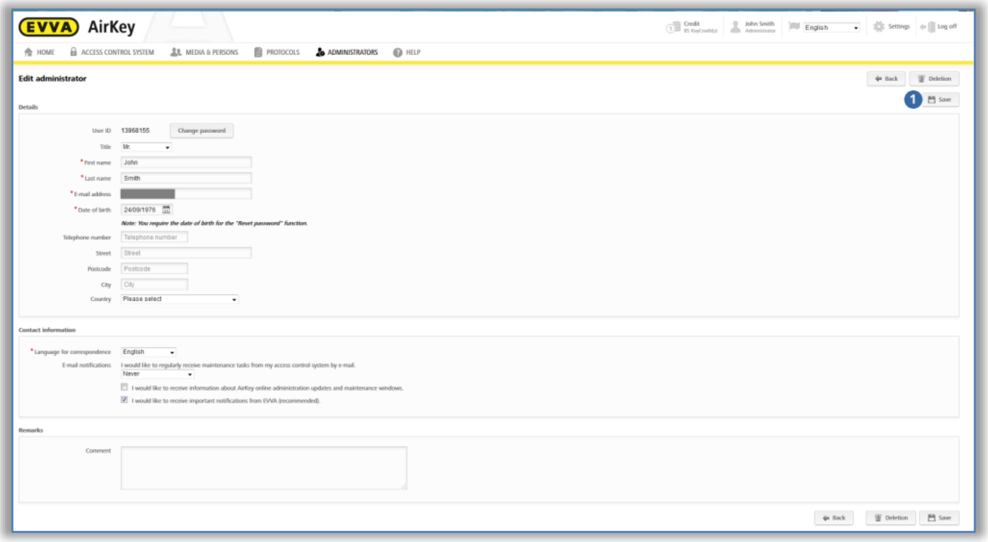
Only **system administrators** can subsequently change details such as the surname, e-mail address, telephone number or contact information of an administrator. The role can also be edited subsequently. However, please note that there must be at least one system administrator per access control system.

The user ID cannot be changed.

- In the main menu select ***Administrators*** → ***Administrators***.
  The system shows a list of all administrators.

Search for administrators, sort columns and restrict the number of entries shown per page in the list on screen as well as export the list to a CSV file.

- Click the administrator whose details you would like to change.
- Change the desired data.
- Click ***Save*** ❶.



Edit administrator

Details

User ID	13968155
Title	Mr.
*First name	John
*Last name	Smith
*E-mail address	[redacted]
*Date of birth	24/09/1976
	Note: You require the date of birth for the "Reset password" function.
Telephone number	Telephone number
Street	Street
Postcode	Postcode
City	City
Country	Please select

Contact information

*Language for correspondence	English
E-mail notifications	I would like to regularly receive maintenance tasks from my access control system by e-mail. Never □ I would like to receive information about AirKey online administration updates and maintenance windows. ☑ I would like to receive important notifications from EVVA (recommended).

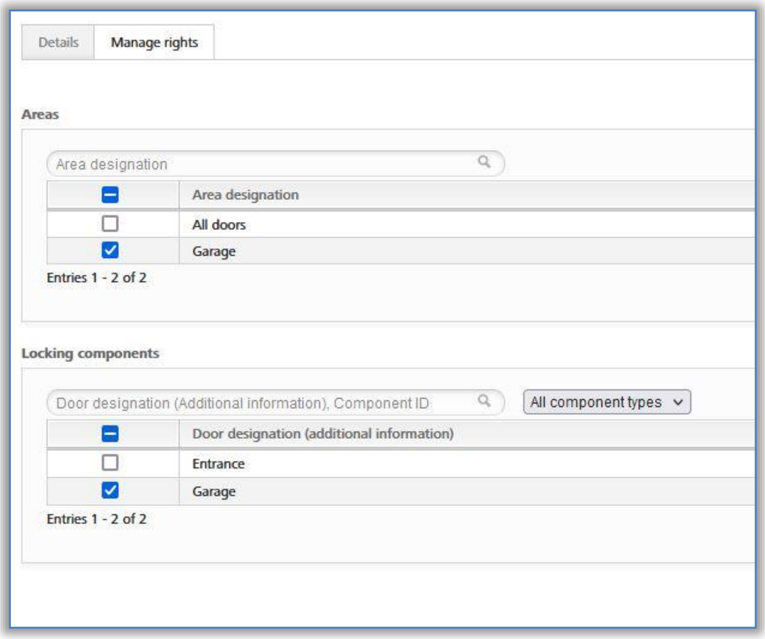
Remarks

Comment

Figure 104: Editing administrators

To manage the rights of **sub-administrators** follow these steps:

- In the main menu, select ***Administrators*** → ***Administrators***.
  The list with all valid administrators is displayed.
- Click on the **sub-administrator** whose rights you want to change.
- Switch to the ***Manage rights*** tab.
- By selecting the checkboxes, you can choose which areas and locking components the sub-administrator is allowed to view and assign authorisations for.



Details | Manage rights

Areas

Area designation

☐	Area designation
☐	All doors
☑	Garage

Entries 1 - 2 of 2

Locking components

Door designation (Additional information), Component ID | All component types

☐	Door designation (additional information)
☐	Entrance
☑	Garage

Entries 1 - 2 of 2

Figure 105: Manage rights of a sub-administrator

- Click on ***Save***.

Areas and locking components for which a **sub-administrator** does not have rights are not available to the **sub-administrator** when assigning authorisations. All areas and locking components are always available to a **system administrator** for the assignment of authorisations.

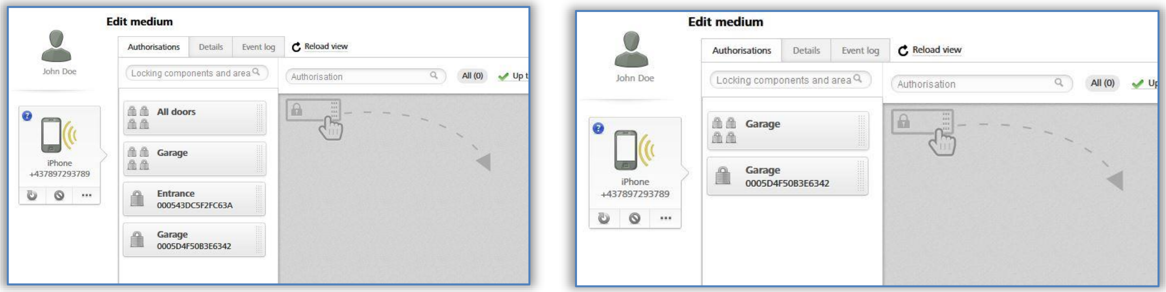


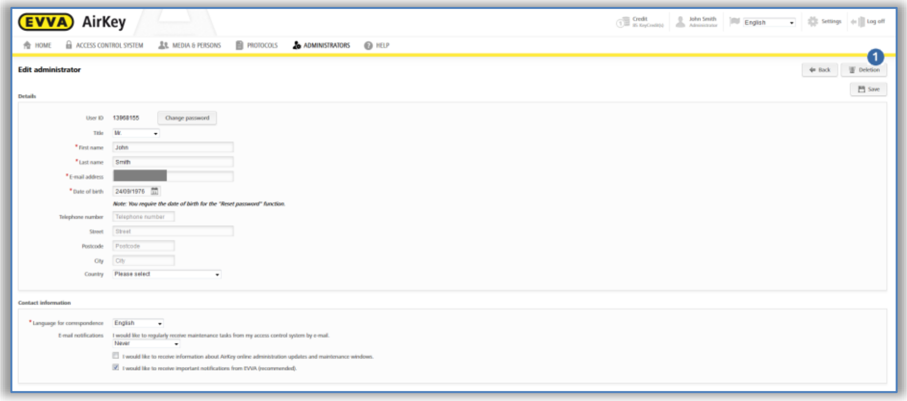
Figure 106: Assigning authorisations by a system administrator respectively by a sub-administrator

The rights management for sub-administrators only applies to areas and locking components. Thus, all persons and media are always displayed to a sub-administrator.

5.3.3 Deleting administrators

An administrator can be deleted only by a different system administrator.

- In the main menu click ***Administrators*** → ***Administrators***.
- Click the corresponding row in the table to select the administrator you would like to delete. The "Edit administrator" page opens.
- Click ***Delete*** ❶.



Edit administrator

Details

User ID 13968155

Title Mr.

*First name John

*Last name Smith

*E-mail address [redacted]

*Date of birth 24/09/1976

Note: You require the date of birth for the "Reset password" function.

Telephone number Telephone number

Street Street

Postcode Postcode

City City

Country Please select

Contact information

*Language for correspondence English

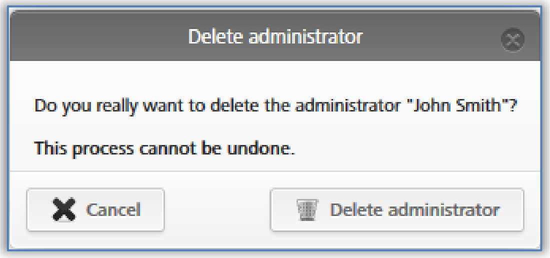
E-mail notifications I would like to regularly receive maintenance tasks from my access control system by e-mail. Never

□ I would like to receive information about AirKey online administration updates and maintenance windows.

☑ I would like to receive important notifications from EVVA (recommended).

Figure 107: Deleting administrators

- Click ***Delete administrator*** to confirm the security prompt.



Do you really want to delete the administrator "John Smith"?

This process cannot be undone.

Figure 108: Deleting administrators

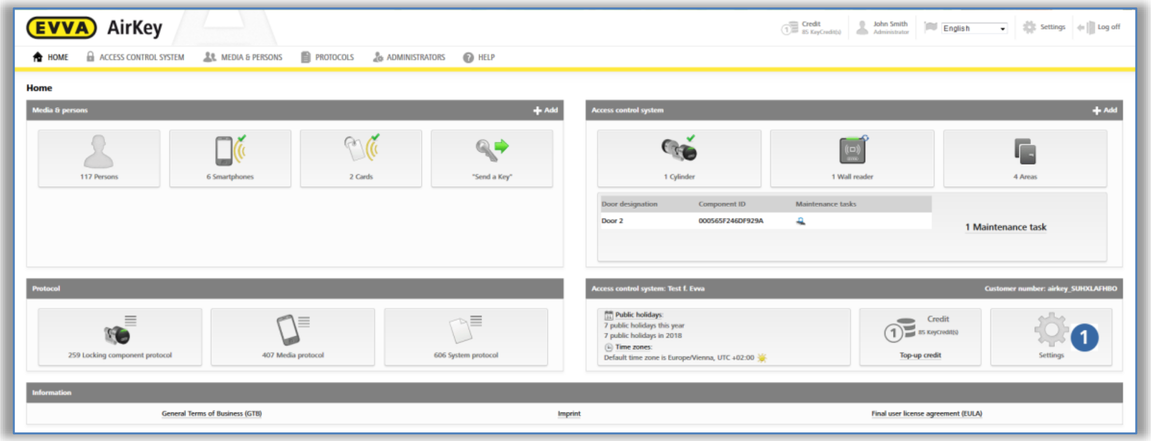
The system reports "The administrator has been deleted" once you have deleted an administrator. Deleted administrators no longer appear on the administrator list and they are consequently no longer able to log on to the AirKey Online Administration.

If the four-eyes principle is enabled for event log viewing, at least two system administrators must remain. Otherwise, an error message is displayed when trying to delete the administrator. Details about the four-eyes principle for event log viewing can be found in the chapter General.

5.4 Access control system settings

Configure basic settings in the AirKey Online Administration settings. These have been described in the following sections.

- On the ***Home*** screen, click the ***Settings*** ❶ tile.
- Alternatively click ***Settings*** in the header.



Door designation	Component ID	Maintenance tasks
Door 2	000565F246DF929A	

Public holidays:
7 public holidays this year
7 public holidays in 2018
Time zones:
Default time zone is Europe/Vienna, UTC +02:00

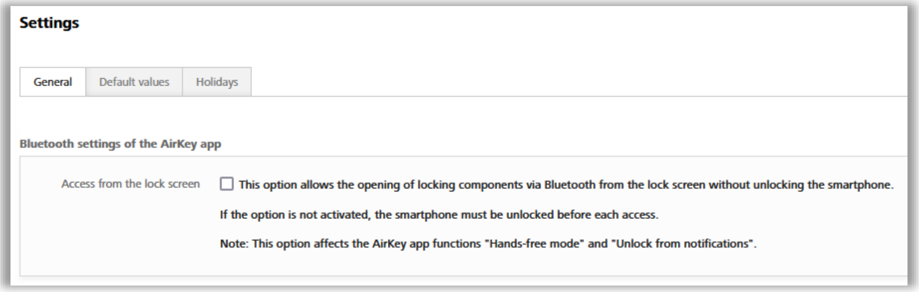
Figure 109: Access control system settings

5.4.1 General

In this tab, the following general settings can be activated for the entire access control system.

Bluetooth settings for the AirKey app

Here you can configure for all smartphones in this access control system whether locking components can be opened via Bluetooth from the lock screen or not. If this option is not activated, the smartphone must be unlocked before each access.



Access from the lock screen ☐ This option allows the opening of locking components via Bluetooth from the lock screen without unlocking the smartphone.

If the option is not activated, the smartphone must be unlocked before each access.

Note: This option affects the AirKey app functions "Hands-free mode" and "Unlock from notifications".

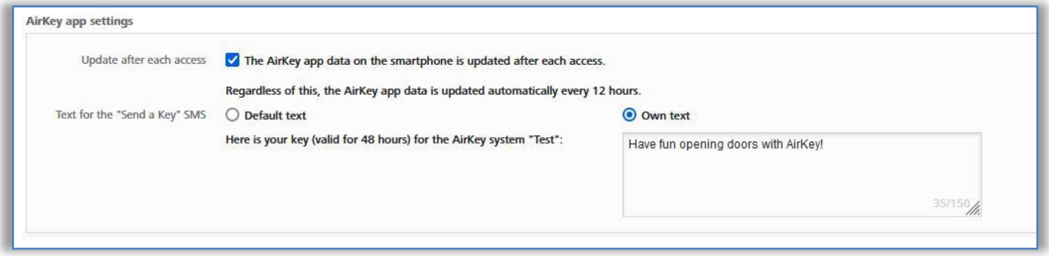
Figure 110: General settings – Bluetooth settings for the AirKey app

This option affects the AirKey app functions "Hands-free mode" and "Unlock from notifications".

Deactivate ***Access from lock screen*** to improve the security level of your AirKey system.

AirKey app settings

Here you can activate the option **Update after each access** and you can configure your own **text for the "Send a Key" SMS**.



AirKey app settings

Update after each access ☑ The AirKey app data on the smartphone is updated after each access.

Regardless of this, the AirKey app data is updated automatically every 12 hours.

Text for the "Send a Key" SMS ○ Default text ● Own text

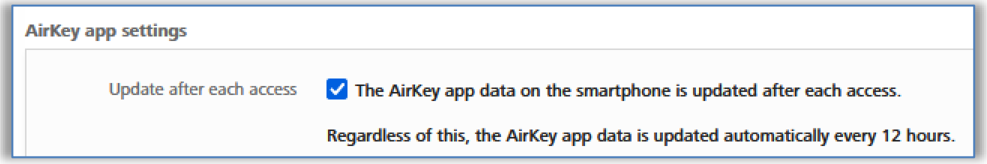
Here is your key (valid for 48 hours) for the AirKey system "Test": Have fun opening doors with AirKey!

35/150

Figure 111: General settings – AirKey app settings

If the **Update after each access** option is activated, the AirKey app data (e.g. log entries or the battery status of locking components) will be updated with a smartphone each time when an access is performed.

- Tick the corresponding checkbox and confirm with ***Save***.



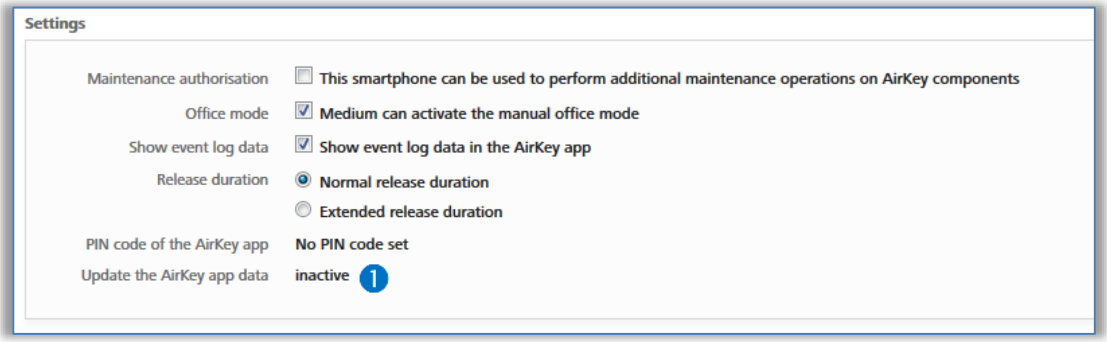
AirKey app settings

Update after each access ☑ The AirKey app data on the smartphone is updated after each access.

Regardless of this, the AirKey app data is updated automatically every 12 hours.

Figure 112: AirKey app settings – update after each access

The functionality is then sent by push notification to all smartphones in this access control system. At the latest after a manual actualisation of the AirKey app data of the smartphone (see chapter Updating smartphones), the functionality should be active on the smartphone. You can find the current status ❶ of the smartphone for this function in the AirKey Online Administration in the details of the smartphone.



Settings

Maintenance authorisation	☐ This smartphone can be used to perform additional maintenance operations on AirKey components
Office mode	☑ Medium can activate the manual office mode
Show event log data	☑ Show event log data in the AirKey app
Release duration	● Normal release duration ○ Extended release duration
PIN code of the AirKey app	No PIN code set
Update the AirKey app data	inactive ❶

Figure 113 Status of the option "Update after each access"

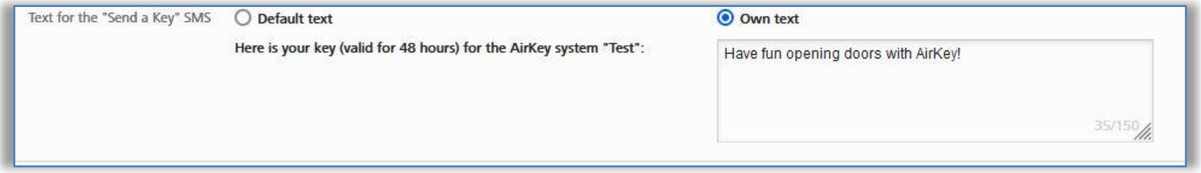
Activate this function to transfer access audit trail entries to the AirKey Online Administration almost in real time when using smartphones.

Updating the AirKey app data after an access process only transfers the data of the smartphone that performed the access process. This update is not displayed visually on the smartphone itself.

A stable internet connection (mobile data or Wi-Fi) is required for this function, since a further access process can only be executed after the AirKey app data has been updated.

Regardless of the option "Update after each access", an attempt is made to update the AirKey app data automatically every 12 hours.

You also have the possibility to configure your own **text for the "Send a Key" SMS**.



Text for the "Send a Key" SMS ○ Default text

Here is your key (valid for 48 hours) for the AirKey system "Test":

● Own text

Have fun opening doors with AirKey!

35/150

Figure 114: AirKey app settings – text for the "Send a Key" SMS

You can choose between the default text and a self-definable text. Select ***Default text*** to use the predefined text «Here is your key (valid for 48 hours) for the AirKey system "<name of access control system>"» or select ***Own text*** to use a self-definable text in the corresponding text field. Confirm your selection by clicking ***Save***.

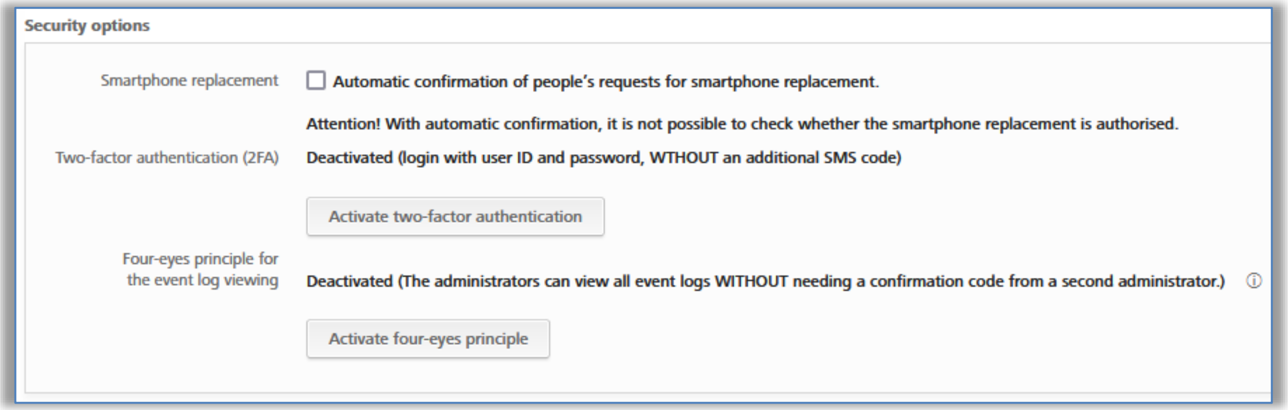
If you use your own text, you can also customize it for each "Send a Key" action, for example, to use a personalised letter of greeting. Details about "Send a Key" can be found in chapter "Send a Key" function.

The own text is limited to 150 digits. In addition the own text will not be translated in other languages if some persons have another correspondence language. Instead, the standard text is automatically translated into the person's correspondence language.

Use a self-defined text to address the smartphone owners personally and to inform them for which access control system they will receive authorisations.

Security options

In the security options, you can configure the **Smartphone replacement**, **Two-factor authentication (2FA)**, and **Four-eyes principle for event log viewing** functions.



Security options

Smartphone replacement □ Automatic confirmation of people's requests for smartphone replacement.

Attention! With automatic confirmation, it is not possible to check whether the smartphone replacement is authorised.

Two-factor authentication (2FA) Deactivated (login with user ID and password, WTHOUT an additional SMS code)

Four-eyes principle for the event log viewing Deactivated (The administrators can view all event logs WITHOUT needing a confirmation code from a second administrator.)

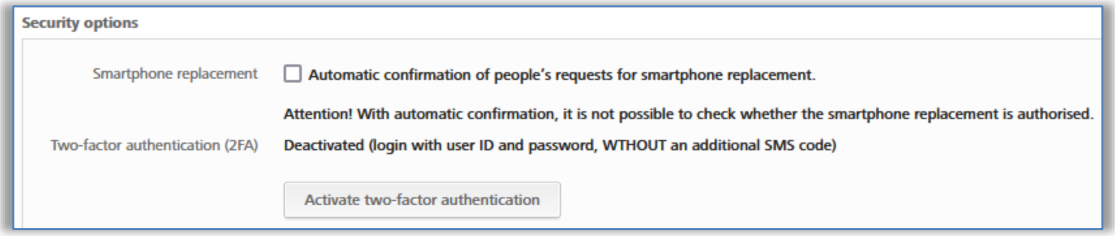
Figure 115: General settings – security options

The checkbox ***Automatic confirmation of people´s request for smartphone replacement*** can be used to automatically confirm replacement operations that have been started via a smartphone.

This means that every smartphone replacement that is started via the smartphone is automatically confirmed immediately, provided that sufficient credit is available. Please note that a KeyCredit will be deducted for each smartphone replacement in which authorisations are transferred. Details about the smartphone replacement can be found in the chapter Smartphone replacement.

The **two-factor authentication**, or **2FA**, is used as an additional security level when logging in to the AirKey Online Administration. In addition to the user ID and password, an additional SMS code is requested as a second factor. If two-factor authentication is activated in the settings, it is applied to all administrators of this access control system.

- To activate it, click the ***Activate two-factor authentication*** button.



Security options

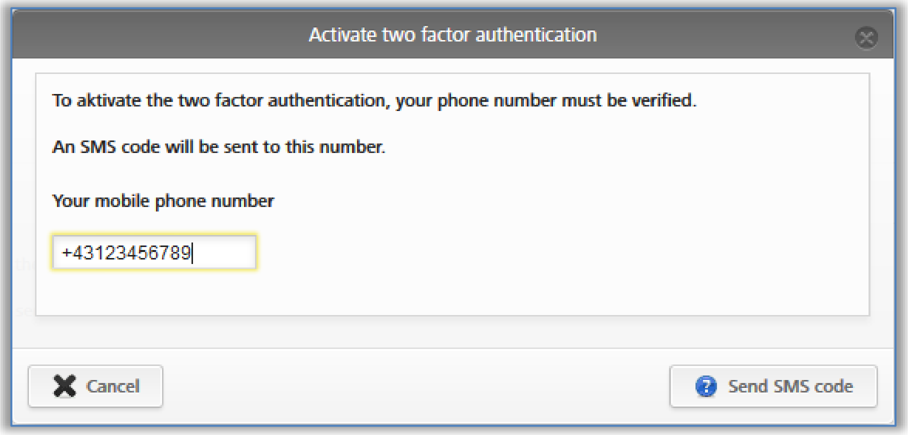
Smartphone replacement □ Automatic confirmation of people's requests for smartphone replacement.

Attention! With automatic confirmation, it is not possible to check whether the smartphone replacement is authorised.

Two-factor authentication (2FA) Deactivated (login with user ID and password, WTHOUT an additional SMS code)

Figure 116: General settings – two-factor authentication (2FA)

- Enter the mobile phone number to be used for two-factor authentication for the currently logged on administrator and click ***Send SMS code***.



Activate two factor authentication

To aktivate the two factor authentication, your phone number must be verified.

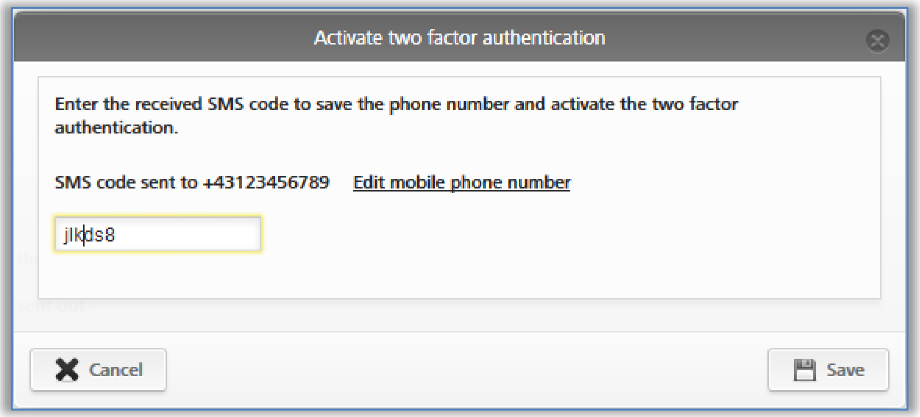
An SMS code will be sent to this number.

Your mobile phone number

+43123456789

Figure 117: Verify mobile phone number settings

- An SMS code is sent to the previously specified telephone number. This SMS code must be entered in the dialogue within the AirKey Online Administration and confirmed with ***Save***.



Activate two factor authentication

Enter the received SMS code to save the phone number and activate the two factor authentication.

SMS code sent to +43123456789 Edit mobile phone number

jlkds8

Figure 118: Enter SMS code settings

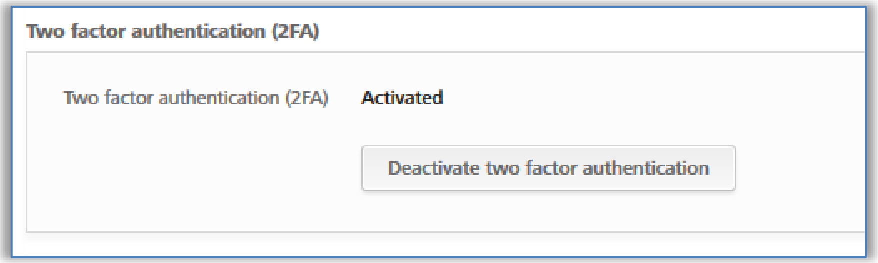
If a valid SMS code has been used, two-factor authentication is activated for all administrators of the access control system. The status in the settings changes accordingly.

! The SMS code is valid for 5 minutes. If the 5 minutes are exceeded, the process must be repeated.

! From the time of activation, a mobile phone is required for each login. Details on the login process with activated two-factor authentication can be found in the chapter AirKey login with two-factor authentication.

To disable two-factor authentication, follow these steps:

> Click on ***Deactivate two-factor authentication***.

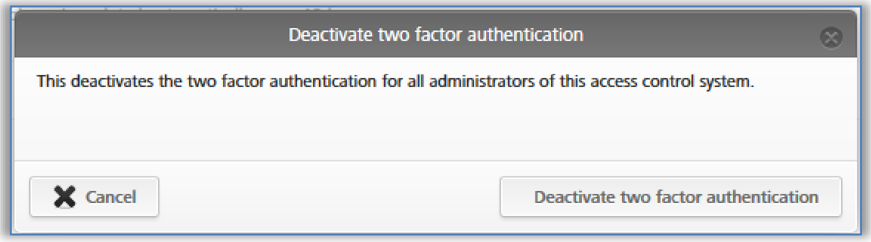


Two factor authentication (2FA)

Two factor authentication (2FA) Activated

Figure 119: Deactivate two-factor authentication

> Confirm the prompt also with ***Deactivate two-factor authentication***.



Deactivate two factor authentication

This deactivates the two factor authentication for all administrators of this access control system.

Figure 120: Deactivate two-factor authentication prompt

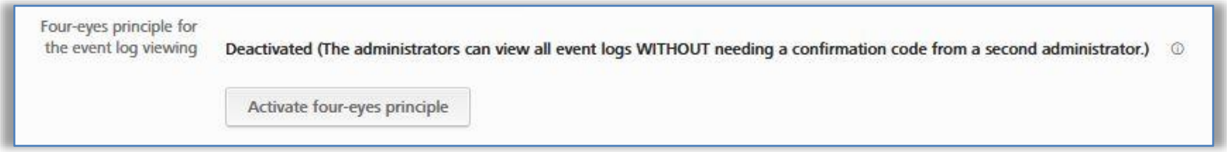
The function is deactivated again for all administrators of the access control system.

The **Four-eyes principle for the event log viewing** function allows you to view the locking component and media event log only if a second system administrator confirm the viewing. This protects personal data even better from being viewed.

To activate the **Four-eyes principle for the event log viewing** at least two system administrators must be available.

To activate the **Four-eyes principle for the event log viewing**, please follow these steps:

- Click on ***Four-eyes principle for the event log viewing***.



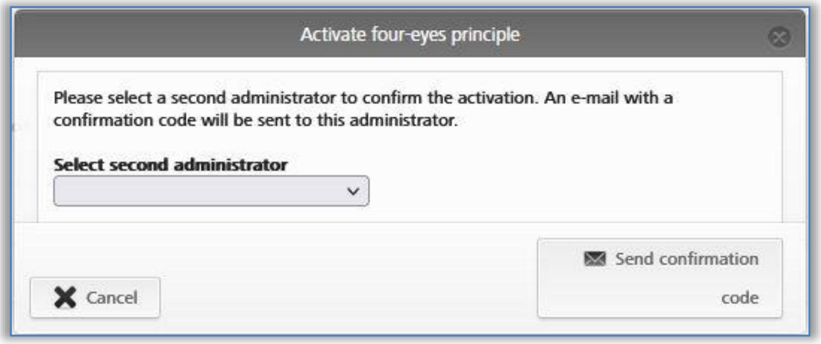
Four-eyes principle for the event log viewing

Deactivated (The administrators can view all event logs WITHOUT needing a confirmation code from a second administrator.)

Activate four-eyes principle

Figure 121: Activating four-eyes principle

- Select a second system administrator from the list to whom a confirmation code should be sent by e-mail and click ***Send confirmation code***.



Activate four-eyes principle

Please select a second administrator to confirm the activation. An e-mail with a confirmation code will be sent to this administrator.

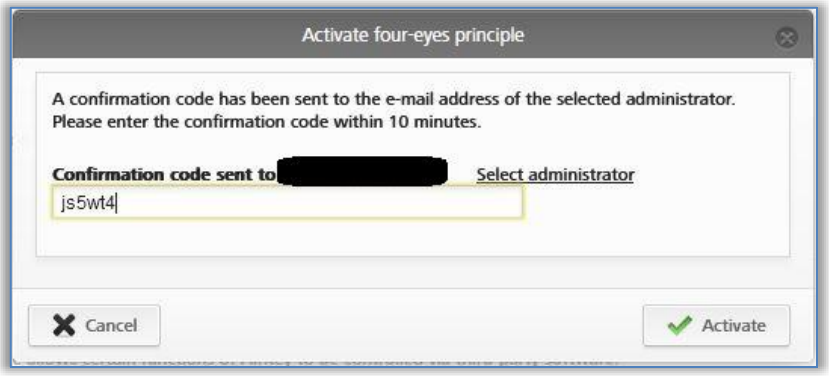
Select second administrator

Cancel

Send confirmation code

Figure 122: Activating four-eyes principle – selecting second administrator

- An e-mail with a confirmation code will then be sent to the selected system administrator.
- This confirmation code must be entered in the AirKey Online Administration within 10 minutes and confirmed with ***Activate***.



Activate four-eyes principle

A confirmation code has been sent to the e-mail address of the selected administrator. Please enter the confirmation code within 10 minutes.

Confirmation code sent to [redacted] Select administrator

js5wt4

Cancel

Activate

Figure 123: Activating four-eyes principle – entering confirmation code

If this process is not completed within 10 minutes, the process must be repeated. If the selected system administrator does not respond, another system administrator can also be selected via the ***Select administrator*** link to activate the four-eyes principle.

You have thus activated the **Four-eyes principle for the event log viewing** for all administrators of this AirKey system. From the next login of a system administrator, the locking component event log and media event log cannot be viewed without the confirmation of a second system administrator.

The system event log is not subject to the four-eyes principle and can be viewed anytime from a system administrator. Sub-administrators cannot view event logs.

For deactivating the **four-eyes principle for the event log viewing** just use the same process as for activating.

Both activation and deactivation are listed in the system event log. The involved system administrators, including the used e-mail address, are logged.

AirKey Cloud Interface (API)

The AirKey Cloud Interface is a REST interface (API) for third-party systems. The interface allows certain functions of AirKey to be controlled via third-party software. Details about the AirKey Cloud Interface can be found in the chapter AirKey Cloud Interface (API).

AirKey Cloud Interface (API) – test environment

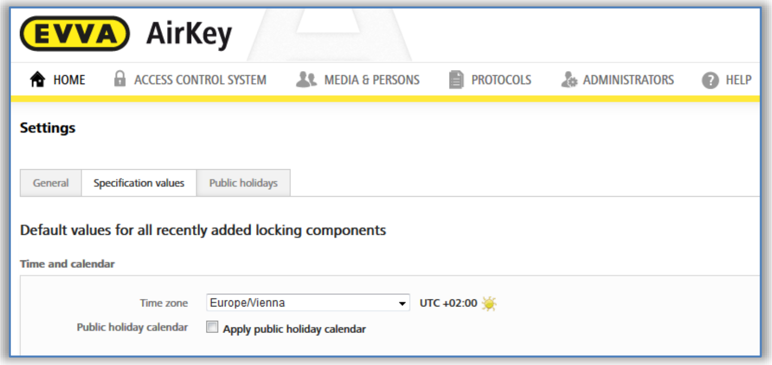
The test environment gives you the opportunity to test the AirKey Cloud Interface (API) in a protected environment with test data before activation. Please refer to the chapter AirKey Cloud Interface (API) for details.

5.4.2 Default values (for all recently added locking components)

These settings are activated automatically if you add a new locking component. We recommend specifying default values prior to the first installation to make it easier to manage systems for administrators. This applies particularly for larger access control systems.

Time and calendar

Access control systems enable the management of locking components located in different time zones. The "Europe/Vienna" time zone (UTC+01:00 in winter and UTC+02:00 in summer), applicable in central Europe, has been set by default.



Settings

Default values for all recently added locking components

Time and calendar

Time zone: Europe/Vienna UTC +02:00

Public holiday calendar: □ Apply public holiday calendar

Figure 124: Default values for new locking components

Simply click the drop-down menu and select the correct time zone from the list if you would like to change the time zone for the entire access control system.

On the ***Home*** screen, click the ***Cylinders*** or ***Wall readers*** tile, select the desired locking component and browse to the ***Settings*** tab if you would like to change the time zone of one locking component. The ***Time and calendar*** section features a drop-down list with the time zones.

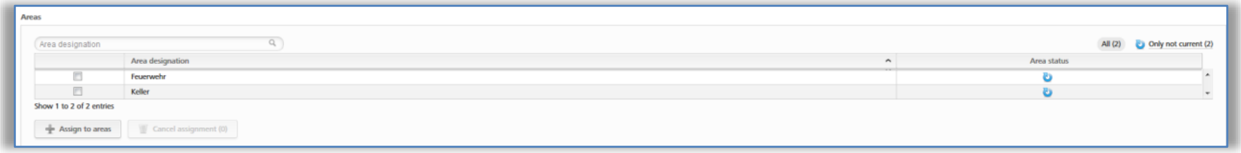
The sun icon in the corresponding time zone section indicates whether summer or winter time is currently active.

☀ Yellow sun = summer time

☀ Grey sun = winter time

Tick the ***Use holiday calendar*** checkbox and the holidays saved and activated in the ***Holidays*** tab (see Holidays section) will be applied to the new locking component.

Areas



Areas

	Area designation	Area status
□	Feuerwehr	↻
□	Keller	↻

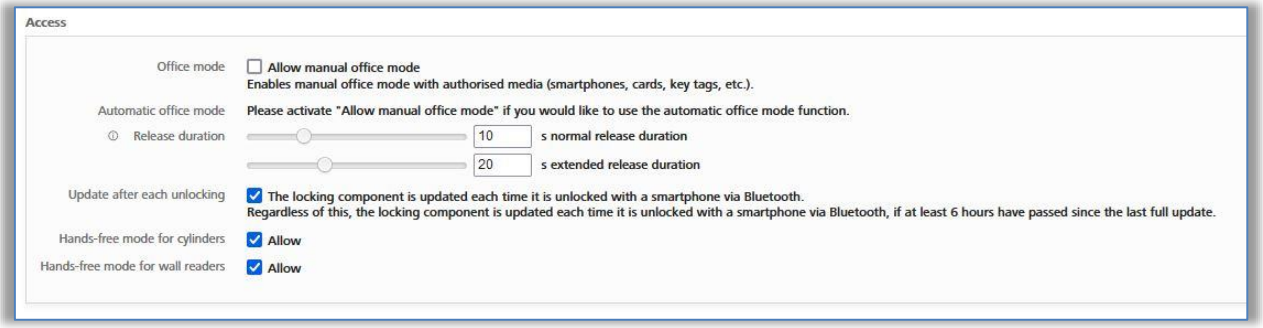
Show 1 to 2 of 2 entries

Figure 125: Default values – areas

This section describes how to automatically assign new locking components to areas you have already created. Please refer to Creating areas for details on where and how to create areas.

This feature is particularly useful for general or fire service keys that must always have access authorisations to all components. It is also possible to once again revoke assigned areas from the corresponding locking components.

Access



Access

Office mode ☐ Allow manual office mode
Enables manual office mode with authorised media (smartphones, cards, key tags, etc.).

Automatic office mode: Please activate "Allow manual office mode" if you would like to use the automatic office mode function.

Release duration: 10 s normal release duration
20 s extended release duration

Update after each unlocking ☑ The locking component is updated each time it is unlocked with a smartphone via Bluetooth.
Regardless of this, the locking component is updated each time it is unlocked with a smartphone via Bluetooth, if at least 6 hours have passed since the last full update.

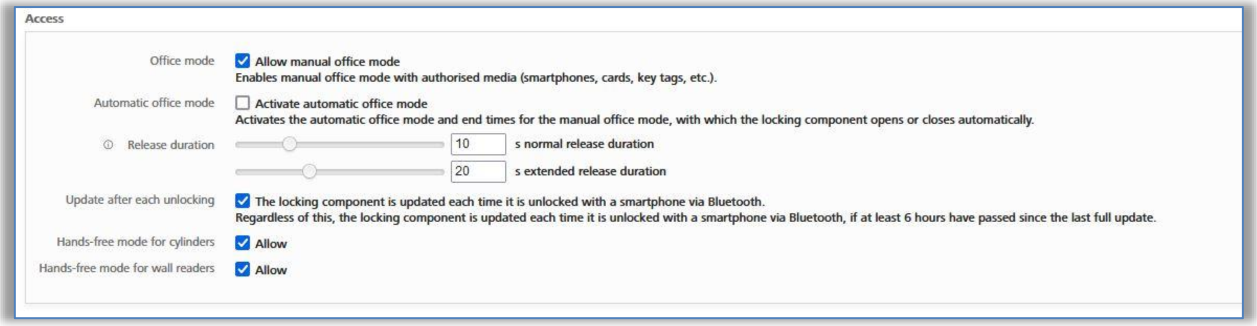
Hands-free mode for cylinders ☑ Allow

Hands-free mode for wall readers ☑ Allow

Figure 126: Default values – access

Here you can allow the manual and automatic office mode, the release duration, the update after each unlocking and the Hands-free mode for cylinders and wall readers for all newly added locking components.

Tick the ***Allow manual office mode*** checkbox to display an additional checkbox: ***Activate automatic office mode***.



Access

Office mode ☑ Allow manual office mode
Enables manual office mode with authorised media (smartphones, cards, key tags, etc.).

Automatic office mode ☐ Activate automatic office mode
Activates the automatic office mode and end times for the manual office mode, with which the locking component opens or closes automatically.

Release duration: 10 s normal release duration
20 s extended release duration

Update after each unlocking ☑ The locking component is updated each time it is unlocked with a smartphone via Bluetooth.
Regardless of this, the locking component is updated each time it is unlocked with a smartphone via Bluetooth, if at least 6 hours have passed since the last full update.

Hands-free mode for cylinders ☑ Allow

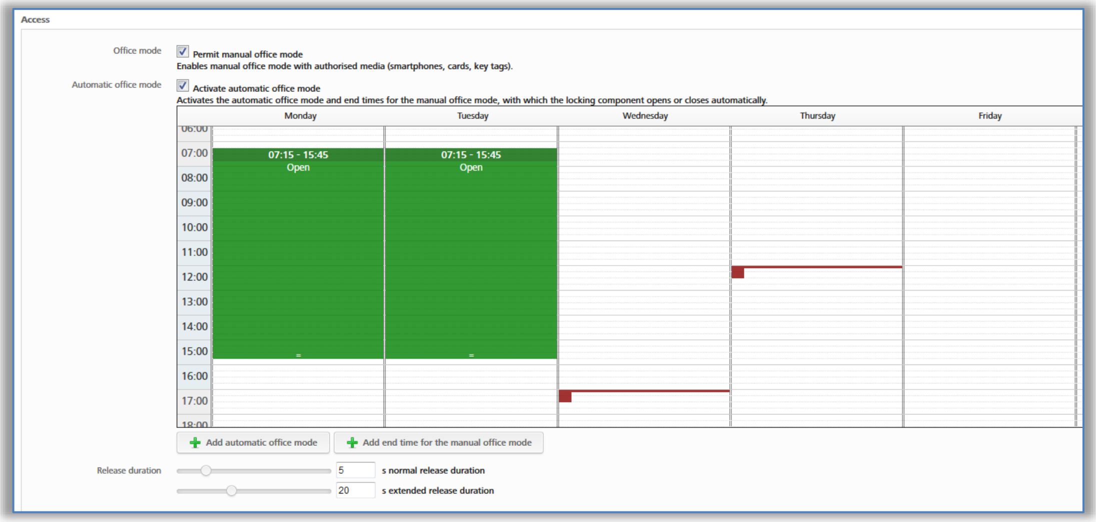
Hands-free mode for wall readers ☑ Allow

Figure 127: Automatic office mode

Automatic office mode permits the specification of periods and unlocking times when the locking component locks or unlocks automatically. For instance, specify that office mode automatically ends each night at 5 pm in an office building. For AirKey cylinders this not only means the door has been locked, but also that the cylinder has been disengaged. Use an authorised medium to engage and subsequently manually unlock a cylinder to open the door.

You can also specify an end time for manual office mode in this dialogue window. This makes sure that office mode is deactivated at this specific time (red bars in the screenshot below), regardless of when it had been activated. You can specify a maximum of 4 entries (periods of time or end time).

Office mode is automatically cancelled, or not started, on holidays, in the event of "battery empty" warnings if the locking component time is incorrect and also during firmware updates.


Access

Office mode ☑ Permit manual office mode
Enables manual office mode with authorised media (smartphones, cards, key tags).

Automatic office mode ☑ Activate automatic office mode
Activates the automatic office mode and end times for the manual office mode, with which the locking component opens or closes automatically.

Release duration 5 s normal release duration
20 s extended release duration

Figure 128: Automatic office mode

The manual office mode can also be activated using access media. In this process, hold the access medium to the locking component, briefly remove it from the reader area and once again hold it to the reader for a second time during the release duration. Proceed identically to end manual office mode.

The release duration specifies how long the locking component is unlocked when using a locking component (i.e. within the context of cylinders this is the period users have to manually turn the cylinder's thumb turn). The standard release duration is 5 seconds and the extended release duration amounts to 20 seconds. Adapt the release duration individually here. The period can be adapted between 1 second and 250 seconds.

The ***Update after each unlocking*** option can be used to activate whether the locking component should be updated after each successful Bluetooth unlocking. Regardless of this, the locking component is updated each time it is unlocked with a smartphone via Bluetooth, if at least 6 hours have passed since the last complete actualisation.

This update is not visible to the user. Neither a signal is shown, nor a message is displayed on the smartphone.

The action can be seen from the administrators in the event log of the AirKey Online Administration.

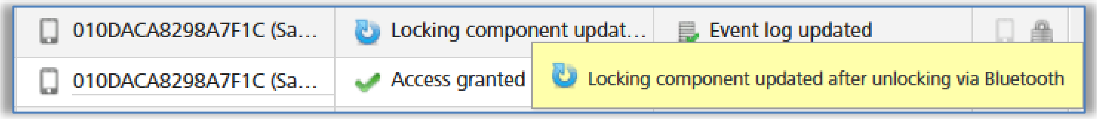

010DACA8298A7F1C (Sa… Locking component updat… Event log updated
010DACA8298A7F1C (Sa… Access granted Locking component updated after unlocking via Bluetooth

Figure 129: Event log – update after unlocking

After a Bluetooth unlocking, only the following data will be updated:

- Blacklist
- Time zone
- Time
- Event logs

The blacklist, the time zone and the time are always updated after a Bluetooth unlocking and the log entries are only updated if the ***Update after each unlocking*** option is activated for the locking component.

If the locking component has other pending maintenance tasks, these must be updated as described in the chapter Updating locking components.

The function depends on the connection quality of the smartphone. Therefore, make sure that you have a stable Internet connection starting with 3G or via Wi-Fi.

The update after a Bluetooth unlocking will also be performed when starting the manual office mode, but not when it is ending.

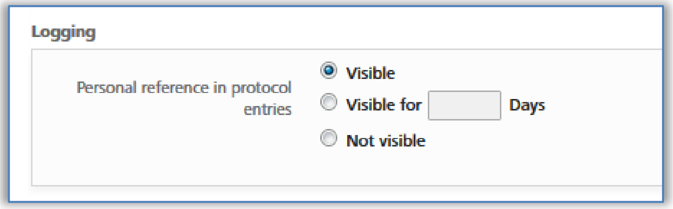
The update after a Bluetooth unlocking takes place within the release duration of the locking component. If the release duration is less than 10 seconds, the update after a Bluetooth unlocking may not work. For this reason, when the function is activated, the value of the normal release duration is automatically set to 10 seconds.

Activating this function increases the battery consumption of battery-powered locking components, such as an AirKey cylinder, and thus affects battery life.

The options ***Hands-free mode for cylinders*** and ***Hands-free mode for wall readers*** are used to allow or not allow the Hands-free mode for all components of the selected component type within the access control system. In addition, it is also possible to select the option for each locking component itself. Details about the changing the configuration for individual locking components can be found in chapter Editing locking components.

Logging

Select the default value for the logging of personal data in event log entries within the context of access events. Three radio buttons are available for this purpose:



Logging

Personal reference in protocol entries

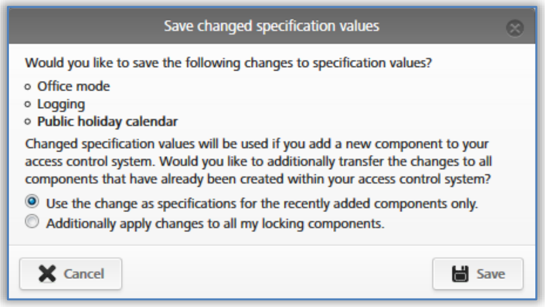
● Visible
○ Visible for ____ Days
○ Not visible

Figure 130: Defining logging / event logs

- ***Visible*** permanently switches on the displaying of personal data for access events.
- ***Visible for … days*** renders personal data for access events anonymous after the defined number of days.
- ***Not visible*** immediately renders all personal data for access events anonymous.

Specified default values can be changed for individual locking components, regardless of the settings specified here.

Click the ***Save*** button to save changed default values. For this purpose, a prompt appears asking to specify whether the changed default values must exclusively apply to recently added or all locking components.


Save changed specification values

Would you like to save the following changes to specification values?

- Office mode
- Logging
- **Public holiday calendar**

Changed specification values will be used if you add a new component to your access control system. Would you like to additionally transfer the changes to all components that have already been created within your access control system?

● Use the change as specifications for the recently added components only.

○ Additionally apply changes to all my locking components.

Figure 131: Save changed specification values?

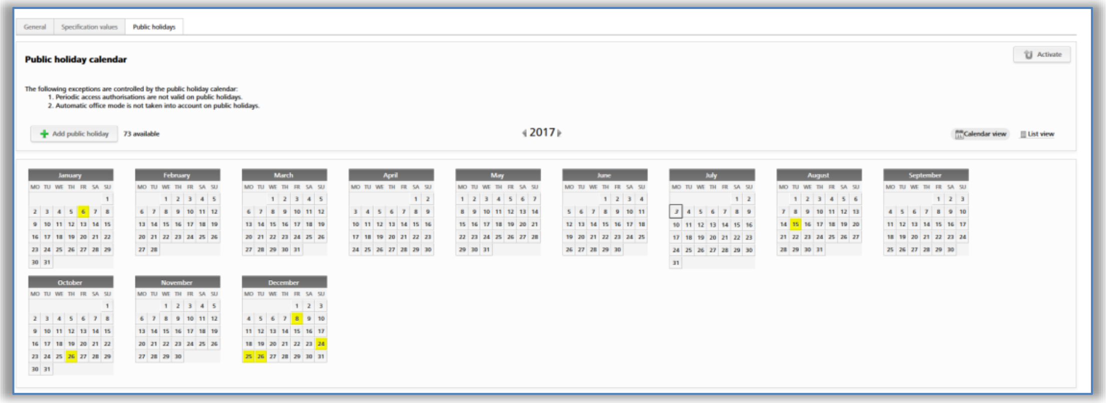
5.4.3 Holidays

Define up to 80 holidays per year in the ***Holidays*** tab (current year and two following years). In AirKey the term "holiday" can be interpreted as a general bank holiday or a period of several days, such as company holidays or school holidays (may reoccur). For instance, specify that a national, public holiday falling on the same date each year is re-entered each year. One week of school holidays merely counts as one holiday in the system if the period was defined with between "Start – End".

Effects of the holiday calendar:

1. Periodic access authorisations are not valid on holidays.
2. Automatic office mode is ignored on holidays.

Click the ***Activate*** button on the right-hand side to globally enable the holiday calendar.

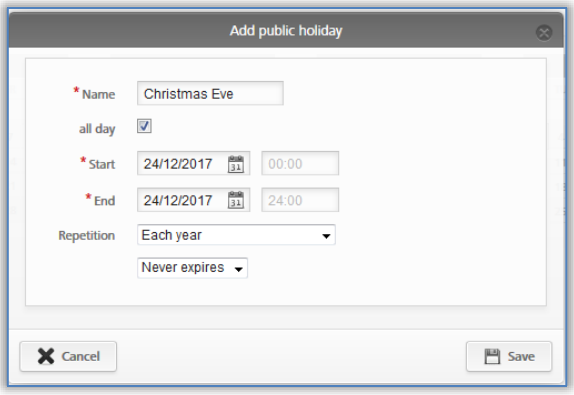

Public holiday calendar

The following exceptions are controlled by the public holiday calendar:
1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

73 available

Figure 132: Holiday calendar (calendar view)

Click the ***Add holiday*** button or click the exact date of the holiday in the calendar view (e.g. 24/12) to open a dialogue window to enter the name of the holiday, specify whether the holiday applies for the entire day or, e.g. the afternoon only, and between which periods the holiday applies (e.g. also specify company holidays here), define how many times it reoccurs and when the specification no longer applies.



*Name: Christmas Eve
all day: ☑
*Start: 24/12/2017 00:00
*End: 24/12/2017 24:00
Repetition: Each year
Never expires

Figure 133: Adding holidays

You can retrospectively edit each entered holiday. For this purpose, simply click the corresponding day to open a text box.

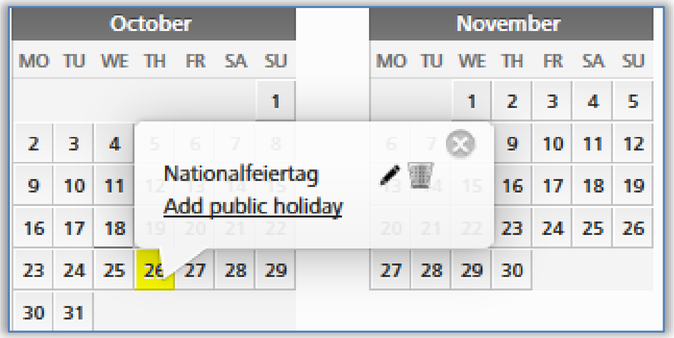
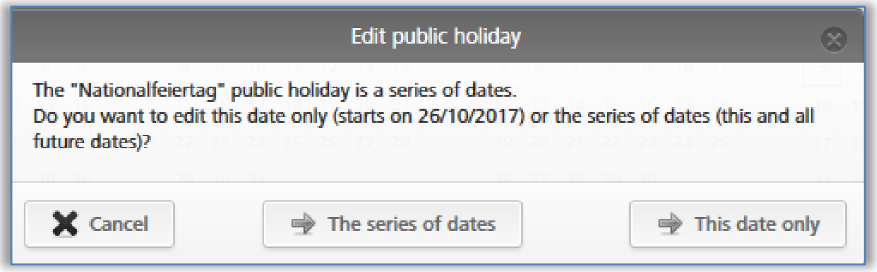


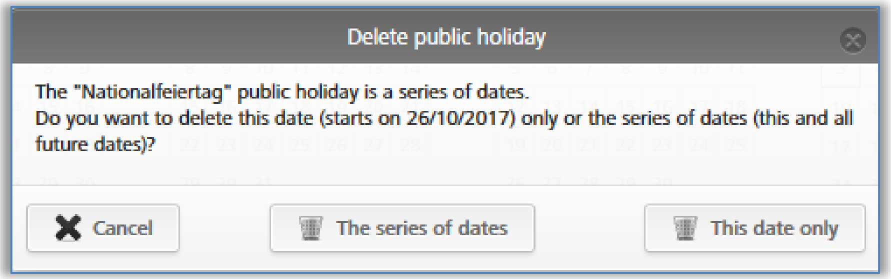
Figure 134: Adding holidays in the calendar

Click the ***Add holiday*** link to add a further holiday on this day. You can enter several holidays on one calendar day. Click the pen icon to edit the holiday. Click the bin to delete the holiday.



The "Nationalfeiertag" public holiday is a series of dates.
Do you want to edit this date only (starts on 26/10/2017) or the series of dates (this and all future dates)?

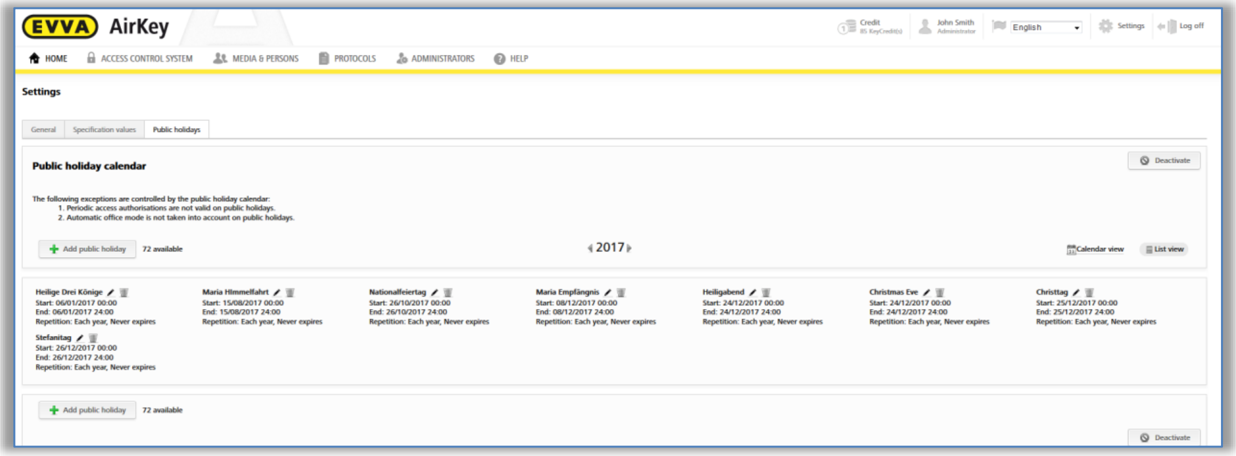
Figure 135: Editing holidays



The "Nationalfeiertag" public holiday is a series of dates.
Do you want to delete this date (starts on 26/10/2017) only or the series of dates (this and all future dates)?

Figure 136: Deleting holidays

As soon as you have entered deadlines, (company) holidays or holidays in the calendar, the system shows you a list overview of all saved holidays, etc.



Public holiday calendar

The following exceptions are controlled by the public holiday calendar:

1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

72 available

Heilige Drei Könige
Start: 06/01/2017 00:00
End: 06/01/2017 24:00
Repetition: Each year, Never expires

Stefanitag
Start: 26/12/2017 00:00
End: 26/12/2017 24:00
Repetition: Each year, Never expires

Maria Himmelfahrt
Start: 15/08/2017 00:00
End: 15/08/2017 24:00
Repetition: Each year, Never expires

Nationalfeiertag
Start: 26/10/2017 00:00
End: 26/10/2017 24:00
Repetition: Each year, Never expires

Maria Empfängnis
Start: 08/12/2017 00:00
End: 08/12/2017 24:00
Repetition: Each year, Never expires

Heiligabend
Start: 24/12/2017 00:00
End: 24/12/2017 24:00
Repetition: Each year, Never expires

Christmas Eve
Start: 24/12/2017 00:00
End: 24/12/2017 24:00
Repetition: Each year, Never expires

Christtag
Start: 25/12/2017 00:00
End: 25/12/2017 24:00
Repetition: Each year, Never expires

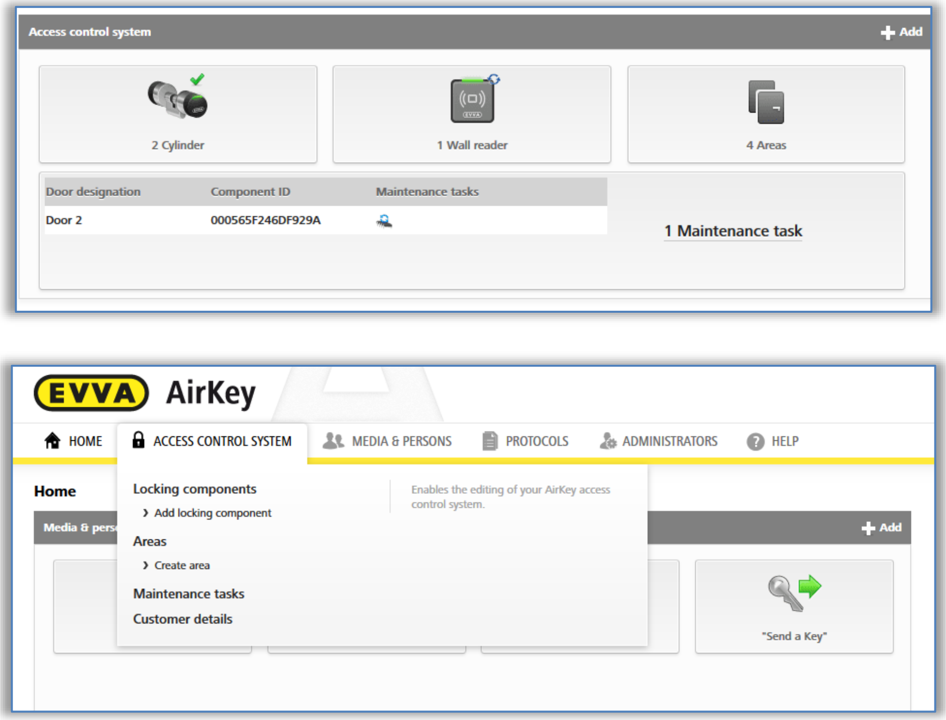
72 available

Figure 137: Holiday calendar (list view)

Select the ***Deactivate*** button to globally deactivate the holiday calendar for the access control system and not save it for added locking components.

5.5 Access control system

Thanks to the tiles on the ***Home*** screen as well as the menus and sub-menus in the ***Access control system*** main menu you can manage your electronic access control system.



Access control system

+ Add

2 Cylinder

1 Wall reader

4 Areas

Door designation	Component ID	Maintenance tasks
Door 2	000565F246DF929A	

1 Maintenance task

Locking components
› Add locking component
Areas
› Create area
Maintenance tasks
Customer details

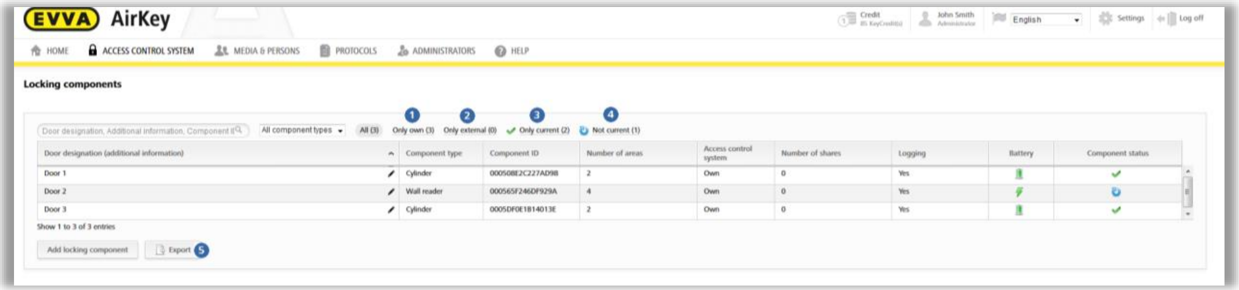
Enables the editing of your AirKey access control system.

Figure 138: Access control system

5.5.1 Locking component overview

For an overview of all locking components within your access control system from the ***Home*** screen click the ***Cylinders*** or ***Wall readers*** tile or go to ***Access control system*** → ***Locking components*** in the main menu. The ***Home*** screen shows how many cylinders or wall readers have been integrated into your access control system at a glance.

All locking components with additional information as well as their status are listed. The first row of the list features the search field as well as filter functions for locking components.



Locking components

Door designation, Additional information, Component I

All component types

All (3) | Only own (3) | Only external (0) | ✓ Only current (2) | Not current (1)

Door designation (additional information)	Component type	Component ID	Number of areas	Access control system	Number of shares	Logging	Battery	Component status
Door 1	Cylinder	000508E2C227AD9B	2	Own	0	Yes	▮	✓
Door 2	Wall reader	000565F246DF929A	4	Own	0	Yes	⚡	↻
Door 3	Cylinder	0005DF0E1814013E	2	Own	0	Yes	▮	✓

Show 1 to 3 of 3 entries

Add locking component | Export

Figure 139: Locking components

- "Only own" ❶ exclusively lists your own locking components
- "Only external" ❷ exclusively lists locking components that have been authorised by an administrator.
- "Only current" ❸ exclusively lists locking components where the status is up to date.

- "Not current" ❹ exclusively lists locking components where the status is not up to date.
- Export the locking component list to a CSV file for further processing ❺.

AirKey allows an authorisation of locking components for external access control systems. The list differentiates between your own and external locking components. Please refer to Sharing locking components for other access control systems for more information.

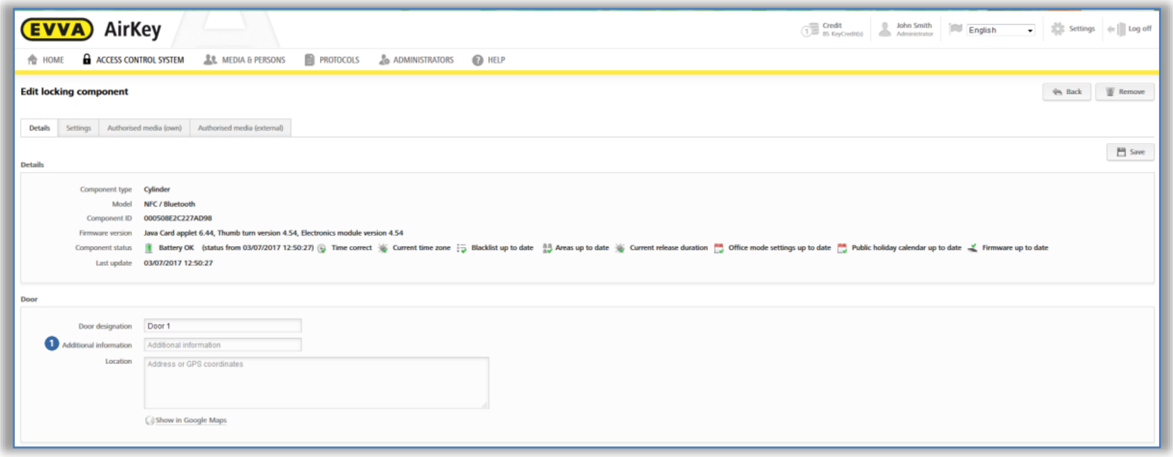
5.5.2 Adding locking components: See chapter 4.11

5.5.3 Editing locking components

The ***Edit locking component*** application window in the ***Details*** tab provides different information, such as component type and model, component ID, firmware version or component status as well as information about doors, areas, and authorisations. You also have the option here to show locking component locations in Google Maps. The ***Settings*** tab shows all configured settings relating time zone and holiday calendar, access as well as logging and repair options.

The battery status shown corresponds to the status at the last update or the last transferred event log entry. For this reason, the actual battery status of the locking component may deviate from the battery status shown in the AirKey Online Administration.

- On the ***Home*** screen, click the ***Cylinders*** or ***Wall readers*** tile.
- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the locking component you would like to edit in the list.
- For instance, assign an optional door designation in the **Details** tab add optional information ❶ or enter the location or address of locking components. The unique characteristics of this data are verified within the access control system.



Edit locking component

Details

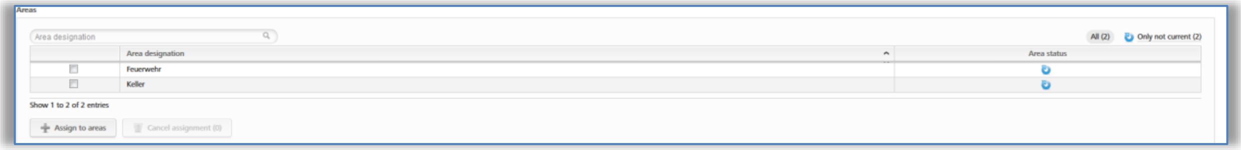
Component type: Cylinder
Model: NFC / Bluetooth
Component ID: 000508E2C227AD98
Firmware version: Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status: Battery OK (status from 03/07/2017 12:50:27) Time correct Current time zone Blacklist up to date Areas up to date Current release duration Office mode settings up to date Public holiday calendar up to date Firmware up to date
Last update: 03/07/2017 12:50:27

Door

Door designation: Door 1
1 Additional information: Additional information
Location: Address or GPS coordinates

Figure 140: Editing locking components

- Go to the Areas section to edit assigned areas for selected locking components.



Areas

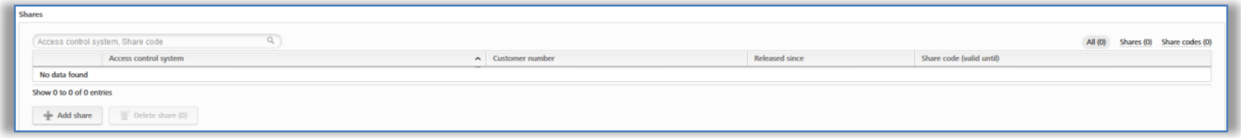
Area designation 🔍 | All (2) | Only not current (2)

	Area designation	Area status
□	Feuerwehr	↻
□	Keller	↻

Show 1 to 2 of 2 entries

Figure 141: Areas

- You can optionally also authorise locking components for other access control systems. You can manage the corresponding authorisations in the "Authorisations" section. Please refer to Working with several access control systems for more information about authorisations.



Shares

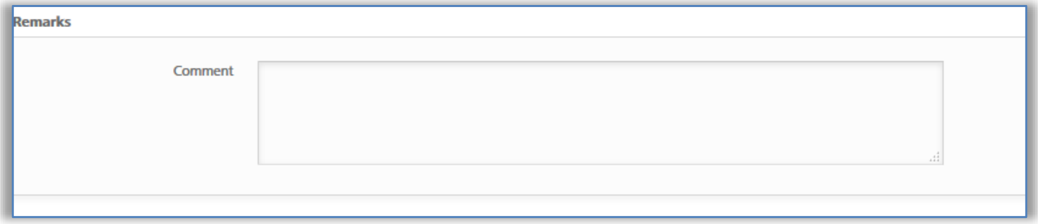
Access control system, Share code 🔍 | All (0) | Shares (0) | Share codes (0)

	Access control system	Customer number	Released since	Share code (valid until)
No data found				

Show 0 to 0 of 0 entries

Figure 142: Shares

- You can optionally enter a comment on a locking component in the ***Remarks*** section.



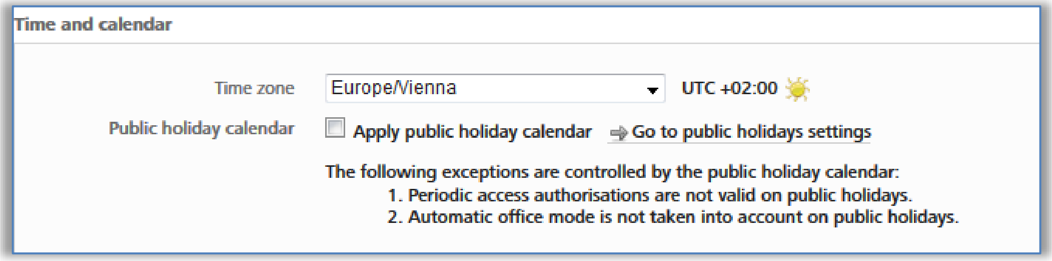
Remarks

Comment

Figure 143: Editing locking components

As mentioned above, you can manage time zones and holiday calendar, access or logging and repair options in the ***Settings*** tab.

- If you use several time zones within a single access control system, you can assign an individual time zone to each locking component. The default time zone is used as standard.
- In this process, you can (de)activate the holiday calendar for each locking component. There is a link to the holiday calendar in case you need to double-check on some holiday settings.



Time and calendar

Time zone: Europe/Vienna — UTC +02:00

Public holiday calendar: □ Apply public holiday calendar

The following exceptions are controlled by the public holiday calendar:

1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

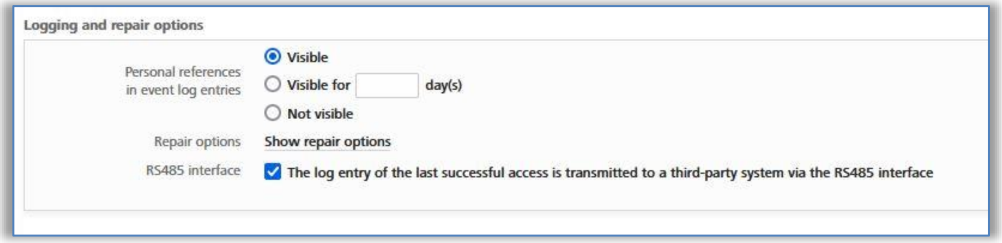
Figure 144: Settings – time and calendar

- You can specify manual office mode for each locking component. Select a locking component and you will have the option to specify automatic office mode.

In addition, you can change the release duration and activate or deactivate the "Update after each unlocking" function. Please also refer to Default values (for all recently added locking components).

In addition, the Hands-free mode can be allowed or not allowed for the individual locking component. If the Hands-free mode is allowed, the Hands-free mode can be activated for this locking component within the AirKey app. Otherwise, it cannot be activated in the app for this locking component. Details about the Hands-free mode can be found in the chapter Hands-free at a glance.

- You can adapt the logging of personal data in event log entries for each locking component. The default settings are used as standard.
  - ***Visible*** permanently switches on the displaying of personal data for access events.
  - ***Visible for … days*** renders personal data for access events anonymous after the defined number of days.
  - ***Not visible*** immediately renders all personal data for access events anonymous.



Logging and repair options

Personal references in event log entries
● Visible
○ Visible for ☐ day(s)
○ Not visible

Repair options: Show repair options

RS485 interface: ☑ The log entry of the last successful access is transmitted to a third-party system via the RS485 interface

Figure 145: Event logs

- This section provides the link to the repair options. You can find further details in the chapter Repair options.
- Compared to all other locking components, Bluetooth wall readers also offer the option to activate the ***RS485 interface***. The log entry of the last successful access can be forwarded to a third-party system via the RS485 interface. You can find further details in the chapter Technical details for the RS485 interface of Bluetooth wallreader.
- Click ***Save*** to confirm any changes to the locking component. A confirmation prompt subsequently appears.

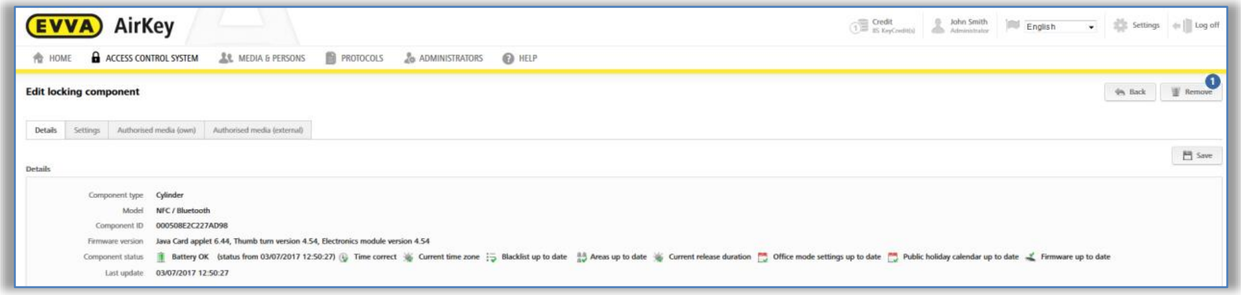
A maintenance task for this locking component may appear depending on the locking component data you edited. The changes are accepted and the maintenance task disappears after having updated the locking component using a smartphone with maintenance authorisation or a coding station.

5.5.4 Removing locking components

You can remove locking components from your access control system if you no longer require them in your access control system.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.

- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the listed locking component you would like to delete from your AirKey system.
- Click ***Remove*** ❶ at the top right.



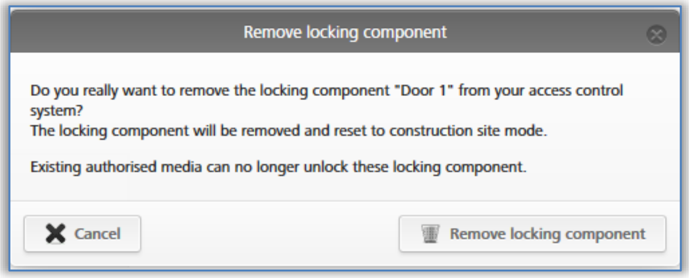
Edit locking component

Details

Component type Cylinder
Model NFC / Bluetooth
Component ID 000508E2C227AD98
Firmware version Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status Battery OK (status from 03/07/2017 12:50:27) Time correct Current time zone Blacklist up to date Areas up to date Current release duration Office mode settings up to date Public holiday calendar up to date Firmware up to date
Last update 03/07/2017 12:50:27

Figure 146: Removing locking components

- Click ***Remove locking component*** to confirm the security prompt.



Remove locking component

Do you really want to remove the locking component "Door 1" from your access control system?
The locking component will be removed and reset to construction site mode.

Existing authorised media can no longer unlock these locking component.

Figure 147: Security prompt

- A confirmation prompt and a maintenance task appear, indicating the locking component must be removed from the access control system.

The process has only been completed once the locking component has been updated using a smartphone with maintenance authorisation or an optionally available coding station. As soon as the locking component has been updated it has been successfully removed from the access control system.

⚠ This process is irrevocable.

The locking component is reset to factory state after having removed it.

Any previously authorised access media are no longer valid to unlock locking components. Corresponding authorisations are automatically deleted and no longer shown.

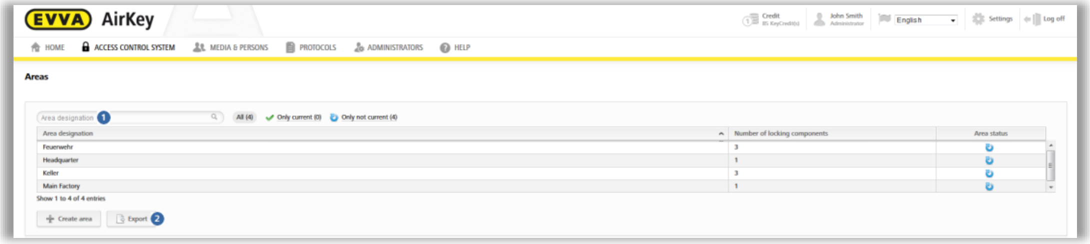
5.5.5 Areas

You can merge several locking components to areas to make it easier to manage authorisations in your access control system.

On the ***Home*** screen, click the ***Areas*** tile or select ***Access control system*** → ***Areas*** in the main menu for a list of all areas including their individual states.

The list of areas enables the following adaptations:

- Enter a search term with a minimum of three characters in the search field ❶.
- Click the corresponding column heading to determine it as the sorting criterion.
- Export the area list to a CSV file for further processing ❷.



Areas

Area designation	Number of locking components	Area status
Feuerwehr	3	↻
Headquarter	1	↻
Keller	3	↻
Main Factory	1	↻

Show 1 to 4 of 4 entries

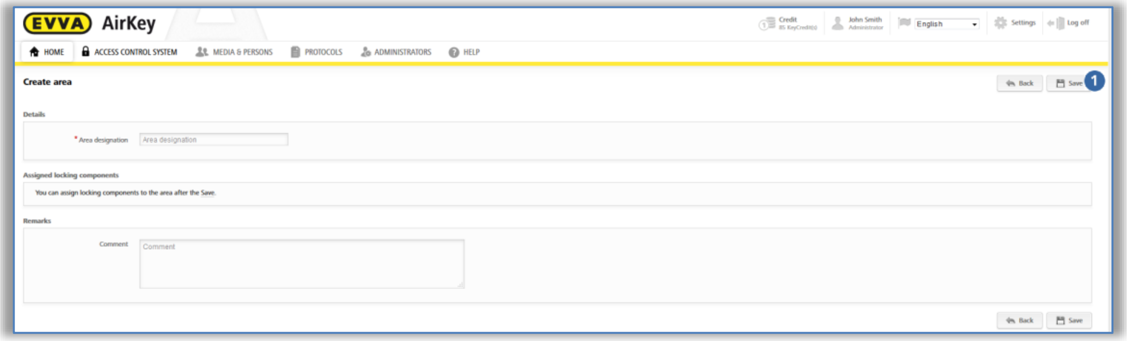
Figure 148: Access control system – areas

- Select the desired area from the list to view the details of the selected area.

5.5.6 Creating areas

No areas have been defined as standard. You must create new areas to be able to add locking components to areas.

- On the ***Home*** screen in the grey ***Access control system*** section, click ***Add*** → ***Create area***.
- Alternatively, select ***Access control system*** → ***Create area*** in the main menu.
- Specify a unique designation for the area.
- Document any additional information on the area in the ***Comment*** field of the ***Remarks*** section.
- Click ***Save*** ❶.



Create area

Details

*Area designation: Area designation

Assigned locking components

You can assign locking components to the area after the Save.

Remarks

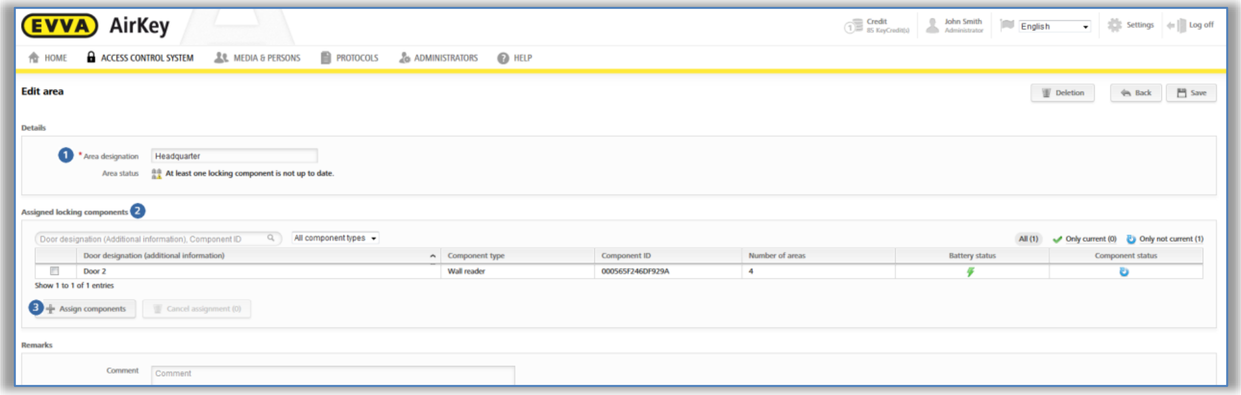
Comment: Comment

Figure 149: Creating areas

The system reports "The area has been saved" once you have created an area. You can only add locking components to areas once they have been successfully saved.

5.5.7 Assigning locking components to areas

- On the ***Home*** screen select the ***Areas*** tile or click ***Access control system*** → ***Areas*** in the main menu.
- Select the area from the list to which you would like to add locking components.
- The details of the selected area appear. ***Area status*** ❶ indicates whether all locking components within the area are up to date. The ***Assigned locking component*** list ❷ lists all locking components assigned to the area.
- Click ***Assign component*** ❸ to add a locking component to the area.



Edit area

Details

* Area designation: Headquarter

Area status: At least one locking component is not up to date.

Assigned locking components

Door designation (Additional information), Component ID | All component types | All (1) | ✓ Only current (0) | Only not current (1)

	Door designation (additional information)	Component type	Component ID	Number of areas	Battery status	Component status
□	Door 2	Wall reader	000565F246DF929A	4	⚡	↻

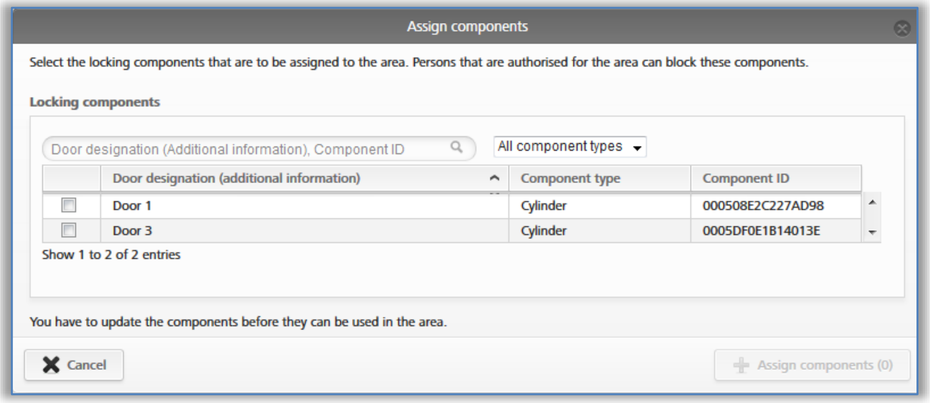
Show 1 to 1 of 1 entries

Remarks

Comment: Comment

Figure 150: Editing areas

A list of all locking components that have not yet been assigned to this area appears.



Select the locking components that are to be assigned to the area. Persons that are authorised for the area can block these components.

Locking components

Door designation (Additional information), Component ID | All component types

	Door designation (additional information)	Component type	Component ID
□	Door 1	Cylinder	000508E2C227AD98
□	Door 3	Cylinder	0005DF0E1B14013E

Show 1 to 2 of 2 entries

You have to update the components before they can be used in the area.

Figure 151: Assigning components

- Select the desired locking components (multiple locking component selections (also different types) are possible).
- Click ***Assign components*** to assign the locking components to the area.
- Click ***Save*** to confirm the changes.

Maintenance tasks are created for the affected locking components that are deleted from the list by updating the corresponding locking components using a smartphone or coding station. You have completed assigning locking components to areas after having updated.

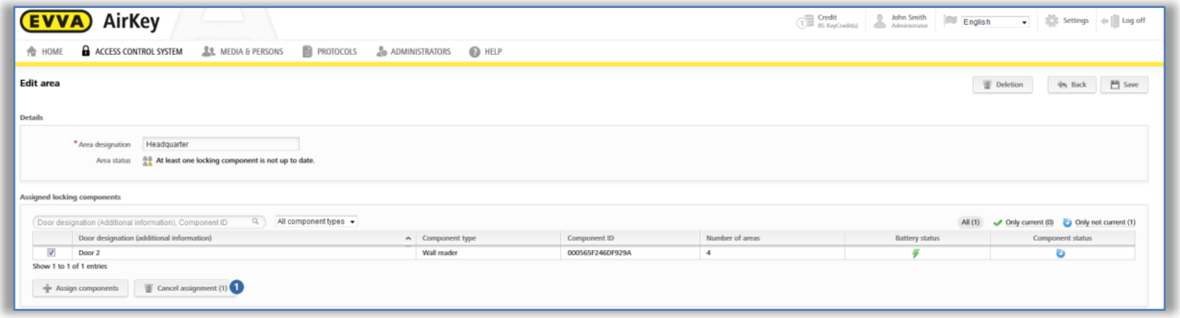
A locking component can be assigned to a maximum of 96 areas.

Alternatively, you can also directly edit the area assignments of locking components in the locking component details. Please refer to Editing locking components for more information.

5.5.8 Cancelling locking component assignments to an area

Proceed as follows to cancel assignments of one or more locking components to an area:

- On the ***Home*** screen select the ***Areas*** tile or click ***Access control system*** → ***Areas*** in the main menu.
- Select the area from the list in which you would like to cancel the locking component assignment.
- Tick the checkboxes of the locking components for which you would like to cancel the assignments to areas. You can select multiple entries.



Edit area

Details

* Area designation: Headquarter

Area status: At least one locking component is not up to date.

Assigned locking components

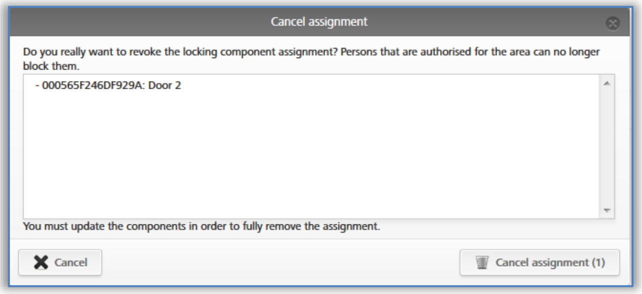
Door designation (Additional information), Component ID

	Door designation (additional information)	Component type	Component ID	Number of areas	Battery status	Component status
☑	Door 2	Wall reader	000565F246DF929A	4		

Show 1 to 1 of 1 entries

Figure 152: Highlighting locking components

- Click ***Cancel assignments*** ❶.
- A dialogue window appears that once again lists the locking components for which the assignments to an area are to be cancelled.
- Also confirm this dialogue with ***Cancel assignment***.



Do you really want to revoke the locking component assignment? Persons that are authorised for the area can no longer block them.

- 000565F246DF929A: Door 2

You must update the components in order to fully remove the assignment.

Figure 153: Cancelling assignments

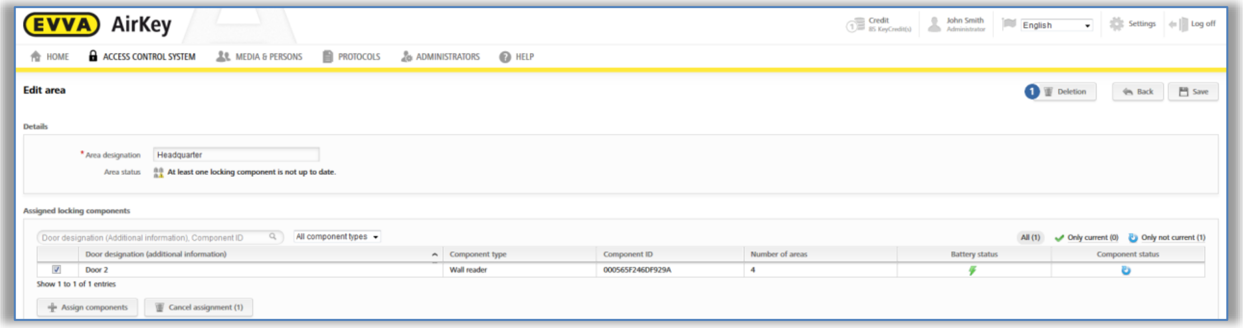
Maintenance tasks are created for the affected locking components that are deleted from the list by updating the corresponding locking components using a smartphone or coding station. You have completed assigning locking components to areas after having updated.

After having updated, persons with media featuring authorisations for this area will be unable to unlock the locking component for which you cancelled the assignment.

Alternatively, you can also directly edit the area assignments of locking components in the locking component details. Please refer to Editing locking components for more information.

5.5.9 Deleting area

- On the ***Home*** screen select the ***Areas*** tile or click ***Access control system*** → ***Areas*** in the main menu.
- Select the area you would like to delete from the list.
- Click ***Delete*** ❶.



Edit area

Details

* Area designation: Headquarter

Area status: At least one locking component is not up to date.

Assigned locking components

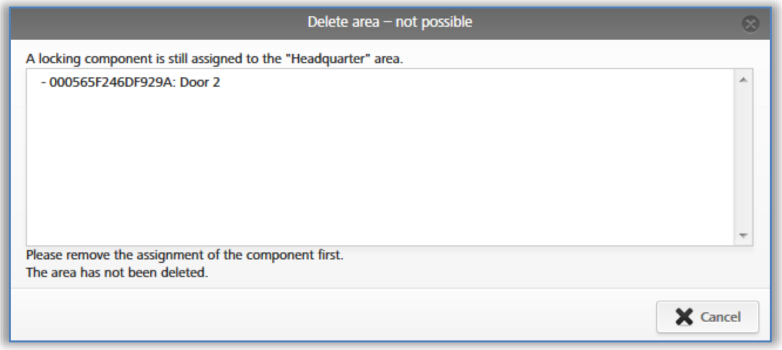
	Door designation (additional information)	Component type	Component ID	Number of areas	Battery status	Component status
☑	Door 2	Wall reader	000565F246DF929A	4	⚡	↻

Show 1 to 1 of 1 entries

Figure 154: Deleting areas

Any existing authorisations on media for a deleted area are automatically deleted and no longer shown. Deletion is irrevocable.

An error message appears if locking components are still assigned to the/this area.



Delete area – not possible

A locking component is still assigned to the "Headquarter" area.

- 000565F246DF929A: Door 2

Please remove the assignment of the component first.
The area has not been deleted.

Figure 155: Deleting areas – not possible

For this reason, initially cancel all locking component assignments to the area and subsequently repeat the illustrated process. Please refer to Cancelling locking component assignments to an area for more information on assigning locking components to areas.

5.5.10 Authorisation overview

The authorisation overview shows all authorisations of media for each individual locking component. The authorisation overview relates to the selected locking component.

All media with authorisations for this locking component are listed. However, the authorisations displayed must not necessarily be currently valid, i.e. media with temporary, single access between 8 am and 5 pm will also be displayed for locking components after 5 pm in the authorisation overview.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile or click ***Access control system*** → Locking components.
- Select the locking component for which you would like to view the authorisation overview from the list.
- Browse from the ***Details*** tab to ***Authorised media (own)*** to view the authorisations of your own system or select ***Authorised media (external)*** to view authorisations from other systems for which the locking component has been authorised.

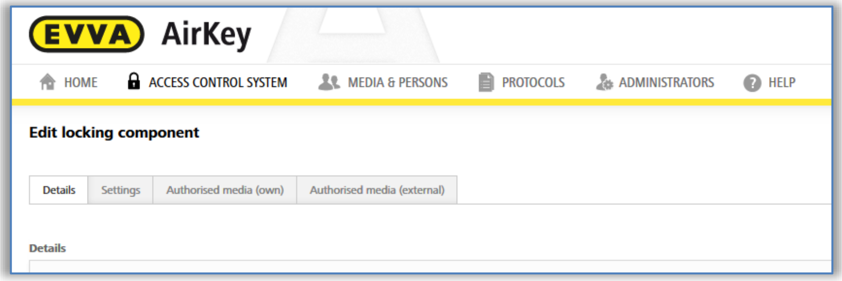
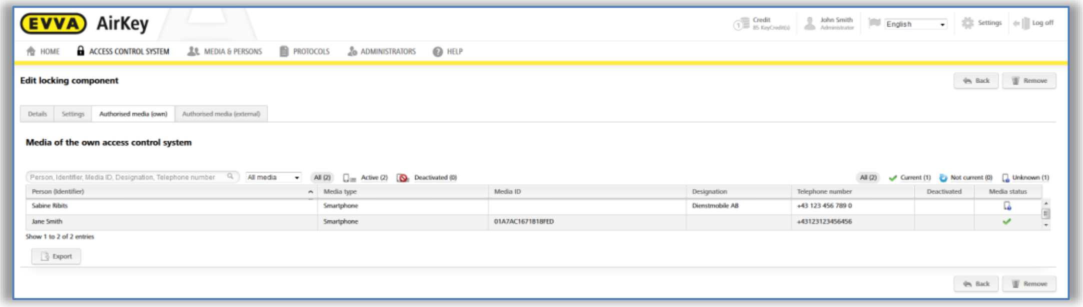


Figure 156: "Editing locking components" page tabs

You are provided with a list of all persons as well as the associated persons. You can also view the media type.



Edit locking component

Media of the own access control system

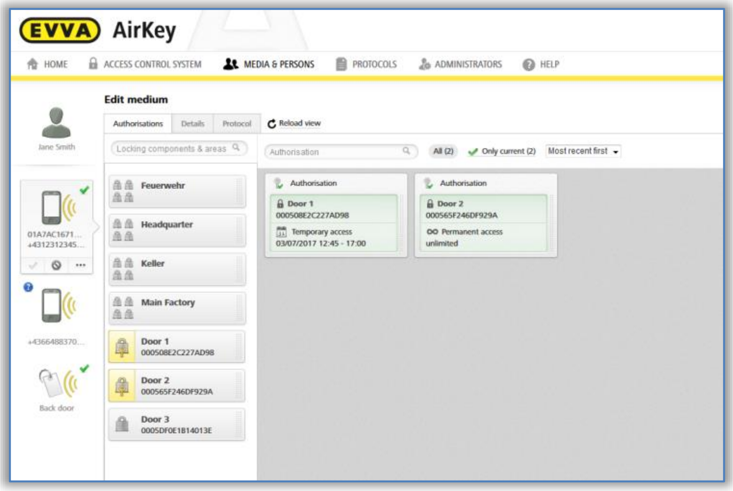
Person (Identifier)	Media type	Media ID	Designation	Telephone number	Deactivated	Media status
Sabine Ribits	Smartphone		Dienstmobile AB	+43 123 456 789 0		
Jane Smith	Smartphone	01A7AC1671818FED		+43123123456456		✓

Show 1 to 2 of 2 entries

Figure 157: Authorised media (own)

You can search, filter or sort this list to view certain authorisations.

Click a person’s name to directly view this person’s authorisation for the medium.



Edit medium

Jane Smith

01A7AC1671...
+4312312345...

+4366488370...

Back door

Feuerwehr

Headquarter

Keller

Main Factory

Door 1
000508E2C227AD98

Door 2
000565F246DF929A

Door 3
0005DF0E1B14013E

Authorisation
Door 1
000508E2C227AD98
Temporary access
03/07/2017 12:45 - 17:00

Authorisation
Door 2
000565F246DF929A
Permanent access
unlimited

Figure 158: Editing media

5.5.11 Maintenance tasks

Certain functions influence the locking component configuration. Such changes to the configuration are known as maintenance tasks. Consequently, maintenance task relate to locking components where the status is not up to date.

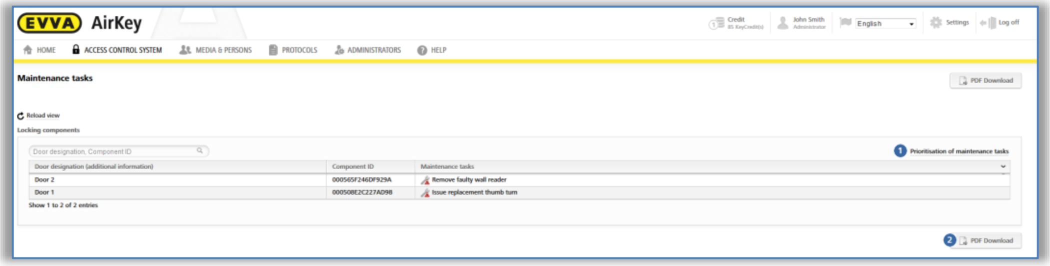
Proceed as follows to view a list of up-to-date maintenance tasks within the access control system:

- On the ***Home*** screen select the ***Maintenance tasks*** link.
- Alternatively click ***Maintenance tasks*** in the status bar.
- You can also select ***Access control system*** → ***Maintenance tasks*** in the main menu.

This section provides a transparent list of maintenance tasks for locking components within your access control system.

You can search for door designations or component IDs in the list of maintenance tasks. You can sort the "Door designation (additional information)", "Component ID", and "Maintenance tasks" columns.

You can also prioritise maintenance tasks ❶ and create a PDF file ❷ to print.



Maintenance tasks

Locking components

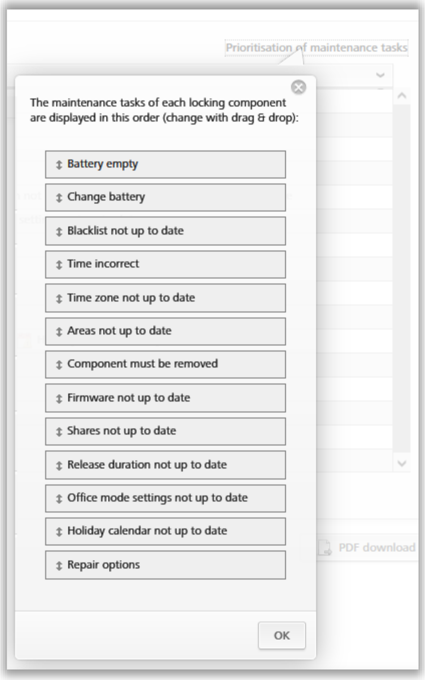
Door designation (additional information)	Component ID	Maintenance tasks
Door 2	000565F246DF929A	Remove faulty wall reader
Door 1	000508E2C227AD98	Issue replacement thumb turn

Show 1 to 2 of 2 entries

Figure 159: Maintenance tasks

Prioritisation of the maintenance tasks is saved per AriKey system / client and also applies to the smartphone app with installed AirKey app and activated maintenance authorisation.

- Click ***Prioritisation of maintenance tasks***.
- Customers have different demands – depending on the applications, drag and drop ❶ the items into the desired order.
- Click ***OK*** to save the changed prioritisation.



The maintenance tasks of each locking component are displayed in this order (change with drag & drop):

- ↕ Battery empty
- ↕ Change battery
- ↕ Blacklist not up to date
- ↕ Time incorrect
- ↕ Time zone not up to date
- ↕ Areas not up to date
- ↕ Component must be removed
- ↕ Firmware not up to date
- ↕ Shares not up to date
- ↕ Release duration not up to date
- ↕ Office mode settings not up to date
- ↕ Holiday calendar not up to date
- ↕ Repair options

Figure 160: Prioritisation of maintenance tasks

The list of maintenance tasks is now shown with changed priorities. Individual items on the list with maintenance tasks have been linked to the detailed pages of the corresponding locking components.

Once a maintenance task has been completed by updating the locking component, the item is automatically removed from the list of maintenance tasks.

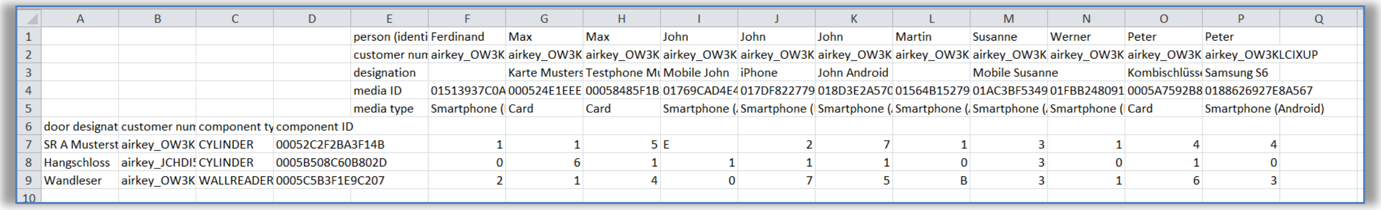
You can create the list of all due maintenance tasks as a PDF file and print it. For this purpose, click the ***PDF download*** button.

5.5.12 Customer data – locking chart

As described before, open the ***Customer data*** menu to retrospectively change information entered upon registration, e.g. the name of the access control system, company name or also the contacts.

The "Edit customer data" page features a button at the top right to export a locking chart for the entire access control system. The locking chart is an overview of all locking components within an access control system as well as its assigned smartphones and access media.

- Click the ***Export locking chart*** button.
- Select the ***Export*** button in the "Export locking chart" dialogue window.
- Click the link of the CSV file that appears in the next dialogue window.
- Open the CSV file with the desired program or save the file.
- Click the ***Close*** button to close the "Export locking chart" dialogue window.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1					person (identi	Ferdinand	Max	Max	John	John	John	Martin	Susanne	Werner	Peter	Peter	
2					customer nun	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3KLCIXUP	
3					designation		Karte Musters	Testphone Mu	Mobile John	iPhone	John Android		Mobile Susanne		Kombischlüss	Samsung S6	
4					media ID	01513937C0A	000524E1EEE	00058485F1B	01769CAD4E4	017DF822779	018D3E2A570	01564B15279	01AC3BF5349	01FBB248091	0005A7592B8	0188626927E8A567	
5					media type	Smartphone (	Card	Card	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Card	Smartphone (Android)	
6	door designat	customer nun	component ty	component ID													
7	SR A Musterst	airkey_OW3K	CYLINDER	00052C2F2BA3F14B		1	1	5	E	2	7	1	3	1	4	4	
8	Hangschloss	airkey_JCHDI5	CYLINDER	0005B508C60B802D		0	6	1	1	1	1	0	3	0	1	0	
9	Wandleser	airkey_OW3K	WALLREADER	0005C5B3F1E9C207		2	1	4	0	7	5	B	3	1	6	3	
10																	

Figure 161: Locking chart

The AirKey Online Administration status is used to calculate the authorisation status, not the ACTUAL status on the medium. Consequently, the locking chart is only correct if all components and media are up to date.

Locking chart legend:

- **0 – Not authorised:** medium not authorised for the locking component or any area assigned to the locking component.
- **1 – Permanent authorisation without expiry date:** medium features exactly one permanent authorisation without expiry date for the locking component or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.
- **2 – Permanent authorisation with expiry date:** (1) does not apply as the medium features exactly one permanent authorisation for the locking component with expiry date in the future or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.
- **3 – Periodic authorisation without expiry date:** (1) and (2) do not apply as the medium features exactly one periodically valid authorisation without expiry date for the locking component or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.
- **4 – Periodic authorisation with expiry date:** (1), (2) and (3) do not apply as the medium features exactly one periodically valid authorisation for the locking component with expiry date in the future or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.
- **5 – Single authorisation:** (1), (2), (3) and (4) do not apply as the medium features exactly one single authorisation for the locking component with expiry date in the future or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.

- **6 – Individual authorisation:** (1), (2), (3), (4) and (5) do not apply as the medium features exactly one individual authorisation with a minimum of one sub-authorisation for the locking component with expiry date in the future or one area to which the locking component has been assigned to and no other authorisations for the locking component or an area assigned to the locking component.
- **7 – Multiple authorisations:** medium features a minimum of two authorisations for the locking component or any area assigned to the locking component that have not expired yet.
- **B – Blacklist:** medium deactivated, i.e. on the locking component blacklist. This will invalidate any authorisations on media.
- **E – Expired authorisation (all types):** any media authorisations for the locking component or any area assigned to the locking component that have not expired yet.

5.6 Media & persons

The ***Media & persons*** main menu ❶ is intended to manage all persons, media, and authorisations within the access control system.

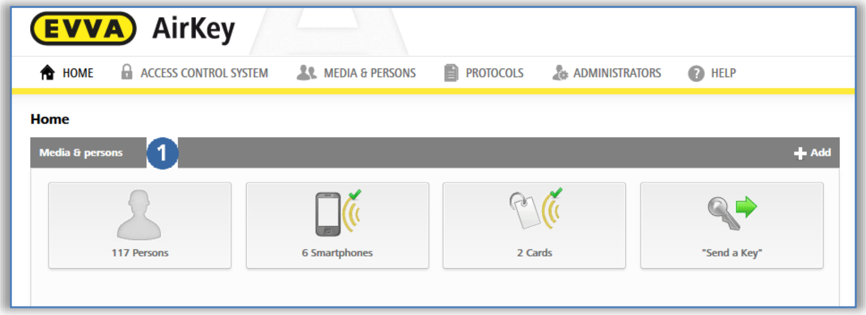


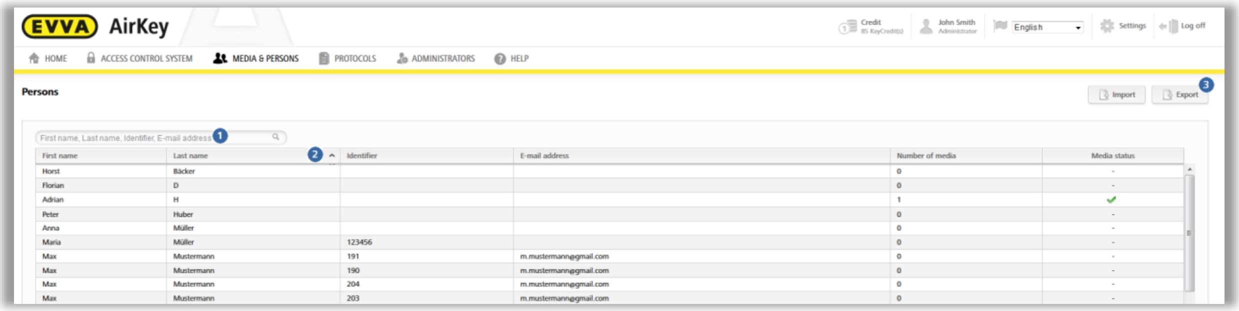
Figure 162: Media & persons

5.6.1 Overview of persons

On the ***Home*** screen, select the ***Persons*** tile or click ***Media & persons*** → ***Persons*** in the main menu for a list of all created persons including the number of media they own as well as their media states.

The list shown enables the following functions:

- Enter a search term with a minimum of three characters in the search field ❶.
  Select first name, last name, ID or e-mail address.
- Click the corresponding column heading to determine it as the sorting criterion ❷.
- You can also export the entire list to a CSV file for further processing ❸.



Persons

First name, Last name, Identifier, E-mail address

First name	Last name	Identifier	E-mail address	Number of media	Media status
Horst	Bäcker			0	-
Florian	D			0	-
Adrian	H			1	✓
Peter	Huber			0	-
Anna	Müller			0	-
Maria	Müller	123456		0	-
Max	Mustermann	191	m.mustermann@gmail.com	0	-
Max	Mustermann	190	m.mustermann@gmail.com	0	-
Max	Mustermann	204	m.mustermann@gmail.com	0	-
Max	Mustermann	203	m.mustermann@gmail.com	0	-

Figure 163: Persons

5.6.2 Creating persons: See chapter 4.7

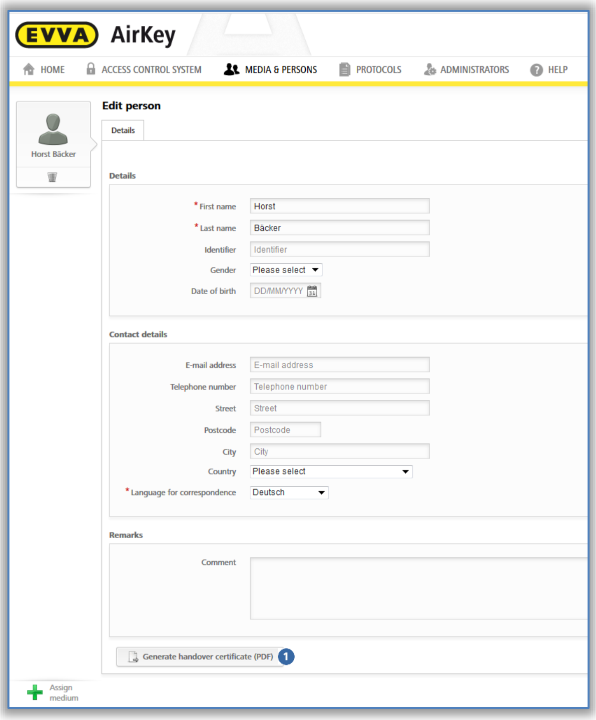
5.6.3 Editing persons

The "Edit person" detail view allows changing personal details and contacting data or assigning a new medium.

- On the ***Home*** screen, select the ***Persons*** tile.
- Alternatively select ***Media & persons*** → ***Persons*** in the main menu.
- Click the name of the person on the person list for which you would like to change details.
- Change the corresponding data.
- Click ***Save***.

You can also create the handover certificate on the "Edit user" page ❶. This is a confirmation that is handed over to users after having created and assigned all required authorisations. The confirmation lists which media and associated authorisations have been handed over to the specific user at the time the confirmation was output.

- Select the user for whom you would like to create a handover confirmation.
- Click the ***Generate handover certificate (PDF)*** on the "Edit person" page.
- The "Create handover certificate (PDF)" dialogue window appears showing the PDF file as a link.
- Click the link and open the PDF file with your PDF reader. Alternatively save the file.
- Click the ***Close*** button to close the dialogue window.



Edit person

Details

* First name: Horst
* Last name: Bäcker
Identifier: Identifier
Gender: Please select
Date of birth: DD/MM/YYYY

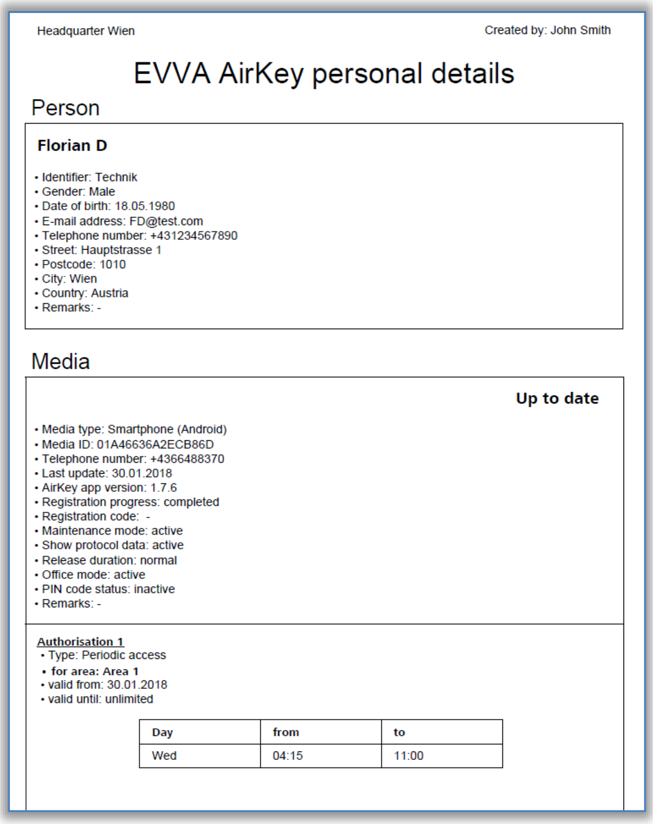
Contact details

E-mail address: E-mail address
Telephone number: Telephone number
Street: Street
Postcode: Postcode
City: City
Country: Please select
* Language for correspondence: Deutsch

Remarks

Comment:

Figure 164: Generate handover certificate



Headquarter Wien — Created by: John Smith

EVVA AirKey personal details

Person

Florian D

- Identifier: Technik
- Gender: Male
- Date of birth: 18.05.1980
- E-mail address: FD@test.com
- Telephone number: +431234567890
- Street: Hauptstrasse 1
- Postcode: 1010
- City: Wien
- Country: Austria
- Remarks: -

Media

Up to date

- Media type: Smartphone (Android)
- Media ID: 01A46636A2ECB86D
- Telephone number: +4366488370
- Last update: 30.01.2018
- AirKey app version: 1.7.6
- Registration progress: completed
- Registration code: -
- Maintenance mode: active
- Show protocol data: active
- Release duration: normal
- Office mode: active
- PIN code status: inactive
- Remarks: -

Authorisation 1

- Type: Periodic access
- **for area: Area 1**
- valid from: 30.01.2018
- valid until: unlimited

Day	from	to
Wed	04:15	11:00

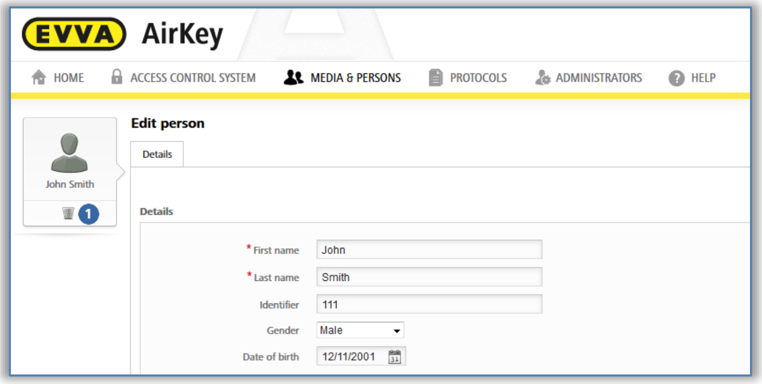
Figure 165: Handover certificate PDF

5.6.4 Deleting persons

You can delete persons if you would like to remove them from your access control system.

You are unable to delete a person who is still assigned to media. For this purpose, ensure that all media have been unassigned from this person before deletion.

- On the ***Home*** screen, select the ***Persons*** tile.
- Alternatively select ***Media & Persons*** → ***Persons*** in the main menu.
- Click the name of the person on the person list you would like to delete.
- Click the ***recycling bin*** ❶ icon.



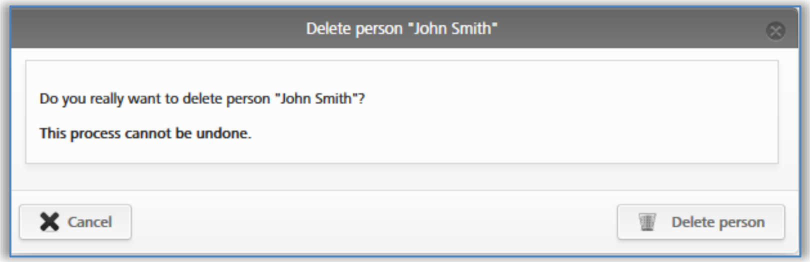
Edit person

Details

* First name John
* Last name Smith
Identifier 111
Gender Male
Date of birth 12/11/2001

Figure 166: Deleting persons

- Click "Delete person" to confirm the security prompt.


Delete person "John Smith"

Do you really want to delete person "John Smith"?

This process cannot be undone.

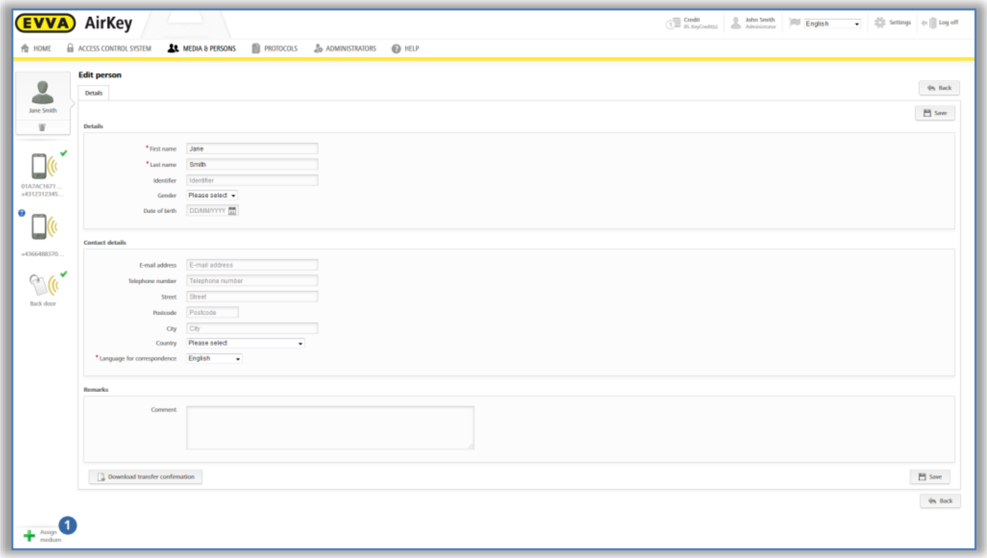
Figure 167: Delete persons – security prompt

Deleted persons are no longer shown on the person list. Personal event logs for locking components and media will continue to be documented in the event log entries dated prior to deletion.

5.6.5 Assigning media to persons

Assign the medium to a person to be able to assign authorisations. This is the only way to link persons to access events.

- On the ***Home*** screen, select the ***Persons*** tile.
- Alternatively select ***Media & persons*** → ***Persons*** in the main menu.
- In the list of persons, click the person you would like to assign a medium to.
- Click the ***Assign medium*** button. ❶



Edit person

Details

Details

*First name: Jane

*Last name: Smith

Identifier: Identifier

Gender: Please select

Date of birth: DD/MM/YYYY

Contact details

E-mail address: E-mail address

Telephone number: Telephone number

Street: Street

Postcode: Postcode

City: City

Country: Please select

*Language for correspondence: English

Remarks

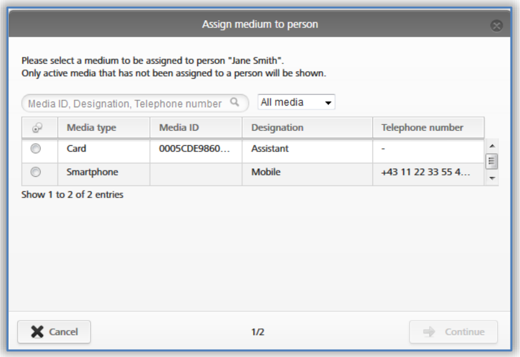
Comment:

Figure 168: Assigning media

A list with all media that you can assign to the person appears.
You can sort the list, filter by media type or search for certain entries.

Exclusively media within your access control system that have not been assigned to persons are listed.

> Select the desired medium and click ***Continue***.



Assign medium to person

Please select a medium to be assigned to person "Jane Smith".
Only active media that has not been assigned to a person will be shown.

Media ID, Designation, Telephone number | All media

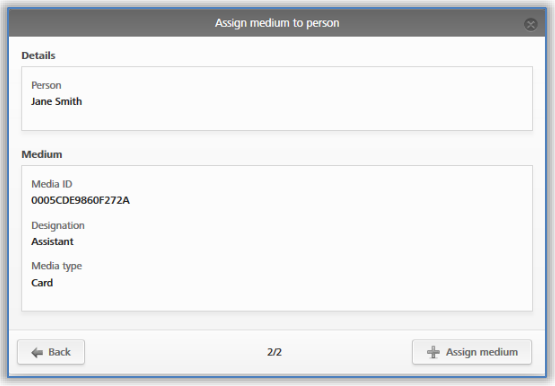
	Media type	Media ID	Designation	Telephone number
○	Card	0005CDE9860…	Assistant	-
○	Smartphone		Mobile	+43 11 22 33 55 4…

Show 1 to 2 of 2 entries

Figure 169: Assigning media to persons

The details are shown after having selected the medium. If required, click ***Back*** and select a different medium.

> Click ***Assign medium*** to complete the process.



Details

Person
Jane Smith

Medium

Media ID
0005CDE9860F272A

Designation
Assistant

Media type
Card

Figure 170: Assigning media to persons

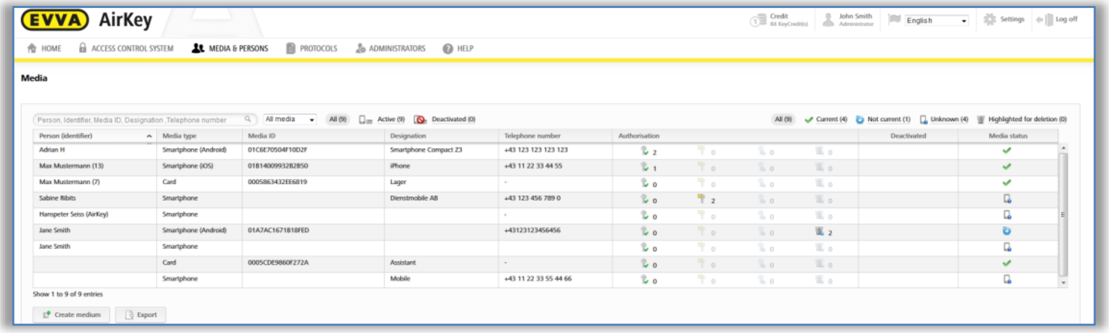
Alternatively, you can also assign media to persons using the medium. Please refer to Assigning persons to media for more information.

You can also assign several media (smartphones, cards, key fobs or combi keys) to a single person.

5.6.6 Overview of media

The ***Media & persons → Media*** main menu provides a list of all media (smartphones, cards, key fobs, and combi keys) to give you an overview of all assigned authorisations, potential deactivations as well as the current media states.

You can search for media in this media list, filter for certain media states, change the sort order or export the entire list to a CSV file.



Media

Person (identifier)	Media type	Media ID	Designation	Telephone number	Authorisation				Deactivated	Media status
Adrian H	Smartphone (Android)	01C6E70504F10D2F	Smartphone Compact Z3	+43 123 123 123 123	2	0	0	0		✓
Max Mustermann (13)	Smartphone (iOS)	01B14009932B2B50	iPhone	+43 11 22 33 44 55	1	0	0	0		✓
Max Mustermann (7)	Card	0005863432EE6819	Lager	-	0	0	0	0		✓
Sabine Ribits	Smartphone		Dienstmobile AB	+43 123 456 789 0	0	2	0	0		☐
Hanspeter Seiss (AirKey)	Smartphone			-	0	0	0	0		☐
Jane Smith	Smartphone (Android)	01A7AC1671B18FED		+43123123456456	0	0	0	2		↻
Jane Smith	Smartphone				0	0	0	0		☐
	Card	0005CDE9860F272A	Assistant	-	0	0	0	0		✓
	Smartphone		Mobile	+43 11 22 33 55 44 66	0	0	0	0		☐

Show 1 to 9 of 9 entries

Figure 171: Media list

5.6.7 Creating media

You must create a medium in your access control system before you can manage it as part of your access control system.

- On the ***Home*** screen, in the grey bar of the ***Media and persons*** section, click ***Add → Add medium***.
- Alternatively select ***Media & persons*** → ***Add medium*** in the main menu.

- Alternatively, browse to the ***Home*** screen and select the ***Smartphones*** or ***Cards*** tile and then click ***Add medium***.

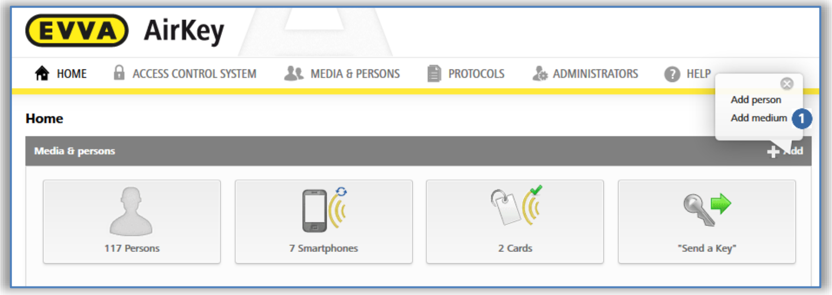
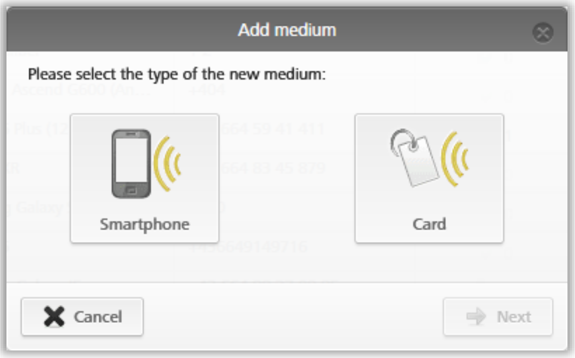


Figure 172: Creating media

- Select the media type of the new medium.


Add medium

Please select the type of the new medium:

Figure 173: Creating new media

The application does not distinguish between cards, key fobs, combi keys, and wristbands. For this reason, also create key fobs, combi keys, and wristbands as ***Card*** media types.

5.6.8 Creating smartphones: See chapter 4.8

5.6.9 Creating cards, key fobs, combi keys or wristbands

If you do not have a coding station available, you can add cards, key fobs, combi keys or wristbands to the access control system using a smartphone with maintenance authorisation. For this purpose, refer to the information in Adding cards, key fobs, and combi keys using a smartphone.

- Enter a designation and click ***Continue***.
- Place the card, key fob, combi key or wristband on the coding station.

The detailed view of this medium automatically opens once you have successfully completed the process.

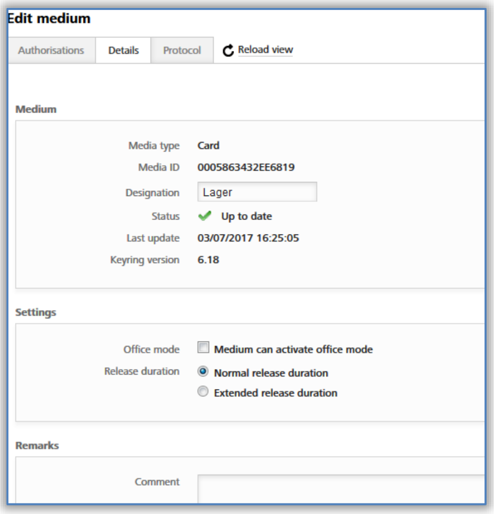
We strongly recommend to create a sufficient number of preconfigured media (cards, key fobs, combi keys or wristbands) featuring permanent authorisations without an expiry date (emergency media) and keep these safe to be able to operate the access control system regardless of the AirKey Online Administration. Please refer to Authorisations for more information on assigning authorisations.

Use the combi key side featuring the RFID icon when adding combi keys using coding stations. Hold the combi key directly on the coding station. The process will not work across the entire coding station reader area – with the current type (HID Omnikey 5421) combi keys are exclusively detected in the top and the bottom third of the coding station.

Please refer to Adding cards, key fobs, and combi keys for more information on adding media to your access control system using smartphones with maintenance authorisations.

5.6.10 Editing media

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the desired medium from the overview list.
- Select the ***Details*** tab to edit the medium.



Medium

Media type: Card
Media ID: 0005863432EE6819
Designation: Lager
Status: ✓ Up to date
Last update: 03/07/2017 16:25:05
Keyring version: 6.18

Settings

Office mode: □ Medium can activate office mode
Release duration: ● Normal release duration
○ Extended release duration

Remarks

Comment:

Figure 174: Editing media – cards

- Click ***Save*** to confirm the changes.

5.6.11 Assigning persons to media: See chapter 4.13

5.6.12 Authorisations

Authorisations control access of persons to locking components. Media must have already been assigned to persons to be able to create authorisations for media. Please refer to Assigning media to persons for more information on how to assign media to persons.

Proceed as follows to view the authorisation overview of a medium:

- Select ***Media & persons*** → ***Media*** in the main menu.
- Select the desired medium from the overview list.
- The medium ❶ has already been selected (several media may be assigned to one person).
- You now see all authorisations ❷ that have already been assigned.

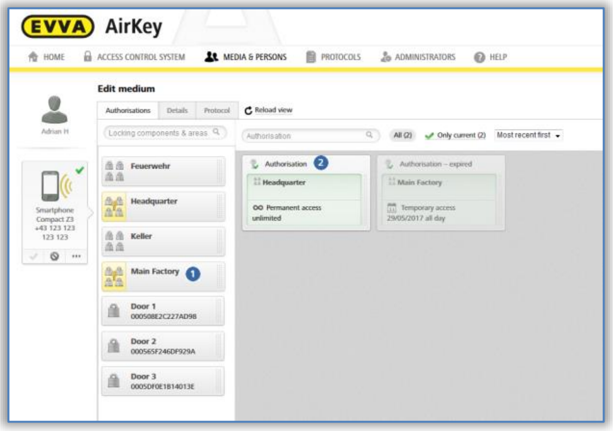


Figure 175: Authorisation overview

Background colour of authorisations:

- ***Green*** = Status up to date, authorisation created and medium updated
- ***Blue*** = Authorisation created, medium not updated yet
- ***Yellow*** = Authorisation has been changed or deleted, but not saved (created)
- ***Grey*** = Authorisation expired

Alternatively, you can also open the authorisation overview via ***Media & persons*** → ***Persons*** and select a person from the person list that has been assigned a medium. Now click on the media icon on the left-hand side below the selected person.

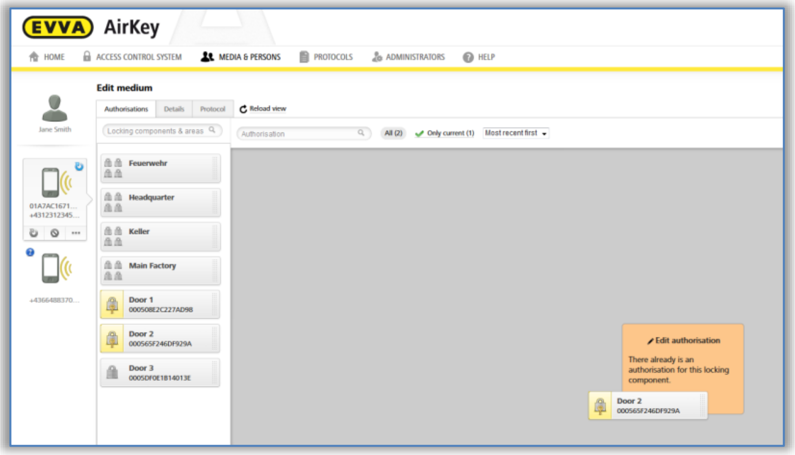
5.6.13 Assigning authorisations: See chapter 4.14

5.6.14 Creating authorisations: See chapter 4.15

5.6.15 Changing authorisations

You can change authorisations in the AirKey Online Administration at any time.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium from the overview list for which you would like to change authorisations.
- In the "Authorisation" tab, click the authorisation you would like to change.
- Alternatively, once again drag and drop the door/area into the centre.

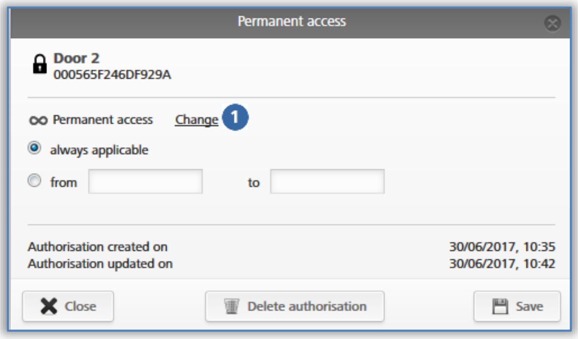


There already is an authorisation for this locking component.

Figure 176: Editing media – changing authorisations

> The system shows the details of existing authorisations.

> Click ***Change*** ❶



Door 2
000565F246DF929A

Permanent access

● always applicable

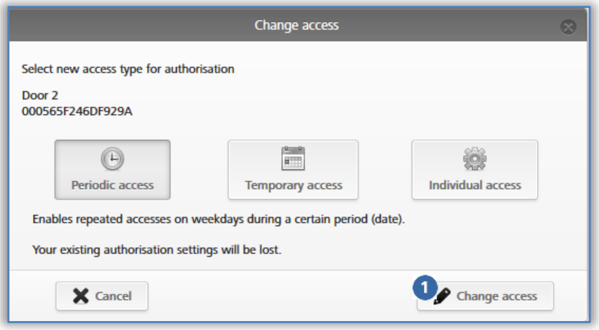
○ from ______ to ______

Authorisation created on 30/06/2017, 10:35
Authorisation updated on 30/06/2017, 10:42

Figure 177: Changing authorisations

> Select the new access type.

> Click ***Change access*** ❶.



Select new access type for authorisation

Door 2
000565F246DF929A

Enables repeated accesses on weekdays during a certain period (date).

Your existing authorisation settings will be lost.

Figure 178: Changing access

> Enter the corresponding values for the respective access type.

> Click ***Save***.

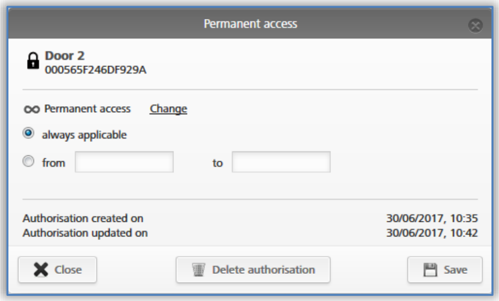
⚠ You must have credit on your KeyCredit account to change authorisations.

- Click on the yellow button ***Create 1 authorisation***. Please refer to Creating authorisations for more information.
- Pull to refresh and update your smartphone or, if you are using cards, key fobs, combi keys or wristbands, use the coding station to update and complete the process.

5.6.16 Deleting authorisations

You can delete any assigned authorisations if they are no longer required.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium from the overview list for which you would like to delete authorisations.
- In the "Authorisation" tab, click the authorisation you would like to delete.



Permanent access

Door 2
000565F246DF929A

Permanent access Change

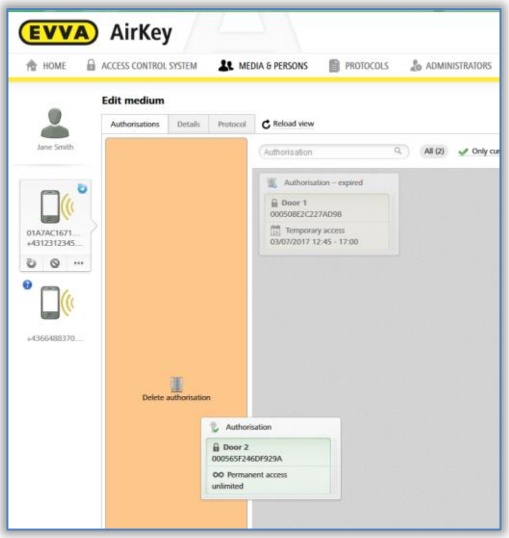
● always applicable

○ from ______ to ______

Authorisation created on 30/06/2017, 10:35
Authorisation updated on 30/06/2017, 10:42

Figure 179: Permanent access

Alternatively drag and drop the door / area from the centre to the box highlighted in orange ***Delete authorisation***.



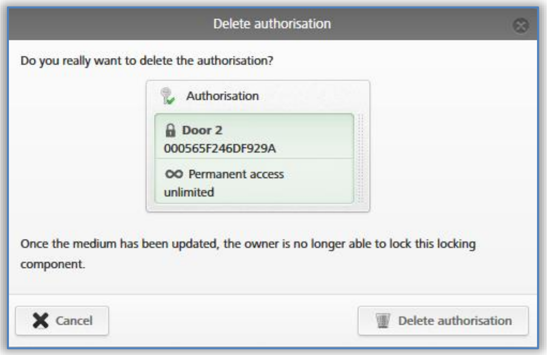
Authorisation – expired
Door 1
000508E2C227AD98
Temporary access
03/07/2017 12:45 - 17:00

Authorisation
Door 2
000565F246DF929A
Permanent access
unlimited

Figure 180: Deleting authorisations

- Click ***Delete authorisation***.

- Click ***Delete authorisation*** to confirm the security prompt.


Delete authorisation

Do you really want to delete the authorisation?

Authorisation

Door 2
000565F246DF929A

Permanent access
unlimited

Once the medium has been updated, the owner is no longer able to lock this locking component.

Figure 181: Deleting authorisations

- Pull to refresh and update your smartphone or, if you are using cards, key fobs, combi keys or wristbands, use the coding station to update and complete the process.

KeyCredits will not be deducted from your account for deletions. Deletions immediately come into effect. However, it is always necessary to update the media to complete the deletion process.

Do not use this function if you lose media. This function exclusively allows you to delete the authorisation if the medium is physically available. If media is lost, use the "Deactivating media" function.

Use the Emptying media function to delete all authorisations on the corresponding medium.

5.6.17 Deactivating media

Use the "Deactivate medium" function if there is a security risk and you intend to render all of the medium’s authorisations invalid, e.g. if a medium has been lost or damaged.

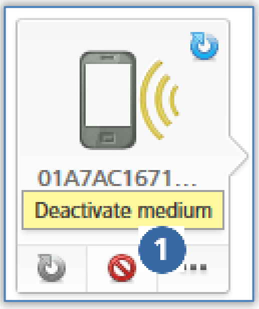
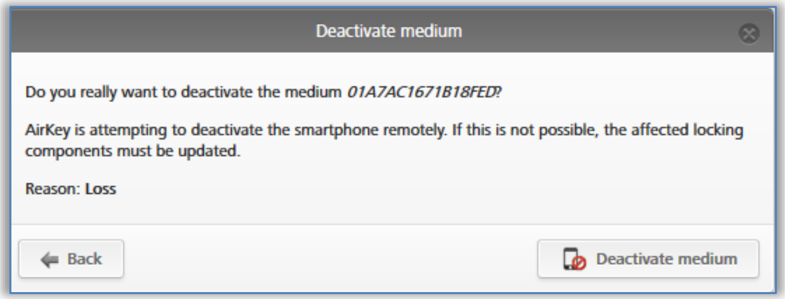


Figure 182: Deactivating media

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the desired medium from the overview list.
- Click ***Deactivate medium*** ❶.
- State the reason for deactivation. Select "Other" to activate the input field (character limit: 50 characters).
- If necessary, enter additional information (at maximum 500 characters) in "Additional comments".
- Click ***Continue***.
- Click ***Deactivate medium*** to confirm the security prompt.



Do you really want to deactivate the medium *01A7AC1671B18FED*?

AirKey is attempting to deactivate the smartphone remotely. If this is not possible, the affected locking components must be updated.

Reason: Loss

Figure 183: Deactivating media – security prompt

A confirmation prompt confirms deactivation of the medium.

Any authorisations assigned to the medium are highlighted for deletion. In the event of cards, key fobs, combi keys and wristbands the system immediately creates a blacklist entry for all locking components to which the medium had been authorised. For smartphones the entry is only triggered if the smartphone was not available for five minutes. A blacklist entry means the system creates a maintenance task for the affected locking component. As a result, affected locking components are out of date until updated.

> Update the locking components for which the medium had been authorised. The maintenance task will consequently disappear from the list and deactivated media are no longer authorised to unlock the locking components.

⚠ Do not use this function to delete individual authorisations assigned to media. Deactivating a medium is a function that affects all the medium's authorisations within an access control system.

Deactivations apply to your access control system only. If a smartphone has been registered in several access control systems, the smartphone's status remains up to date in the other access control systems and the medium is not deactivated.

If one person has registered one smartphone in several access control systems, contact all administrators of the affected access control systems to completely deactivate the smartphone.

❗ The medium remains assigned to the person. Delete the assignment if you would like to delete the medium. Please refer to Cancelling assignments for more information.

5.6.18 Removing deactivated media

You can remove deactivated media from the access control system without the corresponding medium being available. As a result, you can keep the master data in the AirKey Online Administration at a low level in terms of lost, stolen or faulty media.

Removing deactivated media is exclusively possible if the medium has been fully deactivated. Consequently, the medium has either been updated or an updated blacklist has been loaded to all locking components to which the medium had been authorised. It is not possible to remove media until the aforementioned conditions have been met.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- In the overview list, click the deactivated medium you would like to remove.
- Click ***More...*** below the media icon and select ***Remove*** ❶.
- Then confirm the security prompt with ***Remove medium*** to remove the deactivated, currently highlighted medium from the access control system.

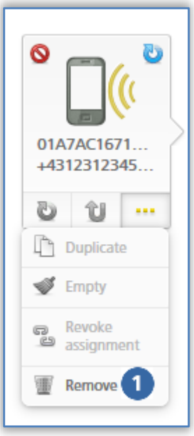
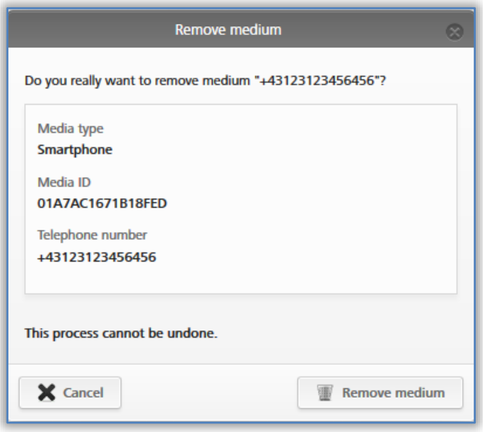


Figure 184: Removing deactivated media



Remove medium

Do you really want to remove medium "+43123123456456"?

Media type
Smartphone

Media ID
01A7AC1671B18FED

Telephone number
+43123123456456

This process cannot be undone.

Figure 185: Removing media – security prompt

- A message appears notifying of successful deletion and the medium is then no longer shown in the access control system.

This process is irrevocable. Media removed using this process are no longer listed in the access control system and they can consequently no longer be used.

This process does not automatically reset media to factory state.

5.6.19 Reactivating media

Deactivated media (highlighted by a red circle ❶) can be reactivated if they have once again become available.

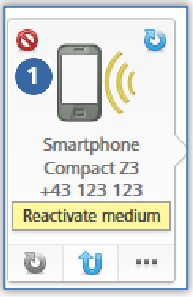


Figure 186: Reactivating deactivated media

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium from the overview list that you would like to reactivate.
- Click ***Reactivate medium*** below the media icon.

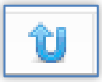
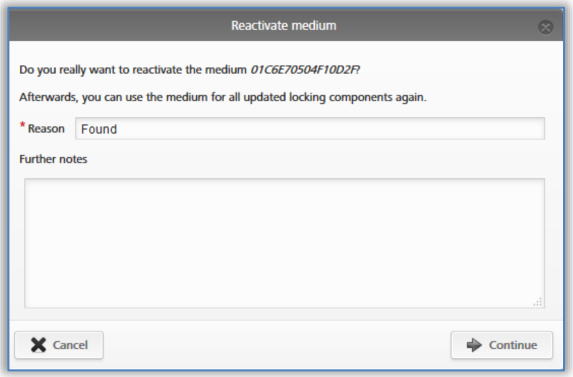


Figure 187: Reactivating media

- Enter the reason for reactivation (at maximum 50 characters) and decide as to whether you would like to reactivate authorisations valid prior to deactivation.

If necessary, enter additional information (at maximum 500 characters) in "Additional comments". The additional information will be documented in the event log entry.



Reactivate medium

Do you really want to reactivate the medium *01C6E70504F10D2F*?

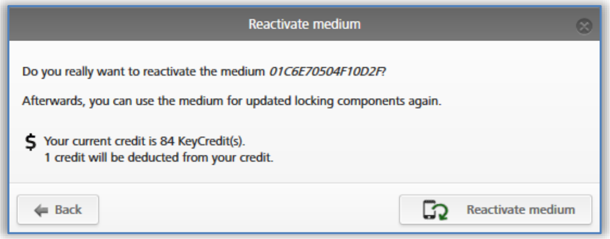
Afterwards, you can use the medium for all updated locking components again.

* Reason: Found

Further notes:

Figure 188: Reactivating media

- Click ***Continue***.
- Click ***Reactivate medium*** and confirm both security prompts (depending on whether you would like to restore authorisations).



Reactivate medium

Do you really want to reactivate the medium *01C6E70504F10D2F*?

Afterwards, you can use the medium for updated locking components again.

$ Your current credit is 84 KeyCredit(s).
1 credit will be deducted from your credit.

Figure 189: Reactivating media – including restoring authorisations

A confirmation prompt completes successful deactivation.

Maintenance tasks are once again created for these locking components, providing there are blacklist entries on the locking component for this particular reactivated medium.

Update the locking components that have been assigned maintenance tasks because of reactivation. The medium can only unlock all locking components once all blacklist entries have been removed, i.e. all affected locking components are up to date.

⚠ Reactivations apply to your access control system only. If a smartphone was deactivated in several access control systems, the smartphone remains deactivated in other access control systems and is still unauthorised to unlock components.

Notify other administrators in all relevant access control systems if persons have registered one smartphone in several access control systems to complete full reactivation.

❗ One KeyCredit is deducted to reactivate authorisations. Consequently, you require credit.

5.6.20 Replacing smartphone

With the "Replace smartphone" function, you transfer the existing AirKey authorisations and settings of a smartphone (except the PIN code and the local Hands-free settings) to another smartphone. The source medium is automatically deactivated after the successful replacement. Details about the smartphone replacement as administrator can be found in the chapter Starting replacement as administrator.

5.6.21 Duplicating media

The "Duplicate medium" function to duplicate media enables you to transfer existing authorisations from one medium to another. In this process, the source medium for duplication must be authorised and the target medium must have already been created and assigned to a person.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium for duplication from the overview list.

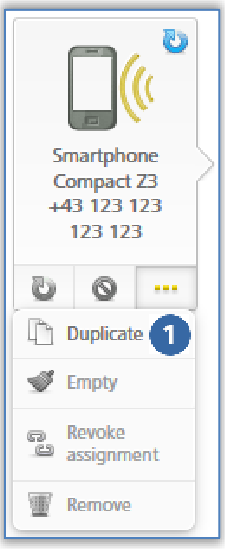
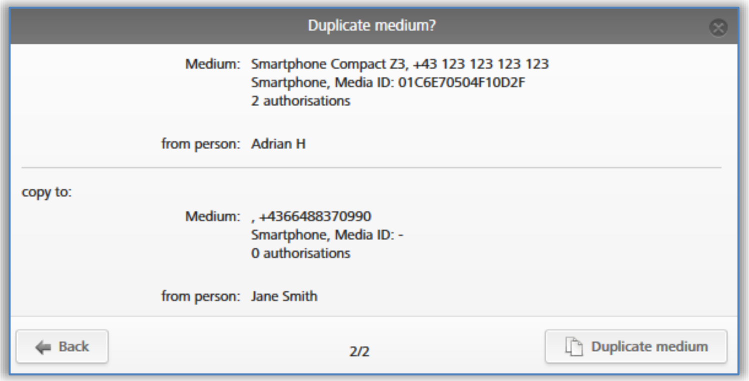


Figure 190: Duplicating media

- Click ***More...*** → ***Duplicate*** ❶.
  An overview list opens showing all media assigned to a person – the medium for duplication is not on this list.
- Select the desired target medium and click ***Continue***.
- Click ***Duplicate medium*** to complete the *process.*



Duplicate medium?

Medium: Smartphone Compact Z3, +43 123 123 123 123
Smartphone, Media ID: 01C6E70504F10D2F
2 authorisations

from person: Adrian H

copy to:

Medium: , +4366488370990
Smartphone, Media ID: -
0 authorisations

from person: Jane Smith

Figure 191: Duplicating media

The system confirms successful duplication. You are forwarded to the authorisation overview of the target medium.

Any existing authorisations on the target medium are overwritten.

Click ***Create authorisations*** to create and update the target medium and complete duplication. Please refer to Creating authorisations for more information on creating media.

One KeyCredit will be deducted from your account for this process. Consequently, you require credit.

If your AirKey Online Administration involves a high number of persons (see Importing personal data) with identical authorisations, you can quickly assign a high number of media featuring the same authorisations to the corresponding persons using the "Duplicate medium" function.

5.6.22 Emptying media

Empty media if you would like to delete all authorisations on them.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Click the medium you would like to clear in the overview list.

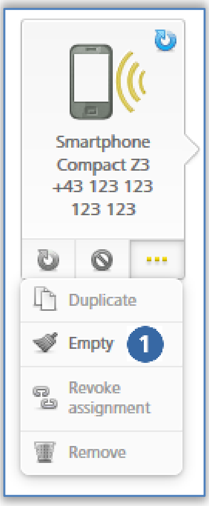
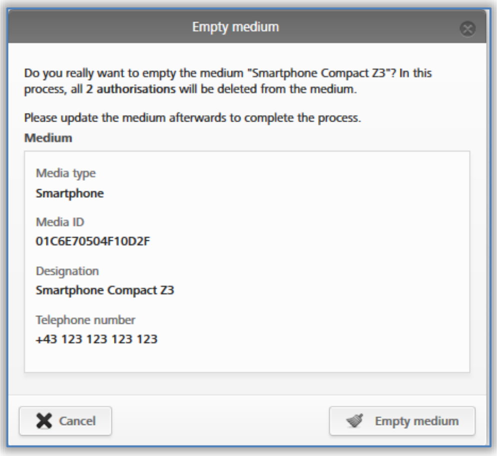


Figure 192: Emptying media

- Click ***More...*** → ***Empty*** ❶.
- Click ***Empty medium*** to complete the process.



Empty medium

Do you really want to empty the medium "Smartphone Compact Z3"? In this process, all 2 authorisations will be deleted from the medium.

Please update the medium afterwards to complete the process.

Medium

Media type
Smartphone

Media ID
01C6E70504F10D2F

Designation
Smartphone Compact Z3

Telephone number
+43 123 123 123 123

Figure 193: Emptying media – security prompt

All authorisations are highlighted for deletion. You must update the medium so all authorisations are finally deleted.

KeyCredits will not be deducted from your account for deletions. However, it is always necessary to update the media to complete the deletion process.

Do not use this function for lost media. This function exclusively allows you to delete the authorisation if the medium is physically available. If media is lost, use the Deactivate media function.

Use the Delete authorisation function if you would like to delete individual authorisations.

5.6.23 Cancelling assignments

Cancel assignments if persons no longer use the medium.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the medium from the overview list for which you would like to cancel assignments to persons.

Alternatively

- On the ***Home*** screen, select the ***Persons*** tile.
- Alternatively select ***Media & persons*** → ***Persons*** in the main menu.
- Click the name of the person on the person list for which you would like to cancel assignments to media.

All media assigned to a person are shown on the left, below the name.

Select the medium for which you would like to cancel assignments.

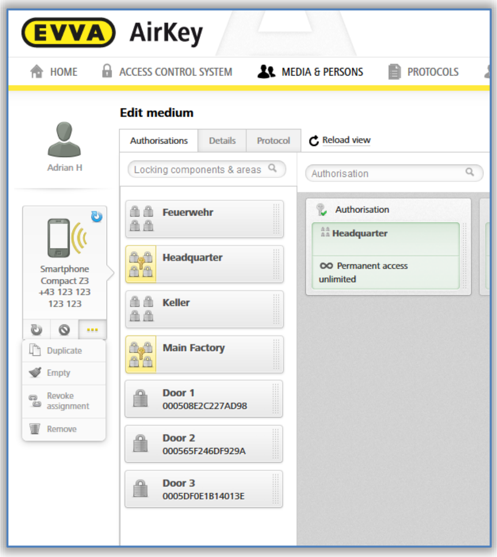


Figure 194: Assigned media

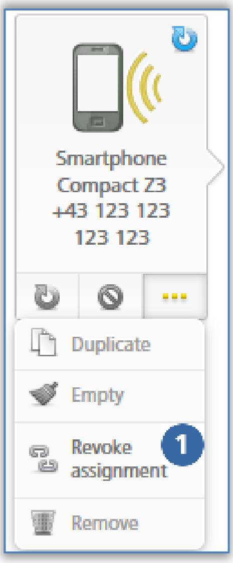
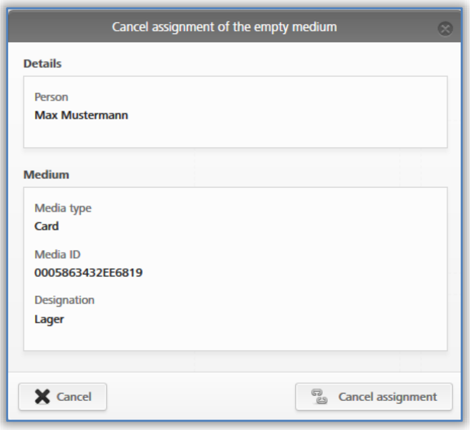


Figure 195: Media – cancelling assignments

- Click ***More...*** → ***Cancel assignment*** ❶ if there are no longer any authorisations on the medium.
- Click ***Cancel assignment*** to confirm the security prompt.



Details

Person
Max Mustermann

Medium

Media type
Card

Media ID
0005863432EE6819

Designation
Lager

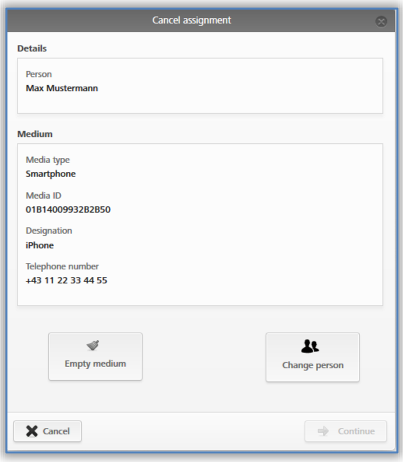
Figure 196: Cancelling assignments without authorisations

A message indicating the assignment has been cancelled successfully appears on the screen. You are automatically forwarded to the personal details of the affected person.

Deactivate the special authorisation "maintenance authorisation" on smartphones to be able to cancel assignments.

Delete any authorisations on the medium first. You can also use the ***Empty medium*** function for the ***Cancel assignment*** function to clear all authorisations of the medium.

If there are authorisations on the medium and you run the ***Cancel assignment*** function, the system shows an alternative dialogue. In this dialogue, you can choose between emptying the media and transferring the medium to another person.



Details

Person
Max Mustermann

Medium

Media type
Smartphone

Media ID
01B14009932B2B50

Designation
iPhone

Telephone number
+43 11 22 33 44 55

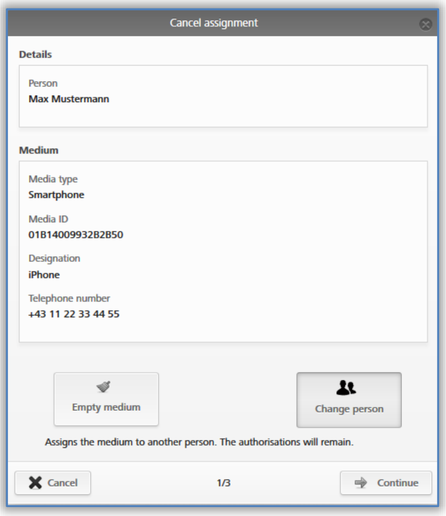
Figure 197: Cancelling assignments with authorisations

If you make use of the ***Empty medium*** function within the context of the ***Cancel assignment*** function, you must once again run the ***Cancel assignment*** function after having updated the medium to successfully complete the deletion process of the authorisations.

Proceed as follows to transfer the medium including all its authorisations to another person:

> Click ***More…*** → ***Cancel assignment***.

> Select ***Change person*** and confirm with ***Continue***.



Details

Person
Max Mustermann

Medium

Media type
Smartphone

Media ID
01B14009932B2B50

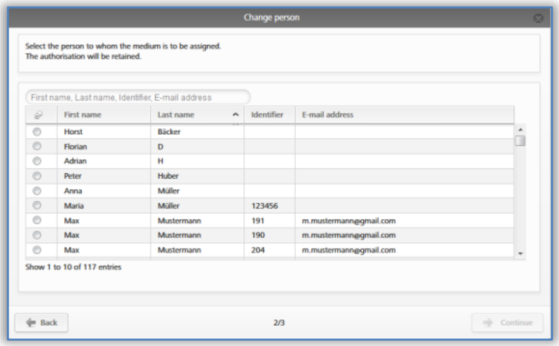
Designation
iPhone

Telephone number
+43 11 22 33 44 55

Assigns the medium to another person. The authorisations will remain.

Figure 198: Cancelling assignments – changing persons

The system shows a list of all created persons. Select the desired person and click ***Continue*** to confirm.



Select the person to whom the medium is to be assigned.
The authorisation will be retained.

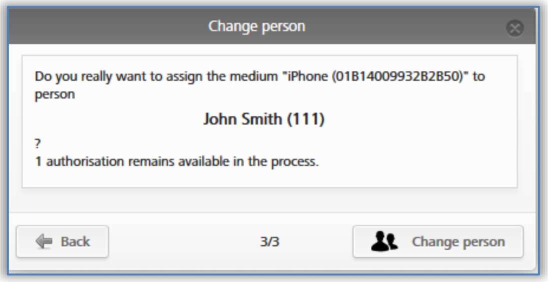
First name, Last name, Identifier, E-mail address

	First name	Last name	Identifier	E-mail address
○	Horst	Bäcker		
○	Florian	D		
○	Adrian	H		
○	Peter	Huber		
○	Anna	Müller		
○	Maria	Müller	123456	
○	Max	Mustermann	191	m.mustermann@gmail.com
○	Max	Mustermann	190	m.mustermann@gmail.com
○	Max	Mustermann	204	m.mustermann@gmail.com

Show 1 to 10 of 117 entries

Figure 199: Changing persons

Click ***Change person*** to confirm the security prompt and successfully complete the process.



Do you really want to assign the medium "iPhone (01B14009932B2B50)" to person

John Smith (111)

?
1 authorisation remains available in the process.

Figure 200: Changing persons

A message indicating the process was successful appears upon completing the process successfully.

5.6.24 Removing media

Remove media if you would like to no longer show or use them in your access control system.

It is exclusively possible to remove media if you have cancelled their assignments to persons. Please refer to Cancelling assignments for more information.

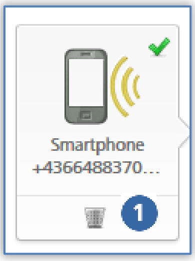
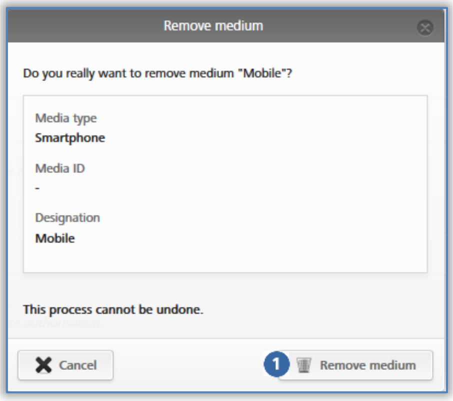


Figure 201: Deleting media – recycle bin

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Click the medium you would like to delete in the overview list.
- Click the recycling bin icon below the media icon ❶.
- Click ***Remove medium*** ❶ to confirm the security prompt.



Remove medium

Do you really want to remove medium "Mobile"?

Media type
Smartphone

Media ID
-

Designation
Mobile

This process cannot be undone.

Figure 202: Removing media

Once the medium has been fully deleted, it is no longer shown on the media overview list. You are forwarded to the media list.

The media returns to factory state once it has been removed from the access control system and you can add it to another access control system.

Option

If you would like to remove media without authorisations and assignments to persons using the coding station, place the medium on the coding station and subsequently select the ***Remove medium*** link within the status message.

5.7 Event logs

The ***Event log*** main menu provides central overview of all events within your access control system. Depending on the general settings for logging and repair options or personal data in event log entries, the system records rejected access (if the medium has an authorisation for the locking component, but the authorisation was not valid at the time of the access attempt) in addition to granted access events and technical events. Any events transferred to the AirKey Online Administration remain saved there for an unrestricted period of time.

We recommend you reload the event logs regularly to be able to have the most recent event log entries available. For this purpose, use the ***Reload view*** function.

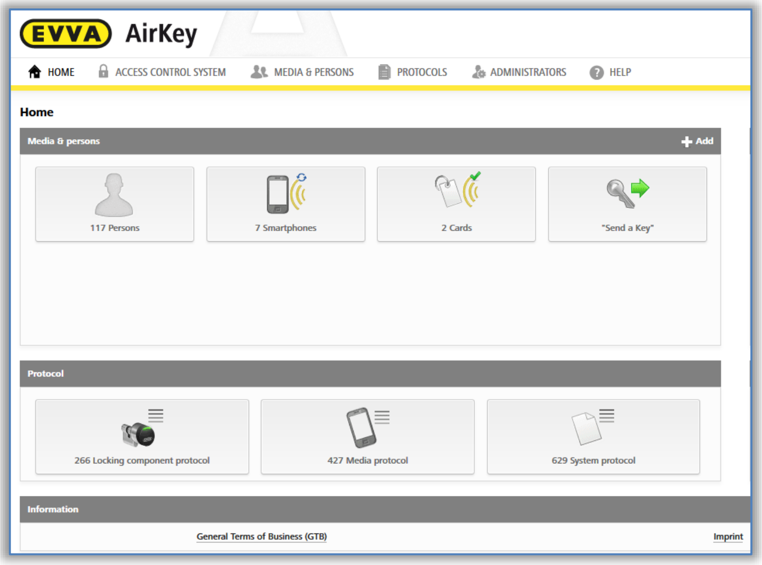


Figure 203: Event logs

We explicitly point out that this access control system may be subject to mandatory reporting / approval processes depending on the applicable, legal stipulations, particular data protection legislation. As a consequence, EVVA Sicherheitstechnologie GmbH shall not assume any liability for or guarantee operation in compliance with valid, legal stipulations.

Activate the **Four-eyes principle for the event log viewing** to ensure even greater protection for personal data. The confirmation of a second system administrator is required to view the locking component event log and the media event log. Details about the activation can be found in the chapter General.

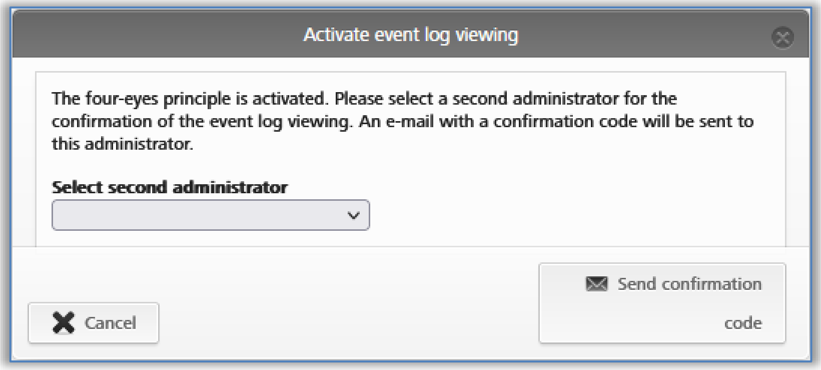
5.7.1 Locking component event log

If the **four-eyes principle for the event log viewing** is not activated, follow the steps below to view the locking component event log:

- On the ***Home*** page, select the ***Locking component event log*** tile.
- Alternatively select ***Event log*** ⟶ ***Locking components & areas***.

If the **four-eyes principle for the event log viewing** is activated, follow the steps below in addition to view the locking component event log:

- Select a second system administrator from the list to whom a confirmation code should be sent by e-mail and click ***Send confirmation code***.

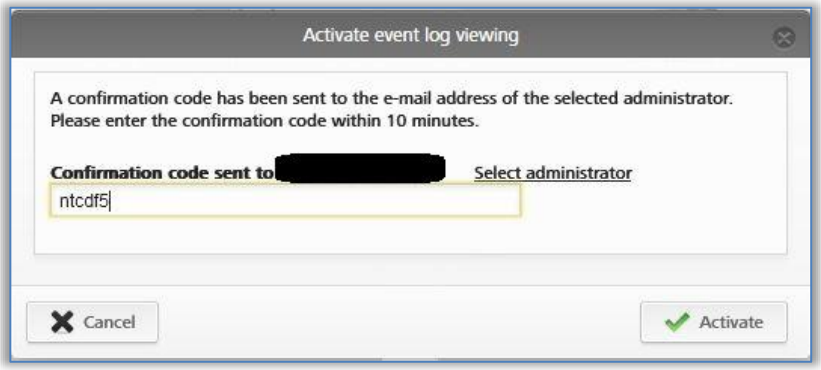

Activate event log viewing

The four-eyes principle is activated. Please select a second administrator for the confirmation of the event log viewing. An e-mail with a confirmation code will be sent to this administrator.

Select second administrator

Figure 204: Activating event log viewing – selecting second administrator

- An e-mail with a confirmation code will then be sent to the selected system administrator.
- This confirmation code must be entered in the AirKey Online Administration within 10 minutes and confirmed with ***Activate***.


Activate event log viewing

A confirmation code has been sent to the e-mail address of the selected administrator. Please enter the confirmation code within 10 minutes.

Confirmation code sent to [redacted] Select administrator

ntcdf5

Figure 205: Activating event log viewing – entering confirmation code

If this process is not completed within 10 minutes, the process must be repeated. If the selected system administrator does not respond, another system administrator can also be selected via the ***Select administrator*** link to activate the event log viewing.

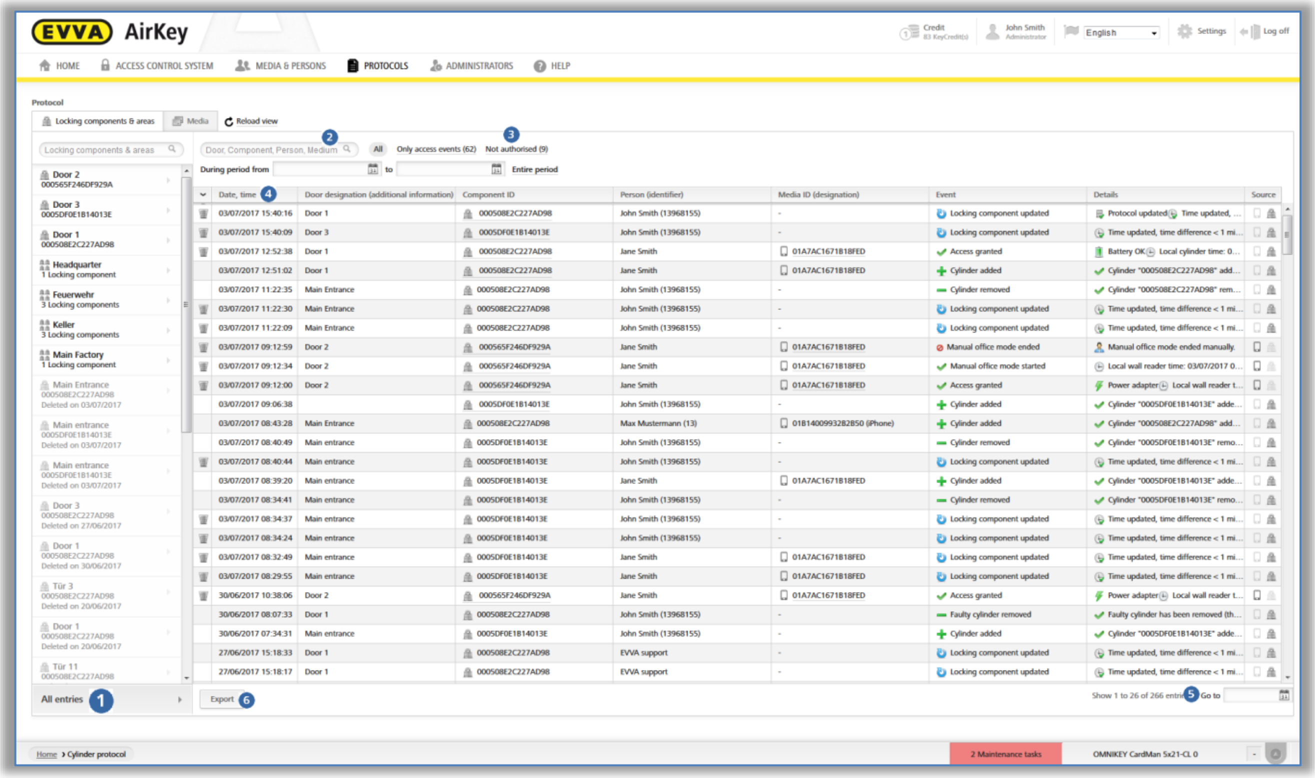
Afterwards the locking component event log will be displayed.

The activation of the event log viewing is valid until the next logout of the system administrator. This means that both the locking component event log and the media event log can be viewed as often as you like.

The list shown features all entries for locking components and areas.

- If necessary, select individual locking components and areas from the left-hand column for which you would like to view event logs. Click ***All entries*** ❶ in the bottom left if you would once again like to view all locking components for a specific area.
- Enter a minimum of three characters in the search field ❷ for a targeted search.

- Click the corresponding link to additionally activate the filter ❸ (e.g. "Not authorised"). This will exclusively list entries where access was denied.
- By default, the list has been sorted by date and time ❹ (most recent entries at the top). Click the "Date, time" column header to change the sort order. It is not possible to sort this table by other column headings.



Door 2
000565F246DF929A
Door 3
0005DF0E1B14013E
Door 1
000508E2C227AD98
Headquarter
1 Locking component
Feuerwehr
3 Locking components
Keller
3 Locking components
Main Factory
1 Locking component
Main Entrance
000508E2C227AD98
Deleted on 03/07/2017
Main entrance
0005DF0E1B14013E
Deleted on 03/07/2017
Main entrance
0005DF0E1B14013E
Deleted on 03/07/2017
Door 3
000508E2C227AD98
Deleted on 27/06/2017
Door 1
000508E2C227AD98
Deleted on 30/06/2017
Tür 3
000508E2C227AD98
Deleted on 20/06/2017
Door 1
000508E2C227AD98
Deleted on 20/06/2017
Tür 11
000508E2C227AD98
All entries

Date, time	Door designation (additional information)	Component ID	Person (identifier)	Media ID (designation)	Event	Details	Source
03/07/2017 15:40:16	Door 1	000508E2C227AD98	John Smith (13968155)	-	Locking component updated	Protocol updated Time updated, ...	
03/07/2017 15:40:09	Door 3	0005DF0E1B14013E	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 12:52:38	Door 1	000508E2C227AD98	Jane Smith	01A7AC1671B18FED	Access granted	Battery OK Local cylinder time: 0...	
03/07/2017 12:51:02	Door 1	000508E2C227AD98	Jane Smith	01A7AC1671B18FED	Cylinder added	Cylinder "000508E2C227AD98" add...	
03/07/2017 11:22:35	Main Entrance	000508E2C227AD98	John Smith (13968155)	-	Cylinder removed	Cylinder "000508E2C227AD98" rem...	
03/07/2017 11:22:30	Main Entrance	000508E2C227AD98	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 11:22:09	Main Entrance	000508E2C227AD98	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 09:12:59	Door 2	000565F246DF929A	Jane Smith	01A7AC1671B18FED	Manual office mode ended	Manual office mode ended manually.	
03/07/2017 09:12:34	Door 2	000565F246DF929A	Jane Smith	01A7AC1671B18FED	Manual office mode started	Local wall reader time: 03/07/2017 0...	
03/07/2017 09:12:00	Door 2	000565F246DF929A	Jane Smith	01A7AC1671B18FED	Access granted	Power adapter Local wall reader t...	
03/07/2017 09:06:38		0005DF0E1B14013E	John Smith (13968155)	-	Cylinder added	Cylinder "0005DF0E1B14013E" adde...	
03/07/2017 08:43:28	Main Entrance	000508E2C227AD98	Max Mustermann (13)	01B14009932B2B50 (iPhone)	Cylinder added	Cylinder "000508E2C227AD98" add...	
03/07/2017 08:40:49	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Cylinder removed	Cylinder "0005DF0E1B14013E" remo...	
03/07/2017 08:40:44	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 08:39:20	Main entrance	0005DF0E1B14013E	Jane Smith	01A7AC1671B18FED	Cylinder added	Cylinder "0005DF0E1B14013E" adde...	
03/07/2017 08:34:41	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Cylinder removed	Cylinder "0005DF0E1B14013E" remo...	
03/07/2017 08:34:37	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 08:34:24	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 08:32:49	Main entrance	0005DF0E1B14013E	Jane Smith	01A7AC1671B18FED	Locking component updated	Time updated, time difference < 1 mi...	
03/07/2017 08:29:55	Main entrance	0005DF0E1B14013E	Jane Smith	01A7AC1671B18FED	Locking component updated	Time updated, time difference < 1 mi...	
30/06/2017 10:38:06	Door 2	000565F246DF929A	Jane Smith	01A7AC1671B18FED	Access granted	Power adapter Local wall reader t...	
30/06/2017 08:07:33	Door 1	000508E2C227AD98	John Smith (13968155)	-	Faulty cylinder removed	Faulty cylinder has been removed (th...	
30/06/2017 07:34:31	Main entrance	0005DF0E1B14013E	John Smith (13968155)	-	Cylinder added	Cylinder "0005DF0E1B14013E" adde...	
27/06/2017 15:18:33	Door 1	000508E2C227AD98	EVVA support	-	Locking component updated	Time updated, time difference < 1 mi...	
27/06/2017 15:18:17	Door 1	000508E2C227AD98	EVVA support	-	Locking component updated	Time updated, time difference < 1 mi...	

Export

Show 1 to 26 of 266 entries Go to

Home › Cylinder protocol

2 Maintenance tasks

OMNIKEY CardMan 5x21-CL 0

Figure 206: Locking components & areas event logs

- If the list is extensive, use the ***Go to*** ❺ field in the bottom right to quickly browse to a certain date.
- Use the ***Export*** ❻ button in the bottom left if you would like to export the entire event log to a CSV file. You can then process this export regardless of the AirKey Online Administration.

All required information, such as date and time, door designation (additional information), component ID, user (user ID), media ID (designation) and the corresponding event are listed within the event log. The "Details" column lists more detailed information on this particular event.

The "Source" column shows whether the event log entry was generated by a medium and/or a locking component.

We recommend you reload the view regularly to be able to have the most recent event log entries available. For this purpose, use the ***Reload view*** function.

Use event log settings to restrict the logging of personal data in event log entries according to data protection legislation. You specify the type of personal data in event logs saved for locking components you add to the access control system in the Default event log value settings or in the locking component details of each locking component.

Regularly update locking components to ensure all event log entries have been transferred from locking components to the AirKey Online Administration. The recommended update intervals depend on the frequency the locking components are used. Observe the Values and limits of locking components.

Events where the access is denied are saved only if the medium has an authorisation for the locking component, but the authorisation was not valid at the time of the access attempt (e.g. the authorisation has expired or is valid in the future).

The battery status shown in the "Details" column does not always correspond to the locking component’s (cylinder) actual battery status and the smartphone’s battery status.

If event logs for locking components are restricted to a certain period, access events continue to be recorded after said period. In this case, the personal data is rendered anonymous.

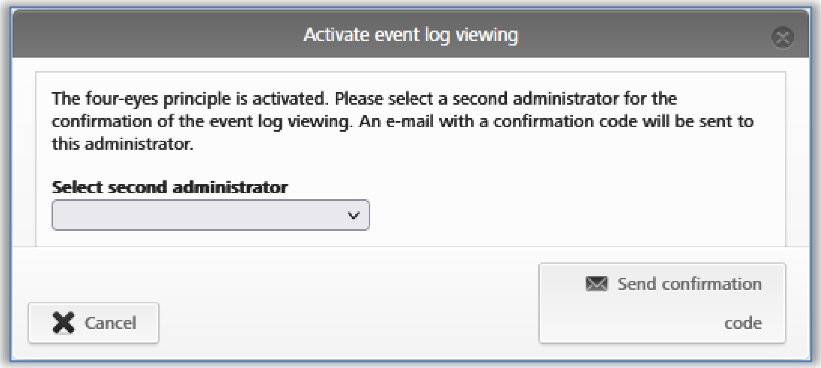
5.7.2 Media event log

If the **four-eyes principle for the event log viewing** is not activated, follow the steps below to view the media event log:

- On the ***Home*** screen, select the ***Media event log*** tile.
- Alternatively select ***Event log*** → ***Media***.

If the **four-eyes principle for the event log viewing** is activated, follow the steps below in addition to view the media event log:

- Select a second system administrator from the list to whom a confirmation code should be sent by e-mail and click ***Send confirmation code***.


Activate event log viewing

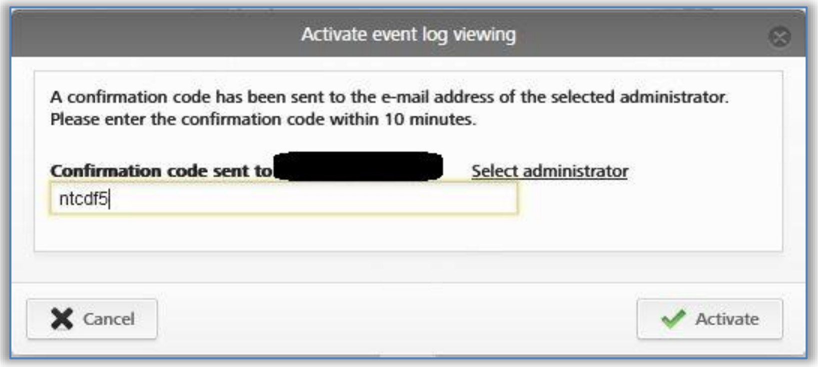
The four-eyes principle is activated. Please select a second administrator for the confirmation of the event log viewing. An e-mail with a confirmation code will be sent to this administrator.

Select second administrator

Figure 207: Activate event log viewing – select second administrator

- An e-mail with a confirmation code will then be sent to the selected system administrator.

- This confirmation code must be entered in the AirKey Online Administration within 10 minutes and confirmed with ***Activate***.



Activate event log viewing

A confirmation code has been sent to the e-mail address of the selected administrator.
Please enter the confirmation code within 10 minutes.

Confirmation code sent to [redacted] Select administrator

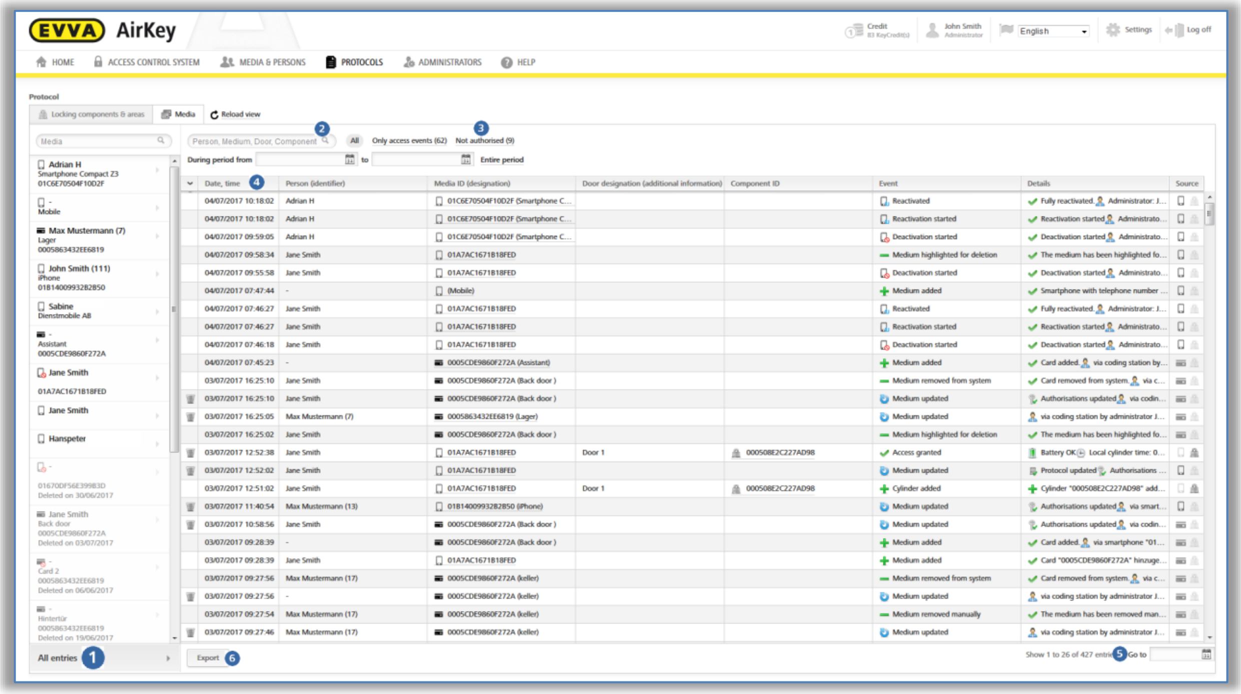
ntcdf5

Figure 208: Activate event log viewing – confirmation code

If this process is not completed within 10 minutes, the process must be repeated. If the selected system administrator does not respond, another system administrator can also be selected via the ***Select administrator*** link to activate event log viewing.

Afterwards the media event log will be displayed.

The activation of the event log viewing is valid until the next logout of the system administrator. This means that both the locking component event log and the media event log can be viewed as often as you like.



During period from … to … Entire period

Adrian H
Smartphone Compact Z3
01C6E70504F10D2F

-
Mobile

Max Mustermann (7)
Lager
0005863432EE6819

John Smith (111)
iPhone
01B14009932B2B50

Sabine
Dienstmobile AB

-
Assistant
0005CDE9860F272A

Jane Smith
01A7AC1671B18FED

Jane Smith

Hanspeter

-
01670DF56E399B3D
Deleted on 30/06/2017

Jane Smith
Back door
0005CDE9860F272A
Deleted on 03/07/2017

-
Card 2
0005863432EE6819
Deleted on 06/06/2017

-
Hintertür
0005863432EE6819
Deleted on 19/06/2017

Date, time	Person (identifier)	Media ID (designation)	Door designation (additional information)	Component ID	Event	Details	Source
04/07/2017 10:18:02	Adrian H	01C6E70504F10D2F (Smartphone C...			Reactivated	Fully reactivated. Administrator: J...	
04/07/2017 10:18:02	Adrian H	01C6E70504F10D2F (Smartphone C...			Reactivation started	Reactivation started Administrato...	
04/07/2017 09:59:05	Adrian H	01C6E70504F10D2F (Smartphone C...			Deactivation started	Deactivation started Administrato...	
04/07/2017 09:58:34	Jane Smith	01A7AC1671B18FED			Medium highlighted for deletion	The medium has been highlighted fo...	
04/07/2017 09:55:58	Jane Smith	01A7AC1671B18FED			Deactivation started	Deactivation started Administrato...	
04/07/2017 07:47:44	-	(Mobile)			Medium added	Smartphone with telephone number ...	
04/07/2017 07:46:27	Jane Smith	01A7AC1671B18FED			Reactivated	Fully reactivated. Administrator: J...	
04/07/2017 07:46:27	Jane Smith	01A7AC1671B18FED			Reactivation started	Reactivation started Administrato...	
04/07/2017 07:46:18	Jane Smith	01A7AC1671B18FED			Deactivation started	Deactivation started Administrato...	
04/07/2017 07:45:23	-	0005CDE9860F272A (Assistant)			Medium added	Card added. via coding station by...	
03/07/2017 16:25:10	Jane Smith	0005CDE9860F272A (Back door)			Medium removed from system	Card removed from system. via c...	
03/07/2017 16:25:10	Jane Smith	0005CDE9860F272A (Back door)			Medium updated	Authorisations updated via codin...	
03/07/2017 16:25:05	Max Mustermann (7)	0005863432EE6819 (Lager)			Medium updated	via coding station by administrator J...	
03/07/2017 16:25:02	Jane Smith	0005CDE9860F272A (Back door)			Medium highlighted for deletion	The medium has been highlighted fo...	
03/07/2017 12:52:38	Jane Smith	01A7AC1671B18FED	Door 1	000508E2C227AD98	Access granted	Battery OK Local cylinder time: 0...	
03/07/2017 12:52:02	Jane Smith	01A7AC1671B18FED			Medium updated	Protocol updated Authorisations ...	
03/07/2017 12:51:02	Jane Smith	01A7AC1671B18FED	Door 1	000508E2C227AD98	Cylinder added	Cylinder "000508E2C227AD98" add...	
03/07/2017 11:40:54	Max Mustermann (13)	01B14009932B2B50 (iPhone)			Medium updated	Authorisations updated via smart...	
03/07/2017 10:58:56	Jane Smith	0005CDE9860F272A (Back door)			Medium updated	Authorisations updated via codin...	
03/07/2017 09:28:39	-	0005CDE9860F272A (Back door)			Medium added	Card added. via smartphone "01...	
03/07/2017 09:28:39	Jane Smith	01A7AC1671B18FED			Medium added	Card "0005CDE9860F272A" hinzuge...	
03/07/2017 09:27:56	Max Mustermann (17)	0005CDE9860F272A (keller)			Medium removed from system	Card removed from system. via c...	
03/07/2017 09:27:56	-	0005CDE9860F272A (keller)			Medium updated	via coding station by administrator J...	
03/07/2017 09:27:54	Max Mustermann (17)	0005CDE9860F272A (keller)			Medium removed manually	The medium has been removed man...	
03/07/2017 09:27:46	Max Mustermann (17)	0005CDE9860F272A (keller)			Medium updated	via coding station by administrator J...	

Show 1 to 26 of 427 entrie

Figure 209: Media event log

The system shows an overview of all entries for media.

- If necessary, select individual media from the left-hand column for which you would like to view event logs. Click ***All entries*** ❶ in the bottom left if you would once again like to view all locking components for a specific area.
- Enter a minimum of three characters in the search field ❷ for a targeted search.
- Set filters, such as "Not authorised" ❸. This will list entries where access was denied.
- Sort the list by date and time ❹.
- Use the ***Go to*** ❺ field in the bottom right to quickly browse to a certain day in an extensive list.
- Use the "Export" ❻ button in the bottom left if you would like to export the entire media event log to a CSV file. You can then process this export regardless of the AirKey Online Administration.

All required information, such as date and time, user (user ID), media ID (designation), door designation (additional information), component ID and the corresponding event are listed within the event log. The "Details" column lists additional information on the particular event.

The "Source" column shows whether the event log entry was generated by a medium and/or a locking component.

Use event log settings to restrict the logging of personal data in event log entries according to data protection legislation. You specify the type of personal data in event logs saved for locking components you add throughout the access control system in the Settings or in the locking component details of each locking component.

You can also view event log entries for specific media in the dedicated media section. For this purpose, select the desired medium from the media list and go to the ***Event log*** tab.

Events where the access is denied are saved only if the medium has an authorisation for the locking component, but the authorisation was not valid at the time of the access attempt (e.g. the authorisation has expired or is valid in the future).

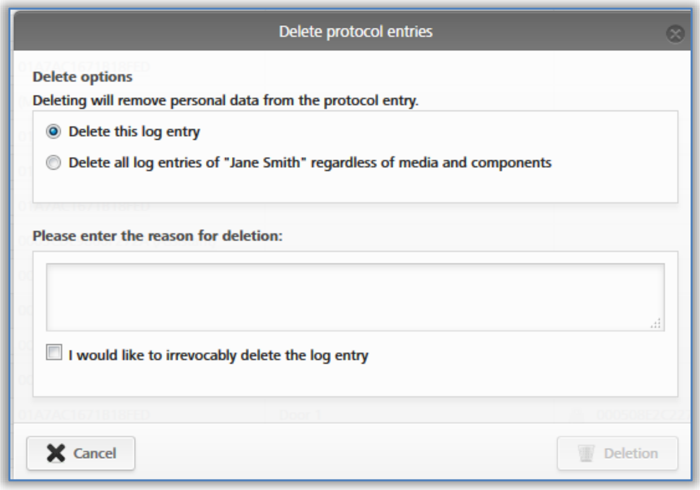
The battery status shown in the "Details" column does not always correspond to the locking component’s (cylinder) actual battery status and the smartphone’s battery status.

If event logs for locking components are restricted to a certain period, access events continue to be recorded after said period. In this case, the personal data is rendered anonymous.

Within the context of locking component and media event log entries relating to persons may also be rendered anonymous retrospectively for reasons of data protection. Any event log entries critical to data protection, such as access events, are shown in the first column with a recycling bin icon.

Proceed as follows to render personal data in event log entries anonymous:

- Search for the event log entry you would like to render anonymous and click the recycling bin icon in the first column.
- A prompt appears asking you whether to delete merely this specific event log entry or all of this person’s entries. Select the desired option.
- Enter the reason for deleting the event log entry.
- Tick ***I would like to irrevocably delete the event log entry***.
- Click ***Deletion*** to complete the process.



Delete protocol entries

Delete options

Deleting will remove personal data from the protocol entry.

● Delete this log entry

○ Delete all log entries of "Jane Smith" regardless of media and components

Please enter the reason for deletion:

□ I would like to irrevocably delete the log entry

Figure 210: Deleting event log entries

Event log entries are not deleted completely; merely the personal data is deleted. As a result, event log entries are rendered anonymous. This process is irrevocable. Use this function with care.

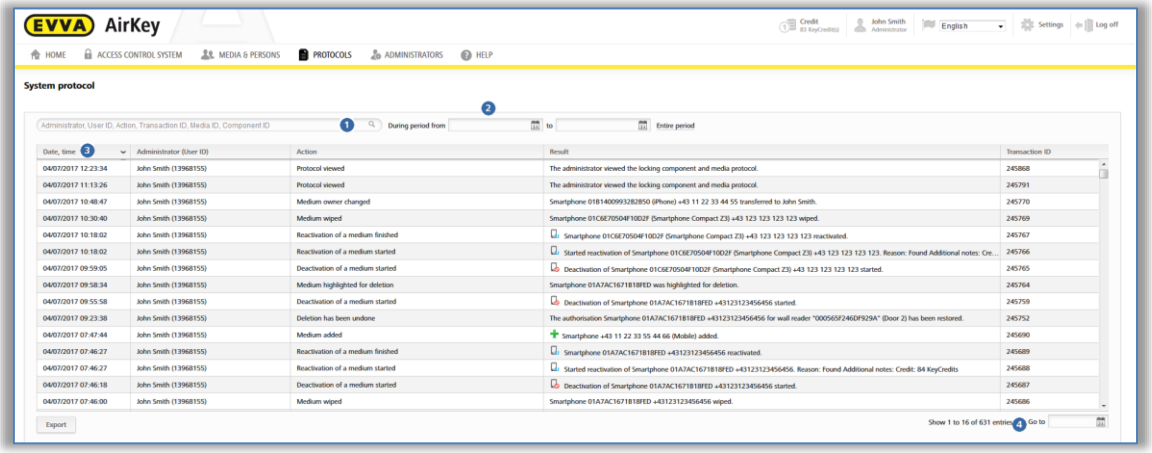
Deleting event log entries adds entries to the event log system.

5.7.3 System event log

- On the ***Home*** screen, select the ***System event log*** tile.
- Alternatively select ***Event log*** → ***System***.

An overview of all actions implemented by administrators appears.

- In the search field ❶ you can search for administrators, user IDs, events, transaction IDs, media IDs or component IDs. Enter a certain period ❷ and determine the column by which you would like to sort ❸.
- Enter a date in the ***Go to*** ❹ field to browse in the system event log directly to a certain date. The continue data set is shown if there are no entries for the entered date.
- Use the ***Export*** button in the bottom left if you would like to export the entire system event log to a CSV file. You can then process this export regardless of the AirKey Online Administration.



System protocol

Administrator, User ID, Action, Transaction ID, Media ID, Component ID — During period from — to — Entire period

Date, time	Administrator (User ID)	Action	Result	Transaction ID
04/07/2017 12:23:34	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245868
04/07/2017 11:13:26	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245791
04/07/2017 10:48:47	John Smith (13968155)	Medium owner changed	Smartphone 01B1400993282850 (iPhone) +43 11 22 33 44 55 transferred to John Smith.	245770
04/07/2017 10:30:40	John Smith (13968155)	Medium wiped	Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 wiped.	245769
04/07/2017 10:18:02	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 reactivated.	245767
04/07/2017 10:18:02	John Smith (13968155)	Reactivation of a medium started	Started reactivation of Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123. Reason: Found Additional notes: Cre…	245766
04/07/2017 09:59:05	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 started.	245765
04/07/2017 09:58:34	John Smith (13968155)	Medium highlighted for deletion	Smartphone 01A7AC1671B18FED was highlighted for deletion.	245764
04/07/2017 09:55:58	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01A7AC1671B18FED +43123123456456 started.	245759
04/07/2017 09:23:38	John Smith (13968155)	Deletion has been undone	The authorisation Smartphone 01A7AC1671B18FED +43123123456456 for wall reader "000565F246DF929A" (Door 2) has been restored.	245752
04/07/2017 07:47:44	John Smith (13968155)	Medium added	Smartphone +43 11 22 33 55 44 66 (Mobile) added.	245690
04/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01A7AC1671B18FED +43123123456456 reactivated.	245689
04/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium started	Started reactivation of Smartphone 01A7AC1671B18FED +43123123456456. Reason: Found Additional notes: Credit: 84 KeyCredits	245688
04/07/2017 07:46:18	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01A7AC1671B18FED +43123123456456 started.	245687
04/07/2017 07:46:00	John Smith (13968155)	Medium wiped	Smartphone 01A7AC1671B18FED +43123123456456 wiped.	245686

Show 1 to 16 of 631 entries Go to

Figure 211: System event log

It is not possible to delete event log entries from the system event log.

The four-eyes principle for the event log viewing does not apply to the system event log. This means that system administrators can view the system event log at any time without the confirmation of a second system administrator.

5.8 Support logins

Creating support logins allows you to create temporary administrators if you need support for AirKey. Users can view all access control system data with support logins.

Persons with support logins are granted administrator authorisations during the validity period.

5.8.1 Creating support logins

> In the main menu select ***Administrators*** → ***Support logins***.

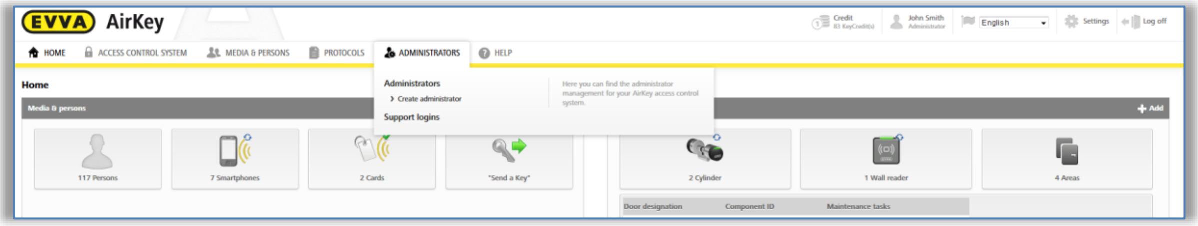
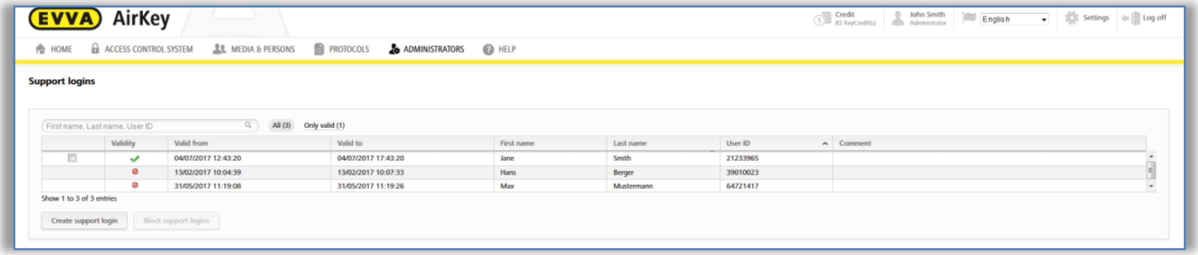


Figure 212: Support logins

Any support logins you already created are shown in a list.



Support logins

First name, Last name, User ID | All (3) | Only valid (1)

	Validity	Valid from	Valid to	First name	Last name	User ID	Comment
□	✓	04/07/2017 12:43:20	04/07/2017 17:43:20	Jane	Smith	21233965	
	⊘	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023	
	⊘	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417	

Show 1 to 3 of 3 entries

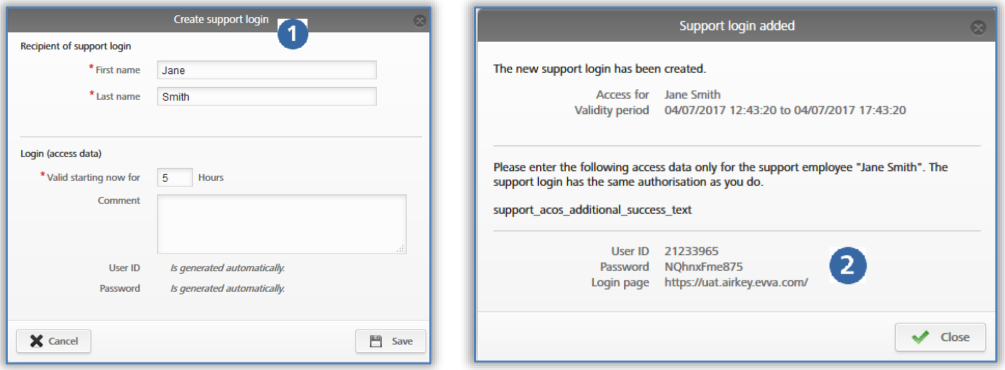
Figure 213: Support login lists

- Click ***Create support login***.
- Complete the form ❶.
  Fields highlighted by * are mandatory fields.

Logins can be assigned for periods between 1 and a maximum of 24 hours.

- Click ***Save***.

The system generates the support login, username and password ❷.



Recipient of support login

*First name: Jane
*Last name: Smith

Login (access data)

*Valid starting now for: 5 Hours
Comment:
User ID: *Is generated automatically.*
Password: *Is generated automatically.*

The new support login has been created.

Access for: Jane Smith
Validity period: 04/07/2017 12:43:20 to 04/07/2017 17:43:20

Please enter the following access data only for the support employee "Jane Smith". The support login has the same authorisation as you do.

support_acos_additional_success_text

User ID: 21233965
Password: NQhnxFme875
Login page: https://uat.airkey.evva.com/

Figure 214: Creating support logins

You will no longer be able to view the password after having closed the dialogue window.

In your own interests, we recommend you send login data securely.

- ***Close*** the "Support login created" dialogue window once you have sent the data to the corresponding support partner.

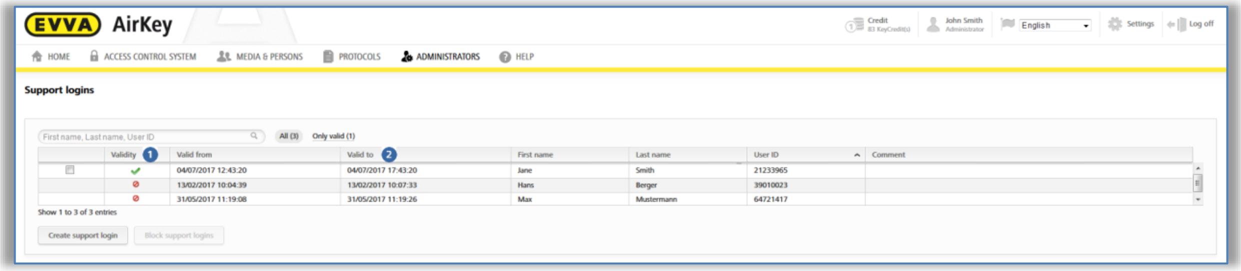
5.8.2 Blocking support logins

Support logins automatically expire after their specified validity period. However, you can also cancel support logins beforehand using the ***Block support logins*** function.

Proceed as follows to cancel support logins prematurely:

- In the main menu select ***Administrators*** → ***Support logins***.

The support logins list shows whether there are currently valid support logins ❶ and their validity period ❷.



Support logins

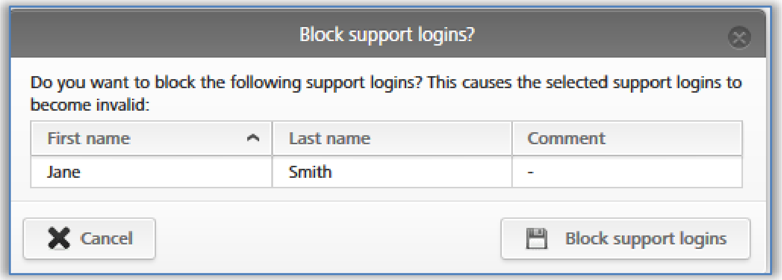
First name, Last name, User ID | All (3) | Only valid (1)

	Validity ❶	Valid from	Valid to ❷	First name	Last name	User ID	Comment
□	✓	04/07/2017 12:43:20	04/07/2017 17:43:20	Jane	Smith	21233965	
	⊘	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023	
	⊘	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417	

Show 1 to 3 of 3 entries

Figure 215: Support logins overview

- Select the recipient of the support login for whom you would like to cancel the support login.
- Click ***Block support logins***.
- Click ***Block support logins*** to confirm the security prompt.



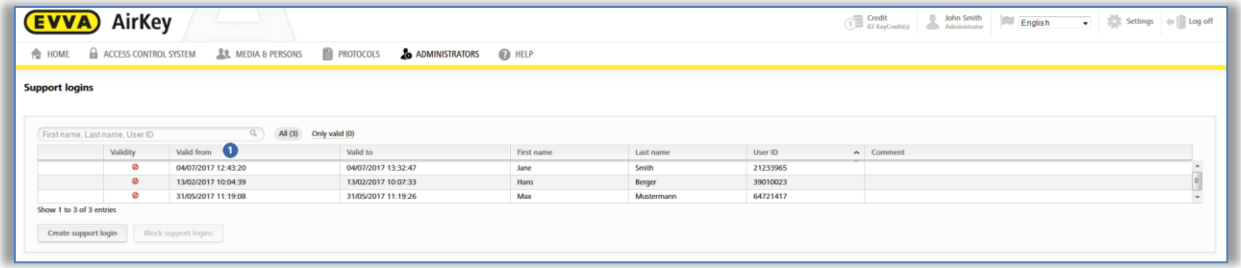
Block support logins?

Do you want to block the following support logins? This causes the selected support logins to become invalid:

First name	Last name	Comment
Jane	Smith	-

Figure 216: Blocking support logins

The icon in the "Validity" ❶ column of the support login list indicates that the login has been blocked.



Support logins

First name, Last name, User ID | All (3) | Only valid (0)

	Validity	Valid from ❶	Valid to	First name	Last name	User ID	Comment
	⊘	04/07/2017 12:43:20	04/07/2017 13:32:47	Jane	Smith	21233965	
	⊘	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023	
	⊘	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417	

Show 1 to 3 of 3 entries

Figure 217: Support login validity

Any actions by recipients of support logins as well as created or blocked support logins are recorded accordingly in the event logs.

5.9 Help

The ***Help*** section in the main menu provides additional descriptions. These are also available on the EVVA AirKey product website at https://www.evva.com/en/airkey/website/. Please contact your specialist EVVA retailer if you require any additional assistance.

6 AirKey app

This section provides an overview of the functions within the AirKey app available on your smartphone.

You must comply with the following requirements to use your smartphone for AirKey:

- The smartphone meets the system requirements.
- The AirKey app has been installed successfully on your smartphone.
- An active Internet connection is available.

! The app's functionality may be impaired if you use app optimisation features, e.g. to preserve the battery level. Potential effects include: Unlocking process takes longer, unlocking in the background not reliably operating, etc.

6.1 Bluetooth components

Click this menu item to open an overview list showing all Bluetooth locking components in range. For instance, use this page to Connect to components, unlock Bluetooth components or connect to NFC components using the icon at the top right.

! Bluetooth components will only be correctly displayed once you have updated the smartphone, i.e. the locking component designation display is not automatically changed within the AirKey app after having adapted it in the AirKey Online Administration.

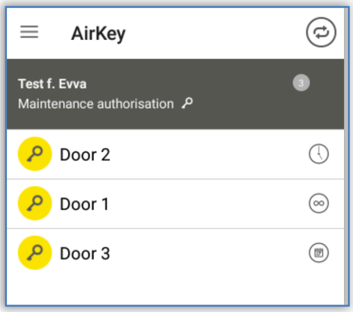
As of Android 6 Google has specified that the authorisation to locate the smartphone must be enabled to identify Bluetooth components.

6.2 Registering smartphones: See chapter 4.9

6.3 Authorisations

If your smartphone has been registered to the access control system and authorisations have already been created and assigned using the AirKey Online Administration, you can view the corresponding smartphone's authorisations at any time.

- Start the AirKey app.
- In the menu, select ***Authorisations***.


AirKey

Test f. Evva
Maintenance authorisation

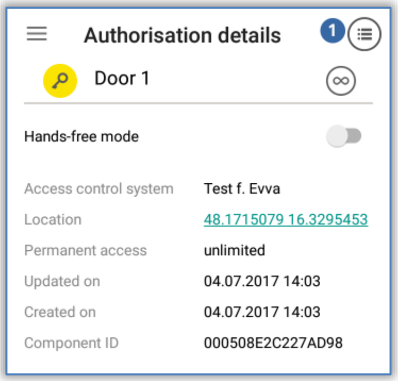
Door 2

Door 1

Door 3

Figure 218: AirKey app – authorisation overview

- Select one of the authorisations to view the details of the corresponding authorisation. This section shows the location data (GPS coordinates or address) as a link. Tap the link to be automatically forwarded to the map provider you set on your smartphone by default.
- You can also activate Hands-free mode individually for each authorisation in the authorisation details. The precondition for this is that the administrator has allowed the Hands-free mode for the locking components, for the AirKey app has not been defined a PIN code, and the Hands-free mode has been activated in the app settings.


Authorisation details ❶

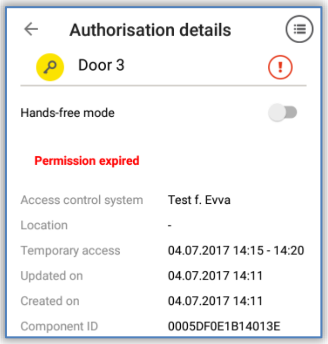
Door 1

Hands-free mode

Access control system	Test f. Evva
Location	48.1715079 16.3295453
Permanent access	unlimited
Updated on	04.07.2017 14:03
Created on	04.07.2017 14:03
Component ID	000508E2C227AD98

Figure 219: AirKey app – authorisation details

The system indicates if the access authorisation has expired.


Authorisation details

Door 3

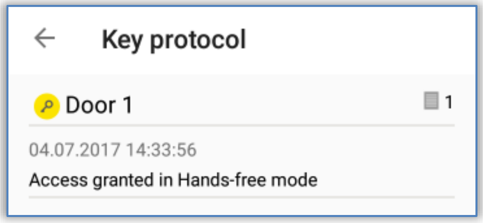
Hands-free mode

Permission expired

Access control system	Test f. Evva
Location	-
Temporary access	04.07.2017 14:15 - 14:20
Updated on	04.07.2017 14:11
Created on	04.07.2017 14:11
Component ID	0005DF0E1B14013E

Figure 220: Authorisation expired

If your smartphone has been authorised to view event log data (see Event log data in the AirKey app), you can view the key event log for the selected authorisations in the authorisation details ❶.



Key protocol

Door 1 1

04.07.2017 14:33:56

Access granted in Hands-free mode

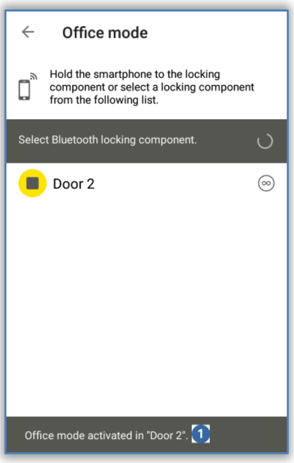
Figure 221: Event log data for authorisations

6.4 Maintenance tasks: See chapter 6.12

6.5 Office mode

Office mode requires having activated manual office mode for the locking component in the AirKey Online Administration (see Editing locking components) for Bluetooth and NFC locking components.

- Select ***Office mode*** in the AirKey app menu.
- Select a Bluetooth locking component from the displayed list or hold the smartphone to the NFC locking component.
- The locking component provides visual and audible feedback.
- A confirmation appears ❶.



Office mode

Hold the smartphone to the locking component or select a locking component from the following list.

Select Bluetooth locking component.

Door 2

Office mode activated in "Door 2". ❶

Figure 222: Office mode confirmation message

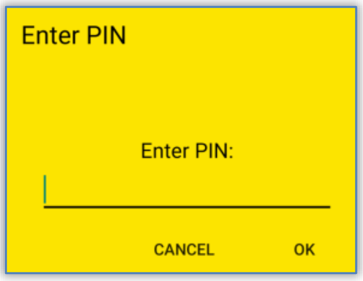
Activating office mode in AirKey components and media increases components' power consumption. Exclusively activate office mode in AirKey components and media that actually use this function.

6.6 Entering PIN code

You can temporarily save an active PIN code for a certain time within the AirKey app by using the ***Enter PIN code*** function.

- Open the menu in the AirKey app and select ***Enter PIN code***.

- Enter the correct PIN code and select ***OK***.


Enter PIN

Enter PIN:

Figure 223: AirKey app – entering PIN code

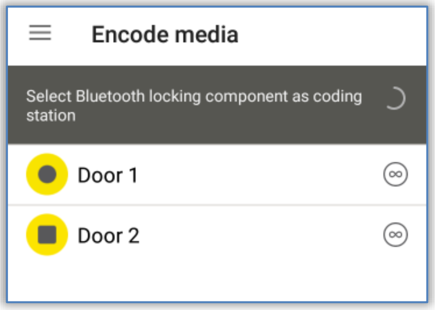
The PIN code is temporarily saved until you quit the AirKey app, move it to the background or activate the screen lock. Use it to unlock locking components without having to enter the PIN code once again.

The PIN code is also saved temporarily if its input is mandatory after having unlocked a locking component for the first time. The PIN code is no longer required the next time you unlock a locking component (same or another component). This also applies until you quit the AirKey app, move it to the background or activate the screen lock.

6.7 Encoding media

Thanks to this AirKey app function you can update access media (excluding smartphones) using locking components that are compatible with Bluetooth (cylinders, wall readers).

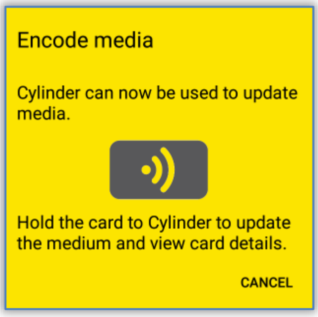
- Select ***Encode media*** in the AirKey menu.
- Select the Bluetooth locking components you would like to update from the list of displayed components.


Encode media

Select Bluetooth locking component as coding station

Figure 224: Encoding media – Bluetooth selection list – locking components

Hold the medium you would like to update to the locking component.



Encode media

Cylinder can now be used to update media.

Hold the card to Cylinder to update the medium and view card details.

CANCEL

Figure 225: Encoding media

> Now follow the instructions described in [Adding cards, key fobs, and combi keys using a smartphone]().

Start the process at the cylinder manually and not with a medium (card, key fob, combi key or wristband) to be able to use the "Encode media" function. Otherwise, the system will complete a normal unlocking procedure instead of establishing a connection to the smartphone.

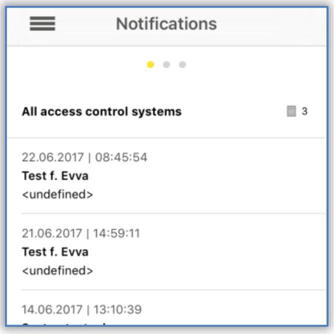
Media updates use the battery power of battery-operated locking components and thus reduce the batteries' service life. For this reason, if you intend to update a significant number of media, we recommend using an AirKey coding station, smartphone with NFC functionality or a wall reader.

Hands-free mode must be deactivated on the smartphone to enable the "Encode media" function.

6.8 Authorisation log

Select ***Authorisation log*** in the AirKey app main menu and the system opens an event log with authorisation changes executed by AirKey access control system administrators for your smartphone.

This event log is always maintained, regardless of the various settings in the AirKey Online Administration and AirKey app.



Notifications

All access control systems 3

22.06.2017 | 08:45:54
Test f. Evva
<undefined>

21.06.2017 | 14:59:11
Test f. Evva
<undefined>

14.06.2017 | 13:10:39

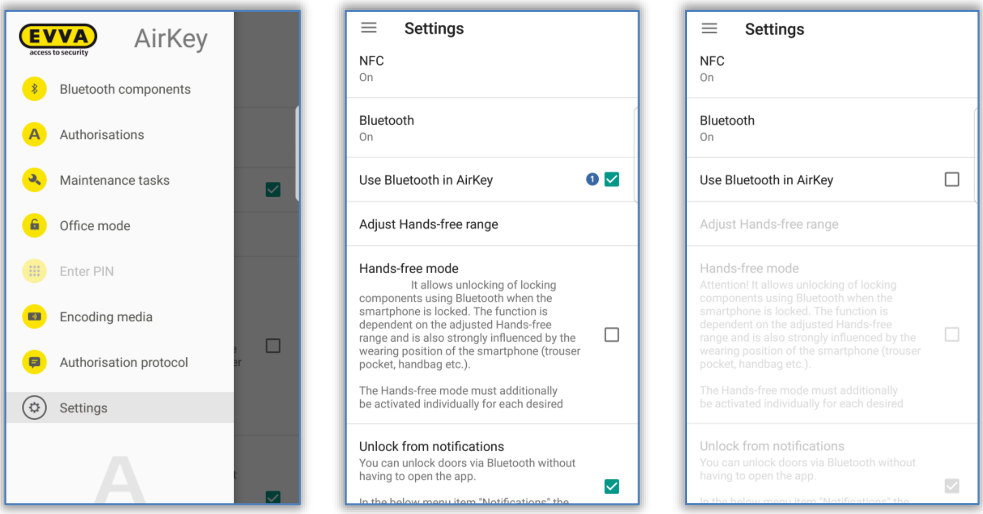
Figure 226: Authorisation log

6.9 AirKey app settings

6.9.1 AirKey app settings on Android smartphones

The ***Settings*** menu item in the AirKey app shows basic information about your Android smartphone. For instance, this section shows whether NFC or Bluetooth have been activated. Tap one of the two entries to open the device settings of your smartphones. In the continue step, specify whether you would like to activate Bluetooth for AirKey. Simply activate the corresponding "Use Bluetooth" ❶ option.

In this case, you can also configure the associated settings ("Adjust the Hands-free range", "Hands-free mode" and "Unlocking from notifications"). In this case, the home screen when you open the AirKey app is "Bluetooth components".



Settings

NFC
On

Bluetooth
On

Use Bluetooth in AirKey ❶ ☑

Adjust Hands-free range

Hands-free mode
It allows unlocking of locking components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the smartphone (trouser pocket, handbag etc.). ☐

The Hands-free mode must additionally be activated individually for each desired

Unlock from notifications
You can unlock doors via Bluetooth without having to open the app. ☑

In the below menu item "Notifications" the

Settings

NFC
On

Bluetooth
On

Use Bluetooth in AirKey ☐

Adjust Hands-free range

Hands-free mode
Attention! It allows unlocking of locking components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the smartphone (trouser pocket, handbag etc.). ☐

The Hands-free mode must additionally be activated individually for each desired

Unlock from notifications
You can unlock doors via Bluetooth without having to open the app. ☑

In the below menu item "Notifications" the

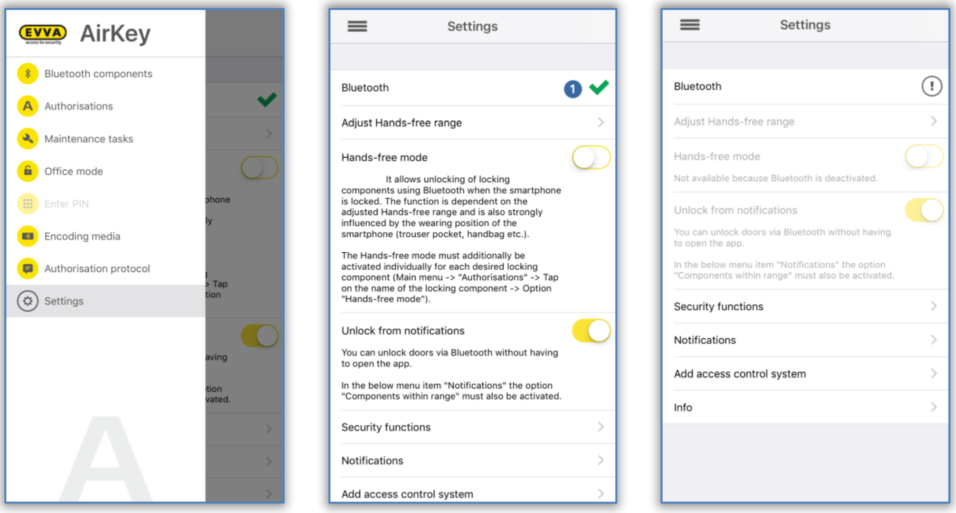
Figure 227: Android smartphone with Bluetooth – main menu / "Use Bluetooth" option activated / Option deactivated.

If you deactivate the "Use Bluetooth" option, the three aforementioned associated functions are automatically deactivated and all other Bluetooth-based functions from the main menu ("Bluetooth components", "Office mode" and "Encode media") include the "Bluetooth deactivated" note. With this configuration the smartphone can exclusively communicate with locking components using NFC.

If the Android smartphone is older and features NFC, but not Bluetooth functionalities, all Bluetooth-based functions and settings are greyed out.

6.9.2 AirKey app settings on iPhones

The ***Settings*** menu item in the AirKey app shows basic information about your iPhone. For instance, this section shows whether Bluetooth has been activated. In this case, you can also configure the associated settings ("Adjust the Hands-free range", "Hands-free mode" and "Unlocking from notifications").



It allows unlocking of locking components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the smartphone (trouser pocket, handbag etc.).

The Hands-free mode must additionally be activated individually for each desired locking component (Main menu -> "Authorisations" -> Tap on the name of the locking component -> Option "Hands-free mode").

You can unlock doors via Bluetooth without having to open the app.

In the below menu item "Notifications" the option "Components within range" must also be activated.

Not available because Bluetooth is deactivated.

You can unlock doors via Bluetooth without having to open the app.

In the below menu item "Notifications" the option "Components within range" must also be activated.

Figure 228: iPhone (Bluetooth only) – main menu / Settings without NFC-based functions / Bluetooth function deactivated

The "Bluetooth" entry in the AirKey settings merely illustrates whether Bluetooth functionality has been activated. You can still tap the "Bluetooth" entry to open the Bluetooth settings in the device settings of your iPhone.

Deactivate Bluetooth in the iPhone device settings and you will NO LONGER be able to unlock any locking components!

Deactivated Bluetooth functionality is displayed accordingly in the AirKey settings and the three associated settings are deactivated automatically, identically to all other Bluetooth-based functions from the main menu ("Bluetooth components", "Office mode" and "Encode media").

6.9.3 Adjusting the Hands-free range

If the function "Adjust the Hands-free range" is selected, a submenu appears. Here you select the locking component type for which the range should be set or whether you want to reset the ranges (for all locking components).

Cylinder range

- Initially touch cylinders to wake them up. The AirKey app then shows all active Bluetooth AirKey cylinders that are currently in range.
- Select the corresponding cylinder and move away from it as far as required to activate automatic smartphone identification.
- Press ***Save***.

Range for wall readers

- The app shows all Bluetooth AirKey wall readers that are currently in range.
- Select the corresponding wall reader and move away from it as far as required to activate automatic smartphone identification.
- Press ***Save***.

In this process, the signal strength is shown on the display. Please note that these parameters may depend on environmental factors, such as radio traffic, etc. and may deviate for the smartphone used.

The standard range is approximately 50-70 cm, however it depends on the manufacturer and device. For reasons of safety, EVVA recommends to adjust the range to approximately 30 cm.

Reset all Bluetooth ranges

By tapping on ***Reset all Bluetooth ranges***, all manually set ranges are deleted and the standard ranges are used again. A warning message confirms that the ranges have been reset.

6.9.4 Hands-free mode

Tick the ***Hands-free mode*** function to activate it. All other information regarding the Hands-free mode can be found in the chapter Hands-free at a glance.

6.9.5 Unlocking from notifications

This function allows unlocking locking components using Bluetooth without opening the AirKey app.

Tick the ***Unlock from notifications*** function to activate it.

For Android smartphones, activating this function starts a service. Even when the AirKey app is terminated, this service permanently searches for Bluetooth locking components within range and leads to increased battery consumption of the smartphone. The service is terminated as soon as the function is deactivated again. Tap on the notification of the service to go directly to the settings of the AirKey app.

As soon as your smartphone is within range of an AirKey locking component for which you have access authorisation, you will receive a notification on the lock screen or home screen of your smartphone. You can then use this notification to unlock the locking component.

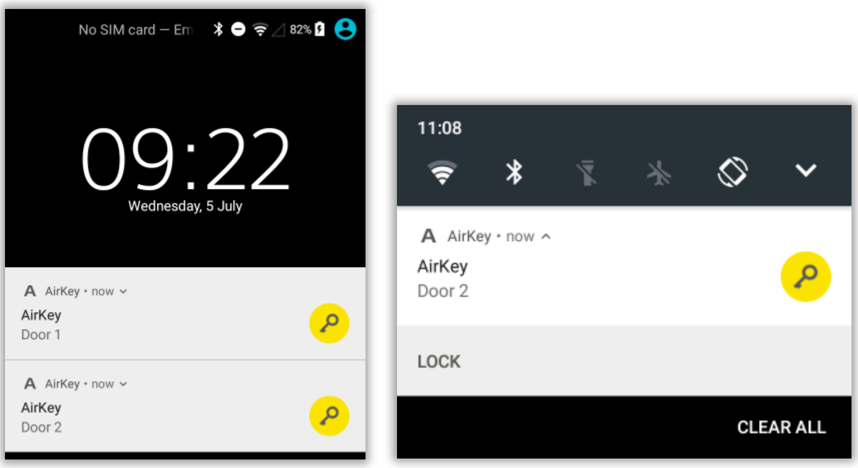


Figure 229: Unlocking from notifications – lock screen

The notification on the smartphone's lock screen is indicated by an **A** ❶ in the top left-hand corner. Pull down the top edge of the screen to show notifications indicating the locking components you can unlock.

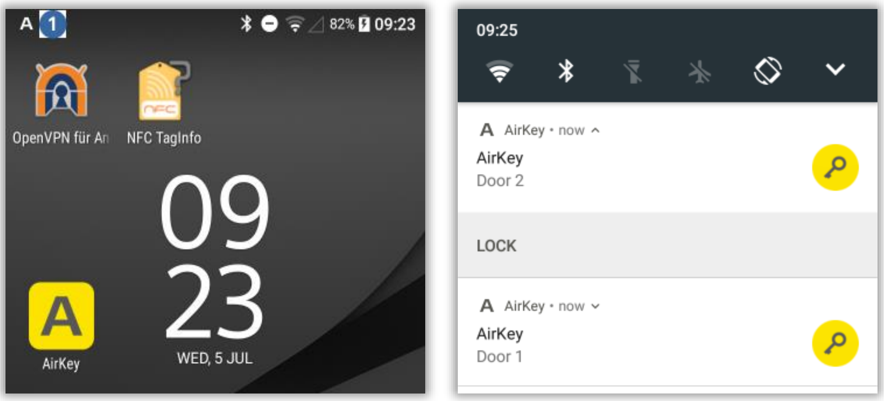


Figure 230: Unlocking from notifications

Depending on your smartphone model, you can interact with the notification by simply tapping the notification or expanding, wiping, or holding down the notification and then tapping ***Unlock***.

Depending on the setting ***Access from lock screen*** in the AirKey Online Administration settings, either you can unlock directly from the lock screen or the lock screen must be unlocked first. For more details, see General.

Unlock from notifications is only possible if the notifications for "Components in range" are activated in the settings of the AirKey app. Details about the configuration of the notifications can be found in the chapter Notifications.

6.9.6 Security functions

The ***Security functions* menu** provides three security levels:

AirKey encryption ❶

This feature involves an additional PIN code. The PIN code consists between 4 and 12 digits and prevents misuse in the event of loss or theft of the smartphone.

EVVA recommends assigning a PIN code. Make sure your PIN code is as long as possible and you do not disclose the PIN code.

Screen lock ❷

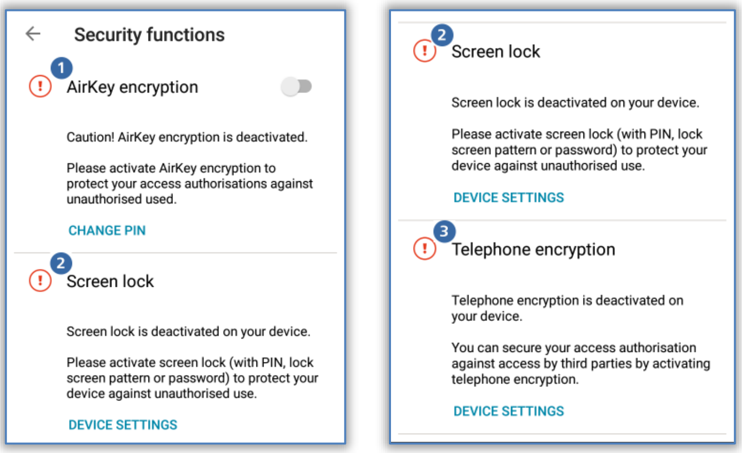
This operating system security function ensures that the smartphone screen is protected from being unlocked by third parties. Select this function and the system will take you directly to the Android smartphone settings.

EVVA recommends to activate the screen lock and disclose the PIN code to the smartphone owner only.

Telephone encryption ❸

This operating system security function ensures that smartphone data is protected from being accessed by third parties. Select this function and the system will take you directly to the Android smartphone settings.

EVVA recommends you activate telephone encryption. For this purpose, please note the information in your smartphone’s User Guide.



Security functions

1 AirKey encryption

Caution! AirKey encryption is deactivated.

Please activate AirKey encryption to protect your access authorisations against unauthorised used.

CHANGE PIN

2 Screen lock

Screen lock is deactivated on your device.

Please activate screen lock (with PIN, lock screen pattern or password) to protect your device against unauthorised use.

DEVICE SETTINGS

2 Screen lock

Screen lock is deactivated on your device.

Please activate screen lock (with PIN, lock screen pattern or password) to protect your device against unauthorised use.

DEVICE SETTINGS

3 Telephone encryption

Telephone encryption is deactivated on your device.

You can secure your access authorisation against access by third parties by activating telephone encryption.

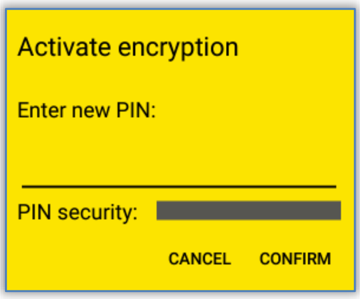
DEVICE SETTINGS

Figure 231: AirKey app – security functions

6.9.6.1 Activating PIN code

Follow the below mentioned steps to activate the PIN code:

- Open the menu in the AirKey app and select ***Settings*** → ***Security functions***.
- Activate the "AirKey encryption" option.
- Define a PIN code, re-enter it and select ***Confirm***.



Activate encryption

Enter new PIN:

PIN security:

Figure 232: AirKey app – activating PIN code

- Re-enter the PIN code and select ***Confirm*** to complete the process.

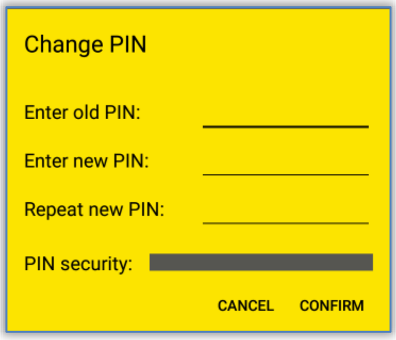
⚠ EVVA recommends assigning a PIN code. Make sure your PIN code is as long as possible and you do not disclose the PIN code. The PIN code strength is already verified upon entering the PIN code using a bar highlighted in traffic light colours (red / orange / green).

! The PIN code is required upon unlocking locking components only. There is no confirmation within the app indicating that the PIN code has been entered correctly. The PIN code may has already been defined and saved beforehand (see Entering PIN code).

6.9.6.2 Changing PIN code

Proceed as follows to retrospectively change a defined PIN code:

- Open the menu in the AirKey app and select ***Settings*** → ***Security functions***.
- Select ***Change PIN code***.
- Enter the old PIN code, define a new PIN code, re-enter it and select ***Confirm***.



Change PIN

Enter old PIN:

Enter new PIN:

Repeat new PIN:

PIN security:

Figure 233: AirKey app – changing PIN code

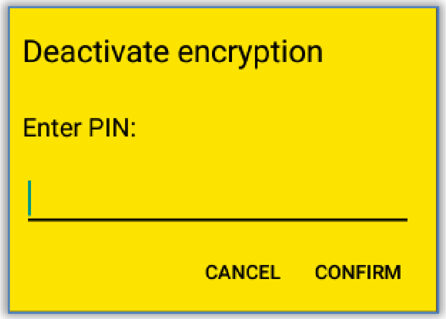
! Make sure your PIN code is as long as possible and you do not disclose the PIN code. The PIN code strength is already verified upon entering the PIN code using a bar highlighted in traffic light colours (red / orange / green).

6.9.6.3 *Deactivating PIN code*

There are two options to deactivate the pin code. If you know the PIN code, you can deactivate it directly in the smartphone's security functions. If you do not know the PIN code, administrators can reset it in the AirKey Online Administration.

Proceed as follows if you know the PIN code:

- Open the menu in the AirKey app and select ***Settings*** → ***Security functions***.
- Deactivate the "AirKey encryption" option.
- Enter the current PIN code and select ***Confirm***.



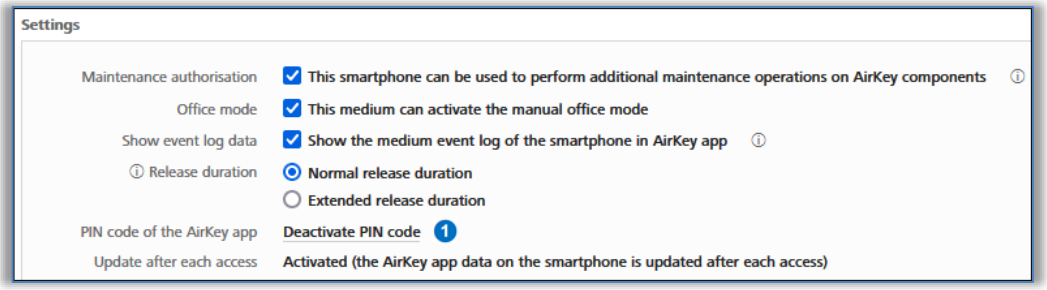
Deactivate encryption

Enter PIN:

Figure 234: AirKey app – deactivating encryption

Proceed as follows in the AirKey Online Administration to deactivate the PIN code if you do not know it:

- Log in to your access control system as an administrator.
- On the ***Home*** screen, click the ***Smartphones*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the smartphone from the overview list for which you would like to deactivate the PIN code.
- Select the ***Details*** tab to edit the details.
- Click the ***Deactivate PIN code*** ❶ link in the "Settings" section.

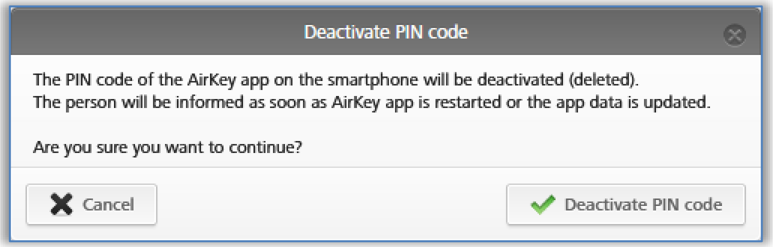


Settings

Maintenance authorisation	☑ This smartphone can be used to perform additional maintenance operations on AirKey components ⓘ
Office mode	☑ This medium can activate the manual office mode
Show event log data	☑ Show the medium event log of the smartphone in AirKey app ⓘ
ⓘ Release duration	● Normal release duration ○ Extended release duration
PIN code of the AirKey app	Deactivate PIN code ❶
Update after each access	Activated (the AirKey app data on the smartphone is updated after each access)

Figure 235: AirKey Online Administration – deactivating PIN code

- Click the ***Deactivate PIN code*** button to confirm the security prompt.



Deactivate PIN code

The PIN code of the AirKey app on the smartphone will be deactivated (deleted).
The person will be informed as soon as AirKey app is restarted or the app data is updated.

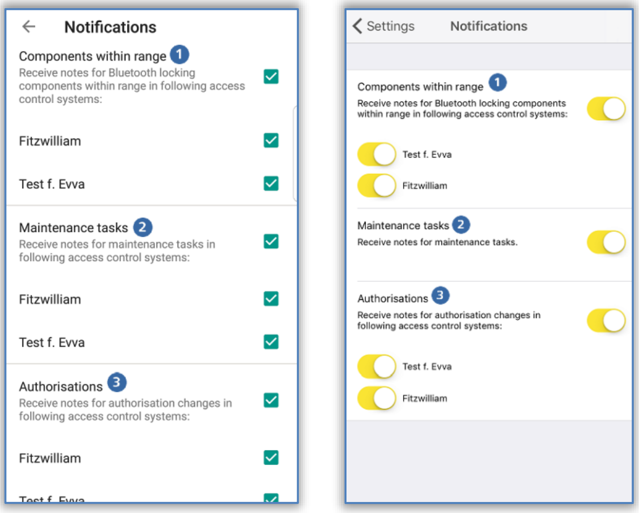
Are you sure you want to continue?

Figure 236: AirKey Online Administration – "Deactivate PIN code" dialogue

You can reactivate the PIN code at any time.

6.9.7 Notifications

Open the ***Settings*** → ***Notifications*** menu item to activate push notifications (messages on the lock and start screen of the smartphone) for components in range, maintenance tasks and authorisations as well as changes to authorisations. If the smartphone has been registered in several access control systems and features a maintenance authorisation, these access control systems will be displayed and are available for selection.



Notifications

Components within range 1
Receive notes for Bluetooth locking components within range in following access control systems: ☑

Fitzwilliam ☑

Test f. Evva ☑

Maintenance tasks 2
Receive notes for maintenance tasks in following access control systems: ☑

Fitzwilliam ☑

Test f. Evva ☑

Authorisations 3
Receive notes for authorisation changes in following access control systems: ☑

Fitzwilliam ☑

Test f. Evva ☑

Components within range 1
Receive notes for Bluetooth locking components within range in following access control systems:

Test f. Evva

Fitzwilliam

Maintenance tasks 2
Receive notes for maintenance tasks.

Authorisations 3
Receive notes for authorisation changes in following access control systems:

Test f. Evva

Fitzwilliam

Figure 237: AirKey app push notifications settings Android / iPhone

Notifications for *components in range* ❶

Activate this setting to receive corresponding push notifications to the lock or start screen of your smartphone as soon as your smartphone is within range of Bluetooth locking components. Use these notifications to unlock the corresponding door without having to manually open the AirKey app (details in the Unlocking from notifications section).

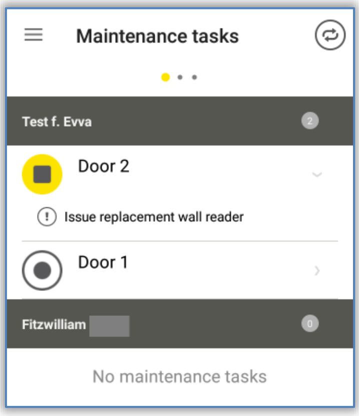
This setting is displayed by smartphones with Bluetooth 4.0 (Bluetooth Low Energy) only.

Notifications for *maintenance tasks* ❷

This setting is displayed by smartphones with maintenance authorisation only.

If this setting has been activated, the main menu of the AirKey app additionally features the ***Maintenance task*** menu item. The corresponding page lists locking components and their maintenance tasks that were created within the AirKey Online Administration.

If the smartphone has been registered in several access control systems, exclusively locking components in access control systems are listed to which the smartphone has been assigned maintenance authorisations. You will receive a push notification on your smartphone as soon as a new maintenance task has been created in the AirKey Online Administration.



Maintenance tasks

Test f. Evva 2

Door 2

Issue replacement wall reader

Door 1

Fitzwilliam [redacted] 0

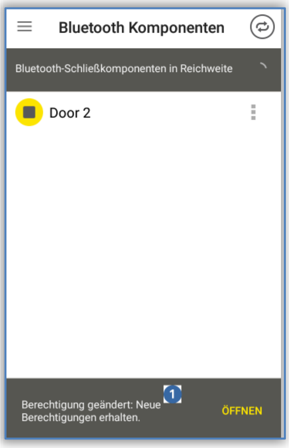
No maintenance tasks

Figure 238: Maintenance tasks

Notifications for ***authorisations*** ❸

This setting is always displayed.

Activate this setting and you will receive a notification ❶ for approximately 2 sec. at the bottom edge of the AirKey app screen (providing the app is open) whenever a new authorisation for your smartphone is created or changed in the AirKey Online Administration.



Bluetooth Komponenten

Bluetooth-Schließkomponenten in Reichweite

Door 2

Berechtigung geändert: Neue Berechtigungen erhalten. 1

ÖFFNEN

Figure 239: Notifications for changes to authorisations

If the AirKey app is not open, you will receive a corresponding push notification on the lock or start screen of your smartphone.

Regardless of the settings for notifications on authorisations a permanent entry will be added to the Authorisation log page.

6.9.8 Adding access control systems

Smartphones may be registered in more than one access control system. If you would like to add your smartphone to a further access control system, enter the registration code using the ***Add access control systems*** function. Please refer to Using smartphones in several systems for more information.

In addition, you can also scan a QR code for a smartphone replacement here. Details about the smartphone replacement can be found in the chapter Smartphone replacement.

6.9.9 Replacing smartphone

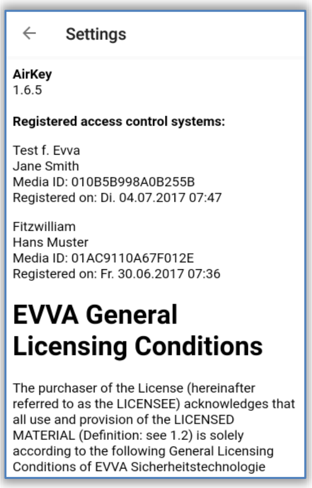
It is possible to transfer the AirKey authorisations and settings of a smartphone to a new smartphone.

Start this process with the command ***Replace smartphone***. You can find further details about this in the chapter Starting replacement from smartphone.

6.9.10 Info

Within the AirKey app there is the option to view the currently installed AirKey app version, the smartphone registration details, the media ID of the smartphone and the EVVA General Licensing Conditions.

- Start the AirKey app.
- Tap **Settings** → ***Info*** *in the menu.*



AirKey
1.6.5

Registered access control systems:

Test f. Evva
Jane Smith
Media ID: 010B5B998A0B255B
Registered on: Di. 04.07.2017 07:47

Fitzwilliam
Hans Muster
Media ID: 01AC9110A67F012E
Registered on: Fr. 30.06.2017 07:36

EVVA General Licensing Conditions

The purchaser of the License (hereinafter referred to as the LICENSEE) acknowledges that all use and provision of the LICENSED MATERIAL (Definition: see 1.2) is solely according to the following General Licensing Conditions of EVVA Sicherheitstechnologie

Figure 240: AirKey app – information

6.10 Updating smartphones

You can manually update smartphones at any time using the AirKey Online Administration to keep the access control system data up to date.

For this purpose swipe from the top to the bottom in the "Authorisations" screen in the AirKey app on an Android smartphone. The update icon appears (rotating circle).

With iPhones, pull down the "Authorisations" screen to the bottom edge. The update icon appears (rotating beams).

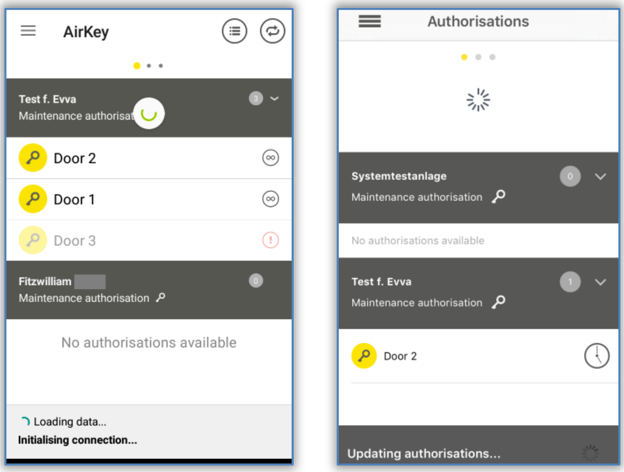

AirKey
Test f. Evva
Maintenance authorisat
Door 2
Door 1
Door 3
Fitzwilliam
Maintenance authorisation
No authorisations available
Loading data...
Initialising connection...
Authorisations
Systemtestanlage
Maintenance authorisation
No authorisations available
Test f. Evva
Maintenance authorisation
Door 2
Updating authorisations...

Figure 241: Updating Android smartphones and iPhones

AirKey uses push notifications to change smartphone data and consequently update smartphones automatically. We cannot guarantee all push notifications can be received correctly. For this reason, check whether the notifications have been received and (if applicable) update your smartphone manually.

The smartphone is automatically updated as soon as you start the AirKey app or every 12 hours an attempt is made to update the smartphone automatically, if the AirKey app has already been started.

During the update the bottom section of the AirKey app shows status information regarding the update. The update is complete once the information is no longer shown.

Optionally, the update can also take place after each access process. To do this, however, the option "Update after each access" must be activated in the respective AirKey access control system. The activation and details of this function are described in the chapter General.

6.11 Connecting to components

Use your smartphone to update any access medium (except smartphones) and any locking component regardless of their association with this access control system.

- Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** ❶ icon.
- Establishing a connection using **Bluetooth** (for Android smartphones): Tap the context menu of the locking component to which you would like to establish a connection (⁝) and then select ***Connect*** ❷.
- Establishing a connection using **Bluetooth** (for iPhones): Swipe the component designation of the locking component to which you would like to establish a connection and then select ***Connect*** ❸.

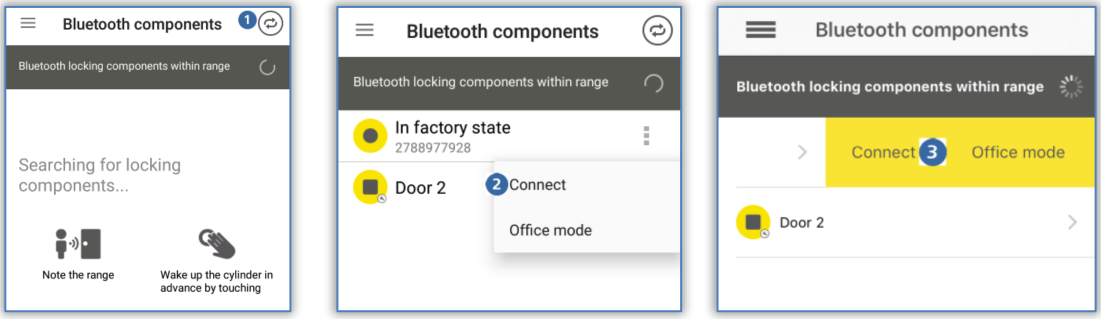
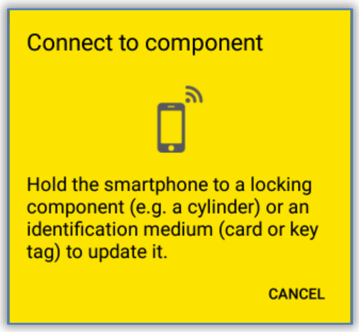

Bluetooth components
1
Bluetooth locking components within range
Searching for locking components...
Note the range
Wake up the cylinder in advance by touching
Bluetooth components
Bluetooth locking components within range
In factory state
2788977928
Door 2
2
Connect
Office mode
Bluetooth components
Bluetooth locking components within range
Connect
3
Office mode
Door 2

Figure 242: AirKey app – connecting to component (Android NFC / Android Bluetooth / iPhone)

> Follow the on-screen instructions and hold the NFC smartphone to the medium or locking component; or bring the Bluetooth smartphone into range of the locking component.



Connect to component

Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

CANCEL

Figure 243: Updating data

Data is updated. Do not remove the smartphone from the components for synchronisation during transfers. A corresponding message will appear once the process has been completed.

Deactivate the Hands-free mode before connecting to a Bluetooth locking component. Otherwise, the connection may be interrupted.

Bluetooth locking components can also be updated automatically after each Bluetooth unlocking. For more information on the "Update after each unlocking" function, see Default values (for all recently added locking components).

Regularly update your locking components. This is the only way to ensure your access control system remains secure and up to date. Please refer to Access control system operation and maintenance for more information on updating locking components.

6.12 Special authorisation "maintenance authorisation"

If the special authorisation "maintenance authorisation" has been enabled on your smartphone in the AirKey Online Administration, you have been authorised for additional maintenance operations for AirKey components. The maintenance authorisation additionally authorises you to unlock locking components in factory state, add and remove locking component and access media (except smartphones) to and from your access control system or update the firmware of locking components or the Keyring version of access media, such as cards, key fobs, combi keys or wristbands.

The "Authorisations" AirKey app page with the "Maintenance authorisation" ❶ entry in the grey bar indicates maintenance authorisation.

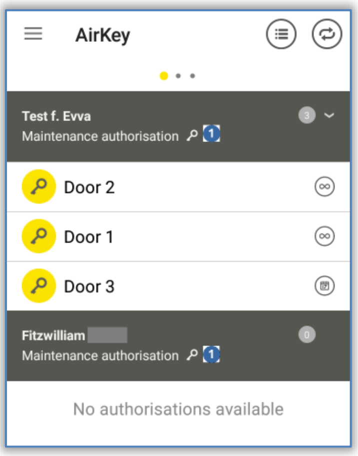

AirKey
Test f. Evva
Maintenance authorisation 1
Door 2
Door 1
Door 3
Fitzwilliam
Maintenance authorisation 1
No authorisations available

Figure 244: Maintenance authorisation

Maintenance authorisation is activated in the details of the corresponding smartphone within AirKey Online Administration. Please refer to Editing media for more information.

The ***Maintenance tasks*** ❶ menu item is additionally enabled in the AirKey app.

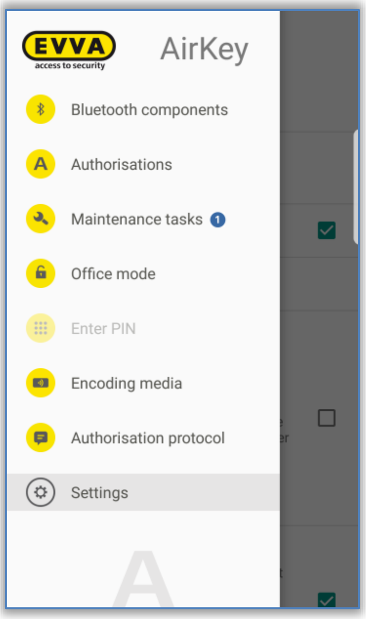
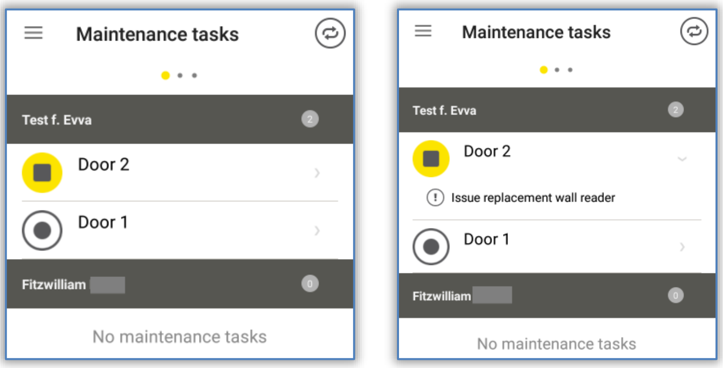


Figure 245: "Maintenance tasks" menu item in the main menu

> Select it to view a list of maintenance tasks for locking components within your access control system. Tap a locking component name to open a list of due maintenance tasks for this locking component.



Maintenance tasks

Test f. Evva 2

Door 2

Door 1

Fitzwilliam [redacted] 0

No maintenance tasks

Maintenance tasks

Test f. Evva 2

Door 2

Issue replacement wall reader

Door 1

Fitzwilliam [redacted] 0

No maintenance tasks

Figure 246: Maintenance tasks

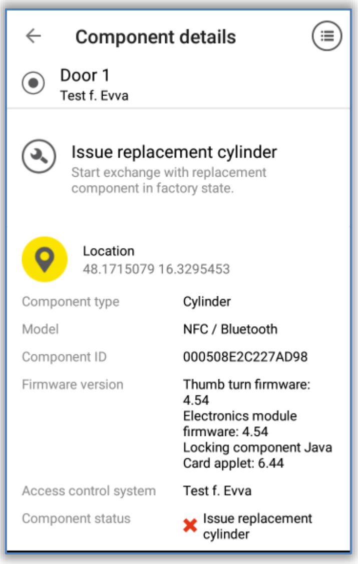
As the maintenance engineer you are responsible for regularly checking maintenance tasks to be able to quickly update any locking components where updates are required.

If you come within range of a Bluetooth locking component (cylinder ◉ or wall reader ▣) with a smartphone featuring maintenance authorisation, the icon of this locking component is highlighted in yellow (e.g. ● for cylinders).

Tap the yellow icon to establish a connection to the locking component and update the component. The system then shows component details. Due firmware updates are indicated in the component details and can be started from here.

If you update locking components as the maintenance engineer, the system shows an overview of locking component details to enable you to directly check the locking component status and cylinder events in an event log.

> Update locking components to show the component details. If available, you also see the location of the locking component as GPS coordinates or the address you manually saved in the AirKey Online Administration. Tap the yellow icon to be automatically forwarded to the map provider you set on your smartphone by default.



Door 1
Test f. Evva

Issue replacement cylinder
Start exchange with replacement component in factory state.

Location
48.1715079 16.3295453

Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Access control system	Test f. Evva
Component status	✖ Issue replacement cylinder

Figure 247: Locking component details view

Regularly update your locking components. This is the only way to ensure your access control system remains secure and up to date. Please refer to Access control system operation and maintenance for more information on updating locking components.

Maintenance authorisation applies exclusively to the access control systems for which it was activated. However, the maintenance authorisation may be activated for several access control systems at once.

Hands-free mode must be deactivated on the smartphone to enable maintenance tasks or locking component updates.

6.13 Adding locking components

Maintenance authorisation must be activated for this access control system and the locking components or access media (except for smartphones) must be in factory state to enable you to add them to your access control system using your smartphone.

6.13.1 Adding media: See chapter 4.12

6.13.2 Adding locking components: See chapter 4.11

6.14 Removing locking components

The locking component or media (except for smartphones) must have been removed from the AirKey Online Administration (see Removing locking components and Removing media) and the smartphone must have the maintenance authorisation to be able to remove locking components.

- Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** ❶ icon.
- Establishing a connection using **Bluetooth** (for Android smartphones): Tap the context menu of the locking component to which you would like to establish a connection (⋮) and then select ***Connect*** ❷.
- Establishing a connection using **Bluetooth** (for iPhones): Swipe the component designation of the locking component to which you would like to establish a connection and then select ***Connect*** ❸.

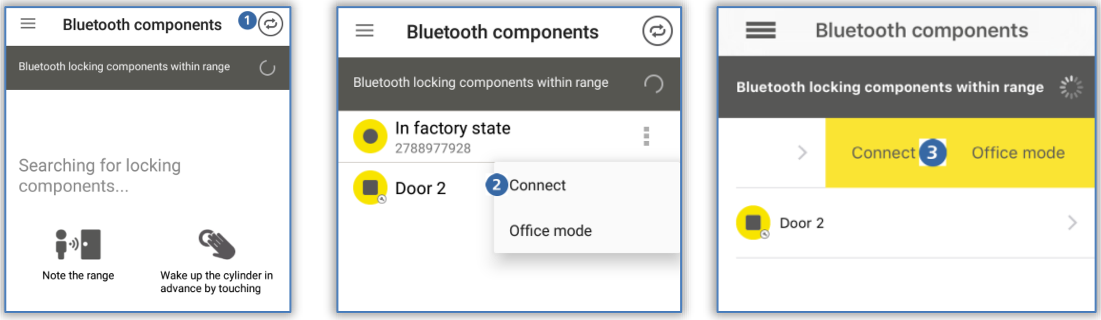
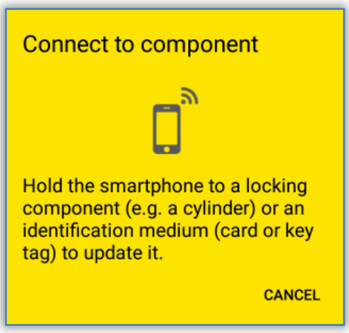

Bluetooth components
1
Bluetooth locking components within range
Searching for locking components...
Note the range
Wake up the cylinder in advance by touching
Bluetooth components
Bluetooth locking components within range
In factory state
2788977928
Door 2
2
Connect
Office mode
Bluetooth components
Bluetooth locking components within range
Connect
3
Office mode
Door 2

Figure 248: AirKey app – connecting to component (Android NFC / Android Bluetooth / iPhone)

- Follow the on-screen instructions and hold the NFC smartphone to the medium or locking component; or bring the Bluetooth smartphone into range of the locking component.

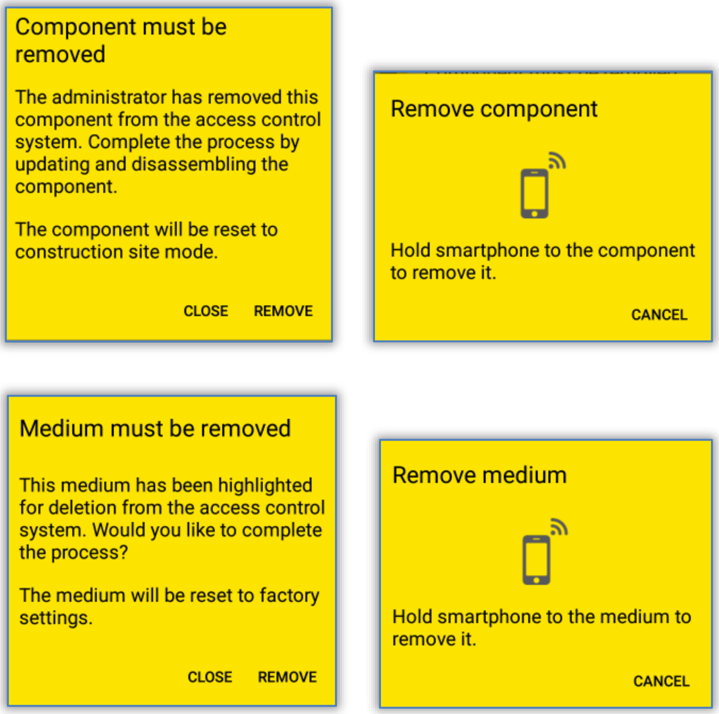

Connect to component

Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

CANCEL

Figure 249: AirKey app – connecting to component

Hold the NFC smartphone to the locking component/medium that has already been removed from the AirKey Online Administration, hold the Bluetooth smartphone within range of the component you would like to remove or directly hold it to the medium you would like to remove and follow the instructions.



Component must be removed

The administrator has removed this component from the access control system. Complete the process by updating and disassembling the component.

The component will be reset to construction site mode.

Remove component

Hold smartphone to the component to remove it.

Medium must be removed

This medium has been highlighted for deletion from the access control system. Would you like to complete the process?

The medium will be reset to factory settings.

Remove medium

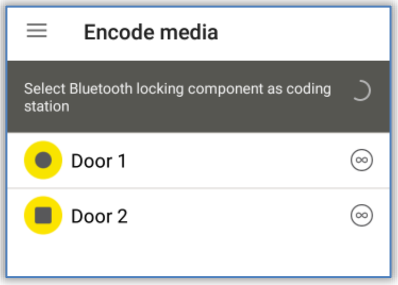
Hold smartphone to the medium to remove it.

Figure 250: Removing locking components

After having successfully updated, the locking components and media are once again in factory state.

If you would like to remove access media from the access control system using an iPhone, this process is identical to that described in ***Encoding media*** in terms of adding.

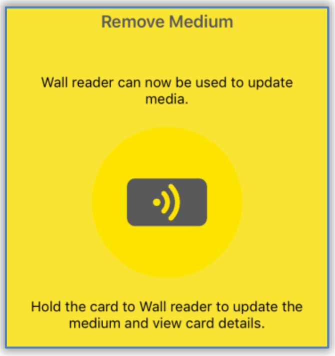
- Select the Bluetooth locking components you would like to update from the list of displayed components.



Select Bluetooth locking component as coding station

Figure 251: Encoding media – Bluetooth selection list – locking components

- Hold the medium you would like to update to the locking component.
- A message appears indicating the locking component is ready.



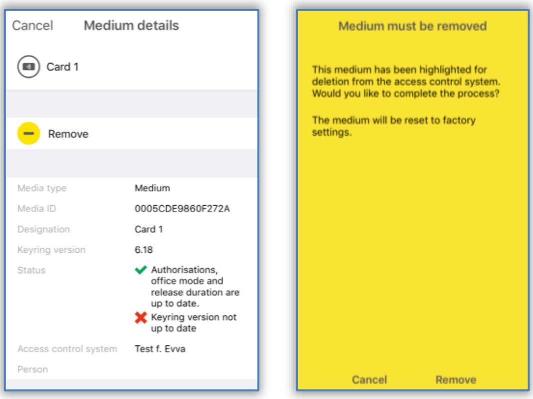
Remove Medium

Wall reader can now be used to update media.

Hold the card to Wall reader to update the medium and view card details.

Figure 252: Removing media using iPhones

> Hold the access medium to the locking component and tap ***Remove***.



Media type	Medium
Media ID	0005CDE9860F272A
Designation	Card 1
Keyring version	6.18
Status	✓ Authorisations, office mode and release duration are up to date. ✗ Keyring version not up to date
Access control system	Test f. Evva
Person	

Medium must be removed

This medium has been highlighted for deletion from the access control system. Would you like to complete the process?

The medium will be reset to factory settings.

Figure 253: Removing media

> A confirmation appears, notifying you that the access medium has been successfully removed from the access control system.

Do not remove the smartphone from the locking component or medium during this process.

The process to remove locking components and media (except for smartphones) is identical.

It is not possible to remove NFC components from the access control system using iPhones. For this purpose, you require an optional coding station or an Android smartphone with NFC functionality.

6.15 Event log data in the AirKey app

You can enable the authorisation to show event log data on smartphones via the AirKey Online Administration. Event log data can be viewed regardless of whether maintenance authorisation has been enabled or not and the function can be activated for each person individually.

Activate or deactivate the display of event log data within the AirKey Online Administration in the smartphone details section. Please refer to Editing media for more information.

Proceed as follows to open the event log within the app:

- Start the AirKey app.
- Select the ***Authorisations*** menu item from the main menu.
- Select the event log icon at the top right ❶.

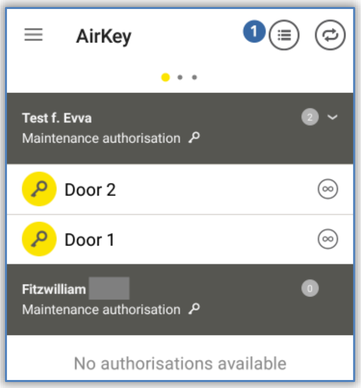

AirKey
1
Test f. Evva
Maintenance authorisation
2
Door 2
Door 1
Fitzwilliam [redacted]
Maintenance authorisation
0
No authorisations available

Figure 254: Event log icon

- The event log of the smartphone will be displayed.

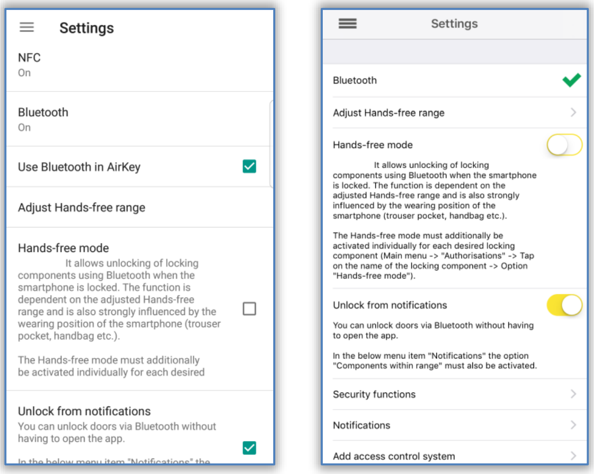
Exclusively event log entries of the person that has been assigned to the smartphone are shown in the AirKey app event log.

6.16 Hands-free at a glance

There is a Hands-free mode for Bluetooth locking components. This is a convenience function as part of which you must no longer select the locking component in the app. The Hands-free function is not identical to the "Locking with Bluetooth" function. However, it can be activated for added convenience.

After having been touched the cylinder sends a Bluetooth signal. With wall readers this process is executed automatically, without having to touch the component. If an AirKey app within the locking range receives this Bluetooth signal, the unlocking process starts. The locking range for cylinders and wall readers can be adapted individually in the app.

- Activate Hands-free mode in the main menu of the AirKey-App in the ***Settings*** menu.



NFC
On

Bluetooth
On

Use Bluetooth in AirKey ☑

Hands-free mode ☐
It allows unlocking of locking components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the smartphone (trouser pocket, handbag etc.).

The Hands-free mode must additionally be activated individually for each desired

Unlock from notifications ☑
You can unlock doors via Bluetooth without having to open the app.

Bluetooth ✓

Hands-free mode
It allows unlocking of locking components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the smartphone (trouser pocket, handbag etc.).

The Hands-free mode must additionally be activated individually for each desired locking component (Main menu -> "Authorisations" -> Tap on the name of the locking component -> Option "Hands-free mode").

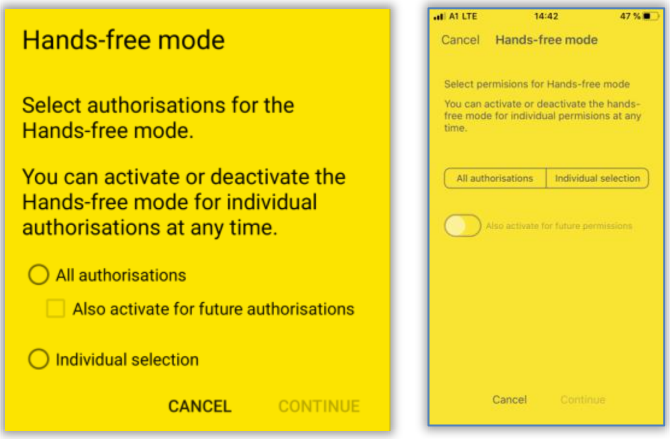
Unlock from notifications
You can unlock doors via Bluetooth without having to open the app.

In the below menu item "Notifications" the option "Components within range" must also be activated.

Figure 255: AirKey-App settings

For Android smartphones, activating this function starts a service. Even when the AirKey app is terminated, this service permanently searches for Bluetooth locking components within range and leads to increased battery consumption of the smartphone. The service is terminated as soon as the function is deactivated again. Tap on the notification of the service to go directly to the settings of the AirKey app.

- The Hands-free mode must also be activated for each locking component or area in the authorisation details at menu item ***Authorisations***. When the Hands-free mode is activated for the first time, a dialogue appears in which the function can be activated automatically for all locking components or individually only for specific locking components.



Hands-free mode

Select authorisations for the Hands-free mode.

You can activate or deactivate the Hands-free mode for individual authorisations at any time.

○ All authorisations

☐ Also activate for future authorisations

○ Individual selection

Select permisions for Hands-free mode

You can activate or deactivate the hands-free mode for individual permisions at any time.

Also activate for future permissions

Figure 256: Select permissions for Hands-free mode

Activate ***Also activate for future authorisations*** to activate Hands-free mode automatically for new authorisations.

Depending on the setting ***Access from lock screen*** in the AirKey Online Administration settings, either you can unlock directly from the lock screen or the lock screen must be unlocked first. For more details, see General.

❗ The Hands-free mode can only be used for locking components for which an administrator has allowed the Hands-free mode. Further details can be found under Editing locking components.

Adjusting the Hands-free range: See chapter 6.9.3

What must be considered when using Hands-free mode?

The function while the smartphone display is locked depends on:

- the configuration of the setting "Access from lock screen" in the AirKey Online Administration;
- manufacturer, operating system, age, number of installed apps, app optimisations (energy-saving mode) of the smartphone;
- interference factors, such as the building type (reinforced concrete designs) and the radio signal;
- where smartphones are kept or carried as well as the configured locking range for the Hands-free function;
- whether or not the smartphone is currently connected to a Wi-Fi network.

These factors will slow down the Hands-free function or it may potentially not work at all. Depending on the operating system (e.g. iOS) the smartphone must have been unlocked and the AirKey app must be running to boost Hands-free mode response times. In this case you save yourself having to select the component you would like to unlock in the app.

Note the following to prevent incorrect locking:

- There is a timeout of 2 minutes for wall readers after each unlocking process. Consequently, it will only be possible to unlock a wall reader using Hands-free mode if this smartphone has not been within the Bluetooth locking range of the wall reader for 2 minutes. This prevents unwanted unlocking processes upon leaving the locking range.
- Ideally there is only one locking component within the locking range of a smartphone.
- Hands-free mode must be deactivated in the app to enable functions, such as "Encode media" or "Update locking components".

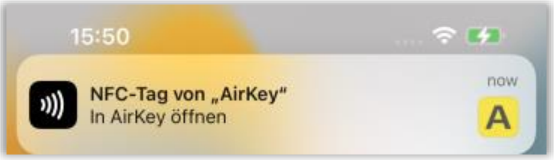
7 Operating locking components

7.1 Access with smartphones

The following requirements must have been met to be able to unlock a locking component:

- NFC or Bluetooth activated on the smartphone
- AirKey app installed and registered.
- Valid authorisation granted to the smartphone (please refer to Registering smartphones and Assigning authorisations for more information).
- Hold the smartphone to the locking component for NFC unlocking processes. The best position for data transfer depends on the smartphone model. The scanning range also depends on the smartphone type and ranges from being in contact to a few millimetres distance. In terms of unlocking processes using Bluetooth the scanning range is firstly dependent on the smartphone type and secondly on your personal settings within the AirKey app on the smartphone intended for Hands-free mode. It's range is a few metres.
- If you are required to enter a PIN code, enter the correct PIN code before you unlock using the smartphone and NFC or Bluetooth (Please refer to Security functions for details about the PIN code).
- Pay attention to the visual signals on the locking component. When using NFC do not remove the smartphone from the locking component or remain within the Bluetooth range until the locking component outputs a green signal. (A blue light merely indicates communication between smartphone and locking component).

With the iPhone models XR, XS, XS Max and newer, you can also unlock Bluetooth locking components via NFC. To do this, hold the smartphone against the locking component and tap the message that an NFC tag has been detected. The AirKey app will then open and a Bluetooth unlocking will be performed.



15:50

NFC-Tag von „AirKey"
In AirKey öffnen

now

Figure 257: iOS NFC tag

Check your authorisation or PIN code if the locking component shows a red light.

You are unable to unlock locking components using NFC when the lock screen is active or during an active call. However, the AirKey app does not necessarily have to be running or active in the foreground to be able to unlock locking components. In contrast you can unlock locking components using Bluetooth when the lock screen is active using push notifications. You must merely activate the "Unlock from notifications" options in the AirKey app settings and "Access from lock screen" in the AirKey Online Administration settings.

7.2 Access with media, such as cards, key fobs, combi keys or wristbands

The medium must have been added to the access control system and feature a valid authorisation to be granted access to a locking component (refer to Adding cards, key fobs and combi keys using a smartphone and Assigning authorisations).

- Hold the medium to the locking component. The data transfer distances depend on the medium type and usually amount to a few millimetres.
- Pay attention to the visual signals on the locking component. Do not remove the medium before the locking component emits a green signal (a blue light merely indicates communication between medium and locking component).

❗ Check your authorisation if the locking component shows a red light.

- The locking component unlocks for the set time and you are granted access.

⚠ The functionality of media, such as cards, key fobs, combi keys or wristbands may be impeded or restricted by other media or metal objects in the vicinity. This may affect media kept in a wallet or purse or on a key ring.

❗ Use the side of the combi key with the RFID icon for identification at the locking component.

8 Access control system operation and maintenance

8.1 Updating locking components

As a rule, you can update any locking component, regardless of its association with the access control system to exchange data between AirKey Online Administration and locking components.

You can update with smartphones or optionally available coding stations. Updates with the smartphone merely require the installed AirKey app and registration in any access control system.

The following tasks are completed upon updating locking components:

- Time reset.
- Event log data and battery status read out.
- Maintenance tasks (blacklist, authorisation in other access control systems, etc.) updated.
- Component details read out.

Follow the on-screen instructions to update a locking component with the smartphone:

> Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** icon ❶.

> Establishing a connection using **Bluetooth** (for Android smartphones): Tap the context menu of the locking component to which you would like to establish a connection (⋮) and then select ***Connect*** ❷.

> Establishing a connection using **Bluetooth** (for iPhones): Swipe the component designation of the locking component to which you would like to establish a connection and then select ***Connect*** ❸.

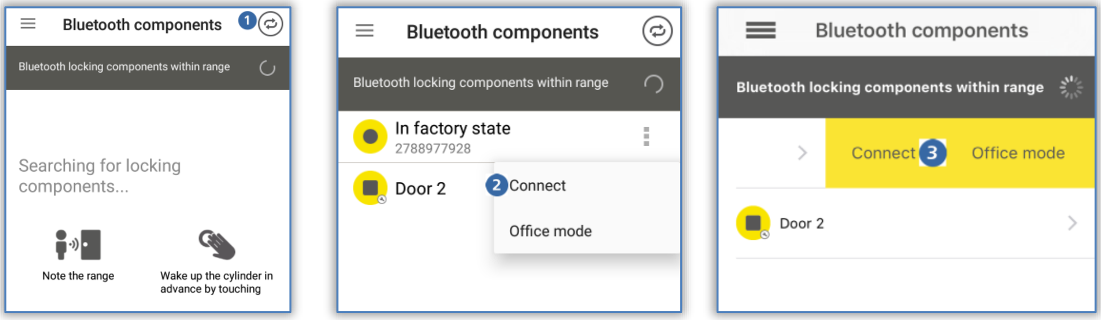
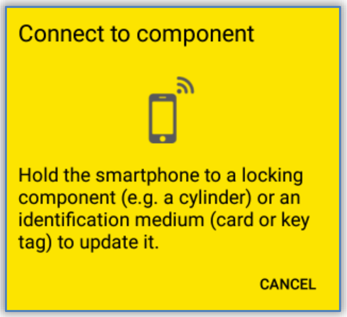

Bluetooth components
1
Bluetooth locking components within range
Searching for locking components...
Note the range
Wake up the cylinder in advance by touching
Bluetooth components
Bluetooth locking components within range
In factory state
2788977928
Door 2
2
Connect
Office mode
Bluetooth components
Bluetooth locking components within range
Connect
3
Office mode
Door 2

Figure 258: AirKey app – connecting to component (Android NFC / Android Bluetooth / iPhone)

> Follow the instructions.



Connect to component

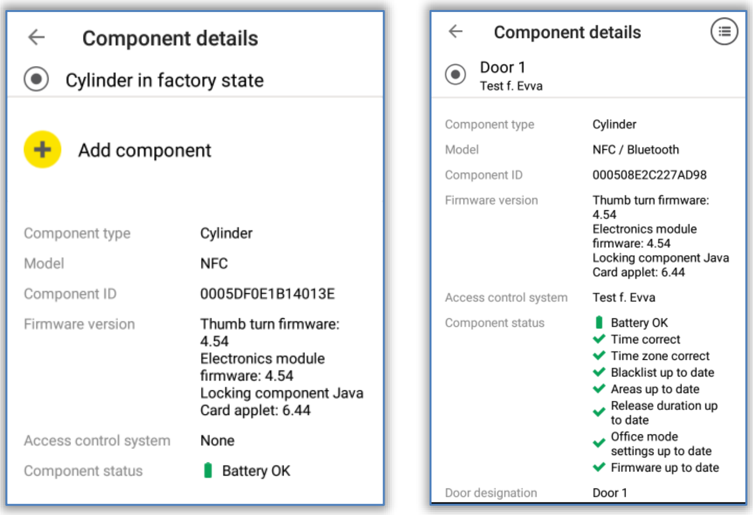
Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

CANCEL

Figure 259: Updating data

Data is updated. During transfers do not remove the NFC smartphone from the component for synchronisation or remain within the locking component range with the Bluetooth smartphone. A corresponding message will appear once the process has been completed.

The information shown in the update message varies depending on whether maintenance authorisation has been activated or not on the smartphone and whether the locking component is in your own or an external access control system.



Component details

Cylinder in factory state

Add component

Component type	Cylinder
Model	NFC
Component ID	0005DF0E1B14013E
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Access control system	None
Component status	Battery OK

Component details

Door 1
Test f. Evva

Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Access control system	Test f. Evva
Component status	Battery OK ✓ Time correct ✓ Time zone correct ✓ Blacklist up to date ✓ Areas up to date ✓ Release duration up to date ✓ Office mode settings up to date ✓ Firmware up to date
Door designation	Door 1

Figure 260: Update messages

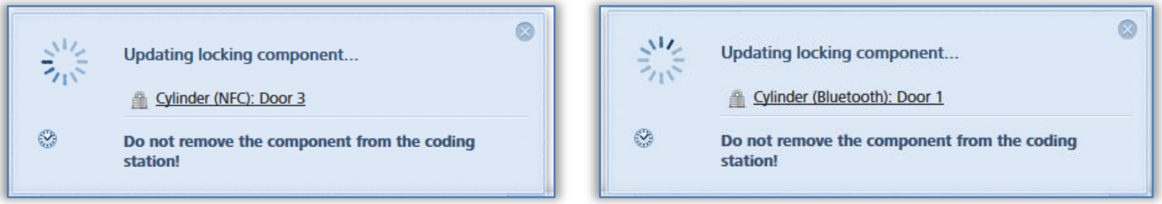
Deactivate the Hands-free mode before connecting to a Bluetooth locking component. Otherwise, the connection may be interrupted.

Bluetooth locking components can also be updated automatically after each Bluetooth unlocking. For more information on the "Update after each unlocking" function, see Default values (for all recently added locking components).

Option **Updating locking components using coding stations**

Proceed as follows to update locking components using coding stations:

- Log in to your access control system and ensure the coding station is connected and has been selected in the AirKey Online Administration.
- Place the locking component on the coding station.



Updating locking component...

Cylinder (NFC): Door 3

Do not remove the component from the coding station!

Updating locking component...

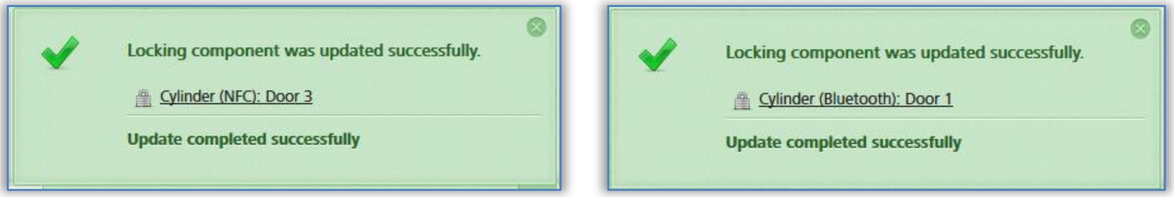
Cylinder (Bluetooth): Door 1

Do not remove the component from the coding station!

Figure 261: Updating locking components using coding stations

- Only remove the locking component from the coding station once the update has completed and the confirmation prompt appears, indicating a successful update.

The information shown in the message indicating successful completion varies depending on whether the locking component is in your own or in an external access control system.



Locking component was updated successfully.

Cylinder (NFC): Door 3

Update completed successfully

Locking component was updated successfully.

Cylinder (Bluetooth): Door 1

Update completed successfully

Figure 262: Locking components updated using coding stations

Regularly update your locking components. This is the only way to ensure your access control system remains secure and up to date.

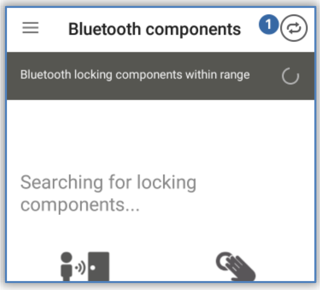
8.2 Updating smartphones: See chapter 6.10

8.3 Updating media

You can update any AirKey medium, regardless of its association to an access control system. You can update with Android smartphones or optionally available coding stations. Updates with the smartphone merely require the installed AirKey app and registration in an access control system.

With iPhones apply the process described in Encoding media to update media and use a locking component as the coding station.

- Select the ***Connect to component*** ❶ icon in the top right of the AirKey app when using an Android smartphone.

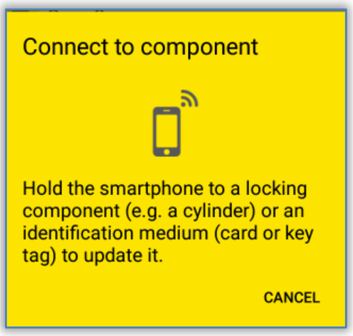

Bluetooth components

Bluetooth locking components within range

Searching for locking components...

Figure 263: "Connect to component" icon (Android smartphones only)

> Follow the on screen instructions and hold the smartphone to the medium.


Connect to component

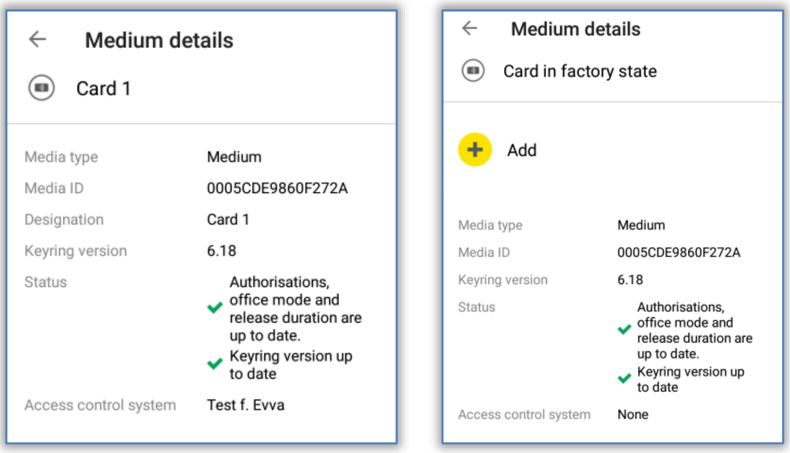
Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

CANCEL

Figure 264: Updating data

Data is updated. Do not remove the smartphone from the object you would like to synchronise during data transfers. A corresponding message will appear once the process has been completed.

When using smartphones to update combi keys directly hold the side of the combi key featuring the RFID icon to the smartphone's NFC antenna aerial.


Medium details

Card 1

Media type	Medium
Media ID	0005CDE9860F272A
Designation	Card 1
Keyring version	6.18
Status	✓ Authorisations, office mode and release duration are up to date. ✓ Keyring version up to date
Access control system	Test f. Evva

Medium details

Card in factory state

Add

Media type	Medium
Media ID	0005CDE9860F272A
Keyring version	6.18
Status	✓ Authorisations, office mode and release duration are up to date. ✓ Keyring version up to date
Access control system	None

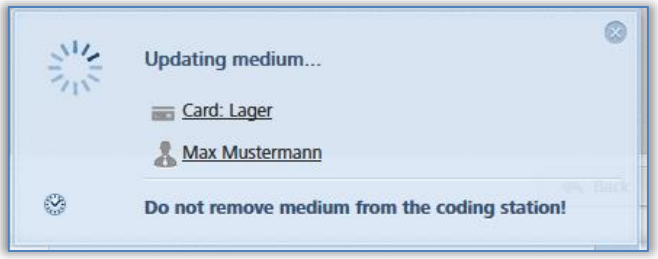
Figure 265: AirKey app updating a medium

Option

Updating media using coding stations

Proceed as follows to update cards, key fobs, combi keys or wristbands using coding stations:

- Log in to your access control system and ensure the coding station is connected and has been selected in the AirKey Online Administration.
- Place the medium on the coding station.



Updating medium...

Card: Lager

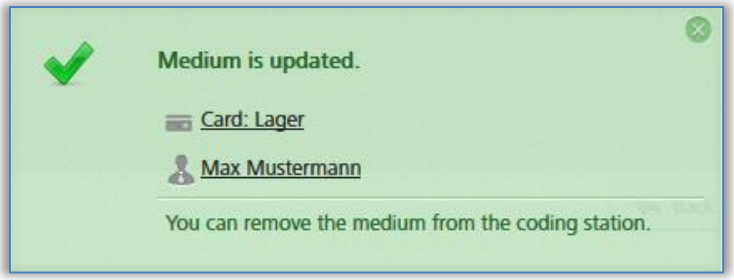
Max Mustermann

Do not remove medium from the coding station!

Figure 266: Updating media using coding stations

- Only remove the medium from the coding station once the update has completed and the confirmation prompt appears indicating a successful update.

The information shown in the notification indicating successful completion varies depending on whether the medium is in your own or in an external access control system.



Medium is updated.

Card: Lager

Max Mustermann

You can remove the medium from the coding station.

Figure 267: Updating your own or external media using coding stations

Regularly update your AirKey media. This is the only way to ensure your access control system remains secure and up to date.

Regularly update media to ensure all event log entries have been transferred from media to the AirKey Online Administration.

When using coding stations to update combi keys, hold the side of combi key featuring the RFID icon to the coding station. Updating is not possible across the entire coding station reader area – with the current type (HID Omnikey 5421) combi keys are exclusively detected in the top and the bottom third of the coding station reader area.

8.4 Updating locking component firmware

If new firmware becomes available for a locking component, a notification is shown in the locking component details of the particular locking component, in the maintenance tasks and upon updating locking components.

Please check the battery status of the locking component (cylinder) prior to firmware updates. If the "Battery low" warning is already active, replace all batteries first to ensure a smooth update process.

The current locking component firmware version is shown in the locking component details section.

You can use smartphones or optionally available coding stations to update locking component firmware.

Activate the special authorisation "maintenance authorisation" on the smartphone to enable firmware updates using the smartphone. Proceed as follows to update firmware using smartphones:

- Establishing a connection using **NFC** (for Android smartphones):
  Tap the ***Connect to component*** ❶ icon.
- Establishing a connection using **Bluetooth** (for Android smartphones): Tap the context menu of the locking component to which you would like to establish a connection (⋮) and then select ***Connect*** ❷.
- Establishing a connection using **Bluetooth** (for iPhones): Swipe the component designation of the the locking component to which you would like to establish a connection and then select ***Connect*** ❸.

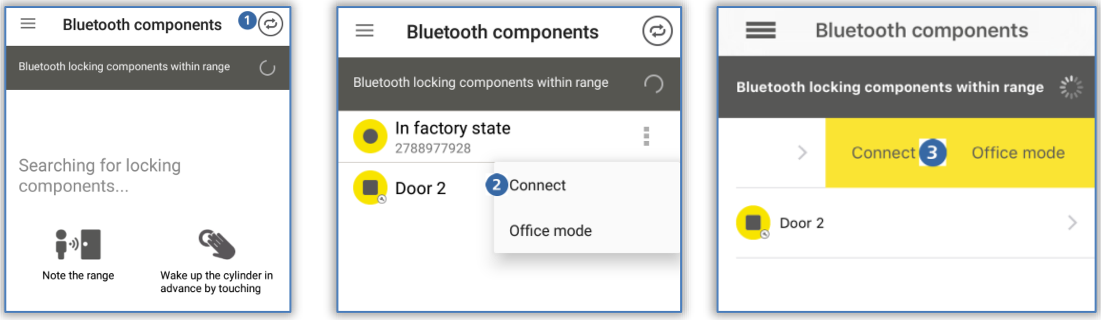
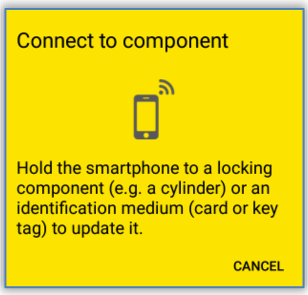

Bluetooth components
1
Bluetooth locking components within range
Searching for locking components...
Note the range
Wake up the cylinder in advance by touching
Bluetooth components
Bluetooth locking components within range
In factory state
2788977928
Door 2
2
Connect
Office mode
Bluetooth components
Bluetooth locking components within range
Connect
3
Office mode
Door 2

Figure 268: AirKey app – connecting to component (Android NFC / Android Bluetooth / iPhone)

- Follow the instructions.



Connect to component

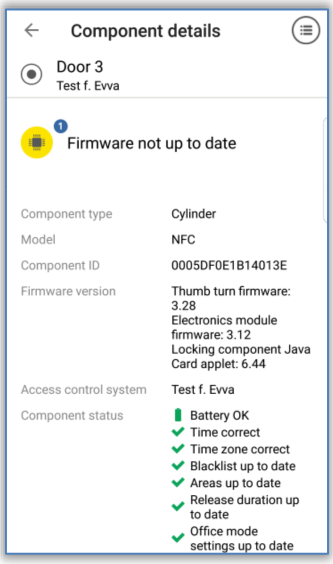
Hold the smartphone to a locking component (e.g. a cylinder) or an identification medium (card or key tag) to update it.

CANCEL

Figure 269: Connecting to component – firmware update

Data is updated. During transfers do not remove the NFC smartphone from the component for synchronisation or remain within the locking component range with the Bluetooth smartphone. A corresponding message will appear once the process has been completed.

- The locking component is updated and component details are shown. The component details indicate the component firmware is not up to date.



Component details

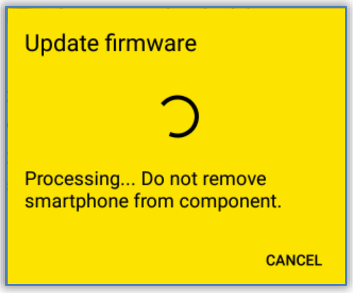
Door 3
Test f. Evva

1 Firmware not up to date

Component type	Cylinder
Model	NFC
Component ID	0005DF0E1B14013E
Firmware version	Thumb turn firmware: 3.28 Electronics module firmware: 3.12 Locking component Java Card applet: 6.44
Access control system	Test f. Evva
Component status	Battery OK ✓ Time correct ✓ Time zone correct ✓ Blacklist up to date ✓ Areas up to date ✓ Release duration up to date ✓ Office mode settings up to date

Figure 270: AirKey app – component details

- Click the ***Update firmware*** ❶ option on this screen.
- Hold the NFC smartphone to the locking component or remain within range with the Bluetooth smartphone.



Update firmware

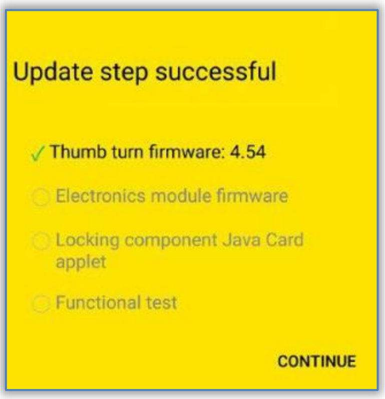
Processing... Do not remove smartphone from component.

CANCEL

Figure 271: AirKey app – updating firmware

Firmware updates may take several minutes, depending on the Internet connection. Permanently hold the NFC smartphone to the locking component or remain within the locking component's range with Bluetooth smartphones during this time.

Do not remove the smartphone from the components you would like to update during transfers. A message indicating the first update step was successful appears once the process is complete.



Update step successful

✓ Thumb turn firmware: 4.54

○ Electronics module firmware

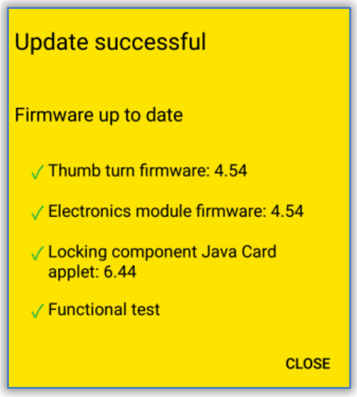
○ Locking component Java Card applet

○ Functional test

Figure 272: AirKey app – update step successful

- Remove the smartphone from the locking component until the locking component flashes and an audible signal sounds.
- Hold the NFC smartphone to the locking component or keep the Bluetooth smartphone within range of the locking component and follow the on-screen instructions.

A message indicating the firmware update was successful appears once it has been completed successfully.



Update successful

Firmware up to date

✓ Thumb turn firmware: 4.54

✓ Electronics module firmware: 4.54

✓ Locking component Java Card applet: 6.44

✓ Functional test

Figure 273: AirKey app – successful update

- Click ***Close*** to confirm the confirmation prompt and complete firmware updates.

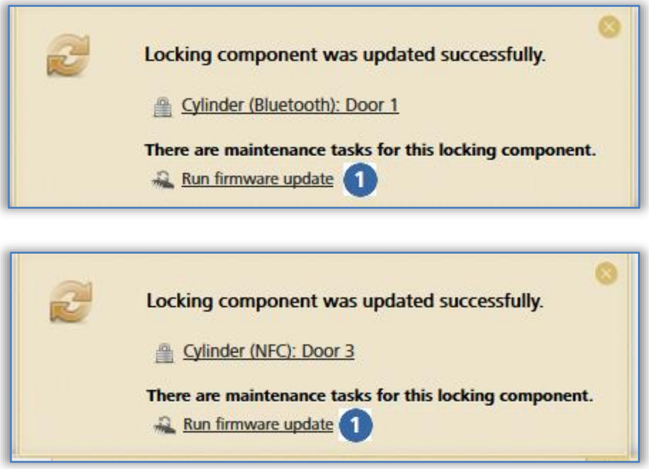
As a result, the locking component status is adapted within the entire system. The maintenance task is no longer shown and the correct firmware version is indicated in the locking component details.

Option

Updating firmware using coding stations:

- Place the locking component on the coding station. Updates launch automatically once the coding station starts communicating with the locking component.

A confirmation appears once the update has been completed.



Locking component was updated successfully.

Cylinder (Bluetooth): Door 1

There are maintenance tasks for this locking component.

Run firmware update ❶

Locking component was updated successfully.

Cylinder (NFC): Door 3

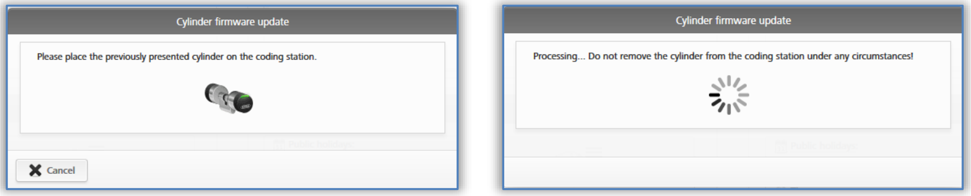
There are maintenance tasks for this locking component.

Run firmware update ❶

Figure 274: Coding station – confirmation upon updating locking components

A corresponding link ❶ is shown if a firmware update is available for the locking component.

- Click ***Execute firmware update*** to start the process.



Cylinder firmware update

Please place the previously presented cylinder on the coding station.

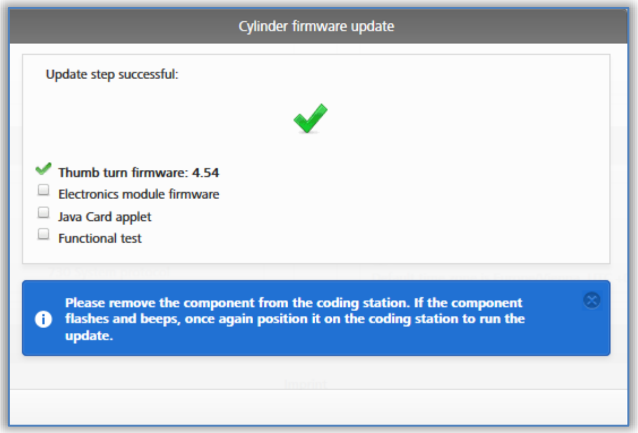
Cylinder firmware update

Processing... Do not remove the cylinder from the coding station under any circumstances!

Figure 275: Coding station – firmware update for cylinder

Firmware updates may take several minutes, depending on the Internet connection. Do not remove the locking component from the coding station during this period.

A confirmation prompt completes the first step of the firmware update.



Update step successful:

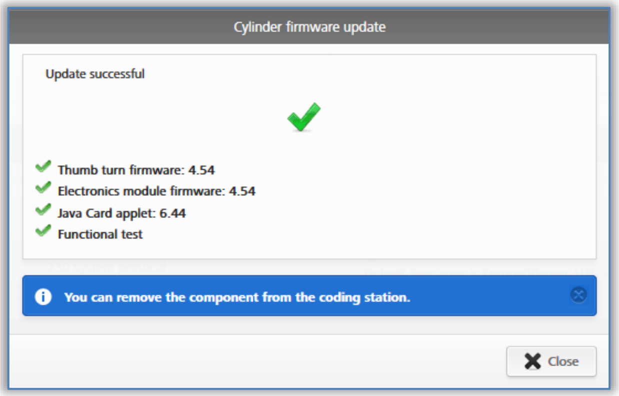
✓ Thumb turn firmware: 4.54
□ Electronics module firmware
□ Java Card applet
□ Functional test

Please remove the component from the coding station. If the component flashes and beeps, once again position it on the coding station to run the update.

Figure 276: Coding station – update step successful

- Remove the locking component from the coding station until the locking component restarts with visual and audible feedback.
- Once again place the locking component on the coding station to complete the process.

A corresponding message will appear once the update has been completed successfully.



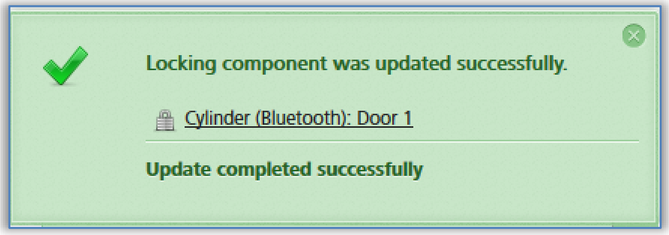
Update successful

✓ Thumb turn firmware: 4.54
✓ Electronics module firmware: 4.54
✓ Java Card applet: 6.44
✓ Functional test

You can remove the component from the coding station.

Figure 277: Coding station – firmware update successful

The locking component is once again updated after having closed the confirmation prompt.


Locking component was updated successfully.

Cylinder (Bluetooth): Door 1

Update completed successfully

Figure 278: Coding station – locking component updated successfully

- Remove the locking component from the coding station after having updated it.

As a result, the locking component status is adapted within the entire system. The maintenance task is no longer shown and the correct firmware version is indicated in the locking component details.

Open the door and secure it against accidentally slamming shut during firmware updates. Subsequently check the locking component operates as intended before you once again close the door.

When updating locking component firmware, ensure a stable Internet connection is available and the data connection does not cut out during the firmware update. For this purpose, a host of settings are available, depending on the corresponding smartphone and operating system (e.g. permit automatic network changes between mobile data networks and Wi-Fi networks).

EVVA recommends to always keep locking component firmware up to date.

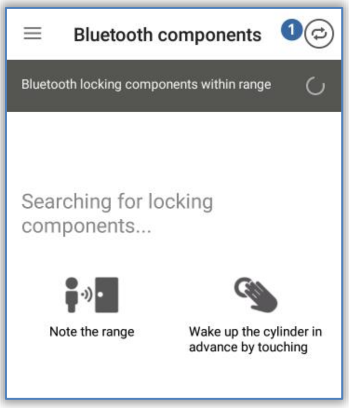
8.5 Updating the Keyring version of media

In the AirKey system, "Keyring" is the name of a software program that manages all AirKey-relevant data stored on passive access media such as cards, key fobs, combi keys, and wristbands. If new Keyring versions become available for such media, this information is shown in the media details of each medium, in the maintenance tasks, on the ***Home*** screen and upon updating locking components.

The medium’s current Keyring version is shown in the locking component details section.

You can use smartphones or optionally available coding stations to update media’s Keyring. Activate the special authorisation "maintenance authorisation" on the smartphone to enable Keyring updates using the smartphone. Proceed as follows to update the Keyring using smartphones:

- Establishing a connection using **NFC** (for Android smartphones):
  Tap the ***Connect to component*** icon ❶.
- Establishing a connection using ***Bluetooth*** (for Android smartphones and iPhones): Select the ***Encoding media*** menu item from the AirKey app main menu – refer to Encoding media.



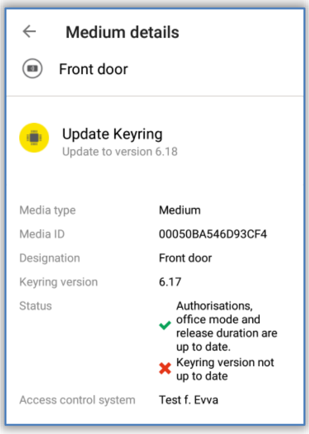
Bluetooth components

Bluetooth locking components within range

Searching for locking components...

Figure 279: AirKey app – connecting to component

- Hold the NFC smartphone to the medium.
- The system updates the medium. It indicates that a new Keyring version is available.



Medium details

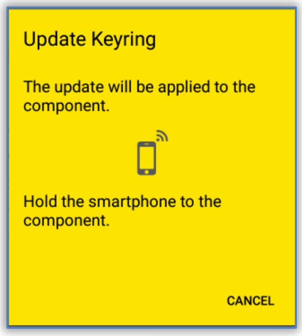
Front door

Update Keyring
Update to version 6.18

Media type	Medium
Media ID	00050BA546D93CF4
Designation	Front door
Keyring version	6.17
Status	✓ Authorisations, office mode and release duration are up to date. ✗ Keyring version not up to date
Access control system	Test f. Evva

Figure 280: AirKey app – media details

- Select the ***Update Keyring*** option***.***
- Hold the smartphone to the medium and follow the on screen instructions.



Update Keyring

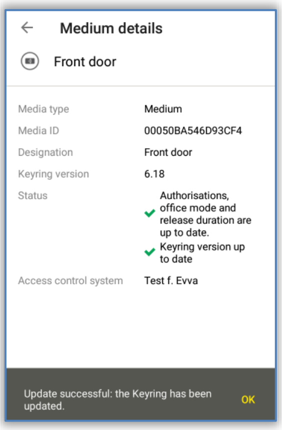
The update will be applied to the component.

Hold the smartphone to the component.

Figure 281: AirKey app – updating the Keyring

Keyring updates may take several minutes, depending on the Internet connection. Permanently hold the smartphone to the medium during this time.

Do not remove the smartphone from the medium you would like to update during data transfers. A message indicating that the Keyring update was successful appears once the process is complete.


Medium details

Front door

Media type	Medium
Media ID	00050BA546D93CF4
Designation	Front door
Keyring version	6.18
Status	✓ Authorisations, office mode and release duration are up to date. ✓ Keyring version up to date
Access control system	Test f. Evva

Update successful: the Keyring has been updated.

Figure 282: AirKey app – Keyring update successful

As a result, the media status is adapted within the entire system. The correct Keyring version is shown in the media details.

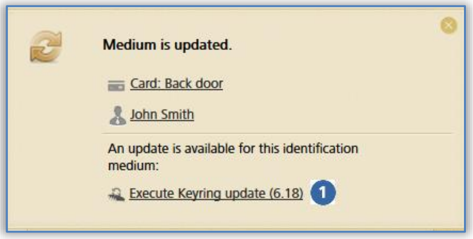
When using smartphones to update combi keys hold the side of combi key featuring the RFID icon to the smartphone.

Option

Updating the Keyring using coding stations:

- Place the medium on the coding station. Updates are started automatically once the coding station identifies the medium.

A confirmation appears once the update has been completed.


Medium is updated.

Card: Back door

John Smith

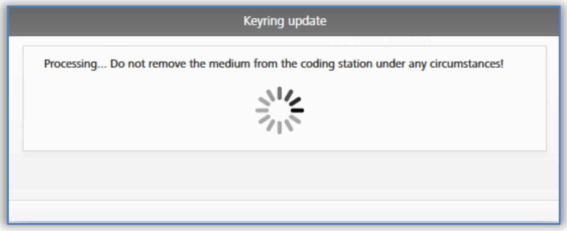
An update is available for this identification medium:

Execute Keyring update (6.18) 1

Figure 283: Coding station – a Keyring update is available

A corresponding link ❶ is shown if a firmware update is available for the locking component.

- Click ***Execute Keyring update (x.x)*** to start the update.



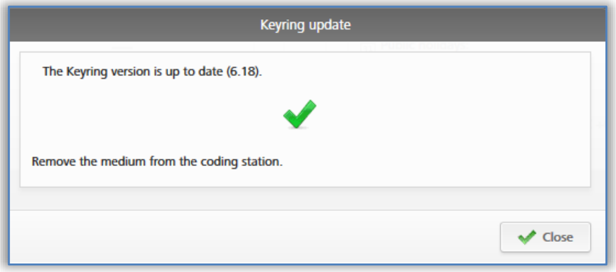
Keyring update

Processing... Do not remove the medium from the coding station under any circumstances!

Figure 284: Coding station – Keyring update

Keyring version updates may take several minutes, depending on the Internet connection. Do not remove the medium from the coding station during this period.

Do not remove medium from the coding station during the Keyring is updating. Keyring version updates are completed by a confirmation prompt.



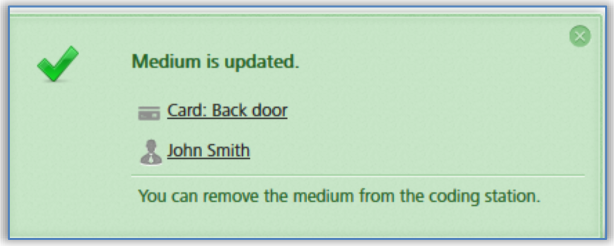
Keyring update

The Keyring version is up to date (6.18).

Remove the medium from the coding station.

Figure 285: Coding station – Keyring update successful

You have now successfully completed the Keyring update. The medium is once again updated after having closed the confirmation prompt.



Medium is updated.

Card: Back door

John Smith

You can remove the medium from the coding station.

Figure 286: Coding station – medium updated successfully

> Remove the medium from the coding station after having updated it.

When using coding stations to update combi keys, hold the side of combi key featuring the RFID icon to the coding station. Updating is not possible across the entire coding station reader area – with the current type (HID Omnikey 5421) combi keys are exclusively detected in the top and the bottom third of the coding station reader area.

As a result, the media status is adapted within the entire system. The correct Keyring version is shown in the media details.

When updating media Keyring versions, ensure a stable Internet connection has been established and the data connection does not change during the Keyring update. For this purpose, a host of settings are available depending on the corresponding smartphone or operating system (e.g. permit automatic network changes between mobile data networks and Wi-Fi networks, avoid unfavourable Internet connections, etc.).

EVVA recommends to always keep media Keyring versions up to date.

8.6 Updating smartphones' app versions

A corresponding message appears on smartphones if a new AirKey app update is available. Depending on the Google Play Store or Apple App Store settings, the AirKey app is automatically updated or updated only after having manually confirmed the update.

You can continue to use the AirKey app as usual once you have completed the app version update.

You require a Google account or Apple ID to download apps from the Google Play Store or Apple App Store.

It may be the case that AirKey app updates are recommended or mandatory. In such cases, a corresponding message appears in the AirKey app. This will restrict certain functions. However, you will continue to be able to unlock locking components.

EVVA recommends always keeping the AirKey app version for smartphones up to date and activating automatic app updates in the Google Play Store or Apple App Store.

8.7 Replacing batteries and using the emergency power device

Regularly replace the batteries in battery-operated locking components. Check the battery status of locking components in the AirKey Online Administration and when updating locking components using smartphones with maintenance authorisation.

The system differentiates three, different battery states.

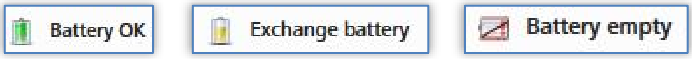


Figure 287: Battery status

The locking component itself outputs a special "battery empty" warning signal upon unlocking media. Please refer to Locking components signals for more information about signals.

8.7.1 Battery replacements in AirKey cylinders

❗ Replace batteries when the door is open and secured so it does not accidentally slam shut.

Please note the AirKey cylinder time remains active for a maximum of one minute after having removed the batteries.

We highly recommend replacing the seals of the AirKey cylinder upon replacing batteries to continue to guarantee the unit is correctly protected from humidity. In this process, the seal between thumb turn sleeve and outside thumb turn as well as the seals in the thumb turn disc of the outside thumb turn are affected. All these seals are available as spare parts. For this purpose, please contact your specialist EVVA retailer.

We highly recommend lubricating AirKey cylinders, at minimum upon replacing batteries. For this purpose, apply a drop of the lubricant recommended by EVVA between the thumb turn sleeve and the cylinder housing from the outside after having removed the outside thumb turn. We additionally recommend you lubricating the rear of the cylinder between cam and cylinder housing if you temporarily remove the AirKey cylinder. For this purpose, please contact your specialist EVVA retailer.

> Lock the locking component using a valid medium.
> Position the assembly tool on the cylinder before it disengages.
> Remove the thumb turn of the cylinder with the positioned assembly tool by turning the screw anti-clockwise.
> Remove the assembly tool from the thumb turn.
> Open the thumb turn by undoing the three screws on the rear of the thumb turn.
> Remove the thumb turn disc of the thumb turn.
> Carefully undo the battery holder by moving it upwards.
> Subsequently replace the batteries. Ensure you re-insert the batteries correctly. In this process, do not use old and new batteries together.
> Carefully secure the battery holder.
> Position the thumb turn disc on the thumb turn and secure it with the three screws.
> Position the assembly tool on the thumb turn.
> Ensure the seal has been positioned correctly on the cylinder axis and once again attach the thumb turn to the cylinder by turning it clockwise until you feel a resistance.
> Remove the assembly tool.
> Subsequently turn the thumb turn anti-clockwise until you notice it engages.
> Ensure the thumb turn and electronics module have engaged correctly.

- In a last step, update the cylinder using your smartphone or coding station to transfer the most recent event log entries to the AirKey Online Administration.
- Check the cylinder operates correctly by attempting to unlock it before you once again close the door.

⚠ On the basis of physical battery properties, you must replace batteries at an earlier stage and monitor the battery states and cylinder functions in low temperatures (below -10 °C) over a prolonged period of time.

⚠ If the component indicates a communication fault after having replaced the batteries, this is caused by the thumb turn attempting to communicate with the electronics module. This does not work if the thumb turn has been screwed to the electronics module.

Check locking components' battery status using smartphones with maintenance authorisation by updating the locking component and then viewing the component details.

If you are unable to replace batteries in due time, there is the option to open the locking component using the optionally available emergency power device.

Please refer to the Emergency power device section for a more detailed description.

⚠ After having operated a locking component using an emergency power device, replace the batteries before once again closing the door.

After use carefully re-seal the white rubber cover featuring the EVVA logo to continue to protect the emergency power device connector from penetrating dust and humidity. For this purpose, do not use pointed objects to prevent damage.

8.8 Repair options

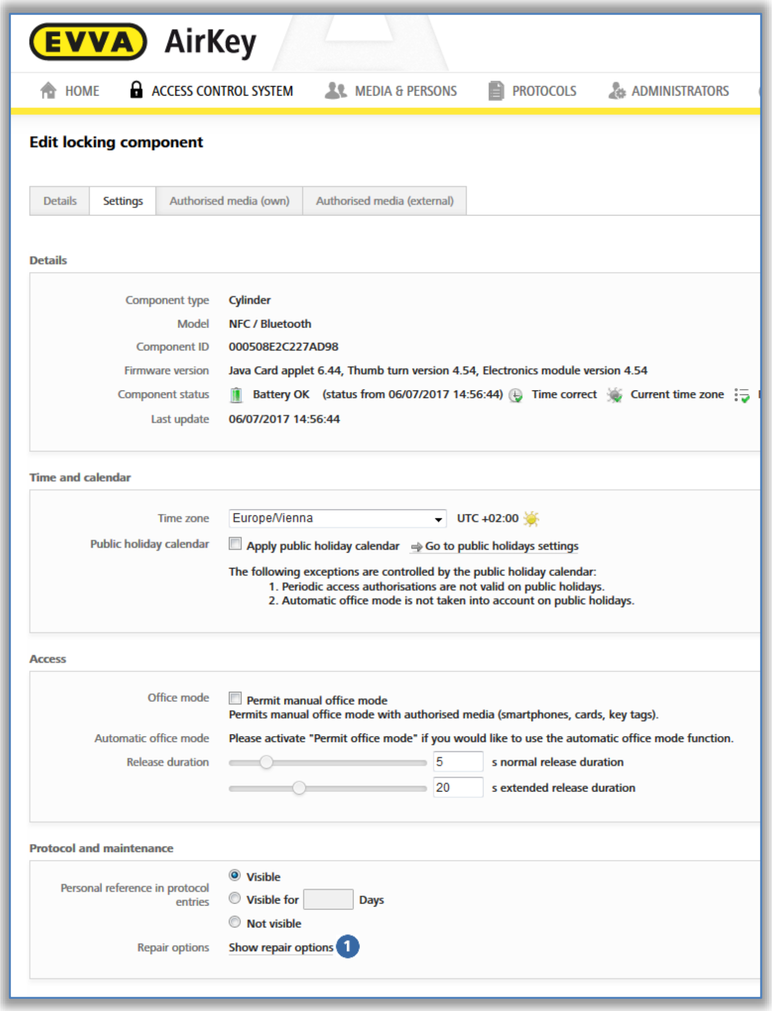
Locking components' repair options enable reactions to locking component faults. There is the option to issue replacement locking components within the access control system or remove a faulty locking component from the access control system.

8.8.1 Issuing and installing replacement locking components

Issuing and subsequently installing replacement locking components to replace existing, faulty locking components with locking components in factory state. As a result, all properties and authorisations for this locking component within the access control system are maintained. After this process, the replacement locking component is no longer in factory state.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.
- Alternatively, select ***Access control system*** → **Locking components** in the main menu.
- Click the locking component you would like to edit in the overview.

> In the ***Settings*** tab go to the ***Logging and repair options*** section and click on ***Show repair options*** ❶.



Edit locking component

Details | Settings | Authorised media (own) | Authorised media (external)

Details

Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status	Battery OK (status from 06/07/2017 14:56:44) Time correct Current time zone
Last update	06/07/2017 14:56:44

Time and calendar

Time zone: Europe/Vienna UTC +02:00

Public holiday calendar: □ Apply public holiday calendar ⇨ Go to public holidays settings

The following exceptions are controlled by the public holiday calendar:
1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

Access

Office mode: □ Permit manual office mode
Permits manual office mode with authorised media (smartphones, cards, key tags).

Automatic office mode: Please activate "Permit office mode" if you would like to use the automatic office mode function.

Release duration: 5 s normal release duration
20 s extended release duration

Protocol and maintenance

Personal reference in protocol entries: ● Visible
○ Visible for Days
○ Not visible

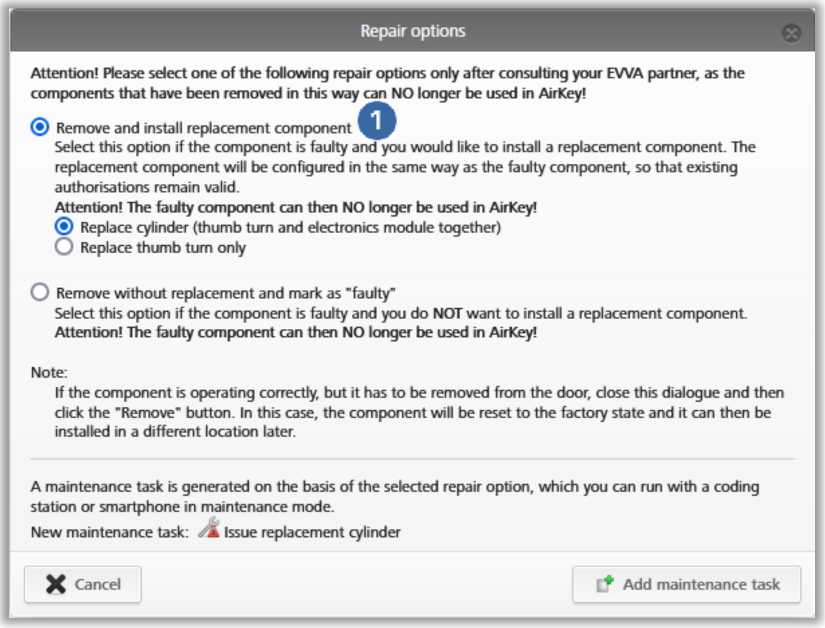
Repair options: Show repair options 1

Figure 288: Editing locking components – repair options

The ***Repair options*** dialogue window opens.

> The ***Disassemble and install the replacement component*** ❶ and ***Replace cylinder (thumb turn and electronics module together)*** radio buttons have been made available by default.

> Alternatively select the ***Replace thumb turn only*** radio button.



Repair options

Attention! Please select one of the following repair options only after consulting your EVVA partner, as the components that have been removed in this way can NO longer be used in AirKey!

● Remove and install replacement component 1

Select this option if the component is faulty and you would like to install a replacement component. The replacement component will be configured in the same way as the faulty component, so that existing authorisations remain valid.

Attention! The faulty component can then NO longer be used in AirKey!

● Replace cylinder (thumb turn and electronics module together)

○ Replace thumb turn only

○ Remove without replacement and mark as "faulty"

Select this option if the component is faulty and you do NOT want to install a replacement component.

Attention! The faulty component can then NO longer be used in AirKey!

Note:

If the component is operating correctly, but it has to be removed from the door, close this dialogue and then click the "Remove" button. In this case, the component will be reset to the factory state and it can then be installed in a different location later.

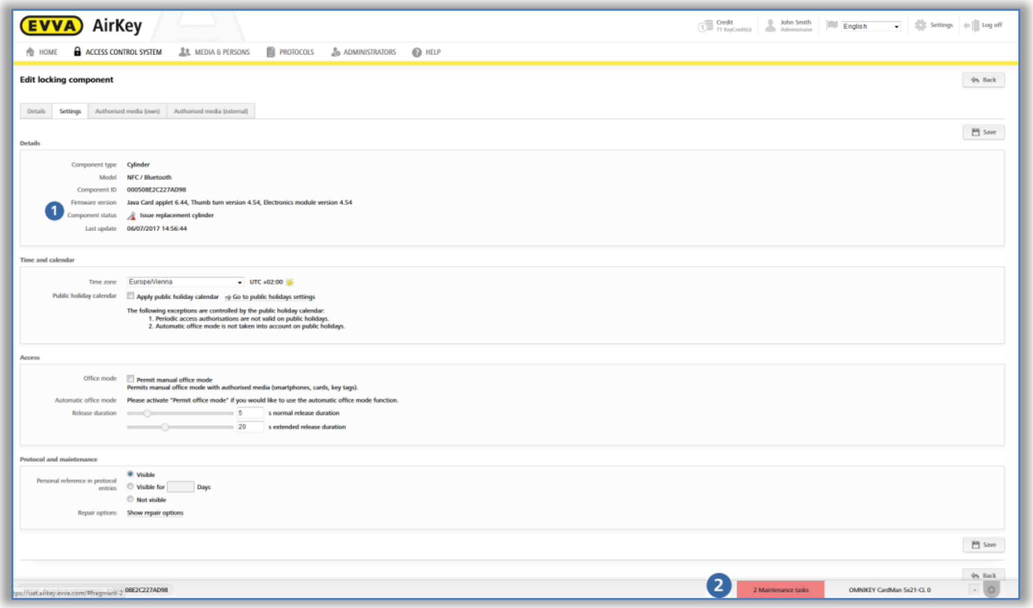
A maintenance task is generated on the basis of the selected repair option, which you can run with a coding station or smartphone in maintenance mode.

New maintenance task: Issue replacement cylinder

Figure 289: Repair options

> Click ***Add maintenance task***.

The locking component status ❶ is updated and shown as a maintenance task ❷.



Edit locking component

Details

Component type: Cylinder
Model: NFC / Bluetooth
Component ID: 000508E2C227AD98
Firmware version: Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status: Issue replacement cylinder
Last update: 06/07/2017 14:56:44

Time and calendar

Time zone: Europe/Vienna UTC +02:00
Public holiday calendar: □ Apply public holiday calendar → Go to public holidays settings
The following exceptions are controlled by the public holiday calendar:
1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

Access

Office mode: □ Permit manual office mode
Permits manual office mode with authorised media (smartphones, cards, key tags).
Automatic office mode: Please activate "Permit office mode" if you would like to use the automatic office mode function.
Release duration: 5 s normal release duration
20 s extended release duration

Protocol and maintenance

Personal reference in protocol entries: ● Visible ○ Visible for Days ○ Not visible
Repair options: Show repair options

2 Maintenance tasks

OMNIKEY CardMan 5x21-CL 0

Figure 290: Component status and maintenance task

As a result, you have completed the preparations to issue and install a replacement locking component within the AirKey Online Administration. Issue and install the replacement locking component using a smartphone with maintenance authorisation or the optionally available coding station to complete the entire process.

The component you would like to replace remains available for updates until the replacement locking component has been completely installed. This guarantees the event logs are complete for the case that there are access events between installing the replacement component and successfully completing replacement component installation.

When replacing locking components by Bluetooth the replaced component and the replacement locking component are shown on the list of Bluetooth components in range. De-energise the replaced component after having replaced it. Only then will it no longer appear on the Bluetooth components list.

Adding and installing replacement locking components using a smartphone

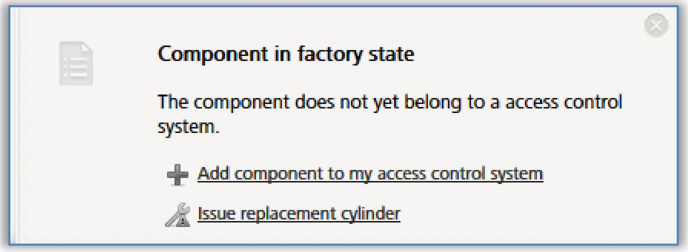
You require a smartphone with maintenance authorisation for the access control system in which you would like to issue and install the replacement locking component.

- Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** icon and hold the smartphone to the locking component in factory state.
- Establishing a connection using **Bluetooth** (for **Android** smartphones): open the context menu of the locking component in factory state which you would like to add to the access control system (⋮) and then select ***Connect***.
- Establishing a connection using **Bluetooth** (for **iPhones**): Swipe the "In factory state" designation of the locking component in factory state which you would like to add to your access control system towards the left and then select ***Connect***.
- After having updated, click ***Issue replacement cylinder*** in the locking component details.
- In the following dialogue, select the locking component you would like to replace and click ***Continue.***
- If you are using NFC, once again hold the smartphone to the locking component in factory state. If you are using Bluetooth, select the locking component in factory state from the list of locking components in range.
- Specify whether you would like to add a maintenance tasks for later installation.
- Click ***Install later*** to cancel the process, providing you must still install the locking component at the door or select ***Complete*** if the component has already been installed at the door.
- Update the locking component after having installed it in the door.

Option Issuing and installing replacement locking components with the coding station.

- Position a replacement locking component in factory state on the coding station.
- Select ***Issue replacement cylinder*** in the bottom right of the

dialogue window and click the locking component you would like to replace.



Component in factory state

The component does not yet belong to a access control system.

Add component to my access control system
Issue replacement cylinder

Figure 291: Component in factory state – issuing replacement cylinders

- Click ***Continue***.
- Position the replacement locking component in factory state on the coding station.
- Only remove the replacement locking component once the corresponding confirmation prompt appears.
- Specify whether you would like to add a maintenance tasks for later installation.
- Click ***Install later*** to cancel the process, providing you must still install the locking component at the door or select ***Complete*** if the component has already been fitted to the door.
- Update the locking component after having installed it in the door.

This process also involves a firmware update if the replacement locking component still features an old firmware version.

You are no longer able to use the replaced locking component following this process. For this reason, exclusively use this function if the locking component is actually faulty and you no longer require it.

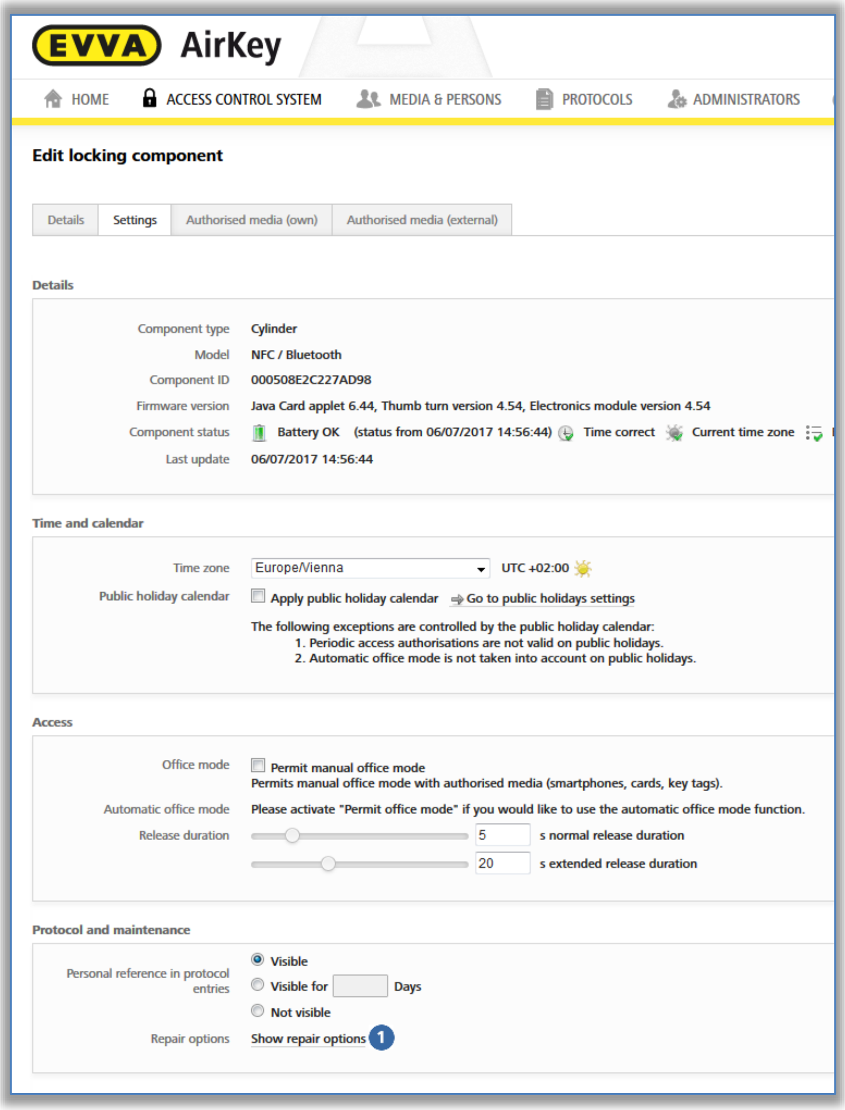
8.8.2 Removing locking components without replacements and highlighting them as "faulty"

If it is not necessary to replace a faulty locking component, but it must no longer appear in the access control system, you can remove it without replacements in the repair options.

It will subsequently no longer be able to update the locking component and it is hence rendered useless.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.
- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the locking component you would like to edit in the overview.

- In the ***Settings*** tab go to the ***Logging and repair options*** section and click on ***Show repair options*** ❶.



EVVA AirKey

Edit locking component

Details

Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status	Battery OK (status from 06/07/2017 14:56:44) Time correct Current time zone
Last update	06/07/2017 14:56:44

Time and calendar

Time zone: Europe/Vienna UTC +02:00

Public holiday calendar: □ Apply public holiday calendar → Go to public holidays settings

The following exceptions are controlled by the public holiday calendar:
1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

Access

Office mode: □ Permit manual office mode
Permits manual office mode with authorised media (smartphones, cards, key tags).

Automatic office mode: Please activate "Permit office mode" if you would like to use the automatic office mode function.

Release duration: 5 s normal release duration
20 s extended release duration

Protocol and maintenance

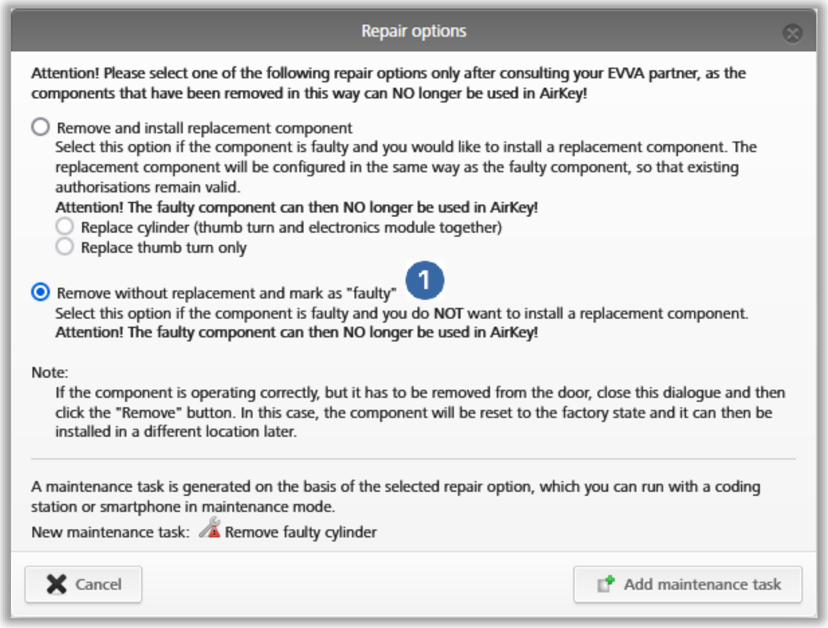
Personal reference in protocol entries: ● Visible ○ Visible for Days ○ Not visible

Repair options: Show repair options 1

Figure 292: Editing locking components – repair options

The "Repair options" dialogue window opens.

- Select ***Disassemble without replacement and mark as "faulty"*** ❶.



Attention! Please select one of the following repair options only after consulting your EVVA partner, as the components that have been removed in this way can NO longer be used in AirKey!

○ Remove and install replacement component
Select this option if the component is faulty and you would like to install a replacement component. The replacement component will be configured in the same way as the faulty component, so that existing authorisations remain valid.
Attention! The faulty component can then NO longer be used in AirKey!
○ Replace cylinder (thumb turn and electronics module together)
○ Replace thumb turn only

● Remove without replacement and mark as "faulty"
Select this option if the component is faulty and you do NOT want to install a replacement component.
Attention! The faulty component can then NO longer be used in AirKey!

Note:
If the component is operating correctly, but it has to be removed from the door, close this dialogue and then click the "Remove" button. In this case, the component will be reset to the factory state and it can then be installed in a different location later.

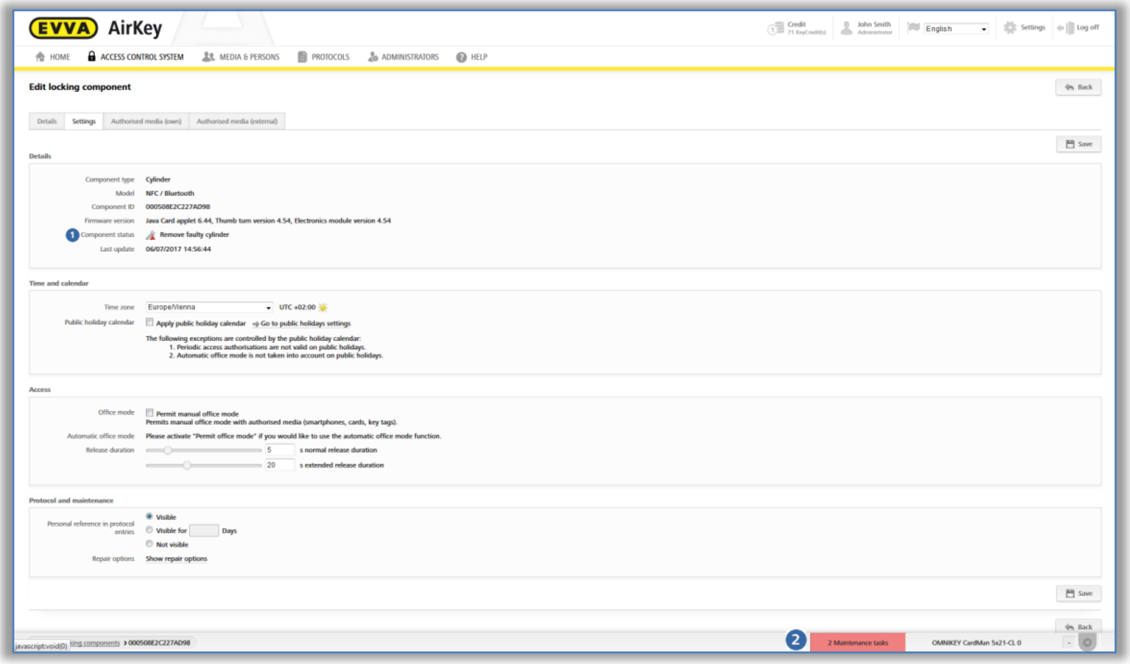
A maintenance task is generated on the basis of the selected repair option, which you can run with a coding station or smartphone in maintenance mode.

New maintenance task: Remove faulty cylinder

Figure 293: Repair options

> Click ***Add maintenance task***.

The locking component status ❶ is updated and shown as a maintenance task ❷.



Edit locking component

Details

Component type: Cylinder
Model: NFC / Bluetooth
Component ID: 000508E2C227AD98
Firmware version: Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status: Remove faulty cylinder
Last update: 06/07/2017 14:56:44

Time and calendar

Time zone: Europe/Vienna UTC +02:00
Public holiday calendar: □ Apply public holiday calendar ⇒ Go to public holidays settings
The following exceptions are controlled by the public holiday calendar:
1. Periodic access authorisations are not valid on public holidays.
2. Automatic office mode is not taken into account on public holidays.

Access

Office mode: □ Permit manual office mode
Permits manual office mode with authorised media (smartphones, cards, key tags).
Automatic office mode: Please activate "Permit office mode" if you would like to use the automatic office mode function.
Release duration: 5 s normal release duration
20 s extended release duration

Protocol and maintenance

Personal reference in protocol entries: ● Visible
○ Visible for Days
○ Not visible
Repair options: Show repair options

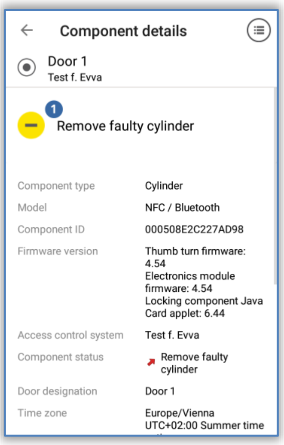
Figure 294: Component status and maintenance task

As a result, any preparations for removing faulty locking components without replacements have been completed within the AirKey Online Administration. Complete the overall process of removing the component using your smartphone with maintenance authorisation or within the AirKey Online Administration.

8.8.3 Removing faulty locking components using smartphones

If it is no longer possible to update faulty locking components, you can use your smartphone to remove the faulty locking component without replacements. This requires a registered smartphone with active maintenance authorisation for this access control system.

- Establishing a connection using **NFC** (for Android smartphones): Tap the ***Connect to component*** icon and hold the smartphone to the locking component you would like to remove.
- Establishing a connection using **Bluetooth** (for **Android** smartphones): Tap the context menu of the the locking component you would like to remove (⋮) and then select ***Connect.***
- Establishing a connection using **Bluetooth** (for **iPhones**): Swipe the designation of the locking component you would like to remove towards the left and then select ***Connect***.
- Component details are shown. Select ***Remove faulty cylinder*** ❶.



Component details

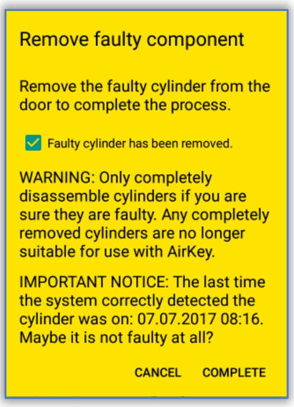
Door 1
Test f. Evva

❶ Remove faulty cylinder

Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Access control system	Test f. Evva
Component status	Remove faulty cylinder
Door designation	Door 1
Time zone	Europe/Vienna UTC+02:00 Summer time

Figure 295: Smartphones – removing faulty components

- Tick the checkbox in the dialogue and click ***Complete*** to confirm.



Remove faulty component

Remove the faulty cylinder from the door to complete the process.

☑ Faulty cylinder has been removed.

WARNING: Only completely disassemble cylinders if you are sure they are faulty. Any completely removed cylinders are no longer suitable for use with AirKey.

IMPORTANT NOTICE: The last time the system correctly detected the cylinder was on: 07.07.2017 08:16. Maybe it is not faulty at all?

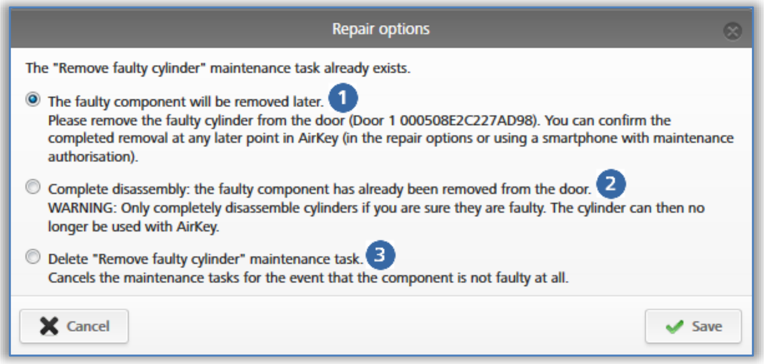
Figure 296: Smartphones – removing faulty components – confirmation

As a result, the process is complete and the locking component is no longer listed within the access control system. The locking component can consequently no longer be used.

8.8.4 Removing faulty locking components using the AirKey Online Administration

If it is no longer possible to update the locking component because of a fault, you must complete removal without replacements in the AirKey Online Administration.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile – depending on the component highlighted as faulty.
- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the locking component you would like to edit in the overview.
- In the ***Settings*** tab go to the ***Logging and repair options*** section and click on ***Show repair options***.
- A dialogue with three options appears.



Repair options

The "Remove faulty cylinder" maintenance task already exists.

● The faulty component will be removed later. 1
Please remove the faulty cylinder from the door (Door 1 000508E2C227AD98). You can confirm the completed removal at any later point in AirKey (in the repair options or using a smartphone with maintenance authorisation).

○ Complete disassembly: the faulty component has already been removed from the door. 2
WARNING: Only completely disassemble cylinders if you are sure they are faulty. The cylinder can then no longer be used with AirKey.

○ Delete "Remove faulty cylinder" maintenance task. 3
Cancels the maintenance tasks for the event that the component is not faulty at all.

Figure 297: Removing faulty locking components

- Select ***The faulty component will be removed later*** ❶ to maintain the current component status and the locking component remains a part of the access control system.
- Click the ***Complete disassembly: The faulty component has already been removed from the door*** ❷ option to complete the process to remove faulty locking components without replacement and the locking component is deleted from the access control system.
- Use the ***Delete "Remove faulty cylinder" maintenance task*** ❸ to revoke removal without replacement. Refer to Revoking maintenance tasks for repair options for more information.

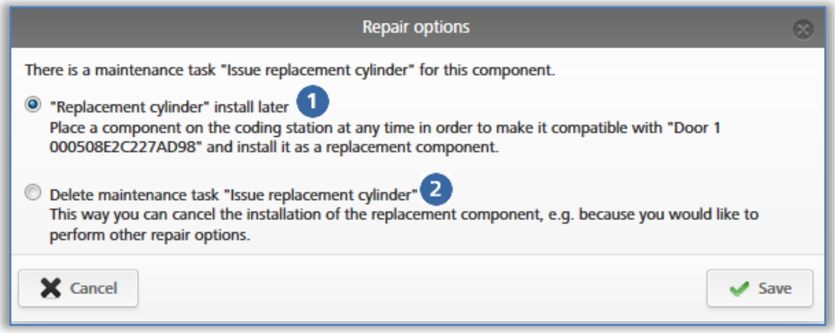
⚠ You are no longer able to use the replaced locking components that have been removed without replacements following this process. For this reason, exclusively use this function if the locking component is actually faulty and you no longer require it.

If you would like to remove an operational locking component from your access control system, proceed as described in Removing locking components.

8.8.5 Revoking maintenance tasks for repair options

If you accidentally created maintenance tasks for replacement locking components or removals without replacements, such maintenance tasks can be deleted retrospectively.

- On the ***Home*** screen select the ***Maintenance tasks*** link.
- Select the desired maintenance task from the list.
- In the ***Settings*** tab go to the ***Logging and repair options*** section and click on ***Show repair options***.
- Depending on the maintenance task that is due, select whether you would like to issue the replacement component (cylinder, thumb turn, wall reader) later ❶ or whether you would like to delete the maintenance task ❷.



Repair options

There is a maintenance task "Issue replacement cylinder" for this component.

● "Replacement cylinder" install later 1
Place a component on the coding station at any time in order to make it compatible with "Door 1 000508E2C227AD98" and install it as a replacement component.

○ Delete maintenance task "Issue replacement cylinder" 2
This way you can cancel the installation of the replacement component, e.g. because you would like to perform other repair options.

Figure 298: Deleting maintenance tasks

- Click ***Save***.

This will remove the maintenance task. The component status of the locking component is updated as per the last locking component status.

Any completed maintenance tasks for repair options cannot be removed.

Also use this function to remove the "Component must be removed" maintenance task if the locking component was removed from the AirKey system without having been faulty.

9 Emergency media

Emergency media are media without expiry dates and permanent authorisations to all locking components within an access control system. Emergency media are used in emergencies (e.g. by the fire service) and must be kept safe. Emergency media can unlock locking components regardless of the time. Merely the power supply of the locking component must be on.

9.1 Issuing emergency media

Create an emergency medium (e.g. card, key fob, combi key or wristband) as described in the Creating cards, key fobs, combi keys, and wristbands section and assign permanent access authorisations to all access control system doors in order to issue emergency media. Ensure that emergency media are updated in the event of system extensions to also guarantee access to additional doors in emergencies. Emergency media also grant access to locking components with an incorrect time settings (e.g. cylinder time reset if batteries are empty). Please refer to Assigning authorisations and Creating authorisations for more information on assigning and creating authorisations.

⚠ Please note that media, such as cards, key fobs, combi keys or wristbands may also become faulty. For this reason, create a corresponding number of emergency media, appropriate for the access control system.

❗ We recommend exclusively using cards, key fobs, combi keys or wristbands as emergency media as smartphones are not suitable for this purpose due to their short battery life.

We recommend you work with areas which contain all doors associated with the access control system to facilitate emergency media management. Then assign a permanently valid authorisation for this area to emergency media.

10 Media replacement

10.1 Smartphone replacement

The smartphone replacement simplifies the change from one smartphone to another, for example, when purchasing a new device.

With smartphone replacement, all AirKey authorisations and settings (except the PIN code and the local Hands-free settings) of the existing smartphone are transferred to the new smartphone.

The replacement can be executed both from Android to iOS and vice versa.

The replacement can be started either by an administrator or directly from the smartphone.

Here in the documentation, the "old" smartphone is called the **source medium** and the "new" smartphone is called the **target medium**.

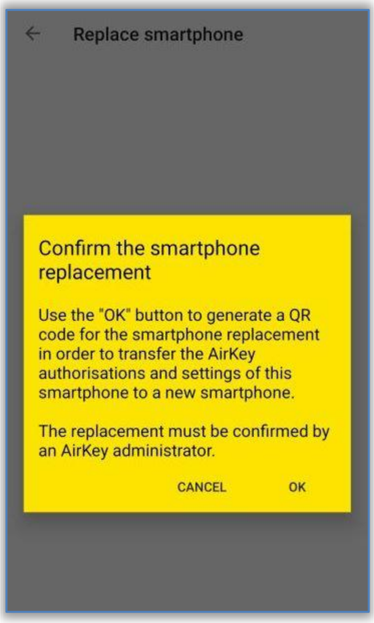
❗ The source medium is automatically deactivated after the replacement has been completed. If the source medium is no longer functional or available, the blacklist of the affected locking components must be updated. Only then the security of the system is re-established.

❗ If authorisations are also transferred to the target medium, a KeyCredit is also deducted from the existing credit. If no KeyCredits are available, the replacement can only be completed once there is a credit available again.

10.1.1 Starting replacement from smartphone

If the source medium is still working, registered and not deactivated, the smartphone replacement can be started directly from the source medium.

- Start the AirKey app.
- Tap on ***Settings* → *Replace smartphone***.
- Confirm with ***OK***.



Replace smartphone

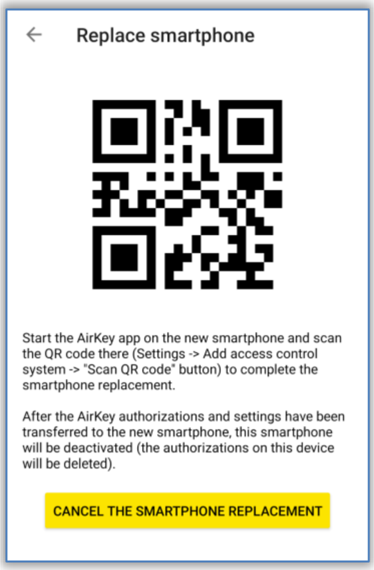
Confirm the smartphone replacement

Use the "OK" button to generate a QR code for the smartphone replacement in order to transfer the AirKey authorisations and settings of this smartphone to a new smartphone.

The replacement must be confirmed by an AirKey administrator.

Figure 299: Confirming the smartphone replacement

> A QR code with a description is shown on the source medium.



Replace smartphone

Start the AirKey app on the new smartphone and scan the QR code there (Settings -> Add access control system -> "Scan QR code" button) to complete the smartphone replacement.

After the AirKey authorizations and settings have been transferred to the new smartphone, this smartphone will be deactivated (the authorizations on this device will be deleted).

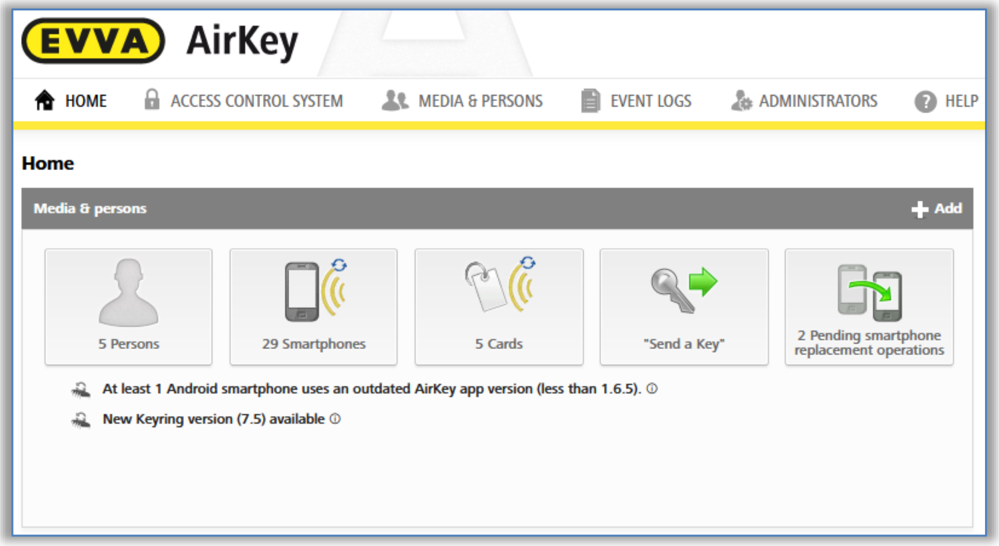
Figure 300: QR code for the smartphone replacement

The steps on the source medium are now complete. The source medium can be used as usual until the replacement is completed. The QR code is valid for 30 days and is displayed again within this period when you tap ***Settings*** → ***Replace smartphone***.

Because a new smartphone is created during the smartphone replacement and KeyCredits are also deducted, the replacement must be confirmed by an administrator within the AirKey Online Administration.

> Login to the AirKey Online Administration.

> On the ***Home*** page click on the tile ***Pending smartphone replacement operations***.



Home

Media & persons

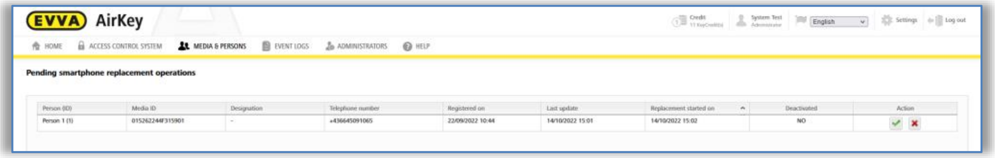
5 Persons | 29 Smartphones | 5 Cards | "Send a Key" | 2 Pending smartphone replacement operations

At least 1 Android smartphone uses an outdated AirKey app version (less than 1.6.5).

New Keyring version (7.5) available

Figure 301: Home score – pending smartphone replacement operations

- By clicking the green check mark in the "Action" column you can confirm the replacement. The red cross symbol will reject the smartphone replacement.

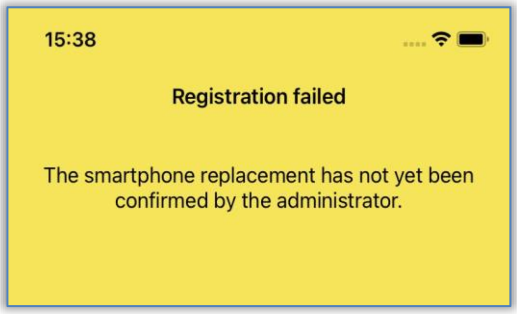


Pending smartphone replacement operations

Person (ID)	Media ID	Designation	Telephone number	Registered on	Last update	Replacement started on	Deactivated	Action
Person 1 (1)	015262244F315901	-	+436645091065	22/09/2022 10:44	14/10/2022 15:01	14/10/2022 15:02	NO	✓ ✗

Figure 302: Pending smartphone replacement operations table

After the administrator’s approval, the replacement can be completed by scanning the QR code on the target medium. If the replacement is rejected by the administrator, the smartphone replacement is cancelled and the QR code is no longer valid and is removed. If the QR code is scanned at the target medium before an administrator has confirmed the replacement, a corresponding error message appears.



Registration failed

The smartphone replacement has not yet been confirmed by the administrator.

Figure 303: Smartphone replacement failed

Administrators can also activate an automatic confirmation of people´s requests for smartphone replacements in the settings of the AirKey Online Administration (see chapter General). This means that every smartphone replacement that is started from a smartphone is automatically confirmed immediately. Keep in mind that a KeyCredit will be deducted for every smartphone replacement where authorisations are transferred.

To scan the QR code with a target media that is not yet registered, follow the steps below:

- Start the AirKey app.
- ***Confirm*** the licensing conditions.
- Tap on ***Scan QR code*** and scan the QR code from the source medium.

To scan the QR code with a target media that is already registered, follow the steps below:

- Start the AirKey app.
- Tap ***Settings*** → ***Add access control system***.
- Tap on ***Scan QR code*** and scan the QR code from the source medium.

The smartphone replacement is now complete and the target medium is successfully registered with the permissions and settings of the source medium. The source medium will be deactivated automatically after the successful replacement.

! If the source medium is registered in more than one access control system, the replacement is started in all access control systems at the same time. This means that several administrators may have to confirm the replacement within the AirKey Online Administration. Only those AirKey authorisations and settings will be transferred to the target medium in which the administrators have confirmed the replacement.

10.1.2 Starting replacement as administrator

If the source medium is no longer available or no longer functional, the replacement can also be started as an administrator.

- Click on the tile ***Smartphone*** on the ***Home*** screen.
- Alternatively select ***Media & Persons*** → ***Media***.
- Select the smartphone you want to replace.
- Click on ***More...*** → ***Replace smartphone*** ❶.

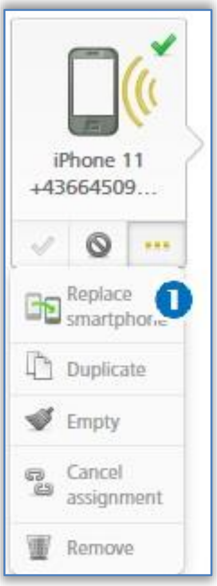
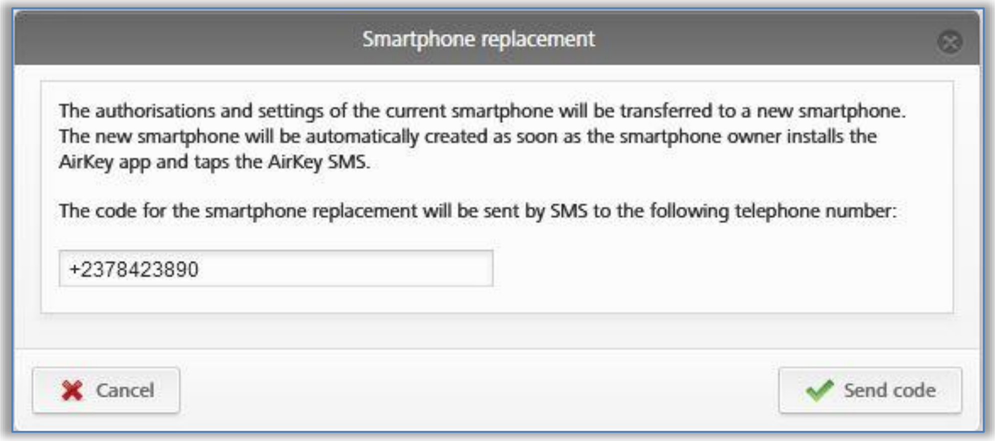


Figure 304: Replacing smartphone

- A dialog appears in which the telephone number of the target medium must be inserted. The telephone number of the source medium will be taken automatically.



Smartphone replacement

The authorisations and settings of the current smartphone will be transferred to a new smartphone. The new smartphone will be automatically created as soon as the smartphone owner installs the AirKey app and taps the AirKey SMS.

The code for the smartphone replacement will be sent by SMS to the following telephone number:

+2378423890

Figure 305: Smartphone replacement

- Check if the telephone number is correct and confirm with ***Send code***.
- A "Send a Key" SMS with a registration link will be sent to the specified telephone number of the target medium.

The smartphone replacement must be finished on the target medium:

- Open the SMS containing the registration link.
- Tap on the registration link and follow the instructions.

The smartphone replacement is now complete and the target medium is successfully registered with the AirKey authorisations and settings of the source medium. The source medium will be deactivated automatically after the successful replacement.

The registration link inside the SMS is valid for 30 days. If the SMS has not been arrived, you can resend the SMS to the target medium:

- Click on ***More...*** → ***Replace smartphone*** ❶.

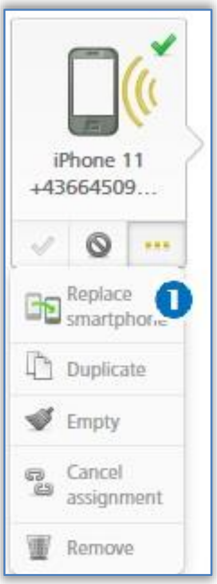
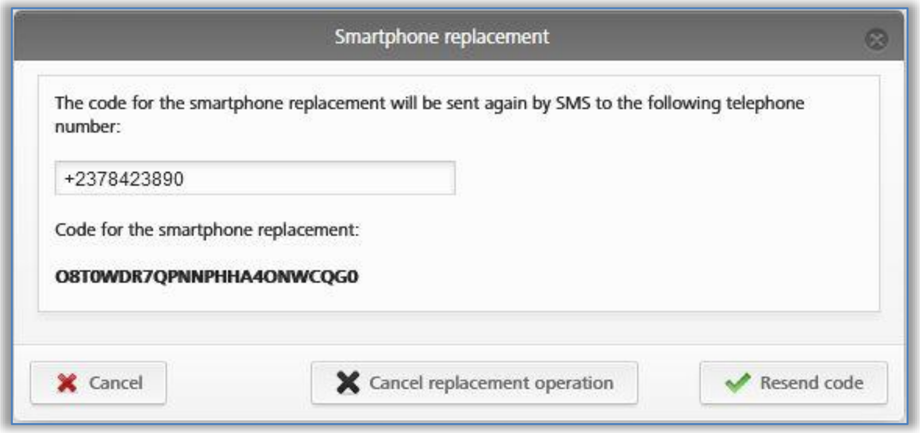


Figure 306: Replacing smartphone

- You can check and correct the telephone number in the dialog.


Smartphone replacement

The code for the smartphone replacement will be sent again by SMS to the following telephone number:

+2378423890

Code for the smartphone replacement:

O8T0WDR7QPNNPHHA4ONWCQG0

Figure 307: Smartphone replacement – resending code

- Click on ***Resend code***.

Within this dialog you have also the possibility to cancel the replacement operation.

If the source medium is registered in more than one access control system, the replacement must be started individually by an administrator for each access control system. Accordingly, an SMS with a registration link is sent for each access control system.

11 Working with several access control systems

The following section describes how to work with several access control systems.

11.1 Sharing locking components with other access control systems

You can share a locking component added to your access control system with another access control system. Authorisations for these shared locking components can then be assigned in another access control system. You can share each locking component with a maximum of 250 access control systems.

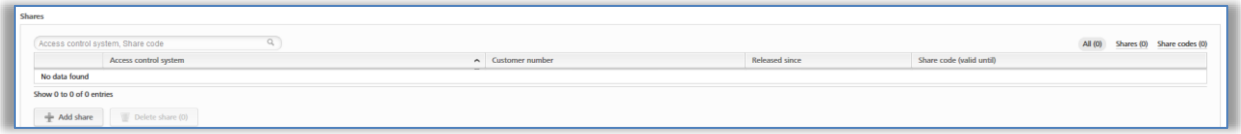
> On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.

> Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.

> Click the door designation of the locking component you would like to share in the overview.

The ***Shares*** section of the locking component details lists any shares that have already been granted.

> Click ***Add share***.



Shares

Access control system, Share code

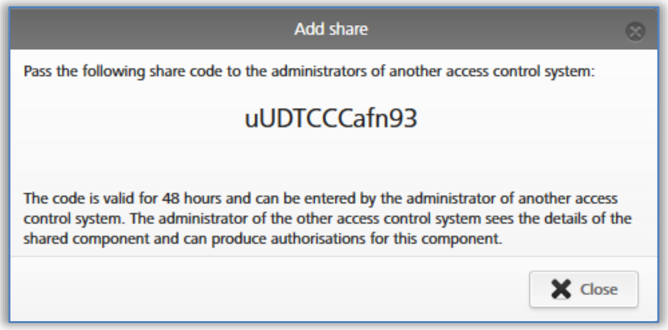
All (0) Shares (0) Share codes (0)

	Access control system	Customer number	Released since	Share code (valid until)
No data found				

Show 0 to 0 of 0 entries

Figure 308: Sharing locking components

> The system generates a 12-character approval code.



Add share

Pass the following share code to the administrators of another access control system:

uUDTCCCafn93

The code is valid for 48 hours and can be entered by the administrator of another access control system. The administrator of the other access control system sees the details of the shared component and can produce authorisations for this component.

Figure 309: Adding shares

> Notify the administrator of the other access control system of this sharing code.

The sharing code remains valid for 48 hours.

You can generate multiple sharing codes for a locking component. They are shown in the share list of the locking component.

The system creates an entry in the share list of the locking component. It shows the sharing code and its validity.

11.2 Adding locking components from other access control systems

If a locking component from another access control system has been activated for you, you must initially add it to your access control system.

> On the ***Home*** screen, select ***Add*** on the grey Access control system bar ⟶ Add locking component ❶.

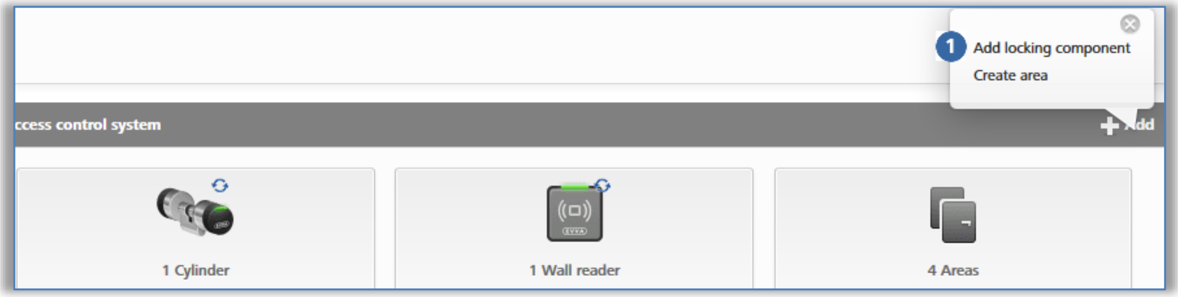
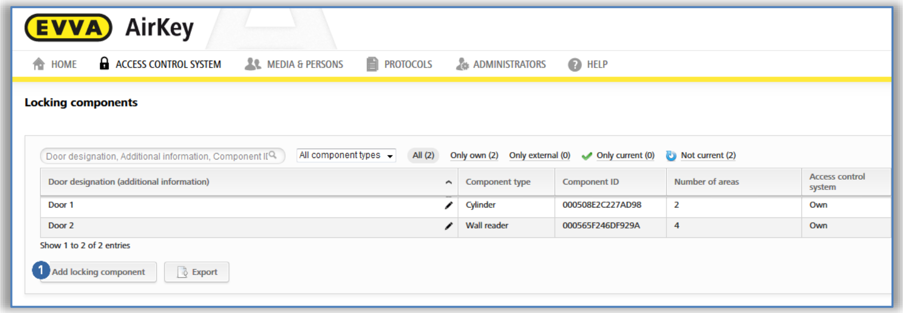


Figure 310: Adding locking components – grey bar

> Alternatively, select ***Access control system*** ⟶ ***Locking components*** in the main menu.

> Click ***Add locking component.*** ❶



Locking components

Door designation, Additional information, Component II

Door designation (additional information)	Component type	Component ID	Number of areas	Access control system
Door 1	Cylinder	000508E2C227AD98	2	Own
Door 2	Wall reader	000565F246DF929A	4	Own

Show 1 to 2 of 2 entries

Figure 311: Adding locking components

> Select the ***Shared locking components*** ❶ type.

> Click Continue.

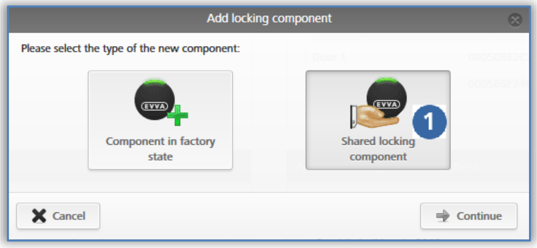
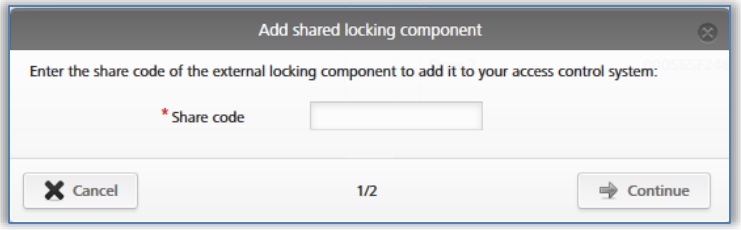

Add locking component
Please select the type of the new component:
Component in factory state
Shared locking component
1
Cancel
Continue

Figure 312: Adding shared locking components

- Enter the sharing code from the other access control system to add the locking component.



Enter the share code of the external locking component to add it to your access control system:

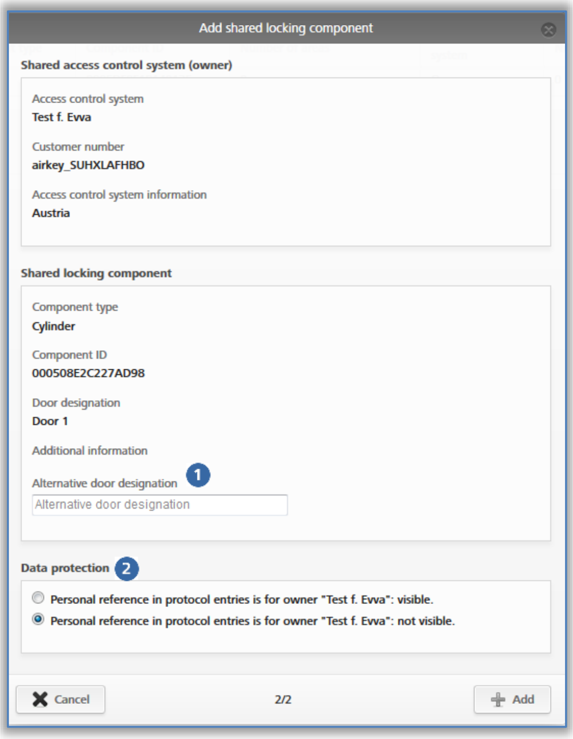
* Share code

Figure 313: Adding shared locking components

An error message appears if the sharing code is incorrect.

Once you have entered a correct sharing code, you can change the following settings:

- Alternative door designation ❶
- In Data protection the personal data in event log entries may be visible to the owner of the locking component or they may have been rendered anonymous ❷.



Shared access control system (owner)

Access control system
Test f. Evva

Customer number
airkey_SUHXLAFHBO

Access control system information
Austria

Shared locking component

Component type
Cylinder

Component ID
000508E2C227AD98

Door designation
Door 1

Additional information

Alternative door designation
Alternative door designation

Data protection

○ Personal reference in protocol entries is for owner "Test f. Evva": visible.
● Personal reference in protocol entries is for owner "Test f. Evva": not visible.

Figure 314: Adding shared locking components

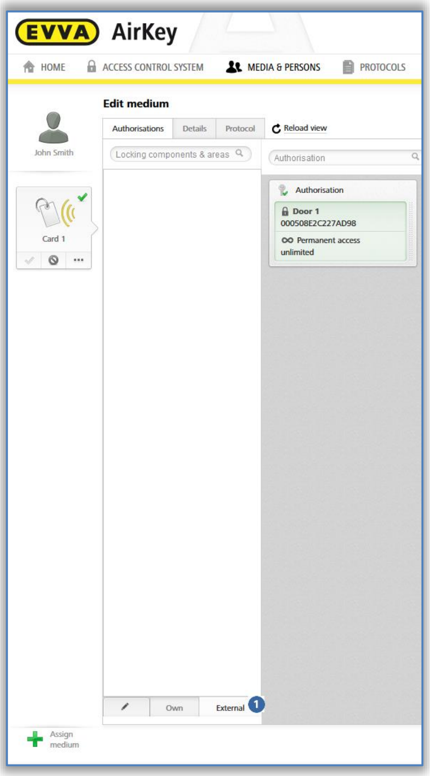
- The system creates a maintenance task.
- Update the locking component using a smartphone with maintenance authorisation or an optionally available coding station.
- This deletes the maintenance task from the list and the share is up to date.
- As soon as you have added the shared locking component, the locking component is listed in the "Access control system" column of the locking component list with the "external" attribute. Each client who has added the locking component can edit the alternative door designation in the "Details" tab and assign the locking component to an area. Open the "Settings" tab and change the radio button in the "Data protection" section to either make personal data in event log entries available to locking component owners or render the data anonymous. You can also configure personal data in event log entries in the "Logging and repair options" section for the enabled access control system. You can also assign access authorisations for shared locking components.

⚠ External locking components cannot be shared with other access control systems.

11.3 Assigning authorisations for shared locking components

Within each access control system to which the authorised locking component was added, the process to assign authorisations differs marginally to that for owners of the locking components. Proceed as follows if you have added a shared locking component to your access control system.

- On the ***Home*** screen, select the ***Smartphones*** or ***Cards*** tile.
- Alternatively select ***Media & persons*** → ***Media*** in the main menu.
- Select the desired medium from the overview list.
- If the medium has been assigned to a person, an overview of authorisations for this medium appears.
- Select the ***External*** ❶ tile below the tiles for all locking components and areas to display a list of all locking components added from external access control systems.



Edit medium

Authorisation

Door 1
000508E2C227AD98

Permanent access
unlimited

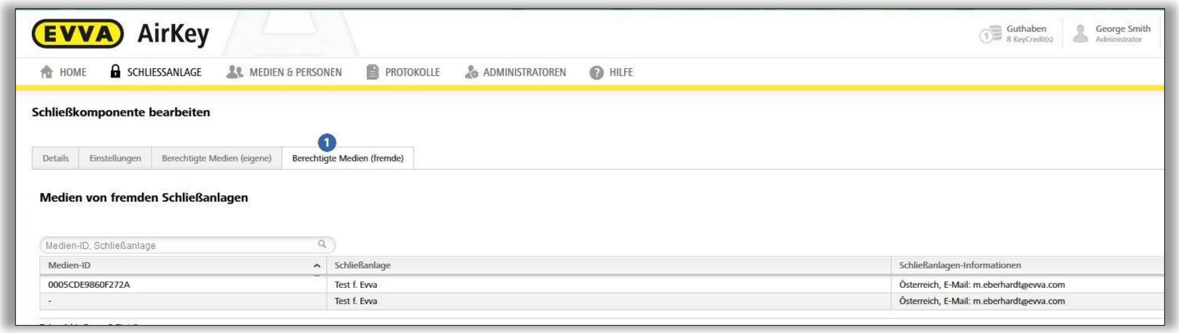
Figure 315: Authorisations for shared locking components

- Drag and drop the button with the selected, shared door to the grey area. The access types are only displayed after having dragged and dropped the selected door / selected area into the centre.
- Drag and drop the selected door / selected area to the corresponding field to select the desired access type.
- Create the authorisation to save it and have one KeyCredit deducted from your account. Please refer to Creating authorisations for more information on creating authorisations. In this process, the KeyCredit is deducted from your access control system's credit, not the credit of the other access control system.

11.4 Viewing authorisations for shared locking components

If you have shared a locking component with another client, you can also see the clients' media authorised for the shared locking component.

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.
- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the locking component for which you would like to view the details in the overview.
- Click ***Authorised media (external)*** ❶ to obtain an overview of all external media with authorisation for this locking component.



Schließkomponente bearbeiten

Medien von fremden Schließanlagen

Medien-ID	Schließanlage	Schließanlagen-Informationen
0005CDE9860F272A	Test f. Evva	Österreich, E-Mail: m.eberhardt@evva.com
-	Test f. Evva	Österreich, E-Mail: m.eberhardt@evva.com

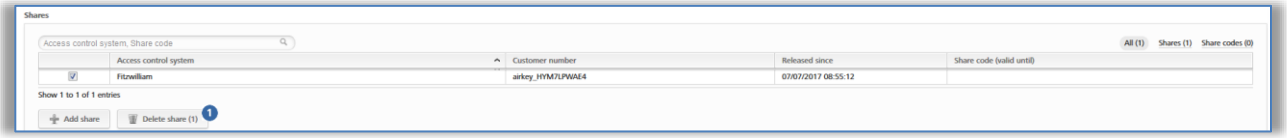
Figure 316: Authorised media (external)

11.5 Revoking shared locking components

You can once again revoke any shared locking components. For this purpose, proceed as follows:

- On the ***Home*** screen, select the ***Cylinders*** or ***Wall readers*** tile.
- Alternatively, select ***Access control system*** → ***Locking components*** in the main menu.
- Click the locking component on the overview list for which you would like to revoke the shared status.

On the ***Details*** tab in the ***Shares*** section, select the corresponding share and click ***Delete share*** ❶.

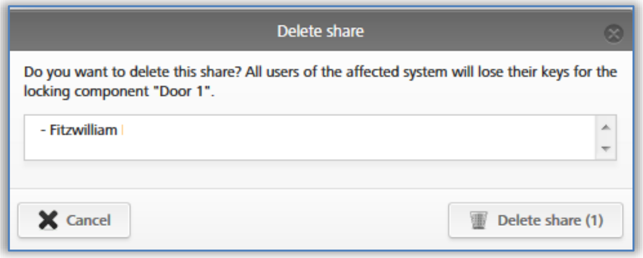


	Access control system	Customer number	Released since	Share code (valid until)
☑	Fitzwilliam	airkey_HYM7LPWAE4	07/07/2017 08:55:12	

Show 1 to 1 of 1 entries

Figure 317: "Shares" section – deleting shares

- Click ***Delete share*** to confirm the security prompt.



Do you want to delete this share? All users of the affected system will lose their keys for the locking component "Door 1".

- Fitzwilliam

Figure 318: Deleting shares

As a result the locking component is removed from the other client's access control system. The system creates a maintenance task.

- Update the locking component for which you have revoked the share using a smartphone with maintenance authorisation or an optionally available coding station. The locking component status is once again up to date after having updated.

Important: Other clients’ media will no longer be able to unlock locking components once you have updated the corresponding locking components.

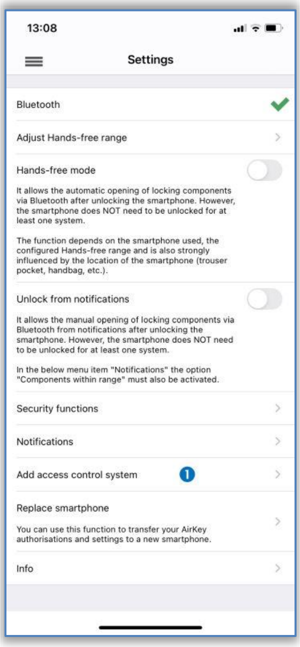
Shared locking components can only be deleted using the access control systems from which the share had originally been enabled.

You must not update the locking component if the sharing code has not been used to date and it has been deleted as described in this section.

11.6 Using smartphones in several systems

You can register your smartphone to several access control systems and use it as a medium.

- Open the main menu of the AirKey app and select ***Settings*** → ***Add access control system*** ❶.



13:08

Settings

Bluetooth ✓

Adjust Hands-free range

Hands-free mode

It allows the automatic opening of locking components via Bluetooth after unlocking the smartphone. However, the smartphone does NOT need to be unlocked for at least one system.

The function depends on the smartphone used, the configured Hands-free range and is also strongly influenced by the location of the smartphone (trouser pocket, handbag, etc.).

Unlock from notifications

It allows the manual opening of locking components via Bluetooth from notifications after unlocking the smartphone. However, the smartphone does NOT need to be unlocked for at least one system.

In the below menu item "Notifications" the option "Components within range" must also be activated.

Security functions

Notifications

Add access control system ❶

Replace smartphone

You can use this function to transfer your AirKey authorisations and settings to a new smartphone.

Info

Figure 319: Adding access control systems

- For Android, the dialogue for entering the registration code is displayed automatically. For iOS, tap on ***Registration code already received*** to skip entering the phone number and proceed to entering the registration code.
- Enter the registration code you received from the access control system administrator and tap ***Register***.
- If you have activated a PIN code for the AirKey app, you must enter and confirm it.

As a result, the smartphone has been registered in another access control system.

If the registration code for another access control system was sent via SMS, it is sufficient to tap on the link of the SMS to automatically start and perform the registration.

Swipe on the smartphone screen to select authorisation overviews of individual access control systems or the overall authorisation overview.

EVVA recommends assigning a PIN code. It serves as an additional level of security. You can subsequently activate or deactivate the PIN code protection. Please refer to the Activating PIN code section for more detailed information.

The Scan QR code button is only required in connection with a smartphone replacement. Details about the smartphone replacement can be found in the chapter Smartphone replacement.

12 AirKey Cloud Interface (API)

The AirKey Cloud Interface is an interface (API) for third-party systems based on REST. The interface allows certain AirKey functions to be controlled via third-party software (e.g. a booking system or check-in).

To do this, the third-party software must be connected to the AirKey Online Administration and specially adapted so that it can send the necessary commands and process the subsequent responses.

The list of possible functions and their corresponding commands can be found in the API description. Your integrator or the programmer of the third-party software takes care of the implementation.

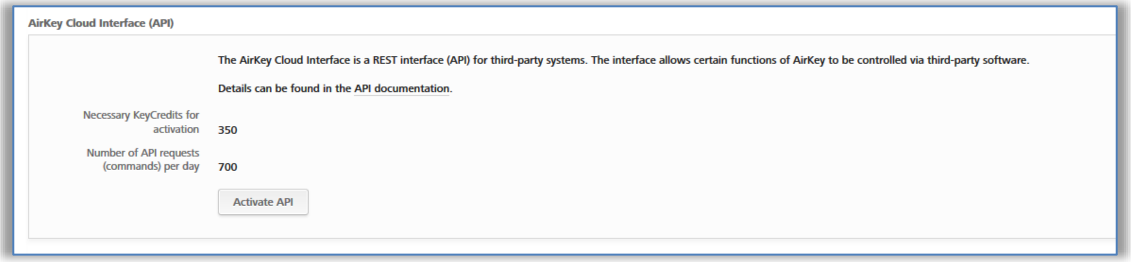
Try out the function of the AirKey Cloud Interface with the EVVA AirKey Cloud Interface Demonstration.

Make sure you have enough credit when using the AirKey Cloud Interface. In this case it is best to use "KeyCredits Unlimited". If the credit has been consumed or is about to be consumed, all administrators of the AirKey access control system will be notified by e-mail. This e-mail notification will only be sent to administrators who have activated the option ***I would like to receive important notifications from EVVA (e.g. about low KeyCredits credit) by e-mail (recommended)***. You can edit this e-mail notification for an administrator at any time (see Editing administrators).

12.1 Activating the AirKey Cloud Interface

At least 350 KeyCredits are required to activate the AirKey Cloud Interface. Use your existing KeyCredits volume credit or use the corresponding scratch card **KeyCredits AirKey Cloud Interface**.

> In the ***Settings*** within Tab ***General*** click on ***Activate API***.



AirKey Cloud Interface (API)

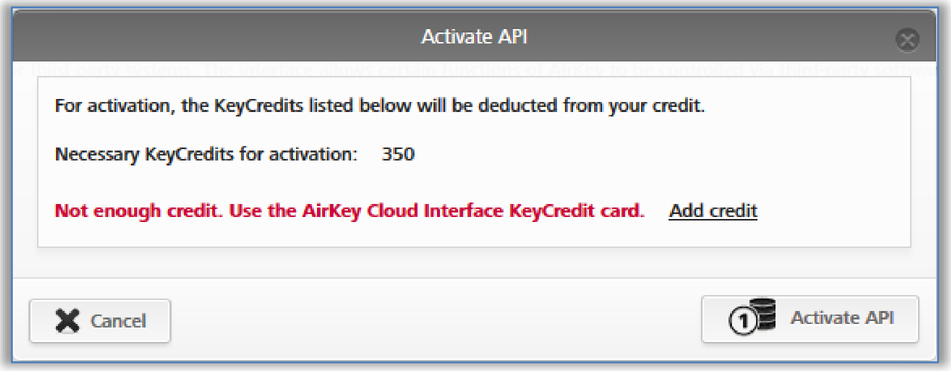
The AirKey Cloud Interface is a REST interface (API) for third-party systems. The interface allows certain functions of AirKey to be controlled via third-party software.

Details can be found in the API documentation.

Necessary KeyCredits for activation	350
Number of API requests (commands) per day	700

Figure 320: General Settings – AirKey Cloud Interface (API)

> If there is enough credit volume, confirm the dialogue again with ***Activate API***. If the credit is not enough, this is indicated with a message. It is then possible to recharge the credit directly via a link.


Activate API

For activation, the KeyCredits listed below will be deducted from your credit.

Necessary KeyCredits for activation: 350

Not enough credit. Use the AirKey Cloud Interface KeyCredit card. Add credit

Figure 321: API activation

Now the AirKey Cloud Interface is activated. The AirKey Cloud Interface must only be activated once per access control system in order to be able to use it.

After activation, you will receive information about the endpoint (API commands must be sent there) and the API request limit (number of possible API requests per day). An API request is a command that is sent to the AirKey system via the third-party software.

The API request limit is reset daily at 00:00 UTC. If the API request limit is exceeded, all administrators of the AirKey access control system will be notified by e-mail. This e-mail notification will only be sent to administrators who have activated the option ***I would like to receive important notifications from EVVA (e.g. about low KeyCredits credit) by e-mail (recommended)***. You can edit this e-mail notification for an administrator at any time (see Editing administrators).

If the API requests per day are not sufficient for your particular use case, please contact EVVA support.

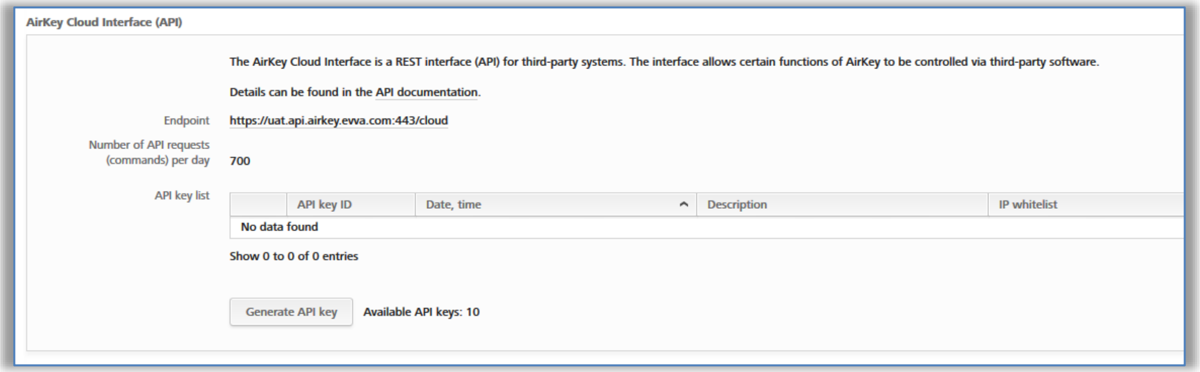
12.2 Generate API key

The communication between AirKey and the third-party software is secured with an API key. Only those who know this API key can send commands to your access control system via the AirKey Cloud Interface. Every access control system with an activated AirKey Cloud Interface uses its own API keys.

Actions executed via the AirKey Cloud Interface are also logged in the system event log of the AirKey access control system. In this case, the first part of the API key, the API key ID, is used as the administrator.

After activation, you can generate the API keys required for communication.

- Click ***Generate API key*** in the ***Settings*** in the ***General*** tab.



AirKey Cloud Interface (API)

The AirKey Cloud Interface is a REST interface (API) for third-party systems. The interface allows certain functions of AirKey to be controlled via third-party software.

Details can be found in the API documentation.

Endpoint https://uat.api.airkey.evva.com:443/cloud

Number of API requests (commands) per day 700

API key list

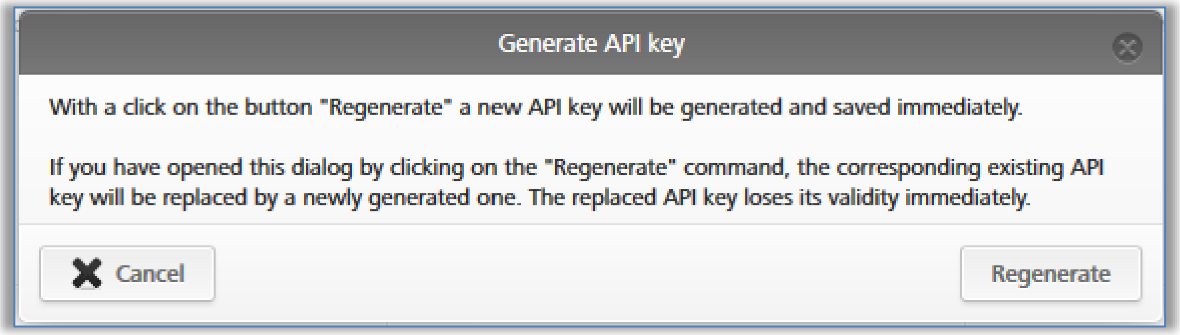
	API key ID	Date, time	Description	IP whitelist
No data found				

Show 0 to 0 of 0 entries

Available API keys: 10

Figure 322: Generate API key

> Confirm the dialogue again with ***Generate API key***.



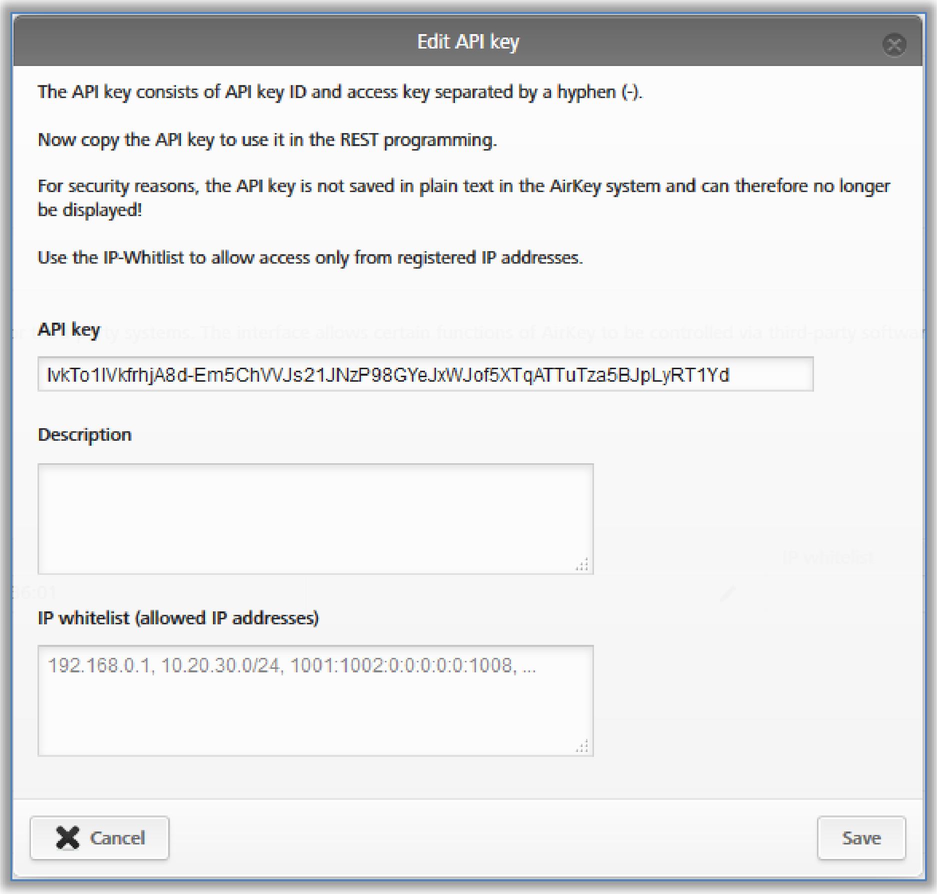
Generate API key

With a click on the button "Regenerate" a new API key will be generated and saved immediately.

If you have opened this dialog by clicking on the "Regenerate" command, the corresponding existing API key will be replaced by a newly generated one. The replaced API key loses its validity immediately.

Figure 323: Generate API key dialogue

> Enter a description, for example the name of the third-party software and optionally limit the IP addresses authorised to send API requests via the IP whitelist.



Edit API key

The API key consists of API key ID and access key separated by a hyphen (-).

Now copy the API key to use it in the REST programming.

For security reasons, the API key is not saved in plain text in the AirKey system and can therefore no longer be displayed!

Use the IP-Whitlist to allow access only from registered IP addresses.

API key

IvkTo1IVkfrhjA8d-Em5ChVVJs21JNzP98GYeJxWJof5XTqATTuTza5BJpLyRT1Yd

Description

IP whitelist (allowed IP addresses)

192.168.0.1, 10.20.30.0/24, 1001:1002:0:0:0:0:0:1008, ...

Figure 324: Generate API key details

Use the function of the IP whitelist to increase security. Enter only those IP addresses for the respective API key which are allowed to send API requests to your AirKey access control system.

Both IPv4 and IPv6 IP addresses are allowed in the IP whitelist. Use the comma (,) as a separator between several IP addresses.

For security reasons, the API key is only displayed completely once. Store it in a safe place respectively use it in your third-party software.

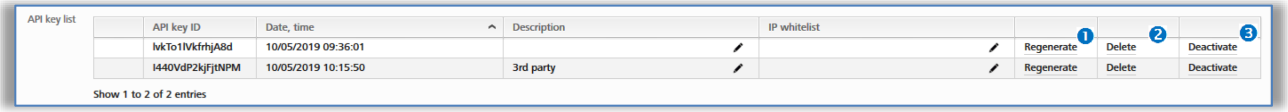
> Save the entries for the API key by clicking on ***Save***.

Up to 10 API keys can be generated per AirKey access control system. Thus, more than one third-party software can control the AirKey access control system.

The generated API key is listed in the general settings and can also be edited there later.

12.3 Edit API key

The description and IP whitelist of existing API keys can be edited later in the ***Settings*** in the ***General*** tab using the pencil icon. In addition, the functions ***Regenerate***, ***Delete*** and ***Deactivate*** or ***Reactivate*** are available for the individual API keys.



	API key ID	Date, time	Description	IP whitelist			
	lvkTo1lVkfrhjA8d	10/05/2019 09:36:01			Regenerate	Delete	Deactivate
	I440VdP2kjFjtNPM	10/05/2019 10:15:50	3rd party		Regenerate	Delete	Deactivate

Show 1 to 2 of 2 entries

Figure 325: Edit API key

12.3.1 Regenerate API key

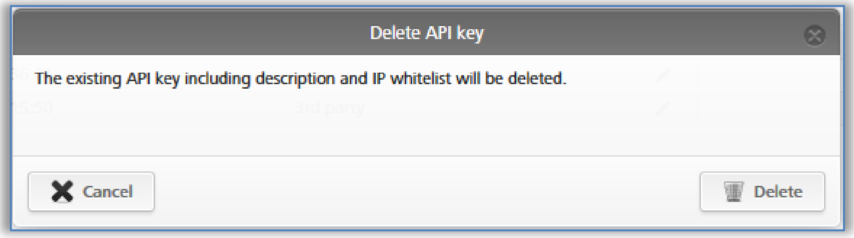
This replaces an existing API key with a new API key. The replaced API key is no longer valid.

- Click in the ***Settings*** in the tab ***General***, in the list of API keys, on ***Regenerate*** ❶.
- All further steps are identical to Generate API key.

12.3.2 Delete API key

This deletes an existing API key. This key will be removed from the list of API keys and is therefore no longer valid. Deleting API keys increases the number of available API keys accordingly.

- Click in the ***Settings*** in the tab ***General***, in the list of API keys, on ***Delete*** ❷.
- Confirm the dialogue with ***Delete*** to finally delete the API-Key.



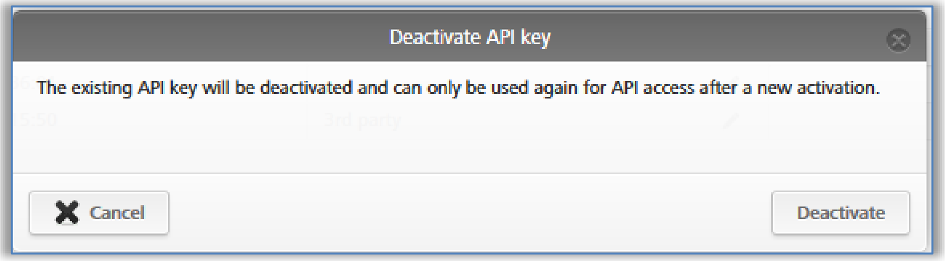
The existing API key including description and IP whitelist will be deleted.

Figure 326: Delete API key

12.3.3 Deactivate and activate API key

This deactivates an existing active API key or activates a deactivated API key. A deactivated API key is invalid and no API requests can be sent to the AirKey access control system. The API key, its description, and IP whitelist do not change because of the deactivation and activation.

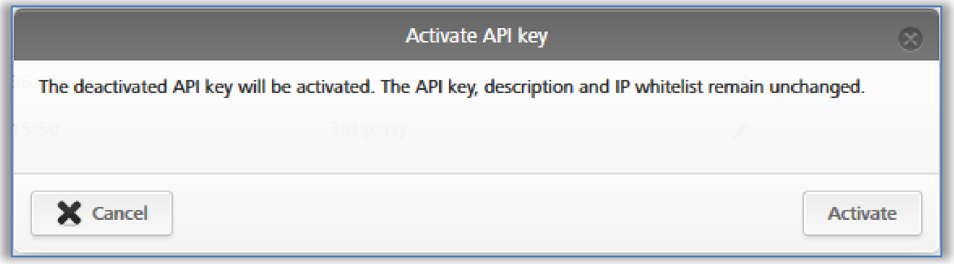
- In the ***Settings*** in the ***General*** tab, in the list of API keys, click ***Deactivate*** ❸ or ***Activate***.
- Confirm the dialogue with ***Deactivate*** or ***Activate*** to complete the process.



Deactivate API key

The existing API key will be deactivated and can only be used again for API access after a new activation.

Figure 327: Deactivate API key



Activate API key

The deactivated API key will be activated. The API key, description and IP whitelist remain unchanged.

Figure 328: Activate deactivated API key

12.4 AirKey Cloud Interface (API) – test environment

The test environment gives you the opportunity to test the AirKey Cloud Interface (API) in a protected environment with test data before activation.

This primarily supports integrators or programmers of third-party systems during integration for the AirKey Cloud Interface. The test environment is also available if the AirKey Cloud Interface has not yet been activated.

No KeyCredits are charged in the test environment. In addition, no SMS are sent via the test environment.

The AirKey Cloud Interface (API) – test environment is accessible via its own endpoint (the API commands must be sent there).
Endpoint: https://integration.api.airkey.evva.com:443/cloud

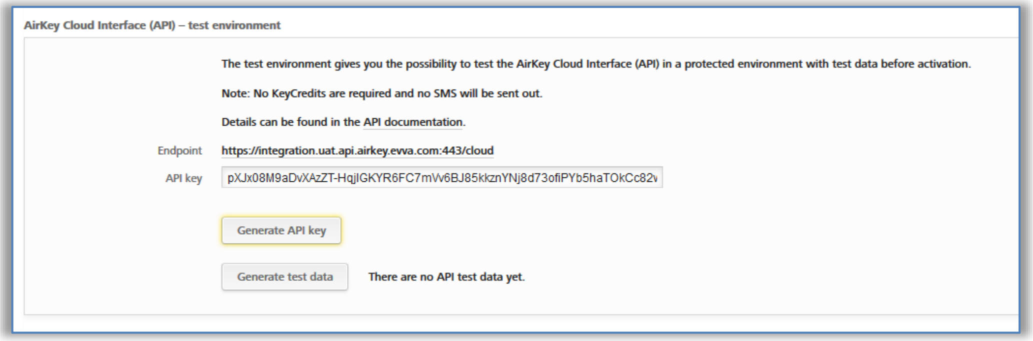
12.4.1 Generate test data

For the first use of the test environment, it is necessary to generate the test data first.

To generate the test data, an API key must first be generated.

> In the ***Settings*** in the ***General*** tab in the section ***AirKey Cloud Interface (API) – test environment***, click ***Generat test data***.

AirKey system manual version 2.7 | 06/03/2024 | Subject to technical changes and misprints



AirKey Cloud Interface (API) – test environment

The test environment gives you the possibility to test the AirKey Cloud Interface (API) in a protected environment with test data before activation.

Note: No KeyCredits are required and no SMS will be sent out.

Details can be found in the API documentation.

Endpoint https://integration.uat.api.airkey.evva.com:443/cloud

API key pXJx08M9aDvXAzZT-HqjIGKYR6FC7mVv6BJ85kkznYNj8d73ofiPYb5haTOkCc82v

There are no API test data yet.

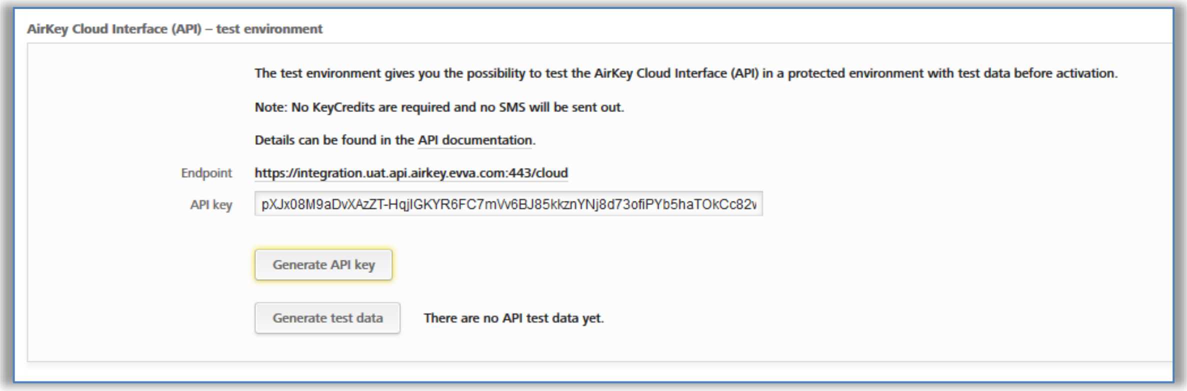
Figure 329: Generate test data

This generated the test data. With the test data it is possible to try every API request from the API documentation. The test data only must be generated only once.

12.4.2 Generate API key

An API key is also required for communication with the AirKey Cloud Interface (API) test environment. Without this API key no API requests can be sent to the test environment. Compared to the correct AirKey Cloud Interface, the API-Key of the test environment is displayed in plain text.

> In the ***Settings*** in the ***General*** tab in the section ***AirKey Cloud Interface (API) – test environment***, click ***Generate API key***.



AirKey Cloud Interface (API) – test environment

The test environment gives you the possibility to test the AirKey Cloud Interface (API) in a protected environment with test data before activation.

Note: No KeyCredits are required and no SMS will be sent out.

Details can be found in the API documentation.

Endpoint https://integration.uat.api.airkey.evva.com:443/cloud

API key pXJx08M9aDvXAzZT-HqjIGKYR6FC7mVv6BJ85kkznYNj8d73ofiPYb5haTOkCc82v

There are no API test data yet.

Figure 330: Generate API key for the test environment

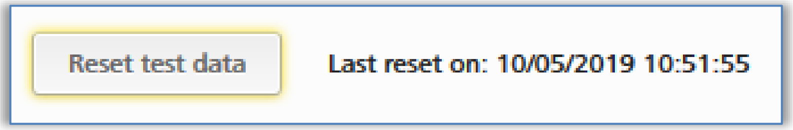
By clicking ***Generate API key*** again, the existing API-Key will be replaced by a new one. The replaced API key can then no longer be used.

An API key must be generated again after each login.

12.4.3 Reset test data

The test data of the AirKey Cloud Interface test environment can be reset to its original state with one click. Thus, all tests can be performed with the same test data.

> In the ***Settings*** in the ***General*** tab in the section ***AirKey Cloud Interface (API) – test environment***, click ***Reset test data***.



Last reset on: 10/05/2019 10:51:55

Figure 331: Reset test data of the test environment

The reset of the test data is confirmed with a success message. The time of the last reset is displayed in the ***AirKey Cloud Interface (API) – test environment*** section.

13 Locking components signals

The locking components indicate events with a host of visual and audible signals.

Signal number	Event	Visual signal*)	Audible signal*)	Note
Signal 1	Unlocking process with authorised medium	🟢🟢🟢🟢🟢	mmmmm	
Signal 2	End of release duration	🔴🔴🔴🔴🔴	lllll	
Signal 3	Unlocking process with unauthorised medium	🔴🔴-🔴🔴-🔴🔴-🔴🔴	hh-hh-hh-hh	
Signal 7	"Battery empty" warning (Shown in the AirKey Online Administration in the table of the locking components and in the details of a locking component as "battery empty" symbol)	🟡🟡--🟡🟡--🟡🟡--🟡🟡	h----h----h----h	The signal is output upon inserting empty batteries instead of signal 8 and upon unlocking before signal 1. 1000 unlocking processes or two weeks of standby mode are guaranteed following the first signals (at room temperature and when using cards, key fobs, combi keys or wristbands).
Signal 8	Insert new batteries or component restart	🔴🔴--🟡🟡--🟢🟢	ll--mm--hh	
Signal 9	Medium without EVVA segmentation; external medium	🔴🔴🔴	None	No longer in use. Only signal 3 is used for this purpose.
Signal 10	Locking component communication or hardware error	🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴	mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm	For instance, indicates a faulty connection between a cylinder's thumb turn and electronics module.

Signal number	Event	Visual signal*)	Audible signal*)	Note
Signal 11	Locking component firmware update	🔵-🔵-🔵-🔵-🔵... (1 s periods, 12 ms impulses)	None	Duration: until communication is complete.
Signal 12	Locking component / media update successful	🟢🟢-🟢🟢	hhhhh	
Signal 13	Locking component / media update unsuccessful	🔴🔴-🔴🔴	lllll	
Signal 14	AirKey medium reader process	🔵-🔵-🔵-🔵-🔵-🔵... (100 ms period, 10 ms pulse)	None	Duration: until communication is complete.
Signal 15	AirKey cylinder wake-up and Bluetooth availability (e.g. as a result of having touched it)	🔵-🔵-🔵-🔵-🔵... (1,5 s periods)	None	
Signal 16	Start of office mode	🟢🟢🟢---🟢🟢🟢	mmm---hhh	
Signal 17	End of office mode	🔴🔴🔴---🔴🔴🔴	hhh---mmm	
Signal 18	Battery emergency mode of an AirKey cylinder	🟡🟡--🟡🟡--🟡🟡--🟡🟡 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴 🟡🟡--🟡🟡--🟡🟡--🟡🟡 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴-- 🔴--🔴--🔴--🔴--🔴 🔴🔴--🟡🟡--🟢🟢 🟡🟡--🟡🟡--🟡🟡--🟡🟡	h----h----h----h mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm h----h----h----h mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm ll--mm--hh h----h----h----h	Cause: One of the batteries was inserted incorrectly or is empty.

*) Descriptions of the signals:

Visual signals: yellow 🟡, red 🔴, green 🟢, blue 🔵

Audible signals: h = high-pitched sound, m = medium-pitched sound, l = low-pitched sound

Each signal corresponds to a duration of 50 ms, pauses are indicated by "-".

14 Values and limits of AirKey

This section describes the maximum number of configurations per medium and locking component.

14.1 AirKey Online Administration

The number of maximum locking components, areas, persons, and media is unlimited.

14.2 Locking components

- The last 1,000 event log entries are saved without updates.
- A maximum of 1,000 blacklist entries can be managed.
- A maximum of 96 areas can be assigned.
- A maximum of 250 shares to further clients can be assigned.

14.3 Cards, key fobs, combi keys or wristbands

- A maximum of 256 event log entries are saved without updates.
- A maximum of 150 authorisations can be assigned to individual doors.
- A maximum of 100 authorisations can be assigned to areas (if you assign 12 individual authorisations with 8 possible access types each, you can only assign a total of 96 authorisations to areas).

14.4 AirKey app

- A maximum of 256 event log entries are saved without updates.
- Unrestricted number of authorisations for individual doors and areas.

15 When are KeyCredits deducted?

KeyCredits are required to operate access control systems, for instance to assign or change access authorisations.

KeyCredits are exclusively deducted in the event of quantity credit. If there is an available time-based credit, the system uses this time-based credit and the quantity credit remains unchanged.

KeyCredits are deducted in the following cases:

- assigning and creating new authorisations
- changing and creating existing authorisations
- reactivating deactivated media, providing the authorisations of the deactivated medium are to be maintained
- replacing smartphones if authorisations will be transferred to the new smartphone
- activating the AirKey Cloud Interface (API).

KeyCredits for new authorisations or changes to authorisations are only deducted once the medium has been created as part of the last step. In this process, one KeyCredit is deducted per creation process. You can also set or change several authorisations at once – in this process, only one KeyCredit is deducted.

No KeyCredits are deducted for deleting authorisations or deactivating or emptying media.

16 Troubleshooting

AirKey is a high-quality, comprehensively tested, electronic access control system. However, should you encounter an error or problems, this section will provide support to rectify the fault.

16.1 No communication possible within the system

Proceed as follows if you are unable to register the smartphone or cannot update locking components:

- Make sure you have an Internet connection available on the smartphone (WLAN or mobile data) and (if applicable) activate it.
- Check if port 443 is disabled in your IT infrastructure. This port is required for the communication within the access control system. Refer to the System requirements section.

16.2 Locking component has trouble identifying or is unable to detect media

Proceed as follows if it is harder than normal or impossible to identify certain media at locking components:

- Make sure the medium does not move on the reader unit during identification and wait until the locking component indicates green. (A blue light merely indicates communication between smartphone and locking component.)
- If the locking component does not react correctly, make sure the medium is positioned correctly. For instance, the combi key must be held against the locking component with the side featuring the RFID icon.
- If this is also unsuccessful, wait 50 seconds without identifying yourself at the reader unit to allow the locking component to recalibrate the electrical field. You can also manually recalibrate the field by holding a metal object to the reader unit.

16.3 Media no longer identified

Proceed as follows if a certain medium is no longer detected at the locking component:

- If this concerns a smartphone, ensure NFC or Bluetooth functionality has been activated If applicable, restart the NFC or Bluetooth connection and make sure the smartphone is positioned on the reader correctly. Please note that there may be differences here, depending on the smartphone type.
- If the reader unit on the locking component or coding station no longer reacts to the medium, hold the medium to the reader unit of a locking component or coding station for a duration of 10 seconds. This then triggers a media self-repair process. You can identify that the process has been completed when the locking component or coding station once again outputs the usual signals.

16.4 Unable to unscrew the thumb turn of an AirKey cylinder

Proceed as follows if you are no longer able to unscrew the thumb turn of an AirKey cylinder:

- Ensure you use the assembly tool for the AirKey cylinder when removing the thumb turn.
- AirKey cylinders with European profiles are equipped with a service bore at the front of the electronics module which can be used to secure the thumb turn sleeve using a matching metal pin. We recommend you use assembly tool set 2.

Procedure:

- Insert the metal pin from assembly tool set 2 into the front service bore of your European profile cylinder.
- In this process, turn the thumb turn until you are able to insert the metal pin considerably deeper into the service bore. Now hold the metal pin in this position and disassemble the thumb turn as usual using the assembly tool.
- Once again remove the metal pin after having removed the thumb turn.
- If you do not have AirKey cylinder with European profile or the AirKey cylinder is fitted in an escutcheon or a rosette with plug pulling protection, hold an authorised medium to the reader unit so the cylinder engages. Attach the assembly tool to the cylinder within the release duration (while the cylinder is engaged). The cylinder then no longer disengages and the thumb turn can be unscrewed more easily.

16.5 Locking component indicates "Hardware error"

If the locking component indicates a hardware error (refer to Locking components signals), it is possible that the thumb turn / reader unit is not connected to the associated electronics module / control unit.

Check the contacts, connectors, and connections as per the assembly manual.

16.5.1 AirKey cylinders

- Ensure the seal has been positioned correctly on the cylinder axis and once again attach the thumb turn to the cylinder by turning it clockwise until you feel a resistance.
- Remove the assembly tool.
- Subsequently turn the thumb turn anti-clockwise until you notice it engages.
- Ensure the thumb turn and electronics module have engaged correctly.

16.5.2 AirKey wall readers

- Ensure the reader unit and the control unit of the AirKey wall reader have been connected correctly. If applicable, check the cabling and the plug connections.

16.6 The electronic thumb turn is hard to operate

Depending on the cylinder’s protrusion beyond the escutcheon or any installed cylinder rosettes, the cylinder may be hard to operate because of the seal causing friction between cylinder housing and electrical thumb turn. There is the option to remove said seals when installing indoors.

However, should you still require support, please do not hesitate to contact your EVVA partner (EVVA support).

17 Important information

17.1 System

⚠ We explicitly point out that this access control system may be subject to mandatory reporting / approval processes depending on the applicable, legal stipulations, particular data protection legislation. As a consequence, EVVA Sicherheitstechnologie GmbH shall not assume any liability for or guarantee operation in compliance with valid, legal stipulations.

⚠ Internet port 443 is used for the communication within the access control system. Ensure this port is not disabled. If you use a mobile data network, the mobile network operator is responsible for managing ports. Please contact your mobile network operator if you encounter any issues when using the mobile data network in connection with AirKey.

⚠ Grant authorisations with validity periods that are as short as possible to maintain a high level of system security and keep the blacklist to a minimum if media is lost. Exclusively create media with authorisations that do not expire as emergency media (e.g. fire service keys).

⚠ Always work with the most recent overall system configuration to maintain a high level of system security.

The following links are available for the security information about individual systems:

Cylinders, padlocks: PDF

Wall readers, control units: PDF

Standards and guidelines

CE tested | EN 1634: 30 minutes | EN 1634: 90 minutes | IP65 rating | EN 15684 | Suitable for locks as per EN 179/1125 (when using the FAP anti-panic function)

SKG | VdS[1]

[1] In progress

18 Technical details for the RS485 interface of Bluetooth wallreader

After a successful access at a Bluetooth wall reader, an APDU with the event log entry of the successful access is sent as payload from the wall reader via the RS485 interface.

In addition to other parameters, the event log entry contains the 5-byte lockingSystemId of the medium (access medium or smartphone) that successfully unlocked the wall reader.

This lockingSystemId (int64) can then be queried via the AirKey Cloud Interface. Example: *GET/v1/media?lockingSystemId=000102030405*

This information can be used to implement various use cases:

- Display the name of the person who has unlocked the wall reader.
- Reading additional parameters, e.g. from the "comment" field of this medium and using this information by third party systems.
- Elevator control: Enter e.g. a minimal JSON string into the comment field of your medium to store a specific floor for an access medium or smartphone and use this information for elevator control.
- Elevator control: Enter e.g. a minimal JSON string into the comment field of an access medium or smartphone to store a specific floor for this medium and use this information for elevator control.

18.1 Activate RS485 interface for Bluetooth wall readers

In order to forward the event log entry via the RS485 interface in the case of a successful access, the corresponding setting must be set on the Bluetooth wall reader in the AirKey Online Administration.

> Select the ***Wall reader*** tile on the ***Home*** page.

> Alternatively, select ***access control system*** → ***Locking components*** in the main menu.

> Click on the Bluetooth wall reader for which you want to activate the function.

> Switch to the ***Settings*** tab.

> Activate the ***RS485 interface*** checkbox at the very bottom.

The Bluetooth wall reader requires the firmware version 5.86 or higher, otherwise a note is displayed that the firmware must be updated to use this function.

18.2 Configuration of the serial RS485 interface

With an RS485 adapter, which is connected to the RS485 interface of the AirKey wall reader, the event log entry of the successful access can be forwarded to a third party system. (e.g. via USB or Ethernet).

The RS485 adapter must be connected to the control unit at the connector for the reader unit in addition to the existing cable of the reader unit.

- Pin 2 of the connector → Doorbus B-
- Pin 3 of the connector → Doorbus A+

Further information on the pin connection can be found on the wiring diagram on the cover of the control unit.

The serial interface must be configured as follows:

- Baudrate: 115200
- Data bit: 8
- Stop bit: 1
- Parity: even
- No CTS flow control

18.3 APDU specification of the event log entry

18.3.1 APDU of the event log entry

APDU Bytes	CLA	INS	P1	P2	LE (data length)	data
Byte	0xCC	0xD6	0xF0	0x00	0x0E	<14 byte event log entry>
Example	0xCC	0xD6	0xF0	0x00	0x0E	0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c

18.3.2 14 byte event log entry

Byte	00	01	02	03	04	05	06	07	08	09	10	11	12	13
Description	lockingSystemId					Timestamp				Unlocking status	customerID (not used)			
Example	0e	4e	25	34	f0	32	76	d3	b9	7a	00	00	02	8c

18.3.2.1 Timestamp format

Byte 1								Byte 2								Byte 3								Byte 4								Byte
8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	8	7	6	5	4	3	2	1	Bits
*	*	*	*	*	*																											R1
						*	*	*	*																							R2
										*	*	*	*	*																		R3
															*	*	*	*	*													R4
																				*	*	*	*	*	*							R5
																										*	*	*	*	*	*	R6
																																Example
0	0	1	1	0	0	1	0	0	1	1	1	0	1	1	0	1	1	0	1	0	0	1	1	1	0	1	1	1	0	0	1	R7

R1 … Year: Year minus 2010 (Year 2022 = **001100**)
R2 … Month: Jan = **01**, Feb = **02**, Mar = **03**, etc.
R3 … Day: value range **01–31**
R4 … Hour: value range **00–23**
R5 … Minutes: value range **00–59**
R6 … Seconds: value range **00–59**
R7 … Example: **00110010 01110110 11010011 10111001** corresponds to 2022-09-27 13:14:57

18.3.2.2 Unlocking status

Byte 1									Description
b8	**b7**	**b6**	**b5**	**b4**	**b3**	**b2**	**b1**		**Bit**
0									**R1**
1									**R2**
	0	0	0						**R3**
	0	0	1						**R4**
	0	1	0						**R5**
	0	1	1						**R6**
	1	0	0						**R7**
	1	1	0						**R8**
	1	0	1						**R9**
	1	1	1						**R10**
				•	•	•	•		**R11**
0	1	1	1	1	0	1	0		**R12**

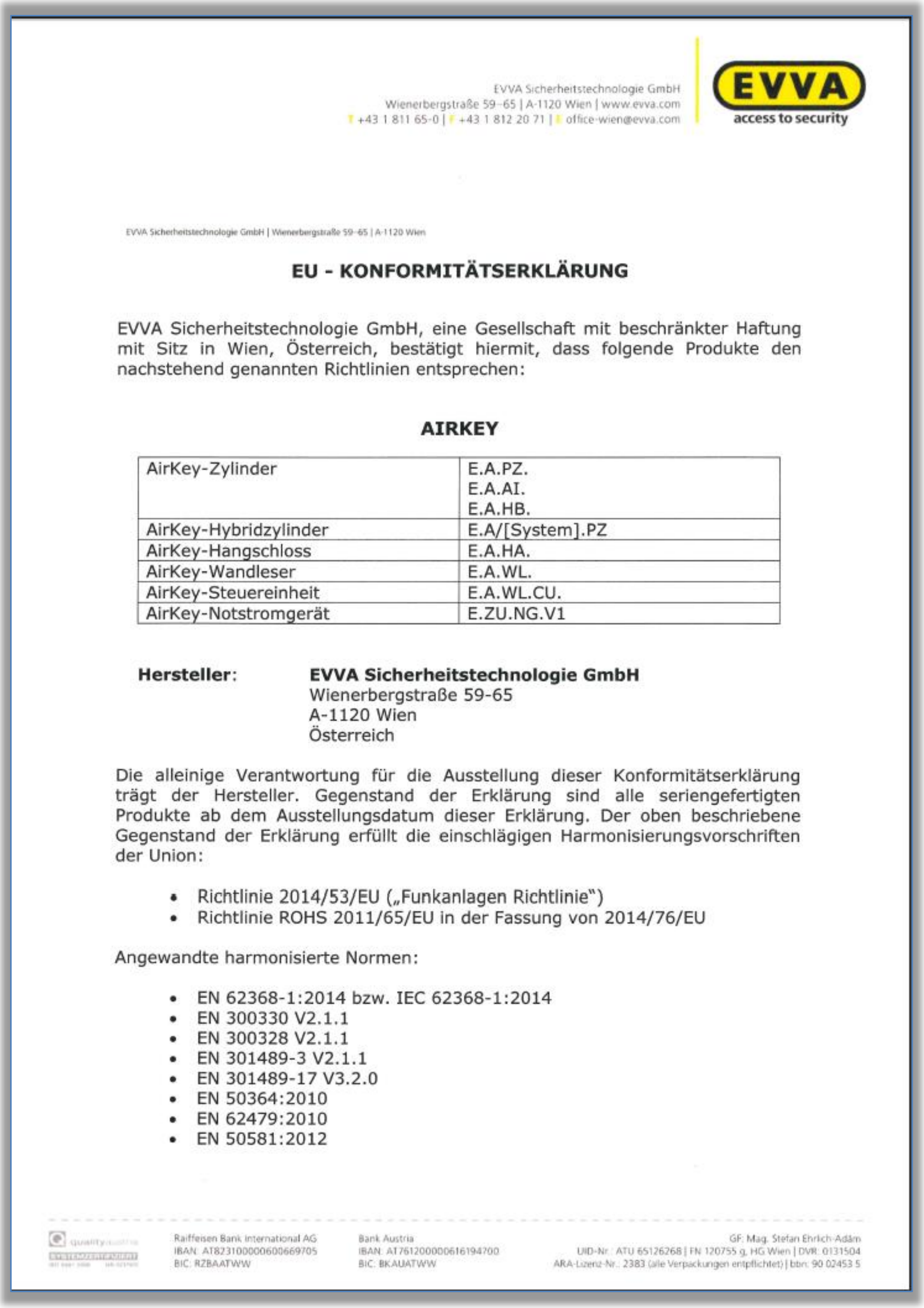
R1 … Time is correct
R2 … Time is incorrect. No power supply for a too long time.
R3 … Access denied: Currently not authorised
R4 … Access denied: Medium is listed on the blacklist of the locking component
R5 … Access denied: Time is incorrect
R6 … Access denied: Signature error
R7 … Access denied: Component does not know the share (sharing in another acces control system)
R8 … Access denied: Holiday is active
R9 … Access granted: Access granted via Hands-free
R10 … Access granted
R11 … Battery status: For wall reader always 100 %
R12 … Example: **0x7a** means time is correct, access granted, 100 % battery status

18.3.3 Example

- APDU: **CC D6 F0 00 0E 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c**
- Event log entry: **0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c**
  - lockingSystemId: **0e 4e 25 34 f0**
  - Timestamp AirKey: **32 76 d3 b9** = 2022-09-27 13:14:57
  - Unlocking status: **7a** = time is correct, access granted, 100 % battery status
  - customerId: **00 00 02 8c**

It is also possible to forward the lockingSystemId of an access media to third-party systems via the coding station. To do this, use the "-notify" parameter when starting the coding station via the command line. Details can be found in the chapter Using the coding station via the command line.

19 Konformitätserklärung



EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA
access to security

EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59–65 | A-1120 Wien

EU - KONFORMITÄTSERKLÄRUNG

EVVA Sicherheitstechnologie GmbH, eine Gesellschaft mit beschränkter Haftung mit Sitz in Wien, Österreich, bestätigt hiermit, dass folgende Produkte den nachstehend genannten Richtlinien entsprechen:

AIRKEY

AirKey-Zylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridzylinder	E.A/[System].PZ
AirKey-Hangschloss	E.A.HA.
AirKey-Wandleser	E.A.WL.
AirKey-Steuereinheit	E.A.WL.CU.
AirKey-Notstromgerät	E.ZU.NG.V1

Hersteller: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Wien
Österreich

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt der Hersteller. Gegenstand der Erklärung sind alle seriengefertigten Produkte ab dem Ausstellungsdatum dieser Erklärung. Der oben beschriebene Gegenstand der Erklärung erfüllt die einschlägigen Harmonisierungsvorschriften der Union:

- Richtlinie 2014/53/EU („Funkanlagen Richtlinie")
- Richtlinie ROHS 2011/65/EU in der Fassung von 2014/76/EU

Angewandte harmonisierte Normen:

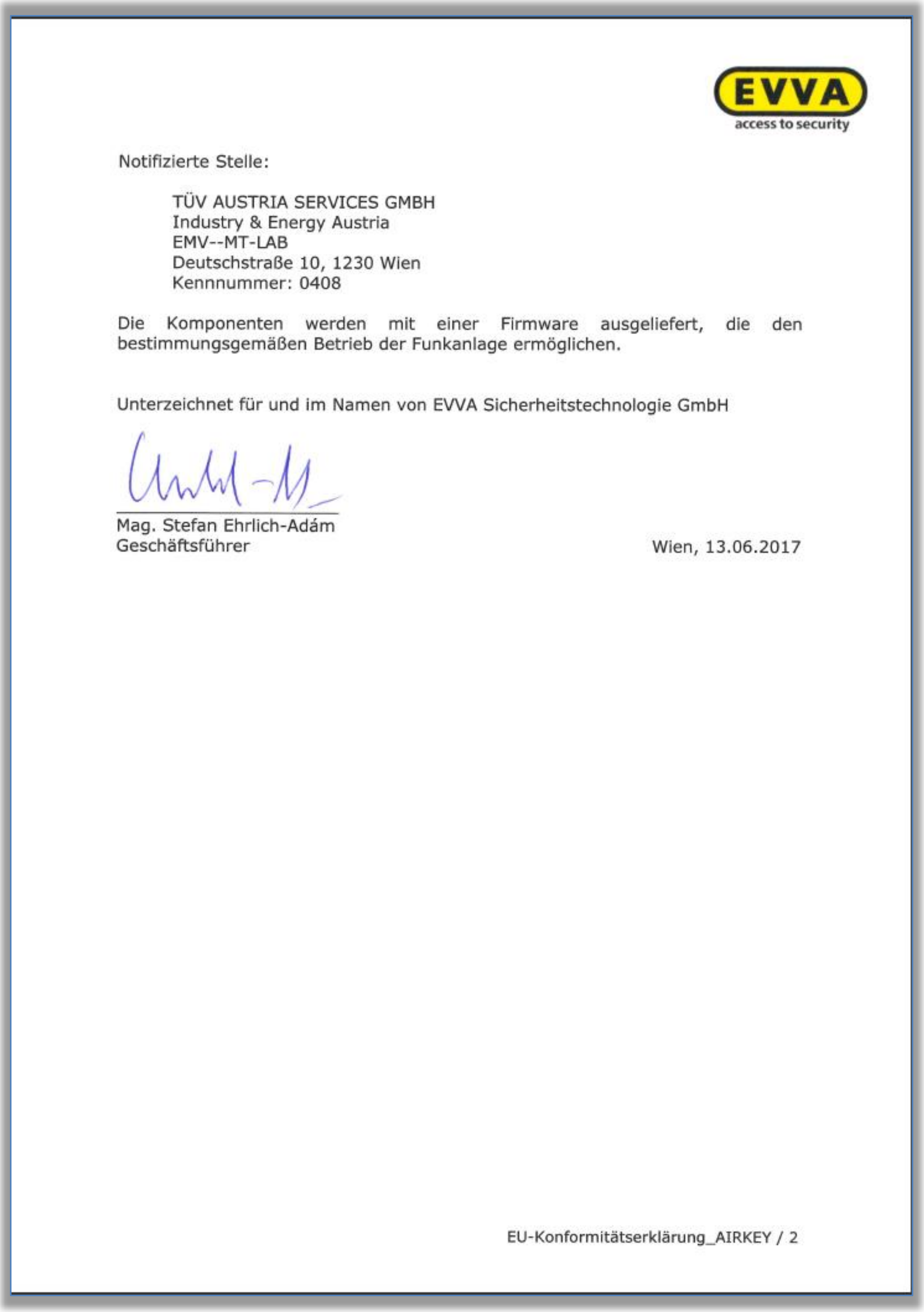
- EN 62368-1:2014 bzw. IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

quality austria
SYSTEMZERTIFIZIERT

Raiffeisen Bank International AG
IBAN: AT823100000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT761200000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5



EVVA
access to security

Notifizierte Stelle:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Wien
Kennnummer: 0408

Die Komponenten werden mit einer Firmware ausgeliefert, die den bestimmungsgemäßen Betrieb der Funkanlage ermöglichen.

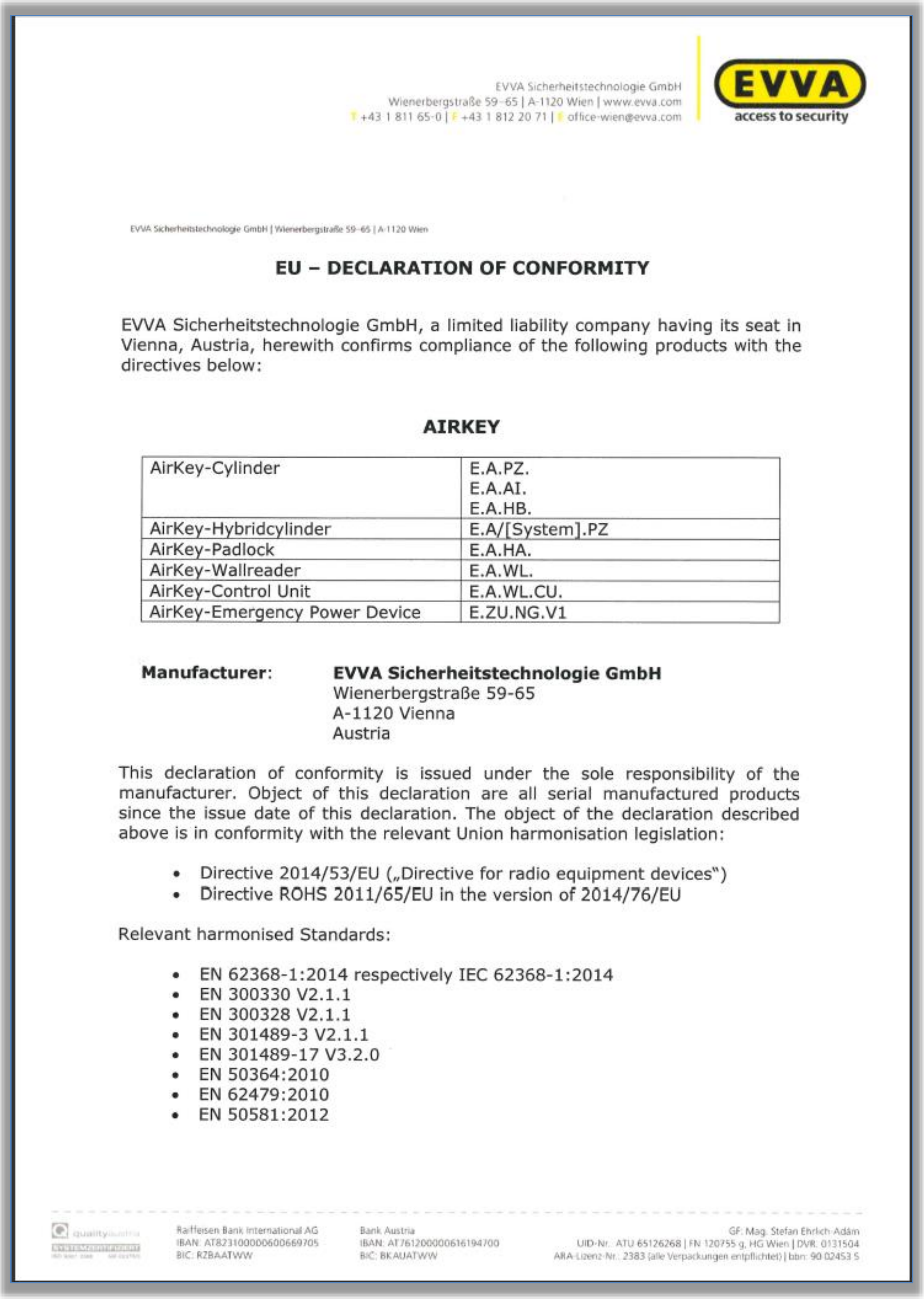
Unterzeichnet für und im Namen von EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Geschäftsführer

Wien, 13.06.2017

EU-Konformitätserklärung_AIRKEY / 2

20 Declaration of Conformity



EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59–65 | A-1120 Wien

EU – DECLARATION OF CONFORMITY

EVVA Sicherheitstechnologie GmbH, a limited liability company having its seat in Vienna, Austria, herewith confirms compliance of the following products with the directives below:

AIRKEY

AirKey-Cylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridcylinder	E.A/[System].PZ
AirKey-Padlock	E.A.HA.
AirKey-Wallreader	E.A.WL.
AirKey-Control Unit	E.A.WL.CU.
AirKey-Emergency Power Device	E.ZU.NG.V1

Manufacturer: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Vienna
Austria

This declaration of conformity is issued under the sole responsibility of the manufacturer. Object of this declaration are all serial manufactured products since the issue date of this declaration. The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

- Directive 2014/53/EU („Directive for radio equipment devices")
- Directive ROHS 2011/65/EU in the version of 2014/76/EU

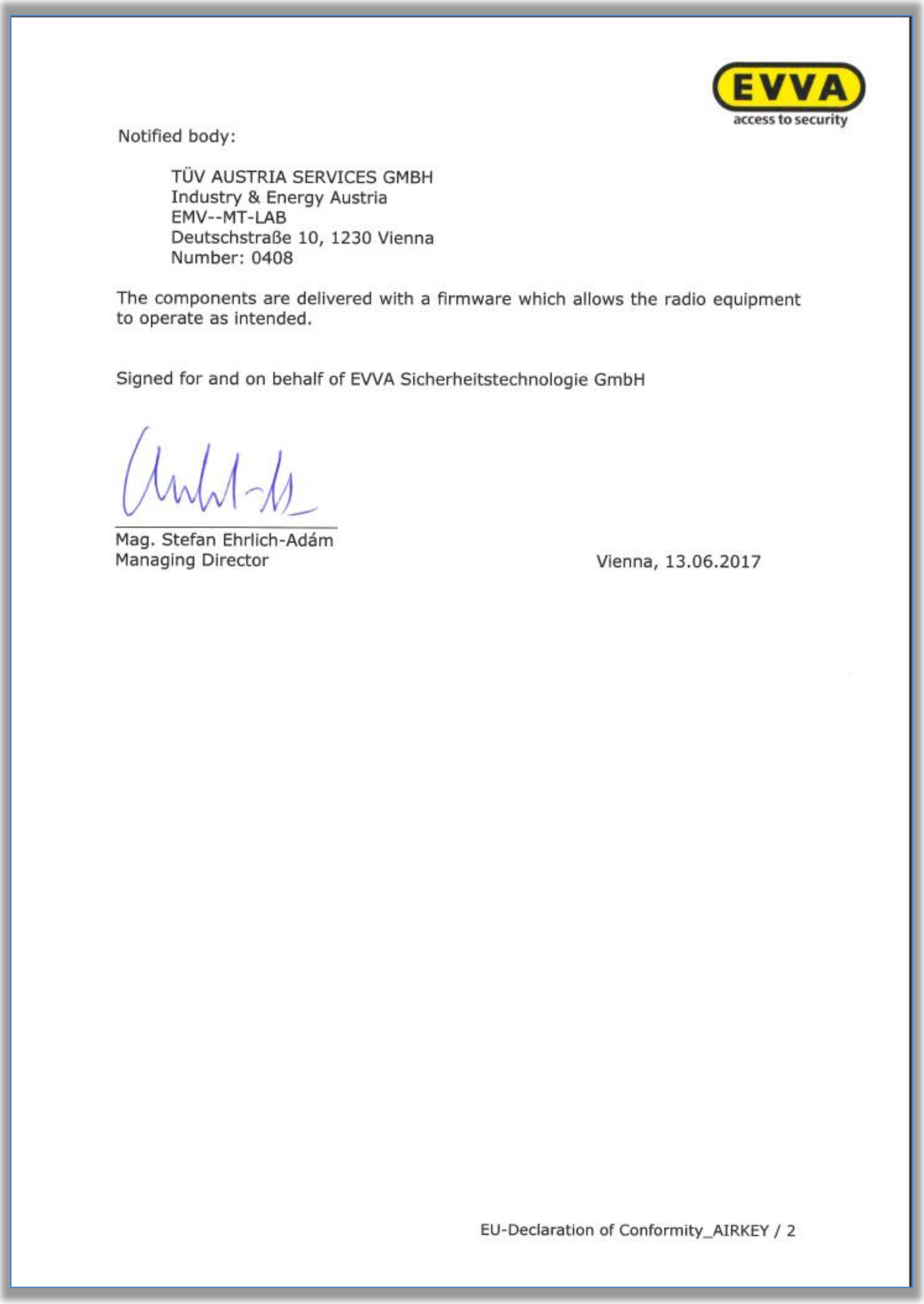
Relevant harmonised Standards:

- EN 62368-1:2014 respectively IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

Raiffeisen Bank International AG
IBAN: AT823100000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT761200000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5



EVVA
access to security

Notified body:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Vienna
Number: 0408

The components are delivered with a firmware which allows the radio equipment to operate as intended.

Signed for and on behalf of EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Managing Director

Vienna, 13.06.2017

EU-Declaration of Conformity_AIRKEY / 2

21 List of figures

22 Glossary

The following terms are used within the context of AirKey:

Designation	Function
Client	Owner of the AirKey system with a unique customer number.
Administrator	User role within the AirKey system authorised to execute all administrative activities within the AirKey Online Administration. It is possible to create several administrators for one client. A minimum of one administrator must be defined for each access control system.
Person	Users using authorisation media. Persons can receive media with access authorisations for areas and locking components.
Media	Media are smartphones or access media that can be added to the AirKey access control system to gain access at authorised locking components.
Access media	These are passive media that can be used in AirKey access control systems in addition to smartphones. These include cards, key fobs, combi keys, and wristbands.
Source medium	This term is used in connection with the "smartphone replacement" and "duplicate medium" functions. It describes the smartphone or the access medium from which the replacement or duplication was started. In the case of the smartphone replacement, the source medium describes the "old" smartphone that will be replaced by a new one.
Target medium	This term is used in connection with the "smartphone replacement" and "duplicate medium" functions. It describes the smartphone or the access medium to which the AirKey authorisations and settings will be transferred. In the case of the smartphone replacement, the target medium describes the "new" smartphone.
Locking components	AirKey cylinders (in all configurations), padlocks, and wall readers that open and close doors within an access control system.
Area	Is an administrative unit in the AirKey Online Administration that comprises several locking components. Areas simplify the administration of the AirKey access control system and the assignment of authorisations for locking components.
KeyCredits	Describes a credit balance within an AirKey access control system. Credit is required to assign new authorisations, change existing authorisations, or activate additional AirKey functionalities.

AirKey Cloud Interface	The AirKey Cloud Interface is an interface (API) for third-party systems based on REST. The interface allows certain AirKey functions to be controlled via third-party software.
RS485 interface	The RS485 interface is a standardized interface that can be used to transmit data. With an AirKey wall reader, the last successful access can be forwarded to third-party software via this interface.
APDU	APDU stands for Application Protocol Data Unit and is used here in the document for the RS485 interface. It describes a data packet which is transmitted via the RS485 interface.
"Send a Key"	Describes a function of the AirKey Online Administration. An administrator can quickly create new smartphones and assign authorisations or edit existing authorisations of smartphones. The smartphone owner receives an SMS which automatically registers the smartphone for AirKey.
Two-factor authentication	The two-factor authentication (2FA) is used as an additional security level when logging into the AirKey Online Administration. In addition to the user ID and password, an SMS code is requested as a second factor at the login.
Four-eyes principle	Describes a process in which an action can only be performed by an additional person. In AirKey, this principle can be used to protect personal data in the event logs.
Firmware	Software program that runs on locking components so that they can perform their AirKey function. The firmware of locking components can be updated in the form of firmware updates.
Keyring	In the AirKey system, "Keyring" is the name of a software program that manages all AirKey-relevant data stored on passive access media such as cards, key fobs, combi keys, and wristbands. If a new Keyring version is available in the AirKey system, the media can be updated with a smartphone with maintenance authorisation or with a coding station.
Maintenance tasks	Displayed within the AirKey Online Administration for locking components that are not up to date. Only when all maintenance tasks of an AirKey access control system have been finished is the system updated and safe.
Maintenance authorisation	Smartphones can exclusively be used to add or delete components (media and locking components) in the access control system if they have been granted a maintenance authorisation. AirKey maintenance engineers can also operate locking components in factory state using smartphones with maintenance authorisations. Activate the maintenance authorisation for the desired smartphone in the AirKey Online Administration.

23 Legal notice

7th edition, November 2022

This edition shall not longer be valid upon publication of a new system manual. Please download the most recent version of the system manual from our homepage: https://www.evva.com/en/airkey/systemmanual/.

This system manual may contain defects or misprints resulting from printing. However, the data in this system manual is revised regularly and corrections are incorporated. We shall not assume any liability for technical or printing errors and their potential consequences.

We reserve the rights to make adaptations and update the document without prior notification.

Legal notice

Publisher
EVVA Sicherheitstechnologie GmbH

Content management
EVVA Sicherheitstechnologie GmbH

Technical contents
Florian Diener, Johannes Ullmann

Technical consultants
Iulian Stanciulescu, Raphael Fasching, Martin Bauer