

AirKey

Systemhandbuch 2.7

1 Inhaltsverzeichnis

2	Einführung, Übersicht.....	9
2.1	Allgemeine rechtliche Hinweise.....	9
2.2	EVVA-Support	10
2.3	Zeichenerklärung.....	11
2.4	Tipps zur optimalen Navigation in diesem Dokument.....	11
3	Systemarchitektur	12
3.1	Schließkomponenten	13
3.1.1	AirKey-Zylinder	13
3.1.2	AirKey-Hybridzylinder	14
3.1.3	AirKey-Hebelzylinder.....	14
3.1.4	AirKey-Hangschloss	15
3.1.5	AirKey-Wandleser	15
3.2	AirKey-App	16
3.3	Smartphones	16
3.4	AirKey-Medien.....	17
3.5	AirKey-Onlineverwaltung	18
3.5.1	Systemvoraussetzungen.....	18
3.6	EVVA-KeyCredits	18
3.7	Codierstation	18
3.8	Notstromgerät.....	19
4	Inbetriebnahme	20
4.1	AirKey-App installieren	20
4.2	In der AirKey-Onlineverwaltung registrieren.....	20
4.3	Anmelden	23
4.4	Interaktive Hilfe	24
4.5	Codierstation installieren	25
4.5.1	Codierstation über die AirKey-Onlineverwaltung verwenden.....	25
4.5.2	Codierstation über die Kommandozeile verwenden.....	28
4.5.3	Einstellungen der Codierstation-Applikation	29
4.5.4	Lösungen für mögliche Probleme mit der Codierstation.....	30
4.6	Guthaben aufladen	33
4.7	Person anlegen.....	34
4.7.1	Personendaten importieren	36
4.8	Smartphone anlegen	42

4.9	Smartphone registrieren	45
4.9.1	Funktion "Send a Key"	47
4.10	Schließkomponenten installieren.....	51
4.10.1	AirKey-Zylinder, -Hybridzylinder, -Hebelzylinder und -Hangschloss	51
4.10.2	AirKey-Wandleser	51
4.11	Schließkomponente hinzufügen	52
4.11.1	Schließkomponente mit dem Smartphone hinzufügen	52
4.11.2	Schließkomponente mit der Codierstation hinzufügen.....	55
4.12	Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen.....	58
4.13	Person einem Medium zuweisen	60
4.14	Berechtigungen vergeben	61
4.14.1	Dauerzutritt	62
4.14.2	Periodischer Zutritt	63
4.14.3	Temporärer Zutritt.....	65
4.14.4	Individueller Zutritt.....	65
4.15	Berechtigung anfertigen	66
5	AirKey-Onlineverwaltung	68
5.1	AirKey-Login	68
5.1.1	AirKey-Login ohne Zwei-Faktor-Authentifizierung	68
5.1.2	AirKey-Login mit Zwei-Faktor-Authentifizierung.....	69
5.1.3	Passwort vergessen	70
5.2	AirKey-Logout	73
5.3	Administratoren.....	73
5.3.1	Administrator anlegen	74
5.3.2	Administrator bearbeiten	76
5.3.3	Administrator löschen	78
5.4	Einstellungen der AirKey-Schließanlage	79
5.4.1	Allgemein	79
5.4.2	Vorgabewerte (für alle neu hinzugefügten Schließkomponenten)	86
5.4.3	Feiertage.....	91
5.5	Schließanlage.....	93
5.5.1	Übersicht der Schließkomponenten	93
5.5.2	Schließkomponente hinzufügen: Siehe Kapitel 4.11	94
5.5.3	Schließkomponente bearbeiten.....	94
5.5.4	Schließkomponente entfernen	97

5.5.5	Bereiche.....	98
5.5.6	Bereich anlegen.....	98
5.5.7	Schließkomponente zu Bereichen zuweisen.....	99
5.5.8	Zuweisung von Schließkomponenten zu einem Bereich aufheben.....	100
5.5.9	Bereich löschen.....	101
5.5.10	Berechtigungsübersicht.....	102
5.5.11	Wartungsaufgaben.....	104
5.5.12	Kundendaten – Schließplan.....	105
5.6	Medien & Personen.....	107
5.6.1	Übersicht der Personen.....	107
5.6.2	Person anlegen: Siehe Kapitel 4.7.....	108
5.6.3	Person bearbeiten.....	108
5.6.4	Person löschen.....	109
5.6.5	Medium einer Person zuweisen.....	110
5.6.6	Übersicht der Medien.....	112
5.6.7	Medium hinzufügen.....	112
5.6.8	Smartphone anlegen: Siehe Kapitel 4.8.....	113
5.6.9	Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder anlegen.....	113
5.6.10	Medium bearbeiten.....	114
5.6.11	Person einem Medium zuweisen: Siehe Kapitel 4.13.....	114
5.6.12	Berechtigungen.....	114
5.6.13	Berechtigungen vergeben: Siehe Kapitel 4.14.....	115
5.6.14	Berechtigung anfertigen: Siehe Kapitel 4.15.....	115
5.6.15	Berechtigung ändern.....	115
5.6.16	Berechtigung löschen.....	117
5.6.17	Medium deaktivieren.....	119
5.6.18	Deaktiviertes Medium entfernen.....	120
5.6.19	Medium reaktivieren.....	121
5.6.20	Smartphone tauschen.....	122
5.6.21	Medium duplizieren.....	122
5.6.22	Medium leeren.....	123
5.6.23	Zuweisung aufheben.....	124
5.6.24	Medium entfernen.....	127
5.7	Protokolle.....	128
5.7.1	Schließkomponentenprotokoll.....	129
5.7.2	Medienprotokoll.....	132

5.7.3	Systemprotokoll	135
5.8	Support-Freigaben	136
5.8.1	Support-Freigabe anlegen.....	136
5.8.2	Support-Freigabe sperren	138
5.9	Hilfe.....	139
6	AirKey-App	140
6.1	Bluetooth-Komponenten	140
6.2	Smartphone registrieren: Siehe Kapitel 4.9.....	140
6.3	Berechtigungen	140
6.4	Wartungsaufgaben: Siehe Kapitel 6.12	142
6.5	Daueröffnung	142
6.6	PIN eingeben	143
6.7	Medien codieren	143
6.8	Berechtigungsprotokoll.....	144
6.9	Einstellungen der AirKey-App	145
6.9.1	Einstellungen der AirKey-App auf Android-Smartphones	145
6.9.2	Einstellungen der AirKey-App auf iPhones	146
6.9.3	Hands-free-Reichweite einstellen	146
6.9.4	Hands-free-Modus	147
6.9.5	Sperren aus Benachrichtigungen	147
6.9.6	Sicherheitsfunktionen.....	149
6.9.6.1	PIN aktivieren	150
6.9.6.2	PIN ändern	150
6.9.6.3	PIN deaktivieren.....	151
6.9.7	Benachrichtigungen	153
6.9.8	Schließenanlage hinzufügen	154
6.9.9	Smartphone tauschen	155
6.9.10	Info	155
6.10	Smartphone aktualisieren	155
6.11	Mit Komponente verbinden	156
6.12	Spezialberechtigung "Wartungsberechtigung".....	158
6.13	Hinzufügen einer AirKey-Komponente	160
6.13.1	Medien hinzufügen: Siehe Kapitel 4.12.....	160
6.13.2	Schließkomponente hinzufügen: Siehe Kapitel 4.11	160
6.14	Entfernen einer AirKey-Komponente	160
6.15	Protokolldaten in der AirKey-App	163

6.16	Hands-free auf einen Blick	164
7	Bedienung von AirKey-Schließkomponenten	167
7.1	Zutritt mit dem Smartphone	167
7.2	Zutritt mit Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder 168	
8	Betrieb & Wartung des AirKey-Systems	169
8.1	Schließkomponenten aktualisieren	169
8.2	Smartphone aktualisieren: Siehe Kapitel 6.10	171
8.3	Medien aktualisieren	171
8.4	Firmware von Schließkomponenten aktualisieren	174
8.5	Keyring-Version von Medien aktualisieren	179
8.6	App-Version des Smartphones aktualisieren	183
8.7	Batteriewechsel und Notstromöffnung	183
8.7.1	Batteriewechsel beim AirKey-Zylinder	184
8.8	Reparaturoptionen	185
8.8.1	Ersatzschließkomponente ausstellen und einbauen	186
8.8.2	Schließkomponente ersatzlos ausbauen und als "defekt" markieren	189
8.8.3	Defekte Schließkomponente mittels Smartphone ausbauen	191
8.8.4	Defekte Schließkomponente mittels AirKey-Onlineverwaltung ausbauen	192
8.8.5	Wartungsaufgaben für Reparaturoptionen rückgängig machen	193
9	Notmedien	195
9.1	Notmedien ausstellen	195
10	Medientausch	196
10.1	Smartphonetausch	196
10.1.1	Tausch als Smartphone-Besitzer starten	196
10.1.2	Tausch als Administrator starten	199
11	Arbeiten mit mehreren AirKey-Schließanlagen	202
11.1	Schließkomponente für andere Schließanlagen freigeben	202
11.2	Schließkomponente aus anderen Schließanlagen hinzufügen	203
11.3	Berechtigungen für freigegebene Schließkomponenten vergeben	205
11.4	Berechtigungen für freigegebene Schließkomponenten einsehen	206
11.5	Freigabe einer Schließkomponente aufheben	207
11.6	Smartphone in mehreren Anlagen verwenden	208
12	AirKey Cloud Interface (API)	210
12.1	Aktivierung des AirKey Cloud Interface	210
12.2	API-Key generieren	211

12.3	API-Key bearbeiten	213
12.3.1	API-Key neu generieren	213
12.3.2	API-Key löschen	213
12.3.3	API-Key de- und aktivieren	214
12.4	AirKey Cloud Interface – Testumgebung	215
12.4.1	Testdaten generieren	215
12.4.2	API-Key generieren.....	215
12.4.3	Testdaten zurücksetzen	216
13	Signalisierung der Schließkomponenten	217
14	Werte und Limits von AirKey	219
14.1	AirKey-Onlineverwaltung	219
14.2	AirKey-Schließkomponenten	219
14.3	Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder.....	219
14.4	AirKey-App	219
15	Wann werden KeyCredits abgebucht?	220
16	Fehlerbehebungen	221
16.1	Keine Kommunikation innerhalb des Systems möglich	221
16.2	Schließkomponente erkennt Medien nur schlecht oder überhaupt nicht.....	221
16.3	Medien werden nicht mehr erkannt	221
16.4	Knauf eines AirKey-Zylinders lässt sich nicht abschrauben	222
16.5	Die Schließkomponente signalisiert einen "Hardwarefehler"	222
16.5.1	AirKey-Zylinder	222
16.5.2	AirKey-Wandler	223
16.6	Der elektronische Knauf ist schwergängig	223
17	Wichtige Hinweise.....	224
17.1	System	224
18	Technische Details zur RS485-Schnittstelle bei Bluetooth-Wandlern	225
18.1	RS485-Schnittstelle für Bluetooth-Wandler aktivieren	225
18.2	RS485-Konfiguration der seriellen Schnittstelle	225
18.3	APDU-Spezifikation des Protokolleintrags des erfolgreichen Zutritts	226
18.3.1	APDU des Protokolleintrags	226
18.3.2	14-Byte-Protokolleintrag	226
18.3.2.1	Timestamp-Format	226
18.3.2.2	Unlocking-Status	227
18.3.3	Beispiel	227
19	Konformitätserklärung	229

20	Declaration of Conformity	231
21	Abbildungsverzeichnis	233
22	Glossar.....	241
23	Impressum	244

2 Einführung, Übersicht

Das vorliegende AirKey-Systemhandbuch beinhaltet Informationen zu Installation, Betrieb und Bedienung des elektronischen Schließsystems AirKey, bestehend aus AirKey-Onlineverwaltung, -App, -Zylindern, -Wandlesern, -Hangschlössern und -Medien.

Die im AirKey-Systemhandbuch beschriebenen Produkte bzw. die Anwendersoftware "AirKey-Onlineverwaltung" dürfen nur von Personal betrieben werden, das für die jeweilige Aufgabenstellung qualifiziert ist. Qualifiziertes Personal ist auf Grund seines Know-hows befähigt, im Umgang mit diesen Produkten / Systemen Risiken zu erkennen und mögliche Gefährdungen zu vermeiden.

2.1 Allgemeine rechtliche Hinweise

- > EVVA schließt den Vertrag zur Nutzung von AirKey nur auf Basis ihrer Allgemeinen Geschäftsbedingungen (EVVA-AGB) sowie ihrer Allgemeinen Lizenzbedingungen (EVVA-ALB) in Bezug auf die Software zum Produkt ab. Diese sind abrufbar unter:
 - <https://www.evva.com/at-de/impressum/> (für Österreich)
 - <https://www.evva.com/de-de/impressum/> (für Deutschland)
 - <https://www.evva.com/ch-de/impressum/> (für die Schweiz)
- > Der Käufer wird ausdrücklich darauf hingewiesen, dass der Einsatz des vertragsgegenständlichen Schließsystems gesetzliche, insbesondere datenschutzrechtliche Genehmigungs-, Melde- und Registrierungspflichten (z.B. Informationsverbundsystem), sowie bei Einsatz im Unternehmen Mitbestimmungsrechte der Belegschaft, auslösen kann. Die Verantwortung für den rechtskonformen Einsatz des Produkts liegt beim Käufer bzw. Kunden und dem Endnutzer.
- > Gemäß der im Produkthaftungsgesetz definierten Haftung des Herstellers für seine Produkte sind die vorstehenden Informationen zu beachten und an die Betreiber und Nutzer weiterzugeben. Die Nichtbeachtung entbindet EVVA von der Haftpflicht.
- > Nicht geeignet in der Umgebung von Kindern unter 36 Monaten, wegen Erstickungsgefahr durch verschluckbare Kleinteile.
- > Nicht vereinbarungsgemäße bzw. unübliche Verwendung, nicht ausdrücklich von EVVA zugelassene Reparaturarbeiten bzw. Modifikationen sowie nicht fachgemäßes Service können zu Funktionsstörungen führen und sind zu unterlassen. Jegliche, nicht ausdrücklich von EVVA zugelassene Änderungen führen zu Verlust von Haftungs-, Gewährleistungs- und gesondert vereinbarten Garantieansprüchen.
- > Architekten und beratende Institutionen sind angehalten, alle erforderlichen Produktinformationen von EVVA einzuholen, um den Informations- und Instruktionspflichten gemäß Produkthaftungsgesetz nachzukommen. Fachhändler und Verarbeiter haben die Hinweise in den EVVA-Dokumentationen zu beachten und diese gegebenenfalls an deren Kunden zu übermitteln.
- > Bitte beachten Sie bei der Projektierung und Installation der Schließkomponente die entsprechenden internationalen und landesspezifischen Vorgaben in den jeweiligen Gesetzen, Verordnungen, Normen und Richtlinien, insbesondere hinsichtlich der Anforderungen an Fluchtwege sowie an Notausgänge.

2.2 EVVA-Support

Mit AirKey steht Ihnen ein ausgereiftes und geprüftes Schließsystem zur Verfügung. Sollten Sie dennoch Unterstützung benötigen, wenden Sie sich bitte an Ihren EVVA-Partner.

Eine Liste an zertifizierten EVVA-Partnern finden Sie auf unserer Homepage unter <https://www.evva.com/at-de/haendlersuche/>.

Wenn Sie die Filter-Option "Elektronik-Partner" auswählen, filtern Sie gezielt nach EVVA-Partnern, die die elektronischen EVVA-Schließsysteme vertreiben und über ein qualifiziertes Fachwissen in diesem Bereich verfügen.

Für bestimmte Supportanfragen nutzen Sie das von EVVA bereitgestellte Onlineformular. Das Onlineformular steht Ihnen derzeit für die folgenden Situationen zur Verfügung:

- > Maximale Eingabe an falschen Guthabencodes überschritten.
- > Guthaben kann nicht aufgeladen werden.
- > Login-Seite der AirKey-Onlineverwaltung nicht erreichbar.
- > Login nicht möglich. Benutzerkennung und/oder E-Mail-Adresse vergessen.
- > Sie haben die Zwei-Faktor-Authentifizierung aktiviert und haben keinen Zugriff auf Ihre Telefonnummer.

Das Support-Onlineformular finden Sie unter folgendem Link:

<https://www.evva.com/de/airkey/support/>.

Allgemeine Informationen zu AirKey finden Sie auf unserer Homepage unter

<https://www.evva.com/de/airkey/website/>.

2.3 Zeichenerklärung

Auf diese Art werden in diesem Systemhandbuch Befehlsfolgen, einzelne Befehle oder Schaltflächen dargestellt.

Beispiel: Hauptmenü **Medien & Personen** → **Person anlegen** oder Schaltflächen wie z.B. **Speichern**.



Achtung, Gefahr eines Sachschadens, wenn die entsprechenden Vorsichtsmaßnahmen nicht eingehalten werden.



Hinweise und zusätzliche Informationen



Tipps und Empfehlungen



Fehlermeldungen

Option

Optionen



2.4 Tipps zur optimalen Navigation in diesem Dokument

In diesem Dokument gibt es auch viele interne Links, die zu anderen Kapiteln oder Textstellen führen. Am schnellsten und bequemsten kommen Sie unter Windows zur ursprünglichen Stelle zurück oder wieder vorwärts mit diesen **Tastenkombinationen**:

 +  (Alt + Cursor-Pfeil nach links) = zurück navigieren

 +  (Alt + Cursor-Pfeil nach rechts) = vorwärts navigieren

Diese Tastenkombinationen funktionieren in vielen PDF-Betrachtern sowie z.B. in Microsoft Word.

Um die Tastenkombinationen auszuprobieren, klicken Sie diesen [Link](#) an und navigieren Sie zurück mit  + .

3 Systemarchitektur

In nachfolgender Abbildung erhalten Sie den Überblick über die von AirKey eingesetzten Komponenten und deren Kommunikationswege. Die einzelnen Komponenten werden im Anschluss beschrieben.

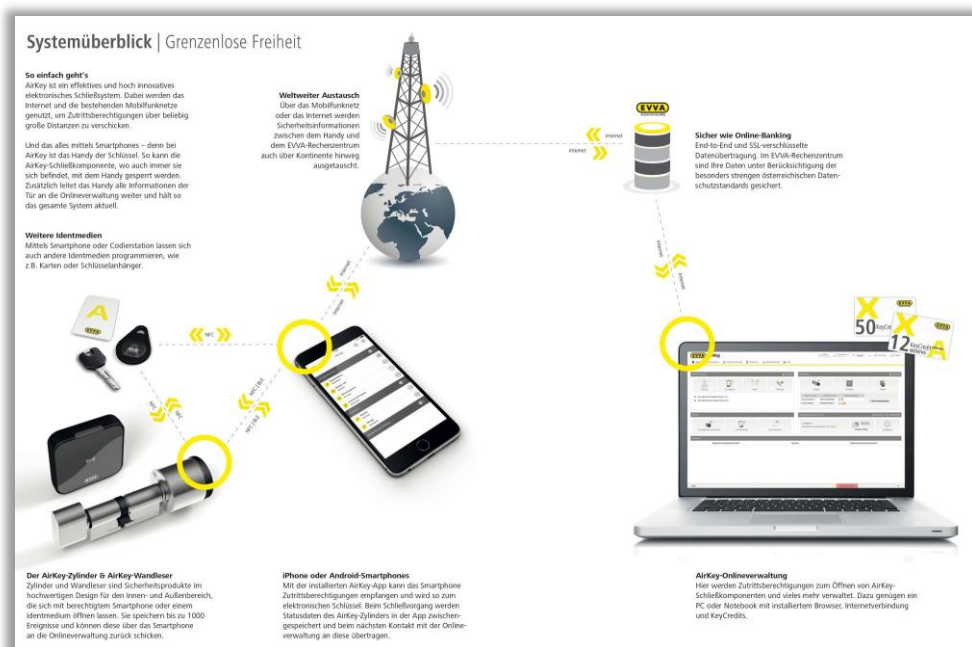


Abbildung 1: Systemarchitektur



Alle übermittelten Daten sind End-to-End, entsprechend aktuellen Verschlüsselungsstandards, vom EVVA-Rechenzentrum bis zur Schließkomponente mit einer Verschlüsselung gesichert.

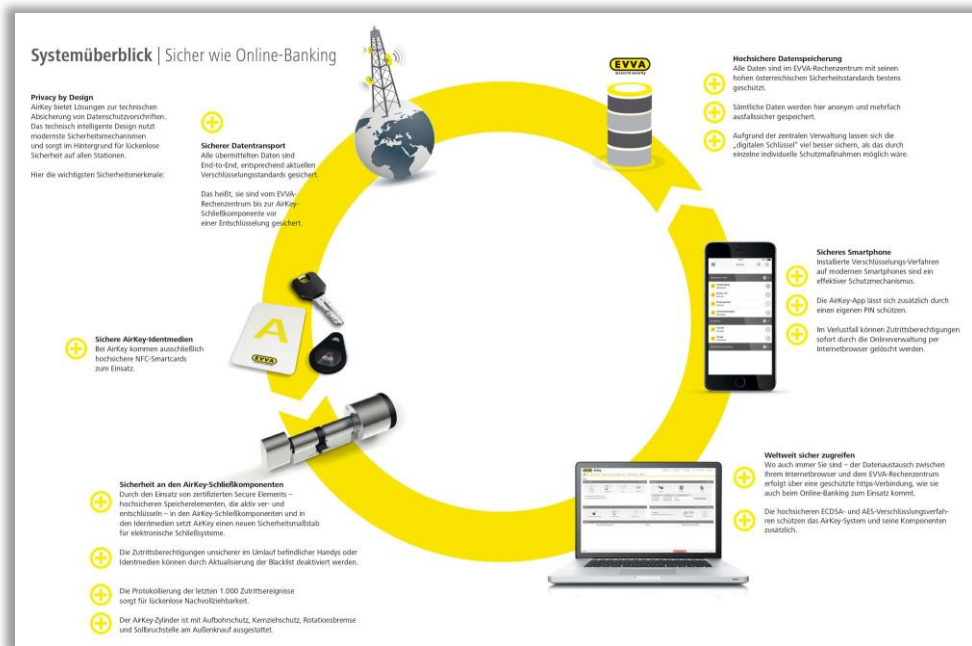


Abbildung 2: Systemüberblick – lückenlose Sicherheit

3.1 Schließkomponenten

Die Schließkomponenten regeln den Zutritt an der Türe. Je nach Berechtigung erfolgt die Freigabe oder Abweisung an der Schließkomponente.

3.1.1 AirKey-Zylinder

Der AirKey-Zylinder ist eine batteriebetriebene Schließkomponente. Diese ist sowohl für den Einsatz im Außen- als auch im Innenbereich zugelassen. In Abhängigkeit von den konkreten Anforderungen kann der AirKey-Zylinder auch in sicherheitsrelevanten Bereichen eingesetzt werden. Der AirKey-Zylinder ist mechanisch vor Vandalismus und Manipulation geschützt. Der AirKey-Zylinder ist unter Berücksichtigung der normativen Vorgaben zum Einbau in Brandschutz- und Fluchttüren* geeignet.

Der AirKey-Zylinder kann als Halb- oder Doppelzylinder ausgeführt sein. Den Doppelzylinder gibt es als Modell mit einseitigem Zutritt und als Modell mit beidseitigem Zutritt. Beim Modell mit einseitigem Zutritt erfolgt eine elektronische Berechtigungsprüfung lediglich auf der Außenseite, beim Modell mit beidseitigem Zutritt auf beiden Seiten. Der elektronische Knauf an der Identifikationsseite ist ohne Berechtigung frei drehend. Die schwarze Kunststoffkappe des AirKey-Zylinders dient als Leseinheit.

Wird ein berechtigtes Medium an den Knauf gehalten, kuppelt der Zylinder für eine begrenzte Zeitdauer ein und ermöglicht durch Drehung des elektronischen Knaufs eine Betätigung des Schlosses. Bitte beachten Sie hierzu auch die Hinweise zur [Bedienung von AirKey-Schließkomponenten](#).



Beachten Sie, dass nach dem Schließen der Türe, diese nicht automatisch verriegelt wird. Die Verriegelung der Türe muss manuell bzw. alternativ über eine entsprechende zusätzliche Einrichtung erfolgen.

Bitte prüfen Sie, ob der ausgewählte AirKey-Zylinder für die von Ihnen vorgesehene Anwendung geeignet ist. Der AirKey-Zylinder steht dazu in unterschiedlichen Bauformen und Konfigurationen zur Verfügung.

Die dafür benötigten Datenblätter sowie der Produktkatalog stehen Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.

Der AirKey-Zylinder besitzt eine optische und eine akustische Signalisierung. Die Erläuterung der verschiedenen Signale finden Sie im Kapitel [Signalisierung der Schließkomponenten](#).

Für die Montage des AirKey-Zylinders beachten Sie bitte die in der Verpackung beigelegte Montageanleitung oder das Montagevideo unter <https://www.evva.com/de/airkey/website/>.

* Für den Einsatz in Flucht- und Paniktüren kann – in Abhängigkeit vom verwendeten Einsteckschloss – die Antipanik-Funktion FAP erforderlich sein. Beachten Sie hierzu die entsprechenden Hinweise bzw. Zertifikate der Schlosshersteller sowie den Produktcode zur Bestellung.

3.1.2 AirKey-Hybridzylinder

Der AirKey-Hybridzylinder besitzt die gleichen Eigenschaften wie der AirKey-Zylinder. Er ist somit sowohl für den Einsatz im Außen- als auch im Innenbereich sowie für die Verwendung in sicherheitsrelevanten Bereichen einsetzbar.

Im Vergleich zum AirKey-Doppelzylinder mit einseitigem Zutritt, befindet sich beim AirKey-Hybridzylinder an der Innenseite, an Stelle des mechanischen Knaufs, ein Schlüsselmodul. Somit erfolgt der Zutritt von außen über eine elektronische Berechtigungsprüfung und der Zutritt von innen über einen mechanischen Schlüssel.



Beachten Sie, dass nach dem Schließen der Türe, diese nicht automatisch verriegelt wird. Die Verriegelung der Türe muss manuell bzw. alternativ über eine entsprechende zusätzliche Einrichtung erfolgen.

Bitte prüfen Sie, ob der AirKey-Hybridzylinder für die von Ihnen vorgesehene Anwendung geeignet ist.

Das dafür benötigte Datenblatt sowie der Produktkatalog steht Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.

Der AirKey-Hybridzylinder besitzt eine optische und eine akustische Signalisierung. Die Erläuterung der verschiedenen Signale finden Sie im Kapitel [Signalisierung der Schließkomponenten](#).

Für die Montage des AirKey-Hybridzylinders beachten Sie bitte die in der Verpackung beigelegte Montageanleitung.

3.1.3 AirKey-Hebelzylinder

Der AirKey-Hebelzylinder ist eine batteriebetriebene Schließkomponente für den Einsatz in Spinden, Vitrinen, diversen Behältnissen, bis hin zu Briefkästen im Außen- als auch im Innenbereich.

Der Zutritt erfolgt über eine elektronische Berechtigungsprüfung an der Außenseite. Auf der Innenseite befindet sich ein Hebel, der für die Verriegelung sorgt. Sowohl das Entriegeln als auch das Verriegeln kann erst nach erfolgreicher Berechtigungsprüfung, durch manuelles Drehen des AirKey-Hebelzylinders, erfolgen. Anders als beim AirKey-Zylinder und Hybridzylinder ist der elektronische Knauf an der Identifikationsseite ohne Berechtigung nicht frei drehend.

Bitte prüfen Sie, ob der AirKey-Hebelzylinder für die von Ihnen vorgesehene Anwendung geeignet ist. Der AirKey-Hebelzylinder steht dazu in unterschiedlichen Bauformen und Konfigurationen zur Verfügung.

Die dafür benötigten Datenblätter sowie der Produktkatalog stehen Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.

Der AirKey-Hebelzylinder besitzt eine optische und eine akustische Signalisierung. Die Erläuterung der verschiedenen Signale finden Sie im Kapitel [Signalisierung der Schließkomponenten](#).

Für die Montage des AirKey-Hebelzylinders beachten Sie bitte die in der Verpackung beigelegte Montageanleitung.

3.1.4 AirKey-Hangschloss

Das AirKey-Hangschloss ist eine batteriebetriebene Schließkomponente für den Einsatz in Schrankenanlagen, Rollläden, Depots und Archivcontainern im Außen- als auch im Innenbereich.

Der Zutritt erfolgt über eine elektronische Berechtigungsprüfung an der Unterseite. Mit einem Bügel aus gehärtetem Stahl erfolgt die Verriegelung. Sowohl das Entriegeln als auch das Verriegeln kann erst nach erfolgreicher Berechtigungsprüfung durch manuelles Drehen am elektronischen Knauf des AirKey-Hangschlosses erfolgen.

Bitte prüfen Sie, ob das AirKey-Hangschloss für die von Ihnen vorgesehene Anwendung geeignet ist. Das AirKey-Hangschloss steht dazu in unterschiedlichen Konfigurationen zur Verfügung.

Das dafür benötigte Datenblatt sowie der Produktkatalog steht Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.

Das AirKey-Hangschloss besitzt eine optische und eine akustische Signalisierung. Die Erläuterung der verschiedenen Signale finden Sie im Kapitel [Signalisierung der Schließkomponenten](#).

Für die Montage des AirKey-Hangschlosses beachten Sie bitte die in der Verpackung beigelegte Montageanleitung.

Montagewerkzeug für den AirKey-Zylinder, -Hybridzylinder, -Hebelzylinder und -Hangschloss

Der AirKey-Zylinder, der Hybridzylinder, der Hebelzylinder und das Hangschloss bieten zum Schutz gegen Manipulation einen speziellen Mechanismus. Der elektronische Knauf lässt sich nur mit einem Spezialwerkzeug abnehmen. Das für die Montage, Demontage und für den Batteriewechsel benötigte Montagewerkzeug liegt standardmäßig nicht bei und muss daher separat bestellt werden.

Den Bestellcode finden Sie im AirKey-Produktkatalog im Downloadbereich unter <https://www.evva.com/de/downloads/>.

3.1.5 AirKey-Wandleser

Der AirKey-Wandleser kann sowohl im Innen- als auch im Außenbereich, Unter- oder Aufputz sowie in sicherheitsrelevanten Bereichen eingesetzt werden.

Bitte verwenden Sie in Außen- oder Nassbereichen sowie bei Unterputzmontage die dafür vorgesehene und dem Produkt beiliegende Dichtung und beachten Sie die Hinweise Ihrer Montageanleitung.

Der AirKey-Wandler wird mit der AirKey-Steuereinheit mittels CAT5-Kabel (max. 100 m, Loop max. = 2 Ohm) verbunden und von dieser stromversorgt. Die AirKey-Steuereinheit wird mittels Netzteils stromversorgt und verfügt bei Stromausfall über eine Datenpufferung von max. 72 h, sofern die AirKey-Steuereinheit zuvor mindestens 6 Stunden in Betrieb war.



Bitte beachten Sie, dass je ein AirKey-Wandler in Verbindung mit einer AirKey-Steuereinheit verwendet werden kann.

Über die AirKey-Wandler-Steuereinheit-Kombination können elektronische Verschlusselemente wie z.B. Motorzylinder, Schwenktüren, Schiebetüren etc. angesteuert werden.



An die Steuereinheit kann auch ein externes Freigabeelement (Push-Button) angeschlossen werden. Wird dieser betätigt, öffnet sich die Türe wie bei einem Zutritt über die Leseinheit. Allerdings wird das Öffnen der Türe über das externe Freigabeelement NICHT protokolliert. Beachten Sie aus Sicherheitsgründen, dass somit der Zutritt zur AirKey-Anlage über Drittsysteme möglich ist, ohne Erstellung eines Eintrags im Zutrittsprotokoll.

Bitte prüfen Sie sorgsam, ob das ausgewählte AirKey-Produkt für die von Ihnen vorgesehene Anwendung / Montagesituation geeignet ist. Das dafür benötigte Datenblatt, der Produktkatalog und die Montageanleitung stehen Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.

3.2 AirKey-App



Die AirKey-App wird von EVVA bereitgestellt und ist im Google Play Store bzw. Apple App Store kostenlos verfügbar.



Die AirKey-App ist Voraussetzung, damit Sie mit Ihrem Smartphone AirKey-Schließkomponenten bedienen können. Zusätzlich kann Ihr Smartphone auch Schließkomponenten und Medien in eine AirKey-Anlage hinzufügen oder aktualisieren. Für die meisten Aktionen der AirKey-App ist eine aktive Internetverbindung notwendig. Ausgenommen hiervon ist die Betätigung von Schließkomponenten.



Durch eine Internetverbindung können gegebenenfalls höhere Telefonkosten anfallen. Bitte beachten Sie dazu Ihren Tarifvertrag.

3.3 Smartphones

Für die Verwendung eines Smartphones im AirKey-System sind zumindest folgende Voraussetzungen zu erfüllen:

- > NFC-fähiges bzw. Bluetooth 4.0 (Bluetooth Low Energy / BLE)-fähiges Smartphone
- > Betriebssystem:
 - Android™ ab 5.0 (nur NFC-Funktionalität möglich)
 - Android™ ab 6.0 (NFC und Bluetooth)
 - Apple™ ab iOS 10 (nur Bluetooth-Funktionalität möglich)
- > AirKey-App aus dem Google Play Store bzw. Apple App Store
- > Android-Smartphones benötigen die Berechtigung "Telefonstatus und Identität abrufen" und die Berechtigung für die Standortermittlung.



Liste der mit dem AirKey-System kompatiblen Smartphones

Bitte beachten Sie, dass die Kompatibilität eines Smartphones von vielen Faktoren abhängig ist und nicht jedes Smartphone, das die Mindestvoraussetzungen erfüllt, kompatibel sein muss. EVVA unterzieht Smartphones daher einem ausführlichen Testprozedere. Eine ständig aktuelle Liste der geprüften und für die Verwendung mit AirKey geeigneten Smartphone-Modelle finden Sie in der [Liste kompatibler Smartphones](#).



Die **Berechtigung "Telefonstatus und Identität abrufen"** ist notwendig, um das Smartphone beim Hinzufügen einer neuen Schließanlage eindeutig identifizieren zu können.

Die **Berechtigung auf den Standort ist nötig, weil Android 6+ die Aktivierung der Standortermittlung verlangt, um nach Bluetooth-Komponenten suchen zu können!** Wenn Sie in der AirKey-App Bluetooth-Funktionen verwenden möchten, müssen Sie in den Geräteeinstellungen sowohl die Funktion Standortermittlung aktivieren als auch der App die Berechtigung auf diese Funktion erteilen. Wenn Sie die Standortermittlung NICHT aktivieren möchten, können Sie eine Verbindung zu den Komponenten (Medien und Schließkomponenten) mittels NFC herstellen.



Bei **Apple-Geräten** (Betriebssystem iOS) gibt es keine Möglichkeit, die Berechtigung "Telefonstatus und Identität abrufen" zu deaktivieren. Zusätzlich kann iOS auch ohne die Berechtigung für die Standortermittlung nach Bluetooth-Komponenten suchen.

3.4 AirKey-Medien

Als Medien stehen derzeit geprüfte Smartphone-Modelle sowie Karten, Schlüsselanhänger, Kombischlüssel und Armbänder in verschiedenen Konfigurationen, wie zum Beispiel in Kombination mit der Technologie *Mifare DESFire EV1* zur Verfügung.

Die entsprechenden Datenblätter sowie der Produktkatalog stehen Ihnen auf unserer Homepage im Downloadbereich zur Verfügung: <https://www.evva.com/de/downloads/>.



Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder werden im Auslieferungszustand geliefert. Um diese in Ihrer AirKey-Schließanlage verwenden zu können, müssen Sie diese zuerst zur Anlage hinzufü-

gen.

3.5 AirKey-Onlineverwaltung

Die AirKey-Onlineverwaltung ist die von EVVA bereitgestellte Online-Software zur Administration und Verwaltung der AirKey-Schließanlage. Das elektronische Schließsystem AirKey funktioniert mit allen gängigen Internetbrowsern sowie Betriebssystemen und erfordert keine spezielle IT-Infrastruktur. Laufender Betrieb und Wartung des AirKey-Rechenzentrums werden durch EVVA übernommen.

3.5.1 Systemvoraussetzungen

- > Betriebssysteme: Windows 10 (oder höher), MacOS 10.15 (oder höher), Linux
- > Derzeit werden folgende Browser unterstützt: Chrome, Firefox, Edge, Safari
- > JavaScript im Browser aktiviert
- > Internetverbindung (1 MBit/s oder schneller)
- > Optional: USB-Port 2.0 für Codierstation
- > Der Internet-Port 443 muss erreichbar sein.



Für die Registrierung einer AirKey-Schließanlage benötigen Sie eine gültige E-Mail-Adresse.

3.6 EVVA-KeyCredits

Für den laufenden Betrieb einer AirKey-Schließanlage sind zur Vergabe bzw. Änderung von Zutrittsberechtigungen KeyCredits erforderlich. KeyCredits stehen als Mengenguthaben (definierte Anzahl an möglichen Berechtigungsänderungen innerhalb eines unbegrenzten Zeitraums) oder als Zeitguthaben (unbeschränkte Anzahl an möglichen Berechtigungsänderungen in einem definierten Zeitraum) zur Verfügung. Abhängig von der Größe und der Dynamik Ihres AirKey-Systems gibt es für jedes Einsatzgebiet das passende KeyCredit-Paket, das Sie bei Ihrem EVVA-Fachhändler erhalten. Weitere Details zu den verfügbaren Paketen finden Sie im AirKey-Produktkatalog unter <https://www.evva.com/de/downloads/>.

3.7 Codierstation

Mit der optionalen Codierstation können AirKey-Schließkomponenten und -Medien in eine AirKey-Schließanlage hinzugefügt oder aktualisiert werden, so wie mit einem Smartphone mit Wartungsberechtigung. Die Codierstation kann über eine eigene Applikation aktiviert werden. Die zu installierende Codierstation-Applikation bietet den Vorteil, dass sie mit aktuellen Browsern kompatibel ist und dass die Codierstation auch nach Abmeldung aus der AirKey-Onlineverwaltung bzw. wenn der Browser beendet wurde, für die Aktualisierung von Schließkomponenten und Medien verwendet werden kann.

Folgende Browser werden unterstützt: Chrome, Firefox und Edge.

Systemvoraussetzungen:

- > USB-Port

- > Java 7 oder höher
- > Treiber für Codierstation

Nähere Informationen dazu finden Sie im Kapitel [Codierstation installieren](#).

3.8 Notstromgerät

Auf allen Schließkomponenten befindet sich an der Stirnseite der Schließkomponente, unterhalb des EVVA-Logos, eine Schnittstelle. Diese erreichen Sie, indem Sie beim Logo auf der linken Seite des Schriftzugs (beim Buchstaben E) leicht nach innen drücken und auf der rechten Seite (beim Buchstaben A) aufklappen. Die eingebaute Schnittstelle dient nur zur Notstromversorgung und wird im Normalbetrieb nicht benötigt.

Das Notstromgerät versorgt die Schließkomponente mit Strom, damit diese im Falle von leeren Batterien bedient werden kann. Schließen Sie hierzu das Verbindungskabel des Notstromgeräts an die entsprechende Schnittstelle an und schalten Sie es anschließend ein. Eine weitere Interaktion am Notstromgerät selbst ist nicht erforderlich. Zur Bedienung der AirKey-Schließkomponente selbst wird weiterhin ein Medium mit gültiger Berechtigung benötigt.

Bitte beachten Sie hierbei, dass das eine Dauerberechtigung ohne eingeschränkten Gültigkeitszeitraum sein muss. Nähere Informationen dazu finden Sie im Kapitel [Notmedien](#). Tauschen Sie nach einer Notstromöffnung sofort die Batterien der Schließkomponente und aktualisieren Sie anschließend die Schließkomponente, um den Zutritt auch mit weiteren Medien wieder zu ermöglichen. Weitere Informationen zur Notstromöffnung finden Sie auch unter [Batteriewechsel und Notstromöffnung](#).



Beachten Sie, dass der AirKey-Wandleser nicht über das Notstromgerät mit Strom versorgt werden kann, da dieser über eine externe Spannungsversorgung in Kombination mit der AirKey-Steuereinheit versorgt wird.

4 Inbetriebnahme

In diesem Kapitel werden die ersten Schritte für eine Inbetriebnahme des AirKey-Systems beschrieben.



Auf der Webseite <https://www.evva.com/de/airkey/website/> finden Sie auch einen Screencast, der die ersten Schritte und die Inbetriebnahme des AirKey-Systems beschreibt.

Für die Unterstützung der Montage von Schließkomponenten bietet EVVA folgendes Material an:


- > **Montageanleitung:**
Als Unterstützung zum Einbau der Schließkomponenten stellt EVVA sprachneutrale Montageanleitungen zur Verfügung. Diese finden Sie in der Verpackung des jeweiligen Produkts bzw. auf der Webseite <https://www.evva.com/de/downloads/>.
- > **Videos:**
Auf der Webseite <https://www.evva.com/de/airkey/website/> stehen Montagevideos bereit.

4.1 AirKey-App installieren

- > Laden Sie die AirKey-App aus dem Google Play Store bzw. Apple App Store.
- > Folgen Sie den Anweisungen zum Installieren der AirKey-App auf dem Smartphone.

4.2 In der AirKey-Onlineverwaltung registrieren

Um die AirKey-Onlineverwaltung zu nutzen, müssen Sie sich bei EVVA mit einer gültigen E-Mail-Adresse registrieren.

- > Wählen Sie in Ihrem Browser die Webseite <https://airkey.evva.com>.
Es öffnet sich die Login-Seite der AirKey-Onlineverwaltung.
- > Wählen Sie die von Ihnen bevorzugte **Sprache**.
- > Klicken Sie auf den Link **AirKey-Registrierung** .

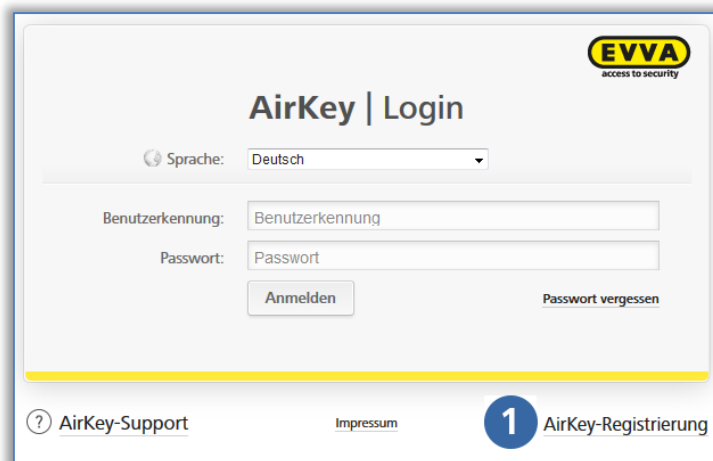


Abbildung 3: Link "AirKey-Registrierung"

In der Registrierungsmaske füllen Sie die Felder aus und registrieren Sie sich bei AirKey.

- > Wählen Sie **Firmenkunde** oder **Privatkunde**.
- > Füllen Sie die Formularfelder aus.
Felder, die mit * gekennzeichnet sind, sind Pflichtfelder.
- > Lösen Sie das Captcha. ①
- > Aktivieren Sie die Checkbox mit dem Link [Allgemeine Geschäftsbedingungen \(EVVA-AGB\)](#) und die Checkbox mit dem Link [Allgemeine Lizenzbedingungen \(EVVA-ALB\)](#) ②. Die zwei entsprechenden PDF-Dokumente werden automatisch geöffnet. Diese Dokumente sind auch unter <https://www.evva.com/de/airkey/impressum/> abrufbar.

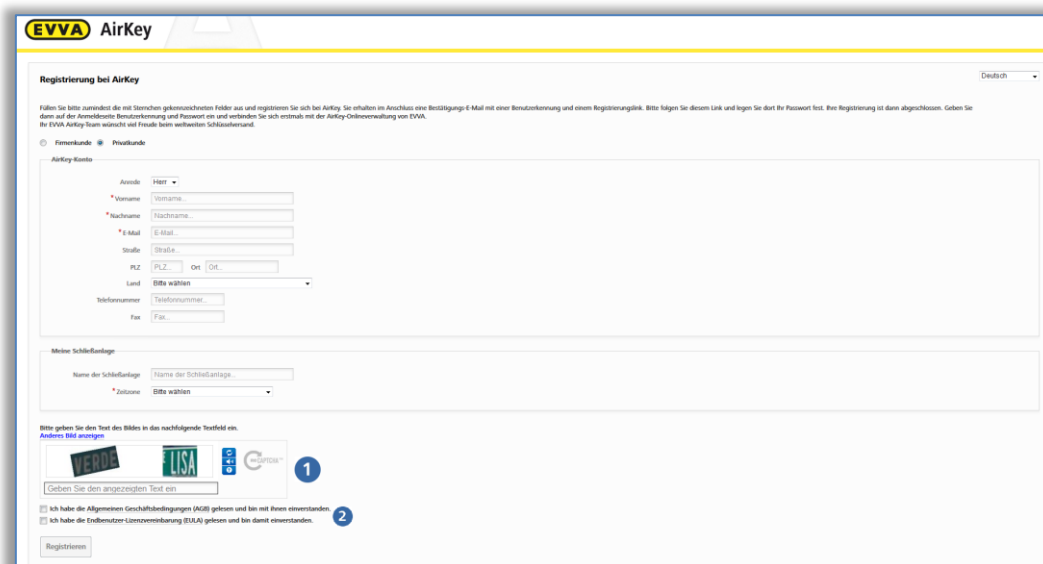


Abbildung 4: Registrierung bei AirKey



Sie können nachträglich bei Bedarf jederzeit die Kundendaten ändern. Dazu klicken Sie in der AirKey-Onlineverwaltung im Hauptmenü auf **Schließanlage** → **Kundendaten**.

- > Klicken Sie auf **Registrieren**. Es öffnet sich das Dialogfenster "Registrierung abschließen".
- > Prüfen Sie nochmals die angegebene E-Mail-Adresse, an diese wird die Bestätigung mit einem Registrierungslink gesendet.
- > Wenn die angezeigte E-Mail-Adresse falsch ist, brechen Sie den Vorgang mit **Abbrechen** ab und korrigieren Sie die Eingabe.
- > Ist die E-Mail-Adresse korrekt, beenden Sie den Vorgang mit **Registrierung abschließen**.

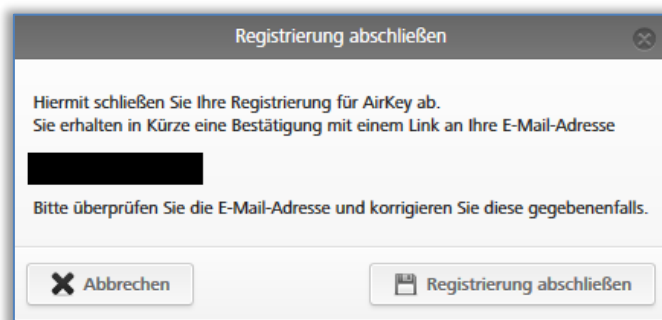


Abbildung 5: Registrierung abschließen

Es wird vom AirKey-System automatisch eine Benutzererkennung und ein Registrierungslink generiert und als Registrierungsmail an die von Ihnen angegebene E-Mail-Adresse gesendet.

- > Öffnen Sie Ihr E-Mail-Programm, dort finden Sie die E-Mail von EVVA mit dem Betreff "EVVA-AirKey-Registrierung".
- > Öffnen Sie die E-Mail und klicken Sie auf den Registrierungslink 1.



Heben Sie diese E-Mail auf. Im Supportfall benötigen Sie die darin enthaltene eindeutige Benutzererkennung und Ihre Kundennummer.

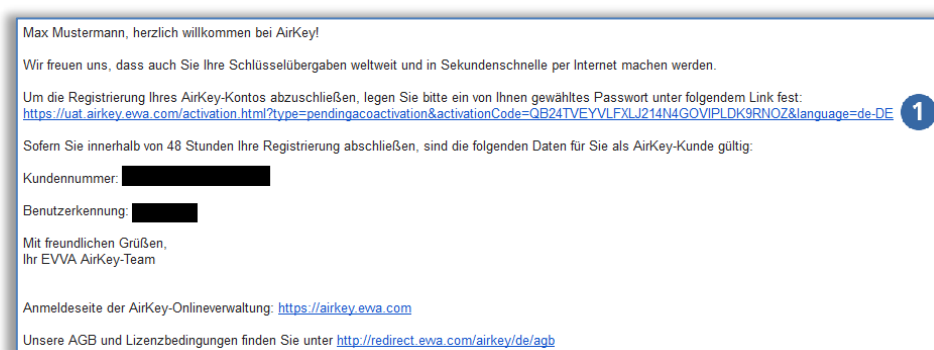


Abbildung 6: E-Mail "EVVA-AirKey-Registrierung"



Der Registrierungslink in der E-Mail ist nur 48 Stunden lang gültig.

Wenn ein abgelaufener oder ungültiger Registrierungslink aufgerufen wird, wird die Webseite "Ungültiger Registrierungslink" angezeigt. In diesem Fall müssen Sie sich erneut registrieren.


Nachdem Sie auf den Registrierungslink geklickt haben, öffnet sich im Browser die AirKey-Willkommenseite, in der Sie Ihre Registrierung abschließen können.

- > Geben Sie ein selbst gewähltes Passwort für die AirKey-Onlineverwaltung ein. Das Passwort muss mindestens 6 Zeichen lang sein, eine Ziffer und einen Groß- und einen Kleinbuchstaben enthalten, andernfalls erhalten Sie eine Fehlermeldung.
- > Wiederholen Sie die Passwordeingabe.
- > Geben Sie Ihr Geburtsdatum ein. Dieses wird als Sicherheitsabfrage verwendet, wenn Sie Ihr Passwort vergessen haben.



Aus Sicherheitsgründen empfehlen wir Ihnen, ein möglichst langes AirKey-Passwort zu wählen und dieses geheim zu halten.

Abbildung 7: Eigenes AirKey-Passwort festlegen, um die Registrierung abzuschließen

- > Wenn die Pflichtfelder ausgefüllt sind und die beiden AirKey-Passwörter übereinstimmen, schließen Sie die Registrierung mit **Speichern**  ab.

Sie haben nun den Registrierungsprozess abgeschlossen und Ihre AirKey-Schließanlage erfolgreich aktiviert.

Ab nun können Sie sich über die Login-Seite der AirKey-Onlineverwaltung jederzeit anmelden. Sie benötigen dafür nur die Benutzerkennung aus der Registrierungsmail und das zuvor festgelegte AirKey-Passwort.

4.3 Anmelden

Die Anmeldung ist erforderlich, um die AirKey-Schließanlage zu konfigurieren bzw. zu verwalten.

- > Wählen Sie in Ihrem Browser die Webseite <https://airkey.evva.com>. Es öffnet sich die Login-Seite der AirKey-Onlineverwaltung.
- > Wählen Sie die von Ihnen bevorzugte **Sprache**. Sie können in der aktiven Sitzung jederzeit rechts in der Menüleiste die Sprache ändern.
- > Tragen Sie Ihre Benutzerkennung aus der Registrierungsmail und das festgelegte Passwort ein und bestätigen Sie mit **Anmelden**. Es öffnet sich die Startseite Ihrer

AirKey-Schließanlage.

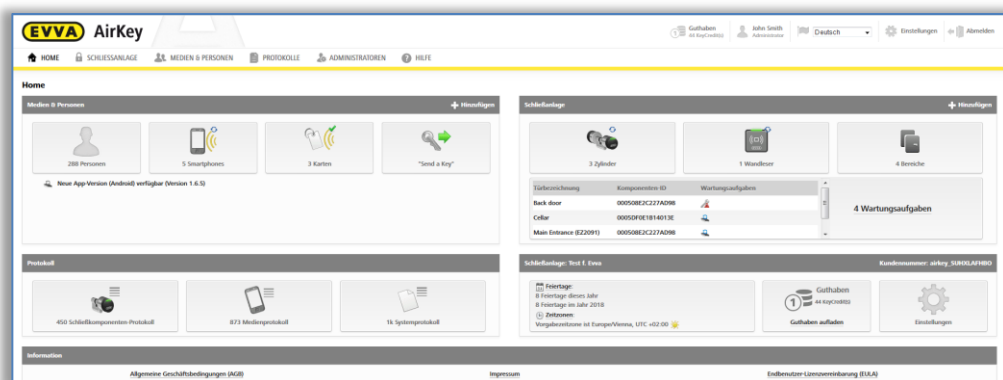


Abbildung 8: Startseite der AirKey-Schließanlage

Auf der Startseite werden alle anlagenrelevanten Daten im Überblick angezeigt. Von hier können Sie zu allen Funktionen und Einstellungen navigieren.

4.4 Interaktive Hilfe

In der AirKey-Onlineverwaltung startet nach dem ersten Login die interaktive Hilfe, die Sie durch das Programm führt und die wichtigsten Funktionen erklärt.

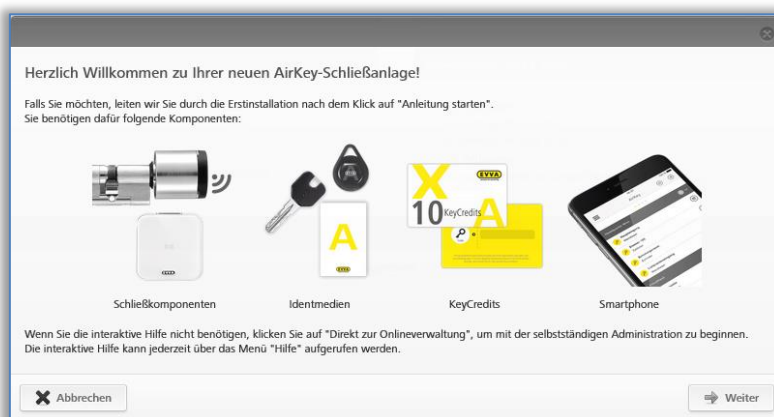


Abbildung 9: Interaktive Hilfe

Als Beispiel wird hier die Funktion "Guthaben aufladen" angezeigt. Die interaktive Hilfe zeigt Ihnen, welche Buttons Sie anklicken müssen und gibt Ihnen Hinweise, welche Informationen Sie in Felder eintragen müssen. Innerhalb der interaktiven Hilfe können Sie auch vor und zurück navigieren.

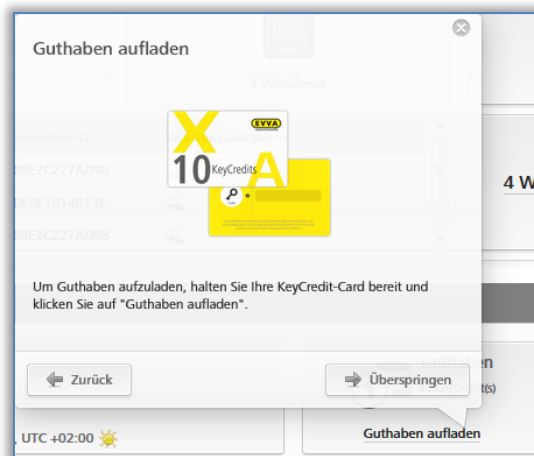


Abbildung 10: Interaktive Hilfe – Guthaben aufladen

Sie können die interaktive Hilfe auch schließen und die AirKey-Onlineverwaltung mithilfe des Systemhandbuchs kennenlernen.



Wenn Sie die interaktive Hilfe geschlossen haben und erneut aufrufen möchten, dann wählen Sie im Hauptmenü **Hilfe** → **Interaktive Hilfe**. Damit können Sie die interaktive Hilfe jederzeit neu starten, so oft Sie möchten.

4.5 Codierstation installieren

Option

Eine AirKey-Codierstation kann optional dazu verwendet, um Schließkomponenten und Medien zu einer AirKey-Schließanlage hinzuzufügen oder sie zu aktualisieren.

Für die Verwendung einer Codierstation im AirKey-System ist es erforderlich, eine Codierstation-Applikation zu installieren.

Es gibt zwei Möglichkeiten, die Codierstation zu verwenden:

- im Browser, über die AirKey-Onlineverwaltung
- ohne Browser, über die Kommandozeile

4.5.1 Codierstation über die AirKey-Onlineverwaltung verwenden

Die zu installierende Applikation für die Codierstation bietet den Vorteil, dass sie mit aktuellen Browsern kompatibel ist und dass die Codierstation auch nach Abmeldung aus der AirKey-Onlineverwaltung bzw. wenn der Browser beendet wurde, für die Aktualisierung von Schließkomponenten und Medien verwendet werden kann.

Das Hinzufügen und Entfernen von Schließkomponenten zu einer Schließanlage sowie das Firmware-Update von Schließkomponenten bzw. das Keyring-Update von Zutrittsmedien ist nur nach Anmeldung in der AirKey-Onlineverwaltung möglich.

Folgende Browser unterstützen die Kommunikation zwischen der AirKey-Onlineverwaltung und der Codierstation-Applikation: Chrome, Firefox und Edge.

Der Download und das Ausführen der Codierstation-Applikation sind browser- und betriebs-systemspezifisch. Die Darstellung in Ihrem Browser kann sich von der hier gezeigten (für Firefox) unterscheiden.

Registrieren Sie sich und loggen Sie sich bei der AirKey-Onlineverwaltung ein (siehe Kapitel [In der AirKey-Onlineverwaltung registrieren](#)).

- > Schließen Sie die Codierstation an eine USB-Schnittstelle Ihres Computers an.
- > Klicken Sie in der AirKey-Onlineverwaltung auf das **+**-Symbol rechts unten **1**.

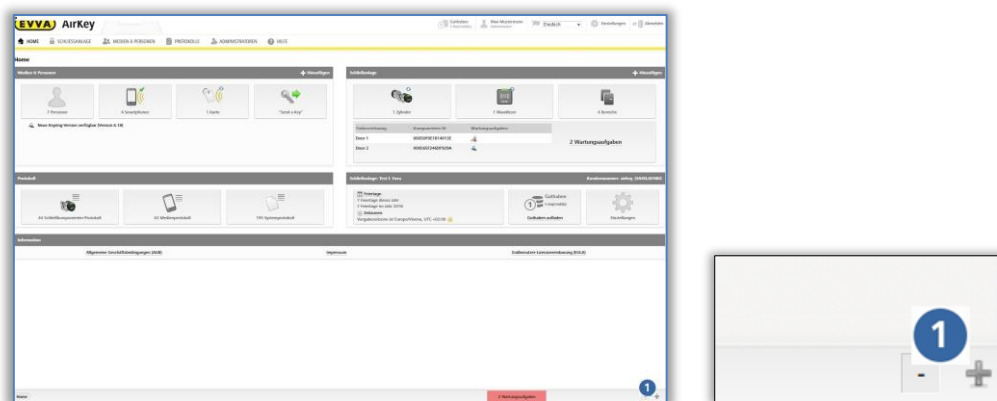


Abbildung 11: Codierstation – Installation der Applikation

Um die Codierstation-Applikation zu installieren, klicken Sie anschließend auf den Link "Codierstation-Applikation installieren und starten" **1**.

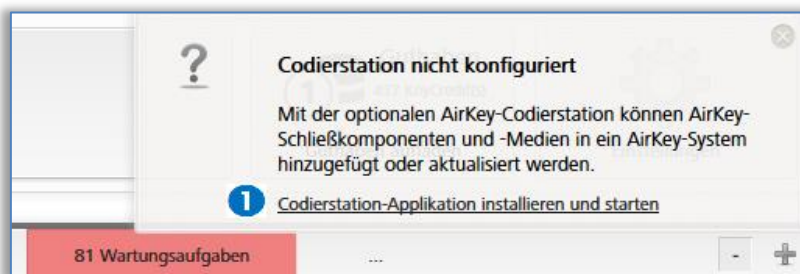


Abbildung 12: Codierstation-Applikation installieren und starten



Nach dem Klick auf den Link haben Sie 60 Sekunden Zeit, um die AirKey.jnlp-Datei zu öffnen (siehe nächsten Schritt). Bei Zeitüberschreitung muss die Installation ab dem aktuellen Schritt wiederholt werden. Alternativ können Sie die AirKey.jnlp-Datei auch speichern und manuell öffnen.

- > Es erscheint der Download-Dialog der AirKey.jnlp-Datei. Öffnen Sie diese mit dem "Java(TM) Web Start Launcher".

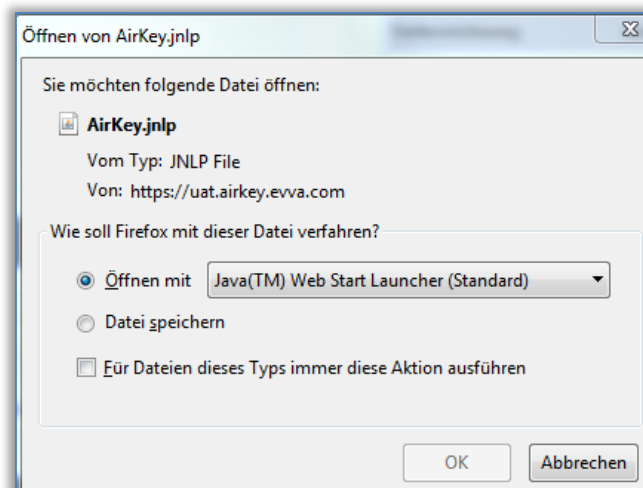


Abbildung 13: Öffnen der AirKey.jnlp-Datei

- > Nach dem Öffnen der Datei wird die Verbindung zur Codierstation aufgebaut.



Abbildung 14: Verbindung zur Codierstation aufbauen

- > Vorhandene Codierstation (z.B. "OMNIKEY CardMan 5x21-CL 0" ⓘ) aus der Liste auswählen.

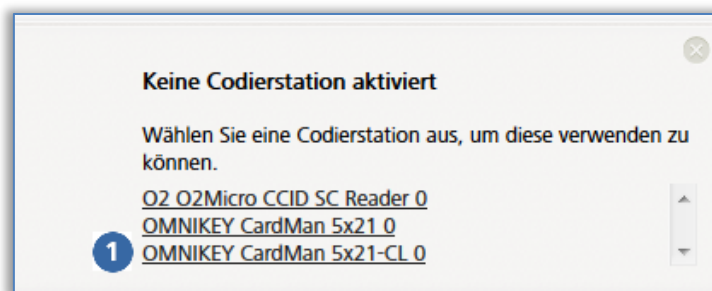


Abbildung 15: Auswahl der Codierstation

- > In der Taskleiste rechts unten erscheint das AirKey-Icon – die Codierstation ist erfolgreich installiert und aktiv.

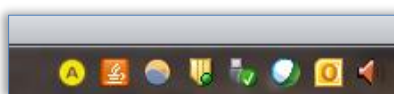


Abbildung 16: AirKey-Icon in der Taskleiste

4.5.2 Codierstation über die Kommandozeile verwenden

Die Codierstation-Applikation kann auch ohne die AirKey-Onlineverwaltung, zum Beispiel über die Kommandozeile, installiert und konfiguriert werden. (Für diese Option sind erweiterte IT-Kenntnisse, vor allem das Arbeiten über die Kommandozeile, notwendig.)

Über die Kommandozeile kann die Codierstation nur zum Aktualisieren von Zutrittsmedien und Schließkomponenten verwendet werden. Ein Firmware-Update der Schließkomponenten ist nur über Browser oder mit einem Smartphone mit Wartungsberechtigung möglich.

- > Speichern Sie die Codierstation-Applikation über den Link <https://airkey.evva.com/smkrest/jnlp/newest-jar-file/> im gewünschten Verzeichnis ab.

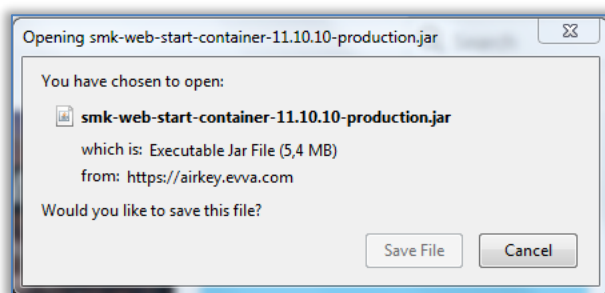


Abbildung 17: Download der Codierstation-Applikation

- > Öffnen Sie die Kommandozeile und navigieren Sie in das Verzeichnis, wo die Codierstation-Applikation zuvor abgelegt wurde.
- > Starten Sie die Codierstation-Applikation mit folgendem Befehl:

```
java -jar <Dateiname>
(z.B. web-start-container-customer-15.10.0-8.jar)
```

Zusätzlich können Sie folgende optionale Parameter angeben:

- **-reader "<Name der Codierstation>":** Mit diesem Parameter kann eine bestimmte Codierstation (z.B. "HID Global OMNIKEY 5022 Smart Card Reader 0") verwendet werden. In diesem Fall wird die Konfigurationsdatei `config_customer.json` ignoriert.
- **-port <WERT [1024-65535]>:** Wenn dieser Parameter nicht angegeben wird, wird standardmäßig der Port 50743 verwendet. Der Port 50743 wird auch verwendet, wenn die Codierstation über die AirKey-Onlineverwaltung im Browser verwendet wird. Wenn Sie mehrere Codierstationen auf einem Computer parallel verwenden möchten, müssen Sie für jede Codierstation einen eigenen Port angeben. Mit dem Parameter **"-port 0"** wird ein zufälliger Port verwendet.
- **-configDir <WERT>:** Im angegebenen Ordner (Standardwert für Windows: `%USERPROFILE%\airkey`) wird die Konfigurationsdatei `config_customer.json` gespeichert. Diese wird beim ersten Start der Codierstation-Applikation automatisch generiert und speichert die zuletzt verwendeten Einstellungen.
- **-workDir <WERT>:** Im angegebenen Ordner wird z.B. die Logdatei `logs\application.log` erstellt, wenn die Codierstation-Applikation gestartet wird. Darin werden alle Aktionen protokolliert, die mit der Codierstation-Applikation durchgeführt wurden. Wenn Sie mehrere Codierstationen parallel

verwenden, ist es sinnvoll, für jede Codierstation einen eigenen Ordner zu verwenden.

- **-notify <Dateiname>**: Definiert eine ausführbare Datei oder ein Skript, das die lockingSystemID als Hex-String (argument1) oder als long-int (argument2) eines auf der Codierstation erfolgreich aktualisierten Zutrittsmediums an ein Drittsystem weiterleiten kann. Dieser Parameter ist hauptsächlich für die Integration von AirKey in Drittsysteme und der Verwendung des AirKey Cloud Interface relevant. Dort kann die lockingSystemId des Zutrittsmediums dann ausgewertet und weiterverarbeitet werden. Zum Beispiel, um die Person herauszufinden, der das Zutrittsmedium gehört. Details zum AirKey Cloud Interface finden Sie im Kapitel [AirKey Cloud Interface \(API\)](#).
- **-version**: Zeigt die Version der Codierstation-Applikation an.
- **-help**: Öffnet die Hilfe und beschreibt alle möglichen Parameter.

- › In der Taskleiste rechts unten erscheint das AirKey-Icon und in der Kommandozeile werden Informationen über das Konfigurationsverzeichnis , das Arbeitsverzeichnis und die verfügbaren Codierstationen angezeigt.

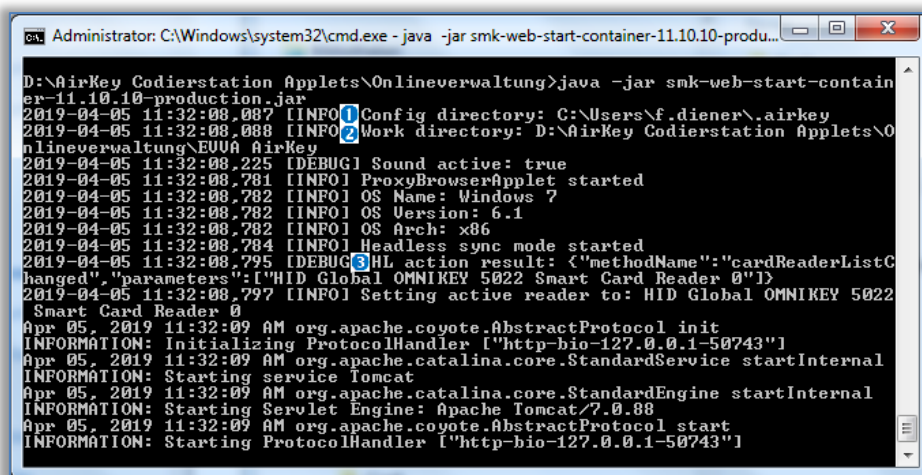


Abbildung 18: Codierstation-Applikation über die Kommandozeile starten

4.5.3 Einstellungen der Codierstation-Applikation

Durch einen Rechtsklick auf das AirKey-Icon öffnet sich das entsprechende Kontextmenü.

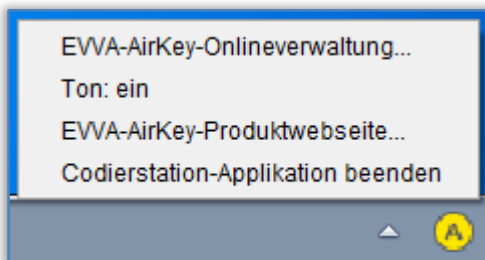


Abbildung 19: Einstellungen der Codierstation-Applikation

Liste der entsprechenden Menüpunkte:

- > **EVVA-AirKey-Onlineverwaltung...** – Link zur Login-Seite der AirKey-Onlineverwaltung
- > **Ton: ein** – es wird ein Hinweiston ausgegeben, nachdem eine Komponente mit der Codierstation aktualisiert wurde. Sinnvoll als akustische Rückmeldung, wenn die Codierstation ohne AirKey-Onlineverwaltung verwendet wird. Bei Klick auf **Ton: ein** wird auf **Ton: aus** gewechselt.
- > **Ton: aus** – es wird kein Hinweiston ausgegeben. Bei Klick auf **Ton: aus** wird auf **Ton: ein** gewechselt.
- > **EVVA-AirKey-Produktwebseite...** – Link zur [AirKey-Produktwebseite](#)
- > **Codierstation-Applikation beenden** – beendet die Codierstation-Applikation.

4.5.4 Lösungen für mögliche Probleme mit der Codierstation

Wenn die Codierstation angeschlossen ist, signalisiert die Leuchtdiode die Betriebsbereitschaft. Wenn die Betriebsbereitschaft nicht signalisiert wird, stecken Sie die Codierstation ab und anschließend wieder an. Installieren Sie gegebenenfalls den Treiber der Codierstation erneut.



Beim Herunterfahren des Computers wird die Codierstation-Applikation automatisch beendet. Für ein automatisches Starten der Applikation beim Neustart des Computers können Sie die heruntergeladene AirKey.jnlp-Datei im Autostart-Ordner ablegen.

Die Codierstation-Applikation beendet sich nach dem Start

Die Codierstation-Applikation verwendet standardmäßig den Port 50743 für die Kommunikation mit dem Browser. Wenn dieser Port von einem anderen Programm verwendet wird, kann die Codierstation-Applikation nicht gestartet werden. Unter Windows 10 oder höher kann dieser Port von Hyper-V verwendet werden. Sie können wie folgt verhindern, dass Hyper-V diesen Port verwendet:

- > Deaktivieren Sie Hyper-V:
`C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V`
- > Starten Sie den Computer neu.
- > Fügen Sie eine Ausnahme für den Port 50743 hinzu:
`C:\> netsh int ipv4 add excludedportrange protocol=tcp startport=50743
 numberofports=1`
- > Reaktivieren Hyper-V:
`C:\> dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All`
- > Starten Sie den Computer neu.

Als Codierstation ist der Kartenleser "Microsoft UICC" ausgewählt



Abbildung 20: Kartenleser "Microsoft UICC" in der AirKey-Onlineverwaltung

Als Lösung kann dieser Kartenleser im Geräte-Manager von Windows deaktiviert werden:
Geräte-Manager → Softwaregeräte → Microsoft UICC ISO Reader → Gerät deaktivieren

Die Verbindung zur Codierstation kann über die AirKey-Onlineverwaltung nicht hergestellt werden (https-Proxy)

Sowohl die AirKey-Onlineverwaltung als auch die Codierstation-Applikation kommunizieren verschlüsselt über den Port 443 mit dem AirKey-System. In Netzwerken, die einen https-Proxy verwenden, kann es aber notwendig sein, eine Ausnahme für "airkey.evva.com" und Subdomains zu definieren, weil die Codierstation-Applikation das Serverzertifikat mittels "certificate pinning" überprüft und damit keine https-Proxies zulässt.

Die Verbindung zur Codierstation kann über die AirKey-Onlineverwaltung nicht hergestellt werden (DNS-Rebinding-Schutz)

Die AirKey-Onlineverwaltung kommuniziert lokal zwischen Browser und der Codierstation-Applikation. Aktionen wie das Auflegen von Schließkomponenten oder Zutrittsmedien auf die Codierstation werden dann in der AirKey-Onlineverwaltung angezeigt.

Der Browser verbindet sich zu der Codierstation-Applikation über "components.airkey.evva.com" (Port 50743). Diese URL wird vom DNS-Server als 127.0.0.1 aufgelöst.

Deswegen kann es notwendig sein, bei aktivem DNS-Rebind-Schutz Ausnahmen für "components.airkey.evva.com" und Subdomains von "airkey.evva.com" hinzuzufügen.

Windows sucht wiederholt nach dem Treiber für die Codierstation

Beim Auflegen einer Schließkomponente oder eines Zutrittsmediums auf die Codierstation versucht Windows, einen Treiber für die Codierstation zu suchen und installieren. Das kann die Kommunikation mit der Codierstation beeinflussen und zu Fehlfunktionen führen.

Als Lösung kann der Smartcard-Plug & Play-Dienst von Windows deaktiviert werden:

- > Windows-Taste + R
- > Tippen Sie "gpedit.msc" ein und bestätigen Sie mit **Enter**.
- > Programm "Editor für lokale Gruppenrichtlinien" → Computerkonfiguration → Administrative Vorlagen → Windows-Komponenten → Smartcard
- > Klicken Sie doppelt die Zeile mit dem Eintrag "Smartcard-Plug & Play-Dienst" auf der rechten Seite.

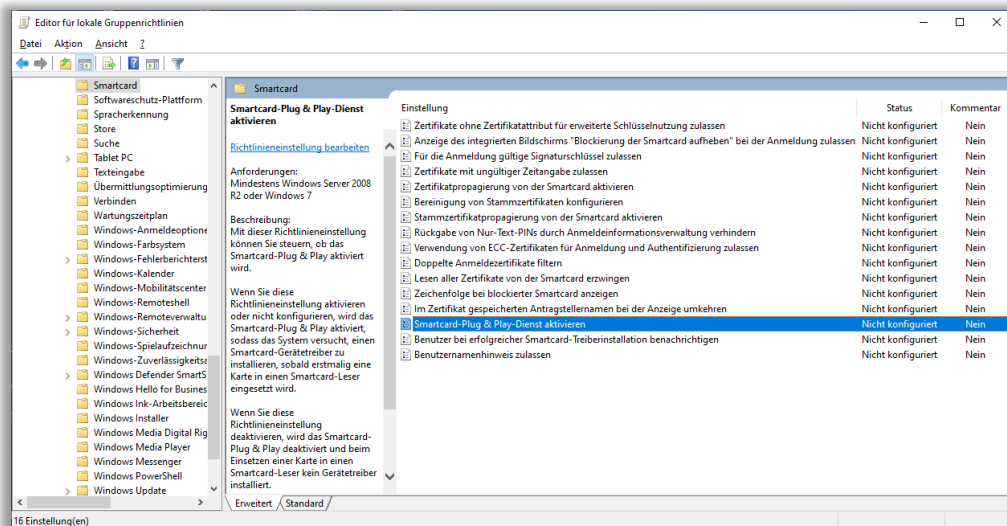


Abbildung 21: Editor für lokale Gruppenrichtlinien

- > Wählen Sie den Radiobutton **Deaktiviert**.
- > Bestätigen Sie mit **OK**.

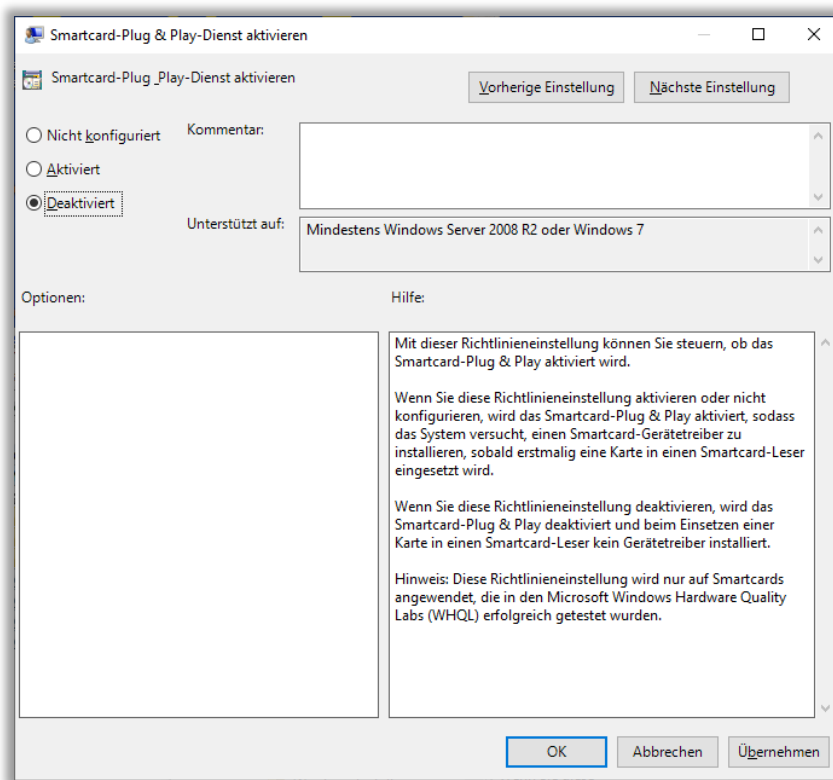


Abbildung 22: Smartcard-Plug & Play-Dienst

Bei MacOS 11.x oder höher kann keine Codierstation ausgewählt werden

Seit MacOS Big Sur (11.x) ist es auf einem Mac nicht mehr möglich, über die AirKey-Onlineverwaltung eine angeschlossene Codierstation auszuwählen. Die Codierstation-Applikation kann zwar erfolgreich gestartet werden, aber in der AirKey-Onlineverwaltung wird keine Codierstation angezeigt.

Als Lösung kann die Codierstation über die Kommandozeile gestartet werden (siehe Kapitel [Codierstation über die Kommandozeile verwenden](#)). Eine Voraussetzung dafür ist allerdings, dass die Java-Version JDK17 (Oracle JDK17 oder OpenJDK17) oder höher installiert ist.

4.6 Guthaben aufladen

Es ist eine KeyCredit-Card notwendig, auf deren Rückseite sich unter dem Rubbelfeld ein Guthabencode befindet.

- > Klicken Sie auf der Startseite **Home** die Kachel **Guthaben aufladen** 1.
- > Alternativ können Sie auf **Guthaben** in der Kopfzeile klicken.

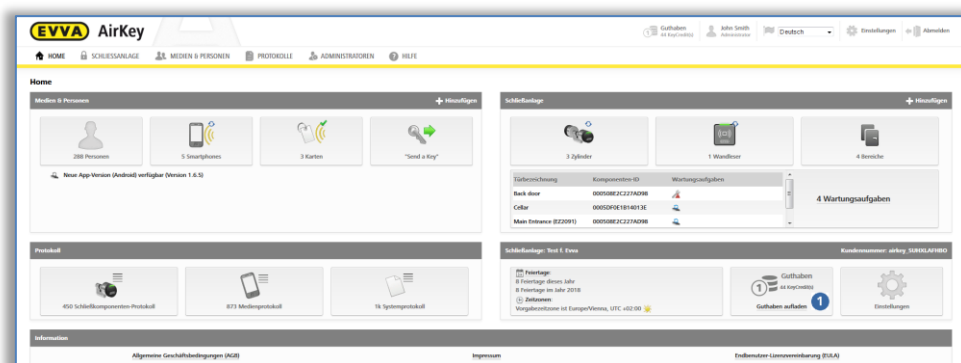


Abbildung 23: Guthaben

- > Sie erhalten eine Übersicht über Ihr aktuelles Guthaben und die bereits getätigten Aufladungen.
- > Klicken Sie auf die Schaltfläche **Guthaben aufladen** 1.

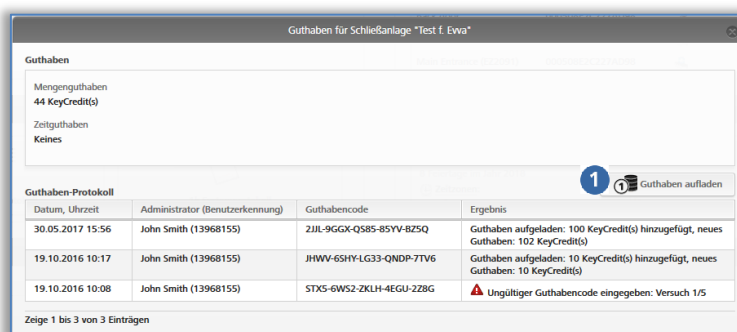


Abbildung 24: Guthaben aufladen

- > Geben Sie im Dialogfenster "Guthaben aufladen" den Code ein, den Sie auf der KeyCredit-Card aufgerubbelt haben.

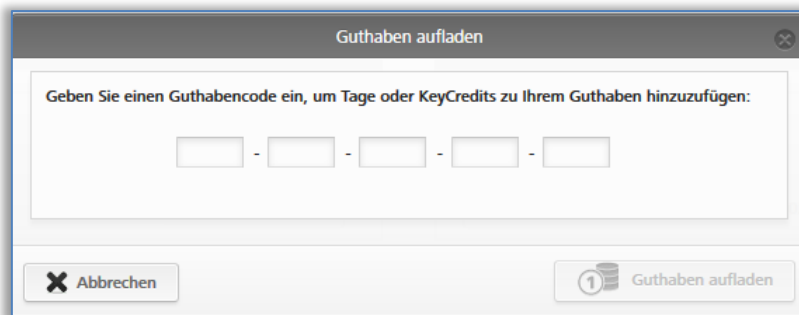


Abbildung 25: Guthabencode eingeben

- > Klicken Sie auf **Guthaben aufladen**.

Wenn Sie den Code korrekt eingegeben haben, wird die Eingabe bestätigt und das Guthaben gebucht.

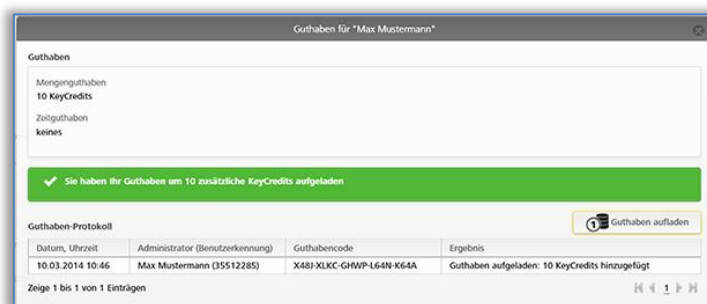



Abbildung 26: Guthaben aufladen

4.7 Person anlegen

Jede Person, die für die AirKey-Schließanlage eine Berechtigung erhalten soll, muss zuvor angelegt werden.

- > Klicken Sie auf der Startseite **Home** im grauen Balken des Blocks **Medien & Personen** auf **Hinzufügen** → **Person anlegen**.
- > Oder wählen Sie auf der Startseite **Home** die Kachel **Personen** → **Person anlegen**.
- > Oder wählen Sie im Hauptmenü **Medien & Personen** → **Person anlegen**.
- > Oder wählen Sie die Schaltfläche **"Send a Key"** und klicken Sie auf **Neu anlegen**. Hier kann eine Person mit einem Smartphone angelegt werden.
- > Füllen Sie die Formularfelder aus. Felder, die mit * gekennzeichnet sind, sind Pflichtfelder.
- > Klicken Sie auf **Speichern** .

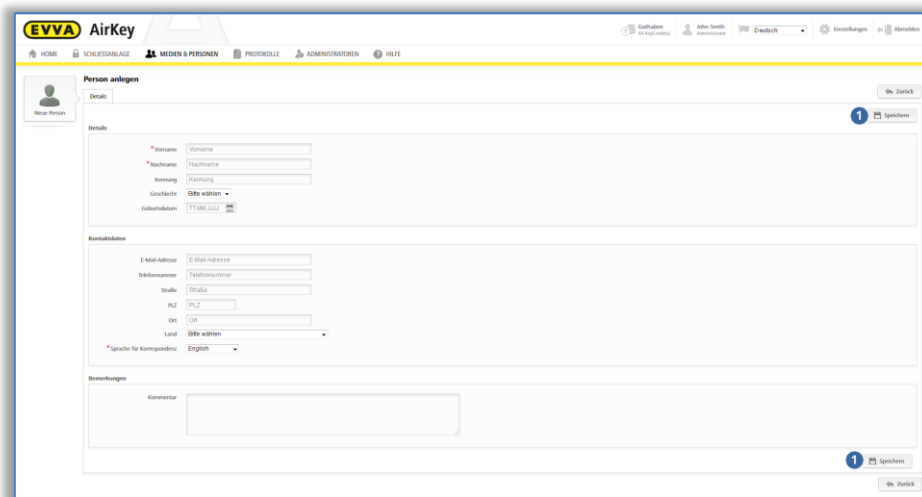


Abbildung 27: Person anlegen



Die Felder Vorname / Nachname / Kennung ergeben eine eindeutige Kombination innerhalb der AirKey-Schließanlage.




Wenn Sie das Feld "Kennung" zusätzlich befüllen, verwenden Sie einen Wert, der gewährleistet, dass die Kombination mit Vorname und Nachname eindeutig ist (z.B. die Personalnummer). Das ist vor allem dann sinnvoll, wenn Personen den gleichen Vor- und Nachnamen besitzen.

Die Feldlänge für "Vorname", "Nachname", "E-Mail-Adresse", "Telefonnummer", "Straße" und "Ort" ist jeweils auf maximal 50 Zeichen begrenzt. Für "PLZ" können max. 10 Zeichen verwendet werden. Im Feld "Kommentar" können Sie einen Text mit bis zu 500 Zeichen eingeben.

Wenn die eingegebene Kombination bereits angelegt wurde, erhalten Sie die Fehlermeldung "Person existiert bereits".

- > Prüfen bzw. korrigieren Sie gegebenenfalls Ihre Eingaben.
- > Klicken Sie auf **Speichern**.

Wenn die Person erfolgreich angelegt wurde, erscheint eine Erfolgsmeldung und unterhalb des Namens wird eine neue Schaltfläche **Medium zuweisen**  eingeblendet.

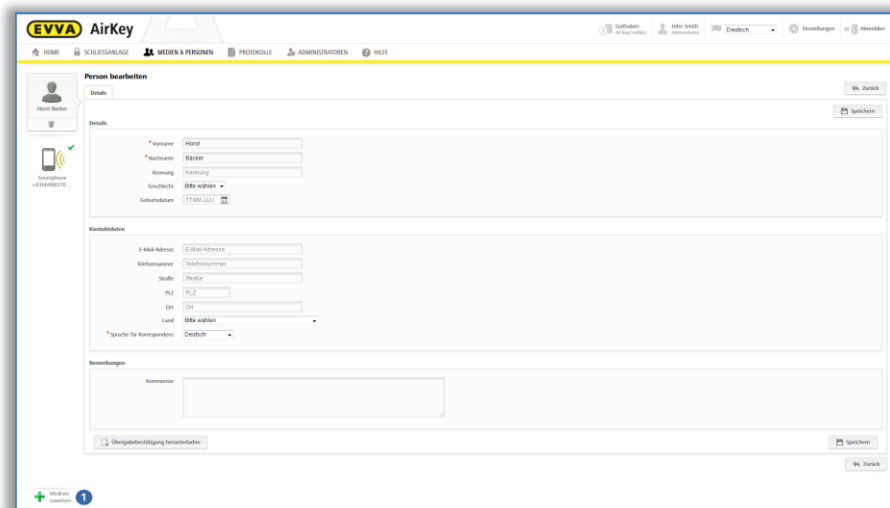


Abbildung 28: Medium zuweisen

Die Person ist damit in der AirKey-Schließanlage angelegt und wird in der Personenliste aufgelistet.

4.7.1 Personendaten importieren

Sie haben bei AirKey auch die Möglichkeit, Personen über externe Dateien anzulegen. Dazu benötigen Sie eine entsprechende CSV-Datei, um diese in die AirKey-Onlineverwaltung zu importieren.

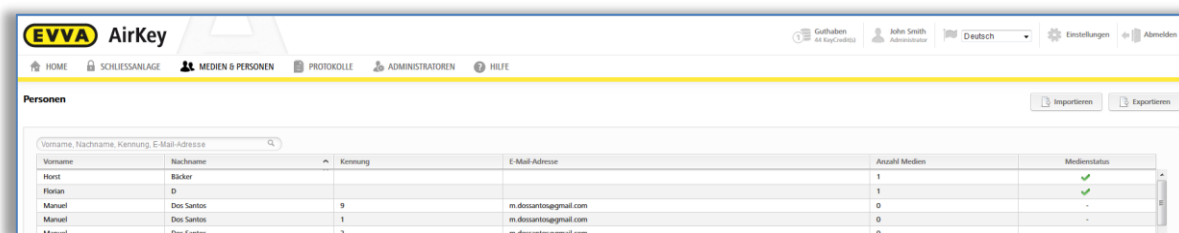


Abbildung 29: Personenliste importieren

Die Aufteilung der Personentabelle folgt dem Blatt **Person anlegen** in der AirKey-Onlineverwaltung, d.h., Spalte A ist Vorname ❶, Spalte B ist Nachname ❷, Spalte C ist Kennung ❸ etc. In genau dieser Reihenfolge werden die Felder der CSV-Datei in die AirKey-Onlineverwaltung importiert.



Abbildung 30: Personen importieren – Personenliste

	1) Vorname (Pflichtfeld, max. 50 Zeichen)	2) Nachname (Pflichtfeld, max. 50 Zeichen)	3) Kennung (max. 50 Zeichen)	4) Geschlecht (M / F)	5) Geburtsdatum (JJJ-MM-TT)	6) E-Mail-Adresse (max. 50 Zeichen)	7) Telefonnummer (als Text formatieren, max. 50 Zeichen)	8) Straße (max. 50 Zeichen)	9) PLZ (max. 10 Zeichen)	10) Ort (max. 50 Zeichen)	11) Land (siehe Excel-Kommentar)	12) Sprache für Korrespondenz (Pflichtfeld, siehe Excel-Kommentar)	13) Kommentar (max. 250 Zeichen)
1													
2													
3	Kleinsten	Datensatz										de-DE	
4													
5	Anna	Ötker	AÖ	F	1997-12-20	email1@gmx.com	+43 664 123 456 789	Schöne Straße 1	1130	Wien	AUT	de-DE	Sonderzeichen: Ö, ß
6	Jan	Český	J.Č.	M	1964-05-17		+420 111 222 333 444	Připotoční 1337	101 00	Prag	CZE	cs-CZ	Sonderzeichen: Č, ě, ř, ý
7													
8	Dany	DeVito	DD									en-UK	Person 1
9	Dany	deVito	Dd									it-IT	Person 2 = Duplikat!
10													
11	Achtung!	Manuelle Zeilenumbrüche in Excel-Zellen sind für den Personen-Import nicht erlaubt!											
12												de-DE	

Abbildung 31: Personen importieren – Feldaufteilung in der Personenliste

Eigenschaften einer CSV-Datei mit zu importierenden Personendaten:

- Die erste Zeile wird immer ignoriert. Deswegen empfiehlt es sich, dort die Feldnamen einzutragen, um die weiteren Daten leichter zu identifizieren. Die erste Zeile kann auch leer sein, sie sollte aber keine Person enthalten, denn diese wird nicht importiert.

- > Leere Zeilen oder Zeilen, die nur Leerzeichen und Tabulatoren (also Leerräume) enthalten, werden ebenfalls ignoriert. Wenn Sie Ihre CSV-Datei übersichtlicher gestalten möchten, können Sie also beliebig viele leere Zeilen verwenden.
- > Jede Zeile muss alle 13 Felder enthalten, die in der Abbildung 30 angezeigt werden.
- > Die Felder werden jeweils durch einen Strichpunkt getrennt.
- > Es gibt nur 3 Pflichtfelder: Vorname (Feld 1), Nachname (Feld 2) und Sprache für Korrespondenz (Feld 12).
- > Wenn die restlichen Felder keine Daten enthalten sollen, müssen sie trotzdem vorhanden sein, und zwar als leere Felder (;;).
- > Das Geschlecht (Feld 4) darf nur **M** (für *male* = männlich) oder **F** (für *female* = weiblich) enthalten oder leer sein. Das gilt für alle Sprachen und M und F dürfen nur in Großbuchstaben verwendet werden.
- > Das Geburtsdatum (Feld 5) muss im Format **JJJJ-MM-TT** (z.B. 1997-12-20) vorhanden sein.
- > Die E-Mail-Adresse (Feld 6) muss das Zeichen @ und weitere Zeichen enthalten oder leer sein.
- > Das Land für die Adresse (Feld 11) muss den 3-stelligen [ISO-3166-1-Code](#) (Spalte ALPHA-3) des Landes enthalten oder leer sein. Der Code darf nur in Großbuchstaben angegeben werden. Beispiele: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL etc.
- > Die Sprache für Korrespondenz (Feld 12) ist ein Pflichtfeld und muss den ISO-Code für die Sprache enthalten. Die Schreibweise in Klein- und Großbuchstaben muss genau eingehalten werden. Nur folgende Codes werden akzeptiert: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- > Eine zu importierende Person wird als bereits vorhanden (Symbol ) angezeigt, wenn die Kombination Vorname + Nachname + Kennung (Felder 1-3) in der AirKey-Onlineverwaltung bereits existiert, auch wenn die restlichen Felder (4-13) unterschiedlich sind. Solche Personen werden nicht importiert. Die Groß-/Kleinschreibung der Namen wird nicht berücksichtigt (z.B. "Danny;DeVito;DD" und "Danny;deVito;Dd" werden als gleiche Person betrachtet und nur die erste Person wird importiert).
- > Eine Person wird in der CSV-Datei als Duplikat interpretiert, wenn die Kombination Vorname + Nachname + Kennung (Felder 1-3) bereits einmal gefunden wurde, auch wenn die restlichen Felder (4-13) unterschiedlich sind. In diesem Fall wird nur die erste Zeile mit einer bestimmten Kombination angezeigt und anschließend importiert. Alle weiteren Duplikate werden ignoriert und in der Tabelle der zu importierenden Personen nicht mehr angezeigt.
- > Eine CSV-Datei darf die Daten von max. 10.000 Personen enthalten. Wenn Sie mehr Personen importieren möchten, erstellen Sie mehrere CSV-Dateien, die Sie separat importieren können.
- > Fehlerhafte Zeilen in der CSV-Datei werden vor dem Import mit dem Symbol  vermerkt und mit einem Tooltip versehen, der alle Fehler beschreibt. Diese Zeilen werden nicht importiert.
- > Unabhängig von eventuell vorhandenen fehlerhaften Zeilen werden alle korrekten Zeilen mit dem Symbol  vermerkt und anschließend importiert.



Die Zeichenkodierung der CSV-Datei muss UTF-8 sein, damit länderspezifische Buchstaben (Ä, ß, ç, Ñ, č etc.) korrekt angezeigt werden. Die Erstellung einer CSV-Datei im UTF-8-Format wird weiter unten detailliert beschrieben.

Erstellung einer CSV-Datei im UTF-8-Format

Folgende Beschreibung gilt auf Windows 10™ unter Verwendung von Microsoft Excel™ und Hilfsprogrammen, die auf Windows 10™ bereits vorhanden sind. Auf anderen Windows-Versionen oder Betriebssystemen kann eine CSV-Datei im UTF-8-Format ähnlich erstellt werden. Notwendige Schritte:

- > Als Ausgangsbasis wird in dieser Beschreibung eine Excel-Tabelle angenommen, die die Daten der zu importierenden Personen enthält.
- > Achten Sie in der Excel-Tabelle darauf, dass die 7. Spalte (Telefonnummer) unbedingt als Text formatiert ist. Bei einer Formatierung als Zahl würden führende Zeichen wie "+" und "0" (Null) bei der Konvertierung verloren gehen. Leerzeichen innerhalb der Telefonnummer sind aber erlaubt und erhöhen die Übersichtlichkeit in der AirKey-Onlineverwaltung.
- > Prüfen Sie mit Hilfe der Suchfunktion in Excel, dass die Tabelle keine der folgenden Zeichen enthält:
 - " (doppelte, gerade Anführungszeichen)
 - ; (Strichpunkt = Trennzeichen in der CSV-Datei, die in die AirKey-Onlineverwaltung importiert werden soll)
- > Excel kann die Daten nicht direkt im UTF-8-Format speichern. Deswegen ist es notwendig, die Daten zuerst im Unicode-Format zu speichern.
- > Rufen Sie dazu in Excel den Menüpunkt **Datei** → **Speichern unter** auf (oder drücken Sie die Taste F12).
- > Tragen Sie im anschließenden Dialogfenster "Speichern unter" den gewünschten Dateinamen ❶ ein.
- > Wählen Sie in der Dropdown-Liste **Dateityp** ❷ das Format **Unicode Text (*.txt)**.
- > Klicken Sie auf **Speichern** ❸.

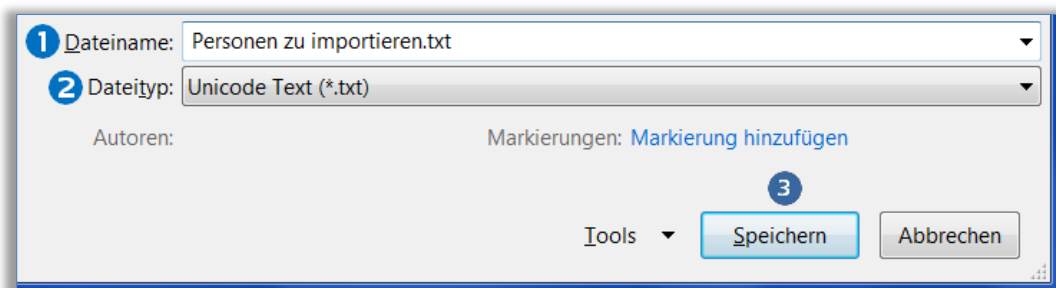


Abbildung 32: Excel – Speichern unter – "Unicode Text (*.txt)"

- > Bestätigen Sie die anschließende Excel-Frage bezüglich "Unicode Text" mit **Ja**.

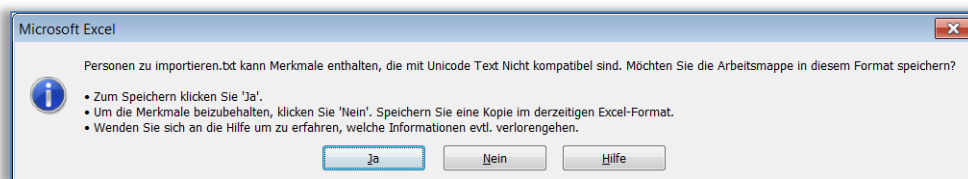


Abbildung 33: Excel – Speichern als "Unicode Text (*.txt)" bestätigen

- > Öffnen Sie die erzeugte Datei (*.txt) mit einem Texteditor. Windows™ verwendet standardmäßig das Programm **Editor**.
- > Das Trennzeichen in der Unicode-Textdatei ist der Tabulator. Alle Tabulatoren müssen durch Strichpunkte (;) ersetzt werden. Dafür markieren Sie zuerst einen Tabulator zwischen 2 Feldern und kopieren ihn.

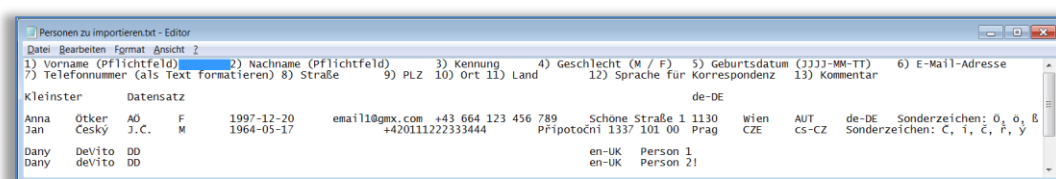


Abbildung 34: Tabulator markieren und in die Zwischenablage kopieren

- > Rufen Sie im **Editor** den Menüpunkt **Bearbeiten** → **Ersetzen** auf, um das Dialogfenster "Ersetzen" zu öffnen.
 - Fügen Sie im Feld **Suchen nach** das Tabulator-Zeichen aus der Zwischenablage, weil dieses Zeichen hier nicht direkt eingegeben werden kann.
 - Tragen Sie im Feld **Ersetzen durch** einen Strichpunkt (;) ein.
 - Klicken Sie auf **Alle ersetzen** ①.

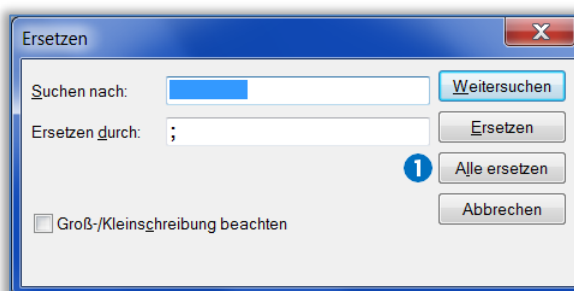


Abbildung 35: "Editor" – alle Tabulatoren durch Strichpunkte ersetzen

- > Schließen Sie das Dialogfenster "Ersetzen" und rufen Sie im **Editor** den Menüpunkt **Datei** → **Speichern unter** auf, um das Dialogfenster "Speichern unter" zu öffnen.
 - Ändern Sie manuell die Dateierweiterung von .txt auf .csv im Feld **Dateiname** ①. Eine spätere Umbenennung ist aufwendiger!
 - Wählen Sie in der Dropdown-Liste **Codierung** ② das Format **UTF-8**.
 - Klicken Sie auf **Speichern** ③.

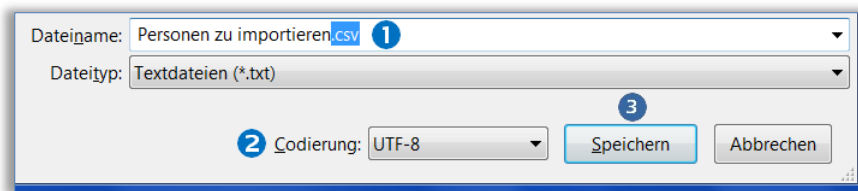


Abbildung 36: Dateieindung .csv manuell eintragen und UTF-8-Codierung auswählen

- > Die auf diese Weise erstellte CSV-Datei kann anschließend in die AirKey-Onlineverwaltung importiert werden.



Die CSV-Datei kann direkt mit Excel geöffnet werden. Führen Sie bitte KEINE Änderungen der CSV-Datei in Excel durch, da beim Speichern die UTF-8-Codierung geändert werden würde!

Geringfügige, nachträgliche Änderungen der Personendaten können in der CSV-Datei durchgeführt werden, wenn diese z.B. mit dem **Editor** geöffnet und anschließend gespeichert wird.

Für umfangreichere Änderungen der Personendaten empfiehlt es sich, die Daten in der ursprünglichen Excel-Datei anzupassen und den ganzen Vorgang zum Erstellen der CSV-Datei im UTF-8-Format zu wiederholen.

CSV-Datei (im UTF-8-Format) in die AirKey-Onlineverwaltung importieren

Um eine CSV-Datei mit Personendaten zu importieren, führen Sie folgende Schritte aus:

- > Wählen Sie auf der Startseite **Home** die Kachel **Personen**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Personen**.
- > Klicken Sie rechts auf **Importieren** 1.

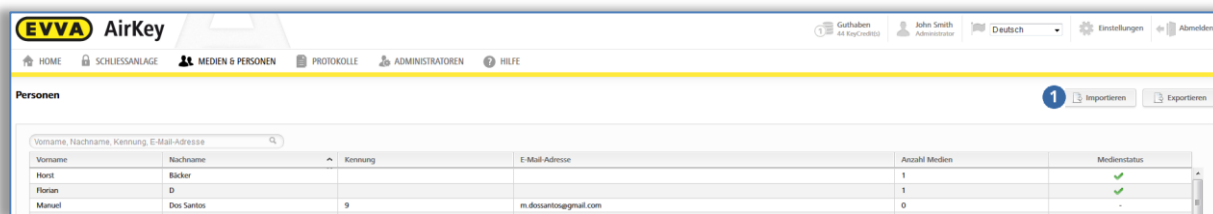


Abbildung 37: Personen importieren

- > Wählen Sie **Datei auswählen**.
- > Wählen Sie jene CSV-Datei aus, die Sie importieren möchten.
- > Sie erhalten einen Überblick über die zu importierenden Personen.
- > Klicken Sie auf **Import starten** 1.

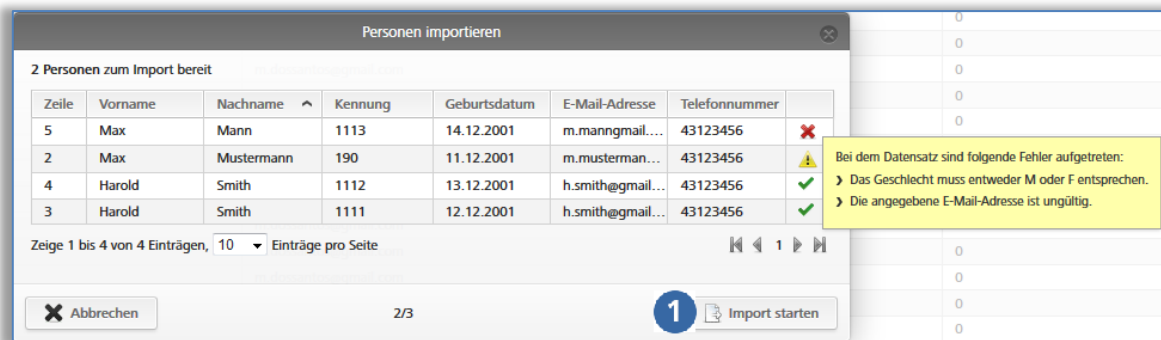


Abbildung 38: Personen importieren

- > Sie erhalten als Meldung über wie viele Personen erfolgreich importiert werden konnten und welche Zeilen fehlerhaft waren.
- > Klicken Sie auf **Schließen**.

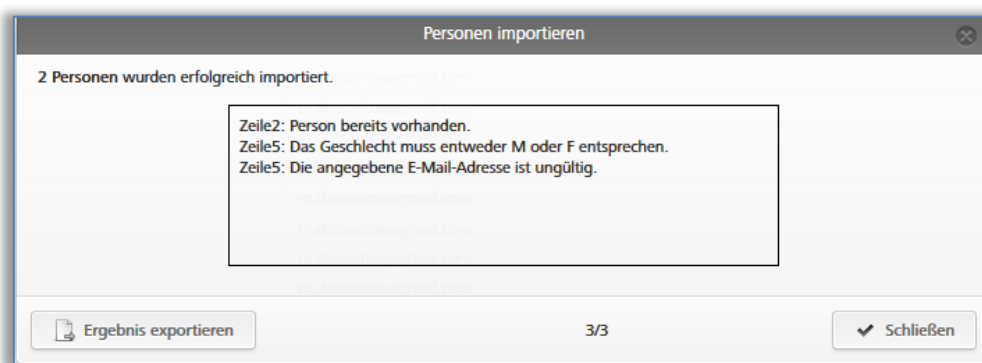


Abbildung 39: Personen importieren – Ergebnis

- > Sie werden in der AirKey-Onlineverwaltung automatisch auf die Übersichtsliste der Personen weitergeleitet.
- > Um die gewünschten Zutrittsberechtigungen den jeweiligen Personen zuzuweisen, kann das wie gewohnt für jede einzelne Person durchgeführt werden wie unter [Medium einer Person zuweisen](#) beschrieben. Identische Zutrittsberechtigungen können schnell und einfach durch Duplizierung vervielfältigt werden. Informationen dazu finden Sie im Kapitel [Medium duplizieren](#).

4.8 Smartphone anlegen

Um ein Smartphone in Ihrer Schließanlage zu verwalten, müssen Sie dieses zuerst anlegen bzw. hinzufügen.

- > Klicken Sie auf der Startseite **Home** im grauen Balken des Blocks **Medien & Personen** auf **Hinzufügen** → **Medium hinzufügen**.
- > Oder wählen Sie auf der Startseite **Home** die Kachel **Smartphones** → **Medium hinzufügen**.
- > Oder wählen Sie im Hauptmenü **Medien & Personen** → **Medium hinzufügen**.



Abbildung 40: Neues Medium vom Typ Smartphone oder Karte

- > Wählen Sie als neues Medium **Smartphone** und klicken Sie auf **Weiter** ①.
- > Geben Sie im Feld "Bezeichnung" eine sinnvolle Information (z.B. den Smartphone-typ) ein.
- > Geben Sie die Telefonnummer des Smartphones ein. Die Telefonnummer muss mit + und Landesvorwahl beginnen, und max. 50 Zeichen enthalten (+, 0-9 und Leerzeichen).
- > Klicken Sie auf **Medium hinzufügen** ①.

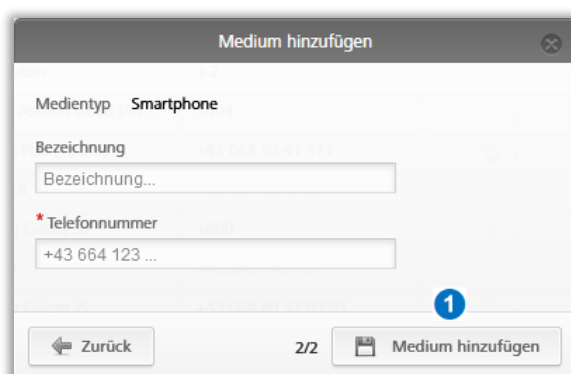


Abbildung 41: Neues Medium hinzufügen



Wenn die Telefonnummer ungültig ist oder die Telefonnummer bereits angelegt wurde, erhalten Sie eine Fehlermeldung.

Sie befinden sich nun in den Details zu diesem Smartphone.

- > Klicken Sie auf **Registrierungscode erstellen** ①, wenn noch kein Registrierungscode erzeugt wurde.

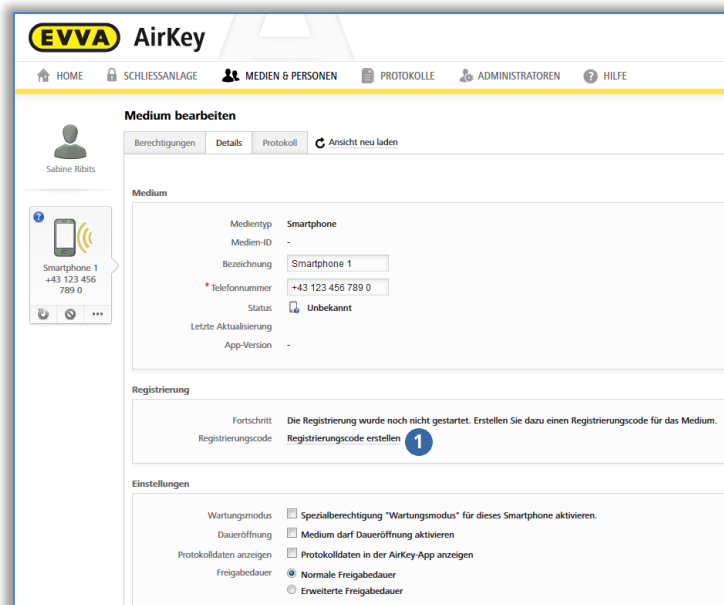


Abbildung 42: Registrierungscode erstellen

Im Block **Registrierung** wird ein gültiger Registrierungscode mit seinem Ablaufdatum angezeigt. Sie können diesen auch per SMS versenden. Dazu müssen Sie nur auf den entsprechenden Link klicken. Es wird dann das genaue Datum und die Uhrzeit angezeigt, wann der Registrierungscode per SMS gesendet wurde.

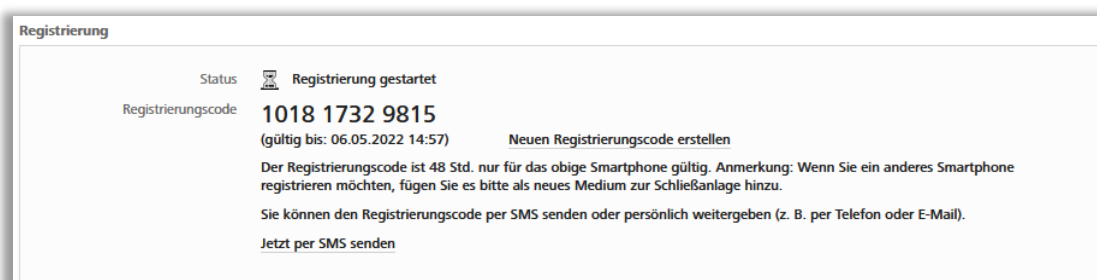


Abbildung 43: Registrierungscode

Im Block **Einstellungen** innerhalb der Details des Smartphones können Sie folgende Einstellungen festlegen:

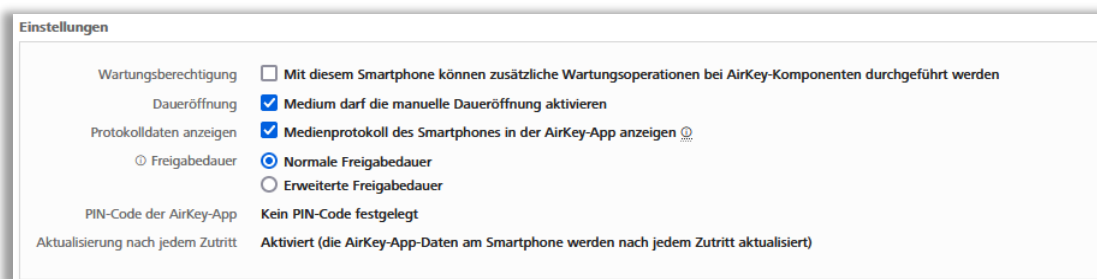


Abbildung 44: Medium bearbeiten – Einstellungen

- › **Wartungsberechtigung:** Diese Spezialberechtigung kann nur bei Smartphones aktiviert werden, die bereits einer Person zugewiesen sind. Mit dieser Funktion bekommt das Smartphone die Berechtigung, schließkomponenten im Auslieferungszustand zu sperren sowie Schließkomponenten und Medien in die AirKey-Schließanlage

hinzuzufügen und zu entfernen. Weiters kann die Firmware von Schließkomponenten und der Keyring von Medien aktualisiert werden.

- > **Medium darf die manuelle Daueröffnung aktivieren:** Wenn diese Option ausgewählt wurde, kann das Zutrittsmedium die Schließkomponente in den Zustand der [automatischen Daueröffnung](#) versetzen. Das Medium muss aber eine gültige Berechtigung für die Schließkomponente haben.
- > **Medienprotokoll des Smartphones in der AirKey-App anzeigen:** Mit dieser Option sieht die Person in der AirKey-App ihre eigenen Zutrittsereignisse sowie weitere relevante Protokolldaten zu ihrem Medium.
- > **Freigabedauer:** Legt fest, wie lange die Freigabe der Schließkomponente bei einer Sperrung mit diesem Smartphone andauert. Die Längen der normalen bzw. der erweiterten Freigabedauer werden bei der Schließkomponente festgelegt (von 1-250 Sekunden).
- > **PIN-Code der AirKey-App:** Gibt den Status an, ob für dieses Smartphone in der AirKey-App der PIN-Code aktiviert ist oder nicht. Wenn dieser aktiviert ist und die Person ihren PIN-Code vergessen hat, kann sie gegebenenfalls hier zurückgesetzt werden.
- > **Aktualisierung nach jedem Zutritt:** Gibt den Status an, ob die AirKey-App-Daten dieses Smartphones nach jedem Zutritt automatisch aktualisiert werden oder nicht. Details zur Aktivierung dieser Funktion finden Sie im Kapitel [Allgemein](#).

4.9 Smartphone registrieren

Das Smartphone kann registriert werden, wenn es bereits in einer Schließanlage angelegt ist und Sie den Registrierungscode kennen.

- > Starten Sie die AirKey-App auf Ihrem Smartphone.
- > Akzeptieren Sie die Lizenzvereinbarung sowie etwaige Abfragen über Zugriffe auf bestimmte Dienste des Smartphones.
- > Wenn das Smartphone mit noch keiner Schließanlage verbunden ist, wird der Dialog für die Eingabe des Registrierungscode automatisch angezeigt.



Bei iOS-Smartphones tippen Sie auf **Registrierungscode bereits erhalten**, um die Eingabe der Telefonnummer zu überspringen und zur Eingabe des Registrierungscode zu gelangen.

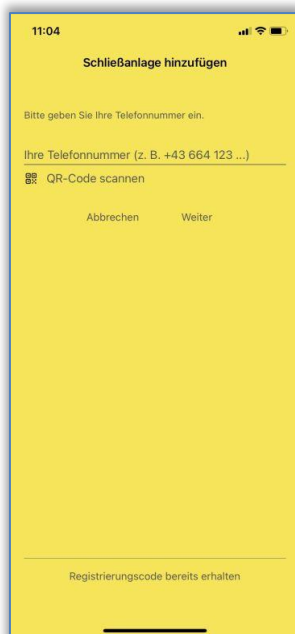


Abbildung 45: AirKey-App – Schließanlage hinzufügen (iOS)

- > Geben Sie den Registrierungscode ein, den Sie vom Administrator der AirKey-Schließanlage erhalten haben.

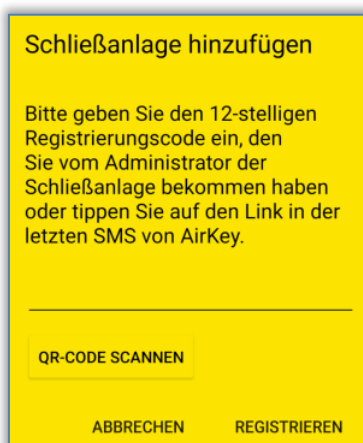


Abbildung 46: AirKey-App – Schließanlage hinzufügen (Android)

- > Bestätigen Sie Ihre Eingabe mit **Registrieren**.



Sie können ein Smartphone auch in mehreren AirKey-Schließanlagen registrieren. Um den Registrierungsdialog erneut zu öffnen, wählen Sie im Hauptmenü der AirKey-App **Einstellungen** → **Schließanlage hinzufügen**. Nähere Informationen dazu finden Sie im Kapitel [Smartphone in mehreren Anlagen verwenden](#).



Wenn der Registrierungscode ungültig oder abgelaufen ist, erhalten Sie eine Fehlermeldung. In diesem Fall wenden Sie sich an den Administrator der Schließanlage, von dem Sie den Registrierungscode erhalten haben.



Der Button **QR-Code scannen** wird nur in Verbindung mit einem Smartphonetausch benötigt. Details zum Smartphonetausch finden Sie im Kapitel [Smartphonetausch](#).

Wenn die AirKey-App oder die App-Daten gelöscht werden, besteht die Möglichkeit, die bereits ausgestellten Berechtigungen ohne Verbrauch von Guthaben wieder auf das Smartphone zu übertragen. Das gilt jedoch nur für dasselbe Gerät und Ihre Schließanlage. Bei einem Gerätewechsel ist das nicht möglich. Informationen zum einfachen Gerätewechsel finden Sie im Kapitel [Smartphonetausch](#).

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones**.
- > Oder wählen Sie in der linken Kopfzeile **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das betroffene Smartphone.
- > Klicken Sie auf den Link **Neuen Registrierungscode erstellen** und kommunizieren Sie den erzeugten Registrierungscode der Person, die ihr Smartphone in der Schließanlage registrieren möchte. Oder versenden Sie diesen direkt via SMS an das Smartphone.
- > Geben Sie den Registrierungscode in der AirKey-App ein – das Smartphone wird in der Schließanlage registriert.



Wenn Ihr Smartphone bereits in einer AirKey-Schließanlage registriert war und aus dieser nicht ordnungsgemäß entfernt wurde, wenn die App-Daten gelöscht wurden und das Smartphone in einer fremden AirKey-Schließanlage registriert wird, dann erscheint eine Meldung, dass das Smartphone bereits in einer AirKey-Schließanlage registriert war. Sofern Sie die Meldung ignorieren, kann das Smartphone wie gewohnt registriert werden. Es wird als neues Medium angelegt, alle bisherigen Daten werden unbenutzbar.



EVVA empfiehlt die Vergabe einer PIN. Diese wird als zusätzliche Sicherheitsstufe verwendet und kann nachträglich aktiviert bzw. deaktiviert werden. Nähere Informationen dazu finden Sie im Kapitel [PIN aktivieren](#).

4.9.1 Funktion "Send a Key"

An alle Personen, die ein Smartphone besitzen, können Sie einen "Schlüssel" auch über die Funktion "Send a Key" versenden. Diese Funktion kann von einem Administrator genutzt werden und erspart dem Smartphone-Besitzer die manuelle Eingabe des Registrierungs-codes für eine neue Schließanlage.

- > Klicken Sie auf die Schaltfläche **"Send a Key"**.

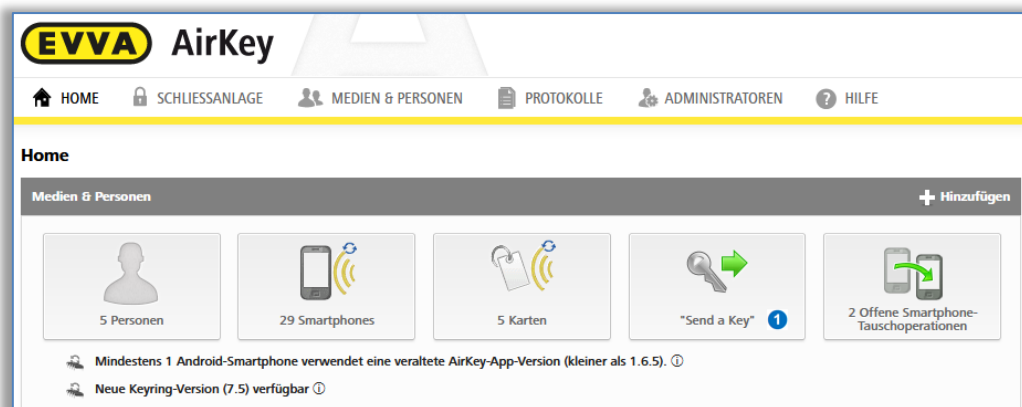


Abbildung 47: "Send a Key"

- > Geben Sie im Suchfeld einen Personennamen, Kennung etc. ein. Wenn Sie wissen, dass die Person noch nicht angelegt ist, wählen Sie **Neu anlegen**.

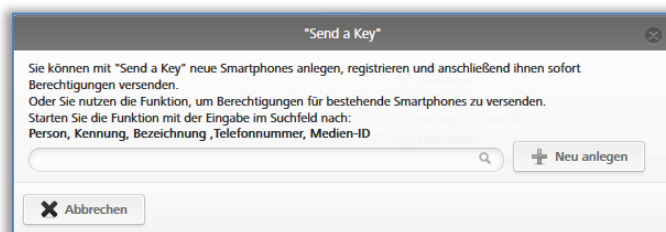


Abbildung 48: "Send a Key" – Suchfeld

- > Sind alle Pflichtfelder ausgefüllt, klicken Sie auf **Weiter**. Es wird sofort eine SMS an die Zielperson gesendet, in der ein Link mit dem Registrierungscode für die AirKey-App enthalten ist. Wenn in den allgemeinen Einstellungen ein eigener Text für die "Send a Key"-SMS ausgewählt wurde, kann hier auch nochmals der Text der SMS angepasst bzw. personalisiert werden. (Informationen zu den allgemeinen Einstellungen finden Sie im Kapitel [Allgemein](#).)

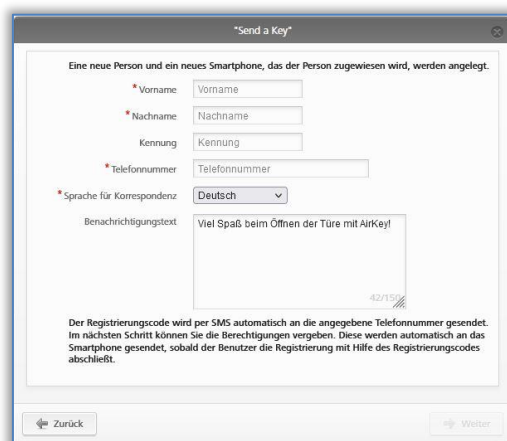


Abbildung 49: "Send a Key" – Person anlegen



Je nach Netzverfügbarkeit des Smartphones kann es einige Zeit dauern, bis die SMS mit dem Registrierungscode empfangen wird.

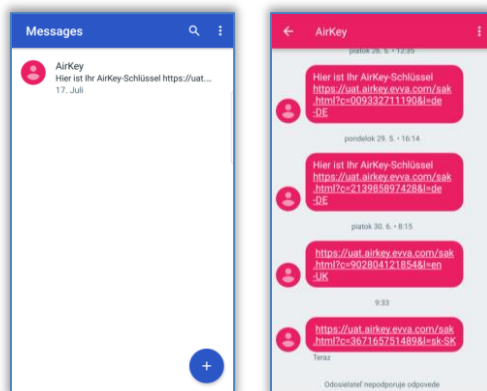


Abbildung 50: SMS mit Link – hier gezeigt mit Samsung Galaxy S7 Edge

- > Nach dem Öffnen des Links aus der SMS mit Hilfe von AirKey wird die Registrierung automatisch gestartet und durchgeführt.

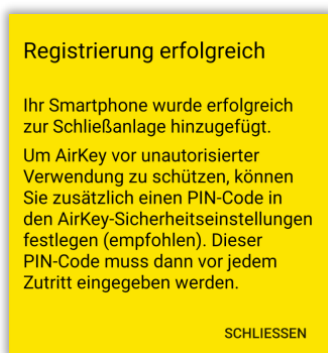


Abbildung 51: Registrierung erfolgreich



Wenn die AirKey-App auf dem Smartphone noch nicht installiert ist, gilt die folgende Vorgehensweise:

- > Tippen Sie auf den Link in der SMS und installieren Sie die App auf dem Smartphone.
- > Starten Sie die AirKey-App.
- > Bei Android-Smartphones wird die Registrierung automatisch gestartet und durchgeführt. Bei iOS-Smartphones tragen Sie Ihre Telefonnummer ein und bestätigen Sie mit **Weiter**. (Der Button **QR-Code scannen** wird nur in Verbindung mit einem Smartphonetausch benötigt. Details zum Smartphonetausch finden Sie im Kapitel [Smartphonetausch](#).)

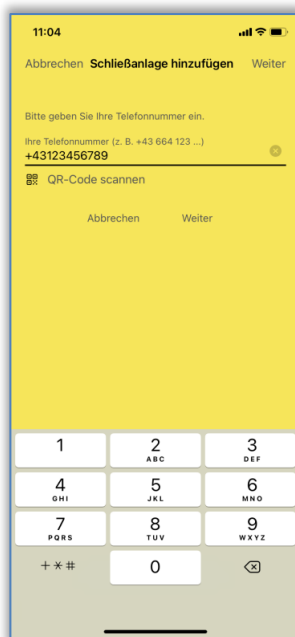


Abbildung 52: Telefonnummer eingeben (iOS)

- > Sie erhalten eine weitere SMS. Bleiben Sie jedoch in der AirKey-App und wählen Sie den 8-stelligen Registrierungscode aus, der oberhalb der Tastatur eingeblendet wird.



Abbildung 53: Registrierungscode (iOS)

Sollte der 8-stellige Registrierungscode nicht als Vorschlag angezeigt werden oder Sie in der Zwischenzeit die AirKey-App geschlossen haben, so müssen Sie den 8-stelligen Registrierungscode aus der SMS kopieren und innerhalb der AirKey-App einfügen.

- > Schließen Sie die Registrierung mit **Registrieren** ab.

In der AirKey-Onlineverwaltung werden Sie nach der Verwendung der Funktion "Send a Key" auf die Seite **Medium bearbeiten** automatisch weitergeleitet, wo Sie die gewünschten Berechtigungen erstellen können. Mit Drag & Drop ziehen Sie die jeweilige Schließkompo-

nente, für die die Zutrittsberechtigung erteilt werden soll, auf die gewünschte Zutrittsart (Dauerzutritt, Temporärer Zutritt, Periodischer Zutritt, Individueller Zutritt) – siehe auch [Berechtigungen vergeben](#).

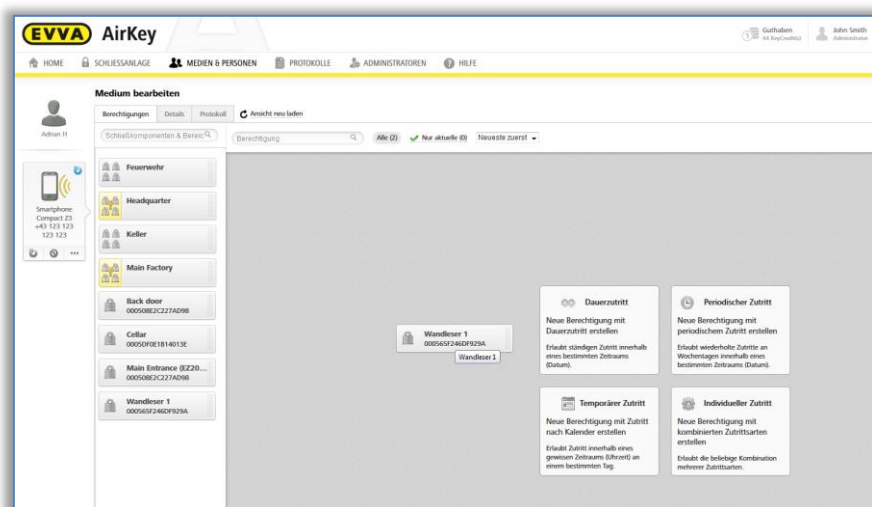


Abbildung 54: Zutrittsarten

4.10 Schließkomponenten installieren

4.10.1 AirKey-Zylinder, -Hybridzylinder, -Hebelzylinder und -Hängeschloss

Für die Montage des AirKey-Zylinders, -Hybridzylinders, -Hebelzylinders und -Hängeschlosses beachten Sie bitte die in der Verpackung beigelegte Montageanleitung oder das Montagevideo unter <https://www.evva.com/de/airkey/website/>.



Bei einem AirKey-Zylinder mit beidseitigem Zutritt muss darauf geachtet werden, dass beide Seiten innerhalb der AirKey-Schließanlage konfiguriert sind, damit man sich nicht ein- bzw. aussperrt.

4.10.2 AirKey-Wandler

Für die Montage des AirKey-Wandlers beachten Sie bitte die in der Verpackung beigelegte Montageanleitung. Zusätzlich finden Sie auf unserer Homepage eine Bohrschablone oder das Montagevideo unter <https://www.evva.com/de/airkey/website/>.



Pro Wandler wird jeweils eine Steuereinheit benötigt. Die Steuereinheit muss im sicheren Innenbereich montiert werden. Prüfen Sie die Verkabelung an Wandler und Steuereinheit.

AirKey-Schließkomponenten werden stets im Auslieferungszustand ausgeliefert.



- Medien im Auslieferungszustand sperren Schließkomponenten im Auslieferungszustand.
- Smartphones mit installierter AirKey-App und Wartungsberechtigung sperren Schließkomponenten im Auslieferungszustand.
- Im Auslieferungszustand erfolgen keine Aufzeichnungen über Sperrversuche.

- > Eine Sperrberechtigung ist erst gegeben, nachdem Sie die AirKey-Schließkomponente zu einer Schließanlage hinzugefügt haben.
- > Beachten Sie bei der Montage die Hinweise in der Montageanleitung. Bei der Montage bzw. Demontage der Schließkomponenten öffnen Sie die Tür und fixieren Sie sie so, dass sie sich nicht zufällig schließt.

4.11 Schließkomponente hinzufügen

Die Schließkomponenten werden mittels eines Smartphones mit Wartungsberechtigung oder einer optionalen Codierstation zu der Schließanlage hinzugefügt und müssen sich im Auslieferungszustand befinden.



Wenn Sie dafür ein Smartphone benutzen möchten, müssen folgende Voraussetzungen erfüllt sein:

- > Die AirKey-App ist installiert.
- > Eine aktive Internetverbindung ist verfügbar.
- > Das Smartphone ist in der Schließanlage registriert.
- > Das Smartphone ist einer Person zugewiesen.
- > Die Wartungsberechtigung wurde dem Smartphone zugewiesen.

4.11.1 Schließkomponente mit dem Smartphone hinzufügen

- > Starten Sie die AirKey-App.
- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden 1**.
- > Verbindung über **Bluetooth** (bei **Android**-Smartphones) herstellen: Tippen Sie bei der Schließkomponente im Auslieferungszustand, die Sie in Ihre Schließanlage hinzufügen wollen, auf das Kontextmenü (:), und wählen Sie dann **Verbinden 2**.
- > Verbindung über **Bluetooth** (bei **iPhones**) herstellen: Wischen Sie die Schließkomponente im Auslieferungszustand, die Sie in Ihre Schließanlage hinzufügen wollen, nach links und wählen Sie dann **Verbinden 3**.

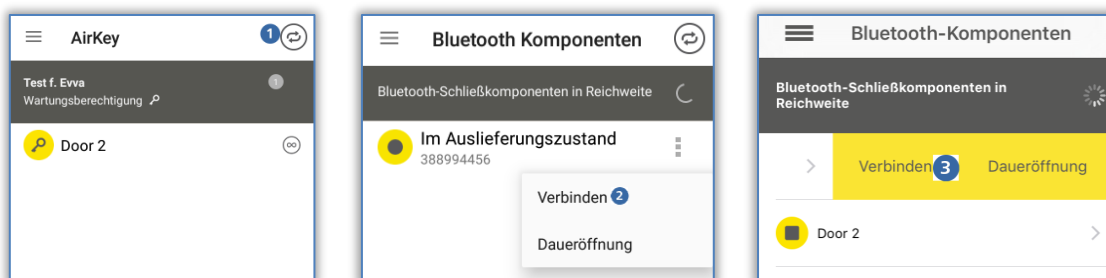


Abbildung 55: AirKey-App – Mit Komponente verbinden (über NFC bei Android-Smartphone / über Bluetooth bei Android-Smartphone / über Bluetooth bei iPhone)

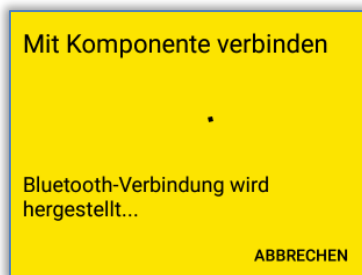


Abbildung 56: AirKey-App – Mit Komponente verbinden

- > Halten Sie das Smartphone an die Schließkomponente im Auslieferungszustand (bei Verbindung über NFC), um eine Verbindung aufzubauen. Über Bluetooth wird die Verbindung automatisch aufgebaut. Entfernen Sie keinesfalls das Smartphone von der Schließkomponente, während die Verbindung aufgebaut wird.

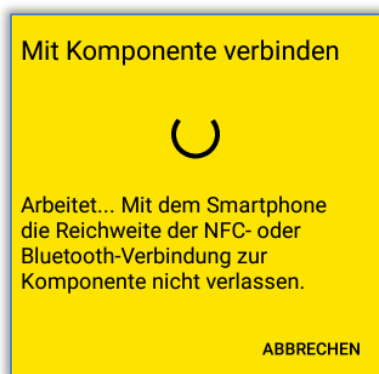


Abbildung 57: AirKey-App – Verbindung wird aufgebaut

- > Sie erhalten nun Informationen über die Schließkomponente.

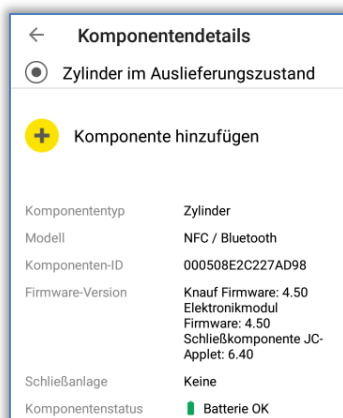


Abbildung 58: Komponente hinzufügen

- > Tippen Sie auf **Komponente hinzufügen**.
- > Geben Sie für die Schließkomponente eine klare Bezeichnung ein.



Bei einem Zylinder mit beidseitigem Zutritt muss darauf geachtet werden, dass beide Seiten innerhalb der AirKey-Anlage konfiguriert sind. Benennen Sie beide Seiten eines Zylinders mit beidseitigem Zutritt jeweils mit einer

klaren Bezeichnung. Legen Sie einen Bereich an, in dem beide Seiten des Zylinders enthalten sind und vergeben Sie eine Bereichsberechtigung, um an beiden Seiten die gleiche Berechtigung zu erhalten.

- > Wenn das Smartphone in mehreren Schließanlagen mit aktiver Wartungsberechtigung registriert ist, wählen Sie die Schließanlage aus, zu der die Schließkomponente hinzugefügt werden soll.

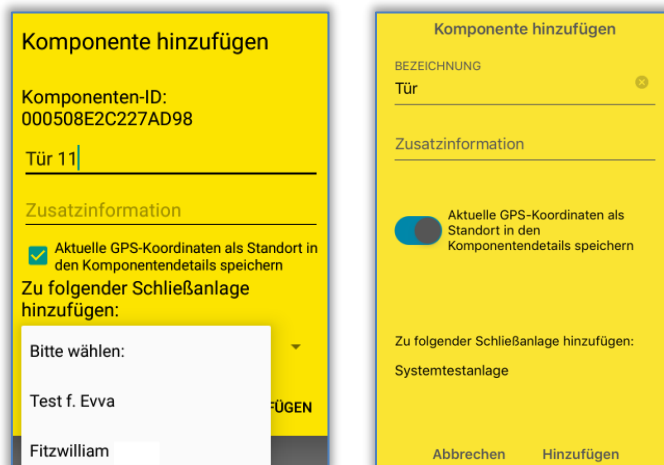


Abbildung 59: AirKey-App – Schließkomponente hinzufügen (Android / iPhone)

- > Tippen Sie auf **Hinzufügen**.
- > Halten Sie das Smartphone erneut an die Schließkomponente im Auslieferungszustand (bei Verbindung über NFC), um eine Verbindung aufzubauen. Über Bluetooth wird die Verbindung automatisch aufgebaut.



Die Daten werden überprüft und die Schließkomponente aktualisiert. Während dieses Vorgangs entfernen Sie das Smartphone nicht von der Schließkomponente.

- > Der Vorgang wird mit einer Erfolgsmeldung abgeschlossen. Die Schließkomponente steht nun in der AirKey-Onlineverwaltung zur weiteren Administration zur Verfügung.

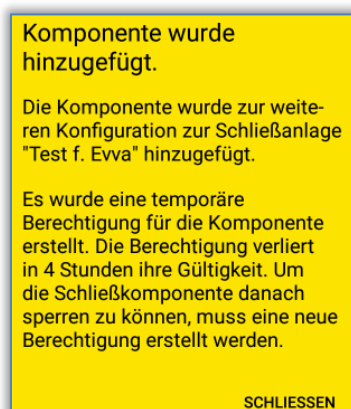


Abbildung 60: AirKey-App – Schließkomponente hinzugefügt

Die Schließkomponente erscheint in der Übersichtsliste der Schließkomponenten in der AirKey-Onlineverwaltung. Wurden beim Hinzufügen der Schließkomponente die GPS-Koordinaten **1** ermittelt, sind sie in der AirKey-Onlineverwaltung bei der Schließkomponente unter dem Reiter **Details** im Block "Tür" zu finden.

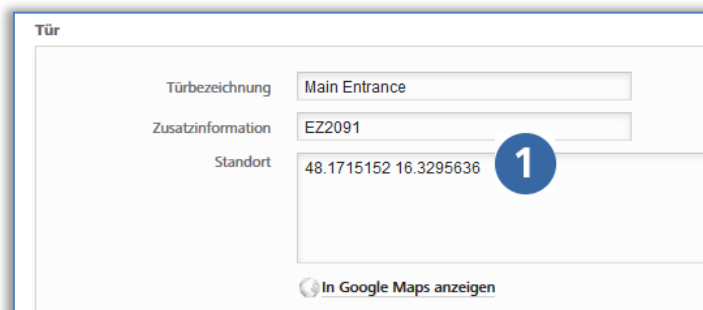


Abbildung 61: GPS-Koordinaten in den Details der Schließkomponente

Alternativ kann im Feld "Standort" die Adresse manuell eingegeben werden, unter der die Schließkomponente zu finden ist.



Die Schließkomponente befindet sich nun nicht mehr im Auslieferungszustand. Medien im Auslieferungszustand oder Smartphones mit Wartungsberechtigung sind somit nicht mehr berechtigt. Das Smartphone, das die Schließkomponente hinzugefügt hat, wird automatisch für 4 Stunden berechtigt. Bitte ändern Sie rechtzeitig diese Berechtigung oder vergeben Sie weitere Medien mit einer gültigen Berechtigung, um weiterhin Zutritt zu dieser Schließkomponente zu erhalten.

4.11.2 Schließkomponente mit der Codierstation hinzufügen

Option

Um die Schließkomponente mit der Codierstation hinzuzufügen, gehen Sie wie folgt vor:

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** oder **Wandler**.
- > Klicken Sie auf die Schaltfläche **Schließkomponente hinzufügen** **1**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.

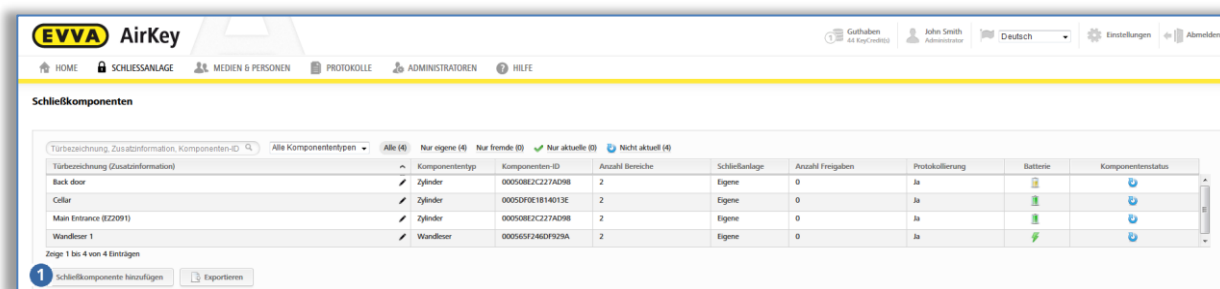


Abbildung 62: Schließkomponente hinzufügen

- > Schließen Sie die Codierstation am Computer an, andernfalls wird ein Systemhinweis **1** eingeblendet.



Abbildung 63: Schließkomponente hinzufügen / keine Codierstation

- > Wählen Sie **Komponente im Auslieferungszustand**.
- > Klicken Sie auf **Weiter**.
- > Geben Sie im nächsten Dialogfenster die Türbezeichnung ein und klicken Sie auf **Weiter**.

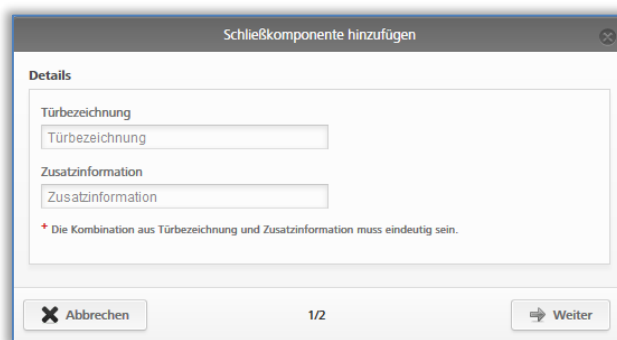


Abbildung 64: Schließkomponente hinzufügen – Namensgebung

- > Folgen Sie den Anweisungen und legen Sie die Schließkomponente auf die Codierstation.

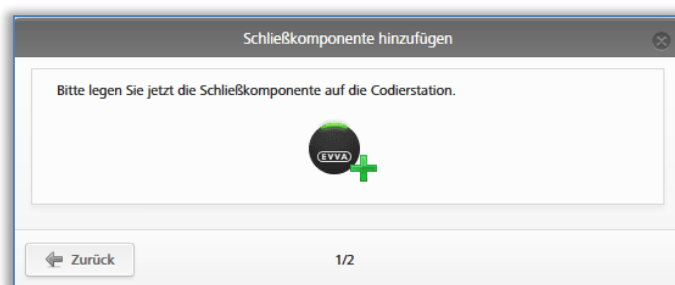


Abbildung 65: Schließkomponente hinzufügen

- > Es erscheint eine Erfolgsmeldung und die Schließkomponente wurde der AirKey-Schließanlage hinzugefügt.



Abbildung 66: Schließkomponente hinzufügen – Erfolgsmeldung

Nach dem Schließen der Erfolgsmeldung gelangen Sie zur Detailansicht der Schließkomponente.

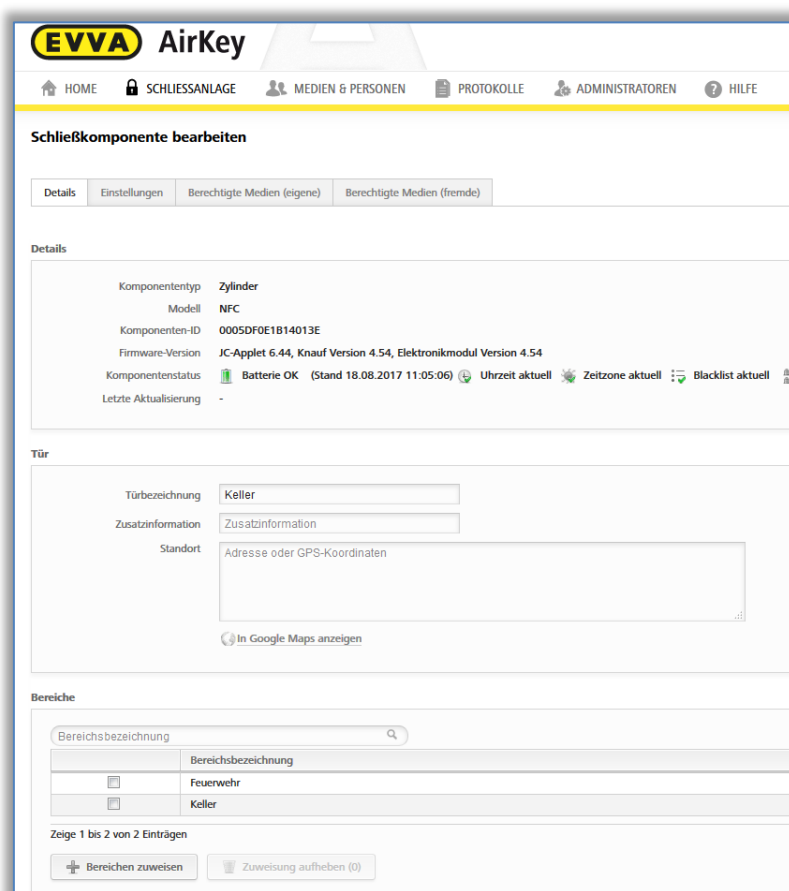


Abbildung 67: Schließkomponentendetails



Die Schließkomponente befindet sich nun nicht mehr im Auslieferungszustand. Medien im Auslieferungszustand oder Smartphones mit Wartungsberechtigung sind somit nicht mehr berechtigt, die Schließanlage hinzu und vergeben Sie eine gültige Berechtigung für die Schließkomponente, um diese weiterhin sperren zu können.



Die Vorgabezeitzone und die Einstellungen zum Datenschutz werden automatisch für die hinzugefügte Schließkomponente je nach gewählter Einstellung festgelegt. Nähere Informationen zu diesen Einstellungen finden Sie im Kapitel [Vorgabewerte \(für alle neu hinzugefügten Schließkomponenten\)](#).



Alternativ können Sie auch einfach eine Schließkomponente im Auslieferungszustand auf die Codierstation legen. Es erscheint rechts unten ein Informationsfenster, mit dem Sie ebenfalls die Schließkomponente über den Link **Komponente zu meiner Schließanlage hinzufügen** in die AirKey-Schließanlage hinzufügen können.

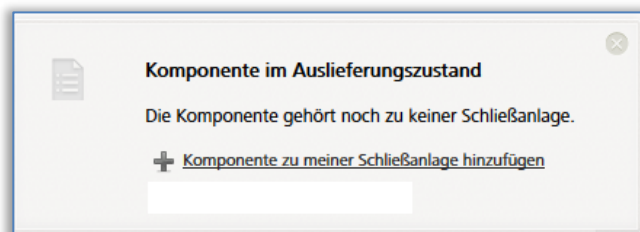


Abbildung 68: Komponente zu meiner Schließanlage hinzufügen

4.12 Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen

Zutrittsmedien im Auslieferungszustand werden mithilfe eines Smartphones mit Wartungsberechtigung oder einer optionalen Codierstation zur AirKey-Schließanlage hinzugefügt.

- > Starten Sie die AirKey-App.



Zum Hinzufügen des Kombischlüssels mit dem Smartphone muss der Kombischlüssel mit jener Seite an das Smartphone angehalten werden, auf der das RFID-Symbol aufgebracht ist. Der Kombischlüssel muss bei den meisten Modellen direkt an das Smartphone angehalten werden.

Diese Aktion kann nur mit einem NFC-fähigen Android-Smartphone durchgeführt werden. Für das Hinzufügen von Medien über Bluetooth mit einem Android-Smartphone oder mit einem iPhone siehe Kapitel [Medien codieren](#).

- > Tippen Sie auf das Symbol **Mit Komponente verbinden**

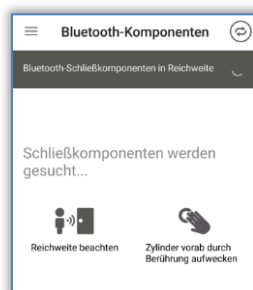


Abbildung 69: AirKey-App – Mit Komponente verbinden

- > Halten Sie das Smartphone an das Medium im Auslieferungszustand. Es wird eine Verbindung zum Medium aufgebaut.

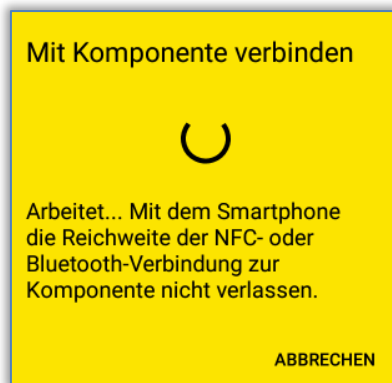


Abbildung 70: AirKey-App – Verbindung wird aufgebaut

- > Entfernen Sie keinesfalls das Medium vom Smartphone, während die Verbindung aufgebaut wird. Sie erhalten nun die Information über das Medium.

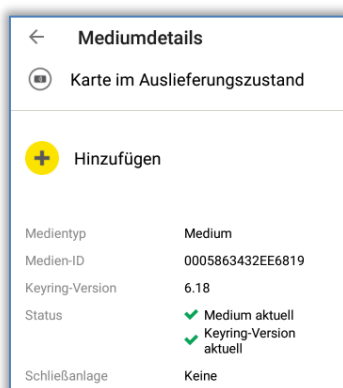


Abbildung 71: Mediumdetails

- > Tippen Sie auf **Hinzufügen**.
- > Geben Sie für das Medium eine Bezeichnung ein.

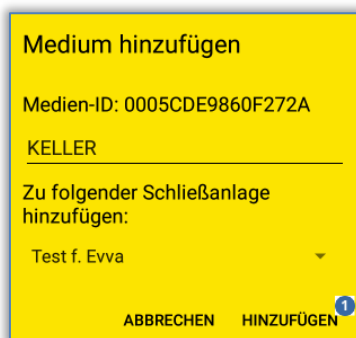


Abbildung 72: Medium hinzufügen – Bezeichnung festlegen

- > Wenn das Smartphone in mehreren Schließanlagen registriert ist, wählen Sie die Schließanlage aus, zu der das Medium hinzugefügt werden soll.
- > Tippen Sie auf **Hinzufügen** ❶.
- > Halten Sie nun erneut das Smartphone an das Medium, um den Vorgang abzuschließen.

- > Der Vorgang wird mit einer Erfolgsmeldung abgeschlossen. Das Medium steht nun in der AirKey-Onlineverwaltung zur Verfügung – und muss noch einer Person zugewiesen werden.



Dieser Vorgang ist für Karten, Schlüsselanhänger, Kombischlüssel und Armbänder identisch. Alle drei werden unter dem Begriff "Karte" geführt.

4.13 Person einem Medium zuweisen

Im nächsten Schritt müssen Sie das Medium einer Person innerhalb der AirKey-Onlineverwaltung zuweisen, um Berechtigungen vergeben zu können. Nur damit erhalten Sie einen Personenbezug bei Zutritten.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** oder **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Medienliste auf jenes Medium, das noch keiner Person zugewiesen ist.
- > Klicken Sie bei der Schaltfläche **Keine Person** auf das **+**-Symbol **1**



Abbildung 73: Person zuweisen

- > Wählen Sie aus der Personenliste jene Person aus, der dieses Medium zugewiesen werden soll.

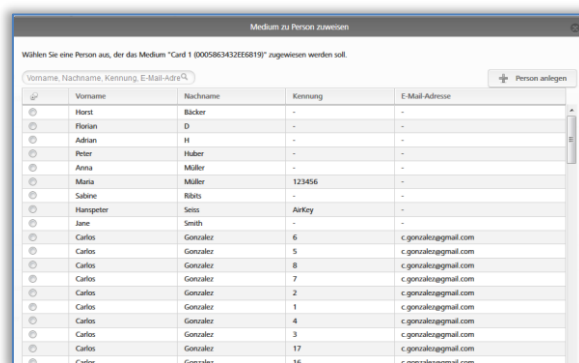



Abbildung 74: Person zu Medium zuweisen

- > Wenn die gewünschte Person noch nicht angelegt ist, gibt es hier den Button **Person anlegen**, durch den Sie zum zweiten Dialogfenster "Medium zu Person zuweisen" gelangen.
- > Bestätigen Sie die ausgewählte Person, die dem Medium zugewiesen werden soll mit **Person zuweisen** .

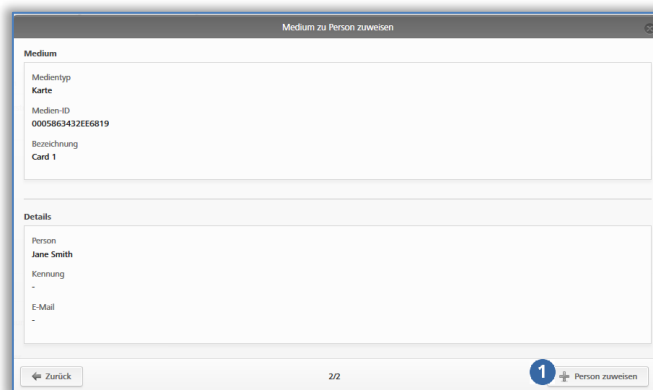


Abbildung 75: Person bestätigen

- > Siehe weiter unter [Berechtigungen vergeben](#).



Als Alternative können Sie auch die Zuweisung eines Mediums zur Person über das Medium durchführen. Nähere Informationen dazu finden Sie im Kapitel [Medium einer Person zuweisen](#).

4.14 Berechtigungen vergeben



Beachten Sie, dass Berechtigungen erst vergeben werden können, wenn ein Medium einer Person zugewiesen wurde.

- > Wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das gewünschte Medium.
- > Sofern das Medium einer Person zugewiesen ist, erscheint die Übersicht der Berechtigungen des Mediums.
- > Sobald Sie die entsprechende Schließkomponente auswählen und auf die graue Fläche ziehen, erscheinen die möglichen Zutrittsarten in den vier punktiert umrandeten Flächen.

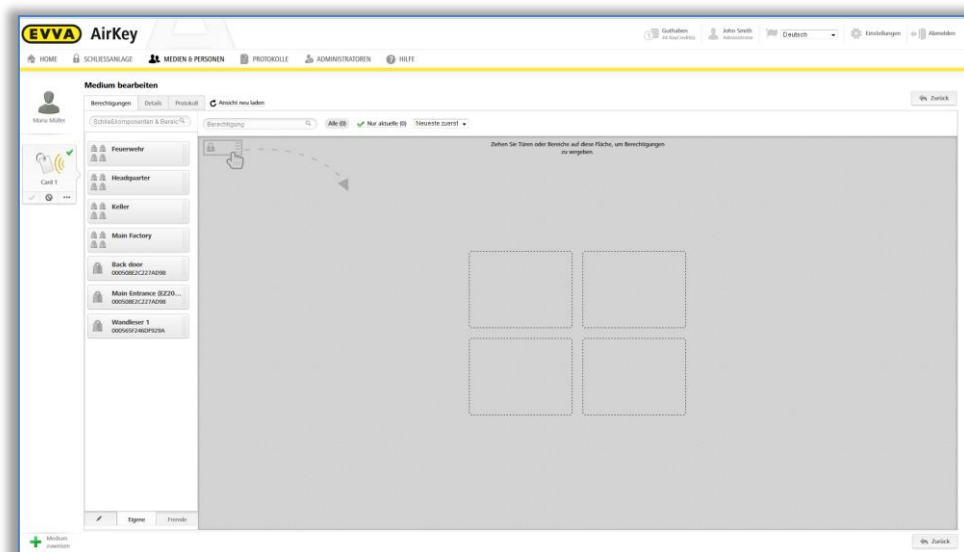


Abbildung 76: Berechtigung vergeben

- > Wählen Sie die gewünschte Zutrittsart, indem Sie die gewählte Tür / den gewählten Bereich per Drag & Drop auf das entsprechende Feld ziehen.



Es stehen vier Zutrittsarten zur Auswahl:

- > Dauerzutritt
- > Periodischer Zutritt
- > Temporärer Zutritt
- > Individueller Zutritt

4.14.1 Dauerzutritt

Dauerzutritt bedeutet, dass rund um die Uhr ein Zutritt möglich ist. Eine Einschränkung der Berechtigung kann bei der Wahl eines Start- und Enddatums erfolgen.

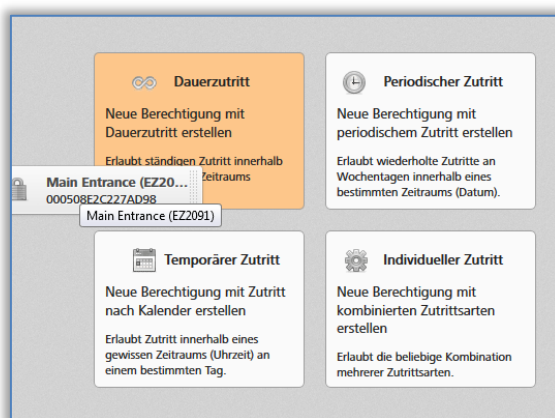


Abbildung 77: Dauerzutrtrittsberechtigung vergeben

- > Bestimmen Sie den Zeitraum für den Dauerzutritt. Es kann zwischen unbegrenztem Dauerzutritt oder einem Dauerzutritt mit festgelegtem Start- und Enddatum gewählt werden.

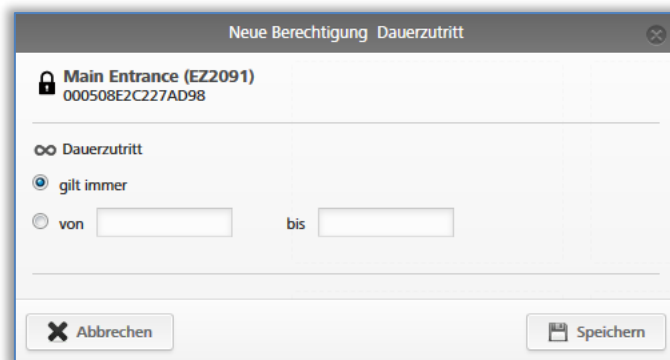


Abbildung 78: Dauerzutrittsberechtigung vergeben

- > Klicken Sie auf **Speichern**.

4.14.2 Periodischer Zutritt

Vergeben Sie eine periodische Zutrittsberechtigung für wiederkehrende Zutritte in einem bestimmten Zeitraum. Dieser wiederkehrende Zutritt ist vergleichbar mit einem Serientermin, der wöchentlich gültig ist.

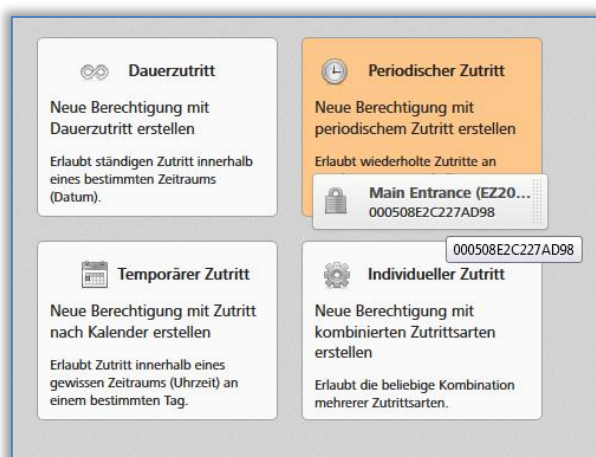


Abbildung 79: Periodischen Zutritt vergeben

Sie erhalten die Ansicht eines Wochenkalenders, in dem Sie für jeden Wochentag jeweils bis zu 4 Zeitbereiche bestimmen können.

- > Bestimmen Sie den Zeitraum für die periodischen Zutritte.

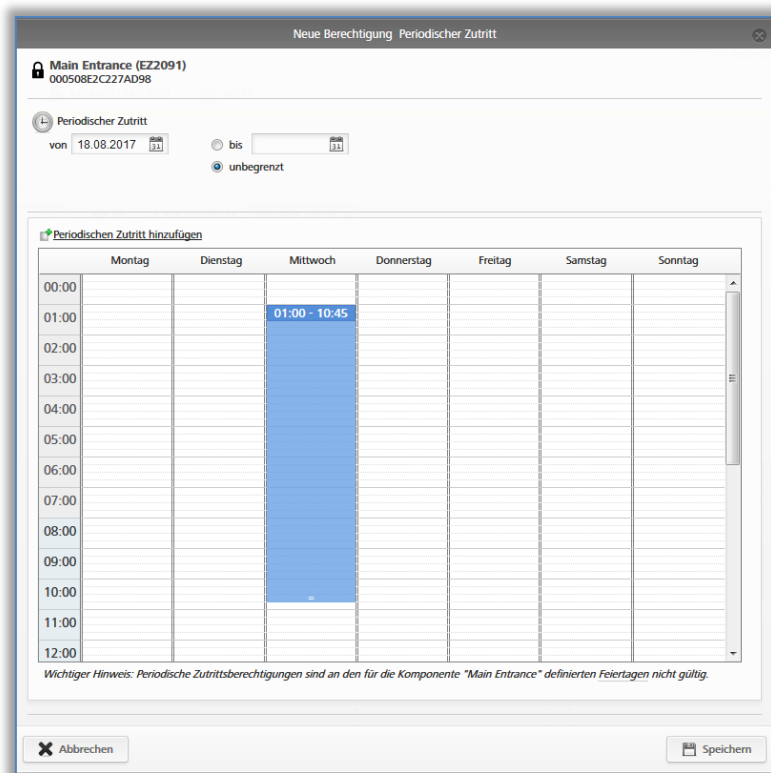


Abbildung 80: Periodischen Zutritt vergeben

- > Der Zeitraum wird über das Markieren direkt im Kalender oder über **Periodischen Zutritt hinzufügen** definiert.

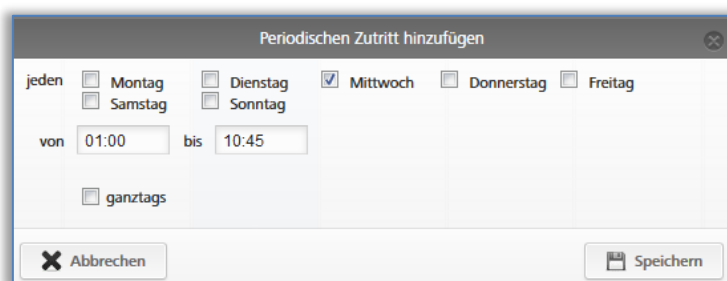


Abbildung 81: Periodischen Zutritt hinzufügen

- > Geben Sie den gewünschten Zeitraum ein und klicken Sie auf **Speichern**.
- > Klicken Sie im Dialogfenster "Neue Berechtigung – Periodischer Zutritt" ebenfalls auf **Speichern**.

4.14.3 Temporärer Zutritt

Vergeben Sie eine Einzelzutrittsberechtigung, wenn diese nur für einen bestimmten Tag in einem bestimmten Zeitraum gültig sein soll.

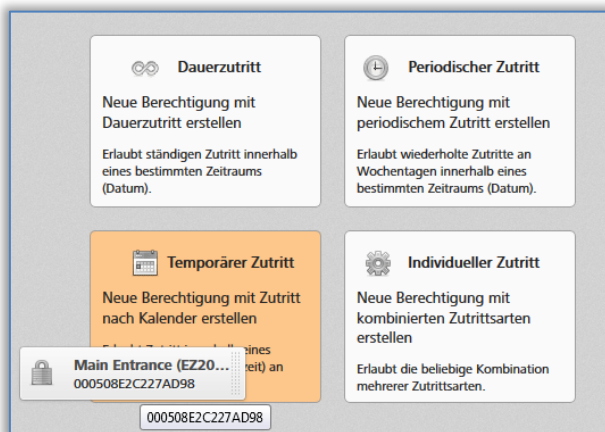


Abbildung 82: Temporäre Zutrittsberechtigung vergeben

- > Geben Sie den gewünschten Zeitraum ein und klicken Sie auf **Speichern**.



Abbildung 83: Temporäre Zutrittsberechtigung vergeben

4.14.4 Individueller Zutritt

Vergeben Sie eine individuelle Zutrittsberechtigung, wenn Sie eine Kombination aus Dauerzutrtritt, Einzelzutritt und periodischem Zutritt benötigen.



Abbildung 84: Individuelle Zutritte vergeben


- > Im Dialogfenster "Neue Berechtigung – Individueller Zutritt" sehen Sie die bereits vergebenen individuellen Zutritte.
- > Klicken Sie auf den Eintrag in einer Zeile, um die Berechtigung zu ändern oder
- > Klicken Sie auf **Zutritt hinzufügen**  für einen neuen Eintrag.



Abbildung 85: Neue Berechtigung – Individueller Zutritt

- > Wählen Sie **Dauerzutritt**, **periodischen Zutritt** oder **Temporärer Zutritt** und definieren Sie jeweils die Vorgaben. Die Parameter entsprechen den bereits beschriebenen Zutrittsberechtigungen.

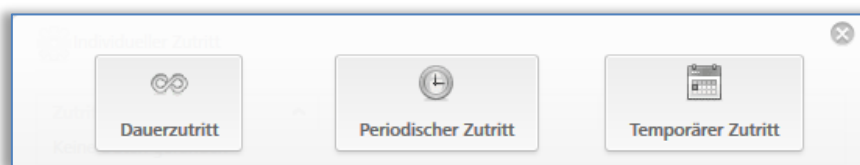


Abbildung 86: Neue Berechtigung – Individueller Zutritt

- > Klicken Sie auf **Speichern**, wenn alle Berechtigungen des individuellen Zutritts konfiguriert wurden.



- > Dauerzutritt und periodischer Zutritt dürfen sich nicht überschneiden.
- > Pro Tag darf maximal ein individueller Zutritt definiert werden.
- > Wenn sich ein individueller Zutritt und ein periodischer Zutritt überschneiden, sind beide gültig.
- > Sie können maximal 8 individuelle Berechtigungen kombinieren.

4.15 Berechtigung anfertigen

Nachdem Sie die Zutrittsberechtigung für ein Medium erstellt haben, müssen Sie den Vorgang mit **Berechtigung anfertigen** und einer abschließenden Aktualisierung des entsprechenden Mediums abschließen.

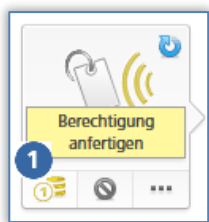


Abbildung 87: Berechtigung anfertigen

Mit dem Ändern einer bestehenden Berechtigung oder dem Erstellen einer neuen Berechtigung verändert sich das Symbol des entsprechenden Mediums. Wenn Sie noch ausreichend Guthaben haben, können Sie jetzt die Berechtigung anfertigen.

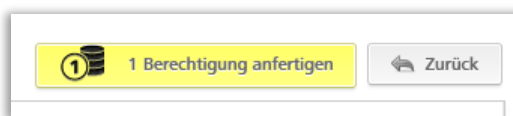


Abbildung 88: Neue oder geänderte Berechtigung anfertigen

- > Klicken Sie auf den gelben Button **1 Berechtigung anfertigen** oder auf das Symbol **1** des Mediums, um die Berechtigung anzufertigen und einen KeyCredit abzubuchen.



Wenn Sie in diesem Schritt über kein Guthaben mehr verfügen, erscheint eine entsprechende Meldung. Sie können gleich über einen Link innerhalb dieser Meldung Ihr Guthaben aufladen. Wenn das Guthaben über diese Meldung aufgeladen wird, so wird die Berechtigung automatisch angefertigt und ein KeyCredit abgebucht.



Damit die Berechtigungen am Medium wirksam werden, müssen Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder an einem Smartphone oder einer Codierstation aktualisiert werden. An Smartphones werden die Berechtigungen mittels Push-Benachrichtigungen gesendet.

In diesem Kapitel der Inbetriebnahme haben Sie gelernt, wie Sie das AirKey-System zu Beginn einrichten. Mit den darin beschriebenen Punkten haben Sie die ersten Schritte kennengelernt und können damit bereits Ihr AirKey-System administrieren. Eine genauere Beschreibung der einzelnen Funktionen der AirKey-Onlineverwaltung und der AirKey-App finden Sie in den folgenden Kapiteln.

5 AirKey-Onlineverwaltung

5.1 AirKey-Login

Der Login ist erforderlich, um die AirKey-Schließanlage zu konfigurieren bzw. zu verwalten. In den Einstellungen der AirKey-Onlineverwaltung kann für den Login eine Zwei-Faktor-Authentifizierung optional aktiviert werden. Die Aktivierung ist im Kapitel [Einstellungen der AirKey-Schließanlage](#) beschrieben.



Aktivieren Sie die Zwei-Faktor-Authentifizierung, um die Sicherheit Ihrer AirKey-Schließanlage zu erhöhen.



Fehlgeschlagene Login-Versuche werden auf der Startseite angezeigt und im Systemprotokoll protokolliert. Die Anzeige auf der Startseite erscheint nur, wenn es seit dem letzten erfolgreichen Login mindestens einen fehlgeschlagenen Login-Versuch gegeben hat.

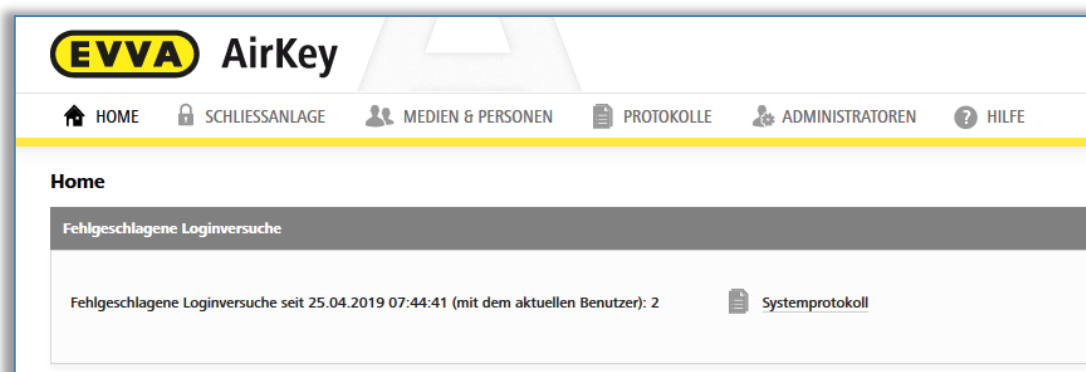


Abbildung 89: Fehlgeschlagene Login-Versuche

5.1.1 AirKey-Login ohne Zwei-Faktor-Authentifizierung

- > Öffnen Sie in Ihrem Browser die Webseite <https://airkey.evva.com>. Es öffnet sich die Login-Seite der AirKey-Onlineverwaltung.
- > Geben Sie die Benutzerkennung ein, die Ihnen in der E-Mail "EVVA-AirKey-Registrierung" mitgeteilt wurde.
- > Geben Sie das selbst gewählte AirKey-Passwort ein und bestätigen Sie mit **Anmelden**.

Direkt nach dem Login gelangen Sie zur Startseite **Home**. Dort finden Sie eine Übersicht über Ihre AirKey-Schließanlage.

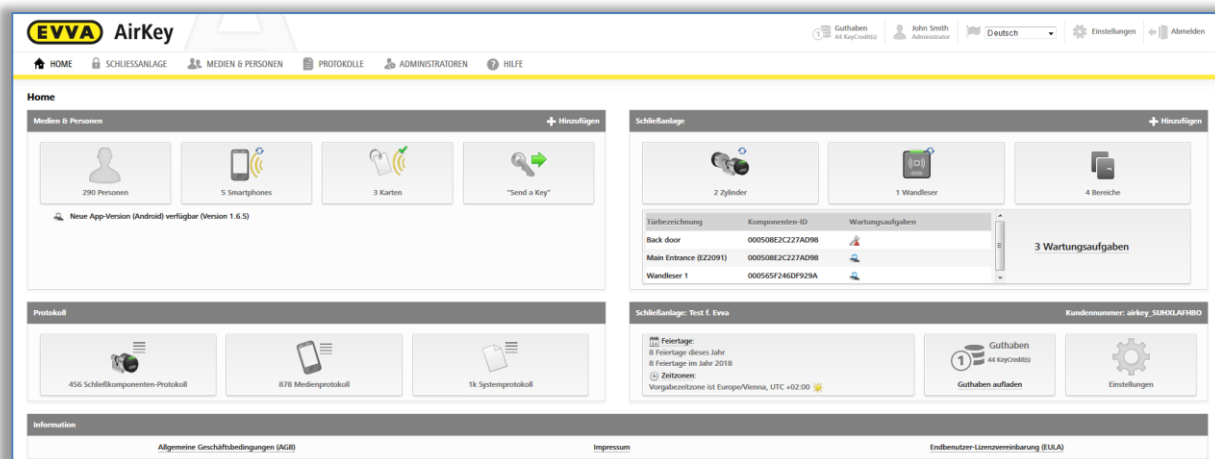


Abbildung 90: AirKey-Onlineverwaltung – Home

5.1.2 AirKey-Login mit Zwei-Faktor-Authentifizierung

- Öffnen Sie in Ihrem Browser die Webseite <https://airkey.evva.com>. Es öffnet sich die Login-Seite der AirKey-Onlineverwaltung.
- Geben Sie die Benutzerkennung ein, die Ihnen in der E-Mail "EVVA-AirKey-Registrierung" mitgeteilt wurde.
- Geben Sie das selbst gewählte AirKey-Passwort ein und bestätigen Sie mit **Anmelden**.
- Sofern für den Administrator noch keine Telefonnummer verifiziert ist, erscheint die Aufforderung, eine Telefonnummer für die Verifizierung einzutragen.
- Geben Sie die Telefonnummer des Smartphones, das für die Zwei-Faktor-Authentifizierung verwendet werden soll, ein und bestätigen Sie diese mit **SMS-Code senden**. Die Telefonnummer muss mit + und Landesvorwahl beginnen, und max. 50 Zeichen enthalten (+, 0-9 und Leerzeichen).

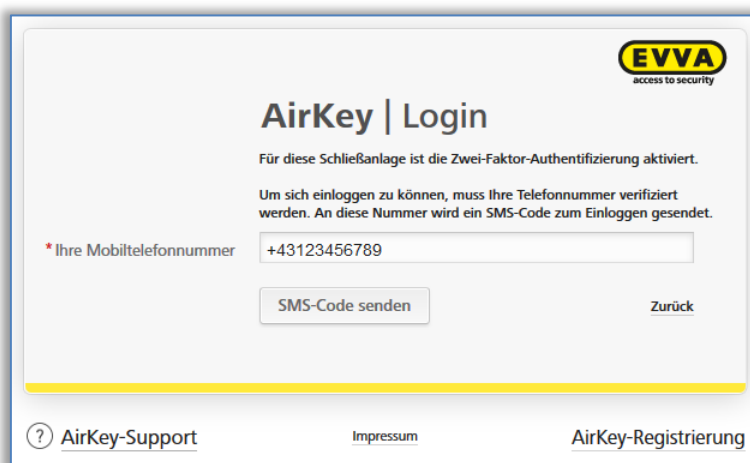


Abbildung 91: Verifizierung der Mobiltelefonnummer bei Login

- Es wird eine SMS mit einem SMS-Code an die angegebene Telefonnummer gesendet.

- > Tragen Sie diesen SMS-Code in den Dialog innerhalb der AirKey-Onlineverwaltung ein und bestätigen Sie mit **Anmelden**.

Abbildung 92: SMS-Code bei Login

- > Die Telefonnummer ist damit für die Zwei-Faktor-Authentifizierung verifiziert und es wird die Startseite Ihrer AirKey-Schließenanlage angezeigt.



Wurde die Telefonnummer bereits verifiziert, muss diese nach der Eingabe von Benutzerkennung und Passwort nicht wieder eingegeben werden. In diesem Fall wird sofort danach ein SMS-Code an die verifizierte Telefonnummer gesendet. Dieser Code muss in der AirKey-Onlineverwaltung für den Login eingetragen werden.



Der SMS-Code ist 5 Minuten gültig. Sind die 5 Minuten überschritten, muss der Login-Vorgang wiederholt werden.



Ohne Zugriff auf die verifizierte Telefonnummer kann keine Anmeldung an der AirKey-Onlineverwaltung erfolgen. Sollten Sie die Telefonnummer ändern wollen, müssen Sie die Telefonnummer in den Details des Administrators ändern (siehe [Administrator bearbeiten](#)). Dazu ist jedoch die aktuell verifizierte Telefonnummer notwendig. Wenn die Telefonnummer nicht mehr verfügbar ist, wenden Sie sich bitte an den [EVVA-Support](#).

5.1.3 Passwort vergessen

Wenn Sie Ihr Passwort vergessen haben, können Sie es selbstständig zurücksetzen. Klicken Sie auf **Passwort vergessen**

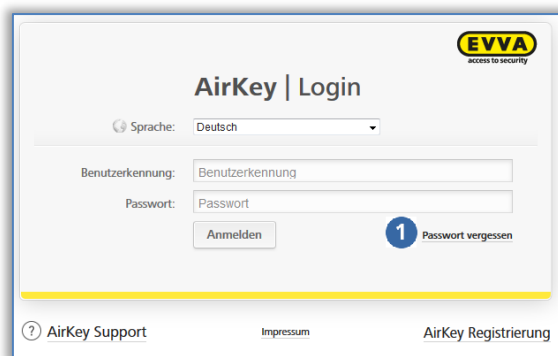


Abbildung 93: Login-Seite der AirKey-Onlineverwaltung

- > Im Dialogfenster "Passwort vergessen?" geben Sie Ihre Benutzerkennung und das bei der Registrierung angegebene Geburtsdatum ein und klicken Sie auf **Passwort zurücksetzen**.

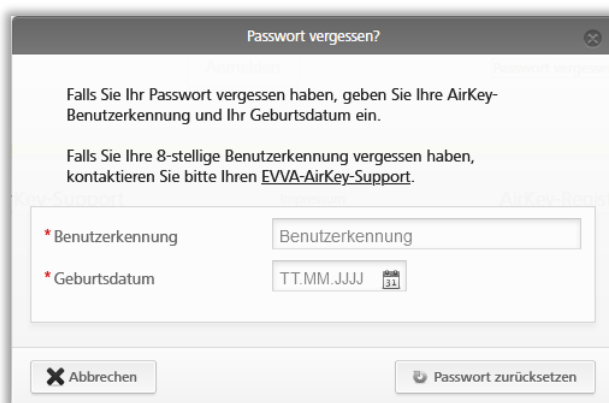


Abbildung 94: Passwort vergessen

- > Bei aktivierter Zwei-Faktor-Authentifizierung erhalten Sie einen SMS-Code an Ihr verifiziertes Smartphone, der im nachfolgenden Dialog eingegeben und mit **Passwort zurücksetzen** bestätigt werden muss. (Dieser Schritt entfällt, wenn die Zwei-Faktor-Authentifizierung nicht aktiviert oder die Telefonnummer nicht verifiziert ist.)

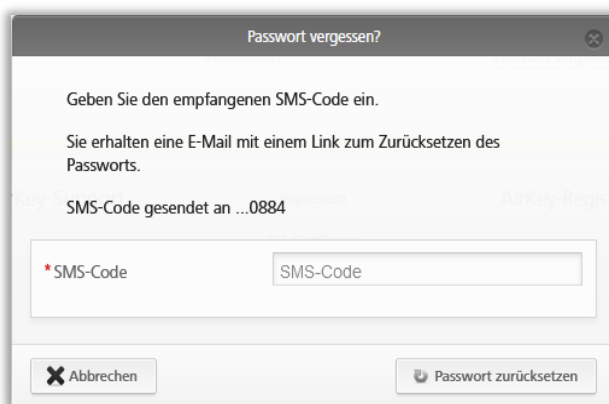


Abbildung 95: SMS-Code bei "Passwort vergessen"



Der SMS-Code ist 5 Minuten gültig. Sind die 5 Minuten überschritten, muss der Vorgang wiederholt werden.



Ohne Zugriff auf die verifizierte Telefonnummer kann der Vorgang nicht abgeschlossen werden. Wenn die Telefonnummer nicht mehr verfügbar ist, wenden Sie sich bitte an den [EVVA-Support](#).

Sie erhalten eine automatisch generierte E-Mail von *EVVA AirKey* mit dem Betreff "EVVA-AirKey-Onlineverwaltung – Zurücksetzen Ihres Passworts".

- > Öffnen Sie die E-Mail von *EVVA AirKey*.
- > Klicken Sie innerhalb der E-Mail auf den Link zum Passwort zurücksetzen, es öffnet sich die Webseite "Passwort zurücksetzen".
- > Geben Sie Ihr neues Passwort ein und wiederholen Sie das Passwort.
- > Klicken Sie auf **Passwort speichern**.

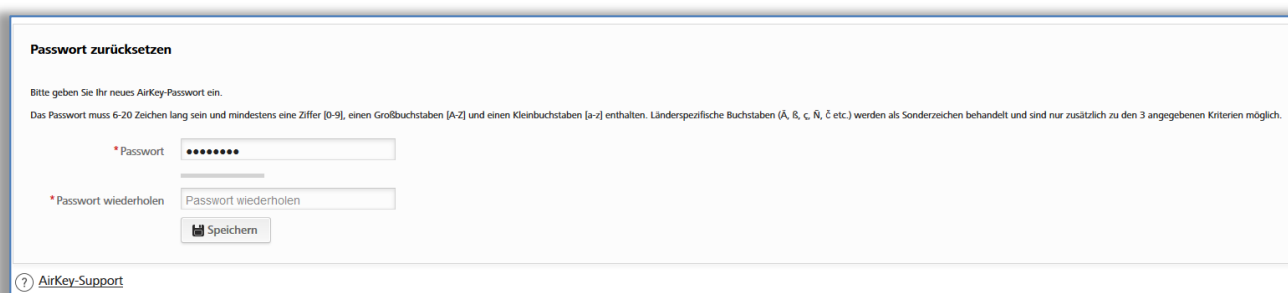


Abbildung 96: AirKey-Passwort zurücksetzen

Sie gelangen zur Login-Seite der [AirKey-Onlineverwaltung](#).

- > Führen Sie den Login wie in [AirKey-Login ohne Zwei-Faktor-Authentifizierung](#) oder [AirKey-Login mit Zwei-Faktor-Authentifizierung](#) beschrieben, mit dem neuen Passwort, durch.

Wenn Ihre Eingaben korrekt sind, öffnet sich die Startseite **Home** der AirKey-Onlineverwaltung. Rechts oben sehen Sie den Namen des eingeloggten Benutzers.



Bei Bedarf können Sie Ihr Passwort auch in der AirKey-Onlineverwaltung ändern. Klicken Sie hierzu in der rechten Kopfzeile der AirKey-Onlineverwaltung auf den Administratornamen und nutzen Sie die Funktion **Passwort ändern**.

Abbildung 97: Mein AirKey-Account

5.2 AirKey-Logout

Um die Sitzung in der AirKey-Onlineverwaltung zu beenden, klicken Sie auf **Abmelden** 1.

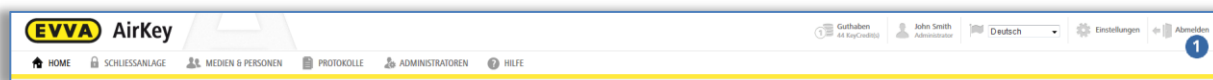


Abbildung 98: AirKey-Onlineverwaltung – Abmelden



Trotz des automatischen Logouts nach 30 Minuten wird dringend empfohlen, dass sich der Administrator nach Abschluss der durchzuführenden Tätigkeiten in der AirKey-Onlineverwaltung immer über **Abmelden** ausloggt.

5.3 Administratoren

Zur Verwaltung des AirKey-Systems gibt es zwei Rollen für Administratoren: **Systemadministratoren** und **Sub-Administratoren**.

Systemadministratoren haben alle Rechte zur Verwaltung der gesamten AirKey-Schließanlage und können auch weitere Administratoren anlegen, bearbeiten und löschen.

Sub-Administratoren besitzen eingeschränkte Rechte und dienen hauptsächlich zur Personen- und Berechtigungsverwaltung. Zusätzlich können **Sub-Administratoren** auch nur für bestimmte Bereiche und Schließkomponenten der AirKey-Schließanlage eingeschränkt

werden. Das bedeutet, dass sie nur Zutrittsberechtigungen für Schließkomponenten und Bereiche erstellen und bearbeiten können, für die sie auch berechtigt sind.



Es muss zumindest ein Systemadministrator pro Schließanlage vorhanden sein.

Die Funktionen der Administratorverwaltung finden Sie im Hauptmenü **Administratoren** .

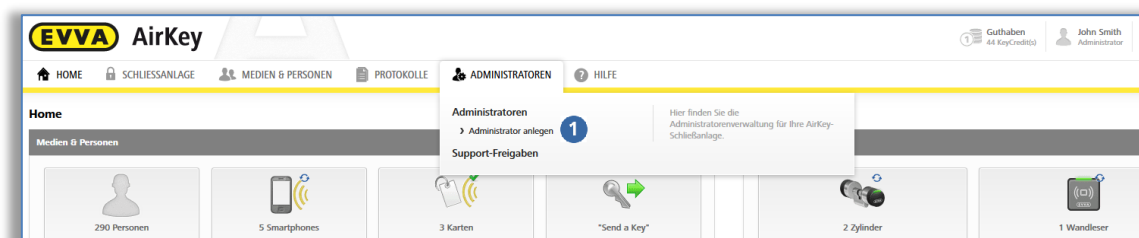


Abbildung 99: Hauptmenü – Administratoren

5.3.1 Administrator anlegen

Administratoren können ausschließlich von Systemadministratoren angelegt werden.

- > Wählen Sie im Hauptmenü **Administratoren** → **Administrator anlegen**.
- > Wählen Sie, ob es sich um die Rolle eines **Systemadministrators** oder **Sub-Administrators** handelt.

Abbildung 100: Details eines Administrators

- > Füllen Sie die Formularfelder aus.
Felder, die mit * gekennzeichnet sind, sind Pflichtfelder.
- > Im Block "Kontaktinformationen" können Sie noch angeben, ob der Administrator E-Mail-Benachrichtigungen zu bestimmten Ereignissen, wie zum Beispiel offene Wartungsaufgaben, anstehende Wartungsfenster oder weitere wichtige Informationen erhalten soll. Die E-Mail-Benachrichtigungen werden in der gewählten Sprache für Korrespondenz gesendet.

Abbildung 101: Kontaktinformationen

- > Klicken Sie auf **Speichern** 1.

Abbildung 102: Administrator anlegen



Kontrollieren Sie vor dem Speichern nochmals die E-Mail-Adresse, an die der Aktivierungslink nach Bestätigung gesendet wird.

- > Um den Vorgang abzuschließen, bestätigen Sie die Sicherheitsabfrage mit **Administrator anlegen**.

Abbildung 103: Administrator anlegen



Das Anlegen eines Administrators wird mit der Erfolgsmeldung "Der Administrator wurde gespeichert" angezeigt.

Der von Ihnen angelegte Administrator erhält nun eine E-Mail von *EVVA AirKey* mit einem Aktivierungslink. Für **Sub-Administratoren** können Sie erst jetzt die Rechte verwalten. Details zur Rechteverwaltung von Sub-Administratoren finden Sie im Folgekapitel [Administrator bearbeiten](#).



Wird der Aktivierungslink nicht innerhalb von 48 Stunden aufgerufen, werden die Daten gelöscht und der Aktivierungslink verliert seine Gültigkeit.

Der von Ihnen angelegte Administrator muss seine Registrierung wie folgt abschließen:

- > E-Mail mit dem Betreff "EVVA-AirKey-Registrierung" öffnen.
- > Aktivierungslink anklicken – es öffnet sich die Webseite "Willkommen bei AirKey!"
- > Selbst gewähltes Passwort eingeben, Passwort wiederholen und Geburtsdatum eintragen.
- > Klicken Sie auf **Speichern**.

Das Anlegen des Administrators ist damit abgeschlossen. Im Anschluss wird man auf die Login-Seite der [AirKey-Onlineverwaltung](#) weitergeleitet, auf der sich der neue Administrator anmelden kann.

5.3.2 Administrator bearbeiten


Nur **Systemadministratoren** können Details, wie z.B. Nachname, E-Mail-Adresse, Telefonnummer oder Kontaktinformationen eines Administrators nachträglich ändern. Auch die Rolle kann nachträglich bearbeitet werden. Beachten Sie aber bitte, dass zumindest ein **Systemadministrator** pro Schließanlage vorhanden sein muss.



Die Benutzerkennung kann nicht geändert werden.

- > Wählen Sie im Hauptmenü **Administratoren** → **Administratoren**.
Es wird die Liste mit allen gültigen Administratoren angezeigt.

In der angezeigten Liste können Sie nach Administratoren suchen, die Spalten sortieren, die angezeigten Einträge pro Seite einschränken und die Liste in eine CSV-Datei exportieren.

- > Klicken Sie auf den Administrator, dessen Detaildaten Sie ändern möchten.
- > Ändern Sie die gewünschten Daten.
- > Klicken Sie auf **Speichern** .

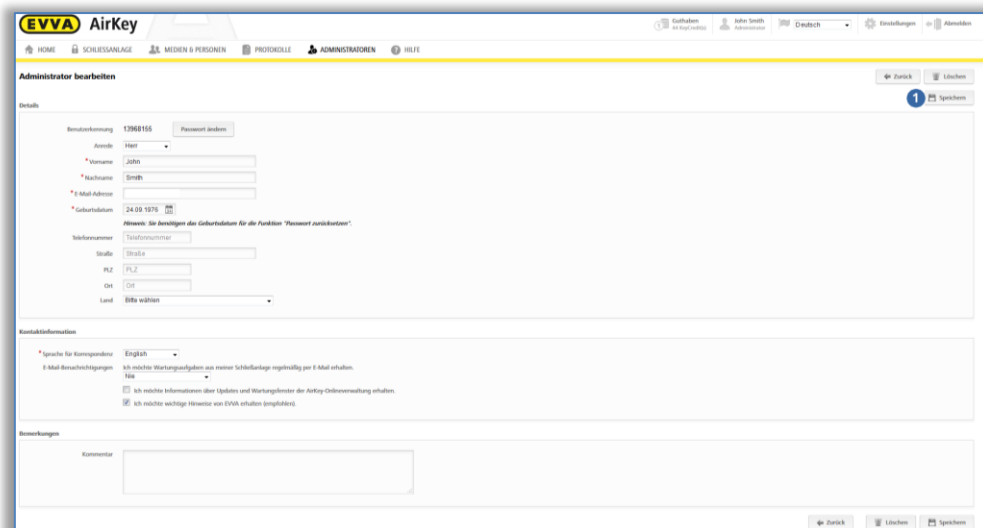


Abbildung 104: Administrator bearbeiten

Um die Rechte von **Sub-Administratoren** zu verwalten, führen Sie folgende Schritte aus:

- > Wählen Sie im Hauptmenü **Administratoren** → **Administratoren**. Es wird die Liste mit allen gültigen Administratoren angezeigt.
- > Klicken Sie auf den **Sub-Administrator**, dessen Rechte Sie ändern möchten.
- > Wechseln Sie in den Reiter **Rechte verwalten**.
- > Durch Markieren der Checkboxen können Sie wählen, welche Bereiche und Schließkomponenten der Sub-Administrator verwalten und Berechtigungen für sie vergeben darf.

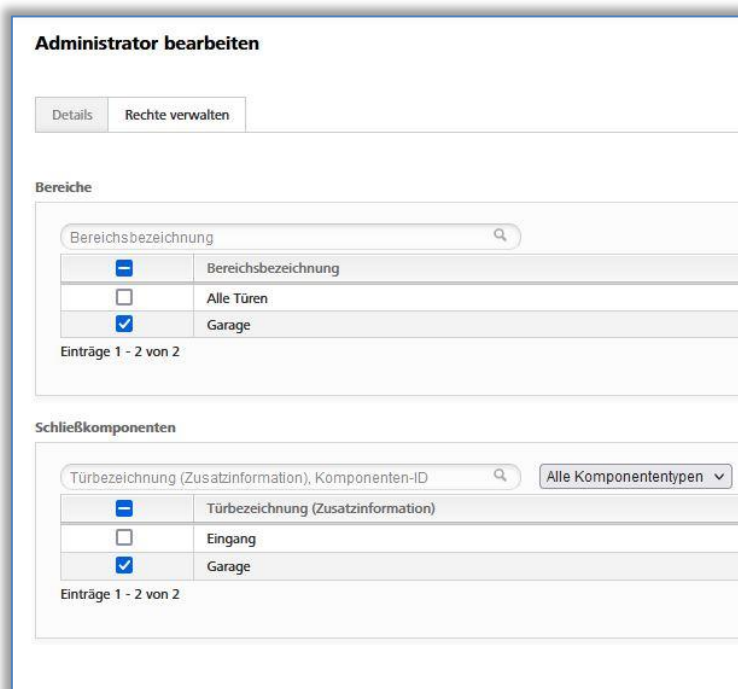


Abbildung 105: Rechte eines Sub-Administrators verwalten

- > Klicken Sie auf **Speichern**.

Bereiche und Schließkomponenten, für die ein **Sub-Administrator** keine Rechte besitzt, stehen dem **Sub-Administrator** bei der Berechtigungsvergabe nicht zur Verfügung. Einem **Systemadministrator** stehen immer alle Bereiche und Schließkomponenten für die Berechtigungsvergabe zur Verfügung.

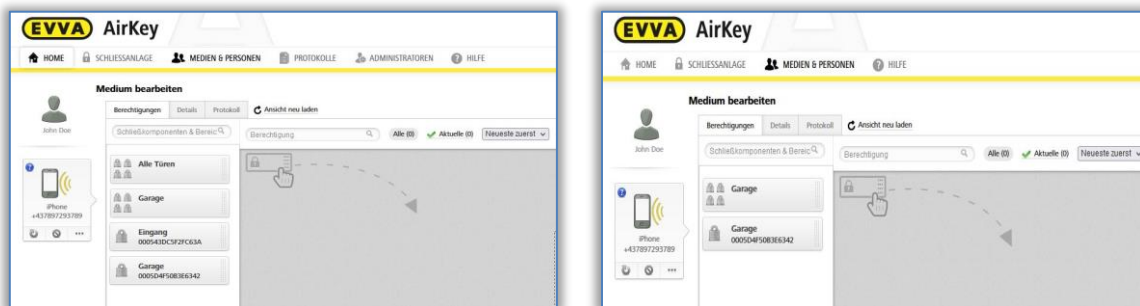


Abbildung 106: Vergabe von Berechtigungen durch einen Systemadministrator bzw. durch einen Sub-Administrator



Die Rechteverwaltung für **Sub-Administratoren** bezieht sich nur auf Bereiche und Schließkomponenten. **Sub-Administratoren** sehen immer alle Personen und Medien.

5.3.3 Administrator löschen

Ein Administrator kann nur durch einen anderen Systemadministrator gelöscht werden.

- > Klicken Sie im Hauptmenü auf **Administratoren** → **Administratoren**.
- > Wählen Sie den zu löschenden Administrator aus, indem Sie die entsprechende Zeile in der Tabelle anklicken. Sie gelangen zur Seite "Administrator bearbeiten".
- > Klicken Sie auf **Löschen**

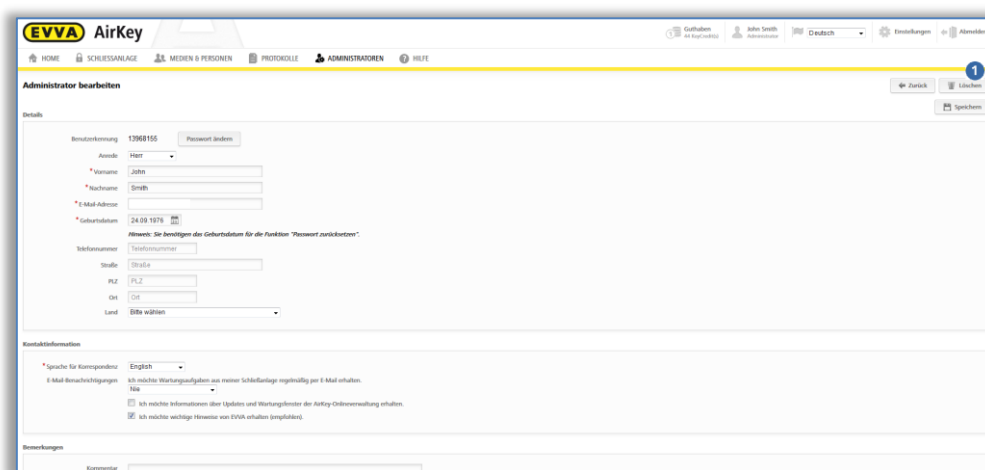


Abbildung 107: Administrator löschen

- > Bestätigen Sie die Sicherheitsabfrage mit **Administrator löschen**.

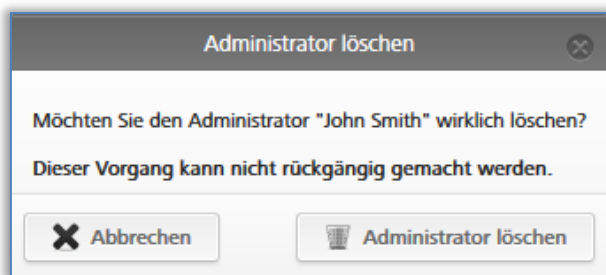


Abbildung 108: Administrator löschen



Das Löschen des Administrators wird mit der Erfolgsmeldung "Der Administrator wurde gelöscht" angezeigt. Der gelöschte Administrator erscheint nicht mehr in der Liste der Administratoren und kann sich nicht mehr in der AirKey-Onlineverwaltung anmelden.



Wenn das **Vier-Augen-Prinzip für die Protokolleinsicht** aktiviert ist, müssen mindestens zwei Systemadministratoren übrig bleiben. Andernfalls wird beim Versuch, den Administrator zu löschen, eine Fehlermeldung angezeigt und der Administrator kann nicht gelöscht werden. Details zum **Vier-Augen-Prinzip für die Protokolleinsicht** finden Sie im Kapitel [Allgemein](#).

5.4 Einstellungen der AirKey-Schließanlage

In den Einstellungen der AirKey-Onlineverwaltung werden grundlegende Einstellungen eingerichtet.

- > Klicken Sie auf der Startseite **Home** auf die Kachel **Einstellungen**
- > Oder klicken Sie in der Kopfzeile auf **Einstellungen**.

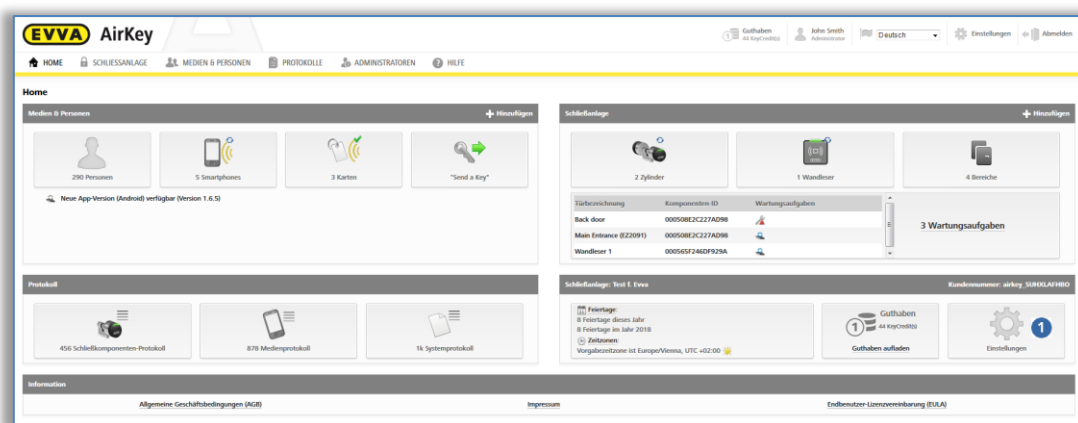


Abbildung 109: Einstellungen der AirKey-Schließanlage

5.4.1 Allgemein

In diesem Reiter können die folgenden allgemeinen Einstellungen für die gesamte Schließanlage aktiviert werden.

Bluetooth-Einstellungen für die AirKey-App

Hier kann für alle Smartphones dieser Schließanlage konfiguriert werden, ob das Öffnen von Schließkomponenten über Bluetooth aus dem Sperrbildschirm möglich ist, oder nicht. Wenn die Option nicht aktiviert ist, muss das Smartphone vor jedem Zutritt entsperrt werden.

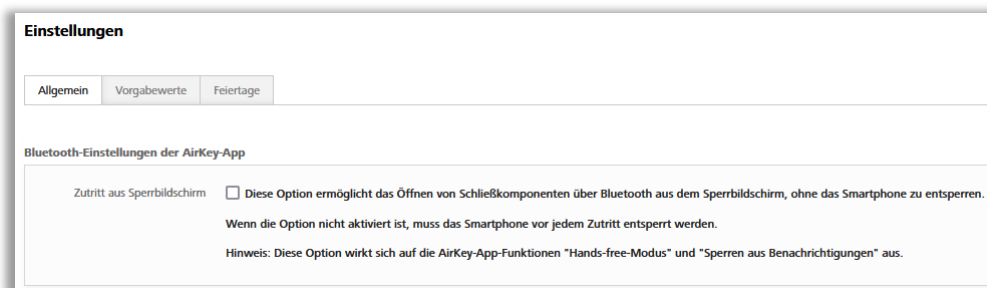


Abbildung 110: Allgemeine Einstellungen – Bluetooth-Einstellungen für die AirKey-App



Diese Option wirkt sich auf die App-Funktionen "Hands-free-Modus" und "Sperrungen aus Benachrichtigungen" aus.



Deaktivieren Sie **Zutritt aus Sperrbildschirm**, um die Sicherheit Ihrer Schließanlage zu erhöhen.

AirKey-App-Einstellungen

Hier kann die Option **Aktualisierung nach jedem Zutritt** aktiviert werden und der **Text für die "Send a Key"-SMS** konfiguriert werden.

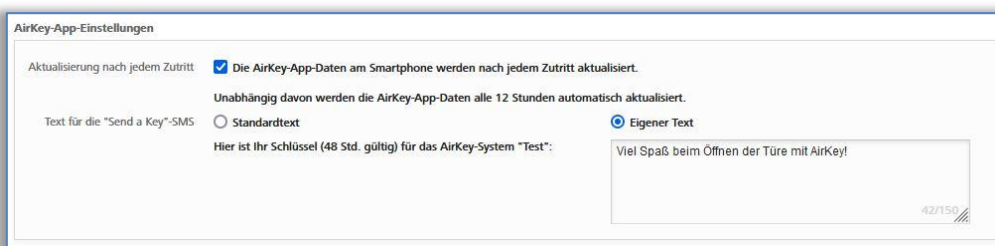


Abbildung 111: Allgemeine Einstellungen – AirKey-App-Einstellungen


Wenn die Option **Aktualisierung nach jedem Zutritt** aktiviert wird, werden die AirKey-App-Daten (zum Beispiel Protokolleinträge oder der Batteriestatus von Schließkomponenten) bei jedem Zutritt mit einem Smartphone aktualisiert.

- > Wählen Sie dazu die entsprechende Checkbox an und bestätigen Sie mit **Speichern**.



Abbildung 112: AirKey-App-Einstellungen – Aktualisierung nach jedem Zutritt

Die Funktionalität wird dann mittels Push-Benachrichtigung an alle Smartphones dieser Schließanlage gesendet. Spätestens nach einer manuellen Aktualisierung der AirKey-App-Daten des Smartphones (siehe Kapitel [Smartphone aktualisieren](#)), sollte die Funktionalität

am Smartphone aktiv sein. Den aktuellen Status  des Smartphones zu dieser Funktion finden Sie in der AirKey-Onlineverwaltung in den Details des Smartphones.

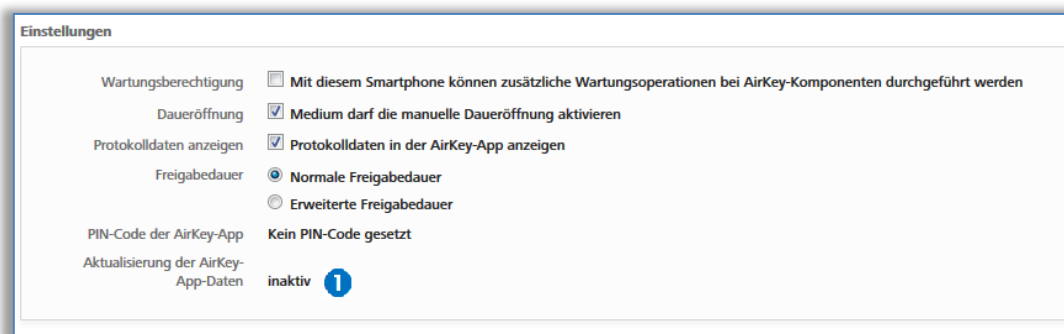


Abbildung 113: Status der Option "Aktualisierung nach jedem Zutritt"



Aktivieren Sie diese Funktion, um bei der Verwendung von Smartphones die Zutritte nahezu in Echtzeit an die AirKey-Onlineverwaltung zu übertragen.



Die Aktualisierung der AirKey-App-Daten nach einem Zutritt überträgt nur die Daten jenes Smartphones, das den Zutritt durchgeführt hat. Am Smartphone selbst wird diese Aktualisierung nicht visuell angezeigt.



Für diese Funktion ist eine stabile Internetverbindung (mobile Daten oder WLAN) notwendig, da ein weiterer Zutritt erst nach abgeschlossener Aktualisierung der AirKey-App-Daten durchgeführt werden kann.



Unabhängig von der Option "Aktualisierung nach jedem Zutritt" wird alle 12 Stunden versucht, die AirKey-App-Daten automatisch zu aktualisieren.

Es besteht auch die Möglichkeit, hier den **Text für die "Send a Key"-SMS** zu konfigurieren.

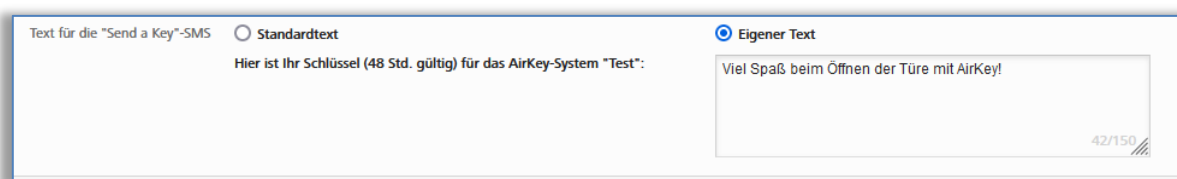


Abbildung 114: AirKey-App-Einstellungen – Text für die "Send a Key"-SMS

Dabei kann zwischen dem Standardtext und einem selbst definierbaren Text gewählt werden. Wählen Sie **Standardtext**, um den vordefinierten Text «Hier ist Ihr Schlüssel (48 Std. gültig) für das AirKey-System "<Name der Schließanlage>» zu verwenden oder wählen Sie **Eigener Text**, um im entsprechenden Textfeld einen selbst definierten Text zu verwenden. Bestätigen Sie die Auswahl anschließend mit **Speichern**.

Wird ein eigener Text verwendet, so kann dieser noch zusätzlich bei jeder "Send a Key"-Aktion angepasst werden, um zum Beispiel eine personalisierte Anrede zu verwenden. Details zu "Send a Key" finden Sie im Kapitel [Funktion "Send a Key"](#).



Der eigene Text ist auf maximal 150 Zeichen limitiert. Zusätzlich wird der eigene Text nicht in andere Sprachen übersetzt, wenn eine Person eine andere Korrespondenzsprache ausgewählt hat. Stattdessen wird der Standardtext automatisch in die Korrespondenzsprache der Person übersetzt.



Verwenden Sie einen selbst definierten Text, um die Smartphone-Besitzer persönlich anzusprechen und Ihnen mitzuteilen, für welche Schließanlage sie Berechtigungen erhalten.

Sicherheitsoptionen

In den Sicherheitsoptionen können Sie die Funktionen **Smartphonetausch**, **Zwei-Faktor-Authentifizierung (2FA)** und **Vier-Augen-Prinzip für die Protokolleinsicht** konfigurieren.

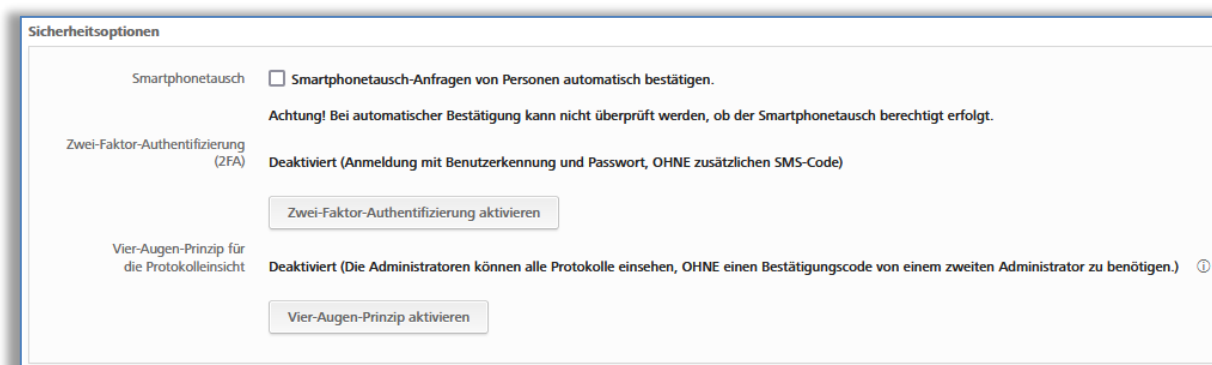


Abbildung 115: Allgemeine Einstellungen – Sicherheitsoptionen

Mit der Checkbox **Smartphonetausch-Anfragen von Personen automatisch bestätigen** können Tauschaktionen, die über ein Smartphone gestartet wurden, automatisch bestätigt werden.



Damit wird jeder Smartphonetausch, der über das Smartphone gestartet wurde, sofort automatisch bestätigt, wenn ausreichend Guthaben vorhanden ist. Bedenken Sie, dass bei jedem Smartphonetausch, bei dem Berechtigungen übertragen werden, ein KeyCredit abgebucht wird. Weitere Details zum Smartphonetausch finden Sie im Kapitel [Smartphonetausch](#).

Die **Zwei-Faktor-Authentifizierung**, oder auch **2FA**, dient als zusätzliche Sicherheitsstufe bei der Anmeldung zur AirKey-Onlineverwaltung. Dabei wird neben der Benutzerkennung und Passwort ein zusätzlicher SMS-Code bei der Anmeldung, als zweiter Faktor, abgefragt. Wird die Zwei-Faktor-Authentifizierung in den Einstellungen aktiviert, so wird diese bei allen Administratoren dieser Schließanlage angewendet.

- > Zum Aktivieren klicken Sie auf den Button **Zwei-Faktor-Authentifizierung aktivieren**.

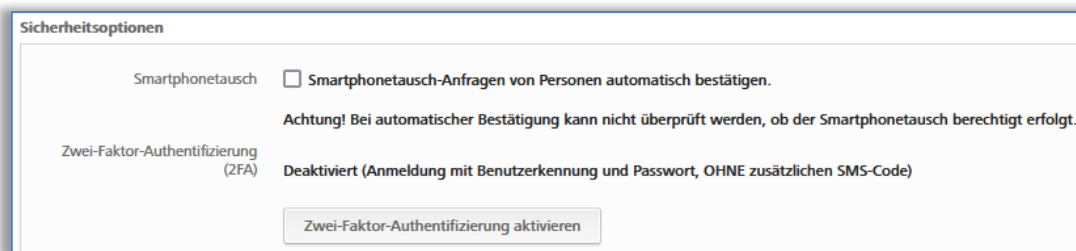


Abbildung 116: Allgemeine Einstellungen – Zwei-Faktor-Authentifizierung (2FA)

- > Tragen Sie die Mobiltelefonnummer ein, die für die Zwei-Faktor-Authentifizierung für den aktuell angemeldeten Administrator verwendet werden soll und klicken Sie auf **SMS-Code senden**.

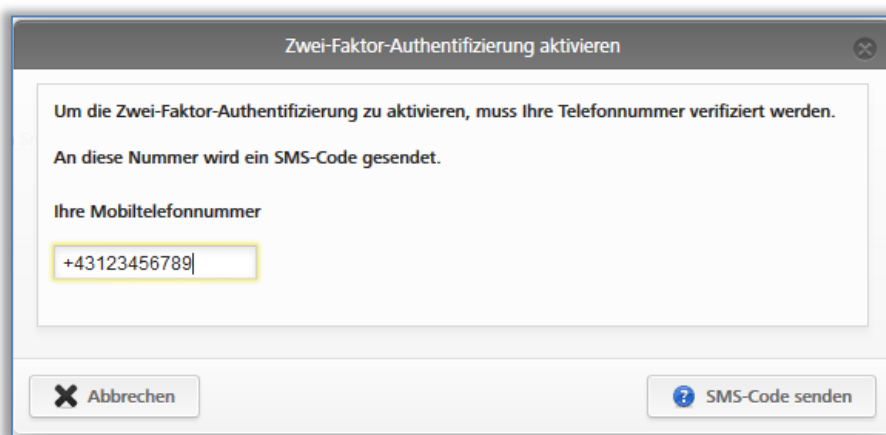


Abbildung 117: Verifizierung der Mobiltelefonnummer in den Einstellungen

- > Es wird ein SMS-Code an die zuvor angegebene Telefonnummer gesendet. Dieser SMS-Code muss im Dialog innerhalb der AirKey-Onlineverwaltung eingegeben und mit **Speichern** bestätigt werden.



Abbildung 118: SMS-Code eingeben Einstellungen

Wenn ein gültiger SMS-Code verwendet wurde, ist die Zwei-Faktor-Authentifizierung für alle Administratoren der Schließanlage aktiviert. Der Status in den Einstellungen ändert sich entsprechend.



Der SMS-Code ist 5 Minuten gültig. Sind die 5 Minuten überschritten, muss der Vorgang wiederholt werden.



Ab dem Zeitpunkt der Aktivierung ist für jeden Login ein Mobiltelefon notwendig. Details zum Login-Vorgang mit aktivierter Zwei-Faktor-Authentifizierung finden Sie im Kapitel [AirKey-Login mit Zwei-Faktor-Authentifizierung](#).

Zum Deaktivieren der Zwei-Faktor-Authentifizierung befolgen Sie bitte folgende Schritte:

- > Klicken Sie auf **Zwei-Faktor-Authentifizierung deaktivieren**.

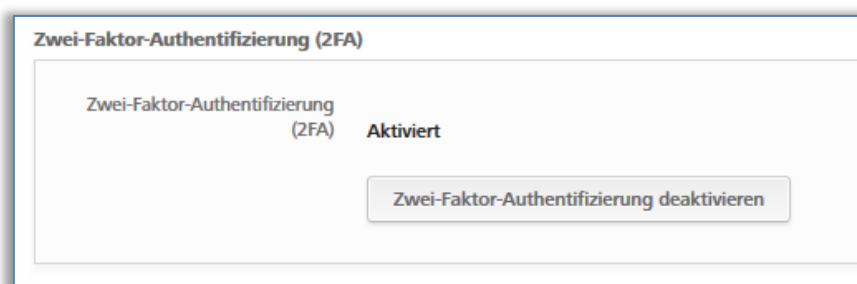


Abbildung 119: Zwei-Faktor-Authentifizierung deaktivieren

- > Bestätigen Sie die Abfrage ebenfalls mit **Zwei-Faktor-Authentifizierung deaktivieren**.

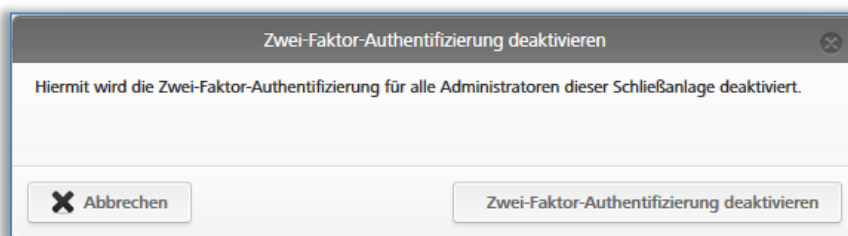


Abbildung 120: Dialog "Zwei-Faktor-Authentifizierung deaktivieren"

Die Funktion ist wieder für alle Administratoren der Schließanlage deaktiviert.

Mit der Funktion **Vier-Augen-Prinzip für die Protokolleinsicht** haben Sie die Möglichkeit, das Schließkomponenten- und Medienprotokoll nur einzusehen, wenn ein zweiter Systemadministrator die Einsicht bestätigt. Damit sind personenbezogene Daten noch besser vor Einsicht geschützt.



Um das **Vier-Augen-Prinzip für die Protokolleinsicht** zu aktivieren, müssen mindestens 2 Systemadministratoren vorhanden sein.

Zum Aktivieren des **Vier-Augen-Prinzips für die Protokolleinsicht** befolgen Sie bitte folgende Schritte:

- > Klicken Sie auf **Vier-Augen-Prinzip aktivieren**.

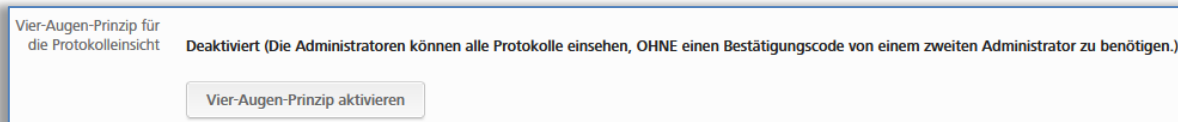


Abbildung 121: Vier-Augen-Prinzip aktivieren

- > Wählen Sie einen zweiten Systemadministrator aus der Liste aus, dem ein Bestätigungscode per E-Mail gesendet werden soll, und klicken Sie auf **Bestätigungscode senden**.

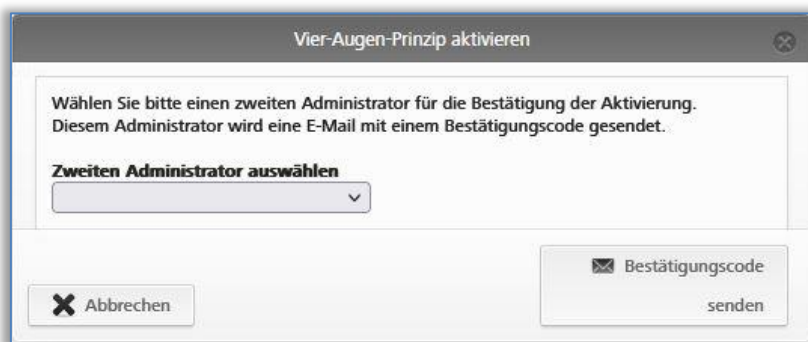


Abbildung 122: Vier-Augen-Prinzip aktivieren – zweiten Administrator auswählen

- > Daraufhin wird eine E-Mail mit einem Bestätigungscode an den ausgewählten Systemadministrator gesendet.
- > Dieser Bestätigungscode muss innerhalb von 10 Minuten in der AirKey-Onlineverwaltung eingegeben und mit **Aktivieren** bestätigt werden.

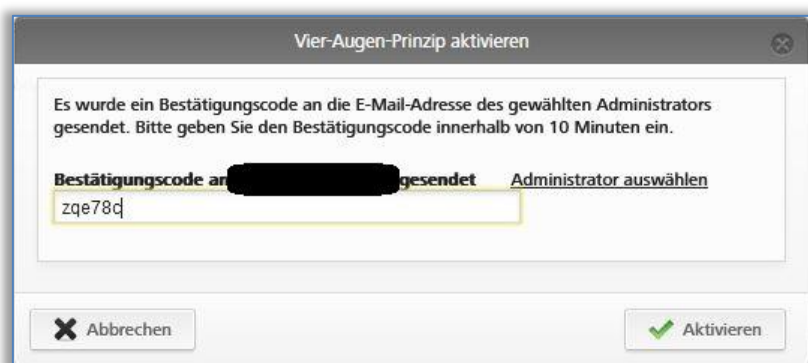


Abbildung 123: Vier-Augen-Prinzip aktivieren – Bestätigungscode eingeben

Wird dieser Vorgang nicht innerhalb von 10 Minuten abgeschlossen, muss der Vorgang wiederholt werden. Wenn der gewählte Systemadministrator nicht reagiert, kann über den Link **Administrator auswählen** auch ein anderer Systemadministrator zum Aktivieren des Vier-Augen-Prinzips ausgewählt werden.

Damit haben Sie das **Vier-Augen-Prinzip für die Protokolleinsicht** für alle Administratoren dieses AirKey-Systems aktiviert. Ab dem nächsten Login eines Systemadministrators können das Schließkomponenten- und Medienprotokoll nicht ohne die Bestätigung eines zweiten Systemadministrators eingesehen werden.



Das Systemprotokoll kann weiterhin eingesehen werden und unterliegt nicht dem Vier-Augen-Prinzip. Sub-Administratoren können keine Protokolle einsehen.

Zum Deaktivieren des **Vier-Augen-Prinzips für die Protokolleinsicht** folgen Sie dem gleichen Ablauf wie bei der Aktivierung.



Sowohl die Aktivierung als auch die Deaktivierung wird im Systemprotokoll gespeichert. Dabei werden auch beide involvierten Systemadministratoren inklusive der verwendeten E-Mail-Adresse protokolliert.

AirKey Cloud Interface (API)

Beim AirKey Cloud Interface handelt es sich um eine REST-Schnittstelle (API) für Drittsysteme. Die Schnittstelle erlaubt es, bestimmte Funktionen von AirKey über eine Drittsoftware zu steuern. Details zum AirKey Cloud Interface finden Sie im Kapitel [AirKey Cloud Interface \(API\)](#).

AirKey Cloud Interface (API) – Testumgebung

Die Testumgebung gibt Ihnen die Möglichkeit, das AirKey Cloud Interface (API) vor der Aktivierung in einem geschützten Umfeld mit Testdaten auszuprobieren. Die Details dazu finden Sie im Kapitel [AirKey Cloud Interface \(API\)](#).

5.4.2 Vorgabewerte (für alle neu hinzugefügten Schließkomponenten)

Diese Einstellungen werden bei neu hinzugefügten Schließkomponenten automatisch aktiviert. Gerade für größere Schließanlagen empfiehlt es sich, die Vorgabewerte vor der ersten Installation zu setzen, um damit die Administration der Anlage zu vereinfachen.

Uhrzeit und Kalender

In einer AirKey-Schließanlage können Sie Schließkomponenten verwalten, die sich in unterschiedlichen Zeitzonen befinden. Als Standardvorgabe ist die Zeitzone "Europe/Vienna" mit UTC+01:00 im Winter bzw. UTC+02:00 im Sommer geltend für Mitteleuropa, voreingestellt.

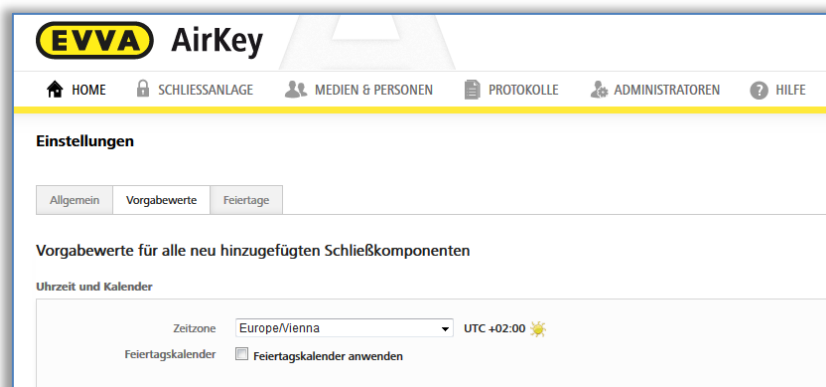


Abbildung 124: Vorgabewerte für neue Schließkomponenten

Wenn Sie die Zeitzone für die gesamte Schließanlage ändern wollen, dann klicken Sie einfach auf die Dropdown-Liste und wählen die korrekte Zeitzone aus der Liste aus.



Wenn Sie die Zeitzone für eine Schließkomponente ändern wollen, klicken Sie auf der Startseite **Home** auf die Kachel **Zylinder** bzw. **Wandleser**, wählen Sie die gewünschte Schließkomponente aus und gehen Sie zum Reiter **Einstellungen**. Unter dem Block **Uhrzeit und Kalender** finden Sie wieder die Dropdown-Liste mit den Zeitzonen.

Das Sonnensymbol bei der jeweiligen Zeitzone zeigt an, ob gerade die Sommer- oder Winterzeit aktiv ist:

- Gelbe Sonne = Sommerzeit
- Graue Sonne = Winterzeit

Wenn Sie das Häkchen bei **Feiertagskalender anwenden** setzen, dann werden die im Reiter **Feiertage** (siehe Kapitel [Feiertage](#)) hinterlegten und aktivierten Feiertage für die neue Schließkomponente übernommen.

Bereiche

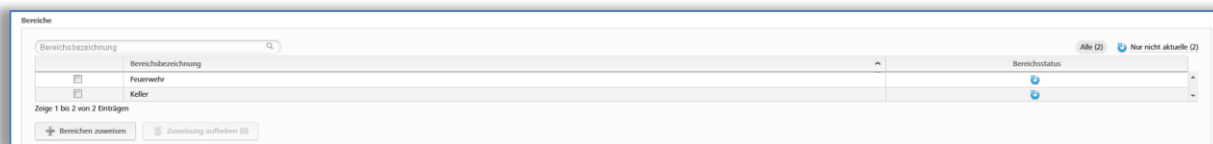


Abbildung 125: Vorgabewerte – Bereiche

In diesem Abschnitt können neue Schließkomponenten automatisch bereits angelegten Bereichen zugeordnet werden. Wo und wie man einen Bereich anlegt, wird im Kapitel [Bereich anlegen](#) genauer erklärt.

Das ist besonders für General- oder Feuerwehrschlüssel sinnvoll, die immer alle Komponenten sperren müssen. Zuweisungen zu Bereichen können bei den jeweiligen Schließkomponenten auch wieder aufgehoben werden.

Zutritt



Abbildung 126: Vorgabewerte – Zutritt

Hier können die manuelle und automatische Daueröffnung, die Freigabedauer, die Aktualisierung nach jedem Sperrvorgang und der Hands-free-Modus für Zylinder und Wandleser für alle neu hinzugefügten Schließkomponenten erlaubt werden.

Wird die Checkbox **Manuelle Daueröffnung erlauben** aktiviert, erscheint zusätzlich eine weitere Checkbox: **Automatische Daueröffnung aktivieren**.



Abbildung 127: Automatische Daueröffnung

Die automatische Daueröffnung erlaubt das Festlegen von Zeiträumen bzw. Schließzeitpunkten, bei denen die Schließkomponente automatisch öffnet oder schließt. Zum Beispiel wird in einem Büro jeden Abend die Daueröffnung um 17:00 Uhr automatisch beendet. Im Falle eines AirKey-Zylinders bedeutet das nicht, dass die Tür auch verriegelt wird, sondern nur, dass der Zylinder auskuppelt. Zum Verriegeln der Tür muss der Zylinder mit einem berechtigten Medium eingekuppelt und im Anschluss manuell verriegelt werden.

Auch das Festlegen eines Endzeitpunktes für die manuelle Daueröffnung kann in diesem Dialogfenster eingetragen werden. Damit ist gesichert, dass unabhängig von der Aktivierung der Daueröffnung, diese zum festgesetzten Zeitpunkt beendet wird (die roten Balken im unteren Screenshot). Pro Tag können maximal 4 Einträge (Zeiträume oder Endzeitpunkte) festgelegt werden.

Daueröffnungen werden an Feiertagen, bei "Batterie leer"-Warnungen, bei falscher Uhrzeit der Schließkomponenten oder auch bei einem Firmware-Update automatisch beendet oder erst gar nicht gestartet.

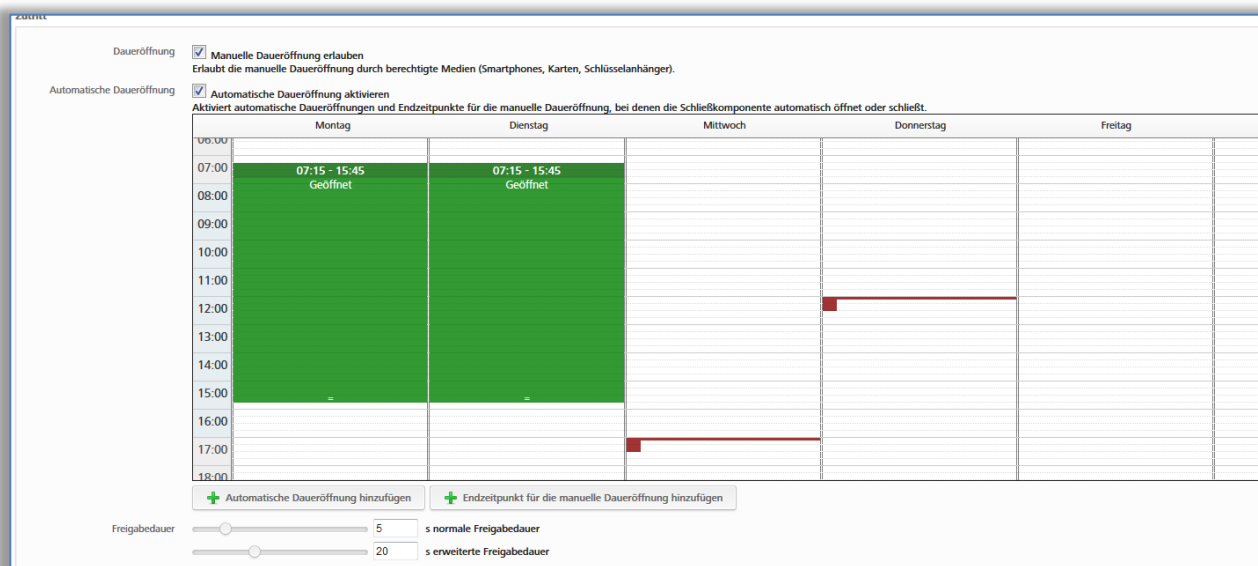


Abbildung 128: Automatische Daueröffnungen und Endzeitpunkte



Die manuelle Daueröffnung kann auch mit Zutrittsmedien aktiviert werden. Dabei wird das Medium an der Schließkomponente angehalten, kurz aus dem Lesebereich entfernt und nochmals innerhalb der Freigabedauer ein zweites Mal präsentiert. Die manuelle Daueröffnung kann auf diese Weise auch beendet werden.

Die **Freigabedauer** legt fest, wie lange die Freigabe der Schließkomponente bei einer Sperrung andauert (z.B. bei einem Zylinder heißt das, wie lange der Benutzer Zeit hat, um den Zylinderknopf manuell zu drehen). Standardmäßig beträgt die normale Freigabedauer 5 Sekunden, die erweiterte 20 Sekunden. Die Freigabedauer kann hier individuell angepasst werden, der Zeitraum reicht von 1 Sekunde bis 250 Sekunden.

Mit der Option **Aktualisierung nach jedem Sperrvorgang** kann aktiviert werden, ob die Schließkomponente nach jedem erfolgreichen Bluetooth-Sperrvorgang aktualisiert werden soll. Unabhängig davon wird die Schließkomponente jedes Mal aktualisiert, wenn sie mit einem Smartphone über Bluetooth gesperrt wird und seit der letzten vollständigen Aktualisierung mindestens 6 Stunden vergangen sind.

Diese Aktualisierung ist für den Anwender nicht merkbar. Es wird also weder ein Signal ausgegeben noch ein Hinweis am Smartphone angezeigt.

Der Administrator sieht die Aktion aber in den Protokollen der AirKey-Onlineverwaltung.

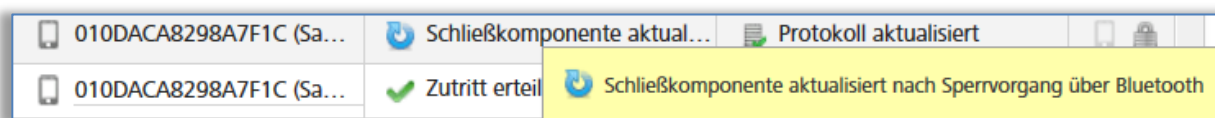


Abbildung 129: Protokollierung – Aktualisierung nach einem Sperrvorgang



Bei der Aktualisierung nach einem Bluetooth-Sperrvorgang werden nur folgende Daten aktualisiert:

- Blacklist
- Zeitzone
- Uhrzeit
- Protokolleinträge

Sofern die Schließkomponente noch weitere andere offene Wartungsaufgaben besitzt, muss diese wie im Kapitel [Schließkomponenten aktualisieren](#) beschrieben, aktualisiert werden.



Die Funktion ist abhängig von der Verbindungsqualität des Smartphones. Achten Sie deshalb auf eine stabile Internetverbindung ab 3G bzw. über WLAN.



Die Aktualisierung nach einem Bluetooth-Sperrvorgang wird auch beim Starten der manuellen Daueröffnung durchgeführt, jedoch nicht, wenn diese beendet wird.



Die Aktualisierung nach einem Bluetooth-Sperrvorgang passiert innerhalb der Freigabedauer der Schließkomponente. Bei einer Freigabedauer von weniger als 10 Sekunden funktioniert die Aktualisierung nach einem Bluetooth-Sperrvorgang möglicherweise nicht. Aus diesem Grund wird beim Aktivieren der Funktion auch automatisch der Wert der normalen Freigabedauer auf 10 Sekunden erhöht.



Die Aktivierung dieser Funktion erhöht den Batterieverbrauch bei batteriebetriebenen Schließkomponenten, wie zum Beispiel einem AirKey-Zylinder, und wirkt sich somit auf die Batterielebensdauer aus.

Die Optionen **Hands-free-Modus für Zylinder** und **Hands-free-Modus für Wandler** dienen dazu, den Hands-free-Modus für alle Komponenten des gewählten Komponententyps innerhalb der Schließanlage zu erlauben oder nicht zu erlauben. Zusätzlich kann auch bei jeder Schließkomponente individuell eingestellt werden, ob diese den Hands-free-Modus erlauben soll. Wie die Konfiguration bei einzelnen Schließkomponenten geändert werden kann, finden Sie im Kapitel [Schließkomponente bearbeiten](#).

Protokollierung

Wählen Sie den Vorgabewert für den Personenbezug in Protokolleinträgen von Zutrittsereignissen. Hierfür stehen drei Radiobuttons zur Auswahl:

Abbildung 130: Protokollierung definieren

Einsehbar lässt die Anzeige personenbezogener Daten von Zutrittsereignissen dauerhaft angezeigt.

Einsehbar für ... Tage anonymisiert die personenbezogenen Daten von Zutrittsereignissen nach der definierten Anzahl an Tagen.

Nicht einsehbar anonymisiert sämtliche personenbezogenen Daten von Zutrittsereignissen dauerhaft.



Die festgelegten Vorgabewerte können, unabhängig von den hier getätigten Einstellungen, für einzelne Schließkomponenten verändert werden.

Geänderte Vorgabewerte müssen mit dem Button **Speichern** gespeichert werden. Dazu erscheint eine Abfrage, ob die geänderten Vorgabewerte nur für neu hinzugefügte oder auf alle Schließkomponenten angewendet werden soll.

Abbildung 131: Geänderte Vorgabewerte speichern

5.4.3 Feiertage

Im Reiter **Feiertage** können Sie bis zu 80 Feiertage pro Jahr (aktuelles Jahr und zwei Folgejahre) definieren. Der Begriff "Feiertag" kann in AirKey sowohl ein gesetzlicher Feiertag als auch ein mehrtägiger Zeitraum, wie z.B. Betriebsurlaub oder Schulferien sein, die sich wiederholen können. Beispielsweise Nationalfeiertage oder Feiertage, die jedes Jahr zum gleichen Datum stattfinden, können Sie mit einer jährlichen Wiederholung versehen. Eine Woche Schulferien bedeutet nur 1 Feiertag, wenn er als Zeitraum mit "Start - Ende" definiert wurde.

Auswirkungen des Feiertagskalenders:

1. Periodische Zutrittsberechtigungen sind an Feiertagen nicht gültig.
2. Automatische Daueröffnungen werden an Feiertagen nicht berücksichtigt.

Damit der Feiertagskalender wirksam wird, müssen Sie ihn mithilfe des Buttons **Aktivieren** auf der rechten Seite global freischalten.

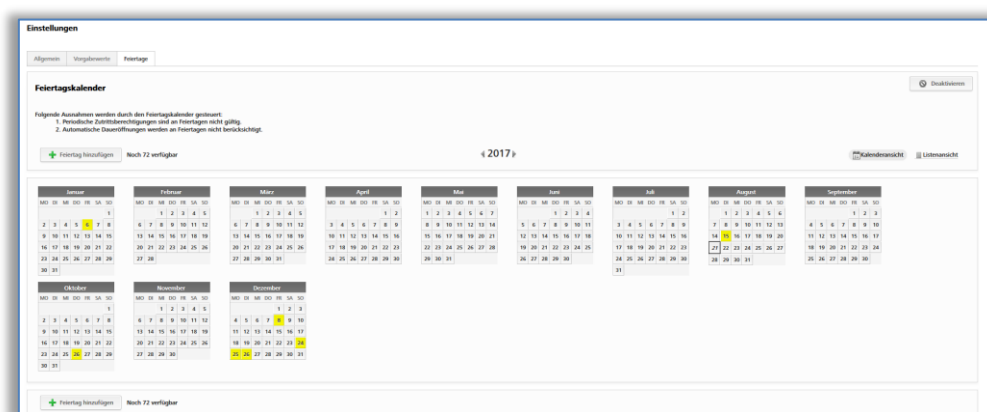


Abbildung 132: Feiertagskalender (Kalenderansicht)

Klicken Sie den Button **Feiertag hinzufügen** oder klicken Sie in der Kalenderansicht das genaue Datum des Feiertages aus (z.B. 24.12.), dann öffnet sich ein Dialogfenster, in dem Sie den Namen des Feiertages eintragen können, ob der Feiertag ganztags gilt, von wann bis wann der Feiertag dauert, z.B. nur am Nachmittag (hier können Sie z.B. auch Betriebsurlaube hinterlegen), wie oft er wiederholt wird und wann die Wiederholung endet.

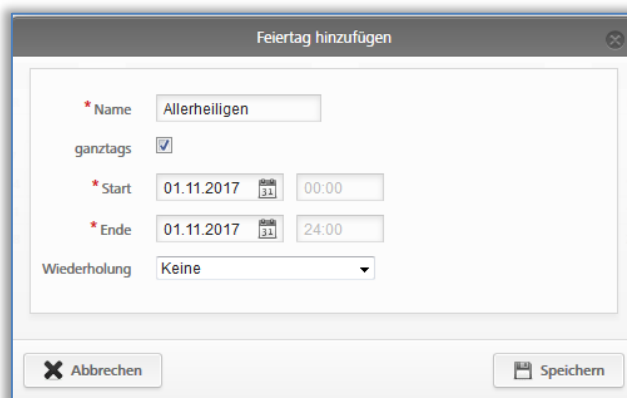


Abbildung 133: Feiertag hinzufügen

Jeder bereits eingetragene Feiertag kann im Nachhinein noch bearbeitet werden, klicken Sie dafür einfach auf den jeweiligen Tag und es öffnet sich eine Textblase.

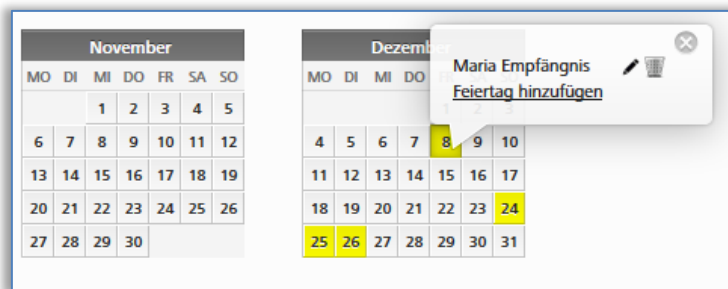


Abbildung 134: Feiertag hinzufügen über Kalender

Durch einen Klick auf den Link **Feiertag hinzufügen**, können Sie einen weiteren Feiertag an diesem Tag hinzufügen. Sie können an einem Kalendertag mehrere Feiertage eintragen. Durch einen Klick auf den Bleistift können Sie den Feiertag bearbeiten, durch einen Klick auf den Mistkübel können Sie den Feiertag löschen.

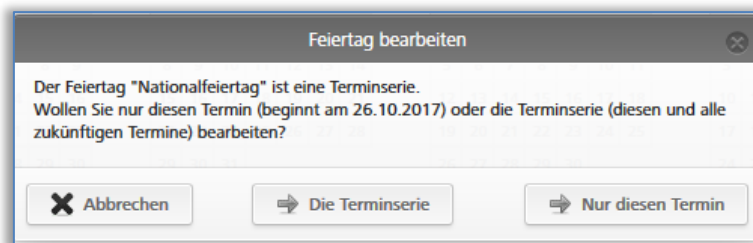


Abbildung 135: Feiertag bearbeiten

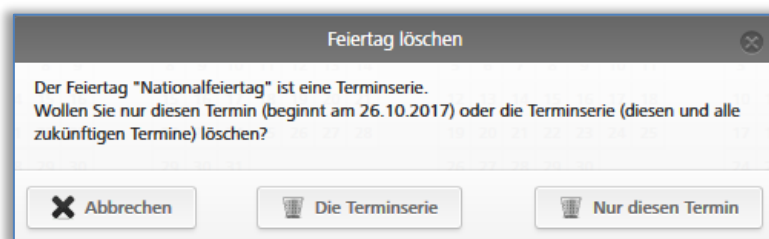


Abbildung 136: Feiertag löschen

Sobald Sie Termine, (Betriebs-)Urlaube oder Feiertage in den Kalender eingetragen haben, wird Ihnen in der Listenansicht eine Übersicht aller gespeicherten Feiertage etc. angezeigt.

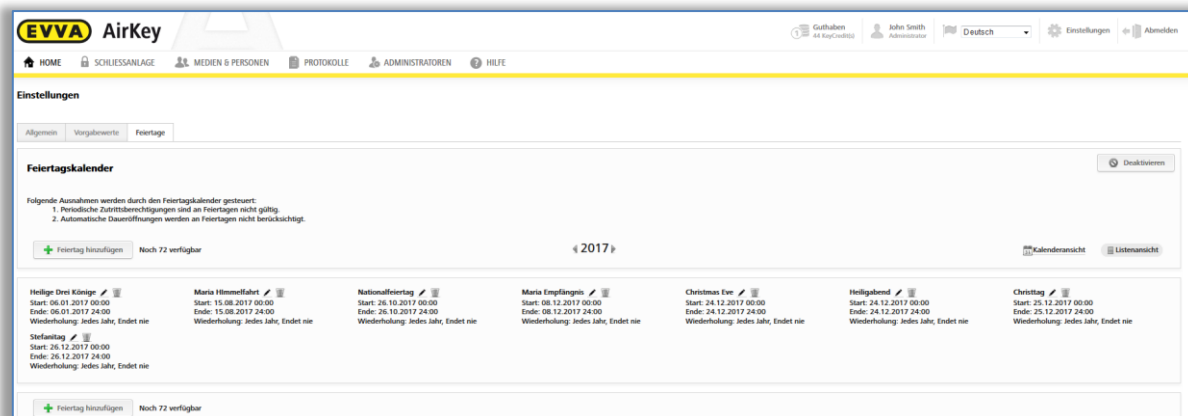


Abbildung 137: Feiertagskalender (Listenansicht)

Wenn Sie den Button **Deaktivieren** auswählen, dann wird der Feiertagskalender global für die Schließanlage deaktiviert und nicht für die hinzugefügten Schließkomponenten übernommen.

5.5 Schließanlage

Die Kacheln auf der Startseite **Home** bzw. die Menü- und Untermenüpunkte im Hauptmenü **Schließanlage** ermöglichen Ihnen die Verwaltung Ihrer AirKey-Schließanlage.

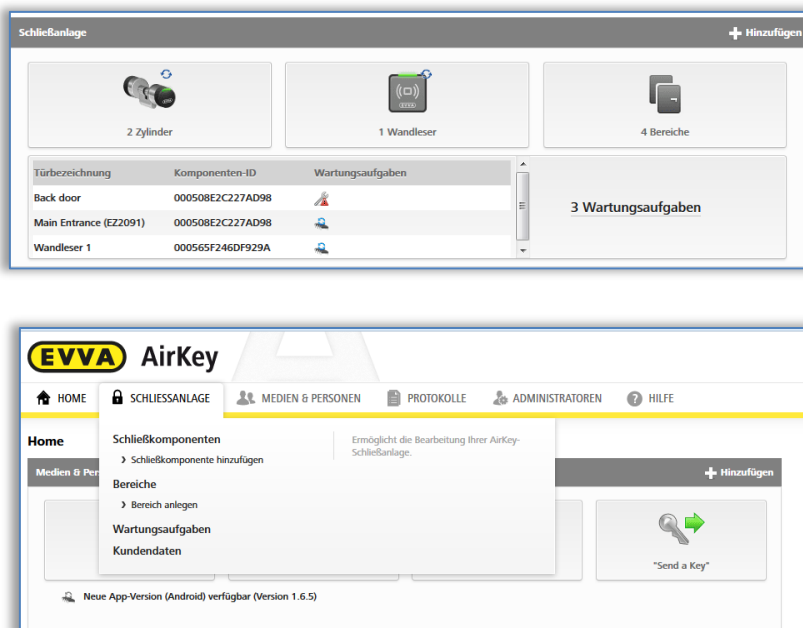


Abbildung 138: AirKey-Schließanlage

5.5.1 Übersicht der Schließkomponenten

Um eine Übersicht aller Schließkomponenten Ihrer AirKey-Schließanlage zu erhalten, klicken Sie auf der Startseite **Home** auf die Kachel **Zylinder** bzw. **Wandler**, oder im Hauptmenü **Schließanlage** → **Schließkomponenten**. Auf der Startseite **Home** sehen Sie auch auf den ersten Blick, wie viele Zylinder bzw. Wandler in Ihrer Schließanlage integriert sind.

Es werden alle Schließkomponenten mit Zusatzinformationen sowie deren Status aufgelistet. In der ersten Zeile der Liste finden Sie neben dem Suchfeld auch die Filterfunktionen für Schließkomponenten.

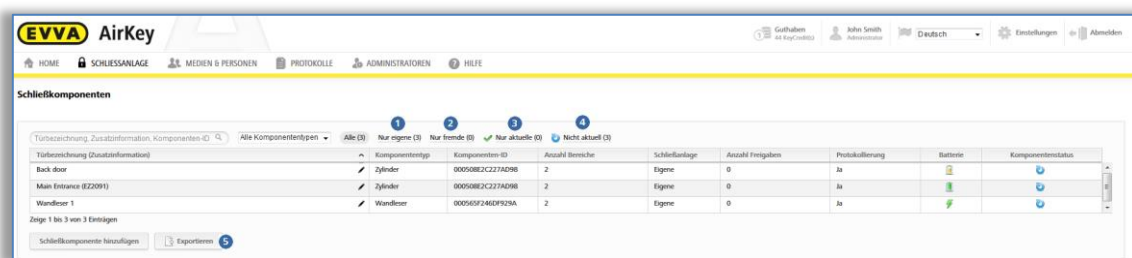


Abbildung 139: Schließkomponenten

- > "Nur eigene" ❶ listet nur die eigenen Schließkomponenten auf.
- > "Nur fremde" ❷ listet nur die von einem Administrator freigegebenen Schließkomponenten auf.
- > "Nur aktuelle" ❸ listet die Schließkomponenten auf, deren Status aktuell ist.
- > "Nicht aktuell" ❹ listet die Schließkomponenten auf, deren Status nicht aktuell ist.
- > Die Schließkomponentenliste kann in eine CSV-Datei zur weiteren Bearbeitung exportiert werden ❺.



AirKey bietet Ihnen die Möglichkeit, Schließkomponenten für eine fremde AirKey-Schließanlage freizugeben. In der Liste werden eigene und fremde Schließkomponenten unterschieden. Nähere Informationen dazu finden Sie im Kapitel [Schließkomponenten für andere Schließanlagen freigeben](#).

5.5.2 [Schließkomponente hinzufügen](#): Siehe Kapitel 4.11

5.5.3 Schließkomponente bearbeiten

Auf der Seite "Schließkomponente bearbeiten" finden Sie im Reiter **Details** verschiedene Informationen, wie z.B. Komponententyp und Modell, Komponenten-ID, Firmware-Version oder Komponentenstatus sowie Informationen zur Tür, zu Bereichen und Freigaben. Zusätzlich haben Sie hier die Möglichkeit, sich den Standort der Schließkomponente auf Google Maps anzeigen zu lassen. Im Reiter **Einstellungen** sehen Sie alle festgelegten Einstellungen zu Zeitzone und Feiertagskalender, Zutritt sowie Protokollierung und Reparaturoptionen.



Der angezeigte Batteriezustand entspricht dem Zustand zum Zeitpunkt der letzten Aktualisierung bzw. des letzten übermitteltem Protokolleintrags. Es kann daher sein, dass der tatsächliche Batteriezustand in der Schließkomponente vom Batteriestand, der in der AirKey-Onlineverwaltung angezeigt wird, abweicht.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** oder **Wandleser**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie auf den Listeneintrag der Schließkomponente, die Sie bearbeiten möchten.
- > Vergeben Sie im Reiter **Details** z.B. eine neue Türbezeichnung, eine optionale Zusatzinformation ❶ oder tragen den Standort bzw. die Adresse der Schließkomponente ein. Diese werden innerhalb der Schließanlage auf Eindeutigkeit überprüft.

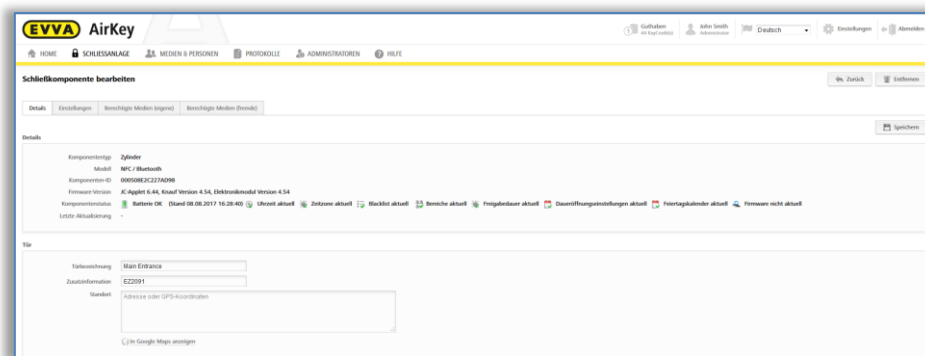


Abbildung 140: Schließkomponente bearbeiten

- > Bereichszuordnungen der ausgewählten Schließkomponente können im Block **Bereiche** bearbeitet werden.

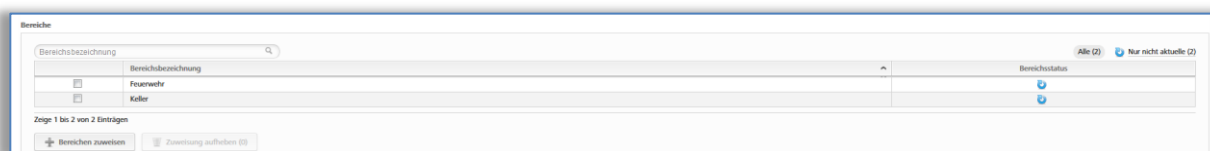


Abbildung 141: Bereiche

- > Optional können Sie die Schließkomponente für weitere Schließanlagen freigeben. Die entsprechenden Freigaben hierzu können Sie im Block **Freigaben** verwalten. Nähere Informationen zu Freigaben finden Sie im Kapitel [Arbeiten mit mehreren AirKey-Schließanlagen](#).

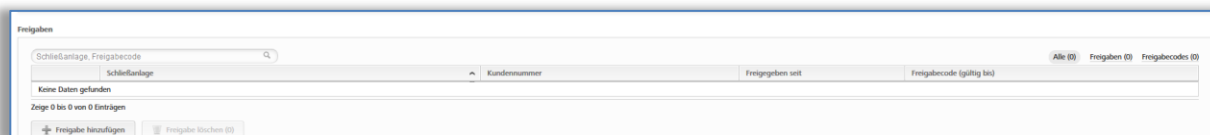


Abbildung 142: Freigaben

- > Optional können Sie einen Kommentar zu einer Schließkomponente im Block **Bemerkungen** eintragen.

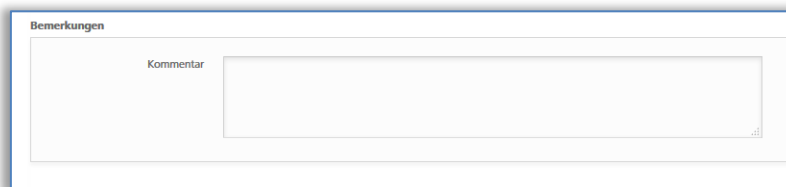


Abbildung 143: Schließkomponente bearbeiten

Im Reiter **Einstellungen** können Sie, wie bereits erwähnt, Optionen zu Zeitzonen und Feiertagskalender, Zutritte oder Protokollierung und Reparaturoptionen verwalten.

- > Bei Verwendung mehrerer Zeitzonen innerhalb einer Schließanlage kann jeder Schließkomponente eine eigene Zeitzone, die bereits in der AirKey-Onlineverwaltung angelegt und konfiguriert wurde, zugewiesen werden. Standardmäßig kommt die als Vorgabe eingestellte Zeitzone zur Anwendung.

- > Der Feiertagskalender kann hier für jede Schließkomponente ausgewählt oder abgewählt werden. Falls Sie Ihre Feiertageinstellungen nicht mehr genau im Kopf haben, gibt es hier einen direkten Link zum Feiertagskalender.

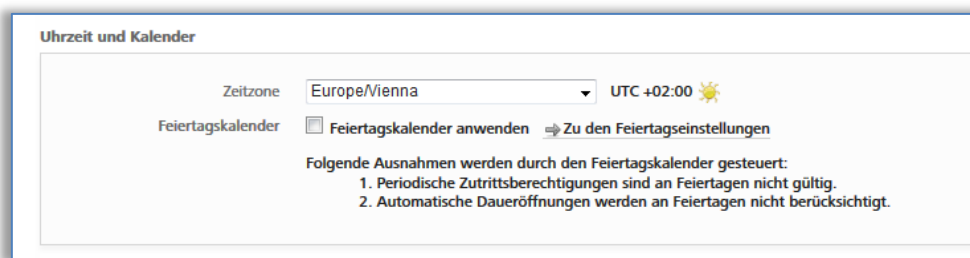


Abbildung 144: Einstellungen – Uhrzeit und Kalender

- > Sie können für jede Schließkomponente eine manuelle Daueröffnung zulassen. Sobald diese ausgewählt ist, erscheint die Möglichkeit, die automatische Daueröffnung zu aktivieren.

Weiters können Sie auch die Freigabedauer ändern oder die Aktualisierung nach jedem Sperrvorgang aktivieren bzw. deaktivieren. Siehe auch Kapitel [Vorgabewerte \(für alle neu hinzugefügten Schließkomponenten\)](#).

Zusätzlich kann der Hands-free-Modus für die einzelne Schließkomponente erlaubt oder nicht erlaubt werden. Wird der Hands-free-Modus erlaubt, so kann innerhalb der AirKey-App der Hands-free-Modus für diese Schließkomponente aktiviert werden. Andernfalls kann dieser in der AirKey-App für diese Schließkomponente nicht aktiviert werden. Details zum Hands-free-Modus finden Sie im Kapitel [Hands-free auf einen Blick](#).

- > Für jede Schließkomponente haben Sie die Möglichkeit, den Personenbezug in Protokolleinträgen anzupassen. Standardmäßig wird die Vorgabe aus den Einstellungen übernommen.
 - **Einsehbar** lässt die Anzeige personenbezogener Daten von Zutrittsereignissen dauerhaft angezeigt.
 - **Einsehbar für ... Tage** anonymisiert die personenbezogenen Daten von Zutrittsereignissen nach der definierten Anzahl an Tagen.
 - **Nicht einsehbar** anonymisiert sämtliche personenbezogenen Daten von Zutrittsereignissen dauerhaft.

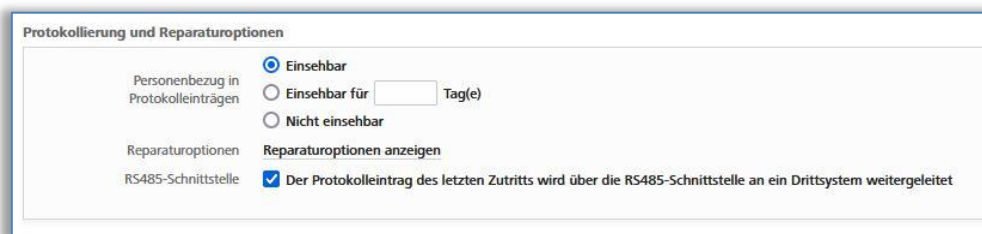


Abbildung 145: Protokollierung

- > Hier finden Sie auch den Link für die Reparaturoptionen. Nähere Informationen dazu finden Sie im Kapitel [Reparaturoptionen](#).

- > Bluetooth-Wandler bieten im Vergleich zu allen anderen Schließkomponenten zusätzlich die Option, die **RS485-Schnittstelle** zu aktivieren. Dabei kann der Protokolleintrag des letzten erfolgreichen Zutritts über die RS485-Schnittstelle an ein Drittsystem weitergeleitet werden. Weitere Details dazu finden Sie im Kapitel [Technische Details zur RS485-Schnittstelle bei Wandlesern](#).
- > Klicken Sie auf **Speichern**, um die Änderungen der Schließkomponente zu übernehmen. Im Anschluss erscheint eine Erfolgsmeldung.



Je nachdem, welche Daten der Schließkomponente bearbeitet wurden, kann es sein, dass eine Wartungsaufgabe für diese Schließkomponente entsteht. Durch die Aktualisierung der Schließkomponente mit einem Smartphone mit Wartungsberechtigung oder einer Codierstation werden die Änderungen übernommen und die Wartungsaufgabe verschwindet.

5.5.4 Schließkomponente entfernen

Sofern Sie eine Schließkomponente nicht mehr in Ihrer AirKey-Schließanlage benötigen, können Sie diese aus Ihrer Schließanlage entfernen.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** oder **Wandler**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie auf den Listeneintrag der Schließkomponente, die Sie aus Ihrer Schließanlage entfernen möchten.
- > Klicken Sie rechts oben auf **Entfernen** 1.



Abbildung 146: Schließkomponente entfernen

- > Bestätigen Sie die Sicherheitsabfrage mit **Schließkomponente entfernen**.

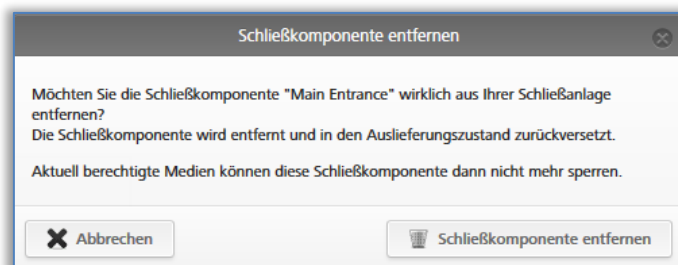


Abbildung 147: Sicherheitsabfrage

- > Es erscheint eine Erfolgsmeldung und eine Wartungsaufgabe, dass die Schließkomponente aus der Schließanlage entfernt werden muss.

Der Vorgang ist erst komplett abgeschlossen, wenn die Schließkomponente mit einem Smartphone mit Wartungsberechtigung oder einer optionalen Codierstation aktualisiert wurde. Sobald die Schließkomponente aktualisiert ist, wurde sie aus der Schließanlage erfolgreich entfernt.



Dieser Vorgang kann nicht rückgängig gemacht werden.

Die Schließkomponente wird nach dem Entfernen in den Auslieferungszustand zurückversetzt.

Zuvor berechnete Zutrittsmedien können die Schließkomponente dann nicht mehr sperren. Die entsprechenden Berechtigungen werden automatisch gelöscht und nicht mehr angezeigt.

5.5.5 Bereiche

Mehrere Schließkomponenten können in Bereichen zusammengefasst werden, um die Verwaltung von Berechtigungen in Ihrer Schließanlage zu vereinfachen.

Auf der Startseite **Home** unter der Kachel **Bereiche** oder im Hauptmenü **Schließanlage** → **Bereiche** erhalten Sie eine Liste aller Bereiche inklusive deren Status.

In der angezeigten Liste der Bereiche können Sie folgende Anpassungen anwenden:

- > Geben Sie im Suchfeld ❶ ein Suchkriterium mit mindestens drei Zeichen ein.
- > Klicken Sie auf die jeweilige Spaltenüberschrift, um diese als Sortierkriterium zu bestimmen.

Die Bereichsliste kann in eine CSV-Datei zur weiteren Bearbeitung exportiert werden ❷.

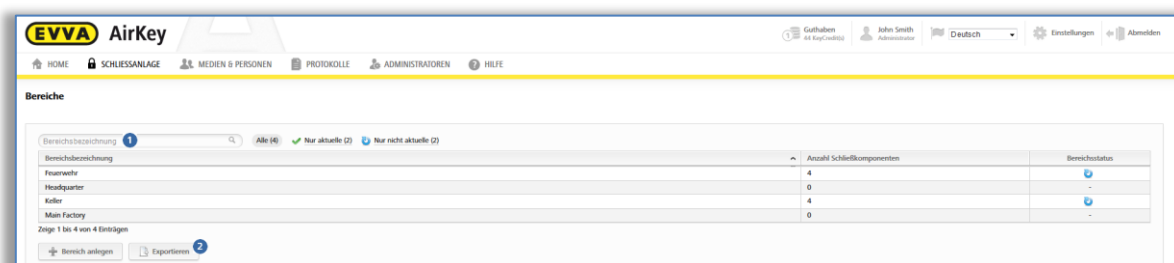


Abbildung 148: Schließanlage – Bereiche

- > Wählen Sie aus der Liste den gewünschten Bereich aus, um die Details des ausgewählten Bereichs zu erhalten.

5.5.6 Bereich anlegen

Standardmäßig sind keine Bereiche angelegt. Sie müssen neue Bereiche anlegen, um Schließkomponenten zu Bereichen hinzufügen zu können.

- > Klicken Sie auf der Startseite **Home** im grauen Balken des Blocks **Schließanlage** auf **Hinzufügen** → **Bereich anlegen**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Bereich anlegen**.
- > Geben Sie dem Bereich einen aussagekräftigen Namen.

- > Weitere Informationen zu diesem Bereich können im Block **Bemerkungen** im Feld **Kommentar** dokumentiert werden.
- > Klicken Sie auf **Speichern** 1.

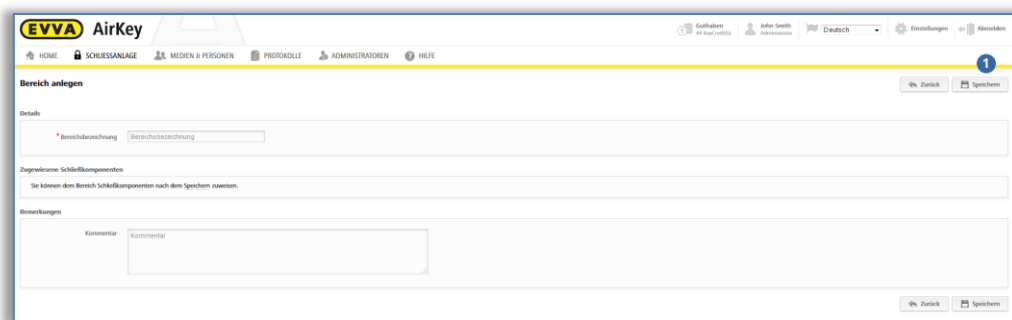


Abbildung 149: Bereich anlegen



Das Anlegen eines Bereiches wird mit der Erfolgsmeldung "Der Bereich wurde gespeichert" angezeigt. Sie können erst Schließkomponenten zu einem Bereich hinzufügen, wenn dieser erfolgreich gespeichert wurde.

5.5.7 Schließkomponente zu Bereichen zuweisen

- > Wählen Sie auf der Startseite **Home** die Kachel **Bereiche** oder im Hauptmenü **Schließanlage** → **Bereiche**.
- > Wählen Sie in der Liste den Bereich, zu dem Sie die Schließkomponente hinzufügen möchten.
- > Es erscheinen die Details des ausgewählten Bereichs. Beim **Bereichsstatus** 1 wird angezeigt, ob alle Schließkomponenten innerhalb des Bereichs aktuell sind. Im Block **Zugewiesene Schließkomponenten** 2 sind alle Schließkomponenten gelistet, die dem Bereich zugewiesen sind.
- > Klicken Sie auf **Komponenten zuweisen** 3, um eine Schließkomponente in den Bereich aufzunehmen.

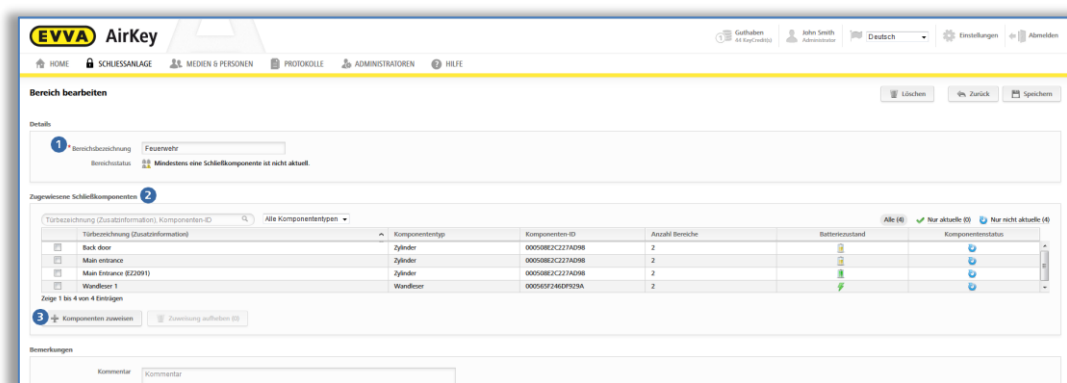


Abbildung 150: Bereich bearbeiten

Es wird eine Liste aller Schließkomponenten angezeigt, die diesem Bereich noch nicht zugeordnet sind.

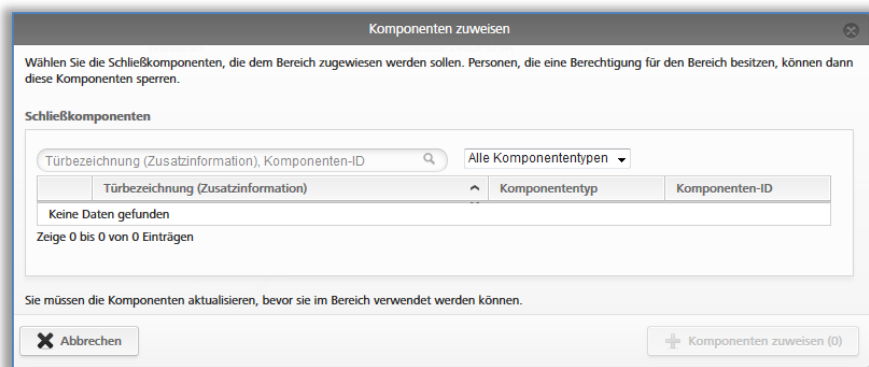


Abbildung 151: Komponenten zuweisen

- > Wählen Sie die gewünschten Schließkomponenten. (Eine Auswahl mehrerer Schließkomponenten, auch unterschiedlichen Typs, ist möglich.)
- > Klicken Sie auf **Komponenten zuweisen**, um die Schließkomponenten dem Bereich zuzuweisen.
- > Klicken Sie auf **Speichern**, um die Änderungen zu übernehmen.

Für die betroffenen Schließkomponenten entstehen Wartungsaufgaben, die durch Aktualisierungen der jeweiligen Schließkomponenten mit einem Smartphone oder einer Codierstation verschwinden. Nach den Aktualisierungen ist die Zuweisung der Schließkomponenten zum Bereich abgeschlossen.



Eine Schließkomponente kann zu maximal 96 Bereichen gleichzeitig zugewiesen sein.



Alternativ können Sie auch die Bereichszuordnung einer Schließkomponente direkt in den Details der Schließkomponente bearbeiten. Nähere Informationen finden Sie im Kapitel [Schließkomponente bearbeiten](#).

5.5.8 Zuweisung von Schließkomponenten zu einem Bereich aufheben

Um die Zuweisung von einer oder mehreren Schließkomponenten zu einem Bereich aufzuheben, gehen Sie wie folgt vor:

- > Wählen Sie auf der Startseite **Home** die Kachel **Bereiche** oder im Hauptmenü **Schließanlage** → **Bereiche**.
- > Wählen Sie in der Liste den Bereich, bei dem die Zuweisung von Schließkomponenten aufgehoben werden soll.
- > Markieren Sie in der Liste der zugewiesenen Schließkomponenten die Checkboxen der Schließkomponenten, deren Zuweisungen aufgehoben werden sollen. Eine Mehrfachauswahl ist möglich.

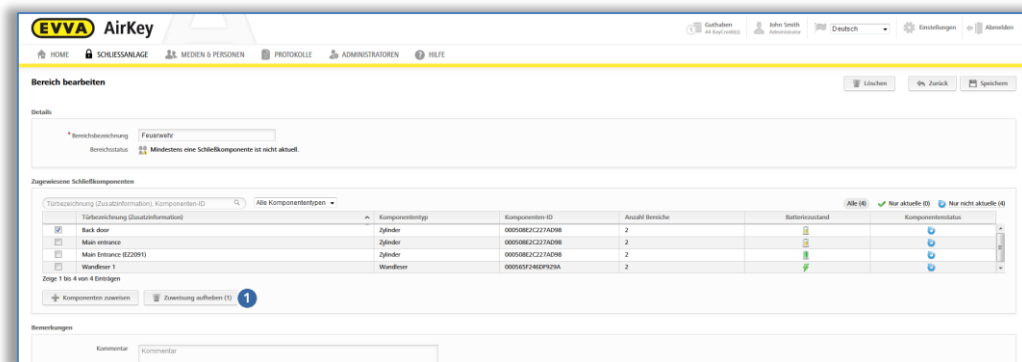


Abbildung 152: Schließkomponenten markieren

- > Klicken Sie auf **Zuweisung aufheben** ❶.
- > Es erscheint ein Dialogfenster, in dem noch einmal angezeigt wird, bei welchen Schließkomponenten die Zuweisung zum Bereich aufgehoben werden soll.
- > Bestätigen Sie den Vorgang ebenfalls mit **Zuweisung aufheben**.

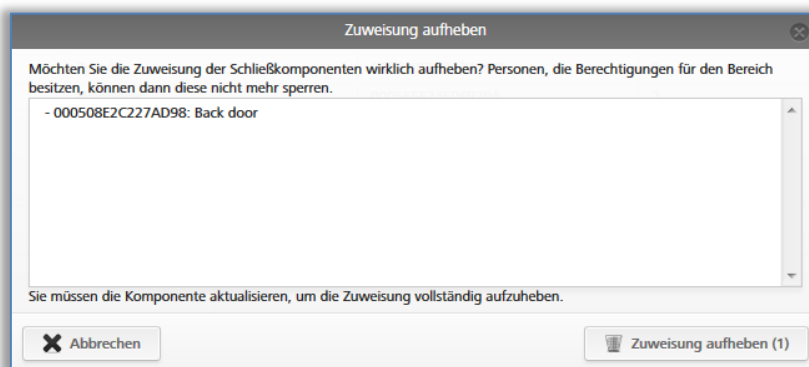


Abbildung 153: Zuweisung aufheben

Für die betroffenen Schließkomponenten entstehen Wartungsaufgaben, die durch Aktualisierungen der jeweiligen Schließkomponenten mit einem Smartphone oder einer Codierstation verschwinden. Nach den Aktualisierungen ist die Zuweisung der Schließkomponenten zum Bereich abgeschlossen.



Nach dem Aktualisieren können Personen, die ein Medium mit der Berechtigung zu diesem Bereich besitzen, die Schließkomponente, bei denen die Zuweisung aufgehoben wurde, nicht mehr sperren.



Alternativ können Sie auch die Bereichszuordnung einer Schließkomponente direkt in den Details der Schließkomponente bearbeiten. Nähere Informationen finden Sie im Kapitel [Schließkomponente bearbeiten](#).

5.5.9 Bereich löschen

- > Wählen Sie auf der Startseite **Home** die Kachel **Bereiche** oder im Hauptmenü **Schließanlage** → **Bereiche**.
- > Wählen Sie in der Liste den Bereich, den Sie löschen möchten.
- > Klicken Sie auf **Löschen** ❶.

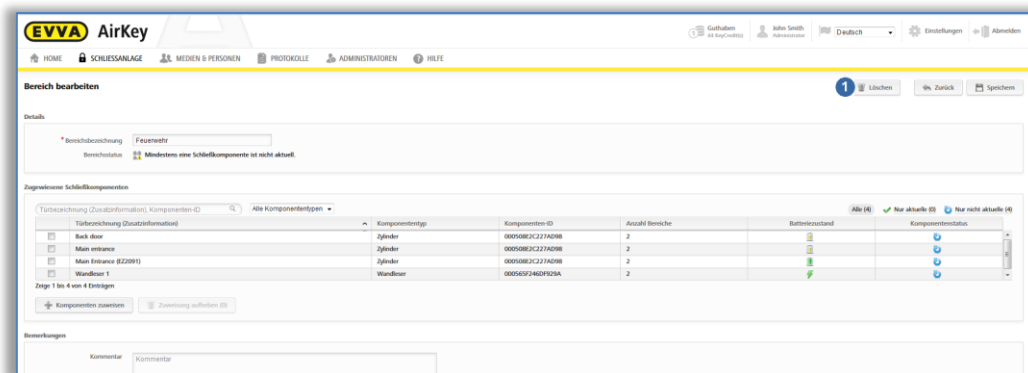


Abbildung 154: Bereich löschen



Für einen gelöschten Bereich werden bestehende Berechtigungen auf dem Medium automatisch gelöscht und nicht mehr angezeigt. Das Löschen kann nicht rückgängig gemacht werden.

Wenn dem Bereich noch Schließkomponenten zugewiesen sind, erhalten Sie eine Fehlermeldung.

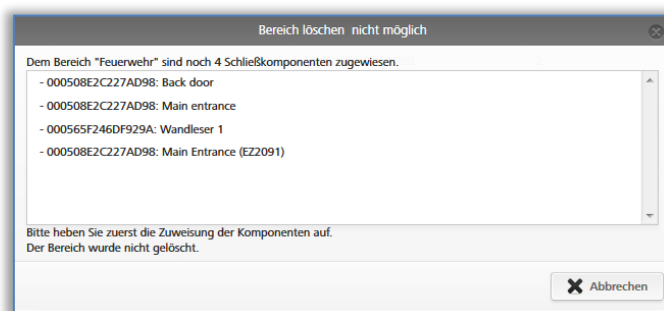


Abbildung 155: Bereich löschen – nicht möglich

Heben Sie daher zunächst die Zuweisung aller Schließkomponenten zum Bereich auf und wiederholen Sie anschließend den oben beschriebenen Ablauf. Nähere Informationen zum Aufheben der Zuordnung von Schließkomponenten zu Bereichen finden Sie im Kapitel [Zuweisung von Schließkomponenten zu einem Bereich aufheben](#).

5.5.10 Berechtigungsübersicht

In der Berechtigungsübersicht werden alle Berechtigungen von Medien zu den einzelnen Schließkomponenten gelistet. Die Berechtigungsübersicht ist auf eine gewählte Schließkomponente bezogen.



Es werden alle Medien gelistet, die eine Berechtigung für eine Schließkomponente besitzen. Angezeigte Berechtigungen müssen allerdings nicht gerade gültig sein, d.h., dass ein Medium mit einem temporären Einzelzutritt von 08:00 bis 17:00 Uhr für eine Schließkomponente auch nach 17:00 Uhr in der Berechtigungsübersicht gelistet wird.

- Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandler** oder im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- Wählen Sie in der Liste die Schließkomponente, für die Sie die Berechtigungsübersicht einsehen möchten.
- Wechseln Sie vom Reiter **Details** auf **Berechtigte Medien (eigene)**, um die Berechtigungen der eigenen Schließanlage einzusehen, oder auf **Berechtigte Medien (fremde)**, um die Berechtigungen von anderen Schließanlagen anzuzeigen, für die die Schließkomponente freigegeben ist.

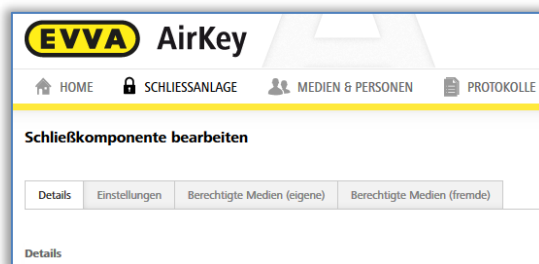


Abbildung 156: Die Reiter der Seite "Schließkomponente bearbeiten"

Sie erhalten eine Liste aller Personen sowie deren zugehörigen Personen gelistet. Ebenso können Sie den Medientyp einsehen.

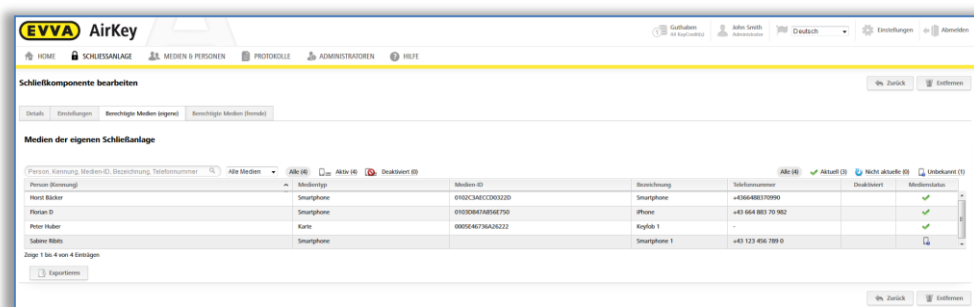


Abbildung 157: Berechtigte Medien (eigene)

Innerhalb dieser Liste kann gesucht, gefiltert und sortiert werden, um bestimmte Berechtigungen zu erhalten.



Klicken Sie auf den Namen einer Person, um aus der Berechtigungsübersicht direkt zu den Berechtigungen des Mediums der Person zu gelangen.

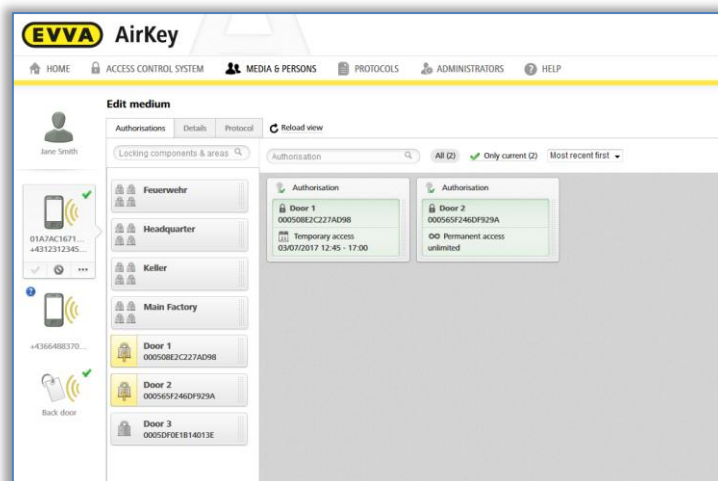


Abbildung 158: Medium bearbeiten

5.5.11 Wartungsaufgaben

Bestimmte Funktionen beeinflussen die Konfiguration von Schließkomponenten. Diese Änderungen der Konfiguration werden als Wartungsaufgaben bezeichnet. Wartungsaufgaben beziehen sich somit auf Schließkomponenten, deren Status nicht aktuell ist.

Eine Liste mit den aktuellen Wartungsaufgaben der AirKey-Schließanlage erhalten Sie wie folgt:

- > Wählen Sie auf der Startseite **Home** den Link **Wartungsaufgaben**.
- > Oder klicken Sie in der Statusleiste auf **Wartungsaufgaben**.
- > Oder wählen Sie im Hauptmenü **Schließanlage** → **Wartungsaufgaben**.

Sie erhalten hier eine übersichtliche Liste der Wartungsaufgaben aller Schließkomponenten Ihrer AirKey-Schließanlage.

In der Liste der Wartungsaufgaben kann nach Türbezeichnung oder Komponenten-ID gesucht werden. Die Spalten "Türbezeichnung (Zusatzinformation)", "Komponenten-ID" und "Wartungsaufgaben" sind sortierbar.

Zusätzlich können Sie eine Priorisierung der Wartungsaufgaben ¹ vornehmen und einen PDF-Download ² der angezeigten Liste durchführen.

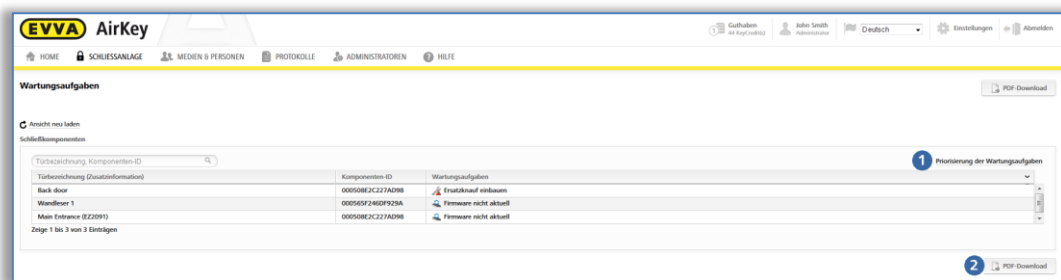


Abbildung 159: Wartungsaufgaben

Die Priorisierung der Wartungsaufgaben wird jeweils pro Schließanlage / Mandant gespeichert und am Smartphone mit installierter AirKey-App und aktivierter Wartungsberechtigung angewendet.

- > Klicken Sie auf **Priorisierung der Wartungsaufgaben**.
- > Je nach Anwendungsfall haben Kunden andere Bedürfnisse – ziehen Sie die Positionen mit Drag & Drop in die von Ihnen gewünschte Reihenfolge.
- > Speichern Sie die geänderte Priorisierung mit **OK**.

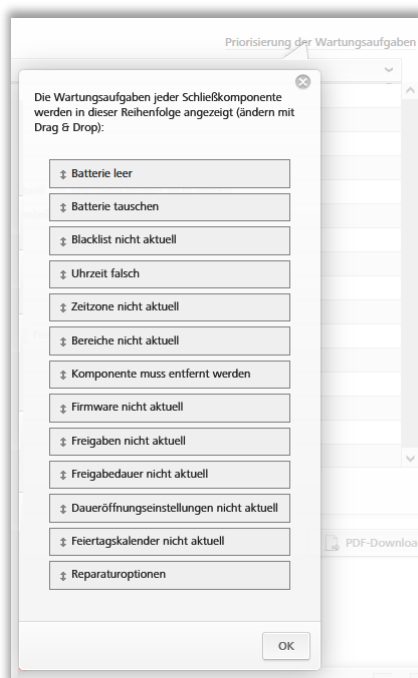


Abbildung 160: Priorisierung der Wartungsaufgaben

Die Liste der Wartungsaufgaben wird nun mit geänderter Priorisierung dargestellt. Die einzelnen Positionen der Liste mit den Wartungsaufgaben sind zu den Detailseiten der jeweiligen Schließkomponente verlinkt.

Wenn eine Wartungsaufgabe durch die Aktualisierung der Schließkomponente erledigt wurde, wird diese Position automatisch aus der Liste der Wartungsaufgaben entfernt.



Die Liste für alle anstehenden Wartungsaufgaben kann als PDF-Datei erstellt und ausgedruckt werden. Nutzen Sie dazu den Button **PDF-Download**.

5.5.12 Kundendaten – Schließplan

Wie bereits erwähnt, kann man im Menü **Kundendaten** verschiedene Informationen, die bei der Registrierung eingegeben wurden, nachträglich ändern, z.B. den Namen der Schließanlage, den Firmennamen oder auch die Kontaktperson.

Auf der Seite "Kundendaten bearbeiten" gibt es rechts oben einen Button, mit dem der Schließplan für die gesamte Schließanlage exportiert werden kann. Der Schließplan ist die

Übersicht aller Schließkomponenten in einer Schließanlage und deren zugeordneten Smartphones und Zutrittsmedien.

- > Klicken Sie auf den Button **Schließplan exportieren**.
- > Wählen Sie im Dialogfenster "Schließplan exportieren" den Button **Exportieren**.
- > Klicken Sie auf den Link der CSV-Datei, der im anschließenden Dialogfenster erscheint.
- > Öffnen Sie die CSV-Datei mit dem gewünschten Programm oder speichern Sie die Datei.
- > Schließen Sie das Dialogfenster "Schließplan exportieren" mit dem Klick auf den Button **Schließen**.

	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_OW3K	airkey_OW3K	airkey_OW3K	
3					designation	Karte	Musters	Testphone	Mi	Mobile	John	iPhone	John	Android	Mobile	Susanne	Kombischlüsse	Samsung	S6
4					media ID	01513937COA	000524E1EEE	00058485F1B	01769CAD4E4	017DF822779	018D3E2A57C	01564B15279	01AC3BF5349	01FBB248091	0005A7592B8	0188626927E8A567			
5					media type	Smartphone (Card	Card	Smartphone (Smartphone (Smartphone (Smartphone (Smartphone (Smartphone (Card	Smartphone (Smartphone (Card	Smartphone (
6					door designat	customer nun	component ty	component ID											
7					SR A Musterst	airkey_OW3K	CYLINDER	00052C2F2B3A3F14B											
8					Hangschloss	airkey_JCHDI!	CYLINDER	0005B508C60B802D											
9					Wandleser	airkey_OW3K	WALLREADER	0005C5B3F1E9C207											
10																			

Abbildung 161: Schließplan



Es wird der Status der AirKey-Onlineverwaltung für die Berechnung des Berechtigungsstatus herangezogen und nicht der IST-Status am Medium. Das heißt, der Schließplan ist nur dann korrekt, wenn alle Komponenten und Medien aktuell sind.

Legende Schließplan:

- > **0 – Nicht berechtigt:** Das Medium besitzt keine Berechtigung für die Schließkomponente und für keinen Bereich, dem die Schließkomponente zugeordnet ist.
- > **1 – Dauerberechtigt ohne Ablaufdatum:** Das Medium besitzt genau eine Dauerberechtigung ohne Ablaufdatum für die Schließkomponente oder einen Bereich dem die Schließkomponente zugeordnet ist und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich dem die Schließkomponente zugeordnet ist.
- > **2 – Dauerberechtigung mit Ablaufdatum:** (1) trifft nicht zu und das Medium besitzt genau eine Dauerberechtigung mit Ablaufdatum in der Zukunft für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist.
- > **3 – Periodische Berechtigung ohne Ablaufdatum:** (1) und (2) treffen nicht zu und das Medium besitzt genau eine periodische Berechtigung ohne Ablaufdatum für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist.
- > **4 – Periodische Berechtigung mit Ablaufdatum:** (1), (2) und (3) treffen nicht zu und das Medium besitzt genau eine periodische Berechtigung mit Ablaufdatum in der Zukunft für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist.

- > **5 – Einzelberechtigung:** (1), (2), (3) und (4) treffen nicht zu und das Medium besitzt genau eine Einzelberechtigung mit Ablaufdatum in der Zukunft für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist.
- > **6 – Individuelle Berechtigung:** (1), (2), (3), (4) und (5) treffen nicht zu und das Medium besitzt genau eine individuelle Berechtigung mit mindestens einer Sub-Berechtigung mit Ablaufdatum in der Zukunft für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, und keine weiteren Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist.
- > **7 – Mehrfach berechtigt:** Das Medium besitzt mindestens zwei Berechtigungen für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, die noch nicht abgelaufen sind.
- > **B – Blacklist:** Das Medium ist deaktiviert, d.h., in die Blacklist der Schließkomponenten eingetragen. Die Berechtigungen des Mediums verlieren dadurch ihre Gültigkeit.
- > **E – Abgelaufene Berechtigung (aller Typen):** Alle Berechtigungen des Mediums für die Schließkomponente oder einen Bereich, dem die Schließkomponente zugeordnet ist, sind abgelaufen.

5.6 Medien & Personen

Im Hauptmenü **Medien & Personen** ❶ verwalten Sie alle Personen, Medien und deren Berechtigungen in der AirKey-Schließanlage.

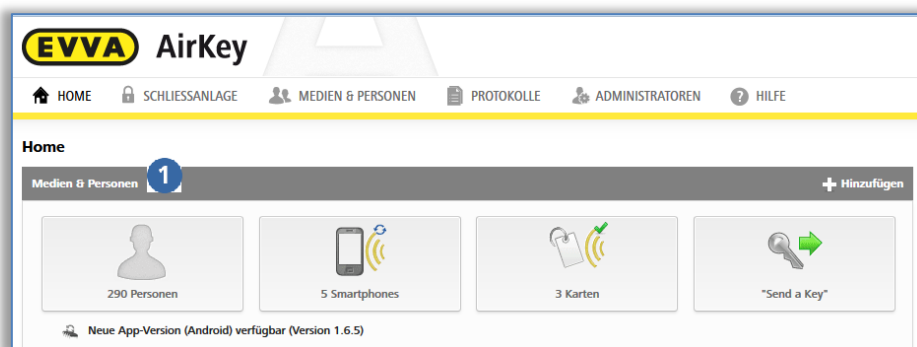


Abbildung 162: Medien & Personen

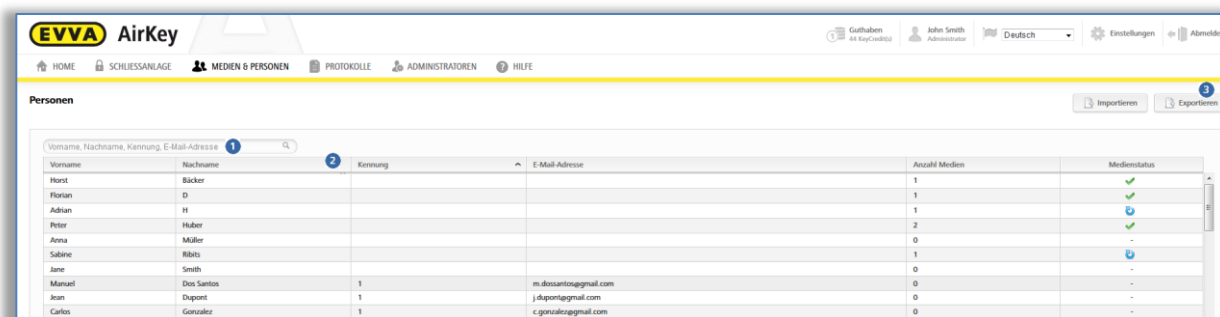
5.6.1 Übersicht der Personen

Wenn Sie auf der Startseite **Home** die Kachel **Personen** wählen oder im Hauptmenü **Medien & Personen** → **Personen**, erhalten Sie eine Liste aller angelegten Personen inklusive die Anzahl der Medien sowie deren Medienstatus.

In der angezeigten Liste können Sie folgende Funktionen anwenden:

- > Geben Sie im Suchfeld ❶ ein Suchkriterium mit mindestens 3 Zeichen ein. Wählen Sie Vorname, Nachname, Kennung oder die E-Mail-Adresse.
- > Klicken Sie auf die jeweilige Spaltenüberschrift, um diese als Sortierkriterium ❷ zu bestimmen.

- > Sie können auch die gesamte Liste in eine CSV-Datei exportieren, um sie weiter zu bearbeiten ③.



Vorname	Nachname	Kennung	E-Mail-Adresse	Anzahl Medien	Medienstatus
Horst	Bäcker			1	
Florian	D			1	✓
Adrian	H			1	ⓘ
Peter	Hüber			2	✓
Anna	Müller			0	-
Sabine	Ribits			1	ⓘ
Jane	Smith			0	-
Manuel	Des Santos	1	m.dossantos@gmail.com	0	-
Juan	Dipont	1	j.dipont@gmail.com	0	-
Carlos	Gonzalez	1	c.gonzalez@gmail.com	0	-

Abbildung 163: Personen

5.6.2 [Person anlegen](#): Siehe Kapitel 4.7

5.6.3 Person bearbeiten

In der Detailansicht "Person bearbeiten" können Sie die Details und Kontaktdaten zu einer Person ändern oder ihr ein neues Medium zuweisen.

- > Wählen Sie auf der Startseite **Home** die Kachel **Personen**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Personen**.
- > Klicken Sie in der Personenliste auf den Namen der Person, bei der Sie Änderungen durchführen möchten.
- > Ändern Sie die entsprechenden Daten.
- > Klicken Sie auf **Speichern**.

Auf der Seite "Person bearbeiten" kann auch die Übergabebestätigung erstellt werden ①. Das ist eine Bestätigung, die nach Erstellung und Zuweisung aller notwendigen Berechtigungen an die Person übergeben wird. Die Bestätigung zeigt, welche Medien mit welchen Berechtigungen, zum Zeitpunkt der Ausstellung, im Besitz der Person sind.

- > Wählen Sie aus der Übersichtsliste die Person aus, für die Sie die Übergabebestätigung erstellen wollen.
- > Klicken Sie auf der Seite "Person bearbeiten" auf den Button **Übergabebestätigung generieren (PDF)**.
- > Es erscheint das Dialogfenster "Übergabebestätigung generieren (PDF)", in dem die PDF-Datei als Link dargestellt ist.
- > Klicken Sie auf den Link und öffnen Sie die PDF-Datei mit Ihrem PDF-Reader oder Sie können die Datei auch speichern.
- > Schließen Sie das Dialogfenster mit dem Button **Schließen**.

Abbildung 164: Übergabebestätigung generieren

Headquarter Wien Aussteller: John Smith

EVVA AirKey-Personendetails

Person

Florian D

- Kennung: Technik
- Geschlecht: Männlich
- Geburtsdatum: 18.05.1980
- E-Mail-Adresse: FD@test.com
- Telefonnummer: +431234567890
- Straße: Hauptstrasse 1
- PLZ: 1010
- Ort: Wien
- Land: Österreich
- Bemerkungen: -

Medien **Aktuell**

- Medientyp: Smartphone (Android)
- Medien-ID: 01A46636A2ECB86D
- Telefonnummer: +4366488370
- Letzte Aktualisierung: 30.01.2018
- AirKey-App-Version: 1.7.6
- Registrierungs-Fortschritt: abgeschlossen
- Registrierungscode: -
- Wartungsmodus: aktiv
- Protokollaten anzeigen: aktiv
- Freigabedauer: normal
- Daueröffnung: aktiv
- PIN-Code-Status: inaktiv
- Bemerkungen: -

Berechtigung 1

- Typ: Periodischer Zutritt
- für Bereich: Area 1
- gültig von: 30.01.2018
- gültig bis: unbegrenzt

Tag	von	bis
Mi	04:15	11:00

Abbildung 165: Beispiel Übergabebestätigung

5.6.4 Person löschen

Wenn Sie eine Person aus der AirKey-Schließanlage entfernen wollen, können Sie die Person löschen.



Eine Person, die noch Medien zugewiesen hat, kann nicht gelöscht werden. Achten Sie daher darauf, dass vor dem Löschen die Zuweisung aller Medien zu dieser Person aufgehoben wurde.

- > Wählen Sie auf der Startseite **Home** die Kachel **Personen**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Personen**.
- > Klicken Sie in der Personenliste auf den Namen der Person, die Sie löschen möchten.
- > Klicken Sie auf das Symbol **Papierkorb**

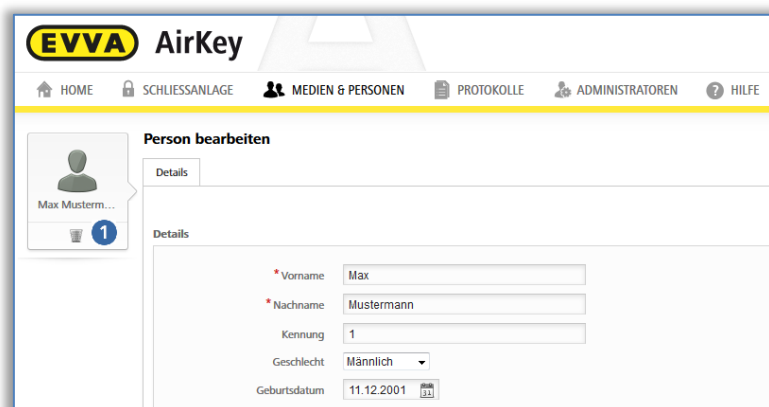


Abbildung 166: Person löschen

- > Bestätigen Sie die Sicherheitsabfrage mit Person löschen.

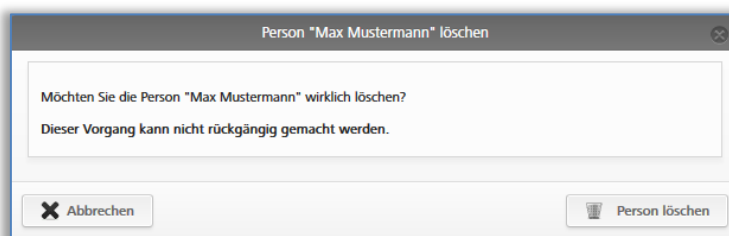


Abbildung 167: Person löschen – Sicherheitsabfrage



Die gelöschte Person wird in der Personenliste nicht mehr geführt. In Protokolleinträgen vor dem Löschen der Person wird der Personenbezug zu Schließkomponenten und Medien weiterhin dokumentiert.

5.6.5 Medium einer Person zuweisen

Sie müssen das Medium einer Person zuweisen, um Berechtigungen vergeben zu können. Nur damit erhalten Sie einen Personenbezug bei Zutritten.

- > Wählen Sie auf der Startseite **Home** die Kachel **Personen**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Personen**.
- > Klicken Sie in der Personenliste auf den Namen der Person, der Sie ein Medium zuweisen möchten.
- > Klicken Sie auf die Schaltfläche **Medium zuweisen**

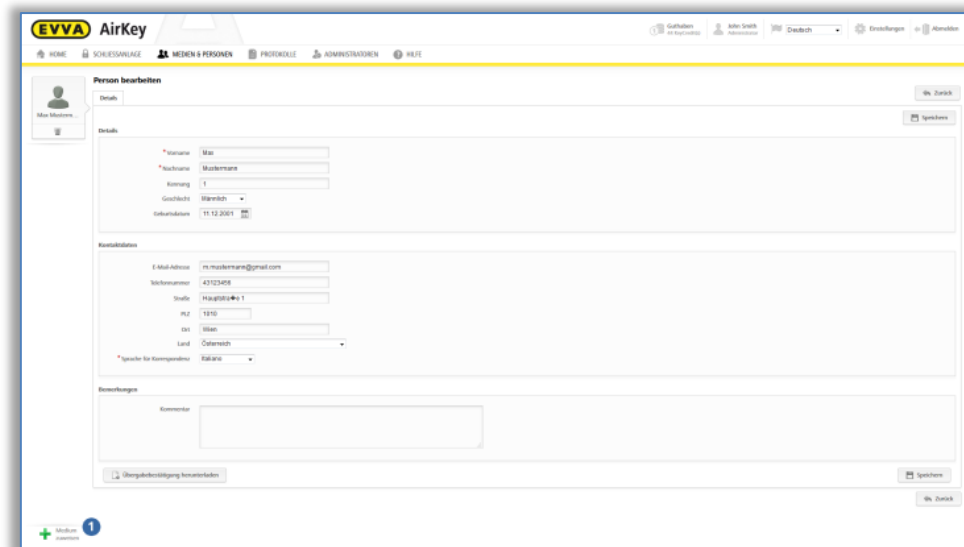


Abbildung 168: Medium zuweisen

Es wird eine Liste mit allen Medien eingeblendet, die Sie der Person zuweisen können. Sie können die Liste sortieren, nach Medientypen filtern oder nach bestimmten Einträgen suchen.



Es werden nur Medien Ihrer Schließanlage angezeigt, die noch keiner Person zugewiesen sind.

- > Wählen Sie das gewünschte Medium aus und klicken Sie auf **Weiter**.

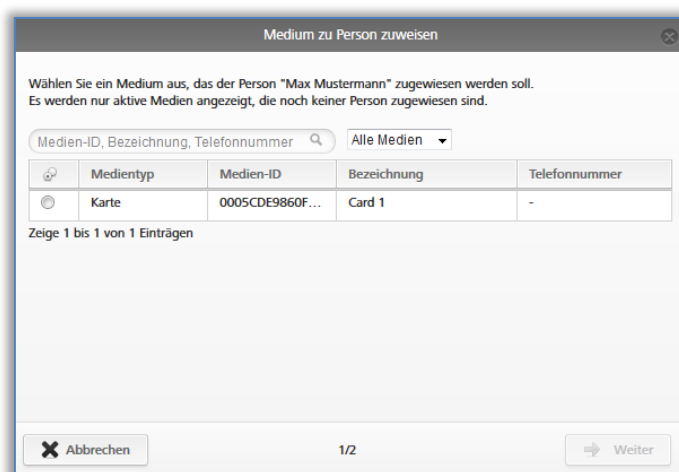


Abbildung 169: Medium zu Person zuweisen

Nach Auswahl des Mediums werden die Details angezeigt. Bei Bedarf klicken Sie auf **Zurück** und wählen ein anderes Medium aus.

- > Klicken Sie auf **Medium zuweisen**, um den Vorgang abzuschließen.

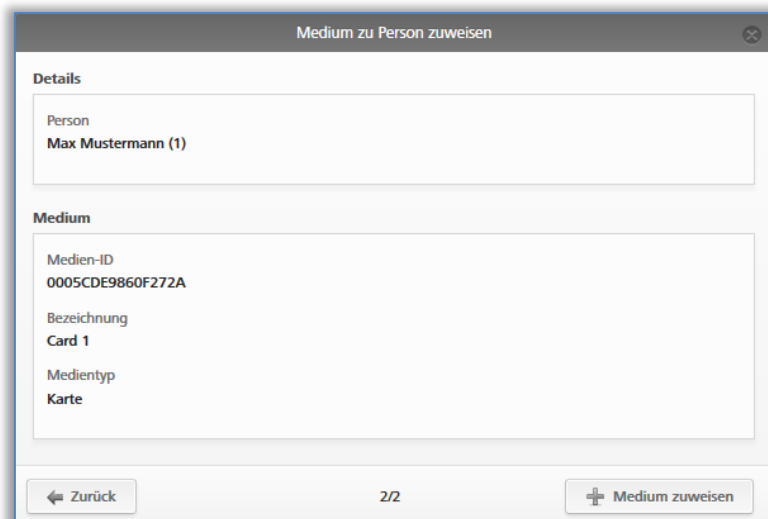


Abbildung 170: Medium zu Person zuweisen



Als Alternative können Sie auch die Zuweisung eines Mediums zur Person über das Medium durchführen. Nähere Informationen dazu finden Sie im Kapitel [Person einem Medium zuweisen](#).



Einer Person können auch mehrere Medien (Smartphones, Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder) zugewiesen werden.

5.6.6 Übersicht der Medien

Im Hauptmenü **Medien & Personen** → **Medien** erhalten Sie eine Liste aller Medien (Smartphones, Karten, Schlüsselanhänger, Kombischlüssel und Armbänder) durch die Sie einen Überblick über vergebene Berechtigungen, eine eventuelle Deaktivierung sowie den aktuellen Medienstatus haben.

Innerhalb dieser Medienliste können Sie nach Medien suchen, bestimmte Medienstatus filtern, die Sortierung ändern, oder die gesamte Liste in eine CSV-Datei exportieren.

Person (Kennung)	Mediumtyp	Medien-ID	Bezeichnung	Telefonnummer	Berechtigung	Deaktiviert	Medienstatus
Horst Räder	Smartphone (Android)	0102CAECCD9322D	Smartphone		2		✓
Florian D	Smartphone (iOS)	0103D847A856E750	iPhone		2		✓
Adrian H	Smartphone (Android)	0103E70504F10D0F	Smartphone Compact Z3	+43 123 123 123 123	0	2	✓
Peter Huber	Karte	0005E46735A26222	Keyfob 1	-	2		✓
Maria Müller (123456)	Karte	0005B63432E8819	Card 1	-	0		✓
Sabine Böhm	Smartphone		Smartphone 1	+43 123 456 789 0	0	2	✓
Hanspeter Süss (AirKey)	Smartphone				0		✓
	Karte	0005CDE9860F272A	Card 1	-	0		✓

Abbildung 171: Medienliste

5.6.7 Medium hinzufügen

Um ein Medium in Ihrer Schließanlage verwalten zu können, müssen Sie dieses zuerst hinzufügen.

- > Klicken Sie auf der Startseite **Home** im grauen Balken des Blocks **Medien & Personen** auf **Hinzufügen** → **Medium hinzufügen**.

- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medium hinzufügen**.
- > Oder wählen auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten** und dort **Medium hinzufügen**.

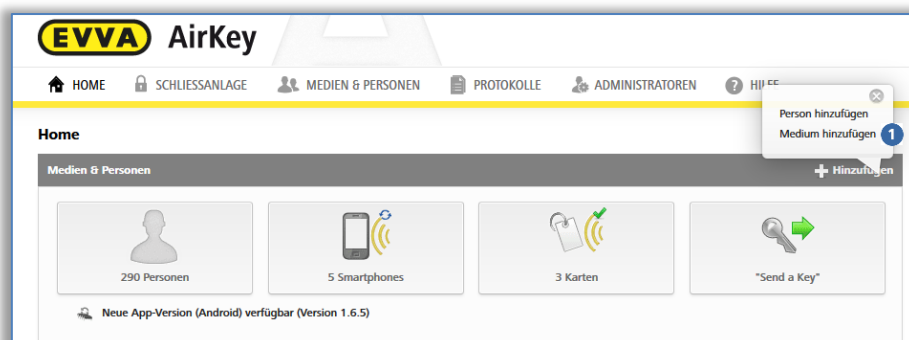


Abbildung 172: Medium hinzufügen

- > Wählen Sie den Medientyp des neuen Mediums.



Abbildung 173: Neues Medium hinzufügen



Karten, Schlüsselanhänger, Kombischlüssel und Armbänder werden aus Applikationssicht nicht unterschieden, deshalb müssen auch Schlüsselanhänger, Kombischlüssel und Armbänder als Medientyp **Karte** angelegt werden.

5.6.8 **Smartphone anlegen:** Siehe Kapitel 4.8

5.6.9 **Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder anlegen**

Sofern Sie keine Codierstation zur Verfügung haben, können Sie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder mit einem Smartphone mit Wartungsberechtigung zur Schließanlage hinzufügen. Befolgen Sie dazu die Informationen unter [Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen](#).

- > Geben Sie eine Bezeichnung ein und klicken Sie auf **Weiter**.
- > Legen Sie die Karte, den Schlüsselanhänger, den Kombischlüssel oder das Armband auf die Codierstation.

Wenn der Vorgang erfolgreich abgeschlossen wurde, öffnet sich automatisch die Detailansicht dieses Mediums.



Es wird ausdrücklich empfohlen, ausreichend vorkonfigurierte Medien (Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder) mit einer unbegrenzten Dauerberechtigung (Notmedien) anzufertigen und an sicheren Orten zu verwahren, um die Schließanlage auch unabhängig von der AirKey-Onlineverwaltung betreiben zu können. Informationen zur Vergabe von Berechtigungen finden Sie im Kapitel [Berechtigungen](#).



Das Hinzufügen eines Kombischlüssels mit der Codierstation muss mit jener Seite des Kombischlüssels erfolgen, auf der das RFID-Symbol aufgebracht ist. Der Kombischlüssel muss direkt an die Codierstation angehalten werden. Das Hinzufügen ist nicht im gesamten Lesebereich der Codierstation möglich – bei der aktuellen Type (HID Omnikey 5421) wird der Kombischlüssel nur im oberen und unteren Drittel der Codierstation erkannt.



Wie Sie Medien mithilfe eines Smartphones mit einer Wartungsberechtigung zu Ihrer AirKey-Schließanlage hinzufügen, erfahren Sie unter [Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen](#).

5.6.10 Medium bearbeiten

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das gewünschte Medium.
- > Wählen Sie den Reiter **Details**, um das Medium zu bearbeiten.

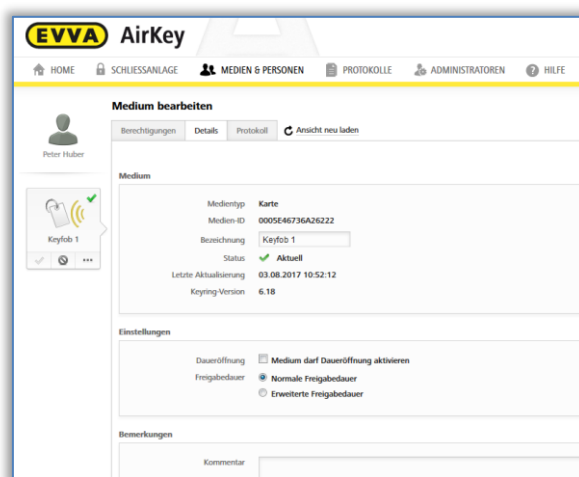


Abbildung 174: Medium bearbeiten – Karte

- > Durch Klicken auf **Speichern** werden die Änderungen übernommen.

5.6.11 [Person einem Medium zuweisen](#): Siehe Kapitel 4.13

5.6.12 Berechtigungen

Über die Berechtigungen regeln Sie den Zutritt von Personen zu Schließkomponenten. Um Berechtigungen für Medien erstellen zu können, müssen Medien bereits einer Person

zugewiesen sein (Nähere Informationen zum Zuweisen eines Mediums zu einer Person finden Sie im Kapitel [Medium einer Person zuweisen](#)).

Die Berechtigungsübersicht eines Mediums erhalten Sie wie folgt:

- > Wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das gewünschte Medium.
- > Das Medium ❶ ist bereits ausgewählt (einer Person können mehrere Medien zugewiesen werden).
- > Sie sehen alle bereits vergebenen Berechtigungen ❷.

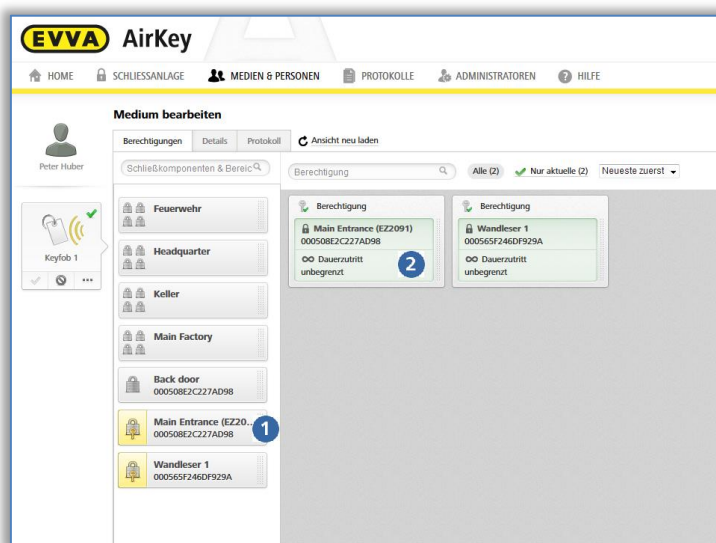


Abbildung 175: Berechtigungsübersicht



Hintergrundfarbe der Berechtigungen:

- **Grün** = Status ist aktuell, die Berechtigung wurde angefertigt und das Medium aktualisiert.
- **Blau** = Berechtigung wurde angefertigt, das Medium noch nicht aktualisiert.
- **Gelb** = Berechtigung wurde geändert oder gelöscht, jedoch noch nicht angefertigt.
- **Grau** = Berechtigung ist abgelaufen.



Als Alternative können Sie die Berechtigungsübersicht auch über das Hauptmenü **Medien & Personen** → **Personen** aufrufen, indem Sie in der Personenliste eine Person wählen, die ein Medium besitzt. Im Anschluss müssen Sie nur auf das Mediensymbol auf der linken Seite unterhalb der ausgewählten Person klicken.

5.6.13 [Berechtigungen vergeben](#): Siehe Kapitel 4.14

5.6.14 [Berechtigung anfertigen](#): Siehe Kapitel 4.15

5.6.15 Berechtigung ändern

Berechtigungen können innerhalb der AirKey-Onlineverwaltung jederzeit geändert werden.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Medium, von dem die Berechtigungen geändert werden sollen.
- > Im Reiter "Berechtigung" klicken Sie auf die Berechtigung, die Sie ändern möchten.
- > Oder ziehen Sie per Drag & Drop die Türe / den Bereich erneut in die Mittelfläche.

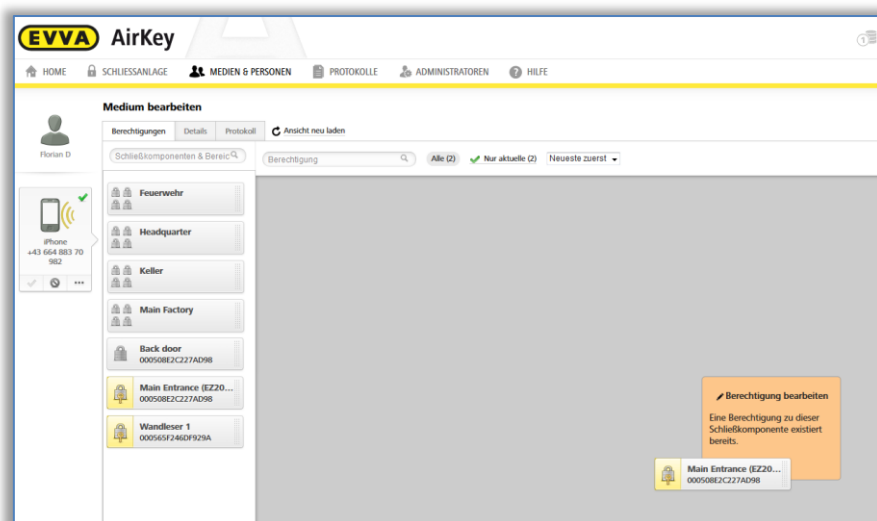


Abbildung 176: Medium bearbeiten – Berechtigung ändern

- > Es werden die Details der bestehenden Berechtigung angezeigt.
- > Klicken Sie auf **Ändern** 1

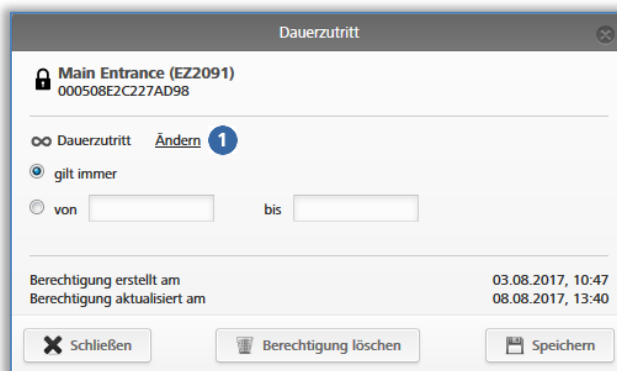


Abbildung 177: Berechtigung ändern

- > Wählen Sie die neue Zutrittsart aus.
- > Klicken Sie auf **Zutritt ändern** 1.

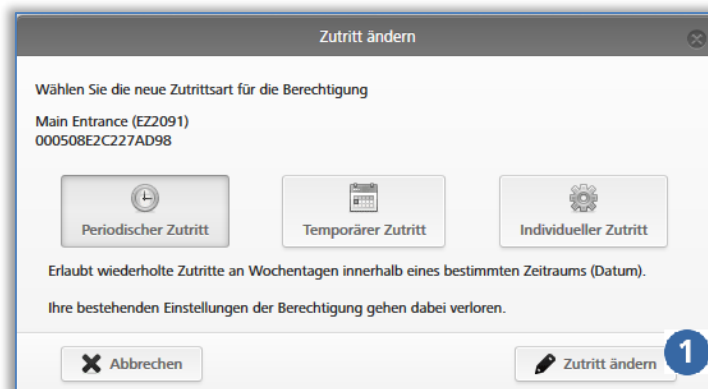


Abbildung 178: Zutritt ändern

- > Geben Sie die geänderten Werte in der jeweiligen Zutrittsart ein.
- > Klicken Sie auf **Speichern**.



Für das Ändern von Berechtigungen ist Guthaben in Form von KeyCredits erforderlich.

- > Klicken Sie auf den gelben Button **1 Berechtigung anfertigen**. Nähere Informationen finden Sie im Kapitel [Berechtigung anfertigen](#).
- > Aktualisieren Sie das Medium mit "Pull to Refresh" bei einem Smartphone oder mit der Codierstation bei einer Karte, einem Schlüsselanhänger, einem Kombischlüssel oder einem Armband, um den Vorgang erfolgreich abzuschließen.

5.6.16 Berechtigung löschen

Wird eine Berechtigung nicht mehr benötigt, so können Sie jederzeit eine bereits vergebene Berechtigung löschen.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Medium, bei dem die Berechtigungen gelöscht werden sollen.
- > Im Reiter "Berechtigung" klicken Sie auf die Berechtigung, die Sie löschen möchten.

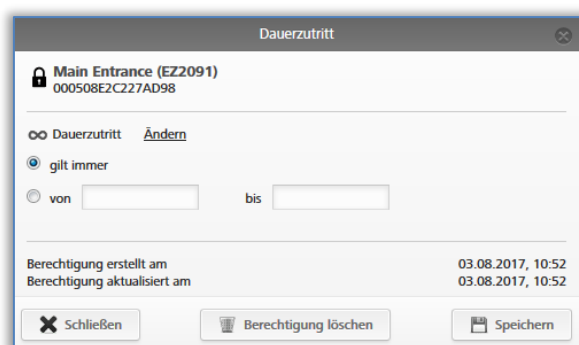


Abbildung 179: Dauerzutritt

- > Oder ziehen Sie per Drag & Drop die Türe / den Bereich aus der Mittelfläche auf das orange hinterlegte Feld **Berechtigung löschen**.

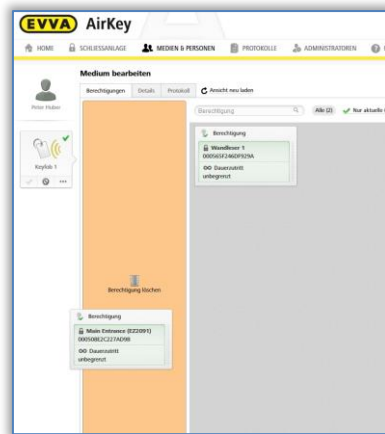


Abbildung 180: Berechtigung löschen

- > Klicken Sie auf **Berechtigung löschen**.
- > Bestätigen Sie die Sicherheitsabfrage mit **Berechtigung löschen**.



Abbildung 181: Berechtigung löschen

- > Aktualisieren Sie das Medium mit "Pull to Refresh" bei einem Smartphone oder mit der Codierstation bei einer Karte, einem Schlüsselanhänger, einem Kombischlüssel oder einem Armband, um den Vorgang erfolgreich abzuschließen.



Das Löschen von Berechtigungen kostet keine KeyCredits und wird sofort wirksam. Eine Aktualisierung des Mediums ist aber zwingend notwendig, um den Löschvorgang erfolgreich abzuschließen.

Verwenden Sie diese Funktion nicht, um auf den Verlust von Medien zu reagieren. Sie können damit nur die Berechtigungen löschen, wenn das Medium physisch vorhanden ist. Verwenden Sie im Verlustfall die Funktion Medium deaktivieren.

Wenn Sie alle Berechtigungen des Mediums löschen möchten, verwenden Sie die Funktion [Medium leeren](#).

5.6.17 Medium deaktivieren

Verwenden Sie die Funktion "Medium deaktivieren", wenn ein Sicherheitsrisiko besteht und alle Berechtigungen des Mediums ungültig werden sollen, z.B. ein Verlust oder Defekt des Mediums besteht.



Abbildung 182: Medium deaktivieren

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das gewünschte Medium.
- > Klicken Sie auf **Medium deaktivieren** ⓘ.
- > Geben Sie den Grund für die Deaktivierung an. Wenn Sie "Anderer" wählen, wird das 50-stellige Eingabefeld aktiv.
- > Geben Sie bei Bedarf zusätzliche Informationen (maximal 500 Zeichen) in "Weitere Notizen" ein.
- > Klicken Sie auf **Weiter**.
- > Bestätigen Sie die Sicherheitsabfrage mit **Medium deaktivieren**.

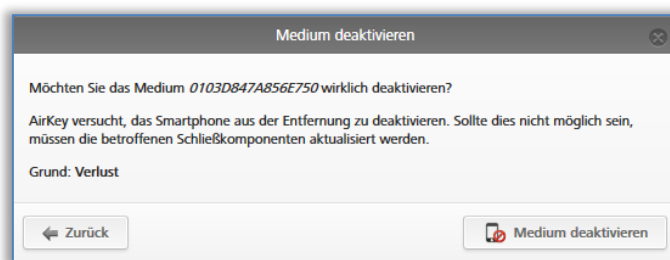


Abbildung 183: Medium deaktivieren – Sicherheitsabfrage

Das Deaktivieren des Mediums wird mit einer Erfolgsmeldung abgeschlossen.

Es werden alle Berechtigungen, die das Medium besitzt, zum Löschen markiert. Im Fall von Karten, Schlüsselanhängern, Kombischlüssel und Armbändern wird sofort ein Eintrag in der Blacklist für alle Schließkomponenten, für die das Medium berechtigt war, hinterlegt. Bei einem Smartphone wird dieser Eintrag erst erstellt, wenn das Smartphone für fünf Minuten nicht erreicht wurde. Ein Eintrag in der Blacklist bedeutet, dass für die betroffenen Schließkomponenten eine Wartungsaufgabe erstellt wird. Bis zur Aktualisierung befinden sich die betroffenen Schließkomponenten in einem nicht aktuellen Zustand.

- > Aktualisieren Sie die Schließkomponenten, für die das Medium eine Berechtigung hatte. Damit wird die Wartungsaufgabe aus der Liste entfernt und die deaktivierten Medien können diese Schließkomponenten nicht mehr sperren.



Verwenden Sie diese Funktion nicht, um einzelne Berechtigungen des Mediums zu löschen. Das Deaktivieren eines Mediums ist eine Funktion, die alle Berechtigungen des Mediums innerhalb einer Schließanlage betrifft.

Die Deaktivierung gilt nur für Ihre Schließanlage. Ist ein Smartphone in mehreren Schließanlagen registriert, ist der Status des Smartphones in den restlichen Schließanlagen aktuell und nicht deaktiviert.

Sollte eine Person ein Smartphone in mehreren Schließanlagen registriert haben, müssen zur vollständigen Deaktivierung des Smartphones die Administratoren aller betroffenen Schließanlagen verständigt werden.



Das Medium bleibt weiterhin der Person zugeordnet. Wenn Sie das Medium löschen möchten, müssen Sie die Zuweisung aufheben. Nähere Informationen dazu finden Sie im Kapitel [Zuweisung aufheben](#).

5.6.18 Deaktiviertes Medium entfernen

Ein deaktiviertes Medium kann aus der Schließanlage entfernt werden, ohne dass das Medium vorhanden ist. Für verlorene, gestohlene oder defekte Medien kann dadurch der Datenstamm in der AirKey-Onlineverwaltung klein gehalten werden.



Das Entfernen eines deaktivierten Mediums ist nur möglich, wenn das Medium vollständig deaktiviert ist. Das bedeutet, dass entweder das Medium aktualisiert wurde oder bei allen Schließkomponenten, bei denen das Medium berechtigt war, die aktuelle Blacklist durch eine Aktualisierung eingespielt wurde. Solange die oben genannten Bedingungen nicht erfüllt sind, steht die Möglichkeit zum Entfernen nicht zur Verfügung.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das deaktivierte Medium, das entfernt werden soll.
- > Klicken Sie unterhalb des Mediensymbols auf Mehr und wählen Sie **Entfernen** ⓘ
- > Bestätigen Sie die anschließende Sicherheitsabfrage mit **Medium entfernen**, um das deaktivierte aktuelle Medium aus der Schließanlage zu entfernen.

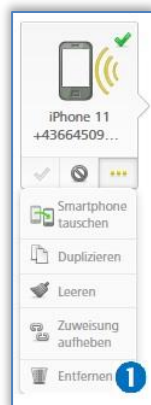


Abbildung 184: Deaktiviertes Medium entfernen

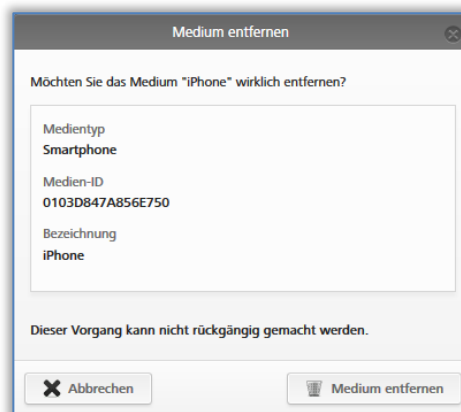


Abbildung 185: Medium entfernen – Sicherheitsabfrage

- > Es erscheint eine Erfolgsmeldung und das Medium wird nicht mehr in der Schließenanlage gelistet.



Dieser Vorgang kann nicht rückgängig gemacht werden. Medien, die auf diesem Weg entfernt wurden, werden nicht mehr in der Schließenanlage gelistet und können somit auch nicht mehr weiterverwendet werden.

Die Medien befinden sich dadurch nicht automatisch im Auslieferungszustand.

5.6.19 Medium reaktivieren

Ein deaktiviertes Medium, ersichtlich am roten Kreissymbol ❶ des Mediums, kann, wenn es wieder zur Verfügung steht, reaktiviert werden.



Abbildung 186: Deaktiviertes Medium reaktivieren

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Medium, bei dem die Reaktivierung gemacht werden soll.
- > Klicken Sie auf **Medium reaktivieren** unterhalb des Mediensymbols.



Abbildung 187: Medium reaktivieren

- > Geben Sie den Grund für die Reaktivierung an (maximal 50 Zeichen) und entscheiden Sie, ob die Berechtigungen, die vor der Deaktivierung gültig waren, wiederhergestellt werden sollen.

Tragen Sie bei Bedarf zusätzliche Informationen (maximal 500 Zeichen) in "Weitere Notizen" ein. Diese zusätzlichen Informationen werden beim entsprechenden Protokoll-eintrag dokumentiert.

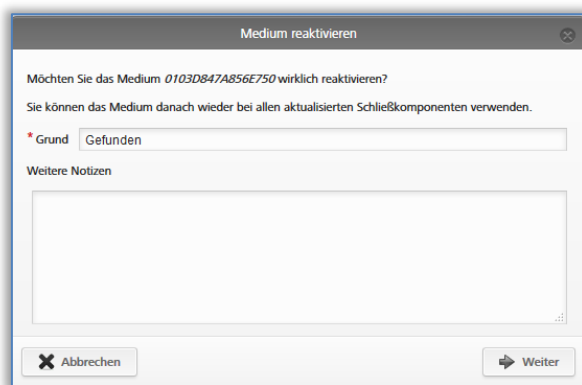


Abbildung 188: Medium reaktivieren

- > Klicken Sie auf **Weiter**.

- > Bestätigen Sie eine der beiden Sicherheitsabfragen (abhängig von der Wahl, ob die Berechtigungen wiederhergestellt werden sollen oder nicht) mit **Medium reaktivieren**.

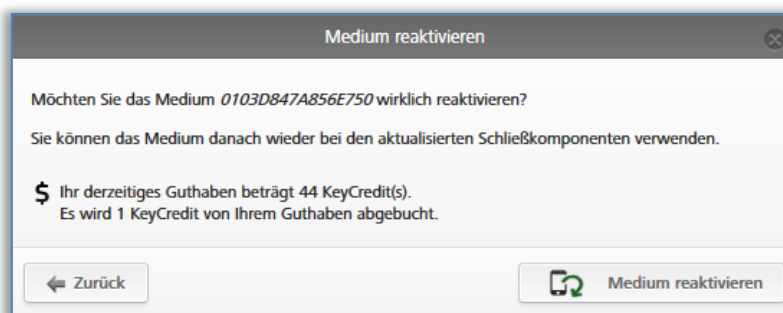


Abbildung 189: Medium reaktivieren – Berechtigungen wiederherstellen

Die erfolgreiche Reaktivierung eines Mediums wird mit einer Erfolgsmeldung abgeschlossen.

Sofern die Blacklist für das reaktivierte Medium auf alle berechtigten Schließkomponenten verteilt wurde, entstehen erneut Wartungsaufgaben für diese Schließkomponenten.

Aktualisieren Sie die Schließkomponenten, die aufgrund der Reaktivierung eines Mediums eine Wartungsaufgabe erhalten haben. Erst wenn alle Einträge in der Blacklist wieder entfernt wurden – das heißt, dass alle betroffenen Schließkomponenten aktuell sind – kann das Medium wieder bei allen Schließkomponenten sperren.



Die Reaktivierung gilt nur für Ihre Schließanlage. Wenn das Smartphone in mehreren Schließanlagen deaktiviert war, ist das Smartphone in anderen Schließanlagen noch immer deaktiviert und kann dort nicht sperren.

Sollte eine Person ein Smartphone in mehreren Schließanlagen registriert haben, müssen zur vollständigen Reaktivierung in allen relevanten Schließanlagen die anderen Administratoren benachrichtigt werden.



Beim Wiederherstellen der Berechtigungen wird ein KeyCredit abgebucht. Ein Guthaben ist somit erforderlich.

5.6.20 Smartphone tauschen

Mit der Funktion "Smartphone tauschen" übertragen Sie die bestehenden AirKey-Berechtigungen und -Einstellungen eines Smartphones (ausgenommen PIN und die lokalen Hands-free-Einstellungen) auf ein anderes Smartphone. Das Quellmedium wird nach erfolgreichem Tausch automatisch deaktiviert. Weitere Informationen zum Smartphonetausch als Administrator finden Sie im Kapitel [Tausch als Administrator starten](#).

5.6.21 Medium duplizieren

Mit der Funktion "Medium duplizieren" übertragen Sie die bestehenden Berechtigungen eines Mediums auf ein anderes Medium. Dabei wird vorausgesetzt, dass das zu duplizierende Quellmedium Berechtigungen besitzt und das Zielmedium bereits angelegt und einer Person zugewiesen wurde.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das zu duplizierende Medium.

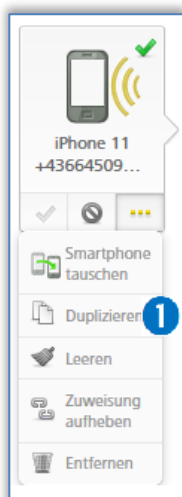


Abbildung 190: Duplizieren eines Mediums

- > Klicken Sie auf **Mehr...** ① → **Duplizieren**.
Es öffnet sich eine Übersichtsliste mit allen einer Person zugeordneten Medien – das zu duplizierende Medium ist nicht in dieser Liste enthalten.
- > Wählen Sie das Zielmedium und klicken Sie auf **Weiter**.
- > Schließen Sie den Vorgang mit **Medium duplizieren** ab.



Abbildung 191: Medium duplizieren

Sie erhalten die Bestätigung über die erfolgreiche Duplizierung. Die Ansicht wechselt zur Berechtigungsübersicht des Zielmediums.



Bestehende Berechtigungen auf dem Zielmedium werden überschrieben.

Um den Vorgang des Duplizierens abzuschließen, muss das Zielmedium mit **Berechtigungen anfertigen** angefertigt und aktualisiert werden. Nähere Informationen zum Anfertigen eines Mediums finden Sie im Kapitel [Berechtigung anfertigen](#).



Dieser Vorgang kostet einen KeyCredit. Ein Guthaben ist somit erforderlich.



Wenn Sie eine große Anzahl von Personen in Ihrer AirKey-Onlineverwaltung haben (siehe [Personendaten importieren](#)), deren Berechtigungen alle identisch sind, dann können Sie mit der Funktion "Medium duplizieren" innerhalb kurzer Zeit eine große Menge an Medien mit den gleichen Berechtigungen den entsprechenden Personen zuweisen.

5.6.22 Medium leeren

Leeren Sie das Medium, wenn Sie alle Berechtigungen des Mediums löschen möchten.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.

- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Medium, das Sie leeren möchten.

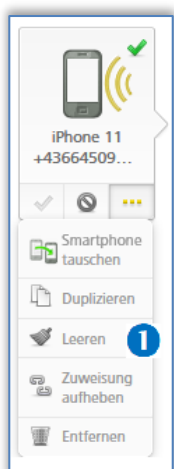


Abbildung 192: Medium leeren

- > Klicken Sie auf **Mehr...** ① → **Leeren**.
- > Schließen Sie den Vorgang mit **Medium leeren** ab.



Abbildung 193: Medium leeren – Sicherheitsabfrage

Es werden alle Berechtigungen als zu löschen markiert. Das Medium muss aktualisiert werden, damit das Löschen der Berechtigungen wirksam wird.



Das Löschen von Berechtigungen kostet keine KeyCredits. Eine Aktualisierung des Mediums ist aber zwingend notwendig, um den Löschvorgang erfolgreich abzuschließen.



Verwenden Sie die Funktion nicht, um auf den Verlust von Medien zu reagieren. Sie können damit nur die Berechtigungen löschen, wenn das Medium vorhanden ist. Verwenden Sie im Verlustfall die Funktion [Medium deaktivieren](#).

Wenn Sie nur einzelne Berechtigungen löschen möchten, verwenden Sie die Funktion [Berechtigung löschen](#).

5.6.23 Zuweisung aufheben

Heben Sie die Zuweisung auf, wenn eine Person ein Medium nicht mehr verwendet.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf jenes Medium, bei dem Sie die Zuweisung zur Person aufheben wollen.

oder

- > Wählen Sie auf der Startseite **Home** die Kachel **Personen**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Personen**.

- > Klicken Sie in der Personenliste auf den Namen der Person, bei der Sie die Zuweisung zu einem Medium aufheben möchten.

Links unterhalb des Namens der Person sind alle ihr zugewiesenen Medien aufgelistet. Wählen Sie das Medium aus, für das Sie die Zuweisung aufheben möchten.

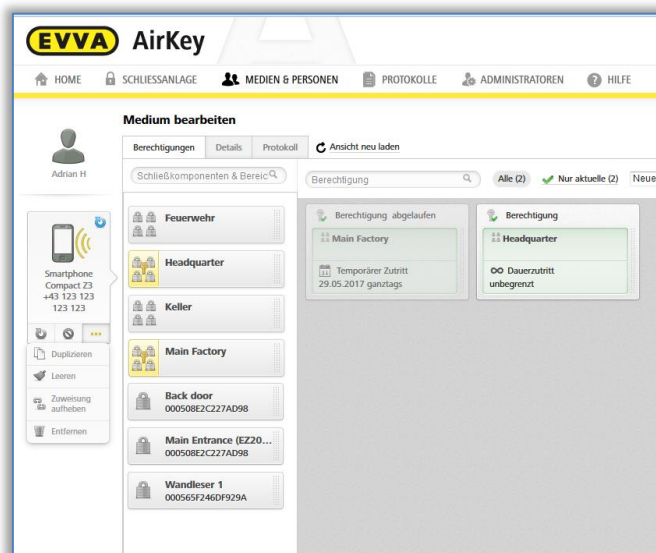


Abbildung 194: Zugewiesene Medien

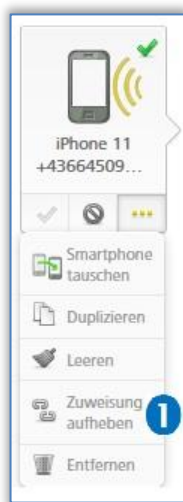


Abbildung 195: Medium – Zuweisung aufheben

- > Klicken Sie auf **Mehr...** → **Zuweisung aufheben**, wenn sich auf dem Medium keine Berechtigungen mehr befinden.
- > Bestätigen Sie die Sicherheitsabfrage mit **Zuweisung aufheben**.

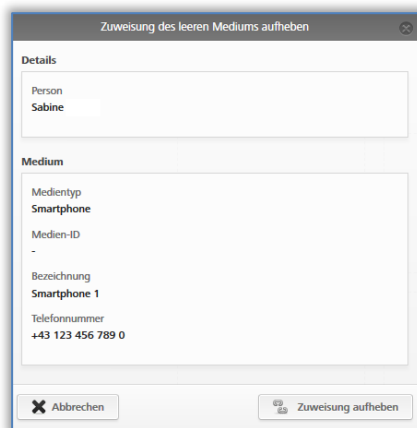


Abbildung 196: Zuweisung aufheben ohne Berechtigungen

Die erfolgreiche Durchführung der Aufhebung einer Zuweisung wird mit einer Erfolgsmeldung abgeschlossen. Die Ansicht wechselt automatisch zu den Personendetails der betroffenen Person.



Bei Smartphones muss die Spezialberechtigung "Wartungsberechtigung" deaktiviert werden, um die Zuweisung aufheben zu können.

Wenn sich auf dem Medium Berechtigungen befinden, müssen Sie diese zuerst löschen. Die Funktion **Medium leeren** kann auch bei der Funktion **Zuweisung aufheben** genutzt werden, um alle Berechtigungen des Mediums zu leeren.

Sofern sich noch Berechtigungen auf dem Medium befinden, wird beim Ausführen der Funktion **Zuweisung aufheben** ein alternativer Dialog angezeigt. In diesem Dialog kann zwischen dem Leeren des Mediums und dem Übertragen des Mediums an eine andere Person gewählt werden.

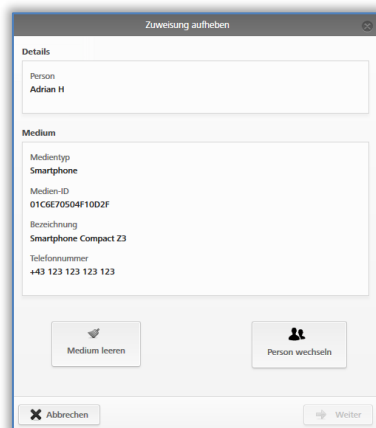


Abbildung 197: Zuweisung aufheben mit Berechtigungen

Sofern die Funktion **Medium leeren** im Zusammenhang mit der Funktion **Zuweisung aufheben** angewendet wird, muss nach der Aktualisierung des Mediums, um den Löschvorgang der Berechtigungen erfolgreich abzuschließen, erneut die Funktion **Zuweisung aufheben** ausgeführt werden.

Wenn das Medium inklusive der Berechtigungen an eine andere Person übertragen werden soll, müssen folgende Schritte durchgeführt werden:

- > Klicken Sie auf **Mehr...** → **Zuweisung aufheben**.
- > Wählen Sie **Person wechseln** und bestätigen Sie mit **Weiter**.

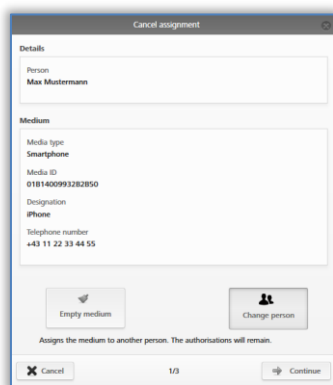


Abbildung 198: Zuweisung aufheben – Person wechseln

Sie erhalten eine Liste aller angelegter Personen. Wählen Sie die gewünschte Person aus und bestätigen Sie mit **Weiter**.

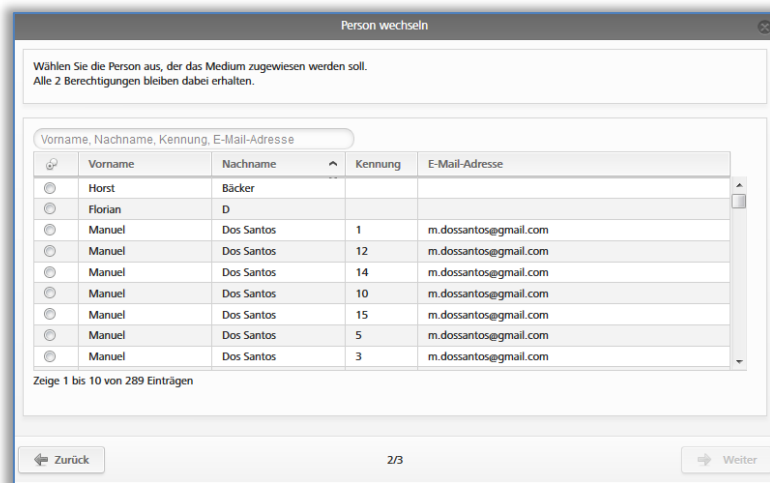


Abbildung 199: Person wechseln

Bestätigen Sie die Sicherheitsabfrage mit **Person wechseln**, um den Vorgang erfolgreich abzuschließen.



Abbildung 200: Person wechseln

Die erfolgreiche Durchführung wird mit einer Erfolgsmeldung abgeschlossen.

5.6.24 Medium entfernen

Entfernen Sie ein Medium, wenn dieses nicht mehr in Ihrer Schließanlage angezeigt bzw. verwendet werden soll.



Ein Medium kann nur entfernt werden, wenn die Zuweisung zur Person aufgehoben wurde. Nähere Informationen zum Aufheben der Zuweisung finden Sie im Kapitel [Zuweisung aufheben](#).

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Medium, das Sie entfernen möchten.
- > Klicken Sie unterhalb des Mediensymbols auf das Symbol Papierkorb **1**.
- > Bestätigen Sie die Sicherheitsabfrage mit **Medium entfernen 1**.

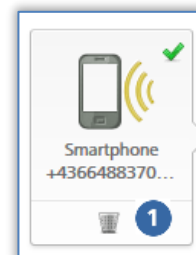


Abbildung 201: Medium entfernen – Papierkorb

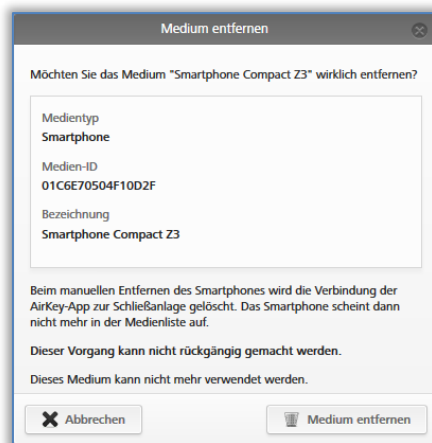


Abbildung 202: Medium entfernen

Wenn das Medium endgültig gelöscht wurde, wird es in der Übersichtsliste der Medien nicht mehr angezeigt. Die Ansicht wechselt in die Medienliste.



Das Medium befindet sich nach dem Entfernen aus der Schließanlage wieder im Auslieferungszustand und kann in einer weiteren AirKey-Schließanlage wieder hinzugefügt werden.

Option

Entfernen Sie ein Medium ohne Berechtigungen und ohne Personenbezug über die Codierstation, indem Sie das Medium auf die Codierstation legen und innerhalb der Statusmeldung auf den Link **Medium aus Anlage entfernen** klicken.

5.7 Protokolle

Im Hauptmenü **Protokolle** erhalten Sie einen zentralen Überblick über alle Ereignisse Ihrer AirKey-Schließanlage. In Abhängigkeit von den allgemeinen Einstellungen hinsichtlich Protokollierung und Reparaturoptionen bzw. der Personenbezug in den Protokolleinträgen werden neben erteilten Zutritten und technischen Ereignissen auch verweigerte Zutritte protokolliert (wenn das Medium eine Berechtigung auf die Schließkomponente besitzt, diese aber zum Zeitpunkt des Zutrittsversuchs nicht gültig war). Alle zur AirKey-Onlineverwaltung übertragenen Ereignisse bleiben dort unbegrenzt gespeichert.



Laden Sie die Ansicht der Protokolle von Zeit zu Zeit neu, um die aktuellen Einträge im Protokoll zu erhalten. Dafür steht Ihnen der Link **Ansicht neu laden** zur Verfügung.

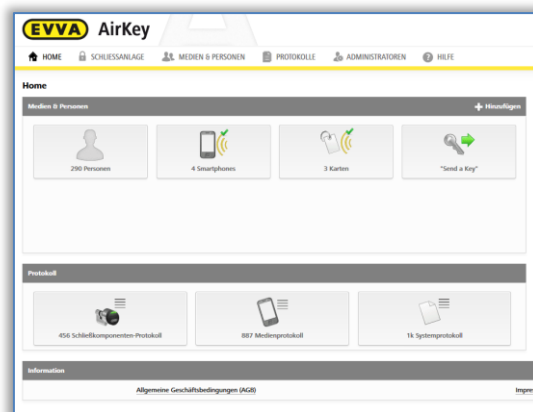


Abbildung 203: Protokolle



Es wird ausdrücklich darauf aufmerksam gemacht, dass das vorliegende AirKey-System nach gesetzlichen Bestimmungen, insbesondere des Datenschutzgesetzes melde-/genehmigungspflichtig sein kann. EVVA Sicherheitstechnologie GmbH übernimmt dementsprechend keinerlei Haftung und Gewähr für einen rechtskonformen Betrieb.



Aktivieren Sie das **Vier-Augen-Prinzip für die Protokolleinsicht**, um einen noch höheren Schutz für personenbezogene Daten zu gewährleisten. Dabei ist für die Einsicht des Schließkomponenten- und Medienprotokolls die Bestätigung eines zweiten Systemadministrators notwendig. Details zur Aktivierung finden Sie im Kapitel [Allgemein](#).

5.7.1 Schließkomponentenprotokoll

Wenn das **Vier-Augen-Prinzip für die Protokolleinsicht** nicht aktiviert ist, führen Sie folgende Schritte zur Einsicht des Schließkomponentenprotokolls aus:

- > Wählen Sie auf der Startseite **Home** die Kachel **Schließkomponentenprotokoll**
- > Alternativ wählen Sie im Hauptmenü **Protokolle** → **Schließkomponenten & Bereiche**.

Wenn das **Vier-Augen-Prinzip für die Protokolleinsicht** aktiviert ist, führen Sie zusätzlich folgende Schritte zur Einsicht des Schließkomponentenprotokolls aus:

- > Wählen Sie einen zweiten Systemadministrator aus der Liste, dem ein Bestätigungscode per E-Mail gesendet werden soll, und klicken Sie auf **Bestätigungscode senden**.

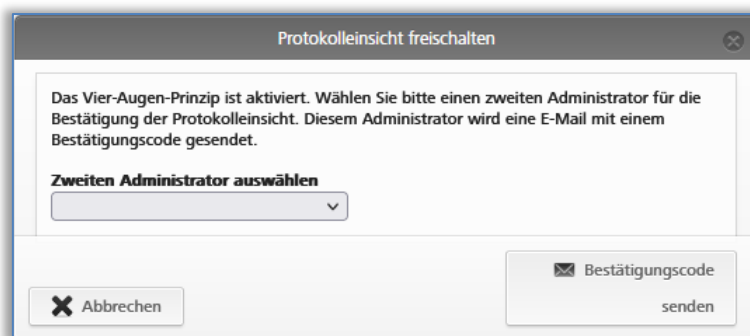


Abbildung 204: Protokolleinsicht freischalten – zweiten Administrator wählen

- > Daraufhin wird eine E-Mail mit einem Bestätigungscode an den ausgewählten Systemadministrator gesendet.
- > Dieser Bestätigungscode muss innerhalb von 10 Minuten in der AirKey-Onlineverwaltung eingegeben und mit dem Button **Freischalten** bestätigt werden.

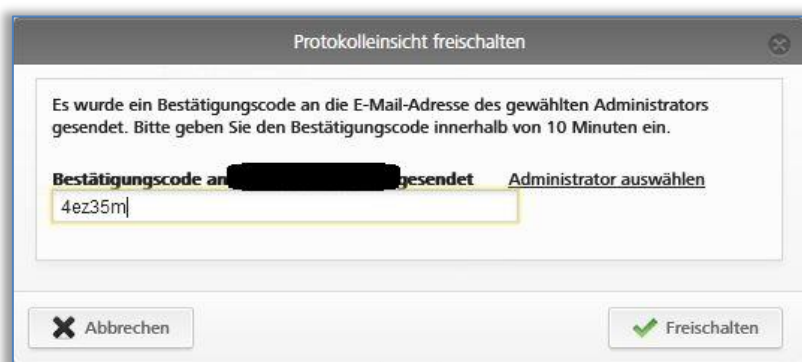


Abbildung 205: Protokolleinsicht freischalten – Bestätigungscode eingeben

Wird dieser Vorgang nicht innerhalb von 10 Minuten abgeschlossen, muss der Vorgang wiederholt werden. Wenn der gewählte Systemadministrator nicht reagiert, kann über den Link **Administrator auswählen** auch ein anderer Systemadministrator zum Freischalten der Protokolleinsicht ausgewählt werden.

Danach wird das Schließkomponentenprotokoll angezeigt.



Die Freischaltung der Protokolleinsicht ist bis zur nächsten Abmeldung des Systemadministrators aktiv. Das bedeutet, dass sowohl das Schließkomponenten- als auch das Medienprotokoll beliebig oft eingesehen werden können.

Die angezeigte Liste beinhaltet Einträge zu Schließkomponenten und Bereichen.

- > Wählen Sie bei Bedarf aus der linken Spalte einzelne Schließkomponenten bzw. Bereiche, für die Sie das Protokoll einsehen möchten. Sofern Sie wieder alle Schließkomponenten und Bereiche einsehen möchten, klicken Sie unten links auf **Alle Einträge** ①.
- > Geben Sie für die gezielte Suche von Einträgen mindestens 3 Zeichen im Suchfeld ② ein.

- > Zusätzlich können Sie den Filter durch Anklicken des gewünschten Links (z.B. "Nicht berechtigt") aktivieren. Dabei werden nur Einträge gelistet, bei denen der Zutritt verweigert wurde.
- > Die Liste ist standardmäßig nach Datum und Uhrzeit sortiert (die neuesten Einträge oben). Durch Anklicken der Spaltenüberschrift "Datum, Uhrzeit" können Sie die Reihenfolge der Sortierung ändern. Eine Sortierung nach anderen Spaltenüberschriften ist in dieser Tabelle nicht möglich.

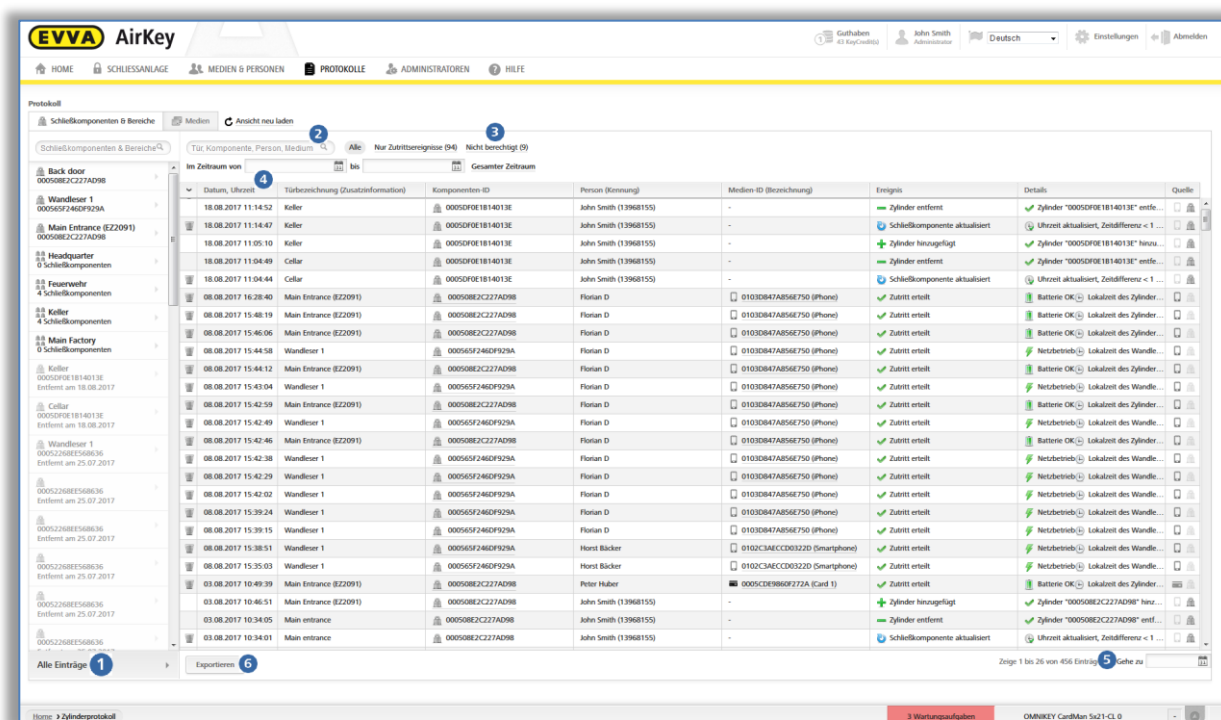


Abbildung 206: Protokoll Schließkomponenten & Bereiche

- > Wenn die Liste sehr viele Einträge enthalten sollte, können Sie rechts unten das Feld **Gehe zu** verwenden, um schnell zu einem bestimmten Kalendertag zu navigieren.
- > Verwenden Sie links unten den Button **Exportieren** , wenn Sie das gesamte Protokoll in eine CSV-Datei exportieren wollen. Diese kann unabhängig von der AirKey-Onlineverwaltung weiterbearbeitet werden.

Innerhalb des Protokolls werden alle notwendigen Informationen wie Datum und Uhrzeit, Türbezeichnung (Zusatzinformation), Komponenten-ID, Person (Kennung), Medien-ID (Bezeichnung) sowie das Ereignis gelistet. Zusätzlich werden nähere Informationen zu diesem Ereignis in der Spalte "Details" angezeigt.

In der Spalte "Quelle" sehen Sie, ob der Protokolleintrag von einem Medium und / oder von einer Schließkomponente stammt.



Laden Sie die Ansicht von Zeit zu Zeit neu, um die aktuellen Einträge im Protokoll angezeigt zu bekommen. Dafür steht Ihnen der Link **Ansicht neu laden** zur Verfügung.

Nutzen Sie die Protokollierungseinstellungen, um den Personenbezug in Protokolleinträgen entsprechend den Datenschutzvorgaben einzuschränken. Die Art des Personenbezugs in Protokolleinträgen für Schließkomponenten bestimmen Sie für neu hinzugefügte Schließkomponenten schließanlagenweit in den Einstellungen der Vorgabewerte für Protokollierung oder pro Schließkomponente in den Details der Schließkomponente.



Nur durch die regelmäßige Aktualisierung von Schließkomponenten kann sichergestellt werden, dass alle Protokolleinträge von Schließkomponenten in die AirKey-Onlineverwaltung übertragen werden. Die empfohlenen Aktualisierungsintervalle sind abhängig von der Frequentierung der Schließkomponente. Achten Sie auf [Werte und Limits](#) bei AirKey-Schließkomponenten.

Ein verweigerter Zutritt wird nur protokolliert, wenn das Medium eine Berechtigung auf die Schließkomponente besitzt, diese aber zum Zeitpunkt des Zutrittsversuchs nicht gültig war (z.B. die Berechtigung ist abgelaufen oder in der Zukunft gültig).

Der angezeigte Batteriestand in der Spalte "Details" ist immer der Batteriestand der AirKey-Schließkomponente (Zylinder) und nicht der Batteriestand des Smartphones.

Sofern bei Schließkomponenten die Protokollierung auf einen gewissen Zeitraum eingeschränkt ist, wird die Protokollierung der Zutrittsereignisse nach Ablauf dieses Zeitraums trotzdem weitergeführt. In diesem Fall wird nur der Personenbezug anonymisiert.

5.7.2 Medienprotokoll

Wenn das **Vier-Augen-Prinzip für die Protokolleinsicht** nicht aktiviert ist, führen Sie folgende Schritte zur Einsicht des Medienprotokolls aus:

- > Wählen Sie auf der Startseite **Home** die Kachel **Medienprotokoll**.
- > Alternativ wählen Sie im Hauptmenü **Protokolle** → **Medien**.

Wenn das **Vier-Augen-Prinzip für die Protokolleinsicht** aktiviert ist, führen Sie zusätzlich folgende Schritte zur Einsicht des Medienprotokolls aus:

- > Wählen Sie einen zweiten Systemadministrator aus der Liste, dem ein Bestätigungscode per E-Mail gesendet werden soll, und klicken Sie auf **Bestätigungscode senden**.

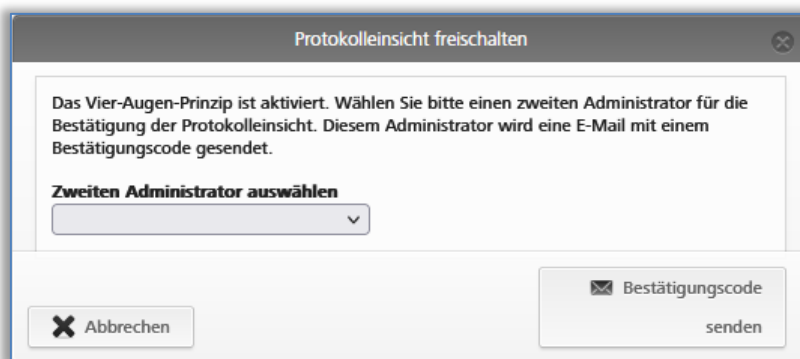


Abbildung 207: Protokolleinsicht freischalten – zweiten Administrator wählen

- > Daraufhin wird eine E-Mail mit einem Bestätigungscode an den ausgewählten Systemadministrator gesendet.
- > Dieser Bestätigungscode muss innerhalb von 10 Minuten in der AirKey-Onlineverwaltung eingegeben und mit dem Button **Freischalten** bestätigt werden.

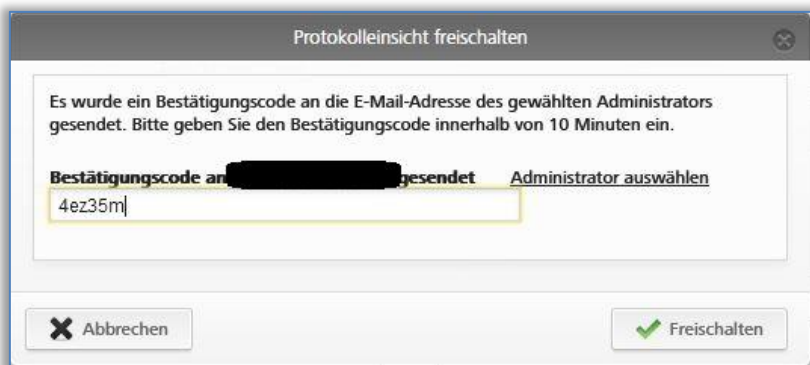


Abbildung 208: Protokolleinsicht freischalten – Bestätigungscode eingeben

Wird dieser Vorgang nicht innerhalb von 10 Minuten abgeschlossen, muss der Vorgang wiederholt werden. Wenn der gewählte Systemadministrator nicht reagiert, kann über den Link **Administrator auswählen** auch ein anderer Systemadministrator zum Freischalten der Protokolleinsicht ausgewählt werden.

Danach wird das Medienprotokoll angezeigt.



Die Freischaltung der Protokolleinsicht ist bis zur nächsten Abmeldung des Systemadministrators gültig. Das bedeutet, dass sowohl das Schließkomponenten- als auch Medienprotokoll beliebig oft eingesehen werden kann.

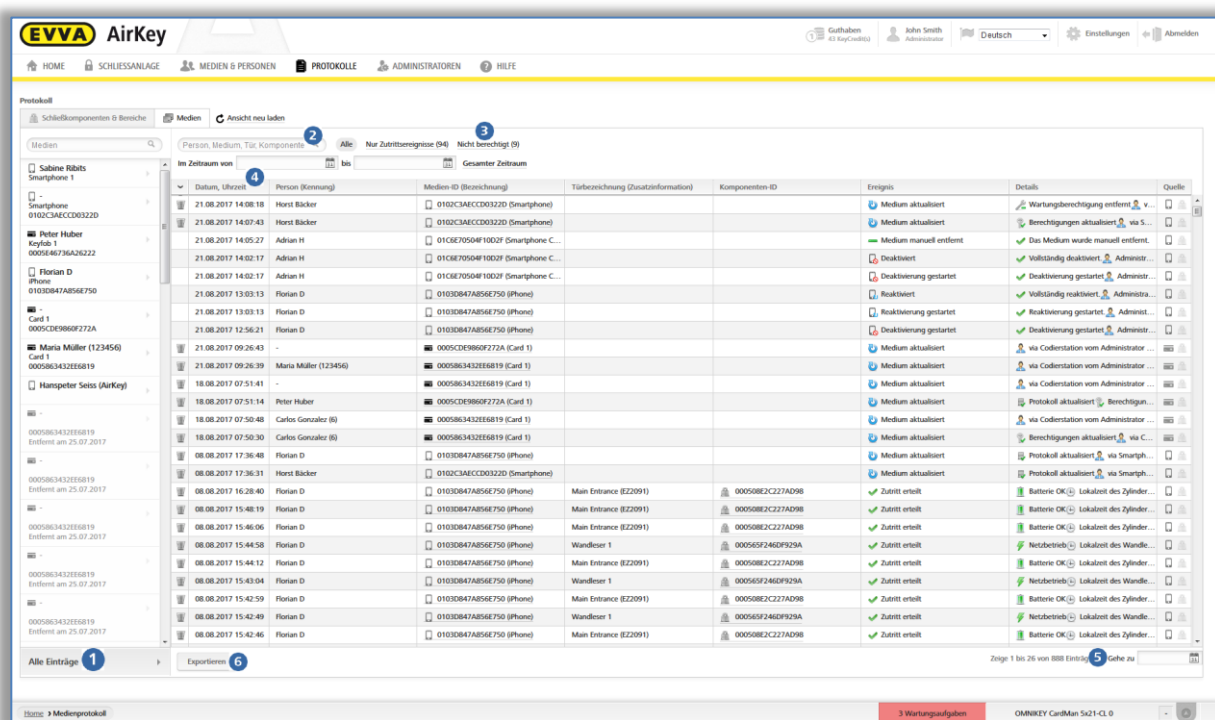


Abbildung 209: Medienprotokoll

Sie erhalten einen Überblick aller Einträge von den Medien.

- > Wählen Sie bei Bedarf einzelne Medien, für die Sie das Protokoll einsehen möchten, aus der linken Spalte. Sofern Sie wieder alle Medien einsehen möchten, klicken Sie unten links auf **Alle Einträge** ❶.
- > Geben Sie für die gezielte Suche von Einträgen mindestens 3 Zeichen im Suchfeld ein ❷.
- > Setzen Sie Filter, wie z.B. "Nicht berechtigt" ❸. Dabei werden Einträge gelistet, bei denen der Zutritt verweigert wurde.
- > Sortieren Sie die Liste nach Datum und Uhrzeit ❹.
- > Verwenden Sie rechts unten das Feld **Gehe zu** ❺, um in einer großen Liste schnell zu einem bestimmten Tag zu navigieren.
- > Verwenden Sie links unten den Button **Exportieren** ❻, wenn Sie das gesamte Medienprotokoll in eine CSV-Datei exportieren wollen. Diese kann unabhängig von der AirKey-Onlineverwaltung weiterbearbeitet werden.

Innerhalb des Protokolls werden alle notwendigen Informationen wie Datum und Uhrzeit, Person (Kennung), Medien-ID (Bezeichnung), Türbezeichnung (Zusatzinformation), Komponenten-ID sowie Ereignis gelistet. Zusätzlich werden genauere Informationen zu dem Ereignis in der Spalte "Details" angezeigt.

In der Spalte "Quelle" sehen Sie, ob der Protokolleintrag von einem Medium und/oder von einer Schließkomponente stammt.

Nutzen Sie die Protokollierungseinstellungen, um den Personenbezug in Protokolleinträgen entsprechend den Datenschutzvorgaben einzuschränken. Die Art des Personenbezugs in Protokolleinträgen für Schließkomponenten bestimmen Sie für neu hinzugefügte Schließkomponenten schließanlagenweit in den [Einstellungen](#), oder pro Schließkomponente in den Details der Schließkomponente.

Die Protokolleinträge eines bestimmten Mediums können auch über das Medium selbst eingesehen werden. Wählen Sie dazu das gewünschte Medium aus der Medienliste und wechseln Sie in den Reiter **Protokoll**.



Ein verweigerter Zutritt wird nur protokolliert, wenn das Medium eine Berechtigung auf die Schließkomponente besitzt, diese aber zum Zeitpunkt des Zutrittsversuchs nicht gültig war (z.B. die Berechtigung ist abgelaufen oder in der Zukunft gültig).

Der angezeigte Batteriestand in der Spalte "Details" ist immer der Batteriestand der AirKey-Schließkomponente (Zylinder) und nicht der Batteriestand des Smartphones.

Sofern bei Schließkomponenten die Protokollierung auf einen gewissen Zeitraum eingeschränkt ist, wird die Protokollierung der Zutrittsereignisse nach Ablauf dieses Zeitraums trotzdem weitergeführt. In diesem Fall wird nur der Personenbezug anonymisiert.

Für das Schließkomponenten- und Medienprotokoll gilt, dass Protokolleinträge mit Personenbezug aus datenschutzrechtlichen Gründen auch nachträglich anonymisiert werden können. Datenschutzkritische Protokolleinträge, wie zum Beispiel Zutritte, sind in der ersten Spalte mit einem Symbol eines Papierkorbs versehen.

Um den Personenbezug in Protokolleinträgen zu anonymisieren, gehen Sie bitte wie folgt vor:

- > Suchen Sie den zu anonymisierenden Protokolleintrag und klicken Sie auf das Papierkorbsymbol in der ersten Spalte.
- > Es erscheint eine Abfrage, ob nur dieser Protokolleintrag oder alle Einträge zu dieser Person gelöscht werden sollen. Wählen Sie die gewünschte Option.
- > Tragen Sie einen Grund für das Löschen des Protokolleintrags ein.
- > Setzen Sie das Häkchen bei der Checkbox **Ich möchte den Protokolleintrag / die Protokolleinträge unwiderruflich löschen**.
- > Um den Vorgang abzuschließen, bestätigen Sie mit **Löschen**.

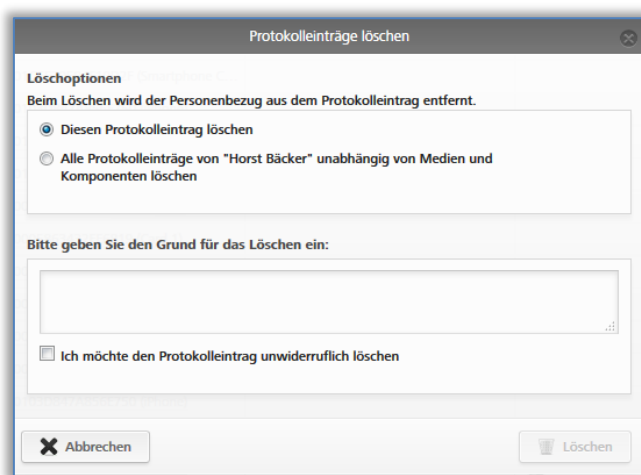


Abbildung 210: Protokolleinträge löschen



Der Protokolleintrag wird nicht komplett gelöscht, sondern nur der Personenbezug. Somit wird der Protokolleintrag anonymisiert. Dieser Vorgang kann nicht rückgängig gemacht werden. Nutzen Sie diese Funktion mit Sorgfalt.



Das Löschen eines Protokolleintrags wird im Systemprotokoll gelistet.

5.7.3 Systemprotokoll

- > Wählen Sie auf der Startseite **Home** die Kachel **Systemprotokoll**.
- > Alternativ wählen Sie im Hauptmenü **Protokolle** → **System**.

Sie erhalten eine Übersicht über alle Aktionen, die von Administratoren durchgeführt wurden.

- > Im Suchfeld ❶ können Sie nach Administrator, Benutzerkennung, Aktion, Transaktions-ID, Medien-ID oder Komponenten-ID suchen. Geben Sie einen bestimmten Zeitraum ❷ ein und bestimmen Sie die Spalte, nach der sortiert ❸ werden soll.

- > Geben Sie im Feld **Gehe zu** ⁴ ein Datum ein, damit Sie im Systemprotokoll direkt zu einem Tag navigieren können. Wenn es für das eingegebene Datum keine Einträge gibt, wird der nächstliegende Eintrag gewählt.
- > Verwenden Sie links unten den Button **Exportieren**, wenn Sie das gesamte Systemprotokoll in eine CSV-Datei exportieren wollen. Diese kann dann unabhängig von der AirKey-Onlineverwaltung weiterbearbeitet werden.

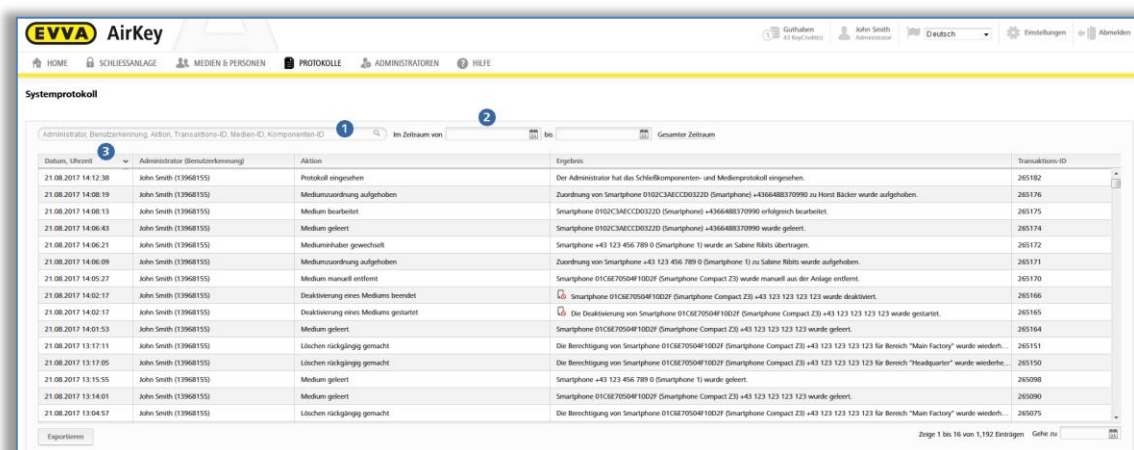


Abbildung 211: Systemprotokoll



Im Systemprotokoll können keine Protokolleinträge gelöscht werden.



Das Vier-Augen-Prinzip für die Protokolleinsicht wird nicht auf das Systemprotokoll angewendet. Das bedeutet, dass Systemadministratoren immer das Systemprotokoll einsehen können.

5.8 Support-Freigaben

Durch das Anlegen einer Support-Freigabe können Sie einen Administrator auf Zeit erstellen sollten Sie einmal Unterstützung in AirKey benötigen. Über die Support-Freigabe können die kompletten Daten der Schließenanlage eingesehen werden.



Der Empfänger hinter der Support-Freigabe hat für die Dauer der Freigabe die gleichen Rechte wie Sie als Administrator.

5.8.1 Support-Freigabe anlegen

- > Wählen Sie im Hauptmenü **Administratoren** → **Support-Freigaben**.

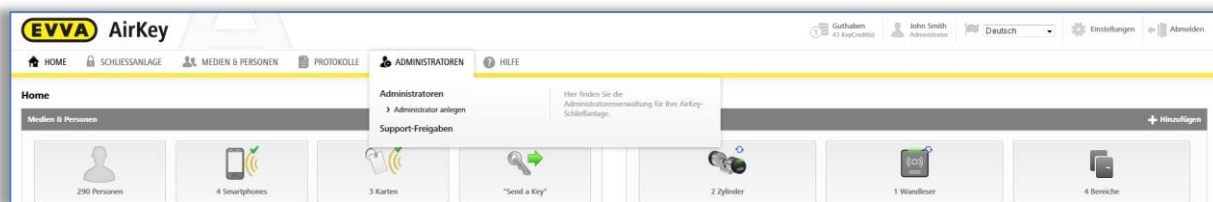


Abbildung 212: Support-Freigaben

Wenn Sie bereits Support-Freigaben erstellt haben, werden diese in einer Liste angezeigt.

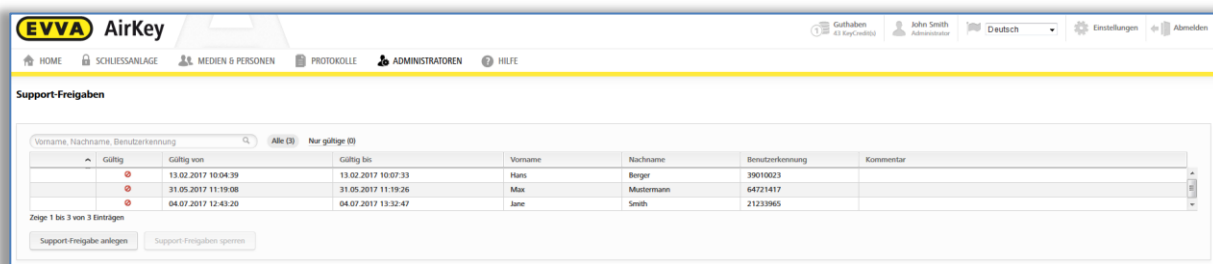


Abbildung 213: Liste Support-Freigaben

- > Klicken Sie auf **Support-Freigabe anlegen**.
- > Füllen Sie das Formular **1** aus.
Felder, die mit * gekennzeichnet sind, sind Pflichtfelder.



Die Dauer der Freigabe liegt zwischen 1 und maximal 24 Stunden.

- > Klicken Sie auf **Speichern**.

Die Support-Freigabe wurde angelegt und eine Benutzerkennung mit Passwort erstellt **2**.

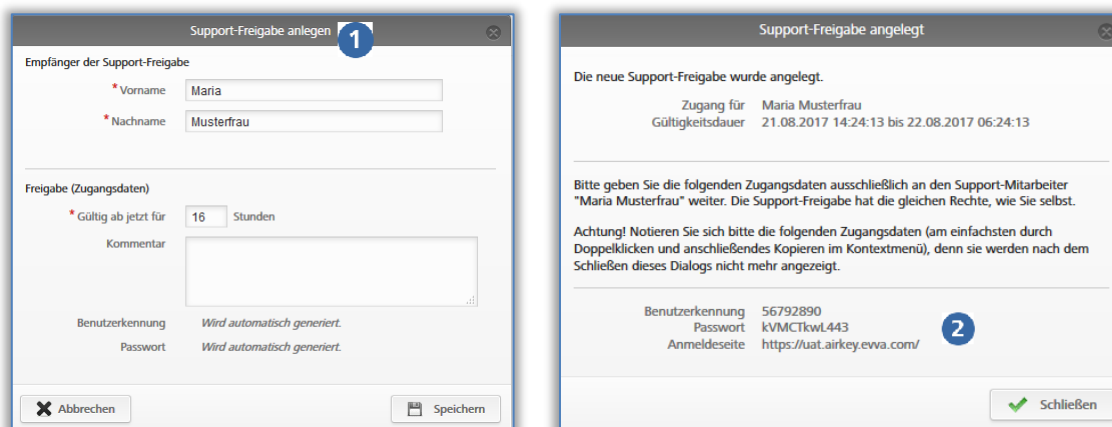


Abbildung 214: Support-Freigabe anlegen



Das Passwort wird nach dem Schließen des Dialogfensters nicht mehr angezeigt.

In Ihrem eigenen Interesse sollten Sie die Login-Daten auf einem sicheren Weg übergeben.

- > **Schließen** Sie das Dialogfenster "Support-Freigabe angelegt", wenn die Daten an den Support-Partner übergeben wurden.

5.8.2 Support-Freigabe sperren

Die Support-Freigabe endet automatisch nach Ablauf der festgelegten Dauer. Sie kann jedoch auch vorzeitig mit der Funktion **Support-Freigabe sperren** aufgehoben werden.

Wenn Sie die Support-Freigabe vorzeitig aufheben möchten, gehen Sie wie folgt vor:

- > Wählen Sie im Hauptmenü **Administratoren** → **Support-Freigaben**.

In der Liste der Support-Freigaben sehen Sie, ob eine Support-Freigabe aktuell gültig ❶ ist und wie lange die Gültigkeit ❷ andauert.

Vorname, Nachname, Benutzername	Gültig ❶	Gültig von	Gültig bis ❷	Vorname	Nachname	Benutzerkennung	Kommentar
	✓	21.08.2017 14:24:13	22.08.2017 06:24:13	Maria	Musterfrau	56792890	
	❶	04.07.2017 12:43:20	04.07.2017 13:32:47	Jane	Smith	21233965	
	❶	31.05.2017 11:19:08	31.05.2017 11:19:26	Max	Mustermann	64721417	
	❶	13.02.2017 10:04:39	13.02.2017 10:07:33	Hans	Berger	39010023	

Abbildung 215: Support-Freigabenübersicht

- > Wählen Sie den Empfänger der Support-Freigabe, für den Sie die Freigabe beenden möchten.
- > Klicken Sie auf **Support-Freigabe sperren**.
- > Bestätigen Sie die Sicherheitsabfrage mit **Support-Freigaben sperren**.

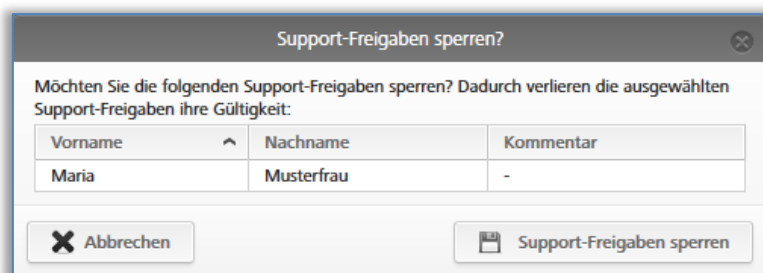


Abbildung 216: Support-Freigaben sperren

In der Liste der Support-Freigaben erkennen Sie am Symbol in der Spalte "Gültig" ❶, dass die Freigabe gesperrt ist.

The screenshot shows the EVVA AirKey web interface. At the top, there is a navigation bar with the EVVA logo, 'AirKey', and user information (John Smith, Administrator). Below the navigation bar, there are menu items: HOME, SCHLEISSANLAGE, MEDIEN & PERSONEN, PROTOKOLLE, ADMINISTRATOREN, and HILFE. The main content area is titled 'Support-Freigaben'. It features a search bar and a table with columns: Gültig, Gültig von, Gültig bis, Vorname, Nachname, Benutzerkennung, and Kommentar. The table contains four entries, each with a red circle icon in the 'Gültig' column. Below the table, there are buttons for 'Support-Freigabe anlegen' and 'Support-Freigaben sperren'.

Gültig	Gültig von	Gültig bis	Vorname	Nachname	Benutzerkennung	Kommentar
⊘	21.08.2017 14:24:13	21.08.2017 14:28:35	Maria	Musterfrau	5678990	
⊘	04.07.2017 12:42:30	04.07.2017 13:32:47	Jane	Smith	2133985	
⊘	31.05.2017 11:19:08	31.05.2017 11:19:26	Max	Mustermann	64721417	
⊘	13.02.2017 10:04:39	13.02.2017 10:07:33	Hans	Berger	39010023	

Abbildung 217: Gültigkeit der Support-Freigaben



Sowohl die durchgeführten Tätigkeiten des Empfängers der Support-Freigabe als auch das Anlegen oder Sperren der Support-Freigabe werden entsprechend in den Protokollen eingetragen.

5.9 Hilfe

Weiterführende Erklärungen finden Sie im Hauptmenü **Hilfe** bzw. auf der EVVA-AirKey-Produktwebseite unter <https://www.evva.com/de/airkey/website/>. Benötigen Sie darüber hinaus Unterstützung, wenden Sie bitte sich an Ihren EVVA-Fachhändler.

6 AirKey-App

Dieses Kapitel bietet Ihnen einen Überblick über die Funktionen, die Sie mit Ihrem Smartphone innerhalb der AirKey-App durchführen können.

Wenn Sie ein Smartphone für AirKey verwenden möchten, müssen folgende Voraussetzungen erfüllt sein:

- > Das Smartphone entspricht den [Systemvoraussetzungen](#) für AirKey.
- > Die AirKey-App wurde auf dem Smartphone erfolgreich installiert.
- > Eine aktive Internetverbindung ist verfügbar.



Durch den Einsatz von "App-Optimierungen", z.B. um den Akku zu schonen, kann die Funktionalität der App beeinflusst werden. Mögliche Auswirkungen davon sind: Sperrvorgang dauert länger, Sperren im Hintergrund funktioniert nicht stabil etc.

6.1 Bluetooth-Komponenten

Bei diesem Menüpunkte kommt man auf eine Übersichtsliste, die alle Bluetooth-Schließkomponenten in Reichweite anzeigt. Über diese Seite kann man sich zum Beispiel mit [Komponenten verbinden](#), Bluetooth-Komponenten sperren oder sich über das Symbols rechts oben mit NFC-Komponenten verbinden.



Die Bezeichnung von Bluetooth-Komponenten wird erst nach einer Aktualisierung des Smartphones richtig angezeigt, d.h., dass sich die Anzeige der Bezeichnung einer Schließkomponente innerhalb der AirKey-App nicht automatisch ändert, wenn diese in der AirKey-Onlineverwaltung angepasst wird.

Ab Android 6 ist von Google vorgegeben, dass zum Erkennen von Bluetooth-Komponenten die Berechtigung zur Standortermittlung am Smartphone erteilt sein muss.

6.2 [Smartphone registrieren](#): Siehe Kapitel 4.9

6.3 Berechtigungen

Wenn Ihr Smartphone in der AirKey-Anlage registriert ist und bereits Berechtigungen über die AirKey-Onlineverwaltung ausgestellt und angefertigt wurden, haben Sie jederzeit Einblick auf die Berechtigungen des Smartphones.

- > Starten Sie die AirKey-App.
- > Wählen Sie im Menü **Berechtigungen**.

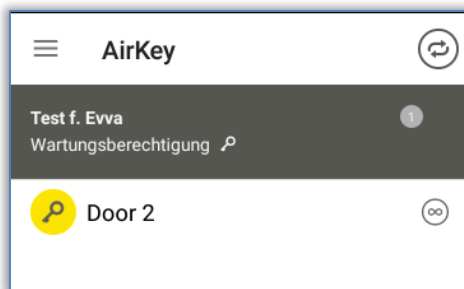


Abbildung 218: AirKey-App – Berechtigungsübersicht

- > Tippen Sie auf eine der Berechtigungen, um die Details zur Berechtigung zu erhalten. Die Standortdaten (GPS-Koordinaten oder Adresse) sind hier als Link dargestellt. Wenn Sie den Link antippen, erfolgt eine automatische Weiterleitung zu dem Kartenanbieter, der auf Ihrem Smartphone als Standard eingestellt ist.
- > In den Berechtigungsdetails können Sie auch individuell für jede Berechtigung den Hands-free-Modus aktivieren. Voraussetzung dafür ist, dass der Administrator den Hands-free-Modus bei der Schließkomponente erlaubt hat, dass für die AirKey-App keine PIN festgelegt wurde und in den Einstellungen der App der Hands-free-Modus aktiviert wurde.

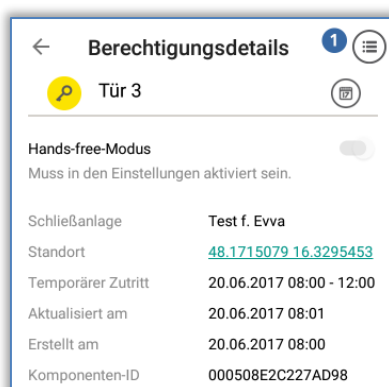


Abbildung 219: AirKey-App – Berechtigungsdetails

Wenn die Berechtigung für den Zutritt abgelaufen ist, wird das entsprechend angezeigt.

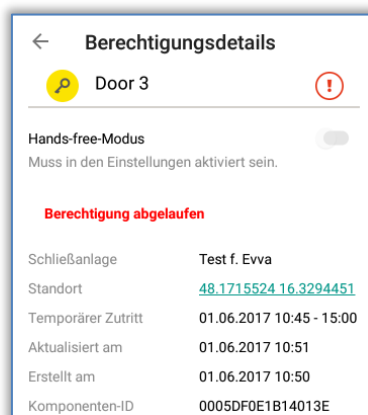


Abbildung 220: Berechtigung abgelaufen



Wenn Ihr Smartphone berechtigt ist Protokolldaten anzuzeigen (siehe [Protokolldaten in der AirKey-App](#)), kann in den Berechtigungsdetails **1** das Schlüsselprotokoll zu der ausgewählten Berechtigung angezeigt werden.



Abbildung 221: Protokolldaten einer Berechtigung

6.4 [Wartungsaufgaben](#): Siehe Kapitel 6.12

6.5 Daueröffnung

Die Daueröffnung setzt voraus, dass in der AirKey-Onlineverwaltung die manuelle Daueröffnung für die AirKey-Schließkomponente aktiviert ist (siehe [Schließkomponente bearbeiten](#)), sowohl für die Bluetooth- als auch die NFC-Schließkomponente.

- > Wählen Sie im AirKey-App Menü **Daueröffnung**.
- > Wählen Sie aus der angezeigten Liste eine Bluetooth-Schließkomponente oder halten Sie das Smartphone an eine NFC-Schließkomponente.
- > Die Schließkomponente signalisiert optisch und akustisch die Sperrung.
- > Sie erhalten eine Erfolgsmeldung **1**.

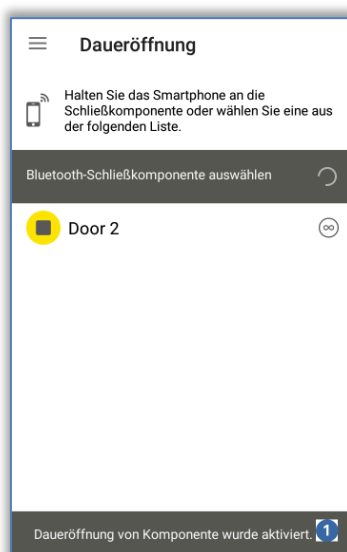


Abbildung 222: Daueröffnung Erfolgsmeldung



Die Aktivierung der Daueröffnung bei Schließkomponenten und Medien erhöht den Stromverbrauch der Komponenten. Aktivieren Sie die Daueröffnung nur bei jenen Schließkomponenten und Medien, die diese Funktion auch nutzen.

6.6 PIN eingeben

Sie können eine aktive PIN für eine bestimmte Zeit innerhalb der AirKey-App zwischenspeichern, indem Sie die Funktion **PIN eingeben** nutzen.

- > Öffnen Sie das Menü innerhalb der AirKey-App und tippen Sie auf **PIN eingeben**.
- > Geben Sie die richtige PIN ein tippen Sie auf **OK**.

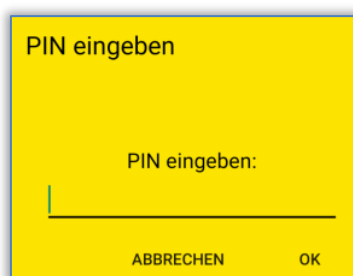


Abbildung 223: AirKey-App – PIN eingeben



Die PIN wird solange zwischengespeichert, bis die AirKey-App beendet, in den Hintergrund gelegt oder die Displaysperre aktiv wird. Damit können Sie Schließkomponenten sperren, ohne die PIN erneut eingeben zu müssen.

Die PIN wird ebenfalls zwischengespeichert, wenn sie zum ersten Entsperrn einer Schließkomponente verlangt wird. Beim nächsten Entsperrn einer Schließkomponente (die gleiche oder auch eine andere) wird die PIN nicht mehr verlangt. Das gilt ebenfalls solange, bis die AirKey-App beendet, in den Hintergrund gelegt wird oder die Displaysperre aktiv wird.

6.7 Medien codieren

Diese AirKey-App Funktion ermöglicht es, Zutrittsmedien (außer Smartphones) über Bluetooth-fähige Schließkomponenten (Zylinder, Wandler) zu aktualisieren.

- > Wählen Sie im AirKey-Menü **Medien codieren**.
- > Aus der Liste der angezeigten Bluetooth-Schließkomponenten wählen Sie jene aus, über die Sie das Medium aktualisieren möchten.

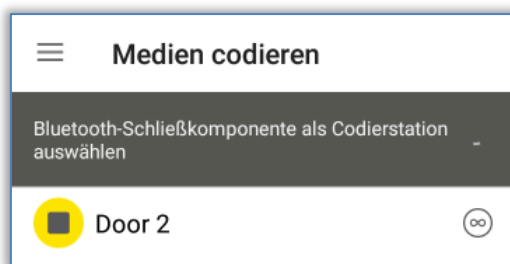


Abbildung 224: Medien codieren – Auswahlliste Bluetooth – Schließkomponenten

- > Halten Sie das Medium, das Sie aktualisieren möchten, an die AirKey-Schließkomponente.



Abbildung 225: Medien codieren

- > Folgen Sie ab jetzt den Anweisungen aus [Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen](#).



Für die Funktion "Medien codieren" muss der Vorgang am Zylinder mit der Hand und nicht mit einem Medium (Karte, Schlüsselanhänger, Kombischlüssel oder Armbänder) gestartet werden. Ansonsten würde ein normaler Sperrvorgang anstatt eines Kommunikationsaufbaus mit dem Smartphone stattfinden.

Bei batteriebetriebenen Schließkomponenten verbraucht der Vorgang der Medienaktualisierung Energie und verkürzt die Lebensdauer der Batterien. Wenn viele Medien aktualisiert werden sollen, empfiehlt es sich deswegen, entweder eine AirKey-Codierstation, ein Smartphone mit NFC-Funktionalität oder einen Wandler zu verwenden.



Der Hands-free-Modus am Smartphone muss deaktiviert werden, um die Funktion "Medien codieren" durchführen zu können.

6.8 Berechtigungsprotokoll

Wählen Sie im Hauptmenü der AirKey-App den Punkt **Berechtigungsprotokoll** und Sie erhalten ein Protokoll über die Berechtigungsänderungen, die vom Administrator der AirKey-Schließanlage für Ihr Smartphone durchgeführt wurden.

Diese Protokollierung findet immer statt, unabhängig von diversen Einstellungen in der AirKey-Onlineverwaltung und AirKey-App.

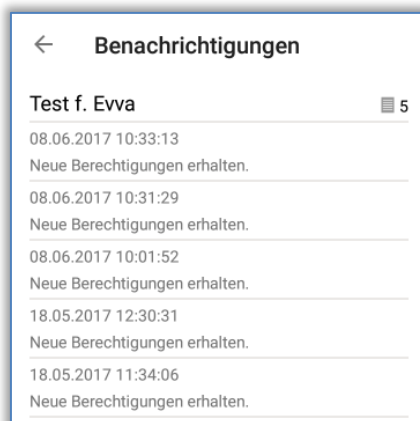


Abbildung 226: Berechtigungsprotokoll

6.9 Einstellungen der AirKey-App

6.9.1 Einstellungen der AirKey-App auf Android-Smartphones

Im Menüpunkt **Einstellungen** der AirKey-App sehen Sie grundlegende Informationen zu Ihrem Android-Smartphone. Hier sehen Sie z.B., ob NFC und Bluetooth aktiviert sind. Tippen Sie auf einen der zwei Einträge, gelangen Sie in die Geräteeinstellungen Ihres Smartphones. Als Nächstes können Sie hier entscheiden, ob Bluetooth für AirKey verwendet werden soll. Aktivieren Sie einfach die entsprechende Option "Bluetooth verwenden".

In diesem Fall können auch die darunterliegenden Einstellungen ("Hands-free-Reichweite einstellen", "Hands-free-Modus" und "Sperrern aus Benachrichtigungen") verwendet werden. Die Startseite beim Öffnen der AirKey-App ist in diesem Fall "Bluetooth-Komponenten".

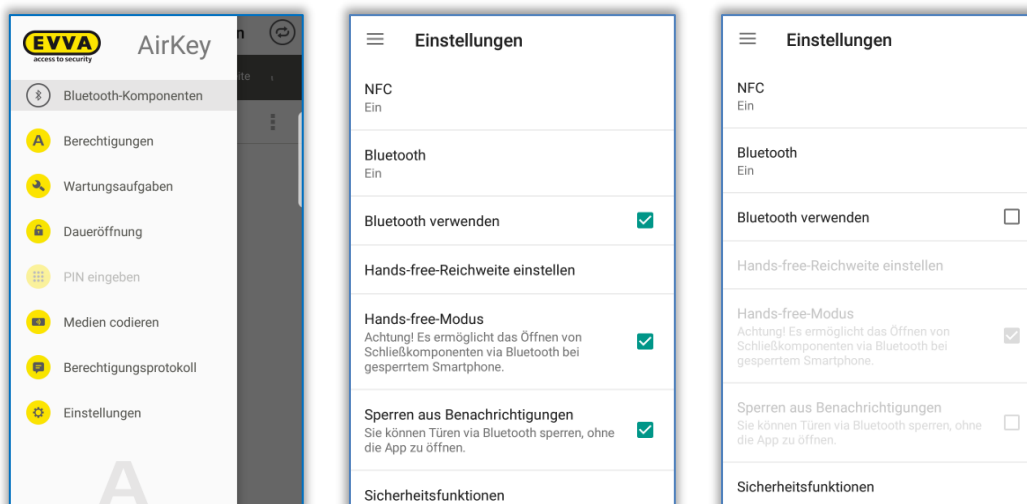


Abbildung 227: Android-Smartphone mit Bluetooth – Hauptmenü / Option "Bluetooth verwenden" aktiviert / Option deaktiviert

Wenn Sie die Option "Bluetooth verwenden" deaktivieren, werden die drei erwähnten Folgeinstellungen automatisch deaktiviert und alle weiteren Bluetooth-abhängigen Funktionen aus dem Hauptmenü ("Bluetooth-Komponenten", "Daueröffnung" und "Medien codieren")

zeigen den Hinweis "Bluetooth ist deaktiviert". Das Smartphone kann in dieser Situation mit den Schließkomponenten nur über NFC kommunizieren.



Wenn das Android-Smartphone älter ist und über NFC- aber nicht über Bluetooth-Funktionalität verfügt, werden alle Bluetooth-abhängigen Funktionen und Einstellungen ausgeblendet.

6.9.2 Einstellungen der AirKey-App auf iPhones

Im Menüpunkt **Einstellungen** der AirKey-App sehen Sie grundlegende Informationen zu Ihrem iPhone. Hier sehen Sie z.B., ob Bluetooth aktiviert ist. In diesem Fall können auch die darunterliegenden Einstellungen ("Hands-free-Reichweite einstellen", "Hands-free-Modus" und "Sperren aus Benachrichtigungen") verwendet werden.

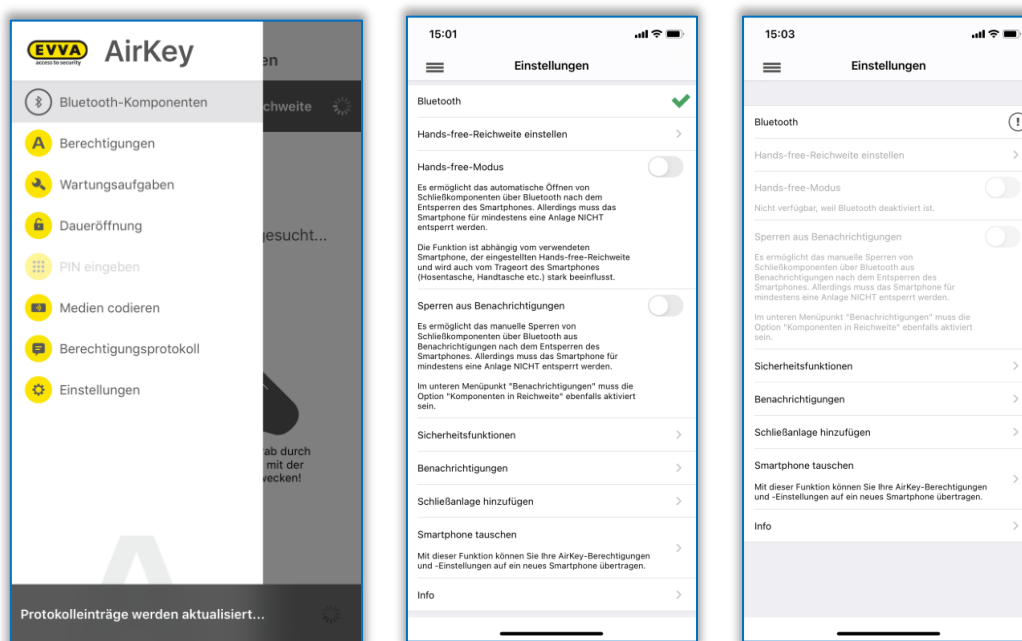


Abbildung 228: iPhone (nur mit Bluetooth) – Hauptmenü / Einstellungen ohne NFC-abhängige Funktionen / Funktion Bluetooth deaktiviert

Der Eintrag "Bluetooth" in den AirKey-Einstellungen zeigt nur, ob die Bluetooth-Funktionalität aktiviert ist oder nicht. Sie können trotzdem auf den Eintrag "Bluetooth" tippen, um zu der Bluetooth-Einstellung in den Geräteeinstellungen Ihres iPhones zu gelangen.



Wenn Sie Bluetooth in den iPhone-Geräteeinstellungen deaktivieren, können Sie KEINE Schließkomponenten mehr sperren!

Die deaktivierte Bluetooth-Funktionalität wird in den AirKey-Einstellungen entsprechend angezeigt und die drei davon abhängigen Folgeinstellungen werden automatisch deaktiviert, genauso wie alle weiteren Bluetooth-abhängigen Funktionen aus dem Hauptmenü ("Bluetooth-Komponenten", "Daueröffnung" und "Medien codieren").

6.9.3 Hands-free-Reichweite einstellen

Wählt man die Funktion "Hands-free-Reichweite einstellen", gelangt man in ein Untermenü. Hier wählt man aus, für welchen Schließkomponententyp die Reichweite eingestellt werden soll oder ob man die Reichweiten (für alle Schließkomponenten) zurücksetzen will.

Reichweite für Zylinder

- > Beim Zylinder zeigt Ihnen die AirKey-App alle in Reichweite befindlichen und aktiven Bluetooth-Zylinder, nachdem diese vorher durch händische Berührung aufgeweckt wurden.
- > Wählen Sie den entsprechenden Zylinder aus und entfernen Sie sich so weit von diesem, wie Sie wünschen, damit die automatische Erkennung des Smartphones funktioniert.
- > Drücken Sie **Speichern**.

Reichweite für Wandleser

- > Beim Wandleser zeigt Ihnen die AirKey-App alle in Reichweite befindlichen Bluetooth-Wandleser.
- > Wählen Sie den entsprechenden Wandleser aus und entfernen Sie sich so weit von diesem, wie Sie wünschen, damit die automatische Erkennung des Smartphones funktioniert.
- > Drücken Sie **Speichern**.



Dabei wird die Stärke des Signals am Display angezeigt. Bitte beachten Sie, dass das abhängig von Umwelteinflüssen, wie Funkverkehr etc. und vom benutzten Smartphone abweichen kann.



Die Standardreichweite beträgt ca. 50-70 cm, ist aber hersteller- und geräteabhängig. Aus Sicherheitsgründen empfiehlt EVVA, die Reichweite auf ca. 30 cm einzustellen.

Alle Bluetooth-Reichweiten zurücksetzen

Durch Tippen auf **Alle Bluetooth-Reichweiten zurücksetzen** werden alle manuell gesetzten Reichweiten gelöscht und wieder die Standardreichweiten verwendet. Eine Hinweismeldung bestätigt das Zurücksetzen der Reichweiten.

6.9.4 Hands-free-Modus

Setzen Sie das Häkchen bei **Hands-free-Modus**, um die Funktion zu aktivieren. Alle weiteren Informationen finden Sie im Kapitel [Hands-free auf einen Blick](#).

6.9.5 Sperren aus Benachrichtigungen

Bei dieser Funktion ist es möglich, AirKey-Schließkomponenten mit Bluetooth zu sperren, ohne die AirKey-App zu öffnen.

Setzen Sie das Häkchen bei **Sperren aus Benachrichtigungen**, um die Funktion zu aktivieren.



Bei Android-Smartphones wird durch die Aktivierung dieser Funktion ein Dienst gestartet. Dieser Dienst sucht auch bei beendeter AirKey-App dauerhaft nach Bluetooth-Schließkomponenten in Reichweite und führt zu einem erhöhten Akku-Verbrauch des Smartphones. Der Dienst wird

beendet, sobald die Funktion wieder deaktiviert wird. Tippt man auf die Benachrichtigung des Dienstes, gelangt man direkt in die Einstellungen der AirKey-App.

Sobald Sie mit Ihrem Smartphone in die Reichweite einer AirKey-Schließkomponente kommen, für die Sie eine Zutrittsberechtigung besitzen, erhalten Sie eine Benachrichtigung auf dem Sperrbildschirm oder Startbildschirm Ihres Smartphones. Über diese Benachrichtigung können Sie dann die Schließkomponente sperren.

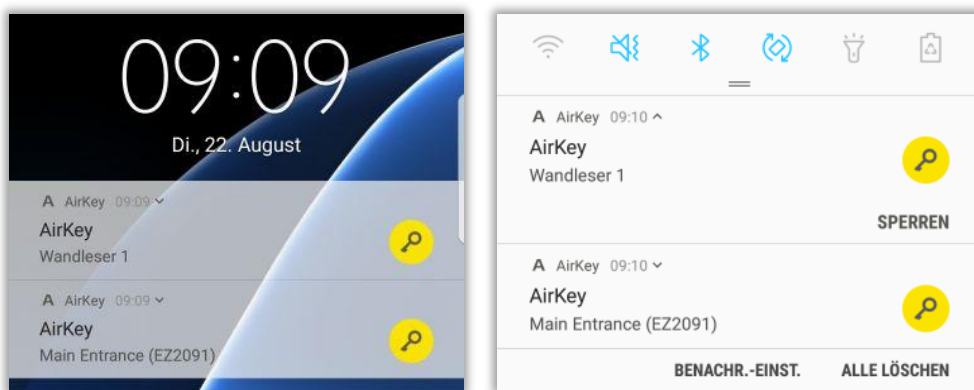



Abbildung 229: Sperrungen aus Benachrichtigung – Sperrbildschirm

Die Benachrichtigung auf dem Startbildschirm des Smartphones erfolgt in Form eines **A**-Symbols , das in der linken oberen Ecke erscheint. Zieht man den oberen Bildschirmrand nach unten, werden die Benachrichtigungen angezeigt, mit denen Schließkomponenten gesperrt werden können.

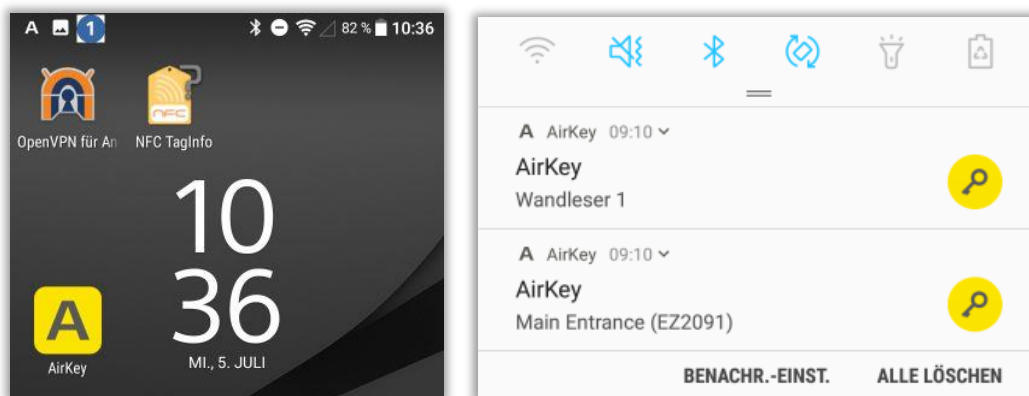


Abbildung 230: Sperrungen aus Benachrichtigung



Abhängig vom Smartphone-Modell interagieren Sie mit der Benachrichtigung durch einfaches Tippen auf die Benachrichtigung oder aufklappen, Wischen oder gedrückt halten der Benachrichtigung und anschließendem Tippen auf **Sperren**.



Abhängig von der Einstellung **Zutritt aus Sperrbildschirm** in den Einstellungen der AirKey-Onlineverwaltung kann entweder direkt aus dem Sperrbildschirm gesperrt werden, oder es muss vorab der Sperrbildschirm aufgehoben werden. Weitere Details finden Sie im Kapitel [Allgemein](#).



Sperren aus Benachrichtigungen ist nur möglich, wenn die Benachrichtigungen für "Komponenten in Reichweite" in den Einstellungen der AirKey-App aktiviert sind. Die Konfiguration der Benachrichtigungen finden Sie im Kapitel [Benachrichtigungen](#).

6.9.6 Sicherheitsfunktionen

Im Menü **Sicherheitsfunktionen** finden Sie drei Sicherheitsebenen:

AirKey-Verschlüsselung ①

Hierbei handelt es sich um eine zusätzliche PIN. Die PIN besteht aus 4 bis 12 Ziffern und verhindert die missbräuchliche Verwendung im Fall eines Verlusts oder Diebstahls des Smartphones.

EVVA empfiehlt die Vergabe einer PIN. Verwenden Sie eine möglichst lange PIN und achten Sie darauf, dass nur Sie in Kenntnis über die PIN sind!

Bildschirm Sperre ②

Die Sicherheitsfunktion des Betriebssystems stellt sicher, dass das Smartphone gegen ein Entsperren des Bildschirms von Dritten gesichert ist. Die Auswahl dieser Funktion navigiert Sie direkt in die Einstellungen des Android-Smartphones.

EVVA empfiehlt das Aktivieren einer Bildschirm Sperre, die nur der Eigentümer des Smartphones kennt!

Telefonverschlüsselung ③

Die Sicherheitsfunktion des Betriebssystems stellt sicher, dass das Smartphone gegen ein Lesen der Daten von Dritten gesichert ist. Die Auswahl dieser Funktion navigiert Sie direkt in die Einstellungen des Android Smartphones.

EVVA empfiehlt das Aktivieren der Telefonverschlüsselung. Bitte beachten Sie dazu die Hinweise der Bedienungsanleitung Ihres Smartphones!

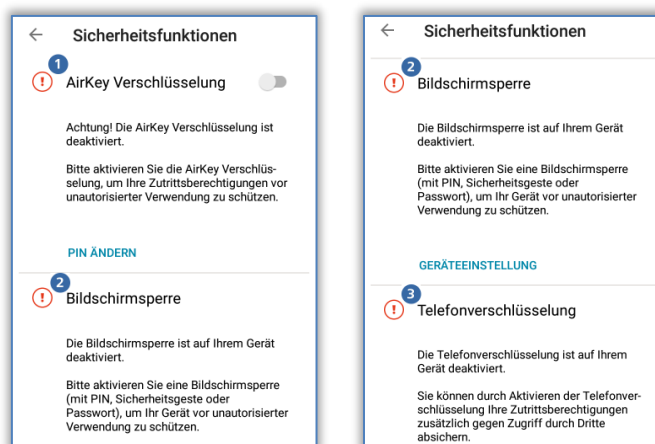


Abbildung 231: AirKey-App – Sicherheitsfunktionen

6.9.6.1 PIN aktivieren

Um die PIN zu aktivieren, führen Sie folgende Schritte aus:

- > Öffnen Sie das Menü innerhalb der AirKey-App und tippen Sie auf **Einstellungen** → **Sicherheitsfunktionen**.
- > Aktivieren Sie die Option "AirKey-Verschlüsselung".
- > Vergeben Sie eine PIN und tippen Sie auf **Bestätigen**.

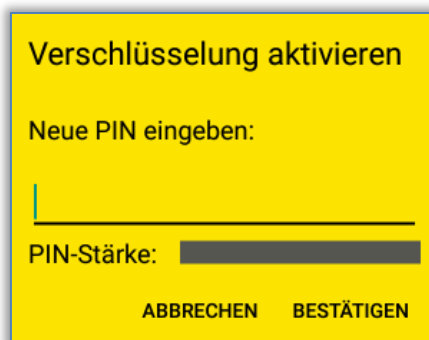


Abbildung 232: AirKey-App – PIN aktivieren

- > Schließen Sie den Vorgang mit erneuter Eingabe der PIN und dem Tippen auf **Bestätigen** ab.



EVVA empfiehlt die Vergabe einer PIN. Verwenden Sie eine möglichst lange PIN und achten Sie darauf, dass nur Sie in Kenntnis über die PIN sind. Schon während der Eingabe der PIN wird die Stärke des Passwortes anhand des Balkens im Ampelsystem (rot / orange / grün) überprüft.



Die PIN wird erst beim Sperrvorgang von Schließkomponenten abgefragt. Innerhalb der App erfolgt keine Bestätigung, dass die PIN richtig eingegeben wurde. Die PIN kann auch schon im Vorhinein festgelegt und gespeichert werden (siehe [PIN eingeben](#)).

6.9.6.2 PIN ändern

Um eine festgelegte PIN nachträglich zu ändern, führen Sie folgende Schritte aus:

- > Öffnen Sie das Menü innerhalb der AirKey-App und tippen Sie auf **Einstellungen** → **Sicherheitsfunktionen**.
- > Tippen Sie auf **PIN ändern**.
- > Tragen Sie die alte PIN ein, wählen Sie eine neue PIN, wiederholen Sie diese und tippen Sie auf **Bestätigen**.

Abbildung 233: AirKey-App – PIN ändern



Verwenden Sie eine möglichst lange PIN und achten Sie darauf, dass nur Sie in Kenntnis über die PIN sind. Schon während der Eingabe der PIN wird die Stärke des Passwortes anhand des Balkens im Ampelsystem (**rot** / **orange** / **grün**) überprüft.

6.9.6.3 PIN deaktivieren

Es gibt zwei Möglichkeiten, die PIN zu deaktivieren. Wenn die PIN noch bekannt ist, kann diese direkt über die Sicherheitsfunktionen des Smartphones deaktiviert werden. Ist die PIN nicht mehr bekannt, so kann die PIN über die AirKey-Onlineverwaltung durch einen Administrator zurückgesetzt werden.

Wenn die PIN bekannt ist, gehen Sie wie folgt vor:

- > Öffnen Sie das Menü innerhalb der AirKey-App und tippen Sie auf **Einstellungen** → **Sicherheitsfunktionen**.
- > Deaktivieren Sie die Option "AirKey-Verschlüsselung".
- > Tragen Sie die aktuelle PIN ein und tippen Sie auf **Bestätigen**.

Abbildung 234: AirKey-App – Verschlüsselung deaktivieren

Wenn die PIN nicht mehr bekannt ist, kann die PIN wie folgt über die AirKey-Onlineverwaltung deaktiviert werden:

- > Melden Sie sich als Administrator in Ihrer Schließanlage an.
- > Klicken Sie auf der Startseite **Home** auf die Kachel **Smartphones**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das Smartphone, bei dem die PIN deaktiviert werden soll.
- > Wählen Sie den Reiter "Details", um diese zu bearbeiten.

- > Klicken Sie auf den Link **PIN-Code-Sperre deaktivieren**  im Block "Einstellungen".

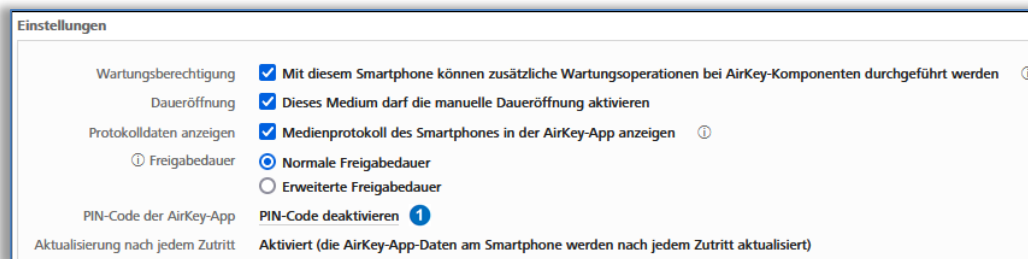


Abbildung 235: AirKey-Onlineverwaltung – PIN-Code deaktivieren

- > Bestätigen Sie die Sicherheitsfrage mit dem Button **PIN-Code deaktivieren**.



Abbildung 236: AirKey-Onlineverwaltung – Dialog "PIN-Code deaktivieren"



Die PIN kann jederzeit wieder aktiviert werden.

6.9.7 Benachrichtigungen

Unter dem Menüpunkt **Einstellungen** → **Benachrichtigungen** hat man die Möglichkeit, Push-Benachrichtigungen (Hinweise auf dem Sperr- oder Startbildschirm des Smartphones) zu Komponenten in Reichweite, Wartungsaufgaben und Berechtigungen bzw. deren Änderungen zu aktivieren. Wenn das Smartphone in mehreren AirKey-Schließanlagen registriert und mit der Wartungsberechtigung ausgestattet ist, dann werden diese Schließanlagen auch angezeigt und können ausgewählt werden.

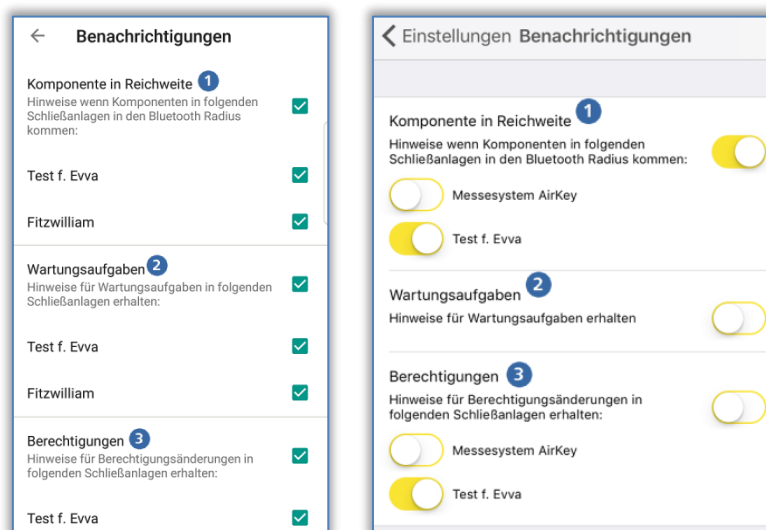


Abbildung 237: AirKey-App – Einstellungen – Benachrichtigungen (Android / iPhone)

Benachrichtigungen für **Komponenten in Reichweite** ①

Wenn diese Einstellung aktiviert ist, erhalten Sie entsprechende Push-Benachrichtigungen auf dem Sperr- oder Startbildschirm Ihres Smartphones, sobald sich Ihr Smartphone in der Reichweite von Bluetooth-Schließkomponenten befindet. Aus diesen Nachrichten heraus können Sie die entsprechende Tür aufsperrern, ohne die AirKey-App manuell öffnen zu müssen (Details in Kapitel [Sperrern aus Benachrichtigungen](#)).



Diese Einstellung wird nur von Smartphones mit Bluetooth 4.0 (Bluetooth Low Energy) angezeigt.

Benachrichtigungen für **Wartungsaufgaben** ②

Diese Einstellung wird nur von Smartphones mit Wartungsberechtigung angezeigt.

Ist diese Einstellung aktiv, wird im Hauptmenü der AirKey-App zusätzlich der Menüpunkt **Wartungsaufgaben** angezeigt. Auf der entsprechenden Seite werden Schließkomponenten und ihre [Wartungsaufgaben](#), die in der AirKey-Onlineverwaltung erstellt wurden, aufgelistet.

Wenn das Smartphone in mehreren Schließanlagen registriert ist, werden nur die Schließkomponenten der Schließanlagen, für die das Smartphone die Wartungsberechtigung besitzt, aufgelistet. Sobald eine neue Wartungsaufgabe in der AirKey-Onlineverwaltung erstellt wird, erhalten Sie auf Ihrem Smartphone eine entsprechende Push-Benachrichtigung.

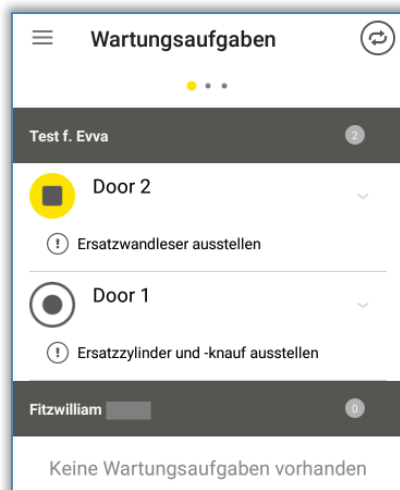


Abbildung 238: Wartungsaufgaben

Benachrichtigungen für **Berechtigungen** ⓘ

Diese Einstellung wird immer angezeigt.

Wenn diese Einstellung aktiviert ist und eine Berechtigung Ihres Smartphones in der AirKey-Onlineverwaltung neu erstellt oder geändert wird, erhalten Sie einen Hinweis ⓘ für ca. 2 s am unteren Bildschirmrand der AirKey-App, wenn diese geöffnet ist.

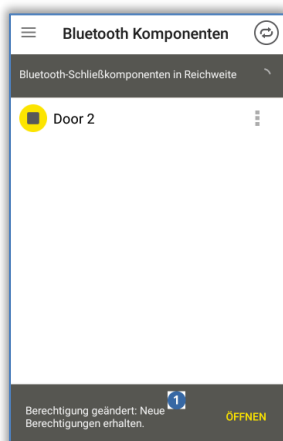


Abbildung 239: Benachrichtigung über eine Berechtigungsänderung

Wenn die AirKey-App nicht geöffnet ist, erhalten Sie eine entsprechende Push-Benachrichtigung auf dem Sperr- oder Startbildschirm Ihres Smartphones.

Unabhängig von der Einstellung für Benachrichtigungen für Berechtigungen erhalten Sie einen dauerhaften Eintrag auf der Seite "Berechtigungsprotokoll".

6.9.8 Schließanlage hinzufügen

Smartphones können in mehr als einer AirKey-Schließanlage registriert sein. Soll Ihr Smartphone in einer weiteren Schließanlage hinzugefügt werden, dann können Sie mit Hilfe der Funktion **Schließanlage hinzufügen** den Registrierungscode eingeben. Weitere Informationen dazu finden Sie im Kapitel [Smartphone in mehreren Anlagen verwenden](#).

Zusätzlich können Sie hier auch einen QR-Code für einen Smartphonetausch einscannen. Details zum Smartphonetausch finden Sie im Kapitel [Smartphonetausch](#).

6.9.9 Smartphone tauschen

Es besteht die Möglichkeit, die AirKey-Berechtigungen und -Einstellungen eines Smartphones auf ein neues Smartphone zu übertragen.

Starten Sie diesen Vorgang dem Befehl **Smartphone tauschen**. Weitere Informationen dazu finden Sie im Kapitel [Tausch als Smartphone-Besitzer starten](#).

6.9.10 Info

Innerhalb der AirKey-App gibt es die Möglichkeit, die Version der aktuell installierten AirKey-App, die Details zur Registrierung des Smartphones, die Medien-ID des Smartphones und die EVVA Allgemeinen Lizenzbedingungen aufzurufen.

- > Starten Sie die AirKey-App.
- > Tippen Sie im Menü auf **Einstellungen** → **Info**.

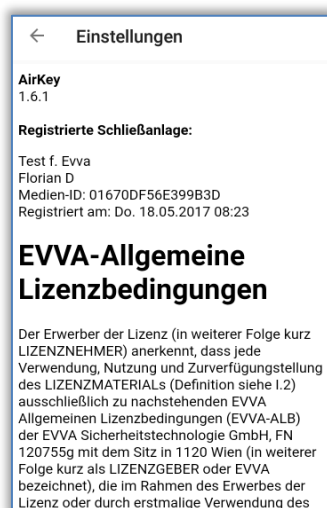


Abbildung 240: AirKey-App – Info

6.10 Smartphone aktualisieren

Um die Daten der AirKey-Schließanlage am Smartphone aktuell zu halten, können Sie das Smartphone jederzeit mit der AirKey-Onlineverwaltung manuell aktualisieren.

Wischen Sie dafür bei einem Android-Smartphone auf der Seite "Berechtigungen" der AirKey-App von oben nach unten über den Bildschirm. Es erscheint das Aktualisierungssymbol (drehender Kreis).

Bei einem iPhone ziehen Sie die Seite "Berechtigungen" bis an den unteren Rand. Es erscheint das Aktualisierungssymbol (drehende Strahlen).

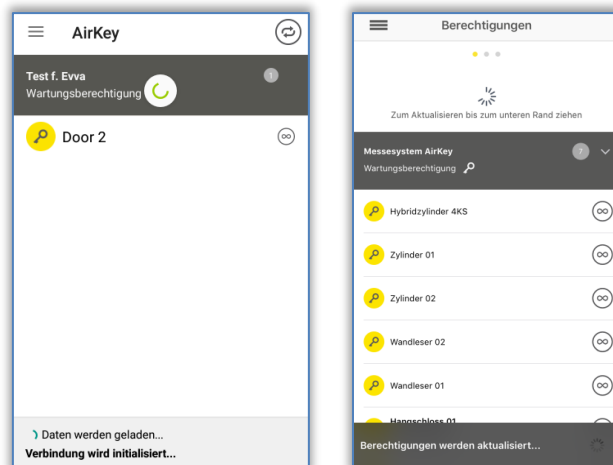


Abbildung 241: Android-Smartphone bzw. iPhone aktualisieren



AirKey nutzt bei Änderungen der Daten eines Smartphones in der AirKey-Onlineverwaltung Push-Benachrichtigungen, um das Smartphone automatisch zu aktualisieren. Es kann keine Zustellgarantie für Push-Benachrichtigungen gegeben werden. Kontrollieren Sie deshalb, ob eine Zustellung erfolgt ist, und aktualisieren Sie Ihr Smartphone gegebenenfalls manuell.



Das Smartphone wird automatisch aktualisiert, sobald Sie die AirKey-App starten bzw. wird alle 12 Stunden versucht, das Smartphone automatisch zu aktualisieren, wenn die AirKey-App bereits gestartet ist.

Im unteren Abschnitt der AirKey-App wird für den Zeitpunkt der Aktualisierung eine Statusinformation zur Aktualisierung eingeblendet. Sofern diese Informationen nicht mehr angezeigt werden, ist die Aktualisierung abgeschlossen.

Optional dazu kann die Aktualisierung auch nach jedem Zutritt erfolgen. Dazu muss allerdings die Option "Aktualisierung nach jedem Zutritt" in der jeweiligen AirKey-Schließanlage aktiviert sein. Die Aktivierung und die Details dieser Funktion sind im Kapitel [Allgemein](#) beschrieben.

6.11 Mit Komponente verbinden

Sie können mit Ihrem Smartphone jedes Zutrittsmedium (ausgenommen Smartphones) und jede AirKey-Schließkomponente, unabhängig von der Zugehörigkeit zu dessen Schließanlage aktualisieren.

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden 1**.
- > Verbindung über **Bluetooth** (bei Android-Smartphones) herstellen: Tippen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen, auf das Kontextmenü (:)) und wählen Sie dann **Verbinden 2**.
- > Verbindung über **Bluetooth** (bei iPhones) herstellen: Wischen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen, auf der Komponentenbezeichnung nach links und wählen Sie dann **Verbinden 3**.

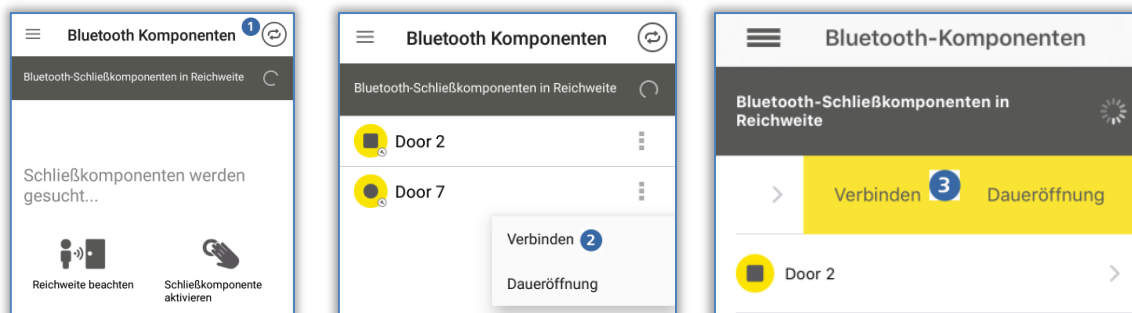


Abbildung 242: AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone)

- > Folgen Sie den Anweisungen und halten Sie das NFC-Smartphone an das Medium bzw. die Schließkomponente; oder halten Sie das Bluetooth-Smartphone in Reichweite der Schließkomponente.

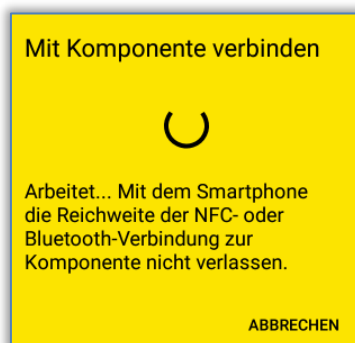


Abbildung 243: AirKey-App – Daten aktualisieren

Die Daten werden aktualisiert. Während der Übertragung darf das Smartphone von der zu synchronisierenden Komponente nicht entfernt werden. Wenn der Vorgang abgeschlossen ist, erhalten Sie eine entsprechende Meldung.



Deaktivieren Sie den Hands-free-Modus, bevor Sie sich mit einer Bluetooth-Schließkomponente verbinden. Andernfalls kann es zu Verbindungsabbrüchen kommen.




Bluetooth-Schließkomponenten können auch automatisch nach jedem Sperrvorgang via Bluetooth aktualisiert werden. Nähere Informationen zur Funktion "Aktualisierung nach jedem Sperrvorgang" finden Sie im Kapitel [Vorgabewerte \(für alle neu hinzugefügten Schließkomponenten\)](#).



Aktualisieren Sie Ihre AirKey-Komponenten regelmäßig. Nur so bleibt Ihre AirKey-Anlage sicher und am aktuellen Stand. Weitere Informationen zum Aktualisieren von AirKey-Komponenten finden Sie im Kapitel [Betrieb & Wartung des AirKey-Systems](#).

6.12 Spezialberechtigung "Wartungsberechtigung"

Wenn bei Ihrem Smartphone die Spezialberechtigung "Wartungsberechtigung" in der AirKey-Onlineverwaltung aktiviert wurde, können Sie zusätzliche Wartungsoperationen bei AirKey-Komponenten durchführen. Die Wartungsberechtigung berechtigt Sie, AirKey-Schließkomponenten im Auslieferungszustand zu sperren, Schließkomponenten und Zutrittsmedien (ausgenommen Smartphones) in Ihrer AirKey-Schließanlage hinzuzufügen und zu entfernen und die Firmware von Schließkomponenten bzw. die Keyring-Version von Zutrittsmedien wie Karten, Schlüsselanhängern, Kombischlüsseln und Armbändern zu aktualisieren.

Sie erkennen die Wartungsberechtigung innerhalb der AirKey-App auf der Seite "Berechtigungen" als Eintrag "Wartungsberechtigung"  im grauen Balken.

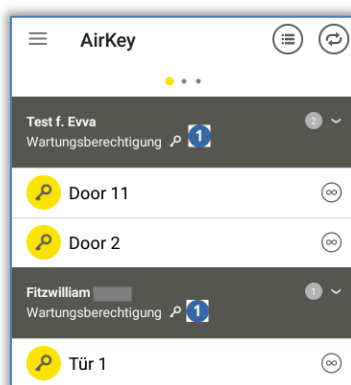



Abbildung 244: Wartungsberechtigung

Die Wartungsberechtigung wird in den Details des entsprechenden Smartphones innerhalb der AirKey-Onlineverwaltung aktiviert. Nähere Details zum Bearbeiten eines Mediums finden Sie im Kapitel [Medium bearbeiten](#).

Zusätzlich wurde im Hauptmenü der AirKey-App auch der Menüpunkt **Wartungsaufgaben**  freigeschaltet.

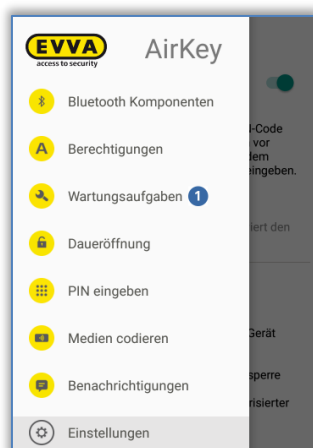


Abbildung 245: Menüpunkt "Wartungsaufgaben" im Hauptmenü

- > Tippen Sie darauf, um eine Liste mit Wartungsaufgaben für Schließkomponenten Ihrer Schließanlage zu erhalten. Wenn Sie auf den Namen einer Schließkomponente

tippen, wird die Liste der offenen Wartungsaufgaben für diese Schließkomponente angezeigt.

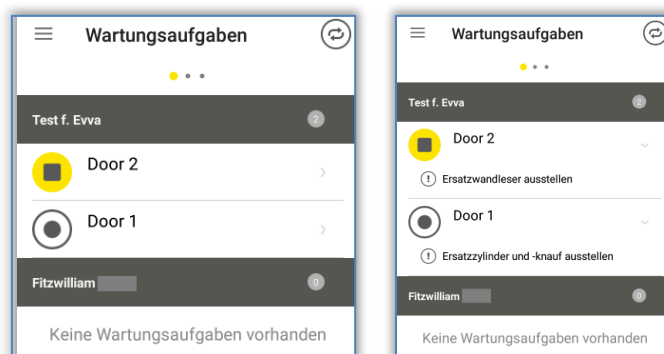





Abbildung 246: Wartungsaufgaben



Prüfen Sie als Wartungstechniker regelmäßig die Wartungsaufgaben, um Schließkomponenten, die aktualisiert werden müssen, schnell zu aktualisieren.

Wenn Sie mit einem Smartphone mit Wartungsberechtigung in die Reichweite einer Bluetooth-Schließkomponente (Zylinder  oder Wandler ) kommen, wird das Symbol dieser Schließkomponente gelb hinterlegt (z.B.  für Zylinder).

Wenn Sie auf das gelbe Symbol tippen, wird eine Verbindung zur Schließkomponente hergestellt und die Aktualisierung der Komponente durchgeführt. Danach werden die Komponentendetails angezeigt. Ein ausstehendes Firmware-Update wird in den Komponentendetails angezeigt und kann von hier aus gestartet werden.

Zusätzlich erhalten Sie als Wartungstechniker beim Aktualisieren von Schließkomponenten eine Übersicht zu den Details der Schließkomponente, um direkt den Status der Schließkomponente und Ereignisse des Zylinders in Form des Protokolls zu überprüfen.

- > Aktualisieren Sie eine Schließkomponente, um die Komponentendetails zu erhalten. Wenn vorhanden, sehen Sie hier auch den Standort der Schließkomponente als GPS-Koordinaten oder die in der AirKey-Onlineverwaltung manuell hinterlegte Adresse. Wenn Sie auf das gelbe Standortssymbol tippen, erfolgt eine automatische Weiterleitung zu dem Kartenanbieter, der auf Ihrem Smartphone als Standard eingestellt ist.

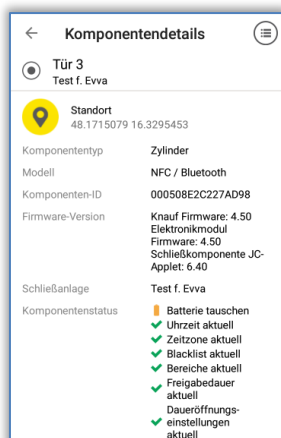


Abbildung 247: Anzeige der Schließkomponentendetails



Aktualisieren Sie Ihre AirKey-Komponenten regelmäßig. Nur so bleibt Ihre AirKey-Anlage sicher und am aktuellen Stand. Weitere Informationen zum Aktualisieren von AirKey-Komponenten finden Sie im Kapitel [Betrieb & Wartung des AirKey-Systems](#).

Die Wartungsberechtigung gilt nur für die Schließanlagen, bei denen diese aktiviert wurde, kann jedoch bei mehreren Schließanlagen gleichzeitig aktiviert werden.



Der Hands-free-Modus am Smartphone muss deaktiviert werden, um Wartungsaufgaben oder Aktualisierungen der Schließkomponenten durchführen zu können.

6.13 Hinzufügen einer AirKey-Komponente

Damit Sie eine Schließkomponente oder ein Zutrittsmedium (ausgenommen Smartphones) mit Ihrem Smartphone zu Ihrer AirKey-Schließanlage hinzufügen können, muss die Wartungsberechtigung für die Schließanlage aktiviert sein und die AirKey-Komponente muss sich im Auslieferungszustand befinden.

6.13.1 [Medien hinzufügen](#): Siehe Kapitel 4.12

6.13.2 [Schließkomponente hinzufügen](#): Siehe Kapitel 4.11

6.14 Entfernen einer AirKey-Komponente

Als Voraussetzung zum Entfernen muss die Schließkomponente oder das Medium (ausgenommen Smartphones) zuerst in der AirKey-Onlineverwaltung entfernt worden sein (siehe [Schließkomponente entfernen](#) und [Medium entfernen](#)) und das Smartphone muss die Wartungsberechtigung aktiviert haben.

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden**

- > Verbindung über **Bluetooth** (bei Android-Smartphones) herstellen: Tippen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen auf das Kontextmenü (:) und wählen Sie dann **Verbinden** ②.
- > Verbindung über **Bluetooth** (bei iPhones) herstellen: Wischen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen auf der Komponentenbezeichnung nach links und wählen Sie dann **Verbinden** ③.

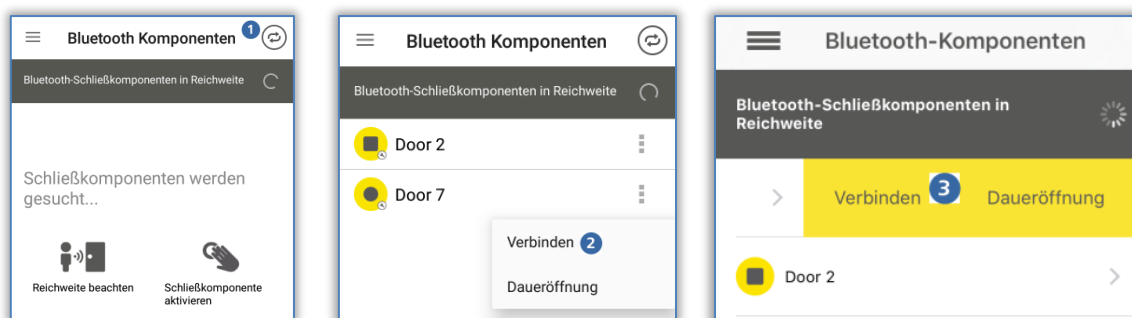


Abbildung 248: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone)

- > Folgen Sie den Anweisungen und halten Sie das NFC-Smartphone an das Medium bzw. die Schließkomponente; oder halten Sie das Bluetooth-Smartphone in Reichweite der Schließkomponente.

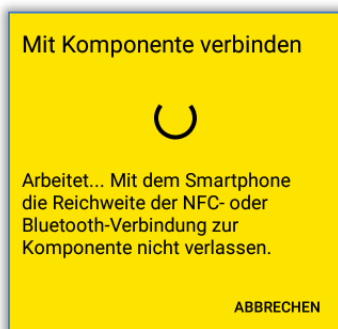


Abbildung 249: AirKey-App – Mit Komponente verbinden

Halten Sie das NFC-Smartphone an die AirKey-Komponente / das Medium, die / das bereits in der AirKey-Onlineverwaltung entfernt wurde bzw. halten Sie das Bluetooth-Smartphone in Reichweite der zu entfernenden Komponente bzw. direkt an das zu entfernende Medium und folgen Sie den Anweisungen.



Abbildung 250: AirKey-Komponente entfernen

Nach erfolgreicher Aktualisierung befinden sich die Schließkomponenten und Medien wieder im Auslieferungszustand.

Wenn ein Zutrittsmedium mit einem iPhone aus der AirKey-Schließanlage entfernt werden soll, so erfolgt das analog zum Hinzufügen über **Medien codieren**.

- > Aus der Liste der angezeigten Bluetooth-Schließkomponenten wählen Sie jene aus, über die Sie das Medium aktualisieren möchten.

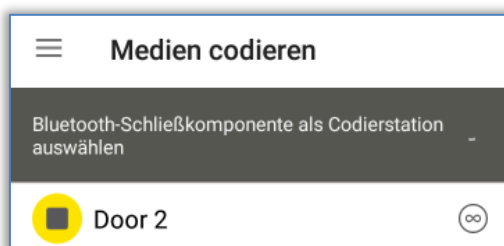


Abbildung 251: Medien codieren – Auswahlliste Bluetooth – Schließkomponenten

- > Halten Sie das Medium, das Sie aktualisieren möchten, an die AirKey-Schließkomponente.
- > Sie erhalten einen Hinweis, dass die AirKey-Schließkomponente bereit ist.

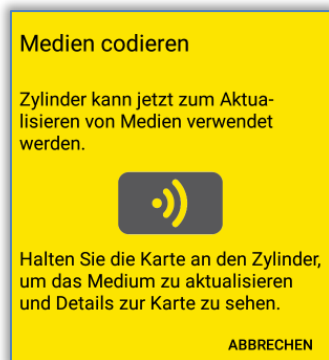


Abbildung 252: Medium mit iPhone entfernen

- > Halten Sie das Zutrittsmedium an die AirKey-Schließkomponente und tippen Sie auf **Entfernen**.

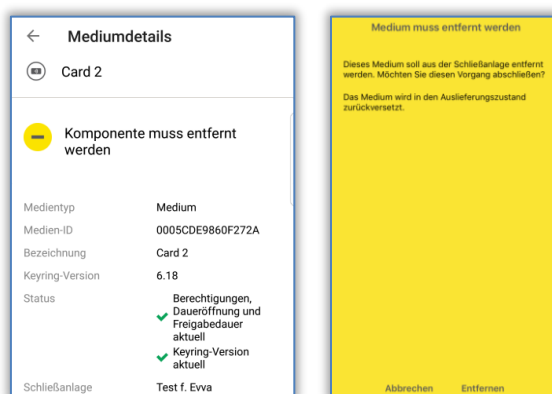


Abbildung 253: Medium entfernen

- > Sie erhalten eine Erfolgsmeldung, dass das Zutrittsmedium erfolgreich aus der AirKey-Schließanlage entfernt wurde.



Entfernen Sie das Smartphone während dieses Vorgangs auf keinen Fall von der Schließkomponente oder dem Medium.



Der Vorgang zum Entfernen von Schließkomponenten und Medien (ausgenommen Smartphones) ist identisch.




NFC-Komponenten können nicht mit dem iPhone aus der Schließanlage entfernt werden. Dazu ist eine optionale Codierstation oder ein NFC-fähiges Android-Smartphone notwendig.

6.15 Protokolldaten in der AirKey-App

Für Smartphones kann die Berechtigung zur Anzeige von Protokolldaten über die AirKey-Onlineverwaltung freigeschaltet werden. Die Anzeige der Protokolldaten ist unabhängig von der Wartungsberechtigung und kann für jede Person einzeln aktiviert werden.

Die Anzeige der Protokolldaten wird innerhalb der AirKey-Onlineverwaltung in den Details des Smartphones aktiviert bzw. deaktiviert. Nähere Details zum Bearbeiten eines Mediums finden Sie im Kapitel [Medium bearbeiten](#).

Das Protokoll rufen Sie innerhalb der App wie folgt auf:

- > Starten Sie die AirKey-App.
- > Wählen Sie im Hauptmenü den Menüpunkt **Berechtigungen**.
- > Wählen Sie rechts oben das Protokoll-Symbol .

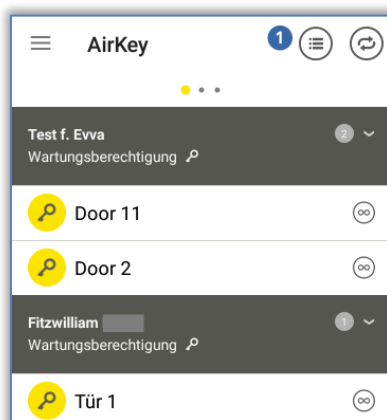


Abbildung 254: Das Protokoll-Symbol

- > Das Protokoll des Smartphones wird angezeigt.



Innerhalb des Protokolls der AirKey-App werden nur Protokolleinträge der Person angezeigt, der das Smartphone zugewiesen wurde.

6.16 Hands-free auf einen Blick

Für Bluetooth-Schließkomponenten gibt es den Hands-free-Modus. Dabei handelt es sich um eine Komfortfunktion, bei der die Schließkomponente in der App nicht mehr ausgewählt werden muss. Die Hands-free-Funktion ist nicht gleichzusetzen mit der Funktion "Sperrern mit Bluetooth", kann aber für zusätzlichen Komfort aktiviert werden.

Der Zylinder sendet nach Berührung ein Bluetooth-Signal aus. Beim Wandler funktioniert das automatisch, ohne Berührung. Empfängt eine AirKey-App in Sperrreichweite dieses Bluetooth-Signal, wird der Sperrvorgang gestartet. Die Sperrreichweite kann für Zylinder und Wandler in der App individuell eingestellt werden.

- > In der AirKey-App muss im Hauptmenü **Einstellungen** der Hands-free-Modus aktiviert werden.

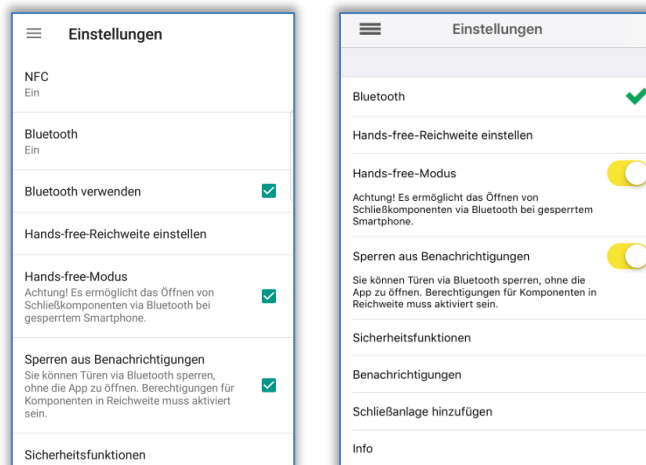


Abbildung 255: Einstellungen der AirKey-App



Bei Android-Smartphones wird durch die Aktivierung dieser Funktion ein Dienst gestartet. Dieser Dienst sucht auch bei beendeter AirKey-App dauerhaft nach Bluetooth-Schließkomponenten in Reichweite und führt zu einem erhöhten Akku-Verbrauch des Smartphones. Der Dienst wird beendet, sobald die Funktion wieder deaktiviert wird. Tippt man auf die Benachrichtigung des Dienstes, gelangt man direkt in die Einstellungen der AirKey-App.

- > Zusätzlich muss pro Schließkomponente oder Bereich in den Berechtigungsdetails im Menüpunkt **Berechtigungen** der Hands-free-Modus aktiviert werden. Beim ersten Aktivieren des Hands-free-Modus erscheint ein Dialog, in dem die Funktion automatisch für alle Schließkomponenten oder individuell nur für einzelne Schließkomponenten aktiviert werden kann.

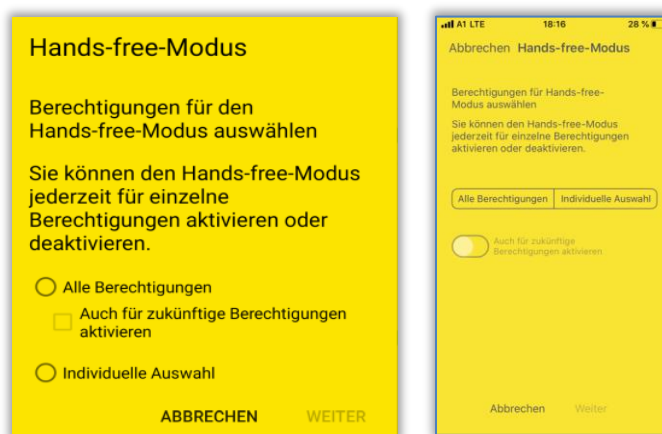


Abbildung 256: Berechtigungen für Hands-free-Modus



Aktivieren Sie **Auch für zukünftige Berechtigungen aktivieren**, um den Hands-free-Modus auch für jede weitere Berechtigung automatisch zu aktivieren.



Abhängig von der Einstellung **Zutritt aus Sperrbildschirm** in den Einstellungen der AirKey-Onlineverwaltung kann entweder direkt aus dem Sperr-

bildschirm gesperrt werden, oder es muss vorab der Sperrbildschirm aufgehoben werden. Weitere Details finden Sie im Kapitel [Allgemein](#).



Der Hands-free-Modus kann nur für Schließkomponenten verwendet werden, bei denen ein Administrator den Hands-free-Modus erlaubt hat. Weitere Details finden Sie im Kapitel [Schließkomponente bearbeiten](#).

Hands-free-Reichweite einstellen: siehe Kapitel 6.9.3

Was ist bei der Nutzung des Hands-free-Modus zu beachten?

Die Funktion bei gesperrtem Smartphone-Display ist abhängig

- > von der Einstellung "Zutritt aus Sperrbildschirm" in den Einstellungen der AirKey-Onlineverwaltung;
- > vom Hersteller, dem Betriebssystem, dem Alter, der Anzahl der installierten Apps, App-Optimierungen (Energiesparfunktion) des Smartphones;
- > von Störfaktoren wie der Gebäudeart (z.B. Stahlbetonbauweise) und dem Funkumfeld;
- > vom Aufbewahrungsort bzw. Trageort des Smartphones sowie der eingestellten Sperrreichweite für die Hands-free-Funktion;
- > ob sich das Smartphone gerade mit einem WLAN verbindet.

Infolge dieser Faktoren wird die Hands-free Funktion langsamer oder funktioniert eventuell gar nicht mehr. Um den Hands-free-Sperrvorgang zu beschleunigen, muss je nach Betriebssystem (z.B. iOS) das Smartphone entsperrt und die AirKey-App gestartet werden. In diesem Fall erspart man sich die Auswahl der zu entsperrenden Komponente innerhalb der App.

Um Fehlsperungen zu vermeiden, ist Folgendes zu beachten:

- > Nach jedem Sperrvorgang gibt es bei Wandlesern ein Time-Out von 2 Minuten. Das bedeutet, dass ein Wandleser erst dann wieder mit Hands-free gesperrt werden kann, wenn sich dieses Smartphone für 2 Minuten nicht in Empfangsreichweite des Wandlers befunden hat. Das verhindert ungewollte Sperrvorgänge beim Verlassen der Sperrreichweite.
- > Idealerweise befindet sich nur jeweils eine Schließkomponente in Sperrreichweite eines Smartphones.
- > Um Funktionen wie z.B. "Medien codieren" oder "Aktualisierungen von Schließkomponenten" durchführen zu können, muss der Hands-free-Modus in der App deaktiviert werden.

7 Bedienung von AirKey-Schließkomponenten

7.1 Zutritt mit dem Smartphone

Um bei einer AirKey-Schließkomponente Zutritt zu erhalten, müssen folgende Voraussetzungen erfüllt sein:

- > NFC bzw. Bluetooth am Smartphone ist aktiviert.
- > Die AirKey-App ist installiert und registriert.
- > Eine gültige Berechtigung für das Smartphone wurde vergeben (Details finden Sie im Kapitel [Smartphone registrieren](#) und [Berechtigungen vergeben](#)).
- > Halten Sie das Smartphone bei Sperrvorgängen über NFC an die Schließkomponente. Die Position mit den besten Leseigenschaften ist abhängig vom Smartphone-Modell. Die Lesereichweite ist ebenfalls abhängig von der Type des Smartphones und reicht von Berührung bis einigen Millimetern Entfernung. Bei Sperrvorgängen über Bluetooth ist die Lesereichweite einerseits abhängig von der Type des Smartphones und andererseits von Ihren persönlichen Einstellungen in der AirKey-App am Smartphone für den Hands-free-Modus. Sie beträgt bis zu einige Meter.
- > Sofern die Eingabe einer PIN gefordert ist, geben Sie die richtige PIN ein, bevor Sie mit dem Smartphone über NFC bzw. Bluetooth sperren. (Details zur PIN finden Sie im Kapitel [Sicherheitsfunktionen](#)).
- > Achten Sie auf die optische Signalisierung der Schließkomponente. Entfernen Sie bei NFC das Smartphone nicht von der Schließkomponente bzw. bleiben Sie bei Bluetooth in Empfangsreichweite, bis die Schließkomponente grün signalisiert. (Die blaue Signalisierung deutet nur auf die Kommunikation zwischen Smartphone und Schließkomponente hin.)
- > Die Schließkomponente gibt für die eingestellte Freigabedauer frei und Sie erhalten Zutritt.



Mit den iPhone-Modellen XR, XS, XS Max und neuer können Sie auch Bluetooth-Schließkomponenten über NFC sperren. Halten Sie dazu das Smartphone an die Schließkomponente und tippen Sie auf die Hinweismeldung, dass ein NFC-Tag erkannt wurde. Daraufhin wird die AirKey-App geöffnet und ein Bluetooth-Sperrvorgang durchgeführt.



Abbildung 257: iOS-NFC-Tag



Prüfen Sie Ihre Berechtigung oder die PIN, wenn die Schließkomponente rot signalisiert.



Das Sperren von Schließkomponenten über NFC ist bei aktiver Displaysperre oder während eines Anrufs nicht möglich. Allerdings muss die AirKey-App nicht gestartet oder im Vordergrund sein, um Schließkomponenten sperren zu können. Das Sperren von Schließkomponenten über Bluetooth ist hingegen bei aktiver Displaysperre möglich. Es muss lediglich in den Einstellungen der AirKey-App die Option "Sperren aus Benachrichtigungen" aktiviert werden und in den Einstellungen der AirKey-Onlineverwaltung "Zutritt aus Sperrbildschirm" erlaubt sein.

7.2 Zutritt mit Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder

Um bei einer AirKey-Schließkomponente Zutritt zu erhalten, muss das Medium in der Schließanlage hinzugefügt sein und eine gültige Berechtigung aufweisen (Details finden Sie im Kapitel [Karten, Schlüsselanhänger, Kombischlüssel und Armbänder mit dem Smartphone hinzufügen](#) und [Berechtigungen vergeben](#)).

- > Halten Sie das Medium an die Schließkomponente. Die Lesereichweite ist abhängig von der Type des Mediums und beträgt in der Regel einige Millimeter.
- > Achten Sie auf die optische Signalisierung der Schließkomponente. Entfernen Sie das Medium nicht, bevor die Schließkomponente grün signalisiert. (Die blaue Signalisierung deutet nur auf die Kommunikation zwischen Medium und Schließkomponente hin.)



Prüfen Sie Ihre Berechtigung, wenn die Schließkomponente rot signalisiert.

- > Die Schließkomponente gibt für die eingestellte Freigabedauer frei und Sie erhalten Zutritt.



Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder können im nahen Umfeld von anderen Medien oder metallischen Gegenständen nur eingeschränkt oder gar nicht funktionieren. Das kann zum Beispiel Medien in einer Geldbörse oder an einem Schlüsselbund betreffen.



Die Identifikation mit einem Kombischlüssel an Schließkomponenten muss mit jener Seite erfolgen, auf der das RFID-Symbol ersichtlich ist.

8 Betrieb & Wartung des AirKey-Systems

8.1 Schließkomponenten aktualisieren

Sie können grundsätzlich jede AirKey-Schließkomponente, unabhängig von der Schließanlagenzugehörigkeit, aktualisieren, um Daten zwischen AirKey-Onlineverwaltung und AirKey-Schließkomponente auszutauschen.

Die Aktualisierung kann mittels Smartphone oder optional mittels Codierstation erfolgen. Die Aktualisierung mit dem Smartphone setzt lediglich die Installation der AirKey-App und die Registrierung in einer beliebigen AirKey-Schließanlage voraus.

Bei der Aktualisierung von Schließkomponenten werden folgende Aktionen durchgeführt:

- Uhrzeit wird neu gesetzt.
- Protokolleinträge und Batteriestatus werden ausgelesen.
- Wartungsaufgaben (Blacklist, Freigaben in anderen Schließanlagen etc.) werden aktualisiert.
- Komponentendetails werden ausgelesen.

Folgen Sie den Anweisungen, um eine AirKey-Schließkomponente mit dem Smartphone zu aktualisieren:

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden 1**.
- > Verbindung über **Bluetooth** (bei Android-Smartphones) herstellen: Tippen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen auf das Kontextmenü (:;) und wählen Sie dann **Verbinden 2**.
- > Verbindung über **Bluetooth** (bei iPhones) herstellen: Wischen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen, auf der Komponentenbezeichnung nach links und wählen Sie dann **Verbinden 3**.

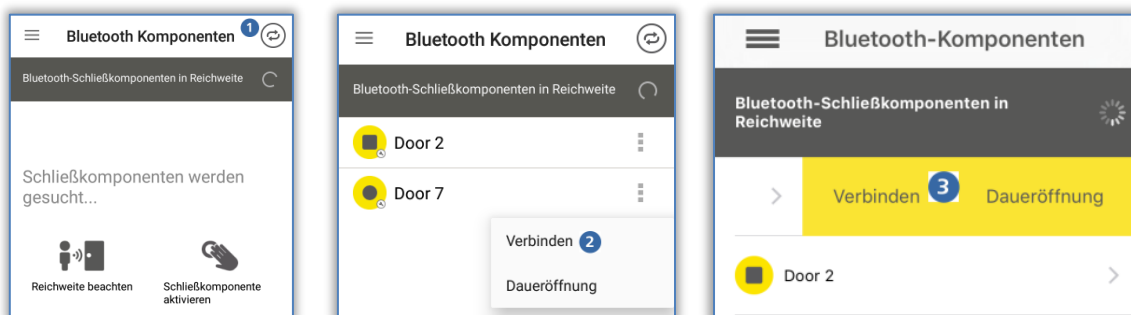


Abbildung 258: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone)

- > Folgen Sie den Anweisungen.

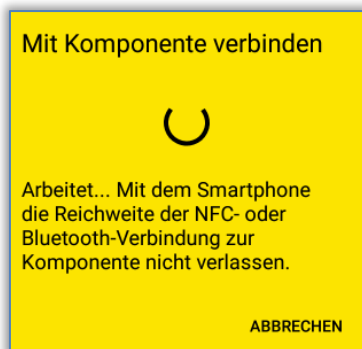


Abbildung 259: Daten aktualisieren

Die Daten werden aktualisiert. Während der Übertragung darf das NFC-Smartphone von der zu synchronisierenden Komponente nicht entfernt werden, bzw. darf das Bluetooth-Smartphone nicht aus der Reichweite der Schließkomponente entfernt werden. Wenn der Vorgang abgeschlossen ist, erhalten Sie eine entsprechende Meldung.



Je nachdem, ob am Smartphone die Wartungsberechtigung aktiviert ist und sich die Schließkomponente in der eigenen oder in einer fremden AirKey-Schließanlage befindet, können sich die angezeigten Informationen der Aktualisierungsmeldung unterscheiden.

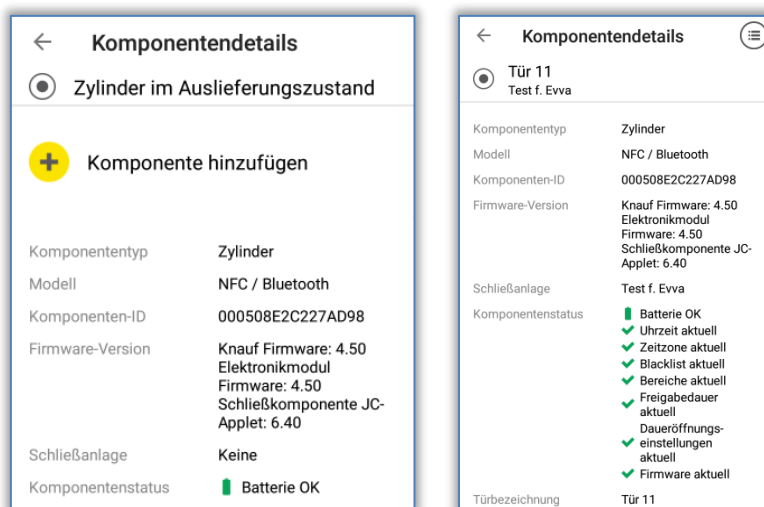


Abbildung 260: Aktualisierungsmeldungen



Deaktivieren Sie den Hands-free-Modus, bevor Sie sich mit einer Bluetooth-Schließkomponente verbinden. Andernfalls kann es zu Verbindungsabbrüchen kommen.



Bluetooth-Schließkomponenten können auch automatisch nach jedem Sperrvorgang via Bluetooth aktualisiert werden. Nähere Informationen zur Funktion "Aktualisierung nach jedem Sperrvorgang" finden Sie im Kapitel [Vorgabewerte \(für alle neu hinzugefügten Schließkomponenten\)](#).

Option

Schließkomponente mit Codierstation aktualisieren

Um die Schließkomponente mit der Codierstation zu aktualisieren, gehen Sie wie folgt vor:

- > Melden Sie sich in Ihrer AirKey-Schließanlage an und achten Sie darauf, dass die Codierstation angesteckt und in der AirKey-Onlineverwaltung ausgewählt wurde.
- > Legen Sie die Schließkomponente auf die Codierstation.

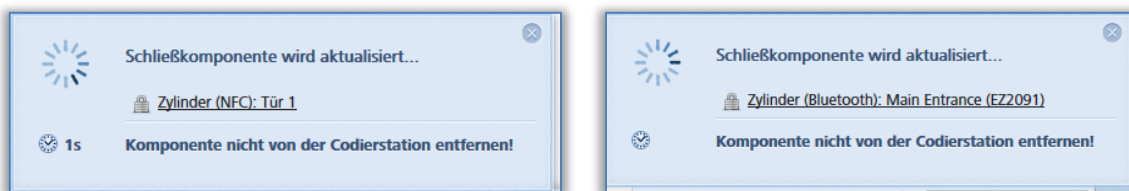


Abbildung 261: Schließkomponente mit Codierstation aktualisieren

- > Entfernen Sie die Schließkomponente erst von der Codierstation, wenn die Aktualisierung abgeschlossen und die Erfolgsmeldung angezeigt wird.



Je nachdem, ob sich die Schließkomponente in der eigenen oder in einer fremden AirKey-Schließanlage befindet, können sich die angezeigten Informationen der Erfolgsmeldung unterscheiden.

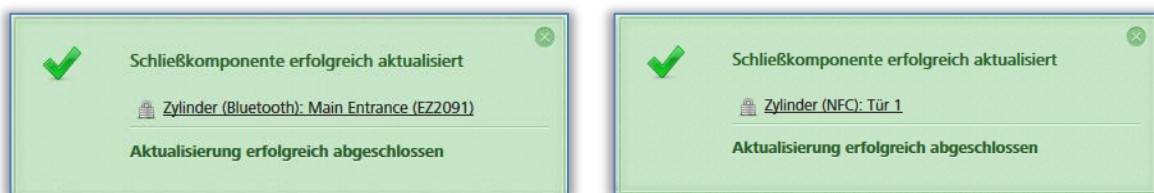


Abbildung 262: Schließkomponente mit Codierstation aktualisiert



Aktualisieren Sie Ihre AirKey-Schließkomponenten regelmäßig. Nur so bleibt Ihre AirKey-Schließanlage sicher und am aktuellen Stand.


8.2 [Smartphone aktualisieren](#): Siehe Kapitel 6.10

8.3 Medien aktualisieren

Sie können jedes AirKey-Medium, unabhängig von der Schließanlagenzugehörigkeit, aktualisieren. Die Aktualisierung kann mittels Android-Smartphone oder optionaler Codierstation erfolgen. Die Aktualisierung mit dem Smartphone setzt lediglich die Installation der AirKey-App und die Registrierung innerhalb einer AirKey-Schließanlage voraus.



Beim iPhone werden die Medien analog zu [Medien codieren](#) aktualisiert, indem man eine AirKey-Schließkomponente als Codierstation verwendet.

- > Tippen Sie bei einem Android-Smartphone auf das Symbol **Mit Komponente verbinden**  rechts oben in der AirKey-App.

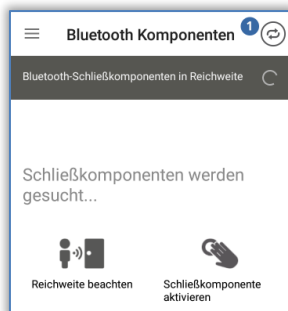


Abbildung 263: Symbol "Mit Komponente verbinden" (nur bei Android-Smartphones)

- > Folgen Sie den Anweisungen und halten Sie das Smartphone an das Medium.

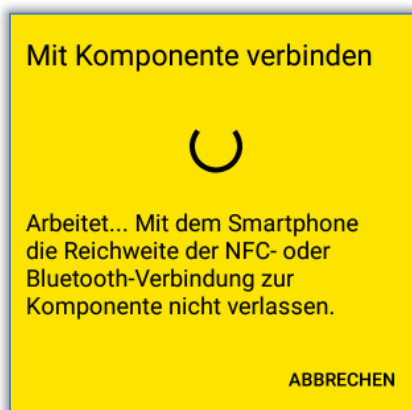


Abbildung 264: Daten aktualisieren

Die Daten werden aktualisiert. Während der Übertragung darf das Smartphone von dem zu synchronisierendem Objekt nicht entfernt werden. Wenn der Vorgang abgeschlossen ist, erhalten Sie eine entsprechende Meldung.



Zur Aktualisierung des Kombischlüssels mit Smartphones muss der Kombischlüssel mit jener Seite an die Stelle der NFC-Antenne des Smartphones direkt gehalten werden, auf der das RFID-Symbol ersichtlich ist.

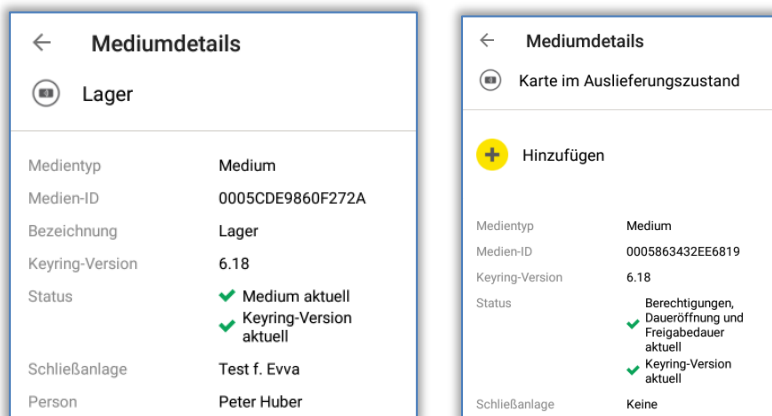


Abbildung 265: AirKey-App aktualisiert ein Medium

Option **Medium mit Codierstation aktualisieren**

Um Medien wie Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder mit der Codierstation zu aktualisieren, gehen Sie wie folgt vor:

- > Melden Sie sich in Ihrer AirKey-Schließanlage an und achten Sie darauf, dass die Codierstation angesteckt und in der AirKey-Onlineverwaltung ausgewählt wurde.
- > Legen Sie das Medium auf die Codierstation.

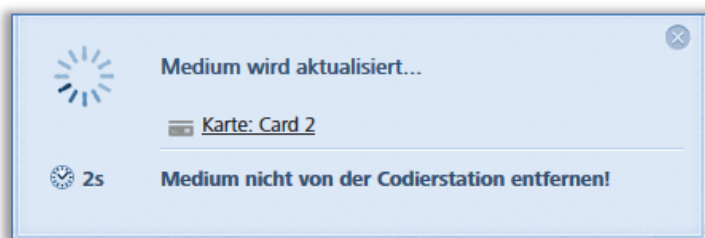


Abbildung 266: Medium mit Codierstation aktualisieren

- > Entfernen Sie das Medium erst von der Codierstation, wenn die Aktualisierung abgeschlossen und die Erfolgsmeldung angezeigt wird.



Je nachdem, ob sich die Medien in der eigenen oder in einer fremden AirKey-Schließanlage befinden, können sich die angezeigten Informationen der Erfolgsmeldung unterscheiden.

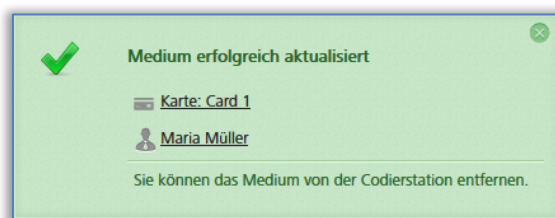


Abbildung 267: Eigenes bzw. fremdes Medium mit Codierstation aktualisiert



Aktualisieren Sie Ihre AirKey-Medien regelmäßig. Nur so bleibt Ihre AirKey-Schließanlage sicher und am aktuellen Stand.



Nur durch die regelmäßige Aktualisierung von Medien kann sichergestellt werden, dass alle Protokolleinträge von Medien in die AirKey-Onlineverwaltung übertragen werden.



Zur Aktualisierung des Kombischlüssels mittels Codierstation muss der Kombischlüssel mit jener Seite auf die Codierstation gelegt werden, auf der das RFID-Symbol ersichtlich ist. Die Aktualisierung ist nicht im gesamten Lesebereich der Codierstation möglich – bei der aktuellen Type (HID Omnikey 5421) wird der Kombischlüssel nur im oberen und unteren Drittel des Lesebereichs der Codierstation erkannt.

8.4 Firmware von Schließkomponenten aktualisieren

Wenn für Schließkomponenten eine neue Firmware verfügbar ist, wird diese Information in den Details der Schließkomponente, in den Wartungsaufgaben und beim Aktualisieren der Schließkomponente angezeigt.



Bitte überprüfen Sie vor einem Firmware-Update den Batteriestatus der Schließkomponente (Zylinder). Bei bestehender Warnung "Batterie leer" sollten zuerst alle Batterien gewechselt werden, um anschließend ein fehlerfreies Update zu gewährleisten.

Die aktuelle Firmware-Version der Schließkomponente wird in den Details der Schließkomponente angezeigt.

Das Firmware-Update von Schließkomponenten kann mittels Smartphone oder mittels optionaler Codierstation erfolgen.

Um Firmware-Updates mit dem Smartphone durchzuführen, muss die Spezialberechtigung "Wartungsberechtigung" am Smartphone aktiviert sein. Führen Sie Firmware-Updates mit dem Smartphone wie folgt aus:

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden 1**.
- > Verbindung über **Bluetooth** (bei Android-Smartphones) herstellen: Tippen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen auf das Kontextmenü (:>) und wählen Sie dann **Verbinden 2**.
- > Verbindung über **Bluetooth** (bei iPhones) herstellen: Wischen Sie bei der Schließkomponente, mit der Sie sich verbinden wollen auf der Komponentenbezeichnung nach links und wählen Sie dann **Verbinden 3**.

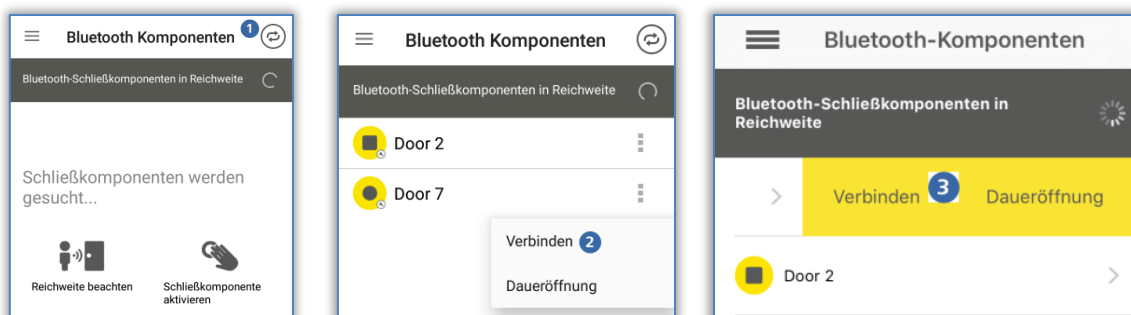


Abbildung 268: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone)

- > Folgen Sie den Anweisungen.

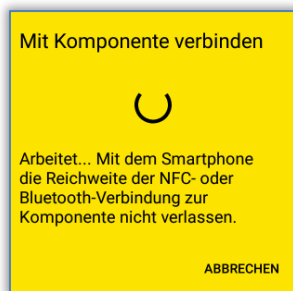


Abbildung 269: Mit Komponente verbinden – Firmware-Update

Die Daten werden aktualisiert. Während der Übertragung darf das NFC-Smartphone von der zu synchronisierenden Komponente nicht entfernt werden, bzw. darf das Bluetooth-Smartphone nicht aus der Reichweite der Schließkomponente entfernt werden. Wenn der Vorgang abgeschlossen ist, erhalten Sie eine entsprechende Meldung.

- > Die Schließkomponente wird aktualisiert und die Komponentendetails werden angezeigt. In den Komponentendetails ist ersichtlich, dass die Firmware der Komponente nicht aktuell ist.

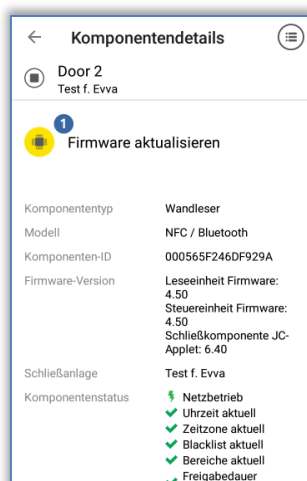



Abbildung 270: AirKey-App – Komponentendetails

- > Wählen Sie in diesem Bildschirm die Option **Firmware aktualisieren** .
- > Halten Sie das NFC-Smartphone an die Schließkomponente bzw. bleiben Sie mit dem Bluetooth-Smartphone in Reichweite.

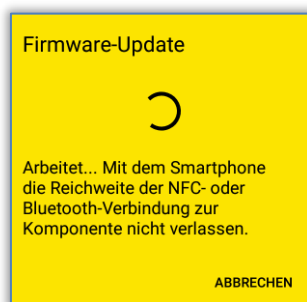


Abbildung 271: AirKey-App – Firmware aktualisieren



Das Aktualisieren der Firmware kann je nach Internetverbindung mehrere Minuten dauern. Halten Sie das NFC-Smartphone in dieser Zeit dauerhaft an die Schließkomponente bzw. bei einem Bluetooth-Smartphone in Reichweite der Schließkomponente.

Während der Übertragung darf das Smartphone von der zu aktualisierenden Komponente nicht entfernt werden. Die erfolgreiche Durchführung des ersten Updateschritts wird mit einer Erfolgsmeldung abgeschlossen.



Abbildung 272: AirKey-App – Updateschritt erfolgreich

- > Entfernen Sie das Smartphone von der Schließkomponente, bis die Schließkomponente blinkt und akustisch signalisiert.
- > Halten Sie das NFC-Smartphone an die Schließkomponente bzw. das Bluetooth-Smartphone in Reichweite der Schließkomponente und folgen Sie den Anweisungen.

Wenn die Aktualisierung der Firmware erfolgreich abgeschlossen ist, erscheint eine Erfolgsmeldung.



Abbildung 273: AirKey-App – Update erfolgreich

- > Bestätigen Sie die Erfolgsmeldung mit **Schließen**, um die Aktualisierung der Firmware abzuschließen.



Der Komponentenstatus der Schließkomponente wurde dadurch im gesamten System angepasst. Die Wartungsaufgabe wird nicht mehr angezeigt und die korrekte Firmware-Version ist in den Details der Schließkomponente zu erkennen.

Option

Firmware mit der Codierstation aktualisieren:

- > Legen Sie die Schließkomponente auf die Codierstation. Wenn die Codierstation eine Kommunikation mit der Schließkomponente startet, wird automatisch eine Aktualisierung begonnen.

Sie erhalten eine Erfolgsmeldung, wenn die Aktualisierung abgeschlossen ist.



Abbildung 274: Codierstation – Erfolgsmeldung bei der Aktualisierung einer Schließkomponente

Wenn für die Schließkomponente ein Firmware-Update vorhanden ist, wird ein entsprechender Link angezeigt **i**.

- > Klicken Sie auf **Firmware-Update durchführen**, um es zu starten.

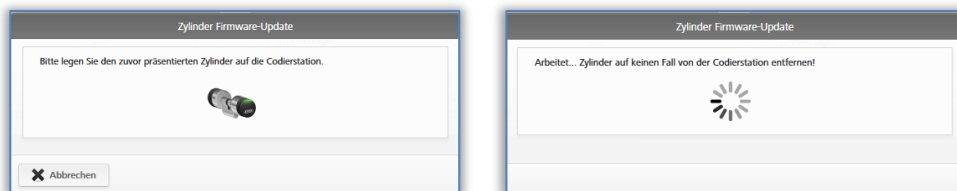


Abbildung 275: Codierstation – Firmware-Update für Zylinder



Das Firmware-Update kann, abhängig von der Internetverbindung, mehrere Minuten dauern. Entfernen Sie die Schließkomponente währenddessen nicht von der Codierstation.

Der erste Schritt des Firmware-Updates wird mit einer Erfolgsmeldung abgeschlossen.

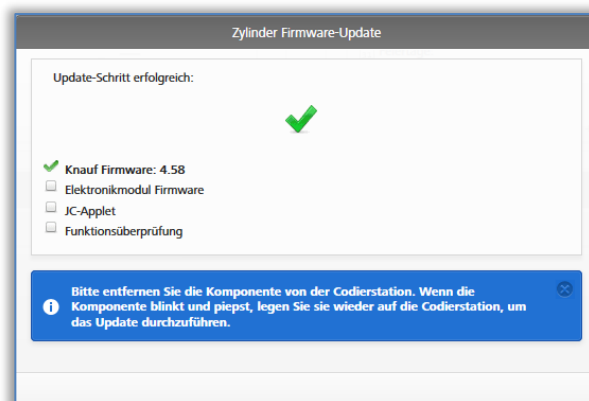


Abbildung 276: Codierstation – Updateschritt erfolgreich

- > Entfernen Sie die Schließkomponente von der Codierstation, bis die Schließkomponente einen Neustart mit akustischer und optischer Signalisierung durchführt.
- > Legen Sie die Schließkomponente wieder auf die Codierstation, um den Vorgang abzuschließen.

Wenn das Update abgeschlossen ist, erhalten Sie eine Erfolgsmeldung.

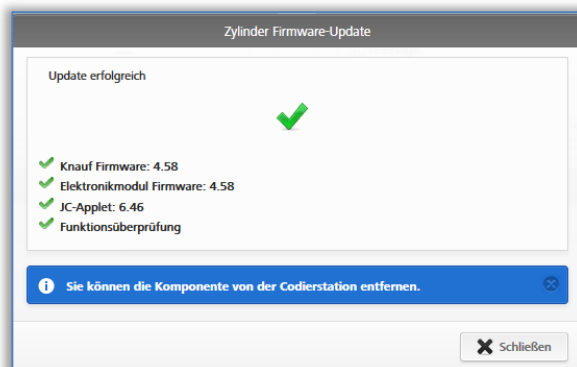


Abbildung 277: Codierstation – Firmware-Update erfolgreich

Die Schließkomponente wird nach dem Schließen der Erfolgsmeldung noch einmal aktualisiert.



Abbildung 278: Codierstation – Schließkomponente erfolgreich aktualisiert

- > Nach der Aktualisierung entfernen Sie die Schließkomponente von der Codierstation.



Der Komponentenstatus der Schließkomponente wurde dadurch im gesamten System angepasst. Die Wartungsaufgabe wird nicht mehr angezeigt und die korrekte Firmware-Version ist in den Details der Schließkomponente zu erkennen.



Für das Firmware-Update öffnen Sie die Tür und fixieren Sie sie so, dass sie sich nicht zufällig schließt. Überprüfen Sie anschließend die ordnungsgemäße Funktion der Schließkomponente, bevor Sie die Tür wieder schließen.



Beim Aktualisieren der Firmware von Schließkomponenten muss darauf geachtet werden, dass eine stabile Internetverbindung verfügbar ist und die Datenverbindung während des Firmware-Updates ohne Unterbrechung zur Verfügung steht. Dafür stehen, abhängig vom jeweiligen Smartphone und Betriebssystem, verschiedenste Einstellungen zur Verfügung (z.B. automatischer Netzwechsel zwischen mobilen Daten und WLAN erlauben).



EVVA empfiehlt, die Firmware von Schließkomponenten immer auf dem aktuellen Stand zu halten.

8.5 Keyring-Version von Medien aktualisieren

Im AirKey-System ist "Keyring" der Name eines Softwareprogramms, das alle AirKey-relevanten Daten verwaltet, die auf passiven Zutrittsmedien wie Karten, Schlüsselanhänger, Kombischlüssel und Armbänder gespeichert sind. Wenn für solche Medien eine neue Keyring-Version verfügbar ist, wird das in den Details der Medien, in den Wartungsaufgaben, auf der Startseite **Home** und beim Aktualisieren von Medien angezeigt.



Die aktuelle Keyring-Version des Mediums wird in den Details des Mediums angezeigt.

Das Keyring-Update von Medien kann mittels Smartphone oder mittels optionaler Codierstation erfolgen. Um Keyring-Updates mit dem Smartphone durchzuführen, muss die Spezialberechtigung "Wartungsberechtigung" am Smartphone aktiviert sein. Führen Sie Keyring-Updates mit dem Smartphone wie folgt aus:

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen:
Tippen Sie auf das Symbol **Mit Komponente verbinden** .
- > Verbindung über **Bluetooth** (bei Android-Smartphones und iPhones): Wählen Sie im Hauptmenü der AirKey-App den Menüpunkt **Medien codieren** – siehe auch [Medien codieren](#).

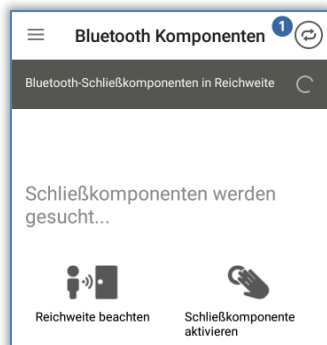


Abbildung 279: AirKey-App – Mit Komponente verbinden

- > Halten Sie das NFC-Smartphone an das Medium.
- > Das Medium wird aktualisiert. Es wird angezeigt, dass eine neue Keyring-Version verfügbar ist.

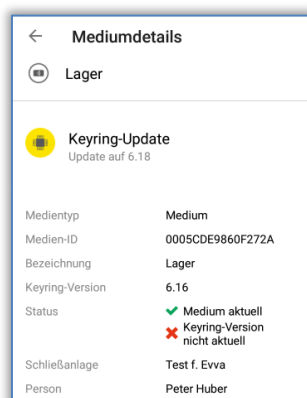


Abbildung 280: AirKey-App – Mediumdetails

- > Wählen Sie die Option **Keyring aktualisieren**.
- > Halten Sie das Smartphone an das Medium und folgen Sie den Anweisungen.

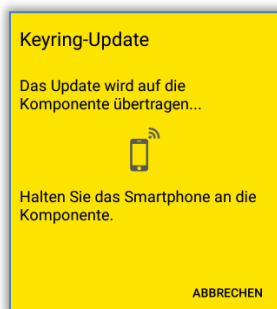


Abbildung 281: AirKey-App – Keyring aktualisieren



Das Aktualisieren der Keyring-Version kann je nach Internetverbindung mehrere Minuten dauern. Halten Sie das Smartphone in dieser Zeit dauerhaft an das Medium.

Während der Übertragung darf das Smartphone von dem zu aktualisierenden Medium nicht entfernt werden. Die erfolgreiche Durchführung des Keyring-Updates wird mit einer Erfolgsmeldung abgeschlossen.

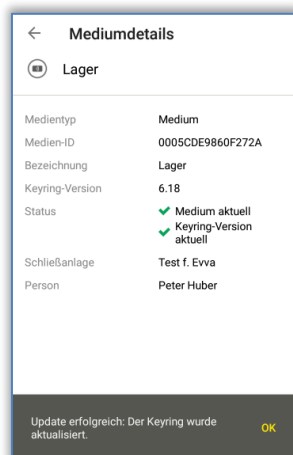


Abbildung 282: AirKey-App – Keyring-Update erfolgreich



Der Status des Mediums wurde dadurch im gesamten System angepasst. Die richtige Keyring-Version wird in den Mediendetails angezeigt.

Zur Aktualisierung des Kombischlüssels mit Smartphones muss der Kombischlüssel mit jener Seite an das Smartphone angehalten werden, auf der das RFID-Symbol ersichtlich ist.

Option

Keyring-Version mit Codierstation aktualisieren:

- > Legen Sie das Medium auf die Codierstation. Wenn die Codierstation das Medium erkennt, wird eine Kommunikation mit dem Medium gestartet.

Sie erhalten eine Erfolgsmeldung, wenn die Aktualisierung abgeschlossen ist.

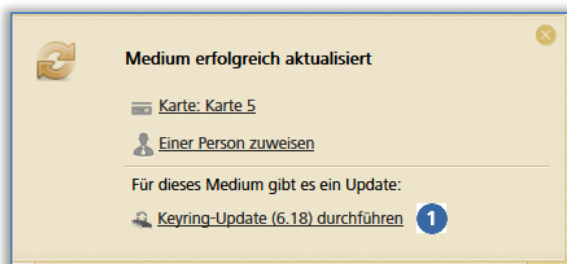


Abbildung 283: Codierstation – Keyring-Update verfügbar

Wenn für das Medium ein Keyring-Update vorhanden ist, wird ein entsprechender Link angezeigt 1.

- > Klicken Sie auf **Keyring-Update (x.x) durchführen**, um das Update zu starten.

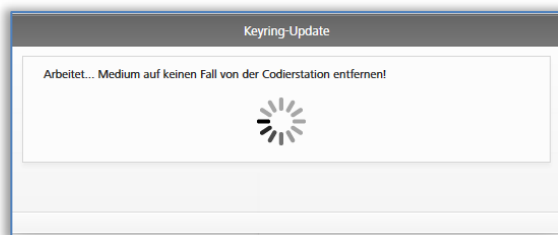


Abbildung 284: Codierstation – Keyring-Update



Das Aktualisieren der Keyring-Version kann abhängig von der Internetverbindung mehrere Minuten dauern. Entfernen Sie das Medium währenddessen nicht von der Codierstation.

Während des Keyring-Updates darf das Medium nicht von der Codierstation entfernt werden. Die Aktualisierung der Keyring-Version wird mit einer Erfolgsmeldung abgeschlossen.

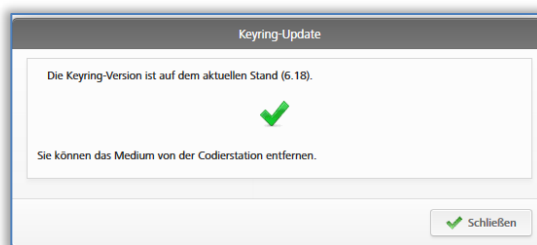


Abbildung 285: Codierstation – Keyring-Update erfolgreich

Das Keyring-Update ist damit erfolgreich abgeschlossen. Das Medium wird nach dem Schließen der Erfolgsmeldung noch einmal aktualisiert.

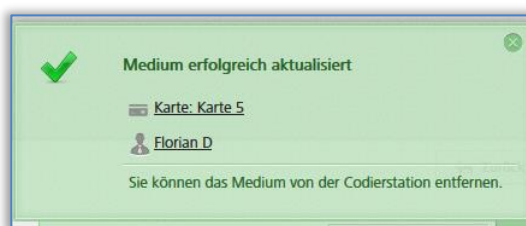


Abbildung 286: Codierstation – Medium erfolgreich aktualisiert

- > Nach der Aktualisierung entfernen Sie das Medium von der Codierstation.



Zur Aktualisierung des Kombischlüssels mittels Codierstation muss der Kombischlüssel mit jener Seite auf die Codierstation gelegt werden, auf der das RFID-Symbol ersichtlich ist. Die Aktualisierung ist nicht im gesamten Lesebereich der Codierstation möglich – bei der aktuellen Type (HID Omnikey 5421) wird der Kombischlüssel nur im oberen und unteren Drittel des Lesebereichs der Codierstation erkannt.

Der Status des Mediums wurde dadurch im gesamten System angepasst. Die richtige Keyring-Version wird in den Mediendetails angezeigt.



Beim Aktualisieren der Keyring-Version von Medien muss darauf geachtet werden, dass eine stabile Internetverbindung besteht und die Datenverbindung während des Keyring-Updates nicht gewechselt wird. Dafür stehen, abhängig vom jeweiligen Smartphone bzw. Betriebssystem, verschiedenste Einstellungen zur Verfügung (z.B.: automatischer Netzwechsel zwischen mobile Daten und WLAN erlauben, schlechte Internetverbindungen vermeiden etc.).



EVVA empfiehlt, die Keyring-Version von Medien immer am aktuellen Stand zu halten.

8.6 App-Version des Smartphones aktualisieren

Wenn für Smartphones eine neue AirKey-App verfügbar ist, so wird eine entsprechende Information am Smartphone angezeigt. Je nach Einstellungen des Google Play Stores bzw. des Apple App Stores wird die AirKey-App automatisch oder nach manueller Bestätigung aktualisiert.

Nach der Aktualisierung der App-Version, kann die AirKey-App wie gewohnt weiterverwendet werden.



Für das Herunterladen von Apps aus dem Google Play Store bzw. dem Apple App Store ist ein Google-Konto bzw. eine Apple-ID erforderlich.



Es kann vorkommen, dass die Aktualisierung der AirKey-App entweder empfohlen wird oder zwingend durchzuführen ist. In solchen Fällen wird innerhalb der AirKey-App eine entsprechende Meldung angezeigt. Dadurch werden bestimmte Funktionen eingeschränkt, das Sperren von Schließkomponenten ist aber in beiden Situationen weiterhin möglich.



EVVA empfiehlt, die Version der AirKey-App für Smartphones immer am aktuellen Stand zu halten und die automatische Aktualisierung von Apps im Google Play Store bzw. Apple App Store zu aktivieren.

8.7 Batteriewechsel und Notstromöffnung

Bei batteriebetriebenen Schließkomponenten müssen in periodischen Abständen die Batterien ausgetauscht werden. Der Batteriestand von Schließkomponenten kann innerhalb der AirKey-Onlineverwaltung und bei der Aktualisierung von Schließkomponenten mit Smartphones mit Wartungsberechtigung eingesehen werden.

Es werden drei unterschiedliche Batteriestatus unterschieden:

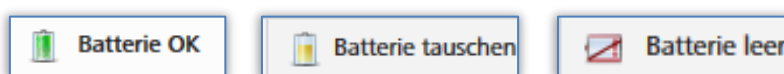


Abbildung 287: Batteriestatus

Die Schließkomponente selbst signalisiert im Falle einer "Batterie leer"-Warnung mit einer speziellen Signalisierung während eines Sperrvorgangs mit einem Medium. Nähere Informationen zur Signalisierung finden Sie im Kapitel [Signalisierung der Schließkomponenten](#).

8.7.1 Batteriewechsel beim AirKey-Zylinder



Führen Sie den Batteriewechsel bei geöffneter und blockierter Tür durch, damit sie sich nicht zufällig schließt.

Bitte beachten Sie, dass die Uhrzeit des AirKey-Zylinders für maximal 1 Minute erhalten bleibt, nachdem Sie die Batterien entfernt haben.

Es wird dringend empfohlen, bei jedem Batteriewechsel die Dichtungen des AirKey-Zylinders zu tauschen, um die Dichtheit weiterhin zu gewährleisten. Dabei handelt es sich um die Dichtung zwischen Knaufachse und Außenknauf sowie um die Dichtungen in der Knaufscheibe des Außenknaufs. All diese Dichtungen sind als Ersatzteile erhältlich. Details hierzu erhalten Sie auf Anfrage bei Ihrem EVVA-Fachhändler.

Es wird dringend empfohlen, zumindest im Zuge eines jeden Batteriewechsels, den AirKey-Zylinder zu schmieren. Hierfür ist nach Abnahme des Außenknaufs zwischen der Knaufachse und dem Zylindergehäuse an der Außenseite mit einem Tropfen des von EVVA empfohlenen Schmiermittels zu schmieren. Zusätzlich wird empfohlen, bei einem temporären Ausbau des AirKey-Zylinders an der Rückseite des Zylinders zwischen Sperrnase und Zylindergehäuse zu schmieren. Details hierzu erhalten Sie auf Anfrage bei Ihrem EVVA-Fachhändler.

- › Sperren Sie mit einem gültigen Medium die Schließkomponente.
- › Bringen Sie das Montagewerkzeug an, bevor der Zylinder wieder auskuppelt.
- › Schrauben Sie den Knauf des Zylinders mit aufgesetztem Montagewerkzeug durch Drehung gegen den Uhrzeigersinn ab.
- › Entfernen Sie das Montagewerkzeug vom Knauf.
- › Öffnen Sie den Knauf, indem Sie die drei Schrauben auf der Rückseite des Knaufs lösen.
- › Nehmen Sie die Knaufscheibe des Knaufs ab.
- › Lösen Sie vorsichtig die Batteriehalterung, indem Sie diese nach oben bewegen.
- › Wechseln Sie anschließend die Batterien. Achten Sie darauf, die Batterien lagerichtig einzulegen. Vermischen Sie dabei keine alten und neuen Batterien.
- › Fixieren Sie vorsichtig die Batteriehalterung.
- › Setzen Sie die Knaufscheibe auf den Knauf auf und fixieren Sie diese mit den drei Schrauben.
- › Bringen Sie das Montagewerkzeug am Knauf an.

- > Achten Sie darauf, dass der Dichtring auf der Achse des Zylinders korrekt aufgesetzt ist und schrauben Sie den Knauf durch Drehung im Uhrzeigersinn wieder auf den Zylinder, bis Sie einen Widerstand spüren.
- > Entfernen Sie das Montagewerkzeug.
- > Drehen Sie den Knauf anschließend gegen den Uhrzeigersinn, bis Sie ein Einrasten bemerken.
- > Achten Sie darauf, dass der Knauf und das Elektronikmodul ordnungsgemäß eingearastet sind.
- > Aktualisieren Sie abschließend den Zylinder mit dem Smartphone oder der Codierstation, um die aktuellen Protokolleinträge in die AirKey-Onlineverwaltung zu übertragen.
- > Prüfen Sie die Funktion des Zylinders mit einem Sperrversuch, bevor Sie die Tür wieder schließen.



Aufgrund der physikalischen Eigenschaften von Batterien müssen bei tiefen Temperaturen (unter -10 °C) über einen längeren Zeitraum die Batterien früher gewechselt werden sowie die Funktion des Zylinders und der Batteriestand beobachtet werden.



Wird nach einem Batterietausch ein Kommunikationsfehler signalisiert, so liegt das daran, dass der Knauf versucht, mit dem Elektronikmodul zu kommunizieren. Das funktioniert nicht, solange der Knauf nicht auf das Elektronikmodul geschraubt wurde.



Prüfen Sie den Batteriestand von Schließkomponenten mittels eines Smartphones mit Wartungsberechtigung, indem Sie die Schließkomponente aktualisieren und im Anschluss die Details der Schließkomponente einsehen.

Sollte es einmal vorkommen, dass die Batterien nicht rechtzeitig getauscht wurden, gibt es die Möglichkeit einer Notstromöffnung mittels optionalen Notstromgeräts.

Eine Ablaufbeschreibung hierzu finden Sie im Kapitel [Notstromgerät](#).



Wechseln Sie nach einer Notstromöffnung die Batterien und aktualisieren Sie die Schließkomponente, bevor Sie die Tür wieder schließen.

Verschließen Sie nach Gebrauch die weiße Gummiabdeckung mit dem EVVA-Logo wieder sorgfältig, um die Buchsenöffnung für den Anschluss des Notstromgerätes weiterhin gegen den Eintritt von Staub und Feuchtigkeit zu schützen. Verwenden Sie hierfür keine spitzen Gegenstände, um mögliche Beschädigungen zu vermeiden.

8.8 Reparaturoptionen

In den Reparaturoptionen von Schließkomponenten kann auf einen Defekt von diesen reagiert werden. Es besteht die Möglichkeit, Ersatzschließkomponenten in der Schließanlage auszustellen oder eine defekte Schließkomponente aus der Schließanlage zu entfernen.

8.8.1 Ersatzschließkomponente ausstellen und einbauen

Mit dem Ausstellen und anschließendem Einbau einer Ersatzschließkomponente wird eine bestehende defekte Schließkomponente durch eine Schließkomponente im Auslieferungszustand ersetzt. Es werden dadurch alle Eigenschaften sowie die Berechtigungen für diese Schließkomponente innerhalb der AirKey-Schließanlage beibehalten. Die Ersatzschließkomponente befindet sich nach Abschluss des Vorgangs nicht mehr im Auslieferungszustand.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandler**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste auf jene Schließkomponente, die Sie bearbeiten möchten.
- > Klicken Sie im Reiter "Einstellungen" im Block **Protokollierung und Reparaturoptionen** auf **Reparaturoptionen anzeigen** 1.

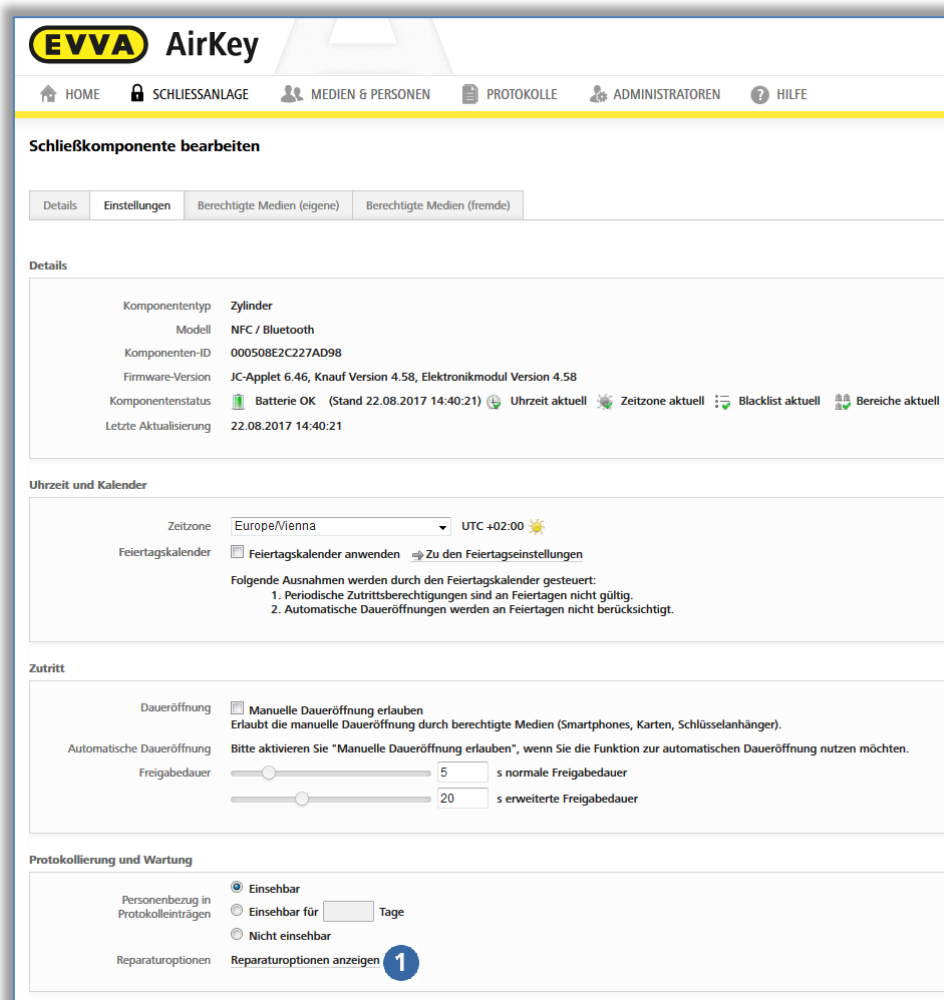


Abbildung 288: Schließkomponente bearbeiten – Reparaturoptionen

Es öffnet sich das Dialogfenster "Reparaturoptionen".

- > Standardmäßig sind die Radiobuttons **Ausbauen und Ersatzkomponenten einbauen** 1 sowie Zylinder wechseln (Knauf und Elektronikmodul zusammen) voreingestellt.

- > Alternativ können Sie auch den Radiobutton **Nur Knauf wechseln** auswählen.

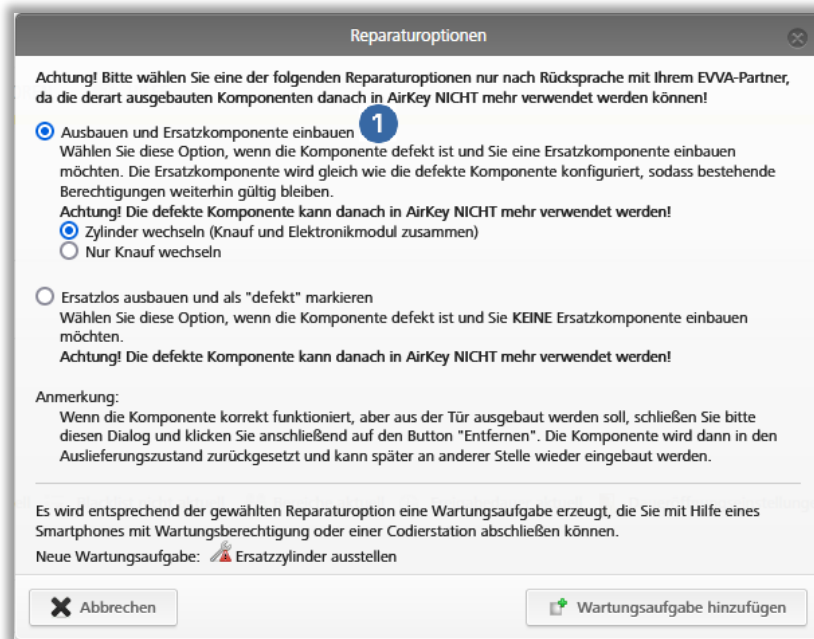


Abbildung 289: Reparaturoptionen

- > Klicken Sie auf **Wartungsaufgabe hinzufügen**.

Der Komponentenstatus ① der Schließkomponente wird aktualisiert und als Wartungsaufgabe angezeigt ②.

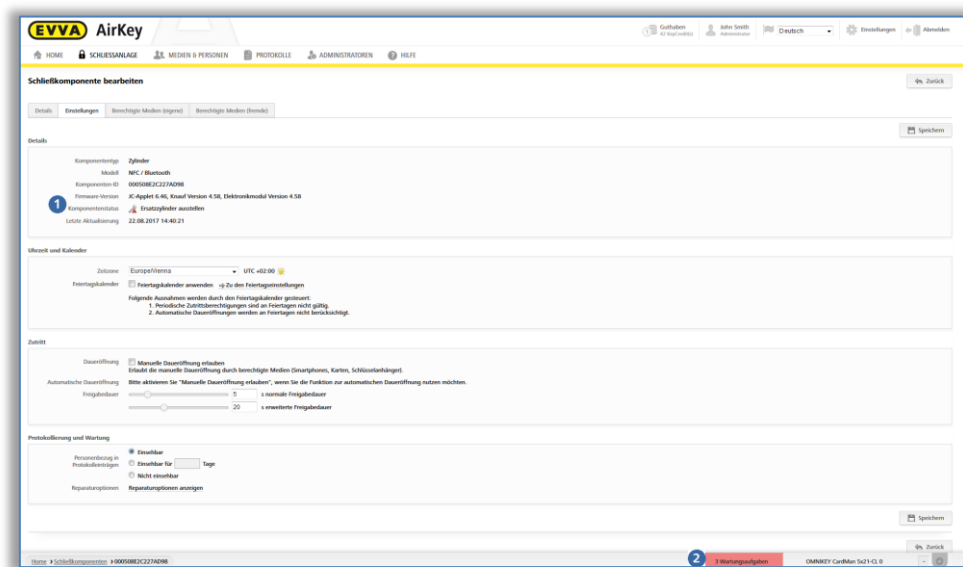


Abbildung 290: Komponentenstatus und Wartungsaufgabe

Die Vorbereitungen für das Ausstellen und den Einbau einer Ersatzschließkomponente sind damit innerhalb der AirKey-Onlineverwaltung abgeschlossen. Um den gesamten Vorgang abzuschließen, müssen Sie die Ersatzschließkomponente mit dem Smartphone mit Wartungsberechtigung oder der optionalen Codierstation ausstellen und einbauen.



Die zu tauschende Komponente ist weiterhin aktualisierbar und zwar so lange bis der Einbau der Ersatzkomponente vollständig abgeschlossen wurde. Damit wird die Vollständigkeit der Protokolle sichergestellt, sollten noch Zutritte zwischen Ersatzkomponente einbauen und Ersatzkomponente erfolgreich eingebaut stattfinden.

Bei einem Austausch von Schließkomponenten mit Bluetooth werden sowohl die Ersetzte als auch die Ersatzkomponente in der Liste der Bluetooth-Komponenten in Reichweite angezeigt. Die ersetzte Komponente muss nach erfolgtem Tausch stromlos gesetzt werden, erst dann verschwindet sie aus der Liste der Bluetooth-Komponenten.

Ersatzschließkomponente mit dem Smartphone ausstellen und einbauen



Voraussetzung ist ein Smartphone mit Wartungsberechtigung für jene Schließanlage, in der die Ersatzschließkomponente ausgestellt und eingebaut werden soll.

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden** halten Sie das Smartphone an die Schließkomponente im Auslieferungszustand.
- > Verbindung über **Bluetooth** (bei **Android**-Smartphones) herstellen: Tippen Sie bei der Schließkomponente im Auslieferungszustand, die Sie in Ihre Schließanlage hinzufügen wollen, auf das Kontextmenü (:) und wählen Sie dann **Verbinden**.
- > Verbindung über **Bluetooth** (bei **iPhones**) herstellen: Wischen Sie bei der Schließkomponente im Auslieferungszustand, die Sie in Ihre Schließanlage hinzufügen wollen, auf der Bezeichnung "Im Auslieferungszustand" nach links und wählen Sie dann **Verbinden**.
- > Klicken Sie nach der Aktualisierung in den Details der Schließkomponente auf **Ersatzzylinder ausstellen**.
- > Tippen Sie im nachfolgenden Dialog auf die Schließkomponente, die ersetzt werden soll und bestätigen Sie mit **Weiter**.
- > Bei der Verwendung von NFC halten Sie erneut das Smartphone an die Schließkomponente im Auslieferungszustand. Bei der Verwendung von Bluetooth wählen Sie die Schließkomponente im Auslieferungszustand aus der Liste der Schließkomponenten in Empfangsreichweite aus.
- > Bestimmen Sie, ob eine Wartungsaufgabe für den späteren Einbau erstellt werden soll.
- > Beenden Sie den Vorgang mit **Später einbauen**, sofern Sie die Schließkomponente noch in der Tür montieren müssen oder wählen Sie **Abschließen**, wenn die Montage in der Tür bereits erfolgt ist.
- > Aktualisieren Sie die Schließkomponente nach der Montage in der Tür.

Option

Ersatzschließkomponente mit der Codierstation ausstellen und einbauen.

- > Legen Sie eine Ersatzschließkomponente im Auslieferungszustand auf die Codierstation.

- > Wählen Sie rechts unten im Dialogfenster **Ersatzzylinder ausstellen** und jene Schließkomponente, die ersetzt werden soll.

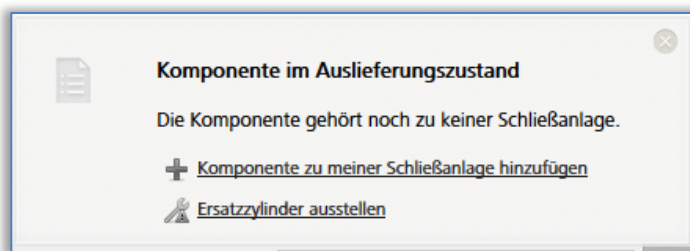


Abbildung 291: Komponente im Auslieferungszustand – Ersatzzylinder ausstellen

- > Klicken Sie auf **Weiter**.
- > Legen Sie die Ersatzschließkomponente im Auslieferungszustand auf die Codierstation.
- > Entfernen Sie die Ersatzschließkomponente erst, nachdem eine entsprechende Erfolgsmeldung angezeigt wird.
- > Bestimmen Sie, ob eine Wartungsaufgabe für den späteren Einbau erstellt werden soll.
- > Beenden Sie den Vorgang mit **Später einbauen**, sofern Sie die Schließkomponente noch in der Tür montieren müssen oder wählen Sie **Abschließen**, wenn die Montage in der Tür bereits erfolgt ist.
- > Aktualisieren Sie die Schließkomponente nach der Montage in der Tür.



Sofern die Ersatzschließkomponente eine alte Firmware-Version besitzt, wird das Firmware-Update während dieses Vorgangs durchgeführt.


Die ersetzte Schließkomponente ist nach diesem Vorgang nicht mehr verwendbar. Führen Sie diese Funktion deshalb nur durch, wenn die Schließkomponente wirklich defekt ist und Sie diese nicht mehr benötigen.

8.8.2 Schließkomponente ersatzlos ausbauen und als "defekt" markieren

Sofern eine defekte Schließkomponente nicht ersetzt werden muss, diese aber dennoch nicht mehr in der Schließanlage aufscheinen soll, so kann diese über die Reparaturoptionen ersatzlos ausgebaut werden.



Die Schließkomponente kann danach nicht mehr aktualisiert werden und wird somit unbrauchbar.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandleser**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste auf jene Schließkomponente, die Sie bearbeiten möchten.
- > Klicken Sie im Reiter **Einstellungen** im Block **Protokollierung und Reparaturoptionen** auf den Link **Reparaturoptionen anzeigen** .

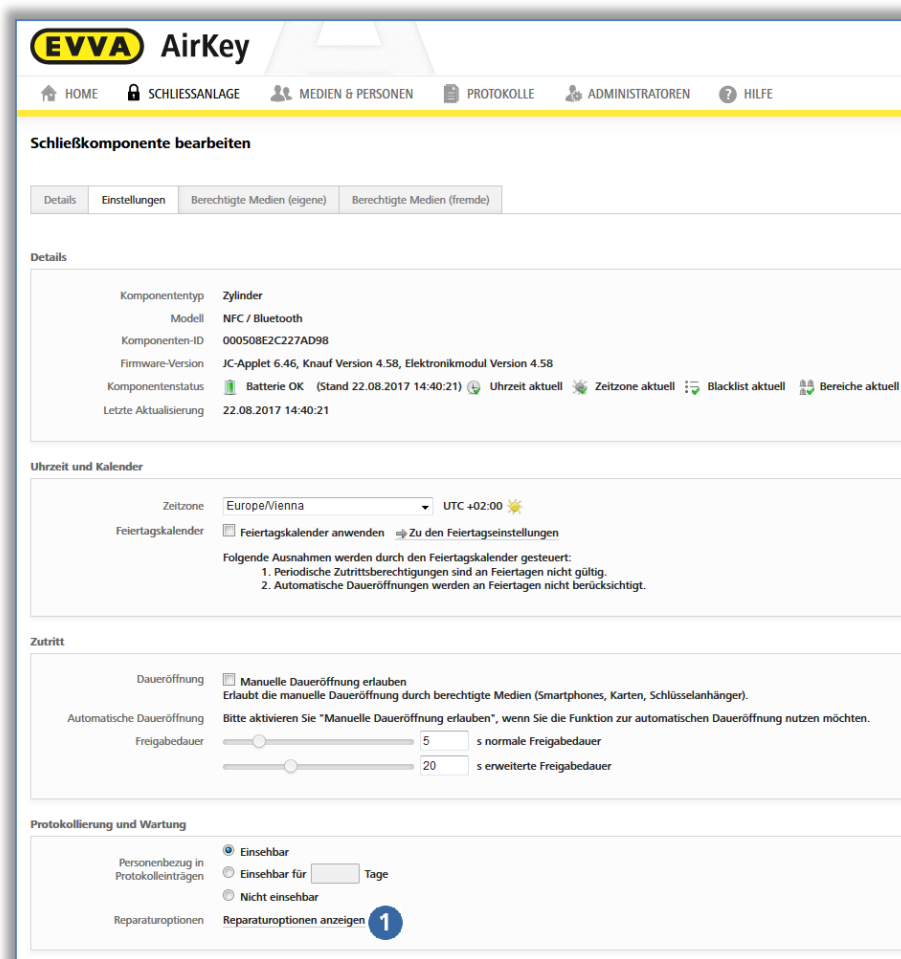


Abbildung 292: Schließkomponente bearbeiten – Reparaturoptionen

Es öffnet sich das Dialogfenster "Reparaturoptionen".

- > Wählen Sie **Ersatzlos ausbauen und als "defekt" markieren** 1.

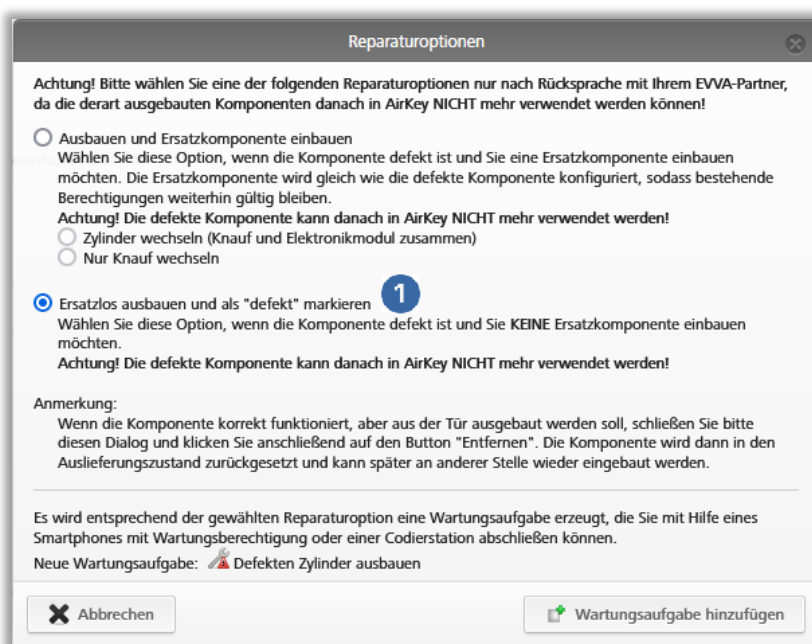


Abbildung 293: Reparaturoptionen

- > Klicken Sie auf **Wartungsaufgabe hinzufügen**.

Der Komponentenstatus ❶ der Schließkomponente wird aktualisiert und als Wartungsaufgabe angezeigt ❷.

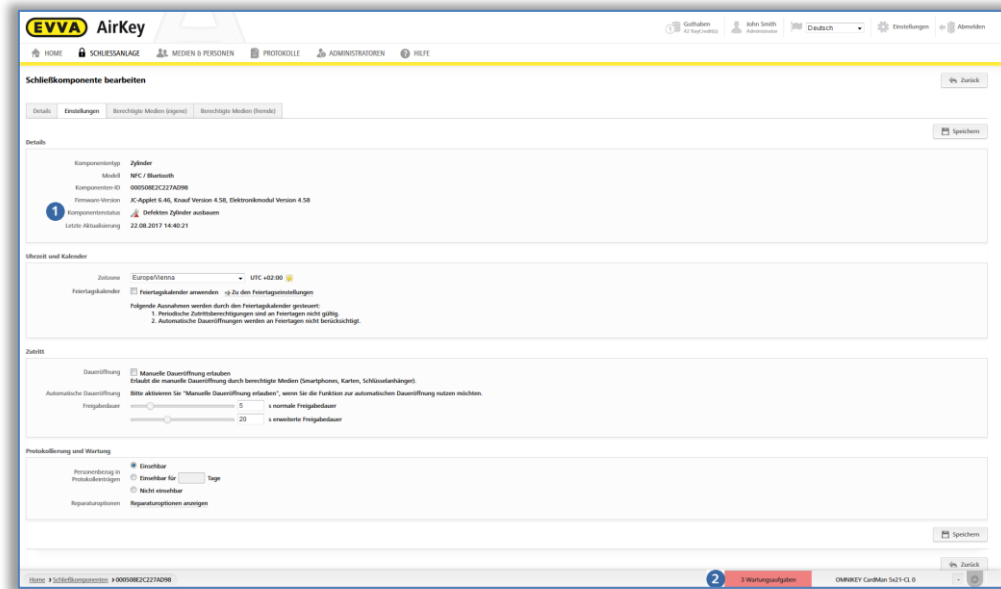


Abbildung 294: Komponentenstatus und Wartungsaufgabe

Die Vorbereitungen für den ersatzlosen Ausbau einer defekten Schließkomponente sind damit innerhalb der AirKey-Onlineverwaltung abgeschlossen. Um den gesamten Vorgang abzuschließen, müssen Sie den Ausbau mittels Smartphone mit Wartungsberechtigung oder innerhalb der AirKey-Onlineverwaltung abschließen.

8.8.3 Defekte Schließkomponente mittels Smartphone ausbauen

Sofern eine Aktualisierung der defekten Schließkomponente noch möglich ist, können Sie den ersatzlosen Ausbau einer defekten Schließkomponente mit dem Smartphone durchführen. Voraussetzung ist ein registriertes Smartphone mit aktiver Wartungsberechtigung für diese AirKey-Schließanlage.

- > Verbindung über **NFC** (bei Android-Smartphones) herstellen: Tippen Sie auf das Symbol **Mit Komponente verbinden** halten Sie das Smartphone an die Schließkomponente, die ausgebaut werden soll.
- > Verbindung über **Bluetooth** (bei **Android**-Smartphones) herstellen: Tippen Sie bei der Schließkomponente, die ausgebaut werden soll auf das Kontextmenü (:) und wählen Sie dann **Verbinden**.
- > Verbindung über **Bluetooth** (bei **iPhones**) herstellen: Wischen Sie bei der Schließkomponente, die ausgebaut werden soll auf der Bezeichnung nach links und wählen Sie dann **Verbinden**.
- > Es werden die Komponentendetails angezeigt. Wählen Sie **Defekten Zylinder ausbauen** ❶.

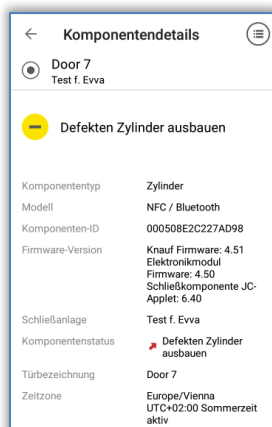


Abbildung 295: Smartphone-defekte Komponente ausbauen

- > Setzen Sie das Häkchen im Dialog und bestätigen Sie mit **Abschließen**.

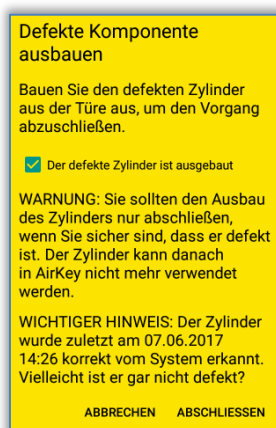


Abbildung 296: Smartphone – defekte Komponente ausbauen – Bestätigung

Damit ist der Vorgang abgeschlossen und die Schließkomponente wird nicht mehr innerhalb der AirKey-Schließanlage gelistet. Die Schließkomponente ist nun nicht mehr verwendbar.

8.8.4 Defekte Schließkomponente mittels AirKey-Onlineverwaltung ausbauen

Sofern die Schließkomponente aufgrund eines Defekts nicht mehr aktualisiert werden kann, muss der ersatzlose Ausbau über die AirKey-Onlineverwaltung abgeschlossen werden.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandleser** – je nachdem, welche Komponente als defekt markiert wurde.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste auf die Schließkomponente, die Sie bearbeiten möchten.
- > Klicken Sie im Reiter **Einstellungen** im Block **Protokollierung und Reparaturoptionen** auf den Link **Reparaturoptionen anzeigen**.
- > Es erscheint ein Dialogfenster, in dem Sie zwischen drei Optionen wählen können.

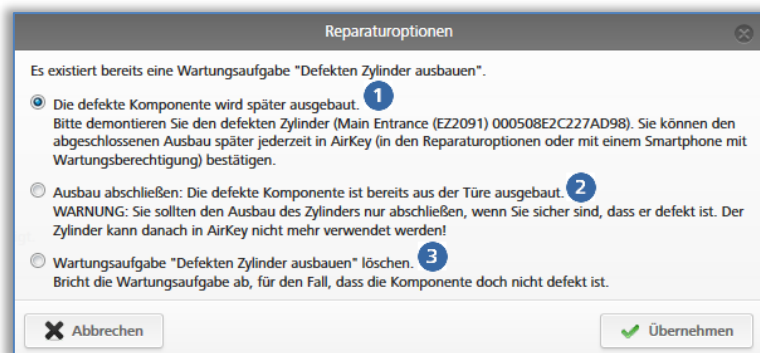


Abbildung 297: Defekte Schließkomponente ausbauen

- > Mit der Option **Die defekte Komponente wird später ausgebaut** ❶ behalten Sie den aktuellen Komponentenstatus bei und die Schließkomponente bleibt weiterhin Teil der AirKey-Schließanlage.
- > Mit der Option **Ausbau abschließen: Die defekte Komponente ist bereits aus der Türe ausgebaut** ❷ wird der Vorgang des ersatzlosen Ausbaus einer defekten Schließkomponente abgeschlossen und die Schließkomponente wird aus der AirKey-Schließanlage entfernt.
- > Mit der Option **Wartungsaufgabe "Defekten Zylinder ausbauen" löschen** ❸ wird der ersatzlose Ausbau wieder rückgängig gemacht. Nähere Informationen finden Sie im Kapitel [Wartungsaufgaben für Reparaturoptionen rückgängig machen](#).



Die Schließkomponente, die ersatzlos ausgebaut wurde, ist nach diesem Vorgang nicht mehr verwendbar. Führen Sie diese Funktion deshalb nur durch, wenn die Schließkomponente wirklich defekt ist und Sie diese nicht mehr benötigen.

Wenn Sie eine funktionsfähige Schließkomponente aus Ihrer Schließanlage entfernen möchten, verwenden Sie die Anleitung unter [Schließkomponente entfernen](#).

8.8.5 Wartungsaufgaben für Reparaturoptionen rückgängig machen

Wenn eine Wartungsaufgabe für eine Ersatz-Schließkomponente oder einen ersatzlosen Ausbau versehentlich erstellt wurde, so kann diese Wartungsaufgabe nachträglich gelöscht werden.

- > Klicken Sie auf der Startseite **Home** auf den Link **Wartungsaufgaben**.
- > Wählen Sie aus der Liste die gewünschte Wartungsaufgabe aus.
- > Klicken Sie im Reiter **Einstellungen** im Block **Protokollierung und Reparaturoptionen** auf den Link **Reparaturoptionen anzeigen**.
- > Wählen Sie je nach offener Wartungsaufgabe, ob die Ersatzschließkomponente (Zylinder, Knauf, Wandleser) später ausgestellt ❶ werden soll oder ob die Wartungsaufgabe gelöscht ❷ werden soll.

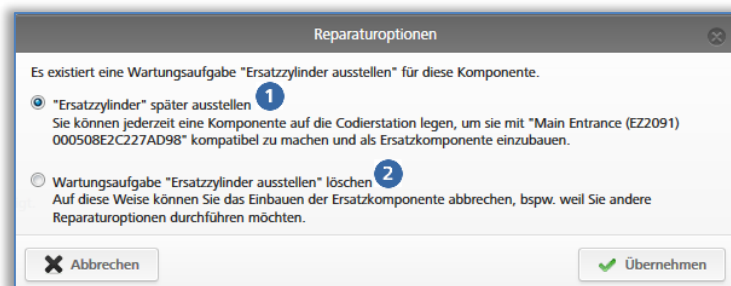


Abbildung 298: Wartungsaufgabe löschen

- > Klicken Sie auf **Übernehmen**.

Die Wartungsaufgabe wird dadurch rückgängig gemacht. Der Komponentenstatus der Schließkomponente wird entsprechend dem letzten Status der Schließkomponente aktualisiert.



Sofern die Wartungsaufgabe der Reparaturoption schon abgeschlossen wurde, kann diese nicht mehr rückgängig gemacht werden.



Verwenden Sie diese Funktion auch, um die Wartungsaufgabe "Komponente muss entfernt werden" rückgängig zu machen, wenn die Schließkomponente ohne Defekt aus der AirKey-Schließanlage entfernt wurde.

9 Notmedien

Ein Notmedium ist ein Medium mit unbegrenzter Dauerberechtigung für alle Schließkomponenten einer AirKey-Schließanlage. Notmedien finden ihren Einsatz in Notsituationen (z.B. beim Einsatz der Feuerwehr) und müssen an einem sicheren Ort verwahrt werden. Notmedien erhalten, unabhängig von der Uhrzeit in der Schließkomponente, Zutritt. Einzig die Stromversorgung von den Schließkomponenten muss sichergestellt werden.

9.1 Notmedien ausstellen

Zum Ausstellen eines Notmediums legen Sie ein Medium in Form einer Karte, Schlüsselanhängers, Kombischlüssels oder Armbänder – wie im Kapitel [Karten, Schlüsselanhänger, Kombischlüssel und Armbänder anlegen](#) beschrieben – an und vergeben Sie den Notmedien Dauerzutrittsberechtigungen zu allen Türen der Schließanlage. Achten Sie darauf, dass die Notmedien im Falle einer Anlagenerweiterung entsprechend aktualisiert werden, um auch zu den neu hinzugefügten Türen im Notfall Zutritt zu haben. Notmedien haben Zutritt auch zu Schließkomponenten mit falscher Uhrzeit (z.B. Zylinder verlieren die Uhrzeit, wenn die Batterien leer sind). Nähere Informationen zur Vergabe und dem Anfertigen von Berechtigungen finden Sie im Kapitel [Berechtigungen vergeben](#) und [Berechtigung anfertigen](#).



Bedenken Sie, dass auch Medien in Form von Karten, Schlüsselanhängern, Kombischlüsseln oder Armbändern defekt werden können. Erstellen Sie daher abhängig von der Schließanlage eine entsprechende Anzahl an Notmedien.



Als Notmedien werden nur Medien in Form von Karten, Schlüsselanhängern, Kombischlüsseln oder Armbändern empfohlen, da Smartphones aufgrund der begrenzten Akkulaufzeit nicht für diesen Zweck geeignet sind.

Um die Verwaltung von Notmedien zu erleichtern, können Sie mit Bereichen arbeiten, in denen alle der Schließanlage zugehörigen Türen enthalten sind. Vergeben Sie dann den Notmedien eine unbegrenzte Dauerberechtigung für diesen Bereich.

10 Medientausch

10.1 Smartphonetausch

Der Smartphonetausch vereinfacht den Wechsel von einem Smartphone zu einem anderen Smartphone, zum Beispiel bei der Anschaffung eines neuen Geräts.

Beim Smartphonetausch werden alle AirKey-Berechtigungen und -Einstellungen (ausgenommen PIN und die lokalen Hands-free-Einstellungen) des bereits vorhandenen Smartphones auf das neue Smartphone übertragen.

Der Tausch kann sowohl von Android zu iOS als auch umgekehrt durchgeführt werden.

Der Tausch kann entweder von einem Administrator in der AirKey-Onlineverwaltung oder direkt vom Smartphone gestartet werden.

Das "alte" Smartphone wird als **Quellmedium** und das "neue" Smartphone als **Zielmedium** bezeichnet.



Das Quellmedium wird nach abgeschlossener Tauschaktion automatisch deaktiviert. Sollte das Quellmedium nicht mehr funktionstüchtig oder verfügbar sein, muss die Blacklist der betroffenen Schließkomponenten aktualisiert werden. Erst danach ist die Sicherheit der Anlage wiederhergestellt.



Wenn im Zuge der Tauschaktion auch Berechtigungen auf das Zielmedium übertragen werden, wird auch ein KeyCredit vom bestehenden Guthaben abgebucht. Wenn keine KeyCredits verfügbar sind, kann der Tausch erst abgeschlossen werden, sobald wieder ein Guthaben vorhanden ist.

10.1.1 Tausch als Smartphone-Besitzer starten

Wenn das Quellmedium noch funktioniert, registriert und nicht deaktiviert ist, kann der Smartphonetausch direkt über das Quellmedium gestartet werden.

- > Starten Sie die AirKey-App am alten Smartphone.
- > Tippen Sie im Menü auf **Einstellungen** → **Smartphone tauschen**.
- > Bestätigen Sie den Dialog mit **OK**.



Abbildung 299: Smartphonetausch bestätigen

- > Ein QR-Code mit einem Hilfetext wird am Quellmedium angezeigt.



Abbildung 300: QR-Code für den Smartphonetausch

Die Schritte am Quellmedium sind damit abgeschlossen. Das Quellmedium kann bis zum Abschluss der Tauschaktion wie gewohnt weiterverwendet werden. Der QR-Code ist 30 Tage gültig und wird innerhalb dieses Zeitraums beim Tippen auf **Einstellungen** → **Smartphone tauschen** erneut angezeigt.

Da beim Smartphonetausch ein neues Smartphone angelegt wird und abhängig von den übertragenen Berechtigungen auch KeyCredits abgebucht werden, muss der Tausch von einem Administrator innerhalb der AirKey-Onlineverwaltung bestätigt werden.

- > Melden Sie sich in der AirKey-Onlineverwaltung an.

- > Klicken Sie auf der Startseite auf die Kachel **Offene Smartphone-Tauschoperationen**.

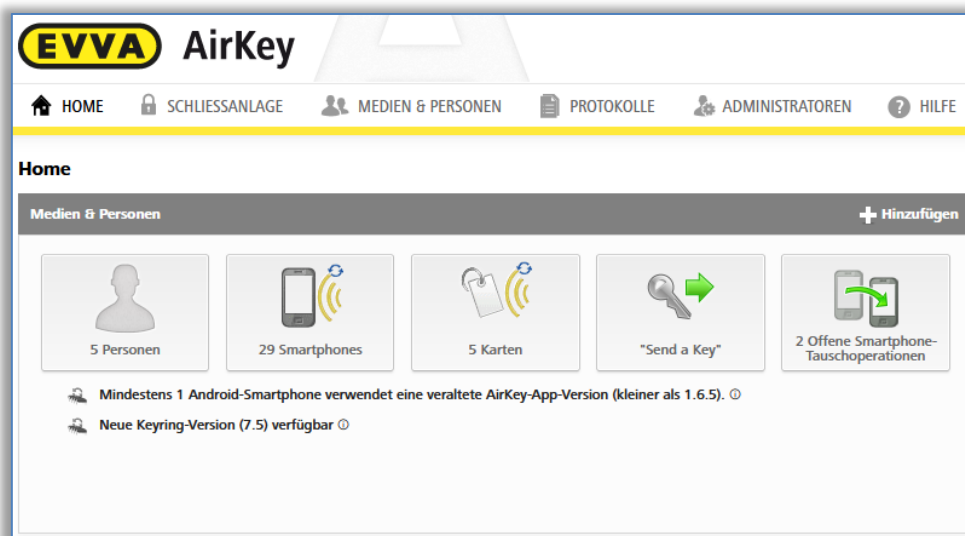


Abbildung 301: Startseite – Offene Smartphone-Tauschoperationen

In der Spalte "Aktion" kann über das grüne Häkchen der Tausch bestätigt oder über das rote "X" abgelehnt werden.

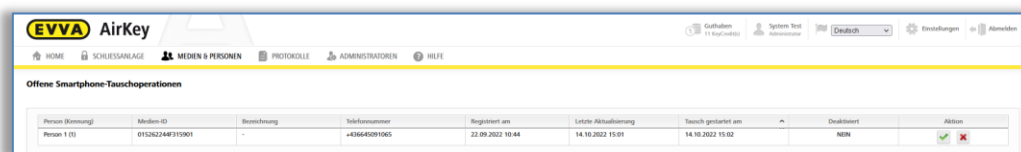


Abbildung 302: Offene Smartphone-Tauschoperationen

Nach der Bestätigung des Administrators kann der Tausch durch Scannen des QR-Codes am Zielmedium abgeschlossen werden. Wird der Tausch vom Administrator abgelehnt, wird der Smartphonetausch abgebrochen und der QR-Code ist nicht mehr gültig und wird entfernt. Wenn der QR-Code am Zielmedium gescannt wird, bevor ein Administrator den Tausch bestätigt hat, erscheint eine entsprechende Fehlermeldung.

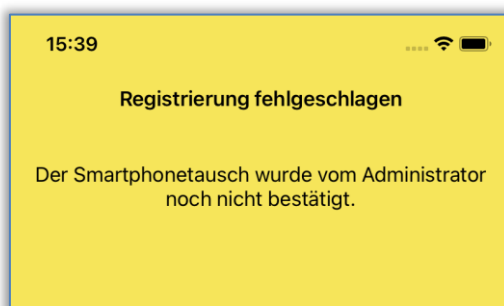


Abbildung 303: Smartphonetausch fehlgeschlagen



Administratoren können auch eine automatische Bestätigung für Smartphone-Tauschaktionen in den Einstellungen der AirKey-Onlineverwaltung aktivieren (siehe Kapitel [Allgemein](#)). Damit wird jeder Smartphonetausch, der über ein Smartphone gestartet wurde, sofort automatisch bestätigt,

wenn ausreichend Guthaben vorhanden ist. Bedenken Sie, dass bei jedem Smartphonetausch, bei dem Berechtigungen übertragen werden, ein KeyCredit abgebucht wird.

Zum Scannen des QR-Codes mit einem noch nicht registriertem Zielmedium befolgen Sie folgende Schritte:

- > Starten Sie die AirKey-App.
- > Bestätigen Sie die EULA.
- > Tippen Sie auf **QR-Code scannen** und scannen Sie den QR-Code vom Quellmedium.

Zum Scannen des QR-Codes mit einem bereits bei AirKey registrierten Zielmedium befolgen Sie folgende Schritte:

- > Starten Sie die AirKey-App.
- > Tippen Sie im Menü auf **Einstellungen** → **Schließenanlage hinzufügen**.
- > Tippen Sie auf **QR-Code scannen** und scannen Sie den QR-Code vom Quellmedium.

Der Smartphonetausch ist damit abgeschlossen und das Zielmedium ist mit den AirKey-Berechtigungen und -Einstellungen des Quellmediums erfolgreich registriert. Das Quellmedium wird nach dem erfolgreichen Tausch automatisch deaktiviert.



Befindet sich das Quellmedium in mehr als einer Schließenanlage, so wird der Tausch in allen Schließenanlagen gleichzeitig gestartet. Das bedeutet, dass eventuell auch mehrere Administratoren den Tausch innerhalb der AirKey-Onlineverwaltung bestätigen müssen. Es werden nur jene AirKey-Berechtigungen und -Einstellungen für die Schließenanlagen auf das Zielmedium übertragen, in denen die Administratoren den Tausch bestätigt haben.

10.1.2 Tausch als Administrator starten

Wenn das Quellmedium nicht mehr verfügbar oder nicht mehr funktionstüchtig ist, kann der Tausch auch als Administrator gestartet werden.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Wählen Sie in der Medienliste das Smartphone aus, das getauscht werden soll.
- > Klicken Sie auf **Mehr...** ⓘ → **Smartphone tauschen**.

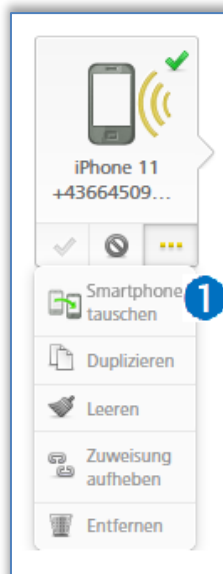


Abbildung 304: Smartphone tauschen

- > Es öffnet sich ein Dialog, in dem die Telefonnummer des Zielmediums eingetragen werden muss. Es wird automatisch die Telefonnummer des Quellmediums übernommen.

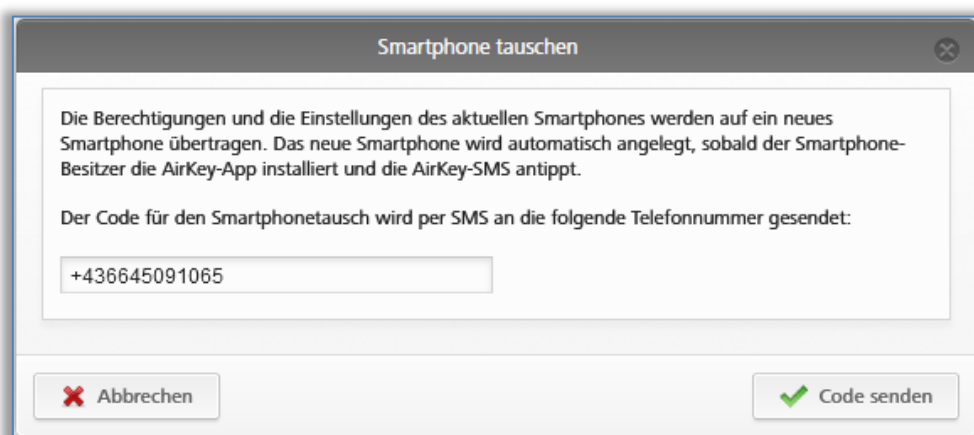


Abbildung 305: Smartphone tauschen

- > Prüfen Sie die Telefonnummer auf Korrektheit und bestätigen Sie mit **Code senden**.
- > An die angegebene Telefonnummer des Zielmediums wird eine AirKey-SMS mit einem Registrierungslink gesendet.

Der Smartphonetausch muss jetzt noch am Zielmedium abgeschlossen werden:

- > Öffnen Sie die SMS mit dem Registrierungslink am Zielmedium.
- > Tippen Sie auf den Registrierungslink und folgen Sie den Anweisungen.

Der Smartphonetausch ist damit abgeschlossen und das Zielmedium ist mit den AirKey-Berechtigungen und -Einstellungen des Quellmediums erfolgreich registriert. Das Quellmedium wird nach dem erfolgreichen Tausch automatisch deaktiviert.

Der Registrierungslink in der SMS ist 30 Tage gültig. Sollte der Registrierungslink nicht per SMS angekommen sein, so kann dieser erneut per SMS gesendet werden:

- > Klicken Sie unterhalb des Smartphones auf **Mehr...** ① → **Smartphone tauschen**.

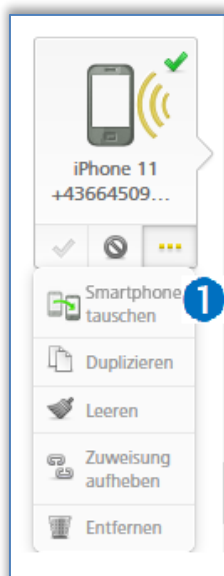


Abbildung 306: Smartphone tauschen

- > Es öffnet sich ein Dialog, bei dem die Telefonnummer erneut geprüft und geändert werden kann.



Abbildung 307: Smartphone tauschen – Code erneut senden

- > Klicken Sie auf **Code erneut senden**.

In diesem Dialog kann auch der Tausch abgebrochen werden, wenn dieser nicht mehr notwendig ist.



Befindet sich das Quellmedium in mehr als einer Schließenanlage, so muss der Tausch von einem Administrator aus jeder Schließenanlage gestartet werden. Dementsprechend wird auch für jede Schließenanlage eine SMS mit einem Registrierungslink gesendet.

11 Arbeiten mit mehreren AirKey-Schließanlagen

Im nachfolgenden Kapitel finden Sie Hinweise zum Arbeiten mit mehreren AirKey-Schließanlagen.

11.1 Schließkomponente für andere Schließanlagen freigeben

Sie können eine Ihrer Schließanlage hinzugefügte Komponente für eine andere Schließanlage freigeben. In der anderen Schließanlage können dann ebenfalls Berechtigungen für diese Schließkomponente vergeben werden. Jede Schließkomponente kann für maximal 250 Schließanlagen freigegeben werden.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandleser**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste auf die Türbezeichnung jener Schließkomponente, die Sie freigeben möchten.

Im Block **Freigaben** der Details der Schließkomponente werden die bereits erteilten Freigaben aufgelistet.

- > Klicken Sie auf **Freigabe hinzufügen**.

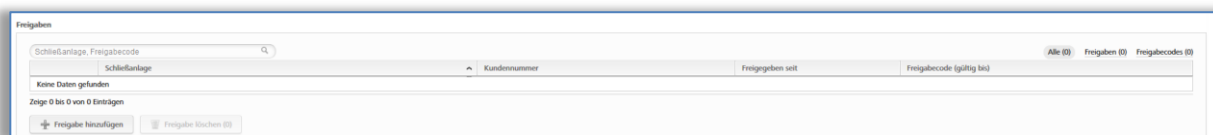


Abbildung 308: Schließkomponente freigeben

- > Es wird ein 12-stelliger Freigabecode generiert.

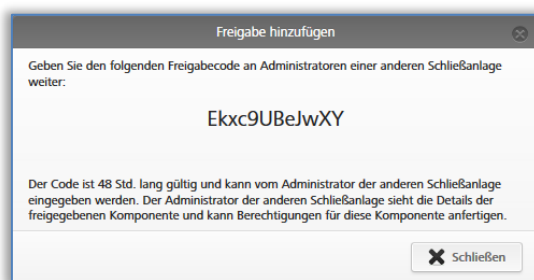


Abbildung 309: Freigabe hinzufügen

- > Kommunizieren Sie diesen Freigabecode an den Administrator der anderen Schließanlage.



Der Freigabecode bleibt 48 Stunden gültig.



Es können für eine Schließkomponente mehrere Freigabecodes generiert werden. Diese werden in der Freigabeliste der Schließkomponente dargestellt.

Es entsteht ein Eintrag in der Freigabeliste der Schließkomponente. Darin kann der Freigabecode und seine Gültigkeit abgelesen werden.

11.2 Schließkomponente aus anderen Schließanlagen hinzufügen

Wenn für Sie eine Schließkomponente aus einer anderen Schließanlage freigegeben wurde, müssen Sie diese in Ihrer Schließanlage hinzufügen.

- Klicken Sie auf der Startseite **Home** im grauen Balken **Schließanlage** auf **Hinzufügen** → **Schließkomponente hinzufügen** ①.

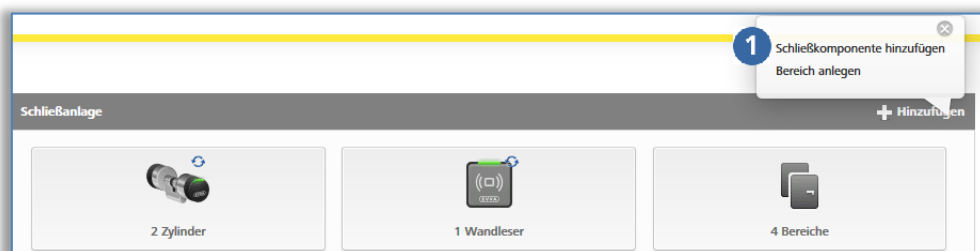


Abbildung 310: Schließkomponente hinzufügen – grauer Balken

- Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- Klicken Sie auf **Schließkomponente hinzufügen** ①.

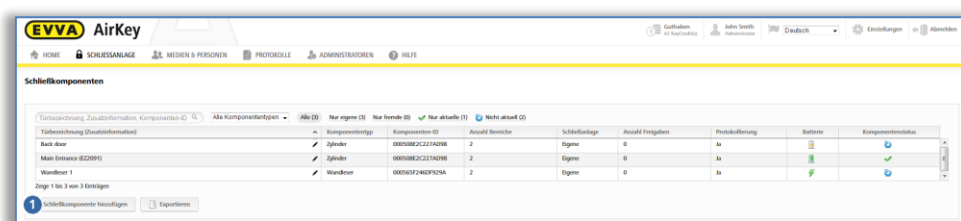


Abbildung 311: Schließkomponente hinzufügen

- Wählen Sie als Art **Freigegebene Schließkomponente** ①.
- Klicken Sie auf **Weiter**.



Abbildung 312: Freigegebene Schließkomponente hinzufügen

- > Geben Sie Freigabecode der anderen Schließanlage ein, um die Schließkomponente hinzuzufügen.

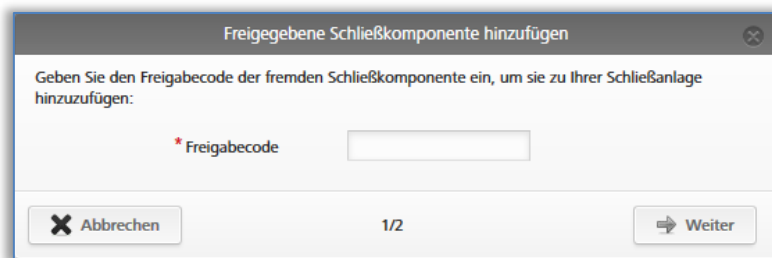


Abbildung 313: Freigegebene Schließkomponente hinzufügen

Wenn der eingegebene Freigabecode falsch ist, erhalten Sie eine Fehlermeldung.

Wenn der eingegebene Freigabecode korrekt ist, können Sie folgende Einstellungen anpassen:

- > Alternative Türbezeichnung ❶
- > Unter Datenschutz kann der Personenbezug in Protokolleinträgen für den Eigentümer der Schließkomponente einsehbar oder nicht einsehbar sein ❷.

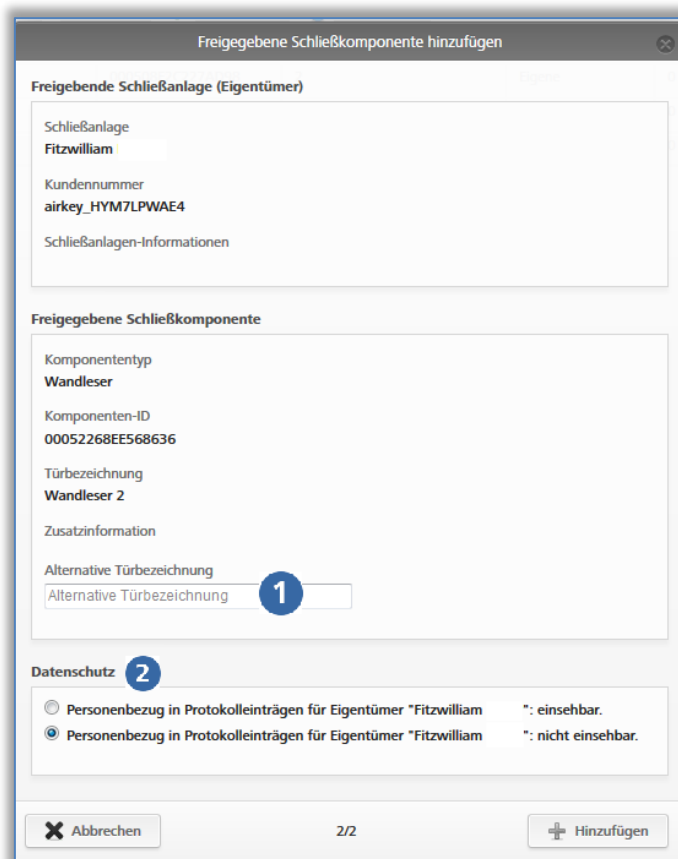


Abbildung 314: Freigegebene Schließkomponente hinzufügen

- > Es wird eine Wartungsaufgabe erstellt.
- > Aktualisieren Sie die Schließkomponente mithilfe eines Smartphones mit Wartungsberechtigung oder einer optionalen Codierstation.


- > Damit wird die Wartungsaufgabe aus der Liste entfernt und die Freigabe ist aktuell.
- > Sobald die freigegebene Schließkomponente hinzugefügt wurde, erscheint die Schließkomponente in der Spalte "Schließenanlage" mit dem Attribut "Fremde" in der Liste der Schließkomponenten. Jener Mandant, der die Schließkomponente hinzugefügt hat, kann im Reiter "Details" die alternative Türbezeichnung bearbeiten sowie die Schließkomponente einem Bereich zuweisen. Im Reiter "Einstellungen" kann im Block "Datenschutz" der Radiobutton geändert werden, um beim Personenbezug in Protokolleinträgen für den Eigentümer der Schließkomponente zwischen "einsehbar" oder "nicht einsehbar" zu unterscheiden. Weiters kann der Personenbezug in Protokolleinträgen im Block "Protokollierung und Reparaturoptionen" für die freigegebene Schließenanlage eingestellt werden. Außerdem können Zutrittsberechtigungen für die freigegebene Schließkomponente vergeben werden.



Eine fremde Schließkomponente kann nicht für andere Schließenanlagen freigegeben werden.

11.3 Berechtigungen für freigegebene Schließkomponenten vergeben

Innerhalb jener AirKey-Schließenanlage, zu der die freigegebene Schließkomponente hinzugefügt wurde, unterscheidet sich der Ablauf zum Vergeben von Berechtigungen geringfügig vom Ablauf des Eigentümers der Schließkomponente. Folgen Sie den Schritten, wenn Sie eine freigegebene Schließkomponente in Ihre Schließenanlage hinzugefügt haben.

- > Wählen Sie auf der Startseite **Home** die Kachel **Smartphones** bzw. **Karten**.
- > Alternativ wählen Sie im Hauptmenü **Medien & Personen** → **Medien**.
- > Klicken Sie in der Übersichtsliste auf das gewünschte Medium.
- > Sofern das Medium einer Person zugewiesen ist, erscheint die Übersicht der Berechtigungen des Mediums.
- > Wählen Sie unterhalb der Kacheln aller Schließkomponenten und Bereiche den Reiter **Fremde** , um alle hinzugefügten Schließkomponenten von fremden Schließenanlagen angezeigt zu bekommen.

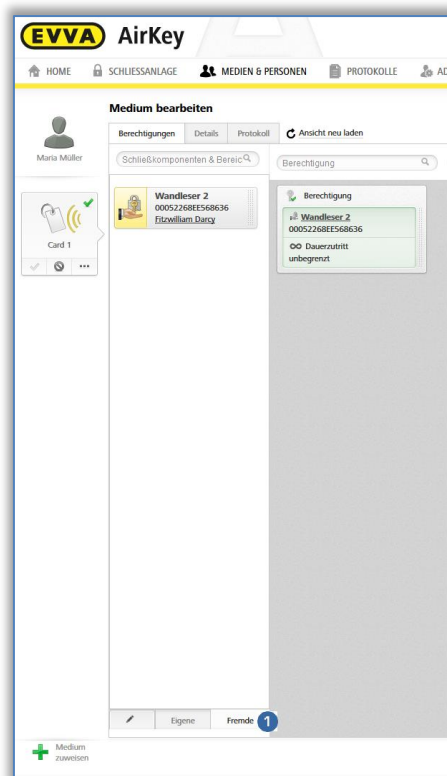


Abbildung 315: Berechtigung freigegebene Schließkomponente

- > Ziehen Sie die Schaltfläche mit der gewählten freigegebenen Tür per Drag & Drop auf die graue Fläche. Erst wenn Sie die gewählte Tür / den gewählten Bereich auf die Mittelfläche bewegen, erscheinen die Zutrittsarten.
- > Wählen Sie die gewünschte Zutrittsart, indem Sie die gewählte Türe / den gewählten Bereich per Drag & Drop auf das entsprechende Feld ziehen.
- > Fertigen Sie die Berechtigung an, in dem Sie einen KeyCredit einlösen. Nähere Informationen zum Anfertigen von Berechtigungen finden Sie im Kapitel [Berechtigung anfertigen](#). Der KeyCredit wird dabei von Guthaben Ihrer Schließanlage, nicht jedoch vom Guthaben der anderen Schließanlage, abgebucht.

11.4 Berechtigungen für freigegebene Schließkomponenten einsehen

Wenn Sie eine Schließkomponente für einen anderen Mandanten freigegeben haben, können Sie auch Medien des anderen Mandanten einsehen, die für die freigegebene Schließkomponente berechtigt sind.

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandleser**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste auf jene Schließkomponente, deren Details Sie einsehen möchten.
- > Klicken Sie auf **Berechtigte Medien (fremde)** **1**, um eine Übersicht über alle fremden Medien, die eine Berechtigung bei dieser Schließkomponente haben, zu erhalten.

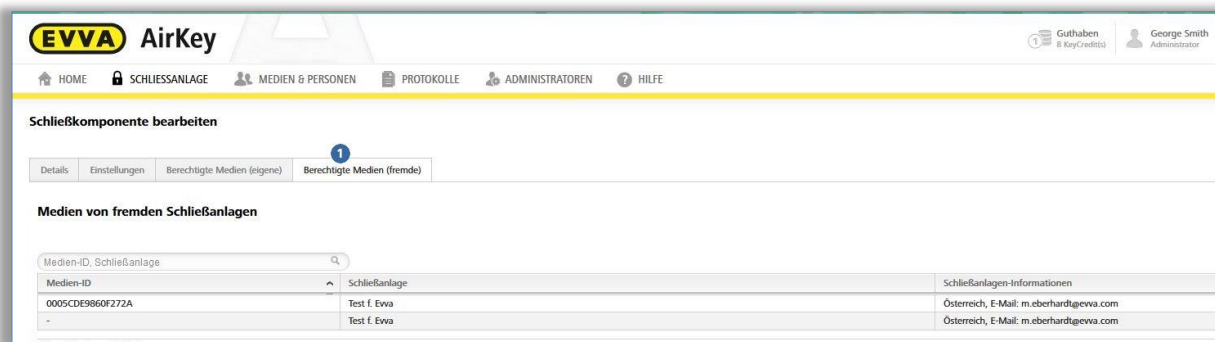


Abbildung 316: Berechtigte Medien (fremde)

11.5 Freigabe einer Schließkomponente aufheben

Sie können die von Ihnen gewährte Freigabe einer Schließkomponente wieder aufheben. Gehen Sie dazu wie folgt vor:

- > Wählen Sie auf der Startseite **Home** die Kachel **Zylinder** bzw. **Wandleser**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie in der Übersichtsliste jene Schließkomponente an, deren Freigabe Sie aufheben möchten.

Wählen Sie im Reiter **Details** im Block **Freigaben** die entsprechende Freigabe aus und klicken Sie auf **Freigabe löschen**

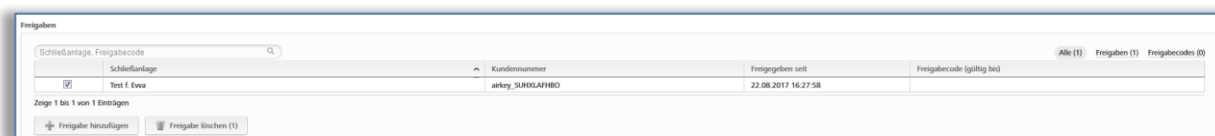


Abbildung 317: Block "Freigaben" – Freigabe löschen

- > Bestätigen Sie die Sicherheitsabfrage mit **Freigabe löschen**.

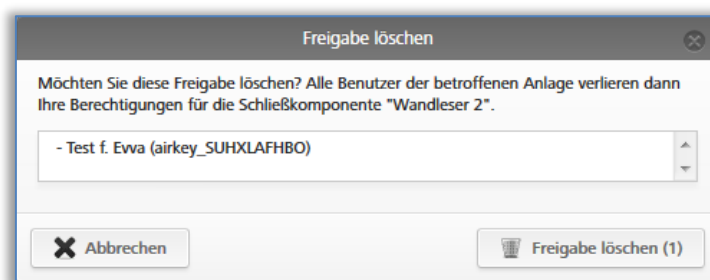


Abbildung 318: Freigabe löschen

Damit wird die Schließkomponente aus der Schließanlage des anderen Mandanten entfernt. Es wird eine Wartungsaufgabe erstellt.

- > Aktualisieren Sie jene Schließkomponente, für die Sie die Freigabe aufgehoben haben mithilfe eines Smartphone mit Wartungsberechtigung oder einer optionalen Codier-

station. Der Status der Schließkomponente ist nach erfolgter Aktualisierung wieder aktuell.



Achtung: Erst wenn die Schließkomponente aktualisiert wurde, können die Medien des anderen Mandanten nicht mehr sperren.

Freigaben von Schließkomponenten können nur aus jenen Schließanlagen gelöscht werden, in denen die Freigaben erfolgt sind.

Sofern der Freigabecode noch nicht verwendet wurde und dieser, wie in diesem Kapitel beschrieben, gelöscht wird, muss die Schließkomponente nicht aktualisiert werden.

11.6 Smartphone in mehreren Anlagen verwenden

Sie können Ihr Smartphone in mehreren Schließanlagen registrieren und als Medium verwenden.

- > Öffnen Sie innerhalb der AirKey-App das Hauptmenü und wählen Sie **Einstellungen** → **Schließanlage hinzufügen** ①.

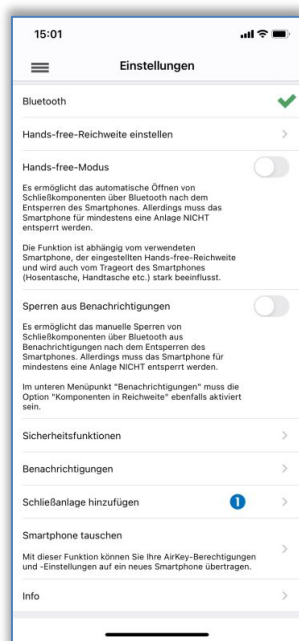


Abbildung 319: Schließanlage hinzufügen

- > Bei Android wird der Dialog für die Eingabe des Registrierungscode automatisch angezeigt. Bei iOS tippen Sie auf **Registrierungscode bereits erhalten**, um die Eingabe der Telefonnummer zu überspringen und zur Eingabe des Registrierungscode zu gelangen.
- > Geben Sie den Registrierungscode ein, den Sie vom Administrator der Schließanlage erhalten haben und tippen Sie auf **Registrieren**.
- > Wenn Sie für die AirKey-App eine PIN aktiviert haben, müssen Sie diese eingeben und bestätigen.

Das Smartphone ist damit in der weiteren AirKey-Schließanlage registriert.



Sofern der Registrierungscode für eine weitere Schließanlage über SMS gesendet wurde, ist es ausreichend, auf den Link der SMS zu tippen, um die Registrierung automatisch zu starten und durchzuführen.



Durch Wischbewegungen am Smartphone können Sie zwischen den Berechtigungsübersichten der einzelnen Schließanlagen oder der Gesamtberechtigungsübersicht wählen.



EVVA empfiehlt die Vergabe einer PIN. Diese wird als zusätzliche Sicherheitsstufe verwendet und kann nachträglich aktiviert bzw. deaktiviert werden. Nähere Informationen dazu finden Sie im Kapitel [PIN aktivieren](#).



Der Button **QR-Code scannen** wird nur in Verbindung mit einem Smartphonetausch benötigt. Details zum Smartphonetausch finden Sie im Kapitel [Smartphonetausch](#).

12 AirKey Cloud Interface (API)

Beim AirKey Cloud Interface handelt es sich um eine Schnittstelle ([API](#)) für Drittsysteme auf Basis von [REST](#). Die Schnittstelle erlaubt es, bestimmte Funktionen von AirKey über eine Drittsoftware (z.B.: ein Buchungssystem oder einen Check-In) zu steuern.

Die Drittsoftware muss dazu mit der AirKey-Onlineverwaltung verbunden und speziell angepasst werden, damit diese die notwendigen Befehle senden und die darauffolgenden Antworten verarbeiten kann.

Den Umfang der möglichen Funktionen und deren entsprechenden Befehle finden Sie in der [API-Dokumentation](#) (in Englisch). Ihr Integrator bzw. der Programmierer der Drittsoftware sorgt für die Implementierung.



Probieren Sie die Funktion des AirKey Cloud Interface exemplarisch anhand der [EVVA AirKey Cloud Interface Demo](#) aus.



Achten Sie auf ausreichend Guthaben bei der Verwendung des AirKey Cloud Interface. Verwenden Sie in diesem Fall am besten KeyCredits Unlimited. Sollte das Guthaben aufgebraucht sein bzw. kurz davorstehen, so werden alle Administratoren der AirKey-Schließanlage mit einer E-Mail-Benachrichtigung darüber informiert. Diese E-Mail-Benachrichtigung wird nur an Administratoren gesendet, die die Option ***Ich möchte wichtige Hinweise von EVVA (z. B. über geringes KeyCredits-Guthaben) per E-Mail erhalten (empfohlen)*** aktiviert haben. Diese E-Mail-Benachrichtigung können Sie jederzeit für einen [Administrator bearbeiten](#).

12.1 Aktivierung des AirKey Cloud Interface



Zur Aktivierung des AirKey Cloud Interface sind mindestens 350 KeyCredits erforderlich. Nutzen Sie dazu Ihr bestehendes Mengenguthaben von KeyCredits oder verwenden Sie die entsprechende Rubbelkarte **KeyCredits AirKey Cloud Interface**.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein** auf **API aktivieren**.

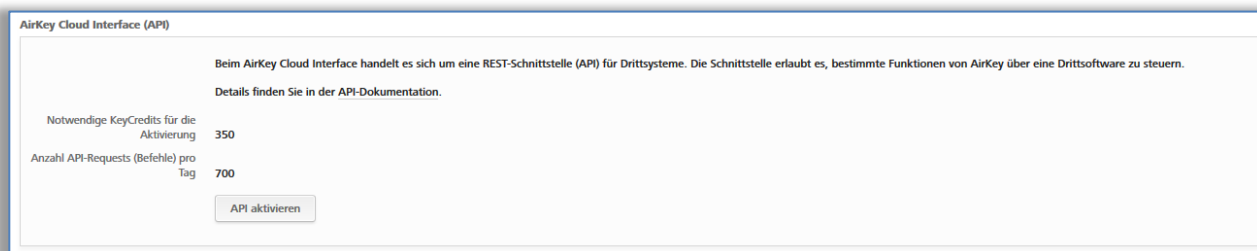


Abbildung 320: Allgemeine Einstellungen – AirKey Cloud Interface (API)

- > Sofern ausreichend Mengenguthaben vorhanden ist, bestätigen Sie den Dialog erneut mit **API aktivieren**. Sollte das Guthaben nicht ausreichend sein, so wird das mit

einer Hinweismeldung angezeigt. Es besteht dann die Möglichkeit, direkt über einen Link, das Guthaben aufzuladen.



Abbildung 321: API aktivieren

Damit ist das AirKey Cloud Interface aktiviert. Das AirKey Cloud Interface muss nur einmalig pro Schließanlage aktiviert werden, um es verwenden zu können.

Nach der Aktivierung erhalten Sie Informationen zum Endpoint (dort müssen die API-Befehle hingesendet werden) und zum API-Request-Limit (Anzahl der möglichen API-Requests pro Tag). Als API-Request wird ein Befehl gezählt, der über die Drittsoftware an das AirKey-System gesendet wird.



Das API-Request-Limit wird täglich um 00:00 Uhr UTC zurückgesetzt. Sollte das API-Request-Limit überschritten werden, so werden alle Administratoren der AirKey-Schließanlage mit einer E-Mail-Benachrichtigung darüber informiert. Diese E-Mail-Benachrichtigung wird nur an Administratoren gesendet, die die Option ***Ich möchte wichtige Hinweise von EVVA (z. B. über geringes KeyCredits-Guthaben) per E-Mail erhalten (empfohlen)*** aktiviert haben. Diese E-Mail-Benachrichtigung können Sie jederzeit für einen [Administrator bearbeiten](#).



Sollten die API-Requests pro Tag für Ihren Anwendungsfall nicht ausreichend sein, wenden Sie sich bitte an den [EVVA-Support](#).

12.2 API-Key generieren

Die Kommunikation zwischen AirKey und der Drittsoftware ist mit einem API-Key gesichert. Nur wer diesen API-Key kennt, kann Befehle über das AirKey Cloud Interface an Ihre Schließanlage senden. Jede Schließanlage mit aktiviertem AirKey Cloud Interface verwendet seine eigenen API-Keys.

Aktionen, die über das AirKey Cloud Interface durchgeführt werden, werden ebenfalls im Systemprotokoll der AirKey-Schließanlage protokolliert. Als Administrator wird in diesem Fall der erste Teil des API-Keys, die API-Key-ID verwendet.

Nach der Aktivierung können Sie die für die Kommunikation notwendigen API-Keys generieren.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein** auf **API-Key generieren**.

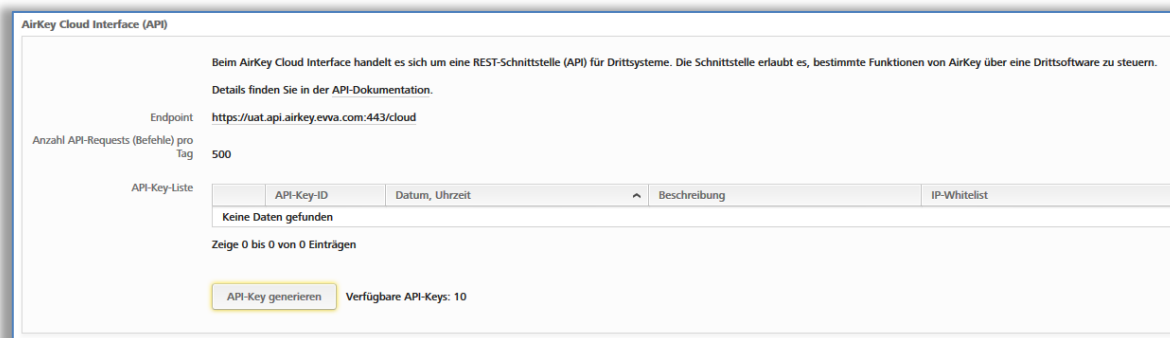


Abbildung 322: API-Key generieren

- > Bestätigen Sie den Dialog erneut mit **API-Key generieren**.

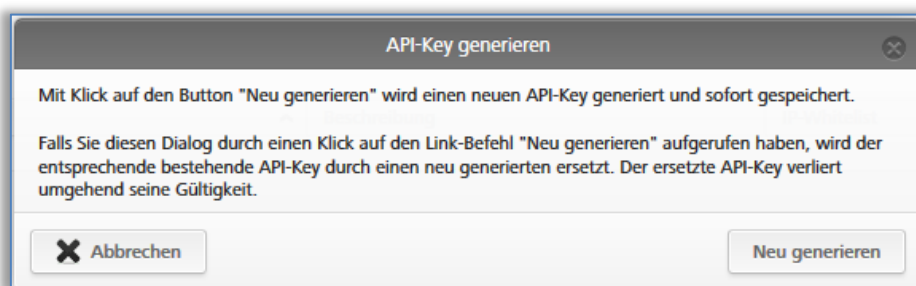


Abbildung 323: Dialog "API-Key generieren"

- > Vergeben Sie eine Beschreibung, zum Beispiel den Namen der Drittsoftware und schränken Sie optional die zum Versand von API-Requests zulässigen IP-Adressen über die IP-Whitelist ein.

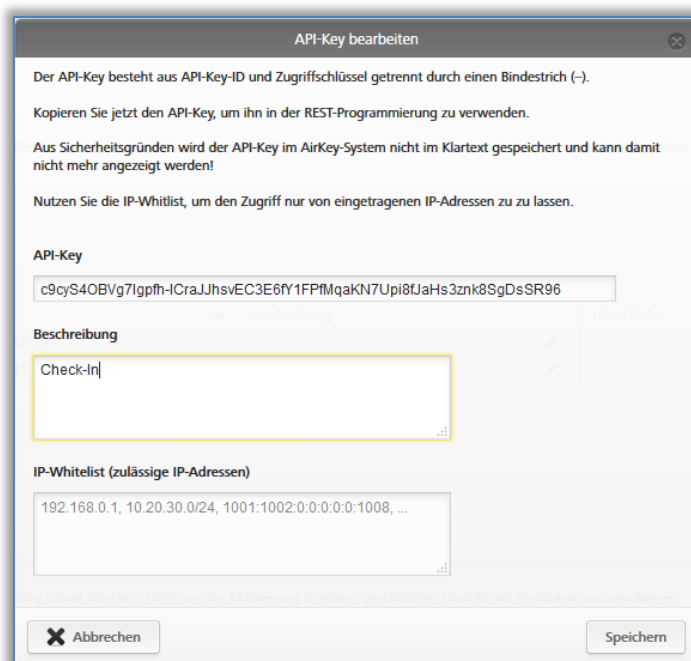


Abbildung 324: API-Key generieren – Details



Nutzen Sie die Funktion der IP-Whitelist, um die Sicherheit zu erhöhen. Tragen Sie nur jene IP-Adressen zum jeweiligen API-Key ein, die API-Requests an Ihre AirKey-Schließanlage versenden dürfen.

In der IP-Whitelist sind sowohl IP-Adressen im Format IPv4 als auch IPv6 erlaubt. Verwenden Sie als Trennzeichen zwischen mehreren IP-Adressen den Beistrich (,).



Der API-Key wird aus Sicherheitsgründen nur einmal vollständig angezeigt. Speichern Sie diesen an einem sicheren Ort ab, bzw. verwenden Sie diesen in Ihrer Drittsoftware.

- > Speichern Sie die Eingaben zum API-Key mit Klick auf **Speichern**.



Pro AirKey-Schließanlage können bis zu 10 API-Keys generiert werden. Somit kann auch mehr als eine Drittsoftware die AirKey-Schließanlage steuern.

Der generierte API-Key wird in den allgemeinen Einstellungen gelistet und kann dort auch nachträglich bearbeitet werden.

12.3 API-Key bearbeiten

Die Beschreibung und die IP-Whitelist von bestehenden API-Keys können nachträglich in den **Einstellungen** im Tab **Allgemein** über das Bleistift-Symbol bearbeitet werden. Zusätzlich stehen für die einzelnen API-Keys die Funktionen **Neu generieren**, **Löschen** und **Deaktivieren** bzw. **Reaktivieren** zur Verfügung.

API-Key-ID	Datum, Uhrzeit	Beschreibung	IP-Whitelist			
gpOkxk3G8V48BV4f	25.04.2019 13:53:22			Neu generieren	Löschen	Deaktivieren
c9cy540BVg7lppfh	25.04.2019 14:47:46	Check-In		Neu generieren	Löschen	Deaktivieren

Zeige 1 bis 2 von 2 Einträgen

Abbildung 325: API-Key bearbeiten

12.3.1 API-Key neu generieren

Hierbei wird ein bestehender API-Key durch einen neuen API-Key ersetzt. Der ersetzte API-Key ist dadurch nicht mehr gültig.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein**, in der Liste der API-Keys, auf **Neu generieren** 1.
- > Alle weiterführenden Schritte sind identisch zu [API-Key generieren](#).

12.3.2 API-Key löschen

Hierbei wird ein bestehender API-Key gelöscht. Dieser wird aus der Liste der API-Keys entfernt und ist somit auch nicht mehr gültig. Das Löschen von API-Keys erhöht die Anzahl der verfügbaren API-Keys entsprechend.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein**, in der Liste der API-Keys, auf **Löschen** ②.
- > Bestätigen Sie den Dialog mit **Löschen**, um den API-Key endgültig zu löschen.

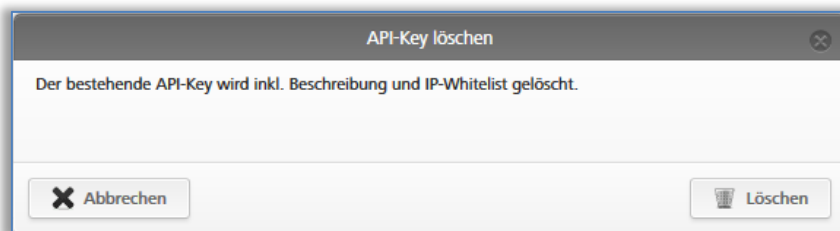


Abbildung 326: API-Key löschen

12.3.3 API-Key de- und aktivieren

Hierbei wird ein bestehender aktiver API-Key deaktiviert, bzw. ein deaktivierter API-Key wieder aktiviert. Ein deaktivierter API-Key ist ungültig und es können keine API-Requests an die AirKey-Schließenanlage gesendet werden. Der API-Key sowie dessen Beschreibung und IP-Whitelist ändern sich durch das De- und Aktivieren nicht.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein**, in der Liste der API-Keys, auf **Deaktivieren** ③ bzw. **Aktivieren**.
- > Bestätigen Sie den Dialog mit **Deaktivieren** bzw. **Aktivieren**, um den Vorgang abzuschließen.

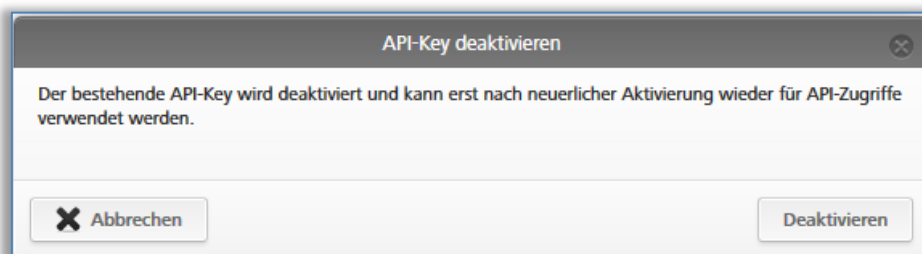


Abbildung 327: API-Key deaktivieren

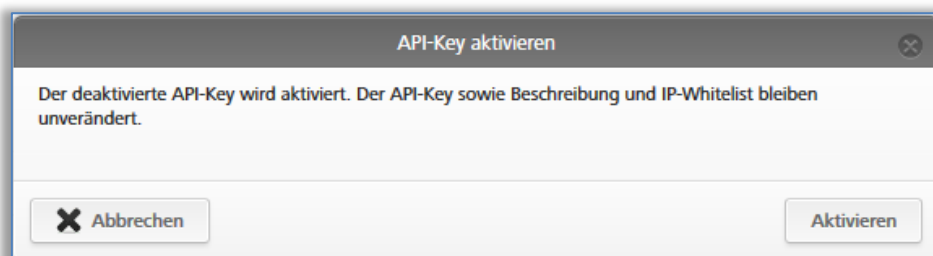


Abbildung 328: API-Key aktivieren

12.4 AirKey Cloud Interface – Testumgebung

Die Testumgebung gibt Ihnen die Möglichkeit, das AirKey Cloud Interface (API) vor der Aktivierung in einem geschützten Umfeld mit Testdaten auszuprobieren.

Das dient vor allem der Unterstützung für Integratoren oder Programmierern von Drittsystemen während der Integration für das AirKey Cloud Interface. Die Testumgebung ist auch verfügbar, wenn das AirKey Cloud Interface noch nicht aktiviert wurde.



In der Testumgebung werden keine KeyCredits abgebucht. Zusätzlich werden über die Testumgebung auch keine SMS gesendet.



Die Testumgebung der AirKey Cloud Interface (API) ist über einen eigenen "Endpoint" (dort müssen die API-Befehle hingesendet werden) erreichbar.
Endpoint: <https://integration.api.airkey.evva.com:443/cloud>

12.4.1 Testdaten generieren

Für die erste Verwendung der Testumgebung ist es notwendig, zuerst die Testdaten zu generieren.



Um die Testdaten zu generieren, muss vorab ein API-Key generiert werden.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein** auf **Testdaten generieren**.

Abbildung 329: Testdaten generieren

Damit wurden die Testdaten generiert. Mit den Testdaten ist es möglich, jeden API-Request aus der [API-Dokumentation](#) auszuprobieren. Die Testdaten müssen nur einmalig generiert werden.

12.4.2 API-Key generieren

Auch für die Kommunikation mit der der Testumgebung der AirKey Cloud Interface (API) ist ein API-Key notwendig. Ohne diesen API-Key können keine API-Requests an die Testumgebung gesendet werden. Im Vergleich zum richtigen AirKey Cloud Interface wird der API-Key der Testumgebung in Klartext angezeigt.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein** im Bereich **AirKey Cloud Interface (API) – Testumgebung** auf **API-Key generieren**.

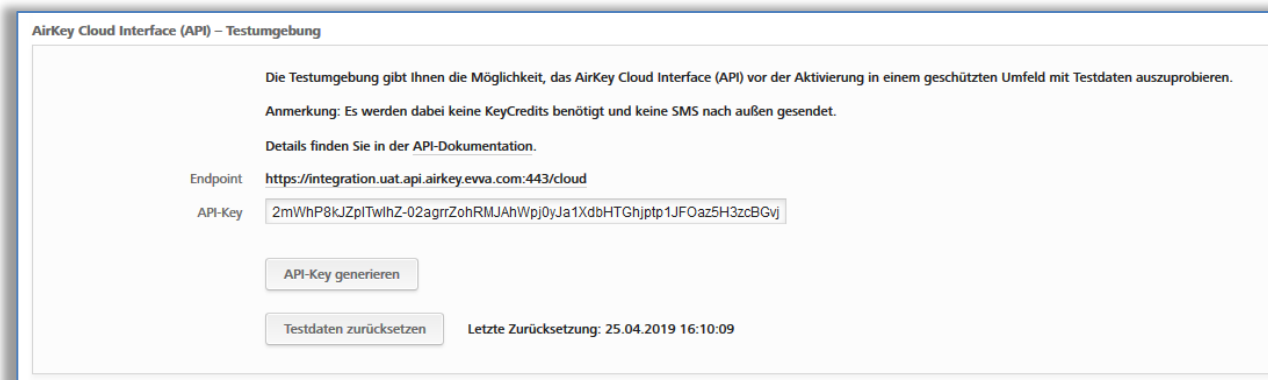


Abbildung 330: API-Key für die Testumgebung generieren



Durch erneutes Klicken auf **API-Key generieren**, wird der bestehende API-Key durch einen neuen ersetzt. Der ersetzte API-Key kann dann nicht mehr verwendet werden.



Nach jedem Login muss erneut ein API-Key generiert werden.

12.4.3 Testdaten zurücksetzen

Die Testdaten der Testumgebung der AirKey Cloud Interface können mit einem Klick wieder in den Ursprungszustand zurückgesetzt werden. Somit können alle Tests mit einheitlichen Testdaten durchgeführt werden.

- > Klicken Sie in den **Einstellungen** im Tab **Allgemein** im Bereich **AirKey Cloud Interface (API) – Testumgebung** auf **Testdaten zurücksetzen**.

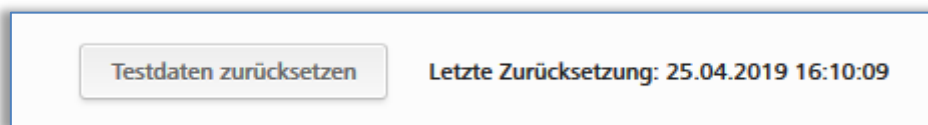


Abbildung 331: Testdaten der Testumgebung zurücksetzen

Das Zurücksetzen der Testdaten wird mit einer Erfolgsmeldung bestätigt. Der Zeitpunkt der letzten Zurücksetzung wird im Abschnitt **AirKey Cloud Interface (API) – Testumgebung** angezeigt.

13 Signalisierung der Schließkomponenten

Die Schließkomponenten zeigen Ereignisse durch verschiedene optische und akustische Signale an.

Signal-nummer	Ereignis	Optisches Signal ^{*)}	Akustisches Signal ^{*)}	Hinweis
Signal 1	Sperrvorgang mit berechtigtem Medium	●●●●●	mmmmm	
Signal 2	Ende Freigabedauer	●●●●●	ttttt	
Signal 3	Sperrvorgang mit nicht berechtigtem Medium	●●-●●-●●-●●	hh-hh-hh-hh	
Signal 7	"Batterie leer"-Warnung (Wird in der AirKey-Onlineverwaltung in der Tabelle der Schließkomponenten und in den Details einer Schließkomponente mit dem Symbol "Batterie leer" angezeigt.)	●●-●●-●●-●●	h----h----h----h -h	Das Signal wird beim Einlegen von leeren Batterien anstatt Signal 8 und beim Sperrvorgang vor Signal 1 angezeigt. 1000 Sperrvorgänge bzw. zwei Wochen Standby-Betrieb sind nach der ersten Signalisierung möglich (bei Raumtemperatur und Verwendung einer Karte, Schlüsselanhängers, Kombischlüssels oder Armband).
Signal 8	Neue Batterien einlegen bzw. Neustart der Komponente	●●-●●-●●-●●	tt--mm--hh	
Signal 9	Medium ohne EVVA-Segmentierung; schließanlagenfremdes Medium	●●●	Keines	Wird nicht mehr verwendet. Für diesen Zweck wird nur Signal 3 verwendet.

Signal-nummer	Ereignis	Optisches Signal*)	Akustisches Signal*)	Hinweis
Signal 10	Kommunikations- bzw. Hardwarefehler einer Schließkomponente		mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm	Wird z.B. bei fehlerhafter Verbindung zwischen Knauf und Elektronikmodul eines Zylinders signalisiert.
Signal 11	Firmware-Update einer Schließkomponente	 (1 s Periode, 12 ms Puls)	Keines	Dauer: bis die Kommunikation abgeschlossen ist
Signal 12	Aktualisierung einer Schließkomponente / eines Mediums erfolgreich		hhhhh	
Signal 13	Aktualisierung einer Schließkomponente / eines Mediums nicht erfolgreich		ttttt	
Signal 14	Lesevorgang eines AirKey-Mediums	 (100 ms Periode, 10 ms Puls)	Keines	
Signal 15	Aufwachen und Bluetooth-Verfügbarkeit eines AirKey-Zylinders (z.B. durch Berührung)	 (1,5 s Periode)	Keines	
Signal 16	Start Daueröffnung		mmm---hhh	
Signal 17	Ende Daueröffnung		hhh---mmm	
Signal 18	Batterie-Notfallmodus eines AirKey-Zylinders		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 tt--mm--hh h---h---h---h	Ursache: Eine der Batterien wurde falsch eingelegt oder ist leer.

*) Erläuterungen zu den Signalen:

Optische Signale: gelb ●, rot ●, grün ●, blau ●

Akustische Signale: h = hoher Ton, m = mittlerer Ton, t = tiefer Ton

Jedes Signal entspricht einer Dauer von 50 ms, Pausen werden mit "-" gekennzeichnet.

14 Werte und Limits von AirKey

In diesem Kapitel werden die maximalen Konfigurationen pro Medium und Schließkomponente zusammengefasst.

14.1 AirKey-Onlineverwaltung

Die Anzahl der maximal möglichen Schließkomponenten, Bereiche, Personen und Medien ist unbegrenzt.

14.2 AirKey-Schließkomponenten

- Die letzten 1000 Protokolleinträge werden ohne Aktualisierung gespeichert.
- Maximal 1000 Blacklist-Einträge können verwaltet werden.
- Maximal 96 Bereichszuordnungen sind möglich.
- Maximal 250 Freigaben zu weiteren Mandanten können vergeben werden.

14.3 Karten, Schlüsselanhänger, Kombischlüssel oder Armbänder

- Maximal 256 Protokolleinträge werden ohne Aktualisierung gespeichert.
- Maximal 150 Berechtigungen zu einzelnen Türen können vergeben werden.
- Maximal 100 Berechtigungen zu Bereichen können vergeben werden.
(Werden 12 individuelle Berechtigungen mit jeweils 8 möglichen Zutritten vergeben, so können insgesamt nur 96 Berechtigungen zu Bereichen vergeben werden.)

14.4 AirKey-App

- Maximal 256 Protokolleinträge werden ohne Aktualisierung gespeichert.
- Unbegrenzte Anzahl an Berechtigungen zu einzelnen Türen und Bereichen.

15 Wann werden KeyCredits abgebucht?

Für den laufenden Betrieb einer AirKey-Schließanlage sind zur Vergabe bzw. Änderung von Zutrittsberechtigungen KeyCredits erforderlich.

KeyCredits werden nur im Falle eines Mengenguthabens abgebucht. Sobald ein gültiges Zeitguthaben vorhanden ist, wird auf das Zeitguthaben zurückgegriffen und das Mengenguthaben bleibt unberührt.

Bei folgenden Aktionen werden KeyCredits abgebucht:

- Beim Vergeben von neuen Berechtigungen und anschließendem Anfertigen
- Beim Ändern von bestehenden Berechtigungen und anschließendem Anfertigen
- Beim Reaktivieren von deaktivierten Medien, sofern die Berechtigungen des deaktivierten Mediums beibehalten werden
- Beim Smartphonetausch, wenn Berechtigungen an das neue Smartphone übertragen werden
- Beim Aktivieren des [AirKey Cloud Interface \(API\)](#)

Die KeyCredits werden im Falle von neuen Berechtigungen oder Berechtigungsänderungen erst abgebucht, wenn das Medium angefertigt wird. Dabei wird pro Anfertigung ein KeyCredit abgezogen. Es können auch mehrere Berechtigungen auf einmal vergeben oder geändert werden – dafür wird nur ein KeyCredit abgebucht.

Für das Löschen von Berechtigungen, das Deaktivieren oder Leeren von Medien werden keine KeyCredits abgebucht.

16 Fehlerbehebungen

Mit AirKey haben Sie sich für ein hochwertiges und ausführlich getestetes elektronisches Schließsystem entschieden. Sollten Sie trotzdem mit einem Fehler oder einem Problem konfrontiert sein, finden Sie in diesem Kapitel Tipps & Tricks, um die Fehler zu beheben.

16.1 Keine Kommunikation innerhalb des Systems möglich

Wenn Sie das Smartphone nicht registrieren oder die Schließkomponenten von AirKey nicht aktualisieren können, prüfen Sie bitte folgende Schritte:

- > Achten Sie darauf, dass am Smartphone eine Internetverbindung besteht (WLAN oder mobile Daten) und aktivieren Sie diese gegebenenfalls.

16.2 Schließkomponente erkennt Medien nur schlecht oder überhaupt nicht

Wenn an einer Schließkomponente, verglichen mit anderen Schließkomponenten, die Medien nur schlecht oder überhaupt nicht erkannt werden, prüfen Sie bitte folgende Schritte:

- > Achten Sie darauf, dass das Medium bei der Identifikation an der Leseinheit ruhig angehalten wird und warten Sie, bis die Schließkomponente grün signalisiert. (Die blaue Signalisierung deutet nur auf die Kommunikation zwischen Smartphone und Schließkomponente hin.)
- > Sofern die Schließkomponente nicht reagiert, achten Sie auf die richtige Lage des Mediums. Der Kombischlüssel muss zum Beispiel mit der Seite angehalten werden, auf der das RFID-Symbol ersichtlich ist.
- > Sollte auch das nicht den gewünschten Erfolg bringen, warten Sie 50 Sekunden ohne einer Identifikation an der Leseinheit, damit die Schließkomponente das elektrische Feld neu kalibrieren kann. Durch das Anhalten eines metallischen Gegenstandes an die Leseinheit können Sie die Re-Kalibrierung auch manuell durchführen.

16.3 Medien werden nicht mehr erkannt

Wenn ein bestimmtes Medium an den Schließkomponenten nicht mehr erkannt wird, prüfen Sie bitte folgende Schritte:

- > Wenn es sich um ein Smartphone handelt, achten Sie darauf, dass NFC oder Bluetooth aktiviert ist. Starten Sie gegebenenfalls die NFC- bzw. Bluetooth-Verbindung erneut und achten Sie darauf, das Smartphone lagerichtig an die Leseinheit anzuhalten. Achten Sie darauf, dass es hier – abhängig vom Typ des Smartphones – Unterschiede geben kann.
- > Sofern die Leseinheit der Schließkomponente oder der Codierstation überhaupt nicht mehr auf das Medium reagiert, halten Sie das Medium für eine Dauer von ungefähr 10 Sekunden an die Leseinheit einer Schließkomponente oder einer Codierstation. Das Medium repariert sich dadurch selbst. Man erkennt den abgeschlossenen Vorgang, wenn die Schließkomponente oder die Codierstation wieder wie gewohnt signalisieren.

16.4 Knauf eines AirKey-Zylinders lässt sich nicht abschrauben

Sollte das Abschrauben des Knaufs eines AirKey-Zylinders nicht mehr möglich sein, so können folgende Maßnahmen eine Abhilfe schaffen:

- > Achten Sie darauf, dass bei der Demontage des Knaufs das Montagewerkzeug für den AirKey-Zylinder verwendet wird.
- > AirKey-Zylinder in Europrofilausführung besitzen an der Stirnseite des Elektronikmoduls eine Servicebohrung, über die die Knaufachse mit einem passenden Metallstift fixiert werden kann. Wir empfehlen hier das Montagewerkzeug Set 2.

Vorgehensweise:

- > Führen Sie den Metallstift aus dem Montagewerkzeug Set 2 in die stirnseitige Servicebohrung Ihres Europrofilzylinders ein.
- > Drehen Sie dabei den Knauf so lange um die eigene Achse, bis sich der Metallstift merklich tiefer in die Servicebohrung einführen lässt. Halten Sie nun den Metallstift in dieser Position und demontieren Sie den Knauf mit dem Montagewerkzeug wie gewohnt.
- > Entfernen Sie den Metallstift nach der Demontage des Knaufs.
- > Wenn Sie keinen AirKey-Zylinder im Europrofil besitzen oder der AirKey-Zylinder in einem Beschlag oder einer Rosette mit Kernziehschutz eingebaut ist, halten Sie ein berechtigtes Medium an die Leseinheit, sodass der Zylinder einkuppelt. Bringen Sie innerhalb der Freigabedauer (während der Zylinder eingekuppelt ist) das Montagewerkzeug am Zylinder an. Der Zylinder kuppelt in diesem Fall nicht mehr aus und der Knauf kann einfacher abgeschraubt werden.

16.5 Die Schließkomponente signalisiert einen "Hardwarefehler"

Wenn die AirKey-Schließkomponente einen Hardwarefehler signalisiert (siehe Kapitel [Signalisierung der Schließkomponenten](#)), so ist es möglich, dass der Knauf / die Leseinheit nicht mit dem zugehörigen Elektronikmodul / der zugehörigen Steuereinheit verbunden ist.

Überprüfen Sie die Kontakte, Stecker und Verbindungen gemäß der Montageanleitung.

16.5.1 AirKey-Zylinder

- > Achten Sie darauf, dass der Dichtring auf der Achse des Zylinders korrekt aufgesetzt ist, und schrauben Sie den Knauf durch Drehung im Uhrzeigersinn wieder auf den Zylinder, bis Sie einen Widerstand spüren.
- > Entfernen Sie das Montagewerkzeug.
- > Drehen Sie den Knauf anschließend gegen den Uhrzeigersinn, bis Sie ein Einrasten verspüren.
- > Achten Sie darauf, dass der Knauf und das Elektronikmodul ordnungsgemäß eingearastet sind.

16.5.2 AirKey-Wandleser

- > Achten Sie darauf, dass die Leseinheit und die Steuereinheit des AirKey-Wandlers ordnungsgemäß verbunden sind. Überprüfen Sie gegebenenfalls die Verkabelung und die Steckverbindungen.

16.6 Der elektronische Knauf ist schwergängig

In Abhängigkeit vom Überstand des Zylinders über einen Beschlag bzw. eine Zylinderrosette kann der Zylinder unter Umständen durch Reibung der Dichtung zwischen Zylindergehäuse und elektronischem Knauf schwergängiger sein. Im Innenbereich besteht in diesen Fällen die Möglichkeit, die Dichtung abzunehmen.

Sollten Sie dennoch Unterstützung benötigen, wenden Sie sich bitte an Ihren EVVA-Partner bzw. an den [EVVA-Support](#).

17 Wichtige Hinweise

17.1 System



Es wird ausdrücklich darauf aufmerksam gemacht, dass das vorliegende AirKey-System nach gesetzlichen Bestimmungen, insbesondere des Datenschutzgesetzes, melde-/genehmigungspflichtig sein kann. Die EVVA Sicherheitstechnologie GmbH übernimmt dementsprechend keinerlei Haftung und Gewähr für einen rechtskonformen Betrieb.



Für die Kommunikation im AirKey-System wird der Internet-Port 443 verwendet. Achten Sie darauf, dass dieser Port nicht gesperrt ist. Bei der Verwendung des mobilen Datennetzes ist der Mobilfunkbetreiber für die Verwaltung der Ports verantwortlich. Sollten Sie ein Problem bei der Verwendung des mobilen Datennetzes in Verbindung mit AirKey haben, wenden Sie sich an Ihren Mobilfunkanbieter.



Stellen Sie Berechtigungen mit möglichst kurzen Laufzeiten aus, um die Systemsicherheit hoch zu halten und bei einem Medienverlust die Einträge in der Blacklist gering zu halten. Medien mit unbegrenzten Berechtigungen ohne Ablaufdatum sollen nur im Falle von Notmedien (z.B. Feuerwehrschlüssel) angefertigt werden.



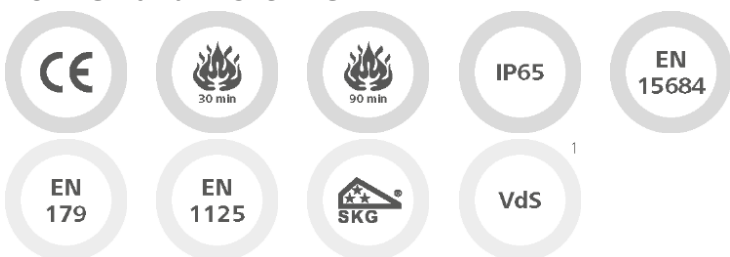
Arbeiten Sie stets mit aktueller Konfiguration des Gesamtsystems, um die Systemsicherheit hoch zu halten.

Sicherheitshinweise zu den einzelnen Systemen finden Sie unter den folgenden Links:

Zylinder, Hängeschloss: [PDF](#)

Wandleser, Steuereinheit: [PDF](#)

Normen und Richtlinien



CE-geprüft | EN 1634: 30 Minuten | EN 1634: 90 Minuten | Schutzart IP65 | EN 15684 | geeignet für Schlösser nach EN 179/1125 (bei Einsatz der Anti-Panik-Funktion FAP)

SKG | VdS¹

¹ In Vorbereitung

18 Technische Details zur RS485-Schnittstelle bei Bluetooth-Wandlern

Nach einem erfolgreichen Zutritt an einem Bluetooth-Wandler wird eine APDU mit dem Protokolleintrag dieses Zutritts vom Wandler über die RS485-Schnittstelle gesendet.

Der Protokolleintrag enthält neben anderen Parametern die 5-Byte lockingSystemId des Mediums (Zutrittsmedium oder Smartphone), das den Wandler erfolgreich entsperrt hat.

Diese lockingSystemId (int64) kann dann über das AirKey Cloud Interface (API) abgefragt werden. Beispiel: `GET/v1/media?lockingSystemId=000102030405`

Mit diesen Informationen lassen sich verschiedene Anwendungsfälle realisieren, wie z.B.:

- Anzeige des Namens der Person, die den Wandler gerade entsperrt hat.
- Auslesen von zusätzlichen Parametern, z.B. aus dem "Kommentar"-Feld dieses Mediums und Verwendung dieser Informationen für Drittsysteme.
- Aufzugskontrolle: Geben Sie z.B. einen minimalen JSON-String in das Kommentarfeld eines Zutrittsmediums oder Smartphones ein, um ein bestimmtes Stockwerk für dieses Medium anzugeben und verwenden Sie diese Information für die Aufzugsteuerung.

18.1 RS485-Schnittstelle für Bluetooth-Wandler aktivieren

Um den Protokolleintrag bei einem erfolgreichen Zutritt über die RS485-Schnittstelle weiterzuleiten, muss die entsprechende Einstellung am Bluetooth-Wandler in der AirKey-Onlineverwaltung aktiviert werden.

- > Wählen Sie auf der Startseite **Home** die Kachel **Wandler**.
- > Alternativ wählen Sie im Hauptmenü **Schließanlage** → **Schließkomponenten**.
- > Klicken Sie auf den Bluetooth-Wandler, bei dem Sie die Funktion aktivieren wollen.
- > Wechseln Sie in den Reiter **Einstellungen**.
- > Markieren Sie ganz unten die Checkbox **RS485-Schnittstelle**.



Der Bluetooth-Wandler benötigt die Firmware-Version 5.86 oder höher, sonst wird ein Hinweis angezeigt, dass die Firmware aktualisiert werden muss, um diese Funktion nutzen zu können.

18.2 RS485-Konfiguration der seriellen Schnittstelle

Mit einem RS485-Adapter, der an der RS485-Schnittstelle des AirKey-Wandlers angeschlossen ist, kann der Protokolleintrag des letzten erfolgreichen Zutritts an ein Drittsystem weitergeleitet werden (z.B. über USB oder Ethernet).

Der RS485-Adapter wird dabei an der Steuereinheit am Stecker für die Leseinheit zusätzlich zum bestehenden Kabel parallel angeschlossen.

- Pin 2 des Steckers → Doorbus B-
- Pin 3 des Steckers → Doorbus A+



Weitere Informationen zur Steckerbelegung findet man auf dem Deckelplan der Steuereinheit.

Die serielle Schnittstelle muss wie folgt konfiguriert sein:

- Baudrate: 115200
- Data-Bit: 8
- Stop-Bit: 1
- Parität: even
- No CTS flow control

18.3 APDU-Spezifikation des Protokolleintrags des erfolgreichen Zutritts

18.3.1 APDU des Protokolleintrags

APDU Bytes	CLA	INS	P1	P2	LE (data length)	data
Byte	0xCC	0xD6	0xF0	0x00	0x0E	<14 Byte Protokolleintrag>
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-Protokolleintrag

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																R7																	
0	0	1	1	0	0	1	0	0	1	1	1	0	1	1	0	1	1	0	1	0	0	0	1	1	1	0	1	1	1	0	0	1	

- R1** ... Jahr: Jahr minus 2010 (Jahr 2022 = **001100**)
R2 ... Monat: Jan = **01**, Feb = **02**, März = **03** etc.
R3 ... Tag: Wertebereich **01-31**
R4 ... Stunde: Wertebereich **00-23**
R5 ... Minuten: Wertebereich **00-59**
R6 ... Sekunden: Wertebereich **00-59**
R7 ... Beispiel: **00110010 01110110 11010011 10111001** entspricht zu 2022-09-27 13:14:57

18.3.2.2 Unlocking-Status

Byte 1								Description
b8	b7	b6	b5	b4	b3	b2	b1	
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** ... Uhrzeit ist aktuell
R2 ... Uhrzeit ist nicht aktuell. Stromversorgung war zu lange nicht verfügbar.
R3 ... Verweigerter Zutritt: Derzeit nicht berechtigt
R4 ... Verweigerter Zutritt: Medium befindet sich auf der Blacklist der Schließkomponente
R5 ... Verweigerter Zutritt: Uhrzeit nicht aktuell
R6 ... Verweigerter Zutritt: Signaturfehler
R7 ... Verweigerter Zutritt: Freigabe nicht aktuell (Freigabe in eine andere Schließanlage)
R8 ... Verweigerter Zutritt: Feiertag ist aktiv
R9 ... Zutritt erteilt: Zutritt via Hands-free
R10 ... Zutritt erteilt
R11 ... Batteriestatus: Für Bluetooth-Wandler immer 100 %
R12 ... Beispiel: **0x7a** bedeutet Uhrzeit aktuell, Zutritt erteilt, Batteriestatus 100 %

18.3.3 Beispiel

- APDU: **CC D6 F0 00 0E 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c**
- Protokolleintrag: **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** = Uhrzeit aktuell, Zutritt erteilt, Batteriestatus 100 %
 - customerId: **00 00 02 8c**



Man kann die lockingSystemId von Zutrittsmedien auch über die Codierstation an Drittsysteme weiterleiten. Nutzen Sie dazu den Parameter "-notify" beim Start der Codierstation über die Kommandozeile. Details dazu finden Sie im Kapitel [Codierstation über die Kommandozeile verwenden](#).

19 Konformitätserklärung

EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59-65 | A-1120 Wien | www.evva.com
+43 1 811 65-0 | +43 1 812 20 71 | office-wien@evva.com



EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59-65 | A-1120 Wien

EU - KONFORMITÄTSEKTLÄRUNG

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



Raiffeisen Bank International AG
IBAN: AT82310000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT76120000616194700
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



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
 +43 1 811 65-0 | +43 1 812 20 71 | 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



Raffaelsen Bank International AG
 IBAN: AT823100000600669705
 BIC: RZBAATWW

Bank Austria
 IBAN: AT761200000616194700
 BIC: BKAUATWW

GF. Mag. Stefan Ehrlich-Adam
 UID-Nr. ATU 65126268 | FN 120755 g, HG Wien | DVR. 0131504
 ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5



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 Abbildungsverzeichnis

Abbildung 1: Systemarchitektur-----	12
Abbildung 2: Systemüberblick – lückenlose Sicherheit -----	12
Abbildung 3: Link "AirKey-Registrierung" -----	21
Abbildung 4: Registrierung bei AirKey -----	21
Abbildung 5: Registrierung abschließen-----	22
Abbildung 6: E-Mail "EVVA-AirKey-Registrierung"-----	22
Abbildung 7: Eigenes AirKey-Passwort festlegen, um die Registrierung abzuschließen -----	23
Abbildung 8: Startseite der AirKey-Schließenanlage-----	24
Abbildung 9: Interaktive Hilfe -----	24
Abbildung 10: Interaktive Hilfe – Guthaben aufladen -----	25
Abbildung 11: Codierstation – Installation der Applikation -----	26
Abbildung 12: Codierstation-Applikation installieren und starten -----	26
Abbildung 13: Öffnen der AirKey.jnlp-Datei -----	27
Abbildung 14: Verbindung zur Codierstation aufbauen -----	27
Abbildung 15: Auswahl der Codierstation-----	27
Abbildung 16: AirKey-Icon in der Taskleiste-----	27
Abbildung 17: Download der Codierstation-Applikation -----	28
Abbildung 18: Codierstation-Applikation über die Kommandozeile starten -----	29
Abbildung 19: Einstellungen der Codierstation-Applikation -----	29
Abbildung 20: Kartenleser "Microsoft UICC" in der AirKey-Onlineverwaltung -----	31
Abbildung 21: Editor für lokale Gruppenrichtlinien-----	32
Abbildung 22: Smartcard-Plug & Play-Dienst-----	32
Abbildung 23: Guthaben -----	33
Abbildung 24: Guthaben aufladen-----	33
Abbildung 25: Guthabencode eingeben -----	34
Abbildung 26: Guthaben aufladen-----	34
Abbildung 27: Person anlegen-----	35
Abbildung 28: Medium zuweisen -----	36
Abbildung 29: Personenliste importieren -----	36
Abbildung 30: Personen importieren – Personenliste -----	37
Abbildung 31: Personen importieren – Feldaufteilung in der Personenliste -----	37
Abbildung 32: Excel – Speichern unter – "Unicode Text (*.txt)" -----	39
Abbildung 33: Excel – Speichern als "Unicode Text (*.txt)" bestätigen -----	40
Abbildung 34: Tabulator markieren und in die Zwischenablage kopieren -----	40
Abbildung 35: "Editor" – alle Tabulatoren durch Strichpunkte ersetzen -----	40
Abbildung 36: Dateiendung .csv manuell eintragen und UTF-8-Codierung auswählen -----	41
Abbildung 37: Personen importieren -----	41
Abbildung 38: Personen importieren -----	42
Abbildung 39: Personen importieren – Ergebnis -----	42
Abbildung 40: Neues Medium vom Typ Smartphone oder Karte -----	43
Abbildung 41: Neues Medium hinzufügen -----	43
Abbildung 42: Registrierungscode erstellen -----	44
Abbildung 43: Registrierungscode-----	44
Abbildung 44: Medium bearbeiten – Einstellungen-----	44
Abbildung 45: AirKey-App – Schließenanlage hinzufügen (iOS)-----	46
Abbildung 46: AirKey-App – Schließenanlage hinzufügen (Android)-----	46

Abbildung 47: "Send a Key" -----	48
Abbildung 48: "Send a Key" – Suchfeld-----	48
Abbildung 49: "Send a Key" – Person anlegen -----	48
Abbildung 50: SMS mit Link – hier gezeigt mit Samsung Galaxy S7 Edge-----	49
Abbildung 51: Registrierung erfolgreich -----	49
Abbildung 52: Telefonnummer eingeben (iOS)-----	50
Abbildung 53: Registrierungscode (iOS) -----	50
Abbildung 54: Zutrittsarten-----	51
Abbildung 55: AirKey-App – Mit Komponente verbinden (über NFC bei Android-Smartphone / über Bluetooth bei Android-Smartphone / über Bluetooth bei iPhone)-----	52
Abbildung 56: AirKey-App – Mit Komponente verbinden -----	53
Abbildung 57: AirKey-App – Verbindung wird aufgebaut -----	53
Abbildung 58: Komponente hinzufügen -----	53
Abbildung 59: AirKey-App – Schließkomponente hinzufügen (Android / iPhone)-----	54
Abbildung 60: AirKey-App – Schließkomponente hinzugefügt -----	54
Abbildung 61: GPS-Koordinaten in den Details der Schließkomponente -----	55
Abbildung 62: Schließkomponente hinzufügen -----	55
Abbildung 63: Schließkomponente hinzufügen / keine Codierstation -----	56
Abbildung 64: Schließkomponente hinzufügen – Namensgebung -----	56
Abbildung 65: Schließkomponente hinzufügen -----	56
Abbildung 66: Schließkomponente hinzufügen – Erfolgsmeldung -----	57
Abbildung 67: Schließkomponentendetails -----	57
Abbildung 68: Komponente zu meiner Schließanlage hinzufügen -----	58
Abbildung 69: AirKey-App – Mit Komponente verbinden -----	58
Abbildung 70: AirKey-App – Verbindung wird aufgebaut -----	59
Abbildung 71: Mediumdetails-----	59
Abbildung 72: Medium hinzufügen – Bezeichnung festlegen -----	59
Abbildung 73: Person zuweisen -----	60
Abbildung 74: Person zu Medium zuweisen-----	60
Abbildung 75: Person bestätigen -----	61
Abbildung 76: Berechtigung vergeben -----	62
Abbildung 77: Dauerzutrittsberechtigung vergeben -----	62
Abbildung 78: Dauerzutrittsberechtigung vergeben -----	63
Abbildung 79: Periodischen Zutritt vergeben -----	63
Abbildung 80: Periodischen Zutritt vergeben -----	64
Abbildung 81: Periodischen Zutritt hinzufügen -----	64
Abbildung 82: Temporäre Zutrittsberechtigung vergeben -----	65
Abbildung 83: Temporäre Zutrittsberechtigung vergeben -----	65
Abbildung 84: Individuelle Zutritte vergeben -----	65
Abbildung 85: Neue Berechtigung – Individueller Zutritt -----	66
Abbildung 86: Neue Berechtigung – Individueller Zutritt -----	66
Abbildung 87: Berechtigung anfertigen -----	67
Abbildung 88: Neue oder geänderte Berechtigung anfertigen -----	67
Abbildung 89: Fehlgeschlagene Login-Versuche-----	68
Abbildung 90: AirKey-Onlineverwaltung – Home-----	69
Abbildung 91: Verifizierung der Mobiltelefonnummer bei Login -----	69
Abbildung 92: SMS-Code bei Login -----	70
Abbildung 93: Login-Seite der AirKey-Onlineverwaltung-----	71

Abbildung 94: Passwort vergessen	71
Abbildung 95: SMS-Code bei "Passwort vergessen"	71
Abbildung 96: AirKey-Passwort zurücksetzen	72
Abbildung 97: Mein AirKey-Account	73
Abbildung 98: AirKey-Onlineverwaltung – Abmelden	73
Abbildung 99: Hauptmenü – Administratoren	74
Abbildung 100: Details eines Administrators	74
Abbildung 101: Kontaktinformationen	75
Abbildung 102: Administrator anlegen	75
Abbildung 103: Administrator anlegen	75
Abbildung 104: Administrator bearbeiten	77
Abbildung 105: Rechte eines Sub-Administrators verwalten	77
Abbildung 106: Vergabe von Berechtigungen durch einen Systemadministrator bzw. durch einen Sub-Administrator	78
Abbildung 107: Administrator löschen	78
Abbildung 108: Administrator löschen	79
Abbildung 109: Einstellungen der AirKey-Schließanlage	79
Abbildung 110: Allgemeine Einstellungen – Bluetooth-Einstellungen für die AirKey-App	80
Abbildung 111: Allgemeine Einstellungen – AirKey-App-Einstellungen	80
Abbildung 112: AirKey-App-Einstellungen – Aktualisierung nach jedem Zutritt	80
Abbildung 113: Status der Option "Aktualisierung nach jedem Zutritt"	81
Abbildung 114: AirKey-App-Einstellungen – Text für die "Send a Key"-SMS	81
Abbildung 115: Allgemeine Einstellungen – Sicherheitsoptionen	82
Abbildung 116: Allgemeine Einstellungen – Zwei-Faktor-Authentifizierung (2FA)	83
Abbildung 117: Verifizierung der Mobiltelefonnummer in den Einstellungen	83
Abbildung 118: SMS-Code eingeben Einstellungen	83
Abbildung 119: Zwei-Faktor-Authentifizierung deaktivieren	84
Abbildung 120: Dialog "Zwei-Faktor-Authentifizierung deaktivieren"	84
Abbildung 121: Vier-Augen-Prinzip aktivieren	85
Abbildung 122: Vier-Augen-Prinzip aktivieren – zweiten Administrator auswählen	85
Abbildung 123: Vier-Augen-Prinzip aktivieren – Bestätigungscode eingeben	85
Abbildung 124: Vorgabewerte für neue Schließkomponenten	86
Abbildung 125: Vorgabewerte – Bereiche	87
Abbildung 126: Vorgabewerte – Zutritt	87
Abbildung 127: Automatische Daueröffnung	88
Abbildung 128: Automatische Daueröffnungen und Endzeitpunkte	88
Abbildung 129: Protokollierung – Aktualisierung nach einem Sperrvorgang	89
Abbildung 130: Protokollierung definieren	90
Abbildung 131: Geänderte Vorgabewerte speichern	90
Abbildung 132: Feiertagskalender (Kalenderansicht)	91
Abbildung 133: Feiertag hinzufügen	91
Abbildung 134: Feiertag hinzufügen über Kalender	92
Abbildung 135: Feiertag bearbeiten	92
Abbildung 136: Feiertag löschen	92
Abbildung 137: Feiertagskalender (Listenansicht)	93
Abbildung 138: AirKey-Schließanlage	93
Abbildung 139: Schließkomponenten	94
Abbildung 140: Schließkomponente bearbeiten	95

Abbildung 141: Bereiche	95
Abbildung 142: Freigaben	95
Abbildung 143: Schließkomponente bearbeiten	95
Abbildung 144: Einstellungen – Uhrzeit und Kalender	96
Abbildung 145: Protokollierung	96
Abbildung 146: Schließkomponente entfernen	97
Abbildung 147: Sicherheitsabfrage	97
Abbildung 148: Schließanlage – Bereiche	98
Abbildung 149: Bereich anlegen	99
Abbildung 150: Bereich bearbeiten	99
Abbildung 151: Komponenten zuweisen	100
Abbildung 152: Schließkomponenten markieren	101
Abbildung 153: Zuweisung aufheben	101
Abbildung 154: Bereich löschen	102
Abbildung 155: Bereich löschen – nicht möglich	102
Abbildung 156: Die Reiter der Seite "Schließkomponente bearbeiten"	103
Abbildung 157: Berechtigte Medien (eigene)	103
Abbildung 158: Medium bearbeiten	104
Abbildung 159: Wartungsaufgaben	104
Abbildung 160: Priorisierung der Wartungsaufgaben	105
Abbildung 161: Schließplan	106
Abbildung 162: Medien & Personen	107
Abbildung 163: Personen	108
Abbildung 164: Übergabebestätigung generieren	109
Abbildung 165: Beispiel Übergabebestätigung	109
Abbildung 166: Person löschen	110
Abbildung 167: Person löschen – Sicherheitsabfrage	110
Abbildung 168: Medium zuweisen	111
Abbildung 169: Medium zu Person zuweisen	111
Abbildung 170: Medium zu Person zuweisen	112
Abbildung 171: Medienliste	112
Abbildung 172: Medium hinzufügen	113
Abbildung 173: Neues Medium hinzufügen	113
Abbildung 174: Medium bearbeiten – Karte	114
Abbildung 175: Berechtigungsübersicht	115
Abbildung 176: Medium bearbeiten – Berechtigung ändern	116
Abbildung 177: Berechtigung ändern	116
Abbildung 178: Zutritt ändern	117
Abbildung 179: Dauerzutritt	117
Abbildung 180: Berechtigung löschen	118
Abbildung 181: Berechtigung löschen	118
Abbildung 174: Medium deaktivieren	119
Abbildung 183: Medium deaktivieren – Sicherheitsabfrage	119
Abbildung 184: Deaktiviertes Medium entfernen	120
Abbildung 185: Medium entfernen – Sicherheitsabfrage	120
Abbildung 186: Deaktiviertes Medium reaktivieren	121
Abbildung 187: Medium reaktivieren	121
Abbildung 188: Medium reaktivieren	121

Abbildung 189: Medium reaktivieren – Berechtigungen wiederherstellen -----	122
Abbildung 190: Duplizieren eines Mediums -----	123
Abbildung 191: Medium duplizieren -----	123
Abbildung 192: Medium leeren -----	124
Abbildung 193: Medium leeren – Sicherheitsabfrage -----	124
Abbildung 194: Zugewiesene Medien -----	125
Abbildung 195: Medium – Zuweisung aufheben -----	125
Abbildung 196: Zuweisung aufheben ohne Berechtigungen -----	125
Abbildung 197: Zuweisung aufheben mit Berechtigungen -----	126
Abbildung 198: Zuweisung aufheben – Person wechseln -----	126
Abbildung 199: Person wechseln -----	127
Abbildung 200: Person wechseln -----	127
Abbildung 193: Medium entfernen – Papierkorb -----	127
Abbildung 202: Medium entfernen -----	128
Abbildung 203: Protokolle -----	129
Abbildung 204: Protokolleinsicht freischalten – zweiten Administrator wählen -----	130
Abbildung 205: Protokolleinsicht freischalten – Bestätigungscode eingeben -----	130
Abbildung 206: Protokoll Schließkomponenten & Bereiche -----	131
Abbildung 207: Protokolleinsicht freischalten – zweiten Administrator wählen -----	132
Abbildung 208: Protokolleinsicht freischalten – Bestätigungscode eingeben -----	133
Abbildung 209: Medienprotokoll -----	133
Abbildung 210: Protokolleinträge löschen -----	135
Abbildung 211: Systemprotokoll -----	136
Abbildung 212: Support-Freigaben -----	137
Abbildung 213: Liste Support-Freigaben -----	137
Abbildung 214: Support-Freigabe anlegen -----	137
Abbildung 215: Support-Freigabenübersicht -----	138
Abbildung 216: Support-Freigaben sperren -----	138
Abbildung 217: Gültigkeit der Support-Freigaben -----	139
Abbildung 218: AirKey-App – Berechtigungsübersicht -----	141
Abbildung 219: AirKey-App – Berechtigungsdetails -----	141
Abbildung 220: Berechtigung abgelaufen -----	141
Abbildung 221: Protokolldaten einer Berechtigung -----	142
Abbildung 222: Daueröffnung Erfolgsmeldung -----	142
Abbildung 223: AirKey-App – PIN eingeben -----	143
Abbildung 224: Medien codieren – Auswahlliste Bluetooth – Schließkomponenten -----	144
Abbildung 225: Medien codieren -----	144
Abbildung 226: Berechtigungsprotokoll -----	145
Abbildung 227: Android-Smartphone mit Bluetooth – Hauptmenü / Option "Bluetooth verwenden" aktiviert / Option deaktiviert -----	145
Abbildung 228: iPhone (nur mit Bluetooth) – Hauptmenü / Einstellungen ohne NFC- abhängige Funktionen / Funktion Bluetooth deaktiviert -----	146
Abbildung 229: Sperren aus Benachrichtigung – Sperrbildschirm -----	148
Abbildung 230: Sperren aus Benachrichtigung -----	148
Abbildung 231: AirKey-App – Sicherheitsfunktionen -----	149
Abbildung 232: AirKey-App – PIN aktivieren -----	150
Abbildung 233: AirKey-App – PIN ändern -----	151
Abbildung 234: AirKey-App – Verschlüsselung deaktivieren -----	151

Abbildung 235: AirKey-Onlineverwaltung – PIN-Code deaktivieren -----	152
Abbildung 236: AirKey-Onlineverwaltung – Dialog "PIN-Code deaktivieren" -----	152
Abbildung 237: AirKey-App – Einstellungen – Benachrichtigungen (Android / iPhone) ----	153
Abbildung 238: Wartungsaufgaben -----	154
Abbildung 239: Benachrichtigung über eine Berechtigungsänderung -----	154
Abbildung 240: AirKey-App – Info -----	155
Abbildung 241: Android-Smartphone bzw. iPhone aktualisieren -----	156
Abbildung 242: AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone) -----	157
Abbildung 243: AirKey-App – Daten aktualisieren -----	157
Abbildung 244: Wartungsberechtigung -----	158
Abbildung 245: Menüpunkt "Wartungsaufgaben" im Hauptmenü -----	158
Abbildung 246: Wartungsaufgaben -----	159
Abbildung 247: Anzeige der Schließkomponentendetails -----	160
Abbildung 248: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone) -----	161
Abbildung 249: AirKey-App – Mit Komponente verbinden -----	161
Abbildung 250: AirKey-Komponente entfernen-----	162
Abbildung 251: Medien codieren – Auswahlliste Bluetooth – Schließkomponenten -----	162
Abbildung 252: Medium mit iPhone entfernen-----	163
Abbildung 253: Medium entfernen -----	163
Abbildung 254: Das Protokoll-Symbol -----	164
Abbildung 255: Einstellungen der AirKey-App-----	165
Abbildung 256: Berechtigungen für Hands-free-Modus -----	165
Abbildung 257: iOS-NFC-Tag-----	167
Abbildung 258: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone) -----	169
Abbildung 259: Daten aktualisieren -----	170
Abbildung 260: Aktualisierungsmeldungen -----	170
Abbildung 261: Schließkomponente mit Codierstation aktualisieren -----	171
Abbildung 262: Schließkomponente mit Codierstation aktualisiert -----	171
Abbildung 263: Symbol "Mit Komponente verbinden" (nur bei Android-Smartphones) ----	172
Abbildung 264: Daten aktualisieren -----	172
Abbildung 265: AirKey-App aktualisiert ein Medium -----	172
Abbildung 266: Medium mit Codierstation aktualisieren -----	173
Abbildung 267: Eigenes bzw. fremdes Medium mit Codierstation aktualisiert -----	173
Abbildung 268: AirKey-App – AirKey-App – Mit Komponente verbinden (Android NFC / Android Bluetooth / iPhone) -----	174
Abbildung 269: Mit Komponente verbinden – Firmware-Update -----	175
Abbildung 270: AirKey-App – Komponentendetails -----	175
Abbildung 271: AirKey-App – Firmware aktualisieren-----	175
Abbildung 272: AirKey-App – Updateschritt erfolgreich-----	176
Abbildung 273: AirKey-App – Update erfolgreich-----	176
Abbildung 274: Codierstation – Erfolgsmeldung bei der Aktualisierung einer Schließkomponente -----	177
Abbildung 275: Codierstation – Firmware-Update für Zylinder-----	177
Abbildung 276: Codierstation – Updateschritt erfolgreich -----	178
Abbildung 277: Codierstation – Firmware-Update erfolgreich -----	178

Abbildung 278: Codierstation – Schließkomponente erfolgreich aktualisiert-----	178
Abbildung 279: AirKey-App – Mit Komponente verbinden -----	180
Abbildung 280: AirKey-App – Mediumdetails -----	180
Abbildung 281: AirKey-App – Keyring aktualisieren-----	180
Abbildung 282: AirKey-App – Keyring-Update erfolgreich -----	181
Abbildung 283: Codierstation – Keyring-Update verfügbar -----	181
Abbildung 284: Codierstation – Keyring-Update -----	182
Abbildung 285: Codierstation – Keyring-Update erfolgreich -----	182
Abbildung 286: Codierstation – Medium erfolgreich aktualisiert-----	182
Abbildung 287: Batteriestatus-----	183
Abbildung 288: Schließkomponente bearbeiten – Reparaturoptionen-----	186
Abbildung 289: Reparaturoptionen-----	187
Abbildung 290: Komponentenstatus und Wartungsaufgabe -----	187
Abbildung 291: Komponente im Auslieferungszustand – Ersatzzylinder ausstellen -----	189
Abbildung 292: Schließkomponente bearbeiten – Reparaturoptionen-----	190
Abbildung 293: Reparaturoptionen-----	190
Abbildung 294: Komponentenstatus und Wartungsaufgabe -----	191
Abbildung 295: Smartphone-defekte Komponente ausbauen -----	192
Abbildung 296: Smartphone – defekte Komponente ausbauen – Bestätigung -----	192
Abbildung 297: Defekte Schließkomponente ausbauen -----	193
Abbildung 298: Wartungsaufgabe löschen-----	194
Abbildung 299: Smartphonetausch bestätigen -----	197
Abbildung 300: QR-Code für den Smartphonetausch -----	197
Abbildung 301: Startseite – Offene Smartphone-Tauschoperationen -----	198
Abbildung 302: Offene Smartphone-Tauschoperationen-----	198
Abbildung 303: Smartphonetausch fehlgeschlagen -----	198
Abbildung 304: Smartphone tauschen -----	200
Abbildung 305: Smartphone tauschen -----	200
Abbildung 306: Smartphone tauschen -----	201
Abbildung 307: Smartphone tauschen – Code erneut senden-----	201
Abbildung 308: Schließkomponente freigeben -----	202
Abbildung 309: Freigabe hinzufügen -----	202
Abbildung 310: Schließkomponente hinzufügen – grauer Balken -----	203
Abbildung 311: Schließkomponente hinzufügen-----	203
Abbildung 312: Freigegebene Schließkomponente hinzufügen -----	203
Abbildung 313: Freigegebene Schließkomponente hinzufügen -----	204
Abbildung 314: Freigegebene Schließkomponente hinzufügen -----	204
Abbildung 315: Berechtigung freigegebene Schließkomponente -----	206
Abbildung 316: Berechtigte Medien (fremde) -----	207
Abbildung 317: Block "Freigaben" – Freigabe löschen -----	207
Abbildung 318: Freigabe löschen-----	207
Abbildung 319: Schließenanlage hinzufügen -----	208
Abbildung 320: Allgemeine Einstellungen – AirKey Cloud Interface (API) -----	210
Abbildung 321: API aktivieren-----	211
Abbildung 322: API-Key generieren-----	212
Abbildung 323: Dialog "API-Key generieren" -----	212
Abbildung 324: API-Key generieren – Details -----	212
Abbildung 325: API-Key bearbeiten-----	213

Abbildung 326: API-Key löschen -----	214
Abbildung 327: API-Key deaktivieren -----	214
Abbildung 328: API-Key aktivieren-----	214
Abbildung 329: Testdaten generieren-----	215
Abbildung 330: API-Key für die Testumgebung generieren-----	216
Abbildung 331: Testdaten der Testumgebung zurücksetzen-----	216

22 Glossar

Innerhalb von AirKey werden unter anderem folgende Begriffe verwendet:

Bezeichnung	Funktion
Mandant	Besitzer der Schließanlage mit einer eindeutigen Kundennummer.
Administrator	Ist eine Benutzerrolle des AirKey-Systems, die berechtigt ist, alle administrativen Tätigkeiten in der AirKey-Onlineverwaltung durchzuführen. Für einen Mandanten können mehrere Administratoren angelegt werden. Für jede AirKey-Schließanlage muss mindestens ein Administrator definiert sein.
Person	Anwender, die Medien benutzen. Den Personen werden Medien mit Zutrittsberechtigungen für Bereiche und Schließkomponenten zugewiesen.
Medien	Sind Smartphones oder Zutrittsmedien, die zu AirKey-Schließanlagen hinzugefügt werden können, um bei berechtigten AirKey-Schließkomponenten Zutritt zu erhalten.
Zutrittsmedien	Sind passive NFC-Medien (ohne eigene Stromversorgung), die neben Smartphones in AirKey-Schließanlagen verwendet werden können. Dazu zählen Karten, Schlüsselanhänger, Kombischlüssel, Armbänder etc.
Quellmedium	Dieser Begriff wird in Zusammenhang mit den Funktionen "Smartphonetausch" und "Medium duplizieren" verwendet. Es beschreibt jenes Smartphone oder Zutrittsmedium, von dem der Tausch oder das Duplizieren gestartet wurde. Im Falle des Smartphonetauschs beschreibt das Quellmedium das "alte" Smartphone, das durch ein neues ersetzt werden soll.
Zielmedium	Dieser Begriff wird in Zusammenhang mit den Funktionen "Smartphonetausch" und "Medium duplizieren" verwendet. Es beschreibt jenes Smartphone oder Zutrittsmedium, dem die AirKey-Berechtigungen und -Einstellungen übertragen werden sollen. Im Falle des Smartphonetauschs beschreibt das Zielmedium das "neue" Smartphone, das ein anderes Smartphone ersetzen soll.
Schließkomponenten	Sind AirKey-Zylinder (in den unterschiedlichsten Bauformen), -Hangschlösser und -Wandler, die Türen in einer Schließanlage öffnen und schließen können.
Bereich	Ist eine administrative Einheit in der AirKey-Onlineverwaltung, die mehrere Schließkomponenten umfasst. Bereiche erleichtern die Verwaltung der AirKey-Schließanlage und die Berechtigungsvergabe für Schließkomponenten.

KeyCredits	Beschreibt ein Guthaben innerhalb einer AirKey-Schließanlage. Guthaben wird benötigt, um neue Berechtigungen zu vergeben, bestehende Berechtigungen zu ändern oder weitere Funktionalitäten von AirKey zu aktivieren.
AirKey Cloud Interface	Beim AirKey Cloud Interface handelt es sich um eine Schnittstelle (API) für Drittsysteme auf Basis von REST . Die Schnittstelle erlaubt es, bestimmte Funktionen von AirKey über eine Drittsoftware zu steuern.
RS485-Schnittstelle	Die RS485-Schnittstelle ist eine standardisierte Schnittstelle, die zur Übertragung von Daten eingesetzt werden kann. Bei einem AirKey-Wandleser kann über diese Schnittstelle der letzte erfolgreiche Zutritt an eine Drittsoftware übermittelt werden.
APDU	APDU steht für Application Protocol Data Unit und wird hier in diesem Dokument bei der RS485-Schnittstelle verwendet. Es beschreibt ein Datenpaket, das über die RS485-Schnittstelle übermittelt wird.
"Send a Key"	Beschreibt eine Funktion der AirKey-Onlineverwaltung. Ein Administrator kann hiermit schnell neue Smartphones anlegen und Berechtigungen vergeben bzw. bestehende Berechtigungen von Smartphones bearbeiten. Der Smartphone-Besitzer erhält eine SMS, über die das Smartphone automatisch für AirKey registriert wird.
Zwei-Faktor-Authentifizierung	Die Zwei-Faktor-Authentifizierung, oder auch 2FA, dient als zusätzliche Sicherheitsstufe bei der Anmeldung zur AirKey-Onlineverwaltung. Dabei wird neben der Benutzerkennung und Passwort ein zusätzlicher SMS-Code bei der Anmeldung, als zweiter Faktor, abgefragt.
Vier-Augen-Prinzip	Beschreibt einen Vorgang, bei dem nur durch eine zusätzliche Person eine Aktion durchgeführt werden kann. Bei AirKey kann dieses Prinzip verwendet werden, um personenbezogene Daten in den Protokollen zu schützen.
Firmware	Software-Programm, das auf Schließkomponenten installiert ist, damit diese deren AirKey-Funktion ausüben können. Die Firmware von Schließkomponenten kann in Form von Firmware-Updates aktualisiert werden.
Keyring	Im AirKey-System ist "Keyring" der Name eines Softwareprogramms, das alle AirKey-relevanten Daten verwaltet, die auf passiven Zutrittsmedien wie Karten, Schlüsselanhänger, Kombischlüssel und Armbänder gespeichert sind. Falls eine neue Keyring-Version im AirKey-System verfügbar ist, können die Medien mit einem Smartphone mit Wartungsberechtigung oder mit einer Codierstation aktualisiert werden.
Wartungsaufgaben	Werden innerhalb der AirKey-Onlineverwaltung für Schließkomponenten angezeigt, die nicht aktuell sind. Erst wenn alle Wartungsaufgaben einer AirKey-Schließanlage erledigt wurden, ist die Anlage aktuell und sicher.

<p>Wartungs- berechtigung</p>	<p>Nur wenn ein Smartphone die Wartungsberechtigung für die Schließanlage besitzt, können damit Komponenten (Medien und Schließkomponenten) in die Schließanlage hinzugefügt bzw. aus ihr entfernt werden. Mit einem Smartphone mit Wartungsberechtigung kann der AirKey-Wartungstechniker Schließkomponenten auch im Auslieferungszustand bedienen.</p> <p>Die Wartungsberechtigung kann in der AirKey-Onlineverwaltung für die gewünschten Smartphones aktiviert werden.</p>
-----------------------------------	--

23 Impressum

7. Ausgabe, November 2022

Mit dem Erscheinen eines neuen Systemhandbuchs verliert diese Ausgabe seine Gültigkeit. Die jeweils aktuelle Version des Systemhandbuchs finden Sie auf unserer Homepage zum Download: <https://www.evva.com/de/airkey/systemmanual/>.

Alle Rechte vorbehalten. Ohne schriftliche Zustimmung des Herausgebers darf dieses Systemhandbuch nicht – auch nicht auszugsweise – in irgendeiner Form reproduziert oder unter Verwendung elektronischer, mechanischer oder chemischer Verfahren vervielfältigt oder verarbeitet werden.

Es ist möglich, dass das vorliegende Systemhandbuch drucktechnische Mängel oder Druckfehler aufweist. Die Angaben in diesem Systemhandbuch werden jedoch regelmäßig überprüft und Korrekturen vorgenommen. Für Fehler technischer oder drucktechnischer Art und ihre Folgen übernehmen wir keine Haftung.

Alle Warenzeichen und Schutzrechte werden anerkannt.

Änderungen im Sinne des technischen Fortschritts können ohne Vorankündigungen vorgenommen werden.

Impressum

Herausgeber

EVVA Sicherheitstechnologie GmbH

Für den Inhalt verantwortlich

EVVA Sicherheitstechnologie GmbH

Technischer Inhalt

Florian Diener, Johannes Ullmann

Technische Berater

Raphael Fasching, Iulian Stanculescu, Martin Bauer