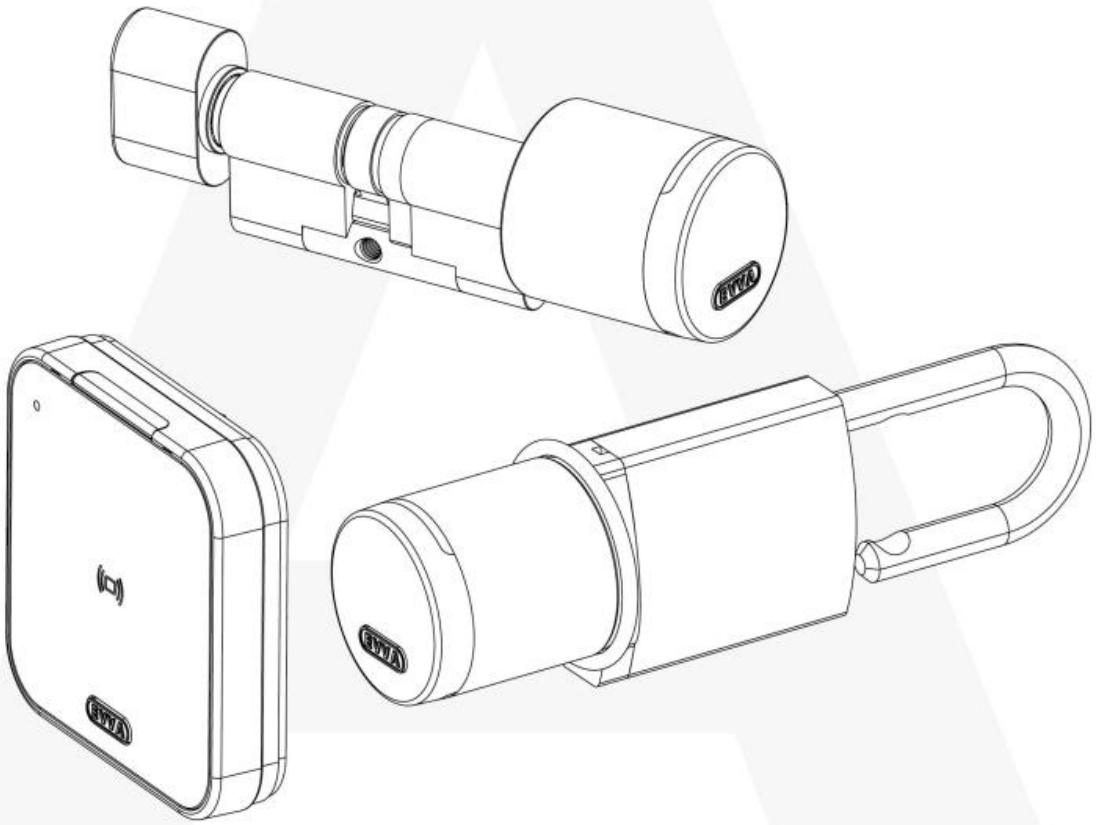


AirKey

Systemhandbok 2.6

1 Innehållsförteckning

2 Inledning, översikt

Denna handbok för AirKey-systemet innehåller information om installation, drift och användning av det elektroniska systemet, som består av AirKey-onlineadministrationen, AirKey-appen, cylindrar, väggläsare, hänglås och medier för systemet.

De produkter och programvaran AirKey-onlineadministration som beskrivs i systemets handbok får endast användas av personal med lämpliga kvalifikationer för respektive uppgift. Med kvalificerad personal avses personer som kan identifiera risker vid hantering av produkterna / systemet och förebygga potentiella faror på grundval av sin expertis.

2.1 Allmän rättslig information

- EVVA ingår avtal för användning av AirKey uteslutande på grundval av företagets Allmänna villkor samt Licensavtalet för slutanvändare (EULA) i fråga om produktens programvara.
- Tänk på att användningen av det AirKey-system som är föremål för detta avtal kan utlösa krav på rättsligt godkännande, rapportering eller registrering, i synnerhet i fråga om dataskydd (t.ex. ett omfattande informationssystem) samt bevilja rätt till medbestämmelse för personal om användning sker inom företagets anläggningar. Kunder och slutanvändare ansvarar för att produkten används i enlighet med gällande bestämmelser.
- Ovannämnda uppgifter måste följas och vidarebefordras till operatörer och användare i enlighet med tillverkarens produktansvar så som det definieras i produktansvarslagen. Om detta inte beaktas frånsäger sig EVVA allt ansvar.
- Produkten lämpar sig inte för användning i miljöer med barn under 36 månader på grund av att den omfattar smådelar som kan sväljas.
- All användning som inte överensstämmer med bestämmelserna i avtalet, användning för ej avsedda ändamål, reparationer eller ändringar som inte uttryckligen godkänts av EVVA samt alla typer av felaktig service kan orsaka felfunktion och tillåts inte. Om kunden genomför ändringar som inte uttryckligen godkänts av EVVA upphör alla anspråk på ansvar och garanti samt eventuella separata garantianspråk att gälla.
- Arkitekter och konsulter är skyldiga att begära all nödvändig produktinformation från EVVA och att ta hänsyn till alla uppgifter för att uppfylla kraven gällande information och anvisningar i produktansvarslagen. Specialiserade återförsäljare och installatörer ska beakta informationen i EVVA-dokumentationen och vidarebefordra sådan information till kunderna om detta är nödvändigt.
- Beakta även gällande internationella och nationella föreskrifter i gällande lagstiftning, direktiv, standarder och direktiv, särskilt i fråga om krav på utrymningsvägar och nödutgångar, i samband med projektplanering och installation av AirKey-enheter.

2.2 EVVA-support

AirKey ger dig ett sofistikerat och testat låssystem. Om du fortfarande behöver support, kontakta din EVVA-partner.

Du kan hitta en lista över certifierade EVVA-partners på vår hemsida https://www.evva.com/se-sv/soekaaterfoersaeljare/.

Om du väljer filteralternativet "Elektronikpartner", filtrerar du specifikt efter EVVA-partners som säljer de elektroniska EVVA-låssystemen och har kvalificerad specialistkunskap inom detta område.

Använd EVVA:s onlineformulär för att få hjälp med specifika frågor. Onlineformuläret används för support i följande situationer:

- När man överskridit det högsta tillåtna antalet försök att ange kreditkoder.
- När man inte kan lägga till kredit.
- När inloggningssidan för AirKey-onlineadministration inte är tillgänglig.
- När man inte kan logga in. När man glömt användar-ID eller e-postadress.
- Du har aktiverat tvåfaktorsautentisering och har inte tillgång till din smarttelefon.

Klicka på följande länk för att öppna formuläret: https://www.evva.com/sv/airkey/support/.

Allmän information om AirKey finns på vår webbplats på https://www.evva.com/sv/airkey/website/.

2.3 Märkningar och symboler

I denna handbok framställs sekvenser av kommandon, enskilda kommandon eller knappar på det sätt som visas nedan.

Exempel: Huvudmeny ***Media & personer*** → ***Skapa person*** eller knappar såsom ***Spara***.

Varning, risk för materiella skador om gällande säkerhetsanvisningar inte följs.

Anmärkningar och ytterligare information

Tips och rekommendationer

Felmeddelanden

Option Alternativ

2.4 Tips för optimal navigering i detta dokument

I detta dokument finns många interna länkar som leder till andra kapitel eller textställen. Det snabbaste och bekvämaste sättet att gå tillbaka till ursprungsläget i Windows eller framåt igen är med hjälp av dessa **genvägar**:

Alt + ◄ (Alt + vänsterpil) = navigera bakåt

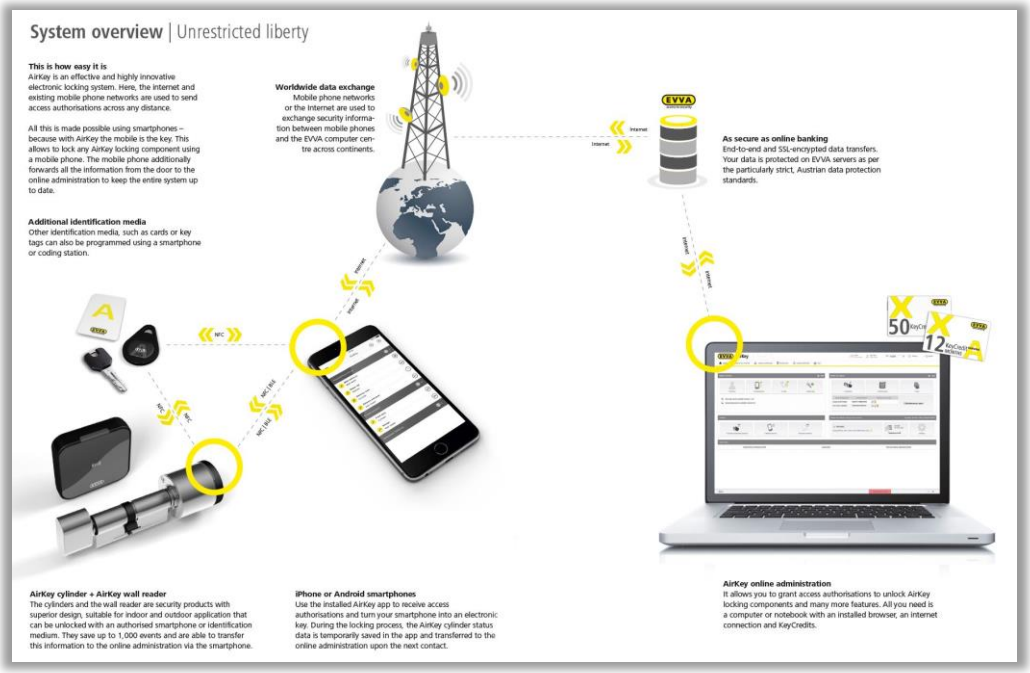
Alt + ► (Alt + högerpil) = navigera framåt

Dessa kortkommandon fungerar i många PDF-läsare och i t.ex. Microsoft Word.

Om du vill testa kortkommandona klickar du på den här länken och går tillbaka med Alt + ◄.

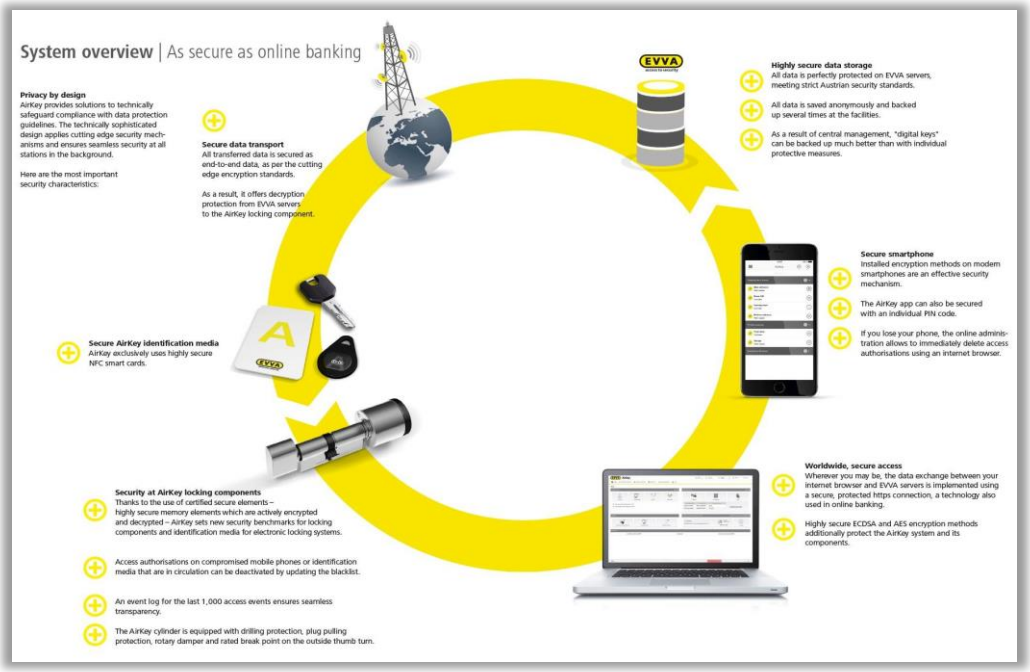
3 Systemarkitektur

På följande figur visas en översikt av AirKey-enheterna och deras kommunikationsmetoder. Detta följs av en beskrivning av de enskilda enheterna.



Figur 1: Systemarkitektur

Alla uppgifter som överförs från EVVAs servar till AirKey-enheter säkras som end-to-end-data med hjälp av de senaste krypteringsstandarderna.



Figur 2: Systemöversikt – sömlös säkerhet

3.1 Låskomponenter

Låskomponenter (cylindrar och väggläsare) kontrolerar tillträdet vid dörrar. Beroende på användarens behörighet, beviljar eller nekar låskomponenter tillträde.

3.1.1 AirKey-cylindrar

AirKey-cylindrar är batteridrivna enheter. Godkända för användning både inom- och utomhus. Beroende på de specifika kraven kan AirKey-cylindrar passa för användning i säkerhetskritiska områden. AirKey-cylindrar är mekaniskt skyddade mot vandalisering och manipulering. AirKey-cylindrar passar för installation i brandskyddsdörrar och nödutgångar * under förutsättning att de är installerade enligt anvisningarna.

AirKey-cylindrar finns som enkel- eller dubbelcylindrar. Dubbelcylindrarna finns för tillträde på ena eller på båda sidorna. Modellen för tillträde från ett håll är utrustade med elektronisk vredknopp på ena sidan. Medans modellerna för tillträde på båda sidorna har elektronisk vredknopp på båda sidorna. Det elektroniska vredet på identifieringssidan roterar fritt om ingen giltig behörighet tillhandahålls. Den svarta plastkåpan på AirKey-cylindern är läsarenheten.

När användaren håller ett behörigt medium mot vredet kopplar cylindern in tillfälligt så att det elektroniska vredet kan manövrera låset. Observera informationen i Använda AirKey-enheter.

Tänk på att dörren inte låses automatiskt när du har stängt den. Dörren måste låsas antingen manuellt eller via en särskilt extra anordning.

Kontrollera om den AirKey-cylinder som är vald passar för användningsområdet. AirKey-cylindern finns tillgänglig i flera olika modeller och utföranden.

Tillhörande datablad samt produktkatalogen finns på vår webbplats i området för nedladdningsbara filer på https://www.evva.com/sv/downloads/.

AirKey-cylindrar avger optiska och akustiska signaler. I kapitel Låskomponenternas signaler hittar man en närmare beskrivning av varje enskild signal.

Följ monteringsanvisningen som medföljer AirKey-cylindern för installation eller monteringsfilmen på https://www.evva.com/sv/airkey/website/.

3.1.2 AirKey-hybridcylindern

AirKey-hybridcylindern har samma egenskaper som AirKey-cylindern. Den kan användas både utom- och inomhus, samt i säkerhetskänsliga miljöer.

* Antipanikfunktionen FAP kan behövas för användning i nödutgångar och panikdörrar, beroende på vilken typ av DIN-lås som är installerat. Observera därför relevanta uppgifter och certifikat från låsets tillverkare samt produktkoden i ordern.

Till skillnad från AirKey-dubbelcylindern med enkelsidigt tillträde sitter det en nyckelmodul på insidan av AirKey-hybridcylindern i stället för ett mekaniskt vred. Således får man tillträde från utsidan via en elektronisk behörighetskontroll och från insidan via en mekanisk nyckel.

Tänk på att dörren inte låses automatiskt när du har stängt den. Dörren måste låsas antingen manuellt eller via en särskilt extra anordning.

Kontrollera att AirKey-hybridcylindern passar för avsedd användning.

Det datablad som behövs för att avgöra detta samt produktkatalogen finns på vår webbplats i området för nedladdningsbara filer på https://www.evva.com/sv/downloads/.

AirKey-hybridcylindern avger optiska och akustiska signaler. I kapitel Låskomponenternas signaler hittar man en närmare beskrivning av varje enskild signal.

Följ monteringsanvisningen som medföljer AirKey-hybridcylindern för installation.

3.1.3 AirKey-industricylinder

AirKey-industricylindern är en batteridriven mekatronikcylinder avsedd att användas i skåp, montrar samt för brevlådor både utomhus och inomhus.

Tillträde sker via ett elektroniskt vred. På insidan sitter en regel för låsning. Med rätt behörighet aktiveras cylindern och manövreras genom att vrida på vredknoppen. Till skillnad från AirKey-cylindern och hybridcylindern är vredknoppen icke fritt roterande utan fast i icke aktiverat läge.

Kontrollera att AirKey-industricylindern passar avsedd användning. AirKey-industricylindern finns tillgänglig i flera olika modeller och utföranden.

Det datablad som behövs för att avgöra detta samt produktkatalogen finns på vår webbplats i området för nedladdningsbara filer på https://www.evva.com/sv/downloads/.

AirKey-industricylindern avger optiska och akustiska signaler. I kapitel Låskomponenternas signaler hittar man en närmare beskrivning av varje enskild signal.

Följ monteringsanvisningen som medföljer AirKey-industricylindern för installation.

3.1.4 AirKey-hänglåset

AirKey-hänglåset är ett batteridrivet mekatronik hänglås att använda på grindar, jalusier och hänglåsbeslag både utom- och inomhus.

Aktivering sker via ett elektroniskt vred. Låsningen sker med en bygel i härdat stål. Med rätt behörighet aktiveras enheten och manövreras genom att vrida på vredknoppen.

Kontrollera att AirKey-hänglåset passar för avsedd användning. AirKey-hänglåset finns tillgängligt i flera olika utföranden.

Det datablad som behövs för att avgöra detta samt produktkatalogen finns på vår webbplats i området för nedladdningsbara filer på https://www.evva.com/sv/downloads/.

AirKey-hänglåset avger optiska och akustiska signaler. I kapitel Låskomponenternas signaler hittar man en närmare beskrivning av varje enskild signal.

Följ monteringsanvisningen som medföljer AirKey-hänglåset för installation.

Monteringsverktyg för AirKey-cylindern, hybridcylinder, industricylinder och hänglås

AirKey-cylindern, hybridcylindern, industricylindern och hänglåset har alla en särskild mekanism som skyddar mot manipulering. Det elektroniska vredet kan endast avlägsnas med specialverktyg. Nödvändiga verktyg för montering, demontering och byte av batterierna medföljer som standard inte i leveransen av AirKey-cylindern och måste beställas separat.

Artikelnumret hittar du i AirKey-produktkatalogen i nedladdningsbara filer på https://www.evva.com/sv/downloads/.

3.1.5 AirKey-väggläsare

AirKey-väggläsaren passar för användning inom- och utomhus, för infälld och utanpåliggande montering och för säkerhetskritiska områden. Använd den speciella tätningen som medföljer produkten vid användning i områden som utsätts för väta samt vid utanpåliggande installation. Observera informationen i monteringsanvisningen.

AirKey-väggläsare ansluts till styrenheten med hjälp av CAT5-kablar (max. 100 m, slinga max. = 2 ohm) för strömförsörjning. AirKey-styrenheten strömförsörjs av nätadaptern. I samband med strömavbrott är den utrustad med en databuffert för högst 72 timmar, under förutsättning att styrenheten varit i drift i minst 6 timmar.

Observera att det behövs en AirKey-styrenhet för varje AirKey-väggläsare.

AirKey-väggläsare och styrenheter används för att styra elektroniska låselement, t.ex. motordrivna cylindrar och skjut- eller svängdörrar.

Potentialfri anslutning för öppnarknapp (tryckknapp). Aktiverar de växlande reläerna NO/NC. Aktivering av reläerna via den potentialfria ingången loggas ej. Kan användas av tredjeparts system. Observera att detta inte syns i händelseloggen.

Kontrollera noggrant att den AirKey-produkt som är vald passar för den avsedda monteringssituationen / det avsedda användningsområdet. Nödvändiga datablad och monteringsanvisningar finns på nedladdningssidan på vår webbplats https://www.evva.com/sv/downloads/.

3.2 AirKey-app

AirKey-appen är gratis och finns för nedladdning på Google Play Store eller Apple App Store.

AirKey-appen är nödvändig för att kunna aktivera AirKey-enheten med en smarttelefon. Smarttelefonen används för att lägga till eller uppdatera AirKey-enheter och medier i systemet. De flesta funktioner i AirKey-appen kräver att man har internet koppling. AirKey-enheter kan även användas offline.

Internetuppkoppling kan medföra extra avgifter. Kontakta din operatör för mer information.

3.3 Smarttelefoner

Smarttelefoner måste uppfylla följande minimikrav för att kunna användas med AirKey-system:

- Smarttelefon med NFC eller Bluetooth 4.0 (Bluetooth Low Energy / BLE)
- Operativsystem:
  - Android™ från 5.0 (endast NFC-funktion)
  - Android™ från 6.0 (NFC och Bluetooth)
  - Apple™ från iOS 10 (endast Bluetooth-funktion)
- AirKey-app från Google Play Store eller Apple App Store
- På Android-telefoner måste alternativet "Läsa telefonens status och identitet" och lokaliseringstjänsterna vara aktiva.

Lista på smarttelefoner som är kompatibla med AirKey-system

Tänk på att smarttelefonens kompatibilitet påverkas av många faktorer och att inte alla telefoner som uppfyller minimikraven är kompatibla. Av denna anledning testar EVVA telefoner kontinuerligt. En uppdaterad lista på testade smarttelefonmodeller som kan användas med AirKey finns i listan på kompatibla smarttelefoner.

Aktivering av **åtkomsten till telefonens status och identitet** är en förutsättning för att smarttelefoner ska kunna identifieras unikt när de läggs till i ett nytt AirKey-system.

Åtkomst till **positionen behövs eftersom Android 6+ kräver aktivering av lokaliseringstjänster för att Bluetooth-enheter ska kunna sökas av!** Vill man använda Bluetooth-funktioner i AirKey-appen måste man aktivera lokaliseringstjänsterna samt ge appen åtkomst till dessa uppgifter i telefonens inställningar. Aktiverar man inte lokaliseringstjänsterna går det att ansluta till komponenterna (medier och AirKey-enheter) med NFC.

På **Apple-enheter** (operativsystem iOS) finns ingen möjlighet att avaktivera åtkomsten till telefonens status och identitet. iOS kan söka efter Bluetooth-enheter utan aktivering av lokaliseringstjänsten.

3.4 AirKey-media

De tillgängliga medierna är testade smarttelefonmodeller samt kort, nyckelbrickor, kombinycklar och armband i olika utföranden, med kombination *Mifare DESFire EV1*.

Motsvarande datablad samt produktkatalogen finns på vår webbplats i området förned-laddningsbara filer på https://www.evva.com/sv/downloads/.

Medier, såsom kort, nyckelbrickor eller kombinycklar levereras i ej aktiverad status. För aktivering måste mediet de läggas till i AirKey-systemet.

3.5 AirKey-onlineadministration

AirKey-onlineadministration är EVVAs onlinebaserade programlösning för administrering av AirKey-system. Det elektroniska AirKey-systemet är kompatibelt med alla vanliga webbläsare och operativsystem och kräver ingen programinstallation eller speciell IT-infrastruktur. EVVA ansvarar för drift och underhåll av AirKey-servrarna.

3.5.1 Systemkrav

- Operativsystem: Windows 10 (eller högre), MacOS 10.15 (eller högre), Linux
- För närvarande kompatibelt med följande operativsystem:
  Chrome, Firefox, Edge, Safari
- JavaScript aktiverat i webbläsaren
- Internetuppkoppling (1 MBit/s eller snabbare faster)
- Valfritt: USB-port 2.0 för kodningsstation
- Internetport 443 måste vara tillgängliga.

Det behövs en giltig e-postadress för att kunna registrera ett AirKey-system.

3.6 EVVA KeyCredits

KeyCredits är ett måste för att administrera AirKey-systemet, till exempel för att tilldela eller ändra behörigheter. KeyCredits är antingen mängdbaserade som krediter (ett specifikt antal behörighetsändringar utan tidsbegränsning) eller tidsbaserade (obegränsat antal behörighetsändringar inom en specifik tidsperiod). Hos specialiserade EVVA-partners finns ett passande KeyCredit-paket för varje behov, skräddarsytt till ditt AirKey-systems storlek och flexibilitet. Mer information om tillgängliga paket finns i AirKey produktkatalog https://www.evva.com/sv/downloads/.

3.7 Kodningsstation

Lägg till eller uppdatera AirKey-enheter och medier i ditt system med den kompletterande kodningsstationen eller en smarttelefon med underhållsbehörighet. Applikationen som installeras för kodstationen har den fördelen att den är kompatibel med alla aktuella

webbläsare. Kodstationen kan även användas för att uppdatera låskomponenter och medier efter utloggning från AirKey-onlineadministrationen.

Applikationen stöder följande webbläsare: Chrome, Firefox och Edge.

Systemkrav:

- USB port
- Java 7 eller högre
- Drivrutin för kodningsstationen

Mer information finns i avsnittet Installation av kodningsstation.

3.8 Nödströmsenhet

Alla AirKey-enheter har en kontakt på framsidan, under EVVA-loggan. Tryck försiktigt inåt på vänster sida av loggan (nära "E") och fäll ut på höger sida (nära "A") för att komma åt det. Anslutningen är endast avsett för försörjning av nödström och behövs inte i normal drift.

Nödströmsenheten strömsätter AirKey-enheterna även om batterierna laddas ur. Anslut nödströmsenhetens kabel till motsvarande kontakt och flytta brytaren till ON Inga andra åtgärder behövs på nödströmsenheten. Det behövs fortfarande ett medium med giltig behörighet för att aktivera AirKey-enheten.

Tänk på att det måste vara en permanent behörighet utan begränsad giltighet. Mer information finns i avsnittet Nödmedier. Byt batterier efter användning av nödströmsenheten och uppdatera AirKey enheten med smarttelefonen. Mer information finns i avsnittet Byta batterier och använda nödströmsenheten.

Observera att AirKey-väggläsaren inte kan försörjas med ström från nödströmsenheten, den strömförsörjs av en extern strömförsörjning i kombination med AirKey-styrenheten.

4 Driftsättning

I det här avsnittet beskrivs de första stegen för att driftsätta AirKey-systemet.

På vår webbplats https://www.evva.com/sv/airkey/website/ finns en film där de första stegen och driftsättning av AirKey-systemet beskrivs.

EVVA erbjuder följande material för hjälp med installationen av AirKey-enheter:

- **Monteringsanvisning**:
  EVVA tillhandahåller installationsanvisningar för AirKey-enheter. De medföljer i förpackningen av motsvarade produkt och finns även på vår webbplats https://www.evva.com/sv/downloads/.
- **Filmer**:
  Installationsfilmer finns på vår webbplats https://www.evva.com/sv/airkey/website/.

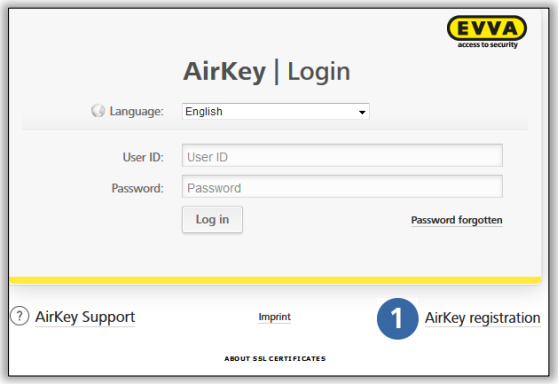
4.1 Installera AirKey-appen

- Ladda ned AirKey-appen från Google Play Store eller Apple App Store.
- Följ installationsanvisningarna för AirKey-appen på din smarttelefon.

4.2 Registrering på AirKey-onlineadministration

Registrera dig hos EVVA med en giltig e-postadress för att kunna använda AirKey-online-administration.

- Öppna följande sida i din webbläsare: https://airkey.evva.com
  Inloggningssidan för AirKey-onlineadministration öppnas.
- Välj önskat ***språk***.
- Klicka på länken för ***AirKey registrering*** ❶.

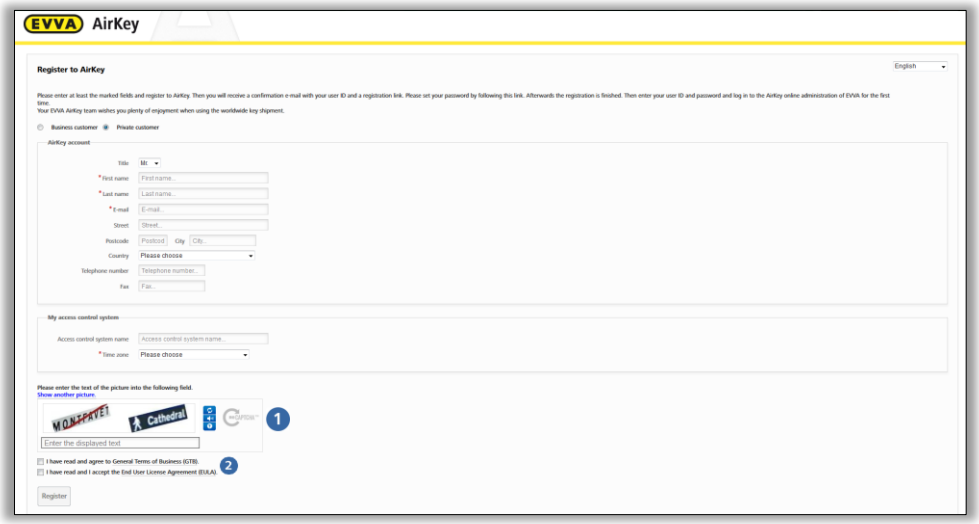


Figur 3: Länk "AirKey-registrering"

Skriv in dina uppgifter och registrera dig för AirKey.

- Välj ***Företag*** eller ***Privatkund***.

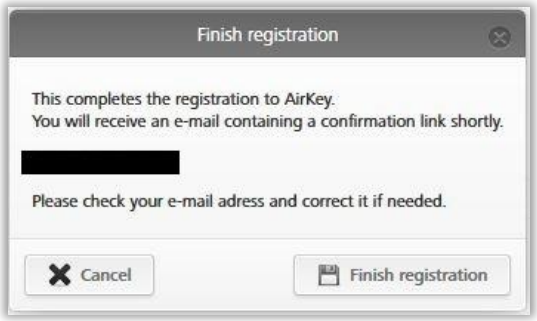
- Fyll i fälten i formuläret.
  Fält som är markerade med * är obligatoriska.
- Lös captcha-koden ❶.
- Kryssa för rutan vid länken Allmänna villkor och vid Licensavtalet för slutanvändare (EULA) ❷. De två motsvarande PDF-dokumenten öppnas automatiskt. Dokumenten finns även på https://www.evva.com/sv/airkey/impressum/.



Figur 4: Registrering för AirKey

Det är möjligt att ändra kunduppgifterna i efterhand om det skulle behövas. Detta görs genom att klicka på ***Låssystem*** → ***Kundinformation*** i huvudmenyn i AirKey-onlineadministration.

- Klicka på ***Registrering***. Fönstret "Slutför registrering" öppnar.
- Kontrollera att den e-postadress som angetts är korrekt, en bekräftelse med en registreringslänk skickas till adressen.
- Klicka på ***Avbryt*** för att avbryta processen och korrigera uppgifterna om e-postadressen är felaktig.
- Klicka ***Slutför registrering*** om e-postadressen är korrekt och slutför processen.

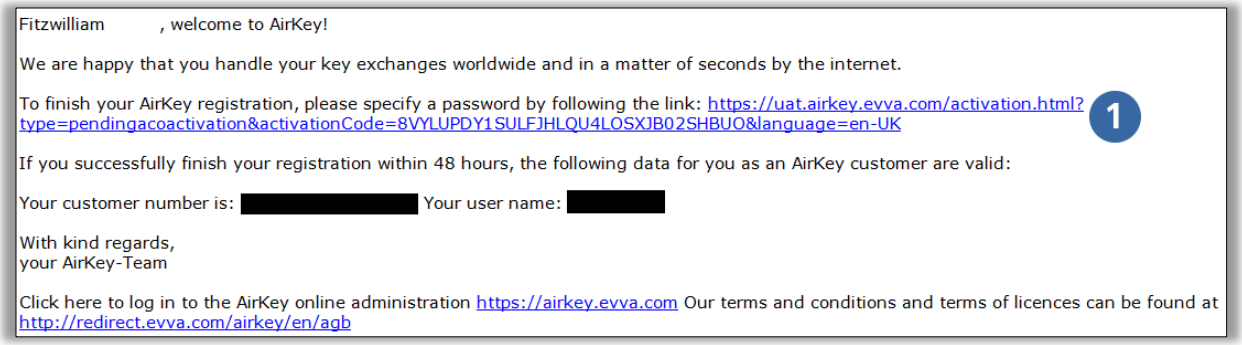


Figur 5: Slutföra registreringen

AirKey-systemet genererar automatiskt ett användar-ID och en registreringslänk och skickar det till den e-postadress som angetts vid registreringen.

- Öppna e-postklienten. Där finns ett e-postmeddelande från *EVVA AirKey* med texten "EVVA AirKey-registrering" i ämnesraden.
- Öppna e-postadressen och klicka på registreringslänken. ❶

Spara e-postmeddelandet på en säker plats. Behöver man support ange användar-ID och kundnummer i e-postadressen.


Fitzwilliam , welcome to AirKey!

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

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

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

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

With kind regards,
your AirKey-Team

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

Figur 6: E-postmeddelande "EVVA AirKey-registrering"

Registreringslänken i e-postadressen är endast giltig i 48 timmar.

Om registreringslänken har gått ut eller är ogiltig visas ett felmeddelande som indikerar att länken är ogiltig. I detta fall måste en ny registrering genomföras.

När man klickar på registreringslänken öppnas välkomstfönstret. Här slutförs registreringen.

- Ange ett personligt lösenord för AirKey-onlineadministration.
  Lösenordet måste innehålla minst 6 tecken, varav minst en siffra och en stor och en liten bokstav. Om lösenordet inte uppfyller kraven visas ett felmeddelande.
- Ange ditt lösenord igen.
- Ange ditt födelsedatum. Födelsedatumet används som säkerhetsfråga så att du kan bekräfta din identitet om du glömmer ditt lösenord.

Vi rekommenderar att AirKey-lösenordet är så långt som möjligt och hålls hemligt.

Figur 7: Ange ett AirKey-lösenord för att slutföra registreringen

> När man har fyllt i alla obligatoriska fält och båda AirKey-lösenorden stämmer överens klicka på ***Spara*** ❶ för att slutföra registreringen.

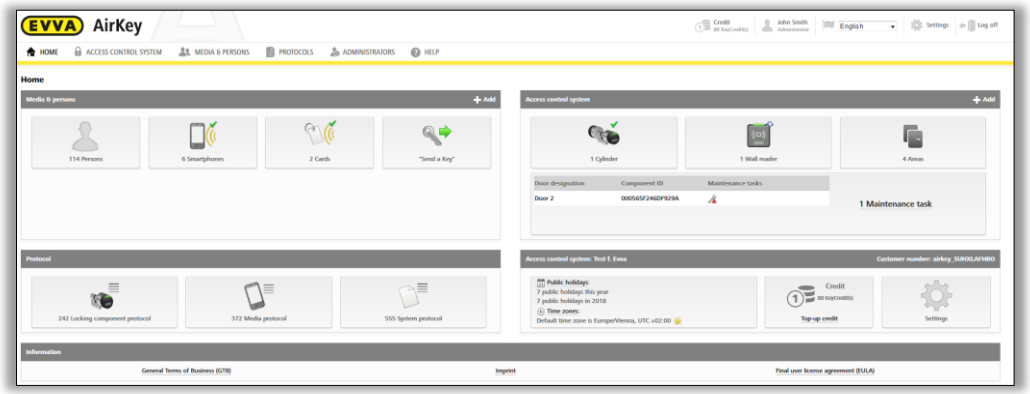
Nu är registreringsprocessen slutförd och ditt AirKey-system har aktiverats korrekt.

Nu är det möjligt att logga in när som helst på inloggningssidan av AirKey-onlineadministration. Man behöver användar-ID från registreringsmeddelandet och det AirKey-lösenord som är valt.

4.3 Logga in

Man måste logga in för att konfigurera och hantera AirKey-systemet.

> Öppna följande sida i webbläsaren: https://airkey.evva.com. Inloggningssidan för AirKey-onlineadministration öppnas.
> Välj önskat ***språk***. Man kan ändra språk i menyraden på höger sidan när som helst under den aktiva sessionen.
> Ange ditt användar-ID från registreringsmeddelandet och ditt lösenord och logga in. AirKey-systemets startsida visas.

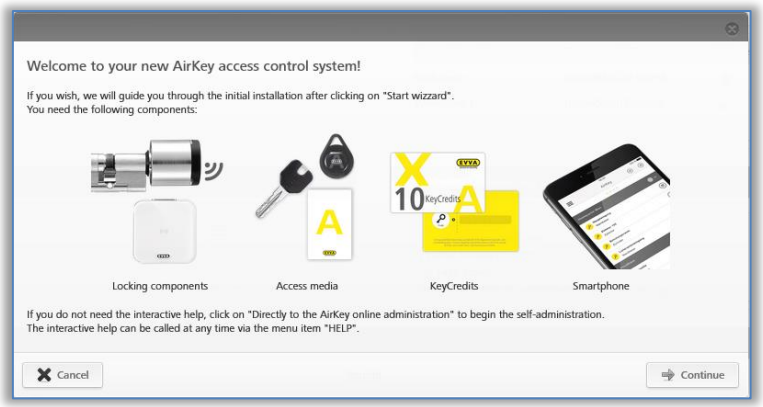


Figur 8: AirKey-systemets startsida

På startsidan Home visas en översikt av alla uppgifter som är relevanta för systemet. Från denna sidan administrerar man systemet.

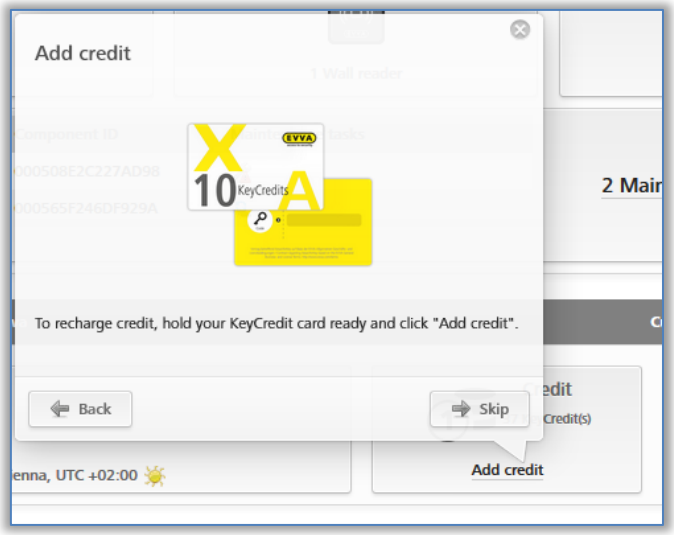
4.4 Interaktiva hjälpen

AirKey-onlineadministration startar den interaktiva hjälpfilen när man har loggat in för första gången för vägledning genom systemet och förklara de viktigaste funktionerna.



Figur 9: Interaktiv hjälp

Det exempel som visas här är funktionen "fylla på kredit". Den interaktiva hjälpen visar vilka knappar man ska klicka på och vilka uppgifter som ska definieras i fälten. Man kan bläddra fram och tillbaka inom den interaktiva hjälpen.



Figur 10: Interaktiv hjälp – fylla på kredit

Man kan välja att stänga den interaktiva hjälpfilen och lära känna AirKey-onlineadministrationen med hjälp av systemmanualen.

Vill man öppna den interaktiva hjälpen igen välj ***Hjälp*** → ***Interaktiva hjälpen*** i huvudmenyn. Man kan starta om den interaktiva hjälpen hur många gånger och när som helst.

4.5 Installation av kodningsstation

Option

AirKey-kodningsstation är en kompletterande enhet för initiering samt uppdatering av enheter och medier i systemet.

4.5.1 Användning av kodningsstationen via AirKey-onlineadministration

Applikationen som installeras för kodstationen har den fördelen att den är kompatibel med alla aktuella webbläsare. Kodstationen kan även användas för att uppdatera låskomponenter och medier efter utloggning från AirKey-onlineadministrationen.

Det är endast möjligt att lägga till och ta bort låskomponenter i ett låssystem samt att uppdatera den inbyggda programvaran för låskomponenter eller göra Keyring-uppdateringar av tillträdesmedier efter inloggning till AirKey-onlineadministrationen. Uppdateringar av medier och låskomponenter är möjligt även efter utloggning från AirKey-onlineadministrationen eller när webbläsaren har stängts.

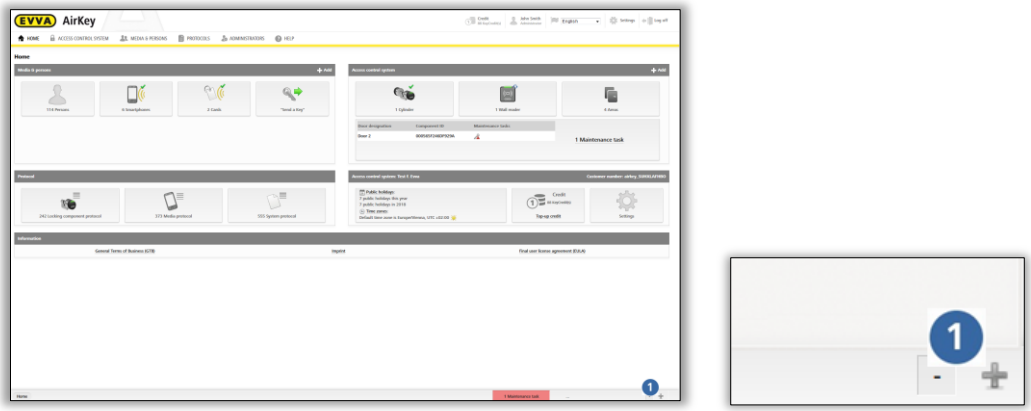
Följande webbläsare stöder kommunikation mellan AirKey-onlineadministration och den lokala kodningsstationen: Chrome, Firefox och Edge.

Nedladdningen och användningen av kodningsstationen är webbläsar-/operativsystem-specifikt. Illustrationen i din webbläsare kan skilja sig åt från bilden här (Firefox).

Registrera och logga in på AirKey-onlineadministration (se kapitel Registrering av AirKey-onlineadministration).

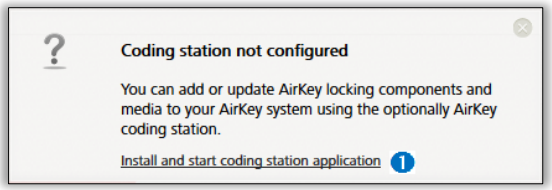
> Anslut kodningsstationen till en USB-port i datorn.

> Klicka på symbolen + längst ned till höger i AirKey-onlineadministration ❶.



Figur 11: Kodningsstation – installation av applikationen

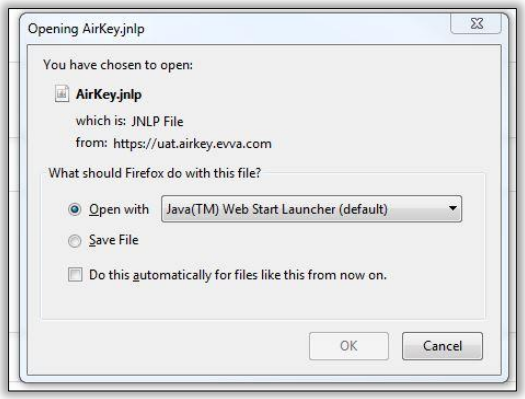
> Klicka därefter på länken "Installera och starta kodningsstationsapplikationen" ❶ för att installera applikationen för kodningsstationen.



Efter att klickat på länken har man 60 sekunder på sig att öppna filen AirKey.jnlp (se Fortsätt steg). Överskrids tiden måste man upprepa installationen från detta steg. Alternativt, spara filen AirKey.jnlp och öppna den manuellt.

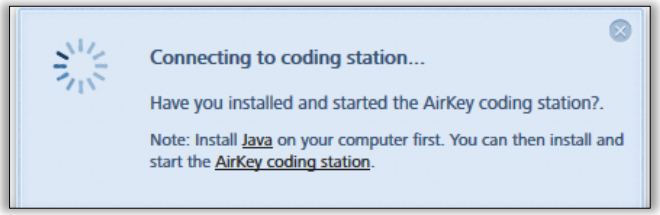
Figur 12: Installera och starta kodningsstationsapplikationen

> Dialogen för nedladdning av AirKey.jnlp visas. Öppna filen med "Java(TM) Web Start Launcher".



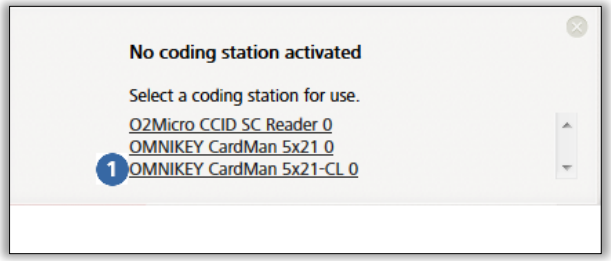
Figur 13: Öppna filen AirKey.jnlp

> Efter att filen öppnats upprättas en anslutning till kodningsstationen.



Figur 14: Upprätta en anslutning till kodningsstationen

> Välj tillgänglig kodningsstation (t.ex. "OMNIKEY CardMan 5x21-CL 0" ❶) från listan.



Figur 15: Välja kodningsstation

> En AirKey-symbol visas i aktivitetsfältet längst ned till vänster – kodningsstationen har installerats korrekt och är aktivt.

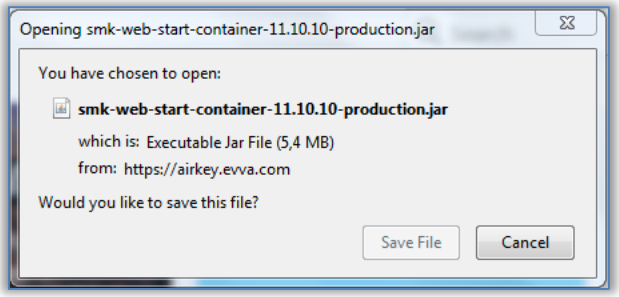
Figur 16: AirKey-symbol i aktivitetsfältet

4.5.2 Användning av kodningsstationen via kommandoraden

Mjukvaran för kodstationen kan installeras och konfigureras via kommandotolken på datorn. (För det här alternativet krävs mer omfattande IT-kunskaper, framför allt kring kommandotolken.)

Via kommandoraden kan kodningsstationen endast användas för uppdatering av tillträdesmedier och låskomponenter. Uppdatering av låskomponenternas firmware kan endast ske via webbläsaren eller med en smarttelefon med underhållsbehörighet.

> Hämta kodstationsappen via länken https://airkey.evva.com/smkrest/jnlp/newest-jar-file/ och spara den i önskad mapp.



Figur 17: Ladda ner applikationen för kodstationen

> Öppna kommandotolken och navigera till den mapp där kodstationsapplikationen finns sparad.

> Starta kodningsstationsapplikationen med följande kommando:

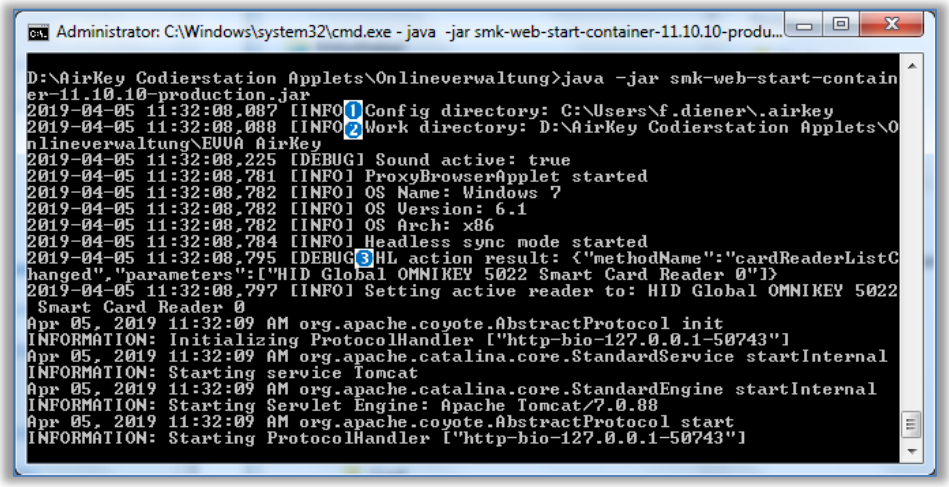
`java -jar <filnamn>`
(t.ex. `web-start-container-customer-15.10.0-8.jar`)

Dessutom kan du ange följande valfria parametrar:

- **`-reader "<namn på kodningsstationen>"`**: Med denna parameter kan en bestämd kodningsstation användas (t.ex. "HID Global OMNIKEY 5022 Smart Card Reader 0"). I detta fall ignoreras konfigurationsfilen `config_customer.json`.
- **`-port <VÄRDE [1024-65535]>`**: Om denna parameter inte anges används porten 50743 som standard. Porten 50743 används även när kodningsstationen används via AirKey-onlineadministration i webbläsaren. Om du vill använda flera kodningsstationer parallellt på en dator måste du ange en egen port för varje kodningsstation. Med parametern "**`-port 0`**" används en slumpmässig port.
- **`-configDir <VÄRDE>`**: I den angivna mappen (standardvärde för Windows: `%USERPROFILE%\.airkey`) sparas konfigurationsfilen `config_customer.json`. Denna genereras automatiskt när kodningsstationsapplikationen startas första gången och de senast använda inställningarna sparas.
- **`-workDir <VÄRDE>`**: I den angivna mappen skapas t.ex. loggfilen `logs\application.log` när kodningsstationsapplikationen startas. I denna protokollförs alla åtgärder som genomförts med kodningsstationsapplikationen. Om du använder flera kodningsstationer parallellt rekommenderar vi att du använder en egen mapp för varje kodningsstation.

- **`-version`**: Visar kodstationsappens version.
- **`-help`**: Öppnar hjälpen och beskriver alla tillgängliga parametrar.

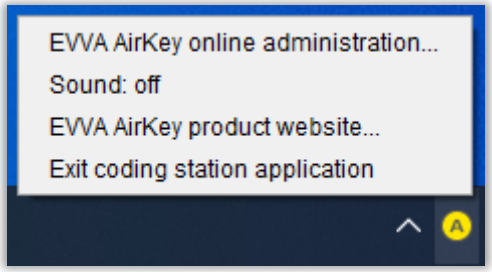
> Nederst till höger i aktivitetsfältet visas AirKey-ikonen och på kommandoraden visas information om konfigurationsmappen ❶, arbetsmappen ❷ och de tillgängliga kodstationerna ❸.



Figur 18: Starta kodstationsappen från kommandoraden

4.5.3 Konfigurera kodningsstationsapplikationen

Högerklicka på AirKey-symbolen för att öppna motsvarande kontextmeny.



Figur 19: Konfigurera kodningsstationsapplikationen

Lista över motsvarande menypunkter:

> ***EVVA AirKey-onlineadministration...*** – öppna länken till inloggningssidan för AirKey-onlineadministration.

> ***Ljud: på*** – när komponenter uppdateras med en kodningsstation avges ett pipljud. Hörbara återkopplingssignaler rekommenderas om kodningsstationen används utan AirKey-onlineadministration. Klicka på ***Ljud: på*** så växlar alternativet till ***Ljud: av***.

> ***Ljud: av*** – ingen signalton avges. Klicka på ***Ljud: av*** så växlar alternativet till ***Ljud: på***.

> ***EVVA-AirKey-produktwebbplats...*** – länk till sidan med AirKey-produkter

> ***Avsluta kodningsstationsapplikationen*** – avslutar applikationen för kodnings-stationen.

4.5.4 Lösningar på möjliga problem med kodningsstationen

LED listen indikerar att kodningsstationen är driftklar och ansluten. Koppla från och koppla in kodningsstationen igen om den inte indikerar driftberedskap. Man kan behöva installera om kodningsstationens drivrutiner.

Den lokala applikationen för kodningsstationen stängs automatiskt när datorn stängs av. Skapa en genväg för att automatiskt starta applikationen när du startar dator med Java™ kontrollpanel (konfigurera Java, applikation: AirKey kortläsare proxy; typ: applikation) och spara i mappen Autostart.

Kodningsstationsapplikationen avslutas efter start

Kodningsstationsapplikationen använder som standard port 50743 för kommunikation med webbläsaren. Om denna port används av ett annat program kan kodningsstations-applikationen inte startas. I Windows 10 eller högre kan denna port användas av Hyper-V. Du kan förhindra att Hyper-V använder den här porten på följande sätt:

- Avaktivera Hyper-V:
  ```
  C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V
  ```
- Starta om datorn.
- Lägg till ett undantag för port 50743:
  ```
  C:\> netsh int ipv4 add excludedportrange protocol=tcp startport=50743
       numberofports=1
  ```
- Återaktivera Hyper-V:
  ```
  C:\> dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All
  ```
- Starta om datorn.

Kortläsaren "Microsoft UICC" har valts som kodningsstation.

Figur 20: Kortläsare "Microsoft UICC" i AirKey-onlineadministration

Som lösning kan kortläsaren UICC avaktiveras i enhetshanteraren i Windows:
Enhetshanteraren → Programvaruenheter → Microsoft UICC ISO Reader → Inaktivera enhet

Det går inte att upprätta anslutning till kodningsstationen via AirKey-onlineadministration (https-proxy)

Både AirKey-onlineadministration och kodningsstationsapplikationen kommunicerar krypterat med AirKey-systemet via port 443. I nätverk som använder https-proxy kan det dock vara nödvändigt att definiera ett undantag för "airkey.evva.com" och subdomäner, eftersom kodningsstationsapplikationen kontrollerar servercertifikatet med "certificate pinning" och därmed inte tillåter https-proxyservrar.

Anslutningen till kodningsstationen kan inte upprättas via AirKey-onlineadministration (DNS-rebindingsskydd)

AirKey-onlineadministration kommunicerar lokalt mellan webbläsaren och kodningsstations-applikationen. Åtgärder som att skapa låskomponenter eller tillträdesmedier på kodnings-stationen visas i AirKey-onlineadministration.

Webbläsaren ansluter till kodningsstationsapplikationen via "components.airkey.evva.com" (port 50743). Denna URL löses upp av DNS-servern som 127.0.0.1.

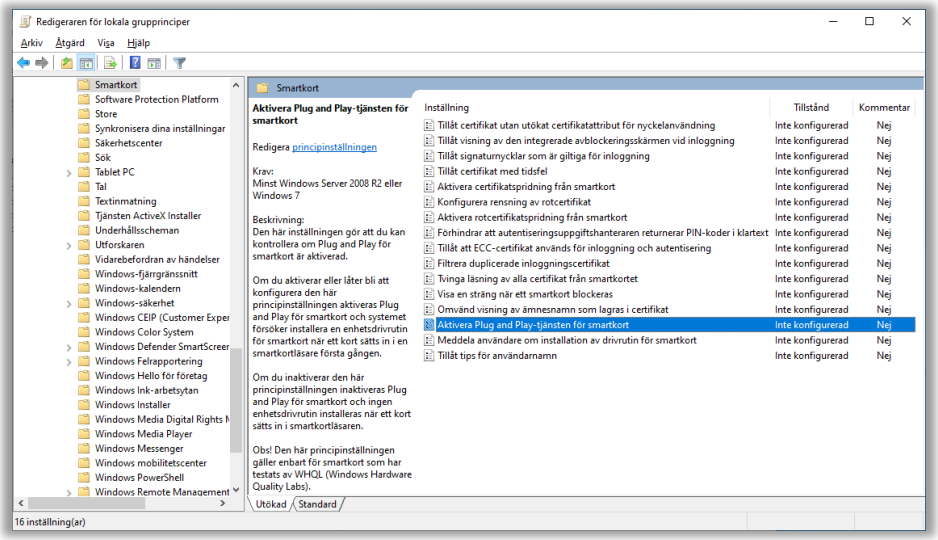
Därför kan det vara nödvändigt att lägga till undantag för "components.airkey.evva.com" och subdomäner från "airkey.evva.com" när DNS-rebindskyddet är aktivt.

Windows söker upprepade gånger efter drivrutinen för kodningsstationen

När en låskomponent eller ett tillträdesmedium placeras på kodningsstationen försöker Windows söka efter och installera en drivrutin för kodningsstationen. Detta kan påverka kommunikationen med kodningsstationen och leda till funktionsfel.

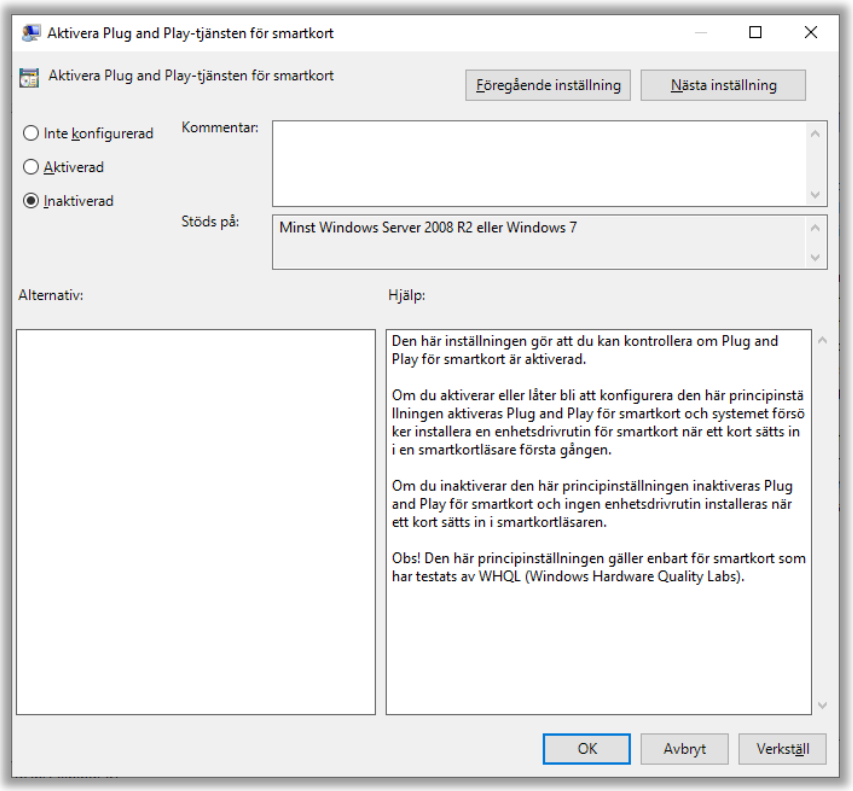
Som lösning kan tjänsten Smartcard-Plug & Play från Windows avaktiveras:

- Windows-knapp + R
- Ange "gpedit.msc" och bekräfta med ***Enter***.
- Program "Redigeraren för lokala grupprinciper" ⟶ Datorkonfiguration ⟶ Administrativa mallar ⟶ Windows-Komponenter ⟶ Smartkort
- Dubbelklicka på raden med posten "Plug & Play-tjänst för smartkort" till höger.



Figur 21: Redigeraren för lokala grupprinciper

- Välj radioknappen ***Inaktiverad***.
- Bekräfta med ***OK***.



Figur 22: Plug & Play-tjänsten för smartkort

För MacOS 11.x eller högre kan ingen kodningsstation väljas

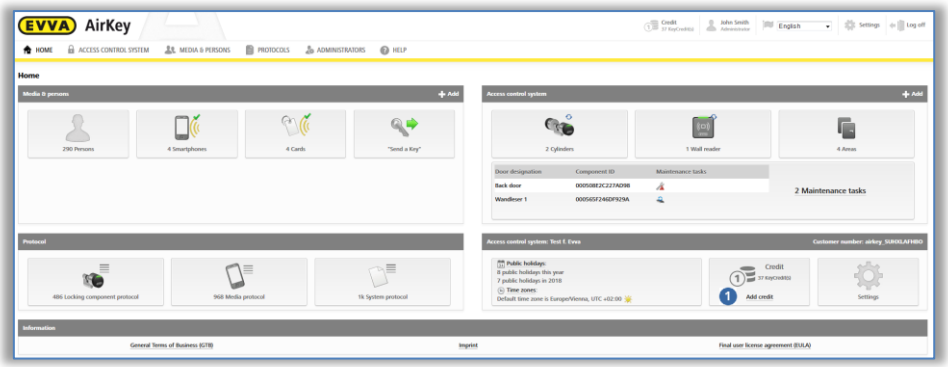
Sedan MacOS Big Sur (11.x) kan man inte längre välja en ansluten kodningsstation på en Mac via AirKey-onlineadministration. Kodningsstationsapplikationen startas visserligen utan problem, men ingen kodningsstation visas i AirKey-onlineadministration.

Som lösning kan kodningsstationen startas via kommandoraden (se kapitel Användning av kodningsstationen via kommandoraden). En förutsättning för detta är dock att Java-versionen JDK17 (Oracle JDK17 eller OpenJDK17) eller högre är installerad.

4.6 Fylla på kredit

För att fylla på kredit behövs ett KeyCredit-kort. På baksidan finns ett skrapfält med en kreditkod.

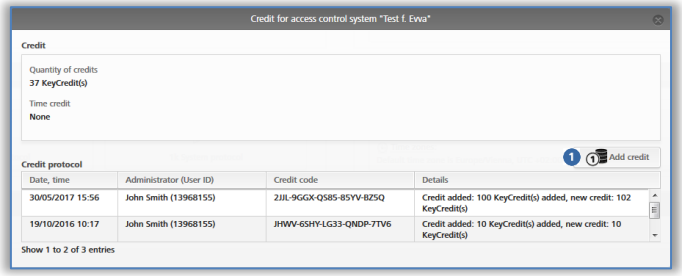
> På startsidan ***Home*** välj knappen ***Fylla på kredit***.
> Alternativt klicka på ***Kredit*** i sidhuvudet.



Figur 23: Kredit

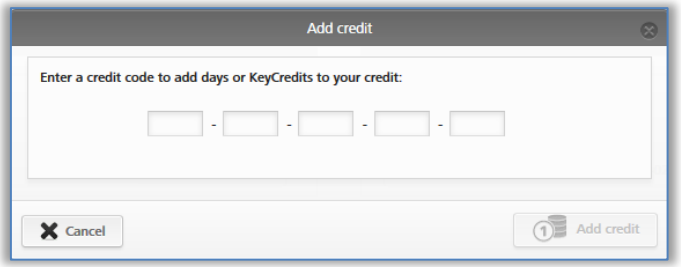
> På displayen visas en översikt av aktuell kredit och eventuella tidigare påfyllningar.

> Klicka på knappen ***Fylla på kredit*** ❶.



Figur 24: Fylla på kredit

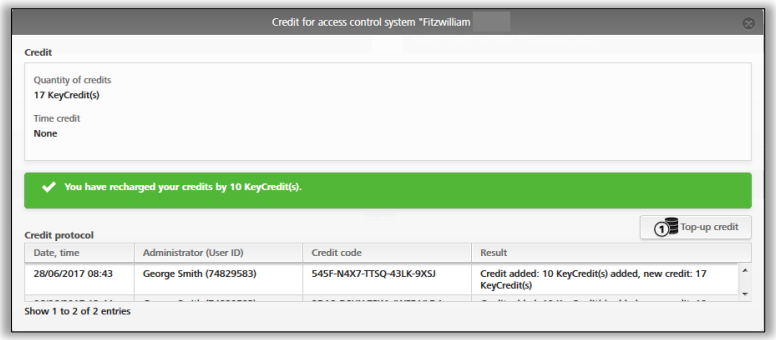
> Ange koden som skrapats fram på KeyCredit-kortet i applikationsfönstret "Fylla på kredit".



Figur 25: Ange kreditkoder

> Klicka på ***Fylla på kredit***.

Är koden korrekt bekräftar systemet de inmatade uppgifterna och fyller på krediten.

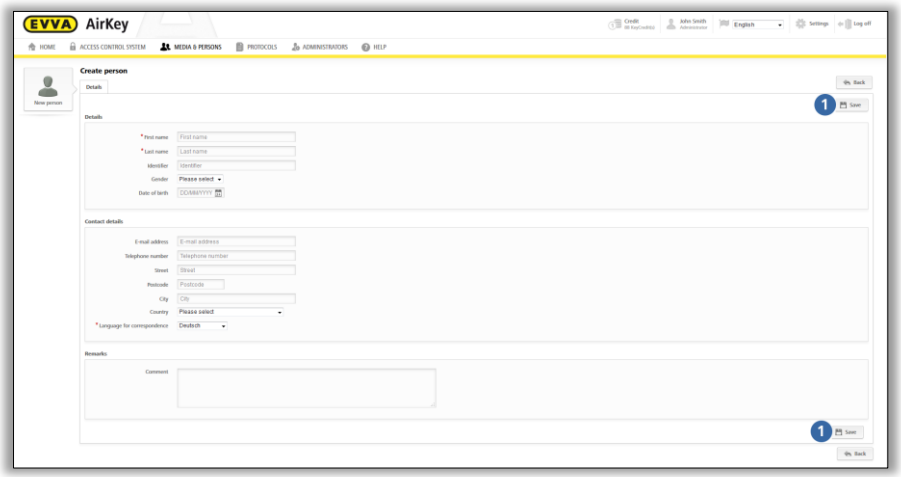


Figur 26: Fylla på kredit

4.7 Skapa personer (användare)

Varje person som ska tilldelas behörighet till AirKey-systemet måste först skapas.

- På startsidan ***Home*** i det grå fältet i avsnittet ***Medier och personer*** klicka ***Lägg till*** → ***Skapa person***.
- Alternativt gå till startsidan ***Home*** och välj ***Personer*** → ***Skapa person***.
- Man kan välja ***Medier och personer*** → ***Skapa person*** i huvudmenyn.
- Eller också klicka på knappen **"*Send a Key*"**och därefter på ***Skapa ny***. Med den här funktionen skapas personer som använder smarttelefon.
- Fyll i fälten i formuläret. Fält som är markerade med * är obligatoriska.
- Klicka på ***Spara*** ❶.



Figur 27: Skapa personer

Fälten med förnamn / efternamn / ID ger en unik kombination inom AirKey-systemet.

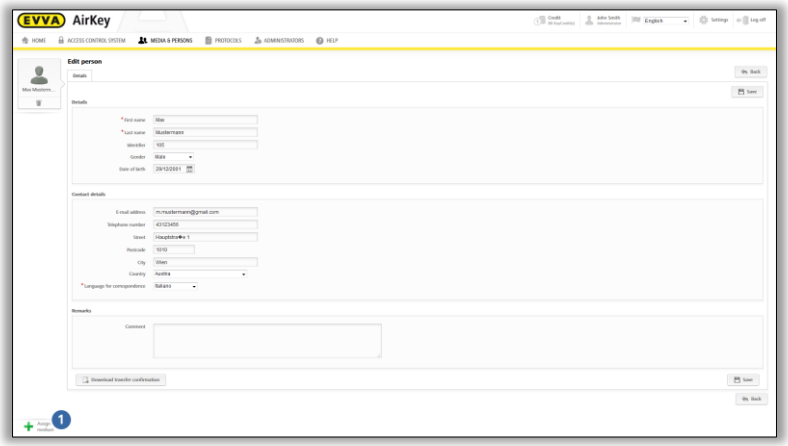
Om man använder fältet "ID" ska man ange ett värde som säkerställer att kombinationen av för- och efternamn är unik (t.ex. personalnummer). OBS ! Detta är viktigt om det finns personer med samma för- och efternamn.

I fälten för e-postadress, telefonnummer, adress, postkod och ort kan man ange högst 50 tecken. "Postnummer" kan innehålla högst 10 tecken. Teckenbegränsningen för texter i kommentarfältet är 500.

Om kombinationen som angetts redan finns kommer systemet att visa meddelandet "Personen finns redan".

- Kontrollera eller korrigera inmatade uppgifter.
- Klicka på ***Spara***.

Har en ny användare skapats visar systemet en bekräftelse och en ny knapp visas under namnet, ***Tilldela medium*** ❶.

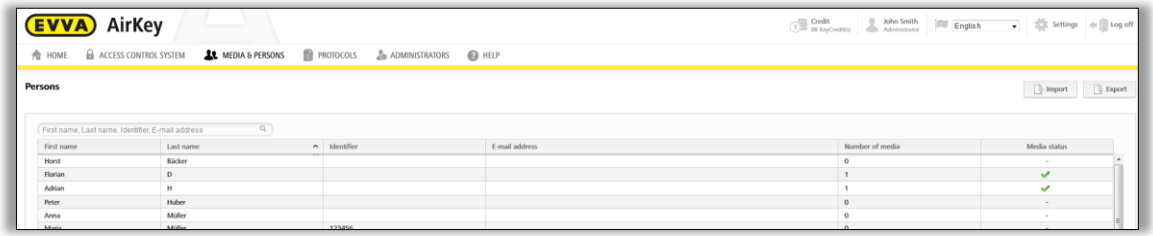


Figur 28: Tilldela medier

En ny användare har nu skapats AirKey-systemet och visas på listan över personer.

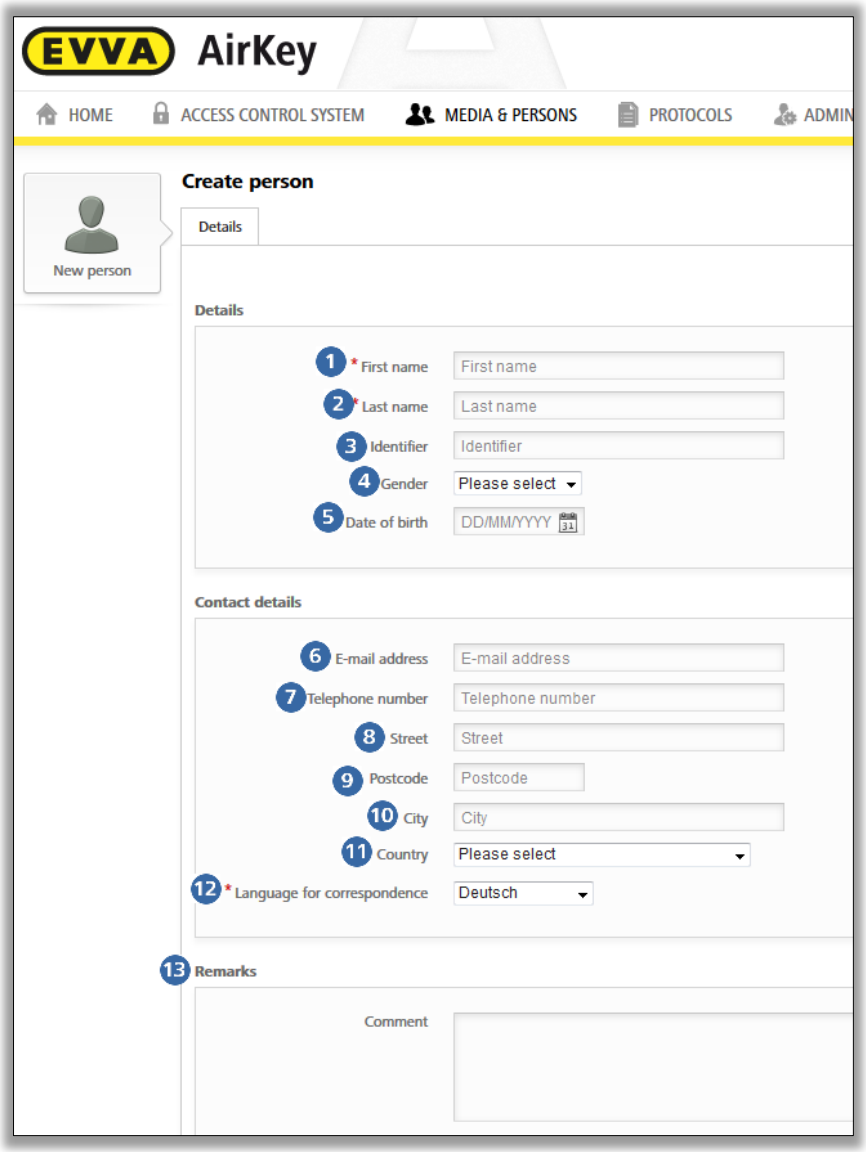
4.7.1 Importera personuppgifter

Personer/användare för AirKey kan även skapas i externa filer. I detta fall behövs en motsvarande CSV-fil för att importera till AirKey-onlineadministration.

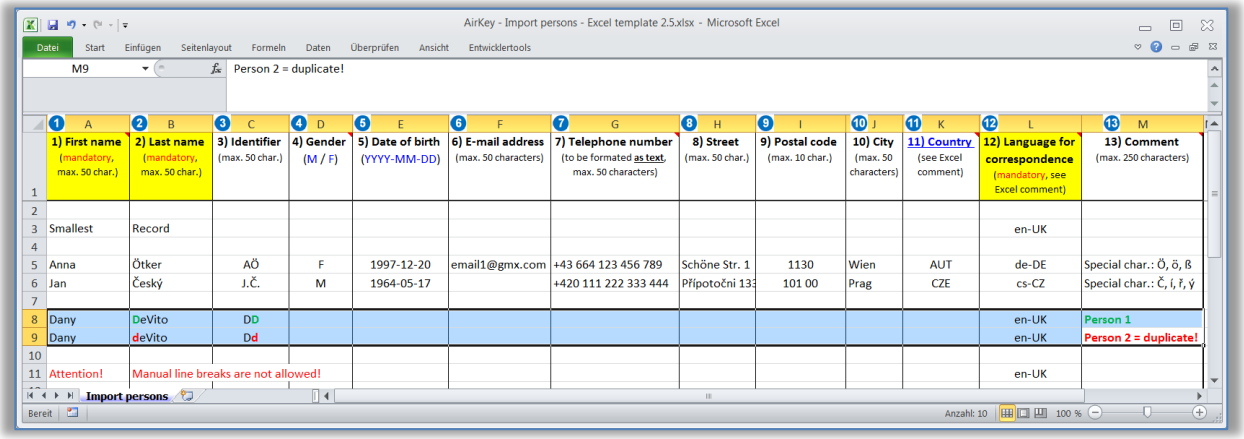


Figur 29: Importera personlista

Parametrarna för tabellen med personuppgifter är identiska med avsnittet ***Skapa person*** i AirKey-onlineadministration, dvs. kolumnen A är förnamnet ❶, kolumnen B är efternamnet ❷, kolumnen C är lösenordet ❸, etc. CSV-filen importeras till AirKey-onlineadministration i denna fas.



Figur 30: Importera personer – personlista



Figur 31: Importera personer – fält i personlistan

CSV-filens egenskaper med personuppgifter för import:

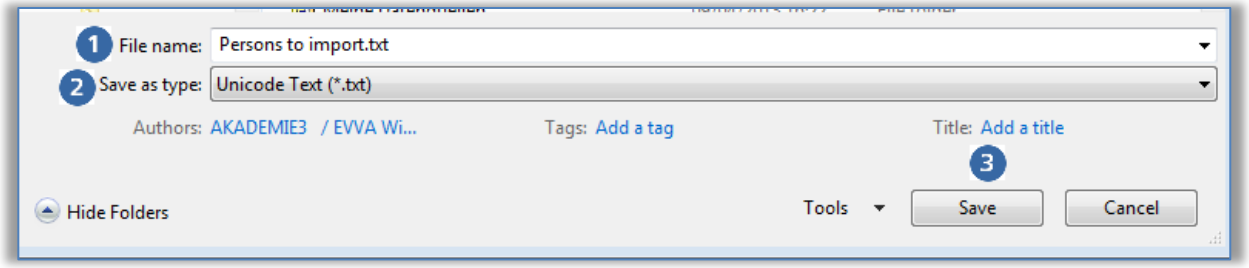
- Den första raden ignoreras alltid. Av denna anledning rekommenderar vi att man anger fältnamnen i denna rad för att underlätta identifieringen av återstående uppgifter. Man kan låta den första raden vara tom. Den får dock inte innehålla personuppgifter eftersom dessa i så fall inte importeras.
- Tomma rader eller rader med endast mellanslag och tabbstopp (blanksteg) ignoreras också. Alltså lämna ett valfritt antal blanksteg om man vill ha mer transparens i CSV-filen.
- Varje fil måste innehålla alla 13 fält (attribut) som visas i Figur 30.
- Fält är separerade med semikolon.
- Det finns endast tre obligatoriska fält: förnamn (fält 1), efternamn (fält 2) och språk för korrespondens (fält 12).
- Om återstående fält inte innehåller uppgifter måste de ändå finnas tillgängliga som tomma fält (;;).
- Fältet för kön (fält 4) får endast innehålla värdet **M** (för *man*) eller **F** (för *kvinna*) eller lämnas tomt. Detta gäller alla språk och M och F ska anges i versaler.
- Ange födelsedatumet (fält 5) i formatet **ÅÅÅÅ-MM-DD** (t.ex. 1997-12-20).
- E-postadressen (fält 6) måste innehålla tecknet **@** inklusive andra tecken eller lämnas tom.
- Landet för adressen (fält 10) måste innehålla den 3-siffriga ISO-3166-1-koden (kolumnen alpha-3) för respektive land eller lämnas tom. Använd endast stora bokstäver för att ange koden. Exempel: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL, etc.
- Fältet för att specificera språket för korrespondens (fält 12) är obligatoriskt och måste innehålla ISO-koden för språket. Observera den exakta stavningen med stora/små bokstäver. Endast följande koder accepteras: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- En person som ska importeras visas som redan tillgänglig (symbol ⚠) om kombinationen förnamn + efternamn + användar-ID (fält 1-3) redan finns i AirKey-online-administration, även om återstående fält (fält 4-13) skiljer sig åt. Dessa personer importeras inte. Systemet skiljer inte mellan gemener och versaler vid namn ("Danny;**D**eVito;D**D**" och "Danny;**d**eVito;D**d**" till exempel, tolkas som samma person och endast det första alternativet importeras).
- Personer tolkas som dubbletter inom CSV-filen om kombinationen av förnamn + efternamn + användar-ID (fält 1-3) redan finns, även om återstående fält (fält 4-13) skiljer sig åt. I detta fall visas endast den första raden med en viss kombination innan den importeras. Eventuella dubbletter ignoreras och visas inte i tabellen över personer som ska importeras.
- En CSV-fil får innehålla data för max. 10 000 personer. Om du vill importera fler personer skapar du flera CSV-filer som du kan importera separat.
- Felaktiga rader i CSV-filen är markerade med symbolen ✖ och läggs till i verktygstipsen där alla fel beskrivs före import. Dessa rader importeras inte.
- Alla korrekta rader markeras med symbolen ✔ innan de importeras, oavsett om det finns eventuella felaktiga rader.

Teckenkodningen i CSV-filen måste var UTF-8 för att landspecifika bokstäver (Ä, ß, ç, Ñ, č etc.) ska kunna visas korrekt. Hur man skapar en CSV-fil i UTF-8-format beskrivs detaljerat nedan.

Skapa en CSV-fil i UTF-8-format

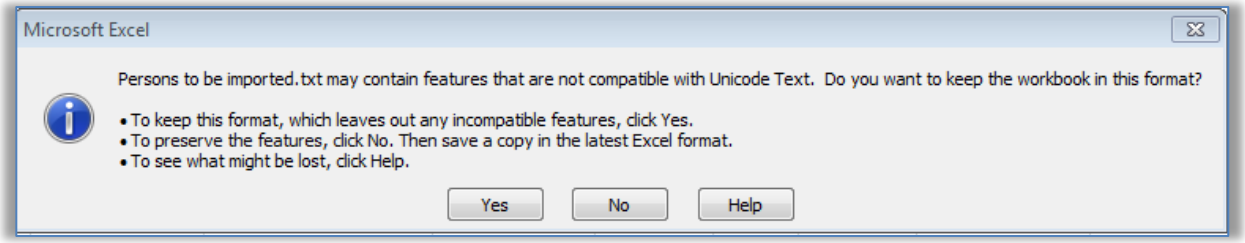
Följande beskrivning gäller för Windows 10™ vid användning av Microsoft Excel™ och de hjälpprogram som redan finns på Windows 10™. På andra Windows-versioner eller operationssystem kan man skapa en CSV-fil i UTF-8-format på liknande sätt. Nödvändiga steg:

- Denna beskrivning utgår från en Excel-tabell som innehåller uppgifterna för de personer som ska importeras.
- I Excel-tabellen är det viktigt att spalt 7 (telefonnummer) är formaterad som text. Om den är formaterad som tal kommer ledande tecken som "+" och "0" (noll) att gå förlorade. Mellanslag inom telefonnummer är dock tillåtna och ger bättre översikt i AirKey-onlineadministration.
- Kontrollera med hjälp av sökfunktionen i Excel att tabellen inte innehåller något av följande tecken:
  - " (dubbla, raka citattecken)
  - ; (semikolon = skiljetecken i den CSV-fil som ska importeras till AirKey-onlineadministration)
- Excel kan inte spara uppgifterna direkt i UTF-8-format. Därför måste uppgifterna först sparas i Unicode-format.
- Detta gör du genom att gå till menypunkten ***Fil*** → ***Spara som*** i Excel (eller tryck på tangenten F12).
- I dialogfönstret "Spara som" som öppnas anger du önskat filnamn ❶.
- I rullgardinslistan ***Filtyp*** ❷ väljer du formatet ***Unicode Text (*.txt)***.
- Klicka på ***Spara*** ❸.



Figur 32: Excel – Spara som – "Unicode Text (*.txt)"

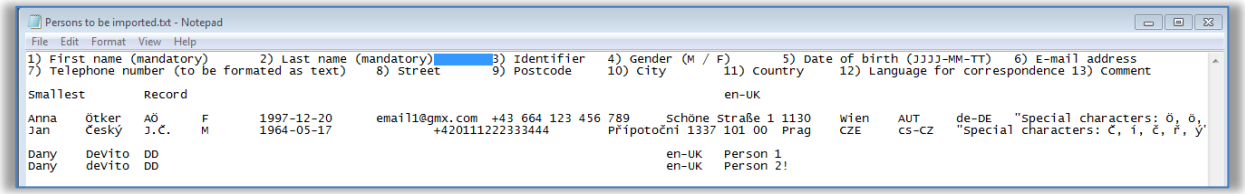
- Bekräfta sedan Excel-frågan gällande "Unicode Text" med ***Ja***.



Figur 33: Excel – Spara som "Unicode Text (*.txt)"

> Öppna den genererade filen (*.txt) i en textredigerare. Windows™ använder som standard programmet ***Editor***.

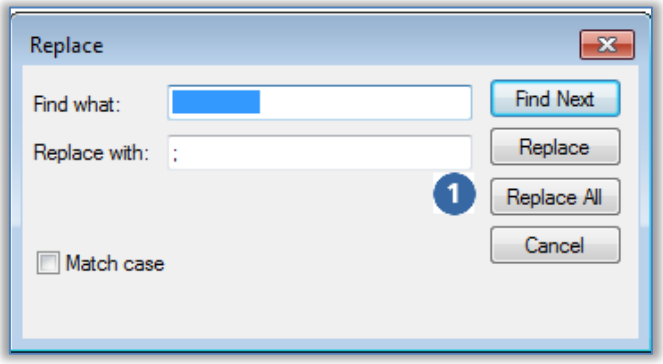
> Skiljetecken i Unicode-textfilen är tabulatorn. Alla tabulatorer måste ersättas med semikolon (;). Detta gör du genom att först markera en tabulator mellan två fält och kopiera den.



Figur 34: Textfilen i "Editor" – markera en Tabulator och kopiera den i urklipp

> I ***Editor*** går du till menypunkten ***Redigera*** → ***Ersätt*** för att öppna dialogfönstret "Ersätt".

- I fältet ***Sök efter*** infogar du tabulatortecknet ur urklipp, eftersom detta tecken inte kan anges direkt här.
- I fältet ***Ersätt med*** anger du ett semikolon (;).
- Klicka på ***Ersätt alla*** ❶.

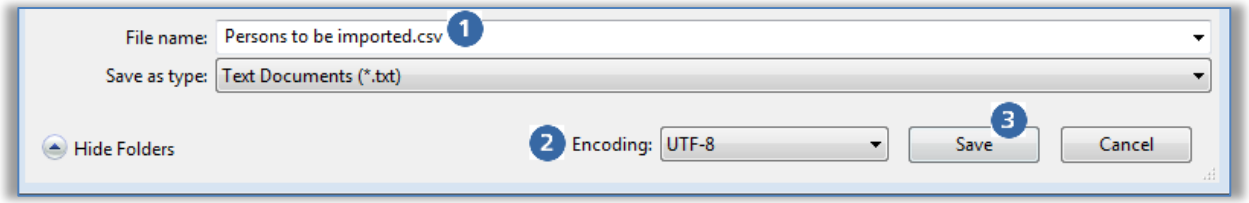


Figur 35: "Editor" – ersätt alla tabulatorer med semikolon

> Stäng dialogfönstret "Ersätt", gå till ***Editor*** och öppna menypunkten ***Redigera*** → ***Spara som*** för att öppna dialogfönstret "Ersätt".

- Ändra filändelsen manuellt från .txt till .csv i fältet ***Filnamn*** ❶. Att ändra ändelsen senare är krångligare!
- I rullgardinslistan ***Kodning*** ❷ väljer du formatet ***UTF-8***.

- Klicka på ***Spara*** ❸.



Figur 36: "Editor" – Spara som – Ange filändelsen .csv manuellt och välj UTF-8-kodning

> Den CSV-fil som sparats på detta sätt kan därefter importeras i AirKey-onlineadministration.

CSV-filen kan öppnas direkt med Excel. Genomför INGA ändringar av CSV-filen i Excel eftersom det kommer att ändra UTF-8-kodningen när du sparar!

Mindre ändringar av personuppgifter i efterhand kan genomföras i CSV-filen, t.ex. genom att öppna denna i ***Editor*** och sedan spara den igen.

Om du vill genomföra större ändringar av personuppgifterna rekommenderar vi att du anpassar den ursprungliga Excel-filen och upprepar hela processen med att skapa CSV-filen i UTF-8-format.

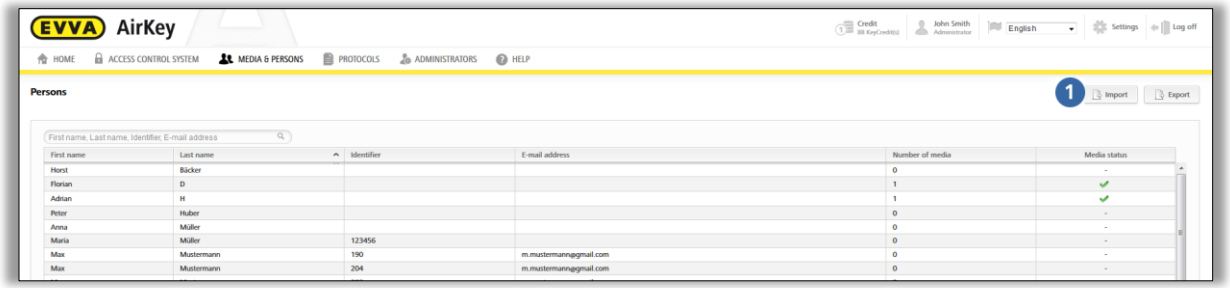
Importera CSV-filen i UTF-8-format i AirKey-onlineadministration

Gör på följande sätt för att importera en CSV-fil med personuppgifter:

> På startsidan ***Home*** välj rutan ***Personer***.

> Alternativt välj ***Medier och personer*** → ***Personer*** i huvudmenyn.

> Klicka på ***Importera*** ❶ på höger sida.



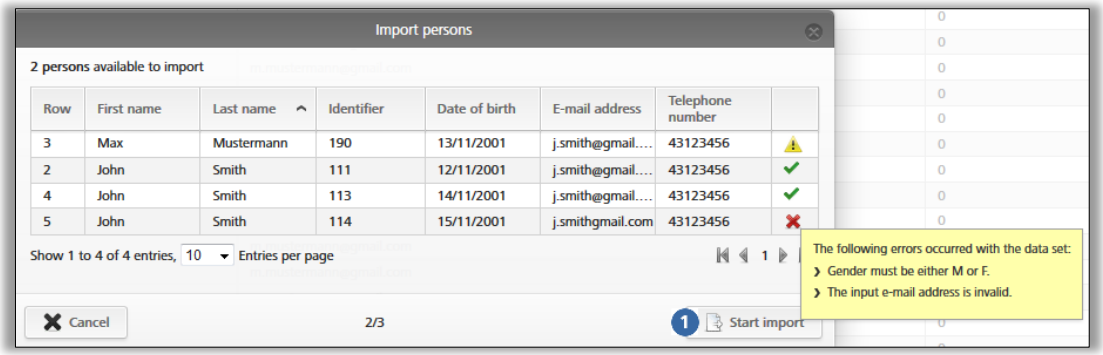
Figur 37: Importera personer

> Klicka på ***Välj fil***.

> Välj den CSV-fil som ska importeras.

> En översikt av de personer som ska importeras visas.

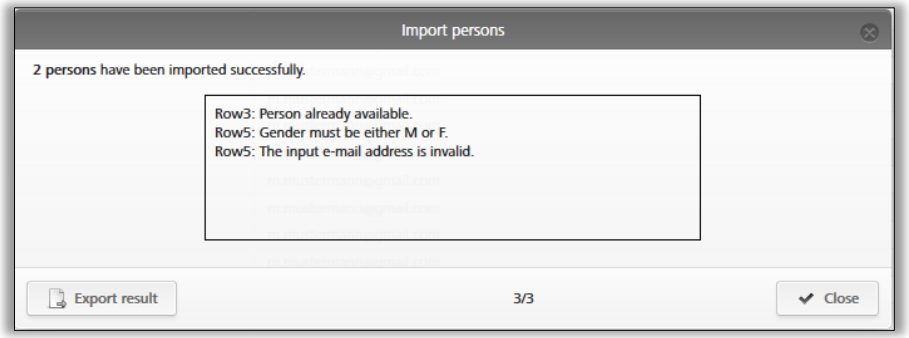
> Klicka på ***Starta import*** ❶.



Figur 38: Importera personer

> En rapport med antalet korrekt importerade personer och felaktiga rader visas.

> Klicka på ***Stäng***.



Figur 39: Importera personer – resultat

> AirKey-onlineadministration vidarebefordrar dig automatiskt till listan med en översikt av personer.

> Tilldela önskade behörigheter till motsvarande personer individuellt på det vanliga sättet som beskrivs i Tilldela medier till personer. Identiska tillträdesbehörigheter kan följaktligen dupliceras snabbt och enkelt. Mer information finns i Duplicera medier.

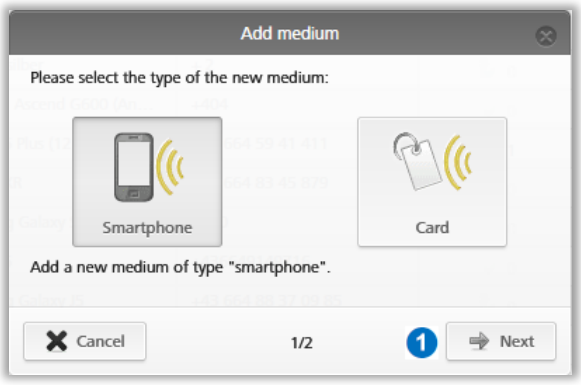
4.8 Skapa smarttelefoner

Innan man kan hantera smarttelefoner som del av ett AirKey-system måste de initieras i systemet.

> På startsidan ***Home*** i det grå fältet i avsnittet ***Medier och personer*** klicka på ***Lägg till → Lägg till medium***.

> Alternativt gå till ***Home*** och välj rutorna ***Smarttelefoner → Lägg till medium***.

> Man kan välja ***Medier och personer → Lägg till medium*** i huvudmenyn.



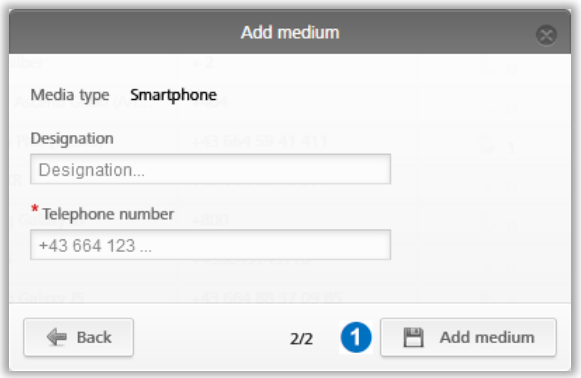
Figur 40: Ny smarttelefon eller kortmedium

> Välj ***Smarttelefon*** som nytt medium och klicka på ***Nästa*** ❶.

> Ange unik information (t.ex. typ av smarttelefon) i fältet "Beteckning".

> Ange smarttelefonens nummer. Telefonens nummer måste börja med **+** och landsnumret, och kan innehålla högst 50 tecken (+, 0-9 och mellanslag).

> Klicka på ***Lägg till medium*** ❶.

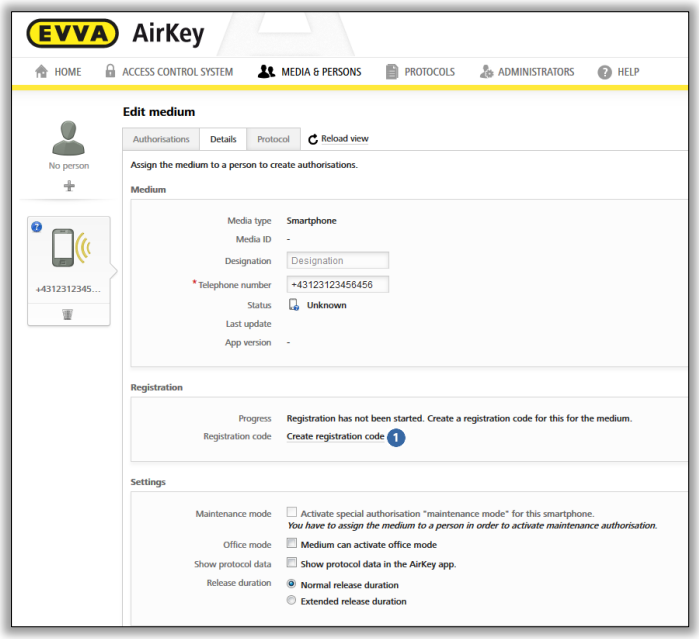


Figur 41: Lägg till nya medier

Om telefonnumret är ogiltigt eller redan har skapats visas ett felmeddelande.

Nu visas informationen för denna smarttelefon.

> Klicka på ***Skapa registreringskod*** ❶ för att skapa den.

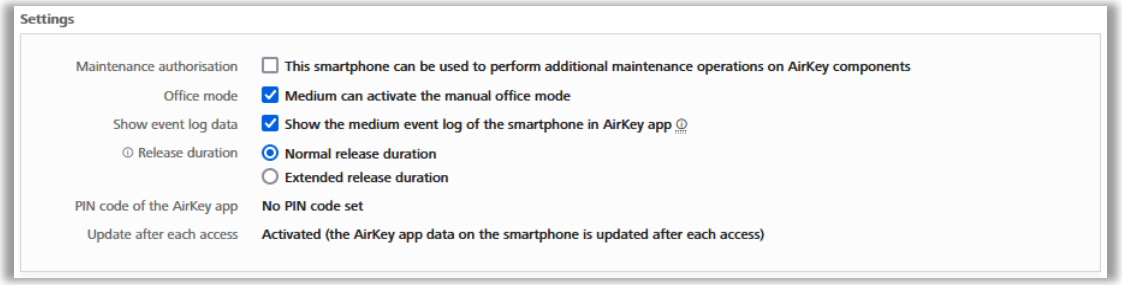


Figur 42: Skapa registreringskod

I avsnittet ***Registrering*** visas en giltig registreringskod och dess utgångsdatum. Man kan skicka det som textmeddelande (sms). Detta görs genom att klicka på motsvarande länk. Exakt datum och tid då registreringskoden skickades som textmeddelande (sms) visas.

Figur 43: Registreringskod

Ange följande parametrar under alternativet ***Inställningar*** i smarttelefonens detaljer:



Figur 44: Redigera medier – inställningar

- **Underhållsbehörighet:** Denna specialbehörighet kan endast aktiveras på en smarttelefon som redan har tilldelats en person. Med denna funktion har smarttelefoner behörighet att låsa upp AirKey-enheter i fabriksläget och att lägga till eller ta bort medier och AirKey-enheter i AirKey-system. När läget är aktiverat är det möjligt att uppdatera firmware för AirKey-enheter och behörigheter för användar media.

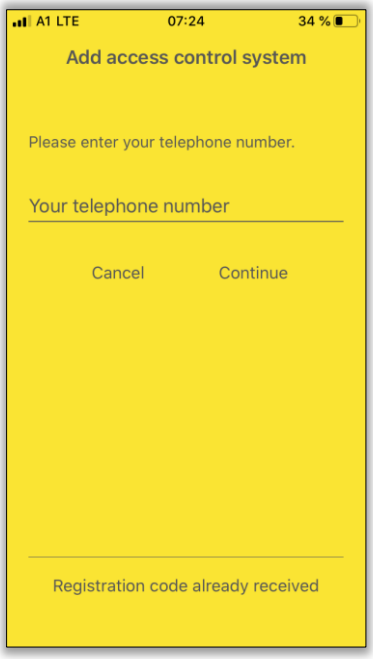
- **Detta medium får aktivera manuellt permanent öppning:** Välj detta alternativ för att tillträdesmedier ska kunna ställa in statusen automatiskt kontorsläge vid AirKey-enheten. Mediet måste dock ha tilldelats en giltig behörighet för motsvarande AirKey-enhet.
- **Visa medieloggen för smarttelefonen i AirKey-appen:** Detta alternativ visar personer deras egna tillträdeshändelser och andra uppgifter i händelseloggar som är relevanta för medierna i AirKey-appen.
- **Öppningstid:** Anger hur länge AirKey-enheten är upplåst (aktiverad) när denna smarttelefon används. Tiden på den normala eller utökade upplåsningstiden specificeras i AirKey-enheterna (från 1–250 sekunder).
- **Pinkod av AirKey-appen:** Visar om pinkod skyddet är aktiverat eller avaktiverat i AirKey-appen för denna smarttelefon. Om det är aktivt och personen har glömt sin pinkod kan den återställas här.
- **Uppdatering efter varje tillträde:** Anger om AirKey-appens data för smarttelefonen uppdateras automatiskt efter varjetillträde eller ej. Mer information om hur den här funktionen aktiveras finns i avsnittet Allmänt.

4.9 Registera smarttelefoner

När man har registrerat en smarttelefon i AirKey och erhållit registreringskoden kan telefonen aktiveras i systemet.

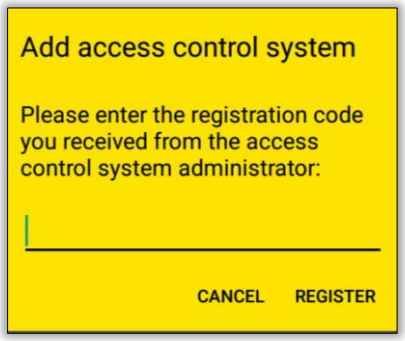
- Starta AirKey-appen på din smarttelefon.
- Godkänn licensavtalet samt frågor om åtkomst till specifika funktioner i smarttelefonen.
- Är smarttelefonen inte ansluten till ett låssystem, visas dialogen för inmatning av registreringskoden automatiskt.

På smarttelefoner med iOS väljer du ***Registreringskod redan mottagen*** för att hoppa över inmatningen av telefonnumret och gå till inmatningen av registreringskoden.



Figur 45: AirKey-app – lägga till låssystem (iOS)

> Ange registreringskoden som du fick från administratören av AirKey-låssystemet.



Figur 46: AirKey-app – lägga till låssystem (iOS)

> Klicka på ***Registrera*** för att bekräfta.

En enskild smarttelefon kan initieras i flera AirKey-system. Välj ***Inställningar*** → ***Lägg till låssystem*** i AirKey-appens huvudmenyn för att öppna registreringsdialogen igen. Mer information hittar du under Använd smarttelefonen i flera system.

Har registreringskoden har gått ut eller är ogiltig visas ett felmeddelande. Kontakta den AirKey-systemadministratör som skickat registreringskoden.

Radderar användaren AirKey-appen eller appens uppgifter, finns det möjlighet att återaktivera smarttelefonen utan att använda ytterligare krediter. Detta gäller dock endast för den specifika telefonen och det AirKey-system där telefonen är registrerad. Denna möjlighet gäller inte för en annan telefon (om telefonen byts ut).

- På startsidan ***Home*** välj rutan ***Smarttelefoner***.
- Man kan välja ***Medier och personer*** → ***Medier*** i (övre vänster hörn) av sidhuvudet.
- Välj den registrerade smarttelefonen översiktslistan.
- Klicka på ***Skapa en ny registreringskod*** och skicka registreringskoden till den person som vill koppla en smarttelefon till AirKey-systemet. Eller skicka den direkt via SMS till smarttelefonen.
- Ange registreringskoden i AirKey-appen så registreras smarttelefonen i systemet.

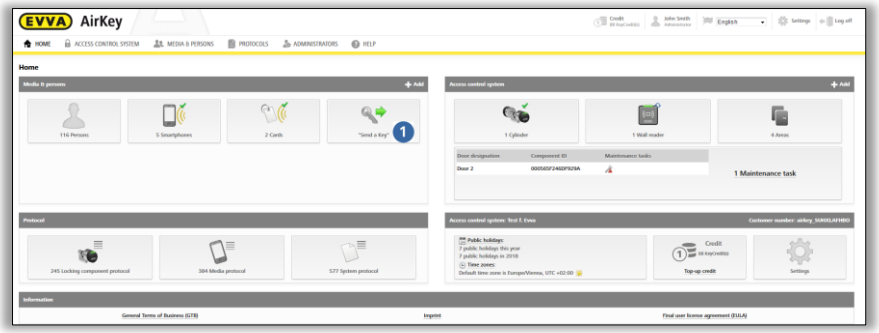
Är telefonen registrerad i ett AirKey-system och inte har radderats korrekt från detta system när appen raderades Visas ett medelande, att den är registrerad i ett annat system. Du kan registrera smarttelefonen som vanligt om du ignorerar meddelandet. Smarttelefonen skapas som ett nytt medium och alla tidigare uppgifter blir ogiltiga.

Vid behov av extra säkerhet, rekommenderar EVVA att använda en pinkod även på Appen. Koden erbjuder extra säkerhet och kan aktiveras eller avaktiveras i efterhand. Närmare information hittar du under Aktivera pinkod.

4.9.1 Funktionen "Send a Key"

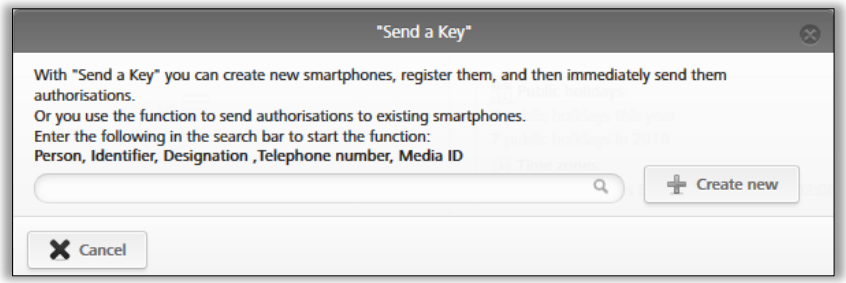
Alla personer som har en Android eller iPhone telefon kan ta emot en nyckel/behörighet. Administratörer kan i mjukvaran nyckel / behörighet per sms med funktionen "Send a Key" innehållande registreringskoden och en uppmaning att ladda ner appen AirKey.

- Klicka på knappen **"*Send a Key*"**.



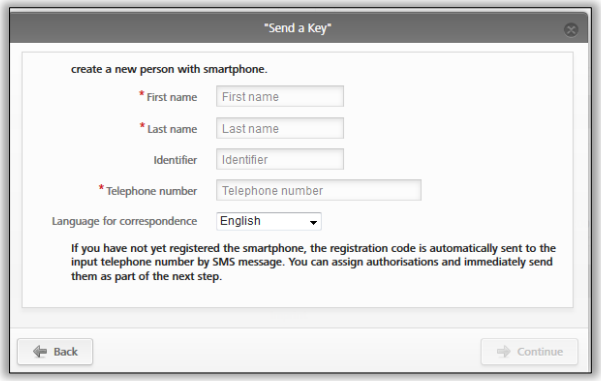
Figur 47: Send a Key

- Ange en persons namn, kod, etc. i sökfältet. Har denna användare ännu inte skapats välj ***Skapa ny***.



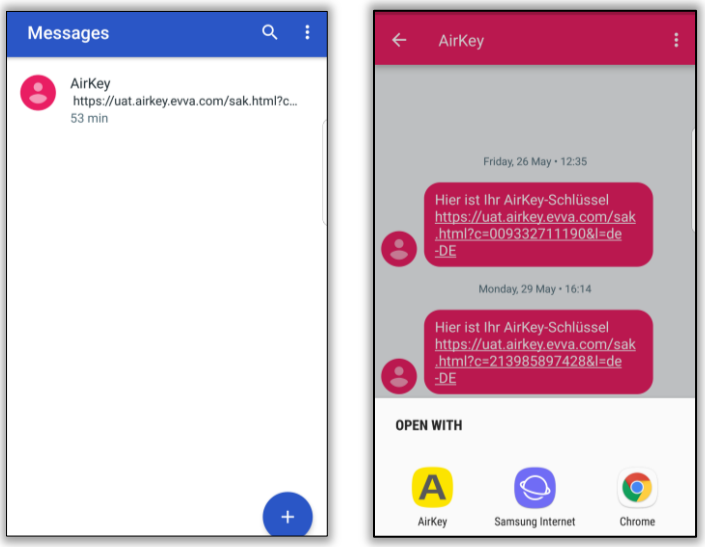
Figur 48: "Send a Key" – sökfält

> Klicka på ***Fortsätt*** när alla obligatoriska fält är ifyllda. Ett sms skickas genast till användaren med en länk till AirKey-appen för registrering till ett AirKey-system.



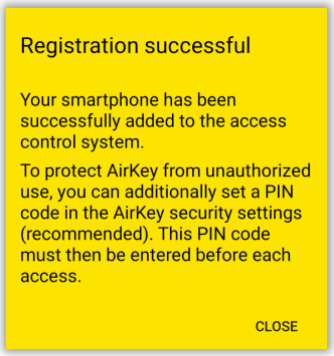
Figur 49: "Send a Key" – skapa användare

Beroende på smarttelefonens nätverkstillgänglighet kan det ta en stund innan sms:et med registreringskoden tas emot.



Figur 50: Sms:et med länk – visas här på en Samsung Galaxy S7 Edge

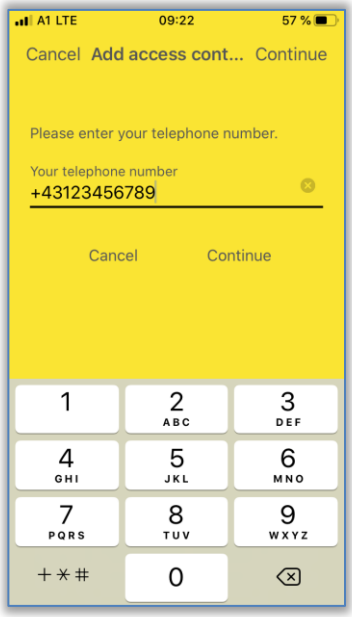
> När du öppnar länken i textmeddelandet med hjälp av AirKey startas och genomförs registreringen automatiskt.



Figur 51: Registrering genomförd

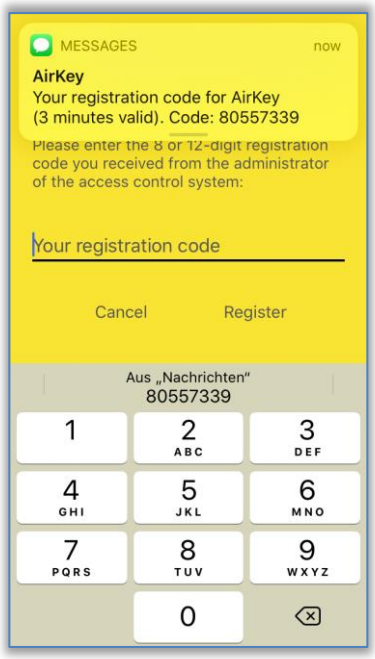
Är AirKey-appen inte installerad på smarttelefonen följ anvisningarna:

- Klicka på länken i textmeddelandet och installera appen.
- Starta AirKey-appen.
- På smarttelefoner med Android startas och genomförs registreringen automatiskt. På smarttelefoner med iOS anger du ditt telefonnummer och bekräftar med ***Fortsätt***.



Figur 52: Ange telefonnummer (iOS)

- Du får ytterligare ett sms. Lämna AirKey-appen öppen och klicka på den åttasiffriga registreringskoden som visas ovanför knappsatsen.

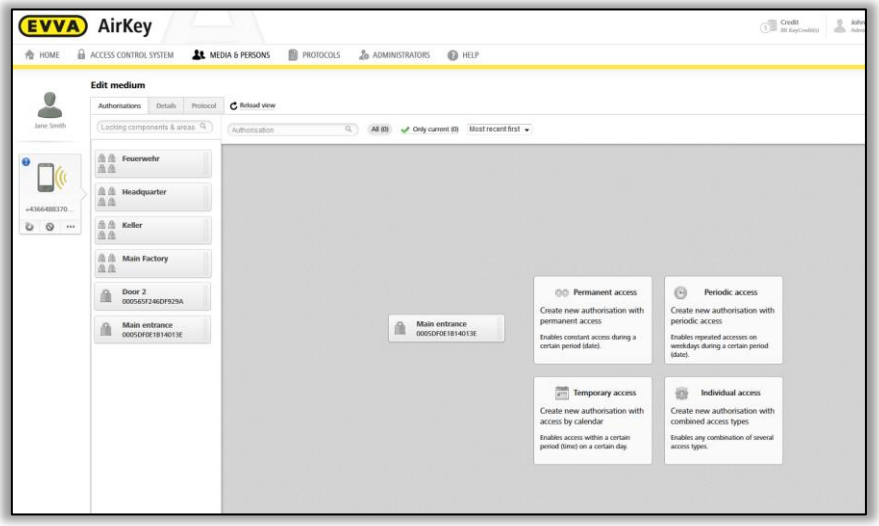


Figur 53: Registreringskod (iOS)

Om den åttasiffriga koden inte visas eller om du råkar stänga AirKey-appen måste du kopiera koden ur textmeddelandet och infoga den i AirKey-appen.

› Slutför registreringen med ***Registrera***.

Klicka på ***Registrera*** för att lägga till smarttelefonen till det nya AirKey-systemet. I AirKey-onlineadministrationen vidarebefordras man till ***Redigera medium*** där man skapar önskade behörigheter. Dra och släpp den AirKey-enhet för vilken man vill ge behörighet till önskad tillträdestyp (permanent tillträde, tillfälligt tillträde, periodiskt tillträde, individuellt tillträde) – se även Tilldela behörigheter.



Figur 54: Tillträdestyper

4.10 Installera låskomponenter

4.10.1 AirKey-cylindrar

För installation av AirKey-cylindern, -hybridcylindern, -regelcylindern och -hänglåset, se monteringsanvisningarna i förpackningen eller titta på monteringsvideon online på https://www.evva.com/sv/airkey/website/.

Se till att båda sidorna av dubbelsidiga AirKey-cylindrar har konfigurerats inom AirKey-systemet för att förhindra att användare blir in- eller utelåsta.

4.10.2 AirKey-väggläsare

Läs monteringsanvisningen som medföljer leveransen för installation av AirKey-väggläsaren. På vår webbplats https://www.evva.com/sv/airkey/website/ finns en borrschablon och en installationsfilm.

Det behövs en styrenhet för varje väggläsare. Styrenheten ska installeras på en säker plats inomhus. Kontrollera kabeldragningen för väggläsaren och styrenheten.

AirKey-enheter levereras alltid i fabriksläge.

Medier i fabriksläge kan aktivera alla AirKey-enheter i fabriksläge.

- Smarttelefoner med installerad AirKey-app och aktiv underhålls-behörighet kan aktivera enheter i fabriksläge.
- Aktiveringar i fabriksläget loggas inte.
- Behörigheter tilldelas först när AirKey-enheten har lagts till systemet.
- Läs alltid anvisningarna i monteringsanvisningen vid installation. Öppna dörren och säkra den så att den inte går i lås av misstag under installation eller demontering av AirKey-enheter.

4.11 Lägga till låskomponenter

Lägg till enheter i AirKey-systemet med hjälp av en smarttelefon med underhållsbehörighet eller en valfri kodningsstation. AirKey-enheterna måste vara i fabriksläge.

För att AirKey-enheter ska kunna läggas till med smarttelefonen måste följande villkor vara uppfyllda:

- AirKey-appen är installerad.
- Det finns en aktiv internetuppkoppling (t.ex. 3G, 4G).
- Smarttelefonen är registrerad i AirKey-systemet.
- Smarttelefonen har tilldelats en person.
- Smarttelefonen har underhållsbehörighet (uppdaterings rättighet).

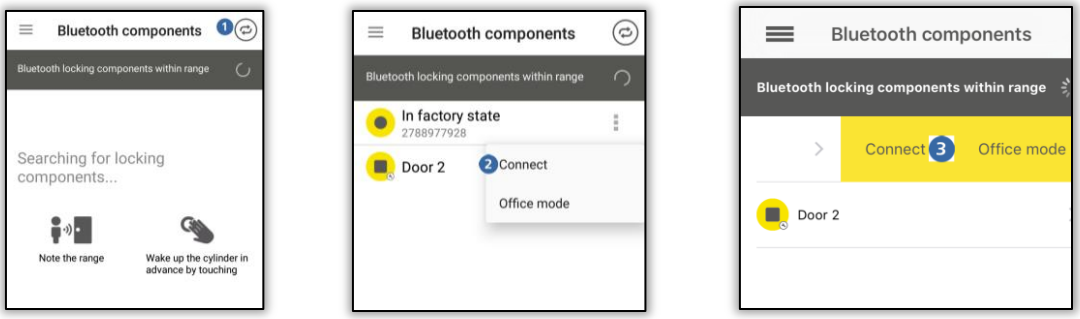
4.11.1 Lägga till AirKey-enheter med smarttelefonen

> Starta AirKey-appen.

> Anslut via **NFC** (för Android-telefoner):
Tryck på symbolen ***Anslut till komponent*** ❶.

> Anslut via **Bluetooth** (för **Android**-telefoner): öppna kontextmenyn i den AirKey-enhet i fabriksläge som du vill lägga till i systemet (⋮) och välj sedan ***Anslut*** ❷.

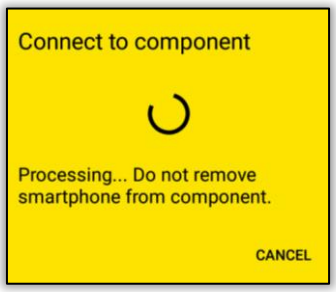
> Anslut via **Bluetooth** (för **iPhones**): drag beteckningen "i fabriksläge" på den AirKey-enhet som ska läggas till i systemet åt vänster och välj ***Anslut*** ❸.



Figur 55: AirKey-app – ansluta till komponent (med NFC för Android-telefoner / med Bluetooth för Android-telefoner / med Bluetooth för iPhones)

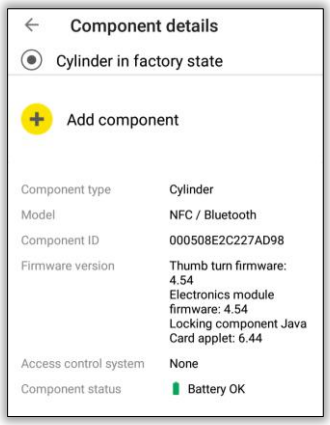
Figur 56: AirKey-app – anslutning till komponenten

> Håll smarttelefonen mot låskomponenten i fabrikssläge (när den är ansluten via NFC) för att upprätta en anslutning. Anslutningen upprättas automatiskt via Bluetooth. Avlägsna inte telefonen från AirKey-enheten medan anslutningen upprättas.



Figur 57: AirKey-app – ansluta

> Du ser nu information om AirKey-enheten.



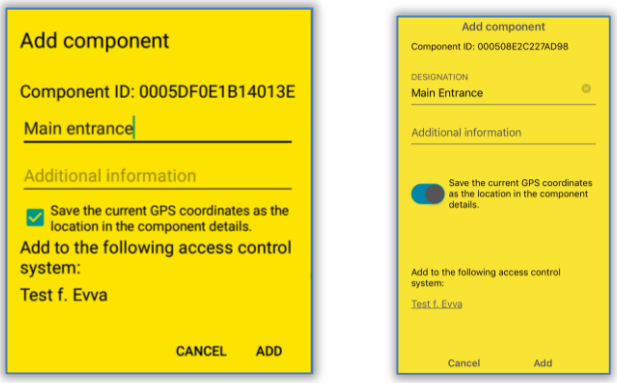
Figur 58: Lägga till enheter

> Tryck på ***Lägg till enhet***.

> Ange en unik beteckning för AirKey-enheten.

Se till att båda sidorna av dubbelsidiga AirKey-cylindrar har konfigurerats inom AirKey-systemet. Tilldela en tydlig beteckning för varje sida av cylindern. Skapa ett område som omfattar båda sidorna av cylindern och tilldela en områdesbehörighet för att få samma behörighet för båda sidorna.

> Välj det AirKey-system till vilket enheten ska läggas till om smarttelefonen är registrerad i flera AirKey-system, med underhållsbehörighet.



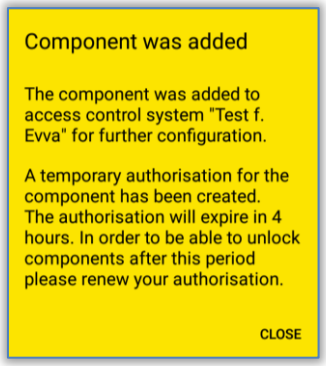
Figur 59: AirKey-app – lägga till AirKey-enheter Android / iPhone

> Tryck på ***Lägg till***.

> Håll smarttelefonen mot låskomponenten i fabriksläge igen (när den är ansluten via NFC) för att upprätta en anslutning. Anslutningen upprättas automatiskt via Bluetooth.

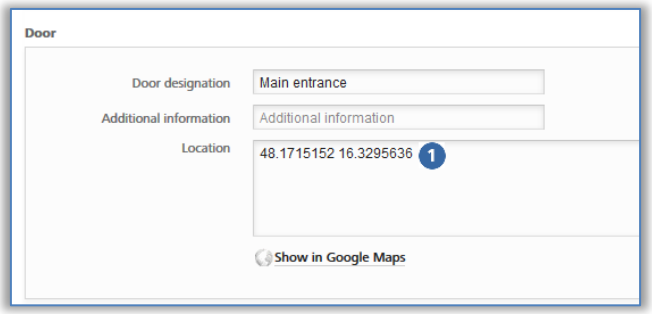
Systemet kontrollerar uppgifterna och uppdaterar enheten. Håll kvar telefonen mot enheten under processen.

> Systemet uppmanar dig att bekräfta processen. AirKey-enheten är nu registrerad i AirKey-onlineadministrationen.



Figur 60: AirKey-app – AirKey-enhet tillagd

Enheten visas i listan med en översikt över enheter i AirKey-onlineadministrationen. Om GPS-koordinaterna ❶ fastställdes när enheten lades till, finns positionen i AirKey-online-administrationen under fliken ***Detaljer*** i området "Dörr".



Figur 61: GPS-koordinater i AirKey-enhetens detaljer

Alternativt ange den adress där enheten är i fältet "Plats".

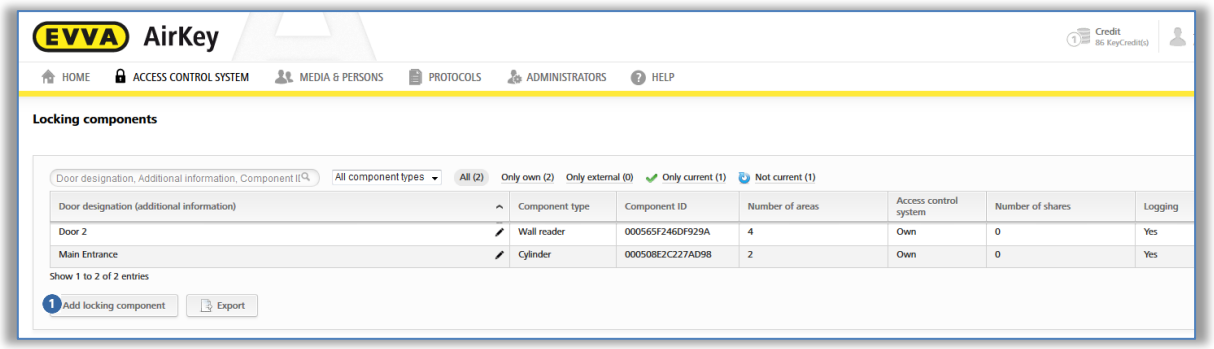
Enheten är inte längre i fabriksläge. Medier i fabriksläge eller smarttelefoner i uppdateringsläge har inte längre behörighet till denna enhet. Den smarttelefon som användes för att lägga till enheten har automatiskt behörighet under fyra timmar. Ändra motsvarande behörighet eller tilldela ytterligare medier med giltig behörighet för att fortsätta att ha tillträde till denna enhet.

4.11.2 Lägga till låskomponenter med hjälp av kodningsstationer

Option

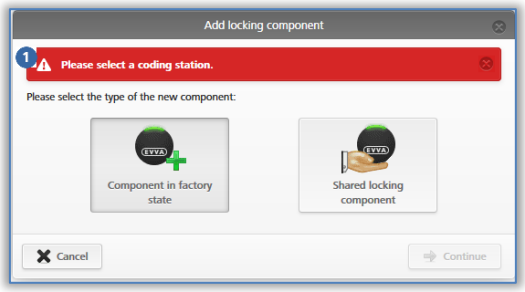
Gör på följande sätt för att lägga till enheter med hjälp av kodningsstationer:

- På startsidan ***Home*** väljer du rutan ***Cylindrar*** eller ***Väggläsare***.
- Klicka på knappen Lägg till låskomponent ❶.
- Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.



Figur 62: Lägg till låskomponent

› Anslut kodningsstationen till datorn, ett systemmeddelande visas om så ej är gjort. ❶

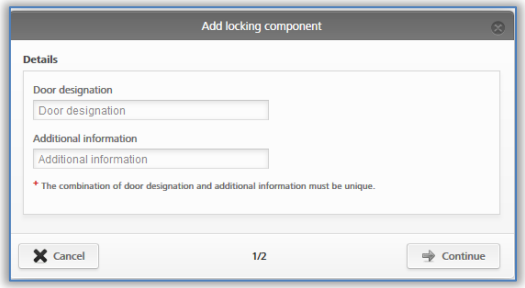


Figur 63: Lägga till låskomponent / ingen kodningsstation

› Välj ***Enhet i fabriksläge.***

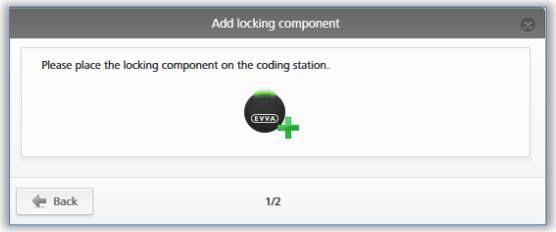
› Klicka på ***Fortsätt***.

› Ange dörrbeteckningen i dialogfönstret och klicka på ***Fortsätt***.



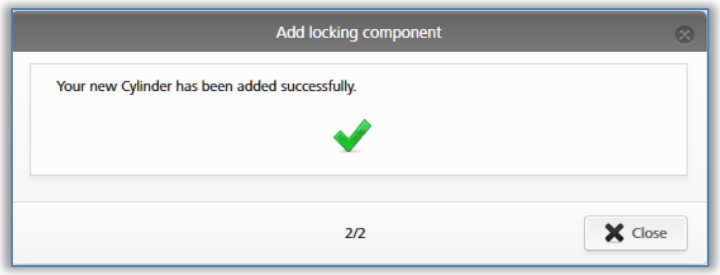
Figur 64: Lägga till låskomponent – tilldela namn

› Följ instruktionerna på displayen och placera enheten på kodningsstationen.



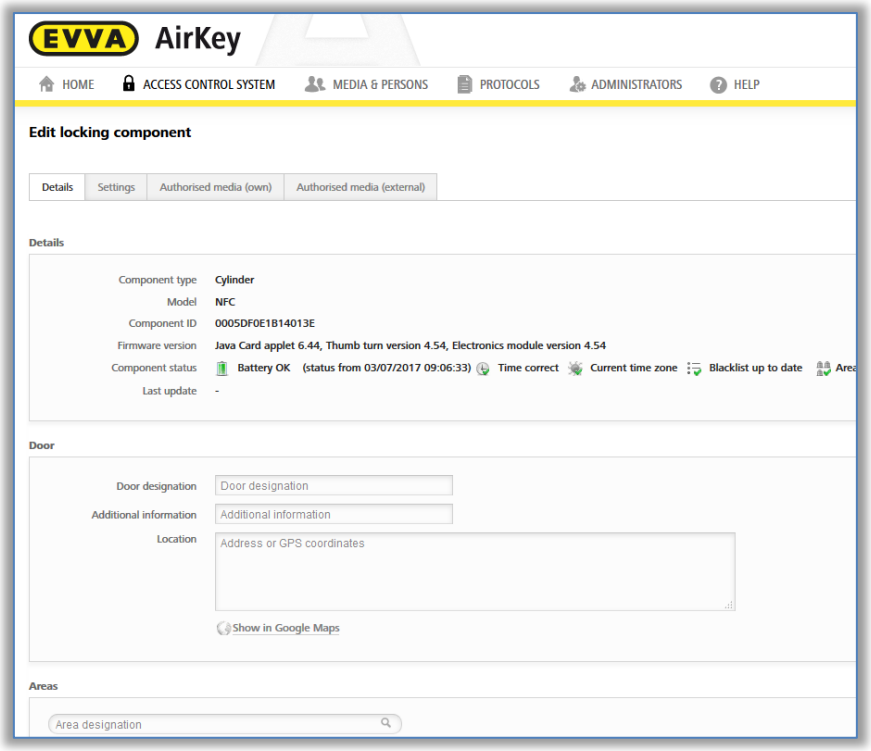
Figur 65: Lägga till låskomponent

› Bekräfta processen och enheten läggs till i AirKey-systemet.



Figur 66: Lägga till låskomponent – bekräftelse

När processen är bekräftad vidarebefordras man till den detaljerade vyn över enheten.



Figur 67: låskomponent detaljer

Enheten är ej i fabriksläge. Medier i fabriksläge eller smarttelefoner i uppdateringsläge har inte längre behörighet att aktivera denna enhet. Lägg till ett medium eller en smarttelefon i systemet och tilldela giltiga behörigheter till enheterna.

Standardtidszonen och de standardmässiga säkerhetsinställningarna konfigureras automatiskt för den enhet som har lagts till i enlighet med de specificerade inställningarna.. Se Standardvärden (för alla nyligen tillagda AirKey-enheter) för mer information om inställningarna.

Alternativt kan man placera en enhet i fabriksläge på kodningsstationen. Ett informationsfönster visas längst ned till höger och gör det möjligt att lägga till enheten i systemet via länken ***Lägg till enhet till mitt låssystem***.

Figur 68: Lägg till enhet till mitt system

4.12 Lägga till kort, nyckelbrickor, armband och kombinycklar med en smarttelefon

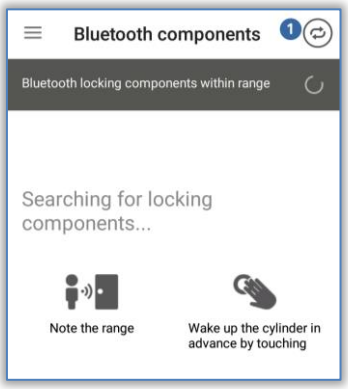
Tillträdesmedier i fabriksläget läggs till i AirKey-system med en smarttelefon med underhålls-behörighet eller en kodningsstation.

> Starta AirKey-appen.

När man använder en smarttelefon för att lägga till kombinycklar i systemet måste man hålla den sida av nyckeln med RFID-symbolen mot telefonens NFC-chip. De flesta modeller kräver att kombinyckeln hålls direkt mot telefonens baksida.

Den här åtgärden görs med en Android-telefon som stöder NFC. Se kapitlet Koda medier för mer information om hur man lägger till medier via Bluetooth med en Android-telefon eller iPhone.

> Tryck på symbolen ***Anslut till komponent*** ❶.

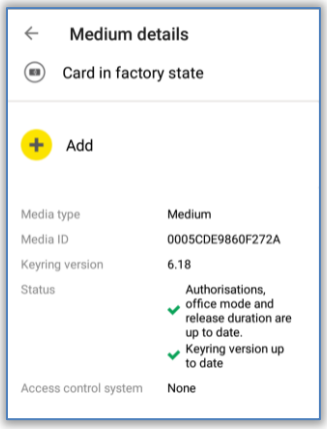


Figur 69: AirKey-app – ansluta till komponent

> Håll telefonens NFC-chip mot mediet i fabriksläge.
En anslutning till mediet upprättas.

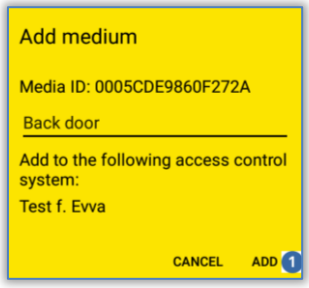
Figur 70: AirKey-app – ansluta

> Håll kvar mediet mot telefonen medan anslutningen upprättas. Nu visas information om mediet.



Figur 71: Detaljer om mediet

> Tryck på ***Lägg till***.
> Ange en beteckning för mediet.



Figur 72: Lägga till medier – fastställa beteckningar

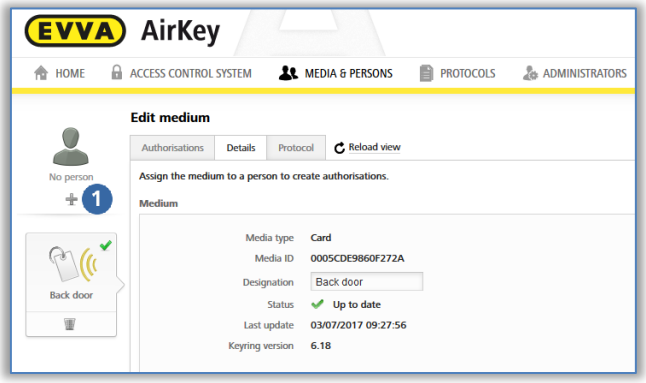
> Välj vilket AirKey-system mediumet ska tillhöra om smarttelefonen är registrerad i flera system.
> Tryck på ***Lägg till*** ❶.
> Håll åter mediet mot telefonen för att slutföra registreringen.
> Systemet bekräftar registreringen. Mediet kan nu tilldelas en person / användare i AirKey-onlineadministration.

Denna process är identisk för kort, nyckelbrickor, armband och kombi-nycklar. Alla tre element grupperas i "kort".

4.13 Tilldela personer till medier

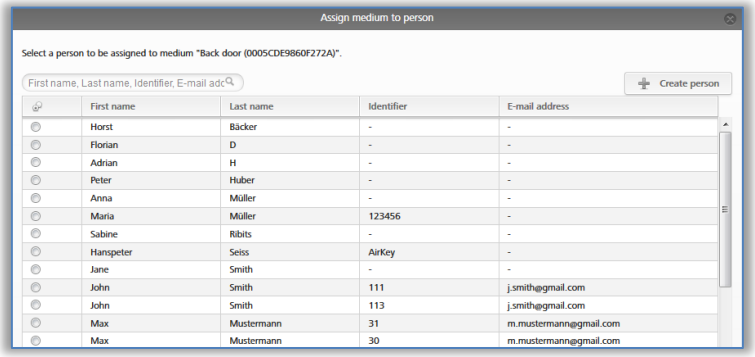
Fortsätt steg,tilldela mediet till en person för att kunna tilldela behörigheter. Detta är enda sättet att koppla personer till behörigheter.

- På startsidan ***Home*** välj rutan ***Smarttelefoner*** eller ***Kort***.
- Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
- Välj det medium som ännu inte har tilldelats någon person i listan över medier.
- Intill knappen ***Ingen person*** klicka på symbolen **+** ❶



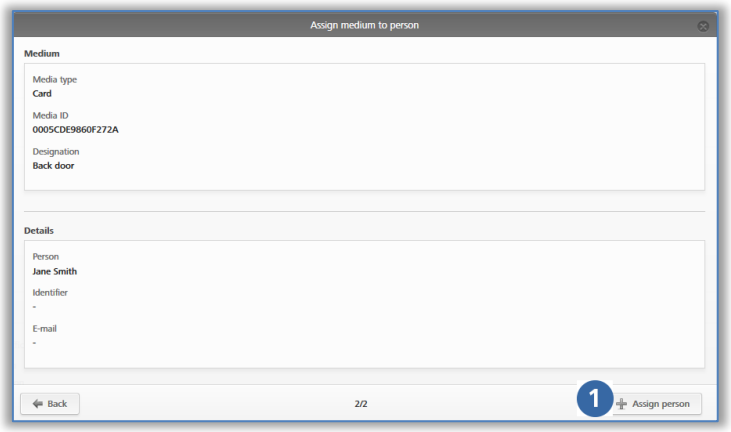
Figur 73: Tilldela personer

- Välj den person i användarlistan till vilken mediumet ska tillhöra.



Figur 74: Tilldela personer till medier

- Om önskad person ännu inte har skapats kan du använda knappen ***Skapa person*** för att komma till det andra dialogfönstret "Tilldela medium till person".
- Välj ***Tilldela till person*** ❶ för att bekräfta tilldelningen av mediet.



Figur 75: Bekräfta person / tilldelning

› Mer information finns i Tilldela behörigheter.

Man kan tilldela medier till personer i fönstret medier. Mer information finns i avsnittet Tilldela medier till personer.

4.14 Tilldela behörigheter

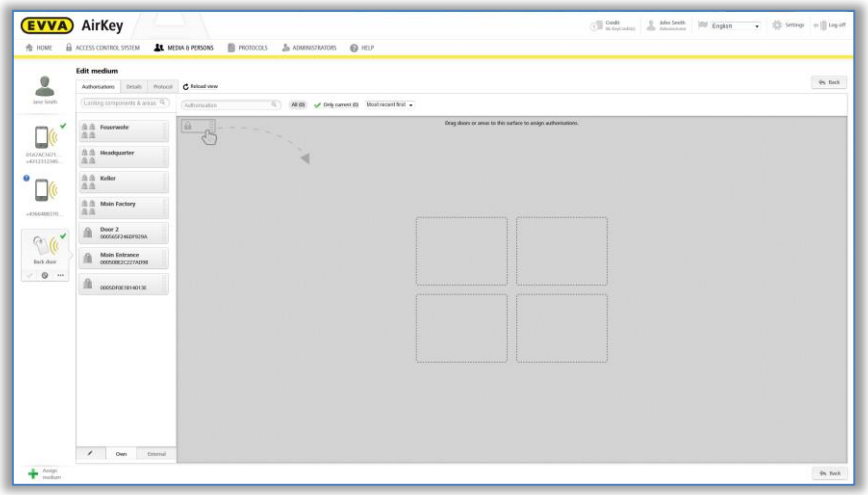
Observera att tilldelning av behörigheter är endast möjligt när ett medium har tilldelats en person.

Välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

› Välj önskat medium i listan för medium.

› Har mediet tilldelats en person visas en översikt över behörigheterna för mediumet.

› Så fort man drar och släpper respektive AirKey-enhet till det grå området visas tillgängliga tillträdestyper i de fyra områdena med streckade kanter.



Figur 76: Tilldela behörigheter

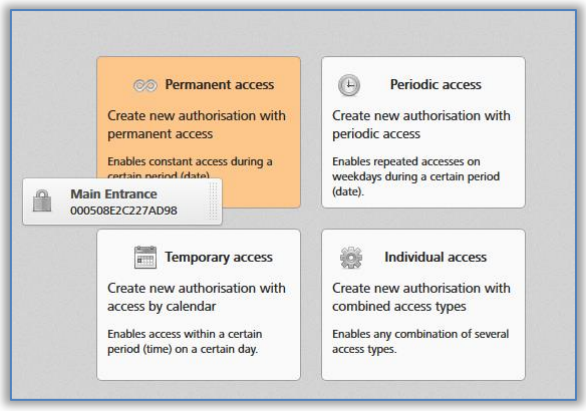
› Dra och släpp vald enhet/valt område i motsvarande fält för att välja önskad behörighet.

Det finns fyra olika tillträdestyper:

- Permanent tillträde
- Periodiskt tillträde
- Tillfälligt tillträde
- Individuellt tillträde

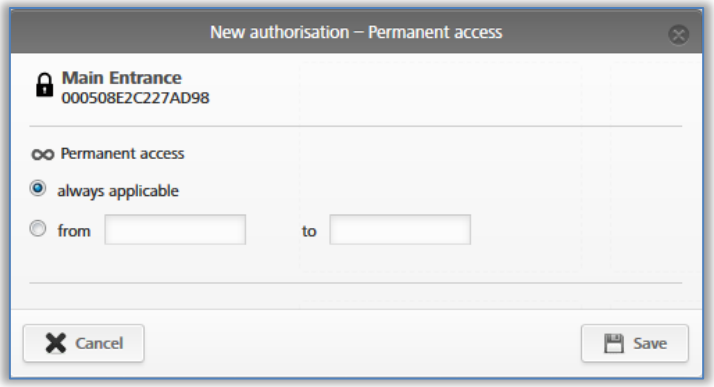
4.14.1 Permanent tillträde

Permanent tillträde innebär att behörigheten gäller när som helst. Specificera ett start- och slutdatum för att begränsa behörigheten.



Figur 77: Tilldela permanenta behörigheter

- Ange perioden för permanenta behörigheter.
  Du kan välja mellan obegränsat, permanent eller permanent behörighet med ett specifikt start- och slutdatum.

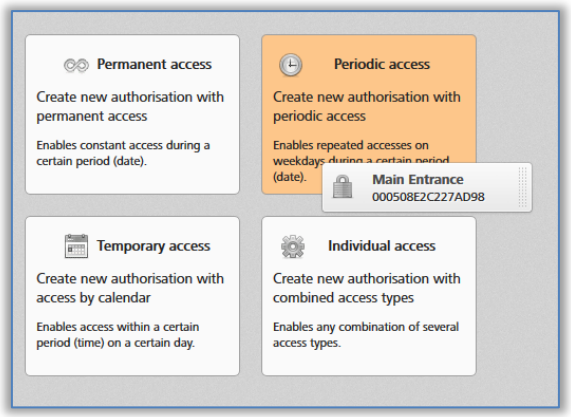


Figur 78: Tilldela permanenta behörigheter

- Klicka på ***Spara***.

4.14.2 Periodiskt tillträde

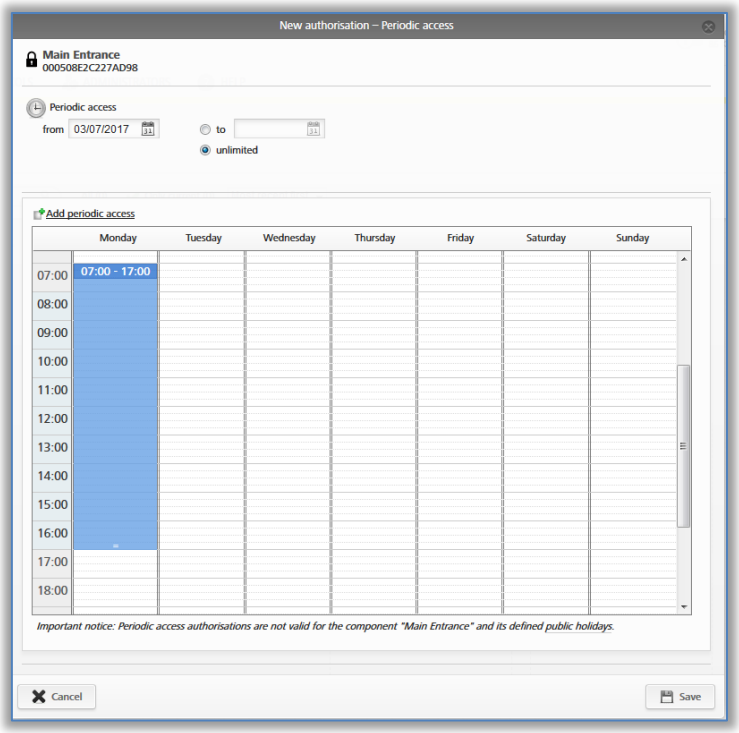
Tilldela periodiskt tillträde för specifika tidsstyrda behörigheter Tidsstyrda behörigheter kan till exempel vara en rad möten som hålls en gång i veckan.



Figur 79: Tilldela periodisk behörighet

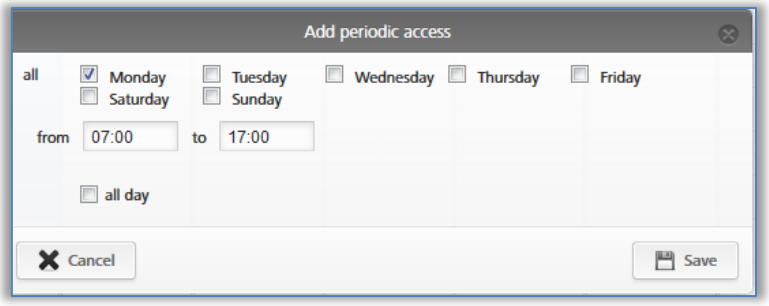
Systemet visar en veckokalender där du kan fastställa upp till fyra perioder/tidszoner för varje dag i veckan.

> Specificera behörighets perioden.



Figur 80: Tilldela periodiskt behörighet

> Markera direkt i kalendern eller klicka på ***Lägg till periodiskt tillträde***.

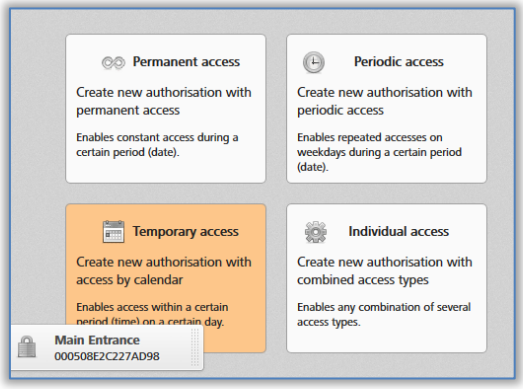


Figur 81: Lägga till periodisk behörighet

> Ange önskad period och klicka på ***Spara***.
> Klicka på ***Spara*** även i fönstret "Ny behörighet – periodiskt tillträde".

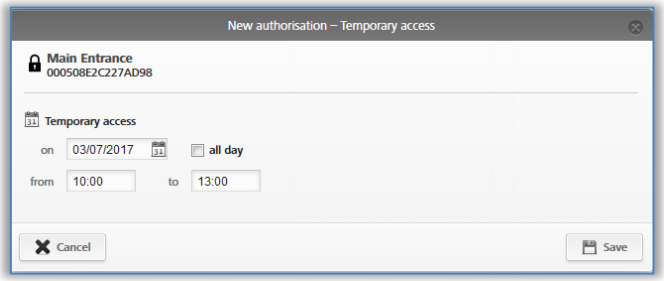
4.14.3 Tillfälligt tillträde

Tilldela enskilda behörigheter för begränsat tillträde en viss dag eller en viss period.



Figur 82: Tilldela tillfälliga behörigheter

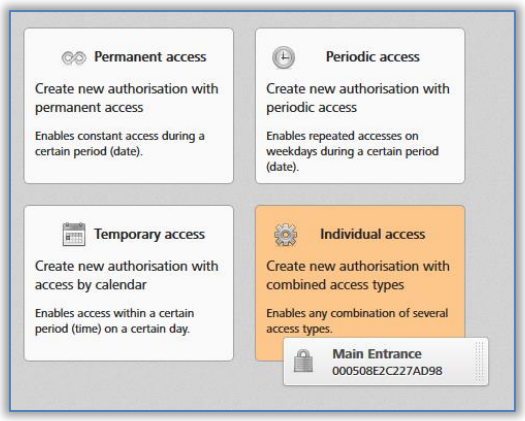
> Ange önskad period och klicka på ***Spara***.



Figur 83: Tilldela tillfälliga behörigheter

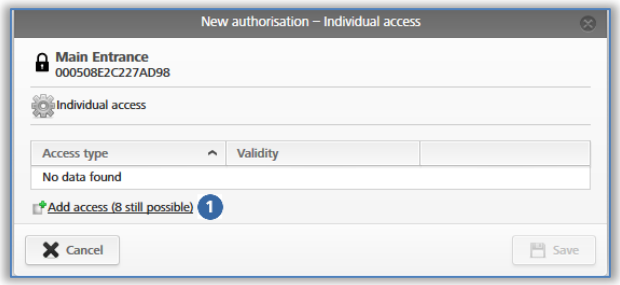
4.14.4 Individuell behörighet

Permanent, enskilt och periodisk behörighet tilldelas individuellt.



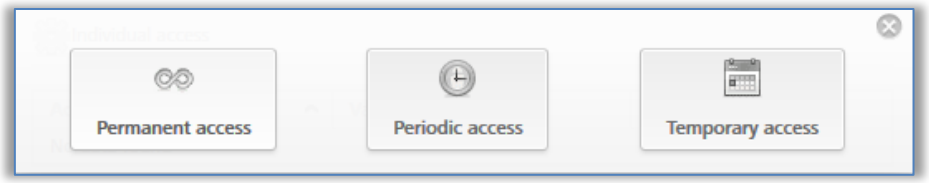
Figur 84: Tilldela enskild behörighet

> I dialogen "Ny behörighet – enskilt tillträde" visas eventuella enskilda behörigheter som du redan har tilldelat.
> Klicka på en post i raden för att ändra behörigheten.
> Alternativt klicka på ***Lägg till en behörighet*** ❶ för att lägga till en ny post.



Figur 85: Ny behörighet – enskilt tillträde

> Välj ***permanent***, ***periodiskt*** eller ***tillfälligt tillträde*** och definiera specifikationerna för respektive alternativ. Parametrarna motsvarar de behörigheter som beskrivs ovan.



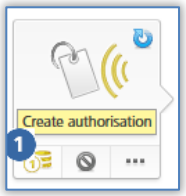
Figur 86: Ny behörighet – enskilt tillträde

> När du har konfigurerat alla enskilda behörigheter klickar du på ***Spara***.

> Perioderna för permanent och periodisk behörighet behöver inte överlappa varandra.
> Det går att fastställa högst en enskild period per dag.
> Om perioderna för det enskilda och det periodiska behörigheterna överlappar varandra är båda typerna giltiga.
> Du kan konfigurera högst åtta enskilda behörigheter.

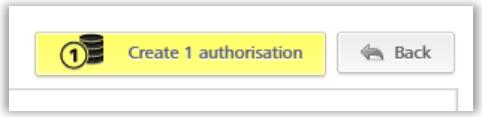
4.15 Skapa behörigheter

När man skapat behörigheterna för ett medium slutförs processen med ***Skapa behörighet*** och uppdatera respektive medium.



Figur 87: Skapa behörigheter

När en befintlig behörighet ändras eller när en ny behörighet skapas ändras symbolen vid motsvarande medium. Skapa behörigheten, under förutsättning att det finns tillräckligt med KeyCredits.

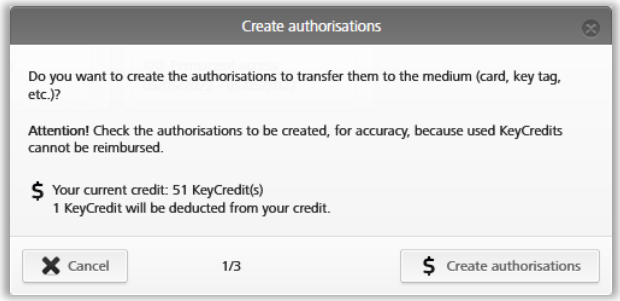


Figur 88: Skapa nya eller ändrade behörigheter

> Klicka på den gula knappen ***Skapa 1 behörighet*** eller symbolen ❶ för mediet.

Har man inte tillräcklig med KeyCredits i denna fas av processen visas ett meddelande. Man kan genast fylla på KeyCredits via länken i meddelandet. Fyller man på kredit genom meddelandet skapas behörigheten automatiskt och en KeyCredit dras av från ditt konto.

> Ett meddelande fås om att krediter har dragits från kreditsaldot när ett medium har skapats.



Figur 89: Skapa behörigheter

> Klicka på ***Skapa behörigheter*** för att bekräfta processen.

Man måste nu uppdatera medier som kort, nyckelbrickor, armband eller kombinycklar med en smarttelefon eller en kodningsstation för att behörigheterna ska aktiveras på medierna. Behörigheter på telefoner skickas som pushmeddelanden (meddelanden).

I det här avsnittet beskrivs hur AirKey-systemet tas i drift och konfigureras korrekt. De processer som beskrivs är de första stegen för att man ska kunna hantera ett AirKey-system. I följande avsnitt beskrivs i detaljerad bild de enskilda funktionerna i AirKey-onlineadministration och av AirKey-appen.

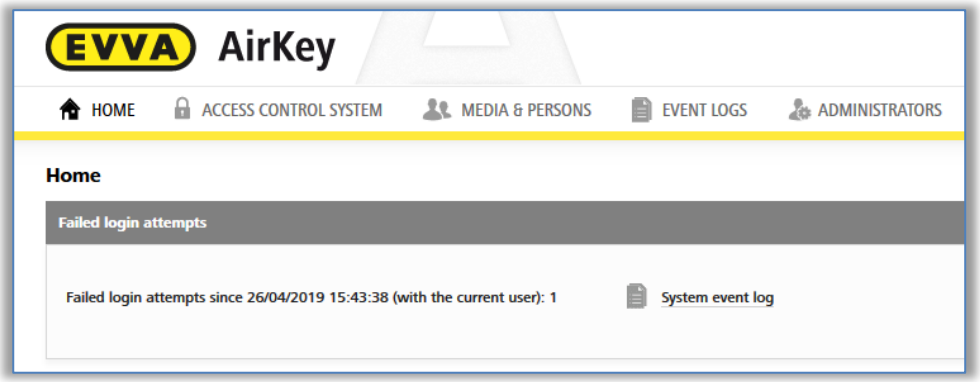
5 AirKey-onlineadministration

5.1 AirKey-inloggning

Inloggning krävs för att kunna konfigurera och underhålla AirKey-låssystemet. I inställningarna för AirKey-onlineadministrationen kan en tvåfaktorsautentisering aktiveras för inloggning vid behov. Hur den här funktionen aktiveras beskrivs i avsnittet Inställningar för AirKey-låssystemet.

Du kan aktivera tvåfaktorsautentiseringen för att höja säkerheten i AirKey-låssystemet.

Misslyckade inloggningsförsök visas på startsidan och registreras i systemloggen. De visas endast på startsidan när det har förekommit minst ett misslyckat inloggningsförsök sedan den senaste lyckade inloggningen.

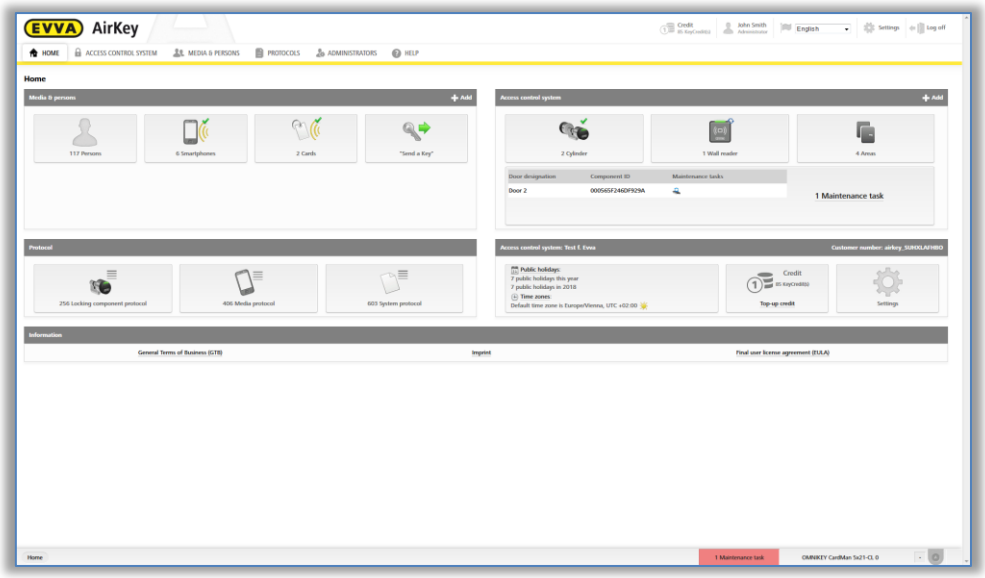


Figur 90: Misslyckade inloggningsförsök

5.1.1 AirKey-inloggning utan tvåfaktorsautentisering

- Öppna följande sida i webbläsaren: https://airkey.evva.com.
  Inloggningssidan för AirKey-onlineadministration öppnas.
- Ange det användar-ID som skickades via ett e-postmeddelandet "EVVA AirKey-registrering".
- Ange det personliga AirKey-lösenordet och bekräfta med ***Logga in***.

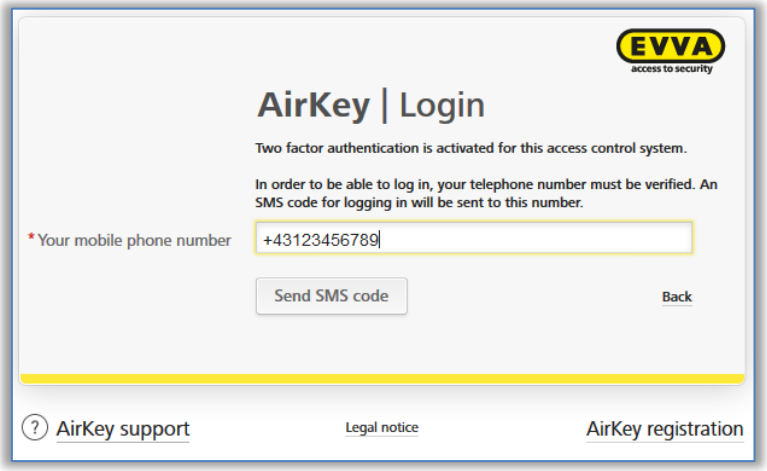
Vid inloggning öppnar programmet startsidan ***Home***. Här finns en översikt av AirKey-systemet.



Figur 91: AirKey-onlineadministration – hem

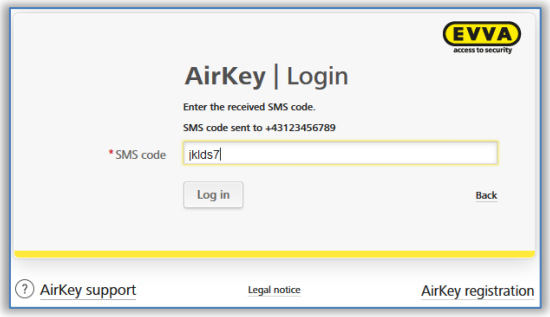
5.1.2 AirKey-inloggning med tvåfaktorsautentisering

- Öppna en webbläsare och gå till webbplatsen https://airkey.evva.com. Inloggningssidan till AirKey-onlineadministrationen öppnas.
- Ange det användar-ID som visas i e-postmeddelandet "EVVA Airkey-registrering".
- Ange ett AirKey-lösenord som du själv väljer och bekräfta med ***Logga in***.
- Om inget telefonnummer har verifierats för administratören visas en uppmaning om att ange ett telefonnummer för verifieringen.
- Ange telefonnumret till den smarttelefon som ska användas för tvåfaktorsautentiseringen och bekräfta med ***Skicka SMS-kod***. Telefonens nummer måste börja med **+** och landsnumret, och kan innehålla högst 50 tecken (+, 0-9 och mellanslag).



Figur 92: Verifiering av mobiltelefonnumret vid inloggning

- Ett SMS med en SMS-kod skickas till det angivna telefonnumret.
- Ange SMS-koden i dialogrutan för AirKey-onlineadministration och bekräfta med ***Logga in***.



Figur 93: SMS-kod vid inloggning

> Telefonnumret är därmed verifierat för tvåfaktorsautentisering och startsidan för AirKey-låssystemet visas.

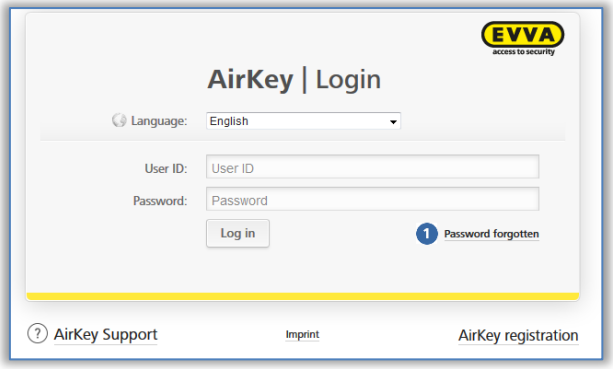
Om telefonnumret redan har verifierats behöver det inte anges igen efter inmatning av användar-ID och lösenord. I det här fallet skickas en SMS-kod direkt till det verifierade telefonnumret, och denna kod ska sedan anges i AirKey-onlineadministrationen för inloggning.

SMS-koden är giltig i 5 minuter. Om det går mer än 5 minuter måste inloggningsprocessen upprepas.

Utan åtkomst till det verifierade telefonnumret går det inte att logga in till AirKey-onlineadministrationen. Om du vill ändra telefonnumret måste du göra det från administratörsuppgifterna (se Redigera administratör). För detta krävs det aktuella verifierade telefonnumret. Om telefonnumret inte är tillgängligt längre kontaktar du EVVA-supporten.

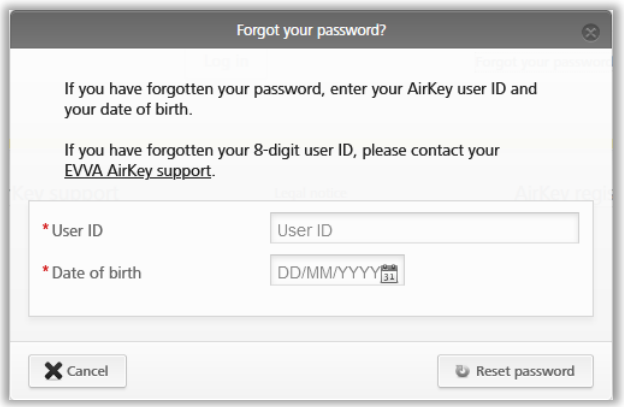
5.1.3 Har man glömt lösenordet?

Vid glömt lösenord kan det återställas. Klicka på ***Glömt lösenord.*** ❶



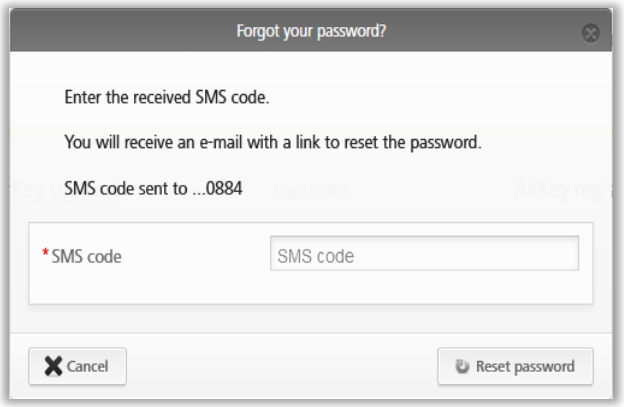
Figur 94: Inloggningssida för AirKey-onlineadministration

> Ange det användar-ID och födelsedatum som uppgavs i dialogfönstret "Glömt lösenord?" och klicka på ***Återställ lösenord***.



Figur 95: Glömt lösenord?

> Med tvåfaktorsautentisering aktiverad får du ett SMS med en kod till din verifierade smarttelefon. Koden anges sedan i det efterföljande fönstret och bekräftas med ***Återställ lösenordet***. (Det här steget utgår om tvåfaktorsautentiseringen inte är aktiverad eller om telefonnumret inte är verifierat.)



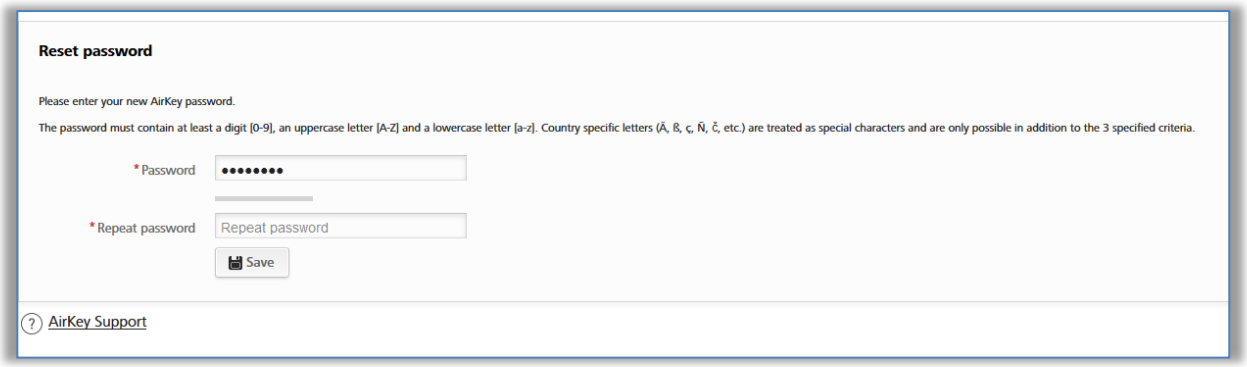
Figur 96: SMS-kod

SMS-koden är giltig i 5 inuter. Om de fem minuterna överskrids måste proceduren upprepas.

Utan åtkomst till det verifierade telefonnumret kan processen inte slutföras. Om telefonnumret inte är tillgängligt längre kontaktar du EVVA-supporten.

Ett automatiskt e-postmeddelande från *EVVA AirKey* skickas med följande referens: "EVVA AirKey-onlineadministration – återställning av lösenord".

> Öppna e-postmeddelandet från *EVVA AirKey*.
> Klicka på länken för återställning av lösenordet i e-postmeddelandet. Webbsidan där man kan återställa lösenordet öppnas.
> Ange ett nytt lösenord och upprepa lösenordet för att bekräfta processen.
> Klicka på ***Spara lösenord***.



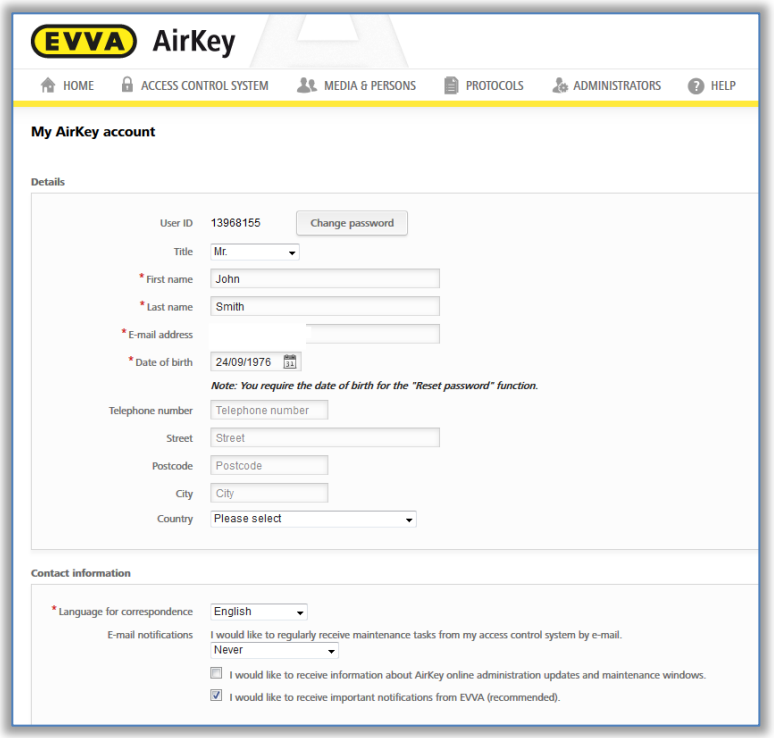
Figur 97: Återställa AirKey-lösenord

Inloggningssidan för AirKey-onlineadministration öppnas.

> Logga in med det nya lösenordet som beskrivs i avsnittet AirKey-inloggning utan tvåfaktorsautentisering eller AirKey-inloggning med tvåfaktorsautentisering.

Om uppgifterna är korrekta kommer startsidan ***Home*** att öppnas. Längst upp till höger visas namnet på den användare som är inloggad.

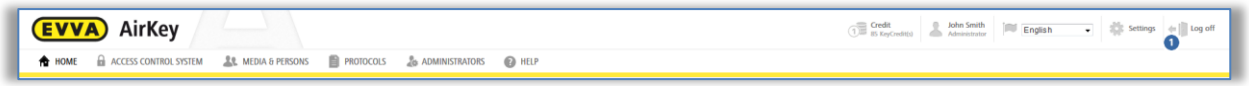
Vid behov kan lösenordet ändras i AirKey-onlineadministration. Detta görs genom att klicka på administratörens namn längst upp till höger i AirKey-onlineadministration och trycka på funktionen ***Ändra lösenord***.



Figur 98: Mitt AirKey-konto

5.2 Logga ut ur AirKey

Klicka på ***Logga ut*** ❶ för att lämna AirKey-onlineadministration.



Figur 99: Logga ut

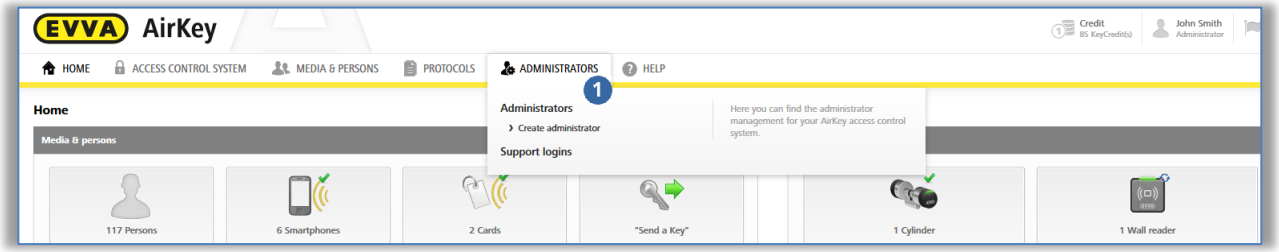
Trots att systemet har en automatisk utloggningsfunktion efter 30 minuter rekommenderar vi att administratörer alltid loggar ut efter att ha utfört uppgifter i AirKey-onlineadministration med knappen ***Logga ut***.

5.3 Administratörer

Administratörer har rättigheter att hantera hela AirKey-systemet.

Det måste finnas minst en administratör per klient och AirKey-system.

I huvudmenyn ***Administratörer*** ❶ finns hanteringsfunktionerna för administratörer.

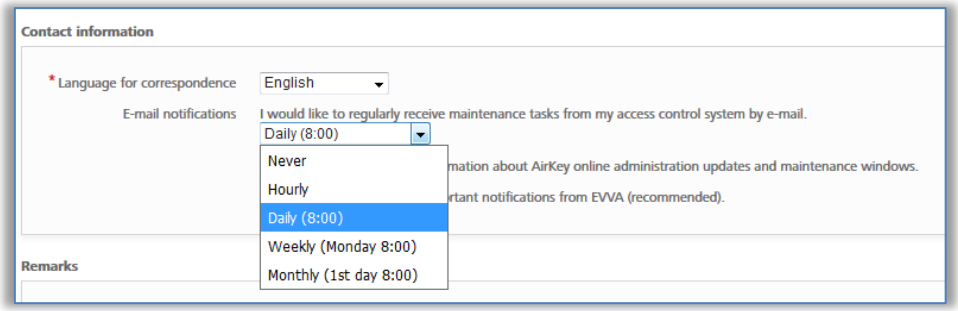


Figur 100: Huvudmenyn Administratörer

5.3.1 Skapa administratörer

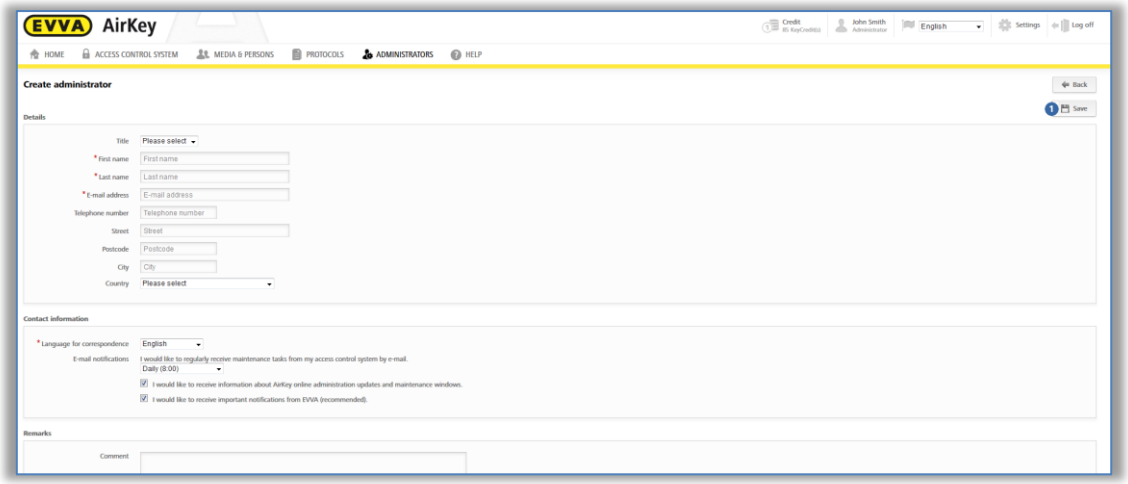
Endast administratörer kan skapa andra administratörer.

- I huvudmenyn väljer man ***Administratörer*** → ***Skapa administratör***.
- Fyll i fälten i formuläret. Fält som är markerade med * är obligatoriska.
- I avsnittet "Kontaktinformation" kan du även ange om administratören ska få e-post-meddelanden vid specifika händelser, till exempel öppna underhållsåtgärder, kommande underhållsfönster eller annan viktig information. E-postaviseringarna skickas på det valda kommunikationsspråket.



Figur 101: Kontaktinformation

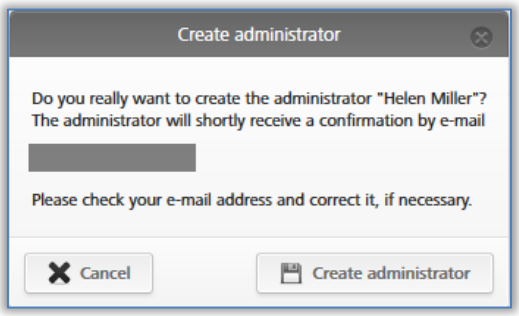
- Klicka på ***Spara*** ❶.



Figur 102: Skapa administratörer

Kontrollera den e-postadress till vilken aktiveringslänken ska skickas, innan man sparar.

> Klicka på ***Skapa administratör*** för att bekräfta säkerhetsfrågan och slutföra processen.



Figur 103: Skapa administratörer

Systemet visar meddelandet "Administratören har sparats" när man har skapat en administratör.

Administratören man just skapat får ett e-postmeddelande från *EVVA AirKey* med en aktiveringslänk.

Uppgifterna raderas och aktiveringslänken blir ogiltig om den inte aktiveras inom 48 timmar.

Administratören som skapats måste slutföra registreringen på följande sätt:

> Öppna e-postmeddelandet med referensen "EVVA AirKey-registrering".
> Klicka på aktiveringslänken. Sidan "Välkommen till AirKey" öppnas.
> Ange det personliga lösenordet, upprepa lösenordet och ange ditt födelsedatum.
> Klicka på ***Spara***.

Processen för att skapa administratören har slutförts. Systemet öppnar nu inloggningssidan för AirKey-onlineadministration så att administratören kan logga in.

5.3.2 Redigera administratörer

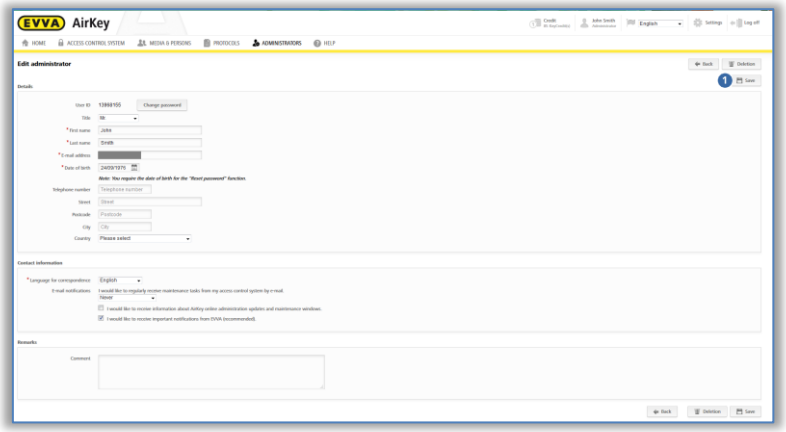
Man kan ändra administratörernas detaljer såsom efternamn, e-postadress, telefonnummer eller kontaktinformation i efterhand.

Användar-ID kan inte ändras.

> I huvudmenyn väljer du ***Administratörer*** → ***Administratörer***.
> Systemet visar en lista över giltiga administratörer.

Sök efter administratörer, sortera kolumner och begränsa antalet poster som visas per sida i listan på displayen samt exportera listan till en CSV-fil.

> Klicka på den administratör vars detaljer som ska ändras.
> Ändra önskade uppgifter.
> Klicka på ***Spara*** ❶.

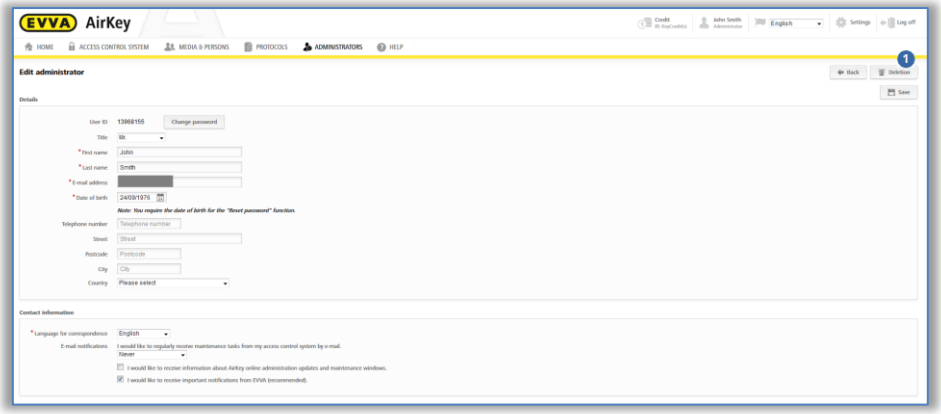


Figur 104: Redigera administratörer

5.3.3 Radera administratörer

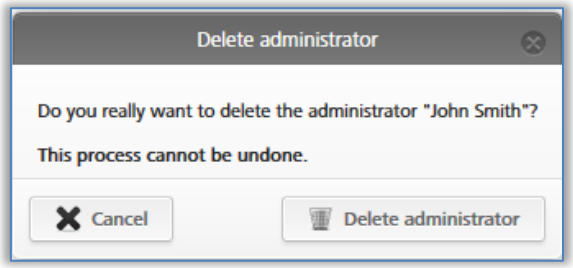
Endast administratörer kan radera andra administratörer.

> I huvudmenyn väljer du ***Administratörer*** → ***Administratörer***.
> Klicka på respektive rad i tabellen för att välja den administratör som ska raderas.
> Sidan "Redigera administratörer" öppnas.
> Klicka på ***Radera*** ❶.



Figur 105: Radera administratörer

> Klicka på ***Ta bort administratör*** för att bekräfta säkerhetsfrågan.



Figur 106: Ta bort administratörer

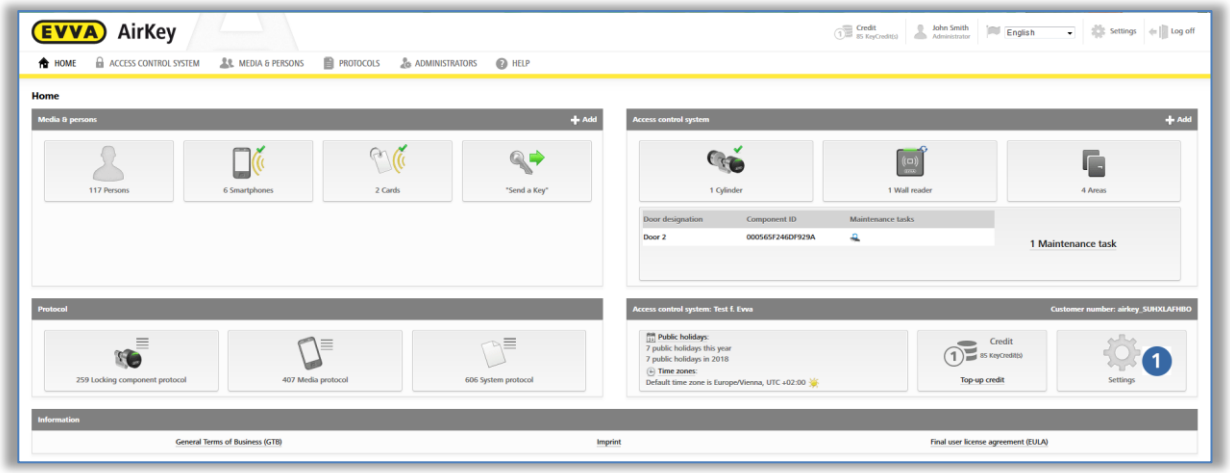
Systemet visar meddelandet "Administratören har raderats" när man har raderat en administratör. Raderade administratörer visas inte längre i listan över administratörer och de kan därmed inte längre logga in i AirKey-onlineadministration.

5.4 AirKey systeminställningar

Konfigurera grundinställningarna i AirKey-onlineadministration. Dessa beskriv i avsnitten nedan.

> På startsidan ***Home*** klicka på rutan ***Inställningar*** ❶.

> Alternativt klicka på ***Inställningar*** i sidhuvudet.



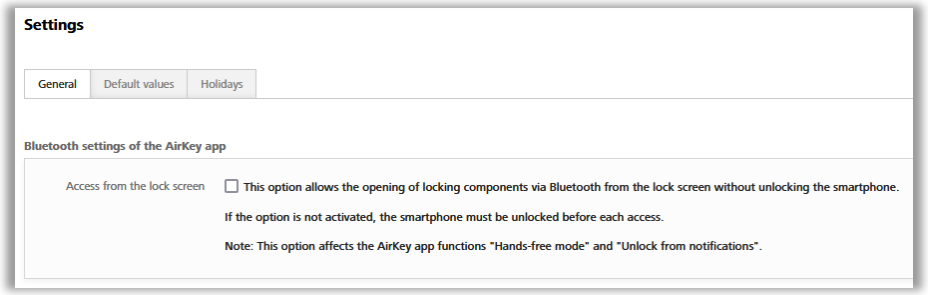
Figur 107: AirKey systeminställningar

5.4.1 Allmänt

På den här fliken kan du aktivera följande allmänna inställningar för hela låssystemet.

Bluetooth-inställningar för AirKey-appen

Här kan man för alla smarttelefoner i detta låssystem konfigurera om det ska gå att aktivera enheter via Bluetooth från låst skärm eller inte. Om alternativet inte är aktiverat måste smarttelefonen låsas upp före varje aktivering.



Figur 108: Allmänna inställningar – Bluetooth-inställningar för AirKey-appen

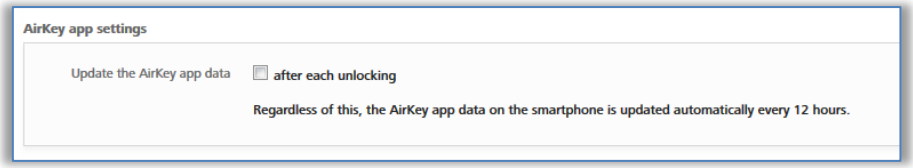
Detta alternativ påverkar app-funktionerna "Hands-free-läge" och "Lås upp från meddelanden".

Avaktivera ***Tillträde från låsskärmen*** för att höja säkerheten på ditt låssystem.

Inställningar för AirKey-appen

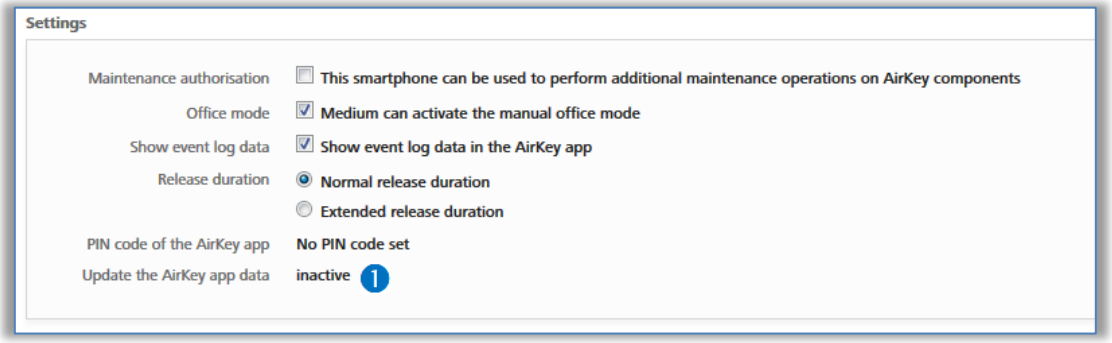
Här kan alternativet "Uppdatering efter varje tillträde". Om det här alternativet aktiveras uppdateras AirKey-appdata (till exempel loggposter och batteristatus för låskomponenterna) vid varje tillträde med en smarttelefon.

> Markera motsvarande kryssruta och bekräfta med ***Spara***.



Figur 109: Allmänna inställningar – Inställningar för AirKey-appen

Funktionaliteten skickas därefter ut till alla smarttelefoner inom låssystemet via push-notiser. Senast efter en manuell uppdatering av AirKey-appdata i smarttelefonen (se kapitlet Uppdatera smarttelefon) bör funktionen vara aktiv på smarttelefonen. Smarttelefonens aktuella status ❶ för den här funktionen finns i detaljerna för smarttelefonen i AirKey-onlineadministrationen.



Figur 110: Status för alternativ "Uppdatering efter varje tillträde"

Du kan aktivera den här funktionen för att överföra tillträdena till AirKey-onlineadministrationen nästan i realtid när du använder en smarttelefon.

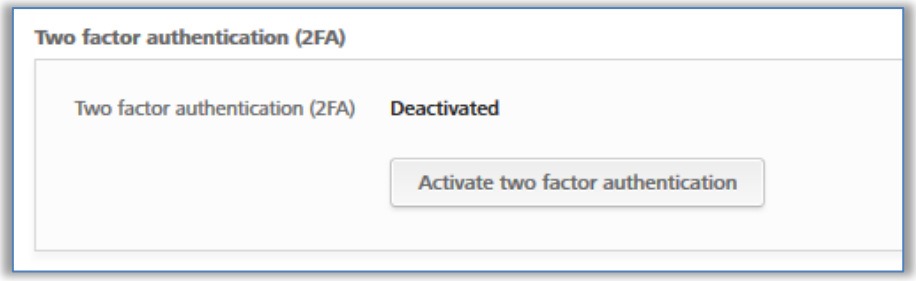
Vid uppdateringen av AirKey-appdata efter ett tillträde överförs endast data från den smarttelefon som har utfört tillträdet. På själva smarttelefonen visas inte denna uppdatering visuellt.

För den här funktionen krävs en stabil internetanslutning (mobildata eller trådlöst lokalt nätverk) eftersom ytterligare tillträdesprocedurer kan utföras först efter genomförd uppdatering av AirKey-appdata.

Oavsett alternativ "Uppdatering efter varje tillträde" görs ett försök att uppdatera AirKey-appdata automatiskt var tolfte timme.

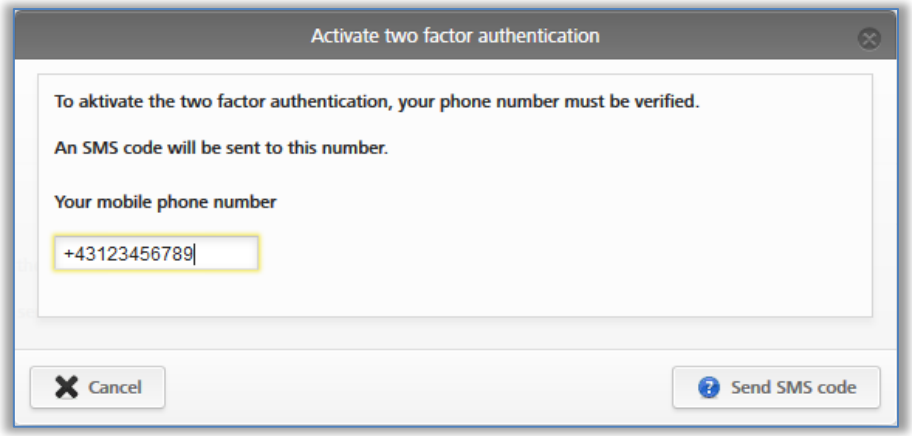
Tvåfaktorsautentisering (2FA)

> Tvåfaktorsautentiseringen, eller 2FA som den också kallas, fungerar som ett extra säkerhetssteg vid inloggning till AirKey-onlineadministrationen. Förutom användar-ID och lösenordet begärs dessutom en SMS-kod under inloggningen som en extra säkerhet. Om tvåfaktorsautentiseringen aktiveras bland inställningarna kommer den att användas av alla som administrerar låssystemet. Klicka på ***Aktivera tvåfaktors-autentisering*** om du vill aktivera funktionen.



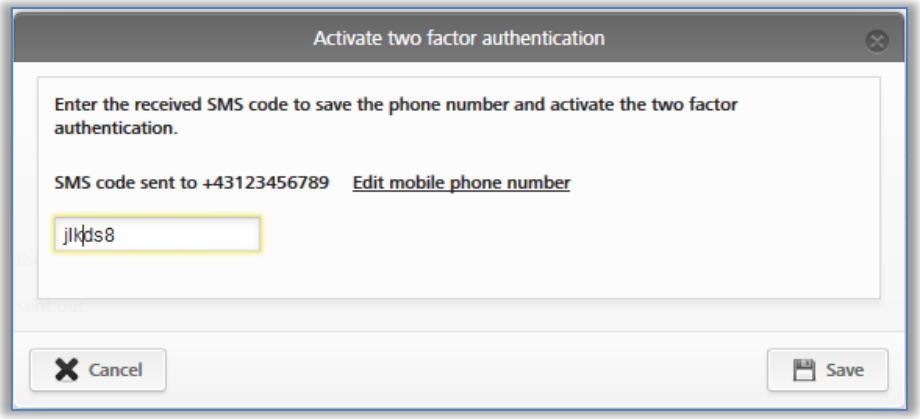
Figur 111: Allmänna inställningar – tvåfaktorsautentisering (2FA)

> Ange det mobiltelefonnummer som ska användas för tvåfaktorsautentisering av den administratör som är inloggad för närvarande och klicka sedan på ***Skicka SMS-kod***.



Figur 112: Ange det mobiltelefonnummer

> En SMS-kod skickas till det telefonnummer som tidigare angetts. SMS-koden ska bekräftas i dialogen inom AirKey-onlineadministrationen, bekfräfta med ***Spara***.



Figur 113: Inställningar för SMS-kodsinmatning

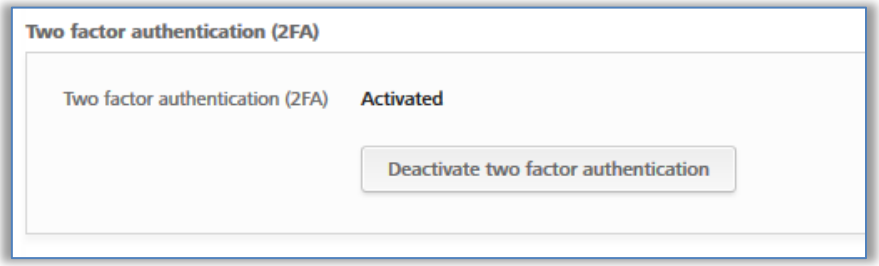
Om en giltig SMS-kod används aktiveras tvåfaktorsautentiseringen för alla som administrerar låssystemet. Statusen ändras på motsvarande sätt bland inställningarna.

SMS-koden är giltig i 5 minuter. Om de fem minuterna överskrids måste proceduren upprepas.

Vid tidpunkten för aktiveringen krävs en mobiltelefon för varje inloggning. Detaljer om hur inloggningsprocessen fungerar med aktiverad tvåfaktors-autentisering finns i avsnittet AirKey-inloggning med tvåfaktorsautentisering.

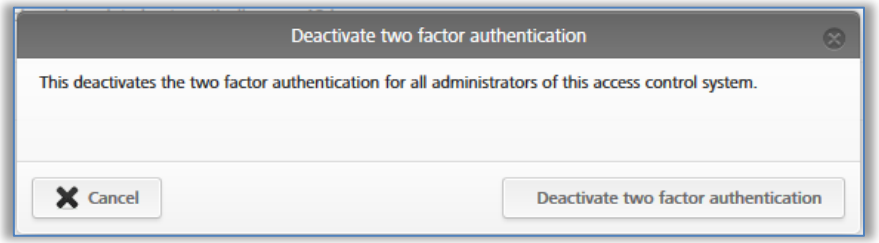
Följ dessa steg om du vill inaktivera tvåfaktorsautentiseringen:

> Klicka på ***Inaktivera tvåfaktorsautentisering***.



Figur 114: Inaktivera tvåfaktorsautentisering

> Bekräfta frågan med ***Inaktivera tvåfaktorsautentisering***.



Figur 115: Inaktivera tvåfaktorsautentisering

Funktionen inaktiveras igen för alla administratörer av låssystemet.

AirKey Cloud Interface (API)

AirKey Cloud Interface är ett REST-gränssnitt (API) för tredjepartssystem. Gränssnittet gör det möjligt att styra vissa funktioner i AirKey via en tredjepartsprogramvara. Mer information om AirKey Cloud Interface finns i avsnittet AirKey Cloud Interface (API).

AirKey Cloud Interface (API) – testmiljö

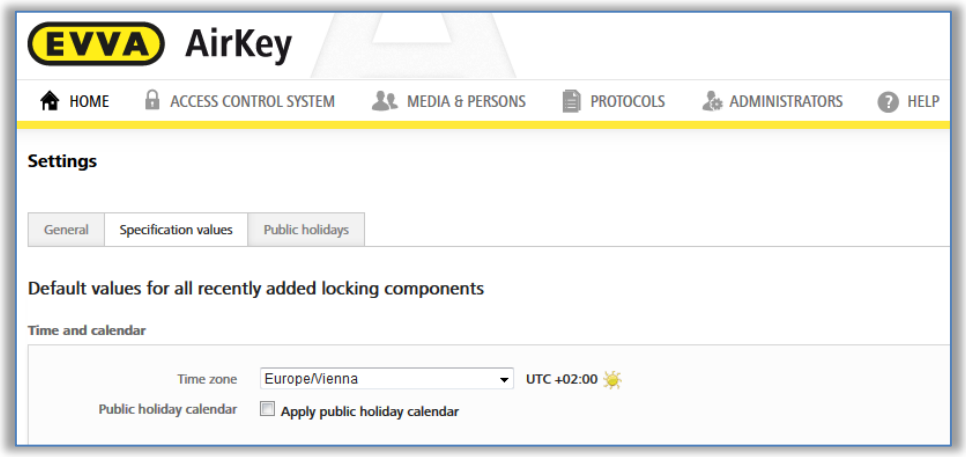
I testmiljön får du möjlighet att testa AirKey Cloud Interface (API) i en skyddad miljö före aktiveringen. Detaljerna kring detta finns i avsnittet AirKey Cloud Interface (API).

5.4.2 Standardvärden (för alla nyligen tillagda låskomponenter)

Dessa inställningar aktiveras automatiskt när man lägger till en ny AirKey-komponent. Vi rekommenderar att standardvärdena specificeras vid den första installationen för att administratörerna lättare ska kunna hantera system. Detta gäller särskilt för större AirKey-system.

Tid och kalender

Med AirKey-system kan man hantera AirKey-enheter som befinner sig i olika tidszoner. Tidszonen "Europa/Wien" (UTC+01:00 för vintertid och UTC+02:00 för sommartid), som gäller i Centraleuropa, är inställd som standard.



Figur 116: Standardvärden för nya AirKey-enheter

Klicka i rullgardinsmenyn och välj korrekt tidszon från listan om man vill ändra tidszonen för hela AirKey-systemet.

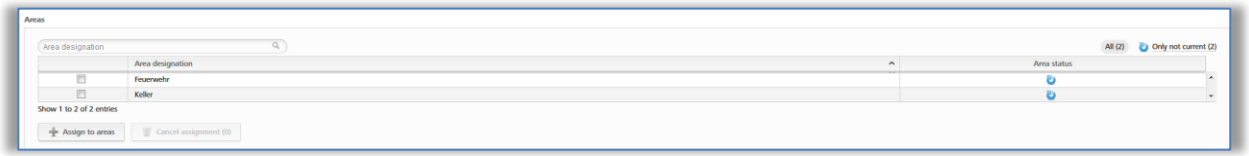
På startsidan ***Home*** klicka på rutan ***Cylindrar*** eller ***Väggläsare***, väljer önskad AirKey-enhet och bläddrar till fliken ***Inställningar*** om man vill ändra tidszonen för en av AirKey-komponenterna. I avsnittet ***Tid och kalender*** finns en rullgardinslista med tidszonerna.

Solsymbolen i respektive tidszon indikerar om sommar- eller vintertid är aktiv för tillfället.

- Gul sol = sommartid
- Grå sol = vintertid

Klicka i rutan ***Använd helgdagskalender*** så kommer de allmänna heldagar som sparats och aktiverats i fliken ***Helgdagar*** (se kapitlet Allmänna helgdagar) att överföras till den nya AirKey-enheten.

Områden

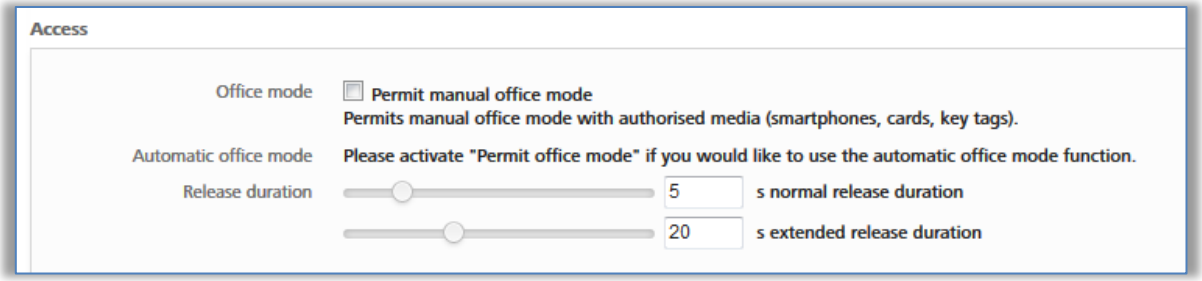


Figur 117: Standardvärden – områden

I det här avsnittet förklaras hur man automatiskt tilldelar nya AirKey-enheter till områden som redan är skapade. Se Tilldela områden för mer information om var och hur man skapar områden.

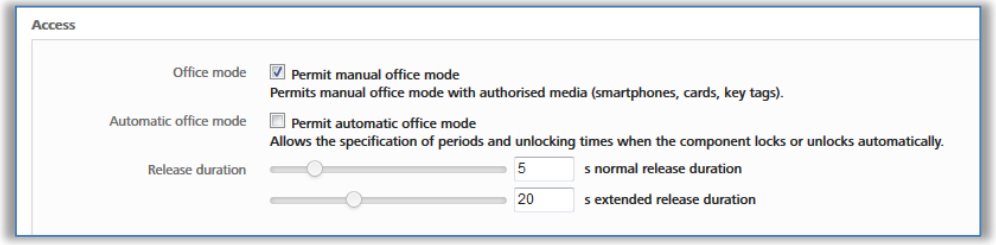
Den här funktionen är särskilt användbar för huvudnycklar eller brandkårsnycklar som alltid måste ha behörighet till alla enheter. Det går även att annullera tilldelade områden från motsvarande AirKey-enheter.

Tillträde



Figur 118: Standardvärden – behörighet

I det här avsnittet beviljas manuella kontorslägen för alla nyligen tillagda AirKey-enheter. Klicka för rutan ***Tillåt manuellt permanent öppning*** för att öppna en extra kryssruta: ***Aktivera automatiskt permanent öppning***.

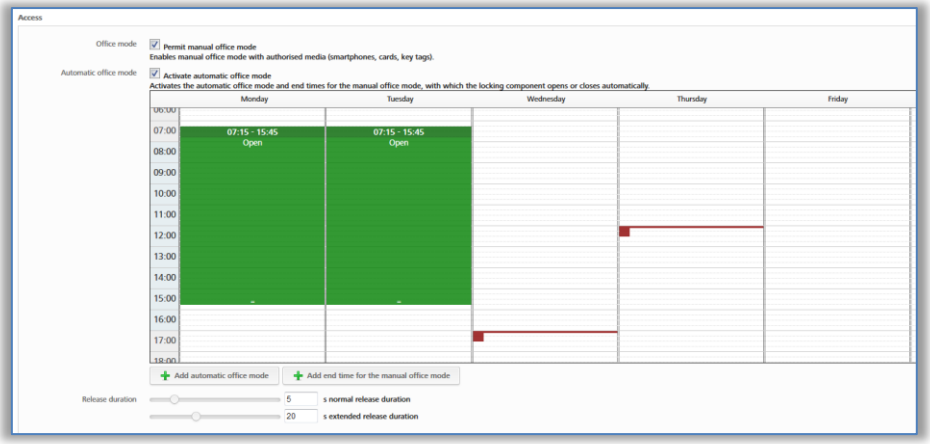


Figur 119: Automatiskt kontorsläge

I det automatiska kontorsläget kan man specificera perioder och upplåsningstider då AirKey-enheten aktiveras eller avaktiveras automatiskt. Man kan till exempel specificera att kontorsläget ska upphöra automatisk varje kväll kl. 17.00 i en kontorsbyggnad. För AirKey-cylindrar betyder det att de är avaktiverade. Man ska alltid fysiskt kontrollera att dörren är låst. Använd ett behörigt medium för att aktivera och därefter manuellt låsaupp dörren.

I detta fönster kan du även ställa in en sluttid för den manuella permanenta öppningen. Detta säkerställer att den permanenta öppningen avslutas vid den definierade tiden (rött fält i skärmdumpen nedan), även om den är aktiverad. Per dag kan högst 4 poster (perioder eller sluttider) ställas in.

På helgdagar, vid varning om tomt batteri, om enheterna har fel tid eller i samband med uppdatering av firmware avslutas de permanenta öppningarna automatiskt eller startas inte alls.



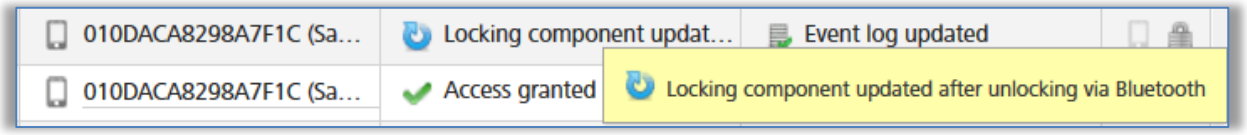
Figur 120: Automatisk permanent öppning

Öppningstiden specificerar hur länge AirKey-enheten är aktiverad (när det gäller till exempel cylindrar är detta den tid då användaren måste vrida cylinderns vred manuellt). Standardtiden för aktivering är 5 sekunder och den förlängda tiden är 20 sekunder. Anpassa tiden för aktivering individuellt här. Tiden kan ställas in på mellan 1 och 250 sekunder.

Med alternativet ***Uppdatering efter varje upplåsning*** gör att enheterna och loggfilen uppdateras vid varje aktivering med Bluetooth. Enheten och loggfilen uppdateras med bluetooth i realtid om det gått minst 6 timmar sedan senaste uppdateringen / aktiveringen.

Användaren märker inte av denna uppdatering. Det avges alltså ingen signal och det visas inget meddelande på smarttelefonen.

Uppdateringen av loggen visas i AirKey-onlineadministrationen.



Figur 121: Loggning – Uppdatering efter upplåsning

Vid aktivering med bluetooth uppdateras följande i loggfilen:

- Blacklist
- Tidszon
- Tid
- Logg

Har enheten ej genomförda firmware-uppdateringar eller funktionsändringar, måste de uppdateras på det sätt som beskrivs i kapitlet Uppdatera låskomponenter.

Denna funktion kräver en bra anslutningskvalitet på telefonen. Se därför till att ha en stabil internetanslutning via 3G resp. via WLAN.

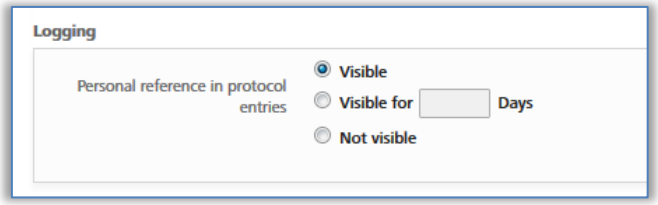
Uppdatering efter en aktivering med Bluetooth genomförs även när den manuella permanenta öppningen startas, dock inte när denna avslutas.

Uppdatering efter en aktivering via Bluetooth sker inom enhetens aktiveringsperiod. Är aktiveringsperioden mindre än 10 sekunder kan det hända att uppdateringen vid aktiveringen med Bluetooth inte fungerar. Aktiveras funktionen "automatisk uppdatering" ökas värdet för aktiverings-perioden automatiskt till 10 sekunder på enheten.

När funktionen är aktiverad ökar batteriförbrukningen hos batteridrivna enheter, t.ex. AirKey-cylindrar. Det påverkar batteriets livslängd.

Loggning

Välj standardvärdet för poster i den personliga händelseloggen inom ramen för tillträdes-händelser. Det finns tre funktioner för detta ändamål:

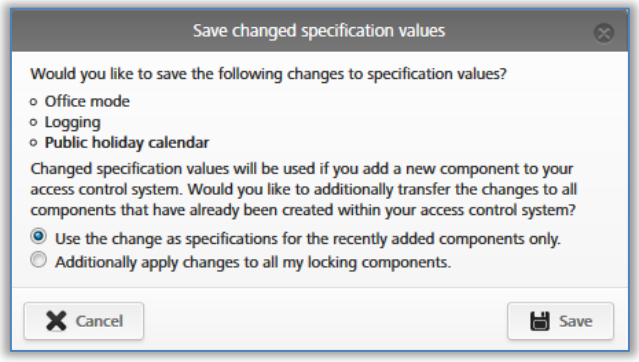


Figur 122: Definiera loggning/händelseloggar

Synliga aktiverar permanent visningen av personuppgifter för tillträdeshändelser.
Synliga för ... dagar personuppgifterna för tillträdeshändelserna blir anonyma efter det specificerade antalet dagar.
Inte synliga anonymiserar omedelbart alla personuppgifter för tillträdeshändelser.

De specificerade standardvärdena kan ändras för enskilda AirKey-enheter, oberoende av inställningarna här.

Klicka på knappen ***Spara*** för att spara de ändrade standardvärdena. Systemet frågar om de ändrade standardvärdena ska gälla för nyligen tillagda eller alla AirKey-enheter.



Figur 123: Spara ändrade specifikationsvärden?

5.4.3 Allmänna heldagar

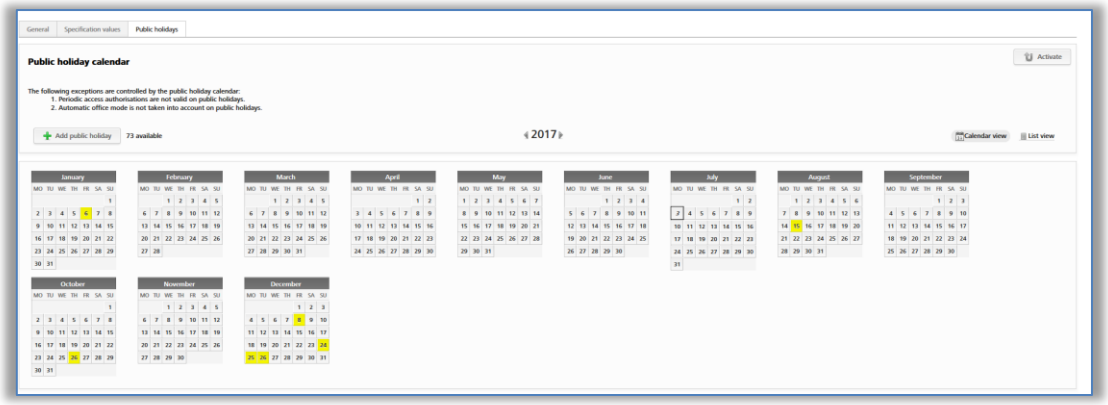
Definiera upp till 80 allmänna helgdagar per år i fliken ***Helgdagar*** (aktuellt år och de två efterföljande åren). I AirKey kan begreppen "Allmän helgdag" tolkas som en allmän helgdag

eller som en period av flera dagar såsom företagssemester eller skollov (kan vara återkommande). Man kan till exempel specificera att en nationell, allmän helgdag som inträffar på samma datum varje år ska anges på nytt varje år. En veckas skollov räknas som en allmän helgdag i systemet om perioden definierats mellan "start – slut".

Effekter i samband med allmän helgdagar:

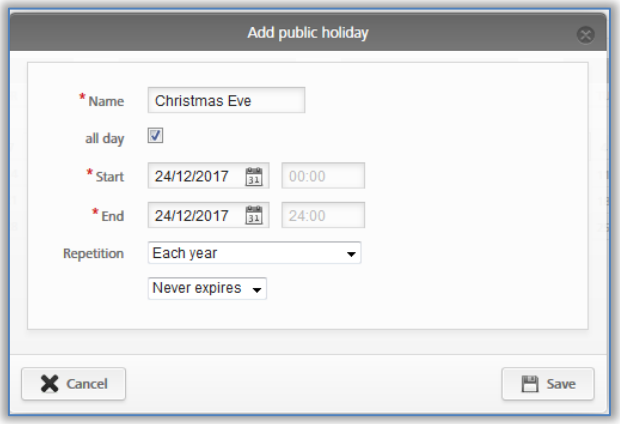
1. Periodisk behörighet gäller inte på allmänna helgdagar.
2. Det automatiska kontorsläget aktiveras inte på allmänna helgdagar.

Klicka på knappen ***Aktivera*** på höger sida för att aktivera den allmänna helgdagskalendern globalt.



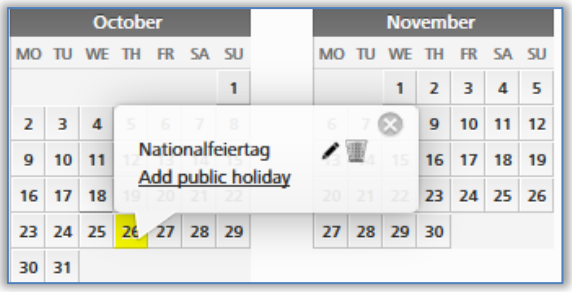
Figur 124: Allmän helgdagskalender (kalendervy)

Klicka på knappen ***Lägg till helgdag*** eller klicka på det exakta datumet för den allmänna helgdagen i kalendervyn (t.ex. 24/12) för att öppna ett dialogfönster för att ange namnet på den allmänna helgdagen, huruvida den allmänna helgdagen varar hela dagen eller t.ex. endast på eftermiddagen och mellan vilka perioder den allmänna helgdagen gäller (specificera t.ex. även företagssemestrar här) samt definiera hur många gånger den återkommer och när de specificerade uppgifterna inte längre gäller.



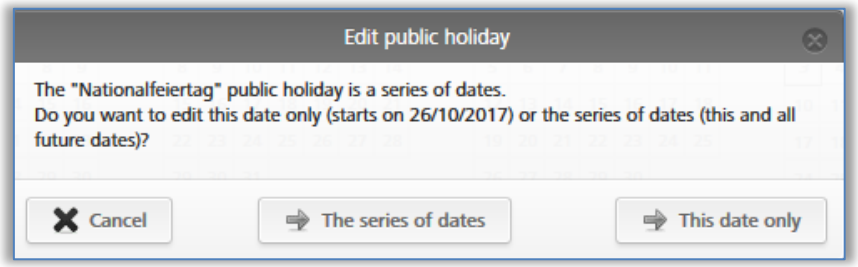
Figur 125: Lägga till helgdag

Man kan redigera varje angiven allmän helgdag i efterhand. Klicka helt enkelt på respektive ruta för att öppna en textruta.

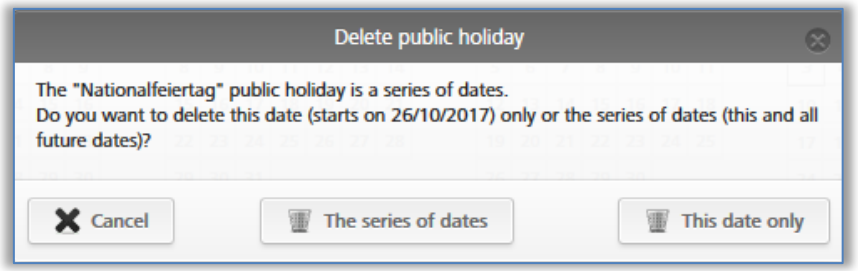


Figur 126: Lägga till allmänna helgdagar i kalendern

Klicka på länken ***Lägg till helgdag*** för att lägga till ytterligare en allmän helgdag på denna dag. Man kan ange flera allmänna helgdagar för samma kalenderdag. Klicka på pennsymbolen för att redigera den allmänna helgdagen. Klicka på soptunnan för att ta bort den allmänna helgdagen.

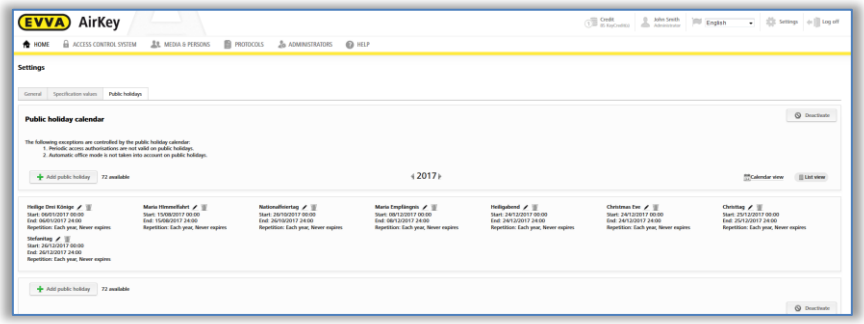


Figur 127: Redigera helgdag



Figur 128: Ta bort allmänna helgdagar

När man har lagt till semestrar eller allmänna helgdagar i kalendern visar systemet en översikt över alla sparade allmänna helgdagar, etc.

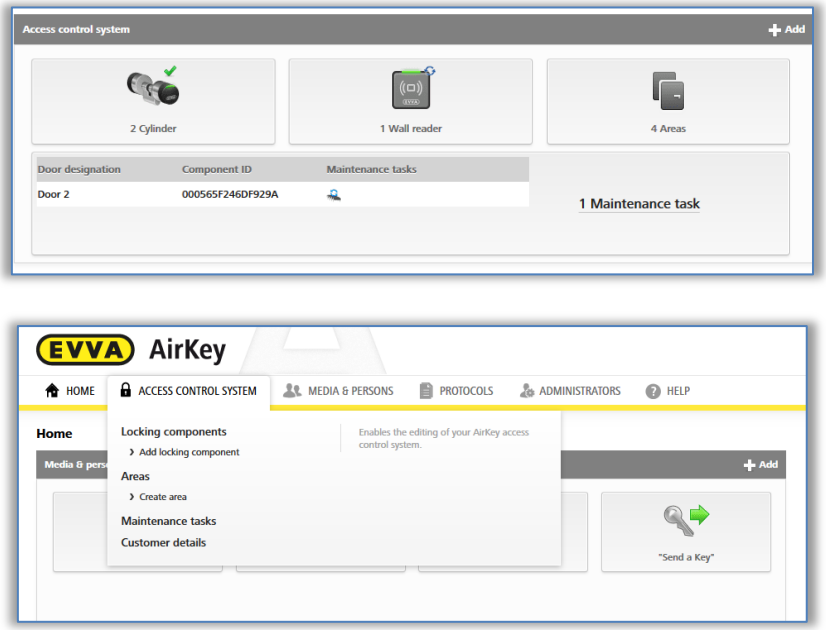


Figur 129: Allmän helgdagskalender (listvy)

Välj knappen ***Avaktivera*** för att avaktivera den allmänna helgdagskalendern för AirKey-systemet och för att inte spara den för tillagda AirKey-enheter.

5.5 AirKey-system

Med rutorna på startsidan ***Home*** samt menyerna och undermenyerna i ***Låssystemets*** huvudmeny kan du hantera ditt elektroniska system.

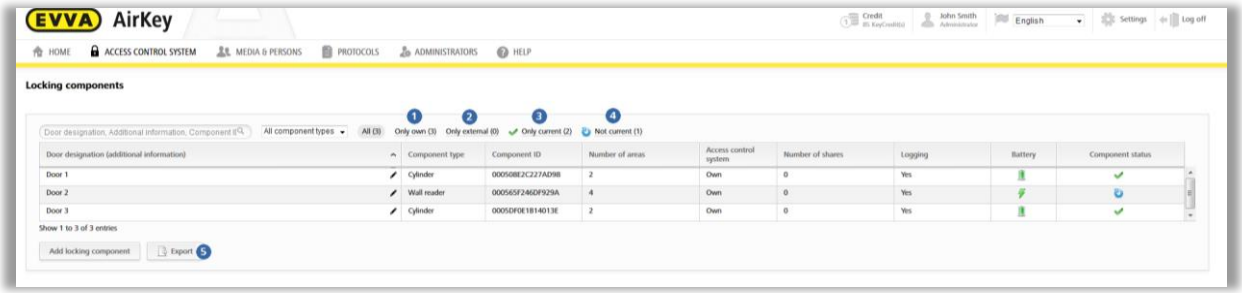


Figur 130: AirKey-system

5.5.1 Översikt över låskomponenter

För att få en översikt över alla enheter inom i systemet från startsidan ***Home*** klicka på rutan ***Cylindrar*** eller ***Väggläsare*** eller gå till ***Låssystem*** → ***Låskomponenter*** i huvudmenyn. På startsidan ***Home*** visas i översikt hur många cylindrar eller väggläsare som har integrerats i ditt system.

Alla enheter listas med extrainformation och status. I den första raden av listan finns sökfältet samt filtreringsfunktioner för enheter.



Figur 131: Låskomponenter

- Vid "Egna" ❶ listas endast dina egna enheter
- Vid "Främmande" ❷ listas enheter som tilldelats från ett annat system (delade enheter).
- Vid "Aktuella" ❸ listas endast enheter med uppdaterad status.
- Vid "Ej aktuella" ❹ listas endast enheter med ej uppdaterad status.
- Exportera ❺ listan med enheter till en CSV-fil för vidare bearbetning.

AirKey gör det möjligt att dela dina enheter med externa Airkey-system. I enhetslistan visas skilnaden mellan dina egna och externa enheter. Mer information finns i avsnittet Auktorisera låskomponenter för andra låssystem.

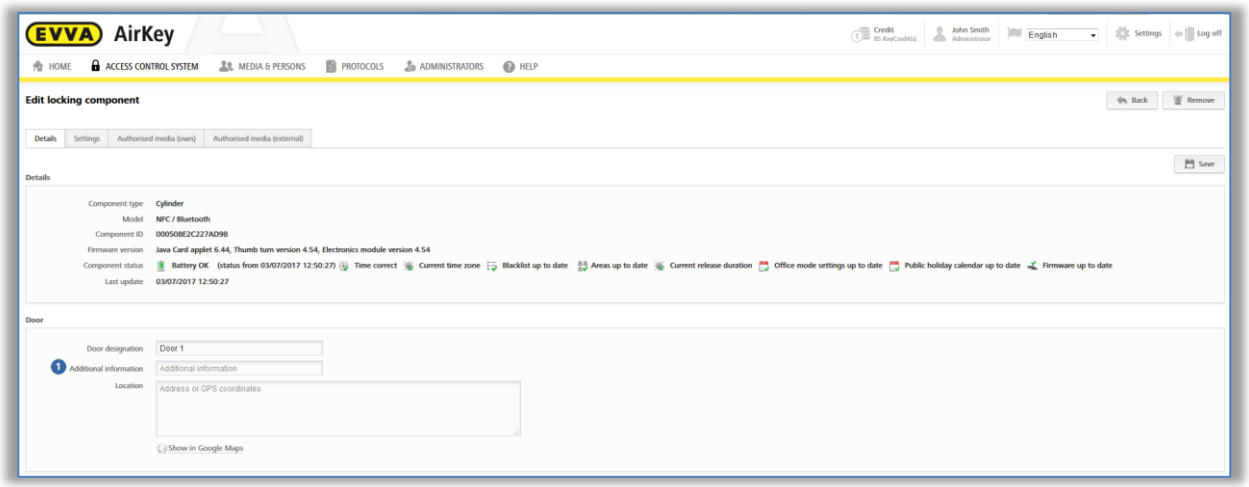
5.5.2 Lägga till låskompnenter: Se kapitel 4.11

5.5.3 Redigera låskomponenter

Applikationsfönstret ***Redigera enhet*** under fliken ***Detaljer*** innehåller olika uppgifter, t.ex. enhetens typ och modell, enhets-ID, programversion och enhetsstatus samt information om dörrar, områden och behörigheter. Här finns även möjlighet att visas AirKey-enhetens position i Google Maps. I fliken ***Inställningar*** ser du alla inställningar för tidszon och helgdagskalender, tillträde samt loggning och reparationsalternativ.

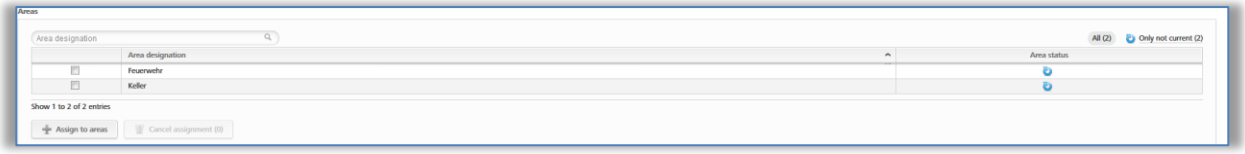
Den batteristatus som visas motsvarar statusen för den senaste uppdateringen eller den senast överförda posten i händelseloggen. Därför kan den faktiska batteristatusen för enheten avvika från den batteristatus som visas i AirKey-onlineadministration.

- På startsidan ***Home*** välj rutan ***Cylindrar*** eller ***Väggläsare***.
- Alternativt kan du välja ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.
- Klicka på den enhet som du vill redigera i listan.
- Du kan till exempel tilldela en valfri dörrbeteckning i fliken **Detaljer**, lägga till valfri information ❶ eller ange positionen eller adressen för enheten. De unika egenskaperna för dessa uppgifter verifieras inom AirKey-systemet.



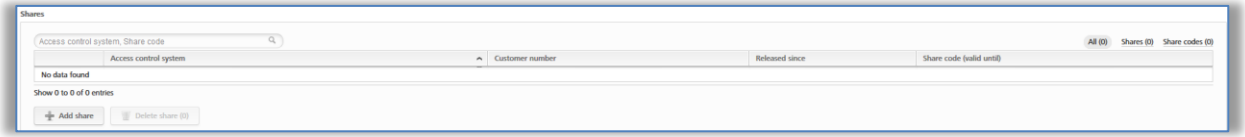
Figur 132: Redigera AirKey-enheter

- Gå till Områden för att redigera tilldelade områden för valda enheter.



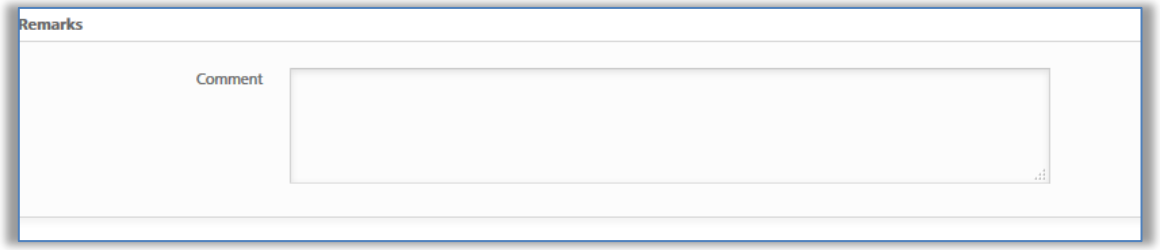
Figur 133: Områden

> Du kan välja att dela enheter med andra AirKey-system. Du kan hantera motsvarade behörigheter i avsnittet "Behörigheter". Se kapitlet Arbeta med flera AirKey-system för mer information om behörigheter.



Figur 134: Dela information

> Om du vill kan du ange en kommentar om en enhet i avsnittet ***Kommentar***.

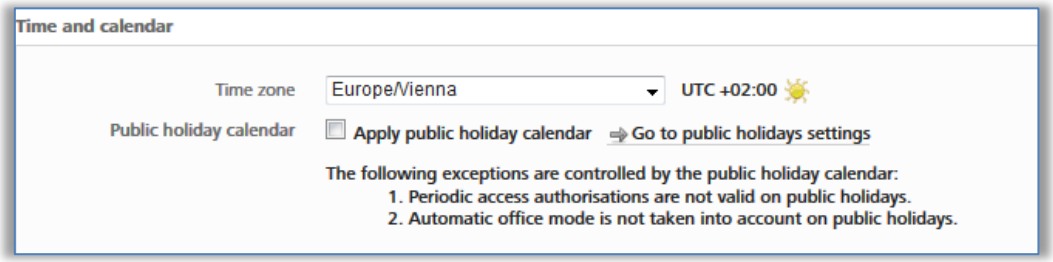


Figur 135: Redigera låskomponenter

I fliken ***Inställningar*** hanteras inställningar för tidszoner, tillträden, loggning och reparationsalternativ.

> Om man arbetar med flera tidszoner inom samma system kan man tilldela en individuell tidszon (som redan har skapats och konfigurerats i AirKey-onlineadministrationen) till varje enhet. Standardtidszonen används som standard.

> I denna process kan man (av)aktivera den allmänna helgdagskalendern för varje enhet. Det finns en länk till den allmänna helgdagskalendern om man behöver dubbelkolla inställningarna för vissa helgdagar.



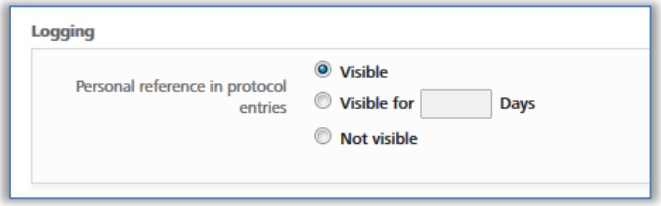
Figur 136: Inställningar – tid och kalender

> Man kan specificera det manuella kontorsläget för varje enhet. Välj en AirKey-enhet för att specificera det manuella kontorsläget för den.

Här kan man ändra tidsinställningar för aktiveringsperioden samt aktivera eller avaktivera funktionen "Uppdatering efter varje upplåsning". Mer information finns i Standardvärden (för alla nyligen tillagda AirKey-enheter).

> Man kan anpassa personliga poster i händelseloggen för varje enhet. Standard-inställningarna används som standard.

- ***Synliga*** aktiverar permanent visningen av personuppgifter för tillträdeshändelser.
- ***Synliga för ... dagar*** anonymiserar personuppgifterna för tillträdeshändelserna efter det specificerade antalet dagar.
- ***Inte synliga*** anonymiserar omedelbart alla personuppgifter för tillträdeshändelser.



Figur 137: Händelseloggar

I detta avsnitt hittar man länken till uppdateringsalternativ. Mer information om reparationsalternativen hittar du under Reparationsalternativ.

> Klicka på ***Spara*** för att bekräfta eventuella ändringar för enheten. Systemet uppmanar dig att bekräfta processen.

En uppdatering för denna enhet kan visas, beroende på vilka uppgifter för enheten som du har redigerat. Ändringarna tas över och uppdaterings uppgifter försvinner när du har uppdaterat enheten med hjälp av en smarttelefon med underhållsbehörighet eller en kodningsstation.

5.5.4 Ta bort låskomponenter

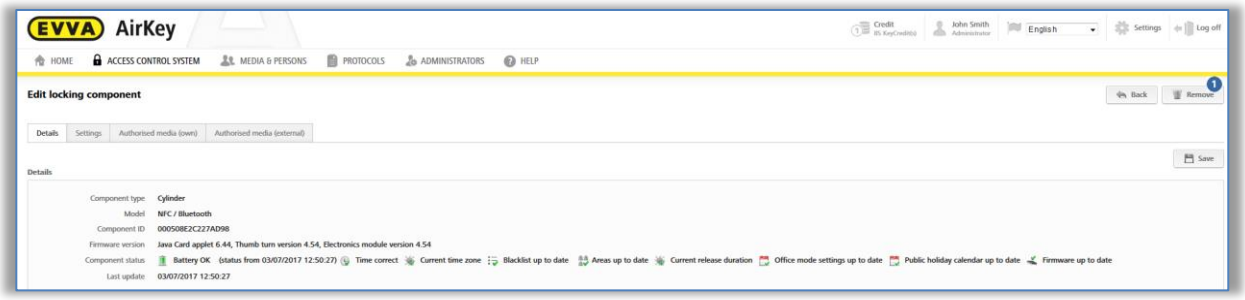
Avaktivera enheter från ett system när de ej behövs.

> På startsidan ***Home*** välj rutan ***Cylindrar*** eller ***Väggläsare***.

> Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.

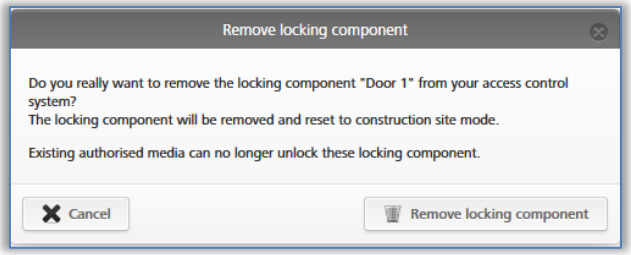
> Klicka på den AirKey-enhet som ska avaktiveras från AirKey-systemet.

> Klicka på ***Ta bort*** ❶ längst upp till höger.



Figur 138: Ta bort låskomponenten

> Klicka på ***Ta bort låskomponenten*** för att bekräfta säkerhetsfrågan.



Figur 139: Säkerhetsfråga

> En säkerhetsfråga och en uppdatering visas för att uppmärksamma på att enheten måste tas bort från AirKey-systemet.

Processen är inte slutförd förrän enheten har uppdaterats med hjälp av en smarttelefon med underhållsbehörighet eller en kodningsstation. När enheten har uppdaterats är den avaktiverad från AirKey-systemet.

Denna process kan inte ångras.

När enheten har tagits bort återställs den till fabriksläge.

Tillträdesmedier som haft behörighet till denna enhet kan inte längre användas för att aktivera enheten. Tillhörande behörigheter tas bort automatiskt och visas inte mer.

5.5.5 Områden

Skapa områden i systemet för att lättare administrera rättigheter.

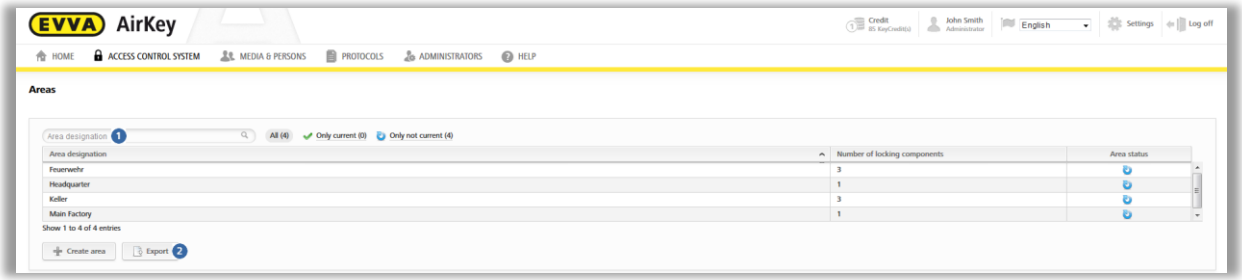
På ***Home*** klickar du på rutan ***Områden*** eller väljer ***Låssystem*** → ***Områden*** i huvudmenyn för att visa en lista över alla områden inklusive deras enskilda statusar.

I listan med områden genomförs följande anpassningar:

> Ange en sökterm med minst tre tecken i sökfältet ❶.

> Klicka på motsvarande kolumn för att fastställa den som sorteringskriterium.

> Exportera listan till en CSV-fil för vidare bearbetning ❷.



Figur 140: AirKey-system – Områden

> Välj önskat område från listan för att se detaljer för det valda området.

5.5.6 Skapa områden

Inga områden är definierade som standard. Skapa nya områden för att kunna lägga till enheter till områden.

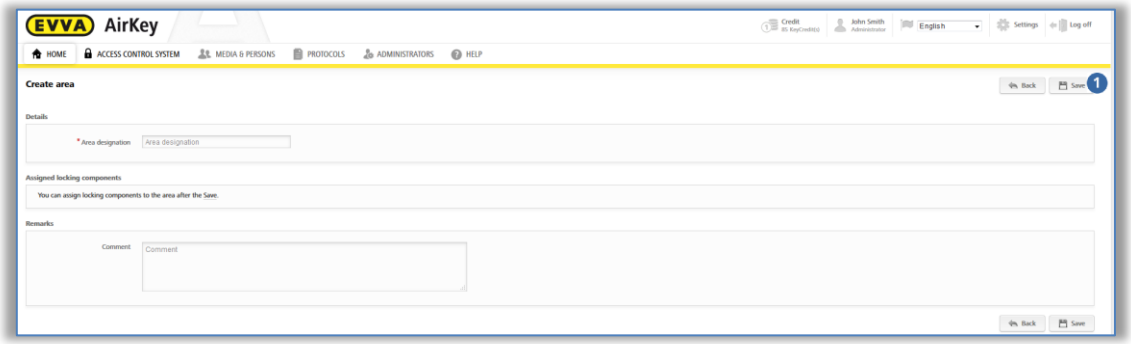
> På startsidan ***Home*** i det grå området ***Låssystem*** klicka på ***Lägg till*** → ***Skapa område***.

> Alternativt välj ***Låssystem*** → ***Skapa område*** i huvudmenyn.

> Ange en unik beteckning för området.

> Dokumentera eventuell tilläggsinformation om området i fältet ***Anmärkningar*** i avsnittet ***Kommentar***.

> Klicka på ***Spara*** ❶.



Figur 141: Skapa områden

Systemet visar meddelandet "Området har sparats" när man har skapat ett område. Man kan endast lägga till enheter till områden när dessa har sparats korrekt.

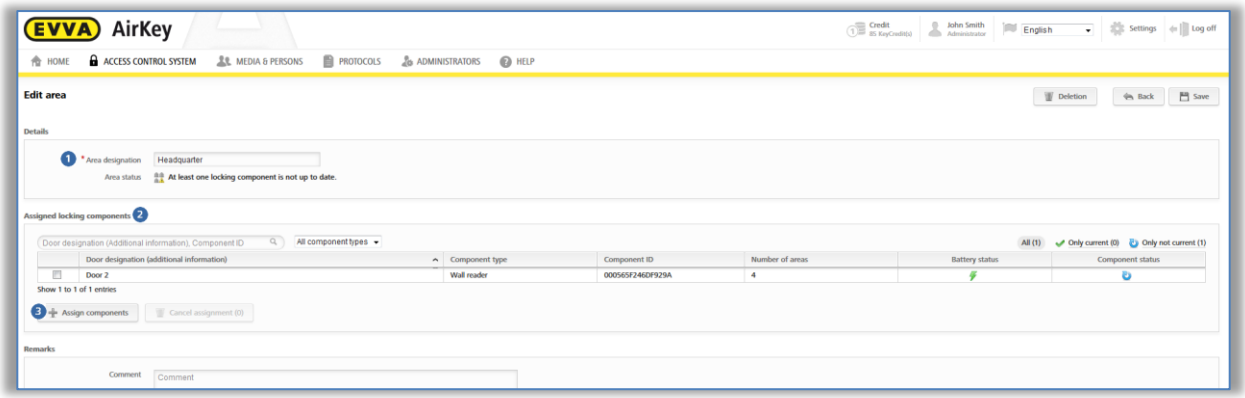
5.5.7 Tilldela AirKey-enheter till områden

> På startsidan ***Home*** välj rutan ***Områden*** eller klickar på ***Låssystem*** → ***Områden*** i huvudmenyn.

> Välj det område på listan som enheten ska läggas till i.

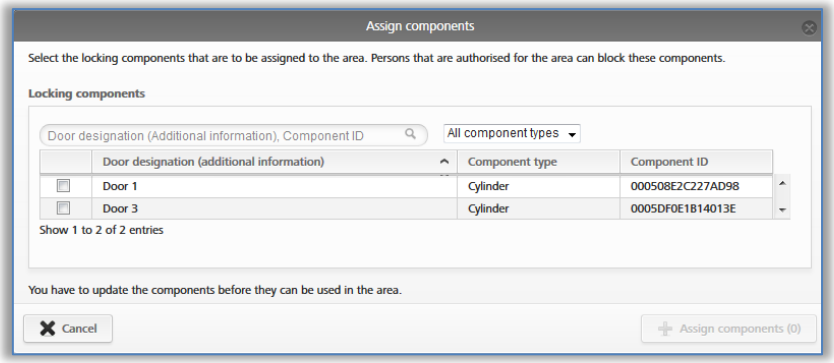
> Detaljer om valt område visas. ***"Områdesstatus"*** ❶ indikerar om alla enheter i området är uppdaterade eller inte. I listan över ***Tilldelade enheter*** listas ❷ alla enheter som är tilldelade till detta område.

> Klicka på ***Tilldela enheter*** ❸ för att lägga till en enhet i området.



Figur 142: Redigera områden

En lista på alla enheter som ännu inte har tilldelats detta område visas.



Figur 143: Tilldela enheter

- Välj önskade enheter (man kan välja flera enheter och även av olika typer).
- Klicka på ***Tilldela enheter*** för att tilldela enheter till området.
- Klicka på ***Spara*** för att bekräfta ändringarna.

Uppdateringar skapas för de berörda enheterna och tas bort från listan efter uppdatering med en smarttelefon eller en kodningsstation. När uppdateringen är klar har tilldelningen av enheter till området slutförts.

En enhet kan tilldelas till högst 96 områden.

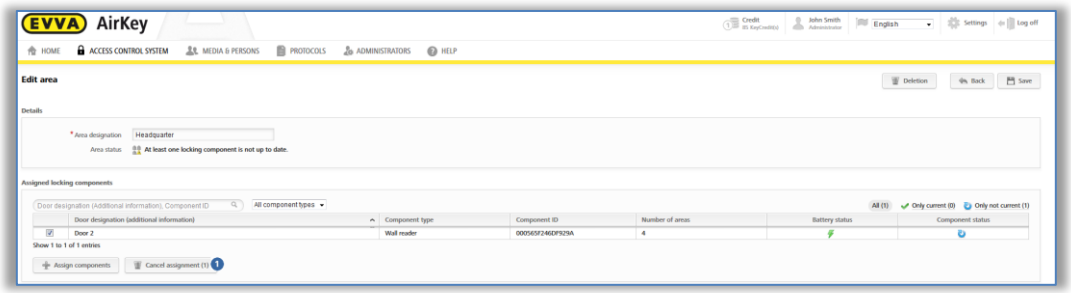
Alternativt kan man redigera tilldelning till områden i enhetens detaljer. Mer information finns i avsnittet Redigera låskomponenter.

5.5.8 Upphäva tilldelningen av låskomponenter till ett område

Gör på följande sätt för att upphäva tilldelningen av en eller flera enheter till ett område:

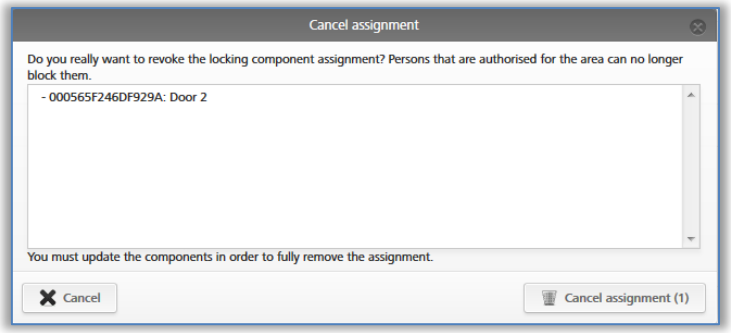
- På startsidan ***Home*** välj rutan ***Områden*** eller klickar på ***Låssystem*** → ***Områden*** i huvudmenyn.

> Välj det område på listan i vilket tilldelningen av enheter ska raderas.
> Markera de enheter som ska raderas från området. Du kan välja flera poster.



Figur 144: Markera AirKey-enheter

> Klicka på ***Radera tilldelning*** ❶.
> Det visas en lista över de enheter för vilka tilldelningen till området ska raderas.
> Bekräfta även denna dialog med ***Radera tilldelning***.



Figur 145: Upphäva tilldelningar

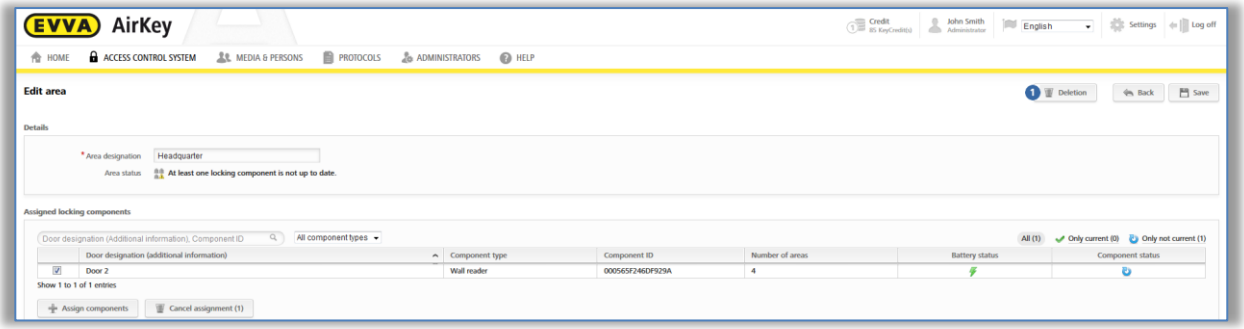
Uppdateringsuppgifter skapas för de berörda enheter som ska raderas från listan och slutförs med en smarttelefon eller en kodningsstation. När uppdateringen är klar har tilldelningen av enheter till området slutförts.

Efter uppdateringen kommer personer som har medier med behörigheter för dessa områden inte att kunna aktivera enheterna för vilka man har raderat tilldelningen.

Alternativt kan man redigera tilldelning av enheter till områden direkt i enhetens detaljer. Mer information finns i avsnittet Redigera låskomponenter.

5.5.9 Radera område

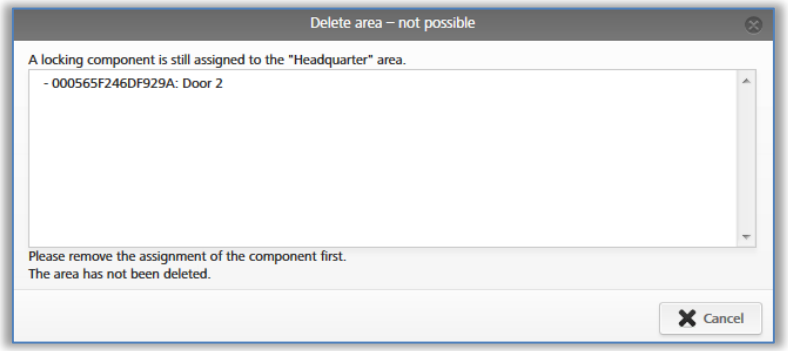
> På startsidan ***Home*** välj rutan ***Områden*** eller klickar på ***Låssystem*** → ***Områden*** i huvudmenyn.
> Välj det område som ska raderas från listan.
> Klicka på ***Radera*** ❶.



Figur 146: Radera områden

Eventuella behörigheter på medier för de raderade områdena tas bort automatiskt och visas inte längre. Raderingen kan inte ångras.

Ett felmeddelande visas om AirKey-enheter fortfarande är tilldelade till området.



Figur 147: Radera områden – ej möjligt

Av denna anledning ska man först radera alla tilldelningar av enheter till områden och därefter upprepa den beskrivna processer. Se kapitlet Upphäva tilldelningen av låskomponenter till ett område för mer information.

5.5.10 Översikt över behörigheter

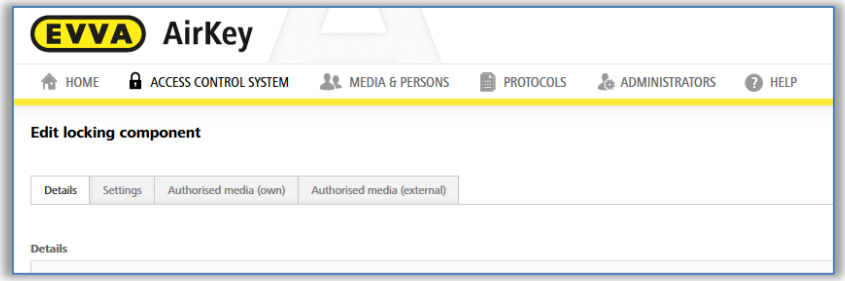
I översikten över behörigheter visas alla behörigheter på medier för varje enskild AirKey-enhet. Översikten över behörigheter gäller den valda enheten.

Alla medier för denna enhet listas. De visade behörigheterna behöver dock inte vara giltiga för tillfället, t.ex. medier med tillfälligt, enskilt tillträde från kl. 8.00 till kl. 17.00 kommer att visas i enhetens översikt även efter kl. 17.00.

> På startsidan ***Home*** välj rutan ***Cylindrar*** eller ***Väggläsare*** eller klickar på ***Låssystem*** → **Låskomponenter**.

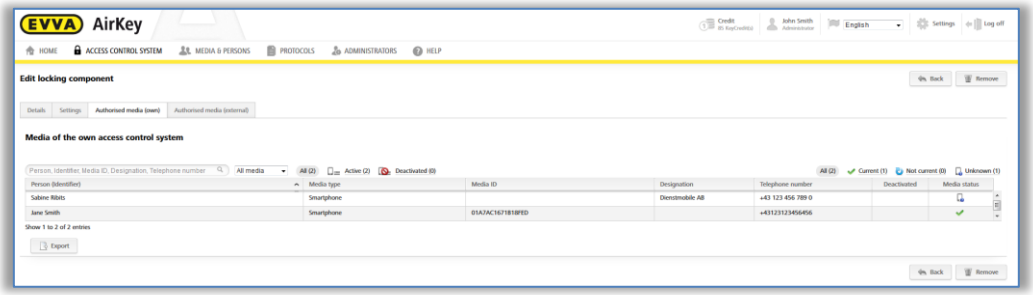
> Välj den enhet för vilken översikten av behörigheter ska visas.

> Bläddra från fliken ***Detaljer*** till ***Behöriga medier (egen)*** för att se behörigheterna för ditt eget system eller välj ***Behöriga medier (externa)*** för att se behörigheter från andra system.



Figur 148: Flikarna "Redigera AirKey-enheter"

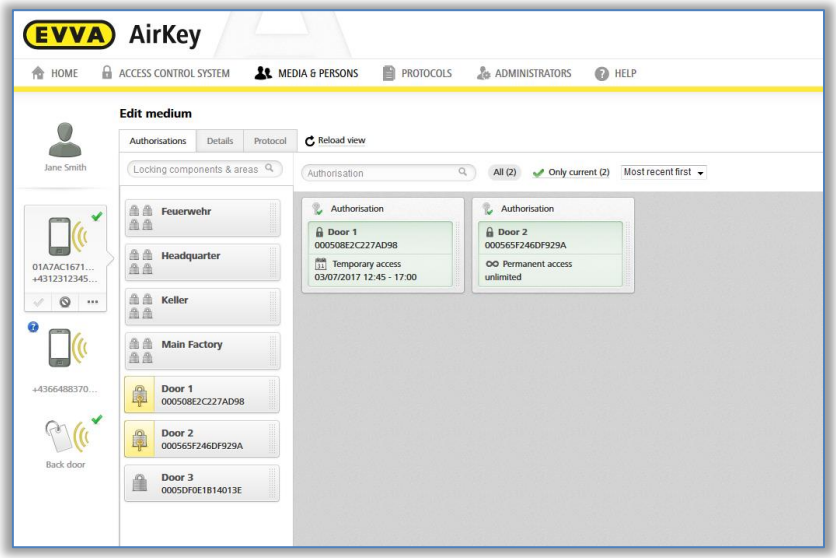
En lista över alla personer samt närstående personer visas. Man kan även se typen av medium.



Figur 149: Behöriga medier (egen)

Man kan söka, filtrera eller sortera listan för att visa specifika behörigheter.

Klicka på en persons namn för att direkt se behörigheter till mediet.



Figur 150: Redigera medier

5.5.11 Underhållsuppgifter / uppdateringar

Vissa funktioner påverkar enhetens konfiguration. Sådana ändringar i konfigurationen kallas underhållsuppgifter / uppdateringar. Följaktligen genomför uppdateringar på enheter som inte är uppdaterade.

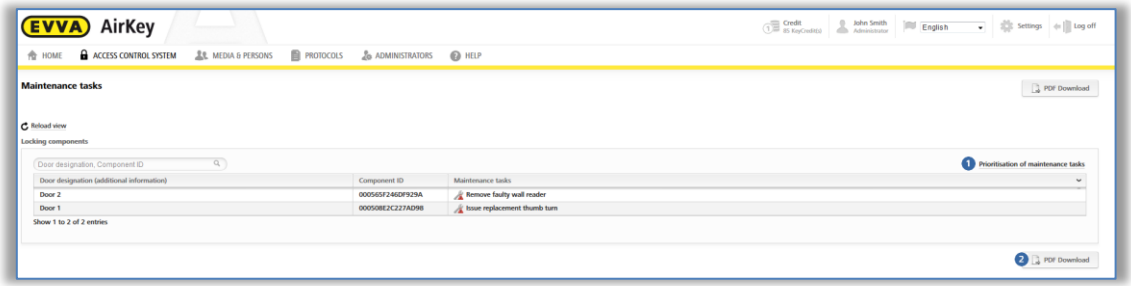
Gör på följande sätt för att se en lista över uppdateringar i systemet:

- På startsidan ***Home*** välj länken ***Uppdaterings uppgifter***.
- Alternativt klickar du på ***Uppdaterings uppgifter*** i statusraden.
- Man kan även välja ***Låssystem*** → ***Uppdaterings uppgifter*** i huvudmenyn.

I detta flik finns en transparent lista på uppdateringar för AirKey-enheter inom AirKey-systemet.

Man kan söka efter dörrbeteckningar eller enhets-ID i listan över uppdateringar. Du kan sortera kolumnen "Dörrbeteckning (extra information)", "Komponent-ID" och "Underhålls-uppgifter".

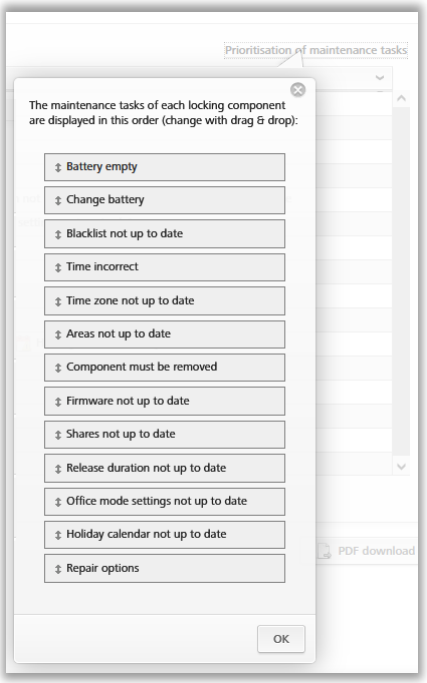
Du kan även prioritera uppdateringar ❶ och skapa en PDF-fil ❷ för utskrift.



Figur 151: Uppdateringar

Prioriteringen av uppdateringar sparas i systemet och visas på smarttelefonen med installerad AirKey-app och aktiverad underhållsbehörighet.

- Klicka på ***Prioritering av underhållsuppgifter***.
- Kunder har olika behov – beroende på applikationerna ska du dra och släppa ❶ objekten i önskad ordning.
- Klicka på ***OK*** för att spara de ändrade uppgifterna.



Figur 152: Prioritering av underhållsuppgifter

Listan med uppdateringar visas nu med de ändrade uppgifterna. Enskilda objekt på listan har länkats till de detaljerade sidorna för motsvarande enheter.

När en uppdatering har slutförts av enheten tas informationen automatiskt bort från listan.

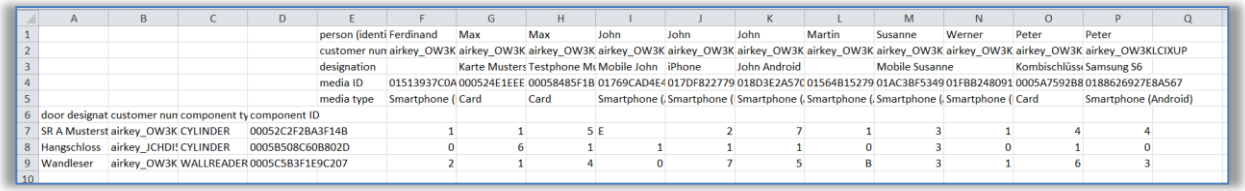
Man kan skapa en lista på alla uppdateringar som ska utföras som PDF-fil och skriva ut det. Detta gör du genom att klicka på knappen ***Ladda ned PDF***.

5.5.12 Kundinformation – låsschema

Man kan i menyn ***Kundinformation*** i efterhand ändra olika uppgifter som angetts vid registreringen, t.ex. namnet på låssystemet, företagsnamnet eller kontaktpersonen.

Längst upp till höger på sidan "Redigera kundinformation" finns en knapp som används för export av låsschemat för hela systemet. Låsschemat är en översikt av alla enheter samt tilldelade smarttelefoner och tillträdesmedier.

- Klicka på knappen ***Exportera låsschema***.
- I dialogfönstret "Exportera låsschema" väljer du knappen ***Exportera***.
- Klicka på den länk i CSV-filen som visas i efterföljande dialogfönster.
- Öppna CSV-filen med önskat program eller spara filen.
- Stäng dialogfönstret "Exportera låsschema" med knappen ***Stäng***.



	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
1					person (identi	Ferdinand	Max	Max	John	John	John	Martin	Susanne	Werner	Peter	Peter	
2					customer nun	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3KLCIXUP	
3					designation		Karte Musters	Testphone Mu	Mobile John	iPhone	John Android		Mobile Susanne		Kombischlüss	Samsung S6	
4					media ID	01513937C0A	000524E1EEE	00058485F1B	01769CAD4E4	017DF822779	018D3E2A57C	01564B15279	01AC3BF5349	01FBB248091	0005A7592B8	0188626927E8A567	
5					media type	Smartphone (	Card	Card	Smartphone (.	Smartphone (	Smartphone (.	Smartphone (.	Smartphone (.	Smartphone (	Card	Smartphone (Android)	
6	door designat	customer nun	component ty	component ID													
7	SR A Musterst	airkey_OW3K	CYLINDER	00052C2F2BA3F14B		1	1	5	E	2	7	1	3	1	4	4	
8	Hangschloss	airkey_JCHDI	CYLINDER	0005B508C60B802D		0	6	1	1	1	1	0	3	0	1	0	
9	Wandleser	airkey_OW3K	WALLREADER	0005C5B3F1E9C207		2	1	4	0	7	5	B	3	1	6	3	
10																	

Figur 153: Låsschema

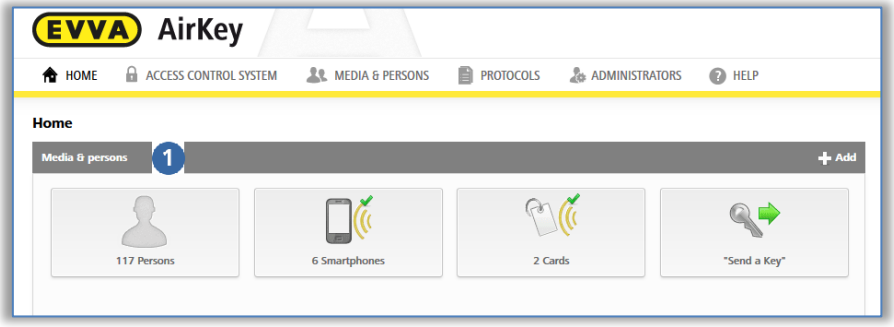
För beräkning av behörighetsstatusen används statusen hos AirKey-onlineadministrationen och inte IST-statusen på mediet. Det innebär att låsschemat är korrekt endast när alla enheter och medier är aktuella / uppdaterade.

Förklaring låsschema:

- **0** – **Ingen behörighet:** Mediet har ingen behörighet för enheten eller för något område enheten är tilldelad till.
- **1** – **Permanent behörighet utan slutdatum:** Mediet har endast en behörighet till enheten eller områden utan slutdatum.
- **2** – **Permanent behörighet med slutdatum:** Punkt (1) är ej tillämplig och mediet har en exakt permanent behörighet med slutdatum för enheten eller det område som är tilldelat enheten och har inga andra behörigheter för enheten eller för något område som är tilldelat enheten.
- **3** – **Periodisk behörighet utan slutdatum:** Punkterna (1) och (2) är ej tillämpliga och mediet har exakt en periodisk behörighet utan slutdatum för enheten eller ett område som är tilldelat enheten och har inga andra behörigheter för enheten eller för något område som är tilldelat enheten.
- **4** – **Periodisk behörighet med slutdatum:** Punkterna (1), (2) och (3) är ej tillämpliga och mediet har exakt en periodisk behörighet med slutdatum för enheten eller ett område som är tilldelat enheten och har inga andra behörigheter för enheten eller för något område som är tilldelat enheten.
- **5** – **Enkel behörighet:** Punkterna (1), (2), (3) och (4) är ej tillämpliga och mediet har exakt en enkel behörighet med slutdatum för enheten eller ett område som är tilldelat enheten och har inga andra behörigheter för enheten eller för något område som är tilldelat enheten.
- **6** – **Individuell behörighet:** Punkterna (1), (2), (3), (4) och (5) är ej tillämpliga och mediet har exakt en individuell behörighet med minst en underbehörighet med slutdatum för enheten eller ett område som är tilldelat enheten och har inga andra behörigheter för enheten eller för något område som är tilldelat enheten.
- **7** – **Multipel behörighet:** Mediet har minst två behörigheter för enheten eller för ett område som är tilldelat enheten. Behörigheterna har ännu inte gått ut.
- **B** – **Blacklist:** Mediet är avaktiverat, dvs. det finns med på blacklist för enheterna. Mediets behörigheter förlorar i så fall sin giltighet.
- **E** – **Utgången behörighet (alla typer):** Alla behörigheter hos mediet för enheten eller ett område som är tilldelat enheten har gått ut.

5.6 Medier och personer

Huvudmenyn ***Medier och personer*** används ❶ för att hantera alla personer, medier och behörigheter inom AirKey-systemet.



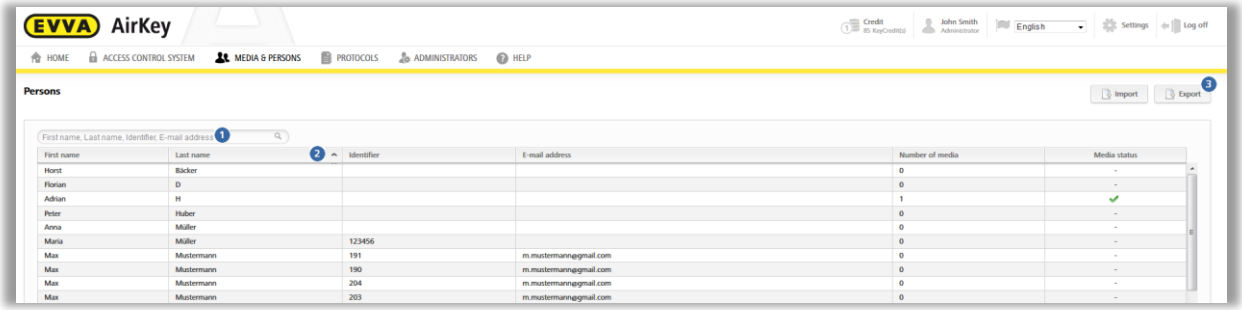
Figur 154: Medier och personer

5.6.1 Översikt över personer

På startsidan ***Home*** välj rutan ***Personer*** eller klickar på ***Medier och personer*** → ***Personer*** i huvudmenyn för att visa en lista över alla skapade personer inklusive antalet medier som de äger samt mediernas status.

Med listan som visas kan du genomföra följande funktioner:

- Ange en sökterm med minst tre tecken i sökfältet ❶.
  Välj förnamn, efternamn, ID eller e-postadress.
- Klicka på motsvarande kolumn för att definierade den som sorteringskriterium ❷.
- Du kan även exportera hela listan till en CSV-fil för vidare bearbetning ❸.



Figur 155: Personer

5.6.2 Skapa personer: Se kapitel 4.7

5.6.3 Redigera personer

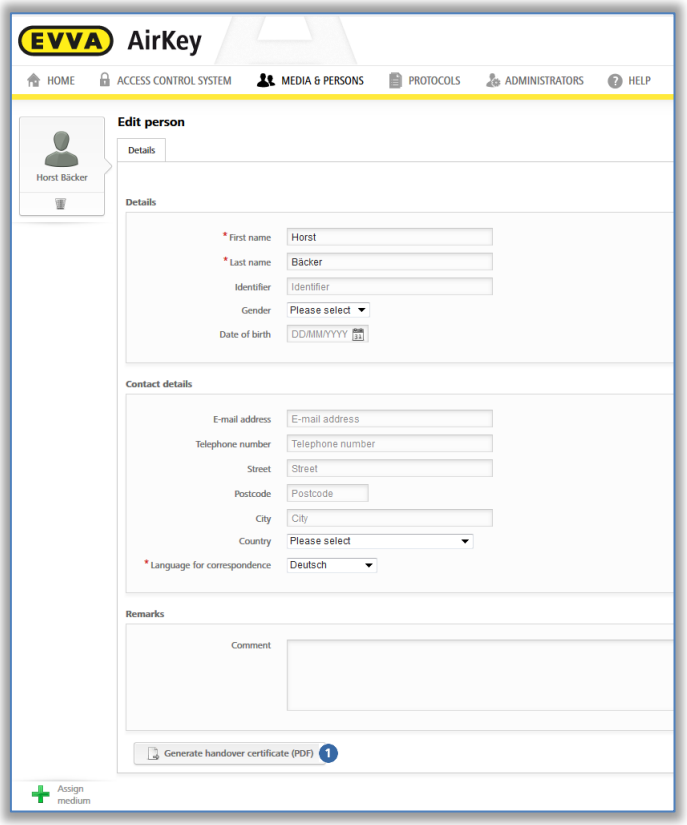
I detaljvyn "Redigera person" kan man ändra personuppgifter och kontaktinformation eller tilldela ett nytt medium.

- På startsidan ***Home*** välj rutan ***Personer***.
- Alternativt välj ***Medier och personer*** → ***Personer*** i huvudmenyn.
- Klicka på namnet på den person som detaljerna ska ändras.
- Ändra önskade uppgifter.

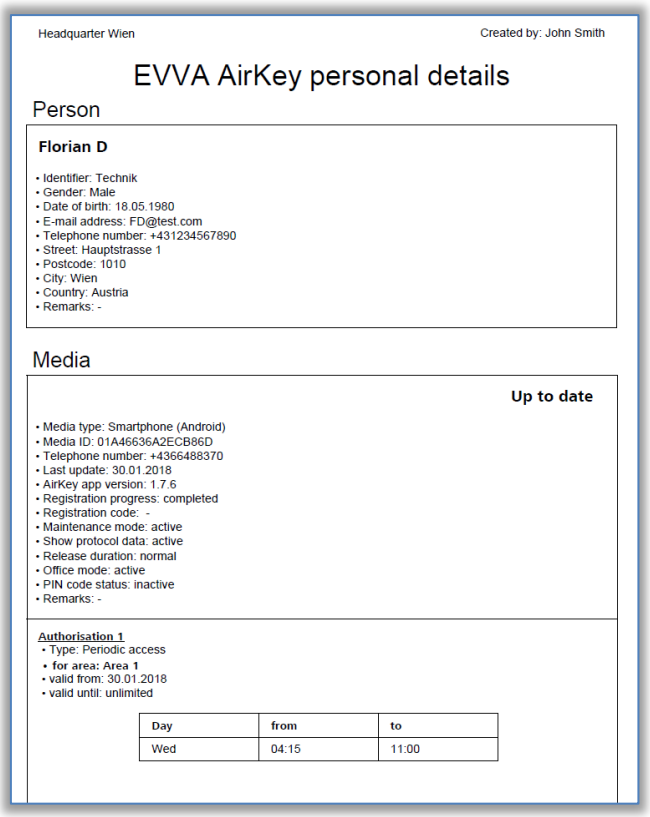
> Klicka på ***Spara***.

På sidan"Redigera person" kan även överföringsbekräftelsen skapas ❶. Detta är en bekräftelse som överförs till personen när alla nödvändiga behörigheter har skapats och tilldelats. Bekräftelsen visar vilka medier med vilka behörigheter som personen innehar vid tiden för utfärdandet.

> I översiktslistan väljer du den person för vilken du vill skapa en överföringsbekräftelse.
> Klicka på knappen ***Generera överföringsbekräftelse (PDF)*** på sidan "Redigera person".
> I dialogfönstret "Generera överföringsbekräftelse (PDF)" visas PDF-filen som länk.
> Klicka på länken och öppna PDF-filen med din PDF-läsare eller spara filen.
> Stäng dialogfönstret med knappen ***Stäng***.



Figur 156: Generera överföringsbekräftelse



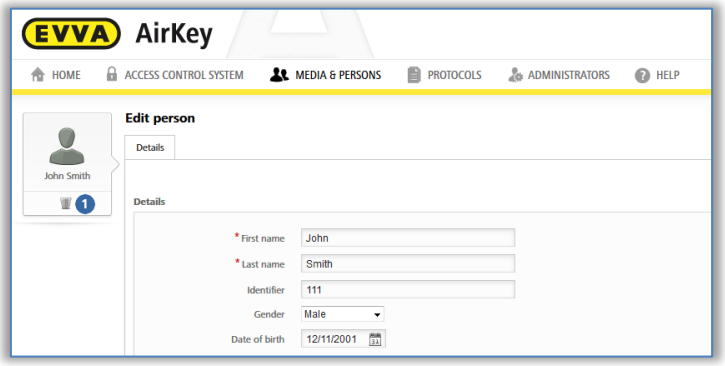
Figur 157: Överföringsbekräftelse (PDF)

5.6.4 Radera personer

Man kan radera personer från AirKey-systemet.

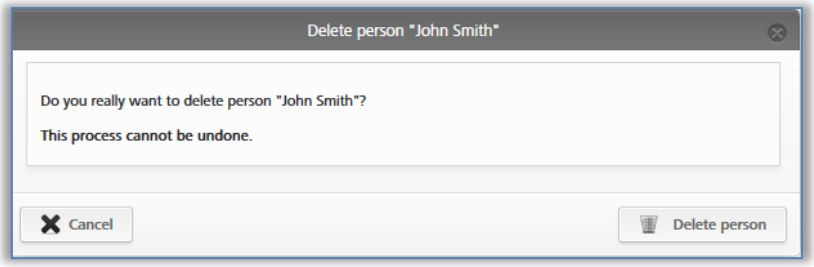
Men inte ta bort personer som fortfarande är tilldelade till medier. Innan radering av en person,Kontrollera att alla tilldelningar av medier har tagits bort från denna person.

- På startsidan ***Home*** väljer du rutan ***Personer***.
- Alternativt välj ***Medier och personer*** → ***Personer*** i huvudmenyn.
- Klicka på namnet på den person i listan som ska raderas.
- Klicka på symbolen med ***soptunnan*** ❶.



Figur 158: Radera personer

> Klicka på "Ta bort person" för att bekräfta säkerhetsfrågan.



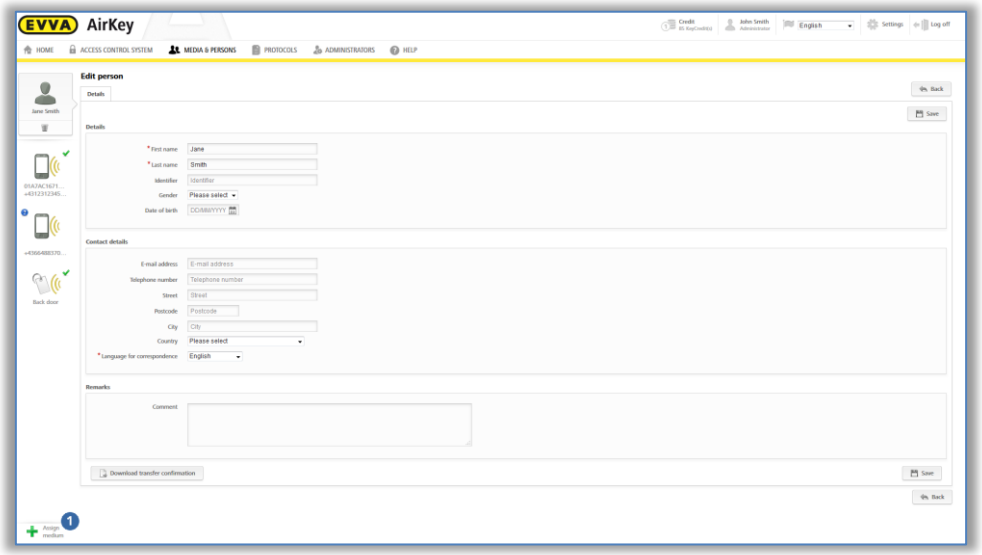
Figur 159: Radera personer – säkerhetsfråga

Raderade personer visas inte längre i listan. Personliga händelseloggar för AirKey-enheter och medier kommer att fortsätta att dokumenteras i händelseloggens poster som är daterade före raderingen.

5.6.5 Tilldela medier till personer

Tilldela mediet till en person för att kunna tilldela behörigheter. Detta är enda sättet att koppla personer till tillträdeshändelser.

> På startsidan ***Home*** välj rutan ***Personer***.
> Alternativt välj ***Medier och personer*** → ***Personer*** i huvudmenyn.
> I listan över personer klicka på den person som ska tilldelas ett medium.
> Klicka på knappen Tilldela medium. ❶

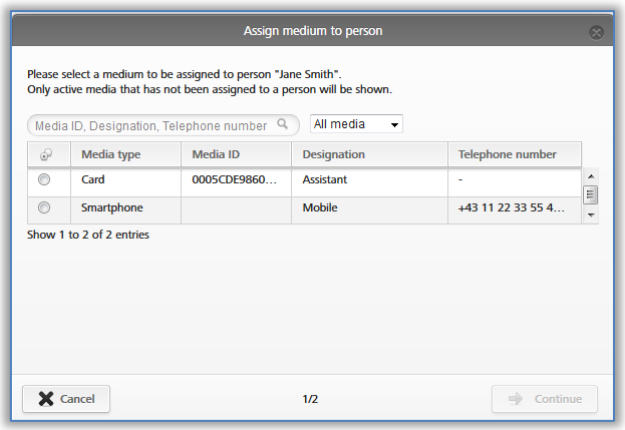


Figur 160: Tilldela medier

En lista med alla medier som kan tilldelas till personen visas.
Man kan sortera listan, filtrera efter mediatypen eller söka efter specifika poster.

Endast medier i AirKey-systemet som inte har tilldelats till personer visas.

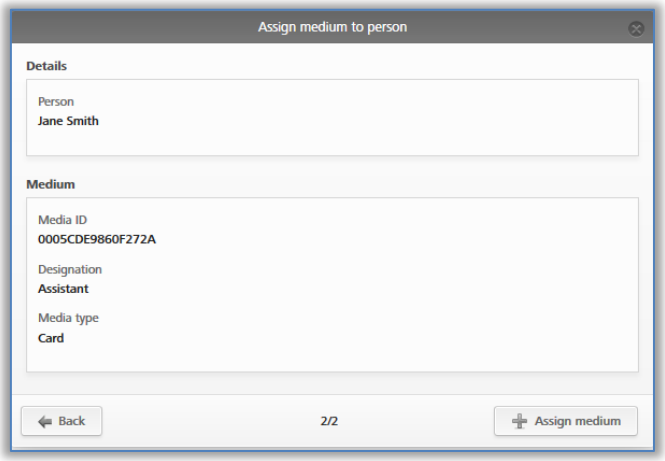
> Välj önskat medium och klicka på ***Fortsätt***.



Figur 161: Tilldela medier till personer

Detaljerna visas efter att mediet är valt. Vid behov klicka på ***Tillbaka*** och välja ett annat medium.

> Klicka på ***Tilldela medium*** för att slutföra processen.



Figur 162: Tilldela medier till personer

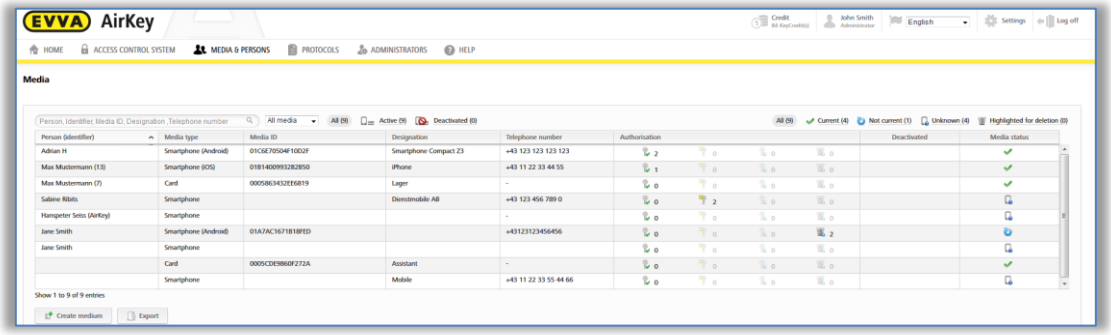
Alternativt kan man även tilldela medier till personer med hjälp av mediet. Mer information finns i avsnittet Tilldela medier till personer.

Du kan även tilldela flera medier (smarttelefoner, kort, nyckelbrickor eller kombinycklar) till samma person.

5.6.6 Översikt över medier

I huvudmenyn ***Medier och personer*** → ***Medier*** finns en lista över alla medier (smarttelefoner, kort, nyckelbrickor eller kombinycklar) med en översikt över alla tilldelade behörigheter, potentiella avaktiveringar samt mediernas aktuella status.

Man kan söka efter medier i medialistan, filtrera efter vissa mediastatusar, ändra sorteringsordningen eller exportera hela listan till en CSV-fil.

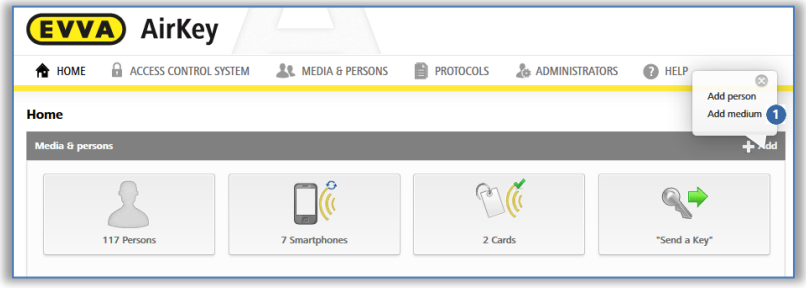


Figur 163: Medialista

5.6.7 Skapa medier

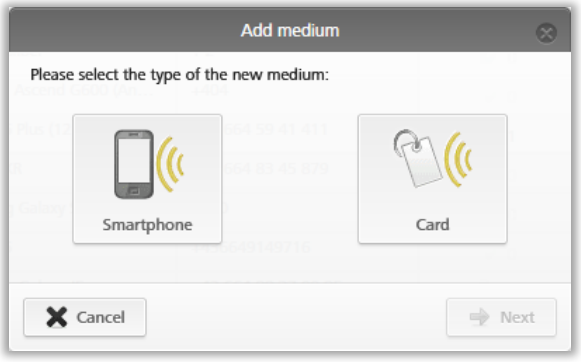
För att hantera medier som del av systemet måste man först skapa dem.

- På startsidan ***Home*** i det grå fältet i avsnittet ***Medier och personer*** klicka på ***Lägg till*** → ***Lägg till medium***.
- Alternativt välj ***Medier och personer*** → **Lägg till medium** i huvudmenyn.
- Alternativt bläddra till startsidan ***Home*** och välj rutan ***Smarttelefoner*** eller ***Kort*** och klicka på ***Lägg till medium***.



Figur 164: Skapa medier

Välj mediatypen för det nya mediet.



Figur 165: Skapa nya medier

Applikationen skiljer inte mellan kort, nyckelbrickor, armband och kombinycklar. Av denna anledning ska man skapa nyckelbrickor, armband och kombinycklar som mediatypen ***Kort***.

5.6.8 Skapa smarttelefoner: Se kapitel 4.8

5.6.9 Skapa kort, nyckelbrickor, armband eller kombinycklar

Finns inte tillgång till en kodningsstation. Lägg till kort, nyckelbrickor, armband eller kombinycklar till systemet med en smarttelefon som har underhållsbehörighet. Mer information finns i Lägga till kort, nyckelbrickor och kombinycklar med en smarttelefon.

- Ange en beteckning och klicka på ***Fortsätt***.
- Placera kortet, nyckelbrickan, armbandet eller kombinyckeln på kodningsstationen.

Den detaljerade vyn för detta medium öppnas automatiskt när processen är slutförd korrekt.

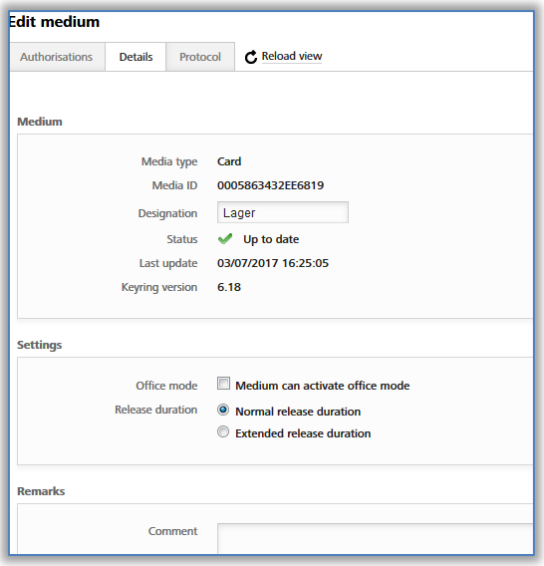
Det är viktigt att man skapar ett tillräckligt antal förkonfigurerade medier (kort, nyckelbrickor, armband eller kombinycklar) med permanenta behörigheter utan begränsningar (nödmedier) och sparar dessa på en säker plats för att kunna betjäna systemet utan tillgång till AirKey-onlineadministration. Mer information om tilldelning av behörigheter finns i Behörigheter.

Använd sidan med RFID-symbolen på kombinyckeln när man lägger till kombinycklar med hjälp av kodningsstationen. Håll kombinyckeln direkt på kodningsstationen. Denna process fungerar inte över kodningsstationens hela avläsningsområde – med den aktuella typen (HID Omnikey 5421) detekteras kombinycklar endast inom övre och den nedre tredjedelen av kodningsstationen.

Se kapitlet Lägga till kort, nyckelbrickor och kombinycklar för mer information om hur man lägger till medier till ett AirKey-system med smarttelefonen som har underhållsbehörighet.

5.6.10 Redigera medier

- På startsidan ***Home*** välj rutan ***Smarttelefoner*** eller ***Kort***.
- Alternativt väljer du ***Medier och personer*** → ***Medier*** i huvudmenyn.
- Välj önskat medium i översiktslistan.
- Välj fliken ***Detaljer*** för att redigera mediet.



Figur 166: Redigera medier – kort

> Klicka på ***Spara*** för att bekräfta ändringarna.

5.6.11 Tilldela personer till medier: Se kapitel 4.13

5.6.12 Behörigheter

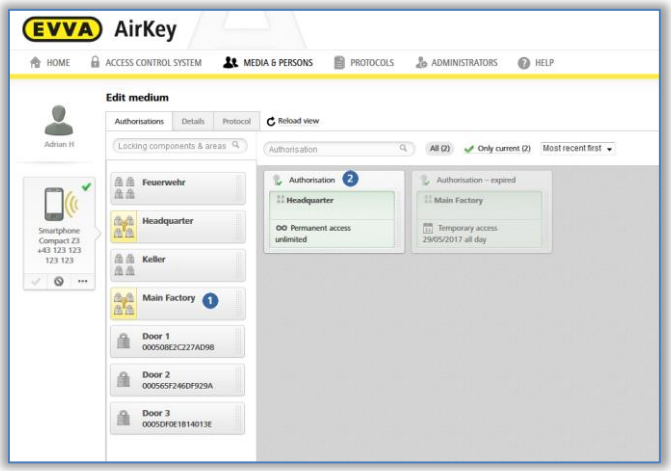
Behörigheter ger personer tillträde till AirKey-enheter. För att kunna skapa behörigheter för medier måste dessa vara tilldelade till personer/användare. Se Tilldela medier till personer för mer information om ämnet.
Gör på följande sätt för att se översikten över behörigheter för ett medium:

> Välj ***Medier och personer*** ⟶ Medier i huvudmenyn.

> Välj önskat medium i översiktslistan.

> Mediet ❶ har redan valts (flera medier kan vara tilldelade samma person).

> Man ser nu alla behörigheter ❷ som har tilldelats.



Figur 167: Översikt över behörigheter

Bakgrundsfärg för behörigheter:

- ***Grön*** = Uppdaterad status, behörighet skapad och medium uppdaterat.
- ***Blå*** = Behörighet skapad, medium ännu inte uppdaterat.
- ***Gul*** = Behörighet har ändrats eller raderats, men inte sparats (skapats).
- ***Grå*** = Behörighet har gått ut.

Alternativt öppna översikten över behörigheter via ***Medier och personer*** → ***Personer*** och välja en person som har tilldelats ett medium i listan. Klicka nu på mediasymbolen på vänster sida under den valda personen.

5.6.13 Tilldela behörigheter: Se kapitel 4.14

5.6.14 Skapa behörigheter: Se kapitel 4.16

5.6.15 Ändra behörigheter

Man kan när som helst ändra behörigheter i AirKey-onlineadministration.

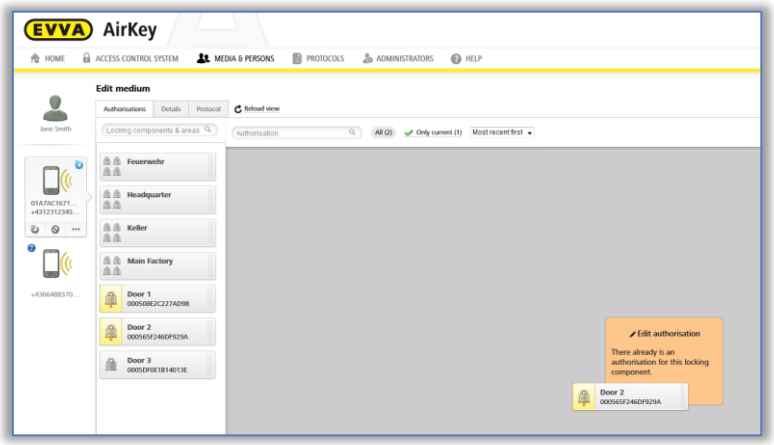
> På startsidan ***Home*** välj rutan ***Smarttelefoner*** eller ***Kort***.

> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

> Välj det medium från listan för vilket man vill ändra behörigheter.

> I fliken "Behörighet" klicka på den behörighet som ska ändras.

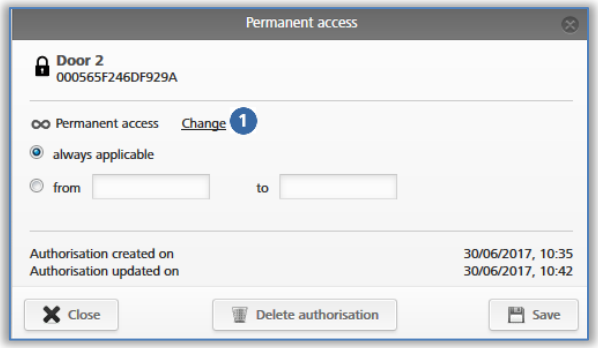
> Alternativt dra och släpp dörren/området till mitten.



Figur 168: Redigera medier – ändra behörigheter

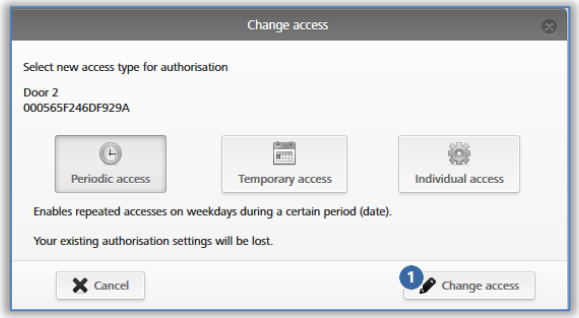
> Systemet visar detaljer för befintliga behörigheter.

> Klicka på ***Ändra*** ❶



Figur 169: Ändra behörigheter

> Välj den nya tillträdestypen.
> Klicka på ***Ändra tillträde*** ❶.



Figur 170: Ändra tillträde

> Ange motsvarande värde för respektive tillträdestyp.
> Klicka på ***Spara***.

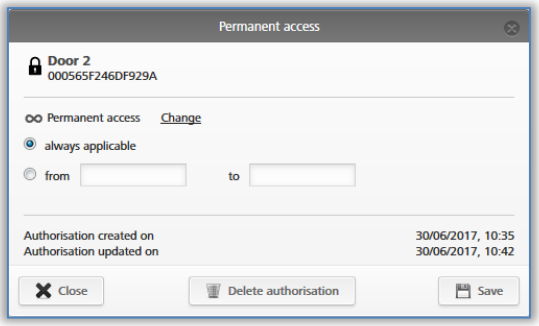
Det måste finnas kredit på ditt KeyCredit-konto för att kunna ändra behörigheter.

> Klicka på den gula knappen ***Skapa 1 behörighet***. Närmare information finns i avsnitt Skapa behörigheter.
> Uppdatera en smarttelefon med "Pull to Refresh" eller ett kort, en nyckelbricka, en kombinyckel eller ett armband med en kodningsstation för att slutföra processen.

5.6.16 Radera behörigheter

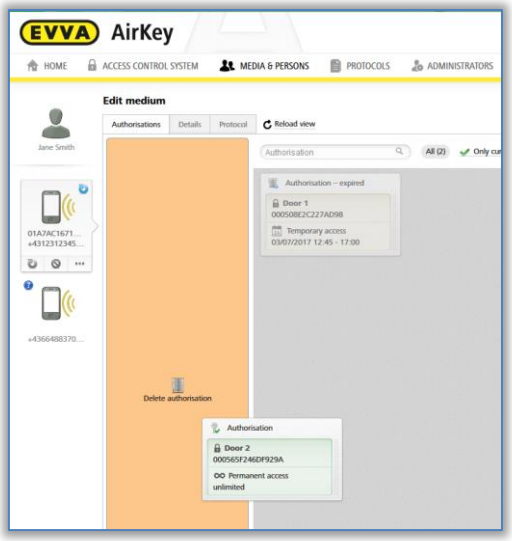
Man kan radera tilldelade behörigheter om de inte längre behövs.

> På startsidan ***Home*** välj rutan ***Smarttelefoner*** eller ***Kort***.
> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
> Välj det medium från listan för vilket behörigheter ska raderas.
> I fliken "Behörighet" klicka på den behörighet som ska raderas.



Figur 171: Permanent tillträde

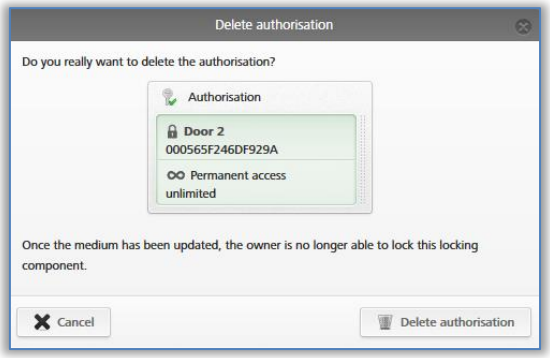
Alternativt dra och släpp dörren/området från mitten till det orange området ***Radera behörighet***.



Figur 172: Radera behörigheter

> Klicka på ***Radera behörighet***.

> Klicka på ***Radera behörighet*** för att bekräfta säkerhetsfrågan.



Figur 173: Radera behörigheter

> Uppdatera en smarttelefon med "Pull to Refresh" eller ett kort, en nyckelbricka, en kombinyckel eller ett armband med en kodningsstation för att slutföra processen.

KeyCredits dras inte från kontot när du raderar behörigheter. Raderingen börjar gälla omedelbart. Mediet måste uppdateras för att slutföra förändringen.

Använd inte funktionen om du tappar bort ett medium. Funktionen används endast för att radera behörigheter på ett fysiskt tillgängligt medium. Om du tappar bort mediet ska du använda funktionen avaktivera / radera medium.

Använd Töm medium för att ta bort alla behörigheter på mediet det gäller.

5.6.17 Avaktivera/radera medier

Använd funktionen "Avaktivera medium" om det finns en säkerhetsrisk och du vill göra alla behörigheter på mediet ogiltiga, till exempel om ett medium har tappats bort eller skadats.

Figur 174: Avaktivera medier

- På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.
- Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
- Välj önskat medium i översiktslistan.
- Klicka på ***Avaktivera medium*** ❶.
- Ange orsaken till avaktiveringen. Välj "Annat" för att aktivera inmatningsfältet (teckenbegränsning: 50 tecken).
- Ange ytterligare information vid behov (max 500 tecken) i "Ytterligare kommentarer".
- Klicka på ***Fortsätt***.
- Klicka på ***Avaktivera medium*** för att bekräfta säkerhetsfrågan.

Figur 175: Avaktivera medier – säkerhetsfråga

En säkerhetsfråga bekräftar att mediet avaktiverats.

Eventuella behörigheter som tilldelats mediet markeras så att de kan raderas. När det gäller kort, nyckelbrickor, armband och kombinycklar skapar systemet omedelbart en post i blacklist för alla aktuella enheter som berörs. För smarttelefonen aktiveras posten endast om telefonen varit utloggad i 5 minuter. En post i blacklist innebär att systemet skapar en uppdateringsuppgift för berörda enheter. En uppdatering krävs för att enheterna skall bli up to date.

- Uppdatera de enheter för vilka mediet har fått behörighet. Uppdateringsuppgifterna försvinner från listan och medier på blacklist, har inte längre behörighet att aktivera enheterna.

Använd inte denna funktion för att radera enskilda behörigheter som är tilldelade till medier. När ett medium avaktiveras påverkas mediets alla behörigheter inom systemet.

Avaktiveringar gäller endast för det berörda systemet. Om en smarttelefon har registrerats i flera system förblir telefonens status uppdaterad i övriga AirKey-system.

Om en person har registrerat en smarttelefon i flera system ska du kontakta administratörerna till de berörda AirKey-systemen för att avaktivera telefonen helt.

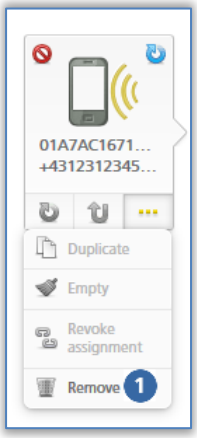
Mediet förblir tilldelat till personen. Ta bort tilldelningen om du vill radera mediet. Mer information finns i avsnittet Radera tilldelningar.

5.6.18 Ta bort avaktiverade medier

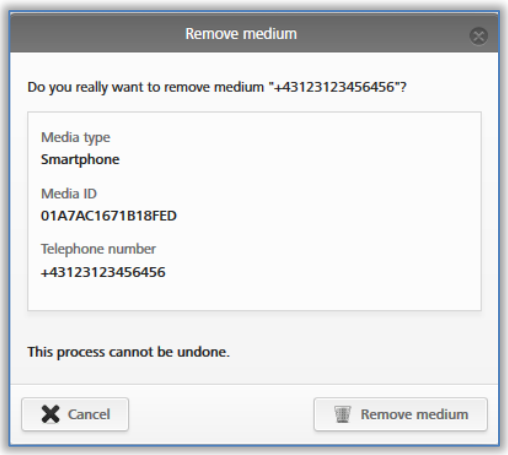
Raddera avaktiverade medier från systemet utan att motsvarande medium är tillgängligt. På detta vis är huvudinformationen i AirKey-onlineadministrationen ren från borttappade, stulna eller felaktiga medier.

Avaktiverade medier kan endast tas bort om mediet har avaktiverats helt. Detta innebär att mediet antingen har uppdaterats eller så har en uppdaterad blacklist överförts till alla enheter för vilka mediet hade behörigheter. Det går inte att ta bort medier förrän villkoren ovan är uppfyllda.

- På ***startsidan Home*** välj ***Smarttelefoner*** eller Kort.
- Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
- I listan över medier, klicka på det avaktiverade mediet som ska bort.
- Klicka på Mer under mediasymbolen och välj ***Ta bort***. ❶
- Bekräfta säkerhetsfrågan med ***Ta bort medium*** för att avlägsna det markerade mediet från systemet.



Figur 176: Ta bort avaktiverade medier



Figur 177: Ta bort medier – säkerhetsfråga

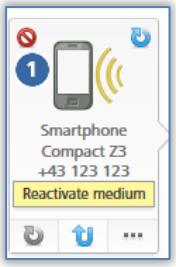
> Ett meddelande visas för att bekräfta att mediet har tagits bort och mediet visas inte längre i systemet.

Denna process kan inte ångras. Media som tagits bort under denna process visas inte längre i systemet och de kan därmed inte längre användas.

Den här processen återställer inte automatiskt mediet till fabriksläge.

5.6.19 Återaktivera medier

Avaktiverade medier (markerade med en röd cirkel ❶) kan återaktiveras om de åter är tillgängliga.



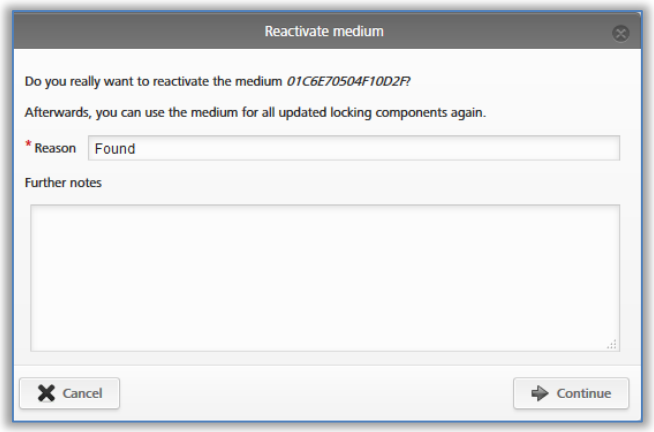
Figur 178: Återaktivera avaktiverade medier

> På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.
> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
> Välj det medium som ska återaktiveras i översiktslistan.
> Klicka på ***Återaktivera medium*** under mediasymbolen.

Figur 179: Återaktivera medier

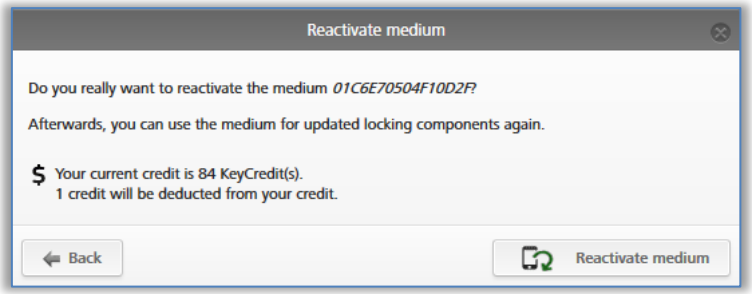
> Ange orsaken till återaktiveringen (max 50 tecken) och avgör om du vill återaktivera behörigheter som var giltiga innan mediet avaktiverades.

Ange ytterligare information vid behov (max 500 tecken) i "Ytterligare kommentarer". Ytterligare information dokumenteras i händelseloggen.



Figur 180: Återaktivera medier

> Klicka på ***Fortsätt***.
> Klicka på ***Återaktivera medium*** och bekräfta båda säkerhetsförfrågningarna (beroende på om ska återställa behörigheterna eller inte).



Figur 181: Återaktivera medier – och återställa behörigheter

Systemet uppmanar dig att bekräfta aktiveringen.

Uppdateringsuppgifter skapas åter för de AirKey-enheter där det finns poster i blacklist för enheterna vilka gäller för detta specifika återaktiverade medium.

Uppdatera de som tilldelats uppdatering behövs till följd av återaktiveringen. Mediet kan åter aktivera de enheter vilka har info på blacklist när de uppdaterats.

Återaktiveringar gäller endast för det berörda AirKey-systemet. Har smart-telefonen avaktiverats i flera system förblir telefonen avaktiverad i övriga system.

Informera administratörer till andra relevanta system om att telefonen är återaktiverad, Om telefonen har behörighet i andra system.

En KeyCredit dras av för återaktivering av behörigheter. Tillgänglig kredit behövs för att genomföra denna åtgärd.

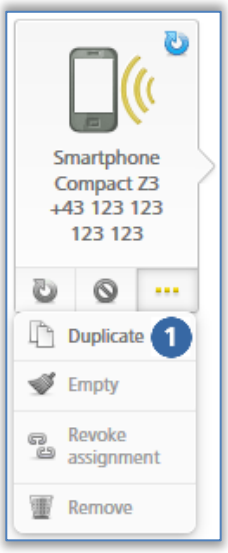
5.6.20 Duplicera medier

Funktionen "Duplicera medium" används för att duplicera medier i syfte att överföra befintliga behörigheter från ett medium till ett annat. I så fall måste källmediet som ska dupliceras vara behörigt och målmediet måste redan ha skapats och tilldelats till en person.

> På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.

> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

> Välj det medium som ska dupliceras i listan.

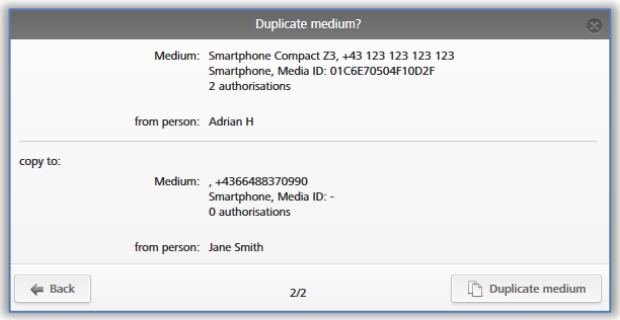


Figur 182: Duplicera medier

> Klicka på ***Mer...*** ❶ → ***Duplicera***.
Nu öppnas en lista över alla medier som är tilldelade personen – mediet som ska dupliceras finns inte med på listan.

> Välj önskat målmedium och klicka på ***Fortsätt***.

> Klicka på ***Duplicera medium*** för att slutföra *processen.*



Figur 183: Duplicera medier

Systemet bekräftar om mediet duplicerats korrekt. Du vidarebefordras till översikten av behörigheter för målmediet.

Befintliga behörigheter på målmediet skrivs över.

Klicka på ***Skapa behörigheter*** för att skapa och uppdatera målmediet och slutföra duplicering. Se kapitlet Skapa behörigheter för mer information om hur man skapar medier.

En KeyCredit dras av från kontot för denna process. Tillgänglig kredit behövs för att genomföra denna åtgärd.

Omfattar förändringen ett stort antal personer (se kapitlet Importera personuppgifter) med identiska behörigheter kan man snabbt tilldela ett stort antal medier med samma behörigheter till respektive person med funktionen "Duplicera medium".

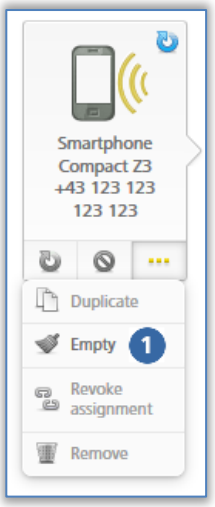
5.6.21 Tömma medier

Töm medier om man vill radera alla behörigheter på dem.

> På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.

> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

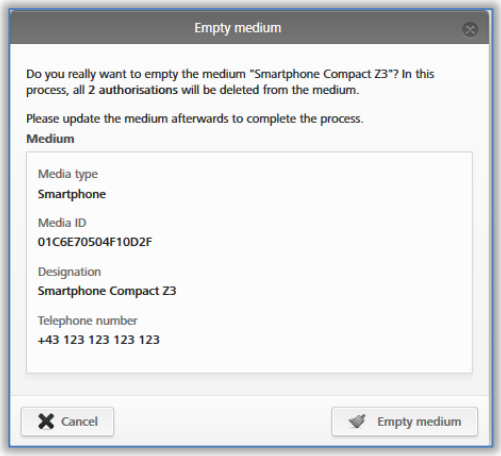
> Klicka på det medium som ska tömmas i översiktslistan.



Figur 184: Tömma medier

> Klicka på ***Mer...*** ❶ → ***Töm***.

> Klicka på ***Töm medium*** för att slutföra processen.



Figur 185: Tömma medier – säkerhetsfråga

Alla behörigheter markeras för radering. Uppdatering av mediet krävs för att alla behörigheter ska tas bort slutgiltigt.

KeyCredits dras inte från kontot vid radering av behörigheter. Uppdatering av mediet behövs för att slutföra raderingen.

Använd inte denna funktion för borttappade medier. Funktionen används endast för att radera behörigheter på ett fysiskt tillgängligt medium. Tappar man bort mediet använd funktionen Avaktivera medium.

Använd funktionen Radera behörighet för att radera enskilda behörigheter.

5.6.22 Upphäva tilldelningar

Radera behörigheter om personen inte använder mediet.

> På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.

> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

> Välj det medium från listan för vilket man ska radera tilldelningen till personen.

Alternativt

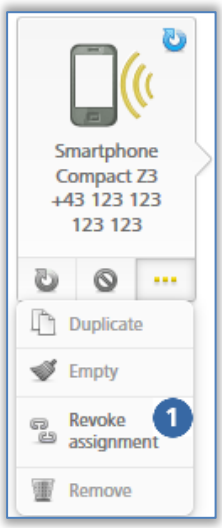
> På **startsidan *Home*** välj ***Personer***.

> Alternativt väljer du ***Medier och personer*** → ***Personer*** i huvudmenyn.

> Klicka på namnet på den person i listan för vilken man ska radera tilldelningen till mediet.

Alla medier som är tilldelade denna person visas på vänster sida under namnet.
Välj det medium som ska raderas.

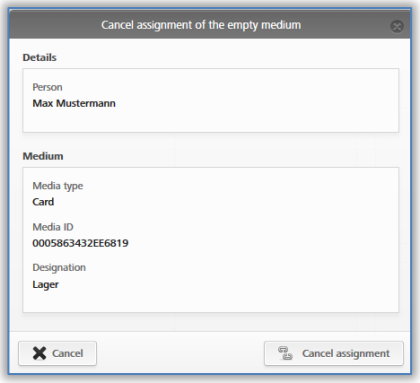
Figur 188: Tilldelade meder



Figur 186: Medier – upphäva tilldelningar

> Klicka på ***Mer...*** ❶ → ***Upphäv tilldelning*** om det inte längre finns några behörigheter på mediet.

> Klicka på ***Upphäv tilldelning*** för att bekräfta säkerhetsfrågan.



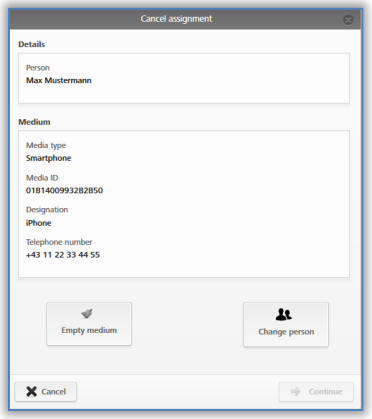
Figur 187: Upphäva tilldelningar utan behörigheter

Ett meddelande om att tilldelningen har upphävts visas på displayen. Man vidarebefordras automatiskt till personuppgifterna för personen det gäller.

Avaktivera "underhållsbehörighet" på smarttelefonen för att radera tilldelningar.

Radera eventuella behörigheter på mediet först. Man kan använda funktionen ***Töm medium*** inom ramen för funktionen ***Upphäv tilldelning*** för att ta bort alla behörigheter på mediet.

Finns det behörigheter på mediet och man utför åtgärden ***Upphäv tilldelning*** visar ***systemet en alternativt*** meddelande. I detta meddelande kan man välja mellan att tömma mediet eller överföra mediet till en annan person.



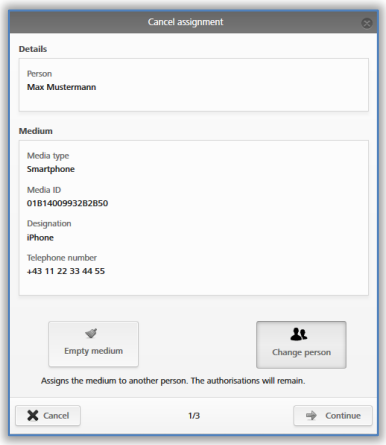
Figur 189: Upphäva tilldelningar med behörigheter

Används funktionen ***Töm medium*** i funktionen ***Upphäv tilldelning*** måste man utföra funktionen ***Upphäv tilldelning*** en gång till efter att ha uppdaterat mediet för att slutföra raderingen av behörigheter korrekt.

Gör på följande sätt för att överföra mediet inklusive alla dess behörigheter till en annan person:

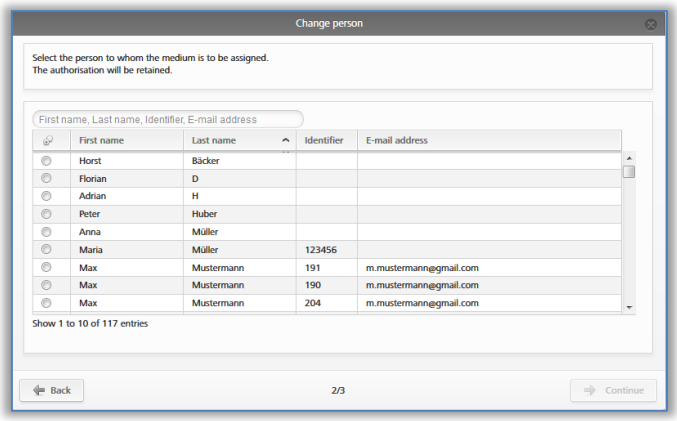
> Klicka på ***Mer...*** → Upphäv tilldelning.

> Välj ***Ändra person*** och bekräfta med ***Fortsätt***.



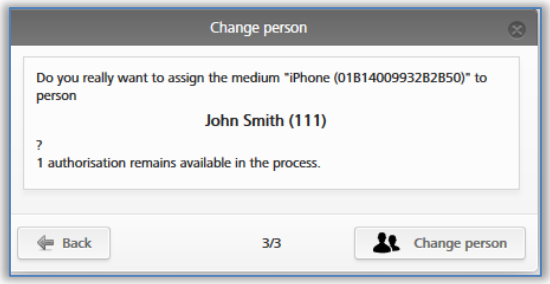
Figur 190: Upphäva tilldelningar – ändra personer

Systemet visar en lista över alla skapade personer. Välj önskad person och klicka på ***Fortsätt*** för att bekräfta.



Figur 191: Ändra personer

Klicka på ***Växla personer*** för att bekräfta säkerhetsfrågan och slutföra processen.



Figur 192: Ändra personer

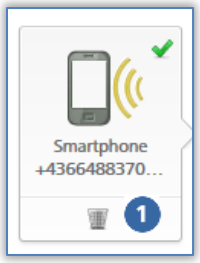
När man har slutfört processen korrekt visas ett meddelande att uppdateringen genomförts.

5.6.23 Ta bort medier

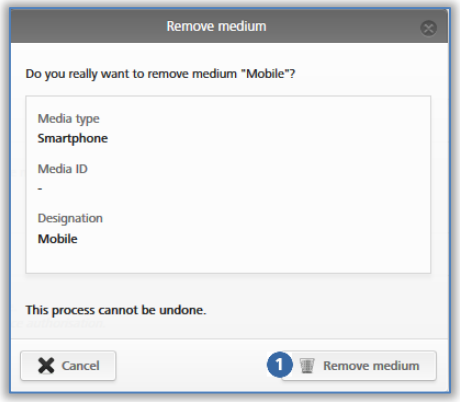
Ta bort medier för att de inte ska visas eller användas i aktuelt AirKey-system.

Medier kan endast tas bort om deras tilldelning till personer har upphävts. Mer information finns i avsnittet Upphäva tilldelningar.

- > På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.
- > Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
- > Klicka på det medium som ska raderas i listan.
- > Klicka på papperskorgssymbolen under mediasymbolen ❶.
- > Klicka på ***Ta bort medium*** ❶ för att bekräfta säkerhetsfrågan.



Figur 193: Radera medier – papperskorg



Figur 194: Ta bort medier

När mediet har tagits bort helt visas det inte längre i listan över medier. Man vidarebefordras till medialistan.

Mediet återställs till fabriksläget när det har tagits bort från systemet och kan läggas till i ett annat AirKey-system.

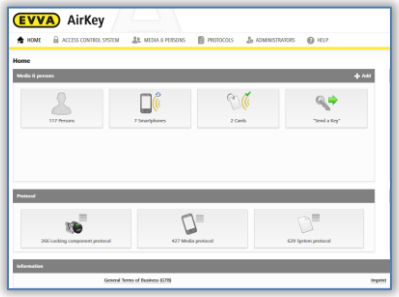
Option

Vill man ta bort medier utan behörigheter och tilldelningar till personer med hjälp av kodningsstationen, placeras mediet på kodningsstationen och man klickar därefter på länken ***Ta bort medium*** i statusmeddelandet.

5.7 Händelseloggar

Huvudmenyn Logg innehåller en översikt av alla händelser i ditt AirKey-system. Beroende på de allmänna inställningarna för händelseloggar, uppdateringsuppgifter eller personliga händelseloggar registrerar systemet nekande tillträden (om respektive medium inte hade tilldelats en giltig behörighet för motsvarande Airkey-enheten vid tiden för identifiering, men det hade tilldelats andra behörigheter inom systemet) samt utförda tillträdeshändelser och tekniska händelser. Händelser som överförs till AirKey-onlineadministration sparas där för en obegränsad tid.

Vi rekommenderar uppdatering av loggarna med jämna mellanrum för att ha tillgång till de senaste loggade händelserna. Detta gör du med funktionen ***Ladda vy på nytt***.



Figur 195: Logg

Observera att AirKey-systemet kan omfattas av krav på rapportering / godkännande beroende på gällande lagstiftning, i synnerhet i fråga om dataskydd. EVVA Sicherheitstechnologie GmbH ansvarar inte och garanterar därför inte att systemet arbetar i enlighet med gällande bestämmelser.

5.7.1 Enhetslogg

> På startsidan ***Home*** välj ***Enhetslogg***.

> Alternativt välj ***Loggar*** → ***Enheter & områden***.

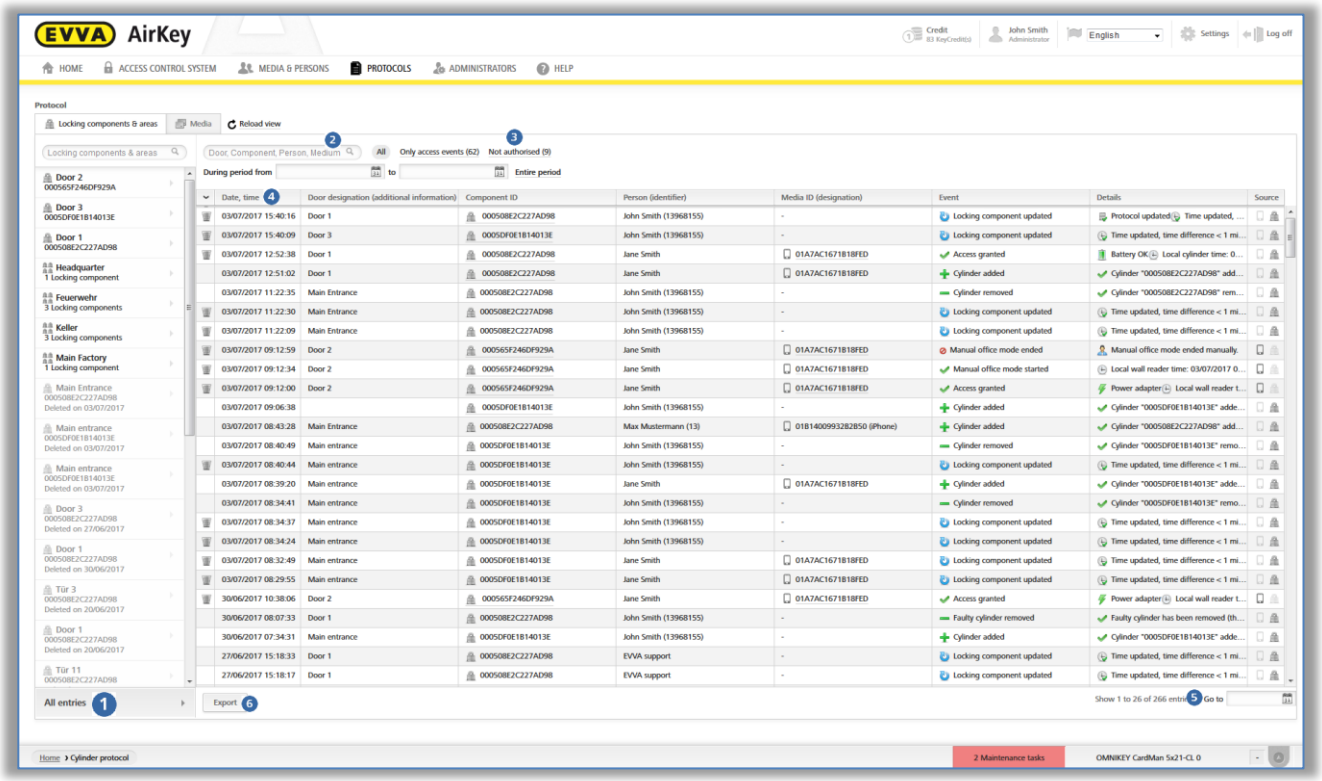
I listan visas alla poster för enheter och områden.

> Vid behov välj de enskilda enheter och områden i den vänstra kolumnen för vilka händelseloggar ska visas. Klicka på ***Alla poster*** ❶ längst ned till vänster för att se alla enheter för ett specifikt område igen.

> Ange minst tre tecken i sökfältet ❷ för en specifik sökning.

> Klicka på motsvarande länk för att även aktivera filtret ❸ (t.ex. "ej behörig"). I detta fall visas endast poster där tillträdet nekats.

> Som standard sorteras listan efter datum och tid ❹ (de senaste posterna längst upp). Klicka på rubriken "Datum, tid" för att ändra ordningen för sorteringen. Det går inte att sortera denna tabell efter andra rubriker.



Figur 196: Händelselogg för enheter och områden

> Om listan är stor kan man använda fältet ***Gå till*** ❺ längst ned till höger för att snabb bläddra till ett visst datum.

> Använd knappen ***Exportera*** ❻ längst ned till höger för att exportera hela händelseloggen till en CSV-fil. Man kan sedan bearbeta CSV- filen utanför AirKey-onlineadministration.

All nödvändig information, som datum och tid (extrainformation), enhets-ID, användare (användar-ID), medie-ID (beteckning) och motsvarande händelse visas i händelseloggen. I kolumnen "Detaljer" visas mer detaljerad information om den specifika händelsen.

Kolumnen "Källa" visar om posten i händelseloggen genererades av ett medium eller en AirKey-enhet.

Vi rekommenderar att man uppdaterar systemet med jämna mellanrum för att se de senaste posterna i händelseloggarna. Detta gör man med funktionen ***Ladda vy på nytt***.

Använd inställningarna för händelseloggen för att begränsa loggningen av personuppgifter i enlighet med gällande dataskyddsbestämmelser. Man specificerar typen av personuppgifter som ska sparas i händelseloggar för de enheter som lägges till i AirKey-systemet under Inställningar för standardvärden i händelselogg eller i enhetens specifikationer.

Uppdatera enheterna regelbundet för att säkerställa att alla poster i händelseloggen är uppdaterade i AirKey-onlineadministrationen. Hur ofta man bör uppdatera beror på hur ofta enheterna aktiveras. Observera Värden och begränsningar för AirKey-enheter.

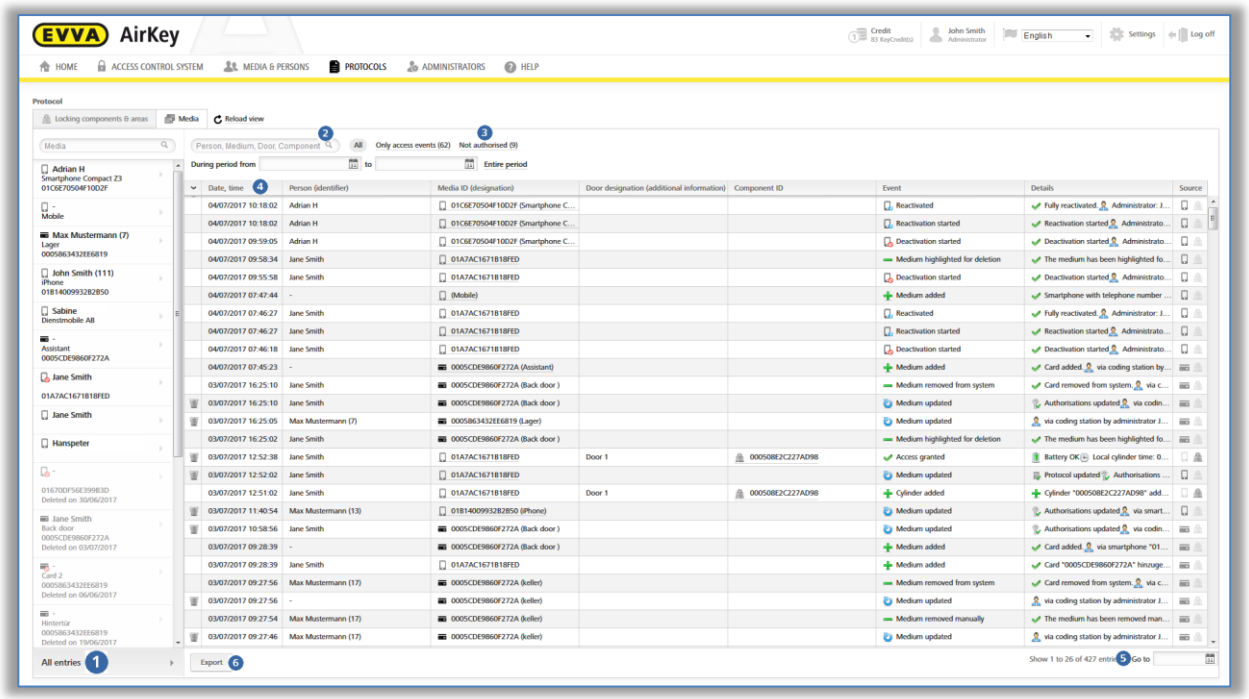
Nekat tillträde sparas endast i loggen om mediet är behörigt för enheten men behörigheten inte är giltig, (t.ex. om behörigheten gått ut eller endast är giltig inom en viss period).

Den batteristatus som visas i kolumnen "Detaljer" överensstämmer inte alltid med enhetens (cylinderns) faktiska batteristatus.

Är loggen för enheten begränsade till en viss period, fortsätter registreringen efter satt period. I detta fall anonymiseras personreferensen.

5.7.2 Medielogg

> På startsidan ***Home*** välj ***Medielogg***.
> Alternativt välj ***Loggar*** → ***Medier***.



Figur 197: Medielogg

Systemet visar en översikt av alla poster för medier.

- Vid behov välj de enskilda medier i den vänstra kolumnen för vilka man vill se händelseloggar. Klicka på ***Alla poster*** ❶ längst ned till vänster för att se alla AirKey-enheter för ett specifikt område igen.
- Ange minst tre tecken i sökfältet ❷ för en specifik sökning.
- Ställ in filter, t.ex. "ej behöriga" ❸. I detta fall visas poster där tillträdet nekats.
- Sortera listan efter datum och tid ❹.
- Om listan är stor, använd fältet ***Gå till*** ❺ längst ned till höger för att snabb bläddra till en viss dag.
- Använd knappen "Export" ❻ längst ned till höger för att exportera hela händelseloggen för medier till en CSV-fil. Man kan sedan bearbeta denna CVS-fil utanför AirKey-onlineadministrationen.

All nödvändig information, som datum och tid (användar-ID), medie-ID (beteckning), dörrbeteckning (extrainformation), enhets-ID och motsvarande händelse visas i händelseloggen. I kolumnen "Detaljer" visas mer extrainformation om den specifika händelsen.

Kolumnen "Källa" visar om posten i händelseloggen genererades av ett medium eller en enhet.

Använd inställningarna för händelseloggen för att begränsa loggningen av personuppgifter i enlighet med gällande dataskyddsbestämmelser. Specificera typen av personuppgifter som ska sparas i händelseloggar för de enheter som läggs till i systemet under Inställningar eller i enhetens detaljer för varje AirKey-enhet.

Man kan även se poster i händelseloggen för specifika medier i det speciella mediaavsnittet. Detta gör man genom att välja önskat medium i medialistan och gå till fliken ***Logg***.

Händelser där tillträde har nekat sparas endast om mediet är behörigt för AirKey-enheten men behörigheten var inte giltig vid tiden för tillträdeshändelsen (t.ex. om behörigheten gått ut eller endast är giltig inom en viss period).

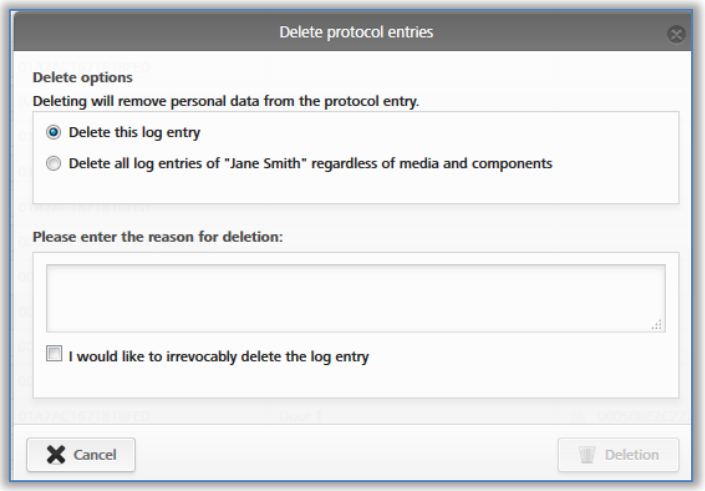
Den batteristatus som visas i kolumnen "Detaljer" motsvarar inte alltid enhetens (cylinderns) faktiska batteristatus.

Om händelseloggar för enheter är begränsade till en viss period, fortsätter tillträdeshändelser att registreras efter denna period. I detta fall anonymiseras personreferensen.

I händelseloggar för enheter och medier kan poster med personreferens anonymiseras i efterhand av dataskyddsskäl. Alla poster i händelseloggen som är kritiska ur dataskyddssynpunkt, t.ex. tillträdeshändelser, visas i den första kolumnen med en papperskorg.

Gör på följande sätt för att anonymisera poster med personreferens i händelseloggen:

- Leta efter den post som ska anonymiseras och klicka på papperskorgssymbolen i den första kolumnen.
- Man får frågan om man vill ta bort endast denna post i händelseloggen eller alla poster för denna person. Välj önskat alternativ.
- Ange orsaken till att du raderar posten.
- Kryssa för ***Jag vill ta bort posten/postserna i loggen permanent***.
- Klicka på ***Radera*** för att slutföra processen.



Figur 198: Radera poster i händelseloggen

Poster i händelseloggen tas inte bort helt, endast personreferensen tas bort. Detta gör att posterna är anonyma. Denna process kan inte ångras. Använd denna funktion med eftertanke.

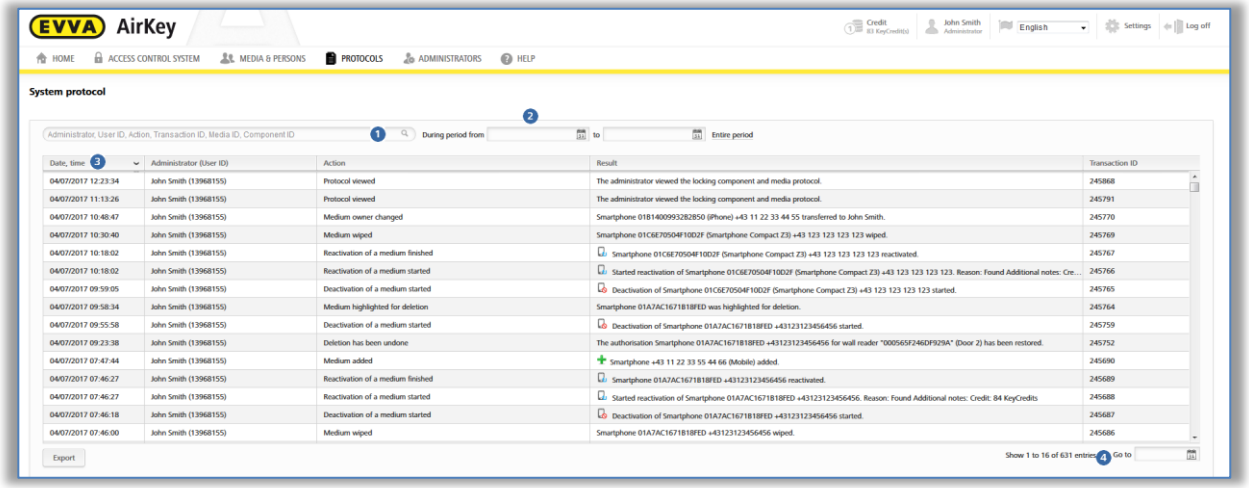
Vid raddering av poster i händelseloggen visas det i händelseloggen för systemet.

5.7.3 Systemlogg

- På startsidan ***Home*** välj ***Systemlogg***.
- Alternativt välj ***Loggar*** → ***System***.

En översikt över alla åtgärder som genomförts av administratörer visas.

- I sökfältet ❶ kan man leta efter administratörer, användar-ID, genomförda åtgärder, transaktions-ID:n, medie-ID:n eller enhets-ID:n. Ange en specifik period ❷ och fastställ vilken kolumn som ska sorteras ❸.
- Ange ett datum i fältet ***Gå till*** ❹ för att bläddra direkt till ett visst datum i systemloggen. Finns det inga poster för valt datum visas Fortsätt post.
- Använd knappen ***Exportera*** längst ned till höger för att exportera hela systemloggen till en CSV-fil. Man kan sedan bearbeta denna CVS-fil utanför AirKey-onlineadministrationen.



Figur 199: Systemlogg

Det går inte att radera poster från systemloggen.

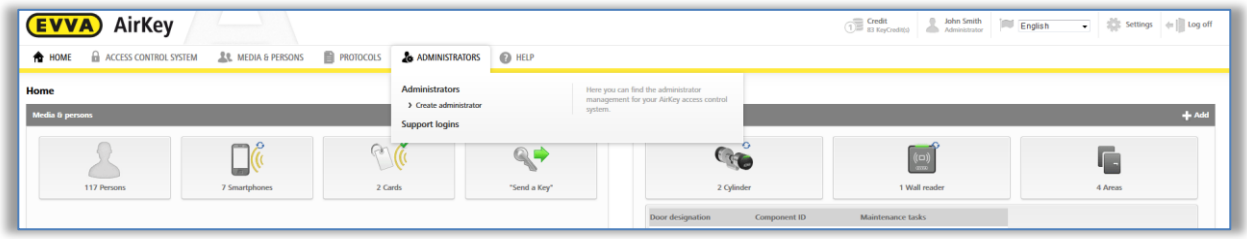
5.8 Supportfrigivningar

Genom att skapa supportfrigivningar kan man utfärda tillfälliga administratörer som behöver support för AirKey. Användare med supportfrigivningar kan se alla uppgifter i AirKey-systemet.

Personer med supportfrigivningar beviljas administratörsbehörigheter under giltighetsperioden.

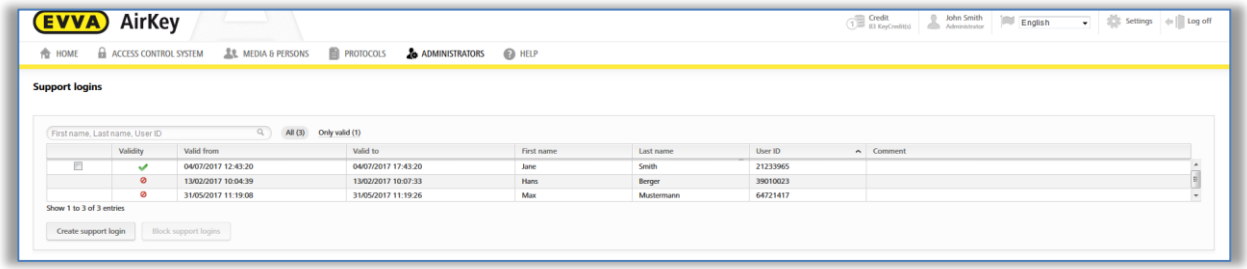
5.8.1 Skapa supportfrigivning

> I huvudmenyn välj ***Administratörer*** → ***Supportfrigivningar***.



Figur 200: Supportfrigivningar

Eventuella supportfrigivningar ar som redan har skapats visas i en lista.



Figur 201: Lista med supportfrigivningar

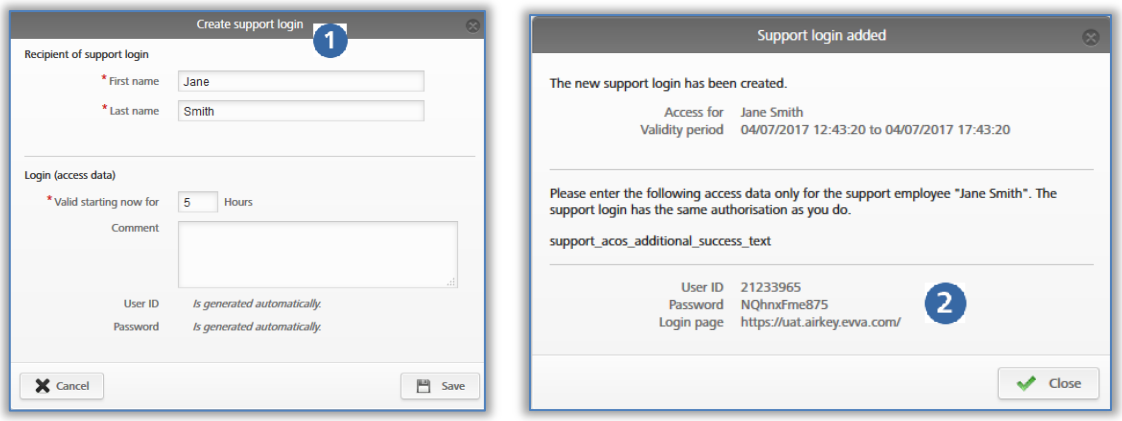
> Klicka på ***Skapa supportfrigivning***.

> Fyll i formuläret ❶.
Fält som är markerade med * är obligatoriska.

Supportfrigivningar kan tilldelas för en period på mellan 1 och högst 24 timmar.

> Klicka på ***Spara***.

Systemet genererar supportfrigivningar användar-ID och lösenord ❷.



Figur 202: Skapa supportfrigivningar

När dialogfönstret stängts kan man inte längre se lösenordet.

Säkerställ att inloggningsuppgifterna skickas på ett säkert sätt.

> ***Stäng*** *dialogfönstret "Supportfrigivning har skapads" när uppgifterna skickats till önskad supportpartner.*

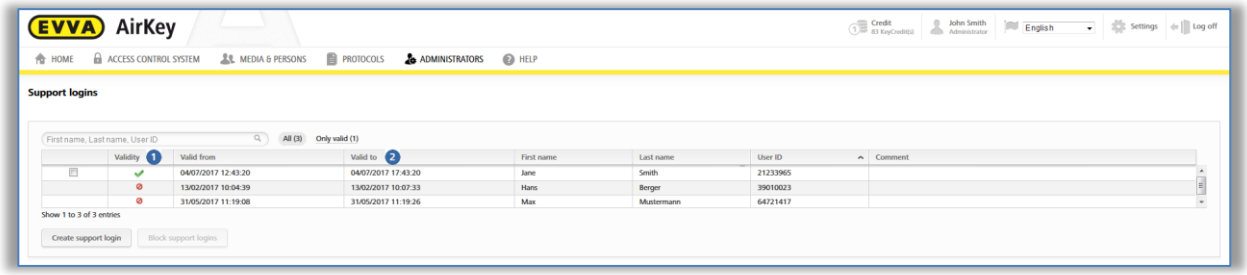
5.8.2 Spärra supportfrigivning

Supportfrigivningar går ut automatiskt efter den angivna giltighetsperioden. Man kan dock återkalla supportfrigivningar ar innan denna tid gått ut med funktionen ***Spärra supportfrigivning***.

Gör på följande sätt för att återkalla supportfrigivningar:

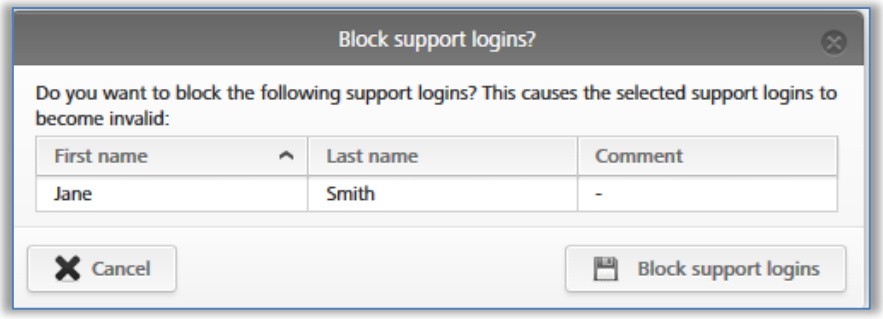
> I huvudmenyn välj ***Administratörer*** → ***Supportfrigivningar.***

I listan med supportfrigivningar visas om dessa är giltiga ❶ samt deras giltighetsperiod ❷.



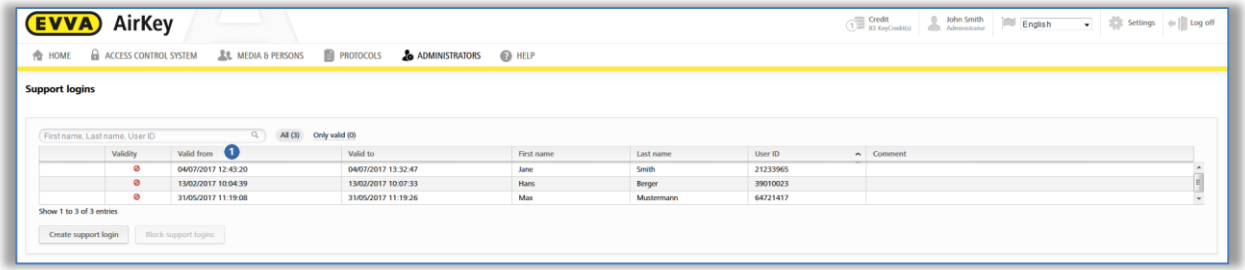
Figur 203: Översikt av supportfrigivningar

> Välj den mottagare som ska återkallas i supportfrigivningar en.
> Klicka på ***Spärra supportfrigivning.***
> Klicka på ***Spärra supportfrigivning*** för att bekräfta säkerhetsfrågan.



Figur 204: Spärra supportfrigivningar

Symbolen i kolumnen "Giltig" ❶ i listan med supportfrigivningar visar att inloggningen har spärrats.



Figur 205: Supportfrigivningar ens giltighet

Alla åtgärder som utförs av supportfrigivningar ars mottagare samt skapade eller spärrade supportfrigivningar ar registreras i händelseloggarna.

5.9 Hjälp

I området ***Hjälp*** i undermenyn hittar man ytterligare beskrivningar. Dessa finns även på EVVA AirKeys produktsida på https://www.evva.com/sv/airkey/website/. Kontakta din EVVA-partner om det behövs ytterligare hjälp.

6 AirKey-app

I detta avsnitt hittar man en översikt av funktionerna i AirKey-appen på smarttelefonen.

Följande villkor måste vara uppfyllda för att telefonen ska kunna användas med AirKey:

- Att den uppfyller AirKey-systemet krav.
- AirKey-appen har installerats korrekt.
- Det finns en aktiv internetuppkoppling.

Appens funktion kan vara försämrad om batteri optimering är aktiverad, t.ex. för att skona batteriet. Det kan leda till bland annat följande effekter: Aktiveringar tar längre tid, aktivering i bakgrunden fungerar inte tillförlitligt, etc.

6.1 Bluetooth-enheter

Klicka på detta alternativ för att visa en översiktslista med alla Bluetooth enheter inom räckvidd. På denna sida kan man till exempel Ansluta till komponener, spärra Bluetooth-enheter eller ansluta till NFC-enheter med hjälp av symbolen längst upp till höger.

Bluetooth-enheter visas korrekt efter att man uppdaterat dem med smarttelefonen, vilket innebär att visningen av enhetens status inte ändras automatiskt i appen när den öppnas.

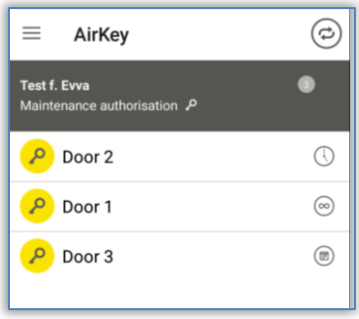
Från och med Android 6 föreskriver Google tillstånd till positionsbestämning på smarttelefonen för att Bluetooth-enheter ska kunna identifieras.

6.2 Registera smarttelefoner: Se kapitel 4.9

6.3 Behörigheter

Är telefonen registrerad i systemet och behörigheter har skapats och tilldelats med AirKey-onlineadministration, kan man när som helst se behörigheterna för motsvarande smart-telefon.

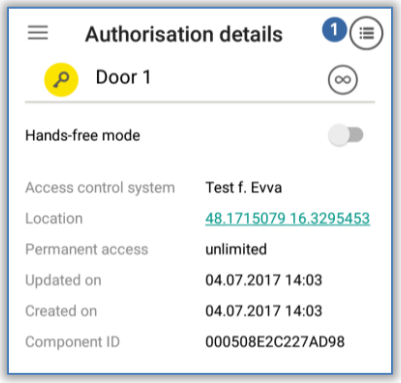
- Starta AirKey-appen.
- Välj ***Behörigheter*** i menyn.



Figur 206: AirKey-app – översikt av behörigheter

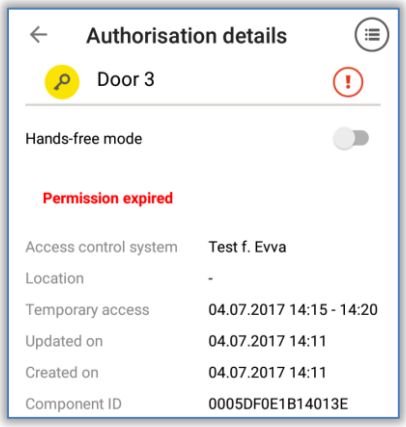
> Välj en av behörigheterna för att se detaljer för den. I detta avsnitt visas platsdata (GPS-koordinater eller adress) som länk. Klicka på länken för att vidarebefordras automatiskt till den kartleverantör som är inställd som standard på din smarttelefon.

> Man kan även aktivera Hands-free-läget individuellt för varje behörighet i behörighetsdetaljerna. Förutsättningen för detta är att Hands-free-läget har aktiverats i appens inställningar.



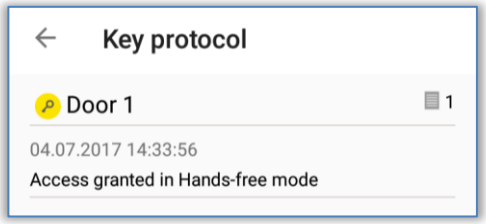
Figur 207: AirKey-app – detaljer för behörigheter.

Systemet visar om behörigheten har gått ut.



Figur 208: Behörighet har gått ut

Har smarttelefonen behörighet att se uppgifter i händelseloggen (se Tillrädeslogg i AirKey-appen) syns huvudhändelseloggen för valda behörigheter i detaljerna för behörigheter ❶.



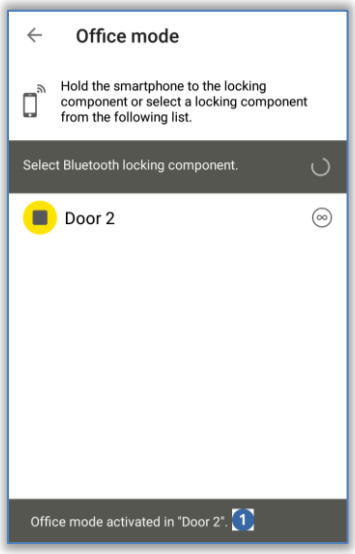
Figur 209: Händelseloggdata för behörigheter

6.4 Uppdateringsuppgifter: Se kapitel 6.12

6.5 Permanent öppning

Kontorsläget kräver att det manuella kontorsläget för AirKey-enheten har aktiverats i AirKey-onlineadministration (se Redigera AirKey-enheter) för Bluetooth- och NFC AirKey-enheter.

- Välj ***Permanent öppning*** i AirKey-appens meny.
- Välj en Bluetooth AirKey-enhet från den lista som visas eller håll smarttelefonen mot NFC AirKey-enheten.
- AirKey-enheten avger visuella och akustiska signaler.
- En bekräftelse visas ❶.



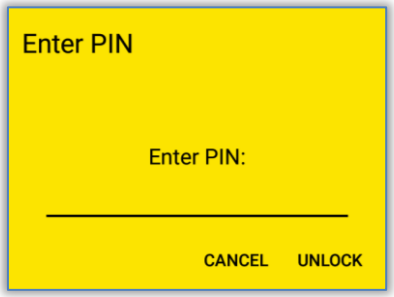
Figur 210: Bekräftelse för permanent öppning

När permanent öppning aktiveras för enheter och medier ökar enheternas strömförbrukning. Aktivera permanent öppning endast för enheter och medier som behöver funktionen.

6.6 Ange pinkod

Man kan tillfälligt spara en aktiv pinkod under en viss period i AirKey-appen med funktionen ***Ange pinkod***.

> Öppna menyn i appen och välj ***Ange pinkod***.
> Mata in rätt pinkod och välj ***Lås upp***.



Figur 211: AirKey-app – ange pinkod

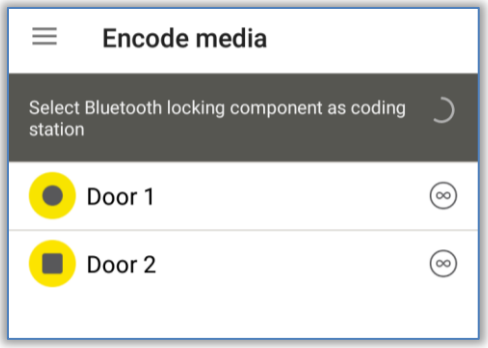
Pinkoden sparas tillfälligt tills man stänger appen, flyttar den till bakgrunden eller aktiverar skärmlåset. Funktionen aktiverar enheter utan att behöva ange pinkoden igen.

Är systemet konfigurerat med pinkod krav fortsätter funktionen vara aktiv efter första aktiveringen av en enhet. Pinkoden behöver då inte anges igen för att aktivera en enhet (samma eller en annan enhet). Funktionen är aktiv tills man stänger appen, flyttar den till bakgrunden eller aktiverar skärmlåset.

6.7 Koda medier

Denna funktion i appen används för att uppdatera medier (utom smarttelefonen) med enheter som stöder Bluetooth (cylindrar, väggläsare).

> Välj ***Koda medier*** i appens meny.
> Välj de Bluetooth enheter som ska uppdateras från listan över visade enheter.



Figur 212: Koda medier – Bluetooth-urvalslista – AirKey-enheter

> Håll det medium som ska uppdateras mot enheten.

Figur 213: Koda medier

> Följ nu instruktionerna i Lägga till kort, nyc kelbrickor och kombinycklar med en smarttelefon.

Starta processen vid cylindern med att beröra läsardelen med handen (använd inte ett medium) enheten skapar kontakt med appen och funktionen "koda medier" kan användas. Används ett medium genomförs en normal aktivering istället för att upprätta en anslutning till smarttelefonen.

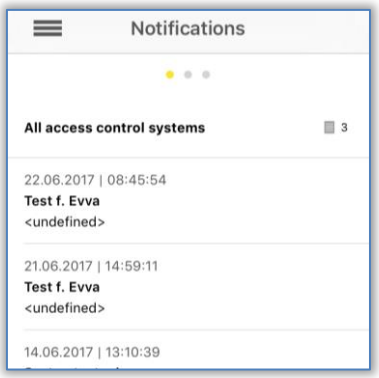
Mediauppdateringar via Bluetooth förbrukar enhetens batteri och minskar därmed batteriets brukstid. Vid uppdatering ett större antal medier rekommenderar vi att man använder en kodningsstation, väggläsare eller smarttelefon med NFC-funktion.

Hands-free-läget på smarttelefonen måste AVAKTIVERAS för att funktionen "Koda medier" ska kunna genomföras.

6.8 Behörighetslogg

Välj ***Behörighetslogg*** i appens huvudmeny, här visas en logg på behörighetsändringar som genomförts av andra administratörer i systemet.

Händelseloggen sparas alltid, oberoende av inställningarna i AirKey-onlineadministration och AirKey-appen.



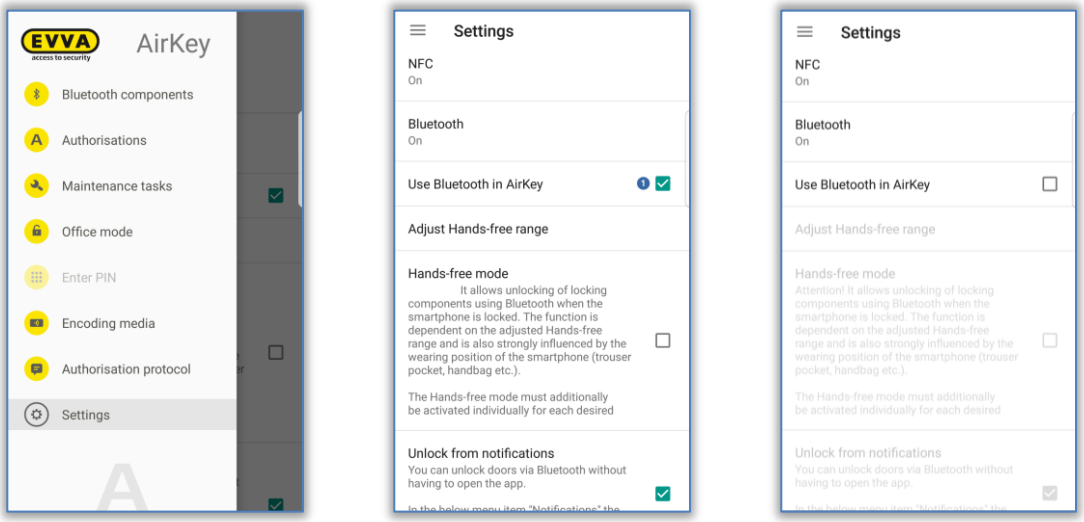
Figur 214: Meddelanden (behörighetslogg)

6.9 Inställningar i AirKey-appen

6.9.1 AirKey-appens inställningar för Android telefoner

Under menypunkten ***Inställningar*** i appen finns grundläggande information om din Android-telefon. Här visas om NFC eller Bluetooth har aktiverats eller inte. Välj ett av de båda alternativen för att öppna inställningarna. I Fortsätt steg anger man om man vill aktivera Bluetooth för AirKey. Aktivera alternativet "Använd Bluetooth" ❶.

Nu kan man konfigurera inställningarna ("Anpassa räckvidd för Hands-free", "Hands-free-läge" och "Aktivering meddelanden"). I AirKey-appen visas startsidan Home "Bluetooth-enheter".



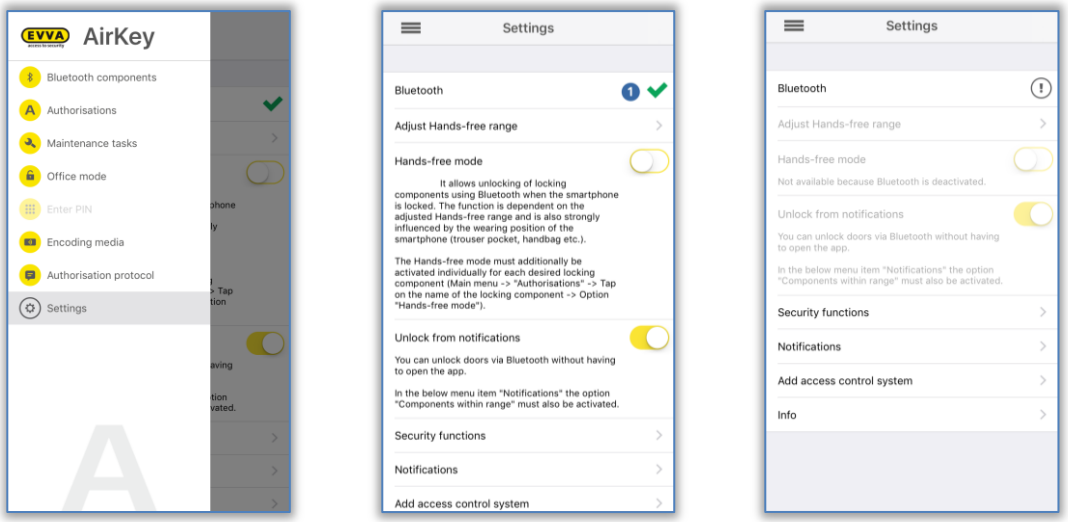
Figur 215: Android-telefon med Bluetooth – huvudmeny / Alternativet "Använd Bluetooth" aktivt / Bluetooth avaktiverad

Vid avaktivering av "Använd Bluetooth" blir de tre ovannämnda, tillhörande funktionerna automatiskt stängda samt alla andra Bluetooth-baserade funktioner från huvudmenyn ("Bluetooth-enheter", "Kontorsläge" och "Koda medier"). Med denna konfiguration kommunicerar telefonen endast med enheterna via NFC.

Är Android-telefonen äldre men har NFC och inte Bluetooth är alla Bluetooth-baserade funktioner och inställningar avaktiverade.

6.9.2 Inställningar för AirKey-app på iPhones

Under menypunkten ***Inställningar*** i appen finns grundläggande information om iPhone. Denna del förklarar om Bluetooth är aktiverad eller inte. Här kan man konfigurera tillhörande inställningar ("Anpassa räckvidd för Hands-free", "Hands-free-läge" och "Aktivering meddelanden").



Figur 216: iPhone (endast Bluetooth) – huvudmeny / inställningar utan NFC-baserade funktioner / alternativet Bluetooth avaktiverad

Funktionen "Bluetooth" i AirKey-inställningarna visar om Bluetooth har aktiverats eller inte. Aktivera "Bluetooth" för att öppna Bluetooth-inställningarna i din iPhone.

Är Bluetooth avaktiverat i iPhone kan man INTE LÄNGRE aktivera några AirKey-enheter!

Stängs funktionen Bluetooth i iPhone avaktiveras alla funktioner i appens huvudmenyn som t.ex. ("Bluetooth-enheter", "Kontorsläge" och "Avkoda medier").

6.9.3 Anpassa räckvidd för Hands-free

När du väljer funktionen "Ställa in Hands-free-räckvidd" kommer du till en undermeny. Här kan du välja för vilka enheter som räckvidden ska ställas in eller om räckvidden ska återställas (för alla låsenheter).

Räckvidd för Cylindrar

- I AirKey-appen visas aktiva Bluetooth-cylindrar i närheten. Dessa ska först ha aktiverats genom fysisk beröring.
- Välj den cylinder för vilken avståndet skall sättas, till den automatiska aktiveringen med Bluetooth.
- Tryck på ***Spara***.

Räckvidd för Väggläsare

- I AirKey-appen visas aktiva Bluetooth-cylindrar i närheten. Dessa ska först ha aktiverats genom fysisk beröring.
- Välj den väggläsare som avståndet skall sättas, för den automatiska aktiveringen med Bluetooth.
- Tryck på ***Spara***.

Signalstyrkan visas på displayen. Tänk på att dessa parametrar kan påverkas av omgivande faktorer, såsom radiotrafik och liknande.

Standardräckvidden är ca 50-70 cm beroende på tillverkare och enhet. Av säkerhetsskäl rekommenderar EVVA att räckvidden ställs in på ca 30 cm.

Återställ alla Bluetooth-räckvidder

Tryck på ***Återställ alla Bluetooth-räckvidder*** för att radera alla manuellt inställda räckvidder och använda standardräckvidderna igen. När räckvidderna har återställts bekräftas detta med ett meddelande.

6.9.4 Hands-free-läge

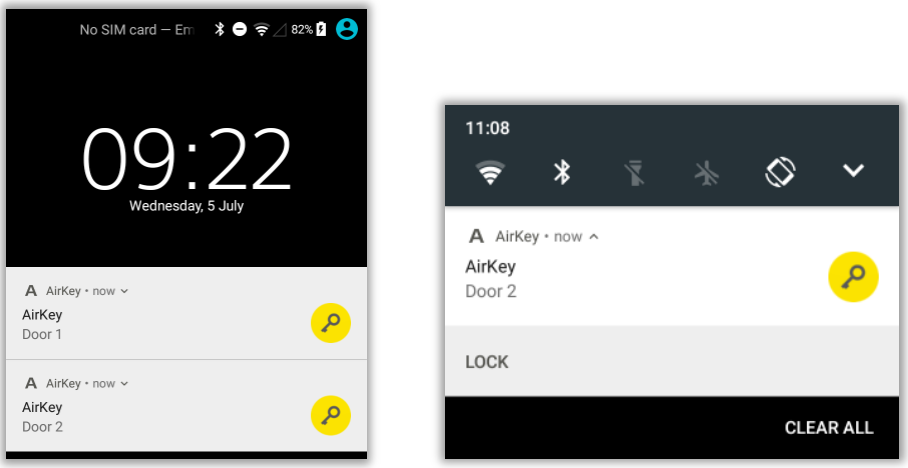
Kryssa för ***Hands-free-läget*** för att aktivera funktionen. Mer information hittar du under Hands-free i översikt.

6.9.5 Lås upp från meddelanden

Denna funktion aktiverar enheter via Bluetooth utan att öppna AirKey-appen.
Kryssa för ***Lås upp från meddelanden*** för att aktivera funktionen.

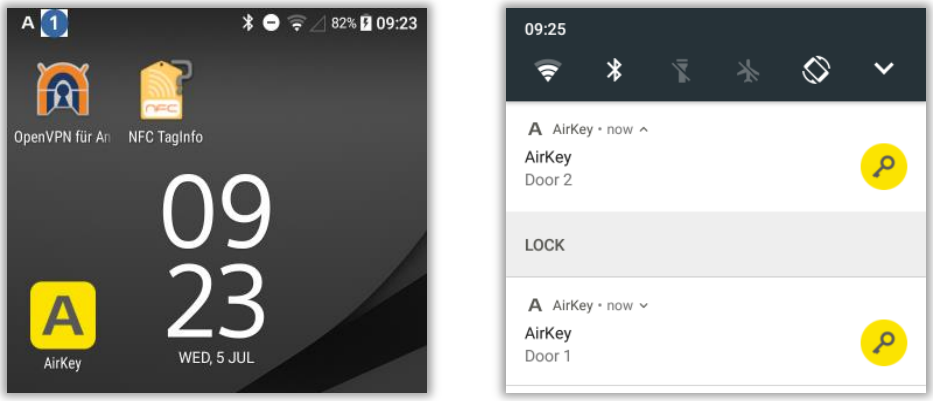
På Android-smarttelefoner startas en tjänst när denna funktion aktiveras. Den här tjänsten söker permanent efter Bluetooth-låskomponenter inom räckvidd även om AirKey-appen är stängd och leder till ökad batteriförbrukning på smarttelefonen. Tjänsten avslutas så fort funktionen avaktiveras. När man trycker på meddelandet från tjänsten kommer man direkt till inställningarna för AirKey-appen.

När din smarttelefon är inom räckvidd för en AirKey-enhet, för vilken du har behörighet, visas ett meddelande på skärmen i smarttelefonen. Via detta meddelande kan du aktivera enheten.



Figur 217: Aktivering meddelanden – skärm

Meddelanden på telefonens display indikeras med ett **A** ❶ längst upp till vänster. Svep ned från ovankanten av displayen för att visa meddelanden gällande de AirKey-enheter som kan aktiveras.



Figur 218: Aktivering meddelanden

Beroende på smarttelefonens modell ska du antingen trycka på meddelandet, öppna det, svepa eller hålla det intryckt och därefter trycka på ***Lås upp***.

Beroende på inställningen ***Tillträde från låsskärmen*** i AirKey-online-administrationen kan aktivering ske direkt från låst skärm eller så måste skärmlåset vara upplåst. Mer information finns under Allmänt.

Lås upp från meddelanden kan endast användas när meddelandena för "Komponenter inom räckvidd" har aktiverats i AirKey-appens inställningar. Konfigurationen för meddelandena beskrivs i kapitel Meddelanden.

6.9.6 Säkerhetsfunktioner

Menyn ***Säkerhetsfunktioner*** har tre säkerhetsnivåer:

AirKey-kryptering ❶
Denna funktion berör en extra pinkod. Pinkoden består av mellan 4 och 12 siffror och säkerställer missbruk vid förlust av telefonen.

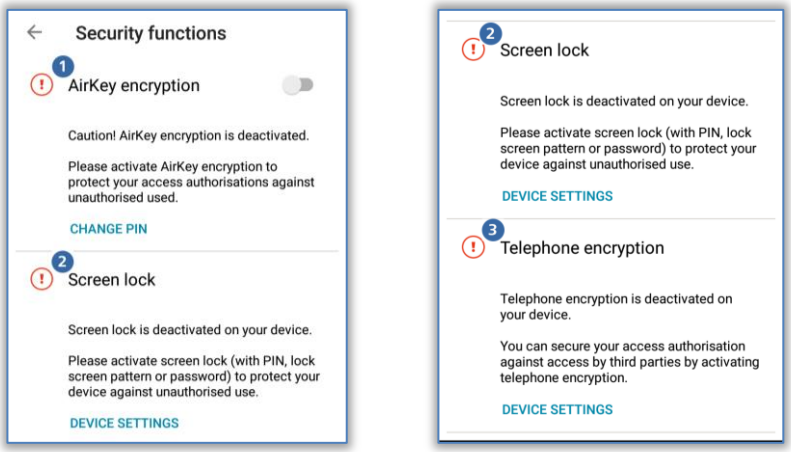
EVVA rekommenderar att man aktiverar en pinkod. Se till att pinkoden är så lång som möjligt och avslöja den inte för andra.

Bilskärmlås ❷
Denna säkerhetsfunktion för operativsystemet säkerställer att telefonens display inte kan låsas upp av tredje part. Välj denna funktion så kommer systemet att vidarebefordra dig direkt till Android-telefonens inställningar.

EVVA rekommenderar att man aktiverar skärmlåset och hemlighåller koden.

Telefonkrypering ❸
Denna säkerhetsfunktion för operativsystemet säkerställer att smarttelefonens uppgifter inte kan avläsas av tredje part. Välj denna funktion så kommer systemet att vidarebefordra dig direkt till Android-telefonens inställningar.

EVVA rekommenderar att man aktiverar telefonkrypteringen. Läs mer om detta i telefonens användarhandbok.

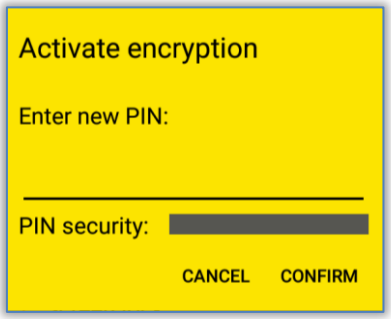


Figur 219: AirKey-app – säkerhetsfunktioner

6.9.6.1 *Aktivera pinkod*

Genomför följande steg för att aktivera pinkoden:

- Öppna menyn i AirKey-appen och välj ***Inställningar*** → ***Säkerhetsfunktioner***.
- Aktivera alternativet "AirKey-kryptering".
- Ange en pinkod, mata in den igen och välj ***Bekräfta***.



Figur 220: AirKey-app – aktivera pinkod

- Ange pinkoden igen och välj ***Bekräfta*** för att slutföra processen.

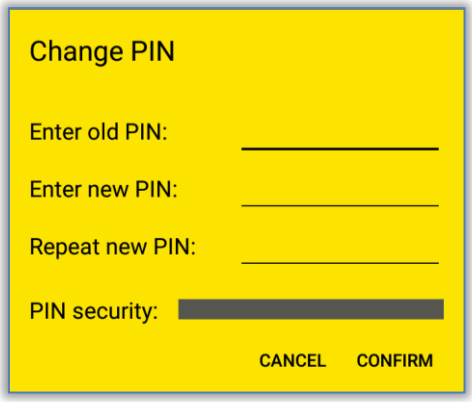
EVVA rekommenderar att man fastställer en pinkod. Se till att pinkoden är så lång som möjligt och avslöja den inte för andra. Lösenordets styrka indikeras med olika färger i ett fält när du matar in pinkoden (röd / orange / grön).

Pinkoden krävs endast när man låser upp AirKey-enheter. Appen visar ingen bekräftelse på att pinkoden har matats in korrekt. Pinkod kan definieras och sparas på förhand (se Ange pinkod).

6.9.6.2 *Ändra pinkod*

Gör på följande sätt för att ändra eller definiera en pinkod i efterhand:

- Öppna menyn i AirKey-appen och välj ***Inställningar*** → ***Säkerhetsfunktioner***.
- Välj ***Ändra pinkod.***
- Ange den gamla pinkoden, mata in den igen och välj ***Bekräfta***.



Figur 221: AirKey-app – ändra pinkod

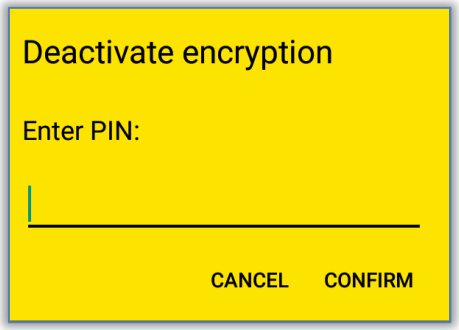
Se till att pinkoden är så lång som möjligt och avslöja den inte för andra. Lösenordets styrka indikeras med olika färger i ett fält när du matar in pinkoden (röd / orange / grön).

6.9.6.3 Avaktivera pinkod

Pinkod kan avaktiveras på två olika sätt. Kan man pinkoden kan den avaktiveras direkt i smarttelefonens säkerhetsfunktioner. Kan man inte pinkoden kan administratörer återställa den i AirKey-onlineadministration.

Gör på följande sätt om man kan pinkoden:

- Öppna menyn i appen och välj ***Inställningar*** → ***Säkerhetsfunktioner***.
- Avaktivera alternativet "AirKey-kryptering".
- Mata in den aktuella pinkoden och välj ***Bekräfta***.



Figur 222: AirKey-app – avaktivera krypteringen

Gör på följande sätt i AirKey-onlineadministration för att avaktivera pinkoden om den inte är känd:

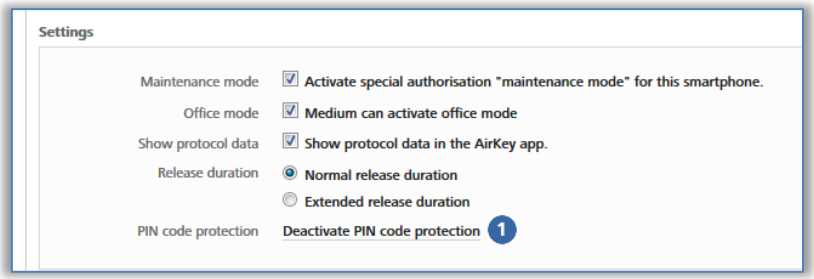
- Logga in på ditt AirKey-system som administratör.
- På startsidan ***Home*** klicka på ***Smarttelefoner***.

> Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.

> Välj den telefon från översiktslistan för vilken pinkoden ska avaktiveras.

> Välj fliken ***Detaljer*** för att redigera detaljerna.

> Klicka på ***Avaktivera pinkod*** ❶ i området "Inställningar".



Figur 223: AirKey-onlineadministration – avaktivera pinkod

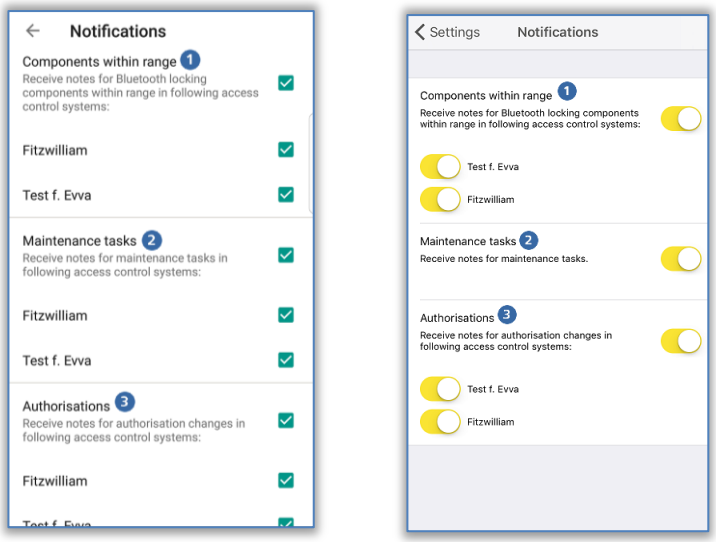
> Klicka på knappen ***Avaktivera pinkod*** för att bekräfta säkerhetsfrågan.

Figur 224: AirKey-onlineadministration – återställa pinkod

Man kan återaktivera pinkod när som helst.

6.9.7 Meddelanden

Öppna menypunkten ***Inställningar*** → ***Meddelanden*** för att aktivera pushmeddelanden (info på displayen) för enheter inom räckvidd, uppdateringar och behörigheter. Om telefonen har registrerats i flera system och har underhållsbehörighet kommer dessa AirKey-system att visas och kan då väljas.



Figur 225: AirKey-appens inställningar för pushmeddelanden på Android / iPhone

Meddelanden för *enheter inom räckvidd* 1

Aktivera denna inställning för att få motsvarande pushmeddelanden på telefonens lås- eller startskärm så fort telefonen befinner sig inom räckvidd för Bluetooth AirKey-enheter. Använd dessa meddelanden för att låsa upp respektive dörr utan att manuellt behöva öppna AirKey-appen (mer information finns i Lås upp från meddelanden).

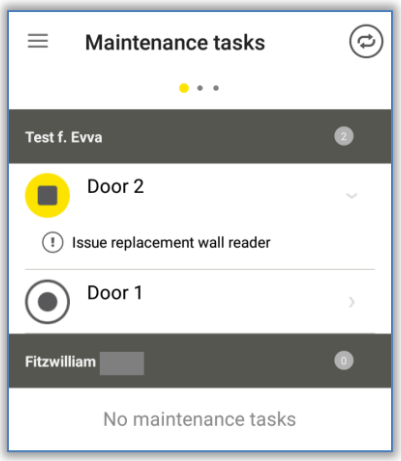
Denna inställning visas endast på telefoner med Bluetooth 4.0 (Bluetooth Low Energy).

Meddelanden om *uppdateringar* 2

Denna inställning visas endast på telefoner med underhållsbehörighet.

Om denna inställning har aktiverats visas menypunkten ***Uppdateringar*** i AirKey-appens meny. På tillhörande sida listas enheter och deras Underhållsuppgifter / uppdateringar som skapats inom AirKey-onlineadministration.

Är smarttelefonen registrerad i flera system, visas endast enheter i AirKey-system för vilka smarttelefonen har tilldelats underhållsbehörigheter. Man får ett pushmeddelande i displayen så fort en ny uppdatering har skapats i AirKey-onlineadministration.

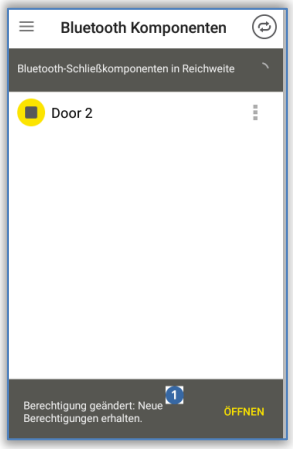


Figur 226: Uppdateringar

Meddelanden för *behörigheter* ❸

Denna inställning visas alltid.

Aktiverar denna inställning för pushmedelanden i displayen ❶ visas ca 2 sekunder längst ned på displayen i appen (om appen är öppen) så fort en ny behörighet för telefonen skapats eller ändrats i AirKey-onlineadministration.



Figur 227: Meddelanden om ändringar i behörigheter

Är appen inte öppen visas motsvarande pushmeddelande på displayen i telefonen.

Oberoende av inställningarna för meddelanden om behörigheter kommer en permanent post att läggas till i loggen (Behörighetslogg).

6.9.8 Lägg till låssystem

Ska telefonen registreras i flera AirKey-system måste en registreringskod anges i appen. Telefonen läggs till med en registreringskod som genereras i motsvarande låssystem. Använd funktionen ***Lägg till låssysem*** i appen. Mer information hittar du i kapitlet Använd smarttelefonen i flera system.

6.9.9 Information

I appen finns den aktuellt installerade AirKey-appversionen, telefonens registreringsdetaljer och medie-ID samt EVVAs allmänna licensvillkor.

> Starta AirKey-appen.

> Tryck på ***Inställningar*** ⟶ ***Info*** *i menyn.*

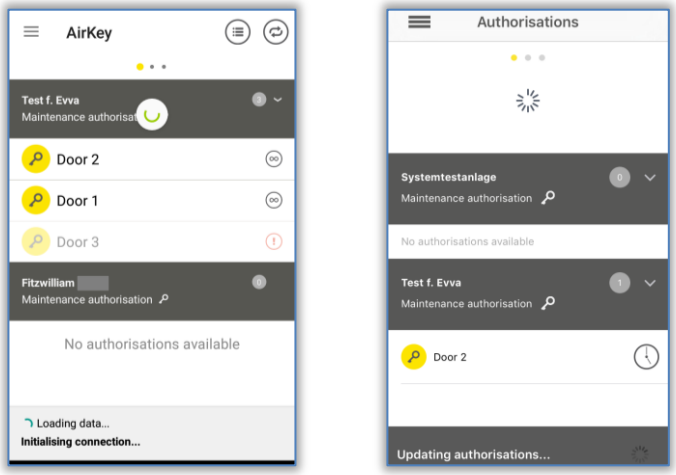
Figur 228: AirKey-app – information

6.10 Uppdatera telefoner

Man kan när som helst uppdatera telefon appen manuellt med hjälp av AirKey-onlineadministration för att hålla systemets uppgifter uppdaterade.

På en Android-telefon svep uppifrån och ned på "Behörigheter" i displayen. Uppdateringssymbolen visas (roterande cirkel).

På en iPhone svep ner "Behörigheter" på displayen till nederkanten. Uppdateringssymbolen visas (roterande balkar).



Figur 229: Uppdatera Android-telefoner och iPhones

AirKey använder pushmeddelanden för att ändra telefonens uppgifter och följaktligen uppdatera telefoner automatiskt. Vi kan inte garantera att alla pushmeddelanden kan tas emot korrekt. Därför bör man kontrollera om meddelandena har tagits emot och (om tillämpligt) uppdatera telefonen manuellt.

Smarttelefonen uppdateras automatiskt när AirKey-appen startas och var tolfte timme gör den automatiskt ett försök att uppdatera om AirKey-appen redan är igång.

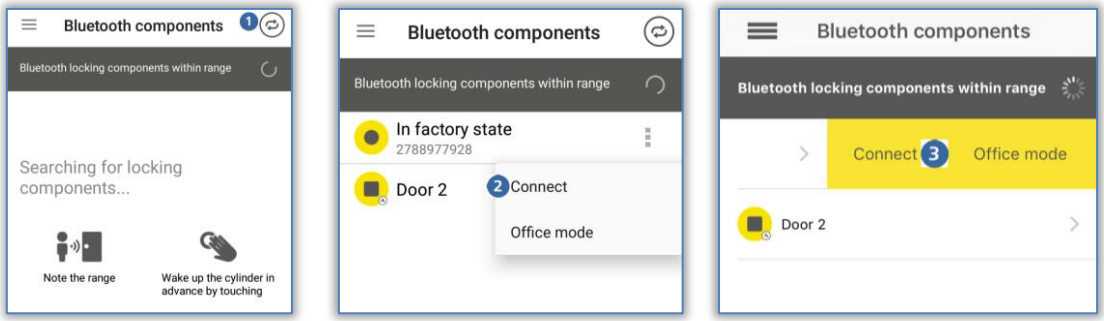
Under uppdateringen visas statusinformation i den nedre delen av AirKey-appen. Uppdateringen är klar när informationen inte längre visas.

Alternativt kan uppdateringen även utföras efter varje tillträde. Då måste dock funktionen "Uppdatering efter varje tillträde" aktiveras i det aktuella AirKey-låssystemet. Aktiveringen och detaljerna hos den här funktionen finns beskrivna i avsnittet Allmänt.

6.11 Ansluta till komponenter

Använd smarttelefonen för att uppdatera eventuella medier (utom telefoner) och enheter oberoende av deras koppling till detta låssystem.

- Upprätta en anslutning med **NFC** (för Android-telefoner):
  Tryck på symbolen ***Anslut till komponent*** ❶.
- Upprätta en anslutning med **Bluetooth** (för **Android**-telefoner): Tryck på kontextmenyn för den AirKey-enhet vilken ska upprättas en anslutning (⋮) och välj sedan ***Anslut*** ❷.
- Upprätta en anslutning med **Bluetooth** (för iPhones): Svep enhetsbeteckningen för den AirKey-enhet till vilken ska upprättas en anslutning och välj sedan ***Anslut*** ❸.



Figur 230: AirKey-app – ansluta till komponent (Android NFC / Android Bluetooth / iPhone)

- Följ anvisningarna på skärmen och håll NFC-telefonen mot mediet eller enheten; med Bluetooth-telefonen stanna inom räckvidden för AirKey-enheten.

Figur 231: Uppdatera data

Data är uppdaterat. Avlägsna inte telefonen från enheterna som ska uppdateras medan överföring pågår. När processen är slutförd visas ett meddelande om detta.

Avaktivera Hands-free-läget innan du ansluter dig till en Bluetooth-enhet (gäller vid uppdatering via funktionen "anslut" i appen). I annat fall kan det leda till avbrott i anslutningen.

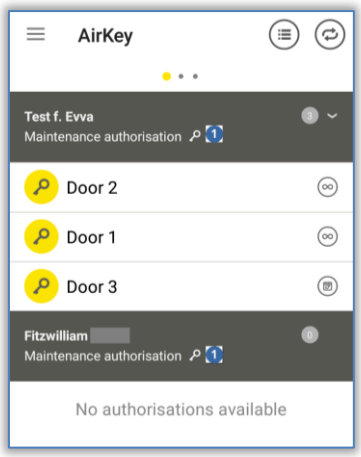
Bluetooth-enheter kan uppdateras automatiskt efter varje aktivering via Bluetooth. Mer information om funktionen "Uppdatering efter varje upplåsning" hittar du under Standardvärden (för alla nyligen tillagda låskomponenter).

Uppdatera AirKey-enheter med jämna mellanrum. Det är enda sättet som säkerställer att AirKey-systemet är säkert och uppdaterat. Se AirKey-systemets drift och underhåll för mer information om uppdatering av AirKey-enheter.

6.12 Specialbehörigheten "underhållsbehörighet"

Är specialbehörigheten "underhållsbehörighet" aktiverat för smarttelefonen i AirKey-online-administration, kan uppdateringar göras på enheter och medier med den. Underhållsbehörigheten ger behörighet att låsa upp AirKey-enheter i fabriksläge, lägga till och ta bort firmware för AirKey-enheter och medier (utom telefoner) i ditt AirKey-system eller uppdatera medier, t.ex. kort, nyckelbrickor eller kombinycklar.

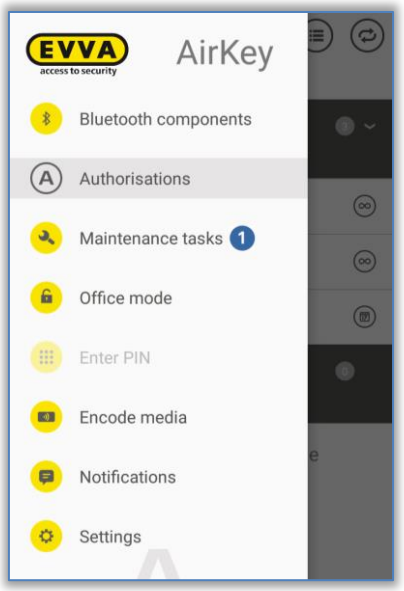
På sidan "Behörigheter" i AirKey-appen vid alternativet "Underhållsbehörighet" ❶ indikeras funktionen i det grå fältet.



Figur 232: Underhållsbehörighet

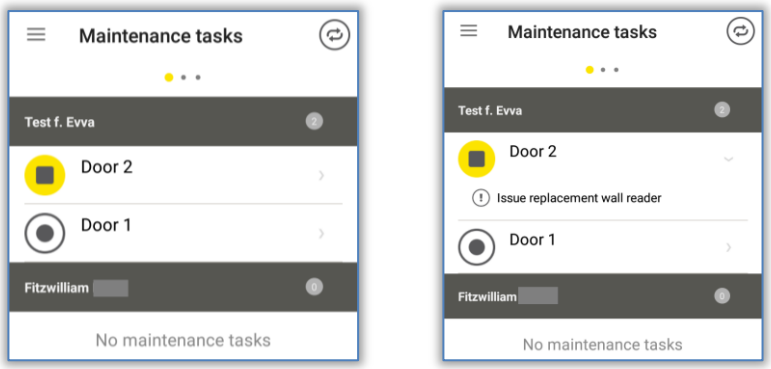
Underhållsbehörigheten aktiveras i detaljerna för motsvarande telefon i AirKey-online-administration. Mer information om redigering av medier finns i Redigera medier.

Dessutom aktiveras menypunkten ***Underhållsuppgifter*** ❶ i AirKey-appen.



Figur 233: Menypunkten "Underhållsuppgifter" i huvudmenyn

> Välj denna punkt för att visa en lista på uppdateringar för enheter inom AirKey-systemet. Tryck på enhets namnet för att öppna en lista med uppdateringar som ska genomföras.



Figur 234: Uppdateringar

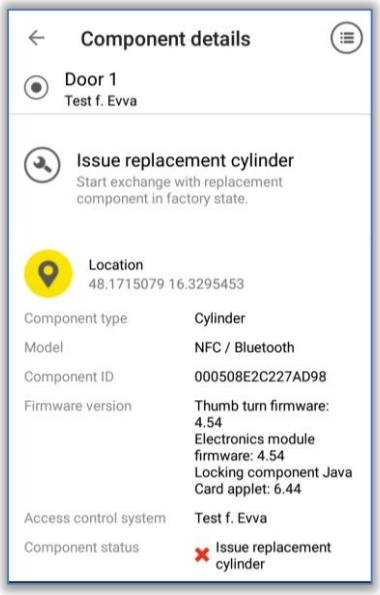
Som servicetekniker är man ansvarig för att regelbundet kontrollera uppdateringsuppgifter för att snabbt kunna uppdatera AirKey-enheter där detta är nödvändigt.

Är man inom räckvidd för en Bluetooth enhet (cylinder ◉ eller väggläsare ◉) med en smarttelefon med underhållsbehörighet, markeras symbolen för denna enhet i gult (t.ex. ◉ för cylindrar).

Tryck på den gula symbolen för att upprätta en anslutning till och uppdatera enheten. Systemet visar då enhetens detaljer. Firmware uppdateringar som måste genomföras indikeras i enhetens detaljer och kan startas härifrån.

Uppdaterar man enheter som servicetekniker visar systemet en översikt över enheternas detaljer så att man direkt kan kontrollera status och händelser i en händelselogg.

> Uppdatera enheten för att visa dess detaljer. Det är möjligt att se enhetens plats som GPS-koordinater eller adressen som sparades manuellt i AirKey-onlineadministrationen. Tryck på den gula symbolen för att vidarebefordras till den förvalda kartapp som är standard på telefonen.



Figur 235: Detaljvy för AirKey-enhet.

Uppdatera enheterna med jämna mellanrum. Det är enda sättet för att säkerhetsställa att AirKey-systemet är säkert och uppdaterat. Se AirKey-systemets drift och underhåll för mer information om uppdatering av enheter.

Uppdateringsläget gäller endast för det AirKey-system som det har aktiverats för. Uppdateringsläget kan dock aktiveras för flera AirKey-system på samma gång.

Hands-free-läget på smarttelefonen måste AVAKTIVERAS för att underhållsuppgifter eller uppdateringar på enheter ska kunna genomföras.

6.13 Lägga till AirKey-enheter

Underhållsbehörigheten måste aktiveras för systemet och enheter måste vara i fabriksläge för att kunna lägga till enheter eller medier (utom telefoner) i ett AirKey-system med telefonen.

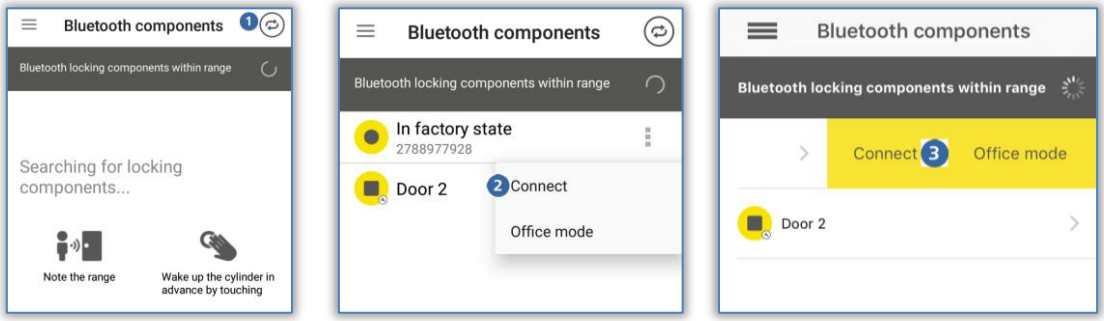
6.13.1 Lägga till medier: Se kapitel 4.12

6.13.2 Lägga till låskomponenter: Se kapitel 4.11

6.14 Ta bort låskomponenter

AirKey-enheten eller mediet (utom telefoner) måste ha tagits bort från i AirKey-online-administrationen (se Ta bort låskomponenter och Ta bort medier) och telefonen måste ha underhållsbehörighet för användas till avaktivering av enheter.

- Upprätta en anslutning med hjälp av **NFC** (för Android-telefoner): Tryck på symbolen ***Anslut till komponent*** ❶.
- Upprätta en anslutning med **Bluetooth** (för Android-telefoner): Tryck på kontext-menyn för den AirKey-enhet till vilken ska anslutas (⋮) och välj sedan ***Anslut*** ❷.
- Upprätta en anslutning med **Bluetooth** (för iPhones): Svep enhetsbeteckningen för den AirKey-enhet som ska anslutas och välj sedan ***Anslut*** ❸.

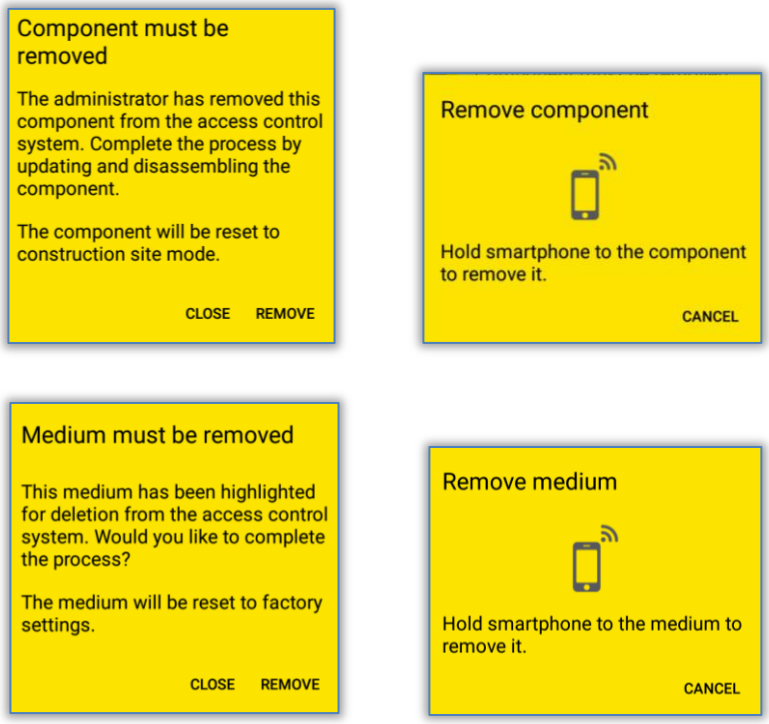


Figur 236: AirKey-app – ansluta till komponent (Android NFC / Android Bluetooth / iPhone)

- Följ anvisningarna på skärmen och håll NFC-telefonen mot mediet eller enheten; med Bluetooth-telefonen stanna inom räckvidden för AirKey-enheten.

Figur 237: AirKey-app – anslutning till komponenten

Håll NFC-telefonen mot den enhet/medium vilket är radderat i AirKey-onlineadministration, stanna med Bluetooth-telefonen inom räckvidden för den enhet som ska bort eller hållmediet mot den enhet som skall överföra radderingen till mediet. Följ anvisningarna.

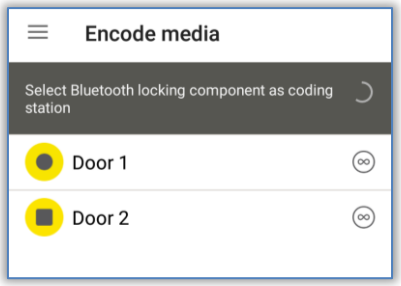


Figur 238: Ta bort AirKey-enheter

När uppdateringen är klar återgår AirKey-enheterna och medierna till fabriksläge.

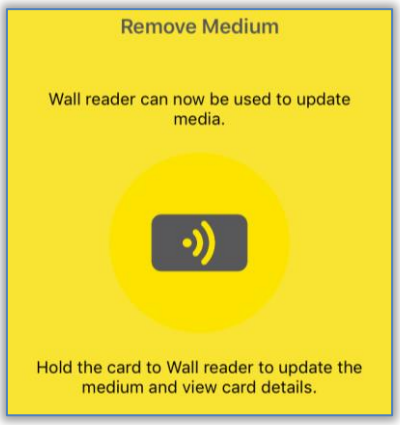
Ska man ta bort medier från AirKey-systemet med en iPhone sker detta på samma sätt som i beskrivningen i ***Koda medier***.

> Välj de Bluetooth AirKey-enheter som ska uppdateras från listan över visade enheter.



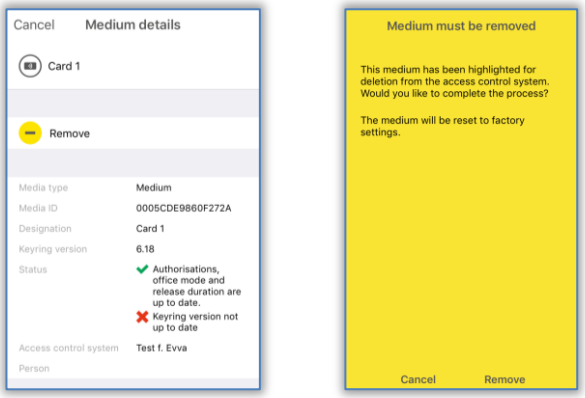
Figur 239: Koda medier – Bluetooth-urvalslista – AirKey-enheter

> Håll det medium som ska uppdateras mot en enhet.
> Ett meddelande om att enheten är redo visas.



Figur 240: Ta bort medier med hjälp av iPhones

> Håll mediet mot en enhet och tryck på ***Ta bort***.



Figur 241: Ta bort medier

> Systemet visar en bekräftelse om att mediet har tagits bort korrekt från systemet.

Avlägsna inte telefonen från AirKey-enheten eller mediet under denna process.

Tillvägagångssättet för att ta bort AirKey-enheter och medier (utom telefoner) är identiskt.

Det går inte att ta bort NFC-enheter från AirKey-systemet med hjälp av iPhones. I detta fall behöver man en kodningsstation eller en Android-telefon med NFC-funktion.

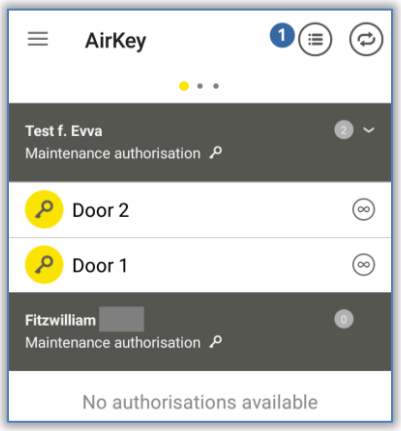
6.15 Tillrädeslogg i AirKey-appen

För smarttelefoner kan behörigheterna för visning av loggdata aktiveras via AirKey-onlineadminstrationen. Visningen av loggdata är oberoende av underhållsbehörigheten och kan aktiveras individuellt för varje användare.

Aktivera eller avaktivera funktionen i AirKey-onlineadministrationens konfiguration för telefonen. Mer information om redigering av medier finns i Redigera medier.

Gör på följande sätt för att öppna händelseloggar inom appen:

- Starta AirKey-appen.
- Välj menypunkten ***Behörigheter*** i huvudmenyn.
- Välj symbolen för händelseloggen längst upp till höger ❶.



Figur 242: Symbol för händelselogg

- Händelseloggen visas.

Endast poster för den person som har tilldelats telefonen visas i AirKey-appens händelselogg.

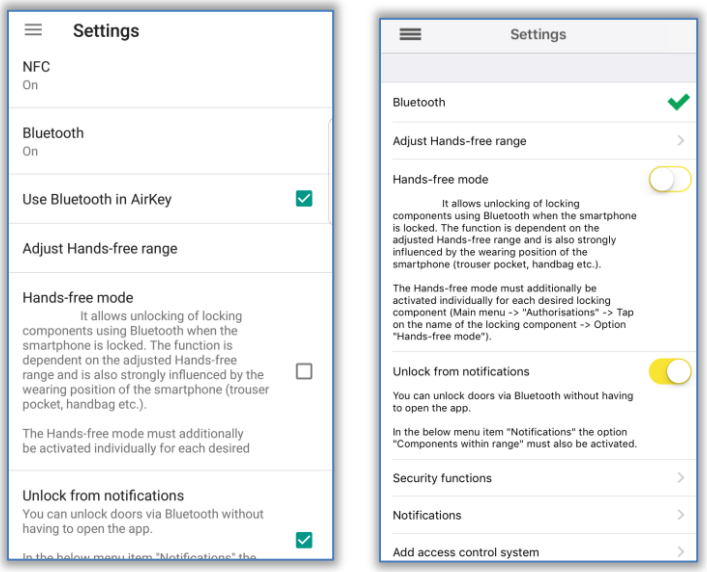
6.16 Hands-free i översikt

Det finns ett hands-free läge för Bluetooth-enheter. Hands-free är en komfortfunktion som innebär att enheten inte längre behöver väljas i appen. Hands-free-funktionen ska inte likställas med funktionen "Aktivera med Bluetooth" men den kan aktiveras för extra komfort.

Efter beröring skickar cylindern en Bluetooth-signal. På väggläsare fungerar detta automatiskt utan beröring. Om en AirKey-app inom enhetens räckvidd tar emot denna

Bluetooth-signal startar aktiveringsprocessen. Avståndet kan ställas in individuellt för cylinder och väggläsare i appen.

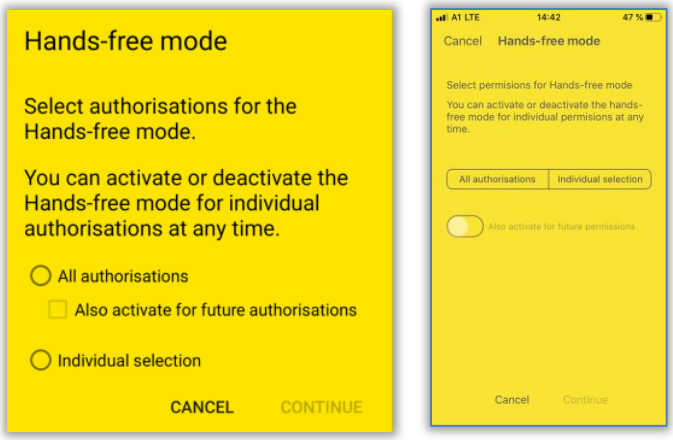
> I huvudmenyn ***Inställningar*** i Airkey-appen måste Hands-free-läget vara aktiverat.



Figur 243: Inställningar AirKey-App

På Android-smarttelefoner startas en tjänst när denna funktion aktiveras. Den här tjänsten söker permanent efter Bluetooth-enheter inom räckvidd även om AirKey-appen är stängd och leder till ökad batteriförbrukning på smarttelefonen. Tjänsten avslutas så fort funktionen avaktiveras. När man trycker på meddelandet från tjänsten kommer man direkt till inställningarna för AirKey-appen.

> För varje enhet eller område måste Hands-free-läget aktiveras i behörighets-detaljerna i menypunkten ***Rättigheter***. Första gången Hands-free-läget aktiveras visas en dialog där funktionen kan aktiveras automatiskt för alla enheter eller individuellt endast för enskilda enheter.



Figur 244: Behörigheter Hands-free-läge

Aktivera funktionen ***Aktivera även för framtida behörigheter*** för att aktivera Hands-free-läget även för alla andra behörigheter.

Beroende på inställningen ***Tillträde från låsskärmen*** i AirKey-online-administrationen kan aktivering ske direkt från låst skärm eller så måste skärmlåset först låsas upp. Mer information finns under Allmänt.

Anpassa räckvidd för Hands-free: Se kapitel 6.9.3 Fehler! Verweisquelle konnte nicht gefunden werden.

Vad ska man tänka på vid användning av Hands-free-läget?

När smarttelefonens display är låst är funktionen beroende av

- inställningen "Tillträde från låsskärmen" i AirKey-onlineadministrationen;
- tillverkare, operativsystem, ålder, antal installerade appar, app-optimeringar (energisparfunktion) på smarttelefonen;
- störfaktorer som typ av byggnad (t.ex. stålbetongkonstruktion) och radiofrekvenser i omgivningen;
- smarttelefonens förvaringsplats resp. transportplats samt den inställda räckvidden för Hands-free-funktionen;
- om smarttelefonen är ansluten till ett trådlöst nätverk.

Dessa faktorer kan göra så att Hands-free-funktionen fungerar långsammare eller inte alls. För att påskynda aktiveringen med Hands-free-funktionen måste man beroende på operativsystem (t.ex. iOS) låsa upp smarttelefonen och starta AirKey-appen. I detta fall behöver man inte välja de enheter som ska låsas upp i appen.

För att undvika felaktiga aktiveringar ska följande beaktas:

- Efter varje aktivering följer en timeout på 2 minuter för väggläsaren. Detta innebär att en väggläsare kan aktiveras med hjälp av Hands-free-funktionen igen, först när smarttelefonen varit utanför väggläsarens mottagningsräckvidd i 2 minuter. Detta motverkar att aktivering sker oavsiktligt när man lämnar räckvidden för enheten.
- I idealfallet finns endast en enhet inom en smarttelefons räckvidd.
- För att funktioner som "Koda medier" eller "Uppdatera enheter" ska kunna genomföras måste Hands-free-läget avaktiveras i telefonens app.

7 Använda AirKey-enheter

7.1 Aktivering med smarttelefonen

Följande krav måste vara uppfyllda för att en AirKey-enhet ska kunna aktiveras:

- NFC eller Bluetooth har aktiverats på telefonen.
- AirKey-appen är installerad och registrerad.
- En giltig behörighet har tilldelats telefonen (se kapitlet Registrera smarttelefoner och Tilldela behörigheter för mer information).
- Placera telefonen mot AirKey-enheten för aktivering via NFC. Den bästa positionen för dataöverföring beror på vilken telefonmodell som används. Avläsningsområdet påverkas även av telefonmodellen och kan variera mellan direkt kontakt och några få millimeters avstånd. För aktivering med Bluetooth beror avläsningsräckvidden för det första på modellen av telefon och för det andra på dina personliga inställningar i AirKey-appen på den telefon som ska användas i Hands-free-läget. Räckvidden är ett par meter.
- Ska man ange en pinkod är det viktigt att korrekt kod aktiverar AirKey-funktionen innan enheten kan kommunicera via NFC eller Bluetooth (se kapitlet Säkerhetsfunktioner för mer information om pinkod).
- Var uppmärksam på visuella signaler på AirKey-enheten. Används NFC ska man placera telefonen mot AirKey-enheten. Används Bluetooth stanna inom räckvidd för AirKey-enheten. Vänta tills enheten avger en grön signal. (Blått ljus indikerar kommunikation mellan telefonen och AirKey-enheten).

Med iPhone-modellerna XR, XS, XS Max eller senare kan du även aktivera Bluetooth-enheter via NFC. Detta gör man genom att hålla smarttelefonen mot enheten och trycka på informationsmeddelandet, en NFC-tagg har identifierats. Därefter öppnas AirKey-appen och aktivering via Bluetooth genomförs.

Figur 245: iOS-NFC-tagg

Kontrollera behörigheten eller pinkod om AirKey-enheten avger ett rött ljus.

Man kan inte aktivera enheter med NFC när skärmlåset är aktivt eller när samtal pågår. AirKey-appen behöver dock inte vara öppen eller aktiv för att enheter ska kunna aktiveras. I motsats till detta kan man aktivera AirKey-enheter med Bluetooth när skärmlåset är aktivt via pushmeddelanden. Man behöver bara aktivera funktionen "Upplåsning meddelanden" i AirKey-appens inställningar. I inställningarna för AirKey-appen måste alternativet

"Lås upp från meddelanden" aktiveras och i AirKey-onlineadministrationen måste "Tillträde från låsskärmen" vara tillåtet.

7.2 Tillräde med medier som kort, nyckelbrickor, armband eller kombinycklar

Mediet måste ha lagts till i systemet och ha en giltig behörighet för att aktivera en AirKey-enhet (se Lägga till kort, nyckelbrickor och kombinycklar med en smarttelefon och Tilldela behörigheter).

- Håll mediet mot AirKey-enheten. Avstånden för dataöverföring beror på mediatypen och är i regel några millimeter.
- Var uppmärksam på visuella signaler på AirKey-enheten. Ta inte bort mediet förrän AirKey-enheten avger en grön signal (blått ljus indikerar enbart kommunikation mellan medium och AirKey-enhet).

Kontrollera din behörighet om din AirKey-enheten avger ett rött ljus.

- AirKey-enheten aktiveras under den inställda tiden och man beviljas tillträde.

Funktionen för medier såsom kort, nyckelbrickor, armband och kombinycklar kan försämras eller begränsas av andra medier eller metallobjekt i närheten. Detta kan påverka medier som förvaras i en plånbok, handväska eller nyckelring med nycklar.

Använd sidan med RFID-ikonen på kombinyckel för identifiering vid AirKey-enheten.

8 AirKey-systemets drift och underhåll

8.1 Uppdatera låskomponenter

I regel kan man uppdatera enheter, oberoende av deras koppling till vilket system, för uppdatering mellan AirKey-onlineadministration och enheter.

Man kan uppdatera med Android/iPhone -telefoner eller med (tillval) kodningsstationer. Uppdatering med telefonen kräver endast att den är installerad med AirKey-appen och registrerad i ett AirKey-system.

Följande uppgifter slutförs när AirKey-enheterna uppdaterats:

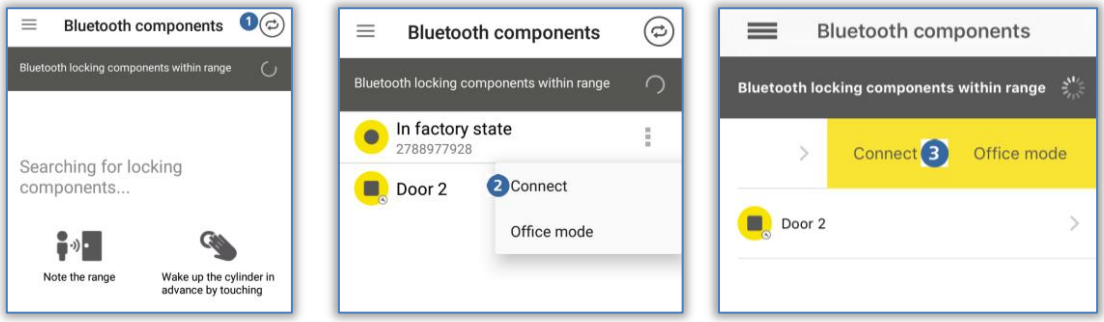
- Tidsåterställning.
- Avläsning av händelseloggen och batteristatus.
- Uppdatering av uppgifter i (black list, behörigheter i andra AirKey-system, etc.).
- Avläsning av enhetsdata.

Följ instruktionerna på displayen för att uppdatera enheten med telefonen.

> Upprätta en anslutning med **NFC** (för Android-telefoner):
Tryck på symbolen ***Anslut till komponent*** ❶.

> Upprätta en anslutning med **Bluetooth** (för Android-telefoner): Tryck på kontext-menyn för den AirKey-enhet till vilken man ska ansluta (⋮) och välj ***Anslut*** ❷.

> Upprätta en anslutning med **Bluetooth** (för iPhones): Svep enhetsbeteckningen för den AirKey-enhet till vilken man ska upprätta en anslutning och välj sedan ***Anslut*** ❸.



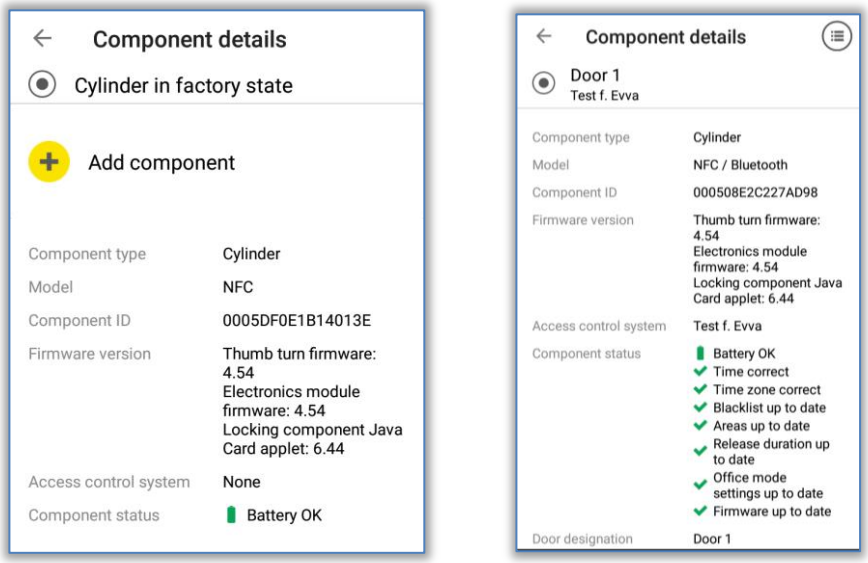
Figur 246: AirKey-app – ansluta till komponent (Android NFC / Android Bluetooth / iPhone)

> Följ anvisningarna.

Figur 247: Uppdatera data

Data är uppdaterat. Under överföringar ska du inte avlägsna NFC-telefonen från den enhet som ska uppdateras och stanna kvar inom Airkey-enhetens räckvidd för Bluetooth. När processen är slutförd visas ett meddelande.

Den information som visas i uppdateringsmeddelandet varierar beroende på om uppdareringsfunktionen har aktiverats på telefonen och på om AirKey-enheten befinner sig i ditt eget eller ett externt AirKey-system.



Figur 248: Uppdateringsmeddelande

Avaktivera Hands-free-läget innan du ansluter dig till en Bluetooth-enhet (gäller vid uppdatering via funktionen "anslut" i appen). I annat fall kan det leda till avbrott i anslutningen.

Bluetooth-enheter kan uppdateras automatiskt efter varje aktivering via Bluetooth. Mer information om funktionen "Uppdatering efter varje upplåsning" hittar du under Standardvärden (för alla nyligen tillagda låskomponenter).

Option **Uppdatera AirKey-enheter med hjälp av kodningsstationer**

Gör på följande sätt för att uppdatera enheter med en kodningsstation:

> Logga in på systemet och se till att kodningsstationen är ansluten och har valts i AirKey-onlineadministration.

> Placera enheten på kodningsstationen.

Figur 249: Uppdatera enheter med en kodningsstation

> Avlägsna inte enheten från kodningsstationen förrän uppdateringen är slutförd och systemet ber dig bekräfta uppdateringen.

Den information som visas i meddelandet om att uppdateringen slutförts korrekt kan variera beroende på om enheten befinner sig i ett eget eller ett externt AirKey-system.

Figur 250: AirKey-enheter uppdaterade med hjälp av kodningsstationer

Uppdatera systemets enheter med jämna mellanrum. Det är de enda sättet som säkerhetsställer att AirKey-systemet är säkert och uppdaterat.

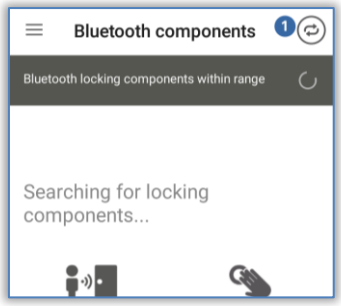
8.2 Uppdatera smarttelefoner: Se kapitel 6.10

8.3 Uppdatera medier

Man kan uppdatera alla AirKey-medier oberoende av deras koppling till ett system. Med Android-telefoner eller kodningsstationer. Uppdatering med telefoner kräver endast att man installerat AirKey-appen och registrerats i ett AirKey-system.

För iPhones ska man följa anvisningarna i Koda medier för att uppdatera medier och använda en AirKey-enhet som kodningsstation.

> Välj symbolen ***Anslut till komponent*** ❶ längst upp till höger i AirKey-appen när man använder en Android-telefon.



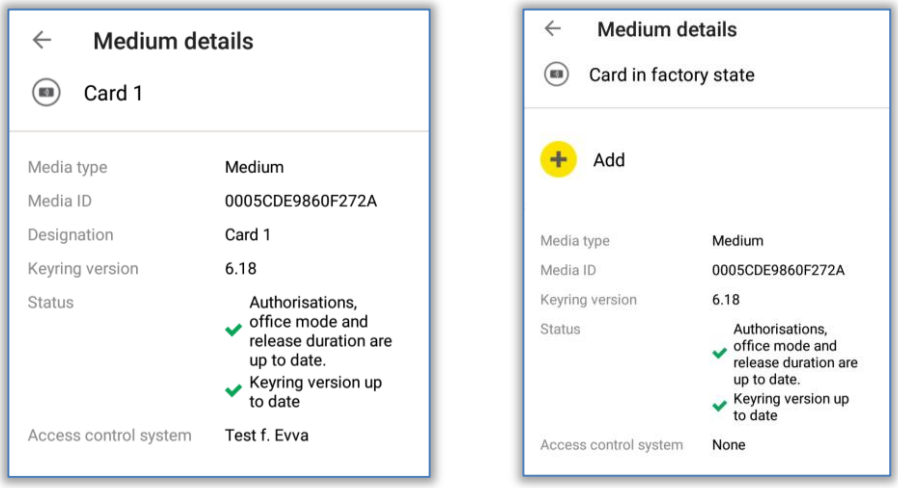
Figur 251: Symbol "Anslut till komponent" (endast Android-telefoner)

> Följ anvisningarna på skärmen och håll telefonen mot mediet.

Figur 252: Uppdatera data

Data är uppdaterat. Avlägsna inte telefonen från det objekt som ska uppdateras medan dataöverföring pågår. När processen är slutförd visas ett meddelande om detta.

Använder man en telefon för att uppdatera kombinycklar ska den sida av kombinyckeln som är försedd med RFID-symbolen hållas mot telefonens NFC-antenn.



Figur 253: AirKey-appen uppdaterar ett medium

Option

Uppdatera medier med en kodningsstation

Gör på följande sätt för att uppdatera kort, nyckelbrickor, armband eller kombinycklar med en kodningsstation:

Logga in på AirKey-systemet och se till att kodningsstationen är ansluten och har valts i AirKey-onlineadministration.

> Placera mediet på kodningsstationen.

Figur 254: Uppdatera medier med kodningsstationen

> Avlägsna inte mediet från kodningsstationen förrän uppdateringen är slutförd och systemet ber dig bekräfta uppdateringen.

Den information som visas i meddelandet om att uppdateringen slutförts korrekt kan variera beroende på om mediet befinner sig i ett eget eller externt AirKey-system.

Figur 255: Uppdatera egna eller externa medier med kodningsstationen

Uppdatera medier med jämna mellanrum. Det är enda sättet för att vara säker på att AirKey-systemet är säkert och uppdaterat.

Uppdatera medierna regelbundet för att säkerställa att alla poster i händelseloggen har överförts från medierna till AirKey-onlineadministrationen.

Används kodningsstationen för att uppdatera kombinycklar ska den sida av kombinyckeln som är försedd med RFID-symbolen hållas mot kodningsstationen. Uppdateringen fungerar inte över kodningsstationens hela avläsningsområde – med den aktuella typen (HID Omnikey 5421) detekteras kombinycklar endast inom övre och den nedre tredjedelen av kodningsstationen.

8.4 Uppdatera AirKey-enheters firmware

Finns det ny firmware till en AirKey-enhet visas ett meddelande i enhetens detaljer, i underhållsuppgifterna samt i samband med uppdatering av enheter.

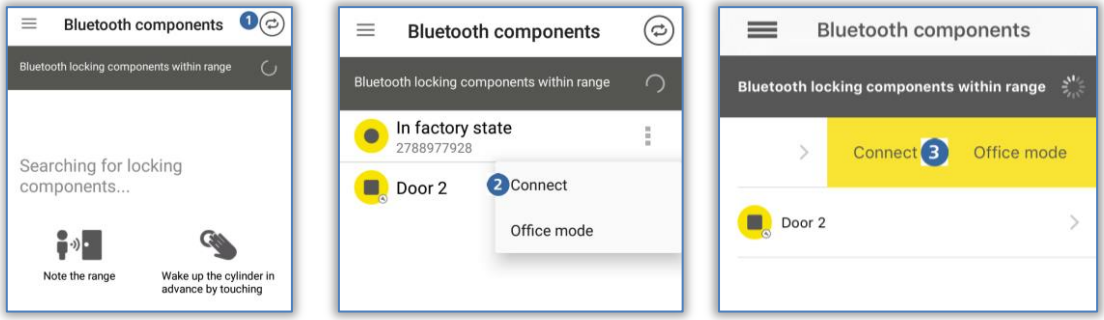
Kontrollera batteristatusen för enheten (cylinder) innan en firmware uppdatering genomförs. Är varningen "Lågt batteri" aktiv, byt alla batterier så att uppdateringen kan ske smidigt.

AirKey-enhetens aktuella firmware visas i enhetens detaljer.

Använd telefonen eller kodningsstationen för att uppdatera firmware till AirKey-enheter.

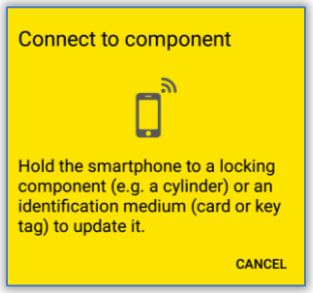
Aktivera specialbehörigheten "underhållsbehörighet" på telefonen, för uppdatering av firmware. Gör följande för att uppdatera firmware med telefonen:

- Upprätta en anslutning med **NFC** (för Android-telefoner):
  Tryck på symbolen ***Anslut till komponent*** ❶.
- Upprätta en anslutning med **Bluetooth** (för Android-telefoner): Tryck på kontextmenyn för den AirKey-enhet till vilken man vill upprätta en anslutning (⋮) och välj sedan ***Anslut*** ❷.
- Upprätta en anslutning med **Bluetooth** (för iPhones): Svep över enhetsbeteckningen för den AirKey-enhet som ska anslutas och välj ***Anslut*** ❸.



Figur 256: AirKey-app – ansluta till komponent (Android NFC / Android Bluetooth / iPhone)

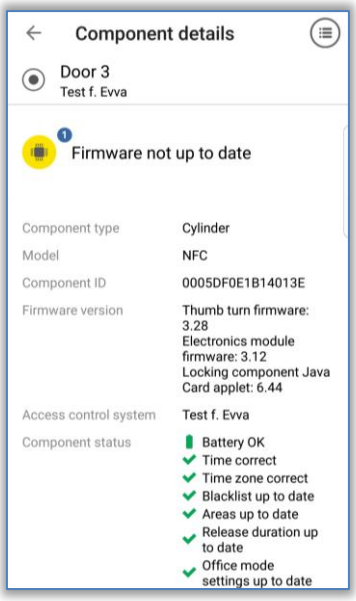
- Följ anvisningarna.



Figur 257: Anslutning till komponenten – firmware uppdatering

Uppgifter är uppdaterade. Under överföringen håll kvar NFC-telefonen mot den enhet som ska synkroniseras och stanna kvar inom Airkey-enhetens räckvidd med Bluetooth-telefonen. När processen är slutförd visas ett meddelande.

- AirKey-enheten är uppdaterad och enhetsdetaljerna visas. I enhetens detaljer indikeras om firmware för enheten inte är uppdaterad.



Figur 258: AirKey-app – enhetens detaljer

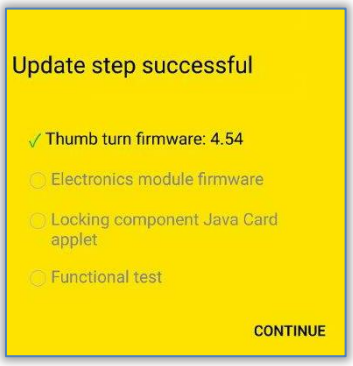
> Klicka på ***Uppdatera firmware*** ❶ på skärmen.

> Håll NFC-telefonen mot AirKey-enheten eller stanna kvar inom Bluetooth-telefonens räckvidd.

Figur 259: AirKey-app – uppdatera firmware

Firmware uppdateringar kan ta flera minuter beroende på internetuppkopplingen. Håll NFC-telefonen permanent mot AirKey-enheten eller stanna kvar inom Airkey-enhetens räckvidd med Bluetooth-telefonen under denna tid.

Avlägsna inte telefonen från den enhet som ska uppdateras medan dataöverföring pågår. När det första steget har genomförts korrekt visas ett meddelande om detta.

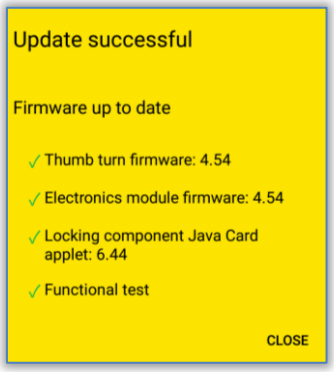


Figur 260: AirKey-app – Uppdateringssteg klart

> Avlägsna telefonen tills enheten blinkar och en ljudsignal avges.

> Håll åter NFC-telefonen mot enheten / med Bluetooth stanna inom enhetens räckvidd och följ anvisningarna på skärmen.

När firmware uppdateringen har genomförts korrekt visas ett meddelande.



Figur 261: AirKey-app – uppdatering lyckades

> Klicka på ***Stäng*** för att bekräfta säkerhetsfrågan och slutföra firmware uppdateringen.

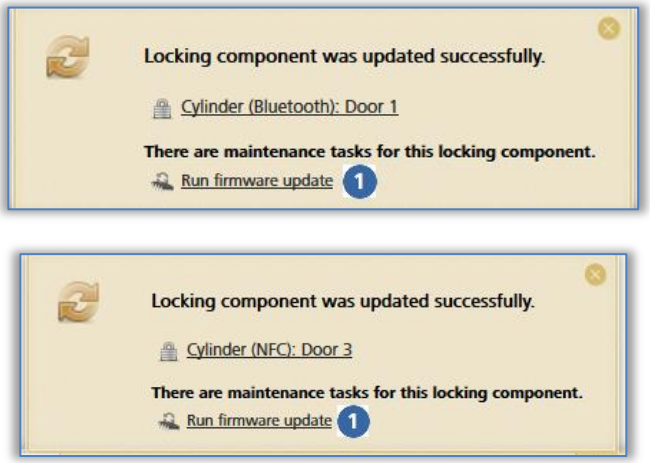
AirKey-enhetens status uppdateras i systemet. Uppmaningen om firmware uppdatering visas inte mer och korrekt firmware visas i enhetens detaljer.

Option

Uppdatera firmware med kodningsstationen:

> Placera enheten på kodningsstationen. Uppdateringen startar automatiskt när kodningsstationen får kontakt med enheten.

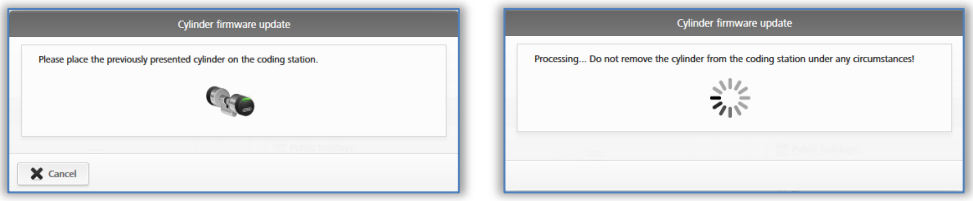
När uppdateringen är slutförd visas ett meddelande.



Figur 262: Kodningsstation – bekräftelse vid uppdatering av AirKey-enheter

En länk visas för en tillgänglig uppdatering ❶ av firmware till enheter.

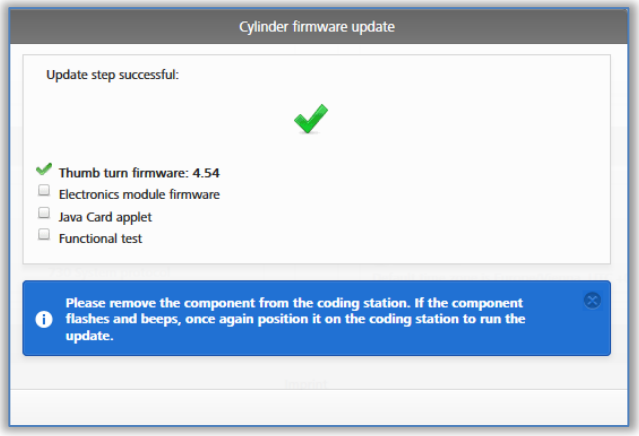
> Klicka på ***Kör firmware uppdatering*** för att starta processen.



Figur 263: Kodningsstation – firmware uppdatering för AirKey-cylinder

Firmware uppdateringar kan ta flera minuter beroende på internetuppkopplingen. Avlägsna inte enheten från kodningsstationen !

Första steget av firmware uppdateringen bekräftas.

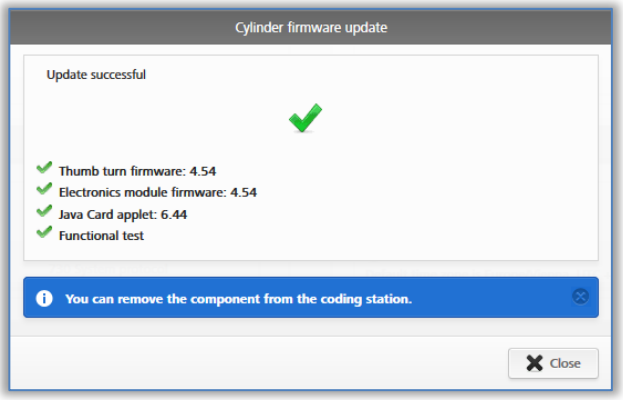


Figur 264: Kodningsstation – uppdatering klar.

> Avlägsna enheten från kodningsstationen. Enheten startar om med en visuell och akustisk signal.

> Placera enheten på kodningsstationen igen för att slutföra processen.

När uppdateringen är slutförd visas ett meddelande.



Figur 265: Kodningsstation – firmware uppdatering klar

AirKey-enheten är uppdaterad när bekräftelsen har stängts.

Figur 266: Kodningsstation – enhet uppdaterad korrekt

> Avlägsna enheten från kodningsstationen när den har uppdaterats.

Enhetens status uppdateras i hela systemet. Uppdateringen visas inte mer och korrekt firmware visas i enhetens detaljer.

Öppna dörren och säkra den så att den inte kan gå i lås av misstag under firmware uppdateringen. Kontrollera att enheten fungerar korrekt innan dörren stängs.

När man uppdaterar AirKey-enhetens firmware är det viktigt att se till att internetuppkopplingen är stabil och att dataanslutningen inte avbryts under uppdateringen. Beroende på telefon och operativsystem finns det en rad inställningar som säkerställer detta (t.ex. tillåt automatiska nätverks-ändringar mellan mobila datanätverk och WiFi-nätverk).

EVVA rekommenderar att man alltid håller firmware versionen uppdaterad för AirKey-enheterna.

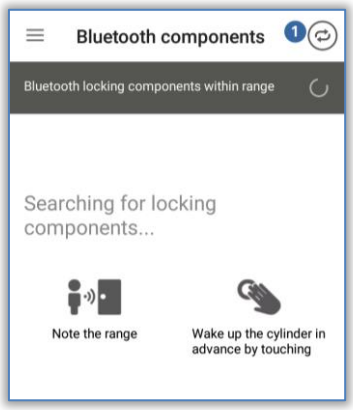
8.5 Uppdatera Keyring-versionen av medier

I AirKey-systemet är "Keyring" namnet på den firmware som lagrar AirKey-relevanta uppgifter som finns sparade på passiva tillträdesmedier såsom kort, taggar, kombinycklar och armband. När nya Keyring-versioner blir tillgängliga för medier, visas denna information i detaljerna för respektive medium på startsidan ***Home*** samt när AirKey-enheter uppdateras.

Mediets aktuella Keyring-version visas i fliken detaljer.

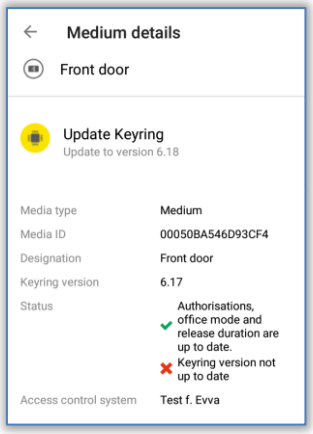
Använd en telefon eller valfri kodningsstation för att uppdatera mediets Keyring. Aktivera specialbehörigheten "underhållsbehörighet" på telefonen för att uppdatera mediets Keyring. Gör på följande sätt för att uppdatera mediets Keyring med telefonen:

- Upprätta en anslutning med **NFC** (för Android-telefoner):
  Tryck på symbolen ***Anslut till komponent*** ❶.
- Upprätta en anslutning med ***Bluetooth*** (för Android-telefoner och iPhones):
  Välj menypunkten ***Koda medier*** i appens huvudmeny – se Koda medier.



Figur 267: AirKey-app – ansluta till komponent

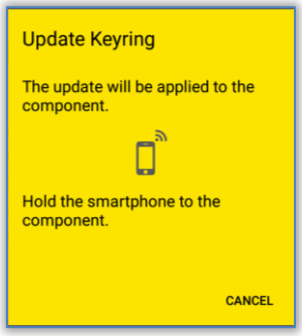
- Håll mediet mot telefonens NFC-chip.
- Systemet uppdaterar mediet. Det indikerar att en ny Keyring-version är tillgänglig.



Figur 268: AirKey-app – mediadetaljer

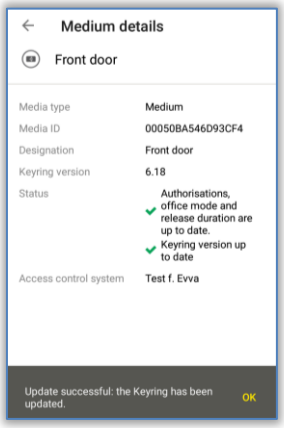
> Välj alternativet ***Uppdatera Keyring***.

> Håll mediet mot telefonens NFC-chip och följ anvisningarna på skärmen.



Figur 269: AirKey-app – uppdatera Keyring

Keyring-uppdateringen kan ta flera minuter beroende på internet-uppkopplingen. Håll kvar mediet mot telefonens NFC-chip under denna tid. Avlägsna inte mediet från smarttelefonen medan dataöverföring pågår. När uppdateringen har genomförts korrekt visas en bekräftelse i appen.



Figur 270: AirKey-app – Keyring-uppdatering korrekt

Mediets status visas i systemet. Korrekt Keyring-version visas i mediets detaljer.

Används telefonen för att uppdatera kombinycklar ska den sida av kombinyckeln som är försedd med RFID-symbolen hållas mot telefonens NFC-chip.

Option

Uppdatera Keyring med kodningsstationen:

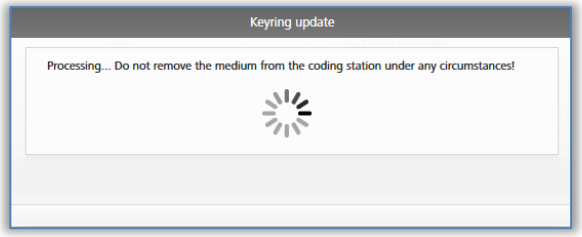
> Placera mediet på kodningsstationen. Uppdateringen startar automatiskt när kodningsstationen identifieras av mediet.

När uppdateringen är slutförd får man en bekräftelse.

Figur 271: Kodningsstation – en Keyring-uppdatering finns tillgänglig

En länk visas när ❶ det finns firmware uppdateringar tillgängliga

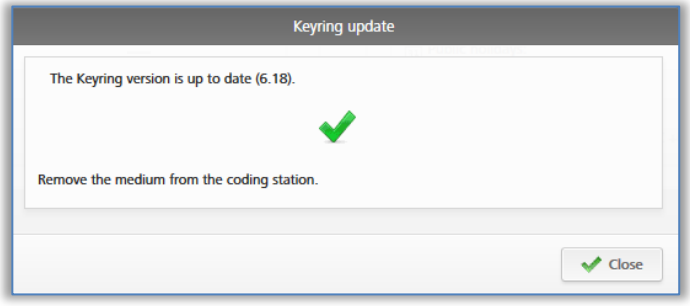
> Klicka på ***Kör Keyring-uppdatering*** för att starta uppdateringen.



Figur 272: Kodningsstation – Keyring-uppdatering

Keyring-uppdateringen kan ta flera minuter beroende på internetuppkopplingen. Avlägsna inte mediet från kodningsstationen under denna tid.

Avlägsna inte mediet från kodningsstationen medan Keyring-versionen uppdateras. Vid uppdatering av Keyring-versionen visas en bekräftelse när det är klart.



Figur 273: Kodningsstation – Keyring-uppdatering klar

Keyring-uppdateringen är slutförd. Uppdateringen är klar när bekräftelsen har stängts.

Figur 274: Kodningsstation – medium uppdaterat

> Ta bort mediet från kodningsstationen när det har uppdaterats.

När man använder kodningsstationen för att uppdatera kombinycklar ska den sida av kombinyckeln som är försedd med RFID-symbolen hållas mot kodningsstationen. Avläsningen fungerar inte över kodningsstationens hela avläsningsområde – med den aktuella typen (HID Omnikey 5421) detekteras kombinycklar endast inom övre och den nedre tredjedelen av kodningsstationen.

Mediets status visas i systemet. Korrekt Keyring-version visas i mediets detaljer.

Vid uppdatering av Keyring-versioner se till att en använda en säker data-kommunikations uppkoppling. Beroende på telefon och operativsystem finns det en rad inställningar som säkerställer detta (t.ex. tillåt automatiska nätverksändringar mellan mobila datanätverk och WiFi-nätverk, undvik ogynnsamma internetanslutningar, etc.).

EVVA rekommenderar att Keyring-versionerna är uppdaterade.

8.6 Uppdatera app-versioner på Android och iPhone telefoner

När en ny uppdatering för AirKey-appen finns tillgänglig visas ett meddelande i telefonen. Beroende på inställningarna för Google Play Store eller Apple App Store uppdateras AirKey-appen automatiskt eller manuellt.

Man kan fortsätta att använda AirKey-appen som vanligt när uppdateringen av appversionen är slutförd.

Det krävs ett konto för Google Play eller en Apple ID för att kunna ladda ned appar från Google Play Store eller Apple App Store.

Uppdateringar av appen kan vara rekommenderade eller obligatoriska. Ett meddelande visas i AirKey-appen.Om uppdatering ej genomförs kan vissa begränsningar förekomma i appen Man kan dock fortsätta aktivera enheter.

EVVA rekommenderar att man alltid håller AirKey-appversionen för telefoner uppdaterad och att man aktiverar automatiska uppdateringar i Google Play Store eller Apple App Store.

8.7 Byta batterier och använda nödströmsenheten

Byt regelbundet batterier på batteridrivna AirKey-enheter. Kontrollera batteristatusen hos enheter i AirKey-onlineadministration och när du uppdaterar enheter med hjälp av telefoner med underhållsbehörighet.

Systemet skiljer mellan tre olika batteristatusar.

Figur 275: Batteristatus

AirKey-enheten avger varningssignalen "Batteri tomt" när ett medium används för att aktivera enheten. Se kapitlet Låskomponenternas signaler för mer information om signaler.

8.7.1 Byta batterier i AirKey-cylindrar

Byt batterier när dörren är öppen och säkrad och inte kan stängas igen av misstag.

Tänk på att AirKey-cylindern förblir aktiv i högst en minut efter att batterierna har tagits bort.

Vi rekommenderar att man byter tätningarna på AirKey-cylindern vid batteri byte så att enheten alltid är korrekt skyddad mot fukt. Detta gäller tätningen mellan vredhylsa och yttervred samt tätningarna i täckbrickan på yttervredet. Alla dessa tätningar finns som reservdelar. Kontakta din EVVA-partner för mer information.

Vi rekommenderar att du smörjer AirKey-cylindern minst varje gång man byter batterier. Detta görs genom att applicera en droppe av ett smörjmedel som rekommenderas av EVVA mellan vredknoppen och cylinderhuset efter att ha tagit bort vredknoppen. Vi rekommenderar även att man smörjer baksidan av cylindern mellan medbringare och cylinderhus vid demontering av AirKey-cylindern. Kontakta din EVVA-partner för mer information.

> Aktivera AirKey-enheten med hjälp av ett giltigt medium.
> Snäpp på monteringsverktyget på cylindern innan den frikopplas.
> Spärra innertappen med det speciella demonteringsverktyget och vrid vredknoppen moturs.

- Avlägsna monteringsverktyget från vredknoppen.
- Öppna vredknoppen genom att skruva loss de tre skruvarna på baksidan av vredknoppen.
- Demontera täckbrickan från vredknoppen.
- Lösgör försiktigt batterihållaren genom att föra den i sidled och vika den uppåt
- Byt sedan ut batterierna. Kontrollera att batterierna monteras korrekt. Blanda inte gamla och nya batterier.
- Säkra försiktigt batterihållaren genom trycka ner och föra den i sidled.
- Montera täckbrickan på vredknoppen med de tre skruvarna. OBS! kontrollera att den är rättvänd mot batterihållaren.
- Snäpp monteringsverktyget på vredknoppen.
- Montera tätningen korrekt på cylinderaxeln och sätt tillbaka vredknoppen på cylindern genom att vrida den medurs tills man känner ett motstånd.
- Snäpp av monteringsverktyget.
- Vrid sedan vredknoppen moturs tills man hör ett snäpp och känner att det hakar fast.
- Kontrollera att vredknoppen sitter fast ordentligt.
- Det sista steget är att uppdatera enheten med telefonen eller en kodningsstation för att överföra de senaste posterna i händelseloggen till AirKey-onlineadministration.
- Kontrollera att cylindern arbetar korrekt genom att aktivera den innan dörren stängs.

Beroende på batteriernas fysiska egenskaper kan man behöva byta ut dem i ett tidigare skede. Övervaka batteristatus och cylinderfunktioner om systemet arbetar i låga temperaturer (under -10 °C) under en längre period

Skulle enheten indikera kommunikationsfel efter att batterierna har bytts ut, beror detta på att cylindern inte har rätt kontakt med vredknoppen (elektronikmodulen). Kommunikationen fungerar inte om vredknoppen är fel monterad på cylinderhuset.

Kontrollera och uppdatera batteristatusen hos AirKey-enheter med telefonen som har underhållsbehörighet för att se det i detaljerna för enheten i tex. appen.

Är batterierna tömda kan man strömförsörja enheten med nödströmsenheten och visa ett behörigt medium för att aktivera cylindern.

Mer information finns i avsnittet Nödströmsenhet.

Glöm ej att byta batterier efter strömsättning med nödströmsenheten.

Efter strömsättning ska man noggrant återförsegla den vita gummiplutten med EVVA-loggan så att damm eller fukt inte kryper in i elektroniken. För att undvika skador använd inte vassa eller spetsiga verktyg vid demontering och montering av gummiplutten.

8.8 Reparationsalternativ

Reparationsalternativen i AirKey-systemet gör det möjligt att snabbt byta ut felaktiga enheter. Man kan välja mellan att ersätta enheter eller ta bort felaktiga enheter i systemet.

8.8.1 Initiera och installera nya AirKey-enheter

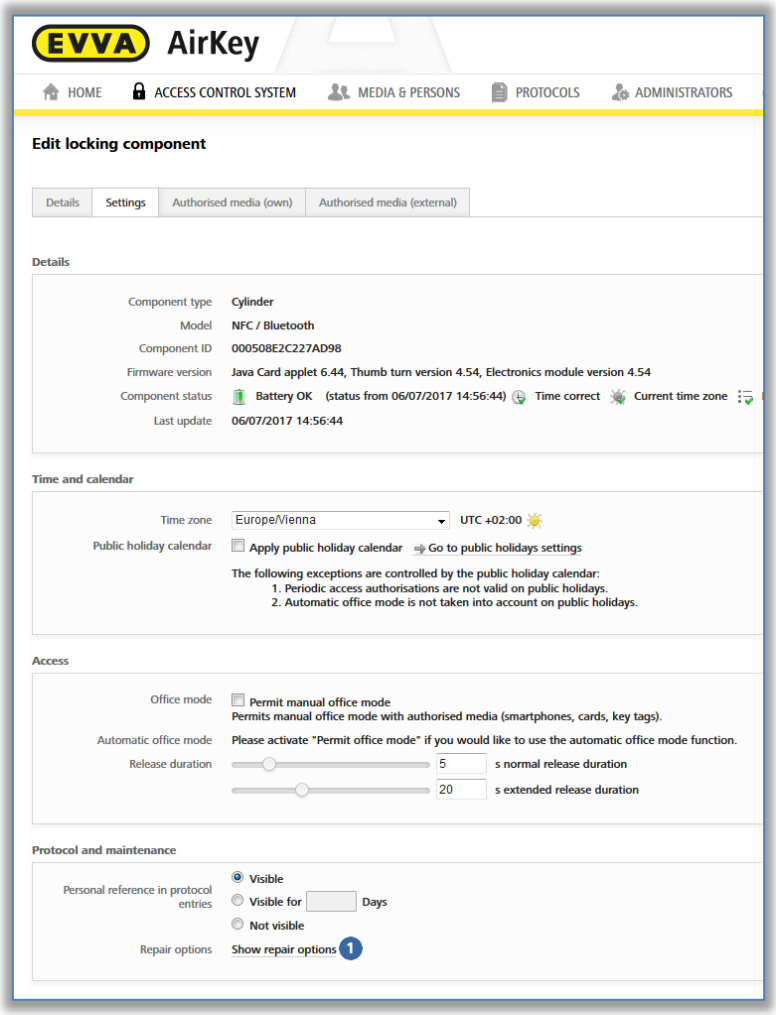
Initiera och installera nya AirKey-enheter för att ersätta befintliga, defekta enheter. Detta innebär att alla egenskaper och behörigheter för denna AirKey-enhet bibehålls inom AirKey-systemet. Efter denna processen befinner sig den nya AirKey-enheten inte längre i fabriksläge.

> På startsidan ***Home*** välj ***Cylindrar*** eller ***Väggläsare***.

> Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.

> Klicka på den låskomponenter som ska redigeras.

> I fliken "Inställningar" välj ***Loggning och reparationsalternativ*** och klickar på ***Visa reparationsalternativ*** ❶.

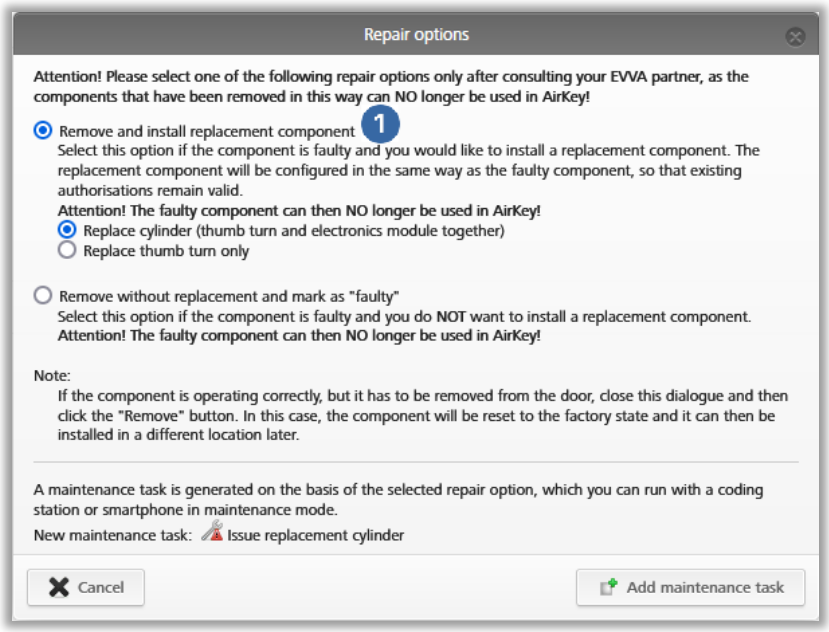


Figur 276: Redigera AirKey-enheter – reparationsalternativ

Dialogfönstret ***Reparationsalternativ*** öppnas.

> Funktionen ***Avinstallera och installera ersättningsenheter*** ❶ och Växla cylinder (vred och elektronikmodul tillsammans) är tillgängliga som standard.

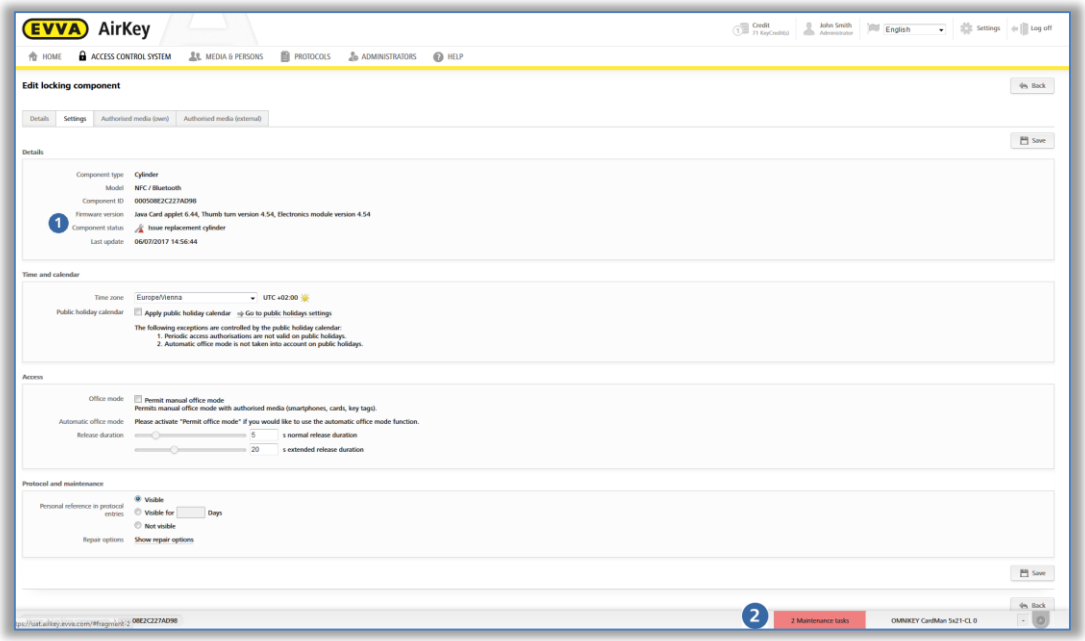
> Alternativt välj funktionen ***Byt endast vred***.



Figur 277: Reparationsalternativ

> Klicka på ***Lägg till underhållsuppgift***.

AirKey-enhetens status ❶ uppdateras och visas som uppdateringsuppgift ❷.



Figur 278: Enhetsstatus och uppdatering

Förberedelserna för att utfärda och installera en ny AirKey-enhet i AirKey-onlineadministration är nu klart. Initiera och installera den nya AirKey-enheten med en telefon med underhållsbehörighet eller en kodningsstation för att slutföra hela processen.

Den enhet som ska tas bort förblir tillgänglig för uppdateringar tills den nya AirKey-enheten har installerats helt. Detta säkerställer att händelseloggar

är fullständiga om det förekommer tillträdeshändelser från det att den nya enheten initierats och fram till att den nya enheten har installerats helt.

Vid byte av AirKey-enheter med Bluetooth visas den gamla och den nya AirKey-enheten i listan över Bluetooth-enheter inom räckvidd. Demontera batterierna eller koppla från strömförsörjningen till den gamla enheten när den har bytts ut. Då kommer den inte längre att visas på listan över Bluetooth-enheter.

Lägga till och installera AirKey-enheter med hjälp av Android/iPhone-telefonen

Det behövs en telefon med underhållsbehörighet för det AirKey-system där man vill initiera och installera den nya enheten.

- Anslut med **NFC** (för Android-telefoner): Tryck på symbolen ***Anslut till komponent*** och håll telefonen mot låskomponenter i fabriksläge.
- Upprätta en anslutning med hjälp av **Bluetooth** (för **Android**-telefoner): öppna kontextmenyn i den låskomponenter i fabriksläge som du vill lägga till i systemet (⋮) och välj sedan ***Anslut***.
- Anslut med **Bluetooth** (för **iPhones**): Svep beteckningen "i fabriksläge" på den nya låskomponenter som ska läggas till i systemet åt vänster och välj sedan ***Anslut***.
- Efter uppdatering klicka på ***Utfärda ersättningscylinder*** i låskomponenter detaljer.
- I följande dialog väljer du den låskomponenter som du vill ersätta och klickar på ***Fortsätt***.
- Används NFC ska du åter hålla telefonen mot låskomponenter i fabriksläge. Används Bluetooth ska man välja låskomponenten i fabriksläge från listan över AirKey-enheter inom räckvidd.
- Ange om man ska uppdatera enheten för senare installation.
- Klicka på ***Installera senare*** för att senarelägga den fysiska installationen i dörren eller välj ***Slutför*** om enheten redan fysiskt är installerad.
- Uppdatera enheten när den är installerad i dörren.

Option

Initiera och installera nya AirKey-enheter med kodningsstationen.

- Placera den nya AirKey-enheten på kodningsstationen.
- Välj ***Utfärda ersättningscylinder*** längst ned till höger av dialogfönstret och klicka på den AirKey-enhet som ska ersättas.

Figur 279: Enhet i fabriksläge – initiera ersättningscylinder

- Klicka på ***Fortsätt***.

- Placera den nya AirKey-enheten på kodningsstationen.
- Avlägsna inte enheten innan en bekräftelse visas.
- Ange om det ska läggas till en uppdatering för senare installation.
- Klicka på ***Installera senare*** för att senarelägga den fysiska installationen i dörren eller välj ***Slutför*** om enheten redan är installerad.
- Uppdatera enheten när du har installerat den vid dörren.

Denna process omfattar även programuppdatering om den nya AirKey-enheten fortfarande har en gammal programversion.

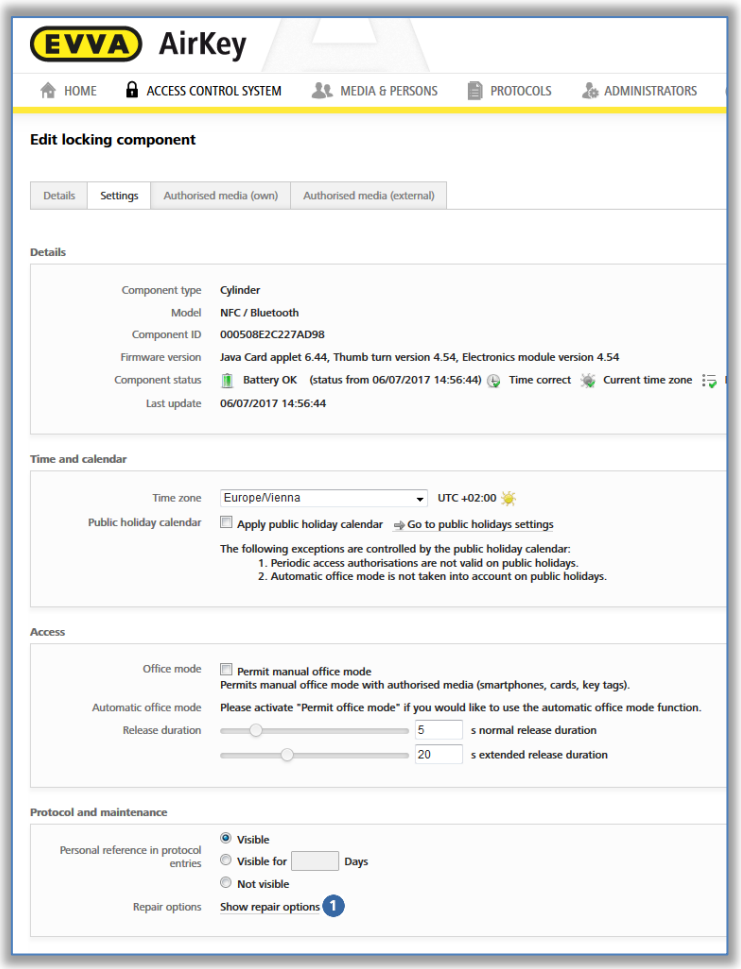
Du kommer inte längre att kunna använda den AirKey-enheten efter denna process. Därför bör man använda denna funktion endast om AirKey-enheten är defekt och skall skrotas.

8.8.2 Ta bort AirKey-enheter utan ersättningar och markera dem som "defekta"

Om en defekt enhet inte behöver ersättas men ändå inte ska visas i AirKey-systemet, kan man ta bort den utan ersättning i reparationsalternativen.

Man kommer då inte längre att kunna uppdatera enheten och den där därmed inte längre brukbar.

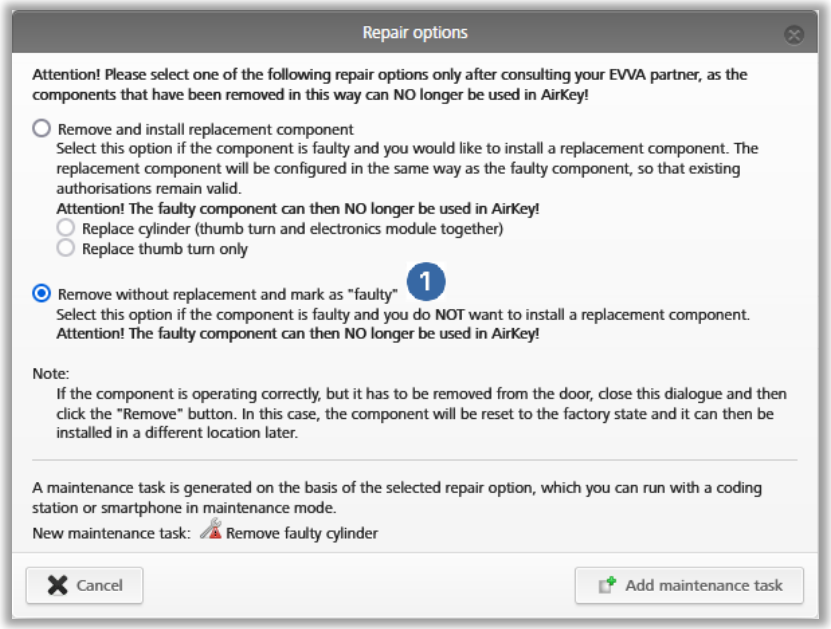
- På startsidan ***Home*** väljer du rutan ***Cylindrar*** eller ***Väggläsare***.
- Alternativt kan du välja ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.
- Klicka på den låskomponenter som ska redigeras i översikten.
- I fliken ***Inställningar*** väljer du ***Loggning*** och reparationsalternativ och klickar på länken Visa ***reparationsalternativ*** ❶.



Figur 280: Redigera AirKey-enheter – reparationsalternativ

Dialogfönstret "Reparationsalternativ" öppnas.

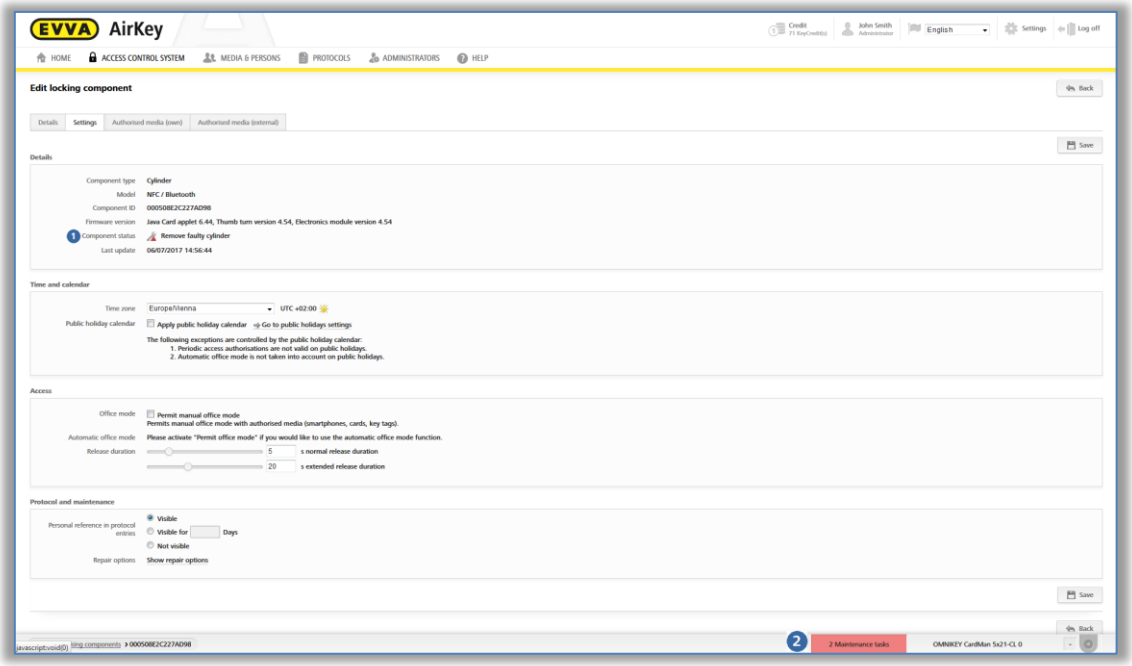
> Välj ***Demontera utan ersättning och markera som "defekt"*** ❶.



Figur 281: Reparationsalternativ

> Klicka på ***Lägg till underhållsuppgift***.

Låskomponenter status ❶ uppdateras och visas som uppdaterad ❷.



Figur 282: Enhetsstatus och uppdateringar

Man har nu slutfört förberedelserna för borttagning av defekta enheter utan ersättning i AirKey-onlineadministration. Slutför hela processen för borttagning av enheten med att använda en telefon med underhållsbehörighet eller en kodningsstation.

8.8.3 Avinstallera defekta AirKey-enheter med Android/iPhone-telefoner

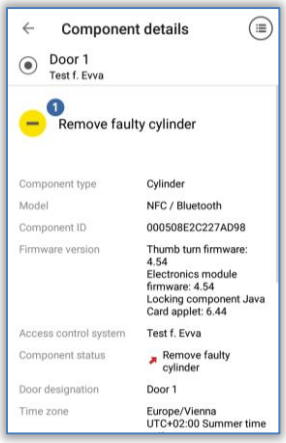
Går det inte att uppdatera /reparera enheten, använd telefonen för att avistallera den defekta enheten utan ersättning. OBS! Detta kräver en registrerad smarttelefon med aktiv underhållsbehörighet för AirKey-låssystemet i fråga.

> Upprätta en anslutning med **NFC** (för Android-telefoner): Tryck på symbolen ***Anslut till komponent*** och håll telefonen mot den enhet som ska avinstalleras.

> Upprätta en anslutning med **Bluetooth** (för **Android**-telefoner): Tryck på kontextmenyn för den AirKey-enhet som du vill ta bort (⋮) och välj sedan ***Anslut***.

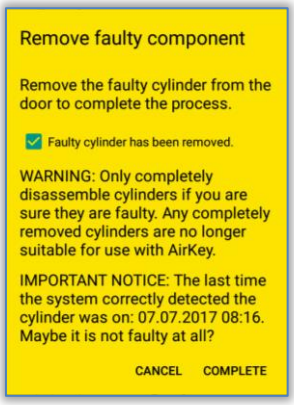
> Upprätta en anslutning med **Bluetooth** (för **iPhones**): Svep beteckningen för den enhet som ska avinstalleras till vänster och välj sedan ***Anslut***.

> Enhetsdetaljerna visas. Välj ***Avinstallera defekt cylinder*** ❶.



Figur 283: Telefon – ta bort felaktiga enheter

> Kryssa för rutan i dialogen och klicka på ***Avsluta*** för att bekräfta.



Figur 284: Telefon – ta bort felaktiga enheter – bekräftelse

Processen är nu slutförd och enheten visas inte längre i AirKey-systemet. Enheten kan inte längre användas.

8.8.4 Avinstallera defekta AirKey-enheter i AirKey-onlineadministration

Går det ej att uppdatera / reparera enheten, avinstallera den i AirKey-onlineadministrationen.

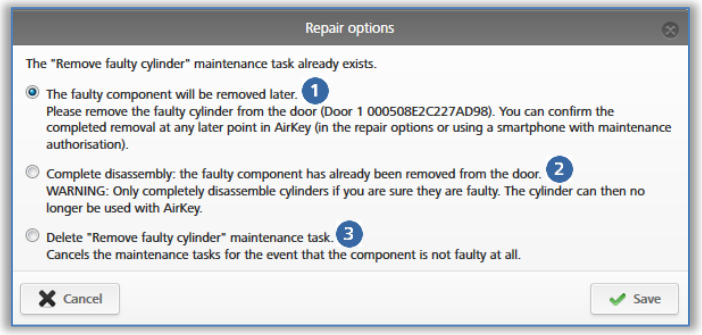
> På startsidan ***Home*** välj ***Cylindrar*** eller ***Väggläsare*** – beroende på vilken enheten som är defekt.

> Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.

> Markera den låskomponenter som ska redigeras.

> I fliken ***Inställningar*** välj ***Loggning*** och reparationsalternativ och klickar på ***Visa reparationsalternativ***.

> En dialog med tre alternativ visas.



Figur 285: Ta bort defekta AirKey-enheter

- Välj ***Den defekta komponenten avistalleras senare*** ❶ för att upprätthålla den aktuella enhetsstatusen så förblir enheten en del i AirKey-systemet.
- Klicka på ***Slutför avinstallation: Den defekta komponenten har redan avinstalleras ur dörren*** ❷ slutför avinstalleringen för att radera den ur systemet.
- Genomför uppdateringen med ***Radera uppdatering "Avinstallera defekt cylinder"*** ❸ för att avinstallera enheten. Se återkalla uppdatering för reparationsalternativ för mer information.

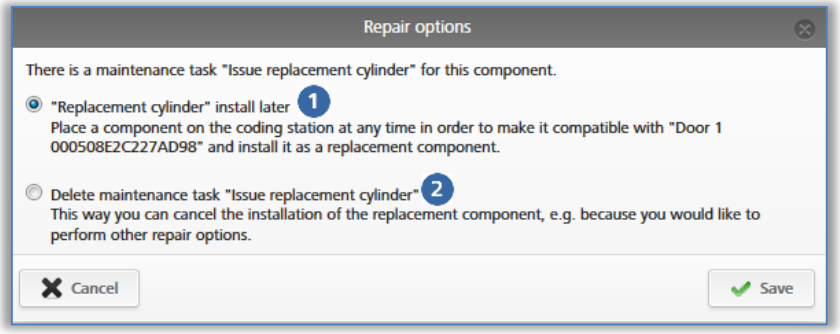
Avinstallerade enheter blir obrukbara efter denna process. Använda denna funktion endast när enheten inte ska användas igen.

För att avinstallera fungerande enhet följ anvisningarna i Ta bort låskomponenter.

8.8.5 Återkalla uppdateringar för reparationsalternativ

Är det skapat uppdateringar för nya enheter eller för avinstallerade enheter radera dessa i systemets mjukvara.

- På startsidan ***Home*** välje ***uppdaterings uppgifter***.
- Välj önskad uppdatering från listan.
- I fliken ***Inställningar*** välj ***Loggning*** och reparationsalternativ och klickar på ***Visa reparationsalternativ***.
- Beroende på uppdateringen, välj utfärda en ersättningsenhet (cylinder, vred, väggläsare) senare ❶ eller radera uppdateringen ❷.



Figur 286: Radera uppdatering

> Klicka på ***Spara***.

Detta raderar uppdateringen. Statusen för AirKey-enheten uppdateras.

En genomförd uppdatering av enheten för reparationsalternativ kan inte tas bort.

Använd även denna funktion för att radera "Enhet måste tas bort" om enheten togs bort från systemet utan att ha varit defekt.

9 Nödmedier

Nödmedier är medier utan utgångsdatum som har permanenta behörigheter till alla enheter i ett AirKey-system. Nödmedier används i nödsituationer (t.ex. av brandkår) och ska förvaras på en säker plats. Nödmedier kan aktivera AirKey-enheter oberoende av tid. Endast strömförsörjningen till AirKey-enheten måste vara aktiv.

9.1 Utfärda nödmedier

Skapa ett nödmedium (t.ex. kort, nyckelbricka, armbandet eller kombinyckel) beskrivs i Skapa kort, nyckelbrickor eller kombinycklar och tilldela permanenta behörigheter till alla enheter i AirKey-systemet. Se till att nödmedierna är uppdaterade om systemet utökas så att även ytterligare enheter kan aktiveras i en nödsituation. Nödmedier aktiverar AirKey-enheter med felaktiga tidsinställningar (t.ex. ej uppdaterad enhet efter batteri byte). Se Tilldela behörigheter och Skapa behörigheter för mer information när man tilldelar och skapar behörigheter.

Tänk på att medier som kort, nyckelbrickor, armband eller kombinycklar kan bli defekta. Därför skapa ett lämpligt antal nödmedier för AirKey-systemet.

Vi rekommenderar att man endast använder kort, nyckelbrickor, armband eller kombinycklar som nödmedier. Telefoner lämpar sig inte för detta ändamål med tanke på batteritiden.

Vi rekommenderar att man skapar ett område som innehåller alla dörrar/enheter kopplade till AirKey-systemet för att underlätta hanteringen av nödmedier. Tilldela en permanent behörighet för detta område till nödmedierna.

10 Arbeta med flera AirKey-system

I följande avsnitt förklaras hur man arbetar med flera AirKey-system.

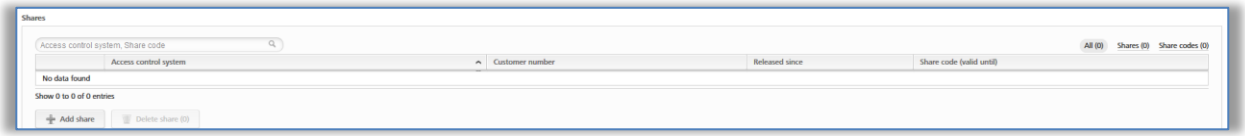
10.1 Dela enheter med andra AirKey-system

Man kan dela en AirKey-enheten flera system. Behörigheter för dessa delade AirKey-enheter kan administreras av respektive systems administratörer. En enhet kan tillhöra max 250 olika AirKey-system.

- På startsidan ***Home*** välj ***Cylindrar*** eller ***Väggläsare***.
- Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.
- Klicka på dörrbeteckningen för den låskomponenter som ska delas.

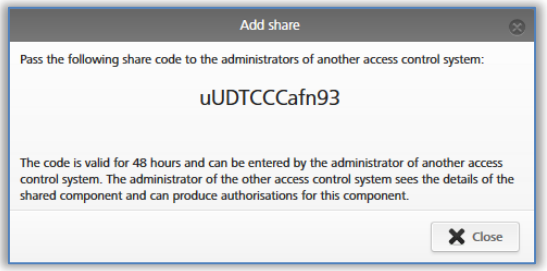
I fliken ***Frisläppt*** i låskomponenter detaljer visas eventuella delningar som redan har utförts.

- Klicka på ***Lägg till***.



Figur 287: Dela AirKey-enheter

- Systemet genererar en 12-teken godkännandekod.



Figur 288: Lägga till delningar

- Meddela administratören i de andra AirKey-systemen om denna delningskod.

Koden gäller i 48 timmar.

Man kan generera flera delningskoden för en AirKey-enhet. Dessa visas i AirKey-enhetens delningslista.

Systemet skapar en post i AirKey-enhetens delningslista. Här visas delningskoden och dess giltighet.

10.2 Lägga till enheter från andra AirKey-system

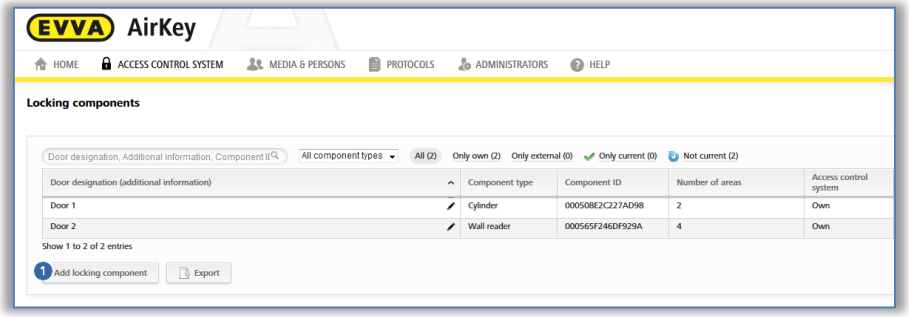
Har en enhet delats från ett system ska man lägga till den i det aktuella AirKey-systemet.

> På startsidan ***Home*** välj ***Lägg till*** i det grå fältet ***Låssystem*** → ***Lägg till låskomponent*** ❶.

Figur 289: Lägga till AirKey-enheter – grått fält

> Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.

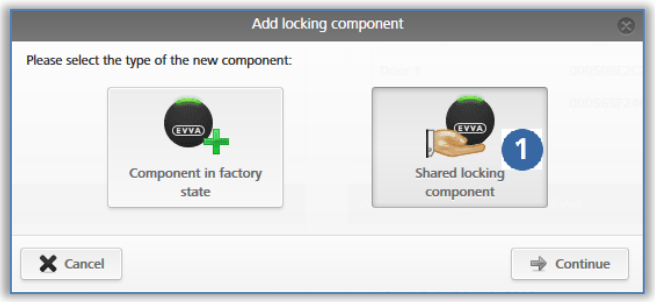
> Klicka på ***Lägg till låskomponent***. ❶



Figur 290: Lägga till AirKey-enheter

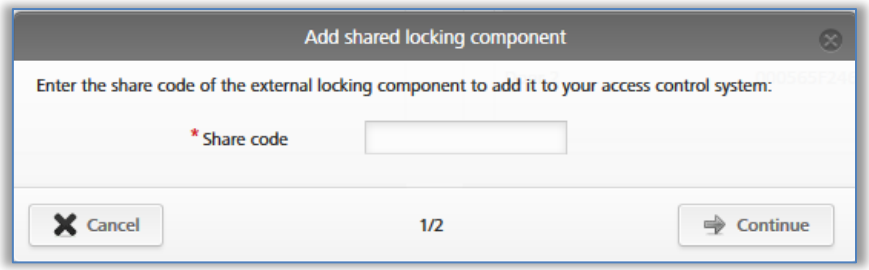
> Välj typen av ***Frigiven låskomponent*** ❶.

> Klicka på ***Fortsätt.***



Figur 291: Lägga till delade låskomponent

> Ange delningskoden från det andra låssystem för att lägga till låskomponenten.

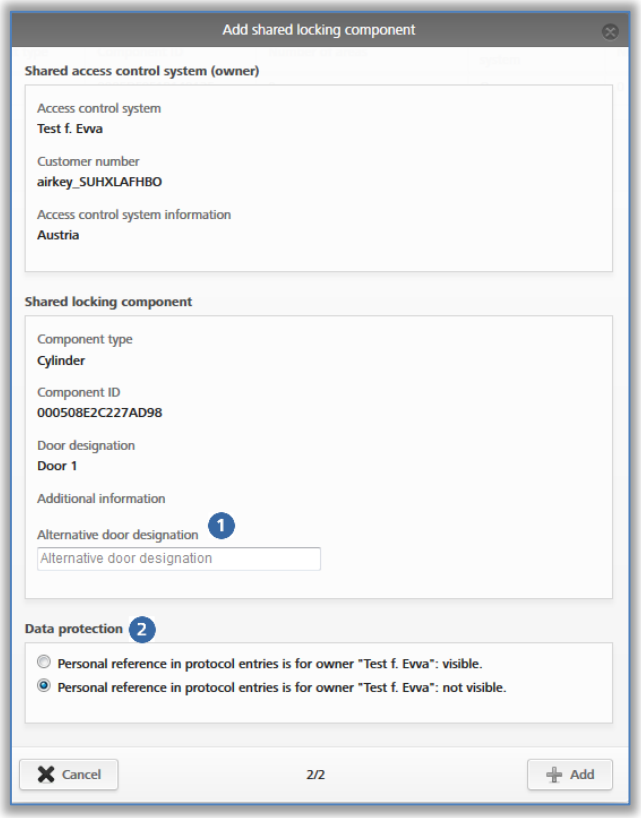


Figur 292: Lägga till delade AirKey-enheter

Är delningskoden är fel visas ett felmeddelande.

När rätt kod angetts är det möjligt att ändra följande inställningar i systemet för enheten:

- Alternativa dörrbeteckningar ❶
- I enlighet med gällande dataskydd kan personliga loggfiler anonymiseras ❷.



Figur 293: Lägga till delade AirKey-enheter

- Systemet skapar en uppdateringsuppgift.
- Uppdatera låskomponenten med en telefon med underhållsbehörighet eller en kodningsstation.
- Detta raderar uppdateringen från listan och delningen bekräftad.
- När den delade enheten är uppdaterad, listas enheten i enhetslistan "Externt". Varje klient som har lagt till enheten kan redigera den alternativa dörrbeteckningen i fliken "Detaljer" och tilldela enheten till ett område. Öppna fliken "Inställningar" för att ändra personliga loggfilen till synlig eller anonym. Loggar med personreferens kan

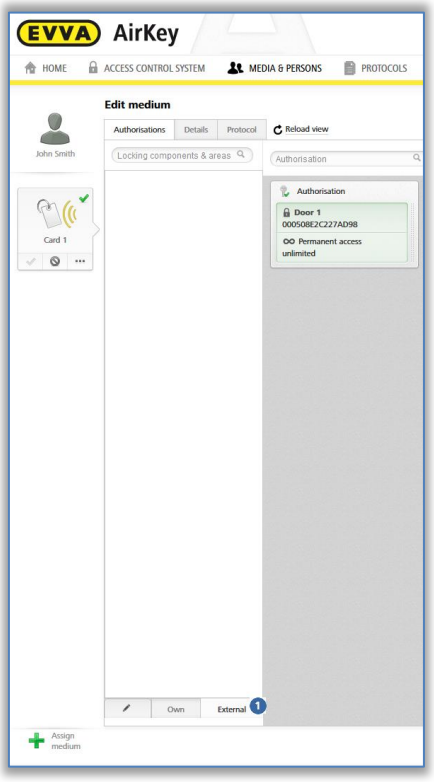
även redigeras i "Händelseloggar och uppdateringar" för det aktuella låssystem. Man kan även tilldela behörigheter för delade låskomponenten.

Externa enheter kan inte delas vidare till andra låssystem.

10.3 Tilldela behörigheter för externa låskomponenten

En extern enhet administreras likt systemets egna enheter. Marginell skillnad på tilldelnings möjligheter. Gör på följande sätt för att ge behörighet till en extern enhet.

- På startsidan ***Home*** välj ***Smarttelefoner*** eller ***Kort***.
- Alternativt välj ***Medier och personer*** → ***Medier*** i huvudmenyn.
- Välj önskat medium i översiktslistan.
- Är mediet tilldelat en person visas en översikt över behörigheterna.
- Välj fliken ***Främmande*** ❶ under fälten för alla låskomponenten och områden för att visa en lista av alla externa enheter.



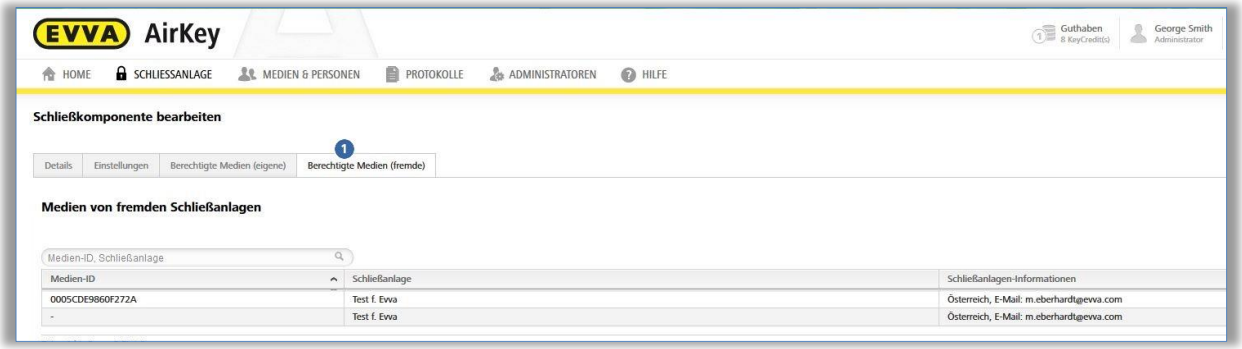
Figur 294: Behörigheter för externa AirKey-enheter

- Drag and Dropp vald, extern enhet till det grå området. Behörighetsvalet visas när enheten eller området har flyttats till det gråa fältet.
- Flytta vald enhet eller område till den behörigheten som erfodras.
- Skapa och spara behörigheten, en KeyCredit dras från kontot. Se kapitlet Skapa behörigheter för mer information om hur du skapar behörigheter. En KeyCredit dras från ditt systems kredit och inte från krediten för det andra AirKey-systemet.

10.4 Visa behörigheter för delade AirKey-enheter

Är en AirKey-enhet delad med ett annat system, ser man det systemets medier med behörighet till den delade enheten.

- På startsidan ***Home*** välj ***Cylindrar*** eller ***Väggläsare***.
- Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.
- Klicka på den AirKey-enhet för vilken ska visas detaljer i översikten.
- Klicka på ***Behöriga medier (extern)*** ❶ här visas en översikt av alla externa medier med behörighet till denna enhet.



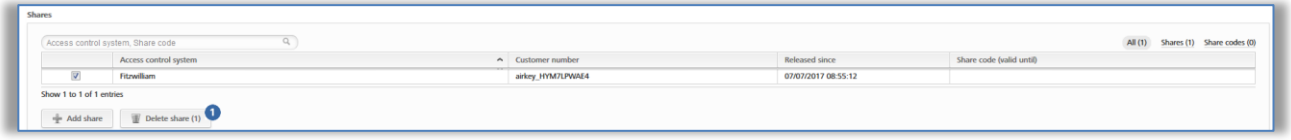
Figur 295: Behöriga medier (externa)

10.5 Återkalla delade AirKey-enheter

Man kan återkalla delade AirKey-enheter. Gör på följande sätt:

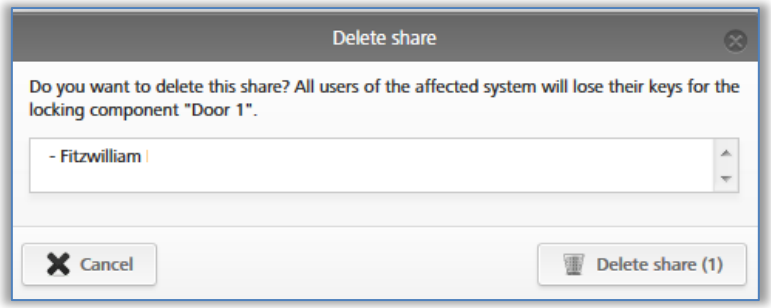
- På *startsidan* ***Home*** välj ***Cylindrar*** eller ***Väggläsare***.
- Alternativt välj ***Låssystem*** → ***Låskomponenter*** i huvudmenyn.
- Välj den AirKey-enhet från översiktslistan för vilken återkallandet gäller.

I fliken ***Detaljer*** i avsnittet ***Frisläppt*** välj respektive delning och klickar på ***Radera tilldelning*** ❶.



Figur 296: Avsnitt "Delningar" – radera delningar

- Klicka på ***Radera tilldelning*** för att bekräfta.



Figur 297: Radera delningar

Resultatet blir att enheten raderas från det andra systemet Systemet skapar en uppdatering för enheten.

> Uppdatera den AirKey-enhet som inte längre ska delas med en telefon med underhållsbehörighet eller en kodningsstation. AirKey-enhetens status är uppdaterad.

Viktigt: Efter denna uppdatering kan det andra systemets medier inte aktivera enheten.

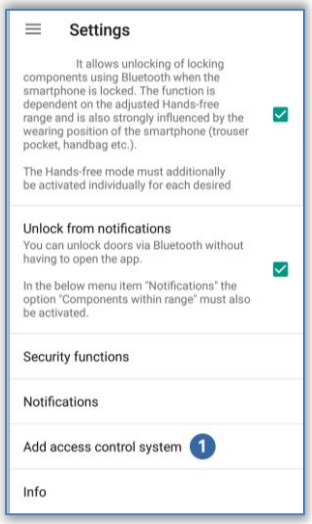
Delade enheter kan endast återtas med det AirKey-system vilket äger enheten.

Man ska inte uppdatera AirKey-enheten om delningskoden inte har använts och den har raderats enligt beskrivningen i detta avsnitt.

10.6 Använd smarttelefonen i flera system

Man kan registrera telefonen för flera AirKey-system och använda den som medium.

> Öppna huvudmenyn för AirKey-appen och välj ***Inställningar*** → ***Lägg till låssystem*** ❶.



Figur 298: Lägga till låssystem

- I Android-telefoner visas dialogen för inmatning av registreringskoden automatiskt. På iOS-telefoner väljer du ***Registreringskod redan mottagen*** för att hoppa över inmatningen av telefonnummer och gå till inmatningen av registreringskoden.
- Ange registreringskoden som erhållits från systemadministratören och välj ***Registrera***.
- Om du har aktiverat en PIN-kod för AirKey-appen måste du ange och bekräfta den.

Telefonen har nu även registrerats i ett annat AirKey-system.

Om registreringskoden för ytterligare ett låssystem har skickats via sms, räcker det att man klickar på länken i meddelandet för att starta och genomföra registreringen automatiskt.

Svep över telefonens skärm för att välja behörighetsöversikter för enskilda AirKey-system eller den allmänna behörighetsöversikten.

Vid behov av extra säkerhet, rekommenderar EVVA att man använder en pinkod även på Appen. Generellt hoppa över denna funktion. Koden erbjuder extra säkerhet och kan aktiveras eller avaktiveras i efterhand. Närmare information hittar du under Aktivera pinkod.

11 AirKey Cloud Interface (API)

AirKey Cloud Interface är ett gränssnitt (API) för tredjepartssystem och bygger på REST. Gränssnittet gör det möjligt att styra vissa funktioner i AirKey via en tredjepartsprogramvara (exempelvis ett boknings- eller incheckningssystem).

Tredjepartsprogramvaran måste då vara ansluten till AirKey-onlineadministrationen och anpassas särskilt så att den kan skicka de kommandon som krävs och sedan bearbeta efterföljande svar.

Omfattningen av de möjliga funktionerna och motsvarande kommandon finns i API-beskrivningen. Den som integrerar eller programmerar tredjepartsprogramvaran ansvarar för implementeringen.

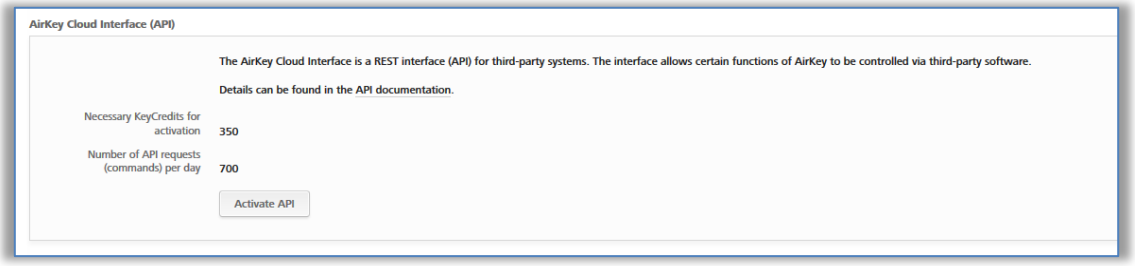
Prova funktionerna hos AirKey Cloud Interface i exempelform med hjälp av EVVA AirKey Cloud Interface Demo.

Se till att du har tillräckligt med KeyCredits när du använder AirKey Cloud Interface. Använd gärna KeyCredits Unlimited. Om krediten är förbrukad eller nästan helt förbrukad informeras alla administratörer av AirKey-låssystemet om detta, via ett e-postmeddelande. E-postmeddelandet skickas endast till administratörer som har aktiverat alternativet ***Jag vill ta emot viktig information från EVVA (t.ex. om lågt KeyCredits-tillgodohavande) via e-post (rekommenderas)***. Dessa e-postaviseringar kan när som helst redigeras (se Redigera administratör).

11.1 Aktivering av AirKey Cloud Interface

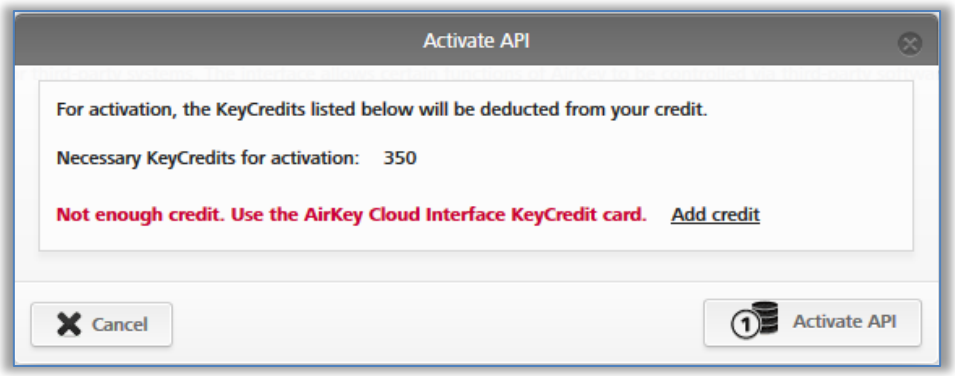
För aktivering av AirKey Cloud Interface krävs minst 350 krediter. Använd din befintliga mängdbaserade kredit av KeyCredits eller motsvarande skrap-kort **KeyCredits AirKey Cloud Interface**.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Aktivera API***.



Figur 299: Allmänna inställningar – AirKey Cloud Interface (API)

> Om det finns tillräckligt med mängdbaserad kredit bekräftar du dialogrutan igen med kommandot ***Aktivera API***. Om krediten inte räcker anges detta med ett meddelande. Då finns det möjlighet att fylla på krediten direkt via en länk.



Figur 300: Aktivera API

Används för att aktivera AirKey Cloud Interface. AirKey Cloud Interface får enbart aktiveras en gång per låssystem för att det ska gå att använda.

Efter aktivering får du information om slutpunkten (dit API-kommandon måste skickas) och om gränsen för API-förfrågningar (antal möjliga API-förfrågningar per dag). Som API-förfrågan räknas ett kommando som skickas till AirKey-systemet via tredjepartsprogramvaran.

Gränsen för API-förfrågningar återställs dagligen klockan 00:00 UTC. Om gränsen för API-förfrågningar överskrids informeras alla administratörer av AirKey-låssystemet om detta via ett e-postmeddelande. E-postmeddelandet skickas endast ut till administratörer som har aktiverat alternativet ***Jag vill ta emot viktig information från EVVA (t.ex. om lågt KeyCredits-tillgodohavande) via e-post (rekommenderas)***. Dessa e-postaviseringar kan när som helst redigeras (se Redigera administratör).

Om API-förfrågningarna för en viss dag inte räcker till för dina användningsändamål är du välkommen att kontakta EVVA-supporten.

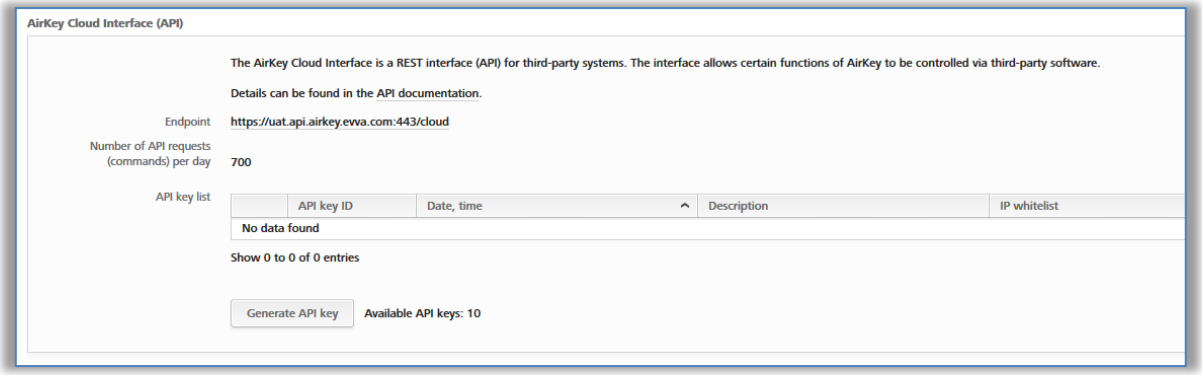
11.2 Generera API-nyckel

Kommunikationen mellan AirKey och tredjepartsprogramvaran skyddas av en API-nyckel. Endast de som känner till denna API-nyckel kan skicka kommandon till låssystemet via AirKey Cloud Interface. Varje låssystem med aktiverat AirKey Cloud-gränssnitt använder egna API-nycklar.

Åtgärder som genomförs via AirKey Cloud Interface loggas även i systemloggen till AirKey-låssystemet. Som administratör används i det här fallet den första delen av API-nyckeln, API-nyckelns ID.

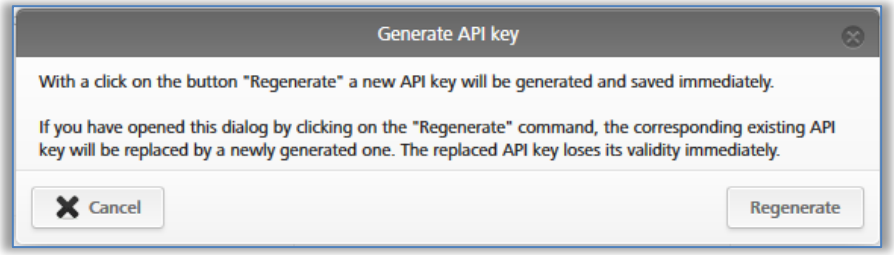
Efter aktiveringen kan du generera de API-nycklar som krävs för kommunikationen.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Generera API-nyckel***.



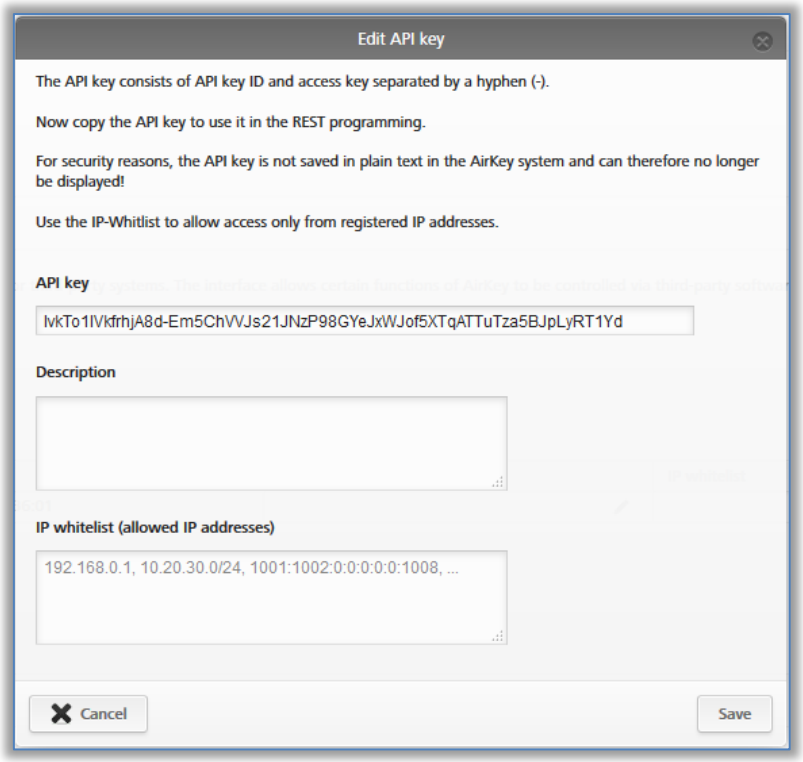
Figur 301: Generera API-nyckel

> Bekräfta dialogen igen med kommandot ***Generera API-nyckel***.



Figur 302: Dialogen Generera API-nyckel

> Ange en beskrivning, till exempel namnet på tredjepartsprogramvaran, och begränsa eventuellt de IP-adresser som är behöriga att skicka API-förfrågningar med hjälp av IP-vitlistan.



Figur 303: Detaljer Generera API-nyckel

Använd funktionen för IP-vitlistning för att höja säkerheten. Ange bara de IP-adresser för respektive API-nyckel som får skicka API-förfrågningar till AirKey-låssystemet.

IP-adresser i formatet IPv4 och IPv6 är tillåtna i IP-vitlistan. Använd ett kommatecken (,) som avgränsningstecken mellan flera olika IP-adresser.

API-nyckeln visas bara i fulltext en gång av säkerhetsskäl. Förvara den på ett säkert ställe och använd den i tredjepartsprogramvaran.

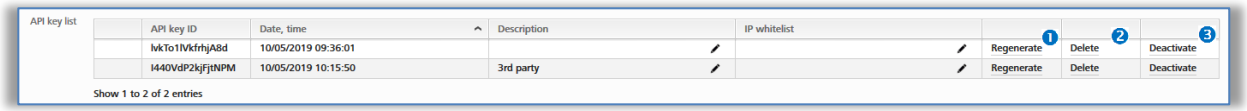
> Spara uppgifterna om API-nyckeln genom att klicka på ***Spara***.

Upp till 10 API-nycklar kan genereras per AirKey-låssystem. Således kan fler än en tredjepartsprogramvara användas för att styra AirKey-låssystemet.

Den genererade API-nyckeln listas i de allmänna inställningarna och kan även redigeras där i efterhand.

11.3 Redigera API-nyckeln

Beskrivningen och IP-vitlistan med befintliga API-nycklar kan sedan redigeras i efterhand bland ***Inställningarna*** på fliken ***Allmänt*** med hjälp av pennsymbolen. Dessutom är funktionerna ***Generera på nytt***, ***Radera***, ***Avaktivera*** respektive ***Återaktivera*** tillgängliga för de enskilda API-nycklarna.



Figur 304: Redigera API-nyckel

11.3.1 Generera API-nyckeln på nytt

En befintlig API-nyckel ersätts med en ny. Den ersatta API-nyckeln upphör då att gälla.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Generera på nytt*** ❶ i listan över API-nycklar.

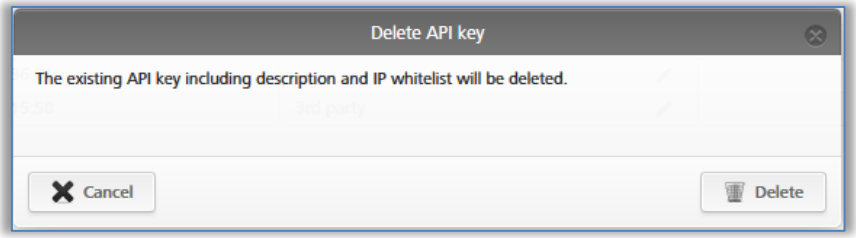
> Alla ytterligare steg är identiska med kommandot Generera API-nyckel.

11.3.2 Ta bort API-nyckel

En befintlig API-nyckel raderas. Den tas bort från listan över API-nycklar och är därmed inte längre giltig. När API-nycklar tas bort ökar antalet tillgängliga API-nycklar på motsvarande sätt.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Ta bort*** ❷ ***i listan över API-nycklar.***

> Bekräfta dialogrutan med kommandot ***Ta bort*** om du vill ta bort API-nyckeln permanent.



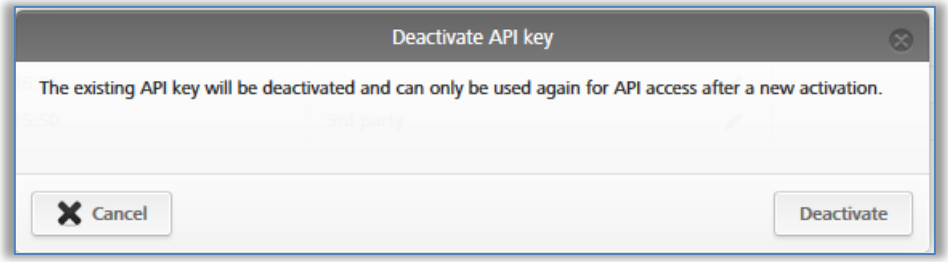
Figur 305: Ta bort API-nyckel

11.3.3 Inaktivera och aktivera API-nyckeln

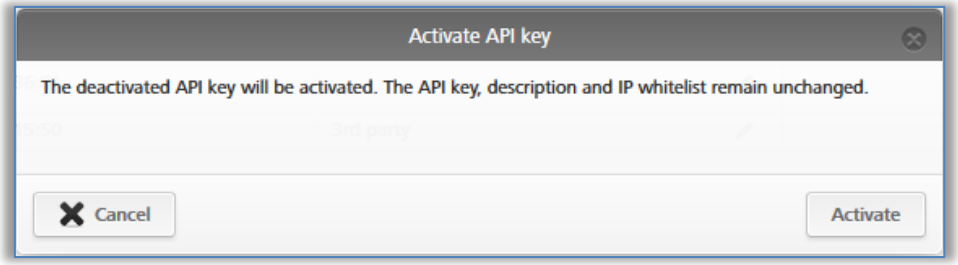
I det här fallet inaktiveras en befintlig aktiv API-nyckel, alternativt aktiveras en inaktiverad API-nyckel igen. Ett inaktiverad API-nyckel är ogiltig och kan inte skicka några API-förfrågningar till AirKey-låssystemet. API-nyckeln samt dess beskrivning och IP-vitlistan ändras inte vid inaktivering respektive aktivering.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Inaktivera*** ❸ respektive ***Aktivera*** i listan över API-nycklar.

> Bekräfta dialogen med ***Inaktivera*** respektive ***Aktivera*** och slutför processen.



Figur 306: Inaktivera API-nyckel



Figur 307: Aktivera API-nyckel

11.4 AirKey Cloud-gränssnitt – testmiljö

I testmiljön får du möjlighet att testa AirKey Cloud Interface (API) med testdata i en skyddad miljö före aktiveringen.
Denna funktion är främst avsedd att underlätta för de som integrerar och programmerar tredjepartssystem som en del av integreringen av AirKey Cloud Interface. Testmiljön är även tillgänglig när AirKey Cloud Interface ännu inte har aktiverats.

I testmiljön förbrukas inga KeyCredits-krediter. Dessutom skickas inga SMS via testmiljön.

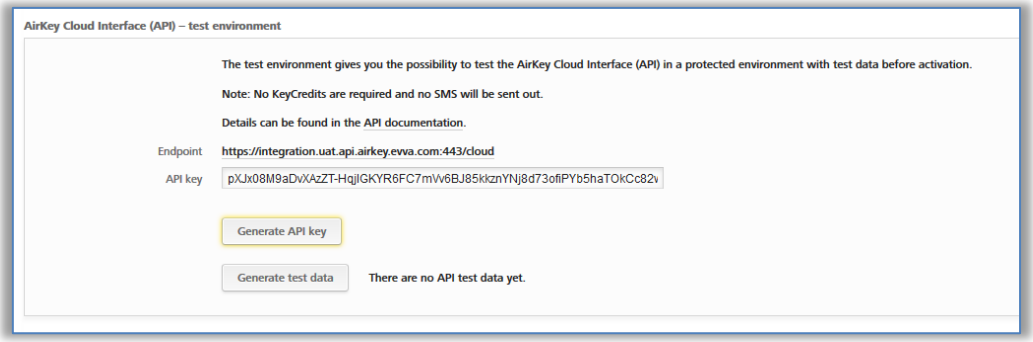
Testmiljön för Airkey Cloud Interface (API) är tillgänglig via en egen slutpunkt (som API-kommandona ska skickas till).
Slutpunkt ("Endpoint"): https://integration.api.airkey.evva.com:443/cloud

11.4.1 Generera testdata

Testdata måste genereras innan testmiljön används för första gången.

För att generera testdata måste en API-nyckel först genereras.

> Gå till ***Inställningar*** på fliken ***Allmänt*** och klicka på ***Generera testdata***.



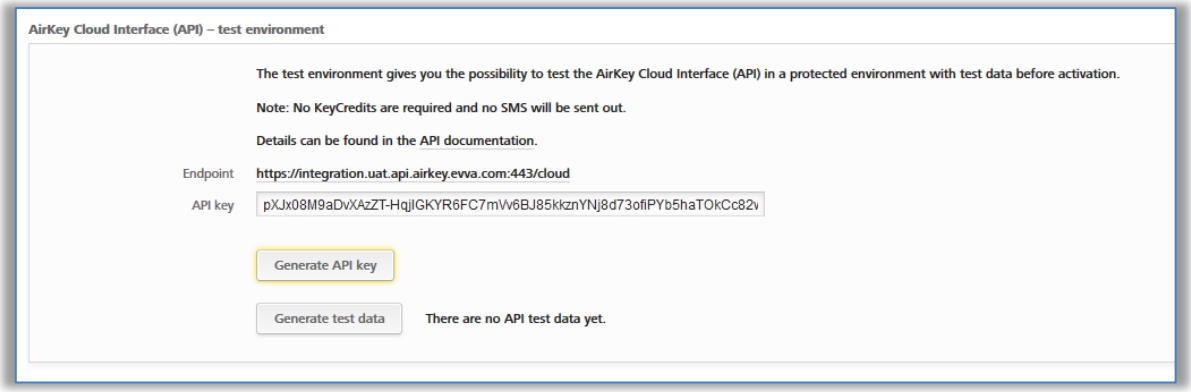
Figur 308: Generera testdata

Testdata genereras nu. Med hjälp av testdata blir det möjligt att prova varje API-förfrågan från API-dokumentationen. Testdata får enbart genereras en gång.

11.4.2 Generera API-nyckel

Dessutom krävs en API-nyckel för kommunikationen med Airkey Cloud Interface (API) – testmiljö. Utan en sådan API-nyckel kan inga API-förfrågningar skickas till testmiljön. Jämfört med det riktiga AirKey Cloud Interface visas API-nyckeln för testmiljön i fulltext.

> Gå till ***Inställningar*** på fliken ***Allmänt*** i området ***AirKey Cloud Interface (API) – testmiljö*** och klicka på ***Generera API-nyckel.***



Figur 309: Generera testmiljö för API-nyckel

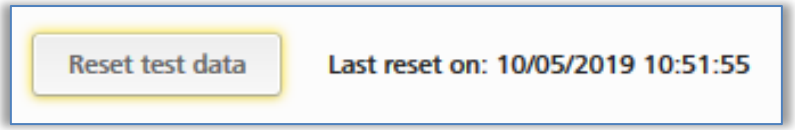
Om du klickar igen på ***Generera API-nyckel*** ersätts den befintliga API-nyckeln med en ny. Den ersatta API-nyckeln kan då inte längre användas.

Efter varje inloggning måste en API-nyckel genereras på nytt.

11.4.3 Återställa testdata

Testdata för AirKey Cloud Interface-gränssnittet – testmiljö kan återställas till det ursprungliga läget med ett klick. På så sätt kan samtliga test genomföras med samma testdata.

> Gå till ***Inställningar*** på fliken ***Allmänt*** i området ***AirKey Cloud Interface (API) – testmiljö*** och klicka på ***Återställ testdata***.



Figur 310: Återställ testdata för testmiljön

Återställningen av testdata bekräftas med motsvarande meddelande. Tidpunkten för den senaste återställningen visas i avsnittet ***Airkey Cloud -gränssnittet (API) – testmiljö***.

12 Låskomponenternas signaler

AirKey-enheter indikerar händelser med en rad olika visuella och akustiska signaler.

Signal-nummer	Händelse	Visuell signal*)	Ljudsignal*)	Obs
Signal 1	Aktivering med behörigt medium	●●●●●	mmmmm	
Signal 2	Aktivering avslutad	●●●●●	lllll	
Signal 3	Försök till aktivering med obehörigt medium	●●-●●-●●-●●	hh-hh-hh-hh	
Signal 7	Varning "Batteri tomt" (Visas i AirKey-onlineadministrationen i listan för enheter och i detaljerna för en enhet med symbolen "Tomt batteri".)	●●--●●--●●--●●	h----h----h----h	Signalen avges vid införande av tomma batterier istället för signal 8 och vid aktivering före signal 1. 1000 aktiveringar eller två veckors standby tid garanteras efter första indikationen (beroende på rumstemperatur och vid användande av kort, taggar, armband eller combi nycklar).
Signal 8	Isättning av nya batterier eller omstart	●●--●●--●●	ll--mm--hh	
Signal 9	Medium utan EVVA-segmentering; externt medium	●●●	Ingen	Används inte längre. För detta ändamål används endast signal 3.
Signal 10	Kommunikationsfel eller hårdvarufel	●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●	mmm--- mmm--- mmm--- mmm--- mmm--- mmm--- mmm--- mmm--- mmm--- mmm	Indikerar till exempel en felaktig anslutning mellan cylinder och elektronikmodul.

Signal-nummer	Händelse	Visuell signal*)	Ljudsignal*)	Obs
Signal 11	Firmware uppdatering	●-●-●-●-●... (1 s-intervall, 12 ms-impuls)	Ingen	Varaktighet: tills kommunikation är slutförd.
Signal 12	Uppdatering av enhet / medium lyckad	●●-●●	hhhhh	
Signal 13	Uppdatering av enhet / medium misslyckades	●●-●●	lllll	
Signal 14	Läser AirKey-medium	●-●-●-●-●-●... (100 ms-intervall, 10 ms-impuls)	Ingen	Varaktighet: tills kommunikation är slutförd.
Signal 15	Aktivera AirKey cylinderns bluetothfunktion genom beröring av cylinderns svarta läsarhuvudet	●-●-●-●-●... (1,5 s intervall)	Ingen	
Signal 16	Kontorsläge startad	●●●---●●●	mmm---hhh	
Signal 17	Kontorsläge avslutat	●●●---●●●	hhh---mmm	
Signal 18	Batterinödläge för en AirKey-cylinder	●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●● ●●--●●--●●--●●	h----h----h----h mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm h----h----h----h mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm ll--mm--hh h----h----h----h	Orsak: Ett av batterierna har satts i på fel sätt eller är förbrukat.

*) Beskrivning av signaler:

Visuella signaler: gul ●, röd ●, grön ●, blå ●

Akustiska signaler: h = hög ton, m = medelhög ton, l = låg ton

Varje signal motsvarar en period på 50 ms, pauser indikeras med "-".

13 Värden och begränsningar för AirKey

I detta avsnitt beskrivs det högsta antalet konfigureringar per medium och AirKey-enhet.

13.1 AirKey-onlineadministration

Antal AirKey-enheter, områden, personer och medier är obegränsat.

13.2 AirKey-enheter

- De senaste 1 000 posterna i loggen sparas.
- Max 1 000 poster i black list kan hanteras.
- Max 96 områden kan tilldelas.
- Max 250 delningar med fler system kan tilldelas.

13.3 Kort, nyckelbrickor, armband eller kombinycklar

- Högst 256 poster i loggen sparas.
- Max 150 behörigheter kan tilldelas till enskilda enheter.
- Max 100 behörigheter kan tilldelas till områden (om du tilldelar 12 enskilda behörigheter med 8 möjliga områden vardera, kan du endast tilldela totalt 96 behörigheter till områden).

13.4 AirKey-app

- Max 256 poster i loggen sparas.
- Obegränsat antal behörigheter för enskilda dörrar och områden.

14 När dras KeyCredits från?

Det behövs KeyCredits för att hantera AirKey-systemet, till exempel för att tilldela eller ändra behörigheter.

KeyCredits dras endast vid mängdbaserade krediter. Är det en tidsbaserad kredit gäller tids axeln.

KeyCredits dras från i följande fall:

- Tilldelning och aktivering av nya behörigheter.
- Ändring och aktivering av befintliga behörigheter.
- Återaktivering av avaktiverade medier, under förutsättning att behörigheterna hos det avaktiverade mediet ska bibehållas.
- Vid aktivering av AirKey Cloud-gränssnittet (API).

KeyCredits för nya behörigheter eller ändringar på behörigheter dras endast från när mediet har skapats och aktiveras. I denna process dras en KeyCredit från för varje behörighet som skapas. Man kan även aktivera eller ändra flera behörigheter på samma gång – i så fall dras endast en KeyCredit.

Inga KeyCredits dras från vid radering av behörigheter eller avaktivering av medier.

15 Felsökning

AirKey är ett testat elektroniskt tillträdeskontrollsystem av högsta kvalitet. Uppstår problem med systemet sök i detta avsnitt.

15.1 Ingen kommunikation inom systemet

Gör på följande sätt när man inte kan registrera telefonen eller inte kan uppdatera AirKey-enheter:

- Kontrollera internetanslutningen på telefonen (WLAN eller mobil- data) och aktivera.
- Kontrollera om portarna 443 är aktiverade i din IT-infrastruktur. Dessa portar krävs för kommunikation med AirKey-systemet. Se kapitlet Systemkrav.

15.2 AirKey-enheten har problem med att identifiera eller kan inte detektera medier

Gör på följande sätt om det är svårare än vanligt eller omöjligt att identifiera vissa medier vid enheter:

- Håll mediet stadigt mot läsarenheten under identifiering och vänta tills enheten lyser grönt. (Blått ljus indikerar kommunikation mellan mediet och enheten).
- Om AirKey-enheten inte reagerar korrekt kontrollera att mediet är rätt placerat. Kombinyckeln måste hållas mot enheten med den sida som är försedd med RFID-symbolen.
- Fungerar det ändå inte avlägsna mediet från enheten och vänta ca 1 min innan man prövar igen. Enheten omkalibrerar det elektriska fältet. Man kan omkalibrera fältet manuellt genom att hålla ett metallobjekt mot läsarenheten.

15.3 Medier identifieras inte längre

Gör på följande sätt om vissa medier inte längre kan identifieras vid AirKey-enheten:

- När det gäller telefonen kontrollera att NFC eller Bluetooth är aktiverat. Starta om aktuell funktion och placera telefonen korrekt mot enheten. Observera att olika telefoner kan skilja sig åt beroende på modell.
- Skulle läsaren på enheten eller kodningsstationen inte reagera på mediet, håll mediet mot läsaren på enheten eller kodningsstationen i 10 sekunder. Detta triggar en självrepareringsprocess på mediet. Man märker att processen är slutförd när enheten eller kodningsstationen avger de vanliga signalerna.

15.4 Det går inte att demontera vredknoppen på en AirKey-cylinder

Gör på följande sätt:

- Använd monteringsverktyget för AirKey-cylindern.
- Cylindern har ett servicehål på framsidan av cylinderkroppen som används för att spärra cylindertappen med hjälp av ett special verktyg. Använd verktygssats 2.

Tillvägagångssätt:

- För in metallpinnen från verktygssats 2 i det främre servicehålet på cylindern.
- Vrid vredet tills man känner att verktyget glider djupare ner i hålet. Håll kvar verktyget i denna position och demontera vredet som vanligt med hjälp av monteringsverktyget.
- Avlägsna verktyget när vredkoppen är demonterad.
- Man kan även hålla ett behörigt medium mot läsaren och aktivera cylindern. Snäpp ihopp monteringsverktyget på cylindern medan den är aktiverad. Cylindern kopplar då inte längre ur och vredknoppen kan lättare demonteras.

15.5 AirKey-enheten indikerar "hårdvarufel"

Indikerar AirKey-enheten ett hårdvarufel (se kapitlet Låskomponenternas signaler) kan det hända att vredetknoppen / läsaren inte har kontakt med elektroniken i cylinderhuset. Kontrollera kontakter, anslutningar och kopplingar enligt monteringsanvisningen.

15.5.1 AirKey-cylindrar

- Se till att tätningen har placerats korrekt på cylinderaxeln och sätt tillbaka vredeknoppen på cylindern genom att vrida den medurs tills man känner ett motstånd.
- Ta bort monteringsverktyget.
- Vrid sedan vredknoppen moturs tills du känner att den hakar fast.
- Se till att vredknoppen med elektronikmodulen sitter fast ordentligt.

15.5.2 AirKey-väggläsare

- Se till att läsar- och kontrollenheten på AirKey-väggläsaren har anslutits korrekt. Kontrollera kablar och anslutningar.

15.6 Vredknoppen är svår att manövrera

Beroende på montaget av cylinderbehöret kan cylindern vara svår att manövrera eftersom tätningen kan ge upphov till friktion mellan cylinderhus och vredknoppen. Tätningen kan tas bort vid installation inomhus.

För hjälp eller support kontakta din EVVA-partner (EVVA-support).

16 Viktig information

16.1 System

Observera att AirKey-systemet kan omfattas av krav på rapportering / godkännande beroende på gällande lagstiftning, i synnerhet i fråga om dataskydd. EVVA Sicherheitstechnologie GmbH ansvarar inte och garanterar därför inte att systemet arbetar i enlighet med gällande bestämmelser.

Internetportar 443 and 7070 används för kommunikation med AirKey-systemet. Se till att dessa portar inte är avaktiverade. Om du använder ett mobilt datanätverk ansvarar operatören för hantering av portarna. Kontakta din mobiloperatör om du upplever problem när du använder mobila datanätverk i kombination med AirKey.

Tilldela behörigheter med så korta giltighetstider som möjligt för att upprätthålla en hög systemsäkerhetsnivå och hålla black list så liten som möjligt om medier tappas bort. Nödmedier (t.ex. brandkårsnycklar) ska endast skapas med behörigheter som inte går ut.

Arbeta alltid med den senaste övergripande systemkonfigurationen för att upprätthålla en hög systemsäkerhetsnivå.

Följande länkar innehåller säkerhetsinformation om enskilda system:

Cylindrar, hänglås: PDF

Väggläsare, styrenheter: PDF

Standarder och riktlinjer

CE-testad | EN 1634: 30 minuter | EN 1634: 90 minuter | IP65-klassning | EN 15684 | Lämpar sig för lås enligt EN 179/1125 (vid användning av antipanikfunktionen FAP)

SKG | VdS[1]

[1] Under utveckling

17 Försäkran om överensstämmelse

EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA access to security

EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59–65 | A-1120 Wien

EU - KONFORMITÄTSERKLÄRUNG

EVVA Sicherheitstechnologie GmbH, eine Gesellschaft mit beschränkter Haftung mit Sitz in Wien, Österreich, bestätigt hiermit, dass folgende Produkte den nachstehend genannten Richtlinien entsprechen:

AIRKEY

AirKey-Zylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridzylinder	E.A/[System].PZ
AirKey-Hangschloss	E.A.HA.
AirKey-Wandleser	E.A.WL.
AirKey-Steuereinheit	E.A.WL.CU.
AirKey-Notstromgerät	E.ZU.NG.V1

Hersteller: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Wien
Österreich

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt der Hersteller. Gegenstand der Erklärung sind alle seriengefertigten Produkte ab dem Ausstellungsdatum dieser Erklärung. Der oben beschriebene Gegenstand der Erklärung erfüllt die einschlägigen Harmonisierungsvorschriften der Union:

- Richtlinie 2014/53/EU („Funkanlagen Richtlinie")
- Richtlinie ROHS 2011/65/EU in der Fassung von 2014/76/EU

Angewandte harmonisierte Normen:

- EN 62368-1:2014 bzw. IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

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

18 Declaration of Conformity

EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA
access to security

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

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

19 Lista över figurer

20 Definitioner

Följande termer används i samband med AirKey:

Beteckning	Funktion
Klient	Ägare av AirKey-systemet med ett unikt kundnummer.
Administratör	Behöriga administratörer i AirKey-systemet för AirKey-onlineadministration. Det går att skapa flera administratörer i samma system. Minst en huvud administratör ska finnas för varje AirKey-system.
Användare (personer)	Användarens medier. Användare tilldelas ett medie som får behörigheter till enheter eller områden.
Medier	Smarttelefoner eller tillträdesmedier som kan läggas till i AirKey-systemet för att aktivera AirKey-enheter.
Tillträdesmedier	Är passiva NFC-medier (utan egen strömförsörjning) som kan aktivera AirKey-enheter utöver smarttelefoner. Hit räknas olika typer av kort, taggar, kombinycklar, armband etc.
Låskomponenter	AirKey-enheter finns i många utföranden för att passa olika användnings-områden.
Områden	En administrativ funktion i AirKey-administrationen där man kan lägga flera låskomponenter till ett område. Områden underlättar administrationen av behörigheter i AirKey-systemet och tilldelningen för olika enheter.
KeyCredits	Beskriver funktionen KeyCredit i AirKey-systemet. KeyCredits krävs för att administrera nya behörigheter, ändra befintliga behörigheter samt för att aktivera andra funktioner i AirKey-systemet.
AirKey Cloud Interface	AirKey Cloud Interface är ett gränssnitt (API) för tredjepartssystem baserat på REST. Gränssnittet gör det möjligt att styra vissa funktioner i AirKey via en tredjepartsprogramvara.
Send a Key	Beskriver en funktion i AirKey-onlineadministrationen. En administratör kan använda den här funktionen för att snabbt skapa nya smarttelefoner och behörigheter, samt för att redigera befintliga behörigheter för smart-telefoner. Användaren av smarttelefonen får ett SMS, och via SMS:et registreras smarttelefon automatiskt för AirKey.
Tvåfaktorsautentisering	Tvåfaktorsautentiseringen, eller 2FA som den också kallas, fungerar som ett extra säkerhetssteg vid inloggning till AirKey-onlineadministrationen. Förutom användar-ID och lösenordet begärs dessutom en SMS-kod under inloggningen som en andra faktor.

Firmware	Mjukvaran i enheterna för att AirKey-funktionerna ska kunna användas. Firmware (mjukvaran) i enheterna kan uppdateras med specifika Firmware uppdateringar som laddas ner från Onlineadministrationen
Keyring	I AirKey-systemet är "Keyring" namnet på den firmware som lagrar AirKey-relevanta uppgifter som finns sparade på passiva tillträdesmedier såsom kort, taggar, kombinycklar och armband. Om det finns en ny Keyring-version i AirKey-systemet kan medierna uppdateras med en smarttelefon med underhållsbehörighet eller med en kodstation.
Underhållsåt-gärder / Uppdateringar	Visas i AirKey-onlineadministrationen för enheter som behöver uppdateras. Först när alla underhållsåtgärder för ett AirKey-låssystem har slutförts är systemet uppdaterat och säkert.
Underhållsbe-hörighet / Uppdateringsbe-hörighet	Smarttelefonen kan användas för att lägga till eller ta bort enheter (medier och låskomponenter) i AirKey-systemet om den har underhållsbehörighet. Servicetekniker kan uppdatera låskomponenter i fabriksläge med en smart-telefon som har underhållsbehörighet. Aktivera underhållsbehörigheten för önskad smarttelefon i AirKey-online-administration.

21 Rättslig information

6:e utgåvan, juni 2022

När den nya systemhandboken ges ut upphör den här versionen att gälla.
Ladda ned den senaste versionen av systemhandboken på vår webbplats:
https://www.evva.com/sv/airkey/systemmanual/.

Systemhandboken kan innehåller felaktigheter och tryckfel. Uppgifterna i handboken revideras och korrigeras dock med jämna mellanrum. Vi ansvarar inte för tekniska fel eller tryckfel och deras potentiella konsekvenser.

Vi förbehåller oss rätten till varumärken och industriella äganderätter.

Vi förbehåller oss rätten att genomföra anpassningar och uppdateringen utan föregående meddelande.

Rättslig information

Utgivare
EVVA Sicherheitstechnologie GmbH

Ansvarig för innehållet
EVVA Sicherheitstechnologie GmbH

Tekniskt innehåll
Florian Diener, Johannes Ullmann

Teknisk rådgivare
Raphael Fasching, Iulian Stanciulescu, Martin Bauer