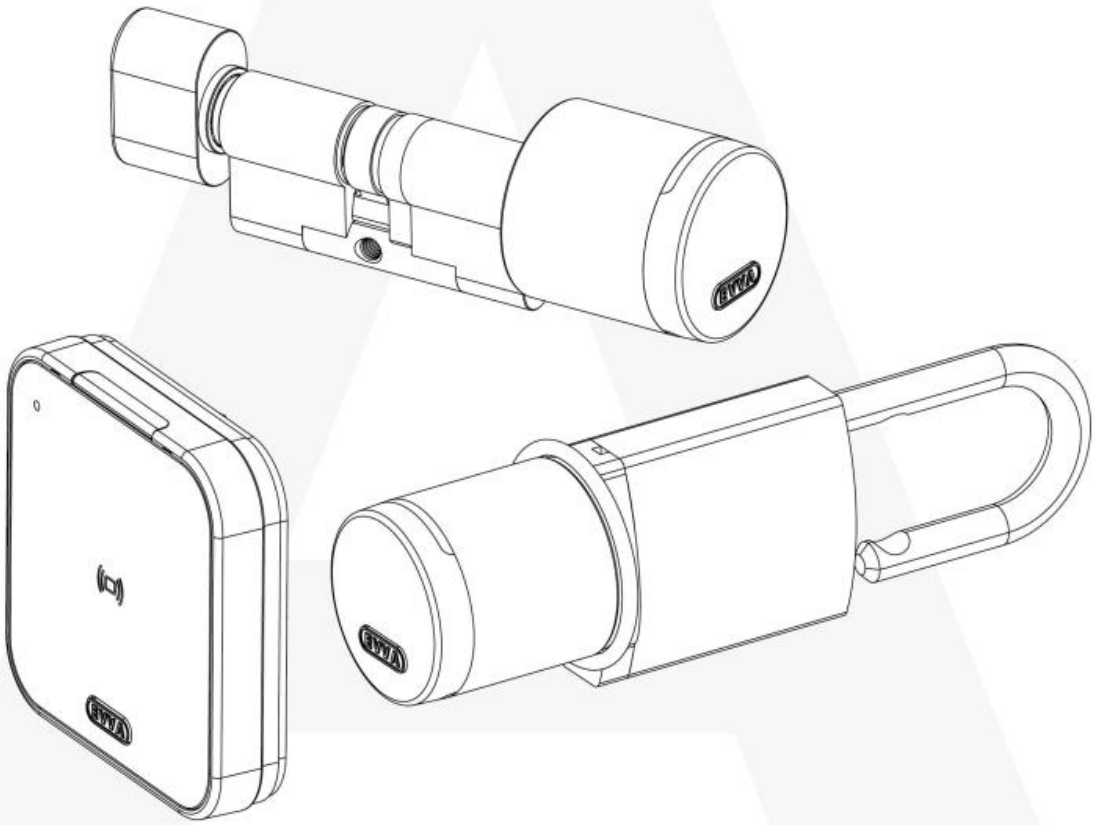


AirKey

Manual del sistema 2.7

1 Índice de contenidos

2 Introducción, vista general

Este manual de sistema de AirKey contiene información sobre la instalación, funcionamiento y uso del sistema de control electrónico de AirKey, que consiste en la Administración online de AirKey, app, cilindros, lectores murales, candados y medios para sistemas AirKey.

Los productos y software de usuario descritos en el manual de sistema de AirKey "Administración online de AirKey" solo pueden ser utilizados por personal cualificado para la tarea pertinente. Gracias a un amplio conocimiento técnico, el personal cualificado está preparado para reconocer y asimismo evitar los posibles riesgos asociados al uso de estos productos o sistemas.

2.1 Aviso legal

- EVVA firma el contrato para el uso de AirKey exclusivamente en base a sus Términos y condiciones generales así como a sus las Condiciones generales de licencia por lo que respecta al software relacionado con el producto.
- En este sentido, se advierte expresamente al comprador que el uso del sistema de control de accesos objeto del contrato puede conllevar obligaciones legales, en particular obligaciones de autorización, comunicación y registro relacionados con las leyes de protección de datos (p. ej. un sistema unificado de información), así como derechos de gestión conjunta del personal si se usa en una empresa. El comprador o clientes y el usuario final serán los responsables de que el producto se use conforme a la ley.
- Conforme a la responsabilidad del fabricante respecto a sus productos tal y como se define en la ley de responsabilidad de productos, deberá tenerse en cuenta la información citada anteriormente, que deberá trasladarse a la empresa donde se encuentre el sistema y al usuario. El no cumplimiento exime a EVVA de responsabilidad civil.
- No resulta adecuado para su uso cerca de niños menores de 36 meses, debido al riesgo de asfixia que conllevan las piezas de reducido tamaño que pueden tragarse.
- No deben llevarse a cabo usos no conformes a lo acordado o no habituales, trabajos de reparación o modificaciones no autorizados expresamente por EVVA, ni reparaciones o mantenimiento no realizados por profesionales, ya que pueden causar averías. Cualquier modificación no autorizada expresamente por EVVA conlleva la pérdida de derechos por responsabilidad, garantía, etc.
- Se ruega a los arquitectos y consultores que soliciten toda la información del producto necesaria a EVVA para poder cumplir con los deberes de información e instrucción conforme a la ley de responsabilidad de productos. Los vendedores autorizados y los contratistas deben tener en cuenta las indicaciones que aparecen en la documentación de EVVA, y transmitirlas a sus clientes de ser necesario.
- En el momento de proyectar e instalar el componentes de cierre, tenga en cuenta las disposiciones internacionales y nacionales correspondientes (leyes, reglamentos, normas y directrices), en particular aquellas referentes a los requisitos aplicables a las rutas de evacuación y las salidas de emergencia.

2.2 Soporte técnico de EVVA

Con AirKey, dispone de un sistema de control de accesos comprobado y verificado. En caso de necesitar soporte, diríjase a su distribuidor de EVVA.

Encontrará una lista de distribuidores de EVVA certificados en nuestra página web https://www.evva.com/int-en/aboutus/contact/international/.

Si selecciona la pestaña "Distributors", encontrará los distribuidores de sistemas de cierre mecánico y electrónico de EVVA con la certificación correspondiente.

Para consultas de asistencia concretas, utilice el formulario online de EVVA. El formulario online está disponible siempre para las continuars situaciones:

- Ha sobrepasado el límite máximo de entrada de códigos de crédito incorrectos.
- No se puede cargar el crédito.
- Página de inicio de sesión de la Administración online de AirKey no disponible.
- No se puede iniciar sesión. Ha olvidado el nombre de usuario y/o dirección de e-mail.
- Ha activado la autentificación de dos factores y no tiene acceso a su número de teléfono.

Encontrará el formulario online accediendo al continuar vínculo: https://www.evva.com/es/airkey/support/.

Encontrará información general de AirKey en nuestra página web https://www.evva.com/es/airkey/website/.

2.3 Explicación de los símbolos

Las secuencias de órdenes, órdenes individuales o botones están representados en este manual de sistema de la continuar manera.

Ejemplo: Menú principal ***Medios y personas*** → ***Crear persona*** o botones como, p. ej., ***Guardar***.

Atención, riesgo de daños a la propiedad si no se respetan las precauciones adecuadas.

Notas e información adicional

Consejos y recomendaciones

Mensajes de error

Option Opciones

2.4 Consejos para una navegación óptima en este documento

En este documento también hay muchos enlaces internos que llevan a otros capítulos o puntos de texto. La forma más rápida y cómoda de volver a la posición original en Windows o avanzar es con estas **combinaciones de teclas**:

Alt + ◀ (Alt + flecha hacia la izquierda del cursor) = navegar hacia atrás

Alt + ▶ (Alt + flecha hacia la derecha del cursor) = navegar hacia delante

Estas combinaciones de teclas funcionan en muchos visores de PDF y, por ejemplo, en Microsoft Word.

Para probar las combinaciones de teclas, haga clic en este enlace y vuelva atrás con Alt + ◀ .

3 Arquitectura de sistema

La figura continuar muestra la visión general de los componentes de cierre y sus vías de comunicación utilizadas con la tecnología de AirKey. Cada componente se describe a continuación.

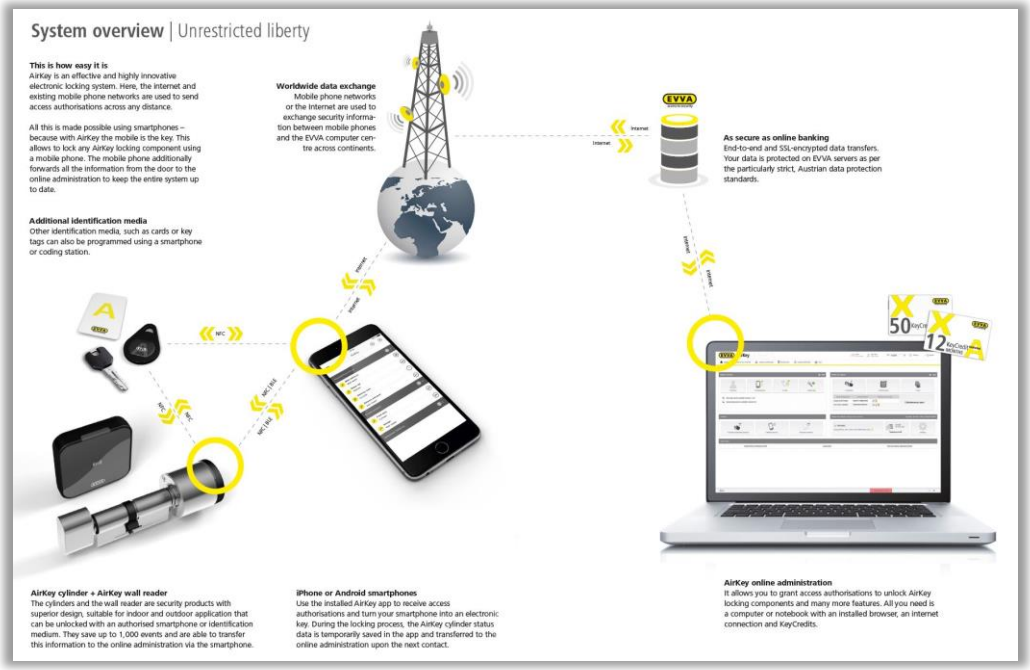


Figura 1: Arquitectura de sistema

Todos los datos se transmiten de forma segura de punto a punto conforme a los estándares actuales de cifrado, desde el centro de datos de EVVA hasta el componentes de cierre antes del descifrado.

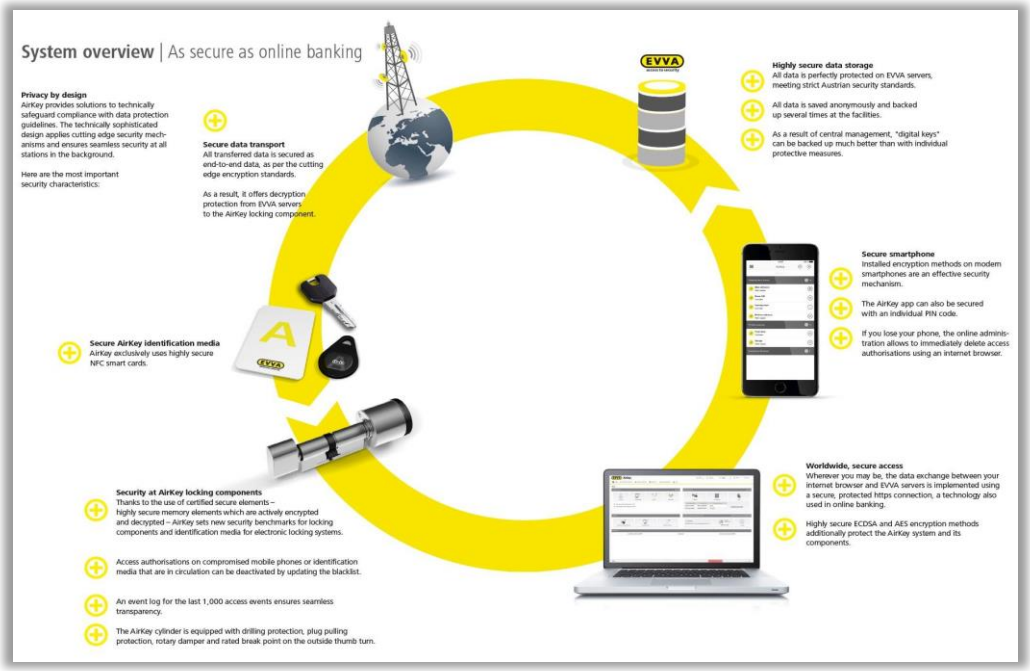


Figura 2: Visión general del sistema – Seguridad integral

3.1 Componentes de cierre

Los componentes de cierre (cilindros y lectores murales de AirKey) regulan los accesos en las puertas. Según las autorizaciones, se produce la activación o denegación en el componentes de cierre.

3.1.1 Cilindros de AirKey

El cilindro AirKey es un componentes de cierre que funciona con pilas. Es apto tanto para uso interior como exterior. De acuerdo con los requisitos específicos, el cilindro de AirKey también se puede utilizar en zonas relevantes para la seguridad. El cilindro de AirKey está protegido mecánicamente contra el vandalismo y la manipulación. El cilindro de AirKey es apto para el uso en puertas antiincendio y vías de escape teniendo en cuenta los requisitos normativos*.

El cilindro de AirKey está disponible como medio o doble cilindro. El doble cilindro está disponible para acceso por un único lado o por ambos lados (doble acceso). En el modelo con acceso por un único lado, solo se comprobará electrónicamente la autorización en el lado exterior; en el modelo con doble acceso, por ambos lados. El pomo electrónico del lado de la identificación gira libremente cuando no se está autorizado. La tapa de plástico negro del cilindro de AirKey sirve como una unidad de lectura.

Si se presenta un medio autorizado junto al pomo, el cilindro se acopla por un tiempo limitado y permite accionar la cerradura mediante el giro del pomo electrónico. Tenga en cuenta las indicaciones que figuran en Utilización de los componentes de cierre.

Tenga en cuenta que, una vez cerrada la puerta, no se cerrará automáticamente. La puerta debe cerrarse manualmente o mediante un dispositivo adicional.

Compruebe que el cilindro de AirKey seleccionado es apropiado para el uso previsto. El cilindro de AirKey está disponible en diferentes formas y configuraciones.

Las fichas técnicas de montaje están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

El cilindro de AirKey presenta dos tipos de señalización: óptica y acústica. Encontrará el significado de las diferentes señales en Señalización de los componentes de cierre.

Para el montaje del cilindro de AirKey, siga las instrucciones de montaje que vienen en la caja, o el vídeo de montaje que se encuentra en https://www.evva.com/es/airkey/website/.

*Para el uso en puertas antiincendio y antipánico, puede requerirse, según la cerradura de embutir utilizada, la función antipánico FAP. Tenga en cuenta la información o certificados proporcionados por los fabricantes de cerraduras, así como el código de producto del pedido.

3.1.2 Cilindro híbrido de AirKey

El cilindro híbrido de AirKey posee las mismas propiedades que el cilindro de AirKey. Es apto tanto para uso interior como exterior, así como para su empleo en zonas en las que la seguridad es de gran relevancia.

En comparación con el cilindro doble de AirKey con acceso por un lado, en el caso del cilindro híbrido de AirKey, en su interior, en lugar del pomo mecánico, encontramos un módulo de llave. Se accede desde fuera mediante una comprobación electrónica de autorizaciones y desde dentro, mediante una llave mecánica.

Tenga en cuenta que, una vez cerrada la puerta, no se cerrará automáticamente. La puerta debe cerrarse manualmente o mediante un dispositivo adicional.

Compruebe que el cilindro híbrido de AirKey es apropiado para el uso previsto.

Las fichas técnicas de montaje están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

El cilindro híbrido de AirKey presenta dos tipos de señalización: óptica y acústica. Encontrará el significado de las diferentes señales en Señalización de los componentes de cierre.

Para el montaje del cilindro híbrido de AirKey, siga las instrucciones de montaje que vienen en la caja.

3.1.3 Cilindro de buzón de AirKey

El cilindro de buzón de AirKey es un componente de cierre que funciona mediante batería y se usa en taquillas, vitrinas y otros compartimentos como buzones, tanto en el exterior como en el interior.

Se accede mediante una comprobación electrónica de autorizaciones en el exterior. En el interior se encuentra una leva que aporta el bloqueo. Tanto el bloqueo como el desbloqueo pueden realizarse únicamente tras la comprobación de autorizaciones, girando manualmente el cilindro de buzón de AirKey. A diferencia del cilindro y el cilindro híbrido de AirKey, el pomo electrónico del lado de la identificación no gira libremente si no se está autorizado.

Compruebe que el cilindro de buzón de AirKey es apropiado para el uso previsto. El cilindro de buzón de AirKey está disponible en diferentes formas y configuraciones.

Las fichas técnicas de montaje están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

El cilindro de buzón de AirKey presenta dos tipos de señalización: óptica y acústica. Encontrará el significado de las diferentes señales en Señalización de los componentes de cierre.

Para el montaje del cilindro de buzón de AirKey, siga las instrucciones de montaje que vienen en la caja.

3.1.4 Candado de AirKey

El candado de AirKey es un componente de cierre que funciona mediante batería y se usa en barreras, persianas enrollables, depósitos y contenedores de archivado, tanto en el exterior como en el interior.

Se accede mediante una comprobación electrónica de autorizaciones en la parte inferior. El cierre se efectúa mediante un arco de acero endurecido. Tanto el cierre como la apertura pueden realizarse únicamente tras la comprobación de autorizaciones, girando manualmente el pomo electrónico del candado de AirKey.

Compruebe que el candado de AirKey es apropiado para el uso previsto. El candado de AirKey está disponible en diferentes configuraciones.

Las fichas técnicas de montaje están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

El candado de AirKey presenta dos tipos de señalización: óptica y acústica. Encontrará el significado de las diferentes señales en Señalización de los componentes de cierre.

Para el montaje del candado de AirKey, siga las instrucciones de montaje que vienen en la caja.

Herramienta de montaje para el cilindro de AirKey, Cilindro híbrido, cilindro de buzón y candado

El cilindro / cilindro híbrido / cilindro de buzón / candado de AirKey presenta un mecanismo especial para la protección contra la manipulación. El pomo electrónico solamente se puede extraer con una herramienta especial. La herramienta de montaje necesaria para el montaje, desmontaje y sustitución de pilas no viene de serie junto al cilindro de AirKey y debe pedirse por separado.

Tiene el código de pedido en el catálogo de AirKey, en el área de descargas:
https://www.evva.com/es/downloads/.

3.1.5 Lectores murales de AirKey

El lector mural de AirKey se puede utilizar tanto en el interior como en el exterior, montado en superficie o en pared, así como en todas las áreas en las que la seguridad sea importante.

En caso de instalación en exterior o zonas expuestas a humedad así como montaje en superficie, utilice la junta incluida para el producto y siga con atención el manual de montaje.

El lector mural de AirKey se conecta a la unidad de control de AirKey mediante el cable CAT5 (máx. 100 m, Loop máx. = 2 Ohm) y recibe corriente de esta. La unidad de control de AirKey recibirá corriente mediante el cable de alimentación y, en caso de interrupción en el suministro, dispone de un búfer de datos de como máximo 72 h, siempre y cuando la unidad de control de AirKey haya estado en funcionamiento durante 6 horas.

Tenga en cuenta que cada lector mural de AirKey se puede utilizar con una unidad de control de AirKey.

A través de la combinación de lector mural y unidad de control AirKey, se pueden controlar elementos electrónicos AirKey, tales como cilindros motorizados, puertas batientes, puertas correderas, etc.

En la unidad de control puede conectarse también un elemento de activación externo (pulsador). Si se activa dicho elemento, se abren las puertas como en el caso de un acceso mediante la unidad de lectura. No obstante, la apertura de las puertas mediante un elemento de activación externo NO se registrará. Por motivos de seguridad, debe tenerse en cuenta que, por lo tanto, es posible acceder a la instalación AirKey mediante sistemas de terceros, sin generar una entrada en el registro de acceso.

Compruebe cuidadosamente si el producto de AirKey seleccionado es adecuado para su uso e instalación previstos. La ficha técnica necesaria y el manual de montaje están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

3.2 App de AirKey

EVVA ofrece la app de AirKey, que está disponible en la Google Play Store o Apple App Store, de forma gratuita.

Se requiere la app de AirKey para poder utilizar los componentes de cierre con el smartphone. Además, el smartphone también puede añadir o actualizar componentes de cierre y medios en un sistema de AirKey. Para la mayoría de las acciones de la app de AirKey, se requiere una conexión activa a Internet. Entre estas acciones se excluye el accionamiento de los componentes de cierre.

La conexión a Internet puede tener un coste elevado. Tenga en cuenta su tarifa de Internet.

3.3 Smartphones

Para la utilización de un smartphone en el sistema de AirKey, se deben cumplir los continuars requisitos:

- Smartphone con NFC o Bluetooth 4.0 (Bluetooth Low Energy / BLE)
- Sistema operativo:
  - Android™ a partir de la versión 5.0 (solo con función NFC)
  - Android™ a partir de la versión 6.0 (NFC y Bluetooth)
  - Apple™ a partir de iOS 10 (solo con función Bluetooth)
- App de AirKey de la Google Play Store o Apple App Store

- Los smartphones Android necesitan la autorización "Consultar la identidad y el estado del teléfono" y la de determinación de la ubicación.

Lista de los smartphones compatibles con el sistema de AirKey

Tenga en cuenta que la compatibilidad de un smartphone depende de muchos factores, y no todos los smartphones que cumplen los requisitos mínimos son compatibles. EVVA somete así a los smartphones a un procedimiento de prueba detallada. Encontrará una lista constantemente actualizada de modelos de smartphones comprobados y listos para el uso de AirKey en lista de spartphones compatibles.

La **autorización "Consultar la identidad y el estado del teléfono"** se precisa para poder identificar inequívocamente el smartphone al agregar un nuevo sistema de control de accesos.

¡La **autorización sobre la ubicación es necesaria porque Android 6+ requiere la activación de la determinación de la ubicación para poder buscar componentes Bluetooth!** Si desea usar funciones Bluetooth en la app de AirKey, debe activar la función de detección de ubicación en la configuración del dispositivo, y también la app que concede la autorización a esta función. Si NO desea activar la detección de ubicación, puede establecer la conexión a los componentes (medios y componentes de cierre) mediante NFC.

En **dispositivos Apple** (sistema operativo iOS), puede desactivar la autorización "Consultar la identidad y el estado del teléfono". Asimismo iOS puede buscar componentes Bluetooth sin la autorización para la detección de ubicación.

3.4 Medios de AirKey

Los medios disponibles son los modelos de smartphones verificados hasta la fecha así como las tarjetas, los llaveros, las llaves combi y las pulseras en diferentes configuraciones como, por ejemplo, en combinación con la tecnología *Mifare DESFire EV1*.

Las fichas técnicas de montaje correspondientes, así como el catálogo de productos, están disponibles en el área de descargas de nuestra página web: https://www.evva.com/es/downloads/.

Los medios (tarjetas, llaveros, pulseras y llaves combi) se suministran en estado de fábrica. Para poder utilizarlos en sistemas de AirKey, se deben añadir primero al sistema.

3.5 Administración online de AirKey

La Administración online de AirKey consiste en el software online proporcionado por EVVA para la administración y gestión de los sistemas AirKey. El sistema de control de accesos electrónico

de AirKey funciona con todos los navegadores de Internet y sistemas operativos convencionales, y no requiere ninguna infraestructura informática especial. EVVA se encargará del funcionamiento y mantenimiento del centro de cálculo de AirKey.

3.5.1 Requisitos del sistema

- Sistemas operativos: Windows 10 (o superior), MacOS 10.15 (o superior), Linux
- Hasta la fecha son compatibles los continuars navegadores:
  Chrome, Firefox, Edge, Safari
- JavaScript activado en el navegador
- Conexión a Internet (1 Mbit/s o superior)
- Opcional: puerto USB 2.0 para la estación codificadora
- El puerto de Internet 443 debe estar accesible.

Para registrar un sistema de control de accesos, se necesita una dirección de e-mail válida.

3.6 KeyCredits EVVA

Para el funcionamiento de un sistema de control de accesos, se necesitan KeyCredits para la concesión o modificación de autorizaciones de acceso. Los KeyCredits están disponibles como cantidades de crédito (número definido de posibles cambios en las autorizaciones dentro de un período de tiempo ilimitado) o como un crédito de tiempo (número ilimitado de posibles cambios de permisos en un tiempo definido). Hay un paquete de KeyCredits adecuado para cada situación, según el tamaño y la dinámica del sistema de AirKey. Lo podrá adquirir a través de su distribuidor de EVVA. Encontrará más detalles sobre los paquetes disponibles en el catálogo de producto de AirKey (https://www.evva.com/es/downloads/).

3.7 Estación codificadora

Con la estación codificadora opcional, podrá añadir o actualizar componentes de cierre y medios de AirKey en un sistema de control de accesos, igual que con un smartphone con autorización de mantenimiento. La estación codificadora puede activarse mediante una aplicación local. La ventaja de la aplicación para instalar en la estación codificadora es que es compatible con los navegadores actuales y que la estación codificadora puede emplearse incluso tras el logout de la sesión en la Administración online de AirKey o cuando se ha cerrado el navegador, para actualizar componentes de cierre AirKey y medios.

Pueden emplearse los continuars navegadores: Chrome, Firefox y Edge.

Requisitos del sistema:

- Puerto USB
- Java 7 o superior
- Controladores de la estación codificadora

Encontrará información más detallada en el capítulo Instalar estación codificadora.

3.8 Alimentador de emergencia

En todos los componentes de cierre hay una interfaz en la parte frontal, debajo del logo de EVVA. Para acceder a ella, presione ligeramente hacia dentro el logo desde la izquierda de la inscripción (letra E), y extraiga la parte saliente de la derecha (letra A). La interfaz incluida sirve únicamente para el suministro de emergencia de energía y no se necesita durante un uso normal.

El alimentador de emergencia suministra electricidad a los componentes de cierre para que puedan utilizarse en caso de quedarse sin pilas. Conecte el cable del alimentador de emergencia en la interfaz correspondiente y enciéndalo a continuación. No se requiere más interacción con el alimentador de emergencia. Para operar los componentes de cierre, sigue siendo necesario un medio con una autorización válida.

Tenga en cuenta que aquí se debe asignar una autorización permanente sin límites en el período de validez. Encontrará información más detallada en el capítulo Medios de emergencia. Después de realizar la apertura de emergencia, sustituya inmediatamente las pilas en el componentes de cierre y después actualícelo para volver a permitir el acceso con otros medios. Encontrará más información sobre la apertura de emergencia en Cambio de pilas y apertura de emergencia.

Tenga en cuenta que el lector mural de AirKey no puede recibir alimentación a través del alimentador de emergencia, ya que funciona con una fuente de alimentación externa en combinación con la unidad de control de AirKey.

4 Puesta en marcha

En este capítulo, se describen los primeros pasos para la puesta en marcha del sistema de AirKey.

En la página principal https://www.evva.com/es/airkey/website/ también encontrará un vídeo que describe los primeros pasos y la puesta en marcha del sistema de AirKey.

Como ayuda en el montaje de componentes de cierre, EVVA ofrece el continuar material:

- **Manual de montaje**:
  Como apoyo a la instalación de los componentes de cierre, EVVA brinda instrucciones de montaje en imágenes, independientes del idioma. Estas se pueden encontrar en la caja de dichos productos y en la página principal https://www.evva.com/es/downloads/.

- **Vídeos**:
  Encontrará vídeos de montaje en la página web https://www.evva.com/es/airkey/website/.

4.1 Instalar la app de AirKey

- Descargue la app de AirKey de la Google Play Store o Apple App Store.
- Siga las instrucciones de instalación de la app de AirKey en el smartphone.

4.2 Registrarse en la Administración online de AirKey

Para utilizar la Administración online de AirKey, debe registrarse en EVVA con una dirección de e-mail válida.

- En el navegador, elija la página https://airkey.evva.com.
  Se abre la página de inicio de sesión de la Administración online de AirKey.
- Elija el ***idioma*** que quiera.
- Haga clic en el vínculo ***Registro AirKey*** ❶.

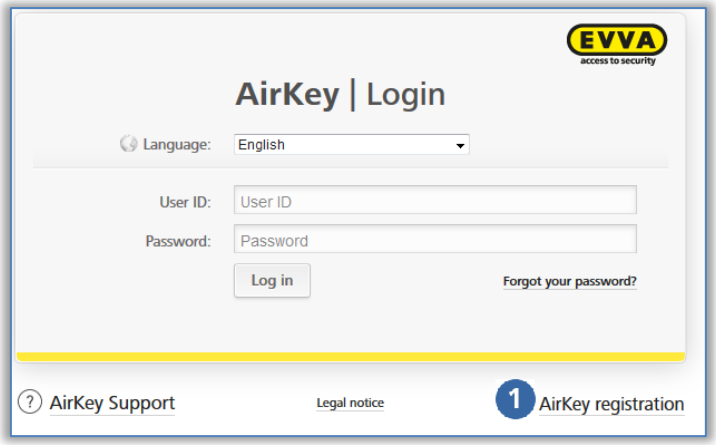


Figura 3: Vínculo "Registro de AirKey"

En el formulario de registro, rellene los campos para registrarse en AirKey.

> Elija ***cliente*** o ***cliente privado***.

> Rellene los campos del formulario.
Los campos marcados con * son obligatorios.

> Resuelva el Captcha ❶.

> Active la casilla con el vínculo Términos y condiciones generales y la casilla con el vínculo Condiciones generales de licencia ❷. Los dos documentos PDF correspondientes se abrirán automáticamente. Estos documentos también se pueden consultar en https://www.evva.com/es/airkey/impressum/.

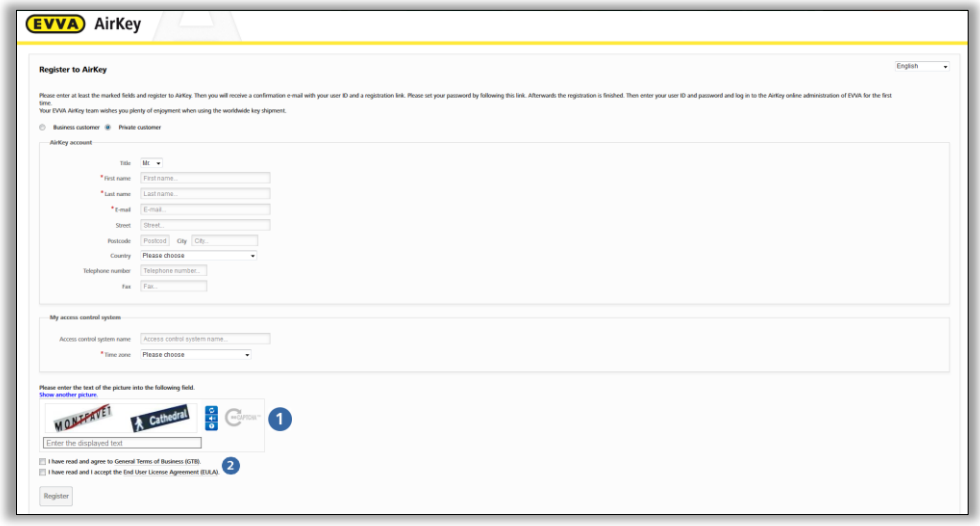


Figura 4: Registro en AirKey

> Podrá cambiar posteriormente los datos de cliente si fuera necesario. Para ello, haga clic en la Administración online de AirKey en el menú principal ***Sistema de control de accesos → Datos de cliente***.

> Haga clic en ***Registrar***. Se abrirá la ventana de usuario "Finalizar registro".

- Verifique de nuevo la dirección de e-mail especificada, pues se enviará ahí la confirmación con un vínculo de registro.
- Si la dirección de e-mail mostrada es incorrecta, cancele la operación con ***Cancelar*** y corrija los datos.
- Si la dirección de e-mail es correcta, finalice el procedimiento con ***Finalizar registro***.

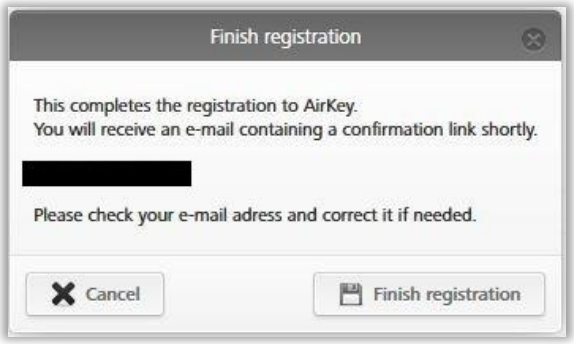


Figura 5: Finalizar registro

El sistema de AirKey generará automáticamente un ID de usuario y un vínculo de registro, que se enviará en forma de e-mail de registro a la dirección de e-mail facilitada.

- Abra su cliente de correo electrónico; encontrará el e-mail de *EVVA AirKey* con el asunto "Registro de EVVA AirKey".
- Abra el e-mail y haga clic en el vínculo de registro ❶.

Guarde este e-mail. En caso de recibir asistencia, necesitará el ID de usuario único y su número de cliente contenidos en este e-mail.

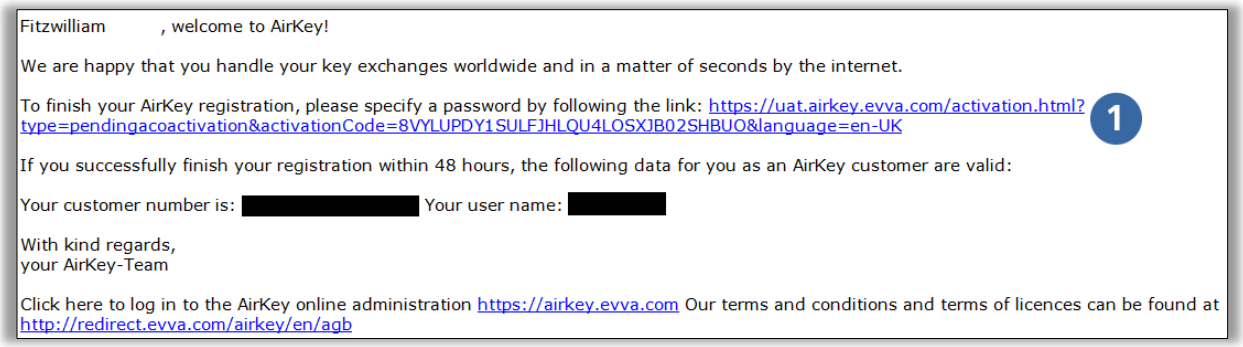


Figura 6: E-mail "Registro de EVVA AirKey"

El vínculo de registro del e-mail tiene una validez de 48 horas únicamente.

Si el vínculo de registro ha caducado o no es válido, aparecerá el mensaje de error "Vínculo de registro no válido". En este caso, deberá registrarse de nuevo.

Tras hacer clic en el vínculo de registro, se abre la ventana de bienvenida en la que puede completar el registro.

- Introduzca una contraseña que haya elegido para la Administración online de AirKey. La contraseña de AirKey debe contener, al menos, 6 caracteres, un número, una letra minúscula y una letra mayúscula. De lo contrario, aparecerá un mensaje de error.
- Introduzca de nuevo su contraseña.
- Introduzca su fecha de nacimiento. Esta se utilizará como pregunta de seguridad si no recuerda su contraseña.

Por motivos de seguridad, le recomendamos que elija una contraseña de AirKey lo más larga posible y que la mantenga en secreto.

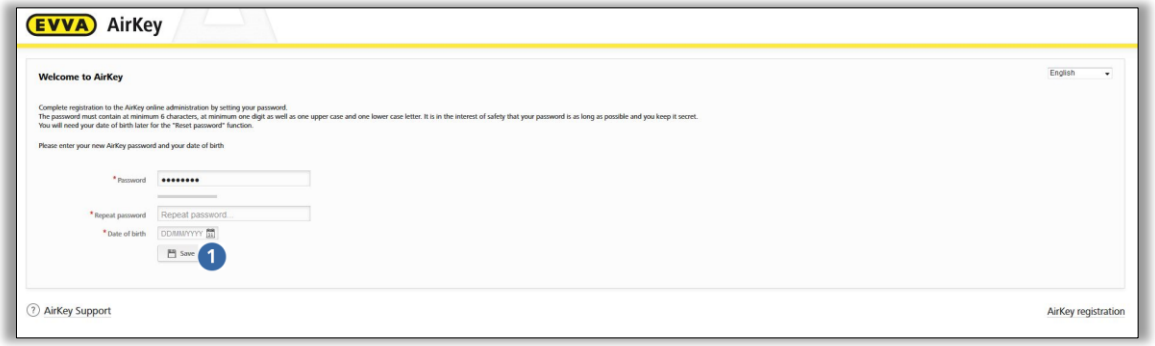


Figura 7: Determinación de la contraseña propia de AirKey para finalizar el registro

- Si los campos están rellenados y las dos contraseñas de AirKey coinciden, cierre el registro mediante la opción ***Guardar*** ❶.

Ya ha completado el proceso de registro y el sistema de control de accesos se ha activado correctamente.

A partir de ahora, puede acceder mediante la página de inicio de sesión a la Administración online de AirKey en cualquier momento. Todo lo que necesita es el ID de usuario del e-mail de registro y la contraseña de AirKey establecida antes.

4.3 Inicio de sesión

Se requiere iniciar sesión para configurar y gestionar el sistema de control de accesos.

- En el navegador, visite la página https://airkey.evva.com.
  Se abre la página de inicio de sesión de la Administración online de AirKey.
- Elija el ***idioma*** que quiera. En la sesión activa, puede modificar el idioma en cualquier momento a la derecha en la barra de menú.
- Introduzca su ID de usuario tal y como figura en el e-mail de registro, así como la contraseña establecida y confirme con ***Iniciar sesión***. Se abrirá la página de inicio de su sistema de control de accesos.

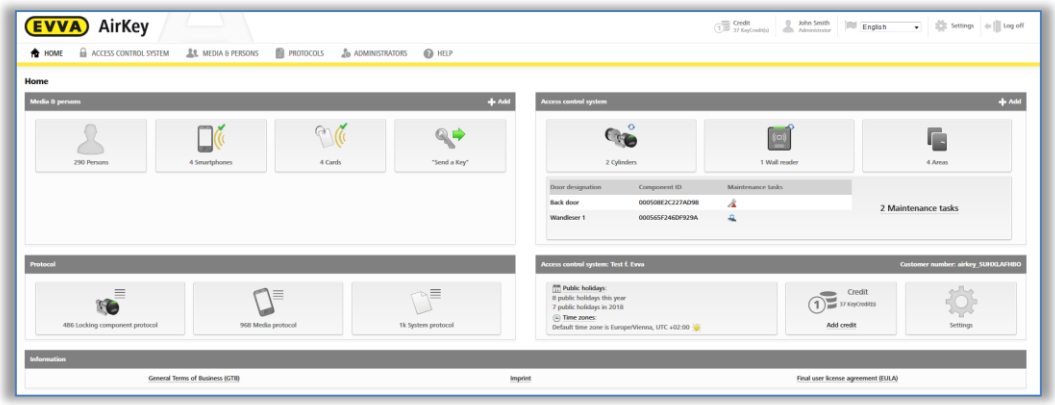


Figura 8: Página de inicio del sistema de control de accesos

En la página de inicio se mostrará, de forma general, toda la información relativa al sistema. Desde aquí se puede acceder a todas las funciones y ajustes.

4.4 Ayuda interactiva

En la Administración online de AirKey, tras el primer inicio de sesión arranca la ayuda interactiva que le guía por el programa y le explica las funciones más importantes.

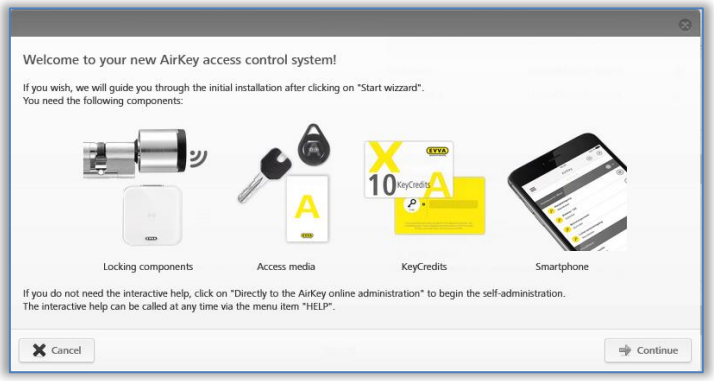


Figura 9: Ayuda interactiva

Como ejemplo, se muestra aquí la función "Recargar crédito". La ayuda interactiva le muestra qué botones debe presionar y qué información debe introducir en los campos. Dentro de la ayuda interactiva, puede navegar adelante y atrás.

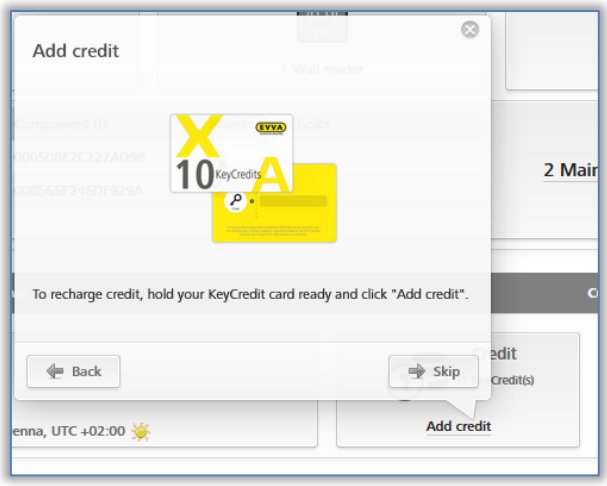


Figura 10: Ayuda interactiva – Cargar crédito

También puede cerrar la ayuda interactiva y conocer la Administración online de AirKey con el manual del sistema.

Si ha cerrado la ayuda interactiva y desea abrirla de nuevo, en el menú principal elija ***Ayuda*** → ***Ayuda interactiva***. Así puede reiniciar la ayuda interactiva en cualquier momento y cuantas veces quiera.

4.5 Instalar estación codificadora

Option La estación codificadora de AirKey también se puede usar para añadir componentes de cierre y medios a un sistema de control de accesos o para actualizarlos.

Para utilizar una estación codificadora en el sistema AirKey es necesario instalar una aplicación de estación codificadora.

Hay dos formas de utilizar la estación codificadora:

- en el navegador a través de la Administración online de AirKey
- sin navegador, mediante la línea de comandos

4.5.1 Utilización de la estación codificadora a través de la Administración online de AirKey

La ventaja de la aplicación para instalar en la estación codificadora es que es compatible con los navegadores actuales y que la estación codificadora puede emplearse incluso tras el logout de la sesión en la Administración online de AirKey o cuando se ha cerrado el navegador, para actualizar componentes de cierre AirKey y medios.

Únicamente es posible añadir o retirar componentes de cierre a/de un sistema de control de accesos, así como realizar la Firmware-Update de componentes de cierre o la Keyring-Update de los medios de acceso tras el login en la Administración online de AirKey. La actualización de medios y componentes de cierre también es posible tras el logout en la Administración online de AirKey o si el navegador se ha cerrado.

Los continuars navegadores soportan la comunicación entre la Administración online de AirKey y la aplicación local de la estación codificadora: Chrome, Firefox y Edge.

La descarga y la ejecución de la aplicación de la estación codificadora son específicas para cada navegador y sistema operativo. La apariencia en su navegador puede diferenciarse de la que aquí se muestra (para Firefox).

Regístrese e inicie sesión en la Administración online de AirKey (véase el capítulo Registrarse en la Administración online de AirKey).

> Conecte la estación de codificación a un puerto USB de su ordenador.

> En la Administración online de AirKey, haga clic en el símbolo + abajo a la derecha ❶.

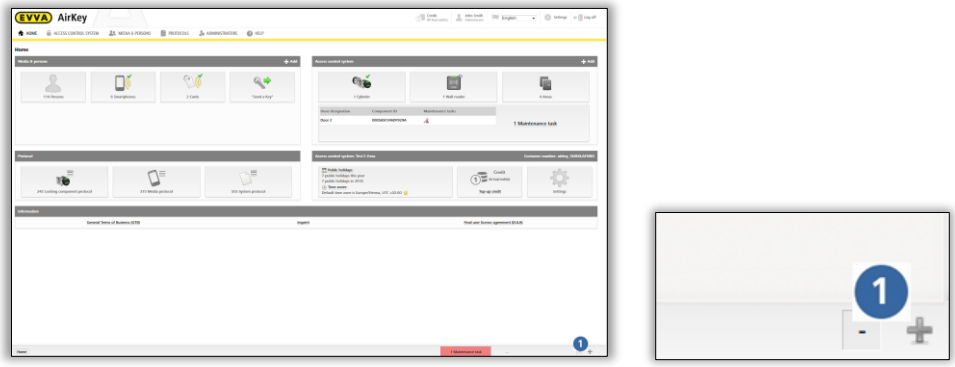


Figura 11: Estación codificadora – Instalación de la aplicación local

> Para instalar la aplicación de la estación codificadora, a continuación haga clic en el vínculo "Instalar e iniciar la aplicación de la estación codificadora" ❶.

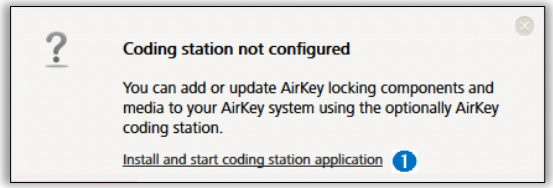


Figura 12: Instalar e iniciar la aplicación de la estación codificadora

Tras hacer clic en el vínculo, tiene 60 segundos para abrir el archivo AirKey.jnlp (consulte el continuar paso). En caso de superarse este plazo, se debe repetir la instalación a partir del paso actual. También puede guardar el archivo AirKey.jnlp y abrirlo manualmente.

> Aparecerá el cuadro de diálogo de descarga del archivo AirKey.jnlp. Ábralo con el "Java(TM) Web Start Launcher".

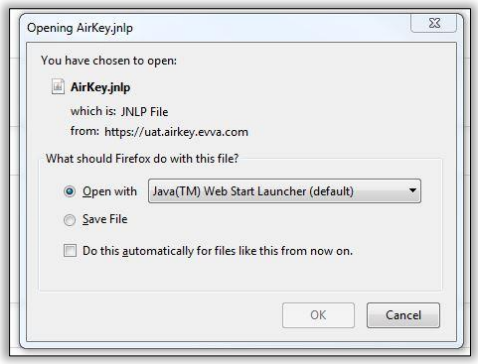


Figura 13: Apertura del archivo AirKey.jnlp

> Tras abrir el archivo, se establecerá la conexión con la estación codificadora.

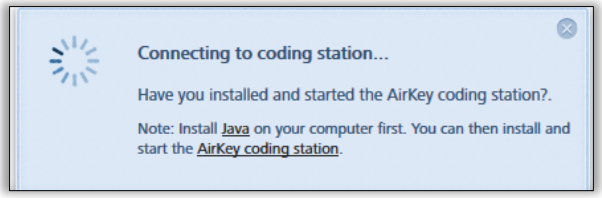


Figura 14: Establecer la conexión con la estación codificadora

> Seleccione la estación codificadora actual (p. ej. "OMNIKEY CardMan 5x21-CL 0" ❶) de la lista.

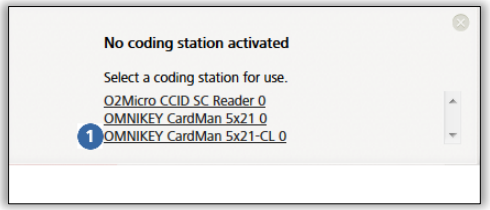


Figura 15: Selección de la estación codificadora

> En la barra de tareas abajo a la derecha, aparecerá un icono de AirKey que indica que la estación codificadora se ha instalado correctamente y está activa.

Figura 16: Icono de AirKey en la barra de tareas

4.5.2 Utilización de la estación codificadora a través de la línea de comandos

La aplicación para la estación codificadora también puede instalarse y configurarse sin la Administración online de AirKey; por ejemplo, mediante la línea de comandos. (Para esta opción se requieren conocimientos de TI más amplios, sobre todo para trabajar con la línea de comandos.)

A través de la línea de comandos, la estación codificadora solo se puede utilizar para actualizar medios de acceso y componentes de cierre. Solo se puede actualizar el firmware de los

componentes AirKey a través del navegador o con un smartphone con autorización de mantenimiento.

> Almacene la aplicación para la estación codificadora mediante el enlace https://airkey.evva.com/smkrest/jnlp/newest-jar-file/ en el directorio deseado.

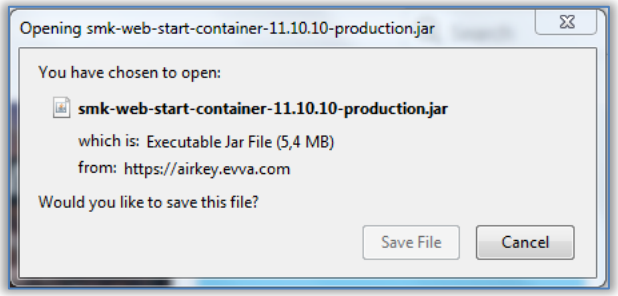


Figura 17: Descargar aplicación para la estación codificadora

> Abra la línea de comandos y navegue por el directorio en el que se había guardado la aplicación para la estación codificadora.

> Inicie la aplicación de la estación codificadora con la siguiente orden:

`java -jar <nombre archivo>`
(p. ej. `web-start-container-customer-15.10.0-8.jar`)

Además, puede especificar los siguientes parámetros opcionales:

- **`-reader "<nombre de la estación codificacadora>"`**: Con este parámetro se puede utilizar una estación codificadora determinada (p. ej. "HID Global OMNIKEY 5022 Smart Card Reader 0"). En este caso, se ignorará el archivo de configuración `config_customer.json`.
- **`-port <VALOR [1024-65535]>`**: Si no se especifica este parámetro, se usará por defecto el puerto 50743. El puerto 50743 también se utiliza cuando la estación codificadora se utiliza en el navegador a través de la Administración online de AirKey. Si desea utilizar varias estaciones codificadoras en paralelo en un ordenador, debe especificar un puerto propio para cada estación codificadora. Con el parámetro "**`-port 0`**" se utiliza un puerto aleatorio.
- **`-configDir <VALOR>`**: En la carpeta especificada (valor predeterminado para Windows: `%USERPROFILE%\.airkey`) se guarda el archivo de configuración `config_customer.json`. Este se genera automáticamente la primera vez que se inicia la aplicación de la estación codificadora y guarda los últimos ajustes utilizados.
- **`-workDir <VALOR>`**: En la carpeta indicada se crea, p. ej., el archivo de registro `logs\application.log` cuando se inicia la aplicación de la estación codificadora. Aquí se registran todas las acciones realizadas con la aplicación de la estación codificadora. Si utiliza varias estaciones codificadoras en paralelo, resulta útil utilizar una carpeta propia para cada estación codificadora.
- **`-notify <nombre archivo>`**: Define un archivo o script ejecutable que puede reenviar la lockingSystemID a un sistema de terceros como cadena hexadecimal (argument1) o como long-int (argument2) de un medio de acceso actualizado

con éxito en la estación codificadora. Este parámetro es principalmente relevante para la integración de AirKey en sistemas de terceros y el uso de AirKey Cloud Interface. Allí se puede evaluar y procesar la lockingSystemId del medio de acceso. Por ejemplo, para averiguar la persona a quien pertenece el medio de acceso. Se describe en detalle AirKey Cloud Interface en el capítulo AirKey Cloud Interface (API).

- **`-version`**: Muestra la versión de la aplicación de la estación codificadora.
- **`-help`**: Abre la Ayuda y describe todos los parámetros posibles.

> En la barra de tareas, en la parte inferior derecha, aparecerá el icono de AirKey y en la línea de comandos se mostrará información sobre el directorio de configuración ❶, el directorio de trabajo ❷ y las estaciones codificadoras disponibles ❸.

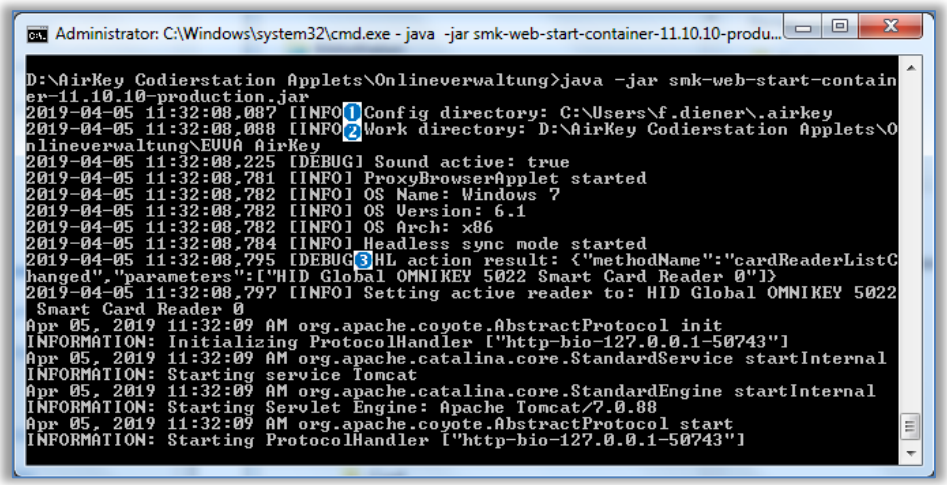


Figura 18: Iniciar la aplicación de la estación codificadora mediante la línea de comandos

4.5.3 Ajustes de la aplicación de la estación codificadora

Al hacer clic con el botón derecho del ratón en el icono de AirKey, se abre el menú contextual correspondiente.

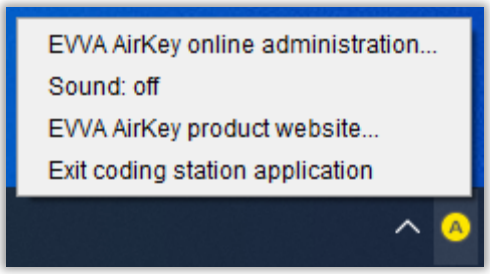


Figura 19: Ajustes de la aplicación de la estación codificadora

Lista de las opciones correspondientes:

> ***Administración online de AirKey*** – vínculo a la página de inicio de sesión de la Administración online de AirKey.

> ***Sonido: activado*** – se emite un pitido cuando se actualiza un componente con la estación codificadora. Resulta útil como aviso acústico cuando se usa la estación codificadora sin la Administración online de AirKey. Haciendo clic en ***Sonido: activado*** se pasará a ***Sonido: desactivado***.

- ***Sonido: desactivado*** – no se emitirá ningún sonido de advertencia. Haciendo clic en ***Sonido: desactivado*** se pasará a ***Sonido: activado***.
- ***Sitio web de EVVA AirKey…*** – vínculo al sitio web de AirKey
- ***Salir de la aplicación de la estación codificadora*** – cierra la aplicación de la estación codificadora.

4.5.4 Soluciones para posibles problemas con la estación codificadora

Cuando la estación codificadora está conectada, el diodo luminoso señala que está lista para funcionar Cuando no hay señal de que la estación codificadora esté lista, desconéctela y vuelva a conectarla. Instale entonces el controlador de la estación codificadora de nuevo.

Al apagar el ordenador, la aplicación local de la estación codificadora finalizará automáticamente. Para un inicio automático de la aplicación al reiniciar el ordenador, puede generar un acceso directo de la aplicación mediante Control Panel (Configure Java) de Java™ (aplicación: AirKey Card Reader Proxy; tipo: aplicación) y guardarlo en la carpeta de Inicio automático.

La aplicación de la estación codificadora finaliza tras el inicio

La aplicación de la estación codificadora utiliza de forma predeterminada el puerto 50743 para la comunicación con el navegador. Si este puerto lo utiliza otro programa, no se puede iniciar la aplicación de la estación codificadora. En Windows 10 o posterior, este puerto puede ser utilizado por Hyper-V. Puede evitar que Hyper-V utilice este puerto de la siguiente manera:

- Desactive Hyper-V:
  ```
  C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V
  ```
- Reinicie el ordenador.
- Añada una excepción para el puerto 50743:
  ```
  C:\> netsh int ipv4 add excludedportrange protocol=tcp startport=50743
       numberofports=1
  ```
- Reactive Hyper-V:
  ```
  C:\> dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All
  ```
- Reinicie el ordenador.

Como estación codificadora está seleccionado el lector de tarjetas "Microsoft UICC"

Figura 20: Lector de tarjetas "Microsoft UICC" en la Administración online de AirKey

Como solución, el lector de tarjetas UICC se puede desactivar en el administrador de dispositivos de Windows: Administrador de dispositivos → Dispositivos de software → Microsoft UICC ISO Reader → Deshabilitar dispositivo

No se puede establecer la conexión con la estación codificadora a través de la Administración online de AirKey (proxy HTTPS)

Tanto la Administración online de AirKey como la aplicación de la estación codificadora se comunican cifradas con el sistema AirKey a través del puerto 443. Sin embargo, en las redes que utilizan un proxy HTTPS puede ser necesario definir una excepción para "airkey.evva.com" y subdominios, ya que la aplicación de la estación codificadora comprueba el certificado del servidor mediante "certificate pinning" y, por lo tanto, no permite proxies HTTPS.

No se puede establecer la conexión con la estación codificadora a través de la Administración online de AirKey (protección de conexión *DNS rebinding*)

La Administración online de AirKey se comunica localmente entre el navegador y la aplicación de la estación codificadora. Las acciones como la colocación de componentes AirKey o medios de acceso en la estación codificadora se mostrarán entonces en la Administración online de AirKey.

El navegador se conecta a la aplicación de la estación codificadora a través de "components.airkey.evva.com" (puerto 50743). El servidor DNS resuelve esta URL como 127.0.0.1.

Por lo tanto, es posible que sea necesario añadir excepciones para "components.airkey.evva.com" y subdominios de "airkey.evva.com" con la protección activa contra revinculación de DNS.

Windows busca repetidamente el controlador de la estación codificadora

Al colocar un componente AirKey o un medio de acceso en la estación codificadora, Windows intenta buscar e instalar un controlador para la estación codificadora. Esto puede influir en la comunicación con la estación codificadora y causar fallos de funcionamiento.

Como solución, el servicio plug & play de tarjetas inteligentes de Windows puede desactivarse:

- Tecla Windows + R
- Escriba "gpedit.msc" y confirme con ***Enter***.
- El programa "Editor de directivas de grupo local" → Configuratión del equipo → Plantillas administrativas → Componentes de Windows → Tarjeta inteligente
- Haga doble clic en la línea con la entrada "servicio plug & play de tarjetas inteligentes" en el lado derecho.

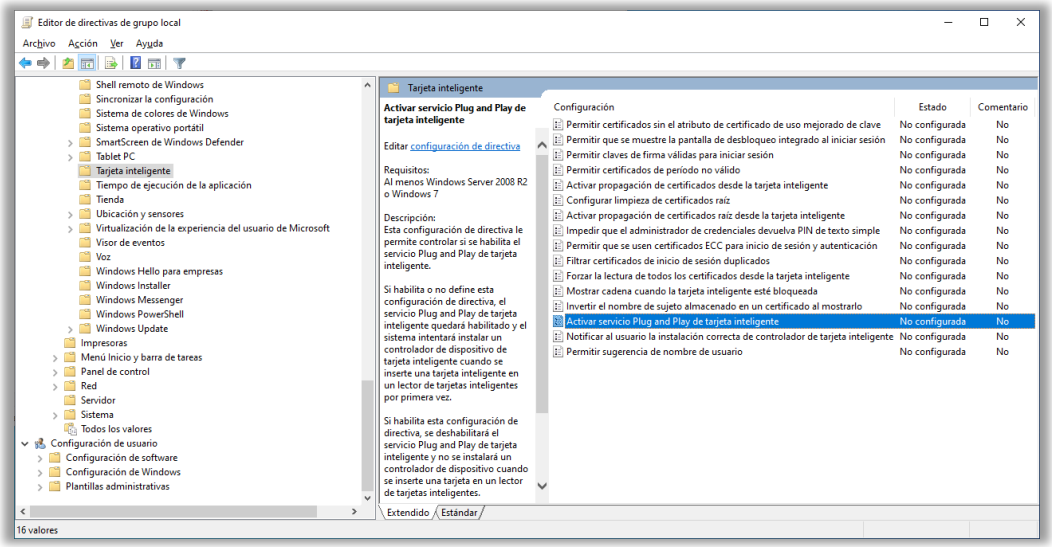


Figura 21: Editor de directivas de grupo local

> Seleccione el botón de opción ***Deshabilitada***.

> Confirme con ***Aceptar***.

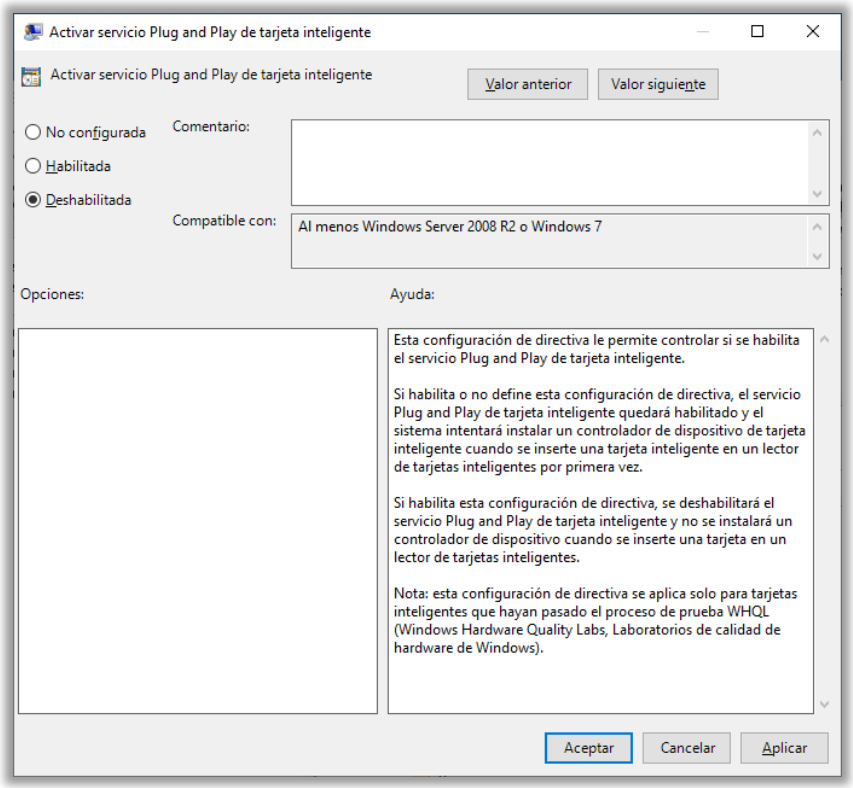


Figura 22: Servicio Plug and Play de tarjeta inteligente

En MacOS 11.x o posterior no se puede seleccionar ninguna estación codificadora

Desde MacOS Big Sur (11.x) ya no es posible seleccionar una estación codificadora conectada a través de la Administración online de AirKey. La aplicación de la estación codificadora se puede iniciar correctamente, pero no se muestra ninguna estación codificadora en la Administración online de AirKey.

Como solución se puede iniciar la estación codificadora a través de la línea de comandos (véase el capítulo Utilización de la estación codificadora a través de la línea de comandos). Sin embargo, es necesario que la versión de Java JDK17 (Oracle JDK17 o OpenJDK17) o posterior esté instalada.

4.6 Cargar crédito

Se necesita una tarjeta de KeyCredits; en la parte posterior hay un recuadro para rascar con un código de recarga.

> En la página de inicio ***Home***, elija la opción ***Recargar crédito*** ❶.

> También puede hacer clic en ***Crédito*** en el encabezado.

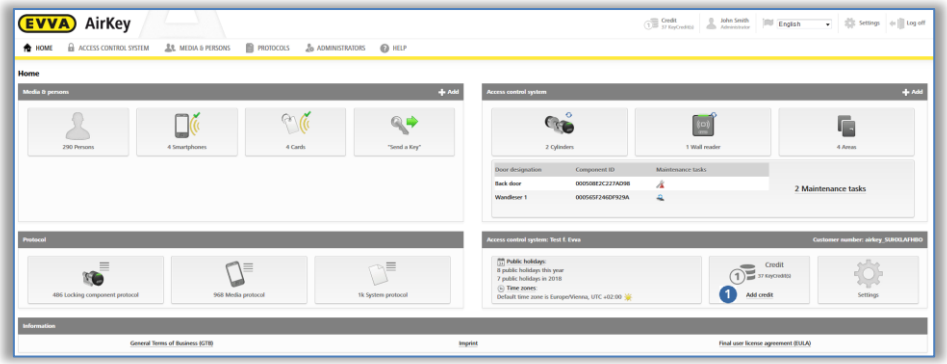


Figura 23: Crédito

> Obtendrá una visión general de su crédito actual y las recargas ya realizadas.

> Haga clic en el botón ***Recargar crédito*** ❶.

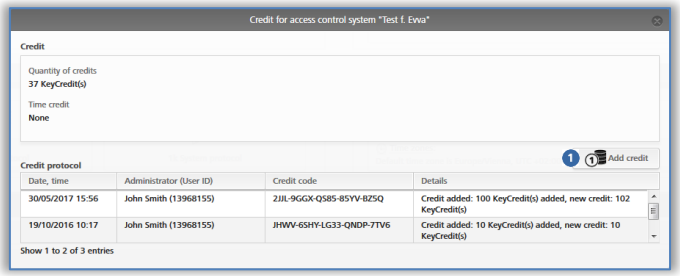


Figura 24: Recargar crédito

> Introduzca el código de la tarjeta KeyCredit en la ventana "Recargar crédito".

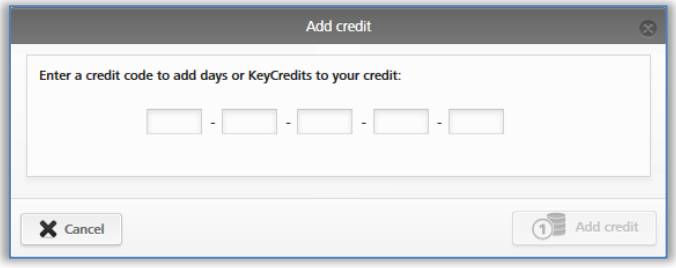


Figura 25: Introducir código de crédito

> Haga clic en ***Recargar crédito***.

Si el código introducido es correcto, se realizará y confirmará la recarga.

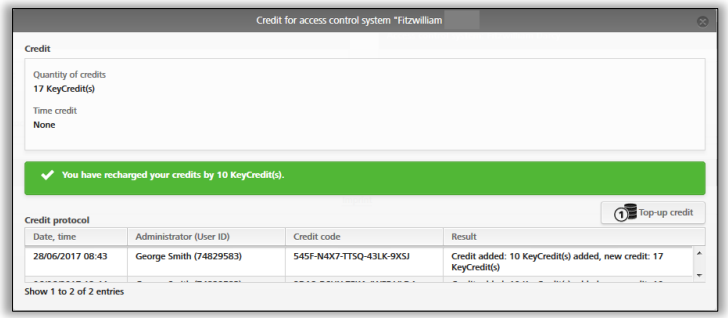


Figura 26: Recargar crédito

4.7 Crear persona

Toda persona que vaya a recibir una autorización para un sistema de control de accesos, debe crearse antes en el sistema.

- En la página de inicio ***Home***, en la barra gris del bloque ***Medios y personas***, haga clic en ***Añadir*** → ***Crear persona***.
- O en la página de inicio ***Home***, elija la opción ***Personas*** → ***Crear persona***
- O en el menú principal, elija ***Medios y personas*** → ***Crear persona***.
- O elija el botón **"*Send a Key*"** y haga clic en ***Crear nuevo***. Aquí puede crear una persona con un smartphone.
- Rellene los campos del formulario. Los campos marcados con * son obligatorios.
- Haga clic en ***Guardar*** ❶.

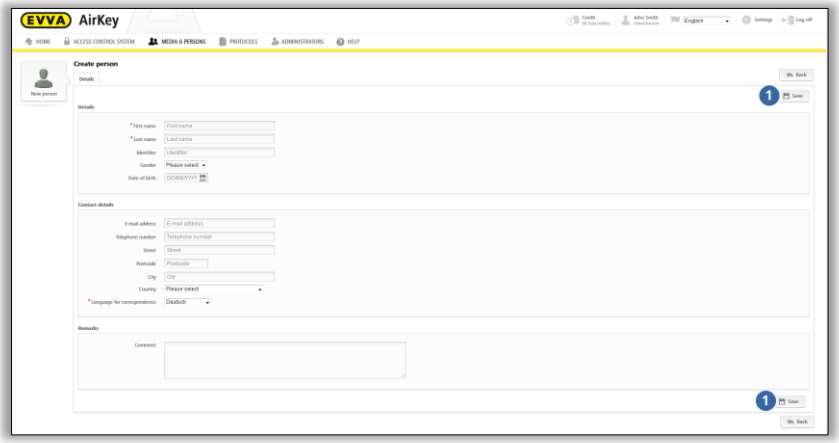


Figura 27: Crear persona

Los campos de nombre, apellido e identificación proporcionan una combinación única dentro del sistema de control de accesos.

Si también rellena el campo "Nombre de usuario", utilice un valor que garantice que la combinación de nombre y apellido es única (p. ej. un número personal). Esto es especialmente útil si hay varias personas con el mismo nombre y apellido.

La longitud del campo de e-mail, número de teléfono, calle, código postal y localidad está limitada a 50 caracteres cada uno. Para el "Código Postal" pueden emplearse 10 caracteres como máximo. En el campo de comentarios, puede incluir un texto de hasta 500 caracteres.

Si ya existe la combinación introducida, recibirá el mensaje de error "La persona ya existe".

> De ser necesario, compruebe o corrija los campos.

> Haga clic en ***Guardar***.

Cuando se cree una nueva persona, aparecerán un mensaje de confirmación y debajo del nombre una nueva opción ***Asignar medio*** ❶.

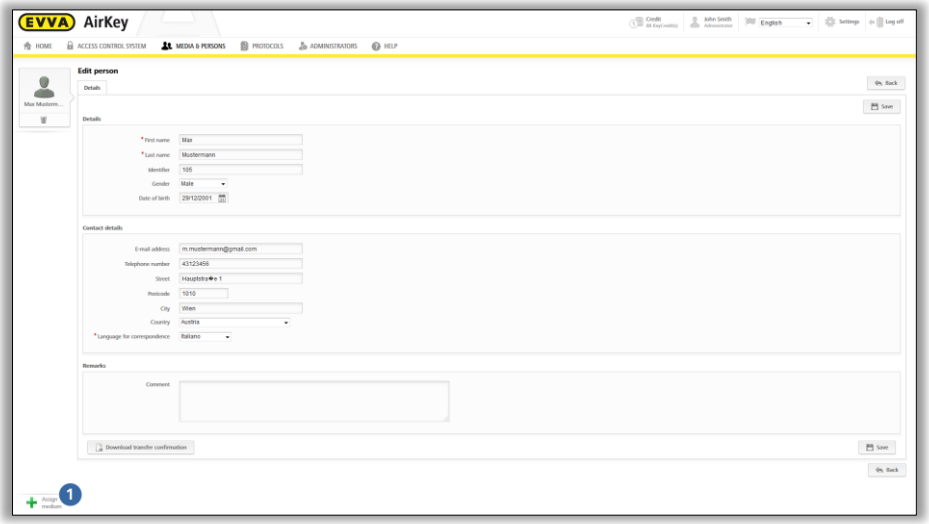


Figura 28: Asignar medio

La persona quedará así creada en el sistema de control de accesos y estará incluida en la lista de personas.

4.7.1 Importar datos de personas

En AirKey también puede crear personas a través de archivos externos. Para ello, necesita un archivo CSV para importarlo en la Administración online de AirKey.

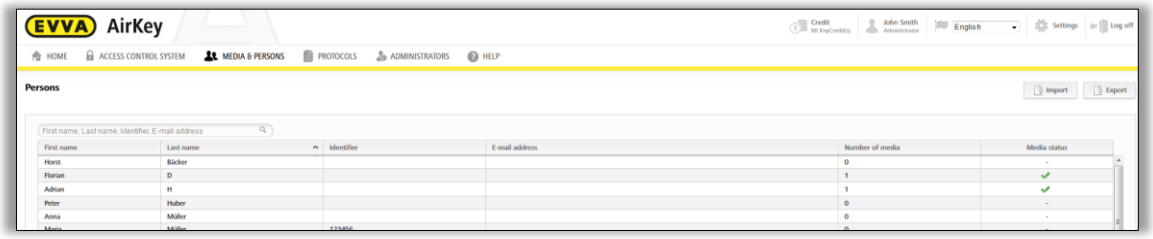


Figura 29: Importar lista de personas

La distribución de la tabla de personas se rige por la hoja ***Crear persona*** en la Administración online de AirKey, es decir la columna A es el nombre ❶, la B es el apellido ❷, la C la nombre de usuario ❸, etc. En este orden exacto, se importará el archivo CSV en la Administración online de AirKey.

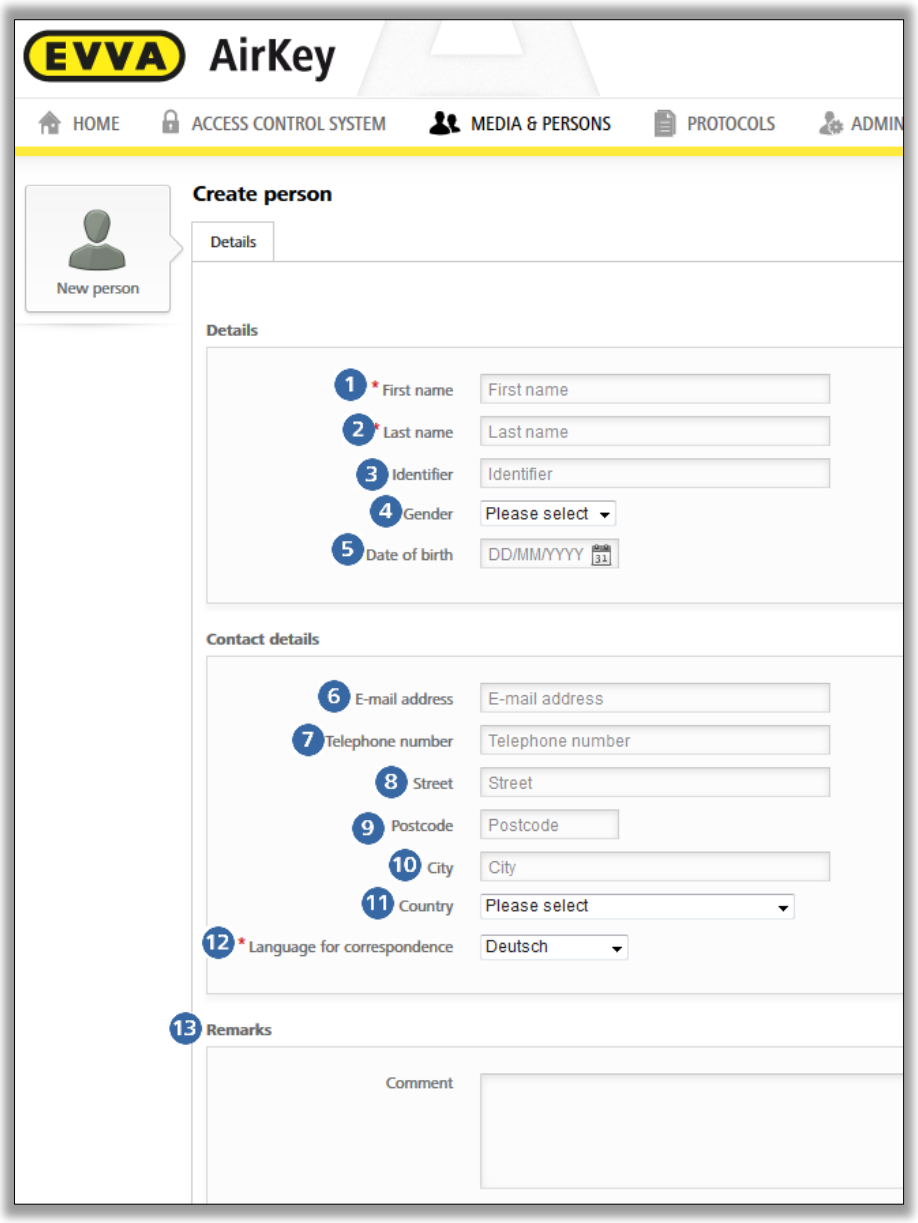


Figura 30: Importar personas – Lista de personas

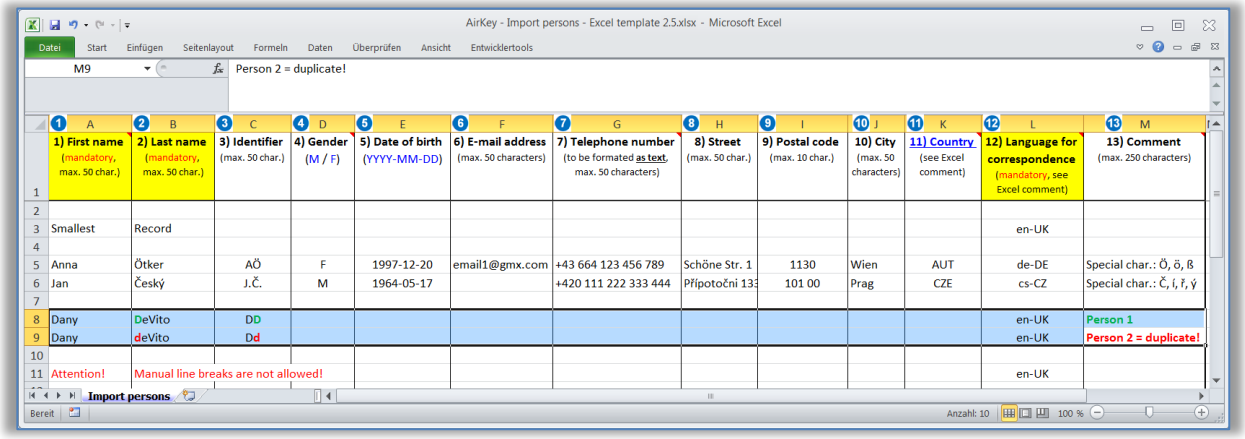


Figura 31: Importar personas – Distribución de campos en la lista de personas

Propiedades de un archivo CSV con los datos de personas que se deben importar:

- La primera fila se ignora siempre. Por eso, se recomienda introducir ahí el nombre de los campos para identificar los demás datos con mayor facilidad. La primera fila también puede quedar vacía, pero no debe contener ninguna persona, ya que no se importará.
- Las filas vacías o que solo contengan espacios y tabuladores también se ignorarán. Si desea organizar el archivo CSV con mayor claridad, también puede introducir cuantas filas vacías quiera.
- Cada fila debe incluir los 13 campos (atributos) representados en la Figura 30.
- Los campos están separados por un punto y coma.
- Solo hay 3 campos obligatorios: nombre (campo 1), apellido (campo 2) e idioma de correspondencia (campo 12).
- Si no hay datos para el resto de campos, deben existir igualmente pero como campos vacíos (;;).
- El sexo (campo 4) solo puede ser **M** (de *male* = hombre) o **F** (de *female* = mujer), o estar vacío. Esto se aplica a todos los idiomas, y M y F se deben usar solo en mayúsculas.
- La fecha de nacimiento (campo 5) debe estar en formato **AAAA-MM-DD** (p. ej. 1997-12-20).
- La dirección de e-mail (campo 6) debe incluir el carácter **@** y otros caracteres, o estar vacío.
- El país de la dirección (campo 10) debe contener los 3 caracteres del código ISO 3166-1 (columna alfa-3) del país, o estar vacío. El código solo se puede escribir en mayúsculas. Ejemplos: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL, etc.
- El idioma de correspondencia (campo 12) es un campo obligatorio y debe contener el código ISO del idioma. Se deben respetar escrupulosamente las minúsculas y mayúsculas. Únicamente se aceptan los siguientes códigos: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- Una persona que se deba importar se muestra como ya existente (símbolo ⚠) si ya existe la combinación de nombre + apellido + identificación (campos 1-3) en la Administración online de AirKey, aunque el resto de campos (4-13) sea diferente. Estas personas no se importan. No se tendrán en cuenta las mayúsculas y minúsculas a la hora de escribir los nombres (p. ej., "Danny;**D**eVito;D**D**" y "Danny;**d**eVito;D**d**" se considerarían la misma persona y únicamente se importaría la primera persona).
- Una persona se interpreta como duplicada en el archivo CSV si ya se ha encontrado la combinación de nombre + apellido + identificación (campos 1-3), aunque el resto de campos (4-13) sea diferente. En este caso, se muestra solo la primera fila con una combinación determinada y, a continuación, se importa. Todos los demás duplicados se ignorarán y no aparecerán en la tabla de personas que se deben importar.
- Un archivo CSV debe contener los datos de máx. 10 000 personas incluidas. Si desea importar más personas, cree varios archivos CSV que puede importar por separado.

- Las filas erróneas del archivo CSV se marcan antes de la importación con el símbolo ✖ y se les confiere una ayuda contextual que describe todos los errores. Estas filas no se importan.
- Con independencia de las filas erróneas que pueda haber, se marcarán todas las correctas con el símbolo ✔ y, a continuación, se importarán.

La codificación de los caracteres del archivo CSV debe ser UTF-8 para que se muestren correctamente las letras específicas de los países (Ä, ß, ç, Ñ, č, etc.). A continuación se describe en detalle la creación de un archivo CSV en formato UTF-8.

Creación de un archivo CSV en formato UTF-8

La siguiente descripción es válida para Windows 10™ empleando Microsoft Excel™ y programas auxiliares que ya existen en Windows 10™. En otras versiones de Windows u otros sistemas operativos puede crearse de forma similar un archivo CSV en formato UTF-8. Pasos necesarios:

- Como punto de partida, en esta descripción se toma una tabla Excel que contiene los datos de las personas a importar.
- Vigile en la tabla Excel que la séptima columna (número de teléfono) esté formateado como texto. Si se formatea como cifras, hay caracteres importantes como "+" y "0" (cero) que se pierden durante la conversión. Sin embargo, sí se permiten espacios en blanco dentro del número de teléfono, lo que aumenta la claridad en la Administración online de AirKey.
- Compruebe, con ayuda de la función de búsqueda en Excel, que la tabla no contenga ninguno de los siguientes caracteres:
  - " (comillas dobles y rectas)
  - ; (punto y coma = carácter de separación en el archivo CSV que debe importarse en la Administración online de AirKey)
- Excel no puede almacenar los datos directamente en formato UTF-8. Por ello es necesario almacenar los datos primero en formato Unicode.
- Acceda para ello en Excel al punto de menú ***Archivo*** → ***Guardar*** (o pulse la tecla F12).
- En la siguiente ventana de diálogo "Guardar como", introduzca el nombre deseado para el archivo ❶.
- En la lista desplegable ***Tipo de archivo*** ❷, elija el formato ***Texto Unicode (*.txt)***.
- Haga clic en ***Guardar*** ❸.

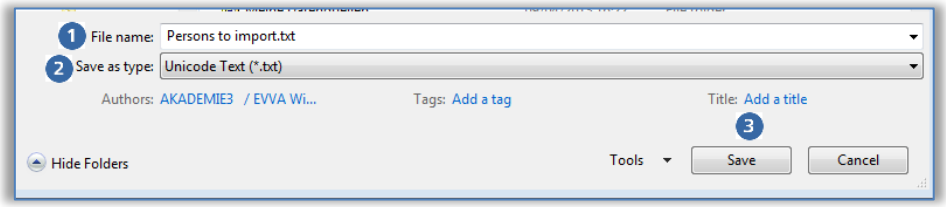


Figura 32: Excel – Guardar como – "Texto Unicode (*.txt)"

- Confirme la siguiente pregunta en Excel en referencia al "Texto Unicode" con un ***Sí***.

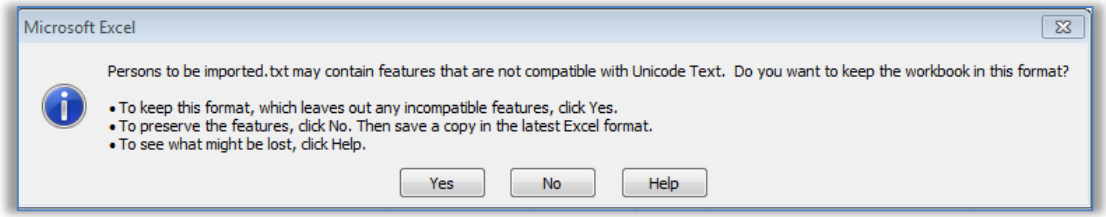


Figura 33: Confirmar el almacenado del Excel como "Texto Unicode (*.txt)"

> Abra el archivo generado (*.txt) con un editor de texto. Windows™ emplea de forma estándar el programa ***Editor***.

> El carácter de separación en el archivo de texto Unicode es el tabulador. Todos los tabuladores deben sustituirse por puntos y comas (;). Para ello marque primero un tabulador entre 2 campos y cópielo.

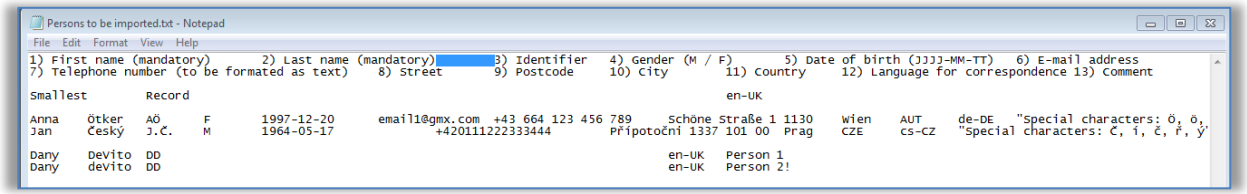


Figura 34: Archivo de texto en "Editor" – marcar un tabulador y copiar en el portapapeles.

> Acceda en ***Editor*** al punto de menú ***Editar*** → ***Sustituir*** para abrir la ventana de diálogo "Sustituir".

- Añada en el campo ***Búsqueda por*** el carácter del tabulador del portapapeles, dado que se trata de un carácter que no puede introducirse directamente aquí.
- Introduzca en el campo ***Sustituir por*** un punto y coma (;).
- Haga clic en ***Sustituir todos*** ❶.

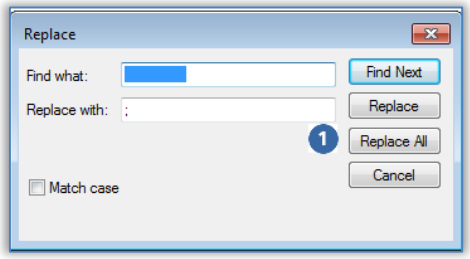


Figura 35: "Editor" – sustituir todos los tabuladores por puntos y comas.

> Cierre la ventana de diálogo "Sustituir" y acceda en ***Editor*** al punto de menú ***Editar*** → ***Guardar como*** para abrir la ventana de diálogo "Sustituir".

- Modifique manualmente el final del archivo (de .txt a .csv) en el campo ***Nombre de archivo*** ❶. Cambiar el nombre posteriormente supone más trabajo.
- En la lista desplegable ***Codificación*** ❷, elija el formato ***UTF-8***.
- Haga clic en ***Guardar*** ❸.

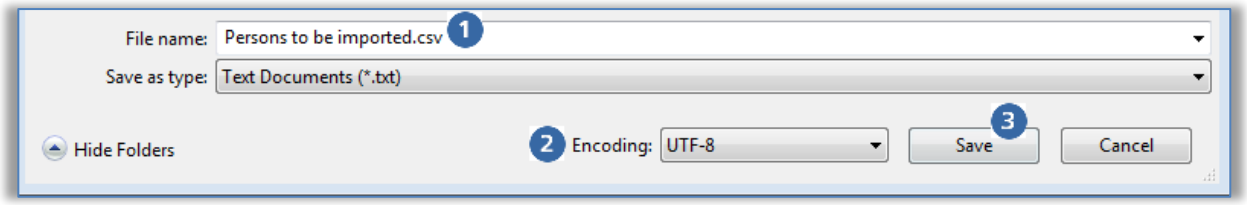


Figura 36: "Editor" – Guardar como – Introducción manual del final del archivo .csv y selección de la codificación UTF-8.

> El archivo CSV creado de esta forma puede importarse a continuación en la Administración online AirKey.

El archivo CSV puede abrirse directamente con Excel. NO realice ninguna modificación en el archivo CSV en Excel; ya que al guardar, la codificación UTF-8 se modificaría.

Pueden realizarse cambios de poca importancia posteriormente en los datos personales del archivo CSV, si dicho archivo se abre y a continuación se guarda p. ej. con ***Editor***.

Para realizar cambios de mayor alcance en los datos personales se recomienda adaptar los datos en el archivo Excel original y repetir todo el proceso para la creación del archivo CSV en formato UTF-8.

Importar archivo CSV en formato UTF-8 en la Administración online de AirKey

Para importar un archivo CSV con datos de personas, proceda así:

> En la página de inicio ***Home***, elija la opción ***Personas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Personas***.

> Haga clic a la derecha en ***Importar*** ❶.

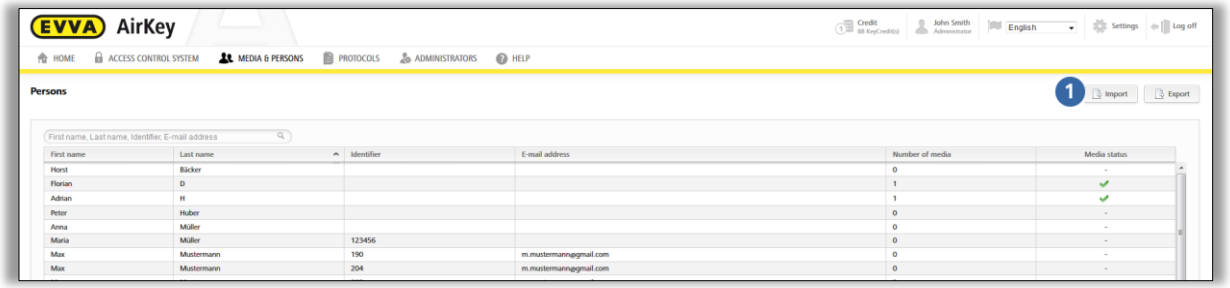


Figura 37: Importar personas

> Elija ***Seleccionar archivo***.

> Seleccione el archivo CSV que desea importar.

> Obtendrá una vista general de las personas que se van a importar.

> Haga clic en ***Iniciar importación*** ❶.

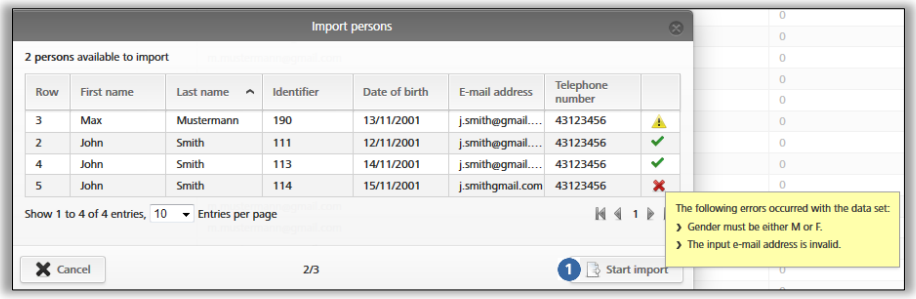


Figura 38: Importar personas

- Recibirá un mensaje con el número de personas que se ha podido importar correctamente y del número de filas erróneas que había.
- Haga clic en ***Cerrar***.

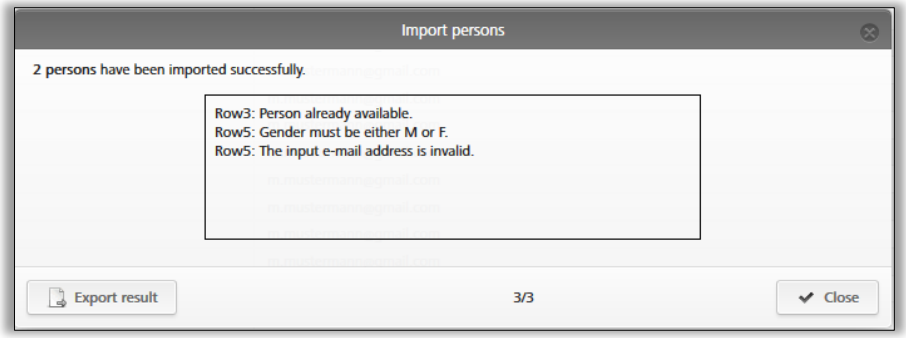


Figura 39: Importar personas – Resultado

- En la Administración online de AirKey, se le redirigirá automáticamente a la lista general de las personas.
- Para asignar las autorizaciones de acceso deseadas a las personas correspondientes, se puede realizar como siempre para cada persona como se describe en Asignar medio a una persona. Las autorizaciones de acceso idénticas se pueden duplicar de forma rápida y sencilla. Tiene información al respecto en Duplicar medio.

4.8 Crear smartphone

Para gestionar un smartphone en su sistema de control de accesos, deberá antes crearlo o añadirlo.

- En la página de inicio ***Home***, en la barra gris del bloque ***Medios y personas***, haga clic en ***Añadir*** → ***Añadir medio***.
- O en la página de inicio ***Home***, elija la opción ***Smartphones*** → ***Añadir medio***.
- O en el menú principal, elija ***Medios y personas*** → ***Añadir medio***.

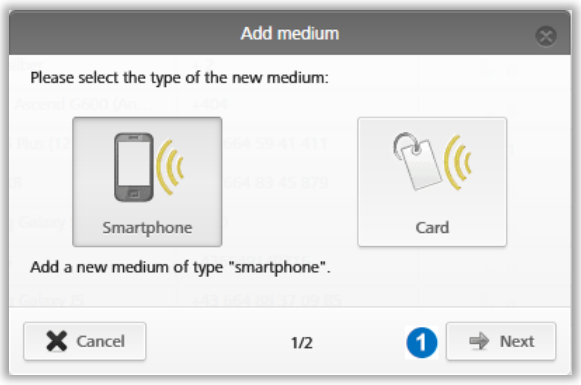


Figura 40: Nuevo medio, smartphone o tarjeta

> Elija como nuevo medio ***Smartphone*** y haga clic en ***Siguiente*** ❶.
> En el campo de denominación, introduzca la información pertinente (p. ej. el tipo de smartphone).
> Introduzca el número de teléfono del smartphone. El número de teléfono debe comenzar con **+** y el prefijo del país, y puede contener un máximo de 50 caracteres (+, 0-9 y espacios).
> Haga clic en ***Añadir medio*** ❶.

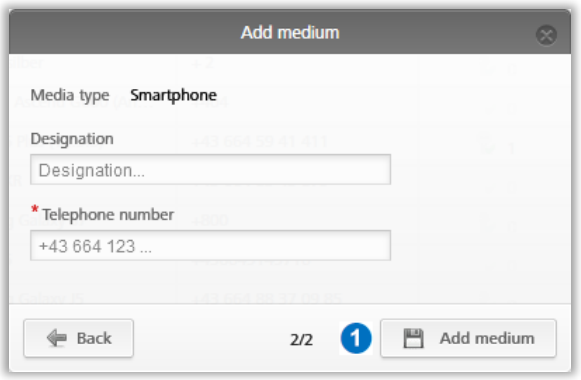


Figura 41: Crear nuevo medio

Si el teléfono no es válido o ya ha sido añadido previamente, recibirá un mensaje de error.

Se encuentra ahora en los detalles para este smartphone.

> Haga clic en ***Crear nuevo código de registro*** ❶ si todavía no se ha creado un código de registro.

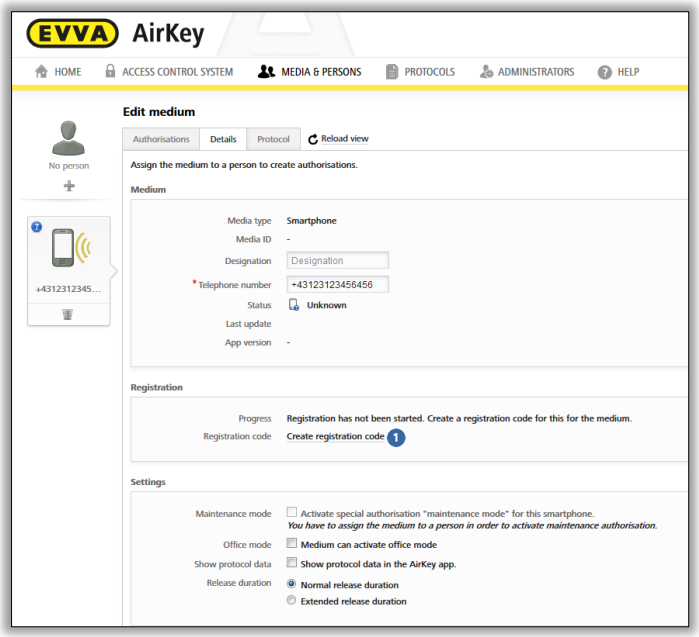


Figura 42: Crear código de registro

En el bloque ***Registro*** se mostrará un código de registro válido con su fecha de caducidad. Puede enviarlo también por SMS. Para ello, debe hacer clic solo en el vínculo correspondiente. Entonces se muestra la fecha y hora exactas en que se envió el código de registro por SMS.

Figura 43: Código de registro

En el bloque ***Ajustes*** dentro de los detalles del smartphone, puede definir los continuars ajustes:

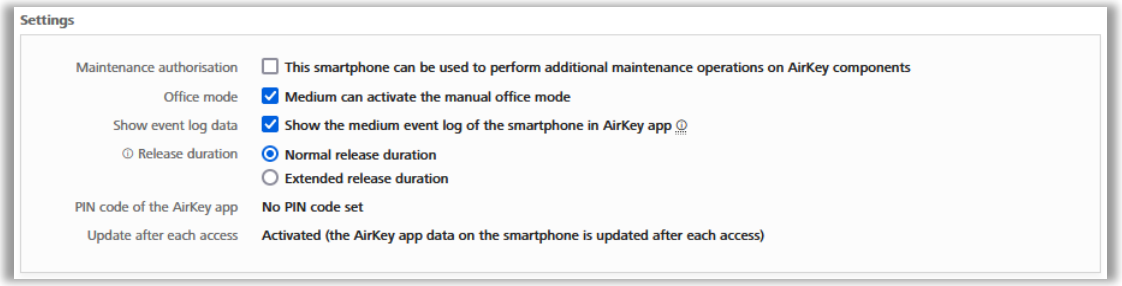


Figura 44: Editar medio – Ajustes

- **Autorización de mantenimiento:** Esta autorización especial solo se puede activar en smartphones a los que ya se les ha asignado una persona. Con esta función, el smartphone recibirá la autorización para desbloquear componentes de cierre en estado de fábrica, así como para añadir y eliminar componentes de cierre y medios en el

sistema de control de accesos. Además, podrá actualizar el firmware de los componentes de cierre y los medios.

- **Este medio puede activar la apertura permanente manual:** Si se ha seleccionado esta opción, el medio de acceso puede cambiar al componentes de cierre al estado de apertura permanente automática. Sin embargo, el medio debe tener una autorización válida para el componentes de cierre.
- **Mostrar lista de eventos del smartphone en la app de AirKey:** Con esta opción, podrá ver el usuario sus propios eventos de acceso, así como otros datos de la lista de eventos relevantes para su medio.
- **Período de apertura:** Fija cuánto dura la activación del componentes de cierre ante una apertura con este smartphone. La duración de la activación normal o ampliada se determine en el componentes de cierre (de 1 a 250 segundos).
- **Código PIN de la app de AirKey:** Indica si este smartphone tiene activado el bloqueo de código PIN o no en la app de AirKey. Si está activado y la persona olvida su código PIN, se puede restablecer.
- **Actualización después de cada acceso:** Indica si los datos de la app de AirKey de este smartphone se actualizarán o no automáticamente en cada proceso de acceso. Encontrará información detallada sobre la activación de esta función en el capítulo Aspectos generales.

4.9 Registrar smartphone

El smartphone se puede registrar cuando está creado dentro de un sistema de control de accesos y conoce el código de registro.

- Inicie la app de AirKey en su smartphone.
- Acepte el acuerdo de licencia así como los permisos de acceso a determinados servicios del smartphone.
- Si el smartphone todavía no está vinculado a ningún sistema AirKey, aparecerá automáticamente el cuadro de diálogo para la introducción del código de registro.

En smartphones con iOS, elija ***Código de registro recibido***, para saltarse el paso de introducir el número de teléfono y pasar a la introducción del código de registro.

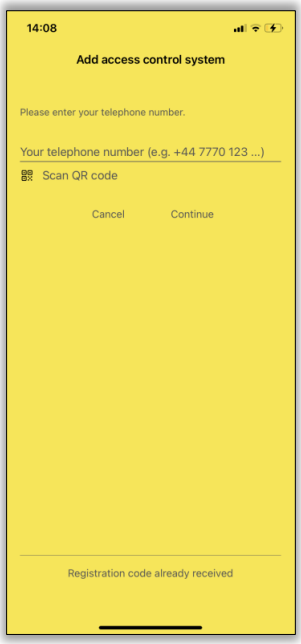


Figura 45: App de AirKey – Añadir sistema de control de accesos (iOS)

> Introduzca el código de registro recibido del administrador del sistema de control de accesos.

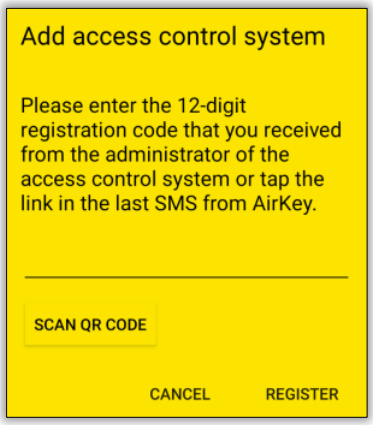


Figura 46: App de AirKey – Añadir sistema de control de accesos (Android)

> Confirme la entrada con ***Registrar***.

También puede registrar un smartphone en varios sistemas AirKey. Para volver a abrir el cuadro de diálogo del registro, elija en el menú principal de la app de AirKey ***Ajustes*** → ***Añadir sistema de control de accesos***. Encontrará más información al respecto en el capítulo Utilizar smartphone en varios sistemas.

Si el código de registro es incorrecto o ha caducado, recibirá un mensaje de error. En este caso, póngase en contacto con el administrador del sistema de quien recibió el código de registro.

El botón ***Escanear código QR*** solo es necesario en relación con un reemplazo de smartphone. Encontrará más detalles sobre el reemplazo de smartphone en el capítulo Reemplazo de smartphone.

Si se borran la app de AirKey o sus datos, existe la posibilidad de transferir de nuevo las autorizaciones ya expedidas sin necesidad de usar el crédito. No obstante, solo será así si se trata del mismo dispositivo y de su sistema de control de accesos. Si cambia de móvil, no será posible. Encontrará información sobre el cambio sencillo de equipos en el capítulo Reemplazo de smartphone.

- En la página de inicio ***Home***, elija la opción ***Smartphones***.
- O en la fila de encabezado, elija ***Medios y personas*** → ***Medios***.
- En la lista general, haga clic en el smartphone del que se trate.
- Haga clic en ***Crear nuevo código de registro*** y comuníquelo a la persona que desea registrar su smartphone en el sistema de control de accesos. O envíelos directamente por SMS al smartphone.
- Introduzca el código de registro en la app de AirKey; el smartphone se registrará en el sistema de control de accesos.

Si su smartphone estaba registrado en un sistema de control de accesos y no fue eliminado de manera correcta, si los datos de la app no se borraron o si el smartphone está registrado en un sistema de control de accesos externo, aparecerá un mensaje informando que el smartphone ya estaba registrado en otro sistema de control de accesos. Si ignora este mensaje, el smartphone se podrá registrar de la manera conocida. Se creará como un medio nuevo y todos los datos previos no serán válidos.

EVVA recomienda utilizar un PIN. Este ofrece un nivel más de seguridad y se podrá activar o desactivar más adelante. Encontrará más información en Activar PIN.

4.9.1 Función "Send a Key"

A todas las personas que tienen un smartphone, puede enviarles una "llave" a través de la función "Send a Key". Un administrador puede usar esta función para evitarle al usuario del smartphone la entrada manual del código de registro para un nuevo sistema de control de accesos.

- Haga clic en el botón **"*Send a Key*"**.

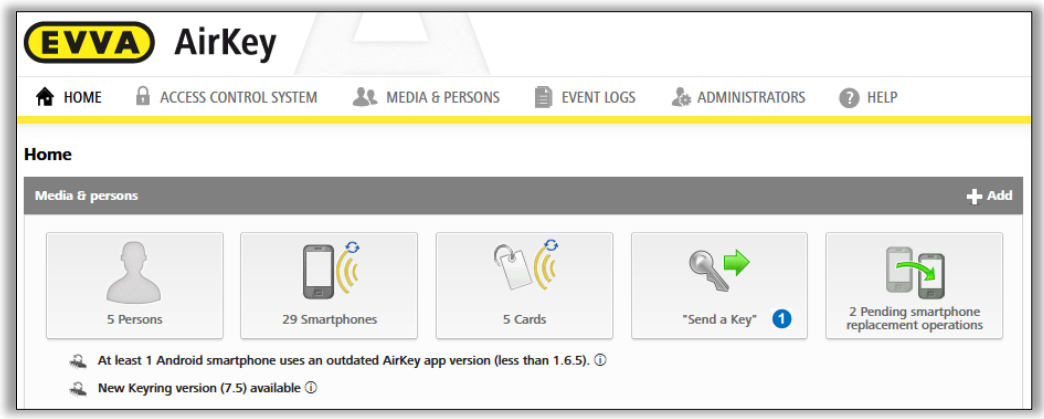


Figura 47: "Send a Key"

> Introduzca un nombre de persona, identificación, etc. en el campo de búsqueda. Si sabe que la persona no se ha creado aún, elija ***Crear a partir de cero***.

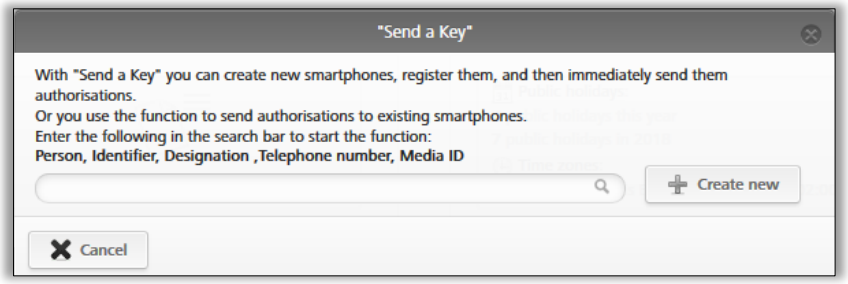


Figura 48: "Send a Key" – Campo de búsqueda

> Una vez cumplimentados todos los campos obligatorios, haga clic en ***Continuar***. Se enviará de inmediato un SMS a la persona de destino donde se incluirá un vínculo con el código de registro de la app de AirKey. Si en los ajustes generales se ha seleccionado un texto propio para el SMS de «Send a Key», aquí también se puede adaptar o personalizar de nuevo el texto del SMS. (Encontrará información sobre los ajustes generales en el capítulo Aspectos generales)

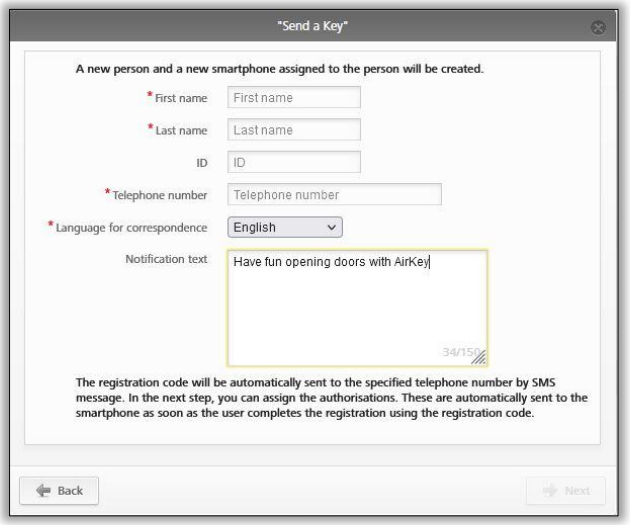


Figura 49: "Send a Key" – Crear persona

Según la disponibilidad de la red del smartphone, la recepción del SMS con el código de registro puede tardar algo.

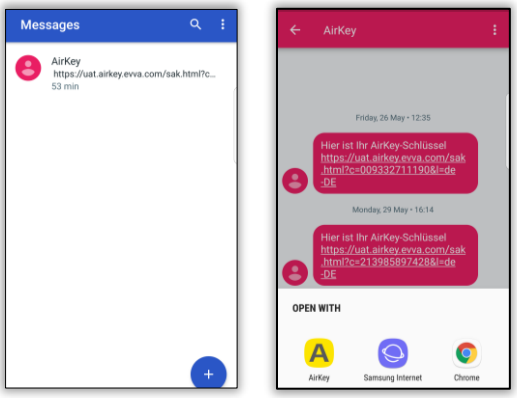


Figura 50: SMS con vínculo – aquí se muestra con el Samsung Galaxy S7 Edge

> Tras abrir el enlace del SMS con ayuda de AirKey, se inicia y realiza automáticamente el registro.

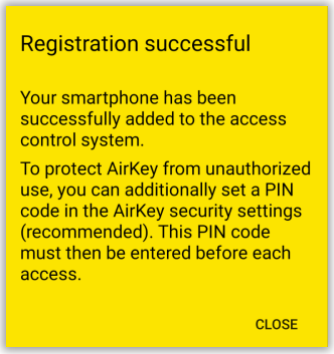


Figura 51: Registro correcto

Si aún no se ha instalado la app de AirKey en el smartphone, se procederá como sigue:

> Haga clic en el enlace del SMS e instale la app en el smartphone.

> Inicie la app de AirKey.

> En el caso de smartphones con Android, se inicia y realiza automáticamente el registro. En el caso de smartphones con iOS, introduzca su número de teléfono y confirme con ***Continuar***. (El botón ***Escanear código QR*** solo es necesario en relación con un reemplazo de smartphone. Encontrará más detalles sobre el reemplazo de smartphone en el capítulo Reemplazo de smartphone).

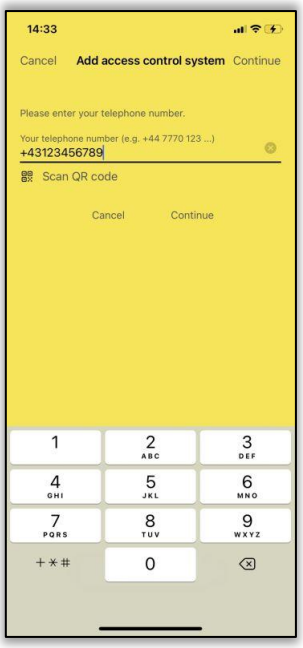


Figura 52: Introducir número de teléfono (iOS)

> Recibirá otro SMS. Pero continúe en la app de AirKey y seleccione el código de registro de 8 dígitos que aparece encima del teclado.

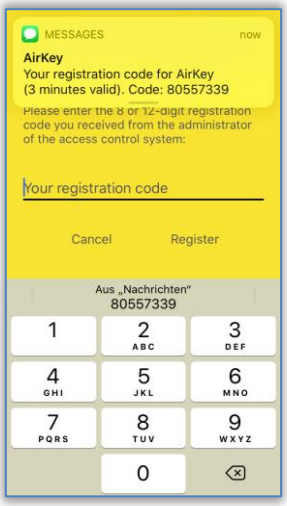


Figura 53: Código de registro (iOS)

Si no se muestra como sugerencia el código de registro de ocho dígitos, o si mientras tanto ha cerrado usted la app de AirKey, deberá copiar el código de registro de 8 dígitos del SMS e introducirlo en la app de AirKey.

> Concluya el registro con ***Registrar***.

En la Administración online de AirKey, se le redirige en la vista de autorizaciones a ***Editar medio*** y puede crear las autorizaciones deseadas. Con la función de arrastrar y soltar, mueva el componentes de cierre correspondiente para el que se debe conceder la autorización de acceso, al tipo de acceso deseado (acceso permanente, acceso temporal, acceso periódico, acceso personalizado); consulte también Otorgar autorizaciones.

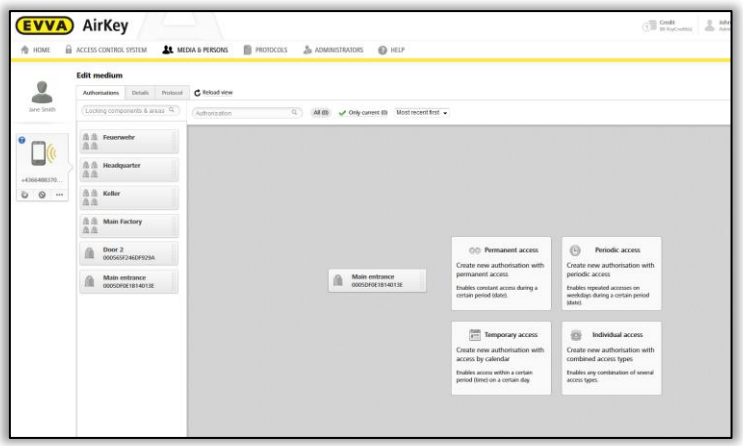


Figura 54: Tipos de acceso

4.10 Instalar componentes de cierre

4.10.1 Cilindros de AirKey

Para el montaje del cilindro / cilindro híbrido / cilindro de buzón / candado AirKey, siga las instrucciones de montaje que vienen en la caja, o el vídeo de montaje que se encuentra en https://www.evva.com/es/airkey/website/.

Para un cilindro de AirKey con acceso por ambos lados, tenga en cuenta que ambos lados tienen que estar configurados en el sistema de control de accesos para evitar quedar encerrado accidentalmente.

4.10.2 Lectores murales de AirKey

Para el montaje del lector mural de AirKey, utilice el manual de montaje incluido en la caja. Además podrá encontrar en nuestra página de inicio una plantilla de taladrado, así como el vídeo de montaje https://www.evva.com/es/airkey/website/.

Por cada lector mural, se requerirá una unidad de control. La unidad de control se deberá instalar en el interior para mayor seguridad. Compruebe el cableado en el lector mural y en la unidad de control.

Los componentes de cierre vienen siempre en estado de fábrica.

- Los medios en estado de fábrica podrán bloquear los componentes de cierre en estado de fábrica.
- Los smartphones que tengan la app de AirKey instalada y autorización de mantenimiento también podrán bloquear componentes de cierre en estado de fábrica.
- En estado de fábrica no se registrarán los intentos de apertura.
- Se da una autorización de apertura después de haber añadido el componentes de cierre a un sistema de control de accesos.
- Tenga en cuenta durante el montaje las observaciones del manual de montaje. En el montaje o desmontaje de los componentes de

cierre, abra la puerta y fíjela de forma que no pueda cerrarse por descuido.

4.11 Añadir componente

Los componentes de cierre se añaden al sistema de control de accesos a través de un smartphone con autorización de mantenimiento o una estación codificadora opcional. Para ello, deberán estar en estado de fábrica.

Si quiere usar un smartphone, deberá tener en cuenta los continuars requisitos:

- La app de AirKey debe estar instalada.
- Debe tener conexión a Internet.
- El smartphone está registrado en el sistema de control de accesos.
- El smartphone está asignado a una persona.
- La autorización de mantenimiento fue asignada al smartphone.

4.11.1 Añadir componentes de cierre con el smartphone

- Inicie la app de AirKey.
- Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.
- Establezca la conexión a través de **Bluetooth** (en smartphones **Android**): En el componentes de cierre en estado de fábrica que quiera añadir al sistema de control de accesos, seleccione el menú contextual (⋮) y elija entonces ***Conectar*** ❷.
- Establezca la conexión a través de **Bluetooth** (en **iPhones**): En el componentes de cierre en estado de fábrica que quiera añadir al sistema de control de accesos, en la identificación "En estado de fábrica" deslícese a la izquierda y elija ***Conectar*** ❸.

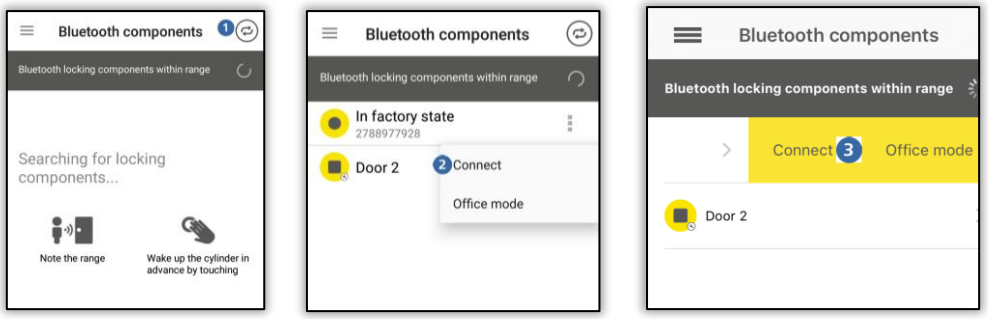


Figura 55: App de AirKey – Conectar con componente (a través de NFC en smartphone de Android / a través de Bluetooth en smartphone de Android / a través de Bluetooth con iPhone)

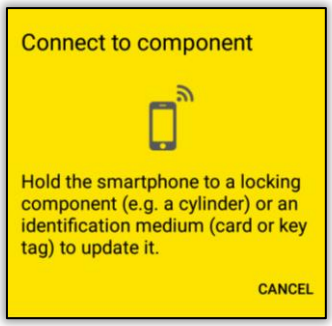


Figura 56: App de AirKey – Conectar con componente

> Mantenga el smartphone junto al componente de cierre en estado de fábrica (en caso de conexión mediante NFC) para establecer una conexión. La conexión se establece automáticamente mediante Bluetooth. Se creará una conexión con el componentes de cierre. No retire el smartphone del componentes de cierre durante la conexión en ningún caso.

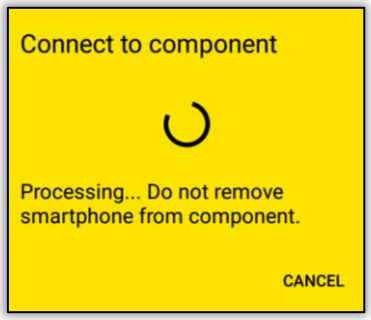


Figura 57: App de AirKey – Estableciendo la conexión

> En este momento, recibirá información del componentes de cierre.

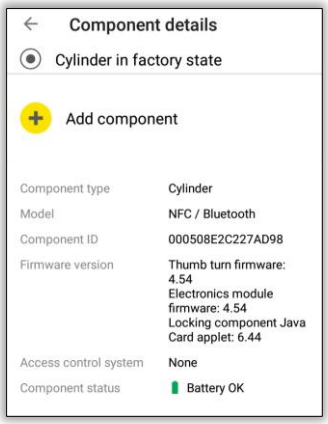


Figura 58: Añadir componente

> Elija ***Añadir componente***.

> Introduzca una denominación única para el componentes de cierre.

Para un cilindro con acceso por ambos lados, deberá tener en cuenta que ambos lados estén configurados dentro del sistema de AirKey. Utilice una denominación clara y única para ambos lados del cilindro con doble acceso.

Cree un área que incluya ambos lados del cilindro y otorgue una autorización de área para tener la misma autorización en ambos lados.

> Si el smartphone está registrado en varios sistemas AirKey con modo de mantenimiento activo, elija el sistema de control de accesos en el que se debe añadir el componentes de cierre.

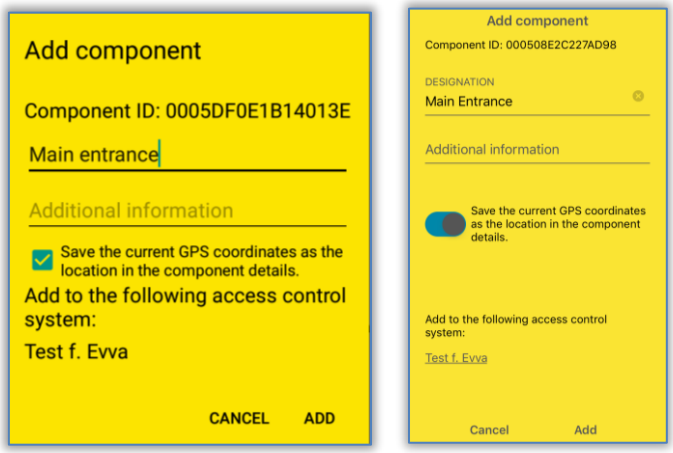


Figura 59: App de AirKey – Añadir componentes de cierre (Android / iPhone)

> Seleccione ***Añadir***.

> Mantenga el smartphone de nuevo junto al componente de cierre en estado de fábrica (en caso de conexión mediante NFC) para establecer una conexión. La conexión se establece automáticamente mediante Bluetooth.

Se comprobarán los datos y se actualizará el componentes de cierre.
No retire el smartphone del componentes de cierre durante este proceso.

> El proceso finalizará con un mensaje de confirmación. El componentes de cierre se encuentra ahora disponible en la Administración online de AirKey para su gestión ahí.

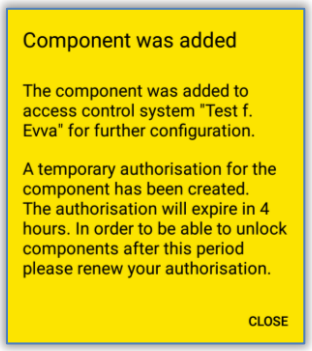


Figura 60: App de AirKey – Componentes de cierre añadido

El componentes de cierre aparece en la lista general de componentes de cierre en la Administración online de AirKey. Si se determinaron las coordenadas GPS ❶ al añadir el componentes de cierre, en la Administración online de AirKey se pueden encontrar en el bloque "Puerta" dentro de la pestaña ***Detalles*** en el componentes de cierre.

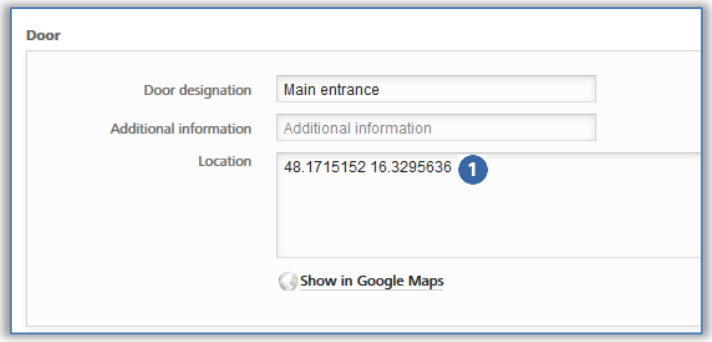


Figura 61: Coordenadas GPS en los detalles del componentes de cierre

También se puede introducir la dirección en el campo "Ubicación" donde se encuentra el componentes de cierre.

El componentes de cierre ya no se encuentra en estado de fábrica. Por ello, los medios en estado de fábrica o los smartphones con modo de mantenimiento dejarán de estar autorizados. El smartphone que ha añadido el componentes de cierre, quedará autorizado automáticamente para 4 horas. Modifique a tiempo esta autorización u otorgue a otros medios una autorización válida para poder mantener el acceso al componentes de cierre.

4.11.2 Añadir componentes de cierre con la estación codificadora

Option

Para añadir el componentes de cierre con la estación codificadora, proceda de la continuar manera:

- En la página de inicio ***Home***, elija la opción ***Cilindros*** o ***Lectores murales***.
- Haga clic en el botón ***Añadir componente*** ❶.
- También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.

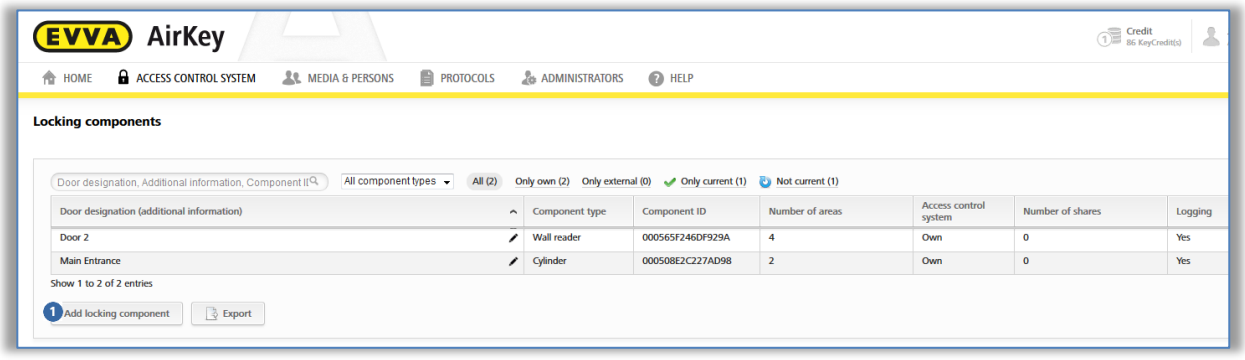


Figura 62: Añadir componentes de cierre

- Conecte la estación codificadora al ordenador; de lo contrario, aparecerá un aviso del sistema ❶.

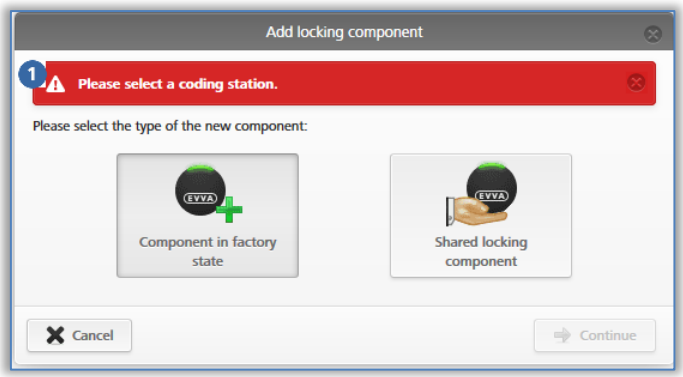


Figura 63: Añadir componentes de cierre / no hay estación codificadora.

> Elija ***Componentes en estado de fábrica***.

> Haga clic en ***Continuar***.

> En el continuar cuadro de diálogo, introduzca la identificación de la puerta y haga clic en ***Continuar***.

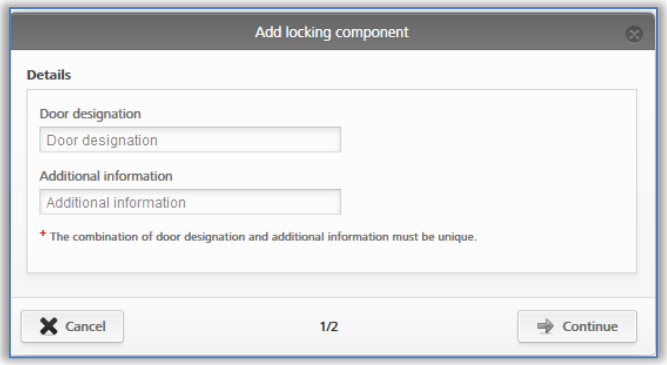


Figura 64: Añadir componentes de cierre – Asignación de nombre

> Siga las instrucciones y sostenga el componente junto a la estación codificadora.

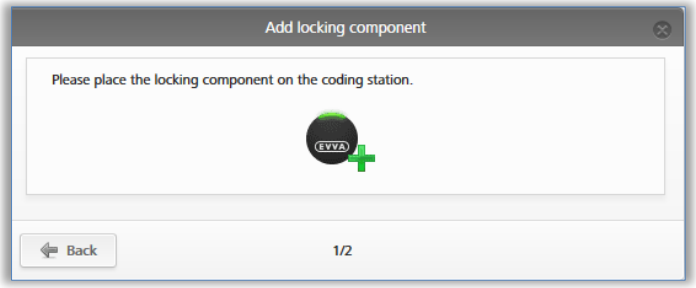


Figura 65: Añadir componentes de cierre

> Aparecerá un mensaje de confirmación, y el componentes de cierre se ha añadido al sistema de control de accesos.

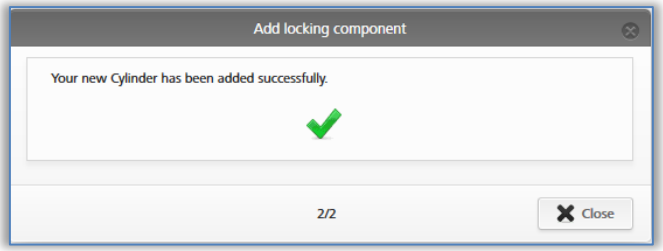


Figura 66: Añadir componentes de cierre – Mensaje de confirmación

Después de cerrar el mensaje de confirmación, aparecerá una vista detallada del componentes de cierre.

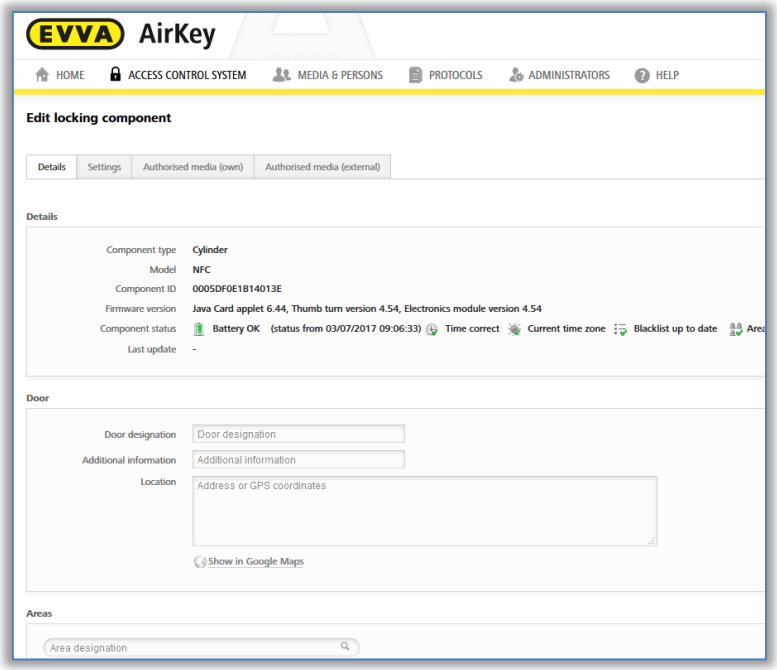


Figura 67: Detalles del componentes de cierre

El componentes de cierre ya no se encuentra en estado de fábrica. Por ello, los medios en estado de fábrica o los smartphones con autorización de mantenimiento ya no podrán bloquear el componentes de cierre. Añada un medio o smartphone al sistema de control de accesos y otorgue una autorización válida al componentes de cierre para poder seguir bloqueándolo.

Los ajustes de la zona horaria y de protección de datos se configuran automáticamente para el componentes de cierre añadido según la configuración seleccionada. Tiene más información sobre estos ajustes en Valores predeterminados (para todos los componentes de cierre añadidos recientemente).

También puede situar un componentes de cierre en estado de fábrica sobre la estación codificadora. En la parte inferior derecha, aparecerá una ventana de información a través de la cual podrá también añadir el componentes de cierre en el sistema de control de accesos mediante el vínculo ***Añadir componentes a mi sistema de control de accesos***.

Figura 68: Añadir componente a mi sistema de control de accesos

4.12 Añadir tarjetas, llaveros, pulseras y llaves combi con el smartphone

Los medios de acceso en estado de fábrica se añaden al sistema de control de accesos mediante un smartphone con autorización de mantenimiento o una estación codificadora opcional.

Para añadir una llave combi con un smartphone, deberá presentar la llave combi al smartphone en el lado en el que se encuentre el símbolo RFID. La llave combi deberá sostenerse directamente junto al smartphone en la mayoría de los modelos.

Esta acción solo se puede realizar con un smartphone de Android que tenga NFC. Para añadir medios a un smartphone de Android o iPhone mediante Bluetooth, consulte el capítulo Codificar medios.

> Inicie la app de AirKey.

> Seleccione el símbolo ***Conectar con componente*** ❶.

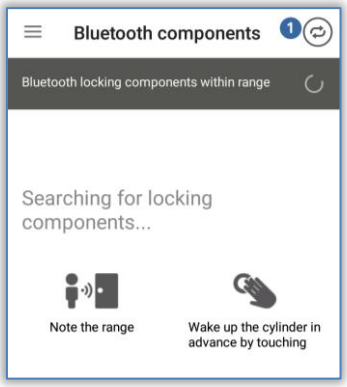


Figura 69: App de AirKey – Conectar con componente

> Mantenga el smartphone junto al medio en estado de fábrica.
Se creará una conexión con el medio.

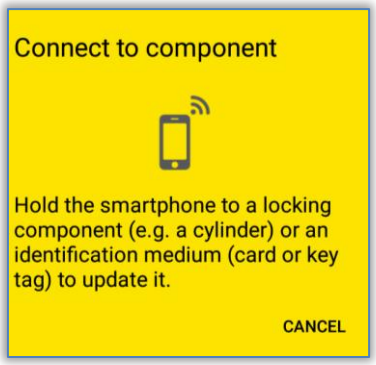


Figura 70: App de AirKey – Estableciendo la conexión

> No retire el smartphone del medio durante la conexión en ningún caso. Recibirá en este momento información del medio.

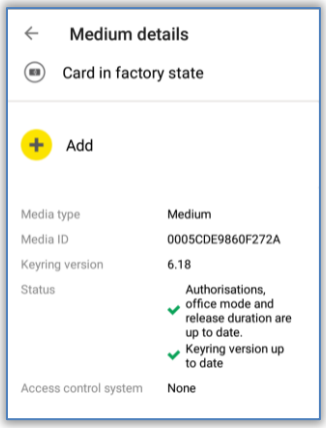


Figura 71: Detalles del medio

> Seleccione ***Añadir.***
> Introduzca una denominación para el medio.

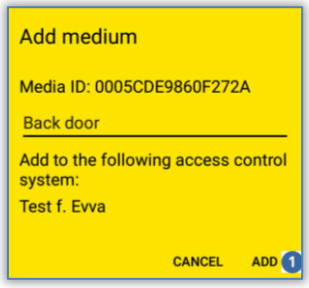


Figura 72: Añadir medio – Determinar denominación

> Si el smartphone está registrado en varios sistemas AirKey, elija aquel en el que se debe añadir el medio.
> Seleccione ***Añadir*** ❶.
> Presente de nuevo el smartphone junto al medio para finalizar el proceso.
> El proceso finalizará con un mensaje de confirmación. El medio está disponible ahora en la Administración online de AirKey, y se debe asignar aún a una persona.

Este proceso es el mismo para tarjetas, llaveros, pulseras y llaves combi. Los tres están bajo la denominación "tarjeta".

4.13 Asignar un medio a una persona

En el continuar paso, deberá asignar el medio a una persona dentro de la Administración online de AirKey para poder otorgar autorizaciones. Solo así tendrá una referencia personal en los accesos.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> En la lista de medios, haga clic en aquel que no esté asignado aún a una persona.

> En el botón ***Ninguna persona***, haga clic en el símbolo **+** ❶

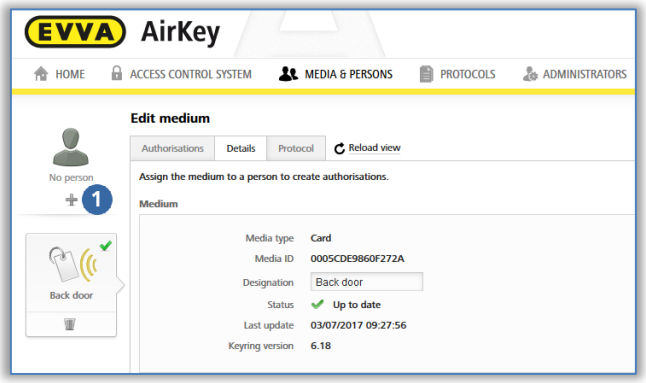


Figura 73: Asignar persona

> En la lista de personas, seleccione aquella a la que se debe asignar el medio.

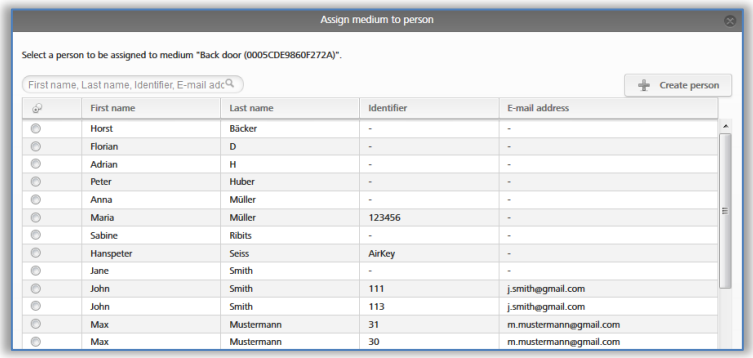


Figura 74: Asignar persona a medio

> Si no se ha creado aún la persona deseada, existe el botón ***Crear persona*** con el accederá a la segunda ventana de diálogo "Asignar medio a persona".

> Confirme la persona seleccionada a la que se debe asignar el medio, con ***Asignar persona*** ❶.

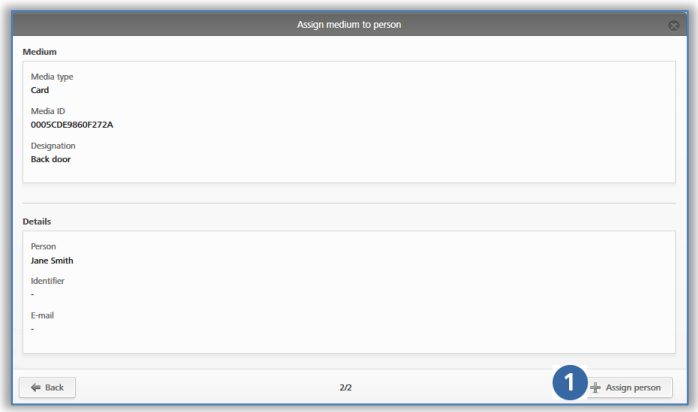


Figura 75: Confirmar persona

> Consulte también Otorgar autorizaciones.

También puede asignar el medio a una persona a través del medio. Encontrará más información en Asignar medio a una persona.

4.14 Otorgar autorizaciones

Tenga en cuenta que solo podrá otorgar autorizaciones si el medio ha sido asignado a una persona.

> En el menú principal, elija ***Medios y personas*** → ***Medios***.

> Haga clic en el medio deseado en la lista general.

> Si el medio está asignado a una persona, aparecerá una vista general de las autorizaciones del medio.

> En cuanto seleccione el componentes de cierre correspondiente y lo arrastre a la superficie azul, aparecerán los posibles tipos de acceso en las cuatro superficies de borde punteado.

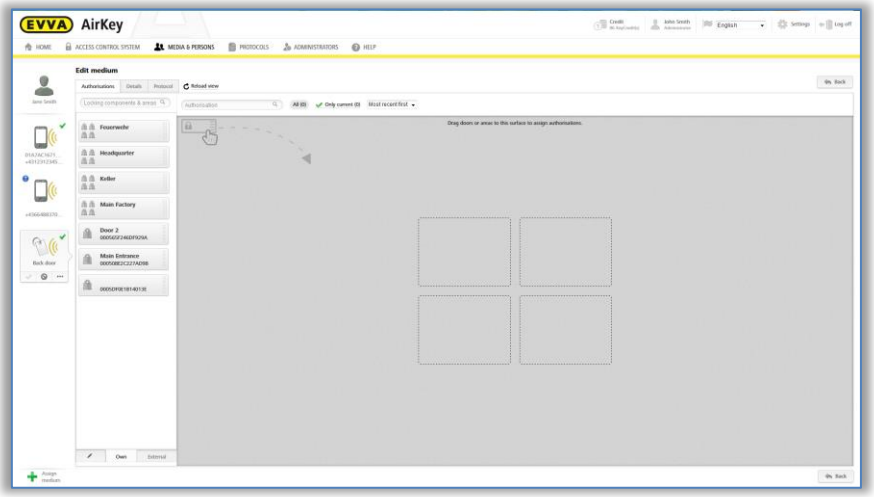


Figura 76: Otorgar autorizaciones

> Elija el tipo de acceso deseado arrastrando y soltando la puerta/área sobre el campo deseado.

Hay cuatro tipos de accesos posibles:

- Acceso permanente
- Acceso periódico
- Acceso temporal
- Acceso individual

4.14.1 Acceso permanente

Acceso permanente significa que el acceso será posible en cualquier momento. Una limitación de la autorización es posible si selecciona una fecha de comienzo y de finalización.

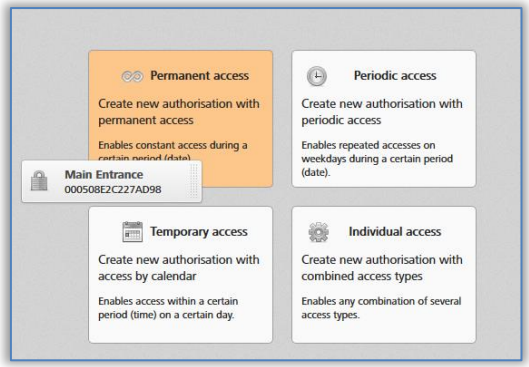


Figura 77: Otorgar autorización de acceso permanente

> Fije el período temporal para el acceso permanente. Puede elegir un período ilimitado o un acceso permanente con fecha determinada de inicio y fin.

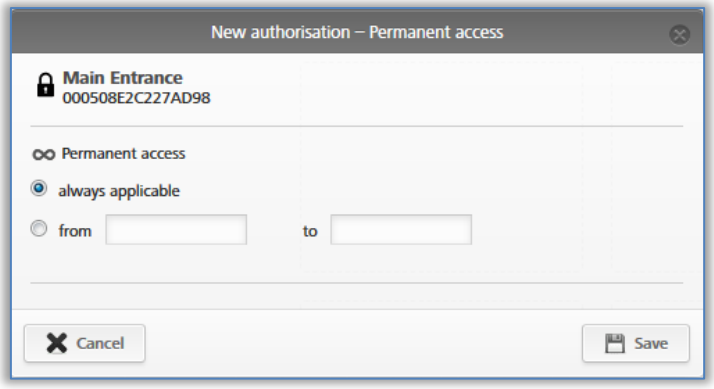


Figura 78: Otorgar autorización de acceso permanente

> Haga clic en ***Guardar***.

4.14.2 Acceso periódico

Otorgue una autorización de acceso periódico para los accesos que se repiten en un período de tiempo determinado. Este acceso periódico es comparable a un evento periódico que tenga lugar semanalmente.

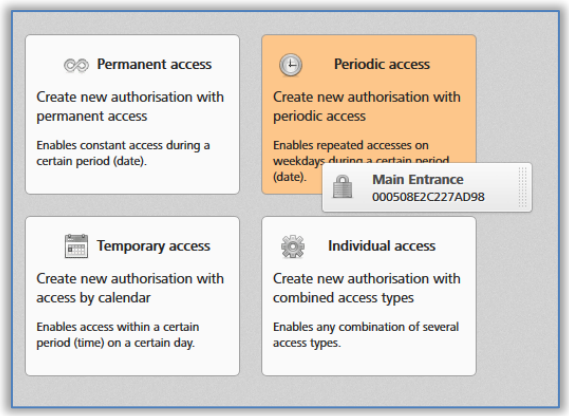


Figura 79: Otorgar acceso periódico.

Se mostrará la vista del calendario semanal, en el que se pueden determinar hasta 4 rangos de tiempo para cada día de la semana.

> Determine el período de tiempo para los accesos periódicos.

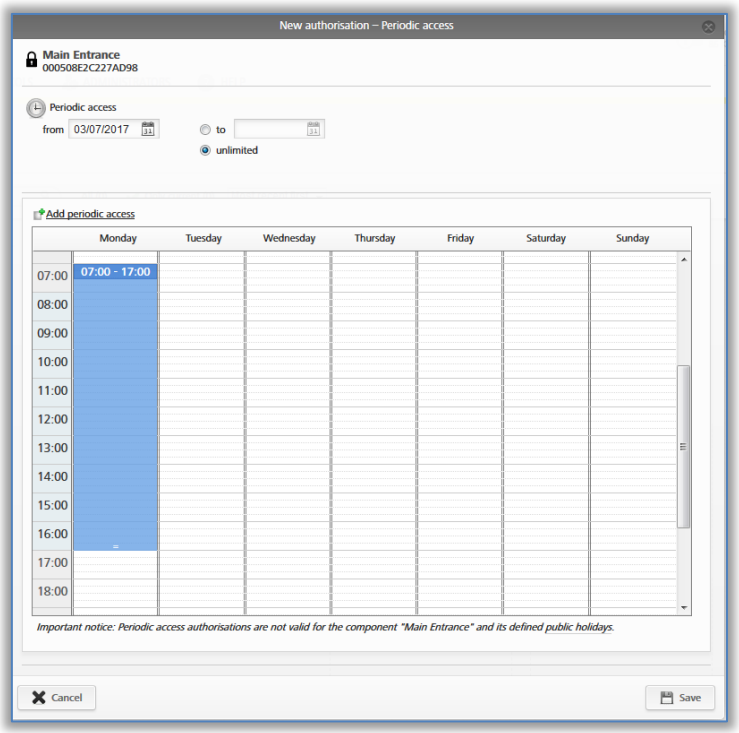


Figura 80: Otorgar acceso periódico.

> El período de tiempo se define marcando directamente en el calendario o a través de ***Añadir acceso periódico***.

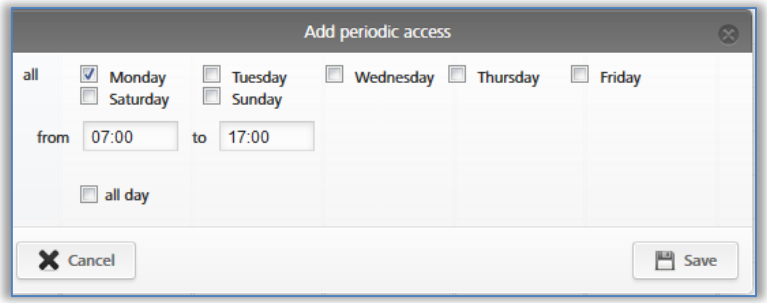


Figura 81: Añadir acceso periódico

> Asigne el período de tiempo deseado y haga clic en ***Guardar***.

> En la ventana "Nueva autorización – Acceso periódico", haga clic también en ***Guardar***.

4.14.3 Acceso temporal

Otorgue una autorización de acceso único cuando solo deba ser válida para un día en un determinado período de tiempo.

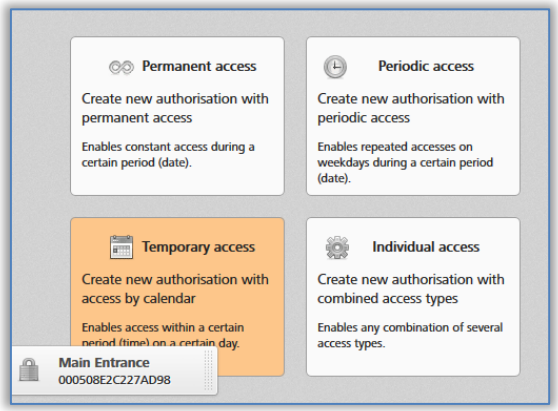


Figura 82: Otorgar autorización de acceso temporal

> Asigne el período de tiempo deseado y haga clic en ***Guardar***.

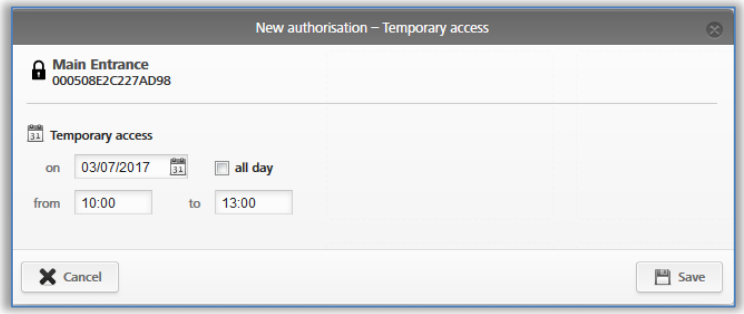


Figura 83: Otorgar autorización de acceso temporal

4.14.4 Acceso individual

Otorgue una autorización de acceso personalizado cuando necesite una combinación de acceso permanente, acceso único y acceso periódico.

Figura 84: Otorgar accesos personalizados

- En el cuadro de diálogo "Nueva Autorización – Acceso individual", verá los accesos personalizados asignados previamente.
- Haga clic en la entrada de una fila para cambiar la autorización.
- Haga clic en ***Añadir acceso*** ❶ para una nueva entrada.

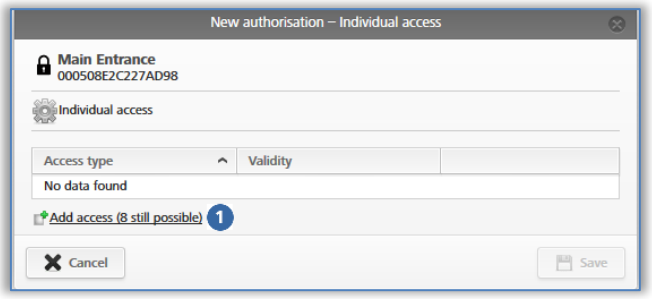


Figura 85: Nueva autorización – Acceso personalizado

- Elija ***acceso permanente***, ***acceso periódico*** o ***acceso temporal*** y defina los requisitos para cada caso. Los parámetros corresponden a las autorizaciones de acceso ya descritas.

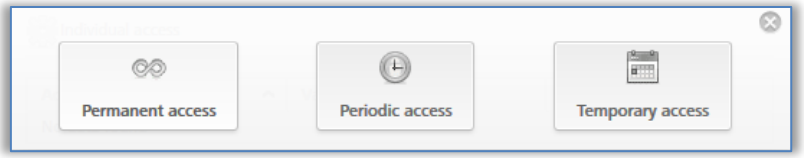


Figura 86: Nueva autorización – Acceso personalizado

- Cuando haya configurado todas las autorizaciones de acceso personalizado, haga clic en ***Guardar***.

- Los accesos permanentes y periódicos no deben solaparse.
- Se permite como máximo un acceso individual al día.
- Cuando un acceso individual y uno periódico se solapan, ambos son válidos.
- Puede combinar como máximo 8 autorizaciones personalizadas.

4.15 Crear autorización

Después de crear la autorización para un medio, tiene que finalizar el proceso haciendo clic en ***Crear autorización*** y actualizando el medio.

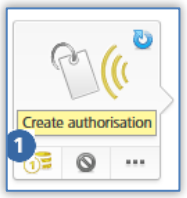


Figura 87: Crear autorización

Al cambiar una autorización o al crear una nueva, cambiará el símbolo del medio correspondiente. Si dispone de suficiente crédito, podrá crear la autorización.

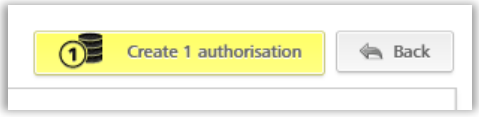


Figura 88: Crear autorización nueva o modificada

> Haga clic en el botón amarillo ***Crear 1 autorización*** o en el símbolo ❶ del medio para crear la autorización y deducir un KeyCredit.

Si no dispone de crédito en este paso, aparecerá el mensaje correspondiente. Puede aumentar el crédito haciendo clic directamente sobre el vínculo mostrado. Si aumenta el crédito a través del citado vínculo, se creará automáticamente la autorización, y en su caso, se deducirá un KeyCredit.

Para que las autorizaciones del medio tengan efecto, los medios como tarjetas, llaveros o llaves combi se deberán actualizar a través de un smartphone o una estación codificadora. En los smartphones, las autorizaciones se envían mediante notificaciones Push.

En este capítulo, ha aprendido cómo inicializar un sistema de AirKey. Ha aprendido los primeros pasos en AirKey y, por ello, está en situación de administrar su sistema de AirKey. En los continuars capítulos, encontrará una descripción más detallada de las funciones específicas de la Administración online de AirKey, así como de la app de AirKey.

5 Administración online de AirKey

5.1 Inicio de sesión de AirKey

Se requiere iniciar sesión para configurar y gestionar el sistema de control de accesos AirKey.En los ajustes de la Administración online de AirKey se puede activar opcionalmente, para el inicio de sesión, una autenticación de dos factores. La activación se describe en el capítulo Ajustes del sistema de control de accesos AirKey.

Active la autenticación de dos factores para aumentar la seguridad de su sistema de control de accesos AirKey.

Los intentos fallidos de inicio de sesión se muestran en la página de inicio y se registran en el historial del sistema. La indicación en la página de inicio únicamente aparece si desde el último inicio de sesión se ha producido como mínimo un intento de inicio de sesión fallido.

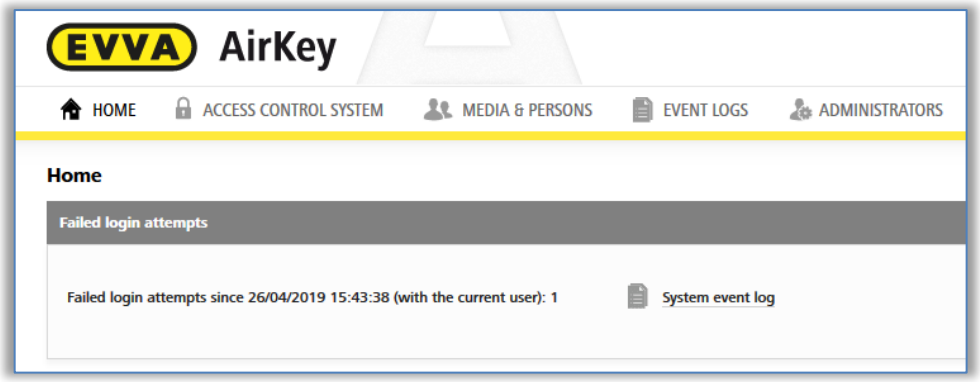


Figura89: Intentos de inicio de sesión fallidos

5.1.1 Inicio de sesión en AirKey sin autenticación de dos factores

- En el navegador, abra el sitio web https://airkey.evva.com.
  Se abre la página de inicio de sesión de la Administración online de AirKey.
- Introduzca la identificación de usuario que se le ha enviado en el e-mail "Registro de EVVA AirKey".
- Introduzca la contraseña que ha elegido y confirme con ***Iniciar sesión***.

Justo después del inicio de sesión, pasa a la página de inicio ***Home***. Aquí encontrará una visión general de su sistema de control de accesos.

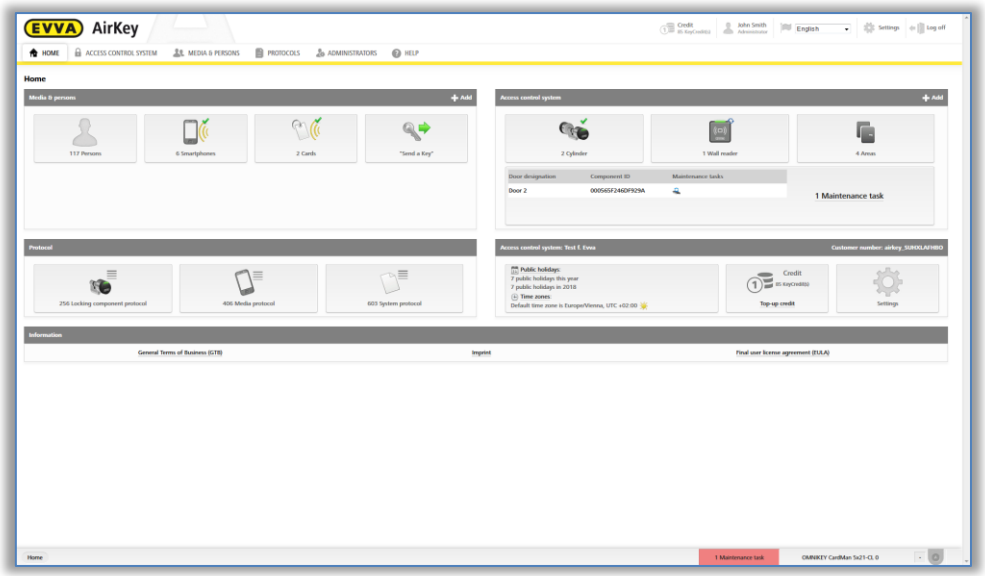


Figura 90: Administración online de AirKey – Home

5.1.2 Inicio de sesión en AirKey con autenticación de dos factores

- En el navegador, abra el sitio web https://airkey.evva.com.
  Se abre la página de inicio de sesión de la Administración online de AirKey.
- Introduzca la identificación de usuario que se le ha enviado en el e-mail "Registro de EVVA AirKey".
- Introduzca la contraseña que ha elegido y confirme con ***Iniciar sesión***.
- Si no existe aún un número de teléfono verificado para el administrador, aparece una notificación de que debe introducirse un número de teléfono para la verificación.
- Introduzca el número de teléfono del smartphone que deba emplearse para la autenticación de dos factores y confírmelo con ***Enviar código SMS***. El número de teléfono debe comenzar con **+** y el prefijo del país, y puede contener un máximo de 50 caracteres (+, 0-9 y espacios).

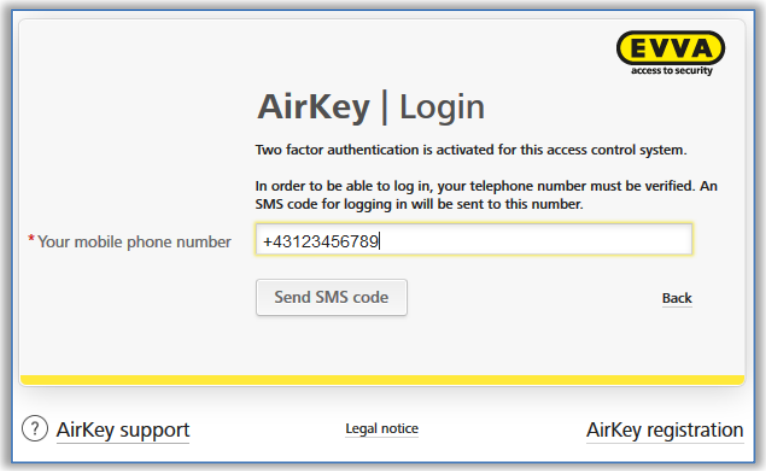


Figura91: Verificación del número de teléfono móvil durante el inicio de sesión

- Se enviará un SMS con un código SMS al número de teléfono indicado.

> Introduzca ese código SMS en el diálogo en la Administración online de AirKey y confirme con ***Iniciar sesión.***

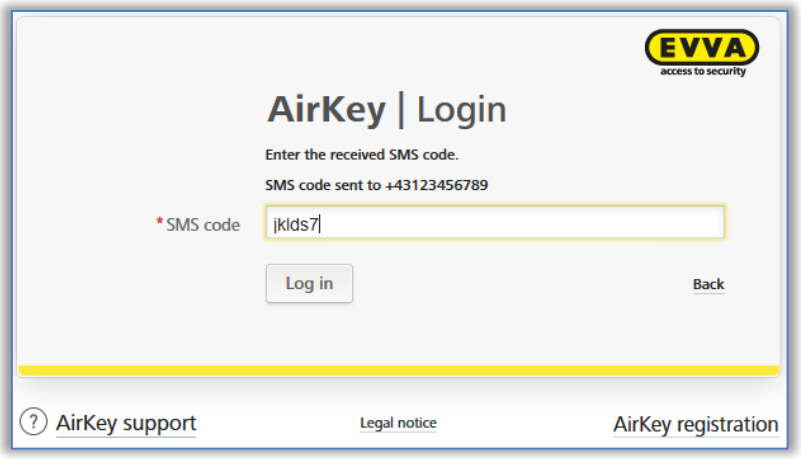


Figura92: Código SMS durante el inicio de sesión

> De esta manera el número de teléfono está verificado para la autenticación de dos factores y se mostrará en la página de inicio de su sistema de control de accesos AirKey.

Si el número de teléfono se había verificado ya, no hace falta volver a introducirlo tras introducir el identificador de usuario y la contraseña. En ese caso, se enviará inmediatamente un código SMS al número de teléfono verificado que debe introducirse en la Administración online de AirKey para el inicio de sesión.

El código SMS es válido durante 5 minutos. Si han pasado los 5 minutos, debe repetirse el proceso de inicio de sesión.

Sin acceso al número de teléfono verificado no puede realizarse un login en la Administración online de AirKey. Si desea cambiar el número de teléfono, debe modificarlo en los datos del administrador (véase Editar administrador). Para ello, es necesario, no obstante, el número de teléfono verificado en la actualidad. Si el número de teléfono ha dejado de estar disponible, póngase en contacto con el Soporte técnico de EVVA.

5.1.3 Contraseña olvidada

Si ha olvidado su contraseña, podrá restablecerla por sí mismo.
Haga clic en ***Contraseña olvidada*** ❶.

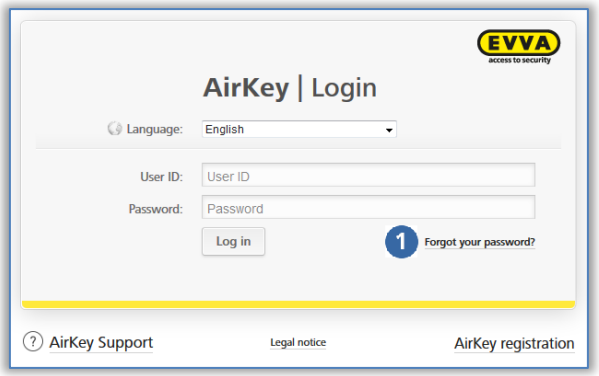


Figura 93: Página de inicio de sesión de la Administración online de AirKey

> En la ventana "¿Contraseña olvidada?", introduzca su identificación de usuario y la fecha de nacimiento introducida en el registro. Tras ello, haga clic en ***Restablecer contraseña***.

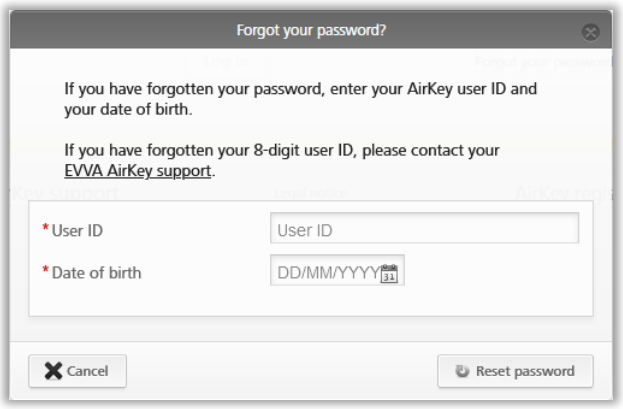


Figura 94: Contraseña olvidada

> Si se ha activado la autenticación de dos factores, recibirá un código SMS en su smartphone verificado que deberá confirmar en el siguiente diálogo y con ***Restablecer contraseña***. (Este paso se suprime si no está activada la autenticación de dos factores o si el número de teléfono no está verificado.)

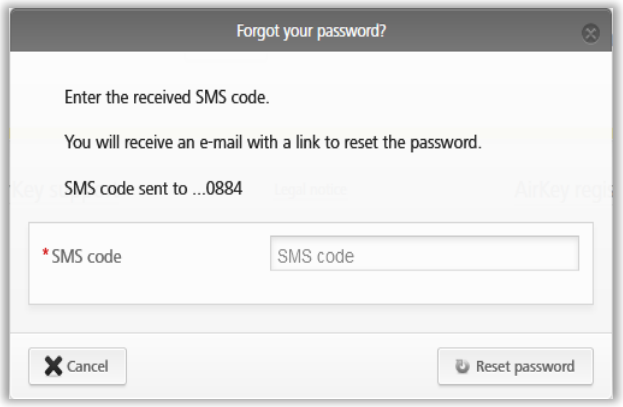


Figura95: Código SMS

El código SMS es válido durante 5 minutos. Si han pasado los 5 minutos, debe repetirse el proceso.

Sin acceso al número de teléfono verificado no puede concluirse el proceso. Si el número de teléfono ha dejado de estar disponible, póngase en contacto con el Soporte técnico de EVVA.

Recibirá un e-mail generado automáticamente por *EVVA AirKey* con el asunto "Administración online de EVVA AirKey – Restablecimiento de su contraseña".

> Abra el e-mail de *EVVA AirKey*.

> Haga clic en el vínculo para restablecer la contraseña. Se abrirá una el sitio web "Restablecer contraseña".

> Introduzca su nueva contraseña y confírmela de nuevo.

> Haga clic en ***Guardar***.

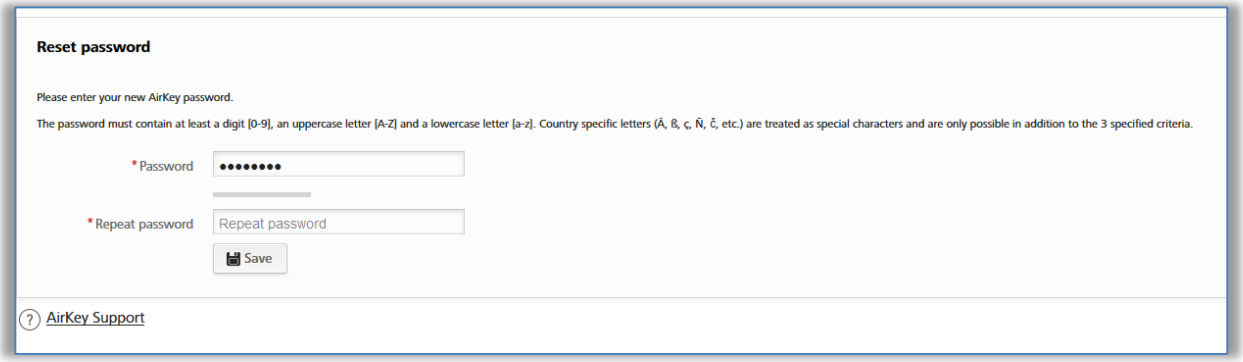


Figura 96: Restablecer contraseña de AirKey

Accederá a la página de inicio de sesión de la Administración online de AirKey.

> Realice el inicio de sesión como se describe en Inicio de sesión de AirKey sin autenticación de dos factores o Inicio de sesión de AirKey con autenticación de dos factores, con la nueva contraseña.

Si los datos introducidos son correctos, se abrirá la página de inicio ***Home*** de la Administración online de AirKey. En la parte superior a la derecha, podrá ver el nombre del usuario conectado.

Si lo necesita, también podrá cambiar su contraseña dentro de la Administración online de AirKey. Para ello, haga clic en el nombre del administrador en la fila del encabezado de la Administración online de AirKey y use la función ***Cambiar contraseña***.

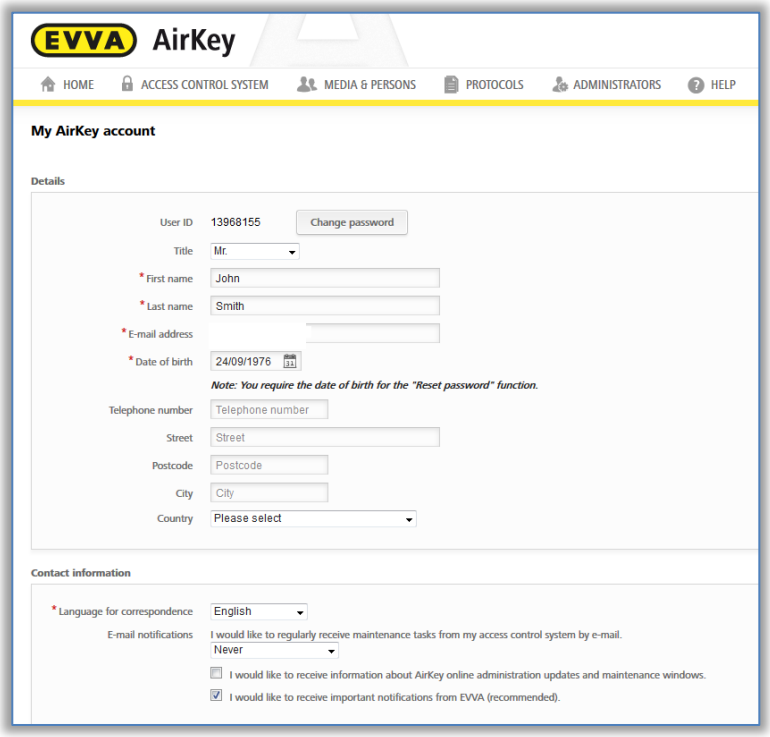


Figura 97: Mi cuenta de AirKey

5.2 Cierre de sesión de AirKey

Para salir de la Administración online de AirKey, haga clic en ***Cerrar sesión*** ❶.

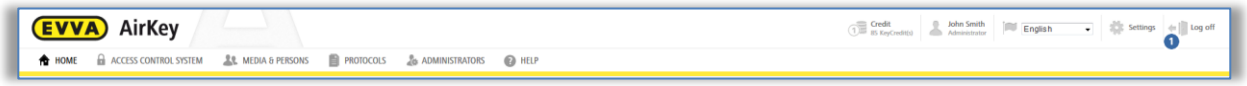


Figura 98: Cerrar sesión

A pesar del cierre de sesión automático tras 30 minutos, se recomienda encarecidamente que el administrador cierre sesión siempre, tras finalizar las tareas ejecutadas, mediante ***Cerrar sesión***.

5.3 Administradores

Para administrar el sistema AirKey hay dos roles para administradores: **Administradores del sistema** y **subadministradores**.

Los **administradores del sistema** disponen de todos los derechos para la administración de todo el sistema de control de accesos AirKey y también pueden crear, editar y borrar administradores adicionales.

Los **subadministradores** disponen de derechos limitados y se utilizan principalmente para la administración de personas y autorizaciones. Además, los **subadministradores** también se

pueden restringir únicamente para determinadas áreas y componentes del sistema de control de accesos AirKey. Esto significa que solo pueden crear y editar autorizaciones de acceso para componentes AirKey y áreas para las que también estén autorizados.

Tiene que haber como mínimo un administrador por sistema de control de accesos.

Las funciones del administrador se encuentran en el menú principal ***Administradores*** ❶.

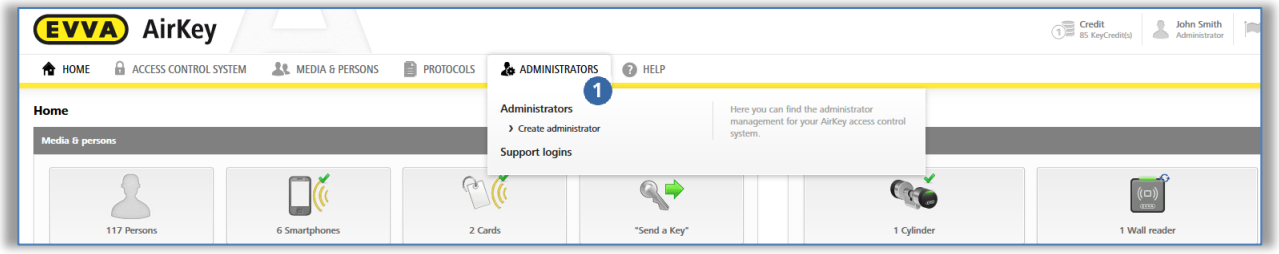


Figura 99: Menú principal – Administradores

5.3.1 Crear administrador

Solo un administrador podrá crear nuevos administradores.

> En el menú principal, elija ***Administradores*** → ***Crear administrador***.

> Seleccione si se trata del rol de ***administrador del sistema*** o ***subadministrador***.

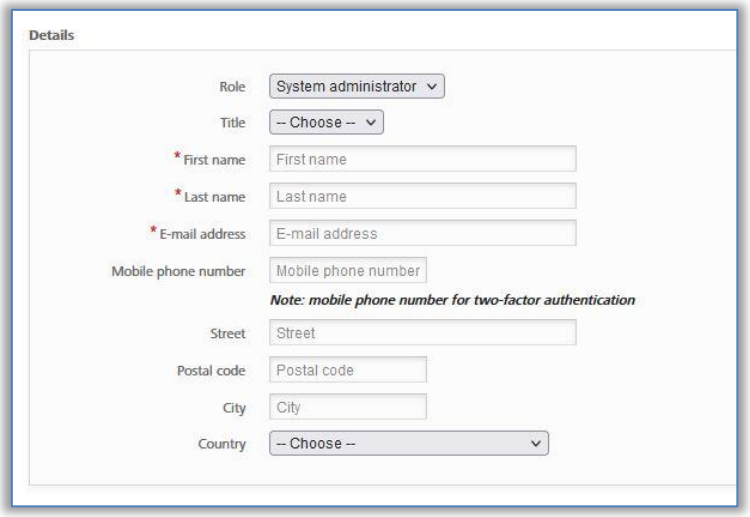


Figura 100: Detalles de un administrador

> Rellene los campos del formulario. Los campos marcados con * son obligatorios.

> En el bloque "Información de contacto", puede indicar también si quiere que el administrador reciba notificaciones de e-mail sobre determinados eventos como, por ejemplo, tareas de mantenimiento pendientes, intervalos de mantenimiento por cumplir u otra información importante. Las notificaciones de e-mail se enviarán en el idioma seleccionado para la correspondencia.

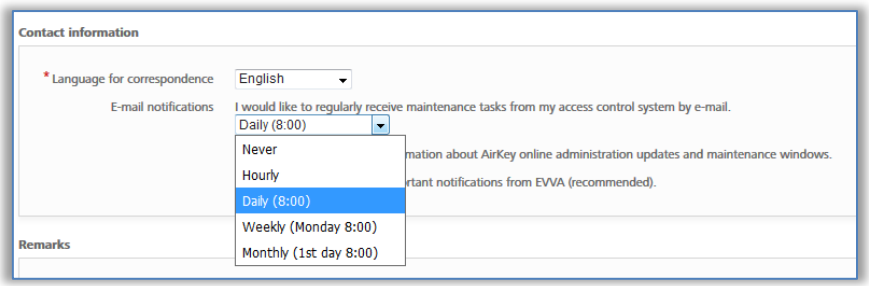


Figura 101: Información de contacto

> Haga clic en ***Guardar*** ❶.

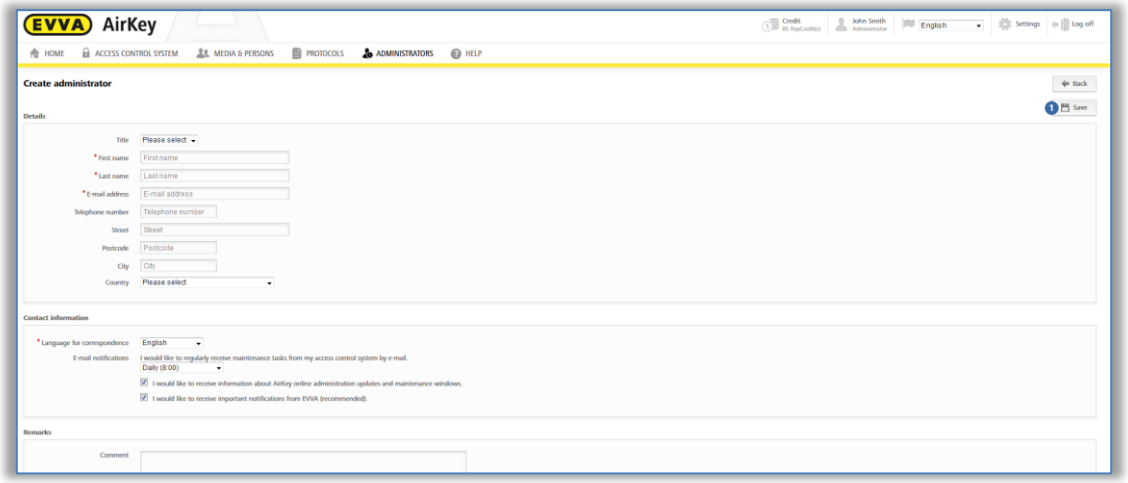


Figura 102: Crear administrador

Antes de guardar, compruebe de nuevo que la dirección de e-mail a la que enviará el vínculo de activación sea la correcta.

> Para finalizar el proceso, confirme la pregunta de seguridad con ***Crear administrador***.

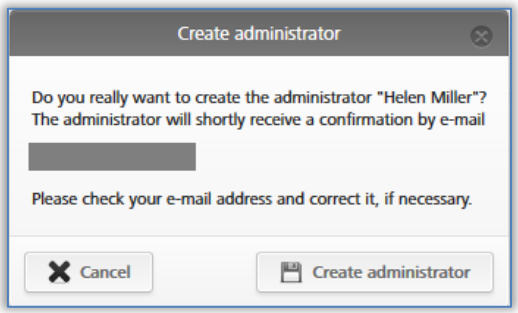


Figura 103: Crear administrador

La creación de un administrador se indicará con el mensaje de confirmación "El administrador ha sido guardado".

El administrador creado recibirá un e-mail de *EVVA AirKey* con un vínculo de activación. Para los **subadministradores** ahora puede administrar los derechos. Los detalles sobre la

administración de derechos de los subadministradores se encuentran en el siguiente capítulo Editar administrador.

Si el vínculo de activación no se usa en 48 horas, los datos serán borrados y el vínculo de activación perderá su validez.

El administrador creado deberá finalizar su registro de la continuar manera:

- Abra el e-mail con el asunto "Registro de EVVA AirKey".
- Haga clic en el vínculo de activación; se abre el sitio web "¡Bienvenido a AirKey!"
- Introduzca la contraseña que ha elegido, repítala e introduzca la fecha de nacimiento.
- Haga clic en ***Guardar***.

Con ello se finalizará el proceso de crear un administrador. A continuación, se le redirigirá a la página de inicio de sesión de la Administración online de AirKey donde el nuevo administrador puede iniciar sesión.

5.3.2 Editar administrador

Únicamente los **administradores del sistema** pueden modificar datos de un administrador; p. ej., apellidos, dirección de correo electrónico, número de teléfono o información de contacto, a posteriori. El rol también se puede editar posteriormente. No obstante, tenga en cuenta que debe haber al menos un **administrador del sistema** por cadasistema de control de accesos.

La identificación del usuario no se puede cambiar.

- En el menú principal, elija ***Administradores*** → ***Administradores***.
  Se mostrará una lista con todos los administradores.

En la lista mostrada, podrá buscar administradores, ordenar columnas, limitar las entradas mostradas por página y exportar la lista a un archivo CSV.

- Haga clic en el administrador que desee editar.
- Modifique los datos según desee.
- Haga clic en ***Guardar*** ❶.

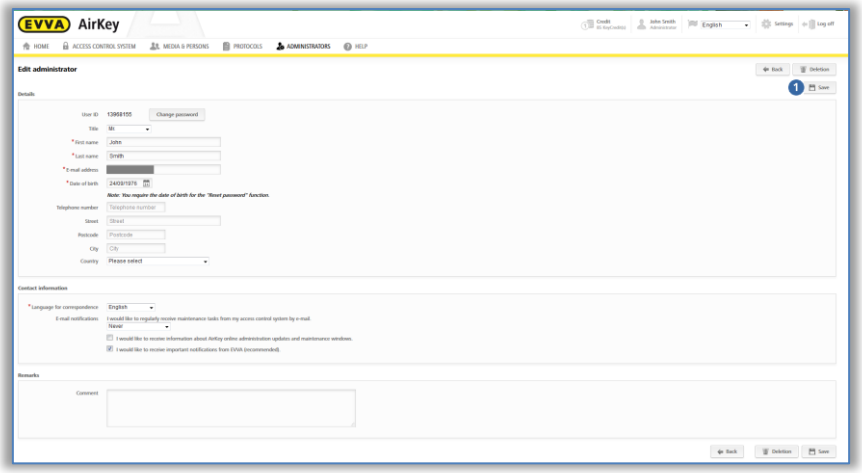


Figura 104: Editar administrador

Para administrar los derechos de los **subadministradores**, siga los siguientes pasos:

> En el menú principal, elija ***Administradores*** → ***Administradores***.
Se mostrará una lista con todos los administradores.

> Haga clic en el **subadministrador** cuyos derechos desee modificar.

> Cambie a la pestaña ***Administrar derechos***.

> Al marcar las casillas de verificación, puede elegir qué áreas y componentes debe administrar el subadministrador y qué autorizaciones debe asignarles.

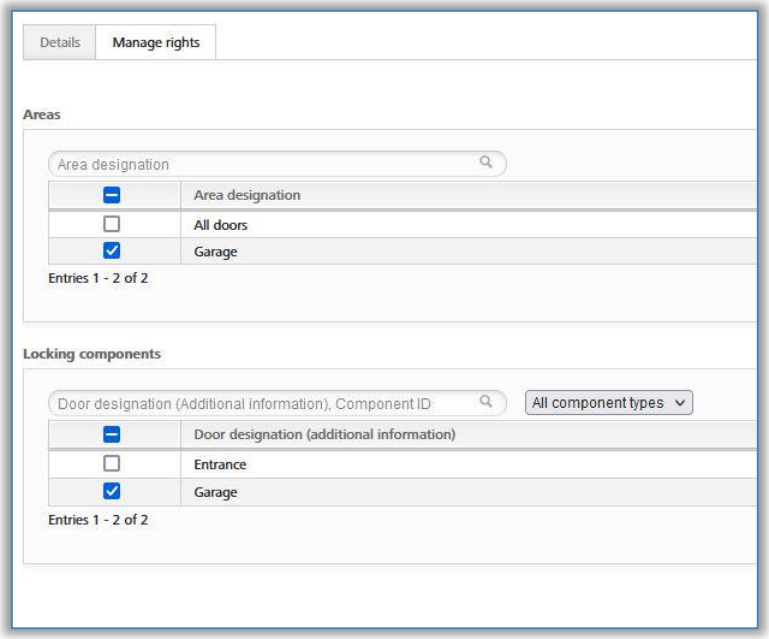


Figura 105: Administrar derechos de un subadministrador

> Haga clic en ***Guardar***.

Las áreas y componentes para los que un **subadministrador** no tiene derechos no están disponibles para el **subadministrador** en la asignación de autorizaciones. Un **administrador del sistema** dispone siempre de todas las áreas y componentes para la asignación de autorizaciones.

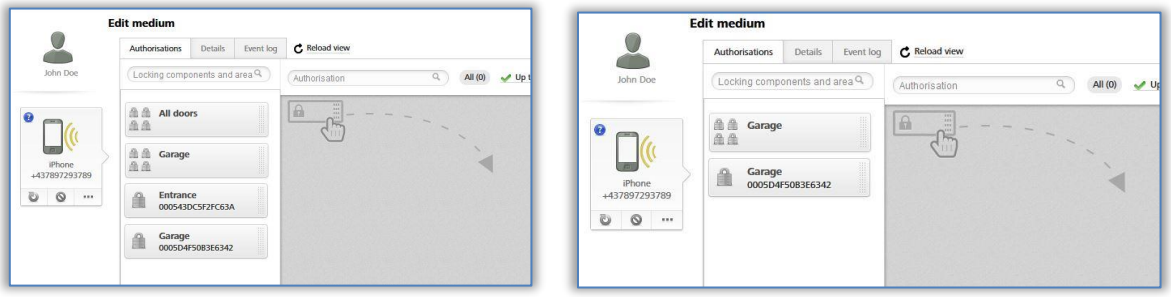


Figura 106: Asignación de autorizaciones por parte de un administrador del sistema o de un subadministrador

La administración de derechos para **subadministradores** se refiere solo a áreas y componentes. Los **subadministradores** siempre ven a todas las personas y medios.

5.3.3 Borrar administrador

Un administrador solo puede ser borrado por otro administrador del sistema.

> En el menú principal, elija ***Administradores*** → ***Administradores***.

> Seleccione el administrador que se debe borrar haciendo clic en la fila pertinente de la tabla. Llegará a la página "Editar administrador".

> Haga clic en ***Eliminar*** ❶.

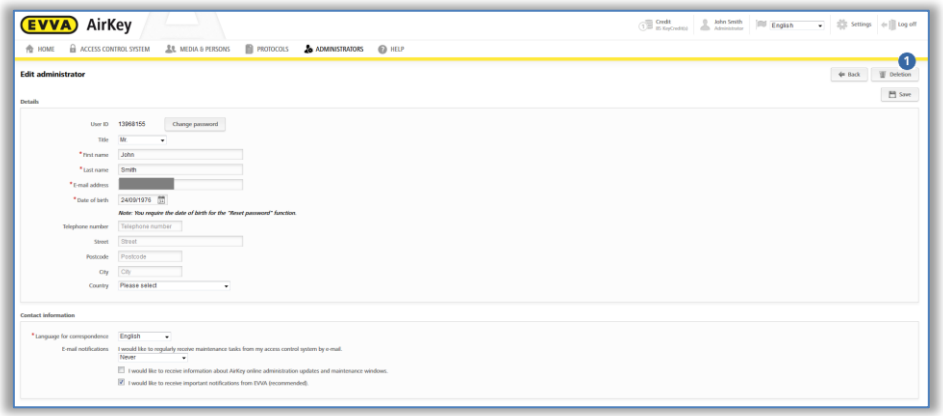


Figura 107: Borrar administrador

> Confirme la pregunta de seguridad con ***Borrar administrador***.

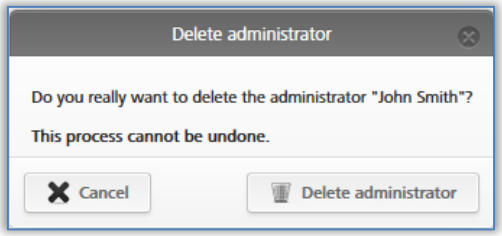


Figura 108: Borrar administrador

El borrado de un administrador se indicará con el mensaje de confirmación "El administrador ha sido borrado". El administrador borrado ya no aparece en la lista de administradores ni podrá iniciar sesión en la Administración online de AirKey.

Si la **función de verificación por dos personas para la visualización de las listas de eventos** está habilitada, deben quedar al menos dos administradores del sistema. De lo contrario, se muestra un mensaje de error al intentar eliminar el administrador y este no se puede borrar. Para obtener más información sobre la **función de verificación por dos personas para la visualización de las listas de eventos**, consulte el capítulo Aspectos generales.

5.4 Ajustes del sistema AirKey

En los ajustes de la Administración online de AirKey, están los ajustes básicos detallados a continuación.

> En la página de inicio ***Home***, haga clic en la opción ***Ajustes*** ❶.

> O en la fila de encabezado haga clic en ***Ajustes***.

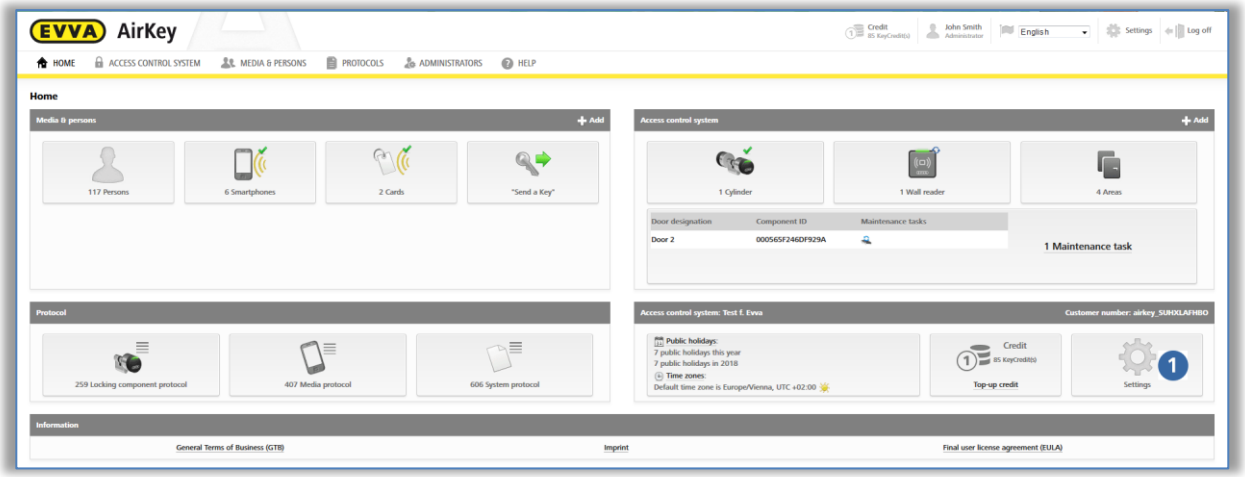


Figura 109: Ajustes del sistema de control de accesos

5.4.1 Aspectos generales

En esta pestaña, se pueden activar los siguientes ajustes generales para todo el sistema de control de accesos.

Ajustes de Bluetooth para la app de AirKey

Aquí puede configurarse, para todos los smartphones de este sistema de control de accesos, si es posible o no abrir los componentes mediante Bluetooth desde la pantalla de bloqueo. Si no está activada esta opción, deberá desbloquearse el smartphone antes de cada acceso.

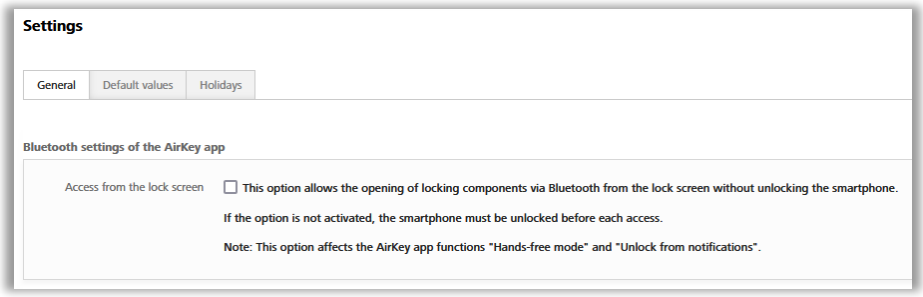


Figura 110: Ajustes generales – ajustes de Bluetooth de la app de AirKey

Esta opción afecta a las funciones "Modo Hands-free (manos libres)" y "Desbloquear desde notificaciones" de la app.

Desactive ***Acceso desde la pantalla de bloqueo*** para aumentar la seguridad de su sistema de control de accesos.

Ajustes para la app de AirKey

Aquí se puede activar la opción **Actualización tras cada acceso** y configurar el **texto para el SMS de «Send a Key»**.

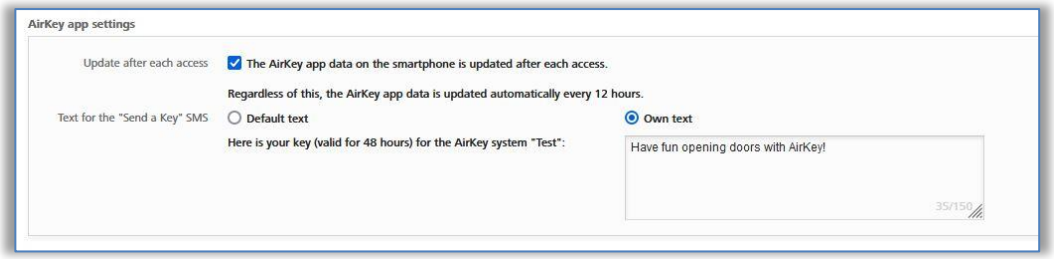


Figura 111: Ajustes generales – ajustes de la app de AirKey

Si se activa la opción **Actualizar tras cada acceso**, los datos de la app de AirKey (por ejemplo, entradas de la lista de eventos o el estado de las pilas de los componentes) se actualizan con cada acceso con un smartphone.

> Para ello, seleccione la casilla de verificación correspondiente y confirme con ***Guardar***.

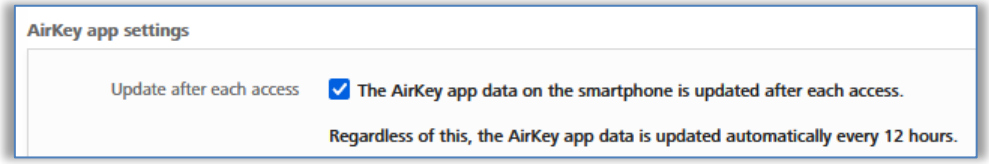


Figura 112: Ajustes para la app de AirKey – actualización después de cada acceso

La funcionalidad se enviará a continuación a todos los smartphones de este sistema de control de accesos mediante una notificación Push. La funcionalidad en el smartphone debería estar activa, como tarde, tras una actualización manual de los datos de la app de AirKey del smartphone (véase el capítulo Actualización del smartphone). El estado actual ❶ del smartphone respecto a esta función lo encontrará en la Administración online de AirKey, en los Datos del smartphone.

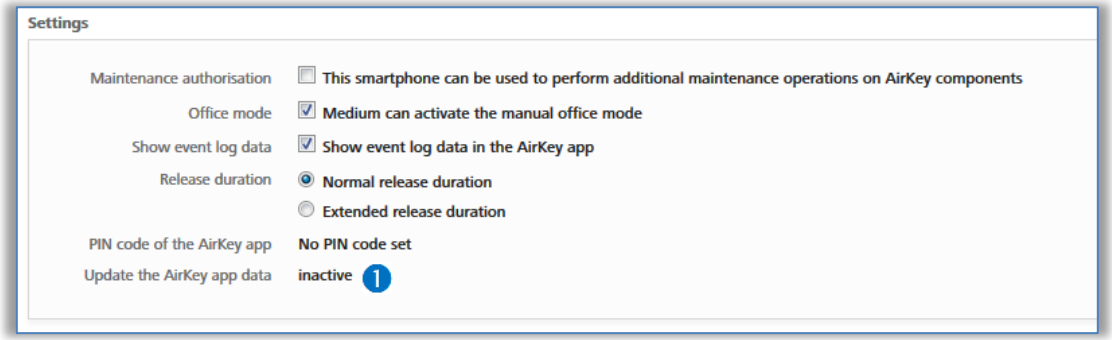


Figura 113: El estado de la opción "Actualización después de cada acceso"

Active esa función para transferir los accesos, en caso de empleo de smartphones, prácticamente en tiempo real a la Administración online de AirKey.

La actualización de los datos de la app de AirKey tras un proceso de acceso transmite únicamente los datos del smartphone en cuestión que haya realizado el proceso de acceso. Esta actualización no se mostrará en el smartphone.

Para esta función se necesita una conexión a Internet estable (datos móviles o WLAN), ya que puede realizarse otro proceso de acceso una vez concluida la actualización de los datos de la app de AirKey.

Con independencia de la opción "Actualización después de cada acceso", se intentará, cada 12 horas, actualizar automáticamente los datos de la app de AirKey.

También existe la posibilidad de configurar aquí el **texto para el SMS de «Send a Key»**.

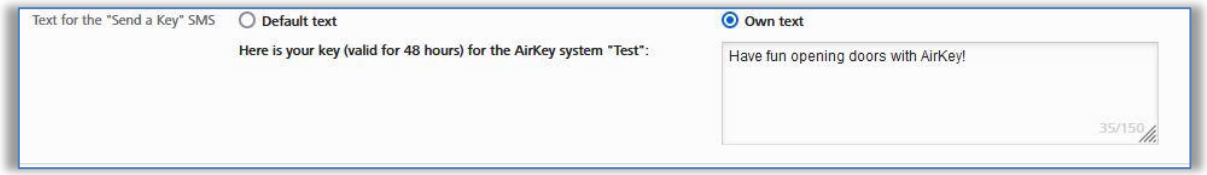


Figura 114: Ajustes para la app de AirKey – Texto para el SMS de "Send a Key"

Para ello, se puede elegir entre el texto predeterminado y un texto a definir por el usuario. Elija ***Texto predeterminado*** para usar el texto predefinido «Aquí tiene su llave (válida 48 h) para el sistema AirKey "<Nombre del sistema de control de accesos>"» o elija ***Texto propio*** para usar un texto personalizado en el campo de texto correspondiente. A continuación, confirme la selección con ***Guardar***.

Si se utiliza un texto propio, este se puede adaptar adicionalmente en cada acción «Send a Key» para, por ejemplo, utilizar un tratamiento personalizado. Encontrará información detallada sobre «Send a Key» en el capítulo Función "Send a Key".

El texto personalizado está limitado a un máximo de 150 caracteres. Además, el texto personalizado no se traducirá a otros idiomas si una persona ha seleccionado otro idioma de correspondencia. En su lugar, el texto predeterminado se traduce automáticamente al idioma seleccionado para la correspondencia con esa persona.

Utilice un texto definido por usted para dirigirse personalmente al propietario del smartphone y comunicarle para qué sistema de control de accesos recibe autorización.

Opciones de seguridad

Las opciones de seguridad le permiten configurar las funciones **reemplazo de smartphone**, **autenticación de dos factores (2FA)** y la **función de verificación por dos personas para la visualización de las listas de eventos**.

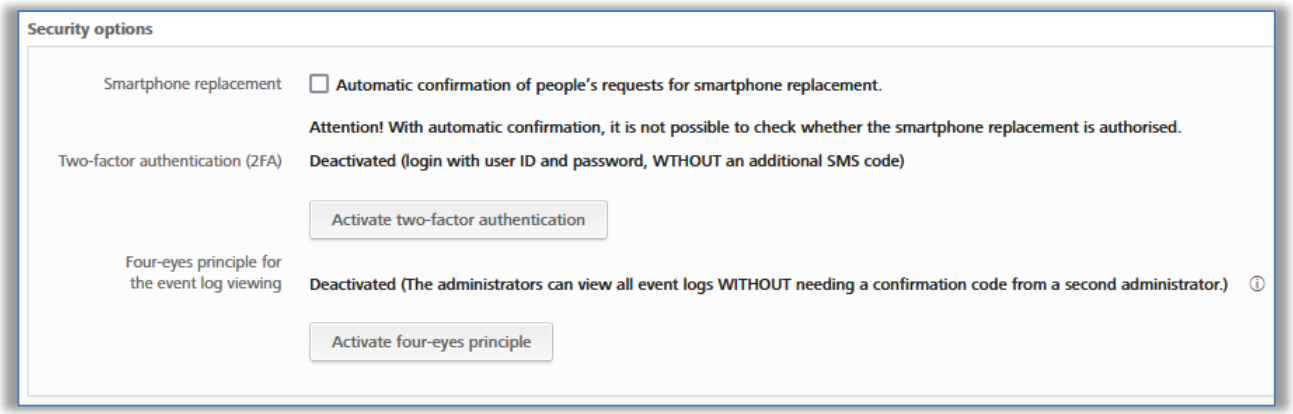


Figura 115: Ajustes generales – Opciones de seguridad

Con la casilla de verificación ***Confirmar automáticamente las solicitudes de operación de reemplazo de smartphone de personas*** se pueden confirmar automáticamente las acciones de reemplazo iniciadas a través de un smartphone.

De este modo, cada reemplazo de smartphone iniciado a través del smartphone se confirma automáticamente si hay crédito suficiente. Tenga en cuenta que para cada reemplazo de smartphone en el que se transfieran autorizaciones, se necesitará un KeyCredit. Encontrará más detalles sobre el reemplazo de smartphone en el capítulo Reemplazo de smartphone.

La **autenticación de dos factores** (conocida también como **2FA**) sirve de nivel de seguridad adicional durante el login en la Administración online de AirKey. Para ello, en el login se pide, además del identificador del usuario y la contraseña, un código SMS adicional como segundo factor. Si se activa la autenticación de dos factores en los ajustes, se empleará para todos los administradores de este sistema de control de accesos.

> Para activarla, haga clic en el botón ***Activar autentificación de dos factores***.

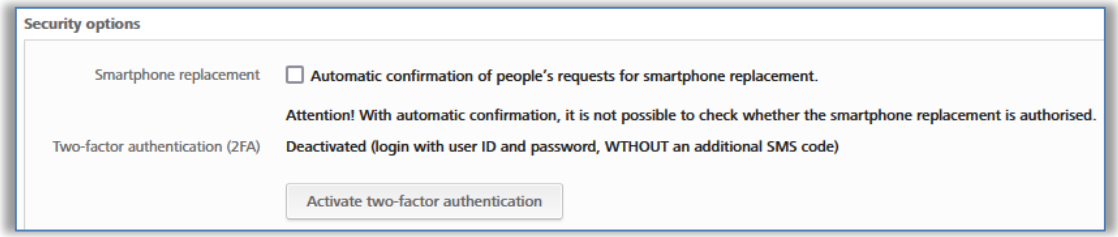


Figura 116: Ajustes generales – autenticación de dos factores (2FA)

> Introduzca el número de teléfono móvil que se empleará para la autenticación de dos factores para el administrador registrado actualmente, y haga clic en ***Enviar código SMS***.

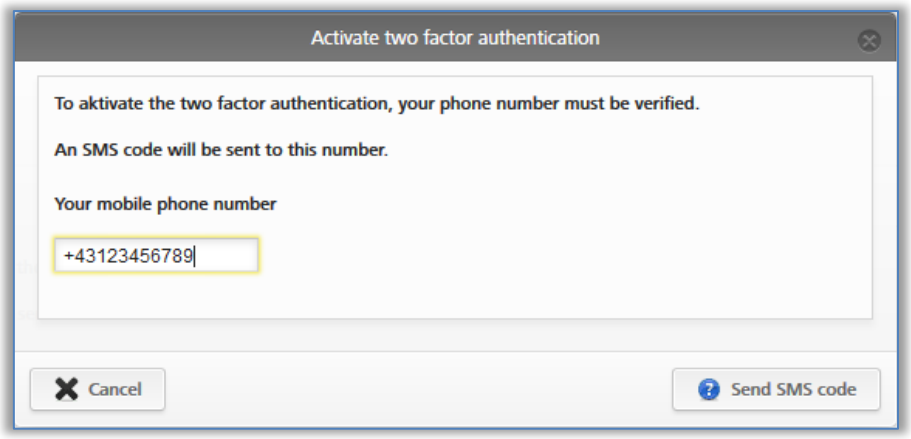


Figura 117: Autenticación de dos factores (2FA)

> Se enviará un código SMS al número de teléfono indicado. Este código SMS debe introducirse en el diálogo en la Administración online de AirKey y confirmarse con ***Guardar***.

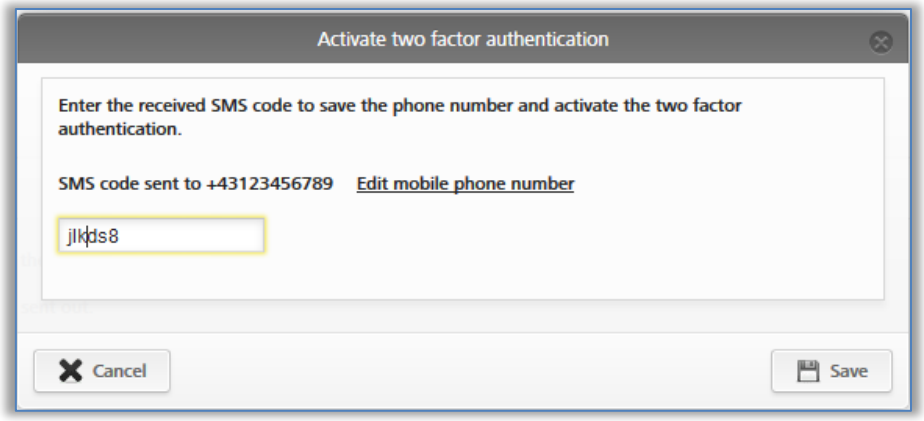


Figura 118: Introducción de código SMS: ajustes

Si se ha empleado un código SMS válido, se activa la autenticación de dos factores para todos los administradores del sistema de control de accesos. El estado en los ajustes se modifica en consonancia.

El código SMS es válido durante 5 minutos. Si han pasado los 5 minutos, debe repetirse el proceso.

A partir del momento de la activación, se requiere un teléfono móvil para cada inicio de sesión. Encontrará información detallada sobre el proceso de inicio de sesión con la autenticación de dos factores activada en el capítulo Inicio de sesión en AirKey con autenticación de dos factores.

Para desactivar la autenticación de dos factores, siga los siguientes pasos:

> Haga clic en ***Desactivación de la autenticación de dos factores***.

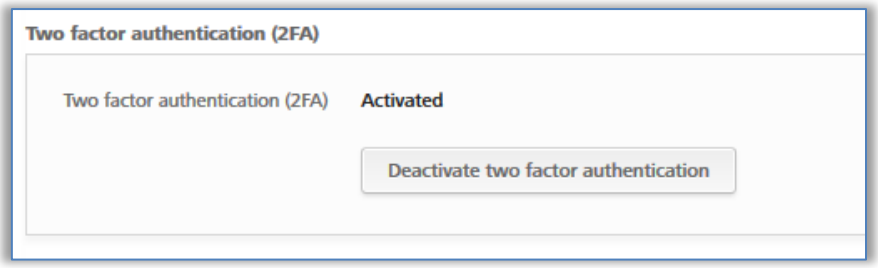


Figura 119: Desactivación de la autenticación de dos factores

> Confirme la consulta igualmente con ***Desactivación de la autenticación de dos factores***.

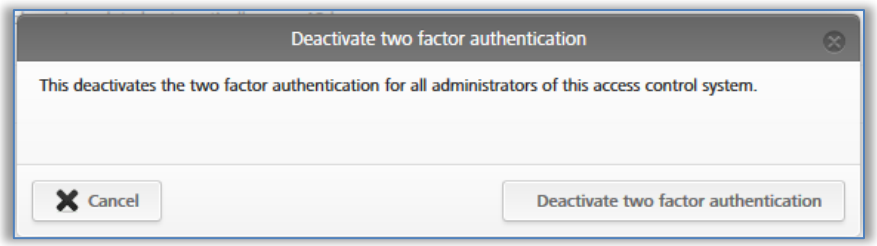


Figura 120: Desactivación de la autenticación de dos factores

La función vuelve a estar desactivada para todos los administradores del sistema de control de accesos.

Con la **función de verificación por dos personas para la visualización de las listas de eventos**, solo podrá ver la lista de eventos de los medios y componentes cuando un segundo administrador del sistema confirme la vista. De este modo, los datos personales están todavía más protegidos.

Para activar la **función de verificación por dos personas para la visualización de las listas de eventos**, debe haber al menos dos administradores del sistema.

Para activar la **función de verificación por dos personas para la visualización de las listas de eventos**, siga los siguientes pasos:

> Haga clic en ***Activar función de verificación por dos personas***.

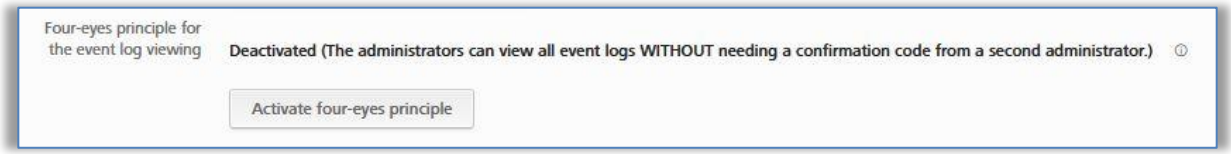


Figura 121: Activación de la función de verificación por dos personas

> Seleccione un segundo administrador del sistema de la lista para enviarle un código de confirmación por correo electrónico y haga clic en ***Enviar código de confirmación***.

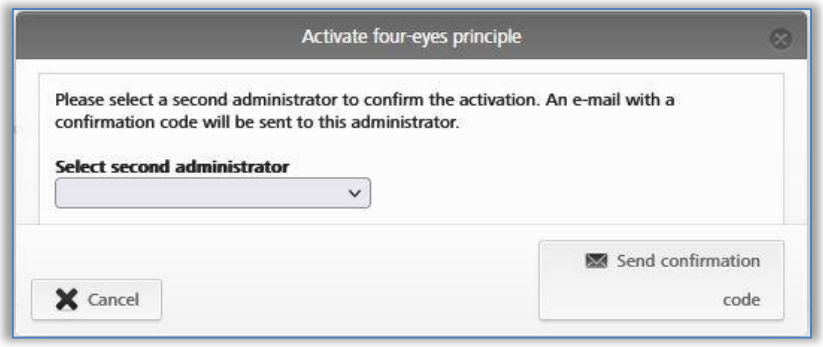


Figura 122: Activación de la función de verificación por dos personas – seleccionar segundo administrador

> A continuación, se enviará un correo electrónico con un código de confirmación al administrador del sistema seleccionado.

> Este código de confirmación debe introducirse en la administración online de AirKey en un plazo de 10 minutos y confirmarse con el botón ***Activar***.

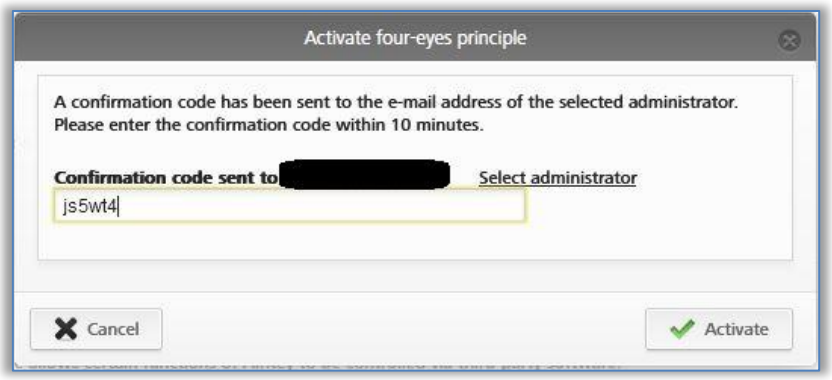


Figura 123: Activación de la función de verificación por dos personas – introducción del código de confirmación

Si este procedimiento no se completa en 10 minutos, deberá repetirse el proceso. Si el administrador del sistema seleccionado no responde, también se puede seleccionar otro administrador del sistema para activar la función de verificación por dos personas a través del enlace ***Seleccionar administrador***.

De este modo, ha activado la **función de verificación por dos personas para la visualización de las listas de eventos** para todos los administradores de este sistema AirKey. A partir del siguiente inicio de sesión de un administrador del sistema, no se podrá ver la lista de eventos de los medios y componentes AirKey sin la confirmación de un segundo administrador del sistema.

La lista de eventos del sistema puede seguir mostrándose y no está sujeta a la función de verificación por dos personas. Los subadministradores no pueden ver ninguna lista de eventos.

Para desactivar la **función de verificación por dos personas para la visualización de las listas de eventos**, siga el mismo procedimiento que para la activación.

Tanto la activación como la desactivación se guardan en la lista de eventos del sistema. Para ello, también se registran ambos administradores del sistema implicados, incluida la dirección de correo electrónico utilizada.

AirKey Cloud Interface(API)

AirKey Cloud Interface es una interfaz REST (API) para sistemas de terceros. La interfaz permite controlar determinadas funciones de AirKey mediante un software de terceros. Se describe en detalle AirKey Cloud Interface en el capítulo AirKey Cloud Interface (API).

AirKey Cloud Interface (API) – entorno de pruebas

El entorno de pruebas le ofrece la posibilidad de probar la AirKey Cloud Interface (API) antes de la activación en un entorno protegido con datos de prueba. Encontrará información detallada al respecto en el capítulo AirKey Cloud Interface (API).

5.4.2 Valores predeterminados (para todos los componentes de cierre recien añadidos)

Estos ajustes se activan automáticamente con componentes de cierre añadidos hace poco. Para grandes sistemas AirKey, se recomienda establecer los valores predeterminados antes de la primera instalación para simplificar la administración del sistema.

Hora y calendario

En un sistema de control de accesos, puede gestionar componentes de cierre que se encuentren en distintas zonas horarias. Como valor estándar, viene preconfigurada la zona horaria de "Europa/Viena" con UTC+01:00 en invierno y UTC+02:00 en verano, válida para Centroeuropa.

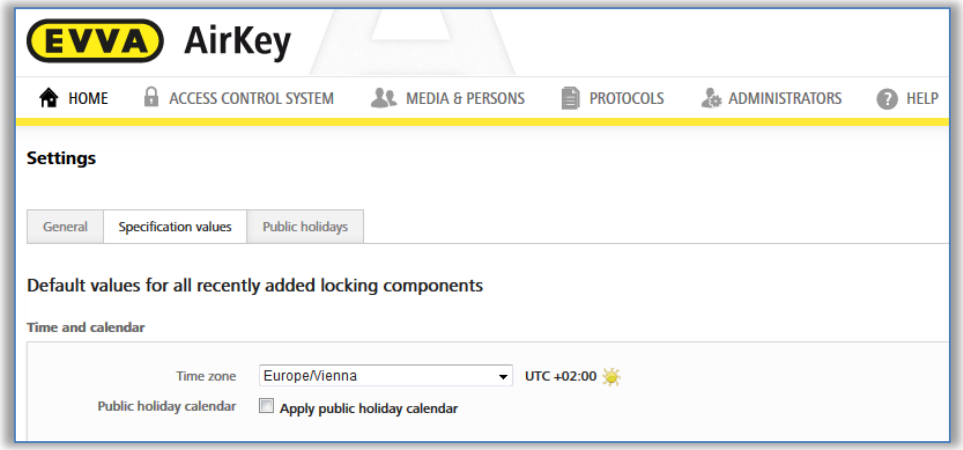


Figura 124: Valores predeterminados para nuevos componentes de cierre

Si quiere modificar la zona horaria para todo el sistema de control de accesos, haga clic en la lista desplegable y seleccione la zona horaria correcta de la lista.

Si desea modificar la zona horaria para un componentes de cierre, haga clic en la página de inicio ***Home*** en la opción ***Cilindros*** o ***Lectores murales***, seleccione el componentes de cierre que quiera y vaya a la pestaña ***Ajustes***.

Bajo el bloque ***Hora y calendario***, tiene de nuevo la lista desplegable con las zonas horarias.

El símbolo del sol en cada zona horaria muestra si se está en horario de verano o invierno:

- Sol amarillo = horario de verano
- Sol gris = horario de invierno

Si marca la casilla ***Utilizar calendario de festivos***, se adoptarán los festivos guardados y activados en la pestaña ***Festivos*** (véase el capítulo Festivos) para el nuevo componentes de cierre.

Áreas

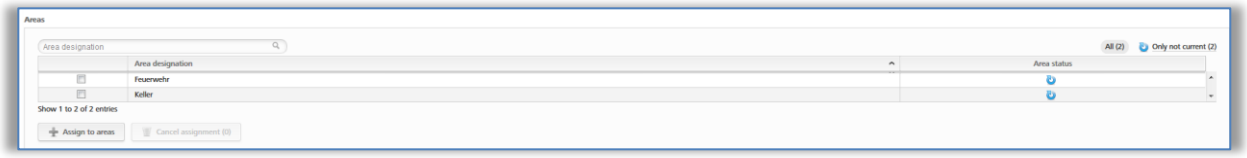


Figura 125: Valores predeterminados – Áreas

En este apartado, se pueden asignar automáticamente nuevos componentes de cierre a áreas ya creadas. Dónde y cómo se crea un área, se explica en Crear área.

Resulta especialmente útil para llaves generales y de bomberos que deban bloquear siempre todos los componentes. Las asignaciones a áreas se pueden anular de nuevo para cada componentes de cierre.

Acceso

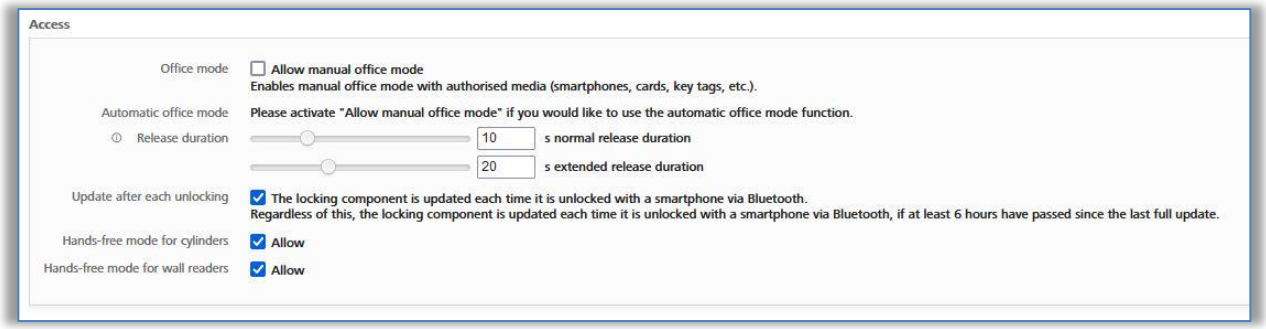


Figura 126: Valores predeterminados – Acceso

Aquí se puede permitir la apertura permanente manual y automática, la duración de la apertura, la actualización después de cada proceso de apertura y el modo Hands-free para cilindros y lectores murales para todos los componentes AirKey añadidos recientemente.

Si la casilla ***Permitir apertura permanente manual*** está activa, aparece además la continuar casilla: ***Activar apertura permanente automática***.

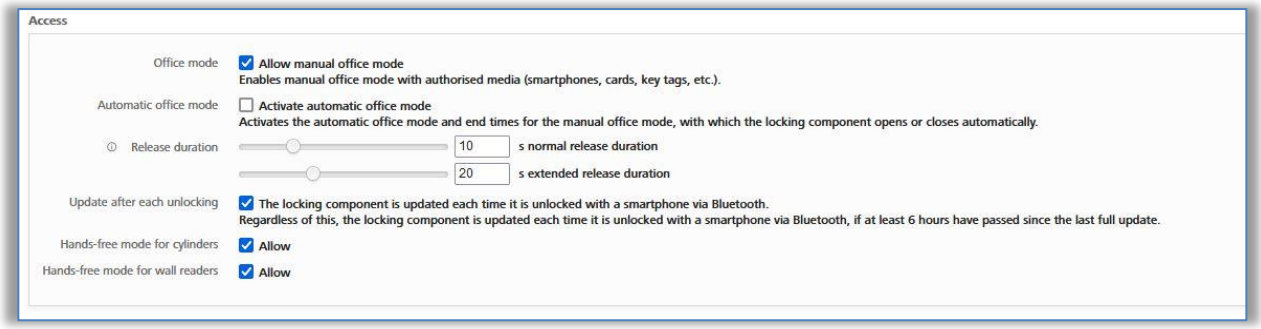


Figura 127: Apertura permanente automática

La apertura permanente automática permite fijar períodos y momentos AirKey en los que el componentes de cierre se abre / cierra automáticamente. Por ejemplo, en un oficina la apertura permanente finaliza automáticamente a las 17:00 h cada tarde. En caso de un cilindro de AirKey, no significa que la puerta esté cerrada, sino solo que el cilindro se desacopla. Para cerrar la puerta, el cilindro debe estar conectado a un medio autorizado y, a continuación, debe cerrarse manualmente.

En esta ventana de diálogo también puede introducirse el momento final establecido para la apertura permanente manual. De esta forma se garantiza que, con independencia de la activación de la apertura permanente, esta finalice en el momento establecido (barras rojas en el siguiente pantallazo). Pueden establecerse un máximo de 4 entradas diarias (períodos o momentos finales).

Las aperturas permanentes finalizan automáticamente (o simplemente no se inician) en festivos, en caso de avisos de "Batería vacía", si los componentes de cierre no están en hora o en caso de actualización del firmware.

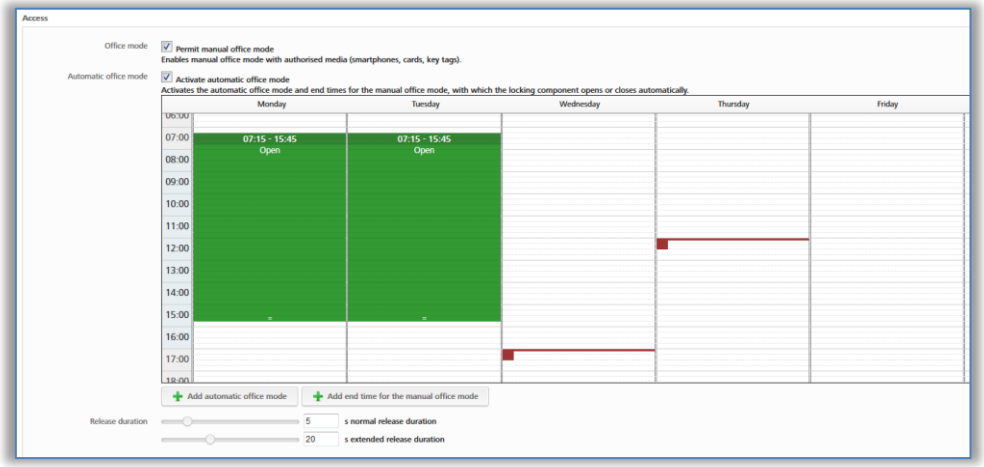


Figura 128: Apertura permanente automática

La duración de la activación determina cuánto dura la activación del componentes de cierre ante una apertura (p. ej. en el caso de un cilindro, quiere decir cuánto tiempo tiene el usuario para girar manualmente el pomo del cilindro). De manera predeterminada, la duración de activación normal es de 5 segundos, y la ampliada de 20. La duración de la activación se puede personalizar aquí, y el período va de 1 a 250 segundos.

La apertura permanente manual puede activarse también con medios de acceso. Para ello se acercará el medio al componente de cierre, se alejará brevemente del área de lectura y se presentará por segunda vez dentro del período de apertura. La apertura permanente manual puede también finalizarse de esta manera.

La opción ***Actualización después de cada desbloqueo*** puede activarse si es necesario actualizar el componente tras cada apertura realizada correctamente mediante Bluetooth. Con independencia de ello, el componente se actualiza cada vez que se activa con un smartphone mediante Bluetooth, cuando han pasado al menos 6 horas desde la última actualización completa.

El usuario del smartphone no notará esta actualización. No se emite un aviso, ni hay indicación alguna en el smartphone.

El administrador, no obstante, verá la lista de eventos actualizada en la Administración online de AirKey.

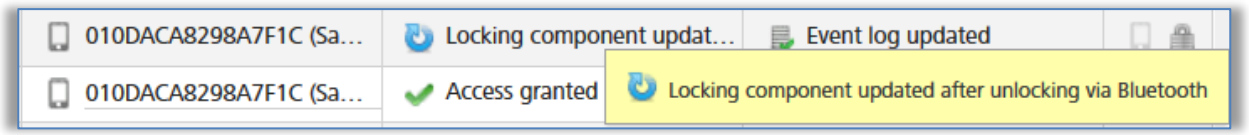


Figura 129: Registro de eventos: Actualización tras el proceso de apertura

Durante la actualización tras un proceso de apertura mediante Bluetooth, únicamente se actualizan los siguientes datos:

- Blacklist
- Zona horaria
- Hora
- Entradas de la lista de eventos

Si el componente tiene aún tareas de mantenimiento pendientes, estas deberán actualizarse tal y como se describe en el capítulo Actualizar componentes de cierre.

El funcionamiento dependerá de la calidad de la conexión del smartphone. Procure, por ello, que su conexión a Internet sea estable y 3G como mínimo, o realice la actualización mediante WLAN.

La actualización tras un proceso de apertura mediante Bluetooth se realizará también al iniciarse la apertura permanente manual, pero no cuando esta finalice.

La actualización tras un proceso de apertura mediante Bluetooth tiene lugar durante el período de apertura del componente. En el caso de un período de apertura de menos de 10 segundos, probablemente no funcionará la actualización tras un proceso de apertura mediante Bluetooth. Por este

motivo, al activarse la función se aumentará automáticamente el valor del período de apertura normal a 10 segundos.

La activación de esta función aumenta el consumo de pilas en el caso de componentes que funcionen con estas como, por ejemplo, un cilindro AirKey; lo que tiene un impacto en la duración de las pilas.

Las opciones ***Modo Hands-free para cilindro*** y ***Modo Hands-free para lector mural*** sirven para permitir o no el modo Hands-free para todos los componentes del tipo de componente seleccionado dentro del sistema de control de accesos. Además, también se puede configurar individualmente para cada componente AirKey si este debe permitir el modo Hands-free. Encontrará información sobre cómo modificar la configuración de cada componente AirKey en el capítulo Editar componente.

Registro de eventos

Seleccione el valor predeterminado de la referencia personal en las entradas de la lista de eventos de acceso. Aquí dispone de tres botones de radio:

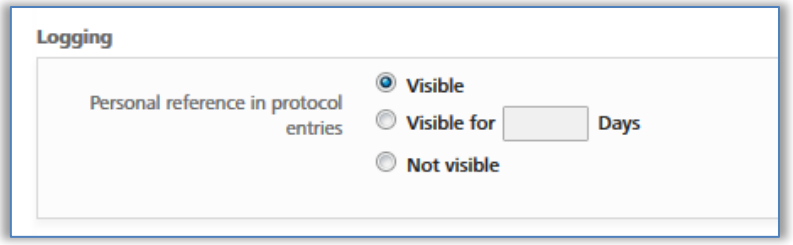


Figura 130: Definir lista de eventos

- ***Visible*** se muestran los datos personales de eventos de acceso manera permanente.
- ***Visible para ... días*** convierte los datos personales de eventos de acceso en anónimos tras el número de días definido.
- ***No visible*** convierte en anónimos todos los datos personales de eventos de acceso de forma permanente.

Los valores predeterminados fijados se podrán modificar para los componentes de cierre específicos en cualquier momento.

Los valores predeterminados modificados se deben guardar con el botón ***Guardar***. Entonces se le pregunta si se deben aplicar los valores predeterminados cambiados solo para los componentes de cierre recién añadidos o para todos.

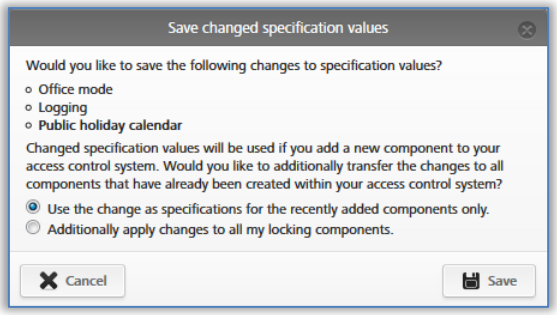


Figura 131: Guardar valores predeterminados modificados

5.4.3 Festivos

En la pestaña ***Festivos***, puede definir hasta 80 festivos al año (año actual y dos sucesivos). El término "festivo" puede ser en AirKey un festivo fijado por ley o un período de varios días, p. ej. las vacaciones de la empresa o las escolares, que se pueden repetir. Por ejemplo, a los festivos nacionales o los que tienen lugar cada año en la misma fecha, se les puede asignar una repetición anual. Una semana de vacaciones escolares conforma solo 1 festivo si se ha definido como período con "Inicio – Fin".

Efectos del calendario de festivos:

1. Las autorizaciones de acceso periódicas no son válidas en festivos.
2. No se contemplan aperturas permanentes automáticas en festivos.

Para que el calendario de festivos sea efectivo, debe activarlo de forma global con el botón ***Activar*** del lado derecho.

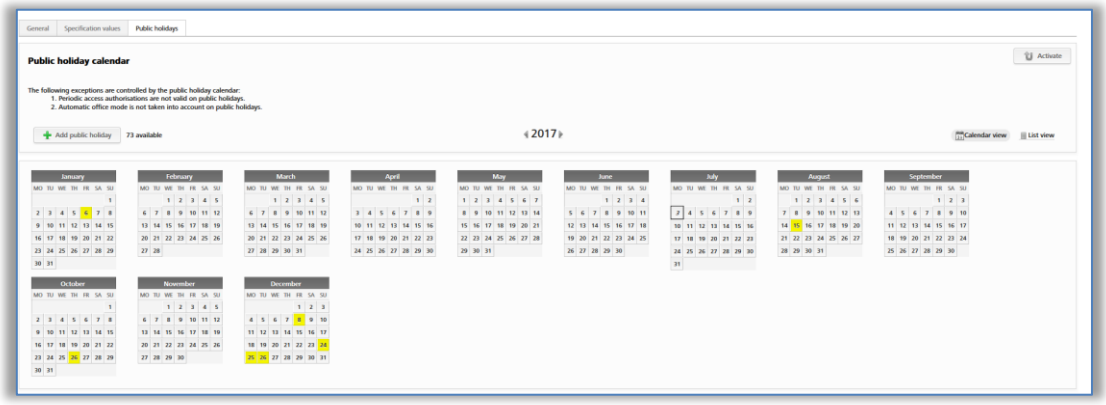


Figura 132: Calendario de festivos (vista de calendario)

Haga clic ***Añadir festivo*** o haga clic en la fecha exacta del festivo (p. ej. 24-12) en la vista de calendario. Entonces se abre una ventana donde puede introducir el nombre del festivo, si el festivo dura todo el día, la duración del festivo, p. ej. solo por la tarde (aquí puede guardar, p. ej. las vacaciones laborales), la frecuencia con que se repite, y cuándo finaliza la repetición.

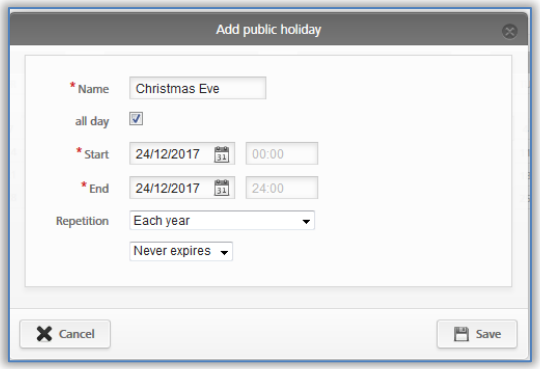


Figura 133: Añadir festivo

Cada festivo ya introducido se puede editar después; haga clic en el día correspondiente y se abrirá un bocadillo de texto.

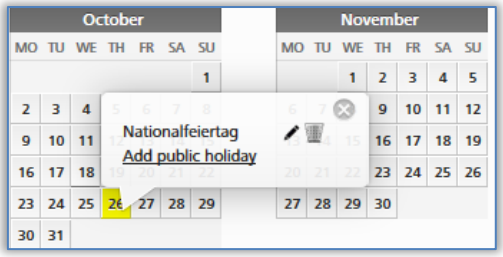


Figura 134: Añadir festivo a través del calendario

Al hacer clic en el vínculo ***Añadir festivo***, puede agregar otro festivo ese día. Puede registrar varios festivos en un día. Al hacer clic en el lápiz, puede editar el festivo; y si hace clic en la papelera, puede borrarlo.

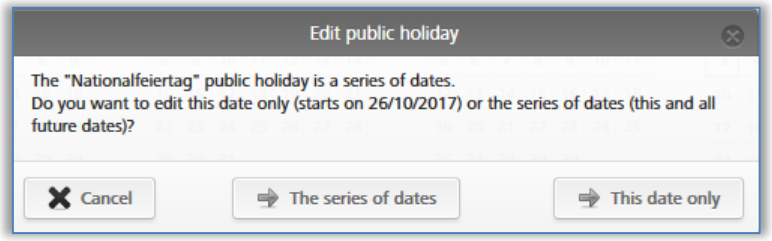


Figura 135: Editar festivo

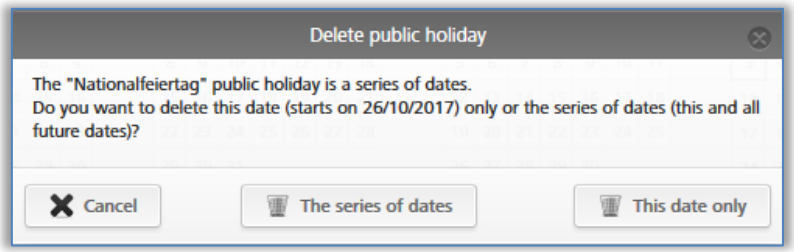


Figura 136: Eliminar festivo

En cuanto se introducen las citas, vacaciones (laborales) o festivos del calendario, se muestra una vista general de todos los festivos guardados, etc. en la vista de la lista.

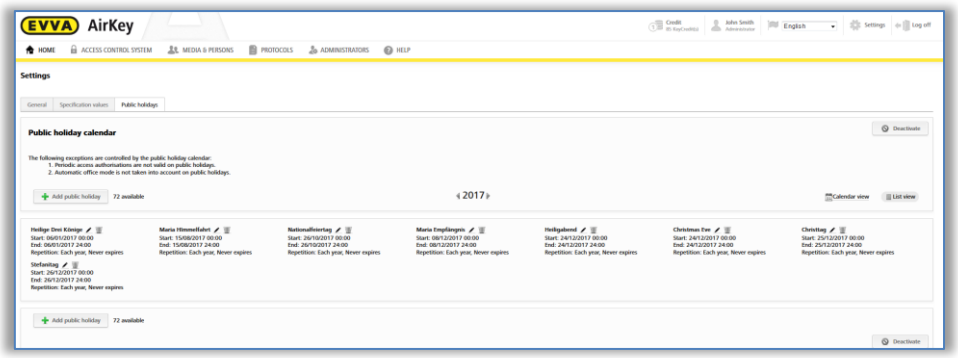


Figura 137: Calendario de festivos (vista de lista)

Si selecciona el botón ***Desactivar***, se desactiva el calendario de festivos a nivel global para el sistema de control de accesos y no se adopta para los componentes de cierre añadidos.

5.5 Sistema de control de accesos

La casilla en la página de inicio ***Home*** y los puntos de menús y submenús en el menú principal ***Sistema de control de accesos*** le permiten administrar el sistema de control de accesos.

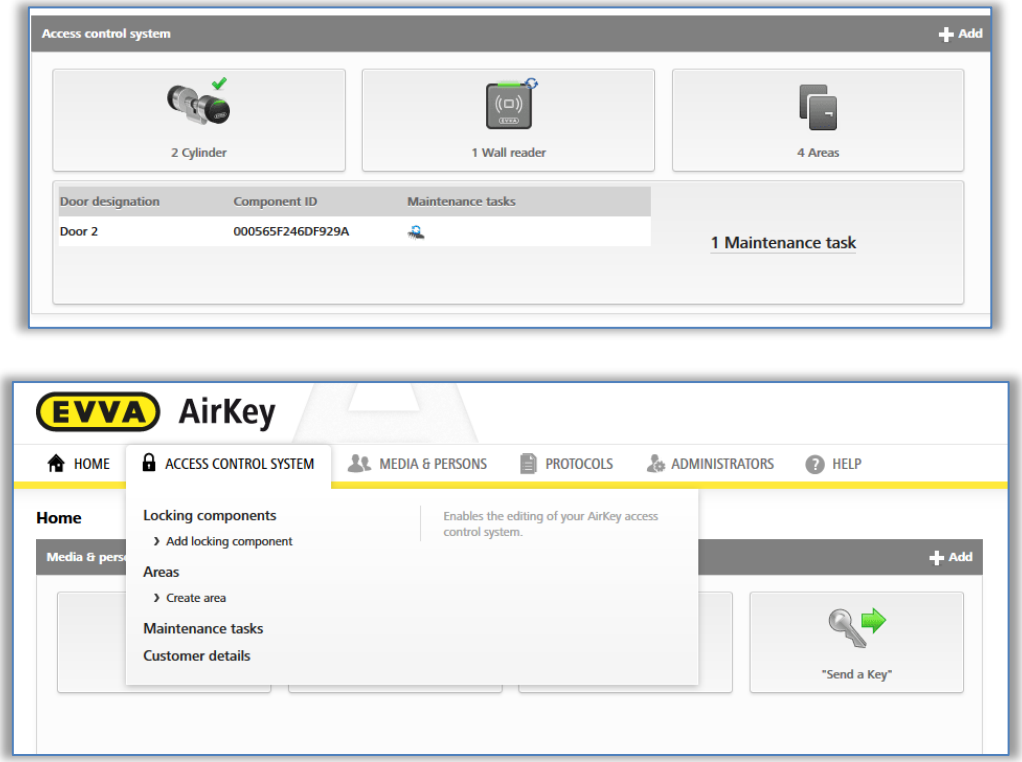


Figura 138: Sistema de control de accesos

5.5.1 Vista general de los componentes de cierre

Para tener una visión general de todos los componentes de cierre del sistema de control de accesos, en la página de inicio ***Home*** haga clic en la casilla ***Cilindros*** o ***Lectores murales***, o en el menú principal ***Sistema de control de accesos*** → ***Componentes de cierre***. En la página de inicio ***Home***, verá en seguida cuántos cilindros o lectores murales integra el sistema de control de accesos.

Se mostrarán todos los componentes de cierre con informaciones adicionales y su estado. En la primera fila de esta lista puede encontrar el campo de búsqueda y las funciones de filtros.

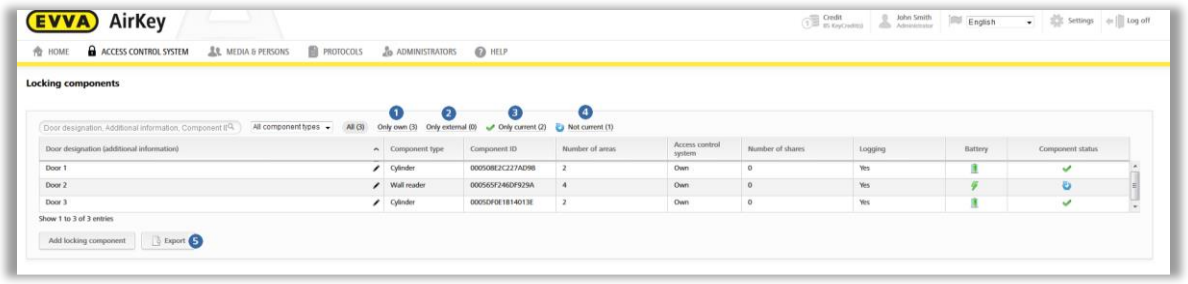


Figura 139: Componentes de cierre

- "Solo propio" ❶ lista solo los propios componentes de cierre.
- "Solo externo" ❷ lista solo los componentes de cierre activados por un administrador.
- "Solo actual" ❸ lista solo los componentes de cierre cuyo estado está al día.
- "No actual" ❹ lista los componentes de cierre cuyo estado no está al día.
- La lista de componentes de cierre se puede exportar a un archivo CSV para seguir editándolos ❺.

AirKey le ofrece la posibilidad de compartir componentes en un sistema de control de accesos externo. En la lista se diferencian tanto los componentes de cierre propios como los externos. Encontrará información más detallada en el capítulo Activar componentes de cierre para otros sistemas de control de accesos.

5.5.2 Añadir componente : Véase el capítulo 4.11

5.5.3 Editar componente

En la ventana ***Editar componente***, la pestaña ***Detalles*** presenta diferente información, p. ej. tipo de componente y modelo, ID del componente, versión de firmware o estado del componente, así como información sobre la puerta, áreas y activaciones. Asimismo puede aquí ver la ubicación del componentes de cierre en Google Maps. En la pestaña ***Ajustes*** verá todos los ajustes definidos para la zona horaria y el calendario de festivos, el acceso, así como el registro de eventos y las opciones de reparación.

El estado de la pila mostrado corresponde al momento de la última actualización y la última entrada de la lista de eventos. Por lo tanto, es posible que el estado real de las pilas en el componentes de cierre sea diferente al mostrado en la Administración online de AirKey.

- En la página de inicio ***Home***, elija la opción ***Cilindros*** o ***Lectores murales***.
- También puede elegir en el menú principal ***Sistema de control de accesos*** → ***Componentes de cierre***.
- Haga clic en la entrada de la lista del componente que desea editar.
- En la pestaña **Detalles**, introduzca, p. ej., una nueva designación de puerta o información adicional opcional ❶, la ubicación o la dirección del componentes de

cierre. Se comprobará que esta información es única en el sistema de control de accesos.

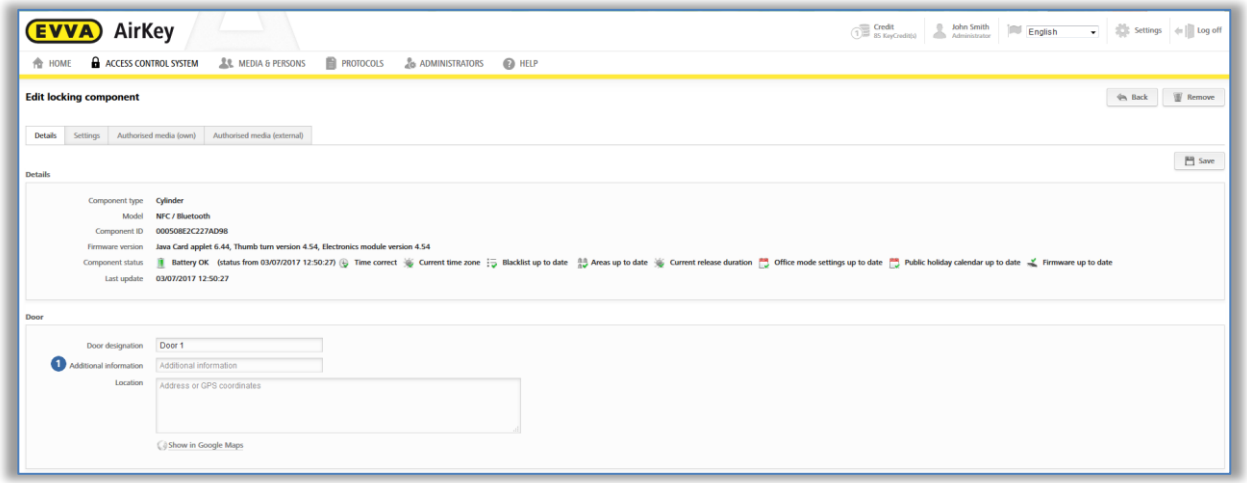


Figura 140: Editar componentes de cierre

> Se pueden editar las asignaciones de área del componentes de cierre seleccionado en el bloque Áreas.

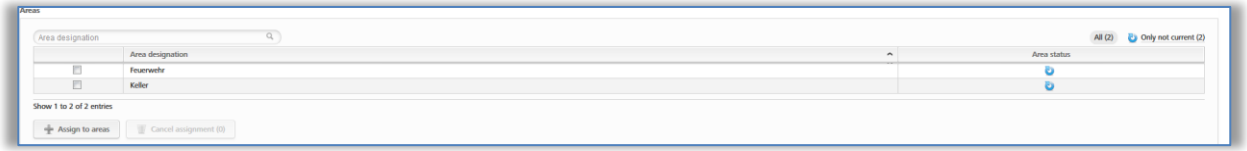


Figura 141: Áreas

> Opcionalmente se puede activar el componentes de cierre para otros sistemas AirKey. Se pueden administrar las activaciones correspondientes en el bloque "Activaciones". Encontrará información más detallada sobre las activaciones en el capítulo Trabajar con varios sistemas AirKey.

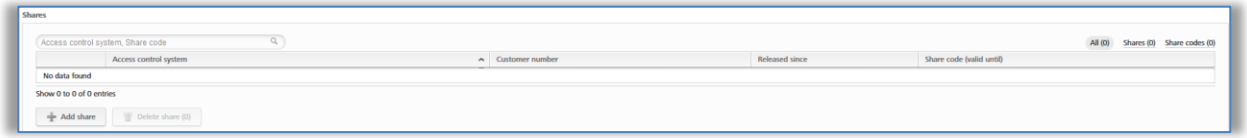


Figura 142: Activaciones

> Opcionalmente puede escribir un comentario sobre un componentes de cierre en el bloque ***Notas***.

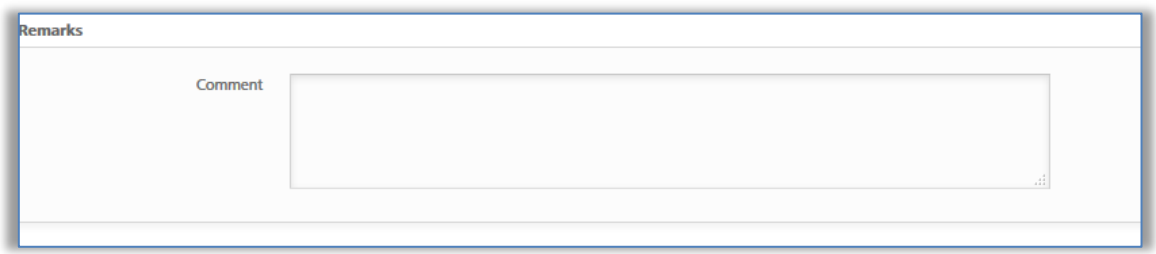


Figura 143: Editar componentes de cierre

En la pestaña ***Ajustes*** podrá gestionar, como se ha mencionado, opciones de zona horaria y calendario de festivos, accesos o registro de eventos y opciones de reparación.

- Cuando utilice varias zonas horarias dentro de un sistema de control de accesos, cada componentes de cierre que ya se haya creado y configurado en la Administración online de AirKey, podrá tener asignada su propia zona horaria. Se utiliza por defecto la zona horaria predeterminada.
- El calendario de festivos se puede seleccionar o no para cada componentes de cierre. Si no recuerda exactamente los ajustes de los festivos, aquí tiene un vínculo directo al calendario de festivos.

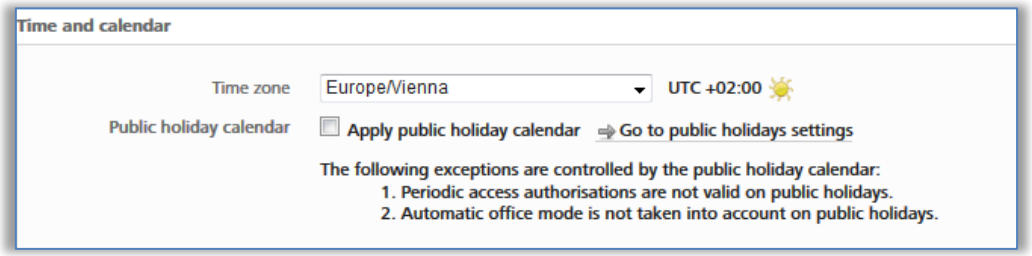


Figura 144: Ajustes – Hora y calendario

- Para cada componente de cierre, puede permitir una apertura permanente manual. En cuanto se elija, aparece la opción de activar la apertura permanente automática.

  Además, usted también puede modificar el período de apertura o activar o desactivar la actualización después de cada desbloqueo. Véase también el capítulo Valores predeterminados (para todos los componentes de cierre recien añadidos).
- Además, el modo Hands-free se puede permitir o no para cada componente AirKey. Si se permite el modo Hands-free, se puede activar el modo Hands-free para este componente AirKey dentro de la app de AirKey. De lo contrario, no se podrá activar en la app de AirKey para este componente AirKey. Encontrará información más detallada sobre el modo Hands-free en el capítulo Hands-free (manos libres) de un vistazo.
- Para cada componentes de cierre, puede adaptar la referencia personal en las entradas de la lista de eventos. Por defecto, el valor predeterminado se toma de la configuración.
  - ***Visible*** se muestran los datos personales de eventos de acceso manera permanente.
  - ***Visible para … días*** convierte los datos personales de eventos de acceso en anónimos tras el número de días definido.
  - ***No visible*** convierte en anónimos todos los datos personales de eventos de acceso de forma permanente.

Figura 145: Lista de eventos

- Aquí encontrará también el vínculo de las opciones de reparación. Encontrará información más detallada sobre las opciones de reparación en Opciones de reparación.
- En comparación con todos los demás componentes AirKey, los lectores murales Bluetooth ofrecen la opción de activar la ***interfaz RS485***. Para ello, la entrada de la lista de eventos del último acceso correcto se puede reenviar a un sistema de terceros a través de la interfaz RS485. Encontrará información más detallada al respecto en el capítulo Detalles técnicos de la interfaz RS485 para lectores murales Bluetooth.
- Haga clic en ***Guardar*** para adoptar los cambios en el componentes de cierre. Aparecerá un mensaje de confirmación.

Dependiendo de los datos del componentes de cierre editados, es posible que aparezca una tarea de mantenimiento para este componentes de cierre. Mediante la actualización del componente con un smartphone con la autorización de mantenimiento o una estación codificadora, se guardarán los cambios y desaparecerá la tarea de mantenimiento.

5.5.4 Eliminar componente de cierre

Si ya no necesita un componentes de cierre en su sistema de control de accesos, puede eliminarlo del sistema de control de accesos.

- En la página de inicio ***Home***, elija la opción ***Cilindros*** o ***Lectores murales***.
- También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.
- Haga clic en la entrada de la lista del componente que desea eliminar del sistema.
- En la parte superior derecha, haga clic en ***Eliminar*** ❶.

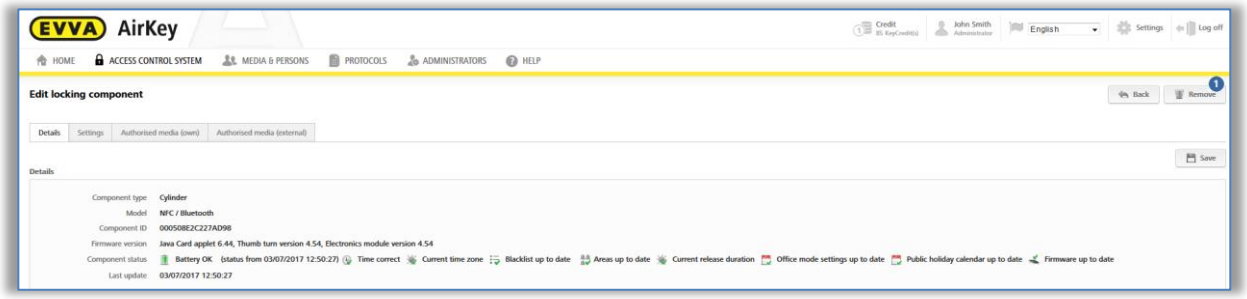


Figura 146: Eliminar componente de cierre

- Confirme la pregunta de seguridad con ***Eliminar componente de cierre***.

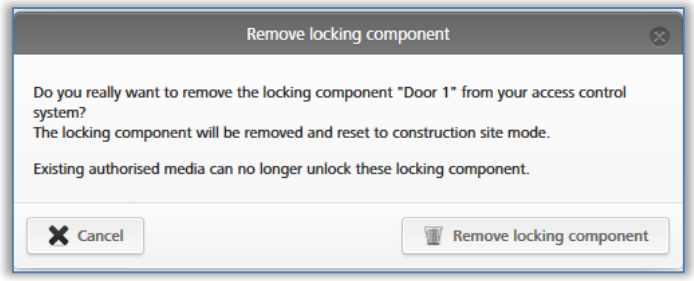


Figura 147: Pregunta de seguridad

> Aparece un mensaje de confirmación y una tarea de mantenimiento, indicando que el componente de cierre debe eliminarse del sistema de control de accesos.

El proceso concluye por completo cuando se actualiza el componente de cierre mediante un smartphone con modo de mantenimiento o una estación codificadora opcional. En cuanto el componente de cierre esté actualizado, se eliminará del sistema de control de accesos.

Este proceso no puede anularse.

Después de eliminarlo, el componente se restablece al modo de fábrica.

Los medios de acceso autorizados antes no pueden bloquear más el componente de cierre. Se eliminan las autorizaciones correspondientes, y no se ven más.

5.5.5 Áreas

Se pueden agrupar varios componentes en áreas paras simplificar la gestión de los permisos en su sistema de control de accesos.

En la página de inicio ***Home***, en la opción ***Áreas*** o en el menú principal ***Sistema de control de accesos → Áreas***, obtendrá una lista de todas las áreas con su estado.

En la lista de áreas, se pueden realizar los continuars ajustes:

> En el campo de búsqueda ❶, introduzca un criterio de búsqueda de tres caracteres como mínimo.

> Haga clic en el encabezado de columna para seleccionarlo como criterio de clasificación.

> La lista de áreas AirKey se puede exportar a un archivo CSV para seguir editándolas ❷.

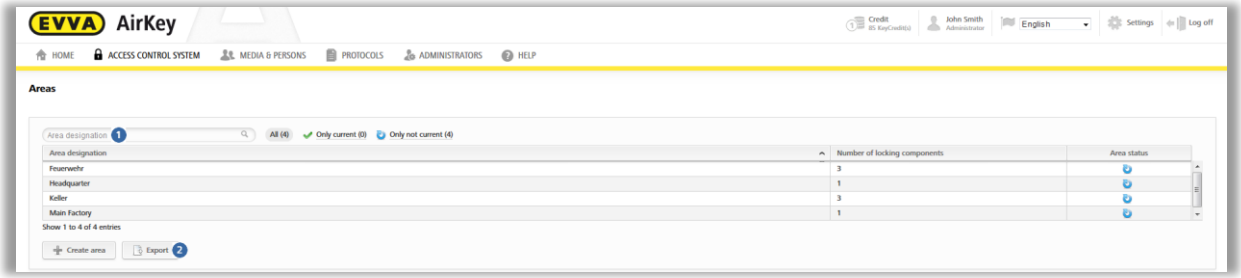


Figura 148: Sistema de control de accesos – Áreas

> Seleccione de la lista el área de la que desee obtener información detallada.

5.5.6 Crear área

No hay áreas creadas de forma predeterminada. Deberá crear nuevas áreas para poder añadir componentes de cierre a áreas.

> En la página de inicio ***Home*** en la barra gris del bloque ***Sistema de control de accesos***, haga clic en ***Añadir*** → ***Crear área***.
> También puede elegir en el menú principal ***Sistema de control de accesos*** → ***Crear área***.
> Elija un nombre significativo para el área.
> Podrá incluir información más detallada sobre el área dentro del bloque ***Notas*** en el campo ***Comentario***.
> Haga clic en ***Guardar*** ❶.

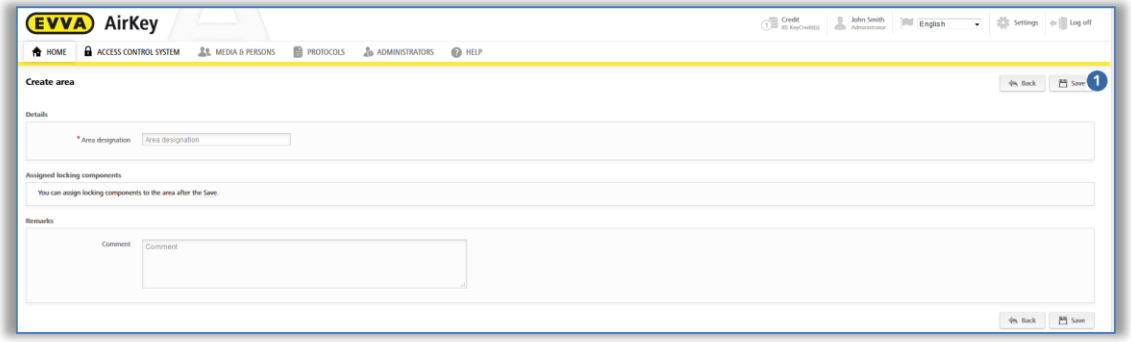


Figura 149: Crear área

La creación de un área se indicará con el mensaje de confirmación "El área ha sido guardada". Podrá añadir componentes de cierre a un área en cuanto esta esté guardada correctamente.

5.5.7 Asignar componentes de cierre a áreas

> En la página de inicio ***Home***, elija la opción ***Áreas*** o en el menú principal ***Sistema de control de accesos*** → ***Áreas***.
> Seleccione de la lista el área en la que desea añadir el componentes de cierre.
> Aparecerán los detalles del área seleccionada. En ***Estado del área*** ❶ figura si todos los componentes de cierre dentro del área están actualizados. En el bloque ***Asignar componentes*** ❷ se relacionan todos los componentes de cierre asignados al área.
> Haga clic en ***Asignar componentes*** ❸ para asignar un componentes de cierre al área.

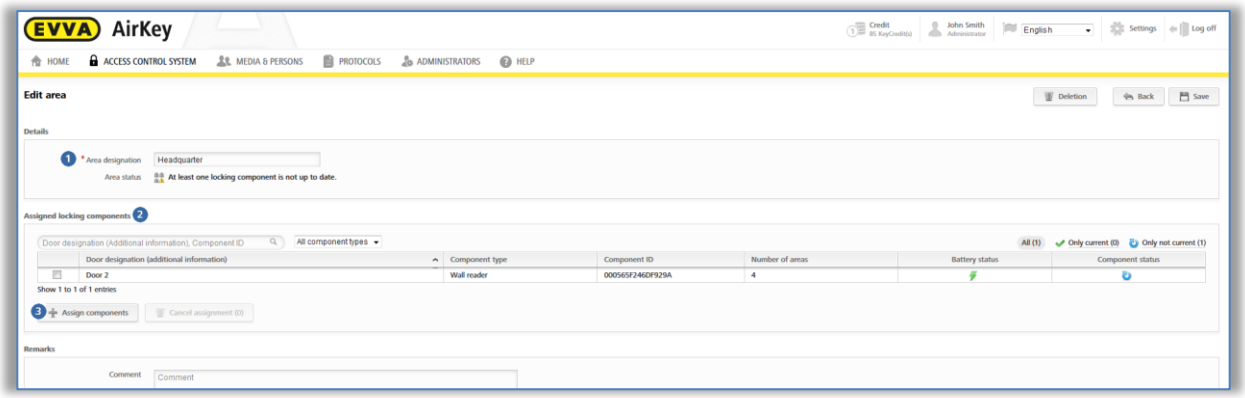


Figura 150: Editar área

Aparecerá una lista con todos los componentes de cierre que no están asignados aún a esta área.

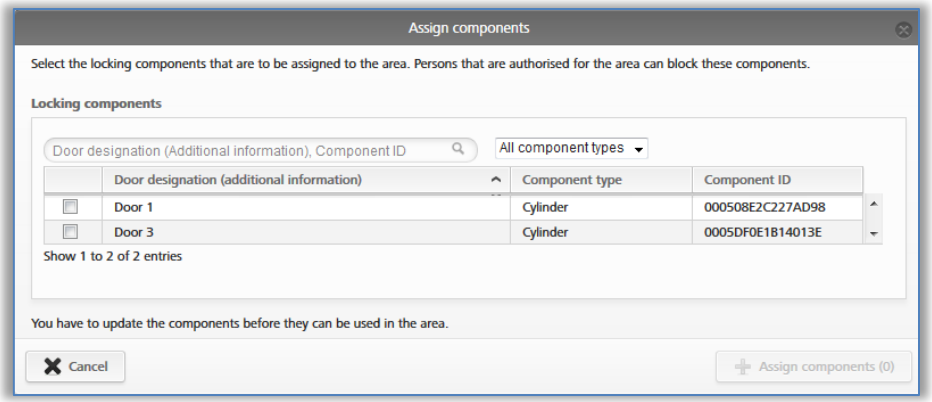


Figura 151: Asignar componentes

- Elija los componentes que desea asignar. (Se pueden seleccionar varios componentes, incluso de diferente tipo.)
- Haga clic en ***Asignar componentes*** para asignar los componentes de cierre al área.
- Haga clic en ***Guardar*** para adoptar los cambios.

Para los componentes de cierre afectados, hay tareas de mantenimiento que pueden desaparecer al actualizar los componentes de cierre correspondientes con un smartphone o una estación codificadora. Tras la actualización, finaliza la asignación de los componentes de cierre al área.

Un componentes de cierre se puede asignar a un máximo de 96 áreas al mismo tiempo.

También podrá editar la asignación a un área de un componentes de cierre directamente en los detalles del componentes de cierre. Encontrará información más detallada en el capítulo Editar componente.

5.5.8 Cancelar la asignación de componentes de cierre a un área

Para anular la asignación de uno o más componentes de cierre a un área, proceda de la continuar manera:

> En la página de inicio ***Home***, elija la opción ***Áreas*** o en el menú principal ***Sistema de control de accesos → Áreas***.

> Elije en la lista el área de la que anular la asignación de componentes de cierre.

> Seleccione en la lista de componentes de cierre asignados las casillas de los componentes de cierre cuyas asignaciones deban ser anuladas. Es posible elegir varios componentes.

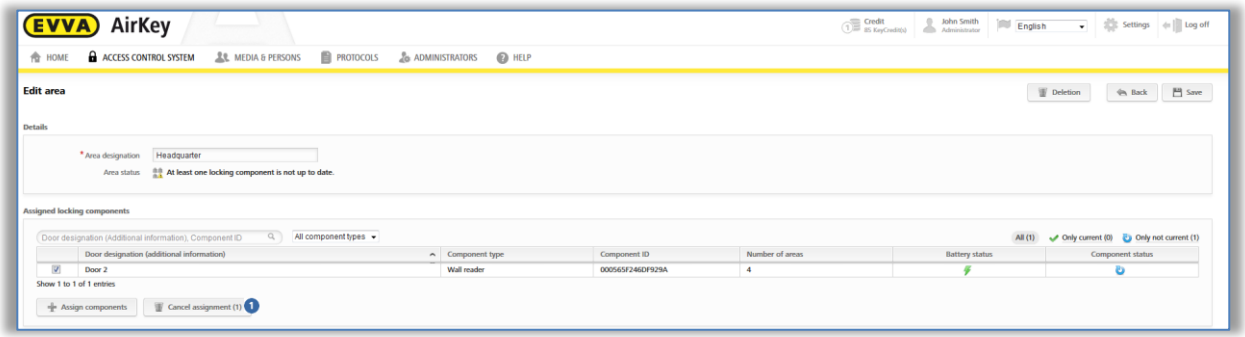


Figura 152: Marcar componentes de cierre

> Haga clic en ***Cancelar asignación*** ❶.

> Aparece una ventana en la que se mostrarán de nuevo los componentes cuya asignación al área se anulará.

> Confirme el cuadro de diálogo también con ***Cancelar asignación***.

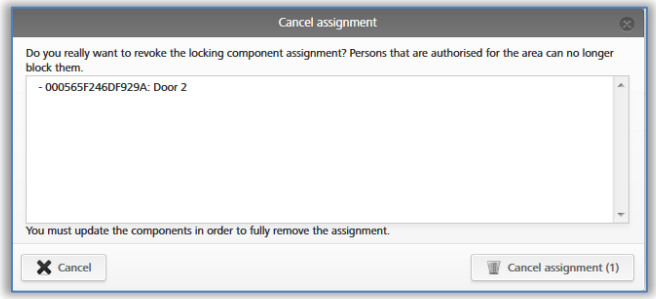


Figura 153: Cancelar asignación

Para los componentes de cierre afectados, hay tareas de mantenimiento que pueden desaparecer al actualizar los componentes de cierre correspondientes con un smartphone o una estación codificadora. Tras la actualización, finaliza la asignación de los componentes de cierre al área.

>

Después de la actualización, las personas que tienen un medio con autorización para esta área ya no pueden operar los componentes de cierre cuya asignación se ha anulado.

También podrá editar la asignación a un área de un componentes de cierre directamente en los detalles del componentes de cierre. Encontrará información más detallada en el capítulo Editar componente.

5.5.9 Borrar área

> En la página de inicio ***Home***, elija la opción ***Áreas*** o en el menú principal ***Sistema de control de accesos → Áreas***.

> Elija en la lista el área que desea borrar.

> Haga clic en ***Eliminar*** ❶.

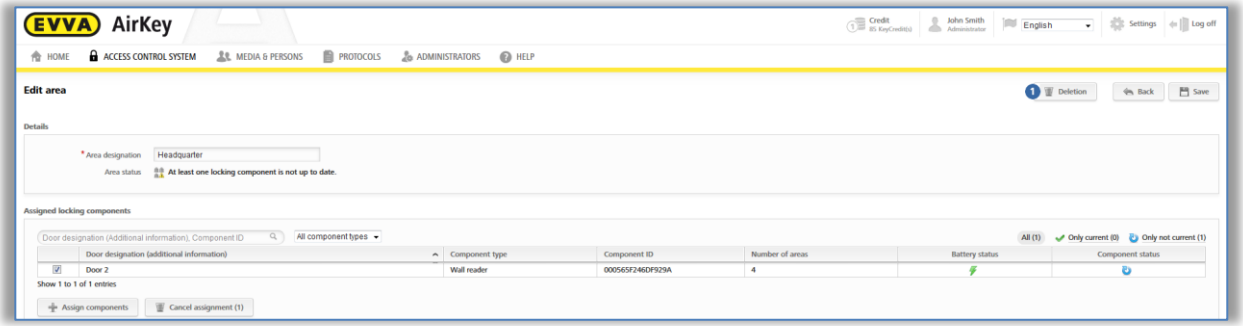


Figura 154: Borrar área

Para un área borrada, se eliminarán automáticamente las autorizaciones existentes sobre el medio, y ya no se mostrarán. El borrado no se podrá deshacer.

Si todavía hay componentes de cierre asignados al área, aparecerá un mensaje de error.

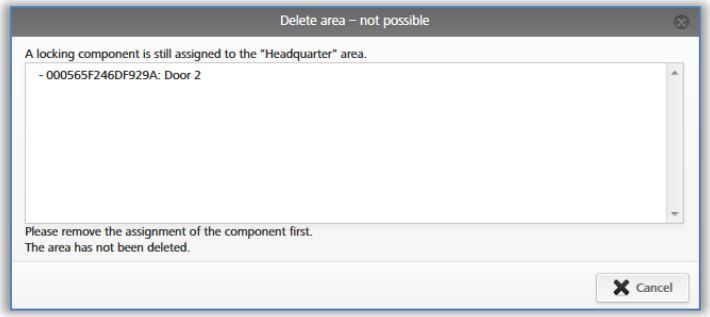


Figura 155: No se puede eliminar el área

> Por ello, anule primero la asignación de todos los componentes de cierre al área y repita a continuación el proceso descrito anteriormente. Encontrará más información sobre la anulación de la asignación de componentes de cierre a áreas en Cancelar asignación de componentes de cierre a un área.

5.5.10 Vista general de autorizaciones

En la vista general de autorizaciones, se muestran todas las autorizaciones de los medios para cada componentes de cierre. La vista general de autorizaciones corresponde al componentes de cierre seleccionado.

Se mostrarán todos los medios que tienen una autorización para un componentes de cierre. Las autorizaciones mostradas no tienen por qué ser válidas en ese momento; es decir, un medio con un acceso único temporal de 08:00 a 17:00 horas para un componentes de cierre, también aparecerá tras las 17:00 horas en la vista general de autorizaciones.

> En la página de inicio ***Home***, elija la opción ***Cilindros*** o ***Lectores murales*** o en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.

> Seleccione de la lista el componente para el que desea ver la vista general de autorizaciones.

> Cambie de la pestaña ***Detalles*** a ***Medios autorizados (propios)*** para ver las autorizaciones de los sistemas AirKey propios, o a ***Medios autorizados (externos)*** para mostrar las autorizaciones de otros sistemas AirKey para el que esté activado el componentes de cierre.

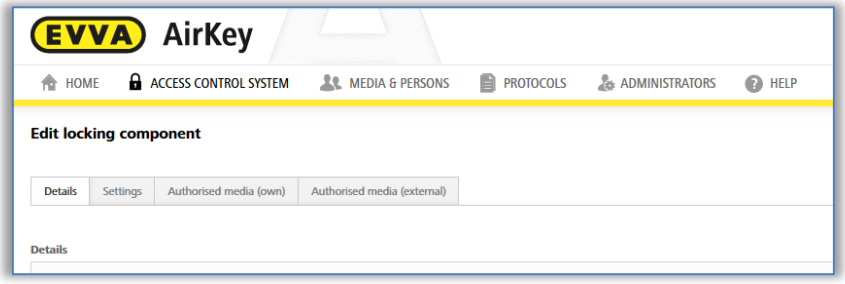


Figura 156: La pestaña de la página "Editar componentes de cierre"

Aparecerá una lista con todas las personas y demás personas relacionadas. Asimismo podrá ver el tipo de medio.

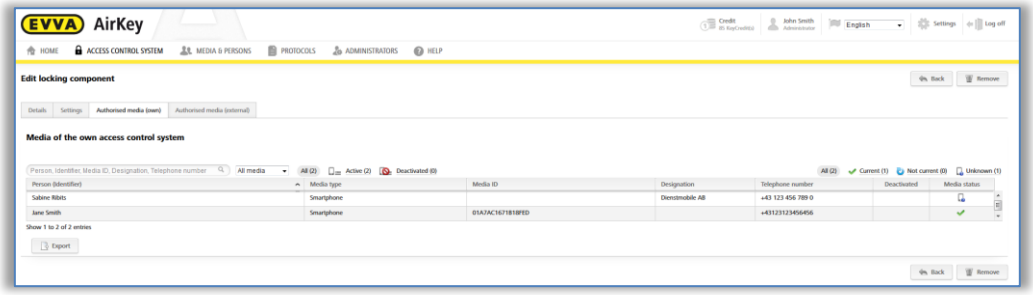


Figura 157: Medios autorizados (propios)

Esta lista se puede buscar, filtrar y ordenar para obtener autorizaciones determinadas.

Haga clic en el nombre de una persona para pasar directamente de la vista general de autorizaciones a las autorizaciones del medio de la persona.

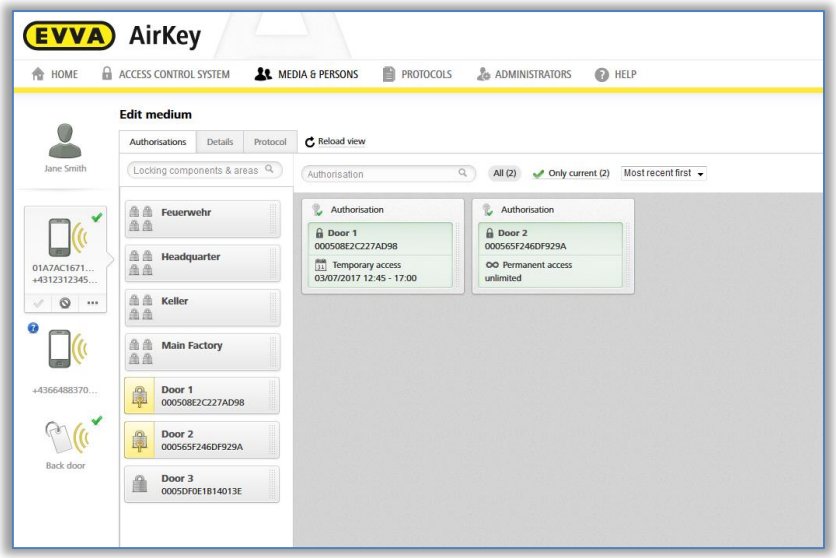


Figura 158: Editar medio

5.5.11 Tareas de mantenimiento

Algunas funciones influyen en la configuración de los componentes de cierre. Estos cambios de la configuración constan como tareas de mantenimiento. Las tareas de mantenimiento se refieren a componentes de cierre cuyo estado no está actualizado.

Aparecerá una lista con las tareas de mantenimiento actuales del sistema de control de accesos tal y como figura a continuación:

- En la página de inicio ***Home***, elija el vínculo ***Tareas de mantenimiento***.
- O haga clic en la barra de estado en ***Tareas de mantenimiento***.
- O elija en el menú principal ***Sistema de control de accesos*** → Tareas de mantenimiento.

Aparecerá una lista general con las tareas de mantenimiento de todos los componentes de cierre del sistema de control de accesos.

En la lista de tareas de mantenimiento, se pueden hacer búsquedas según denominación de la puerta o ID del componente. Se puede ordenar las columnas "Denominación de la puerta (información adicional)", "ID del componente" y "Tareas de mantenimiento".

Además puede establecer prioridades de las tareas de mantenimiento ❶ y descarga PDF ❷ de la lista mostrada.

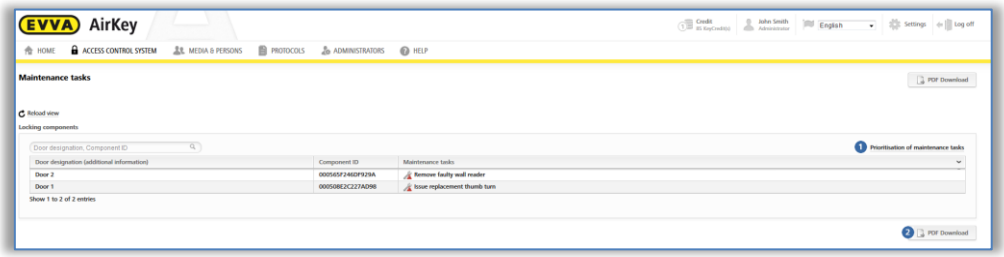


Figura 159: Tareas de mantenimiento

La prioridad de las tareas de mantenimiento se guardará para cada sistema de control de accesos / cliente, y también se aplicará en el smartphone con la app de AirKey instalada y la autorización de mantenimiento activada.

> Haga clic en ***Prioridad de las tareas de mantenimiento***.
> Según el caso, los clientes tienen diferentes necesidades de uso: arrastre los elementos para establecer el orden que desee.
> Guarde la prioridad modificada con ***Aceptar***.

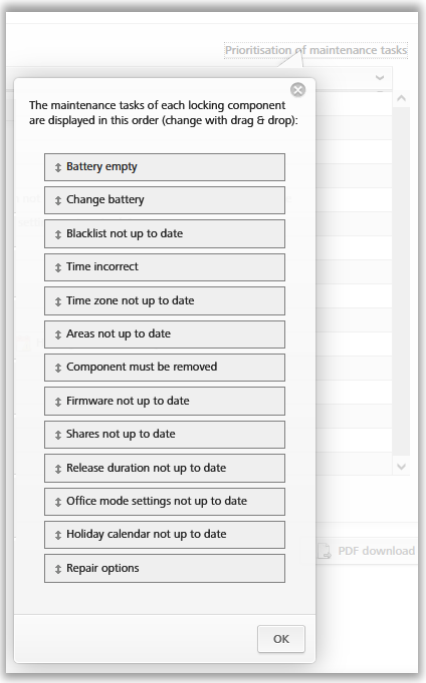


Figura 160: Prioridad de las tareas de mantenimiento

La lista de tareas de mantenimiento se mostrará ahora con la nueva prioridad. Los elementos de la lista de tareas de mantenimiento están vinculados a las páginas con los detalles de cada componentes de cierre.

Cuando se complete una tarea de mantenimiento mediante la actualización del componentes de cierre, el elemento se elimina automáticamente de la lista de tareas de mantenimiento.

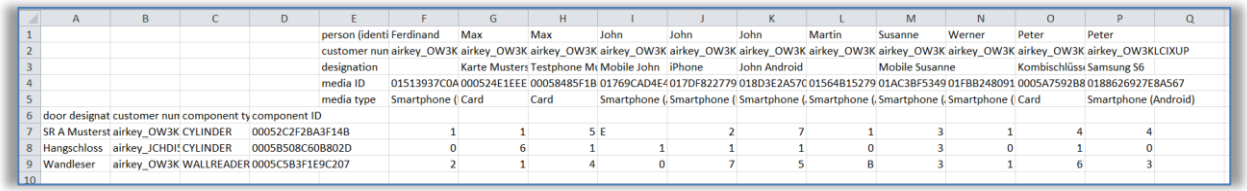
La lista de todas las tareas de mantenimiento pendientes se puede exportar a un archivo PDF e imprimir. Para ello, use el botón ***Descarga PDF***.

5.5.12 Datos de cliente – plan de cierre

Como se ha mencionado ya, se puede modificar posteriormente en el menú ***Datos de cliente*** diversa información introducida durante el registro como, p. ej. el nombre del sistema de control de accesos, el nombre de la empresa o incluso la persona de contacto.

En la página "Editar los datos de cliente" hay un botón a la derecha, en la parte superior, con el que puede exportarse el plan de cierre de todo el sistema de control de accesos. El plan de cierre es una vista general de todos los componentes de cierre de un sistema de control de accesos y los smartphones y medios de acceso asignados.

- Haga clic en el botón ***Exportar plan de cierre***.
- En la ventana de diálogo "Exportar plan de cierre", elija el botón ***Exportar***.
- Haga clic en el vínculo del archivo CSV que aparecerá a continuación en la ventana de diálogo.
- Abra el archivo CSV con el programa deseado o guárdelo.
- Cierre la ventana de diálogo "Exportar plan de cierre" haciendo clic en el botón ***Cerrar***.



	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																	

Figura 161: Plan de cierre

Se pondrá el estado de la Administración online de AirKey para el cálculo del estado de autorización y no el estado real en el medio. Eso significa que el plan de cierre solo será correcto si todos los componentes y medios están actualizados.

Leyenda del plan de cierre:

- **0** – **No autorizado:** El medio carece de autorización para el componente de cierre y para el área a la que se ha asignado el componente de cierre.
- **1** – **Autorización permanente sin fecha de vencimiento:** El medio cuenta con autorización permanente sin vencimiento para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.
- **2** – **Autorización permanente con fecha de vencimiento:** (1) no es aplicable y el medio cuenta con autorización permanente con vencimiento futuro para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.
- **3** – **Autorización periódica sin fecha de vencimiento:** (1) y (2) no son aplicables y el medio cuenta con autorización periódica sin vencimiento para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.
- **4** – **Autorización periódica con fecha de vencimiento:** (1), (2) y (3) no son aplicables y el medio cuenta con autorización periódica con vencimiento futuro para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.
- **5** – **Autorización única:** (1), (2), (3) y (4) no son aplicables y el medio cuenta con autorización individual con vencimiento futuro para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.
- **6** – **Autorización individual:** (1), (2), (3), (4) y (5) no son aplicables y el medio cuenta con una autorización individual con, como mínimo, una subautorización con

vencimiento futuro para el componente de cierre o para un área a la que se ha asignado el componente de cierre; pero no con otras autorizaciones para el componente de cierre o para un área al que esté asignado.

- **7 – Autorización múltiple:** El medio cuenta con, como mínimo, dos autorizaciones que aún no han vencido para el componente de cierre o para un área a la que se ha asignado el componente de cierre.
- **B – Lista negra:** El medio está desactivado; es decir, se ha introducido en la lista negra de los componentes de cierre. Las autorizaciones del medio pierden de esta forma su validez.
- **E – Autorización vencida (todos los tipos):** Todas las autorizaciones del medio para el componente de cierre o para un área a la que se ha asignado el componente de cierre han vencido ya.

5.6 Medios y personas

En el menú principal ***Medios y personas*** ❶ podrá gestionar a todas las personas, medios y autorizaciones en el sistema de control de accesos.

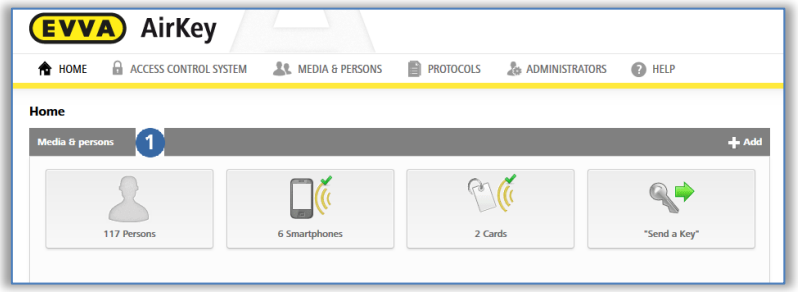


Figura 162: Medios y personas

5.6.1 Vista general de las personas

Si en la página de inicio ***Home*** elige el botón ***Personas*** o en el menú principal ***Medios y personas*** → ***Personas,*** obtendrá una lista de todas las personas creadas con el número de medios y su estado.

En la lista mostrada, podrá utilizar las continuars funciones:

- En el campo de búsqueda ❶, introduzca un criterio de búsqueda de tres caracteres como mínimo.
  Elija el nombre, apellido, ID o la dirección de e-mail.
- Haga clic en el encabezado de columna para seleccionarlo como criterio de clasificación ❷.
- También puede exportar la lista entera en un archivo CSV para seguir editándolo ❸.

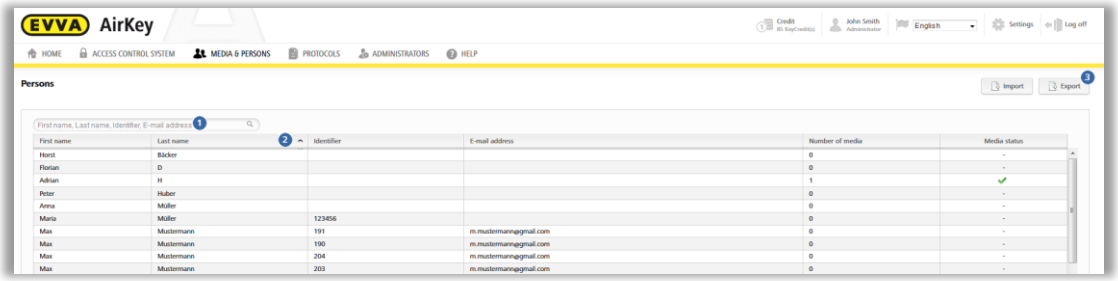


Figura 163: Personas

5.6.2 Crear persona: Véase el capítulo 4.7

5.6.3 Editar persona

En la vista detallada "Editar persona", podrá cambiar los detalles y datos de contacto de una persona o asignarle un nuevo medio.

- En la página de inicio ***Home***, elija la opción ***Personas***.
- También puede elegir en el menú principal ***Medios y personas*** → ***Personas***.
- En la lista de personas, haga clic sobre el nombre de la persona para quien desea hacer modificaciones.
- Modifique los datos según desee.
- Haga clic en ***Guardar***.

En la página "Editar persona" también se puede crear una confirmación de entrega ❶. Se trata de una autorización que se entrega a la persona tras la creación y asignación de todas las autorizaciones necesarias. La confirmación muestra los medios con sus correspondientes autorizaciones de los que dispone la persona en ese momento.

- Elija en la lista de vistas generales la persona para la que desea crear la confirmación de entrega.
- Haga clic en la página "Editar persona" en el botón ***Generar confirmación de entrega (PDF)***.
- Aparecerá la ventana de diálogo "Generar confirmación de entrega (PDF)" en la que el archivo PDF se representa como vínculo.
- Haga clic en el vínculo y abra el archivo PDF con su lector de PDF. También puede guardar el archivo.
- Cierre la ventana de diálogo con el botón ***Cerrar***.

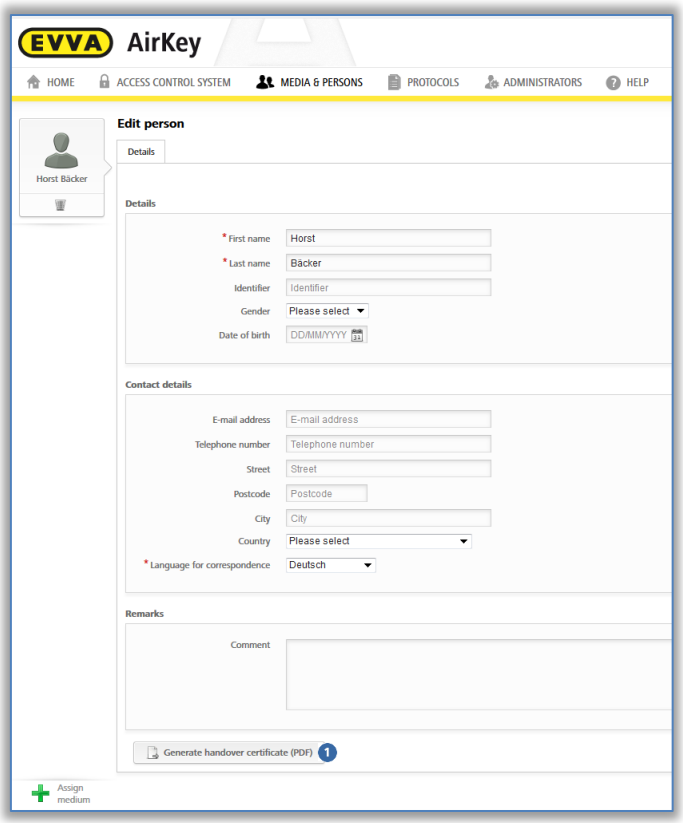


Figura 164: Generar confirmación de entrega

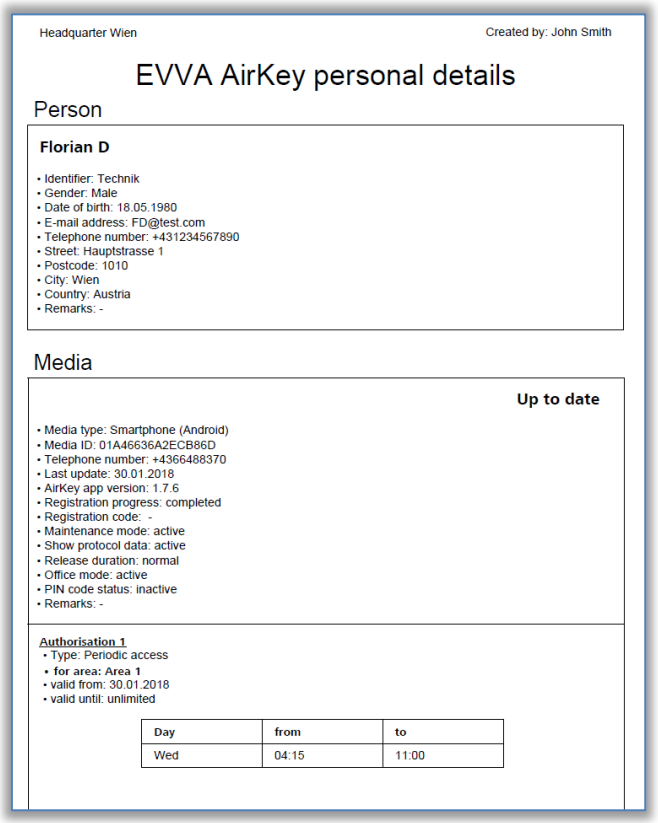


Figura 165: Confirmación de entrega (PDF)

5.6.4 Borrar persona

Cuando desee eliminar una persona del sistema de control de accesos, podrá borrarla.

No se puede borrar una persona con medios asignados aún. Tenga en cuenta que se deben desvincular todos los medios de una persona antes de borrarla.

- En la página de inicio ***Home***, elija la opción ***Personas***.
- También puede elegir en el menú principal ***Medios y personas*** → ***Personas***.
- En la lista de personas, haga clic en el nombre de la persona que desea borrar.
- Haga clic en el símbolo de ***Papelera*** ❶.

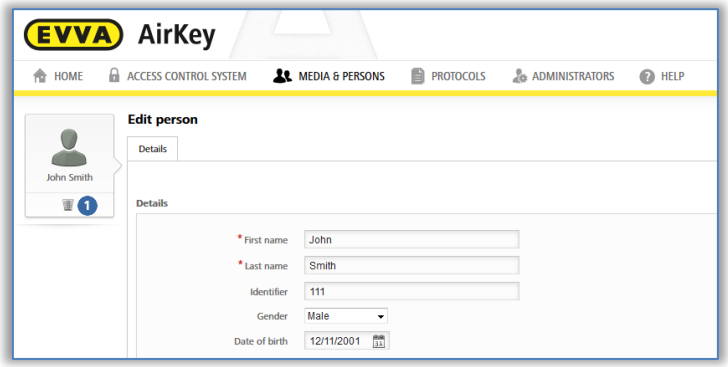


Figura 166: Borrar persona

- Confirme la pregunta de seguridad para borrar a la persona.

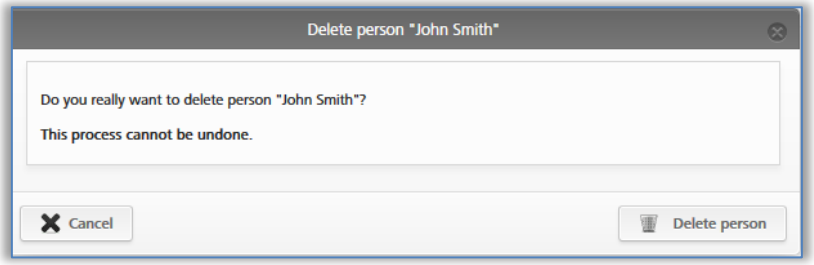


Figura 167: Pregunta de seguridad de borrar persona

La persona borrada no aparecerá más en la lista de personas. En las entradas de la lista de eventos antes de borrar la persona, seguirá documentada la referencia personal sobre los componentes de cierre y los medios.

5.6.5 Asignar un medio a una persona

Deberá asignar el medio a una persona para poder otorgar autorizaciones. Solo así podrá tener una referencia personal en los accesos.

- En la página de inicio ***Home***, elija la opción ***Personas***.
- También puede elegir en el menú principal ***Medios y personas*** → ***Personas***.
- En la lista de personas, haga clic sobre el nombre de la persona para quien desea asignar un medio.
- Haga clic en el botón ***Asignar medio*** ❶.

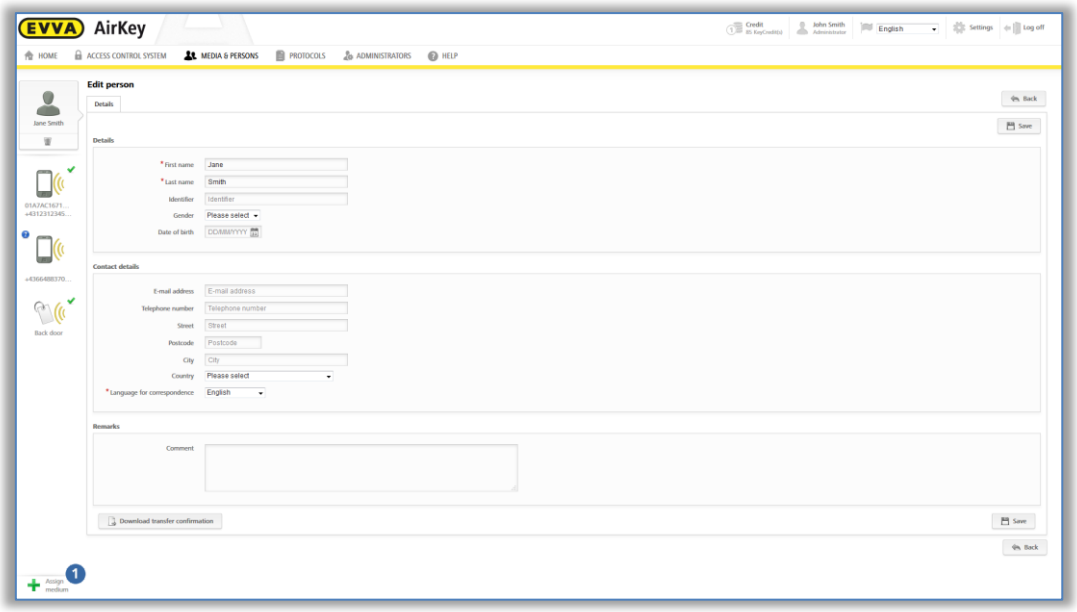


Figura 168: Asignar medio

Aparecerá una lista con todos los medios que se pueden asignar a la persona.
Puede ordenar la lista, filtrar según los tipos de medios o buscar entradas específicas.

Solo se mostrarán medios del sistema de control de accesos que no estén asignados aún a ninguna persona.

> Elija el medio deseado y haga clic en ***Continuar***.

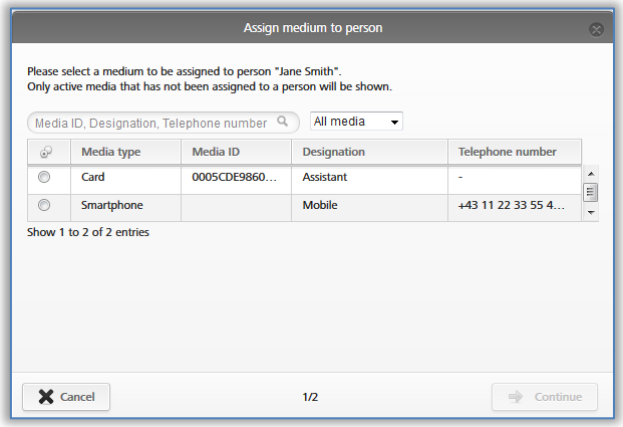


Figura 169: Asignar el medio a una persona

Se mostrarán los detalles después de seleccionar el medio. Si lo necesita, haga clic en ***Atrás*** y seleccione otro medio.

> Haga clic en ***Asignar medio*** para finalizar el proceso.

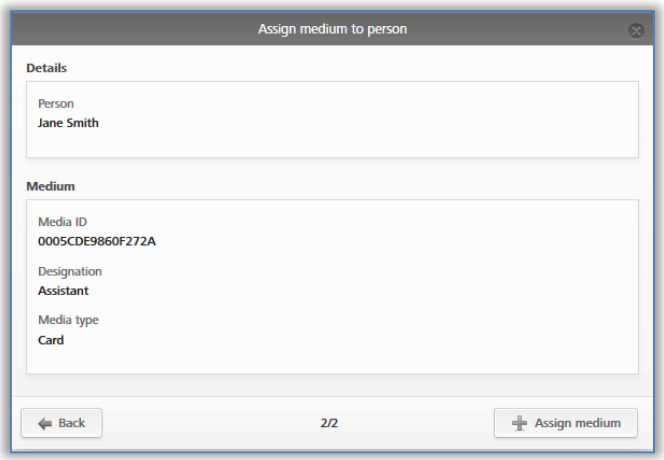


Figura 170: Asignar el medio a una persona

También puede asignar un medio a una persona a través del medio. Encontrará más información en Asignar un medio a una persona.

Se pueden asignar varios medios (smartphones, tarjetas, llaveros o llaves combi) a una persona.

5.6.6 Vista general de los medios

En el menú principal ***Medios y personas*** → ***Medios***, aparecerá una lista de todos los medios (smartphones, tarjetas, llaveros y llaves combi) con la que tendrá una vista general de las autorizaciones otorgadas, una posible desactivación y el estado actual del medio

En esta lista de medios, podrá buscar por medio, filtrar según un estado de medio determinado, cambiar el orden o exportar toda la lista a un archivo CSV.

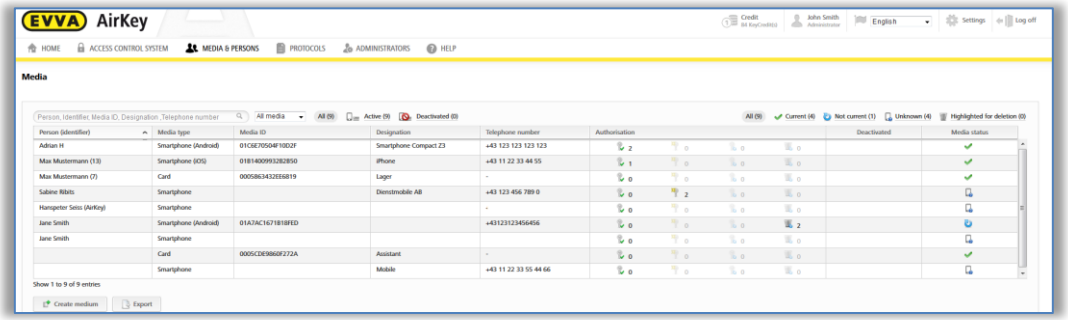


Figura 171: Lista de medios

5.6.7 Crear medio

Para poder gestionar un medio en un sistema de control de accesos, deberá crearlo primero.

- En la página de inicio ***Home***, en la barra gris del bloque ***Medios y personas***, haga clic en ***Añadir*** → ***Añadir medio***.
- También puede elegir en el menú principal ***Medios y personas*** → ***Crear medio***.
- O en la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas*** y ahí ***Crear medio***.

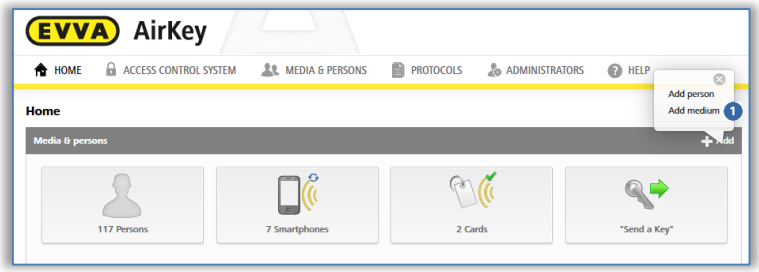


Figura 172: Crear medio

> Elija el tipo del nuevo medio.

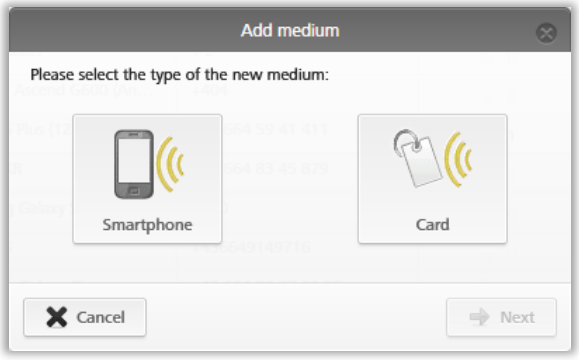


Figura 173: Crear nuevo medio

Desde el punto de vista de la aplicación, no se distinguirá entre tarjetas, llaveros, pulseras y llaves combi, por lo que los llaveros, pulseras y las llaves combi también se deben crear como ***Tarjeta***.

5.6.8 Crear smartphone: Véase el capítulo 4.8

5.6.9 Crear tarjeta, llavero, pulseras o llave combi

Si no tiene una estación codificadora, también puede añadir tarjetas, llaveros, pulseras y llaves combi al sistema de control de accesos mediante un smartphone con autorización de mantenimiento. Siga la información de Añadir tarjetas, llaveros y llaves combi con el smartphone.

> Introduzca una denominación y haga clic en ***Continuar***.

> Inserte la tarjeta, el llavero, la pulsera o la llave combi en la estación codificadora.

Una vez concluido el proceso satisfactoriamente, se abrirá automáticamente la vista detallada de este medio.

Se recomienda expresamente crear suficientes medios preconfigurados (tarjetas, llaveros, pulseras o llaves combi) con autorización permanente ilimitada (medios de emergencia) y guardarlos en un lugar seguro para poder operar el sistema de control de accesos con independencia de la Administración online de AirKey. Encontrará más información sobre la concesión de autorizaciones en Autorizaciones.

Para añadir una llave combi con la estación codificadora, deberá presentar la llave combi en el lado donde se encuentre el símbolo RFID. La llave combi debe mantenerse directamente sobre la estación codificadora. Añadir una llave combi no es posible en toda el área de lectura de la estación de codificación; con el modelo actual (HID Omnikey 5421), la llave combi solo es reconocida en los tercios superior e inferior de la estación codificadora.

Para saber cómo añadir medios al sistema de control de accesos mediante un smartphone con autorización de mantenimiento, vaya a Añadir tarjetas, llaveros y llaves combi con un smartphone.

5.6.10 Editar medio

- En la página de inicio **Home**, elija la opción ***Smartphones*** o ***Tarjetas.***
- También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
- Haga clic en el medio deseado en la lista general.
- Seleccione la pestaña ***Detalles*** para modificar el medio.

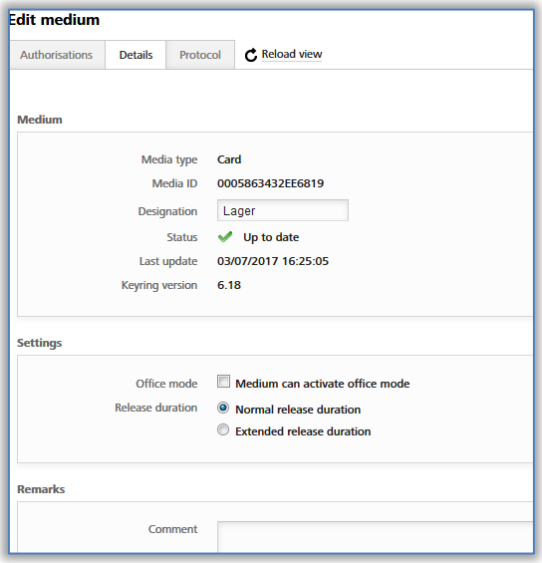


Figura 174: Editar medio – tarjeta

- Al hacer clic en ***Guardar***, se guardarán los cambios.

5.6.11 Asignar un medio a una persona: Véase el capítulo 4.13

5.6.12 Autorizaciones

Mediante las autorizaciones, controla el acceso de las personas a los componentes de cierre. Para poder crear autorizaciones para los medios, los medios deberán estar asignados ya a una persona (encontrará más información sobre la asignación de un medio a una persona en Asignar un medio a una persona).
La vista general de las autorizaciones de un medio se muestra de la continuar manera:

- En el menú principal, elija ***Medios y personas*** → ***Medios***.
- Haga clic en el medio deseado en la lista general.

> El medio ❶ ya está seleccionado (se pueden asignar varios medio a una persona).

> Podrá ver todas las autorizaciones ya asignadas ❷.

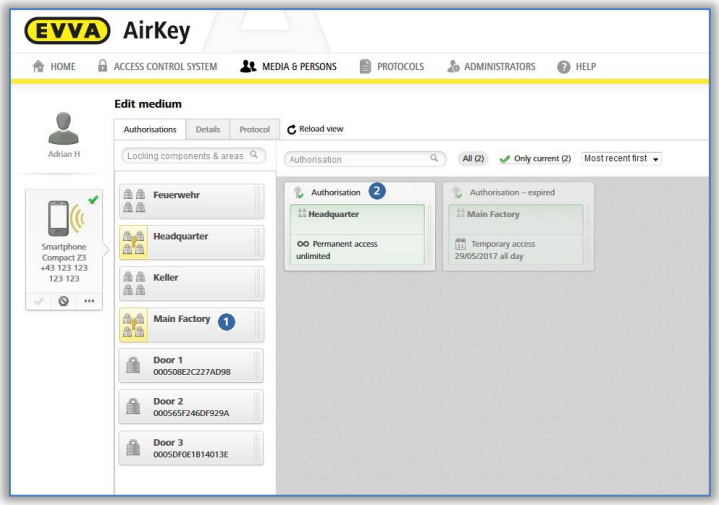


Figura 175: Vista general de autorizaciones

Color de fondo de las autorizaciones:

- ***Verde*** = el estado está actualizado, se creó la autorización y se actualizó el medio.
- ***Azul*** = se creó la autorización pero aún no actualizó el medio.
- ***Amarillo*** = se modificó o borró la autorización, pero no se ha finalizado.
- ***Gris*** = la autorización ha caducado.

También podrá acceder a la vista general de autorizaciones mediante el menú principal ***Medios y personas*** → ***Personas*** tras elegir una persona de la lista que tenga un medio. A continuación, solo deberá hacer clic en el símbolo de medios a la izquierda debajo de la persona seleccionada.

5.6.13 Otorgar autorizaciones: Véase el capítulo 4.14

5.6.14 Crear autorización: Véase el capítulo 4.15

5.6.15 Modificar autorizaciones

Las autorizaciones se pueden cambiar en cualquier momento en la Administración online de AirKey.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** *o* ***Tarjetas.***

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> En la lista general, haga clic sobre el medio del que desea modificar las autorizaciones.

> En la pestaña "Autorización", haga clic en la que desea modificar.

> O arrastre de nuevo las puertas / áreas a la parte central.

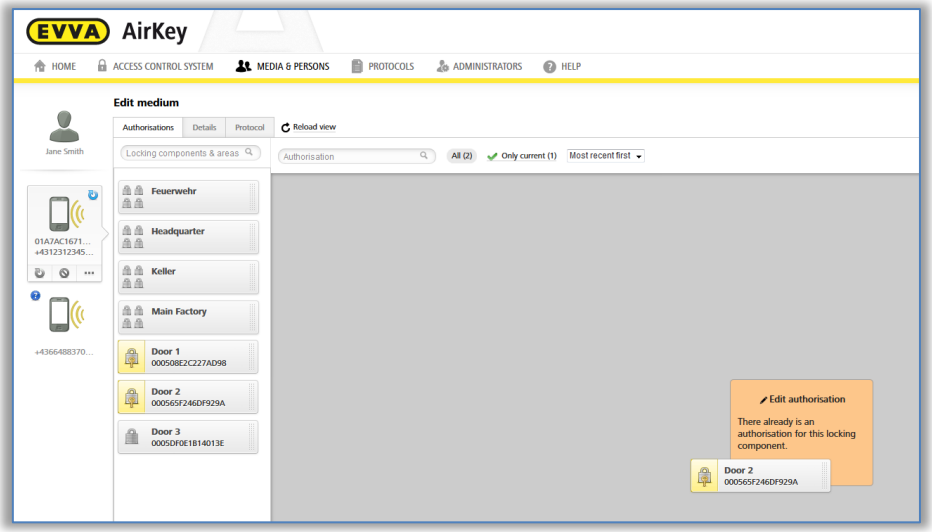


Figura 176: Editar medio – Modificar autorización

> Se mostrarán los detalles de la autorización existente.
> Haga clic en ***Cambiar*** ❶

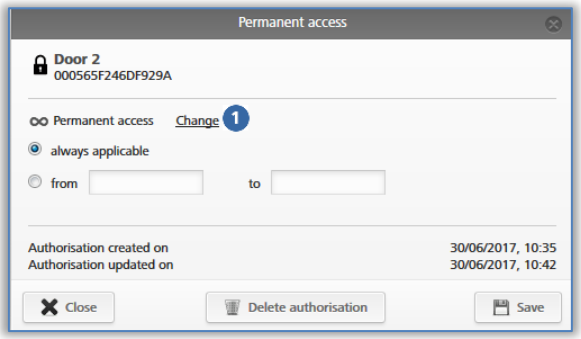


Figura 177: Modificar autorización

> Seleccione el nuevo tipo de acceso.
> Haga clic en ***Cambiar acceso*** ❶.

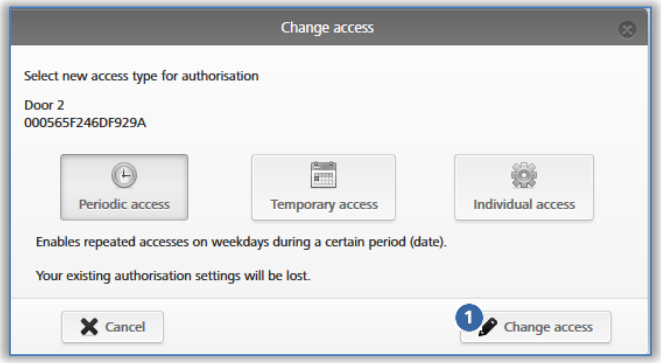


Figura 178: Modificar acceso

> Introduzca los valores modificados en el tipo de acceso correspondiente.
> Haga clic en ***Guardar.***

Para modificar autorizaciones, se requieren crédito en forma de KeyCredits.

> Haga clic en el botón amarillo ***Crear 1 autorización***. Tiene más información en Crear autorización.

> Actualice el medio con "Pull to Refresh" con un smartphone o con la estación codificadora en el caso de una tarjeta, llavero, pulseras o llave combi para finalizar bien el proceso.

5.6.16 Borrar autorización

Si una autorización no se necesita más, se puede borrar en cualquier momento.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> En la lista general, haga clic sobre el medio del que desea borrar las autorizaciones.

> En la pestaña "Autorización", haga clic en la que desea borrar.

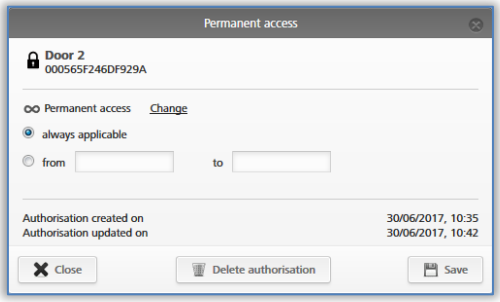


Figura 179: Acceso permanente

> O arrastre las puertas / áreas desde la parte central al campo naranja ***Eliminar autorización***.

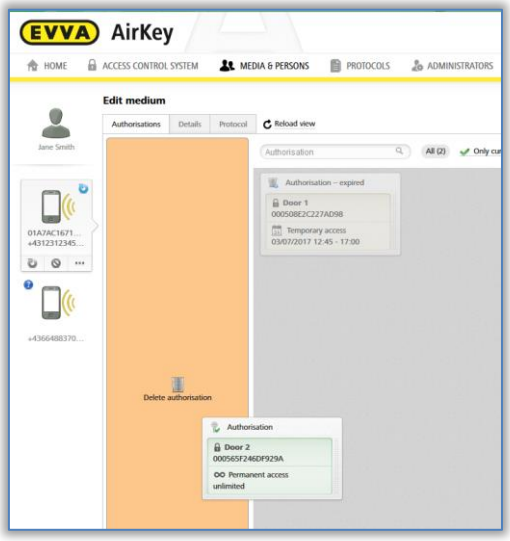


Figura 180: Borrar autorización

> Haga clic en ***Eliminar autorización***.

> Confirme la pregunta de seguridad con ***Eliminar autorización***.

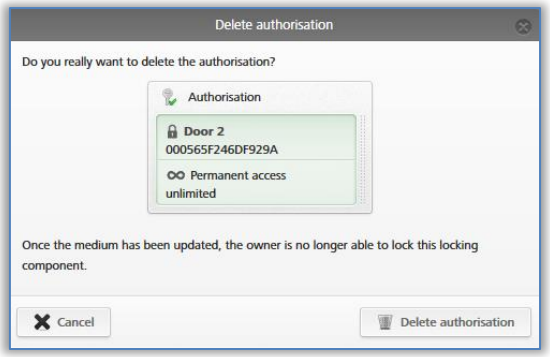


Figura 181: Borrar autorización

> Actualice el medio con "Pull to Refresh" con un smartphone o con la estación codificadora en el caso de una tarjeta, llavero, pulseras o llave combi para finalizar bien el proceso.

El borrado de autorizaciones no cuesta ningún KeyCredit y tiene efecto inmediato. No obstante, la actualización del medio es necesaria para finalizar el proceso de borrado.

No utilice esta función en caso de pérdida del medio. Solo puede borrar autorizaciones de esta forma cuando el medio esté disponible físicamente. En caso de pérdida, utilice la función Desactivar medio.

Si quiere borrar todas las autorizaciones del medio, emplee la función Vaciar medio.

5.6.17 Desactivar medio

Use la función "Desactivar medio" si hay un riesgo de seguridad y se deben invalidar todas las autorizaciones del medio, p. ej. en caso de pérdida o defecto del medio.

Figura 182: Desactivar medio

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas.***
> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
> Haga clic en el medio deseado en la lista general.
> Haga clic en ***Desactivar medio*** ❶.
> Indique la razón para la desactivación. Si elige "Otra", se activará un campo de 50 caracteres.
> Si fuese necesario, introduzca información adicional (máximo 500 caracteres) en "Información adicional".
> Haga clic en ***Continuar***.
> Confirme la pregunta de seguridad con ***Desactivar medio.***

Figura 183: Desactivar medio – Pregunta de seguridad

La desactivación del medio finaliza con un mensaje de confirmación.

Se marcarán todas las autorizaciones del medio para ser borradas. En el caso de tarjetas, llaveros, pulseras y llaves combi, se guardará de inmediato una entrada en la lista negra para todos los componentes de cierre para los que el medio estaba autorizado. En el caso de un smartphone, se creará esta entrada si no se puede contactar con el smartphone en 5 minutos. La entrada en la lista negra implicará la creación de una tarea de mantenimiento para los componentes de cierre afectados. Hasta su actualización, los componentes de cierre afectados estarán en un estado no actualizado.

> Actualice los componentes de cierre para los que el medio tenía una autorización. De esa manera, la tarea de mantenimiento se eliminará de la lista, y los medios desactivados ya no podrán bloquear estos componentes de cierre.

No use esta función para borrar autorizaciones del medio. La desactivación de un medio es una función que afecta a todas las autorizaciones del medio dentro de un sistema de control de accesos.

La desactivación tiene solo efectos en su sistema de control de accesos. Si un smartphone está registrado en varios sistemas AirKey, el estado del smartphone seguirá actualizado en el resto de sistemas AirKey y no desactivado.

Si una persona tiene un smartphone registrado en varios sistemas AirKey, será necesario avisar a los administradores de todos los sistemas AirKey afectados para la desactivación del smartphone.

El medio seguirá estando asignado a la persona. Si desea borrar el medio, deberá anular la asignación. Tiene más información en Revocar asignación.

5.6.18 Eliminar medio desactivado

Un medio desactivado se podrá eliminar de un sistema de control de accesos, aunque el medio no esté disponible. Para los medios perdidos, robados o defectuosos, la base de datos se puede mantener pequeña en la Administración online de AirKey.

La eliminación de un medio desactivado solo es posible si el medio está totalmente desactivado. Eso significa que el medio se actualizó o que, en el caso de los componentes de cierre donde el medio estaba autorizado, la lista negra actualizada se puso al día por una actualización. Hasta que no se satisfagan las condiciones indicadas arriba, no podrá procederse a la eliminación.

- En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas.***
- También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
- En la lista general, haga clic sobre el medio desactivado que se debe eliminar.
- Debajo del símbolo del medio, haga clic en Más y elija Eliminar ❶.
- Confirme la pregunta de seguridad a continuación con ***Eliminar medio*** para eliminar el medio desactivado del sistema de control de accesos.

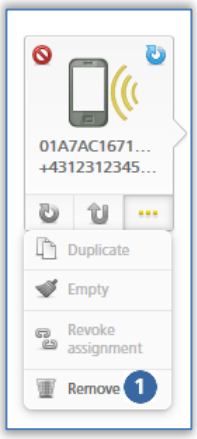


Figura 184: Eliminar medio desactivado

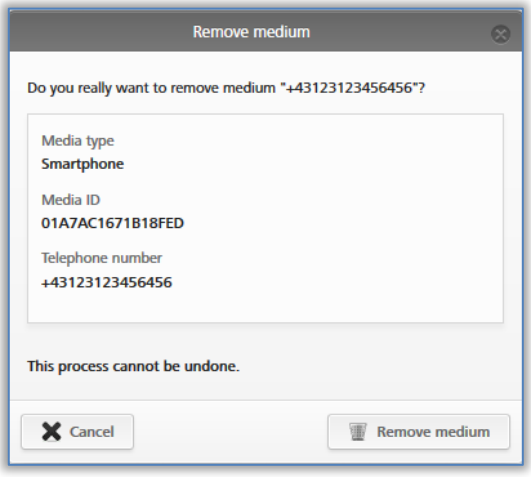


Figura 185: Desactivar medio – Pregunta de seguridad

- Aparecerá un mensaje de confirmación y el medio no aparecerá más en el sistema de control de accesos.

Este proceso no puede anularse. Los medios que sean eliminados del sistema de este modo no se mostrarán más en el sistema de control de accesos y ya no podrán administrarse más.

Los medios no pasarán automáticamente al estado de fábrica.

5.6.19 Reactivar medio

Un medio desactivado, reconocible por el símbolo del círculo rojo ❶ del medio, se puede reactivar si sigue disponible.

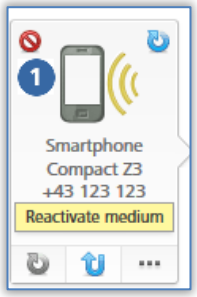


Figura 186: Eliminar medio desactivado

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.
> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
> En la lista general, haga clic sobre el medio que se debe reactivar.
> Haga clic en ***Reactivar medio*** debajo del símbolo del medio.

Figura 187: Reactivar medio

> Indique la razón para la reactivación (máx. 50 caracteres) y decida si desea volver a restablecer las autorizaciones existentes antes de la desactivación.
> Si fuese necesario, introduzca información adicional (máximo 500 caracteres) en "Información adicional". Las informaciones adicionales se documentarán en la entrada de la lista de eventos correspondiente.

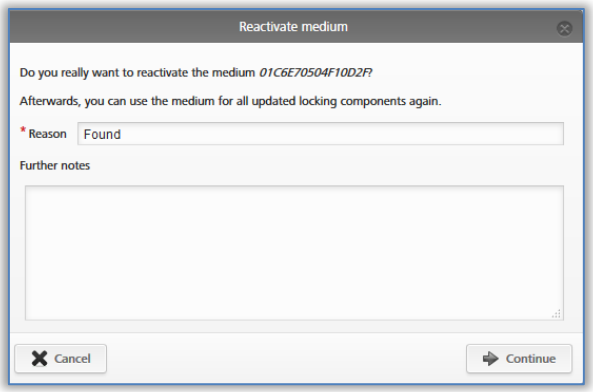


Figura 188: Reactivar medio

> Haga clic en ***Continuar***.
> Confirme una de las dos preguntas de seguridad (dependiendo de desea restablecer las autorizaciones o no) con ***Reactivar medio***.

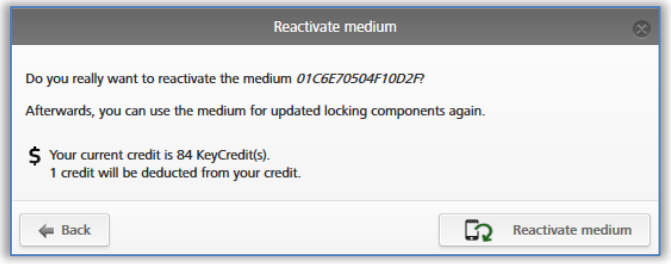


Figura 189: Reactivar medio – Restablecer autorizaciones

La reactivación de un medio finaliza con un mensaje de confirmación.

Si la lista negra del medio reactivado se ha distribuido a todos los componentes autorizados, se crearán de nuevo tareas de mantenimiento para estos componentes de cierre.

Actualice los componentes de cierre que hayan recibido una tarea de mantenimiento por la reactivación de un medio. Cuando se hayan eliminado todas las entradas de la lista negra (es decir, que todos los componentes de cierre afectado hayan sido actualizados), se podrá volver a bloquear el medio en todos los componentes de cierre.

La reactivación del medio es solo válida para su sistema de control de accesos. Si el smartphone se ha desactivado en varios sistemas AirKey, el smartphone seguirá desactivado en otros sistemas AirKey y no se podrá bloquear ahí.

Si una persona ha registrado un smartphone en varios sistemas AirKey, se deberá informar a los demás administradores para la reactivación completa en todos los sistemas AirKey relevantes.

Para el restablecimiento de las autorizaciones, se precisa de un KeyCredit. Para ello, precisa disponer de crédito.

5.6.20 Reemplazo de smartphone

Con la función «**Reemplazar smartphone**» transferirá las autorizaciones y ajustes de AirKey existentes de un smartphone (excepto el PIN y los ajustes locales de modo Hands-free) a otro smartphone. El medio de origen se desactiva automáticamente tras un reemplazo correcto. Encontrará más información sobre el reemplazo de smartphone como administrador en el capítulo Iniciar reemplazo como administrador.

5.6.21 Duplicar medio

Con la función "Duplicar medio", pasa las autorizaciones que tiene un medio a otro. Para ello, es requisito previo que el medio a duplicar disponga de autorizaciones, así como que el medio de destino esté registrado y esté asignado a una persona.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> Haga clic en el medio a duplicar en la lista general.

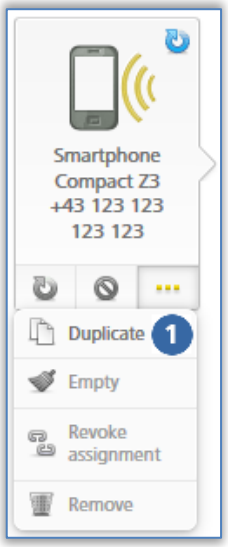


Figura 190: Duplicación de un medio

> Haga clic en ***Más...*** ❶ → ***Duplicar***.
Se abre una lista general con todos los medios asignados a una persona; el medio a duplicar ya no está en esta lista.
> Elija el medio de destino y haga clic en ***Continuar***.
> Finalice el proceso con ***Duplicar medio***.

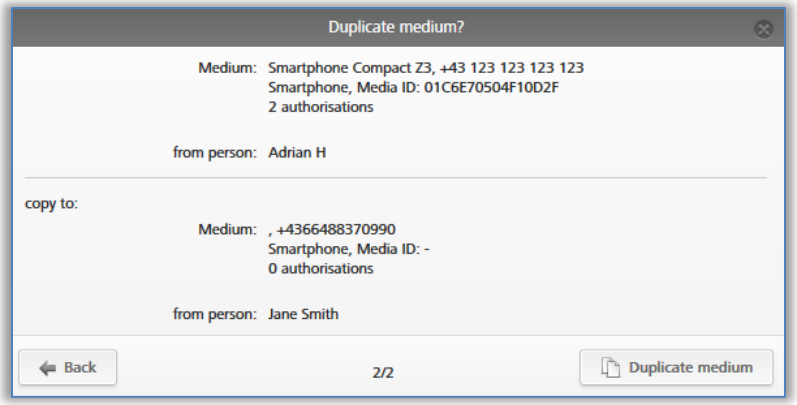


Figura 191: Duplicar medio

Recibirá una confirmación del duplicado. La vista cambiará a una visión general de las autorizaciones del medio de destino.

Se sobrescribirán las autorizaciones existentes en el medio de destino.

Para finalizar el proceso de duplicado, se debe crear y actualizar el medio de destino con ***Crear las autorizaciones***. Tiene más información sobre crear un medio en Crear autorización.

Este proceso cuesta un KeyCredit. Para ello, precisa disponer de crédito.

Si tiene a un gran número de personas en su Administración online de AirKey (véase Importar datos personales) con idénticas autorizaciones, puede asignar entonces una gran cantidad de medios con las mismas autorizaciones a las personas correspondientes en poco tiempo con la función "Duplicar medio".

5.6.22 Vaciar medio

Vacíe el medio si desea borrar todas las autorizaciones del mismo.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.
> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
> En la lista general, haga clic sobre el medio que desea vaciar.

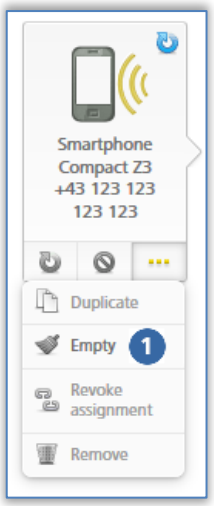


Figura 192: Vaciar medio

> Haga clic en ***Más...*** ❶ → ***Vaciar***.

> Finalice el proceso con ***Vaciar medio***.

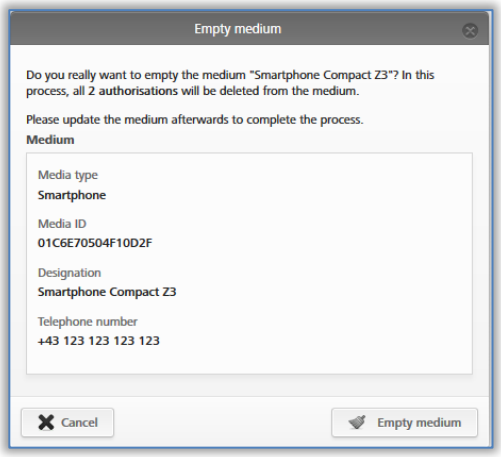


Figura 193: Vaciar medio – Pregunta de seguridad

Todas las autorizaciones se marcarán para ser borradas. El medio debe ser actualizado para que sea efectivo el borrado de las autorizaciones.

El borrado de autorizaciones no cuesta KeyCredits. No obstante, la actualización del medio es necesaria para finalizar el proceso de borrado.

No utilice esta función en caso de pérdida del medio. Solo puede borrar autorizaciones de esta forma cuando el medio esté disponible. En caso de pérdida, utilice la función Desactivar medio.

Si tan solo desea eliminar determinadas autorizaciones, utilice la función Borrar autorización.

5.6.23 Revocar asignación

Anule la asignación si una persona ya no utiliza un medio.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> En la lista, haga clic sobre el medio para el que desee anular la asignación a una persona.

o

> En la página de inicio ***Home***, elija la opción ***Personas***.

> También puede elegir en el menú principal ***Medios y personas*** → ***Personas***.

> En la lista de personas, haga clic en el nombre de la persona para quien desea anular la asignación a un medio.

A la izquierda, debajo del nombre de la persona, se encuentran listados todos los medios asignados. Elija el medio para el que desea anular la asignación.

Figura 194: Medios asignados

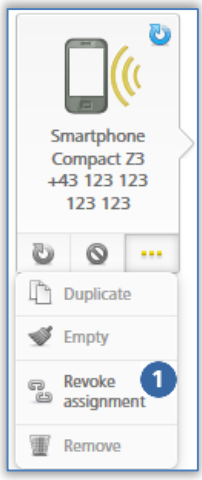


Figura 195: Medio – Revocar asignación

> Haga clic en ***Más...*** ❶ → ***Revocar asignación*** si ya no hay más autorizaciones sobre el medio.

> Confirme la pregunta de seguridad con ***Revocar asignación***.

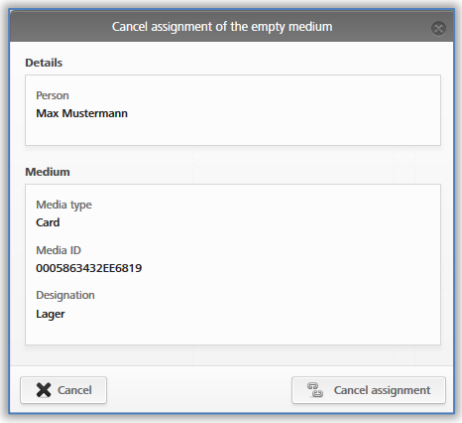


Figura 196: Revocar asignación sin autorizaciones

La anulación de una asignación finalizará con un mensaje de confirmación. La vista cambiará automáticamente a los detalles de la persona.

En los smartphones, debe desactivarse la autorización especial "autorización de mantenimiento" para poder anular la asignación.

Si todavía existen autorizaciones en el medio, se deberán borrar antes. La función ***Vaciar medio*** también se puede usar con la función ***Revocar asignación*** para vaciar todas las autorizaciones del medio.

SI quedan aún autorizaciones en el medio, aparecerá un cuadro de diálogo alternativo al ejecutar la función ***Revocar asignación***. En este cuadro de diálogo, puede elegirse entre vaciar el medio o transferir el medio a otra persona.

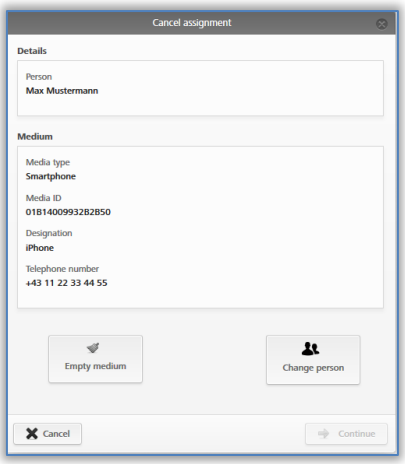


Figura 197: Revocar asignación con autorizaciones

Siempre que se aplique la función ***Vaciar medio*** junto con la función ***Revocar asignación***, se debe ejecutar de nuevo la función ***Revocar asignación*** tras la actualización del medio para finalizar el proceso de borrado de autorizaciones.

Si el medio (incluidas sus autorizaciones) se debe transferir a otra persona, ejecute los continuars pasos:

> Haga clic en ***Más...*** → ***Revocar asignación***.

> Elijar ***Cambiar persona*** y confirme con ***Continuar***.

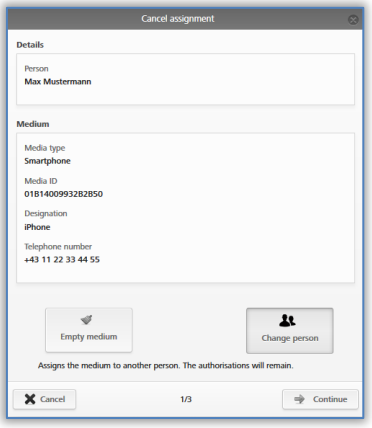


Figura 198: Anular asignación – Cambiar persona

Obtendrá una lista de todas las personas creadas. Seleccione a la persona deseada y confirme con ***Continuar***.

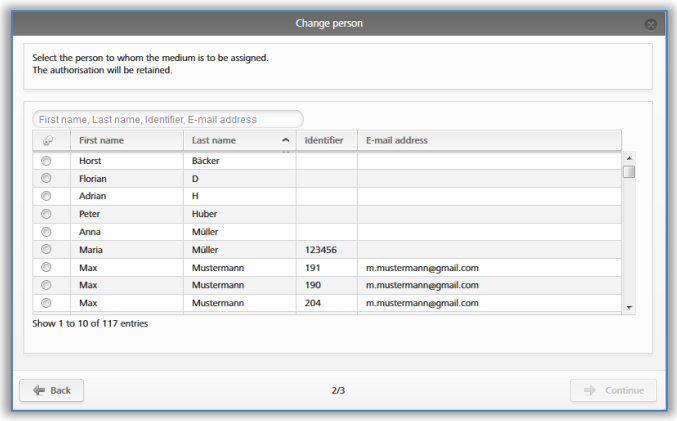


Figura 199: Cambiar persona

Confirme la pregunta de seguridad con ***Cambiar persona*** para finalizar el proceso.

Figura 200: Cambiar persona

El proceso finaliza con un mensaje de confirmación.

5.6.24 Eliminar medio

Elimine un medio si este no se debe mostrar o usar más en su sistema de control de accesos.

Tan solo podrá eliminar el medio si se ha anulado la asignación a la persona. Encontrará más información sobre la anulación de la asignación en Revocar asignación.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas***.
> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
> En la lista general, haga clic sobre el medio que desea eliminar.
> Haga clic en el símbolo de la papelera ❶, situado bajo el símbolo del medio.
> Confirme la pregunta de seguridad con ***Eliminar medio*** ❶.

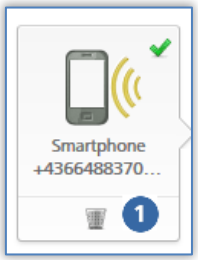


Figura 201: Eliminar medio – Papelera

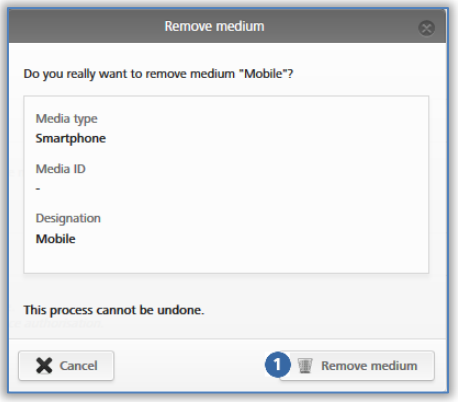


Figura 202: Eliminar medio

Cuando el medio sea eliminado definitivamente, no se mostrará más en la lista general de medios. La vista cambiará a la lista de medios.

Después de ser eliminado del sistema de control de accesos, el medio se encontrará de nuevo en estado de fábrica y se podrá añadir otra vez a otro sistema de control de accesos.

Option

Elimine un medio sin autorizaciones y sin referencia personal a través de la estación codificadora colocándolo sobre esta y haciendo clic en el vínculo ***Eliminar medio del sistema*** dentro del mensaje de estado.

5.7 Listas de eventos

En el menú principal ***Listas de eventos***, obtiene una vista general central sobre todos los eventos de su sistema de control de accesos. Dependiendo de los ajustes general del registro de eventos, mantenimiento y referencia personal en las entradas de la lista de eventos, podrá registrar también accesos denegados (si el medio correspondiente dispone de una autorización existente, aunque no válida en el momento de la apertura, para el componentes de cierre) junto a accesos concedidos y eventos técnicos. Todos los eventos transferidos a la Administración online de AirKey se almacenarán ahí de forma indefinida.

Vuelva a cargar la vista de las listas de eventos de vez en cuando para ver las entradas más actuales en la lista de eventos. Para ello, dispone del vínculo ***Recargar la vista***.

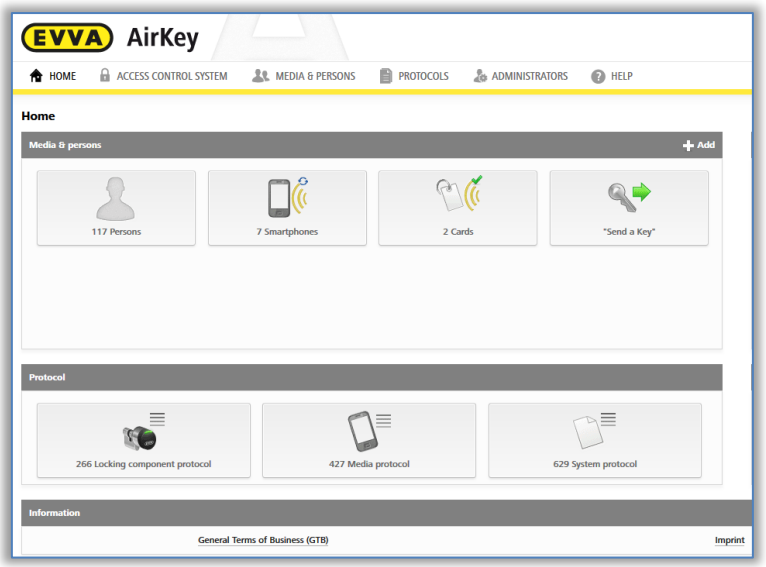


Figura 203: Lista de eventos

Se declara de manera explícita que el presente sistema de AirKey puede ser objeto de registro / autorización de acuerdo con disposiciones legales, en particular con la ley de protección de datos. Por lo tanto, EVVA Sicherheits-technologie GmbH no asume ninguna responsabilidad por el uso de acuerdo con los requisitos legales.

Active la **función de verificación por dos personas para la visualización de las listas de eventos** para garantizar una protección aún mayor de los datos personales. Además, para la vista de la lista de eventos de los medios y componentes, se requiere la confirmación de un segundo administrador del sistema. Encontrará información detallada sobre la activación en el capítulo Aspectos generales

5.7.1 Lista de eventos de componentes de cierre

Si no está activada la **función de verificación por dos personas para la visualización de las listas de eventos**, realice los siguientes pasos para ver la lista de eventos de los componentes de cierre:

- En la página de inicio ***Home***, elija la opción ***Lista de eventos de componentes de cierre***.
- También puede elegir en el menú principal ***Listas de eventos → Componentes de cierre y áreas.***

Si está activada la **función de verificación por dos personas para la visualización de las listas de eventos**, siga adicionalmente los siguientes pasos para ver la lista de eventos de los componentes de cierre:

- Seleccione un segundo administrador del sistema de la lista para enviarle un código de confirmación por correo electrónico y haga clic en ***Enviar código de confirmación***.

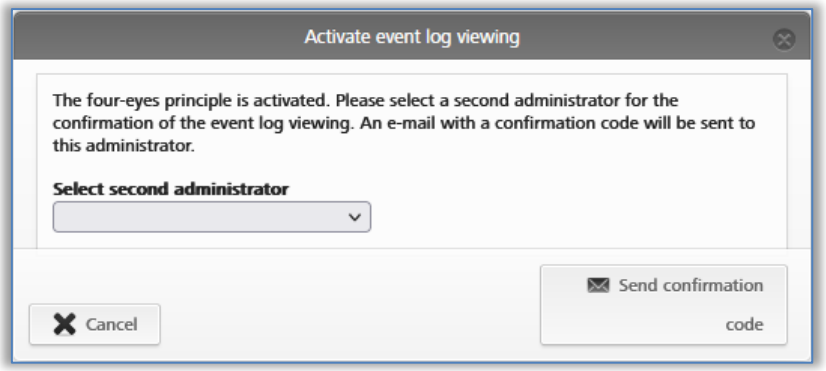


Figura 204: Activación de la visualización de las listas de eventos – seleccionar segundo administrador

> A continuación, se enviará un correo electrónico con un código de confirmación al administrador del sistema seleccionado.

> Este código de confirmación debe introducirse en la administración online de AirKey en un plazo de 10 minutos y confirmarse con el botón ***Activar.***

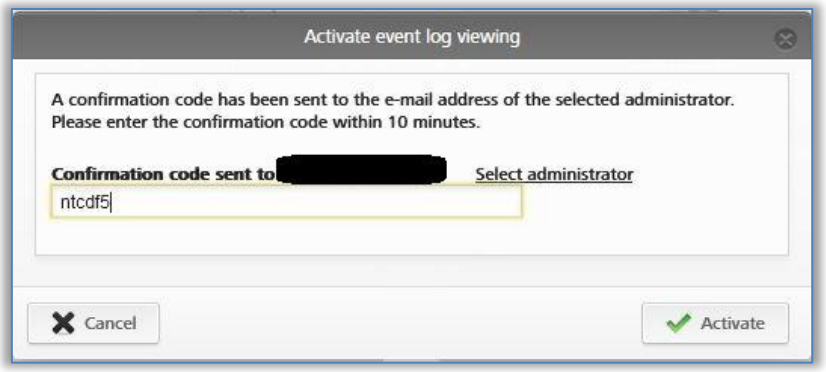


Figura 205: Activación de la visualización de las listas de eventos – introducción del código de confirmación

Si este procedimiento no se completa en 10 minutos, deberá repetirse el proceso. Si el administrador del sistema seleccionado no responde, también se puede seleccionar otro administrador del sistema mediante el enlace ***Seleccionar administrador*** para activar la visualización de las listas de eventos.

A continuación, se muestra la lista de eventos de los componentes de cierre.

La activación de la visualización de las listas de eventos estará activa hasta el siguiente cierre de sesión del administrador del sistema. Esto significa que tanto el protocolo de componentes AirKey como el de medios se pueden ver tantas veces como se desee.

La lista mostrada incluye entradas para componentes de cierre y áreas.

> En caso necesario, en la columna izquierda elija los componentes de cierre o áreas para los que desee ver el lista de eventos. Si desea ver otra vez todos los componentes de cierre y áreas, haga clic en abajo a la izquierda en ***Todas las entradas*** ❶.

- Para la búsqueda de entradas, introduzca al menos 3 caracteres en el campo de búsqueda ❷.
- También se puede activar el filtro ❸ haciendo clic en el vínculo deseado (p. ej. "No autorizado"). Entonces se relacionarán solo entradas para las que se denegó el acceso.
- La lista se ordena, de forma predeterminada, por fecha y hora ❹ (las últimas entradas arriba). Haciendo clic en el encabezado de columna "Fecha, hora", puede modificar la secuencia de la clasificación. Esta tabla no se puede ordenar por otros encabezados de columna.

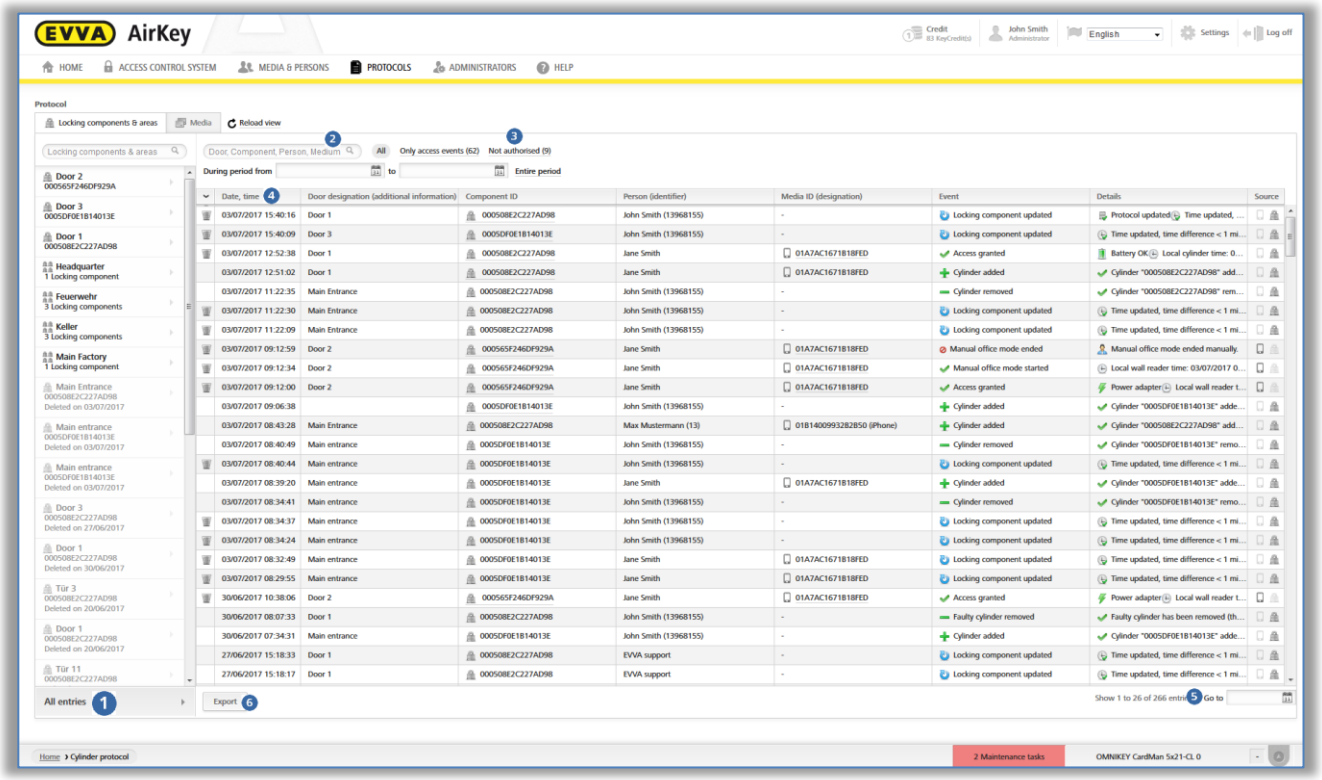


Figura 206: Lista de eventos de componentes de cierre y áreas

- Si la lista debe incluir muchas entradas, puede usar el campo ***Ir a*** ❺ abajo a la derecha para navegar a un día determinado.
- Abajo a la izquierda, utilice el botón ***Exportar*** ❻ si quiere exportar toda la lista de eventos a un archivo CSV. que se puede seguir editando fuera de la Administración online de AirKey.

Dentro de la lista de eventos, se enumeran todas las informaciones necesarias, como la fecha y hora, la denominación de la puerta (información adicional), ID del componente, persona (identificación), ID del medio (denominación) y el evento. También se muestra más información del evento en la columna "Detalles".

En la pestaña "Fuente" puede ver si la entrada de la lista de eventos procede de un medio y/o de un componentes de cierre.

Vuelva a cargar la vista de vez en cuando para ver las entradas más actuales en la lista de eventos. Para ello, dispone del vínculo ***Recargar la vista***.

Utilice los ajustes de registro para limitar la referencia personal en las entradas de la lista de eventos conforme a las pautas de protección de datos. Para los nuevos componentes de cierre añadidos recientemente, determine el tipo de referencia personal en las entradas de la lista de eventos para componentes de cierre a nivel de sistema de control de accesos en los Ajustes de los valores predeterminados para el registro de eventos o en los detalles del componentes de cierre correspondiente.

Solo con la actualización periódica de los componentes de cierre se puede garantizar que todas las entradas de la lista de eventos de los componentes de cierre se hayan transferido a la Administración online de AirKey. Los intervalos recomendados para la actualización dependen de la frecuencia de los componentes de cierre. Tenga en cuenta los Valores y límites en los componentes AirKey.

Solo se registrará un acceso denegado si el medio tiene una autorización para el componentes de cierre, pero esta no era válida en el momento del acceso (por ejemplo, la autorización ha caducado o solo es válida en un período de tiempo determinado).

El estado de las pilas mostrado en la columna "Detalles" es siempre el del componentes de cierre (cilindro) y no el del smartphone.

En los componentes de cierre, si el registro de los eventos está limitado a un determinado período de tiempo, el registro de los eventos AirKey seguirá también al vencer este período. En este caso, solo la referencia personal será anónima.

5.7.2 Lista de eventos de los medios

Si no está activada la **función de verificación por dos personas para la visualización de las listas de eventos**, realice los siguientes pasos para ver la lista de eventos de los medios:

- En la página de inicio ***Home***, elija la opción ***Lista de eventos de los medios***.
- También puede elegir en el menú principal ***Listas de eventos*** → ***Medios***.

Si está activada la **función de verificación por dos personas para la visualización de las listas de eventos**, siga adicionalmente los siguientes pasos para ver la lista de eventos de los medios:

- Seleccione un segundo administrador del sistema de la lista para enviarle un código de confirmación por correo electrónico y haga clic en ***Enviar código de confirmación***.

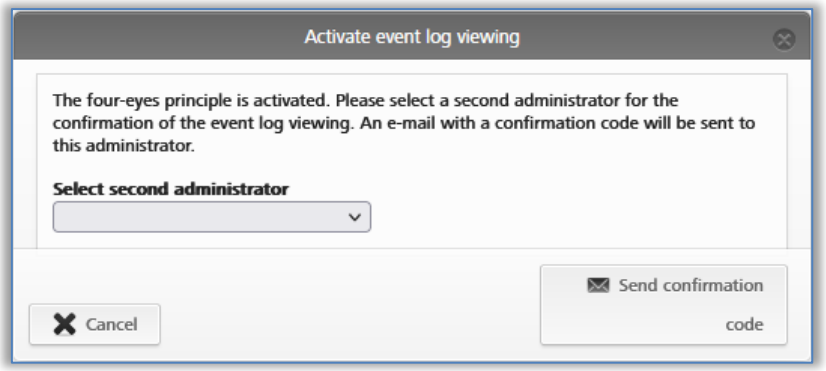


Figura 207: Activación de la visualización de las listas de eventos – seleccionar segundo administrador

> A continuación, se enviará un correo electrónico con un código de confirmación al administrador del sistema seleccionado.

> Este código de confirmación debe introducirse en la administración online de AirKey en un plazo de 10 minutos y confirmarse con el botón ***Activar.***

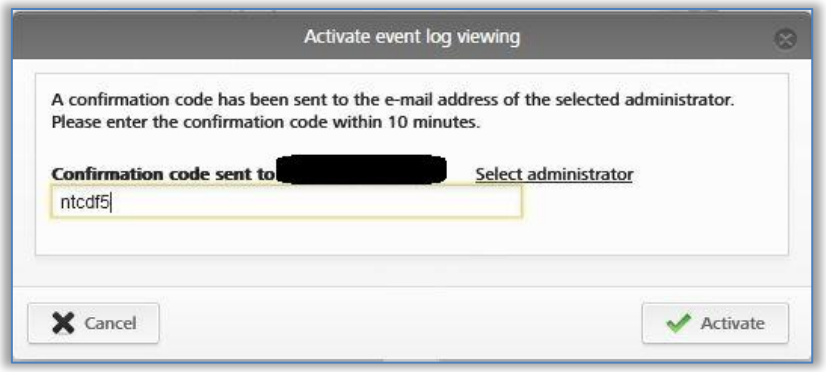


Figura 208: Activación de la visualización de las listas de eventos – introducción del código de confirmación

Si este procedimiento no se completa en 10 minutos, deberá repetirse el proceso. Si el administrador del sistema seleccionado no responde, también se puede seleccionar otro administrador del sistema mediante el enlace ***Seleccionar administrador*** para activar la visualización de las listas de eventos.

A continuación, se muestra la lista de eventos de los medios.

La activación de la visualización de las listas de eventos es válida hasta el siguiente cierre de sesión del administrador del sistema. Esto significa que tanto el protocolo de componentes AirKey como el de medios se pueden ver tantas veces como se desee.

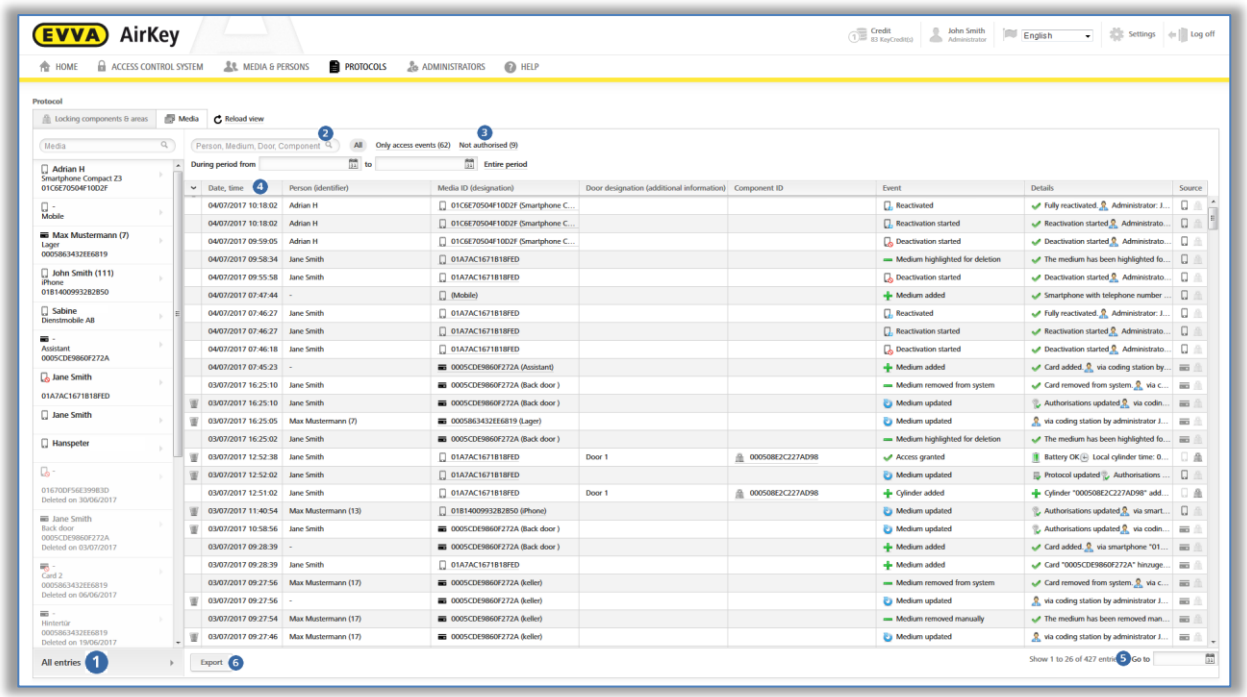


Figura 209: Lista de eventos de medios

Recibirá una lista general con todas las entradas de los medios.

- En caso necesario, elija los medios cuya lista de eventos desea ver en la columna izquierda. Si desea ver de nuevo todos los medios, haga clic abajo a la izquierda en ***Todas las entradas*** ❶.
- Para la búsqueda de entradas, introduzca al menos 3 caracteres en el campo de búsqueda ❷.
- Establezca el filtro, p. ej. "No autorizado" ❸. Entonces se relacionarán las entradas para las que se denegó el acceso.
- Ordene la lista por fecha y hora ❹.
- Utilice el campo ***Ir a*** ❺ abajo a la derecha para ir rápido a un día determinado en una gran lista.
- Use el botón ***Exportar*** ❻ abajo a la izquierda si desea exportar toda la lista de eventos de los medios a un archivo CSV que se puede seguir editando fuera de la Administración online de AirKey.

Dentro de la lista de eventos, se enumeran todas las informaciones necesarias, como la fecha y hora, persona (identificación), ID del medio (denominación), denominación de la puerta (información adicional), ID del componente y el evento. También se muestra más información del evento en la columna "Detalles".

- En la pestaña "Fuente" puede ver si la entrada de la lista de eventos procede de un medio y/o de un componentes de cierre.
- Utilice los ajustes de registro de eventos para limitar la referencia personal en las entradas de la lista de eventos conforme a las pautas de protección de datos. Para los nuevos componentes de cierre añadidos recientemente, determine el tipo de referencia

personal en las entradas de la lista de eventos para componentes de cierre a nivel de sistema de control de accesos en los Ajustes o en los detalles del componentes de cierre correspondiente.

> Las entradas de la lista de eventos de un medio determinado también se pueden ver a través del medio. Para ello, elija el medio deseado en la lista de medios y cambie a la pestaña ***Lista de eventos***.

Solo se protocolizará un acceso denegado si el medio tiene una autorización para el componentes de cierre, pero esta no era válida en el momento del acceso (por ejemplo, la autorización ha caducado o solo es válida en un período de tiempo determinado).

El estado de las pilas mostrado en la columna "Detalles" es siempre el del componentes de cierre (cilindro) y no el del smartphone.

En los componentes de cierre, si el registro de eventos está limitado a un determinado período de tiempo, el registro de los eventos AirKey seguirá también al vencer este período. En este caso, solo la referencia personal será anónima.

Para la lista de eventos de los componentes de cierre y de los medios, las entradas de la lista de eventos con referencia se podrán anonimizar también a posteriori por motivos legales de protección de datos. Las entradas críticas para la protección de datos como, por ejemplo, accesos, tienen el símbolo de la papelera de en la primera columna.

Para anonimizar la referencia personal en las entradas de la lista de eventos, proceda de la continuar manera:

> Busque la entrada de la lista de eventos que quiera anonimizar y haga clic en el símbolo de la papelera en la primera columna.

> Se le pregunta si solo se debe borrar esta entrada de la lista de eventos todas las entradas sobre esta persona. Elija la opción deseada.

> Introduzca un motivo para borrar la entrada de la lista de eventos.

> Marque la casilla ***Deseo eliminar irrevocablemente la entrada de la lista***.

> Para finalizar el proceso, confirme con ***Eliminar***.

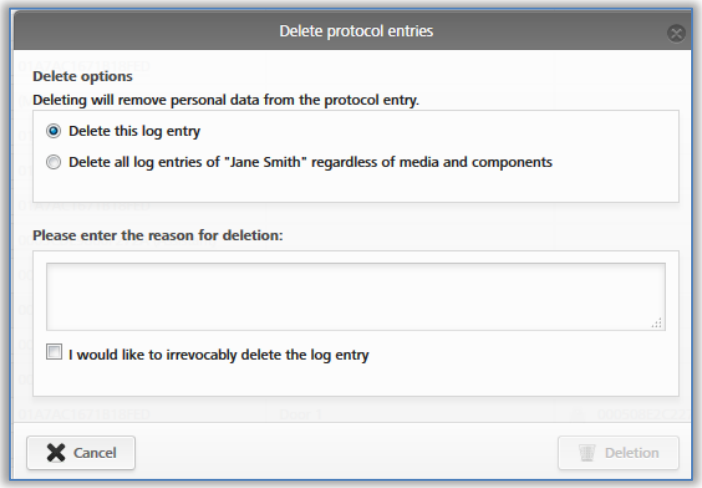


Figura 210: Borrar entradas de la lista de eventos

La entrada de la lista de eventos no se borra por completo, sino solo la referencia personal. De esta manera, se anonimiza la entrada de la lista de eventos. Este proceso no puede deshacerse. Use esta función con precaución.

El borrado de una entrada de la lista de eventos se relaciona en la lista de eventos del sistema.

5.7.3 Lista de eventos del sistema

- En la página de inicio ***Home***, elija la opción ***Lista de eventos del sistema***.
- También puede elegir en el menú principal ***Listas de eventos*** → ***Sistema***.

Obtendrá una vista general de todas las acciones ejecutadas por los administradores.

- En el campo de búsqueda ❶, puede buscar por administrador, identificador de usuario, acción, ID de transacción, ID de medio o de componente. Introduzca un período de tiempo determinado ❷ y seleccione la columna que se debe usar para ordenar ❸.
- Introduzca una fecha en ***Ir a*** ❹ para poder ir directamente en esa fecha a un día en la lista de eventos del sistema. Si no hay ninguna entrada para la fecha introducida, se elegirá la entrada más cercana.
- Use el botón ***Exportar*** abajo a la izquierda si desea exportar toda la lista de eventos del sistema a un archivo CSV que se puede seguir editando fuera de la Administración online de AirKey.

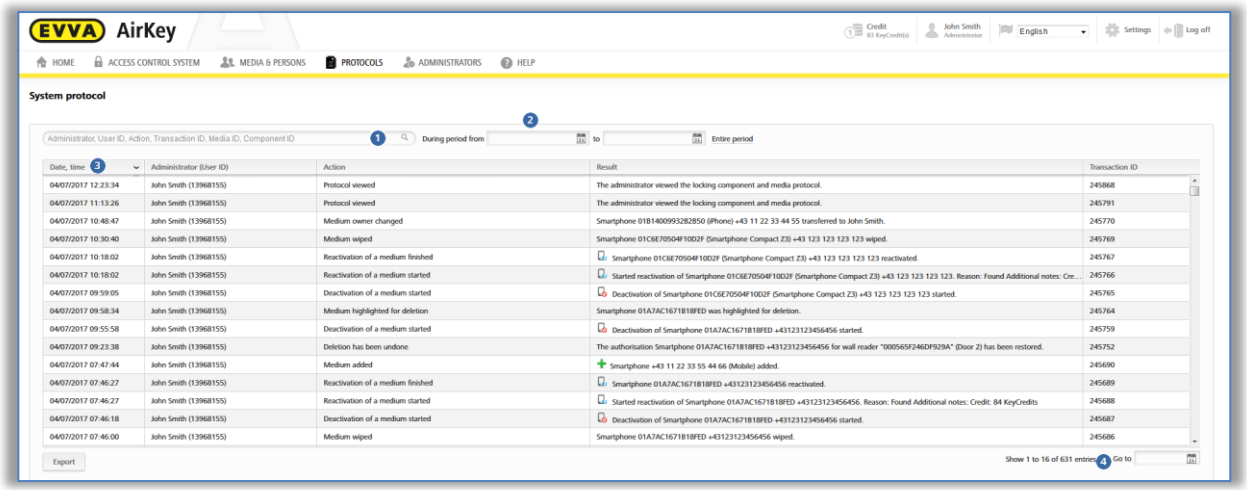


Figura 211: Lista de eventos del sistema

En la lista de eventos del sistema, no se puede borrar ninguna entrada de la lista.

La función de verificación por dos personas para la visualización de las listas de eventos no se aplica a la lista de eventos del sistema. Esto significa que los administradores del sistema siempre pueden ver la lista de eventos del sistema.

5.8 Logins para soporte

Mediante la creación de una autorización de soporte, puede crear un administrador temporal en caso de necesitar asistencia en AirKey. A través de la autorización de soporte, se pueden ver todos los datos del sistema de control de accesos.

El destinatario de la autorización de soporte tendrá los mismos derechos que el administrador durante el período de autorización.

5.8.1 Crear login de soporte

> En el menú principal, elija ***Administradores*** → ***Logins para soporte***.

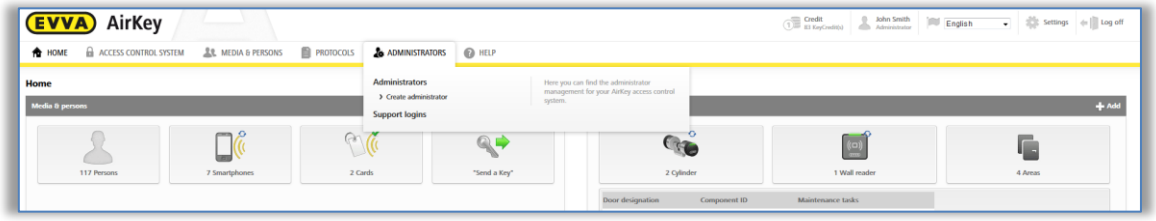


Figura 212: Logins para soporte

Si ya ha creado logins para soporte, se mostrarán en una lista.

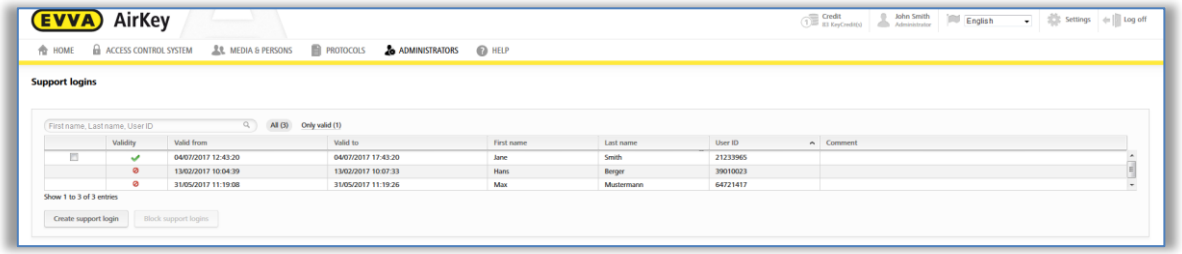


Figura 213: Lista de logins para soporte

> Haga clic en ***Crear login de soporte***.

> Rellene el formulario ❶.
Los campos marcados con * son obligatorios.

La duración de la autorización está entre 1 y 24 horas como máximo.

> Haga clic en ***Guardar***.

La autorización de soporte se ha creado, junto con un identificador de usuario y contraseña ❷.

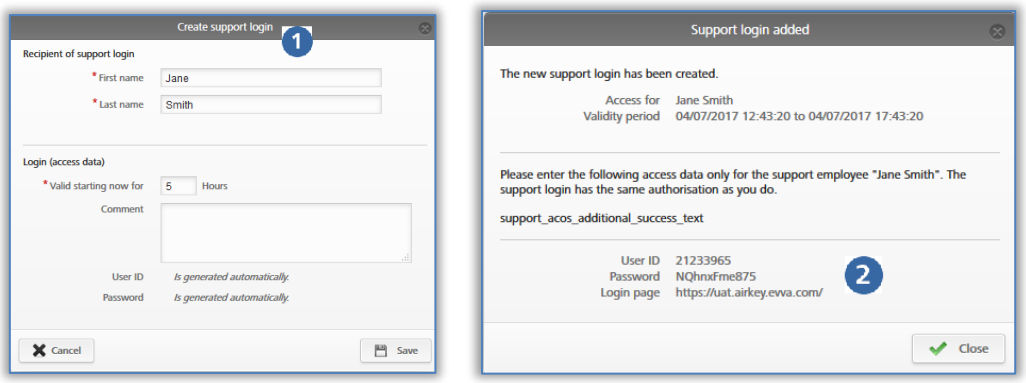


Figura 214: Crear login de soporte

La contraseña no se mostrará más después de cerrar la ventana.

Por su propio interés, les recomendamos que los datos de inicio de sesión se comuniquen de una manera segura.

> ***Cierre*** la ventana de diálogo "Soporte de login añadido" si se han facilitado los datos al socio de soporte.

5.8.2 Bloquear logins de soporte

La autorización de soporte terminará automáticamente tras vencer la duración fijada. No obstante, también se puede anular antes con la función ***Bloquear logins de soporte***.

Si desea anular con anterioridad la autorización de soporte, proceda de la continuar manera:

> En el menú principal, elija ***Administradores*** → ***Logins para soporte***.

En la lista de autorizaciones de soporte, verá si una autorización de soporte es válida en ese momento ❶, así como la duración de la validez ❷.

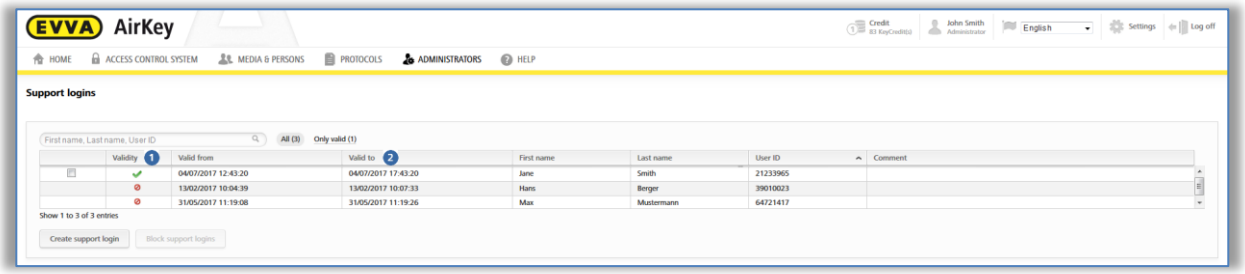


Figura 215: Vista general de las autorizaciones de soporte

> Elija el destinatario de la autorización de soporte cuya autorización desea finalizar.

> Haga clic en ***Bloquear logins de soporte***.

> Confirme la pregunta de seguridad con ***Bloquear logins de soporte***.

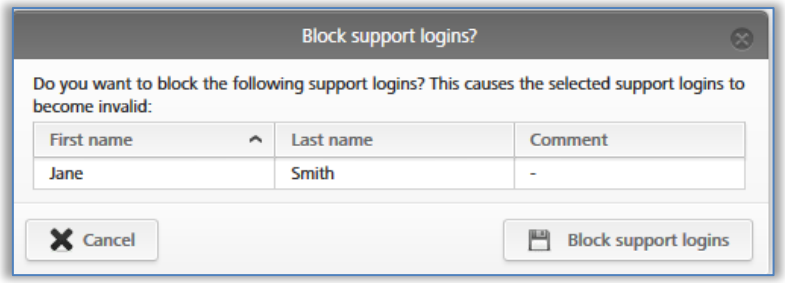


Figura 216: Bloquear logins de soporte

En la lista de autorizaciones de soporte, podrá reconocer con el símbolo en la columna "Validez" ❶ que la autorización está bloqueada.

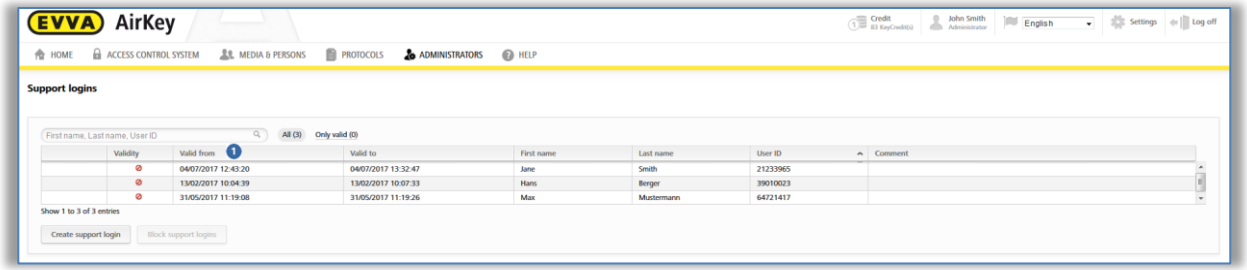


Figura 217: Validez de las logins de soporte

Tanto las tareas realizadas del destinatario de la autorización de soporte, como la creación y bloqueo de la autorización de soporte, se registrarán en las listas de eventos.

5.9 Ayuda

Encontrará más información en el menú principal ***Ayuda*** o en el sitio web de EVVA AirKey en https://www.evva.com/es/airkey/website/. Si necesita asistencia, diríjase a su distribuidor de EVVA.

6 App de AirKey

Este capítulo le ofrece una visión general acerca de las funciones que puede ejecutar con su smartphone dentro de la aplicación de AirKey.

Para utilizar un smartphone con AirKey, tiene que cumplir los continuars requisitos:

- El smartphone cumple los requisitos del sistema para AirKey.
- La app de AirKey se ha instalado correctamente en el smartphone.
- Debe haber una conexión disponible a Internet.

Mediante el uso de "optimizaciones de app", p. ej. para respetar la batería, se puede ver afectada la funcionalidad de la app. Posibles efectos: El proceso de apertura dura más, los bloqueos de fondo funcionan de manera inestable, etc.

6.1 Componentes Bluetooth

En este punto de menú, se llega a una lista general que muestra todos los componentes de cierre con Bluetooth al alcance. En esta página, se puede, p. ej., conectar con componentes, desbloquear componentes Bluetooth o conectar con componentes NFC mediante el símbolo arriba a la derecha.

La denominación de los componentes Bluetooth se muestra tras una actualización del smartphone, es decir la indicación de la denominación de un componentes de cierre dentro de la app de AirKey no se modifica automáticamente si no se ajusta en la Administración online de AirKey.

A partir de Android 6, Google ha establecido que para el reconocimiento de los componentes de Bluetooth se requerirá autorización para la determinación de la ubicación en el smartphone.

6.2 Registrar smartphone: Véase el capítulo 4.9

6.3 Autorizaciones

Si su smartphone está registrado en el sistema de AirKey y ya dispone de autorizaciones creadas en la Administración online de AirKey, podrá visualizar las autorizaciones del smartphone en cualquier momento.

- Inicie la aplicación de AirKey.
- En el menú, elija ***Autorizaciones***.

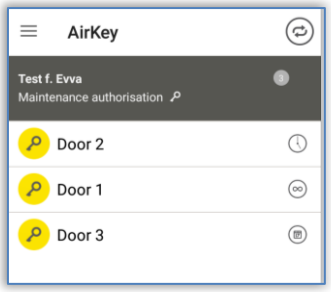


Figura 218: App de AirKey – Vista general de autorizaciónes

> Haga clic en una de las autorizaciónes para ver los detalles de la misma. Los datos de ubicación (coordenadas GPS o dirección) se representan aquí como vínculo. Si hace clic en el vínculo, se le reenvía automáticamente al proveedor de mapas configurado de forma predeterminada en su smartphone.

> En los detalles de la autorización, también puede activar individualmente para cada autorización el modo Hands-free. El requisito para ello es que el administrador haya permitido el modo Hands-free en el componente AirKey, que no se haya configurado ningún PIN para la app de AirKey y que se haya activado el modo Hands-free en los ajustes de la app.

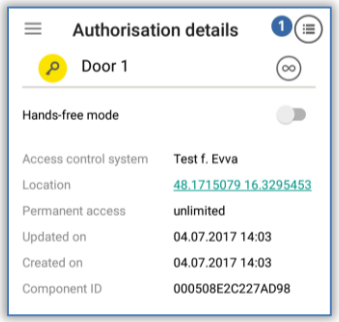


Figura 219: App de AirKey – Detalles de la autorización

Si la autorización de acceso ha caducado, se mostrará de forma pertinente.

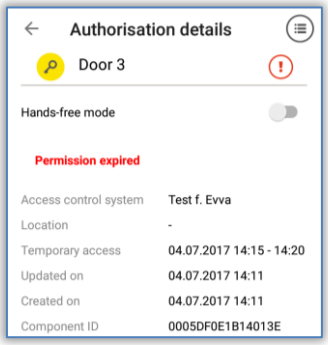


Figura 220: Autorización caducada

Si su smartphone está autorizado para mostrar los datos de la lista de eventos (véase Datos de la lista de eventos en la app de AirKey), podrá ver la lista de eventos de la llave para la autorización seleccionada en los detalles de la autorización ❶.

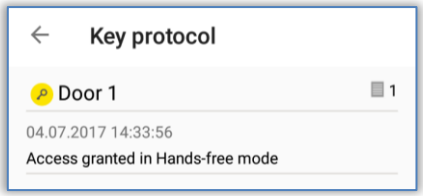


Figura 221: Datos de la lista de eventos de una autorización

6.4 Tareas de mantenimiento: Véase el capítulo 6.12

6.5 Apertura permanente

La apertura permanente requiere que, en la Administración online de AirKey, la apertura permanente manual esté activada para los componentes de cierre (véase Editar componente), para el componente tanto Bluetooth como NFC.

- En el menú de la app de AirKey, elija ***Apertura permanente***.
- De la lista mostrada, elija un componentes de cierre Bluetooth o sostenga el smartphone junto a un componentes de cierre NFC.
- El componentes de cierre señaliza la apertura a nivel óptico y acústico.
- Recibirá un mensaje de confirmación ❶.

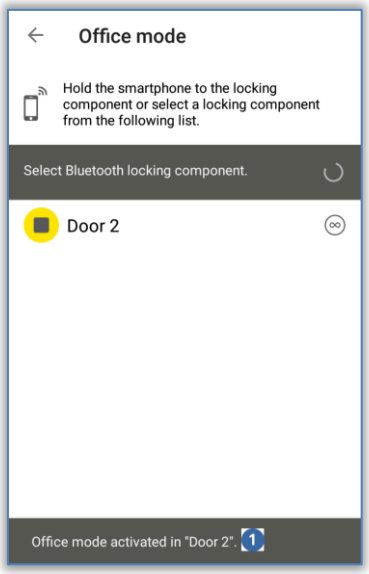


Figura 222: Mensaje de confirmación de apertura permanente

La activación de la apertura permanente en los componentes de cierre y los medios aumenta el consumo eléctrico de los componentes. Active la apertura permanente únicamente en los componentes de cierre y los medios que utilicen también esa función.

6.6 Introducir PIN

Puede guardar un PIN activo para un período de tiempo determinado en la app de AirKey utilizando la función ***Introducir PIN***.

> Abra el menú dentro de la app de AirKey y haga clic en ***Introducir PIN***.

> Introduzca el PIN correcto y haga clic en ***Aceptar***.

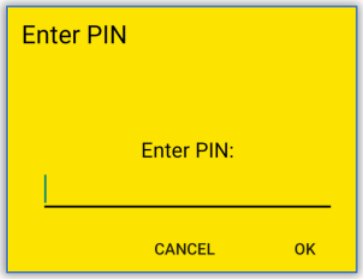


Figura 223: App de AirKey – Introducir PIN

El PIN se guarda hasta que se cierre la app de AirKey, quede de fondo o se active el bloqueo de pantalla. Así puede bloquear componentes de cierre sin tener que introducir el PIN otra vez.

El PIN también se guarda cuando se le pide para el primer desbloqueo de un componentes de cierre. La próxima vez que desbloquee un componentes de cierre (el mismo u otro), ya no se pedirá más el PIN. Así será hasta que se cierre la app de AirKey, quede de fondo o se active el bloqueo de pantalla.

6.7 Codificar medios

Esta función de la app de AirKey permite actualizar medios de acceso (excepto smartphones) a través de componentes de cierre compatibles con Bluetooth (cilindros, lectores murales).

> En el menú de AirKey, elija ***Codificar medios***.

> En la lista de los componentes de cierre con Bluetooth mostrados, seleccione aquel con el que desea actualizar el medio.

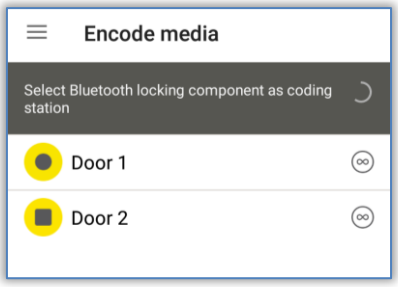


Figura 224: Codificar medios – Lista de selección de componentes de cierre con Bluetooth

> Sostenga el medio que desea actualizar junto al componentes de cierre.

Figura 225: Codificar medios

> Siga ahora las indicaciones de Añadir tarjetas, llaveros y llaves combi con el smartphone.

Para la función "Codificar medios", el proceso en el cilindro se debe iniciar a mano y no con un medio (tarjeta, llavero, pulseras o llave combi). Si no, se daría un proceso de apertura normal en vez del establecimiento de la comunicación con el smartphone.

En componentes de cierre con pilas, el proceso de actualización de medios consume energía y reduce la duración de las pilas. Si se deben actualizar muchos medios, se recomienda usar una estación codificadora de AirKey, un smartphone con función NFC o un lector mural.
El modo Hands-free del smartphone deberá desactivarse para poder llevar a cabo la función "Codificación de medios".

6.8 Protocolo de autorización

En el menú principal de la app de AirKey, elija el punto ***Protocolo de autorización*** y recibirá una lista de eventos sobre las modificaciones de las autorizaciones llevadas a cabo por el administrador del sistema de control de accesos para su smartphone.

Este registro de eventos tiene lugar siempre, con independencia de los diferentes ajustes de la Administración online de AirKey y la app de AirKey.

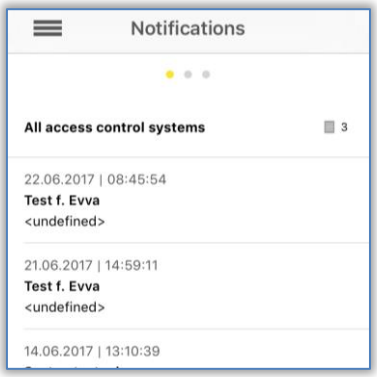


Figura 226: Protocolo de autorización

6.9 Ajustes de la app de AirKey

6.9.1 Ajustes de la app de AirKey en smartphones Android

En el menú principal ***Ajustes*** de la app de AirKey, verá información básica sobre su smartphone Android. Aquí ve, p. ej., si están activados el Bluetooth y NFC. Si hace clic en una de las dos entradas, accederá a los ajustes del smartphone. A continuación, puede decidir si se debe usar el Bluetooth para AirKey. Active la opción "Emplear Bluetooth" ❶.

En este caso, también se pueden usar los ajustes inferiores ("Ajustar el alcance del modo Hands-free", "Modo Hands-free" y "Desbloquear desde notificaciones"). En este caso, la página de inicio al abrir la app de AirKey es "Componentes de Bluetooth".

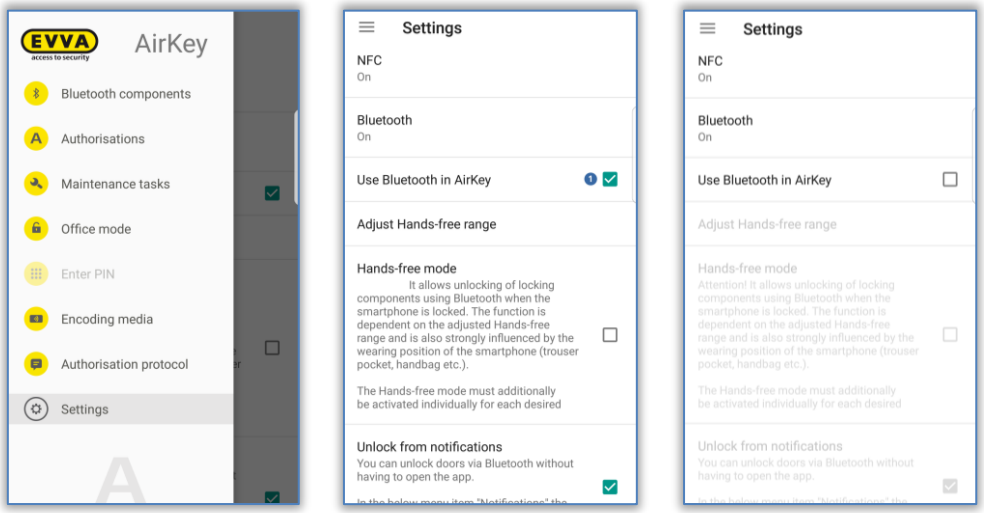


Figura 227: Smartphone Android con Bluetooth – Menú principal / Opción "Emplear Bluetooth" activada / Opción Bluetooth desactivada

Si desactiva la opción "Emplear Bluetooth", se desactivan automáticamente los tres ajustes posteriores mencionados, y todas las demás funciones dependientes del Bluetooth en el menú principal ("Componentes de Bluetooth", "Apertura permanente" y "Codificar medios") muestran el aviso "Bluetooth está desactivado". En esta situación, el smartphone se puede comunicar con los componentes de cierre solo por NFC.

Si el smartphone Android es más antiguo y dispone de función NFC pero no de Bluetooth, se inhabilitarán todas las funciones y ajustes dependientes del Bluetooth.

6.9.2 Ajustes de la app de AirKey en iPhones

En el menú principal ***Ajustes*** de la app de AirKey, verá información básica sobre su iPhone. Aquí ve, p. ej., si está activado el Bluetooth. En este caso, también se pueden usar los ajustes inferiores ("Ajustar el alcance del modo Hands-free", "Modo Hands-free" y "Desbloquear desde notificaciones").

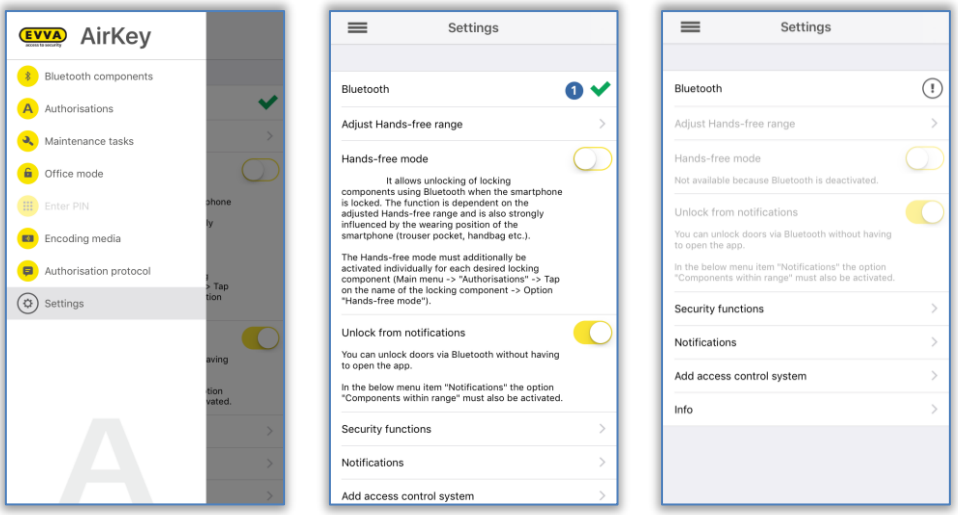


Figura 228: iPhone (solo con Bluetooth) – Menú principal / Ajustes sin funciones dependientes de NFC / Opción Bluetooth desactivado

La entrada "Bluetooth" en los ajustes de AirKey muestran solo si la función Bluetooth está activa o no. En todo caso, puede hacer clic en la entrada "Bluetooth" para acceder a la configuración del Bluetooth en los ajustes del iPhone.

¡Si desactiva el Bluetooth en los ajustes del iPhone, no podrá bloquear más NINGÚN componentes de cierre!

La función Bluetooth desactivada se muestra en los ajustes de AirKey, y los tres ajustes posteriores dependientes se desactivan automáticamente, así como todas las demás funciones dependientes del Bluetooth en el menú principal ("Componentes de Bluetooth", "Apertura permanente" y "Codificar medios").

6.9.3 Ajustar el alcance del modo Hands-free

Si se elige la función "Ajustar el alcance del modo Hands-free", se accede a un submenú. Aquí se escoge para qué tipo de componente se debe ajustar el alcance o si se desean restablecer los alcances (para todos los componentes).

Alcance para cilindros

- En los cilindros, la app de AirKey le muestra todos los cilindros Bluetooth activos y dentro del alcance después de que se hayan activado mediante contacto manual.
- Seleccione el cilindro correspondiente y aléjese de él cuanto quiera para que funcione la detección automática del smartphone.
- Presione ***Guardar.***

Alcance para lectores murales

- En el lector mural, la app de AirKey le muestra todos los lectores murales Bluetooth dentro del alcance.
- Seleccione el lector mural pertinente y aléjese de él lo que quiera para que funcione la detección automática del smartphone.
- Presione ***Guardar.***

Entonces se muestra la fuerza de la señal en la pantalla. Tenga en cuenta que puede variar en función de las condiciones ambientales, como radiocomunicaciones, etc., y del smartphone usado.

El alcance estándar es de unos 50-70 cm, aunque depende del fabricante y del equipo. Por motivos de seguridad, EVVA recomienda ajustar el alcance a unos 30 cm.

Restablecer todos los alcances de Bluetooth

Eligiendo ***Restablecer todos los alcances de Bluetooth*** se borrarán todos los alcances establecidos manualmente y se volverán a emplear los alcances estándar. Una comunicación de advertencia confirma que se han restablecido los alcances.

6.9.4 Modo Hands-free (manos libres)

Marque la casilla ***Modo Hands-free (manos libres)*** para activar la función. Encontrará toda la información al respecto en Hands-free (manos libres) de un vistazo.

6.9.5 Desbloquear desde notificaciones

Con esta función, se pueden desbloquear componentes de cierre con Bluetooth sin abrir la app de AirKey.

Marque la casilla ***Desbloquear desde notificaciones*** para activar la función.

En el caso de smartphones con Android, se iniciará un servicio al activarse esta función. Este servicio buscará también de forma permanente, incluso con la app de AirKey cerrada, componentes dentro del alcance Bluetooth; lo que supone un mayor consumo de batería del smartphone. El servicio finalizará en cuanto se vuelva a desactivar la función. Si se toca ligeramente en la notificación del servicio, se accede directamente a los ajustes de la app de AirKey.

En cuanto el smartphone está al alcance de un componente AirKey para el que dispone de una autorización de acceso, recibirá una notificación en la pantalla de bloqueo o de inicio del smartphone. Mediante esta notificación se puede entonces operar el componente.

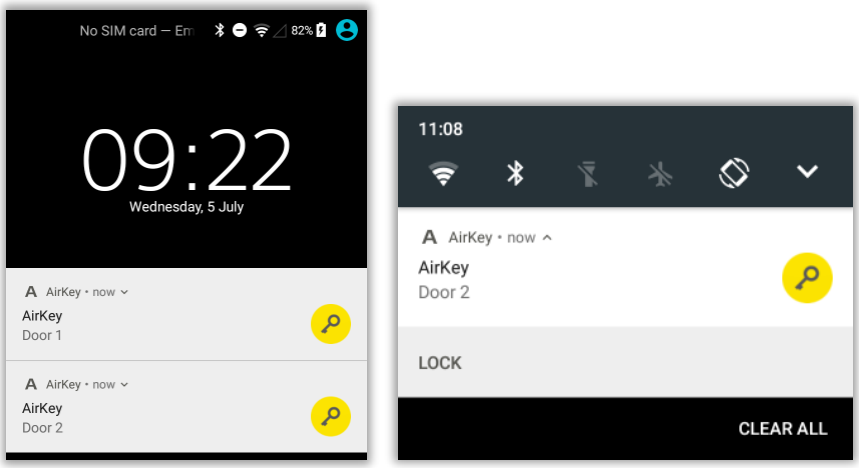


Figura 229: Desbloquear desde notificaciones – Pantalla de bloqueo

La notificación en la pantalla de inicio del smartphone se da en forma de **A** ❶ que aparece en la esquina superior izquierda. Al arrastrar abajo el borde superior de la pantalla, se muestran las notificaciones sobre los componentes de cierre que se pueden desbloquear.

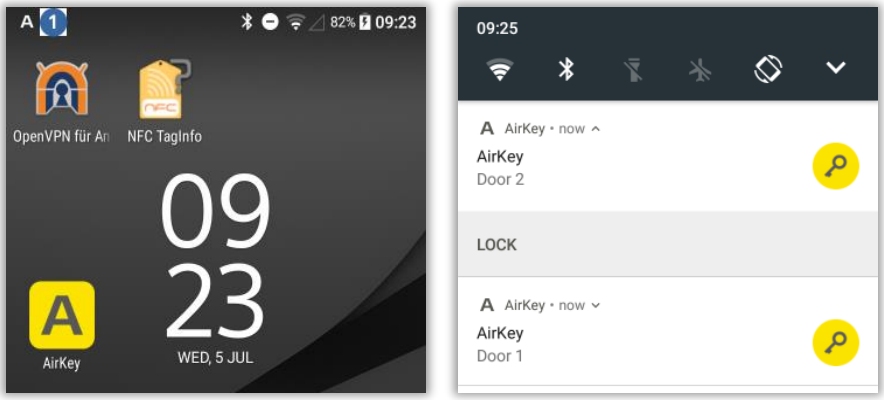


Figura 230: Desbloquear desde notificaciones

Dependiendo del modelo de smartphone, interactuará con la notificación simplemente tocándola ligeramente o manteniéndola pulsada, deslizando el dedo por ella, etc. A continuación, pulse en ***Desbloquear***.

En función del ajuste ***Acceso desde la pantalla de bloqueo*** en los ajustes de la Administración online de AirKey podrá operar los componentes directamente desde la pantalla de bloqueo o deberá salirse antes de dicha pantalla. Encontrará más información en Aspectos generales.

Desbloquear desde notificaciones únicamente es posible si están activadas las notificaciones para "Componentes dentro del alcance" en los ajustes de la app de AirKey. Encontrará la configuración de las notificaciones en el capítulo Notificaciones.

6.9.6 Funciones de seguridad

En el menú ***Funciones de seguridad***, encontrará tres niveles de seguridad:

Encriptación AirKey ❶
Se trata de un PIN adicional. El PIN está compuesto de 4 a 12 cifras e impide un uso indebido en caso de pérdida o robo del smartphone.

EVVA recomienda adjudicar un PIN. Utilice un PIN lo más largo posible, y manténgalo en secreto.

Bloqueo de pantalla ❷
La función de seguridad del sistema operativo garantiza que el smartphone esté protegido frente al desbloqueo de la pantalla por parte de terceros. Puede seleccionar esta función desde los ajustes de su smartphone Android.

EVVA recomienda activar el bloqueo de pantalla, y que solo lo conozca el propietario del smartphone.

Encriptación del teléfono ❸
La función de seguridad del sistema operativo Android garantiza que los datos del smartphone están protegidos frente a la lectura de terceros. Puede seleccionar esta función desde los ajustes de su smartphone Android.

EVVA recomienda que active el cifrado del teléfono. Tenga en cuenta las indicaciones del manual de instrucciones de su smartphone.

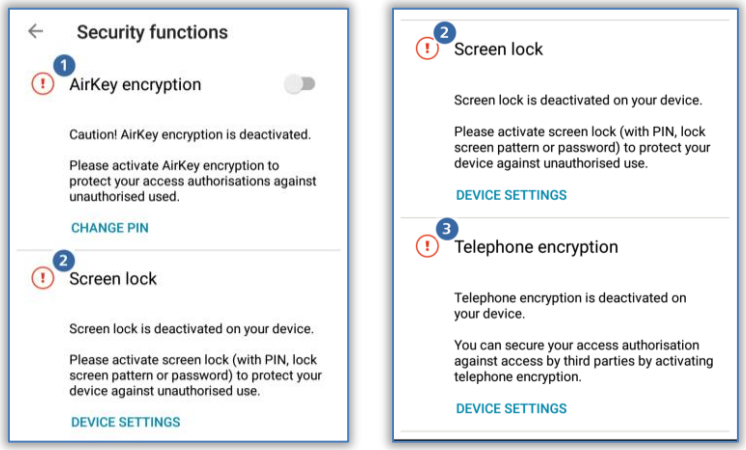


Figura 231: App de AirKey – Funciones de seguridad

6.9.6.1 Activar PIN

Para activar el PIN, siga los siguientes pasos:

> Abra el menú dentro de la app de AirKey y haga clic en ***Ajustes*** → ***Funciones de seguridad***.

> Active la opción "Encriptación AirKey".

> Asigne un PIN y haga clic en ***Confirmar***.

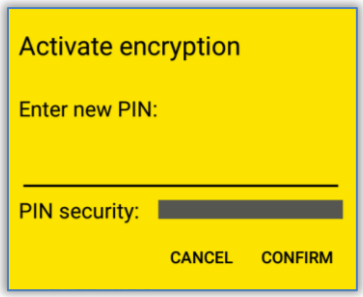


Figura 232: App de AirKey – Activar PIN

> Finalice el proceso introduciendo de nuevo el PIN y seleccione ***Confirmar***.

EVVA recomienda adjudicar un PIN. Utilice un PIN lo más largo posible, y manténgalo en secreto. Mientras introduce el PIN, se comprobará la calidad de la contraseña con la barra de semáforo (rojo / ámbar / verde).

Se le pedirá entonces el PIN durante el proceso de apertura de componentes de cierre. Dentro de la aplicación, no aparecerá ningún mensaje de confirmación acerca de la validez del PIN. El PIN se puede haber introducido y guardado antes (véase Introducir PIN).

6.9.6.2 Cambiar PIN

Para modificar un PIN a posteriori, siga los continuars pasos:

> Abra el menú dentro de la app de AirKey y haga clic en ***Ajustes*** → ***Funciones de seguridad***.

> Haga clic en ***Cambiar PIN***.

> Introduzca el PIN antiguo, seleccione uno nuevo, repítalo y haga clic en ***Confirmar***.

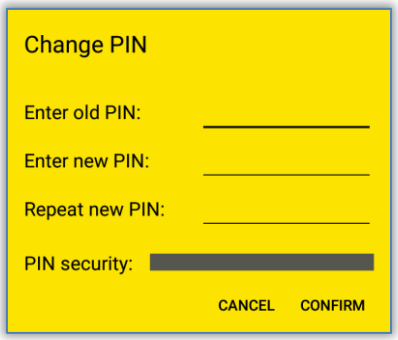


Figura 233: App de AirKey – Modificar PIN

Utilice un PIN lo más largo posible, y manténgalo en secreto. Mientras introduce el PIN, se comprobará la calidad de la contraseña con la barra de semáforo (rojo / ámbar / verde).

6.9.6.3 Desactivar PIN

Hay dos posibilidades para desactivar el PIN. Si conoce el PIN, se puede desactivar a través de las funciones de seguridad del smartphone. Si no se conoce el PIN, solo un administrador podrá restablecerlo mediante la Administración online de AirKey.

Si conoce el PIN, siga el continuar proceso:

- Abra el menú dentro de la app de AirKey y haga clic en ***Ajustes*** → ***Funciones de seguridad***.
- Desactive la opción "Encriptación AirKey".
- Introduzca el PIN existente y seleccione **Confirmar.**

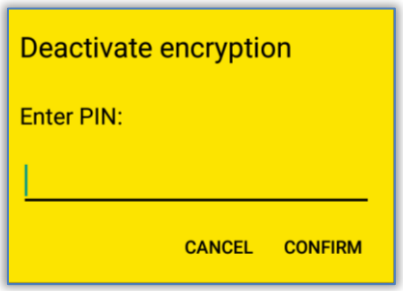


Figura 234: App de AirKey – Desactivar PIN

Si se desconoce el PIN, se puede desactivar a través de la Administración online de AirKey así:

- Inicie sesión como administrador en el sistema de control de accesos.
- En la página de inicio ***Home***, haga clic en la opción ***Smartphones***.
- También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
- En la lista general, haga clic en el smartphone para el que se debe desactivar el PIN.
- Seleccione la pestaña ***Detalles*** para editarlos.
- Haga clic en el vínculo ***Desactivar código PIN*** ❶ en el bloque "Ajustes".

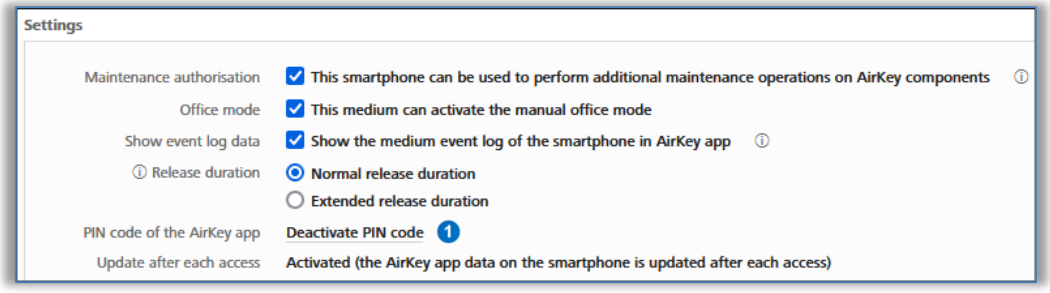


Figura 235: App de AirKey – Desactivar código PIN

- Confirme la pregunta de seguridad con el botón ***Desactivar código PIN***.

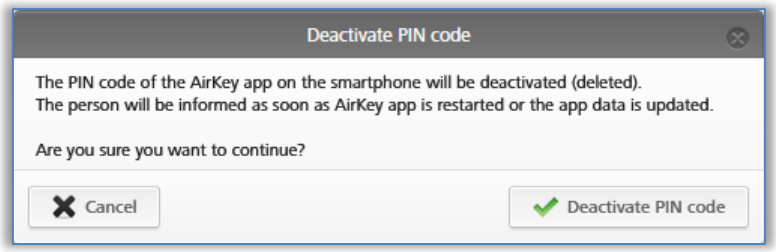


Figura 236: Administración online de AirKey – Desactivar código PIN

El PIN se puede activar de nuevo en cualquier momento.

6.9.7 Notificaciones

En la opción ***Ajustes*** → ***Notificaciones***, se pueden activar las notificaciones Push (avisos en la pantalla de bloqueo o inicio del smartphone) sobre componentes dentro del alcance, tareas de mantenimiento, notificaciones y sus cambios. Si el smartphone está registrado en varios sistemas AirKey y está equipado con la autorización de mantenimiento, estos sistemas AirKey también se mostrarán y se podrán seleccionar.

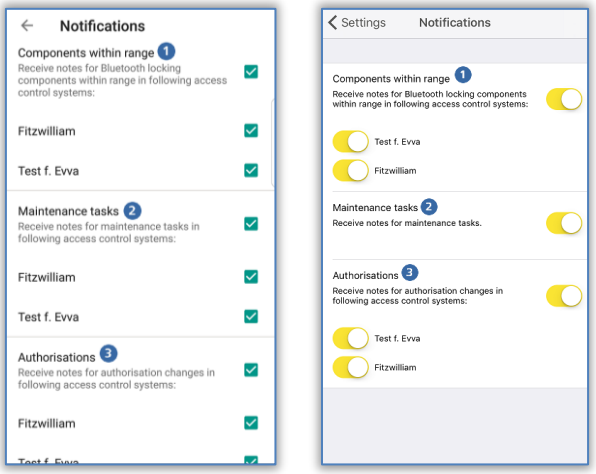


Figura 237: Notificaciones Push de la app de AirKey – Ajustes Android / iPhone

Notificaciones para *componentes dentro del alcance*

Si este ajuste está activado, recibirá las notificaciones Push correspondientes en la pantalla de bloqueo o inicio del smartphone siempre que este esté dentro del alcance de los componentes de cierre Bluetooth. A partir de estas notificaciones, se puede bloquear la puerta pertinente sin tener que abrir manualmente la app de AirKey (detalles en el capítulo Desbloquear desde notificaciones).

Este ajuste solo se muestra en smartphones con Bluetooth 4.0 (Bluetooth Low Energy).

Notificaciones para *tareas de mantenimiento* ❷

Este ajuste solo se muestra en smartphones con autorización de mantenimiento.

Si este ajuste está activo, en el menú principal de la app de AirKey también aparece la opción ***Tareas de mantenimiento***. En la página correspondiente, se relacionan los componentes de cierre y sus tareas de mantenimiento que se han creado en la Administración online de AirKey.

Si el smartphone está registrado en varios sistemas AirKey, solo aparecerán los componentes de cierre de los sistemas AirKey para los que el smartphone posee la autorización de mantenimiento. En cuanto se cree una nueva tarea de mantenimiento en la Administración online de AirKey, recibirá la notificación Push pertinente en el smartphone.

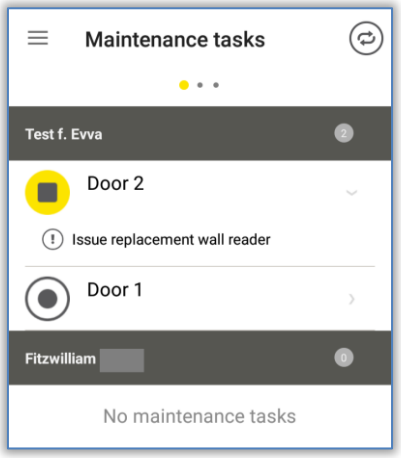


Figura 238: Tareas de mantenimiento

Notificaciones para *autorizaciónes* ❸

Este ajuste aparece siempre.

Si este ajuste está activo y se crea o modifica una autorización del smartphone en la Administración online de AirKey, recibirá un aviso ❶ durante unos 2 s en el borde inferior de la pantalla de la app de AirKey si está abierta.

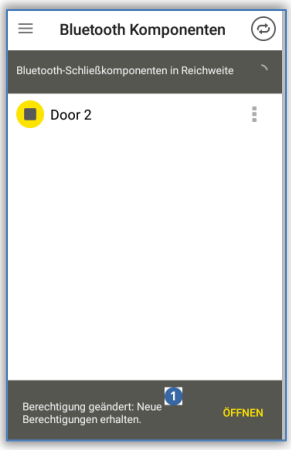


Figura 239: Notificación a través de una modificación de autorización

Si no está abierta la app de AirKey, recibirá la notificación Push correspondiente en la pantalla de bloqueo o inicio del smartphone.

Con independencia del ajuste sobre notificaciones para autorizaciones, recibirá una entrada permanente en la página de protocolo de autorización.

6.9.8 Añadir sistema de control de accesos

Los smartphones pueden estar registrados en más de un sistema de control de accesos. Si se debe añadir el smartphone a otro sistema de control de accesos, puede introducir el código de registro con la función ***Añadir sistema de control de accesos***. Encontrará más información al respecto en el capítulo Utilizar smartphone en varios sistemas.

Además, aquí también puede escanear un código QR para un reemplazo de smartphone. Encontrará más detalles sobre el reemplazo de smartphone en el capítulo Reemplazo de smartphone.

6.9.9 Reemplazo de smartphone

Existe la posibilidad de transferir las autorizaciones y los ajustes de AirKey de un smartphone a un nuevo smartphone.

Inicie este proceso con la orden ***Reemplazar smartphone***. Encontrará más información al respecto en el capítulo Iniciar reemplazo como propietario del smartphone.

6.9.10 Info

Dentro de la app de AirKey, puede consultar la versión instalada de la app de AirKey, los detalles de registro del smartphone, el ID del medio del smartphone y las condiciones generales de la licencia de EVVA.

> Inicie la app de AirKey.

> En el menú, elija ***Ajustes*** → ***Info***.

Figura 240: App de AirKey – Info

6.10 Actualizar smartphone

Para que los datos del sistema de control de accesos estén siempre actualizados en el smartphone, este se puede actualizar manualmente con la Administración online de AirKey en cualquier momento.

En un smartphone Android, deslice el dedo de arriba abajo en la pantalla hasta la página "Autorizaciónes" de la app de AirKey. Aparecerá el símbolo de actualización (círculo giratorio).

Con un iPhone, arrastre la página "Autorizaciónes" hasta el borde inferior. Aparecerá el símbolo de actualización (rayo giratorio).

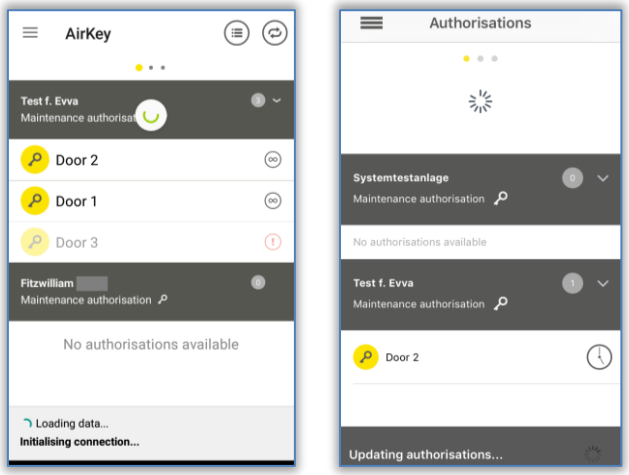


Figura 241: Actualizar smartphone Android o iPhone

AirKey utiliza notificaciones Push para actualizar el smartphone de manera automática cuando se dan cambios de datos. En cualquier caso, no se puede garantizar la entrega de las notificaciones Push. Controle si la entrega fue bien y actualice el smartphone de manera manual, de ser necesario.

El smartphone se actualizará de manera automática: en cuanto se inicie la app de AirKey o cada 12 horas si la app de AirKey ya está iniciada.

En la parte inferior de la app de AirKey, se activará la información de estado sobre la actualización en el momento que se produzca. En cuanto no se vea más esta información, la actualización habrá concluido.

Opcionalmente, puede realizarse la actualización también tras cada proceso de acceso. No obstante, para ello debe estar activada la función "Actualización después de cada acceso" en el sistema de control de accesos AirKey correspondiente. La activación y los detalles de esta función están descritos en el capítulo Aspectos generales.

6.11 Conectar con componente

Con su smartphone, podrá actualizar cualquier medio de acceso (salvo smartphones) y componentes de cierre, independientemente de su pertenencia al sistema de control de accesos.

> Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.

> Establezca la conexión a través de **Bluetooth** (en smartphones Android): En el componentes de cierre con el que desea conectarse, seleccione el menú contextual (⋮) y elija entonces ***Conectar*** ❷.

> Establezca la conexión a través de **Bluetooth** (en iPhones): En el componentes de cierre con el que desea conectarse, deslícese a la izquierda hasta la denominación del componente y elija entonces ***Conectar*** ❸.

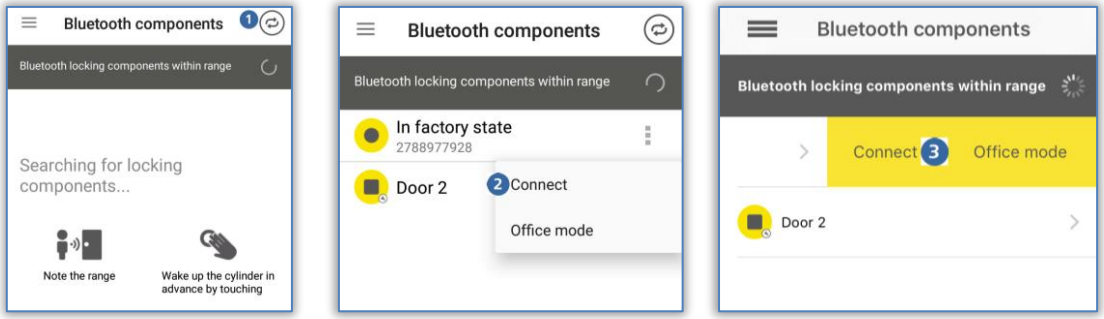


Figura 242: App de AirKey – Conectar con componente (Android NFC / Android Bluetooth / iPhone)

> Siga las indicaciones y sostenga el smartphone con NFC junto al medio o componente de cierre; o el smartphone Bluetooth al alcance componente de cierre.

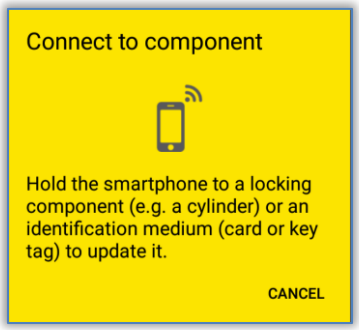


Figura 243: Actualizar datos

Los datos se están actualizando. No retire el smartphone del componente durante la transferencia. Cuando el proceso acabe, recibirá una notificación.

Desactive el modo Hands-free antes de conectarse con un componente con Bluetooth. De lo contrario podría interrumpirse la conexión.

Los componentes con Bluetooth también pueden actualizarse automáticamente tras cada proceso de apertura a través de Bluetooth. Encontrará más información sobre la función "Actualización después de cada desbloqueo" en Valores predeterminados (para todos los componentes de cierre recien añadidos).

Actualice sus componentes de AirKey con regularidad. Solo así su sistema de AirKey estará al día y será seguro. Puede encontrar más información acerca de la actualización de componentes de AirKey en Funcionamiento y mantenimiento del sistema de AirKey.

6.12 Autorización especial "autorización de mantenimiento"

Si se ha activado la autorización especial "autorización de mantenimiento" en la Administración online de AirKey de su smartphone, podrá ejecutar otras operaciones de mantenimiento en los componentes de AirKey. La autorización de mantenimiento le autoriza a desbloquear componentes de cierre en estado de fábrica, añadir o eliminar componentes de cierre y medios de acceso (salvo smartphones) al sistema de control de accesos, y actualizar el firmware de los componentes de cierre y la versión Keyring de los medios como tarjetas, llaveros y llaves combi.

Reconocerá la autorización de mantenimiento dentro de la app de AirKey en la página ***Autorizaciones*** como entrada "Autorización de mantenimiento" ❶ en la barra gris.

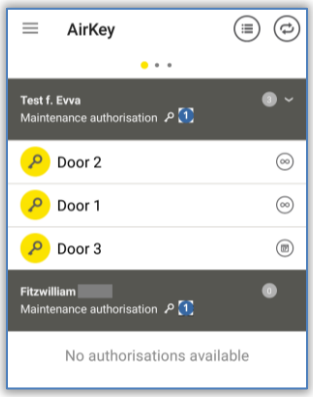


Figura 244: Autorización de mantenimiento

La autorización de mantenimiento se activa en los detalles del smartphone correspondiente, dentro de la Administración online de AirKey. Puede encontrar más detalles sobre la edición de un medio en Editar medio.

En el menú principal de la app de AirKey, también se activa la opción ***Tareas de mantenimiento*** ❶.

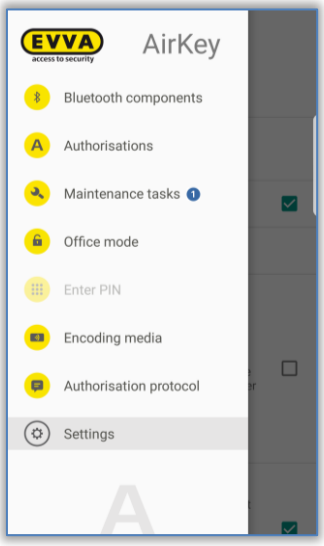


Figura 245: Opción "Tareas de mantenimiento" en el menú principal

> Haga clic ahí para obtener una lista de las tareas de mantenimiento para los componentes de cierre de su sistema de control de accesos. Si hace clic en el nombre de un componentes de cierre, se muestra la lista de las tareas de mantenimiento pendientes para este componentes de cierre.

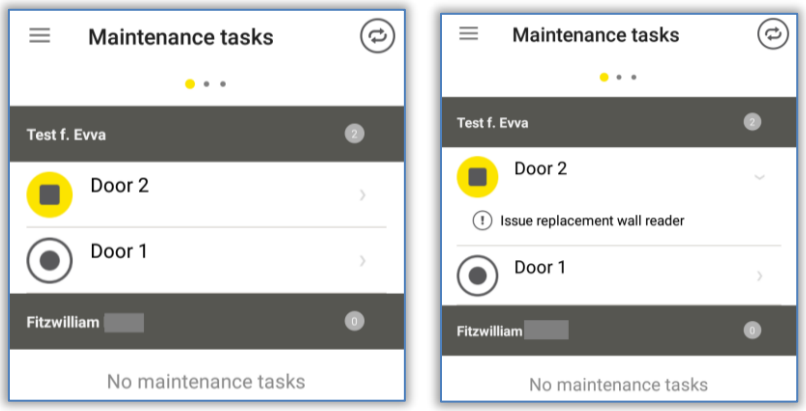


Figura 246: Tareas de mantenimiento

Como técnico de mantenimiento, revise periódicamente las tareas de mantenimiento para actualizar rápido los componentes de cierre que se deban actualizar.

Si entra dentro del alcance de un componentes de cierre Bluetooth (cilindro ◉ o lector mural ◙) con un smartphone con autorización de mantenimiento, el símbolo de este componentes de cierre se marca en amarillo (p. ej. ● para cilindro).

Si hace clic en el símbolo amarillo, se establecerá una conexión con el componentes de cierre y se ejecutará la actualización del componente. Entonces se mostrarán los detalles del componente. Se ve una actualización de firmware pendiente en los detalles del componente, que se puede iniciar desde aquí.

Al actualizar los componentes de cierre, como técnico de mantenimiento obtendrá también una vista general de los detalles del componentes de cierre para revisar directamente el estado de este y los eventos del cilindro en forma de lista de eventos.

> Actualice un componentes de cierre para obtener los detalles del mismo. Si está disponible, verá aquí también la ubicación del componentes de cierre como coordenadas GPS o la dirección guardada manualmente en la Administración online de AirKey. Si hace clic en el símbolo de ubicación amarillo, se le reenviará automáticamente al proveedor de mapas configurado de forma predeterminada en su smartphone.

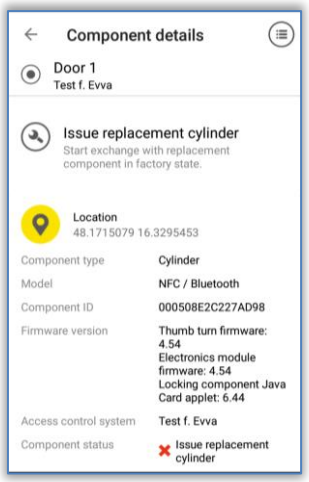


Figura 247: Visualización de los detalles del componentes de cierre

Actualice sus componentes de AirKey con regularidad. Solo así su sistema de AirKey estará al día y será seguro. Puede encontrar más información acerca de la actualización de componentes de AirKey en Funcionamiento y mantenimiento del sistema de AirKey.

El modo de mantenimiento solo es válido para los sistemas AirKey donde se activó. No obstante, se puede activar en varios sistemas AirKey a la vez.
El modo Hands-free del smartphone deberá desactivarse para poder llevar a cabo tareas de mantenimiento o actualizaciones de los componentes de cierre.

6.13 Añadir un componente de AirKey

Para poder añadir un componentes de cierre o medio de acceso (salvo smartphones) con su smartphone al sistema de control de accesos, deberá tener activado el modo de mantenimiento para el sistema de control de accesos, y el componente de AirKey deberá encontrarse en estado de fábrica.

6.13.1 Añadir medios: Véase el capítulo 4.12

6.13.2 Añadir componente: Véase el capítulo 4.11

6.14 Eliminar un componente de AirKey

Como requisito para la eliminación, se debe eliminar primero el componentes de cierre o el medio (salvo smartphones) en la Administración online de AirKey (véase Eliminar componentes de cierre y Eliminar medio), y el smartphone debe tener activado el modo de mantenimiento.

> Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.

> Establezca la conexión a través de **Bluetooth** (en smartphones Android): En el componentes de cierre con el que desea conectarse, seleccione el menú contextual (⋮) y elija entonces ***Conectar*** ❷.

> Establezca la conexión a través de **Bluetooth** (en iPhones): En el componentes de cierre con el que desea conectarse, deslícese a la izquierda hasta la denominación del componente y elija entonces ***Conectar*** ❸.

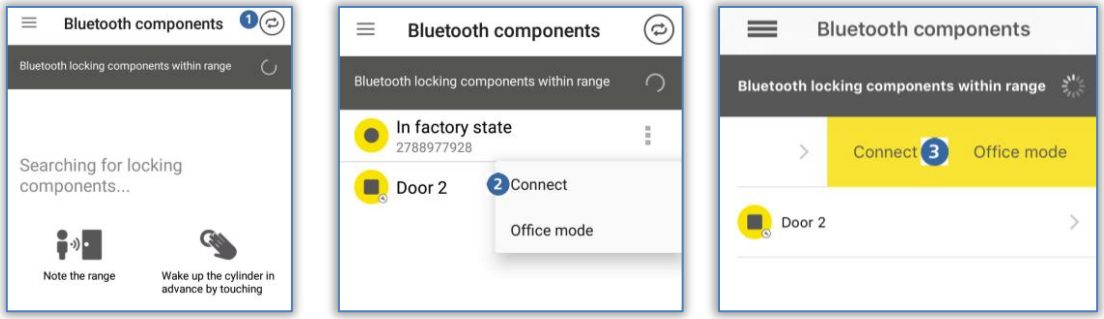


Figura 248: App de AirKey – Conectar con componente (Android NFC / Android Bluetooth / iPhone)

> Siga las indicaciones y sostenga el smartphone con NFC junto al medio o componente de cierre; o el smartphone Bluetooth al alcance componente de cierre.

Figura 249: App de AirKey – Conectar con componente

Sostenga el smartphone con NFC junto al componente de AirKey o medio que ya se ha eliminado de la Administración online de AirKey; o sostenga el smartphone Bluetooth dentro del alcance del componente que se debe eliminar o directamente junto al medio que se debe eliminar, y siga las indicaciones.

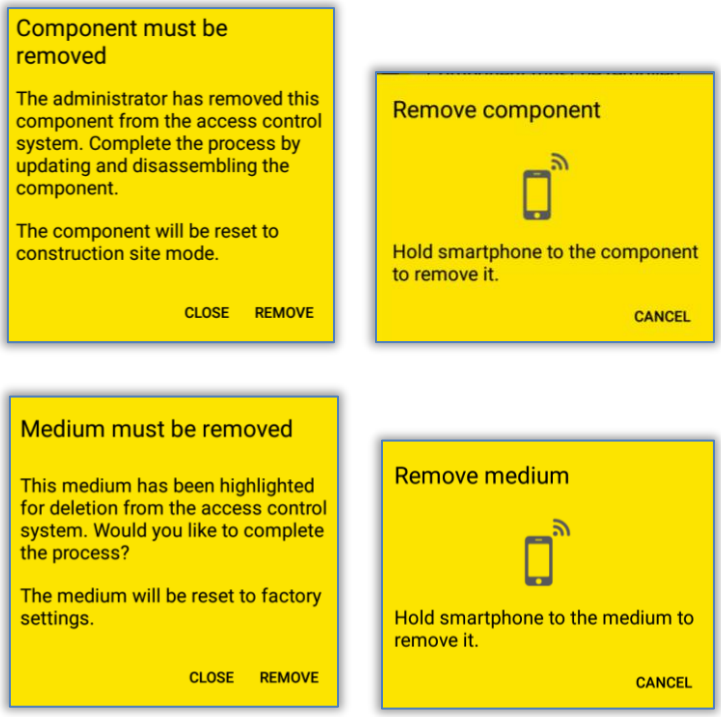


Figura 250: Eliminar componentes de cierre

Tras la actualización, los componentes de cierre y medios se encontrarán de nuevo en estado de fábrica.

Si se debe eliminar un medio de acceso con un iPhone del sistema de control de accesos, vaya a ***Codificar medios*** como al añadirlo.

> En la lista de los componentes de cierre con Bluetooth mostrados, seleccione aquel con el que desea actualizar el medio.

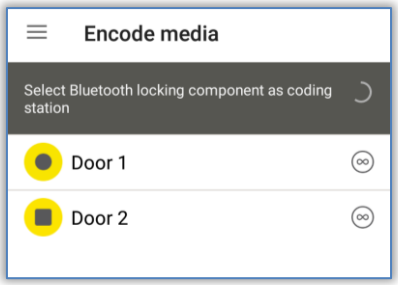


Figura 251: Codificar medio – Lista de selección de componentes de cierre con Bluetooth

> Sostenga el medio que desea actualizar junto al componentes AirKey.
> Recibirá un mensaje: el componentes AirKey está listo.

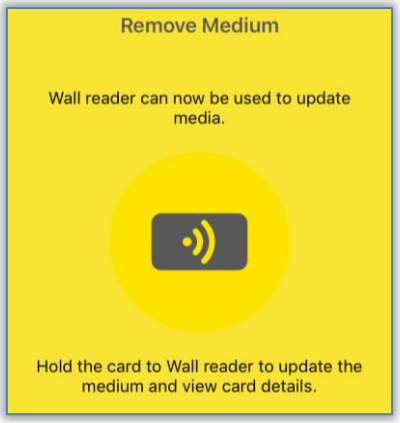


Figura 252: Eliminar medio con iPhone

> Sostenga el medio de acceso junto al componentes de cierre y haga clic en ***Eliminar***.

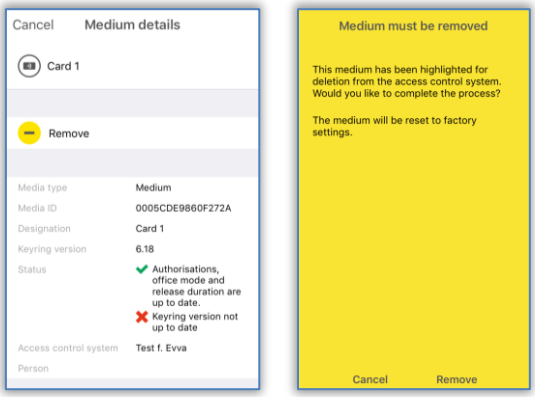


Figura 253: Eliminar medio

> Recibirá un mensaje de confirmación donde se le indicará que el medio de acceso se ha eliminado del sistema de control de accesos.

No retire el smartphone del componentes de cierre o medio durante este proceso.

El proceso para eliminar componentes de cierre y medios (salvo smartphones) es idéntico.

Los componentes NFC no se pueden eliminar del sistema de control de accesos con el iPhone. Para ello, necesita una estación codificadora opcional o un smartphone Android con NFC.

6.15 Datos de la lista de eventos en la app de AirKey

En smartphones, se puede activar la autorización para ver datos de la lista de eventos a través de la Administración online de AirKey. La visualización de datos de la lista de eventos es independiente del modo de mantenimiento y se puede activar de manera individual para cada persona.

La visualización de datos de la lista de eventos se puede activar y desactivar dentro de la Administración online de AirKey en los detalles del smartphone. Puede encontrar más detalles sobre la edición de un medio en Editar medio.

La lista de eventos se abre en la app así:

- Inicie la app de AirKey.
- En el menú principal, elija la opción ***Autorizaciones***.
- Arriba a la derecha, elija el símbolo de la lista de eventos ❶.

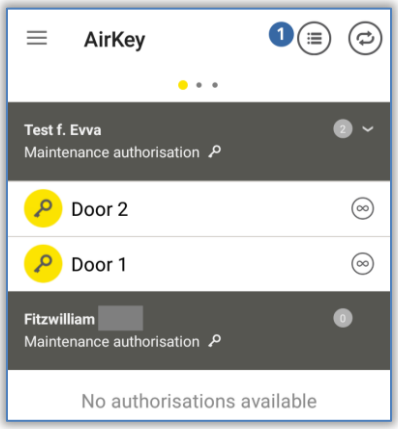


Figura 254: El símbolo de la lista de eventos

- Se muestra la lista de eventos.

Dentro de la lista de eventos de la app de AirKey, solo se ven las entradas de la lista de eventos de la persona a la que se asignó el smartphone.

6.16 Hands-free (manos libres) de un vistazo

Para componentes de cierre Bluetooth, existe el modo Hands-free. Se trata de una función que aporta comodidad, puesto que deja de ser necesario seleccionar el componente de cierre en la app. La función Hands-free no debe equipararse a la función "Bloqueo con Bluetooth", pero puede activarse para mayor comodidad.

El cilindro emite una señal de Bluetooth tras el contacto. En el caso del lector mural, el funcionamiento es automático, sin contacto. Si una app de AirKey en el ámbito de alcance del bloqueo recibe esta señal de Bluetooth, se inicia el proceso de bloqueo. El alcance del bloqueo puede ajustarse individualmente en la app para el cilindro y el lector mural.

- En la app AirKey, se debe activar el modo Hands-free en el menú principal ***Ajustes***.

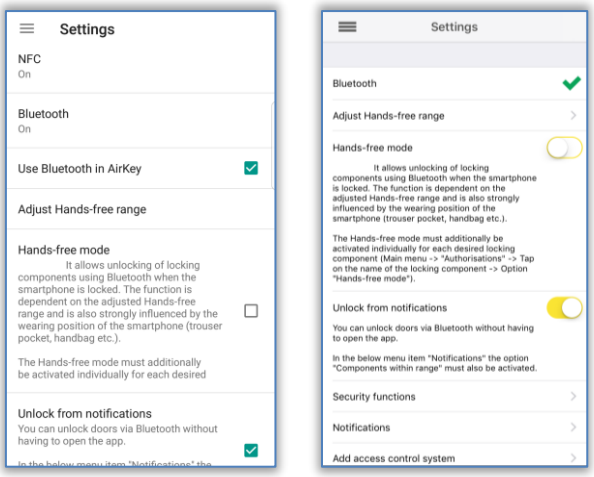


Figura 255: Ajustes AirKey-App

En el caso de smartphones con Android, se iniciará un servicio al activarse esta función. Este servicio buscará también de forma permanente, incluso con la app de AirKey cerrada, componentes dentro del alcance Bluetooth; lo que supone un mayor consumo de batería del smartphone. El servicio finalizará en cuanto se vuelva a desactivar la función. Si se toca ligeramente en la notificación del servicio, se accede directamente a los ajustes de la app de AirKey.

> Adicionalmente, se debe activar el modo Hands-free (manos libres) para cada componente o zona, en los detalles de autorización en el punto del menú ***Autorizaciones***. La primera vez que se activa el modo Hands-free aparece un cuadro de diálogo en el que puede activarse la función automáticamente para todos los componentes o, de forma individual, únicamente para algunos de ellos.

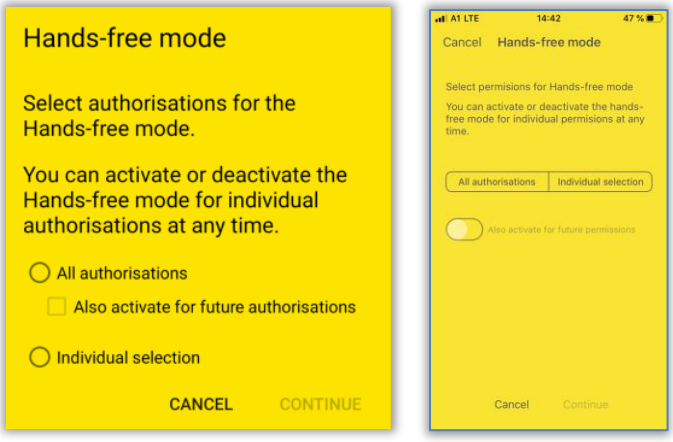


Figura 256: Autorizaciones para el modo Hands-free

Active ***También activar para futuras autorizaciones*** para activar automáticamente el modo Hands-free también para otras autorizaciones.

En función del ajuste ***Acceso desde la pantalla de bloqueo*** en los ajustes de la Administración online de AirKey, podrá operar el componente directa-

mente desde la pantalla de bloqueo o deberá salirse antes de dicha pantalla. Encontrará más información en Aspectos generales.

El modo Hands-free solo se puede utilizar para componentes AirKey en los que un administrador haya autorizado el modo Hands-free. Encontrará información más detallada en el capítulo Editar componente.

Ajustar el alcance del modo Hands-free: Véase el capítulo 6.9.3

¿Qué debe tenerse en cuenta al utilizar el modo Hands-free?

El funcionamiento en el caso de pantalla de smartphone bloqueada dependerá

- del ajuste "Acceso desde la pantalla de bloqueo" en los ajustes de la Administración online de AirKey;
- del fabricante, del sistema operativo, de la antigüedad del modelo, del número de app instaladas, de las optimizaciones de app (función de ahorro de energía) del smartphone;
- de factores perturbadores como el tipo de edificación (p. ej. la construcción con hormigón armado) y el entorno de radio;
- del lugar de conservación o el lugar al que se traslade el smartphone, así como del alcance de bloqueo ajustado para la función de Hands-free;
- de si el smartphone se acaba de conectar a WLAN.

Debido a estos factores, la función de Hands-free funcionará más lentamente o no funcionará en absoluto en algún momento. Para acelerar el proceso de bloqueo de Hands-free, debe desbloquearse el smartphone según el sistema operativo (p. ej. iOS) e iniciar la app de AirKey. En este caso, se evita seleccionar los componentes a desbloquear dentro de la app.

Para evitar bloqueos erróneos, deberá tenerse en cuenta lo siguiente:

- En el caso de lectores murales, tras cualquier proceso de apertura de los mismos debe haber un tiempo de descanso de 2 minutos. Eso significa que un lector mural solo puede volver a activarse en modo Hands-free si el smartphone en cuestión permanece durante 2 minutos fuera del alcance de recepción del lector mural. Esto evita activaciones no deseadas al abandonar el rango de alcance de operación.
- Idealmente solo se encontrará un componente de cierre en el rango de alcance de bloqueo de un smartphone.
- Para poder realizar funciones como, p. ej., "Codificación de medios" o "Actualizaciones de componentes", deberá desactivarse el modo Hands-free en la app.

7 Utilización de componentes de cierre

7.1 Acceso con el smartphone

Para obtener acceso con un componentes de cierre, se deben cumplir las continuars condiciones:

- El NFC o Bluetooth está activado en el smartphone.
- La app de AirKey está instalada y registrada.
- Se ha otorgado una autorización válida para el smartphone (encontrará más información en Registrar smartphone y Otorgar autorizaciones).
- Sostenga el smartphone junto al componentes de cierre durante los procesos de apertura mediante NFC. La posición con la mejor capacidad de lectura dependerá del modelo del smartphone. El alcance de la lectura también depende del tipo de smartphone y va desde estar en contacto hasta unos milímetros de distancia. En procesos de apertura por Bluetooth, el alcance de lectura depende, por un lado, del tipo de smartphone y, por otro, de los ajustes personales de la app de AirKey en el smartphone para el modo de Hands-free. Asciende a algunos metros.
- Si se requiere la entrada de un PIN, introdúzcalo antes de proceder a la apertura con el smartphone a través de NFC o Bluetooth. (Tiene más información sobre el PIN en Funciones de seguridad).
- Preste atención a la señalización óptica del componentes de cierre. No retire el smartphone del componentes de cierre cuando use el NFC, o permanezca dentro del alcance de recepción en el caso de Bluetooth, hasta que el componentes de cierre se señalice en verde. (La señalización azul se refiere solo a la comunicación entre el smartphone y el componentes de cierre.)

Con los modelos de iPhone XR, XS, XS Max y los más recientes puede operar también componentes con Bluetooth mediante etiquetas NFC. Para ello, sostenga el smartphone junto al componente y toque ligeramente la comunicación de advertencia reconocible gracias a una etiqueta NFC. A continuación se abrirá la app de AirKey y se realizará un proceso de apertura mediante Bluetooth.

Figura 257: Etiqueta NFC de iOS

Compruebe su autorización o el PIN siempre que el componentes de cierre muestre una señal roja.

No se pueden bloquear componentes de cierre a través de NFC con el bloqueo de pantalla activo o durante una llamada. No es necesario iniciar la app de AirKey o ejecutarla en segundo plano para poder bloquear los componentes de cierre. En cambio, se pueden bloquear componentes de cierre mediante Bluetooth con el bloqueo de pantalla activo a través de notificaciones Push. Únicamente hay que activar la opción "Desbloquear desde notificaciones" en los ajustes de la app de AirKey y permitir "Acceso desde la pantalla de bloqueo" en los ajustes de la Administración online de AirKey.

7.2 Acceso con medios como tarjetas, llaveros, pulsares o llaves combi

Para obtener acceso a un componentes de cierre, se debe añadir el medio al sistema de control de accesos y tener asignada una autorización válida (encontrará más información en Añadir tarjetas, llaveros y llaves combi con el smartphone y Otorgar autorizaciones).

> Mantenga el medio junto al componentes de cierre. El alcance de la lectura depende del tipo de medio y es generalmente de unos milímetros.

> Preste atención a la señalización óptica del componentes de cierre. No retire el medio antes de que el componentes de cierre se señalice en verde. (La señalización azul se refiere solo a la comunicación entre el medio y el componentes de cierre.)

>

>

Compruebe su autorización siempre que el componente muestre una señal roja.

>

> El componentes de cierre se desbloquea durante el tiempo establecido y se le permite así el acceso.

Los medios como tarjetas, llaveros, pulsares o llaves combi pueden verse limitados o no funcionar cerca de otros medios u objetos metálicos. Esto podría afectar, por ejemplo, a medios que se encuentren en el monedero o en un llavero.

La identificación con la llave combi se debe realizar por el lado donde se vea el símbolo RFID.

8 Funcionamiento y mantenimiento del sistema de AirKey

8.1 Actualizar componentes de cierre

Podrá actualizar cualquier componentes de cierre independientemente del sistema de control de accesos al que pertenezca, para así intercambiar datos entre la Administración online de AirKey y los componentes de cierre.

La actualización se puede realizar mediante el smartphone u opcionalmente con la estación codificadora. La actualización con el smartphone solo requiere la instalación de la app de AirKey y el registro dentro de cualquier sistema de control de accesos.

Durante la actualización de los componentes de cierre, se realizarán las continuars acciones:

- Se restablecerá la hora.
- Se leerán las entradas de la lista de eventos y el estado de las pilas.
- Se actualizarán las tareas de mantenimiento (lista negra, activaciones en otros sistemas AirKey, etc.)
- Se leerán los detalles del componente.

Siga las instrucciones para actualizar un componentes de cierre con el smartphone:

> Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.

> Establezca la conexión a través de **Bluetooth** (en smartphones Android): En el componentes de cierre con el que desea conectarse, seleccione el menú contextual (⋮) y elija entonces ***Conectar*** ❷.

> Establezca la conexión a través de **Bluetooth** (en iPhones): En el componentes de cierre con el que desea conectarse, deslícese a la izquierda hasta la denominación del componente y elija entonces ***Conectar*** ❸.

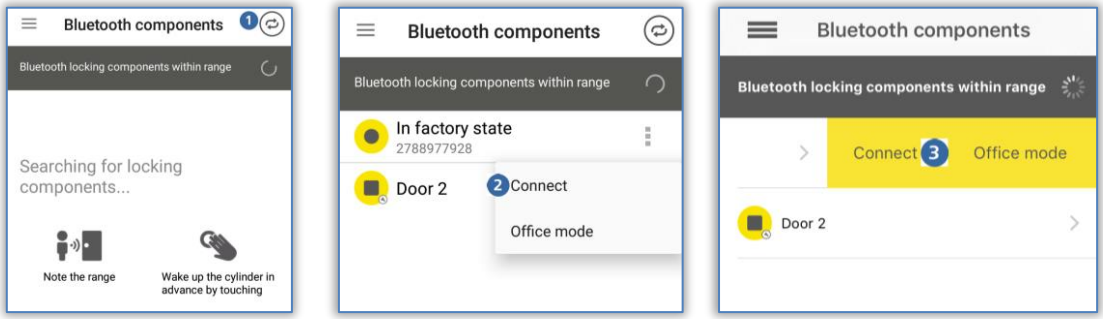


Figura 258: App de AirKey – Conectar con componente (Android NFC / Android Bluetooth / iPhone)

> Siga las indicaciones.

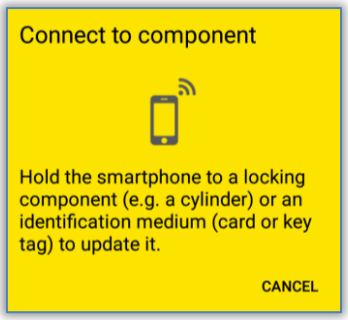


Figura 259: Actualizar datos

Los datos se están actualizando. Durante la transferencia, el smartphone con NFC no se puede alejar del componente que se va a sincronizar; y el teléfono con Bluetooth no puede salir del alcance del componentes de cierre. Cuando el proceso acabe, recibirá una notificación.

Dependiendo de si el modo de mantenimiento está activado en el smartphone y de si el componentes de cierre se encuentra en el sistema de control de accesos propio o en otro diferente, la información que muestra el mensaje de actualización puede variar.

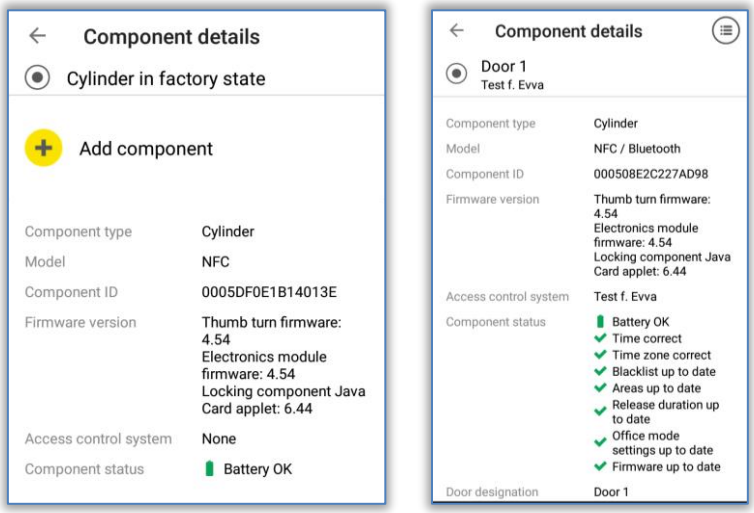


Figura 260: Mensajes de actualización

Desactive el modo Hands-free antes de conectarse con un componente con Bluetooth. De lo contrario podría interrumpirse la conexión.

Los componentes con Bluetooth también pueden actualizarse automáticamente tras cada proceso de apertura a través de Bluetooth. Encontrará más información sobre la función "Actualización después de cada desbloqueo" en Valores predeterminados (para todos los componentes de cierre recien añadidos).

Option **Actualizar componentes de cierre con estación codificadora**

Para actualizar el componentes de cierre con la estación codificadora, proceda de la continuar manera:

> Inicie sesión en su sistema de control de accesos y asegúrese de que la estación codificadora esté conectada y seleccionada en la Administración online de AirKey.

> Presente el componentes de cierre sobre la estación codificadora.

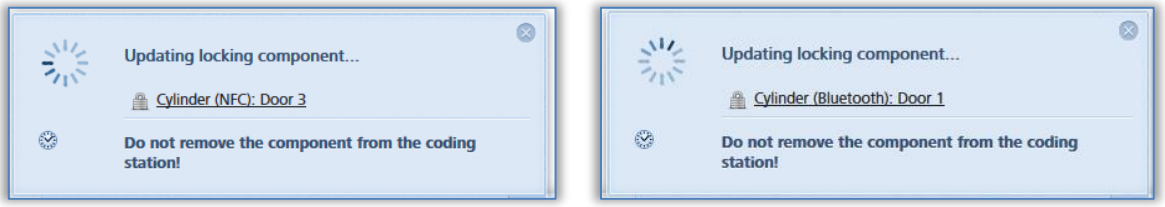


Figura 261: Actualizar componentes de cierre con estación codificadora

> Aleje el componentes de cierre de la estación codificadora cuando se haya completado la actualización y se muestre el mensaje de confirmación.

Dependiendo de si el componentes de cierre se encuentra en el sistema de control de accesos propio o en otro diferente, la información que muestra el mensaje de confirmación puede variar.

Figura 262: Componentes de cierre actualizado con estación codificadora

Actualice sus componentes de cierre con regularidad. Solo así su sistema de control de accesos estará al día y será seguro.

8.2 Actualizar smartphone: Véase el capítulo 6.10

8.3 Actualizar medios

Podrá actualizar cualquier medio de AirKey, independientemente del sistema de control de accesos al que pertenezca. La actualización se puede realizar mediante el smartphone Android o la estación codificadora opcional. La actualización con el smartphone solo requiere la instalación de la app de AirKey y el registro dentro de un sistema de control de accesos.

Con un iPhone, los medios se actualizan igual a como se explica en Codificar medios; para ello, utilice un componentes de cierre como estación codificadora.

> En un smartphone Android, haga clic en el símbolo ***Conectar con componente*** arriba a la derecha en la app de AirKey.

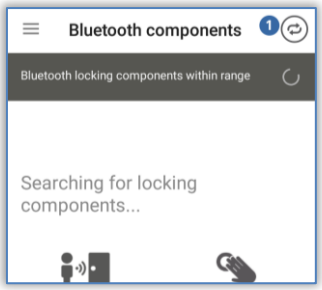


Figura 263: Símbolo "Conectar con componente" (solo con smartphones Android)

> Siga las instrucciones y sostenga el smartphone junto al medio.

Figura 264: Actualizar datos

Los datos se están actualizando. No retire el smartphone del objeto que se debe sincronizar durante la transferencia. Cuando el proceso acabe, recibirá una notificación.

Para actualizar la llave combi con smartphones, esta se debe sostener con el lado que tenga el símbolo RFID directamente donde esté la antena NFC del smartphone.

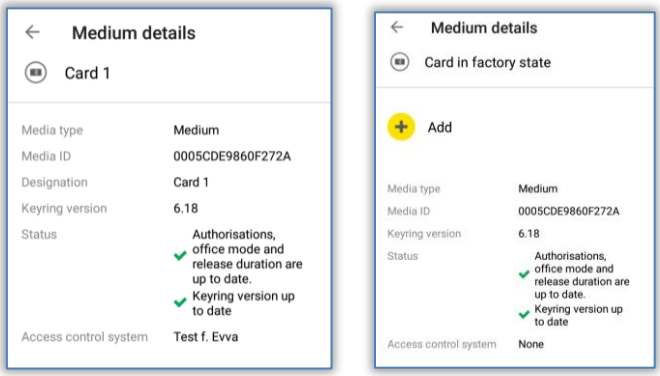


Figura 265: La app de AirKey actualiza un medio

Option **Actualizar medio con estación codificadora**

Para actualizar medios como tarjetas, llaveros, pulsares o llaves combi con la estación codificadora, proceda de la continuar manera:

> Inicie sesión en su sistema de control de accesos y asegúrese de que la estación codificadora esté conectada y seleccionada en la Administración online de AirKey.

> Sostenga el medio sobre la estación codificadora.

Figura 266: Actualizar medio con estación codificadora

> Aleje el medio de la estación codificadora cuando se haya completado la actualización y se muestre el mensaje de confirmación.

Dependiendo de si el medio se encuentra en el sistema de control de accesos propio o en otro diferente, la información que muestra el mensaje de confirmación puede variar.

Figura 267: Medio propio o ajeno actualizado con estación codificadora

Actualice sus medios de AirKey con regularidad. Solo así su sistema de control de accesos estará al día y será seguro.

Solo con la actualización periódica de los medios, se puede garantizar que todas las entradas de la lista de eventos de los medios se hayan transferido a la Administración online de AirKey.

Para actualizar la llave combi con una estación codificadora, deberá colocar la llave combi sobre la estación codificadora por el lado en el que se encuentre el símbolo RFID. Actualizar una llave combi no es posible en toda el área de lectura de la estación codificadora; con el modelo actual (HID Omnikey 5421), la llave combi solo se reconoce por los tercios superior e inferior de la estación codificadora.

8.4 Actualizar firmware de componentes de cierre

Cuando un nuevo firmware está disponible para los componentes de cierre, se mostrará esta información en los detalles del componentes de cierre, en las tareas de mantenimiento y al actualizar el componentes de cierre.

Compruebe el estado de las pilas del componentes de cierre (cilindro) antes de actualizar el firmware. Si se muestra el aviso "pila vacía", deberán cambiarse primero las pilas para poder garantizar una actualización sin fallos.

Se mostrará la versión actual del firmware del componentes de cierre en los detalles.

El firmware de los componentes de cierre se puede actualizar mediante un smartphone o una estación codificadora opcional.

Para actualizar el firmware con el smartphone, la autorización especial "autorización de mantenimiento" del smartphone debe estar activada. Realice las actualizaciones de firmware con el smartphone de la continuar manera:

- Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.
- Establezca la conexión a través de **Bluetooth** (en smartphones Android): En el componentes de cierre con el que desea conectarse, seleccione el menú contextual (⋮) y elija entonces ***Conectar*** ❷.
- Establezca la conexión a través de **Bluetooth** (en iPhones): En el componentes de cierre con el que desea conectarse, deslícese a la izquierda hasta la denominación del componente y elija entonces ***Conectar*** ❸.

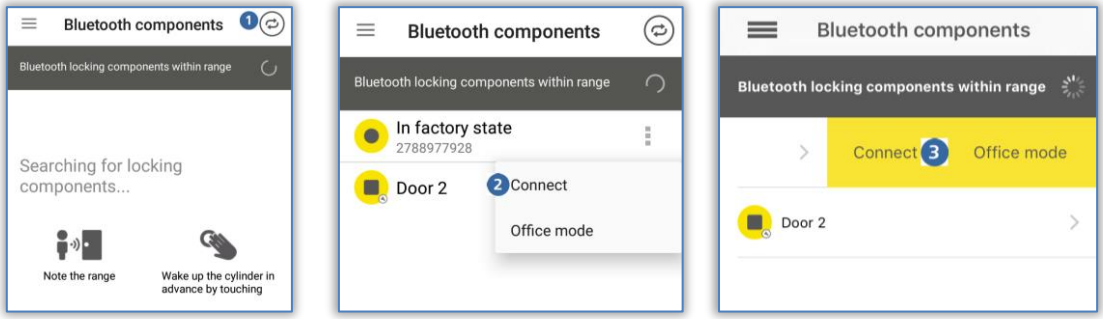


Figura 268: App de AirKey – Conectar con componente (Android NFC / Android Bluetooth / iPhone)

- Siga las indicaciones.

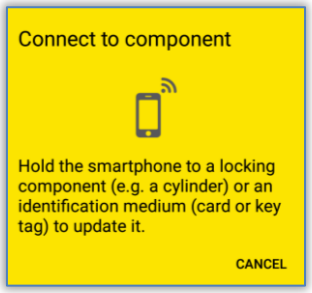


Figura 269: Conectar con componente – Actualización de firmware

Los datos se están actualizando. Durante la transferencia, el smartphone con NFC no se puede alejar del componente que se va a sincronizar; y el teléfono con Bluetooth no puede salir del alcance del componentes de cierre. Cuando el proceso acabe, recibirá una notificación.

- El componentes de cierre se actualizará y se mostrarán los detalles del componente. En los detalles del componente figura si el firmware del componente no está actualizado.

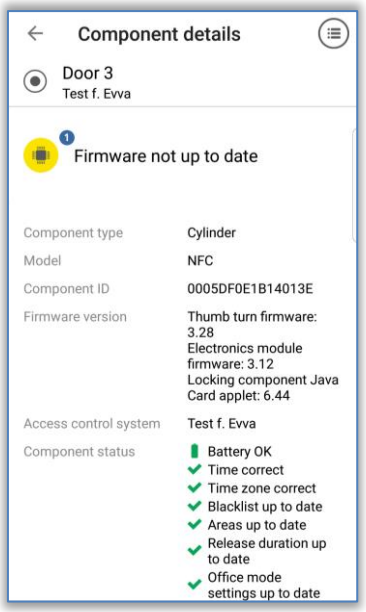


Figura 270: App de AirKey – Detalles del componente

> En esta pantalla, haga clic en la opción ***Actualizar firmware*** ❶.

> Sostenga el smartphone NFC junto al componentes de cierre, y permanezca con el smartphone Bluetooth dentro del alcance.

Figura 271: App de AirKey – Actualizar firmware

La actualización del firmware puede tardar varios minutos según la conexión a Internet. Durante este tiempo, sostenga el smartphone NFC junto al componentes de cierre, o dentro del alcance del componentes de cierre en el caso de un smartphone Bluetooth.

Durante la transferencia, no se debe retirar el smartphone del componente que se va a actualizar. El primer paso de la actualización finaliza con un mensaje de confirmación.

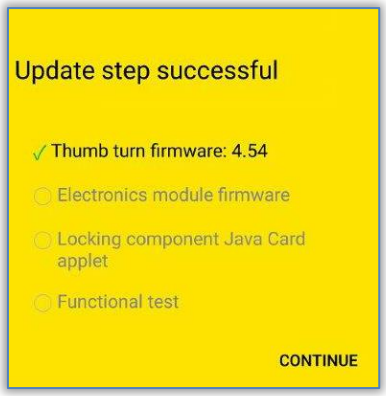


Figura 272: App de AirKey – Paso de actualización finalizado

> Retire el smartphone del componentes de cierre hasta que este parpadee y produzca una señal acústica.
> Sostenga el smartphone NFC junto al componentes de cierre, o mantenga el smartphone Bluetooth dentro del alcance del componentes de cierre, y siga las indicaciones.

Cuando la actualización del firmware finalice con éxito, aparecerá un mensaje de confirmación.

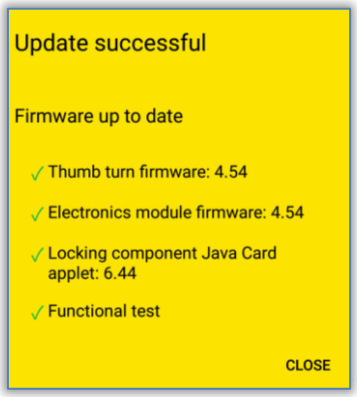


Figura 273: App de AirKey – Actualización correcta

> Acepte el mensaje de confirmación con ***Cerrar*** para finalizar la actualización del firmware.

El estado del componentes de cierre se ajustará en todo el sistema. La tarea de mantenimiento ya no se mostrará más y la versión correcta del firmware aparecerá en los detalles del componentes de cierre.

Option

Actualizar firmware con estación codificadora:

> Presente el componentes de cierre sobre la estación codificadora. Cuando la estación codificadora inicie una comunicación con el componentes de cierre, comenzará automáticamente la actualización.

Recibirá un mensaje de confirmación cuando la actualización termine.

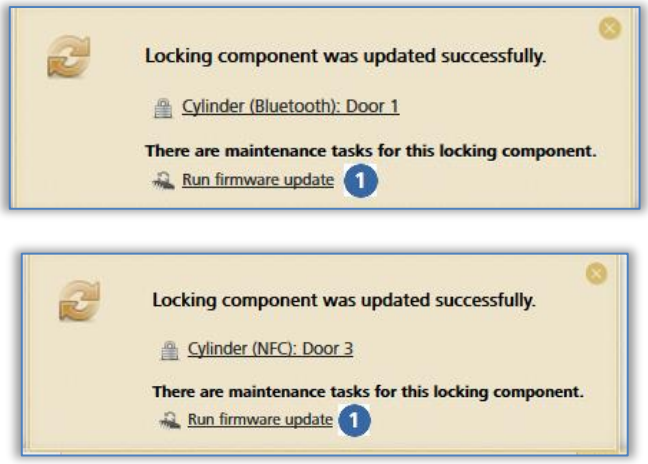


Figura 274: Estación codificadora – Mensaje de confirmación en la actualización de un componentes de cierre

Cuando haya una actualización de firmware para el componentes de cierre, aparecerá un vínculo ❶.

> Haga clic en ***Ejecutar actualización de firmware*** para iniciarla.

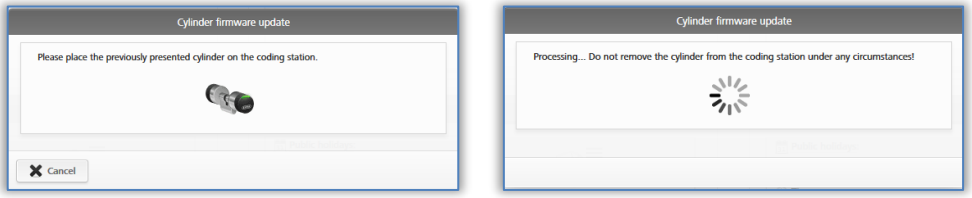


Figura 275: Estación codificadora – Actualización de firmware de cilindro

La actualización del firmware puede durar unos minutos según la conexión a Internet. Durante este proceso, no retire el componentes de cierre de la estación codificadora.

El primer paso de la actualización del firmware finalizará con un mensaje de confirmación.

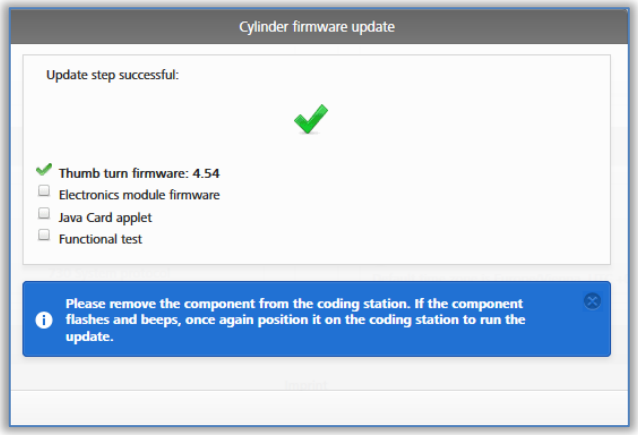


Figura 276: Estación codificadora – Paso de actualización finalizado

> Retire el componentes de cierre de la estación codificadora hasta que este se reinicie con una señal acústica y óptica.

> Presente otra vez el componentes de cierre sobre la estación codificadora para concluir el proceso.

Una vez finalizada la actualización, recibirá un mensaje de confirmación.

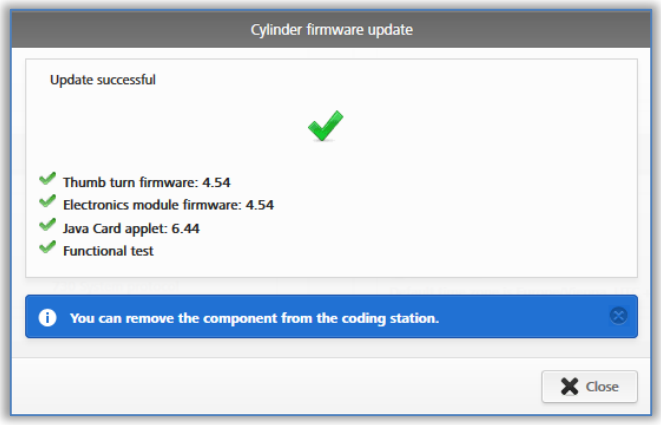


Figura 277: Estación codificadora – Actualización de firmware finalizada

El componentes de cierre se actualizará de nuevo tras cerrar el mensaje de confirmación.

Figura 278: Estación codificadora – Componentes de cierre actualizado

> Tras la actualización, retire el componentes de cierre de la estación codificadora.

El estado del componentes de cierre se ajustará en todo el sistema. La tarea de mantenimiento ya no se mostrará más y la versión correcta del firmware aparecerá en los detalles del componentes de cierre.

Para la actualización del firmware, abra la puerta y fíjela de forma que no pueda cerrarse por descuido. A continuación, compruebe el buen funcionamiento del componentes de cierre antes de volver a cerrar la puerta.

Durante la actualización del firmware de los componentes de cierre, deberá disponerse de una conexión a Internet estable, y no se deberá interrumpir la conexión de datos durante la actualización del firmware. Para ello, existen diversos ajustes según el smartphone y el sistema operativo (por ejemplo, cambio automático entre datos móviles y WiFi).

EVVA recomienda mantener el firmware de los componentes de cierre siempre actualizado.

8.5 Actualizar versión de Keyring de medios

En AirKey, "Keyring" es el nombre de un programa de software que administra todos los datos relevantes de AirKey almacenados en los medios de acceso pasivos como tarjetas, llaveros, llaves combi y pulseras. Cuando una nueva versión de Keyring está disponible para los medios, se mostrará en los detalles de los medios, en la página de inicio ***Home*** y al actualizar los medios.

Se mostrará la versión del Keyring actual del medio en los detalles de este.

El Keyring de los medios se puede actualizar mediante un smartphone o una estación codificadora opcional. Para actualizar el Keyring con el smartphone, la autorización especial "autorización de mantenimiento" del smartphone debe estar activada. Realice las actualizaciones del Keyring con el smartphone de la continuar manera:

- Establezca la conexión a través de **NFC** (en smartphones Android): Seleccione el símbolo ***Conectar con componente*** ❶.
- Conexión con **Bluetooth** (en smartphones Android y iPhones): En el menú principal de la app de AirKey, elija la opción ***Codificar medios***; véase también Codificar medios.

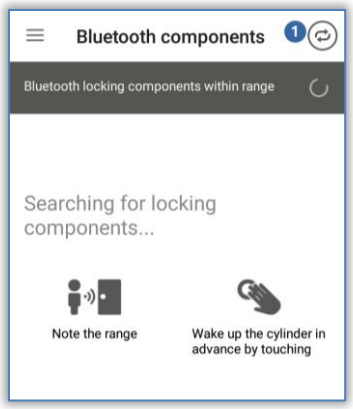


Figura 279: App de AirKey – Conectar con componente

- Sostenga el smartphone NFC junto al medio.
- El medio se actualiza. Se mostrará que existe una nueva versión del Keyring.

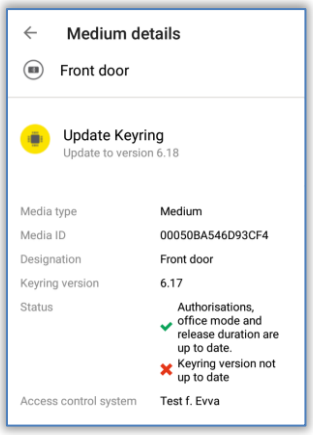


Figura 280: App de AirKey – Detalles del medio

> Elija la opción ***Actualización de Keyring***.

> Sostenga el smartphone junto al medio y siga las instrucciones.

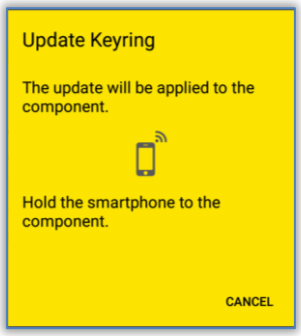


Figura 281: App de AirKey – Actualizar Keyring

La actualización del Keyring puede tardar varios minutos según la conexión a Internet. Coloque el smartphone durante todo el proceso junto al medio.

No retire el smartphone del medio que se va a actualizar durante la transmisión. La actualización correcta del Keyring finalizará con un mensaje de confirmación.

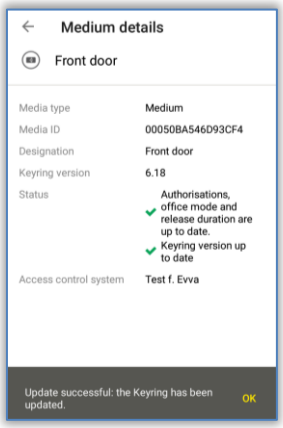


Figura 282: App de AirKey – Actualización correcta de Keyring

El estado del medio se ajustará en todo el sistema. La versión correcta del Keyring se verá en los detalles del medio.

Para actualizar una llave combi con un smartphone, deberá colocar la llave combi junto al smartphone por el lado en el que se encuentre el símbolo RFID.

Option **Actualizar versión de Keyring con estación codificadora:**

> Sostenga el medio sobre la estación codificadora. Cuando la estación codificadora reconozca el medio, comenzará la comunicación con el medio.

Recibirá un mensaje de confirmación cuando la actualización termine.

Figura 283: Estación codificadora – Actualización del Keyring disponible

Cuando haya una actualización del Keyring para el medio, aparecerá un vínculo ❶.

> Haga clic en ***Ejecutar actualización del Keyring (x.x)*** para iniciarla.

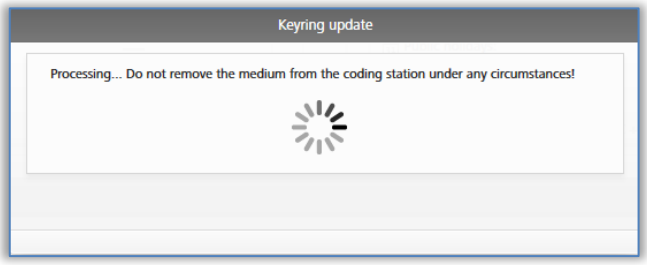


Figura 284: Estación codificadora – Actualización del Keyring

La actualización del Keyring puede durar unos minutos según la conexión a Internet. Durante este proceso, no retire el medio de la estación codificadora.

No retire el medio de la estación codificadora durante la actualización del Keyring. La actualización de la versión del Keyring finaliza con un mensaje de confirmación.

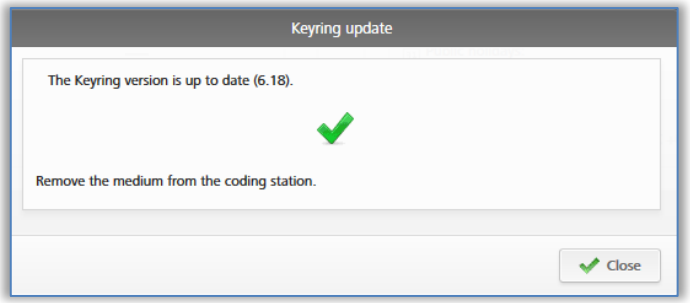


Figura 285: Estación codificadora – Actualización del Keyring finalizada

Así finaliza la actualización del Keyring. El medio se actualiza de nuevo tras cerrar el mensaje de confirmación.

Figura 286: Estación codificadora – Medio actualizado

> Tras la actualización, retire el medio de la estación codificadora.

Para actualizar la llave combi con una estación codificadora, deberá colocar la llave combi sobre la estación codificadora por el lado en el que se encuentre el símbolo RFID. Actualizar una llave combi no es posible en toda el área de lectura de la estación codificadora; con el modelo actual (HID Omnikey 5421), la llave combi solo se reconoce por los tercios superior e inferior de la estación codificadora.

El estado del medio se ajustará en todo el sistema. La versión correcta del Keyring se verá en los detalles del medio.

Para la actualización de la versión del Keyring de los medios, deberá disponerse de una conexión a Internet estable, y no se deberá cambiar la conexión de datos durante la actualización del Keyring. Para ello, según el smartphone o sistema operativo, existen los más diversos ajustes (p. ej.: cambio automático entre datos móviles y WiFi), evitar malas conexiones a Internet, etc.).

EVVA recomienda mantener la versión del Keyring de los medios siempre actualizada.

8.6 Actualizar versión de app del smartphone

Cuando esté disponible una nueva app de AirKey para smartphones, recibirá la información correspondiente en el smartphone. Conforme a los ajustes de la Google Play Store o de la Apple App Store, la app de AirKey se actualizará automáticamente o tras confirmación manual.

Tras actualizar la versión de la app, podrá seguir usándola como hasta ese momento.

Para descargar apps de la Google Play Store o Apple App Store, se necesita una cuenta de Google o un ID de Apple.

Puede ocurrir que la actualización del app de AirKey sea recomendable u obligatoria. En estos casos, se mostrará un mensaje al respecto dentro de la app de AirKey. Debido a ello, ciertas funciones se verán limitadas. Sin embargo, en ambos casos la apertura de los componentes de cierre no se verá afectada.

EVVA recomienda mantener actualizada la versión de la app de AirKey para smartphones, así como activar la actualización automática de aplicaciones en la Google Play Store o Apple App Store.

8.7 Cambio de pilas y apertura de emergencia

Las pilas de los componentes de cierre que funcionen con estas se deberán cambiar periódicamente. El estado de las pilas de los componentes de cierre puede verse en la Administración online de AirKey, así como en smartphones con autorización de mantenimiento al actualizar los componentes de cierre.

Hay tres estados de pila diferentes:

Figura 287: Estado de pilas

El componentes de cierre también avisará, si aparece el mensaje de "pila vacía", mediante una señalización especial durante el proceso de apertura con un medio. Tiene más información sobre la señalización en Señalización de los componentes de cierre.

8.7.1 Cambio de pilas en el cilindro de AirKey

Proceda al cambio de pilas con la puerta abierta y bloqueada para que no se cierre por descuido.

Tenga en cuenta que la hora del cilindro de AirKey se mantendrá como máximo durante un minuto desde que extraiga las pilas.

Se recomienda encarecidamente sustituir, con cada cambio de pilas, las juntas del cilindro de AirKey para mantener la estanqueidad. Cambie tanto

las juntas entre el eje del pomo y el pomo exterior, así como las juntas del disco del pomo exterior. Todas las juntas se pueden adquirir como piezas de repuesto. Puede solicitar más detalles a su proveedor de EVVA.

Se recomienda lubricar el cilindro de AirKey al menos con cada cambio de pilas. Para ello, se debe lubricar con unas gotas del lubricante recomendado por EVVA, tras desmontar el pomo exterior, entre el eje del pomo y el cuerpo del cilindro en la parte exterior. Además, si desmonta el cilindro de AirKey, se recomienda lubricar la parte trasera del cilindro entre la leva y el cuerpo del cilindro. Puede solicitar más detalles a su proveedor de EVVA.

- Bloquee el componentes de cierre con un medio válido.
- Fije la herramienta de montaje antes de que el cilindro se desacople.
- Desenrosque el pomo del cilindro con la herramienta de montaje girándolo en sentido contrario a las agujas del reloj.
- Saque la herramienta de montaje del pomo.
- Abra el pomo aflojando los tres tornillos en la parte posterior del mismo.
- Desmonte el disco del pomo.
- Suelte con cuidado el seguro de las pilas moviéndolo hacia arriba.
- Cambie las pilas. Coloque las pilas en la posición correcta. No mezcle pilas nuevas con usadas.
- Fije con cuidado el seguro de las pilas.
- Coloque el disco del pomo sobre el mismo y fíjelo con los tres tornillos.
- Fije la herramienta de montaje en el pomo.
- Tenga cuidado de que la junta de estanquidad está correctamente colocada en el eje del cilindro y enrosque de nuevo el pomo en el sentido de las agujas del reloj sobre el cilindro hasta que sienta una resistencia.
- Retire la herramienta de montaje.
- Gire, a continuación, el pomo en sentido contrario a las agujas del reloj, hasta que sienta cómo se acopla.
- Preste atención a que el pomo y el módulo electrónico estén correctamente acoplados.
- Actualice el cilindro con el smartphone o la estación codificadora para transferir las entradas de la lista de eventos a la Administración online de AirKey.
- Compruebe que el cilindro funcione correctamente con una prueba de apertura antes de volver a cerrar la puerta.

Debido a las características físicas de las pilas, estas deberán cambiarse con más regularidad si la temperatura es muy baja (por debajo de -10 °C) durante un largo período de tiempo, y se deberá comprobar el funcionamiento del cilindro y el estado de las pilas.

Si se señaliza un error de comunicación al cambiar las pilas, es que el pomo intenta comunicarse con el módulo electrónico. Esto no funcionará mientras el pomo no esté atornillado sobre el módulo electrónico.

Compruebe el estado de las pilas de los componentes de cierre a través de un smartphone con autorización de mantenimiento, actualizando el componentes de cierre y, con posterioridad, viendo los detalles del componentes de cierre.

Si las pilas no se cambiasen a tiempo, se puede dar una apertura de emergencia mediante un alimentador de emergencia opcional.

Tiene una descripción del proceso en Alimentador de emergencia.

Tras la apertura de emergencia, cambie las pilas y actualice el componentes de cierre antes de volver a cerrar la puerta.

Tras su uso, vuelva a cerrar con cuidado la cubierta de goma blanca con el logo de EVVA para seguir protegiendo la apertura de la conexión del alimentador de emergencia frente a la entrada de polvo y humedad. No utilice objetos punzantes para evitar posibles daños.

8.8 Opciones de reparación

En las opciones de reparación de componentes de cierre, se puede proceder a reparar un defecto. Existe la posibilidad de expedir componentes de cierre de repuesto en el sistema de control de accesos o de retirar un componentes de cierre defectuoso del sistema de control de accesos.

8.8.1 Crear y montar componentes de cierre de repuesto

Con la expedición y la instalación posterior de un componentes de cierre de repuesto, se sustituye un componentes de cierre defectuoso por otro en estado de fábrica. Con esta opción, se mantendrán todas las características y autorizaciones para este componentes de cierre dentro del sistema de control de accesos. El componentes de cierre de repuesto no se encontrará más en estado de fábrica tras finalizar el proceso.

> En la página de inicio ***Home***, haga clic en la opción ***Cilindros*** o ***Lectores murales***.
> También puede elegir en el menú principal ***Sistema de control de accesos*** → ***Componentes de cierre***.
> En la lista general, haga clic sobre el componentes de cierre que desea editar.
> En la pestaña "Ajustes", haga clic en el bloque ***Registro de eventos y mantenimiento*** en ***Mostrar opciones de reparación*** ❶.

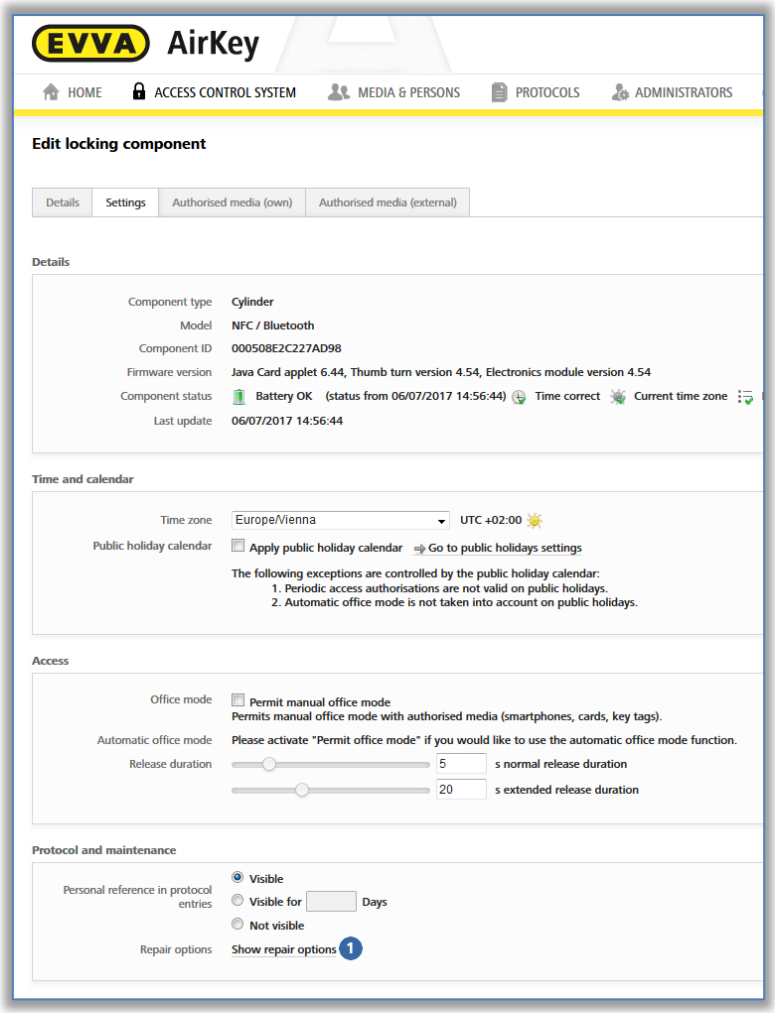


Figura 288: Editar componentes de cierre – Opciones de reparación

Se abre una ventana ***Opciones de reparación***.

> De forma predeterminada, están preajustados los botones de radio ***Desmontaje e instalación de componente de reemplazo*** 1 y Sustituir clindro (pomo y módulo electrónico de manera conjunta).

> También puede seleccionar el botón de radio ***Sustituir únicamente el pomo***.

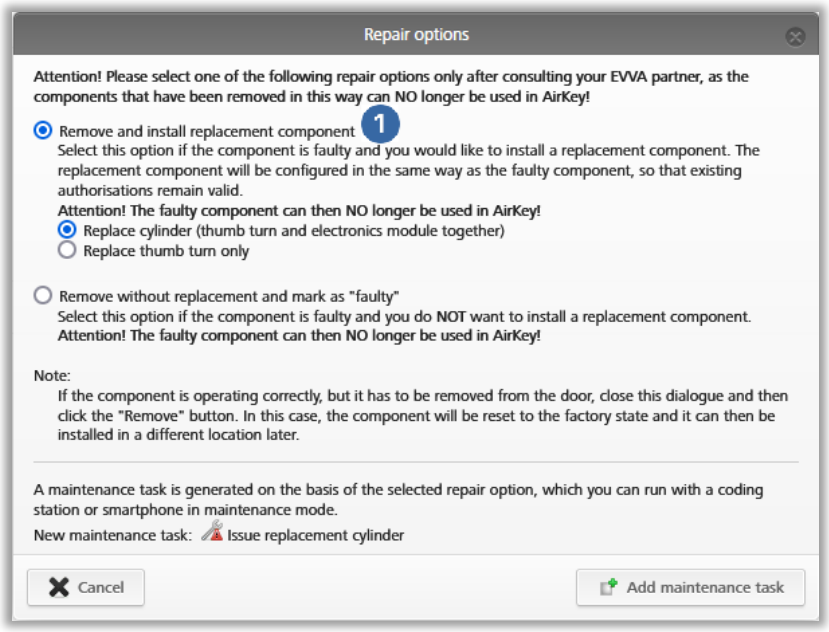


Figura 289: Opciones de reparación

> Haga clic en ***Añadir tarea de mantenimiento***.

El estado ❶ del componentes de cierre se actualizará y se mostrará como tarea de mantenimiento ❷.

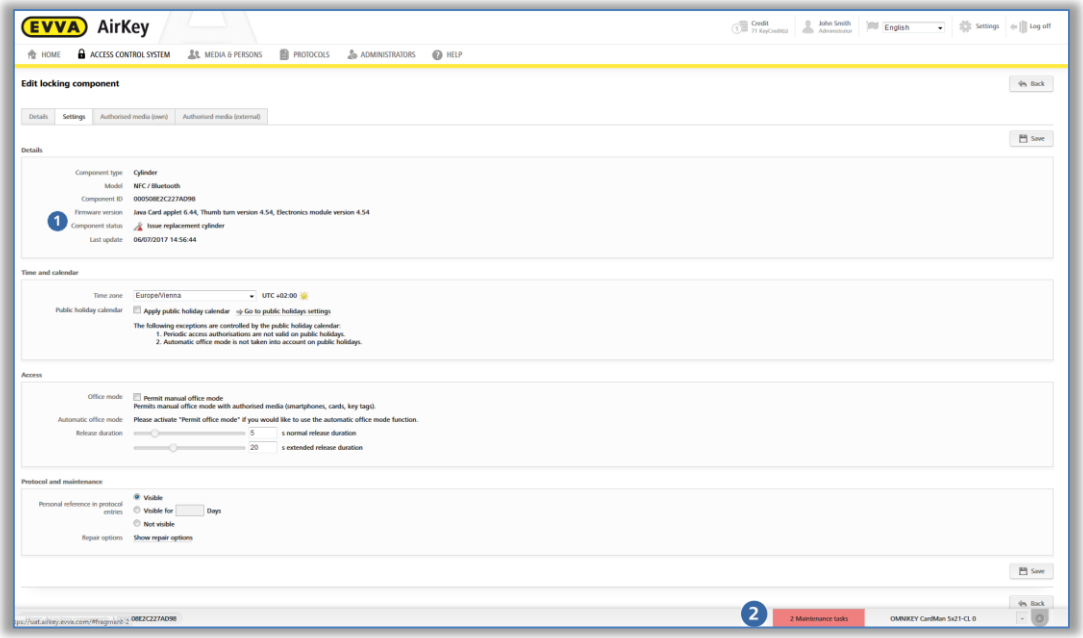


Figura 290: Estado de componente y tarea de mantenimiento

Los preparativos para la expedición y el montaje de un componentes de cierre de repuesto se finalizan dentro de la Administración online de AirKey. Para finalizar todo el proceso, deberá expedir y montar el componentes de cierre de repuesto con el smartphone con autorización de mantenimiento o la estación codificadora opcional.

El componente reemplazado se puede seguir actualizando hasta que el montaje del componente de repuesto haya finalizado del todo. Para garantizar la integridad de las listas de eventos, debe haber accesos entre el comienzo y el final del montaje del componente de repuesto.

Al reemplazar componentes de cierre con Bluetooth, los componentes sustituidos y los de repuesto se muestran en la lista de componentes Bluetooth al alcance. Los componentes sustituidos deben quedar sin corriente tras su reemplazo y entonces desaparecen de la lista de componentes Bluetooth.

Crear y montar componentes de cierre de repuesto con el smartphone

Para ello, se requiere un smartphone con autorización de mantenimiento para el sistema de control de accesos donde se debe crear y montar el componentes de cierre de repuesto.

- Establezca la conexión a través de **NFC** (en smartphones Android): Haga clic en el símbolo ***Conectar con componente*** y sostenga el smartphone junto al componentes de cierre en estado de fábrica.
- Establezca la conexión a través de **Bluetooth** (en smartphones **Android**): En el componentes de cierre en estado de fábrica que quiera añadir al sistema de control de accesos, seleccione el menú contextual (⋮) y elija entonces ***Conectar***.
- Establezca la conexión a través de **Bluetooth** (en **iPhones**): En el componentes de cierre en estado de fábrica que quiera añadir al sistema de control de accesos, en la identificación "En estado de fábrica" deslícese a la izquierda y elija ***Conectar***.
- Tras la actualización, en los detalles del componentes de cierre haga clic en ***Expedir cilindro de reemplazo***.
- En el continuar cuadro de diálogo, haga clic en el componentes de cierre que se debe sustituir y confirme con ***Continuar***.
- Al utilizar NFC, sostenga de nuevo el smartphone junto al componentes de cierre en estado de fábrica. Al utilizar Bluetooth, elija el componentes de cierre en estado de fábrica de la lista de componentes de cierre dentro del alcance de recepción.
- Determine si se debe crear una tarea de mantenimiento para el montaje posterior.
- Finalice el proceso con ***Instalar más tarde*** si debe montar el componentes de cierre aún en la puerta, o elija ***Finalizar*** si ya ha concluido el montaje en la puerta.
- Actualice el componentes de cierre tras el montaje en la puerta.

Option Crear y montar componentes de cierre de repuesto con la estación codificadora.

- Sostenga un componentes de cierre de repuesto en estado de fábrica sobre la estación codificadora.
- Abajo a la derecha en la ventana, elija ***Expedir cilindro de reemplazo*** y el componentes de cierre que se deba sustituir.

Figura 291: Componente en estado de fábrica – Crear cilindro de repuesto

> Haga clic en ***Continuar***.
> Sostenga el componentes de cierre de repuesto en estado de fábrica sobre la estación codificadora.
> Retire el componentes de cierre de repuesto solo tras ver el mensaje de confirmación correspondiente.
> Determine si se debe crear una tarea de mantenimiento para el montaje posterior.
> Finalice el proceso con ***Instalar más tarde*** si debe montar el componentes de cierre aún en la puerta, o elija ***Finalizar*** si ya ha concluido el montaje en la puerta.
> Actualice el componentes de cierre tras el montaje en la puerta.
>
> Si el componentes de cierre de repuesto tiene una versión de firmware antigua, se actualizará este durante el proceso.

El componentes de cierre sustituido ya no se podrá utilizar tras este proceso. Por ello, esta función se debe emplear solo si el componentes de cierre está defectuoso realmente y si no lo necesita más.

8.8.2 Desmontar componentes de cierre sin reemplazo y marcar como "defectuoso"

Si no se debe sustituir un componentes de cierre defectuoso, pero no debe seguir apareciendo en el sistema de control de accesos, este se podrá desmontar sin reemplazo mediante las opciones de reparación.

El componentes de cierre no se podrá actualizar ni usar más.

> En la página de inicio ***Home***, haga clic en la opción ***Cilindros*** o ***Lectores murales***.
> También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.
> En la lista general, haga clic sobre el componentes de cierre que desea editar.
> En la pestaña ***Ajustes***, dentro del bloque ***Registro de eventos y mantenimiento***, haga clic en el vínculo ***Mostrar opciones de reparación*** ❶.

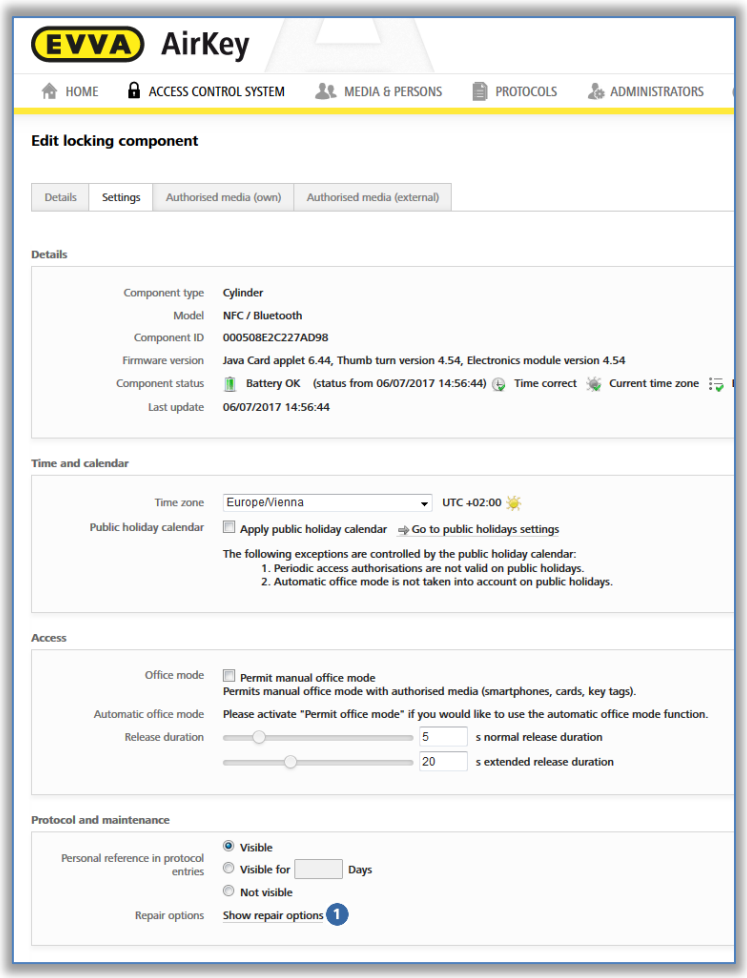


Figura 292: Editar componentes de cierre – Opciones de reparación

Se abre una ventana "Opciones de reparación".

> Elija ***Desmontar sin reemplazar y marcar como "defectuoso"*** ❶.

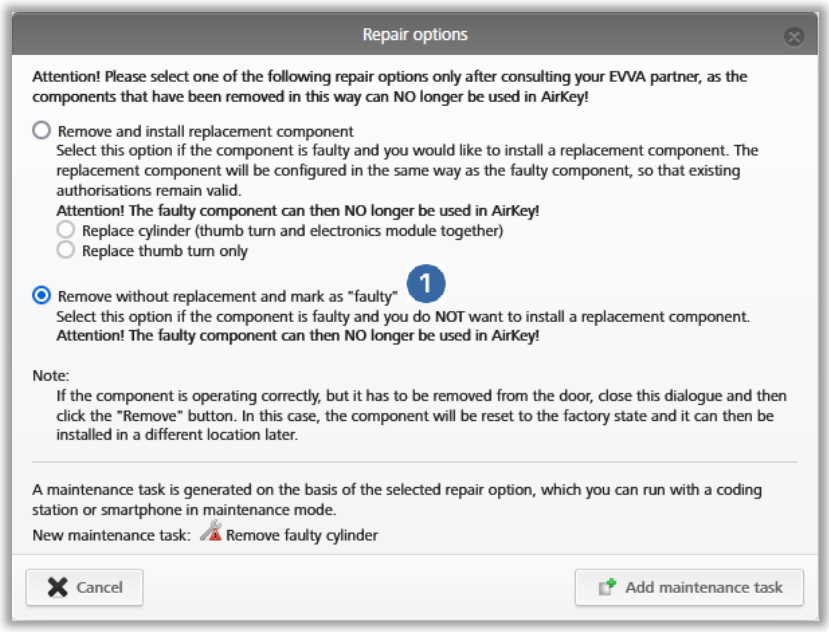


Figura 293: Opciones de reparación

> Haga clic en ***Añadir tarea de mantenimiento***.

El estado ❶ del componentes de cierre se actualizará y se mostrará como tarea de mantenimiento ❷.

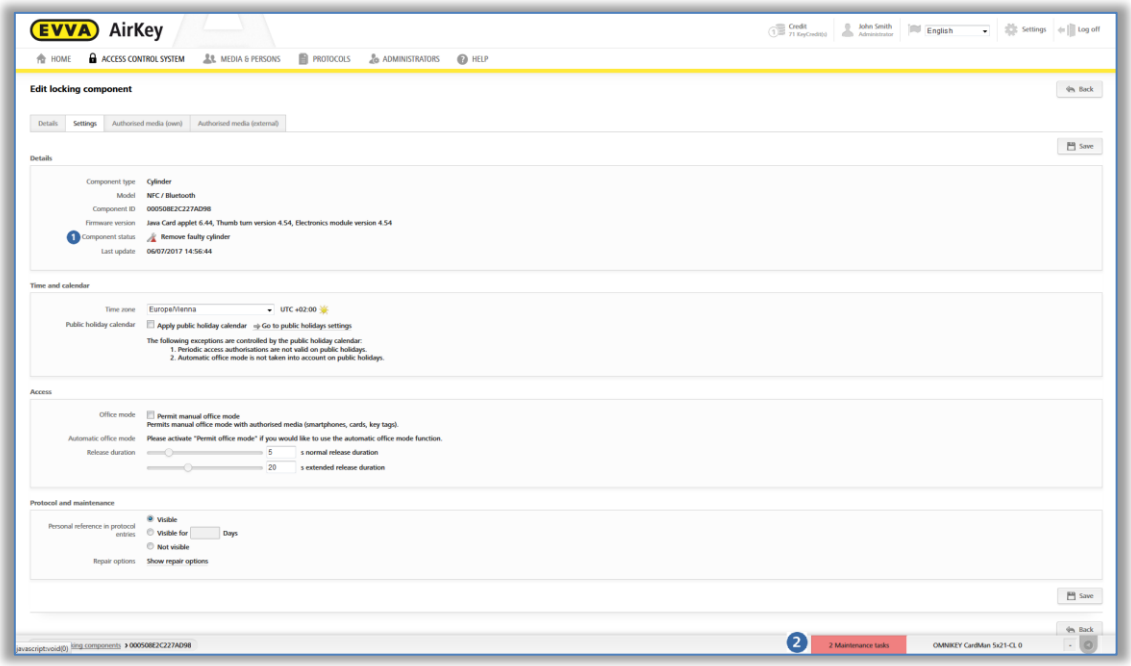


Figura 294: Estado de componente y tarea de mantenimiento

Los preparativos para desmontar un componentes de cierre defectuoso sin reemplazo finalizan dentro de la Administración online de AirKey. Para finalizar todo el proceso, deberá finalizar el desmontaje por medio de un smartphone con autorización de mantenimiento o dentro de la Administración online de AirKey.

8.8.3 Desmontar componentes de cierre defectuoso mediante smartphone

Si se puede actualizar aún el componentes de cierre defectuoso, puede realizar el desmontaje sin reemplazo de un componentes de cierre defectuoso a través del smartphone. Se requiere un smartphone registrado con modo de mantenimiento activado para este sistema AirKey.

> Establezca la conexión a través de **NFC** (en smartphones Android): Haga clic en el símbolo ***Conectar con componente*** y sostenga el smartphone junto al componentes de cierre que se debe desmontar.

> Establezca la conexión a través de **Bluetooth** (en smartphones **Android**): En el componentes de cierre que se debe desmontar, seleccione el menú contextual (⋮) y elija entonces ***Conectar***.

> Establezca la conexión a través de **Bluetooth** (en **iPhones**): En el componentes de cierre que se debe desmontar, deslícese a la izquierda hasta la denominación y elija entonces ***Conectar***.

> Se mostrarán los detalles del componente. Elija ***Desmontar cilindro defectuoso*** ❶.

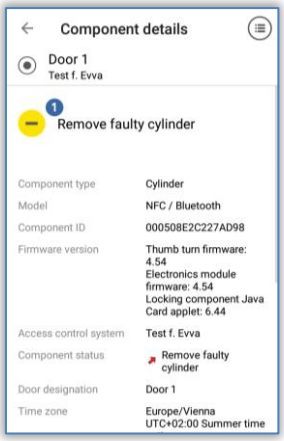


Figura 295: Desmontar componente defectuoso con smartphone

> Marque la casilla del cuadro de diálogo y confirme con ***Finalizar***.

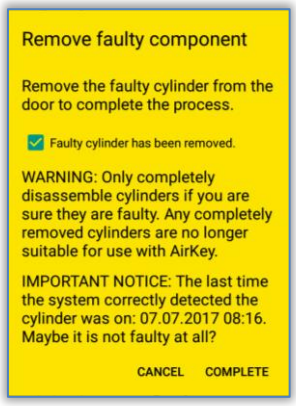


Figura 296: Desmontar componente defectuoso con smartphone – Confirmación

De esta manera, se finaliza el proceso y el componentes de cierre no aparecerá más listado en el sistema de control de accesos. El componente ya no se podrá usar más.

8.8.4 Desmontar componente defectuoso mediante Administración online de AirKey

Si no se puede actualizar más el componentes de cierre por un defecto, se deberá efectuar el desmontaje sin reemplazo a través de la Administración online de AirKey.

> En la página de inicio ***Home***, elija la opción ***Cilindros*** o ***Lectores murales***, según el componente marcado como defectuoso.

> También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.

> En la lista general, haga clic sobre el componentes de cierre que desea editar.

> En la pestaña ***Ajustes***, dentro del bloque ***Registro de eventos y mantenimiento***, haga clic en el vínculo ***Mostrar opciones de reparación***.

> Aparecerá una ventana en la que podrá elegir tres opciones.

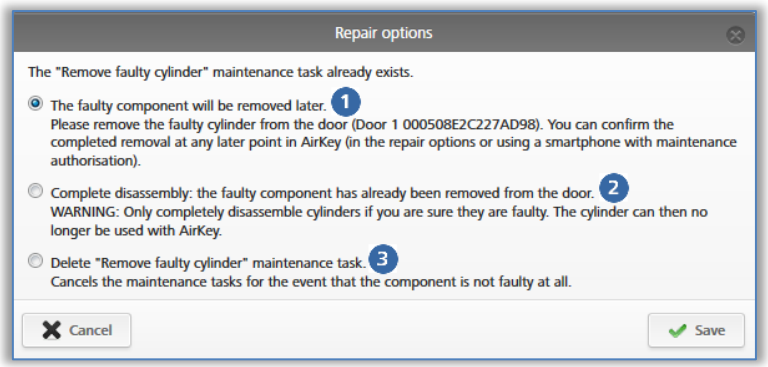


Figura 297: Desmontar componentes de cierre defectuoso

- Con la opción ***El componente defectuoso será eliminado más tarde*** ❶, mantendrá el estado actual del componente y este seguirá formando parte del sistema de control de accesos.
- Con la opción ***Desmontaje completo: El componente defectuoso ya ha sidoeliminado de la puerta*** ❷ finalizará el proceso de desmontaje sin reemplazo de un componentes de cierre defectuoso, y este se eliminará del sistema de control de accesos.
- Con la opción ***Eliminar tarea de mantenimiento "Eliminar cilindro defectuoso"*** ❸, se deshará de nuevo el desmontaje sin reemplazo. Encontrará más información en Deshacer tareas de mantenimiento para opciones de reparación.

El componentes de cierre desmontado sin reemplazo ya no se puede emplear más tras este proceso. Por ello, esta función se debe emplear solo si el componentes de cierre está defectuoso realmente y si no lo necesita más.

Cuando quiera eliminar un componentes de cierre que funcione de su sistema de control de accesos, utilice las instrucciones en Eliminar componentes de cierre.

8.8.5 Deshacer tareas de mantenimiento para opciones de reparación

Si se crea por error una tarea de mantenimiento para un componentes de cierre de repuesto o uno desmontado sin reemplazo, esta tarea de mantenimiento se puede borrar posteriormente.

- En la página de inicio ***Home***, elija el vínculo ***Tareas de mantenimiento***.
- En la lista, seleccione la tarea de mantenimiento deseada.
- En la pestaña ***Ajustes***, dentro del bloque ***Registro de eventos y mantenimiento***, haga clic en el vínculo ***Mostrar opciones de reparación***.
- Según la tarea de mantenimiento abierta, elija si el componentes de cierre de repuesto (cilindro, pomo, lector mural) se debe expedir más adelante ❶ o si se debe borrar la tarea de mantenimiento ❷.

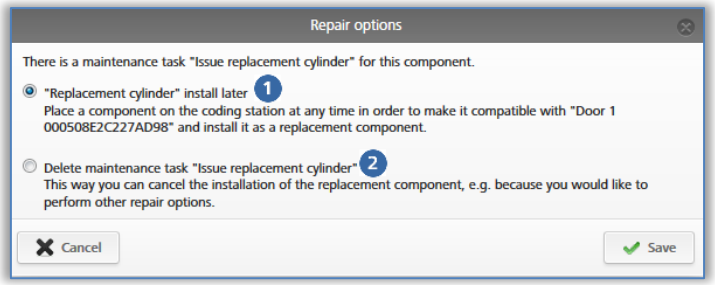


Figura 298: Borrar tarea de mantenimiento

> Haga clic en ***Guardar***.

La tarea de mantenimiento se deshará. El estado del componentes de cierre se actualizará según el último estado de este.

En cuanto se haya completado la tarea de mantenimiento, esta no se podrá deshacer.

Utilice también esta función para deshacer la tarea de mantenimiento "Se debe eliminar el componente" cuando el componentes de cierre sin defectos se haya eliminado del sistema de control de accesos.

9 Medios de emergencia

Un medio de emergencia es un medio con autorización permanente ilimitada para todos los componentes de cierre de un sistema de control de accesos. Los medios de emergencia se utilizan en situaciones de emergencia (por ejemplo, en caso de actuación de los bomberos) y deben guardarse en un lugar seguro. Los medios de emergencia tienen acceso con independencia de la hora en el componentes de cierre. Solo se requiere garantizar el suministro eléctrico de los componentes de cierre.

9.1 Crear medios de emergencia

Para crear un medio de emergencia, sostenga un medio en forma de tarjeta, llavero o llave combi (como se describe en el capítulo Crear tarjetas, llaveros, pulseras y llaves combi) y otorgue a los medios de emergencia autorizaciones de acceso permanente para todas las puertas del sistema de control de accesos. Tenga en cuenta que, en caso de ampliación del sistema, los medios de emergencia se deberán actualizar para tener acceso a las puertas adicionales en caso de emergencia. Los medios de emergencia tienen acceso también a componentes de cierre con la hora equivocada (p. ej. los cilindros pierden la hora cuando se gastan las pilas). Encontrará más información sobre la concesión y creación de autorizaciones en Otorgar autorizaciones y Crear autorización.

Tenga en cuenta que los medios en forma de tarjetas, llaveros, pulseras o llaves combi también pueden ser defectuosos. Por ello, según el sistema de control de accesos, cree la correspondiente cantidad de medios de emergencia.

Como medios de emergencia, se recomienda únicamente usar medios en forma de tarjetas, llaveros, pulseras o llaves combi, ya que los smartphones no son adecuados para este fin debido a la duración limitada de la batería.

Para facilitar la gestión de los medios de emergencia, puede trabajar con áreas que incluyan todas las puertas pertenecientes al sistema de control de accesos. Otorgue entonces a los medios de emergencia una autorización permanente ilimitada para esta área.

10 Reemplazo de medios

10.1 Reemplazo de smartphone

El reemplazo de smartphone facilita el cambio de un smartphone a otro; por ejemplo, al comprar un nuevo dispositivo.

Con el reemplazo de smartphone, se transfieren al nuevo smartphone todas las autorizaciones y ajustes de AirKey (excepto el PIN y los ajustes locales de modo Hands-free) del smartphone ya existente.

El reemplazo se puede realizar tanto de Android a iOS como a la inversa.

El reemplazo puede iniciarlo un administrador en la administración online de AirKey o directamente desde el smartphone.

El smartphone «antiguo» se denomina **medio de origen** y el smartphone «nuevo», **medio de destino**.

El medio de origen se desactiva automáticamente una vez finalizada la acción de reemplazo. Si el medio de origen ya no funciona o no está disponible, se debe actualizar la lista negra de los componentes AirKey afectados. Solo después se restablece la seguridad de la instalación.

Si, durante la acción de reemplazo, también se transfieren autorizaciones al medio de destino, también se deducirá un KeyCredit del saldo existente. Si no hay KeyCredits disponibles, el reemplazo solo se puede finalizar en cuanto se disponga de nuevo de saldo.

10.1.1 Iniciar reemplazo como propietario del smartphone

Si el medio de origen sigue funcionando, está registrado y no está desactivado, se puede iniciar el reemplazo de smartphone directamente mediante el medio de origen.

> Inicie la app de AirKey en el smartphone antiguo.
> En el menú, pulse ***Ajustes*** → ***Reemplazar smartphone.***
> Confirme el diálogo con ***OK***.

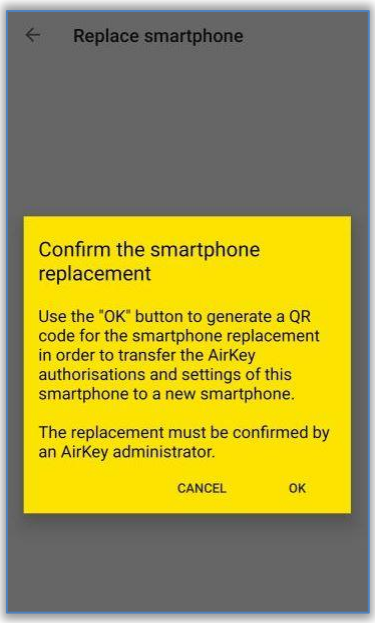


Figura 299: Confirmar operación de reemplazo de smartphone

> En el medio de origen se muestra un código QR con un texto de ayuda.

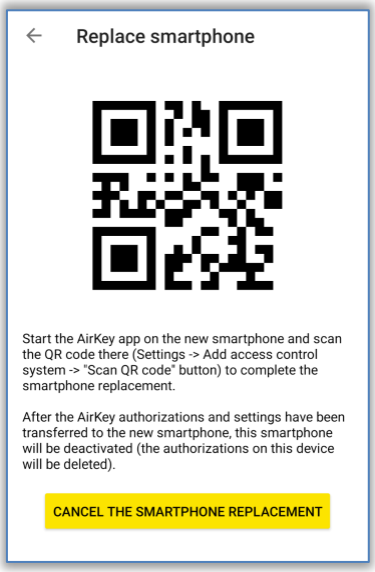


Figura 300: Código QR para la operación de reemplazo de smartphone

Los pasos en el medio de origen han concluido. El medio de origen puede seguir utilizándose como de costumbre hasta que finalice la acción de reemplazo. El código QR es válido durante 30 días y se vuelve a mostrar en este periodo al pulsar ***Ajustes*** → ***Reemplazar smartphone***.

Dado que con el reemplazo de smartphone se crea un nuevo smartphone y, en función de las autorizaciones transmitidas, también se necesitan KeyCredits, un administrador debe confirmar el reemplazo dentro de la administración online de AirKey.

> Inicie sesión en la administración online de AirKey.

> En la página de inicio, haga clic en la opción ***Operaciones pendientes de reemplazo de smartphone***.

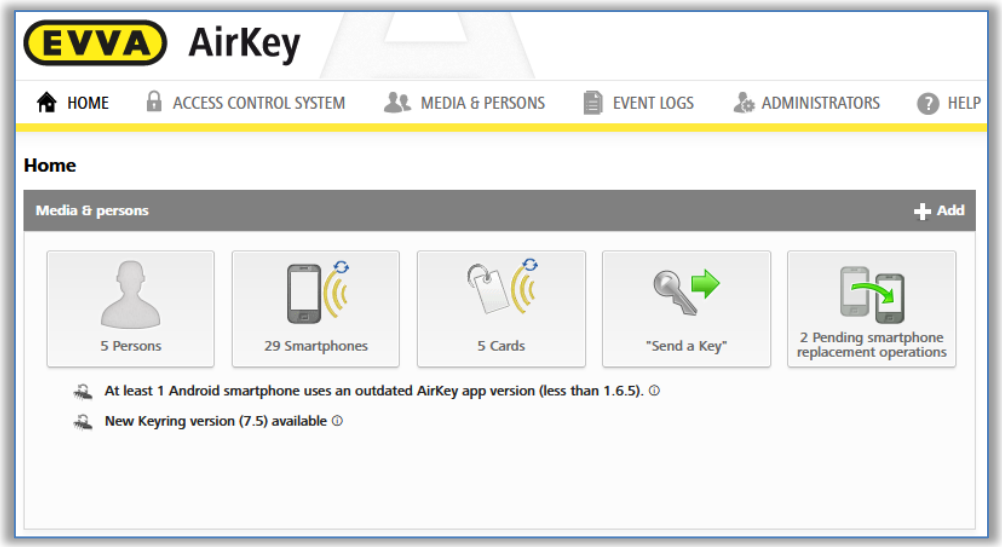


Figura 301: Página de inicio – operaciones pendientes de reemplazo de smartphone

> En la columna «Acción» se puede confirmar el reemplazo con la marca de verificación verde, o rechazarlo con la «X» roja.

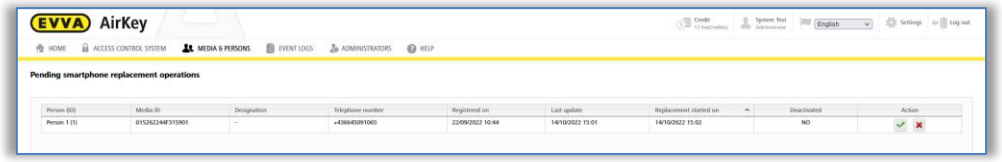


Figura 302: Operaciones pendientes de reemplazo de smartphone

Tras la confirmación del administrador, se puede finalizar el reemplazo escaneando el código QR en el medio de destino. Si el administrador rechaza el reemplazo, se interrumpe el reemplazo de smartphone y el código QR ya no es válido y se elimina. Si se escanea el código QR en el medio de destino antes de que un administrador confirme el reemplazo, aparecerá el mensaje de error correspondiente.

Figura 303: Ha fallado el reemplazo de smartphone

Los administradores también pueden activar una confirmación automática para las acciones de reemplazo de smartphone en los ajustes de la administración online de AirKey (véase el capítulo Aspectos generales). De este modo, cada reemplazo de smartphone iniciado a través de un smartphone se confirma automáticamente si hay crédito suficiente. Tenga en cuenta que para cada reemplazo de smartphone en el que se transfieran autorizaciones, se necesitará un KeyCredit.

Para escanear el código QR con un medio de destino no registrado aún, siga los siguientes pasos:

> Inicie la app de AirKey.
> Confirme el acuerdo de licencia del usuario final.
> Pulse ***Escanear código QR*** y escanee el código QR del medio de origen.

Para escanear el código QR con un medio de destino ya registrado en AirKey, siga los siguientes pasos:

> Inicie la app de AirKey.
> En el menú, pulse ***Ajustes*** → ***Añadir sistema de control de accesos.***
> Pulse ***Escanear código QR*** y escanee el código QR del medio de origen.

El reemplazo de smartphone ha finalizado y el medio de destino se ha registrado correctamente con las autorizaciones y ajustes de AirKey del medio de origen. El medio de origen se desactiva automáticamente tras un reemplazo correcto.

Si el medio de origen se encuentra en más de un sistema de control de accesos, el reemplazo se inicia simultáneamente en todos los sistemas de control de accesos. Esto significa que es posible que varios administradores tengan también que confirmar el reemplazo dentro de la administración online de AirKey. Solo se transfieren al medio de destino las autorizaciones y los ajustes de AirKey para los sistemas de control de accesos en los que los administradores han confirmado el reemplazo.

10.1.2 Iniciar reemplazo como administrador

Si el medio de origen ya no está disponible o ya no funciona, también se puede iniciar el reemplazo como administrador.

> En la página de inicio ***Home***, elija la opción ***Smartphones***.
> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.
> Seleccione en la lista de medios el smartphone que se debe reemplazar.
> Haga clic en ***Más...*** ❶ → ***Reemplazar smartphone***.

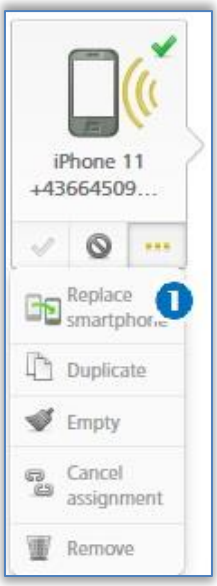


Figura 304: Reemplazo de smartphone

> Se abre un diálogo en el que se debe introducir el número de teléfono del medio de destino. El número de teléfono del medio de origen se acepta automáticamente.

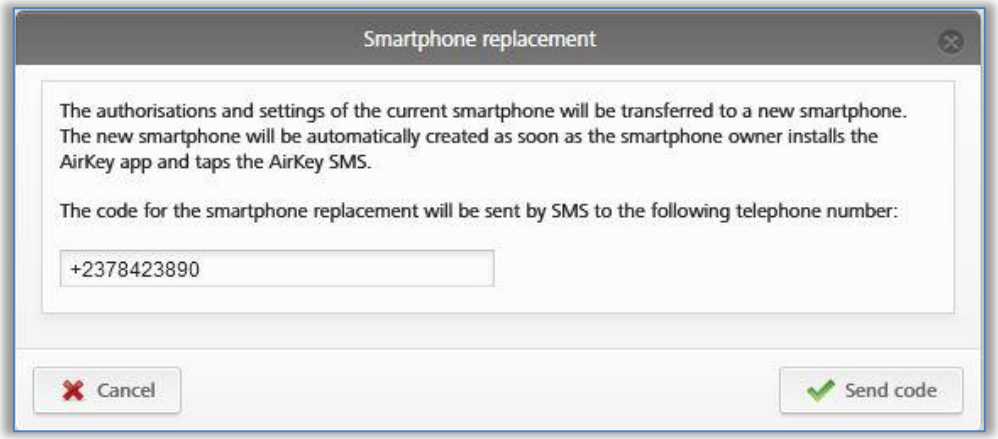


Figura 305: Reemplazo de smartphone

> Compruebe que el número de teléfono es correcto y confirme con ***Enviar código***.
> Se enviará un SMS de AirKey con un enlace de registro al número de teléfono del medio de destino indicado.

El reemplazo de smartphone debe finalizarse ahora en el medio de destino:

> Abra el SMS con el enlace de registro en el medio de destino.
> Pulse el enlace de registro y siga las instrucciones.

El reemplazo de smartphone ha finalizado y el medio de destino se ha registrado correctamente con las autorizaciones y ajustes de AirKey del medio de origen. El medio de origen se desactiva automáticamente tras un reemplazo correcto.

El enlace de registro del SMS es válido durante 30 días. Si el enlace de registro no ha llegado por SMS, se puede volver a enviar por SMS:

> Haga clic debajo del smartphone en ***Más...*** ❶ → ***Reemplazar smartphone***.

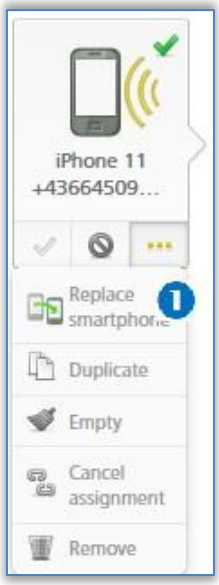


Figura 306: Reemplazo de smartphone

> Se abre un diálogo en el que se puede comprobar de nuevo y modificar el número de teléfono.

Figura 307: Reemplazo de smartphone – Reenviar código

> Haga clic en ***Reenviar código***.

En este diálogo también se puede cancelar el reemplazo, si ya no es necesario.

Si el medio de origen se encuentra en más de un sistema de control de accesos, un administrador debe iniciar el reemplazo de cada sistema de control de accesos. En consecuencia, también se envía un SMS con un enlace de registro para cada sistema de control de accesos.

11 Trabajar con varios sistemas AirKey

En el continuar capítulo, encontrará información sobre cómo trabajar con varios sistemas AirKey.

11.1 Activar componente de cierre para otros sistemas de control de accesos

Puede activar un componente añadido a su sistema de control de accesos para otro sistema de control de accesos. En el otro sistema de control de accesos, también se podrán otorgar autorizaciones para este componentes de cierre. Cada componentes de cierre se puede activar para un máximo de 250 sistemas AirKey.

> En la página de inicio ***Home***, haga clic en la opción ***Cilindros*** o ***Lectores murales***.
> También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.
> En la lista general, haga clic en la denominación de la puerta del componentes de cierre que desea activar.

En el bloque ***Autorizaciónes para compartir cilindros*** de los detalles del componentes de cierre, se relacionan las activaciones ya concedidas.

> Haga clic en ***Añadir activación*** para compartir.

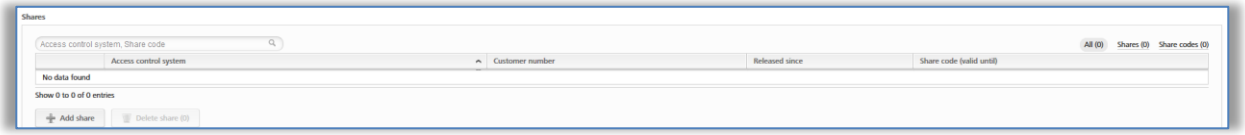


Figura 308: Activar componentes de cierre

> Se generará un código de activación de 12 caracteres.

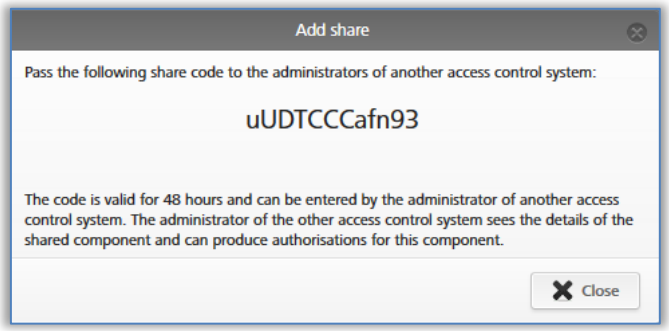


Figura 309: Añadir activación

> Comunique este código de activación al administrador del otro sistema de control de accesos.

El código de activación es válido durante 48 horas.

Se pueden generar varios códigos de activación para un componentes de cierre. Estos se mostrarán en la lista de activaciones del componentes de cierre.

Aparecerá una entrada en la lista de activaciones del componentes de cierre. En esta se puede ver el código de activación y su validez.

11.2 Añadir componentes de cierre de otros sistemas de control de accesos

Cuando se le active un componentes de cierre desde otro sistema de control de accesos, deberá añadirlo a su sistema de control de accesos.

> En la página de inicio ***Home*** en la barra gris ***Sistema de control de accesos***, haga clic en ***Añadir*** → ***Añadir componente*** ❶.

Figura 310: Añadir componentes de cierre – Barra gris

> También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.

> Haga clic en ***Añadir componentes de cierre*** ❶.

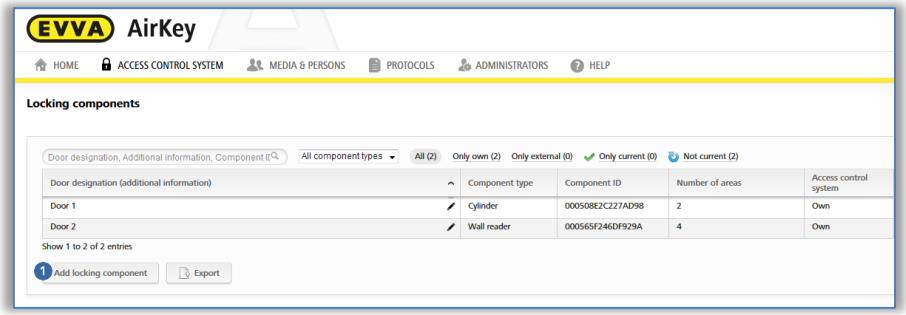


Figura 311: Añadir componentes de cierre

> Elija el tipo ***Componente de cierre compartido*** ❶.

> Haga clic en ***Continuar***.

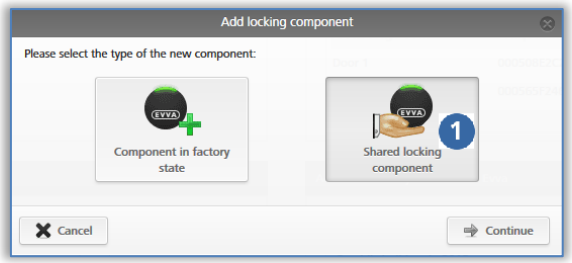


Figura 312: Añadir componentes de cierre compartido

> Introduzca el código de activación del otro sistema de control de accesos para añadir el componentes de cierre.

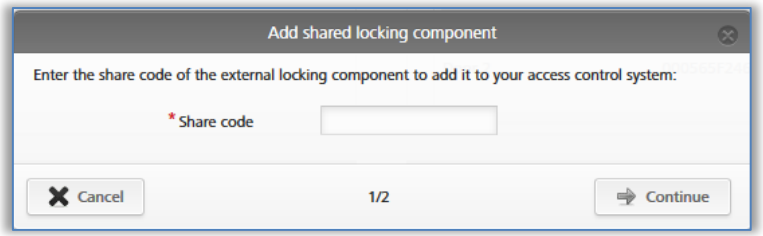


Figura 313: Añadir componentes de cierre compartido

Si el código de activación introducido no es correcto, recibirá un mensaje de error.

Si el código de activación introducido es correcto, podrá editar los continuars ajustes:

> Designación de puerta alternativa ❶

> Conforme a la protección de datos, la referencia personal en las entradas de la lista de eventos para el propietario del componentes de cierre se podrá ver o no ❷.

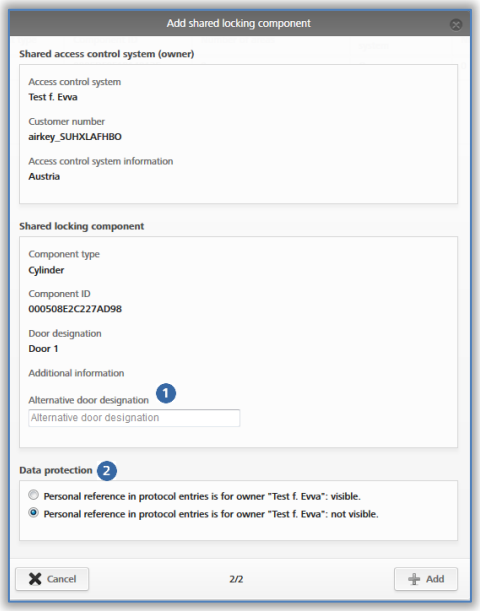


Figura 314: Añadir componentes de cierre activado

> Se creará una tarea de mantenimiento.

> Actualice el componentes de cierre mediante un smartphone con autorización de mantenimiento o una estación codificadora opcional.

> De este modo, se eliminará la tarea de mantenimiento de la lista y la activación estará actualizada.

> Una vez añadido el componentes de cierre activado, aparece el componentes de cierre en la columna "Sistema de control de accesos" con el atributo "Externo" en la lista de componentes de cierre. El cliente que haya añadido el componentes de cierre, puede editar la designación alternativa de la puerta y asignar el componentes de cierre a un área en la pestaña "Detalles". En la pestaña "Ajustes", se puede modificar el botón de radio del bloque "Protección de datos" para diferenciar entre "visible" y "no visible" el componentes de cierre en la referencia personal en las entradas de la lista de eventos para el propietario. Además se puede configurar la referencia personal en las entradas de la lista de eventos en el bloque "Registro de eventos y mantenimiento" para el sistema de control de accesos activado. Las autorizaciones de acceso se pueden otorgar asimismo para el componentes de cierre activado.

No se puede activar un componentes de cierre externo para otros sistemas AirKey.

11.3 Otorgar autorizaciones para componentes de cierre activados

Dentro del sistema de control de accesos donde se añadió el componentes de cierre activado, el desarrollo del otorgamiento de autorizaciones apenas se diferencia del desarrollo del propietario del componentes de cierre. Siga los pasos si ha añadido un componentes de cierre activado en el sistema de control de accesos.

> En la página de inicio ***Home***, elija la opción ***Smartphones*** o ***Tarjetas.***

> También puede elegir en el menú principal ***Medios y personas*** → ***Medios***.

> Haga clic en el medio deseado en la lista general.

> Si el medio está asignado a una persona, aparecerá una vista general de las autorizaciones del medio.

> Debajo de las casillas de todos los componentes de cierre y áreas, elija la pestaña ***Externo*** ❶ para ver todos los componentes de cierre añadidos de sistemas AirKey externos.

>

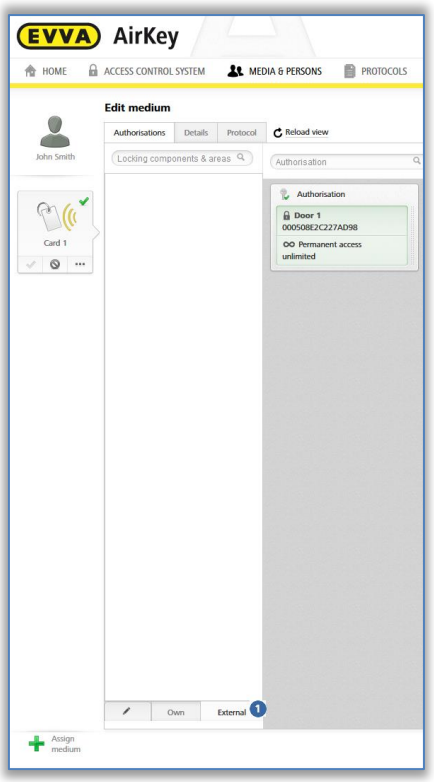


Figura 315: Autorización para componentes de cierre activado

- Arrastre y suelte el botón con la puerta activada seleccionada en la superficie gris. Tan solo cuando arrastre la puerta o área escogida a la parte central, aparecerán los tipos de acceso.
- Elija el tipo de acceso deseado arrastrando y soltando la puerta / área sobre el campo correspondiente.
- Cree la autorización para canjear un KeyCredit. Tiene más información sobre crear autorizaciones en Crear autorización. El KeyCredit se deducirá del crédito de su sistema de control de accesos, y no del otro sistema de control de accesos.

11.4 Ver autorizaciones para componentes de cierre activados

Si ha activado un componentes de cierre para otro cliente, puede ver también los medios del otro cliente que están autorizados para el componentes de cierre activado.

- En la página de inicio ***Home***, haga clic en la opción ***Cilindros*** o ***Lectores murales***.
- También puede elegir en el menú principal ***Sistema de control de accesos*** → ***Componentes de cierre***.
- En la lista general, haga clic sobre el componentes de cierre cuyos detalles quiere ver.
- Haga clic en ***Medios autorizados (externos)*** ❶ para obtener una vista general de todos los medios externos que tienen una autorización para este componentes de cierre.

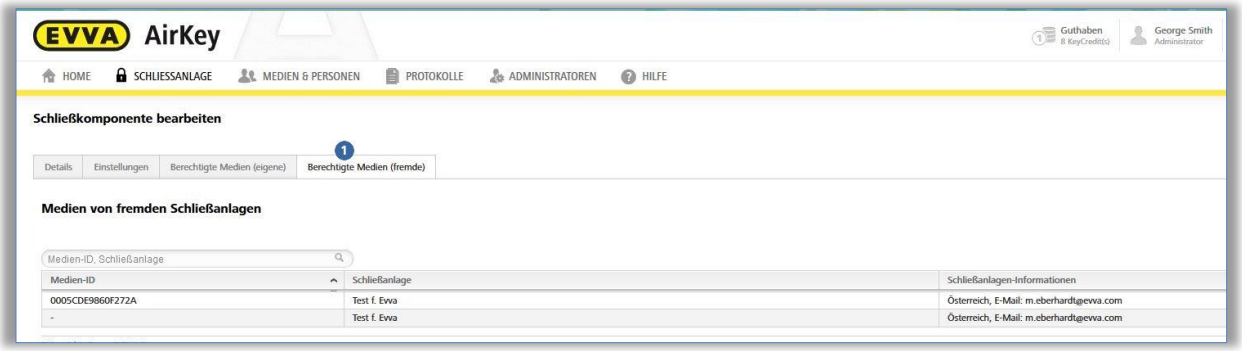


Figura 316: Medios autorizados (externos)

11.5 Anular activación de un componentes de cierre

Puede volver a anular la activación concedida por usted de un componentes de cierre. Proceda de la continuar manera:

> En la página de inicio ***Home***, haga clic en la opción ***Cilindros*** o ***Lectores murales***.

> También puede elegir en el menú principal ***Sistema de control de accesos*** → Componentes de cierre.

> En la lista general, haga clic en el componentes de cierre cuya activación desea anular.

En la pestaña ***Detalles***, en el bloque ***Autorizaciónes para compartir cilindros***, seleccione la activación correspondiente y haga clic en ***Eliminar autorización para compartir*** 1.

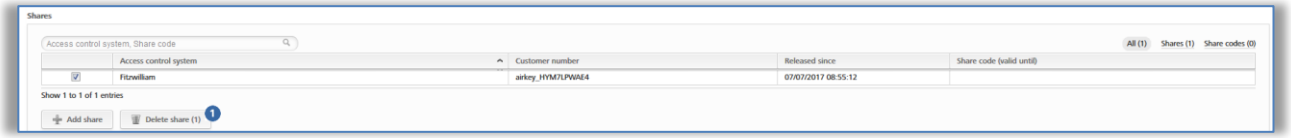


Figura 317: Bloque "Activaciones" – Borrar activación

> Confirme la pregunta de seguridad con ***Eliminar activación***.

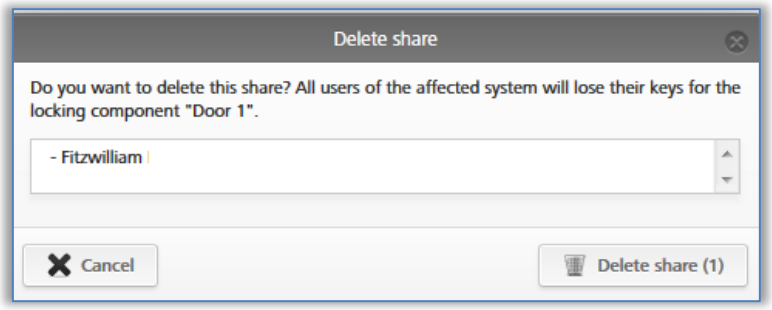


Figura 318: Borrar activación

Así se elimina el componentes de cierre del sistema de control de accesos del otro cliente. Se creará una tarea de mantenimiento.

> Actualice el componentes de cierre para el que ha anulado la activación, mediante un smartphone con autorización de mantenimiento o una estación codificadora opcional. El estado del componentes de cierre vuelve a estar actualizado tras este proceso.

Atención: Cuando se haya actualizado el componentes de cierre, ya no se podrán bloquear más los medios del otro cliente.

Las activaciones de componentes de cierre solo se pueden borrar de sistemas AirKey donde se hayan dado las activaciones.

Si el código de activación no se ha usado aún y se borra como se describe en este capítulo, el componentes de cierre no se debe actualizar.

11.6 Utilizar smartphone en varios sistemas

Puede registrar su smartphone en varios sistemas AirKey y utilizarlo como medio.

> Dentro de la app de AirKey, abra el menú principal y elija ***Ajustes*** → ***Añadir sistema de control de accesos*** ❶.

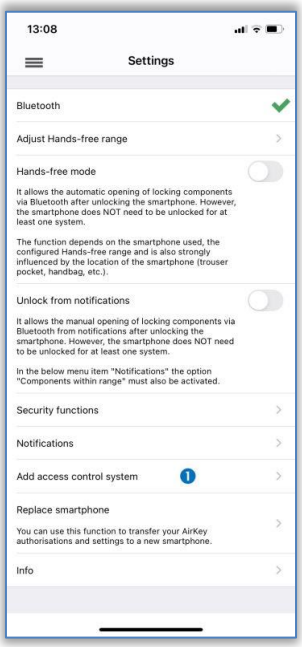


Figura 319: Añadir sistema de control de accesos

> Si se trata de un smartphone con Android, aparecerá automáticamente el cuadro de diálogo para la introducción del código de registro. En el caso de iOS, elija ***Código de registro recibido***, para saltarse el paso de introducir el número de teléfono y pasar a la introducción del código de registro.

> Introduzca el código de registro que ha recibido del administrador del sistema de control de accesos y haga clic en ***Registrar***.

> Si ha activado un código PIN para la app de AirKey, debes introducirlo y confirmarlo.

El smartphone quedará registrado así en el sistema de control de accesos.

Si se ha enviado por SMS un código de registro para otro sistema de control de accesos, bastará con tocar ligeramente el enlace del SMS para iniciar y llevar a cabo automáticamente el registro.

En el smartphone, podrá deslizarse entre las vistas de las autorizaciones de los diferentes sistemas AirKey o la vista general de todas las autorizaciones.

EVVA recomienda usar un PIN. Este ofrece un nivel más de seguridad y se podrá activar o desactivar más adelante. Encontrará más información en Activar PIN.

El botón ***Escanear código QR*** solo es necesario en relación con un reemplazo de smartphone. Encontrará más detalles sobre el reemplazo de smartphone en el capítulo Reemplazo de smartphone.

12 AirKey Cloud Interface (API)

AirKey Cloud Interface es una interfaz (API) para sistemas de terceros basada en REST. La interfaz permite controlar determinadas funciones de AirKey mediante un software de terceros (p. ej., un sistema de reserva o de facturación).

Para ello, el software de terceros debe conectarse con la Administración online de AirKey y adaptarse de forma especial para que envíe las órdenes necesarias y pueda procesar la respuestas resultantes.

Encontrará cómo manejar las funciones posibles y sus órdenes correspondientes en la documentación de la API (en inglés). Su integrador o el programador del software de terceros se ocupará de la implementación.

Experimente cómo funciona AirKey Cloud Interface con la Demo de EVVA AirKey Cloud Interface.

Asegúrese de tener suficiente crédito para emplear AirKey Cloud Interface. En este caso lo mejor es emplear KeyCredits Unlimited. Si se hubiera consumido el crédito o quedara poco, se informará de ello a todos los administradores del sistema de control de accesos AirKey con una notificación de e-mail. Esta notificación de e-mail se enviará únicamente a administradores que hayan activado la opción ***Me gustaría recibir por e-mail (recomendado) información importante de EVVA (p. ej., si tengo pocos KeyCredits)***. Puede editarse la opción de notificación por e-mail en cualquier momento para un administrador (véase el capítulo Editar administrador).

12.1 Activación de AirKey Cloud Interface

Para la activación de AirKey Cloud Interface se requieren como mínimo 350 KeyCredits. Para ello, utilice la cantidad de créditos KeyCredits de la que disponga o emplee la tarjeta para rascar correspondiente **KeyCredits AirKey Cloud Interface**.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales*** en ***Activar API***.

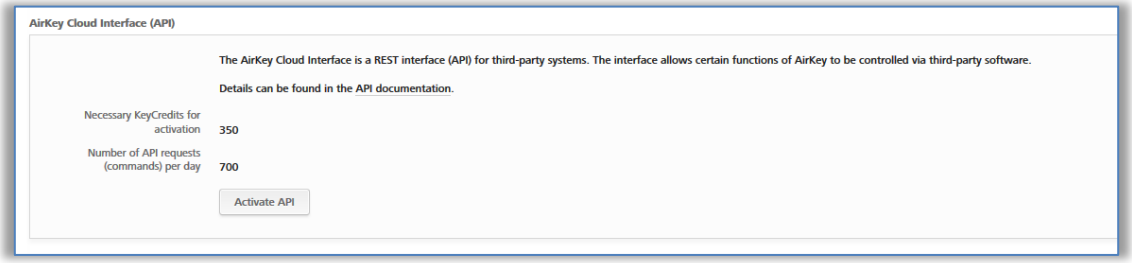


Figura 320: Ajustes generales – AirKey Cloud Interface (API)

> Si tiene suficientes créditos de cantidad, confirme de nuevo el diálogo con ***activar API***. Si el crédito fuera insuficiente, se indicará con una comunicación de advertencia.

Entonces se contará con la posibilidad de cargar más crédito directamente mediante un enlace**.**

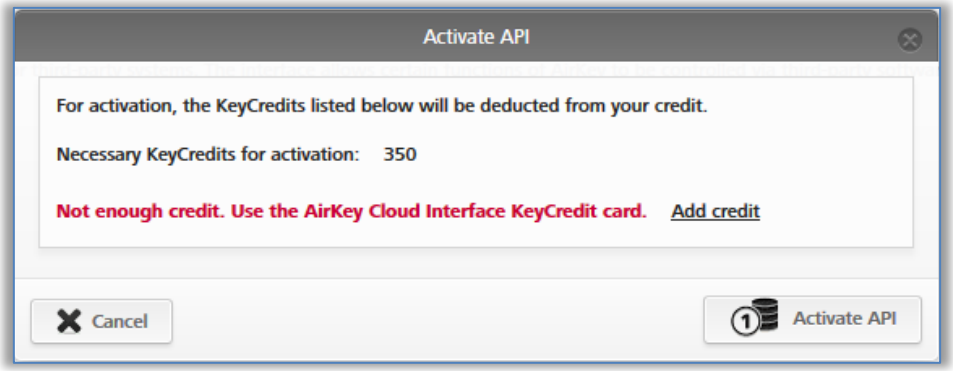


Figura 321: Activación de API

De esta forma se activa AirKey Cloud Interface. AirKey Cloud Interface únicamente debe activarse una vez por sistema de control de accesos para poder emplearse.

Tras la activación recibirá información sobre Endpoint (donde deben enviarse las órdenes de la API) y sobre API-Request-Limit (número de API-Requests que pueden realizarse al día). Se considera una API-Request una orden que se envía mediante software de terceros al sistema AirKey.

El API-Request-Limit se restaura diariamente a las 00:00 h UTC. Si se hubiera superado el API-Request-Limit, se informará de ello a todos los administradores del sistema de control de accesos AirKey con una notificación de e-mail. Esta notificación de e-mail se enviará únicamente a administradores que hayan activado la opción ***Me gustaría recibir por e-mail (recomendado) información importante de EVVA (p. ej., si tengo pocos KeyCredits)***. Puede editarse la opción de notificación por e-mail en cualquier momento para un administrador (véase el capítulo Editar administrador).

So las API-Requests por día no fueran suficientes en su caso, póngase en contacto con el Soporte técnico de EVVA.

12.2 Generar clave de API

La comunicación entre AirKey y el software de terceros se protege con una API-Key. Únicamente quien conozca esta API-Key podrá enviar órdenes a través de AirKey Cloud Interface a su sistema de control de accesos. Cada sistema de control de accesos con AirKey Cloud Interface activada emplea sus propias API-Keys.

Las acciones que se lleven a cabo a través de AirKey Cloud Interface se registrarán igualmente en el historial del sistema del sistema de control de accesos AirKey. Como administrador, en este caso se empleará la primera parte de la API-Key, el API-Key-ID.

Tras la activación puede generar las API-Keys necesarias para la comunicación.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales*** en ***Generar API-Key***.

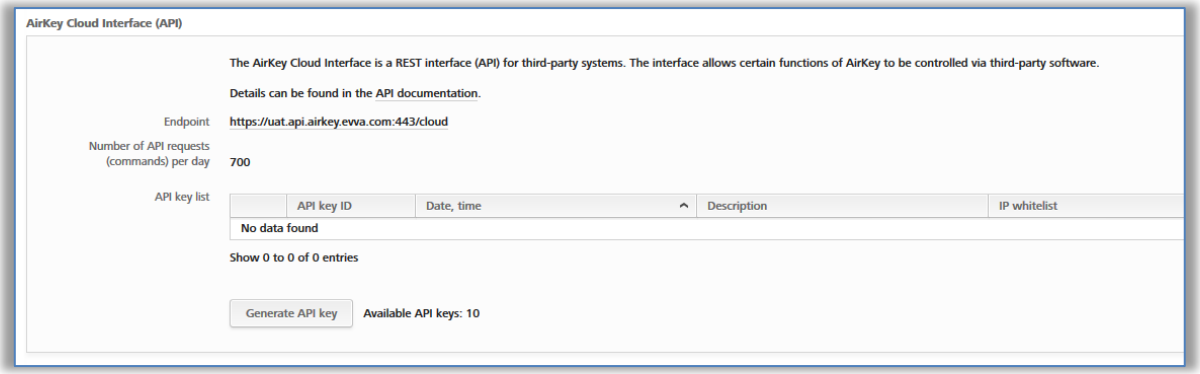


Figura 322: Generación de clave de API

> Confirme de nuevo el diálogo con ***Generar API-Key***.

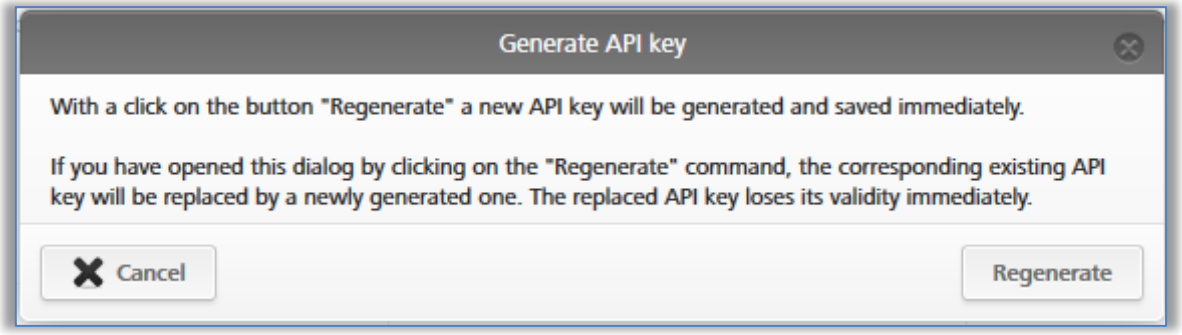


Figura 323: Diálogo de generación de la clave de API

> Adjudique una descripción (por ejemplo, el nombre del software de terceros) y limite, opcionalmente, las direcciones IP autorizadas para enviar API-Requests mediante la IP-Whitelist.

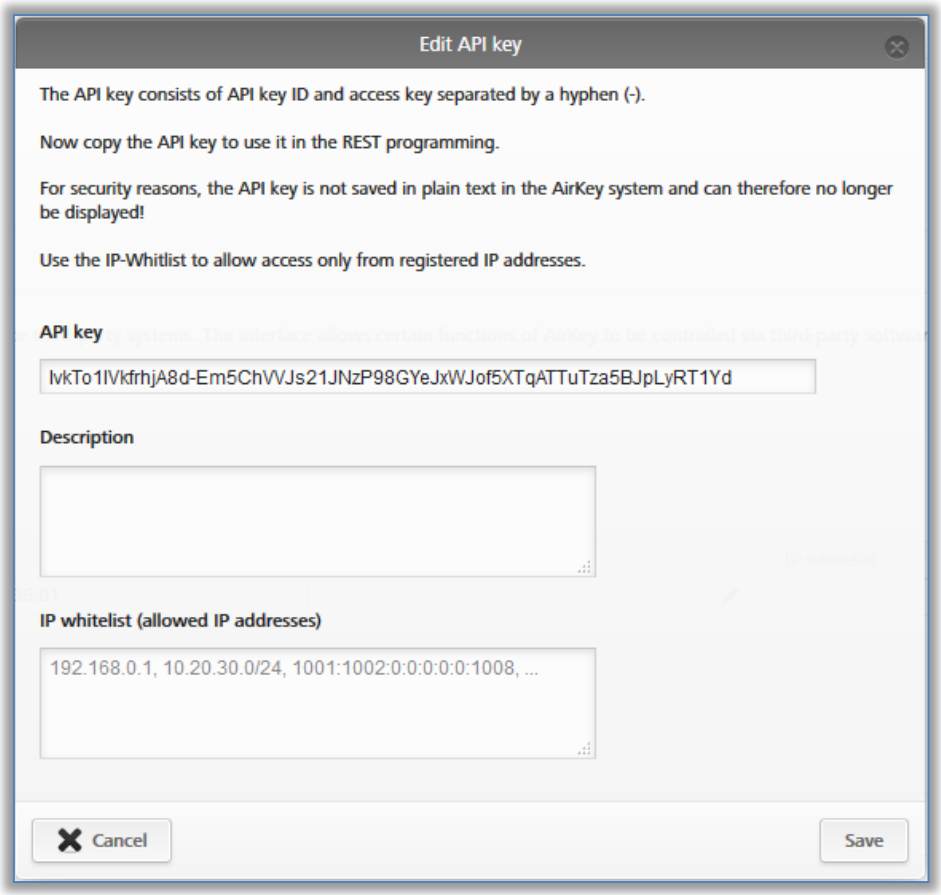


Figura 324: Detalles de la generación de la clave de API

>

Utilice la función de la IP-Whitelist para aumentar la seguridad. Introduzca únicamente aquellas direcciones IP de la API-Key correspondiente autorizada para enviar API-Requests a su sistema de control de accesos AirKey.

En la IP-Whitelist se permiten direcciones IP tanto en formato IPv4 como en IPv6. Emplee como carácter de separación entre varias direcciones IP la coma (,).

Por motivos de seguridad, la API-Key únicamente se mostrará por completo una vez. Guárdela en un lugar seguro o empléela en su software de terceros.

> Guarde los datos introducidos sobre la API-Key haciendo clic en ***Guardar***.

Por cada sistema de control de accesos AirKey pueden generarse hasta 10 API-Keys. Por lo tanto, el sistema de control de accesos AirKey puede controlar más de un software de terceros.

La API-Key generada aparecerá en los ajustes generales, donde puede editarse también posteriormente.

12.3 Editar clave de API

La descripción y la IP-Whitelist de API-Keys existentes pueden editarse posteriormente en ***Ajustes*** en la pestaña ***Aspectos generales*** mediante el símbolo del lápiz. Además están disponibles para cada API-Key las funciones ***Regenerar***, ***Borrar*** y ***Desactivar*** o ***Reactivar***.

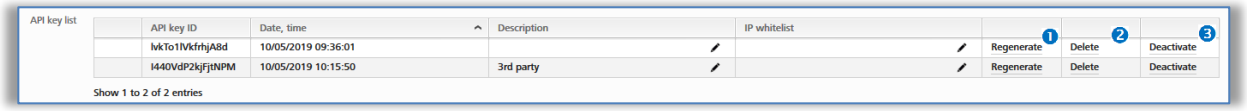


Figura 325: Edición de la clave de API

12.3.1 Regenerar clave de API

Se trata de sustituir una API-Key existente por otra nueva. La API-Key sustituida deja, de esta forma, de ser válida.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales*** en la lista de API-Keys, en ***Regenerar*** ❶.

> Todos los pasos siguientes son idénticos a los de Generar API-Key.

12.3.2 Borrar clave de API

Se trata de eliminar una API-Key existente. Se retirará de la lista de API-Keys y dejará de ser válida. Eliminar API-Keys aumenta el número de API-Keys disponibles en consonancia.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales***, en la lista de API-Keys, en ***Borrar*** ❷.

> Confirme el diálogo con ***Borrar*** para eliminar definitivamente la API-Key.

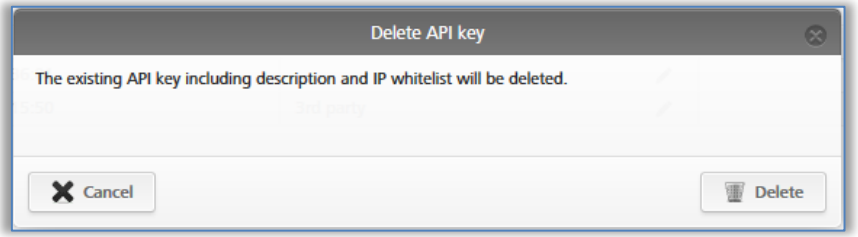


Figura 326: Borrado de clave de API

12.3.3 Desactivación y activación de la API-Key

Se trata de desactivar una API-Key existente activa o volver a activar una API-Key desactivada. Una API-Key desactivada no es válida y no pueden enviarse API-Requests al sistema de control de accesos AirKey. Ni la API-Key ni su descripción ni la IP-Whitelist se modifican con la activación / desactivación.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales,*** en la lista de API-Keys, en ***Desactivar*** ❸ o ***Activar***.

> Confirme el diálogo con ***Desactivar*** o ***Activar*** para concluir el proceso.

Figura 327: Desactivación de la clave de API

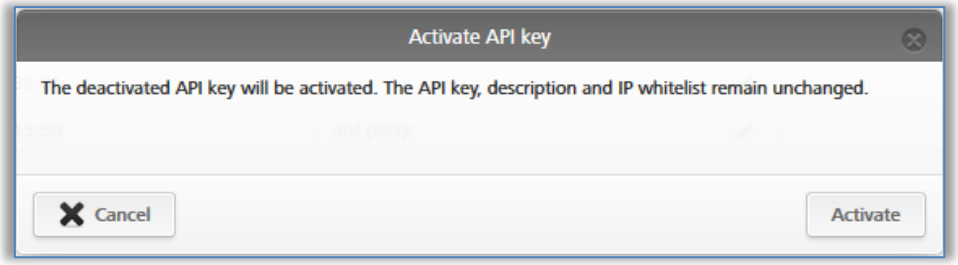


Figura 328: Activación de la clave de API

12.4 AirKey Cloud Interface – entorno de pruebas

El entorno de pruebas le ofrece la posibilidad de probar la AirKey Cloud Interface (API) antes de la activación en un entorno protegido con datos de prueba.

Esto sirve sobre todo como apoyo para los integradores o programadores de sistemas de terceros en el curso de la integración para AirKey Cloud Interface. El entorno de pruebas también está disponible aunque no se haya activado aún AirKey Cloud Interface.

En el entorno de pruebas no se deducen KeyCredits. Tampoco se envía ningún SMS en este caso.

Puede llegarse al entorno de pruebas de AirKey Cloud Interface (API) a través de un "Endpoint" propio (donde deben enviarse las órdenes de la API). Endpoint: https://integration.api.airkey.evva.com:443/cloud

12.4.1 Generar datos de prueba

Para el primer uso del entorno de pruebas es necesario generar primero los datos de prueba.

Para generar los datos de prueba debe generarse antes una API-Key.

> Haga clic en ***Ajustes*** en la pestaña ***Aspectos generales*** en ***Datos de prueba***.

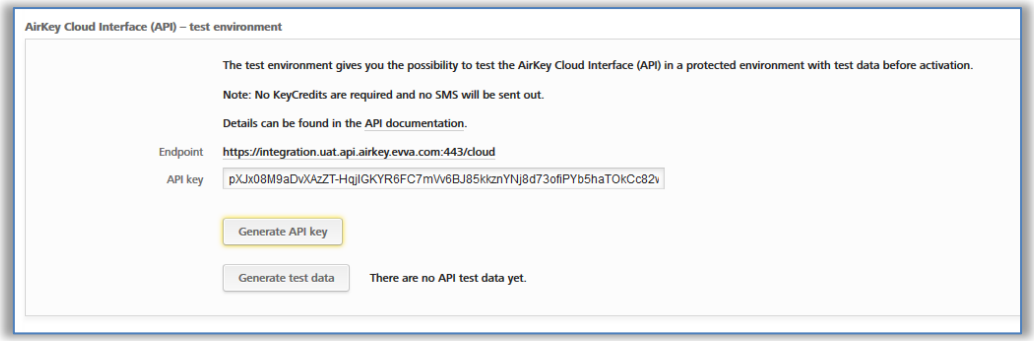


Figura 329: Generación de datos de prueba

De esta forma se generan los datos de prueba. Con los datos de prueba es posible probar cualquier API-Request de la Documentación API. Los datos de prueba solo pueden generarse una vez.

12.4.2 Generar clave de API

También se necesita una API-Key para la comunicación con el entorno de pruebas de AirKey Cloud Interface (API). Sin esta API-Key no pueden enviarse API-Requests al entorno de pruebas. En comparación con la AirKey Cloud Interface auténtica, la API-Key del entorno de pruebas se mostrará en texto sin codificar.

> Haga clic en ***Ajustes***, en la pestaña ***Aspectos generales***, en el área ***AirKey Cloud Interface (API) – entorno de pruebas*** en ***Generar API-Key***.

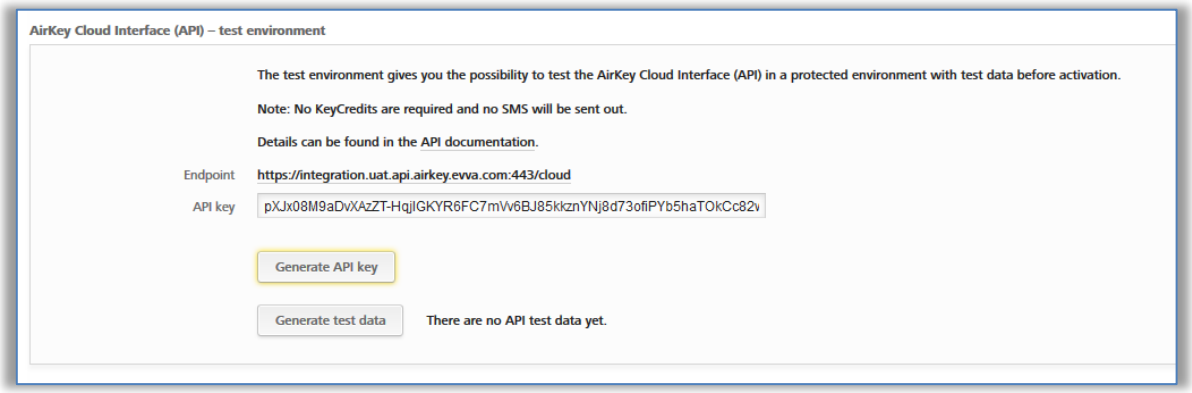


Figura 330: Generación de la clave de API para el entorno de pruebas

Haciendo clic de nuevo en ***Generar API-Key***, se sustituirá la API-Key existente por una nueva. A partir de ese momento, ya no podrá emplearse la API-Key sustituida.

Tras cada inicio de sesión debe generarse de nuevo una API-Key.

12.4.3 Restablecer datos de prueba

Los datos de prueba del entorno de pruebas de AirKey Cloud Interface pueden restaurarse con un clic, volviendo a su estado original. De esta forma pueden realizarse todas las pruebas con datos de prueba uniformes.

> Haga clic en ***Ajustes***, en la pestaña ***Aspectos generales***, en el área ***AirKey Cloud Interface (API) – entorno de pruebas*** en ***Restablecer datos de prueba***.

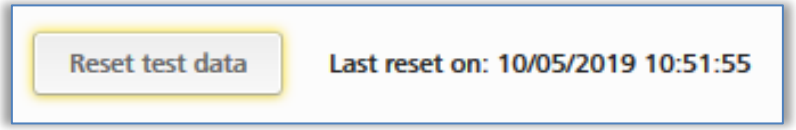


Figura 331: Restauración de los datos de prueba del entorno de pruebas

La restauración de los datos de prueba se confirmará con un mensaje. El momento de la última restauración se muestra en la sección ***AirKey Cloud Interface (API) – entorno de pruebas***.

13 Señalización de los componentes de cierre

Los componentes muestran eventos mediante señales acústicas y ópticas.

Número de señal	Evento	Señal óptica*)	Señal acústica*)	Nota
Señal 1	Proceso de apertura con medio autorizado	●●●●●	mmmmm	
Señal 2	Fin de duración de activación	●●●●●	bbbbb	
Señal 3	Proceso de apertura con medio no autorizado	●●-●●-●●-●●	aa-aa-aa-aa	
Señal 7	Aviso de "pila vacía" (Si se indica en la Administración online de AirKey, en la tabla de los componentes y en los Detalles, un componente con el símbolo "Pila gastada".)	●●--●●--●●--●●	a----a----a----a	Esta señal se emite cuando se introducen pilas vacías en lugar de la señal 8 y con el proceso de apertura antes de la señal 1. 1.000 procesos de apertura o 2 semanas en standby son todavía posibles tras la primera señalización (a temperatura ambiente y uso de una tarjeta, llavero o llave combi).
Señal 8	Inserción de nuevas pilas o reinicio del componente	●●--●●--●●	bb--mm--aa	
Señal 9	Medio sin segmentación de EVVA; medio ajeno al sistema de control de accesos	●●●	ninguna	Ya no se emplea. Con este fin se emplea únicamente la señal 3.
Señal 10	Error de comunicación y hardware de un componentes de cierre	●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--	mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm	Se señaliza, por ejemplo, cuando la conexión entre el pomo y el módulo electrónico de un cilindro no sea correcta.

Número de señal	Evento	Señal óptica*)	Señal acústica*)	Nota
Señal 11	Actualización de firmware de un componentes de cierre	●-●-●-●-●… (período de 1 s, pulso de 12 ms)	ninguna	Duración: hasta que la comunicación finalice
Señal 12	Actualización correcta de un componentes de cierre / medio	●●-●●	aaaaa	
Señal 13	Actualización incorrecta de un componentes de cierre / medio	●●-●●	bbbbb	
Señal 14	Proceso de lectura de un medio de AirKey	●-●-●-●-●-●… (período de 100 ms, pulso de 10 ms)	ninguna	Duración: hasta que la comunicación finalice
Señal 15	Activación y disponibilidad Bluetooth de un cilindro AirKey (p. ej., tras tocarlo)	●-●-●-●-●… (período de 1,5 s)	ninguna	
Señal 16	Inicio de apertura permanente	●●●---●●●	mmm---aaa	
Señal 17	Fin de apertura permanente	●●●---●●●	aaa---mmm	
Señal 18	Modo de emergencia de batería de un cilindro de AirKey	●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●●--●● ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--●-- ●--●--●--●--● ●●--●●--●● ●●--●●--●●--●●	a----a----a----a mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm a----a----a----a mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm bb--mm--aa a----a----a----a	Causa: Una de las pilas se ha colocado incorrectamente o está agotada.

*) Explicaciones sobre las señales:

Señal óptica: amarillo ●, rojo ●, verde ●, azul ●

Señal acústica: a = tono alto, m = tono medio, b = tono bajo

Cada señal corresponde a una duración de 50 ms, las pausas se marcarán con "-".

14 Valores y límites de AirKey

En este capítulo, se resumen las configuraciones máximas por medio y componentes de cierre.

14.1 Administración online de AirKey

El número máximo de componentes de cierre, áreas, personas y medios es ilimitado.

14.2 Componentes de cierre

- Se guardarán las 1.000 últimas entradas de la lista de eventos sin actualización.
- Se pueden gestionar como máximo 1.000 entradas de la lista negra.
- Como máximo se pueden asignar 96 áreas.
- Se puede otorgar un máximo de 250 activaciones a otros clientes.

14.3 Tarjetas, llaveros, pulsares o llaves combi

- Se guardarán 256 entradas de la lista de eventos como máximo sin actualización.
- Se puede otorgar un máximo de 150 autorizaciones a diferentes puertas.
- Se puede otorgar un máximo de 100 autorizaciones para áreas (si se conceden 12 autorizaciones individuales con 8 accesos posibles cada una, se podrán otorgar solo 96 autorizaciones para áreas en total).

14.4 App de AirKey

- Se guardarán 256 entradas de la lista de eventos como máximo sin actualización.
- Número ilimitado de autorizaciones a diferentes puertas y áreas.

15 ¿Cuándo se deducen KeyCredits?

Para el funcionamiento de un sistema de control de accesos, se necesitan KeyCredits para la concesión o modificación de autorizaciones de acceso.

Solo se gastarán KeyCredits en el caso de tener un número limitado de los mismos. Si existe un crédito temporal, se utilizará este y no se tocará el número de KeyCredits previamente existente.

Las continuars acciones requieren el gasto de KeyCredits:

- Para el otorgamiento de nuevas autorizaciones y creaciones posteriores
- Para la modificación de autorizaciones existentes y creaciones posteriores
- Para la reactivación de medios desactivados, siempre que se conserven las autorizaciones del medio desactivado
- Durante el reemplazo de smartphone, si se transfieren autorizaciones al nuevo smartphone.
- Durante la activación de AirKey Cloud Interface (API)

En el caso de nuevas autorizaciones o su modificación, solo se deducirán KeyCredits cuando se cree el medio. Por cada nueva creación, se gastará un KeyCredit. Se pueden otorgar o modificar varias autorizaciones a la vez; solo se deducirá un KeyCredit.

El borrado de autorizaciones, la desactivación o el vaciado de medios no requieren el uso de KeyCredits.

16 Solución de fallos

Con AirKey, ha optado por un sistema de control de accesos de calidad testado de manera exhaustiva. Pero si se encontrase con un error o problema, en este capítulo tiene consejos y trucos para solucionar el fallo.

16.1 No hay comunicación dentro del sistema

Si no puede registrar el smartphone o los componentes de cierre no se pueden actualizar, pruebe los continuars pasos:

- Compruebe que el smartphone tenga una conexión activa a Internet (WiFi o datos móviles) y actívela en caso necesario.
- Compruebe si el puerto 443 está bloqueado en su infraestructura de TI. Este puerto se necesita para la comunicación dentro del sistema de AirKey y debe estar accesible. Véase el capítulo Requisitos del sistema.

16.2 El componentes de cierre no reconoce bien o en absoluto los medios

Cuando los medios en un componentes de cierre no se detectan bien o en absoluto, en comparación con otros componentes de cierre, pruebe los continuars pasos:

- Asegúrese de sostener tranquilamente el medio con la identificación en la unidad de lectura y espere a que el componentes de cierre se señalice en verde. (La señalización azul se refiere solo a la comunicación entre el smartphone y el componentes de cierre.)
- Si el componentes de cierre no responde, revise que la posición del medio sea correcta. La llave combi, por ejemplo, debe sostenerse con el lado donde se ve el símbolo RFID.
- Si sigue sin funcionar, espere 50 segundos sin una identificación en la unidad de lectura para que el componentes de cierre pueda recalibrar el campo eléctrico. Al sostener un objeto metálico junto a la unidad de lectura, se puede realizar la calibración también manualmente.

16.3 Ya no se reconocen los medios

Si un medio determinado no se reconoce más en los componentes de cierre, compruebe los continuars pasos:

- Si se trata de un smartphone, cerciórese de que el NFC o Bluetooth esté activado. Dado el caso, reinicie la conexión NFC o Bluetooth y asegúrese de sostener bien el smartphone junto a la unidad de lectura. Tenga en cuenta que, dependiendo del tipo de smartphone, puede haber diferencias en este punto.
- Si la unidad de lectura del componentes de cierre o de la estación codificadora no reacciona más al medio, sosténgalo unos 10 segundos junto a la unidad de lectura de un componentes de cierre o de una estación codificadora. El medio se repara así solo. Notará que el proceso ha terminado cuando el componentes de cierre o la estación codificadora emitan las señales habituales de nuevo.

16.4 No se puede desenroscar el pomo de un cilindro de AirKey

Si no se puede desenroscar más el pomo de un cilindro de AirKey, estas medidas pueden serle útiles:

- Asegúrese de que, para el desmontaje del pomo, se use la herramienta de montaje para el cilindro de AirKey.
- Los cilindros de AirKey en versión Europerfil presentan una pequeña abertura de servicio en la parte frontal del módulo electrónico a través de la cual se puede fijar el eje del pomo con una clavija metálica adecuada. Aquí recomendamos la herramienta de montaje del set 2.
-
- Pasos a seguir:
- Meta la clavija metálica de la herramienta de montaje del set 2 en la abertura de servicio de la parte frontal del cilindro de Europerfil.
- Gire el pomo sobre su eje hasta que la clavija metálica se pueda introducir a mayor profundidad en la abertura de servicio. Mantenga ahora la clavija metálica en esta posición y desmonte el pomo con la herramienta de montaje de la manera normal.
- Extraiga la clavija metálica tras desmontar el pomo.
- Si no tiene ningún cilindro de AirKey en Europerfil o su cilindro de AirKey está integrado en un herraje o roseta con protección antitaladro, sostenga un medio autorizado en la unidad de lectura para que el cilindro se acople. Durante la duración de la activación (mientras el cilindro esté acoplado), coloque la herramienta de montaje junto al cilindro. En este caso, el cilindro ya no se desacoplará más y el pomo se podrá desmontar de manera sencilla.

16.5 El componentes de cierre señala un "error de hardware"

Si un componentes de cierre señala un error de hardware (véase Señalización de los componentes de cierre), es posible que el pomo o la unidad de lectura no esté conectado al módulo electrónico o la unidad de control correspondiente.

Compruebe los contactos, conectores y conexiones de acuerdo con el manual de montaje.

16.5.1 Cilindro de AirKey

- Tenga cuidado de que la junta de estanqueidad esté correctamente colocada en el eje del cilindro y enrosque de nuevo el pomo en el sentido de las agujas del reloj sobre el cilindro hasta que sienta una resistencia.
- Retire la herramienta de montaje.
- Gire, a continuación, el pomo en sentido contrario a las agujas del reloj hasta que sienta cómo se acopla.
- Preste atención a que el pomo y el módulo electrónico estén correctamente acoplados.

16.5.2 Lector mural de AirKey

> Preste atención a que la unidad de lectura y la unidad de control del lector mural de AirKey estén conectadas correctamente. Dado el caso, compruebe el cableado y las conexiones enchufables.

16.6 El pomo electrónico opera con dificultad

Dependiendo de lo que sobresalga el cilindro sobre un herraje o roseta, puede ocurrir que el cilindro pueda moverse con dificultad por el roce con la junta entre el cuerpo del cilindro y el pomo electrónico. En zonas interiores, se puede extraer la junta en estos casos.

En caso de necesitar más soporte, diríjase a su distribuidor de EVVA (Soporte técnico de EVVA).

17 Notas importantes

17.1 Sistema

Se declara de manera explícita que el presente sistema de AirKey puede ser objeto de registro/autorización de acuerdo con disposiciones legales, en particular con la ley de protección de datos. Por lo tanto, EVVA Sicherheitstechnologie GmbH no asume ninguna responsabilidad por el uso de acuerdo con los requisitos legales.

Para la comunicación en el sistema de AirKey, se utilizan los puertos de Internet 443 y 7070. Compruebe que estos puertos no estén bloqueados. Si utiliza una red móvil de datos, el proveedor de telefonía móvil será el responsable de la administración de los puertos. Si tiene un problema con la red de datos móviles en relación con AirKey, diríjase a su proveedor de telefonía móvil.

Expida autorizaciones con períodos de validez cortos para mantener la seguridad del sistema y evitar aumentar las entradas en la lista negra en caso de pérdida de medios. Solo deberán crearse medios con autorizaciones ilimitadas sin fecha de caducidad para medios de emergencia (por ejemplo: llave para bomberos).

Utilice siempre el sistema con la última configuración para mantener la seguridad del mismo.

Tiene notas sobre la seguridad de los diferentes sistemas en los continuars vínculos:

Cilindro, candado: PDF

Lector mural, unidad de control: PDF

Normas y directivas

CE-conforme | EN 1634: 30 minutos | EN 1634: 90 minutos | Grado de protección IP65 | EN 15684 | apto para cerraduras según EN 179/1125 (cuando se aplica la función antipánico FAP)

SKG | VdS[1]

[1]En preparación

18 Detalles técnicos de la interfaz RS485 para lectores murales Bluetooth

Tras un acceso correcto a un lector mural Bluetooth, se envía un APDU con la entrada de la lista de eventos de dicho acceso desde el lector mural a través de la interfaz RS485.

La entrada de la lista de eventos contiene, entre otros parámetros, la lockingSystemId de 5 bytes del medio (medio de acceso o smartphone) que ha desbloqueado correctamente el lector mural.

Este lockingSystemId (int64) se puede consultar a través de AirKey Cloud Interface (API).Ejemplo: *GET/v1/media?lockingSystemId=000102030405*

Con esta información se pueden llevar a cabo diferentes casos de aplicación, como p. ej.:

- Muestra el nombre de la persona que acaba de desbloquear el lector mural.
- Leer parámetros adicionales; p. ej., del campo «Comentario» de este medio, y uso de esa información para sistemas de terceros.
- Control del ascensor: Por ejemplo, introduzca una cadena JSON mínima en el campo de comentarios de un medio de acceso o smartphone para especificar una planta específica para ese medio, y utilice esta información para el control del ascensor.

18.1 Activar interfaz RS485 para lector mural Bluetooth

Para reenviar la entrada de la lista de eventos en caso de un acceso correcto a través de la interfaz RS485, se debe activar el ajuste correspondiente en el lector mural Bluetooth en la administración online de AirKey.

> En la página de inicio ***Home***, elija la opción ***Lector mural***.
> También puede elegir en el menú principal ***Sistema de control de accesos*** → ***Componentes***.
> Haga clic en el lector mural Bluetooth en el que desea activar la función.
> Cambie a la pestaña ***Ajustes***.
> Marque la casilla de verificación de la ***interfaz RS485*** en la parte inferior.

El lector mural Bluetooth necesita la versión de firmware 5.86 o superior; de lo contrario, se indica que el firmware debe actualizarse para poder utilizar esta función.

18.2 Configuración de la interfaz de serie RS485

Con un adaptador RS485 conectado a la interfaz RS485 del lector mural AirKey, se puede reenviar la entrada de la lista de eventos del último acceso correcto a un sistema de terceros (p. ej., a través de USB o Ethernet).

El adaptador RS485 se conecta en paralelo al cable existente en la unidad de control en el conector para la unidad de lectura.

- Patilla 2 del conector → Doorbus B-
- Patilla 3 del conector → Doorbus A+

Para obtener más información sobre la asignación de conectores, consulte el esquema de la tapa de la unidad de control.

El puerto serie debe configurarse de la siguiente manera:

- Tasa de baudios: 115200
- Bit de datos: 8
- Bit de parada: 1
- Paridad: even
- No CTS flow control

18.3 Especificación de APDU de la entrada de la lista de eventos del acceso correcto

18.3.1 APDU de la entrada de la lista de eventos

APDU Bytes	CLA	INS	P1	P2	LE (data length)	data
Byte	0xCC	0xD6	0xF0	0x00	0x0E	<14 byte event log entry>
Example	0xCC	0xD6	0xF0	0x00	0x0E	0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c

18.3.2 Entrada de la lista de eventos de 14 bytes

Byte	**00**	**01**	**02**	**03**	**04**		**05**	**06**	**07**	**08**		**09**		**10**	**11**	**12**	**13**
Description	**lockingSystemId**						**Timestamp**					**Unlocking status**		**customerID (not used)**			
Example	0e	4e	25	34	f0		32	76	d3	b9		7a		00	00	02	8c

18.3.2.1 Formato de la marca de tiempo

Byte 1									Byte 2									Byte 3									Byte 4								Byte
8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1	Bits
*	*	*	*	*	*																													R1
						*	*		*	*																								R2
											*	*	*	*	*																			R3
																*		*	*	*	*													R4
																						*	*	*	*		*	*						R5
																													*	*	*	*	*	*	R6
																																		Example
0	0	1	1	0	0	1	0		0	1	1	1	0	1	1	0		1	1	0	1	0	0	1	1		1	0	1	1	1	0	0	1	R7

R1 … Año: año menos 2010 (año 2022 = **001100**)
R2 … Maand: ene = **01**, feb = **02**, mar = **03** etc.
R3 … Dag: rango de valores**01**–**31**
R4 … Uur: rango de valores**00**–**23**
R5 … Minuten: rango de valores**00**–**59**
R6 … Seconden: rango de valores**00**–**59**
R7 … Ejemplo: **00110010 01110110 11010011 10111001**corresponde a2022-09-27 13:14:57

18.3.2.2 Estado de desbloqueo

Byte 1									Description
b8	b7	b6	b5	b4	b3	b2	b1		Bit
0									R1
1									R2
	0	0	0						R3
	0	0	1						R4

	0	1	0						**R5**
	0	1	1						**R6**
	1	0	0						**R7**
	1	1	0						**R8**
	1	0	1						**R9**
	1	1	1						**R10**
				•	•	•	•		**R11**
0	1	1	1	1	0	1	0		**R12**

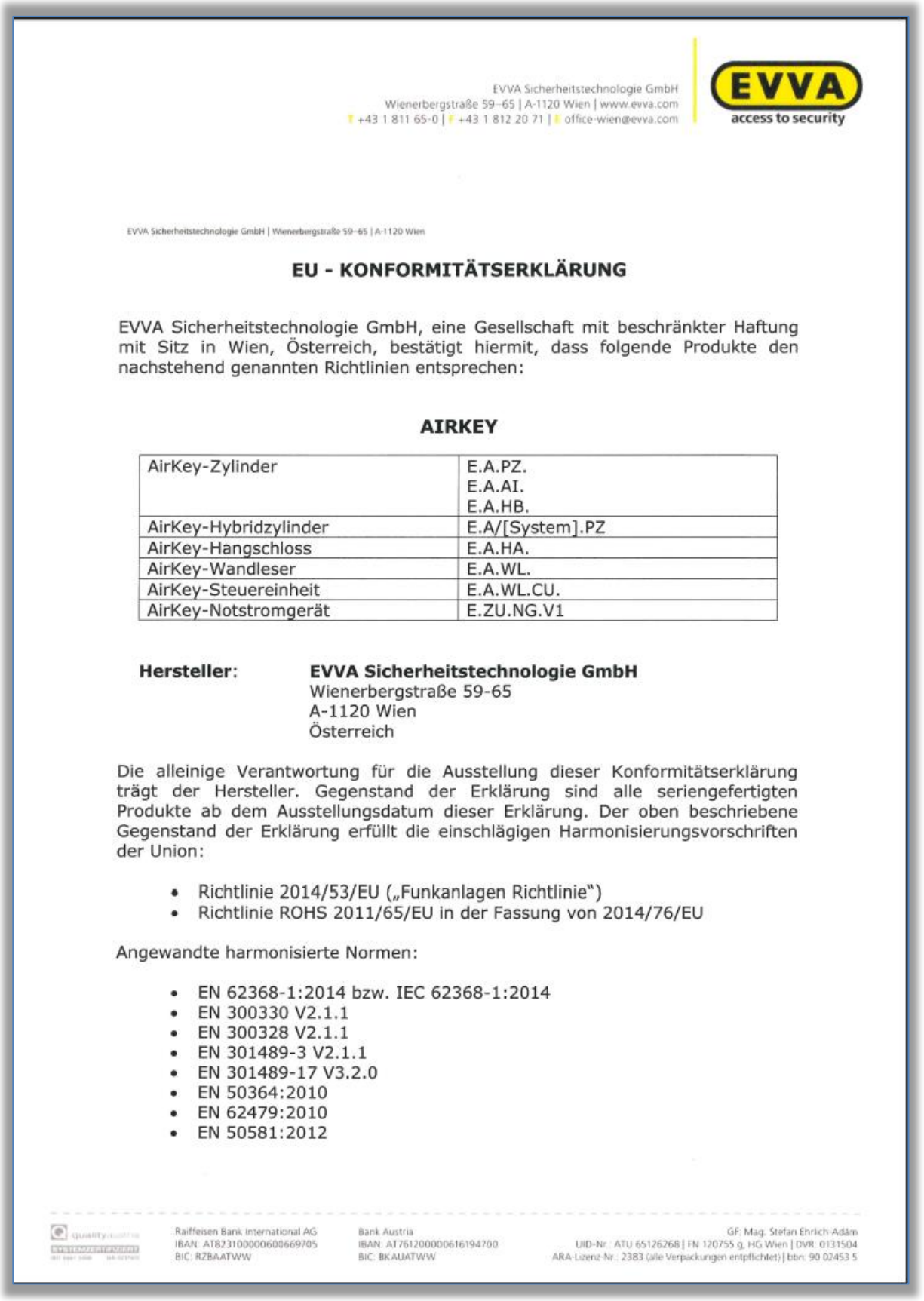
R1 … Hora correcta
R2 … Hora incorrecta. El suministro de corriente no ha estado disponible durante demasiado tiempo.
R3 … Acceso denegado: actualmente se carece de autorización
R4 … Acceso denegado: El medio se encuentra en la lista negra del componente AirKey
R5 … Acceso denegado: Hora incorrecta
R6 … Acceso denegado: Error de firma
R7 …Acceso denegado: Apertura no actual (apertura en otro sistema de control de accesos)
R8 … Acceso denegado: Festivo activo
R9 … Acceso autorizado: Acceso mediante modo Hands-free
R10 … Acceso autorizado
R11 … Estado de las pilas: Para lectores murales Bluetooth siempre 100 %
R12 … Ejemplo: **0x7a** significa hora actual, acceso concedido, estado de la batería 100 %

18.3.3 Ejemplo

- APDU: **CC D6 F0 00 0E 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c**
- Entrada de la lista de eventos: 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c
  - lockingSystemId: **0e 4e 25 34 f0**
  - Timestamp AirKey: **32 76 d3 b9** = 2022-09-27 13:14:57
  - Unlocking status: **7a** = la hora es actual, el acceso está concedido, el estado de la batería es del 100 %
  - customerId: **00 00 02 8c**

La lockingSystemId de los medios de acceso también se puede reenviar a sistemas de terceros a través de la estación codificadora. Para ello, utilice el parámetro «**-notify**» al iniciar la estación codificadora a través de la línea de comandos. Encontrará información más detallada al respecto en el capítulo Utilización de la estación codificadora a través de la línea de comandos.

19 Declaración de conformidad



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

Raiffeisen Bank International AG
IBAN: AT823100000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT761200000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5

Notifizierte Stelle:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Wien
Kennnummer: 0408

Die Komponenten werden mit einer Firmware ausgeliefert, die den bestimmungsgemäßen Betrieb der Funkanlage ermöglichen.

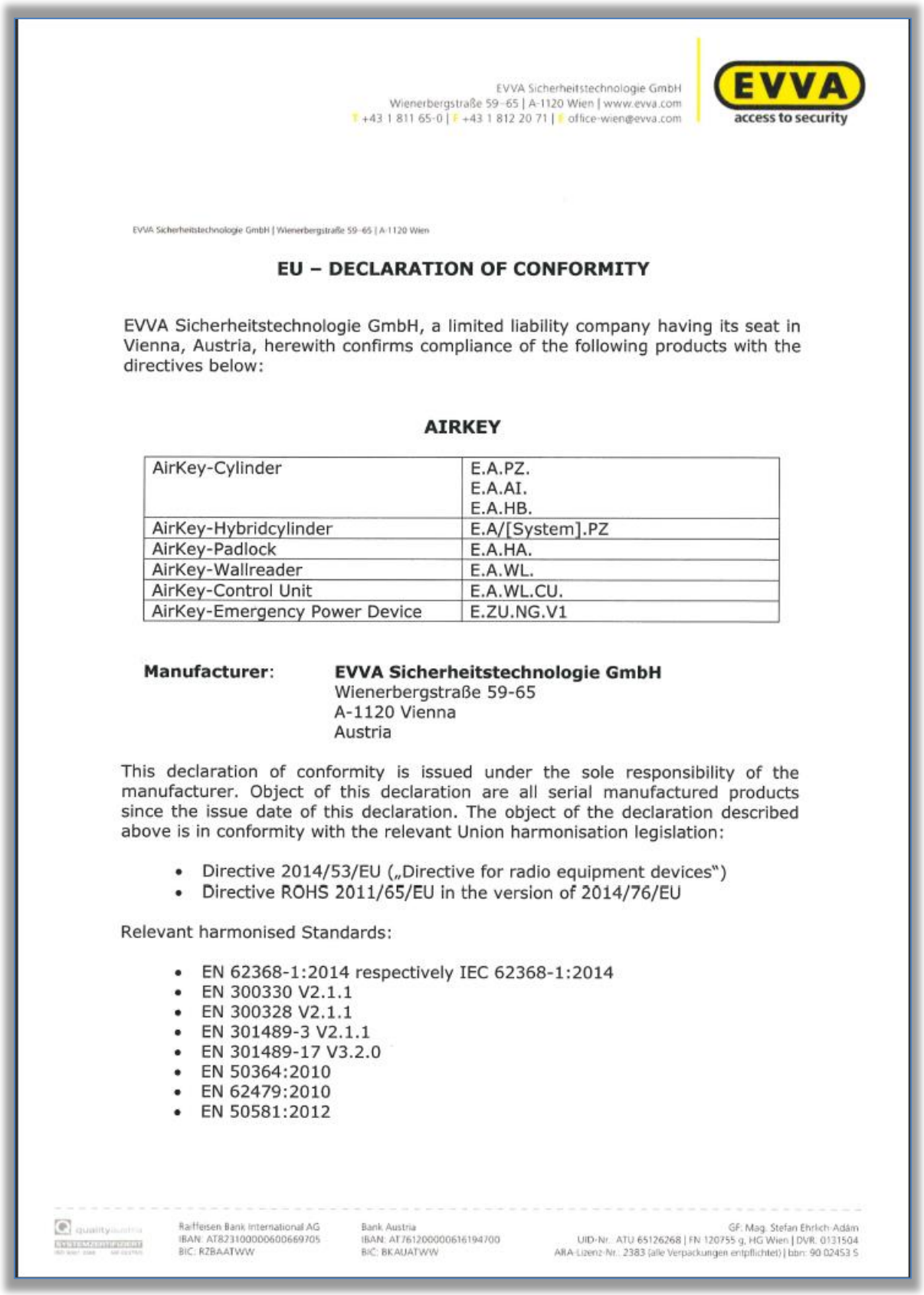
Unterzeichnet für und im Namen von EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Geschäftsführer

Wien, 13.06.2017

EU-Konformitätserklärung_AIRKEY / 2

20 Declaration of Conformity



EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com
T +43 1 811 65-0 | F +43 1 812 20 71 | E office-wien@evva.com

EVVA
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

qualityaustria

Raiffeisen Bank International AG
IBAN: AT823100000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT761200000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5

Notified body:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Vienna
Number: 0408

The components are delivered with a firmware which allows the radio equipment to operate as intended.

Signed for and on behalf of EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Managing Director

Vienna, 13.06.2017

EU-Declaration of Conformity_AIRKEY / 2

21 Índice de ilustraciones

22 Glosario

En lo referente a AirKey se utilizan, entre otros, los continuars términos:

Denominación	Función
Cliente	Propietario del sistema de control de accesos con un número de cliente único.
Administrador	Es un rol de usuario del sistema de AirKey autorizado para ejecutar todas las actividades administrativas en la Administración online de AirKey Se pueden asignar varios administradores para un mismo cliente. Se debe definir, como mínimo, un administrador para cada sistema de control de accesos.
Persona	Usuarios que utilizan medios. Se asignarán los medios con autorizaciones de acceso para las áreas y componentes de acceso a las personas.
Medios	Son smartphones o medios de acceso que se pueden añadir a sistemas de control de accesos AirKey para tener acceso a componentes de cierre AirKey autorizados.
Medios de acceso	Son medios NFC pasivos (sin fuente de alimentación propia) que se pueden emplear junto con smartphones en sistemas de control de accesos AirKey. Son, por ejemplo, tarjetas, llaveros, llaves combi, pulseras etc.
Medio de origen	Este término se utiliza en relación con las funciones «Reemplazo de smartphone» y «Duplicar medio». Describe el smartphone o medio de acceso desde el que se inició el reemplazo o la duplicación. En caso de reemplazo de smartphone, el medio de origen describe el smartphone «antiguo» que debe sustituirse por uno nuevo.
Medio de destino	Este término se utiliza en relación con las funciones «Reemplazo de smartphone» y «Duplicar medio». Describe el smartphone o medio de acceso al que se deben transferir las autorizaciones y los ajustes de AirKey. En caso de reemplazo de smartphone, el medio de destino describe el «nuevo» smartphone que debe sustituir a otro smartphone.
Componentes de cierre	Son cilindros (de las más diversas formas), candados y lectores murales de AirKey que pueden abrir y cerrar puertas en un sistema de control de accesos AirKey.
Área	Es una unidad administrativa de la Administración online de AirKey que incluye diversos componentes de cierre. Las áreas facilitan la administración del sistema de control de accesos AirKey y la adjudicación de autorizaciones para componentes de cierre.

KeyCredits	Describe un crédito dentro de un sistema de control de accesos AirKey. Se requiere crédito para conceder nuevas autorizaciones, modificar las existentes o activar otras funcionalidades de AirKey.
AirKey Cloud Interface	AirKey Cloud Interface es una interfaz (API) para sistemas de terceros basada en REST. La interfaz permite controlar determinadas funciones de AirKey mediante un software de terceros.
Interfaz RS485	La interfaz RS485 es una interfaz estandarizada que se puede utilizar para la transferencia de datos. En el caso de un lector mural de AirKey, a través de esta interfaz se puede transferir el último acceso correcto a un software de terceros.
APDU	APDU son las siglas de Application Protocol Data Unit (Unidad de datos de protocolo de aplicación) y se utiliza aquí para la interfaz RS485. Describe un paquete de datos transmitido a través de la interfaz RS485.
"Send a Key"	Describe una función de la Administración online de AirKey. Permite a un administrador crear nuevos smartphones y conceder nuevas autorizaciones rápidamente, así como editar las autorizaciones de Smartphonesya existentes. El propietario del smartphone recibe un SMS mediante el que se registra automáticamente el smartphone para AirKey.
Autenticación de dos factores	La autenticación de dos factores (conocida también como 2FA) sirve de nivel de seguridad adicional durante el login en la Administración online de AirKey. Para ello, en el login se pide, además del identificador del usuario y la contraseña, un código SMS adicional como segundo factor.
Función de verificación por dos personas	Describe un proceso en el que únicamente se puede realizar una acción con una persona adicional. En AirKey, este principio se puede utilizar para proteger los datos personales en las listas de eventos.
Firmware	Programa de software que funciona en componentes de cierre para que estos puedan ejercer su función AirKey. El firmware de los componentes de cierre puede actualizarse mediante Firmware-Updates.
Keyring	En AirKey, "Keyring" es el nombre de un programa de software que administra todos los datos relevantes de AirKey almacenados en los medios de acceso pasivos como tarjetas, llaveros, llaves combi y pulseras. En el caso de que esté disponible una nueva versión de Keyring en el sistema AirKey, pueden actualizarse los medios con un smartphone con autorización de mantenimiento o con una estación codificadora.
Tareas de mantenimiento	Se indican en la Administración online de AirKey para los componentes de cierre que no estén actualizados. Únicamente cuanto se han realizado todas las tareas de mantenimiento de un sistema de control de accesos AirKey puede considerarse que la instalación es segura y está actualizada.

Modo de mantenimiento	Solo cuando un smartphone cuenta con la autorización de mantenimiento para el sistema de control de accesos, se pueden añadir o eliminar con él componentes (medios y componentes de cierre) en el sistema de control de accesos. Con un smartphone que tenga autorización de mantenimiento, el técnico de mantenimiento de AirKey también puede operar componentes de cierre incluso en estado de fábrica. La autorización de mantenimiento se puede activar en la Administración online de AirKey para los smartphones que quiera.

23 Aviso legal

7ª edición, noviembre de 2022

La publicación de un nuevo manual de sistema anula la validez de esta edición.
Podrá descargar la última versión del manual de sistema en nuestra página web:
https://www.evva.com/es/airkey/systemmanual/.

Es posible que este manual contenga defectos técnicos de impresión o errores tipográficos. El contenido de este manual de sistema se revisa regularmente y se realizan las correcciones oportunas. La empresa no será responsable de los errores técnicos o de impresión ni de sus consecuencias.

Podrán realizarse cambios sin previo aviso debido a mejoras técnicas.

Aviso legal

Editor
EVVA Sicherheitstechnologie GmbH

Responsable del contenido
EVVA Sicherheitstechnologie GmbH

Contenido técnico
Florian Diener, Johannes Ullmann

Asesores técnicos
Raphael Fasching, Iulian Stanciulescu, Martin Bauer