

AirKey

Manual do sistema 2.7

1 Índice

2	Introdução, visão geral	9
2.1	Informações de foro legal	9
2.2	Assistência da EVVA.....	10
2.3	Esclarecimento dos símbolos	11
2.4	Sugestões para uma navegação ideal neste documento	11
3	Arquitetura do sistema	12
3.1	Componentes de bloqueio	13
3.1.1	Cilindro AirKey	13
3.1.2	Cilindro híbrido AirKey.....	14
3.1.3	Cilindro de patilha AirKey	14
3.1.4	Cadeado AirKey.....	15
3.1.5	Leitor de parede AirKey	15
3.2	Aplicação AirKey	16
3.3	Smartphones	16
3.4	Meios AirKey	17
3.5	Administração online do AirKey	18
3.5.1	Pré-requisitos do sistema	18
3.6	KeyCredits da EVVA	18
3.7	Estação de codificação.....	18
3.8	Alimentação de emergência	19
4	Primeira utilização	20
4.1	Instalar a aplicação AirKey	20
4.2	Registo na Administração online do AirKey	20
4.3	Iniciar sessão	23
4.4	Ajuda interativa.....	24
4.5	Instalar a estação de codificação	24
4.5.1	Utilizar a estação de codificação através da Administração online do AirKey ...	25
4.5.2	Utilizar a estação de codificação através da linha de comando	27
4.5.3	Definições da aplicação da estação de codificação	28
4.5.4	Soluções para possíveis problemas com a estação de codificação	29
4.6	Adicionar crédito.....	32
4.7	Criar pessoa.....	34
4.7.1	Importar dados de pessoas	35
4.8	Criar smartphone.....	42

4.9	Registrar smartphone	44
4.9.1	Função "Send a Key"	46
4.10	Instalar os componentes de bloqueio	50
4.10.1	Cilindro AirKey	50
4.10.2	Leitor de parede AirKey	50
4.11	Adicionar componente de bloqueio	51
4.11.1	Adicionar componentes de bloqueio com o smartphone	51
4.11.2	Adicionar componente de bloqueio com a estação de codificação	54
4.12	Adicionar cartões, porta-chaves, pulseiras e chaves combinadas com o smartphone	57
4.13	Atribuir uma pessoa a um meio	59
4.14	Atribuir autorizações	60
4.14.1	Acesso permanente	61
4.14.2	Acesso periódico	62
4.14.3	Acesso temporário	64
4.14.4	Acesso individual	64
4.15	Criar autorização	65
5	Administração Online do AirKey	67
5.1	Login no AirKey	67
5.1.1	Login no AirKey sem a autenticação de dois fatores	67
5.1.2	Login no AirKey com a autenticação de dois fatores	68
5.1.3	Esqueceu-se da sua senha	69
5.2	Logout do AirKey	72
5.3	Administradores	72
5.3.1	Criar administrador	73
5.3.2	Editar administrador	75
5.3.3	Eliminar administrador	77
5.4	Definições do sistema de controlo de acessos AirKey	78
5.4.1	Informações gerais	78
5.4.2	Valores por defeito (para todos os componentes de bloqueio adicionados como novos)	85
5.4.3	Dias de férias/feriados	90
5.5	Sistema de controlo de acessos	92
5.5.1	Vista geral dos componentes de bloqueio	93
5.5.2	Adicionar componente de bloqueio: ver o capítulo 4.11	93
5.5.3	Editar componente de bloqueio	93
5.5.4	Remover o componente de bloqueio	96

5.5.5	Áreas	97
5.5.6	Criar área	98
5.5.7	Atribuir componente de bloqueio a áreas	99
5.5.8	Cancelar a atribuição de componentes de bloqueio a uma área	100
5.5.9	Eliminar área	101
5.5.10	Vista geral das autorizações	102
5.5.11	Tarefas de manutenção	103
5.5.12	Dados de cliente – plano de bloqueio	105
5.6	Meios e pessoas	107
5.6.1	Vista geral das pessoas	107
5.6.2	Criar pessoa: ver o capítulo 4.7	107
5.6.3	Editar pessoa	107
5.6.4	Eliminar pessoa	109
5.6.5	Atribuir meio a uma pessoa	110
5.6.6	Vista geral dos meios	111
5.6.7	Adicionar meio	112
5.6.8	Criar smartphone: ver o capítulo 4.8	113
5.6.9	Criar cartão, porta-chaves, pulseiras ou chave combinada	113
5.6.10	Editar meio	113
5.6.11	Atribuir uma pessoa a um meio: ver o capítulo 4.13	114
5.6.12	Autorizações	114
5.6.13	Atribuir autorizações: ver o capítulo 4.14	115
5.6.14	Criar autorização: ver o capítulo 4.16	115
5.6.15	Alterar autorização	115
5.6.16	Apagar autorização	116
5.6.17	Desativar meio	118
5.6.18	Remover o meio desativado	119
5.6.19	Reativar meio	120
5.6.20	Troca de smartphone	122
5.6.21	Duplicar meio	122
5.6.22	Esvaziar meio	123
5.6.23	Cancelar atribuição	123
5.6.24	Remover meio	127
5.7	Protocolos	128
5.7.1	Protocolo de componentes de bloqueio	129
5.7.2	Protocolo dos meios	131

5.7.3	Protocolo do sistema	135
5.8	Ativações de apoio	136
5.8.1	Criar ativação de apoio	136
5.8.2	Bloquear login de apoio	137
5.9	Ajuda	138
6	Aplicação AirKey	139
6.1	Componentes Bluetooth	139
6.2	Registar smartphone: ver o capítulo 4.9	139
6.3	Autorizações	139
6.4	Tarefas de manutenção: ver o capítulo 6.12	141
6.5	Abertura permanente	141
6.6	Introduzir PIN	142
6.7	Codificar meios	142
6.8	Protocolo de autorização	143
6.9	Definições da aplicação AirKey	144
6.9.1	Definições da aplicação AirKey em smartphones Android	144
6.9.2	Definições da aplicação AirKey em iPhones	144
6.9.3	Definir o alcance do modo hands-free	145
6.9.4	Modo Hands-free (mãos livres)	146
6.9.5	Desbloqueios a partir de notificações	146
6.9.6	Funções de segurança	147
6.9.6.1	Ativar PIN	148
6.9.6.2	Alterar PIN	149
6.9.6.3	Desativar PIN	150
6.9.7	Notificações	151
6.9.8	Adicionar sistema de controlo de acessos	153
6.9.9	Troca de smartphone	153
6.9.10	Info	153
6.10	Atualizar o smartphone	154
6.11	Conecte com o componente	155
6.12	Autorização especial "autorização de manutenção"	156
6.13	Adicionar um componente AirKey	158
6.13.1	Adicionar meios: ver o capítulo 4.12	159
6.13.2	Adicionar componente de bloqueio: ver o capítulo 4.11	159
6.14	Remover um componente AirKey	159
6.15	Dados protocolares da aplicação AirKey	161

6.16	Vista geral da função Hands-free (mãos livres).....	162
7	Utilização dos componentes de bloqueio AirKey	165
7.1	Acesso com o smartphone	165
7.2	Acesso com meios como cartões, porta-chaves, pulseiras ou chaves combinadas	166
8	Operação e manutenção do sistema AirKey	167
8.1	Atualizar componentes de bloqueio	167
8.2	Atualizar o smartphone: ver o capítulo 6.10	169
8.3	Atualizar meios	169
8.4	Atualizar firmware de componentes de bloqueio	172
8.5	Atualizar a versão de meios Keyring.....	177
8.6	Atualizar a versão da aplicação do smartphone.....	181
8.7	Substituição das pilhas e alimentação de emergência	182
8.7.1	Substituição das pilhas no cilindro AirKey	182
8.8	Opções de reparação.....	184
8.8.1	Emitir e instalar componentes de bloqueio de substituição	184
8.8.2	Desinstalar o componente de bloqueio sem ser substituído e marcá-lo como "com defeito"	188
8.8.3	Desinstalar o componente de bloqueio através do smartphone	191
8.8.4	Desinstalar o componente de bloqueio através da Administração online do AirKey	192
8.8.5	Reverter tarefas de manutenção para opções de reparação.....	193
9	Meios de emergência.....	194
9.1	Emitir meios de emergência	194
10	Media replacement.....	195
10.1	Troca de smartphone	195
10.1.1	Iniciar a troca como proprietário do smartphone.....	195
10.1.2	Iniciar a troca como administrador.....	198
11	Trabalhar com vários sistemas de bloqueio AirKey	201
11.1	Ativar componentes de bloqueio para outros sistemas de bloqueio.....	201
11.2	Adicionar componente de bloqueio de outros sistemas de bloqueio	202
11.3	Atribuir autorizações a componentes de bloqueio ativados para partilha	205
11.4	Consultar autorizações de componentes de bloqueio ativados para partilha.....	206
11.5	Cancelar a partilha de um componente de bloqueio.....	206
11.6	Utilizar o smartphone em vários sistemas	207
12	AirKey Cloud Interface (API)	209
12.1	Ativação da AirKey Cloud Interface	209
12.2	Gerar chave para a API	210

12.3	Editar chave da API	213
12.3.1	Regenerar chave da API	213
12.3.2	Eliminar chave da API	213
12.3.3	Desativar e ativar chave da API.....	213
12.4	AirKey Cloud Interface – Ambiente de teste	214
12.4.1	Gerar dados de teste	214
12.4.2	Gerar chave para a API	215
12.4.3	Repor dados de teste	216
13	Sinalização dos componentes de bloqueio	217
14	Valores e limites do AirKey.....	219
14.1	Administração Online do AirKey	219
14.2	Componentes de bloqueio AirKey	219
14.3	Cartões, porta-chaves, pulseiras ou chaves combinadas	219
14.4	Aplicação AirKey	219
15	Quando são debitados os KeyCredits?	220
16	Resolução de problemas	221
16.1	A comunicação não é possível no sistema	221
16.2	O componente de bloqueio tem dificuldades em reconhecer o meio ou não reconhece mesmo	221
16.3	Os meios já não são reconhecidos	221
16.4	Não é possível desenroscar o puxador de um cilindro AirKey	222
16.5	O componente de bloqueio sinaliza um "Erro de hardware"	222
16.5.1	Cilindro AirKey	223
16.5.2	Leitor de parede AirKey	223
16.6	O puxador eletrónico está perro	223
17	Indicações importantes.....	224
17.1	Sistema.....	224
18	Detalhes técnicos da interface RS485 para leitores de parede com Bluetooth	225
18.1	Ativar interface RS485 para leitor de parede com Bluetooth	225
18.2	Configuração da porta de série RS485.....	226
18.3	Especificação APDU do registo protocolar do acesso bem-sucedido	227
18.3.1	APDU do registo protocolar	227
18.3.2	Registo protocolar de 14 bytes	227
18.3.2.1	Formato Timestamp.....	227
18.3.2.2	Unlocking status (Estado de desbloqueio)	227
18.3.3	Exemplo.....	228
19	Declaração de conformidade	229

20	Declaration of Conformity	231
21	Índice das figuras	233
22	Glossário	241
23	Ficha técnica	244

2 Introdução, visão geral

O presente manual do sistema AirKey contém informações sobre a instalação, funcionamento e utilização do sistema de controlo de acessos eletrónico AirKey, o qual inclui uma Administração online do AirKey, uma aplicação, cilindros, leitores de parede, cadeado e meios para instalação do AirKey.

Os produtos e o software do utilizador para Administração online do AirKey descritos no manual do sistema apenas podem ser operados por pessoal qualificado para a respetiva posição de trabalho. O pessoal qualificado, graças ao seu know-how, está habilitado a manipular estes produtos / sistemas, a reconhecer riscos e a evitar possíveis situações de perigo.

2.1 Informações de foro legal

- > A EVVA celebra o contrato de utilização de AirKey apenas com base nos seus [Termos e condições gerais de negócios](#), bem como nas suas [Condições gerais de licenciamento](#) a respeito do software do produto.
- > O comprador é expressamente informado de que o uso do sistema de controlo de acessos concedido ao abrigo deste contrato pode acionar obrigações legais, em especial a autorização legal de proteção de dados, identificação e registo obrigatório (p. ex., sistema de informação comum), assim como direitos de codeterminação dos funcionários, no caso de utilização na empresa. O comprador ou cliente e o utilizador final são responsáveis pela utilização correta do produto.
- > De acordo com o definido pela legislação relativa à responsabilidade de produto no âmbito da responsabilidade do fabricante pelos seus produtos, as informações supra devem ser tidas em consideração e ser encaminhadas para a entidade exploradora e utilizador. O não cumprimento isenta a EVVA de toda a responsabilidade.
- > Não adequado em ambientes com crianças com idade inferior a 36 meses, devido ao risco de asfixia por ingestão de peças pequenas.
- > Uma utilização não adequada em relação ao estipulado contratualmente, ou incomum, modificações ou trabalhos de reparação que não possuam uma autorização expressa da EVVA, bem como o uso de uma assistência não qualificada podem levar a falhas no funcionamento, pelo que deverá abster-se de o fazer. Quaisquer alterações que não possuam uma autorização expressa da EVVA incorrem na perda do direito à reivindicação da responsabilidade, garantia ou requisitos acordados em separado.
- > Arquitetos ou instituições de consultoria são obrigados a obter todas as informações necessárias relativas ao produto da EVVA, para atender os deveres de informação e de instrução de acordo com a Lei de Responsabilidade de Produto. Os vendedores e os revendedores têm de ter em consideração as indicações incluídas na documentação da EVVA e eventualmente transmiti-las aos seus clientes.
- > Durante o planeamento e a instalação do componente de bloqueio, considere os respetivos requisitos internacionais e específicos do país incluídos na legislação, regulamentos, normas e diretivas aplicáveis, em especial com respeito aos requisitos relativos aos caminhos de evacuação e saídas de emergência.

2.2 Assistência da EVVA

Com AirKey, tem à sua disposição um sistema de controlo de acessos sofisticado e testado. Caso, todavia, ainda precise de apoio, queira entrar em contacto com um parceiro da EVVA perto de si.

Poderá encontrar uma lista com os parceiros da EVVA certificados na nossa homepage em <https://www.evva.com/int-en/aboutus/contact/international/>.

Caso seleccione a opção de filtro "Parceiro eletrónico", procure parceiros EVVA filtrando de forma orientada, portanto, parceiros que comercializem o sistema de controlo de acessos eletrónico EVVA e que possuam um conhecimento qualificado nesta área.

Para colocar determinadas questões à assistência, utilize o formulário online da EVVA preparado para esse fim. O formulário online, neste momento, está ao seu dispor para as seguintes situações:

- > Excedido o número máximo de códigos de crédito errados.
- > Não é possível carregar créditos.
- > Página de login da Administração online do AirKey não está acessível.
- > Não é possível fazer o login. Esquecimento da identificação do utilizador e/ou endereço de e-mail.
- > Identificação por dois fatores.

Poderá encontrar o formulário online através do link seguinte:

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

Poderá obter informações gerais sobre o AirKey na nossa homepage em

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

2.3 Esclarecimento dos símbolos

Desta forma, são ilustradas, neste manual, sequências de comandos, comandos individuais e botões.

Exemplo: Menu principal **Meios e Pessoas** → **Criar pessoa** ou botões como, p. ex., **Guardar**.



Atenção, perigo de danos, caso as medidas de precaução não sejam respeitadas.



Indicações e informações adicionais



Sugestões e recomendações



Mensagens de erro

Option

Opções

2.4 Sugestões para uma navegação ideal neste documento

Neste documento, existem também muitas hiperligações que remetem para outros capítulos ou textos. A forma mais rápida e cómoda de regressar à posição original no Windows ou avançar é utilizando estas **combinações de teclas**:



(Alt + seta do cursor para a esquerda) = retroceder na navegação



(Alt + seta do cursor para a direita) = avançar na navegação

Estas combinações de teclas funcionam em muitos visualizadores de PDF e, por exemplo, no Microsoft Word.

Para experimentar as combinações de teclas, clique neste [link](#) e retroceda na navegação com .

3 Arquitetura do sistema

Na figura seguinte, poderá ter uma visão global dos componentes que compõem o AirKey e dos seus caminhos de comunicação. Cada componente está descrito de forma interligada.

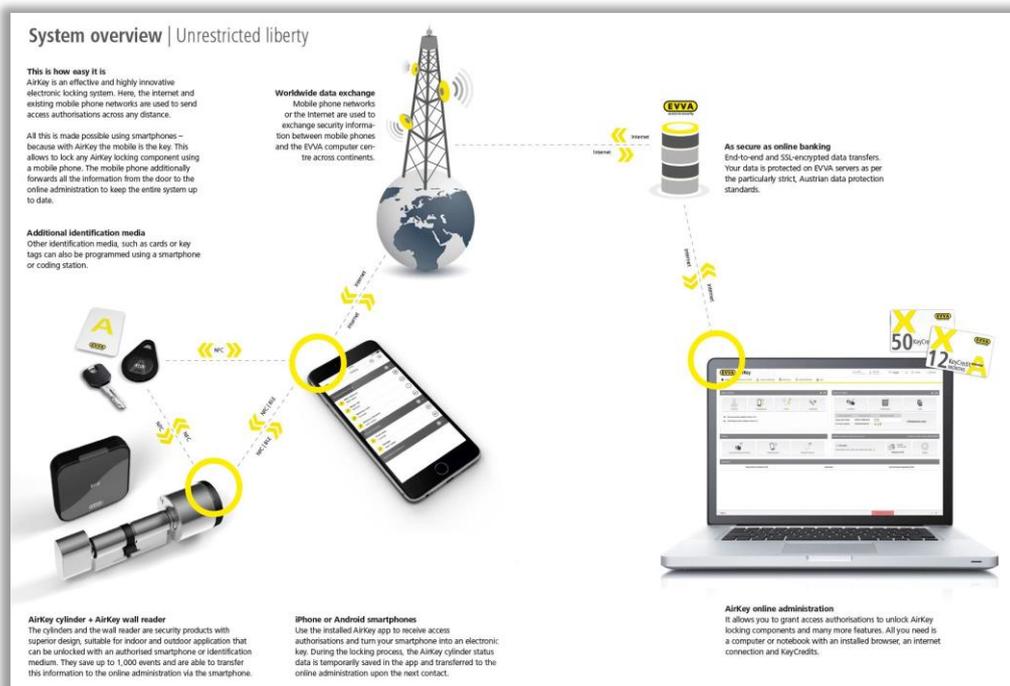


Figura 1: Arquitetura do sistema



Todos os dados transmitidos são "End-to-End", estão protegidos com criptografia de acordo com os padrões atuais de criptografia, desde o centro de dados da EVVA até ao componente de bloqueio.

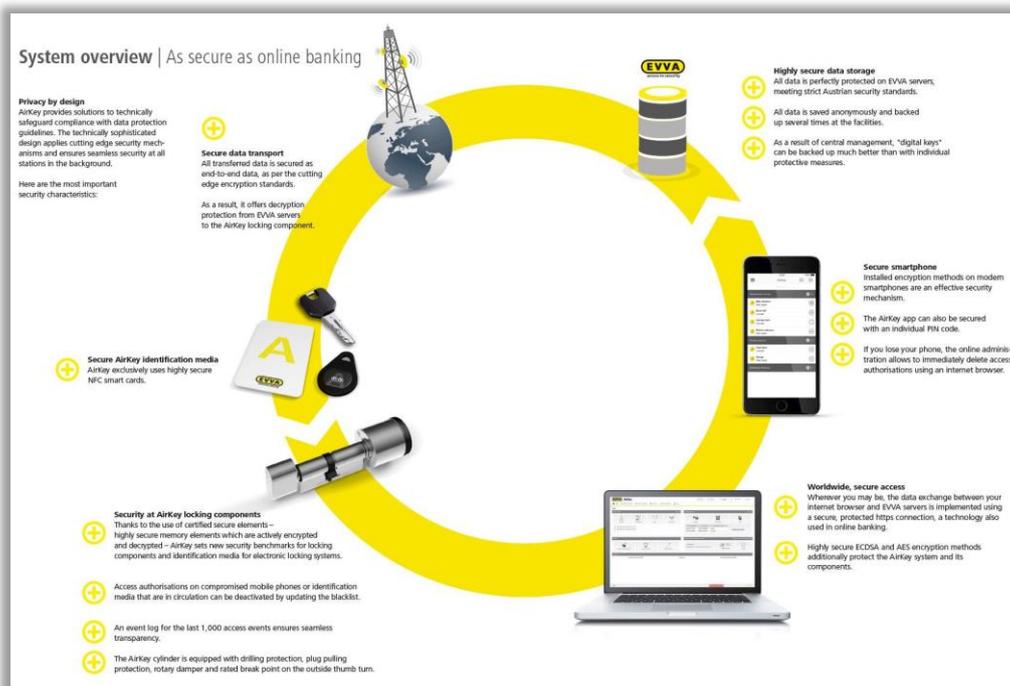


Figura 2: Vista geral do sistema – Segurança sem lacunas

3.1 Componentes de bloqueio

Os componentes de bloqueio (cilindro e leitor de parede AirKey) regulam o acesso à porta. Consoante a autorização, decorre uma ativação ou rejeição no componente de bloqueio.

3.1.1 Cilindro AirKey

O cilindro AirKey é um componente de bloqueio que funciona a pilhas. Este também pode ser utilizado em ambientes interiores e exteriores. Dependendo dos requisitos em concreto, o cilindro AirKey também pode ser utilizado em áreas cuja segurança seja relevante. O cilindro AirKey está protegido mecanicamente de atos de vandalismo e manipulação. O cilindro AirKey é adequado, sob consideração das indicações normativas, para montagem em portas antifogo e de saída de emergência*.

O cilindro AirKey existe na versão de meio cilindro ou cilindro duplo. Existem dois modelos de cilindro duplo: modelo com acesso unilateral e modelo com acesso bilateral. No modelo com acesso unilateral, decorre um teste de autorização eletrónica apenas do lado exterior, no modelo com acesso bilateral, o acesso decorre dos dois lados. O puxador eletrónico no lado de identificação pode ser girado livremente sem autorização. A tampa de plástico preta do cilindro AirKey serve de unidade de leitura.

Se um meio autorizado for colocado encostado ao puxador, o cilindro engata durante um período de tempo limitado e possibilita uma ativação da fechadura ao girar o puxador eletrónico. Neste caso, considere também as indicações para [utilização de componentes de bloqueio AirKey](#).



Certifique-se de que, depois de fechar a porta, esta não seja bloqueada automaticamente. O bloqueio da porta tem de ser realizado manualmente ou, em alternativa, através de um dispositivo adicional correspondente.

Verifique se o cilindro AirKey selecionado é adequado para a utilização que pretende. O cilindro AirKey está disponível em diversos modelos e configurações.

As fichas técnicas necessárias e o catálogo de produtos estão à sua disposição na nossa homepage, na área de downloads em <https://www.evva.com/pt/downloads/>.

O cilindro AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em [Sinalização dos componentes de bloqueio](#).

Para a montagem do cilindro AirKey, tenha em atenção as instruções de montagem entregues com a embalagem ou o vídeo online com instruções de montagem em <https://www.evva.com/pt/airkey/website/>.

* Para utilização em portas de saída de emergência e antipânico – dependendo da fechadura utilizada – pode ser necessária a função antipânico FAP. Para isso, considere as respetivas indicações e certificados do fabricante da fechadura e o código de produto para encomenda.

3.1.2 Cilindro híbrido AirKey

O cilindro híbrido AirKey possui as mesmas características que o cilindro AirKey. O cilindro adequa-se a uma utilização em áreas interiores e exteriores, bem como em áreas onde a segurança é importante.

Comparativamente ao cilindro duplo AirKey com acesso unilateral, o cilindro híbrido AirKey dispõe, no lado interior, de um módulo de chave no lugar do puxador mecânico. Por conseguinte, o acesso a partir de fora é feito através de uma verificação de autorização eletrônica, e o acesso a partir de dentro é feito através de uma chave mecânica.



Certifique-se de que, depois de fechar a porta, esta não seja bloqueada automaticamente. O bloqueio da porta tem de ser realizado manualmente ou, em alternativa, através de um dispositivo adicional correspondente.

Certifique-se de que o cilindro híbrido AirKey é adequado à utilização que pretende.

A ficha técnica necessária e o catálogo de produtos estão à sua disposição na nossa homepage, na área de downloads em <https://www.evva.com/pt/downloads/>.

O cilindro híbrido AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em [Sinalização dos componentes de bloqueio](#).

Para a montagem do cilindro híbrido AirKey, tenha em atenção as instruções de montagem entregues com a embalagem.

3.1.3 Cilindro de patilha AirKey

O cilindro de patilha AirKey é um componente de bloqueio acionado a pilha para utilização em armários, vitrinas, diferentes receptáculos e caixas de correio, tanto em áreas interiores como exteriores.

O acesso é feito através de uma verificação de autorização eletrônica no lado exterior. No lado interior, o bloqueio é garantido por uma patilha. Tal como o desbloqueio, o bloqueio só pode ser executado depois de concluída a verificação da autorização, rodando manualmente o cilindro de patilha AirKey. Ao contrário do cilindro AirKey e do cilindro híbrido, o puxador eletrónico, disponível no lado de identificação, não pode ser rodado sem autorização.

Certifique-se de que o cilindro de patilha AirKey é adequado à utilização que pretende. O cilindro de patilha AirKey está disponível em diversos modelos e configurações.

A ficha técnica necessária e o catálogo de produtos estão à sua disposição na nossa homepage, na área de downloads em <https://www.evva.com/pt/downloads/>.

O cilindro de patilha AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em [Sinalização dos componentes de bloqueio](#).

Para a montagem do cilindro de patilha AirKey, tenha em atenção as instruções de montagem entregues com a embalagem.

3.1.4 Cadeado AirKey

O cadeado AirKey é um componente de bloqueio acionado a pilha para utilização em cacifos / compartimentos de armários, persianas, depósitos de armazenamento e arquivos, tanto em áreas interiores como exteriores.

O acesso é feito através de uma verificação de autorização eletrónica no lado inferior. O bloqueio é feito através de um arco em aço temperado. Tal como o desbloqueio, o bloqueio só pode ser executado depois de concluída a verificação da autorização, rodando manualmente o puxador eletrónico do cadeado AirKey.

Certifique-se de que o cadeado AirKey é adequado à utilização que pretende. O cadeado AirKey está disponível em diversos modelos e configurações.

A ficha técnica necessária e o catálogo de produtos estão à sua disposição na nossa homepage, na área de downloads em <https://www.evva.com/pt/downloads/>.

O cadeado AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em [Sinalização dos componentes de bloqueio](#).

Para a montagem do cadeado AirKey, tenha em atenção as instruções de montagem entregues com a embalagem.

Ferramentas de montagem para o cilindro AirKey

O cilindro AirKey, o cilindro híbrido, o cilindro de patilha e o cadeado oferecem um mecanismo especial de proteção contra manipulação. O puxador eletrónico só pode ser retirado com uma ferramenta especial. A ferramenta necessária para a montagem, desmontagem e substituição das pilhas não é normalmente fornecida juntamente com o cilindro e precisa de ser encomendada em separado.

Poderá obter o código para a encomenda no catálogo de produtos AirKey na área de downloads em <https://www.evva.com/pt/downloads/>.

3.1.5 Leitor de parede AirKey

O leitor de parede AirKey pode ser utilizado tanto em ambientes interiores como exteriores, com montagem embutida ou em superfície, e ainda em ambientes onde a segurança é relevante.

Utilize, em ambientes exteriores ou húmidos/molhados e em posição embutida, a vedação prevista para tal é fornecida em conjunto com o produto e observe as instruções do seu manual de montagem.

O leitor de parede AirKey é conectado à unidade de controlo AirKey através do cabo CAT5 (máx. 100 m, circuito máx. = 2 Ohm) e é alimentado por este. A unidade de controlo AirKey é alimentada pelo adaptador de corrente e dispõe de uma memória temporária (buffer) de

um máx. de 72 h, caso a corrente falhe, contanto que a unidade de controlo AirKey tenha funcionado antes, pelo menos, durante 6 horas.



Tenha em atenção que cada leitor de parede AirKey pode ser utilizado em conexão a uma unidade de controlo AirKey.

Através da combinação unidade de controlo – leitor de parede AirKey, podem ser ativados elementos de bloqueio eletrónicos como, p. ex., cilindro motorizado, portas giratórias, portas deslizantes etc.



À unidade de controlo pode ser ligado um elemento de ativação externo (botão de pressão). Se este for acionado, a porta abre-se, tal como acontece com um acesso pela unidade de leitura. Porém, a abertura da porta através do elemento de ativação externo NÃO fica registada em protocolo. Por razões de segurança, tenha em atenção que o acesso ao sistema AirKey através de sistemas de terceiros é, por conseguinte, possível sem ocorrer o registo no protocolo de acessos.

Verifique com atenção se o produto AirKey selecionado é adequado para a utilização / situação de montagem que pretende. A ficha de especificações técnicas necessária para esse fim e o manual de montagem estão disponíveis na nossa homepage na área de download em <https://www.evva.com/pt/downloads/>.

3.2 Aplicação AirKey



A aplicação AirKey é disponibilizada pela EVVA e pode ser obtida gratuitamente na Google Play Store ou Apple App Store.



A aplicação AirKey é condição prévia para poder utilizar os componentes de bloqueio AirKey pelo smartphone. Além disso, o seu smartphone pode adicionar ou atualizar componentes de bloqueio e meios num sistema AirKey. Para a maior parte das ações da aplicação AirKey, é necessária uma ligação ativa à Internet. A exceção aqui é o acionamento de componentes de bloqueio.



Ao fazer a ligação à Internet, é possível que haja um aumento dos custos. Tenha em atenção o seu contrato tarifário.

3.3 Smartphones

Para a utilização de um smartphone no sistema AirKey, devem ser preenchidas, pelo menos, as condições seguintes:

- > Smartphone com ligação NFC e/ou Bluetooth 4.0 (Bluetooth Low Energy / BLE)
- > Sistema operativo:
 - Android™ a partir de 5.0 (apenas possível a funcionalidade NFC)
 - Android™ a partir de 6.0 (NFC e Bluetooth)

- Apple™ a partir de iOS 10 (apenas possível a funcionalidade Bluetooth)
- > A aplicação AirKey pode ser obtida na Google Play Store ou Apple App Store
- > Os smartphones Android precisam da autorização "Aceder a estado do telefone e Identidade" e da autorização para a determinação da localização.



Lista dos smartphones compatíveis com o sistema AirKey

Tenha em atenção o facto de a compatibilidade de um smartphone depender de muitos fatores e de nem todos os smartphones, mesmo preenchendo os requisitos mínimos, serem compatíveis. Neste contexto, a EVVA submete os smartphones a minuciosos procedimentos de teste. Poderá encontrar uma lista continuamente atualizada dos modelos de smartphone adequados para utilização com o AirKey em [lista de smartphones compatíveis](#).



A **autorização "Aceder a estado do telefone e Identidade"** é necessária para poder identificar inequivocamente o smartphone ao adicionar um novo sistema de controlo de acessos.

A **autorização da localização é necessária, porque o Android 6+ exige a ativação da determinação da localização, para poder procurar componentes Bluetooth!** Se pretender utilizar funções Bluetooth na aplicação AirKey, terá de ativar a função de determinação da localização nas definições do dispositivo, assim como conceder a autorização da aplicação para esta função. Se **NÃO** pretender ativar a determinação da localização, poderá estabelecer uma ligação aos componentes (meios e componentes de bloqueio) através de NFC.



No caso dos **dispositivos Apple** (sistema operativo iOS), não há qualquer possibilidade de desativar a autorização "Aceder a estado do telefone e Identidade". Adicionalmente, o iOS também pode procurar a determinação da localização sem a autorização com base nos componentes Bluetooth.

3.4 Meios AirKey

Como meios, estão, atualmente, disponíveis modelos de smartphone testados, assim como cartões, porta-chaves, chaves combinadas e pulseiras em diferentes configurações, por exemplo, em combinação com a tecnologia *Mifare DESFire EV1*.

As respetivas fichas técnicas e o catálogo de produtos estão à sua disposição na nossa homepage, na área de downloads em <https://www.evva.com/pt/downloads/>.



Os meios como, p. ex., cartões, porta-chaves ou chaves combinadas são fornecidos no estado de fábrica. Para poder utilizar estes meios no seu sistema de controlo de acessos AirKey, terá de adicioná-los, em primeiro lugar, ao sistema.

3.5 Administração online do AirKey

A Administração online do AirKey é o software online fornecido pela EVVA para a administração e gestão do sistema de controlo de acessos AirKey. O sistema de controlo de acessos eletrónico AirKey funciona com todos os browsers da Internet e sistemas operativos mais populares e não exige nenhuma infraestrutura de TI em especial. A operação e manutenção contínua do centro de dados do AirKey são assumidos pela EVVA.

3.5.1 Pré-requisitos do sistema

- > Sistemas operativos: Windows 10 (ou superior), MacOS 10.15 (ou superior), Linux
- > Neste momento, são suportados os seguintes browsers:
Chrome, Firefox, Edge, Safari
- > JavaScript ativado no browser
- > Ligação à Internet (1 MBit/s ou velocidade superior)
- > Opcional: porta USB 2.0 para a estação de codificação
- > A porta de Internet 443 deve estar acessível.



Para o registo de um sistema de controlo de acessos AirKey, precisa de um endereço de e-mail válido.

3.6 KeyCredits da EVVA

Para a operação contínua de um sistema de controlo de acessos AirKey são necessários KeyCredits para a concessão e alteração de autorizações de acesso. Os KeyCredits estão à disposição como créditos de quantidade (número definido de possíveis alterações das autorizações com tempo ilimitado) ou como créditos de tempo (número ilimitado de possíveis alterações das autorizações dentro de um período de tempo definido). Dependendo do tamanho e da dinâmica do seu sistema AirKey, para cada área de aplicação, existe um pacote de KeyCredits adequado, o qual pode obter junto do seu vendedor de produtos EVVA. Poderá encontrar mais detalhes a respeito dos pacotes disponíveis no catálogo de produtos AirKey em <https://www.evva.com/pt/downloads/>.

3.7 Estação de codificação

Com a estação de codificação opcional, os componentes de bloqueio e os meios AirKey podem ser adicionados a um sistema de controlo de acessos AirKey ou atualizados, assim como o podem ser através de um smartphone com autorização de manutenção. A aplicação a ser instalada para a estação codificadora oferece a vantagem de ser compatível com os atuais browsers e de a estação codificadora poder ser utilizada para atualizar os componentes de bloqueio e os meios, mesmo depois de sair da Administração online do AirKey ou de ter fechado o browser.

São suportados os seguintes browsers: Chrome, Firefox e Edge.

Pré-requisitos do sistema:

- > Porta USB

- > Java 7 ou superior
- > Driver para a estação de codificação

Poderá obter mais informações a este respeito no capítulo [Instalar a estação de codificação](#).

3.8 Alimentação de emergência

Em todos os componentes de bloqueio, existe na parte frontal do componente, por baixo do logotipo EVVA, uma interface. Esta pode ser acedida, pressionando um pouco para dentro o logotipo, na parte esquerda do texto (letra E) e abrindo para fora para o lado direito (letra A). A interface integrada serve apenas para a alimentação de emergência e não é necessária para o funcionamento normal.

O dispositivo de alimentação de emergência alimenta eletricamente os componentes de bloqueio para que possam ser utilizados no caso de as pilhas estarem gastas. Conecte, neste caso, o cabo do dispositivo de alimentação de emergência na respetiva interface e ligue-o. Não é necessária qualquer interação adicional no dispositivo de alimentação de emergência. Para a utilização do próprio componente de bloqueio AirKey, é necessário um meio com autorização válida.

Tenha em atenção, neste caso, para o facto de ter de ser uma autorização permanente sem data de validade. Poderá obter mais informações a este respeito no capítulo [Meios de emergência](#). Substitua imediatamente as pilhas do componente de bloqueio em caso de alimentação de emergência e atualize, depois, o componente de bloqueio para voltar a possibilitar o acesso também com outros meios. Poderá também obter mais informações a respeito da alimentação de emergência nas rubricas [Substituição das pilhas e Alimentação de emergência](#).



Tenha em atenção que o leitor de parede AirKey não pode ser alimentado pelo dispositivo de alimentação de emergência, uma vez que este é alimentado por uma fonte de alimentação externa em combinação com a unidade de controlo AirKey.

4 Primeira utilização

Neste capítulo, estão descritos os primeiros passos para a primeira colocação em funcionamento do sistema AirKey.



Na homepage <https://www.evva.com/pt/airkey/website/>, poderá encontrar também um screencast, o qual descreve os primeiros passos e a colocação em funcionamento do sistema AirKey.

Como apoio à montagem dos componentes de bloqueio, a EVVA oferece o material seguinte:

- > **Manual de instruções de montagem:**
Para dar apoio na inserção dos componentes de bloqueio, a EVVA tem à disposição instruções de montagem tendo em conta a neutralidade do idioma. Estas poderão ser encontradas na embalagem do respetivo produto ou na homepage em <https://www.evva.com/pt/downloads/>.
- > **Vídeos:**
Na homepage <https://www.evva.com/pt/airkey/website/> existem vídeos à disposição com explicações a respeito da montagem.

4.1 Instalar a aplicação AirKey

- > Carregue a aplicação AirKey a partir da Google Play Store ou Apple App Store
- > Siga as instruções para a instalação da aplicação AirKey no smartphone.

4.2 Registo na Administração online do AirKey

Para utilizar a Administração online do AirKey, tem de se registar na EVVA com um endereço de e-mail válido.

- > Selecione no seu browser a página <https://airkey.evva.com>.
Abre-se a página de login da Administração online do AirKey.
- > Selecione o seu **idioma**.
- > Clique no link **Registo AirKey** .

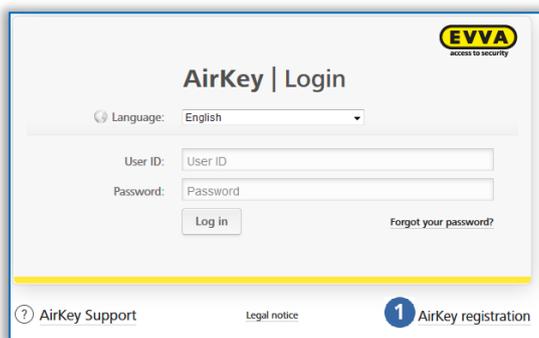


Figura 3: Link "Registo AirKey"

No formulário de registo, preencha os campos e registe-se no AirKey.

- > Selecione **Cliente empresarial** ou **Cliente privado**.
- > Preencha os campos do formulário.
Os campos assinalados com * são de preenchimento obrigatório.
- > Resolva o Captcha 1.
- > Ative a caixa de seleção com o link [Termos e condições gerais de negócios](#) e a caixa de seleção com o link [Condições gerais de licenciamento](#) 2. Os dois respetivos documentos PDF são abertos automaticamente. Estes documentos estão disponíveis em <https://www.evva.com/pt/airkey/impressum/>.

Figura 4: Registo no AirKey



Caso necessite, poderá, posteriormente, em qualquer momento, alterar os dados de cliente. Para tal, clique na Administração online do AirKey, no menu principal, em **Sistema de controlo de acessos** → **Dados de cliente**.

- > Clique em **Registar**. Abre-se a janela da aplicação "Concluir registo".
- > Verifique, mais uma vez, o endereço de e-mail indicado, neste irá incluído um link para a confirmação do registo.
- > Se o endereço de e-mail indicado estiver incorreto, interrompa o processo com **Cancelar** e corrija a inserção.
- > Se o endereço de e-mail estiver correto, carregue em **Concluir registo**.

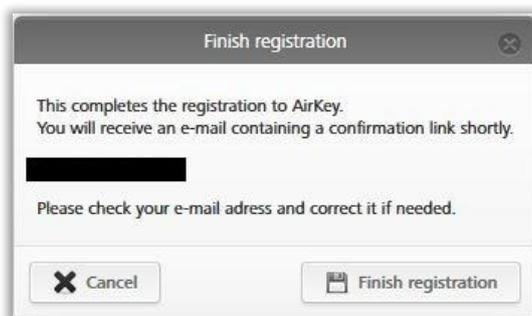


Figura 5: Concluir registo

É automaticamente gerada, a partir do sistema AirKey, uma identificação do utilizador e um link de confirmação do registo e é enviado um e-mail para o endereço de e-mail indicado por si.

- > Abra o seu programa de correio eletrónico, pois encontrará aí o e-mail da EVVA com o assunto "Registo no AirKey EVVA".
- > Abra o e-mail e clique no link de confirmação do registo **1**.



Guarde este e-mail. Caso necessite de suporte técnico terá que fornecer a sua identificação de utilizador e o seu número de utilizador único contido neste e-mail.

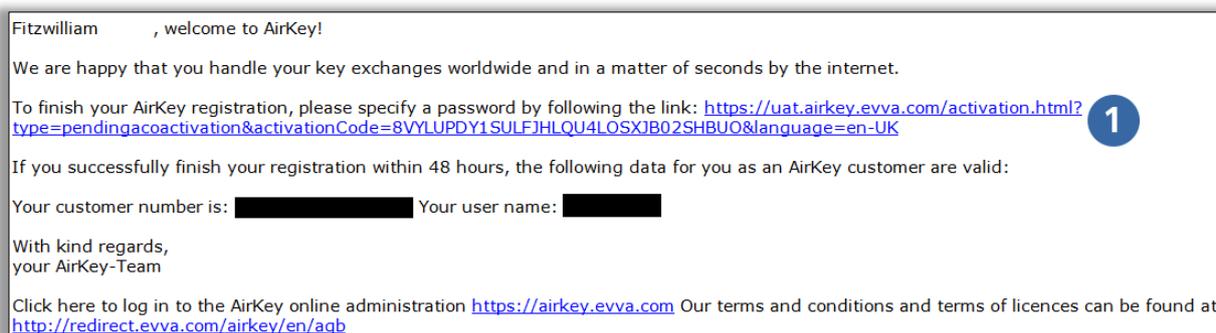


Figura 6: E-mail "Registo no AirKey EVVA"



O link de confirmação do registo no e-mail só é válido por 48 horas.

Se este link expirar ou invalidar, aparece a mensagem de erro "Link de confirmação do registo inválido". Neste caso, deverá voltar a registar-se.

Depois de ter clicado no link de confirmação do registo, abre-se uma janela de boas-vindas, onde poderá concluir o seu registo.

- > Insira uma senha escolhida por si para a Administração online do AirKey. A senha tem de ter, pelo menos, 6 caracteres e incluir um número, uma letra maiúscula e uma letra minúscula, caso contrário receberá uma mensagem de erro.
- > Repita a inserção da senha.
- > Indique a sua data de nascimento. Esta é utilizada como pergunta de segurança, caso se tenha esquecido da sua senha.



Por razões de segurança, recomendamos que escolha uma senha o mais comprida possível para o AirKey e que a mantenha em sigilo.

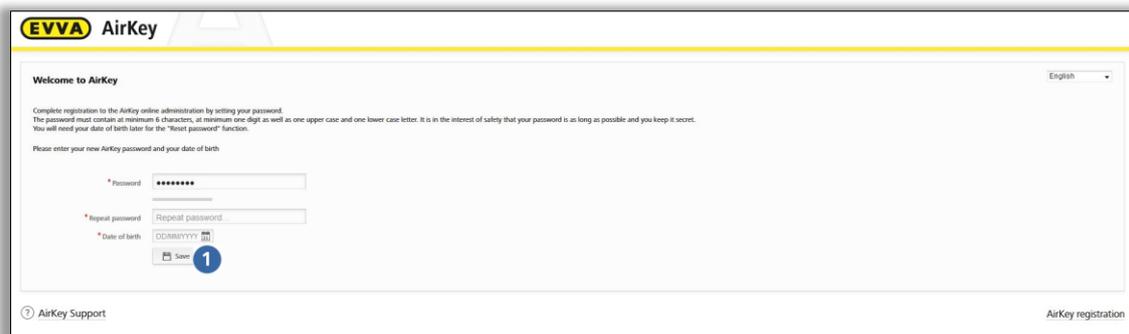


Figura 7: Determine a sua própria senha para concluir o registo

- > Quando os campos obrigatórios tiverem sido preenchidos e as duas senhas do AirKey corresponderem, conclua o registo carregando em **Guardar** 1.

Agora, concluiu o processo de registo e ativou com sucesso o seu sistema AirKey.

A partir de agora, poderá iniciar sessão na Administração online do AirKey na página de login, sempre que quiser. Para tal, precisará da identificação de utilizador e da senha determinada anteriormente para o AirKey.

4.3 Iniciar sessão

O início de sessão é necessário para configurar e administrar o sistema de controlo de acessos AirKey.

- > Selecione no seu browser a página <https://airkey.evva.com>.
Abre-se a página de login da Administração online do AirKey.
- > Selecione o seu **idioma**. Na sessão ativa, poderá alterar o idioma, a qualquer momento, à direita na barra de menu.
- > Insira a identificação de utilizador recebida no e-mail de confirmação do registo e a senha escolhida e confirme a ação em **Iniciar sessão**. Abre-se a página inicial do seu sistema de controlo de acessos AirKey.

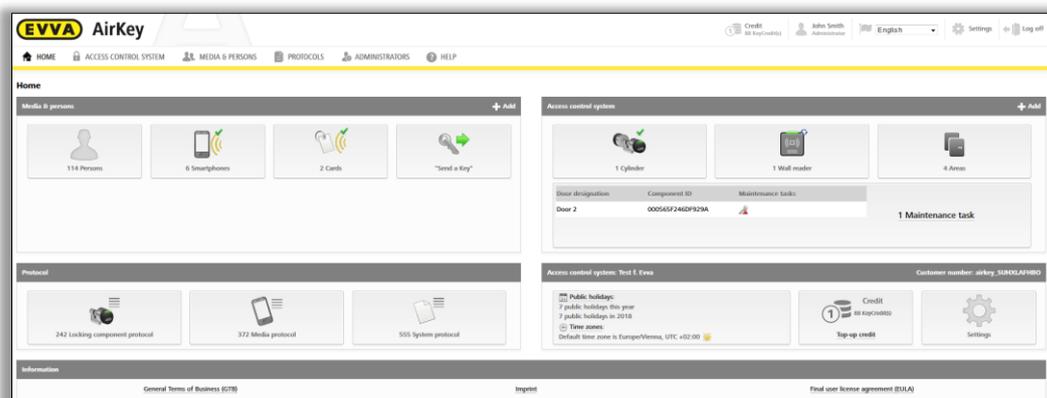


Figura 8: Página inicial do sistema de controlo de acessos AirKey

Na página inicial, todos os dados relevantes do sistema são indicados na vista geral. A partir daqui, poderá navegar para todas as funções e definições.

4.4 Ajuda interativa

Na Administração online do AirKey, depois do primeiro login, é ativada uma Ajuda interativa, que serve de guia pelo programa e esclarece sobre as funções mais importantes.

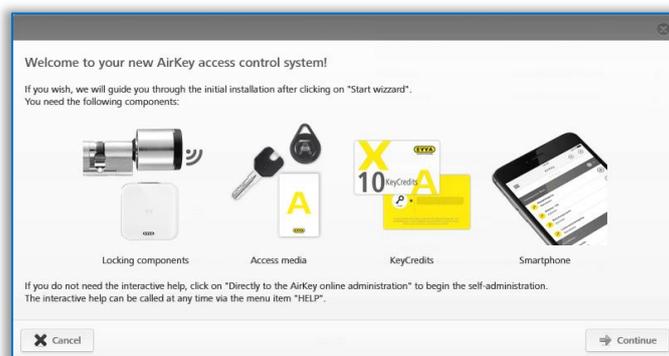


Figura 9: Ajuda interativa

A título de exemplo, é exibida a função "Carregar crédito". A ajuda interativa mostra quais os botões que tem de clicar e fornece indicações sobre que informações tem de inserir nos campos. No âmbito da ajuda interativa, poderá navegar para a frente e para trás.

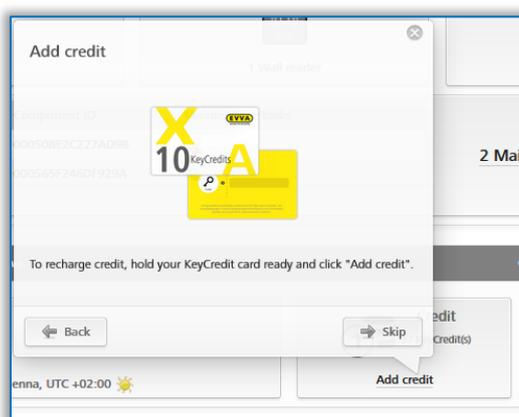


Figura 10: Ajuda interativa – Carregar crédito

Também poderá fechar a ajuda interativa e aprender sobre a Administração online do AirKey através do manual do sistema.



Se, depois de ter fechado a ajuda interativa, pretender abri-la novamente, seleccione, no menu principal, **Ajuda** → **Ajuda interativa**. Desta forma, poderá abrir a ajuda interativa sempre que quiser.

4.5 Instalar a estação de codificação

Option

Pode ser utilizada, a título opcional, uma estação de codificação para adicionar ou atualizar componentes de bloqueio e meios num sistema de controlo de acessos AirKey.

Para utilizar uma estação de codificação no sistema AirKey, é necessário instalar uma aplicação da estação de codificação.

Existem duas formas de utilizar a estação de codificação:

- no browser, através da Administração online do AirKey
- sem browser, através da linha de comando

4.5.1 Utilizar a estação de codificação através da Administração online do AirKey

A aplicação a ser instalada para a estação codificadora oferece a vantagem de ser compatível com os atuais browsers e de a estação codificadora poder ser utilizada para atualizar os componentes de bloqueio e os meios, mesmo depois de sair da Administração online do AirKey ou de ter fechado o browser.

A adição e a remoção de componentes de bloqueio de um sistema de bloqueio, bem como a atualização do firmware dos componentes de bloqueio e a atualização do Keyring dos meios de acesso só são possíveis depois de entrar na Administração online do AirKey. As atualizações dos meios e dos componentes de bloqueio também são possíveis depois de sair da Administração online do AirKey ou fechar o browser.

Os browsers seguintes suportam a comunicação entre a Administração online do AirKey e a aplicação da estação de codificação local: Chrome, Firefox e Edge.

O download e a execução da aplicação da estação de codificação são específicos do browser e do sistema operativo. A apresentação visualizada no seu browser pode divergir da aqui ilustrada (para Firefox).

Registe-se e inicie sessão na Administração online do AirKey (ver o capítulo [Registo na Administração online do AirKey](#)).

- > Conecte a estação de codificação numa porta USB do seu computador.
- > Clique na Administração online do AirKey no sinal **+** à direita em baixo **1**.

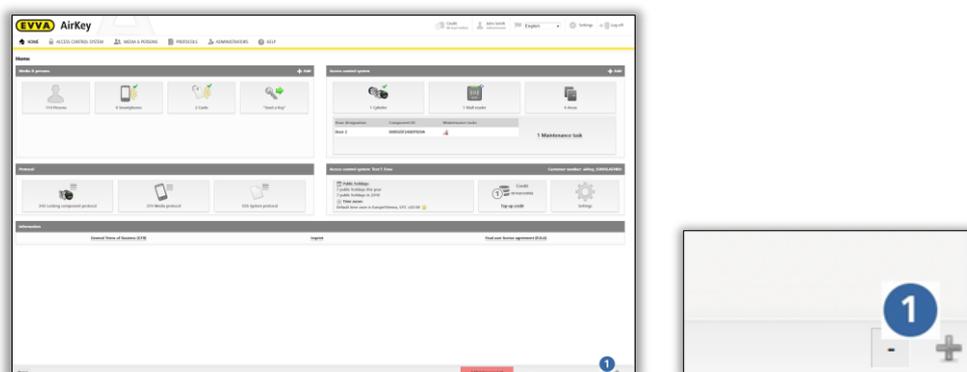


Figura 11: Estação de codificação – instalação da aplicação

- > Para instalar a aplicação da estação de codificação, clique no link "Iniciar e iniciar a aplicação da estação de codificação" **1**.

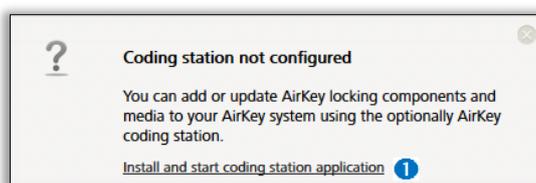


Figura 12: Instalar e iniciar a aplicação da estação de codificação



Depois de clicar no link, tem 60 segundos para abrir o ficheiro AirKey.jnlp (ver o passo seguinte). Caso exceda este tempo, a instalação tem de ser repetida a partir do passo atual. Em alternativa, também poderá guardar o ficheiro AirKey.jnlp e abri-lo manualmente.

- > Aparece a caixa de diálogo para download do ficheiro AirKey.jnlp. Abra-o com o "Java(TM) Web Start Launcher".

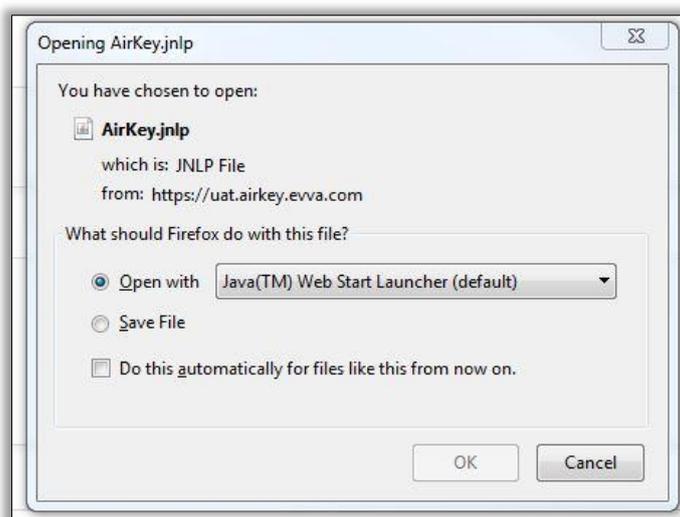


Figura 13: Abertura do ficheiro AirKey.jnlp

- > Depois de abrir o ficheiro, é estabelecida a ligação à estação de codificação.

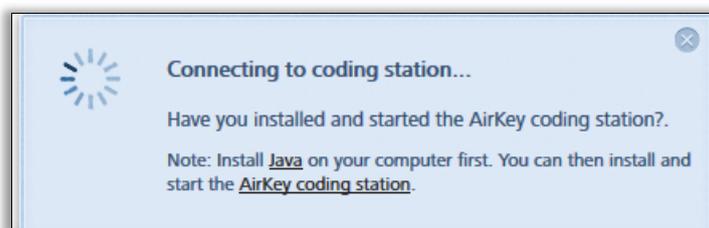


Figura 14: Estabelecimento da ligação à estação de codificação

- > Selecionar a estação de codificação existente (p. ex., "MNIKEY CardMan 5x21-CL 0" ) da lista.

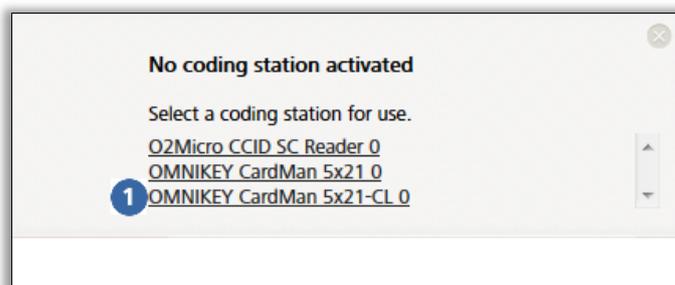


Figura 15: Seleção da estação de codificação

- > Na barra de tarefas à direita, em baixo, aparece um ícone do AirKey  – a estação de codificação foi instalada com sucesso e está ativa.



Figura 16: Ícone do AirKey na barra de tarefas

4.5.2 Utilizar a estação de codificação através da linha de comando

A aplicação da estação codificadora também pode ser instalada e configurada sem a Administração online do AirKey, por exemplo, através da linha de comando. (Para esta opção, são necessários conhecimentos avançados de TI, em especial, trabalho na linha de comando.)

Através da linha de comando, a estação de codificação só pode ser utilizada para atualizar os meios de acesso e os componentes de bloqueio. A atualização do firmware dos componentes de bloqueio só é possível através do browser ou de um smartphone com autorização de manutenção.

- > Guarde a aplicação da estação codificadora através do link <https://airkey.evva.com/smcrest/jnlp/newest-jar-file/> no diretório que desejar.

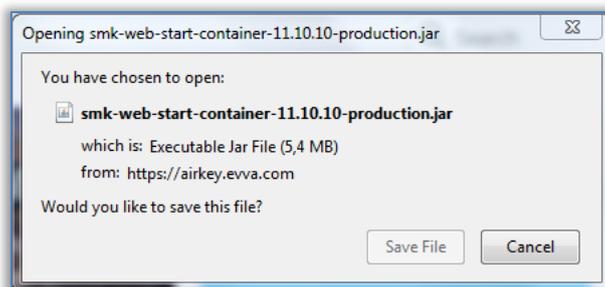


Figura 17: Download da aplicação da estação codificadora

- > Abra a linha de comando e navegue para o diretório, onde a aplicação da estação codificadora foi depositada anteriormente.
- > Inicie a aplicação da estação de codificação com o seguinte comando:

```
java -jar <nome do ficheiro>
```

(p. ex. web-start-container-customer-15.10.0-8.jar)

Adicionalmente, pode especificar os seguintes parâmetros opcionais:

- **-reader "<nome da estação de codificação>":** Este parâmetro permite utilizar uma estação de codificação específica (p. ex. "HID Global OMNIKEY 5022 Smart Card Reader 0"). Neste caso, o ficheiro de configuração `config_customer.json` é ignorado.
- **-port <VALOR [1024-65535]>:** Se este parâmetro não for especificado, a porta 50743 é utilizada por defeito. A porta 50743 também é utilizada quando a estação de codificação é utilizada no browser através da Administração online do AirKey. Se quiser utilizar várias estações de codificação num computador em

paralelo, tem de indicar uma porta própria para cada estação de codificação. Com o parâmetro "-port 0" (porta 0) é utilizada uma porta aleatória.

- **-configDir <VALOR>**: Na pasta especificada (valor por defeito para Windows: %USERPROFILE%\airkey) é guardado o ficheiro de configuração config_customer.json. Este é gerado automaticamente aquando do primeiro início da aplicação da estação de codificação e guarda as últimas definições utilizadas.
- **-workDir <VALOR>**: Na pasta especificada é criado, por exemplo, o ficheiro de registo (log) logs\application.log, quando a aplicação da estação de codificação é iniciada. Aqui são registadas todas as ações que foram executadas com a aplicação da estação de codificação. Se utilizar várias estações de codificação em paralelo, faz sentido utilizar uma pasta própria para cada estação de codificação.
- **-notify <nome do ficheiro>**: Define um ficheiro executável ou um script que pode encaminhar a lockingSystemID como string hexadecimal (argument1) ou como long-int (argument2) de um meio de acesso atualizado com sucesso na estação de codificação para um sistema de terceiros. Este parâmetro é relevante principalmente para a integração do AirKey em sistemas de terceiros e para a utilização da AirKey Cloud Interface. Aí, a lockingSystemId do meio de acesso pode ser avaliada e processada. Por exemplo, para encontrar a pessoa à qual pertence o meio de acesso. Os detalhes da AirKey Cloud Interface estão descritos no capítulo [AirKey Cloud Interface \(API\)](#).
- **-version**: indica a versão da aplicação da estação codificadora.
- **-help**: abre a Ajuda e descreve todos os parâmetros possíveis.

> No canto inferior direito da barra de tarefas aparece o ícone do AirKey  e, na linha de comando, são exibidas informações sobre o diretório de configuração ❶, o diretório de trabalho ❷ e as estações codificadoras ❸ disponíveis.

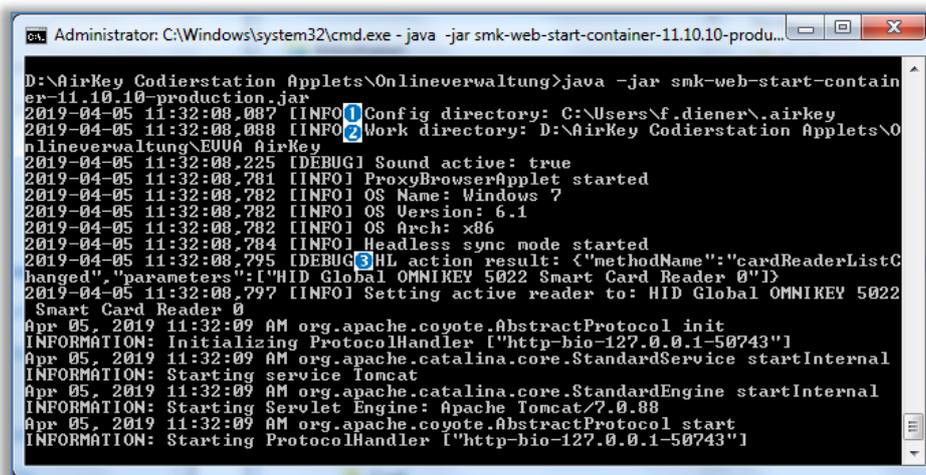


Figura 18: Iniciar a aplicação da estação codificadora, linha de comando

4.5.3 Definições da aplicação da estação de codificação

Ao clicar à direita no ícone AirKey , o respetivo menu contextual abre-se.

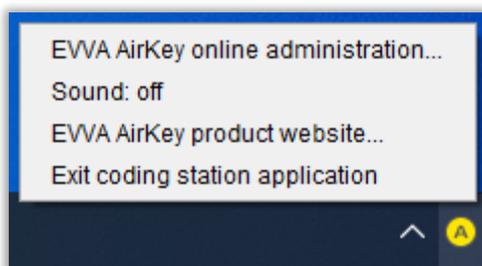


Figura 19: Definições da aplicação da estação de codificação

Lista dos respetivos pontos do menu:

- > **Administração online do AirKey EVVA** – link para a página de login da Administração online do AirKey
- > **Som: ligado** – é emitido um som bipe, sempre que um componente for atualizado com a estação de codificação. Faz sentido como aviso sonoro se a estação de codificação não for utilizada com a Administração online do AirKey. Ao clicar em **Som: ligado**, este mudará para **Som: desligado**.
- > **Som: desligado** – não será emitido qualquer som. Ao clicar em **Som: desligado**, este mudará para **Som: ligado**.
- > **Sítio Web do produto AirKey EVVA...** – link para o sítio Web do [Produto AirKey](#)
- > **Sair a aplicação da estação codificadora** – termina a aplicação da estação de codificação.

4.5.4 Soluções para possíveis problemas com a estação de codificação

Se a estação de codificação estiver conectada, o LED sinaliza que está pronta para o serviço. Se não for sinalizada a disponibilidade operacional, desconecte o cabo da estação de codificação e volte a conectá-lo. Se necessário, volte a instalar o driver da estação de codificação.



Ao desligar o computador, a aplicação local da estação de codificação fecha automaticamente. Para a iniciação automática da aplicação ao reiniciar o computador, poderá criar através do Java™ Control Panel (Configure Java) uma ligação da aplicação (utilização: AirKey Card Reader Proxy; tipo: utilização) e colocá-la na pasta Autostart.

A aplicação da estação de codificação encerra depois de iniciar

A aplicação da estação de codificação utiliza por defeito a porta 50743 para comunicar com o browser. Se esta porta for utilizada por outro programa, a aplicação da estação de codificação não pode ser iniciada. No Windows 10 ou superior, esta porta pode ser utilizada por Hyper-V. Pode evitar que o Hyper-V utilize esta porta da seguinte forma:

- > Desativar Hyper-V:

```
C:\> dism.exe /Online /Disable-Feature:Microsoft-Hyper-V
```
- > Reinicie o computador.
- > Adicione uma exceção para a porta 50743:

```
C:\> netsh int ipv4 add excludedporrange protocol=tcp startport=50743  

    numberofports=1
```

- > Reativar Hyper-V:
C:\> `dism.exe /Online /Enable-Feature:Microsoft-Hyper-V /All`
- > Reinicie o computador.

Como estação de codificação, está selecionado o leitor de cartões "Microsoft UICC"



Figura 20: Leitor de cartões "Microsoft UICC" na Administração online do AirKey

Como solução, o leitor de cartões UICC pode ser desativado no gestor de dispositivos do Windows: Gestor de Dispositivos → Dispositivos de software → Microsoft UICC ISO Reader → Desativar dispositivo

Não é possível estabelecer a ligação à estação de codificação através da Administração online do AirKey (proxy https)

Tanto a Administração online do AirKey como a aplicação da estação de codificação comunicam de forma encriptada com o sistema AirKey através da porta 443. Em redes que utilizam um proxy https, poderá ser necessário definir uma exceção para "airkey.evva.com" e subdomínios, pois a aplicação da estação de codificação verifica o certificado do servidor através de "certificate pinning" e, assim, não permite quaisquer proxies https.

Não é possível estabelecer a ligação à estação de codificação através da Administração online do AirKey (proteção de DNS rebinding)

A Administração online do AirKey comunica localmente entre o browser e a aplicação da estação de codificação. Ações como a colocação de componentes de bloqueio ou meios de acesso na estação de codificação são, então, exibidas na Administração online do AirKey.

O browser liga-se à aplicação da estação de codificação através de "components.airkey.evva.com" (Porta 50743). Este URL é identificado pelo servidor DNS como 127.0.0.1.

Por isso, pode ser necessário adicionar exceções para "components.airkey.evva.com" e subdomínios de "airkey.evva.com" com a proteção de *DNS rebinding* ativa.

O Windows procura repetidamente o driver para a estação de codificação

Ao colocar um componente de bloqueio ou um meio de acesso na estação de codificação, o Windows tenta procurar e instalar um driver para a estação de codificação. Isto pode influenciar a comunicação com a estação de codificação e provocar falhas de funcionamento.

Como solução, o serviço Smart Card Plug & Play do Windows pode ser desativado:

- > Tecla Windows + R
- > Introduza "gpedit.msc" e confirme com **Enter**.
- > O programa "Editor de Políticas de Grupo Local" → Configuração de computador → Modelos administrativos → Componentes do Windows → Smart Card
- > Clique duas vezes na linha com a entrada "serviço Smart Card Plug & Play" do lado direito.

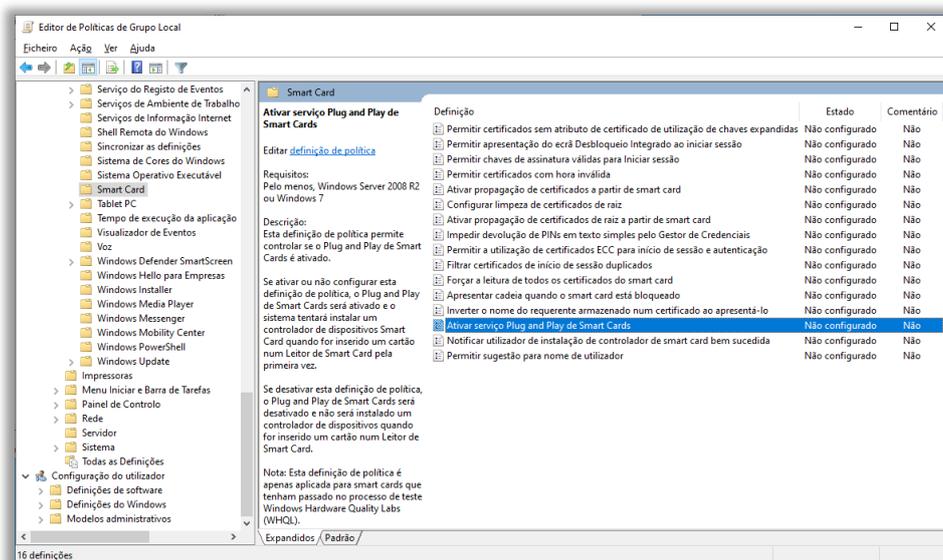


Figura 21: Editor de Políticas de Grupo Local

- > Selecione o botão de opção **Desativado**.
- > Confirme com **OK**.

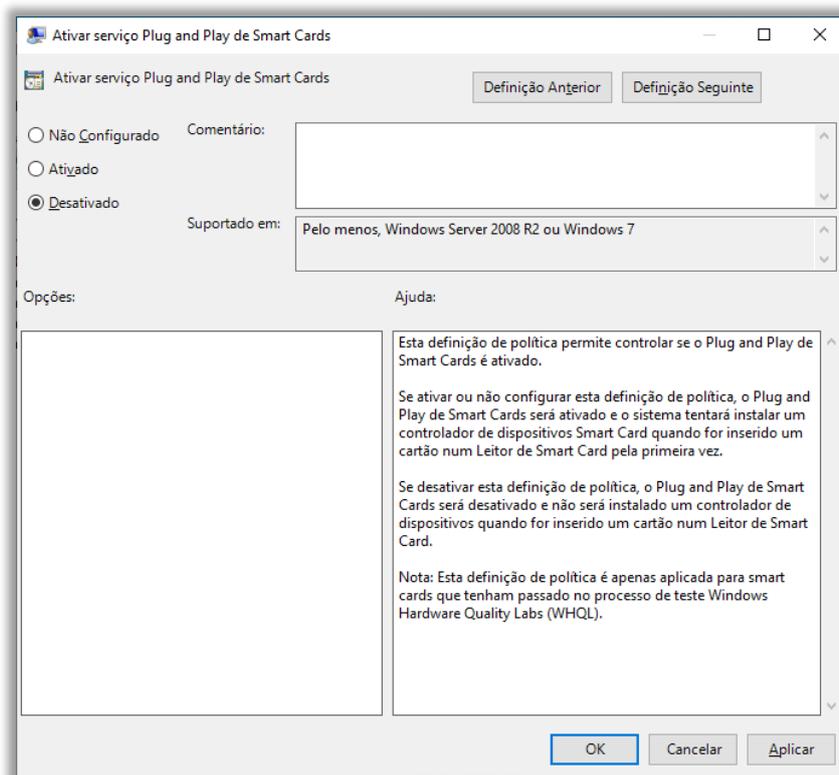


Figura 22: Serviço Plug and Play de Smart Cards

No MacOS 11.x ou superior não é possível selecionar uma estação de codificação

Desde o MacOS Big Sur (11.x) que já não é possível selecionar uma estação de codificação conectada num Mac através da Administração online do AirKey. A aplicação da estação de codificação pode ser iniciada com sucesso, mas não é mostrada nenhuma estação de codificação na Administração online do AirKey.

Como solução, a estação de codificação pode ser iniciada através da linha de comando (ver capítulo [Utilizar a estação de codificação através da linha de comando](#)). No entanto, uma condição prévia é que a versão Java JDK17 (Oracle JDK17 ou OpenJDK17) ou superior esteja instalada.

4.6 Adicionar crédito

É necessário um cartão KeyCredit, que apresenta um campo na parte de trás com um código de crédito.

- > Na página inicial **Home**, clique na caixa de seleção **Adicionar crédito** ①.
- > Em alternativa, poderá clicar em **Crédito** na linha de cabeçalho.

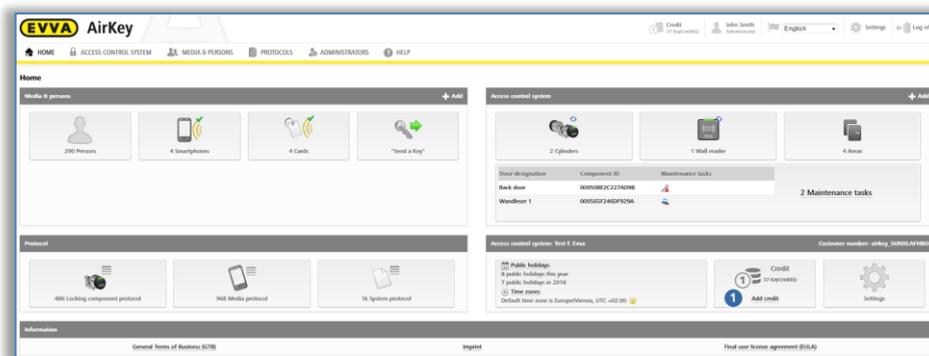


Figura 23: Créditos

- > Obtém uma visão global dos créditos atuais e dos carregamentos já efetuados.
- > Clique no botão **Adicionar crédito** 1.

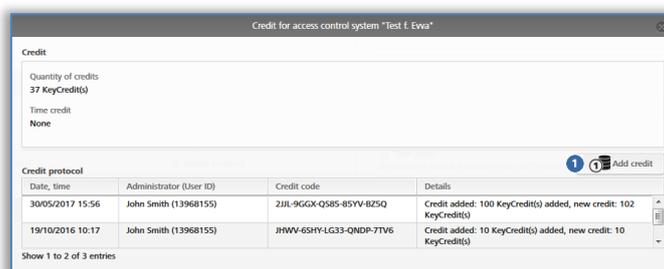


Figura 24: Adicionar crédito

- > Insira na janela da aplicação "Adicionar crédito" o código, indicado no cartão KeyCredit.

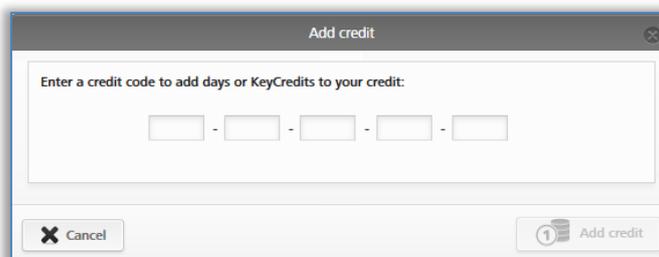


Figura 25: Inserir o código de crédito

- > Clique em **Adicionar crédito**.

Caso tenha inserido o código correto, a inserção será confirmada e o crédito debitado.

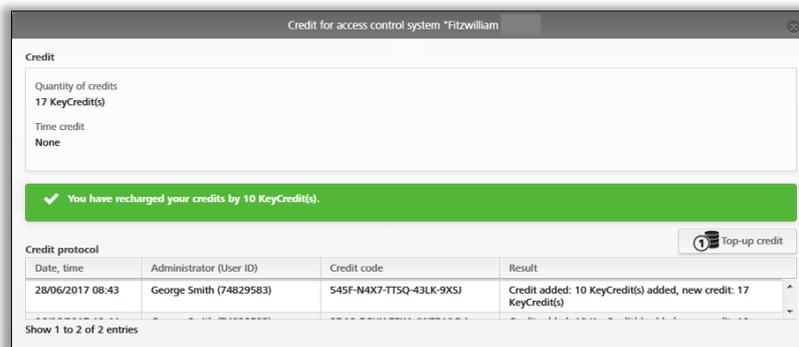


Figura 26: Adicionar crédito

4.7 Criar pessoa

Qualquer pessoa que deva receber uma autorização para o sistema de controlo de acessos AirKey tem de ser previamente criada.

- > Na página inicial **Home**, na barra cinzenta **Adicionar**, selecione no bloco **Adicionar Meios e Pessoas** → **Criar pessoa**.
- > Ou selecione, na página inicial **Home**, a caixa de seleção **Pessoas** → **Criar pessoa**.
- > Ou selecione no menu principal **Meios e pessoas** → **Criar pessoa**.
- > Ou selecione o botão "**Send a Key**" e clique em **Criar novo**. Aqui, uma pessoa pode ser criada com um smartphone.
- > Preencha os campos do formulário. Os campos assinalados com * são de preenchimento obrigatório.
- > Clique em **Guardar** 1.

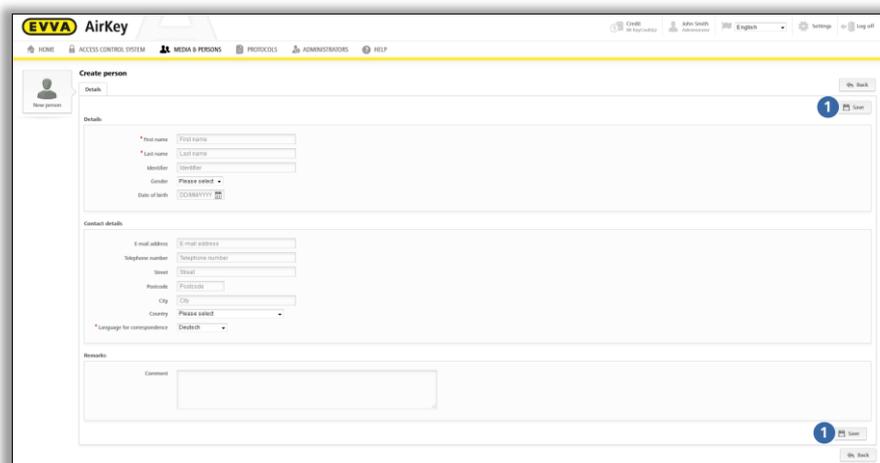


Figura 27: Criar pessoa



Os campos Primeiro nome / Último nome / Identificação proporcionam uma combinação exclusiva no âmbito do sistema de controlo de acessos AirKey.



Quando preenche o campo "Identificação" adicionalmente, utiliza um valor que garante que a combinação com o primeiro e o último nome seja exclusiva (p. ex., o número pessoal). Isto faz muito sentido, quando há

peças com o mesmo primeiro e último nome.

O comprimento dos campos do endereço de e-mail, do número de telefone, da rua, do código postal e da localidade está limitado a um máximo de 50 caracteres. Para "CP" só podem ser utilizados, no máximo, 10 dígitos. No campo do comentário, poderá inserir um texto com um máximo de 500 caracteres.

Caso a combinação inserida já tenha sido criada, receberá a mensagem de erro "A pessoa já existe".

- > Verifique e corrija os seus dados.
- > Clique em **Guardar**.

Se a pessoa tiver sido criada com sucesso, aparece uma mensagem de confirmação e por baixo do nome é exibido um novo botão **Atribuir meio**

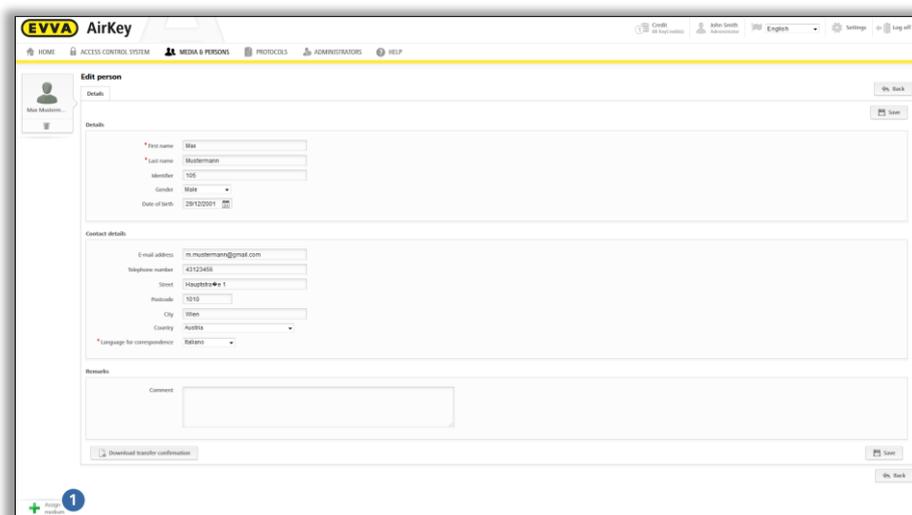


Figura 28: Atribuir meio

A pessoa é, assim, criada no sistema de controlo de acessos AirKey e fica registada na lista de pessoas.

4.7.1 Importar dados de pessoas

Com o AirKey, tem também a possibilidade de criar pessoas através de ficheiros externos. Para isso, precisa do respetivo ficheiro CSV para importar para a Administração online do AirKey.

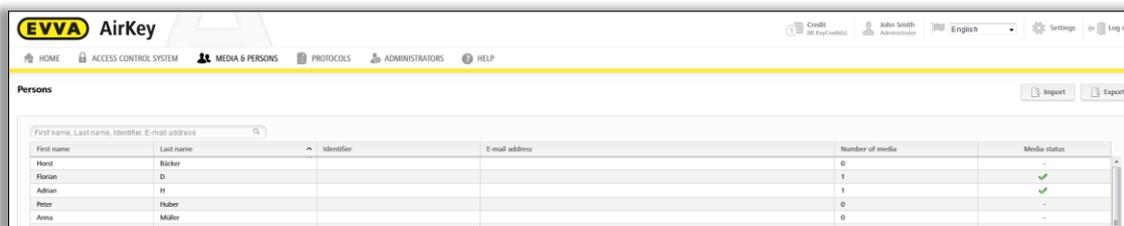


Figura 29: Importar lista de pessoas

A distribuição da tabela de pessoas é feita com base na página **Criar pessoa** na Administração online do AirKey, ou seja, a coluna A é Primeiro nome , a coluna B é Último

nome ②, a coluna C é Identificação ③ etc. É exatamente por este ordem que o ficheiro CSV é importado para a Administração online do AirKey.

Figura 30: Importas pessoas – Lista de pessoas

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

Figura 31: Importar pessoas – Distribuição dos campos na lista de pessoas

Características de um ficheiro CSV com os dados da pessoas a importar:

- > A primeira linha é sempre ignorada. Por isso, recomendamos registar aí os nomes dos campos para identificar os restantes dados com mais facilidade. A primeira linha também pode estar vazia, mas não pode conter pessoas, pois esta não será importada.
- > As linhas vazias ou as linhas que contenham apenas caracteres sem espaços e tabuladores (também espaços vazios) são igualmente ignoradas. Se pretender configurar o seu ficheiro CSV de forma clara, também poderá utilizar muitas linhas vazias à vontade.
- > Cada linha tem de conter todos os 13 campos (atributos), apresentados na Figura 30.
- > Os campos são separados por um ponto e vírgula.
- > Só existem 3 campos obrigatórios: Primeiro nome (campo 1), Último nome (campo 2) e Idioma para correspondência (campo 12).
- > Não obstante os restantes campos não integrarem dados, estes têm de estar disponíveis e, neste caso, como campos vazios (;;).
- > O sexo (campo 4) só pode incluir **M** (para *masculino* = homem) ou **F** (para *feminino* = mulher) ou ficar vazio. Isto aplica-se a todos os idiomas e o M e F apenas podem ser utilizados em maiúsculas.
- > A data de nascimento (campo 5) tem de estar disponível no formato **AAAA-MM-DD** (p. ex., 1997-12-20).
- > O endereço de e-mail (campo 6) tem de conter o carácter @ e outros caracteres ou ficar vazio.
- > O país para o endereço (campo 10) tem de conter o [código ISO 3166-1 alfa-3](#) de 3 dígitos do país ou ficar vazio. O código só pode ser indicado em maiúsculas. Exemplo: AUT, DEU, GBR, NLD, SWE, FRA, ITA, ESP, PRT, CZE, SVK, POL etc.
- > O idioma para correspondência (campo 12) é um campo obrigatório e tem de conter o código ISO para o idioma. A escrita em letras maiúsculas e minúsculas tem de ser criteriosamente respeitada. Apenas os códigos seguintes são aceites: cs-CZ, de-DE, en-UK, es-ES, fr-FR, it-IT, nl-NL, pl-PL, pt-PT, sk-SK, sv-SE.
- > Uma pessoa a importar é exibida como já existindo (símbolo ) , se a combinação Primeiro nome + Último nome + Identificação (campos 1-3) já existir na Administração online do AirKey, mesmo que os restantes campos (4-13) sejam diferentes. Estas pessoas não são importadas. A escrita dos nomes em maiúsculas / minúsculas não é relevante (p. ex., "Danny;**De**Vito;**DD**" e "Danny;**de**Vito;**Dd**" referem-se à mesma pessoa e só a primeira pessoa é importada).
- > Uma pessoa é interpretada como duplicada no ficheiro CSV, quando a combinação Primeiro nome + Último nome + Identificação (campos 1-3) já tiver sido encontrada uma vez, mesmo que os restantes campos (4-13) sejam diferentes. Neste caso, apenas é exibida a primeira linha com uma determinada combinação e, depois, importada. Todos os restantes duplicados são ignorados e não são exibidos na tabela das pessoas a importar.
- > Um ficheiro CSV pode conter os dados de, no máximo, 10 000 pessoas. Se quiser importar mais pessoas, crie vários ficheiros CSV que podem ser importados separadamente.

- > As linhas com erro no ficheiro CSV são assinaladas com o símbolo **✘** antes da importação e acompanhadas de uma tooltip que descreve todos os erros. Estas linhas não são importadas.
- > Independentemente das linhas existentes com eventuais erros, todas as linhas corretas são assinaladas com o símbolo **✔** e são, depois, importadas.



A codificação de caracteres do ficheiro CSV tem de ser UTF-8 para que as letras específicas do país (Ä, ß, ç, Ñ, č etc.) sejam corretamente exibidas. A criação de um ficheiro CSV no formato UTF-8 está descrita em detalhe abaixo.

Criação de um ficheiro CSV no formato UTF-8

A descrição seguinte aplica-se ao Windows 10™ utilizando o Microsoft Excel™ e os programas de ajuda já disponíveis no Windows 10™. Poderá ser criado um ficheiro CSV no formato UTF-8, de forma idêntica, noutras versões de Windows ou sistemas operativos. Passos necessários:

- > Como base inicial, esta descrição inclui uma tabela Excel que contém os dados das pessoas a importar.
- > Preste atenção, na tabela Excel, ao facto de a 7.ª coluna (número de telefone) estar obrigatoriamente formatada como texto. Ao formatar como algarismo, os caracteres principais, tais como "+" e "0" (zero), seriam perdidos na conversão. Os espaços incluídos no número de telefone são, no entanto, permitidos e aumentam a clareza na administração Online do AirKey.
- > Fazendo uso da função "Localizar" do Excel, verifique se a tabela não contém nenhum dos seguintes caracteres:
 - " (aspas duplas subidas, retas)
 - ; (ponto e vírgula = separador no ficheiro CSV, que deve ser importado para a administração Online do AirKey)
- > O Excel não pode guardar os dados diretamente no formato UTF-8. Por isso, é necessário, em primeiro lugar, guardar os dados no formato Unicode.
- > Para tal, selecione no ponto do menu do Excel **Ficheiro** → **Guardar como** (ou prima a tecla F12).
- > Insira na janela de diálogo subsequente "Guardar como" o nome do ficheiro pretendido ❶.
- > Selecione na lista dropdown de **Guardar com o tipo** ❷ o formato **Texto Unicode (*.txt)**.
- > Clique em **Guardar** ❸.

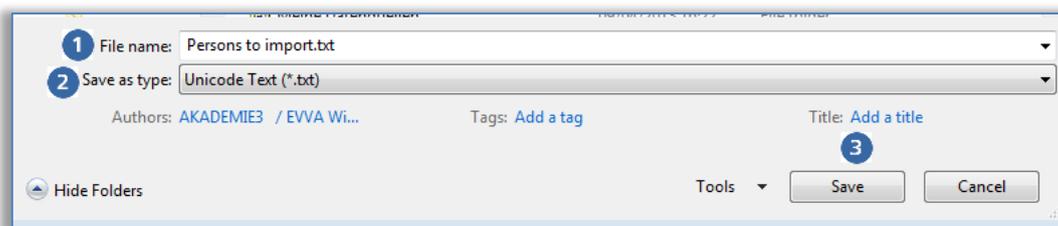


Figura 32: Excel – Guardar como – "Texto Unicode (*.txt)"

- > Confirme a pergunta do Excel a respeito do "Texto Unicode" com **Sim**.

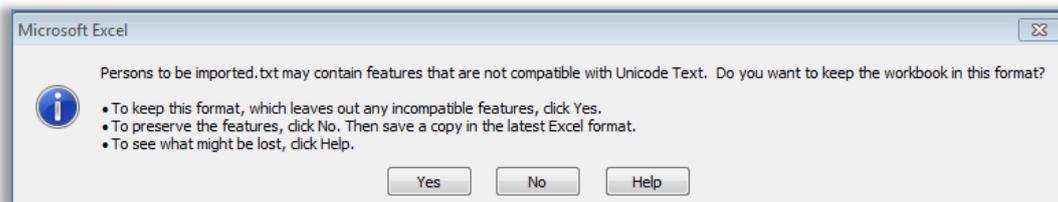


Figura 33: Excel – Confirmar Guardar como "Texto Unicode (*.txt)"

- > Abra o ficheiro (*.txt) criado com um editor de texto. O Windows™ utiliza, por defeito, o **Editor** do programa.
- > O separador no ficheiro de texto Unicode é o espaço executado pelo tabulador. Todos os espaços de tabulação têm de ser substituídos por pontos e vírgulas (;). Para tal, marque, primeiro, o espaço de tabulação entre 2 campos e copie-o.

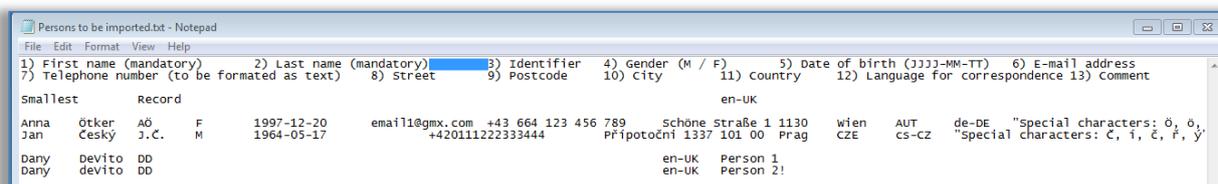


Figura 34: Ficheiro de texto no "Editor" – marcar o espaço de tabulação e copiar para a área de transferência

- > Selecione no **Editor** o ponto do menu **Editar** → **Substituir**, para abrir a janela de diálogo "Substituir".
 - A partir da área de transferência, insira no campo **Localizar** o carácter relativo ao espaço de tabulação, pois este carácter não pode ser digitado aqui diretamente.
 - Insira no campo **Substituir por** um ponto e vírgula (;).
 - Clique em **Substituir tudo** ①.

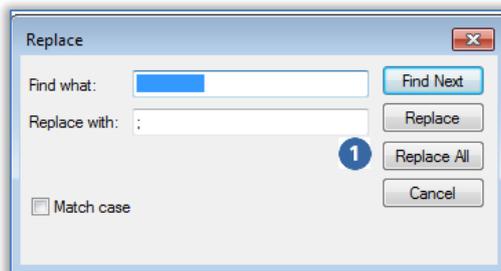


Figura 35: "Editor" – substituir todos os espaços de tabulação por pontos e vírgulas

- > Feche a janela de diálogo "Substituir" e selecione no **Editor** o ponto do menu **Editar** → **Guardar como** para abrir a janela de diálogo "Substituir".
 - Altere, manualmente, a terminação .txt do ficheiro para .csv no campo **Nome de ficheiro** ❶. Será mais complicado executar uma renomeação posteriormente!
 - Selecione na lista dropdown **Codificação** ❷ o formato **UTF-8**.
 - Clique em **Guardar** ❸.

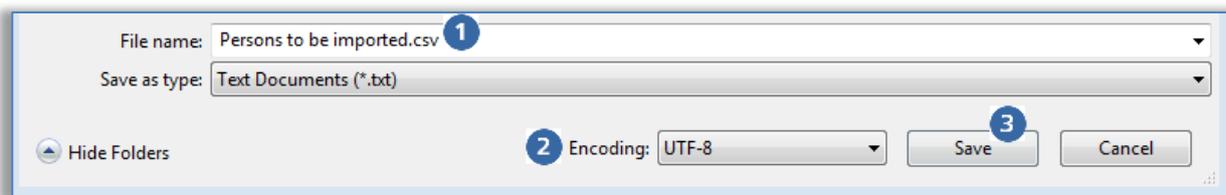


Figura 36: "Editor" – Guardar como – inserir, manualmente, a terminação .csv do ficheiro e seleccionar a codificação UTF-8

- > O ficheiro CSV, assim criado, pode agora ser importado para a administração Online do AirKey.



O ficheiro CSV pode ser diretamente aberto com o Excel. Não faça **NENHUMA** alteração ao ficheiro CSV no Excel, pois, ao guardar, a codificação UTF-8 será alterada!

Podem ser realizadas, posteriormente, pequenas alterações aos dados pessoais no ficheiro CSV, se, p. ex., este for aberto com o **Editor** e, depois, guardado.

Para efetuar alterações mais abrangentes aos dados pessoais, recomendamos alterar os dados no ficheiro original do Excel e repetir todo o processo de criação do ficheiro CSV no formato UTF-8.

Importação do ficheiro CSV no formato UTF-8 para a administração Online do AirKey

Para importar um ficheiro CSV com dados de pessoas, realize o seguinte:

- > Na página inicial **Home**, selecione a caixa de seleção **Pessoas**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Pessoas**.
- > Clique à direita em **Importar** ❶.

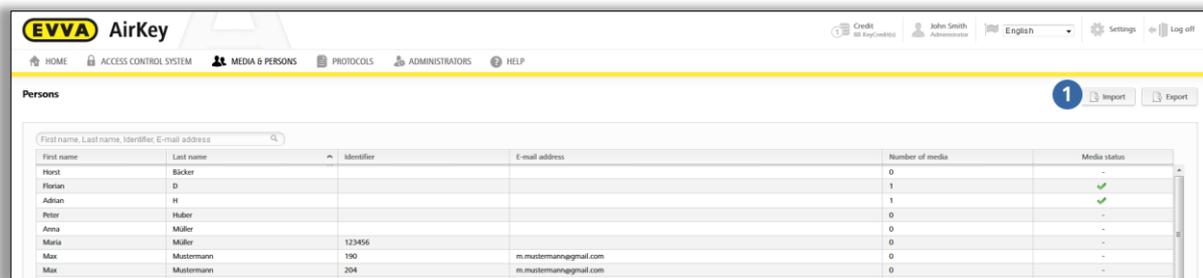


Figura 37: Importar Pessoas

- > Selecione **Selecionar ficheiro**.
- > Selecione o ficheiro CSV que pretende importar.
- > Obterá uma vista geral das pessoas a importar.
- > Clique em **Iniciar a importação** 1.

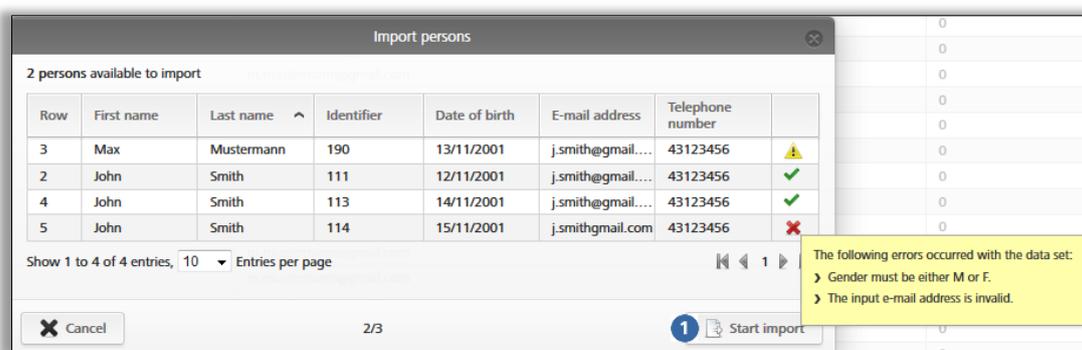


Figura 38: Importar Pessoas

- > Recebe uma mensagem de confirmação da importação de muitas pessoas com sucesso e sobre que linhas continham erro.
- > Clique em **Fechar**.

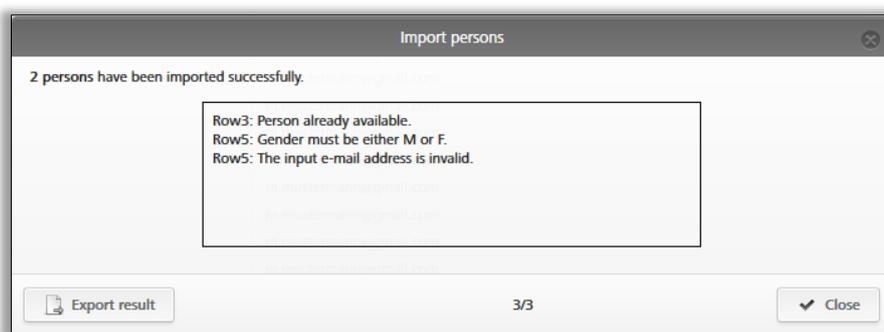


Figura 39: Importar pessoas – Resultado

- > Na Administração online do AirKey irá ser encaminhado automaticamente para a lista geral das pessoas.
- > Para atribuir às respetivas pessoas as autorizações de acesso pretendidas como é habitual, poderá ser feito para cada pessoa como descrito em [Atribuir meio a uma pessoa](#). Autorizações de acesso idênticas podem ser reproduzidas em duplicado rápida e facilmente. Poderá encontrar informações a este respeito em [Duplicar meio](#).

4.8 Criar smartphone

Para administrar um smartphone no seu sistema de controlo de acessos, tem de, em primeiro lugar, criá-lo e adicioná-lo.

- > Clique na página inicial **Home**, na barra cinzenta **Adicionar**, selecione no bloco de **Adicionar Meios e Pessoas** → **Adicionar meio**.
- > Ou selecione, na página inicial **Home**, a caixa de seleção **Smartphones** → **Adicionar meio**.
- > Ou selecione no menu principal **Meios e Pessoas** → **Adicionar meio**.

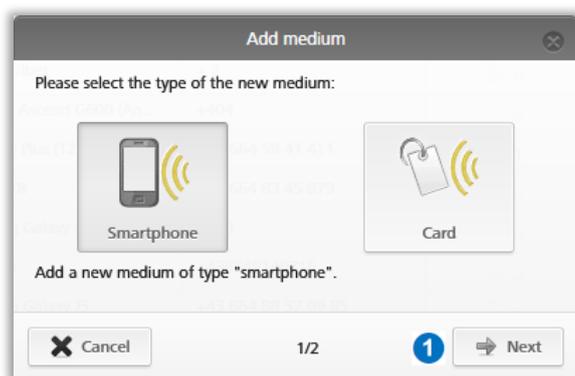


Figura 40: Novo meio smartphone ou cartão

- > Selecione como novo meio **Smartphone** e clique em **Seguinte** 1.
- > No campo "Designação", insira informações pertinentes (p. ex., o modelo de smartphone).
- > Insira o número de telefone do smartphone. O número de telefone deve começar com **+** e o código do país, e pode conter um máximo de 50 caracteres (+, 0-9 e espaços).
- > Clique em **Adicionar meio** 1.

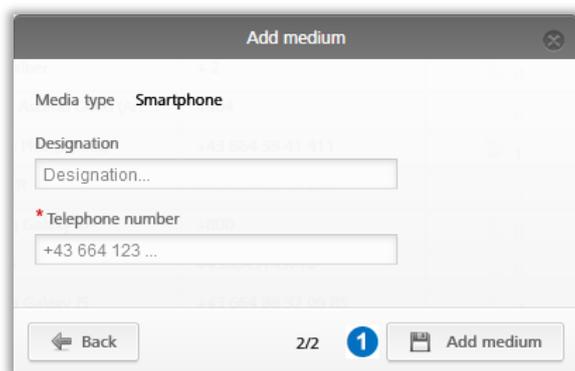


Figura 41: Criar novo meio



Se o número de telefone for inválido ou já tiver sido criado, receberá uma mensagem de erro.

Encontra-se agora na área de detalhes deste smartphone.

- > Clique em **Criar código de registo** , caso não tenha sido ainda criado nenhum código de registo.

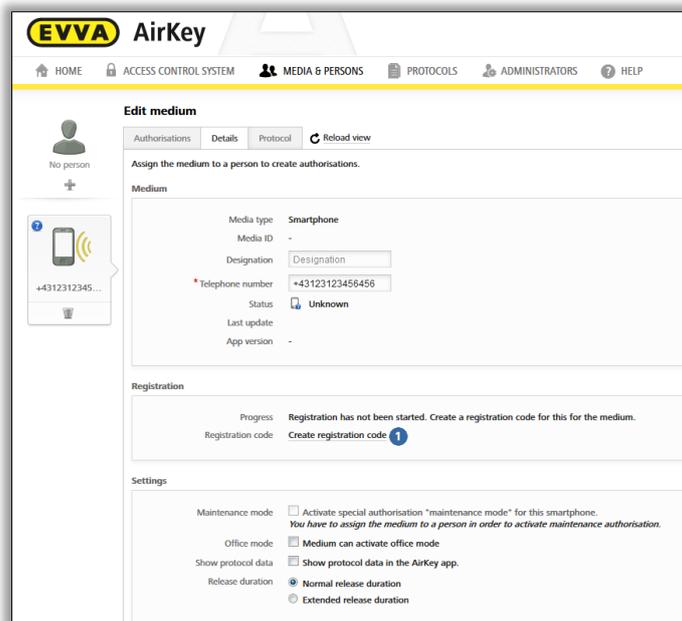


Figura 42: Criar código de registo

No bloco de **Registo**, é exibido um código de registo válido com a sua data de validade. Também poderá enviar este via SMS. Para isso, basta clicar no link correspondente. É indicada a data e hora exatas, quando for enviado o código de registo via SMA.

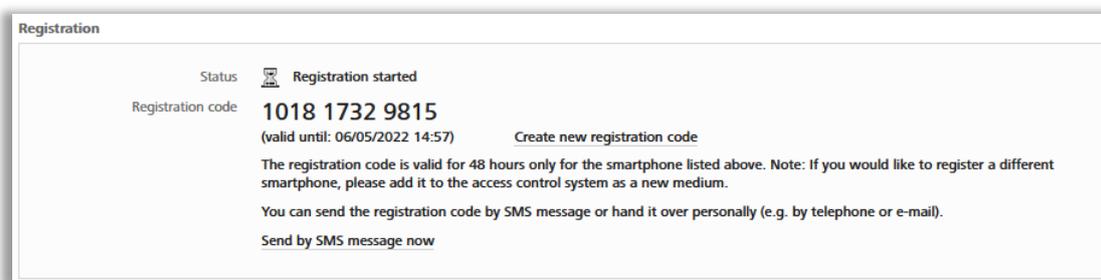


Figura 43: Código de registo

No bloco **Definições**, no âmbito dos detalhes do smartphone, poderá definir as configurações seguintes:

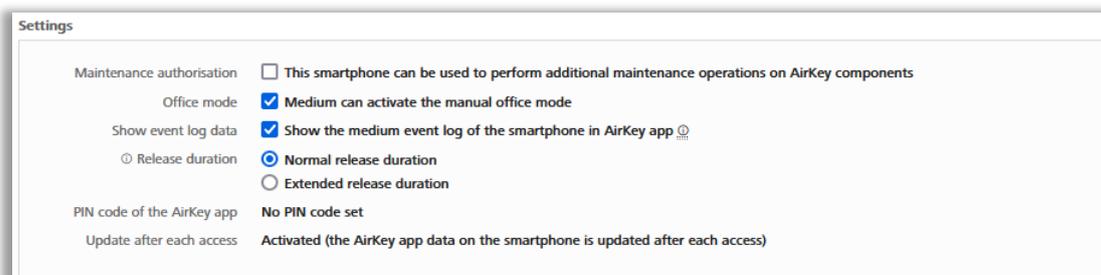


Figura 44: Editar meio – Definições

- > **Autorização de manutenção:** esta autorização especial apenas pode ser ativada em smartphones que já foram atribuídos a uma pessoa. Desta forma, o smartphone recebe a autorização, para desbloquear componentes de bloqueio no estado de fábrica, bem como para adicionar ou remover componentes de bloqueio e meios do sistema de controlo de acessos AirKey. Além disso, os firmwares de componentes de bloqueio e meios Keyring podem ser atualizados.
- > **Este meio pode ativar a abertura permanente manual:** se esta opção tiver sido selecionada, o meio de acesso pode mudar o componente de bloqueio para o estado de [abertura permanente automática](#). O meio tem, no entanto, de ter uma autorização válida para o componente de bloqueio.
- > **Mostrar o protocolo de meio do smartphone na aplicação AirKey:** com esta opção, a pessoa vê na aplicação AirKey as suas próprias ocorrências em termos de acesso e outros dados protocolares relevantes para o seu meio.
- > **Tempo de ativação:** fica determinado o tempo durante o qual a ativação do componente de bloqueio se mantém no caso de um bloqueio com este smartphone. Os tempos de ativação com duração normal ou alargada são determinados para os componentes de bloqueio (de 1-250 segundos).
- > **Código PIN na aplicação AirKey:** indica o estado, se este smartphone tem o bloqueio com código PIN ativado na aplicação AirKey, ou não. Se este estiver ativado e a pessoa se tiver esquecido do seu código PIN, dado o caso, é possível proceder a uma reposição.
- > **Atualização após cada acesso:** fornece o estado, ou seja, se os dados da AirKey App deste smartphone são automaticamente atualizados após cada processo de acesso, ou não. Poderá encontrar detalhes para a ativação desta função no capítulo [Geral](#).

4.9 Registrar smartphone

O smartphone pode ser registado se já tiver sido criado num sistema de controlo de acessos e se conhecer o código de registo.

- > Inicie a aplicação AirKey no seu smartphone.
- > Aceite o acordo de licença e os eventuais controlos para acesso a determinados serviços do smartphone.
- > Se o smartphone ainda não estiver conectado a nenhum sistema de controlo de acessos, a caixa de diálogo para a introdução do código de registo é automaticamente exibida.



Em smartphones iOS, toque em **Código de registo já recebido** para saltar a introdução do número de telefone e para aceitar a introdução do código de registo.

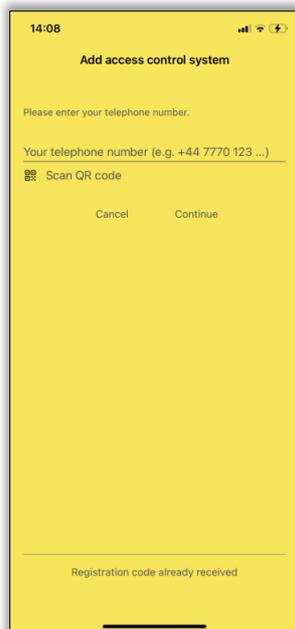


Figura 45: AirKey App – Adicionar sistema de controlo de acessos (iOS)

- > Introduza o código de registo que recebeu do administrador do sistema de controlo de acessos AirKey.

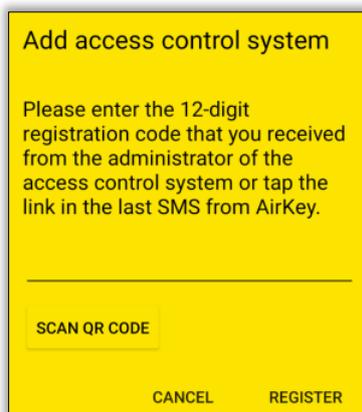


Figura 46: Aplicação AirKey – Adicionar sistema de controlo de acessos (Android)

- > Confirme a sua introdução com **Registar**.



Poderá registar um smartphone igualmente em vários sistemas de bloqueio AirKey. Para voltar a abrir a caixa de diálogo de registo, seleccione, no menu principal da aplicação AirKey, **Definições** → **Adicionar sistema de controlo de acessos**. Poderá encontrar mais informações a este respeito no capítulo [Utilizar o smartphone em vários sistemas](#).



Se o código de registo for inválido ou tiver expirado, receberá uma mensagem de erro. Neste caso, contacte o administrador do sistema de controlo de acessos, de quem recebeu o código de registo.



O botão **Ler o código QR** só é necessário em combinação com a troca do smartphone. Poderá encontrar detalhes sobre a troca do smartphone no capítulo [Troca de smartphone](#).

Se tiver eliminado a aplicação AirKey ou os dados da aplicação, existe a possibilidade de transferir as autorizações já emitidas para o smartphone sem uso do crédito novamente. Isto aplica-se, no entanto, apenas para o mesmo dispositivo e o seu sistema de controlo de acessos. Caso haja uma troca de dispositivos, isto não será possível. [Poderá obter mais informações a respeito da troca fácil do dispositivo no capítulo Troca de smartphone](#).

- > Na página inicial **Home**, selecione a caixa de seleção **Smartphones**.
- > Ou selecione na linha de cabeçalho à esquerda **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no smartphone em questão.
- > Clique em **Criar novo código de registo** e comunique o código de registo criado à pessoa que pretende registar o smartphone ao sistema de controlo de acessos. Ou envie-os diretamente por SMS ao smartphone.
- > Insira o código de registo na aplicação AirKey – o smartphone é registado no sistema de controlo de acessos.



Se o seu smartphone já tiver sido registado num sistema de controlo de acessos AirKey e não tiver sido removido deste corretamente, se os dados da aplicação tiverem sido eliminados e o smartphone for registado num outro sistema de controlo de acessos AirKey, é emitida uma mensagem a informar que o smartphone já foi registado num sistema de controlo de acessos AirKey. Se ignorar a mensagem, o smartphone pode ser registado como habitualmente. Será criado como novo meio, todos os dados até agora associados serão inutilizados.



A EVVA recomenda a atribuição de um PIN. Este é utilizado como mais um nível de segurança e pode ser, posteriormente, ativado ou desativado. Poderá encontrar mais informações a este respeito em [Ativar PIN](#).

4.9.1 Função "Send a Key"

Poderá enviar a todas as pessoas que possuem um smartphone uma "chave" também pela função "Send a Key". Esta função pode ser utilizada por um administrador e poupa ao proprietário do smartphone a introdução manual do código de registo para um novo sistema de controlo de acessos.

- > Clique no botão **"Send a Key"**.

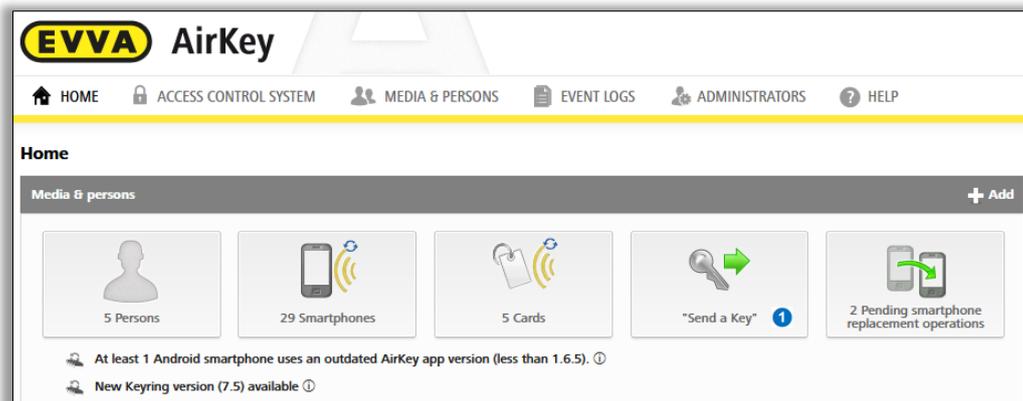


Figura 47: "Send a Key"

- › Insira no campo de pesquisa um nome de pessoa, uma identificação etc. Se souber que o perfil da pessoa ainda não foi criado, selecione **Criar novo**.

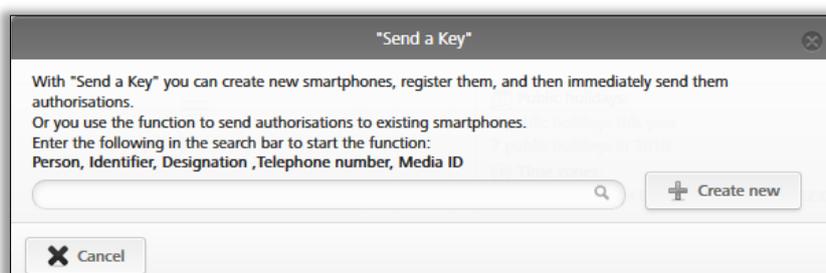


Figura 48: "Send a Key" – Campo de pesquisa

- › Assim que todos os campos obrigatórios estiverem preenchidos, clique em **Continuar**. É imediatamente enviada uma SMS à pessoa-alvo, onde está incluído um link com o código de registo para a aplicação AirKey. Se, nas configurações gerais, tiver sido selecionado um texto próprio para SMS "Send a Key", é possível adaptar ou personalizar novamente o texto da SMS. (Consulte o capítulo [Informações gerais](#) para obter informações sobre definições gerais.)

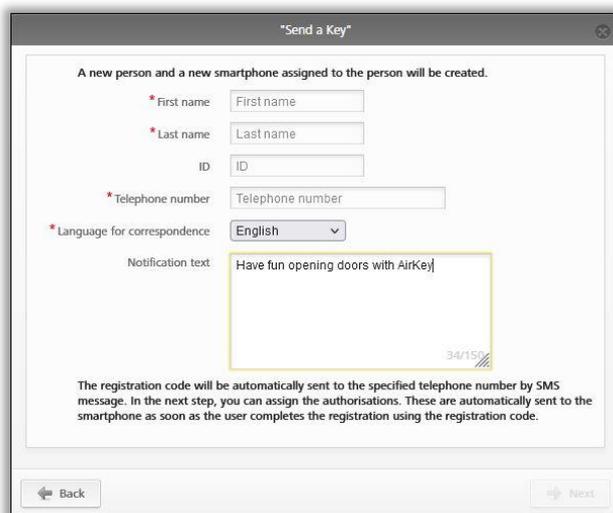


Figura 49: "Send a Key" – Criar pessoa



De acordo com a disponibilidade de rede do smartphone, poderá demorar algum tempo até que a SMS com o código de registo seja recebida.

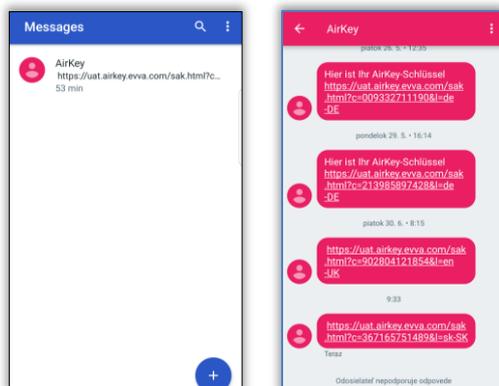


Figura 50: SMS com link – aqui apresentado com o Samsung Galaxy S7 Edge

- Após abrir o link da SMS com a ajuda do AirKey, o registo é automaticamente iniciado e executado.

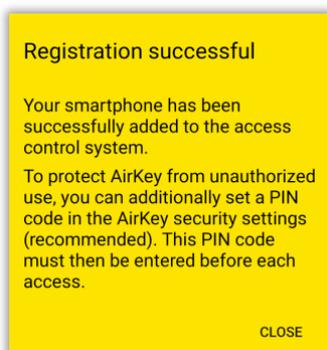


Figura 51: Registo com sucesso



Se a aplicação AirKey ainda não estiver instalada no smartphone, aplica-se o procedimento seguinte:

- Clique no link exibido na SMS e instale a aplicação no smartphone.
- Inicie a aplicação AirKey.
- Em smartphones Android, o registo é automaticamente iniciado e executado. Nos smartphones iOS, introduza o seu número de telefone e confirme com **Continuar**. (O botão **Ler código QR** só é necessário em combinação com a troca do smartphone. Poderá encontrar detalhes sobre a troca do smartphone no capítulo [Troca de smartphone](#).)



Figura 52: Registrar o número de telefone (iOS)

- > Receberá uma nova SMS. Permaneça ainda na aplicação AirKey e selecione o código de registo de 8 dígitos, o qual é exibido acima do teclado.

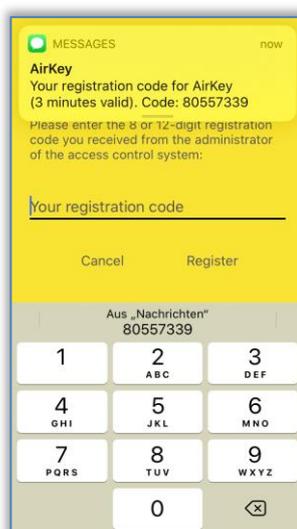


Figura 53: Código de registo (iOS)

Se o código de registo de 8 dígitos não for exibido como sugestão ou tiver fechado, entretanto, a aplicação AirKey, terá de copiar o código de registo de 8 dígitos da SMS e inserir na aplicação AirKey.

- > Conclua o registo com **Registrar**.

Na Administração online do AirKey, é-se encaminhado para a exibição de autorizações **Editar meio** e pode-se criar as autorizações pretendidas. Com Drag & Drop, arraste o respetivo componente de bloqueio, para o qual deve ser concedida a autorização de acesso,

para o tipo de acesso (acesso permanente, acesso, acesso periódico, acesso individual) – ver também [Atribuir autorizações](#).

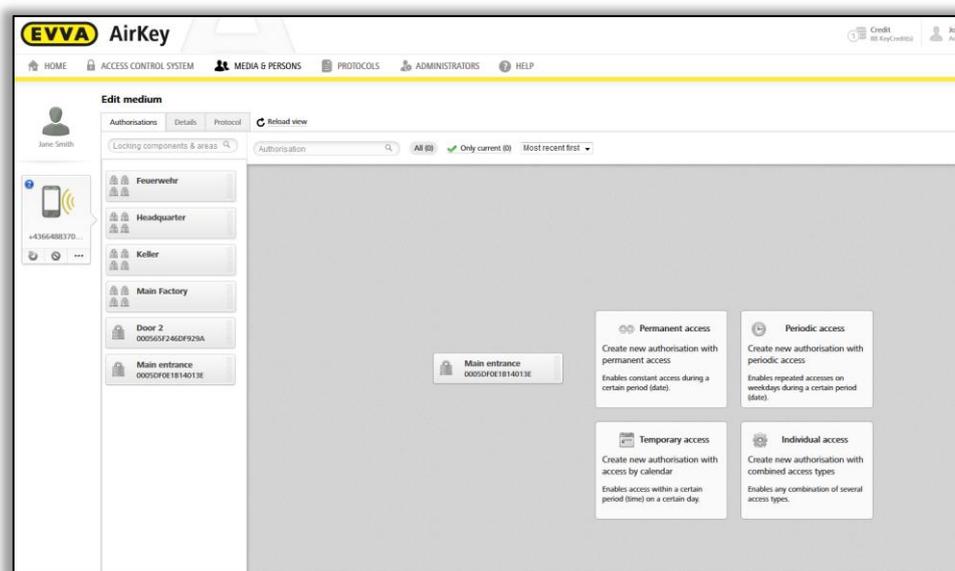


Figura 54: Tipos de acesso

4.10 Instalar os componentes de bloqueio

4.10.1 Cilindro AirKey

Para a montagem do cilindro AirKey, cilindro híbrido AirKey, cilindro de patilha AirKey e cadeado AirKey, observe as instruções de montagem entregues com a embalagem ou veja o vídeo online com as instruções de montagem em <https://www.evva.com/pt/airkey/website/>.



No caso de cilindro AirKey com acesso bilateral, tem se garantir de que os dois lados estão configurados no âmbito do sistema de controlo de acessos AirKey, para que não se fique trancado nem por dentro nem por fora.

4.10.2 Leitor de parede AirKey

Para a montagem do leitor de parede AirKey, tenha em atenção as instruções de montagem entregues com a embalagem. Além disso, na nossa homepage, poderá encontrar um molde de perfuração ou um vídeo com instruções de montagem em <https://www.evva.com/pt/airkey/website/>.



É necessária uma unidade de controlo por leitor de parede. A unidade de controlo tem de ser montada na área de segurança interna. Verifique os cabos de conexão entre o leitor de parede e a unidade de controlo.

Os componentes de bloqueio AirKey são fornecidos sempre no estado de fábrica.



- > Os meios no estado de fábrica bloqueiam os componentes de bloqueio no estado de fábrica.
- > Os smartphones com aplicação AirKey instalada e autorização de manutenção bloqueiam os componentes de bloqueio no estado de fábrica
- > No estado de fábrica não há registo de tentativas de bloqueio.
- > Uma autorização de bloqueio só é dada, depois de ter adicionado o componente de bloqueio AirKey a um sistema de controlo de acessos.
- > Para a montagem, observe as indicações incluídas no manual de instruções de montagem. Na montagem e desmontagem dos componentes de bloqueio, abra a porta e fixe-a de forma a que esta não possa fechar acidentalmente.

4.11 Adicionar componente de bloqueio

Os componentes de bloqueio são adicionados através de um smartphone com autorização de manutenção ou uma estação de codificação opcional ao sistema de controlo de acessos e têm de se encontrar no estado de fábrica.



Se pretender usar um smartphone, têm de ser preenchidos os seguintes pré-requisitos:

- > A aplicação AirKey está instalada.
- > Está disponível uma ligação ativa à Internet.
- > O smartphone está registado no sistema de controlo de acessos.
- > O smartphone está atribuído a uma pessoa.
- > A autorização de manutenção foi atribuída ao smartphone.

4.11.1 Adicionar componentes de bloqueio com o smartphone

- > Inicie a aplicação AirKey.
- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente 1**.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones **Android**): toque no caso do componente de bloqueio no estado de fábrica, que pretende adicionar no seu sistema de controlo de acessos, no menu contextual (:) e selecione, depois, **Conectar 2**.
- > Se estabelecer a ligação por **Bluetooth** (em **iPhones**): deslize no caso do componente de bloqueio no estado de fábrica, que pretende adicionar no seu sistema de controlo de acessos, a designação "No estado de fábrica" para a esquerda e selecione, depois, **Conectar 3**.

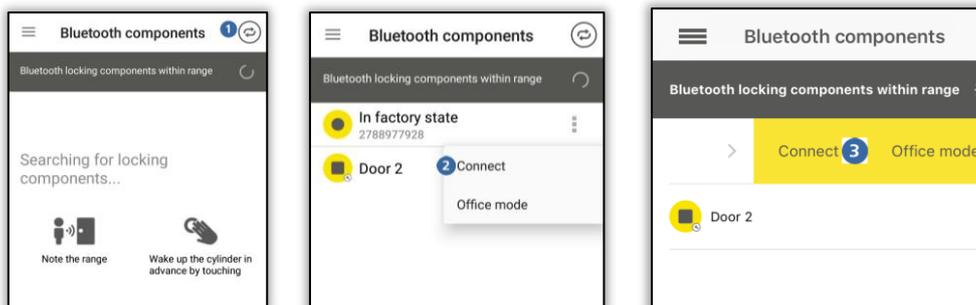


Figura 55: Aplicação AirKey – Conecte com o componente (por NFC no caso de smartphone Android / por Bluetooth no caso de Smartphone Android / por Bluetooth no caso de iPhone)

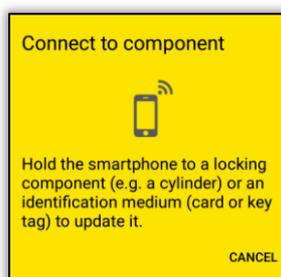


Figura 56: Aplicação AirKey – Conecte com o componente

- > Encoste o smartphone ao componente de bloqueio no estado de fábrica (no caso de ligação por NFC) para estabelecer a ligação. A ligação é automaticamente estabelecida via Bluetooth. Em nenhum caso afaste o smartphone do componente de bloqueio enquanto a ligação estiver a ser estabelecida.



Figura 57: Aplicação AirKey – A ligação está a ser estabelecida

- > Neste momento, obterá as informações sobre o componente de bloqueio.

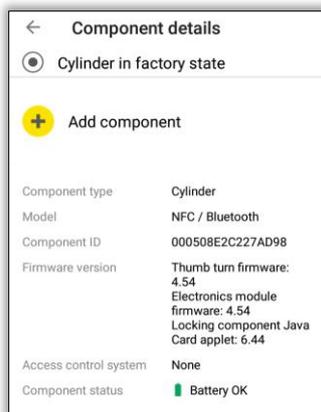


Figura 58: Adicionar componente

- > Toque em **Adicionar componente**.
- > Insira uma designação inequívoca para o componente de bloqueio.



No caso de cilindro com acesso bilateral, tem de se garantir de que os dois lados estão configurados no âmbito do sistema AirKey. Denomine os dois lados de um cilindro com acesso bilateral com designações inequívocas. Adote uma área abrangida pelos dois lados do cilindro e atribua uma autorização de área, para se receber a autorização a ambos os lados.

- > Se o smartphone estiver registado em vários sistemas de bloqueio com modo de manutenção ativo, selecione o sistema de controlo de acessos, ao qual o componente de bloqueio deva ser adicionado.

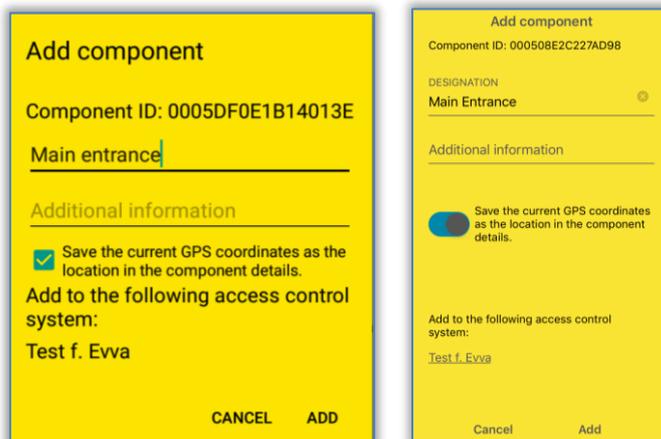


Figura 59: Aplicação AirKey – Adicionar componente de bloqueio Android / iPhone

- > Toque em **Adicionar**.
- > Encoste novamente o smartphone ao componente de bloqueio no estado de fábrica (no caso de ligação por NFC) para estabelecer a ligação. A ligação é automaticamente estabelecida via Bluetooth.



Os dados são verificados e o componente de bloqueio é atualizado. Durante este processo, não afaste o smartphone do componente de bloqueio.

- > O processo é concluído com uma mensagem de confirmação. O componente de bloqueio está agora disponível na Administração online do AirKey para continuar a ser administrado.

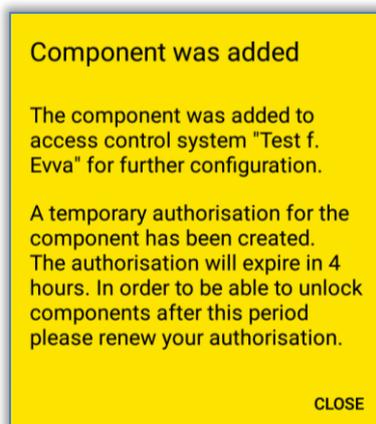


Figura 60: Aplicação AirKey – Componente de bloqueio adicionado

O componente de bloqueio é exibido na lista geral de componentes de bloqueio na Administração online do AirKey. Ao adicionar o componente de bloqueio, se tiverem sido averiguadas as coordenadas de GPS , estas podem ser encontradas na Administração online do AirKey no componente de bloqueio sob o separador **Detalhes** no bloco "Porta".

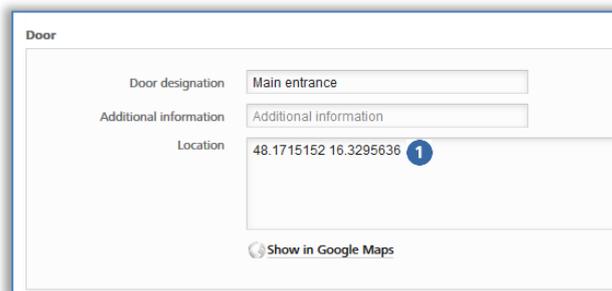


Figura 61: Coordenadas de GPS nos Detalhes do componente de bloqueio

Em alternativa, no campo "Localização", pode ser inserido o endereço, sob o qual o componente de bloqueio pode ser encontrado.



O componente de bloqueio, agora, já não se encontra no estado de fábrica. Os meios no estado de fábrica ou os smartphones com modo de manutenção já não estão autorizados. O smartphone que o componente de bloqueio adicionou, é automaticamente autorizado durante 4 horas. Altere esta autorização oportunamente ou atribua outros meios com uma autorização válida, para obter acesso a este componente de bloqueio.

4.11.2 Adicionar componente de bloqueio com a estação de codificação

Option

Para adicionar o componente de bloqueio com a estação de codificação, proceda da seguinte forma:

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **leitor de parede**.
- > Clique no botão Adicionar componente de bloqueio 1.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componentes de bloqueio.

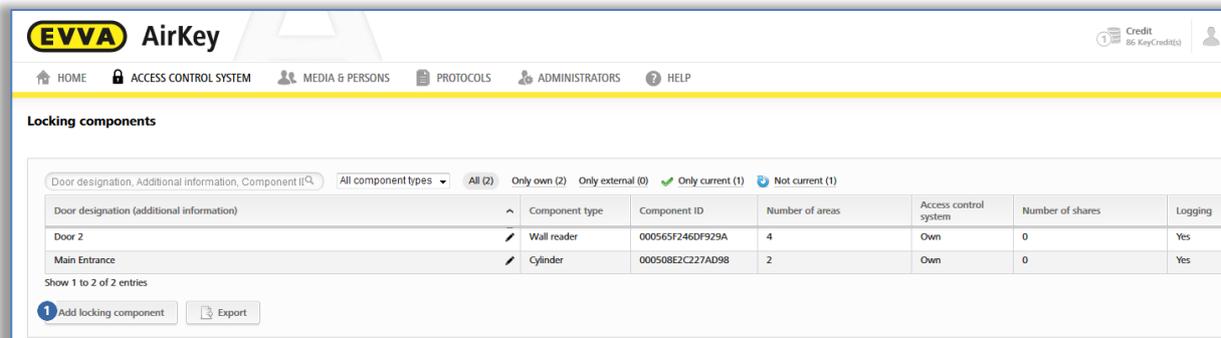


Figura 62: Adicionar componente de bloqueio

- > Ligue a estação de codificação ao computador, caso contrário surge uma indicação do sistema 1.

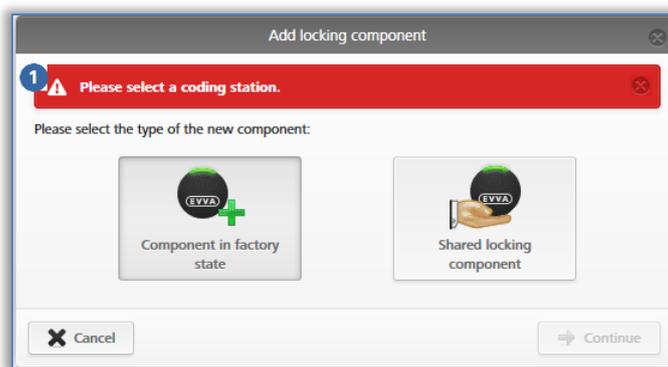


Figura 63: Adicionar componente de bloqueio / sem estação de codificação

- > Selecione **Componente no estado de fábrica**.
- > Clique em **Continuar**.
- > No próxima caixa de diálogo, insira a designação da porta e clique em **Continuar**.

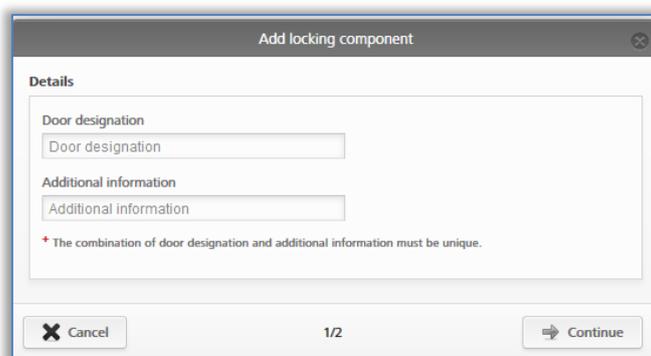


Figura 64: Adicionar componente de bloqueio – Atribuição do nome

- > Siga as instruções e coloque o componente de bloqueio sobre a estação de codificação.

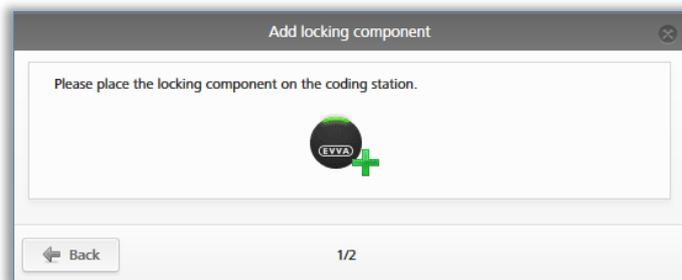


Figura 65: Adicionar componente de bloqueio

- > Aparece uma mensagem de confirmação e o componente de bloqueio foi adicionado ao sistema de controlo de acessos AirKey.

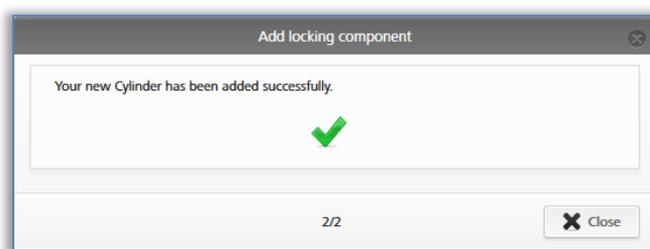


Figura 66: Adicionar componente de bloqueio – Mensagem de confirmação do processo

Depois de fechar a mensagem de confirmação do processo, acede à vista dos detalhes do componente de bloqueio.

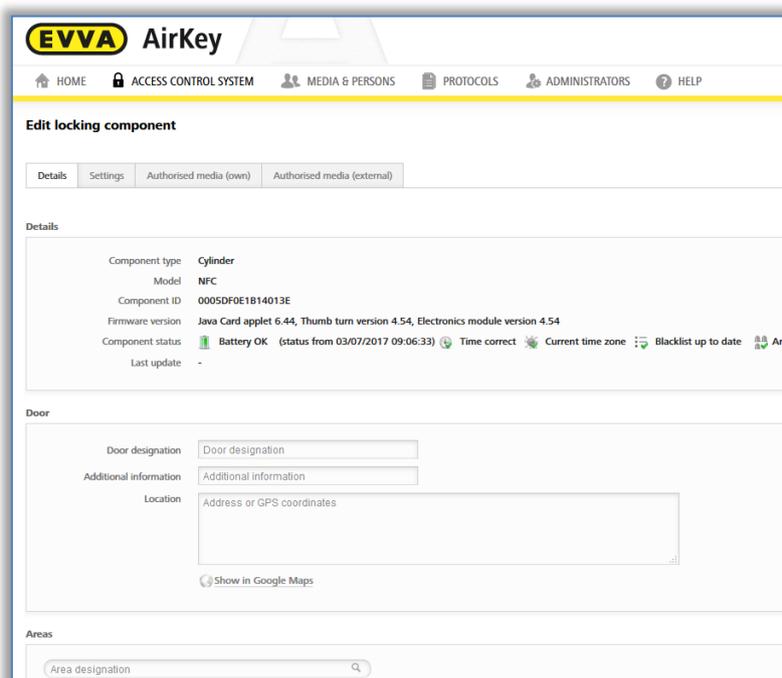


Figura 67: Detalhes do componente de bloqueio



O componente de bloqueio, agora, já não se encontra no estado de fábrica. Os meios no estado de fábrica ou os smartphones com autorização de manutenção já não estão autorizados a bloquear o componente de bloqueio. Adicione um meio ou smartphone ao sistema de controlo de acessos e atribua uma autorização válida para o componente de bloqueio para poder continuar a bloquear.



O fuso horário predefinido e as definições da proteção de dados são automaticamente configurados para o componente de bloqueio adicionado de acordo com cada definição selecionada. Poderá obter mais informações a respeito das definições em [Valores predefinidos \(para todos os componentes de bloqueio recentemente adicionados\)](#).



Em alternativa, poderá colocar simplesmente um componente de bloqueio no estado de fábrica sobre a estação de codificação. Do lado direito, em baixo, aparece uma janela informativa, com a qual pode igualmente adicionar ao sistema de controlo de acessos AirKey o componente de bloqueio através do link **Adicionar componente ao meu sistema de controlo de acessos**.



Figura 68: Adicionar componente ao meu sistema de controlo de acessos

4.12 Adicionar cartões, porta-chaves, pulseiras e chaves combinadas com o smartphone

Os meios de acesso no estado de fábrica são adicionados ao sistema de controlo de acessos AirKey através de um smartphone com autorização de manutenção ou uma estação de codificação opcional.



Para adicionar uma chave combinada com o smartphone, a chave combinada tem de ser mantida encostada ao smartphone, com o lado que tem o símbolo RFID. A chave combinada, na maioria dos modelos, tem de ser mantida diretamente encostada ao smartphone.

Esta ação apenas pode ser realizada com um smartphone Android que suporte NFC. Para adicionar meios por Bluetooth com um smartphone Android ou com um iPhone, ver o capítulo [Codificar meios](#).

- > Inicie a aplicação AirKey.
- > Toque no símbolo **Conecte com o componente** 1.

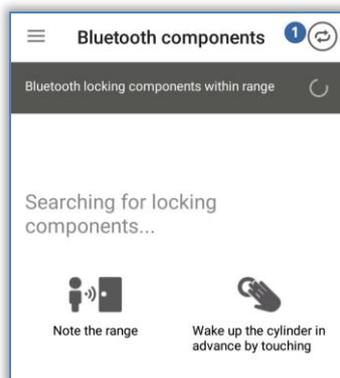


Figura 69: Aplicação AirKey – Conecte com o componente

- > Mantenha o smartphone encostado ao meio no estado de fábrica. É estabelecida a conexão para o meio.

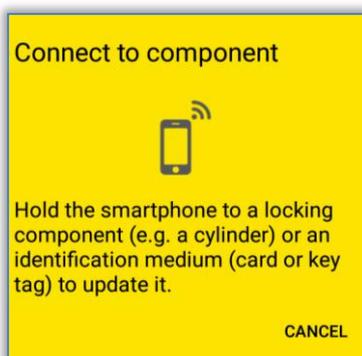


Figura 70: Aplicação AirKey – A ligação está a ser estabelecida

- > Em nenhum caso afaste o meio do smartphone enquanto a ligação estiver a ser estabelecida. Neste momento, obterá as informações sobre o meio.

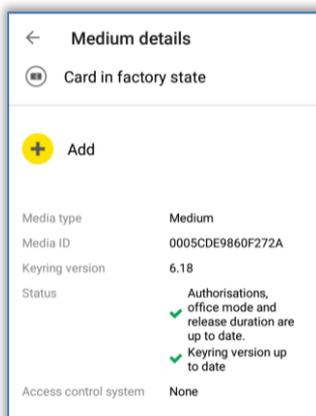


Figura 71: Detalhes do meio

- > Toque em **Adicionar**.
- > Insira um nome para o meio.

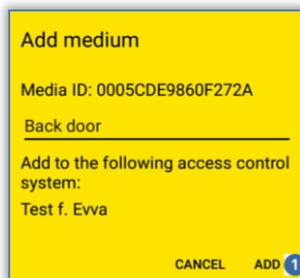


Figura 72: Adicionar meio – Atribuir um nome

- > Se o smartphone estiver registado em vários sistemas de bloqueio, selecione o sistema de controlo de acessos, ao qual o meio deva ser adicionado.
- > Toque em **Adicionar** 1.
- > Agora, mantenha novamente o smartphone encostado ao meio para concluir o processo.
- > O processo é concluído com uma mensagem de confirmação. O meio encontra-se agora à disposição na Administração online do AirKey – e tem ainda de ser atribuído a uma pessoa.



Este processo é idêntico para cartões, porta-chaves, pulseiras e chaves combinadas. Todos os três são realizados sob o nome "Cartão".

4.13 Atribuir uma pessoa a um meio

No passo seguinte, tem de atribuir o meio a uma pessoa no âmbito da Administração online do AirKey para poder atribuir autorizações. Só assim obterá uma referência pessoal nos acessos.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista dos meios, no meio ao qual não foi ainda atribuída nenhuma pessoa.
- > Clique no botão **Sem pessoa** sobre o sinal **+** 1

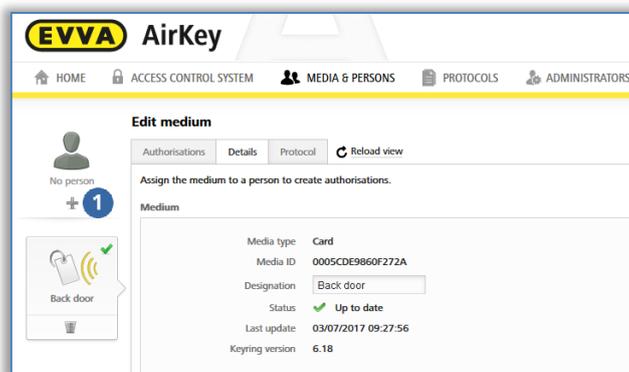


Figura 73: Atribuir pessoa

- > Selecione da lista de pessoas a pessoa a quem este meio deva ser atribuído.

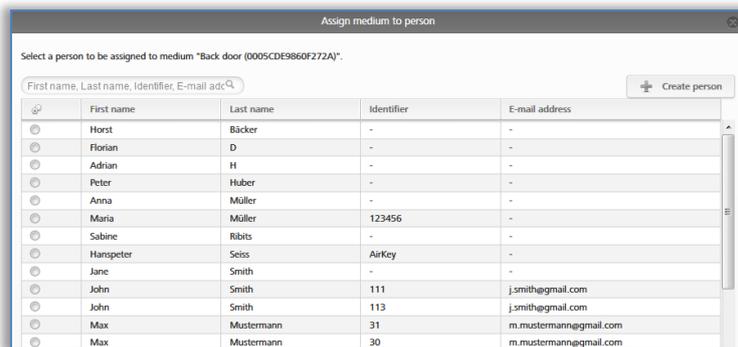


Figura 74: Atribuir pessoa ao meio

- > Caso a pessoa pretendida ainda não esteja criada, o botão **Criar pessoa** aqui disponível permite-lhe ter acesso à segunda janela de diálogo "Atribuir meio à pessoa".
- > Confirme a pessoa selecionada para ser atribuída ao meio, com **Atribuir pessoa 1**.



Figura 75: Confirmar pessoa

- > Ver mais em [Atribuir autorizações](#).



Em alternativa, poderá fazer a atribuição de um meio à pessoa através do meio. Poderá encontrar mais informações em [Atribuir meio a uma pessoa](#).

4.14 Atribuir autorizações



Tenha em atenção que as autorizações só podem ser atribuídas se um meio tiver sido atribuído a uma pessoa.

- > Selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desejado.
- > Contanto que o meio esteja atribuído a uma pessoa, aparece a vista geral das autorizações do meio.
- > Assim que selecionar o respetivo componente de bloqueio e arrastar para a área cinzenta, aparecem os possíveis tipos de acesso nas áreas com moldura pontilhada.

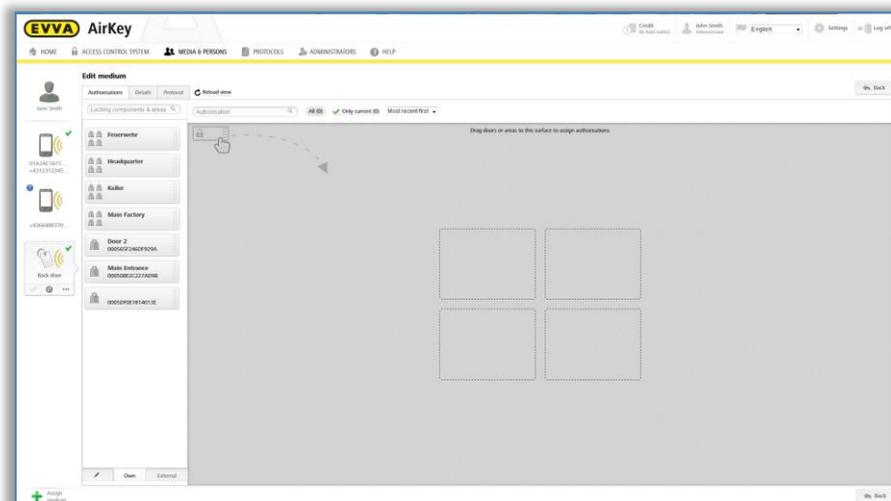


Figura 76: Atribuir autorização

- > Selecione o tipo de acesso pretendido, arrastando por Drag & Drop a porta selecionada / a área selecionada para o campo correspondente.



Existem quatro tipos de acesso à disposição:

- > Acesso permanente
- > Acesso periódico
- > Acesso temporário
- > Acesso individual

4.14.1 Acesso permanente

Por acesso permanente entende-se que o acesso é possível durante 24 horas. Poderá limitar-se a autorização, selecionando uma data de início e de fim.

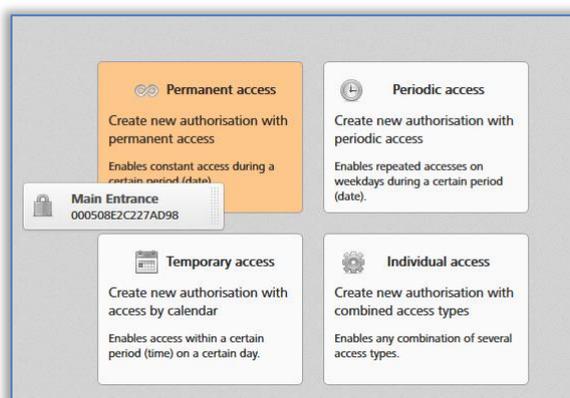


Figura 77: Atribuir uma autorização de acesso permanente

- > Defina o período para o acesso permanente. Poderá seleccionar entre um acesso permanente sem período limitado ou um acesso permanente com datas de início e de fim definidas.

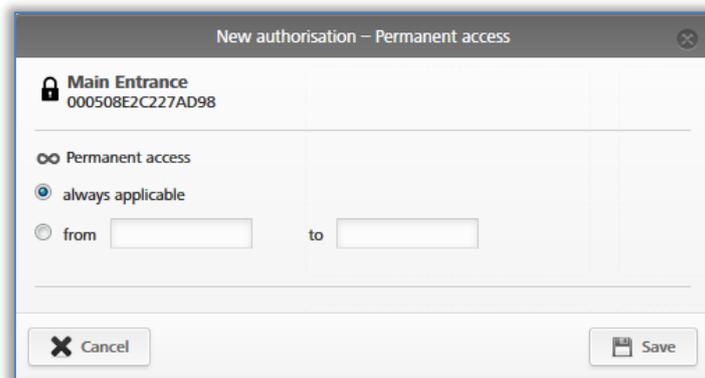


Figura 78: Atribuir uma autorização de acesso permanente

- > Clique em **Guardar**.

4.14.2 Acesso periódico

Atribua uma autorização de acesso periódico para acessos recorrentes durante um determinado período de tempo. Este acesso recorrente é comparável a um agendamento série, válido semanalmente.

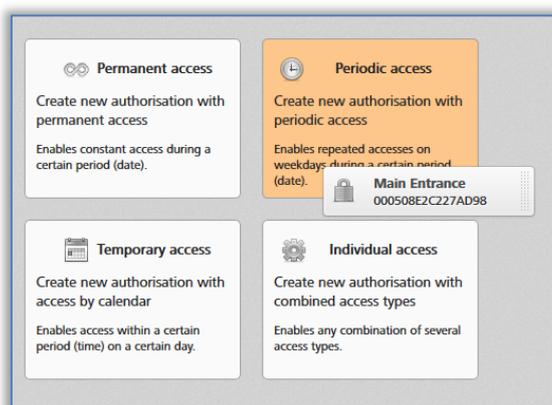


Figura 79: Atribuir acesso periódico

Será exibido no ecrã um calendário semanal, em que pode especificar até 4 intervalos de tempo.

- > Defina o período para o acesso periódico.

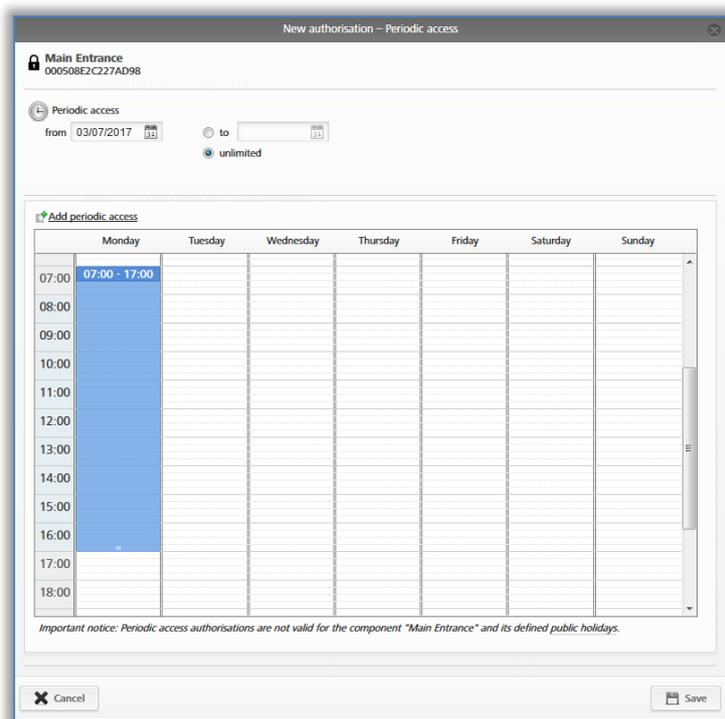


Figura 80: Atribuir acesso periódico

- > O período de tempo é definido marcando diretamente no calendário ou em **Adicionar acesso periódico**.

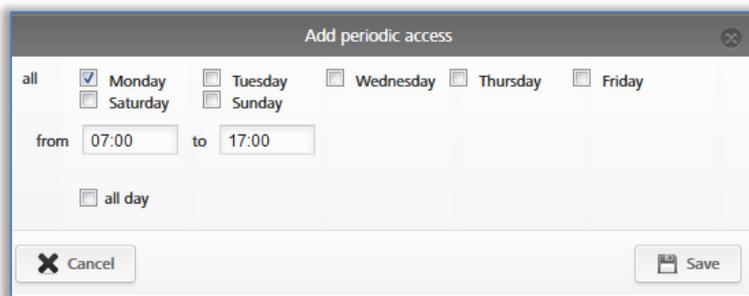


Figura 81: Adicionar acesso periódico

- > Insira o período de tempo pretendido e clique em **Guardar**.
- > Clique, na janela "Nova autorização – Acesso periódico", e novamente em **Guardar**.

4.14.3 Acesso temporário

Atribua uma autorização única se esta for válida somente para um determinado dia dentro de um determinado período de tempo.

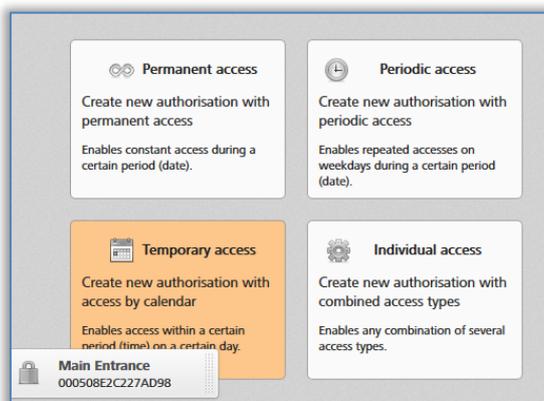


Figura 82: Atribuir autorização de acesso temporário

- > Insira o período de tempo pretendido e clique em **Guardar**.

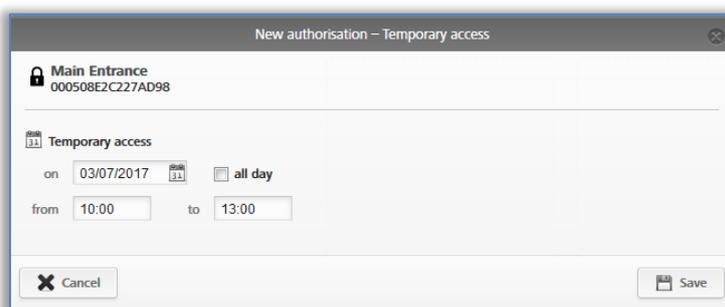


Figura 83: Atribuir autorização de acesso temporário

4.14.4 Acesso individual

Atribua uma autorização de acesso individual se precisar de uma combinação de acesso permanente, acesso individual e acesso periódico.

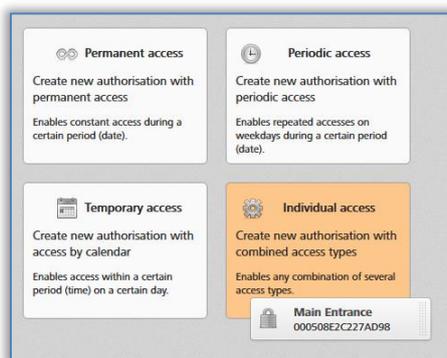


Figura 84: Atribuir acessos individuais

- > Na janela de diálogo "Nova autorização – Acesso individual", veja os acessos individuais já atribuídos.
- > Clique numa linha do registo para alterar a autorização ou

- > Clique em **Adicionar acesso** 1 para um novo registo.

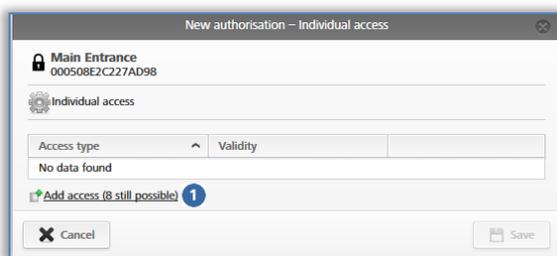


Figura 85: Nova autorização – Acesso individual

- > Selecione **acesso permanente**, **acesso periódico** ou **acesso temporário** e defina as especificações. Os parâmetros correspondem às autorizações de acesso já descritas.

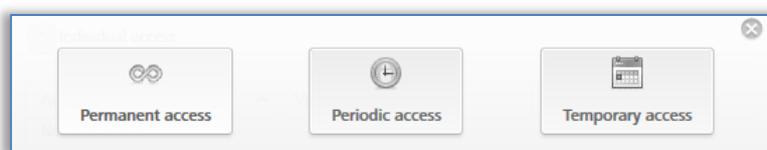


Figura 86: Nova autorização – Acesso individual

- > Clique em **Guardar**, quando todas as autorizações do acesso individual tiverem sido configuradas.



- > O acesso permanente e o acesso periódico não se podem sobrepor.
- > Por dia, apenas pode ser criado, no máximo, um acesso individual.
- > Caso se sobreponham um acesso individual e um acesso periódico, ambos são válidos.
- > Poderá combinar um máximo de 8 autorizações individuais.

4.15 Criar autorização

Depois de a autorização do acesso ter sido criada para um meio, terá de concluir o processo com **Criar autorização** e com uma última atualização do respetivo meio.



Figura 87: Criar autorização

Com a alteração de uma autorização existente ou a criação de uma nova autorização, muda o símbolo do respetivo meio. Caso ainda tenha créditos suficientes, poderá criar a autorização agora.

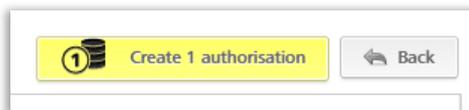


Figura 88: Criar autorização nova ou alterada

- > Clique no botão amarelo **Criar 1 autorização** ou no símbolo 1 do meio para criar a autorização e debitar um KeyCredit.



Caso, neste passo, já não disponha de mais créditos, aparece a respetiva mensagem. Poderá carregar o seu crédito de imediato através de um link incluído nesta mensagem. Se o crédito for carregado através desta mensagem, a autorização será automaticamente criada e um KeyCredit debitado.



Para que as autorizações sejam validadas no meio, os meios como, p. ex., cartões, porta-chaves, pulseiras ou chaves combinadas, têm de ser atualizados num smartphone ou numa estação de codificação. As autorizações são enviadas aos smartphones através de informações Push (notificações).

Neste capítulo da colocação em funcionamento aprendeu como adaptar o sistema AirKey no início. Com base nos pontos descritos, teve oportunidade de conhecer os primeiros passos e já pode administrar o seu sistema AirKey a partir destes. Poderá encontrar uma descrição mais precisa de cada uma das funções da Administração online do AirKey e da aplicação AirKey nos capítulos seguintes.

5 Administração Online do AirKey

5.1 Login no AirKey

O login é necessário para configurar e administrar o sistema de bloqueio AirKey. Nas definições da Administração online do AirKey, pode ser opcionalmente ativada a autenticação de dois fatores para o login. A ativação está descrita no capítulo [Definições do sistema de bloqueio AirKey](#).



Ative a autenticação de dois fatores para aumentar a segurança do seu sistema de bloqueio AirKey.



As tentativas de login falhadas são exibidas na página inicial e são registadas no protocolo do sistema. A indicação na página inicial só aparece se tiver ocorrido, pelo menos, uma tentativa de login falhada desde o último login bem-sucedido.

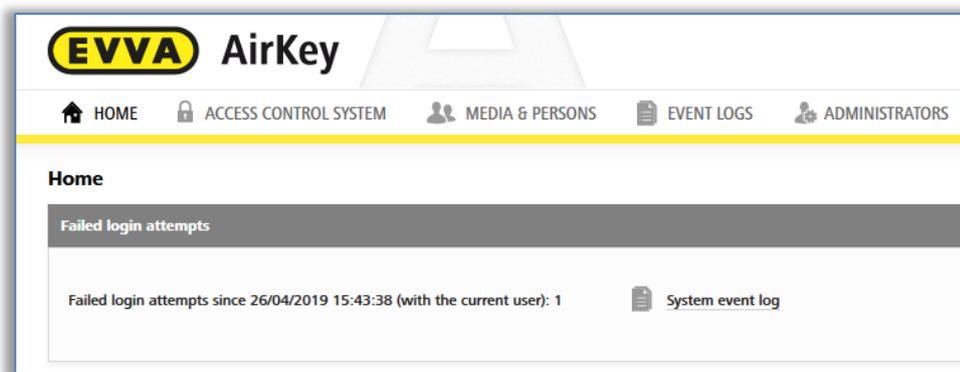


Figura 89: Tentativa de login falhada

5.1.1 Login no AirKey sem a autenticação de dois fatores

- > Abra, no seu browser, a página Web <https://airkey.evva.com>.
Abre-se a página de login da Administração online do AirKey.
- > Insira a identificação de utilizador que recebeu no e-mail "Registo no AirKey EVVA".
- > Insira a senha escolhida por si e confirme com **Iniciar sessão**.

Diretamente depois do login, tem acesso à página inicial **Home**. Aí, encontra uma vista geral do seu sistema de controlo de acessos AirKey.

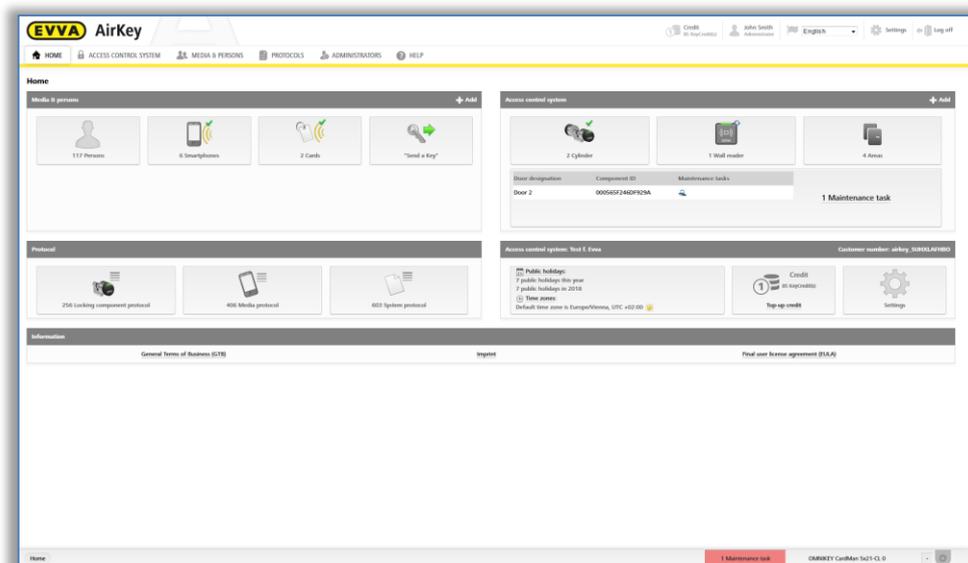


Figura 90: Administração online do AirKey – Home

5.1.2 Login no AirKey com a autenticação de dois fatores

- > Abra, no seu browser, a página Web <https://airkey.evva.com>. Abre-se a página de login da Administração online do AirKey.
- > Insira a identificação do utilizador, que recebeu no e-mail "Registo no AirKey EVVA".
- > Insira a senha escolhida por si para o AirKey e confirme com **Iniciar sessão**.
- > Se ainda não tiver sido verificado nenhum número de telefone para o administrador, aparece o pedido para inserir um número de telefone para a verificação.
- > Indique o número de telefone do smartphone que deverá ser utilizado para a autenticação de dois fatores, e confirme com **Enviar código por SMS**. O número de telefone deve começar com + e o código do país, e pode conter um máximo de 50 caracteres (+, 0-9 e espaços).

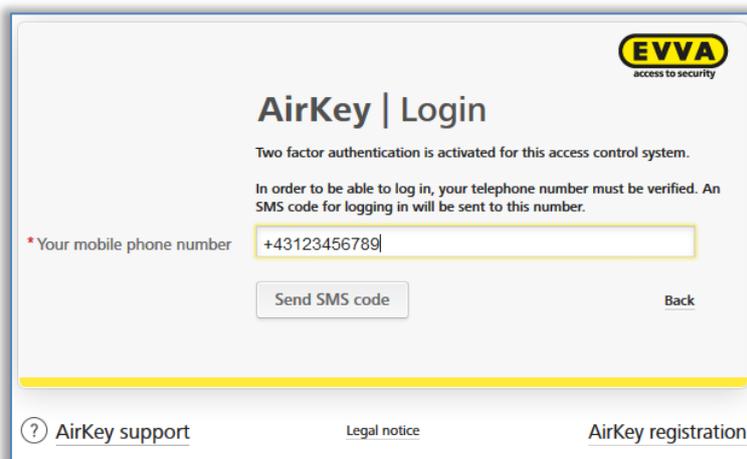


Figura 91: Verificação do número de telemóvel ao fazer login

- > Será enviada uma SMS com um código para o número de telefone especificado.

- > Insira o código da SMS na caixa de diálogo no âmbito da Administração online do AirKey e confirme com **Iniciar sessão**.

Figura 92: Código da SMS para o login

- > O número de telefone é verificado para a autenticação de dois fatores e é exibida a página inicial do seu sistema de bloqueio AirKey.



Se o número de telefone já tiver sido verificado, este não tem de ser inserido novamente após inserir a identificação do utilizador e senha. Neste caso, é imediatamente enviado um código por SMS para o número de telefone verificado, o qual tem de ser registado na Administração online do AirKey para o login.



O código da SMS é válido durante 5 minutos. Depois de excedidos estes 5 minutos, o processo de login terá de ser repetido.



Caso não tenha acesso ao número de telefone verificado, nenhum login poderá ser feito na Administração online do AirKey. Se pretender alterar o número de telefone, terá de alterar o número de telefone nos detalhes do administrador (ver [Editar administrador](#)). Para esse efeito, porém, é necessário o número de telefone atualmente verificado. Se o número de telefone já não estiver disponível, contacte a [Assistência da EVVA](#).

5.1.3 Esqueceu-se da sua senha

Se se tiver esquecido da senha, poderá proceder por si mesmo à sua reposição.

Clique em **Esqueceu a sua password?** .

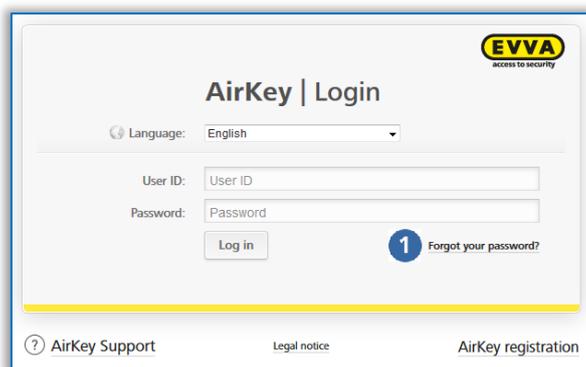


Figura 93: Página de login da Administração online do AirKey

- > Na janela de diálogo "Esqueceu-se da sua senha?", insira a sua identificação de utilizador e a data de nascimento fornecida durante o seu registo e clique em **Redefinir password**.



Figura 94: Esqueceu-se da sua senha

- > Com a autenticação de dois fatores ativada, recebe um código por SMS no seu smart-phone verificado, o qual tem de ser inserido na caixa de diálogo e confirmado com **Repor senha**. (Este passo não é necessário se a autenticação de dois fatores não estiver ativa ou se o número de telefone não for verificado.)



Figura 95: código por SMS



O código da SMS é válido durante 5 minutos. Depois de excedidos estes 5 minutos, o processo terá de ser repetido.



Caso não tenha acesso ao número de telefone verificado, o processo não poderá ser concluído. Se o número de telefone já não estiver disponível, contacte a [Assistência da EVVA](#).

Receberá um e-mail do AirKey EVVA gerado automaticamente com o assunto "Administração online do AirKey EVVA – Reposição da sua senha".

- > Abra o e-mail do AirKey EVVA.
- > No e-mail, clique no link para repor a senha; abre-se a página Web "Repor senha".
- > Insira a nova senha e repita a senha.
- > Clique em **Guardar password**.

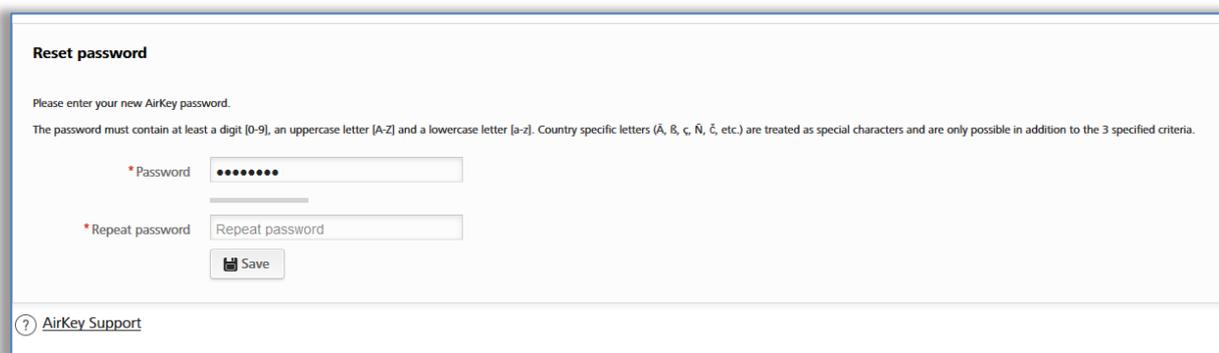


Figura 96: Repor a senha do AirKey

Vai para a página de login da [Administração online do AirKey](#).

- > Execute o login, tal como descrito em [Login do AirKey sem autenticação de dois fatores](#) ou [Login do AirKey com a autenticação de dois fatores](#), com a nova senha.

Se os dados introduzidos por si estiverem corretos, abre-se a página inicial **Home** da Administração online do AirKey. À direita, em cima, vê o nome do utilizador com sessão iniciada.



Se necessário, também poderá alterar a sua senha na Administração online do AirKey. Para tal, clique, na linha de cabeçalho à direita, da Administração online do AirKey, no nome do administrador e utilize a função **Alterar password**.

Figura 97: A minha conta AirKey

5.2 Logout do AirKey

Para sair da Administração online do AirKey, clique em **Terminar sessão** 1.

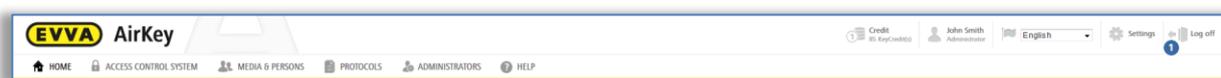


Figura 98: Terminar sessão



Apesar de existir o logout automático, após 30 minutos, recomenda-se fortemente que o administrador, depois de ter concluído as tarefas a realizar na Administração online do AirKey, faça sempre o logout em **Terminar sessão**.

5.3 Administradores

Para gerir o sistema AirKey, existem duas funções para os administradores: **Administradores do sistema e subadministradores**.

Os administradores do sistema têm todos os direitos para administrar todo o sistema de controlo de acessos AirKey e também podem criar, editar e eliminar outros administradores.

Os subadministradores possuem direitos limitados e servem principalmente para a gestão de pessoas e de autorizações. Adicionalmente, os **subadministradores** só podem ser

limitados a determinadas áreas e componentes de bloqueio do sistema de controlo de acessos AirKey. Isto significa que apenas podem criar e editar autorizações de acesso para componentes de bloqueio e áreas para as quais também estão autorizados.



Tem de ser criado, pelo menos, um administrador sistema de controlo de acessos.

As funções de gestão do administrador podem ser encontradas no menu principal **Administradores** 1.

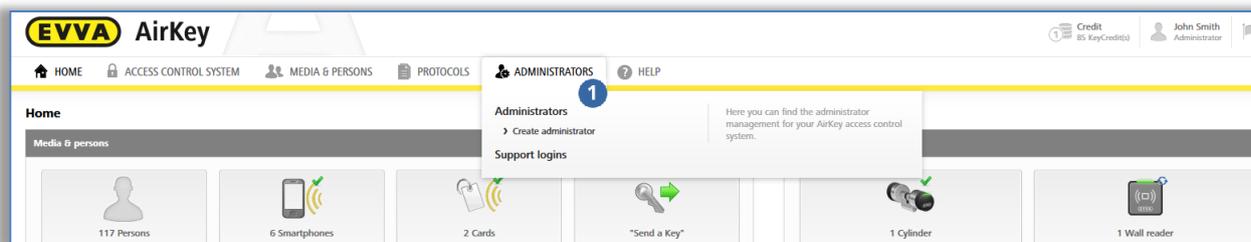


Figura 99: Menu principal – Administradores

5.3.1 Criar administrador

Os administradores podem ser criados exclusivamente por outros administradores.

- > No menu principal, selecione **Administradores** → **Criar administrador**.
- > Selecione caso se trate da função de **administrador do sistema** ou de **subadministrador**.

Figura 100: Detalhes de um administrador

- > Preencha os campos do formulário. Os campos assinalados com * são de preenchimento obrigatório.
- > No bloco "Informações de contacto", poderá ainda especificar se o administrador deverá receber notificações por e-mail relativas a determinados eventos, tais como tarefas de manutenção em aberto, janelas de manutenção pendentes ou outras informações importantes. As notificações por e-mail são enviadas no idioma selecionado, para correspondência.

Figura 101: Informações de contacto

- > Clique em **Guardar** 1.

Figura 102: Criar administrador



Antes de guardar, verifique novamente o endereço de e-mail, para onde o link de ativação vai ser enviado após a confirmação.

- > Para concluir o processo, confirme a pergunta de segurança com **Criar administrador**.

Figura 103: Criar administrador



A criação de um administrador é indicada com a mensagem de confirmação "O administrador foi guardado".

O administrador criado por si receberá agora um e-mail do AirKey EVVA com um link de ativação. Para **subadministradores**, só agora pode gerir os direitos. Poderá encontrar

detalhes sobre a gestão de direitos de subadministradores no capítulo seguinte [Editar administrador](#).



Se o link de ativação não for utilizado no espaço de 48 horas, os dados serão eliminados e o link de ativação perderá a sua validade.

O administrador criado por si terá de concluir o seu registo da seguinte forma:

- > Abrir o e-mail com o assunto "Registo no AirKey EVVA".
- > Clicar no link de ativação – Abre-se a página Web "Bem-vindo ao AirKey!"
- > Inserir a senha escolhida pelo próprio, repetir a senha e inserir a data de nascimento.
- > Clicar em **Guardar**.

A criação do administrador está, assim, concluída. Depois, é-se encaminhado para a página de login da [Administração online do AirKey](#), onde o novo administrador pode iniciar sessão.

5.3.2 Editar administrador

Só os **administradores do sistema** poderão alterar detalhes como, por exemplo, último nome, endereço de e-mail, número de telefone ou informações de contacto de um administrador em momento posterior. Também é possível editar a função posteriormente. Tenha em atenção, no entanto, que pelo menos um **administrador do sistema** tem de estar disponível por sistema de controlo de acessos.



Não é possível alterar a identificação de utilizador.

- > No menu principal, selecione **Administradores** → **Administradores**.
É exibida a lista com todos os administradores.

Na lista exibida, poderá procurar por administradores, ordenar as colunas, limitar os registos exibidos por página e exportar a lista para um ficheiro CSV.

- > Clique no administrador de quem pretende alterar dados de perfil.
- > Altere os dados pretendidos.
- > Clique em **Guardar** .

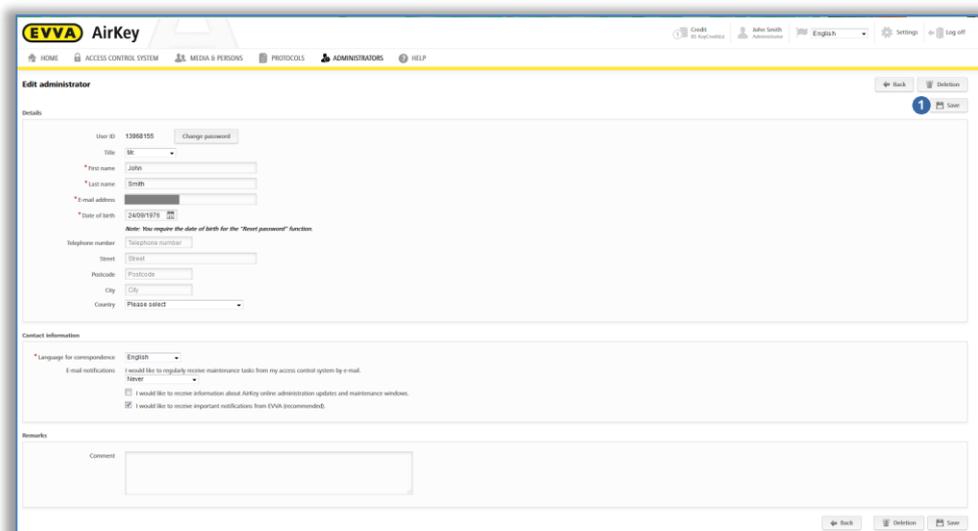


Figura 104: Editar administrador

Para gerir os direitos de **subadministradores**, siga os seguintes passos:

- > No menu principal, selecione **Administradores** → **Administradores**. É exibida a lista com todos os administradores válidos.
- > Clique no **subadministrador** cujos direitos pretende alterar.
- > Mude para o separador **Gerir direitos**.
- > Ao marcar as caixas de seleção, pode selecionar as áreas e os componentes de bloqueio que o subadministrador pode gerir, e atribuir autorizações.

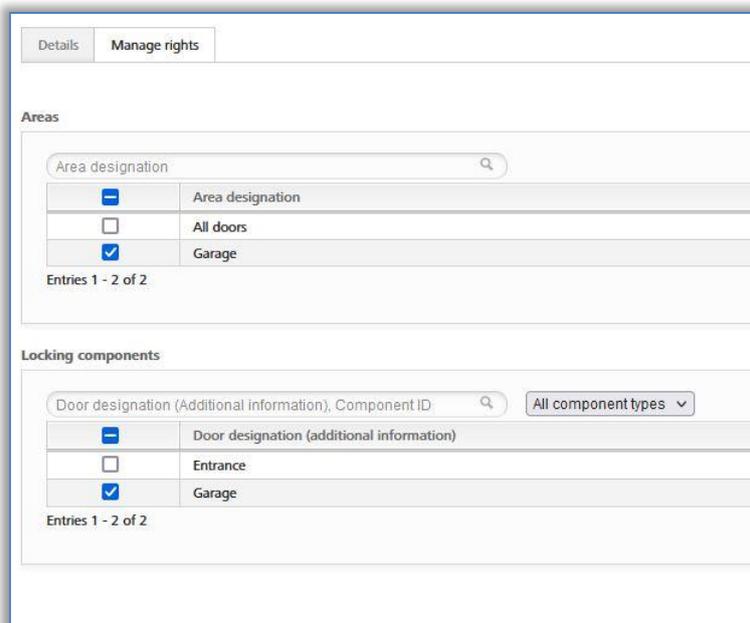


Figura 105: Gerir os direitos de um subadministrador

- > Clique em **Guardar**.

As áreas e componentes de bloqueio para os quais um **subadministrador** não possui direitos, não estão disponíveis para o **subadministrador** na atribuição de autorização. Para

a atribuição de autorização, estão sempre disponíveis todas as áreas e componentes de bloqueio ao **administrador do sistema**.

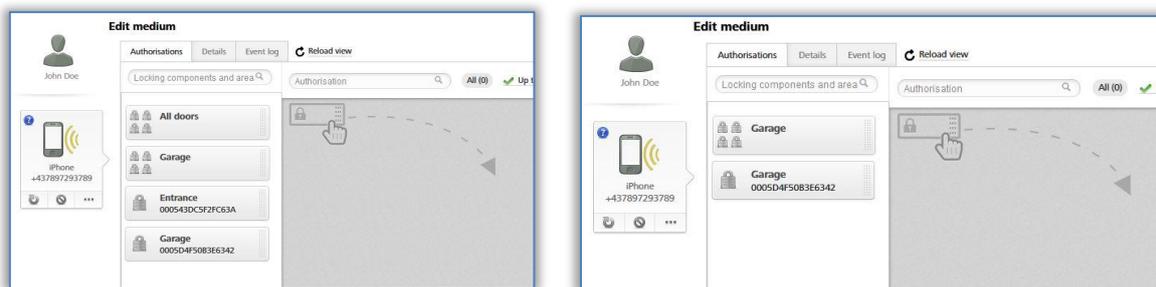


Figura 106: Atribuição de autorizações por um administrador do sistema ou por um subadministrador



A gestão de direitos para **subadministradores** diz respeito apenas a áreas e componentes de bloqueio. **Os subadministradores** veem sempre todas as pessoas e meios.

5.3.3 Eliminar administrador

Um administrador só pode ser eliminado por outro administrador do sistema.

- > No menu principal, clique em **Administradores** → **Administradores**.
- > Selecione o administrador a eliminar, clicando na respetiva linha da tabela. Vai para a página "Editar administrador".
- > Clique em **Apagar** 1.

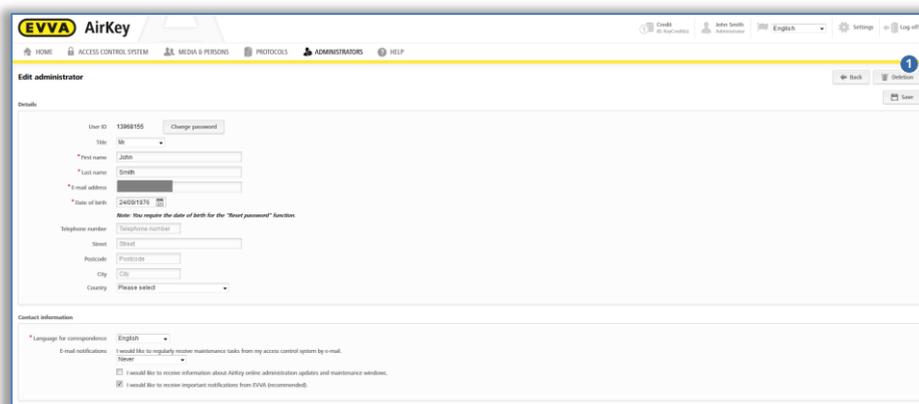


Figura 107: Eliminar administrador

- > Confirme a pergunta de segurança com **Apagar administrador**.

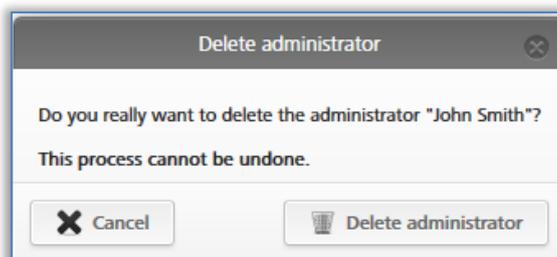


Figura 108: Eliminar administrador



A eliminação de um administrador é indicada com a mensagem de confirmação "O administrador foi apagado". O administrador eliminado já não aparece na lista de administradores e já não pode iniciar sessão na Administração online do AirKey.



Se o **princípio dos quatro olhos para a visualização dos protocolos** estiver ativado, têm de restar, pelo menos, dois administradores do sistema. Caso contrário, ao tentar eliminar o administrador, é apresentada uma mensagem de erro e o administrador não pode ser eliminado. Poderá encontrar detalhes sobre o **princípio dos quatro olhos para a visualização dos protocolos** no capítulo [Informações gerais](#).

5.4 Definições do sistema de controlo de acessos AirKey

Nas definições da Administração online do AirKey, devem ser feitas configurações básicas, descritas em detalhe a seguir.

- > Na página inicial **Home**, clique na caixa de seleção **Definições** 1.
- > Ou clique na linha de cabeçalho em **Definições**.

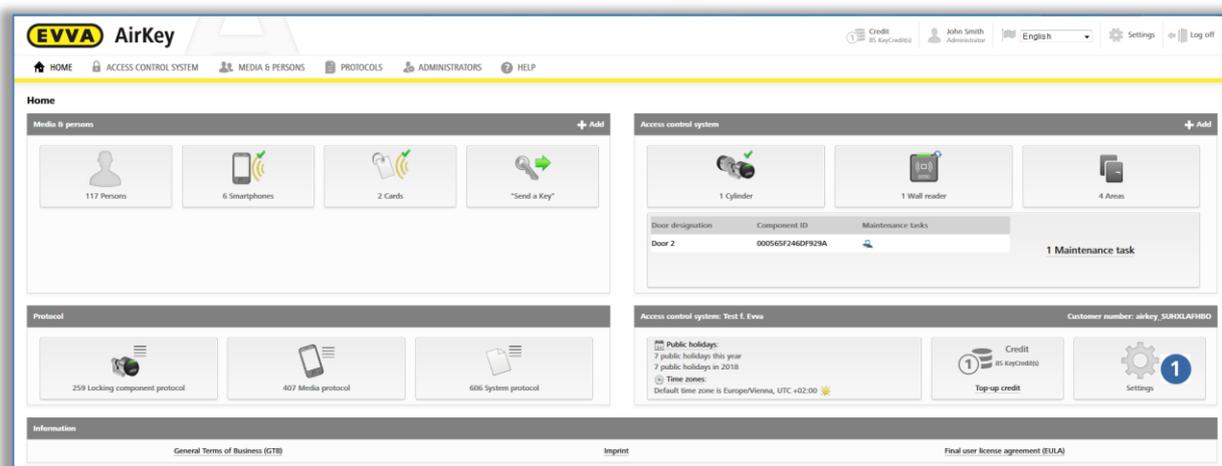


Figura 109: Definições do sistema de controlo de acessos AirKey

5.4.1 Informações gerais

Neste separador, as definições gerais descritas a seguir podem ser ativadas para todo o sistema de bloqueio.

Definições de Bluetooth para a aplicação AirKey

Aqui, este sistema de controlo de acessos poderá ser configurado em todos os smartphones para a possibilidade, ou não, de abrir os componentes de bloqueio por Bluetooth a partir do ecrã de bloqueio. Se a opção não estiver ativada, o smartphone tem de ser desbloqueado antes de cada acesso.

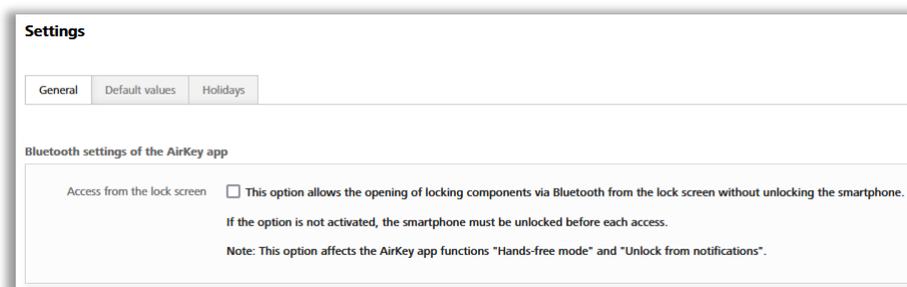


Figura 110: Definições gerais – Definições de Bluetooth para a aplicação AirKey



Esta opção afeta as funções da aplicação "Modo Hands-free (mãos livres)" e "Desbloquear a partir de notificações".



Desative o **Acesso a partir do ecrã de bloqueio** para aumentar a segurança do seu sistema de controlo de acessos.

Definições para a aplicação AirKey

Aqui, pode ser ativada a opção **Atualização após cada acesso** e o **texto para SMS "Send a Key"** pode ser configurado.

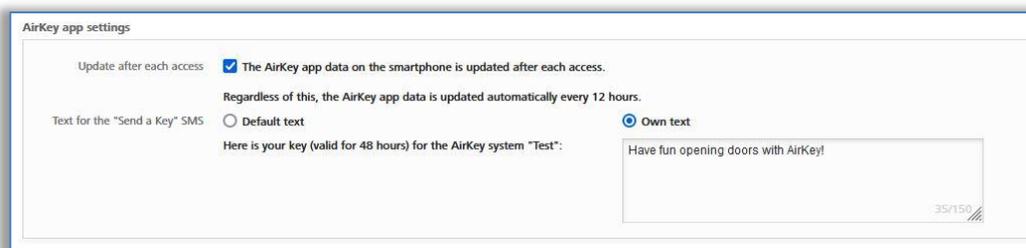


Figura 111: Definições gerais – Definições para a aplicação AirKey

Quando a opção **Atualização após cada acesso** é ativada, os dados da aplicação AirKey (por exemplo, registos protocolares ou o estado da bateria dos componentes de bloqueio) são atualizados com um smartphone em cada acesso.

- > Selecione a caixa de seleção correspondente e confirme com **Guardar**.

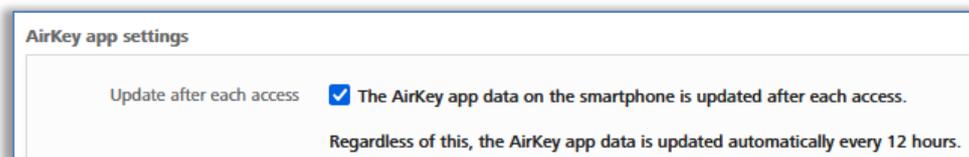


Figura 112: Definições para a aplicação AirKey – Atualização após cada acesso

A funcionalidade é então enviada através de notificação Push a todos os smartphones deste sistema de bloqueio. Após, uma atualização manual dos dados da AirKey App do smartphone (ver o capítulo [Atualizar smartphone](#)), a funcionalidade deverá estar ativa no smartphone. Poderá encontrar o atual estado ⓘ do smartphone com respeito a esta função na Administração online do AirKey, nos detalhes do smartphone.

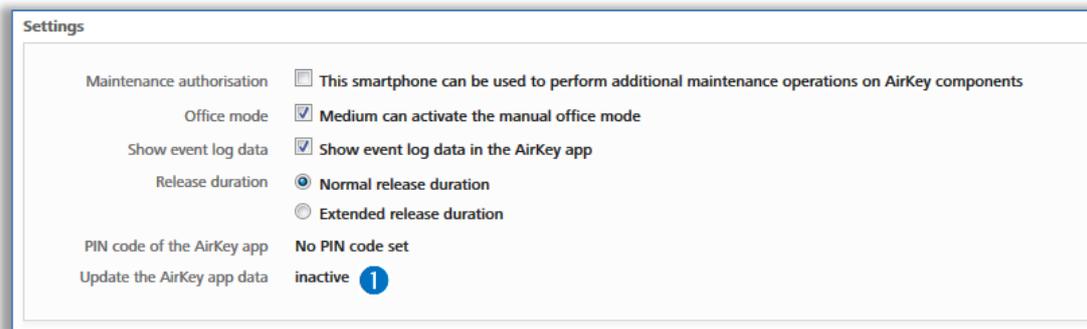


Figura 113: O estado da opção "Atualização após cada acesso"



Ative esta função para, no caso de utilização de smartphones, transferir os acessos praticamente em tempo real à Administração online do AirKey.



A atualização dos dados da AirKey App, após um processo de acesso, só transfere os dados do smartphone que executou o processo de acesso. Esta atualização não é visualizada no smartphone em si.



Para esta função, é necessária uma ligação à Internet estável (dados móveis ou WLAN), uma vez que a realização de outro processo de acesso só pode ser executado após a atualização dos dados da AirKey App ter sido concluída.



Independentemente da opção "Atualização após cada acesso" é feita uma tentativa de atualização automática dos dados da AirKey App a cada 12 horas.

Também é possível configurar aqui o **texto para SMS "Send a Key"**.

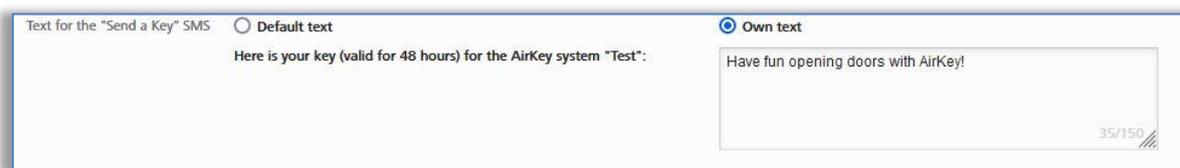


Figura 114: Definições para a aplicação AirKey – Texto para o SMS "Send a Key"

É possível escolher entre o texto padrão e um texto que pode ser definido pelo próprio. Selecione o **texto padrão** para utilizar o texto predefinido «Aqui é a sua chave (válido por 48 horas) para o sistema AirKey "<Nome do sistema de controlo de acessos>"» ou selecione o **seu próprio texto** para utilizar um texto definido pelo próprio no respetivo campo de texto. Em seguida, confirme a seleção com **Guardar**.

Se for utilizado um texto próprio, este pode ainda ser adaptado em cada ação "Send a Key", por exemplo, para utilizar um título personalizado. Poderá encontrar detalhes sobre "Send a Key" no capítulo [Função "Send a Key"](#).



O seu texto está limitado a um máximo de 150 caracteres. Além disso, o seu próprio texto não será traduzido para outros idiomas se uma pessoa tiver selecionado outro idioma de correspondência. Em vez disso, o texto padrão é traduzido automaticamente para o idioma de correspondência da pessoa.



Utilize um texto definido pelo próprio para abordar pessoalmente os proprietários do smartphone e informá-los para que sistema de controlo de acessos recebem autorizações.

Opções de segurança

Nas opções de segurança, pode configurar as funções **Troca de smartphone**, **Autenticação de dois fatores (2FA)** e **Princípio dos quatro olhos para a visualização dos protocolos**.

Figura 115: Definições gerais – Opções de segurança

Com a caixa de seleção **Confirmar automaticamente os pedidos de troca do smartphone por pessoas**, as ações da troca que iniciaram com um smartphone podem ser automaticamente confirmadas.



Desta forma, qualquer troca de smartphone iniciada através do smartphone é imediatamente confirmada, se houver crédito suficiente. Lembre-se de que em cada troca do smartphone, durante a qual são transferidas autorizações, é debitado um KeyCredit. Poderá encontrar mais detalhes sobre a troca do smartphone no capítulo [Troca de smartphone](#).

A **autenticação de dois fatores** constitui um nível de segurança adicional ao fazer login na Administração online do AirKey. Além da identificação do utilizador e da senha, é pedido um código adicional recebido por SMS para o login como segundo fator. Se a autenticação de dois fatores for ativada nas definições, esta será aplicada em todos os administradores deste sistema de bloqueio.

- > Para ativar, clique no botão **Ativar a autenticação de dois fatores**.

Figura 116: Definições gerais – Autenticação de dois fatores

- > Registe o número de telemóvel que deverá ser utilizado para a autenticação de dois fatores para o administrador no momento, e clique em **Enviar código por SMS**.

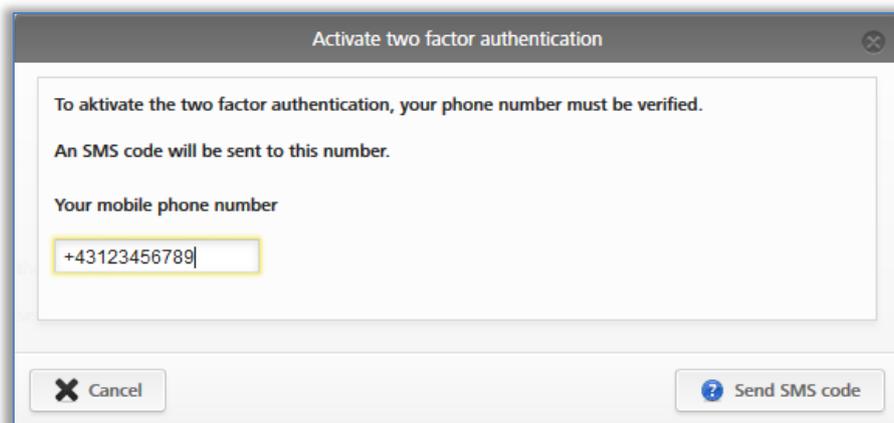


Figura 117: Registe o número de telemóvel

- > É enviado um código por SMS para o número de telefone indicado anteriormente. Este código enviado por SMS tem de ser inserido na caixa de diálogo no âmbito da Administração online do AirKey e confirmado com **Guardar**.

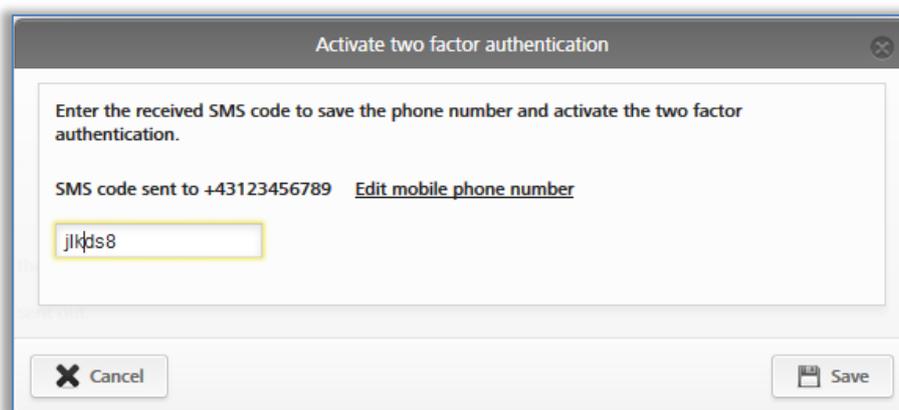


Figura 118: Insira o código da SMS

Se for utilizado um código de SMS válido, a autenticação de dois fatores é ativada para todos os administradores do sistema de bloqueio. O estado nas definições altera-se de forma correspondente.



O código da SMS é válido durante 5 minutos. Depois de excedidos estes 5 minutos, o processo terá de ser repetido.



A partir do momento da ativação, é necessário um telemóvel para cada login. Poderá obter os detalhes para o processo de login com a autenticação de dois fatores ativada no capítulo [Login no AirKey com a autenticação de dois fatores](#).

Para desativar a autenticação de dois fatores, siga os passos seguintes:

- > Clique em **Desativar a autenticação de dois fatores**.

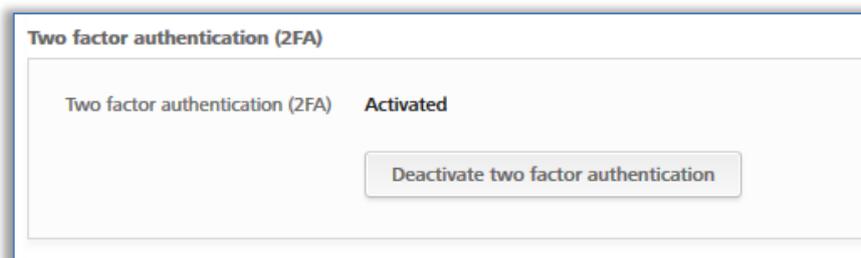


Figura 119: Desativar a autenticação de dois fatores

- > Confirme a mensagem também com **Desativar a autenticação de dois fatores**.



Figura 120: Desativar a autenticação de dois fatores

A função fica novamente desativada para todos os administradores do sistema de bloqueio.

Com a função **Princípio dos quatro olhos para a visualização dos protocolos**, tem a possibilidade de visualizar o protocolo dos componentes de bloqueio e dos meios apenas quando um segundo administrador do sistema confirmar a visualização. Desta forma, os dados pessoais permanecem ainda mais protegidos contra visualização.



Para ativar o **princípio dos quatro olhos para a visualização dos protocolos**, têm de existir, pelo menos, 2 administradores do sistema.

Para ativar o **Princípio dos quatro olhos para a visualização dos protocolos**, siga os seguintes passos:

- > Clique em **Ativar o princípio dos quatro olhos**.

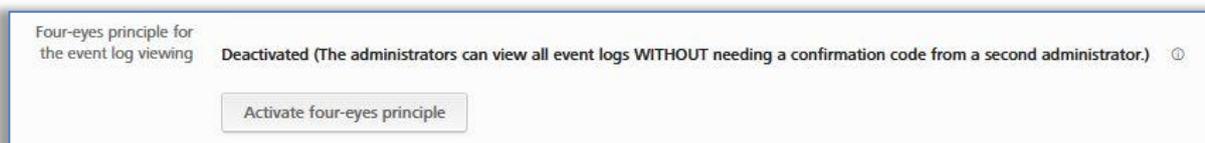


Figura 121: Ativação do princípio dos quatro olhos

- > Selecione um segundo administrador do sistema da lista, para o qual deve ser enviado um código de confirmação por e-mail, e clique em **Enviar código de confirmação**.

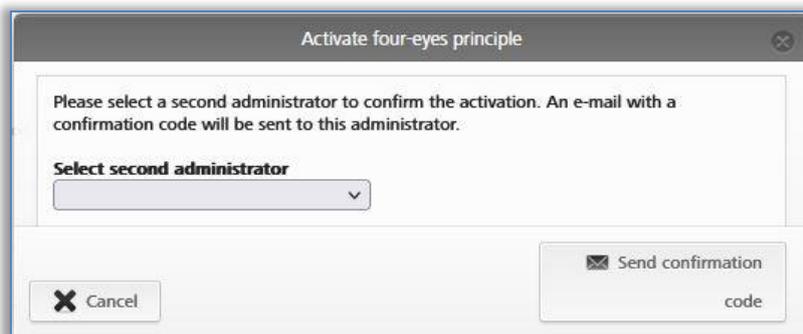


Figura 122: Ativação do princípio dos quatro olhos – selecção do segundo administrador

- > Em seguida, é enviado um e-mail com um código de confirmação ao administrador do sistema selecionado.
- > Este código de confirmação tem de ser introduzido na administração online do AirKey no espaço de 10 minutos e confirmado com **Ativar**.

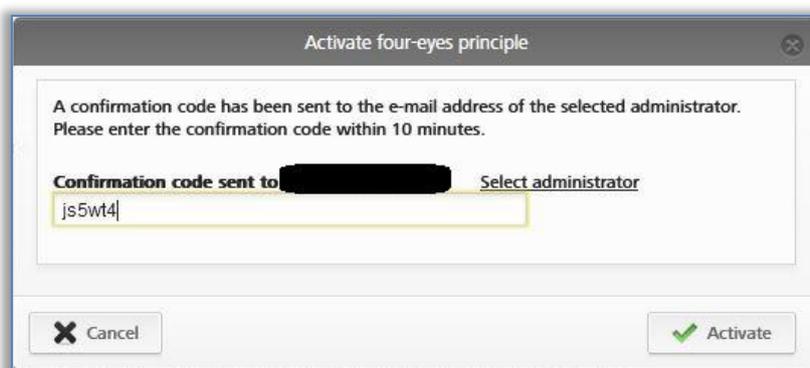


Figura 123: Ativação do princípio dos quatro olhos – introdução do código de confirmação

Se o procedimento não for concluído dentro de 10 minutos, é necessário repetir o procedimento. Se o administrador do sistema selecionado não reagir, pode selecionar um outro administrador do sistema pelo link **Selecionar administrador** para ativar o princípio dos quatro olhos.

Desta forma, ativou o **princípio dos quatro olhos para a visualização dos protocolos** para todos os administradores deste sistema AirKey. A partir do login seguinte de um administrador do sistema, não é possível visualizar o protocolo dos componentes de bloqueio e dos meios sem a confirmação de um segundo administrador do sistema.



O protocolo do sistema pode continuar a ser visualizado e não está sujeito ao princípio dos quatro olhos. Os subadministradores não podem visualizar protocolos.

Para desativar o **princípio dos quatro olhos para a visualização dos protocolos**, siga o mesmo procedimento da ativação.



Tanto a ativação como a desativação são guardadas no protocolo do sistema. São protocolizados ambos os administradores do sistema envolvidos, incluindo o endereço de e-mail utilizado.

AirKey Cloud Interface (API)

A AirKey Cloud Interface é uma interface REST (API) para sistemas de terceiros. A interface permite controlar determinadas funções do AirKey através de um software de terceiros. Os detalhes da AirKey Cloud Interface estão descritos no capítulo [AirKey Cloud Interface \(API\)](#).

AirKey Cloud Interface (API) – Ambiente de teste

O ambiente de teste dá-lhe a possibilidade de experimentar a AirKey Cloud Interface (API) com dados de teste antes da ativação, num ambiente protegido. Poderá consultar os detalhes no capítulo [AirKey Cloud Interface \(API\)](#).

5.4.2 Valores por defeito (para todos os componentes de bloqueio adicionados como novos)

Estas definições são automaticamente ativadas em novos componentes de bloqueio adicionados. Já para sistemas de bloqueio maiores, recomendamos definir os valores por defeito antes da primeira instalação para simplificar a administração do sistema.

Horas e calendário

Num sistema de controlo de acessos AirKey, poderá administrar componentes de bloqueio que se encontrem em diferentes fusos horários. Como valor por defeito padrão está predefinido o fuso horário "Europa/Viena" com UTC+01:00 no inverno e UTC+02:00 no verão, válido para a Europa Central.

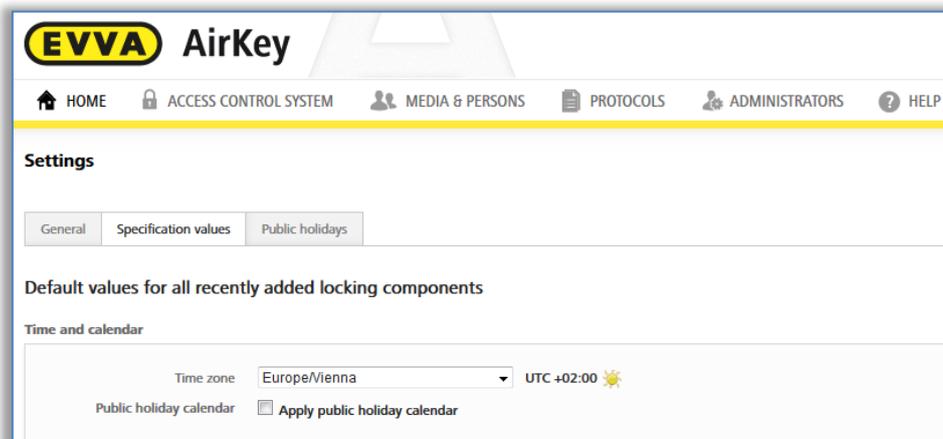


Figura 124: Valores por defeito para novos componentes de bloqueio

Se pretender alterar o fuso horário para todo o sistema de controlo de acessos, clique simplesmente na lista dropdown e selecione o fuso horário correto a partir dessa lista.



Se pretender alterar o fuso horário para um componente de bloqueio, clique, na página inicial **Home**, na caixa de seleção **Cilindro** ou **Leitor de parede**, selecione o componente de bloqueio pretendido e aceda ao separador **Definições**. No bloco **Horas e calendário** volta a encontrar a lista dropdown com os fusos horários.

O símbolo do sol em cada um dos respetivos fusos horários mostra se é o horário de inverno ou de verão que está ativo:

-  Sol amarelo = horário de verão
-  Sol cinzento = horário de inverno

Se colocar o visto em **Utilizar o calendário de férias/feriados**, os **dias de férias/feriados** (ver o capítulo [Dias de férias/feriados](#)) serão salientados e ativados no separador para o novo componente de bloqueio.

Áreas

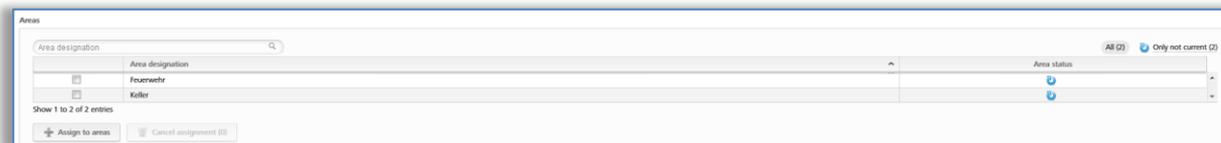


Figura 125: Valores por defeito – Áreas

Nesta secção, novos componentes de bloqueio podem ser automaticamente atribuídos a áreas já criadas. Onde e como se cria uma área está esclarecido com maior exatidão em [Criar área](#).

Isto é especialmente útil para a Defesa Geral e Departamento de Bombeiros que têm de bloquear sempre todos os componentes. As atribuições às áreas podem ser novamente canceladas nos respetivos componentes de bloqueio.

Acesso

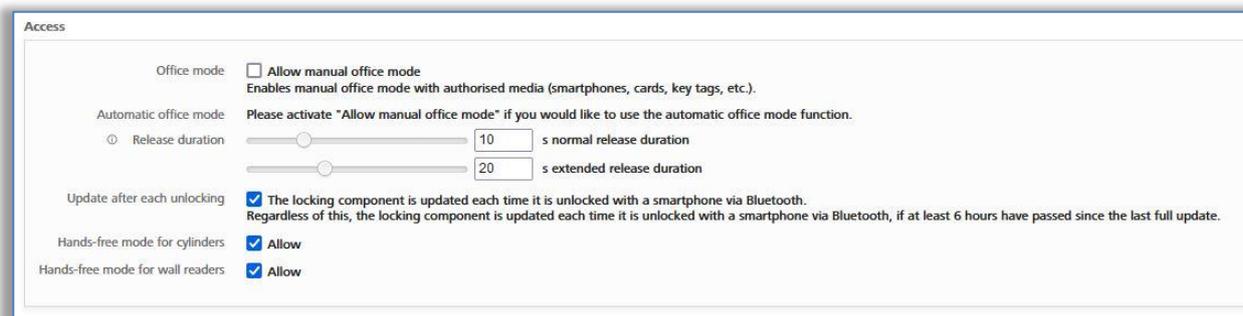


Figura 126: Valores por defeito – Acesso

Aqui, podem ser permitidas a abertura permanente manual e automática, o tempo de ativação, a atualização após cada processo de bloqueio e o modo Hands-free (mãos-livres) para o cilindro e leitor de parede para todos os novos componentes de bloqueio adicionados.

Se a caixa de seleção **Permitir abertura permanente manual** for ativada, aparece adicionalmente uma outra caixa de seleção: **Ativar abertura permanente automática**.

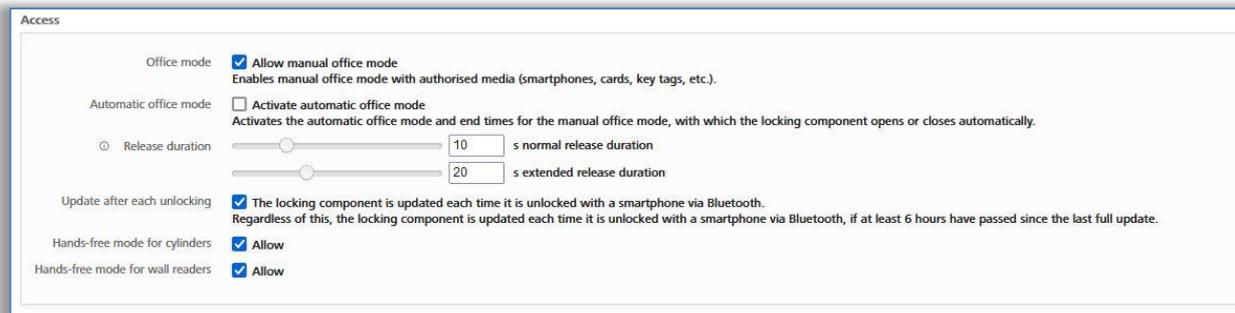


Figura 127: Abertura permanente automática

A abertura permanente automática permite a definição dos períodos de tempo e momentos de bloqueio em que o componente de bloqueio se abre ou fecha. Por exemplo, num escritório, a abertura permanente terminará automaticamente todos os dias, ao final da tarde, às 17:00 horas. No caso de um cilindro AirKey, isto não significa que a porta também seja bloqueada, mas só que o cilindro desengata. Para bloquear a porta, o cilindro tem de engatar com um meio autorizado e, depois, tem de ser manualmente bloqueado.

A definição de um período de tempo para a abertura permanente manual também pode ser inserida nesta janela de diálogo. Isso garante que, independentemente da ativação da abertura permanente, esta seja terminada no período definido (barras vermelhas na imagem abaixo). Podem ser definidas por dia, no máximo, 4 entradas (períodos de tempo ou horas como fim de tempo).

As aberturas permanentes terminam ou nem chegam a ter início nos feriados, no caso de sinalização de "Pilha gasta", se a hora no componente de bloqueio não estiver correta ou se decorrer uma atualização automática do firmware.

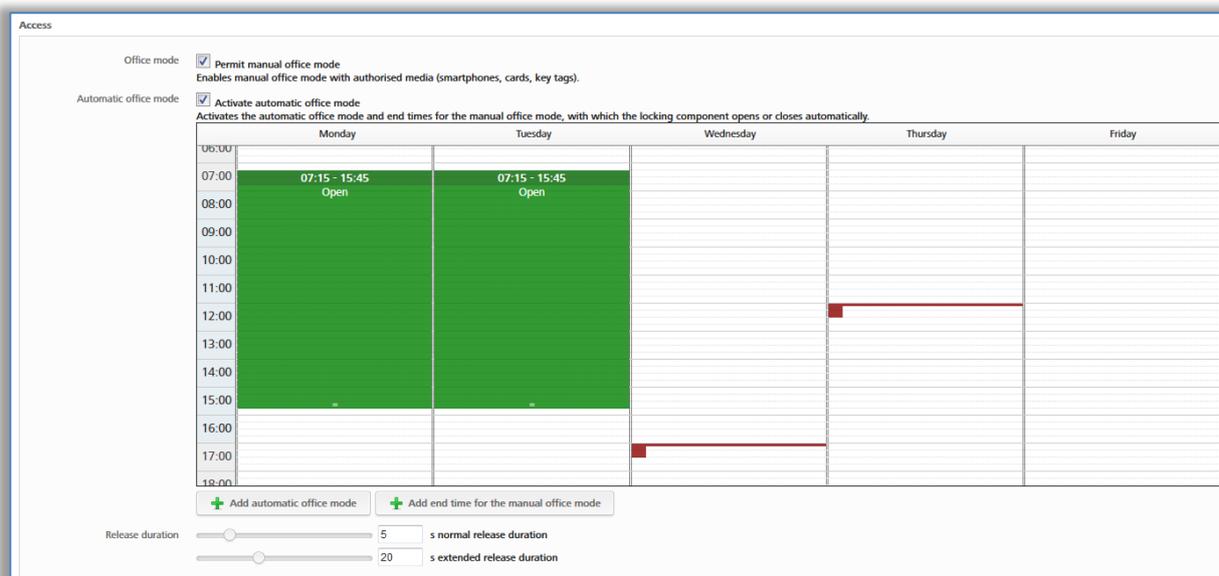


Figura 128: Abertura permanente automática



A abertura permanente manual também pode ser ativada com meios de identificação. Neste caso, o meio deve ser encostado ao componente de bloqueio, deve ser afastado da área de leitura durante um breve espaço de tempo e novamente apresentado, dentro do tempo de ativação, uma

segunda vez. A abertura permanente manual também pode ser terminada deste modo.

O tempo de ativação determina quanto tempo demora a ativação do componente de bloqueio no caso de um bloqueio (p. ex., no caso de um cilindro, isto significa quanto tempo o utilizador tem para girar manualmente o puxador de cilindro). Por defeito, o tempo de ativação normal é de 5 segundos, o alargado é de 20 segundos. O tempo de ativação pode ser ajustado individualmente aqui, o intervalo vai de 1 segundo a 250 segundos.

Com a opção **Atualização após cada desbloqueio** pode ativar se o componente de bloqueio deve ser atualizado após cada processo de desbloqueio bem-sucedido via Bluetooth. Independentemente disso, o componente de bloqueio é atualizado de cada vez que é bloqueado com um smartphone via Bluetooth e tenham passado, pelo menos, 6 horas desde a última atualização completa.

Esta atualização não é perceptível para o utilizador. Não é emitido, portanto, nenhum sinal, nem é exibida nenhuma indicação no smartphone.

O administrador visualiza a ação, mas só nos protocolos de registo da Administração online do AirKey.

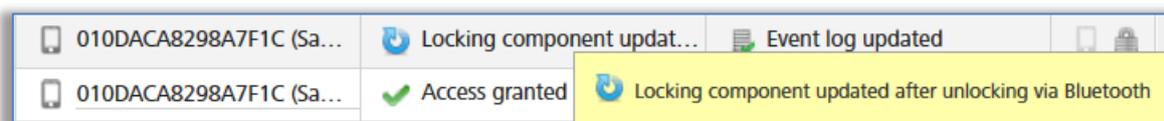


Figura 129: Protocolização – Atualização após o processo de desbloqueio



Na atualização após um processo de desbloqueio via Bluetooth, os seguintes dados são atualizados:

- Blacklist
- Fuso horário
- Hora
- Registos protocolares

Se o componente de bloqueio possuir ainda outras tarefas de manutenção abertas, este tem de ser atualizado, tal como descrito no capítulo [Atualizar componentes de bloqueio](#).



A função depende da qualidade de ligação do smartphone. Assegure, portanto, uma ligação estável à Internet a partir de 3G ou via WLAN.



A atualização após um processo de desbloqueio via Bluetooth também é executada ao iniciar a abertura permanente manual, mas não quando esta termina.



A atualização após um processo de desbloqueio via Bluetooth ocorre dentro do tempo de ativação do componente de bloqueio. Se o tempo de ativação for inferior a 10 segundos, é possível que a atualização não funcione após um processo de desbloqueio via Bluetooth. Por esta razão, ao ativar a função, o valor do tempo de ativação normal é automaticamente aumentado

para 10 segundos.



A ativação desta função aumenta o consumo da pilha dos componentes de bloqueio que funcionam a pilha, como é o caso de um cilindro AirKey, e, como tal, isso influencia o tempo de vida útil da pilha.

As opções do **modo Hands-free (mãos-livres) para cilindro** e **modo Hands-free (mãos-livres) para leitor de parede** destinam-se a permitir ou a não permitir o modo Hands-free (mãos-livres) para todos os componentes do tipo de componente selecionado dentro do sistema de controlo de acessos. Além disso, também é possível definir individualmente, para cada componente de bloqueio, se este deve permitir o modo Hands-free (mãos-livres). Poderá encontrar como alterar a configuração em componentes de bloqueio individuais no capítulo [Editar componente de bloqueio](#).

Registo em protocolo

Selecione o valor por defeito para a referência pessoal nos registos protocolares dos acessos. Neste caso, existem para seleção três botões de opção:

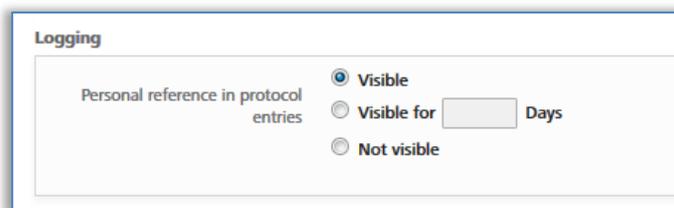


Figura 130: Definir o registo em protocolo

- > **Visíveis** permite que a indicação dos dados dos acessos referentes à pessoa fique permanentemente visível.
- > **Visíveis para ... dias** torna anónimos os dados dos acessos referentes à pessoa depois do número de dias definido.
- > **Não visíveis** torna permanentemente anónimos todos os dados dos acessos referentes à pessoa.



Os valores definidos por defeito, independentemente das configurações aqui feitas, podem ser alterados individualmente para um componente de bloqueio.

Os valores por defeito alterados têm de ser guardados com o botão **Guardar**. Para tal, surge a pergunta, se os valores por defeito alterados devem ser aplicados apenas aos novos componentes de bloqueio adicionados ou a todos os componentes de bloqueio.

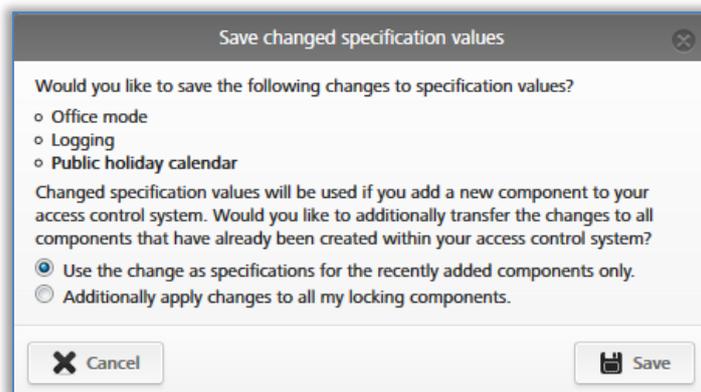


Figura 131: Guardar os valores por defeito alterados

5.4.3 Dias de férias/feriados

No separador **Dias de férias/feriados**, poderá definir até 80 dias de férias/feriados por ano (ano corrente e dois anos seguintes). O termo "dia de férias/feriado", no AirKey, pode ser um feriado oficial ou um período de vários dias, p. ex., férias da empresa ou férias escolares, que se pode repetir. Por exemplo, os feriados nacionais ou dias de férias que estejam definidos para a mesma data todos os anos, poderá definir como repetição anual. Uma semana de férias escolares significa apenas 1 dia de férias, se tiver definido um período de tempo com "Início – Fim".

Impacto do calendário de dias de férias/feriados:

1. Autorizações de acesso periódicas não são válidas nos dias de férias/feriados.
2. As aberturas permanentes automáticas não são consideradas nos dias de férias.

Para que o calendário de dias de férias/feriados seja aplicável, terá de o ativar globalmente através do botão **Ativar** do lado direito.

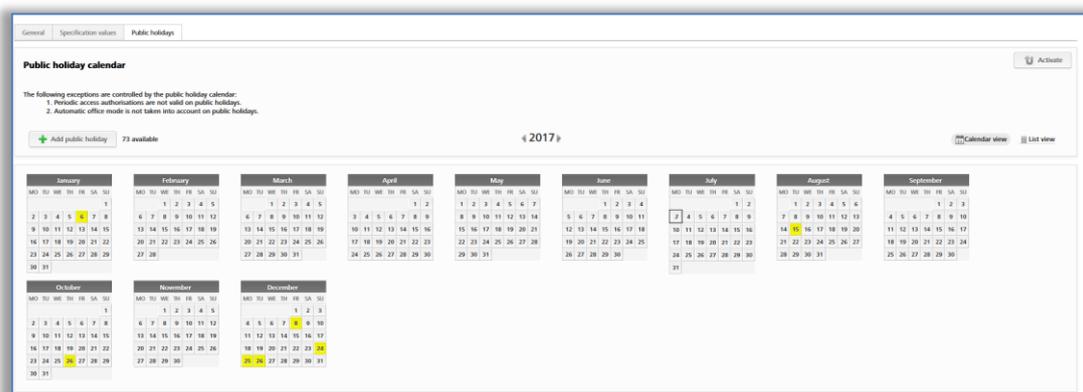


Figura 132: Calendário de dias de férias/feriados (vista geral do calendário)

Clique no botão **Adicionar dia de férias/feriado** ou clique, na vista geral do calendário, na data exata do dia de férias/feriado (p. ex., 24.12.); abre-se, de seguida, uma janela de diálogo, onde pode registar o nome do dia de férias/feriado, se o dia de férias/feriado abrange todo o dia, quando começa e quando termina, p. ex., só de tarde (aqui, poderá, p. ex., também registar as férias da empresa), a frequência com que se repete e quando termina a repetição.

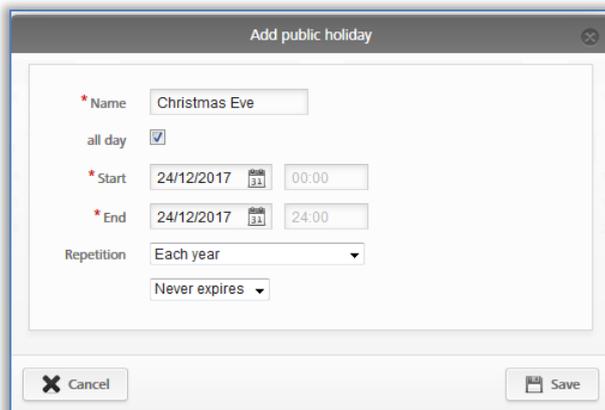


Figura 133: Adicionar dia de férias/feriado

Cada dia de férias/feriado registrado pode ser posteriormente editado, bastando clicar, para tal, no respetivo dia, sendo que se abrirá uma caixa de texto.

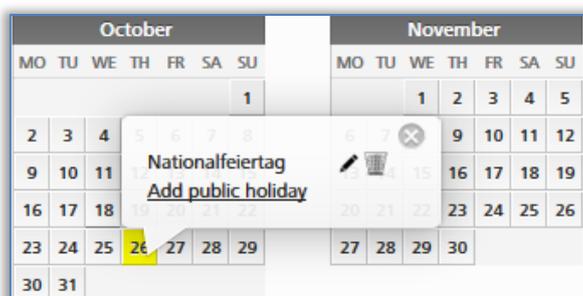


Figura 134: Adicionar dia de férias/feriado pelo calendário

Ao clicar no link **Adicionar dia de férias/feriado**, poderá adicionar um outro dia livre para este dia. Poderá registar num dia de calendário vários dias livres. Se clicar no lápis, poderá editar o dia de férias/feriado; se clicar no caixote de lixo, poderá eliminar o dia de férias/feriado.

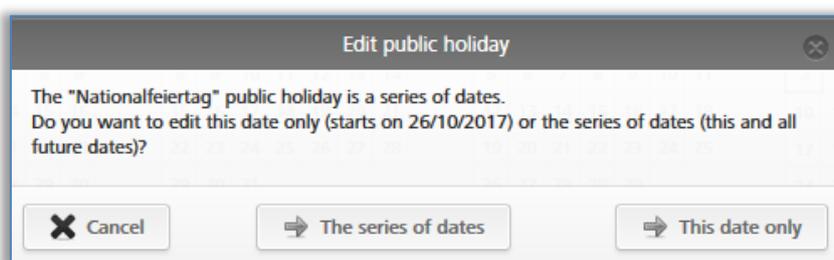


Figura 135: Editar dia de férias/feriado



Figura 136: Eliminar dia de férias/feriado

Assim que tiver registado datas, férias (da empresa) ou feriados no calendário, ser-lhe-á exibida uma lista com a vista geral de todos os dias de férias/feriados etc., guardados.

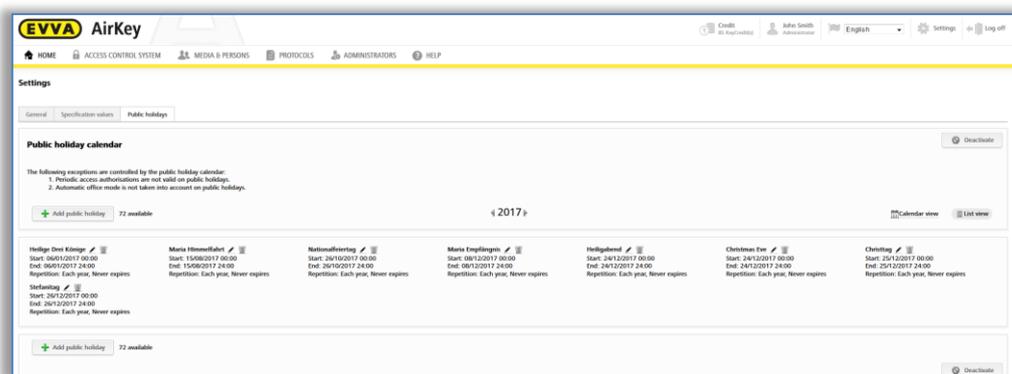


Figura 137: Calendário de dias de férias/feriados (lista geral)

Se seleccionar o botão **Desativar**, o calendário de dias de férias/feriados será globalmente desativado para o sistema de controlo de acessos e não será assumido para os componentes de bloqueio adicionados.

5.5 Sistema de controlo de acessos

As caixas de seleção na página inicial **Home** e os pontos dos menus e dos submenus no Menu principal **Sistema de controlo de acessos** permitem-lhe administrar o seu sistema de controlo de acessos AirKey.

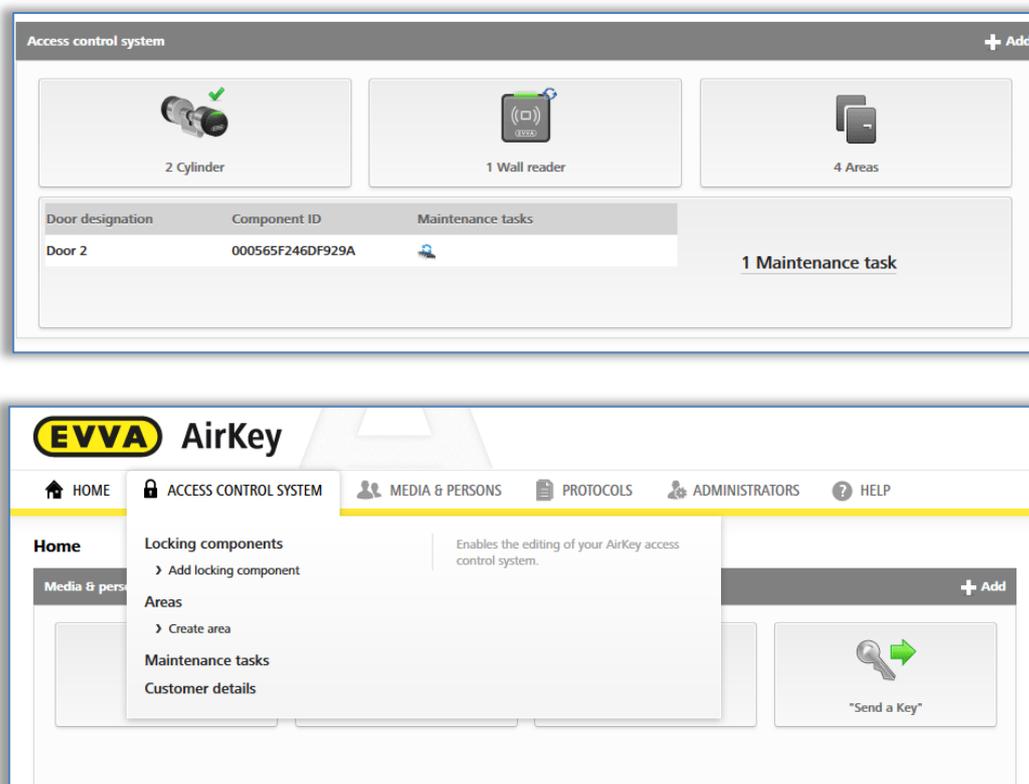
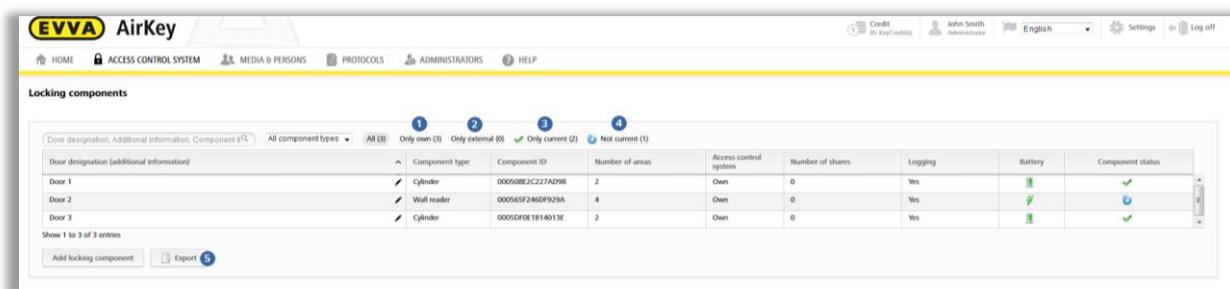


Figura 138: Sistema de controlo de acessos AirKey

5.5.1 Vista geral dos componentes de bloqueio

Para obter uma visão global de todos os componentes de bloqueio do seu sistema de controlo de acessos AirKey, clique, na página inicial **Home**, na caixa de seleção **Cilindro** ou **Leitor de parede**, ou, no menu principal, em **Sistema de controlo de acessos** → **Componentes de controlo de acessos**. Na página inicial **Home**, poderá ver também, a um primeiro olhar, quantos cilindros ou leitores de parede estão integrados no seu sistema de controlo de acessos.

Todos os componentes de bloqueio estão listados com informações adicionais e o seu estado. Na primeira linha da lista, ao lado do campo de pesquisa, poderá encontrar igualmente as funções de filtro para os componentes de bloqueio.



Door designation (additional information)	Component type	Component ID	Number of areas	Access control system	Number of shares	Logging	Battery	Component status
Door 1	Cylinder	00050B2C227AD98	2	Open	0	Yes		
Door 2	Wall reader	000503F246D929A	4	Open	0	Yes		
Door 3	Cylinder	00050FE1814013E	2	Open	0	Yes		

Figura 139: Componentes de bloqueio

- > "Só do próprio" ① apresenta apenas os componentes de bloqueio do próprio.
- > "Só de terceiros" ② apresenta apenas os componentes de bloqueio ativados para partilha por um administrador.
- > "Só atualizados" ③ apresenta uma lista dos componentes de bloqueio, cujo estado está atualizado.
- > "Não atualizados" ④ apresenta uma lista dos componentes de bloqueio, cujo estado não está atualizado.
- > A lista dos componentes de bloqueio pode ser exportada para um ficheiro CSV para posterior edição ⑤.



O AirKey oferece-lhe a possibilidade de ativar componentes de bloqueio de terceiros num sistema de controlo de acessos AirKey. Na lista apresenta-se a diferenciação entre componentes de bloqueio do próprio e de terceiros. Poderá obter mais informações no capítulo [Ativar componentes de bloqueio para outros sistemas de bloqueio](#).

5.5.2 [Adicionar componente de bloqueio](#): ver o capítulo 4.11

5.5.3 Editar componente de bloqueio

Na janela de aplicação **Editar componente de bloqueio** poderá encontrar no separador **Detalhes**—diferentes informações como, p. ex., tipo e modelo de componente, ID do componente, versão de firmware ou estado do componente, assim como informações sobre a porta, áreas e ativações. Adicionalmente, terá aqui a possibilidade de visualizar a localização do componente de bloqueio no Google Maps. No separador **Definições** pode visualizar todas as configurações definidas com relação ao fuso horário e ao calendário de férias/feriados, acesso e registo protocolar e opções de manutenção.



O estado das pilhas indicado corresponde ao estado no momento da última atualização ou do último registo transmitido ao protocolo. Pode acontecer, assim, que o estado das pilhas no componente de bloqueio não corresponda exatamente ao estado da pilha visualizado na Administração online do AirKey.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componente de bloqueio.
- > Clique na entrada da lista do componente de bloqueio que pretende editar.
- > Atribua no separador **Detalhes**, por exemplo, uma nova designação para a porta, um novo dado opcional adicional ⓘ ou registe a localização ou o endereço do componente de bloqueio. Estes serão verificados no sistema de controlo de acessos quanto à sua singularidade.

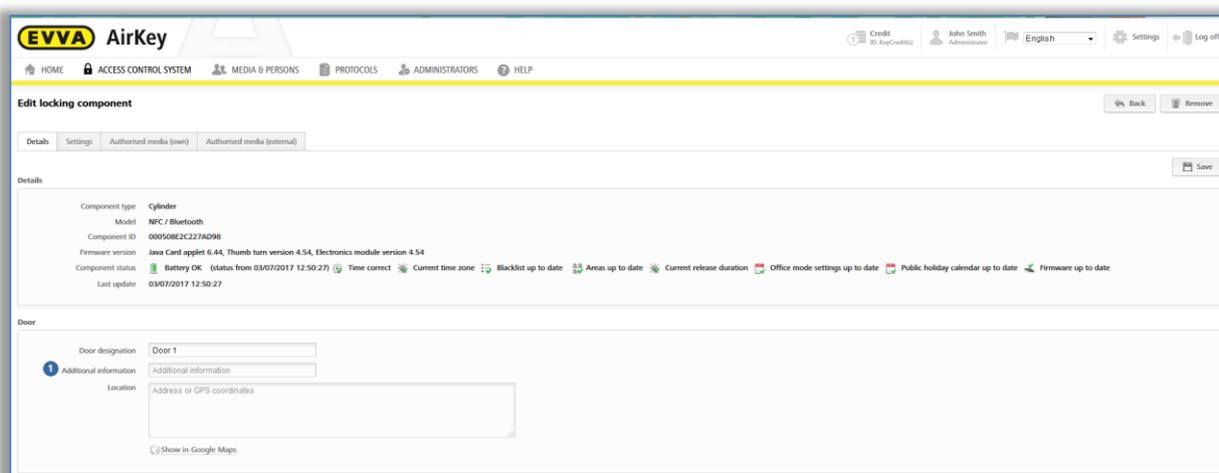


Figura 140: Editar componente de bloqueio

- > A atribuição de áreas para o componente de bloqueio selecionado pode ser editada no bloco [Áreas](#).

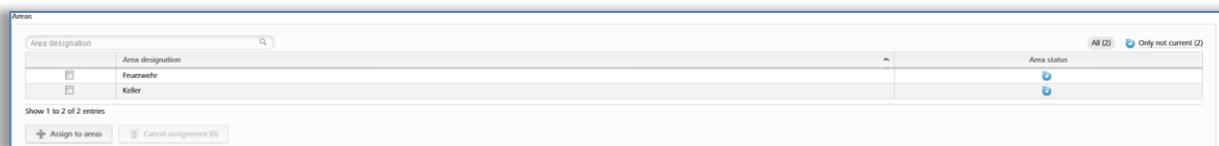


Figura 141: Áreas

- > Opcionalmente, poderá ativar o componente de bloqueio para outros sistemas de bloqueio. Poderá administrar as respetivas ativações, neste caso, no bloco Ativação de partilha. Poderá obter mais informações a respeito das ativações no capítulo [Trabalhar com vários sistemas de bloqueio AirKey](#).

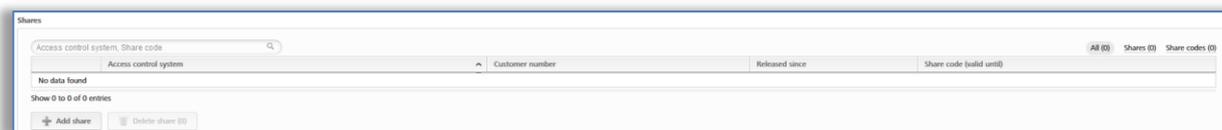


Figura 142: Ativações

- > Opcionalmente, poderá inserir um comentário sobre o componente de bloqueio no bloco **Observações**.

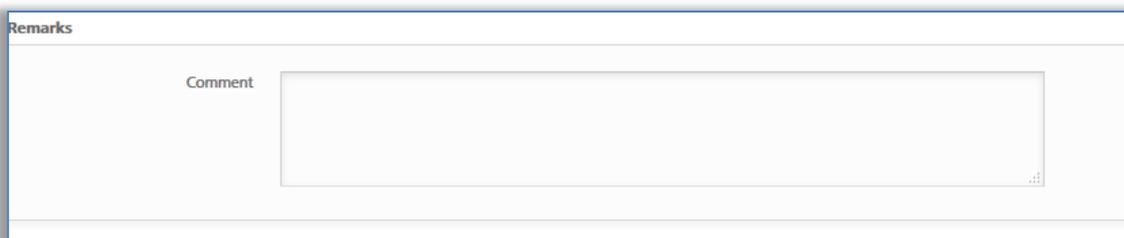


Figura 143: Editar componente de bloqueio

No separador **Definições**, poderá, como já mencionado, administrar opções para o fuso horário e calendário de férias/feriados, acessos ou registos protocolares e opções de reparação.

- > No caso de aplicar vários fusos horários no âmbito de um sistema de controlo de acessos, a cada componente de bloqueio pode ser atribuído um fuso horário próprio, que já esteja criado e configurado na Administração online do AirKey. Normalmente, aplica-se por defeito o fuso horário definido.
- > O calendário de dias de férias/feriados pode ser aqui selecionado ou retirado para cada componente de bloqueio. Caso já não se lembre exatamente das suas definições em relação aos dias de férias/feriados, está disponível aqui um link para o calendário de dias de férias/feriados.

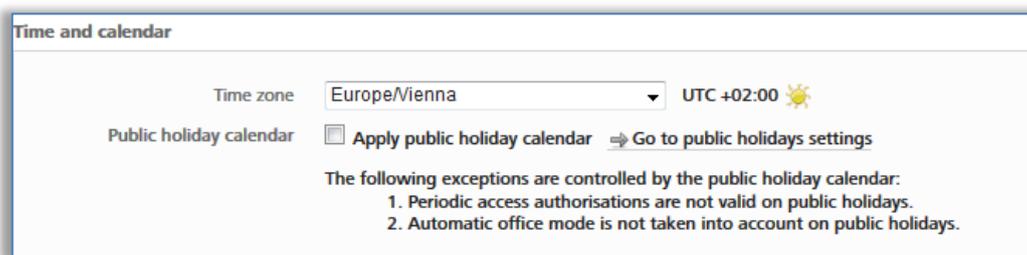


Figura 144: Definições – Horas e calendário

- > Poderá permitir para cada componente de bloqueio uma abertura permanente manual. Assim que esta esteja selecionada, surge a possibilidade de ativar para a abertura permanente automática.

Além disso, poderá alterar o tempo de ativação ou ativar / desativar a atualização após cada desbloqueio. Ver também o capítulo [Valores por defeito \(para todos os novos componentes de bloqueio adicionados\)](#).

- > Adicionalmente, o modo Hands-free (mãos-livres) pode ser permitido, ou não, para o componente de bloqueio individual. Se for permitido o modo Hands-free (mãos-livres), o modo mãos-livres pode ser ativado na aplicação AirKey para este componente de bloqueio. Caso contrário, este não pode ser ativado na aplicação

AirKey para este componente de bloqueio. Para mais detalhes sobre o modo Hands-free (mãos livres), consulte o capítulo [Vista geral da função Hands-free \(mãos livres\)](#).

- > Para cada componente de bloqueio, tem a possibilidade de adequar a referência pessoal em registos protocolares. Normalmente, o valor por defeito é assumido das definições.
 - **Visíveis** permite que a indicação dos dados dos acessos referentes à pessoa fique permanentemente visível.
 - **Visíveis para ... dias** torna anónimos os dados dos acessos referentes à pessoa depois do número de dias definido.
 - **Não visíveis** torna permanentemente anónimos todos os dados dos acessos referentes à pessoa.

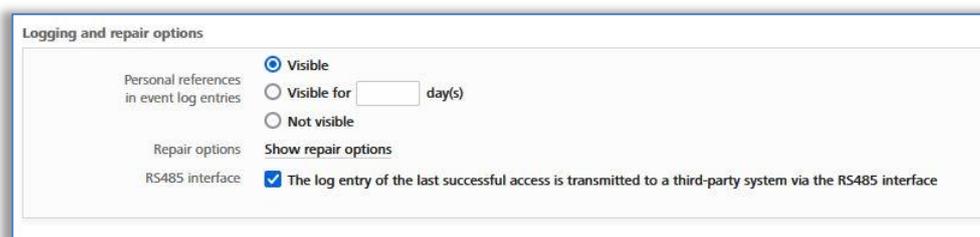


Figura 145: Registo em protocolo

- > Aqui, poderá encontrar também o link para as opções de reparação. Poderá obter mais informações sobre as opções de reparação em [Opções de reparação](#).
- > Em comparação com todos os outros componentes de bloqueio, os leitores de parede com Bluetooth oferecem adicionalmente a opção de ativar a **interface RS485**. O registo protocolar do último acesso bem-sucedido pode ser reencaminhado para um sistema de terceiros através da interface RS485. Poderá encontrar mais detalhes a este respeito no capítulo [Detalhes técnicos da interface RS485 para leitores de parede com Bluetooth](#).
- > Clique em **Guardar** para assumir as alterações do componente de bloqueio. De seguida, surge uma mensagem de confirmação.



Dependendo dos dados do componente de bloqueio que foram editados, pode dar-se o caso de surgir uma tarefa de manutenção para este componente de bloqueio. Através da atualização do componente de bloqueio com um smartphone com autorização de manutenção ou uma estação de codificação, as alterações são assumidas e a tarefa de manutenção desaparece.

5.5.4 Remover o componente de bloqueio

Assim que já não precisar de um componente de bloqueio no sistema de controlo de acessos AirKey, este pode ser removido do seu sistema de controlo de acessos.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componente de bloqueio.
- > Clique na entrada da lista do componente de bloqueio que pretende remover do seu sistema de controlo de acessos.

- > Clique, à direita, em cima, em **Remover** 1.

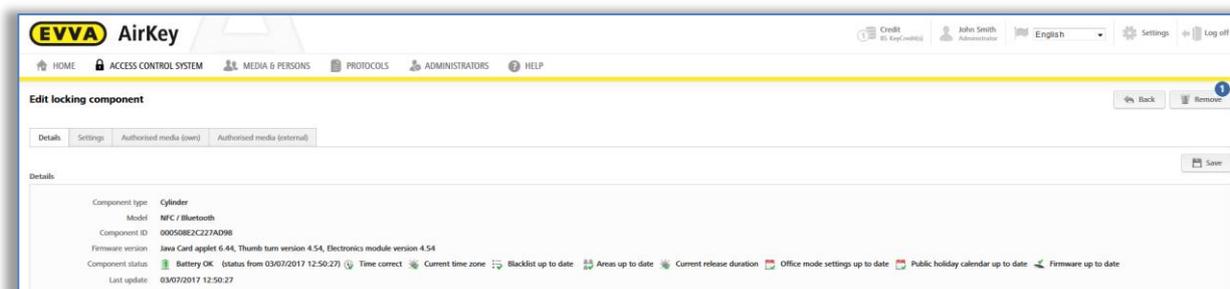


Figura 146: Remover componente de bloqueio

- > Confirme a pergunta de segurança com **Remover componente de bloqueio**.

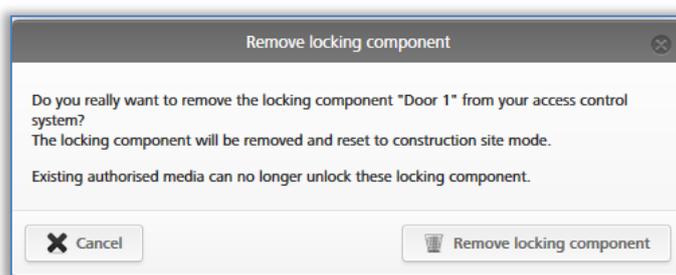


Figura 147: Pergunta de segurança

- > Surge uma mensagem de confirmação do processo e uma tarefa de manutenção que obriga a que o componente de bloqueio tenha de ser removido do sistema de controlo de acessos.

O processo só fica completo, quando o componente de bloqueio for atualizado com um smartphone com autorização de manutenção ou, opcionalmente, com uma estação de codificação. Contudo que o componente de bloqueio tenha sido atualizado, terá sido removido do sistema de controlo de acessos com sucesso.



Esta ação não pode ser revertida.

O componente de bloqueio, depois de removido, volta ao estado de fábrica e é reposto.

Os meios de acesso autorizados já não poderão bloquear mais o componente de bloqueio. As respetivas autorizações são automaticamente eliminadas e deixam de ser visualizadas.

5.5.5 Áreas

Podem ser reunidos vários componentes de bloqueio nas áreas para simplificar a administração das autorizações no seu sistema de controlo de acessos.

Poderá obter uma lista com todas as áreas na página inicial **Home** sob a caixa de seleção **Áreas** ou no menu principal **Sistema de controlo de acessos** → **Áreas**.

Na lista apresentada com as áreas, poderá fazer os ajustes seguintes:

- > No campo de pesquisa ❶, insira um critério de pesquisa com, pelo menos, três caracteres.
- > Clique no título da respetiva coluna para definir como critério de seleção.
- > A lista das área pode ser exportada para um ficheiro CSV para posterior edição ❷.

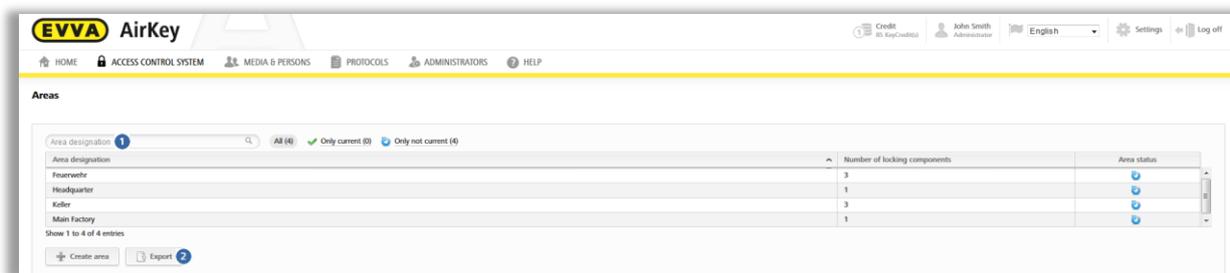


Figura 148: Sistema de controlo de acessos – Áreas

- > Selecione da lista a área pretendida para obter os detalhes da área selecionada.

5.5.6 Criar área

Normalmente, não estão criadas áreas. Terá de criar novas áreas para poder adicionar componentes de bloqueio a áreas.

- > Clique, na página inicial **Home**, na barra cinzenta do bloco **Sistema de controlo de acessos**, em **Adicionar** → **Criar área**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → **Criar área**.
- > Dê à área um nome inconfundível.
- > Poderá registar mais informações a respeito desta área no bloco **Observações** no campo **Comentário**.
- > Clique em **Guardar** ❶.

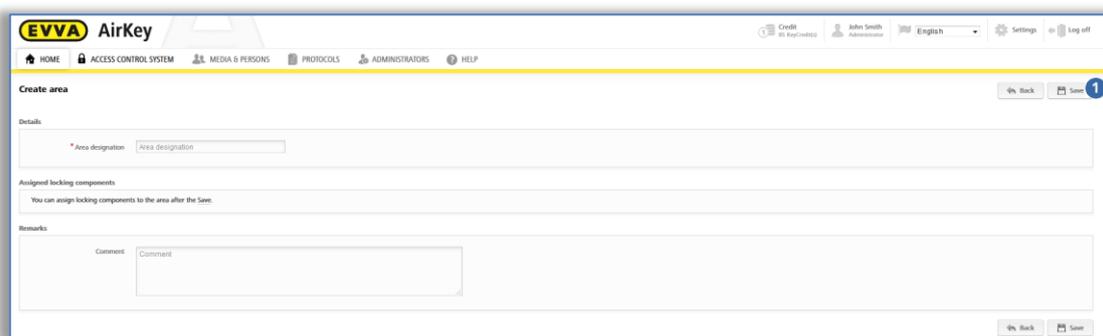


Figura 149: Criar área



A criação de uma área é indicada com a mensagem de confirmação "A área foi guardada". Só poderá adicionar componentes de bloqueio a uma área, depois de esta ter sido guardada com sucesso.

5.5.7 Atribuir componente de bloqueio a áreas

- > Selecione, na página inicial **Home**, a caixa de seleção **Áreas** ou no menu principal **Sistema de controlo de acessos** → **Áreas**.
- > Selecione, na lista, a área a que pretende adicionar o componente de bloqueio.
- > Os detalhes da área selecionada são exibidos. No **Estado da área** ❶ é visualizado se todos os componentes de bloqueio naquela área estão atualizados. No bloco **Atribuir componentes de bloqueio** ❷, estão listados todos os componentes de bloqueio que foram atribuídos à área.
- > Clique em **Atribuir componentes** ❸ para incluir um componente de bloqueio na área.

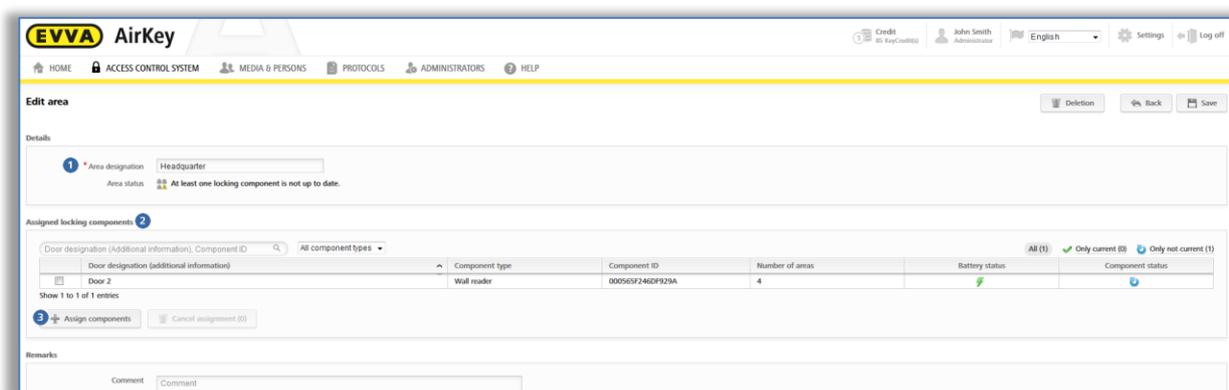


Figura 150: Editar área

É visualizada uma lista de todos os componentes de bloqueio que ainda não foram agregados a esta área.

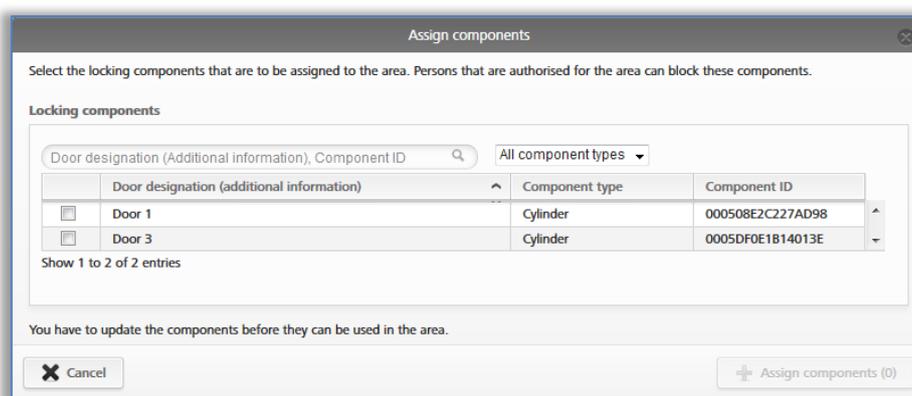


Figura 151: Atribuir componentes

- > Selecione os componentes de bloqueio pretendidos. (É possível uma seleção de vários componentes de bloqueio, também de diferentes tipos.)
- > Clique em **Atribuir componentes** para atribuir os componentes de bloqueio à área.
- > Clique em **Guardar** para assumir as alterações.

Surgem tarefas de manutenção para os componentes de bloqueio em questão, as quais podem desaparecer ao atualizar os respetivos componentes de bloqueio com um smartphone ou uma estação de codificação. Após as atualizações, a atribuição dos componentes de bloqueio à área fica concluída.



Um componente de bloqueio pode ser atribuído a um máximo de 96 áreas ao mesmo tempo.



Em alternativa, também poderá editar a atribuição da área a um componente de bloqueio diretamente nos detalhes do componente de bloqueio. Poderá encontrar mais informações a este respeito em [Editar componente de bloqueio](#).

5.5.8 Cancelar a atribuição de componentes de bloqueio a uma área

Para cancelar a atribuição de um ou mais componentes de bloqueio a uma área, proceda da seguinte forma:

- > Selecione, na página inicial **Home**, a caixa de seleção **Áreas** ou no menu principal **Sistema de controlo de acessos** → **Áreas**.
- > Selecione, na lista, a área a que foram atribuídos componentes de bloqueio e cuja atribuição deva ser cancelada.
- > Marque, na lista dos componentes de bloqueio atribuídos, as caixas de seleção dos componentes de bloqueio cuja atribuição deva ser cancelada. É possível fazer uma seleção múltipla.

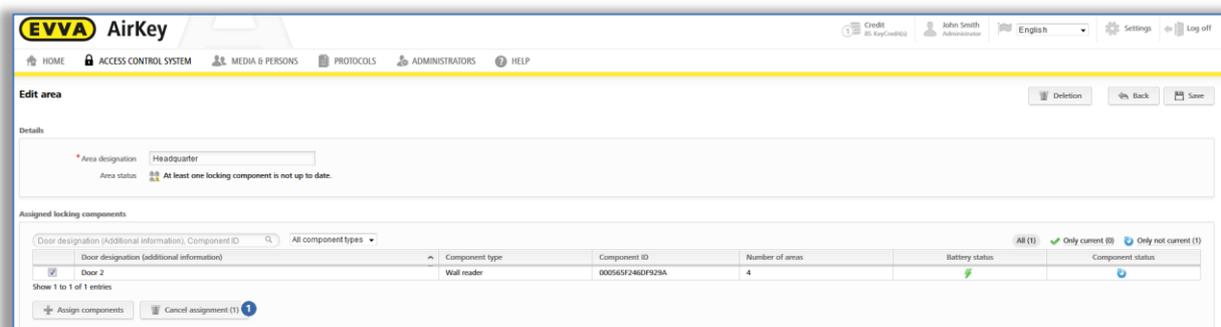


Figura 152: Marcar os componentes de bloqueio

- > Clique em **Cancelar atribuição** .
- > Surge uma janela de diálogo, onde se pode visualizar mais uma vez em que componentes de bloqueio a atribuição à área deva ser cancelada.
- > Confirme a pergunta de segurança igualmente com **Cancelar atribuição**.

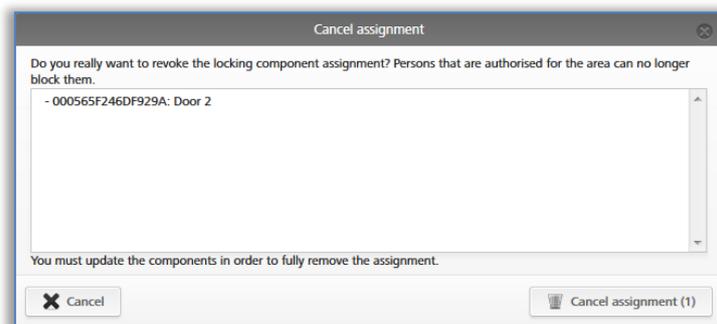


Figura 153: Cancelar atribuição

Surgem tarefas de manutenção para os componentes de bloqueio em questão, as quais podem desaparecer ao atualizar os respetivos componentes de bloqueio com um smartphone ou uma estação de codificação. Após as atualizações, a atribuição dos componentes de bloqueio à área fica concluída.



Depois de atualizar, as pessoas que possuem um meio com a autorização para esta área deixam de poder bloquear o componente de bloqueio cuja atribuição foi cancelada.



Em alternativa, também poderá editar a atribuição da área a um componente de bloqueio diretamente nos detalhes do componente de bloqueio. Poderá encontrar mais informações a este respeito em [Editar componente de bloqueio](#).

5.5.9 Eliminar área

- > Selecione, na página inicial **Home**, a caixa de seleção **Áreas** ou no menu principal **Sistema de controlo de acessos** → **Áreas**.
- > Selecione, na lista, a área que pretende eliminar.
- > Clique em **Apagar**

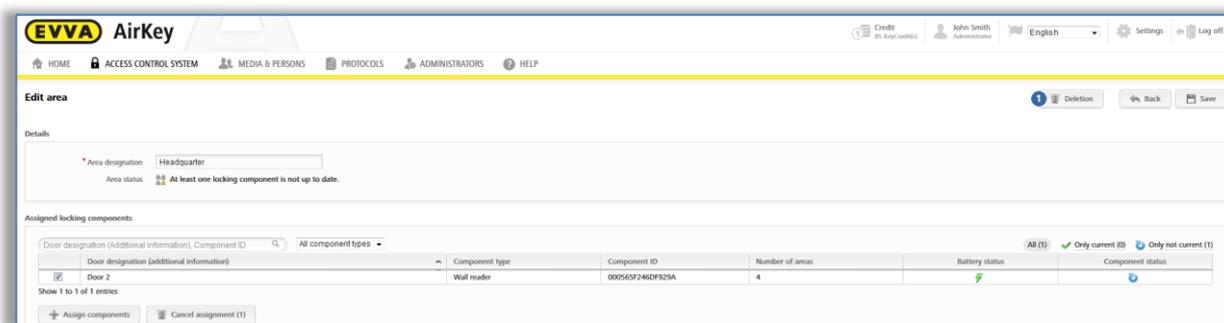


Figura 154: Apagar área



As autorizações existentes para uma área eliminada são automaticamente eliminadas no meio e deixam de ser visualizadas. Esta eliminação não pode ser revertida.

Caso ainda haja componentes de bloqueio atribuídas a esta área, receberá uma mensagem de erro.

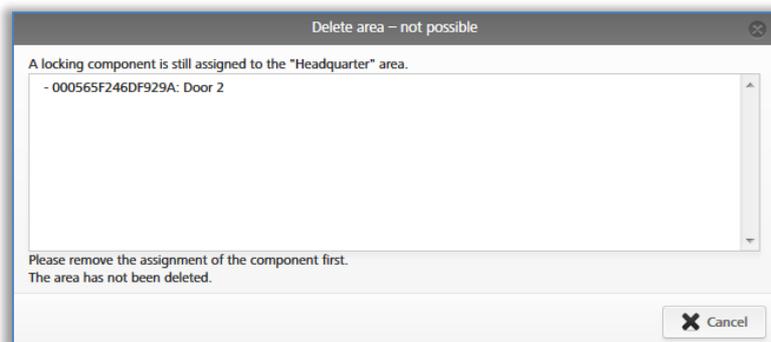


Figura 155: Eliminar área - não é possível

- > Cancele, primeiro, a atribuição de todos os componentes de bloqueio à área e repita, depois, o processo acima descrito. Poderá obter mais informações a respeito do cancelamento da atribuição de componentes de bloqueio a áreas em [Cancelar a atribuição de componentes de bloqueio a uma área](#).

5.5.10 Vista geral das autorizações

Na vista geral das autorizações, estão listadas todas as autorizações de meios a cada componente de bloqueio. A vista geral das autorizações está relacionada com um componente de bloqueio selecionado.



São listados todos os meios que possuem uma autorização para um componente de bloqueio. As autorizações exibidas não têm de estar, todavia, válidas, ou seja, um meio com um acesso único temporário das 08h00 às 17h00 é também listado na vista geral de autorizações para um componente de bloqueio mesmo depois das 17h00.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede** ou no menu principal **Sistema de controlo de acessos** → **Componentes de bloqueio**.
- > Selecione, na lista, o componente de bloqueio para o qual pretende visualizar a vista geral das autorizações.
- > Mude do separador **Detalhes** para **Meios autorizados (próprio)** para visualizar as autorizações do sistema de controlo de acessos próprio ou para **Meio autorizado (externo)** para visualizar as autorizações de sistemas de bloqueio de terceiros, para os quais o componente de bloqueio está ativado.

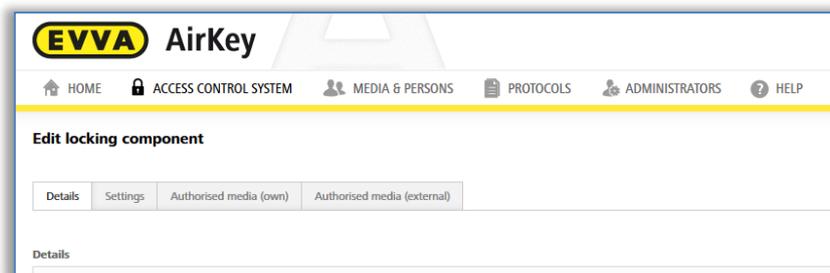


Figura 156: Separador da página "Editar componente de bloqueio"

Obtém uma lista de todas as pessoas e suas pessoas associadas listadas. Poderá também visualizar o tipo de meio.

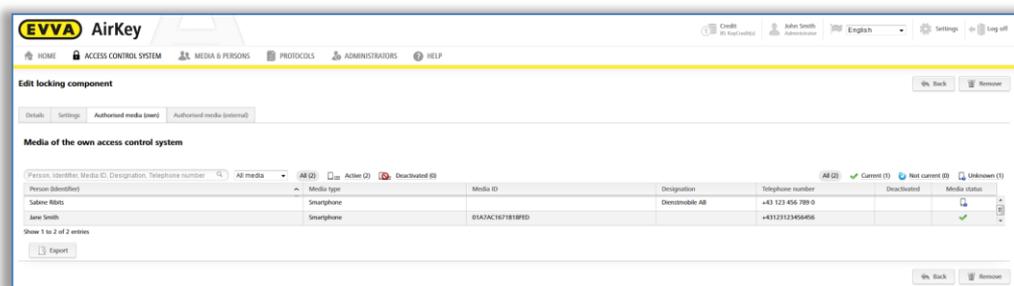


Figura 157: Meios autorizados (do próprio)

Dentro desta lista pode-se procurar, filtrar e classificar para receber determinadas autorizações.



Clique no nome de uma pessoa para ter acesso a partir da vista geral de autorizações diretamente às autorizações do meio da pessoa.

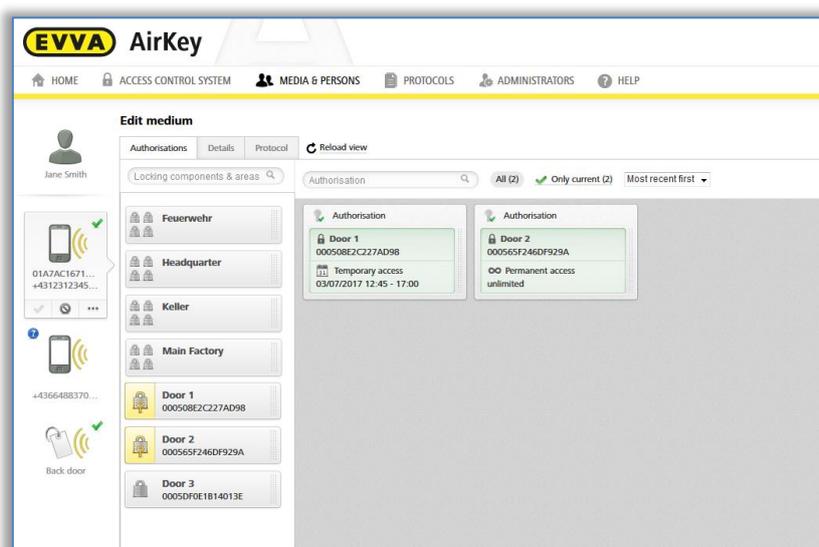


Figura 158: Editar meio

5.5.11 Tarefas de manutenção

Determinadas funções influenciam a configuração dos componentes de bloqueio. Estas alterações à configuração são consideradas tarefas de manutenção. As tarefas de manutenção estão associadas aos componentes de bloqueio cujo estado não está atualizado.

Poderá ter acesso a uma lista com as atuais tarefas de manutenção do sistema de controlo de acessos AirKey da seguinte forma:

- > Selecione na página inicial **Home** o link **Tarefas de manutenção**.
- > Ou clique na barra de estado em **Tarefas de manutenção**.
- > Ou selecione no menu principal **Sistema de controlo de acessos** → **Tarefas de manutenção**.

Recebe uma lista geral das tarefas de manutenção de todos os componentes de bloqueio do seu sistema de controlo de acessos AirKey.

Na lista de tarefas de manutenção, pode-se procurar pela designação da porta ou ID do componente. As colunas "Designação da porta (informação adicional)", "ID do componente" e "Tarefas de manutenção" podem ser ordenadas.

Adicionalmente, poderá proceder a uma priorização das tarefas de manutenção **1** e ao download de um PDF **2** da lista visualizada.

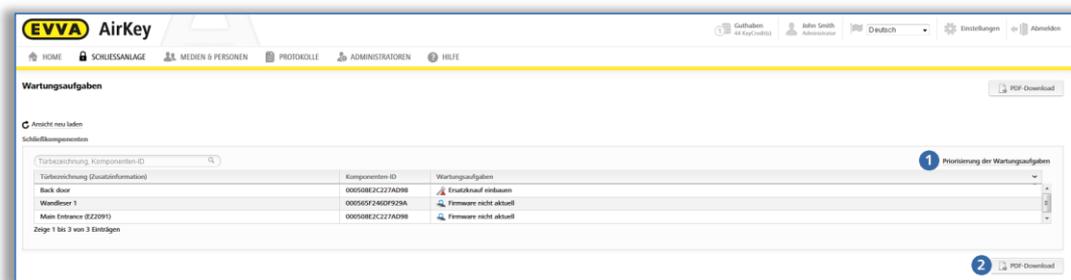


Figura 159: Tarefas de manutenção

A priorização das tarefas de manutenção é memorizada por sistema de controlo de acessos / cliente e utilizada no smartphone com a aplicação AirKey instalada e com a autorização de manutenção ativada.

- > Clique em **Priorização das tarefas de manutenção**.
- > De acordo com o caso de aplicação, os clientes poderão ter outras necessidades – com a função Drag & Drop leve as posições para a sequência desejada.
- > Guarde a alteração à priorização com **OK**.

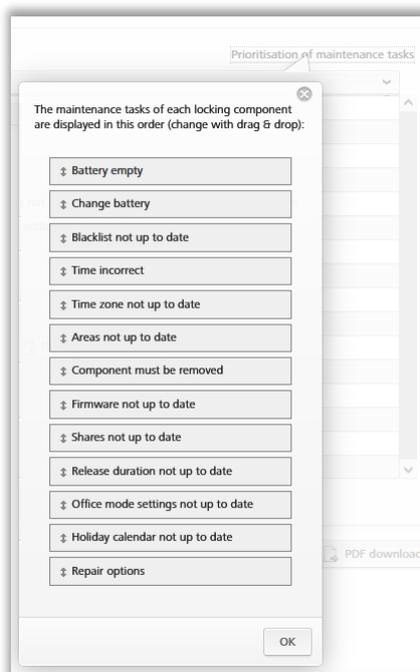


Figura 160: Priorização das tarefas de manutenção

A lista das tarefas de manutenção é apresentada, agora, com a priorização alterada. Cada posição da lista com as tarefas de manutenção está vinculada às páginas de detalhes do respetivo componente de bloqueio.

Se uma tarefa de manutenção tiver sido implementada através da atualização do componente de bloqueio, esta posição é automaticamente removida da lista de tarefas de manutenção.



A lista para todas as tarefas de manutenção existentes pode ser criada em ficheiro PDF e impressa. Utilize, para tal, o botão **Download de PDF**.

5.5.12 Dados de cliente – plano de bloqueio

Tal como anteriormente mencionado, no menu **Dados de cliente**, diversas informações, que foram inseridas durante o registo, podem ser alteradas em momento posterior, p. ex., o nome do sistema de bloqueio, o nome da empresa, assim como a pessoa de contacto.

Na página "Editar os dados de cliente", em cima, à direita, existe um botão, com o qual o plano de bloqueio de todo o sistema de bloqueio pode ser exportado. O plano de bloqueio inclui todos os componentes de bloqueio num sistema de bloqueio e os seus smartphones e meios de identificação atribuídos.

- > Clique no botão **Exportar plano de bloqueio**.
- > Selecione, na janela de diálogo "Exportar plano de bloqueio", o botão **Exportar**.
- > Clique no link do ficheiro CSV, que aparece na janela de diálogo subsequente.
- > Abra o ficheiro CSV com o programa desejado ou guarde o ficheiro.
- > Feche a janela de diálogo "Exportar plano de bloqueio" com um clique no botão **Fechar**.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q					
1					person (identi	Ferdinand	Max	Max	John	John	John	Martin	Susanne	Werner	Peter	Peter						
2					customer nun	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K					
3					designation		Karte Musters	Testphone Mt	Mobile John	iPhone	John Android		Mobile Susanne		Kombischlüssi	Samsung S6						
4					media ID	01513937COA	000524E1EEE	00058485F1B	01769CAD4E4	017DF822779	018D3E2A57C	01564B15279	01AC3BF5349	01FBB248091	0005A7592B8	0188626927E8A567						
5					media type	Smartphone (Card	Card	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	0	3	0	0	1	0	
9					Wandleler	airkey_OW3K	WALLREADER	0005CSB3F1E9C207		2	1	4		0	7	5	B		3	1	6	3
10																						

Figura 161: Plano de bloqueio



O estado da administração Online do AirKey é que é utilizado para a avaliação do estado de autorização, não o estado REAL no meio. Isto significa que o plano de bloqueio só estará correto quando todos os componentes e meios estiverem atualizados.

Legendas do plano de bloqueio:

- > **0 – Não autorizado:** O meio não possui nenhuma autorização para o componente de bloqueio e para nenhuma área à qual o componente de bloqueio esteja atribuído.
- > **1 – Com autorização permanente sem data de validade:** O meio possui estritamente uma autorização permanente sem data de validade para o componente de

bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.

- > **2 – Autorização permanente com data de validade:** (1) não se aplica e o meio possui estritamente uma autorização permanente com data de validade em momento futuro para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.
- > **3 – Autorização periódica sem data de validade:** (1) e (2) não se aplicam e o meio possui estritamente uma autorização periódica sem data de validade para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.
- > **4 – Autorização periódica com data de validade:** (1), (2) e (3) não se aplicam e o meio possui estritamente uma autorização periódica com data de validade em momento no futuro para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.
- > **5 – Autorização única:** (1), (2), (3) e (4) não se aplicam e o meio possui estritamente uma autorização única com data de validade em momento no futuro para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.
- > **6 – Autorização individual:** (1), (2), (3), (4) e (5) não se aplicam e o meio possui estritamente uma autorização individual com, pelo menos, uma subautorização com data de validade em momento no futuro para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído e mais nenhuma autorização para o componente de bloqueio ou uma área à qual o componente de bloqueio esteja atribuído.
- > **7 – Várias autorizações:** O meio possui, pelo menos, duas autorizações para o componente de bloqueio ou uma área, à qual o componente de bloqueio esteja atribuído, que ainda não expiraram.
- > **B – Blacklist:** O meio está desativado, portanto, está registado na Blacklist do componente de bloqueio. As autorizações do meio perdem, desta forma, a sua validade.
- > **E – Autorização expirada (de todos os tipos):** Todas as autorizações do meio para o componente de bloqueio ou uma área, à qual o componente de bloqueio esteja atribuído, expiraram.

5.6 Meios e pessoas

No menu principal **Meios e pessoas** ¹ administre todas as pessoas, meios e autorizações no sistema de controlo de acessos AirKey.

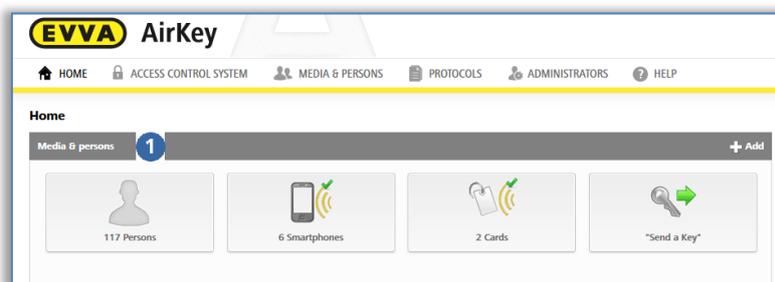


Figura 162: Meios e pessoas

5.6.1 Vista geral das pessoas

Se seleccionar, na página inicial **Home**, a caixa de selecção **Pessoas** ou, no menu principal, **Meios e pessoas** → **Pessoas**, obterá uma lista de todas as pessoas criadas, incluindo o número de meios e o seu estado.

Na lista visualizada, poderá utilizar as funções seguintes:

- > No campo de pesquisa ¹, insira um critério de pesquisa com, pelo menos, 3 caracteres. Selecione o primeiro nome, último nome, identificação ou endereço de e-mail.
- > Clique no título da respetiva coluna para definir como critério de selecção ².
- > Também poderá exportar toda a lista para um ficheiro CSV para posterior edição ³.

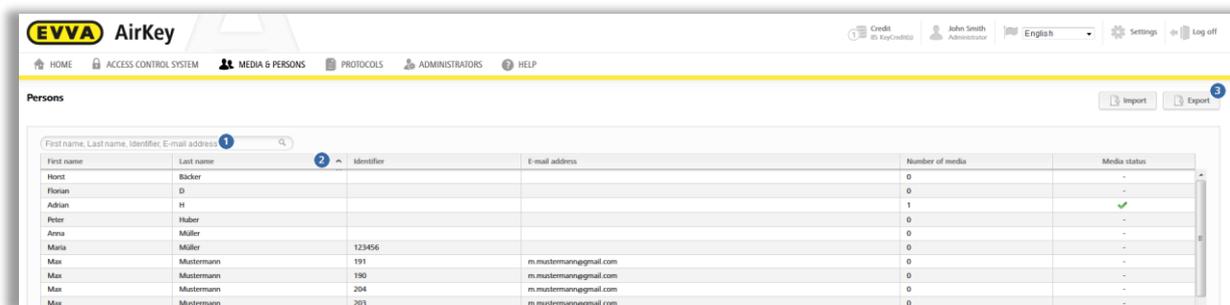


Figura 163: Pessoas

5.6.2 Criar pessoa: ver o capítulo 4.7

5.6.3 Editar pessoa

Na vista de detalhes "Editar pessoa", poderá alterar os detalhes e os dados de contacto de uma pessoa ou atribuir-lhe um novo meio.

- > Selecione, na página inicial **Home**, a caixa de selecção **Pessoas**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa a quem pretende fazer alterações.
- > Altere os respetivos dados.
- > Clique em **Guardar**.

>

Na página "Editar pessoa", também pode ser criada a confirmação de transferência **1**. Trata-se de uma confirmação que, após a criação e a atribuição de todas as autorizações necessárias, é enviada à pessoa. A confirmação mostra o tipo de meios e o tipo de autorizações destes meios que a pessoa possui no momento da emissão.

- > Selecione da lista geral a pessoa para a qual pretende criar uma confirmação de transferência.
- > Na página "Editar pessoa" clique no botão **Gerar o certificado de entrega (PDF)**.
- > Aparece a janela de diálogo "Gerar o certificado de entrega (PDF)", sendo que o ficheiro PDF aparece como link.
- > Clique no link e abra o ficheiro PDF com o seu leitor de PDF; em alternativa, pode também guardar o ficheiro.
- > Feche a janela de diálogo com o botão **Fechar**.

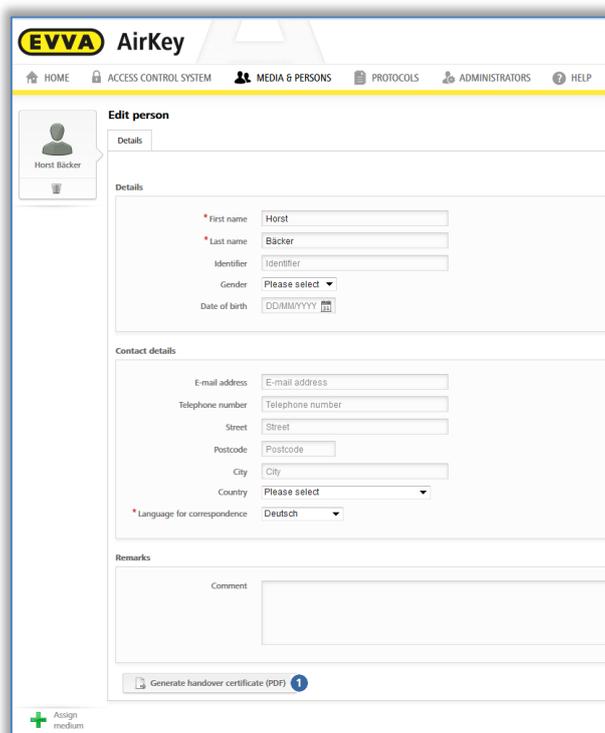


Figura 164: Gerar o certificado de entrega

Headquarter Wien Created by: John Smith

EVVA AirKey personal details

Person

Florian D

- Identifier: Technik
- Gender: Male
- Date of birth: 18.05.1980
- E-mail address: FD@test.com
- Telephone number: +431234567890
- Street: Hauptstrasse 1
- Postcode: 1010
- City: Wien
- Country: Austria
- Remarks: -

Media Up to date

- Media type: Smartphone (Android)
- Media ID: 01A46636A2ECB86D
- Telephone number: +4366488370
- Last update: 30.01.2018
- AirKey app version: 1.7.6
- Registration progress: completed
- Registration code: -
- Maintenance mode: active
- Show protocol data: active
- Release duration: normal
- Office mode: active
- PIN code status: inactive
- Remarks: -

Authorisation 1

- Type: Periodic access
- for area: Area 1
- valid from: 30.01.2018
- valid until: unlimited

Day	from	to
Wed	04:15	11:00

Figura 165: Certificado de entrega (PDF)

5.6.4 Eliminar pessoa

Se pretender remover uma pessoa do sistema de controlo de acessos AirKey, poderá eliminar a pessoa.



Não é possível eliminar uma pessoa a quem ainda haja meios atribuídos. Assegure-se, por isso, de que, antes de a eliminar, tenha cancelado a atribuição de todos os meios relativamente a esta pessoa.

- > Selecione, na página inicial **Home**, a caixa de seleção **Pessoas**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa que pretende eliminar.
- > Clique no símbolo **Caixote do lixo** **1**.

Figura 166: Eliminar pessoa

- > Confirme a pergunta de segurança com Eliminar pessoa.

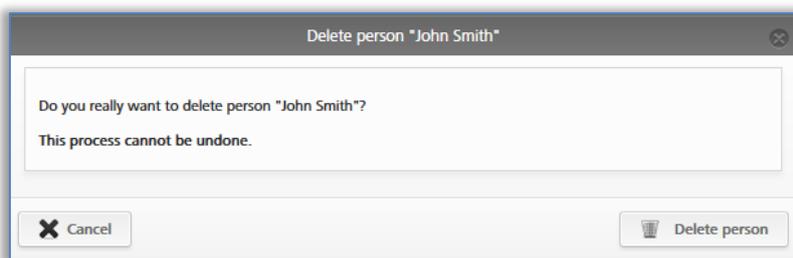


Figura 167: Eliminar pessoa – Pergunta de segurança



A pessoa eliminada deixará de aparecer na lista de pessoas. Nos registos protocolares, antes de eliminar a pessoa, a referência pessoal aos componentes de bloqueio e meios continua a ser documentada.

5.6.5 Atribuir meio a uma pessoa

Tem de atribuir o meio a uma pessoa para poder atribuir autorizações. Só assim obterá uma referência pessoal nos acessos.

- > Selecione, na página inicial **Home**, a caixa de seleção **Pessoas**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa a quem pretende atribuir um meio.
- > Clique no botão **Atribuir meio** .

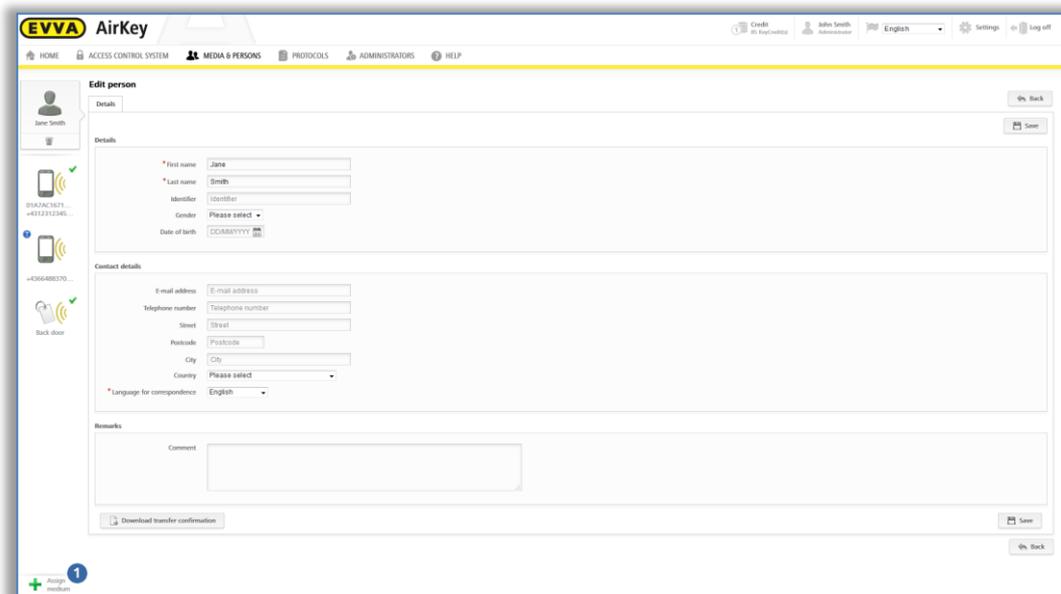


Figura 168: Atribuir meio

É salientada uma lista com todos os meios que pode atribuir à pessoa. Poderá ordenar a lista, filtrar por tipos de meios ou procurar determinados registos.



Só são apresentados meios do seu sistema de controlo de acessos que ainda não foram atribuídos a nenhuma pessoa.

- > Selecione o meio pretendido e clique em **Continuar**.

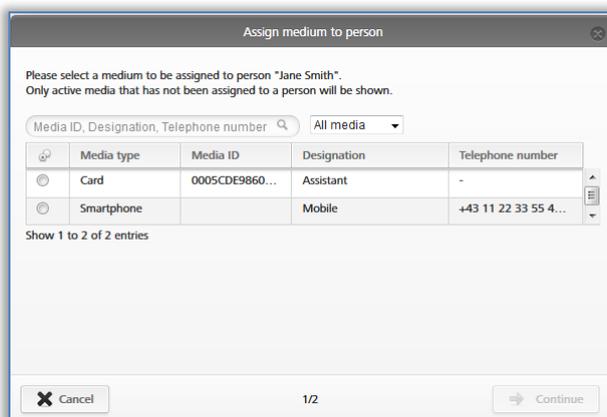


Figura 169: Atribuir meio à pessoa

Depois de seleccionar o meio, são exibidos os detalhes. Se necessário, clique em **Voltar** e selecione um outro meio.

- > Clique em **Atribuir meio**, para concluir o processo.

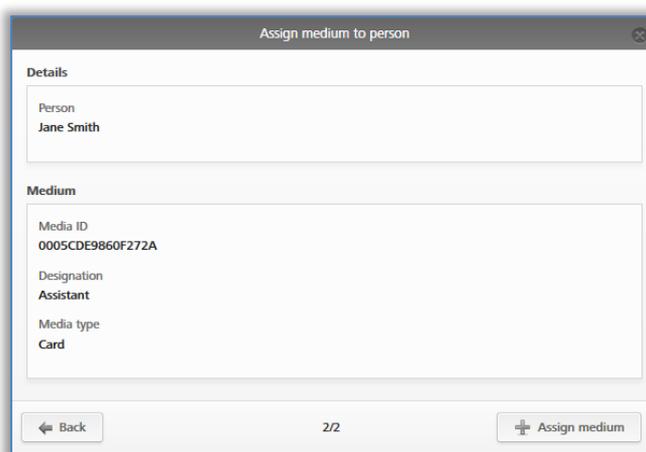


Figura 170: Atribuir meio à pessoa



Em alternativa, poderá fazer a atribuição de um meio à pessoa através do meio. Poderá encontrar mais informações em [Atribuir pessoa a um meio](#).



Podem ser atribuídos vários meios a uma pessoa (smartphones, cartões, porta-chaves ou chaves combinadas).

5.6.6 Vista geral dos meios

No menu principal **Meios e pessoas** → **Meios** obterá uma lista com todos os meios (smartphones, cartões, porta-chaves e chaves combinadas) através da qual pode visualizar, em geral, as autorizações atribuídas, uma eventual desativação e o atual estado do meio.

Nesta lista com os meios, poderá procurar meios, filtrar determinado estado do meio, alterar a ordem ou exportar toda a lista para um ficheiro CSV.

Person Identifier	Media ID	Designation	Telephone number	Authorization	Media status
Adrian H	01C8270504F1032F	Smartphone Compact Z3	+43 123 123 123 123	2	Deactivated
Mia Mustermann (13)	0181400953282850	iPhone	+43 11 22 33 44 55	1	Active
Mia Mustermann (7)	00058543255819	Legit	-	-	Active
Sabine Rißes		Demobile AB	+43 123 456 789 0	2	Active
Hamperer Sets (AirKey)			-	-	Active
Jane Smith	01A7AC1671818FED		+43123123456456	2	Active
Jane Smith			-	-	Active
	0005CDE986F272A	Assistant	-	-	Active
		Mobile	+43 11 22 33 55 44 66	0	Active

Figura 171: Lista de meios

5.6.7 Adicionar meio

Para administrar um meio no seu sistema de controlo de acessos, tem de criá-lo, em primeiro lugar.

- > Clique, na página inicial **Home**, na barra cinzenta do bloco **Meios e pessoas**, em **Adicionar** → **Adicionar meio**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Adicionar meio**.
- > Ou selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões** e aí em **Adicionar meio**.

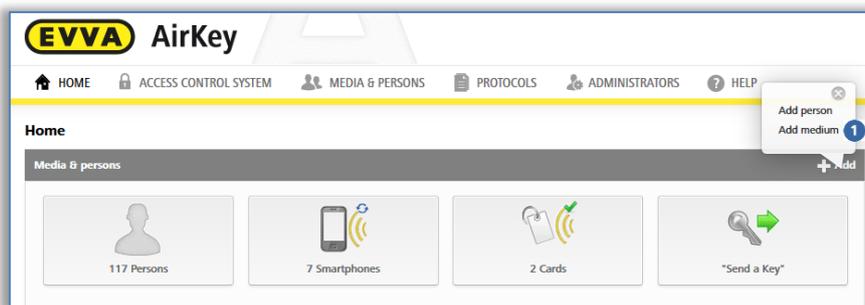


Figura 172: Adicionar meio

- > Selecione o tipo de meio do novo meio.

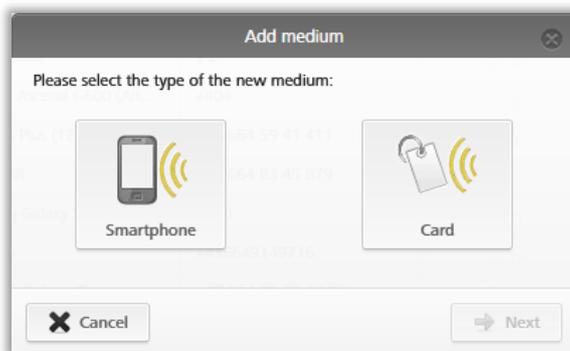


Figura 173: Criar novo meio



Do ponto de vista da aplicação, não há diferença entre cartões, porta-chaves, pulseiras e chaves combinadas, por isso, os porta-chaves e as chaves combinadas precisam de ser criados como tipo de meio **Cartão**.

5.6.8 [Criar smartphone](#): ver o capítulo 4.8

5.6.9 Criar cartão, porta-chaves, pulseiras ou chave combinada

Contanto que não tenha disponível uma estação de codificação, poderá adicionar ao sistema de controlo de acessos cartões, porta-chaves, pulseiras ou chaves combinadas com um smartphone com autorização de manutenção. Para tal, siga as informações em [Adicionar cartões, porta-chaves e chaves combinadas com o smartphone](#).

- > Insira uma designação e clique em **Continuar**.
- > Coloque o cartão, o porta-chaves, o pulseira ou a chave combinada sobre estação de codificação.

Se o processo tiver sido concluído com sucesso, abre-se automaticamente uma vista com os detalhes deste meio.



Recomenda-se fortemente realizar uma pré-configuração suficiente dos meios (cartões, porta-chaves, pulseiras ou chaves combinadas) com autorizações permanentes sem data de validade (meios de emergência) e guardá-los em locais seguros, para que o sistema de controlo de acessos também possa funcionar independentemente da Administração online do AirKey. Poderá obter informações a respeito da atribuição de autorizações em [Autorizações](#).



A adição de uma chave combinada com a estação de codificação tem de ser feita com o lado da chave combinada onde se encontra o símbolo RFID. A chave combinada tem de ser encostada diretamente à estação de codificação. A adição não é possível em toda a área de leitura da estação de codificação – no caso do tipo em questão (HID Omnikey 5421), a chave combinada só é reconhecida no terço superior e inferior da estação de codificação.



Poderá saber como pode adicionar meios com um smartphone com autorização de manutenção ao seu sistema de controlo de acessos AirKey em [Adicionar cartões, porta-chaves e chaves combinadas com um smartphone](#).

5.6.10 Editar meio

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desejado.
- > Selecione o separador **Detalhes** para editar o meio.

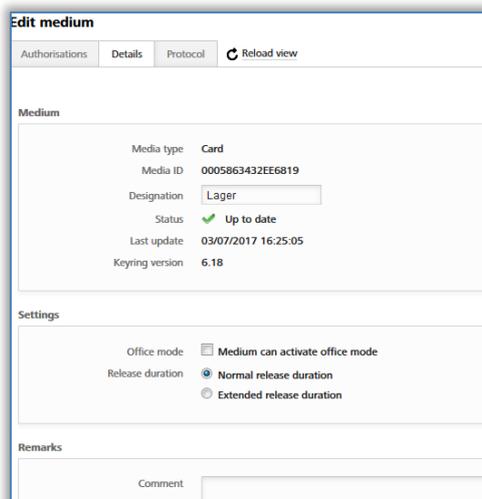


Figura 174: Editar meio – Cartão

- > Ao clicar em **Guardar**, as alterações são assumidas.

5.6.11 [Atribuir uma pessoa a um meio](#): ver o capítulo 4.13

5.6.12 Autorizações

Poderá regular o acesso de pessoas aos componentes de bloqueio através das autorizações. Para poder criar autorizações para os meios, os meios já têm de estar atribuídos a uma pessoa (poderá obter mais informações a respeito da atribuição de um meio a uma pessoa em [Atribuir meio a uma pessoa](#)).

Poderá obter a vista geral das autorizações de um meio da seguinte forma:

- > Selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desejado.
- > O meio ❶ já está selecionado (podem ser atribuídos vários meios a uma pessoa).
- > Aqui, visualiza todas as autorizações já atribuídas ❷.

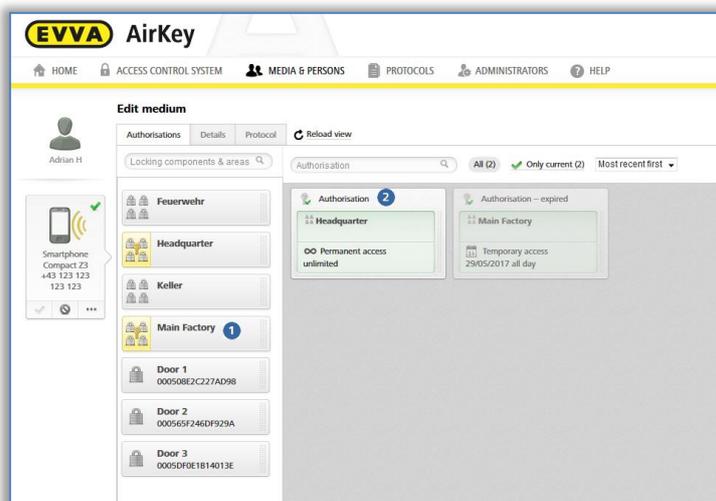


Figura 175: Vista geral das autorizações



Cor de fundo das autorizações:

- **Verde** = O estado está atualizado, a autorização foi criada e o meio atualizado.
- **Azul** = A autorização foi criada, o meio ainda não está atualizado.
- **Amarelo** = A autorização foi alterada ou eliminada, ainda não foi criada.
- **Cinzeno** = A autorização já expirou.



Em alternativa, poderá ter acesso à vista geral das autorizações também pelo menu principal **Meios e pessoas** → **Pessoas**, se selecionar, da lista de pessoas, uma pessoa que possua um meio. Nesta sequência, terá de clicar apenas no símbolo do meio do lado esquerdo, por baixo da pessoa selecionada.

5.6.13 [Atribuir autorizações](#): ver o capítulo 4.14

5.6.14 [Criar autorização](#): ver o capítulo 4.16

5.6.15 Alterar autorização

As autorizações podem ser alteradas a qualquer momento na Administração online do AirKey.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio cujas autorizações devam ser alteradas.
- > No separador "Autorização", clique na autorização que pretende alterar.
- > Ou arraste por Drag & Drop a porta / área novamente para a área central.

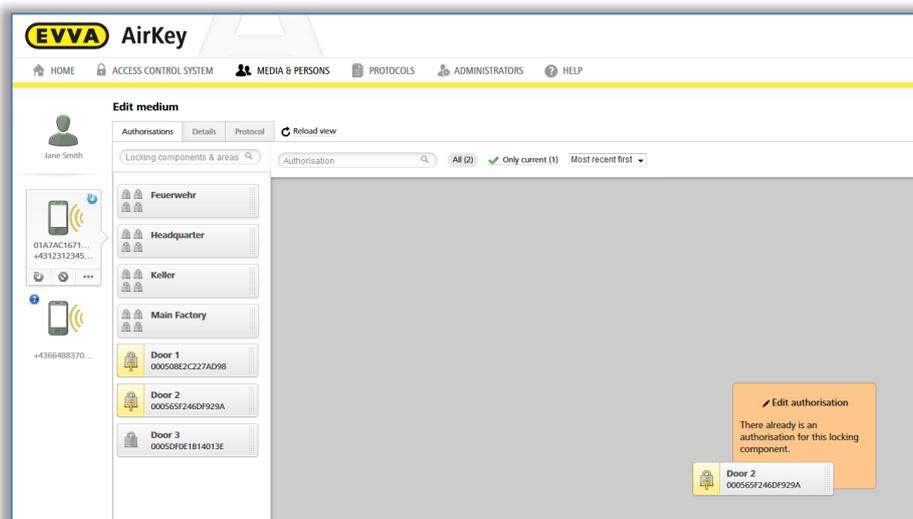


Figura 176: Editar meio – Alterar autorização

- > São visualizados os detalhes da autorização existente.
- > Clique em **Alterar**

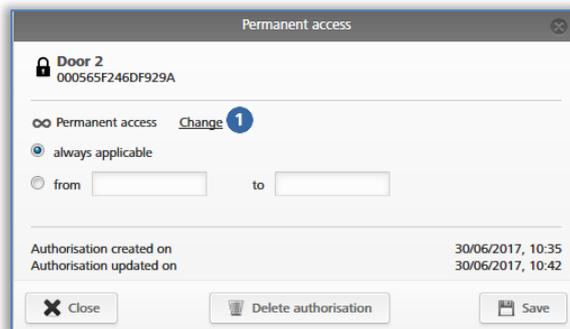


Figura 177: Alterar autorização

- > Selecione o novo tipo de acesso.
- > Clique em **Alterar acesso** 1.

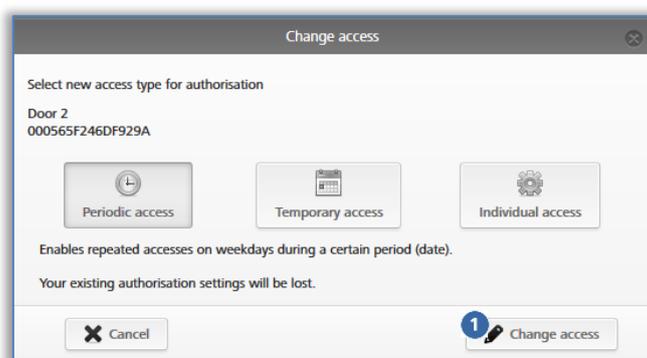


Figura 178: Alterar acesso

- > Insira os valores alterados no respetivo tipo de acesso.
- > Clique em **Guardar**.



Para alterar autorizações, são necessários créditos sob a forma de KeyCredits.

- > Clique no botão amarelo **Criar 1 autorização**. Poderá encontrar mais informações a este respeito em [Criar autorização](#).
- > Atualize o meio com "Pull to Refresh" num smartphone ou com a estação de codificação no caso de um cartão, um porta-chaves, um pulseira ou uma chave combinada, para concluir o processo com sucesso.

5.6.16 Apagar autorização

Caso uma autorização deixe de ser necessária, poderá eliminar a qualquer momento essa autorização já atribuída.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio cujas autorizações devam ser eliminadas.
- > No separador "Autorização", clique na autorização que pretende eliminar.

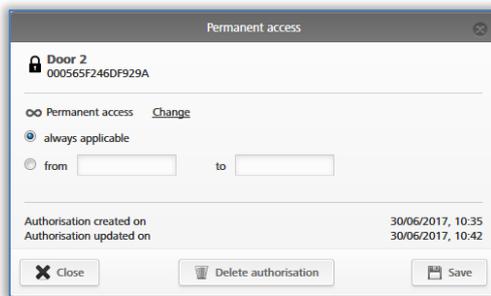


Figura 179: Acesso permanente

- > Ou arraste por Drag & Drop a porta / área para fora da área central para o campo de fundo laranja **Apagar autorização**.

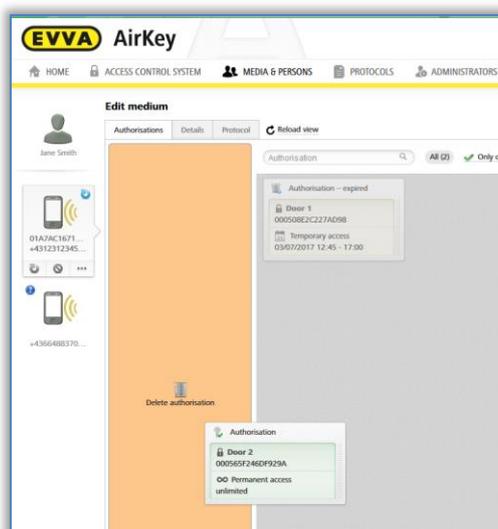


Figura 180: Eliminar autorização

- > Clique em **Apagar autorização**.
- > Confirme a pergunta de segurança com **Apagar autorização**.



Figura 181: Eliminar autorização

- > Atualize o meio com "Pull to Refresh" num smartphone ou com a estação de codificação no caso de um cartão, um porta-chaves, um pulseira ou uma chave combinada, para concluir o processo com sucesso.



A eliminação de autorizações não gasta KeyCredits e tem efeito imediato. É obrigatória a atualização do meio para concluir o processo de eliminação com sucesso.

Não utilize esta função para reagir à perda de meios. Só poderá eliminar aqui autorizações, caso o meio esteja disponível fisicamente. Utilize, no caso de perda, a função Desativar meio.

Se pretender eliminar todas as autorizações do meio, utilize a função [Esvaziar meio](#).

5.6.17 Desativar meio

Utilize a função "Desativar meio", se existir um risco de segurança e todas as autorizações do meio deverem ser invalidadas, p. ex., devido a perda ou a um defeito do meio.



Figura 182: Desativar meio

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desejado.
- > Clique em **Desativar meio** 1.
- > Dê um motivo para a desativação. Se selecionar "Outros", o campo de introdução de 50 dígitos fica ativo.
- > Se necessário, forneça informações adicionais (máximo 500 caracteres) em "Outras observações".
- > Clique em **Continuar**.
- > Confirme a pergunta de segurança com **Desativar meio**.



Figura 183: Desativar meio – Pergunta de segurança

A desativação do meio é concluída com uma mensagem de confirmação.

Todas as autorizações que o meio possui são marcadas para eliminar. No caso de cartões, porta-chaves, pulseiras e chaves combinadas é realizado imediatamente um registo na lista negra para todos os componentes de bloqueio, para os quais o meio estava autorizado. No caso de um smartphone, este registo só é criado se o smartphone não tiver sido alcançado em cinco minutos. Um registo na lista negra significa que é criada uma tarefa de manutenção para o componente de bloqueio em questão. Até à atualização, os componentes de bloqueio em questão encontram-se num estado não atualizado.

- > Atualize os componentes de bloqueio para os quais o meio tinha uma autorização. Desta forma, a tarefa de manutenção é removida da lista negra e os meios desativados já não podem voltar a bloquear estes componentes de bloqueio.



Não utilize esta função para eliminar individualmente cada autorização do meio. A desativação de um meio é uma função que diz respeito a todas as autorizações do meio num sistema de controlo de acessos.

A desativação apenas se aplica ao seu sistema de controlo de acessos. Se um smartphone estiver registado em vários sistemas de bloqueio, o estado do smartphone nos restantes sistemas de bloqueio permanece atualizado e não desativado.

Se uma pessoa registou um smartphone em vários sistemas de bloqueio, os administradores de todos os sistemas de bloqueio envolvidos têm de ser notificados da desativação completa do smartphone.



O meio permanece atribuído à pessoa. Se pretender eliminar o meio, terá de cancelar a atribuição. Poderá encontrar mais informações a este respeito em [Cancelar atribuição](#).

5.6.18 Remover o meio desativado

Um meio desativado pode ser removido do sistema de controlo de acessos, sem que o meio tenha de estar presente. No caso de meios perdidos, roubados ou com defeito, os dados podem ser mantidos na Administração online do AirKey.



A remoção do meio desativado só é possível se o meio estiver completamente desativado. Isto significa que ou o meio foi atualizado em todos os componentes de bloqueio onde o meio tinha autorização, ou a lista negra foi gravada com uma atualização. Enquanto as condições acima não forem preenchidas, não é possível remover.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desativado que deve ser removido.
- > Clique, por baixo do símbolo do meio, no sinal Mais e selecione **Remover** 
- > Confirme, depois, a pergunta de segurança com **Remover meio** para remover o atual meio desativado do sistema de controlo de acessos.

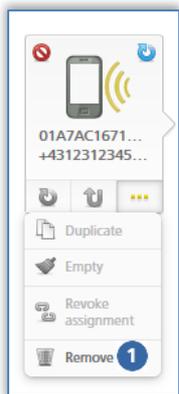


Figura 184: Remover o meio desativado

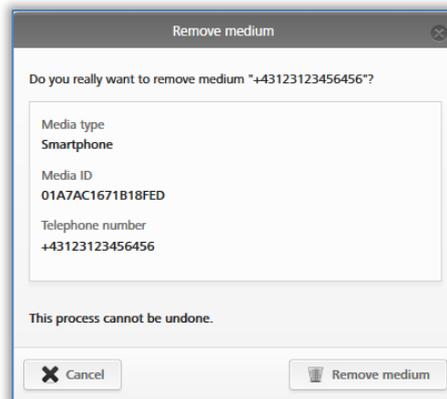


Figura 185: Remover meio – Pergunta de segurança

- > Surge uma mensagem de confirmação do processo e o meio deixa de estar listado no sistema de controlo de acessos.



Esta ação não pode ser revertida. Os meios que foram removidos deste forma deixam de estar listados no sistema de controlo de acessos e não poderão ser reutilizados.

Os meios encontram-se no estado de fábrica, mas não automaticamente.

5.6.19 Reativar meio

Um meio desativado, visível pelo círculo vermelho 1 do meio, pode ser reativado se voltar a estar disponível.



Figura 186: Reativar o meio desativado

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio que deva ser reativado.
- > Clique em **Reativar meio** por baixo do símbolo do meio.



Figura 187: Reativar meio

- > Indique o motivo para a reativação (máximo de 50 caracteres) e decida se as autorizações, que estavam válidas antes da desativação, devem ser restabelecidas.
- > Se necessário, registe informações adicionais (máximo 500 caracteres) em "Outras observações". Estas informações adicionais serão documentadas no respetivo registo protocolar.

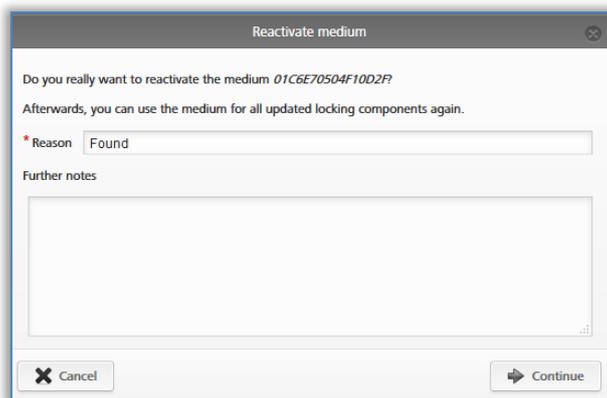


Figura 188: Reativar meio

- > Clique em **Continuar**.
- > Confirme uma das duas perguntas de segurança (dependendo da decisão, se as autorizações devem ser restabelecidas, ou não) com **Reativar meio**.

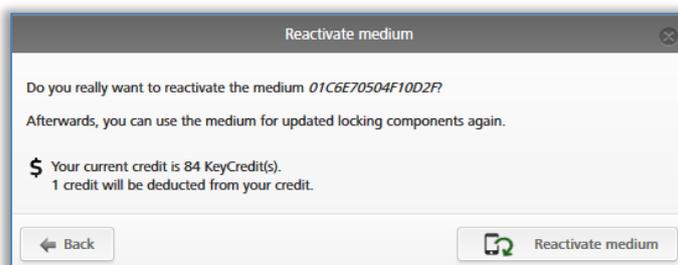


Figura 189: Reativar meio – Restabelecer autorizações

A reativação bem-sucedida de um meio é concluída com uma mensagem de confirmação.

Contanto que a lista negra para o meio reativado foi distribuída por todos os componentes de bloqueio autorizados, surgem novas tarefas de manutenção para estes componentes de bloqueio.

Atualize os componentes de bloqueio que receberam uma tarefa de manutenção devido à reativação de um meio. Só quando todos os registos na lista negra tiverem sido novamente removidos – ou seja, significa que todos os componentes de bloqueio em questão estão atualizados – é que o meio pode voltar a bloquear em todos os componentes de bloqueio.



A reativação apenas se aplica ao seu sistema de controlo de acessos. Se o smartphone tiver sido desativado em vários sistemas de bloqueio, o smartphone continua desativado nos outros sistemas de bloqueio e não pode bloquear nesses.

Se uma pessoa registou um smartphone em vários sistemas de bloqueio, os restantes administradores têm de ser notificados da desativação completa em todos os sistemas de bloqueio relevantes.



Ao restabelecer as autorizações, é debitado um KeyCredit. Neste caso, é necessário um crédito.

5.6.20 Troca de smartphone

Com a função "**Troca de smartphone**", transfira as autorizações e definições do AirKey existentes de um smartphone (exceto PIN e as definições locais do modo mãos-livres) para outro smartphone. O meio de origem é automaticamente desativado após uma troca bem-sucedida. Poderá obter mais informações sobre a troca do smartphone como administrador no capítulo [Iniciar a troca como administrador](#).

5.6.21 Duplicar meio

Com a função "Duplicar meio", transfira as autorizações existentes de um meio para um outro meio. Neste caso, existe a pré-condição de que o meio original a duplicar possua autorizações e que o meio duplicado já esteja criado e atribuído a uma pessoa.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio a duplicar.

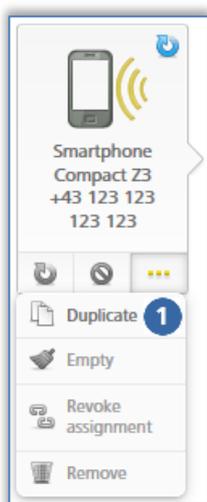


Figura 190: Duplicar um meio

- > Clique em **Mais...** ⓘ → **Duplicar**.
Abre-se uma lista geral com todos os meios atribuídos a uma pessoa – o meio a duplicar não está incluído nesta lista.
- > Selecione o meio alvo e clique em **Continuar**.
- > Confirme o processo com **Duplicar meio**.

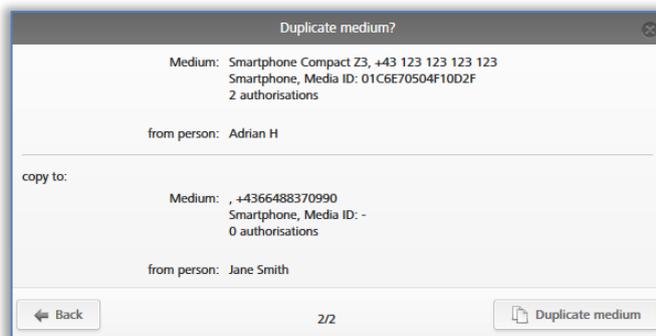


Figura 191: Duplicar meio

Recebe a confirmação de que a duplicação foi realizada com sucesso. O ecrã muda para a vista geral de autorizações do meio alvo.



As autorizações existentes no meio alvo são reescritas.

Para concluir o processo de duplicação, o meio alvo tem de ser produzido com **Criar as autorizações** e atualizado. Poderá obter mais informações a respeito da produção de um meio em [Criar autorização](#).



Este processo custa um KeyCredit. Neste caso, é necessário um crédito.

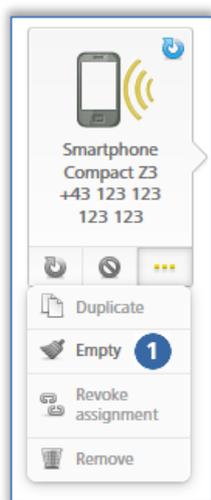


Se tiver um grande número de pessoas na sua Administração online do AirKey (ver [Importar dados de pessoas](#)) e se as autorizações destas forem todas idênticas, poderá, através da função "Duplicar meio", em pouco tempo, atribuir uma grande quantidade de meios com as mesmas autorizações às respetivas pessoas.

5.6.22 Esvaziar meio

Esvazie o meio quando pretender eliminar todas as autorizações do meio.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio que pretende esvaziar.



- > Clique em **Mais...** ⓘ → **Vazio**.
- > Conclua o processo com **Meio vazio**.

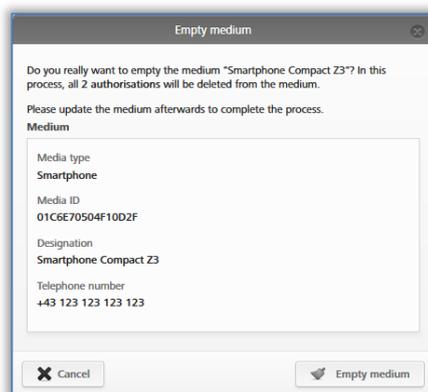


Figura 192: Meio vazio

Figura 193: Meio vazio – Pergunta de segurança

Todas as autorizações são marcadas para eliminar. O meio tem de ser atualizado para que a eliminação das autorizações possa ter efeito.



A eliminação das autorizações não gasta KeyCredits. É obrigatória a atualização do meio para concluir o processo de eliminação com sucesso.

Não utilize esta função para reagir à perda de meios. Só poderá eliminar aqui autorizações, caso o meio esteja à disposição. Utilize, no caso de perda, a função [Desativar meio](#).

Se pretender eliminar uma autorização, utilize a função [Apagar autorização](#).

5.6.23 Cancelar atribuição

Cancele a atribuição se uma pessoa deixar de utilizar um meio.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.

- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio cuja atribuição à pessoa pretenda cancelar.

OU

- > Selecione, na página inicial **Home**, a caixa de seleção **Pessoas**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa de quem pretende cancelar a atribuição a um meio.

À esquerda, por baixo do nome da pessoa, estão listados todos os meios que lhe foram atribuídos.

Selecione o meio cuja atribuição pretende cancelar.

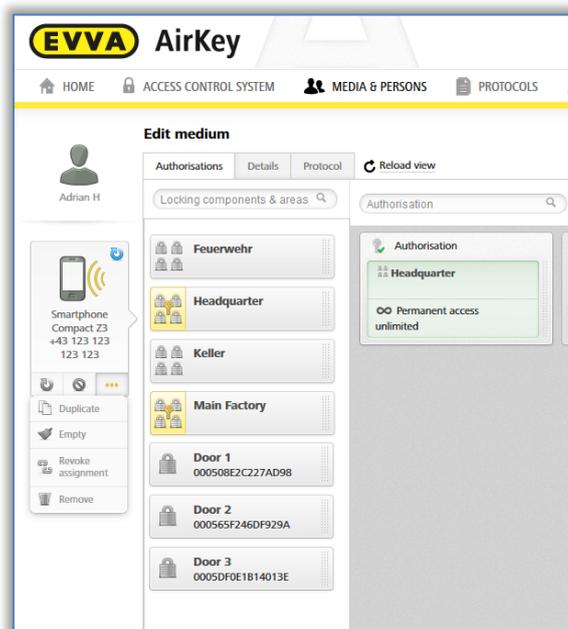


Figura 194: Meios atribuídos

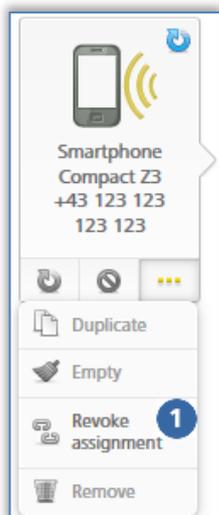


Figura 195: Meio – Cancelar atribuição

- > Clique em **Mais...** ① → **Cancelar atribuição**, se já não encontrar no meio nenhuma autorização.
- > Confirme a pergunta de segurança com **Cancelar atribuição**.

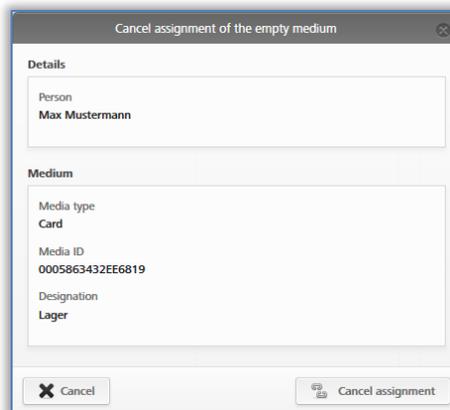


Figura 196: Cancelar atribuição sem autorizações

O cancelamento bem-sucedido de uma atribuição é concluído com uma mensagem de confirmação. O ecrã muda automaticamente para os detalhes da pessoa em questão.



No caso de smartphones, a autorização especial "autorização de manutenção" tem de ser desativada para se poder cancelar a atribuição.

Se se encontrarem autorizações no meio, estas têm de ser eliminadas em primeiro lugar. A função **Meio vazio** pode também ser utilizada para a função **Cancelar atribuição** para esvaziar todas as autorizações do meio.

Contanto que ainda se encontrem autorizações no meio, é exibida na execução da função **Cancelar atribuição** uma caixa de diálogo alternativa. Neste diálogo, pode-se seleccionar entre esvaziar o meio ou transferir o meio para uma outra pessoa.

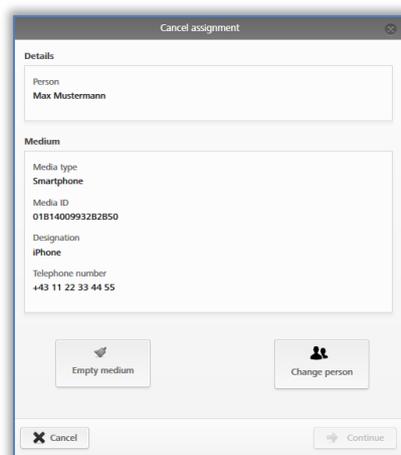


Figura 197: Cancelar atribuição com autorizações

Contanto que a função **Meio vazio** seja utilizada com a função **Cancelar atribuição**, após a atualização do meio, para concluir com sucesso o processo de eliminação das autorizações, a função **Cancelar atribuição** tem de ser novamente executada.

Caso o meio, incluindo as autorizações, deva ser transferido a outra pessoa, tem de se realizar os passos seguintes:

- > Clique em **Mais...** → Cancelar atribuição.
- > Selecione **Alterar pessoa** e confirme com **Continuar**.

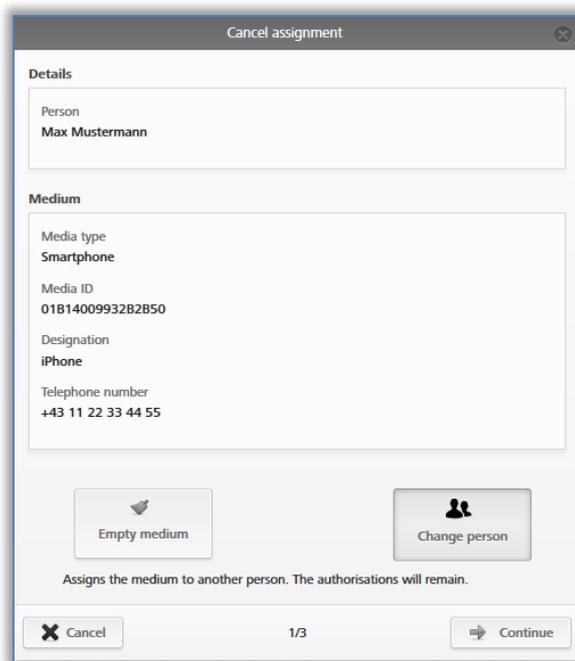


Figura 198: Cancelar atribuição – Mudar pessoa

Obtém uma lista de todas as pessoas criadas. Selecione a pessoa desejada e confirme com **Continuar**.

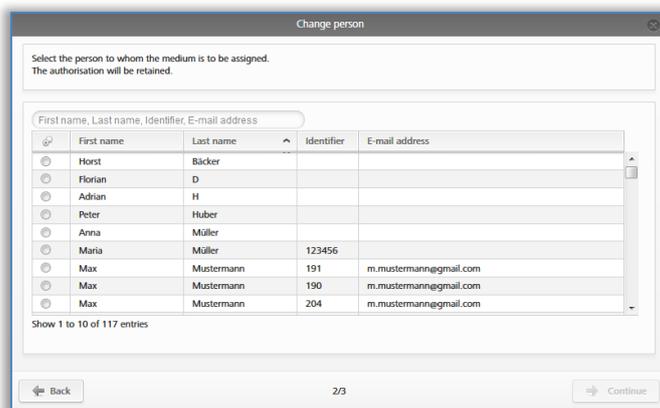


Figura 199: Mudar pessoa

Confirme a pergunta de segurança com **Alterar pessoa** para concluir o processo com sucesso.



Figura 200: Mudar pessoa

A execução bem-sucedida é concluída com uma mensagem de confirmação.

5.6.24 Remover meio

Remova um meio quando este deixar de ser visualizado ou de ser utilizado no seu sistema de controlo de acessos.



Só se pode remover um meio se a atribuição à pessoa tiver sido cancelada. Poderá obter mais informações a respeito do cancelamento da atribuição em [Cancelar atribuição](#).

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio que pretende remover.
- > Clique, por baixo do símbolo do meio, no símbolo do caixote do lixo 1.
- > Confirme a pergunta de segurança **Remover meio** 1.

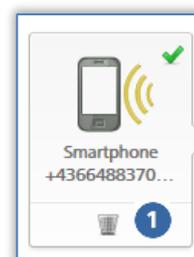


Figura 201: Remover meio - Caixote do lixo

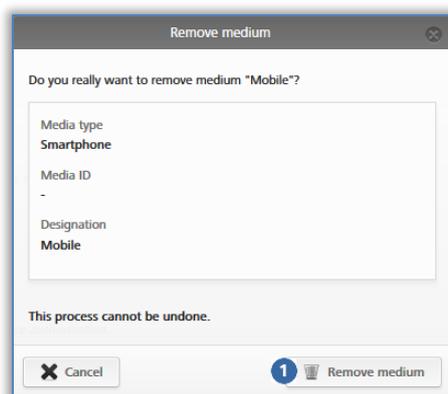


Figura 202: Remover meio

Quando o meio tiver sido finalmente removido, este deixará de aparecer na lista geral dos meios. O ecrã muda para a lista dos meios.



Depois de remover o meio do sistema de controlo de acessos, este volta ao estado de fábrica e pode ser novamente adicionado a outro sistema de controlo de acessos AirKey.

Option

Remova um meio sem autorizações e sem referência pessoal através da estação de codificação, colocando o meio sobre a estação de codificação e clicando, na notificação do estado, no link **Remover o meio do sistema**.

5.7 Protocolos

No menu principal **Protocolos** obtém uma visão global central de todos os eventos do seu sistema de controlo de acessos AirKey. Dependendo das configurações gerais relativas ao registo em protocolo e à manutenção ou referência pessoal nos registos protocolares, a par dos acessos concedidos e dos eventos técnicos, também os acessos recusados (se o respetivo meio tinha uma autorização para o componente de bloqueio AirKey, embora geralmente existente, não válida no momento de bloquear) são registados em protocolo. Todos os eventos registados para a Administração online do AirKey ficam aí guardados ilimitadamente.



Recarregue a vista dos protocolos de tempos a tempos para obter os registos mais atuais no protocolo. Para esse fim, está disponível o link **Recarregar vista**.

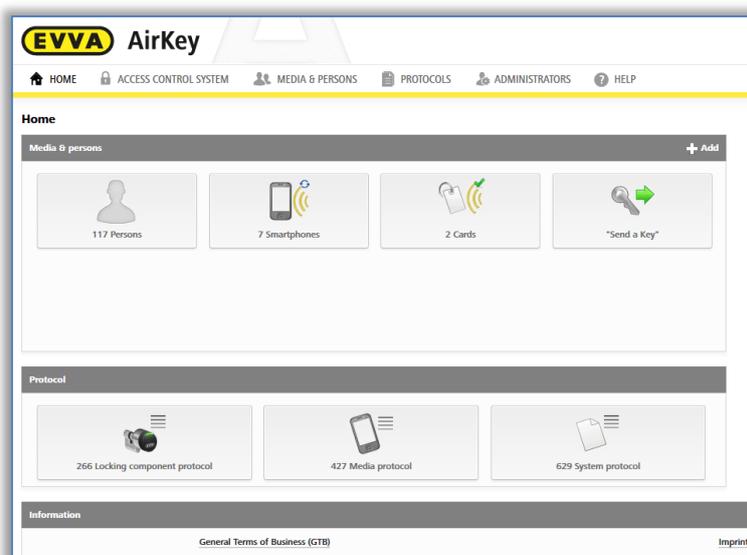


Figura 203: Protocolos



Informa-se expressamente que o presente sistema AirKey pode estar sujeito ao dever de notificação / aprovação de acordo com determinações legais, em especial a lei de proteção de dados. Na sequência disto, a EVVA Sicherheitstechnologie GmbH não assume qualquer responsabilidade nem compromisso por um funcionamento sujeito à conformidade com a lei.



Ative o **princípio dos quatro olhos para a visualização dos protocolos** para garantir uma proteção ainda maior dos dados pessoais. Para a visualização do protocolo de componentes de bloqueio e meios, é necessário obter a confirmação de um segundo administrador do sistema. Poderá encontrar detalhes para a ativação no capítulo [Informações gerais](#).

5.7.1 Protocolo de componentes de bloqueio

Se o **princípio dos quatro olhos para a visualização dos protocolos** não estiver ativo, execute os seguintes passos para visualizar o protocolo dos componentes de bloqueio:

- > Selecione, na página inicial **Home**, a caixa de seleção **Protocolo de componentes de bloqueio**.
- > Em alternativa, selecione, no menu principal, **Protocolos** → **Componentes de bloqueio e áreas**.

Se o **princípio dos quatro olhos para a visualização dos protocolos** estiver ativo, execute os seguintes passos adicionais para visualizar o protocolo dos componentes de bloqueio:

- > Selecione um segundo administrador do sistema da lista, a quem deve ser enviado um código de confirmação por e-mail, e clique em **Enviar código de confirmação**.

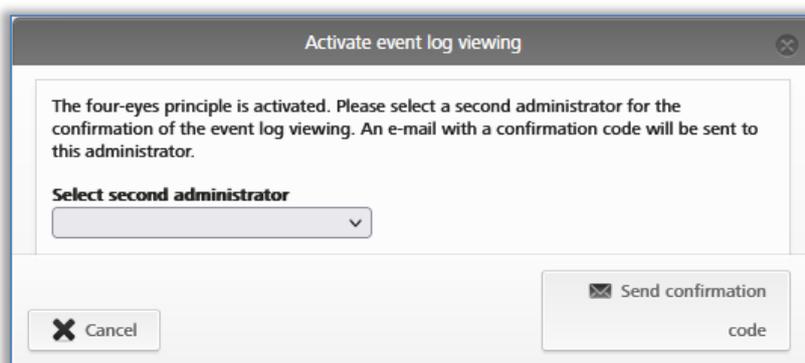


Figura 204: Ativação da visualização dos protocolos – seleção do segundo administrador

- > Em seguida, é enviado um e-mail com um código de confirmação ao administrador do sistema selecionado.
- > Este código de confirmação tem de ser introduzido na administração online do AirKey dentro de 10 minutos e confirmado com o botão **Ativar**.

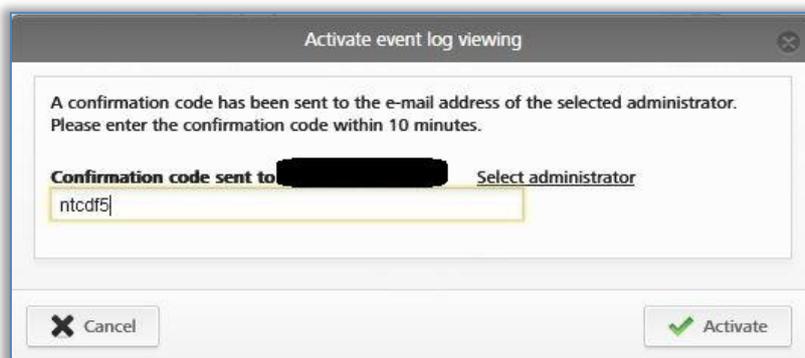


Figura 205: Ativação da visualização dos protocolos – introdução do código de confirmação

Se o procedimento não for concluído dentro de 10 minutos, é necessário repetir o procedimento. Se o administrador do sistema selecionado não reagir, pode selecionar um outro administrador do sistema pelo link **Selecionar administrador** para ativar a visualização do protocolo.

Em seguida, é exibido o protocolo dos componentes de bloqueio.



A ativação da visualização dos protocolos está ativa até ao próximo logout do administrador do sistema. Isto significa que tanto o protocolo dos componentes de bloqueio como o protocolo dos meios podem ser visualizado as vezes que quiser.

A lista visualizada inclui registos relativos aos componentes de bloqueio e áreas.

- > Se necessário, selecione a partir da coluna esquerda cada componente de bloqueio e/ou área para os quais pretende consultar o protocolo. Se pretender consultar novamente todos os componentes de bloqueio e áreas, clique em baixo, à esquerda, em **Todos as entradas** 1.
- > Insira, para a pesquisa orientada de registos, pelo menos, 3 caracteres no campo de pesquisa 2.
- > Adicionalmente, poderá ativar o filtro 3, clicando no link pretendido (p. ex., "Não autorizado"). Aí, só são listados os registos cujo acesso foi recusado.
- > Normalmente, a lista é ordenada por data e hora 4 (registos novos em cima). Ao clicar, na coluna com o título "Data, Hora", poderá alterar a ordem sequencial. A ordenação por outro título de coluna não é possível nesta tabela.

Figura 206: Protocolo Componentes de bloqueio e áreas

- > Caso a lista deva incluir muitas entradas, poderá utilizar à direita, em baixo, o campo **Ir para** 5, para navegar rapidamente para um determinado dia de calendário.

- > Utilize, à esquerda, em baixo, o botão **Exportar** , se pretender exportar o protocolo por completo para um ficheiro CSV. Esta ação pode ser processada sem depender da Administração online do AirKey.

No protocolo, são listadas todas as informações necessárias como, p. ex., data e hora, designação da porta (informações adicionais), ID dos componentes, pessoa (identificação), ID dos meios (nome) e o evento. Adicionalmente, podem ser visualizadas mais informações a respeito deste evento na coluna "Detalhes".

Na coluna "Fonte" poderá ver se o registo protocolar provém de um meio e/ou de um componente de bloqueio.



Recarregue a vista de tempos a tempos para poder visualizar os registos mais atuais no protocolo. Para esse fim, está disponível o link **Recarregar vista**.

Utilize as definições para o registo em protocolo para limitar a referência pessoal nos registos protocolares de acordo com a proteção de dados. Poderá determinar o tipo de referência pessoal nos registos protocolares de componentes de bloqueio para novos componentes de bloqueio adicionados em Definições dos valores por defeito para registo em protocolo ou por componente de bloqueio nos detalhes do componente de bloqueio.



Apenas através da atualização regular dos componentes de bloqueio se pode assegurar que todos os registos protocolares dos componentes de bloqueio são transferidos para a Administração online do AirKey. Os intervalos de atualização recomendados dependem da frequência dos componentes de bloqueio. Observe os [valores e limites](#) nos componentes de bloqueio AirKey.

Um acesso recusado apenas é registado em protocolo se o meio possuir uma autorização para o componente de bloqueio, que não estava válida no momento do acesso (p. ex., a autorização expirou ou apenas é válida durante um determinado período de tempo).

O estado das pilhas indicado na coluna "Detalhes" é sempre o estado das pilhas do componente de bloqueio AirKey (cilindro) e não o estado da bateria do smartphone.

Se, nos componentes de bloqueio, o registo em protocolo estiver limitado a um determinado período de tempo, o registo em protocolo dos acessos continuará apesar de expirado este prazo. Neste caso, a referência pessoal torna-se anónima.

5.7.2 Protocolo dos meios

Se o **princípio dos quatro olhos para a visualização dos protocolos** não estiver ativado, execute os seguintes passos para visualizar o protocolo dos meios:

- > Selecione, na página inicial **Home**, a caixa de seleção **Protocolo dos meios**.
- > Em alternativa, selecione, no menu principal, **Protocolos** → **Meios**.

Se o **princípio dos quatro olhos para a visualização dos protocolos** estiver ativado, execute adicionalmente os seguintes passos adicionais para visualizar o protocolo dos meios:

- > Selecione um segundo administrador do sistema da lista, a quem deve ser enviado um código de confirmação por e-mail, e clique em **Enviar código de confirmação**.

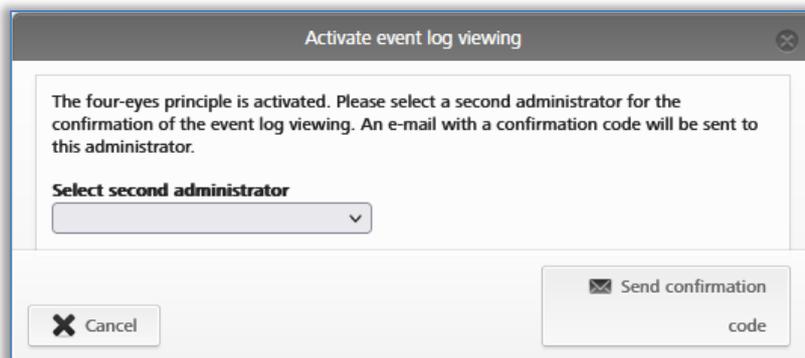


Figura 207: Ativação da visualização dos protocolos – selecção do segundo administrador

- > Em seguida, é enviado um e-mail com um código de confirmação ao administrador do sistema selecionado.
- > Este código de confirmação tem de ser introduzido na administração online do AirKey dentro de 10 minutos e confirmado com o botão **Ativar**.

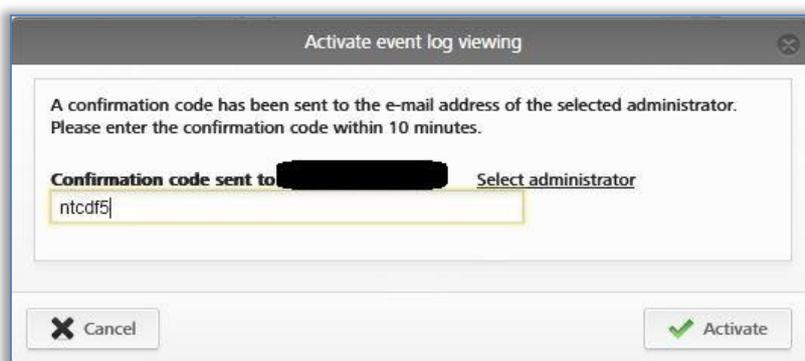


Figura 208: Ativação da visualização dos protocolos – introdução do código de confirmação

Se o procedimento não for concluído dentro de 10 minutos, é necessário repetir o procedimento. Se o administrador do sistema selecionado não reagir, pode seleccionar um outro administrador do sistema pelo link **Selecionar administrador** para ativar a visualização do protocolo.

Em seguida, é apresentado o protocolo dos meios.



A ativação da visualização dos protocolos é válida até ao próximo logout do administrador do sistema. Isto significa que tanto o protocolo dos componentes de bloqueio como o protocolo dos meios podem ser visualizados as vezes que quiser.

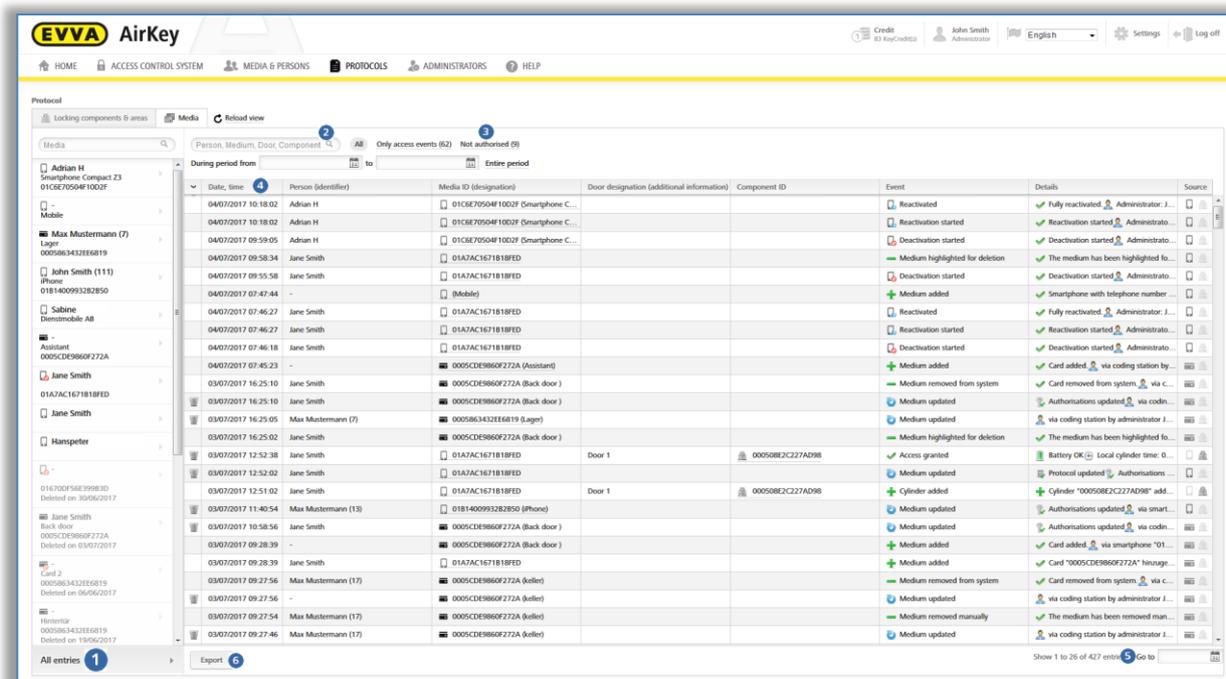


Figura 209: Protocolo dos meios

Obtém uma vista geral de todas os registos dos meios.

- > Se necessário, selecione, na coluna à esquerda, os meios individualmente para os quais pretende consultar o protocolo. Se pretender consultar novamente todos os meios, clique em baixo, à esquerda, em **Todas as entradas** 1.
- > Insira, para a pesquisa orientada de registos, pelo menos, 3 caracteres no campo de pesquisa 2.
- > Utilize o filtro, p. ex., "Não autorizado" 3. Aí, são listados os registos cujo acesso foi recusado.
- > Ordene a lista de acordo com a data e a hora 4.
- > Utilize, do lado direito, em baixo, o campo **Ir para** 5 para navegar rapidamente numa lista grande para um determinado dia.
- > Utilize, à esquerda, em baixo, o botão **Exportar** 6, se pretender exportar o protocolo dos meios por completo para um ficheiro CSV. Esta ação pode ser processada sem depender da Administração online do AirKey.

No protocolo, são listadas todas as informações necessárias como, p. ex., a data e a hora, a pessoa (identificação), a ID do meio (nome), a designação da porta (informação adicional), a ID do componente e o evento. Adicionalmente, podem ser visualizadas informações mais concretas a respeito do evento na coluna "Detalhes".

- > Na coluna "Fonte" poderá ver se o registo protocolar provém de um meio e/ou de um componente de bloqueio.
- > Utilize as definições para o registo em protocolo para limitar a referência pessoal nos registos protocolares de acordo com a proteção de dados. Poderá definir o tipo de referência pessoal nos registos protocolares para componentes de bloqueio para novos componentes de bloqueio adicionados nas [Definições](#) ou, por componente de bloqueio, nos detalhes do componente de bloqueio.

- > Os registos protocolares de um determinado meio podem ser igualmente consultados através do próprio meio. Selecione, para tal, o meio pretendido da lista de meios e mude para o separador **Protocolo**.



Um acesso recusado apenas é registado em protocolo se o meio possuir uma autorização para o componente de bloqueio, que não estava válida no momento do acesso (p. ex., a autorização expirou ou apenas é válida durante um determinado período de tempo).

O estado das pilhas indicado na coluna "Detalhes" é sempre o estado das pilhas do componente de bloqueio AirKey (cilindro) e não o estado da bateria do smartphone.

Se, nos componentes de bloqueio, o registo em protocolo estiver limitado a um determinado período de tempo, o registo em protocolo dos acessos continuará apesar de expirado este prazo. Neste caso, a referência pessoal torna-se anónima.

Para o protocolo de componentes de bloqueio e de meios aplica-se o seguinte: os registos protocolares com referência pessoal, por razões legais de proteção dos dados, podem ser tornados anónimos mesmo posteriormente. Os registos protocolares críticos em termos de proteção de dados como, por exemplo, acessos, têm o símbolo do caixote de lixo na primeira coluna.

Para tornar a referência pessoal anónima nos registos protocolares, proceda da seguinte forma:

- > Procure o registo protocolar a tornar anónimo e clique no símbolo do caixote de lixo na primeira coluna.
- > Primeiro surge uma pergunta para saber se apenas este registo protocolar ou todos os registos devem ser eliminados para esta pessoa. Selecione a opção pretendida.
- > Indique um motivo para a eliminação do registo protocolar.
- > Insira o visto em ***Eu quero apagar irrevogavelmente o registo de entrada/Gostaria de excluir permanentemente as entradas de protocolo.***
- > Para concluir o processo, confirme com **Apagar**.

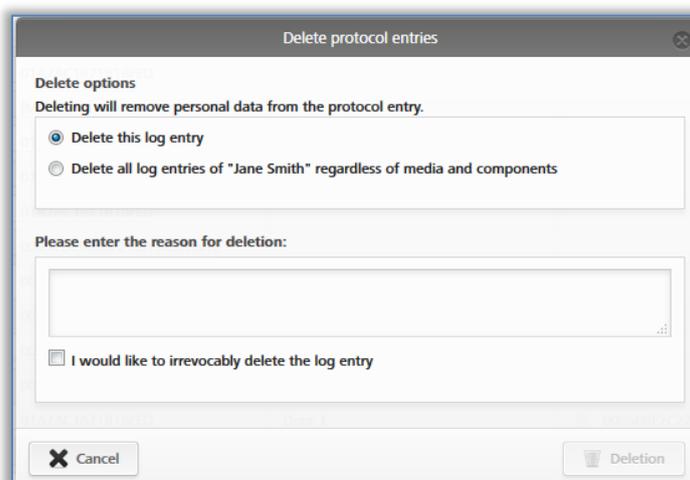


Figura 210: Apagar os registos protocolares



O registo protocolar não é totalmente eliminado, mas somente a referência pessoal. O registo protocolar ficou, assim, anónimo. Esta ação não pode ser revertida. Utilize esta função com prudência.



A eliminação do registo protocolar é listado no protocolo do sistema.

5.7.3 Protocolo do sistema

- > Selecione, na página inicial **Home**, a caixa de seleção **Protocolo do sistema**.
- > Em alternativa, selecione, no menu principal, **Protocolos** → **Sistema**.

Obtém uma vista geral com todas as ações realizadas pelos administradores.

- > No campo de pesquisa **1**, poderá pesquisar por administrador, identificação de utilizador, ação, ID de transação, ID do meio ou ID do componente. Insira um determinado período de tempo **2** e defina a coluna com base na qual se deve ordenar **3**.
- > Insira no campo **Ir para** **4** uma data para poder navegar diretamente para um separador no protocolo do sistema. Caso não haja registos para a data inserida, é selecionado o registo mais próximo.
- > Utilize, à esquerda, em baixo, o botão **Exportar**, se pretender exportar o protocolo do sistema por completo para um ficheiro CSV. Esta ação pode ser processada sem depender da Administração online do AirKey.

Date, time	Administrator (User ID)	Action	Result	Transaction ID
04/07/2017 12:23:34	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245868
04/07/2017 11:13:26	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245791
04/07/2017 10:46:47	John Smith (13968155)	Medium owner changed	Smartphone 018140099328250 (iPhone) +43 11 22 33 44 55 transferred to John Smith.	245770
04/07/2017 10:30:40	John Smith (13968155)	Medium wiped	Smartphone 01C8E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 wiped.	245769
04/07/2017 10:18:02	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01C8E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 reactivated.	245767
04/07/2017 10:18:02	John Smith (13968155)	Reactivation of a medium started	Started reactivation of Smartphone 01C8E70504F10D2F (Smartphone Compact Z3) +43 123 123 123. Reason: Found Additional notes: Cre...	245766
04/07/2017 09:59:05	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01C8E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 started.	245765
04/07/2017 09:58:34	John Smith (13968155)	Medium highlighted for deletion	Smartphone 01A7AC1671818FED was highlighted for deletion.	245764
04/07/2017 09:55:58	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01A7AC1671818FED +43123123456456 started.	245759
04/07/2017 09:23:38	John Smith (13968155)	Deletion has been undone	The authorisation Smartphone 01A7AC1671818FED +43123123456456 for wall reader '000565F246D929A' (Door 2) has been restored.	245752
04/07/2017 07:47:44	John Smith (13968155)	Medium added	Smartphone +43 11 22 33 55 44 66 (Mobile) added.	245690
04/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01A7AC1671818FED +43123123456456 reactivated.	245689
04/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium started	Started reactivation of Smartphone 01A7AC1671818FED +43123123456456. Reason: Found Additional notes: Credit: 84 KeyCredits	245688
04/07/2017 07:46:18	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01A7AC1671818FED +43123123456456 started.	245687
04/07/2017 07:46:00	John Smith (13968155)	Medium wiped	Smartphone 01A7AC1671818FED +43123123456456 wiped.	245686

Figura 211: Protocolo do sistema



No protocolo do sistema, não pode ser eliminado nenhum registo protocolar.



O princípio dos quatro olhos para a visualização dos protocolos não se aplica ao protocolo do sistema. Isto significa que os administradores do sistema podem visualizar sempre o protocolo do sistema.

5.8 Ativações de apoio

Ao criar uma ativação de apoio, poderá criar um administrador no momento em que precisar de ajuda pontual com o AirKey. Através da ativação de apoio, todos os dados do sistema de controlo de acessos podem ser consultados.



O recetor da ativação de apoio, durante o tempo de ativação, tem os mesmos direitos que os seus como administrador.

5.8.1 Criar ativação de apoio

- > No menu principal, seleccione **Administradores** → **Login de apoio**.

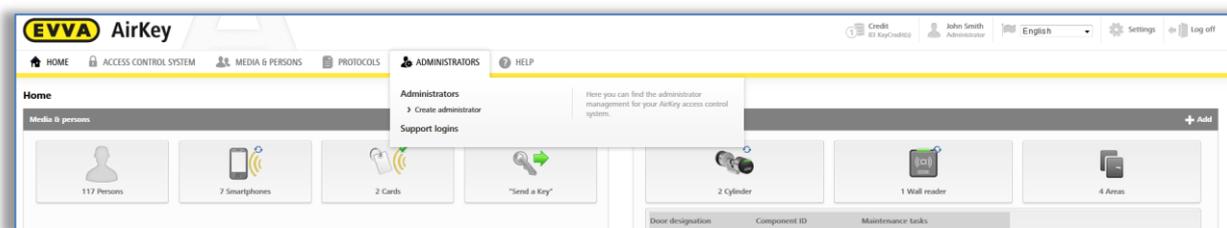


Figura 212: Ativações de apoio

Se já emitiu ativações de apoio, estas serão exibidas numa lista.

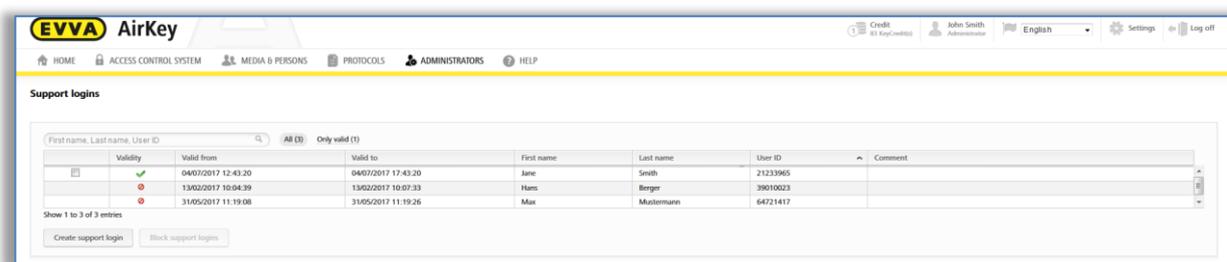


Figura 213: Lista de ativações de apoio

- > Clique em **Criar login de apoio**.
- > Preencha o formulário ❶.
Os campos assinalados com * são de preenchimento obrigatório.



A duração da ativação varia entre 1 a 24 horas.

- > Clique em **Guardar**.

A ativação de apoio foi criada e é emitida uma identificação de utilizador com senha ❷.

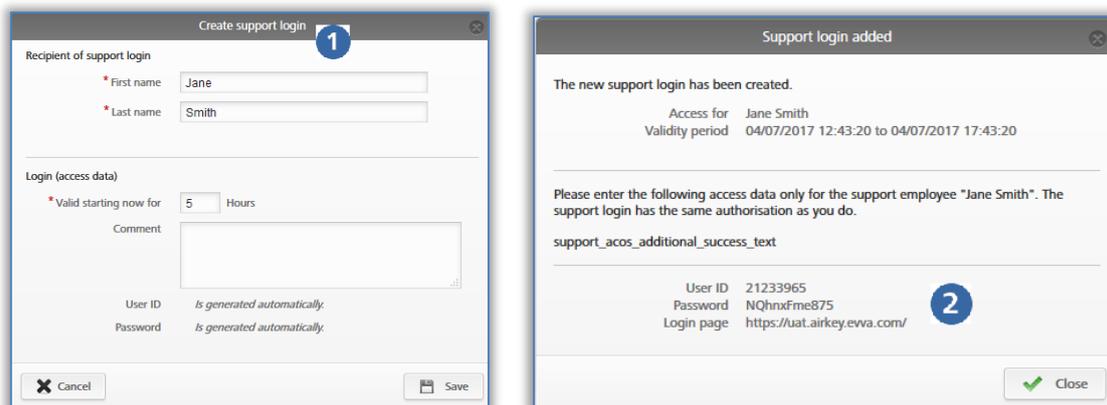


Figura 214: Criar ativação de apoio



Depois de fechar a janela de diálogo, a senha deixa de ser indicada.

É do seu próprio interesse transmitir os dados de login de forma segura.

- > **Feche** a janela de diálogo "Ativação de apoio criada" quando os dados tiverem sido transmitidos ao parceiro de apoio.

5.8.2 Bloquear login de apoio

A ativação de apoio termina automaticamente depois de decorrido o prazo definido. Mas pode ser cancelada antecipadamente através da função **Bloquear login de apoio**.

Se pretender cancelar a ativação de apoio antecipadamente, proceda da seguinte forma:

- > No menu principal, seleccione **Administradores** → **Login de apoio**.

Na lista das ativações de apoio poderá ver se existe atualmente uma ativação de apoio válida ❶ e o tempo de duração da mesma ❷.

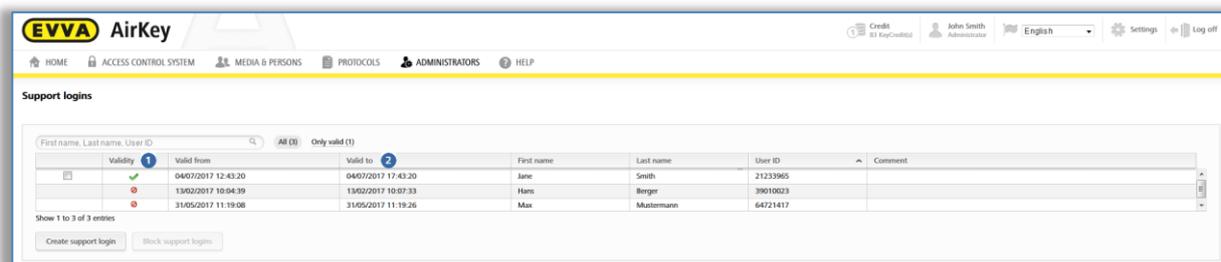


Figura 215: Vista geral das ativações de apoio

- > Seleccione o recetor da ativação de apoio para o qual pretende finalizar a ativação.
- > Clique em **Bloquear login de apoio**.
- > Confirme a pergunta de segurança com **Bloquear login de apoio**.

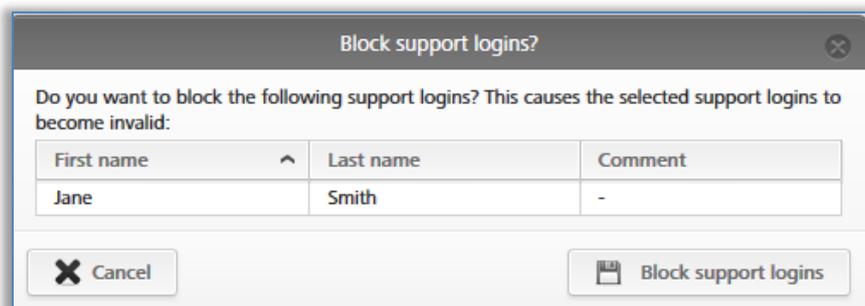


Figura 216: Bloquear ativação de apoio

Na lista de ativações de apoio, poderá reconhecer que a ativação está bloqueada no símbolo na coluna "Válidez" ❶.

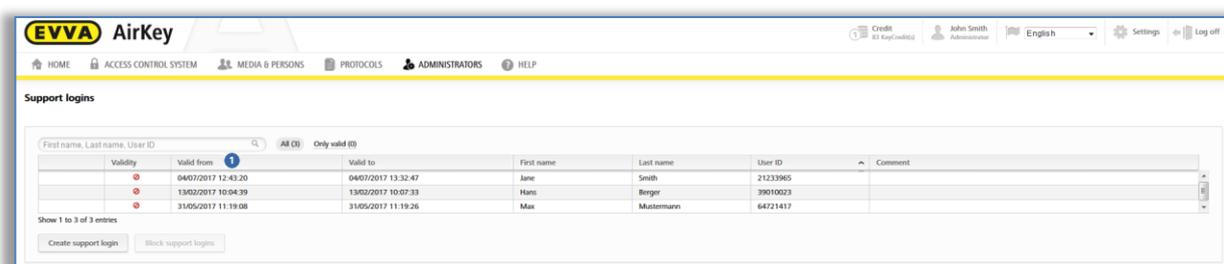


Figura 217: Validade das ativações de apoio



Tanto as atividades realizadas do recetor da ativação de apoio como a criação e o bloqueio da ativação de apoio são registadas nos respetivos protocolos.

5.9 Ajuda

Poderá encontrar mais esclarecimentos no menu principal em **Ajuda** e na página Web do produto AirKey da EVVA em <https://www.evva.com/pt/airkey/website/>. Caso precise de mais apoio, dirija-se ao seu vendedor de produtos EVVA.

6 Aplicação AirKey

Este capítulo dá-lhe uma visão global das funções que pode executar com o seu smartphone na aplicação AirKey.

Se pretender utilizar um smartphone para o AirKey, tem de preencher os seguintes pré-requisitos:

- > O smartphone tem de corresponder aos [Pré-requisitos do sistema](#) para o AirKey.
- > A aplicação AirKey deve ter sido instalada no smartphone com sucesso.
- > Deve estar disponível uma ligação ativa à Internet.
- >



Através da utilização de "otimizações da app", p. ex., para poupar a bateria, a funcionalidade da aplicação pode ser afetada. Os possíveis efeitos são: o processo de desbloqueio dura mais, o bloqueio em segundo plano não funciona de forma estável etc.

6.1 Componentes Bluetooth

Neste ponto do menu, acede a uma lista geral que mostra todos os componentes de bloqueio ao alcance por Bluetooth. Através desta página, pode-se [Conectar componentes](#), desbloquear componentes com Bluetooth ou conectar-se através do símbolo à direita, em cima, com componentes NFC.



A designação dos componentes com Bluetooth só poderá ser corretamente visualizada após atualização do smartphone, ou seja, a visualização da designação de um componente de bloqueio na aplicação AirKey não termina automaticamente, se esta for ajustada na Administração online do AirKey.

A partir do Android 6, a Google especificou que, para reconhecer os componentes de Bluetooth, a autorização para a determinação da localização deve ser concedida no smartphone.

6.2 [Registar smartphone](#): ver o capítulo 4.9

6.3 Autorizações

Se o seu smartphone estiver registado no sistema AirKey e já tiverem sido criadas e emitidas autorizações através da Administração online do AirKey, terá sempre acesso às autorizações do smartphone.

- > Inicie a aplicação AirKey.
- > Selecione no menu **Autorizações**.

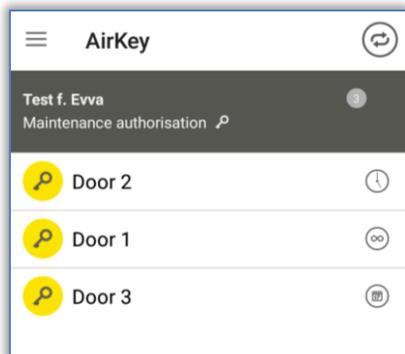


Figura 218: Aplicação AirKey – Vista geral das autorizações

- > Toque numa das autorizações para obter os detalhes da autorização. O dados de localização (coordenadas de GPS ou endereço) são aqui fornecidos como link. Se clicar no link, é automaticamente feito o encaminhamento para o fornecedor de cartões, que estará configurado por defeito no seu smartphone.
- > Nos detalhes da autorização, poderá ativar também individualmente para cada autorização o modo Hands-free (mãos-livres). O requisito para tal é que o administrador tenha autorizado o modo Hands-free (mãos-livres) no componente de bloqueio, que não tenha definido nenhum PIN para a aplicação AirKey e que tenha sido ativado o modo Hands-free (mãos-livres) nas definições da aplicação.

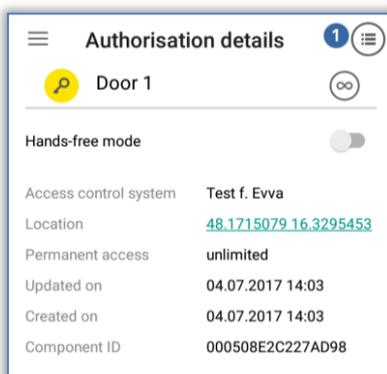


Figura 219: Aplicação AirKey – Detalhes da autorização

Se a autorização para o acesso tiver expirado, isso também será exibido.

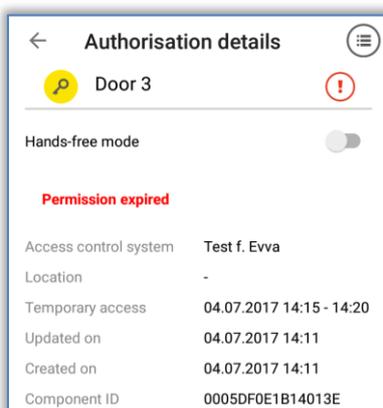


Figura 220: Autorização expirada



Se o seu smartphone tiver autorização para mostrar dados protocolares (ver [Dados protocolares na aplicação AirKey](#)), o protocolo da chave da autorização pode ser exibido nos detalhes da autorização .

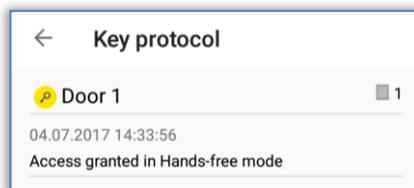


Figura 221: Dados protocolares de uma autorização

6.4 [Tarefas de manutenção](#): ver o capítulo 6.12

6.5 Abertura permanente

A abertura permanente tem a condição de a abertura permanente manual para o componente de bloqueio AirKey estar ativada na Administração online do AirKey (ver [Editar componente de bloqueio](#)), assim como para os componentes de bloqueio com NFC e com Bluetooth.

- > Selecione no menu da aplicação AirKey **Abertura permanente**.
- > Selecione da lista visualizada um componente de bloqueio com Bluetooth ou encoste o smartphone a um componente de bloqueio com NFC.
- > O componente de bloqueio sinaliza opticamente e acusticamente um bloqueio.
- > Recebe uma mensagem de confirmação .

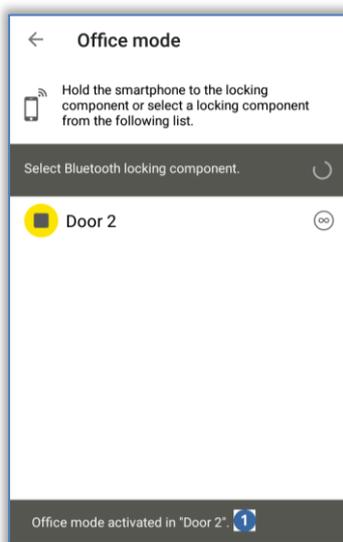


Figura 222: Mensagem de confirmação da abertura permanente



A ativação da abertura permanente em componentes de bloqueio e meios aumenta o consumo de energia dos componentes. Ative a abertura permanente apenas naqueles componentes de bloqueio e meios que utilizam efetivamente esta função.

6.6 Introduzir PIN

Poderá armazenar em cache um PIN ativo durante um certo tempo na aplicação AirKey através da função **Introduzir PIN**.

- > Abra o menu na aplicação AirKey e toque em **Introduzir PIN**.
- > Introduza o PIN correto e toque em **OK**.

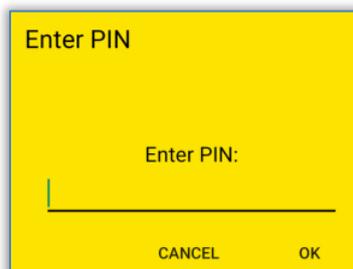


Figura 223: Aplicação AirKey – Introduzir PIN



O PIN é guardado em cache até a aplicação AirKey fechar, passar para segundo plano ou até que o bloqueio do ecrã fique ativo. Desta forma, poderá bloquear componentes de bloqueio sem ter de introduzir novamente o PIN.

O PIN também será armazenado em cache se for solicitado no primeiro desbloqueio de um componente de bloqueio. No desbloqueio seguinte de um componente de bloqueio (o mesmo ou outro) o PIN já não será solicitado. Isto mantém-se assim até a aplicação AirKey fechar, passar para segundo plano ou até que o bloqueio do ecrã fique ativo.

6.7 Codificar meios

Esta função da aplicação AirKey possibilita-lhe atualizar meios de acesso (exceto smartphones) através dos componentes de bloqueio com Bluetooth (cilindros, leitores de parede).

- > Selecione no menu do AirKey **Codificar meios**.
- > Da lista apresentada com os componentes de bloqueio com Bluetooth, selecione aquele através do qual pretende atualizar o meio.

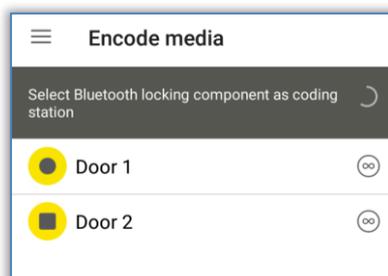


Figura 224: Codificar meios – Lista de seleção dos componentes de bloqueio com Bluetooth

- > Encoste o meio que pretende atualizar ao componente de bloqueio AirKey.

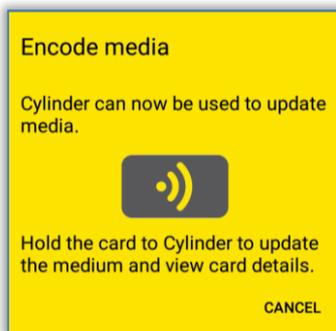


Figura 225: Codificar meios

- > Siga agora as instruções [Adicionar cartões, porta-chaves ou chaves combinadas com o smartphone](#).



Para a função "Codificar meios", o processo tem de iniciar no cilindro com a mão e não com um meio (cartão, porta-chaves, pulseiras ou chave combinada). Caso contrário, dar-se-ia uma bloqueio normal em vez de uma comunicação com o smartphone.

No caso dos componentes de bloqueio com funcionamento a pilhas, o processo de atualização do meio requer energia e encurta a duração das pilhas. Se forem atualizados muito meios, recomenda-se, portanto, o uso de uma estação de codificação AirKey, um smartphone com funcionalidade NFC ou um leitor de parede.

O modo Hands-free no smartphone tem de ser desativado para se poder executar a função "Codificar meios".

6.8 Protocolo de autorização

Selecione, no menu principal da aplicação AirKey, o ponto **Protocolo de autorização** e obtém um protocolo com as alterações das autorizações que foram realizadas pelo administrador do sistema de controlo de acessos AirKey para o seu smartphone.

Este registo em protocolo é sempre executado independentemente das diversas configurações na Administração online do AirKey e na aplicação AirKey.

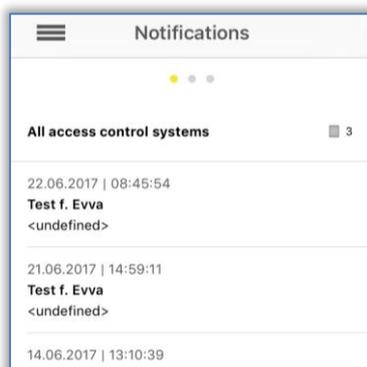


Figura 226: Protocolo de autorizações

6.9 Definições da aplicação AirKey

6.9.1 Definições da aplicação AirKey em smartphones Android

No ponto do menu **Definições** da aplicação AirKey, poderá visualizar informações básicas sobre o seu smartphone Android. Aqui, poderá ver, p. ex., se as funções NFC e Bluetooth estão ativadas. Toque numa das duas entradas, aceda às definições do seu dispositivo smartphone. A seguir, poderá decidir se deverá utilizar o Bluetooth para o AirKey. Ative simplesmente a respetiva opção "Utilizar Bluetooth" ⓘ.

Neste caso, podem ser utilizadas as definições em baixo ("Definir o alcance do modo hands-free", "Modo hands-free" e "Desbloquear a partir de notificações"). A página inicial ao abrir a aplicação AirKey é, neste caso, "Componentes com Bluetooth".

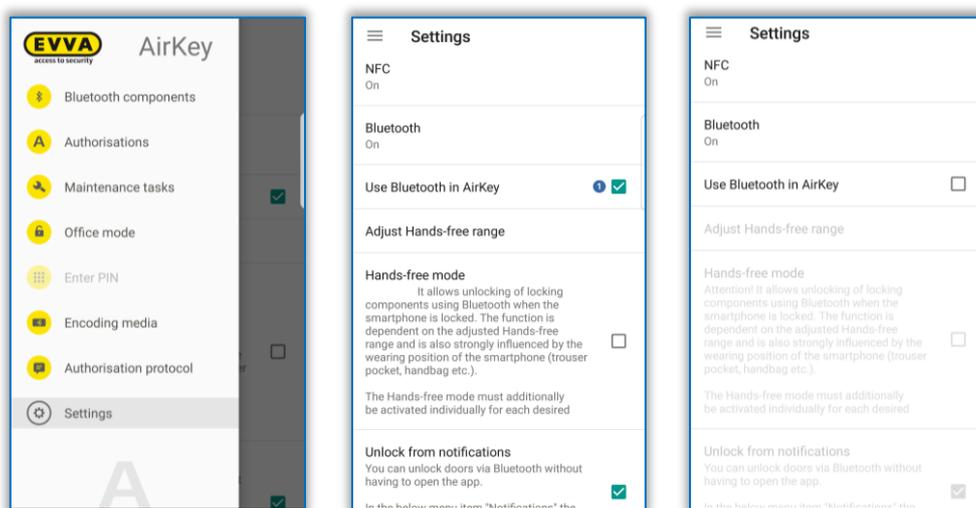


Figura 227: Smartphone Android com Bluetooth – Menu principal / Opção "Utilizar Bluetooth" ativada / Opção Bluetooth desativada

Quando desativa a opção "Utilizar Bluetooth", as três configurações seguintes mencionadas são automaticamente desativadas e todas as funções dependentes do Bluetooth são do menu principal ("Componentes com Bluetooth", "Abertura permanente" e "Codificar meios") mostram a indicação "Bluetooth está desativado". O smartphone, nesta situação, pode comunicar com os componentes de bloqueio somente através de NFC.



Se o smartphone Android for mais antigo e dispuser de uma funcionalidade NFC, mas não Bluetooth, todas as configurações e funções dependentes de Bluetooth são dispensadas.

6.9.2 Definições da aplicação AirKey em iPhones

No ponto do menu **Definições** da aplicação AirKey, poderá visualizar informações básicas sobre o seu iPhone. Aqui, poderá ver, p. ex., se a função Bluetooth está ativada. Neste caso, podem ser utilizadas as definições em baixo ("Definir o alcance do modo hands-free", "Modo hands-free" e "Desbloquear a partir de notificações").

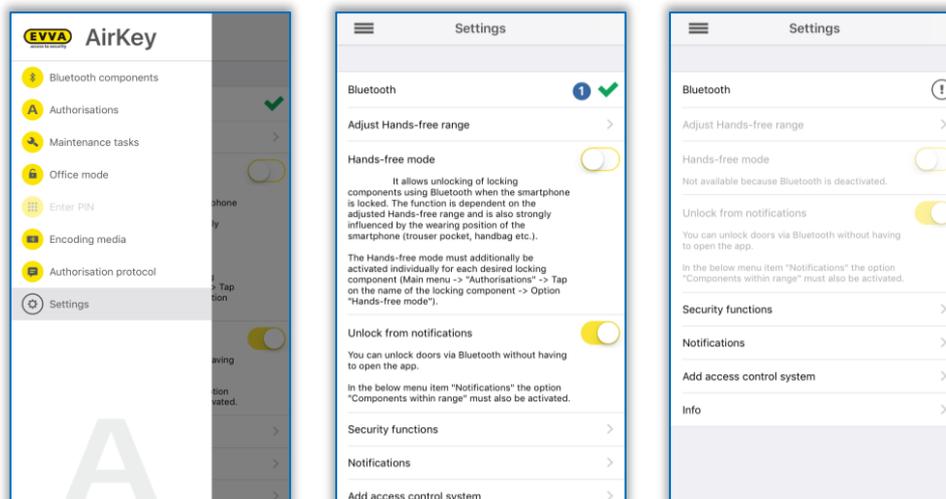


Figura 228: iPhone (só com Bluetooth) – Menu principal / Definições sem funções NFC / Opção Bluetooth desativada

A entrada "Bluetooth" nas definições do AirKey só mostra se a funcionalidade Bluetooth está ativa ou não. Poderá, no entanto, tocar na entrada "Bluetooth" para aceder à configuração de Bluetooth nas definições do seu dispositivo iPhone.



Se desativar o Bluetooth nas definições do dispositivo iPhone, já não poderá bloquear NENHUM componente de bloqueio!

A funcionalidade Bluetooth desativada é respetivamente indicada nas definições do AirKey e as três definições seguintes que lhe dizem respeito são automaticamente desativadas, tal como todas as outras funções do menu principal dependentes do Bluetooth ("Componentes com Bluetooth", "Abertura permanente" e "Codificar meios").

6.9.3 Definir o alcance do modo hands-free

Ao selecionar a função "Definir o alcance do modo Hands-free", tem acesso a um submenu. Aqui, seleciona para que tipo de componente de bloqueio deve ser definido o alcance ou se pretende repor os alcances (para todos os componentes de bloqueio).

Alcance para cilindros

- No caso do cilindro, a aplicação AirKey mostra-lhe todos os cilindros com Bluetooth ativos e que se encontram dentro do alcance, depois de estes terem sido estimulados por contacto manual.
- Seleccione o respetivo cilindro e afaste-se deste tanto quanto quiser para que possa funcionar o reconhecimento automático do smartphone.
- Prima **Guardar**.

Alcance para leitores de parede

- No caso do leitor de parede, a aplicação AirKey mostra-lhe os leitores de parede com Bluetooth que estão dentro do alcance.

- > Selecione o respetivo leitor de parede e afaste-se deste tanto quanto quiser para que possa funcionar o reconhecimento automático do smartphone.
- > Prima **Guardar**.



Aqui, é exibida a força do sinal no ecrã. Tenha em atenção que isto depende das condições ambientais como, p. ex., tráfego nas radiocomunicações etc., e pode variar de acordo com o smartphone utilizado.



O alcance normal é de aprox. 50-70 cm, mas depende do fabricante e do dispositivo. Por razões de segurança, a EVVA recomenda definir o alcance para aprox. 30 cm.

Repor todos os alcances de Bluetooth

Ao tocar em **Repor todos os alcances de Bluetooth**, todos os alcances definidos manualmente são eliminados e são reutilizados os alcances definidos por defeito. Uma mensagem indicativa confirma a reposição dos alcances.

6.9.4 Modo Hands-free (mãos livres)

Coloque um visto em **Modo Hands-free (mãos livres)** para ativar a função. Poderá encontrar todas as informações adicionais em [Vista geral da função hands-free \(mãos livres\)](#).

6.9.5 Desbloqueios a partir de notificações

Nesta função, é possível bloquear componentes de bloqueio AirKey com Bluetooth sem ter de abrir a aplicação AirKey.

Coloque um visto em **Desbloquear a partir de notificações** para ativar a função.



Em smartphones Android, através da ativação desta função, é iniciado um serviço. Este serviço procura continuamente, mesmo com a aplicação AirKey encerrada, componentes de bloqueio com Bluetooth dentro do alcance e aumenta o consumo da bateria do smartphone. O serviço termina assim que a função for novamente desativada. Caso toque nas notificações do serviço, tem acesso direto às definições da aplicação AirKey.

Se estiver com o seu smartphone dentro do alcance de um componente de bloqueio AirKey, para o qual possui uma autorização de acesso, receberá uma notificação no ecrã de bloqueio ou no ecrã inicial do seu smartphone. Através desta notificação, poderá bloquear o componente de bloqueio.

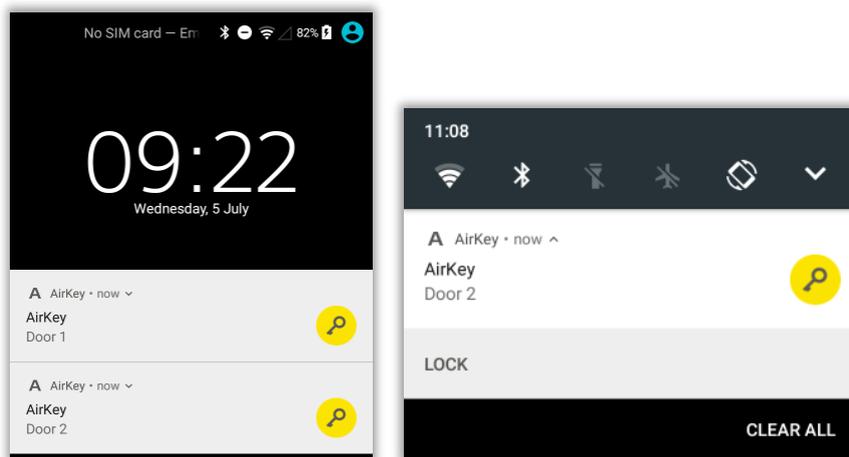


Figura 229: Desbloqueios a partir de notificações – Ecrã de bloqueio

A notificação no ecrã inicial do smartphone aparece sob a forma de **A** ⓘ, que aparece no canto esquerdo superior. Se se arrastar a margem do ecrã superior para baixo, as notificações podem ser visualizadas e pode saber-se que componentes de bloqueio podem ser desbloqueados.

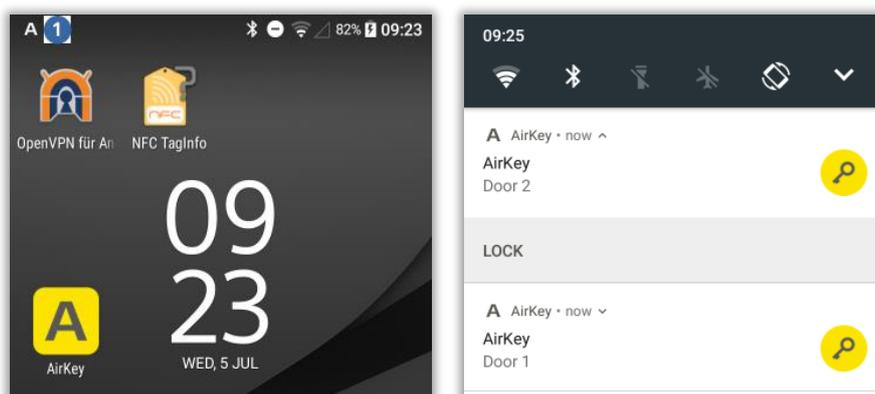


Figura 230: Desbloqueios a partir de notificações



Dependendo do modelo de smartphone, interaja com a notificação expandindo, deslizando ou mantendo pressionada a notificação e tocando, depois, em **Desbloquear**.



Dependendo da configuração **Acesso a partir do ecrã de bloqueio** nas definições da Administração online do AirKey, pode bloquear diretamente a partir do ecrã de bloqueio ou o ecrã de bloqueio tem de ser cancelado previamente. Poderá encontrar mais detalhes em [Informações gerais](#).



O bloqueio a partir de notificações só é possível se as notificações para "Componentes dentro do alcance" estiverem ativadas nas definições da aplicação AirKey. Poderá encontrar a configuração das notificações no capítulo [Notificações](#).

6.9.6 Funções de segurança

No menu **Funções de segurança** poderá encontrar três níveis de segurança:

Encriptação AirKey ①

Aqui, trata-se de um PIN adicional. O PIN consiste entre 4 a 12 dígitos e impede uma utilização indevida no caso de perda ou roubo do smartphone.

A EVVA recomenda a atribuição de um PIN. Utilize um PIN que seja o maior possível e garanta que é a única pessoa que sabe a identificação de utilizador e o PIN!

Bloqueio de ecrã ②

A função de segurança do sistema operativo assegura uma proteção do smartphone contra o desbloqueio do ecrã por parte de terceiros. A seleção desta função permite-lhe navegar diretamente para as definições do smartphone Android.

A EVVA recomenda a ativação de um bloqueio de ecrã que seja apenas do conhecimento do proprietário!

Encriptação de telefone ③

A função de segurança do sistema operativo assegura uma proteção do smartphone contra a leitura de dados por parte de terceiros. A seleção desta função permite-lhe navegar diretamente para as definições do smartphone Android.

A EVVA recomenda a ativação da encriptação do telefone. Observe também as indicações incluídas no manual de utilização do seu smartphone!

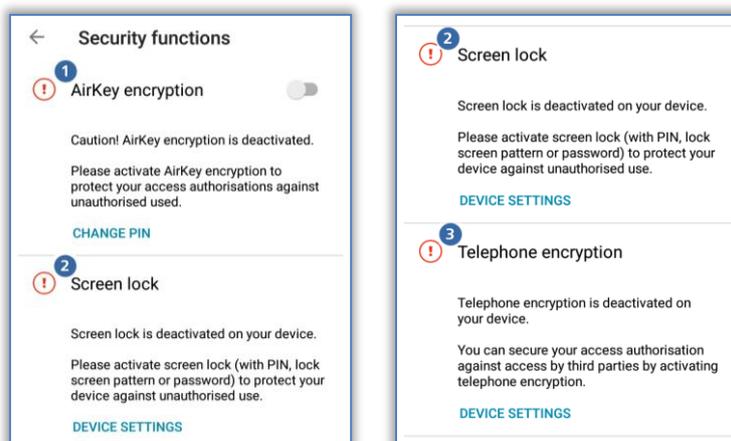


Figura 231: Aplicação AirKey – Funções de segurança

6.9.6.1 Ativar PIN

Para ativar o PIN, siga os seguintes passos:

- > Abra o menu na aplicação AirKey e toque em **Definições** → **Funções de segurança**.
- > Ative a opção "Encriptação AirKey".
- > Atribua um PIN e toque em **Confirmar**.

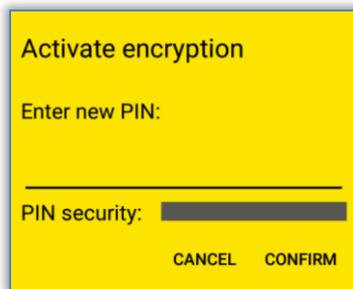


Figura 232: Aplicação AirKey – Ativar PIN

- > Conclua o processo com nova introdução do PIN e validando em **Confirmar**.



A EVVA recomenda a atribuição de um PIN. Utilize um PIN que seja o maior possível e garanta que é a única pessoa que sabe a identificação de utilizador e o PIN. Mesmo durante a introdução do PIN, a força da senha é verificada na barra de sinalização luminosa (**vermelho** / **laranja** / **verde**).



O PIN é pedido no processo de desbloqueio dos componentes de bloqueio. Na aplicação não ocorre qualquer confirmação de que o PIN foi bem introduzido. O PIN pode ser definido previamente e guardado (ver [Introduzir PIN](#)).

6.9.6.2 Alterar PIN

Para alterar posteriormente um PIN definido, proceda aos seguintes passos:

- > Abra o menu na aplicação AirKey e toque em **Definições** → **Funções de segurança**.
- > Toque em **Alterar PIN**.
- > Introduza o PIN anterior, escolha um novo PIN, volte a repetir e toque em **Confirmar**.



Figura 233: Aplicação AirKey – Alterar PIN



Utilize um PIN que seja o maior possível e garanta que é a única pessoa que sabe a identificação de utilizador e o PIN. Mesmo durante a introdução do PIN, a força da senha é verificada na barra de sinalização luminosa (**vermelho** / **laranja** / **verde**).

6.9.6.3 Desativar PIN

Existem duas possibilidades para desativar o PIN. Se ainda souber o PIN, este pode ser diretamente desativado nas funções de segurança do smartphone. Se já não souber o PIN, este pode ser repostado por um administrador da Administração online do AirKey.

Se souber o PIN, proceda ao seguinte:

- > Abra o menu na aplicação AirKey e toque em **Definições** → **Funções de segurança**.
- > Desative a opção "Encriptação AirKey".
- > Introduza o PIN atual e toque em **Confirmar**.

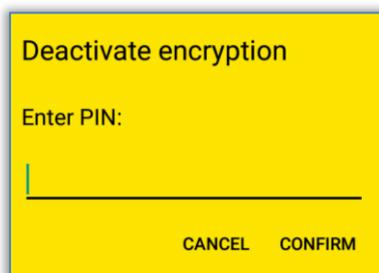


Figura 234: Aplicação AirKey – Desativar PIN

Se já não souber o PIN, o PIN pode ser desativado pela Administração online do AirKey da seguinte forma:

- > Inicie a sessão como administrador no seu sistema de controlo de acessos.
- > Na página inicial **Home**, clique na caixa de seleção **Smartphones**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no smartphone onde o PIN deve ser desativado.
- > Selecione o separador **Detalhes**, para editá-lo.
- > Clique no link **Desativar código PIN** 1 no bloco "Definições".

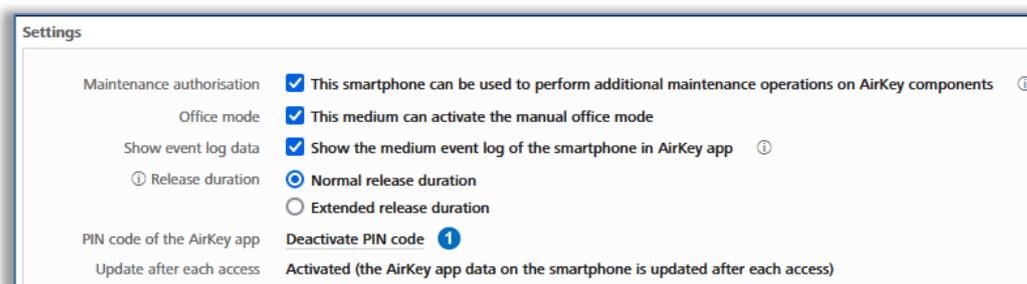


Figura 235: Administração online do AirKey – Desativar código PIN

- > Confirme a pergunta de segurança com o botão **Desativar código PIN**.

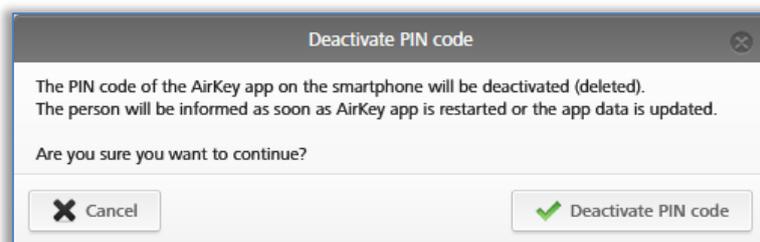


Figura 236: Administração online do AirKey – Desativar código PIN



O PIN pode voltar a ser ativado a qualquer momento.

6.9.7 Notificações

No ponto do menu **Definições** → **Notificações** tem-se a possibilidade de ativar notificações Push (indicações sobre o ecrã de bloqueio ou de iniciação do smartphone) sobre componentes que estão alcance, tarefas de manutenção e autorizações, ou alterações a elas. Quando o smartphone está registado em vários sistemas de bloqueio AirKey e provido da autorização de manutenção, os sistemas de bloqueio também podem ser visualizados e selecionados.

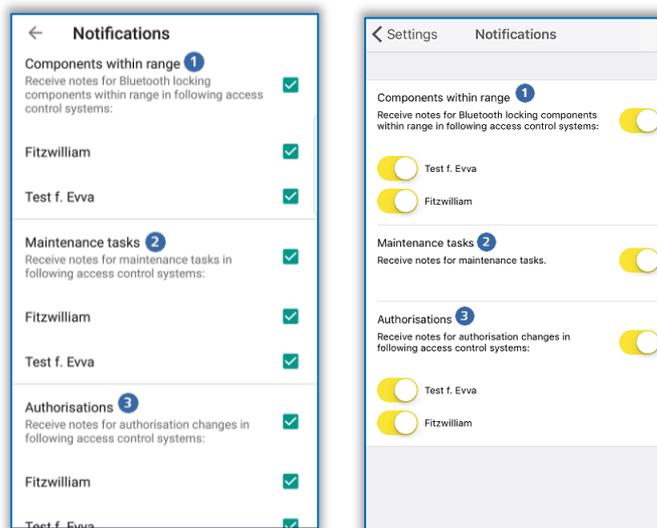


Figura 237: Notificações Push da aplicação AirKey, Definições Android / iPhone

Notificações sobre **componentes no alcance** 1

Se esta definição estiver ativa, receberá as respetivas notificações Push no ecrã de bloqueio ou de iniciação do seu smartphone, desde que o seu smartphone se encontre ao alcance dos componente de bloqueio com Bluetooth. A partir destas notificações, poderá bloquear a respetiva porta sem ter de abrir a aplicação AirKey manualmente (detalhes no capítulo [Desbloqueios a partir de notificações](#)).



Esta definição apenas aparece em smartphones com Bluetooth 4.0 (Bluetooth Low Energy).

Notificações sobre as **tarefas de manutenção** ②

Esta definição apenas pode ser visualizada em smartphones com autorização de manutenção.

Se esta definição estiver ativa, será exibida no menu principal da aplicação AirKey adicionalmente ao ponto do menu **Tarefas de manutenção**. Na respetiva página vêm listados os componentes de bloqueio e as suas [tarefas de manutenção](#), emitidas na Administração online do AirKey.

Se o smartphone estiver registado em vários sistemas de bloqueio, apenas são listados os componentes de bloqueio dos sistemas de bloqueio, para os quais o smartphone possui autorização de manutenção. Assim que uma nova tarefa de manutenção for emitida na Administração online do AirKey, receberá a respetiva notificação Push no seu smartphone.

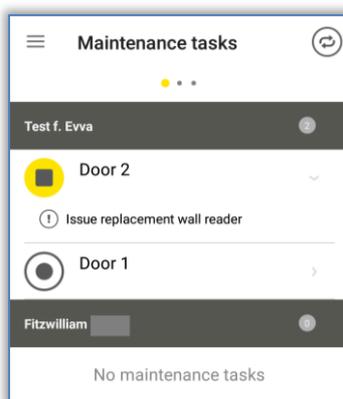


Figura 238: Tarefas de manutenção

Notificações sobre **autorização** ③

Esta definição será sempre indicada.

Se esta definição estiver ativada e uma autorização do seu smartphone for novamente emitida ou alterada na Administração online do AirKey, receberá uma indicação ① durante aprox. 2 seg na margem inferior do ecrã da aplicação AirKey, se esta estiver aberta.

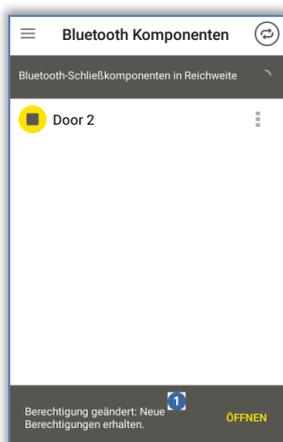


Figura 239: Notificação sobre alteração da autorização

Se a aplicação AirKey não estiver aberta, receberá a respetiva notificação Push no ecrã de bloqueio ou de iniciação do seu smartphone.

Independentemente da definição para as notificações sobre autorizações, obterá uma entrada permanente na página das Protocolo de autorizações.

6.9.8 Adicionar sistema de controlo de acessos

Os smartphones podem estar registados em mais de um sistema de controlo de acessos AirKey. Se o seu smartphone for adicionado a outro sistema de controlo de acessos, poderá, através da função **Adicionar sistema de controlo de acessos**, introduzir o código de registo. Poderá encontrar mais informações a este respeito no capítulo [Utilizar o smartphone em vários sistemas](#).

Adicionalmente, também pode fazer aqui a leitura de um código QR para a troca do smartphone. Poderá encontrar detalhes sobre a troca do smartphone no capítulo [Troca de smartphone](#).

6.9.9 Troca de smartphone

Existe a possibilidade de transferir as autorizações e definições do AirKey de um smartphone para um novo smartphone.

Inicie este processo no comando **Troca de smartphone**. Poderá obter mais informações a este respeito no capítulo [Iniciar a troca como proprietário do smartphone](#).

6.9.10 Info

Na aplicação AirKey, existe a possibilidade de aceder à versão da atual aplicação AirKey instalada, aos detalhes de registo do smartphone, à ID dos meios do smartphone e às condições gerais de licenciamento da EVVA.

- > Inicie a aplicação AirKey.
- > Toque, no menu, em **Definições** → **Info**.



Figura 240: Aplicação AirKey – Info

6.10 Atualizar o smartphone

Para manter os dados do sistema de controlo de acessos AirKey atuais no smartphone, poderá atualizar manualmente o smartphone a qualquer momento através da Administração online do AirKey.

Para tal, no ecrã dum smartphone Android, na página "Autorizações" da aplicação AirKey, arraste de cima para baixo. Aparece o símbolo de atualização (círculo a girar).

Num iPhone, arraste a página "Autorizações" até à margem inferior. Aparece o símbolo de atualização (raios a girar).

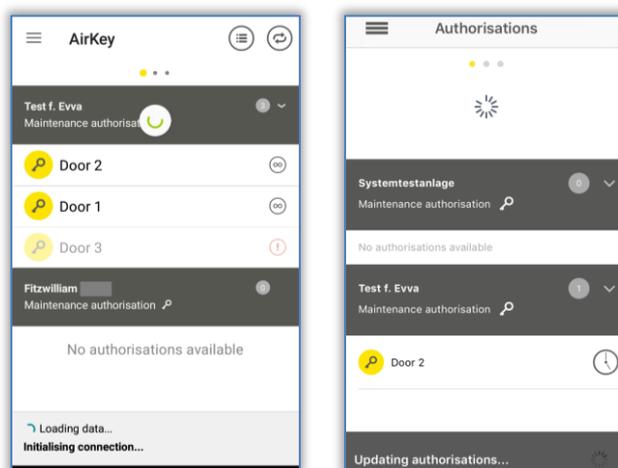


Figura 241: Aualizar o smartphone Android ou o iPhone



O AirKey utiliza, no caso de alterações aos dados de um smartphone, notificações Push para atualizar automaticamente o smartphone. Não é possível dar garantias de envio no caso das notificações Push. Por isso, controle se o envio foi feito e atualize o seu smartphone manualmente, se for o caso.



O smartphone será automaticamente atualizado assim que iniciar a aplicação AirKey, ou, a cada 12 horas o smartphone tenta atualizar automaticamente, caso a aplicação AirKey já tenha sido iniciada.

Na secção inferior da aplicação AirKey, será salientada uma informação do estado para atualização no momento da atualização. Se estas informações deixarem de aparecer, significa que a atualização está concluída.

Opcionalmente, a atualização também pode decorrer após cada processo de acesso. No entanto, para isso, a função "Atualização após cada acesso" tem de estar ativa no respetivo sistema de bloqueio AirKey após cada processo de desbloqueio. A ativação e os detalhes desta função estão descritos no capítulo [Informações gerais](#).

6.11 Conecte com o componente

Poderá atualizar com o seu smartphone cada um dos meios de acesso (exceto smartphones) e cada um dos componentes de bloqueio AirKey, independentemente da sua associação ao seu sistema de controlo de acessos.

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente 1**.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones Android): toque, no caso do componente de bloqueio que pretende conectar, no menu contextual (:) e seleccione, depois, **Conectar 2**.
- > Se estabelecer a ligação por **Bluetooth** (em iPhones): arraste, no caso do componente de bloqueio que pretende conectar, na designação do componente para a esquerda e seleccione, depois, **Conectar 3**.

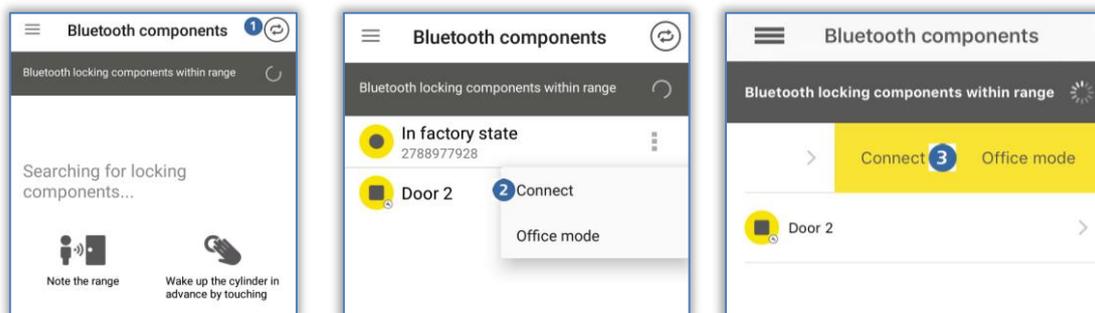


Figura 242: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone)

- > Siga as instruções e encoste o smartphone com NFC ao meio ou ao componente de bloqueio; ou o smartphone com Bluetooth ao alcance ao componente de bloqueio.



Figura 243: Atualizar dados

Os dados estão a ser atualizados. Durante a transferência, o smartphone não pode ser afastado do componente a sincronizar. Depois de o processo estar concluído, receberá a mensagem correspondente.



Desative o modo Hands-free antes de se conectar a um componente de bloqueio com Bluetooth. Caso contrário, poderá provocar interrupções na ligação.



Os componentes de bloqueio com Bluetooth também podem ser atualizados automaticamente após cada processo de desbloqueio via Bluetooth. Poderá encontrar mais informações sobre a função "Atualização após cada desbloqueio" em [Valores por defeito \(para todos os componentes de bloqueio adicionados como novos\)](#).



Atualize os seus componentes AirKey regularmente. Só assim o seu sistema AirKey será seguro e estará o mais atualizado possível. Poderá obter mais informações a respeito da atualização dos componentes AirKey em [Operação e manutenção do sistema AirKey](#).

6.12 Autorização especial "autorização de manutenção"

Se, no seu smartphone, a autorização especial "autorização de manutenção" foi ativada pela Administração online do AirKey, poderá realizar operações de manutenção adicionais em componentes AirKey. A autorização de manutenção autoriza-o a desbloquear componentes de bloqueio AirKey no estado de fábrica, a adicionar e a remover componentes de bloqueio e meios de acesso (exceto smartphones) no seu sistema de controlo de acessos AirKey e a atualizar os firmwares de componentes de bloqueio, ou a versão de meios Keyring como, p. ex., cartões, porta-chaves e chaves combinadas.

Reconhece a autorização de manutenção na aplicação AirKey na página **Autorizações** como registo "Autorização de manutenção"  na barra cinzenta.

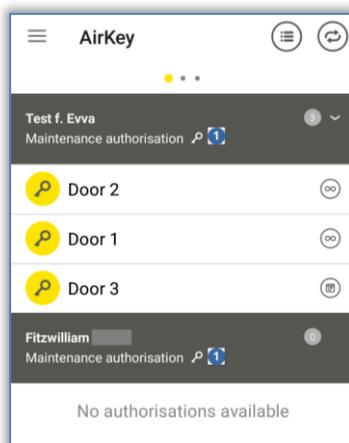


Figura 244: Autorização de construção local

A autorização de manutenção é ativada nos detalhes do respetivo smartphone no âmbito da Administração online do AirKey. Poderá obter mais informações a respeito da edição de um meio em [Editar meio](#).

Adicionalmente, no menu principal da aplicação AirKey, foi também ativado o ponto do menu **Tarefas de manutenção** .

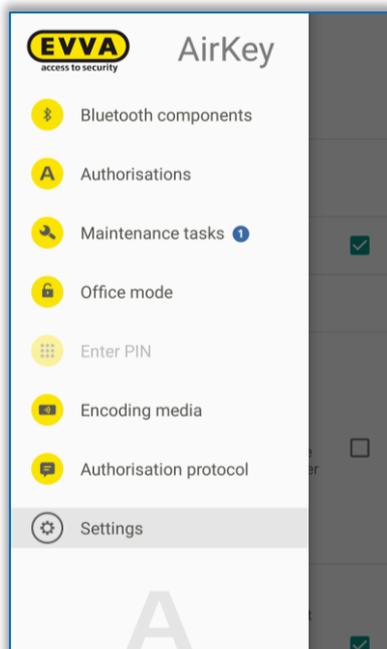


Figura 245: Ponto do menu "Tarefas de manutenção" no menu principal

- > Toque em cima para obter uma lista das tarefas de manutenção para os componentes de bloqueio do seu sistema de controlo de acessos. Se tocar no nome de um componente de bloqueio, visualiza a lista com as tarefas de manutenção em aberto para este componente de bloqueio.

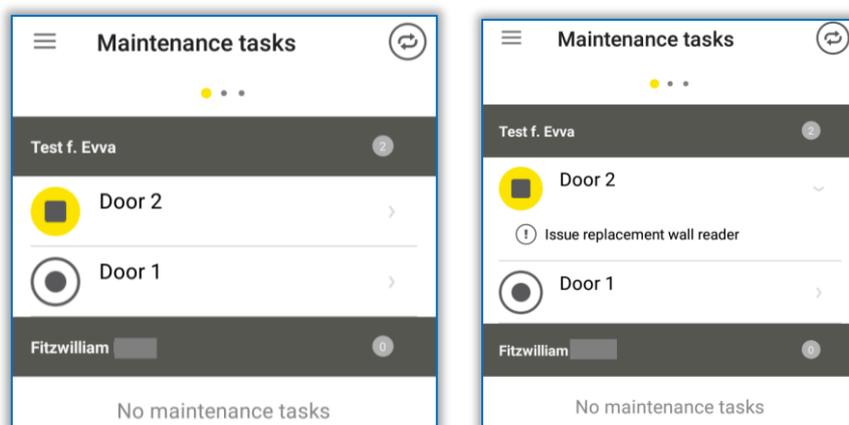


Figura 246: Tarefas de manutenção



Como técnico de manutenção, verifique regularmente as tarefas de manutenção para atualizar o mais rapidamente possível os componentes de bloqueio que têm de ser atualizados.

Se entrar no alcance de um componente de bloqueio com Bluetooth com um smartphone com autorização de manutenção (cilindro ou leitor de parede), o símbolo deste componente de bloqueio tem um fundo amarelo (p. ex. para cilindro).

Se tocar no símbolo amarelo, é estabelecida uma ligação ao componente de bloqueio e a atualização do componente é executada. Depois, aparecem os

detalhes do componente. É exibida uma atualização pendente do firmware nos detalhes do componente e poderá começar a partir daqui.

Além disso, como técnico de manutenção, obtém uma vista geral dos detalhes do componente de bloqueio ao atualizá-lo para verificar diretamente o estado do componente de bloqueio e os eventos do cilindro sob a forma de protocolo.

- > Atualize um componente de bloqueio para obter os detalhes do componente. Se existente, veja aqui também a localização do componente de bloqueio como coordenadas de GPS ou o endereço registado manualmente na Administração online do AirKey. Se tocar no símbolo amarelo da localização, é automaticamente feito o encaminhamento para o fornecedor de cartões, que estará configurado por defeito no seu smartphone.

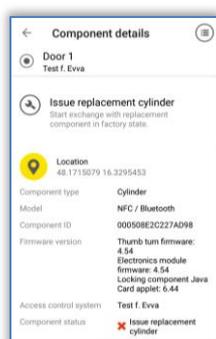


Figura 247: Visualização dos detalhes do componente de bloqueio



Atualize os seus componentes AirKey regularmente. Só assim o seu sistema AirKey será seguro e estará o mais atualizado possível. Poderá obter mais informações a respeito da atualização dos componentes AirKey em [Operação e manutenção do sistema AirKey](#).

O modo de manutenção serve apenas para os sistemas de bloqueio onde estiver ativado, podendo ser ativado em vários sistemas de bloqueio ao mesmo tempo.



O modo Hands-free no smartphone tem de ser desativado para se poder executar tarefas de manutenção ou atualizações do componente de bloqueio.

6.13 Adicionar um componente AirKey

Para poder adicionar um componente de bloqueio ou um meio de acesso (exceto smartphones) com o seu smartphone ao seu sistema de controlo de acessos AirKey, o modo de manutenção tem de estar ativado para o sistema de controlo de acessos e o componente AirKey tem de estar no estado de fábrica.

6.13.1 [Adicionar meios](#): ver o capítulo 4.12

6.13.2 [Adicionar componente de bloqueio](#): ver o capítulo 4.11

6.14 Remover um componente AirKey

Como pré-condição para remover, o componente de bloqueio ou o meio (exceto smartphones) tem de ser removido, em primeiro lugar, na Administração online do AirKey (ver [Remover componente de bloqueio](#) e [Remover meio](#)) e o smartphone tem de ter o modo de manutenção ativado.

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente** ❶.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones Android): toque, no caso do componente de bloqueio que pretende conectar, no menu contextual (:) e selecione, depois, **Conectar** ❷.
- > Se estabelecer a ligação por **Bluetooth** (em iPhones): arraste, no caso do componente de bloqueio que pretende conectar, na designação do componente para a esquerda e selecione, depois, **Conectar** ❸.

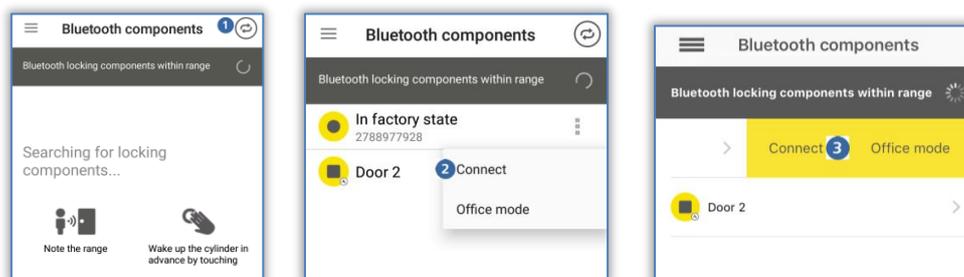


Figura 248: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone)

- > Siga as instruções e encoste o smartphone com NFC ao meio ou ao componente de bloqueio; ou o smartphone com Bluetooth ao alcance ao componente de bloqueio.

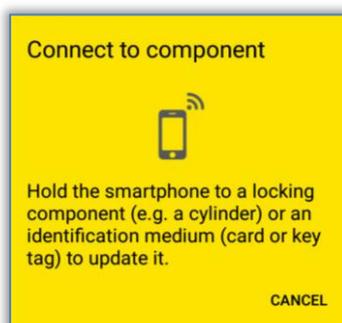


Figura 249: Aplicação AirKey – Conecte com o componente

Encoste o smartphone com NFC ao componente AirKey / ao meio, o qual já foi removido da Administração online do AirKey ou coloque o smartphone com Bluetooth dentro do alcance do componente a remover ou encoste diretamente ao meio a remover e siga as instruções.

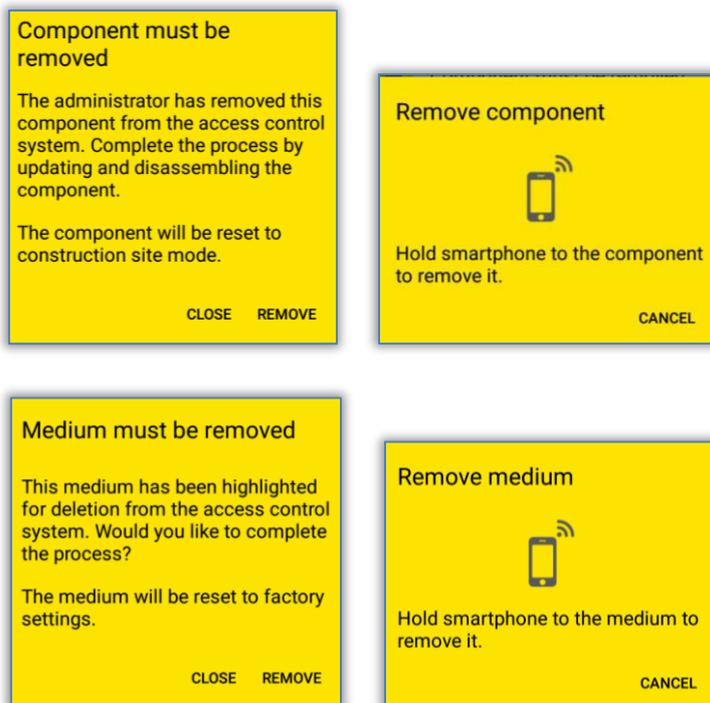


Figura 250: Remover componente AirKey

Após atualização bem-sucedida, os componentes de bloqueio e os meios encontram-se novamente no estado de fábrica.

Se um meio de acesso tiver de ser removido com um iPhone do sistema de controlo de acessos AirKey, o processo decorre à semelhança do processo para adicionar através de **Codificar meios**.

- > Da lista apresentada com os componentes de bloqueio com Bluetooth, selecione aquele através do qual pretende atualizar o meio.

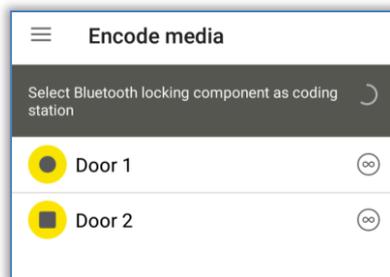


Figura 251: Codificar meios – Lista de seleção dos componentes de bloqueio com Bluetooth

- > Encoste o meio que pretende atualizar ao componente de bloqueio AirKey.
- > Receberá uma notificação a informar que o componente de bloqueio AirKey está pronto.

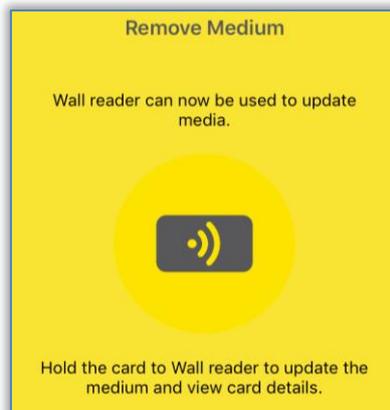


Figura 252: Remover um meio com o iPhone

- > Encoste o meio de acesso ao componente de bloqueio AirKey e toque em **Remover**.

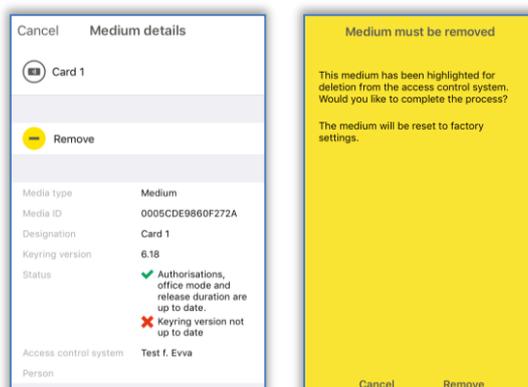


Figura 253: Remover meio

- > Receberá uma mensagem de confirmação de que o meio de acesso foi removido do componente de bloqueio AirKey com sucesso.



Em nenhum momento afaste o smartphone do componente de bloqueio ou meio durante este processo.



O processo para remover os componentes de bloqueio e meios (exceto smartphones) é idêntico.



Os componentes com NFC não podem ser removidos com o iPhone do sistema de controlo de acessos. Para isso, é necessária a opção de uma estação de codificação ou de um smartphone Android com ligação NFC.

6.15 Dados protocolares da aplicação AirKey

Para os smartphones, pode ser ativada a autorização para visualizar dados protocolares através da Administração online do AirKey. A visualização dos dados protocolares não depende da autorização de manutenção e pode ser ativada para uma pessoa individualmente.

A visualização dos dados protocolares pode ser ativada e desativada na Administração online do AirKey nos detalhes do smartphone. Poderá obter mais informações a respeito da edição de um meio em [Editar meio](#).

Poderá aceder o protocolo na aplicação como descrito a seguir:

- > Inicie a aplicação AirKey.
- > No menu principal, selecione o ponto de menu **Autorizações**.
- > À direita, em cima, selecione o símbolo do protocolo .

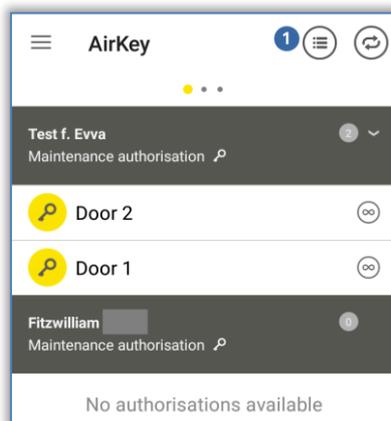


Figura 254: Símbolo do protocolo

- > O protocolo é exibido.



No protocolo da aplicação AirKey, são apresentados os registos protocolares da pessoa a quem foi atribuído o smartphone.

6.16 Vista geral da função Hands-free (mãos livres)

Para componentes de bloqueio com Bluetooth está disponível o modo Hands-free. Trata-se, assim, de uma função de conforto, sendo que o componente de bloqueio já não tem de ser selecionado na aplicação. A função Hands-free não se equipara à função "Desbloquear com Bluetooth", mas pode ser ativada para conforto extra.

O cilindro, após contacto, envia um sinal Bluetooth. No caso do leitor de parede, o funcionamento é automático, sem contacto. Se uma aplicação AirKey receber este sinal Bluetooth dentro do alcance de bloqueio, o processo de desbloqueio será iniciado. O alcance de bloqueio pode ser individualmente ajustado, na aplicação, para cilindro e leitor de parede.

- > Na aplicação do AirKey, no menu principal **Definições** o modo Hands-free tem de ser ativado.

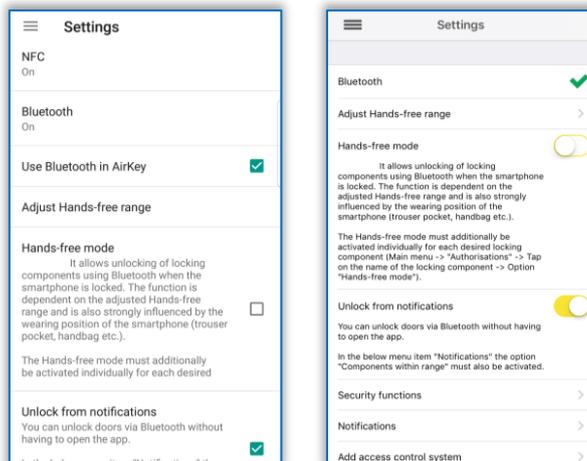


Figura 255: Definições AirKey-App



Em smartphones Android, é iniciado um serviço ao ativar esta função. Este serviço procura continuamente, mesmo com a aplicação AirKey encerrada, componentes de bloqueio com Bluetooth dentro do alcance e aumenta o consumo da bateria do smartphone. O serviço termina assim que a função for novamente desativada. Caso toque nas notificações do serviço, tem acesso direto às definições da aplicação AirKey.

- > Adicionalmente, para cada componente de bloqueio ou área, nos detalhes de autorização, no ponto de menu **Autorizações**, o modo Hands-free (mãos livres) tem de ser ativado. Ao ativar o modo Hands-free pela primeira vez, aparece uma caixa de diálogo em que a função pode ser ativada automaticamente para todos os componentes de bloqueio ou individualmente apenas para um componente de bloqueio.

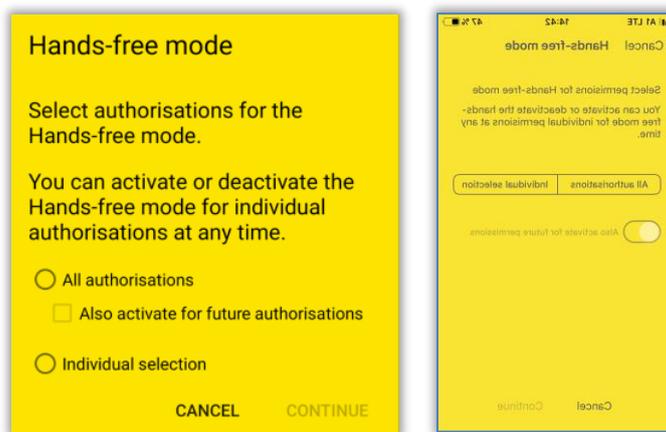


Figura 256: Autorizações para o modo Hands-free



Ative **Ativar também para futuras autorizações** para ativar automaticamente o modo Hands-free igualmente para cada autorização adicional.



Dependendo da configuração **Acesso a partir do ecrã de bloqueio** nas definições da Administração online do AirKey, pode bloquear diretamente a partir do ecrã de bloqueio ou o ecrã de bloqueio tem de ser cancelado

previamente. Poderá encontrar mais detalhes em [Informações gerais](#).



O modo Hands-free (mãos-livres) só pode ser utilizado para componentes de bloqueio em que um administrador autorizou o modo mãos-livres. Poderá encontrar mais detalhes no capítulo [Editar componente de bloqueio](#).

Definir o alcance do modo hands-free: ver o capítulo 6.9.3

O que se deve ter em conta ao utilizar o modo Hand-free?

No caso de o visor do smartphone estar bloqueado, a função depende

- > da configuração "Acesso a partir do ecrã de bloqueio" nas definições da Administração online do AirKey;
- > do fabricante, do sistema operativo, da antiguidade, do número de aplicações instaladas, das otimizações das aplicações (função de poupança de energia) do smartphone;
- > de fatores interferentes, tais como o tipo de edifício (p. ex., construção em betão armado) e o ambiente de sinais de rádio;
- > do local onde o smartphone é guardado e transportado e do alcance de bloqueio ajustado para a função Hand-free;
- > do facto de o smartphone se estar a ligar, nesse momento, a uma WLAN.

Como consequência destes fatores, a função Hand-free torna-se mais lenta ou deixa mesmo de funcionar. Para acelerar o processo de desbloqueio via Hands-free, o smartphone, de acordo com o sistema operativo (p. ex., iOS), tem de ser desbloqueado e a aplicação AirKey iniciada. Neste caso, não é necessária a seleção do componente a ser desbloqueado na aplicação.

Para se evitar bloqueios inoportunos, deve considerar-se o seguinte:

- > Após cada processo de desbloqueio, ao ler o leitor de parede, decorre um intervalo de 2 minutos. Isto significa que um leitor de parede só poderá ser novamente desbloqueado com a função Hands-free quando o smartphone em questão não for detetado durante 2 minutos na área de alcance de receção do leitor de parede. Esta situação impede processos de desbloqueio indesejáveis ao deixar a área de alcance de desbloqueio.
- > Idealmente, só um componente de bloqueio deverá encontrar-se na área de alcance de bloqueio de um smartphone.
- > Para executar funções como "Codificar meios" ou "Atualizações de componentes de bloqueio", o modo Hands-free tem de ser desativado na aplicação.

7 Utilização dos componentes de bloqueio AirKey

7.1 Acesso com o smartphone

Para obter acesso a um componente de bloqueio AirKey, os requisitos seguintes terão de ser preenchidos:

- > A ligação NFC ou Bluetooth está ativada no smartphone.
- > A aplicação AirKey está instalada e registada.
- > Foi atribuída uma autorização válida ao smartphone (poderá obter os detalhes em [Registar smartphone](#) e [Atribuir autorizações](#)).
- > No caso de processos de desbloqueio, encoste o smartphone ao componente de bloqueio via NFC. A posição com as melhores características de leitura depende do modelo de smartphone. O alcance para a leitura também depende do tipo de smartphone e basta estar a uns milímetros de encostar. No caso de processos de desbloqueio via Bluetooth, o alcance para leitura depende, por um lado, do tipo de smartphone e, por outro, das definições pessoais na aplicação AirKey no smartphone com respeito ao modo hands-free. Este pode estar a alguns metros.
- > Se for pedida a introdução de um PIN, introduza o PIN correto, antes de bloquear com o smartphone via NFC ou Bluetooth. (Poderá obter detalhes a respeito do PIN em [Funções de segurança](#)).
- > Observe a sinalização ótica do componente de bloqueio. No caso de ligação NFC, não remova o smartphone do componente de bloqueio e, no caso de Bluetooth, permaneça dentro do alcance de receção até que o componente de bloqueio sinalize a verde. (A sinalização a azul significa apenas que existe comunicação entre o smartphone e o componente de bloqueio.)
- > O componente de bloqueio aceita o tempo de ativação definido e dá-lhe acesso.



Com os modelos iPhone XR, XS, XS Max e os novos, também poderá bloquear componentes de bloqueio com Bluetooth via NFC. Encoste o smartphone ao componente de bloqueio e toque na mensagem indicativa de que o tag NFC foi detetado. Tal abrirá a aplicação AirKey e executará um processo de desbloqueio via Bluetooth.



Figura 257: Tag iOS NFC



Verifique a sua autorização ou o PIN, se o componente de bloqueio sinalizar a vermelho.



O bloqueio de componentes de bloqueio via NFC não é possível com o bloqueio de ecrã ativo ou durante um telefonema. Naturalmente, a aplicação AirKey não pode estar iniciada ou em segundo plano para se poder bloquear componentes de bloqueio. O bloqueio de componentes de bloqueio via Bluetooth, ao contrário, é possível com o bloqueio de ecrã ativo através de notificações Push. Só é preciso ser ativada a opção "Desbloquear a partir de notificações" nas definições da aplicação AirKey e nas definições da Administração online do AirKey "Acesso a partir do ecrã de bloqueio".

7.2 Acesso com meios como cartões, porta-chaves, pulseiras ou chaves combinadas

Para obter um acesso com um componente de bloqueio AirKey, o meio tem de estar adicionado no sistema de controlo de acessos e apresentar uma autorização válida (poderá obter detalhes em [Adicionar cartões, porta-chaves e chaves combinadas com o smartphone](#) e [Atribuir autorizações](#)).

- > Mantenha o meio encostado ao componente de bloqueio. O alcance para a leitura depende do tipo de meio e a distância é, regra geral, de alguns milímetros.
- > Observe a sinalização ótica do componente de bloqueio. Não afaste o meio enquanto o componente de bloqueio não sinalizar a verde. (A sinalização a azul significa apenas que existe comunicação entre o meio e o componente de bloqueio.)



Verifique a sua autorização, se o componente de bloqueio sinalizar a vermelho.

- > O componente de bloqueio autoriza durante o tempo definido, obtendo, portanto, acesso.



Os meios como cartões, porta-chaves, pulseiras e chaves combinadas funcionam muito limitadamente, ou não funcionam, se estiverem próximos de outros meios ou objetos metálicos. Uma situação para aqui é, por exemplo, o meio estar num porta-moedas ou num chaveiro.



A identificação com uma chave combinada nos componentes de bloqueio tem de decorrer do lado onde se possa ver o símbolo RFID.

8 Operação e manutenção do sistema AirKey

8.1 Atualizar componentes de bloqueio

Em geral, poderá atualizar cada componente de bloqueio AirKey, sem depender do sistema de controlo de acessos a que pertence, para partilhar dados entre a Administração online do AirKey e o componente de bloqueio AirKey.

A atualização pode decorrer através do smartphone ou, opcionalmente, através da estação de codificação. A atualização com o smartphone impõe unicamente a instalação da aplicação AirKey e o registo num sistema de controlo de acessos AirKey à sua escolha.

Na atualização de componentes de bloqueio, são realizadas as seguintes ações:

- As horas são redefinidas.
- Os registos protocolares e o estado das pilhas são lidos.
- As tarefas de manutenção são atualizadas (lista negra, ativações noutros sistemas de bloqueio etc.).
- Os detalhes dos componentes são lidos.

Siga as instruções para atualizar um componente de bloqueio AirKey com o smartphone:

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente** ①.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones Android): toque, no caso do componente de bloqueio que pretende conectar, no menu contextual (:) e selecione, depois, **Conectar** ②.
- > Se estabelecer a ligação por **Bluetooth** (em iPhones): arraste, no caso do componente de bloqueio que pretende conectar, na designação do componente para a esquerda e selecione, depois, **Conectar** ③.

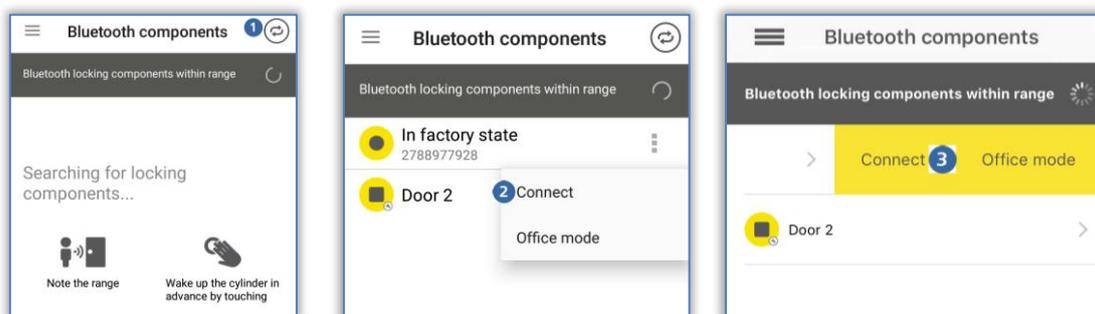


Figura 258: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone)

- > Siga as instruções.



Figura 259: Atualizar dados

Os dados estão a ser atualizados. Durante a transmissão, o smartphone com NFC não pode ser afastado do componente a sincronizar, ou, no caso de smartphone com Bluetooth, este não pode ser afastado do raio de alcance do componente de bloqueio. Depois de o processo estar concluído, receberá a mensagem correspondente.



Conforme a situação, se o modo de manutenção está ativado no smartphone e o componente de bloqueio se encontra no sistema de controlo de acessos AirKey do próprio ou de terceiros, as informações visualizadas podem divergir da mensagem de atualização.

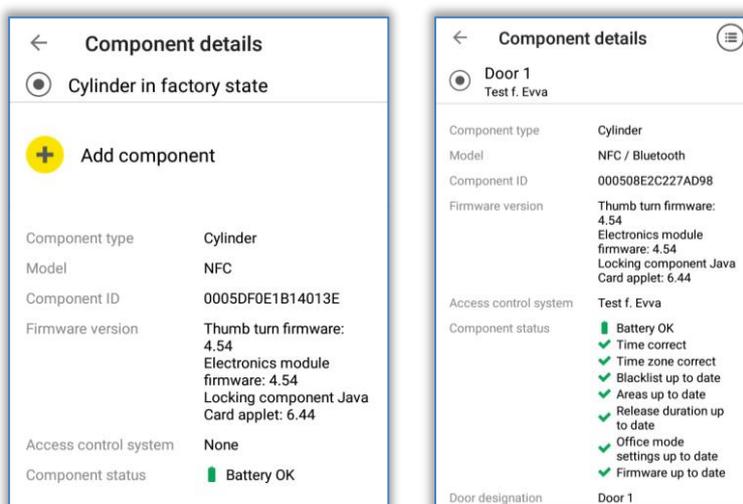


Figura 260: Mensagens de atualização



Desative o modo Hands-free antes de se conectar a um componente de bloqueio com Bluetooth. Caso contrário, poderá provocar interrupções na ligação.



Os componentes de bloqueio com Bluetooth também podem ser atualizados automaticamente após cada processo de desbloqueio via Bluetooth. Poderá encontrar mais informações sobre a função "Atualização após cada desbloqueio" em [Valores por defeito \(para todos os componentes de bloqueio adicionados como novos\)](#).

Option

Atualizar o componente de bloqueio com a estação de codificação

Para atualizar o componente de bloqueio com a estação de codificação, proceda da seguinte forma:

- > Inicie a sessão no seu sistema de controlo de acessos AirKey e assegure que a estação de codificação está em posição e que foi selecionada na Administração online do AirKey.
- > Coloque o componente de bloqueio sobre a estação de codificação.



Figura 261: Atualizar o componente de bloqueio com a estação de codificação

- > Só remova o componente de bloqueio da estação de codificação quando a atualização estiver concluída e visualizar a mensagem de confirmação.



Conforme a situação, se o componente de bloqueio se encontra no sistema de controlo de acessos AirKey do próprio ou de terceiros, as informações visualizadas podem divergir da mensagem de confirmação do processo.

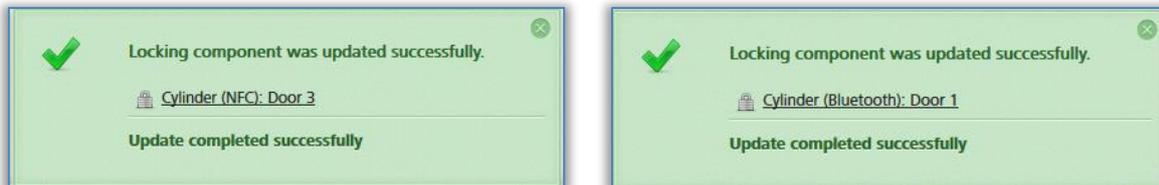


Figura 262: Componente de bloqueio atualizado com a estação de codificação



Atualize os seus componentes de bloqueio AirKey regularmente. Só assim o seu sistema de controlo de acessos AirKey será seguro e estará o mais atualizado possível.

8.2 [Atualizar o smartphone](#): ver o capítulo 6.10

8.3 Atualizar meios

Poderá atualizar qualquer meio AirKey, independentemente da sua associação com o sistema de controlo de acessos. A atualização pode decorrer através do smartphone Android ou, opcionalmente, através da estação de codificação. A atualização com o smartphone impõe unicamente a instalação da aplicação AirKey e o registo num sistema de controlo de acessos AirKey.



No caso do iPhone, os meios podem ser atualizados à semelhança do processo [Codificar meios](#), sendo que se utiliza um componente de bloqueio

AirKey como estação de codificação.

- > Num smartphone Android, toque no símbolo **Conecte com o componente** ①, à direita, em cima, na aplicação AirKey.

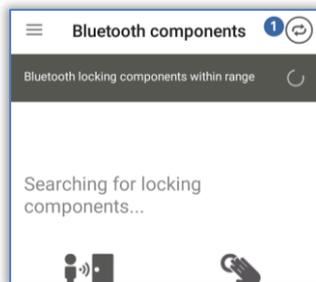


Figura 263: Símbolo "Conecte com o componente" (só em smartphones Android)

- > Siga as instruções e encoste o smartphone ao meio.

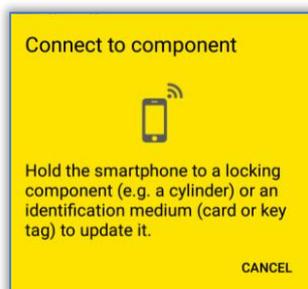


Figura 264: Atualizar dados

Os dados estão a ser atualizados. Durante a transferência, o smartphone não pode ser afastado do objeto a sincronizar. Depois de o processo estar concluído, receberá a mensagem correspondente.



Para atualizar a chave combinada com o smartphone, a chave combinada tem de ser mantida encostada ao smartphone junto à antena NFC do smartphone, com o lado que tem o símbolo RFID.

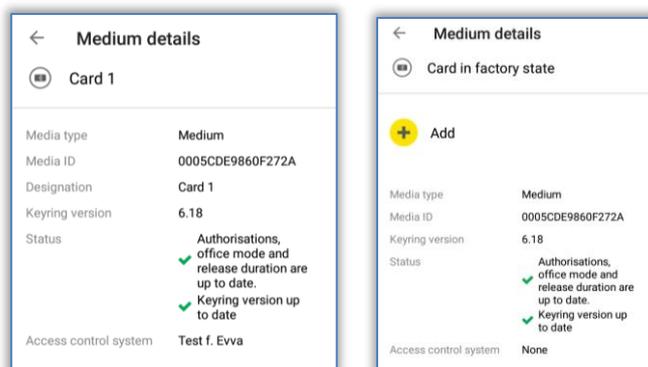


Figura 265: Aplicação AirKey atualiza um meio

Option

Atualizar o meio com a estação de codificação

Para atualizar meios como cartões, porta-chaves, pulseiras ou chaves combinadas com a estação de codificação, proceda da seguinte forma:

- > Inicie a sessão no seu sistema de controlo de acessos AirKey e assegure que a estação de codificação está em posição e que foi selecionada na Administração online do AirKey.
- > Coloque o meio sobre a estação de codificação.



Figura 266: Atualizar o meio com a estação de codificação

- > Só remova o meio da estação de codificação se a atualização estiver concluída e visualizar a mensagem de confirmação.



Conforme a situação, se os meios se encontram no sistema de controlo de acessos AirKey do próprio ou de terceiros, as informações visualizadas podem divergir da mensagem de confirmação do processo.



Figura 267: Meio próprio ou de terceiros atualizado com a estação de codificação



Atualize os seus meios AirKey regularmente. Só assim o seu sistema de controlo de acessos AirKey será seguro e estará o mais atualizado possível.



Apenas através da atualização regular dos meios se pode assegurar que todos os registos protocolares dos meios são transferidos para a Administração online do AirKey.



Para adicionar a chave combinada pela estação de codificação, a chave combinada tem de ser colocada sobre a estação de codificação com o lado que tem o símbolo RFID. A atualização não é possível em toda a área de leitura da estação de codificação – no caso do tipo em questão (HID Omnikey 5421), a chave combinada só é reconhecida no terço superior e inferior da estação de codificação.

8.4 Atualizar firmware de componentes de bloqueio

Se estiver disponível um novo firmware para os componentes de bloqueio, esta informação pode ser visualizada nos detalhes do componente de bloqueio, nas tarefas de manutenção e na atualização do componente de bloqueio.



Antes de atualizar um firmware, verifique o estado das pilhas do componente de bloqueio (cilindro). Se existir um aviso de "Pilhas gastas", tem de se substituir, primeiro, as pilhas para garantir que a atualização decorre sem problemas.

A versão atual do firmware do componente de bloqueio é visualizada nos detalhes do componente de bloqueio.

A atualização do firmware dos componentes de bloqueio pode decorrer através do smartphone ou, opcionalmente, através de uma estação de codificação.

Para realizar atualizações de firmwares com o smartphone, a autorização especial "autorização de manutenção" tem de estar ativada no smartphone. Proceda a atualizações dos firmwares com o smartphone como a seguir descrito:

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente** ①.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones Android): toque, no caso do componente de bloqueio que pretende conectar, no menu contextual (:) e selecione, depois, **Conectar** ②.
- > Se estabelecer a ligação por **Bluetooth** (em iPhones): arraste, no caso do componente de bloqueio que pretende conectar, na designação do componente para a esquerda e selecione, depois, **Conectar** ③.

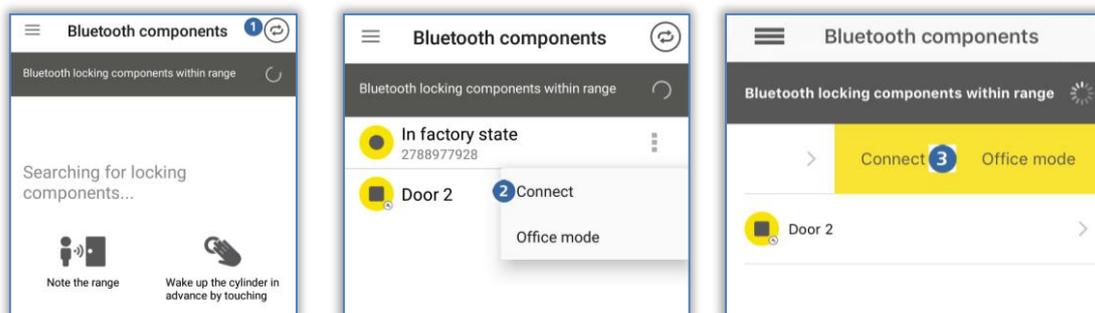


Figura 268: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone)

- > Siga as instruções.

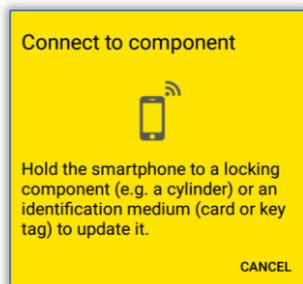


Figura 269: Conecte com o componente – Atualização do firmware

Os dados estão a ser atualizados. Durante a transmissão, o smartphone com NFC não pode ser afastado do componente a sincronizar, ou, no caso de smartphone com Bluetooth, este não pode ser afastado do raio de alcance do componente de bloqueio. Depois de o processo estar concluído, receberá a mensagem correspondente.

- > O componente de bloqueio é atualizado e os detalhes do componente podem ser visualizados. Nos detalhes do componente pode visualizar-se que o firmware do componente não está atualizado.

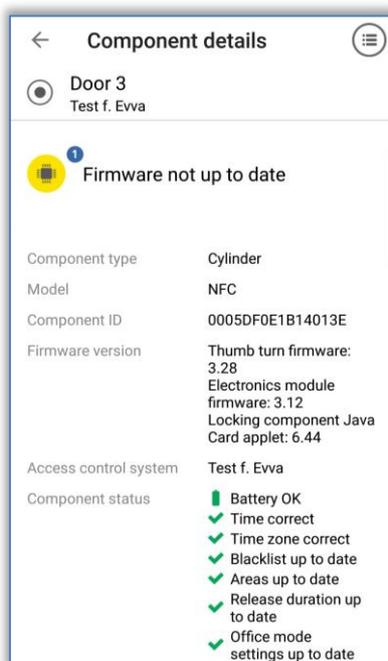


Figura 270: Aplicação AirKey – Detalhes do componente

- > Clique, neste ecrã, na opção **Atualizar firmware** .
- > Encoste o smartphone com ligação NFC ao componente de bloqueio ou mantenha o smartphone com ligação Bluetooth dentro do raio de alcance.



Figura 271: Aplicação AirKey – Atualizar firmware



A atualização do firmware pode durar alguns minutos dependendo da ligação à Internet. Encoste o smartphone com ligação NFC ao componente de bloqueio, neste momento durante algum tempo, ou mantenha o smartphone com ligação Bluetooth dentro do raio de alcance do componente de bloqueio.

Durante a transferência, o smartphone não pode ser afastado do componente a atualizar. A execução bem-sucedida do primeiro passo da atualização é concluída com uma mensagem de confirmação.

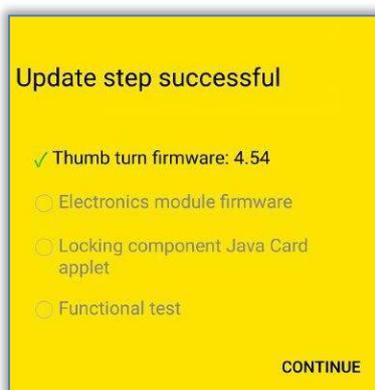


Figura 272: Aplicação AirKey – Passo de atualização executado com sucesso

- > Afaste o smartphone do componente de bloqueio até que o componente de bloqueio pisque e sinalize com tom sonoro.
- > Encoste o smartphone com ligação NFC ao componente de bloqueio ou mantenha o smartphone com ligação Bluetooth dentro do raio de alcance do componente de bloqueio e siga as instruções.

Quando a atualização do firmware tiver sido concluída com sucesso, aparecerá a respetiva mensagem de confirmação.

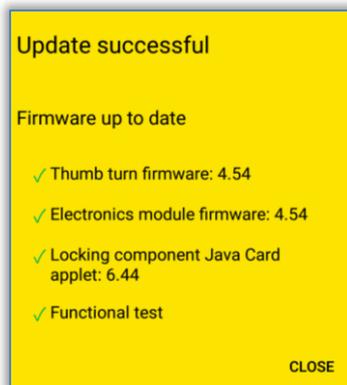


Figura 273: Aplicação AirKey – Atualização executada com sucesso

- > Confirme a mensagem de confirmação com **Fechar**, para concluir a atualização do firmware.



O estado do componente de bloqueio foi, assim, ajustado a todo o sistema. A tarefa de manutenção deixa de ser indicada e a versão de firmware correta deve ser reconhecida nos detalhes do componente de bloqueio.

Option

Atualizar o firmware com a estação de codificação:

- > Coloque o componente de bloqueio sobre a estação de codificação. Quando a estação de codificação inicia uma comunicação com o componente de bloqueio, inicia automaticamente uma atualização.

Receberá uma mensagem a confirmar que a atualização foi executada com sucesso.



Figura 274: Estação de codificação – Mensagem de confirmação da atualização de um componente de bloqueio

Se estiver disponível uma atualização do firmware para um componente de bloqueio, é indicado um link correspondente 1.

- > Clique em **Executar atualização do firmware** para iniciá-la.

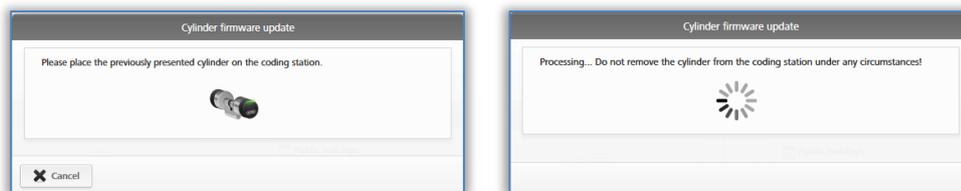


Figura 275: Estação de codificação – Atualização do firmware do cilindro



A atualização do firmware pode durar vários minutos, dependendo da ligação Internet. Não remova o componente de bloqueio da estação de codificação durante esse período.

O primeiro passo da atualização do firmware é concluído com uma mensagem de confirmação.

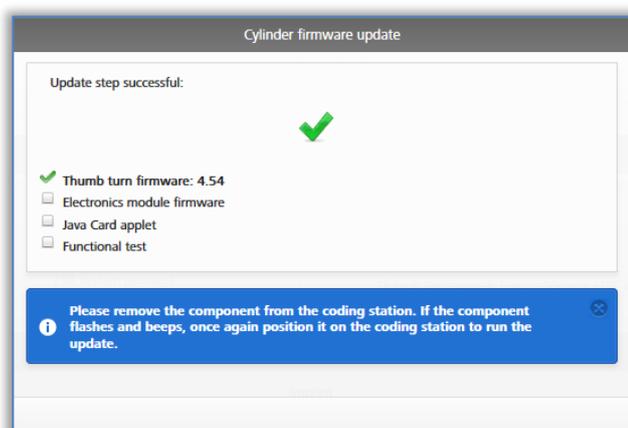


Figura 276: Estação de codificação – Passo da atualização executado com sucesso

- > Remova o componente de bloqueio da estação de codificação até que este reinicie com uma sinalização sonora e ótica.
- > Coloque o componente de bloqueio novamente na estação de codificação para concluir o processo.

Quando a atualização estiver concluída, receberá uma mensagem de confirmação.

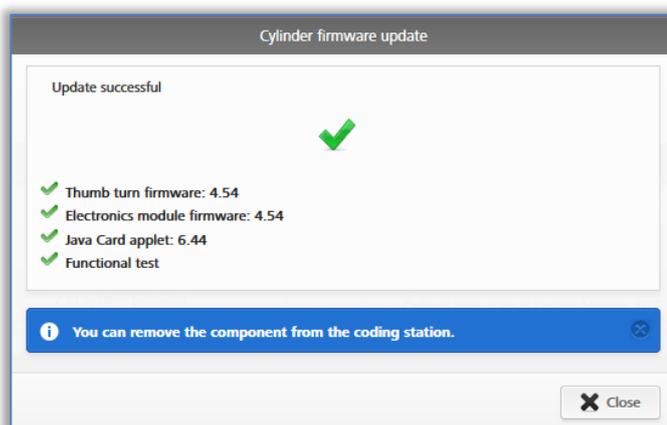


Figura 277: Estação de codificação – Atualização do firmware executada com sucesso

O componente de bloqueio é novamente atualizado após fechar a mensagem de confirmação.



Figura 278: Estação de codificação – Componente de bloqueio atualizado com sucesso

- > Após a atualização, remova o componente de bloqueio da estação de codificação.



O estado do componente de bloqueio foi, assim, ajustado a todo o sistema. A tarefa de manutenção deixa de ser indicada e a versão de firmware correta deve ser reconhecida nos detalhes do componente de bloqueio.



Para a atualização do firmware, abra a porta e fixe-a de forma a que esta não possa fechar acidentalmente. Depois, verifique o funcionamento correto do componente de bloqueio antes de voltar a fechar a porta.



Ao atualizar o firmware de componentes de bloqueio, tem de se garantir de que se tem à disposição uma ligação à Internet estável e que a ligação dos dados durante a atualização do firmware está disponível sem interrupções. Existem, para isso, várias definições à disposição, que dependem do respetivo smartphone e sistema operativo (p. ex., permitir a comutação automática da rede entre dados móveis e WLAN).



A EVVA recomenda ter a versão de firmware dos componentes de bloqueio sempre atualizada.

8.5 Atualizar a versão de meios Keyring

No sistema AirKey, "Keyring" é o nome de um programa de software que gere todos os dados relevantes do AirKey, que são memorizados nos meios de acesso passivos, como cartões, porta-chaves, chaves combinadas e pulseiras. Se estiver disponível uma nova versão de Keyring para os meios, isto pode ser visualizado nos detalhes dos meios, nas tarefas de manutenção, na página inicial **Home** e ao atualizar os meios.



A versão atual do firmware do meio é visualizada nos detalhes do meio.

A atualização dos meios Keyring pode decorrer através do smartphone ou, opcionalmente, através de uma estação de codificação. Para realizar atualizações de Keyrings com o

smartphone, a autorização especial "autorização de manutenção" tem de estar ativada no smartphone. Proceda a atualizações dos Keyrings com o smartphone como se descreve seguidamente:

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente 1**.
- > Ligação por **Bluetooth** (em smartphones Android e iPhones): no menu principal da aplicação AirKey, seleccione o ponto do menu **Codificar meios** – ver também [Codificar meios](#).

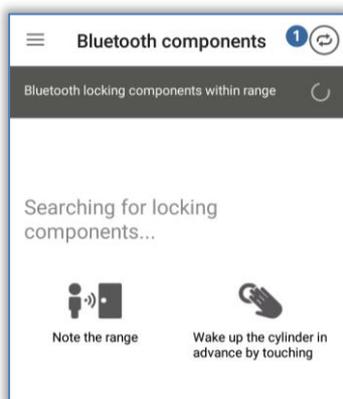


Figura 279: Aplicação AirKey – Conecte com o componente

- > Mantenha o smartphone com ligação NFC encostado ao meio.
- > O meio é atualizado. É indicado que está disponível uma nova versão de Keyring para si.

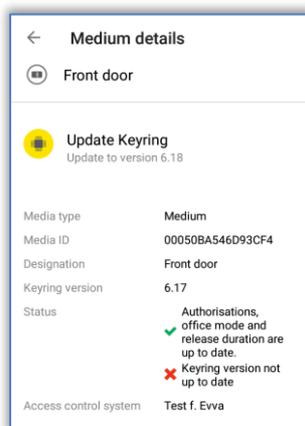


Figura 280: Aplicação AirKey – Detalhes do meio

- > Seleccione a opção **Atualização do Keyring**.
- > Encoste o smartphone ao meio e siga as instruções.

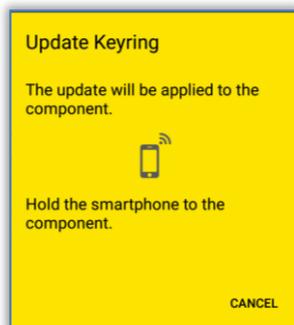


Figura 281: Aplicação AirKey – Atualizar Keyring



A atualização do Keyring pode durar alguns minutos dependendo da ligação à Internet. Mantenha o smartphone, neste momento, encostado ao meio durante algum tempo.

Durante a transferência, o smartphone não pode ser afastado do meio a atualizar. A execução bem-sucedida da atualização do Keyring é concluída com uma mensagem de confirmação.

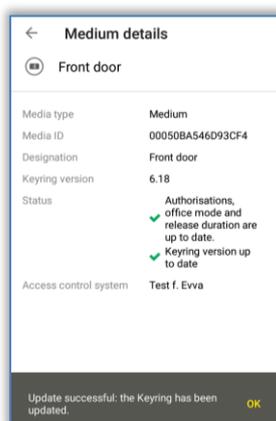


Figura 282: Aplicação AirKey – Atualização do Keyring executada com sucesso



O estado do meio foi, assim, ajustado a todo o sistema. A versão de Keyring correta é indicada nos detalhes do meio.

Para atualizar a chave combinada com o smartphone, a chave combinada tem de ser encostada ao smartphone, com o lado que tem o símbolo RFID.

Option

Atualizar a versão de Keyring com a estação de codificação:

- > Coloque o meio sobre a estação de codificação. Se a estação de codificação reconhecer o meio, é iniciada uma comunicação com o meio.

Receberá uma mensagem a confirmar que a atualização foi executada com sucesso.



Figura 283: Estação de codificação – Atualização do Keyring disponível

Se estiver disponível uma atualização do Keyring para o meio, é indicado um link correspondente 1.

- > Clique em **Executar atualização do Keyring (x.x)** para iniciá-la.

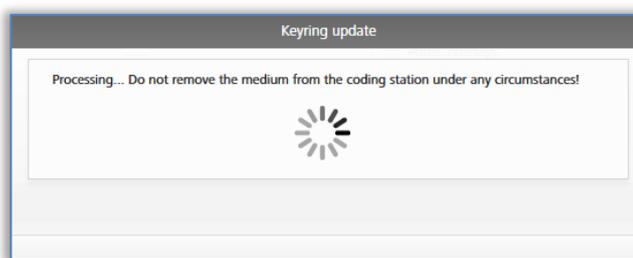


Figura 284: Estação de codificação – Atualização do Keyring



A atualização do Keyring pode durar alguns minutos dependendo da ligação à Internet. Não remova o meio da estação de codificação durante esse período.

Durante a atualização do Keyring, o meio não pode ser removido da estação de codificação. A atualização do Keyring é concluída com uma mensagem de confirmação.

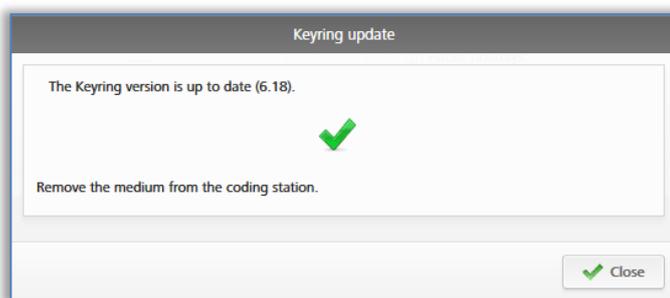


Figura 285: Estação de codificação – Atualização do Keyring executada com sucesso

A atualização do Keyring foi, assim, concluída com sucesso. O meio é novamente atualizado após fechar a mensagem de confirmação.



Figura 286: Estação de codificação – Meio atualizado com sucesso

- > Após a atualização, remova o meio da estação de codificação.



Para adicionar a chave combinada pela estação de codificação, a chave combinada tem de ser colocada sobre a estação de codificação com o lado que tem o símbolo RFID. A atualização não é possível em toda a área de leitura da estação de codificação – no caso do tipo em questão (HID Omnikey 5421), a chave combinada só é reconhecida no terço superior e inferior da estação de codificação.

O estado do meio foi, assim, ajustado a todo o sistema. A versão de Keyring correta é indicada nos detalhes do meio.



Ao atualizar a versão de meios Keyring, tem de se garantir de que se tem à disposição uma ligação à Internet estável e que a ligação dos dados durante a atualização do Keyring está disponível sem interrupções. Existem, para isso, várias definições à disposição, que dependem do respetivo smartphone e sistema operativo (p. ex., permitir a comutação automática da rede entre dados móveis e WLAN, evitar más ligações à Internet etc.).



A EVVA recomenda ter a versão de meios Keyring sempre atualizada.

8.6 Atualizar a versão da aplicação do smartphone

Se estiver disponível uma nova aplicação AirKey para o smartphone, será indicada a respetiva informação no smartphone. De acordo com as definições da Google Play Store ou da Apple App Store, a aplicação AirKey é atualizada automaticamente ou após confirmação manual.

Depois da atualização da versão da aplicação, a aplicação AirKey, como habitualmente, pode continuar a ser utilizada.



Para carregar aplicações da Google Play Store ou da Apple App Store é necessário uma conta Google ou uma Apple ID.



Pode acontecer que a atualização da aplicação AirKey seja recomendada ou obrigatória. Nestes casos, na aplicação AirKey será exibida a mensagem correspondente. Desta forma, determinadas funções serão limitadas, o

bloqueio de componentes de bloqueio continua a ser possível em ambas as situações.



A EVVA recomenda manter sempre a aplicação AirKey atualizada para o smartphone e ativar a atualização automática de aplicações na Google Play Store ou na Apple App Store.

8.7 Substituição das pilhas e alimentação de emergência

No caso de componentes de bloqueio que funcionam a pilhas, as pilhas têm de ser substituídas dentro de intervalos de tempo. O estado das pilhas dos componentes de bloqueio pode ser consultado na Administração online do AirKey na atualização de componentes de bloqueio com smartphones com autorização de manutenção.

Distinguem-se entre três diferentes estados das pilhas:



Figura 287: Estado das pilhas

O componente de bloqueio sinaliza ele próprio no caso de aviso de "pilhas gastas" com uma sinalização especial durante um processo de desbloqueio com um meio. Poderá obter mais informações a respeito da sinalização em [Sinalização dos componentes de bloqueio](#).

8.7.1 Substituição das pilhas no cilindro AirKey



Proceda à substituição das pilhas com a porta aberta e bloqueada contra fecho, para que esta não possa fechar-se acidentalmente.

Certifique-se de que o relógio do cilindro AirKey mantém-se, no máximo, 1 minuto, depois de as pilhas terem sido removidas.

Recomenda-se fortemente substituir as vedações do cilindro AirKey de cada vez que se substitui as pilhas para garantir sempre a vedação. Aqui, trata-se da vedação entre o eixo do puxador e o puxador do lado de fora e das vedações no disco do puxador do lado de fora. Todas estas vedações estão disponíveis como peças de reposição. Poderá obter detalhes a este respeito junto do seu vendedor de produtos EVVA.

Recomenda-se fortemente, pelo menos, a seguir a uma substituição das pilhas, lubrificar o cilindro AirKey. Para este fim, deve-se lubrificar com um lubrificante recomendado pela EVVA, depois de retirar o puxador do lado de fora, aplicando uma gota de lubrificante entre o eixo do puxador e a caixa do cilindro, na parte de fora. Adicionalmente, no caso de desinstalar temporariamente o cilindro AirKey, recomenda-se, lubrificar na parte de trás do cilindro, entre a saliência de bloqueio e a caixa do cilindro. Poderá obter detalhes a este respeito junto do seu vendedor de produtos EVVA.

- > Bloqueie o componente de bloqueio com um meio válido.

- > Utilize a ferramenta de montagem, antes de o cilindro voltar a desengatar.
- > Desaperte o puxador do cilindro com a ferramenta de montagem encaixada, girando no sentido anti-horário.
- > Remova a ferramenta de montagem do puxador.
- > Abra o puxador, desapertando os três parafusos na parte de trás do puxador.
- > Retire o disco do puxador.
- > Desaperte cuidadosamente o suporte das pilhas, movimentando-o para cima.
- > Substitua, depois, as pilhas. Assegure-se de que as novas pilhas são colocadas na posição correta. Não misture pilhas usadas com novas.
- > Volte a fixar o suporte das pilhas.
- > Coloque o disco do puxador no puxador e aperte-o com os três parafusos.
- > Coloque a ferramenta de montagem no puxador.
- > Assegure-se de que o anel vedante fica corretamente colocado no eixo do cilindro e enrosque o puxador, girando-o no sentido horário sobre o cilindro até sentir resistência.
- > Remova a ferramenta de montagem.
- > Gire o puxador, depois, no sentido anti-horário até notar que engata no sítio.
- > Assegure-se de que o puxador e o módulo eletrônico ficam corretamente engatados.
- > Em seguida, atualize o cilindro com o smartphone ou com a estação de codificação para transferir os registos protocolares atuais para a Administração online do AirKey.
- > Verifique o funcionamento do cilindro experimentando bloquear antes de voltar a fechar a porta.



Devido às características físicas das pilhas, estas precisam de ser substituídas com antecedência se estiverem expostas a temperaturas muito baixas (inferiores a -10 °C) durante muito tempo, assim como deverá verificar o funcionamento do cilindro e o estado das pilhas.



Se for sinalizado um erro de comunicação depois da substituição das pilhas, significa que o puxador está a tentar comunicar com o módulo eletrônico. Isto não funciona, se o puxador não tiver sido enroscado no módulo eletrônico.



Verifique o estado das pilhas dos componentes de bloqueio através do smartphone com autorização de manutenção, atualizando o componente de bloqueio e consultando, depois, os detalhes do componente de bloqueio.

Se se der o caso de as pilhas não serem substituídas a tempo, é possível uma alimentação de emergência através do dispositivo de alimentação de emergência opcional.

Poderá obter a descrição desta medida em [Dispositivo de alimentação de emergência](#).



Durante a alimentação de emergência, substitua as pilhas e atualize o componente de bloqueio antes de voltar a fechar a porta.

Depois de usar, volte a fechar cuidadosamente a tampa de borracha, com o

logotipo EVVA para proteger a entrada do conector para a ligação do dispositivo de alimentação contra a penetração de poeiras e humidade. Não utilize aqui objetos pontiagudos para evitar possíveis danos.

8.8 Opções de reparação

Nas opções de reparação de componentes de bloqueio, pode existir uma reação a um defeito existente nestes. É possível emitir componentes de bloqueio de substituição no sistema de controlo de acessos ou remover um componente de bloqueio com defeito do sistema de controlo de acessos.

8.8.1 Emitir e instalar componentes de bloqueio de substituição

Ao emitir e ao instalar, depois, um componente de bloqueio de substituição, um componente de bloqueio existente com defeito é substituído por um componente de bloqueio no estado de fábrica. Neste processo, todas as características e autorizações para este componente de bloqueio permanecem inalteradas no sistema de controlo de acessos AirKey. O componente de bloqueio de substituição, depois de o processo estar concluído, deixa de estar no estado de fábrica.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → **Componente de bloqueio**.
- > Clique, na lista geral, no componente de bloqueio que pretende editar.
- > No separador "Definições", clique no bloco **Registo em protocolo e manutenção** em **Mostrar opções de reparação** .

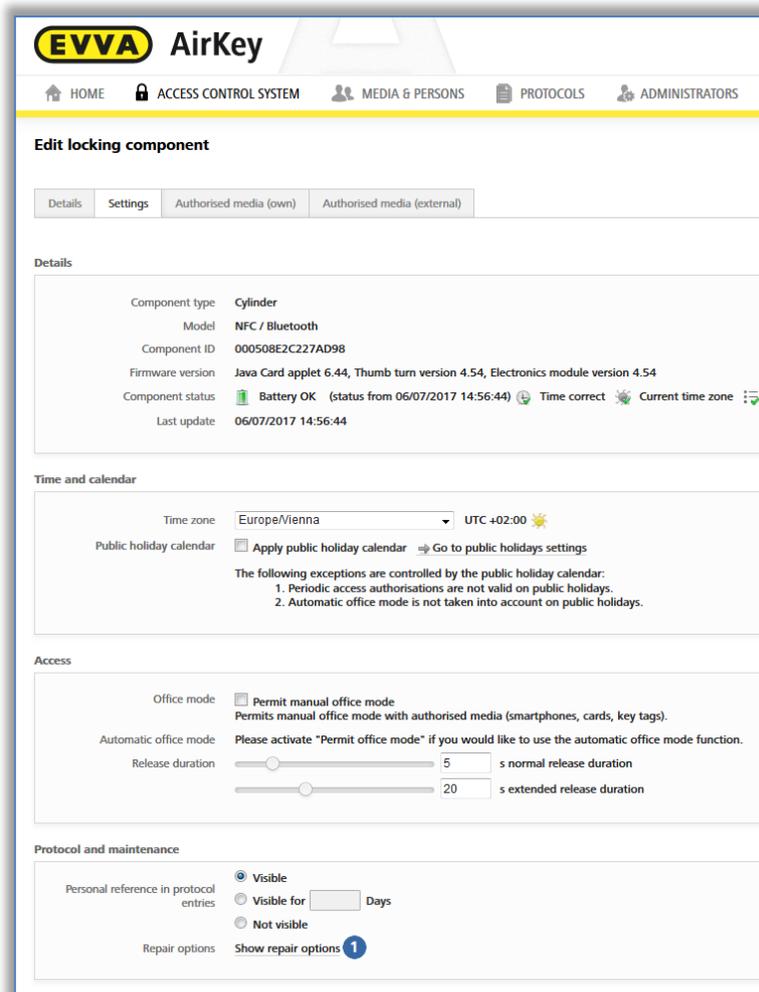


Figura 288: Editar componente de bloqueio – Opções de reparação

Abre-se a janela de diálogo **Opções de reparação**.

- > Normalmente, os botões de opção **Demontagem e instalação de componentes de substituição** **1** e Substituir o cilindro (puxador e módulo eletrónico em conjunto) estão predefinidos.
- > Em alternativa, poderá selecionar o botão de opção **Substituir apenas o puxador eletrónico**.

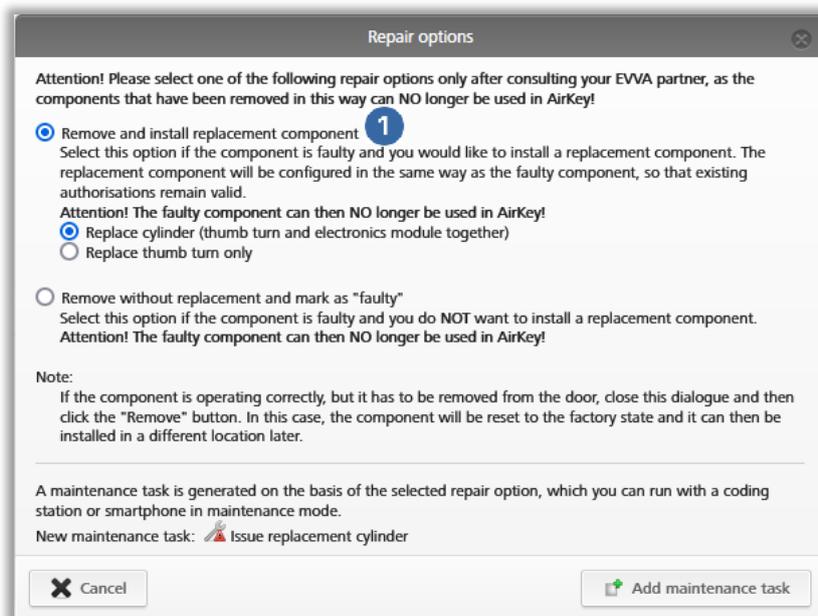


Figura 289: Opções de reparação

- > Clique em **Adicionar tarefa de manutenção**.

O estado do componente ❶ de bloqueio é atualizado e indicado como tarefa de manutenção ❷.

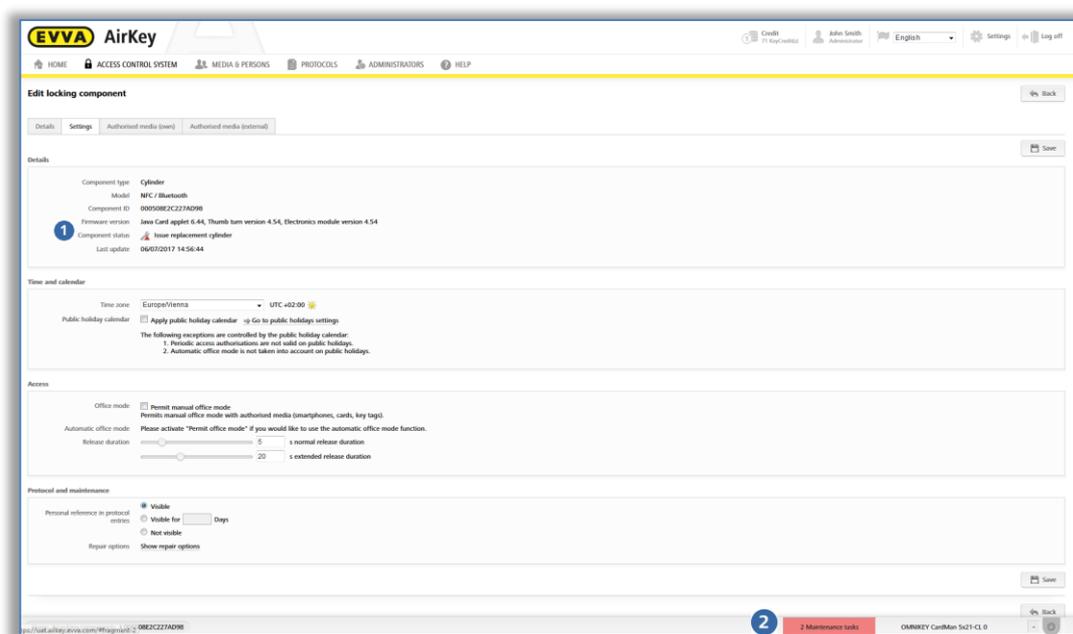


Figura 290: Estado do componente e tarefa de manutenção

Os preparativos para a emissão e instalação de um componente de bloqueio de substituição são concluídos na Administração online do AirKey. Para concluir todo o processo, tem de emitir e instalar o componente de bloqueio de substituição com o smartphone com autorização de manutenção ou com a estação de codificação opcional.



O componente a substituir pode ser atualizado, contanto que a instalação do componente de substituição fique totalmente concluída. Desta forma, assegura-se a integridade dos protocolos, caso ainda se tenha de estabelecer acessos entre instalar componentes de substituição e componentes de substituição instalados com sucesso.

No caso de uma substituição de componentes de bloqueio com Bluetooth, os componentes substituídos e os de substituição podem ser visualizados na lista dos componentes com Bluetooth dentro do alcance. O componente substituído, após a substituição bem-sucedida, tem de ser desligado da alimentação elétrica; só, então, depois, sairá da lista dos componentes com Bluetooth.

Emitir e instalar componente de bloqueio de substituição com o smartphone



É pré-requisito ter um smartphone com autorização de manutenção para cada sistema de controlo de acessos onde o componente de bloqueio de substituição deva ser emitido e instalado.

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente**, encoste o smartphone ao componente de bloqueio no estado de fábrica.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones **Android**): toque no caso do componente de bloqueio no estado de fábrica, que pretende adicionar no seu sistema de controlo de acessos, no menu contextual (:) e seleccione, depois, **Conectar**.
- > Se estabelecer a ligação por **Bluetooth** (em **iPhones**): deslize no caso do componente de bloqueio no estado de fábrica, que pretende adicionar no seu sistema de controlo de acessos, a designação "No estado de fábrica" para a esquerda e seleccione, depois, **Conectar**.
- > Depois da atualização, clique, nos detalhes do componente de bloqueio, em **Emitir cilindro de substituição**.
- > Na caixa de diálogo a seguir, toque no componente de bloqueio que pretende substituir e confirme com **Continuar**.
- > Ao utilizar a ligação via NFC, encoste novamente o smartphone ao componente de bloqueio no estado de fábrica. Ao utilizar a ligação via Bluetooth, seleccione, da lista dos componentes de bloqueio ao alcance, o componente de bloqueio no estado de fábrica.
- > Especifique se deve ser emitida uma tarefa de manutenção para posterior instalação.
- > Termine o processo com **Instalar mais tarde**, contanto que ainda tenha de montar o componente de bloqueio na porta ou seleccione **Concluir**, se a montagem na porta já tiver sido feita.
- > Atualize o componente de bloqueio depois de montado na porta.

Option

Emitir e instalar componente de bloqueio de substituição com a estação de codificação.

- > Coloque um componente de bloqueio de substituição no estado de

fábrica sobre a estação de codificação.

- > Selecione, à direita, em baixo, na janela de diálogo **Emitir cilindro de substituição** e o componente de bloqueio que pretende substituir.

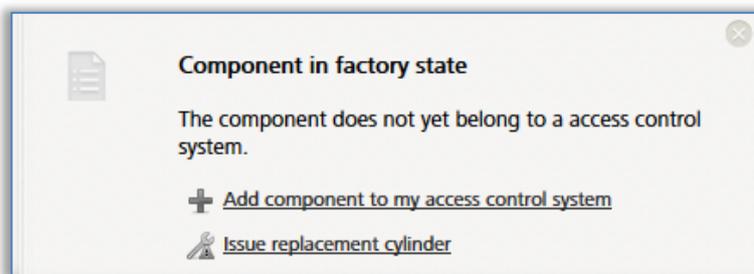


Figura 291: Componente no estado de fábrica – Emitir cilindro de substituição

- > Clique em **Continuar**.
- > Coloque o componente de bloqueio de substituição no estado de fábrica sobre a estação de codificação.
- > Remova o componente de bloqueio de substituição somente depois de surgir a respetiva mensagem de confirmação.
- > Especifique se deve ser emitida uma tarefa de manutenção para posterior instalação.
- > Termine o processo com **Instalar mais tarde**, contanto que ainda tenha de montar o componente de bloqueio na porta ou selecione **Concluir**, se a montagem na porta já tiver sido feita.
- > Atualize o componente de bloqueio depois de montado na porta.
- >
- > Se o componente de bloqueio de substituição possuir uma versão de firmware anterior, será executada a atualização do firmware durante este processo.



O componente de bloqueio substituído, depois deste processo, já não poderá ser utilizado. Execute esta função apenas se o componente de bloqueio tiver um defeito ou não precisar mais do mesmo.

8.8.2 Desinstalar o componente de bloqueio sem ser substituído e marcá-lo como "com defeito"

Se um componente de bloqueio com defeito não tiver de ser substituído, e não dever aparecer mais no sistema de controlo de acessos, este poderá ser desinstalado através das opções de reparação sem substituição.



Este componente de bloqueio não poderá, depois, ser novamente atualizado, sendo inutilizado.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**.

- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componente de bloqueio.
- > Clique, na lista geral, no componente de bloqueio que pretende editar.
- > No separador **Definições**, clique no bloco **Registo em protocolo e manutenção** no link **Mostrar opções de reparação** 1.

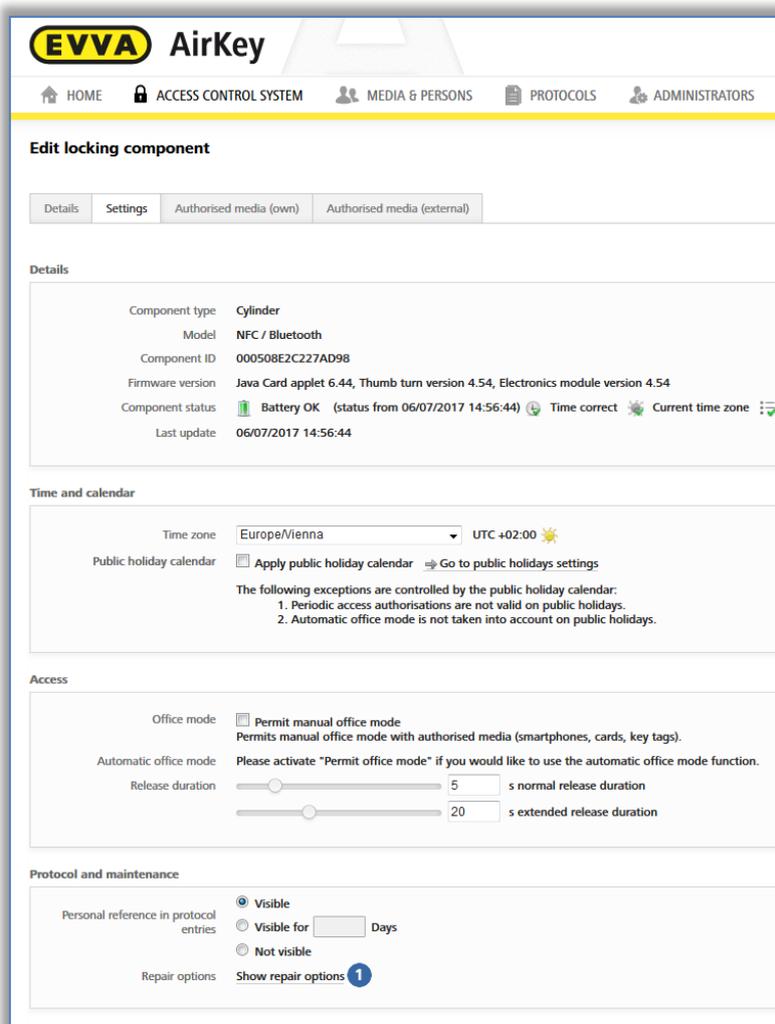


Figura 292: Editar componente de bloqueio – Opções de reparação

Abre-se a janela de diálogo "Opções de reparação".

- > Selecione **Desmonte sem substituição e marque como "defective"** 1.

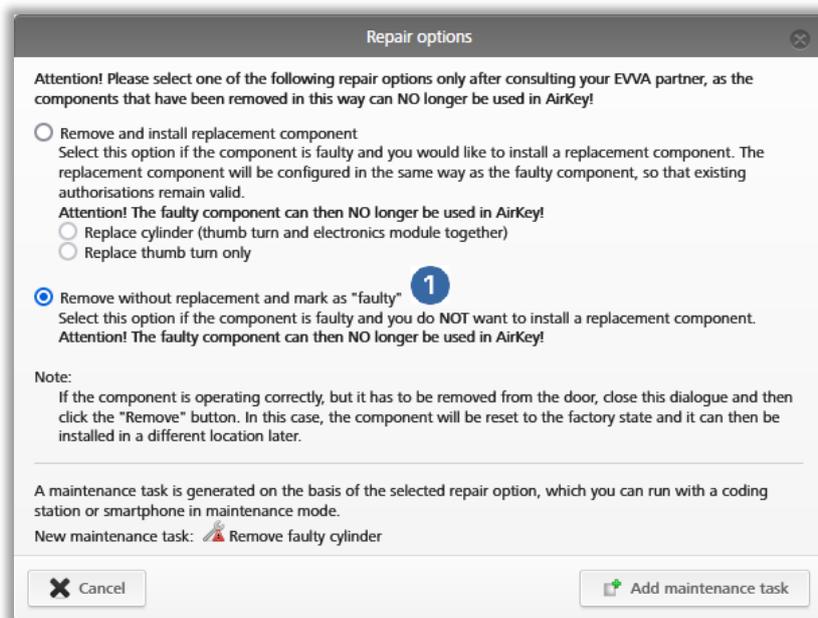


Figura 293: Opções de reparação

- > Clique em **Adicionar tarefa de manutenção**.

O estado do componente ❶ de bloqueio é atualizado e indicado como tarefa de manutenção ❷.

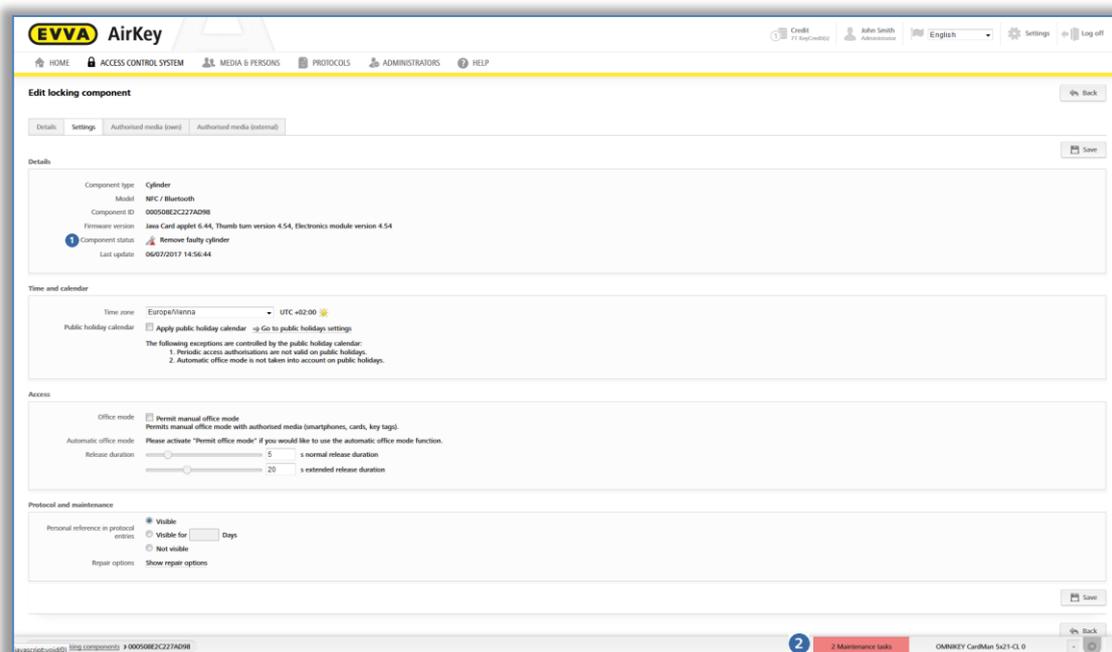


Figura 294: Estado do componente e tarefa de manutenção

Os preparativos para a desinstalação sem substituição de um componente de bloqueio com defeito são concluídos na Administração online do AirKey. Para concluir todo o processo, terá de concluir a desinstalação através do smartphone com autorização de manutenção ou na Administração online do AirKey.

8.8.3 Desinstalar o componente de bloqueio através do smartphone

Se ainda for possível uma atualização do componente de bloqueio com defeito, poderá executar a desinstalação de um componente de bloqueio com defeito sem substituição pelo smartphone. Um pré-requisito é o smartphone registado com autorização de manutenção ativa para este sistema de bloqueio AirKey.

- > Se estabelecer a ligação por **NFC** (em smartphones Android): toque no símbolo **Conecte com o componente**, encoste o smartphone ao componente de bloqueio que deverá ser desinstalado.
- > Se estabelecer a ligação por **Bluetooth** (em smartphones **Android**): no caso do componente de bloqueio que deve ser desinstalado, toque no menu contextual (:) e selecione **Conectar**.
- > Se estabelecer a ligação por **Bluetooth** (em **iPhones**): arraste, no caso do componente de bloqueio que deve ser desinstalado, a designação para a esquerda e selecione, depois **Conectar**.
- > Podem ser visualizados os detalhes do componente. Selecione **Remova o cilindro com defeito** ⓘ.

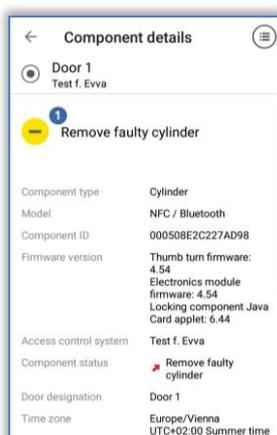


Figura 295: Desinstalar componente com defeito com o smartphone

- > Insira o visto na caixa de diálogo e confirme com **Concluir**.

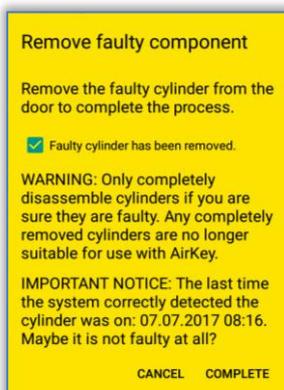


Figura 296: Desinstalar componente com defeito com o smartphone – Confirmação

Desta forma, o processo é concluído e o componente de bloqueio deixa de ser listado no sistema de controlo de acessos AirKey. O componente de bloqueio, agora, já não pode ser reutilizado.

8.8.4 Desinstalar o componente de bloqueio através da Administração online do AirKey

Se o componente de bloqueio não puder ser atualizado devido a um defeito, a desinstalação sem substituição tem de ser concluída na Administração online do AirKey.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede** – dependendo do componente que tenha sido marcado como tendo defeito.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → **Componente de bloqueio**.
- > Clique, na lista geral, no componente de bloqueio que pretende editar.
- > No separador **Definições**, clique no bloco **Registo em protocolo e manutenção** no link **Mostrar opções de reparação**.
- > Surge uma caixa de diálogo que informa que pode escolher entre três opções.

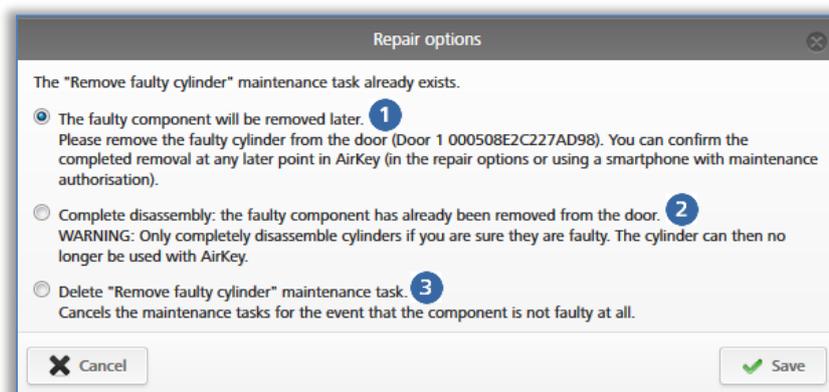


Figura 297: Desinstalar componente de bloqueio com defeito

- > Com a opção **O componente defeituoso será removidos posteriormente** ❶, mantém o estado atual do componente e o componente de bloqueio continua a fazer parte do sistema de controlo de acessos AirKey.
- > Com a opção **Desmontagem completa: O componente defeituoso já tenha sido removido da porta** ❷, o processo de desinstalação sem substituição de um componente de bloqueio com defeito é concluído e o componente de bloqueio é removido do sistema de controlo de acessos AirKey.
- > Com a opção **Apagar a tarefa de manutenção "Remove faulty cylinder"** ❸, a desinstalação sem substituição é revertida. Poderá encontrar mais informações sob a rubrica [Reverter tarefas de manutenção para opções de reparação](#).



O componente de bloqueio que foi desinstalado sem substituição, depois deste processo, já não pode ser reutilizado. Execute esta função apenas se o componente de bloqueio tiver um defeito ou não precisar mais do mesmo.

Quando pretender remover um componente de bloqueio funcional do seu sistema de controlo de acessos, consulte as instruções sob o ponto [Remover componente de bloqueio](#).

8.8.5 Reverter tarefas de manutenção para opções de reparação

Se tiver sido emitida uma tarefa de manutenção para um componente de bloqueio de substituição ou uma desinstalação sem substituição, esta tarefa de manutenção pode ser posteriormente eliminada.

- > Clique, na página inicial **Home**, no link **Tarefas de manutenção**.
- > Selecione da lista a tarefa de manutenção pretendida.
- > No separador **Definições**, clique no bloco **Registo em protocolo e manutenção** no link **Mostrar opções de reparação**.
- > Selecione, de acordo com a tarefa de manutenção aberta, se o componente de bloqueio de substituição (cilindro, puxador, leitor de parede) deve ser emitido ❶ mais tarde ou se a tarefa de manutenção deve ser eliminada ❷.

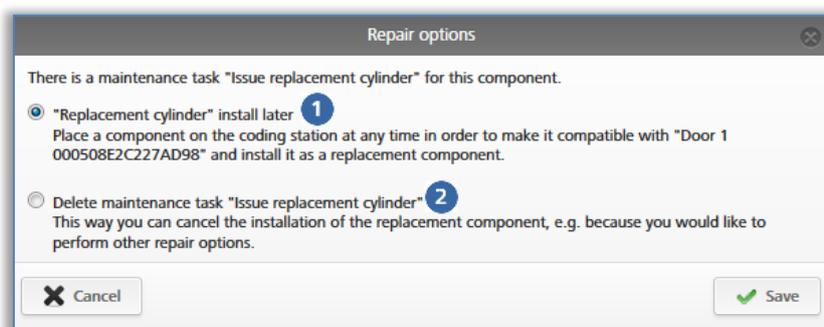


Figura 298: Eliminar tarefa de manutenção

- > Clique em **Assumir**.

A tarefa de manutenção será, assim, revertida. O estado do componente de bloqueio é atualizado em relação ao último estado do componente de bloqueio.



Se a tarefa de manutenção da opção de reparação já tiver sido concluída, esta não poderá ser mais revertida.



Utilize esta função também para reverter a tarefa de manutenção "Componente tem de ser removido", se o componente de bloqueio sem defeito tiver sido removido do sistema de controlo de acessos AirKey.

9 Meios de emergência

Um meio de emergência é um meio com autorização permanente ilimitada para todos os componentes de bloqueio de um sistema de controlo de acessos AirKey. Os meios de emergência têm aplicação em situações de emergência (p. ex, para uso dos bombeiros) e têm de ser mantidos em local seguro. Os meios de emergência obtêm acesso independentemente das horas no componente de bloqueio. Só a alimentação elétrica dos componentes de bloqueio é que tem de ser assegurada.

9.1 Emitir meios de emergência

Para emitir um meio de emergência, crie um meio sob a forma de cartão, porta-chaves, pulseira ou chave combinada – tal como descrito no capítulo [Criar cartões, porta-chaves e chaves combinadas](#) – e atribua ao meio de emergência autorizações de acesso permanente a todas as portas do sistema de controlo de acessos. Assegure-se de que os meios de emergência, no caso de expansão do sistema, sejam correspondentemente atualizados, para que, em caso de emergência, tenham igualmente acesso às novas portas adicionadas. Os meios de emergência têm também acesso a componentes de bloqueio com as horas erradas (p. ex., os cilindros param as horas quando as pilhas estão gastas). Poderá obter mais informações a respeito da atribuição e produção de autorizações em [Atribuir autorizações](#) e [Criar autorização](#).



Lembre-se que também os meios sob a forma de cartões, porta-chaves, pulseiras ou chaves combinadas podem avariar. Neste contexto, produza o respetivo número de meios de emergência em conformidade com o sistema de controlo de acessos.



Como meios de emergência, só os meios sob a forma de cartão, porta-chaves, pulseiras ou chave combinada são recomendados, uma vez que os smartphones não são adequados para este fim devido ao tempo limitado da bateria.

Para facilitar a administração dos meios de emergência, poderá trabalhar com áreas nas quais todas as portas do sistema de controlo de acessos estão incluídas. Atribua, portanto, aos meios de emergência uma autorização permanente ilimitada para estas áreas.

10 Media replacement

10.1 Troca de smartphone

A troca do smartphone facilita a mudança de um smartphone para outro smartphone, por exemplo, ao adquirir um novo dispositivo.

Durante a troca do smartphone, todas as autorizações e definições do AirKey (exceto o PIN e as definições locais do modo mãos-livres) do smartphone já existente são transferidas para o novo smartphone.

A troca pode ser efetuada tanto de Android para iOS como vice-versa.

A troca pode ser iniciada por um administrador na administração online do AirKey ou diretamente a partir do smartphone.

O smartphone "antigo" é designado como **meio de origem** e o "novo" smartphone é designado como **meio de destino**.



O meio de origem é automaticamente desativado após a conclusão da ação de troca. Se o meio de origem já não estiver funcional ou disponível, a lista negra dos componentes de bloqueio afetados tem de ser atualizada. Só depois disso é que a segurança do sistema é restabelecida.



Se, no âmbito da ação de troca, também forem transferidas autorizações para o meio de destino, um KeyCredit será debitado do crédito existente. Se não houver KeyCredits disponíveis, a troca só pode ser concluída quando um crédito estiver novamente disponível.

10.1.1 Iniciar a troca como proprietário do smartphone

Se o meio de origem ainda estiver a funcionar, ainda estiver registado e não estiver desativado, a troca do smartphone pode ser iniciada diretamente através do meio de origem.

- > Inicie a aplicação AirKey no smartphone antigo.
- > No menu, toque em **Definições** → **Troca de smartphone**.
- > Confirme a caixa de diálogo com **OK**.

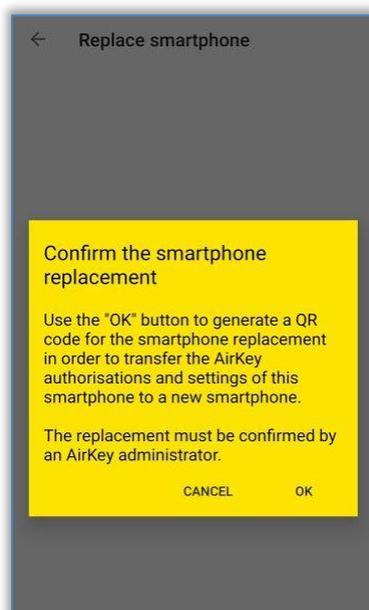


Figura 299: Confirmar a troca do smartphone

- > Um código QR com um texto de ajuda é exibido no meio de origem.

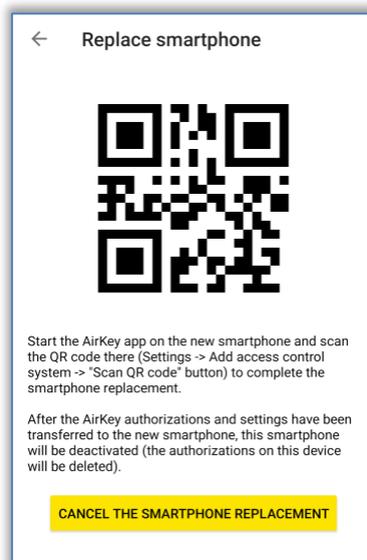


Figura 300: Código QR para a troca do smartphone

Os passos no meio de origem estão concluídos. O meio de origem pode continuar a ser utilizado como habitualmente até a ação de troca estar concluída. O código QR é válido durante 30 dias e é apresentado novamente ao tocar em **Definições** → **Troca de smartphone**.

Uma vez que, na troca do smartphone, é criado um novo smartphone e, dependendo das autorizações transmitidas, também são debitados KeyCredits, a troca tem de ser confirmada por um administrador dentro da administração online do AirKey.

- > Inicie sessão na administração online do AirKey.
- > Na página inicial, clique no botão **Operações de troca do smartphone em curso**.

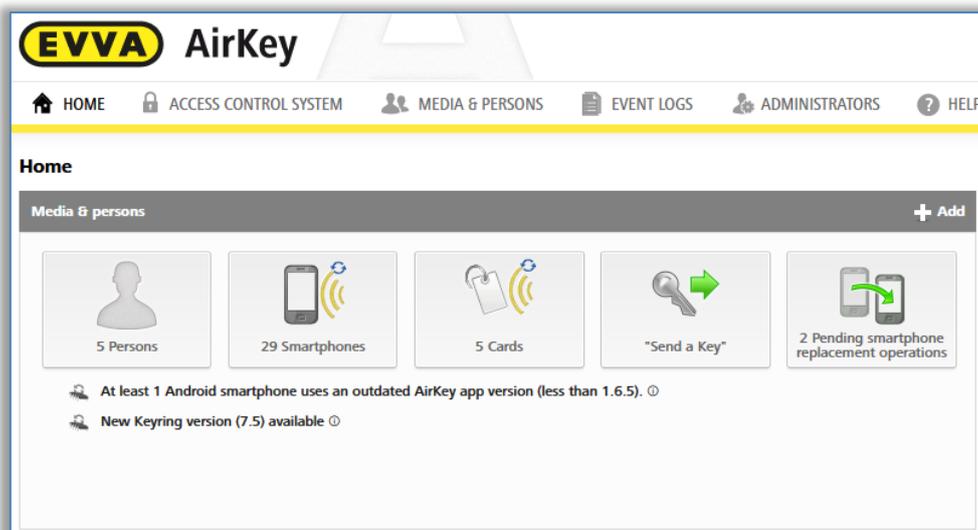


Figura 301: Página inicial – operações de troca do smartphone em curso

- > Na coluna "Ação", a troca pode ser confirmada através do visto verde ou recusada através do "X" vermelho.

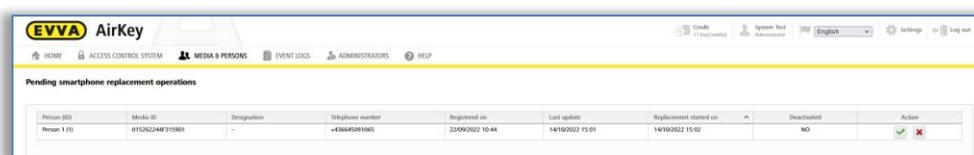


Figura 302: Operações de troca do smartphone em curso

Após a confirmação do administrador, a troca pode ser concluída através da leitura do código QR no meio de destino. Se a troca for recusada pelo administrador, a troca do smartphone é cancelada e o código QR deixa de ser válido e é eliminado. Se o código QR for lido no meio de destino antes de um administrador confirmar a troca, aparece uma mensagem de erro correspondente.



Figura 303: Falha na troca do smartphone



Os administradores também podem ativar a confirmação automática para as ações de troca do smartphone nas definições da administração online do AirKey (ver capítulo [Informações gerais](#)). Desta forma, qualquer troca de smartphone iniciada através de um smartphone é imediatamente confirmada, se houver crédito suficiente. Lembre-se de que em cada troca do smartphone, durante a qual são transferidas autorizações, é debitado um KeyCredit.

Para digitalizar o código QR com um meio de destino ainda não registado, siga os seguintes passos:

- > Inicie a aplicação AirKey.
- > Confirme o EULA.
- > Toque em **Ler código QR** e leia o código QR do meio de origem.

Para fazer a leitura do código QR com um meio de destino já registado no AirKey, siga os seguintes passos:

- > Inicie a aplicação AirKey.
- > No menu, toque em **Definições** → **Adicionar sistema de controlo de acessos**.
- > Toque em **Ler código QR** e leia o código QR do meio de origem.

A troca do smartphone foi concluída e o meio de destino foi registado com sucesso com as autorizações e definições do meio de origem AirKey. O meio de origem é automaticamente desativado após a troca bem-sucedida.



Se o meio de origem se encontrar em mais do que um sistema de controlo de acessos, a troca é iniciada em simultâneo em todos os sistemas de controlo de acessos. Isto significa que vários administradores podem ter de confirmar a troca na administração online do AirKey. Apenas são transferidas as autorizações e definições do AirKey para os sistemas de controlo de acessos para o meio de destino em que os administradores confirmaram a troca.

10.1.2 Iniciar a troca como administrador

Se o meio de origem já não estiver disponível ou já não estiver operacional, a troca também pode ser iniciada como administrador.

- > Na página inicial **Home**, seleccione botão **Smartphones**.
- > Em alternativa, seleccione, no menu principal, **Meios e pessoas** → **Meios**.
- > Seleccione na lista de meios o smartphone que deve ser trocado.
- > Clique em **Mais... 1** → **Troca de smartphone**.

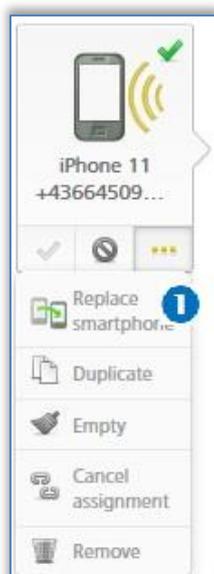


Figura 304: Troca de smartphone

- > Abre-se uma caixa de diálogo, na qual tem de ser introduzido o número de telefone do meio de destino. O número de telefone do meio de origem é assumido automaticamente.

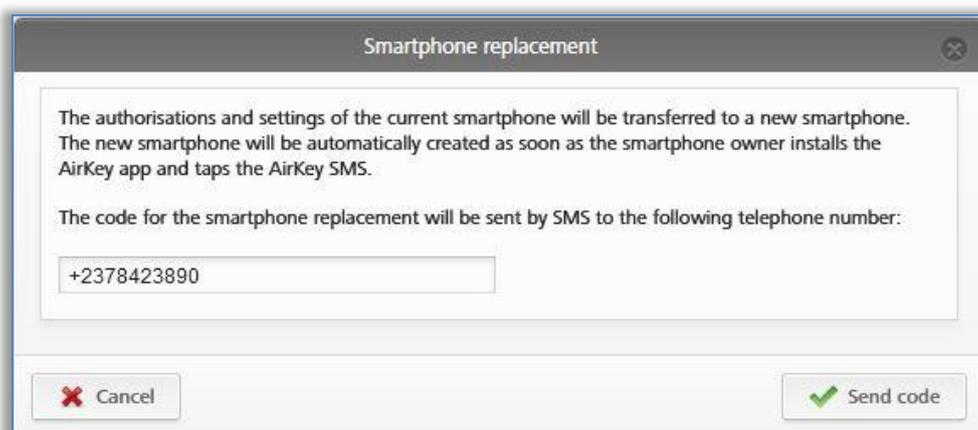


Figura 305: Troca de smartphone

- > Verifique se o número de telefone está correto e confirme com **Enviar código**.
- > É enviada uma SMS do AirKey com um link de registo para o número de telefone indicado do meio de destino.

A troca do smartphone ainda tem de ser concluída no meio de destino:

- > Abra a SMS com o link de registo no meio de destino.
- > Toque no link de registo e siga as instruções.

A troca do smartphone foi concluída e o meio de destino foi registado com sucesso com as autorizações e definições do meio de origem AirKey. O meio de origem é automaticamente desativado após a troca bem-sucedida.

O link de registo na SMS é válido por 30 dias. Se o link de registo não tiver chegado por SMS, pode ser enviado novamente por SMS:

- > Clique por baixo do smartphone em **Mais... 1** → **Troca de smartphone**.

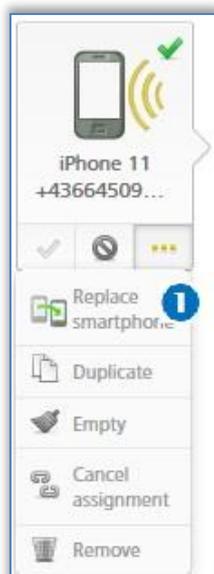


Figura 306: Troca de smartphone

- > Abre-se uma caixa de diálogo, onde o número de telefone pode ser verificado e alterado novamente.

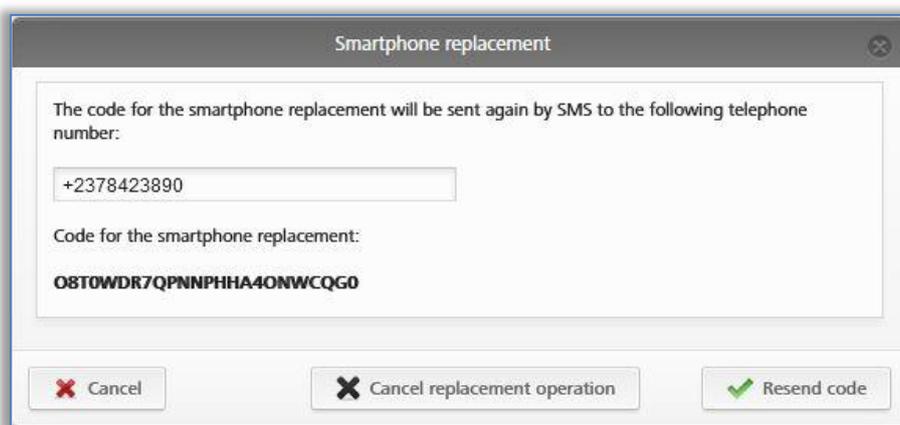


Figura 307: Troca de smartphone - Reenviar código

- > Clique em **Reenviar código**.

Neste diálogo, a troca também pode ser cancelada, caso já não seja necessária.



Se o meio de origem se encontrar em mais do que um sistema de controlo de acessos, a troca tem de ser iniciada por um administrador de cada sistema de controlo de acessos. Da mesma forma, também é enviada uma SMS com um link de registo para cada sistema de controlo de acessos.

11 Trabalhar com vários sistemas de bloqueio AirKey

No capítulo seguinte, poderá encontrar indicações sobre como trabalhar com vários sistemas de bloqueio AirKey.

11.1 Ativar componentes de bloqueio para outros sistemas de bloqueio

Poderá ativar um componente adicionado no seu sistema de controlo de acessos para outro sistema de controlo de acessos. No outro sistema de controlo de acessos, podem ser igualmente atribuídas autorizações a este componente de bloqueio. Cada componente de bloqueio pode ser ativado para partilha num máximo de 250 sistemas de bloqueio.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componente de bloqueio.
- > Clique, na lista geral, na designação de porta desse componente de bloqueio que pretende ativar.

No bloco **Partilhas** dos detalhes do componente de bloqueio, são listadas as ativações já concedidas.

- > Clique em **Adicionar partilha**.

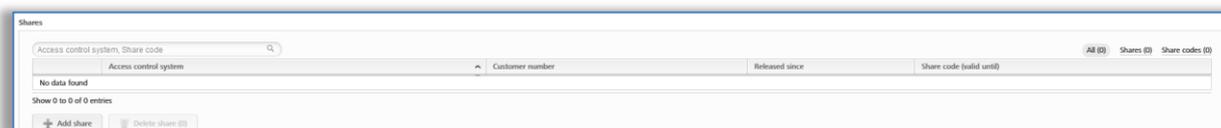


Figura 308: Ativar componente de bloqueio para partilha

- > É gerado um código de ativação de 12 caracteres.

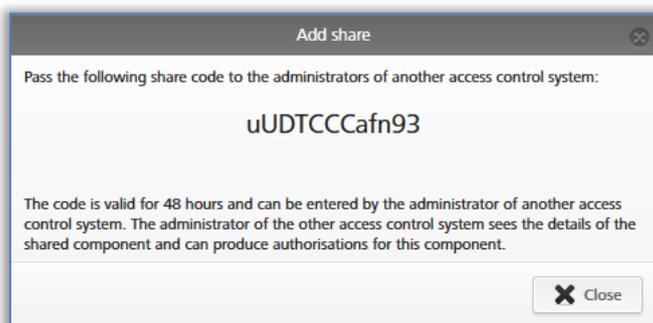


Figura 309: Adicionar partilha

- > Comunique este código de ativação para partilha ao administrador de outro sistema de controlo de acessos.



O código de ativação para partilha permanece válido 48 horas.



Podem ser gerados, para um componente de bloqueio, vários códigos de ativação para partilha. Estes são apresentados na lista de ativações para partilha do componente de bloqueio.

É feito um registo na lista de ativações para partilha do componente de bloqueio. Aí, pode ser consultado o código de ativação para partilha e a sua validade.

11.2 Adicionar componente de bloqueio de outros sistemas de bloqueio

Se foi ativado para si um componente de bloqueio de um outro sistema de controlo de acessos, terá de adicioná-lo ao seu sistema de controlo de acessos.

- > Clique, na página inicial **Home**, na barra cinzenta **Sistema de controlo de acessos**, em Adicionar → Adicionar componente de bloqueio 1.



Figura 310: Adicionar componente de bloqueio – barra cinzenta

- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → Componente de bloqueio.
- > Clique em **Adicionar componente de bloqueio** 1.

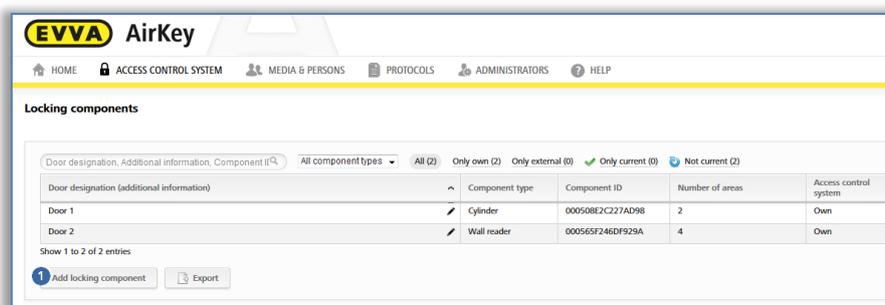


Figura 311: Adicionar componente de bloqueio

- > Selecione como tipo **Componente de bloqueio partilhado** 1.
- > Clique em **Continuar**.

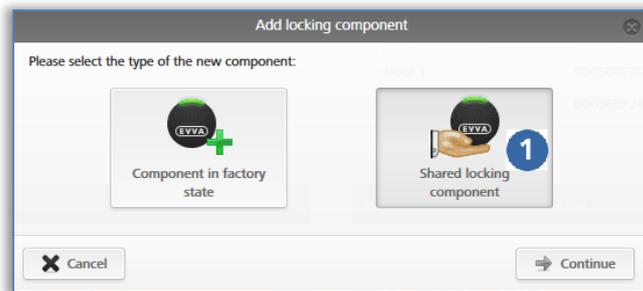


Figura 312: Adicionar componente de bloqueio ativado para partilha

- > Introduza o código de ativação para partilha do outro sistema de controlo de acessos para adicionar o componente de bloqueio.

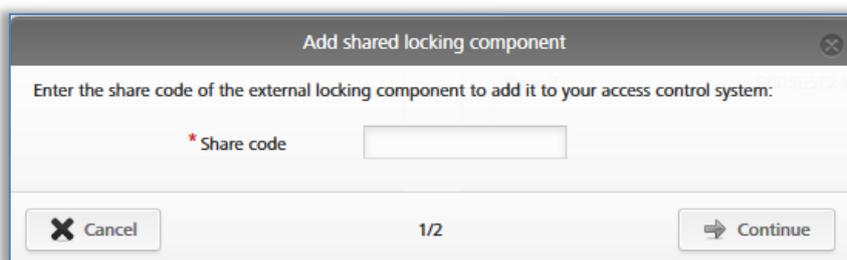


Figura 313: Adicionar componente de bloqueio ativado para partilha

Se o código de ativação para partilha introduzido estiver errado, receberá uma mensagem de erro.

Se o código de ativação para partilha introduzido estiver correto, poderá inserir os ajustes seguintes:

- > Designação de porta alternativa ①
- > Sob a proteção de dados, a referência pessoal nos registos protocolares para o proprietário do componente de bloqueio pode estar visível ou invisível ②.

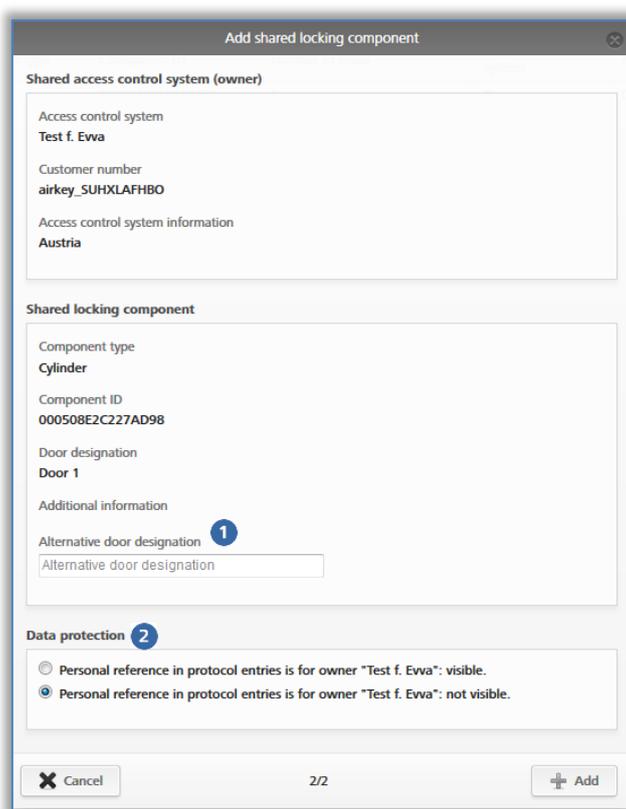


Figura 314: Adicionar componente de bloqueio ativado para partilha

- > É criada uma tarefa de manutenção.
- > Atualize o componente de bloqueio através de um smartphone com autorização de manutenção ou através de estação de codificação opcional.
- > Desta forma, a tarefa de manutenção é removida da lista e a ativação para partilha é atualizada.
- > Se o componente de bloqueio ativado para partilha tiver sido adicionado, o componente de bloqueio irá aparecer na coluna "Sistema de controlo de acessos" com o atributo "de terceiros" na lista dos componentes de bloqueio. O cliente que tiver adicionado o componente de bloqueio, no separador "Detalhes", pode editar a designação de porta em alternativa e atribuir o componente de bloqueio a uma área. No separador "Definições", o botão de opção pode ser alterado no bloco "Proteção de dados" para escolher, na referência pessoal nos registos protocolares para o proprietário do componente de bloqueio, se deverá ficar "visível" ou "invisível". Além disso, a referência pessoal pode ser definida nos registos protocolares no bloco "Registo em protocolo e manutenção" para o sistema de controlo de acessos ativado para partilha. Adicionalmente, as autorizações de acesso para o componente de bloqueio ativado para partilha podem ser atribuídas.



Um componente de bloqueio de terceiros não pode ser ativado para partilha para outros sistemas de bloqueio.

11.3 Atribuir autorizações a componentes de bloqueio ativados para partilha

Nesse sistema de controlo de acessos AirKey ao qual foi adicionado um componente de bloqueio ativado para partilha, o processo para a atribuição de autorizações difere ligeiramente do processo do proprietário do componente de bloqueio. Siga os passos se tiver adicionado um componente de bloqueio ativado para partilha ao seu sistema de controlo de acessos.

- > Selecione, na página inicial **Home**, a caixa de seleção **Smartphones** ou **Cartões**.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas** → **Meios**.
- > Clique, na lista geral, no meio desejado.
- > Contanto que o meio esteja atribuído a uma pessoa, aparece a vista geral das autorizações do meio.
- > Selecione, por baixo da caixa de todos os componentes de bloqueio e áreas, o separador **Externo** , para poder visualizar todos os componentes de bloqueio adicionados de sistemas de bloqueio de terceiros.

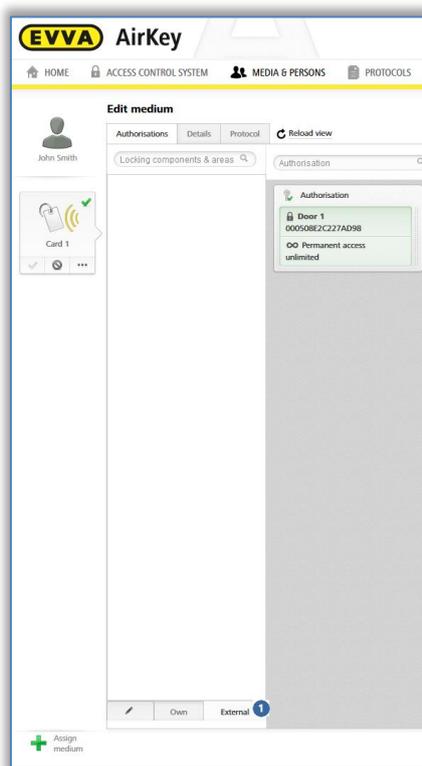


Figura 315: Autorização de componente de bloqueio ativado para partilha

- > Arraste (Drag & Drop) o botão com a porta ativada para partilha selecionada para a superfície cinzenta. Só quando mover a porta selecionada / área selecionada para o campo central, é que aparecem os tipos de acesso.
- > Selecione o tipo de acesso pretendido, arrastando por Drag & Drop a porta selecionada / a área selecionada para o campo correspondente.

- > Conclua a autorização, descontando um KeyCredit. Poderá obter mais informações a respeito da produção de autorizações em [Criar autorização](#). O KeyCredit é debitado dos créditos do seu sistema de controlo de acessos, mas não do outro sistema de controlo de acessos.

11.4 Consultar autorizações de componentes de bloqueio ativados para partilha

Se tiver partilhado um componente de bloqueio com outro cliente, também poderá consultar os meios do outro cliente que possuem autorização para o componente de bloqueio ativado para partilha.

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → **Componente de bloqueio**.
- > Clique, na lista geral, no componente de bloqueio cujos detalhes pretende consultar.
- > Clique em **Meio autorizado (externo)** , para obter uma vista geral de todos os meios de terceiros que têm uma autorização neste componente de bloqueio.

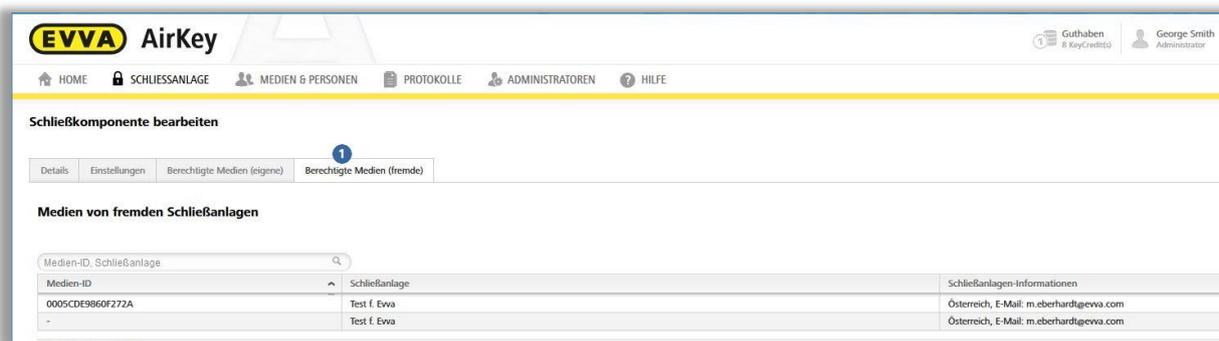


Figura 316: Meios autorizados (de terceiros)

11.5 Cancelar a partilha de um componente de bloqueio

Poderá voltar a cancelar a partilha concedida por si de um componente de bloqueio. Para o efeito, proceda da seguinte forma:

- > Selecione, na página inicial **Home**, a caixa de seleção **Cilindro** ou **Leitor de parede**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos** → **Componente de bloqueio**.
- > Clique, na lista geral, no componente de bloqueio cuja partilha pretende cancelar.

Selecione, no separador **Detalhes**, no bloco **Ativação de partilha** a respetiva ativação de partilha e clique em **Apagar partilha** .

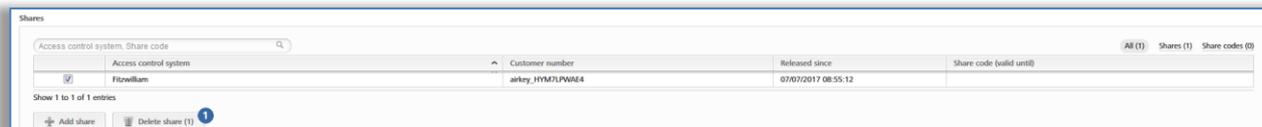


Figura 317: Bloco "Ativação de partilha" – Eliminar partilha

- > Confirme a pergunta de segurança com **Apagar partilha**.

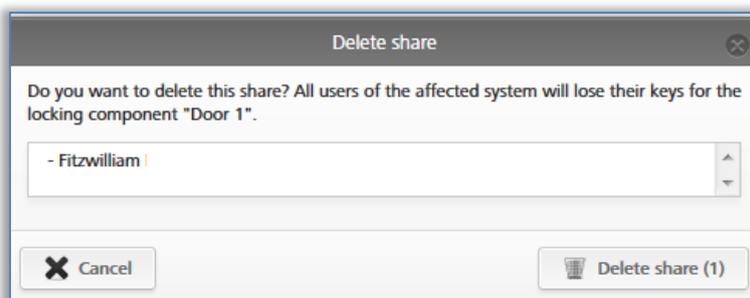


Figura 318: Eliminar partilha

Desta forma, o componente de bloqueio é removido o sistema de controlo de acessos de outro cliente. É criada uma tarefa de manutenção.

- > Atualize o componente de bloqueio para o qual a partilha foi cancelada através de um smartphone com autorização de manutenção ou da estação de codificação opcional. O estado do componente de bloqueio, depois da atualização, voltou a ficar atual.



Atenção: Só depois de o componente de bloqueio ter sido atualizado é que os meios do outro cliente deixa de poder bloquear.

As partilhas dos componentes de bloqueio só podem ser eliminadas dos sistemas de bloqueio onde as partilhas estavam ativadas.

Se o código de ativação da partilha não chegou a ser utilizado e é eliminado conforme descrito neste capítulo, o componente de bloqueio não tem de ser atualizado.

11.6 Utilizar o smartphone em vários sistemas

Poderá registar o seu smartphone em vários sistemas de bloqueio e utilizá-lo como meio.

- > Na aplicação AirKey, abra o menu principal e selecione **Definições** → **Adicionar sistema de controlo de acessos** 1.

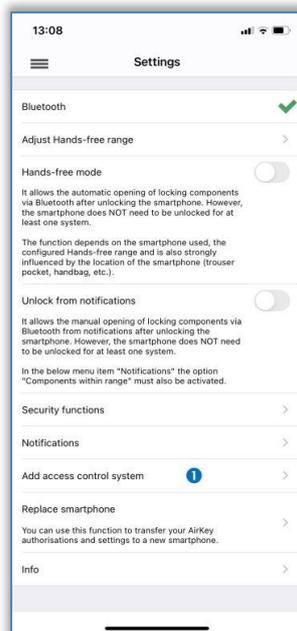


Figura 319: Adicionar sistema de chave mestra

- > No sistema Android, a caixa de diálogo para a introdução do código de registo é automaticamente exibida. Em sistemas iOS, toque em **Código de registo já recebido** para saltar a introdução do número de telefone e para aceitar a introdução do código de registo.
- > Introduza o código de registo, que recebeu do administrador do sistema de controlo de acessos e toque em **Registar**.
- > Se tiver activado um código PIN para a aplicação AirKey, deve introduzi-lo e confirmá-lo.

O smartphone está, assim, registado no outro sistema de controlo de acessos.



Desde que o código de registo para um outro sistema de controlo de acessos tenha sido enviado por SMS, é suficiente tocar no link da SMS para iniciar e executar automaticamente o registo.



Fazendo movimentos de arraste no smartphone, poderá seleccionar entre vistas gerais de autorizações de cada sistema de controlo de acessos e a vista geral de todas as autorizações.



A EVVA recomenda a atribuição de um PIN. Este é utilizado como mais um nível de segurança e pode ser, posteriormente, ativado ou desativado. Poderá encontrar mais informações a este respeito em [Ativar PIN](#).



O botão **Ler o código QR** só é necessário em combinação com a troca do smartphone. Poderá encontrar detalhes sobre a troca do smartphone no capítulo [Troca de smartphone](#).

12 AirKey Cloud Interface (API)

A AirKey Cloud Interface é uma interface ([API](#)) para sistemas de terceiros, que tem por base o [REST](#). A interface permite controlar determinadas funções do AirKey através de um software de terceiros (p. ex., sistema de reserva ou check-in).

O software de terceiros tem de estar associado à Administração online do AirKey e, em especial, ajustado, para que este possa enviar os comandos necessários e editar as respetivas respostas.

Poderá encontrar a amplitude das possíveis funções e respetivos comandos na [documentação da API](#) (em inglês). O seu integrador ou programador dos softwares de terceiros trata da implementação.



Experimente a função da AirKey Cloud Interface a partir da [Demo da EVVA AirKey Cloud Interface](#).



Certifique-se de que tem saldo suficiente para utilizar a AirKey Cloud Interface. Neste caso, será melhor utilizar os KeyCredits Unlimited. Se o saldo estiver esgotado ou quase a esgotar-se, todos os administradores do sistema de bloqueio AirKey são informados através de uma notificação por e-mail. Esta notificação por e-mail é apenas enviada aos administradores que tiverem ativado a opção **Gostaria de receber informações importantes da EVVA (p. ex., sobre um pequeno crédito de KeyCredits) por e-mail (recomendado)**. Poderá, a qualquer momento, editar esta notificação por e mail para um (ver o capítulo [Editar administrador](#)).

12.1 Ativação da AirKey Cloud Interface



Para a ativação da AirKey Cloud Interface são necessários, pelo menos, 350 KeyCredits. Utilize, para isso, o seu saldo de KeyCredits existente ou o respetivo cartão de raspadinha **KeyCredits AirKey Cloud Interface**.

- > Clique na área de **Definições**, na tab **Geral**, e em seguida **Ativar API**.

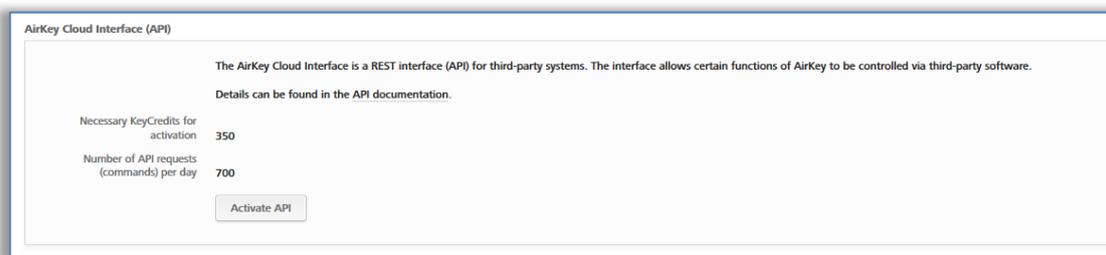


Figura 320: Definições gerais – AirKey Cloud Interface (API)

- > Contanto que exista saldo suficiente, confirme a caixa de diálogo novamente com **Ativar API**. Se o saldo não for suficiente, esta situação será indicada por uma mensagem. Poderá carregar o saldo diretamente através de um link.

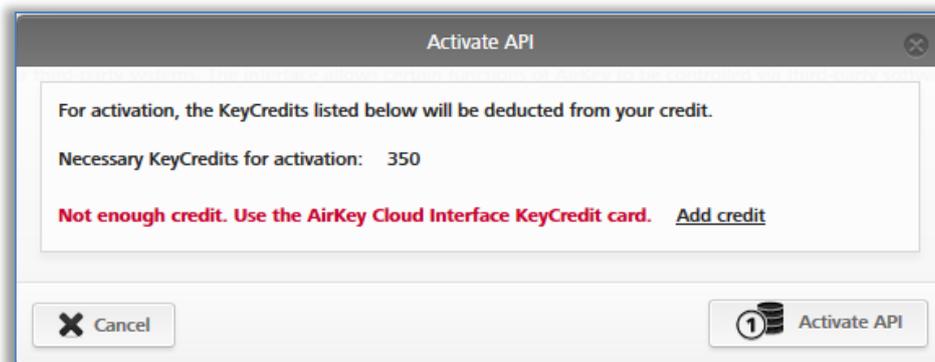


Figura 321: Ativar API

A AirKey Cloud Interface é, assim, ativada. A AirKey Cloud Interface tem de ser ativada apenas uma vez por sistema de bloqueio para se poder utilizar.

Após a ativação, receberá as informações sobre o "Endpoint" (aqui, os comandos da API têm de ser enviados) e sobre o limite de "Requests" da API (número dos possíveis comandos da API por dia). Um "Request" da API é um comando enviado pelo software de terceiros ao sistema AirKey.



O limite de "Requests" da API é repostado diariamente às 00:00 horas (UTC). Se o limite de "Requests" da API for excedido, todos os administradores do sistema de bloqueio AirKey são informados através de uma notificação por e-mail. Esta notificação por e-mail é apenas enviada aos administradores que tiverem ativado a opção **Gostaria de receber informações importantes da EVVA (p. ex., sobre um pequeno crédito de KeyCredits) por e-mail (recomendado)**. Poderá, a qualquer momento, editar esta notificação por e mail para um (ver o capítulo [Editar administrador](#)).



Se os "Requests" da API por dia não forem suficientes no seu caso concreto, entre em contacto com a [Assistência da EVVA](#).

12.2 Gerar chave para a API

A comunicação entre o AirKey e o software de terceiros é protegido por uma chave da API. Só quem conhece esta chave da API pode enviar comandos pela AirKey Cloud Interface ao sistema de bloqueio. Cada sistema de bloqueio com a AirKey Cloud Interface ativada utiliza as suas próprias chaves da API.

As ações que são executadas pela AirKey Cloud Interface são igualmente registadas no protocolo do sistema de bloqueio AirKey. Como administrador, é utilizada, neste caso, a primeira parte da chave da API, a ID da chave da API.

Após a ativação, poderá gerar as chaves da API necessárias para a comunicação.

- > Clique na área de **Definições**, na tab **Geral**, em **Gerar chave para a API**.

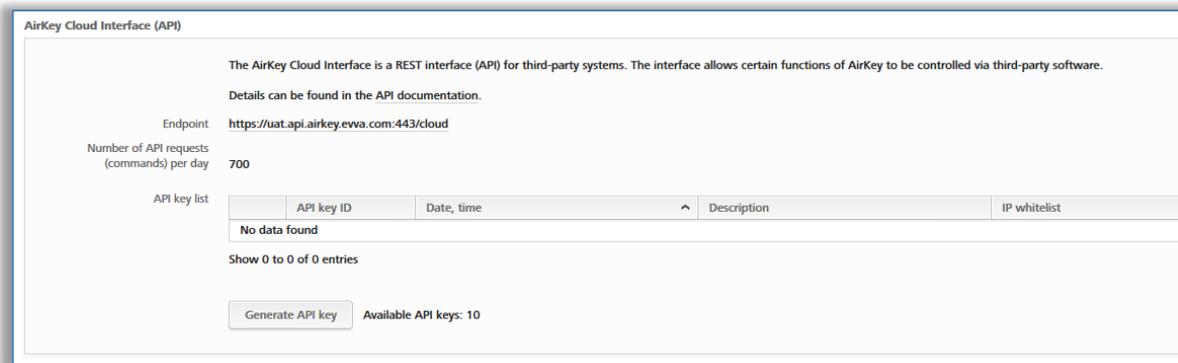


Figura 322: Gerar chave para a API

- > Confirme a caixa de diálogo novamente com **Gerar chave para a API**.

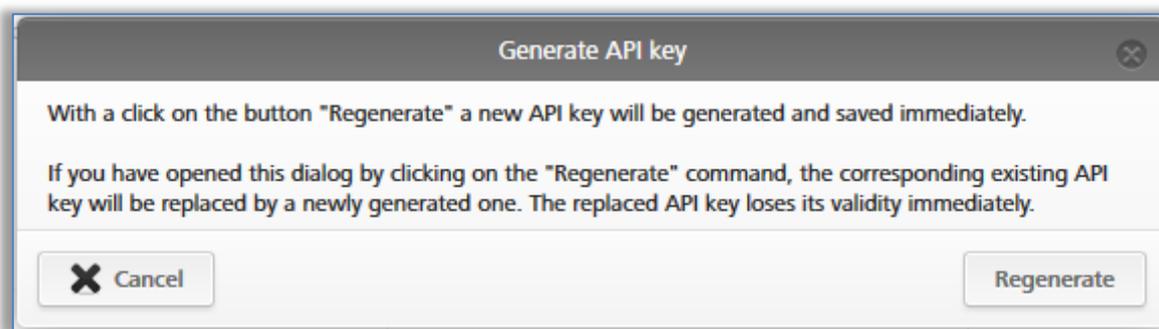


Figura 323: Gerar chave para a API, caixa de diálogo

- > Insira uma descrição, por exemplo, o nome do software de terceiros e restrinja opcionalmente os endereços IP permitidos para o envio de "Requests" da API através da lista de endereços IP permitidos.

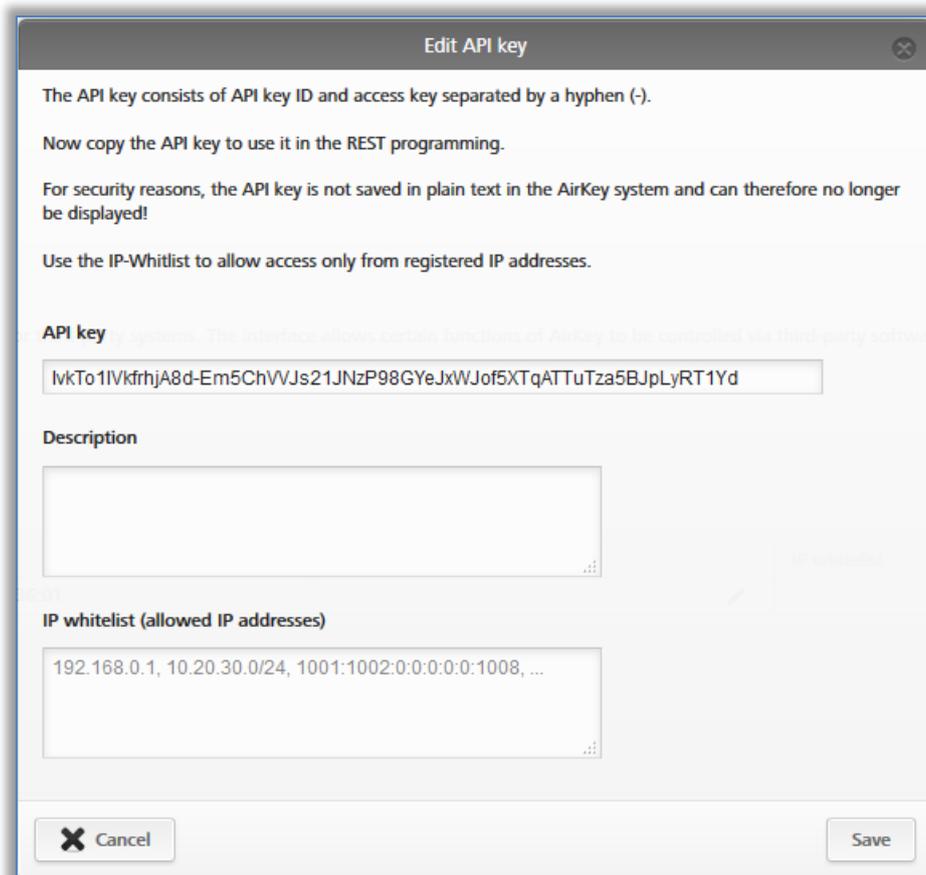


Figura 324: Gerar chave para a API, detalhes



Utilize a função da lista de endereços IP permitidos para aumentar a segurança. Registre apenas os endereços IP para cada chave da API, que podem enviar "Requests" da API ao seu sistema de bloqueio AirKey.

Na lista de endereços IP permitidos, incluem-se tanto os endereços IP de formato IPv4 como de formato IPv6. Utilize como separador entre os vários endereços IP a vírgula (,).



Por motivos de segurança, a chave da API só pode ser visualizada uma vez. Guarde-a em local seguro e utilize-a no seu software de terceiros.

- > Guarde os dados introduzidos para a chave da API clicando em **Guardar**.



Por cada sistema de bloqueio AirKey, podem ser geradas até 10 chaves para a API. Desta forma, vários softwares de terceiros podem comandar o sistema de bloqueio AirKey.

A chave da API gerada está listada nas definições gerais e pode ser editada posteriormente.

12.3 Editar chave da API

A descrição e a lista de endereços IP permitidos das chaves da API existentes podem ser editadas posteriormente em **Definições**, na tab **Geral**, por meio do símbolo do lápis. Adicionalmente, para cada chave individual da API, estão disponíveis as funções **Regenerar**, **Eliminar** e **Desativar** ou **Reativar**.



API key ID	Date, time	Description	IP whitelist	Regenerate	Delete	Deactivate
lkTo1VkrfhjA8d	10/05/2019 09:36:01			Regenerate	Delete	Deactivate
I440VdIP2kjfjNPM	10/05/2019 10:15:50	3rd party		Regenerate	Delete	Deactivate

Figura 325: Editar chave da API

12.3.1 Regenerar chave da API

Neste caso, uma chave da API já existente será substituída por uma nova chave. A chave da API substituída perderá a validade.

- > Clique na área de **Definições**, na tab **Geral**, na lista das chaves da API, em **Regenerar** ①.
- > Todos os passos a executar são idênticos a [Gerar chave da API](#).

12.3.2 Eliminar chave da API

Neste caso, uma chave da API já existente será eliminada. Esta será removida da lista das chaves da API e perderá a sua validade. A eliminação de chaves da API aumenta o número de chaves da API disponíveis de forma correspondente.

- > Clique na área de **Definições**, na tab **Geral**, na lista das chaves da API, em **Eliminar** ②.
- > Confirme a caixa de diálogo com **Eliminar** para eliminar de forma permanente a chave da API.



Figura 326: Eliminar chave da API

12.3.3 Desativar e ativar chave da API

Aqui, uma chave da API já existente e ativa é desativada, ou uma chave da API desativada é reativada. Uma chave da API desativada fica inválida e nenhum "Request" pode ser enviado ao sistema de bloqueio AirKey. A chave da API, assim como a sua descrição e a lista de endereços IP permitidos, não se altera só por ser desativada ou reativada.

- > Clique na área de **Definições**, na tab **Geral**, na lista das chaves da API, em **Desativar**  ou **Ativar**.
- > Confirme a caixa de diálogo com **Desativar** ou **Ativar** para concluir o processo.

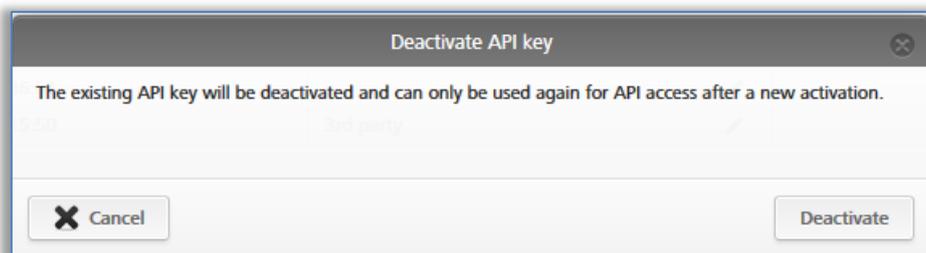


Figura 327: Desativar a chave da API



Figura 328: Ativar a chave da API

12.4 AirKey Cloud Interface – Ambiente de teste

O ambiente de teste dá-lhe a possibilidade de experimentar a AirKey Cloud Interface (API) com dados de teste, antes da ativação, num ambiente protegido.

Isto serve, sobretudo, como suporte para os integradores ou programadores de sistemas de terceiros no processo da integração da AirKey Cloud Interface. O ambiente de teste também está disponível mesmo se a AirKey Cloud Interface ainda não tenha sido ativada.



No ambiente de teste, não são debitados KeyCredits. Da mesma forma, também não são enviados SMS no âmbito do ambiente de teste.



O ambiente de teste da AirKey Cloud Interface (API) é acessível através de um "Endpoint" próprio (aqui, os comandos da API têm de ser enviados).
Endpoint: <https://integration.api.airkey.evva.com:443/cloud>

12.4.1 Gerar dados de teste

Na primeira vez que se utiliza o ambiente de teste, é necessário gerar, primeiro, os dados de teste.



Para gerar os dados de teste, tem de ser gerada, anteriormente, uma chave para a API.

- > Clique na área de **Definições**, na tab **Geral**, em **Gerar dados de teste**.

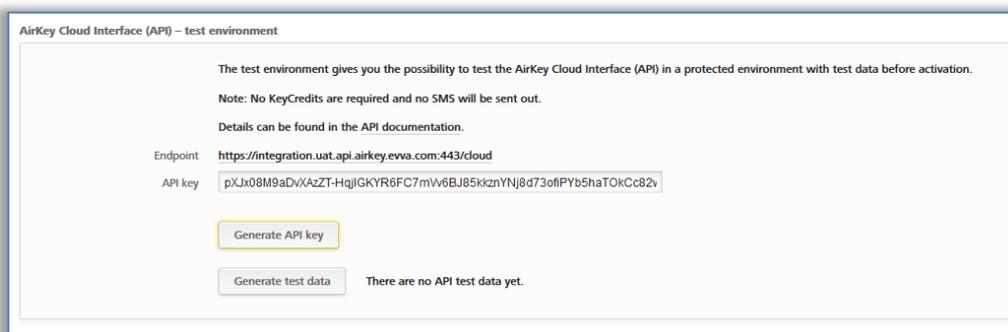


Figura 329: Gerar dados de teste

Os dados de teste são, assim, gerados. Com os dados de teste, é possível experimentar cada "Request" da API a partir da [Documentação da API](#). Os dados de teste têm de ser gerados apenas uma vez.

12.4.2 Gerar chave para a API

É necessária uma chave da API para a comunicação com o Ambiente de teste da AirKey Cloud Interface (API). Sem esta chave da API, nenhum "Request" pode ser enviado ao ambiente de teste. Comparativamente à AirKey Cloud Interface verdadeira, a chave da API do ambiente de teste é exibida em texto simples.

- > Clique na área de **Definições**, na tab **Geral**, na área **AirKey Cloud Interface (API) - Ambiente de teste**, em **Gerar chave para a API**.

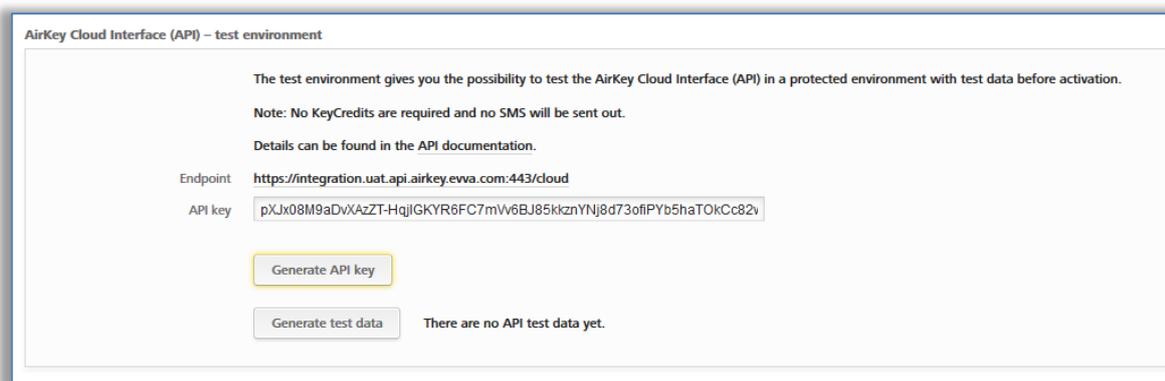


Figura 330: Gerar chave da API para ambiente de teste



Ao voltar a clicar em **Gerar chave para a API**, a chave da API já existente é substituída por uma nova. A chave da API substituída deixará de poder ser utilizada.



Após cada login, tem de ser gerada uma chave da API novamente.

12.4.3 Repor dados de teste

Os dados de teste do Ambiente de teste da AirKey Cloud Interface podem, com mais um clique, ser repostos ao seu estado original. Desta forma, todos os testes podem ser executados com os mesmos dados de teste.

- > Clique na área de **Definições**, na tab **Geral**, na área **AirKey Cloud Interface (API) – Ambiente de teste**, em **Repor dados de teste**.



Figura 331: Repor dados de teste do ambiente de teste

A reposição dos dados de teste é confirmada com uma mensagem sobre o sucesso da ação. O momento da última reposição é informado na secção **AirKey Cloud Interface (API) – Ambiente de teste**.

13 Sinalização dos componentes de bloqueio

Os componentes de bloqueio indicam eventos através de sinais óticos e sonoros.

Número do sinal	Evento	Sinal ótico*)	Sinal sonoro*)	Indicação
Sinal 1	Processo de abertura com meio autorizado	●●●●●	mmmmm	
Sinal 2	Fim do tempo de partilha	●●●●●	bbbbbb	
Sinal 3	Processo de abertura com meio não autorizado	●●-●●-●●-●●	aa-aa-aa-aa	
Sinal 7	Aviso de "Pilhas gastas" (Na Administração online do AirKey, na tabela dos componentes de bloqueio e nos detalhes de um componente de bloqueio, é indicado com o símbolo de "pilha gasta".)	●●-●●-●●-●●-●●	a----a----a--- -a	O sinal é emitido ao inserir de pilhas gastas no lugar do sinal 8 e no caso de processo de desbloqueio antes do sinal 1. São possíveis 1000 processos de desbloqueio ou duas semanas de funcionamento standby após a primeira sinalização (à temperatura ambiente e utilização de um cartão, porta-chaves, pulseiras e chave combinada).
Sinal 8	Inserir novas pilhas e reiniciação do componente	●●-●●-●●-●●	bb--mm--aa	
Sinal 9	Meio sem segmentação EVVA; meio de sistema de controlo de acessos de terceiros	●●●	Nenhum	Não está mais em uso. Apenas o sinal 3 é usado para esse fim.
Sinal 10	Erro de comunicação e de hardware de um componente de bloqueio	●-●-●-●-●-●-●-●- ●-●-●-●-●-●-●-●- ●-●-●-●-●-●-●-●- ●-●-●-●-●-●-●-●-	mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm--- mmm---mmm	É sinalizado, p. ex., devido a uma falha de conexão entre o puxador e o módulo eletrónico de um cilindro.

14 Valores e limites do AirKey

Neste capítulo, estão sumariadas as configurações máximas por meio e componente de bloqueio.

14.1 Administração Online do AirKey

O número máximo possível de componentes de bloqueio, áreas, pessoas e meios é ilimitado.

14.2 Componentes de bloqueio AirKey

- Os últimos 1000 registos protocolares são guardados sem atualização.
- Podem ser administrados, no máximo, 1000 registos na lista negra.
- São possíveis, no máximo, 96 atribuições de áreas.
- Podem ser atribuídas, no máximo, 250 partilhas a outros clientes.

14.3 Cartões, porta-chaves, pulseiras ou chaves combinadas

- Podem ser guardados, no máximo, 256 registos protocolares sem atualização.
- Podem ser atribuídas, no máximo, 150 autorizações a cada porta.
- Podem ser atribuídas, no máximo, 100 autorizações a áreas (se forem atribuídas 12 autorizações individuais com 8 acessos possíveis, só pode ser atribuído um total de 96 autorizações a áreas).

14.4 Aplicação AirKey

- Podem ser guardados, no máximo, 256 registos protocolares sem atualização.
- Número ilimitado de autorizações a portas individuais e áreas.

15 Quando são debitados os KeyCredits?

Para a operação contínua de um sistema de controlo de acessos AirKey são necessários KeyCredits para a concessão e alteração de autorizações de acesso.

Os KeyCredits apenas são debitados no caso de créditos de quantidade. Enquanto estiver disponível um crédito de tempo válido, é feito o uso de créditos de tempo e os créditos de tempo permanecem inalterados.

São debitados KeyCredits no âmbito das ações seguintes:

- Ao atribuir novas autorizações e subsequente produção
- Ao alterar autorizações existentes e subsequente produção
- Ao reativar meios desativados, contanto que as autorizações do meio desativado sejam mantidas
- Na troca do smartphone, quando as autorizações são transferidas para o novo smartphone
- Ao ativar a [AirKey Cloud Interface \(API\)](#)

Os KeyCredits, no caso de novas autorizações ou alterações das autorizações, apenas são debitados se o meio for produzido. Sendo assim, é debitado um KeyCredit por produção. Podem ser atribuídas ou alteradas várias autorizações de uma só vez – para isso, é debitado apenas um KeyCredit.

Não serão debitados KeyCredits para eliminar autorizações, desativar ou esvaziar meios.

16 Resolução de problemas

Ao adquirir o AirKey, decidiu-se por uma sistema de controlo de acessos eletrónico de elevada qualidade e exaustivamente testado. Caso, no entanto, face a um erro ou a um problema, poderá encontrar neste capítulo sugestões e recomendações para eliminar o erro ou problema.

16.1 A comunicação não é possível no sistema

Se não conseguir registar o smartphone ou atualizar o componente de bloqueio do AirKey, proceda aos seguintes passos:

- > Assegure-se de que o smartphone tem ligação à Internet (WLAN ou dados móveis) e ative-a, se necessário.
- > Verifique se a Porta 443 na sua infraestrutura de TI está bloqueada. Estas portas são necessárias para estabelecer a comunicação no sistema AirKey e têm de estar acessíveis. Ver o capítulo [Pré-requisitos do sistema](#).

16.2 O componente de bloqueio tem dificuldades em reconhecer o meio ou não reconhece mesmo

Se um componente de bloqueio, comparativamente a outros componentes de bloqueio, tiver dificuldades em reconhecer o meio ou não reconhecer mesmo, proceda aos seguintes passos:

- > Assegure-se de que o meio, na identificação, seja encostado à unidade de leitura até o componente de bloqueio sinalizar a verde. (A sinalização a azul significa apenas que existe comunicação entre o smartphone e o componente de bloqueio.)
- > Se o componente de bloqueio não reagir, preste atenção à posição correta do meio. A chave combinada, por exemplo, tem de ser encostada com o lado onde se vê o símbolo RFID.
- > Se, depois destes passos, ainda não surtir qualquer efeito, aguarde aprox. 50 segundos sem qualquer identificação na unidade de leitura, para que o componente de bloqueio possa voltar a calibrar o campo elétrico. Ao encostar um objeto metálico à unidade de leitura, poderá executar a "re-calibração" também manualmente.

16.3 Os meios já não são reconhecidos

Se um determinado meio deixar de ser reconhecido nos componentes de bloqueio, proceda aos seguintes passos:

- > Caso se trate de um smartphone, assegure-se de que a ligação NFC ou Bluetooth está ativada. Se necessário, volte a estabelecer a ligação NFC ou Bluetooth e certifique-se de que o smartphone está encostado na posição correta à unidade de leitura. Tenha em consideração que – dependendo do tipo de smartphone – podem existir divergências.

- > Se a unidade de leitura do componente de bloqueio ou da estação de codificação deixar de reagir ao meio, coloque o meio encostado à unidade de leitura de um componente de bloqueio ou sobre uma estação de codificação durante aprox. 10 segundos. O meio executa uma autorreparação. Percebe-se que o processo está concluído quando o componente de bloqueio ou a estação de codificação sinalizar como é habitual.

16.4 Não é possível desenroscar o puxador de um cilindro AirKey

Caso não se consiga desenroscar o puxador de um cilindro AirKey, talvez ajude executando o seguinte:

- > Lembre-se de utilizar a ferramenta de desmontagem para o cilindro AirKey para desmontar o puxador.
- > Os cilindros AirKey na versão de perfil Euro possuem na parte frontal do módulo eletrónico uma furação para manutenção, através da qual o eixo do puxador pode ser fixado com uma haste metálica adequada. Neste caso, recomendamos o conjunto de ferramentas de montagem 2.

Procedimento:

- > Insira a haste metálica do conjunto de ferramentas 2 na furação da parte frontal do seu cilindro de perfil Euro.
- > Gire o puxador em torno do próprio eixo até a haste metálica se deixar entrar bem fundo na furação para manutenção. Segure agora a haste metálica nesta posição e desmonte o puxador com a ferramenta de montagem, como é habitual.
- > Remova a haste metálica depois de desmontar o puxador.
- > Se não possuir nenhum cilindro AirKey em perfil Euro ou se o cilindro estiver integrado num invólucro ou numa roseta com proteção do núcleo, encoste um meio autorizado à unidade de leitura para fazer com que o cilindro engate. Utilize a ferramenta de montagem no cilindro dentro do período de ativação (enquanto o cilindro está engatado). Agora, o cilindro já não desengata e o puxador pode ser facilmente desenroscado.

16.5 O componente de bloqueio sinaliza um "Erro de hardware"

Se o componente de bloqueio AirKey sinalizar um erro de hardware (ver [Sinalização dos componentes de bloqueio](#)), é possível que o puxador / a unidade de leitura não esteja ligado(a) ao módulo eletrónico / unidade de controlo correspondente.

Verifique os contactos, fichas e ligações de acordo com o manual de instruções de montagem.

16.5.1 Cilindro AirKey

- > Assegure-se de que o anel vedante fica corretamente colocado no eixo do cilindro e enrosque o puxador, girando-o no sentido horário sobre o cilindro até sentir resistência.
- > Remova a ferramenta de montagem.
- > Gire o puxador, depois, no sentido anti-horário até sentir que engata no sítio.
- > Assegure-se de que o puxador e o módulo eletrónico ficam corretamente engatados.

16.5.2 Leitor de parede AirKey

- > Certifique-se de que a unidade de leitura e a unidade de controlo do leitor de parede AirKey estão corretamente conectados. Dado o caso, verifique, os cabos e os conectores.

16.6 O puxador eletrónico está perro

Dependendo da projeção do cilindro pelo invólucro ou roseta, o cilindro, mediante as circunstâncias, pode estar perro devido à fricção da vedação entre a caixa do cilindro e o puxador eletrónico. A possibilidade que existe é retirar a vedação da parte interna.

Caso, todavia, ainda precise de apoio, queira entrar em contacto com um parceiro da EVVA perto de si ([Assistência da EVVA](#)).

17 Indicações importantes

17.1 Sistema



Informa-se expressamente que o presente sistema AirKey pode estar sujeito ao dever de notificação/aprovação de acordo com determinações legais, em especial a lei de proteção de dados. Na sequência disto, a EVVA Sicherheitstechnologie GmbH não assume qualquer responsabilidade nem compromisso por um funcionamento sujeito à conformidade com a lei.



Para a comunicação no sistema AirKey, são utilizadas as Portas 443 e 7070 para ligação à Internet. Certifique-se de que estas portas não estejam bloqueadas. Ao utilizar a rede de dados móveis, a operadora de redes móveis é responsável pela administração das portas. Caso tenha um problema ao utilizar a rede de dados móveis para ligar o AirKey, contacte a sua operadora de redes móveis.



Emita autorizações com o menor prazo possível para manter a elevada segurança do sistema e, no caso de perda de um meio, manter o mínimo de registos possível na lista negra. Os meios com autorizações ilimitadas sem data de validade, só podem ser produzidos para fins de meios de emergência (p. ex., chave para os bombeiros).



Trabalhe sempre com a configuração atual do sistema na íntegra para manter a elevada segurança do sistema.

Poderá encontrar indicações de segurança a respeito de cada sistema sob os links seguintes:

Cilindro, cadeado: [PDF](#)

Leitor de parede, unidade de controlo: [PDF](#)

Normas e diretivas



Certificação CE | EN 1634: 30 minutos | EN 1634: 90 minutos | Tipo de proteção IP65 | EN 15684 | adequado para fechaduras conforme EN 179/1125 (na utilização da função antipânico FAP)

SKG | VdS¹

¹ Em preparação

18 Detalhes técnicos da interface RS485 para leitores de parede com Bluetooth

Após um acesso bem-sucedido a um leitor de parede com Bluetooth, um APDU com o registo protocolar deste acesso é enviado pelo leitor de parede através da interface RS485.

O registo protocolar contém, para além de outros parâmetros, a `lockingSystemId` de 5 bytes do meio (meio de acesso ou smartphone), que desbloqueou com sucesso o leitor de parede.

Este `lockingSystemId` (int64) pode então ser consultado através da AirKey Cloud Interface (API). Exemplo: `GET/v1/media?lockingSystemId=000102030405`

Com estas informações é possível realizar diferentes casos de aplicação, como, p. ex.:

- Indicação do nome da pessoa que acabou de desbloquear o leitor de parede.
- Leitura de parâmetros adicionais, p. ex., do campo "Comentário" deste meio e utilização destas informações para sistemas de terceiros.
- Controlo do elevador: Introduza, por exemplo, um mínimo de uma string JSON no campo de comentários de um meio de acesso ou smartphone, para indicar um determinado andar para este meio e utilize esta informação para o controlo do elevador.

18.1 Ativar interface RS485 para leitor de parede com Bluetooth

Para encaminhar o registo protocolar para um acesso bem-sucedido através da interface RS485, a respetiva configuração no leitor de parede com Bluetooth tem de ser ativada na administração online do AirKey.

- > Na página inicial **Home**, seleccione o botão **Leitor de parede**.
- > Em alternativa, seleccione, no menu principal, **Sistema de controlo de acessos** → **Componentes de bloqueio**.
- > Clique no leitor de parede com Bluetooth para o qual pretende ativar a função.
- > Abra o separador **Definições**.
- > Marque abaixo a caixa de seleção **Interface RS485**.



O leitor de parede com Bluetooth requer a versão de firmware 5.86 ou superior, caso contrário, é exibida uma indicação de que o firmware tem de ser atualizado para poder utilizar esta função.

18.2 Configuração da porta de série RS485

Com um adaptador RS485 ligado à interface RS485 do leitor de parede AirKey, o registo protocolar do último acesso bem-sucedido pode ser reencaminhado para um sistema de terceiros (p. ex., via USB ou Ethernet).

O adaptador RS485 é ligado em paralelo à unidade de controlo no conector macho para a unidade de leitura, adicionalmente ao cabo existente.

- Pino 2 da ficha → Doorbus B-
- Pino 3 da ficha → Doorbus A+



Poderá encontrar mais informações sobre a atribuição de fichas no plano da tampa da unidade de controlo.

A porta de série tem de ser configurada da seguinte forma:

- Taxa Baud: 115200
- Bit de dados: 8
- Bit de paragem: 1
- Paridade: even
- No CTS flow control

18.3 Especificação APDU do registo protocolar do acesso bem-sucedido

18.3.1 APDU do registo protocolar

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 Registo protocolar 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 Timestamp

Byte 1								Byte 2								Byte 3								Byte 4								Byte Bits
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	
*	*	*	*	*	*	*	*																									R1
						*	*	*	*																							R2
										*	*	*	*	*	*																	R3
														*	*	*	*	*	*													R4
																				*	*	*	*	*	*							R5
																		*	*	*	*	*	*									R6
Example								Example								Example								R7								
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	

R1 ... Ano: ano menos 2010 (ano 2022 = **001100**)

R2 ... Mês: jan = **01**, feb = **02**, mrt = **03** etc.

R3 ... Dia: intervalo de valores **01-31**

R4 ... Hora: intervalo de valores **00-23**

R5 ... Minutos: intervalo de valores **00-59**

R6 ... Segundos: intervalo de valores **00-59**

R7 ... Exemplo: **00110010 01110110 11010011 10111001** corresponde a 2022-09-27 13:14:57

18.3.2.2 Unlocking status (Estado de desbloqueio)

Byte 1								Description	
b8	b7	b6	b5	b4	b3	b2	b1		
0									Bit
1									R1
	0	0	0						R2
	0	0	1						R3
	0	1	0						R4
	0	1	1					R5	
								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 é atual
- R2** ... Hora não é atual. A fonte de alimentação esteve indisponível durante demasiado tempo.
- R3** ... Acesso recusado: De momento não autorizado
- R4** ... Acesso recusado: O meio encontra-se na lista negra do componente de bloqueio
- R5** ... Acesso recusado: Hora não atual
- R6** ... Acesso recusado: Erro de assinatura
- R7** ... Acesso recusado: Ativação não atual (ativação noutra sistema de controlo de acessos)
- R8** ... Acesso recusado: Dia de férias/feriado está ativo
- R9** ... Acesso concedido: Acesso via Hands-free (mãos-livres)
- R10** ... Acesso concedido
- R11** ... Estado da bateria: 100% para leitores de parede com Bluetooth
- R12** ... Exemplo: **0x7a** significa hora atual, acesso concedido, estado da bateria 100%

18.3.3 Exemplo

- APDU: **CC D6 F0 00 0E 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c**
- Registo protocalar: 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** = hora é actual, acesso concedido, estado da bateria 100 %
 - customerId: **00 00 02 8c**



Também é possível encaminhar a lockingSystemId dos meios de acesso para sistemas de terceiros através da estação de codificação. Para isso, utilize o parâmetro **"-notify"** ao iniciar a estação de codificação através da linha de comando. Poderá encontrar detalhes a este respeito no capítulo [Utilizar a estação de codificação através da linha de comando](#).

19 Declaração de conformidade

EVVA Sicherheitstechnologie GmbH
Wienerbergstraße 59-65 | A-1120 Wien | www.evva.com
+43 1 811 65-0 | +43 1 812 20 71 | office-wien@evva.com



EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59-65 | A-1120 Wien

EU - 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

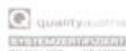
Hersteller: **EVVA Sicherheitstechnologie GmbH**
Wienerbergstraße 59-65
A-1120 Wien
Österreich

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: AT82310000600669705
BIC: RZBAATWW

Bank Austria
IBAN: AT76120000616194700
BIC: BKAUATWW

GF: Mag. Stefan Ehrlich-Adám
UID-Nr.: ATU 65126268 | FN 120755 g, HG Wien | DVR: 0131504
ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5



Notifizierte Stelle:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Wien
Kennnummer: 0408

Die Komponenten werden mit einer Firmware ausgeliefert, die den bestimmungsgemäßen Betrieb der Funkanlage ermöglichen.

Unterzeichnet für und im Namen von EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Geschäftsführer

Wien, 13.06.2017

EU-Konformitätserklärung_AIRKEY / 2

20 Declaration of Conformity

EVVA Sicherheitstechnologie GmbH
 Wienerbergstraße 59-65 | A-1120 Wien | www.evva.com
 +43 1 811 65-0 | +43 1 812 20 71 | office-wien@evva.com



EVVA Sicherheitstechnologie GmbH | Wienerbergstraße 59-65 | A-1120 Wien

EU – DECLARATION OF CONFORMITY

EVVA Sicherheitstechnologie GmbH, a limited liability company having its seat in Vienna, Austria, herewith confirms compliance of the following products with the directives below:

AIRKEY

AirKey-Cylinder	E.A.PZ. E.A.AI. E.A.HB.
AirKey-Hybridcylinder	E.A/[System].PZ
AirKey-Padlock	E.A.HA.
AirKey-Wallreader	E.A.WL.
AirKey-Control Unit	E.A.WL.CU.
AirKey-Emergency Power Device	E.ZU.NG.V1

Manufacturer: **EVVA Sicherheitstechnologie GmbH**
 Wienerbergstraße 59-65
 A-1120 Vienna
 Austria

This declaration of conformity is issued under the sole responsibility of the manufacturer. Object of this declaration are all serial manufactured products since the issue date of this declaration. The object of the declaration described above is in conformity with the relevant Union harmonisation legislation:

- Directive 2014/53/EU („Directive for radio equipment devices“)
- Directive ROHS 2011/65/EU in the version of 2014/76/EU

Relevant harmonised Standards:

- EN 62368-1:2014 respectively IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012



Raffaelsen Bank International AG
 IBAN: AT823100000600669705
 BIC: RZBAATWW

Bank Austria
 IBAN: AT761200000616194700
 BIC: BKAUATWW

GF. Mag. Stefan Ehrlich-Adam
 UID-Nr. ATU 65126268 | FN 120755 g, HG Wien | DVR. 0131504
 ARA-Lizenz-Nr.: 2383 (alle Verpackungen entpflichtet) | bbn: 90 02453 5



Notified body:

TÜV AUSTRIA SERVICES GMBH
Industry & Energy Austria
EMV--MT-LAB
Deutschstraße 10, 1230 Vienna
Number: 0408

The components are delivered with a firmware which allows the radio equipment to operate as intended.

Signed for and on behalf of EVVA Sicherheitstechnologie GmbH

Mag. Stefan Ehrlich-Adám
Managing Director

Vienna, 13.06.2017

EU-Declaration of Conformity_AIRKEY / 2

21 Índice das figuras

Figura 1: Arquitetura do sistema	12
Figura 2: Vista geral do sistema – Segurança sem lacunas	12
Figura 3: Link "Registo AirKey"	20
Figura 4: Registo no AirKey	21
Figura 5: Concluir registo	21
Figura 6: E-mail "Registo no AirKey EVVA"	22
Figura 7: Determine a sua própria senha para concluir o registo	23
Figura 8: Página inicial do sistema de controlo de acessos AirKey	23
Figura 9: Ajuda interativa	24
Figura 10: Ajuda interativa – Carregar crédito	24
Figura 11: Estação de codificação – instalação da aplicação	25
Figura 12: Instalar e iniciar a aplicação da estação de codificação	25
Figura 13: Abertura do ficheiro AirKey.jnlp	26
Figura 14: Estabelecimento da ligação à estação de codificação	26
Figura 15: Seleção da estação de codificação	26
Figura 16: Ícone do AirKey na barra de tarefas	27
Figura 17: Download da aplicação da estação codificadora	27
Figura 18: Iniciar a aplicação da estação codificadora, linha de comando	28
Figura 19: Definições da aplicação da estação de codificação	29
Figura 20: Leitor de cartões "Microsoft UICC" na Administração online do AirKey	30
Figura 21: Editor de Políticas de Grupo Local	31
Figura 22: Serviço Plug and Play de Smart Cards	32
Figura 23: Créditos	33
Figura 24: Adicionar crédito	33
Figura 25: Inserir o código de crédito	33
Figura 26: Adicionar crédito	34
Figura 27: Criar pessoa	34
Figura 28: Atribuir meio	35
Figura 29: Importar lista de pessoas	35
Figura 30: Importas pessoas – Lista de pessoas	36
Figura 31: Importar pessoas – Distribuição dos campos na lista de pessoas	36
Figura 32: Excel – Guardar como – "Texto Unicode (*.txt)"	39
Figura 33: Excel – Confirmar Guardar como "Texto Unicode (*.txt)"	39
Figura 34: Ficheiro de texto no "Editor" – marcar o espaço de tabulação e copiar para a área de transferência	39
Figura 35: "Editor" – substituir todos os espaços de tabulação por pontos e vírgulas	40
Figura 36: "Editor" – Guardar como – inserir, manualmente, a terminação .csv do ficheiro e selecionar a codificação UTF-8	40
Figura 37: Importar Pessoas	41
Figura 38: Importar Pessoas	41
Figura 39: Importar pessoas – Resultado	41
Figura 40: Novo meio smartphone ou cartão	42
Figura 41: Criar novo meio	42
Figura 42: Criar código de registo	43
Figura 43: Código de registo	43

Figura 44: Editar meio – Definições -----	43
Figura 45: AirKey App – Adicionar sistema de controlo de acessos (iOS)-----	45
Figura 46: Aplicação AirKey – Adicionar sistema de controlo de acessos (Android) -----	45
Figura 47: "Send a Key" -----	47
Figura 48: "Send a Key" – Campo de pesquisa-----	47
Figura 49: "Send a Key" – Criar pessoa -----	47
Figura 50: SMS com link – aqui apresentado com o Samsung Galaxy S7 Edge -----	48
Figura 51: Registo com sucesso -----	48
Figura 52: Registrar o número de telefone (iOS)-----	49
Figura 53: Código de registo (iOS)-----	49
Figura 54: Tipos de acesso -----	50
Figura 55: Aplicação AirKey – Conecte com o componente (por NFC no caso de smartphone Android / por Bluetooth no caso de Smartphone Android / por Bluetooth no caso de iPhone) -----	52
Figura 56: Aplicação AirKey – Conecte com o componente -----	52
Figura 57: Aplicação AirKey – A ligação está a ser estabelecida -----	52
Figura 58: Adicionar componente -----	53
Figura 59: Aplicação AirKey – Adicionar componente de bloqueio Android / iPhone -----	53
Figura 60: Aplicação AirKey – Componente de bloqueio adicionado -----	54
Figura 61: Coordenadas de GPS nos Detalhes do componente de bloqueio -----	54
Figura 62: Adicionar componente de bloqueio-----	55
Figura 63: Adicionar componente de bloqueio / sem estação de codificação -----	55
Figura 64: Adicionar componente de bloqueio – Atribuição do nome -----	55
Figura 65: Adicionar componente de bloqueio-----	56
Figura 66: Adicionar componente de bloqueio – Mensagem de confirmação do processo ---	56
Figura 67: Detalhes do componente de bloqueio-----	56
Figura 68: Adicionar componente ao meu sistema de controlo de acessos -----	57
Figura 69: Aplicação AirKey – Conecte com o componente-----	58
Figura 70: Aplicação AirKey – A ligação está a ser estabelecida -----	58
Figura 71: Detalhes do meio -----	58
Figura 72: Adicionar meio – Atribuir um nome -----	59
Figura 73: Atribuir pessoa -----	59
Figura 74: Atribuir pessoa ao meio -----	60
Figura 75: Confirmar pessoa -----	60
Figura 76: Atribuir autorização -----	61
Figura 77: Atribuir uma autorização de acesso permanente-----	61
Figura 78: Atribuir uma autorização de acesso permanente-----	62
Figura 79: Atribuir acesso periódico-----	62
Figura 80: Atribuir acesso periódico-----	63
Figura 81: Adicionar acesso periódico-----	63
Figura 82: Atribuir autorização de acesso temporário -----	64
Figura 83: Atribuir autorização de acesso temporário -----	64
Figura 84: Atribuir acessos individuais-----	64
Figura 85: Nova autorização – Acesso individual -----	65
Figura 86: Nova autorização – Acesso individual -----	65
Figura 87: Criar autorização -----	65
Figura 88: Criar autorização nova ou alterada -----	65
Figura 89: Tentativa de login falhada -----	67

Figura 90: Administração online do AirKey – Home -----	68
Figura 91: Verificação do número de telemóvel ao fazer login -----	68
Figura 92: Código da SMS para o login -----	69
Figura 93: Página de login da Administração online do AirKey -----	70
Figura 94: Esqueceu-se da sua senha -----	70
Figura 95: código por SMS -----	70
Figura 96: Repor a senha do AirKey -----	71
Figura 97: A minha conta AirKey -----	72
Figura 98: Terminar sessão-----	72
Figura 99: Menu principal – Administradores -----	73
Figura 100: Detalhes de um administrador -----	73
Figura 101: Informações de contacto -----	74
Figura 102: Criar administrador -----	74
Figura 103: Criar administrador -----	74
Figura 104: Editar administrador -----	76
Figura 105: Gerir os direitos de um subadministrador -----	76
Figura 106: Atribuição de autorizações por um administrador do sistema ou por um subadministrador-----	77
Figura 107: Eliminar administrador -----	77
Figura 108: Eliminar administrador -----	77
Figura 109: Definições do sistema de controlo de acessos AirKey -----	78
Figura 110: Definições gerais – Definições de Bluetooth para a aplicação AirKey -----	79
Figura 111: Definições gerais – Definições para a aplicação AirKey -----	79
Figura 112: Definições para a aplicação AirKey – Atualização após cada acesso -----	79
Figura 113: O estado da opção "Atualização após cada acesso" -----	80
Figura 114: Definições para a aplicação AirKey – Texto para o SMS "Send a Key"-----	80
Figura 115: Definições gerais – Opções de segurança -----	81
Figura 116: Definições gerais – Autenticação de dois fatores -----	81
Figura 117: Registe o número de telemóvel -----	82
Figura 118: Insira o código da SMS -----	82
Figura 119: Desativar a autenticação de dois fatores -----	83
Figura 120: Desativar a autenticação de dois fatores -----	83
Figura 121: Ativação do princípio dos quatro olhos -----	83
Figura 122: Ativação do princípio dos quatro olhos – selecção do segundo administrador --	84
Figura 123: Ativação do princípio dos quatro olhos – introdução do código de confirmação--	84
Figura 124: Valores por defeito para novos componentes de bloqueio -----	85
Figura 125: Valores por defeito – Áreas -----	86
Figura 126: Valores por defeito – Acesso -----	86
Figura 127: Abertura permanente automática -----	87
Figura 128: Abertura permanente automática -----	87
Figura 129: Protocolização – Atualização após o processo de desbloqueio -----	88
Figura 130: Definir o registo em protocolo -----	89
Figura 131: Guardar os valores por defeito alterados-----	90
Figura 132: Calendário de dias de férias/feriados (vista geral do calendário) -----	90
Figura 133: Adicionar dia de férias/feriado -----	91
Figura 134: Adicionar dia de férias/feriado pelo calendário-----	91
Figura 135: Editar dia de férias/feriado -----	91
Figura 136: Eliminar dia de férias/feriado -----	91

Figura 137: Calendário de dias de férias/feriados (lista geral) -----	92
Figura 138: Sistema de controlo de acessos AirKey-----	92
Figura 139: Componentes de bloqueio-----	93
Figura 140: Editar componente de bloqueio -----	94
Figura 141: Áreas -----	94
Figura 142: Ativações-----	95
Figura 143: Editar componente de bloqueio -----	95
Figura 144: Definições – Horas e calendário-----	95
Figura 145: Registo em protocolo-----	96
Figura 146: Remover componente de bloqueio-----	97
Figura 147: Pergunta de segurança -----	97
Figura 148: Sistema de controlo de acessos – Áreas -----	98
Figura 149: Criar área -----	98
Figura 150: Editar área -----	99
Figura 151: Atribuir componentes-----	99
Figura 152: Marcar os componentes de bloqueio-----	100
Figura 153: Cancelar atribuição -----	101
Figura 154: Apagar área -----	101
Figura 155: Eliminar área – não é possível -----	102
Figura 156: Separador da página "Editar componente de bloqueio" -----	102
Figura 157: Meios autorizados (do próprio) -----	103
Figura 158: Editar meio-----	103
Figura 159: Tarefas de manutenção -----	104
Figura 160: Priorização das tarefas de manutenção -----	104
Figura 161: Plano de bloqueio-----	105
Figura 162: Meios e pessoas -----	107
Figura 163: Pessoas-----	107
Figura 164: Gerar o certificado de entrega -----	108
Figura 165: Certificado de entrega (PDF)-----	109
Figura 166: Eliminar pessoa -----	109
Figura 167: Eliminar pessoa – Pergunta de segurança-----	110
Figura 168: Atribuir meio -----	110
Figura 169: Atribuir meio à pessoa -----	111
Figura 170: Atribuir meio à pessoa -----	111
Figura 171: Lista de meios -----	112
Figura 172: Adicionar meio -----	112
Figura 173: Criar novo meio-----	112
Figura 174: Editar meio – Cartão -----	114
Figura 175: Vista geral das autorizações -----	114
Figura 176: Editar meio – Alterar autorização-----	115
Figura 177: Alterar autorização -----	116
Figura 178: Alterar acesso-----	116
Figura 179: Acesso permanente-----	117
Figura 180: Eliminar autorização-----	117
Figura 181: Eliminar autorização -----	117
Figura 174: Desativar meio-----	118
Figura 183: Desativar meio – Pergunta de segurança -----	118
Figura 184: Remover o meio desativado -----	120

Figura 185: Remover meio – Pergunta de segurança -----	120
Figura 186: Reativar o meio desativado -----	120
Figura 187: Reativar meio -----	120
Figura 188: Reativar meio -----	121
Figura 189: Reativar meio – Restabelecer autorizações -----	121
Figura 190: Duplicar um meio -----	122
Figura 191: Duplicar meio -----	122
Figura 192: Meio vazio -----	123
Figura 193: Meio vazio – Pergunta de segurança -----	123
Figura 194: Meios atribuídos -----	124
Figura 195: Meio – Cancelar atribuição -----	125
Figura 196: Cancelar atribuição sem autorizações -----	125
Figura 197: Cancelar atribuição com autorizações -----	125
Figura 198: Cancelar atribuição – Mudar pessoa -----	126
Figura 199: Mudar pessoa -----	126
Figura 200: Mudar pessoa -----	127
Figura 193: Remover meio – Caixote do lixo -----	127
Figura 202: Remover meio -----	127
Figura 203: Protocolos -----	128
Figura 204: Ativação da visualização dos protocolos – selecção do segundo administrador	129
Figura 205: Ativação da visualização dos protocolos – introdução do código de confirmação -----	129
Figura 206: Protocolo Componentes de bloqueio e áreas -----	130
Figura 207: Ativação da visualização dos protocolos – selecção do segundo administrador	132
Figura 208: Ativação da visualização dos protocolos – introdução do código de confirmação -----	132
Figura 209: Protocolo dos meios -----	133
Figura 210: Apagar os registos protocolares -----	134
Figura 211: Protocolo do sistema -----	135
Figura 212: Ativações de apoio -----	136
Figura 213: Lista de ativações de apoio -----	136
Figura 214: Criar ativação de apoio -----	137
Figura 215: Vista geral das ativações de apoio -----	137
Figura 216: Bloquear ativação de apoio -----	138
Figura 217: Validade das ativações de apoio -----	138
Figura 218: Aplicação AirKey – Vista geral das autorizações -----	140
Figura 219: Aplicação AirKey – Detalhes da autorização -----	140
Figura 220: Autorização expirada -----	140
Figura 221: Dados protocolares de uma autorização -----	141
Figura 222: Mensagem de confirmação da abertura permanente -----	141
Figura 223: Aplicação AirKey – Introduzir PIN -----	142
Figura 224: Codificar meios – Lista de seleção dos componentes de bloqueio com Bluetooth -----	142
Figura 225: Codificar meios -----	143
Figura 226: Protocolo de autorizações -----	143
Figura 227: Smartphone Android com Bluetooth – Menu principal / Opção "Utilizar Bluetooth" ativada / Opção Bluetooth desativada -----	144

Figura 228: iPhone (só com Bluetooth) – Menu principal / Definições sem funções NFC / Opção Bluetooth desativada -----	145
Figura 229: Desbloqueios a partir de notificações – Ecrã de bloqueio -----	147
Figura 230: Desbloqueios a partir de notificações-----	147
Figura 231: Aplicação AirKey – Funções de segurança-----	148
Figura 232: Aplicação AirKey – Ativar PIN -----	149
Figura 233: Aplicação AirKey – Alterar PIN -----	149
Figura 234: Aplicação AirKey – Desativar PIN -----	150
Figura 235: Administração online do AirKey – Desativar código PIN -----	150
Figura 236: Administração online do AirKey – Desativar código PIN -----	151
Figura 237: Notificações Push da aplicação AirKey, Definições Android / iPhone -----	151
Figura 238: Tarefas de manutenção -----	152
Figura 239: Notificação sobre alteração da autorização-----	152
Figura 240: Aplicação AirKey – Info-----	153
Figura 241: Aualizar o smartphone Android ou o iPhone -----	154
Figura 242: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone) -----	155
Figura 243: Atualizar dados -----	155
Figura 244: Autorização de construção local -----	156
Figura 245: Ponto do menu "Tarefas de manutenção" no menu principal -----	157
Figura 246: Tarefas de manutenção -----	157
Figura 247: Visualização dos detalhes do componente de bloqueio -----	158
Figura 248: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone) -----	159
Figura 249: Aplicação AirKey – Conecte com o componente -----	159
Figura 250: Remover componente AirKey -----	160
Figura 251: Codificar meios – Lista de seleção dos componentes de bloqueio com Bluetooth -----	160
Figura 252: Remover um meio com o iPhone -----	161
Figura 253: Remover meio -----	161
Figura 254: Símbolo do protocolo -----	162
Figura 255: Definições AirKey-App-----	163
Figura 256: Autorizações para o modo Hands-free-----	163
Figura 257: Tag iOS NFC -----	165
Figura 258: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone) -----	167
Figura 259: Atualizar dados -----	168
Figura 260: Mensagens de atualização -----	168
Figura 261: Atualizar o componente de bloqueio com a estação de codificação -----	169
Figura 262: Componente de bloqueio atualizado com a estação de codificação -----	169
Figura 263: Símbolo "Conecte com o componente" (só em smartphones Android) -----	170
Figura 264: Atualizar dados -----	170
Figura 265: Aplicação AirKey atualiza um meio -----	170
Figura 266: Atualizar o meio com a estação de codificação -----	171
Figura 267: Meio próprio ou de terceiros atualizado com a estação de codificação -----	171
Figura 268: Aplicação AirKey – Conecte com o componente (Android NFC / Android Bluetooth / iPhone) -----	172
Figura 269: Conecte com o componente – Atualização do firmware -----	173

Figura 270: Aplicação AirKey – Detalhes do componente-----	173
Figura 271: Aplicação AirKey – Atualizar firmware-----	174
Figura 272: Aplicação AirKey – Passo de atualização executado com sucesso -----	174
Figura 273: Aplicação AirKey – Atualização executada com sucesso-----	175
Figura 274: Estação de codificação – Mensagem de confirmação da atualização de um componente de bloqueio-----	175
Figura 275: Estação de codificação – Atualização do firmware do cilindro-----	176
Figura 276: Estação de codificação – Passo da atualização executado com sucesso -----	176
Figura 277: Estação de codificação – Atualização do firmware executada com sucesso ---	177
Figura 278: Estação de codificação – Componente de bloqueio atualizado com sucesso --	177
Figura 279: Aplicação AirKey – Conecte com o componente -----	178
Figura 280: Aplicação AirKey – Detalhes do meio-----	178
Figura 281: Aplicação AirKey – Atualizar Keyring -----	179
Figura 282: Aplicação AirKey – Atualização do Keyring executada com sucesso -----	179
Figura 283: Estação de codificação – Atualização do Keyring disponível-----	180
Figura 284: Estação de codificação – Atualização do Keyring -----	180
Figura 285: Estação de codificação – Atualização do Keyring executada com sucesso ----	180
Figura 286: Estação de codificação – Meio atualizado com sucesso-----	181
Figura 287: Estado das pilhas -----	182
Figura 288: Editar componente de bloqueio – Opções de reparação-----	185
Figura 289: Opções de reparação -----	186
Figura 290: Estado do componente e tarefa de manutenção -----	186
Figura 291: Componente no estado de fábrica – Emitir cilindro de substituição -----	188
Figura 292: Editar componente de bloqueio – Opções de reparação-----	189
Figura 293: Opções de reparação -----	190
Figura 294: Estado do componente e tarefa de manutenção -----	190
Figura 295: Desinstalar componente com defeito com o smartphone -----	191
Figura 296: Desinstalar componente com defeito com o smartphone – Confirmação-----	191
Figura 297: Desinstalar componente de bloqueio com defeito -----	192
Figura 298: Eliminar tarefa de manutenção -----	193
Figura 299: Confirmar a troca do smartphone -----	196
Figura 300: Código QR para a troca do smartphone -----	196
Figura 301: Página inicial – operações de troca do smartphone em curso-----	197
Figura 302: Operações de troca do smartphone em curso-----	197
Figura 303: Falha na troca do smartphone -----	197
Figura 304: Troca de smartphone-----	199
Figura 305: Troca de smartphone-----	199
Figura 306: Troca de smartphone-----	200
Figura 307: Troca de smartphone – Reenviar código -----	200
Figura 308: Ativar componente de bloqueio para partilha -----	201
Figura 309: Adicionar partilha -----	201
Figura 310: Adicionar componente de bloqueio – barra cinzenta -----	202
Figura 311: Adicionar componente de bloqueio -----	202
Figura 312: Adicionar componente de bloqueio ativado para partilha -----	203
Figura 313: Adicionar componente de bloqueio ativado para partilha -----	203
Figura 314: Adicionar componente de bloqueio ativado para partilha -----	204
Figura 315: Autorização de componente de bloqueio ativado para partilha -----	205
Figura 316: Meios autorizados (de terceiros)-----	206

Figura 317: Bloco "Ativação de partilha" – Eliminar partilha -----	207
Figura 318: Eliminar partilha -----	207
Figura 319: Adicionar sistema de chave mestra-----	208
Figura 320: Definições gerais – AirKey Cloud Interface (API) -----	209
Figura 321: Ativar API -----	210
Figura 322: Gerar chave para a API-----	211
Figura 323: Gerar chave para a API, caixa de diálogo -----	211
Figura 324: Gerar chave para a API, detalhes-----	212
Figura 325: Editar chave da API-----	213
Figura 326: Eliminar chave da API -----	213
Figura 327: Desativar a chave da API -----	214
Figura 328: Ativar a chave da API -----	214
Figura 329: Gerar dados de teste -----	215
Figura 330: Gerar chave da API para ambiente de teste -----	215
Figura 331: Repor dados de teste do ambiente de teste-----	216

22 Glossário

No âmbito do AirKey, são utilizados os seguintes termos, entre outros:

Designação	Função
Cliente	Proprietário do sistema de controlo de acessos com número de cliente exclusivo.
Administrador	Trata-se de um papel como utilizador do sistema AirKey, o qual possui autorização para executar todas as tarefas administrativas na Administração online do AirKey. Para um cliente, pode haver vários administradores criados. Para cada sistema de controlo de acessos AirKey, tem de haver, pelo menos, um administrador definido.
Pessoa	Utilizadores que usam meios. Os meios são atribuídos às pessoas com base em autorizações de acesso para as áreas e componentes de bloqueio.
Meios	São smartphones ou meios de acesso, que podem ser adicionados ao sistema de bloqueio AirKey para a obtenção de acesso aos componentes de bloqueio AirKey autorizados.
Meios de acesso	Os meios NFC passivos (sem fonte de alimentação própria) são aqueles que, a par dos smartphones, podem ser utilizados em sistemas de bloqueio AirKey. Incluem-se aqui cartões, porta-chaves, chaves combinadas, pulseiras etc.
Meio de origem	Este termo é utilizado em combinação com as funções "Troca de smartphone" e "Duplicar meio". Descreve o smartphone ou o meio de acesso a partir do qual foi iniciada a troca ou a duplicação. No caso de troca do smartphone, o meio de origem descreve o smartphone "antigo" que deve ser substituído por um novo.
Meio de destino	Este termo é utilizado em combinação com as funções "Troca de smartphone" e "Duplicar meio". Descreve o smartphone ou o meio de acesso ao qual devem ser transmitidas as autorizações e definições do AirKey. No caso de troca do smartphone, o meio de destino descreve o "novo" smartphone que deverá substituir um outro smartphone.
Componentes de bloqueio	Cilindros AirKey (nos mais diversos modelos), cadeados AirKey eleitores de parede AirKey, que podem abrir e fechar portas num sistema de bloqueio.
Área	Uma unidade administrativa na Administração online do AirKey é aquela que abrange vários componentes de bloqueio. As áreas facilitam a administração do sistema de bloqueio AirKey e a atribuição de autorizações para componentes de bloqueio.

KeyCredits	Constituem um saldo no âmbito de um sistema de bloqueio AirKey. O saldo é utilizado para atribuir novas autorizações, alterar autorizações existentes ou ativar mais funcionalidades do AirKey.
AirKey Cloud Interface	A AirKey Cloud Interface é uma interface (API) para sistemas de terceiros, que tem por base o REST . A interface permite comandar determinadas funções do AirKey através de um software de terceiros.
Interface RS485	A interface RS485 é uma interface padronizada que pode ser utilizada para transferir dados. No caso de um leitor de parede AirKey, o último acesso bem-sucedido pode ser transmitido a um software de terceiros através desta interface.
APDU	APDU significa Unidade de Dados de Protocolo da Aplicação e é utilizado neste documento na interface RS485. Descreve um pacote de dados que é transmitido através da interface RS485.
"Send a Key"	Descreve uma função da Administração online do AirKey. Um administrador pode, por este meio, aplicar rapidamente novos smartphones e atribuir ou editar autorizações existentes de smartphones. O proprietário do smartphone recebe uma SMS, através da qual o smartphone é registado automaticamente no AirKey.
Autenticação de dois fatores	A autenticação de dois fatores constitui um nível de segurança adicional ao fazer login na Administração online do AirKey. Além da identificação do utilizador e da senha, é pedido um código adicional recebido por SMS para o login, como segundo fator.
Princípio dos quatro olhos	Descreve um processo em que uma ação só pode ser realizada com mais uma pessoa. No caso do AirKey, este princípio pode ser utilizado para proteger dados pessoais nos protocolos.
Firmware	Programa de software utilizado para os componentes de bloqueio, para que estes possam executar a sua função no AirKey. O firmware dos componentes de bloqueio pode ser atualizado a partir de updates do firmware.
Keyring	No sistema AirKey, "Keyring" é o nome de um programa de software que gere todos os dados relevantes do AirKey, que são memorizados nos meios de acesso passivos, como cartões, porta-chaves, chaves combinadas e pulseiras. Caso esteja disponível uma nova versão de Keyring no sistema AirKey, os meios poderão ser atualizados com um smartphone com autorização de manutenção ou com uma estação de codificação.

Tarefas de manutenção	São indicadas no âmbito da Administração online do AirKey para componentes de bloqueio que não estão atualizados. O sistema apenas estará atualizado e seguro quando todas as tarefas de manutenção de um sistema de bloqueio AirKey tiverem sido concluídas.
Autorização de manutenção	<p>Só quando um smartphone possui uma autorização de manutenção para o sistema de controlo de acessos é que os componentes (meios e componentes de bloqueio) podem ser adicionados ou removidos com ele no sistema de controlo de acessos. Com um smartphone com autorização de manutenção, o técnico de manutenção do AirKey pode utilizar o componente de bloqueio também no estado de fábrica.</p> <p>A autorização de manutenção pode ser ativada na Administração online do AirKey para o smartphone desejado.</p>

23 Ficha técnica

7ª edição, novembro de 2022

Com a edição de um novo manual do sistema, esta edição perde a sua aplicabilidade. Poderá encontrar a versão mais atual do manual do sistema na nossa homepage para download: <https://www.evva.com/pt/airkey/systemmanual/>.

Todos os direitos reservados. Sem o consentimento escrito do editor, o presente manual do sistema não pode ser integral ou parcialmente reproduzido sob nenhuma forma nem duplicado ou processado por nenhum meio eletrónico, mecânico ou químico.

É possível que este manual apresente falhas de impressão ou erros tipográficos. As informações constantes deste manual serão, contudo, regularmente verificadas e corrigidas. Não assumimos qualquer responsabilidade por erros técnicos ou de impressão e suas consequências.

Todas as marcas registadas e direitos autorais são reconhecidos.

Poderão ser implementadas alterações sem aviso prévio devido a melhorias técnicas.

Ficha técnica

Editor

EVVA Sicherheitstechnologie GmbH

Responsável pelos conteúdos

EVVA Sicherheitstechnologie GmbH

Conteúdos técnicos

Florian Diener, Johannes Ullmann

Consultores técnicos

Raphael Fasching, Iulian Stanciulescu, Martin Bauer