







## 1 Índice

2	Intr	oduç	ao, visão geral	)
	2.1	Info	rmações de foro legal	)
	2.2	Assi	stência da EVVA10	)
	2.3	Escl	arecimento dos símbolos11	L
	2.4	Sug	estões para uma navegação ideal neste documento11	L
3	Arq	uitet	ura do sistema12	2
	3.1	Con	nponentes de bloqueio13	3
	3.1	.1	Cilindro AirKey	3
	3.1	.2	Cilindro híbrido AirKey14	ł
	3.1	.3	Cilindro de patilha AirKey14	ł
	3.1	.4	Cadeado AirKey15	5
	3.1	.5	Leitor de parede AirKey15	5
	3.2	Apli	cação AirKey16	5
	3.3	Sma	artphones16	5
	3.4	Meio	os AirKey17	7
	3.5	Adm	ninistração online do AirKey18	3
	3.5	.1	Pré-requisitos do sistema18	3
	3.6	Key	Credits da EVVA18	3
	3.7	Esta	ação de codificação18	3
	3.8	Alim	nentação de emergência19	)
4	Prir	neira	utilização20	)
	4.1	Inst	alar a aplicação AirKey20	)
	4.2	Reg	isto na Administração online do AirKey20	)
	4.3	Inic	iar sessão23	3
	4.4	Ajuo	da interativa24	ł
	4.5	Inst	alar a estação de codificação24	ł
	4.5	.1	Utilizar a estação de codificação através da Administração online do AirKey 25	5
	4.5	.2	Utilizar a estação de codificação através da linha de comando27	7
	4.5	.3	Definições da aplicação da estação de codificação28	3
	4.5	.4	Soluções para possíveis problemas com a estação de codificação29	)
	4.6	Adio	cionar crédito32	2
	4.7	Cria	r pessoa34	ł
	4.7	.1	Importar dados de pessoas	5
	4.8	Cria	r smartphone42	)



	4.9 Reg	listar smartphone
	4.9.1	Função "Send a Key"46
	4.10 II	nstalar os componentes de bloqueio50
	4.10.1	Cilindro AirKey
	4.10.2	Leitor de parede AirKey
	4.11 A	dicionar componente de bloqueio51
	4.11.1	Adicionar componentes de bloqueio com o smartphone
	4.11.2	Adicionar componente de bloqueio com a estação de codificação54
	4.12 A	dicionar cartões, porta-chaves, pulseiras e chaves combinadas com o
	smartphor	ne57
	4.13 A	tribuir uma pessoa a um meio59
	4.14 A	tribuir autorizações60
	4.14.1	Acesso permanente61
	4.14.2	Acesso periódico
	4.14.3	Acesso temporário
	4.14.4	Acesso individual
	4.15 C	riar autorização65
5	Adminis	tração Online do AirKey67
	5.1 Log	in no AirKey67
	5.1.1	Login no AirKey sem a autenticação de dois fatores
	5.1.2	Login no AirKey com a autenticação de dois fatores
	5.1.3	Esqueceu-se da sua senha69
	5.2 Log	out do AirKey
	5.3 Adr	ninistradores
	5.3.1	Criar administrador73
	5.3.2	Editar administrador75
	5.3.3	Eliminar administrador77
	5.4 Def	inições do sistema de controlo de acessos AirKey78
	5.4.1	Informações gerais
	5.4.2 novos)	Valores por defeito (para todos os componentes de bloqueio adicionados como 85
	5.4.3	Dias de férias/feriados90
	5.5 Sist	ema de controlo de acessos92
	5.5.1	Vista geral dos componentes de bloqueio93
	5.5.2	Adicionar componente de bloqueio: ver o capítulo 4.11
	5.5.3	Editar componente de bloqueio93
	5.5.4	Remover o componente de bloqueio96



5.5	.5	Áreas
5.5	.6	Criar área
5.5	.7	Atribuir componente de bloqueio a áreas99
5.5	.8	Cancelar a atribuição de componentes de bloqueio a uma área 100
5.5	.9	Eliminar área
5.5	.10	Vista geral das autorizações102
5.5	.11	Tarefas de manutenção 103
5.5	.12	Dados de cliente – plano de bloqueio105
5.6	Mei	os e pessoas107
5.6	.1	Vista geral das pessoas107
5.6	.2	Criar pessoa: ver o capítulo 4.7107
5.6	.3	Editar pessoa
5.6	.4	Eliminar pessoa
5.6	.5	Atribuir meio a uma pessoa110
5.6	.6	Vista geral dos meios
5.6	.7	Adicionar meio
5.6	.8	Criar smartphone: ver o capítulo 4.8113
5.6	.9	Criar cartão, porta-chaves, pulseiras ou chave combinada113
5.6	.10	Editar meio
5.6	.11	Atribuir uma pessoa a um meio: ver o capítulo 4.13 114
5.6	.12	Autorizações
5.6	.13	Atribuir autorizações: ver o capítulo 4.14115
5.6	.14	Criar autorização: ver o capítulo 4.16 115
5.6	.15	Alterar autorização115
5.6	.16	Apagar autorização116
5.6	.17	Desativar meio
5.6	.18	Remover o meio desativado119
5.6	.19	Reativar meio
5.6	.20	Troca de smartphone
5.6	.21	Duplicar meio
5.6	.22	Esvaziar meio
5.6	.23	Cancelar atribuição123
5.6	.24	Remover meio
5.7	Prot	tocolos
5.7	.1	Protocolo de componentes de bloqueio 129
5.7	.2	Protocolo dos meios



	5.7.	3	Prot	tocolo do sistema135	)
	5.8	Ativ	açõe	es de apoio136	5
	5.8.	1	Cria	ar ativação de apoio136	5
	5.8.	2	Bloo	quear login de apoio137	7
	5.9	Aju	da		3
6	Apli	caçã	o Air	rKey	)
	6.1	Con	npon	nentes Bluetooth	)
	6.2	Reg	istar	r smartphone: ver o capítulo 4.9139	)
	6.3	Aut	oriza	nções	)
	6.4	Tare	efas	de manutenção: ver o capítulo 6.12141	_
	6.5	Abe	rtura	a permanente	_
	6.6	Intr	oduz	zir PIN	)
	6.7	Cod	ifica	r meios	)
	6.8	Prot	tocol	o de autorização143	}
	6.9	Defi	iniçõ	es da aplicação AirKey144	ŀ
	6.9.	1	Def	inições da aplicação AirKey em smartphones Android 144	ŀ
	6.9.	2	Def	inições da aplicação AirKey em iPhones144	ŀ
	6.9.	3	Def	inir o alcance do modo hands-free145	)
	6.9.	4	Мос	do Hands-free (mãos livres)146	5
	6.9.	5	Des	bloqueios a partir de notificações146	5
	6.9.	6	Fun	ções de segurança147	7
	6.	9.6.	1	Ativar PIN148	3
	6.	9.6.	2	Alterar PIN	)
	6.	9.6.	3	Desativar PIN	)
	6.9.	7	Not	ificações151	_
	6.9.	8	Adio	cionar sistema de controlo de acessos153	3
	6.9.	9	Tro	ca de smartphone	3
	6.9.	10	Info	o 153	3
	6.10	A	tuali	zar o smartphone154	ł
	6.11	С	onec	te com o componente	5
	6.12	A	utori	ização especial "autorização de manutenção"	5
	6.13	A	dicio	nar um componente AirKey158	3
	6.13	3.1	Adio	cionar meios: ver o capítulo 4.12159	)
	6.13	3.2	Adio	cionar componente de bloqueio: ver o capítulo 4.11	)
	6.14	R	emo	ver um componente AirKey 159	)
	6.15	D	ados	s protocolares da aplicação AirKey161	_



	5 V	ista geral da função Hands-free (mãos livres)162
7 U	tilizaçâ	io dos componentes de bloqueio AirKey 165
7.1	Ace	sso com o smartphone165
7.2	Ace	sso com meios como cartões, porta-chaves, pulseiras ou chaves combinadas 166
8 O	peraçã	io e manutenção do sistema AirKey167
8.1	Atu	alizar componentes de bloqueio167
8.2	Atu	alizar o smartphone: ver o capítulo 6.10169
8.3	Atu	alizar meios
8.4	Atu	alizar firmware de componentes de bloqueio172
8.5	Atu	alizar a versão de meios Keyring177
8.6	Atu	alizar a versão da aplicação do smartphone181
8.7	Sub	stituição das pilhas e alimentação de emergência
8.	.7.1	Substituição das pilhas no cilindro AirKey182
8.8	Оро	;ões de reparação184
8.	.8.1	Emitir e instalar componentes de bloqueio de substituição184
8.	.8.2	Desinstalar o componente de bloqueio sem ser substituído e marcá-lo como
"c	com de	:feito"
8.	.8.3	Desinstalar o componente de bloqueio através do smartphone
8. Ai	.8.4 irKey	Desinstalar o componente de bloqueio através da Administração online do 192
8.	.8.5	Reverter tarefas de manutenção para opções de reparação193
9 M	eios d	e emergência
9.1	Em	
		itir meios de emergência194
10 M	ledia re	itir meios de emergência194 eplacement
10 M 10.1	ledia re 1 T	itir meios de emergência
10 M 10.1	ledia re 1 T 0.1.1	itir meios de emergência
10 M 10.1 10	ledia re 1 T 0.1.1 0.1.2	itir meios de emergência
10 M 10.1 10 10	ledia re 1 T 0.1.1 0.1.2 rabalha	itir meios de emergência
10 M 10.1 10 10 10 10 10 10 11	ledia ro 1 T 0.1.1 0.1.2 rabalha 1 A	itir meios de emergência
10 M 10.1 10 10 10 10 10 11 11.1 11.2	ledia re 1 T 0.1.1 0.1.2 rabalha 1 A 2 A	itir meios de emergência
10 M 10.1 10 11 11 11.2 11.3	ledia re 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A	itir meios de emergência
10 M 10.1 10 11 Tr 11.2 11.3 11.4	ledia re 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A 4 C	itir meios de emergência
10 M 10.1 10 11 Tr 11.2 11.3 11.4 11.5	ledia re 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A 4 C 5 C	itir meios de emergência
10 M 10.1 10 11 Tr 11.2 11.3 11.4 11.5 11.6	ledia ro 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A 4 C 5 C 5 U	itir meios de emergência
10 M 10.1 10 11 Tr 11.2 11.2 11.2 11.4 11.6 12 Ai	ledia ra 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A 4 C 5 C 5 U irKey (	itir meios de emergência
10 M 10.1 10.1 10.1 10.1 11.1 11.2 11.2 11.2	ledia ra 1 T 0.1.1 0.1.2 rabalha 1 A 2 A 3 A 4 C 5 C 5 U irKey ( 1 A	itir meios de emergência



12.3	Edi	tar chave da API
12.3	8.1 R	Regenerar chave da API 213
12.3	8.2 E	liminar chave da API
12.3	8.3 C	Desativar e ativar chave da API213
12.4	Airl	Key Cloud Interface – Ambiente de teste
12.4	l.1 G	Gerar dados de teste
12.4	1.2 0	Gerar chave para a API
12.4	4.3 R	Repor dados de teste
13 Sina	lizaçã	o dos componentes de bloqueio 217
14 Valo	res e	limites do AirKey
14.1	Adr	ministração Online do AirKey
14.2	Cor	nponentes de bloqueio AirKey219
14.3	Car	tões, porta-chaves, pulseiras ou chaves combinadas
14.4	Apl	icação AirKey
15 Qua	ndo s	ão debitados os KeyCredits? 220
16 Reso	olução	de problemas
16.1	A c	omunicação não é possível no sistema221
16.2	0 c	componente de bloqueio tem dificuldades em reconhecer o meio ou não
reconh	nece n	nesmo
16.3	Os	meios já não são reconhecidos 221
16.4	Não	o é possível desenroscar o puxador de um cilindro AirKey
16.5	0 c	componente de bloqueio sinaliza um "Erro de hardware"
16.5	5.1 C	Cilindro AirKey
16.5	5.2 L	eitor de parede AirKey 223
16.6	Οp	puxador eletrónico está perro 223
17 Indi	caçõe	s importantes
17.1	Sis	tema
18 Deta	alhes	técnicos da interface RS485 para leitores de parede com Bluetooth 225
18.1	Ativ	var interface RS485 para leitor de parede com Bluetooth
18.2	Cor	nfiguração da porta de série RS485226
18.3	Esp	pecificação APDU do registo protocolar do acesso bem-sucedido 227
18.3	8.1 A	PDU do registo protocolar
18.3	8.2 R	Registo protocolar de 14 bytes 227
18	3.3.2.	1 Formato Timestamp 227
18	3.3.2.2	2 Unlocking status (Estado de desbloqueio) 227
18.3	8.3 E	xemplo
19 Decl	aracã	o de conformidade 229



20	Declaration of Conformity 2	231
21	Índice das figuras 2	233
22	Glossário 2	241
23	Ficha técnica 2	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 <u>Termos</u> <u>e condições gerais de negócios</u>, bem como nas suas <u>Condições gerais de licenciamento</u> 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 <u>https://www.evva.com/int-en/aboutus/contact/international/</u>.

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

Poderá obter informações gerais sobre o AirKey na nossa homepage em <u>https://www.evva.com/pt/airkey/website/</u>.



## 2.3 Esclarecimento dos símbolos

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

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

Atenção, perigo de danos, caso as medidas de precaução não



Indicações e informações adicionais

Sugestões e recomendações



Mensagens de erro

sejam respeitadas.

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

Alt + 
 (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 Alt +  $\blacktriangleleft$ .



# 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.





## **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<sup>\*</sup>.

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 <u>utilização de componentes de bloqueio AirKey</u>.



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 <u>https://www.evva.com/pt/downloads/</u>.

O cilindro AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em <u>Sinalização dos componentes de bloqueio</u>.

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

<sup>\*</sup> 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 eletrónica, 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 <u>https://www.evva.com/pt/downloads/</u>.

O cilindro híbrido AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em <u>Sinalização dos componentes de bloqueio</u>.

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 eletrónica 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 semautorização.

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 <u>https://www.evva.com/pt/downloads/</u>.

O cilindro de patilha AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em <u>Sinalização dos componentes de bloqueio</u>.

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 <u>https://www.evva.com/pt/downloads/</u>.

O cadeado AirKey possui uma sinalização ótica e sonora. Poderá encontrar a explicação dos diferentes sinais em <u>Sinalização dos componentes de bloqueio</u>.

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 <u>https://www.evva.com/pt/downloads/</u>.

### 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 <a href="https://www.evva.com/pt/downloads/">https://www.evva.com/pt/downloads/</a>.

## 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<sup>™</sup> a partir de 5.0 (apenas possível a funcionalidade NFC)
  - Android<sup>™</sup> a partir de 6.0 (NFC e Bluetooth)



- Apple<sup>™</sup> 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 <u>lista de smartphones compatíveis</u>.



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 <u>autorização da localização</u> 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 <u>https://www.evva.com/pt/downloads/</u>.



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 <u>https://www.evva.com/pt/downloads/</u>.

## 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 <u>Meios de emergência</u>. 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 <u>Substituição das pilhas e Alimentação de emergência</u>.



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 <u>https://www.evva.com/pt/airkey/website/</u>, 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 <a href="https://www.evva.com/pt/downloads/">https://www.evva.com/pt/downloads/</a>.

> Vídeos:

Na homepage <u>https://www.evva.com/pt/airkey/website/</u> 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 <u>https://airkey.evva.com</u>.
   Abre-se a página de login da Administração online do AirKey.
- > Selecione o seu *idioma*.
- Clique no link *Registo AirKey* **1**.

🕢 Language:	AirKey   Login	ccess to accurity
User ID: Password:	User ID Password Log in	Forgot your password?
?) AirKey Support	Legal notice	1 AirKey registration

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 <u>Termos e condições gerais de negócios</u> e a caixa de seleção com o link <u>Condições gerais de licenciamento</u> 2. Os dois respetivos documentos PDF são abertos automaticamente. Estes documentos estão disponíveis em <u>https://www.evva.com/pt/airkey/impressum/</u>.

Register to AirKey	English
fease enter at least the marked fields ime. Dur EVVA AinKey team wishes you pl	and register to keep. The you will notice a confirmation e-wai with your serv D and a registration lost. Prease set your parameter by following this link. Alterwork the registration is finited. Then enter your user D and paramet and tog in to the Anter unless administration of UVA. For the first ing of explorement when using the workloads by dynamet.
Business customer  Private	Optioner
AirKey account	
Title	lite •
* First name	Partname
* Last name	Laaf name
*t-mail	E-mi.
Street	
Postcode	Pestod Gy Ch-
Country Teleshore comber	Hazar Crosse
fax	Fig.
My access control system	
Access control system name	Access control system name
* Time zone	Please choose -
Issue enter the text of the picture is the another picture.	the the folder of the folder o



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**  $\rightarrow$  **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 **0**.



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.

Fitzwilliam , welcome to AirKey!
We are happy that you handle your key exchanges worldwide and in a matter of seconds by the internet.
To finish your AirKey registration, please specify a password by following the link: <a href="https://uat.airkey.evva.com/activation.html?">https://uat.airkey.evva.com/activation.html?</a>
If you successfully finish your registration within 48 hours, the following data for you as an AirKey customer are valid:
Your customer number is: Your user name:
With kind regards, your AirKey-Team
Click here to log in to the AirKey online administration <u>https://airkey.evva.com</u> Our terms and conditions and terms of licences can be found at <u>http://redirect.evva.com/airkey/en/agb</u>

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 carateres 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.



EVVA) AirKey		
Welcome to AirKey		English
Complete registration to the AirKey onli The password must contain at minimum You will need your date of birth later fo Please enter your new AirKey password	s admeniatation by vetting your pressnord. d waacher, an immunim one dig it a well as one upper case and one lower case letter. It is in the interest of safety that your parawood is as long as possible and you keep it secret. In them paramoter the function.	
* Password		
* Repeat password	Repeat password	
* Date of birth		
AirKey Support		AirKey registra

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 <u>https://airkey.evva.com</u>.
   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.

EVVA AirKey	RS 🕡 HELP	() Credit & JoyCost() Administrative	English • Etings $\phi$ in Log off
lone			
Media & persons	+ Add Access control system		+ Add
114 Presents 2 Sametylevers 2 Cardo	"General a Keys" Decer 2	1 Cylorber Composent ID Composent ID Costof 774607020M	4 Areas
Pertocal	Access control system	i: Test É, Evva	Castomer number: airkey_SUHXLAFHBO
342 Looking component protocol	Defail: holiday:     7 public holiday:	16 year 2018 a EuropeoVienna, UTC +62:00 💥 Tape up	Credit Settings
efermation General Terms of Business (GTB)	Imprint	l Final user licens	e agreement (TULA)

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.

you wish, we will guide you through the initi	al installation after clicking on	"Start wizzard".		
ou need the following components:				
			-	
	A	V		
			1 · · · · ·	
	11-			
		2.		
0000				
Locking components	Access media	KeyCredits	Smartphone	
you do not need the interactive help, click or	Directly to the AirKey online	administration" to begin the se	elf-administration.	
he between allow he he was he willow at any time of	ia the menu item "HELP"	3		

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.

Add credit	3 Wall reader
	2 Mair
To recharge credit, hold your KeyCredit c	ard ready and click "Add credit".
🗲 Back	Skip Scredit(s)
enna, UTC +02:00 🔆	Add credit



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, selecione, no menu principal, **Ajuda**  $\rightarrow$  **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 <u>Registo na</u> <u>Administração online do AirKey</u>).

- > Conecte a estação de codificação numa porta USB do seu computador.
- > Clique na Administração online do AirKey no sinal + à direita em baixo **0**.



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.





0

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".

Y <mark>ou h</mark> ave chosen to	open:
AirKey.jnlp	
which is: JNLP	File
from: https://	uat.airkey.evva.com
What should Firefo	x do with this file?
Open with	Java(TM) Web Start Launcher (default)
Save File	
🔲 Do this auto	matically for files like this from now on.
	OK Cancel

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.

	No coding station activated	
	Select a coding station for use.	
	O2Micro CCID SC Reader 0 OMNIKEY CardMan 5x21 0	*
1	OMNIKEY CardMan 5x21-CL 0	-

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 <u>https://airkey.evva.com/smkrest/jnlp/newest-jar-file/</u> 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 <u>AirKey Cloud Interface (API)</u>.
- -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 , o diretório de trabalho e as estações codificadoras disponíveis.

📾 Administrator: C:\Windows\system32\cmd.exe - java -jar smk-web-start-container-11.10.10-produ 🗖 💷 💌
D:\AirKey_Codierstation_Applets\Onlineverwaltung>java -jar_smk-web-start-contain
er-11.10.10-production.jar 2019-04-05 11:32:08.087 [INFO] Config directory: C:\Users\f.diener\.airkey 2019-04-05 11:32:08.088 [INFO] Work directory: D:\AirKey Codierstation Annlets\0
nlineverwaltung\EUUA AirKey 2019-04-05 11:32:08,225 [DEBUG] Sound active: true
2019-04-05 11:32:08,781 LINFOI ProxyBrowserApplet started 2019-04-05 11:32:08,782 [INFO] OS Name: Windows 7 2019-04-05 11:32:08 782 [INFO] OS Neme: 6 1
2019-04-05 11:32:08,782 [INFO] OS Arch: x86 2019-04-05 11:32:08,784 [INFO] <u>H</u> eadless sync mode started
2019-04-05 11:32:08,795 [DEBUG]HL action result: {"methodName":"cardReaderListC hanged","parameters":["HID Global OMNIKEY 5022 Smart Card Reader 0"]} 2049-04-05 11:22:09 292 [UNCO] Satting action reader to: UID Clobal OMNIKEY 5022
Smart Card Reader 0 Apr 05, 2019 11:32:80 AM org.apache.coyote.AbstractProtocol init
INFORMATION: Initializing ProtocolHandler ["http-bio-127.0.0.1-50743"] Apr 05, 2019 11:32:09 AM org.apache.catalina.core.StandardService startInternal
Apr 05, 2019 11:32:09 AM org.apache.catalina.core.StandardEngine startInternal INFORMATION: Starting Servlet Engine: Apache Tomcat/7.0.88
Apr 05, 2019 11:32:09 AM org.apache.coyote.AbstractProtocol start INFORMATION: Starting ProtocolHandler ["http-bio-127.0.0.1-50743"]
4

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 excludedportrange 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  $\rightarrow$  Dispositivos de software  $\rightarrow$  Microsoft UICC ISO Reader  $\rightarrow$  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"  $\rightarrow$  Configuração de computador  $\rightarrow$  Modelos administrativos  $\rightarrow$  Componentes do Windows $\rightarrow$  Smart Card
- Clique duas vezes na linha com a entrada "serviço Smart Card Plug & Play" do lado direito.

Editor de Políticas de Grupo Local			-	
<u>Eicheiro Ação Ver Ajuda</u>				
🗢 🏟 🙍 📷 🗟 📾 🕅 🖘				
Jondo Argo 2 a Bodo      Argo 2 a Bodo      Argo 2 a Bodo      Serviço do Registo de Eventos     Serviço do Registo de Eventos     Serviço do Registo de Eventos     Serviço do Informação Internet     Shall Remota do Windows     Sistema Ade Cores do Windows     Windows Defender SmantScreen     Windows Defender SmantScreen     Windows Defender SmantScreen     Windows Defender SmantScreen     Windows Mobility Center     Windows Update     Windows Update     Windows Update     Windows Update     Windows     Windows     Sude do Coreshol     Sistema de Tarefas	Smart Card      Ativar serviço Plug and Play de     Smart Card      Editar <u>definição de política</u> Requisitos:     Pelo menos, Windows Server 2008 R2     ou Vindows 7      Descrição:     Esta definição de política permite     controlar se o Plug and Play de Smart     Cards é ativado.     Se ativar ou não configurar esta     definição de política, o Plug and Play     de Smart     Cards cards ativado e     sistem a tentrá instalar um     controlador de dispositivos Smart     Card quando for inserido um carbáo     num Leitor de Smart     Card quando for inserido um carbáo     num Leitor de Smart     Card quando for de Smart     Se destivar esta definição de política,     Se destivar esta definição de política.	Definição Permitir cartificados sem atributo de certificado de utilização de chaves expandidas Permitir claves de assinutura válidas para liniciar sessão Permitir citaricados com nos anivalida Atriva propagação de certificados a partir de smart card Configurar Impesa de certificados de rais a partir de smart card Atriva propagação de certificados de rais a partir de smart card Atriva propagação de certificados de rais a partir de smart card Atriva propagação de certificados de rais a partir de smart card Atriva propagação de certificados de rais a partir de smart card Permitir a utilização de extificados de rais a partir de smart card Permitir a utilização de certificados de seis de utenticação Firtar certificados de inicial esseis de utenticação Firtar certificados de inicial esseis de utenticação Inverter o nome do requerente amacensado num certificado a papesentá-lo Notrificar utilizardo e rintata pada de controlador de smart card Notrificar utilizado e de inicial esta de controlador de smart card Notrificar utilizado e de inicial esta de controlador de smart card Notrificar utilizado e de inicial esta de controlador de smart card bem sucedida Permitir sugestão para nome de utilizador	Estado Não configurado Não configurado	Comentár Não Não Não Não Não Não Não Não Não Não
<ul> <li>Painel de Controlo</li> <li>Rede</li> <li>Servidor</li> <li>Sistema</li> <li>Todas as Definicões</li> </ul>	o Plug and Play de Smart Cards será desativado e não será instalado um controlador de dispositivos quando for inserido um cartão num Leitor de Smart Card.			
Gonfiguração do utilizador     Definições de software     Definições do Windows     Modelos administrativos	Nota: Esta definição de política é apenas aplicada para smart cards que tenham passado no processo de teste Windows Hardware Quality Labs (WHQL).			
< >> 16 definições	Expandidos Padrão			

Figura 21: Editor de Políticas de Grupo Local

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



						_			
Ativar serviço Plug	and Play de Smart	Cards					_		×
Ativar serviço Plug	and Play de Smart	Cards		Definição	An <u>t</u> erior	Defi <u>n</u>	jição Segui	inte	
○ Não <u>C</u> onfigurado	Comentário:								^
⊖ Ati <u>v</u> ado									
<u>     D</u> esativado									~
	Suportado em:	Pelo menos,	Windows Ser	ver 2008 R2 o	u Window	s 7			^
									~
Opções:			Ajuda:						
			Esta definiç Smart Card Se ativar ou Play de Sm controlado cartão num Se desativa Cards será dispositivo Card. Nota: Esta cards que t Hardware C	ão de polític s é ativado. 1 não configu at Cards ser 1 de dispositi 1 Leitor de Sn r esta definiç desativado e s quando for definição de enham passa Quality Labs (	a permite Irar esta de á ativado e vos Smart nart Card p ão de política não será ir inserido u política é a ido no pro WHQL).	controla efinição : o sister Card qu bela prin tica, o P nstalado m cartã apenas a cesso do	de política ma tentará iando for i neira vez. lug and Pl um contr o num Leir iplicada pa e teste Wir	g and Play a, o Plug a instalar u nserido u ay de Sma olador de tor de Sm ira smart idows	r de ^
					OK		Cancelar	<u>A</u> pl	icar

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 <u>Utilizar a estação de codificação através da linha de comando</u>). 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.



The second		g monocour age research	1005			
tie die 8 persons			<b>+</b> Add	Access control system		
290 Persons	4 Smartphones	4 Cards	"Send a Kry"	2 Cylinders	1 Wall reader	
				Door dissignation Component ID Back door 00550822C22AD98 Wandleser 1 0005657246D1923A	Maintenance tasks	2 Maintenance tasks
tocol				Access control system: Test I. Evva		Customer number: airkey_\$5003
486 Locking component prote	ocol 968 Media pr	otacol	Tik System protocol	(j)) Public holdays B public holdays this year 7 public holdays in 2018 (c) Time zones Delault time zones is EuropetVienna, UTC +02:00 🔆		ayovattai

Figura 23: Créditos

- > Obtém uma visão global dos créditos atuais e dos carregamentos já efetuados.
- > Clique no botão **Adicionar crédito 0**.

redit					
Quantity of credits 37 KeyCredit(s) Time credit None					
				Add cre	dit
redit protocol	Administrator (Licor ID)	Credit code		1 J Add cre	dit
redit protocol Date, time	Administrator (User ID)	Credit code	C Inte Default t	Details	dit
Tredit protocol Date, time 30/05/2017 15:56	Administrator (User ID) John Smith (13968155)	Credit code 2JJL-9GGX-QS85-85Y	V-BZ5Q	Details Credit added: 100 KeyCredit(s) added, new credit: 102 KeyCredit(s)	sdit

Figura 24: Adicionar crédito

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

A	dd credit
Enter a credit code to add days or KeyCredits	to your credit:
X Cancel	Add credit

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.



	u	edit for access control system. Pitzwilli	3111	
redit				
Quantity of credits				
17 KeyCredit(s)				
Time credit				
None	harned your credits by 10 KeyCred	it/s)		
Vou have rec	harged your credits by 10 KeyCred	it(s).	O Top-up crea	lit
None You have rec redit protocol Date, time	harged your credits by 10 KeyCred Administrator (User ID)	it(s). Credit code	Result	lit

#### 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*  $\rightarrow$  *Criar pessoa*.
- > Ou selecione no menu principal **Meios e pessoas**  $\rightarrow$  **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**.

) AirKey		I Croft Ant Smith Adventure I English • 445 Setting
ACCESS CONTROL SYSTEM	IDIA & PERSONS III PROTOCOLS 🔔 ADMINISTRATIONS 😰 HELP	
Create nerroe		
Create person		
Details		
* First name	First name	
* Lasit name	Last name	
Identifier	identifier	
Gender	Tease select +	
Date of birth	DOMENTRY II	
Contact details		
E-mail address	E-mail address	
Telephone number	Telephone number	
Street	direat	
Pesicode	Postcode	
City	Dity	
· Lanauae for correspondence	Deutsch	
Remarks		
Comment		
		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



pessoas 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 carateres. Para "CP" só podem ser utilizados, no máximo, 10 dígitos. No campo do comentário, poderá inserir um texto com um máximo de 500 carateres.

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 0**.

Edit person		
Details		
Details		
* Best av	rre Mat	
* Last re	w Nuteman	
Ident	fer 195	
Ger	Arr Male •	
Date of b	eb 29/12/2001 ())	
Contact details		
E-mail add	xx m muskemann@amail.com	
Telephone num	43122466	
9	eet Haudstrate 1	
Posto	ada 1010	
	Jay Witen	
Cou	ty Audita ·	
<ul> <li>Language for corresponde</li> </ul>	xe fallano •	
Remarks		
Comm	red	
Download transfer co	fermion	

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.

EVVA) A	irKey		() an Keyl	Creditol Administrator English	• Settings (c)
HOME 🔒 ACCES	SS CONTROL SYSTEM	PROTOCOLS 🕹 ADMINISTRATORS 👔	HELP		
rsons					📑 Import
Eirstnama Lastnama	Identifier E-mail address				
(That name, cast name,					
First name	Last name	↑ Identifier	E-mail address	Number of media	Media status
First name Horst	Last name Bäcker	↑ Identifier	E-mail address	Number of media 0	Media status
First name Horst Florian	Last name Båcker D	▲ Identifier	E-mail address	Number of media 0 1	Media status
First name Horst Florian Adrian	Last name Bicker D H	▲ Identifier	E-mail address	Number of media 0 1 1	Media status
First name Horst Florian Adrian Peter	Last name Bicker D H Hkber	Identifier	E-mail address	Number of media 0 1 1 0 0	Media status
First name Horst Florian Adrian Peter Anna	Last name Bicker D H Huber Muller	Identifier	E-nul addres	Number of media 0 1 1 0 0 0 0 0	Media status

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 **1**, 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.

	ACCESS CONTROL SYSTEM	MEDIA & PERSONS	PROTOCOLS	adn
	Create person			
	Details			
New person				
	Details			
	1 * First name	First name		
	2* Last name	Lastname		
	3 Identifier	Identifier		
	4 Gender	Please select 👻		
	5 Date of birth	DD/MM/YYYY 31		
	Contact details			
	6 E-mail address	E-mail address		
	Telephone number	Telephone number		
	8 Street	Street		
	9 Postcode	Postcode		_
	Country	City Please select	_	
	12*Language for correspondence	Deutsch -		
(	3 Remarks			

#### Figura 30: Importas pessoas - Lista de pessoas

The second														
	<mark>⊌ "</mark> ) • (°' -   <del>•</del>	·				AirKey - Import pe	ersons - Excel template 2.5.	xisx - Microsoft	Excel				_ 0	$\mathbb{Z}$
D	atei Start I	Einfügen Seitenla	ayout Formeln	Daten	Überprüfen Ansich	t Entwicklertools							♥ 🕜 🗆 6	F 83
	M9	<b>v</b> (n	f <sub>sc</sub> Person 2 =	duplicate!										^
														-
										_				-
	<b>1</b> A	2 в	3 C	4 D	6 E	6 F	🕖 G	\rm В н	9	1 III I	🛈 к	12 L	<b>13</b> M	[ <b>^</b>
	1) First name	2) Last name	3) Identifier	4) Gender	5) Date of birth	6) E-mail address	7) Telephone number	8) Street	9) Postal code	10) City	11) Country	12) Language for	13) Comment	
	(mandatory,	(mandatory,	(max. 50 char.)	(M / F)	(YYYY-MM-DD)	(max. 50 characters)	(to be formated as text,	(max. 50 char.)	(max. 10 char.)	(max. 50	(see Excel	correspondence	(max. 250 characters)	
	max. 50 char.)	max. 50 char.)					max. 50 characters)			cnaracters)	comment)	(mandatory, see		
1												Excercomment)		_ =
2														
3	Smallest	Record										en-UK		
4		Öul	40		1007 12 20	14.0	42 664 422 456 700	Calification A	1120	146	AUT.	1.05	Caradal share & F. O	
5	Anna	Utker	AU	F	1997-12-20	email1@gmx.com	+43 004 123 450 789	Schone Str. 1	1130	wien	AUT	de-DE	Special char.: 0, o, is	
0	Jan	Cesky	J.C.	M	1964-05-17		+420 111 222 333 444	Pripotocni 13	101 00	Prag	CZE	CS-CZ	Special char.: C, I, r, y	
/	0	- 10											-	4
8	Dany	Devito	DD									en-UK	Person 1	
9	Dany	devito	Ua									en-UK	Person 2 = duplicate	-è
10	Aug													
11	Attention!	ivianual line bre	eaks are not all I	oweat								en-UK	1	
H -	Import	persons 🏷						11						
Breit 🖸 Anzahi: 10 🗰 🛄 100 % 🖯									6 <del></del>	+) .:				

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 carateres 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 caráter @ e outros carateres ou ficar vazio.
- O país para o endereço (campo 10) tem de conter o <u>código ISO 3166-1 alfa-3</u> 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 <sup>1</sup>), 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; DeVito; DD" e "Danny; deVito; 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 carateres do ficheiro CSV tem de ser UTF-8 para que as letras específicas do país ( $\ddot{A}$ ,  $\beta$ ,  $\varsigma$ ,  $\tilde{N}$ ,  $\check{c}$  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<sup>™</sup> utilizando o Microsoft Excel<sup>™</sup> e os programas de ajuda já disponíveis no Windows 10<sup>™</sup>. 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 carateres 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 carateres:
  - " (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*  $\rightarrow$  *Guardar como* (ou prima a tecla F12).
- Insira na janela de diálogo subsequente "Guardar como" o nome do ficheiro pretendido 1.
- Selecione na lista dropdown de Guardar com o tipo 2 o formato Texto Unicode (\*.txt).
- > Clique em **Guardar §**.



			18010177115 11077	Pile miner	
1 File name:	Persons to import.txt				-
2 Save as type:	Unicode Text (*.txt)				-
Authors:	AKADEMIE3 / EVVA Wi	Tags: Add a tag		Title: Add a title	
Hide Folders			Tools	▼ Save Ca	incel

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.

Person	s to be impo	orted.txt - No	otepad										
File Edit	Format	View Hel	p										
1) Firs 7) Tele	t name ( phone nu	mandator mber (to	y) b be f	<ol> <li>Last name ormated as text)</li> </ol>	(mandatory) 8) Street	<ol> <li>Identifier</li> <li>Postcode</li> </ol>	4) Gender (M / 10) City	F) 5) Date 11) Country	e of birth 12) Langu	(כנננ) age fo	MM-TT) 6) E-ma r correspondence	il address 13) Comment	*
Smalles	t	Record						en-UK					
Anna Jan	ötker Český	AÖ J.Č.	F M	1997-12-20 1964-05-17	email1@gmx.com +420111	+43 664 123 45 222333444	6 789 Schöne Přípotočni 1337	Straße 1 1130 101 00 Prag	Wien A CZE d	AUT IS-CZ	de-DE "Specia "Special charac	l characters: ters: Č, í, č,	ö, ö, ř, ý
Dany Dany	DeVito deVito	DD DD					en-UK en-UK	Person 1 Person 2!					- 1

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 caráter relativo ao espaço de tabulação, pois este caráter não pode ser digitado aqui diretamente.
  - Insira no campo **Substituir por** um ponto e vírgula (;).
  - Clique em *Substituir tudo* **0**.



Replace		
Find what:		Find Next
Replace with:	;	Replace
	0	Replace All
Match case	:	Cancel

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 1. Será mais complicado executar uma renomeação posteriormente!
  - Selecione na lista dropdown *Codificação* ❷ o formato UTF-8.
  - Clique em *Guardar* **s**.

File name:	Persons to be imported.csv
Save as type:	Text Documents (*.txt) 🔹
Hide Folders	2 Encoding: UTF-8 Save Cancel

Figura 36: "Editor" - Guardar como - inserir, manualmente, a terminação .csv do ficheiro e selecionar 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**  $\rightarrow$  **Pessoas**.
- Clique à direita em **Importar 0**.



EVVA A	irKey			1 Credit Administrator	nglish 🔹 🏥 Settings 🤞 📗 Log off
ACCES	S CONTROL SYSTEM	PROTOCOLS	ADMINISTRATORS 👔 HELP		
Persons					1 B Import
First name, Last name,	Identifier, E-mail address				
First name	Last name	Identifier	E-mail address	Number of media	Media status
Horst	Bäcker			0	- 4
Florian	D			1	
					~
Adrian	н			1	
Adrian Peter	H Huber			1	
Adrian Peter Anna	H Huber Müller			1 0 0	
Adrian Peter Anna Maria	H Huber Müller Müller	123456		1 0 0 0	· · ·
Adrian Peter Anna Maria Max	H Huber Müller Müller Mustermann	123456 190	m.mstemanagenal.com	1 0 0 0 0	

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 0**.

Row	First name	Last name	Identifier	Date of birth	E-mail address	Telephone		0
						number		0
3	Max	Mustermann	190	13/11/2001	j.smith@gmail	43123456	<u> </u>	0
2	John	Smith	111	12/11/2001	j.smith@gmail	43123456	× .	0
4	John	Smith	113	14/11/2001	j.smith@gmail	43123456	×	0
5	John	Smith	114	15/11/2001	j.smithgmail.com	43123456	×	0
how 1 t	ow 1 to 4 of 4 entries, 10 V Entries per page						The following errors occurred with the data > Gender must be either M or F. > The input e-mail address is invalid.	

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*.

	Import persons	8
2 persons have been im	ported successfully.	
	Row3: Person already available. Row5: Gender must be either M or F. Row5: The input e-mail address is invalid.	
Export result	3/3	✓ Close

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 <u>Atribuir meio a uma</u> <u>pessoa</u>. Autorizações de acesso idênticas podem ser reproduzidas em duplicado rápida e facilmente. Poderá encontrar informações a este respeito em <u>Duplicar meio</u>.



#### 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.

- > Ou selecione, na página inicial *Home*, a caixa de seleção *Smartphones* →
   *Adicionar meio*.
- > Ou selecione no menu principal **Meios e Pessoas**  $\rightarrow$  **Adicionar meio**.

		Add medium	$\otimes$
Please select	t the type of th	he new medium:	li e
scend G600 (	An +4	04	
365 (12		664 59 41 411 664 83 45 879	<b>M</b>
Galacy Sr	nartphone		Card
Add a new r	medium of typ	e "smartphone".	
X Cance	el	1/2	1 🔿 Next

Figura 40: Novo meio smartphone ou cartão

- > Selecione como novo meio *Smartphone* e clique em *Seguinte* **0**.
- 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**.

	Add medium	8
Media tune Sma	atabone	
media type one	in the local sector of the	
Designation	+43 664 59 41 411	
Designation		
* Telephone numb	er asoo	
+43 664 123		

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* **1**, caso não tenha sido ainda criado nenhum código de registo.

A HOME		
HI HOME III		
	Edit medium	
	Authorisations Details Protoco	Reload view
No person	Assign the medium to a person to creat	ate authorisations.
•	Media type Media ID	Smartphone -
	Designation	Designation
+4312312345	Status	-43123123400400
W	Last update	
	App version	-
	Registration	
	Progress	Registration has not been started. Create a registration code for this for the medium.
	Registration code	Create registration code 1
	Settings	
	Maintenance mode	Activate special authorisation "maintenance mode" for this smartphone. You have to assign the medium to a person in order to activate maintenance authorisation.
	Office mode	Medium can activate office mode
	Show protocol data	Show protocol data in the AirKey app.
	Release duration	Normal release duration

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.

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

Figura 43: Código de registo

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

Settings	
Maintenance authorisation	This smartphone can be used to perform additional maintenance operations on AirKey components
Office mode	✓ Medium can activate the manual office mode
Show event log data	✓ Show the medium event log of the smartphone in AirKey app 🚇
① Release duration	Normal release duration     Extended release duration
PIN code of the AirKey app	No PIN code set
Update after each access	Activated (the AirKey app data on the smartphone is updated after each access)

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 <u>abertura permanente automática</u>. 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 <u>Geral</u>.

#### 4.9 Registar 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.



14:08	al 🗟 🕑
Add access o	control system
Please enter your telephone	number.
Your telephone number	(e.g. +44 7770 123)
Scan QR code	
Cancel	Continue
Registration code	e already received

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.

Add access	s control s	system
Please enter t registration co from the adm access contro link in the last	the 12-digit ode that you inistrator of ol system or t SMS from a	received the tap the AirKey.
SCAN QR CODE		
	CANCEL	REGISTER

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, selecione, no menu principal da aplicação AirKey, **Definições** → **Adicionar sistema de controlo de acessos**. Poderá encontrar mais informações a este respeito no cpítulo <u>Utilizar o smartphone em vários sistemas</u>.



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.



# 0

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 <u>Troca de smartphone</u>.

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 <u>Troca de smartphone</u>.

- > Na página inicial *Home*, selecione a caixa de seleção *Smartphones*.
- > Ou selecione na linha de cabeçalho à esquerda **Meios e pessoas**  $\rightarrow$  **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 <u>Ativar PIN</u>.

#### 4.9.1 Função "Send a Key"

Poderá enviar a todas as pessoas que possuírem 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".



EVVA Ai	rKey				
ACCESS	CONTROL SYSTEM	MEDIA & PERSONS	EVENT LOGS	ADMINISTRATORS	HELP
Home Media & persons					+ Add
5 Persons	29 Smartphones	5	Cards	"Send a Key"	2 Pending smartphone replacement operations
At least 1 Android	smartphone uses an outdated on (7.5) available ①	AirKey app version (les	s than 1.6.5). 🛈		

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*.

	"Send a Key"	8
With "Send a Key" you can create new smar authorisations. Or you use the function to send authorisatic Enter the following in the search bar to star Person, Identifier, Designation, Telephone	tphones, register them, and then immediately send them ons to existing smartphones. t the function: number, Media ID	
X Cancel	Q Treate new	



> 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 <u>Informações gerais</u> para obter informações sobre definições gerais.)

A new person and a new sr	martphone assigned to the person will be created.
* First name	First name
* Last name	Lastname
ID	ID
* Telephone number	Telephone number
*Language for correspondence	English v
Notification text	Have fun opening doors with AirKey
The registration code will b	34/15%
The registration code will b	be automatically sent to the specified telephone number by sk

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.

 Messages
 Image: Compare the second secon

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 <u>Troca de smartphone</u>.)



Cancer	Add access cont	rol system	Continu
Please enter	your telephone num	ber.	
Your telephor +4312345	ne number (e.g. +44 7 6789	770 123)	0
🐯 Scan (	QR code		
	Cancel	Continue	
1	2	I	3 DEF
1 сні	2 лес 5 хкг		3 DEF 6 MNO
1 оні 7 раяs	2 480 55 51 8 107		З def Mno 9 wxyz
1 4 7 Pars + * #	2 5 5 8 7 100 0		3 def 6 MNo 9 wxyz X

Figura 52: Registar 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.

MESSAGE	S	now
AirKey Your registra (3 minutes v	ation code for Ai alid). Code: 805	rKey 57339
Please enter code you rec of the access	the 8 or 12-digit eived from the a control system:	registration dministrator
Your regist	ration code	
Con	aal Ba	nistor
Can	cer Re	gister
	Aus "Nachrichten 80557339	
	0	-
1	АВС	3 Def
1 4 6H1	2 АВС 5 ЈКL	3 Def 6 MNO
1 4 бні 7 ракs	Z ABC 5 JKL 8 TUV	3 Def 6 MNO 9 WXYZ

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 *Registar*.

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 <u>Atribuir autorizações</u>.

		DIA & PERSONS		ISTRATORS		Come and a	St John eyCratettal Adma
HOME Delivery Home	ACCESS CONTROL SYSTEM LA Detable Edit Metal Authoritations Detable Protocol (Locting components & areas Q Authoritations (Locting components & areas Q Authoritations A	DA 6 PESONS	опосотя 🚡 Армин — Д. (Антер 	Main entrance moscrift 19 401 x 21 10 10 10 10 10 10 10 10 10 10 10 10 10	Permanent access Create new authorisation with permanent access Dealer contrast access darg a certain period lated.     Temporary access Conten new authorization with	Periodic access Create new authorisation with periodic access Cualen moved access on weekdaga.dumg a certain period sites)      Individual access Create new authorisation with	
					Create new autobasedon why access by calendar Enables access within a certain period (time) on a certain day.	Contined access types combined access types Enables any combination of several access types.	

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



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



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.

Add component	Add component Component ID: 000508E2C227AD98
Add component Component ID: 0005DF0E1B14013E	DESIGNATION Main Entrance
Main entrance       Additional information	Save the current GPS coordinates as the location in the component details.
Save the current GPS coordinates as the location in the component details. Add to the following access control system:	Add to the following access control system:
Test f. Evva CANCEL ADD	Test f. Ewa

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 **1**, estas podem ser encontradas na Administração online do AirKey no componente de bloqueio sob o separador **Detalhes** no bloco "Porta".

loor	
Door designation	Main entrance
Additional information	Additional information
Location	48.1715152 16.3295636 1
	Show in Google Maps

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 **0**.
- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos**  $\rightarrow$  Componentes de bloqueio.

EVVA AirKey					1 Credit 86 KeyCre	dit(s)
👚 HOME 🔒 ACCESS CONTROL SYSTEM 🤱 MEDIA & PERSONS 🖺 PROTOCOLS	Lange Administrators	HELP				
Locking components	Only own (2) Only exter	nal (0) 🛛 🖌 Only current (1)	Not current (1)			
Door designation (additional information)	Component type	Component ID	Number of areas	Access control system	Number of shares	Logging
Door 2	✓ Wall reader	000565F246DF929A	4	Own	0	Yes
Main Entrance	✓ Cylinder	000508E2C227AD98	2	Own	0	Yes
Show 1 to 2 of 2 entries           Add locking component         B Export						

Figura 62: Adicionar componente de bloqueio

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

nponent	$\otimes$
	$\otimes$
Shared locking component	
÷	Continue
	hponent

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*.

Door designation		
Door designation		
Additional information		
Additional information		
+ The combination of door designatio	n and additional information must be u	inique.

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.

$\otimes$
_
se
0

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.

f HOM	ACCE	ESS CON	TROL SYSTEM	MEDIA & PERSONS	PROTOCOLS	ADMINISTRATORS	HELP
Edit lock	king compon	nent					
Details	Settings A	Authorised	d media (own)	Authorised media (external)			
Details							
	Componer						
	Component Firmware v Component Last u	nt type Model nent ID version t status update	Cylinder NFC 0005DF0E1B1 Java Card appl Battery O -	4013E let 6.44, Thumb turn version 4.5 K (status from 03/07/2017 09:	4, Electronics module v 06:33) 🕒 Time correc	ersion 4.54 t 🐞 Current time zone 🚦	Blacklist up to date at
Door	Componen Firmware v Component Last u	nt type Model nent ID version t status update	Cylinder NFC 0005DF0E1B1 Java Card appl 1 Battery O	4013E let 6.44, Thumb turn version 4.5 K (status from 03/07/2017 09:	4, Electronics module v 06:33) 🛞 Time correc	ersion 4.54 t 🐞 Current time zone 🚦	$\overline{\phi}$ Blacklist up to date $\frac{d}{day}$
Door	Componen Firmware v Component Last t	nt type Model nent ID version t status update	Cylinder NFC 0005DF0E1B1 Java Card appl Battery O -	4013E let 6.44, Thumb turn version 4.5 K (status from 03/07/2017 09:	4, Electronics module v 06:33) 🚯 Time correc	rsion 4.54 t 🐞 Current time zone 🏦	General State Description of the second seco
Door	Component Firmware v Component Last u Door desig	nt type Model nent ID version t status update gnation mation	Cylinder NFC 0005DF0E1B1 Java Card appl 1 Battery O -	4013E let 6.44, Thumb turn version 4.5 K (status from 03/07/2017 09: ation formation	4, Electronics module v 06:33) 🚱 Time correc	ersion 4.54 t ` Current time zone 🗄	Glacklist up to date
Door	Component Component Component Last u Door desig Additional inforr Lo	nt type Model nent ID version t status update gnation mation ocation	Cylinder NFC 0005DF0E1B1 Baava Card appl Baava Card appl Baava Card appl Baava Card appl Baava Card appl Door design Additional inti Address or C	4013E let 6.44, Thumb turn version 4.5 K (status from 03/07/2017 09/ atton formation SPS coordinates	4, Electronics module v 06:33) (a) Time correc	ersion 4.54 t 🐞 Current time zone 🚦	Blacklist up to date

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 <u>Valores predefinidos (para todos os componentes de bloqueio recentemente adicionados)</u>.



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 <u>Codificar meios</u>.

- > Inicie a aplicação AirKey.
- > Toque no símbolo Conecte com o componente 0.





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.



Add medium	
Media ID: 00050	CDE9860F272A
Back door	
Add to the follo	wing access control
system.	
Test f. Evva	

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**  $\rightarrow$  **Meios**.
- > Clique, na lista dos meios, no meio ao qual não foi ainda atribuída nenhuma pessoa.
- Clique no botão Sem pessoa sobre o sinal + 0





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



		4	Assign medium to person	
elect a pe	erson to be assigned to medi	um "Back door (0005CDE9860F272	2A)".	
		2		
First nar	me, Last name, Identifier, E	-mail adc4		Create perso
P	First name	Last name	Identifier	E-mail address
0	Horst	Bäcker	-	·
0	Florian	D	-	
0	Adrian	н	-	
0	Peter	Huber		
0	Anna	Müller		•
0	Maria	Müller	123456	
0	Sabine	Ribits		
0	Hanspeter	Seiss	AirKey	·
0	Jane	Smith		•
0	John	Smith	111	j.smith@gmail.com
0	John	Smith	113	j.smith@gmail.com
0	Max	Mustermann	31	m.mustermann@gmail.com
0	Max	Mustermann	30	m mustermannermail.com

Figura	74:	Atribuir	pessoa	ao	meio
riguiu	/	/ (crib an	pessoa	uo	meno

- 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 0**.

	Assign medium to person	8
Medium		
Media type Card		
Media ID 0005CDE9860F272A		
Designation Back door		
Detaile		
Person		
Jane Smith		
Identifier		
E-mail		
ter Back	2/2	Assign person

Figura 75: Confirmar pessoa

- > Ver mais em <u>Atribuir autorizações</u>.

Em alternativa, poderá fazer a atribuição de um meio à pessoa através do meio. Poderá encontrar mais informações em <u>Atribuir meio a uma pessoa</u>.

#### 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**  $\rightarrow$  **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.



EVVA A HOME i	) AirKey	()] Cell Attaches At
Jare South	Edit medium Autonatore Gelali Insout C biolal iew Lasting Grapowett & Sense G (supervised) (supervised) (supervised) (supervised)	(4) But
LIARCAST. 4113136. • DOESTIT. • DOESTIT. • DOESTIT. • DOESTIT.	Arrenda      Arrenda	
+ Ansign medium	len Maria	fer last

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.

Main 0005	Permanent access  Create new authorisation with permanent access  Enables constant access during a creatin neriod (fate) Entrance 0852C227A098	Periodic access Create new authorisation with periodic access Enables repeated accesses on weekdays during a certain period (date).
	Temporary access Create new authorisation with access by calendar Enables access within a certain period (time) on a certain day.	Create new authorisation with combined access types Enables any combination of several access types.

Figura 77: Atribuir uma autorização de acesso permanente

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



New a	uthorisation – Permanent access	$\otimes$
Main Entrance 000508E2C227AD98		
Permanent access     always applicable     from	to	
X Cancel		E Save

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.

© Permanent access	Periodic access
Create new authorisation with permanent access	Create new authorisation with periodic access
Enables constant access during a certain period (date).	Enables repeated accesses on weekdays during a certain period (date). Main Entrance 000508E2C227AD98
( <del>2</del>	
Temporary access	Individual access
Create new authorisation with	Create new authorisation with
access by calefiual	Enables any combination of several

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.



000508	E2C227AD98							
Period	ic access							
from (	3/07/2017	© to	31					
		O unlimi	ted					
Add pe	riodic access							
	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday	
07:00	07:00 - 17:00							
08:00								
09:00								
10:00								
11:00								
12:00								
13:00								=
14:00								
15:00								
16:00								
17:00	-							
18:00								
Importar	t notice: Periodic a	coss suthorisation	ns are not valid for t	he component "Mai	n Entrance" and it	s defined public hol	idaus	
mponan	c notice. renoale a	cccs autionsation	is and not valid for t	ne component Mai	n chuance and it	s actinea paone non	0093.	



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

	Add periodic access				
all	Monday Saturday	<ul><li>Tuesday</li><li>Sunday</li></ul>	🔲 Wednesday 🔲 Thursday	Friday	
from	07:00	to 17:00	]	_	
	🔲 all day				
×	Cancel			💾 Save	

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.

© Permanent access	Periodic access
Create new authorisation with permanent access	Create new authorisation with periodic access
Enables constant access during a certain period (date).	Enables repeated accesses on weekdays during a certain period (date).
Temporary access	Individual access
Create new authorisation with access by calendar	Create new authorisation with combined access types
	Enables any combination of several

Figura 82: Atribuir autorização de acesso temporário

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

New auth	orisation – Temporary access 🛛 🛞			
Main Entrance 000508E2C227AD98				
Temporary access				
on 03/07/2017 all day				
from 10:00 to 13:00				
X Cancel	🔛 Save			

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.

© © Permanent access	Periodic access
Create new authorisation with permanent access Enables constant access during a certain period (date).	Create new authorisation with periodic access Enables repeated accesses on weekdays during a certain period (date)
Temporary access Create new authorisation with access by calendar Enables access within a certain period (time) on a certain day.	individual access Create new authorisation with combined access types Enables any combination of several access types.
	Main Entrance

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.

Main Entrance 000508E2C227AD98				
Individual access				
Access type	^	Validity		
No data found				
Add access (8 still p	ossible) 1			

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.

e	0
Periodic access	Temporary access
	(L) Periodic access

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.

1	Create 1 authorisation	🖨 Back

Figura 88: Criar autorização nova ou alterada

Clique no botão amarelo *Criar 1 autorização* ou no símbolo **0** 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 craida 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 <u>Definições do sistema de bloqueio AirKey</u>.



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

0

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.

EVVA AirKey					
🏫 номе	ACCESS CONTROL SYSTEM	K MEDIA & PERSONS	EVENT LOGS		
Home Failed login at	ttempts				
Failed login a	ttempts since 26/04/2019 15:43:38 (r	with the current user): 1	System event log	9	

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 <u>https://airkey.evva.com</u>.
   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 <u>https://airkey.evva.com</u>.
   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).

	AirKey   Login		
	Two factor authentication is activated for this access control system.		
	SMS code for logging in will be sent to	this number.	
* Your mobile phone number	+43123456789		
	Send SMS code	Back	
? AirKey support	Legal notice	AirKey registration	

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*.

	AirKey   Login Enter the received SMS code. SMS code sent to +43123456789	EVVA access to security
*SMS code	jklds7	Back
? AirKey support	Legal notice	AirKey registration

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 <u>Editar administrador</u>). Para esse efeito, porém, é necessário o número de telefone atualmente verificado. Se o número de telefone já não estiver disponível, contacte a <u>Assistência da EVVA</u>.

#### 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? 1**.



	AirKey   Login	<b>EVVA</b> access to security
() Language:	English -	
User ID: Password:	User ID Password Log in	1 Forgot your password?
? AirKey Support	Legal notice	AirKey registration

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*.

	Forgot your password?	8
	.og in	Forgot your passwor
If you have forgotter your date of birth.	n your password, enter your A	irKey user ID and
If you have forgotter EVVA AirKey support	n your 8-digit user ID, please c	ontact your
* User ID	User ID	
* Date of birth		
X Cancel		Reset password

Figura 94: Esqueceu-se da sua senha

Com a autenticação de dois fatores ativada, recebe um código por SMS no seu smartphone 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.)

Enter the received SMS code	<u>.</u>	
You will receive an e-mail w	th a link to reset the p	assword.
SMS code sent to0884		
* SMS code	SMS code	

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 <u>Assistência da EVVA</u>.

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*.

Reset password							
Please enter your new AirKey pass	word.						
The password must contain at least a digit [0-9], an uppercase letter [A-2] and a lowercase letter [a-2]. Country specific letters (Å, §, ç, Ñ, č, etc.) are treated as special characters and are only possible in addition to the 3 specified criteria.							
* Password	•••••						
* Repeat password	Repeat password						
	🖶 Save						
? AirKey Support							

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**.

THOME ACCESS CON	ITROL SYSTEM	Let MEDIA & PERSONS	PROTOCOLS	Lange Administrators	🕜 HE
My AirKey account					
User ID	13968155	Change password			
Title	Mr.	•			
* First name	John				
* Last name	Smith				
* E-mail address					
* Date of birth	24/09/1976	200 31			
	Note: You requ	ire the date of birth for the "Re	set password" function.		
Telephone number	Telephone nu	mber			
Street	Street				
Postcode	Postcode				
City	City				
Country	Please select	•			
Contact information					
* Language for correspondence	English	_			
1 /11 /11 // // // // // // // // // //	Englian	•			

Figura 97: A minha conta AirKey

#### 5.2 Logout do AirKey

Para sair da Administração online do AirKey, clique em **Terminar sessão 0**.

EVVA AirKey	The Credit Score Control Contr
🎓 HOME 🔒 ACCESS CONTROL SYSTEM 🎎 MEDIA & PERSONS 📋 PROTOCOLS 🍰 ADMINISTRATORS 🚳 HELP	

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**.

EVV	AirKey						The Gredit StreyCredit(s)
🏫 номе	ACCESS CONTROL SYSTEM	Letter Source Media & Persons	PROTOCOLS		1 HELP		
Home Media & perso	ons			Administrators Create administrator Support logins	Here mana system	you can find the administrator agement for your AirKey access control m.	
	117 Persons	6 Smartphones	P	((() rds	"Send a Key"	1 Cylinder	(C)) 1 Wall reader

Figura 99: Menu principal – Administradores

## 5.3.1 Criar administrador

Os administradores podem ser criados exclusivamente por outros administradores.

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

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

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.



Contact information		
* Language for correspondence	English -	
E-mail notifications	I would like to regularly receiv Daily (8:00)	e maintenance tasks from my access control system by e-mail.
	Never	mation about AirKey online administration updates and maintenance windows.
	Hourly	rtant notifications from EVVA (recommended).
	Daily (8:00)	
	Weekly (Monday 8:00)	
lemarks	Monthly (1st day 8:00)	

Figura 101: Informações de contacto

> Clique em **Guardar 1**.

EVVA) Airk	ey 🕒 🕅 Dodates 🖁 Marsonite 🕼 Marsonite 🕅 Kanglah 🔹 🖏 Settings of 👘 Langla h
ACCESS CON	IROLSYSTEM 🙏 MEDNA 9 HOSONS 📓 PHOTOCOLS 🎍 ADMINISTRADOK 🕢 HEP
reate administrator	Ф Тал
etails	1 Issee
Title	Pisse stick -
• First name	Fishname
* Last name	Lastname
*E-mail address	E-mail address
Telephone number	Telephone number
Street	Street
Postcode	Postcode
City	Oh
Country	Please select +
ntact information	
*Language for correspondence	Endeh •
E-mail notifications	woodd like to mydaify morien maintenance taolo from ny access control splem by e-mail. Daify (0.07)
	🗵 I would like to receive information about ArKey online administration updates and maintenance windows.
	E / Hound like to income important nutifications from EVW (economode)).
marks	
Comment	

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 <u>Editar</u> 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 <u>Administração online do AirKey</u>, 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**  $\rightarrow$  **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 1**.



EVVA Airk	Key	The Sector Secto
the home 🔒 access com	titol system 🏦 media 6 persons 📓 protocols 👗 administrators 🎯 help	
Edit administrator		ter Back
Details		1 📇 Save
User ID	13964155 Ouange password	
Title	lit.	
* First name	nhoi	
*Last name	Smith	
*E-mail address		
*Date of birth	2409/1976	
	Note: You require the date of birth for the "Reset password" function.	
Telephone number	Telephone number	
Street	Street	
Postcode	Postcode	
City	City	
Country	Please select •	
Contact information		
*Language for correspondence	English •	
E-mail notifications	I would like to regularly receive maintenance tasks from my access control system by e-mail.	
	Never •	
	Twolar are to recove internation about Anny owner antimototation quarters and manimization windows.     Iwould like to receive important notifications from EVIA (recommended).	
Remarks		
Comment		
		👾 Eack 👿 Deletion 🛅 Save

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.

Area de	esignatio	n	Q	
		Area designation		
		All doors		
		Garage		
ntries 1 ing con	- 2 of 2	ų.		
ntries 1 ing con Door d	- 2 of 2 nponents lesignatio	: on (Additional information), Component ID	Q	All component types v
ntries 1 ing con Door d	- 2 of 2	n (Additional information), Component ID Door designation (additional information)	٩)	All component types v
ntries 1 ing con	- 2 of 2 nponents esignatic	on (Additional information), Component ID Door designation (additional information) Entrance	٩)	All component types v
ntries 1 ing com Door d	- 2 of 2 nponents lesignatic Q	on (Additional information), Component ID Door designation (additional information) Entrance Garage	٩)	All component types v

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**.

	Authorisations Details Event log	C Reload view		Authoritant Datalla Davation	A Paland Mary
				Authorisations Details Event log	C Reload View
John Doe	(Locking components and area Q)	Authorisation Q All (0) 🖌 Up t	John Doe	Locking components and area Q	Authorisation ۹ All (0) 🖌 U
	高島 All doors 高島		0	🔒 🏯 Garage	A
Phone	음 음 Garage				
137897293789	28 28		iPhone	Garage 0005D4E50B3E6342	
0	Entrance 000543DC5F2FC63A		+437897293789	0000000000	
	Garage 0005D4F50B3E6342		00		

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

0

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**  $\rightarrow$  **Administradores**.
- Selecione o administrador a eliminar, clicando na respetiva linha da tabela. Vai para a página "Editar administrador".
- > Clique em **Apagar 1**.

Nome 🔒 Access con				
	INVESTIGATION PROFESSION PROFESSION PROFESSION			
lit administrator			i Back	W Deletic
tails				🗎 Sa
User ID	13968155 Change parased			
Title	M			
* First name	John			
* Last name	Smith			
*E-mail address				
* Date of birth	2409/1976			
	Note: You require the date of birth for the "Beset panneord" function.			
Telephone number	Telephone mumber			
Street	Street			
Postcode	Pestozde			
City	City			
Country	Please select •			
stact information				
Language for correspondence	English •			
E-mail notifications	t would like to regularly receive maintenance tasks from my access control system by e-mail. Never			
	I would like to receive information about AirKey online administration updates and maintenance windows.			
	🗵 i would like to receive important notifications from EVAA (recommended).			

Figura 107: Eliminar administrador

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



Figura 108: Eliminar administrador



# 0

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 <u>Informações gerais</u>.

# 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**.

EVVA AirKey			The Credit Soft Administrator	English
👚 HOME 🔒 ACCESS CONTROL SYSTEM 🏼 🎎 MEDIA & PERSONS 📄 PROTOCOLS 🐁 ADMINI	ISTRATORS 🕜 HELP			
Home				
Media 8 persons	+ Add	Access control system		+ Add
2 117 Presents 6 Smultphones 2 Cards	"Send a Key"	1 Cylinder	((c)) 1 Wall reader	4 Areas
		Door designation Component ID Door 2 000565F246DF929A	Maintenance tasks	1 Maintenance task
Protocol		Access control system: Test f. Evva		Customer number: airkey_SUHXLAFHBO
209 Ladding component protocol	606 System protocol	Time         Public holidays           7 public holidays this year         7 public holidays in 2018           ③ Time ranes:         Default time zone is Europe/Vienna, UTC +02:00		redit açoxates edt
Information				
General Terms of Business (GTB)	Imprin	<u>11</u>	Final user license ag	greement (EULA)

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.



General	Default values H	Holidays
uetooth s	ettings of the AirKey	арр
uetooth se Acce	ettings of the AirKey	app
uetooth se Acce	ettings of the AirKey ss from the lock screen	app
uetooth se	ettings of the AirKey ss from the lock screen	app This option allows the opening of locking components via Bluetooth from the lock screen without unlocking the smartphe If the option is not activated, the smartphone must be unlocked before each access.

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.

Update after each access	✓ The AirKey app data on the smartphone is updated after each acce	ss.	
	Regardless of this, the AirKey app data is updated automatically every	12 hours.	
Text for the "Send a Key" SMS	O Default text	Own text	
	Here is your key (valid for 48 hours) for the AirKey system "Test":	Have fun opening doors with AirKey!	

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*.

AirKey app settings	AirKey app settings						
Update after each access	The AirKey app data on the smartphone is updated after each access.						
	Regardless of this, the AirKey app data is updated automatically every 12 hours.						

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 <u>Atualizar smartphone</u>), a funcionalidade deverá estar ativa no smartphone. Poderá encontrar o atual estado **1** do smartphone com respeito a esta função na Administração online do AirKey, nos detalhes do smartphone.



ttings	
Maintenance authorisation	This smartphone can be used to perform additional maintenance operations on AirKey components
Office mode	Medium can activate the manual office mode
Show event log data	Show event log data in the AirKey app
Release duration	Normal release duration
	Extended release duration
PIN code of the AirKey app	No PIN code set
Update the AirKey app data	inactive 1
	-





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".

Text for the "Send a Key" SMS	O Default text	Own text		
	Here is your key (valid for 48 hours) for the AirKey system "Test":	Have fun opening doors with AirKey!		
		35/15	°//,	

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 <u>Função "Send a Key"</u>.



O seu texto está limitado a um máximo de 150 carateres. 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.

Security options	
Smartphone replacement	Automatic confirmation of people's requests for smartphone replacement.
	Attention! With automatic confirmation, it is not possible to check whether the smartphone replacement is authorised.
Two-factor authentication (2FA)	Deactivated (login with user ID and password, WTHOUT an additional SMS code)
Four-eyes principle for	Activate two-factor authentication
the event log viewing	Activate four-eyes principle

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 <u>Troca de smartphone</u>.

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**.

Security options	
Smartphone replacement	Automatic confirmation of people's requests for smartphone replacement.
	Attention! With automatic confirmation, it is not possible to check whether the smartphone replacement is authorised.
Two-factor authentication (2FA)	Deactivated (login with user ID and password, WTHOUT an additional SMS code)
	Activate two-factor authentication

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*.

Activate two factor authentication
To aktivate the two factor authentication, your phone number must be verified. An SMS code will be sent to this number.
Your mobile phone number +43123456789
Cancel

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*.

Activate two factor authentication	$\otimes$
Enter the received SMS code to save the phone number and activate the two factor authentication.	
SMS code sent to +43123456789 Edit mobile phone number	
Cancel	Save

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 <u>Login no AirKey com a autenticação de dois fatores</u>.

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

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



Two factor authentication (2FA)	
Two factor authentication (2FA)	Activated
	Deactivate two factor authentication

Figura 119: Desativar a autenticação de dois fatores

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

Deactiva	te two factor authentication 🛛 🛞		
This deactivates the two factor authentication for all administrators of this access control system.			
X Cancel	Deactivate two factor authentication		

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**.

Four-eyes principle for the event log viewing	Deactivated (The administrators can view all event logs WITHOUT needing a confirmation code from a second administrator.	0
	Activate four-eyes principle	

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*.



Activate four-	-eyes principle
Please select a second administrator to confin confirmation code will be sent to this adminis	m the activation. An e-mail with a strator.
Select second administrator	

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*.

A confirmation code has been sent to th Please enter the confirmation code with	e e-mail address of the selected administrator. in 10 minutes.
Confirmation code sent to	Select administrator
js5wt4	

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 <u>AirKey Cloud Interface (API)</u>.

#### 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 <u>AirKey Cloud Interface (API)</u>.

# 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.

EVVA AirKey						
ACCESS CON	ITROL SYSTEM	Letter Media & Persons	PROTOCOLS	ADMINISTRATORS	P HELP	
Settings						
General Specification values	Public holidays					
Default values for all recent	Default values for all recently added locking components					
Time and calendar						
Time zone	Europe/Vienna	a <b>→</b> U	FC +02:00 🔆			
Public holiday calendar	Apply public	holiday calendar				

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 <u>Dias de férias/feriados</u>) serão salientados e ativados no separador para o novo componente de bloqueio.

#### Áreas

	Areas			
	Area designation	Q)	All (2) 👌 Only not cum	rent (2)
		Area designation	Area status	
		feuerwehr	Ö	<b>^</b>
		Keller	Ö	
	Show 1 to 2 of 2 entries			
L	$\frac{1}{2}$ Assign to areas	Gancel assignment [0]		

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 <u>Criar área</u>.

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

Office mode	Allow manual office mode Enables manual office mode with authorised media (smartphones, cards, key tags, etc.).
Automatic office mode	Please activate "Allow manual office mode" if you would like to use the automatic office mode function.
③ Release duration	10 s normal release duration
	20 s extended release duration
Update after each unlocking	The locking component is updated each time it is unlocked with a smartphone via Bluetooth. Regardless of this, the locking component is updated each time it is unlocked with a smartphone via Bluetooth, if at least 6 hours have passed since the last full update.
Hands-free mode for cylinders	✓ Allow

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**.



Office mode	☑ Allow manual office mode Enables manual office mode with authorised media (smartphones, cards, key tags, etc.).
Automatic office mode	Activate automatic office mode Activates the automatic office mode and end times for the manual office mode, with which the locking component opens or closes automatically.
© Release duration	10 s normal release duration
	20 s extended release duration
Update after each unlocking	The locking component is updated each time it is unlocked with a smartphone via Bluetooth. Regardless of this, the locking component is updated each time it is unlocked with a smartphone via Bluetooth, if at least 6 hours have passed since the last full update.
Hands-free mode for cylinders	✓ Allow
inds-free mode for wall readers	



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 percetível 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.

010DACA8298A7F1C (Sa	👌 Locking compor	nent updat	틣 Event log updated	
010DACA8298A7F1C (Sa	<ul> <li>Access granted</li> </ul>	🙋 Locking	component updated after unlocking vi	a Bluetooth

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 <u>Atualizar</u> <u>componentes de bloqueio</u>.

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

0

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 Handsfree (mãos-livres). Poderá encontrar como alterar a configuração em componentes de bloqueio individuais no capítulo <u>Editar componente de bloqueio</u>.

#### 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:

Logging	
Personal reference in protocol entries	<ul> <li>Visible</li> <li>Visible for Days</li> <li>Not visible</li> </ul>

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.



Save changed specification values	8
Would you like to save the following changes to specification values?	
<ul> <li>Office mode</li> </ul>	
<ul> <li>Logging</li> <li>Public holiday calendar</li> </ul>	
Changed specification values will be used if you add a new component to your access control system. Would you like to additionally transfer the changes to all components that have already been created within your access control system?	
<ul> <li>Use the change as specifications for the recently added components only.</li> <li>Additionally apply changes to all my locking components.</li> </ul>	
X Cancel	e

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.

Image: Specification values         Pathic holdsage: Specification values <t< th=""></t<>										
e following exceptions are co	strolled by the public holiday calend	ar.								
1. Periodic access author 2. Automatic office mod	isations are not valid on public holic e is not taken into account on public	lays. : holidays.								
🕂 Add public holiday	73 available			∉201	7 ⊧			Calendar view	II List view	
January	February	March	April	May	June	July	August	September		
TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU		
245678	6 7 8 9 10 11 12	1 2 3 4 5 6 7 8 9 10 11 12	3 4 5 6 7 8 9	1 2 3 4 5 6 7	5 6 7 8 9 10 11	2456789	7 8 9 10 11 12 13	4 5 6 7 8 9 10		
10 11 12 13 14 15	13 14 15 16 17 18 19	13 14 15 16 17 18 19	10 11 12 13 14 15 16	15 16 17 18 19 20 21	12 13 14 15 16 17 18	10 11 12 13 14 15 16	14 15 16 17 18 19 20	11 12 13 14 15 15 17		
17 18 19 20 21 22	20 21 22 23 24 25 26	20 21 22 23 24 25 26	17 18 19 20 21 22 23	22 23 24 25 26 27 28	19 20 21 22 23 24 25	17 18 19 20 21 22 23	21 22 23 24 25 26 27	18 19 20 21 22 23 24		
24 25 26 27 28 29	27 28	27 28 29 30 31	24 25 26 27 28 29 30	29 30 31	26 27 28 29 30	24 25 26 27 28 29 30	28 29 30 31	25 26 27 28 29 30		
31						31				
October	November	December								
TU WE TH FR SA SU	MO TU WE TH FR SA SU	MO TU WE TH FR SA SU								
1	1 2 3 4 5	1 2 3								
3 4 5 6 7 8	6 7 8 9 10 11 12	4 5 6 7 8 9 10								
10 11 12 13 14 15	13 14 15 16 17 18 19	11 12 13 14 15 16 17								
17 18 19 20 21 22	20 21 22 23 24 25 26	18 19 20 21 22 23 24 26 26 27 28 28 20 31								
21	17 10 17 10	10 10 10 10 10 11								
1.00										

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.



all day 📝	
*Start 24/12/2017 <u>31</u> 00:00	
*End 24/12/2017 (24:00	
Repetition Each year	
Never expires 👻	

Figura 133: Adicionar dia de férias/feriado

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

		00	tob	er						Nov	/eml	ber		
мо	TU	WE	TH	FR	SA	SU		мо	TU	WE	TH	FR	SA	SU
						1				1	2	3	4	5
2	3	4							7 (	8	9	10	11	12
9	10	11	12	latio	nalf	eiert	ag	1			16	17	18	19
16	17	18	19	20	21	22	лиау			22	23	24	25	26
23	24	25	26	27	28	29		27	28	29	30			
30	31													

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 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.

<b>EVVA</b> AirKey				G	Credit & John Smith Int	English • Settings & Dog off
ACCESS CONTROL SYSTEM	M 🤽 MEDIA & PERSONS 📋 PRO	STOCOLS 🍰 ADMINISTRATORS 🔞 H	ELP			
iettings						
General Specification values Public hold	fays					
Public holiday calendar						S Deactivate
The following exceptions are controlled by the 1. Periodic access authorisations are no 2. Automatic office mode is not taken i	public holiday calendar: st valid on public holidays. into account on public holidays.					
+ Add public holiday 72 available			∉2017⊮			Calendar view
Heilige Drei Könige 🖌 🕎 Start: 06/01/2017 00:00	Maria Himmelfahrt 🖊 🕱 Start: 15/08/2017 00:00	Nationalfeiertag / III Start: 26/10/2017 00:00 End: 26/10/2017 24:00	Maria Empfängnis 🖌 🏢 Start: 08/12/2017 00:00 End: 08/12/2017 24:00	Heiligsbend / W Start: 24/12/2017 00:00 End: 24/12/2017 24:00	Christmas Eve / 1	Christiag / 1 Start: 25/12/2017 00:00 End: 25/12/2017 24:00
End: 05/01/2017 24:00 Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires
End: 0601/2017 24:00 Repetition: Each year, Never expires Stefanitag / II Start: 26/12/2017 00:00 End: 26/12/2017 24:00 Repetition: Each year, Never expires	cm. 1999e2017 2400 Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires
End: 0601/2017 24:00 Repetition: End ways, Never expires Stefanistics / # Start: 2017 2017 00:00 Repetition: End year, Never expires	um, ravererr 2400 Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Never expires	Repetition: Each year, Niever expires

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

Se selecionar 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.

	2 Cylinder	((C)) 1 Wall reader	4 Areas				
Door designa Door 2	tion Component ID 000565F246DF929	Maintenance tasks	1 Maintenance task				
EVV/	AirKey	MEDIA & PERSONS     PROTOCOLS	& Administrators 👔 Help				

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**  $\rightarrow$  **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.

										-
ng components										
		0 0	0	0						
oor designation, Additional information, Component IIQ ) All component types 👻	All (3)	inly own (3) Only exten	nal (0) 🧈 Only current (2)	Not current (1)						
oor designation (additional information)	~	Component type	Component ID	Number of areas	Access control system	Number of shares	Logging	Battery	Component status	
loor 1	1	Cylinder	000508E2C227AD98	2	Own	0	Yes	1	~	
loor 2	1	Wall reader	000565F246DF929A	4	Own	0	Yes	#	ð	
loor 3	/	Cylinder	0005DF0E1B14013E	2	Own	0	Yes		~	
w 1 to 3 of 3 entries										

Figura 139: Componentes de bloqueio

- » "Só do próprio" 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" <sup>3</sup> apresenta uma lista dos componentes de bloqueio, cujo estado está atualizado.
- "Não atualizados" 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 <u>Ativar componentes de bloqueio</u> <u>para outros sistemas de bloqueio</u>.

## 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.



# 0

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**  $\rightarrow$  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 **0** ou registe a localização ou o endereço do componente de bloqueio. Estes serão verificados no sistema de controlo de acessos quanto à sua singularidade.

HOME ACCESS COL	Key 🗇 Credit 🏖 Melan & Petrosons 🖺 Photocols 🔈 Administrators 💿 HEP	English • Settings of	Log off			
Detab       Settings       Authorized media (sotemut)       Authorized media (sotemut)						
Details Component type Model Component ID Firmware version Component status Last update	etalis Component type Gondar Component Compone					
Door designation Door designation Additional information Location	Door 1       Additional Internation       Address or OPB coordinates       Cj Stow in Google Maps					

Figura 140: Editar componente de bloqueio

 A atribuição de áreas para o componente de bloqueio selecionado pode ser editada no bloco <u>Áreas</u>.

Areas	Bi Contraction of the second s						
0	(Ves designation Q) (MIQ) (2						
		Area designation	^	Area status			
		Feuerwehr		Ö			
		Keller		G			
Sh	Show 1 is 2 of 2 entries.						
	Assign to areas						

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 <u>Trabalhar com vários sistemas de bloqueio AirKey.</u>



hares						
(Access control system, Share code Q			A	All (0) Shares (0)	Share codes (0)	
Access control system	Customer number	Released since	Share code (valid until)			
No data found	-					
Show 0 to 0 of 0 entries						
Add share						

Figura 142: Ativações

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

Remarks	
Comment	

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.

Time zone	Europe/Vienna	▼ UTC +02:00 ¥
Public holiday calendar	🔲 Apply public holiday calendar 🛛 🔿 G	o to public holidays settings
	The following exceptions are controlled 1. Periodic access authorisations 2. Automatic office mode is not	l by the public holiday calendar: s are not valid on public holidays. : taken into account on public holidays.

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 <u>Valores por defeito (para todos os novos componentes de bloqueio adicionados)</u>.

> 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 (mãoslivres), 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 Handsfree (mãos livres), consulte o capítulo <u>Vista geral da função Hands-free (mãos livres)</u>.

- 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.

Personal references in event log entries	Visible	
	<b>Visible for</b>	day(s)
	O Not visible	
Repair options	Show repair options	
RS485 interface	The log entry of th	e last successful access is transmitted to a third-party system via the RS485 interfac

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 <u>Opções de reparação</u>.
- 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 <u>Detalhes técnicos da interface RS485 para leitores de</u> <u>parede com Bluetooth</u>.
- 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*  $\rightarrow$  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**.

EVVA) Air	Key	1 Credit Log of Advances and Ad
ACCESS C	DNTROL SYSTEM 🎎 MEDIA & PERSONS 📓 PROTOCOLS 🍰 ADMINISTRATORS 🚯 HELP	
Edit locking component		49; Back
Details Settings Author	sed media (own) Authorised media (esternal)	
Details		E Save
Component type	2 Cylinder	
Mode	I NFC / Bluetooth	
Component ID	000508E2C227AD98	
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54	
Component status	s 🧵 Battery OK (status from 03/07/2017 12:50:27) 🚯 Time correct 🐞 Current time zone 😓 Blacklist up to date 🛔 Areas up to date 🐞 Current relev	ase duration   📅 Office mode settings up to date 🎇 Public holiday calendar up to date 🛫 Firmware up to date
Last update	03/07/2017 12:50:27	



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

Remove locking component						
Do you really want to remove the locking component "Door 1" from your access control system? The locking component will be removed and reset to construction site mode.						
Existing authorised media can no longer unlock these locking component.						
Cancel						

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. Contanto 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**  $\rightarrow$  **Áreas**.

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

Figura 147: Pergunta de segurança



- No campo de pesquisa 

   insira um critério de pesquisa com, pelo menos, três carateres.
- > 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 2.

EVVA AirKey	(1) Credit John Smith Administrator Registrator	Settings (a) Log off
🏫 HOME 🔒 ACCESS CONTROL SYSTEM 🏭 MEDIA & PERSONS 🖺 PROTOCOLS 🝰 ADMINISTRATORS 🛞 HELP		
Areas		
Area designation	lumber of locking components	Area status
Fearwehr		
Headquarter		0
Keler		8
Main Factory		<b>U</b> -
Show T to 4 of 4 emins      Craste area     Deport     Deport		

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**  $\rightarrow$  **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* **1**.

EVVA AirKey	The stray of the set o
🖈 HOME 🔒 ACCESS CONTROL SYSTEM 🏦 MEDIA & PERSONS 📄 PROTOCOLS 🍰 ADMINISTRATORS 🚳 HELP	
reate area	4h, Back 🛅 Save
rtails	
*Area designation Area designation	
signed locking components	
You can assign locking components to the area after the Save.	
marks	
Comment Comment	
	Vis Back 🗎 Save

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* é visualizado se todos os componentes de bloqueio naquela área estão atualizados. No bloco *Atribuir componentes de bloqueio* •, estão listados todos os componentes de bloqueio que foram atribuídos à área.
- Clique em *Atribuir componentes* <sup>3</sup> para incluir um componente de bloqueio na área.

	AirKey			() 1 2 2	iredit John Smith 5 KeyGredit(s) Administrator	English +	Settings	(= []]] Log off
🏦 НОМЕ 🔒 АСС	CESS CONTROL SYSTEM 🔉 MEDIA & PERSONS 📄 PROTOCOLS 🍰 ADMIN	ISTRATORS 🚯 HELP						
Edit area						W Deletion	🖗 Back	Save
Details								
Area designation Area designation	ignation Headquarter a status \$\$  \$\$  \$\$  \$\$  At least one locking component is not up to date.							
Assigned locking compone	ients 2							
Door designation (Ad	dditional Information), Component ID 9, All component types •					All (1) 🖌 Only cu	rrent (0) 👌 Only	not current (1)
Door desi	signation (additional information)	Component type	Component ID	Number of areas	Battery status		Component status	
Show 1 to 1 of 1 entries		wai reader	0003037240073234	-	,			
3 + Assign compone	ents assignment (0)							
Remarks								
Co	omment Comment							

Figura 150: Editar área

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

Door de	esignation (Additional information), Component ID Q A	component types 👻		
	Door designation (additional information)	Component type	Component ID	
	Door 1	Cylinder	000508E2C227AD98	*
	Door 3	Cylinder	0005DF0E1B14013E	-

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 <u>Editar</u> <u>componente de bloqueio</u>.

#### 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.

EVVA	AirKey			() Gredit BS KayGre	dit(s) 2 John Smith Administrator Regist	t ▼ Settings ⊕  ]] Log off			
🟦 HOME 🔒 A	ACCESS CONTROL SYSTEM 🤱 MEDIA & PERSONS 📄 PROTOCOLS 🕹 ADM	NISTRATORS 👔 HELP							
Edit area	🗑 Dektion 🕸 Back 🛗 Save								
Details									
*Area d	*Area designation Headquarter Area status 🏥 At least one looking component is not up to date.								
Assigned locking comp	ponents								
Door designation	(Additional information), Component ID				All (1)	Only current (0) Only not current (1)			
Door	designation (additional information)	Component type	Component ID	Number of areas	Battery status	Component status			
Door 2	2	Wall reader	000565F246DF929A	4	7	G			
Show 1 to 1 of 1 entr	The name of the second delification of the secon								

Figura 152: Marcar os componentes de bloqueio

- > Clique em *Cancelar atribuição* **1**.
- 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*.



	Cancel assignment	6
Do you really want to revoke the block them.	e locking component assignment? Persons that are authorised for the area can n	o longer
- 000565F246DF929A: Door	2	*
		-
fou must update the compone	nts in order to fully remove the assignment.	
<b>AA</b>		

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 <u>Editar</u> <u>componente de bloqueio</u>.

## 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 1**.

<b>EVVA</b> AirKey			1 Credit	edit(s) John Smith Administrator English	Settings	(e  ) Log off
A HOME ACCESS CONTROL SYSTEM ▲ MEDIA & PERSONS PROTOCOLS ▲ ADMIN	NISTRATORS 👔 HELP					
Edit area				0 1	Deletion 🗠 Back	Save
Details						
*Area designation Headquarter Area status 👫 At least one locking component is not up to date.						
Assigned locking components						
Door designation (Additional information), Component ID Q All component types •				All (1)	🛹 Only current (0) 👌 Only n	ot current (1)
Door designation (additional information)	Component type	Component ID	Number of areas	Battery status	Component status	
Door 2	Wall reader	000565F246DF929A	4	Ŧ	G	
Show 1 to 1 of 1 entries						

#### 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.



Delete area – not possible	8
A locking component is still assigned to the "Headquarter" area.	
- 000565F246DF929A: Door 2	*
Please remove the assignment of the component first. The area has not been deleted.	•

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 <u>Cancelar a</u> <u>atribuição de componentes de bloqueio a uma área</u>.

#### 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.

EV	VA	AirKey				
🏫 ном	e 🔒	ACCESS CONTROL SYSTEM	<b>MEDIA &amp; PERSONS</b>	PROTOCOLS	Lange Administrators	HELP
Edit lock	ing com	ponent				
Details	Settings	Authorised media (own)	Authorised media (external)			
Details						

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.

EVVA AirKey			्री Credit	Administrator Int En	gish •	Settings $\Leftrightarrow []]$ Log off		
ACCESS CONTROL SYSTEM	DCOLS 🍰 ADMINISTRATORS 🔞 HELP							
Edit locking component					44	Back W Remove		
Details Settings Authorised media (own) Authorised media (internal)								
Media of the own access control system								
(Person, Identifier, Nedia ID, Designation, Telephone number Q.) All media •	All (2) 📋 Active (2) 💽 Deactivated (0)			All (2)	Current (1) 👌 Not cur	rent (0) 🛛 🔒 Unknown (1)		
Person (identifier)	Media type	Media ID	Designation	Telephone number	Deactivated	Media status		
Sabire Ribits	Smartphone		Dienstmobile A8	+43 123 456 789 0				
						L (1)		
Jane Smith	Smartphone	01A7AC1671818FED		+43123123456456				

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.

NE 🖬	ACCESS CONTROL SYSTEM	EDIA & PERSONS PROTOCOLS	ADMINISTRATORS 👔 HELP
	Edit medium		
-	Authorisations Details Protocol	C Reload view	
mith	(Locking components & areas ۹)	(Authorisation Q	All (2) 🕜 Only current (2) Most recent first 👻
	A Feuerwehr	& Authorisation	2 Authorisation
((	AA	Door 1	Door 2 00055552450F9294
671 2345	A A Headquarter A A	111 Temporary access 03/07/2017 12:45 - 17:00	OO Permanent access unlimited
)	A A Keller		
(0	<ul> <li>A A Main Factory</li> <li>A A</li> </ul>		
8370	Door 1 000508E2C227AD98		
()	Door 2 000565F246DF929A		
loor	Door 3		

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.

EVVA AirKey			I athaban Annestation Annestation I I Deutsch V Constrainty Annestation
🛧 HOME 🔒 SCHLIESSANLAGE 🤽 MEDIEN & PERSONEN 🗎 PROTOKOLLE 🐊	D ADMINISTRATOREN	HILFE	
Wartungsaufgaben			[ ] PDF-Download
C Areicht neu laden Schlieftkomponenten			
(Türbezeichnung, Komponenten-ID Q.)			Priorisierung der Wartungsaufgaben
Türbezeichnung (Zusatzinformation)	Komponenten-ID	Wartungsaufgaben	, v
Back door	000508E2C227AD98	A Ersatzknauf einbauen	
Wandleser 1	000565F246DF929A	🕰 Firmware nicht aktuell	1
Main Entrance (EZ2091)	000508E2C227AD98	🕰 Firmware nicht aktuell	
Zeige 1 bis 3 von 3 Einträgen			
			2 📑 PDF-Download

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.

1	A	В	С	D	E	F	G	н	I.	J	K	L	M	N	0	Р	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_OW38	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	airkey_OW3K	LCIXUP
3					designation		Karte Musters	Testphone M	Mobile John	iPhone	John Android		Mobile Susan	ne	Kombischlüss	Samsung S6	
4					media ID	01513937C0A	000524E1EEE	00058485F18	01769CAD4E4	017DF822779	018D3E2A570	01564B15279	01AC3BF5349	01FBB248091	L 0005A7592B8	0188626927E	BA567
5					media type	Smartphone (	Card	Card	Smartphone (	Smartphone	Smartphone (	Smartphone (	Smartphone (	Smartphone (	Card	Smartphone (	Android)
6	door designat	customer nun	component ty	component ID	)												
7	SR A Musterst	airkey_OW3K	CYLINDER	00052C2F2BA	3F14B	1	1	5	E	2	7	1	3	1	. 4	4	
8	Hangschloss	airkey_JCHDI	CYLINDER	0005B508C60	B802D	0	6	1	1	1	1	0	3	0	1	0	
9	Wandleser	airkey_OW3K	WALLREADER	0005C5B3F1E	9C207	2	1	4	0	7	5	В	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.
- A 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 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 •** administre todas as pessoas, meios e autorizações no sistema de controlo de acessos AirKey.

ACC 🔒 ACC	CESS CONTROL SYSTEM	Section 2 Media & Persons	PROTOCOLS	Lange Administrators	HELP	
lome						
Media & persons	1					<b>+</b> Ac
2			P	(í		
117.0	)	6 Smartphones	2 Ca	rds	"Send a Key"	

Figura 162: Meios e pessoas

#### 5.6.1 Vista geral das pessoas

Se selecionar, na página inicial **Home**, a caixa de seleção **Pessoas** ou, no menu principal, **Meios e pessoas**  $\rightarrow$  **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 

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

EVVA AirKey								
ACCESS	🚖 HOME 🔒 ACCESS CONTROL SYSTEM 🤽 MEDIA 6 PERSONS 🖺 PROTOCOLS 🔈 ADMINISTRATIONS 🌚 HELP							
Persons	ersons							
First name	Last name 2 ^	Identifier	E-mail address	Number of media	Media status			
Horst	Bäcker			0				
Florian	D			0				
Adrian	н			1	~			
Peter	Huber			0				
Anna	Müller			0	· .			
Maria	Müller	123456		0	· ·			
Max	Mustermann	191	m.mustermann@gmail.com	0				
Max	Mustermann	190	m.mustermann@gmail.com	0	-			
Max	Mustermann	204	m.mustermann@gmail.com	0	· .			
Max	Mustermann	203	m.mustermann@gmail.com	0				

Figura 163: Pessoas

## 5.6.2 <u>Criar pessoa</u>: 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 seleção *Pessoas*.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas**  $\rightarrow$  **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**. Tratase 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*.

HOME 🔒 ACCESS CONTROL SYSTEM	MEDIA & PERSONS	PROTOCOLS	La Administrators	🕜 HE
Edit norron				
Details				
Horst Bäcker				
Tetails				
* First name	Horst			
* Last name	Bäcker			
Identifier	Identifier			
Gender	Please select 🔻			
Date of birth	DD/MM/YYYY			
Contact details				
E-mail address	E-mail address			
Telephone number	Telephone number			
Street	Street			
Postcode	Postcode			
City	City			
Country	Please select	•		
* Language for correspondence	Deutsch 👻			
Remarks				
Commut				
Comment				
Generate handover certification	ate (PDF) 1			

Figura 164: Gerar o certificado de entrega

>


Headquarter Wien			Cre	eated by: John Smith
	EVVA Airl	Key perso	nal detail	s
Person		51		
Florian D				
Identifier: Technik     Gender: Male     Date of birth: 18.0     E-mail address: F     Telephone numbe     Street: Hauptstras     Postcode: 1010     City: Wien     Country: Austria     Remarks: -	15.1980 D@test.com r: +431234567890 sse 1			
Media				
				Up to date
Media type: Smar Media ID: 014466 Telephone numbe Last update: 30.0 AirKey app versio Registration prog Registration code Maintenance mod Show protocol dat Release duration: Office mode: activ PIN code status: 1 Remarks: -	tphone (Android) 336A2ECB86D 7: +436648370 1.2018 r: 1.7.6 ress: completed - e: - ctive normal re nactive nactive			
Authorisation 1 • Type: Periodic au • for area: Area 1 • valid from: 30.01 • valid until: unlimi	ccess 			
	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**  $\rightarrow$  **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa que pretende eliminar.
- > Clique no símbolo *Caixote do lixo* **1**.

EVVA	AirKey				
🏫 номе 🔒	ACCESS CONTROL SYSTEM	MEDIA & PERSONS	PROTOCOLS	Administrators	P HELP
John Smith	Edit person Details Details				
	* First name * Last name Identifier Gender Date of birth	John Smith 111 Male • 12/11/2001 [33]			

Figura 166: Eliminar pessoa



> Confirme a pergunta de segurança com Eliminar pessoa.

Delete person "John Smith"	⊗
Do you really want to delete person "John Smith"? This process cannot be undone.	
Cancel	Telete person

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**  $\rightarrow$  **Pessoas**.
- > Clique, na lista de pessoas, no nome da pessoa a quem pretende atribuir um meio.
- > Clique no botão **Atribuir meio 0**.

Edit	person						
De	als						
Det	alls						
	* First name	Jane					
	* Last name	Smith					
	Identifier	Identifier					
	Gender	Please select +					
	Date of birth	DOMINIOU 📰					
Cos	tact details						
	E-mail address	E-mail address					
·	Telephone number	Telephone number					
	Street	Street					
	Postcode	Postcode					
	Gity	City					
	Country	Please select	•				
	*Language for correspondence	English -					
Res	narks						
	Comment						
	Download transfer confin	nation					

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

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

	Assign medium to person	⊗
Details		
Person Jane Smith		
Medium		
Media ID 0005CDE9860F272A Designation Assistant Media type Card		
🗲 Back	2/2	Assign medium

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 <u>Atribuir pessoa a um meio</u>.



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**  $\rightarrow$  **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.



IOME 🖻 ACCESS CON	ROL SYSTEM L MEDIA 8	PERSONS 🗎 PROTOCOLS	help 🚯 ADMINISTRATORS							
rson, Identifier, Media ID, De	signation ,Telephone number	9, All media 🔹 All (9)	Active (9) 🔂 Deactivated (0)				All (9)	Current (4)	Not current (1)	n (4) I Highlighted for deletio
erson (identifier)	Media type	Media ID	Designation	Telephone number	Authorisation				Deactivated	Media status
drian H	Smartphone (Android)	01C6E70504F10D2F	Smartphone Compact Z3	+43 123 123 123 123	🖫 2	<b>7</b> o	% o	<b>4</b> 0		×
ax Mustermann (13)	Smartphone (iOS)	0181400993282850	iPhone	+43 11 22 33 44 55	S 1	<b>*</b> o	<b>%</b> o	щ о		<b>v</b>
ax Mustermann (7)	Card	0005863432EE6819	Lager		20	P o	% o	Ж. о		×
bine Ribits	Smartphone		Dienstmobile A8	+43 123 456 789 0	۵ 🖇	7 2		<b>a</b> 0		G.
nspeter Seiss (AirKey)	Smartphone				۵ 🖇	<b>1</b> o		щ о		G.
ne Smith	Smartphone (Android)	01A7AC1671B18FED		+43123123456456	۵ 🖇	7 0	% o	16 2		G
ve Smith	Smartphone				20	<b>*</b> o		щ о		G.
	Card	0005CDE9860F272A	Assistant		20	<b>7</b> o		Т. о		×
	Smartphone		Mobile	+43 11 22 33 55 44 66	20	7 0		<b>3</b> o		G.

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**  $\rightarrow$  **Adicionar meio**.
- Ou selecione, na página inicial *Home*, a caixa de seleção *Smartphones* ou *Cartões* e aí em *Adicionar meio*.

EVV	AirKey					
🏫 номе	ACCESS CONTROL SYSTEM	Length America Media & Persons	PROTOCOLS	Lange Administrators	P HELP	
Home						Add person Add medium
Media & perse	ons					+ Xdd
	8		P	(í	9	•
	117 Persons	7 Smartphones	2 Ca	rds	"Send a	Key"

Figura 172: Adicionar meio

> Selecione o tipo de meio do novo meio.

Please	select the type of th	e new medium:	_	0
	Smartphone	664 59 41 411 664 83 45 879	Card	
×	Cancel	6649149716	I Ne	xt

Figura 173: Criar novo meio



Do ponto de vista da aplicação, não há diferença entre cartões, portachaves, 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 <u>Criar smartphone</u>: 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 <u>Adicionar</u> <u>cartões, porta-chaves e chaves combinadas com o smartphone</u>.

- > 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 <u>Autorizações</u>.



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 <u>Adicionar cartões, porta-chaves e chaves combinadas com um smartphone</u>.

## 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**  $\rightarrow$  **Meios**.
- > Clique, na lista geral, no meio desejado.
- > Selecione o separador **Detalhes** para editar o meio.



Authorisations	Details	Protoc	col C Reload view
Medium			
	Med	ia type	Card
	M	edia ID	0005863432EE6819
	Desig	nation	Lager
	Status		Up to date
	Last update		03/07/2017 16:25:05
	Keyring v	version	6.18
Settings			
	Office	mode	Medium can activate office mode
	Release du	uration	Normal release duration
			Extended release duration
Remarks			
	Cor	nment	

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 <u>Atribuir meio a uma pessoa</u>).

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

- > Selecione, no menu principal, *Meios e pessoas*  $\rightarrow$  *Meios*.
- > Clique, na lista geral, no meio desejado.
- O meio 1 já está selecionado (podem ser atribuídos vários meios a uma pessoa).
- > Aqui, visualiza todas as autorizações já atribuídas 2.

	Edit medium	
2	Authorisations Details Protoco	Reload view
idrian H	Locking components & areas	Authorisation Q All (2) V Only current (2) Most recent first V
<b>~</b>	B B Feuerwehr	Authorisation     Authorisation - expired     Authorisation - expired     Authorisation - expired     Authorisation - expired
artphone mpact Z3	Headquarter	OO Permanent access unlimited 29/05/2017 all day
123 123 23 123	A A Keller A A	
	Main Factory	
	Door 1 000508E2C227AD98	
	Door 2	







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.
- *Cinzento* = 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**  $\rightarrow$  **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.

	Edit medium				
	Authorisations Details Protocol	C Reload view			
Jane Smith	(Locking components & areas Q)	Authorisation	All (2)	ecent first 👻	
<b>—</b> / <sup>0</sup>	A A Feuerwehr				
	Headquarter				
4312312345	A A Keller				
	AA				
<b>))</b>	음음 Main Factory 음음				
4366488370	Door 1 000508E2C227AD98				
	Door 2 000565F246DF929A				✓ Edit authorisation
					There already is an

Figura 176: Editar meio – Alterar autorização

- São visualizados os detalhes da autorização existente.
- > Clique em **Alterar 1**



Permanent access	8
Door 2 000565F246DF929A	
CO Permanent access Change	
always applicable	
© from to	
Authorisation created on Authorisation updated on	30/06/2017, 10:35 30/06/2017, 10:42
Close	E Save

Figura 177: Alterar autorização

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

elect new access type for author Door 2 00565F246DF929A	isation			
Periodic access	Temporary access	Individual access		
Enables repeated accesses on w	veekdays during a certain period (da	nte).		
Enables repeated accesses on weekdays during a certain period (date). Your existing authorisation settings will be lost.				

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 <u>Criar autorização</u>.
- 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**  $\rightarrow$  **Meios**.
- > Clique, na lista geral, no meio cujas autorizações devam ser eliminadas.
- > No separador "Autorização", clique na autorização que pretende eliminar.



Permanent access	8
Door 2 000565F246DF929A	
OO Permanent access Change	
<ul> <li>always applicable</li> </ul>	
© from to	
Authorisation created on Authorisation updated on	30/06/2017, 10:35 30/06/2017, 10:42
Close Delete authorisation	Save

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*.

🏠 НОМЕ 🛛	ACCESS CONTROL	SYSTEM	AL ME	DIA & PERSONS	LS a	& ADMIN	IISTRATORS
	Edit medium						
-	Authorisations	Details	Protocol	C Reload view			
Jane Smith				Authorisation	Q.)	All (2)	🛹 Only c
				K Authorisation - expired			
$\square$				B Door 1			
AC1671				Temporary access			
2312345				03/07/2017 12:45 - 17:00			
0							
<b>(</b> ()							
366488370							
366488370							
366488370	Delete	authorisatio	n				
366488370	Delete	authorisatio	n D Authors	ation			
1366488370	Delete	authorisatio	n V Authori Door 2	uton			

Figura 180: Eliminar autorização

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

	Authorisation	
	Door 2 000565F246DF929A OO Permanent access unlimited	
nce the medium h omponent.	has been updated, the owner is no long	er able to lock this locking

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 <u>Esvaziar meio</u>.

#### 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*  $pessoas \rightarrow Meios$ .
- > 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 carateres) em "Outras observações".
- > Clique em *Continuar.*
- > Confirme a pergunta de segurança com **Desativar meio.**

Deactivate	medium 🛞	
Do you really want to deactivate the medium 01A7A	C1671B18FED?	
AirKey is attempting to deactivate the smartphone remotely. If this is not possible, the affected locking		
Reason: Loss		
de Back	Deactivate medium	

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 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 <u>Cancelar atribuição</u>.

#### 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**  $\rightarrow$  **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 0**
- Confirme, depois, a pergunta de segurança com *Remover meio* para remover o atual meio desativado do sistema de controlo de acessos.



Remove medium
Do you really want to remove medium "+43123123456456"?
Media type
Smartphone
Media ID
01A7AC1671B18FED
Telephone number
+43123123456456
This process cannot be undone.

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 **0** do meio, pode ser reativado se voltar a estar disponível.

0		ت ((		
Smartphone				
Compact Z3				
+43 123 123				
Reactivate medium				
G	Û			

Figura 186: Reativar o meio desativado

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

- 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.

	Û
Figura	187: Reativar meio

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



		Reactiv	ate medium		8
Do you rea	ally want to reactiv	ate the medium 010	:6E70504F10D2F?		
Afterward	s, you can use the	medium for all upda	ted locking compone	nts again.	
* Reason	Found				
urther no	tes				

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*.

Reactivate medium	8
Do you really want to reactivate the medium 01C6E70504F10D2P? Afterwards, you can use the medium for updated locking components again.	
<ul> <li>Your current credit is 84 KeyCredit(s).</li> <li>1 credit will be deducted from your credit.</li> </ul>	
Seck	Reactivate medium

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 <u>Iniciar a troca como administrador</u>.

#### 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**  $\rightarrow$  **Meios**.
- > Clique, na lista geral, no meio a duplicar.

Sma Cor +43 1:	artphone mpact Z3 123 123 23 123	> Cl Al pe > Sc > Cl	lique em <b>Mais</b> bre-se uma lista g essoa – o meio a elecione o meio a confirme o process	D → Duplicar. geral com todos os n duplicar não está ind lvo e clique em Con so com Duplicar me	neios atribuídos a um cluído nesta lista. <b>tinuar</b> . <b>tio</b> .
	O ···· uplicate 1 npty		Medium: from person:	Duplicate medium? Smartphone Compact Z3, +43 123 123 123 12 Smartphone, Media ID: 01C6E70504F10D2F 2 authorisations Adrian H	3
Re Base Re	evoke signment emove		copy to: Medium: from person:	, +4366488370990 Smartphone, Media ID: - 0 authorisations Jane Smith	
Figura 190:	: Duplicar um m	eio	General Back	2/2	Duplicate medium

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 <u>Criar autorização</u>.





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 <u>Importar dados de pessoas</u>) 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**  $\rightarrow$  **Meios**.
- > Clique, na lista geral, no meio que pretende esvaziar.

20.	> Clique em <b>Mais <math><b>0</b> \rightarrow \mathbf{Vazio}</math></b> .
	> Conclua o processo com <i>Meio vazio</i> .
Smartphone	Empty medium
Compact Z3 +43 123 123 123 123	Do you really want to empty the medium 'Smartphone Compact 23"? In this process, all 2 authorisations will be deleted from the medium. Please update the medium afterwards to complete the process. Medium
0 5	Media type Smartphone
Duplicate	Media ID 01C6E70504F10D2F
🖋 Empty 1	Designation Smartphone Compact Z3
Revoke assignment	Telephone number +43 123 123 123 123
Remove	🗶 Cancel 🛛 🖋 Emoty medium

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 <u>Desativar meio</u>.

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**  $\rightarrow$  **Meios**.
- > Clique, na lista geral, no meio cuja atribuição à pessoa pretenda cancelar.
- <u>ou</u>
- > Selecione, na página inicial *Home*, a caixa de seleção *Pessoas*.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas**  $\rightarrow$  **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 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 selecionar entre esvaziar o meio ou transferir o meio para uma outra pessoa.

Cancel assign	iment 🛞
Details	
Person Max Mustermann	
Medium	
Media type Smartyhone Media ID 0181400993282850 Designation #Phone Teliphone number 1493 11 22 33 44 55	
Empty medium	La Change person
X Cancel	Continue

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...**  $\rightarrow$  Cancelar atribuição.
- > Selecione *Alterar pessoa* e confirme com *Continuar*.

	Cancel assignment	8
Details		
Person Max Mustermann		
Medium		
Media type Smartphone		
Media ID 01B14009932B2B50		
Designation iPhone		
Telephone number +43 11 22 33 44 55		
Sempty medium		Le Change person
Assigns the medium to anot	ther person. The authorisations	s will remain.
X Cancel	1/3	Continue

Figura 198: Cancelar atribuição – Mudar pessoa

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

First r	name, Last name, Ide	entifier, E-mail address			
P	First name	Last name	Identifier	E-mail address	
0	Horst	Bäcker			
$\odot$	Florian	D			
$\bigcirc$	Adrian	н			
$\bigcirc$	Peter	Huber			
$\bigcirc$	Anna	Müller			
$\bigcirc$	Maria	Müller	123456		
$\bigcirc$	Max	Mustermann	191	m.mustermann@gmail.com	
$\bigcirc$	Max	Mustermann	190	m.mustermann@gmail.com	
$\bigcirc$	Max	Mustermann	204	m.mustermann@gmail.com	

Figura 199: Mudar pessoa

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



	Change person	8
Do you really want to a person	ssign the medium "iPhone (01B1400993;	2B2B50)" to
	John Smith (111)	
? 1 authorisation remains	available in the process.	
4		
Back	3/3	Change person

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 <u>Cancelar atribuição</u>.

- 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.



Figura 201: Remover meio – Caixote do lixo

Confirme a pergunta de segurança *Remover meio* **0**.

Remove medium 🛛 🛞
Do you really want to remove medium "Mobile"?
Media type
Smartphone
Media ID
-
Designation
Mobile
This process cannot be undone.
X Cancel

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**.

a nome	ACCESS CONTROL SYSTEM	MEDIA & PERSONS	PROTOCOLS ,	& ADMINISTRATORS	🕜 HELP	
ome						
Media & per	sons					Add
	117 Persons	7 Smartphones	2 Cards		"Send a Key"	
Protocol						
20	66 Locking component protocol	427 Med	ia protocol	629 5	ystem protocol	

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 <u>Informações gerais</u>.



## 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**  $\rightarrow$  **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*.

Activate event log viewing		8
The four-eyes principle is activated. Please select a second a confirmation of the event log viewing. An e-mail with a conthis administrator. Select second administrator	dministrator for the firmation code will be sent to	
X Cancel	Send confirmation	1

Figura 204: 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*.

ALUV	ate event log viewing
A confirmation code has been sent to Please enter the confirmation code w	o the e-mail address of the selected administrator. vithin 10 minutes.
Confirmation code sent to	Select administrator
ntcdf5	

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* <sup>1</sup>.
- Insira, para a pesquisa orientada de registos, pelo menos, 3 carateres no campo de pesquisa 2.
- > Adicionalmente, poderá ativar o filtro <sup>3</sup>, 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.

HOME ACCESS CONT	ROL SYSTE	M 🔉 MEDIA & P	ERSONS PROTOCOLS 🔬 AD	MINISTRATORS 🕑 HELP					_
col									
Locking components & areas	🗇 Med	a C Reload view		•					
cking components & areas	9	Door Component Perso	All Only access event	s (62) Not authorised (9)					
		Puring period from	to	Entire period					
Door 2 1565F246DF929A	- II								
Door 3		Date, time	Door designation (additional information)	Component ID	Person (identifier)	Media ID (designation)	Event	Details	So
ISDF0E1B14013E		03/07/2017 15:40:16	Door 1	000508E2C227AD98	John Smith (13968155)	•	Locking component updated	Protocol updated in time updated,	
Door 1 508E2C227AD98		F 03/07/2017 15:40:09	Door 3	@ 00050F0E1814013E	John Smith (13968155)		Cocking component updated	Ime updated, time difference < 1 mi	
leadquarter		03/07/2017 12:52:38	Door 1	@ 000508E2C227AD98	Jane Smith		Access granted	Battery OK Local cylinder time: 0	
cking component		03/07/2017 12:51:02	Door 1	000508E2C227AD98	Jane Smith	U UIA/ACI6/IBI8/ED	Cylinder added	Cylinder '000508E2C227AD98' add	
euerwehr cking components		03/07/2017 11:22:35	Main Entrance	000508E2C227AD98	(12808155)	-	Cylinder removed	Cylinder '000508E2C227AD98' rem	
(eller	-113	03/07/2017 11:22:30	Main Entrance	@ 000508E2C22/AD98	John Smith (13968155)	-	Cocking component updated	Ime updated, time difference < 1 mi	
cking components		03/07/2017 11:22:09	Main Entrance	@ 000508E2C22/AD98	John Smith (13968155)		Cocking component updated	Ime updated, time difference < 1 mi	1
Main Factory		03/07/2017 09:12:59	Door 2	@ 000565F246DF929A	Jane Smith		Manual office mode ended	X Manual office mode ended manually.	
component		03/07/2017 09:12:34	Door 2	值 000565F246DF929A	Jane Smith		Manual office mode started	E Local wall reader time: 03/07/2017 0	1
08E2C227AD98	112	03/07/2017 09:12:00	Door 2	值 000565F246DF929A	Jane Smith	U 01A7AC1671B18FED	Access granted	Power adapter Local wall reader t	
ted on 03/07/2017		03/07/2017 09:06:38		值 0005DF0E1B14013E	John Smith (13968155)		Cylinder added	Cylinder "0005DF0E1814013E" adde	
Main entrance 5DF0E1B14013E		03/07/2017 08:43:28	Main Entrance	@ 000508E2C227AD98	Max Mustermann (13)	[_] 01B14009932B2B50 (Phone)	Cylinder added	Cylinder "000508E2C227AD98" add	
ted on 03/07/2017	_	03/07/2017 08:40:49	Main entrance	@ 0005DF0E1B14013E	John Smith (13968155)	•	Cylinder removed	Cylinder "0005DF0E1814013E" remo	
Main entrance SDF0E1B14013E	1	03/07/2017 08:40:44	Main entrance	@ 0005DF0E1B14013E	John Smith (13968155)		<ul> <li>Locking component updated</li> </ul>	Time updated, time difference < 1 mi	
ted on 03/07/2017		03/07/2017 08:39:20	Main entrance	@ 0005DF0E1B14013E	Jane Smith	U 01A7AC1671B18FED	Cylinder added	Cylinder "0005DF0E1B14013E" adde	
loor 3		03/07/2017 08:34:41	Main entrance	@ 0005DF0E1B14013E	John Smith (13968155)	•	<ul> <li>Cylinder removed</li> </ul>	Cylinder "0005DF0E1814013E" remo	
ted on 27/06/2017	1	03/07/2017 08:34:37	Main entrance	值 0005DF0E1814013E	John Smith (13968155)	•	<ul> <li>Locking component updated</li> </ul>	Time updated, time difference < 1 mi	
Door 1	1	03/07/2017 08:34:24	Main entrance	A 0005DF0E1814013E	John Smith (13968155)		<ul> <li>Locking component updated</li> </ul>	Time updated, time difference < 1 mi	
ted on 30/06/2017	1	03/07/2017 08:32:49	Main entrance	A 0005DF0E1B14013E	Jane Smith	01A7AC1671B18FED	<ul> <li>Locking component updated</li> </ul>	Time updated, time difference < 1 mi	
iūr 3	1	03/07/2017 08:29:55	Main entrance	@ 0005DF0E1B14013E	Jane Smith	01A7AC1671B18FED	<ul> <li>Locking component updated</li> </ul>	Time updated, time difference < 1 mi	•
08E2C227AD98 ted on 20/06/2017	1	30/06/2017 10:38:06	Door 2	@ 000565F246DF929A	Jane Smith	01A7AC1671B18FED	Access granted	Power adapter Local wall reader t	-
loor 1		30/06/2017 08:07:33	Door 1	@ 000508E2C227AD98	John Smith (13968155)		<ul> <li>Faulty cylinder removed</li> </ul>	<ul> <li>Faulty cylinder has been removed (th</li> </ul>	
508E2C227AD98 ted on 20/06/2017		30/06/2017 07:34:31	Main entrance	A 0005DF0E1B14013E	John Smith (13968155)		Cylinder added	Cylinder "0005DF0E1B14013E" adde	
Gr 11		27/06/2017 15:18:33	Door 1	A 000508E2C227AD98	EVVA support	•	Locking component updated	Time updated, time difference < 1 mi	
508E2C227AD98	*	27/06/2017 15:18:17	Door 1	產 000508E2C227AD98	EVVA support	•	Locking component updated	Time updated, time difference < 1 mi	
entries	Þ	Export 6						Show 1 to 26 of 266 entric 5 Go to	

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* s, para navegar rapidamente para um determinado dia de calendário.



> Utilize, à esquerda, em baixo, o botão *Exportar* <sup>3</sup>, 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 frequentação dos componentes de bloqueio. Observe os <u>valores e limites</u> 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**  $\rightarrow$  **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*.

Activate event	log viewing
The four-eyes principle is activated. Please select confirmation of the event log viewing. An e-ma this administrator. Select second administrator	t a second administrator for the il with a confirmation code will be sent to
· · · · · ·	

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*.

A confirmation code has been sent to the Please enter the confirmation code within	e e-mail address of the selected administrator. in 10 minutes.
Confirmation code sent to	Select administrator
ntcdf5	

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 selecionar 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.



HOME 🔒 ACCESS CO	ONTROL SYS	TEM 🎎 MEDIA & P	ERSONS PROTOCOLS	ADMINISTRATORS 🔞 HELP					
col Locking components & areas edia	a)	dia C Reload view	Component Q (All Only a	(3) cccess events (62) Not authorised (9)					
Adrian H	*	During period from	ji to	Entire period					
artphone Compact Z3 C6E70504F10D2F		✓ Date, time 4	Person (identifier)	Media ID (designation)	Door designation (additional information)	Component ID	Event	Details	Source
-		04/07/2017 10:18:02	Adrian H	01C6E70504F10D2F (Smartphone C	-		Q. Reactivated	✓ Fully reactivated. 🤱 Administrator: J	0.0
ale		04/07/2017 10:18:02	Adrian H	01C6E70504F10D2F (Smartphone C			. Reactivation started	✓ Reactivation started 🤱 Administrato	
Max Mustermann (7)		04/07/2017 09:59:05	Adrian H	01C6E70504F10D2F (Smartphone C			Deactivation started	✓ Deactivation started & Administrato	0.0
863432EE6819	_	04/07/2017 09:58:34	Jane Smith	01A7AC1671B18FED			<ul> <li>Medium highlighted for deletion</li> </ul>	The medium has been highlighted fo	0
ohn Smith (111)		04/07/2017 09:55:58	Jane Smith	01A7AC1671B18FED			Deactivation started	✓ Deactivation started & Administrato	0
400993282850		04/07/2017 07:47:44		(Mobile)			🕂 Medium added	Smartphone with telephone number	0
bine	, E	04/07/2017 07:46:27	Jane Smith	01A7AC1671B18FED			G Reactivated	✓ Fully reactivated. 🤱 Administrator: J	Q
mobie AB	-	04/07/2017 07:46:27	Jane Smith	01A7AC1671B18FED			Reactivation started	✓ Reactivation started Administrato	
lant		04/07/2017 07:46:18	Jane Smith	01A7AC1671B18FED			Deactivation started	Deactivation started Administrato	
CDE9860F272A	_	04/07/2017 07:45:23	-	0005CDE9860F272A (Assistant)			+ Medium added	Card added. 2 via coding station by	-
ne Smith		03/07/2017 16:25:10	Jane Smith	0005CDE9860F272A (Back door )			<ul> <li>Medium removed from system</li> </ul>	✓ Card removed from system. 🤱 via c	80
AC1671B18FED	_	103/07/2017 16:25:10	Jane Smith	<ul> <li>0005CDE9860F272A (Back door )</li> </ul>			Medium updated	🕵 Authorisations updated 🤱 via codin	80
ne Smith		103/07/2017 16:25:05	Max Mustermann (7)	0005863432EE6819 (Lager)			Medium updated	2 via coding station by administrator J	80
lanspeter		03/07/2017 16:25:02	Jane Smith	0005CDE9860F272A (Back door )			<ul> <li>Medium highlighted for deletion</li> </ul>	The medium has been highlighted fo	-
anspend	·	······································	Jane Smith	01A7AC1671B18FED	Door 1	@ 000508E2C227AD98	Access granted	Battery OK ⊕ Local cylinder time: 0	0.
		12:52:02	Jane Smith	01A7AC1671B18/ED			Medium updated	📮 Protocol updated 🐩 Authorisations	
ODFS6E399B3D		03/07/2017 12:51:02	Jane Smith	01A7AC1671B18FED	Door 1	@ 000508E2C227AD98	+ Cylinder added	+ Cylinder "000508E2C227AD98" add	
ted on 30/06/2017		11:40:54	Max Mustermann (13)	01B14009932B2B50 (Phone)			Medium updated	Authorisations updated & via smart	
ane smith ( door		······································	Jane Smith	0005CDE9860F272A (Back door )			Medium updated	📡 Authorisations updated 🤶 via codin	80
sted on 03/07/2017		03/07/2017 09:28:39		0005CDE9860F272A (Back door )			🕂 Medium added	Card added. 2 via smartphone "01	-
		03/07/2017 09:28:39	Jane Smith	01A7AC1671B18FED			+ Medium added	Card "0005CDE9860F272A" hinzuge	80
2 863432EE6819		03/07/2017 09:27:56	Max Mustermann (17)	<ul> <li>0005CDE9860F272A (keller)</li> </ul>			<ul> <li>Medium removed from system</li> </ul>	Card removed from system. 2 via c	80
ed on 06/06/2017		······································		<ul> <li>0005CDE9860F272A (keller)</li> </ul>			Medium updated	🤱 via coding station by administrator J	-
rtür		03/07/2017 09:27:54	Max Mustermann (17)	0005CDE9860F272A (keller)			- Medium removed manually	The medium has been removed man	80
5863432EE6819		103/07/2017 09:27:46	Max Mustermann (17)	0005CDE9860F272A (keller)			Medium updated	via coding station by administrator J	-

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 carateres no campo de pesquisa 2.
- > Utilize o filtro, p. ex., "Não autorizado" S. 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* s para navegar rapidamente numa lista grande para um determinado dia.
- > Utilize, à esquerda, em baixo, o botão **Exportar o**, 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 <u>Definições</u> 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**.

Delete protocol e	ntries 🛛 🛞
Delete options	
Deleting will remove personal data from the protocol en	itry.
O Delete this log entry	
Delete all log entries of "Jane Smith" regardless of	media and components
Please enter the reason for deletion:	
I would like to irrevocably delete the log entry	
X Cancel	Deletion

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**  $\rightarrow$  **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* 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.

VVA AirKey 📄 Collegation 🖉 English 🔹 🎄 Settings 📲 English 🔹 🎄 Settings							
KOME 🔒 ACCESS CONTIOL SISTEM 🎎 MEDIA 6 PERSONS 🔮 PROTOCOLS 🍰 Administratoris 🛞 HELP							
<b>m protocol</b>	on Transaction ID. Media ID. Component ID	During period from	to a little point				
Nate, time 3 🗸	Administrator (User ID)	Action	Result	Transaction ID			
4/07/2017 12:23:34	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245868			
4/07/2017 11:13:26	John Smith (13968155)	Protocol viewed	The administrator viewed the locking component and media protocol.	245791			
V07/2017 10:48:47	John Smith (13968155)	Medium owner changed	Smartphone 0181400993282850 (Phone) +43 11 22 33 44 55 transferred to John Smith.	245770			
W07/2017 10:30:40	John Smith (13968155)	Medium wiped	Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 123 wiped.	245769			
4/07/2017 10:18:02	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 123 reactivated.	245767			
407/2017 10:18:02	John Smith (13968155)	Reactivation of a medium started	💭 Started reactivation of Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 123. Reason: Found Additional notes: Cre	245766			
4/07/2017 09:59:05	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01C6E70504F10D2F (Smartphone Compact Z3) +43 123 123 123 123 123 started.	245765			
4/07/2017 09:58:34	John Smith (13968155)	Medium highlighted for deletion	Smartphone 01A7AC1671B18FED was highlighted for deletion.	245764			
4/07/2017 09:55:58	John Smith (13968155)	Deactivation of a medium started	C Deactivation of Smartphone 01A7AC1671B18FED +43123123456456 started.	245759			
4/07/2017 09:23:38	John Smith (13968155)	Deletion has been undone	The authorisation Smartphone 01A7AC1671B18FED +43123123456456 for wall reader "000565F246DF929A" (Door 2) has been restored.	245752			
4/07/2017 07:47:44	John Smith (13968155)	Medium added	🛨 Smartphone +43 11 22 33 55 44 66 (Mobile) added.	245690			
4/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium finished	Smartphone 01A7AC1671B18FED +43123123456456 reactivated.	245689			
4/07/2017 07:46:27	John Smith (13968155)	Reactivation of a medium started	D Started reactivation of Smartphone 01A7AC1671B18FED +43123123456456. Reason: Found Additional notes: Credit: 84 KeyCredits	245688			
4/07/2017 07:46:18	John Smith (13968155)	Deactivation of a medium started	Deactivation of Smartphone 01A7AC1671B18FED +43123123456456 started.	245687			
	John Smith (13968155)	Medium wiped	Smartphone 01A7AC1671B18FED +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, selecione **Administradores**  $\rightarrow$  **Login de apoio**.

<b>EVVA</b> AirKey							Credit Sohn Smith Administrator	English • English • Dog off
ACCESS CONTROL SYSTEM	L MEDIA & PERSONS	PROTOCOLS	ADMINISTRATORS	🔞 HELP				
Home Media @ persons		م د	Administrators > Create administrator Support logins		Here you can fine management for system.	l the administrator your AirKey access control	_	+ Add
A 117 Persons	7 Smartphones	2 Cards	(	Send a Key'		2 Cylinder	((ii)) 1 Wall reader	4 Arres
						Door designation Component ID	Maintenance tasks	

Figura 212: Ativações de apoio

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

EVVA	AirKe					Ċ	Credit E3 KeyCredit(s)	John Smith Administrator	English	🔹 🏥 Setting	s 👍 📗 Log off
🏦 номе 🔒	🏫 home 🔒 Access contriol system 🎎 media 6 persons 📓 protocols 🔈 Administrations 🚳 Help										
Support logins											
First name, Last	name, User ID	<ul> <li>All (3) Only val</li> </ul>	id (1)								
	Validity	Valid from	Valid to	First name	Last name	User ID	Comment				
<b>F</b>	~	04/07/2017 12:43:20	04/07/2017 17:43:20	Jane	Smith	21233965					*
	0	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023					=
	0	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417					*
Show 1 to 3 of 3 en	login Block :	support logins									

Figura 213: Lista de ativações de apoio

- > Clique em *Criar login de apoio*.
- Preencha o formulário ①.
   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 2.



	Create support login	$\otimes$	Support login added
ecipient of support login			
* First name	Jane		The new support login has been created.
* Last name	Smith		Access for Jane Smith Validity period 04/07/2017 12:43:20 to 04/07/2017 17:43:20
ogin (access data) * Valid starting now for Comment	5 Hours		Please enter the following access data only for the support employee "Jane Smith". The support login has the same authorisation as you do. support_acos_additional_success_text
User ID Password	Is generated automatically. Is generated automatically.	.t.	User ID 21233965 Password NQhnxFme875 Login page https://uat.airkey.ewa.com/
X Cancel		E Save	🗸 Ci

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, selecione **Administradores**  $\rightarrow$  **Login de apoio**.

Na lista das ativações de apoio poderá ver se existe atualmente uma ativação de apoio válida **1** e o tempo de duração da mesma **2**.

EVVA	) AirKe						Tedit Sin Smith Administrator	English - Settings	(⇔  )]] Log off
🏫 НОМЕ	ACCESS CONTROL	SYSTEM 🎎 MEDIA & PERSONS	PROTOCOLS & ADMINISTRATORS	HELP					
Support login	s ast name. User ID	Q All (3) Only v	alid (1)						
	Validity 1	Valid from	Valid to 2	First name	Last name	User ID	Comment		
(F)	~	04/07/2017 12:43:20	04/07/2017 17:43:20	Jane	Smith	21233965			*
	0	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023			
	0	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417			*
Show 1 to 3 of 3 Create suppo	Block	support logins							

Figura 215: Vista geral das ativações de apoio

- > Selecione 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**.



Block support logins?							
Do you want to block the following support logins? This causes the selected support logins to become invalid:							
First name	^	Last name	Comment				
Jane		Smith	-				

Figura 216: Bloquear ativação de apoio

Na lista de ativações de apoio, poderá reconhecer que a ativação está bloqueada no símbolo na coluna "Válidade" **1**.

номе 🔒	ACCESS CONTRO	AL SYSTEM	PROTOCOLS 🕹 ADMINISTRATO	RS 🕜 HELP				
port logins								
First name, Last	name, User ID	9. Al (3)	Only valid (0)					
	Validity	Valid from	Valid to	First name	Last name	User ID	<ul> <li>Comment</li> </ul>	
	0	04/07/2017 12:43:20	04/07/2017 13:32:47	Jane	Smith	21233965	-	
	0	13/02/2017 10:04:39	13/02/2017 10:07:33	Hans	Berger	39010023		
	0	31/05/2017 11:19:08	31/05/2017 11:19:26	Max	Mustermann	64721417		

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

- > O smartphone tem de corresponder aos <u>Pré-requisitos do sistema</u> 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 por 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 <u>Conectar componentes</u>, 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 <u>Registar smartphone</u>: 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**.



≡ AirKey	¢
<b>Test f. Evva</b> Maintenance authorisation <i>P</i>	•
P Door 2	J
🔑 Door 1	$\odot$
P Door 3	

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.

← Authorisati	on details
🔎 Door 3	()
Hands-free mode	
Permission expired	
Access control system	Test f. Evva
Location	
Temporary access	04.07.2017 14:15 - 14:20
Updated on	04.07.2017 14:11
Created on	04.07.2017 14:11
Component ID	0005DF0E1B14013E

Figura 220: Autorização expirada





Se o seu smartphone tiver autorização para mostrar dados protocolares (ver <u>Dados protocolares na aplicação AirKey</u>), o protocolo da chave da autorização pode ser exibido nos detalhes da autorização **1**.

$\leftarrow$ Key protocol	
🤌 Door 1	1
04.07.2017 14:33:56	
Access granted in Hands-free mode	

Figura 221: Dados protocolares de uma autorização

# 6.4 <u>Tarefas de manutenção</u>: 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 <u>Editar</u> <u>componente de bloqueio</u>), 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 oticamente e acusticamente um bloqueio.
- Recebe uma mensagem de confirmação 0.



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 do 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 <u>Adicionar cartões, porta-chaves ou chaves combinadas com</u> <u>o smartphone</u>.

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.

	Notifications	
	• • •	
All access	control systems	3
22.06.2017	08:45:54	
Test f. Evva <undefined< td=""><td>&gt;</td><td></td></undefined<>	>	
21.06.2017	14:59:11	
Test f. Evva	•	
<undefined< td=""><td>&gt;</td><td></td></undefined<>	>	
14.06.2017	13:10:39	

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" **1**.

Neste caso, podem ser utilizadas as definições em baixo ("Definir o alcance do modo handsfree", "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").


<b>EVVA</b> AirKey		Settings		Settings	
Bluetooth components		Bluetooth	0 ~	Bluetooth	(
A Authorisations	<b>~</b>	Adjust Hands-free range	>	Adjust Hands-free range	
Maintenance tasks	>			Unida free mode	
Office mode		It allows unlocking of locking	$\bigcirc$	Not available because Bluetooth is d	eactivated.
	phone	components using Bluetooth when the smartphone is locked. The function is dependent on the adjusted Hands-free range and is also strongly influenced by the wearing position of the		Unlock from notifications	
Encoding media	ř.	smartphone (trouser pocket, handbag etc.).		You can unlock doors via Bluetooth v to open the app.	without having
Authorisation protocol	Tap	The Hands-free mode must additionally be activated individually for each desired locking component (Main menu -> "Authorisations" -> Tap on the name of the locking component -> Online		In the below menu item "Notification: "Components within range" must also	s" the option o be activated.
Settings	tion	"Hands-free mode").		Security functions	>
		Unlock from notifications		Notifications	>
	aving	You can unlock doors via Bluetooth without having to open the app.		Add access control system	
	tion vated.	In the below menu item "Notifications" the option "Components within range" must also be activated.			
	>	Security functions	>	Info	
	>	Notifications	>		
	>	Add access control system	>		

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.
- Selecione 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 <u>Vista geral da função hands-free (mãos livres)</u>.

# 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 1**, 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.

A 🚺	՝≵ 👄 🤤 ⊿ 82% 🖬 09:23	09:25
OpenVPN für An		A AirKey now A AirKey Door 2
	09	LOCK
AirKey	23 WED, 5 JUL	A AirKey · now ~ AirKey Door 1

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**.

0

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 <u>Informações gerais</u>.



**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 <u>Notificações</u>.

# 6.9.6 Funções de segurança

No menu *Funções de segurança* poderá encontrar três níveis de segurança:



#### Encriptação AirKey 0

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 😢

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 6

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  $Definições \rightarrow Funções de segurança$ .
- > Ative a opção "Encriptação AirKey".
- > Atribua um PIN e toque em **Confirmar**.



Activate encryption		
Enter new PIN:		
r in security.	CANCEL	CONFIRM

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 <u>Introduzir</u> <u>PIN</u>).

# 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.

Change PIN		
Enter old PIN:		
Enter new PIN:		
Repeat new PIN:		
PIN security:		
	CANCEL	CONFIRM

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 reposto 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**.

Deactivate encryption		
Enter PIN:		
<u> </u>		
	CANCEL	CONFIRM

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**  $\rightarrow$  **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".

Settings		
Maintenance authorisation	✓ This smartphone can be used to perform additional maintenance operations on AirKey components	1
Office mode	This medium can activate the manual office mode	
Show event log data	Show the medium event log of the smartphone in AirKey app ①	
<ol> <li>Release duration</li> </ol>	O Normal release duration	
	O Extended release duration	
PIN code of the AirKey app	Deactivate PIN code 1	
Update after each access	Activated (the AirKey app data on the smartphone is updated after each access)	

Figura 235: Administração online do AirKey - Desativar código PIN

> Confirme a pergunta de segurança com o botão **Desativar código PIN**.



7 Deactivate PIN cod	e 😞		
The PIN code of the AirKey app on the smartphone will be deactivated (deleted). The person will be informed as soon as AirKey app is restarted or the app data is updated.			
Are you sure you want to continue?			
X Cancel	Veactivate PIN code		

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**  $\rightarrow$  **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.





#### Notificações sobre componentes no alcance

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 <u>Desbloqueios a partir de notificações</u>).



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 <u>tarefas de manutenção</u>, 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 8

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.

$\equiv$ Bluetooth Komponenten	¢
Bluetooth-Schließkomponenten in Reichweite	ì
Door 2	:
Berechtigung geändert: Neue	NEN

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 <u>Utilizar o smartphone</u> <u>em vários sistemas</u>.

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 <u>Troca de smartphone</u>.

# 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 <u>Iniciar a troca como proprietário do smartphone</u>.

# 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 <u>Informações gerais</u>.



# 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 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**.

$\equiv$ Bluetooth components $0$	■ Bluetooth components	٩	Bluetooth compo	onents
Bluetooth locking components within range	Bluetooth locking components within range	0	Bluetooth locking components w	ithin range  👬
Secreting for looking	In factory state 2788977928	1	> Connect 3	Office mode
components	Door 2 Connect Office mode		Door 2	>
Note the range Wake up the cylinder in advance by touching				

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.



# 0

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 <u>Valores por defeito (para todos os componentes de bloqueio</u> 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 <u>Operação e manutenção do sistema AirKey</u>.

# 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" **1** 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 <u>Editar meio</u>.

Adicionalmente, no menu principal da aplicação AirKey, foi também ativado o ponto do menu **Tarefas de manutenção 1**.





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.

$\equiv$ Maintenance tasks		$\equiv$ Maintenance tasks $\textcircled{O}$
• • •		•••
Test f. Evva	2	Test f. Evva 🔹
Door 2	>	Door 2     () Issue replacement wall reader
Door 1	>	Door 1
Fitzwilliam	0	Fitzwilliam
No maintenance tasks		No maintenance tasks

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  $\odot$  ou leitor de parede  $\odot$ ), o símbolo deste componente de bloqueio tem um fundo amarelo (p. ex.  $\odot$  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 <u>Operação e manutenção do sistema AirKey</u>.

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 <u>Remover componente de bloqueio</u> e <u>Remover meio</u>) 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 0.
- 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* <sup>(3)</sup>.

$\equiv$ Bluetooth components $0$	$\equiv$ Bluetooth components	(7)	Bluetooth	components
Bluetooth locking components within range	Bluetooth locking components within range	0	Bluetooth locking compo	nents within range  💥
Searching for locking	In factory state 2788977928	1	Connect	Office mode
components	Door 2 Ocnnect			
•••	Office mode		Door 2	>
Note the range Wake up the cylinder in advance by touching				

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.



removed The administrator has removed this component from the access control system. Complete the process by updating and disassembling the component. The component will be reset to construction site mode. CLOSE REMOVE	Remove component
Medium must be removed This medium has been highlighted for deletion from the access control system. Would you like to complete the process? The medium will be reset to factory settings. CLOSE REMOVE	Remove medium

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**.

Cancel Mediu	m details	Med	ium must	be remove
Card 1		This mediu deletion fro Would you	m has been om the acces like to comp	highlighted f is control sys lete the proc
- Remove		The medius settings.	m will be res	et to factory
Media type	Medium			
Media ID	0005CDE9860F272A			
Designation	Card 1			
Keyring version	6.18			
Status	<ul> <li>Authorisations, office mode and release duration are up to date.</li> <li>Keyring version not up to date</li> </ul>			
Access control system	Test f. Evva			
Person				



 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 <u>Editar meio</u>.

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 **0**.



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.



■ Settings		=	Settings	
NFC On		Bluetooth		
Bluetooth	- 1	Adjust Hands-free	e range	
Use Bluetooth in AirKey		Hands-free mode It allows u components using B is locked. The funct	nlocking of locking luetooth when the smartphone on is dependent on the	(
Adjust Hands-free range		adjusted Hands-free influenced by the we smartphone (trouse	range and is also strongly earing position of the r pocket, handbag etc.).	
Hands-free mode It allows unlocking of locking components using Bluetooth when the		The Hands-free mod activated individually component (Main m on the name of the I "Hands-free mode")	de must additionally be y for each desired locking enu -> "Authorisations" -> Tap ocking component -> Option	
lependent on the adjusted Hands-free ange and is also strongly influenced by the		Unlock from notif	ications	
wearing position of the smartphone (trouser pocket, handbag etc.).		You can unlock door to open the app.	s via Bluetooth without having	
The Hands-free mode must additionally be activated individually for each desired		In the below menu it "Components within	em "Notifications" the option range" must also be activated.	
the local data and the strend sectors of		Security functions	3	
UNIOCK TROM NOTIFICATIONS You can unlock doors via Bluetooth without having to open the app.		Notifications		
In the below many item "Netifications" the		Add access control	ol system	

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 <u>Editar componente de bloqueio</u>.

#### 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 <u>Registar smartphone</u> e <u>Atribuir autorizações</u>).
- 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 <u>Funções de segurança</u>).
- > 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.







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 <u>Adicionar cartões, porta-chaves e chaves combinadas com o smartphone</u> e <u>Atribuir autorizações</u>).

- 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 0.
- 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.

■ Bluetooth components	$\equiv$ Bluetooth components	Ø	Bluetooth co	Bluetooth components		
Bluetooth locking components within range	Bluetooth locking components within range	0	Bluetooth locking componen	ts within range  🕺		
Searching for locking	In factory state 2788977928	1	> Connect	Office mode		
components	Door 2 2Connect	_	Door 2	>		
Note the range Wake up the cylinder in advance by touching						

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.

<ul><li>Component</li><li>Cylinder in factorial</li></ul>	t details tory state	<ul> <li>Component</li> <li>Door 1 Test f. Evva</li> </ul>	t details (≣
+ Add compon	ent	Component type Model Component ID Firmware version	Cylinder NFC / Bluetooth 000508E2C227AD98 Thumb turn firmware:
Component type Model	Cylinder NFC		4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44
Component ID	0005DF0E1B14013E	Access control system	Test f. Evva
Firmware version	Thumb turn firmware: 4.54 Electronics module firmware: 4.54 Locking component Java Card applet: 6.44	Component status	<ul> <li>Battery OK</li> <li>Time correct</li> <li>Time zone correct</li> <li>Blacklist up to date</li> <li>Areas up to date</li> <li>Release duration up to date</li> </ul>
Access control system	None		<ul> <li>Office mode</li> <li>settings up to date</li> </ul>
Component status	Battery OK		<ul> <li>Firmware up to date</li> </ul>
		Door designation	Door 1

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.

0

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 <u>Valores por defeito (para todos os componentes de bloqueio</u> 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.

~	S Locking component was updated successfully.	~	Locking component was updated successfully.	0
	A Cylinder (NFC): Door 3		Cylinder (Bluetooth): Door 1	
	Update completed successfully		Update completed successfully	

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 <u>Atualizar o smartphone</u>: ver o capítulo 6.10

# 8.3 Atualizar meios

Poderá atualizar qualquer meio AriKey, 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 <u>Codificar meios</u>, 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.

<ul><li>Medium details</li><li>Card 1</li></ul>		<ul> <li>← Medium details</li> <li>(a) Card in factory state</li> </ul>		
Media type Media ID	Medium 0005CDE9860F272A	+ Add		
Designation	Card 1	Media type	Medium	
Keyring version	6.18	Media ID	0005CDE9860F272A	
Status	Authorisations, office mode and release duration are up to date. Keyring version up to date	Keyring version Status	6.18 Authorisations, office mode and release duration are up to date. Keyring version up to date	
Access control system	Test f. Evva	Access control system	None	

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* <sup>(3)</sup>.



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 0**.
- 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.



Cylinder firmware update	Cylinder firmware update
Please place the previously presented cylinder on the coding station.	Processing Do not remove the cylinder from the coding station under any circumstances!
	21/2
	C Public holidays
K Cancel	

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.

	Cylinder firmware update	
Up	date step successful:	
	✓	
<b>~</b> 1	Thumb turn firmware: 4.54	
	Electronics module firmware	
	Functional test	
i	Please remove the component from the coding station. If the component flashes and beeps, once again position it on the coding station to run the update.	C

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 0.
- Ligação por *Bluetooth* (em smartphones Android e iPhones): no menu principal da aplicação AirKey, selecione o ponto do menu *Codificar meios* – ver também <u>Codificar meios</u>.



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

- > Selecione a opção *Atualização do Keyring*.
- > Encoste o smartphone ao meio e siga as instruções.



Update Keyring
The update will be applied to the component.
Hold the smartphone to the component.
CANCEL

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.



2	Medium is updated.
	Card: Back door
	🚴 John Smith
	An update is available for this identification medium:
	🚜 Execute Keyring update (6.18) 1

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.

Keyring update		
Processing Do not remove the medium from the coding station under any circumstances!		
214		
11		

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.

Keyring update	
The Keyring version is up to date (6.18).	
✓	
Remove the medium from the coding station.	
V Close	

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.


~	Medium is updated.	
	Card: Back door	
	🚴 John Smith	
	You can remove the medium from the coding station.	

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

Manual do sistema AirKey | Versão 2.7 | xx/xx/2022 | Sujeito a alterações técnicas e erros de impressão



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:

Battery OK	Exchange battery	Battery empty

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 <u>Sinalização dos componentes de bloqueio</u>.

#### 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, tratase 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 eletrónico 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 eletrónico. Isto não funciona, se o puxador não tiver sido enroscado no módulo eletrónico.



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*  $\rightarrow$  *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* <sup>1</sup>.



ACCESS CO	NTROL SYSTEM 🤐 MEDIA & PERSONS 📄 PROTOCOLS 🎄 ADMINISTRATORS
Edit locking component	
Details Settings Authoris	ed media (own) Authorised media (external)
Details	
Component type	Cylinder
Model	NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status	👔 Battery OK (status from 06/07/2017 14:56:44) 🕒 Time correct 👾 Current time zone
Last update	06/07/2017 14:56:44
<b>Fime and calendar</b> Time zone	Europe/Vienna 🗸 UTC +02:00 🔆
Time and calendar Time zone Public holiday calendar	Europe/vienna       ▼       UTC +02:00          ■ Apply public holiday calendar       → Go to public holidays settings         The following exceptions are controlled by the public holiday calendar:       1. Periodic access authorisations are not valid on public holidays.         2. Automatic office mode is not taken into account on public holidays.
Time and calendar Time zone Public holiday calendar	UTC +02:00 Order of the set of t
Time and calendar Time zone Public holiday calendar Access Office mode	UTC +02:00  UTC +
Time and calendar Time zone Public holiday calendar Access Office mode Automatic office mode	UTC +02:00  UTC +
Time and calendar Time zone Public holiday calendar Access Office mode Release duration	UTC +02:00  UTC +
Time and calendar Time zone Public holiday calendar Access Office mode Release duration	Europe/vienna       UTC +02:00 **         Apply public holiday calendar       Go to public holidays settings         The following exceptions are controlled by the public holidays calendar:       1. Periodic access authorisations are not valid on public holidays.         2. Automatic office mode is not taken into account on public holidays.         Permit manual office mode         Permits manual office mode         Permits manual office mode if you would like to use the automatic office mode function.         5       s normal release duration         20       s extended release duration
Time and calendar Time zone Public holiday calendar Access Office mode Release duration Protocol and maintenance	Europe/vienna       UTC +02:00 >>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>
Time and calendar Time zone Public holiday calendar Public holiday calendar Access Office mode Release duration Protocol and maintenance Personal reference in protocol	Europe/vienna       ▼       UTC +02:00 ※         Apply public holiday calendar       Go to public holidays settings         The following exceptions are controlled by the public holidays calendar:       1. Periodic access autorbiastions are not valid on public holidays.         2. Automatic office mode is not taken into account on public holidays.         Permit manual office mode         Permits manual office mode         Permit manual office mode         Sea activate         Permit office mode* if you would like to use the automatic office mode function.         5       s normal release duration         20       s extended release duration
Time and calendar Time zone Public holiday calendar Public holiday calendar Access Office mode Release duration Protocol and maintenance Personal reference in protocol entries	UTC +02:00  UTC +

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* 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.



	Repair options	
Attention! Please select one of the follow components that have been removed in t	ving repair options only after consult this way can NO longer be used in A	ing your EVVA partner, as the \irKey!
<ul> <li>Remove and install replacement comp Select this option if the component is replacement component will be confi- authorizations remain valid</li> </ul>	ponent <b>1</b> faulty and you would like to install a gured in the same way as the faulty	a replacement component. The component, so that existing
Attention! The faulty component can Replace cylinder (thumb turn and Replace thumb turn only	then NO longer be used in AirKey! electronics module together)	
Remove without replacement and ma Select this option if the component is Attention! The faulty component can	ark as "faulty" faulty and you do NOT want to inst then NO longer be used in AirKey!	all a replacement component.
Note:		
If the component is operating correct click the "Remove" button. In this cas installed in a different location later.	ly, but it has to be removed from the e, the component will be reset to th	e door, close this dialogue and then le factory state and it can then be
A maintenance task is generated on the l station or smartphone in maintenance m	basis of the selected repair option, w ode.	which you can run with a coding
New maintenance task: ZA Issue replace	ement cylinder	
X Cancel		Add maintenance task

Figura 289: Opções de reparação

> Clique em **Adicionar tarefa de manutenção**.

O estado do componente **1** de bloqueio é atualizado e indicado como tarefa de manutenção **2**.

EVVA Airl	Cey 🕞 Credt 👔 Credit 🐊 Administrator 🕅 English 🔹 🎄 Settin	gs 🔄 🗍 Log e
ACCESS CO	trol system 🏦 media 6 persons 📋 protocols 🎄 administrators 🔞 help	
Edit locking component		4h Back
Details Settings Authoris	d media (swr) Autorited media (internal)	
		💾 Sav
betails		
Component type	Cylinder	
Model Component ID	NFC / Buestonh	
Firmware version	Java Grd applet 6.44, Thumb tum version 4.54, Bectronics module version 4.54	
Component status	A hua relacement opinder	
Last update	06/07/2017 14:56:44	
ime and calendar		
Time zone	Europe/Henna • UTC 40200 🐲	
Public holiday calendar	Apply public holiday calendar 🎂 Go to public holidays settings	
	The following exceptions are controlled by the public building obtained. I. Privata: except and indextandoms are not attain public building. 2. Automate effice mode is not taken into accent on public buildings.	
ccess		
Office mode	Permit manual efficie mode	
Automatic office mode	Please activate "Permit office mode" if you would like to use the automatic office mode function.	
Release duration	5 i normal release duration	
	20 setender reliaze duration	
otocol and maintenance		
Personal reference in protocol	® Vulde	
entries	○ Value for Days	
Repair options	Show repair options	
		_
		E 9
	2	49. Ba
Horare All of Lines representation (CP)	. OREZCZ7AD96 2 Maintenance tasks OMWREY CardMan Sc21-CL.0	

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.



# 0

O componente a substituir pode ser atualizado, contanto que a instalação do componente de substituição fique totalmente concluída. Desta forma, assegura-se a integralidade 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 selecione, 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 selecione, 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, selecione, 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 selecione *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.

	Component in factory state	
-	The component does not yet belong to a access control system.	
	Add component to my access control system	
	Issue replacement cylinder	

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.
- 0

>

> 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 marcálo 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**  $\rightarrow$  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**.

THE ACCESS CON	NTROL SYSTEM 🤱 MEDIA & PERSONS 📄 PROTOCOLS 🎄 ADMINISTRATORS
Edit locking component	
Details Settings Authorise	d media (own) Authorised media (external)
Details	
Component type Model	Cylinder NFC / Bluetooth
Component ID	000508E2C227AD98
Firmware version	Java Card applet 6.44, Thumb turn version 4.54, Electronics module version 4.54
Component status Last update	Battery OK (status from 06/07/201714:56:44) 🐚 Time correct 👒 Current time zone : 06/07/2017 14:56:44
Time and calendar	
Time zone	Europe/Vienna 👻 UTC +02:00 🔆
Public holiday calendar	Apply public holiday calendar 🚽 Go to public holidays settings
	The following exceptions are controlled by the public holiday calendar: 1. Periodic access authorisations are not valid on public holidays. 2. Automatic office mode is not taken into account on public holidays.
Access	
Office mode	Permit manual office mode Permits manual office mode with authorised media (smartphones, cards, key tags).
Automatic office mode	Please activate "Permit office mode" if you would like to use the automatic office mode function.
	5 s normal release duration
Release duration	20 s extended release duration
Release duration	
Release duration	
Release duration Protocol and maintenance Personal reference in protocol	Visible
Release duration Protocol and maintenance Personal reference in protocol entries	Visible     Visible for     Days

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" 0**.



Repair options	Ø
Attention! Please select one of the following repair options only after consulting your EVVA partner, as the components that have been removed in this way can NO longer be used in AirKey!	
Remove and install replacement component Select this option if the component is faulty and you would like to install a replacement component. The replacement component will be configured in the same way as the faulty component, so that existing authorisations remain valid	
Attention! The faulty component can then NO longer be used in AirKey! <ul> <li>Replace cylinder (thumb turn and electronics module together)</li> </ul>	
<ul> <li>Replace thumb turn only</li> <li>Remove without replacement and mark as "faulty"</li> <li>Select this option if the component is faulty and you do NOT want to install a replacement component.</li> </ul>	
Attention! The faulty component can then NO longer be used in AirKey!	
Note: If the component is operating correctly, but it has to be removed from the door, close this dialogue and the click the "Remove" button. In this case, the component will be reset to the factory state and it can then be installed in a different location later.	en e
A maintenance task is generated on the basis of the selected repair option, which you can run with a coding station or smartphone in maintenance mode.	
wew mainenance task. « A remove lauty cylinder	
X Cancel	sk

Figura 293: Opções de reparação

> Clique em Adicionar tarefa de manutenção.

O estado do componente **1** de bloqueio é atualizado e indicado como tarefa de manutenção **2**.

(EVVA) AirKey			TI KeyCredit)	Administrator	English	<ul> <li>Settings</li> </ul>	tog of
ACCESS CONTROL SYSTEM	is 📋 protocols 🍰 administrators	HELP					
Edit locking component							4h Back
Details Settings Authorised media (own) Authorised media (externa	0						
Details							💾 Save
Component type Cylinder							
Model NFC / Bluetooth							
Firmware version Java Card applet 6.44, Thumb turn version	4.54, Electronics module version 4.54						
1 Component status 🛛 🔏 Remove faulty cylinder							
Last update 06/07/2017 14:56:44							
Time and colendar							
Time zone Europe/Nenna -	UTC +02:00 🌞						
Public holiday calendar 🛛 Apply public holiday calendar 👳 Go 🕈	o public holidays settings						
The following exceptions are controlled by 1. Periodic access authorisations a 2. Automatic office mode is not ta	y the public holiday calendar: re not valid on public holidays. ken into account on public holidays.						
Access							
Office mode Permit manual office mode	ed media (smartnhones cards key taos)						
Automatic office mode Please activate "Permit office mode" if you	would like to use the automatic office mode function.						
Release duration 5	s normal release duration						
2	s extended release duration						
Protocol and maintenance							
Personal reference in protocol							
entries Visible for Days							
Repair options Show repair options							
							E Save
					_		🦛 Back
criptivoid(0) king components > 000508E2C227AD98			2	2 Maintenance tasks	OMNIKEY Ca	rdMan 5x21-CL 0	. 0

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 1.



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*  $\rightarrow$  *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.

Repair options	8
The "Remove faulty cylinder" maintenance task already exists.	
The faulty component will be removed later. Please remove the faulty cylinder from the door (Door 1 000508E2C227AD98). You can confirm the completed removal at any later point in AirKey (in the renair options or using a smartphone with maintenance).	
<ul> <li>Complete disassembly: the faulty component has already been removed from the door.</li> <li>WARNING: Only completely disassemble cylinders if you are sure they are faulty. The cylinder can then no</li> </ul>	-
longer be used with AirKey.  Delete "Remove faulty cylinder" maintenance task.  Cancels the maintenance tasks for the event that the component is not faulty at all.	
Cancel	

Figura 297: Desinstalar componente de bloqueio com defeito

- Com a opção O componente defeituoso será removidos posteriormente O, 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 2, 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"** <sup>(2)</sup>, a desinstalação sem substituição é revertida. Poderá encontrar mais informações sob a rubrica <u>Reverter tarefas de manutenção para opções de reparação</u>.



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 <u>Remover componente de bloqueio</u>.

#### 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 1 mais tarde ou se a tarefa de manutenção deve ser eliminada 2.

Repair options	$\otimes$
There is a maintenance task "Issue replacement cylinder" for this component.	
Place a component on the coding station at any time in order to make it compatible with "Door 1 000508E2C227AD98" and install it as a replacement component.	
Delete maintenance task "Issue replacement cylinder" This way you can cancel the installation of the replacement component, e.g. because you would like to perform other repair options.	
Savel	e

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 <u>Criar cartões, porta-chaves e chaves combinadas</u> – 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 <u>Atribuir autorizações</u> e <u>Criar autorização</u>.



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, portachaves, 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**  $\rightarrow$  **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**.



EVVA A	irKey				
ACCES	SS CONTROL SYSTEM	State of the second sec	EVENT LOGS	Lange Administrators	P HELP
Home					
Media & persons					+ Add
8		D.			]
5 Persons	29 Smartphones	5 Cards	"Send a Key	" 2 Pending smar replacement op	tphone erations
🔬 At least 1 Androi	d smartphone uses an ou sion (7.5) available ①	ıtdated AirKey app version (le:	ss than 1.6.5). 🛈		

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.

A (AVV	irKey					()) Credit 11 KejConkitté	A System	tert 🔤 English	V Settings	= []] Log (
	IS CONTROL SYSTEM	NA & PERSONS	👃 ADMINISTRATORS 🛛 🔞 HELP							
ng smartphone	replacement operations									
and annual shares	reprocernent operations									
anna APA	. Harden D	Barinasilas	Yahuduun oomtaa	Resident of	Introduc	Reducered stated or		Recented	ketion	

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 <u>Informações gerais</u>). 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**  $\rightarrow$  **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*, selecione botão *Smartphones*.
- > Em alternativa, selecione, no menu principal, **Meios e pessoas**  $\rightarrow$  **Meios**.
- > Selecione na lista de meios o smartphone que deve ser trocado.
- > Clique em *Mais…* → *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.

The row smartphone will be automatically created as soon as the smartphone owner installs the AirKey app and taps the AirKey SMS. The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	w smartphone will be automatically created as soon as the smartphone owner installs the app and taps the AirKey SMS. de for the smartphone replacement will be sent by SMS to the following telephone number: 8423890	The code for the smartphone will be automatically created as soon as the smartphone owner installs the AirKey app and taps the AirKey SMS. The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	The authorisations and settings of t	he current smartphone will be transferred to a new smartphone
AirKey app and taps the AirKey SMS. The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	app and taps the AirKey SMS. de for the smartphone replacement will be sent by SMS to the following telephone number: 8423890	AirKey app and taps the AirKey SMS. The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	The new smartphone will be autom	atically created as soon as the smartphone owner installs the
The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	de for the smartphone replacement will be sent by SMS to the following telephone number:	The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	AirKey app and taps the AirKey SMS	
The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890	de for the smartphone replacement will be sent by SMS to the following telephone number: 8423890	The code for the smartphone replacement will be sent by SMS to the following telephone number: +2378423890		
+2378423890	8423890	+2378423890		
+2378423890	8423890	+2378423890	The code for the smartphone replace	ement will be sent by SMS to the following telephone number:
			The code for the smartphone replac	ement will be sent by SMS to the following telephone number:
			The code for the smartphone replace	ement will be sent by SMS to the following telephone number:
			The code for the smartphone replace +2378423890	ement will be sent by SMS to the following telephone number:

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...**  $\bullet \rightarrow$  **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.

The code for the smar number:	phone replacement will be sent again by SMS to the fo	llowing telephone
+2378423890		
Code for the smartpho	ne replacement:	
O8TOWDR7QPNNPH	HA40NWCQG0	

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**  $\rightarrow$  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**.

arts								
Access control system, Share code Q	Access control system, thank code Q, (All 10). Shares (b) Share code (c)							
Access control system A Cautomer number Released since Share code (valid until)								
No data found	No data found							
Show 0 to 0 of 0 entries	Show 0 to 0 of 0 entries							
Add share								

Figura 308: Ativar componente de bloqueio para partilha

> É gerado um código de ativação de 12 carateres.



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.

0

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 **0**.

ig component a + Add	1 Add locking compone Create area	ccess control system
		Circo e construction de la construcción de la const

Figura 310: Adicionar componente de bloqueio - barra cinzenta

- > Em alternativa, selecione, no menu principal, **Sistema de controlo de acessos**  $\rightarrow$  Componente de bloqueio.
- > Clique em *Adicionar componente de bloqueio* **0**.

			0		
HOME ACCESS CONTROL SYSTEM		ADMINISTRATORS	HELP		
king components					
Door designation, Additional information, Component I(Q) All component types  All (2)	Or	nly own (2) Only exter	nal (0) 🕜 Only current (0)	Not current (2)	
Door designation, Additional information, Component IIQ All component types  All (2) Door designation (additional information)	0r	Only exter	nal (0) 🕜 Only current (0) Component ID	Not current (2) Number of areas	Access contro system
Door designation, Additional information, Component IIQ, All component types  All (2) Door designation (additional information) Door 1	0r	nly own (2) Only exter Component type Cylinder	Anal (0) I Only current (0) Component ID 000508E2C227AD98	<ul> <li>Not current (2)</li> <li>Number of areas</li> <li>2</li> </ul>	Access contro system Own
Door designation, Additional information, Component IIQ All component types  All (2) Door designation (additional information) Door 1 Door 2	0 ^ /	nly own (2) Only exter Component type Cylinder Wall reader	Image         Only current (0)           Component ID         000508E2C227AD98           000565F246DF929A         000565F246DF929A	<ul> <li>Not current (2)</li> <li>Number of areas</li> <li>2</li> <li>4</li> </ul>	Access contro system Own Own
Door designation, Additional information, Component (IQ)         All component types         All (2)           Door designation (additional information)         Door 1         Door 1           Door 1         Door 2         Door 2           Door 1 2         Door 3         Door 3	0 1	nly own (2) Only exter Component type Cylinder Wall reader	aal (0)  Only current (0) Component ID 000508E2C227AD98 000565F246DF929A	<ul> <li>Not current (2)</li> <li>Number of areas</li> <li>2</li> <li>4</li> </ul>	Access contro system Own Own
Door designation, Additional information, Component IIQ, All component types All (2) Door designation (additional information) Door 1 Door 2 how 1 to 2 of 2 entries	0 1	nly own (2) Only exter Component type Cylinder Wall reader	Imall (0)         Image: Only current (0)           Component ID         000508E2C227AD98           000565F246DF929A         000565F246DF929A	<ul> <li>Not current (2)</li> <li>Number of areas</li> <li>2</li> <li>4</li> </ul>	Access contro system Own Own

Figura 311: Adicionar componente de bloqueio

- Selecione como tipo Componente de bloqueio partilhado 0.
- > Clique em *Continuar.*



Add locking	g component
Please select the type of the new component:	
Component in factory	Shared locking component

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.

	Add shared locking compo	onent 😞
Enter the share code of	the external locking component to add	it to your access control system:
* Sł	hare code	
X Cancel	1/2	Continue

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.



	Add shared loci	king component	¢
ihared access control syst	em (owner)		
Access control system			
Test f. Evva			
Customer number			
airkey_SUHXLAFHBO			
Access control system info	rmation		
Austria			
ihared locking componen	t		
Component type			
Cylinder			
Component ID			
000508E2C227AD98			
Door designation			
Door 1			
Additional information			
Alternative door designation	n 1		
Alternative door designa	tion	]	
Data protection 2			
Personal reference in	protocol entries is for	owner "Test f. Evva": visible	e.
Personal reference in	protocol entries is for	owner "Test f. Evva": not v	isible.
¥ Cancel	2/	7	Add
Concer	21	2	TAU

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**  $\rightarrow$  **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 <u>Criar autorização</u>. 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*  $\rightarrow$  *Componente de bloqueio*.
- > Clique, na lista geral, no componente de bloqueio cujos detalhes pretende consultar.
- Clique em *Meio autorizado (externo)* **1**, para obter uma vista geral de todos os meios de terceiros que têm uma autorização neste componente de bloqueio.

EVVA) AirKey		(1) Subschein State Smith
🟫 HOME 🔒 SCHLIESSANLAGE 🏼 🎎 MEDI	en & personen 📋 protokolle 🛛 & administratoren 🕜 hilfe	
chließkomponente bearbeiten		
Details Einstellungen Berechtigte Medien (eigene)	Berechtigte Medien (fremde)	
Medien von fremden Schließanlagen		
Medien von fremden Schließanlagen		
Medien von fremden Schließanlagen	٩)	
Medien von fremden Schließanlagen Medien-ID, Schließanlage Medien-ID	<ul> <li>schließanlage</li> </ul>	Schließanlagen-Informationen
Medien von fremden Schließanlagen Medien-ID, Schließanlage Medien-ID 0005CDE98607272A	<ul> <li>Schiefanlage</li> <li>Test f. Eva</li> </ul>	Schließanlagen-informationen Österreich, E-Mail: m.eberhardtigewa.com



# 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**  $\rightarrow$  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 1**.



Sha	res							
	Access control sys	stem, Share code Q				All (1)	Shares (1)	Share codes (0)
	Access control system A Customer number Released since Share code (valid until)							
	<b>V</b>	Fitzwilliam	- 4	airkey_HYM7LPWAE4	07/07/2017 08:55:12			
	Show 1 to 1 of 1 entr	ies						
	🏦 Add share	I Delete share (1)						

Figura 317: Bloco "Ativação de partilha" - Eliminar partilha

> Confirme a pergunta de segurança com **Apagar partilha**.

	Delete share	$\otimes$
Do you want to delete this share locking component "Door 1".	e? All users of the affected system will lose their k	eys for the
- Fitzwilliam		A.
X Cancel	Telete :	share (1)

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 <sup>1</sup>.



=	Settings	
Bluetooth		~
Adjust Hands-free	range	>
Hands-free mode		
It allows the automat via Bluetooth after u the smartphone doe least one system.	ic opening of locking components nlocking the smartphone. However s NOT need to be unlocked for at	5
The function depend configured Hands-fr influenced by the loo pocket, handbag, etc	is on the smartphone used, the ee range and is also strongly ration of the smartphone (trouser c.).	
Unlock from notifi	cations	
It allows the manual Bluetooth from notifi smartphone. Howew to be unlocked for at	opening of locking components via cations after unlocking the er, the smartphone does NOT need least one system.	i.
In the below menu it "Components within	em "Notifications" the option range" must also be activated.	
Security functions		>
Notifications		>
Add access contro	ol system 🕕	>
Replace smartphc	ne	
You can use this fun authorisations and s	ction to transfer your AirKey ettings to a new smartphone.	>
Info		>

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 selecionar 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 <u>Ativar PIN</u>.



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 <u>Troca de smartphone</u>.



# 12 AirKey Cloud Interface (API)

A AirKey Cloud Interface é uma interface (<u>API</u>) para sistemas de terceiros, que tem por base o <u>REST</u>. 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 <u>documenta-</u> <u>ção da API</u> (em inglês). O seu integrador ou programador dos softwares de terceiros trata da implementação.



Experimente a função da AirKey Cloud Interface a partir da <u>Demo da EVVA</u> <u>AirKey Cloud Interface</u>.

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 <u>Editar administrador</u>).

# **12.1** Ativação da AirKey Cloud Interface

0

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**.

AirKey Cloud Interface (API)	
	The AirKey Cloud Interface is a REST interface (API) for third-party systems. The interface allows certain functions of AirKey to be controlled via third-party software.
Necessary KeyCredits for activation	350
Number of API requests (commands) per day	700
	Activate 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.



For activation, the KeyCredits listed below will be deducted from your credit.	
Necessary KeyCredits for activation: 350	
Not enough credit. Use the AirKey Cloud Interface KeyCredit card. Add credit	

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 reposto 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 impor***tantes 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 <u>Editar administrador</u>).



Se os "Requests" da API por dia não forem suficientes no seu caso concreto, entre em contacto com a <u>Assistência da EVVA</u>.

# 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**.



AirKey Cloud Interface (API)				
Endpoint Number of API requests (commands) per day	The AirKey Cloud Interface is a RE Details can be found in the <u>API dc</u> https://uat.api.airkey.evva.com:44 700	ST interface (API) for third-party systems. The interface ocumentation. 3/cloud	allows certain functions of AirKey to be controlled via	third-party software.
API key list	API key ID No data found Show 0 to 0 of 0 entries Generate API key Available	Date, time	Description	IP whitelist

Figura 322: Gerar chave para a API

> Confirme a caixa de diálogo novamente com *Gerar chave para a API*.

Generate API key	$\otimes$	
With a click on the button "Regenerate" a new API key will be generated and saved immediately.		
If you have opened this dialog by clicking on the "Regenerate" command, the corresponding existing API key will be replaced by a newly generated one. The replaced API key loses its validity immediately.		
X Cancel Regenerate		

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.



Edit API key	8
The API key consists of API key ID and access key separated by a hyphen (-).	
Now copy the API key to use it in the REST programming.	
For security reasons, the API key is not saved in plain text in the AirKey system and can be displayed!	therefore no longer
Use the IP-Whitlist to allow access only from registered IP addresses.	
API key	l via third-party softwar
- lvkTo1lVkfrhjA8d-Em5ChVVJs21JNzP98GYeJxWJof5XTqATTuTza5BJpLyRT1Yd	
Description	
	r IP with the list.
IP whitelist (allowed IP addresses)	
192.168.0.1, 10.20.30.0/24, 1001:1002:0:0:0:0:0:0:008,	
X Cancel	Save

Figura 324: Gerar chave para a API, detalhes



Utilize a função da lista de endereços IP permitidos para aumentar a segurança. Registe 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, achave da APIsó 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 list		API key ID	Date, time	Description		IP whitelist		•	0
		lvkTo1lVkfrhjA8d	10/05/2019 09:36:01		/	1	Regenerate	Delete	Deactivate
		I440VdP2kjFjtNPM	10/05/2019 10:15:50	3rd party	1	1	Regenerate	Delete	Deactivate
	Show 1 to	2 of 2 entries							

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 <u>Gerar chave da API</u>.

### 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* <sup>(5)</sup> ou *Ativar*.
- > Confirme a caixa de diálogo com **Desativar** ou **Ativar** para concluir o processo.

Deactivate API key	8
The existing API key will be deactivated and can only be used again for API access	s after a new activation.
X Cancel	Deactivate

#### Figura 327: Desativar a chave da API

	Activate API key	8
The deactivated API	key will be activated. The API key, description	n and IP whitelist remain unchanged.
15:50		
X Cancel		Activate

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.

AirKey Cloud Interface (API) – test	environment		
	The test environment gives you the possibility to test the AirKey Cloud Interface (API) in a protected environment with test data before activation.		
	Note: No KeyCredits are required and no SMS will be sent out.		
	Details can be found in the API documentation.		
Endpoint	https://integration.uat.api.airkey.evva.com:443/cloud		
API key	pXJx08M9aDvXAzZT-HqiJGKYR6FC7mVv6BJ85kkznYNj8d73ofiPYb5haTOkCc82v		
	Generate API key Generate test data There are no API test data yet.		

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 <u>Documentação da API</u>. 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.

AirKey Cloud Interface (API) – test	environment
	The test environment gives you the possibility to test the AirKey Cloud Interface (API) in a protected environment with test data before activation.
	Note: No KeyCredits are required and no SMS will be sent out.
	Details can be found in the API documentation.
Endpoint	https://integration.uat.api.airkey.evva.com:443/cloud
API key	pXJx08M9aDvXAzZT-HqjlGKYR6FC7mVv6BJ85kkznYNj8d73ofiPYb5haTOkCc82vaCc82
	Generate API key       Generate test data       There are no API test data yet.

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 <sup>*)</sup>	Sinal sonoro <sup>*)</sup>	Indicação
Sinal 1	Processo de aber- tura com meio autorizado	••••	mmmmm	
Sinal 2	Fim do tempo de partilha	••••	bbbbb	
Sinal 3	Processo de aber- tura 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 indica- do com o símbolo de "pilha gasta".)	••••	aa -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 desblo- queio ou duas sema- nas 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 pil- has e reiniciação do componente	• • • • • •	bbmmaa	
Sinal 9	Meio sem segmen- tação EVVA; meio de sistema de con- trolo de acessos de terceiros	•••	Nenhum	Não está mais em uso. Apenas o sinal 3 é usado para esse fim.
Sinal 10	Erro de comunica- ção e de hardware de um componen- te de bloqueio	••-•-•-•-•-•-•-•-••-••-•••••••••••••	mmmmmm mmmmmm mmmmmm mmmmmm	É sinalizado, p. ex., devido a uma falha de conexão entre o puxa- dor e o módulo eletró- nico de um cilindro.



Número do sinal	Evento	Sinal ótico <sup>*)</sup>	Sinal sonoro <sup>*)</sup>	Indicação
Sinal 11	Atualização do firmware de um componente de bloqueio	•-•-•-•-• (1 seg período, 12 ms impulso)	Nenhum	Duração: até que a comunicação esteja concluída
Sinal 12	Atualização de um componente de bloqueio / de um meio executada com sucesso	••-••	ааааа	
Sinal 13	Falha na atualiza- ção de um compo- nente de bloqueio / de um meio	••-••	ЬЬЬЬЬ	
Sinal 14	Processo de leitura de um meio AirKey	•-•-• (100 ms período, 10 ms impulso)	Nenhum	Duração: até que a comunicação esteja concluída
Sinal 15	Ativação e dispo- nibilidade Blue- tooth dum cilindro AirKey (p. ex., depois de tocá-lo)	●-●-●-●-● (1,5 s período)	Nenhum	
Sinal 16	Início abertura permanente	•••	mmmaaa	
Sinal 17	Fim abertura permanente	•••	aaammm	
Sinal 18	Alimentação de emergência de um cilindro AirKey		aaa mmmmmm mmmmmm mmmmmm aaa mmmmmm mmmmmm mmmmmm mmmmmm bbmmaa aaaa	Causa: uma das pilhas foi colocada de forma incorreta ou está vazia.

\*) Explicação dos sinais:

Sinais óticos: amarelo ●, vermelho ●, verde ●, azul ●

Sinais sonoros: a = tom alto, m = tom médio, b = tom baixo

Cada sinal corresponde a uma duração de 50 ms, as pausas são caracterizadas por "-".



## **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 <u>AirKey Cloud Interface (API)</u>

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 <u>Pré-requisitos do sistema</u>.

# **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 <u>Sinalização dos</u> <u>componentes de bloqueio</u>), 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 (<u>Assistência da EVVA</u>).



## **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



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 | VdS<sup>1</sup>

<sup>&</sup>lt;sup>1</sup> 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, selecione o botão Leitor de parede.
- > Em alternativa, selecione, 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  $\rightarrow$  Doorbus B-
- Pino 3 da ficha  $\rightarrow$  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 bemsucedido

<b>APDU Bytes</b>	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

#### 18.3.1 APDU do registo protocolar

#### 18.3.2 Registo protocolar de 14 bytes

Byte	00	01	02	03	04	05	06	07	08		09	10	11	12	13
Description	lo	ockin	gSys	temI	d	Timestamp				Unlocking	customerID			D	
											status	(	not u	used	)
Example	0e	4e	25	34	fO	32 76 d3 b9				7a	00	00	02	8c	

#### 18.3.2.1 Formato Timestamp

By	te 1								Byt	te 2								By	te 3								Byt	e 4							Byte
8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1		8	7	6	5	4	3	2	1	Bits
*	*	*	*	*	*																														R1
						*	*		*	*																									R2
											*	*	*	*	*																				R3
																*		*	*	*	*														R4
																						*	*	*	*		*	*							R5
								1									1									1			*	*	*	*	*	*	R6
																																			Example
0	0	1	1	0	0	1	0		0	1	1	1	0	1	1	0		1	1	0	1	0	0	1	1		1	0	1	1	1	0	0	1	R7

- **R1** ... 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)

			Byt	e 1				Description
b8	b7	b6	b5	b4	b3	b2	b1	Bit
0								R1
1								R2
	0	0	0					R3
	0	0	1					R4
	0	1	0					R5
	0	1	1					R6



	1	0	0					R7
	1	1	0					R8
	1	0	1					R9
	1	1	1					R10
				٠	٠	٠	٠	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 noutro 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 protocolar: 0e 4e 25 34 f0 32 76 d3 b9 7a 00 00 02 8c
  - IockingSystemId: 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 <u>Utilizar a estação de codificação através da linha de comando</u>.

## 19 Declaração de conformidade

EVVA Sicherheitstechnologie GmbH Wienerbergstraße 59–65 | A-1120 Wien | www.evva.com T +43 1 811 65-0 | F +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.	
60000000000000000000000000000000000000	E.A.AI.	
	E.A.HB.	
AirKey-Hybridzylinder	E.A/[System].PZ	
AirKey-Hangschloss	E.A.HA.	
AirKey-Wandleser	E.A.WL.	
AirKey-Steuereinheit	E.A.WL.CU.	
AirKey-Notstromgerät	E.ZU.NG.V1	

Hersteller:

#### EVVA Sicherheitstechnologie GmbH

Wienerbergstraße 59-65 A-1120 Wien Österreich

Die alleinige Verantwortung für die Ausstellung dieser Konformitätserklärung trägt der Hersteller. Gegenstand der Erklärung sind alle seriengefertigten Produkte ab dem Ausstellungsdatum dieser Erklärung. Der oben beschriebene Gegenstand der Erklärung erfüllt die einschlägigen Harmonisierungsvorschriften der Union:

- Richtlinie 2014/53/EU ("Funkanlagen Richtlinie")
- Richtlinie ROHS 2011/65/EU in der Fassung von 2014/76/EU

Angewandte harmonisierte Normen:

- EN 62368-1:2014 bzw. IEC 62368-1:2014
- EN 300330 V2.1.1
- EN 300328 V2.1.1
- EN 301489-3 V2.1.1
- EN 301489-17 V3.2.0
- EN 50364:2010
- EN 62479:2010
- EN 50581:2012

 Raiffeisen Bank International AG IBAN\_AT823100000600669705 BIC: RZBAATWW Bank Austria IBAN: AT761200000616194700 BIC: BKAUATWW GF: Mag. Stefan Ehrlich-Adám UID-Nr.: ATU 65126268 | FN 120755 g. HG Wien | DVR: 0131504 ARA-Lzenz-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

#### **Declaration of Conformity** 20





EVWA 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

	١.,	i de la com	e de la		
1223	-	SPAIR	1141	 	
1620.9		2188			

Raffeisen Bank International AG IBAN: AT823100000600669705 BIC: RZBAATWW

Bank Austria IBAN: AT761200000616194700 BIC: BKAUATWW

GF: Mag. Stefan Ehrlich: Adám UID-Nr. ATU 65126268 | FN 120755 g, HG Wien | DVR. 0131504 ARA Lizenz:Nr. 2383 (alle Verpackungen entpflichtet) | bbr: 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

1-1

Mag. Stefan Ehrlich-Adám Managing Director

Vienna, 13.06.2017

EU-Declaration of Conformity\_AIRKEY / 2



## 21 Índice das figuras

Figura 1: Arguitetura do sistema	
Figura 2: Vista geral do sistema – Seguranca sem lacunas	12
Figura 3: Link "Registo AirKev"	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: Aiuda 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.inlp	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: Servico 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 fichei	ro 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: Registar 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 smartphon	e
Android / por Bluetooth no caso de Smartphone Android / por Bluetooth no caso de iPhone	e)
	-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 (PDE)	109
Figura 166	: Eliminar nessoa	109
Figura 167	: Eliminar pessoa – Pergunta de segurança	110
Figura 168	: Atribuir meio	110
Figura 160	: Atribuir meio à nessoa	110
Figura 170	: Atribuir meio à pessoa	111
Figura 170	: Lista de mejos	117
Figura 172	: Adicionar moio	112
Figura 172		112
Figure 174	: Editar maio Cartão	114
Figure 175	. Luital IIIelo - Calitao	114
Figure 175	Editar maia Alterar autorização	115
Figura 170	v: Eultar meio – Alterar autorização	116
Figure 170	. Alterar acosco	110
rigura 178		116
Figura 1/9		11
rigura 180	: Eliminar autorização	11/
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 1	L20
Figura 186:	Reativar o meio desativado 1	L20
Figura 187:	Reativar meio	
Figura 188:	Reativar meio	
Figura 189:	: Reativar meio – Restabelecer autorizações	
Figura 190:	Duplicar um meio 1	122
Figura 191:	Duplicar meio 1	122
Figura 192:	Meio vazio1	L23
Figura 193:	Meio vazio - Pergunta de segurança1	123
Figura 194:	Meios atribuídos 1	124
Figura 195:	Meio – Cancelar atribuição 1	125
Figura 196:	Cancelar atribuição sem autorizações1	125
Figura 197:	Cancelar atribuição com autorizações1	125
Figura 198:	Cancelar atribuição – Mudar pessoa 1	126
Figura 199:	Mudar pessoa 1	126
Figura 200:	Mudar pessoa 1	127
Figura 193:	Remover meio – Caixote do lixo 1	127
Figura 202:	Remover meio 1	127
Figura 203:	Protocolos 1	128
Figura 204:	Ativação da visualização dos protocolos - selecção do segundo administrador1	129
Figura 205:	Ativação da visualização dos protocolos - introdução do código de confirmação	0
	1	129
Figura 206:	Protocolo Componentes de bloqueio e áreas 1	130
Figura 207	Ativação da vienalização dos protocolos — colossão do cogundo administrador1	1 2 2
rigula 207.	Ativação da visualização dos protocolos – selecção do segundo administradori	132
Figura 208:	Ativação da visualização dos protocolos – selecção do segundo administrador a Ativação da visualização dos protocolos – introdução do código de confirmação	0
Figura 208:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação	0 132
Figura 209: Figura 209:	Ativação da visualização dos protocolos – selecção do segundo administrador Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios 1	0 132 132 133
Figura 207: Figura 208: Figura 209: Figura 210:	Ativação da visualização dos protocolos – selecção do segundo administrador Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios 1 Apagar os registos protocolares 1	0 132 133 134
Figura 209: Figura 208: Figura 209: Figura 210: Figura 211:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios 1 Apagar os registos protocolares 1 Protocolo do sistema 1	0 132 133 133 134 135
Figura 209: Figura 209: Figura 209: Figura 210: Figura 211: Figura 212:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação 	0 132 133 134 135 136
Figura 209: Figura 209: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios 1 Apagar os registos protocolares 1 Protocolo do sistema 1 Ativações de apoio 1 Lista de ativações de apoio 1	0 132 133 134 135 136 136
Figura 207: Figura 208: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 214:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação 	o 132 133 134 135 136 136 136
Figura 207: Figura 208: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 214: Figura 215:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação 	0 132 133 134 135 136 136 137 137
Figura 209: Figura 209: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 213: Figura 214: Figura 215: Figura 216:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios 1 Apagar os registos protocolares 1 Protocolo do sistema 1 Ativações de apoio 1 Lista de ativações de apoio 1 Criar ativação de apoio 1 Vista geral das ativações de apoio 1 Bloquear ativação de apoio 1	0 132 133 134 135 136 136 137 137
Figura 207: Figura 208: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 214: Figura 214: Figura 215: Figura 216: Figura 217:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação 	l 32 o l 32 l 33 l 34 l 35 l 35 l 36 l 36 l 37 l 37 l 38 l 38 l 38
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios	132 0 132 133 134 135 136 136 137 138 138 138
Figura 209: Figura 209: Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 213: Figura 214: Figura 215: Figura 216: Figura 217: Figura 218: Figura 219:	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios	132 0 132 133 134 135 136 136 137 138 138 138 140 140
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios	132 0 132 133 134 135 136 136 137 137 138 138 138 140 140
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1      Ativação da visualização dos protocolos – introdução do código de confirmação      1      Protocolo dos meios	132 o 132 133 134 135 136 136 136 137 137 137 138 138 140 140 140
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1      Ativação da visualização dos protocolos – introdução do código de confirmação      1      Protocolo dos meios	132 0 132 133 134 135 136 136 137 138 138 138 138 140 140 140 140 141
Figura 207: Figura 208: 	Ativação da visualização dos protocolos - selecção do segundo administrador 1      Ativação da visualização dos protocolos - introdução do código de confirmação	132 o 132 133 134 135 136 136 137 137 137 138 138 140 140 140 141 141
Figura 207: Figura 208: 	Ativação da visualização dos protocolos - selecção do seguindo administrador 1      Ativação da visualização dos protocolos - introdução do código de confirmação	132 o 132 133 134 135 136 136 137 138 137 138 138 140 140 140 140 141 141 142 :h
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação 	132 o 132 133 134 135 136 136 137 137 137 138 138 138 140 140 140 141 141 141 142 :h
Figura 207: Figura 208:  Figura 209: Figura 210: Figura 211: Figura 212: Figura 213: Figura 213: Figura 214: Figura 214: Figura 215: Figura 216: Figura 217: Figura 218: Figura 219: Figura 220: Figura 220: Figura 221: Figura 222: Figura 223: Figura 223: Figura 225:	Ativação da visualização dos protocolos – selecção do segundo administrador i Ativação da visualização dos protocolos – introdução do código de confirmação 	132 o 132 133 134 135 136 136 136 137 137 137 137 137 138 140 140 140 141 142 141 142 142 th 142
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios	132 0 132 133 134 135 136 136 137 138 138 138 140 140 140 141 141 142 141 142 143 143
Figura 207: Figura 208: 	Ativação da visualização dos protocolos – selecção do segundo administrador 1 Ativação da visualização dos protocolos – introdução do código de confirmação Protocolo dos meios	132 o 132 133 134 135 136 136 137 137 137 138 138 140 140 140 141 142 141 142 143 143



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 Bluetoo	oth
	160
Figura 252: Remover um meio com o iPhone	101
Figura 253: Remover Melo	161
	162
Figura 255: Definições AirKey-App	163
	165
Figura 257: Tag IOS NFC	102
Pigura 258: Aplicação Airkey – Conecte com o componente (Android NFC / Android	167
Figure 250. Atustizer dedee	107
Figura 259: Atualizar uduos	100
Figura 260: Mensagens de atualização	168
Figura 261: Atualizar o componente de bioquelo com a estação de codificação	169
Figura 262: Componente de bioqueio atualizado com a estação de codificação	109
Figura 263: Simbolo "Conecte com o componente" (so em smartphones Androld)	170
	170
Figura 265: Aplicação Airkey atualiza um meio	171
	171
Figura 267: Meio proprio ou de terceiros atualizado com a estação de codificação	1/1
Figura 268: Aplicação Airkey – Conecte com o componente (Android NFC / Android	1 7 0
Bluetootn / IPnone)	172
Figura 269: Conecte com o componente – Atualização do firmware	1/3



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:	Opcões 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 OR 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	- 200
Figura 300:	Adicionar partilha	201
Figura 310:	Adicionar componente de bloqueio - barra cinzenta	201
Figura 311:	Adicionar componente de bloqueio	- 202
Figura 212	Adicionar componente de bloqueio ativado para partilha	- 202
Figure 212	Adicionar componente de bloqueio ativado para partilha	- 203
Figure 214	Adicionar componente de bloqueio ativado para partilha	- 203
Figure 215	Autorização do componente de bloqueio ativado para partilha	204
Figure 21C	Autorização de componente de bioqueio ativado para partina	- 205
riyura 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

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, pul- seiras 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 admi- nistração do sistema de bloqueio AirKey e a atribuição de autorizações para componentes de bloqueio.

No âmbito do AirKey, são utilizados os seguintes termos, entre outros:



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 ( <u>API</u> ) para sistemas de terceiros, que tem por base o <u>REST</u> . A interface permite comandar determinadas funções do AirKey através de um software de terceiros.
Interface RS485	A <u>interface RS485</u> 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	<u>APDU</u> 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 adminis- trador 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	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.
	A autorização de manutenção pode ser ativada na Administração online do AirKey para o smartphone desejado.



## 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: <a href="https://www.evva.com/pt/airkey/systemmanual/">https://www.evva.com/pt/airkey/systemmanual/</a>.

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