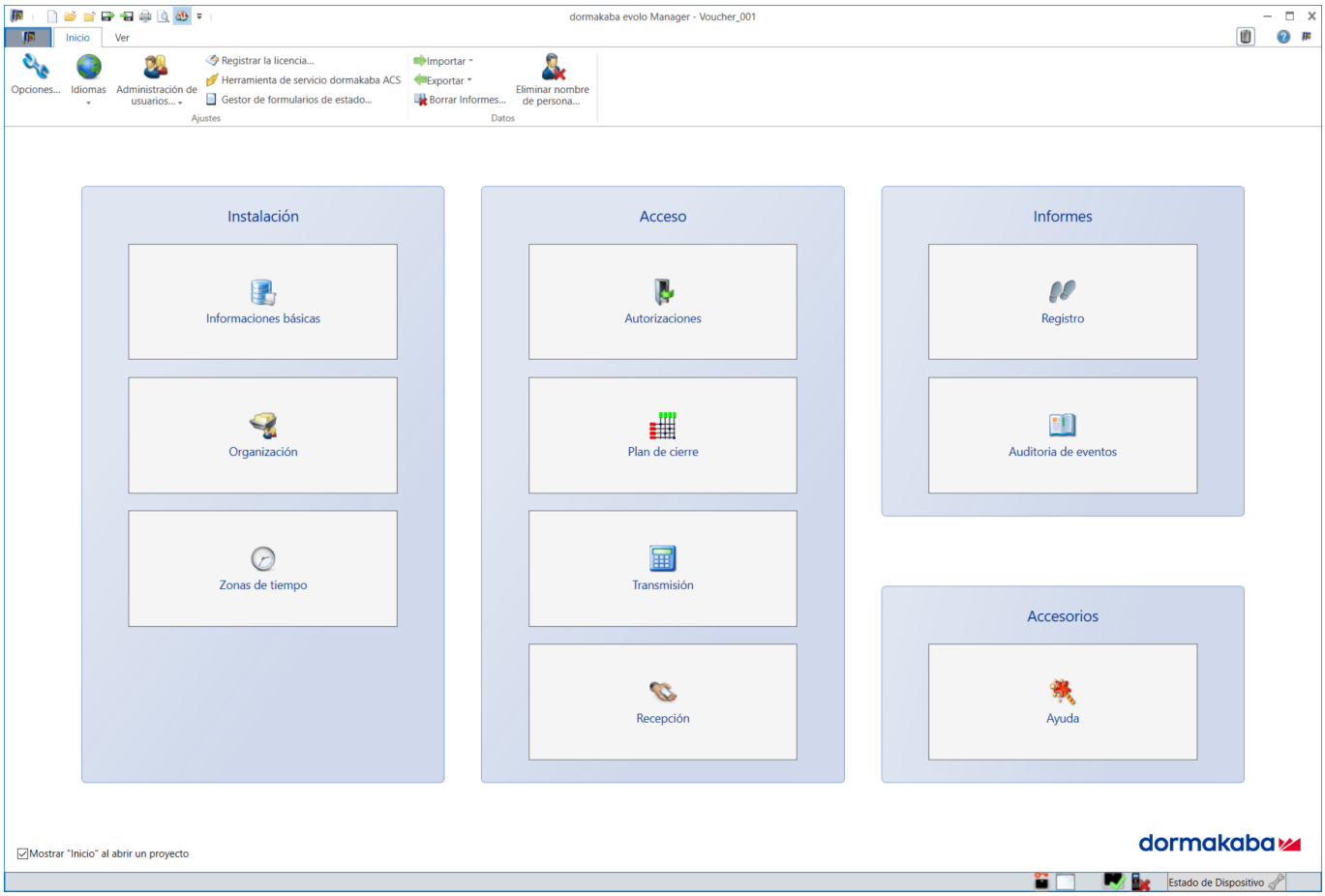
evolo Manager

V7.2

Instrucciones de operación



Público - 06/2026

ES

Índice de materias

1 Acerca de este documento

1.1 Validez

Este documento describe el producto:

Denominación del producto:	KEM (dormakaba evolo Manager)
Versión:	7.1

1.2

1.3 Público destinatario

Este documento se orienta únicamente a personal cualificado.

En las descripciones se asume que el personal es cualificado y formado por el fabricante. Las descripciones no pueden reemplazar la formación en el producto.

Este documento también sirve para dar información a las personas con las siguientes tareas:

- Puesta en funcionamiento del producto en la red
- Adaptación específica al cliente mediante el ajuste de parámetros

1.4 Contenido y finalidad

El contenido de esta guía se limita a lo siguiente:

- El manejo
  - del software dormakaba evolo Manager (KEM)
  - del software dormakaba CheckIn
  - del software KEM Operator
- La puesta en marcha de componentes inalámbricos
- La puesta en marcha de componentes de Mobile Access Descripción en Capítulo
- La puesta en marcha del terminal
- Puesta en servicio del gestor de accesos y del lector de códigos PIN.
- La instalación de la versión multiusuario
- El uso de la Herramienta de servicio ACS

Los ejemplos y proyectos de sistemas de bloqueo utilizados en este manual son ficticios y únicamente tienen fines de demostración.

1.5 Definiciones

Esta guía incluye expresiones especializadas que están explicadas en el glosario. Para facilitar la lectura de la guía, en este documento se usarán las siguientes abreviaturas.

Denominación abreviada	Denominación del producto
Software KEM	dormakaba evolo Manager
Servicio evolo	Servicio dormakaba evolo
Herramienta de servicio ACS	Herramienta de servicio ACS de dormakaba
Programador 1460	Programador 1460 dormakaba
Programador 1364	Programador 1364 KABA
Programador	Programador 1460/Programador 1364
Lector de sobremesa	Lector de sobremesa 91 08 dormakaba
Terminal	Terminal 96 00 dormakaba
Gestor de acceso	Gestor de acceso dormakaba 9200(-K7)
Lector compacto	Lector compacto 9112
Unidad de detección	Unidad de detección 9002
Cilindros mecatrónicos	Cilindro mecatrónico dormakaba
Cilindros digitales	Cilindros digitales dormakaba
c-lever	C-lever dormakaba
c-lever	C-lever pro dormakaba
evolo	evolo
elolegic	elolegic
elostar	elostar
Gateway	Gateway inalámbrica
Actuador	Componente
NFC	Near Field Communication
Bluetooth	Bluetooth®
Smartphone	Dispositivo en el que está instalada la aplicación dormakaba Mobile Access
mobile access App	dormakaba mobile access App
VCP	(Versatile Configuration Package) Paquete de configuración

1.6 Documentación complementaria

Los siguientes documentos están disponibles a través del distribuidor:

- Instrucciones de funcionamiento del programador 1460
- Descripción del sistema evolo
- Pauta de planificación del sistema inalámbrico
- Pautas de planificación de Mobile Access
- Manuales técnicos de los componentes utilizados

1.7 Disponibilidad de los documentos

Encontrará documentación complementaria en el sitio web de dormakaba. Los manuales técnicos se encuentran almacenados en un área protegida (Extranet). Se puede acceder a ellos a través de la cuenta de usuario de un técnico o de una cuenta de usuario temporal.

https://www.dormakaba.com/extranet-emea-de

1.8 Advertencias

Este manual contiene indicaciones que debe observar para su seguridad personal y para evitar daños materiales. Las indicaciones relativas a su seguridad personal están resaltadas mediante un triángulo de advertencia y las indicaciones relativas únicamente a los daños materiales no aparecen con triángulo de advertencia. En función del nivel de riesgo, las advertencias se representan de más a menos riesgo de esta forma:

⚠ PELIGRO

Riesgo elevado

Indica una amenaza inminente que, de producirse, ocasionará lesiones corporales graves o la muerte.

⚠ ADVERTENCIA

Riesgo medio

Indica una probable situación peligrosa que puede ocasionar lesiones corporales graves o la muerte.

⚠ ATENCIÓN

Riesgo reducido

Indica una posible situación de peligro, que puede provocar lesiones leves.

AVISO

Instrucciones para el uso correcto del producto

El incumplimiento de estas instrucciones puede provocar fallos de funcionamiento. El producto puede resultar dañado.

En caso de que aparezcan varios niveles de riesgo, siempre se debe tener en cuenta la advertencia que indique el mayor riesgo. Si una advertencia alerta de daños personales, la misma advertencia también puede alertar de daños materiales.

Otros símbolos de advertencia:

Peligro general

Peligro de explosión

Peligro por corriente eléctrica

DES: peligro por descarga electrostática

Para el manejo seguro del producto, aparecerán indicaciones e información útiles de esta forma:

Consejos de uso e información útil.
Ayudan a hacer un uso óptimo del producto y sus funciones.

2 Introducción

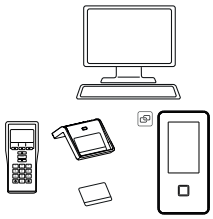
2.1 Para todas las tareas de gestión de personas y medios

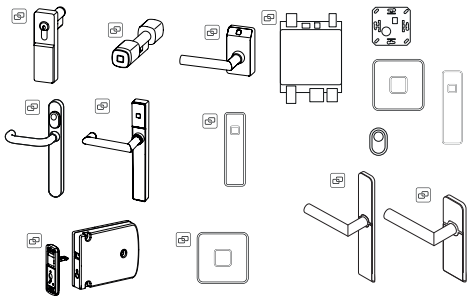
La gestión de personas y medios es una parte importante del plan de seguridad. El software KEM permite ambas tareas de gestión.

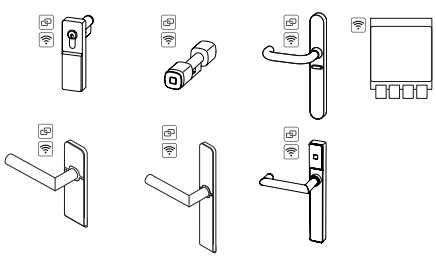
- Programación de los componentes de evolo MIFARE y LEGIC advant, así como de los componentes de Kaba elolegic y Kaba elostar
- Gestión de teléfonos inteligentes (medios) y autorizaciones (componentes) para Mobile Access.
- Gestión de listas de personas
- Auditoría de las emisiones, retiradas y pérdidas de medios
- Auditoría de los cambios en el sistema de cierre
- Asignación de autorizaciones limitadas en el tiempo
- Asignación de autorizaciones permanentes
- Lectura de resultados de componentes (Traceback [▶ 6.12])

2.2 Componentes de un sistema de cierre

Ejemplos de componentes de hardware y cadenas de herramientas:







2.3 Planes de autorizaciones

El software KEM permite los tipos de autorizaciones Lista blanca, CardLink y modo Mixto.

Mobile Access solo es compatible con la Lista blanca.

2.3.1 Resumen de tipos de autorizaciones y modos de proyecto

Modo de proyecto
Si se usa un modo de proyecto, la configuración correspondiente se aplica a todos los componentes del proyecto.

Tipo de autorización			
Capítulo **Lista blanca** [▶ 2.3.2]			
	UID organizativo	Función UID, datos de Traceback como UID	
	Safe UID	UID cifrado, Traceback	
	Card ID	CID cifrado	
Capítulo [▶ 2.3.3] **CardLink**			
	UID organizativo	Datos de Traceback como UID	
	Datos de Traceback como CID		
	Card ID		
Capítulo [▶ 2.3.4] **Modo mixto** En función del tipo de autorización programada en el medio de usuario, en el componente se aplicará la Lista blanca en primer lugar. Si el medio no se encuentra en la Lista blanca, se aplicará CardLink. Si en la Lista blanca se rechaza el medio, se utilizará CardLink. Si aquí tampoco se encuentra una autorización válida, el medio será finalmente rechazado.			
	UID organizativo	Función UID, datos de Traceback como UID	
	Safe UID	UID cifrado, Traceback	
	Card ID	CID cifrado	
CardLink y Lista blanca En función de la configuración de los componentes, se aplicará la autorización CardLink o Lista blanca.			
	UID organizativo	Lista blanca	Función UID, datos de Traceback como UID
		CardLink	Traceback como UID
	Safe UID	Lista blanca	UID cifrado
	Card ID	Lista blanca	CID cifrado
		CardLink	Datos de Traceback como CID

2.3.2 Autorización Lista blanca

- Con las autorizaciones Lista blanca, los medios con autorización de acceso se registrarán en la memoria de los componentes.
- Los medios no registrados en la memoria de los componentes no obtendrán autorización de acceso.
- La memoria de un componente puede registrar hasta 4000 medios (en el caso de Touch-Go E310, hasta 2000 medios).

Los cambios de autorizaciones en los componentes requieren el medio master autorizado para ello.

2.3.3 Autorización CardLink

Con este concepto, las autorizaciones de acceso se escriben en los medios de usuario. A continuación, se aplican a los componentes. Las autorizaciones se gestionan a través de los medios de usuario. Puesto que con esta planificación no es necesario programar los componentes manualmente, los trabajos de gestión en los componentes desaparecen. Basta

con una sola inicialización de los componentes para CardLink. Este tipo de autorización también permite validar (activar durante un período determinado) los medios de usuario para conceder autorizaciones de acceso a los componentes individuales.

Algunas ventajas:

- Es posible escribir una autorización CardLink directamente en el medio de usuario.
- Se puede asignar una selección específica de puertas o grupos de puertas al medio de usuario de un visitante.
- En caso de haber medios de usuario adicionales, no es necesario hacer más ajustes en los componentes.

La validación se encarga de que, en caso de pérdida, los medios de usuario solo sean válidos hasta que caduque el período de validación.

Área de administración
La área de administración es la zona de actuación en la cual tiene efecto un gestor de acceso, es decir, una serie de puntos de acceso (p. ej., puertas) y los medios correspondientes.
La autorización de un medio solo se analiza si los registros de las zonas gestionadas del medio y el punto de acceso coinciden. Si hay discrepancias, el medio se rechaza como no autorizado.

Límites de CardLink (V1.1):

Parámetros	Valor/zona (cantidad)
Puertas (por área de administración)	65535 (números de puerta 512 - 65024)
Grupos de puertas (por área de administración)	511 (números de grupos de puertas 1 - 511)
Zonas gestionadas	256
Medios en un sistema	ilimitado
Derechos de grupos de puertas en un medio	511 (en función del espacio de memoria del medio)
Derechos individuales en un medio	Máximo de 255 (en función del espacio de memoria del medio)
Reservas en un medio	Máximo de 100 (en función del espacio de memoria del medio)
Duración de la validación	8 (1x siempre, 1x 24h, 1x hasta las ... h, 4x n horas)

2.3.4 Modo Mixto

El modo Mixto inalámbrico todavía no es compatible con la gateway inalámbrica.

Un componente configurado en modo Mixto analiza la información de acceso de un medio presentado para Lista blanca y CardLink.
Un medio de usuario tiene permiso en

- Lista blanca
- CardLink
- Lista blanca y CardLink

Orden del análisis:

1 Lista blanca

2 CardLink

Análisis de la Lista blanca		
	El medio consta en la Lista blanca:	
	El medio está autorizado.	El componente se abre. El análisis finaliza. CardLink ya no se analiza.
	El medio no está autorizado o no está en la Lista blanca.	Análisis de CardLink.
Análisis de CardLink		
En el medio hay almacenada una autorización CardLink:		
	El medio está en la Lista de bloqueo.	Los medios bloqueados en CardLink se introducen en la Lista de bloqueo. Véase también el capítulo. El medio queda rechazado. El análisis finaliza.
	El medio está autorizado.	El componente se abre. El análisis finaliza.
	El medio no está autorizado (p. ej., ha excedido el tiempo establecido)	El medio queda rechazado. El análisis finaliza.
	En el medio no hay ninguna autorización CardLink almacenada (p. ej., la autorización para el componente no existe).	

Los componentes MRD con una versión de firmware 42.xx o superior son compatibles con este modo.

2.3.5 Resumen de las tecnologías y los tipos de autorización

	Tipos de autorización					
Tecnologí-as	**UID Lista blanca**	**CID Lista blanca**	**CardLink 1.0**	**CardLink 1.1**	**Medios TRB***	**Safe UID**
Medios						
MIFARE classic	✓	✓	✗	✓	✗	✓
MIFARE DESFire	✓	✓	✗	✓	✓	✓
LEGIC advant 14443	✓	✓	✗	✓	✓	✓ [1]
LEGIC advant 15693	✓	✓	✗	✓	✗	✓ [1]
Componentes						
MultiRFID Dispositivo (MRD)[2]	✓	✓	✓	✓	✓	✓
elolegic (LEGIC prime)	✓	-	✓	✗	✗	✓ [1]
elostar	✓	✗	✗	✗	✗	-

Leyenda:

✓ es posible

✗ no es posible

* Traceback de medios

[1] LEGIC (Safe) UID

[2] Tipos de autorización en función de la tecnología escogida

2.3.6 Mobile Access

Los requisitos previos, la instalación y la configuración de medios y componentes para Mobile Access se describen en el capítulo especial Mobile Access. En la descripción se dan por supuestos conocimientos sobre el funcionamiento de KEM.

3 Instalación y configuración

3.1 Requisitos del sistema

Antes de poder instalar el software KEM, el sistema operativo de Windows debe estar actualizado a la versión más reciente.

Los componentes adicionales son parte de la instalación. En caso de que todavía no formen parte del sistema, se instalarán.

A partir de la versión 7.2 de KEM, los sistemas de 32 bits ya no son compatibles.

La siguiente tabla presenta los requisitos mínimos para la instalación.

Sistema operativo (64 bits)	Windows 11 Windows 10 Windows Server 2025 Windows Server 2022 Windows Server 2019 Windows Server 2016
Procesador	Arquitectura x64 **AVISO Los procesadores basados en ARM no son compatibles.**
Memoria de trabajo	1 GB (recomendación: 2 GB RAM)
Memoria en el disco duro	6 GB (incluidos todos los componentes adicionales de Microsoft)
Interfaces	2x USB
Resolución de la pantalla	1024 x 768 píxeles (recomendación: 1920 x 1200)
Componentes adicionales	.Net Framework 4.8 Microsoft SQL Server 2019 Express Herramienta de servicio ACS de dormakaba
Compatibilidad	SQL Server 2025 SQL Server 2022 SQL Server 2019 SQL Server 2017

3.2 Instalación del software

Solo es posible instalar software en un ordenador si se dispone de derechos de administrador.

Cualquier cortafuegos que tenga instalado debe estar desactivado durante toda la instalación.

Puede escoger una de estas variantes de instalación:

- Instalación independiente. Consulte
  El software dormakaba evolo Manager y el SQL Server utilizado se encuentran en el mismo ordenador.
- Instalación de cliente/servidor. Consulte
  El software dormakaba evolo Manager se instala en uno o más ordenadores cliente y el SQL Server utilizado por todos ellos se encuentra en un ordenador aparte denominado "servidor".

3.2.1 Instalación en versión independiente

El software se instala mediante un asistente de instalación (InstallShield).
Instale el software y SQL Server.

- Tras la descarga del paquete del software, inicie el asistente de instalación.
- El asistente de instalación ejecuta la instalación.
- Lea y acepte el contrato de licencia del software. Si no acepta el contrato de licencia, el software no se instalará.
- El directorio de instalación se puede cambiar pulsando el botón "Modificar". Recomendamos mantener el formato estándar en lo que respecta a la carpeta de destino, p. ej.:

  `C:\Archivos de programa\Kaba\dormakaba evolo Manager V7.X\ <estructura del directorio de instalación en un sistema de 64 bits>.`
- Durante la instalación, ponga atención a los mensajes e indicaciones que aparezcan en la pantalla.
- Cuando se le solicite, siga adelante o reinicie el equipo.

3.2.2 Instalación en versión cliente/servidor

El sistema cliente/servidor únicamente funcionará dentro del mismo dominio. De no ser así, entre ambos dominios debe colocarse una relación de confianza.

Siga los pasos de instalación en orden según se especifica en los siguientes capítulos.

3.2.2.1 Instalación del servidor

Instale el software dormakaba evolo Manager (KEM) y SQL Server en el servidor. Durante la instalación, el SQL Server recibirá los datos de inicio de sesión correspondientes. El software KEM no es necesario para el funcionamiento y se puede utilizar para realizar pruebas.

1. Descomprima la descarga en cualquier directorio del disco duro e inicie el asistente de instalación.
2. El asistente de instalación ejecuta la instalación.
3. El asistente de instalación comprueba qué componentes de software se deben instalar y los muestra en una ventana.
4. Paso del contrato de licencia del software: lea y acepte el contrato de licencia del software. Si no acepta el contrato de licencia, el software no se podrá instalar.
5. En el paso de la carpeta de destino: el directorio de instalación se puede cambiar de forma individual pulsando el botón "Modificar". Recomendamos mantener el formato estándar en lo que respecta a la carpeta de destino, p. ej.: `C:\Archivos de programa\Kaba\dormakaba evolo Manager V7.X\ <estructura del directorio de instalación en un sistema de 64 bits>`
6. Configurar unidad de red/carpeta: en esta unidad de red, el servicio del cliente usuario y el de SQL Server deben tener derechos de acceso. Consulte el capítulo [▶ 3.2.2.5]

3.2.2.2 Instalación del cliente

El software se instala mediante un asistente de instalación (InstallShield).

1. Descomprima la descarga en cualquier directorio del disco duro e inicie el asistente de instalación.
2. El asistente de instalación ejecuta la instalación.

Paso 3: El SQL Server no debe instalarse en el cliente. Microsoft SQL Server aparecerá con el estado "Omitido" en el asistente.

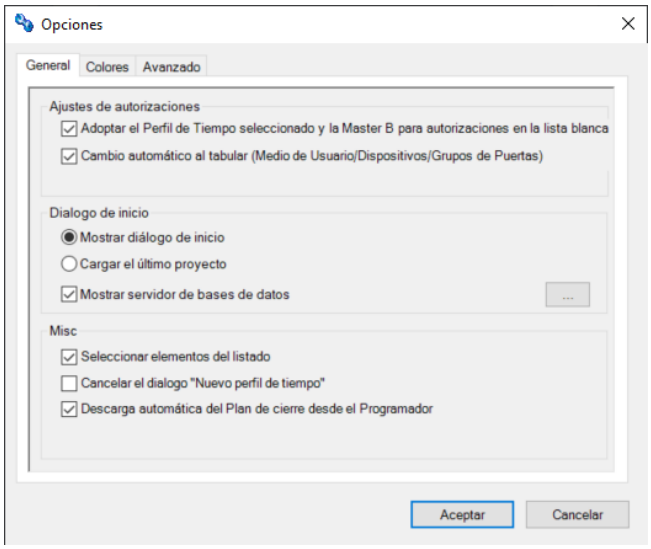
3. El asistente de instalación comprueba qué componentes de software se deben instalar y los muestra en una ventana.
4. Paso del contrato de licencia del software: lea y acepte el contrato de licencia del software. Si no acepta el contrato de licencia, el software no se podrá instalar.

5. En el paso de la carpeta de destino: el directorio de instalación se puede cambiar de forma individual pulsando el botón "Modificar". Recomendamos mantener el formato estándar en lo que respecta a la carpeta de destino, p. ej.: `C:\Archivos de programa\Kaba\dormakaba evolo Manager V7.X\ (estructura del directorio de instalación en un sistema de 64 bits)`
6. Configurar unidad de red/carpeta: en esta unidad de red, el servicio del cliente usuario y el de SQL Server deben tener derechos de acceso. Consulte [▸ 3.2.2.5]

3.2.2.3 Activar la visualización del servidor de base de datos

1. Inicie el servidor en el que se haya instalado la base de datos (SQL Server).
2. Inicie el software dormakaba evolo Manager en el cliente.
3. Cierre el primer cuadro de diálogo "dormakaba evolo Manager" o seleccione "Cancelar".
4. En la barra de funciones "Inicio", seleccione el menú "Opciones".
5. En la ventana de opciones, vaya a la pestaña "General".
6. En la categoría "Diálogo de inicio", active la casilla "Mostrar servidores de bases de datos".
7. Si es necesario, haga clic en el botón "..." y seleccione un servidor de base de datos de la lista de favoritos o añada un nuevo servidor de base de datos.
8. Pulse "OK".

⇨ Al abrir o crear un proyecto es posible seleccionar servidores de bases de datos disponibles que estén en los favoritos. Para editar la selección, consulte el capítulo "Editar servidores de bases de datos [▸ 3.2.3]".



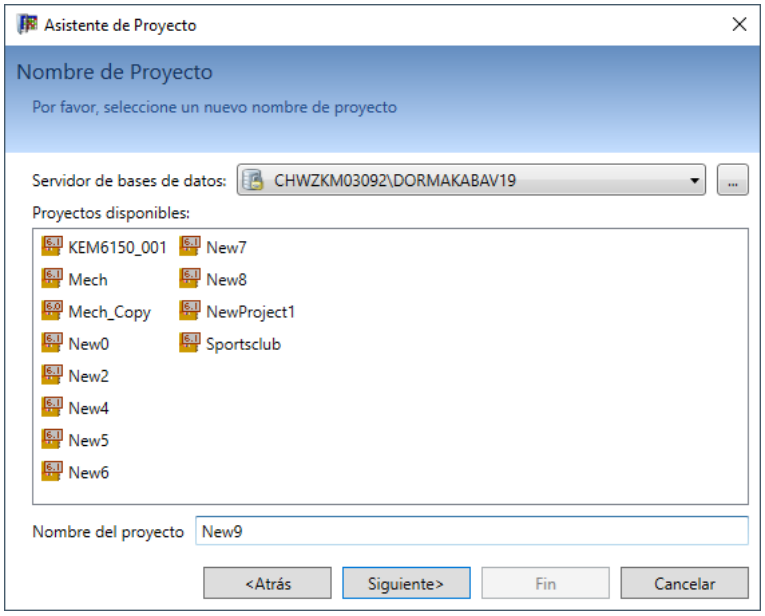
3.2.2.4 Abrir un proyecto en el servidor de base de datos o crear uno nuevo

Si se usa un servidor de base de datos central, se debe seleccionar en cada cliente.

Un mismo proyecto KEM no puede ser abierto por varios clientes a la vez.

Procedimiento para crear un nuevo proyecto

1. Inicie el software KEM en el cliente.
2. Para crear un nuevo proyecto, seleccione "Nuevo proyecto [▸ 6.1.1]" (Ctrl + N).
3. Siga el asistente.
4. Seleccione el servidor de base de datos. Si el servidor no aparece en la lista, cambie a Editar servidores de bases de datos [▸ 3.2.3].
5. Ponga nombre al proyecto y pulse "Siguiente".
6. Siga el asistente.

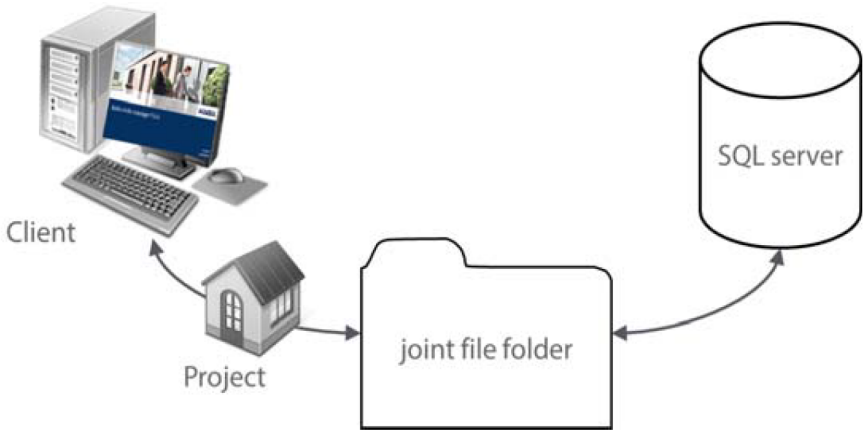


Procedimiento para abrir un proyecto

1. Inicie el software KEM en el cliente.
2. Si se trata de un proyecto existente, seleccione el servidor de base de datos de la lista. Si el servidor no aparece en la lista, cambie a Editar servidores de bases de datos [▸ 3.2.3].
3. Seleccione el nombre del proyecto (Proyectos disponibles).
4. Pulse "Abrir".

3.2.2.5 Carpeta común para importar y exportar proyectos del cliente/servidor

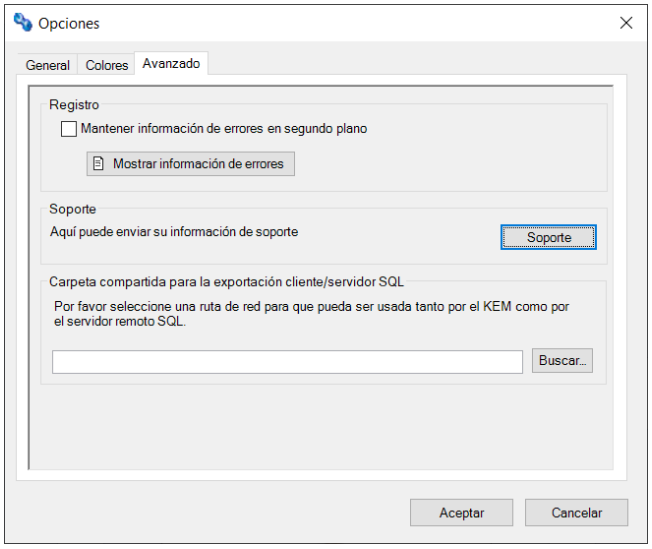
El SQL Server y el cliente necesitan acceso completo a una carpeta común.
El administrador del sistema es el encargado de facilitar dicha carpeta.



Para configurar la carpeta común en KEM es necesario disponer de derechos de administrador.
Escoja una de las 2 opciones:

- Inicie sesión en Windows como administrador.
- Ejecute KEM como administrador.

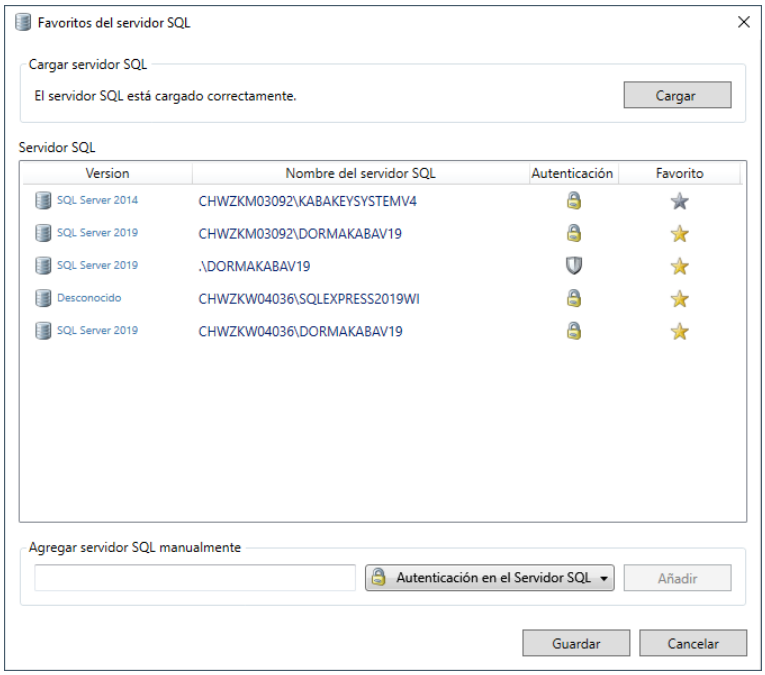
1. En la barra de funciones "Inicio", seleccione el menú "Opciones".
2. En la ventana de opciones, vaya a la pestaña "Avanzado".
3. En la categoría "Carpeta común de exportación del cliente/SQL Server", introduzca la ruta de red de la carpeta común (p. ej., `\\Server\Share`).
4. Pulse "OK".



3.2.3 Editar servidores de bases de datos

En "Opciones", "Mostrar servidores de bases de datos" debe estar seleccionado para poder utilizar esta opción. Consulte el capítulo [▸ 3.2.2.3]

Añadir un servidor de base de datos

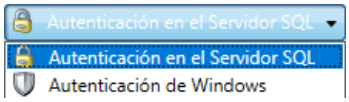


1. Seleccione "Abrir proyecto".
2. Pulse "...".
   ⇨ Aparecerá la ventana de selección de los favoritos de SQL Server.
3. Pulse "Cargar".
   ⇨ Aparecerán todos los servidores de bases de datos que se encuentren.
4. Marque o desmarque de favoritos los servidores que desee.
   ⇨ Los elementos seleccionados aparecen con la estrella pintada de color amarillo.
5. Pulse "Guardar".
   ⇨ Los servidores marcados se pueden seleccionar en la lista dentro del cuadro de diálogo.

Añadir un servidor de base de datos manualmente
Si el servidor de base de datos deseado no figura en la lista, añádalo manualmente.

Procedimiento:

1. Introduzca "Nombre del ordenador\Nombre de instancia de SQL Server" en la línea "Añadir SQL Server manualmente".
2. Seleccione el método de autenticación.



3. Pulse "Añadir".
4. Pulse "Guardar".

⇨ El servidor quedará registrado en la lista y marcado como favorito.

⇨ El servidor se podrá seleccionar en la lista dentro del cuadro de diálogo.

3.2.4 SQL Server con autenticación de Windows

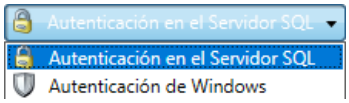
Por defecto, KEM usa la autenticación de SQL Server entre KEM y SQL Server. Los usuarios con necesidades de seguridad más específicas pueden usar la autenticación de Windows.

En el menú "Opciones > General", la opción "Mostrar servidores de bases de datos" debe estar seleccionada.

Esta variante de conexión de SQL Server ÚNICAMENTE es para personas con un conocimiento avanzado de la configuración y administración de un SQL Server.

Con esta opción, la gestión de usuarios de KEM puede quedar limitada por los derechos de SQL Server.

KEM usa 2 métodos de autenticación:



- Autenticación de SQL Server (estándar)
- Autenticación de Windows

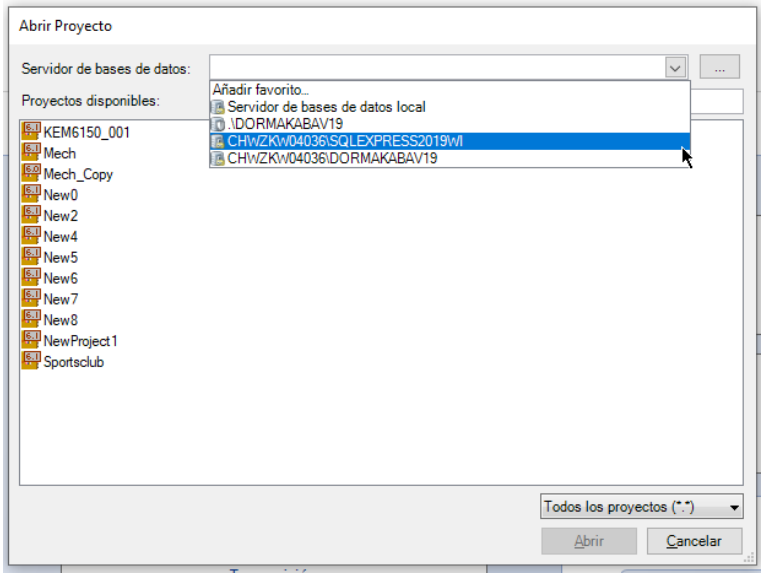
Es posible decidir el método de forma individual para cada instancia de SQL Server.

3.2.4.1 Funcionamiento con autenticación de Windows

3.2.4.1.1 Configurar la autenticación en KEM

Al abrir un proyecto o crear uno nuevo, seleccione el servidor de base de datos con autenticación de Windows que se encuentre en la lista de favoritos. Luego aparecerán los proyectos presentes en el servidor de base de datos seleccionado.

El usuario debe disponer del derecho a ver los elementos de la base de datos en el SQL Server.



Si el servidor deseado no figura en la lista, pulse el punto 3 para editar [▸ 3.2.3] la lista de servidores de bases de datos.

3.2.4.2 Configurar SQL Server

La configuración del SQL Server no se puede llevar a cabo con KEM. Se recomienda utilizar el software existente para este fin. P. ej., SQL Server Management Studio de Microsoft.
El software puede descargarse de Microsoft.

- No hay soporte de dormakaba para este software. En caso de necesitar ayuda, contacte con Microsoft.

El usuario tiene la sesión iniciada en Windows y ejecuta KEM (cuenta de dominio). Para facilitar la configuración del servidor y de la base de datos, registre la cuenta de dominio como inicio de sesión del SQL Server y asigne los siguientes roles:

1. En el SQL Server, cree un inicio de sesión para el usuario de Windows con derechos dbcreator.
2. Establezca el rol de base de datos "db_owner" en todas las bases de datos que necesite el usuario.
3. Conecte dormakaba evolo Manager mediante autenticación de Windows con el SQL Server.

Si solo va a utilizar la autenticación de Windows, cambie el SQL Server a "Windows Authentication mode".

3.3 Configurar el programa

Configuración única del programa tras la instalación del software.

El primer inicio del software después de la instalación se debe realizar como administrador.

- El asistente de configuración se inicia.
- El asistente de configuración le guía por la configuración.

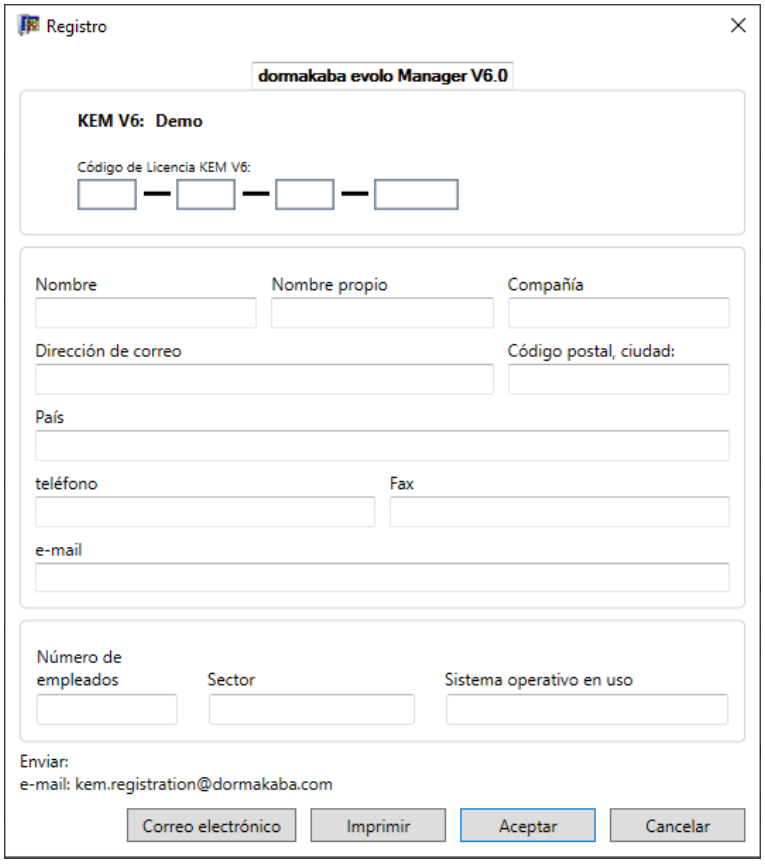
Paso **Más ajustes básicos**:
El operador KEM ofrece una interfaz de usuario muy simplificada del software KEM. Sin embargo, esto implica una limitación de ciertas funciones. [▸ 13.1]

Paso **Modo de licencia**:
El ID de producto (número de licencia) necesario para este paso está en la tarjeta de licencia.

3.3.1 Registrar la licencia del software

Inicie la sesión en el sistema como administrador o ejecute el software como administrador.

Para registrar el ID de producto (número de licencia), rellene el formulario y envíelo a la oficina de registro indicada por una de estas vías.



- Si pulsa el botón **Correo electrónico**, enviará el formulario rellenado a la oficina de registro por correo electrónico.

3.3.2 Registrar y actualizar el número de licencia

Inicie la sesión en el sistema como administrador o ejecute el software como administrador.

Registro de la licencia del software. [▸ 3.3.1]

1. Pulse el botón "Registrar número de licencia" de la barra de funciones "Inicio".
2. Introduzca el número de licencia (de actualización).
   ⇨ Los campos inferiores se abren subrayados en rojo.
3. Introduzca el número de licencia registrado.
   ⇨ Ambos números de licencia están insertados.

4. Cierre la ventana con **OK**.

3.4 Autorizaciones de acceso

El software KEM gestiona datos sensibles y relacionados con la seguridad. La limitación de autorizaciones de la Administración de usuarios [▸ 5.3.1] permite dar mayor seguridad a los datos.

3.5 Instalar el servicio evolo

Solo es posible instalar software en un ordenador si se dispone de derechos de administrador.
Cualquier cortafuegos que tenga instalado debe estar desactivado durante toda la instalación.

El servicio evolo solo es necesario si se va a utilizar un terminal o un gestor de acceso en el sistema.

Instale el servicio evolo en el ordenador en el que está instalado el servidor de base de datos KEM.

Para que el terminal funcione en línea, el servidor debe estar siempre disponible.

- Funcionamiento del servidor 24/7.
  ⇨ Si el servidor no está disponible, los medios solo se validan.
  ⇨ Si el servidor no está disponible, el Traceback de medios no se lee.

Requisitos previos

- El usuario ha iniciado sesión como administrador o tiene derechos de administrador.

Procedimiento

1. Inicie el programa de instalación.
2. Siga las instrucciones del instalador.

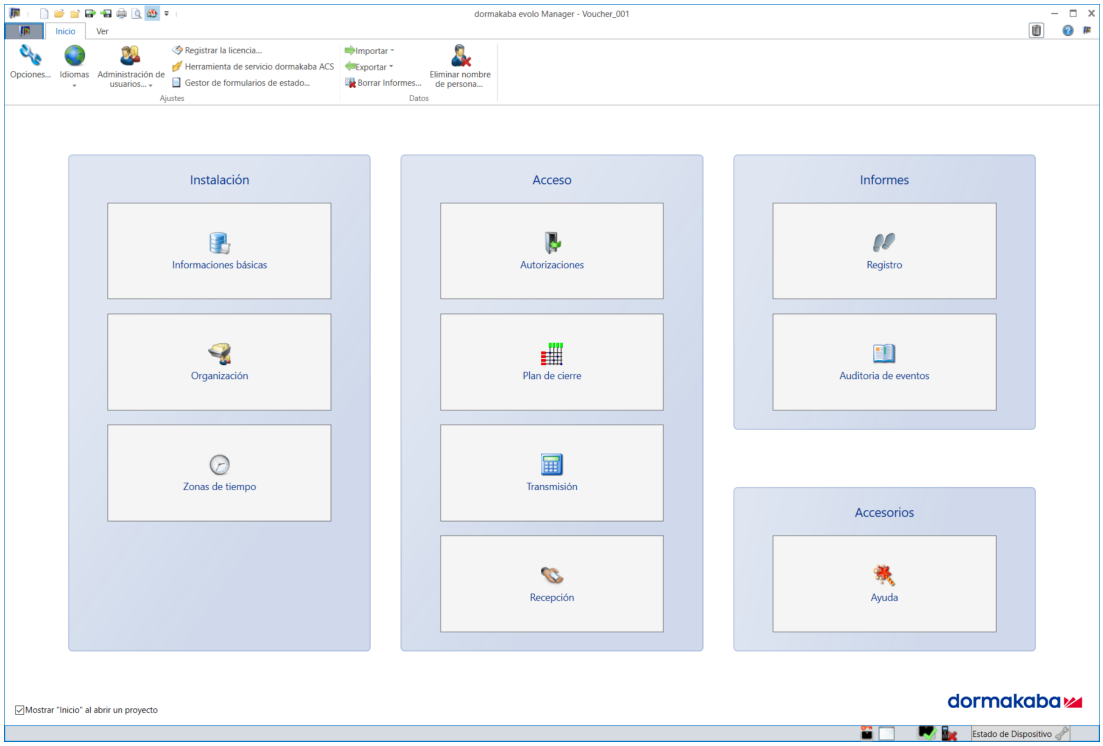
⇨ La configuración del servicio se realiza automáticamente mediante KEM.

⇨ Una vez finalizada la instalación, el servicio evolo se inicia automáticamente.

4 Resumen

4.1 Pantalla de inicio (Home)

La pantalla de inicio ofrece todas las funciones en el orden requerido. La pantalla de inicio ayuda a los nuevos usuarios a orientarse en el sistema.



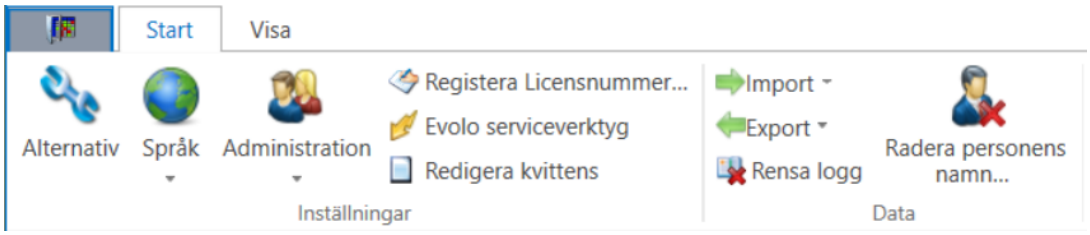
Los elementos de la pantalla proporcionan ayuda para las siguientes tareas:

- Configurar los elementos básicos, la organización y los perfiles temporales
- Definir el acceso en función de las autorizaciones, el plan de cierre o la recepción
- Transferir datos de acceso al programador, a la gateway inalámbrica y luego a cada uno de los componentes
- Mostrar informes de los registros o de los datos de Traceback
- En trabajos complejos, ayuda mediante los asistentes (Wizards)

4.2 Barras de funciones

4.2.1 Inicio

En la barra de funciones "Inicio" están ordenadas por temas todas las funciones de ajuste y de datos del software.



Ajustes	
Opciones	Consulte [▶ 5.1]
Idiomas	Consulte [▶ 5.2]
Administración de usuarios	Consulte [▶ 5.3.1]
Registrar número de licencia	Consulte [▶ 3.3.2]

Herramienta de servicio ACS	Consulte
Formularios de gestión de medios	Consulte [▶ 5.4]
Datos	
Importar	Consulte [▶ 12.1]
Exportar	Consulte [▶ 12.1]
Borrar informes	Consulte [▶ 12.4]
Borrar nombre de persona	Consulte

4.2.2 Ver

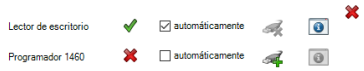
En la barra de funciones "Ver" están ordenadas por temas todas las funciones necesarias para el trabajo cotidiano (p. ej., la pantalla de inicio).

Ver		
Inicio	Pantalla de inicio	Consulte [▶ 4.1]
Instalación		
Informaciones básicas	Medios Actuadores Master Grupos de puertas Terminales Gateways	Consulte Consulte Consulte Consulte [▶ 6.6] Consulte Consulte
Organización	Personas	Consulte [▶ 6.7]
Perfiles temporales	Perfiles temporales Validación Vacaciones/días especiales	Consulte Consulte [▶ 6.4.2] Consulte [▶ 6.4.1]
Acceso		
Autorizaciones	Autorización Lista blanca Autorización CardLink Asignación grupal de actuadores Configurar CardLink	Consulte [▶ 6.9.1] Consulte [▶ 6.9.2]
Plan de cierre	Resumen De forma electrónica CardLink/Lista blanca De forma mecánica Derechos de grupos (CardLink) Asignación de grupos de puertas	Consulte [▶ 6.8]
Transmisión	Transferencia (a programador, gateways y actuadores)	Consulte [▶ 6.10]
Recepción	Recepción (CardLink y Lista blanca)	Consulte
Informes		
Traceback	Actuador Medio	Consulte [▶ 6.12]
Auditoría de eventos	Lista de registros Lista de auditorías	Consulte [▶ 6.13.1] Consulte
Accesorios		
Asistentes (Wizards)	Trabajos con Wizards (Asistentes)	Consulte

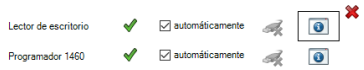
4.3 Estados de los dispositivos, información y propiedades

La línea de estado muestra todos los dispositivos vinculados como activos o inactivos. La información sobre el estado de los lectores de sobremesa y de las configuraciones de medios también aparece representada.

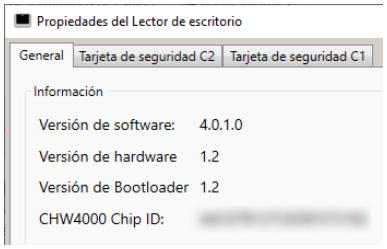
1. Pulse el botón "Estados de los dispositivos" para abrir la ventana de información.



2. En esta ventana podrá conectar o desconectar manualmente los dispositivos vinculados si la casilla "automático" está desmarcada.
   Para realizar la conexión o desconexión manual, pulse el símbolo del dispositivo en cuestión.



3. Adicionalmente, haciendo clic en el símbolo de información puede consultar la información sobre el lector de sobremesa, así como ver y ajustar las propiedades del programador (F4\botón "Mostrar propiedades del programador..."). El siguiente ejemplo le muestra el caso de un lector de sobremesa LEGIC.



Encontrará más información sobre las tarjetas de seguridad C1 y C2 en el capítulo o en la descripción del sistema de evolo.

4.4 Asistentes (Wizards)

Este capítulo contiene información sobre todos los asistentes disponibles en el software KEM. En la selección de programa solo podrá escoger los asistentes que se puedan utilizar con la tecnología seleccionada.

4.4.1 Pérdida de medios

Este asistente le permite aplicar las medidas necesarias para preservar la seguridad del sistema.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.2 Tarjeta de sustitución

Este asistente le ayudará a crear una tarjeta de sustitución y a preservar la seguridad del sistema.

	MIFARE	LEGIC advantt	elolegic	elostar
	✓	✓	✗	✗

4.4.3 Lectura de registros de la tarjeta de servicio

Este asistente lee los datos de Traceback y de estado de los componentes desde el medio de servicio en el proyecto.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.4 Crear nuevos grupos de puertas

Este asistente proporciona ayuda para crear nuevos grupos de puertas

	MIFARE	LEGIC advant	elolegic*	elostar
	✓	✓	✓	✗

*Solo compatible con U-Line

4.4.5 Crear Master

El asistente le facilita la creación de un medio Master programador.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✗	✗	✗

4.4.6 Actualizar Master temporal

El asistente le facilita la actualización de un Master T. El asistente no se activará hasta que se haya leído la tarjeta de seguridad.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.7 Crear nuevo medio de servicio

El asistente le facilita la creación de un medio de servicio. El medio de servicio será necesario para bloquear medios de usuario concretos en componentes específicos.

	MIFARE	LEGIC advant	elolegic*	elostar
	✓	✓	✓	✗

*Una tarjeta Prime puede convertirse en un medio de servicio. Se aplica la siguiente restricción: No se puede leer el estado.

4.4.8 Copiar medios

El asistente le ayuda a copiar las autorizaciones de un medio a otros medios.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✓	✓

4.4.9 Copiar componentes

El asistente le ayuda a copiar las autorizaciones de un componente a otros componentes.

	MIFARE	LEGIC advant	elologic	elostar
	✓	✓	✓	✓

4.4.10 Cerradura de armario

El asistente le ayuda a crear o leer un medio de cerradura de armario.

	MIFARE	LEGIC advant	elologic	elostar
	✗	✗	✓	✗

4.4.11 Cerradura de armario 21 10

El asistente le ayuda a crear o leer medios para la cerradura de armario 21 10. Las compatibilidades son las siguientes:

	MIFARE	LEGIC advant	elologic	elostar
	✓	✓	✗	✗

4.4.12 Actualizar la configuración de la llave MIFARE DESFire

El asistente ayuda a ajustar la configuración de la llave en un medio de usuario MIFARE DESFire.
Para la descripción y el procedimiento, consulte el capítulo [▶ 6.3.4].

	MIFARE	LEGIC advant	elologic	elostar
	✓	✗	✗	✗

4.4.13 Importar vale de llave digital de Mobile Access

El asistente ayuda a importar llaves digitales para aplicaciones de Mobile Access que estén contenidas en un documento PDF.

Para la descripción y el procedimiento, consulte el capítulo.

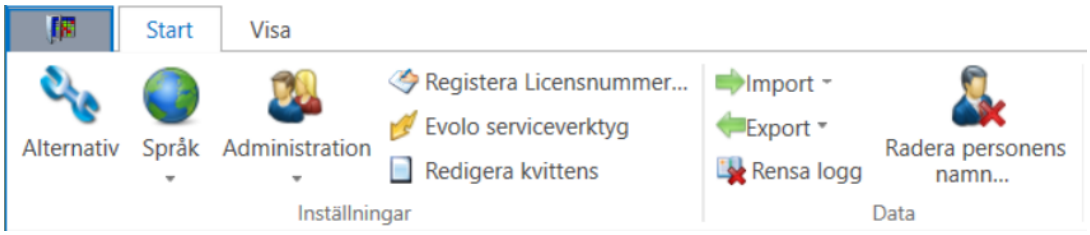
	MIFARE	LEGIC advant	elologic	elostar
	✓	✓	✗	✗

5 Ajustes

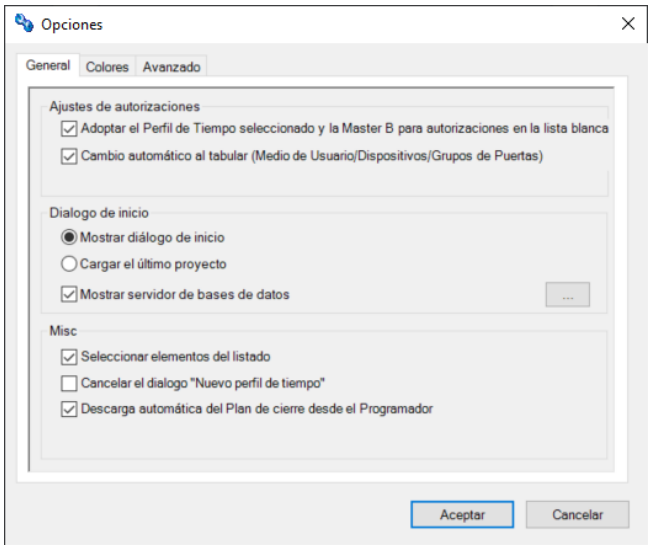
El software KEM tiene varios ajustes básicos disponibles.

5.1 Opciones

- En la barra de funciones "Inicio", seleccione "Opciones (Ctrl+shift+O).



Generalidades

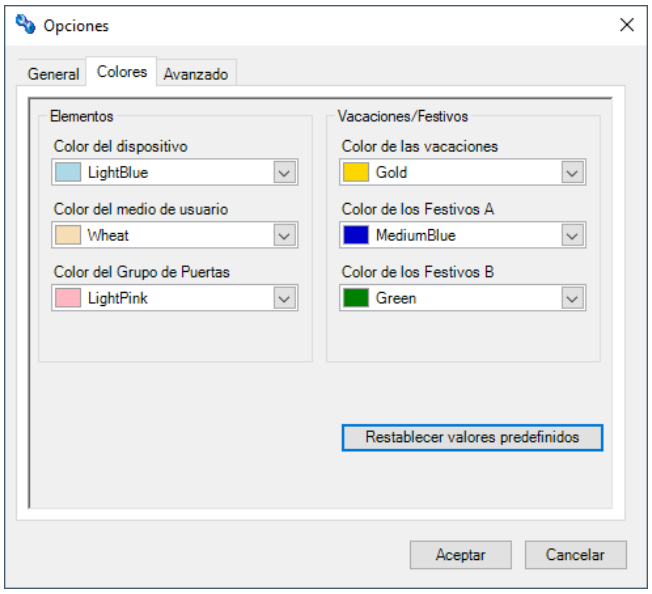


Generalidades	
Ajustes de la autorización	
Adoptar autorizaciones de perfil temporal y de selección del Master B para la Lista blanca	Los ajustes marcados se adoptan automáticamente en la ventana de autorización.
Cambio de pestaña automático (medios de usuario/actuadores/ grupos de puertas)	Una ayuda de programación para el usuario experimentado.
Diálogo de inicio	
Mostrar diálogo de inicio	Esta opción permite activar o desactivar el diálogo de inicio.
Cargar el último proyecto abierto	Se abre el último proyecto editado (plan de cierre). Si solo existe un proyecto, se abrirá este.
Mostrar servidor de base de datos	En el cuadro de diálogo "Abrir" aparecerá el servidor de base de datos respectivo. Haga clic en el botón "..." para seleccionar o añadir un servidor de base de datos de la lista.
Misceláneo	
Seleccionar elementos del listado	En las autorizaciones se marcarán las líneas con los elementos disponibles para seleccionar.
Cancelar el diálogo "Nuevo perfil de tiempo"	Esto oculta el cuadro de diálogo para seleccionar los perfiles temporales V2 y V3 o V3 y V4.

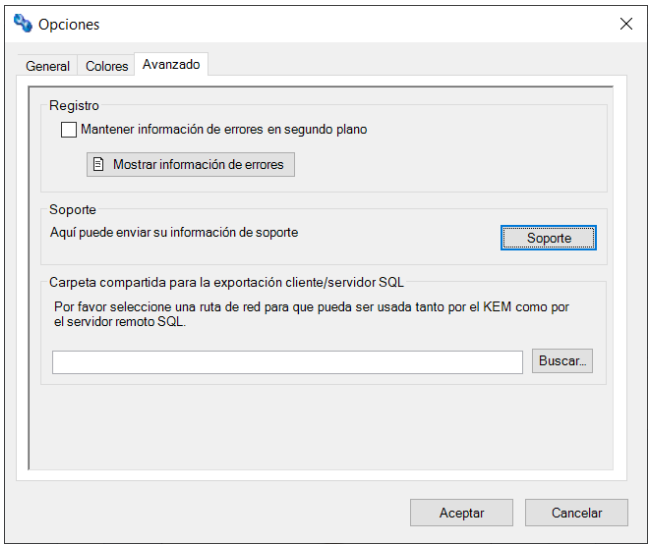
Transferencia automática del plan de cierre al programador.	Con esta opción se puede automatizar la transferencia del plan de cierre desde el programador.
Mensajes si hay datos pendientes de actualización de CardLink	Si hay datos de actualización de CardLink que aún no se han transferido, al cerrar el proyecto aparece un cuadro de diálogo con la opción de transferirlos antes de cerrar. Al hacer clic en "Sí", el usuario accede al menú de transferencia. Esta opción está activada por defecto. El mensaje solo aparece si hay lectores de actualizaciones CardLink (autónomos o inalámbricos) configurados en el proyecto.

Colores

Para mejorar la orientación, se puede ajustar el color de los distintos elementos.



Avanzado



Avanzado	
Registro	
Recoger información de depuración en segundo plano	La información sobre el comportamiento del programa se registra en un archivo. Este archivo ayuda al equipo de asistencia a solucionar los problemas.
Servicio al cliente	
Enviar paquetes al servicio de soporte al cliente	Crea un mensaje de correo electrónico y adjunta el paquete de datos con esta información:

	• Registro • Datos de proyecto • Datos de registro
Carpeta común para exportación del cliente/SQL Server	
Para exportación del cliente/ SQL Server	Introduzca la ruta de la unidad que se pueda usar tanto para KEM como para el SQL Server activo.

5.2 Cambiar el idioma

El software KEM está disponible en varios idiomas.

1. En la barra de funciones "Inicio", seleccione el menú "Idiomas".
2. Seleccione el idioma que desee de la lista.

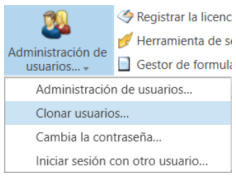
⇨ Podrá seguir trabajando en el idioma configurado de forma inmediata.

5.3 Administración de usuarios

En el espacio Administración de usuarios es posible añadir, editar y borrar usuarios para el proyecto activo. Desde aquí puede conceder varios roles y derechos (derechos de usuario) a los usuarios. La administración de usuarios está inactiva si no hay ningún usuario registrado.

La administración de usuarios se debe registrar individualmente para cada proyecto.
Es posible aplicar un proyecto preconfigurado.
Se requiere el derecho "Gestión de usuarios" en el rol asignado para cambiar la configuración o bien crear o eliminar usuarios.

La funcionalidad del botón "Administración de usuarios" depende de la función del usuario que tenga la sesión iniciada.

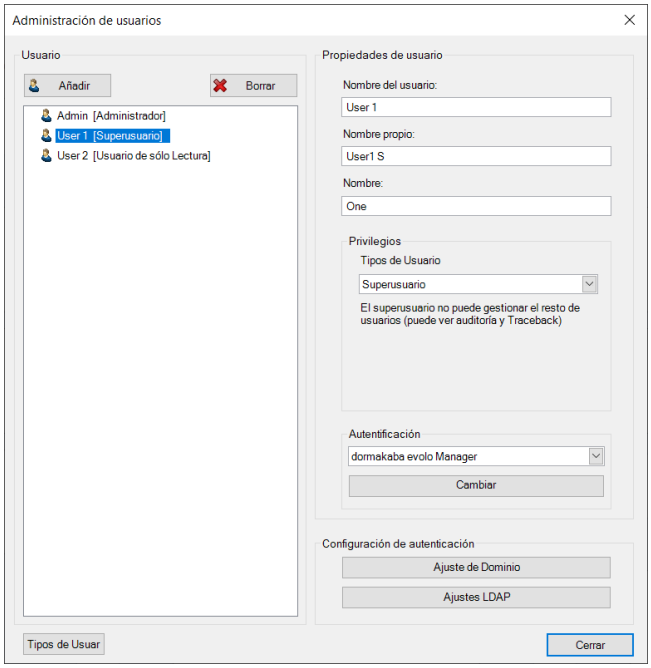


Seleccione la función en el menú de selección.

- Administración de usuarios
  Consulte el capítulo
- Clonar usuarios
  Consulte el capítulo [▸ 5.3.2]
- Cambiar la contraseña
  Consulte el capítulo [▸ 5.3.1.5]
- Iniciar sesión como otro usuario
  Consulte el capítulo [▸ 5.3.1.6]

5.3.1 Editar propiedades de usuario

Solo se puede seleccionar 1 usuario para editar a la vez.



- Añadir usuarios. (consulte el capítulo [▶ 5.3.1.1])
- Borrar usuarios. (consulte el capítulo [▶ 5.3.1.4])
- Editar roles y derechos. (consulte el capítulo [▶ 5.3.1.2])
- Cambiar/restablecer contraseña de usuario. (consulte el capítulo [▶ 5.3.1.5])
- Asignar un método de autenticación al usuario. (consulte el capítulo)
- Configuración de autenticación. (consulte el capítulo)

Procedimiento de inicio de sesión para la autenticación de usuario

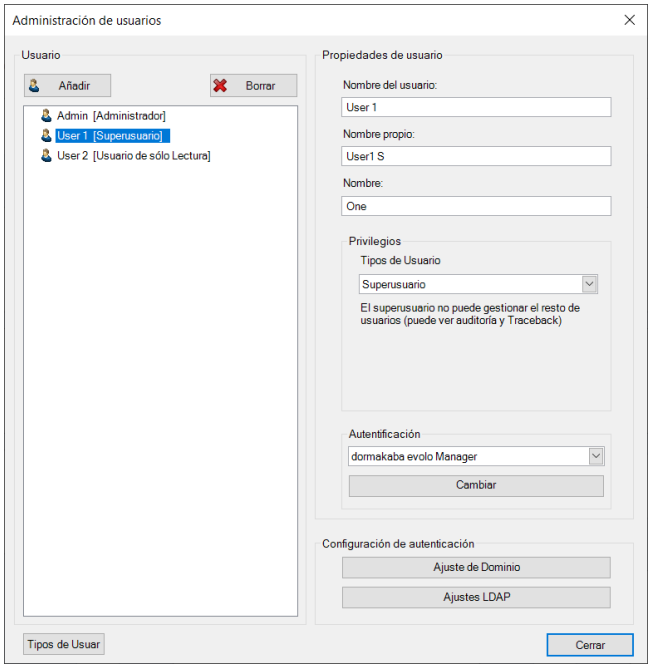
- Usuario de KEM (consulte el capítulo [▶ 5.3.1.3.1])
- Usuario local (Windows) y usuario de dominio (red Windows) (consulte el capítulo [▶ 5.3.1.3.2])
- Usar LDAP (servicio de directorio de red) (consulte el capítulo [▶ 5.3.1.3.3])

5.3.1.1 Añadir usuarios

Si la administración de usuarios no está activada, primero se debe crear un usuario con el rol "Administrador".
Si solo se introduce un usuario, el derecho de usuario "Administrador" no se puede cambiar.

Procedimiento para crear nuevos usuarios:

1. Haga clic en "Nuevo".

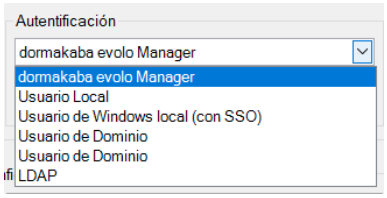


⇨ En el lado izquierdo se añadirá un nuevo usuario.

2. Introduzca las propiedades del usuario en el lado derecho.

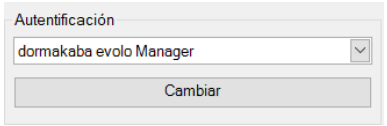
Para utilizar el inicio de sesión de Windows, LDAP o SSO, la información debe coincidir con la información almacenada allí.
La asignación de una nueva contraseña solo es necesaria para el procedimiento de inicio de sesión de "dormakaba evolo Manager".

3. Seleccione el método de autenticación de usuario de la lista.



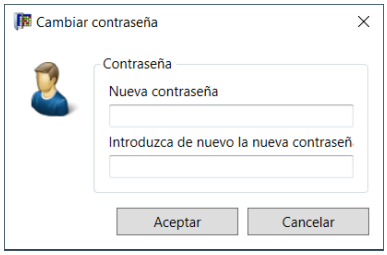
⇨ La información sobre la configuración de autenticación solo debe introducirse una vez por proyecto antes de asignar el procedimiento de autenticación a un usuario. Consulte también en el capítulo.

4. Haga clic en "Cambiar contraseña" para abrir el cuadro de diálogo de contraseña.



⇨ La contraseña solo debe introducirse utilizando el método de autenticación "dormakaba evolo Manager".

5. Introduzca y confirme la contraseña de usuario.

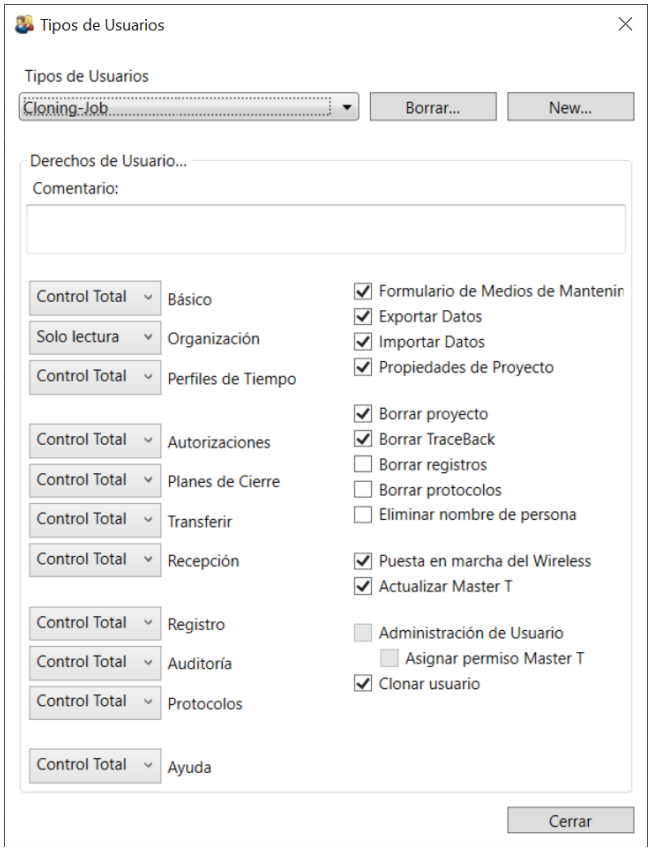


6. Pulse "OK".
7. Haga clic en "Cerrar" para finalizar la administración de usuarios.
   ⇨ La autenticación de usuario con contraseña se activa para el usuario.

⇨ El usuario puede iniciar sesión en este proyecto.

5.3.1.2 Roles y derechos

Introducción
La seguridad del sistema aumenta cuando a los usuarios se les asignan roles que tienen derechos apropiados para las tareas. De esta manera se puede diferenciar entre administración y funcionamiento normal de un sistema y se pueden evitar cambios involuntarios en la configuración. El administrador y el usuario de un sistema pueden ser la misma persona.
Es posible realizar un cambio de rol o usuario a través del cuadro de diálogo "Iniciar sesión como otro usuario".



Derechos de usuario con varios roles
A los usuarios se les pueden asignar varios roles:

En el software KEM no se pueden modificar ni eliminar los roles predeterminados.

Roles predeterminados en KEM:

- Usuarios
- Superusuario
- Administrador
- Solo recepción
- Usuario dormakaba CheckIn
- Usuario ReadOnly

Para crear nuevos roles con derechos individuales, consulte el capítulo [▸ 5.3.1.2.1].

Propiedades de los derechos de los roles
A los roles se les pueden asignar diversos derechos sobre las vistas y para ejecutar funciones. Existen diferentes niveles de visibilidad y acceso que el administrador selecciona al crear un rol. Aquí no se puede cambiar nada de las funciones predefinidas en KEM. Si quiere cambiar la configuración predefinida, deberá crear un nuevo rol y asignarlo al usuario.

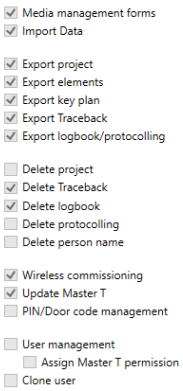
Derechos de usuario sobre las vistas

El usuario no puede ver ni abrir la vista.

El usuario solo tiene derecho de lectura en esta vista.

El usuario puede realizar cambios en esta vista.

Derechos de usuario sobre las funciones



Active la casilla para habilitar una función para este rol.

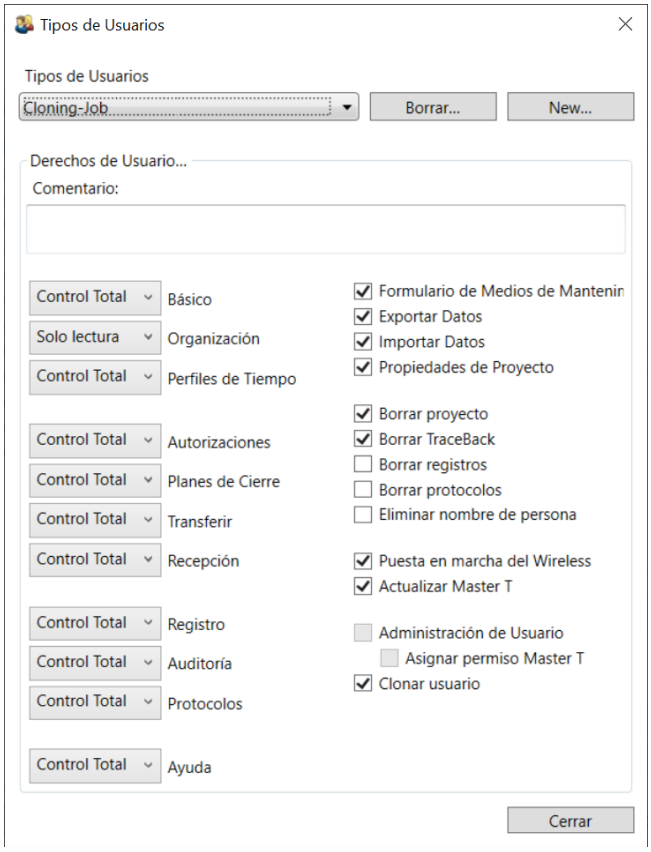
Derecho de usuario para la puesta en marcha inalámbrica

Los derechos de usuario para la puesta en marcha inalámbrica se pueden ajustar en los roles del usuario. Estos derechos solo pueden ajustarlos los usuarios con el derecho **Gestión de usuarios**.

Derechos de usuario para Master T

Los derechos de usuario para Master T se pueden ajustar en los roles del usuario.

- El derecho "Actualizar Master T": Los titulares de este derecho pueden activar un Master T durante un período de tiempo ajustable. Consulte el capítulo [▶ 6.3.2.2].
- El derecho "Asignar Master T": Los titulares de este derecho en su rol pueden asignar o revocar el derecho "Actualizar Master T" a otro usuario.
- Un Master T solo pueden añadirlo los usuarios que en los roles de usuario tengan configurado "Acceso completo" en el apartado "Elementos básicos".



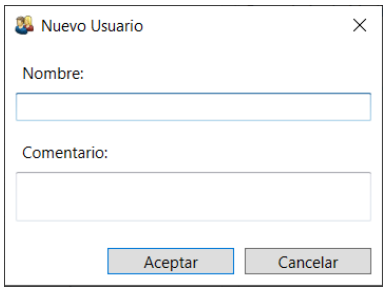
Si la administración de usuarios está activa en un proyecto, un proyecto solo puede ser eliminado por un usuario cuyo rol incluya el derecho "Eliminar proyecto". Sobre la administración de usuarios, consulte [▶ 5.3.1].

5.3.1.2.1 Crear nuevo rol

Crear nuevos roles con derechos individuales.

Procedimiento

1. Haga clic en "Nuevo".
2. Introduzca el nombre del nuevo rol.



3. Introduzca un comentario si es necesario.
4. Pulse "OK".
   ⇨ El nuevo rol se selecciona automáticamente para su posterior configuración.
5. Configure los derechos y los permisos de acceso.
6. Haga clic en "Cerrar".

⇨ El rol se puede asignar a un usuario.

5.3.1.2.2 Eliminar rol

No se puede eliminar un rol si está asignado a un usuario.

1. Seleccione el rol que quiera eliminar de la lista.
2. Haga clic en "Eliminar".
3. Pulse "OK".

⇨ El rol se ha eliminado.

5.3.1.3 Procedimiento de inicio de sesión

Al configurar la gestión de usuarios, se crean detalles de inicio de sesión para administradores y usuarios. Hay varios procedimientos de inicio de sesión con y sin soporte SSO para elegir.

5.3.1.3.1 KEM

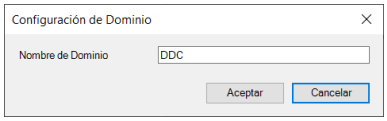
El software KEM proporciona su propio método de inicio de sesión.
Para iniciar sesión, introduzca su nombre de usuario y contraseña.

5.3.1.3.2 Windows

Un usuario de Windows que ya haya iniciado sesión localmente en el PC inicia sesión con su nombre de usuario y contraseña de Windows.
Si se utiliza SSO, el usuario inicia sesión en el proyecto con su función sin que se le vuelva a solicitar ninguna contraseña.

Un usuario conocido a través de una red de dominio de Windows inicia sesión en el proyecto utilizando el nombre de usuario y la contraseña del dominio.
Si se utiliza SSO, el usuario inicia sesión en el proyecto con su función sin que se le vuelva a solicitar ninguna contraseña.

La configuración del dominio solo debe ingresarse una vez por proyecto en la configuración de autenticación. El nombre de dominio se puede obtener del administrador de red del dominio.



Si se agrega un usuario de Windows en la administración de usuarios de KEM, entonces el nombre de usuario de KEM y el nombre de usuario de Windows deben coincidir

5.3.1.3.3 LDAP

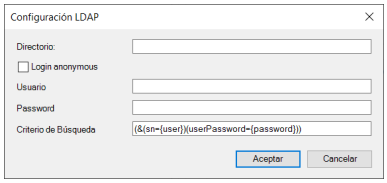
Un usuario conocido a través de LDAP inicia sesión en el proyecto con su rol después de introducir su nombre de usuario y contraseña.

Los detalles de inicio de sesión son administrados por el administrador de la red a través de un servidor LDAP. Los datos se pueden obtener del administrador de la red. Solo es necesario introducirlos una vez por proyecto en la configuración de autenticación.

Requisitos previos

- Se conoce la ruta de acceso a la autenticación LDAP.
- Se conoce el nombre de usuario de un usuario LDAP.
- Se conoce la contraseña LDAP del usuario.

Procedimiento



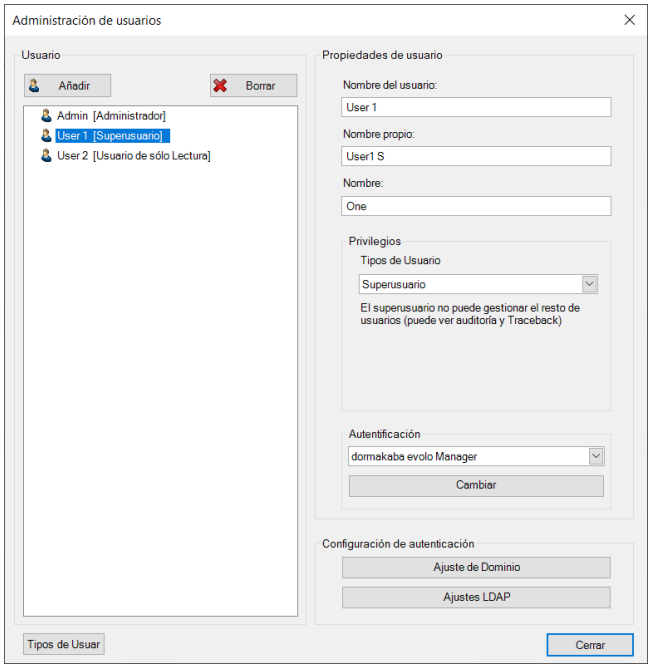
1. Haga clic en "Configuración LDAP" dentro de Administración de usuarios.
2. Introduzca la ruta para la autenticación LDAP en el campo "Ruta".
3. Introduzca el nombre de usuario y la contraseña.
4. Haga clic en "Probar inicio de sesión".
   ⇨ Se realiza la autenticación LDAP del usuario.
   ⇨ Resultado: "Inicio de sesión correcto"
   La ruta guardada puede utilizarse para este y otros usuarios LDAP.

⇨ Resultado: "Error"
Compruebe los datos introducidos e inténtelo de nuevo. Si el error se repite, póngase en contacto con el administrador.

5. Haga clic en "Aceptar" en la ventana de resultados.
6. Pulse "OK".
   ⇨ La ruta se guarda en KEM y el cuadro de diálogo se cierra.
   ⇨ La ruta no se guarda si la ventana se cierra con "Cancelar".

5.3.1.4 Borrar usuarios

Administrador



1. Seleccione el usuario que quiera borrar.
2. Haga clic en "Eliminar".
   ⇨ El usuario queda borrado.
3. Haga clic en "Cerrar".

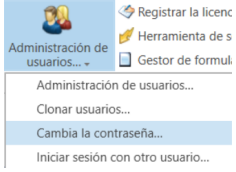
Cuando se haya borrado el último usuario (**Admin**), la administración de usuarios se desactivará.

5.3.1.5 Cambiar/restablecer contraseña

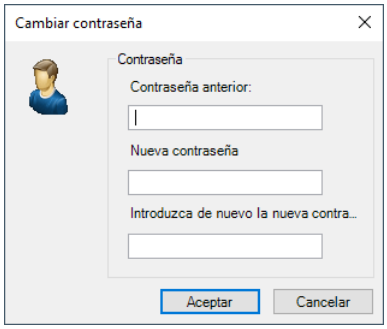
Cambiar la contraseña solo es posible con la autenticación de "dormakaba evolo Manager".

Cambiar contraseña propia
Se requiere la contraseña anterior para cambiar la contraseña.

1. Haga clic en "Administración de usuarios" en la barra de herramientas "Inicio".



2. Haga clic en el botón "Cambiar contraseña" de la selección.



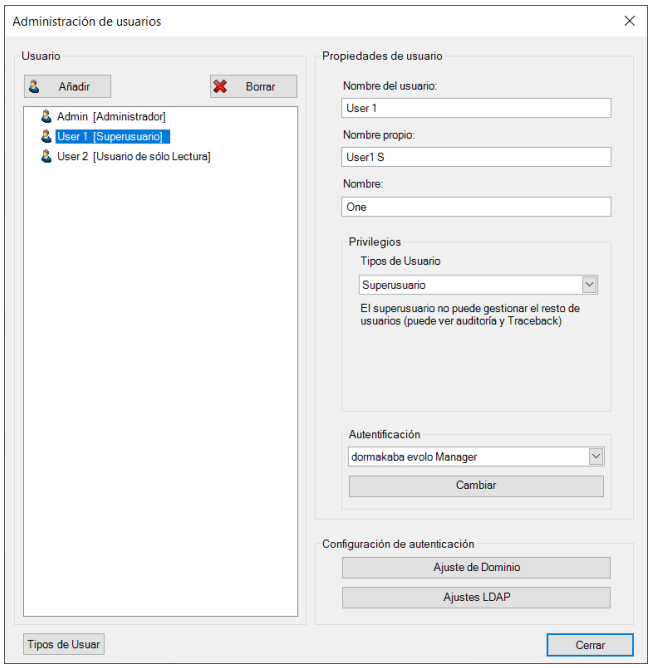
3. Introduzca la nueva contraseña.
4. Pulse "OK".

Restablecer la contraseña

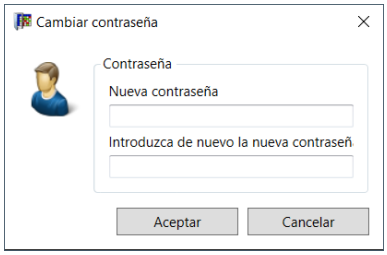
Se requiere el derecho "Gestión de usuarios".

Un usuario con el derecho "Gestión de usuarios" puede asignar una nueva contraseña a un usuario. Para ello no se necesita la antigua contraseña del usuario en cuestión.
Para cambiar la contraseña de administrador, consulte "Cambiar contraseña propia".

1. Haga clic en "Administración de usuarios" en la barra de herramientas "Inicio".
2. Haga clic en el botón "Administración de usuarios" de la selección.



3. Seleccione el usuario.
4. Haga clic en "Cambiar contraseña".



5. Introduzca la nueva contraseña.
6. Pulse "OK".
7. Haga clic en "Cerrar".

5.3.1.6 Iniciar sesión como otro usuario

Procedimiento

1. En el menú "Inicio", haga clic en "Administración de usuarios".

2. Haga clic en el elemento del menú "Iniciar sesión como otro usuario".
3. Especifique nombre de usuario y contraseña.
4. Haga clic en "Iniciar sesión".

5.3.2 Clonar usuarios

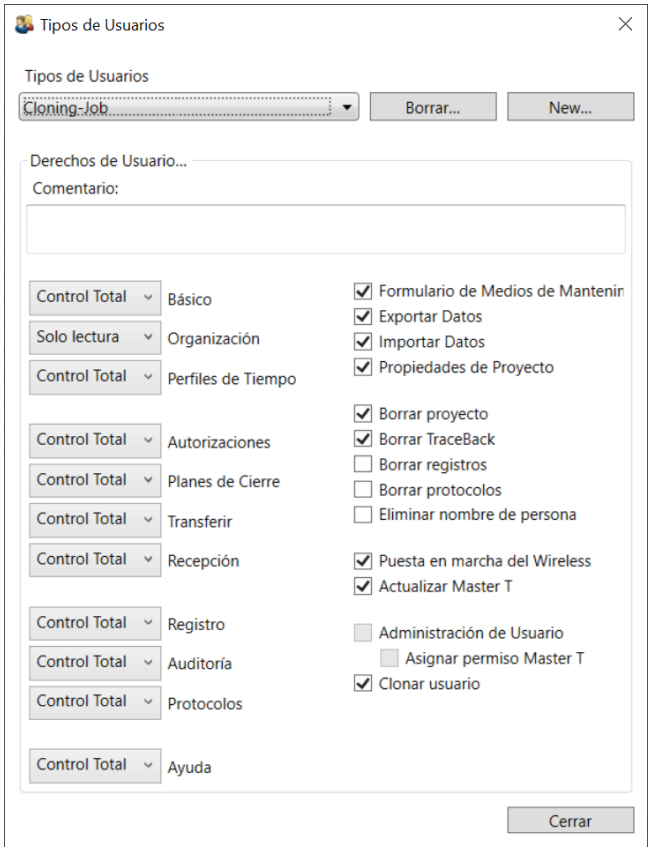
Un usuario cuyo rol incluye el derecho "Clonar usuarios" puede crear un nuevo usuario que tenga el mismo rol y los mismos derechos que el propio usuario.

El derecho "Clonar usuarios" no está incluido en los roles predeterminados de KEM. Para poder asignar este derecho a un usuario, se debe crear un nuevo rol que contenga el derecho. El derecho "Gestión de usuarios" y el derecho "Clonar usuarios" no se pueden asignar en el mismo rol al mismo tiempo.

Consulte el capítulo

- Roles y derechos
- Crear nuevo rol [▶ 5.3.1.2.1]

Ejemplo:



Requisitos previos

- El usuario que ha iniciado sesión tiene el derecho "Clonar usuarios".

Al nuevo usuario se le asigna el mismo método de autenticación de usuario que al usuario que está realizando la clonación.

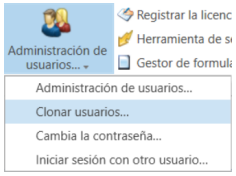
- Método con dormakaba evolo Manager: Asigne una nueva contraseña al usuario clonado.
- Otros métodos: Se debe crear un usuario con el nuevo nombre de usuario en el sistema respectivo antes de iniciar sesión en KEM.
  El nuevo usuario se crea en KEM aunque aún no exista en el sistema. KEM luego muestra un mensaje de advertencia.

El usuario recién creado tiene el mismo rol que el creador y también tiene el derecho "Clonar usuarios".

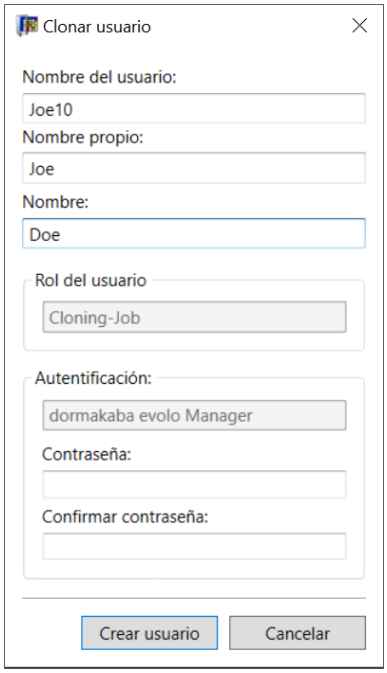
- En la administración de usuarios, el rol del nuevo usuario puede ser ajustado por un administrador o un usuario con el derecho "Gestión de usuarios".

Procedimiento para el método de autenticación "dormakaba evolo Manager"

1. Haga clic en "Administración de usuarios" en la barra de herramientas "Inicio".



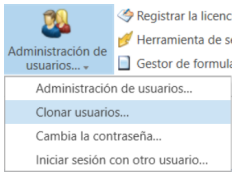
2. Seleccione la función "Clonar usuarios".



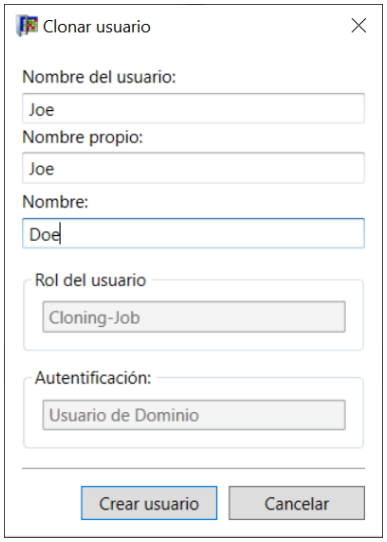
3. Introduzca un nuevo nombre de usuario.
   Opcionalmente, ingrese el nombre y apellido del nuevo usuario.
4. Asigne y confirme una nueva contraseña.
5. Haga clic en "Crear usuario".
   ⇨ El nuevo usuario se ha creado.

Procedimiento del método de autenticación "Usuario de LDAP, Windows o dominio"

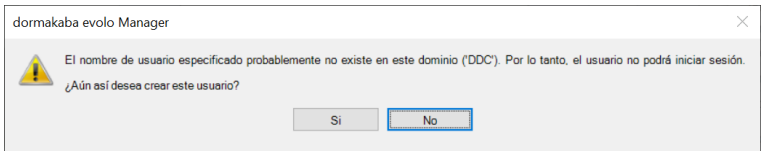
1. Haga clic en "Administración de usuarios" en la barra de herramientas "Inicio".



2. Seleccione la función "Clonar usuarios".



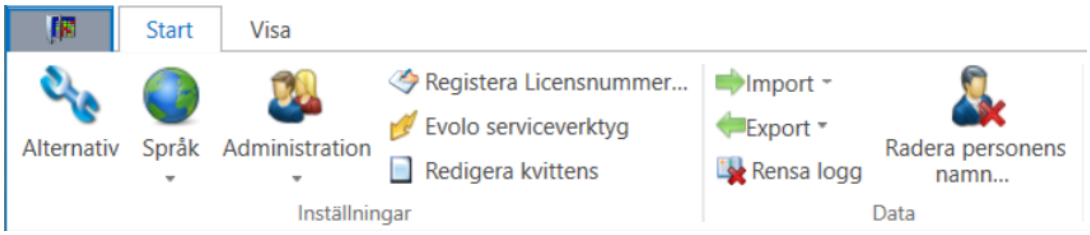
3. Introduzca un nuevo nombre de usuario.
   Para usuarios de Windows y de dominio, el nombre debe coincidir con el nombre de inicio de sesión del nuevo usuario.
   Opcionalmente, ingrese el nombre y apellido del nuevo usuario.
4. Haga clic en "Crear usuario".



5. Es posible que el usuario que se está creando no tenga una cuenta LDAP, de Windows o de dominio (captura de pantalla de muestra).
   Haga clic en "Sí" para crear la entrada de usuario.
   Haga clic en "No" para cancelar la clonación.
   ⇨ "Sí": Se ha creado la entrada para el nuevo usuario.
   ⇨ "No": No se ha creado la entrada para el nuevo usuario. El proceso termina.

Asegúrese de que el nuevo usuario tenga la cuenta de dominio o Windows adecuada y tenga la sesión iniciada antes de iniciar sesión en KEM por primera vez.

5.4 Ajustar formularios de gestión de medios



1. Pulse el botón "Formularios de gestión de medios" de la barra de funciones "Inicio".
2. Active la opción "Personalizado".
3. Realice los ajustes en la zona deseada. Aquí tiene un ejemplo de la emisión de medios.

4. Pulse el botón "Guardar y cerrar".

Recomendación: Si solo se requieren pequeños ajustes del texto, el texto estándar puede copiarse en el portapapeles y pegarse en el campo definido por el usuario. Aquí se pueden realizar los ajustes deseados.

Aviso: si quiere que se incluyan los comentarios, la opción "Imprimir siempre" debe estar seleccionada previamente.

Requisitos de formato

Para el formato del texto personalizado, debe tener en cuenta lo siguiente:

Datos de imagen:

Formato de datos de imagen	JPG o GIF (máx. 100 kB) Logotipo 160 x 40 píxeles Flecha 100 x 40 píxeles
Formato del texto	Etiquetas HTML

Etiquetas HTML:

	Escritura	**Resultado**
Negrita	`<b>Ejemplo</b>`	**Ejemplo**
Subrayado	`<u>Ejemplo</u>`	Ejemplo
Cursiva	`<i>Ejemplo</i>`	*Ejemplo*
Letra grande	`<big>Ejemplo</big>`	Ejemplo
Letra pequeña	`<small>Ejemplo</small>`	Ejemplo
Salto de línea	`Ejemplo Texto`	Ejemplo Texto

6 Parametrizar sistema de cierre

6.1 Crear/abrir/borrar proyecto

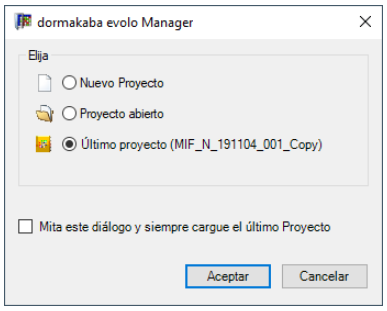
6.1.1 Crear proyecto

El software funciona de manera adaptada a cada proyecto. Antes de poder crear planes de cierre, usuarios o medios, primero se debe crear un proyecto.

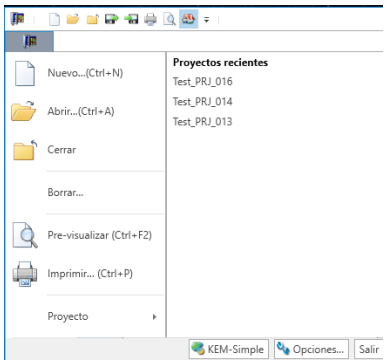
Puede crear un nuevo proyecto al inicio del programa o mediante el menú "Archivo".

Procedimiento

1. En la ventana de selección al iniciar el programa o en el menú "Archivo", seleccione la opción "Nuevo proyecto" (Ctrl+N).
   Aviso: la casilla para saltar el cuadro de diálogo al inicio del programa no está activada.

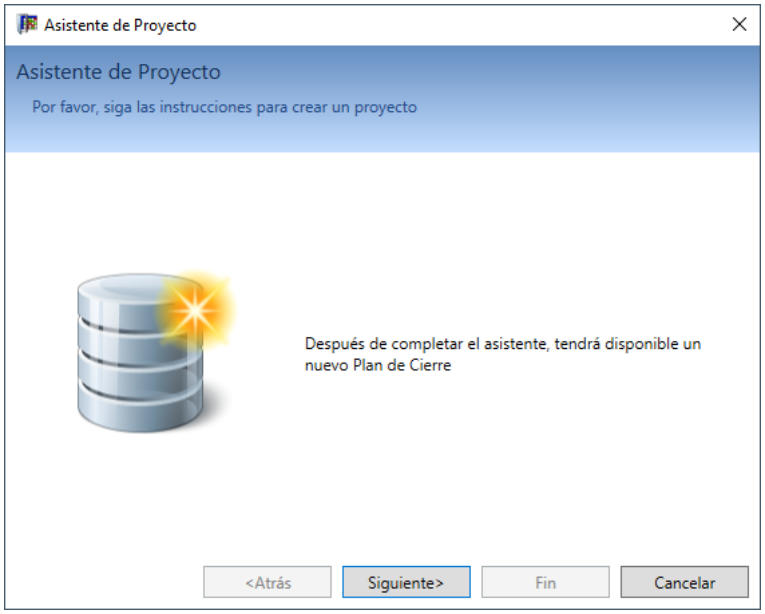


⇨ Aspecto al inicio del programa.

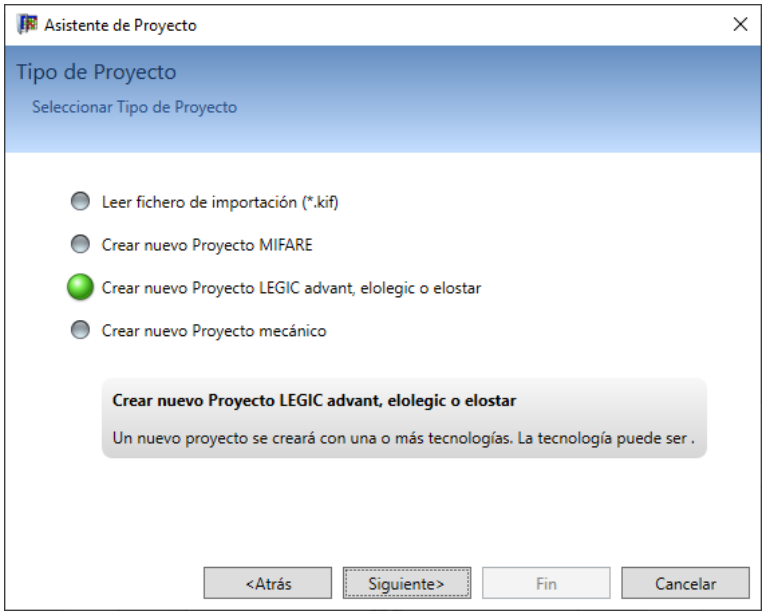


⇨ Aspecto del menú "Archivo"

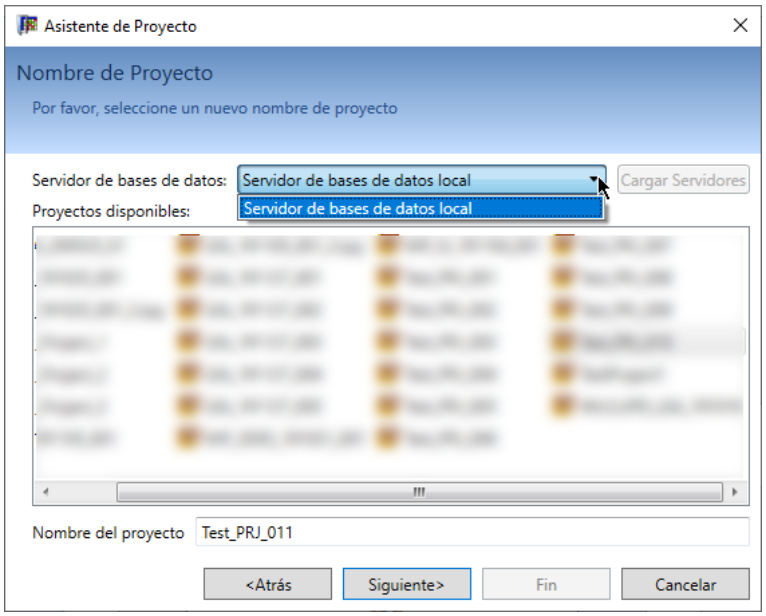
⇨ El asistente para crear un nuevo proyecto se inicia.



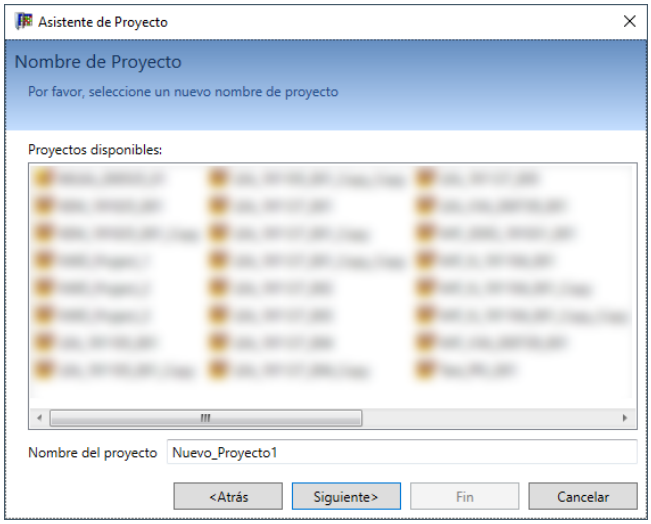
2. Pulse "Siguiente".



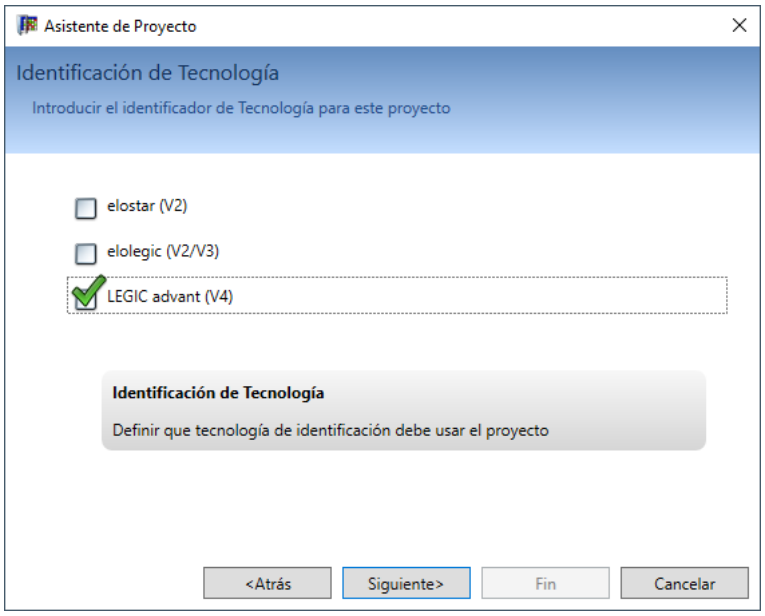
3. Seleccione el tipo de proyecto (consulte la tabla "Tipo de proyecto").
4. Pulse "Siguiente".



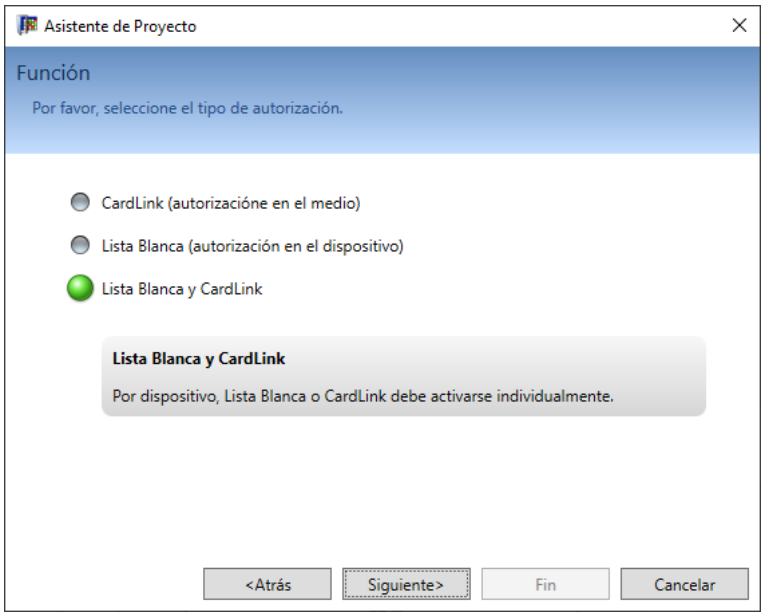
5. Seleccione el servidor de base de datos de la lista.
   Aviso: Sáltese este paso si "Mostrar servidores de bases de datos" en "Opciones" no está seleccionado. Consulte el capítulo [▶ 5.1]. En este caso, la selección de lista "Servidor de base de datos" no es visible.
   Si el servidor no consta en la lista, añádalo de la forma descrita en el capítulo "Editar servidores de bases de datos" [▶ 3.2.3].



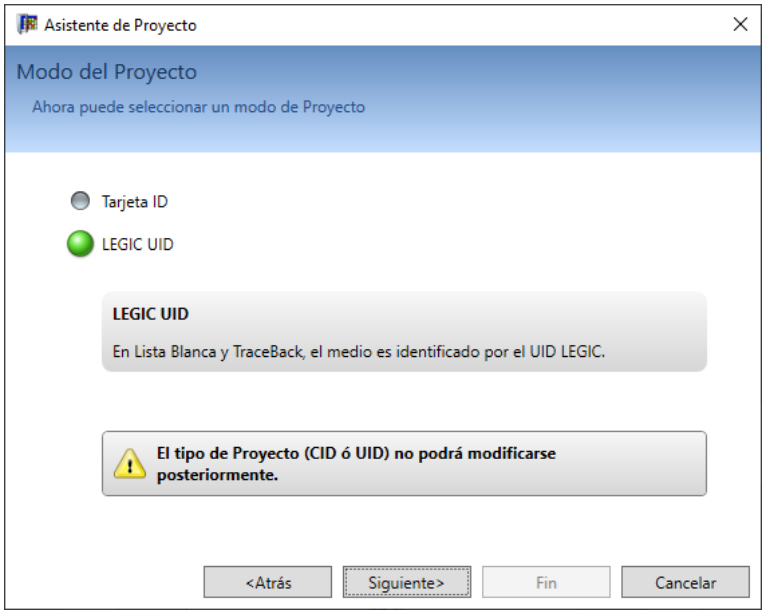
6. Escriba el nombre del proyecto en el campo "Nombre del proyecto".
7. Pulse "Siguiente".



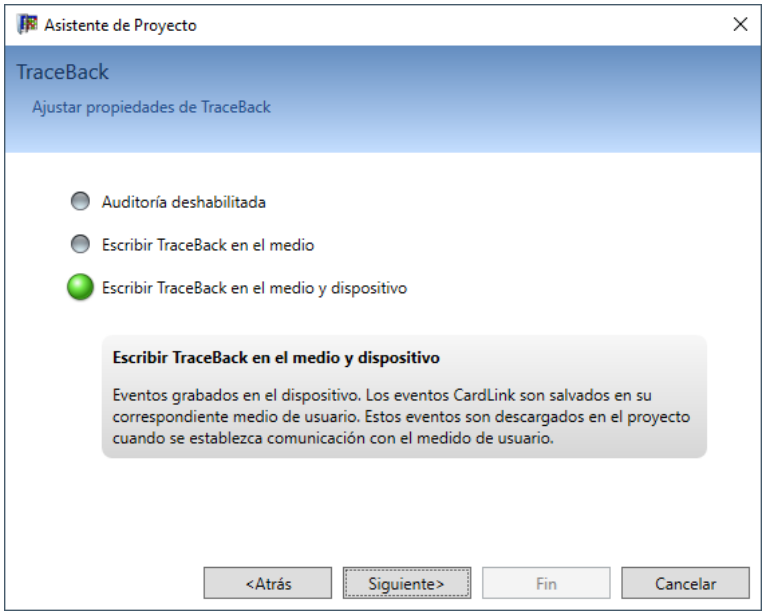
8. Seleccione la tecnología de identificación (LEGIC; consulte la tabla "Tecnologías de identificación").
9. Pulse "Siguiente".



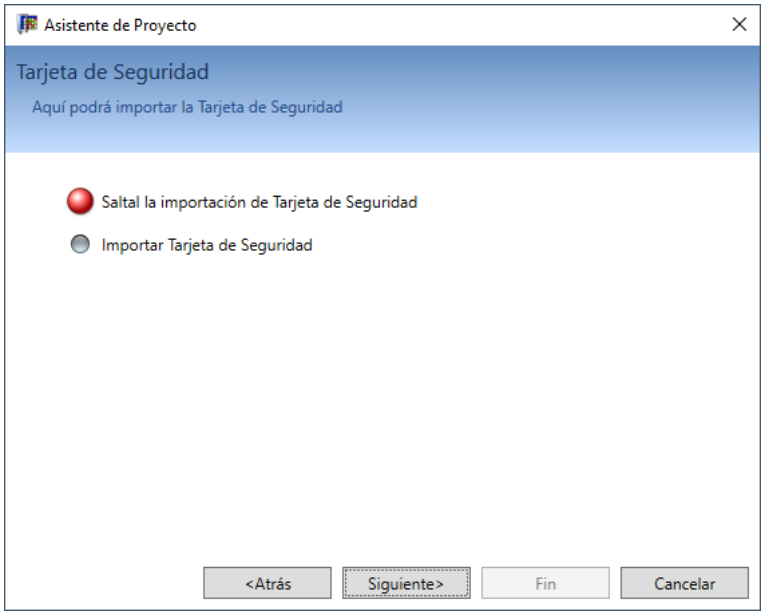
10. Seleccione un tipo de autorización (consulte la tabla "Tipo de autorización"). Encontrará más información sobre los tipos de autorización en los capítulos [▸ 2.3.2] y [▸ 2.3.3].
11. Pulse "Siguiente".



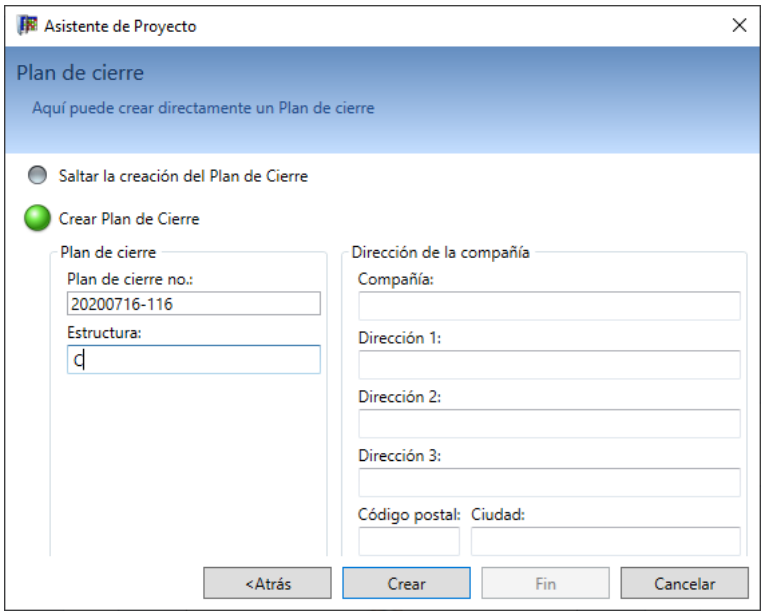
12. Seleccione un modo de proyecto (consulte la tabla "Modo de proyecto"). Para más información sobre los modos de proyecto, consulte el capítulo .
13. Pulse "Siguiente".



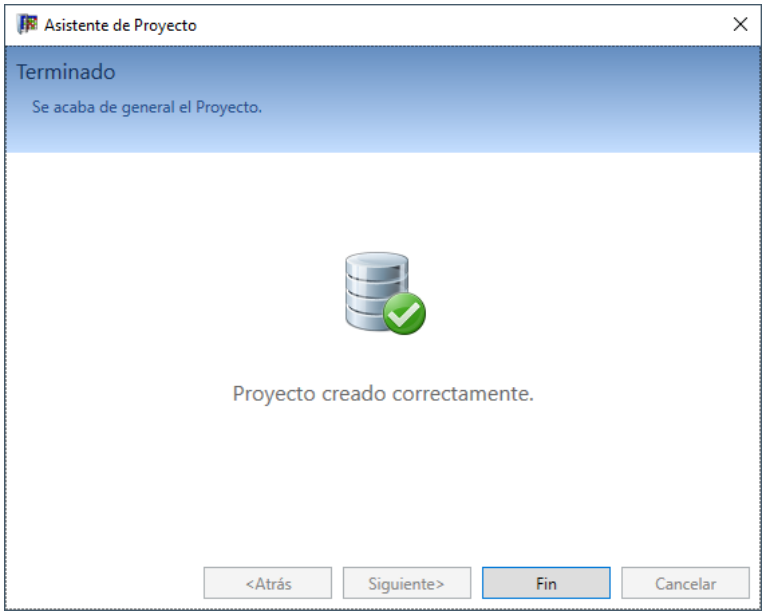
14. Seleccione las propiedades de Traceback (consulte la tabla "Propiedades de Traceback").
15. Pulse "Siguiente".



16. Lea la tarjeta de seguridad (consulte la tabla "Tarjetas de seguridad"). La tarjeta de seguridad también se puede leer más tarde.
17. Pulse "Siguiente".



18. Seleccione "Crear plan de cierre" y rellene los campos de entrada.
    Si va a crear o a importar el plan de cierre más tarde, seleccione "No crear plan de cierre".
19. Pulse "Crear".



20. Pulse "Listo".

⇨ El nuevo proyecto y su plan de cierre están creados y se pueden parametrizar.

Tablas de parámetros

Las tablas incluyen indicaciones para realizar la parametrización al configurar un proyecto.

Tabla tipo de proyecto

Tipo de proyecto	Descripción
Leer archivo importado	Se importa un archivo KIF (proyecto/sistema).
Nuevo proyecto MIFARE	Se crea un proyecto MIFARE. Una vez seleccionada la tecnología, no se puede cambiar.
Nuevo proyecto LEGIC advant, elolegic o elostar	Se crea un proyecto LEGIC con una o más tecnologías de identificación. Es posible cambiar entre las tecnologías disponibles en cualquier momento.
Nuevo proyecto mecánico	Se crea un proyecto mecánico. Se crea un proyecto vacío únicamente para componentes mecánicos. Posteriormente será posible ampliar este proyecto activando una tecnología LEGIC/ elolegic/elostar o MIFARE con componentes electrónicos.

Tabla Tecnologías de identificación

Tecnología de identificación Tecnología	Descripción
elostar V2	El proyecto se crea para componentes elostar V2.
elolegic V2/V3	El proyecto se crea para componentes LEGIC V2 o V3.
LEGIC advant V4	El proyecto se crea para componentes LEGIC V4.

Tabla Tipo de autorización

Tipo de autorización	Descripción
CardLink	Las autorizaciones se guardan en los medios para que los componentes solo deban configurarse una vez.
Lista blanca	Las autorizaciones se guardan en los componentes.
CardLink y Lista blanca	Los componentes se pueden ajustar de forma individual para CardLink o para la Lista blanca.

Tabla Modo de proyecto

Modo de proyecto	Descripción
Card ID	Los medios se identifican mediante un número de tarjeta programado. Para ello, los medios deben tener la configuración correspondiente.
Safe UID (por defecto)	El UID se cifra y se comprueba de forma adicional. Para ello se necesitan aplicaciones especiales en los medios. Los medios suministrados por dormakaba ya las incluyen de fábrica.
UID organizativo	Solo se utiliza el UID. Este modo es ideal para el tipo de autorización "Lista blanca" para aplicaciones de organización que no requieran un alto nivel de seguridad.

Tabla Propiedades de Traceback

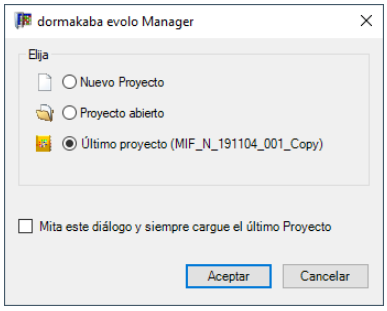
Propiedades	Descripción
Traceback apagada	No se escribe ningún dato de Traceback.
Escribir Traceback en los componentes	El componente escribe registros de Traceback en la memoria.
Escribir Traceback en el componente y en el medio	En una autorización CardLink, el componente comprueba si el medio requiere un registro de Traceback. Entonces el componente escribe un registro de Traceback en el medio y en su propia memoria.
Recomendamos activar solo la "Traceback de actuadores". Si activa la Traceback de medios, la velocidad de escritura y lectura se reduce. Esto implica más consumo energético de los componentes y menos vida útil de la batería. El Traceback de medios solo es posible en los medios MIFARE DESFire y LEGIC advant 14443A.	

Tabla Tarjetas de seguridad

Modo de proyecto	Tarjeta de seguridad MIFARE	Tarjeta de seguridad LEGIC	Aviso
Card ID	C		
CardLink	C		
Otras		C1 o C2	Las tarjetas de seguridad LEGIC C1 o C2 disponen de 16 espacios de almacenamiento por lector de sobremesa. Para crear un nuevo proyecto con más tarjetas de seguridad, debe borrar un espacio de almacenamiento en las propiedades del lector de sobremesa.

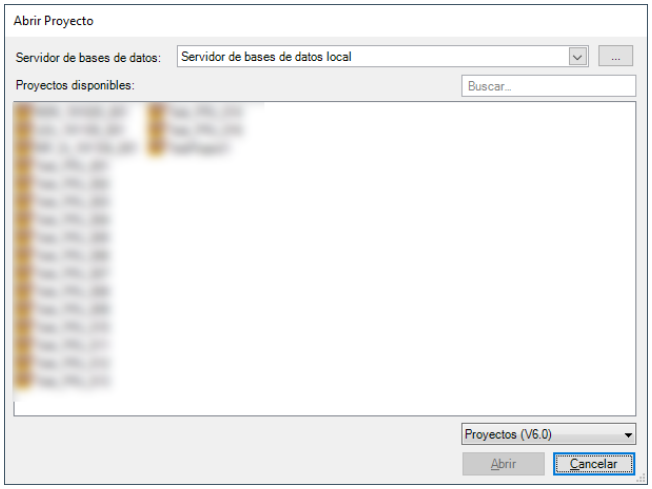
6.1.2 Abrir proyecto

Para abrir un proyecto ya creado, seleccione uno de los proyectos utilizados recientemente o pulse "Abrir" en el menú "Archivo".

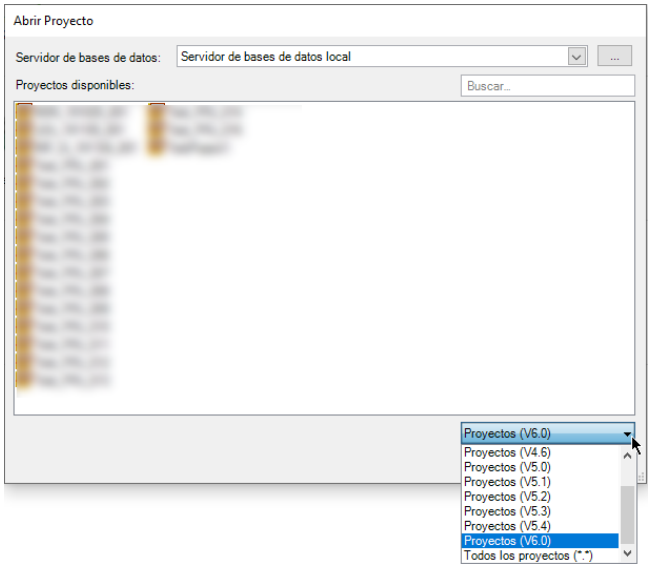


En el cuadro de diálogo "Abrir proyecto" aparecen todos los proyectos disponibles en el servidor de base de datos seleccionado.

Aviso: la selección del servidor de base de datos solo es posible si esta opción está seleccionada en "Opciones/General/Mostrar servidores de bases de datos". Consulte el capítulo [▸ 5.1].



Delimitar la selección de proyecto:



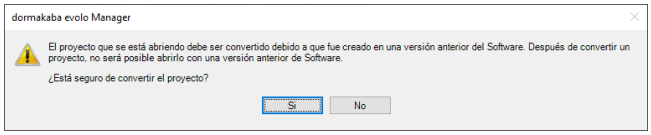
"Todos los proyectos(*.*)" muestra todos los proyectos del servidor de base de datos seleccionado. También se muestran proyectos de otras versiones de KEM. Tras seleccionar la versión de KEM de la lista, solo aparecerán los proyectos creados con la versión seleccionada.

Tiene las siguientes opciones:

Aviso: Si "Mostrar servidores de bases de datos" no está seleccionado en las Opciones, solo se podrán seleccionar y abrir los proyectos mostrados.

- Seleccione un servidor de base de datos de la lista.
  Consulte "Editar servidores de bases de datos: selección del servidor de base de datos" [▸ 3.2.3].
- Seleccione una entrada de la lista de proyectos.
  Pulse "Abrir".

Si necesita abrir un proyecto de una versión de KEM anterior, se iniciará el convertidor automáticamente.
Tiene las siguientes opciones:



- Si selecciona "Sí":
  - Se creará una copia de seguridad de la versión antigua del proyecto en el servidor de base de datos.
  - El proyecto se convertirá en un proyecto de la versión actual de KEM.
  - El proceso de conversión puede tardar un poco.
- Si selecciona "No":
  - El proyecto no se convertirá.
  - El conversor se cerrará.

6.1.3 Borrar proyecto

AVISO

Pérdida de datos

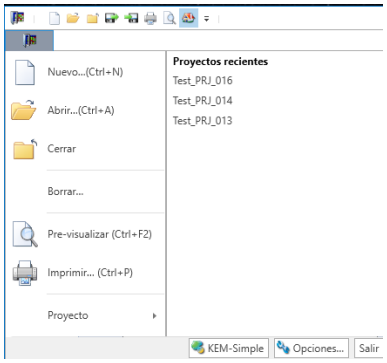
Los proyectos quedan eliminados permanentemente. No es posible recuperar un proyecto borrado.

- Antes de borrar un proyecto, cree una copia de seguridad del proyecto o expórtelo. Consulte [▸ 12.1]

Si la administración de usuarios está activa en un proyecto, un proyecto solo puede ser eliminado por un usuario cuyo rol incluya el derecho "Eliminar proyecto". Sobre la administración de usuarios, consulte [▸ 5.3.1].

Procedimiento

1. En el menú "Archivo", pulse el botón "Borrar".

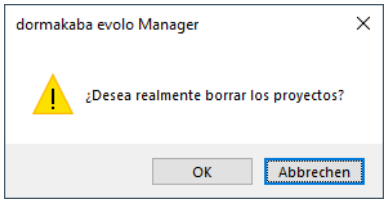


   ⇨ En el cuadro de diálogo "Borrar" aparecen todos los proyectos disponibles en el servidor de base de datos seleccionado.

2. Si lo necesita, delimite la selección de proyecto por versiones de KEM.

⇨ "Todos los proyectos(*.*)" muestra todos los proyectos del servidor de base de datos seleccionado. También se muestran proyectos de otras versiones de KEM. Tras seleccionar la versión de KEM de la lista, solo aparecerán los proyectos creados con la versión seleccionada.

3. Seleccione los proyectos de la lista que quiera borrar.
   Seleccione "Borrar".

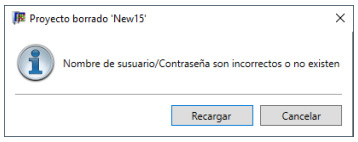
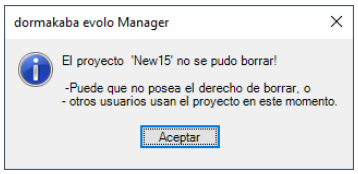


4. Confirme el borrado de los proyectos seleccionados.
   Aviso: los proyectos con administración de usuarios [▶ 5.3.1] activa requieren la introducción de los datos del administrador con su contraseña para borrarse.

Borrar proyectos creados con versiones de KEM anteriores a la 6.1:

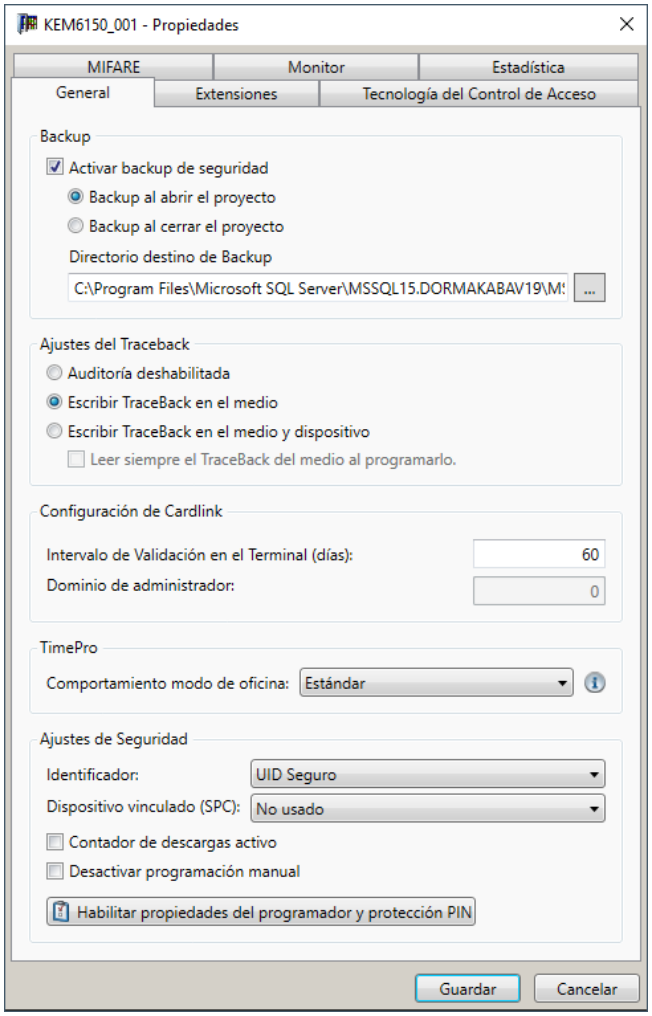
- La gestión de usuarios no está activa:
  El proyecto se puede borrar sin ningún requisito.
- La gestión de usuarios está activa:
  Para borrar un proyecto, serán necesarios el nombre de usuario y la contraseña de un administrador.

Posibles errores/problemas

Mensaje	Motivo	Solución
 Nombre de usuario desconocido o contraseña incorrecta Nombre de usuario/ contraseña incorrecto o desconocido.	El nombre de usuario y/o la contraseña no coinciden con los datos consignados para el proyecto que quiere borrar.	• Vuelva a intentarlo con otro usuario. • Cancelar
El nombre de usuario y la contraseña son correctos, pero no tiene el derecho para borrar proyectos: utilice un usuario con el derecho "Borrar proyectos".	El usuario introducido no cuenta con el derecho necesario.	• Seleccione otro usuario con el derecho necesario (p. ej., el administrador) • Cancelar
	• Un proyecto abierto por otro usuario no se puede borrar. • El propio proyecto no se puede borrar.	Cierre el proyecto y vuelva a intentar borrar el proyecto.

6.2 Propiedades de proyecto

6.2.1 Generalidades



Las propiedades de proyecto se pueden visualizar pulsando la tecla F4.

Copia de seguridad		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
Activar la copia de seguridad	Se crea una copia de seguridad de forma automática en el directorio indicado para la ruta de copias de seguridad.	✓	✓	✓	✓
Copia al abrir un proyecto	La copia de seguridad se crea al abrir el proyecto.	✓	✓	✓	✓
Copia al cerrar un proyecto	La copia de seguridad se crea al cerrar el proyecto.	✓	✓	✓	✓
Ajustes de Traceback					
Traceback apagado	No se realiza ninguna actividad de Traceback.	✓	✓	✓	✓
Escribir Traceback en actuador	El Traceback se escribe en la memoria del componente.	✓	✓	✓	✓
Escribir el Traceback en actuadores y medios	El Traceback se escribe en la memoria del componente y en el medio. En MIFARE, el Traceback de medios solo es compatible con medios DESFire.	✓	✓	✗	✗

Al programar medios, leer siempre el Traceback del medio	Antes de programar una autorización CardLink, se leen los datos de Traceback del medio.	✓	✓	✗	✗
Propiedades de CardLink					
Ciclo de funcionamiento posterior en días	Tiempo durante el cual un medio todavía se puede validar cuando ya ha caducado su tiempo de validación.	✓	✓	✗	✗
Área de administración	El valor estándar es 0	✓	✓	✗	✗
TimePro	Comportamiento del modo Office				
Estándar	Activación/desactivación inmediata	✓	✓	✓	✗
Con retraso	Mantener el medio 2 s para activar/ desactivar. Solo componentes MRD.	✓	✓	✗	✗
Ajustes de seguridad					
Identificación	UID o UID organizativo.	✓	✓	✗	✗
Vinculación del actuador (SPC)	• No utilizado • para exportar el actuador • para exportar el actuador y ajustar la hora	✓	✓	✗	✗
Contador de programación de actuador activo	Numeración de la configuración del actuador. Esto garantiza que no se pueda cargar ninguna configuración obsoleta.	✓	✓	✗	✗
Evitar programación manual		✓	✓	✓	✗
Mostrar propiedades del programador y protección con PIN	Las propiedades del programador se muestran y se pueden modificar. Se puede activar la protección con PIN.	✓	✓	✗	✗
Ampliaciones					
Usar terminal	Activa el terminal para la transferencia de autorizaciones.	✓	✓	✓	✗
Uso inalámbrico	Activa la opción inalámbrica para la transferencia de autorizaciones.	✓	✓	✗	✗
Auditorías de autorizaciones	Auditoría de cualquier actividad para controlar los cambios a nivel de autorizaciones en un sistema CardLink.	✓	✓	✗	✗

Aviso: En elolegic solo es compatible la U-Line

6.2.1.1 Propiedades de CardLink

Ciclo de funcionamiento posterior en días
Un actuador de validación puede validar un medio hasta que caduque su ciclo de funcionamiento posterior. De esta forma, el medio vuelve a considerarse fiable.

El ciclo de funcionamiento posterior puede configurarse de 0 a 255 días. El valor por defecto es 60.

Área de administración
Posibles zonas gestionadas: 256

El valor por defecto es 0.

Si tiene preguntas sobre la área de administración, contacte con el servicio técnico. El ajuste de la área de administración solo puede modificarse con la ayuda del servicio técnico.

6.2.1.2 Ajustes de seguridad

En el programador se puede definir un PIN propio de 6 dígitos.
No es posible cambiar el PIN desde KEM.
El PIN solo se puede cambiar/borrar directamente desde el programador.
El programador se debe desbloquear de forma independiente antes de realizar cualquier intercambio de datos con KEM.
Encontrará la información correspondiente en el manual del programador.

El SPC (código de protección del sistema, por sus siglas en inglés) es una protección adicional para un sistema de cierre; una vez activado el sistema, solo es posible intercambiar datos y autorizaciones entre los componentes que pertenezcan al sistema de cierre.

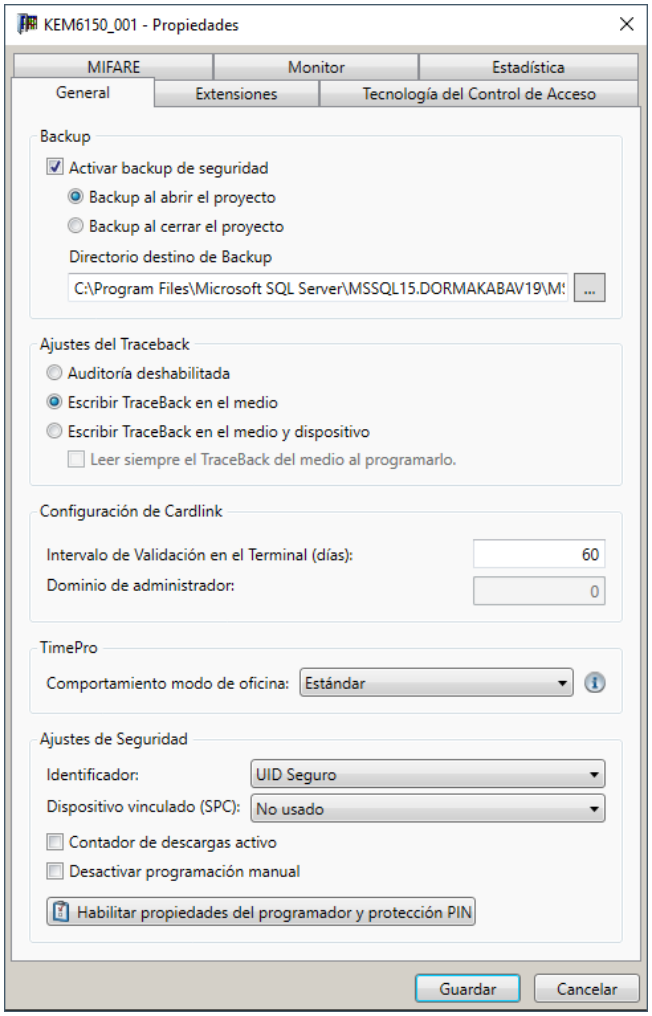
Ajustes
Los ajustes del código de protección del sistema se pueden llevar a cabo en las propiedades de proyecto. Encontrará explicaciones en el capítulo [▸ 6.2.1].

Se recomienda activar la protección con PIN y el SPC.
Para ello, debe tener en cuenta estas propiedades:

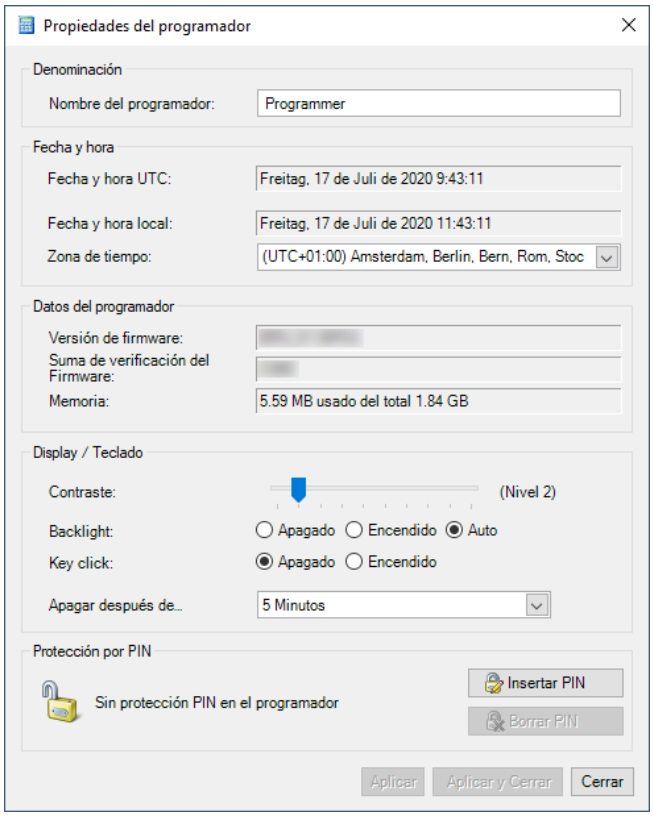
- La vinculación del actuador (SPC) y la protección con PIN solo son compatibles con el programador 1460.
- Si no se ha realizado una exportación al programador 1460 y a los componentes, un SPC existente sigue siendo válido.
- La desactivación del SPC requiere un restablecimiento INI de todos los componentes. A continuación, hay que reprogramarlos.
- Los ajustes SPC de los componentes ya no se pueden cambiar.

Procedimiento para activar la protección con PIN

1. Abra las propiedades de proyecto (F4).



2. Pulse el botón "Mostrar propiedades del programador y protección con PIN".
3. Seleccione "Definir PIN".



4. Introduzca un PIN numérico de 4 dígitos.

5. Pulse el botón "OK".

Con el PIN activado y el programador conectado, tiene las siguientes opciones:

- Introducir el PIN en el programador.
- Restablecer el PIN.
  Aviso: Se borrarán todos los datos del programador. El programador deberá volver a sincronizarse con el software.

Borrar PIN

Si necesita volver a borrar un PIN, pulse el botón "Borrar PIN" de la ventana "Propiedades del programador".

Importar datos protegidos del programador

El programador solo puede importar los datos de un sistema de cierre protegido con SPC si el SPC del programador y el SPC del software coinciden.

6.2.2 Extensiones

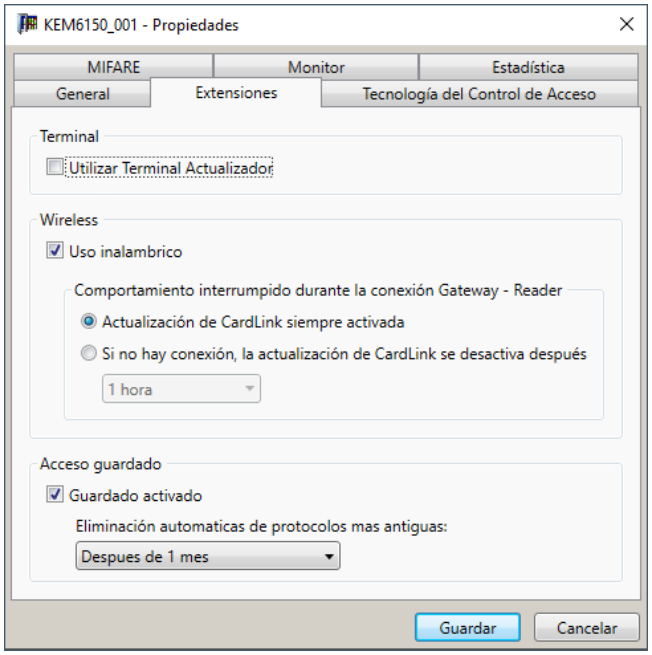
6.2.2.1 Auditorías de autorizaciones

La activación de la lista de auditorías puede generar una gran cantidad de datos.

Solo podrá ver y editar esta sección si se cumplen las siguientes condiciones:

- En Tipo de proyecto está seleccionado "CardLink" o "Lista blanca y CardLink".
- La gestión de usuarios está activa.

En un entorno CardLink se registran todas las acciones que ocasionen cambios en las autorizaciones.



Activar las auditorías de autorizaciones

Requisito

- El usuario debe tener la sesión iniciada como administrador.

Procedimiento

1. Marque la casilla.

2. De entre las opciones de la lista, seleccione el tiempo durante el cual se conservarán las entradas más antiguas antes de borrarse automáticamente.
   El borrado de las entradas más antiguas se produce al abrir el proyecto.
3. Pulse "Guardar".

Abra la lista de auditorías con el menú "Navegador/Registros". Consulte el capítulo Registros [▶ 6.13].

Desactivar las auditorías de autorizaciones

Si la petición se acepta, al desactivar las auditorías se borran todos los datos de auditoría.

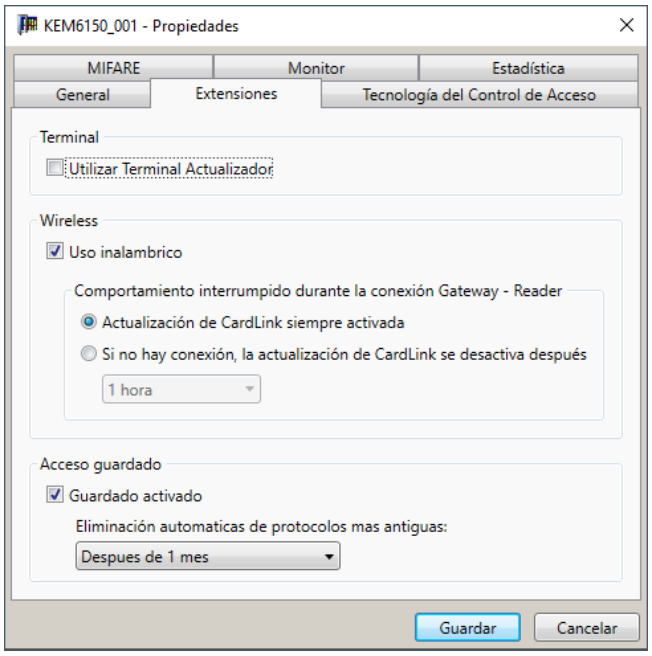
- Si necesita conservar las auditorías, antes de desactivar la función debe exportar la lista de auditorías. Consulte el capítulo [▶ 6.13.2].

Requisito

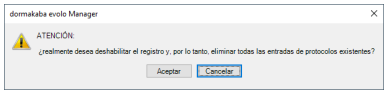
- El usuario debe tener la sesión iniciada como administrador.

Procedimiento

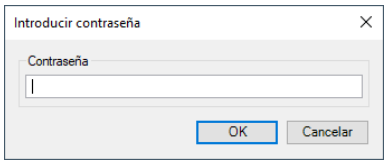
1. Desactive la casilla.



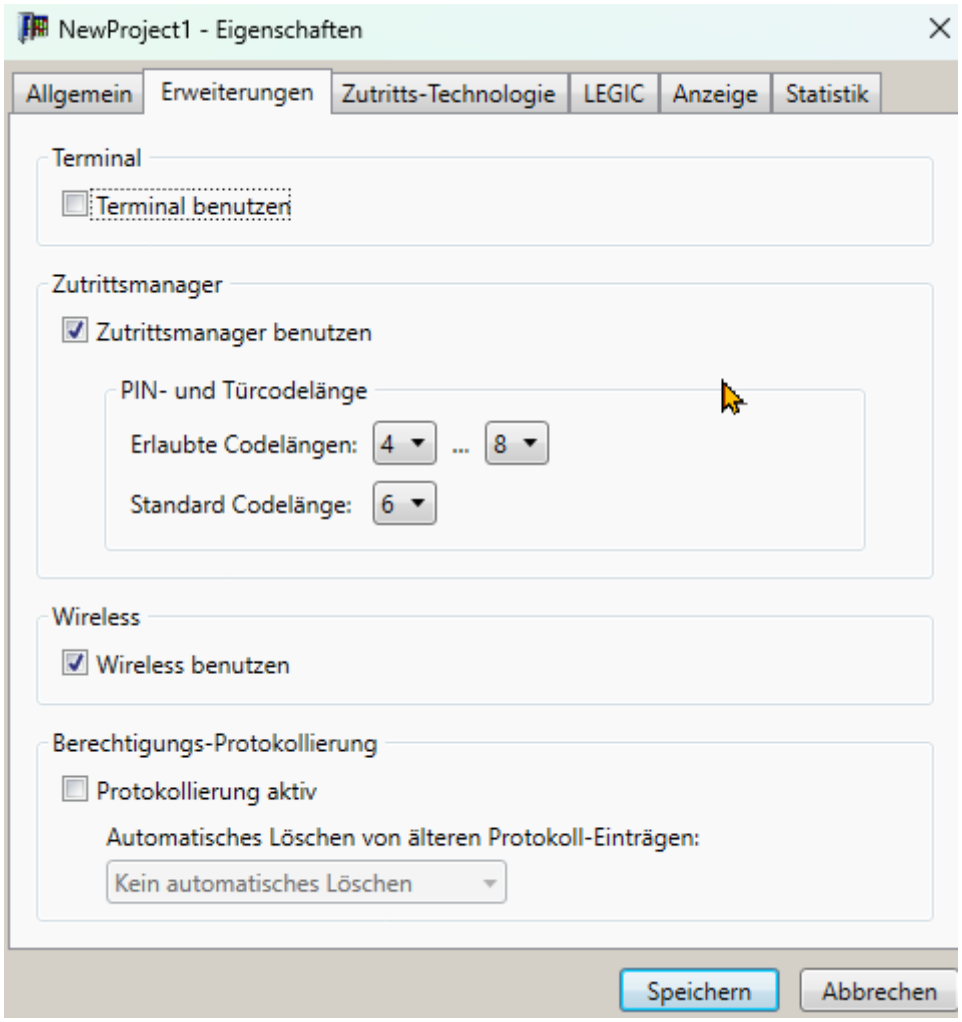
2. Pulse "OK".



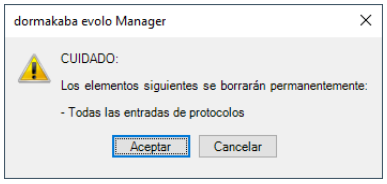
3. Introduzca la contraseña y pulse "OK".



4. Pulse "Guardar".

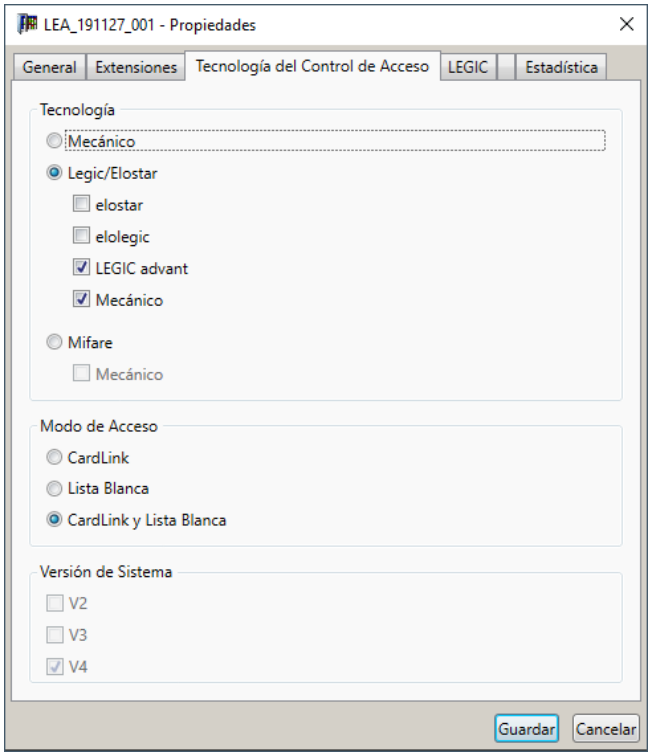


5. Pulse "OK".



⇨ Las entradas de auditorías se han borrado.

6.2.3 Tecnología de acceso



Seleccione la tecnología y el modo de acceso. Combinaciones posibles:

Autorizaciones de acceso		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
CardLink	Activar CardLink	✓	✓	✓	✗
Lista blanca	Activar Lista blanca	✓	✓	✓	✓
CardLink y Lista blanca	Activar CardLink y Lista blanca	✓	✓	✓	✗
Versión del sistema					
V4	Versión del perfil temporal	✓	✓	✗	✗
V3	Versión del perfil temporal	✓	✓	✓	✗
V2	Versión del perfil temporal	✗	✗	✓	✓

LEGIC advant

Si selecciona LEGIC como tecnología de acceso, las tecnologías activas se pueden definir de forma automática o manual. Los ajustes se aplican a todo el proyecto.

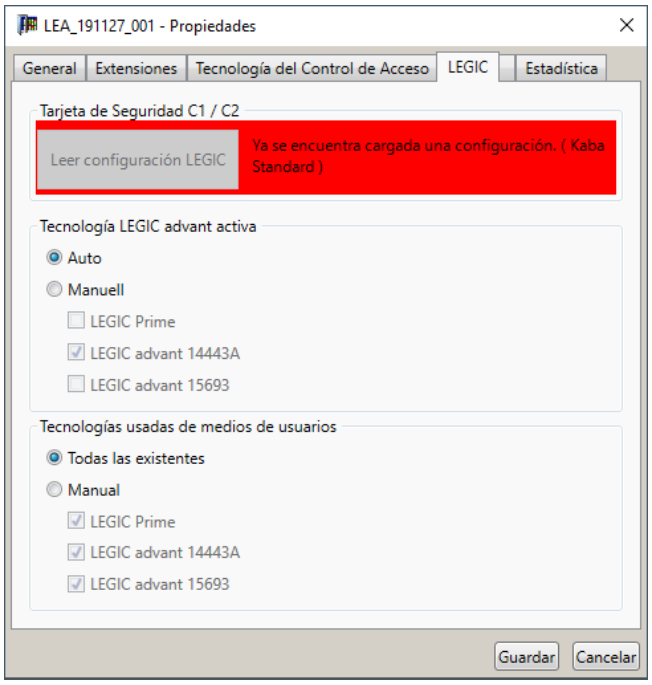
En los medios, las distintas tecnologías de acceso tienen asignadas zonas de memoria diferenciadas.

Los medios LEGIC CTC son compatibles con todas las tecnologías.

Tecnologías activas de LEGIC advant:

- Automática:
  La tecnología activa se reconoce y se ajusta automáticamente.

- Manual:
  Debe seleccionar una o varias tecnologías de las que aparecen.
  Aviso: los medios que no pertenezcan a las tecnologías seleccionadas ya no se podrán leer ni escribir.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693



Tecnologías usadas por los medios de usuario:

Solo se pueden leer o escribir registros de datos de las tecnologías activas.

- Todas las disponibles:
  La tecnología activa determina qué tecnología se lee o se escribe en el medio de usuario.
- Manual:
  Debe seleccionar una o varias tecnologías de las que aparecen.
  Aviso: los medios que no pertenezcan a las tecnologías seleccionadas ya no se podrán leer ni escribir.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

Modo de acceso

Lista blanca	El componente se abre/cierra con autorizaciones de Lista blanca.
CardLink	El componente se abre/cierra con autorizaciones de CardLink.
CardLink con validación	El componente se abre/cierra con autorizaciones de CardLink. Los medios autorizados que se presenten en el componente se validan.
CardLink con actualización	El componente se abre/cierra con autorizaciones de CardLink. Los medios autorizados que se presenten en el componente se validan. Siempre se realiza una actualización de las autorizaciones de CardLink de los medios presentados.
Mixto	El componente se abre/cierra con autorizaciones CardLink o Lista blanca.
Mixto con validación	El componente se abre/cierra con autorizaciones de CardLink o Lista blanca. Los medios autorizados que se presenten en el componente se validan.
Mixto con actualización	El componente se abre/cierra con autorizaciones de CardLink o Lista blanca. Siempre se realiza una actualización de las autorizaciones de CardLink de los medios presentados.

Actualización

Se realizan una actualización de las autorizaciones y la validación de los medios presentados.
Los medios incluidos en la Lista de bloqueo perderán la validez. A partir de este momento ya no será posible el acceso a CardLink.

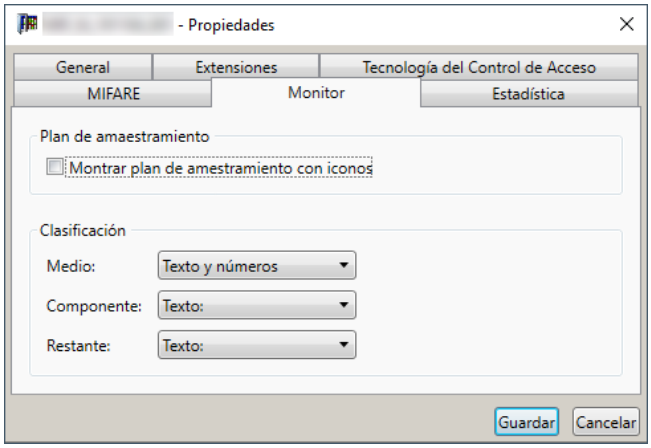
La validación no se lleva a cabo si:

- El medio consta en la Lista de bloqueo.
- El medio está fuera de su ciclo de funcionamiento posterior.

La actualización no se lleva a cabo si:

- El medio consta en la Lista de bloqueo.

6.2.4 Visualizar



Plan de cierre
Para que aparezcan iconos de los medios y componentes, active la casilla "Mostrar plan de cierre con iconos".

Clasificación
Los siguientes ajustes determinan el criterio de ordenación en los campos de texto que se seleccionen para la clasificación. Las adaptaciones se aplican a las pestañas del menú "Elementos básicos", p. ej., medios o actuadores.

Ajustes:

- Texto: Ordenación alfabética
  Ejemplo: 1.OG, 10.OG, 11. OG, 2.OG, 20.OG
- Texto y cifras: Ordenación alfanumérica
  Ejemplo: 1.OG, 2.OG, 10.OG, 11. OG, 20.OG

6.3 Medios

Las tarjetas de seguridad sirven para individualizar y unificar el sistema.

Los medios Master sirven para programar un sistema. Los medios Master y el sistema tienen una tarjeta de seguridad asignada.

La autorización de los usuarios en los componentes requiere el uso de medios de usuario.

Los nuevos tipos de medios con cifrado triple CTC (Legic), AES y 3DES (MIFARE) solo se pueden usar en KEM si se cumplen estos requisitos de hardware y software:

- Versión de KEM a partir de la 5.4
- Lector de sobremesa MRD
- Versión de firmware del componente a partir de la 42.xx

Los siguientes requisitos se aplican al uso de medios MIFARE o LEGIC EV3:

- dormakaba evolo Manager (KEM) a partir de la versión 6.2
- Lector de sobremesa MRD 91 08
- Firmware de los componentes a partir de la versión 42.xx

6.3.1 Tarjetas de seguridad

Las tarjetas de seguridad se usan en un entorno LEGIC o MIFARE. Las funciones de las tarjetas de seguridad son distintas según la tecnología que use.

6.3.1.1 Descripción

LEGIC advant tiene 2 tarjetas seguridad:

- La tarjeta de seguridad C1 es para la segmentación de medios específicos de un sistema.
- La tarjeta de seguridad C2 es para la inicialización del sistema con lectores de sobremesa y componentes de validación en CardLink.

MIFARE tiene la tarjeta de seguridad C:

- La tarjeta de seguridad C es necesaria para integrar la llave perteneciente a un sistema de un entorno MIFARE en el sistema de cierre. Define la llave del sistema y la organización de la memoria de los medios de usuario.

Aumento de la seguridad del sistema con cifrado AES o 3DES

Disponer de cifrado aumenta la seguridad de un sistema. El cifrado AES ofrece una seguridad más elevada que el cifrado 3DES.

Es posible aplicar el cifrado AES o 3DES con una tarjeta de seguridad MIFARE y medios de usuario MIFARE DESFire.

Al pedir la tarjeta de seguridad para un nuevo sistema, considere usar AES o 3DES.

No se recomienda aplicar AES o 3DES a un sistema existente mediante una nueva tarjeta de seguridad.

6.3.1.2 Funciones de seguridad LEGIC/MIFARE

Tarjeta de seguridad C1/C2 (LEGIC) (Solo se puede cargar con los modos de proyecto Card ID o CardLink)		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
Configurar medios LEGIC	Tarjeta de seguridad C1 para segmentar, leer y escribir los medios. Tarjeta de seguridad C2 para leer y escribir los medios de forma duradera.	✗	✓	✓	✗
Tarjeta de seguridad C (MIFARE) (Solo se puede cargar con los modos de proyecto Card ID o CardLink)					
Leer Sitekey en proyecto	La tarjeta de seguridad C se lee para introducirla en el proyecto y este se individualiza. Tras un reinicio del sistema no se debe presentar ninguna tarjeta de seguridad C al mismo lector de sobremesa.	✓	✗	✗	✗
Estado de autorización (color)					
roja	El lector de sobremesa no está autorizado				
naranja	Las funciones de lectura y escritura de medios están activas (LEGIC)				
verde	Se pueden segmentar medios				

Leyenda

✓ = Propiedad disponible

✗ = Propiedad no disponible

6.3.2 Medios Master

6.3.2.1 Crear Master programador

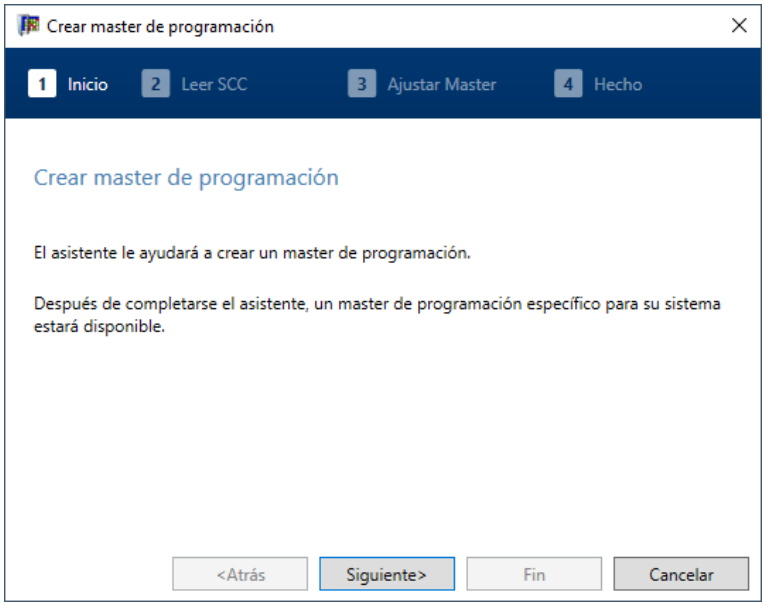
Mediante varios tipos de programación, las autorizaciones de acceso de medios de usuario se pueden transferir a los componentes usando los medios de programación actuales (Master A, Master B y Master T).

- Los Master programadores solo se pueden inicializar en el contexto de la tecnología MIFARE.
- Los Master programadores de la tecnología LEGIC están incluidos en los elementos básicos.

Autorizaciones	**Master**		
	A	**A/B**	**B**
Lista blanca sin cadena de herramientas	--	Recomendado	Posible
Lista blanca con cadena de herramientas	--	Posible	Recomendado
CardLink	Posible	--	Recomendado
Combinación de **CardLink** y **Lista blanca**	Posible	Posible	Recomendado

Procedimiento

1. Abra el espacio "Asistentes" de la barra de funciones "Navegador".
2. Inicie el asistente "Crear Master".



3. Siga el asistente.
4. En el paso 2, coloque la tarjeta de seguridad C en el lector de sobremesa.

5. En el paso 3, coloque el nuevo Master programador A en el lector de sobremesa y rellene el campo "Denominación" del asistente.
6. En el paso 4, pulse el botón "Listo".

6.3.2.2 Master T

El Master temporal (Master T) es una forma especial de medio de programación para componentes autónomos. En un sistema de cierre se pueden usar medios Master temporales. Estos solo son válidos durante un período definido por el usuario y tienen funciones limitadas. Solo es posible utilizar un Master T si los componentes del sistema se han configurado con el programador tras la lectura de la tarjeta de seguridad.

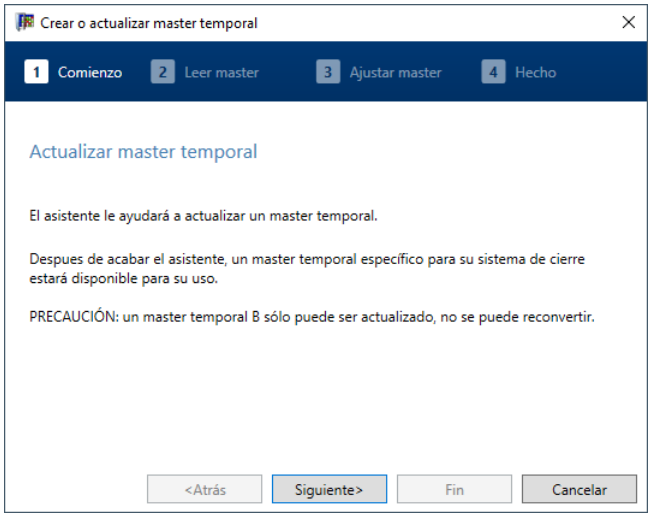
Actualizar Master T

Se debe haber realizado la lectura de la tarjeta de seguridad.

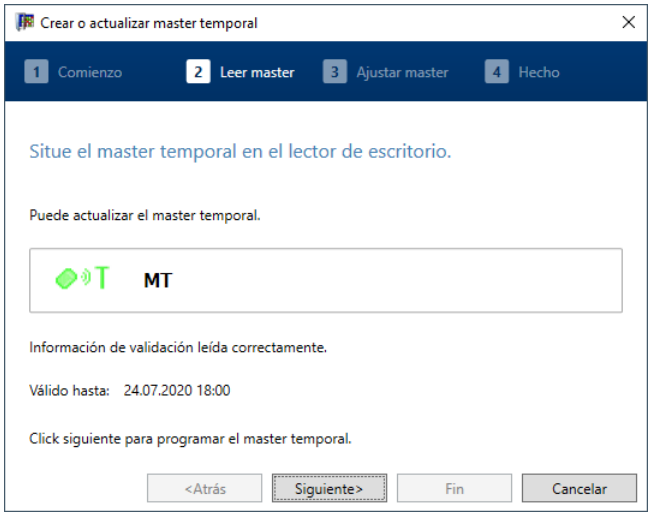
Actualizar un medio Master temporal mediante el asistente.

Un Master T también se puede leer en la sección "Elementos básicos".

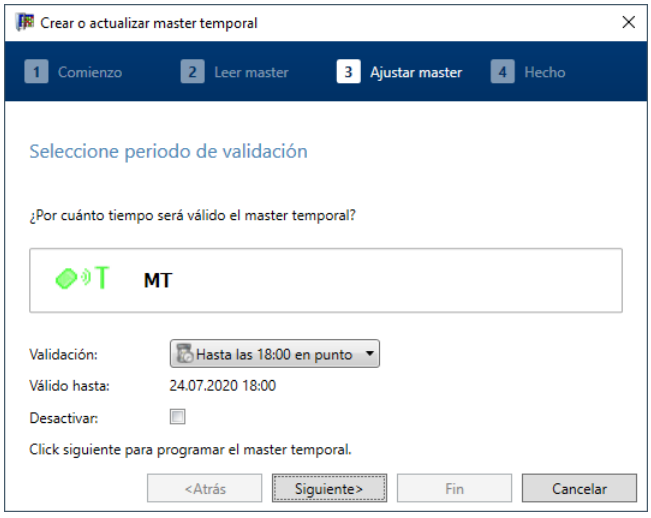
1. Abra el espacio "Asistentes" de la barra de funciones "Navegador".
2. Inicie el asistente "Actualizar Master temporal".



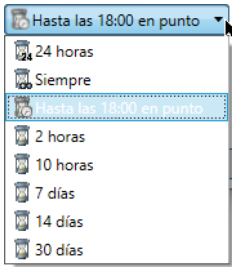
3. Ponga un medio Master T en el lector de sobremesa.



4. Pulse el botón **Siguiente**

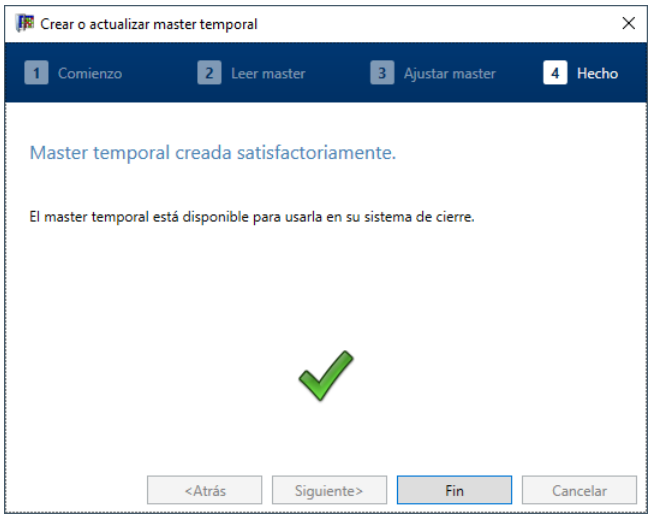


5. Seleccione la duración de la validación



⇨ Tras la selección, aparecerá la caducidad de la validación.

6. Pulse el botón **Siguiente**



⇨ A partir de ahora, el medio es válido como Master hasta que caduque.

7. Finalice el asistente pulsando el botón **Listo**.

6.3.2.3 Usar Master T

Master T para LEGIC:
El software permite definir medios Master T para LEGIC. Un Master T viene derivado de la tarjeta de seguridad y solo se puede usar como medio master temporal.

Master T para MIFARE:
El software permite definir medios Master T para MIFARE. Un Master T viene derivado de la tarjeta de seguridad C.

Los medios Master T para LEGIC y MIFARE poseen las siguientes propiedades:

- Se pueden usar en los dos tipos de autorización CardLink y Lista blanca.
- Pueden actualizar los componentes (los componentes deben estar configurados).
- Pueden ajustar la hora de los componentes.
- Pueden leer la Traceback.

Sistemas MIFARE en funcionamiento de Lista blanca
Indicaciones para usar un Master T de forma posterior.

En los sistemas MIFARE, antes del primer uso de un Master T se debe transferir la Sitekey del sistema a los componentes. En sistemas existentes sin Sitekey, es necesario derivar una Sitekey de la tarjeta de seguridad C y transferirla a los componentes.

Procedimiento para transferir la Sitekey de forma posterior a los componentes de un sistema:

Requisitos previos

- El sistema debe estar registrado en KEM.
- El Master B del sistema debe estar disponible.
- La tarjeta de seguridad C debe estar disponible.

Procedimiento

1. Haga la lectura de la tarjeta de seguridad C del sistema en KEM.
2. Escriba la Sitekey en el Master B del sistema. (Asistente 'Crear Master')
3. Localice los componentes con el Master y transfiera la Sitekey.
4. Actualice la configuración del componente.
   ⇨ La Sitekey se transfiere.
   ⇨ El Master T se puede utilizar.

6.3.3 Programar medios de usuario

- Configurar medios para CardLink Consulte [▸ 6.9.2]

- Configurar medios para Lista blanca Consulte [▶ 6.9.1]
- Preparar medios en Lista blanca para CardLink Consulte [▶ 6.9.2]

Si el tipo de autorización es Whitelist o CardLink y el modo de proyecto es ID de tarjeta, el ID de tarjeta debe asignarse manualmente para los nuevos medios. Esto no puede modificarse posteriormente. Si la Card ID ya está concedida a un medio, aparecerá en el cuadro de diálogo.

6.3.4 Actualizar la configuración de la llave MIFARE DESFire

Descripción
Primero se configura un medio vacío según el concepto ARIOS y luego se programan las aplicaciones y archivos. Después de la programación, no se pueden agregar ni eliminar más aplicaciones sin la llave de mantenimiento de medios, aunque todavía haya espacio de almacenamiento disponible. Este asistente abre los medios para que se puedan programar aplicaciones y datos adicionales sin utilizar la llave de mantenimiento de medios.

Nuevos medios MIFARE DESFire
Los medios MIFARE DESFire nuevos y vacíos se configuran con la configuración de ARIOS durante la autenticación con una llave de sitio ARIOS. Luego se configuran los ajustes de llave para que se puedan programar aplicaciones adicionales (a partir de KEM V 7.0).

Medios MIFARE DESFire ya programados
Para los medios existentes, la configuración de llaves se puede ajustar agregando una aplicación adicional con un archivo vacío y así el medio se puede abrir para aplicaciones adicionales. Esta aplicación adicional nunca se utiliza y luego se elimina nuevamente. Esto da como resultado que se pierda algo de espacio de almacenamiento en los medios. En KEM, este proceso se lleva a cabo mediante un asistente.

La configuración solo se puede ajustar en los medios de usuario MIFARE DESFire.

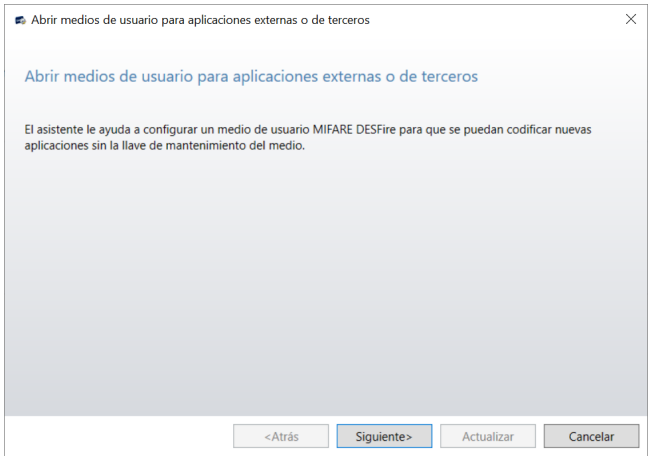
- Los medios deben estar registrados en el proyecto.
- Otros medios serán rechazados y este asistente no los procesará.
- Los medios ya configurados pierden algo de espacio de almacenamiento como resultado del proceso.

Requisitos previos

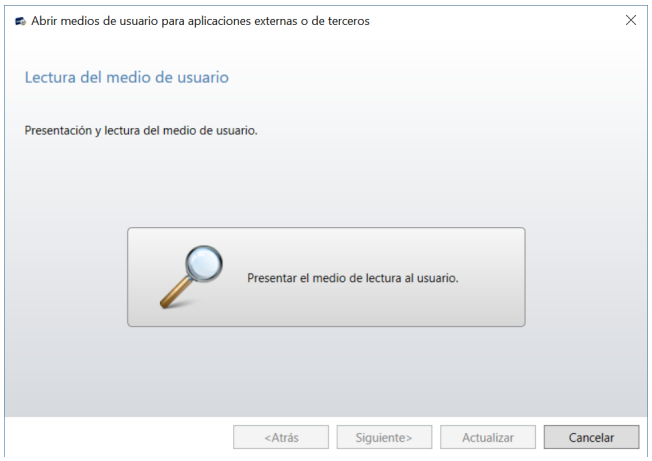
- KEM a partir de V7
- Hay un lector de sobremesa MRD conectado al sistema.
- Proyecto MIFARE
- La tarjeta de seguridad del proyecto se ha leído.
  Si la tarjeta de seguridad no se ha leído, el asistente no es visible y no se puede iniciar.
- El medio de usuario está registrado en el proyecto.

Procedimiento

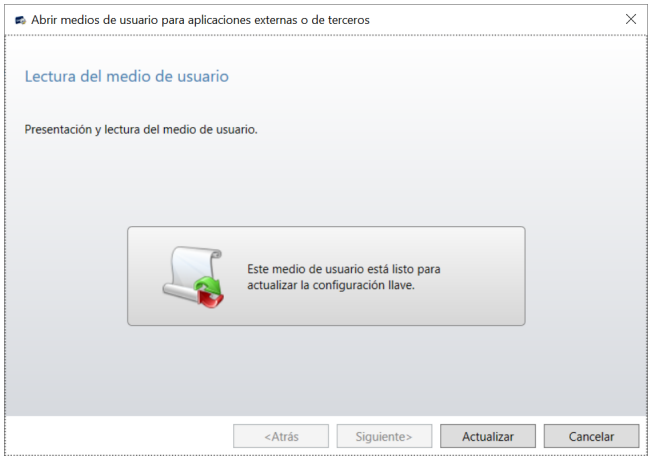
1. Vaya a "Navegador/asistentes".
2. Inicie el asistente "Actualizar configuración de llave MIFARE DESFire".



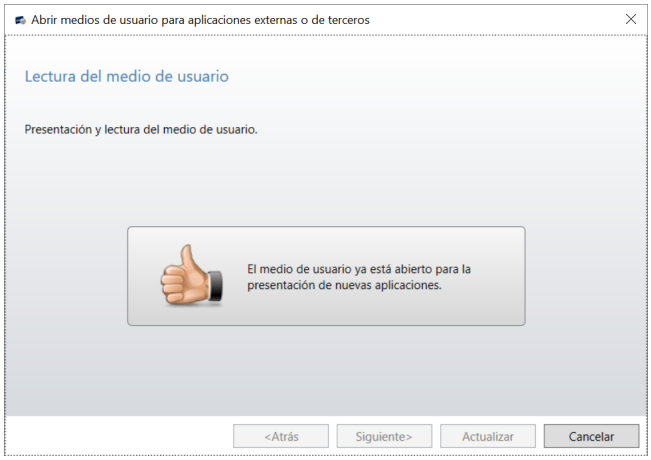
3. Haga clic en "Siguiente".



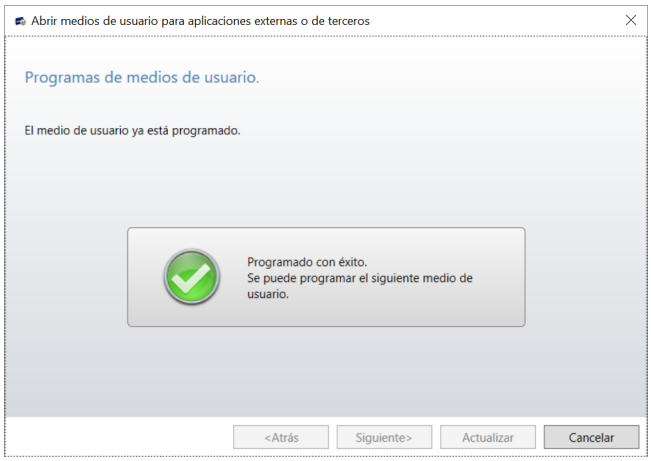
4. Coloque un medio de usuario del proyecto en el lector de sobremesa.



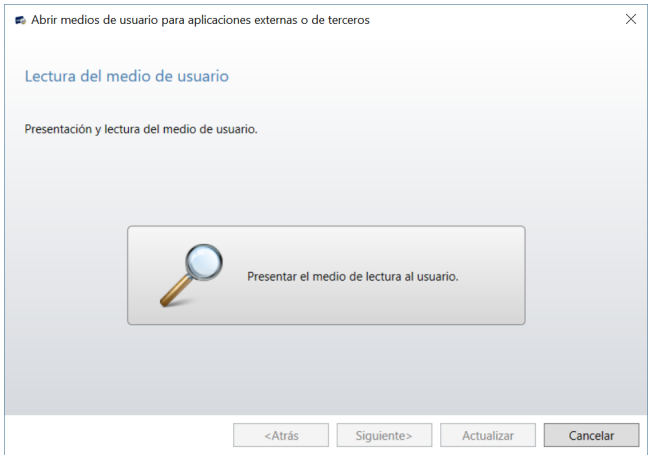
⇨ Si el medio ya está abierto, el asistente lo indicará. En este caso, retire el medio e inserte otro medio de usuario.



5. Haga clic en "Actualizar".
   ⇨ La configuración se ajusta.



6. Retire el medio procesado del lector de sobremesa.
   ⇨ Edite los demás medios repitiendo los pasos 3 a 5.



7. Haga clic en "Cancelar" para finalizar el asistente.

6.4 Perfiles temporales

Con los perfiles temporales se determina cuándo un medio está autorizado para acceder a un componente.

Además de las autorizaciones de acceso básicas, con los perfiles temporales también se limitan las autorizaciones en el tiempo. Los perfiles temporales se configuran en el software KEM y luego se transfieren a los componentes con el programador o de forma inalámbrica.

Los perfiles temporales se pueden asignar a usuarios o a componentes.

Requisito
Todos los elementos con la opción de perfil temporal activa deben tener la fecha y la hora bien configuradas.

Descripción

Autorización Lista blanca	• Con perfil temporal individual. Cada componente cuenta con 15 perfiles temporales disponibles para definir de 12 intervalos temporales (V3/V4) o 4 intervalos temporales (V2) cada uno. Se permiten 7 intervalos de tiempo para perfiles temporales remotos.
	• Con un perfil temporal de funciones TimePro. Perfil temporal Office o perfil temporal Day/Night.
Autorización CardLink	• Con perfil temporal (derecho de Grupos de puertas, derecho individual, reserva). En todo el sistema se pueden usar 15 perfiles temporales editables distintos y 1 perfil temporal fijo.
	• con validación

Se pueden crear 1000 perfiles temporales. Los primeros 16 perfiles temporales están reservados para CardLink y Lista blanca. Todos los perfiles temporales subsiguientes son exclusivamente para la Lista blanca. Se pueden crear 159 perfiles temporales remotos.

El perfil temporal ofrece las siguientes opciones en los detalles del perfil temporal:

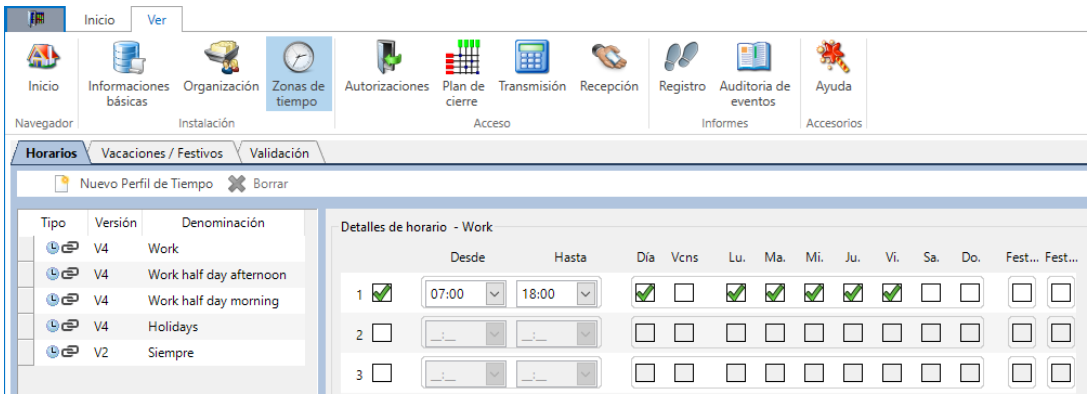
- Período "de" - "a" en combinación con las 2 opciones siguientes:
- "Día" y la selección de uno o varios días de la semana
- Vacaciones o días especiales. Los ajustes de vacaciones y días especiales se llevan a cabo en la pestaña "Vacaciones/días especiales".

Los perfiles temporales remotos no deben contener intervalos temporales que se solapen.

El perfil temporal "siempre" es fijo y no se puede parametrizar ni borrar.

Procedimiento para la parametrización

1. Abra el menú "Perfiles temporales" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Perfiles temporales".
3. Pulse el botón "Nuevo perfil temporal" y registre un nuevo perfil.
4. En el campo "Denominación", introduzca un nombre para el perfil temporal.
5. Para activar los detalles que desee del perfil temporal, active las casillas correspondientes de la fila de opciones.



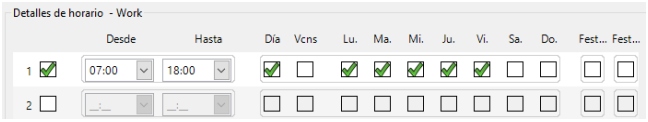
Ejemplo:

1 Solo en días laborables (Lu a Vi)

2 Solo en Vacaciones

3 En días laborables y vacaciones (Lu a Do)

4 En días especiales A, consulte [▸ 6.4.1]



6.4.1 Vacaciones/días especiales

Diferencias en vacaciones/días especiales entre el perfil temporal V2, el V3 y el V4:

Perfil temporal V4	Días especiales A y B
Perfil temporal V3	Días especiales A
Perfil temporal V2	• Día especial A • Ninguna limitación relativa a "Día" en las vacaciones
Perfil temporal remoto	Solo puede utilizarse para actuadores gestionados a distancia. • Se puede definir un máximo de 7 intervalos temporales, que no deben solaparse. • En el gestor de accesos se descargan como máximo los próximos 32 días de vacaciones o especiales del futuro.

Un bloque vacacional activo se superpone a las funciones TimePro seleccionadas.

Al realizar una actualización con el programador, el software siempre adopta las vacaciones y días especiales futuros desde el momento de la actualización.

Perfiles temporales para vacaciones

Los días especiales dentro de un bloque vacacional se superponen al bloque vacacional. El perfil temporal de los días especiales tiene prioridad ante el perfil temporal del bloque vacacional.

Para períodos de días seguidos (p. ej., vacaciones), se puede conceder o retirar la autorización de acceso. La duración de un período se fija introduciendo la fecha inicial y la final. Los componentes con V4 admiten 20 bloques vacacionales, mientras que los componentes con V3/V2 admiten 10. En el perfil temporal V2, los días de vacaciones se fijan con la selección de los bloques vacacionales. No es posible realizar una limitación con el campo de opción "Día".

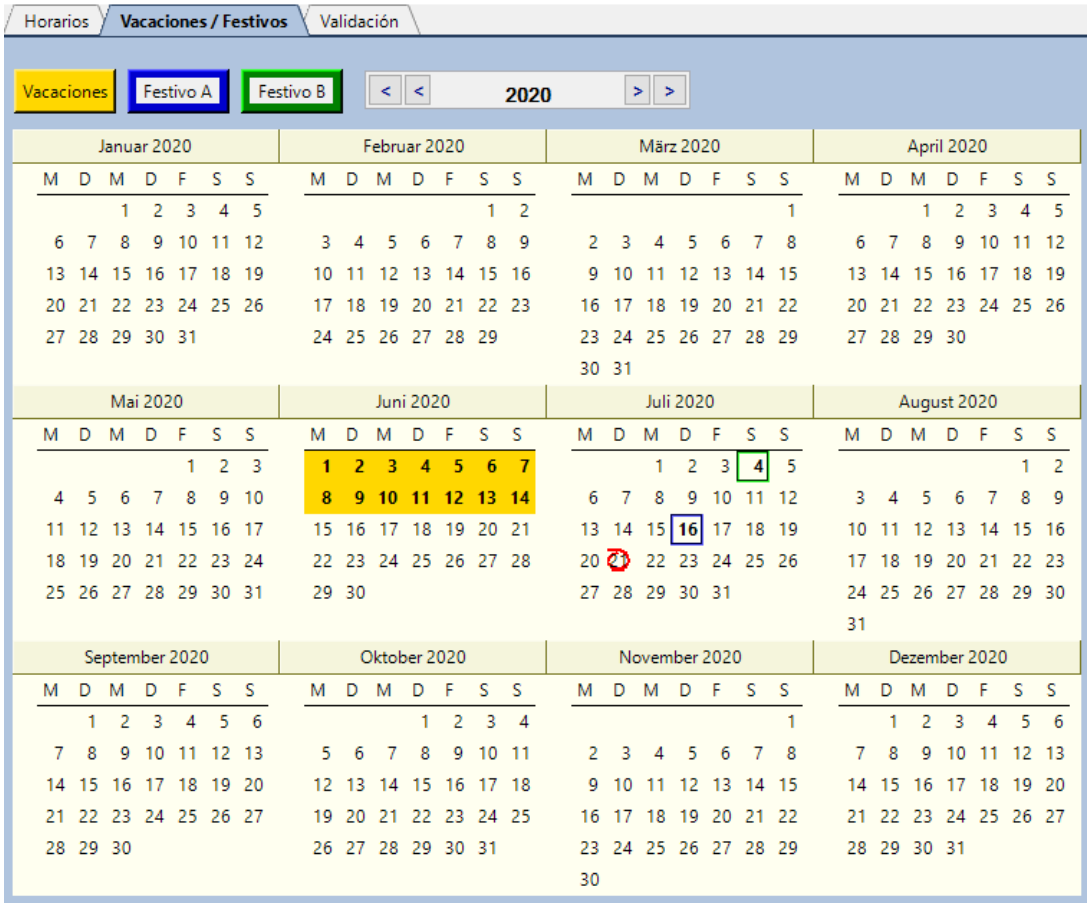
Intervalo temporal para días especiales

Un intervalo temporal individual para los días especiales seleccionados.
Para los días especiales (p. ej., días de vacaciones), en V3 y V4 se pueden fijar 2 días distintos para cada uno: Día especial A y Día especial B. Así se crearán 2 intervalos temporales, p. ej., un intervalo temporal para el día antes de un día festivo (Día especial A) y el día festivo (Día especial B). Para cada uno de los 2 tipos de días especiales se puede consignar un total de 32 días especiales.

Registrar vacaciones

Registrar vacaciones	Marque el área deseada con el botón izquierdo del ratón y pulse el botón "Bloque vacacional".
Registrar festivo (Día especial A y/o B)	Marque el festivo con el botón izquierdo del ratón y pulse el botón "Día especial A" o "Día especial B".
Mostrar bloque vacacional	Vaya con el ratón al bloque vacacional o al día especial registrado y espere a la descripción emergente. En la descripción emergente aparecerán los datos del bloque vacacional.
Mostrar menú contextual	- Vaya con el ratón al bloque vacacional o al día especial registrado. - Abra el menú contextual con el botón derecho del ratón. - Para cambiar el nombre a la entrada, pulse "Cambiar nombre del bloque vacacional". Podrá cambiar el nombre del bloque vacacional o el día especial en la ventana de introducción y llamarlo, por ejemplo, "Vacaciones de verano". El texto

	introducido aparecerá en la descripción emergente, en las propiedades y en el formulario de impresión. - Para borrar la entrada, seleccione "Borrar bloque vacacional".



6.4.2 Validación

La validación solo está disponible en el tipo de autorización CardLink.

Con una autorización CardLink, las autorizaciones de acceso se escriben directamente en los medios de usuario. Para la validación también se escriben un sello temporal y una duración de la validación en los medios de usuario. Un medio de usuario solo se puede validar en un componente que esté configurado para ello.
La validación determina la duración de la validez de un medio. Hay ocho validaciones disponibles. No pueden borrarse ni ampliarse. Sin embargo, 6 de ellas son editables. Consulte [▸ 6.9.2]

Ciclo de funcionamiento posterior:

Transcurrida la duración de la validación, el medio se debe volver a validar. El medio se puede validar de nuevo dentro del ciclo de funcionamiento posterior configurado.

6.5 Componentes

6.5.1 Programar componentes

- Configurar componentes para CardLink Consulte [▶ 6.9.2]
- Configurar componentes para Lista blanca Consulte [▶ 6.9.1]

6.5.2 Función TimePro

Un bloque vacacional activo se superpone a las funciones TimePro seleccionadas.

Ajustar funciones TimePro

Función TimePro	Descripción
Estándar	Sin perfil temporal. La apertura requiere un medio autorizado.
Office	• Dentro del perfil temporal introducido, los componentes pueden ponerse en estado abierto presentando medios autorizados. Presente el medio. En el caso de buzones/ascensores, presente el medio 3 s. El componente hace una breve señal verde. En estado abierto, no hace falta ningún medio. • Si se presentan medios de usuario en estado abierto, los componentes se vuelven a cerrar. Presente el medio. En el caso de buzones/ascensores, presente el medio 3 s. El componente hace una breve señal verde y, a continuación, roja. • Si el perfil temporal ha vencido, los componentes se cierran de forma automática. La apertura requiere un medio autorizado. Fuera del perfil temporal, es necesario un medio autorizado.
Day/Night	El componente se abre y se cierra automáticamente en función del perfil temporal configurado. Fuera del perfil temporal configurado, es necesario un medio autorizado.

Configuración del comportamiento del modo Office

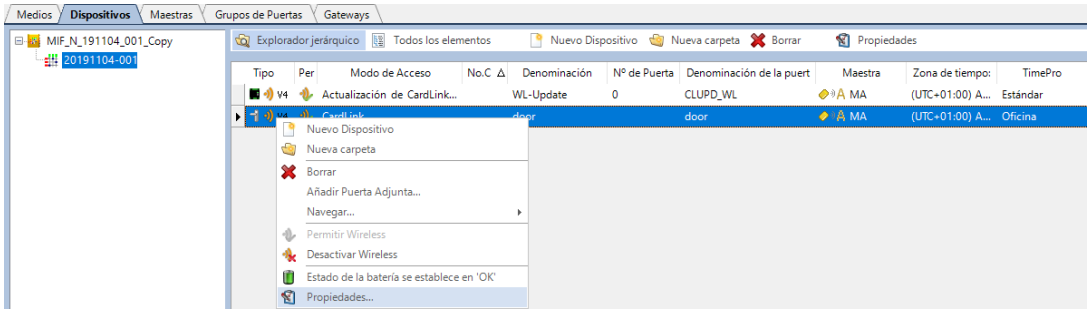
El comportamiento del modo Office se configura en Propiedades de proyecto/General/TimePro. La configuración determina el tiempo durante el cual se debe mantener el medio para la activación/desactivación.

- Estándar: activación/desactivación inmediatas.
- Con retraso: mantenga el medio durante 2 segundos. Solo se aplica a los actuadores E3XX, no a los lectores de PIN o códigos.

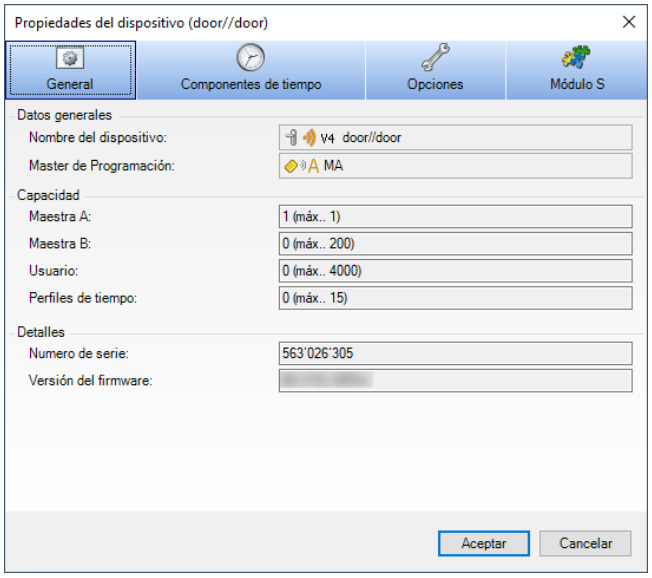
6.5.3 Editar propiedades

La edición de las propiedades está restringida para el lector de códigos PIN.

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".
3. Seleccione todos o algunos de los componentes.
4. Abra el menú contextual.
5. Pulse el botón "Propiedades...".

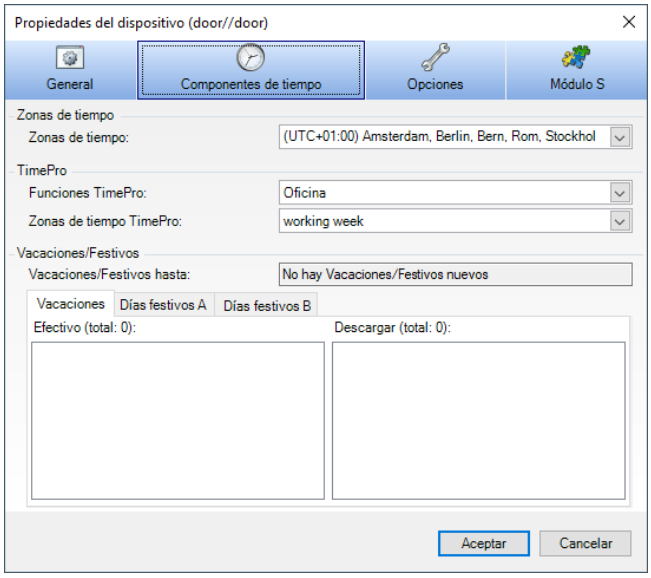


6.5.3.1 Generalidades



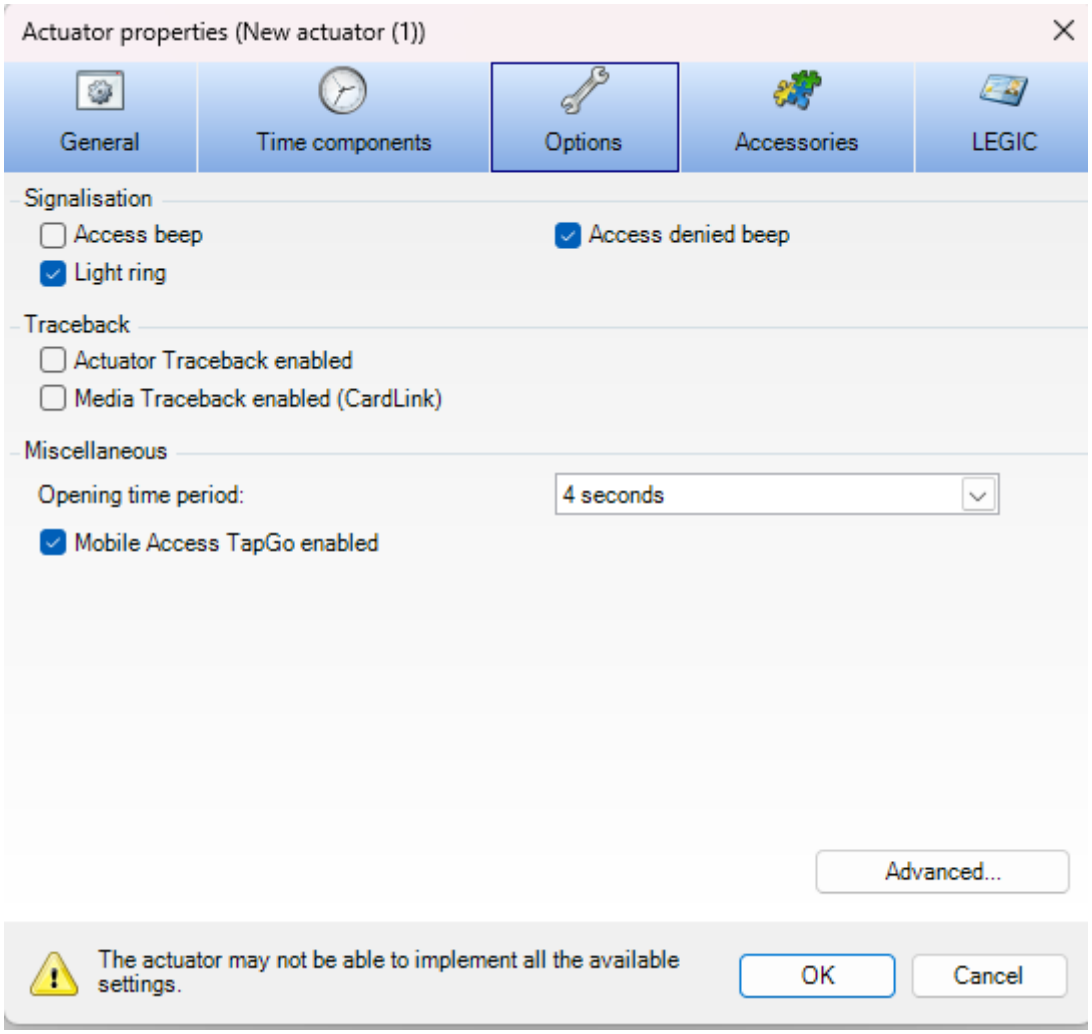
Datos generales	
Nombre del actuador	Denominación detallada del componente
Master programador	El Master programador que tenga asignado este componente.
Capacidad	En este apartado se detallan las entradas y los valores máximos de las entradas.
Master A	Cantidad de Master A asignados (cantidad máxima de Master A asignados)
Master B	Cantidad de Master B asignados (cantidad máxima de Master B asignados)
Usuario	Cantidad de usuarios asignados (cantidad máxima de usuarios asignados)
Perfiles temporales	Cantidad de perfiles temporales asignados (cantidad máxima de perfiles temporales asignados)
Detalles	Los detalles no aparecerán hasta que se haya leído el resultado de la parametrización con el programador o de forma inalámbrica.
Número de serie	El número de serie guardado en el componente
La versión del firmware	La versión de firmware utilizada en el componente

6.5.3.2 Componentes de tiempo



Zona horaria	Ajuste de la zona horaria local
Función TimePro	
Estándar	Ningún perfil temporal preferente guardado en el componente.
Office	• Dentro del perfil temporal configurado, los componentes pueden ponerse en estado abierto presentando medios autorizados. • En estado abierto, los componentes se cierran si se presenta un medio de usuario. • Al final del período configurado, los componentes se cierran automáticamente.
Day/Night	Con el perfil temporal se determina el tiempo durante el cual los componentes se encuentran en estado abierto. El componente se abre y se cierra automáticamente en función del perfil temporal configurado.
Perfil temporal TimePro	Si "Office" o "Day/Night" está seleccionado como función TimePro, seleccione un perfil temporal.
Vacaciones/días especiales	El perfil muestra las vacaciones y los días especiales actuales y los descargados.

6.5.3.3 Opciones



Los elementos en esta ventana tienen las siguientes funciones:

Opción	Descripción
Bip de autorización	Activa o desactiva la señal acústica para el acceso autorizado.
Anillo luminoso	Activa o desactiva la señal óptica.
Bip de no autorización	Activa o desactiva la señal acústica para el acceso no autorizado.
Traceback del actuador activa	La Traceback se escribe en la memoria del componente. [▶ 6.1.1]
Traceback de los medios activa (CardLink)	Si la opción está seleccionada en las propiedades de proyecto, la Traceback se escribe en la memoria del componente y en el medio [▶ 6.1.1].
Duración de la apertura	El mecanismo de apertura está abierto durante este tiempo.
Potencia de transmisión del actuador	Solo cuando el uso inalámbrico está activado: selección de la potencia de transmisión del componente. Las opciones son: Potencia de transmisión alta Potencia de banda normal Potencia de transmisión baja Seleccione la potencia de transmisión que permita alcanzar la gateway de forma segura. Esta función afecta al consumo de energía del componente. Si reduce la potencia de transmisión al nivel necesario para alcanzar la gateway, los componentes autónomos podrán ahorrar energía.
Avanzado	Opciones avanzadas: • Intervalo Object In Field

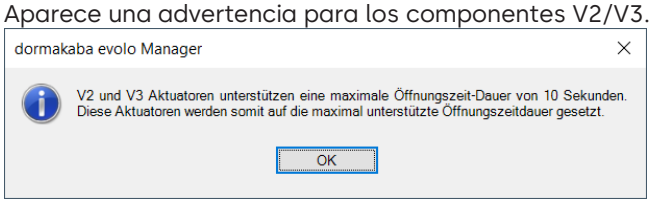
	• Bolt Recreation Time

Recomendamos desactivar el sonido para el estado "Autorizado". Esto reduce el consumo de energía. Este sonido está desactivado por defecto en todos los componentes, excepto en los cilindros mecatrónicos.

Duración de la apertura
Se refiere al período de tiempo en el que el mecanismo de apertura del componente está activo. Los tiempos ajustables son los mismos para los componentes V2/V3 y V4 así como para las tecnologías disponibles.

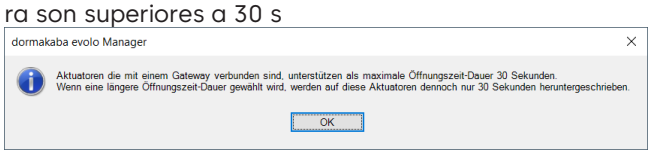
Seleccione la duración de la lista.

En el caso de los componentes V2/V3, se puede seleccionar un máximo de 10 segundos.
Con una selección múltiple de componentes V2/V3 y V4, todos los tiempos están disponibles para su selección. Los componentes V2/V3 se establecen en 10 segundos si el valor seleccionado es mayor.
Aparece una advertencia para los componentes V2/V3.

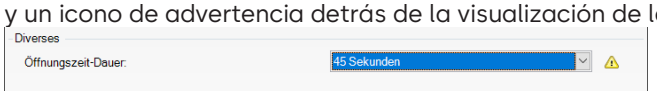


La gateway inalámbrica no puede transmitir tiempos de apertura superiores a 30 s.

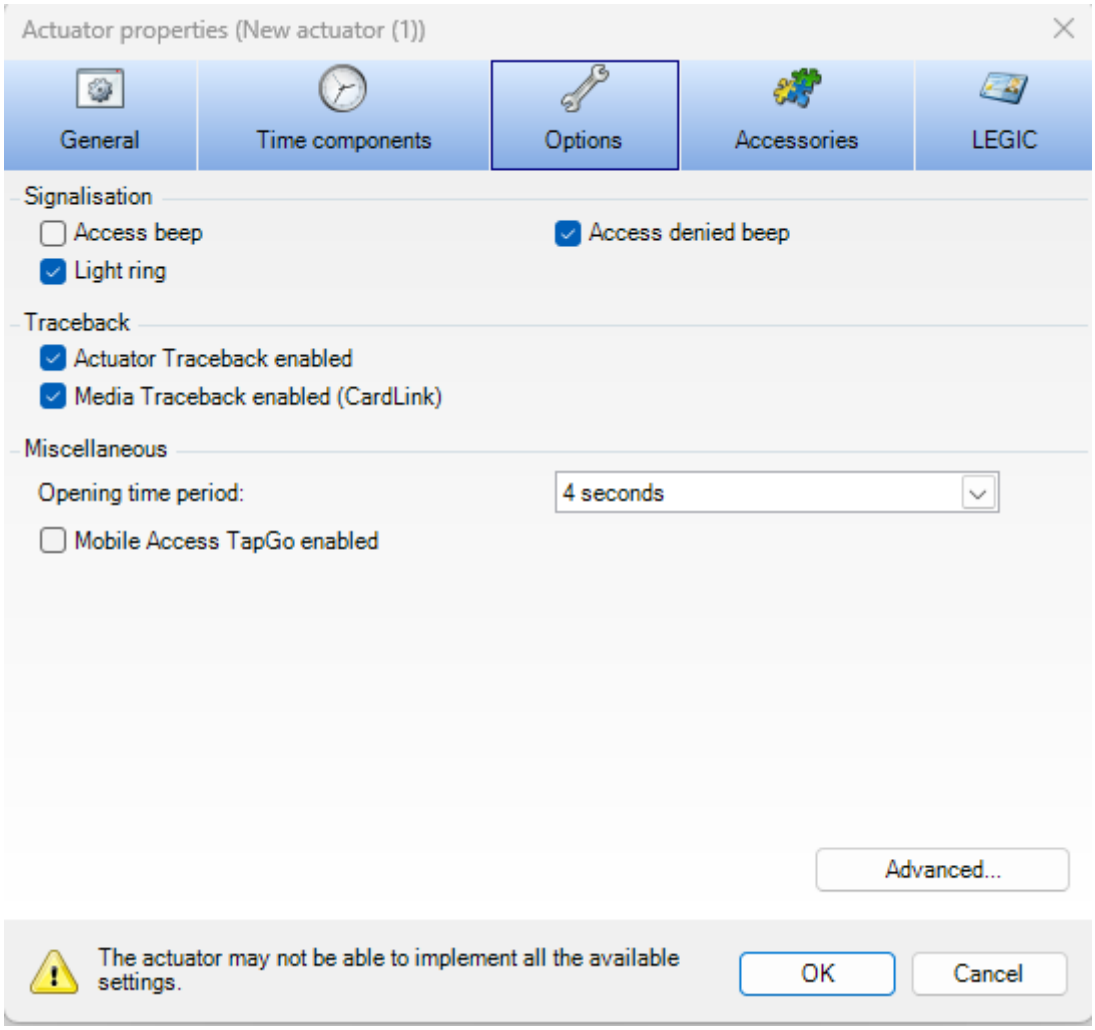
- En el KEM, aparece una ventana emergente con una advertencia si los tiempos de apertura son superiores a 30 s



y un icono de advertencia detrás de la visualización de la hora seleccionada.



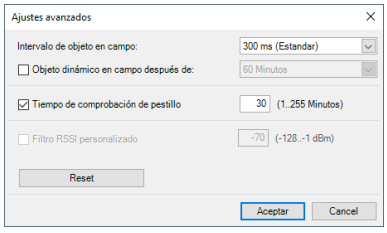
Lector de actualizaciones de CardLink
La casilla solo aparece en esta ventana si el componente seleccionado está parametrizado como Lector de actualizaciones de CardLink.



6.5.3.4 Avanzado

Intervalo Object In Field (OIF):
Esta opción solo está disponible para componentes V4.

El componente comprueba a intervalos regulares si hay algún medio en el campo de la antena. Para ahorrar energía se alarga el tiempo entre dos comprobaciones. Si selecciona "Object In Field" dinámico, el tiempo se va ampliando gradualmente hasta llegar al valor máximo. Si se presenta un medio, el proceso vuelve a empezar. Es posible aumentar el tiempo de reacción al presentar un medio.



Configurar el OIF:

1. Escoja el valor del intervalo en el menú de selección.
2. Pulse el botón "OK".

Configurar el OIF dinámico:

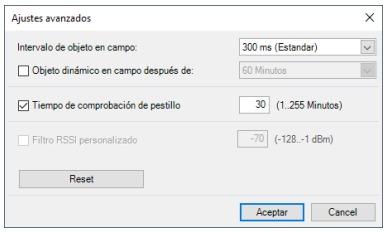
1. Marque la casilla "Object In Field dinámico".
2. Escoja el valor inicial del intervalo en el menú de selección.
3. Seleccione el tiempo de inicio.
4. Pulse el botón "OK".

Para que el OIF dinámico sea efectivo, entre dos procesos de lectura debe haber tiempos de pausa más largos.

Tabla: Ahorro de energía gracias al OIF dinámico. Los valores son orientativos. El ahorro energético real depende de más factores y ajustes.

Aplicación	Ajustes		Ahorro	Efectos
Ejemplos	**OiF Intervalo**	**Din. OiF**	**máximo**	
Configuración estándar del componente. **Accesos muy frecuentados**	300 ms	APAGADO	0 %	Normal
Accesos poco frecuentados	300 ms	ENCENDIDO 30 min	15 %	Tiempo de reacción más largo en el primer medio presentado después de una pausa larga. Con otros medios, dentro del período configurado el tiempo de reacción será normal.
• 20 procesos por la mañana y 20 por la tarde dentro del período configurado. Entre ellos, 1 proceso por hora durante 10 horas.	300 ms	ENCENDIDO 30 min	19 %	
• 1 proceso por hora durante 10 horas	300 ms	ENCENDIDO 30 min	22 %	
Accesos de uso ocasional • 2 procesos por la mañana y 2 por la tarde dentro del período configurado. Entre ellos, ningún proceso.	300 ms	ENCENDIDO 30 min	30 %	Tiempo de reacción más largo en el primer uso tras una pausa larga. • La lectura de un medio presentado puede tardar hasta 1 s.
• Pausas más largas entre procesos • un día o más sin ningún proceso	1000 ms	APAGADO	34 %	

Bolt Recreation Time
Con "Bolt Recreation Time" se define con qué intervalos temporales debe comprobarse el estado de acoplamiento de la unidad mecatrónica.
Esta función no está disponible en todos los dispositivos.



Configurar el Bolt Recreation Time:

1. Marque la casilla.
2. Escoja el tiempo en el menú de selección.
3. Pulse el botón "OK".

Restablecer
Pulse el botón 'Restablecer': Los valores de esta ventana se restablecerán a los valores por defecto.
Los valores estándar son:

- Intervalo Object In Field: 300 ms
- Object in Field dinámico: desactivado
- Bolt Recreation Time: 30

6.5.3.5 Accesorios

En función del tipo de componente, en Accesorios se pueden seleccionar diferentes opciones como el Módulo S o Pass-Lock (solo para c-lever y c-lever pro). Encontrará información sobre la función "escape return" en la breve guía "Kaba c-lever escape return (k1evo818xy".

6.5.3.5.1 Módulo S

El módulo S es compatible con una conexión inalámbrica (consulte el capítulo [▸ 11.2.3] para conocer los requisitos).

Ejemplo de una clínica:
Durante el horario de atención, los pacientes deben poder acceder a la clínica. La puerta principal se puede desbloquear para los pacientes con un pulsador. De esta forma, los pacientes no necesitan ningún medio y pueden entrar en la clínica.

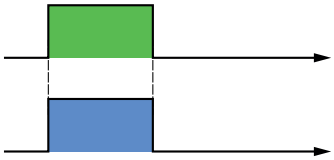
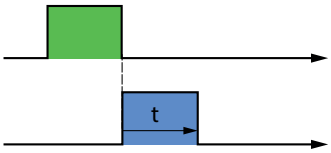
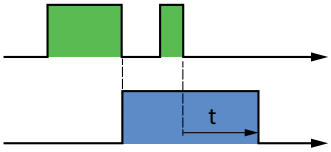
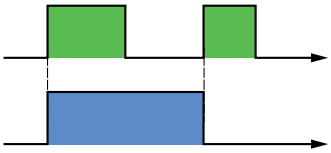
6.5.3.5.1.1 Modo de funcionamiento del portero automático con funcionalidad de módulo S

El contacto conectado a la entrada digital permite modificar el comportamiento de . El contacto anula las autorizaciones y activa el comportamiento programado en dormakaba evolo Manager o Kaba exos.

Posibles contactos: conmutadores, temporizadores o sistemas de control a nivel de edificio (p. ej., equipo de alarma)

Comportamiento elegible en dormakaba evolo Manager o Kaba exos

"Activo si:"

La entrada está activa	Si la entrada está activa (verde), el comportamiento programado está activo (azul).	
Limitación temporal	La medición de la duración temporal empieza con la desactivación de la entrada.	
	Si la entrada se vuelve a activar antes de que transcurra la duración configurada, el comportamiento programado se extiende.	
Modo de funcionamiento por impulso	La activación del primer flanco de la entrada hace que se active el comportamiento programado. La activación del siguiente flaco hace que se desactive el comportamiento.	

Leyenda

Entrada activa (verde)

Comportamiento programado activo (azul)

"Si activo:"	Efecto
Siempre abierta	Siempre abierta
Siempre cerrada	Siempre cerrada, no es posible acceder
Apertura con cualquier medio	Se puede abrir con cualquier medio (escribe el UID del medio en la Traceback)
Apagar TimePro	TimePro se desactiva

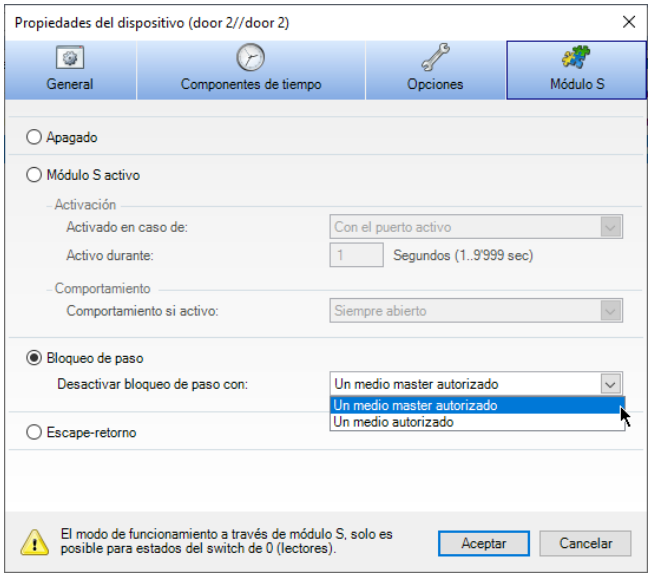
Definir la lógica
La funcionalidad Módulo S está dotada de una función de autoaprendizaje. Al inicializar (restablecimiento INI) , se interpretará la posición determinada del contacto como posición de salida. Si cambia la posición del contacto, se activa el comportamiento programado en "Activación". Permite definir un contacto de cierre o de apertura.

6.5.3.5.2 Pass-Lock

Para la opción Pass-Lock, escoja las siguientes propiedades de la lista:

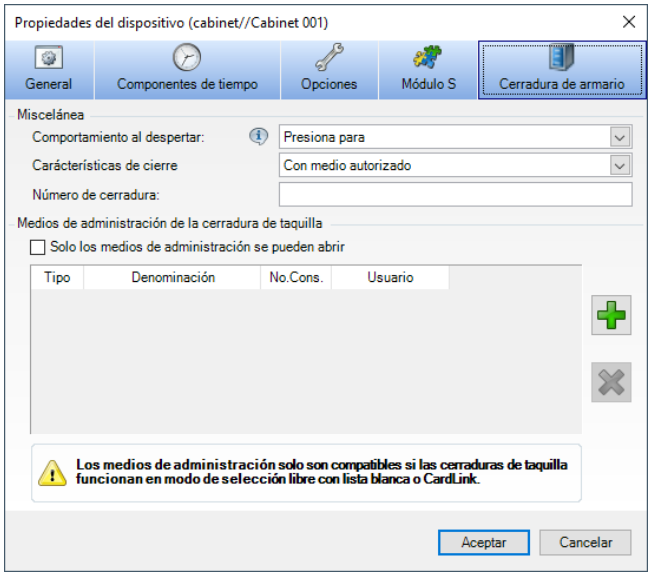
- Medio master autorizado
- Medio de usuario autorizado

El tipo de medio que seleccione aquí le permitirá volver a abrir desde fuera la puerta parametrizada de esta forma tras activar Pass-Lock. La puerta siempre se podrá abrir desde dentro.



6.5.3.6 Cerradura de armario 21 10

Estas propiedades solo se pueden parametrizar para una cerradura de armario 21 10.



En esta ventana se puede parametrizar lo siguiente:

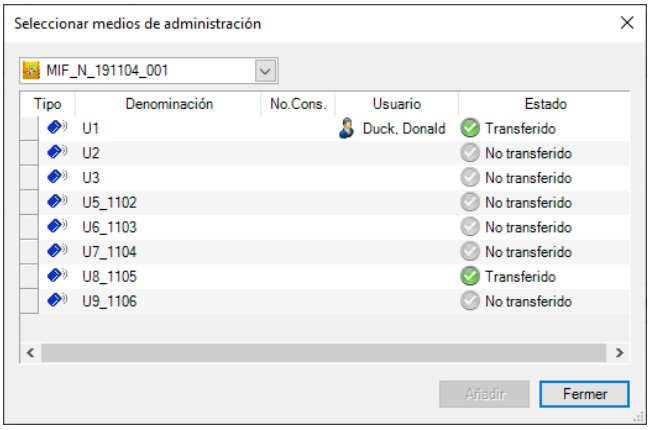
- Comportamiento de activación:
  a) Presionando: para activar la electrónica y establecer la capacidad de lectura, presione la puerta brevemente. Si después se presenta un medio, se comprobará la autorización.
  b) Object in Field: La cerradura de armario comprueba periódicamente si hay algún medio en el campo de la antena. Cuando un medio se encuentre en el campo de la antena, se leerá y se comprobará la autorización.
- Comportamiento de cierre:
  a) Con medio autorizado: el armario solo se puede abrir o cerrar con un medio autorizado.
  b) Sin medio: el armario se cierra presionando su puerta.

- Número de cerradura de armario:
  El número del armario en el que se encuentra la cerradura.

  Es posible emitir el mismo número varias veces si, por ejemplo, los armarios están en zonas distintas de un edificio.
  Este medio tiene asignado un UID o CID único almacenado en su memoria. Durante el proceso de cierre, este UID o CID se almacena en la cerradura y, por tanto, se asigna a este armario. Entonces, el armario solo podrá abrirse utilizando el mismo medio. En el caso de los números de cerraduras de armario otorgados para más de un armario, el UID o CID del medio de cierre será la marca individual de cada cerradura.

  El número de cerradura del armario quedará registrado en el medio durante el proceso de cierre. Si no está otorgado (campo vacío), se registrará el número de serie de la cerradura del armario.

- Medios de administración:



  Si la casilla está marcada, los medios de administración parametrizados solo pueden abrir un armario y no pueden cerrarlo.
  Los medios de administración se añaden y se eliminan desde el menú contextual y a través de los dos botones del lateral derecho.

6.5.3.7 Buzones/ascensores

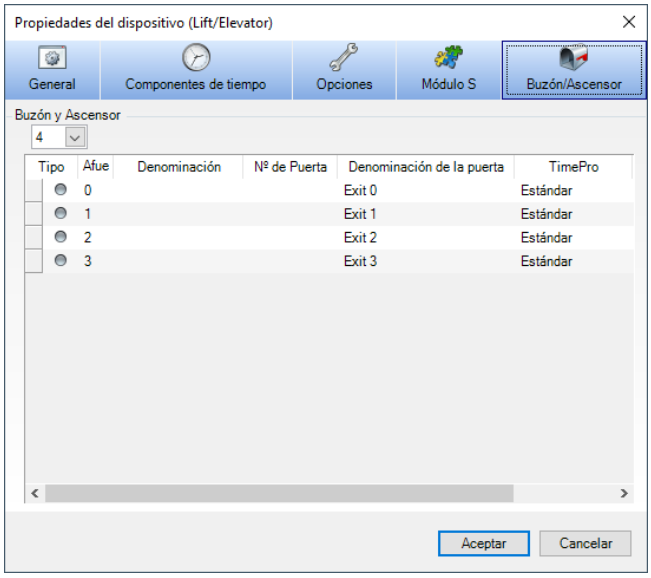
El medio de usuario solo permite ir en ascensor a las plantas o abrir los buzones para los cuales el usuario tenga autorización.

Solo es compatible con la Lista blanca. El uso de CardLink no es posible.
En la Lista blanca (UID/Card ID) se puede configurar un máximo de 1000 usuarios para buzones/ascensores.

El hardware y firmware adecuados permiten usar Mobile Access con Bluetooth.
Esto se puede configurar de forma normal en el KEM.

Crear pisos/buzones

En el menú de selección (0..49), escoja el número de pisos/buzones que necesite.
Puede crear un máximo de 49 pisos/buzones.



Configurar pisos/buzones

- Out
  Número de salidas físicas del componente.
  La salida "0" se encuentra en el dispositivo básico y las demás salidas (1..8), (9..16), etc., están en los módulos adicionales.
  (Una vez configurado, no se puede modificar)
- Denominación
  Introduzca una denominación para este elemento. P. ej.:
  Buzón: "Familia Müller"
  Ascensor: "Salida" o "1.er piso"
- N.º de puerta:
  Elemento de ordenación numérica dentro de un sistema de cierre.
- Denominación de puerta
  Denominación del elemento dentro del sistema de cierre.
- TimePro
  Ajuste de la función TimePro
  Las funciones específicas se describen en el capítulo "TimePro" [▶ 6.5.2].
- Perfil temporal TimePro
  Si "Day/Night" u "Office" está seleccionado, escoja un perfil de la lista. Para crear perfiles temporales, consulte el capítulo "Perfiles temporales".
  En el perfil "Office", presente el medio durante 3 segundos para conectar las salidas.

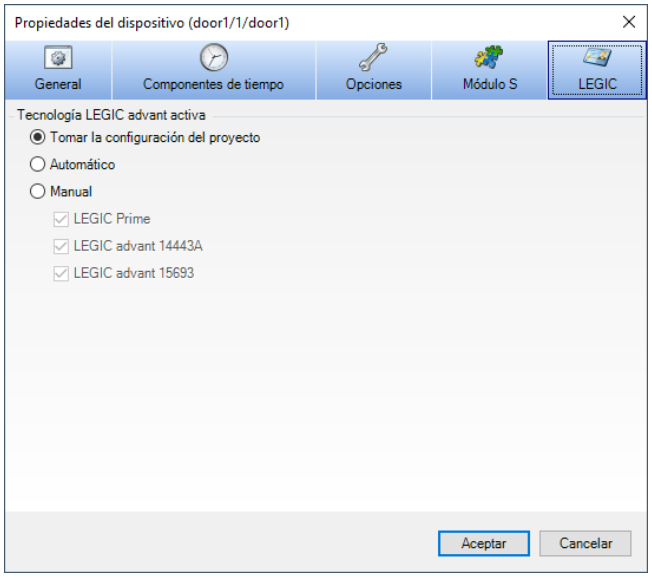
Relación de salidas y los componentes necesarios:

Número de salidas	Número de componentes
1	91 15 (lector remoto con 1 relé de salida)
hasta 9	91 15 + 1 x 90 30 (módulo de ampliación con 8 relés de salida)
hasta 17	91 15 + 2 x 90 30
hasta 25	91 15 + 3 x 90 30
hasta 33	91 15 + 4 x 90 30
hasta 41	91 15 + 5 x 90 30
hasta 49	91 15 + 6 x 90 30

6.5.3.8 LEGIC

Tecnología LEGIC
La tecnología Legic se puede seleccionar en las propiedades de proyecto. El componente tiene otra opción más de selección a disposición.

Estas son las configuraciones posibles:



- Adoptar configuración del proyecto
  El componente utiliza la configuración extraída de las propiedades del proyecto. El lector de códigos PIN asume las propiedades del gestor de accesos.
- Auto
  La tecnología se selecciona automáticamente.
- Manual
  Es posible seleccionar una o varias tecnologías.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

1. En el caso de elementos básicos/actuadores, seleccione las propiedades del actuador haciendo clic en el botón derecho del ratón.
2. En las propiedades, seleccione la pestaña LEGIC.
3. Seleccione la tecnología.
4. Seleccione OK.

El componente utiliza la tecnología seleccionada. Los medios que no utilicen la tecnología seleccionada no se reconocerán y se ignorarán.

6.5.4 Comprobar el estado de la batería

Los componentes con batería CR2 (p. ej., los cilindros digitales) solo muestran el estado de batería "ok" o "BatLow".

Puede comprobar el estado de la batería de los componentes en la siguiente situación:

- Está en un entorno inalámbrico.

  Si consulta el estado de la batería mediante el software del sistema, la información se enviará a la gateway.
- Con el programador 1460 (directamente en el componente).

  El estado de la batería se puede leer en el programador abriendo el menú "Información del actuador". Si se leen datos de Traceback y el programador está conectado con KEM, encontrará el estado de la batería en la línea de información de los componentes, en la pestaña "Actuadores".
- En un entorno CardLink.

  El estado de la batería del componente se transfiere junto a los datos de auditoría del medio de usuario.

6.5.5 Migrar componentes con V3 a V4

Las funciones ampliadas perfil temporal V2, TimePro "Day/Night drive" y Módulo S dejarán de ser compatibles tras la migración.

Requisitos previos

- Los componentes de hardware deben admitir V4.
- Los medios Master para V4 deben estar registrados en el proyecto.
- Los perfiles temporales para V4 deben estar registrados en el proyecto.
- Solo se pueden adoptar los perfiles temporales compatibles.
- Las propiedades y funciones se deben transferir a V4 con las mismas propiedades y funciones.
- Las demás autorizaciones se deben mantener.

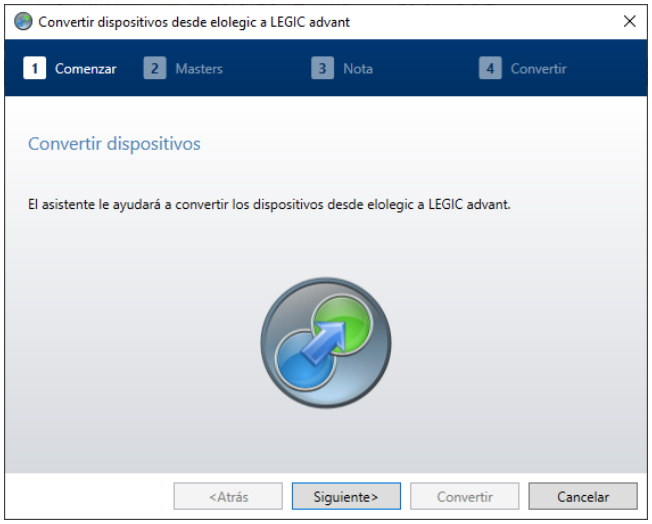
Migración con el menú contextual

La migración no se puede deshacer.
Recomendamos hacer una copia de seguridad del proyecto existente antes de realizar una migración.

1. Abra el menú "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".
3. Seleccione todos o algunos de los componentes.
4. Abra el menú contextual.
5. Seleccione la entrada del menú "Migración, de elolegic a LEGIC advant".

No se pueden migrar todos los componentes ni tampoco componentes individuales. Así, p. ej., los cilindros elolegic **no** se pueden convertir en cilindros digitales ni en c-lever.

6. Siga el asistente.
   El número de pasos depende del tipo de componente.



7. Tras la migración, pulse el botón "Cerrar".

6.6 Grupos de puertas

Registrar grupos de puertas hace que gestionar las autorizaciones de puertas sea más fácil.

Los grupos de puertas solo están disponibles en el tipo de autorización CardLink.

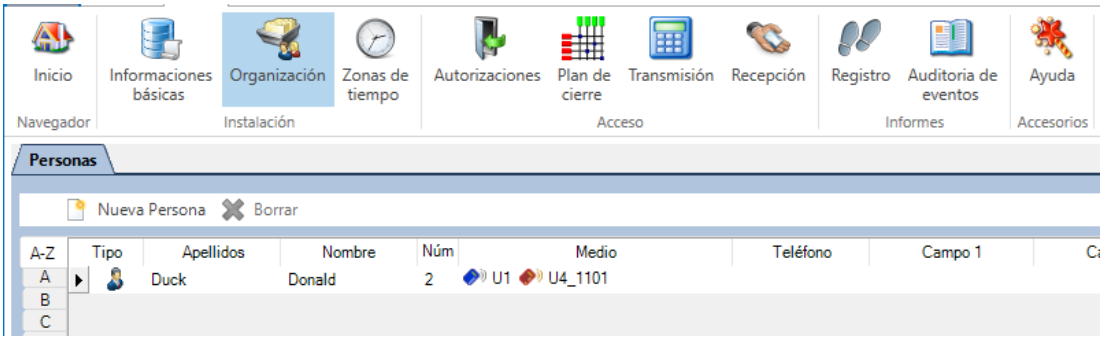
6.7 Personas

Crear varias personas con el mismo nombre puede generar problemas si se va a borrar el nombre de una persona.

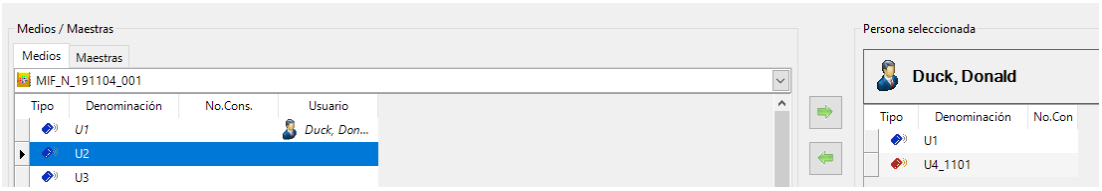
- En este caso, si hay varias personas con el mismo nombre, los nombres de todas estas personas se borrarán del libro de registro, de la lista de auditoría y del Traceback.

Para la gestión de medios, se crea una lista de personas con los medios que tiene asignados cada una.

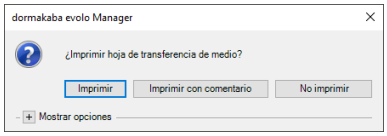
1. Abra el espacio "Organización" de la barra de funciones "Navegador".
2. Registre un nuevo usuario pulsando el botón "Nueva persona".



3. Asignar medios a las personas de la lista:
   -- La persona a la que quiere asignar un medio está marcada en la lista y su nombre aparece en la parte inferior derecha.
   -- Mueva de izquierda a derecha el medio seleccionado con la flecha (del medio) o desplácelo de izquierda a derecha con el método de arrastrar y soltar.



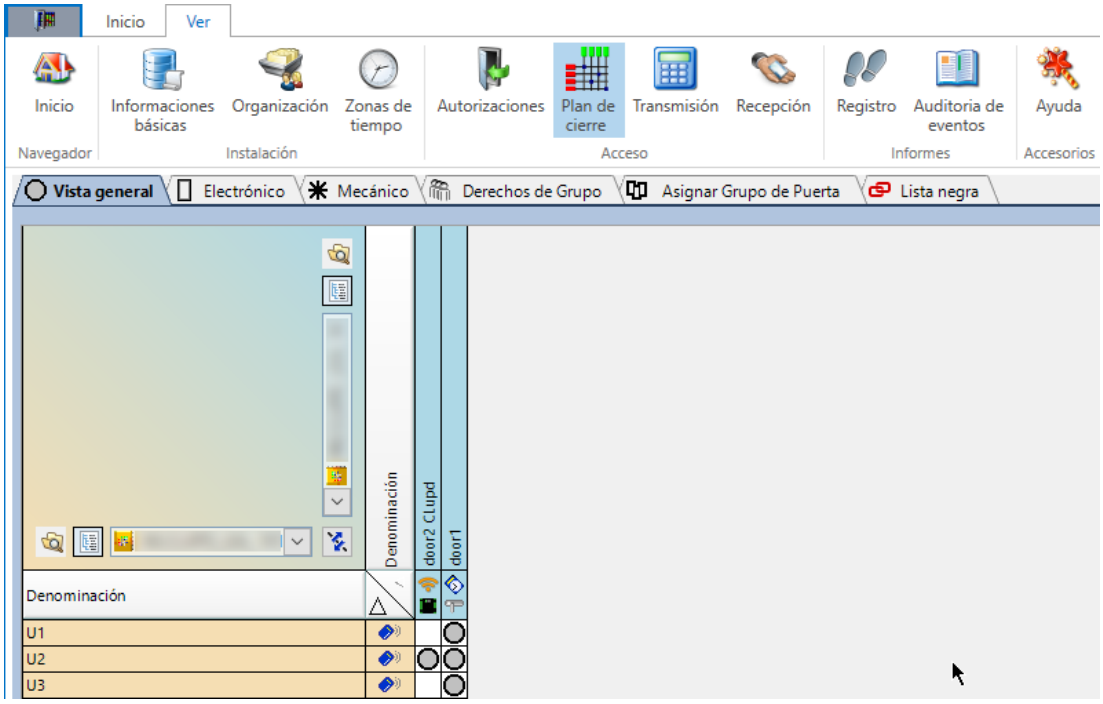
4. En el cuadro de diálogo de impresión, seleccione si el formulario de emisión se debe imprimir con o sin comentarios.



6.8 Plan de cierre

Las autorizaciones se representan de forma clara en la matriz de un plan de cierre.

Mediante el menú contextual de un punto de red podrá activar la función "Exportar plan de cierre a Excel". El plan de cierre se exportará como archivo Excel.



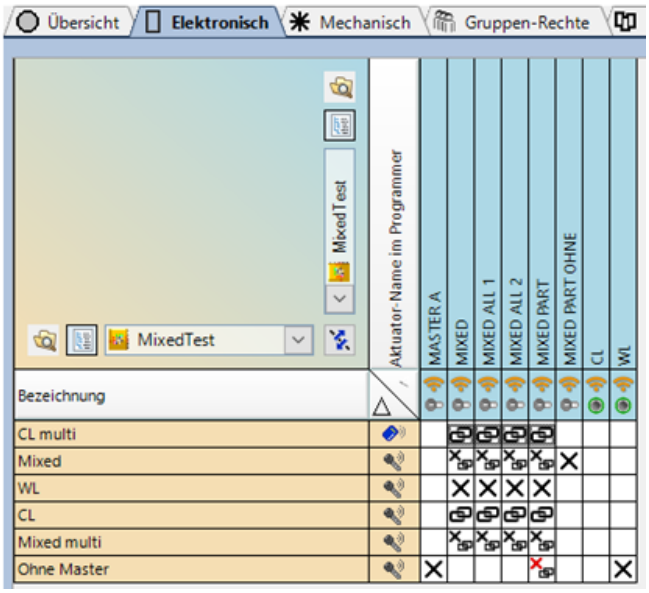
Resumen	• Autorizaciones de todos los medios en los componentes • Autorizaciones en los componentes mecánicos • No se puede editar.
Electrónico CardLink/Lista blanca	• Autorizaciones de los medios electrónicos en los componentes • Se puede editar.
De forma mecánica	• Autorizaciones en los componentes mecánicos • Se puede editar.
Derechos de grupos (CardLink)	• Autorización de grupos de puertas de los medios electrónicos • Se puede editar.
Asignación de grupos de puertas (CardLink)	• Asignación de grupos de puertas de los medios electrónicos • Se puede editar.

Explicación de los símbolos en la matriz:

Símbolo	Descripción
○	Autorización concedida La pestaña "Resumen" le mostrará si una autorización está concedida.
✳	Autorización mecánica La pestaña "Mecánica" le mostrará si una autorización está concedida.

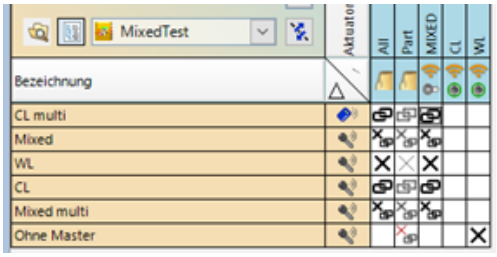
Cuando pasa el ratón sobre un icono, se muestran sugerencias sobre herramientas con los valores del punto en la matriz de permisos.

Plan de cierre electrónico 1:1



Símbo-lo	Descripción
	Sin autorización
	Autorización de Lista blanca establecida.
	Autorización de Lista blanca establecida, falta el Master B.
	Autorización de Lista blanca y CardLink establecida (posibilidad de realizar múltiples reservas).
	Autorización de Lista blanca establecida sin Master B y autorización de CardLink establecida (posibilidad de realizar múltiples reservas).
	Autorización de CardLink establecida.
	Múltiples reservas establecidas (al menos 2).

Plan de cierre electrónico n:n



Símbo-lo	Descripción
	Sin autorización
	Autorización de Lista blanca establecida
	Autorización de Lista blanca parcialmente establecida
	Autorización de Lista blanca establecida, falta el Master B.

Símbo-lo	Descripción
	Al menos una autorización de Lista blanca sin Master B.
	Autorización de Lista blanca y CardLink (posibilidad de realizar múltiples reservas)
	Autorización de Lista blanca y CardLink y/o modo mixto parcialmente establecida.
	Autorización de Lista blanca sin Master B y autorización de CardLink (posibilidad de realizar múltiples reservas)
	Al menos una autorización de Lista blanca sin Master B. Autorización de Lista blanca y CardLink y/o modo mixto parcial
	Autorización de CardLink establecida.
	Múltiples reservas efectuadas (al menos 2).

6.9 Autorizaciones

El software KEM permite distintas estructuras de autorizaciones. Se distingue entre el tipo de autorización CardLink y el tipo de autorización Lista blanca.

Autorización CardLink	Las autorizaciones de acceso están guardadas en los medios.
Lista de bloqueo (CardLink)	Si quiere bloquear un medio de usuario que esté en su período de validez, lo debe registrar en la Lista de bloqueo. De esta forma revocará la autorización del medio de usuario en cuestión.
Autorización Lista blanca	Una lista blanca es el conjunto de medios registrados en la memoria del componente con autorización para el componente o el gestor de acceso.
Elección de armario libre con Lista blanca	Esta función solo se puede configurar para la cerradura de armario 21 10.
Elección de armario libre con CardLink	Esta función solo se puede configurar para la cerradura de armario 21 10.

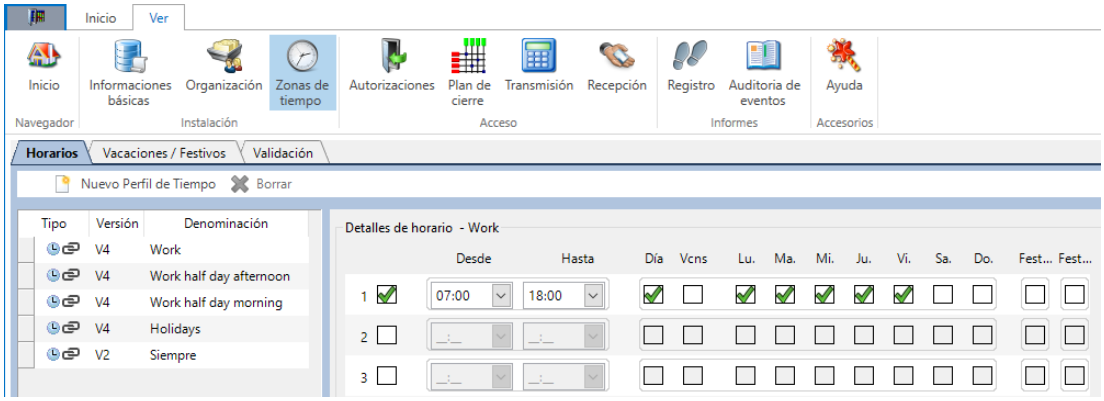
Aviso: cualquier modificación de un perfil temporal se debe transferir a los componentes mediante un programador o de forma inalámbrica. [▸ 6.10]

6.9.1 Configurar autorización Lista blanca

Los requisitos previos y la información general sobre el gestor de acceso se encuentran en el capítulo Gestor de acceso.

Configurar perfiles temporales

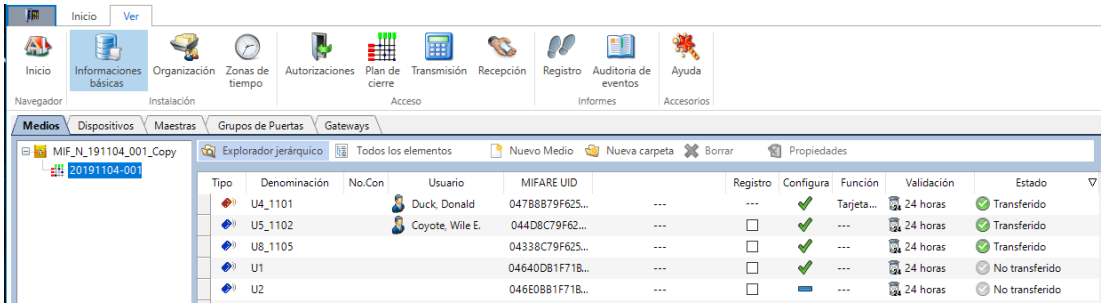
1. Abra el espacio "Perfiles temporales" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Perfiles temporales".
3. Pulse el botón "Nuevo perfil temporal" y registre un nuevo perfil.
4. Seleccione el tipo de perfil temporal.
5. En el campo Denominación, introduzca un nombre para el perfil temporal. P. ej., "Semana laboral".
6. Active las casillas correspondientes con los detalles del perfil temporal deseados.



Leer/importar medios

Los medios se pueden registrar manualmente con el cuadro de diálogo "Nuevo medio". Se puede importar una lista de los medios.

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Medios".
3. Ponga el medio en el lector de sobremesa.
4. Rellene los campos "Designación" y "N.º de serie".
   De ser necesario, introduzca también el "Card ID".
5. Pulse el botón "Guardar".
6. Pulse el botón "Cerrar".

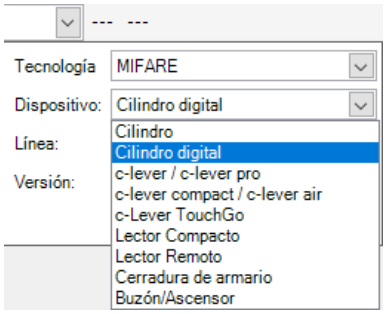


Crear componentes y asignar Master

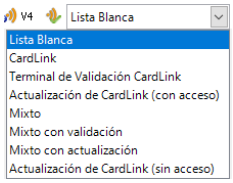
La importación de componentes se realiza preferentemente mediante archivos KIF.
Procedimiento en caso de no disponer de archivo KIF:

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".

3. Pulse el botón "Nuevo actuador".
4. En la columna "Tipo", escoja de la lista la tecnología, el factor de forma, la línea y la versión.



5. Pulse el botón "OK".
6. Seleccione el modo de acceso de la lista.



7. Rellene los campos "N.º de serie", "Denominación" y "N.º de puerta".
8. Asigne un Master programador al componente.

Buzones/ascensores

Este componente tiene hasta 49 salidas conmutadas. Estos deben configurarse en las propiedades en un segundo paso.
Este tipo solo se puede seleccionar en proyectos con V4.

Crear dispositivo básico y salidas de conmutación:

1. Haga clic en "Crear nuevo actuador".
2. En el factor de forma seleccione "Buzones/ascensores".
3. Seleccione la línea "E305" (independiente) o "E345" (móvil con Bluetooth).
   ⇨ La versión de define en "V4".
   ⇨ El modo de acceso se define en "Lista blanca".
4. Pulse "OK".
   ⇨ El dispositivo básico se ha creado.
5. Introduzca o seleccione el número de serie, la denominación, el número y la denominación de la puerta, el Master programador y la zona horaria.
   Aviso: el modo de acceso, TimePro y los perfiles temporales del dispositivo básico no se pueden configurar.
   ⇨ El dispositivo básico está configurado. Ahora debe parametrizar la cantidad y la denominación de las salidas de conmutación.
6. Seleccione el componente.
7. Abra el menú contextual.
8. Seleccione las propiedades.
9. Seleccione la propiedad "Buzones/ascensores".
10. En el menú de selección, escoja la cantidad de salidas de conmutación.
    Aviso: dentro de la lista, seleccione "0" para los componentes sin salida y hasta "49" para los componentes con 49 salidas.
11. En los detalles, introduzca la denominación de cada salida.
    Aviso: TimePro y los perfiles temporales se pueden configurar específicamente para cada salida.
12. Pulse "OK".

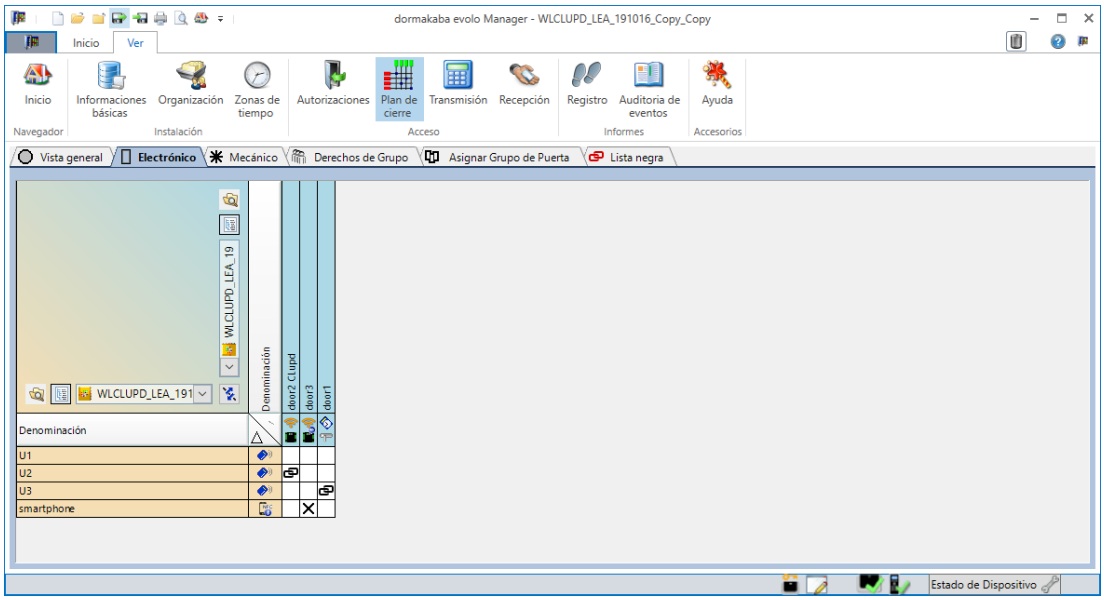
⇨ Las salidas están configuradas y se pueden asignar autorizaciones a las salidas de forma individual.

Asignar medios (con perfil temporal)

El botón "Autorizaciones" de la barra de funciones "Navegador" le permite asignar medios a los componentes.

1. Abra el espacio "Plan de cierre" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Lista blanca" o "Electrónico (CardLink)".
3. Con la matriz podrá activar la asignación que desee.

4. Asigne un perfil temporal a la intersección seleccionada.
5. Pulse el botón "OK".



Los símbolos de la matriz están explicados en el capítulo [▶ 6.8].

Preparar medios en Lista blanca para CardLink

Si crea un proyecto con autorización Lista blanca, puede preparar los medios de usuario para un proyecto futuro con autorización CardLink. Las autorizaciones CardLink se guardarán en los medios y ya no será necesario volverlas a activar cuando cambie los actuadores a CardLink.

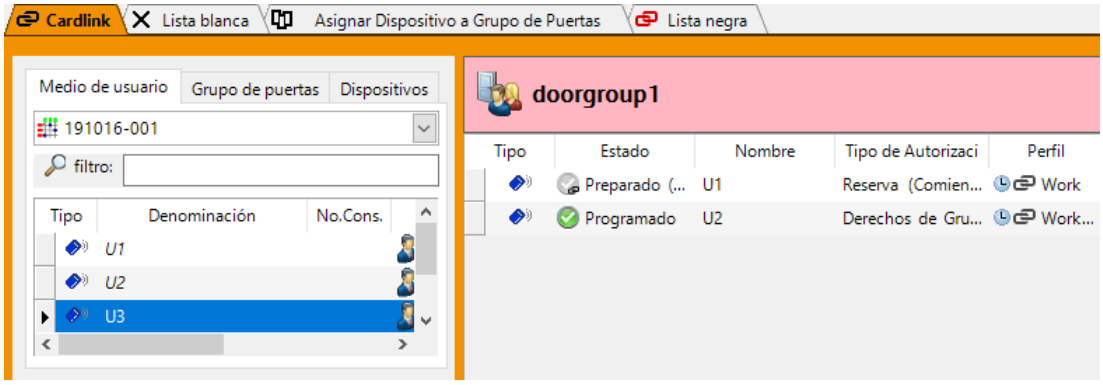
También es posible cambiar posteriormente de un proyecto con autorización Lista blanca a uno con autorización CardLink.

Requisitos previos en las propiedades de proyecto (F4):

- El proyecto debe estar completamente creado en el modo Lista blanca.
- Tecnologías de acceso:
  - elolegic
  - LEGIC advant
  - MIFARE
- Modo de acceso
  - Lista blanca y CardLink
- Tarjeta de seguridad
  - La tarjeta de seguridad está disponible o ya se ha leído para introducirla en el proyecto.

Preparación para CardLink

1. Abra las propiedades de proyecto (F4).
2. Cambie el modo de acceso a "Modo Lista blanca y CardLink".
3. Lea la tarjeta de seguridad para introducirla en el proyecto si todavía no lo está.
4. Cierre las propiedades de proyecto.
5. Abra el espacio "Autorizaciones" de la barra de funciones "Navegador".
6. Vaya a la pestaña "CardLink".
7. Vaya a la subpestaña "Medios de usuario".

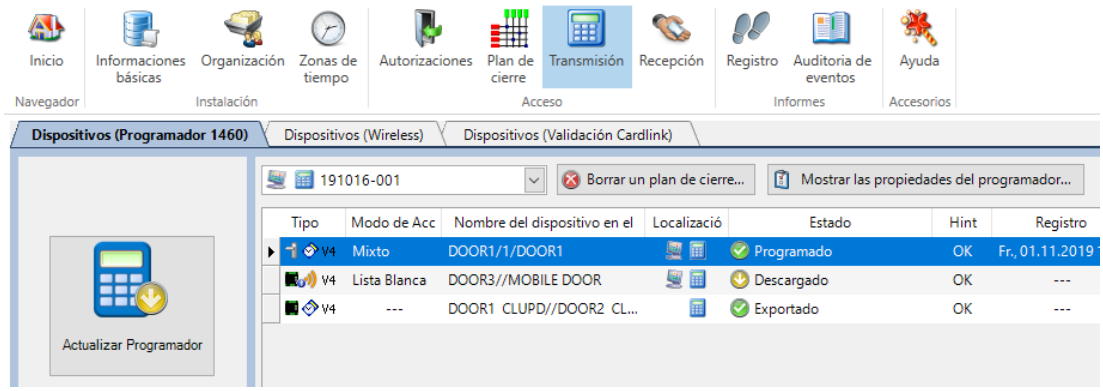


8. Arrastre de uno en uno los medios de usuario de la lista de la ventana izquierda hasta la ventana superior derecha. El medio de usuario aparece en la ventana.
9. Seleccione el tipo de autorización y el perfil temporal.
10. Vaya a la subpestaña "Actuadores".
11. Arrastre de uno en uno los componentes de la lista de la ventana izquierda hasta la ventana derecha grande.
    Los componentes de nueva asignación aparecerán en gris si todavía no están en modo CardLink.
12. Coloque el medio de usuario correspondiente en el lector de sobremesa y prográmelo.
    Ahora los medios de usuario están preparados para CardLink.

Programar componentes

1. Conecte el programador y el ordenador con un cable USB.
   ⇨ El programador aparecerá en la barra de estado.

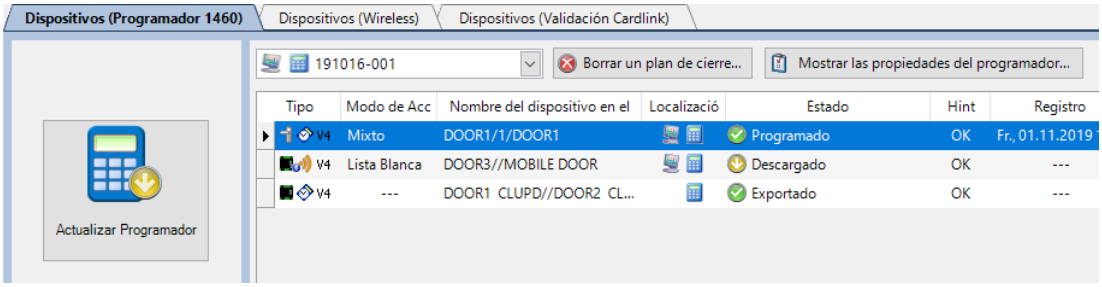
2. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
3. Seleccione el plan de cierre de la lista.
4. Pulse el botón "Actualizador programador".
   ⇨ Los datos se cargan en el programador.



5. Desconecte el programador del ordenador.
6. Transfiera los datos a los componentes de forma individual mediante el programador.

Confirmar programación

1. Conecte el programador y el ordenador con un cable USB.
2. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
3. Seleccione el plan de cierre de la lista.



⇨ Los datos se actualizan automáticamente. Los componentes programados aparecen con el estado "Actual" en la columna Estado.

No desconecte el programador durante la transferencia de datos: si lo desconecta, la transferencia podría ser fallida o incompleta.

6.9.2 Configurar autorización CardLink

Si las auditorías de autorizaciones están activadas, todas las actividades relacionadas con las autorizaciones de un sistema CardLink quedarán registradas.

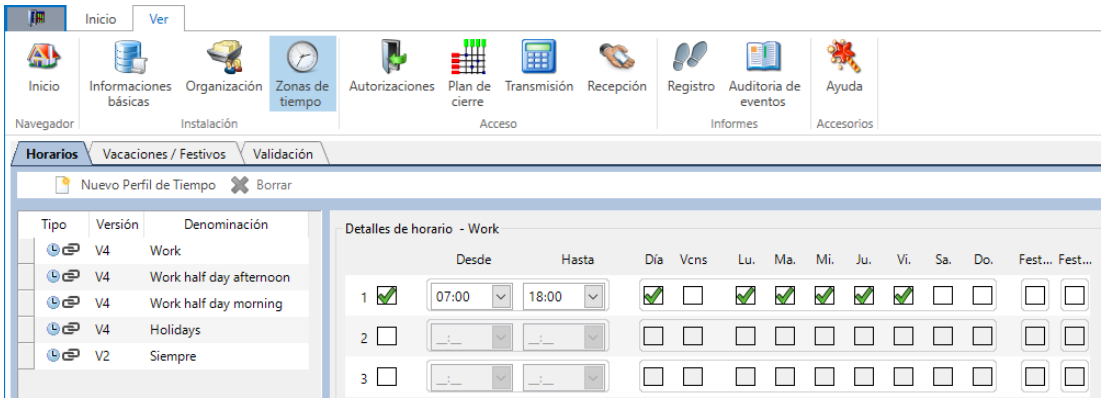
- Para activar o desactivar las auditorías, consulte el capítulo [▶ 6.2.2.1].
- Para la visualización/exportación de las auditorías, consulte el capítulo.

Información sobre las tecnologías

- dormakaba evolo es compatible con CardLink
- Kaba elolegic solo permite usar CardLink con componentes U-Line
- Kaba elostar no es compatible con CardLink

Configurar perfiles temporales para grupos de puertas

1. Abra el menú "Perfiles temporales" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Perfiles temporales".
3. Pulse el botón "Nuevo perfil temporal" y registre un nuevo perfil.
4. Introduzca un nombre en el campo Denominación.
5. Active los detalles del perfil temporal.



Configurar las horas de validación

1. Abra el espacio "Perfiles temporales" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Validación".
3. Cambie el tipo de hora de finalización o los tipos ajustables. En la tabla encontrará las distintas opciones de cambio.

⇨ Las horas de validación configuradas se pueden usar para configurar perfiles temporales de componentes y medios en la zona Elementos básicos.

Validaciones inalterables	24 horas
Validaciones inalterables	"Siempre" (ilimitado)
Validación con hora ajustable	Hora de finalización (solo horas en punto)

5x validaciones con duración ajustable	Días y horas

Las validaciones con hora o duración ajustable permiten rellenar el campo Denominación de forma personalizada.

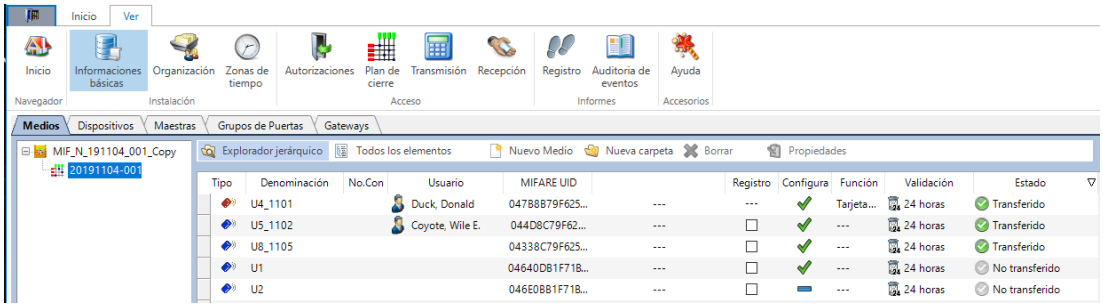
Los perfiles temporales y las fechas de validación configurados se pueden usar en componentes y medios específicos en la zona "Elementos básicos":

- En estos campos de la pestaña "Actuadores"
  - TimePro
  - Perfil temporal TimePro
- En este campo de la pestaña "Medios"
  - Validación de medio

Leer/importar medios

Con el programador 1364 se leen los medios elostar y elolegic. Para los medios LEGIC, también se puede usar el lector de sobremesa.

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Medios".



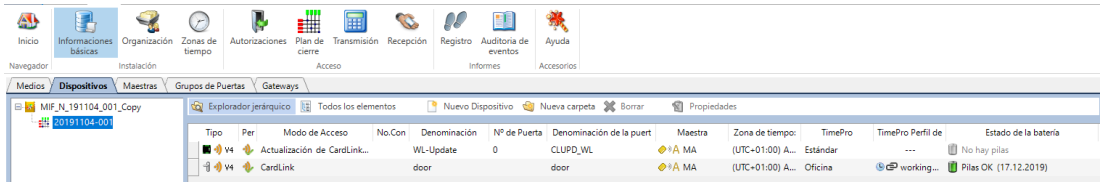
3. Seleccione el plan de cierre en el cual quiera leer los medios para introducirlos.
4. Ponga un medio en el lector de sobremesa.
5. Rellene los campos "Denominación", "N.º de serie" y "Usuario".
6. Pulse el botón "Guardar".

Los medios se pueden registrar manualmente con el botón "Nuevo medio". También se puede importar una lista de medios. [▸ 12.1]

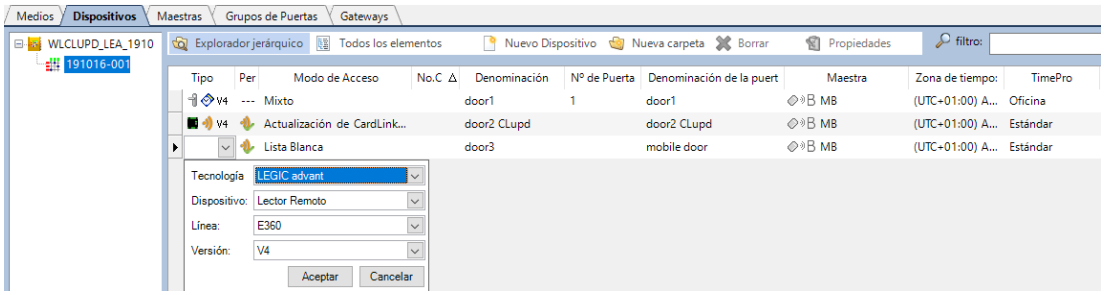
Crear componentes y asignar Master

Procedimiento

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".



3. Cree y registre el componente con "Nuevo actuador".
4. En el campo "Tipo", seleccione los valores adecuados de las listas Tecnología, Factor de formato, Línea y Versión.



5. En el campo Modo de acceso, seleccione el modo para el tipo seleccionado.
6. Rellene los campos N.º de serie, Denominación y N.º puerta.
7. En el campo TimePro, seleccione un tipo de perfil.
8. Confírmelo con "OK".
9. Seleccione el Master programador de la lista en Master programador.

La importación de componentes se puede realizar preferentemente mediante archivos KIF.

Definir componentes para la validación

En los proyectos de LEGIC advant, el componente para la validación debe activarse con la tarjeta de seguridad C2.

Autorización de escritura en LEGIC advant

Procedimiento

1. Presente el medio master para inicializar la programación.
2. Mantenga pulsada la tarjeta de seguridad C2 durante 20 segundos para activar la autorización de escritura. El LED del componente se ilumina en verde durante el proceso.
3. Después de 3 pitidos, el LED verde se apaga y el proceso finaliza.

Tras un restablecimiento INI, los datos de autorización quedan borrados.
Vuelva a realizar la autorización.

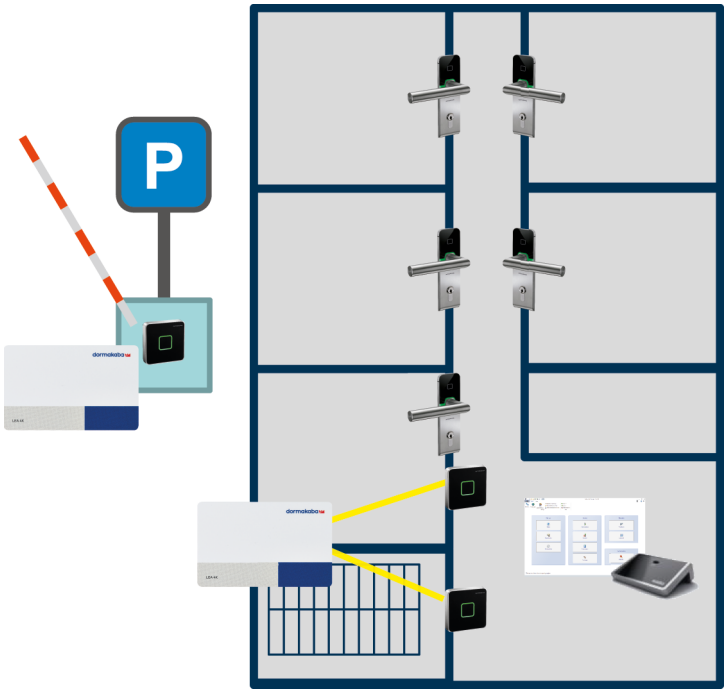
1. Abra la página "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".
3. Seleccione el modo de validación de la lista.
4. Seleccione los medios o componentes.

Definir el tiempo de validación para medios o componentes

Procedimiento

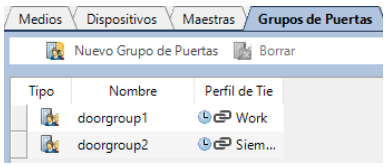
1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores".
3. Seleccione el tiempo de validación que desee de la lista debajo de "Validación de actuadores".

Ejemplo:
En un edificio, la validación se escribe en los medios con los componentes de validación (p. ej., tiempo de validación de 1 día). De esta forma, un medio solo es válido durante un día. Para que un usuario que haya estado ausente durante un tiempo pueda abrir la barrera del aparcamiento con un medio caducado, el componente de la barrera del aparcamiento se puede configurar en modo de validación "Actuador 120 días". Si el usuario se ausenta durante más de 120 días, tampoco podrá acceder al aparcamiento.



Configurar grupos de puertas

1. Abra el menú "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Grupos de puertas".
3. Pulse el botón "Nuevo grupo de puertas".
4. Registre un nuevo grupo.
5. En el campo "Nombre", introduzca un nombre para este grupo de puertas.
6. Seleccione un perfil temporal para este grupo de puertas de la lista debajo de "Perfil temporal".



Asignación grupal de componentes (asignación a los grupos de puertas)

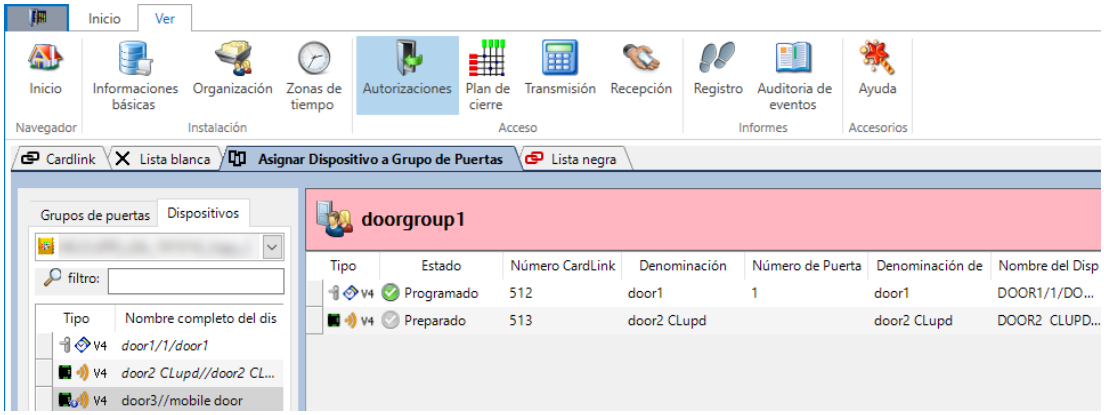
También es posible crear grupos de puertas con el asistente "Crear nuevos grupos de puertas".

Procedimiento

1. Abra el espacio "Autorizaciones" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Asignación grupal de actuadores".
3. Vaya a la subpestaña "Grupos de puertas".
4. Seleccione el grupo de puertas de la lista.
5. Arrastre el grupo de puertas hasta la ventana superior derecha. El grupo de puertas seleccionado aparecerá en la ventana.

6. Vaya a la subpestaña "Actuadores".

7. Arrastre los componentes que desee de la lista de la ventana izquierda hasta la ventana derecha (Grupo de puertas...).



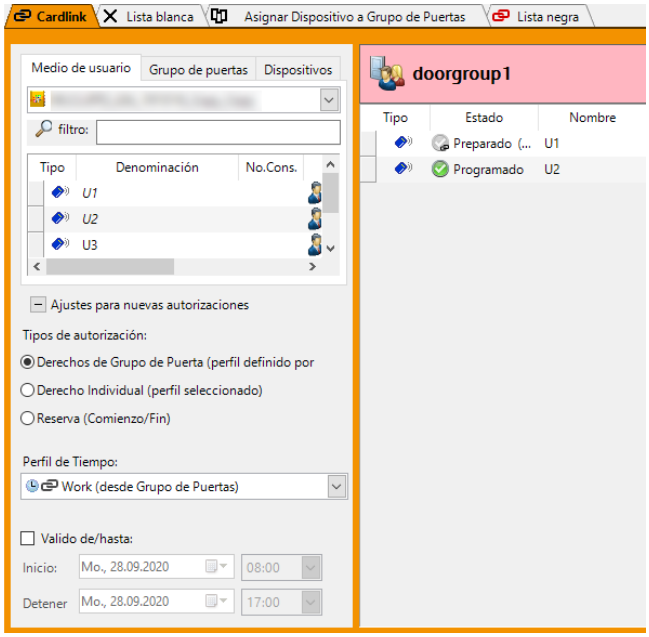
Es posible asignar varios grupos de puertas diferentes a un solo componente.

Crear autorización de CardLink

Procedimiento

1. Abra el espacio "Autorizaciones" de la barra de funciones "Navegador".
2. Vaya a la pestaña "CardLink".
3. Vaya a la subpestaña "Grupos de puertas".
4. Seleccione un grupo de puertas de la lista.
5. Arrastre el grupo de puertas seleccionado hasta la ventana superior derecha.
   ⇨ El grupo de puertas seleccionado aparecerá en la ventana.
6. Vaya a la subpestaña "Medios de usuario".

7. Arrastre los medios de usuario que desee de la lista de la ventana izquierda hasta la ventana derecha.
8. Aparecen las propiedades de autorización de CardLink.
9. Pulse el botón "OK".
   ⇨ El medio de usuario o los medios de usuario seleccionados aparecen en la ventana.



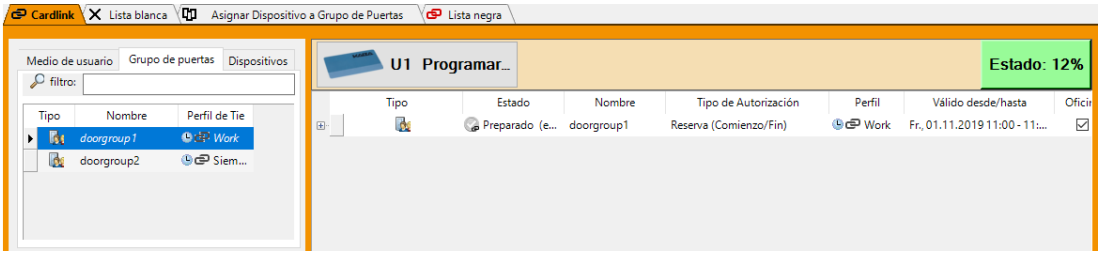
10. Coloque un medio de usuario en el lector de sobremesa y prográmelo.
11. Programe los componentes de las puertas con un programador o de forma inalámbrica.

Programar medios

Los medios también se pueden programar en las zonas "Recepción" o "Plan de cierre".

Procedimiento

1. Abra el espacio "Autorizaciones" de la barra de funciones "Navegador".
2. Vaya a la pestaña CardLink.
3. Vaya a la subpestaña "Medios de usuario".
4. Arrastre las propiedades "Derecho de grupo", "Derecho individual" o "Reserva" hasta la ventana superior derecha.
5. Coloque el medio que quiera programar en el lector de sobremesa.
6. Pulse el botón Programar (nombre del medio)...



Programar actuadores

- Los componentes LEGIC advant y MIFARE se programan con el programador 1460.

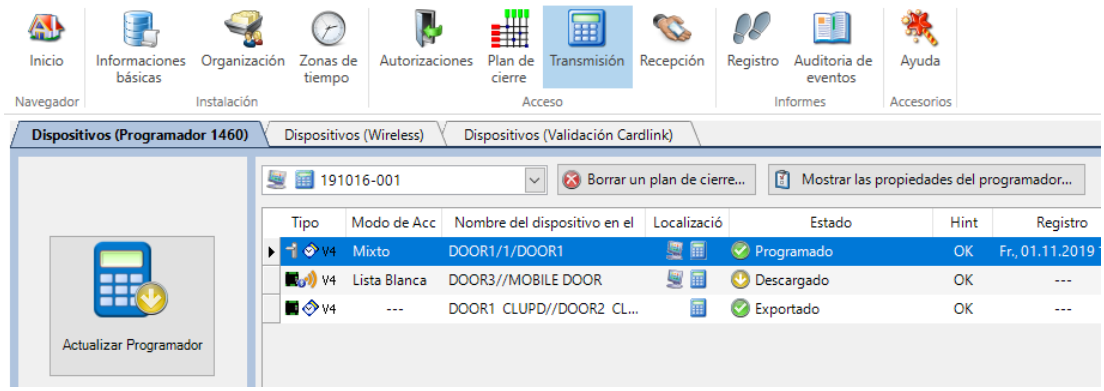
- Los componentes elolegic y elostar se programan con el programador Kaba elo 13 64.

Si un proyecto contiene tecnologías distintas (p. ej., LEGIC advant y elolegic o elostar), se requieren ambos tipos de programador. Estos aparecerán cada uno en su propia pestaña.

Procedimiento

1. Conecte el programador y el ordenador con un cable USB.
   ⇨ El programador aparecerá en la barra de estado.

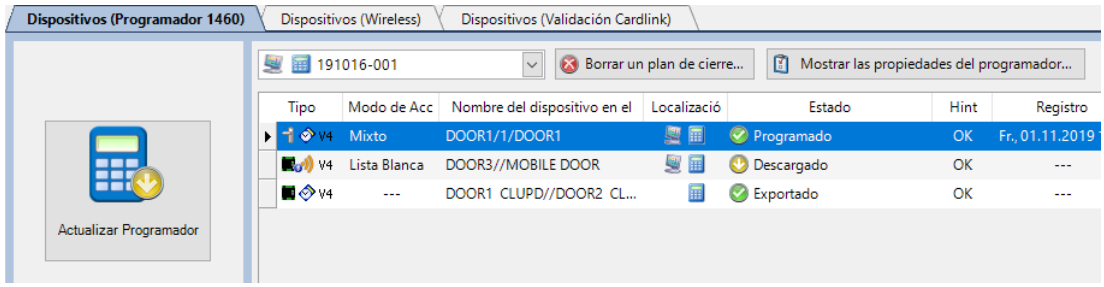
2. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
3. Seleccione el plan de cierre de la lista.
4. Pulse el botón "Actualizador programador".
   ⇨ Los datos se cargan en el programador.



5. Desconecte el programador del ordenador.
6. Transfiera los datos a los componentes mediante el programador.

Confirmar programación

1. Conecte el programador y el ordenador con un cable USB.
2. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
3. Seleccione el plan de cierre de la lista.



   ⇨ Los datos se actualizan automáticamente. Los componentes programados aparecen con el estado "Actual" en la columna Estado.

No desconecte el programador durante la transferencia de datos: si lo desconecta, la transferencia podría ser fallida o incompleta.

6.9.3 Actualización de CardLink con componentes independientes

Transferir una gran cantidad de conjuntos de datos puede llevar algún tiempo.

La función Actualización de CardLink se utiliza para actualizar validaciones y autorizaciones en medios de usuario. Este capítulo contiene información sobre la versión independiente sin gateway inalámbrica.
Para la versión independiente se utiliza un lector remoto 91 15 con módulo de expansión 90 43. Esto se conoce como lector de actualizaciones de Cardlink.

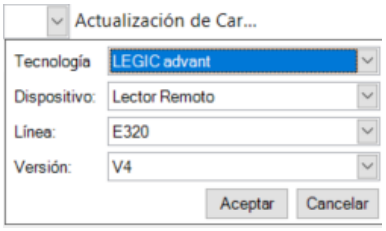
Se requieren al menos las siguientes versiones de firmware de los componentes:

- Programador 1460: 1.36
- Lector remoto 91 15 con módulo de expansión 90 43: 42.40

Si usa LEGIC, también deberá efectuar la autorización de escritura en el lector remoto.

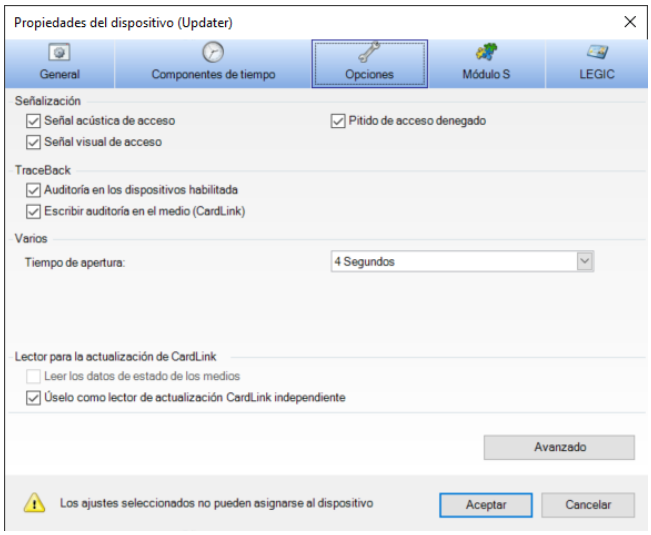
Requisitos previos
Ajustes del lector usado:

Un componente usado para la actualización de CardLink debe presentar esta parametrización:



- El "Tipo de actuador" debe ser el lector remoto E320, 360 (inalámbrico)
- En Elementos básicos está seleccionado uno de los siguientes modos de acceso:
  - CardLink (con actualización)
  - Mixto (con actualización)
  - Actualización

Ajustes en las propiedades del lector remoto
La casilla Lector de actualizaciones de CardLink está activada: Los datos de actualización de CardLink se transfieren al componente a través del programador 1460.



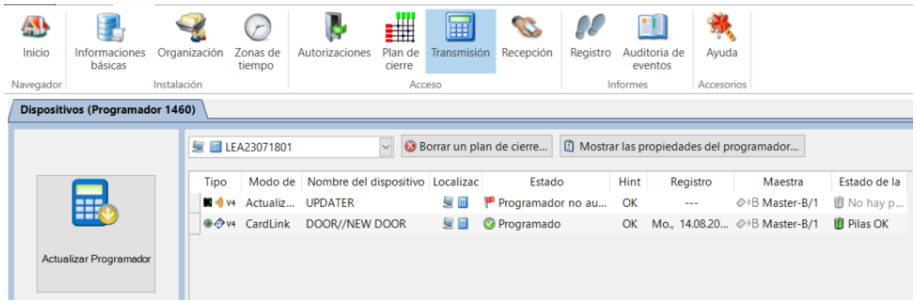
- Se ha seleccionado "Usar como lector de actualizaciones de CardLink independiente"

Actualización de los conjuntos de datos del lector de actualizaciones de CardLink

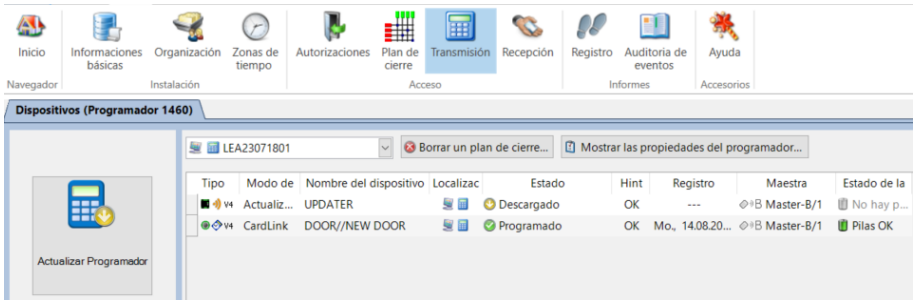
Transferir una gran cantidad de conjuntos de datos puede llevar algún tiempo.

Procedimiento

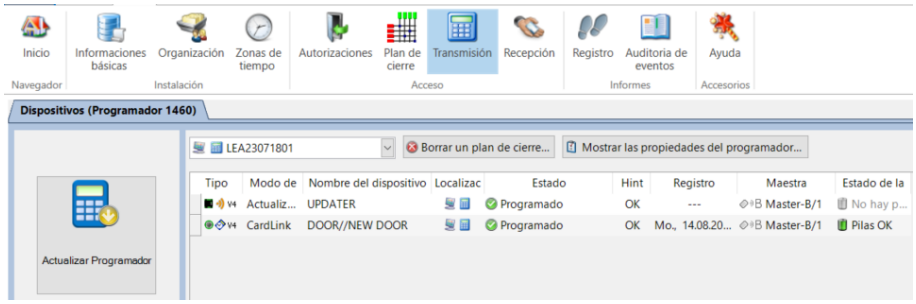
1. Vaya al menú "Transferencia" del navegador.
2. Vaya a la pestaña "Actuadores (programador 1460)".



3. Pulse el botón "Actualizar programador".



4. Consulte el lector de actualizaciones de CardLink con el programador.
5. Inicie sesión en el dispositivo con el Master.
6. Seleccione "Actualizar configuración" en el programador.
   ⇨ Los datos modificados se cargan en el componente.
   ⇨ Los nuevos derechos de acceso y validaciones se transferirán al medio la próxima vez que se presente el medio en cuestión.
   ⇨ Los comentarios de actualización de CardLink se pueden transferir al programador. Para obtener una descripción, consulte "Recopilación de comentarios sobre la actualización de CardLink con el programador".
7. Conecte el programador al KEM.
8. En el menú "Transferencia", vaya a la pestaña "Actuadores (programador 1460)".
   ⇨ Los comentarios del proceso de actualización transferida al programador se transfieren automáticamente al KEM.



Solicite comentarios sobre la actualización de CardLink al programador

Los comentarios sobre si un usuario ha "recopilado" sus autorizaciones del lector de actualizaciones de CardLink se transfieren al KEM a través del programador. Para ello se debe consultar el lector de actualizaciones de CardLink con el programador.

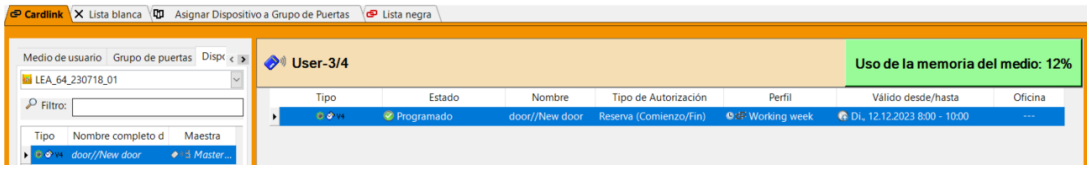
Requisitos previos

- Los permisos modificados del usuario se han transferido al lector de actualizaciones de CardLink.

- Programador 1460
- Medio Master (para iniciar sesión en el componente)

Procedimiento

1. Consulte el lector de actualizaciones de CardLink con el programador.
2. Inicie sesión en el dispositivo con el Master.
3. En el programador, seleccione el elemento de menú "Actualización de Cardlink" en el menú "Leer actuador".
   ⇨ Cuando se han leído los datos, el programador manda el mensaje "Lectura correcta".
4. Conecte el programador al KEM.
5. Vaya al menú "Transferencia".
   ⇨ Los datos se sincronizan automáticamente con el KEM.
   ⇨ En "Autorizaciones/CardLink" se muestra "Actual" para los medios de usuario correspondientes cuando las autorizaciones asignadas han sido "recopiladas" en el lector de actualizaciones de CardLink.



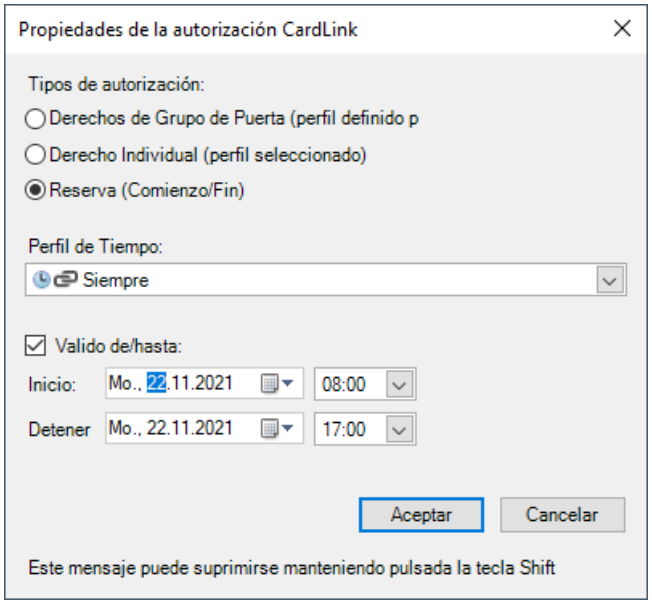
6.9.4 Reserva

Este apartado describe la concesión de derechos para puertas o grupos de puertas específicos durante uno o más períodos de tiempo. Esta función solo está disponible en CardLink.

6.9.4.1 Crear

Crear reserva individual

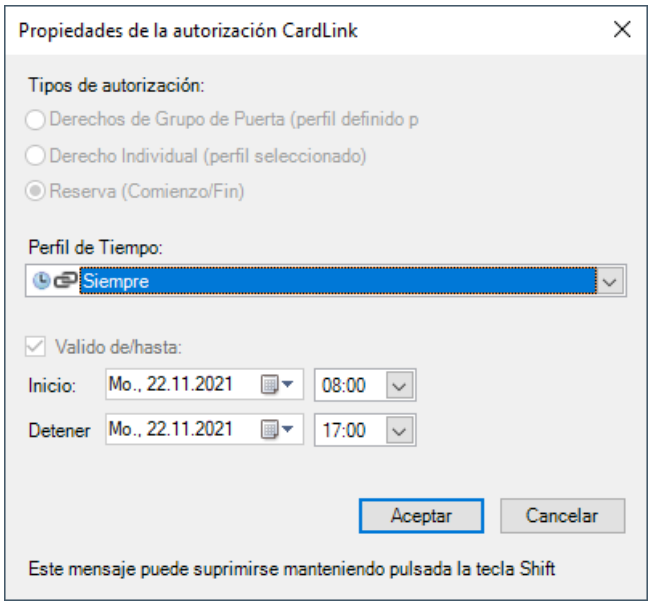
1. Abra el menú "Navegador/Autorizaciones".
2. Seleccione la pestaña "CardLink".
3. Seleccione el medio que quiera programar en la pestaña "Medios de usuario".
4. Arrastre el medio seleccionado con el ratón hasta la barra superior derecha.
5. Arrastre hasta el campo inferior derecho la puerta o el grupo de puertas cuyos parámetros quiera ajustar.



6. Seleccione los ajustes para la reserva.
7. Pulse "OK".
   ⇨ Los datos están preparados y todavía se deben escribir en el medio.
   ⇨ Para crear más reservas, repita el proceso.

Reservas limitadas
Si ya se han creado 2 reservas o si no se han borrado las reservas caducadas, en la creación de más reservas tendrá las siguientes opciones de configuración:

- Seleccionar el perfil temporal para la reserva.
- Introducir el período de validez.



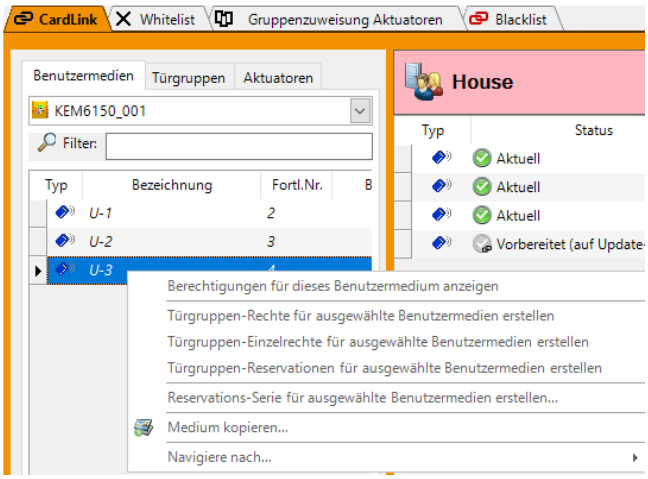
6.9.4.2 Crear serie de reservas

En el caso de los eventos recurrentes, se creará una serie de reservas para un medio y el período de validez correspondiente. Así, durante dicho período y en las horas y días indicados el usuario del medio tendrá acceso a la puerta o grupo de puertas que se muestre.

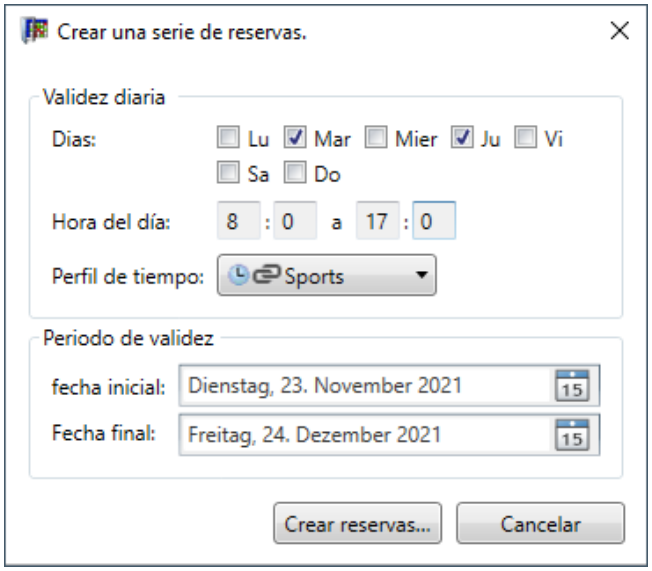
En función del espacio de almacenamiento del medio, se pueden crear hasta 100 reservas.

Procedimiento

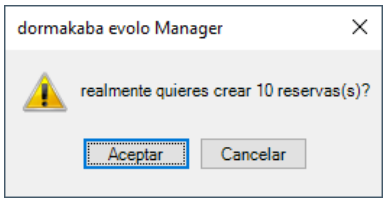
1. Abra el menú "Navegador/Autorizaciones".
2. Seleccione la pestaña "CardLink".
3. En la pestaña "Grupos de puertas" o "Actuadores", seleccione un elemento.



4. Arrastre el elemento seleccionado con el ratón hasta la barra superior derecha.
   ⇨ Queda seleccionado el actuador o el grupo de puertas para la serie de reservas.
5. En la pestaña "Medios", seleccione el medio para el cual quiera crear una serie de reservas.
6. Seleccione la entrada "Crear serie de reservas" en el menú contextual del medio.



7. Seleccione los ajustes.
8. Pulse "Crear reservas".



9. Pulse "OK".
   ⇨ Los datos están preparados y todavía se deben transferir al medio.
10. Los datos se transfieren al medio.
    ⇨ Escriba los datos de CardLink en el medio de usuario.
    ⇨ Cargue los datos de CardLink en el punto de actualización de CardLink (p. ej., lector inalámbrico o terminal). Consulte el capítulo.

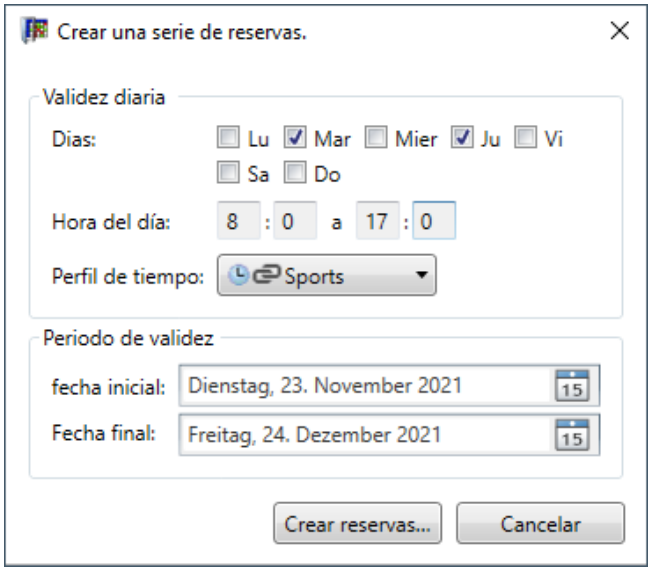
Ejemplo:
En un club deportivo, todos los equipos tienen horas de entrenamiento fijas para la temporada de invierno y cada uno necesita un acceso específico. Las competiciones son los sábados o domingos.

Equipo	**Horas**		
Equipo 1: gimnasia	Lunes de 18:00 a 20:00 Vestuarios 1 y 2	Miércoles de 18:00 a 20:00 Vestuarios 1 y 2	Viernes de 18:00 a 20:00 Vestuarios 1 y 2
Equipo 2: fútbol	Lunes de 20:00 a 22:00 Vestuarios 3 y 4	Jueves de 20:00 a 22:00 Vestuarios 3 y 4	
Equipo 3: hockey	Martes de 19:00 a 21:00 Vestuarios 1 y 2	Viernes de 20:00 a 22:00 Vestuarios 3 y 4	
Competiciones	Sábado De 14:00 a 18:00	Domingo De 14:00 a 18:00	

La gestión del acceso a las instalaciones se realiza mediante CardLink. El administrador crea los accesos necesarios para la serie de reservas basándose en la planificación. Los entrenadores y los miembros de los equipos tienen medios en los que están guardadas las series de reservas. Con la asignación de un grupo de puertas, durante su intervalo temporal cada equipo tiene concedido el acceso a 2 vestuarios y a las instalaciones.

Las competiciones se gestionan en un grupo aparte.

A modo de ejemplo, en KEM se introduce lo siguiente para los medios del equipo 1 en el menú de creación de series de reservas:



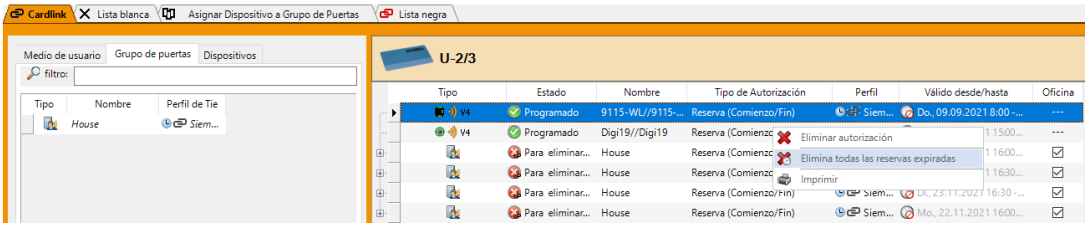
A continuación, se crean series de reservas para los demás equipos.

6.9.4.3 Borrar

Procedimiento para borrar reservas antiguas o caducadas.

1. Abra el menú "Navegador/Autorizaciones".
2. Seleccione la pestaña "CardLink".
3. Seleccione la pestaña "Medios de usuario".
4. Seleccione el medio de usuario.

5. Arrastre el medio de usuario seleccionado hasta la barra superior derecha.
6. En el campo derecho, seleccione la autorización/reserva que quiera borrar.



7. En el menú contextual, seleccione:
   "Eliminar autorización"
   "Eliminar todas las reservas caducadas"
   ⇨ La entrada se preparará para borrarse.
8. La modificación se transfiere al medio.
   ⇨ Programe el medio con el lector de sobremesa.
   ⇨ Envíe los datos al Lector de actualizaciones de CardLink. Consulte el capítulo.

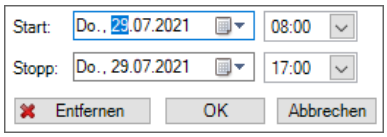
6.9.4.4 Ajustar

Ajustar la validez de un grupo de puertas mostrado en el campo "Validez de/a".

Procedimiento

1. Abra el menú "Navegador/Autorizaciones".
2. En la pestaña "Grupos de puertas" o "Actuadores", seleccione un elemento para que aparezca.

3. En la columna "Validez de/a", seleccione la entrada que quiera ajustar.



4. Ajuste los datos de la entrada seleccionada.
5. Pulse "OK" para confirmar los ajustes.
   Pulse "Eliminar" para eliminar la entrada.
   ⇨ Los datos están preparados y todavía se deben transferir al medio.

6.9.5 Modo Mixto

En modo Mixto, las autorizaciones se guardarán en un medio CardLink o Lista blanca. Si el medio se presenta en un componente configurado con modo Mixto, el componente primero comprueba si hay una autorización Lista blanca. Si no encuentra ninguna autorización, entonces comprueba si hay una autorización CardLink. El componente se abre si el medio está autorizado con uno de estos tipos de autorización.

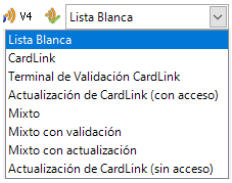
Si el medio aparece en ambos tipos de autorización y se clasifica como "no autorizado" en uno de ellos, quedará rechazado.

Ejemplo: el componente no se abrirá si un medio tiene una autorización CardLink válida, pero también dispone de una autorización Lista blanca con un perfil temporal caducado.

Instalación

El modo Mixto inalámbrico todavía no es compatible con la gateway inalámbrica.

El modo Mixto se selecciona en la pestaña "Actuadores", en el menú "Elementos básicos" del modo de acceso.



6.9.6 Copiar autorizaciones de medios y componentes

Esta función le permite copiar medios o componentes junto con sus autorizaciones.
Son posibles las siguientes opciones:

- Copiar dentro del plan de cierre de un proyecto.
- Copiar a otros planes de cierre de un proyecto.
- Copiar a uno o varios medios.
- Copiar a uno o varios componentes.

Requisitos previos

- Se deben poder copiar medios y componentes de un proyecto con Lista blanca o CardLink.

- Se deben copiar todas las autorizaciones de Lista blanca y/o CardLink.

Copiar medios
Los medios se pueden copiar con el botón "Asistentes" o en la zona "Autorizaciones" mediante la función "Copiar medio". Seleccione un medio como referencia y cópielo a uno o varios medios de destino.

Los componentes modificados se deben actualizar con el programador o de forma inalámbrica. Los medios con una autorización CardLink se deben actualizar con un lector de sobremesa o un terminal.

Procedimiento

1. Abra el espacio "Asistentes" de la barra de funciones "Navegador".
2. Pulse el botón "Copiar medio".
3. Siga el asistente.
4. Tras la copia, pulse el botón "Cerrar".

Copiar componentes
Los componentes se pueden copiar con el botón "Asistentes" o desde las autorizaciones mediante el menú contextual "Copiar actuador".

Seleccione un componente como referencia y cópielo a uno o varios componentes de destino.

Los componentes modificados se deben actualizar con el programador o de forma inalámbrica. Los medios con una autorización CardLink se deben actualizar con un lector de sobremesa o un terminal.

1. Abra el espacio "Asistentes" de la barra de funciones "Navegador".
2. Pulse el botón "Copiar actuador".
3. Siga el asistente.
4. Tras la copia, pulse el botón "Cerrar".

6.10 Transmisión

La transferencia es el intercambio de datos entre el software KEM, el programador y/o la gateway (GW) para la opción inalámbrica con los componentes.

Además de los campos Tipo, Denominación, Usuario y otros, el campo Ruta también se puede activar. En Ruta aparecerá la ruta actual de un plan de cierre con las subcarpetas. La ruta se puede ordenar.

Inalámbrico
Los componentes con la opción inalámbrica aparecerán como inactivos en la pestaña "Actuadores (Inalámbrico)" hasta que se complete la puesta en marcha de estos componentes (y estén conectados con la GW) [▶ 11.3]. Antes poner en marcha la opción inalámbrica, los componentes se deben programar una vez con el programador 1460. Puesta en marcha la opción inalámbrica y realizada la transferencia de datos al software desde el programador 1460, los componentes aparecen automáticamente como activos en la pestaña "Actuadores (Inalámbrico)". En este registro se pueden consultar distintas propiedades, cargar el Traceback y actualizar la parametrización. El componente ya no se deberá localizar con el programador.

Autónomo

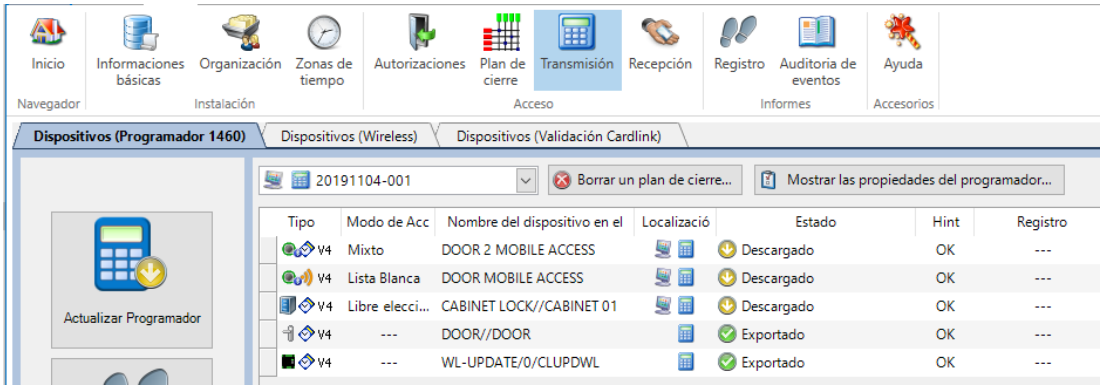
Programador 1460

Los componentes LEGIC advant y MIFARE se programan con el programador 1460.

1. Conecte el programador con el ordenador mediante un cable USB.
2. Seleccione el plan de cierre de la lista.
3. Pulse el botón "Actualizador programador".

⇨ Los datos se cargan en el programador.

Todas las órdenes se refieren al plan de cierre seleccionado.



Actualizar el programador	Los datos actuales de los componentes se cargan en el programador.
Actualizar la Traceback	Los datos actuales de Traceback se cargan en el software KEM mediante el programador.
Borrar todos los archivos	Se borran todos los datos de los componentes que se encuentren en el programador.

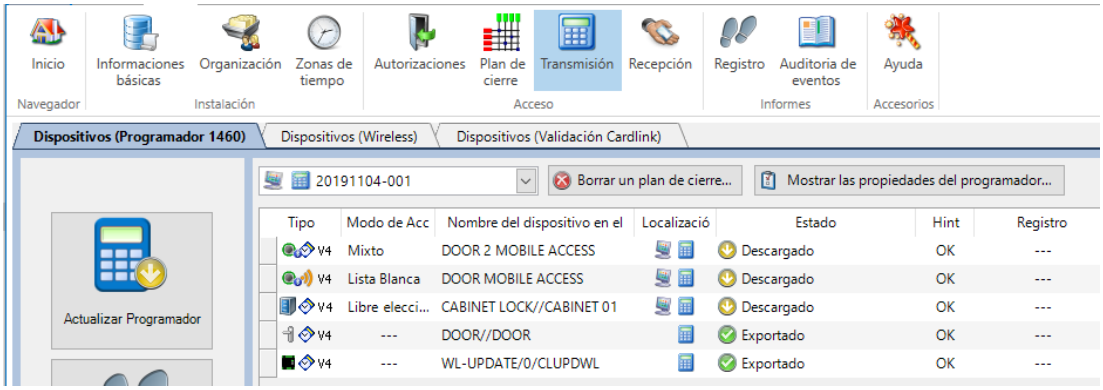
No desconecte el programador durante la transferencia de datos: si lo desconecta, la transferencia podría ser fallida o incompleta.

Programador 1364

Los componentes Kaba elolegic y Kaba elostar se programan con el programador Kaba elo 1364.

1. Conecte el programador 1364 con el ordenador mediante un cable USB.
   ⇨ El programador aparecerá en la barra de estado.
2. Seleccione el plan de cierre de la lista.
3. Pulse el botón "Actualizador programador".

⇨ Los datos se cargan en el programador.



Actualizar el programador 1364	Los datos actuales de los componentes se cargan en el programador 1364.
Cargar estado de todos los actuadores	El estado de todos los componentes se carga en el programador 1364.

Actualizar la Traceback	Los datos actuales de Traceback se cargan en el software KEM mediante el programador 1364.

No desconecte el programador durante la transferencia de datos: si lo desconecta, la transferencia podría ser fallida o incompleta.

6.10.1 Error de datos

Si en el campo "Estado" aparece "Error de datos", la entrada del componente se debe revisar. Para que aparezca una descripción del error más precisa, ponga el puntero encima de "Error de datos" hasta que aparezca la descripción emergente.

La siguiente tabla muestra las posibles descripciones de error.

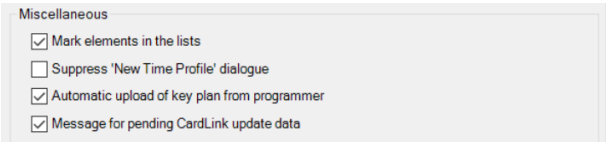
Aviso de error	Descripción	Solución
Error de datos	El actuador todavía no tiene ningún Master programador asignado.	Asigne un Master al componente o lea un Master para introducirlo en el proyecto y luego asignarlo al componente.
	El Master programador asignado no tiene un UID válido.	Compruebe el UID del Master programador.
	El modo de acceso todavía no se ha establecido.	Asigne el modo de acceso.
	TimePro todavía no tiene ningún perfil temporal asignado.	Cree y/o asigne un perfil temporal.
	El perfil temporal utilizado por TimePro es defectuoso.	Compruebe el perfil temporal y corríjalo.
	Uno de los perfiles temporales utilizados no es correcto.	Compruebe el perfil temporal y corríjalo.
	Uno de los medios de usuario usados tiene un UID defectuoso.	Compruebe los UID de los medios de usuario.
	Uno de los medios de usuario usados tiene un CID defectuoso.	Compruebe los CID de los medios de usuario.
	Hay una autorización sin ningún Master B asignado.	Asigne un Master B al componente o lea un Master B para introducirlo en el proyecto y luego asignarlo al componente.
	Uno de los Master B utilizados tiene un UID defectuoso.	Compruebe/complete los UID de los Master B utilizados.
	La selección "Tecnologías activas LEGIC advant" de las propiedades de proyecto se ha configurado como "Manual". Sin embargo, hay medios de usuario que no utilizan la tecnología deseada y tienen autorización en este actuador.	Compruebe la selección de tecnología o las propiedades de proyecto. Compruebe los medios de usuario y las autorizaciones.

Cuando elimine la causa, el "Error de datos" ya no aparecerá.

6.11 Datos de actualización de CardLink

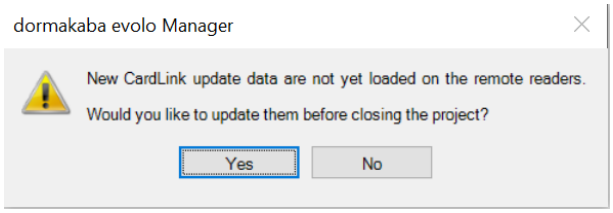
Si aún no se han transferido los datos de actualización de CardLink, el usuario será informado al cerrar un proyecto y podrá decidir si aún desea llevar a cabo esta operación.

Requisitos previos



- En Opciones está activado (por defecto) "Mensaje si hay datos de actualización de CardLink pendientes".
- Existe un lector remoto con función "Actualización CardLink".
- No se han transferido los nuevos datos de actualización para el lector remoto.

Comportamiento



- El cuadro de diálogo se abre si aún no se han transferido los datos de actualización de CardLink.
- Haga clic en "Sí" para transferir estos datos antes de cerrar el proyecto. El usuario es dirigido al menú "Transferir" y puede transferir los datos.
- Haga clic en "No" y el proyecto se cerrará sin transferir los datos.

6.12 Traceback

La función Traceback permite controlar actividades. Los datos de Traceback se pueden transferir al software del sistema desde el medio de usuario o desde el componente para que aparezcan allí.

Tiene las siguientes opciones:

- Transferir los datos de Traceback del componente.
- Transferir los datos de Traceback del medio.
- Cargar los datos de Traceback de forma inalámbrica.

Escogido el método, el procedimiento es este:

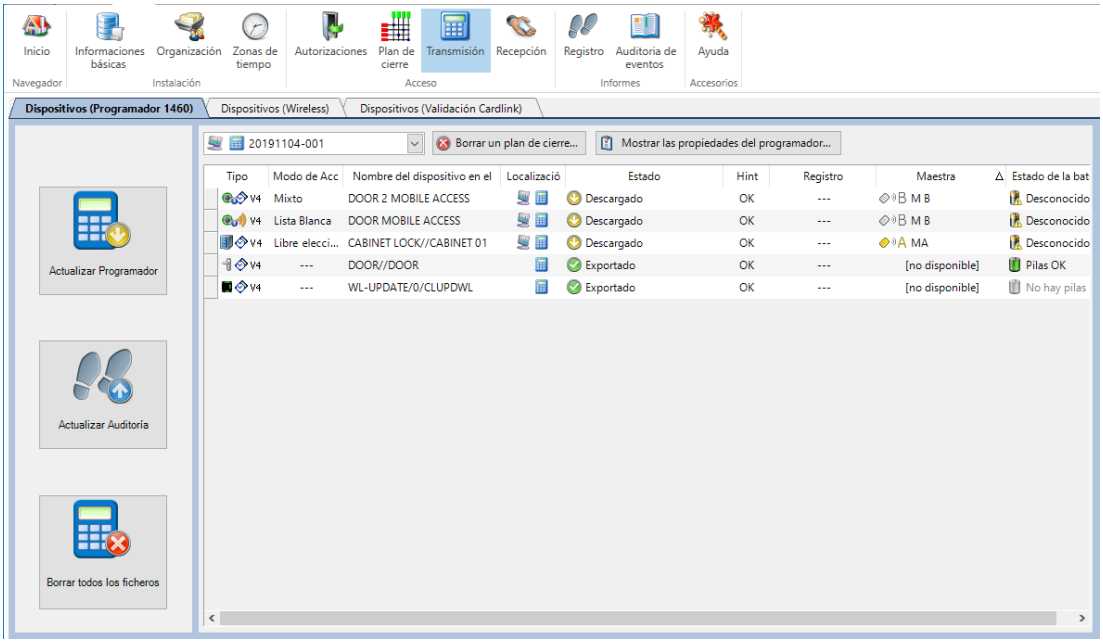
Transferir los datos de Traceback del componente

La información de Traceback está guardada en la memoria del componente. Los datos de Traceback se leen y transfieren al software del sistema con el programador.

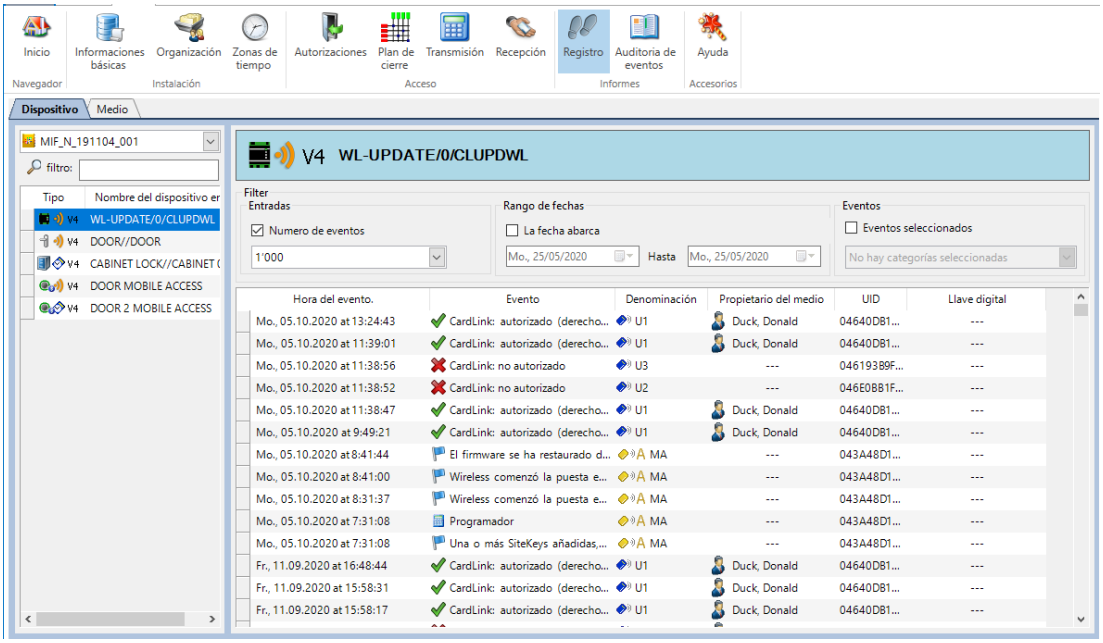
Requisito: los datos de Traceback de los componentes deben haber sido leídos con el programador.

Procedimiento

1. Conecte el programador con el ordenador mediante un cable USB.
2. Pulse el botón "Transferencia" de la barra de funciones "Navegador".
3. Seleccione el plan de cierre de la lista.
4. Pulse el botón "Actualizar Traceback".
   ⇨ El programador carga los datos en el software del sistema.



5. Pulse el botón "Traceback" de la barra de funciones "Navegador".
6. Vaya a la pestaña "Actuador".
7. Si el plan de cierre no está seleccionado, seleccione uno.
8. Seleccione el componente de la lista con un doble clic. También puede arrastrar y soltar un elemento de la lista hasta la barra superior derecha.

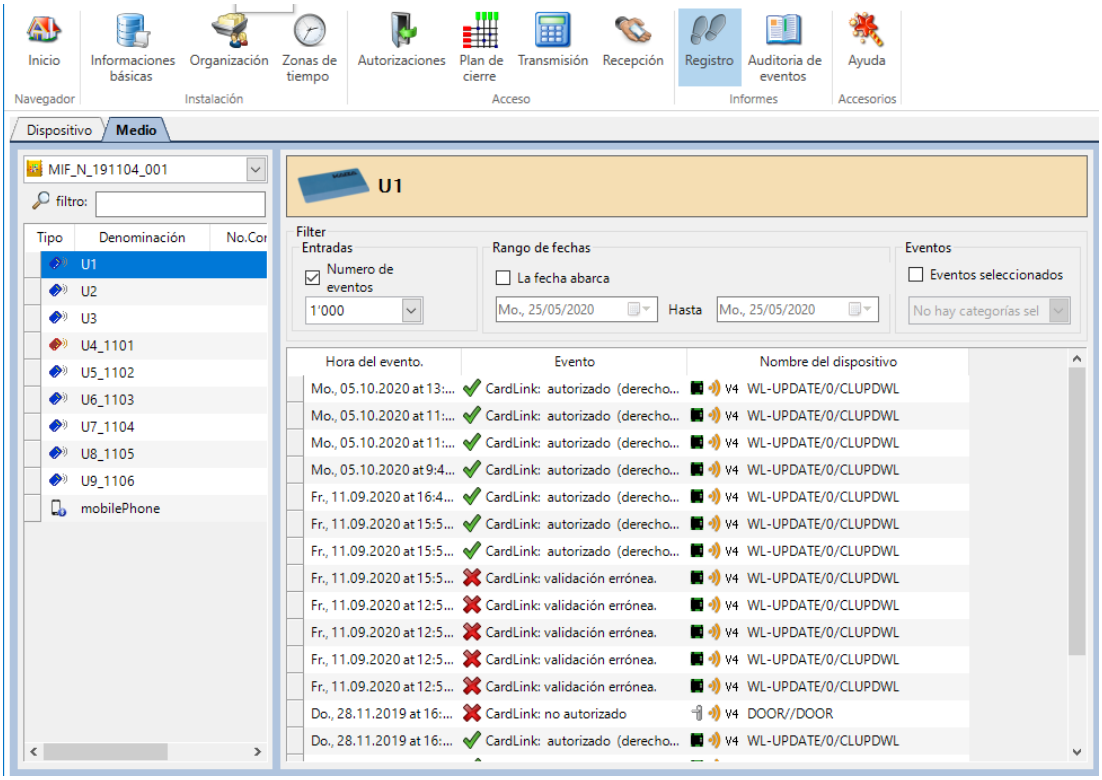


Transferir los datos de Traceback del medio

El componente escribe los datos de Traceback en el medio que se le presente. Estos datos de Traceback se pueden transferir al software del sistema mediante el lector de sobremesa. Esta función se puede activar en las Propiedades de proyecto.

Procedimiento

1. Pulse el botón "Traceback" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Medio".
3. Ponga el medio en el lector de sobremesa.
4. Pulse el botón "Leer Traceback de (nombre del medio)...".



Cargar los datos de Traceback de forma inalámbrica

Los datos de Traceback de los componentes conectados de forma inalámbrica se pueden cargar mediante la gateway inalámbrica.

Procedimiento:

1. En el menú "Transferencia", seleccione los componentes para la transferencia.
2. Pulse "Cargar Traceback".
   - ⇨ Se envía la petición a la gateway y se transfiere a los componentes.
   - ⇨ Los componentes transfieren los datos a KEM por vía de la gateway .
   - ⇨ Si en "Estado de Traceback" aparece el sello temporal de la petición, la transferencia está completa.

Tabla de los códigos de Traceback

La siguiente tabla explica el significado de los datos de Traceback leídos.

#	Códigos de Traceback Resultado	Explicación/solución
01	Acceso concedido	El medio presentado está autorizado.
02	Acceso denegado (sin autorización)	El medio presentado no está autorizado.
03	Acceso denegado (hora incorrecta)	El medio se ha presentado fuera de su intervalo temporal.
04	Acceso concedido (alimentación de emergencia)	Cambie las pilas. Consulte el capítulo Asistencia técnica en el manual del componente.
05	Master A/B	Inicio de la programación manual (codificación)
06	Programador	Inicio del acceso del programador
07	Hora definida	La hora se ha establecido. El ajuste correcto de la hora garantiza el buen funcionamiento de las funciones de los componentes ligadas al tiempo.
08	Modo módulo (externo)	(elolegic)
09	Abrir TimePro Office	
0A	Cerrar TimePro Office	
0B	Acceso denegado (hora TwinTime incorrecta)	(elolegic)
0C	Acceso denegado (SPC incorrecto)	(elolegic)

#	Códigos de Traceback Resultado	Explicación/solución
0D	El cilindro digital no se acopla	(elolegic) Compruebe la unidad mecatrónica y la electrónica.
0E	Acceso denegado (error de TwinTime)	(elolegic)
0F	Cerrar modo abierto	(solo para lectores remotos y lectores compactos)
10	Tras la modificación correcta de la configuración del actuador, el firmware se ha reiniciado	
11	Acceso concedido (autorización de visitante)	(elolegic)
12	Avería en módulo de bloqueo	No se ha podido cerrar
13	Avería en módulo de bloqueo corregida	Se ha efectuado el cierre
14	Advertencia posición de acople	solo para cilindros digitales
15	Posición de acople correcta	solo para cilindros digitales
16	Sin configuración después de la actualización de FW	La configuración se ha perdido y debe volver a transferirse.
19	Abrir TimePro Day/Night	El componente se abre a la hora configurada.
1A	Cerrar TimePro Day/Night u Office (el tiempo ha expirado)	El componente se cierra a la hora configurada.
1B	Abrir modo de paso	El componente se abre con el modo de paso.
1C	Cerrar modo de paso	El componente se cierra con el modo de paso.
20	Una o varias Sitekey se han añadido, modificado o borrado.	
21	No todas las Sitekey se han podido leer en el Master.	
22	Acceso denegado (sin autorización móvil)	(elolegic) El componente no está configurado para Mobile Access. Compruebe: • Requisitos de Mobile Access.
23	Acceso denegado (hora incorrecta)	(elolegic)
2B	Acceso denegado (hora TwinTime incorrecta)	(elolegic)
30	Lanzado	solo LEGIC Advant/Prime: la tarjeta de seguridad C2 ha concedido la autorización de escritura al componente.
31	Retirado	solo LEGIC Advant/Prime: la tarjeta de seguridad C2 ha retirado la autorización de escritura al componente. Después de un proceso como el restablecimiento INI, la autorización de escritura se debe volver a conceder.
32	Acceso denegado (hora incorrecta)	(elolegic)
33	Acceso denegado (hora incorrecta)	(elolegic)
35	VCP ok.	Se ha realizado la configuración VCP del componente. Los VCP incluyen la llave criptográfica para Mobile Access.
36	Error de VCP: error general	
37	Error de VCP: contraseña incorrecta	Compruebe la contraseña.
38	Error de VCP: Custom Data Format defectuoso	longitud o formato incorrecto
39	Error de VCP: almacén de llaves lleno	Los 128 espacios de almacenamiento de llaves virtuales están ocupados.
3A	Error de VCP: KeySet ID de proyecto erróneo	KeySet ID de proyecto no coincide con el ID de proyecto de la base de datos

#	Códigos de Traceback Resultado	Explicación/solución
3B	Acceso denegado Error de VCP: llave VCP errónea	(elolegic) hora TwinTime errónea (evolo) VCP de otra Legic Connect Company
3D	Error de VCP: el administrador ya está configurado	
3E	Error de VCP: no hay administrador configurado	
3F	Error de VCP: LEGIC Chip ID erróneo	
40	Módulo S (inicio modo abierto)	El componente se ha abierto con el módulo S.
41	Módulo S (inicio modo cerrado)	El componente se ha cerrado con el módulo S.
42	Módulo s (inicio modo cualquier medio)	
43	Módulo s (inicio funcionamiento normal)	El Módulo S está fuera de servicio. El componente vuelve a funcionar con normalidad.
44	Módulo S (final interrupción de alimentación)	(elolegic)
45	Módulo S (sin acceso por modo cerrado)	El componente está cerrado con el módulo S. El medio no está autorizado.
46	Módulo S (acceso concedido)	
47	Módulo S (modo de inicio: Medio autorizado)	
48	Módulo S (inicio apagar TimePro)	
50	Se ha realizado la modificación	
56	Modificación fallida (Lista blanca llena)	(elolegic) Lista blanca: se ha alcanzado la cantidad máxima de usuarios para el funcionamiento en Lista blanca de este componente.
57	Modificación fallida (Lista de bloqueo llena)	CardLink: se ha alcanzado la cantidad máxima de entradas en la Lista de bloqueo del componente.
58	Modificación fallida (error general)	
59	Actualización de validación efectuada	El medio se ha podido validar.
5A	Actualización de validación fallida (sin autorización)	
5B	Actualización de validación fallida (tiempo erróneo)	
5C	Actualización de validación fallida (validación caducada)	
5D	Actualización de CardLink efectuada	
5E	Actualización de CardLink fallida	Los datos de CardLink no se han podido guardar en el componente.
60	CardLink: sin autorización	
61	CardLink: validación no válida	
62	CardLink: Área de administración errónea	
63	CardLink: tiempo erróneo	
64	CardLink: error al actualizar la validación	(elolegic)
65	Medio bloqueado, validación borrada	CardLink: Medio de la Lista de bloqueo en el actuador de validación: Header borrado
6A	CardLink: autorizado (derecho individual)	
6B	CardLink: autorizado (derecho de grupo de puertas)	
6C	CardLink: autorizado (reserva)	
6D	Acceso denegado (HW incorrecto)	Sin autorización, vinculación errónea
6E	Acceso denegado	Sin autorización, archivo defectuoso
70	Acceso concedido (apertura manual)	(elolegic) Lockerlock/CabinetLock: Apertura manual (sin medio, UID=0)

#	Códigos de Traceback Resultado	Explicación/solución
71	Acceso concedido (con medio de administración)	Lockerlock/CabinetLock: Apertura/cierre con medio de mantenimiento
72	Duración máxima de ocupación superada	(elolegic) Lockerlock: Duración máxima de ocupación superada
73	Ningún segmento libre de selección de armario o sin sitio	Lockerlock/CabinetLock: archivo/segmento no disponible o ningún sitio libre
74	Error de cierre (CabinetLock)	Cabinet Lock: error de bloqueo de interruptor de activación
75	Alarma disparada (CabinetLock)	Cabinet Lock: alarma disparada
76	cierre manual sin medio (CabinetLock)	Cabinet Lock: cierre manual sin medio
80	RCID: Acceso concedido	
81	RCID: sin autorización	
82	RCID: validación no válida	
83	RCID: tiempo erróneo	
85	RCID: medio en Lista de bloqueo	
8A	Puesta en marcha inalámbrica iniciada	El componente intenta conectarse a una gateway inalámbrica en la cual la puesta en marcha inalámbrica está activa.
8B	Puesta en marcha inalámbrica efectuada	El componente se ha conectado a una gateway inalámbrica en la cual la puesta en marcha inalámbrica está activa.
8C	Puesta en marcha inalámbrica fallida	El componente no se ha podido conectar a una gateway inalámbrica. Compruebe: • El componente está configurado para el funcionamiento inalámbrico. • La puesta en marcha inalámbrica está iniciada en la gateway. • La gateway inalámbrica para la puesta en marcha está dentro del rango inalámbrico.
8D	Función inalámbrica desconectada	
90	Pass-Lock activado	Antipánico: modo de pánico activado
91	Pass-Lock desactivado	Antipánico: modo de pánico desactivado
95	Escape-Return activado	La puerta se puede abrir por fuera sin medio. Para cerrarla/cambiar de modo, pulse el botón de la puerta.
96	Escape-Return: cerrar con botón	La puerta solo se puede abrir por fuera con un medio válido. Para abrirla/cambiar de modo, pulse el botón de la puerta.
97	Cerrado con autorización	
98	Siempre abierto con autorización	
9A	Acceso remoto: Abierto	
9B	Acceso remoto: Control de acceso	
9C	Acceso remoto: Bloqueado	
9D	Acceso remoto: Funcionamiento normal	
9E	Acceso remoto: Abierto una vez	
9F	Acceso denegado (bloqueado)	Mando no autorizado por estar en modo "Shutdown"
B0	Puertas forzadas	Puerta forzada (vigilancia del estado de la puerta)

#	Códigos de Traceback Resultado	Explicación/solución
BB	Acceso denegado (hora TwinTime incorrecta)	(elolegic)
C2	Acceso denegado (SPC incorrecto)	(elolegic)
C3	Acceso denegado (SPC incorrecto)	(elolegic)
C4	Actualización de la licencia de SL1 a SL2	Configuración a través de medio de actualización.
C5	Actualización de la licencia de SL1 a SL3	Configuración a través de medio de actualización.
C6	Actualización de la licencia de SL2 a SL3	Configuración a través de medio de actualización.
C7	Actualización de la licencia de SL4 a SL3	Configuración a través de medio de actualización.
C8	Actualización de la licencia a Bluetooth	Configuración de Bluetooth a través de medio de actualización.
D0	Cambio de batería (activado por medio especial)	
D1	Cambio de batería (activado por el programador 1460)	
D2	Cambio de batería (detectado automáticamente)	
D3	Cambio de batería (activado por la gateway inalámbrica)	
D5	Desactivar la detección optimizada de batería baja	
D6	Activar la detección optimizada de batería baja	
D7	Desactivar la detección optimizada de batería baja	
E2	Acceso denegado (error al leer el segmento)	(elolegic) Medio defectuoso. Sustituya el medio.
E3	Acceso denegado (error al leer el segmento)	(elolegic) Medio defectuoso. Sustituya el medio.
EB	Acceso denegado (error al leer el segmento)	(elolegic) Medio defectuoso. Sustituya el medio.
F0	Acceso denegado (medio en la Lista de bloqueo)	CardLink/AoC/OSS/MobileLink: los medios de la Lista de bloqueo no son válidos.
F2	Acceso denegado (medio en la Lista de bloqueo)	(elolegic) Los medios de la Lista de bloqueo no son válidos.
F3	Acceso denegado (medio en la Lista de bloqueo)	(elolegic) Los medios de la Lista de bloqueo no son válidos.
FB	Acceso denegado (medio en la Lista de bloqueo)	(elolegic) Los medios de la Lista de bloqueo no son válidos.
FF	Acceso concedido (autorización de grupo)	(elolegic)
100	Traceback solicitado de forma inalámbrica.	La pasarela conectada ha solicitado los datos de Traceback al componente de forma inalámbrica.

6.13 Registros

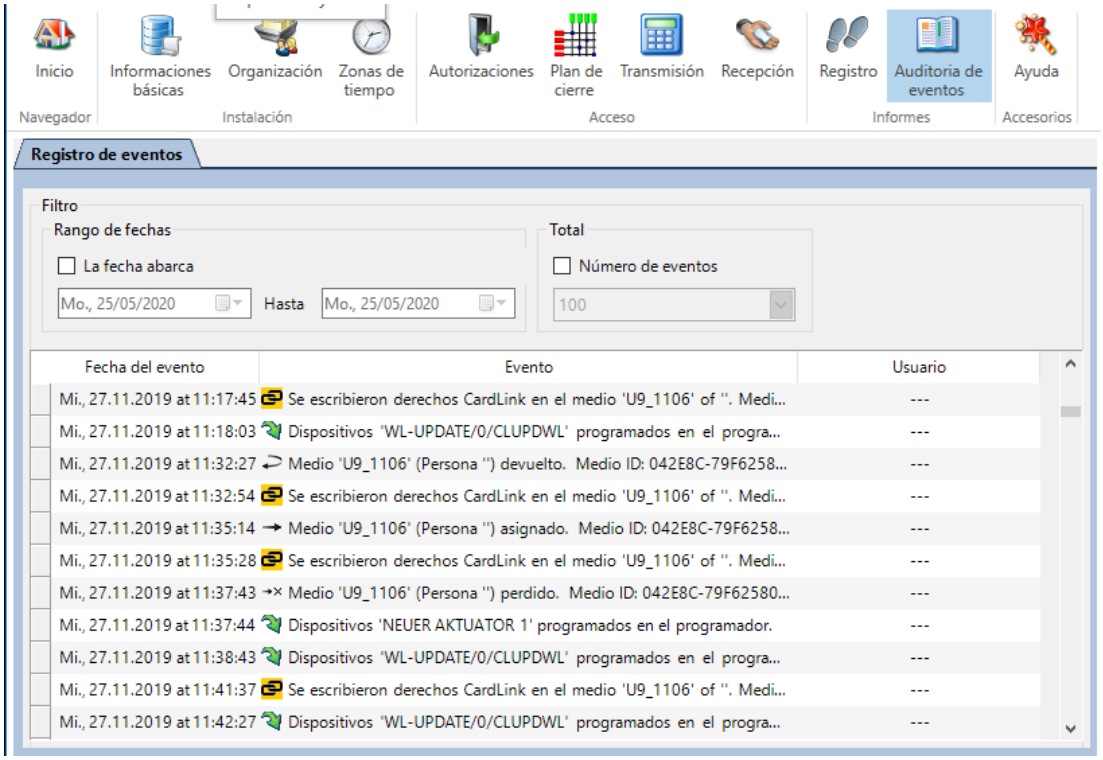
6.13.1 Lista de registros

La función de registros del software del sistema registra la hora y el usuario en estos eventos:

- Un proyecto se ha
  - abierto
  - cerrado
  - exportado
  - importado
- Se ha producido una descarga o una carga de datos del programador.
- Se ha producido una descarga o una carga de datos de los componentes.
- Un medio se ha
  - emitido

  - retirado
  - registrado como perdido
- Se han leído los datos de Traceback.

La lista de los registros mostrados se puede limitar activando los filtros.



6.13.2 Lista de auditorías

La activación de la lista de auditorías puede generar una gran cantidad de datos.

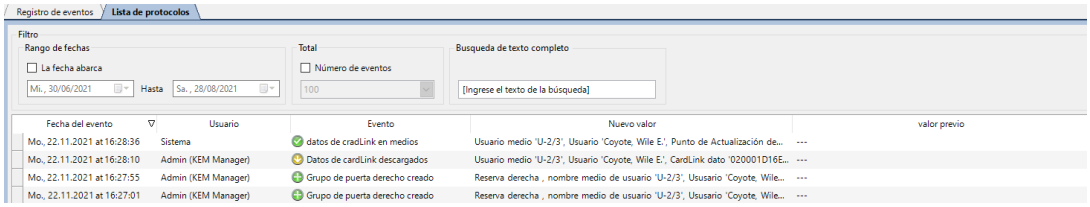
En la lista de auditorías se registran el momento y el usuario de cualquier modificación relativa a las autorizaciones que se haya realizado.

Para activar o desactivar la lista de auditorías, consulte el capítulo [▶ 6.2.2.1].

Se registran los siguientes datos:

- El momento de la acción
- El usuario con la sesión iniciada
- El tipo de evento
- Los valores previos al cambio
- Los valores posteriores al cambio

La lista de auditorías mostradas se puede limitar activando los filtros.



La lista solo se podrá imprimir si antes se ha exportado mediante un programa externo.

Las funciones de exportación requieren los derechos correspondientes.

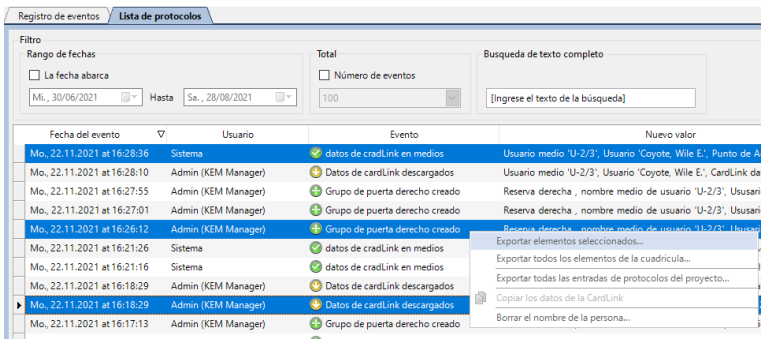
- El usuario con la sesión iniciada necesita el derecho "Exportar datos".

En el menú contextual encontrará otras funciones a su disposición:

- Exportar entradas seleccionadas. Consulte el capítulo [▶ 6.13.2.1]
- Exportar todas las entradas de la lista de auditorías. Consulte el capítulo [▶ 6.13.2.2]
- Exportar todas las entradas de auditoría del proyecto. Consulte el capítulo [▶ 6.13.2.3]
- Copiar los datos CardLink en el portapapeles. Consulte el capítulo [▶ 6.13.2.4]
- Borrar nombre de persona. Consulte el capítulo [▶ 6.13.2.5]

6.13.2.1 Exportar las entradas seleccionadas de la lista de auditorías.

La función exporta las entradas seleccionadas en un archivo CSV.



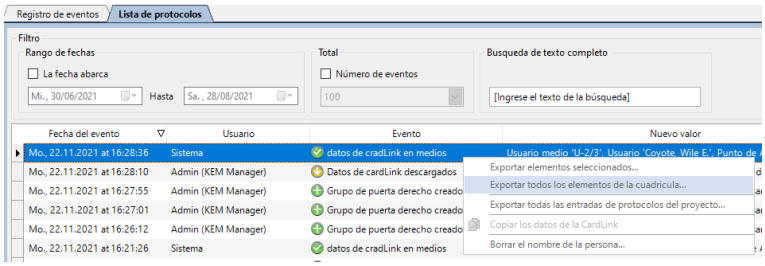
Procedimiento

1. Seleccione las entradas que desee.
2. Si selecciona varias entradas, abra el menú contextual haciendo clic con el botón derecho en una de las entradas.

3. Seleccione "Exportar entradas seleccionadas".
4. Seleccione el lugar donde se va a guardar y ponga un nombre al archivo.
5. Pulse "Guardar".
   ⇨ Las entradas seleccionadas se guardan.

6.13.2.2 Exportar todas las entradas de la lista de auditorías

La función exporta en un archivo CSV todas las entradas de la lista de auditorías presentes en KEM.

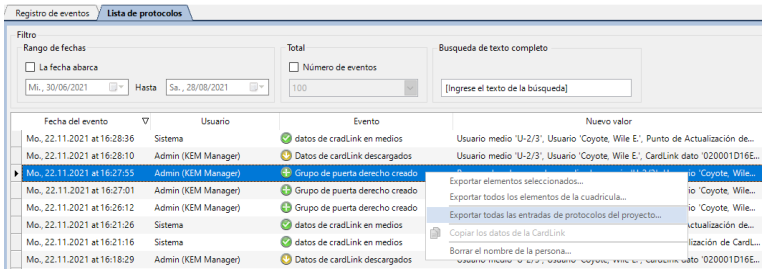


Procedimiento:

1. Abra el menú contextual con el botón derecho del ratón.
2. Seleccione "Exportar todos los elementos de la lista".
3. Seleccione el lugar donde se va a guardar y ponga un nombre al archivo.
4. Pulse "Guardar".
   ⇨ Las entradas se guardan.

6.13.2.3 Exportar todas las entradas de auditoría del proyecto

La función exporta en un archivo CSV todas las entradas de la lista de auditorías del proyecto. También se exportan las entradas que no estén presentes en KEM.



Procedimiento:

1. Abra el menú contextual haciendo clic con el botón derecho en una de las entradas.
2. Seleccione "Exportar todas las entradas de auditoría del proyecto".
3. Seleccione el lugar donde se va a guardar y el nombre del archivo.
4. Pulse "Guardar".
   ⇨ Los datos se guardan en un archivo CSV.

6.13.2.4 Copiar los datos CardLink en el portapapeles

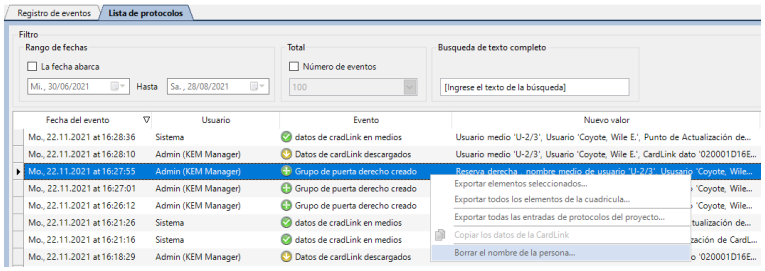
La función copia los datos CardLink de la entrada seleccionada en el portapapeles si es que la entrada contiene datos CardLink.

El servicio técnico utiliza esta función para, entre otras cosas, analizar los datos CardLink de un medio de usuario.

6.13.2.5 Borrar nombre de persona

El usuario que ha iniciado sesión requiere el derecho "Borrar nombre de persona".

El asistente borra el nombre de una persona de la lista de auditorías. Consulte el capítulo [▶ 17.1]. En lugar del nombre de usuario, se muestra el texto "Nombre borrado".



7 Mobile Access

Configuración de componentes y medios para Mobile Access en KEM.

AVISO

La llave digital de evolo smart disponible se sobrescribe en la aplicación Mobile Access.

Las autorizaciones del sistema evolo smart se pierden.

La llave digital de un sistema KEM sobrescribe la llave digital de un sistema evolo smart guardada en la aplicación Mobile Access. Con este proceso se pierden las autorizaciones de evolo smart. Entonces, el usuario estará autorizado en el sistema KEM, pero ya no lo estará en evolo smart.

- Los usuarios de la aplicación Mobile Access que ya cuenten con una llave digital de evolo smart u otro sistema KEM no necesitan una llave nueva, sino que utilizan la llave existente en KEM.
- Los usuarios envían la llave digital existente al administrador de KEM.

⇨ Las autorizaciones de evolo smart se mantienen.

⇨ El usuario también está autorizado en KEM.

En este capítulo solo se describen los pasos y opciones adicionales necesarios para configurar Mobile Access en KEM.
Mobile Access solo funciona con componentes compatibles con él a nivel de hardware.

7.1 Requisitos previos

Para el proyecto:

- V4
- Lista blanca o CardLink y lista blanca

Para los componentes:
Estos componentes son compatibles con Mobile Access:

- c-lever pro
- c-lever air
- c-lever compact
- Cilindros digitales
- Lector compacto
- Lector remoto

Los componentes deben cumplir los siguientes requisitos:

- SL2 como mínimo. Encontrará más información relativa al SL en la descripción del sistema evolo.
- Line E300, E320 o E321 a partir de la versión de firmware 42.32 (solo para NFC)
- Line E340, E360 o E361 (para NFC y Bluetooth).
- Solo se puede operar con Lista blanca o modo Mixto (autorizaciones en la Lista blanca). CardLink no es compatible.

Para la gestión:

- Debe disponer de un teléfono inteligente con Android o iOS.
- La aplicación VCP Installer debe estar instalada en el teléfono inteligente.
- Los componentes correspondientes deben ser compatibles con Mobile Access.
- Debe disponer de llaves digitales.

Para el usuario:

- Debe disponer de un teléfono inteligente con Android o iOS.
  - Android: Bluetooth y/o NFC
  - iOS: Bluetooth
- La aplicación dormakaba Mobile Access debe estar instalada en el teléfono inteligente.

7.2 Configurar teléfono inteligente como medio en KEM

AVISO

La llave digital de evolo smart disponible se sobrescribe en la aplicación Mobile Access.

Las autorizaciones del sistema evolo smart se pierden.

La llave digital de un sistema KEM sobrescribe la llave digital de un sistema evolo smart guardada en la aplicación Mobile Access. Con este proceso se pierden las autorizaciones de evolo smart. Entonces, el usuario estará autorizado en el sistema KEM, pero ya no lo estará en evolo smart.

- Los usuarios de la aplicación Mobile Access que ya cuenten con una llave digital de evolo smart u otro sistema KEM no necesitan una llave nueva, sino que utilizan la llave existente en KEM.
- Los usuarios envían la llave digital existente al administrador de KEM.

⇨ Las autorizaciones de evolo smart se mantienen.

⇨ El usuario también está autorizado en KEM.

Solo es compatible con las autorizaciones de Lista blanca. El uso de CardLink no es posible.

Configurado el teléfono inteligente como medio, se le pueden asignar usuarios y autorizaciones.

Requisitos previos

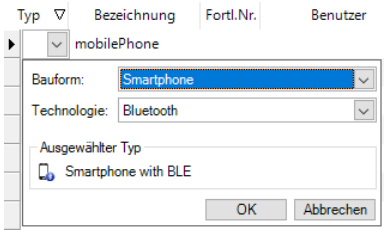
- Debe disponer de un teléfono inteligente.
- Debe disponer de una llave digital.

La llave digital consta de 20 caracteres hexadecimales y se muestra en el VALE DE LLAVE DIGITAL en ID móvil (1).

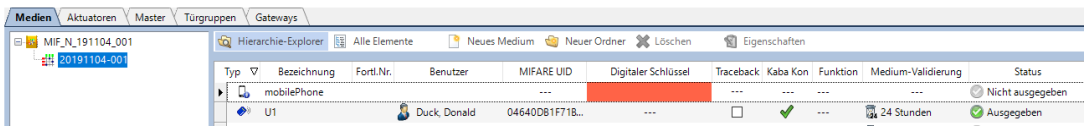
Ejemplo:

Procedimiento

1. En "Elementos básicos", seleccione la pestaña "Medios".
2. Cree un medio.



3. Seleccione "Teléfono inteligente" como tipo de medio.
4. Seleccione la tecnología Bluetooth y/o NFC según las capacidades del teléfono inteligente.



5. Agregue la llave digital.
   ⇨ Para importar llaves digitales, consulte.

⇨ Asigne el teléfono inteligente como medio a un componente con función Mobile Access.

7.3 Importar llaves digitales

AVISO

La llave digital de evolo smart disponible se sobrescribe en la aplicación Mobile Access.

Las autorizaciones del sistema evolo smart se pierden.

La llave digital de un sistema KEM sobrescribe la llave digital de un sistema evolo smart guardada en la aplicación Mobile Access. Con este proceso se pierden las autorizaciones de evolo smart. Entonces, el usuario estará autorizado en el sistema KEM, pero ya no lo estará en evolo smart.

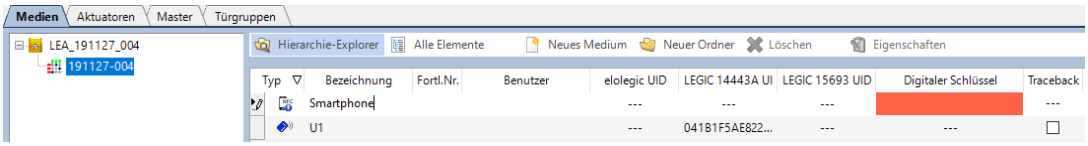
- Los usuarios de la aplicación Mobile Access que ya cuenten con una llave digital de evolo smart u otro sistema KEM no necesitan una llave nueva, sino que utilizan la llave existente en KEM.
- Los usuarios envían la llave digital existente al administrador de KEM.

⇨ Las autorizaciones de evolo smart se mantienen.

⇨ El usuario también está autorizado en KEM.

Las llaves digitales se introducen en KEM de distintas formas:

- Introducción manual
- Copiar y pegar
- En una lista de medios.
- Importe desde uno o más archivos PDF de vales.



7.3.1 Introducción manual

La llave digital está disponible electrónicamente como texto en un correo electrónico o en un PDF.

Introducción usando el teclado

Requisitos previos

- La página "Elementos básicos/medios" debe estar abierta.
- Debe haber un teléfono inteligente creado como medio de usuario.

Procedimiento

1. Seleccione de la lista el teléfono inteligente al que quiera agregar la llave.
2. La llave digital se registra en el teléfono inteligente seleccionado introduciéndola con el teclado en el campo "Llave digital".

Introducción copiando y pegando

Requisitos previos

- La página "Elementos básicos/medios" debe estar abierta en KEM.
- Debe haber un teléfono inteligente creado como medio de usuario.

Procedimiento

1. Abra el documento que contenga la llave digital.
2. Seleccione y copie la llave digital.
3. Vaya a la sección de KEM "Elementos básicos/medios".
4. Seleccione de la lista el teléfono inteligente al que quiera agregar la llave.
5. En la columna "Llave digital", agregue la entrada.

7.3.2 Importar desde archivo

Importar de una lista de medios

Los datos del teléfono inteligente y de la llave digital están registrados en una lista de medios. La lista de medios se importa al proyecto a través del menú "Inicio/importar".

Importar desde vale en PDF

Hay una o más llaves digitales registradas en un documento de vale. Luego se importan a KEM mediante un asistente.

Estado del vale

- Los vales están disponibles como documento PDF con capacidad de búsqueda.
- Los documentos PDF con imágenes escaneados se rechazan porque no son válidos. Este suele ser el caso cuando el PDF se ha impreso y escaneado nuevamente. En este caso, introduzca las llaves usando el teclado como se describe en "Introducción manual" [▶ 7.3.1].

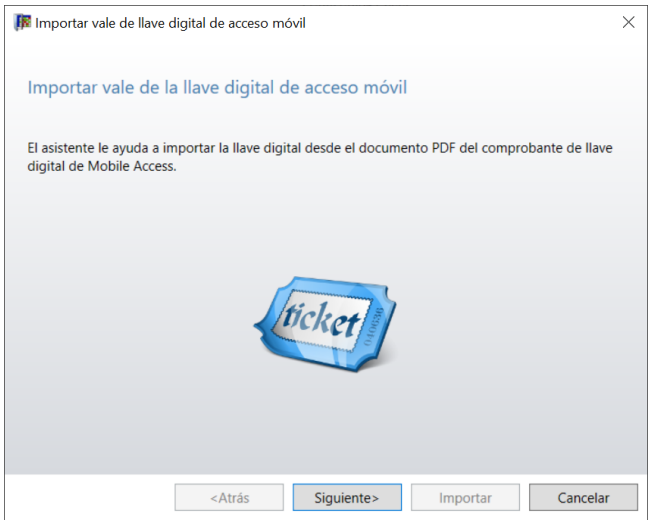
Puntos de partida para el asistente

El asistente se puede iniciar desde diferentes puntos del KEM:

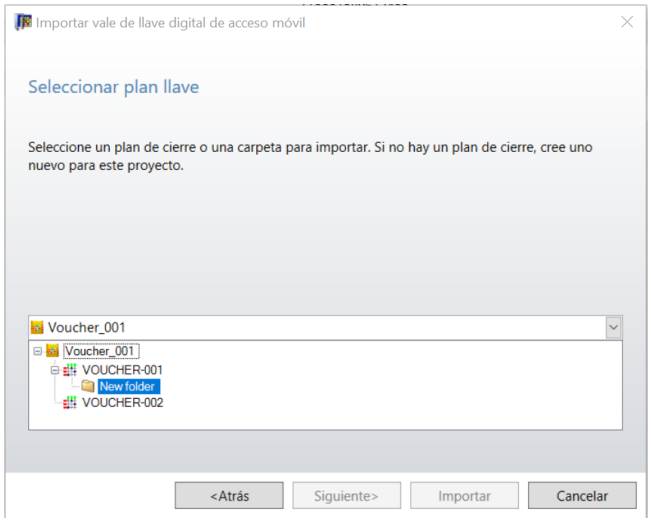
- Desde el menú "Importar", en "Inicio".
- Desde "Navegador/asistentes".
- Desde el menú contextual de un medio de Mobile Access (smartphone) en "Navegador/elementos básicos/medios".

Procedimiento

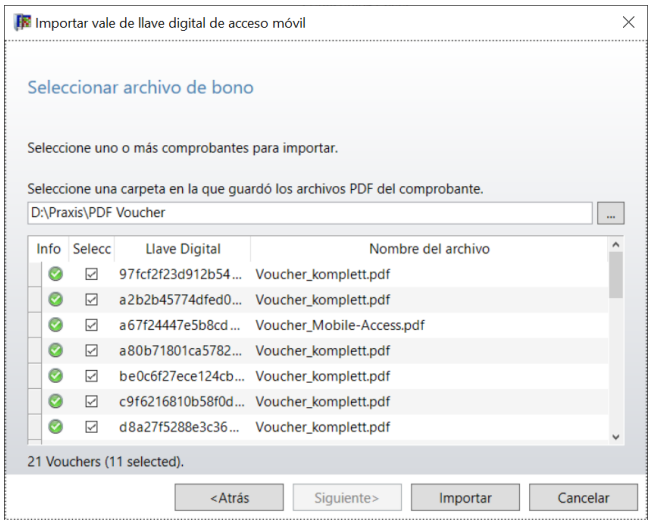
1. Inicie el asistente.



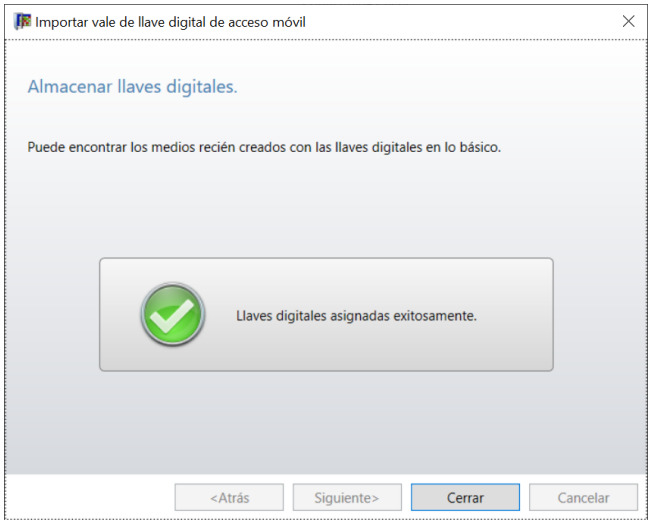
2. Haga clic en "Siguiente".
3. Si un proyecto contiene varios planes de cierre o carpetas:
   Seleccione el plan de cierre o la carpeta a la que quiera asignar las llaves digitales importadas.
   ⇨ Si el proyecto solo contiene un plan de cierre, se omitirá este paso.



4. Seleccione la carpeta que contenga el documento del vale.
5. Haga clic en "Siguiente".
6. Utilice las casillas de verificación para seleccionar la llave digital que se va a importar.
   - ⇨ De forma predeterminada, se seleccionan todas las llaves válidas dentro de la carpeta. Las llaves que ya se han importado se muestran como no válidas.
   - ⇨ Si la llave es válida o no válida se muestra en la columna "Información".
   - ⇨ No se pueden importar llaves no válidas.
   - ⇨ Las llaves solo pueden aparecer una vez en un proyecto.
7. Haga clic en "Importar".

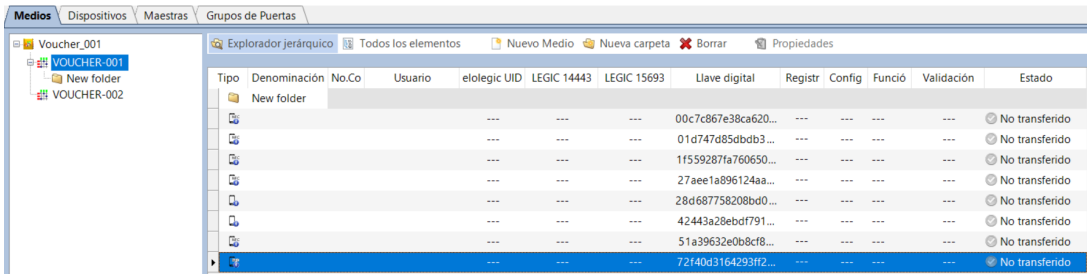


   - ⇨ Se realiza la importación.
8. Haga clic en "Cerrar".



⇨ El asistente se cierra.

⇨ Para cada llave digital se ha creado un medio de Mobile Access (smartphone) en la pestaña "Medios".



7.3.3 Importar vales a un medio de Mobile Access

Si se crea un teléfono inteligente como medio de usuario en KEM, la llave digital del archivo del vale se puede importar a este medio.

Estado del vale

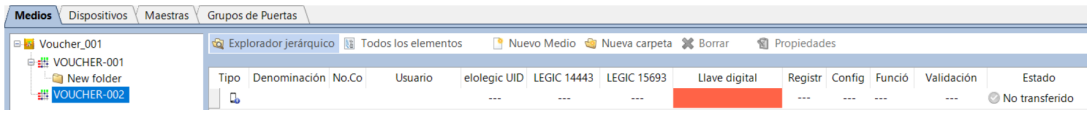
- Los vales están disponibles como documento PDF con capacidad de búsqueda.
- Los documentos PDF con imágenes escaneados se rechazan porque no son válidos. Este suele ser el caso cuando el PDF se ha impreso y escaneado nuevamente. En este caso, introduzca las llaves usando el teclado como se describe en "Introducción manual" [▶ 7.3.1].

Requisito

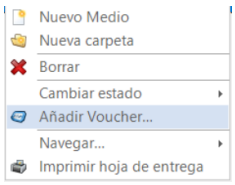
- El medio de usuario se crea como un teléfono inteligente.

Procedimiento

1. Vaya a "Navegador/elementos básicos/medios".

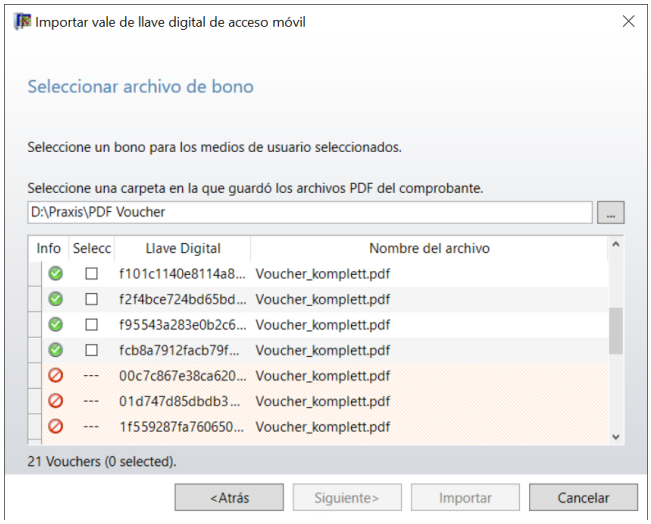


2. Utilice el botón derecho del ratón para abrir el menú contextual del medio de Mobile Access (smartphone) al que quiera agregar una llave digital.



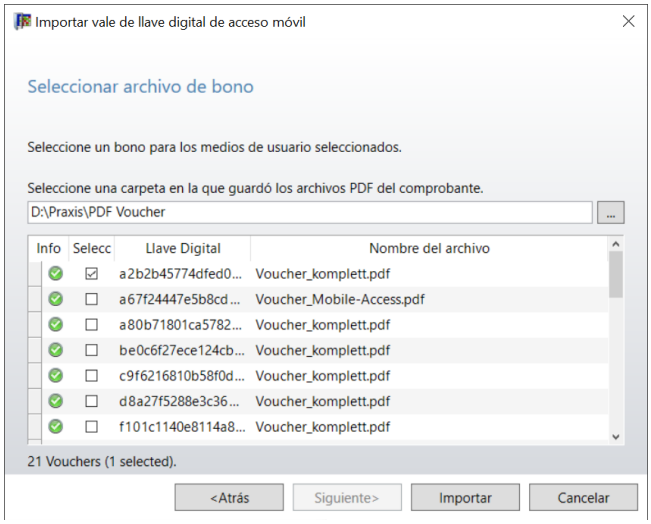
3. Seleccione "Agregar vale".
   ⇨ El asistente se inicia.
4. Seleccione la carpeta que contenga el documento del vale.

5. Utilice la casilla de verificación para seleccionar la llave digital que quiera importar.



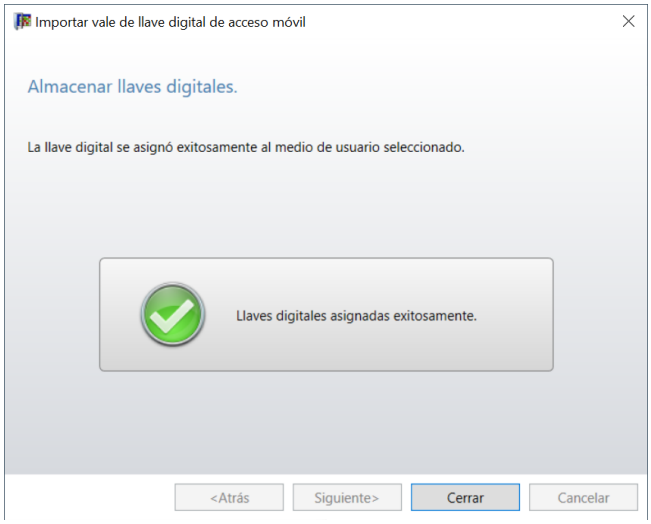
- ⇨ De forma predeterminada, no hay ninguna llave seleccionada dentro de la carpeta.
- ⇨ Solo se puede seleccionar una llave.
- ⇨ Si la llave es válida o no válida se muestra en la columna "Información". Se puede seleccionar una llave válida; las llaves que ya se han importado se muestran como no válidas.
- ⇨ Las llaves no válidas no se pueden seleccionar ni importar.
- ⇨ Las llaves solo pueden aparecer una vez por proyecto.

6. Haga clic en "Importar".



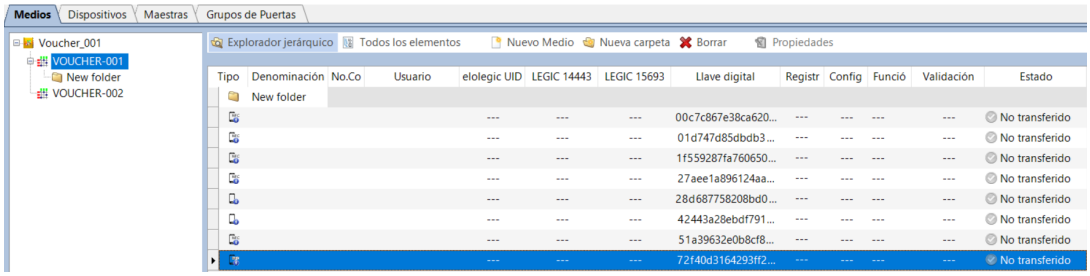
- ⇨ Se realiza la importación.

7. Haga clic en "Cerrar".



⇨ El asistente se cierra.

⇨ La llave digital se ha añadido al medio de Mobile Access.



7.4 Autorizaciones

Si hay teléfonos inteligentes y componentes configurados para Mobile Access, las autorizaciones se asignan a los componentes como los demás tipos de medios, como se describe en el capítulo.

7.5 Configurar componentes para Mobile Access

Si se cumplen los requisitos para Mobile Access, un componente se puede configurar en KEM de la forma habitual.

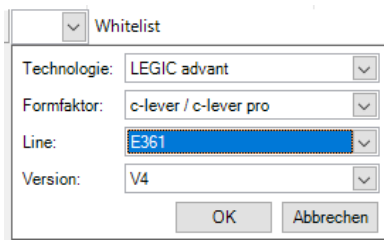
1 Configurar componente en KEM

2 Prepare el componente para Mobile Access con la aplicación VCP Installer.
Los VCP incluyen las llaves criptográficas.

3 Transfiera los datos de configuración de KEM al componente.

7.5.1 Crear componentes en KEM

Los componentes para Mobile Access se crean en el proyecto de un sistema de cierre en Elementos básicos/actuadores.



Al crear un componente en Line para Mobile Access, escoja de entre estas opciones:

- Line E3xx: Mobile Access (solo NFC)
- Line E340: Mobile Access (NFC y Bluetooth)

- Line E360: Inalámbrico y Mobile Access
- Line E361: Inalámbrico con vigilancia de puertas y Mobile Access

Mobile Access está disponible a partir de la versión de firmware 42.32.

7.5.2 Solicitar paquete de configuración LEGIC

Si no dispone del archivo VCP deseado, se debe solicitar a dormakaba. Encontrará la descripción específica en https://www.dormakaba.com/en/software-downloads/downloads-kem-software

7.5.3 Inicializar Mobile Access en el componente

Tras un restablecimiento INI, el paquete de configuración LEGIC se borra del componente.

Requisitos previos

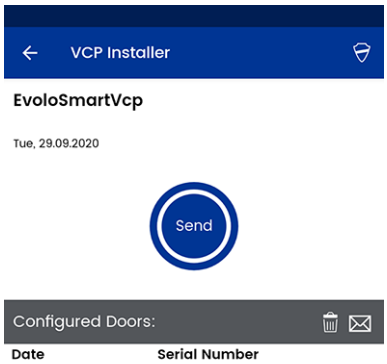
Smartphone
- La aplicación VCP Installer debe estar instalada y el proceso de registro con número de teléfono debe estar completo.
  Se ha introducido el código de registro obtenido por SMS.
- Tiene acceso a Internet (WLAN o datos móviles).
- Conoce el nombre y la contraseña del paquete de configuración LEGIC. Completado el proceso de registro, dormakaba le comunica el nombre y la contraseña del paquete.

Componente
- El componente debe estar listo para funcionar.
- Debe disponer de un medio Master.

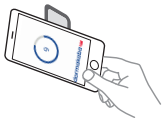
Procedimiento

Transferir el paquete de configuración LEGIC al componente

- Acercar el medio maestro a la antena durante aprox. 1 segundo.
- Inicie la aplicación VCP Installer en el teléfono inteligente.
- Seleccione el paquete de configuración LEGIC.
- Seleccionar "Enviar".



- Introduzca la contraseña del paquete de configuración LEGIC.



- Sostenga el teléfono inteligente delante del componente.

Señalización/significado		
	Componente/antena	**Smartphone**
Durante la transmisión de los datos:	• La luz verde se ilumina.	
Correctamente iniciado:	• Se emiten 3 señales acústicas.	• Verde • Número de serie del componente
El componente está inicializado.		
Incorrectamente iniciado:	• Se emite 1 señal acústica breve. • La luz roja se ilumina brevemente. • Se emite 1 señal acústica larga. • La luz roja se ilumina brevemente. • Se emite 1 señal acústica breve.	• Rojo

7.6 Transmisión

Los componentes que reciban autorizaciones Mobile Access se deben inicializar con la aplicación VCP Installer antes del primer uso de las autorizaciones.

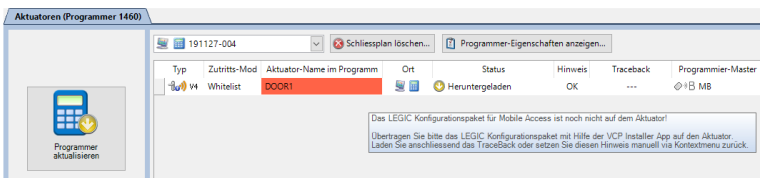
Los datos de Mobile Access no se pueden emplear si no se ha realizado la inicialización del componente mediante la aplicación VCP Installer.

Las autorizaciones guardadas en KEM se transfieren con el programador o de forma inalámbrica.

7.6.1 Confirmar VCP Installer

Para poder utilizar Mobile Access, el componente se debe inicializar con la aplicación VCP Installer.

El nombre del actuador aparecerá en rojo en el menú de transferencia si el componente todavía no ha recibido el paquete de configuración LEGIC. La ventana emergente incluye una advertencia.



La advertencia puede desaparecer de 2 formas:

- automática (recomendado)
- manual

Confirmación automática

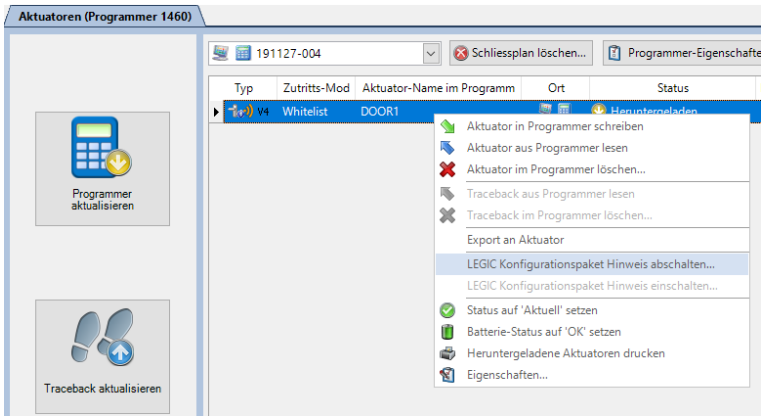
La advertencia desaparece automáticamente si, después de inicializar el componente con la aplicación VCP Installer, la Traceback del componente se carga y se actualiza en KEM.

Encontrará información sobre cómo cargar datos de Traceback en el capítulo [▶ 6.12].

Procedimiento:

1. Inicialice el componente con la aplicación VCP Installer. Consulte el capítulo [▶ 7.5.3].
2. Cargue la Traceback del componente con el programador o de forma inalámbrica.
3. Actualice la Traceback en KEM.
   ⇨ La advertencia desaparece y el nombre del actuador ya no aparece en rojo.

Confirmación manual



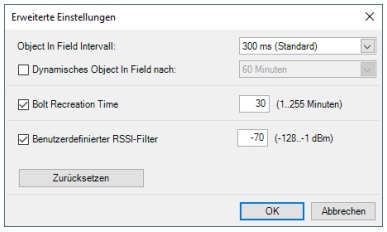
1. Inicialice el componente con la aplicación VCP Installer. Consulte el capítulo [▶ 7.5.3].
2. Seleccione el componente en cuestión.
3. Abra el menú contextual con el botón derecho del ratón.
4. Seleccione la opción "Eliminar advertencia de paquete de configuración LEGIC".
   ⇨ La advertencia desaparece y el nombre del actuador ya no está en rojo.

7.7 Propiedades

En este capítulo solo se describen las propiedades relevantes para Mobile Access.

7.7.1 Propiedades de actuador

7.7.1.1 Filtro RSSI



El filtro RSSI determina el valor límite de la intensidad de la señal y la distancia para que se reconozca un teléfono inteligente.

Si le es imprescindible modificar los ajustes para que distintos componentes queden diferenciados de forma segura, consúltelo antes con el servicio técnico.

Encontrará más información en PG Mobile Access.

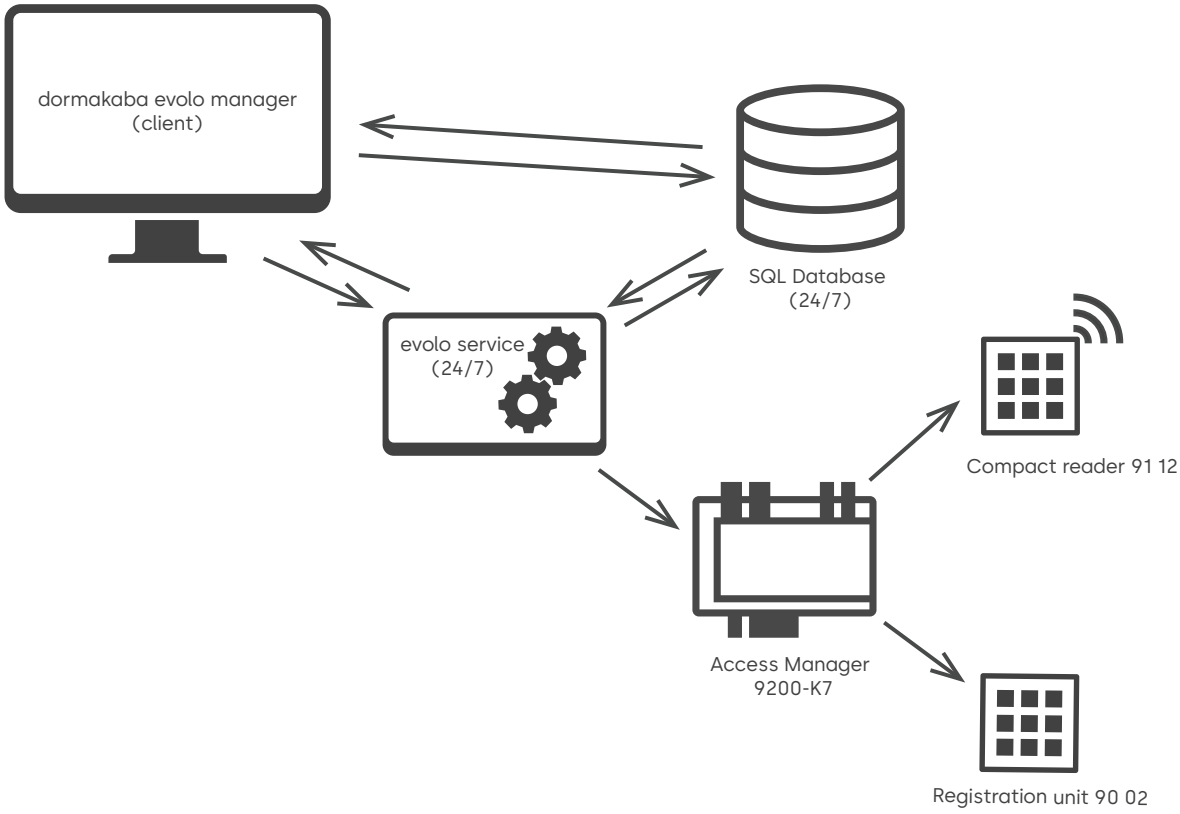
8 Dispositivos compatibles con código PIN

Introducción

Este capítulo describe cómo integrar, configurar y operar los dispositivos compatibles con PIN y código de puerta dormakaba 90 02 unidad de registro y dormakaba 91 12 Compact Reader en dormakaba evolo Manager (KEM). Incluye una visión general de la arquitectura de comunicación, el hardware compatible, la información de licencia, la gestión de credenciales y las posibilidades de trazabilidad. El uso de los dispositivos con código PIN amplía el control de acceso clásico basado en soportes con funciones de PIN y código de puerta dentro del entorno KEM.

Resumen

Los lectores de código PIN están conectados a un gestor de acceso 92 00-K7 B-Client AC30, que toma las decisiones de acceso de forma local (es decir, sin conexión). El gestor de acceso se comunica con KEM a través del Servicio evolo, que está instalado como componente de middleware de forma local o en un equipo remoto. KEM administra de forma centralizada los usuarios, las credenciales y las autorizaciones; el Servicio evolo transmite estos datos de forma segura (mediante HTTPS) al gestor de acceso y devuelve información de estado y eventos a la base de datos de KEM. Este enfoque garantiza una administración centralizada con decisiones de acceso descentralizadas y operativas sin conexión a nivel del gestor de acceso.



En la práctica diaria, el lector reenvía los datos al gestor de acceso en cuanto un usuario introduce un PIN, presenta un soporte LEGIC o MIFARE o utiliza Mobile Access. El gestor de acceso comprueba las autorizaciones o los registros de la Whitelist almacenados, así como los perfiles horarios. Si la autorización es válida, se activa la salida correspondiente y se concede al usuario el acceso a la zona. De lo contrario, se deniega el acceso. Todos los eventos se registran y se notifican a KEM para su trazabilidad.

8.1 Concepto de comunicación y seguridad

Los lectores compatibles con PIN no están conectados directamente a KEM. En su lugar, la comunicación se gestiona a través del Servicio evolo, que actúa como middleware entre KEM y el gestor de acceso. El flujo de comunicación es el siguiente:

- Los cambios de configuración y de autorización se crean en KEM.
- El Servicio evolo detecta estas actualizaciones y las transmite.
- El gestor de acceso almacena localmente los datos recibidos.
- Cuando se presenta una credencial, el gestor de acceso decide localmente sobre la concesión o la denegación del acceso.
- Los datos de eventos y la información de estado se notifican al Servicio dormakaba evolo y se almacenan en la base de datos SQL.

Si la conexión de red con KEM se interrumpe temporalmente, las decisiones de acceso siguen funcionando, ya que se toman localmente dentro del gestor de acceso. Por lo tanto, los usuarios obtienen acceso incluso cuando el dispositivo no tiene una conexión activa con KEM.

Modelo de seguridad
Toda la comunicación entre el Servicio dormakaba evolo y el gestor de acceso está protegida mediante HTTPS. Esto garantiza una transmisión cifrada de los datos de configuración y de autorización. Los puertos utilizados de forma predeterminada son HTTP: 8085 y HTTPS: 8086. En la práctica, la mayoría de las instalaciones se configuran exclusivamente mediante HTTPS.

8.2 Dispositivos compatibles

Los siguientes componentes de hardware son compatibles con la función PIN en el sistema KEM:

dormakaba unidad de registro 90 02
La unidad de registro 90 02 actúa principalmente como dispositivo de antena. Es adecuada para instalaciones en las que no se requiere Mobile Access. El acceso de los usuarios se habilita mediante:

- Acceso mediante soporte
- Acceso mediante PIN

Compact Reader 91 12
El Compact Reader 9112 amplía el conjunto de funciones mencionado anteriormente. Cuando se requiere acceso basado en smartphone, es la única opción adecuada. El acceso de los usuarios se habilita mediante:

- Acceso mediante soporte
- Acceso mediante PIN
- Mobile Access mediante smartphone

Gestor de acceso 92 00 K7 B-Client AC30
El gestor de acceso 92 00 K7 B-Client AC30 es el controlador de campo central en el concepto de lector PIN. Actúa como unidad de decisión que almacena las autorizaciones localmente y evalúa las credenciales sin necesidad de una conexión permanente con KEM. El dispositivo cumple las siguientes funciones:

- Recibe datos de configuración y de autorización desde KEM a través del Servicio evolo mediante comunicación HTTPS
- Almacena las entradas de la Whitelist
- Controla los dispositivos conectados, como antenas y lectores
- Registra los eventos de acceso concedidos y denegados y los sincroniza de vuelta con KEM

8.3 Licencias

La licencia define los límites operativos de cada gestor de acceso. Establece cuántos dispositivos y credenciales se pueden administrar. Cada licencia de gestor de acceso indica:

- Número máximo de antenas/lectores
- Número máximo de entradas de la Whitelist (registros maestros)

El límite superior de registros maestros suele situarse entre 8.000 y 10.000 entradas y rara vez supone una restricción en la práctica. El límite de dispositivos, en cambio, es notablemente más restrictivo y debe tenerse en cuenta en la planificación del sistema. La interfaz del sistema muestra el uso de la licencia para garantizar la transparencia durante la configuración.

Cada gestor de acceso funciona dentro de los límites de dispositivos con licencia. Para KEM 7.2 se aplican los siguientes valores:

- Por cada gestor de acceso se pueden utilizar un máximo de cuatro dispositivos, siempre que la licencia de dispositivos permita ese número.
- Las configuraciones de hardware compatibles pueden incluir dos dispositivos 90 02 como antenas (A y B), así como hasta dos lectores RS485.

8.4 Métodos de acceso

KEM admite varios métodos de acceso y permite así un uso flexible según los requisitos de seguridad del proyecto. Los métodos compatibles son:

- **PIN personal**

  Se asigna a un único usuario y no es visible para otros usuarios, tampoco en la interfaz de usuario de KEM.

- **Código de puerta**

  Un código de puerta se diferencia de un PIN personal en que se asigna a uno o varios lectores (y no a una persona) y puede compartirse entre varios empleados. Los códigos de puerta resultan adecuados, por ejemplo, para el personal de limpieza, las salas técnicas o las zonas de aparcamiento.

- **Soporte** (LEGIC Prime, LEGIC advant ISO 14443 A, LEGIC advant ISO 15693, MIFARE DESFire, MIFARE Classic)

  Estas tecnologías de credenciales garantizan la compatibilidad con las instalaciones existentes.

- **Credenciales móviles** (solo Compact Reader 91 12)

Todos los métodos de acceso pueden restringirse mediante perfiles horarios.

Las instalaciones MIFARE requieren que las Site-Keys estén almacenadas en el lector. Estas Keys no se transmiten automáticamente desde el gestor de acceso. Proceda de la siguiente manera:

Abrir la vista de transferencia en KEM.

Seleccionar la pestaña Actuadores (gestor de acceso).

Seleccionar la antena o el lector al que se debe enviar la Site-Key, abrir el menú contextual y seleccionar Enviar Site-Key...

Cuando se solicite, presentar la Tarjeta de Seguridad C en el lector de sobremesa.

Si un proyecto contiene lectores MIFARE pero no incluye una credencial maestra, pueden producirse problemas durante la puesta en marcha.

Perfiles horarios y modos de funcionamiento

Todos los métodos de acceso pueden restringirse mediante perfiles horarios configurables. Además, se admiten los siguientes modos:

- Funcionamiento de oficina
- Modo día/noche
- Configuraciones de zona horaria específicas del proyecto

8.5 Configurar KEM para dispositivos compatibles con código PIN

Para utilizar dispositivos compatibles con código PIN, realice los siguientes pasos en el orden indicado.

Instalar el Servicio evolo

El Servicio evolo es necesario como componente de middleware que permite la comunicación entre KEM y el gestor de acceso. Si aún no está disponible, proceda como se describe en la sección Instalar el servicio evolo [▶ 3.5]. El Servicio evolo puede instalarse en el mismo equipo que KEM o en un equipo independiente dentro de la misma red. La decisión depende de la infraestructura y de los requisitos de seguridad del proyecto correspondiente.

Configurar el Servicio evolo

Tras la instalación del servicio, continúe como se describe en la sección Configurar el Servicio evolo para el gestor de acceso [▶ 10.3].

Añadir un gestor de acceso

En el siguiente paso, añada un nuevo gestor de acceso a su proyecto.

1. En la interfaz de usuario de KEM, navegue a Ver, luego a Informaciones básicas, pestaña Gestor de acceso, y haga clic en Añadir nuevo gestor de acceso... En el asistente que aparece, haga clic en Siguiente.
   ⇨ Si la configuración de RF del gestor de acceso no está disponible, haga clic en Añadir de todos modos.
2. Introduzca la dirección IP y el nombre del nuevo gestor de acceso y haga clic en Siguiente.
3. En el siguiente paso se comprueba automáticamente la disponibilidad del nuevo gestor de acceso. Tras la confirmación, haga clic en Siguiente.
   ⇨ La configuración automática posterior puede tardar unos minutos.
4. Haga clic en Finalizar para completar el proceso.

Añadir antenas y lectores al gestor de acceso

1. Abrir las propiedades del gestor de acceso recién añadido.
2. En la pestaña Propiedades generales, seleccionar una zona horaria. En proyectos LEGIC, seleccionar adicionalmente las tecnologías LEGIC deseadas.
3. Configurar cada antena y cada lector conforme a la licencia. En las listas desplegables, seleccionar el tipo de lector, la entrada y la salida de señal físicas del dispositivo, la denominación para distinguir el dispositivo, así como el número y la denominación de la puerta. Tener en cuenta la indicación sobre el ajuste correcto del interruptor giratorio situado en la parte posterior del dispositivo físico.

Utilizar el interruptor DIP del Compact Reader para seleccionar las tecnologías MIFARE y LEGIC, así como las topologías RS-485 (topología en bus o en estrella).

Utilizar el interruptor giratorio para definir la dirección interna del dispositivo. Para la comunicación con la antena correcta, utilizar la posición 3 para el lector 1 y la posición 4 para el lector 2.

Las antenas están conectadas directamente a Ant. A o Ant. B en el gestor de acceso. No se requiere ninguna configuración adicional.

Activar el acceso de usuarios

A los usuarios se les concede acceso a puertas, actuadores o componentes habilitando su soporte en el proyecto, ya sea un código PIN, un código de puerta o un dispositivo móvil. Proceda de la siguiente manera:

1. En la interfaz de usuario de KEM, navegar a Soportes.
2. En el explorador jerárquico del proyecto, hacer clic en Nuevo Soporte.
3. Seleccionar el modelo y el tipo del soporte. Por ejemplo, elegir Código o PIN en las listas desplegables correspondientes. Tras la creación, editar el PIN o el código haciendo doble clic en la columna Denominación del nuevo PIN o código. Ejemplo: introducir el código PIN.
4. En la columna Usuario, abrir la lista desplegable y seleccionar el usuario al que se debe conceder acceso mediante este PIN.

En el caso de los códigos de puerta: los códigos de puerta no pueden asignarse a usuarios concretos.

1. Opcional: modificar el PIN o el código de puerta según se desee o utilizar uno generado automáticamente.

2. Autorizar el código PIN para su uso. Navegar a la vista Autorizaciones y hacer doble clic en la lista de la izquierda sobre el soporte de código PIN recién creado. Se abre una vista en la que se enumeran los actuadores para los que está activado este soporte. En los proyectos nuevos, esta lista está inicialmente vacía.
3. Desde la lista de actuadores situada en la parte izquierda de la interfaz de usuario, arrastrar y soltar los actuadores deseados sobre el soporte de código PIN. Por ejemplo, arrastrar una antena y un lector. Esperar hasta que los dispositivos se hayan programado automáticamente y estén disponibles para el soporte.

⇨ El usuario con el tipo de soporte de código PIN correspondiente está ahora activado para los dispositivos compatibles con código PIN seleccionados y obtiene acceso a los puntos de acceso que opera.

8.6 Proceso de usuario para el acceso en componentes o puntos de acceso compatibles con código PIN

1. Cuando el usuario se acerca a la puerta a la que necesita acceder, utilizar el medio de identificación asignado. Ejemplo: utilizar el código PIN personal.
2. Introducir el código PIN en el lector. Si el código es correcto, se concede el acceso y la puerta se abre. Esto se señaliza adicionalmente mediante una breve señal acústica y una luz indicadora verde parpadeante en el dispositivo.

9 Terminal

A partir de KEM V7.1, solo se admiten los terminales 9600-K6 y 9600-K7.

Antes de utilizar un terminal por primera vez, se debe instalar el servicio evolo.

- Instalar el servicio evolo [▶ 3.5]

9.1 Función

En un entorno CardLink, se puede utilizar un terminal para asignar centralmente derechos de acceso y validar los medios del usuario. La validación y los derechos de acceso se configuran en el software del sistema. Al presentar un medio de usuario, el terminal recupera los derechos de acceso proporcionados desde la base de datos KEM y los escribe en el medio o los elimina desde allí. El medio está validado.

La base de datos y el servicio evolo deben estar siempre disponibles para el terminal; de lo contrario, no se podrán proporcionar actualizaciones de CardLink. En ese caso solo se podrán validar los medios de usuario existentes cuyos datos de validación estén almacenados en el terminal. El número de posibles conjuntos de datos de validación almacenados en el terminal depende de la licencia del terminal adquirida.

La guía de instalación del terminal le proporcionará información detallada sobre el montaje y más indicaciones de instalación del terminal.

9.2 Instalación

Los siguientes pasos son necesarios para utilizar terminales en KEM:

1. Instalar el servicio evolo [▶ 3.5].
2. Habilitar el uso de terminales [▶ 9.2.1].
3. Añadir terminal al proyecto [▶ 9.2.2].

9.2.1 Activar terminal

Antes de que se puedan utilizar terminales en el KEM, se debe preparar el uso de terminales.

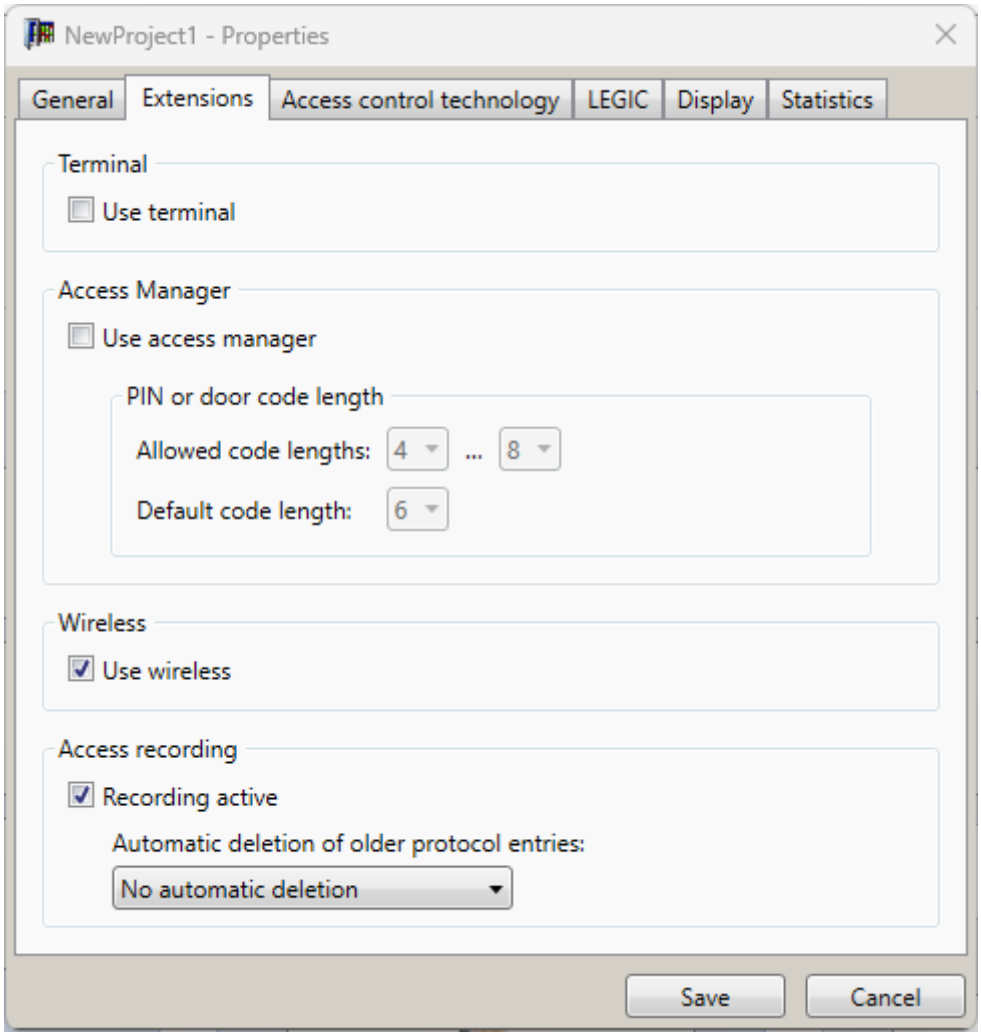
El uso del terminal solo se activa en las propiedades del proyecto una vez que el asistente se ha ejecutado correctamente.

Inicie KEM como administrador si el servicio evolo está instalado en un ordenador remoto. Esto solo es necesario para la configuración.

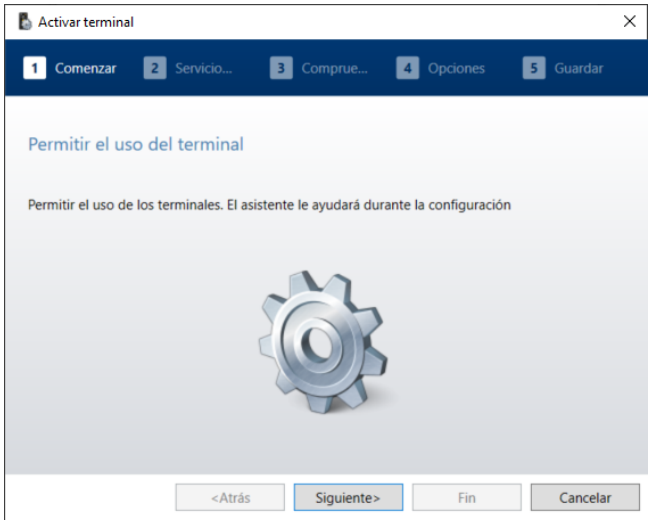
Se requieren derechos de administrador en el ordenador para configurar los puertos del cortafuegos. Esto solo es necesario para la configuración.

Procedimiento de activación

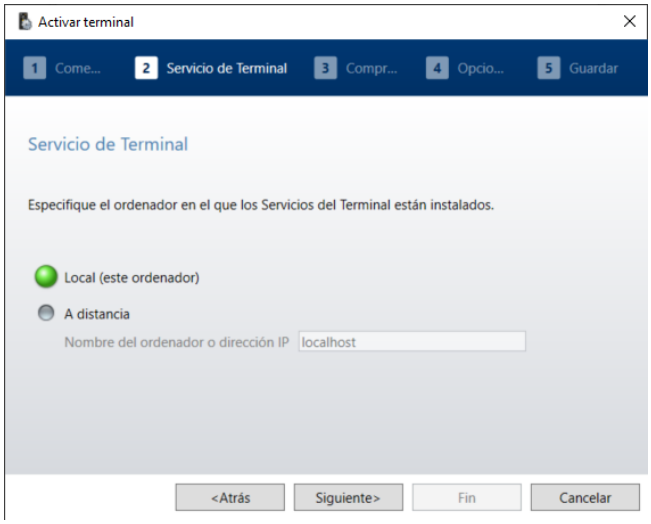
1. Abra las propiedades del proyecto (F4).
2. En la pestaña "Ampliaciones", active la casilla "Utilizar terminal".
   ⇨ Se inicia el asistente para configurar el uso del terminal en el KEM.



3. Siga el asistente.



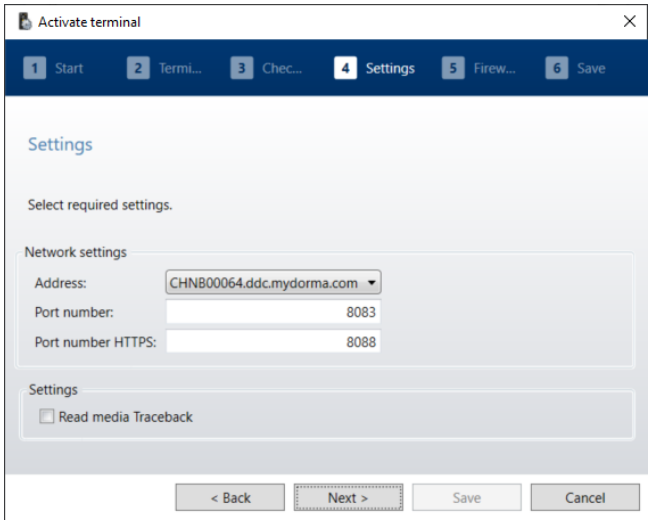
4. En el paso 2, especifique el ordenador en el que está instalado el servicio evolo.



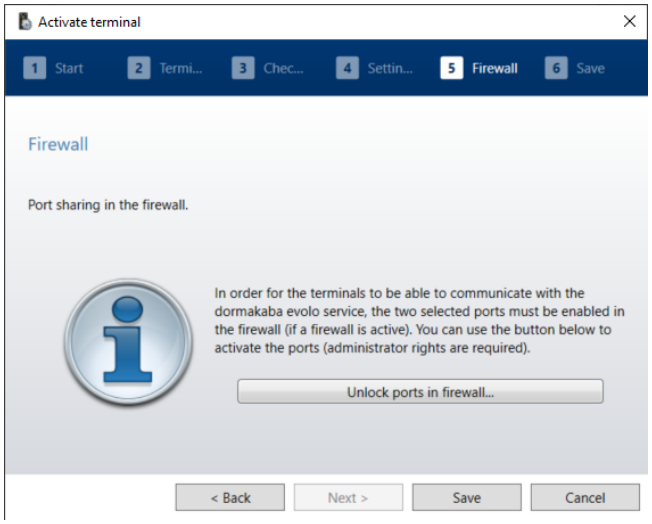
⇨ Local: El servicio evolo está instalado en el ordenador en el que también está instalado KEM.

⇨ Remoto: El servicio evolo está instalado en un ordenador diferente a KEM. Especifique el nombre o la dirección IP del otro ordenador.

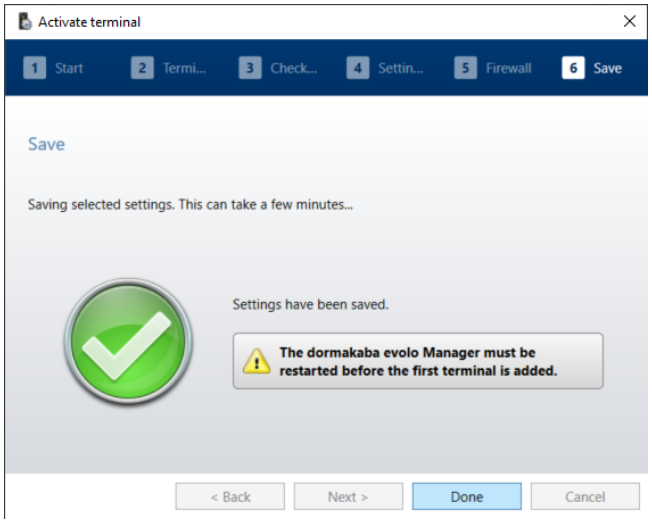
5. Haga clic en "Siguiente".
6. En el paso 4, seleccione la dirección IP o el nombre del ordenador en el que está instalado el servicio evolo.
   Para ello especifique el número de puerto. El puerto 8083 se utiliza como configuración predeterminada. Si el puerto ya está ocupado, se puede ajustar el número de puerto.
   Introduzca el número de puerto HTTPS. El puerto estándar para HTTPS es el 8084.
   Opcionalmente se puede activar la lectura del Traceback de medios.



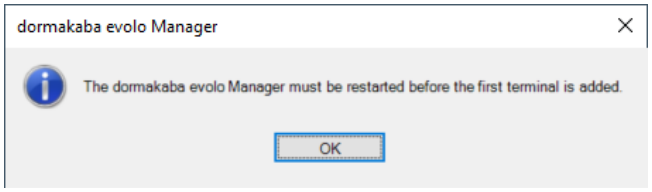
7. Haga clic en "Siguiente".
   ⇨ Si hay un cortafuegos activado en el ordenador, los puertos deseados deben activarse en el cortafuegos. El asistente llevará esto a cabo para el usuario. Para ello, el usuario necesita derechos de administrador en el ordenador.



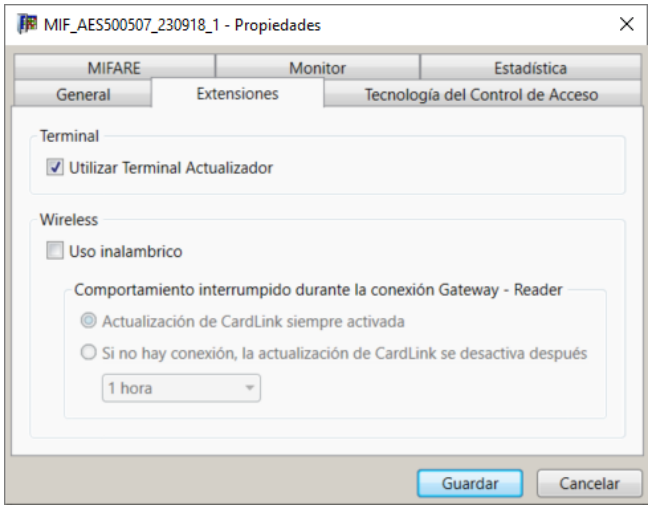
8. Haga clic en "Habilitar puertos del cortafuegos".
   ⇨ La activación se realiza en una ventana de comandos de Windows. Cuando el período de activación finalice, cierre la ventana pulsando cualquier botón.
9. Pulse "Guardar".
   ⇨ Los ajustes se guardan en KEM.
10. Haga clic en "Listo".



   ⇨ Antes de poner en servicio el primer terminal, el evolo Manager debe cerrarse y reiniciarse para que los ajustes surtan efecto.



   ⇨ En las propiedades del proyecto, la casilla "Utilizar terminal" estará activada.



11. Pulse "Guardar".

⇨ La pestaña "Terminales" se agrega a Elementos básicos.

⇨ Ahora se pueden agregar terminales en "Elementos básicos/terminales" [▸ 9.2.2].

9.2.2 Añadir terminales

Información y requisitos

En el software del sistema, no es posible usar un terminal en varios proyectos. Acto seguido la configuración anterior se sobrescribirá para otro proyecto y el terminal ya no podrá utilizarse en el proyecto anterior.

Los terminales deben estar conectados a la red.

Se ha habilitado el uso de terminales en el proyecto.

Nuevo terminal en la red

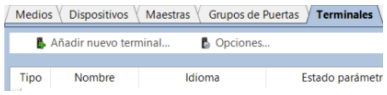
Un terminal 9600-K6 o 9600-K7 no configurado muestra lo siguiente en la pantalla cuando se conecta a la red y se enciende:

- Su propio número de serie
- Su propia dirección IP
- "Waiting for registration"

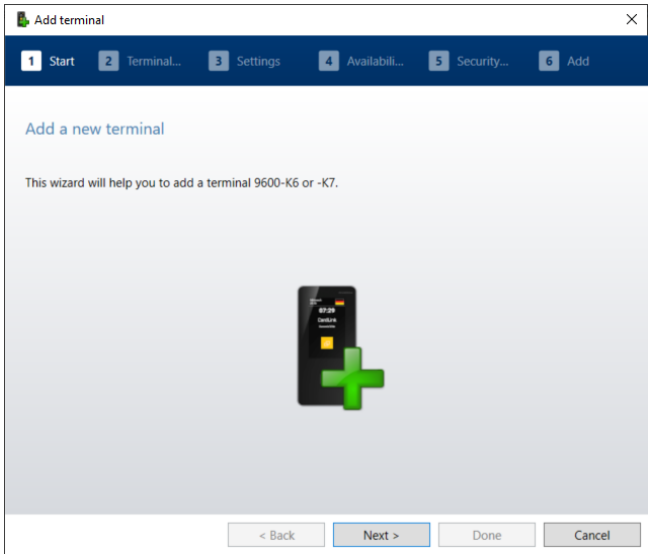
El terminal está listo para la configuración.

Procedimiento

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Terminales".
3. Haga clic en "Añadir nuevo terminal".



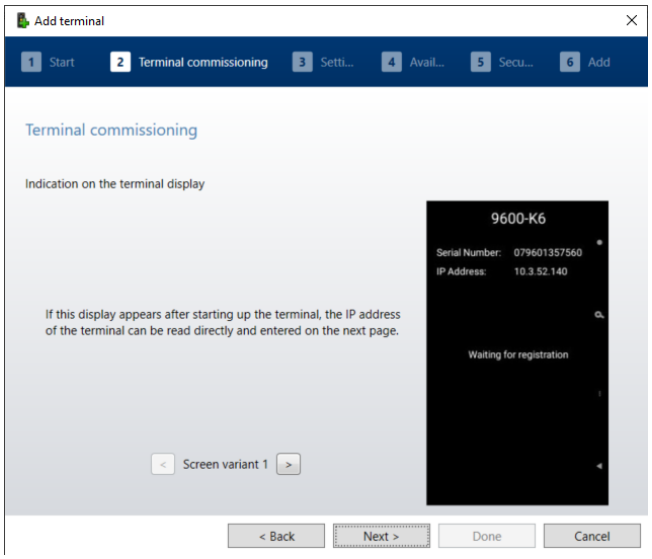
4. Siga el asistente.

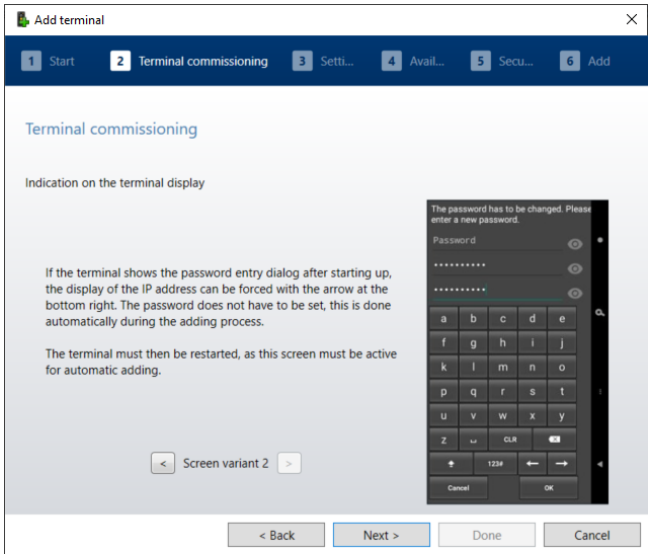


⇨ **Aviso:** Si no se ha leído la tarjeta de seguridad de este proyecto, debe confirmar que desea continuar sin leer la tarjeta de seguridad.

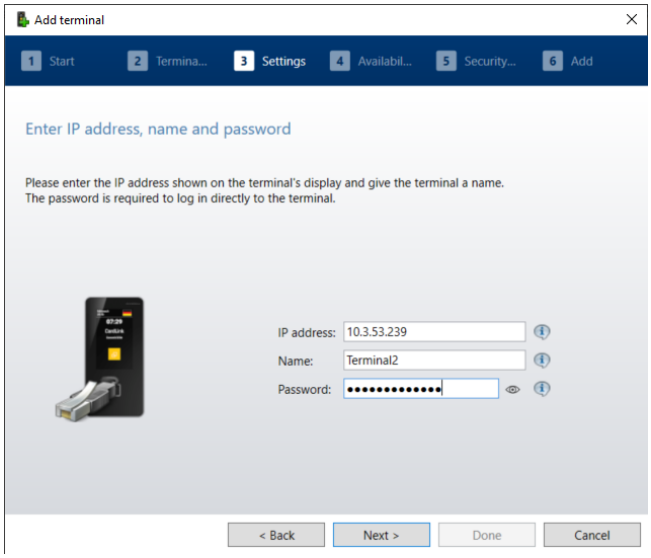
5. Haga clic en "Siguiente".

⇨ Se lee y se anota la dirección IP del terminal para el siguiente paso.

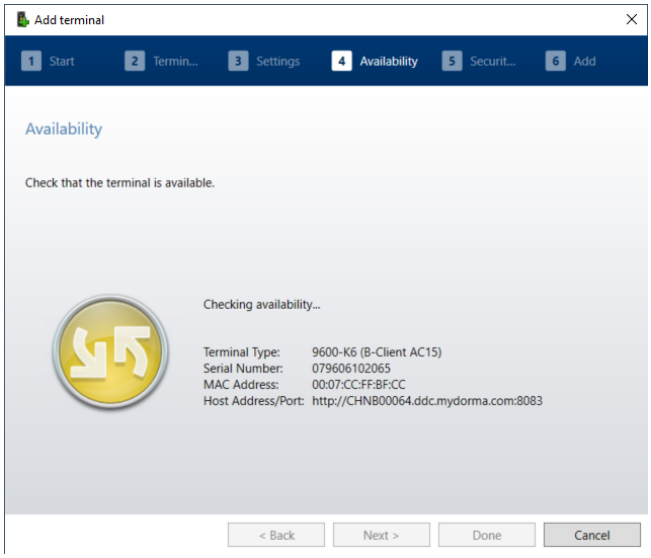


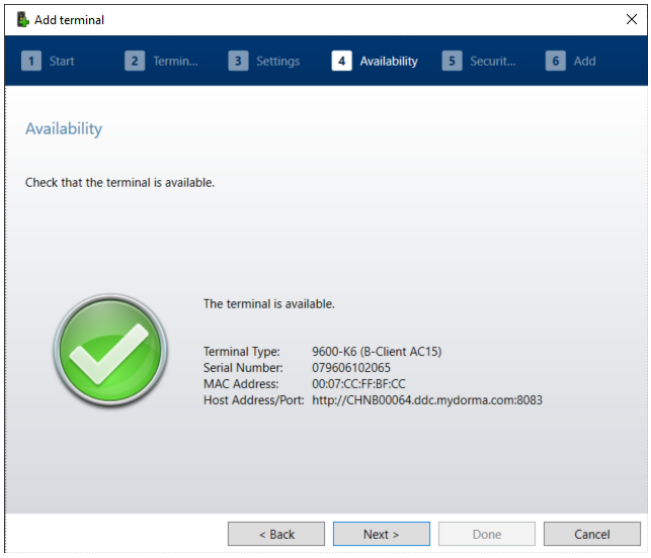


6. En el paso 3, introduzca la dirección IP del terminal, introduzca un nombre y asigne una contraseña para el terminal.

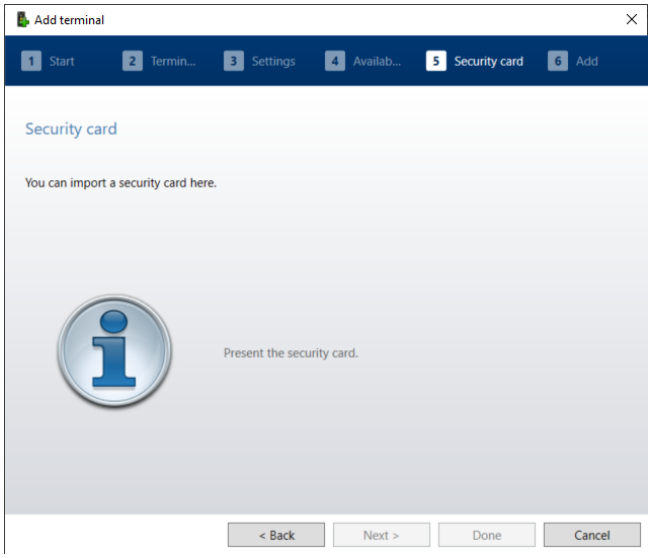


7. Haga clic en "Siguiente".
   ⇨ KEM comprueba si el terminal especificado está disponible en la red.

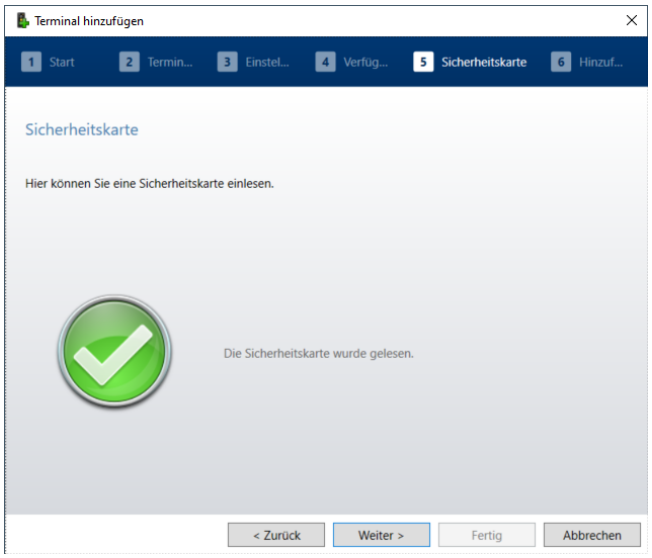




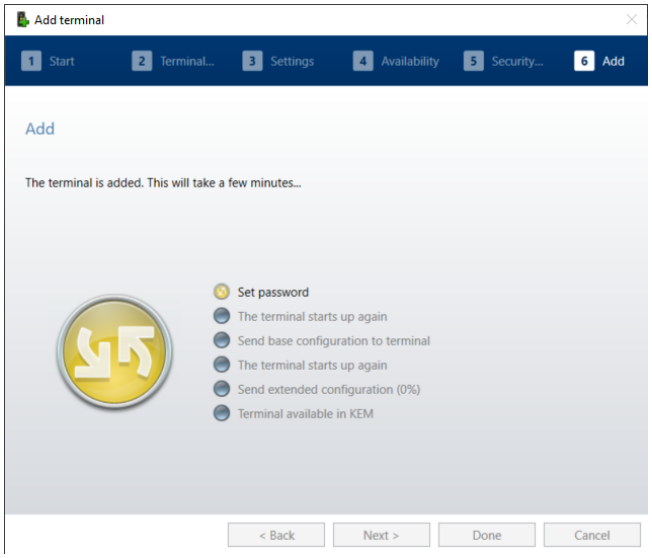
8. Haga clic en "Siguiente".



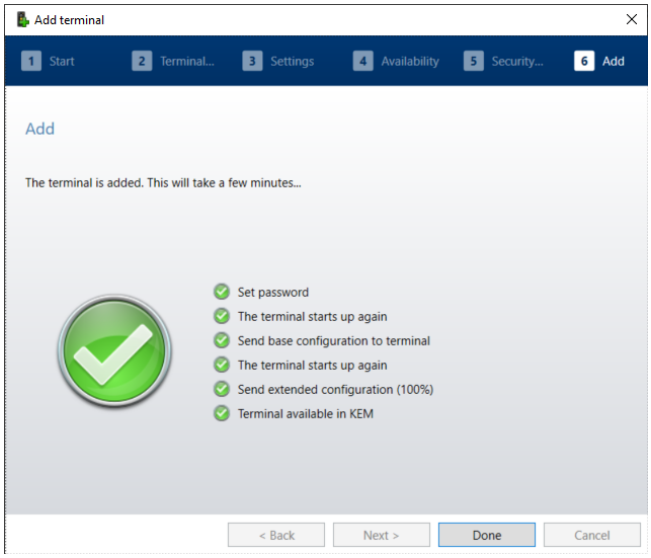
9. Lea la tarjeta de seguridad (en caso de que esté configurada para el proyecto).



10. Haga clic en "Siguiente".



⇨ El terminal se configura para su uso en KEM. Esto puede tardar unos minutos. Este proceso no puede cancelarse ni detenerse.



11. Haga clic en "Listo".

⇨ El terminal se ha añadido al proyecto.

⇨ El asistente finaliza.

Para el funcionamiento del terminal consulte.

Solo para proyectos LEGIC

El terminal todavía se debe lanzar en un proyecto LEGIC con la tarjeta de seguridad C2 para activar la autorización de escritura.

Para otorgar autorización de escritura, consulte cada terminal y presente la tarjeta de seguridad C2.

9.2.3 Restablecer/eliminar terminal

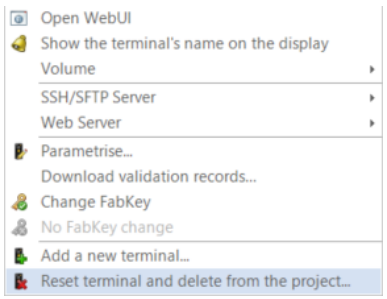
Proceso para eliminar un terminal de un proyecto.

Requisitos previos

- El terminal es accesible en el proyecto. El terminal se puede restablecer y eliminar del proyecto (recomendado).
- El terminal no es accesible en el proyecto. El terminal solo se puede eliminar del proyecto.

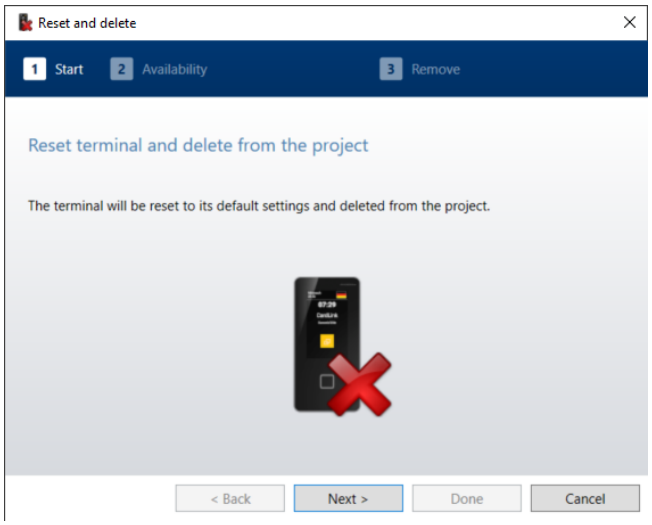
Procedimiento

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Terminales".
3. Seleccione en la lista el terminal que desea eliminar.
4. Haga clic con el botón derecho del ratón para abrir el menú contextual de la entrada del terminal.

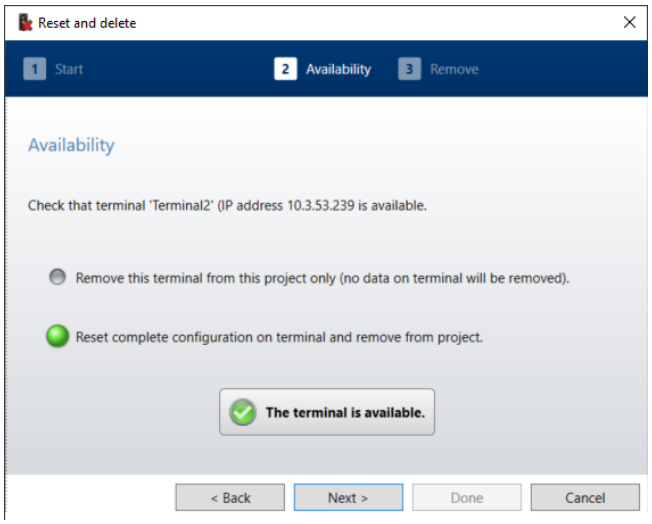


5. Seleccione el elemento del menú "Restablecer terminal y eliminar del proyecto".

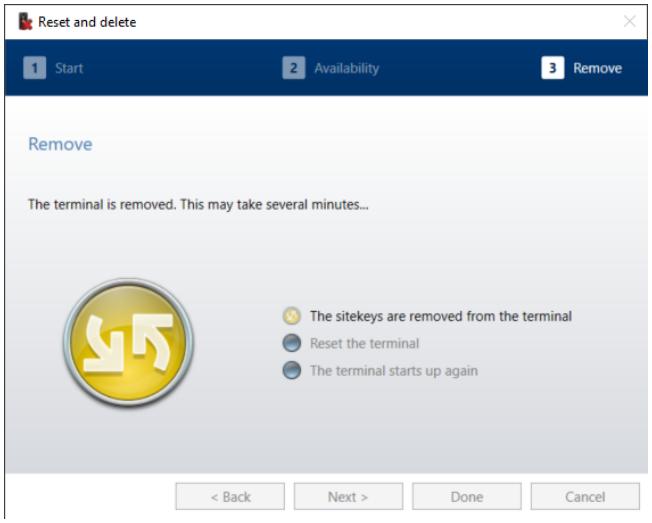
⇨ Se iniciará el asistente de eliminación de terminal.



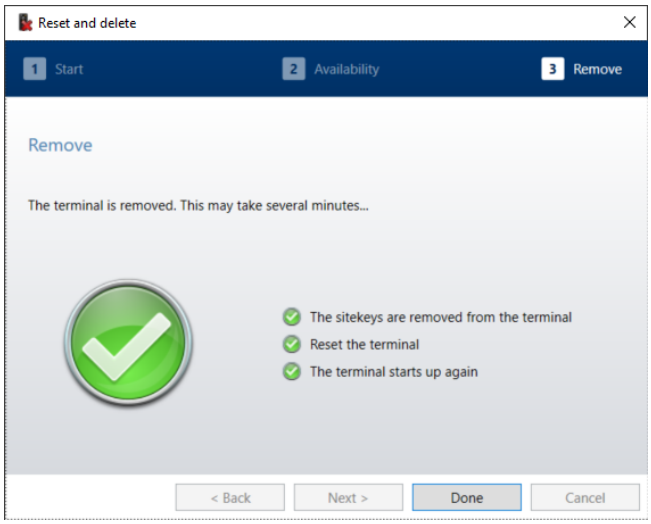
6. Haga clic en "Siguiente".
   ⇨ El asistente comprueba si se puede acceder al terminal.



7. Seleccione si solo se debe eliminar el terminal del proyecto o si también se debe restablecer el terminal. Si se restablece un terminal, todos los datos guardados en él se perderán y este podrá integrarse en otro proyecto.
8. Haga clic en "Siguiente".



⇨ El proceso no se puede cancelar.
El asistente elimina los datos del proyecto MIFARE o LEGIC correspondientes del terminal.



9. Haga clic en "Listo".
⇨ Se retira el terminal y finaliza el asistente.

9.3 Manejo

9.3.1 Programar medios

Antes de poder usar el terminal, todos los medios de usuario pertenecientes al proyecto deben programarse para su uso con el terminal.

Si los medios no se suministran preprogramados, deben programarse una vez con el KEM.

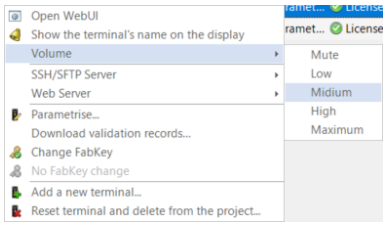
9.3.2 Volumen

El terminal ofrece la posibilidad de señalización acústica. El volumen puede ajustarse mediante el menú contextual del terminal correspondiente. El volumen se puede ajustar en 5 niveles. El ajuste del volumen debe realizarse por separado para cada terminal.

Procedimiento

1. En Básico/Terminales, seleccione el terminal cuyo volumen quiera ajustar.
2. Abra el menú contextual con el botón derecho del ratón.

3. Despliegue la opción de menú "Volumen".
4. Seleccione el volumen deseado entre "Silencio" y "Máximo".



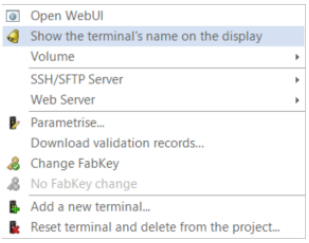
⇨ El terminal reproduce 4 tonos al volumen seleccionado.

9.3.3 Servidor SSH/SFTP

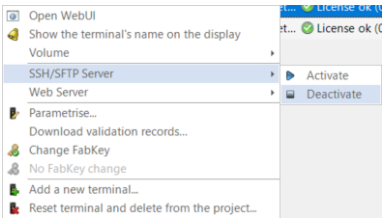
El servidor SSH/SFTP del terminal puede activarse o desactivarse. Tras la configuración para KEM, el servidor está desactivado por defecto y puede activarse/desactivarse manualmente aquí.

Procedimiento

1. En Básico/Terminales, seleccione el terminal cuyo servidor SSH/SFTP quiera activar o desactivar.
2. Abra el menú contextual con el botón derecho del ratón.



3. Despliegue la opción de menú "Servidor SSH/SFTP".



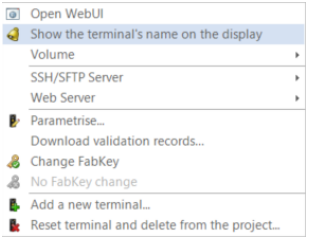
4. Seleccione "Activar" o "Desactivar".
   ⇨ Por defecto está desactivado

9.3.4 Servidor web

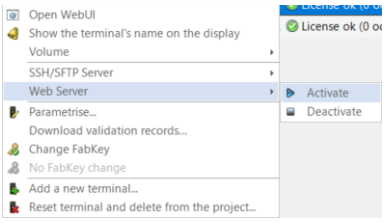
El servidor web del terminal puede activarse o desactivarse. Permite acceder a la interfaz web del terminal. Tras la configuración para KEM, el servidor está activado por defecto.

Procedimiento

1. En Básicos/Terminales, seleccione el terminal cuyo servidor web quiera activar o desactivar.
2. Abra el menú contextual con el botón derecho del ratón.



3. Despliegue la entrada "Servidor Web".



4. Seleccione "Activar" o "Desactivar".
   ⇨ Activado por defecto

9.3.5 Conjuntos de datos de validación

Los conjuntos de datos de validación son necesarios para la validación de medios en el terminal. Cuando se inicializa el terminal, se descargan los datos de validación existentes. KEM los actualiza automáticamente durante el funcionamiento. El proceso también se puede iniciar manualmente. Esto puede ser necesario, por ejemplo, si el terminal no está disponible durante un largo período de tiempo.

Procedimiento

1. En el menú "Elementos básicos/terminales", haga clic con el botón derecho para abrir el menú contextual del terminal.

2. Seleccione el elemento del menú "Descargar conjuntos de validación".
   ⇨ Los conjuntos de validación se cargan y se guardan en el terminal.

En línea/sin conexión

En funcionamiento en línea, el terminal tiene una conexión activa con el servicio evolo.

- El servicio evolo y la base de datos están en funcionamiento.
- KEM no es necesario.
- Los datos de acceso actuales están disponibles y se pueden escribir en el medio del usuario.
- Los medios de usuario se pueden validar.

En el modo sin conexión no hay ninguna conexión con la base de datos.

- El servicio evolo no está en funcionamiento.
- KEM no es necesario.
- Los datos de acceso no se pueden actualizar en un medio de usuario.
- Los medios de usuario se pueden validar.

La cantidad máxima de medios que se pueden validar sin conexión depende de la licencia adquirida para el terminal.

- Si el tamaño de la licencia no es suficiente, se mostrará una advertencia en KEM.
- Solo se pueden validar los medios cuyo conjunto de datos esté almacenado en el terminal.

⇨ Recomendación: Dimensionar la licencia del terminal según el número de medios que se vayan a validar.

9.3.6 Cambio de clave de fabricación

Solo en proyectos MIFARE.

Los medios escritos por empresas de terceros reciben una clave de fabricación para este paso de producción con la que se programan los medios. Para el uso del usuario final, la clave de fabricación se reemplaza una vez por una clave de aplicación. Cada aplicación en un medio tiene su propia clave de fabricación, que es reemplazada por su propia clave de aplicación durante este intercambio. El cambio de los terminales conectados se puede activar en el menú contextual. La función está desactivada de forma predeterminada.

Si la función está activada, las llaves se intercambian la primera vez que se presenta un medio.

Activar

1. Vaya a "Elementos básicos/terminales".
2. Seleccione uno o varios terminales.
3. Abra el menú contextual con el botón derecho del ratón.

4. Seleccione el elemento del menú "Cambio de clave de fabricación activo".
   ⇨ La función está activada para todos los terminales.

Desactivar

1. Vaya a "Elementos básicos/terminales".
2. Seleccione uno o varios terminales.
3. Abra el menú contextual con el botón derecho del ratón.
4. Seleccione el elemento del menú "Sin cambio de clave de fabricación".
   ⇨ La función está desactivada para todos los terminales.

9.3.7 Parametrizar

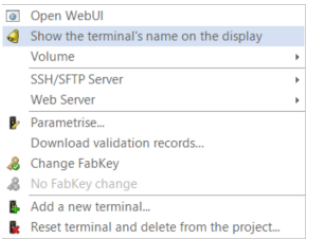
Información y requisitos

La tarjeta de seguridad de la tecnología usada se debe haber leído.

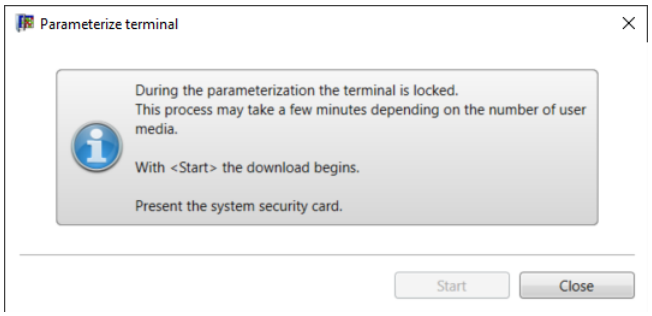
El terminal está instalado pero no parametrizado.

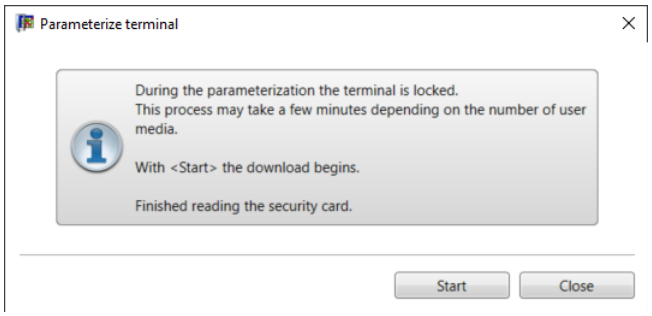
Procedimiento

1. Vaya a "Elementos básicos/terminales".
2. Seleccione un terminal.
3. Abra el menú contextual con el botón derecho del ratón.



4. Haga clic en "Parametrizar...".
5. Solo en MIFARE: Coloque la tarjeta de seguridad del sistema en el lector de sobremesa.





6. Haga clic en "Inicio".
   ⇨ Los datos se transfieren. La duración depende del número de medios de usuario configurados.
7. El asistente lleva acabo la parametrización.
   ⇨ En el último paso, el terminal realiza un reinicio. Este proceso puede durar algunos minutos.

⇨ El terminal está parametrizado y disponible en el software.

El terminal todavía se debe lanzar en un proyecto LEGIC con la tarjeta de seguridad C2 para activar la autorización de escritura.

8. Presente la tarjeta de seguridad C2 en el terminal y espere a las señales (1 pitido + 3 pitidos después de 20 s).
   ⇨ El terminal ha recibido su autorización de escritura (lanzamiento) y se puede utilizar en el proyecto.
   Los proyectos MIFARE no requieren este paso.

9.4 Autorizaciones de CardLink

En el tipo de autorización de CardLink, las autorizaciones y los datos de validación para un medio de usuario se almacenan en el servidor de la base de datos y, en caso necesario, se recuperan del terminal si el medio de usuario correspondiente está disponible.

Una vez que los datos CardLink se transfieren al servidor de la base de datos, KEM ya no es necesario.

Procedimiento (ejemplo)

1. Vaya a "Autorizaciones/CardLink".
2. Seleccione la pestaña "Medios de usuario".
3. Arrastre el medio hasta el campo superior derecho.
   ⇨ A continuación, este medio recibe sus nuevas autorizaciones a través del terminal.

4. Seleccione la pestaña "Grupos de puertas" o "Actuadores".
5. Arrastre y suelte un grupo de puertas o un actuador en el campo de la derecha.
   ⇨ Realizada la introducción, el conjunto de datos se encuentra en el estado "Nuevo". Los datos se transfieren directamente a la base de datos. Durante el funcionamiento, KEM no está obligado a recopilar datos del usuario. Cuando los medios de usuario han obtenido su autorización de acceso del terminal, el estado en el KEM cambia a Actual después de la siguiente sincronización.

Si el Traceback de medios está habilitado, los datos de rastreo se transmiten a KEM y se pueden ver.

9.5 Migración de proyectos desde V7.0

A partir de V7.1, los nuevos terminales solo pueden ponerse en servicio mediante SSH/SFTP y https. El certificado necesario lo proporciona el KEM. Además, el puerto para la comunicación segura debe estar definido y habilitado en el cortafuegos. El asistente ofrece la posibilidad de hacerlo. Este capítulo describe el proceso de migración de un proyecto de terminal creado en la versión 7.0 a la versión actual (a partir de la versión 7.1). Los proyectos con terminales antiguos no pueden migrarse.

Requisitos previos

- Se necesitan derechos de administrador en el ordenador para instalar el servicio evolo y el KEM.
- En V7.0, los terminales del proyecto correspondiente están correctamente instalados y activos.
- Están disponibles los archivos de instalación (msi) para el servicio evolo a partir de la versión 7.1.

- Están disponibles los archivos de instalación (msi) de evolo Manager a partir de la versión 7.1.

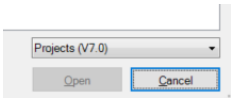
evolo Manager 7.0 y evolo Manager a partir de la versión 7.1 pueden instalarse en paralelo. El servicio evolo solo puede existir y estar activo una vez en un ordenador.

Procedimiento

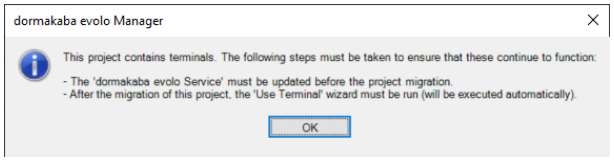
1. Actualice el servicio evolo a la versión actual.
2. Instale el evolo Manager versión 7.1 o superior.
   ⇨ Si las versiones de evolo Service y KEM no coinciden, aparece un mensaje de error.

Migración

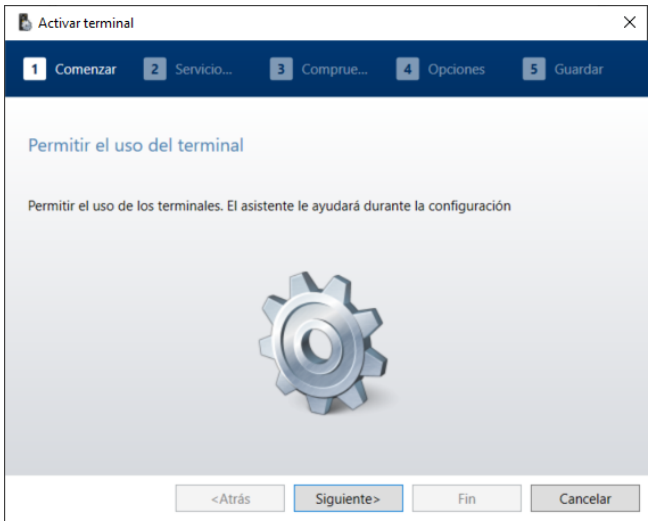
1. Inicie el evolo Manager actual.
2. Abra el proyecto que quiera migrar.
   ⇨ Filtre los proyectos a partir de la versión 7.0 en la selección de proyectos.



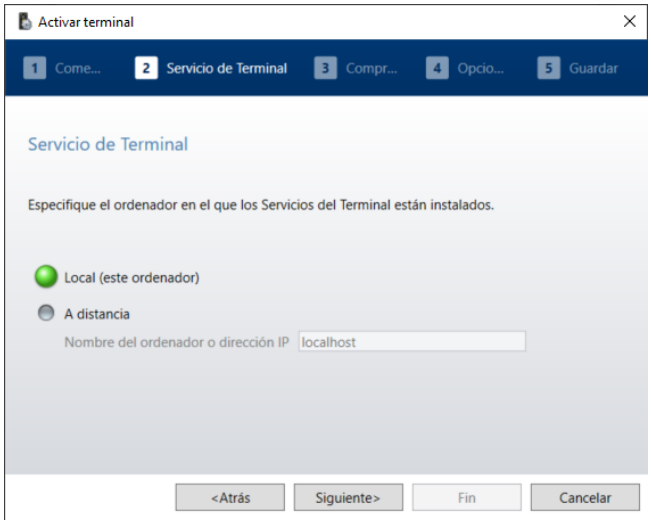
3. Seleccione el proyecto que quiera migrar.
   ⇨ KEM reconoce el proyecto más antiguo.



4. Pulse "OK".
5. Haga clic en "Sí" y migre el proyecto.
   ⇨ KEM pasa al asistente "Activar terminal" después de la migración. A continuación, se recoge y guarda la nueva información requerida.
6. Siga el asistente.



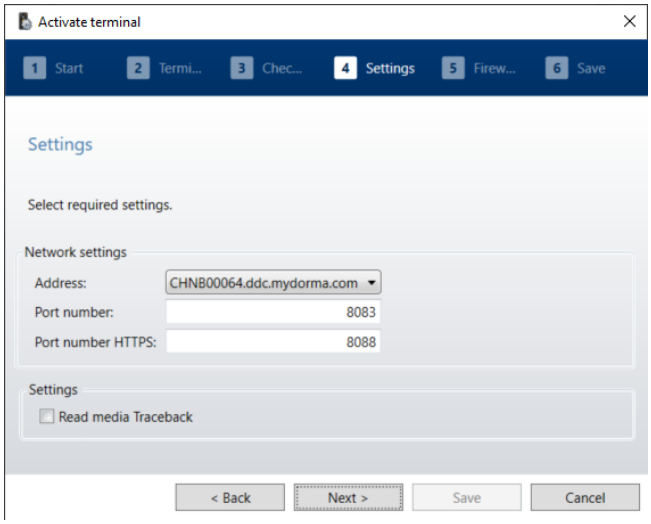
7. En el paso 2, especifique el ordenador en el que está instalado el servicio evolo.



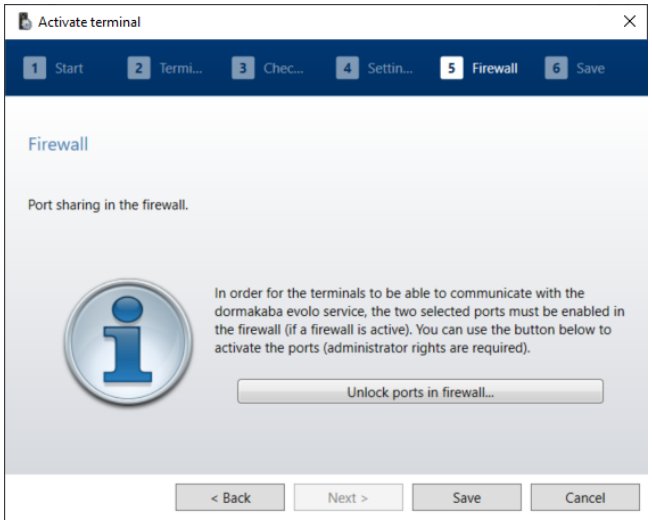
⇨ Local: El servicio evolo está instalado en el ordenador en el que también está instalado KEM.

⇨ Remoto: El servicio evolo está instalado en un ordenador diferente a KEM. Especifique el nombre o la dirección IP del otro ordenador.

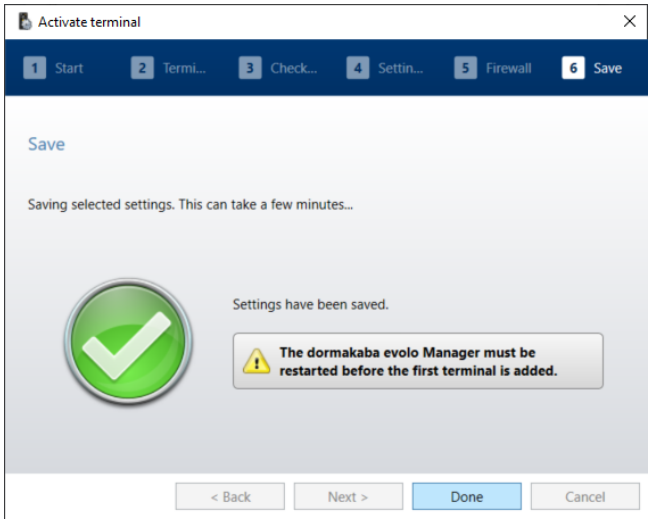
8. Haga clic en "Siguiente".
9. En el paso 4, seleccione la dirección IP o el nombre del ordenador en el que está instalado el servicio evolo.
   Para ello especifique el número de puerto. El puerto 8083 se utiliza como configuración predeterminada. Si el puerto ya está ocupado, se puede ajustar el número de puerto.
   Introduzca el número de puerto HTTPS. El puerto estándar para HTTPS es el 8084.
   Opcionalmente se puede activar la lectura del Traceback de medios.



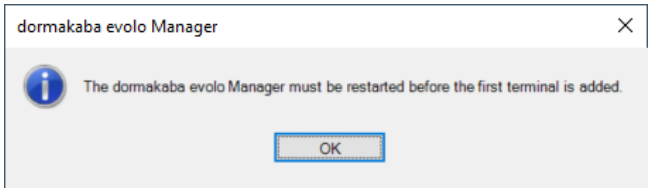
10. Haga clic en "Siguiente".
    ⇨ Si hay un cortafuegos activado en el ordenador, los puertos deseados deben activarse en el cortafuegos. El asistente llevará esto a cabo para el usuario. Para ello, el usuario necesita derechos de administrador en el ordenador.



11. Haga clic en "Habilitar puertos del cortafuegos".
    ⇨ La activación se realiza en una ventana de comandos de Windows. Cuando el período de activación finalice, cierre la ventana pulsando cualquier botón.
12. Pulse "Guardar".
    ⇨ Los ajustes se guardan en KEM.
13. Haga clic en "Listo".



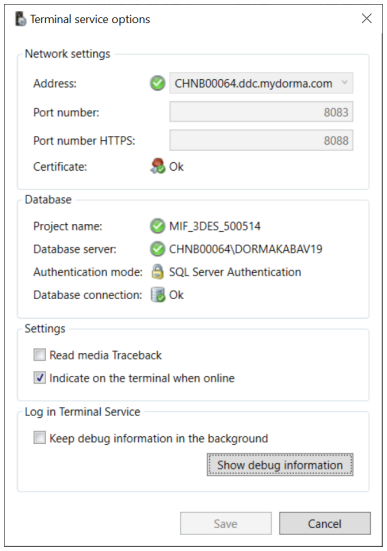
    ⇨ Antes de poner en servicio el primer terminal, el evolo Manager debe cerrarse y reiniciarse para que los ajustes surtan efecto.



⇨ Se abre el proyecto.

⇨ Compruebe el resultado de la migración.

En la pestaña Terminales de las opciones, compruebe si el puerto HTTPS establecido y el certificado están configurados.


Terminal service options
Network settings
Address:
CHNB00064.ddc.mydorma.com
Port number:
8083
Port number HTTPS:
8088
Certificate:
Ok
Database
Project name:
MIF_3DES_500514
Database server:
CHNB00064\DORMAKABAV19
Authentication mode:
SQL Server Authentication
Database connection:
Ok
Settings
Read media Traceback
Indicate on the terminal when online
Log in Terminal Service
Keep debug information in the background
Show debug information
Save
Cancel

10 Gestor de acceso

Para utilizar un gestor de acceso, el Servicio evolo debe estar instalado. Consulte Instalar el servicio evolo [▶ 3.5].

El dormakaba gestor de acceso 92 00 K7 es un dispositivo de control de acceso por hardware diseñado para sistemas de seguridad comerciales e industriales. Se trata de un controlador de acceso con capacidad de red que, como elemento central de un sistema de seguridad física, conecta entre sí lectores, puertas y software de administración. Su función principal consiste en comprobar, como terminal de control de acceso, si un soporte o una credencial (Tarjeta de Seguridad o smartphone mediante Mobile Access) dispone de las autorizaciones necesarias y, en caso de autorización, conceder el acceso al usuario.

10.1 Requisitos previos

Para que un gestor de acceso pueda incorporarse a un proyecto, deben cumplirse las siguientes condiciones:

- El Servicio evolo debe estar instalado y configurado, ya que es necesario para la comunicación entre KEM y el gestor de acceso. Consulte la sección Instalar el servicio evolo [▶ 3.5]. La versión del Servicio evolo instalado debe coincidir con la versión de KEM.
- Debe estar garantizada la conectividad de red, incluida una configuración IP correcta y los puertos abiertos (por ejemplo, HTTPS 8086), para que el dispositivo pueda ser localizado y comprobado. El gestor de acceso debe ser accesible y compatible, es decir, las comprobaciones de firmware y de comunicación deben superarse durante la configuración.
- Debe existir una licencia válida para el gestor de acceso 92 00 K7 B-Client AC30, ya que esta determina cuántos lectores y antenas se pueden añadir.

10.2 Funcionamiento

Debe haber una unidad de gestor de acceso implementada en el entorno de hardware existente. Para más información sobre la instalación física in situ de un gestor de acceso, consulte https://portal.dormakaba.com/, área *Downloads*; busque allí el manual técnico del gestor de acceso, en el que se describe el procedimiento de forma detallada.

La configuración y la incorporación a su proyecto se describen en las secciones Configurar el Servicio evolo para el gestor de acceso [▶ 10.3] y Configurar KEM para dispositivos compatibles con código PIN [▶ 8.5].

Ver también esto

Configurar KEM para dispositivos compatibles con código PIN [▶ 141]

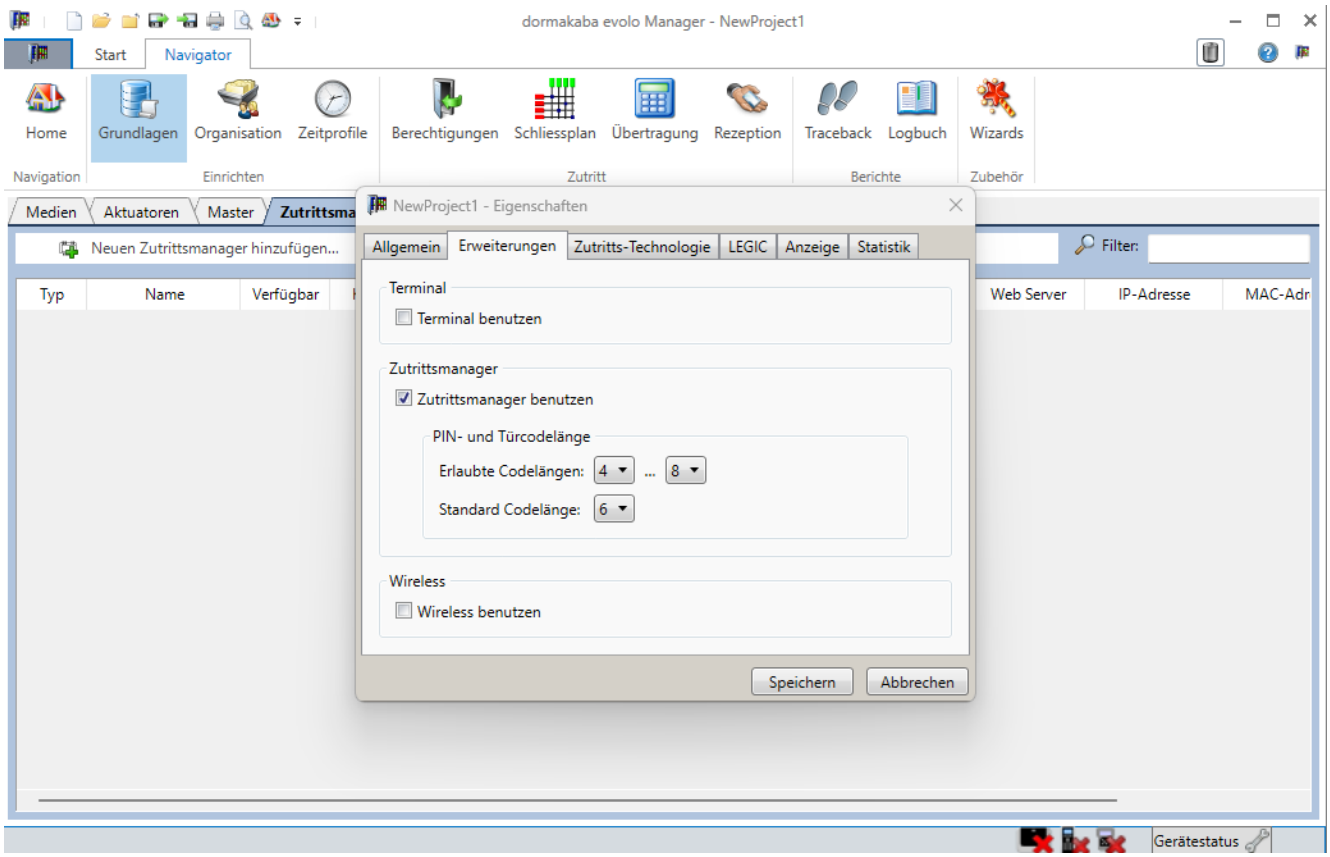
10.3 Configurar el Servicio evolo para el gestor de acceso

Para más información, consulte el capítulo Gestor de acceso.

Para utilizar dispositivos compatibles con código PIN en su proyecto, debe configurar el Servicio evolo para el gestor de acceso.

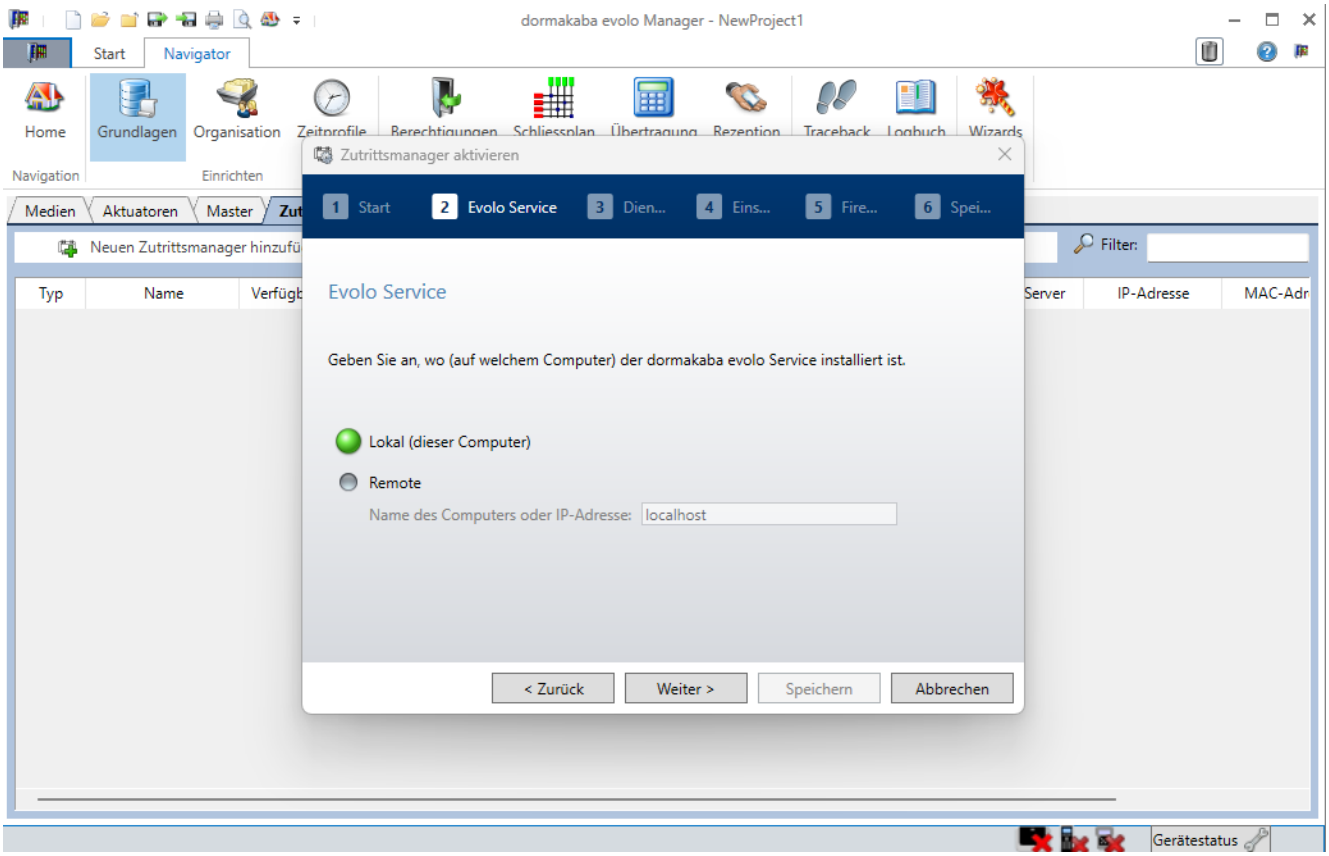
Comience por crear un nuevo dispositivo en KEM e introducir su dirección IP para que el sistema pueda localizarlo en la red. A continuación, KEM comprueba automáticamente la comunicación con el Servicio evolo y verifica la compatibilidad del dispositivo, incluido el estado del firmware. Tras una comprobación correcta, el gestor de acceso se integra e inicia su primera sincronización, que puede tardar unos minutos antes de estar operativo.

Procedimiento

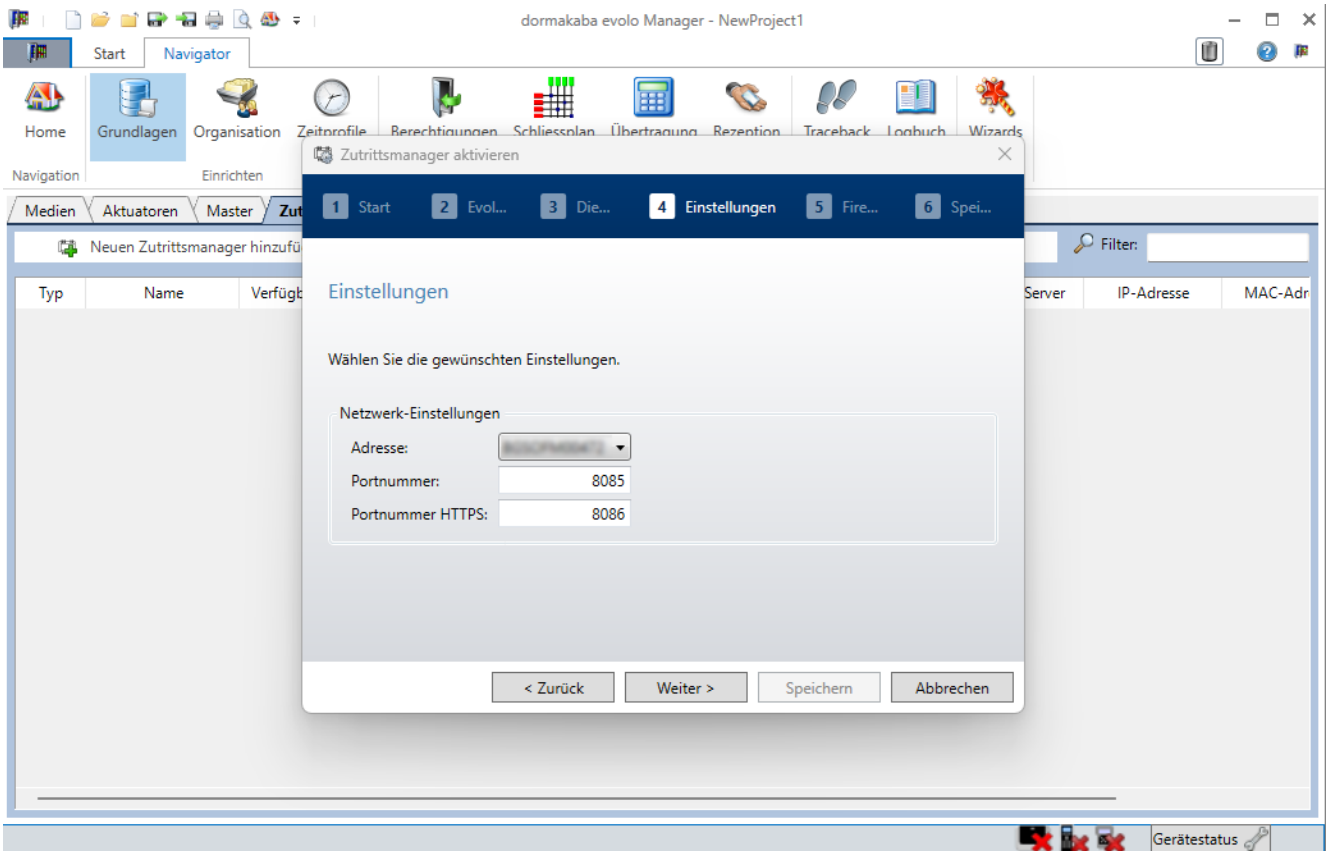


1. En la interfaz de usuario de KEM, pulsar *F4* para abrir las propiedades del proyecto y cambiar a la pestaña *Extensiones*.
2. Activar la casilla de verificación Usar gestor de acceso. Esto inicia el *asistente Activar gestor de acceso*. Hacer clic en *Siguiente*.

En los proyectos MIFARE, al añadir el gestor de acceso también deben añadirse Site-Keys.



3. Indicar dónde está instalado el Servicio evolo. En el caso de una instalación remota, introducir el nombre de host o la dirección IP y hacer clic en Siguiente.
   ⇨ Se comprueba si el servicio está presente y activo. Tras finalizar la comprobación, hacer clic en Siguiente.



4. Indicar la configuración de red y los parámetros del Servicio evolo. Introducir la dirección y los puertos HTTP y HTTPS.

5. Cuando se solicite, abrir los puertos necesarios en el cortafuegos. Utilizar la opción proporcionada, que ejecuta un script que añade una regla en el cortafuegos. Tras completar este paso, hacer clic en Guardar. Esto reinicia el Servicio evolo, lo que es necesario para su funcionamiento.
6. Reiniciar KEM para que los cambios surtan efecto.
7. Opcional: tras configurar el gestor de acceso, volver a la pestaña Extensiones. Mediante los menús desplegables correspondientes se pueden editar la longitud mínima y máxima del código de puerta, así como la longitud estándar del código. Esto también es posible en un momento posterior.
8. Hacer clic en Guardar para cerrar las propiedades modificadas del proyecto.

⇨ El gestor de acceso está ahora operativo. Si es necesario, puede añadirse a un proyecto como se describe en Configurar KEM para dispositivos compatibles con código PIN [▸ 8.5].

Ver también esto

Configurar KEM para dispositivos compatibles con código PIN [▸ 141]

11 Inalámbrico

Este capítulo describe la creación y puesta en marcha de componentes inalámbricos. Encontrará más información sobre el funcionamiento inalámbrico en:

- Manual de manejo del programador 1460
- Guía técnica de la gateway inalámbrica 90 40
- Pauta de planificación PG inalámbrico

11.1 Integrar gateway inalámbrica

Si una gateway ya está configurada para un proyecto, se puede utilizar para otro después de haberle realizado un restablecimiento INI.

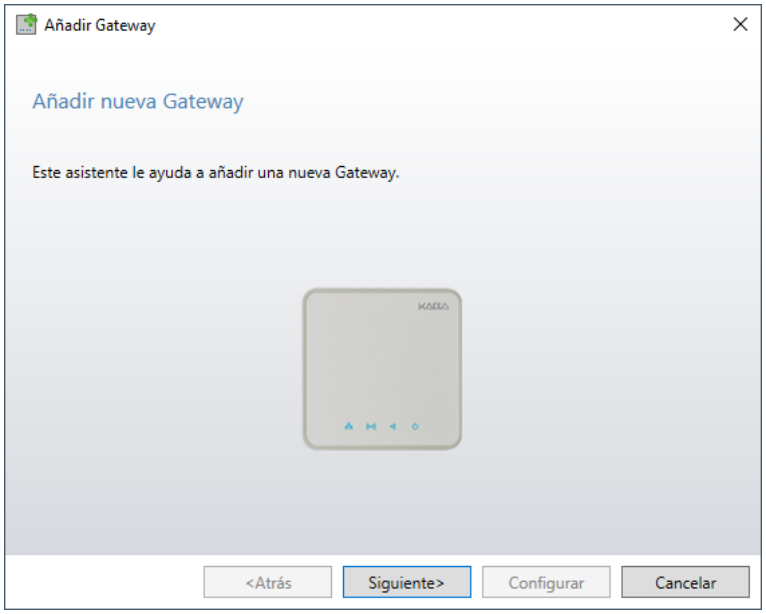
Preparar KEM:

1. Inicie el software KEM.
2. En el software KEM, abra las "Propiedades de proyecto" (F4).
3. En la pestaña "Ampliaciones", active la casilla "Utilizar capacidad inalámbrica".
4. Guarde la configuración.
   ⇨ La pestaña "Gateways" se añade a los Elementos básicos.
   ⇨ La pestaña "Actuadores (Inalámbrico)" se añade al menú "Transferencia".

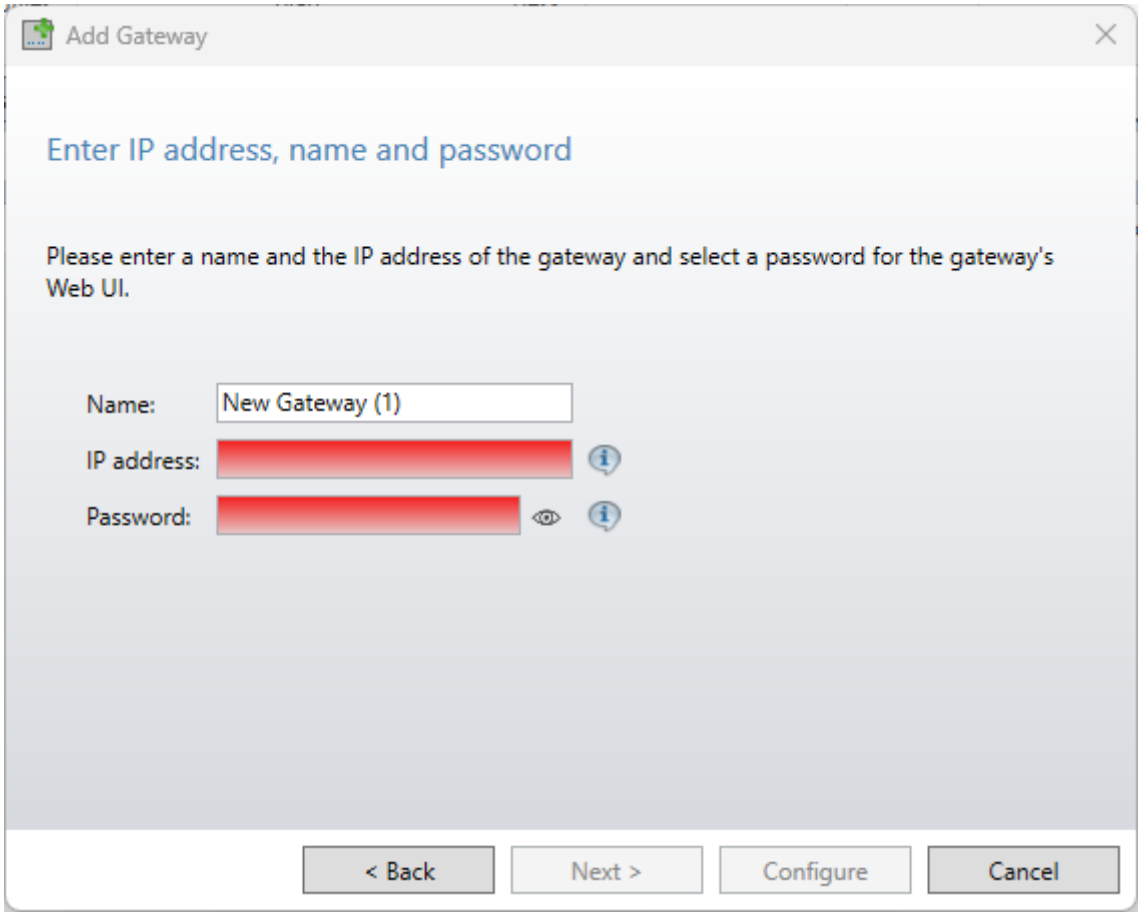
Añadir gateway en KEM:

✓ Debe conocer la dirección IP de la gateway.

1. Vaya a la pestaña "Gateways".
2. Pulse el botón "Añadir nueva gateway".



3. Siga el asistente.



Introduzca aquí la dirección IP por cable de la gateway.
Si no es posible asignar una dirección IP fija a la gateway inalámbrica, el servidor DHCP se debe parametrizar de tal forma que en cada nueva conexión con una gateway inalámbrica le asigne siempre la misma dirección IP.

4. Parametrice la gateway.
   ⇨ La vista del menú "Transferencia" y de la pestaña "Programador 1460" cambia a la pestaña "Actuadores (Inalámbrico)".

11.2 Editar los componentes inalámbricos

El modo Mixto inalámbrico todavía no es compatible con la gateway inalámbrica.

11.2.1 Configurar los componentes

La configuración de los componentes con la opción inalámbrica funciona de forma análoga a la de los componentes autónomos.

Además, debe tener en cuenta que:

- La capacidad inalámbrica solo se puede seleccionar en componentes que funcionen en modo V4.
  – En el campo "Tipo" de la pestaña "Actuadores", seleccione E32x de la lista.
- La opción Permitir capacidad inalámbrica debe estar activada
- En la actualización de CardLink mediante el lector remoto, debe seleccionar la opción "Actualización de CardLink" de la columna "Modo de acceso".
  En Legic, debe conceder la autorización de escritura al lector remoto para que los datos se puedan escribir en los medios. Véase Conceder autorización de escritura (lanzar) [▸ 11.2.2]

11.2.2 Conceder autorización de escritura (lanzar)

(Solo LEGIC)

En los siguientes casos hace falta una autorización de escritura:

- Validación de segmentos CardLink con escritura protegida en aplicaciones CardLink.

Requisito

- Para la autorización de escritura hace falta una tarjeta de seguridad C2.
- El componente debe encontrarse en funcionamiento normal y esperar una entrada por RFID.

Procedimiento

1. Presente el Master programador.
2. Presente la tarjeta de seguridad C2 durante unos 15 s.
   ⇨ Luz verde durante el proceso.
   ⇨ Señalización si el proceso es correcto: 3 pitidos
   Si ya se había concedido la autorización de escritura con la misma tarjeta de seguridad C2, se señalizará inmediatamente con 3 pitidos.
   ⇨ Ninguna señalización: La autorización de escritura **no** se ha concedido.
   Posibles causas
   - La tarjeta de seguridad C2 se ha retirado del campo RFID demasiado pronto.
3. Retire la tarjeta de seguridad C2 del campo RFID.

11.2.3 Módulo S, Pass-Lock o Escape-Return vía inalámbrica

Requisitos previos
El uso de las funciones Módulo S, Pass-Lock o Escape-Return vía inalámbrica requiere al menos las siguientes versiones de firmware:

Componente:	42.38
Gateway inalámbrica:	4.10.0

Las funciones se configuran en las propiedades del componente, en "Accesorios". Consulte el capítulo.

11.3 Puesta en marcha de componentes inalámbricos

Este capítulo describe cómo poner en marcha y parametrizar componentes inalámbricos mediante la gateway inalámbrica.

Para la puesta en marcha, debe realizar ciertos pasos en el componente y en la gateway.

11.3.1 Iniciar la puesta en marcha inalámbrica

Inicio de la puesta en marcha inalámbrica de la gateway.

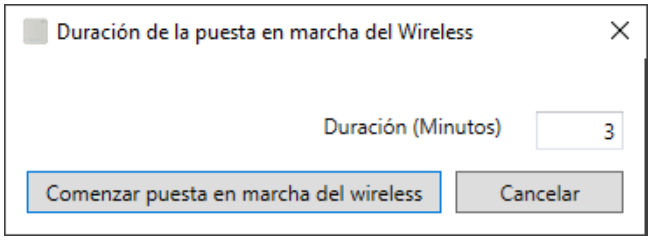
Para que los componentes se puedan conectar con la gateway, esta debe tener iniciada la puesta en marcha inalámbrica. La puesta en marcha se puede iniciar de esta forma:

- Con el software del sistema KEM
- En la interfaz web de la gateway

Para el funcionamiento con varias gateways, siempre inicie la puesta en marcha inalámbrica únicamente en una de ellas.
Los componentes se podrían conectar con una gateway no deseada.

Puesta en marcha con KEM

1. Inicie el software del sistema KEM
2. Vaya al apartado "Elementos básicos" de la pestaña "Gateways".
3. Seleccione la gateway.
4. Abra el menú contextual de la gateway seleccionada.
5. Active la opción "Iniciar la puesta en marcha inalámbrica...".



6. Establezca la duración de la puesta en marcha (en minutos).
   Período necesario para añadir/poner en marcha los componentes.
   ⇨ Durante este tiempo, los componentes se pueden conectar con la gateway.
7. "Iniciar la puesta en marcha inalámbrica..."
   ⇨ El componente debe conectarse con la gateway dentro del intervalo temporal configurado.
8. Conecte el componente mediante el programador [▶ 11.3.2] dentro del intervalo temporal configurado.

Si no se han podido poder en marcha todos los componentes necesarios dentro de intervalo temporal configurado, puede repetir el proceso.

Puesta en marcha mediante la interfaz web

La interfaz web de la gateway se puede iniciar a través del gestor de archivos o mediante KEM.

En el gestor de archivos, la gateway debe aparecer en Red.

1. En el gestor de archivos, seleccione la gateway para la puesta en marcha.
2. Inicie la interfaz web de la gateway.

⇨ La interfaz web de la gateway se inicia.

La gateway debe estar creada y configurada en KEM:

1. En KEM, seleccione la gateway para la puesta en marcha.
2. Abra el menú contextual de la gateway seleccionada haciendo clic en el botón derecho.
3. Seleccione la opción "Abrir WebUI".

⇨ La interfaz web de la gateway se inicia.

Después de iniciar la interfaz web de la gateway:

1. Inicie sesión en la gateway como administrador.
2. Active la función "Puesta en marcha inalámbrica".
3. Configure el tiempo para la puesta en marcha.
   ⇨ Durante este tiempo, los componentes se pueden conectar con la gateway.
4. Inicie la puesta en marcha inalámbrica.
5. Conecte el componente mediante el programador [▶ 11.3.2] dentro del intervalo temporal configurado.

Si no se han podido poder en marcha todos los componentes necesarios dentro de intervalo temporal configurado, puede repetir el proceso.
Los componentes que ya estén conectados con la gateway seguirán estándolo.

11.3.2 Conectar componentes inalámbricos

Conectar componentes inalámbricos con una gateway inalámbrica:

Requisitos previos

- El componente debe estar parametrizado para el uso inalámbrico.
- La gateway inalámbrica debe estar parametrizada en el software del sistema.
- La gateway inalámbrica debe estar conectada con el software del sistema.

Procedimiento

1. En la gateway, inicie la puesta en marcha inalámbrica [▶ 11.3.1].
   ⇨ Debe realizar los pasos siguientes dentro del intervalo temporal allí configurado:
2. Localice con el programador el componente que quiera conectar.
3. Inicie la sesión en el componente con el Master programador.
4. Seleccione el menú "Actuador/inalámbrico" en el programador.
5. Seleccione la opción del menú "Conectar".
6. Inicie el proceso de conexión con "Intro".
   ⇨ Luego tendrán lugar estos eventos:
   - Buscar red...
   - GW encontrada
   - Puesta en marcha...
   - Conectado con GW
7. Compruebe el estado de conexión en el menú "Inalámbrico".

⇨ La puesta en marcha inalámbrica se ha completado y el software del sistema puede contactar con el componente de forma inalámbrica.

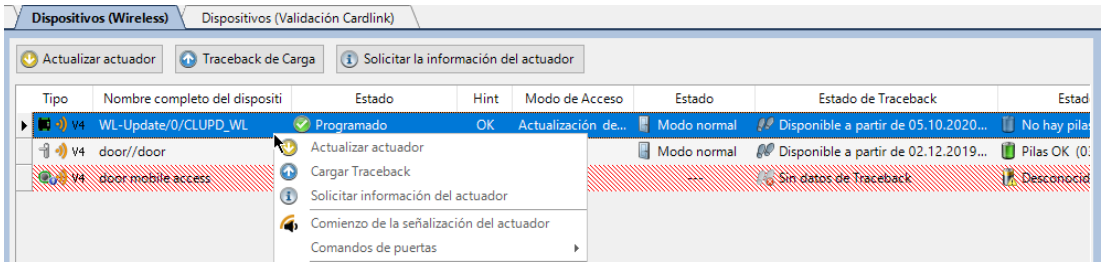
11.4 Actualización de componentes inalámbricos

El componente debe estar instalado y conectado de forma inalámbrica.

Procedimiento

1. Seleccione el espacio "Transferencia" del menú "Navegador".
2. Vaya a la pestaña "Actuadores (Inalámbrico)".
3. Seleccione el componente que quiera actualizar.
4. En el menú contextual, seleccione "Actualizar actuador".

⇨ El componente seleccionado se actualiza.



11.5 Descargar Traceback de componentes inalámbricos.

Los componentes guardan sus datos de Traceback en su memoria interna.

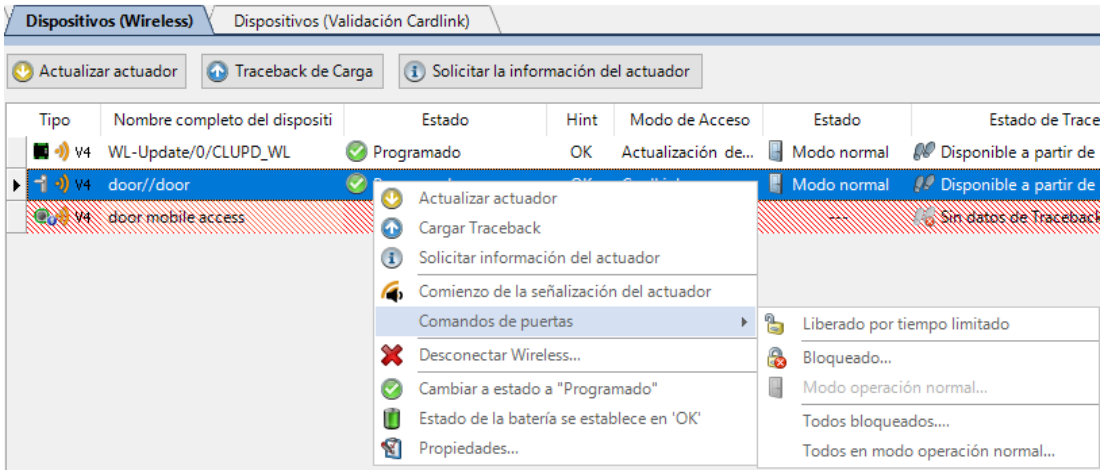
En la vista "Transferencia" se pueden transferir los datos de Traceback al software KEM. Consulte [▶ 6.12]

11.6 Abrir y cerrar componentes de forma inalámbrica

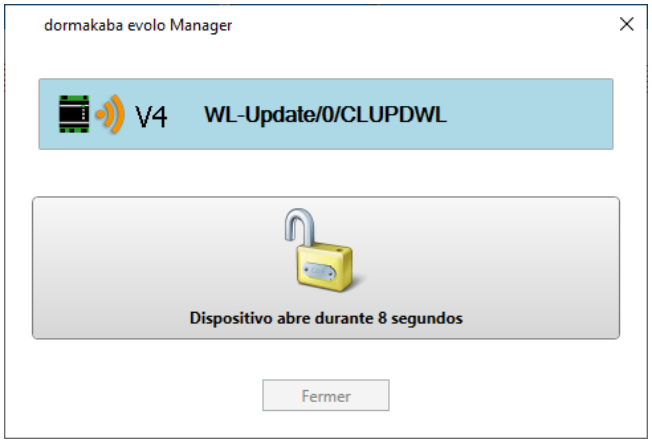
11.6.1 Habilitar componentes con limitación temporal

1. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores (Inalámbrico)".
3. Seleccione el componente.
4. Abra el menú contextual.

5. Seleccione la opción del menú "Órdenes de puerta".



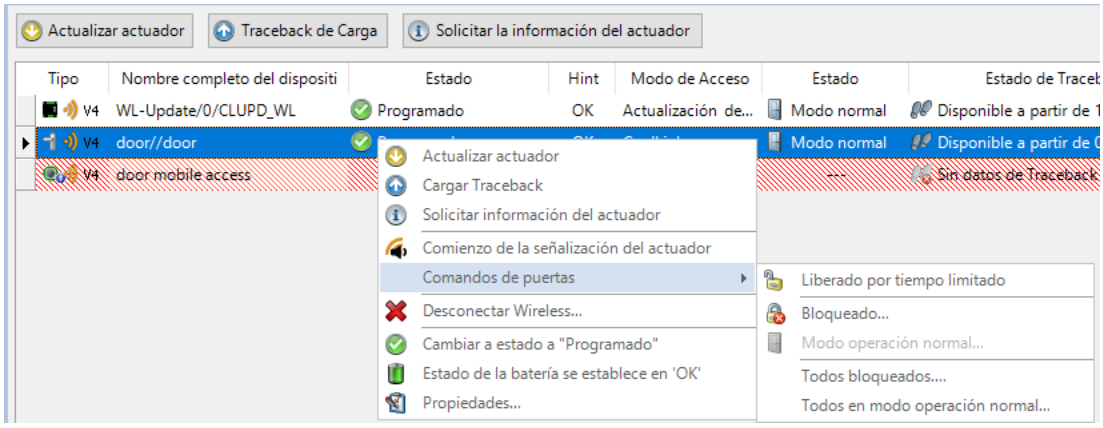
6. Seleccione la opción del menú "Habilitar componentes con limitación temporal".
   ⇨ La orden se envía al componente.
   ⇨ El componente se abre 10 s.



7. Lleve a cabo la acción en el componente. Transcurrido el intervalo temporal configurado, el componente vuelve al funcionamiento normal.

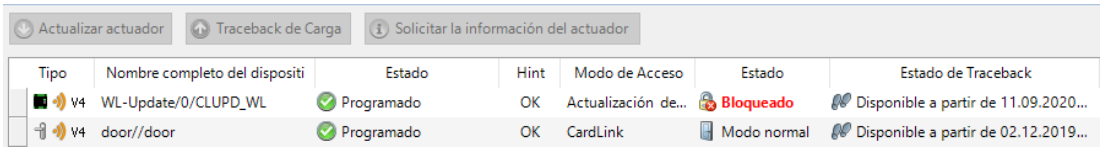
11.6.2 Bloquear componentes

1. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores (Inalámbrico)".
3. Seleccione el componente.
4. Abra el menú contextual.
5. Seleccione la opción del menú "Órdenes de puerta".



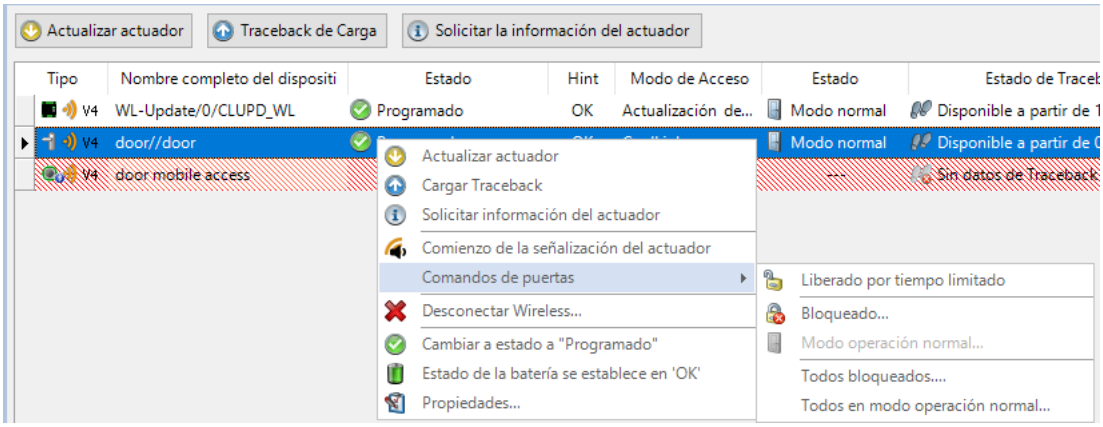
6. Seleccione "Bloquear...".
   ⇨ La solicitud se envía al componente.
   ⇨ El componente se bloquea.

Para desbloquearlo, consulte el siguiente capítulo [▸ 11.6.3].



11.6.3 Restaurar el funcionamiento normal de los componentes

1. Abra el espacio "Transferencia" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Actuadores (Inalámbrico)".
3. Seleccione el componente.
4. Abra el menú contextual.
5. Seleccione la opción del menú "Órdenes de puerta".



6. Seleccione "Funcionamiento normal...".

⇨ La solicitud se envía al componente.

⇨ El componente vuelve al funcionamiento normal.

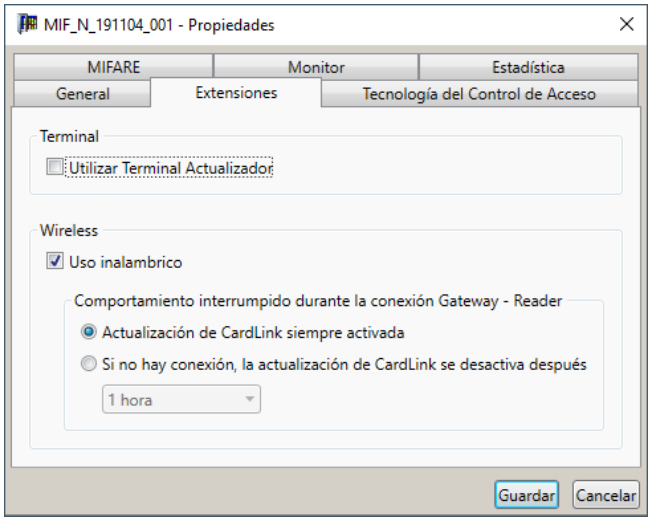
11.7 Actualización de CardLink

El modo Mixto inalámbrico todavía no es compatible con la gateway inalámbrica.

La función Actualización de CardLink se puede utilizar de forma inalámbrica para actualizar validaciones y autorizaciones de medios de usuario.
Para ello se utiliza un lector remoto con opción inalámbrica. Esto se conoce como lector de actualizaciones inalámbrico.

Si usa LEGIC, también deberá efectuar la autorización de escritura en el lector remoto.

Requisitos previos
En las propiedades de proyecto deben constar los siguientes ajustes:



Ajustes del lector usado:

Un componente usado para la actualización de CardLink debe presentar esta parametrización:

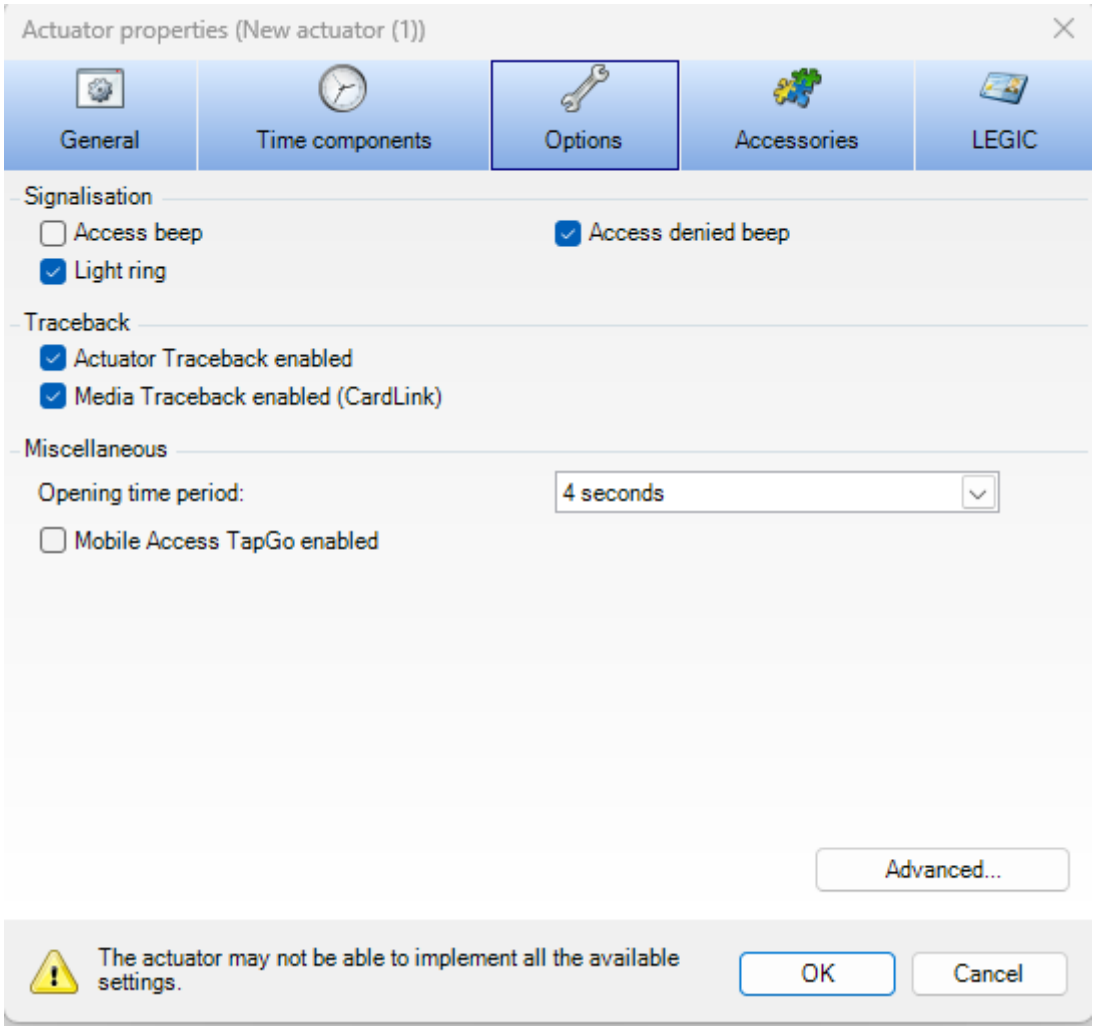
- El "Tipo de actuador" debe ser el lector remoto E320 (Inalámbrico)
- La opción Permitir capacidad inalámbrica debe estar activada
- Uno de estos modos de acceso debe estar seleccionado:
  - Actualización de CardLink con acceso
  - Actualización de CardLink sin acceso (con validación)
- El componente debe estar ligado a una pasarela inalámbrica, como se describe en la sección Inalámbrico.

La selección del comportamiento en caso de interrupción de la conexión significa lo siguiente:

- Actualización de CardLink siempre activa:
  Siempre se puede hacer uso de los derechos preparados.
- Si no hay conexión, la actualización de CardLink estará inactiva después del tiempo seleccionado:
  Se puede hacer uso de los derechos preparados hasta que transcurra el tiempo configurado.

Los datos de CardLink correspondientes se deben haber transferido completamente al lector de actualizaciones antes de que se interrumpa la conexión.

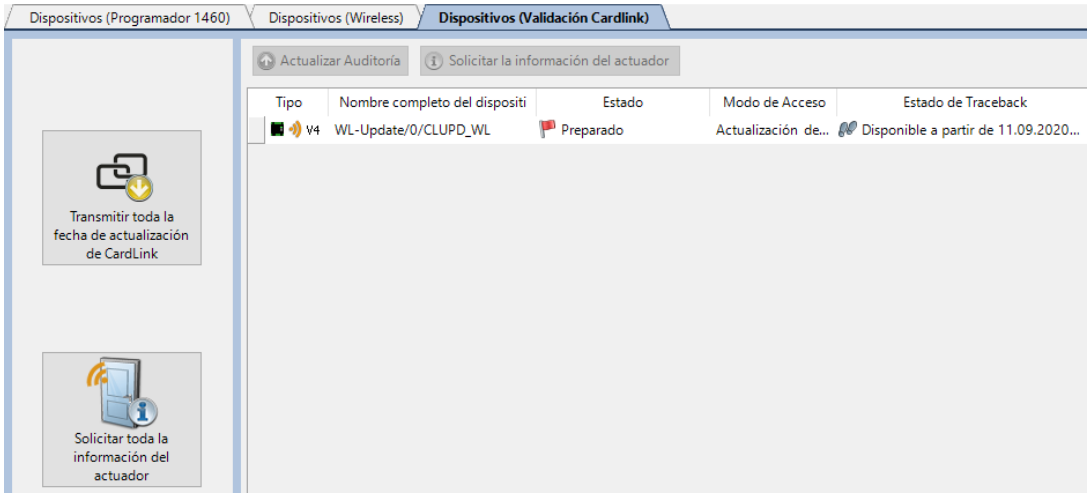
Ajustes en las propiedades del componente
La casilla Lector de actualizaciones de CardLink está activada: El componente relee de los medios de usuario los datos de estado de los componentes visitados.



Actualización de los conjuntos de datos del Lector de actualización inalámbrica

Se puede enviar un máximo de 3 500 conjuntos de datos desde medios de usuario a un lector de actualizaciones de CardLink.

1. Vaya al menú "Transferencia" del navegador.
2. Vaya a la pestaña "Actuadores (Actualización de CardLink)".
   ⇨ En esta ventana solo aparecerán los componentes utilizados para la actualización de CardLink.



3. Pulse el botón "Actualizar todos los datos de actualización de CardLink".

⇨ Completadas las tareas de transferencia, aparece el mensaje "En el lector".

Los terminales conectados (no inalámbricos) se deben actualizar por separado, como se explica en el capítulo Terminal.

11.8 Actualización inalámbrica del firmware

La actualización inalámbrica del firmware permite el cambio a una versión posterior/anterior del firmware de uno o varios componentes mediante la gateway inalámbrica.

Para ello, los componentes deben estar conectados a KEM mediante una gateway inalámbrica.

Requisitos previos

Todos los componentes deben cumplir los requisitos.
Los componentes que no los cumplan no se tendrán en cuenta para la actualización inalámbrica del firmware.

- Versión de firmware de la gateway inalámbrica: a partir de la 4.8.1
- Versión de firmware del componente: a partir de la 42.34
- No debe aparecer el mensaje "Batería baja".
- La opción "Permitir capacidad inalámbrica" debe estar activada.
- El componente debe estar conectado con la gateway inalámbrica.
- Los archivos del nuevo firmware deben estar disponibles y en una ruta que conozca.

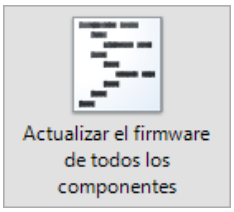
Símbolos utilizados
Símbolos utilizados en el resumen del asistente de actualización:

Símbo-lo	Significado
	OK Actualización posible
	OK Ninguna actualización necesaria
	Versión anterior Se utiliza una versión de firmware anterior.
	Actualización no posible

11.8.1 Asistente de actualización

El asistente de actualización se inicia desde el menú "Transferencia/actuadores (Inalámbrico)" o "Transferencia/actuadores (actualización de CardLink)". El asistente ayuda a seleccionar los archivos de firmware y a transferirlos a la gateway inalámbrica.

Actualizar el firmware de todos los componentes:



Esta opción inicia el asistente de actualización para todos los componentes mostrados. No es necesario seleccionar componentes.

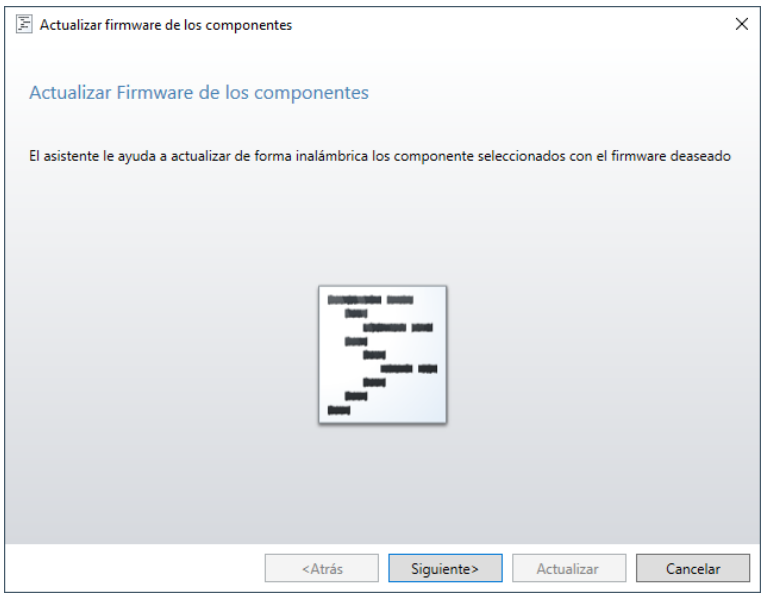
Después de iniciar el asistente de actualización, siga sus indicaciones.

Actualizar el firmware con selección de componentes y selección múltiple:
En el menú "Transferencia/actuadores (Inalámbrico)" o "Transferencia/actuadores (actualización de CardLink)", seleccione los componentes cuyo firmware quiera actualizar.

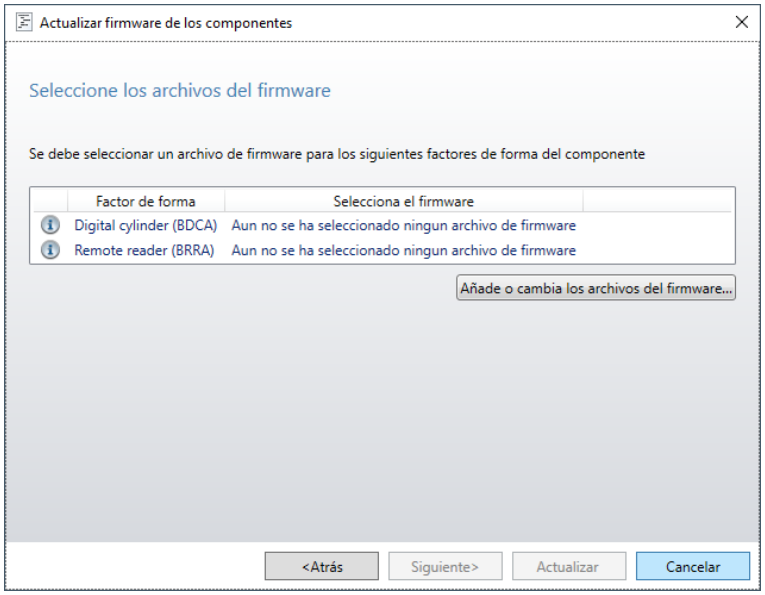
- Seleccionados los componentes, pulse el botón "Actualizar firmware del actuador" para iniciar el asistente de actualización.

Esta opción inicia el asistente de actualización para uno o varios componentes seleccionados.

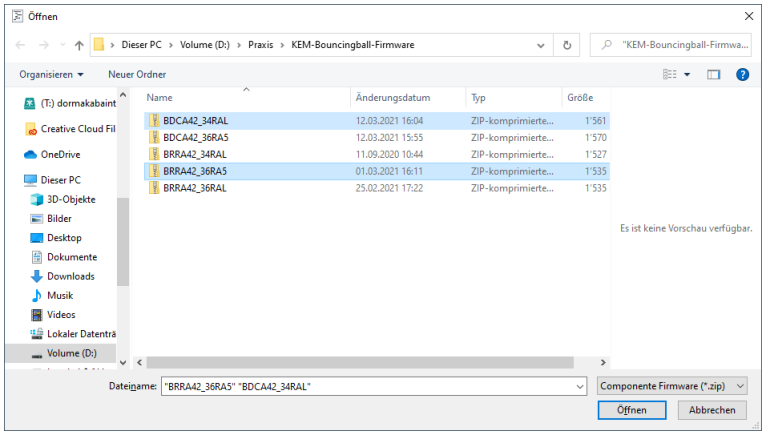
Siga el asistente.



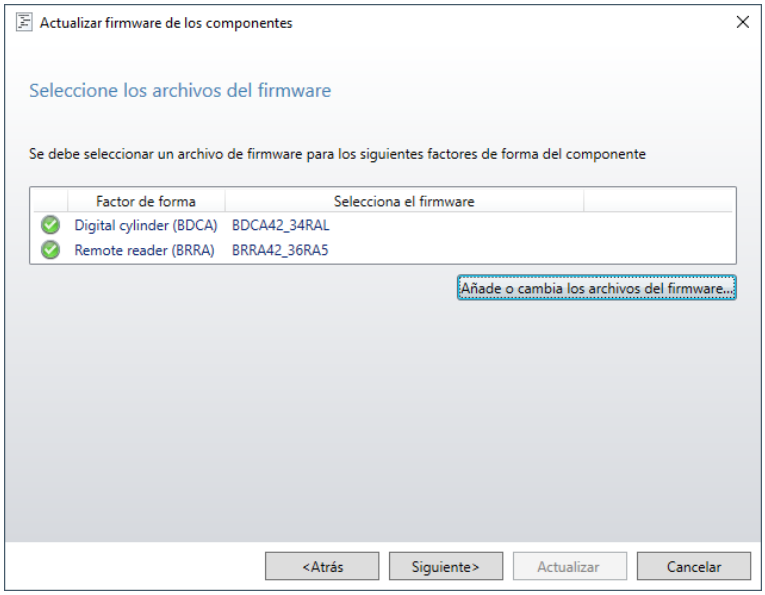
Seleccionar archivos de firmware
Seleccione los archivos del nuevo firmware para los componentes.
En una misma línea aparecen varios componentes con el mismo factor de forma.



Cada factor de forma de la lista debe tener un archivo de firmware seleccionado.



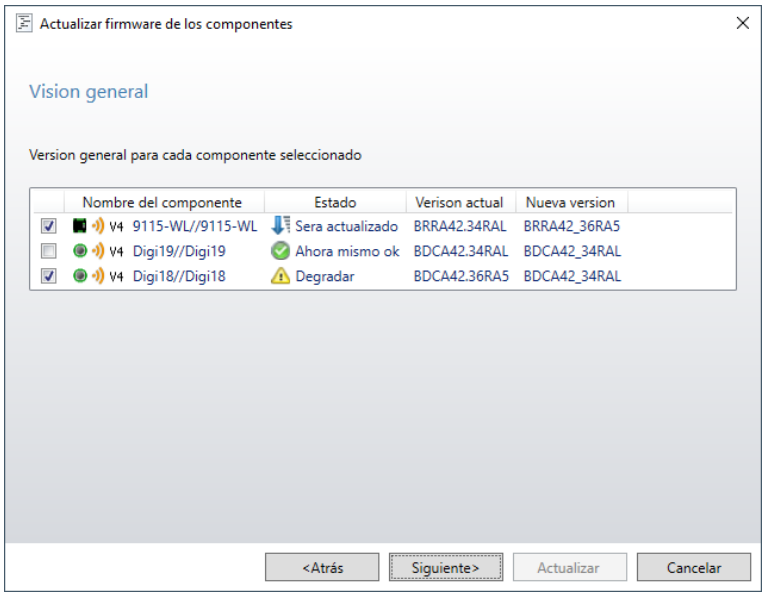
Si todos los archivos de firmware de todos los factores de forma están en la misma carpeta, es posible hacer una selección múltiple.

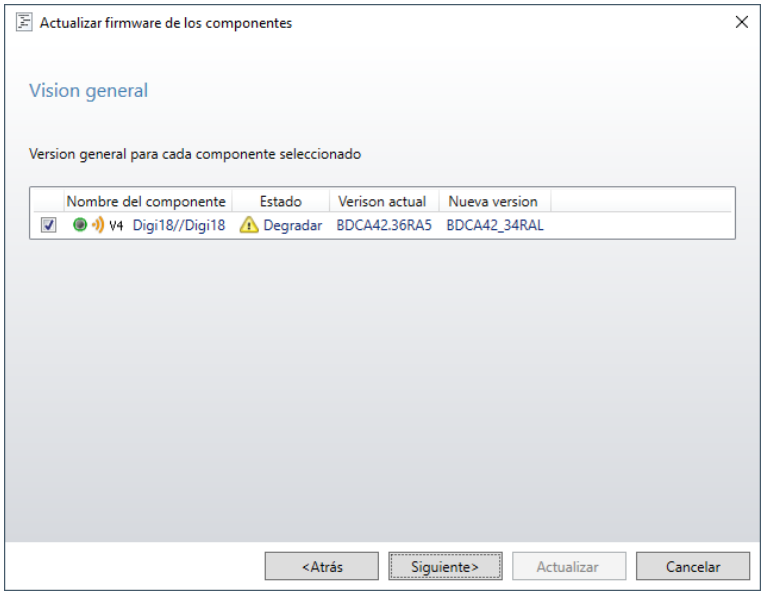


Resumen/control

En este paso aparecen de forma resumida todos los componentes seleccionados con su versión actual de firmware y la que se vaya a instalar. La casilla de cada componente muestra si el componente en cuestión formará parte de esta actualización del firmware.

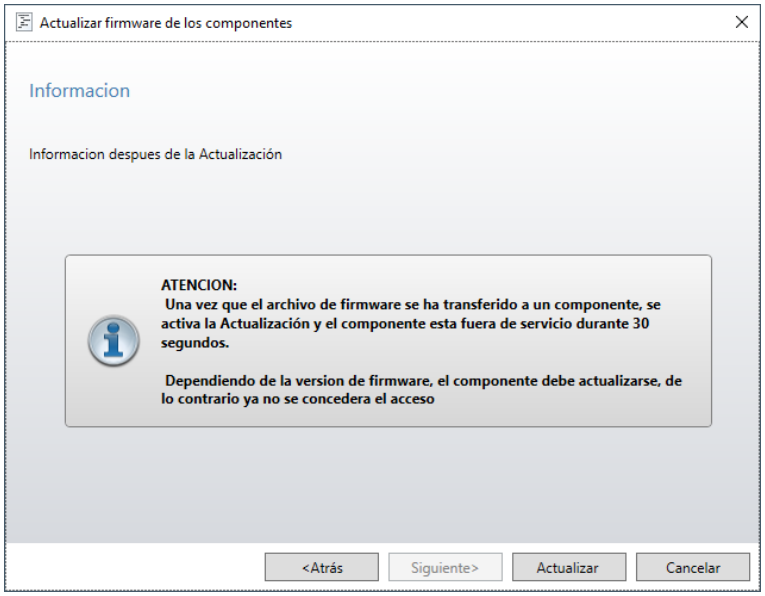
Por defecto, todas las casillas están activadas. Para excluir un componente de la actualización, desactive su casilla.





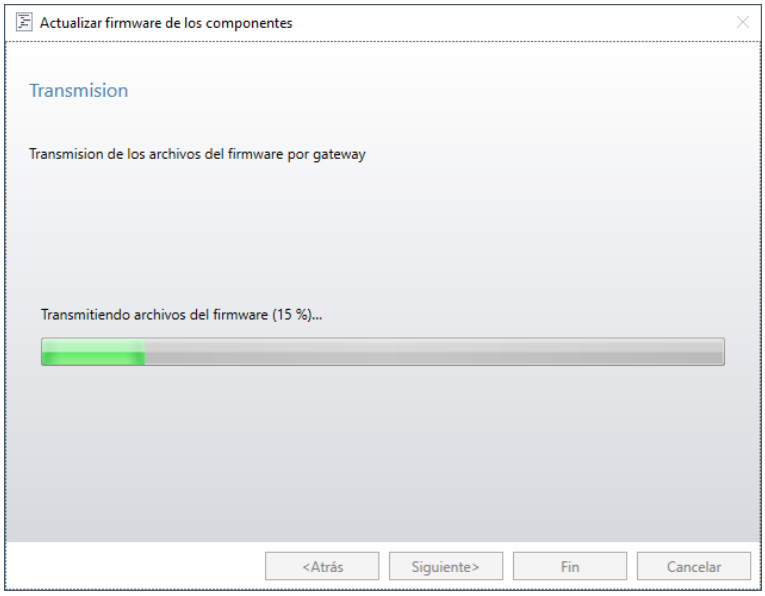
Los componentes con la casilla desactivada no formarán parte de la actualización.

Información importante antes de empezar a actualizar

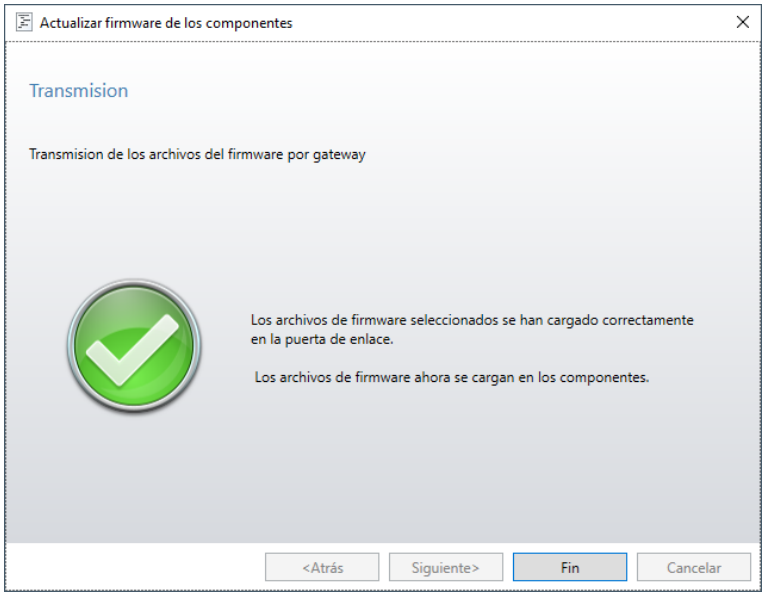


Si el proceso de actualización ya ha empezado, solo se puede cancelar en KEM a través del menú contextual del componente.

Al pulsar el botón "Actualizar" empezará el proceso de actualización.



La transferencia de los archivos a la gateway inalámbrica no se puede cancelar.



En función del firmware utilizado, se pierden los datos de configuración o la autorización de escritura del componente. Después de la actualización, el componente se deberá volver a configurar desde KEM.

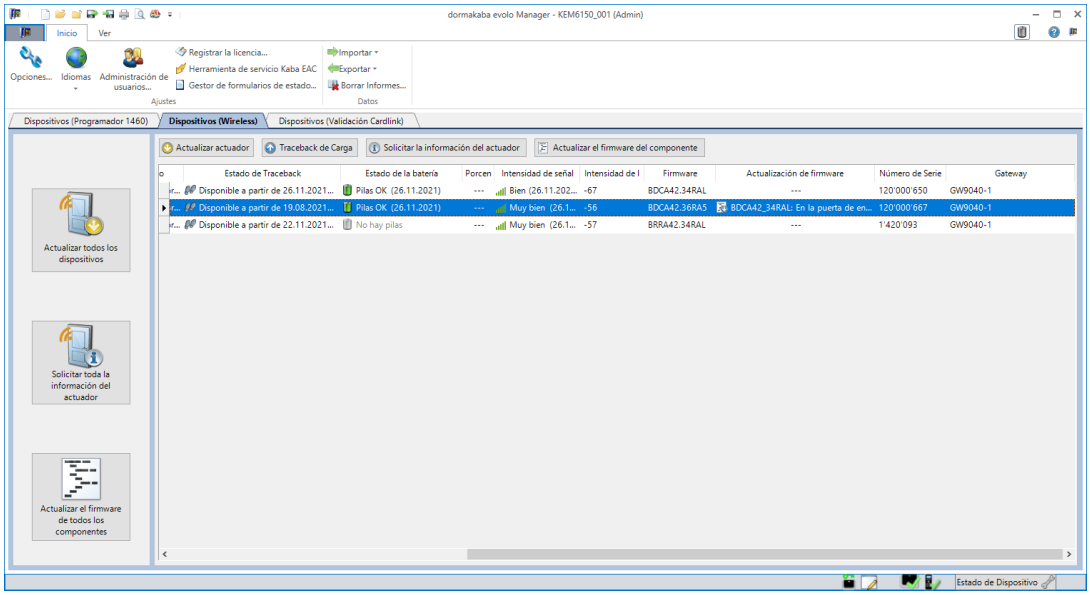
La transferencia de los archivos de firmware de la gateway inalámbrica al componente tarda un poco.

Durante la instalación del firmware en el componente, este estará inoperativo durante unos 30 segundos.

- La transferencia e instalación de los archivos de firmware en los componentes aparece en KEM, en el menú "Transferencia/actuadores (Inalámbrico)".
- Desde el menú contextual del componente se puede cancelar el proceso de actualización del componente en cuestión en cualquier momento.

Tras completarse la transferencia a la gateway inalámbrica, los archivos se distribuirán e instalarán en los componentes. El asistente de actualización ya habrá cumplido su función. Seleccione "Listo" para finalizar el asistente.

Indicador de progreso/información sobre el firmware

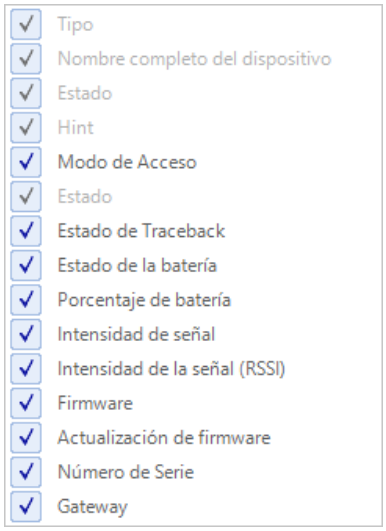


En las columnas "Firmware" y "Actualización de firmware" del menú "Transferencia/actuadores (Inalámbrico)" o "Transferencia/actuadores (actualización de CardLink)" aparece información sobre el firmware actual, sobre el nuevo firmware y sobre el estado de la actualización del firmware.

Firmware	Actualización de firmware
BDCA42.34RAL	BDCA42_36RA5: En la puerta de enlace

Firmware	Actualización de firmware
BDCA42.34RAL	---
BDCA42.36RA5	BDCA42_34RAL: Transmitiendo (11%)...

Si no ve la columna "Actualización de firmware", selecciónela en el menú contextual de los títulos de columnas para que aparezca. Para que se muestre el menú contextual, haga clic con el botón derecho del ratón en el título de una columna.



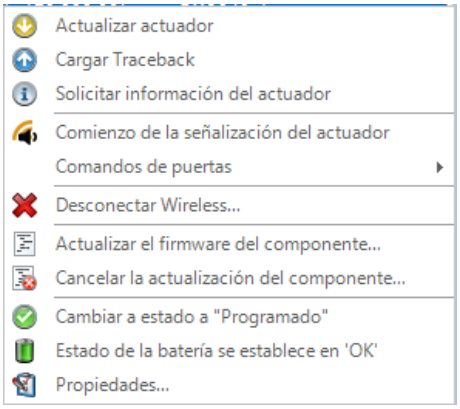
Si la gateway inalámbrica no puede contactar con un componente en 24 horas, deberá volver a lanzar la actualización.

Cancelar actualización del firmware

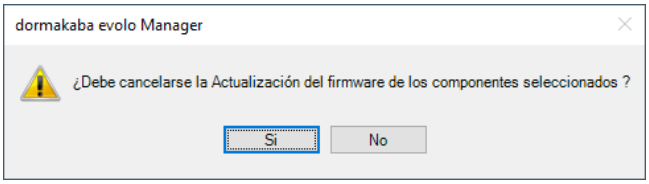
Opciones para cancelar la actualización del firmware:

- Cancelación desde KEM, en el menú "Transferencia/actuadores (Inalámbrico)" o "Transferencia/actuadores (actualización de CardLink)":

– En el menú contextual del componente, seleccione la entrada "Cancelar actualización del firmware del actuador".



– Confirme la cancelación.



– La transferencia del firmware al componente se interrumpe y el nuevo firmware no se instala.
El componente no sufre ninguna modificación.

12 Datos

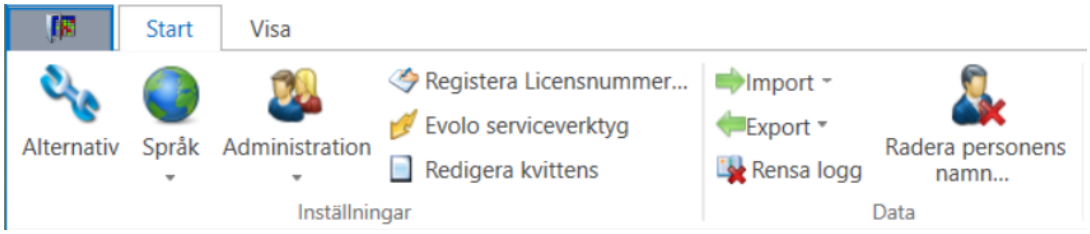
12.1 Importar y exportar datos

Para intercambiar datos de sistema, tiene distintas opciones a disposición.

Importar	
Importar proyecto	Importa un archivo de proyecto KEM.
Archivo de importación Kaba (.kif)	Archivo de sistema que se puede solicitar a dormakaba. De esta forma no tendrá registrar manualmente los componentes integrados en un sistema de cierre.
Lista de medios (.txt)	Importa los datos de los medios a partir de un archivo de texto
Lista de actuadores (.txt)	Importa los datos de los actuadores a partir de un archivo de texto
Lista de personas (.txt)	Importa los datos de las personas a partir de un archivo de texto
Datos de calendario (.txt)	Importa los datos del calendario a partir de un archivo de texto
Llaves digitales	Importa llaves digitales desde documentos de vale (PDF). Para ello, se inicia un asistente que sirve de ayuda para la importación. Para más información, consulte Importar llaves digitales.
Exportar	
Exportar proyecto	Exporta el archivo del proyecto KEM.
Exportar proyecto anonimizado	Anonimiza y exporta el archivo de proyecto de KEM. Para más información, Exportar proyecto anonimizado [▸ 12.2].
Lista de medios (.txt)	Exporta los datos de los medios en un archivo de texto
Lista de actuadores (.txt)	Exporta los datos de los actuadores en un archivo de texto
Lista de personas (.txt)	Exporta los datos de las personas en un archivo de texto
Datos de calendario (.txt)	Exporta los datos del calendario en un archivo de texto

Ejemplo de importación

1. En la barra de funciones "Inicio", abra el menú "Importar datos".
2. Seleccione, por ejemplo, lista de medios...



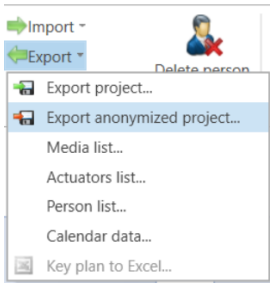
3. Seleccione el plan de cierre con los medios mediante el menú desplegable.
4. Pulse el botón "OK".
5. Busque la lista de medios en la unidad correspondiente e impórtela.

Recomendación:

Si el formato de importación no está claro, realice primero una exportación para que se pueda analizar el formato.

12.2 Exportar proyecto anonimizado

El asistente anonimiza un proyecto y lo exporta a una carpeta de destino especificada. El proyecto en el KEM no se modificará.
Esta función puede ser útil, por ejemplo, para el servicio técnico.



Se suprimirá o sustituirá lo siguiente:

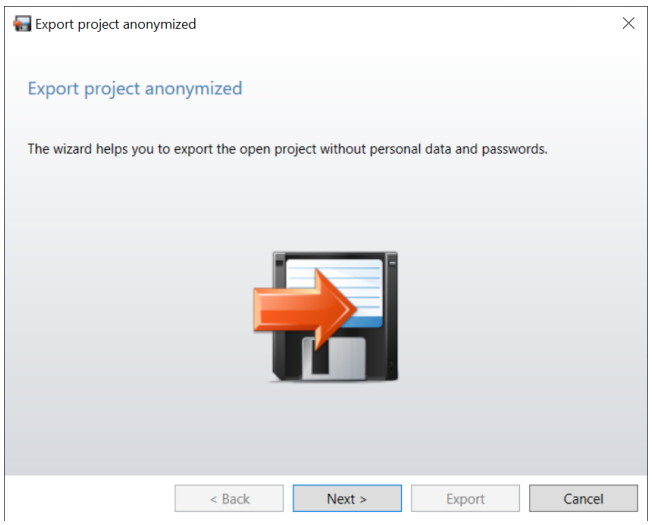
- Se elimina la administración de usuarios.
- Se borran las contraseñas de las pasarelas.
- Los nombres de las personas se sustituyen por los ID de la base de datos.
- Se eliminan los datos personales (por ejemplo, campos adicionales o número de teléfono).
- Los nombres de persona de los datos de registro se sustituyen por "Suprimido".
- Los nombres de persona de los datos de protocolo se sustituyen por "Suprimido".
- Los nombres de persona de los datos de Traceback se sustituyen por "Suprimido".

Requisito

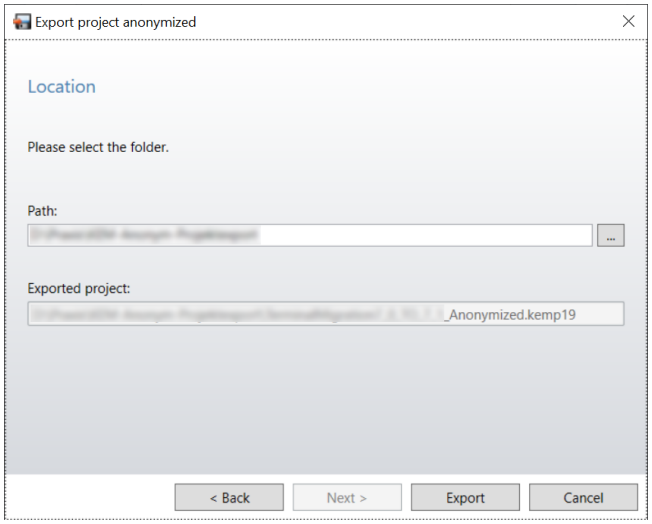
- Si la administración de usuarios está activa, el usuario tiene la sesión iniciada como administrador.
- Si la administración de usuarios no está activa, la función está disponible.
- El proyecto que se quiere exportar está abierto.

Procedimiento

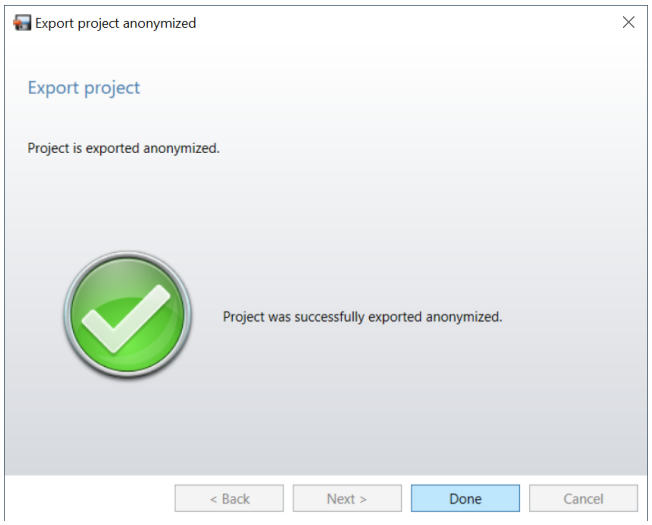
1. Haga clic en "Exportar" en el menú "Inicio".
2. Haga clic en "Exportar proyecto anonimizado".
   ⇨ Se inicia el asistente.



3. Haga clic en "Siguiente".



4. Seleccione la ruta de la carpeta de destino.
   ⇨ El nombre de archivo del proyecto exportado se muestra en "Proyecto exportado".
5. Haga clic en "Exportar".
   ⇨ Se exporta el proyecto.



6. Haga clic en "Listo".
   ⇨ El asistente finaliza.

12.3 Ajustar las propiedades tras la migración del proyecto

Tras la migración de un proyecto, varias funciones dejan de estar disponibles o tienen las propiedades alteradas. En el caso de proyectos existentes, siempre se crea una copia. El archivo de proyecto copiado recibe el nuevo nombre "ProjektName_Copy".

Por lo general:
• La información de la zona horaria debe ser reasignada. (La zona horaria ajustada en el ordenador se utiliza como zona horaria "por defecto").
Para la versión KEM 4.4:
• No es posible crear nuevos Master B temporales. Los Master B temporales ya existentes pueden seguir utilizándose y actualizándose.
Para la versión KEM 3.2:
• Las funciones OKS (como las modificaciones, TwinTime o TwinTime Terminal) dejan de ser compatibles.
• La programación manual ya no puede desactivarse para componentes individuales. Solo puede establecerse en las propiedades del proyecto. Tras la migración, todos los componentes tienen desactivada la opción "Evitar codificación".
• Los componentes pasivos dejan de ser compatibles.

12.4 Borrar informes

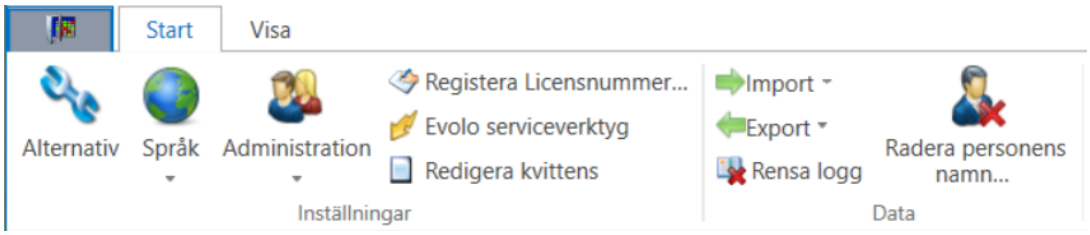
Borrar entradas del registro y de Traceback.

Todas las entradas con la fecha indicada y las anteriores se borran de forma permanente. Por motivos de seguridad, antes de emitir la orden se recomienda crear una copia de seguridad del proyecto.

Antes del borrado, exporte el proyecto KEM.

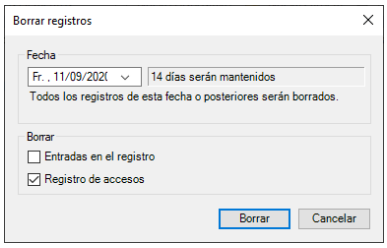
Ejemplo:
En este ejemplo, se deben borrar todas las entradas antiguas de Traceback incluyendo las del día 9/3/2017.

1. En la barra de funciones "Inicio", abra el espacio "Borrar informes".



2. Seleccione la fecha.
3. Active la casilla Entradas de Traceback.
4. Pulse el botón "Borrar".

⇨ Todas las entradas de Traceback con la fecha especificada y más antiguas quedarán borradas.



13 Operador KEM

El operador KEM es una interfaz de usuario simplificada del software KEM. Sin embargo, esto también implica algunas restricciones en las funciones.

13.1 Limitaciones

Limitaciones de las funciones	
Modo de acceso	El modo de acceso de todos los componentes se aplica a todo el proyecto CardLink o Lista blanca.
Plan de cierre	Los proyectos con varios planes de cierre no son compatibles.
Mecánico	Los proyectos que solo contengan componentes mecánicos no son compatibles.
Perfiles temporales	Solo son compatibles los proyectos V4 puros (MIFARE o LEGIC advant).
Administración de usuarios	No es parte de las funciones.
Recepción	No es parte de las funciones.
Registros	No es parte de las funciones.
Traceback	No es parte de las funciones.
Organización	Las personas pueden registrarse y utilizarse por apellido y nombre. No se ofrece más información personal.
Vacaciones/días especiales	No se pueden modificar.
Validación	Se pueden utilizar estos tipos de validación: – Duración en días y horas – 24 horas (1 día) – Hora de finalización – "Siempre"

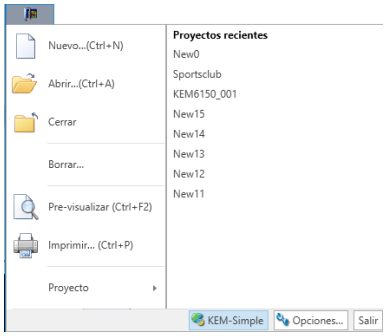
13.2 Crear proyecto

Para crear un proyecto Lista blanca con CID (Card ID) o un proyecto CardLink, se deben leer las tarjetas de seguridad.
En función del tipo de medio utilizado, la tarjeta de seguridad variará:

- Tarjeta de seguridad C para utilizar medios MIFARE
- Tarjeta de seguridad C1 o C2 para utilizar medios LEGIC.

Procedimiento

1. En la barra de funciones a la izquierda de la pestaña, abra el menú contextual **"Inicio"**.
2. Pulse el botón Operador KEM.



3. Abra el menú contextual junto a la pestaña "Inicio".
4. Menú Nuevo... (Ctrl + N) para abrirlo.
5. Siga el asistente.

6. En el paso 2, seleccione el tipo de proyecto.
7. Siga el asistente.
8. Complete el procedimiento pulsando Listo.

⇨ El proyecto queda creado.

⇨ El asistente se cierra.

13.3 Crear Master programador

Para el acceso de administrador a componentes (actuadores) autónomos, hace falta un Master programador. [▸ 6.3.2.1]

13.4 Asistentes (Wizards)

Actualizar el programador

	Asistente para transferir datos del plan de cierre al programador.

Pérdida de medios

	Con este asistente se aplican las medidas necesarias para preservar la seguridad del sistema. **Aviso:** el plan de cierre o el proyecto ya deben existir en el programador.

Lectura de registros de la tarjeta de servicio

	Este asistente lee los datos de estado de los componentes del medio de servicio en el proyecto.

Añadir medio

	Este asistente le ayuda a incorporar más medios.

Editar componentes

	Con este asistente, el usuario puede hacer lo siguiente con la lista de componentes: - visualizarla - editarla - añadir nuevos componentes

Perfiles temporales

	Este asistente ayuda al usuario a crear, modificar o borrar un perfil temporal.

Crear nuevo medio de servicio

	El asistente ofrece ayuda para crear un medio de servicio para CardLink. El medio de servicio será necesario para bloquear identificaciones concretas en componentes específicos.

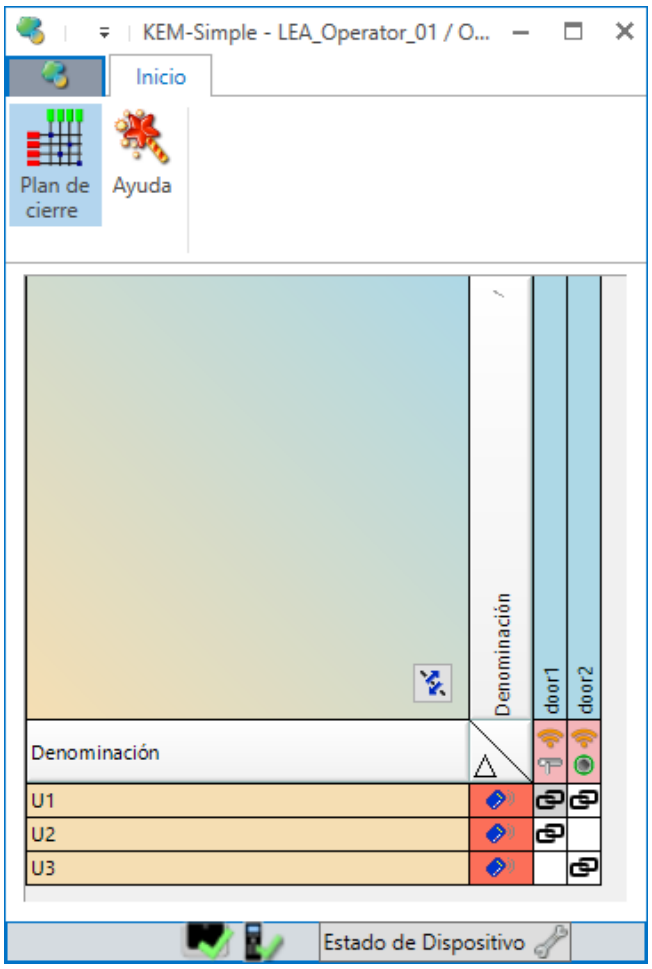
Configurar CardLink

	Este asistente ayuda a establecer la configuración básica de CardLink. **Aviso:** los componentes ya deben estar creados en el proyecto. - Establecer componentes autorizados para validar - Establecer el período de validación

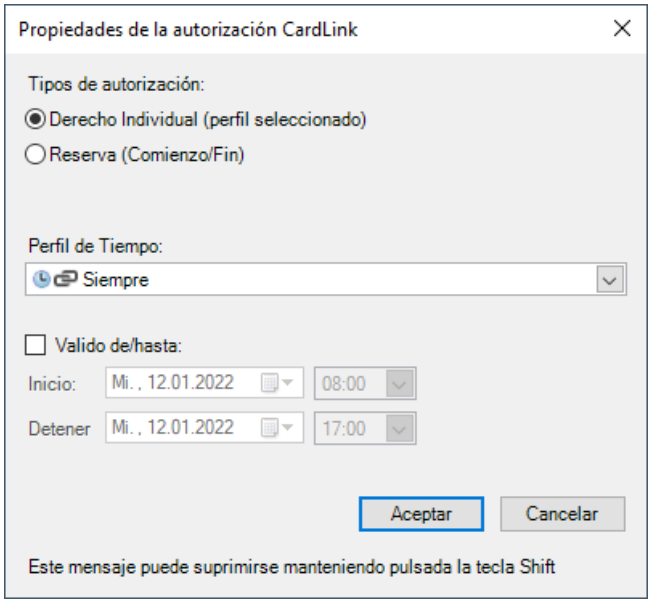
13.5 Manejo

Procedimiento

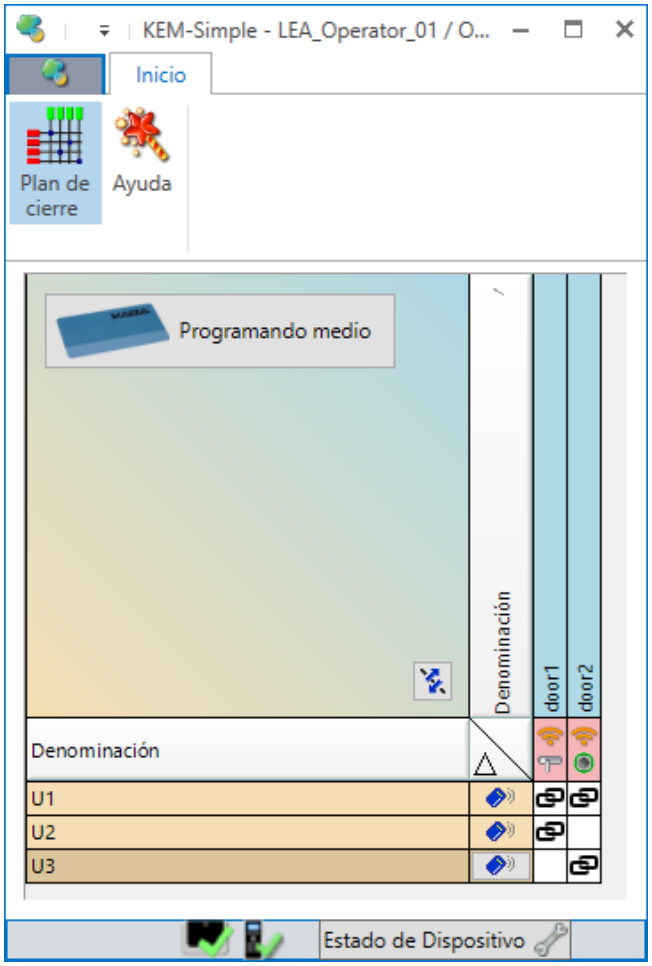
1. Active la asignación deseada haciendo clic en el campo de la cuadrícula correspondiente.



2. Asigne el tipo de autorización y el perfil temporal.
3. Pulse el botón "OK".



4. Ponga un medio en el lector de sobremesa.



5. Pulse el botón "Programar medio...".
   ⇨ Las autorizaciones se escriben en el medio.

Tras la primera configuración del software KEM, así como en modificaciones de los perfiles temporales y los componentes, se deben transferir las actualizaciones. Con el asistente **Actualizar programador**, [▸ 13.4] los datos modificados se transfieren al programador. En el siguiente paso se actualizan los componentes con el programador.

Paso del operador KEM al software KEM o finalización del programa

1. Pulsando el botón "dormakaba evolo Manager" del menú "Archivo" cambiará la vista a la pantalla de inicio del software KEM.
2. Con el botón "Finalizar" se cierra el software KEM.

14 Recepción

La función de recepción simplifica la asignación de autorizaciones individuales. Se conceden a medios individuales o múltiples. El proceso no va ligado al usuario. Los derechos preparados para una selección de componentes y grupos de puertas se transfieren al medio con un perfil temporal seleccionado.

La función Recepción está disponible para CardLink y para Lista blanca.

14.1 Proceso en CardLink

En pocos pasos es posible programar, emitir o retirar medios.

Emisión de medios

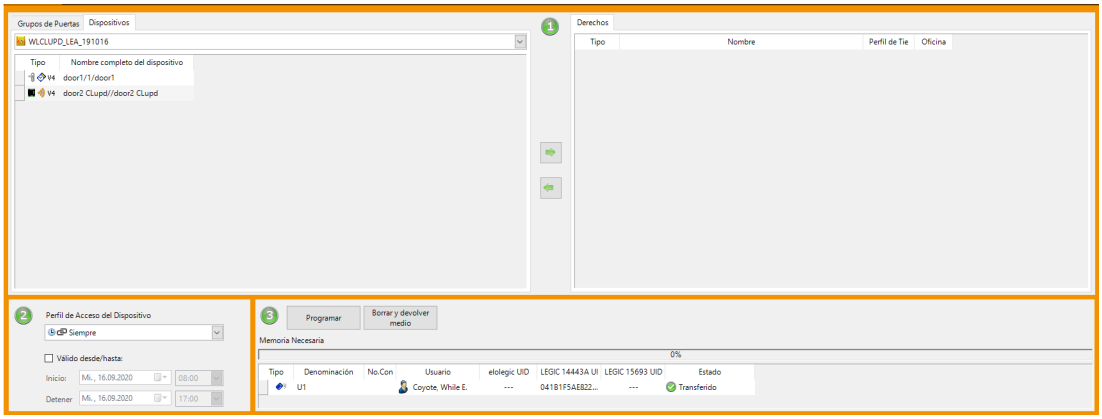
1. Desplace los grupos de puertas y/o los componentes con el botón "Flecha" (del medio) hasta la pestaña "Derechos preparados".
2. Asigne un perfil temporal y/o una duración de la validez.
3. Coloque un medio en el lector de sobremesa y pulse "Programar".

⇨ Los datos se escriben en el medio.

Retirada de medios

1. Ponga el medio en el lector de sobremesa.
2. Pulse el botón "Borrar y retirar".

⇨ Las autorizaciones de acceso del medio quedan borradas.



14.2 Proceso en Lista blanca

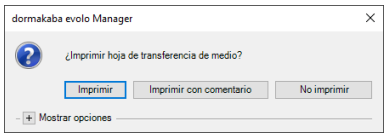
Requisitos previos

- Las autorizaciones de los medios están preconfiguradas.
- Las personas a las que quiera asignar medios deben estar registradas en la lista de personas.

Emisión de medios

Encima del lector de sobremesa hay un medio no asignado.

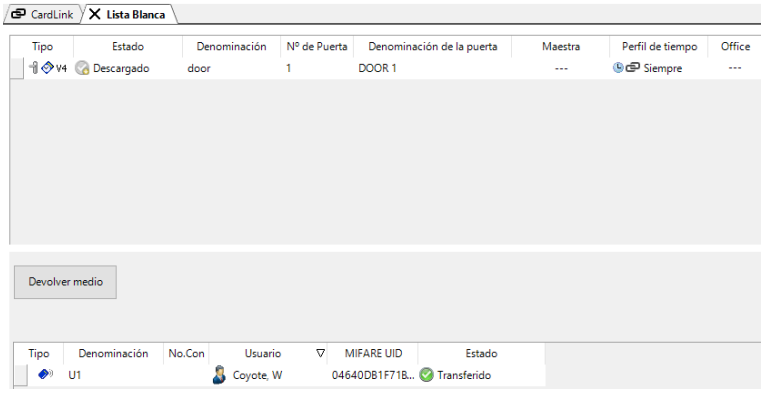
1. Seleccione la persona de la lista "Usuarios" a quien quiera asignar el medio.
2. En el siguiente cuadro de diálogo, imprima el comprobante de emisión.



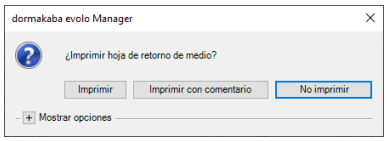
Retirada de medios

La retirada de medios solo está activa si un medio se ha asignado a un usuario y este mismo medio está encima del lector de sobremesa.

Un medio que está encima del lector de sobremesa está asignado a una persona



1. Pulse el botón "Retirada de medios".
   ⇨ La asignación a la persona que conste en el medio queda borrada.
2. En el siguiente cuadro de diálogo, imprima el comprobante de retirada.



⇨ Las autorizaciones asignadas al medio se mantienen.

⇨ El medio se puede asignar a otra persona con las mismas autorizaciones.

15 dormakaba CheckIn

El dormakaba CheckIn es un programa de gestión compacto y cómodo para el proceso de entrada y salida. Con él se pueden gestionar las autorizaciones de acceso de huéspedes y personal de pequeños hoteles, pensiones y B&B.

15.1 Crear proyecto para dormakaba CheckIn

Requisitos previos

Al crear un proyecto para dormakaba CheckIn, se deben tener en cuenta los siguientes puntos:

- dormakaba CheckIn solo funciona con autorizaciones CardLink.
- Todas las puertas (y, en su caso, los respectivos grupos de puertas) deben estar registrados en el proyecto.
- En el software KEM, la columna CheckIn debe aparecer en las pestañas **Actuadores** y **Grupos de puertas**.
- La programación de los componentes debe estar al día.
- Debe haber una llave de bloqueo (llave de servicio) creada.

1. Inicie el software KEM.
2. Cree un proyecto o abra un proyecto existente.

(Administración de) Usuarios

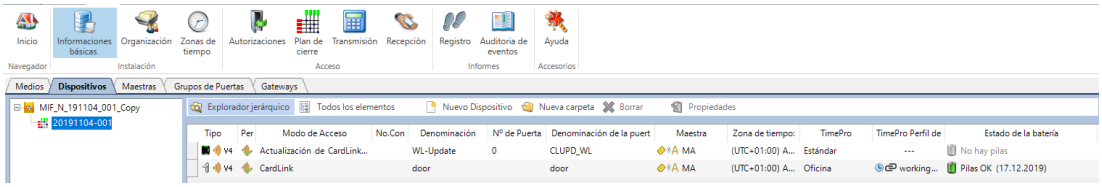
Para usar dormakaba CheckIn, los usuarios del programa deben estar registrados y creados. Para ello será necesario un usuario con el rol "Administrador" y, como mínimo, un usuario con el rol "Usuario de dormakaba CheckIn".
La creación puede empezar justo al iniciar el asistente de CheckIn o también en los ajustes de la administración de usuarios.

15.2 Registrar proyecto dormakaba CheckIn en KEM

15.2.1 Leer/importar medios

- Configurar medios con autorización CardLink. [▸ 6.9.2]

15.2.2 Crear componentes y asignar Master



- Configurar componentes en la pestaña "Actuadores" [▸ 6.9.2].

Si en la columna CheckIn un componente tiene un n.º de puerta registrado y la casilla activada, significa que está disponible para los espacios en la vista de CheckIn. Si la casilla de la columna CheckIn no está activada, el componente no aparece en la vista de CheckIn.

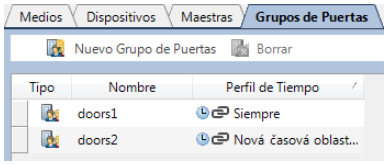
15.2.3 Configurar grupos de puertas

Procedimiento

1. Configurar grupos de puertas. [▸ 6.9.2]

Es posible agrupar otras entradas (como garajes subterráneos, ascensores, restaurantes, zonas de bienestar, gimnasios, etc.) como grupos de puertas. Para que aparezcan en dormakaba CheckIn, estos grupos de puertas deben tener la marca correspondiente en la columna CheckIn de la pestaña KEM.

2. Seleccione una de estas opciones en la columna CheckIn:
   a) No utilizado
   b) Utilizado
   c) Utilizado, preseleccionado



15.2.4 Programar puertas con el programador

- Programar componentes. [▸ 6.9.2]

15.3 Configurar y activar dormakaba CheckIn

Requisito
El proyecto debe estar completamente creado en KEM.

Procedimiento
Para la configuración y la activación, debe dar los siguientes pasos:

1. Pulse el botón "Asistentes" de la barra de funciones "Navegador".
2. Inicie el asistente de CheckIn.
3. Siga el asistente.
4. Los requisitos específicos se pueden definir en los datos estándar de dormakaba CheckIn.

Si se ha creado un perfil de usuario, el proyecto solo se podrá abrir con el nombre de usuario y la contraseña correspondientes. El nombre de usuario determina si se abrirá dormakaba CheckIn o el software KEM.

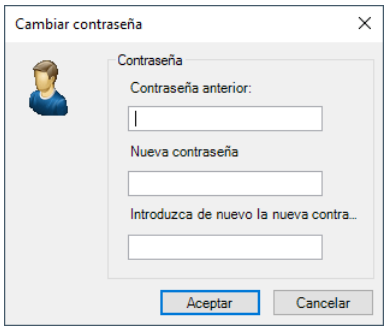
Modificación de la imagen de fondo
Modificar la imagen de fondo en la vista de CheckIn.

Formatos de imagen compatibles: PNG, JPG, BMP

- Seleccione la imagen de fondo en el paso 4 del asistente de CheckIn.

15.3.1 Registrar usuarios en la administración de usuarios

1. En la barra de funciones "Inicio", seleccione "Administración de usuarios".
2. Pulse el botón "Nuevo".
   ⇨ En el lado izquierdo se añadirá un nuevo usuario.
3. Introduzca las propiedades del usuario en el lado derecho.
4. Active la opción "Contraseña de dormakaba evolo Manager".
5. Pulse el botón "Modificar" para abrir el cuadro de diálogo de contraseña.
6. Introduzca la contraseña.
7. Pulse el botón "OK".



⇨ La autenticación de usuarios con contraseña está activada.

⇨ La opción Administrador dentro de los derechos de usuarios está activada.

Si solo se introduce un usuario, el derecho de usuario Admin [Administrador] no se puede cambiar.

8. Finalice la administración de usuarios pulsando el botón "Cerrar".

Borrar usuarios

1. En la barra de funciones "Inicio", seleccione "Administración de usuarios".
2. Seleccione el usuario que quiera borrar.
3. Pulse el botón "Borrar".
   ⇨ El usuario queda borrado.
4. Pulse el botón "Cerrar".

Cuando se haya borrado el último usuario (**Admin**), la administración de usuarios se desactivará.

Cambiar contraseñas de usuarios

1. En la barra de funciones "Inicio", seleccione "Administración de usuarios".
2. Seleccione el usuario.
3. Vaya a la zona "Autenticación".
4. Pulse el botón "Cambiar".
5. Introduzca la contraseña y pulse "OK".
6. Pulse el botón "Cerrar".

15.4 Manejo

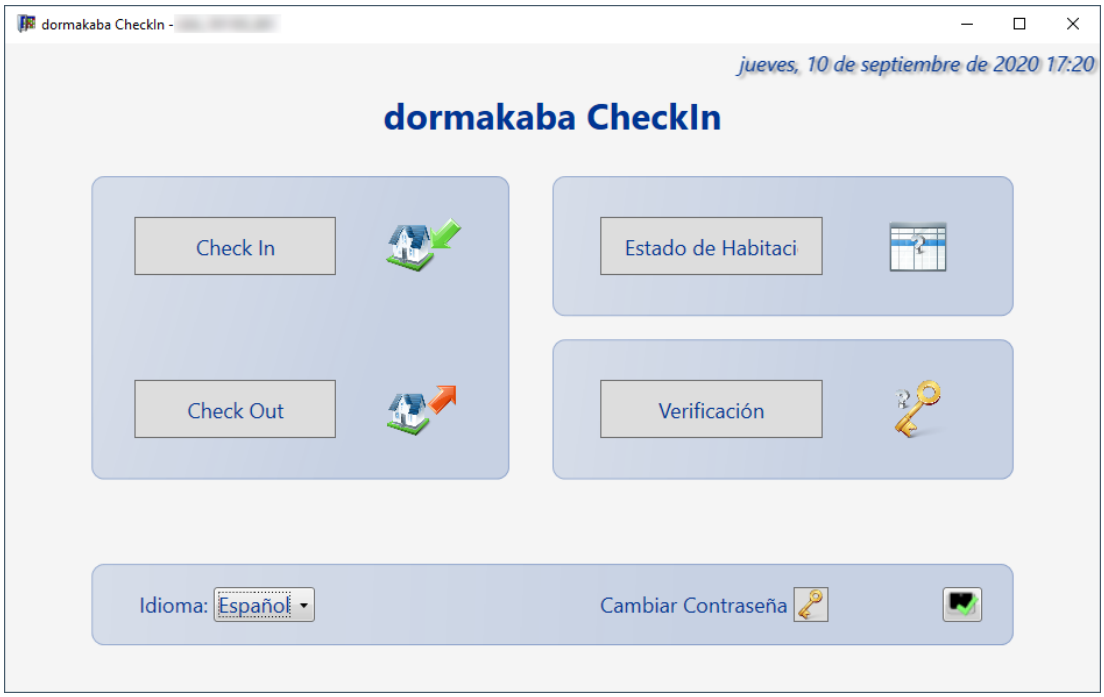
15.4.1 Abrir CheckIn

1. Inicie el software dormakaba evolo Manager (KEM).
2. Seleccione una de estas opciones:
   a) Crear nuevo proyecto:
   - Cree un nuevo proyecto completo en KEM.
   - Configure y active el proyecto de CheckIn. A partir de aquí, el proceso es el descrito en .
   b) Abrir proyecto con CheckIn (proyecto existente):
   - Seleccione un proyecto de CheckIn.
   - Introduzca el nombre de usuario y la contraseña del proyecto de CheckIn correspondiente.
   - Pulse el botón "OK".
   b) Abrir proyecto sin CheckIn (proyecto existente):
   - Abra el proyecto de CheckIn en KEM.
   - Introduzca el nombre de usuario "Admin" y la contraseña del proyecto de KEM correspondiente.
   - Pulse el botón "OK".

15.4.2 Entrada (Check-in)

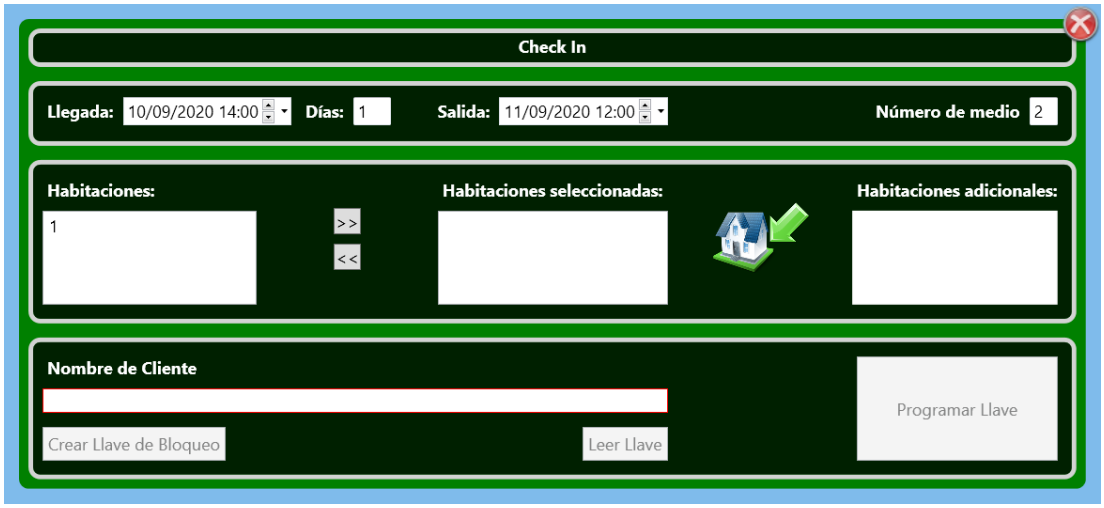
dormakaba CheckIn debe estar abierto.

1. Pulse el botón "Check-in".



2. Ponga un medio vacío en el lector de sobremesa.

3. Compruebe y ajuste la fecha y hora de entrada.
4. Introduzca la cantidad de días o la fecha de Check-out (salida).
5. Compruebe y ajuste la fecha y hora de salida.
6. Ajuste la cantidad de llaves que se van a emitir.
7. Seleccione el espacio en el campo "Espacios" y actívelo desplazándolo a "Espacios seleccionados".
8. Active otras entradas (p. ej., zona de bienestar o gimnasio).
9. Introduzca el nombre del huésped.
10. Finalice el proceso pulsando el botón "Programar llave".



15.4.3 Generar llave de bloqueo

"Generar llave de bloqueo" crea una llave de bloqueo para que pueda bloquear llaves (p. ej., una llave perdida).

Requisito

- dormakaba CheckIn debe estar abierto.
- Debe haber un medio de servicio configurado.

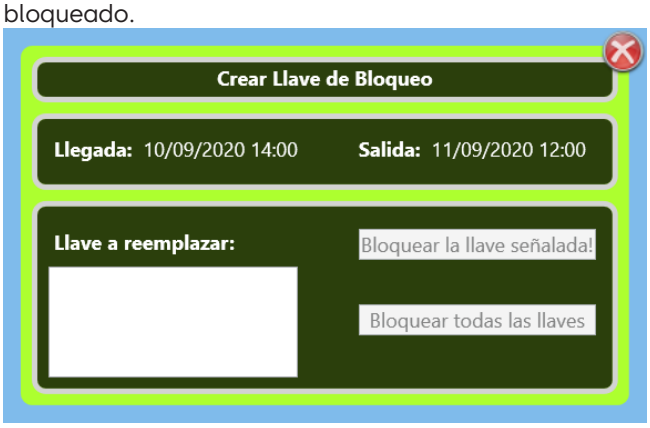
Procedimiento

1. Pulse Check-in.
2. Coloque la llave de bloqueo (medio de servicio) encima del lector de sobremesa.
3. Seleccione uno o varios espacios.

Si quiere bloquear varios espacios, puede seleccionarlos de forma conjunta y transferirlos a la llave de bloqueo. Cada llave de bloqueo generada borra siempre la llave de bloqueo precedente del medio en cuestión.

4. Pulse el botón Generar llave de bloqueo.
5. Seleccione la llave que quiera bloquear.
6. Pulse el botón "Bloquear llave seleccionada" o "Bloquear todas las llaves".
   ⇨ La llave de bloqueo queda creada.
7. Presente esta llave de bloqueo en los componentes de los espacios en cuestión. En cada componente, espere hasta la confirmación y las señales (1 señal acústica larga y 1 señal óptica en verde).

⇨ A partir de este punto deja de ser posible acceder a los espacios con el medio bloqueado.



Con gateway y Lector de actualización inalámbrica:

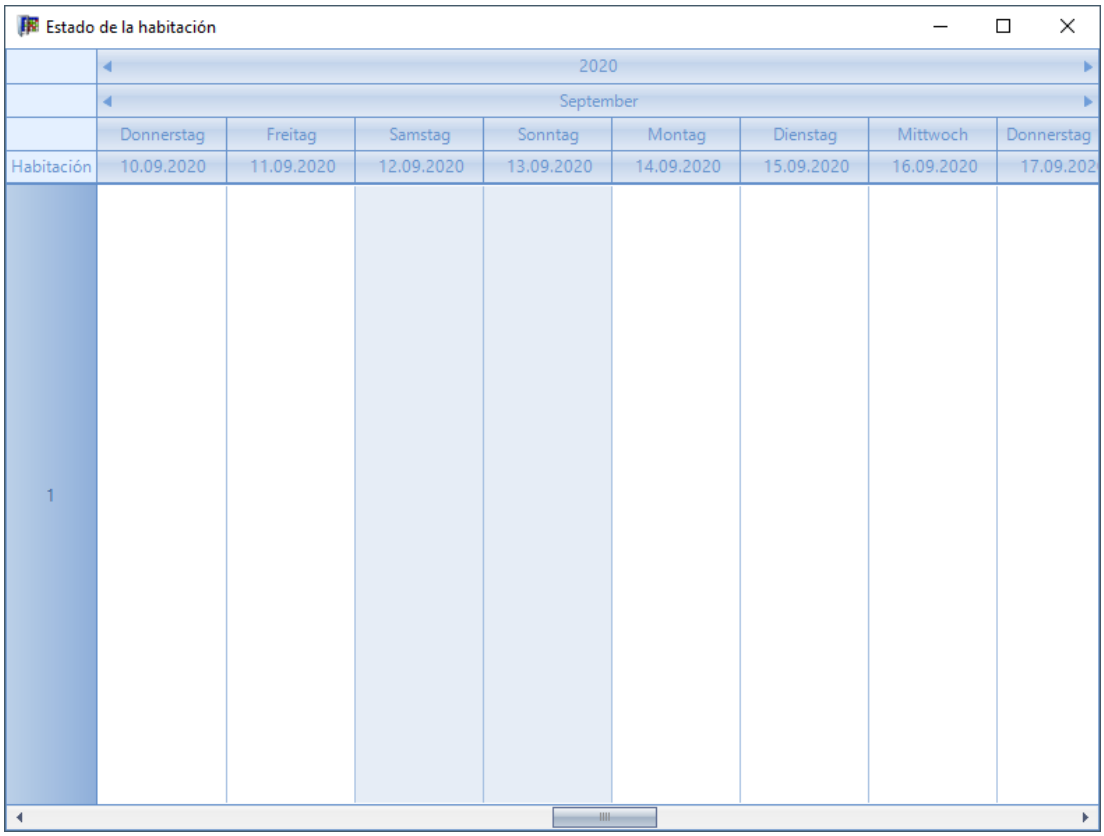
De forma paralela a la generación de la llave de bloqueo, la gateway transfiere la Lista de bloqueo al medio de servicio y a los componentes inalámbricos.

Indicador de estado del símbolo de la gateway en la pantalla de inicio:

Transferencia OK	
Transferir datos	La Lista de bloqueo se está transfiriendo a los componentes inalámbricos mediante la gateway.
Error de transmisión	Inicie la sesión en KEM como administrador para ver los detalles.

15.4.4 Estado del espacio

El estado del espacio es un resumen de las reservas actuales del espacio.



15.4.5 Salida (Check-out)

dormakaba CheckIn debe estar abierto.

1. Ponga el medio del huésped en el lector de sobremesa.

2. Complete el proceso pulsando el botón "Check-out".

⇨ El proceso de salida se ha completado y las autorizaciones del medio se han borrado.

15.4.6 Verificación

La verificación ofrece la posibilidad de comprobar los datos que contiene una llave presentada (p. ej., una llave encontrada).

1. Coloque la llave o la llave de bloqueo encima del lector de sobremesa.
2. Aparecen los datos actuales.

15.4.7 Cambiar de CheckIn a KEM

1. Salga del programa CheckIn con "ESC".
2. Abra KEM con el nombre de usuario (p. ej., "Hotel Paloma") y la contraseña.

16 Medio perdido

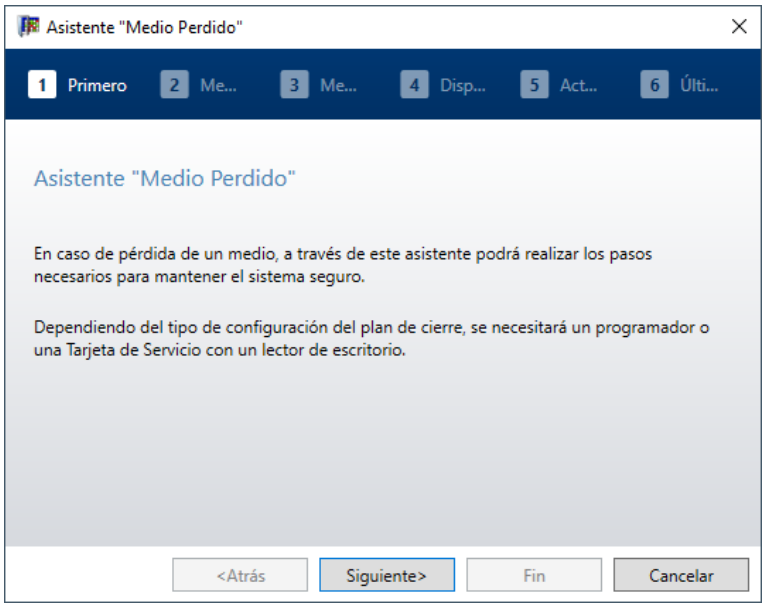
Las autorizaciones de acceso de un medio perdido deben retirarse.

16.1 Bloquear/reemplazar medio con el asistente

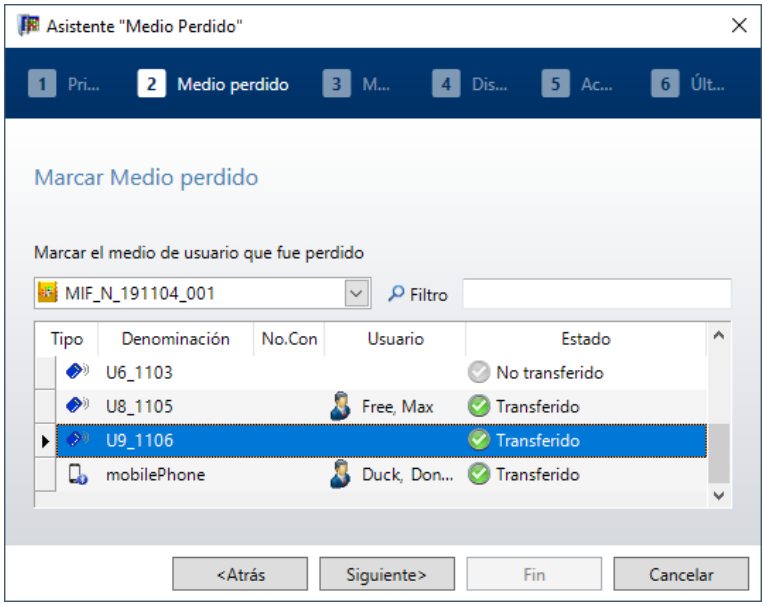
Asistente de pérdida de medios
Los medios perdidos se bloquean con la ayuda del asistente de pérdida de medios. En ese caso, ya no podrán validarse ni utilizarse en un componente. Los medios bloqueados se consideran no autorizados y se rechazan.

Procedimiento para bloquear un medio:

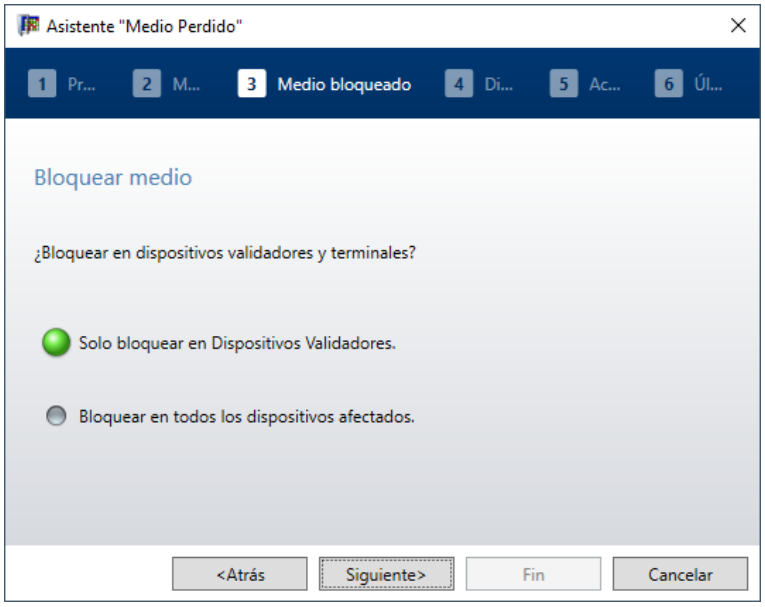
1. Seleccione el menú "Asistentes".
2. Inicie el asistente "Pérdida de medios".



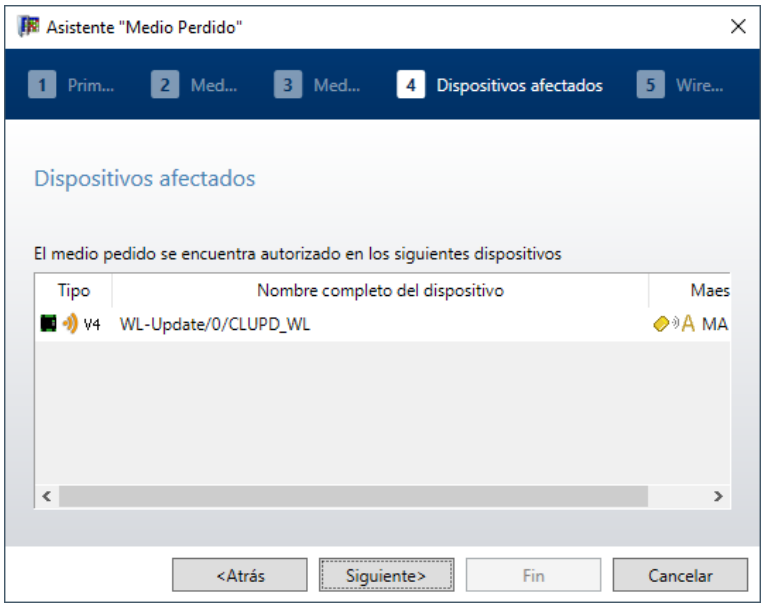
3. Seleccione el medio en cuestión de la lista de medios.



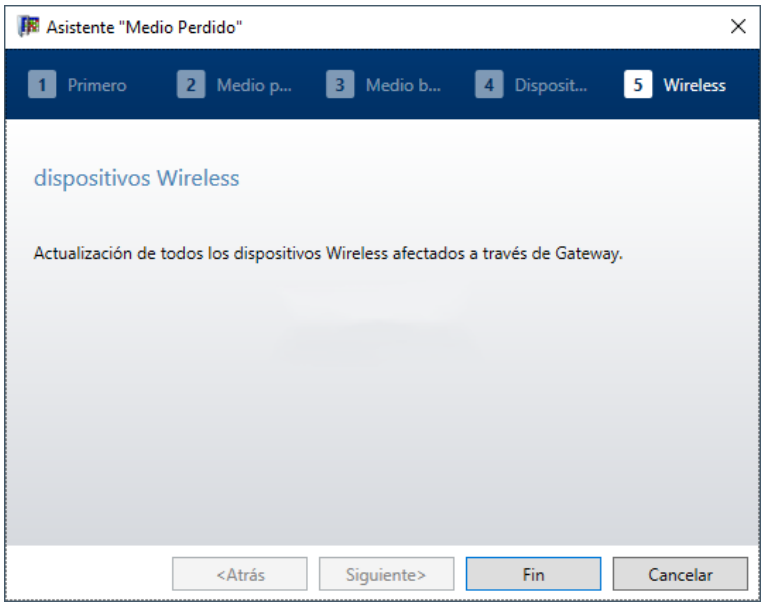
4. Seleccione el tipo de bloqueo.



5. Seleccione los componentes en cuestión.



6. Seleccione el método de transferencia del bloqueo.



El bloqueo no será efectivo hasta que se hayan transferido los datos a los componentes en cuestión.

Asistente de medio de sustitución
Este asistente le permite transferir las autorizaciones de un medio anterior o perdido a un nuevo medio. El medio anterior o perdido queda bloqueado.

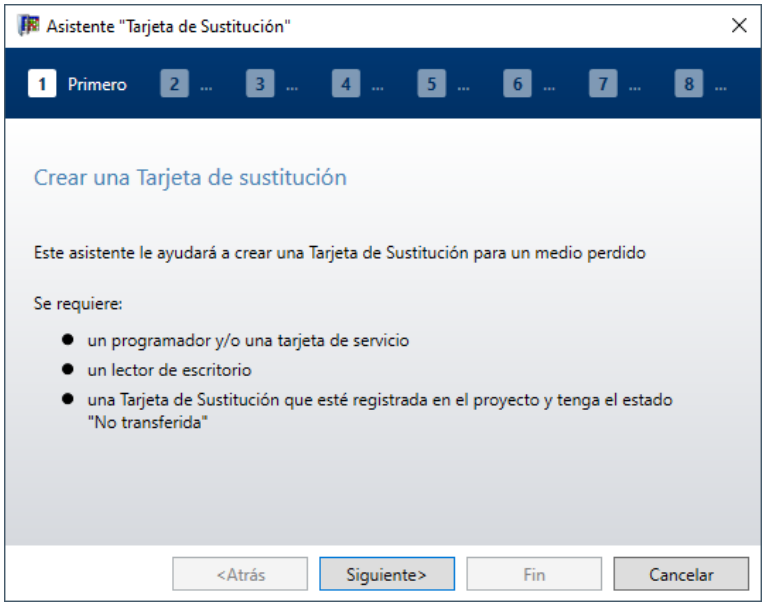
Inicie el asistente con el proyecto activo en el menú de selección. También se pueden crear documentos de repuesto para otros proyectos.

Requisitos previos:

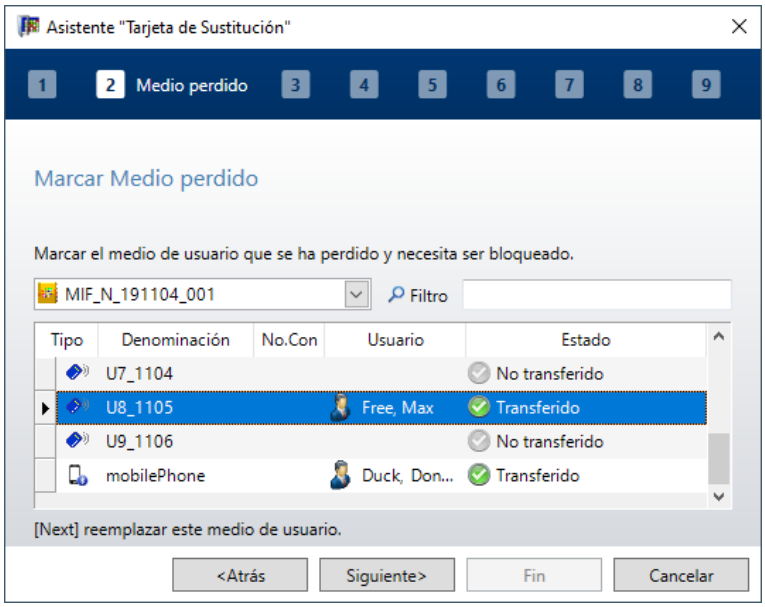
- Un programador 1460. El programador no es necesario si se utiliza el medio de servicio.
- Un medio de servicio. El medio de servicio es necesario si no hay ningún programador disponible.
- Un lector de sobremesa.
- Un medio de sustitución. El medio de sustitución debe estar introducido en el proyecto. El medio de sustitución no debe estar emitido.

Procedimiento:

1. En KEM, seleccione el menú Asistentes.
2. Seleccione el asistente "Medio de sustitución".



3. Seleccione el medio perdido del usuario.



4. Siga las instrucciones del asistente.

El medio perdido se ha bloqueado y las autorizaciones del usuario se transfieren a un nuevo medio.

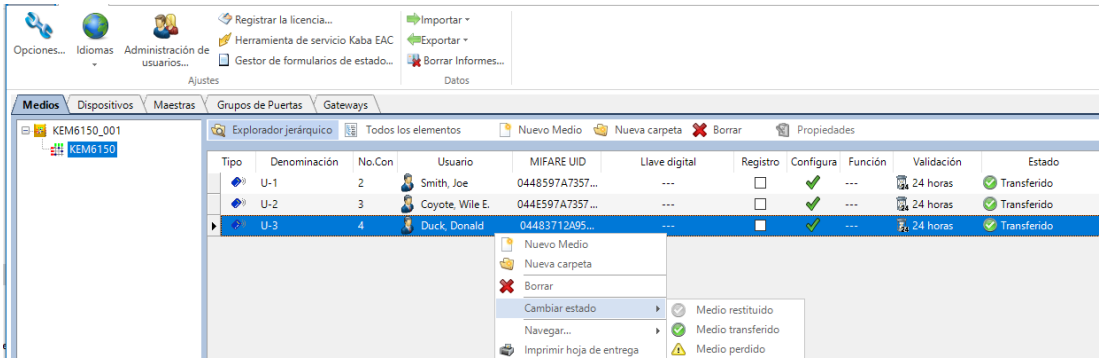
Una vez transferido el bloqueo a los componentes, el medio perdido ya no se podrá utilizar.

16.2 CardLink

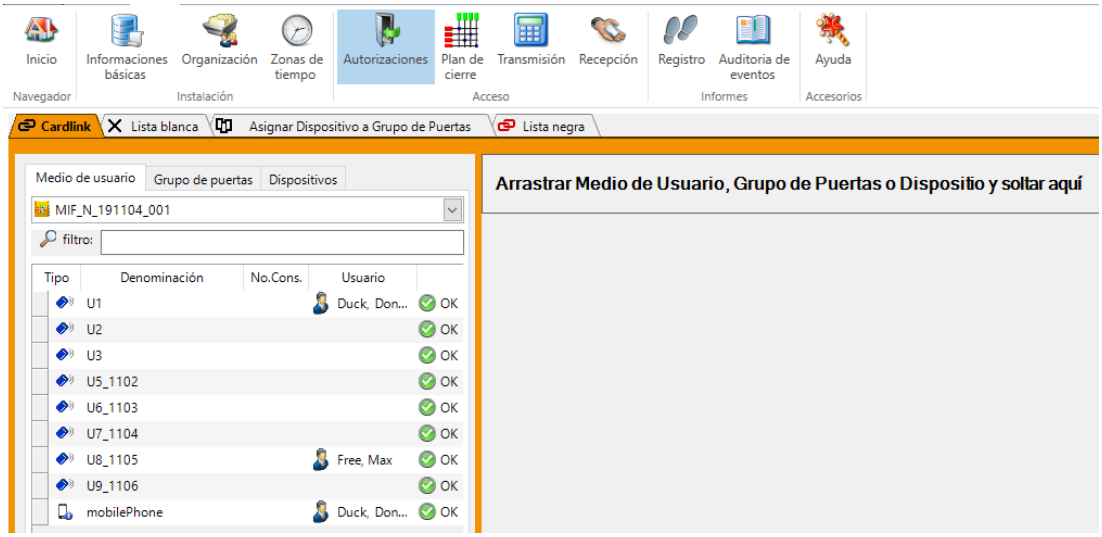
- La validación ya no se renueva para los medios de usuario perdidos. Esto invalida estos medios de usuario y se bloquea el acceso.
- Si quiere bloquear un medio de usuario cuya duración de la validación todavía esté activa, debe bloquearlo en todos los componentes en cuestión.

Procedimiento

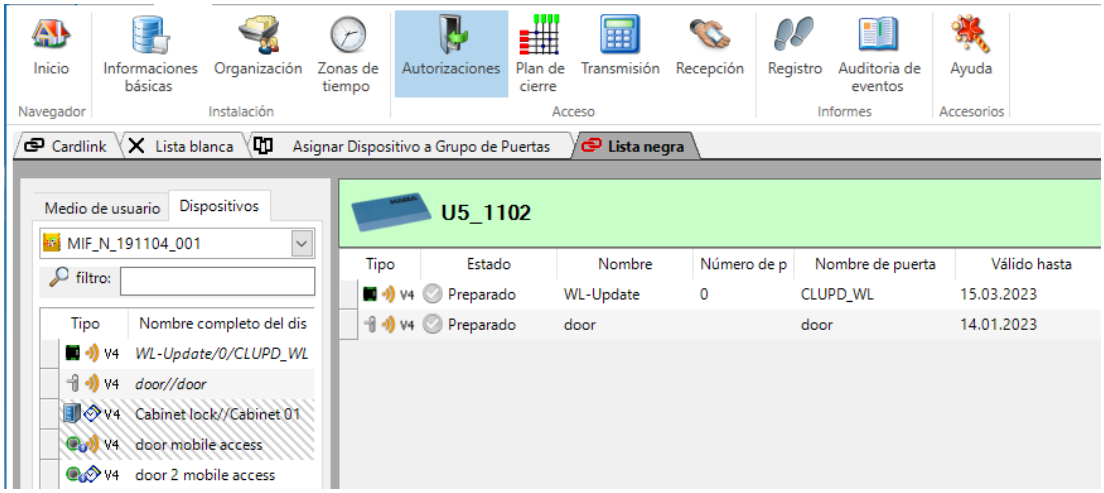
1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Medios".
3. Seleccione todos los medios o un medio perdido concreto.
4. Abra el menú contextual.
5. Vaya a "Cambiar estado".



6. Seleccione el estado "Perdido".
7. De ser necesario, puede imprimir un formulario.
8. Abra el espacio "Autorizaciones" de la barra de funciones "Navegador".



9. En la lista de bloqueo aparecen los componentes afectados que se deben actualizar.
10. Programar componente. [▶ 6.9.2]
11. Confirmar programación. [▶ 6.9.1]



La Lista de bloqueo solo está disponible en el tipo de autorización CardLink.

- Si el funcionamiento se lleva a cabo con componentes de validación, el medio de usuario se debe introducir en la Lista de bloqueo. A partir de este punto, el medio perdido ya no se podrá validar. El medio dejará de estar operativo cuando caduque la duración de la validación.
- Si se utiliza junto con componentes autónomos, el medio se debe registrar en la Lista de bloqueo (CardLink) y, a continuación, transferir a todos los componentes autónomos del respectivo sistema mediante el programador o el medio de servicio.
- Todos los medios registrados en la Lista de bloqueo estarán bloqueados para los componentes correspondientes.

16.3 CardLink con terminal

En el uso con terminal, en el software KEM se asigna el estado "Perdido" al medio. El medio ya no recibe validación por parte del terminal.

16.4 Lista blanca

- Es importante retirar las autorizaciones de un medio perdido.
- Si se utiliza junto con componentes autónomos sin capacidad inalámbrica, la lista actual de medios autorizados se transfiere a todos los componentes autónomos mediante el programador.

  Si se utiliza junto con componentes autónomos con capacidad inalámbrica, la lista actual de medios autorizados se transfiere a todos los componentes autónomos mediante una gateway.

  Un medio perdido ya no formará parte de esta lista.

Procedimiento

1. Abra el espacio "Elementos básicos" de la barra de funciones "Navegador".
2. Vaya a la pestaña "Medios".
3. Seleccione el medio perdido. Si quiere registrar varios medios como perdidos, selecciónelos.
4. Abra el menú contextual.
5. Vaya a "Cambiar estado".
6. Seleccione el estado "Perdido".
7. De ser necesario, puede imprimir un formulario.
8. Programar los componentes. [▸ 6.9.1]
   Inicie la transferencia de forma inalámbrica mediante una gateway.
9. Confirmar la programación. [▸ 6.9.1]

17 Borrar nombre de persona

Esta característica elimina el nombre de una persona del proyecto. Se distingue entre personas (usuarios de medios) y usuarios de KEM (administración de usuarios).

Si la administración de usuarios está activa, se necesita el derecho "Borrar nombre de persona" para acceder a la función. Esto se puede activar en los roles de la administración de usuarios. El rol "Administrador" tiene este derecho por defecto.
Si la administración de usuarios no está activa, solo se pueden borrar los nombres de las personas.

Efectos de borrar el nombre de la persona

- La persona se elimina de la organización.
- Las entradas de auditoría no se eliminan.
  El nombre será reemplazado por "Nombre borrado".
- Las entradas del libro de registro no se eliminan.
  El nombre será reemplazado por "Nombre borrado".
- Las entradas de Traceback no se eliminan.
  El nombre será reemplazado por "Nombre borrado".
- Los medios asociados con la persona están configurados como "No emitido".
  El estado "Perdido" permanece.

Efectos de borrar el nombre de usuario

- El usuario no se elimina de la administración de usuarios.
  El usuario debe ser eliminado por separado de la administración de usuarios.
- Las entradas de auditoría no se eliminan.
  El nombre será reemplazado por "Nombre borrado".
- Las entradas del libro de registro no se eliminan.
  El nombre será reemplazado por "Nombre borrado".

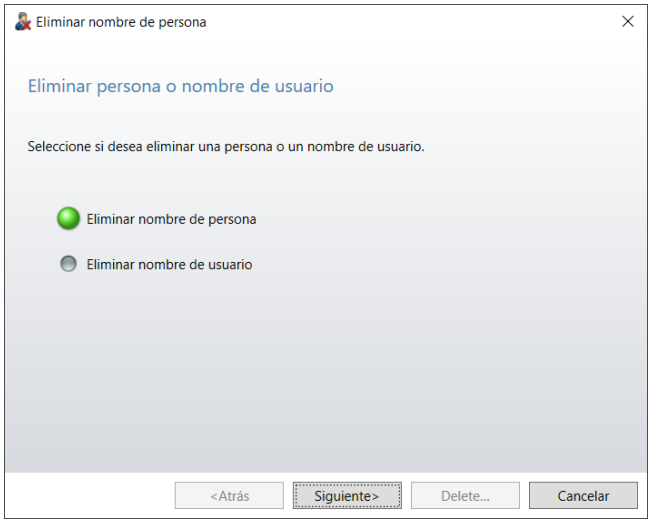
Se puede acceder al asistente "Borrar nombre de persona" desde varios menús:

- Inicio/Borrar nombre de persona
- Navegador/organización/personas
- Navegador/Traceback
- Navegador/libro de registro

17.1 Asistente para borrar nombres de personas

La acción se puede cancelar en cualquier momento hasta que se complete el asistente.
Después de ejecutar el asistente, ya no es posible deshacerla.

1. Haga clic en "Borrar nombre de persona".
2. Introduzca la contraseña.
   ⇨ Si la administración de usuarios no está activa, no se requiere contraseña.
3. Seleccione si desea borrar un nombre de persona o un nombre de usuario.
   Si la administración de usuarios no está activa, solo se pueden borrar los nombres de las personas.



4. Seleccione el nombre de la lista o introdúzcalo en el campo.
5. Haga clic en "Siguiente".

   ⇨ La descripción general contiene información sobre la frecuencia con la que aparece el nombre en las zonas afectadas.

6. Haga clic en "Eliminar".
   ⇨ El nombre se elimina de las listas de las áreas.
   ⇨ Las entradas se conservan.

Si hay varias personas con el mismo nombre, se borrarán los nombres de todas ellas.
Los usuarios deben eliminarse por separado desde la administración de usuarios.

18 Mantenimiento y cuidado

18.1 Protección de datos

Un fallo repentino del sistema puede dañar los datos de un ordenador. Es importante guardar los datos en medios de almacenamiento externos de forma regular y tener estos soportes en un sitio seguro (p. ej., en una cámara acorazada o en una caja de seguridad).

En las Propiedades de proyecto se pueden automatizar las copias de seguridad.

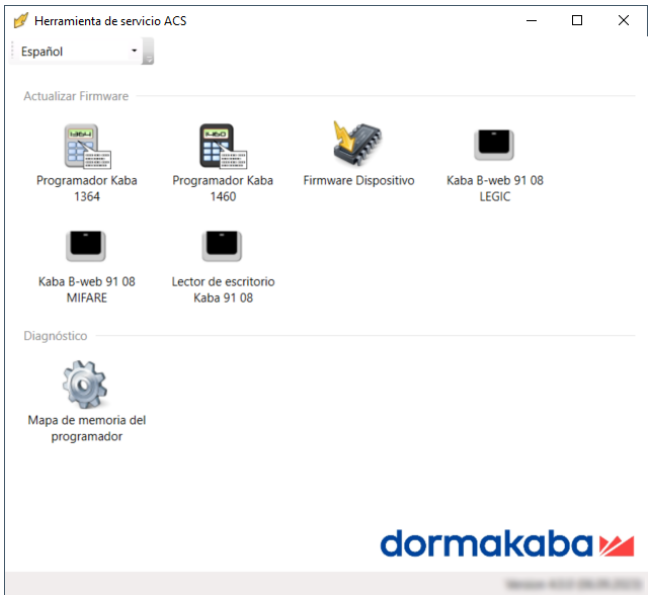
18.2 Actualizar dormakaba evolo Manager

Las actualizaciones se pueden adquirir del canal de distribución. Todas las actualizaciones de una versión principal (por ejemplo, de 7.0 a 7.2) son gratuitas. La instalación se debe realizar de la forma descrita en el capítulo Instalación del software.

19 Herramienta de servicio ACS

La Herramienta de servicio ACS es un programa de ayuda para actualizar los datos del firmware y para crear diagnósticos.

La Herramienta de servicio ACS también se puede iniciar de forma directa (no es necesario que el software del sistema esté iniciado).



Programador 1364	Asistente para actualizar el firmware del programador.
Programador 1460	Asistente para actualizar el firmware del programador.
Firmware de los actuadores	Asistente para transferir el firmware de los componentes al programador.
Lector de sobremesa 91 08 LEGIC/MIFARE/MRD	Asistente para actualizar el firmware del lector de sobremesa para la tecnología seleccionada
Mapa de memoria del programador 1460	El asistente crea un archivo ZIP con el contenido de la memoria del programador. Una ayuda para resolver problemas cuando se requiera asistencia.

Antes de la actualización, el firmware debe descargarse de Internet/Extranet y guardarse en una ubicación del disco duro local.

El programador 1364 ya no está disponible y ya no es compatible. Firmware más reciente descargable: 1.38

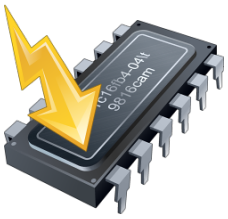
19.1 Programador 1460 - Actualizar firmware

1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el programador con el ordenador.
3. Pulse el botón "Programador 1460".
4. Siga el asistente.
5. Seleccione el archivo del firmware actual y pulse "Siguiente".
   ⇨ El programador se actualiza.
6. Pulse el botón "Listo".

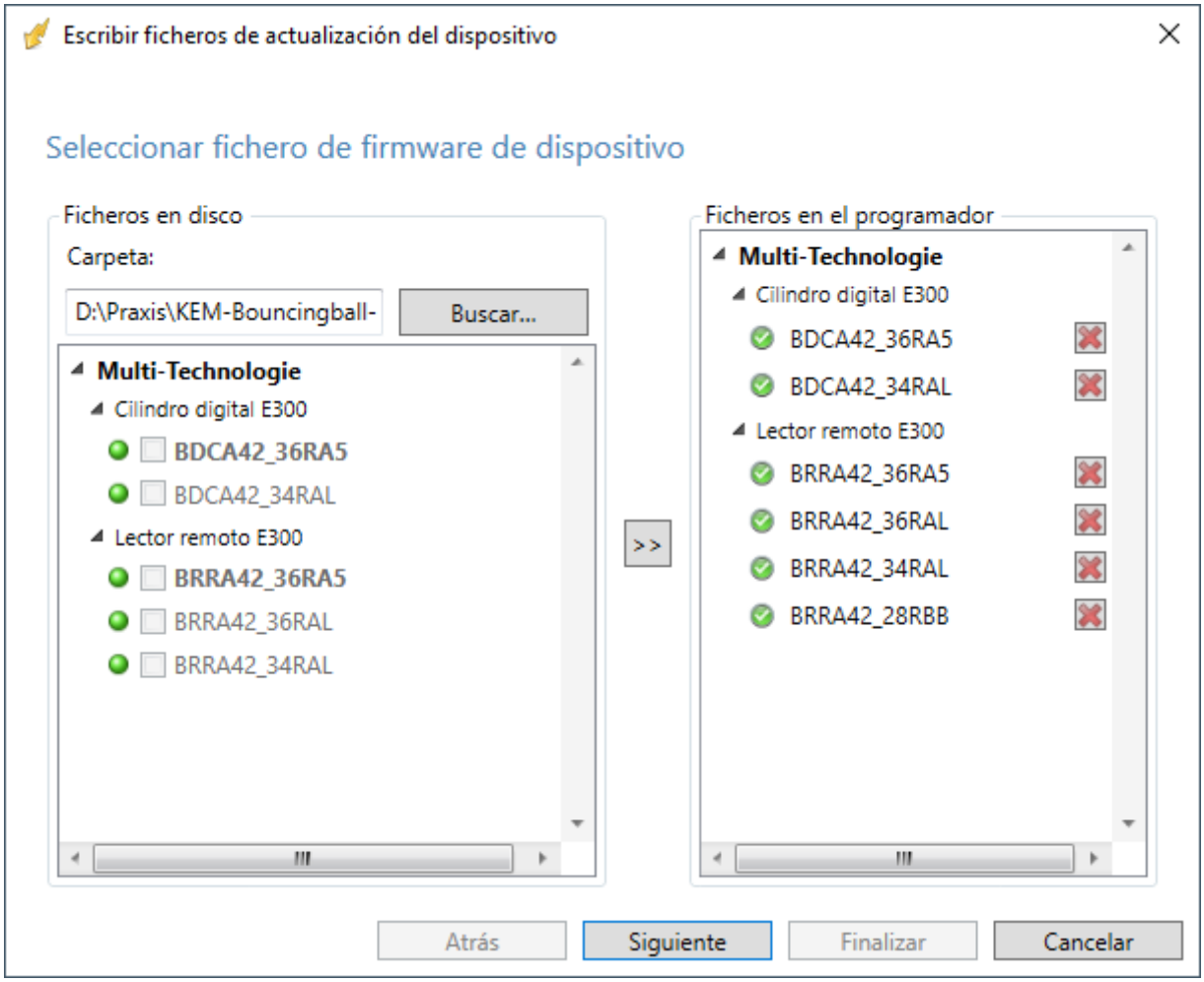
19.2 Programador 1364 - Actualizar firmware

1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el programador 1364 con el ordenador.
3. Pulse el botón "Programador 1364".
4. Siga el asistente.
5. Seleccione el archivo del firmware actual y pulse "Siguiente".
   ⇨ El programador se actualiza.
6. Pulse el botón "Listo".

19.3 Actuadores - Actualizar firmware



1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el programador con el ordenador.
3. Pulse el botón "Firmware de los actuadores".
4. Siga el asistente.
5. Seleccione el archivo del firmware actual.
   Aviso: Los archivos que aparezcan como inactivos ya están en el programador. Los archivos actuales están marcados con una chincheta verde.
6. Transfiera los archivos marcados al lado del programador mediante el botón "Flecha" (del medio).
7. Pulse el botón "Siguiente".
   ⇨ Los archivos de firmware seleccionados se transfieren al programador.



También se pueden copiar varios archivos de firmware directamente del explorador a la carpeta "Archivos del programador".

8. Pulse el botón "Listo".

⇨ Los archivos de firmware ahora están en el programador y se pueden utilizar para actualizar el firmware. La actualización del firmware se describe en el manual de instrucciones del programador 1460.

19.4 Actualizar lector de sobremesa 91 08

Lector de sobremesa MIFARE/LEGIC

1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el lector de sobremesa con el ordenador.
3. Haga clic en "Lector de sobremesa 91 08 <tecnología seleccionada>".
4. Siga el asistente.
5. Seleccione el archivo del firmware actual.
6. Haga clic en "Siguiente".
   ⇨ El lector de sobremesa se actualiza.
7. Haga clic en "Listo".

Lector de sobremesa MRD

1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el lector de sobremesa con el ordenador.

3. Haga clic en "Lector de sobremesa 91 08".
   ⇨ Se inicia la herramienta adicional "LEGIC Flasher Pro".
4. En el menú "Archivo", seleccione el archivo de firmware para la actualización.
5. Haga clic en "Descargar".
   ⇨ El lector de sobremesa se actualiza.
6. Salga de la herramienta adicional.

19.5 Crear mapa de memoria del programador

El mapa de memoria solo se puede crear con el programador 1460.

1. Inicie el programa de ayuda "Herramienta de servicio ACS".
2. Conecte el programador con el ordenador.
3. Haga clic en "Mapa de memoria del programador".
4. Siga el asistente.
5. Seleccione la ubicación de almacenamiento.
6. Introduzca el nombre del archivo.
7. Haga clic en "Siguiente".
   ⇨ El mapa de memoria se crea.
8. Haga clic en "Listo".

Actuador de validación autónomo

Los actuadores autónomos también se pueden utilizar como actuadores de validación.

Actuadores

Los actuadores son componentes que se instalan en puertas o depósitos y que se abren con medios autorizados.

Aplicaciones de medios

Las aplicaciones de medios son segmentos definidos en los medios (p. ej., para CardLink). Para poder utilizar aplicaciones y otras aplicaciones, las aplicaciones de medios deben encontrarse en los medios de usuario.

Autónomo

Así se denominan los actuadores que no están conectados con el software central y que deciden de forma independiente sus autorizaciones de acceso.

CardLink

CardLink es un sistema en el que las autorizaciones de acceso quedan depositadas en los medios. Esto permite gestionar las autorizaciones de acceso y programar medios de forma centralizada.

Clave de sistema

La clave de sistema o Sitekey es una clave específica que se asigna de forma individual a cada sistema de cierre. Un chip de seguridad crea esta clave automáticamente. Este chip de seguridad adicional está integrado en cualquier componente y, después de su inicialización, fija el bloqueo y desbloqueo individuales de todos los datos que el sistema escribe en los medios de usuario.

Componentes

Todos los actuadores, los medios y las partes de la cadena de herramientas se denominan componentes. Los componentes se distinguen por sus modelos y funciones.

Derechos de acceso

El derecho de acceso es el "derecho" para abrir una puerta o grupo de puertas en ciertas condiciones.

Días especiales

Intervalo temporal individual para los días especiales seleccionados. Se pueden crear 2 días especiales distintos: Día especial A y Día especial B. Para ello, puede crear dos intervalos temporales.

Grupo de puertas

Un grupo de puertas agrupa varias personas o puertas. El grupo de puertas se guarda como identificación en los actuadores y se le asigna un perfil temporal.

Intervalo temporal

Un intervalo temporal define el período (teniendo en cuenta vacaciones, días especiales, días de la semana, etc.) en el cual se permite el acceso. Un conjunto de intervalos temporales constituye un perfil temporal.

Lista blanca

La Lista blanca es una lista de los medios autorizados que se introduce en los actuadores. El medio solo obtendrá acceso si está incluido en la Lista blanca del actuador. Al eliminarse de la Lista blanca, un medio pierde la autorización.

Lista de bloqueo

En una autorización CardLink, los actuadores disponen de una lista de medios que ya no tienen autorización de acceso. Los medios solo obtendrán acceso si no están registrados en la Lista de bloqueo del actuador.

Master A

Un Master A es el medio programador prioritario de una estructura A/B. El Master A solo puede programar medios Master B o CardLink.

Master B

Un Master B es el medio programador que sigue a un Master A dentro de una estructura A/B. En una estructura B, es el medio programador prioritario. En ambas estructures (A/B), un Master B programa los medios de usuario de cada sistema de cierre.

Master T

El Master temporal es una forma especial de medio de programación para componentes autónomos. Estos solo son válidos durante un cierto tiempo y tienen funciones limitadas.

Medios

Término genérico para tarjetas de seguridad, medios Master (medios programadores) y medios de usuario.

Modo de paso

La función que permite poner la c-lever en posición abierta de forma manual.

Número de identificación (UID)

Cualquier medio lleva un número único de identificación de medio. El número lo emite del fabricante del medio y no se puede alterar.

Perfil temporal

Un perfil temporal es la definición del transcurso temporal de una autorización. Con él se define el inicio, el final y durante qué período un medio tiene acceso a un actuador. Los perfiles temporales se pueden definir previamente o crearse antes de la asignación de autorizaciones.

Reinicio

Los módulos electrónicos de los componentes se pueden inicializar de nuevo. Con este proceso se borrarán todos los datos (autorizaciones y Traceback) y los componentes electrónicos volverán al estado de entrega.

RTC

El reloj en tiempo real (o Real Time Clock) es el reloj eléctrico que está dentro de los componentes.

Safe UID

El Safe UID es una función de seguridad de MIFARE. En Safe UID, el número de identificación (UID) recibe un cifrado adicional y se deposita en la memoria del medio. El UID solo se reconocerá como válido si los datos de los medios de usuario coinciden.

Sitekey

La Sitekey (MIFARE) o clave de sistema es una clave específica que se asigna de forma individual a cada sistema de cierre. Un chip de seguridad crea esta clave automáticamente. Este chip de seguridad adicional está integrado en cualquier componente y, después de su inicialización, fija el bloqueo y desbloqueo individuales de todos los datos que el sistema escribe en los medios de usuario.

Software KEM

Software de gestión y configuración de sistemas de acceso.

Stamp

Stamp (LEGIC) es la llave específica que se asigna de forma individual a cada sistema de cierre. Al mismo tiempo, también se inicializan los medios de usuario.

Tarjeta de seguridad C, C1 y C2

Una tarjeta de seguridad permite inicializar un sistema de cierre con cada llave individual. Cada sistema de cierre requiere una tarjeta de seguridad específica.

Traceback de actuador

La Traceback de un actuador es un registro de eventos de todas las autorizaciones efectuadas y transferidas, así como de los intentos de acceso y los accesos efectivos. Se actualiza automáticamente y queda depositado en la memoria del actuador (si es compatible con ello). En cualquier momento se puede leer y transferir a la central.

Traceback de medios

Un Traceback de medios es un registro de eventos que se puede guardar en los medios de usuario. Estos datos pueden ser leídos por el lector de sobremesa o el terminal y transferidos al software dormakaba evolo Manager.

Validación

La validación (sello temporal en los medios de usuario) es una activación de la autorización de acceso.

www.dormakaba.com

dormakaba Schweiz AG
Mühlebühlstrasse 23
8620 Wetzikon
Suiza
T: +41 44 931 61 11

www.dormakaba.com