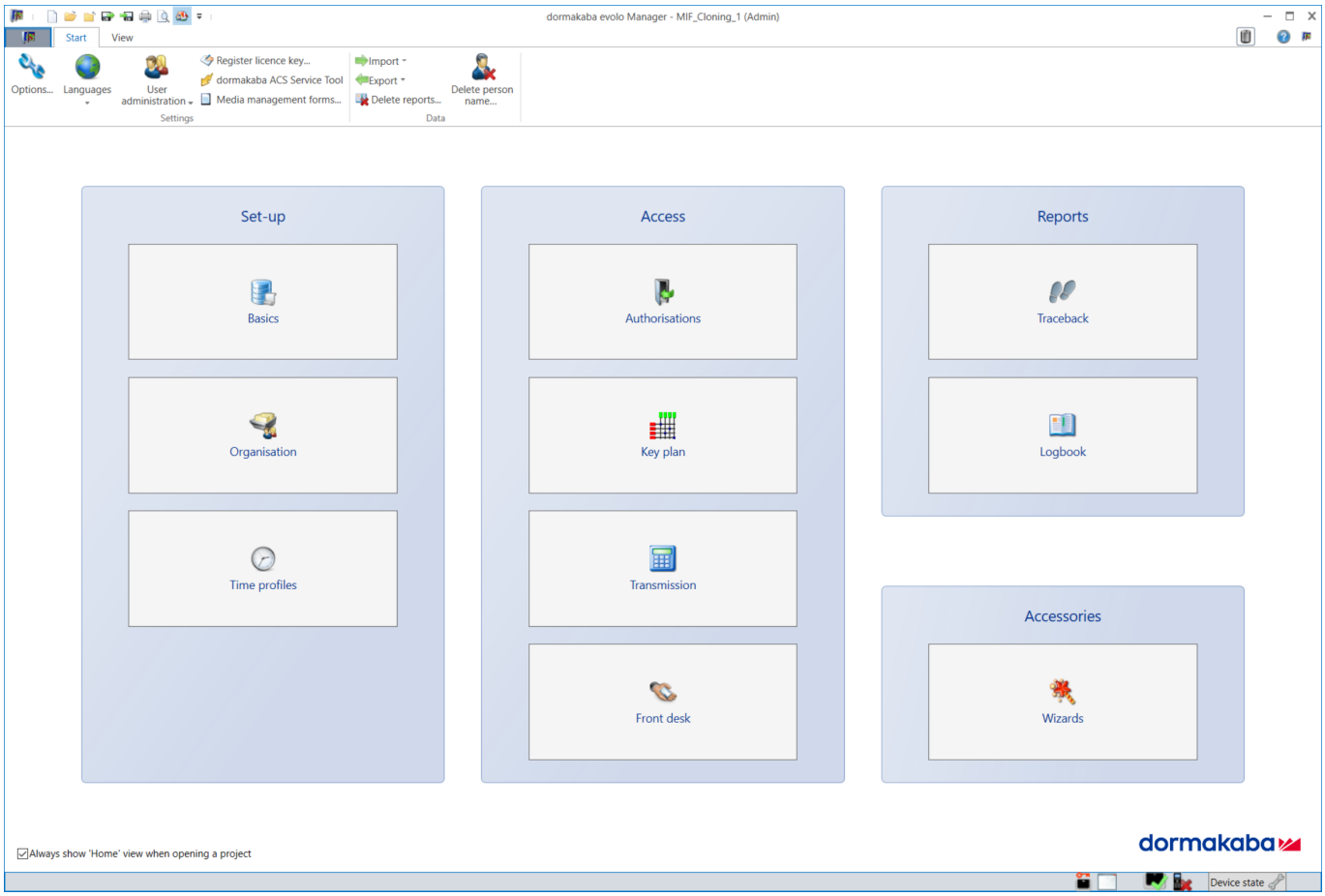
evolo Manager

V7.2

Operating Manual



Public - 06/2026

EN

Table of content

1 About this document

1.1 Validity

This document describes the product:

Product designation:	KEM (dormakaba evolo Manager)
Release:	7.2

1.2 New features and changes for version 7.2

Change	Description
Multiple content updates	This manual now contains multiple updates to reflect the updates to KEM. For example, third-party products that are no longer supported by KEM have been removed, and multiple screenshots have been updated to reflect the latest state of KEM's user interface.
PIN-code-enabled devices	KEM now supports an integrated PIN code functionality via the dormakaba 90 02 and 91 12 access devices, allowing users to authenticate directly at the reader using configurable personal PINs or shared door codes. In addition, mobile credentials (Compact Reader 9112 only) are supported, with all authorizations securely transferred from KEM to the Access Manager for local, fully traceable access decisions. For more information, see PIN-code-enabled devices.
Access Manager	KEM now employs the Access Manager 92 00, which serves as the central field controller within the KEM system. An Access Manager is responsible for managing connected readers and making local access decisions. For more information, see Access Manager.

1.3 Audience

This document is intended for specialist personnel only.

The descriptions are tailored to specialist personnel trained by the manufacturer. The descriptions are no replacement for product training.

This document also serves as a source of information for people performing the following tasks:

- Commissioning the product within the network
- Customer-specific adjustments with product parameterisation

1.4 Content and purpose

The content of these instructions is limited to the following:

- Operation of the
  - dormakaba evolo Manager (KEM) software.
  - dormakaba CheckIn software.
  - KEM Operator software.
- Putting wireless components into operation.
- Putting components with Mobile Access into operation. Description in section.
- Putting the terminal into operation.
- Putting the access manager and PIN code reader into operation.
- Installing the multi-user version.

- Using the ACS Service Tool.

Examples and projects of master key systems used in this manual are fictitious and are presented for demonstration purposes only.

1.5 Definition of terms

This user manual contains specialist terms and expressions that are explained in the glossary. In order to make reading the manual easier, the following short designations have been used in this document.

Short name	Product designation
KEM software	dormakaba evolo Manager
evolo Service	dormakaba evolo Service
ACS Service Tool	dormakaba ACS Service Tool
Programmer 1460	dormakaba programmer 1460
Programmer 1364	KABA Programmer 1364
Programmer	Programmer 1460/Programmer 1364
Desktop reader	dormakaba desktop reader 91 08
Terminal	dormakaba terminal 96 00
Access manager	dormakaba access manager 9200(-K7)
Compact reader	Compact reader 9112
Registration unit	Registration unit 9002
Mechatronic cylinder	dormakaba mechatronic cylinder
Digital cylinder	dormakaba digital cylinder
c-lever	dormakaba c-lever
c-lever	dormakaba c-lever pro
evolo	evolo
elolegic	elolegic
elostar	elostar
Gateway	Wireless gateway
Actuator	Component
NFC	Near Field Communication
Bluetooth	Bluetooth®
Smartphone	Device on which the dormakaba mobile access app is installed
mobile access app	dormakaba mobile access app
VCP	Versatile Configuration Package Configuration package

1.6 Additional documents

The following documents are available from the sales partners:

- Programmer 1460 user manual
- evolo system description
- Wireless planning guidelines
- Planning guideline, Mobile Access
- Technical manuals for the components used

1.7 Document availability

Supplementary documentation is available at the following link:

https://techdoc.dormakaba.com/cds

1.8 Warnings

This manual contains information that you must observe for your own personal safety and to avoid material damage. The information regarding your personal safety is highlighted via a warning triangle; information regarding isolated material damage does not have a warning triangle. Depending on the hazard level, the warning information is displayed in decreasing order as follows:

⚠ DANGER

High risk

Indicates an imminent danger which could cause severe physical injury or death.

⚠ WARNING

Medium risk

Indicates a possibly dangerous situation which may lead to severe physical injury or death.

⚠ CAUTION

Low risk

Indicates a possibly dangerous situation which may lead to minor physical injury.

NOTICE

Important information on the correct use of the product

Failure to comply with these instructions could lead to malfunctions. It is possible to damage the product.

The warning information for the highest level in each case is always used when several hazard levels occur at the same time. If warning information warns about personal injury, the same piece of warning information may also warn about material damage.

Other warning symbols:

General hazard

Risk of explosion

Danger from electric voltage

ESD: Danger from electrostatic discharge

Useful tips and information regarding safe operation of the product are labelled as follows:

Tips for usage, useful information.
These help to make the best use of the product and its functions.

2 Introduction

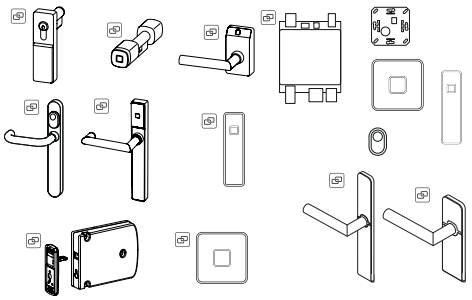
2.1 For all tasks in staff and media management

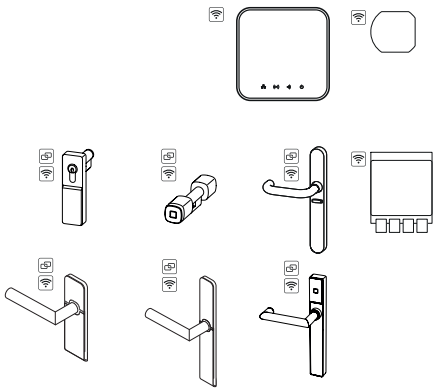
Administration of persons and media is an important component of the security concept. The KEM software fulfils both administration functions.

- Programming of evolo components MIFARE and LEGIC advant, as well as Kaba elolegic and Kaba elostar components
- Management of smartphones (media) and authorisations (components) for Mobile Access.
- Administration of lists of persons
- Logged media issues, returns and losses
- Logged changes to the locking system
- Assignment of limited-time authorisations
- Assignment of permanent authorisations
- Read out events from components (traceback [▶ 6.12])

2.2 Components of a master key system

Examples of hardware components and tool chain:





2.3 Authorisation concepts

The KEM software supports the following authorisation types: Whitelist, CardLink and mixed mode.

Mobile Access only supports Whitelist.

2.3.1 Overview of authorisation types and project mode

Project mode
If a project mode is used, this setting affects all the components in the project.

Authorisation type			
Whitelist section [▶ 2.3.2]			
	UID organisational	UID function, traceback data as UID	
	Safe UID	Encrypted UID, traceback	
	Card ID	Encrypted CID	
CardLink section [▶ 2.3.3]			
	UID organisational	Traceback data as UID	
	Traceback data as CID		
	Card ID		
Mixed mode section [▶ 2.3.4] Depending on the programmed authorisation type on the user medium, the whitelist is first used in the component. If the medium is not found on the whitelist, CardLink is used. CardLink will be used if the medium is rejected in the whitelist. If no valid authorisation is found here either, the medium will be irrevocably rejected.			
	UID organisational	UID function, traceback data as UID	
	Safe UID	Encrypted UID, traceback	
	Card ID	Encrypted CID	
CardLink and whitelist Depending on the settings of the components, the CardLink or whitelist authorisation is used.			
	UID organisational	Whitelist	UID function, traceback data as UID
		CardLink	Traceback as UID
	Safe UID	Whitelist	Encrypted UID
	Card ID	Whitelist	Encrypted CID
		CardLink	Traceback data as CID

2.3.2 Whitelist authorisation

- If there are whitelist authorisations, the media are entered into the memory of the components with access authorisation.
- The memory of a component can register up to 4,000 media (TouchGo E310 up to 2,000 media).
- Access Manager only: The number of media that can be registered depends on the particular customer license.

Modifications of component authorisations require the master medium authorised for this.

2.3.3 CardLink authorisation

With this concept, the access authorisations are written onto the user media. These are then used on the components. The authorisations are managed via the user media. No management work needs to take place on the components because the manual programming of the components is not necessary for this concept. The components for CardLink only need to be initialised once. This authorisation type also makes it possible to validate (activate for a certain period of time) user media for access authorisation on the standalone components.

Some benefits:

- A CardLink authorisation can be written directly onto the user medium.
- A visitor can be assigned an individual selection of doors or door groups on the user medium provided.
- If there are additional user media, no further configuration is necessary on the components.

Validation ensures that lost user media only remain valid until the validation period expires.

Administration area
The administration area is the area of action of an access administrator, who administers a number of access points (e.g. doors) and the associated media.
The authorization of a medium is evaluated only if the entries of the administration areas of medium and access point match. If they do not match, the medium is rejected as not authorized.

CardLink limits (V1.1):

Parameter	Value/range (number)
Doors (per administration area)	65535 (door numbers 512–65024)
Door groups (per administration area)	511 (door group numbers 1–511)
Administration areas	256
Media in a system	Unlimited
Door group rights on a medium	511 (depending on memory capacity on the medium)
Individual rights on a medium	Maximum 255 (depending on memory capacity on the medium)
Reservations on a medium	Maximum 100 (depending on memory capacity on the medium)
Validation period	8 (1x always, 1x 24h, 1x till .. o'clock, 4x n hours)

2.3.4 Mixed mode

Mixed mode via wireless is not yet supported by the wireless gateway.

A component configured in mixed mode evaluates the access information of a presented medium for the whitelist and CardLink.
A user medium is authorised for

- Whitelist
- CardLink
- Whitelist and CardLink

Sequence of the evaluation:

1 Whitelist

2 CardLink

Evaluate whitelist		
	The medium is on the whitelist:	
	The medium is authorised.	The component opens. The evaluation is finished. CardLink is no longer evaluated.
	The medium is not authorised or not present in the whitelist.	Evaluate CardLink.
Evaluate CardLink		
A CardLink authorisation is saved on the medium:		
	The medium is on the blacklist.	Blocked media are listed in the CardLink blacklist. Also see section. The medium is rejected. The evaluation is finished.
	The medium is authorised.	The component opens. The evaluation is finished.
	The medium is not authorised, e.g. outside the time frame.	The medium is rejected. The evaluation is finished.
	No CardLink authorisation is saved on the medium, e.g. there is no authorisation for the component.	

MRD components with firmware version 42.xx or higher support this mode.

2.3.5 Overview of the technologies and types of authorisation

	Authorization types					
Technologies	**Whitelist UID**	**Whitelist CID**	**CardLink 1.0**	**CardLink 1.1**	**Media TRB***	**Safe UID**
Media						
MIFARE classic	✓	✓	✗	✓	✗	✓
MIFARE DESFire	✓	✓	✗	✓	✓	✓
LEGIC advant 14443	✓	✓	✗	✓	✓	✓ [1]
LEGIC advant 15693	✓	✓	✗	✓	✗	✓ [1]
Components						
MultiRFID Device (MRD)[2]	✓	✓	✓	✓	✓	✓
elolegic (LEGIC prime)	✓	-	✓	✗	✗	✓ [1]
elostar	✓	✗	✗	✗	✗	-

Legend:

✓ is possible

✗ is not possible

* Media traceback

[1] LEGIC (Safe) UID

[2] Authorization types based on technology selected

2.3.6 Mobile Access

The requirements, set-up and parameter setting of media and components for Mobile Access is described in a special section under Mobile Access. Knowledge required for operating the KEM is specified in the description.

3 Installation and configuration

3.1 System requirements

Before the KEM software can be installed, the Windows operating system must be updated to the latest version.
The additional components are part of the installation and are installed if they are not yet present on the system.

As of KEM Version 7.2, 32-bit systems are no longer supported.

The following table shows the minimum requirements for the installation.

Operating system (64-bit)	Windows 11 Windows 10 Windows Server 2025 Windows Server 2022 Windows Server 2019 Windows Server 2016
Processor	x64 architecture **NOTICE! ARM-based processors are not supported.**
Main memory	1 GB (2 GB RAM recommended)
Hard drive memory	6 GB (including all Microsoft additional components)
Interfaces	2x USB
Screen resolution	1024 x 768 pixels (1920 x 1200 pixels recommended)
Additional components	.Net Framework 4.8 Microsoft SQL Server 2019 Express dormakaba ACS Service Tool
Compatible	SQL Server 2025 SQL Server 2022 SQL Server 2019 SQL Server 2017

3.2 Installing software

You can only install software on the computer with administrator rights.
It may be necessary to disable any firewall present while installing the software.

Choose from the following installation options:

- Single-user installation. See Installing the single-user version
  The dormakaba evolo Manager software and the SQL Server used are on one computer.
- Client/server installation. Install client/server version
  The dormakaba evolo Manager software is installed on one or more client computers and the shared SQL Server is located on a separate computer called the server.

3.2.1 Installing the single-user version

The software is installed using an installation wizard (InstallShield).
Install the software including SQL Server.

- After downloading the software package, start the installation wizard.
- The installation wizard carries out the installation.
- Read and accept the software licence agreement. The software will not be installed if the licence agreement is not accepted.
- The installation directory can be modified by selecting the 'Change' button. We suggest keeping the default specifications for the target folder, e.g.

  `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\<Installation directory structure of a 64-bit system>.`
- Pay attention to the messages and notes on the screen during installation.
- Only continue or restart the PC when prompted.

3.2.2 Installing the client/server version

A client/server operation can only be operated within the same domain. In other cases, a corresponding trust must be set between the two domains.

Proceed as follows:

3.2.2.1 Installing the server

Install the dormakaba evolo Manager (KEM) software including SQL Server on the server. The SQL Server receives the corresponding login data through the installation. The KEM software is not required for operation and can be used for testing.

1. Unzip the download into any directory on the hard drive and start the installation wizard.
2. The installation wizard carries out the installation.
3. The installation wizard checks which software components are still to be installed and shows these in a window.
4. Software licence contract step: Read and accept the licence contract. If the licence contract is not accepted, the software cannot be installed.
5. In the target folder step: The installation directory can be customised using the 'Change' button. We suggest keeping the default specifications for the target folder, e.g. `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\<Installation directory structure of a 64-bit system>`
6. Set up network drive/folder: The client user and SQL Server service must have access rights to this network drive. See section [▸ 3.2.2.5]

3.2.2.2 Installing the client

The software is installed using an installation wizard (InstallShield).

1. Unzip the download into any directory on the hard drive and start the installation wizard.
2. The installation wizard carries out the installation.

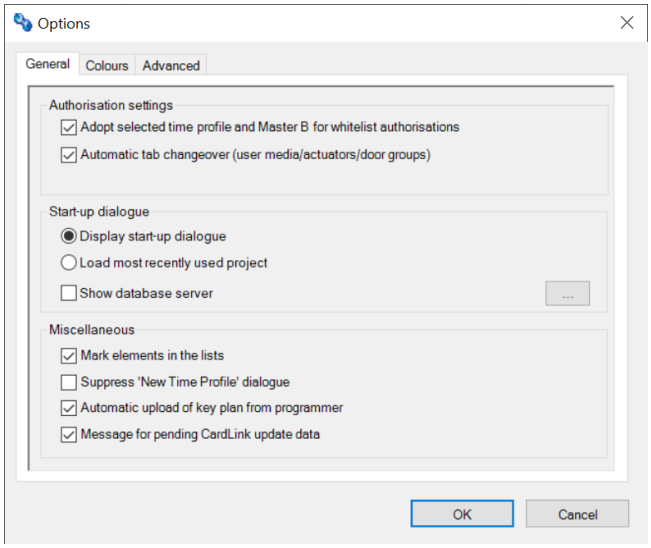
Step 3: The SQL Server does not have to be installed on the client. The status 'Skipped' will be shown in the wizard for Microsoft SQL Server.

3. The installation wizard checks which software components are still to be installed and shows these in a window.
4. Software licence contract step: Read and accept the licence contract. If the licence contract is not accepted, the software cannot be installed.
5. In the target folder step: The installation directory can be customised using the 'Change' button. We suggest keeping the default specifications for the target folder, e.g. `C:\Program Files\Kaba\dormakaba evolo Manager V7.X\ (installation directory structure of a 64-bit system)`
6. Set up network drive/folder: The client user and SQL Server service must have access rights to this network drive. See [▸ 3.2.2.5]

3.2.2.3 Activate database server display

1. Start the server on which the database (SQL Server) has been installed.
2. Launch the dormakaba evolo Manager software on the client.
3. The 1st 'dormakaba evolo Manager' dialogue window or select 'Cancel'.
4. Select the 'Options' menu from the 'Start' toolbar.
5. Navigate to the 'General' tab in the 'Options' window.
6. In the 'Start-up dialogue' section, activate the 'Show database server' checkbox.
7. If necessary, click on the '...' button and either select a database server from the list of favourites or add a new database server.
8. Click 'OK'.

⇨ Available database servers can be selected in Favourites when opening or creating a project. To edit the selection, see the 'Edit database server' [▶ 3.2.3] section.



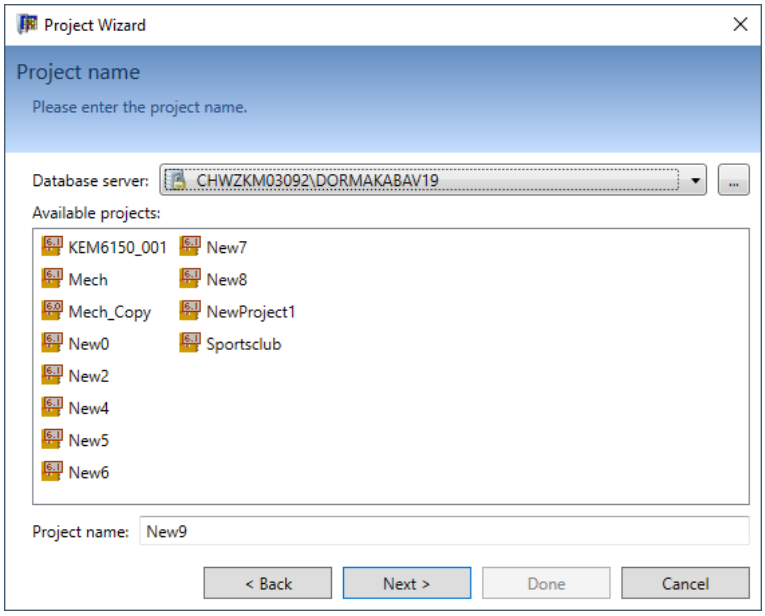
3.2.2.4 Opening a project on the database server or creating a new one

If a central database server is used, it must be selected on each client.

A KEM project cannot be opened by several clients simultaneously.

Procedure for creating a new project

1. Start the KEM software on the client.
2. Select 'New project [▶ 6.1.1]' to create a new project (Ctrl+N).
3. Follow the wizard's instructions.
4. Select the database server. If the server does not appear in the list, go to Edit database server [▶ 3.2.3].
5. Create the project name and click 'Next'.
6. Follow the wizard's instructions.

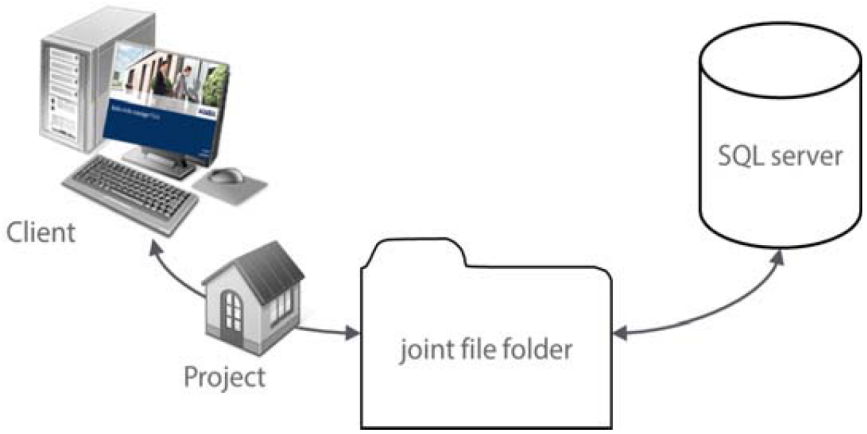


Procedure for opening a project

1. Start the KEM software on the client.
2. Select the database server from the list for an existing project. If the server does not appear in the list, go to Edit database server [▶ 3.2.3].
3. Select the project name (existing projects).
4. Click 'Open'.

3.2.2.5 Shared folder for client/server project import and export

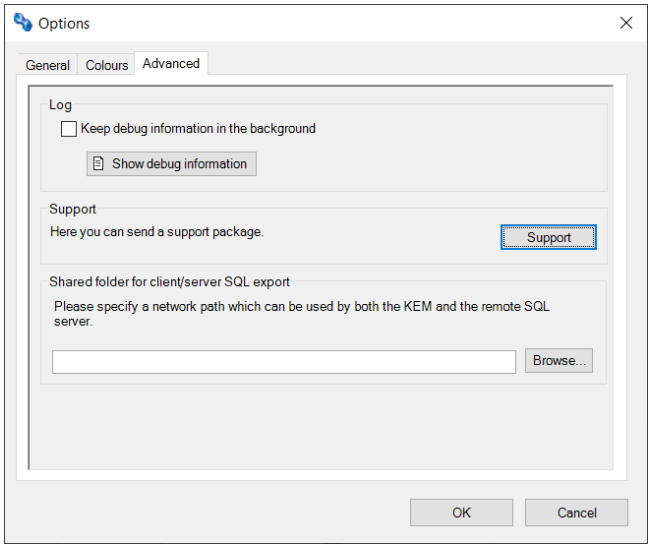
The SQL Server and the client require full access to a shared folder.
The folder is provided by the local system administrator.



Administrator rights are required to set up the shared folder in the KEM.
Select one of 2 options:

- Log in to Windows as an administrator.
- Execute KEM as an administrator.

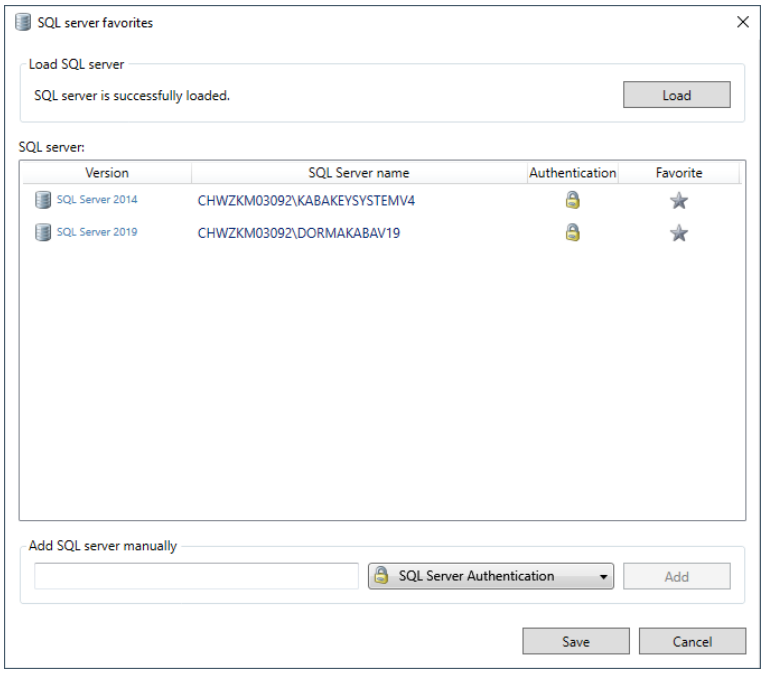
1. In the Start toolbar, select the 'Options' menu.
2. In the Options window, navigate to the 'Advanced' tab.
3. In the 'Shared folder for client/server SQL export' section, specify the network path of the shared folder (for example, `\\Server\Share`).
4. Click 'OK'.



3.2.3 Edit database server

In 'Options', 'Display database server' must be selected to use this option. See section [▸ 3.2.2.3].

Add database servers



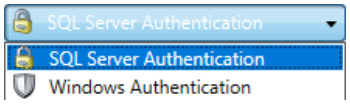
1. Choose 'Open project'.
2. Click ' ... '.
   ⇨ The SQL Server Favourites selection window appears.
3. Click 'Load'.
   ⇨ All database servers found are displayed.
4. Mark/unmark the desired server(s) as favourite.
   ⇨ The star is coloured yellow for the selected entries.
5. Click 'Save'.
   ⇨ The selected servers can be selected from the list in the dialogue.

Add database server manually
If the desired database server is not in the list, manually add the server.

Procedure:

1. Enter 'Computer name\SQL Server instance name' in the 'Add SQL Server manually' row.

2. Select authentication method.



3. Click 'Add'.
4. Click 'Save'.

⇨ The server is added to the list and marked as a favourite.

⇨ The server can be selected from the list in the dialogue.

3.2.4 SQL Server with Windows authentication

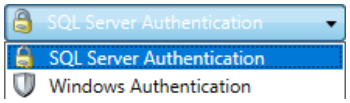
By default, KEM uses SQL Server authentication between the KEM and the SQL Server. Users with expanded security requirements can use Windows authentication.

In the 'Options > General' menu, the 'Display database server' option must be activated.

This SQL Server connection variant is ONLY suitable for persons who have an in-depth understanding of the configuration and administration of SQL Server.

With this option, the KEM user management can be restricted by the rights of the SQL Server.

KEM uses 2 authentication methods:



- SQL Server authentication (default)
- Windows authentication

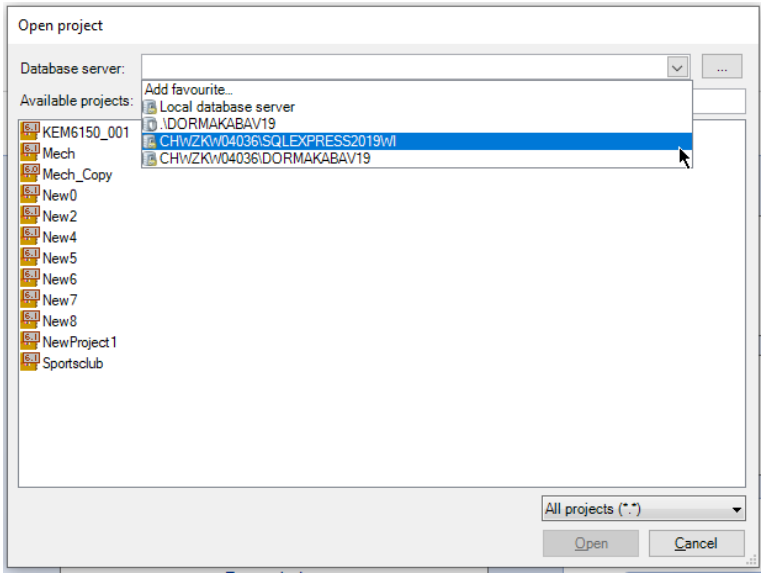
The method can be assigned to each SQL Server instance individually.

3.2.4.1 Operation with Windows authentication

3.2.4.1.1 Set up authentication in the KEM

When opening or creating a new project, select the database server with Windows authentication from the Favourites list. The projects stored on the selected database server are displayed.

The user must have the right to view database entries on the SQL Server.



If the desired server is not in the list, click on the 3 dots to edit [▸ 3.2.3] the list of database servers.

3.2.4.2 Set up SQL Server

The SQL Server settings cannot be performed with KEM. We recommend using existing software for this purpose. For example, SQL Server Management Studio from Microsoft. The software can be downloaded from Microsoft.

- dormakaba does not support this software. If you need support, please contact Microsoft.

The user is logged in to Windows and is running KEM (Domain Account). To keep the server and database rules simple, register the domain account as a SQL Server login and assign the following roles:

1. On the SQL Server, create a login for the Windows user with dbcreator rights.
2. Set the database role 'db_owner' on all databases that the user needs.
3. Connect the dormakaba evolo Manager to the SQL Server using Windows authentication.

If only Windows authentication is to be used, switch the SQL Server to 'Windows authentication mode'.

3.3 Configuring the program

Once-only program configuration following software installation.

The first software start-up following installation must be carried out as an administrator.

- The configuration wizard starts.
- The configuration wizard runs through the configuration.

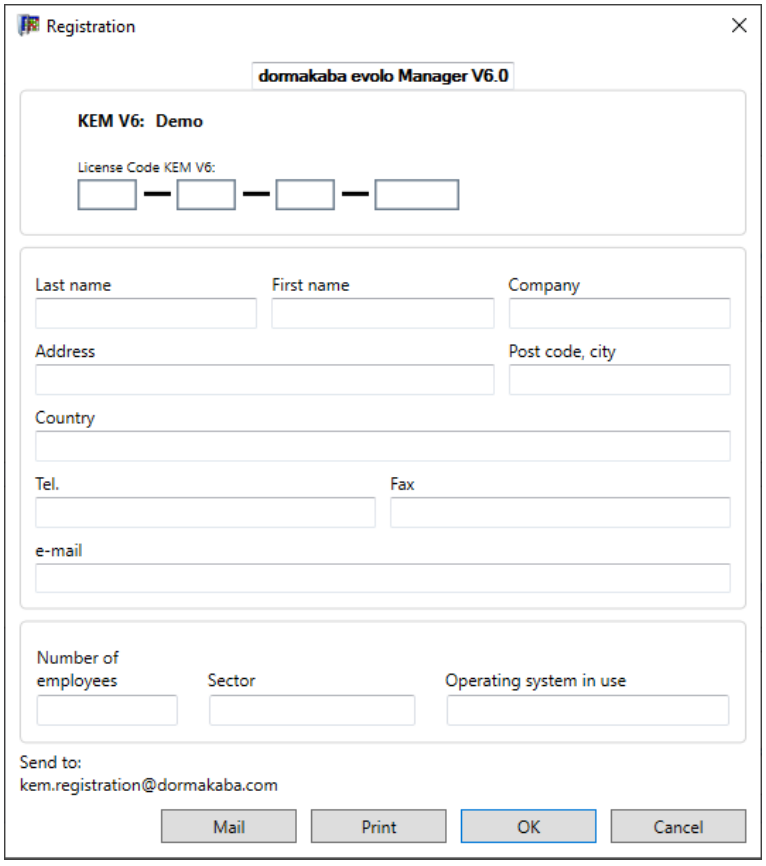
Additional basic settings step:
The KEM operator offers a greatly simplified user interface for the KEM software. However, this means there are some functionality limitations. [▶ 13.1]

License mode step:
The product ID (licence number) required for this step can be found on the licence card.

3.3.1 Registering the software licence

Login to the system as administrator or execute the software as administrator.

To register the product ID (licence number), fill out the form and send it to the indicated registration authority in one of the following ways.



- Send the filled-out form via e-mail to the registration authority using the button **Send by e-mail**.

3.3.2 Registering and upgrading the licence number

Login to the system as administrator or execute the software as administrator.

Registering the software licence. [▶ 3.3.1]

1. Select the 'Register licence key' button in the Start toolbar.
2. Enter the (upgrade) licence number.
   ⇨ The fields below open with a red background.
3. Enter the registered licence number.
   ⇨ Both licence numbers have been entered.

4. Close the window by clicking on **OK**.

3.4 Access authorisations

The KEM software manages sensitive and security-relevant data. Increased data security is achieved with the user administration [▶ 5.3.1] by restricting authorisations.

3.5 Install evolo Service

You can only install software on the computer with administrator rights.
It may be necessary to disable any firewall present while installing the software.

The evolo service is only required if a terminal or an access manager is to be used in the system.

Install evolo Service on the same computer as the KEM database server.

For the terminal to operate online, the server must always be available.

- The server must operate 24/7.
  ⇨ If the server is not available, media will only be validated.
  ⇨ If the server is not available, the media traceback log will not be read back.

For version V7.2 the evolo Service is affected by an unresolved vulnerability, which will be fixed in a later version. Take the following measures to mitigate the potential risks:

- Operate the machine where the service is running only in a protected network without any external connectivity.
- Activate a firewall on the machine and restrict any incoming traffic to only the CardLink update terminals and Access Manager for PIN codes. All other traffic should be completely blocked.

⇨ For more information, see the dormakaba Security Support Center at https://www.dormakabagroup.com/en/security and Security Advisory DKSA-26-31-031.

Requirements

- The user is registered as an administrator or has administrator rights.

Procedure

1. Start the setup program.
2. Follow the installer's instructions.

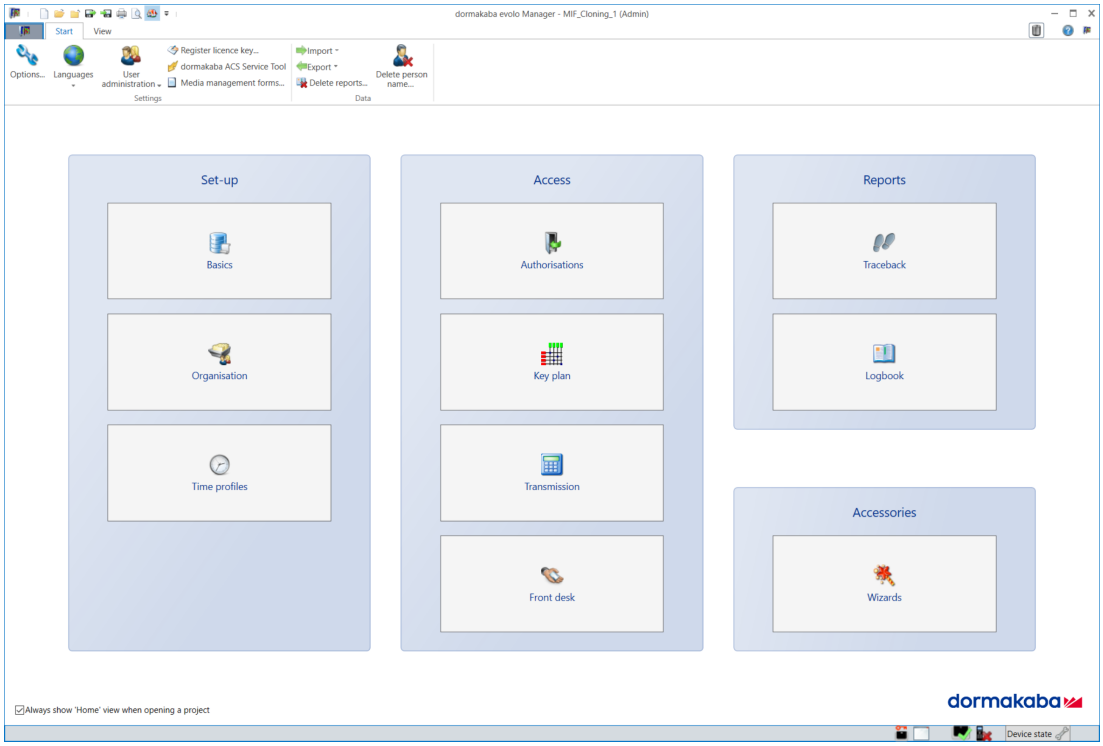
⇨ The service is automatically configured by KEM.

⇨ After the installation is completed, the evolo service starts automatically.

4 Overview

4.1 Start screen (Home)

The start screen makes all functions available in the required sequence. The start screen helps new users to navigate the system.



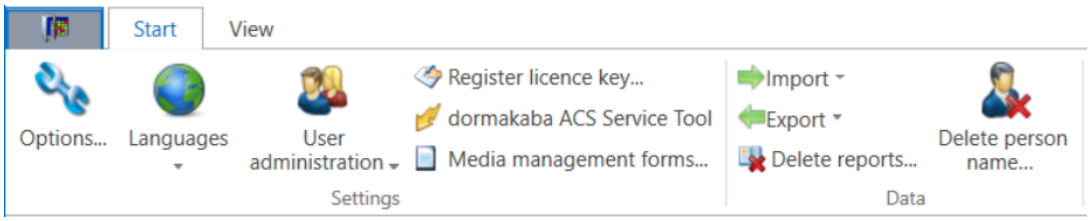
The screen elements help with the following activities:

- Setting up the basics, organisation and time profiles
- Defining access using authorisations, the locking plan or the front desk
- Transferring access data to the programmer, the wireless gateway and then to the individual components
- Displaying reports from the logbook or the traceback data
- Supported by the wizards for complex jobs

4.2 Toolbars

4.2.1 Start

All settings and data functions for the software are arranged thematically in the Start toolbar.

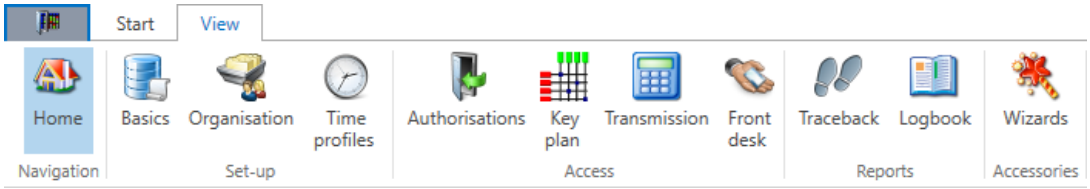


Settings	
Optional extras	See [▶ 5.1]
Languages	See [▶ 5.2]
User administration	See [▶ 5.3.1]
Register licence key	See [▶ 3.3.2]

ACS Service Tool	See
Media management forms	See [▶ 5.4]
Data	
Import	See [▶ 12.1]
Export	See [▶ 12.1]
Delete reports	See [▶ 12.4]
Delete personal name	See

4.2.2 Navigator

All functions that are needed for daily work, such as the start screen, are arranged thematically in the *View* toolbar.



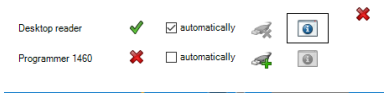
View		
Home	Start screen	Start screen (Home) [▶ 4.1]
Set up		
Basics	Media	Media
	Actuators	
	Masters	Master media
	Door groups	Door groups [▶ 6.6]
	Terminals	Terminal
	Wireless	Wireless
	Access manager	Access Manager
Organisation	Persons	Persons [▶ 6.7]
Time profiles	Time profiles	Time profiles
	Validation	Validation [▶ 6.4.2]
	Holidays/special days	Holidays/special days [▶ 6.4.1]
Access		
Authorisations	Whitelist authorisation	Setting up whitelist authorisation [▶ 6.9.1]
	CardLink authorisation	Setting up CardLink authorisation [▶ 6.9.2]
	Actuators group assignment	
	Configure CardLink	
Key plan	Overview	Key plan [▶ 6.8]
	Electronic CardLink/Whitelist	
	Mechanical	
	Group right (CardLink)	
	Door group assignment	
Transfer	Transfer (to programmer, gateways and actuators)	Transfer [▶ 6.10]
Front desk	Front desk (CardLink and Whitelist)	Reception

Reports		
Traceback	Actuator	Traceback [▶ 6.12]
	Medium	
Logbook	Logbook list	Logbook list [▶ 6.13.1]
	Protocol list	Protocol list
Accessories		
Wizards	Working with wizards	Wizards

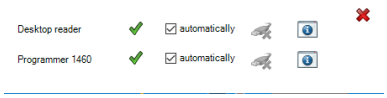
4.3 Device status, information and properties

The status bar displays all connected devices as active or inactive. The status of the desktop reader and of the media configurations is also displayed for your information.

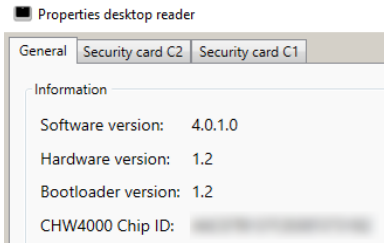
1. Click on the 'Device status' button to open the information window.



2. The connected devices can be manually connected or disconnected in this window if the tick is removed from the 'automatically' checkbox.
   Click on the device symbol for manual connecting or disconnecting.



3. In addition, you can click on the information symbol in order to see information about the desktop reader and to view or adjust programmer properties (F4\'Display programmer properties...' button), as shown in the following example using a LEGIC desktop reader.



Additional information about security cards C1 and C2 can be found in section or in the evolo system description.

4.4 Wizards

This chapter covers all the wizards available in the KEM software. In the program selection, only wizards which can be used with the selected technology are offered.

4.4.1 Lost media

This wizard helps you take the necessary steps to keep the site secure.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.2 Replacement badge

This wizard helps you create a replacement badge while maintaining site security.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.3 Read back service medium

This wizard reads traceback and status data of the components from the service medium into the project.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.4 Generating new door group

This wizard helps you create new door groups.

	MIFARE	LEGIC advant	elolegic*	elostar
	✓	✓	✓	✗

* Only possible for U-line

4.4.5 Create master

The wizard will help you to create a programming master.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✗	✗	✗

4.4.6 Update a temporary master

This wizard helps you update a Master T. The wizard is only enabled once the security card has been read in.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.7 Create new service medium

The wizard helps create a service medium The service medium is needed to disable individual user media at certain components.

	MIFARE	LEGIC advant	elolegic*	elostar
	✓	✓	✓	✗

* A prime card can be converted to a service medium. The following restriction applies: the status cannot be read out.

4.4.8 Copy media

This wizard helps you copy the authorisations from one medium to other media.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✓	✓

4.4.9 Copy components

The wizard helps copy authorisations from one component to other components.

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✓	✓

4.4.10 Locker lock

This wizard helps you create or read a locker lock medium.

	MIFARE	LEGIC advant	elolegic	elostar
	✗	✗	✓	✗

4.4.11 Locker lock 21 10

This wizard helps you create or read media for locker lock 21 10. The following are supported:

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

4.4.12 Update MIFARE DESFire key settings

The wizard helps you to adjust the key settings on a MIFARE DESFire user medium.
For the description and procedure, see chapter [▶ 6.3.4].

	MIFARE	LEGIC advant	elolegic	elostar
	✓	✗	✗	✗

4.4.13 Import Mobile Access digital key voucher

The wizard helps you to import digital keys for Mobile Access applications from a PDF document.

For the description and procedure, see chapter.

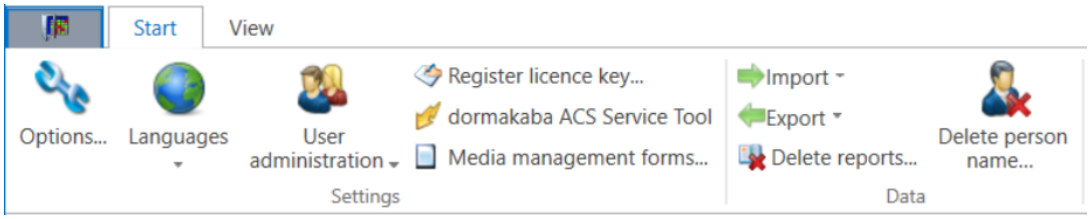
	MIFARE	LEGIC advant	elolegic	elostar
	✓	✓	✗	✗

5 Settings

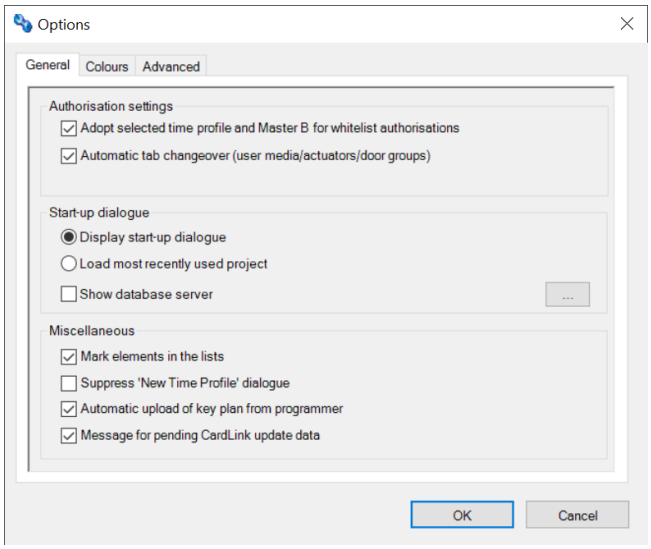
Various basic settings are available for the KEM software.

5.1 Optional extras

- Select the "Options" area (Ctrl+Shift+O) in the Start toolbar.



General

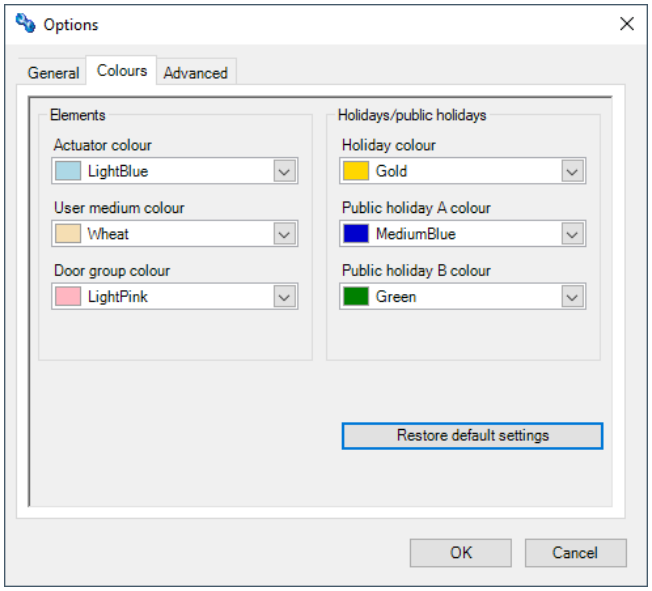


General	
Authorisation settings	
Accept time profile and Master B selection for whitelist authorisations	The selected settings are automatically applied in the authorisation window.
Automatic tab switching (user media/actuators/ door groups)	A programming aid for experienced users.
Start dialogue	
Display Start dialogue	With this option, the Start dialogue can be switched on or off.
Load the last opened project	The last edited project (key plan) opens. (If there is only one project, this will be opened.)
Display database server	The respective database server is displayed in the Open dialogue. Click the '...' button to select a database server from the list or add a new one.
Miscellaneous	
Selection of items in the lists	For the authorisations, the rows with the elements available for selection are marked.
Suppress the 'New time profile' dialogue.	This suppresses the dialogue for selecting the time profiles V2 and V3 or V3 and V4.
Automatic transfer of key plan to the programmer.	This option can be used to automate the transfer of the key plan to the programmer.

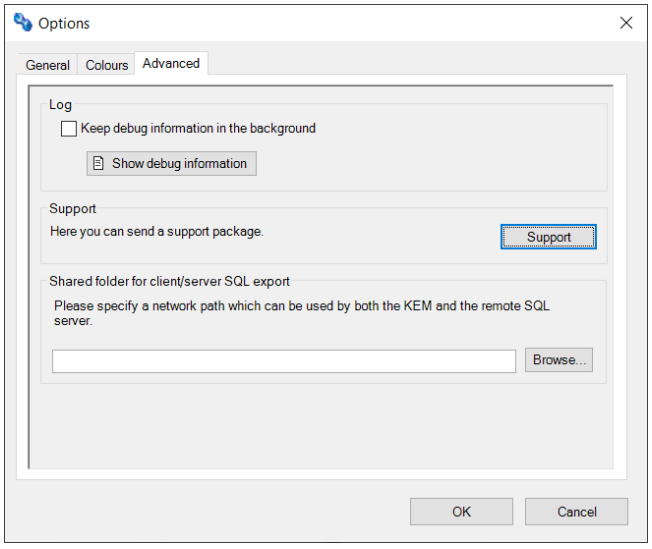
Messages for pending CardLink update data	If there is CardLink update data present that has not yet been transferred, a dialogue window appears when the project is closed offering the option of transferring the data before closing. Clicking 'Yes' takes the user to the transfer menu. This option is activated by default. The message only appears if CardLink update readers (standalone or wireless) are configured in the project.

Colours

The colour of various elements can be changed to provide better guidance.



Advanced



Advanced	
Log	
Collect debug information in the background	The information about program behaviour is recorded in a file. This file helps Support with troubleshooting.
Support	
Support – deliver package	Creates an e-mail and adds the data package with the following information: • Registration • Project data • Log files

Shared folder for client/server SQL export	
For client/server SQL export	Specify a network path which can be used by both KEM and the remote SQL server.

5.2 Changing the language

The KEM software is available in multiple languages.

1. Select the Languages menu from the Start toolbar.
2. Select the desired language from the list.

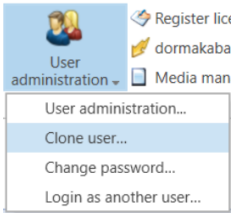
⇨ You can then continue working in the chosen language immediately.

5.3 User administration

Users can be added, edited and deleted for the active project in the 'User administration' area. Different roles and rights (user rights) can be assigned to the users. If no user is entered, user administration is inactive.

User administration should be registered separately for each project.
A pre-configured project can be passed on.
Users need the 'User management' right to be allowed to change settings or to create or delete users in the assigned role.

The function of the 'User administration' button depends on the role of the registered user.

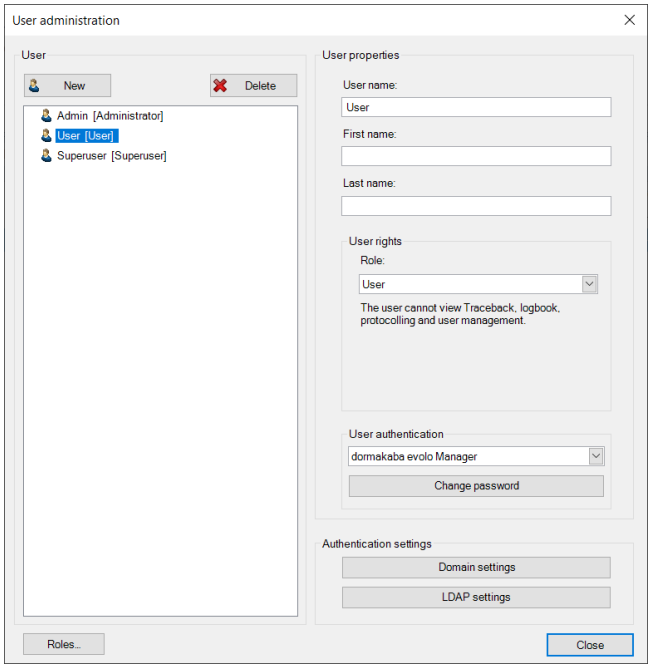


Select the function from the selection menu.

- User administration
  See section
- Clone users
  See section [▸ 5.3.2]
- Change password
  See section [▸ 5.3.1.5]
- Log in as a different user
  See section [▸ 5.3.1.6]

5.3.1 Edit user properties

Only one user at a time can be selected for editing.



- Adding a user. (See section [▶ 5.3.1.1])
- Deleting a user. (See section [▶ 5.3.1.4])
- Editing roles and rights. (See section [▶ 5.3.1.2])
- Changing/resetting user passwords. (See section [▶ 5.3.1.5])
- Assigning an authentication method to a user. (See section)
- Authentication settings. (See section)

Login procedures for user authentication

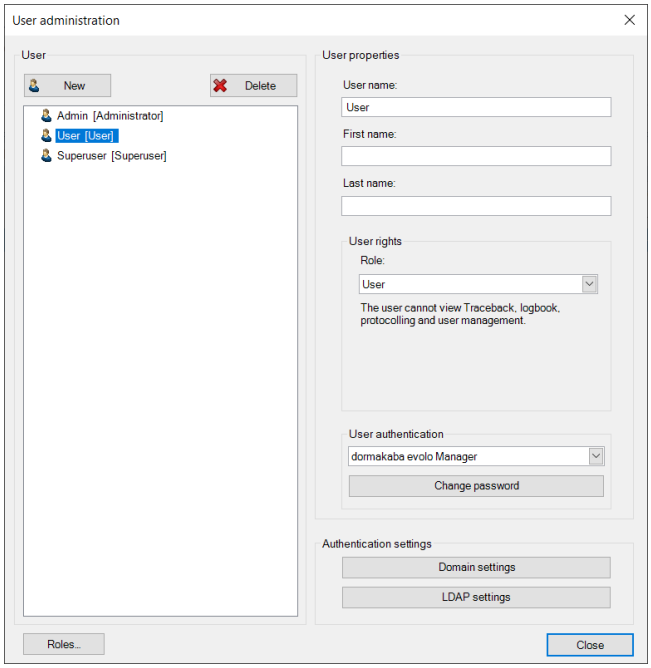
- KEM users (see section [▶ 5.3.1.3.1])
- Local users (Windows) and domain users (Windows network) (see section [▶ 5.3.1.3.2])
- Using LDAP (network directory service) (see section [▶ 5.3.1.3.3])

5.3.1.1 Adding a user

If user administration is deactivated, a user with the role of 'Administrator' must first be created.
If only a single user is registered, the 'Administrator' user right cannot be changed.

Procedure for creating new users:

1. Click 'New'.

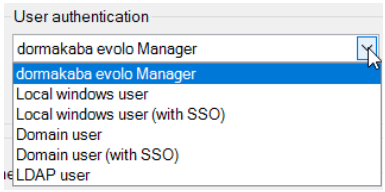


⇨ A new user is added on the left side.

2. Register the user properties on the right side.

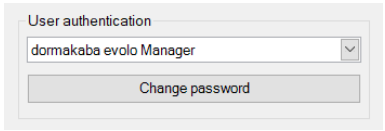
To be able to use Windows login, LDAP login or SSO, the details entered here must match the data entered for the respective login methods.
It is only necessary to assign a new password if using the 'dormakaba evolo Manager' login procedure.

3. Select the user authentication method from the list.



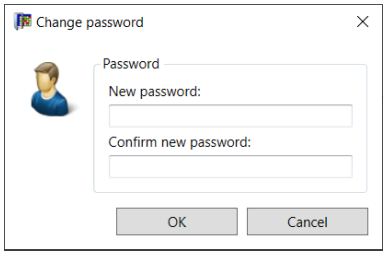
⇨ The details of the authentication settings only need to be entered once in each project before the authentication procedure is assigned to a user. See also section.

4. Click 'Change password' to open the password dialogue.



⇨ The password only needs to be entered for the 'dormakaba evolo Manager' authentication method.

5. Enter and confirm the user password.

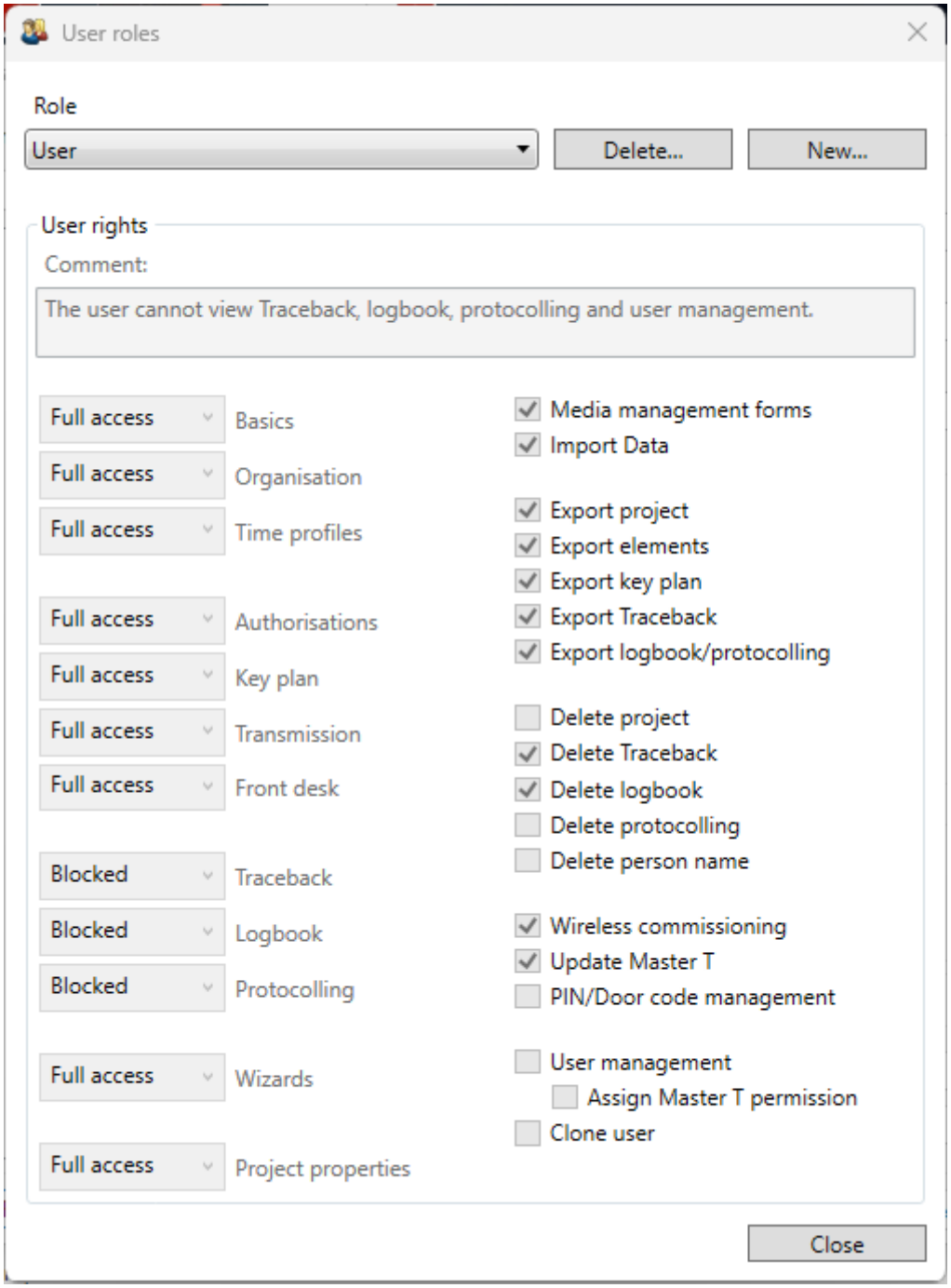


6. Click 'OK'.
7. Click 'Close' to exit 'User administration'.
   ⇨ User authentication with password is now activated for the user in question.

⇨ The user can log in to this project.

5.3.1.2 Roles and rights

Introduction
Issuing users with roles that are furnished with rights that are appropriate to their tasks improves the security of the system. This also allows the site to distinguish between administrative and regular operation and prevents any unintentional changes being made to its configuration. A person can be both an administrator and user of the site.
Users can change their role or switch to a different user account using the 'Log in as a different user' dialogue.



User rights with different roles
Users can be assigned different roles:

Roles specified in the KEM software cannot be changed or deleted.

Roles specified in KEM:

- Users

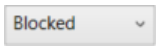
- Super user
- Administrator
- Only reception
- dormakaba CheckIn user
- ReadOnly user

To create new roles with individual rights, see section [▸ 5.3.1.2.1].

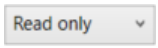
Properties of user role rights

Different user roles can be assigned various rights that permit them to access views and execute functions. When the administrator creates a user role, they can select between different viewing and access levels. No changes can be made here for roles that are predefined in KEM. If you want to change the predefined settings, you must create a new role and assign it to the user.

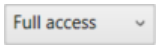
User rights for views



The user cannot view or open the view.

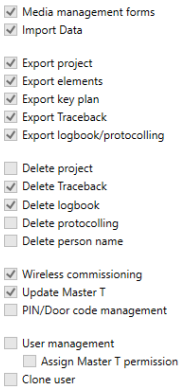


The user only has read authorisation in this view.



The user can make modifications in this view.

User rights for functions



Activate the checkboxes to enable functions for the current role.

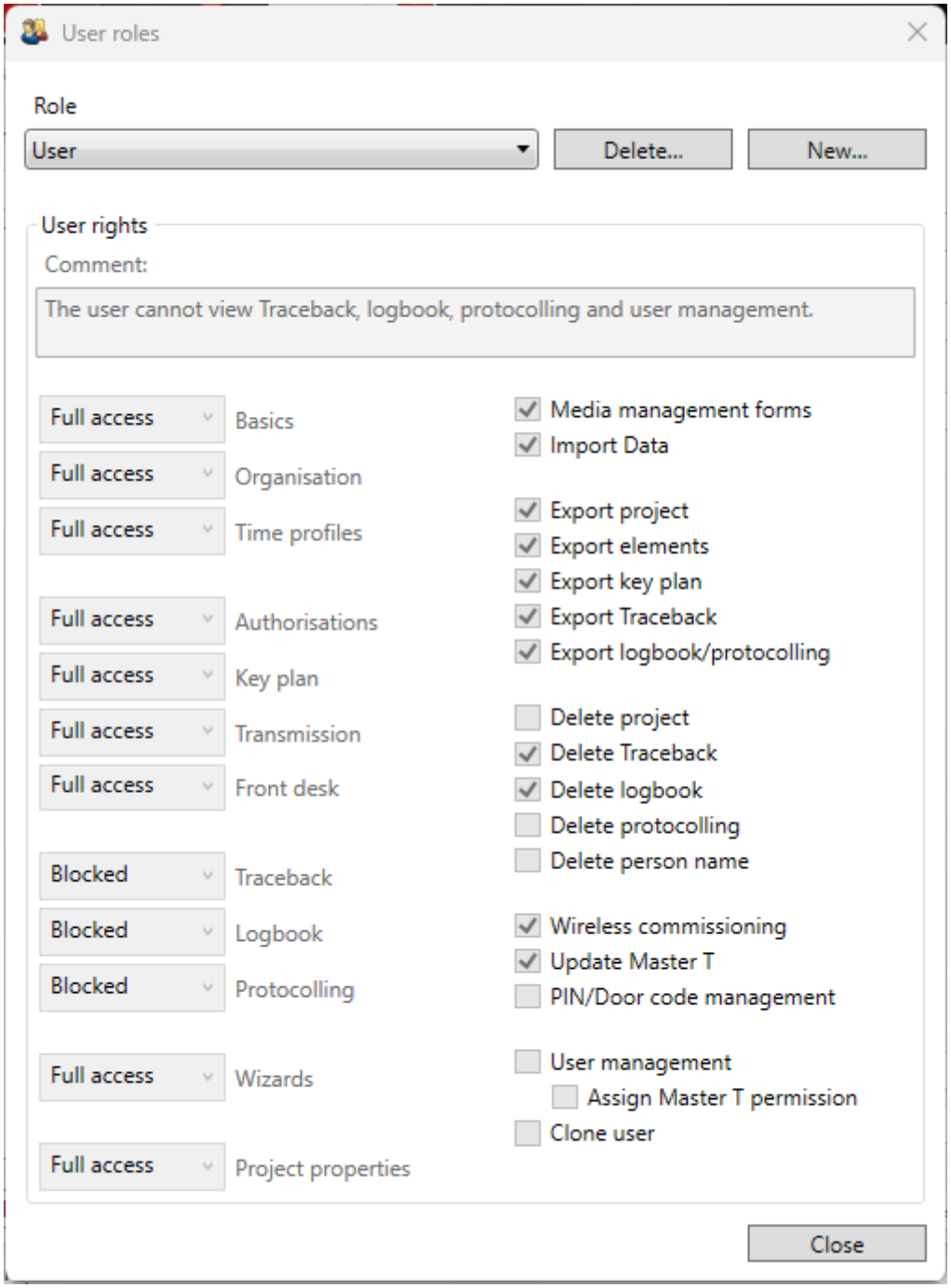
User rights for wireless commissioning

The user rights for wireless commissioning can be modified in User roles. These rights can only be modified by users with the **user management** right.

User rights for Master T

User rights for Master T can be customised in the user roles.

- The 'Update Master T' right: holders of this right can activate a Master T for an adjustable period of time. See section [▸ 6.3.2.2].
- The 'Assign Master T' right: users who are assigned this right within their role can assign or revoke the 'Update Master T' right to or from another user.
- Only users who have 'Full access' set in the user roles in the 'Basics' sub-item can add a Master T.



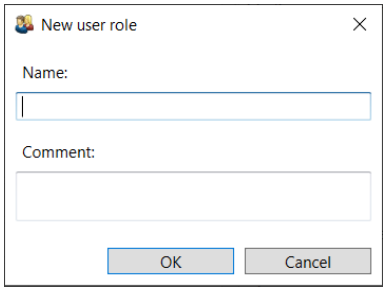
If user administration is active in a project, then a project can only be deleted by a user whose role includes the 'Delete project' right. For user administration, see [▶ 5.3.1].

5.3.1.2.1 Create new role

Create new roles with individual rights.

Procedure

1. Click 'New'.
2. Enter the name of the new role.



3. Enter a commentary if necessary.
4. Click 'OK'.
   ⇨ The new role will be automatically selected for further configuration.
5. Configure the access rights and authorisations.
6. Click 'Close'.

⇨ The role can be assigned to a user.

5.3.1.2.2 Delete role

A role cannot be deleted if it is assigned to a user.

1. Select the role to be deleted from the list.
2. Click 'Delete'.
3. Click 'OK'.
   ⇨ The role has been deleted.

5.3.1.3 Login procedure

Login data is created for administrators and users when setting up 'User management'. You can choose from various login procedures with and without SSO support.

5.3.1.3.1 KEM

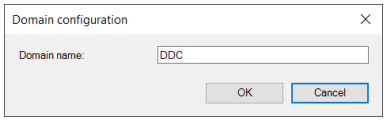
The KEM software provides its own login method.
Enter your user name and password to log in.

5.3.1.3.2 Windows

A Windows user who is already logged on locally to the PC logs in using their Windows user name and Windows password.
If SSO is used, the user is logged in to the project in their assigned role without any further password query.

Users who are known via a Windows domain network can log in to the project using the user name and password of the domain.
If SSO is used, the user is logged in to the project in their assigned role without any further password query.

The domain settings only need to be entered in the authentication settings once per project. The domain name can be obtained from the network administrator of the domain.



If a Windows user is added in KEM user administration, then the KEM user name and the Windows user name must match.

5.3.1.3.3 LDAP

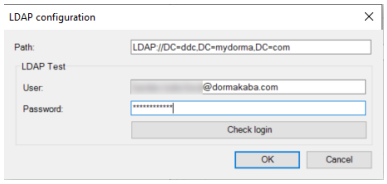
A user known via LDAP is logged in to the project in their role after entering their user name and password.

The login data is managed by the network administrator via an LDAP server. The data can be obtained from the network administrator. They only need to be entered in the authentication settings once per project.

Requirements

- The path to LDAP authentication is known.
- The user name of an LDAP user is known.
- The user's LDAP password is known.

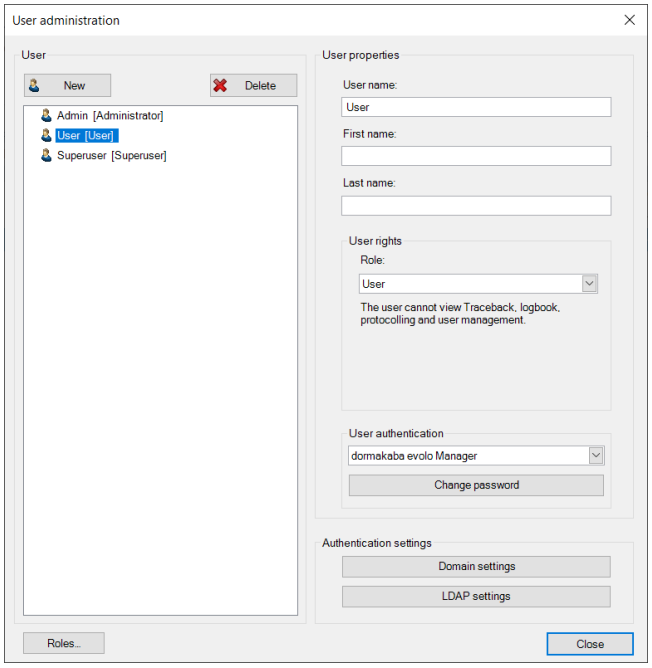
Procedure



1. Click 'LDAP settings' in user administration.
2. Enter the path for LDAP authentication in the 'Path' field.
3. Enter the user name and password.
4. Click 'Test login'.
   ⇨ The user is authenticated using LDAP authentication.
   ⇨ Result: 'Login successful'
   The saved path can be used for this and other LDAP users.
   ⇨ Result: 'Error'
   Check the entries and try again. If the error occurs again, contact the administrator.
5. Click 'OK' in the results window.
6. Click 'OK'.
   ⇨ The path is saved in KEM and the dialogue window is closed.
   ⇨ The path is not saved if the window is closed using 'Cancel'.

5.3.1.4 Delete user

Administrator



1. Select the user to be removed.
2. Click 'Delete'.
   ⇨ The user is deleted.
3. Click 'Close'.

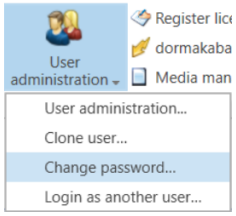
When the last user (**Admin**) is deleted, the user administration is disabled.

5.3.1.5 Change/reset password

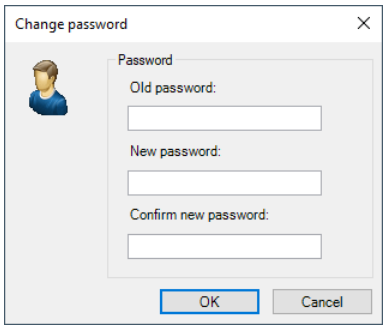
You can only change the password if you have 'dormakaba evolo Manager' authentication.

Change your own password
You need your old password in order to change your password.

1. Click 'User administration' in the 'Start' toolbar.



2. Click 'Change password' in the selection.

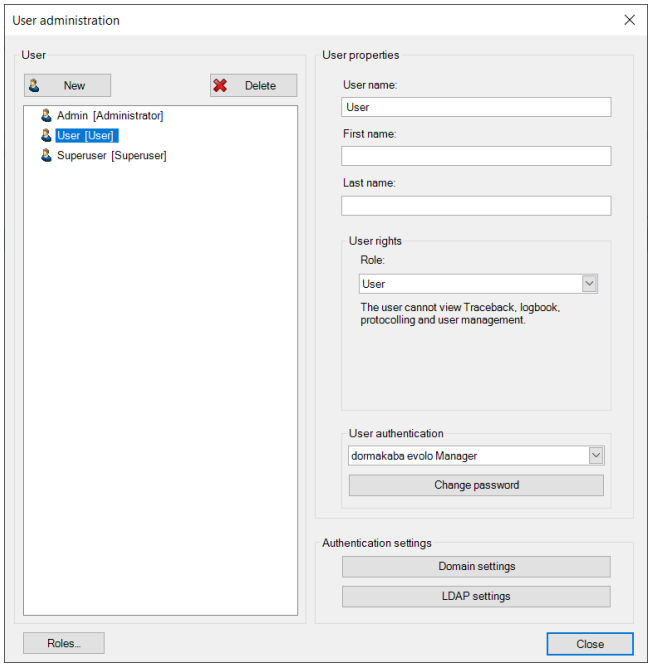


3. Enter the new password.
4. Click 'OK'.

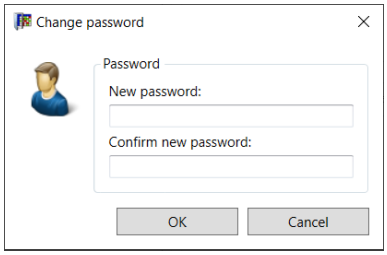
Reset password
You need the 'User management' right to do this.

Users with the 'User management' right can assign a new password to a user. The old user password is not required for this.
To change the administrator password, see 'Change your own password'.

1. Click 'User administration' in the 'Start' toolbar.
2. Click 'User administration' in the selection.



3. Select the user.
4. Click 'Change password'.



5. Enter the new password.
6. Click 'OK'.
7. Click 'Close'.

5.3.1.6 Log in as a different user

Procedure

1. Click 'User administration' in the 'Start' menu.
2. Click on the menu item 'Log in as a different user'.
3. Enter the user name and password.
4. Click 'Log in'.

5.3.2 Clone users

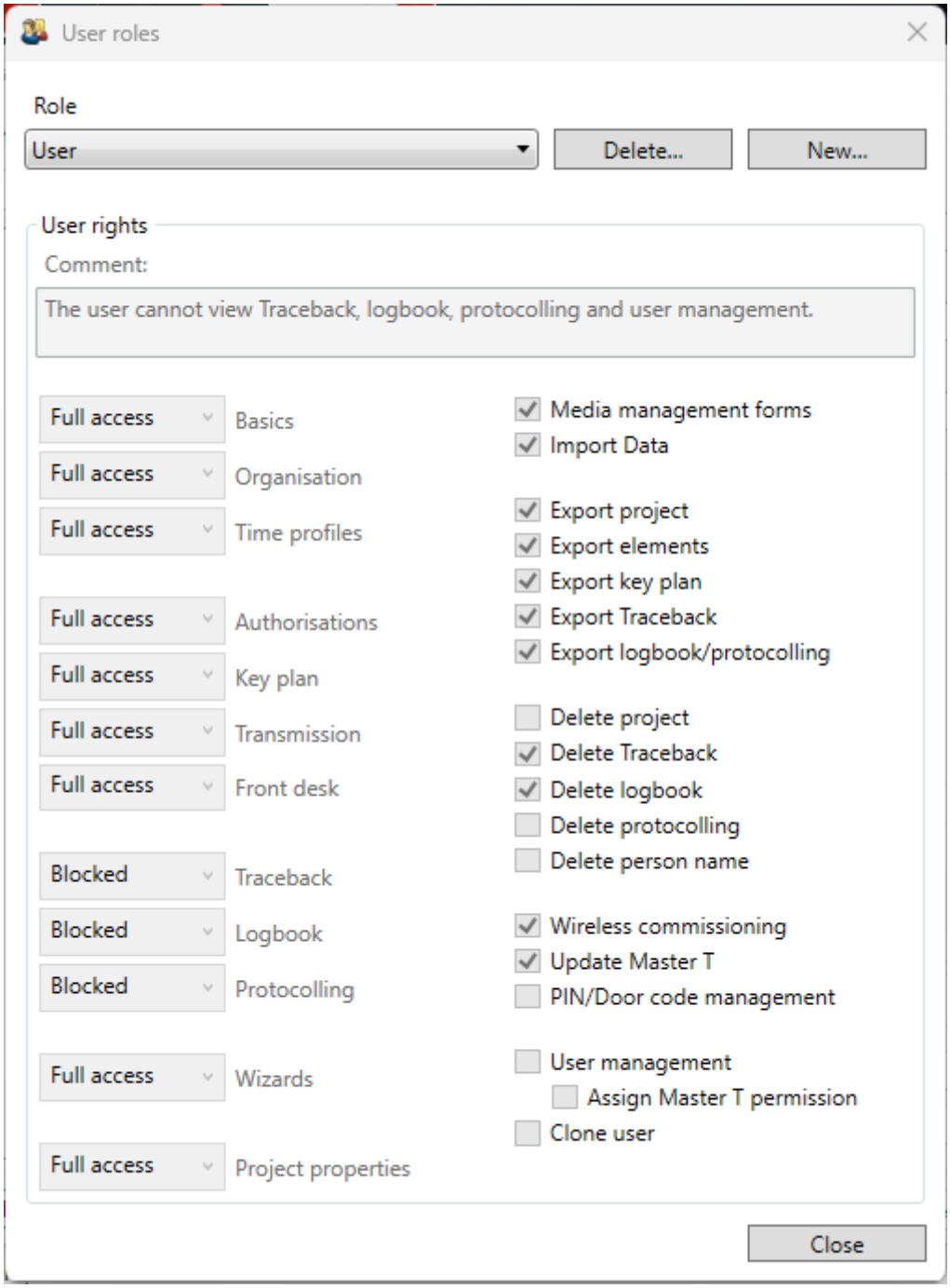
Users whose role includes the 'Clone user' right can create new users with the same role and rights as the current user.

The 'Clone user' right is not included in the predefined roles in KEM. To be able to assign this right to a user, a new role that contains this right must be created. The 'User management' right and 'Clone user' right cannot be simultaneously assigned to the same role.

See section

- Roles and rights
- Create new role [▸ 5.3.1.2.1]

Example:



Requirements

- The registered user has the right to clone users.

The new user is assigned the same user authentication method as the cloning user.

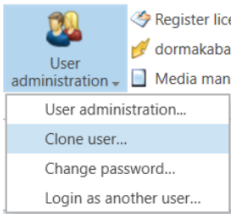
- dormakaba evolo Manager method: Assign a new password to the cloned user.
- Other methods: A user with the new username must be created in the respective system before logging in to KEM.
  The new user is created in KEM even if it does not yet exist in the system. KEM then shows a warning.

The newly created user has the same role as the creator and also has the 'Clone user' right.

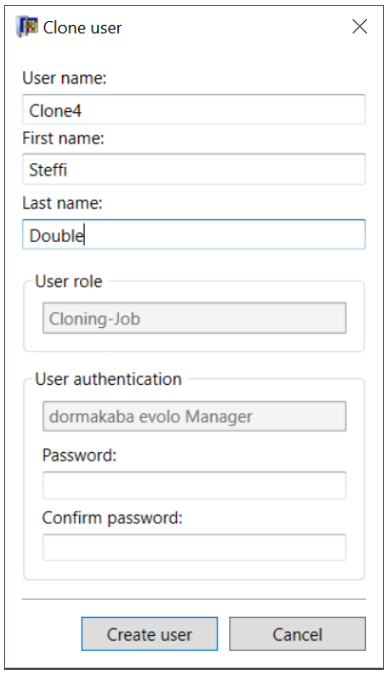
- The role of the new user can be adjusted in 'User administration' by an administrator or a user with user management administration rights.

Procedure for dormakaba evolo Manager authentication method

1. Click 'User administration' in the 'Start' toolbar.



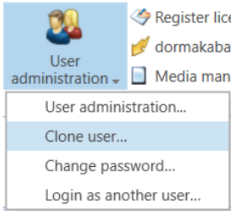
2. Select the 'Clone user' function.



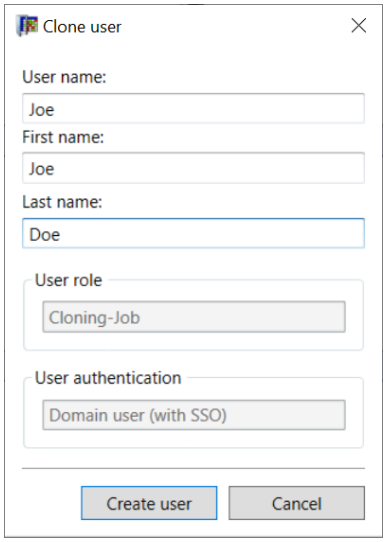
3. Enter a new username.
   Optionally enter the first name and last name of the new user.
4. Assign and confirm a new password.
5. Click on 'Create user'.
   ⇨ The new user has now been created.

Procedure for LDAP, Windows user or domain user authentication method

1. Click 'User administration' in the 'Start' toolbar.



2. Select the 'Clone user' function.

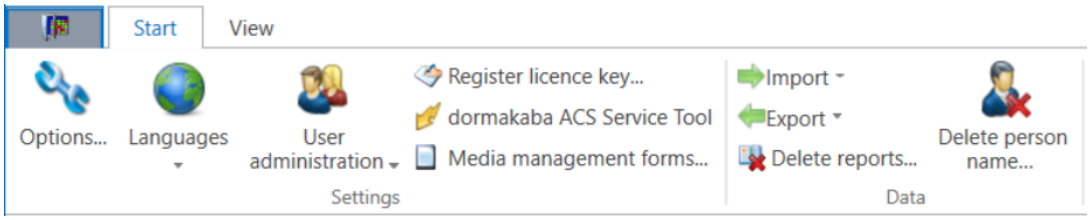


3. Enter a new username.
   For Windows and domain users, the name must match the new user's login name.
   Optionally enter the first name and last name of the new user.
4. Click on 'Create user'.

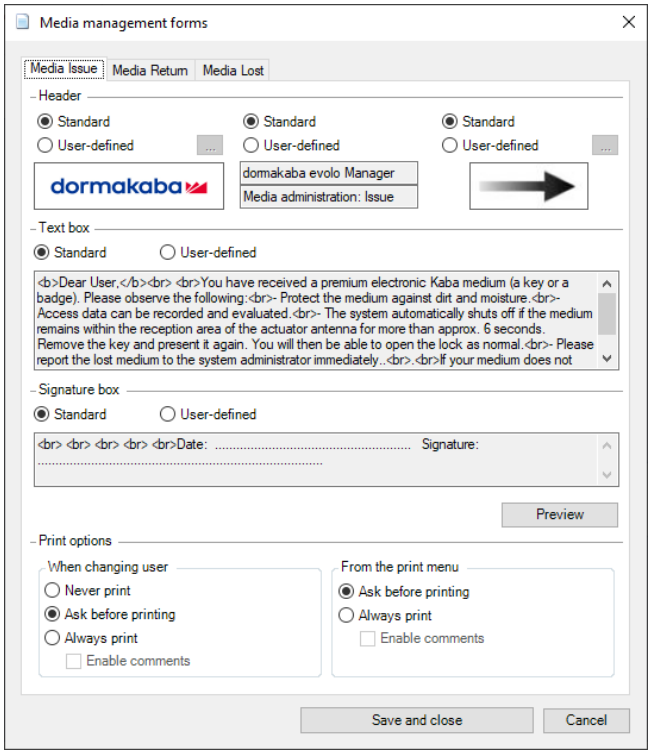
5. The user being created may not have an LDAP, Windows or domain account (example screenshot).
   Click 'Yes' to create the user entry.
   Click 'No' to cancel cloning.
   ⇨ Yes: the entry for the new user has been created.
   ⇨ No: the entry for the new user was not created. The process is finished.

Make sure the new user has the appropriate Windows or domain account and is logged in before logging in to KEM for the first time.

5.4 Customising media management forms



1. Press the 'Media management forms' button on the Start toolbar.
2. Activate the 'User-defined' option.
3. Make changes in the desired area. The example here refers to the media issue.



4. Click the 'Save and quit' button.

Tip: If only small changes to the text are necessary, the default text can be copied to the clipboard and pasted into the user-defined field. Here the desired changes can be made.

Note: If comments should also be shown, then the 'Always print' option must be selected ahead of time.

Format guidelines
The following applies to the formatting of user-defined texts:

Image data:

Image data format	JPG or GIF (max. 100 kB) Logo 160 x 40 pixels Arrow 100 x 40 pixels
Text formatting	HTML tags

HTML tags:

	Notation	Result
Bold	`<b>Example</b>`	**Example**
Underlined	`<u>Example</u>`	Example
Italic	`<i>Example</i>`	*Example*
Large font	`<big>Example</big>`	Example
Small font	`<small>Example</small>`	Example
Line break	`Example Text`	Example Text

6 Parameterising a master key system

6.1 Create/open/delete project

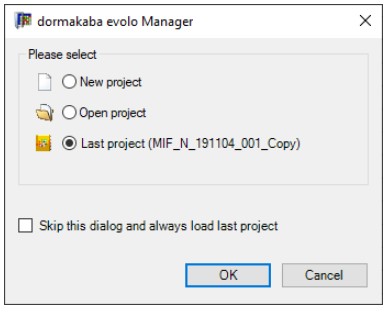
6.1.1 Creating a project

The software operates based on projects. A project must first be created before key plans, users or media can be created.

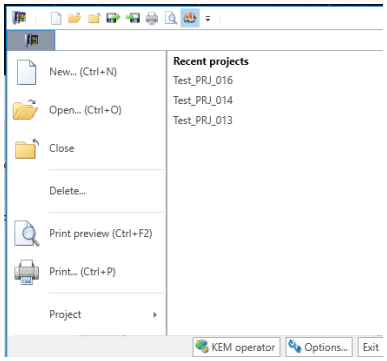
A new project can be created either when the program starts or using the 'File' menu.

Procedure

1. In the selection window when the program starts or in the 'File' menu, select the 'New project' option (Ctrl+N).
   Note: The checkbox for skipping the dialog when the program starts is not activated.

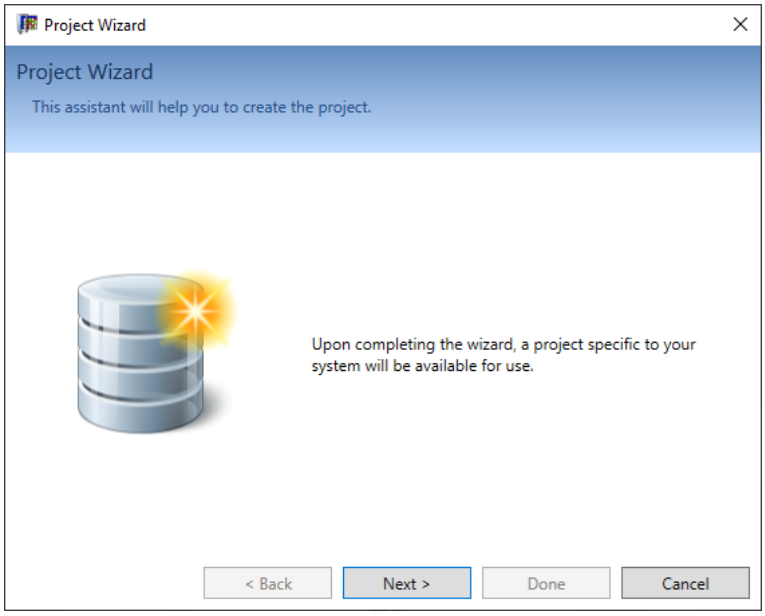


   ⇨ View when the program starts.

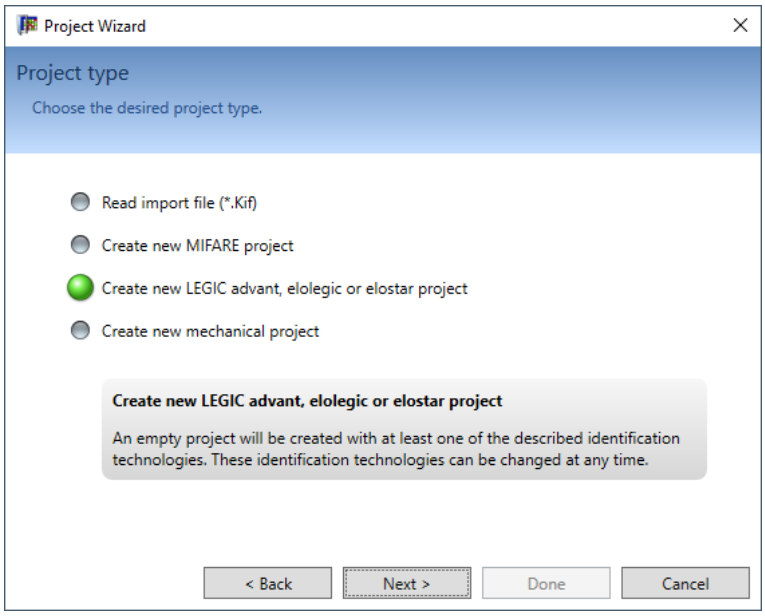


   ⇨ View in the 'File' menu

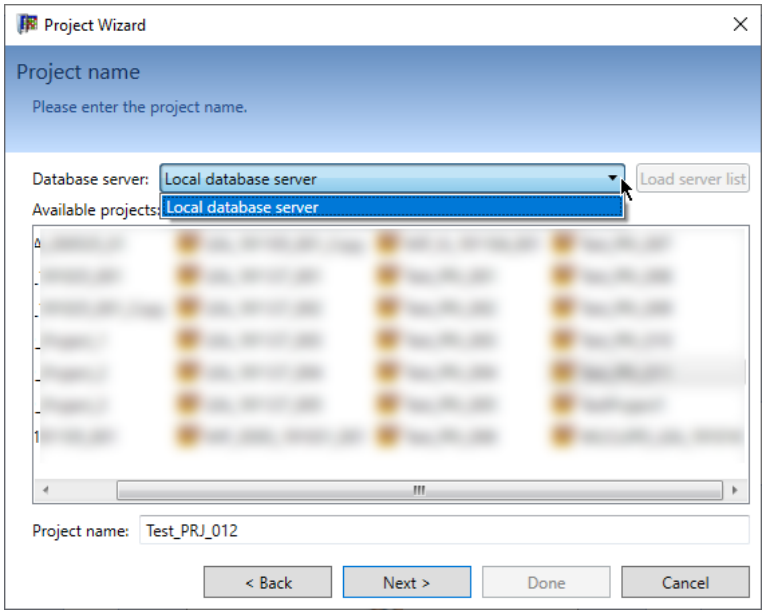
   ⇨ The wizard for creating a new project is started.



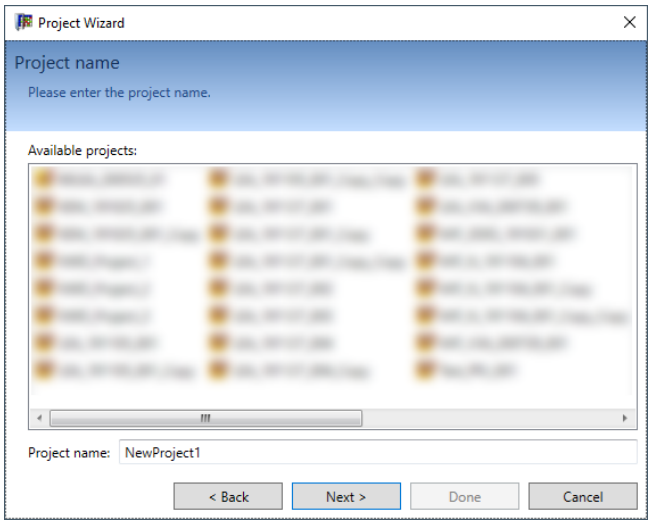
2. Click 'Next'.



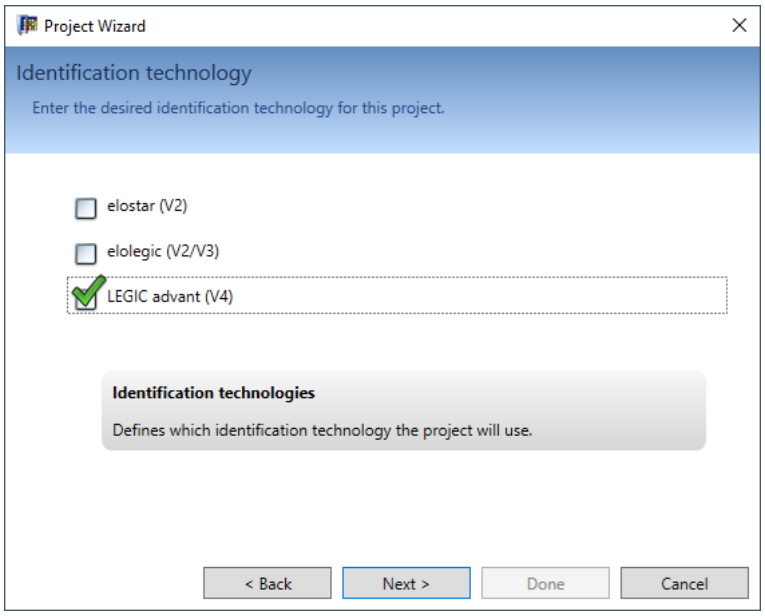
3. Select the project type (see "Project type" table).
4. Click 'Next'.



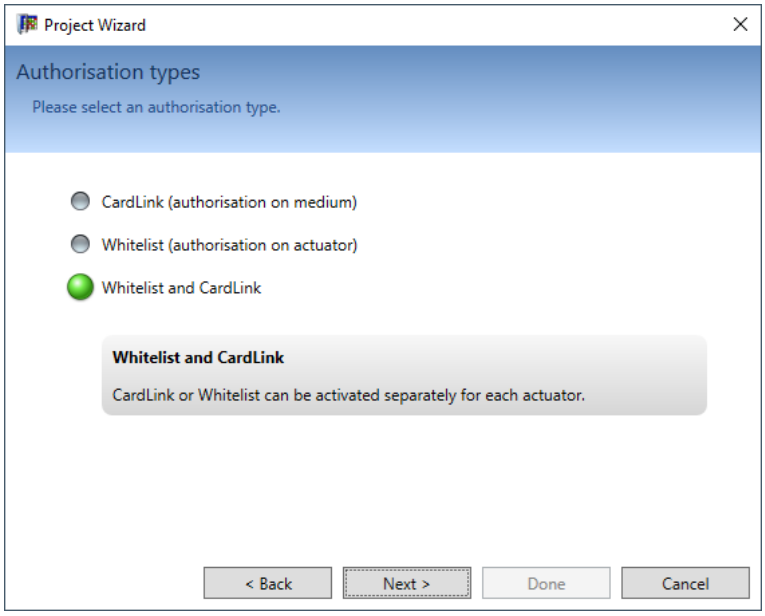
5. Select the database server from the list.
   Note: Skip this step if 'Display database server' is not selected under 'Options'. See section [▶ 5.1]. The 'Database servers' list selection is concealed in this case.
   If the server is not on the list, add it as described in the Edit database server [▶ 3.2.3] section.



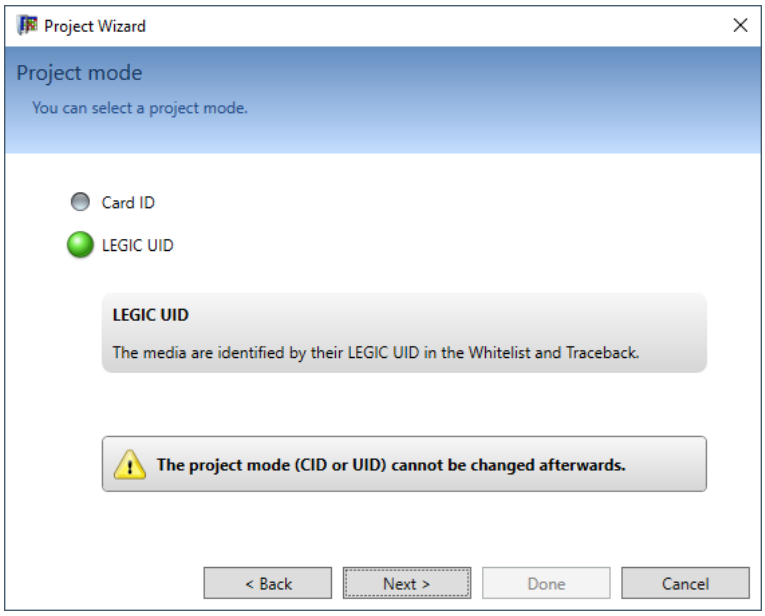
6. Enter the project name in the 'Project name' input field.
7. Click 'Next'.



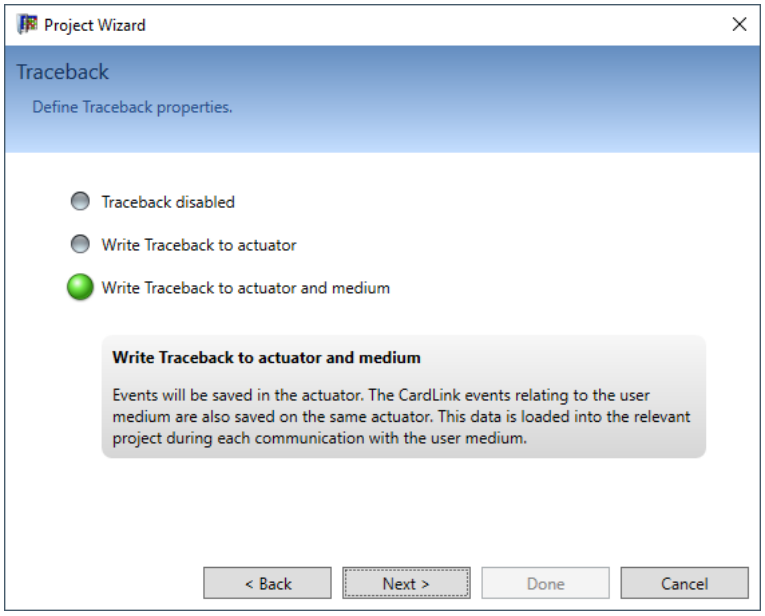
8. Select the identification technology (LEGIC; see "Identification technology" table).
9. Click 'Next'.



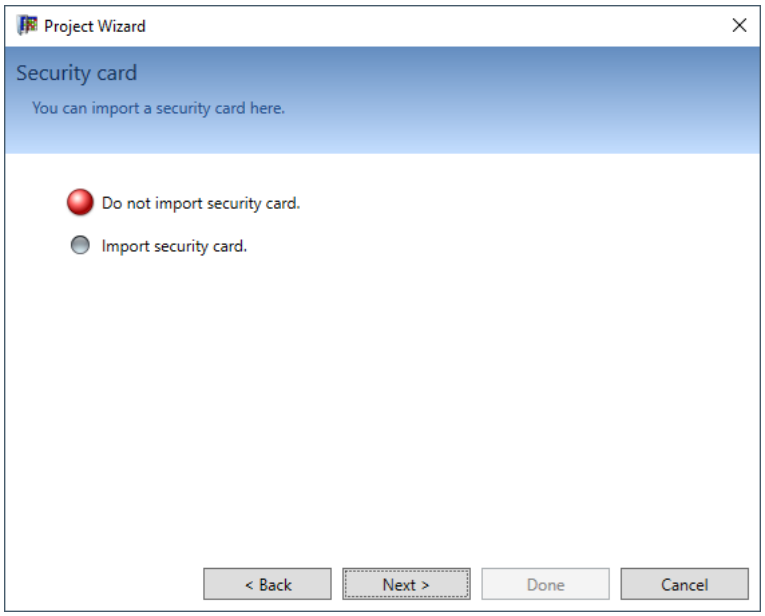
10. Select an authorization type (see "Authorization type" table). For further information on the authorization types, see sections [▸ 2.3.2] and [▸ 2.3.3].
11. Click 'Next'.



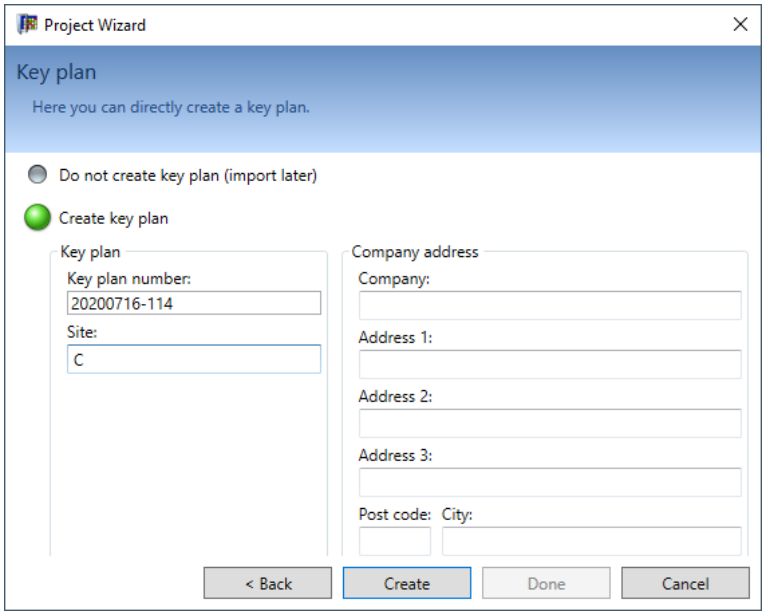
12. Select a project mode (see "Authorization mode" table below). For further information on the project mode, see section Overview of authorisation types and project mode.
13. Click 'Next'.



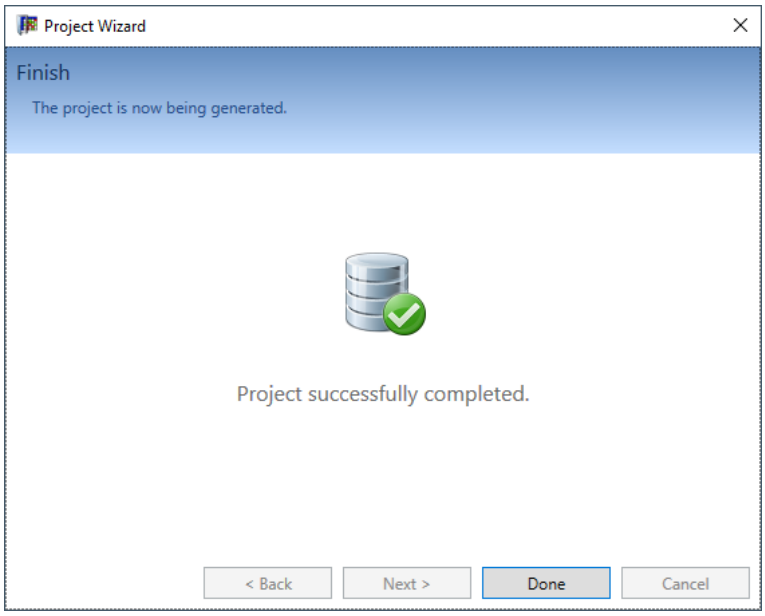
14. Select the traceback properties (see "Traceback properties" table below).
15. Click 'Next'.



16. Read in the security card (see "Security cards" table below). The security card can also be read in at a later time.
17. Click 'Next'.



18. Select 'Create key plan' and fill out the input fields.
    Select 'Do not create key plan' if the key plan is to be created or imported at a later time.
19. Click 'Create'.



20. Click 'Finish'.

⇨ The new project and the key plan have been created and can be parametrised.

Parameter tables

The tables include notes on parameter setting during project setup.

Project type table

Project type	Description
Read in import file	A KIF file (project/created file) is imported.
New MIFARE project	A MIFARE project is created. Once a technology is selected, it cannot be changed.
New LEGIC advant, elolegic or elostar project	A LEGIC project is created with one or more identification technologies. You can switch between the technologies provided at any time.
New mechanical project	A mechanical project is created. An empty project will be created only for mechanical components. This project can be expanded later to include electronic components by activating a LEGIC/elolegic/ elostar or MIFARE technology.

Identification technology table

Identification technology	Description
elostar V2	The project is created for elostar V2 components.
elolegic V2/V3	The project is created for LEGIC V2 or V3 components.
LEGIC advant V4	The project is created for LEGIC V4 components.

Authorization type table

Authorization type	Description
CardLink	The authorizations are saved on the media so that the components only need to be configured once.
Whitelist	The authorizations are saved in the components.
CardLink and whitelist	The components can be set individually for CardLink or for whitelist.

Project mode table

Project mode	Description
Card ID	The media are identified by a programmed card number. The media must be configured accordingly for this.
Safe UID (default)	The UID is additionally encrypted and checked. Special applications on the media are needed for this. Media obtained by dormakaba have these by default.
UID organizational	Only the UID is used. This mode is suitable for the "Whitelist" authorization type for organizational applications without high demands for security.

Traceback properties table

Properties	Description
Traceback switched off	No traceback is written.
Write traceback in component	The component writes the traceback entries in the memory.
Write traceback in component and on medium	For CardLink authorization, the component checks whether the medium requires a traceback entry. The component then writes the traceback entry on the medium and in its own memory.
We recommend activating 'Actuator traceback' only. Activating media traceback reduces the write and read speed. This results in high power consumption for components and a reduced service life for the battery. Media traceback is only possible for MIFARE DESFire and LEGIC advant 14443A media.	

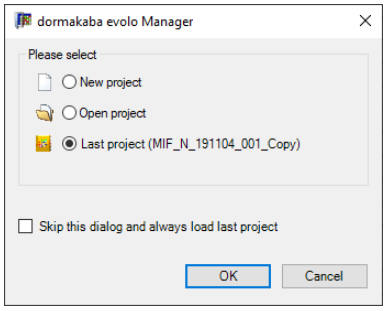
Security cards table

Project mode	MIFARE security card	LEGIC security card	Notes
Card ID	C		
CardLink	C		
Others		C1 or C2	For LEGIC security cards C1 or C2, there are 16 storage spaces available per desktop reader. For a new project with additional security cards, one storage space must be cleared in the properties of the desktop reader.


Security Card
ARIOS
dormakaba

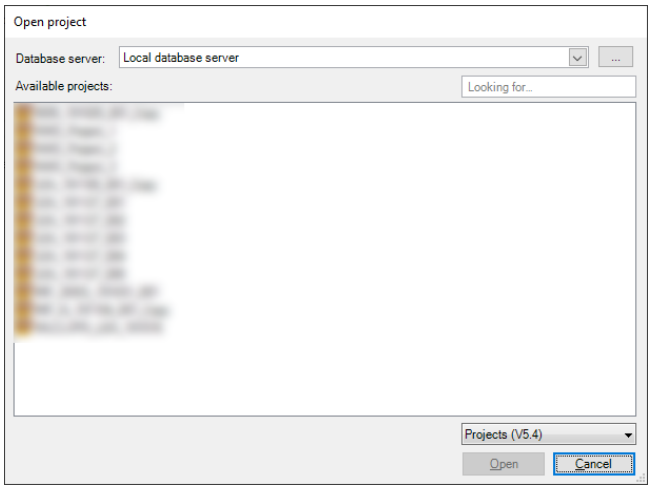
6.1.2 Opening a project

In the 'File' menu, select one of the recently used projects to open a previously created project or click 'Open'.

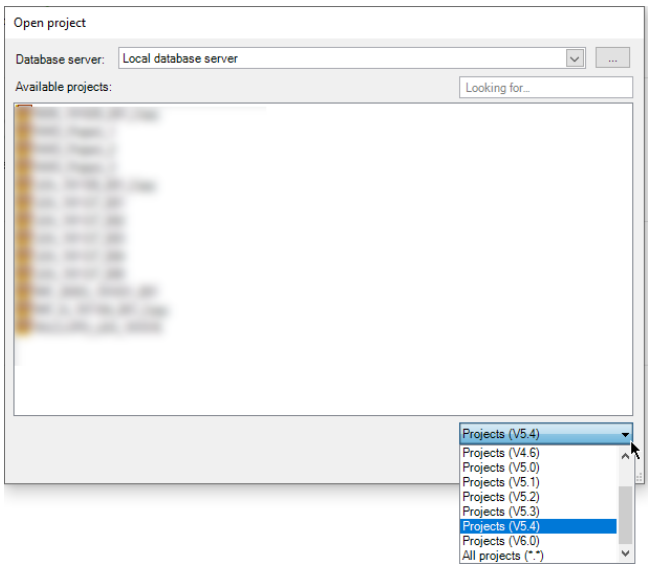


In the 'Open project' dialogue, all projects available on the selected data server are displayed.

Note: It is only possible to select the database server if this is selected in 'Options/General/ Display database server'. See section [▸ 5.1].



Limit project selection:



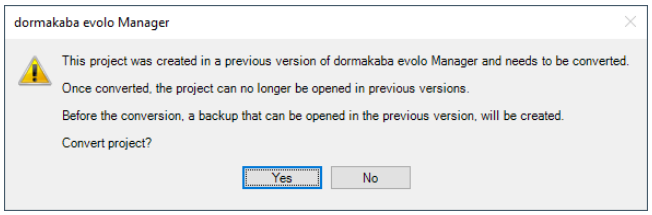
When 'All projects(*.*)' is selected, all the projects on the selected database server are displayed. Here, projects from other KEM versions are also shown. After selecting a KEM version from the list, only the projects created with the selected version are shown.

The following options:

Note: If 'Display database server' is not selected in the options, only the displayed projects can be selected and opened.

- Select a database server from the list.
  See 'Edit database server: Selecting database server' [▶ 3.2.3].
- Select an entry from the project list.
  Click 'Open'.

If a project from a previous KEM version needs to be opened, the converter starts automatically.
There are the following options:



- Select 'Yes':
  - A backup copy of the old project version is created on the database server.
  - The project is converted into a project of the current KEM version.
  - The conversion process can take some time.
- Select 'No':
  - The project will not be converted.
  - The converter closes.

6.1.3 Delete project

NOTICE

Data loss

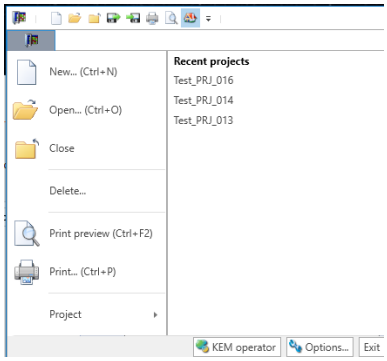
Projects will be permanently removed. It is not possible to restore a deleted project.

- Before deleting a project, create a backup of the project or export the project. See [▶ 12.1]

If user administration is active in a project, then a project can only be deleted by a user whose role includes the 'Delete project' right. For user administration, see [▶ 5.3.1].

Procedure

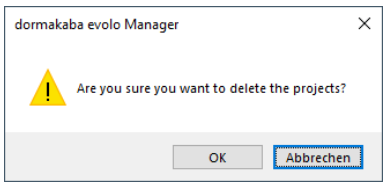
1. Click on the 'Delete' button in the 'File' menu.



   ⇨ In the 'Delete' dialogue, all projects available on the selected data server are displayed.

2. If necessary, limit the project selection to KEM versions.
   ⇨ When 'All projects(*.*)' is selected, all the projects on the selected database server are displayed. Here, projects from other KEM versions are also shown. After selecting a KEM version from the list, only the projects created with the selected version are shown.

3. Select the projects to be deleted from the list.
   Select 'Delete'.

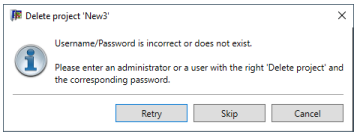
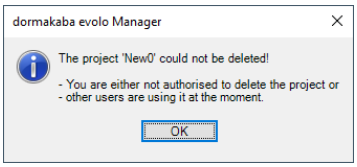


4. Confirm the deletion of the selected projects.
   Note: For projects with active user administration [▶ 5.3.1], entering the administrator with password is required for deletion.

Delete projects that were created with KEM versions prior to 6.1:

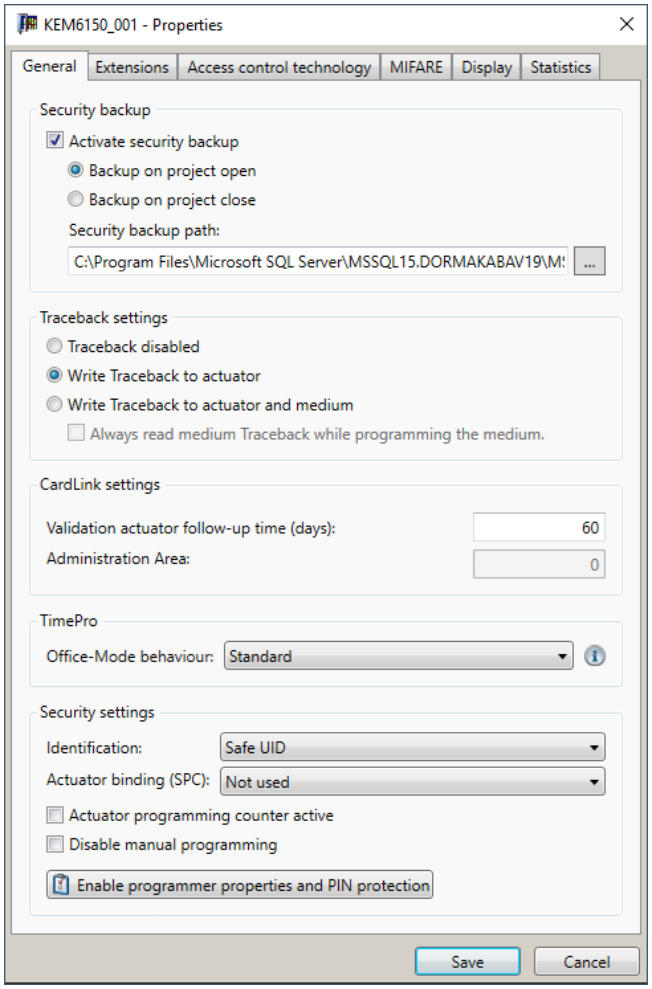
- User management is not active:
  The project can be deleted without asking.
- User management is active:
  To delete a project, an administrator's user name and password are required.

Errors/problems that occur

Message	Reason	Solution
 User name not known or incorrect password Incorrect or unknown user name/password.	The user name and/or password do not match the data stored for the project to be deleted.	• Try again with another user • Quit
User name and password correct, but no right to delete project: Please use a user with the 'Delete project' right.	The specified user does not have the required right.	• Select another user with the required right (e.g. administrator) • Quit
	• A project opened by another user cannot be deleted. • Your own project cannot be deleted.	Close the project and try again to delete the project.

6.2 Project properties

6.2.1 General



The project properties can be displayed using the F4 command button.

Security backup		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
Activate security backup	A security backup is automatically created in the directory indicated in the security backup path.	✓	✓	✓	✓
Save upon opening project	The security backup is created when opening the project.	✓	✓	✓	✓
Save upon closing project	The security backup is created when closing the project.	✓	✓	✓	✓
Traceback settings					
Traceback switched off	No traceback is made.	✓	✓	✓	✓
Write traceback in actuator	Write traceback in the component's memory.	✓	✓	✓	✓
Write traceback in actuator and on medium	Write traceback in the component's memory and on the medium. Media traceback with MIFARE is only possible for DESFire media.	✓	✓	✗	✗

Always read medium traceback when programming the medium	Prior to any programming of a CardLink authorisation, first the traceback data are read on the medium.	✓	✓	✗	✗
CardLink properties					
Follow-up time in days	Time period for how long a medium can still be validated after the validation time period has expired.	✓	✓	✗	✗
Administration area	The default value is 0.	✓	✓	✗	✗
TimePro	Office mode behaviour				
Standard	Immediate activation/deactivation	✓	✓	✓	✗
Delayed	Present medium for activation/deactivation for 2 seconds. MRD components only.	✓	✓	✗	✗
Security settings					
Identification	UID or UID organisational.	✓	✓	✗	✗
Actuator binding (SPC)	• Not used • For actuator export • For actuator export and clock adjustment	✓	✓	✗	✗
Actuator programming counter active	Numbering of actuator configuration. This ensures that no outdated configuration can be loaded.	✓	✓	✗	✗
Disable manual programming		✓	✓	✓	✗
Display programmer properties and PIN protection	The programmer properties are displayed and can be modified. PIN protection can be activated.	✓	✓	✗	✗
Extensions					
Use terminal	Activates the terminal for authorisation transfer.	✓	✓	✓	✗
Use wireless	Activates the wireless option for authorisation transfer.	✓	✓	✗	✗
Logging authorisation	Logging all activities for tracking authorisation-relevant modifications in a CardLink system.	✓	✓	✗	✗

Note: elolegic only supports U-Line.

6.2.1.1 CardLink properties

Follow-up time in days
Until the follow-up time expires, a medium can still be validated by a validation actuator. This again classifies the medium as trusted.

The follow-up time can be set between 0 and 255 days. The preset value is 60.

Administration area
Possible administration areas: 256

The preset value is 0.

Contact Support if you have any questions regarding the administration area. The setting of the administration area can be changed by Support only.

6.2.1.2 Security settings

A separate 6-digit PIN can be set in the programmer.
This PIN cannot be changed by KEM.
This PIN can be directly changed/deleted only in the programmer.
The programmer must be unblocked separately before data can be exchanged with KEM.
Information on this can be found in the programmer manual.

The SPC (System Protection Code) is an additional protection for a master key system. Only components of the master key system associated with each other can exchange data and authorizations after activation of the code.

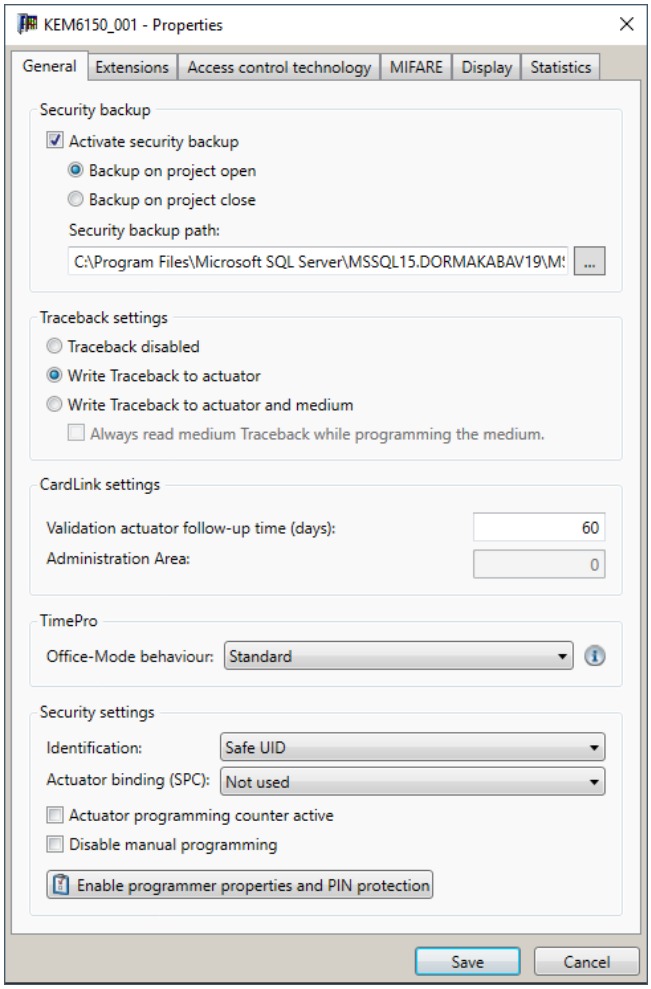
Settings
The settings for the system protection code can be made in the project properties. For explanations, see section [▶ 6.2.1].

It is recommended that you activate PIN protection together with the SPC.
Note the following properties when doing so:

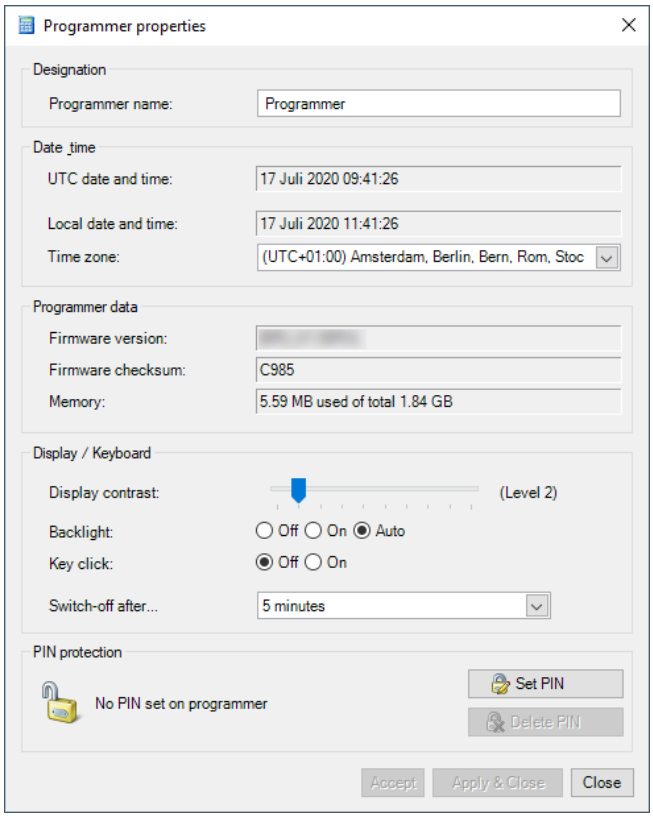
- The actuator binding (SPC) and PIN protection are only supported with programmer 1460.
- As long as an export to programmer 1460 and to the components has not been carried out, an existing SPC is valid.
- Deactivating the SPC requires an INI reset of all components.
  These must then be re-programmed.
- The SPC settings of the components can no longer be modified.

Procedure for activating PIN protection

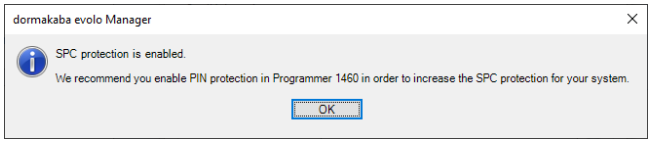
1. Open project properties (F4).



2. Click on the 'Enable programmer properties and PIN protection' button.
3. Select 'Set PIN'.



4. Enter a 4-digit numeric PIN.
5. Click on the 'OK' button.



If a PIN has been activated and the programmer is connected, you have the following options:

- Enter the PIN into the programmer.
- Reset the PIN.
  Note: All data on the programmer are deleted. The programmer must be re-synchronised with the software.

Delete PIN
You can delete a PIN using the 'Delete PIN' button in the 'Programmer properties' window.

Import protected data from the programmer
The data of a master key system protected by SPC can only be imported from the programmer if the programmer's SPC and the software's SPC correspond.

6.2.2 Extensions

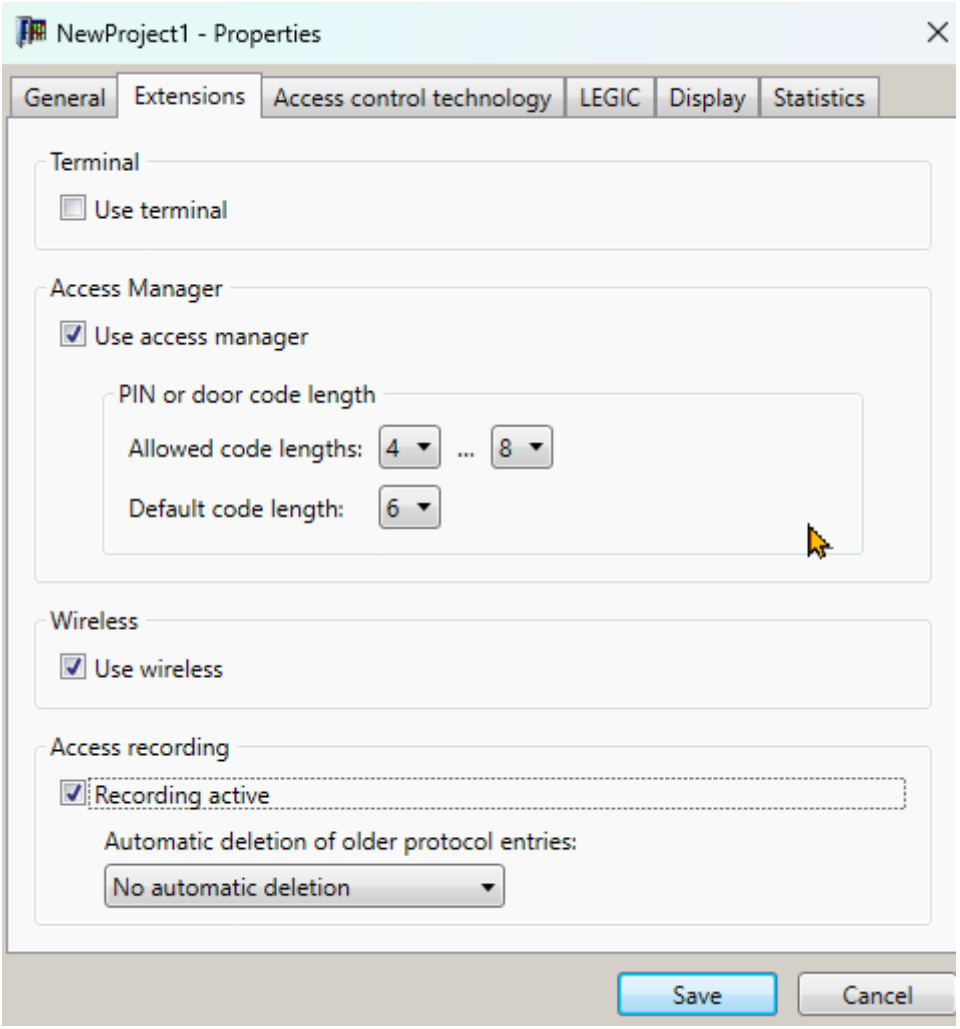
6.2.2.1 Logging authorisation

Activating the protocol list can generate large amounts of data.

The section is only available for viewing and editing under the following conditions:

- 'CardLink' or 'Whitelist and CardLink' is selected as project type.
- User management is active.

In a CardLink environment, all actions that change authorisations are logged.



Activating logging authorisation

Requirement

- The user is registered as an administrator.

Procedure

1. Activate the checkbox.
2. From the list, select the time period after which older entries should be automatically deleted.
   The older entries are deleted when the project is opened.
3. Click 'Save'.

Access the protocol list by using the 'Navigator/Logbook' menu. See Logbook [▶ 6.13] section.

Deactivating logging authorisation

Deactivating logging will delete all log data when the query is approved.

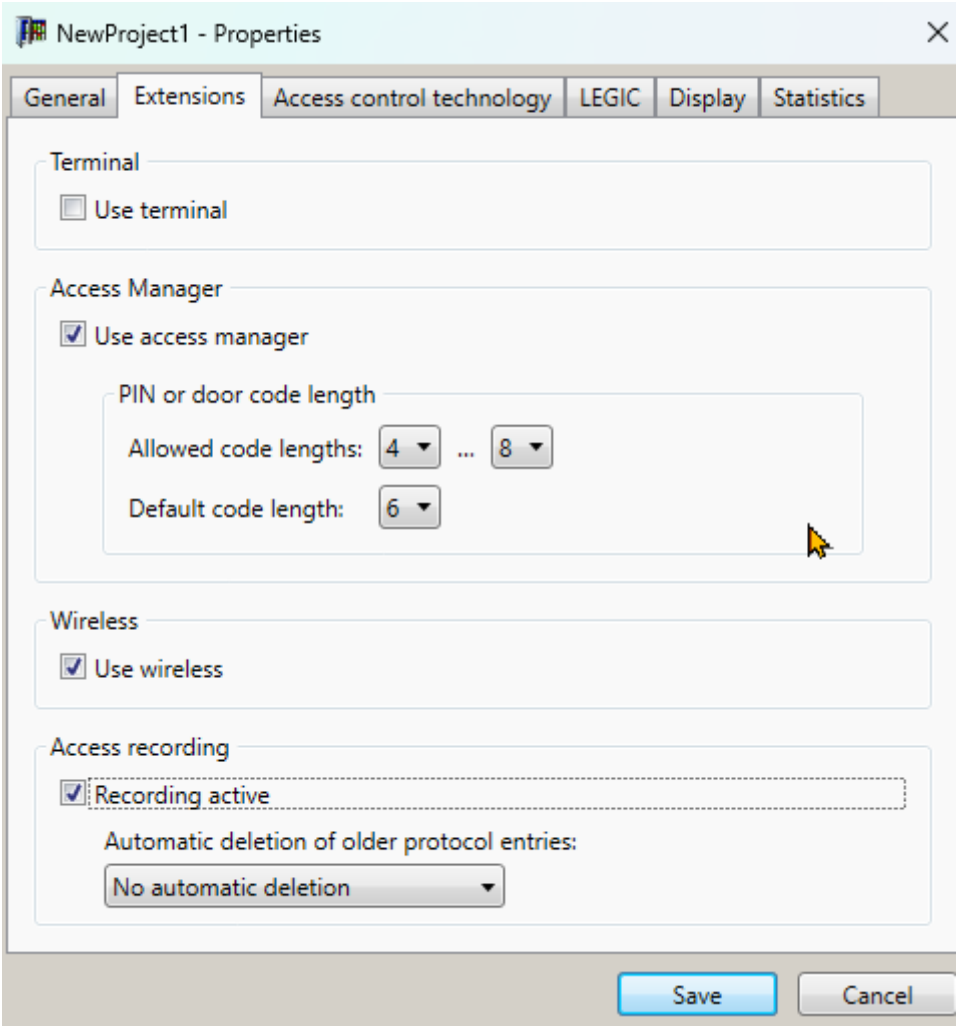
- If the log is to be retained, then the protocol list must be exported before the function is deactivated. See section [▶ 6.13.2].

Requirement

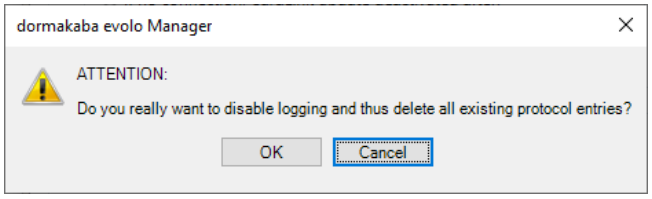
- The user is registered as an administrator.

Procedure

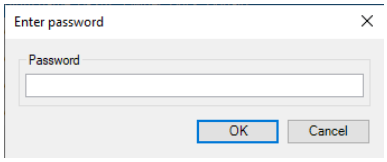
1. Deactivate the checkbox.



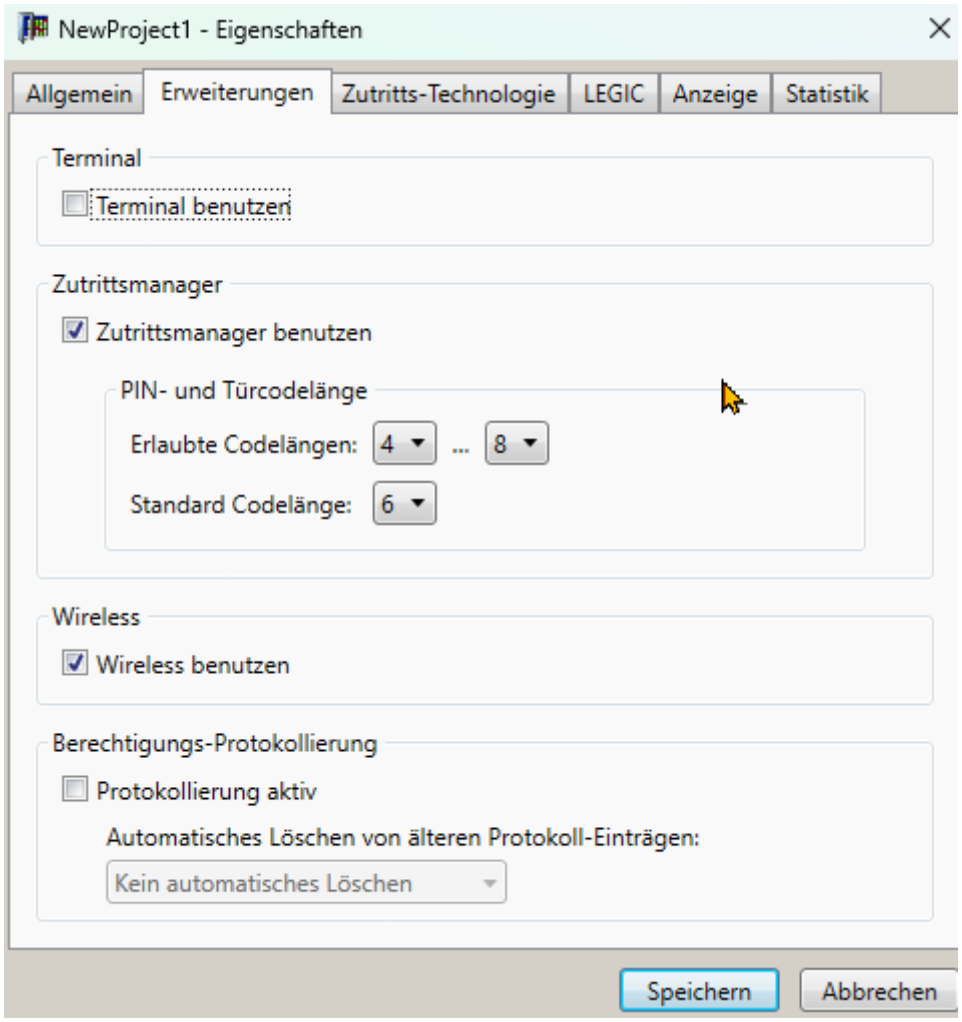
2. Click 'OK'.



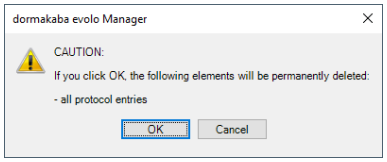
3. Enter the password and click 'OK'.



4. Click 'Save'.

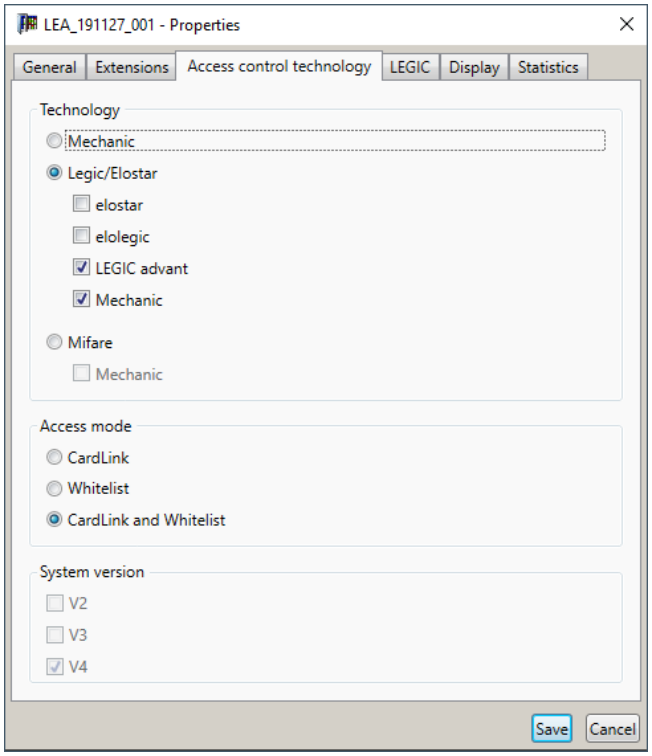


5. Click 'OK'.



⇨ The log entries are deleted.

6.2.3 Access technology



Select the access technology and access mode. Possible combinations:

Access authorisations		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
CardLink	Activate CardLink	✓	✓	✓	✗
Whitelist	Activate Whitelist	✓	✓	✓	✓
CardLink and Whitelist	Activate CardLink and Whitelist	✓	✓	✓	✗
System version					
V4	Time profile version	✓	✓	✗	✗
V3	Time profile version	✓	✓	✓	✗
V2	Time profile version	✗	✗	✓	✓

LEGIC advant

If LEGIC is selected as access technology, the active technologies can be determined automatically or manually. The settings apply to the entire project.

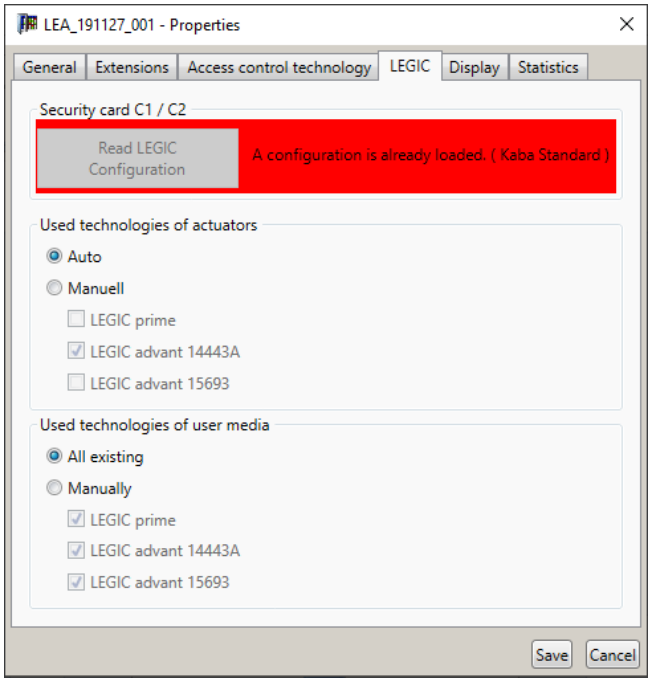
Different memory areas are assigned to the different access technologies on the media.

LEGIC CTC media support all technologies.

Active LEGIC advant technologies:

- Auto:
  The active technology is automatically detected and set.
- Manual:
  Select one or more of the technologies displayed.
  Note: Media of technologies that are not selected can no longer be read or written on.

- LEGIC prime
- LEGIC advant 14443A
- LEGIC advant 15693



Technologies of the user media in use:

Only data records of active technologies can be read or written.

- All existing:
  The active technology determines which technology is read or written on the user medium.
- Manual:
  Select one or more of the technologies displayed.
  Note: Media of technologies that are not selected can no longer be read or written on.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

Access mode

Whitelist	The component opens/closes with whitelist authorisations.
CardLink	The component opens/closes with CardLink authorisations.
CardLink with validation	The component opens/closes with CardLink authorisations. Media that are presented and authorised at the component are validated.
CardLink with update	The component opens/closes with CardLink authorisations. Media that are presented and authorised at the component are validated. The CardLink authorisations of the presented media are always updated.
Mixed	The component opens/closes with CardLink or whitelist authorisations.
Mixed with validation	The component opens/closes with CardLink or whitelist authorisations. Media that are presented and authorised at the component are validated.
Mixed with update	The component opens/closes with CardLink or whitelist authorisations. The CardLink authorisations of the presented media are always updated.
Update	The authorisations and validation of the presented media are updated. Media included in the blacklist will be invalidated. CardLink access is no longer possible from this moment on.

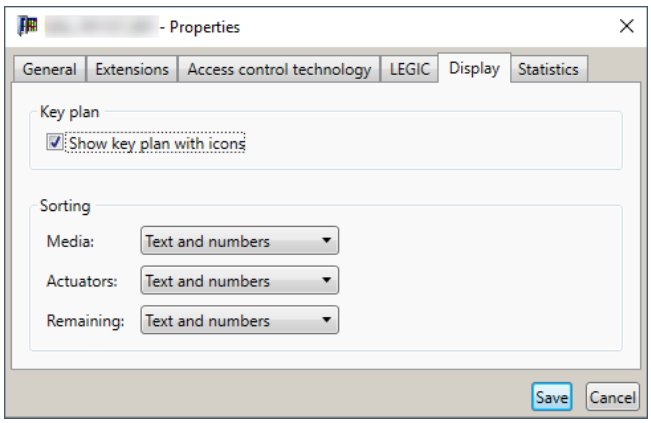
A validation is not carried out:

- the medium is on the blacklist.
- the medium is outside of the follow-up time.

An update is not carried out:

- the medium is on the blacklist.

6.2.4 Display



Key plan
To display the icons of media and components, activate the 'Display locking plan with icons' checkbox.

Sorting
The following settings determine the sorting behaviour in the text fields that are selected for sorting. Customisations are applicable for the tabs in the 'Basics' menu, e.g. media, actuators.

Settings:

- Text: Alphabetical sorting
  Example: 1.OG, 10.OG, 11. OG, 2.OG, 20.OG
- Text and numbers: Alphanumeric sorting
  Example: 1.OG, 2.OG, 10.OG, 11. OG, 20.OG

6.3 Media

Security cards are used for individualisation and unification of the system.

Master media are used for programming a system. Master media and system are assigned to a security card.

User media are needed for authorization of the users at the components.

New media types with triple CTC (LEGIC), AES and 3DES encryption (MIFARE) can be used in KEM only if the following requirements for the hardware and software are met:

- KEM version 5.4 or higher
- MRD desktop reader
- Firmware version of the component 42.xx or higher

In addition, users can also use a PIN code assigned to them. This is possible using the dormakaba 90 02 registration unit and the dormakaba 91 12 compact reader.

The following requirements apply to the use of MIFARE or LEGIC EV3 media:

- dormakaba evolo Manager (KEM) from version 6.2
- MRD desktop reader 91 08
- Firmware of components from version 42.xx

6.3.1 Security cards

The security cards are used in a LEGIC or MIFARE environment. Depending on the technology used, the functions of the security cards differ.

6.3.1.1 Description

For LEGIC advant, there are 2 security cards:

- Security card C1 for system-specific segmentation of media.
- Security card C2 for initialising the system with desktop readers and validation components in CardLink.

For MIFARE, there is security card C:

- Security card C is needed to integrate the system-specific key of a MIFARE environment into the master key system. It defines the system key as well as the memory organisation of the user media.

Increasing the security of a system with AES or 3DES encryption

An encryption increases the security of a system. The AES encryption offers a higher level of security than the 3DES encryption.

AES or 3DES encryption is possible with a MIFARE security card and MIFARE DESFire user media.

Take AES or 3DES into account when ordering the security card for a new system.

Retrofitting of an existing system to AES or 3DES using a new security card is not recommended.

6.3.1.2 LEGIC/MIFARE security functions

Security card C1/C2 (LEGIC) (Can only be loaded with project mode Card ID or CardLink.)		**MIFARE**	**LEGIC advant**	**elolegic**	**elostar**
Configure LEGIC media	Security card C1 for segmenting, reading and writing on the media. Security card C2 for permanently reading and writing on the media.	✗	✓	✓	✗
Security card C (MIFARE) (Can only be loaded with project mode Card ID or CardLink.)					
Read site key into project	Security card C is read into the project and the project is customised. A security card C does not need to be presented for the same desktop reader after a system restart.	✓	✗	✗	✗
Authorization status (colour statuses)					
Red	Desktop reader is not authorized.				
Orange	Read and write functionality for media is enabled (LEGIC).				
Green	Segmenting of media is possible.				

Legend

✓ = property available

✗ = property not available

6.3.2 Master media

6.3.2.1 Creating a programming master

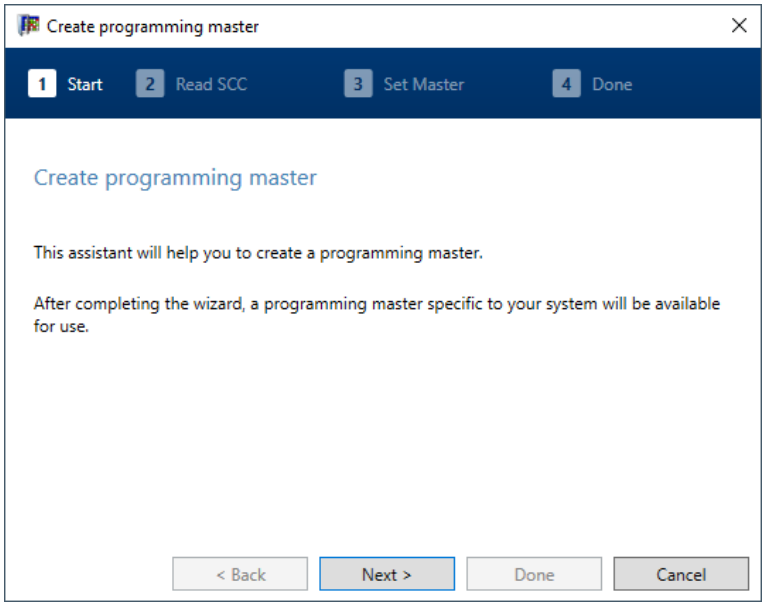
The access authorisations for user media can be transferred to the components with the current programming media (master A, master B and master T) using various programming types.

- Programming masters can only be initialised within the MIFARE technology.
- Programming masters for the LEGIC technology can be found in the basics.

Authorisations	**Master**		
	A	**A/B**	**B**
Whitelist without tool chain	--	Recommended	Possible
Whitelist with tool chain	--	Possible	Recommended
CardLink	Possible	--	Recommended
Combination of **CardLink** and **Whitelist**	Possible	Possible	Recommended

Procedure

1. Open the 'Wizards' menu from the Navigator toolbar.
2. Launch the 'Create master' wizard.



3. Follow the instructions in the wizard.
4. In step 2, place security card C on the desktop reader.

5. In step 3, place the new programming master A on the desktop reader and fill in the 'Designation' field in the wizard.
6. In step 4, click on the 'Finish' button.

6.3.2.2 Master T

The temporary master (Master T) is a special form of the programming media for standalone components. Temporary master media can be used in a master key system. These are only valid for a user-defined period of time and have limited functions. A Master T can only be used if the components of the site have been configured with the programmer after reading in the safety card.

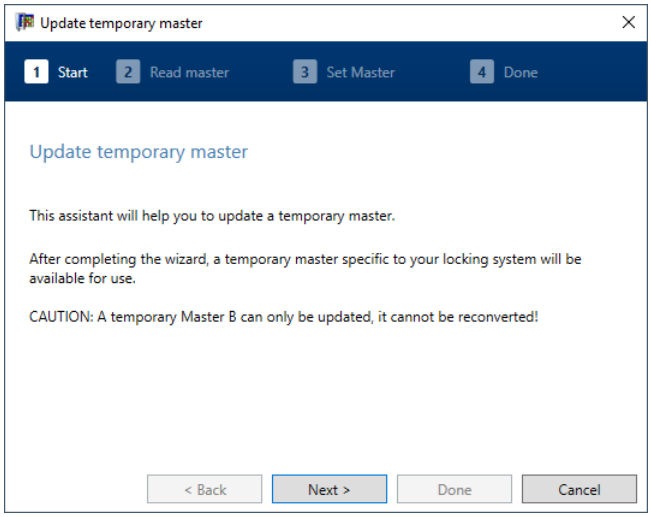
Update Master T

The security card must be already read in.

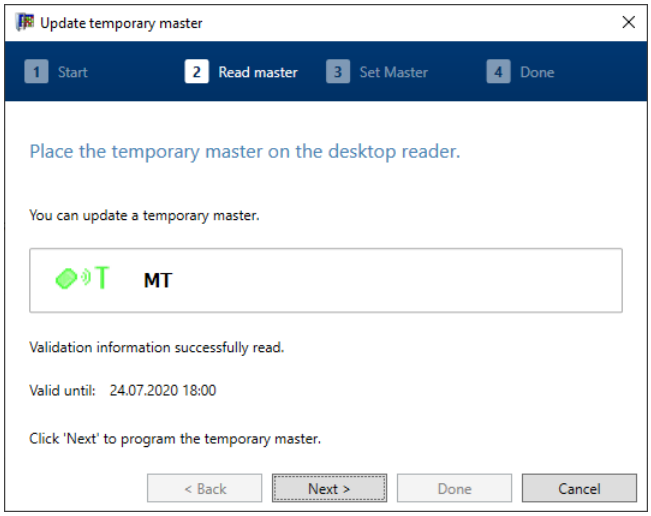
Update a temporary master medium with the help of the wizard.

A Master T can also be read in under "Basics".

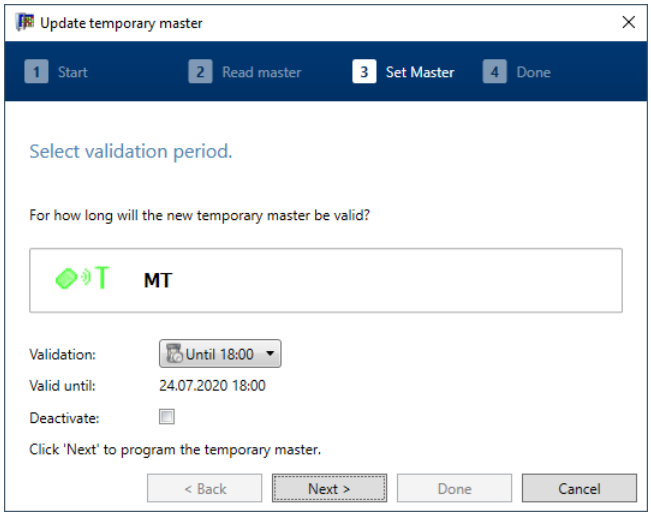
1. In the 'View' toolbar, open the 'Wizards' area.
2. Start the 'Update temporary master' wizard.



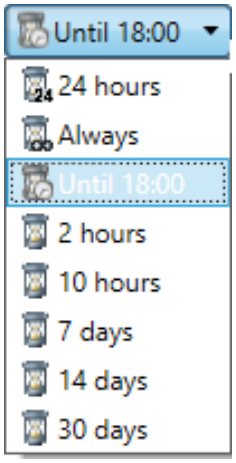
3. Place a Master T medium on the desktop reader.



4. Click on the **Next** button.

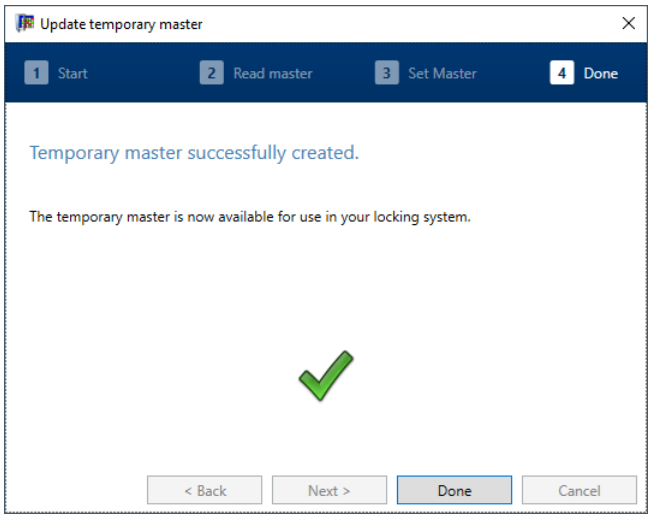


5. Choose validation period.



⇨ After the selection, the time of expiry of the validation is displayed.

6. Click on the **Next** button.



⇨ The medium is now valid as master until the expiry time.

7. Finish the wizard by clicking on the **Finish** button.

6.3.2.3 Using a Master T

Master T for LEGIC:
Master T media can be defined for LEGIC using the software. A Master T is extrapolated from the security card and can only be used as a temporary master medium.

Master T for MIFARE:
Master T media can be defined for MIFARE using the software. A master T can be extrapolated from security card C.

The master T media for LEGIC and MIFARE have the following properties:

- Application in both authorisation types: CardLink and whitelist.
- Updating the components (the components must be configured).
- The clock of the components can be adjusted.
- Read out the traceback.

MIFARE systems in whitelist operation
Notes on the subsequent use of a Master T.

In MIFARE systems, before using a Master T for the first time, the system's site key must be transferred to the components. In existing systems without a site key, a site key must be derived from security card C and transferred to the components.

Procedure for the subsequent transfer of the site key to the components of a system:

Requirements

- The system is registered in KEM.

- The system's Master B is present.
- Security card C is present.

Procedure

1. Read the system security card C into KEM.
2. Write the master B of the system with the site key ('Create master' wizard).
3. Locate the components with the master and transfer the site key.
4. Update the configuration of the component.
   ⇨ The site key is transferred.
   ⇨ The Master T can be used.

6.3.3 Programming user media

- Set up media for CardLink See [▸ 6.9.2]
- Set up media for whitelist See [▸ 6.9.1]
- Prepare media in whitelist for CardLink See [▸ 6.9.2]

If the authorisation type is whitelist or CardLink and the project mode is card ID, the card ID must be assigned manually for new media. This cannot be changed retrospectively. If the card ID is already assigned to a medium, this is displayed in the dialogue.

6.3.4 Update MIFARE DESFire key settings

Description
A blank medium is first configured according to the ARIOS concept and then the device software and files are programmed. After programming, no further device software can be added or deleted without the media maintenance key, even if there is still storage space available. This wizard opens the medium so that additional device software and data can be programmed without using the media maintenance key.

New MIFARE DESFire media
New, blank MIFARE DESFire media are configured with ARIOS settings during authentication with an ARIOS site key. The key settings are then adjusted so that additional device software can be programmed (from KEM V 7.0).

Pre-programmed MIFARE DESFire media
The key settings of existing media can be adjusted by adding further device software with an empty file and using this to open the medium for further device software. This additional device software is never used and is then deleted again. This results in some storage space being lost on the medium. In KEM, this process is carried out using a wizard.

The settings can only be adjusted on MIFARE DESFire user media.

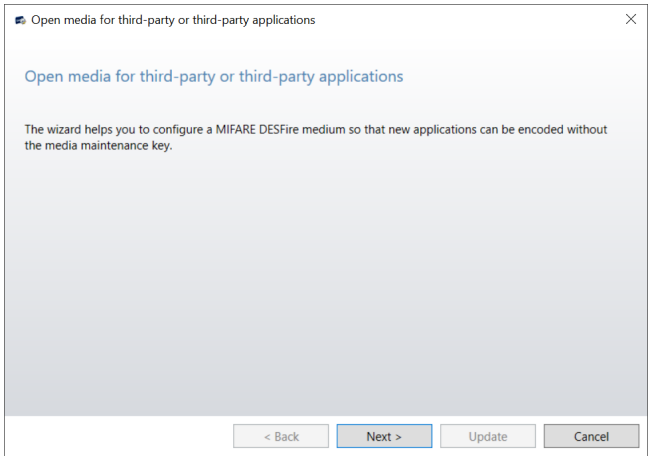
- The media must be recorded in the project.
- Other media will be rejected and will not be processed by this wizard.
- Media that has already been configured loses some storage space as a result of the process.

Requirements

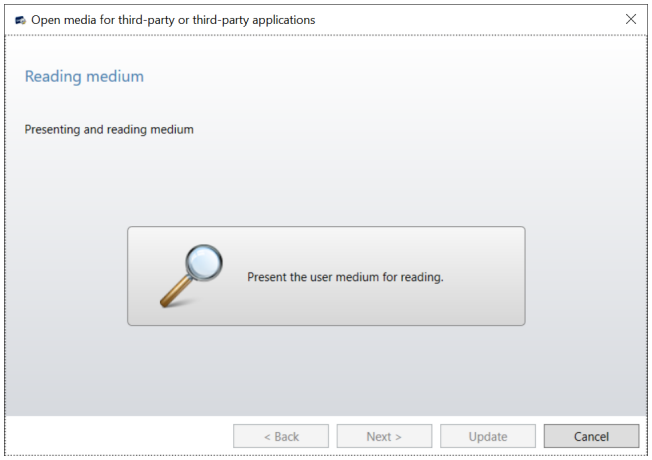
- KEM from V7
- An MRD desktop reader is connected to the system.
- MIFARE project
- The project's security card has been scanned.
  The wizard is not visible and cannot be started before the security card is scanned.
- The user medium is recorded in the project.

Procedure

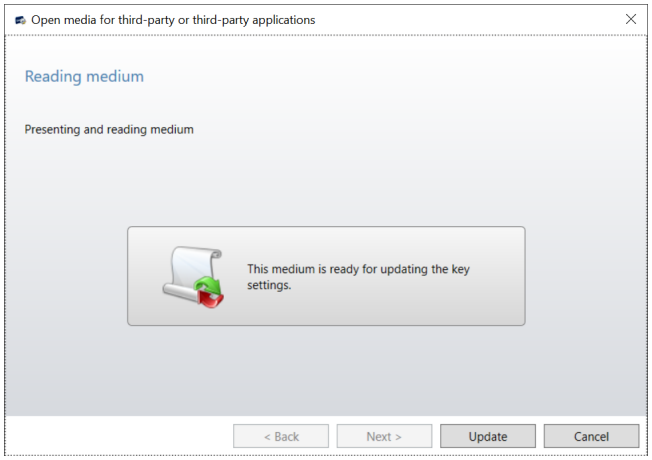
1. Navigate to 'Navigator/Wizards'.
2. Start the 'Update MIFARE DESFire key settings' wizard.



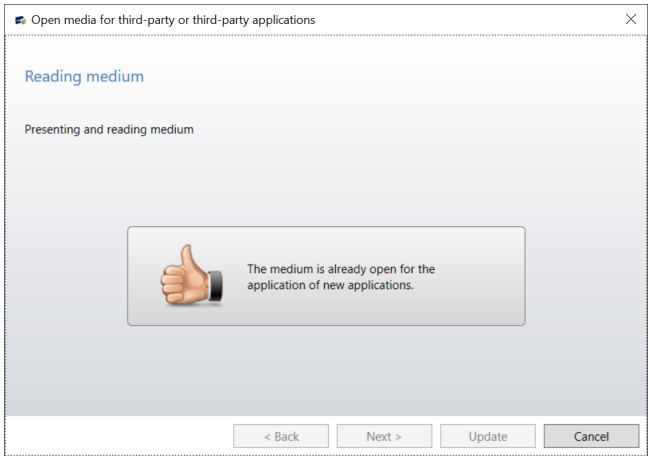
3. Click 'Next'.



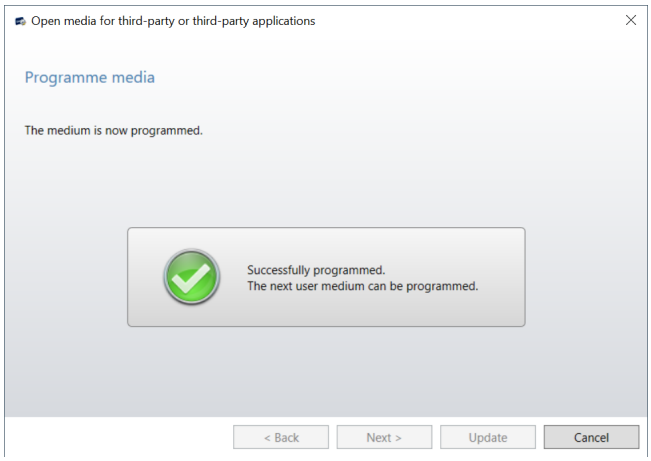
4. Place a user medium from the project on the desktop reader.



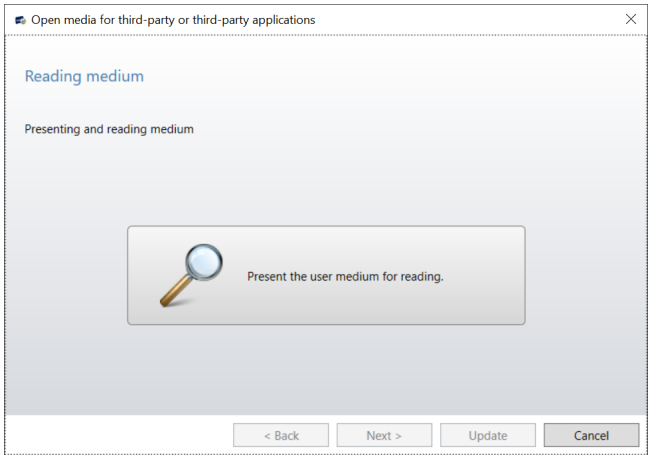
⇨ If the medium is already open, the wizard will indicate this. In this case, remove the medium and insert another user medium.



5. Click on 'Update'.
   ⇨ The settings will be adjusted.



6. Remove the processed medium from the desktop reader.
   ⇨ Edit additional media by repeating steps 3 to 5.



7. Click 'Cancel' to exit the wizard.

6.4 Time profiles

Time profiles determine at which times a medium is authorised on a component.

In addition to the basic access authorisations, time profiles restrict the times of authorisations. The time profiles are configured in the KEM software and then transferred to the component with the programmer or wirelessly.

The time profiles can be assigned to users and components.

Requirement

The date and time are correctly set for all the elements involved in the time profiles option.

Description

Whitelist authorisation	• With individual time profile. Each component has 15 freely-definable time profiles each with 12 time windows (V3/V4) or 4 time windows (V2). 7 time windows are permitted for remote time profiles.
	• With a time profile having TimePro functions. Office time profile or Day/Night time profile.
CardLink authorisation	• With time profile (door group right, individual right, reservation). 15 different editable time profiles and 1 fixed time profile can be used system-wide.
	• With validation

1,000 time profiles can be created. The first 16 time profiles are reserved for CardLink and the whitelist. All subsequent time profiles are exclusively for the whitelist. 159 remote time profiles can be created.

The time profile provides the following options in the time profile details:

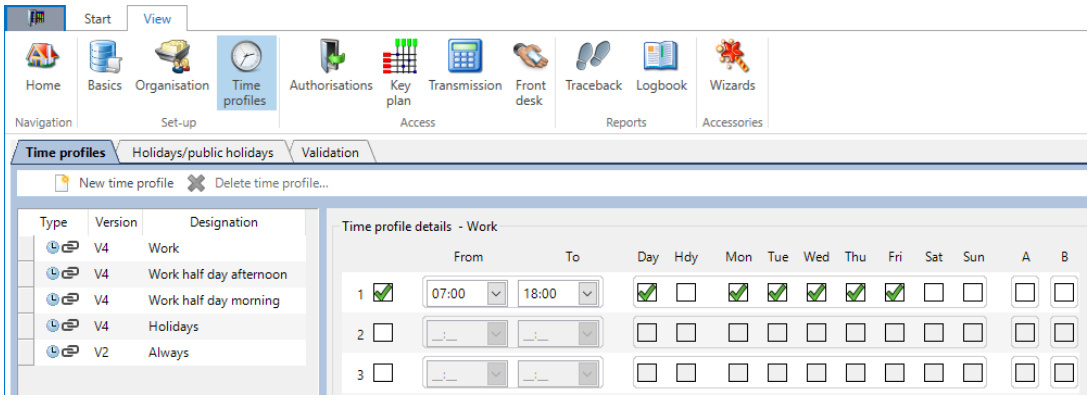
- Period 'from'–'to' in combination with the following 2 options:
- 'Day' and the selection of one or more weekdays
- Holidays, special days. The settings for holidays and special days can be made on the "Holidays/special days" tab.

Remote time profiles must not contain any overlapping time windows.

The time profile "Always" is fixed and cannot be parameterised or deleted.

Procedure for parameter setting

1. In the 'View' toolbar, open the 'Time profiles' menu.
2. Go to the 'Time profiles' tab.
3. Click on the "New time profile" button and register a new profile.
4. Enter the name for the time profile into the "Designation" field.
5. Click on the option boxes in the row to activate the desired time profile details.



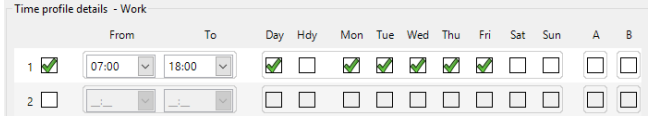
Example:

1 Only on weekdays (Mon to Fri)

2 Only on holidays

3 On weekdays and on holidays (Mon to Sun)

4 On special days A, see [▶ 6.4.1]



6.4.1 Holidays/special days

Differences for holidays/special days between time profile V2, time profile V3 and time profile V4:

Time profile V4	Special days A and B
Time profile V3	Special days A
Time profile V2	• Special day A • No restriction for 'Day' with regard to holidays
Remote time profile	Can only be used for remotely managed actuators. • A maximum of 7 time windows can be defined, which must not overlap. • A maximum of the next 32 holiday or special days in the future are downloaded to the access manager.

An active block of holidays overlaps with selected TimePro functions.

During an update with the programmer, the holidays and special days in the future as seen from the time of the update are always applied by the software.

Time profiles for holidays

Special days within a holiday block overlaps with the holiday block. The time profile of the special days then has priority over the time profile of the holiday block.

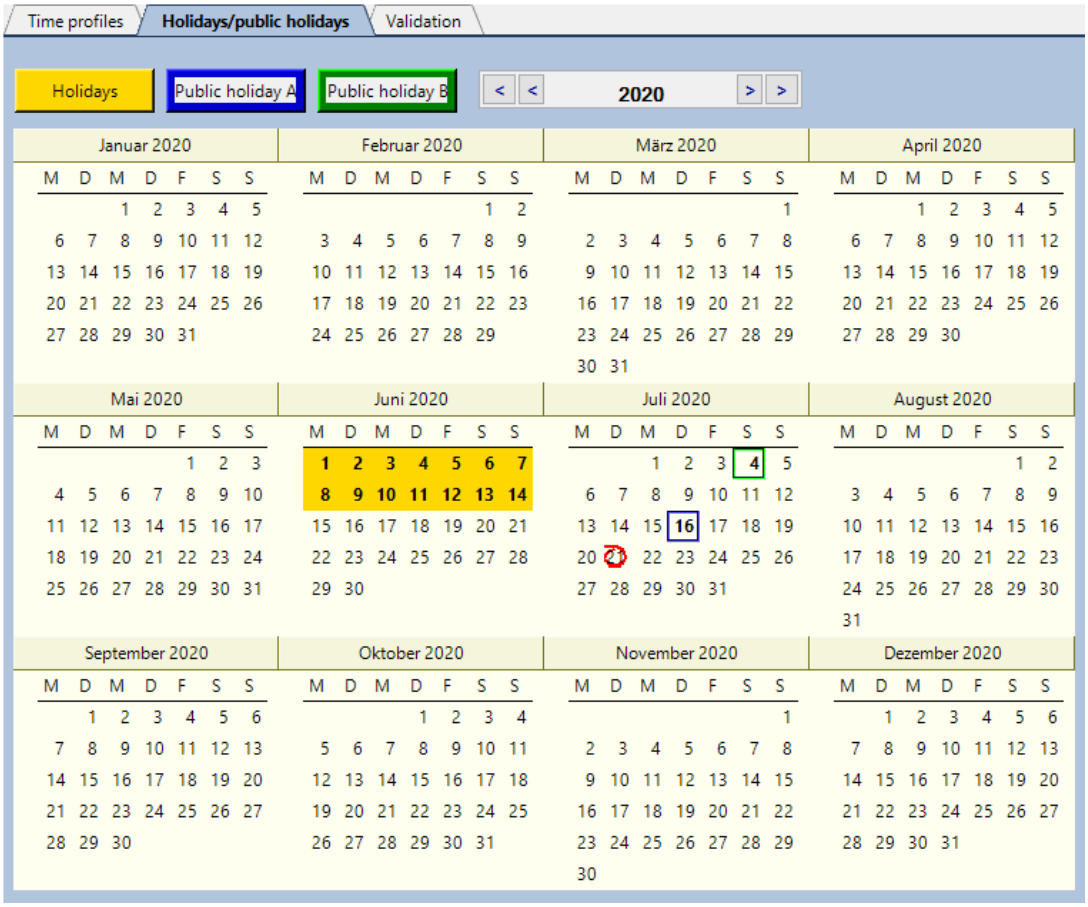
Access authorisation can be issued or revoked for periods of sequential days (e.g. holidays). The length of a period can be established by entering the start and end date. 20 holiday blocks can be defined in components with V4, and in components with V3/V2 10 holiday blocks can be defined. In the V2 time profile, the holidays can be permanently defined by selecting the holiday blocks. It is not possible to set a restriction using the optional field 'Day'.

Time window for special days

An individual time window for selected special days.
In V3 and V4, 2 different days, special day A and special day B can be created for special days (e.g. holidays). This way, 2 time windows are created, e.g. a time window for one day before a holiday (special day A) and the holiday (special day B). For each of the 2 special day types, a total of 32 special days can be stored.

Create holidays

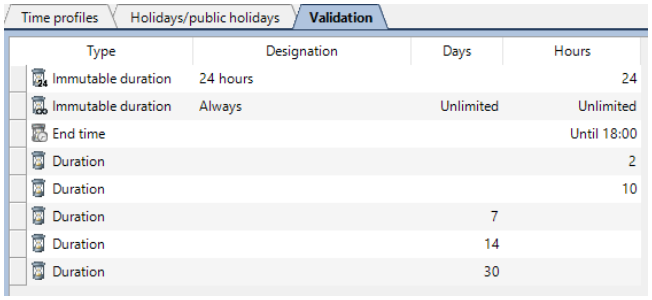
Create holidays	Mark the desired area with the left mouse button and click the button 'Holiday block'.
Create holiday (special day A and/or B)	Mark the holiday with the left mouse button and click the button 'Special day A' or 'Special day B'.
Show holiday block	Hover with the mouse over the entered holiday block or the special day and wait for the tooltip. The data of the holiday block will be shown in the tooltip.
Show context menu	- Hover with the mouse over the entered holiday block or the special day. - Open the context menu with the right mouse button. - Select 'Rename holiday block' to rename it. The holiday block or special day can be renamed in the input window e.g. to 'Summer holidays'. The entered text is shown in the tooltip, in the properties and in the print form. - Select 'Delete holiday block' to delete it.



6.4.2 Validation

Validation is only available in the CardLink authorization type.

In case of CardLink authorization, the access authorizations are written directly in the user media. For validation, a time stamp and a validation period are additionally written in the user media. A user medium can be validated only at a component configured for the same.
The validation determines the length of time for which a medium is valid. There are eight validation choices. These cannot be deleted or expanded. 6 of these validations can be edited. See [▶ 6.9.2]



Follow-up time:

After the validation period has expired, the medium must be re-validated. The medium can be re-validated within the set follow-up time.

6.5 Components

6.5.1 Program the components

- Set up components for CardLink See [▶ 6.9.2]
- Set up components for whitelist See [▶ 6.9.1]

6.5.2 TimePro function

An active block of holidays overlaps with selected TimePro functions.

Set up TimePro function

TimePro function	Description
Standard	No time profile. An authorised medium is needed for opening.
Office	• Within the time profile entered, components can be set to open status by presenting an authorised medium. Present the medium. Present the medium for three seconds for a letter-box/lift. The component briefly lights up green. When open, no medium is necessary. • If user media are presented while open, the components close. Present the medium. Present the medium for three seconds for a letter-box/lift. The component briefly lights up green and then red. • If the time profile has expired, the components automatically close. An authorised medium is needed for opening. Outside the time profile, an authorised medium is needed.
Day/Night	The component opens and closes automatically, according to the set time profile. Outside the set time profile, an authorised medium is needed.

Setting the office mode behaviour

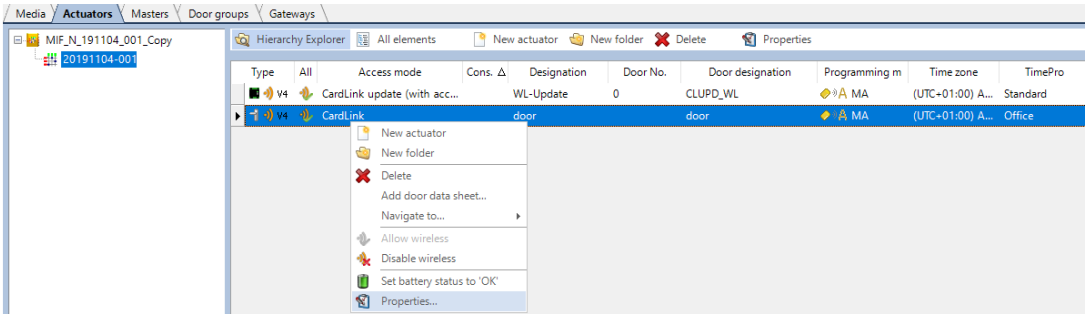
The behaviour in office mode is set in the project properties/general/TimePro. The setting determines the time for which the medium needs to be presented for activation/deactivation.

- Default: Immediate activation/deactivation.
- Delayed: Present the medium for 2 seconds. Only applies to E3XX actuators, not to PIN or code readers.

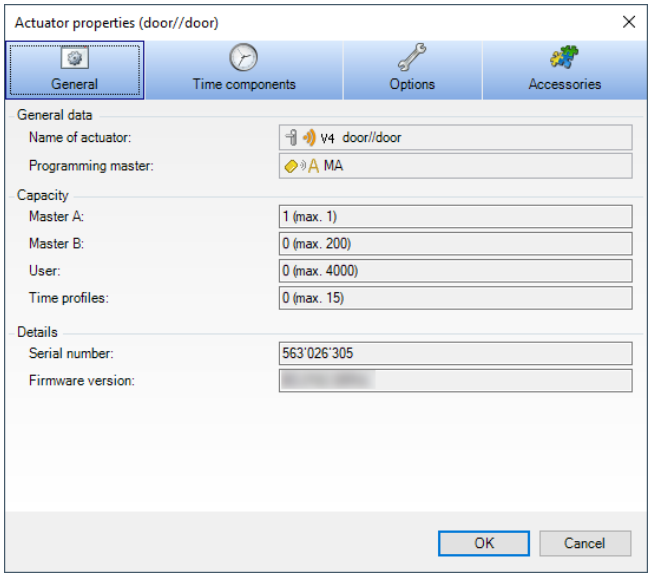
6.5.3 Edit properties

Editing the properties is restricted to the PIN code reader.

1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Actuators' tab.
3. Select all or individual components.
4. Open the context menu.
5. Click the 'Properties...' button.

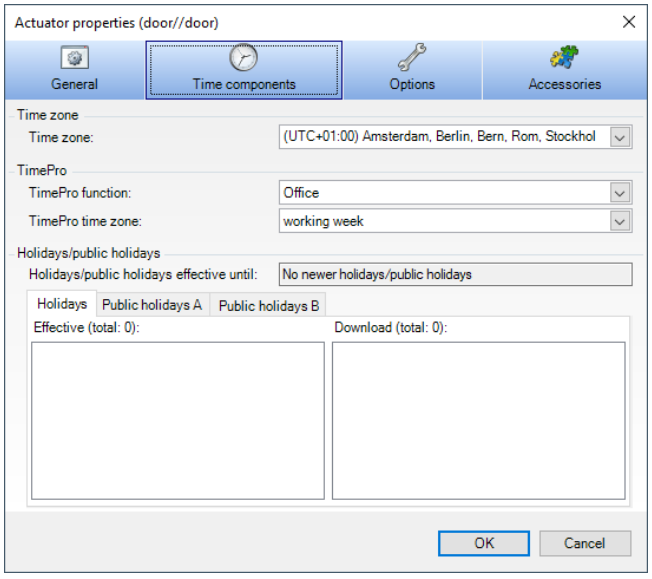


6.5.3.1 General



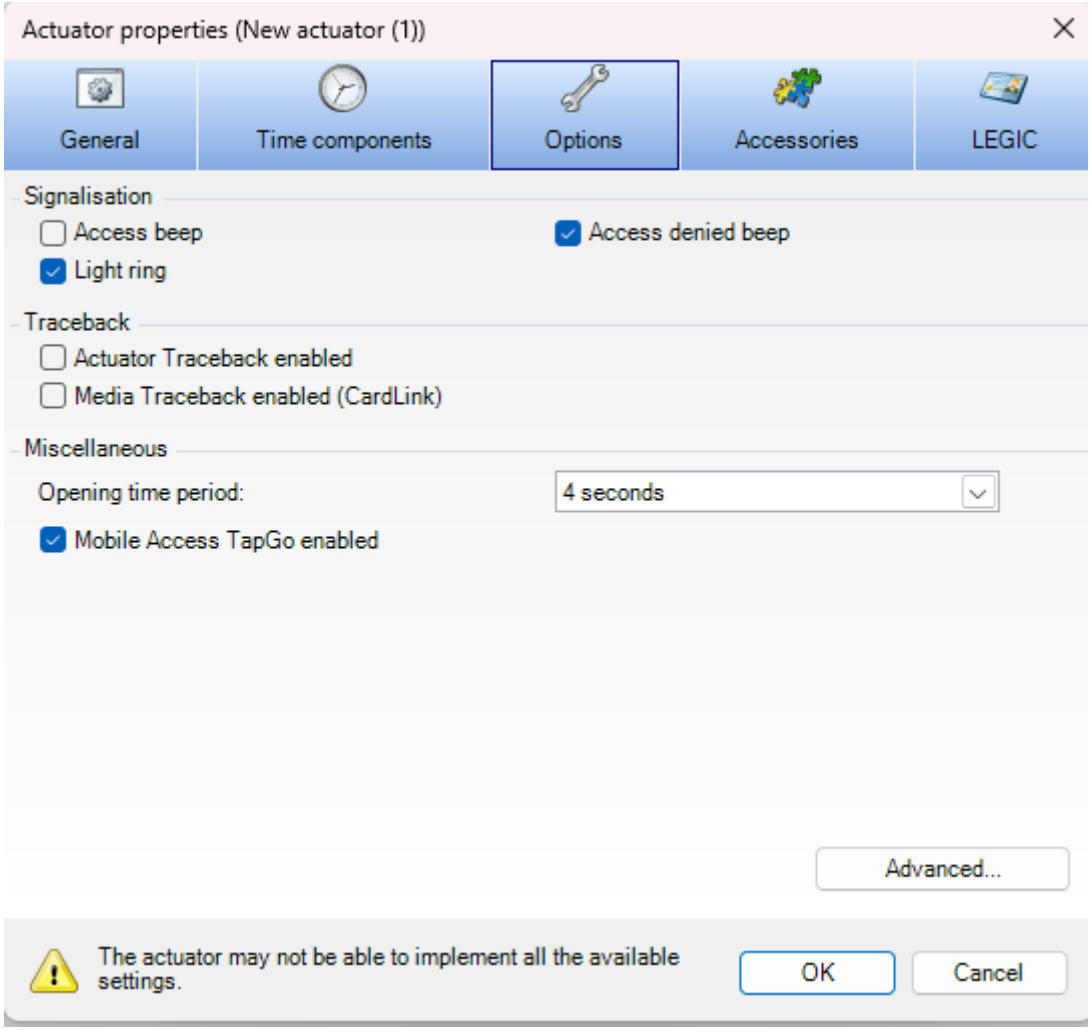
General information	
Actuator name	Detailed designation of the component
Programming master	The programming master to which this component is assigned
Capacity	This section lists the entries and the maximum values of the entries.
Master A	Number of the assigned Master As (maximum number of Master As to be assigned)
Master B	Number of the assigned Master Bs (maximum number of Master Bs to be assigned)
Users	Number of the assigned users (maximum number of users to be assigned)
Time profiles	Number of the assigned time profiles (maximum number of time profiles to be assigned)
Details	Details are displayed only after the result of the parameter setting had been read back with the programmer or wirelessly.
Serial number	The serial number saved in the component
Firmware version	The firmware version used in the component

6.5.3.2 Time components



Time zone	Setting the local time zone
TimePro function	
Standard	No higher-level time profile saved in the component.
Office	• Within the set time profile, change the components to open status by presenting an authorised medium. • If a user medium is presented while open, the components close. • At the end of the set period, the components close automatically.
Day/Night	The time profile determines the time period in which the components are open. The component opens and closes automatically, according to the set time profile.
TimePro time profile	Select a time profile if "Office" or "Day/Night" is selected as the TimePro function.
Holidays/special days	The profile shows the current and downloaded holidays and special days.

6.5.3.3 Optional extras



The elements in this window have the following functions:

Option	Description
Access beep	Turns the auditory signal for authorised access on or off.
Illumination unit	Turns the visual display on or off.
Access denied beep	Turns the auditory signal for unauthorised access on or off.

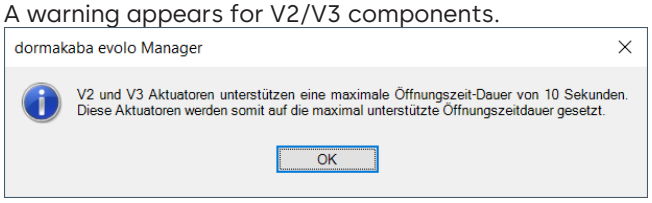
Actuator traceback active	Write traceback in the component's memory. [▶ 6.1.1]
Media traceback active (CardLink)	If the option has been selected in the project properties, then the traceback is written in the component's memory and on the medium [▶ 6.1.1].
Opening time duration	The opening mechanism is active for this time period.
Actuator transmitting power	Only if wireless is activated: selection of transmitting power of the component. Options available for selection are: high transmitting power normal transmitting power low transmitting power Choose the transmitting power so that the gateway is securely reached. This function has effects on the energy consumption of the component. Energy can be saved for standalone components by reducing the transmitting power to the degree needed for reaching the gateway.
Advanced	Advanced options: • Object in field interval • Bolt recreation time

We recommend deactivating the sound for "Access" status. This reduces power consumption. This sound is already deactivated by default for all components other than mechatronic cylinders.

Opening time duration
The opening mechanism of the component is active for this period. The adjustable times are the same for V2/V3 and V4 components as well as for the available technologies.

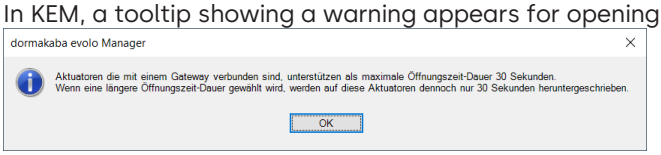
Select the duration from the list.

A maximum of 10 seconds can be selected for V2/V3 components.
If you select multiple V2/V3 and V4 components, all durations are available for selection. V2/V3 components are set to 10 seconds if the selected value is greater.
A warning appears for V2/V3 components.

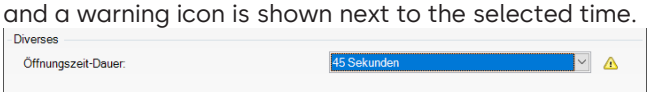


The wireless gateway cannot transfer opening times >30 s.

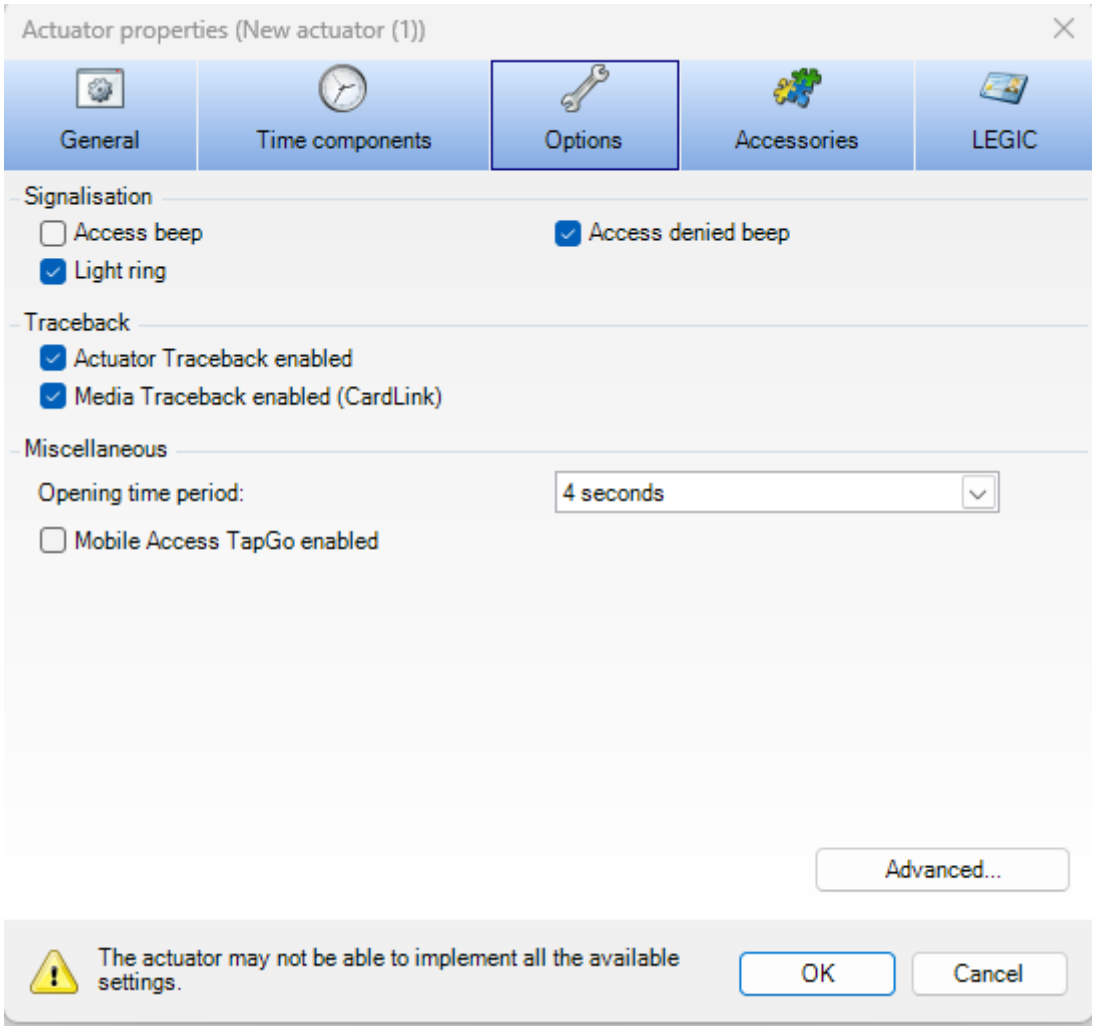
- In KEM, a tooltip showing a warning appears for opening times > 30 s



and a warning icon is shown next to the selected time.



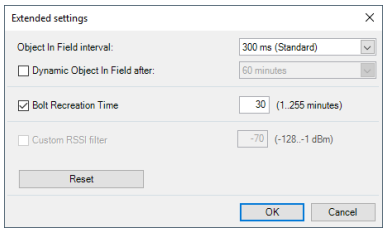
CardLink update reader
The checkbox only appears in this window if the selected component is configured as a CardLink update reader.



6.5.3.4 Advanced

Object in field interval (OIF):
This option is only available for V4 components.

The component checks at regular intervals whether a medium is within the field of the antenna. To save energy, the time interval between two checks can be extended. With a dynamic 'Object in Field', this time period is extended out to the maximum value step by step. If a medium is held up, the process begins again. A longer reaction time is possible for holding up a medium.



Set OIF:

1. Select the value of the interval in the selection menu.
2. Click the 'OK' button.

Set dynamic OIF:

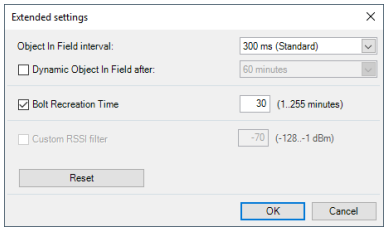
1. Select the checkbox 'dynamic object in field.'
2. Select the start value for the interval in the selection menu.
3. Select the start time.
4. Click the 'OK' button.

In order to activate dynamic OIF, it is necessary to have long rest times between two read operations.

Table: Saving energy through dynamic OIF. The values are approximate values. Actual energy saved still depends on other factors and settings.

Application	Settings		Energy saved	Effects
Examples	**OiF Interval**	**Dyn. OiF**	**Maximum**	
Default setting of component. **Highly frequented access points**	300 ms	OFF	0%	Normal
Low frequented access points	300 ms	ON 30 min	15%	Extended reaction time when first holding up a medium after a long pause. Normal for other media within the set time.
• 20 operations in the morning and 20 in the evening within the set time. Between that time one operation per hour for 10 hours.	300 ms	ON 30 min	19%	
• One operation per hour for 10 hours	300 ms	ON 30 min	22%	
Rarely needed access points • Two operations in the morning and two in the evening within the set time. No operations between that time.	300 ms	ON 30 min	30%	Extended reaction time for first use after a long pause. • Reading out a held-up medium can take up to one second.
• Long rest periods between the operations • No operation for one or more days	1,000 ms	OFF	34%	

Bolt recreation time
"Bolt recreation time" defines the time interval in which the engagement status of the mechatronic unit should be checked.
This function is not available for all devices.



Set bolt recreation time:

1. Select the checkbox.
2. Select a time in the selection menu.
3. Click the 'OK' button.

Reset
Click the 'Reset' button: The values in this window will be reset to their default values.
Default values are:

- Object in field interval: 300 ms
- Dynamic object in field: deactivated
- Bolt recreation time: 30

6.5.3.5 Accessories

Based on the type of component, various options like S-Module and Pass-Lock (only for c-lever, c-lever pro) can be selected under Accessories. Information on the function 'escape return' is described in the brief instructions 'Kaba c-lever escape return (k1evo818xy)'.

6.5.3.5.1 S-Module

The S-Module is supported in wireless mode (for requirements, see section [▶ 11.2.3]).

Medical practice example:
Patients must have access to a medical practice during opening times. The main door can be released for patients using a button. The patients do not require any media and the media practice can be accessed.

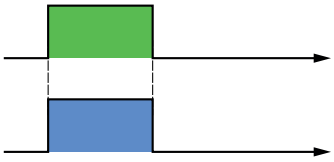
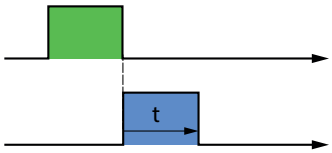
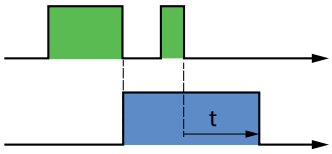
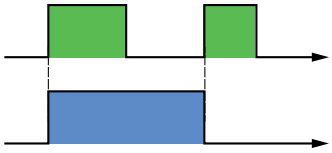
6.5.3.5.1.1 Operating mode: electric strike with S-module functionality

The behaviour of can be changed using the contact connected to the digital input. The contact overrides the authorisations and activates the behaviour programmed in dormakaba evolo Manager or in Kaba exos.

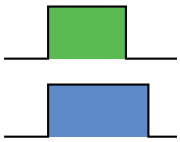
Possible contacts: switch, time switch or building control system (e.g. alarm system)

Behaviour available for selection in dormakaba evolo Manager or Kaba exos

'Active if:'

As long as input active	As long as the input is active (green), the programmed behaviour is active (blue).	
Period limited	The measurement of the duration starts with the inactivation of the input.	
	If the input is reactivated before the set duration elapses, the programmed behaviour is extended.	
Pulse mode	With the first flank of the input to active, the programmed behaviour is activated. With the next flank to active, the behaviour is inactivated.	

Legend



Input active (green)

Programmed behaviour active (blue)

'If active:'	Impact
Always open	Always open
Always closed	Always closed, no access possible
Open with any medium	Can be opened with any medium (writes UID of the medium to TraceBack)
Switch off TimePro	TimePro is inactivated

Defining the logic

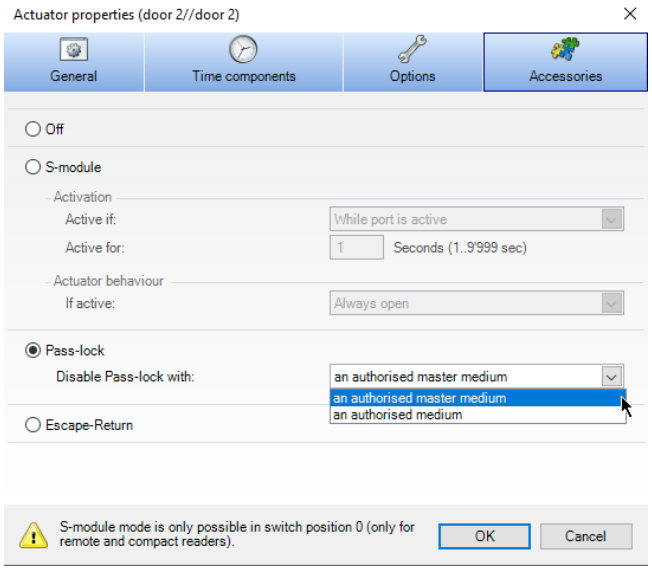
The S-module functionality includes an auto-learn function. Upon initialisation (INI reset) of the current position of the contact is interpreted as the base position. If the position of the contact changes, the behaviour programmed under 'Activation' is activated. This way, a normally open or normally closed contact can be defined.

6.5.3.5.2 Pass-Lock

Select the following properties from the list for the pass-lock option:

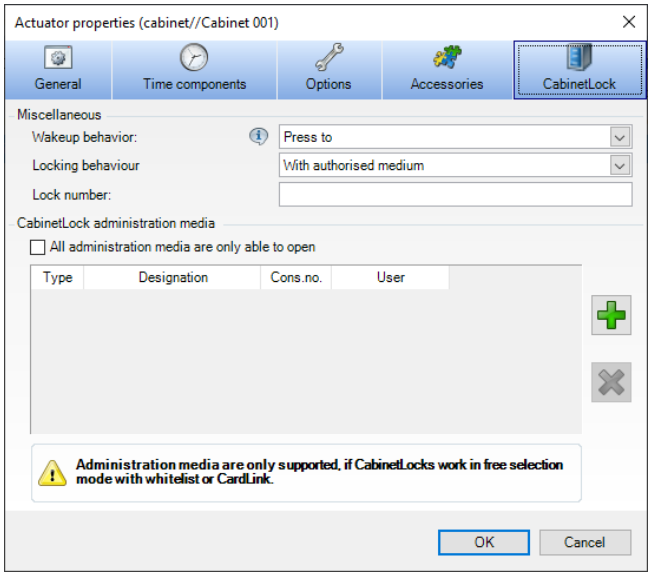
- Authorised master medium
- Authorised user medium

With the media type selected here, the door parametrised like this can be opened from the outside again after activation of pass-lock. The door can always be opened from inside.



6.5.3.6 Locker lock 21 10

These properties can only be parametrised for a locker lock 21 10.



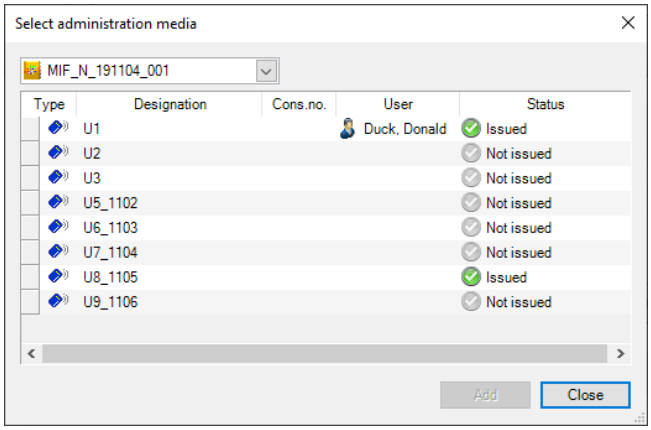
The following can be parametrised in this window:

- Wakeup behaviour:
  a) By pressing: to activate the electronics and establish readability, press on the door slightly. If a medium is then presented, authorisation is checked.
  b) Object in field: the locker lock periodically checks whether a medium is within the antenna field. As soon as a medium is within the antenna field, it is read out and authorisation checked.
- Closing behaviour:
  a) With authorised medium: the locker can only be opened or locked with an authorised medium.
  b) Without medium: the locker locks when pressing on the door.
- Locker lock number:
  The number of the locker in which the lock is located.

These numbers can be assigned multiple times, e.g. if lockers are located in different areas of a building.
A UID or CID saved on the medium is uniquely assigned to this medium. During closing, this UID or CID is saved in the lock and thereby assigned to this locker. The locker can then only be opened with the same medium. If a locker lock number is assigned multiple times, the UID or CID of the locking medium takes priority.

When closing the locker, the locker lock number is entered onto the medium. If it is not assigned (empty field), then the serial number of the locker lock is entered.

- Administration media:



With this checkbox activated, the parametrised administration media can only open a locker but not lock it again.
Administration media can be added or removed via the context menu as well as the two buttons on the right side.

6.5.3.7 Letterbox/lift

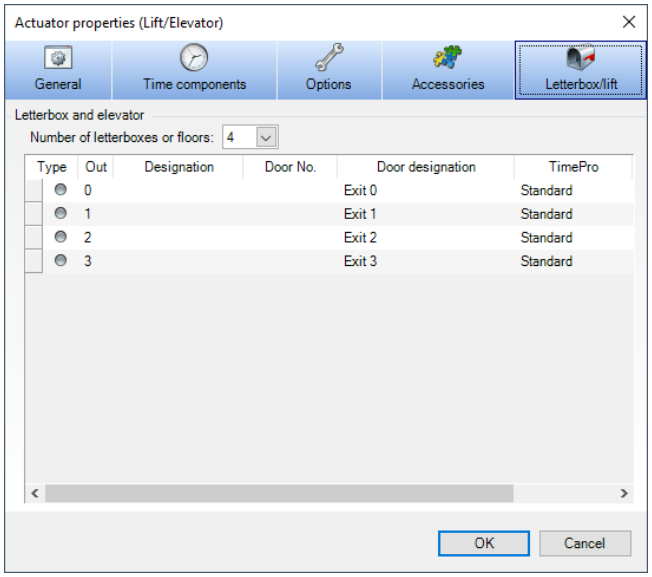
A user can only select those floors in a lift or open those letterboxes for which their user medium authorises them to do so.

Only whitelist is supported. CardLink is not possible.
In the Whitelist (UID/Card ID), a maximum of 1,000 users can be configured for the letterbox/lift.

Mobile Access with Bluetooth is possible by using the appropriate hardware and firmware.
This can normally be configured in KEM.

Create floors/letterboxes

Select the number of floors/letterboxes necessary in the selection menu (0–49).
Up to 49 floors/letterboxes can be created.



Configure floors/letterboxes

- Out
  Number of physical outputs of the component.
  Output "0" is located on the main device; other outputs (1–8), (9–16) etc. can be found on the additional modules.
  (Defined, cannot be modified)
- Name
  Indicate a name for this element. For example:
  Letterbox: "Miller family"
  Lift: "Exit" or "1st Floor"
- Door no.
  Numerical sequence element within the locking system.
- Door designation
  Designation of the element within the locking system.
- TimePro
  Set up TimePro function
  The individual functions are described in the "TimePro" [▶ 6.5.2] section.
- TimePro time profile
  If "Day/Night" or "Office" is selected, select a profile from the list. To create time profiles, see the "Time profiles" section.
  For "Office", hold the medium up for three seconds to actuate the outputs.

Ratio of outputs to needed components:

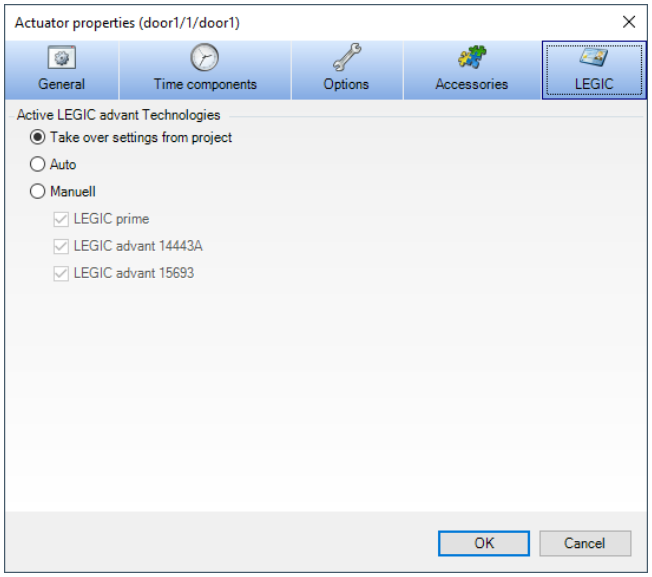
Number of outputs	Number of components
One	91 15 (remote reader with one relay output)
Up to nine	91 15 + 1 x 90 30 (extension module with eight relay outputs)
Up to 17	91 15 + 2 x 90 30
Up to 25	91 15 + 3 x 90 30
Up to 33	91 15 + 4 x 90 30
Up to 41	91 15 + 5 x 90 30
Up to 49	91 15 + 6 x 90 30

6.5.3.8 LEGIC

LEGIC technology

The LEGIC technology can be selected in the project properties. There is another selection option for the component.

The following settings are possible:



- Accept setting from the project
  The component uses the settings from the project properties. The PIN code reader takes over the properties of the access manager.
- Auto
  The technology is automatically selected.
- Manual
  One or more technologies can be selected.
  - LEGIC prime
  - LEGIC advant 14443A
  - LEGIC advant 15693

1. Select the actuator properties with right-click in basics/actuators.
2. Under properties, select the LEGIC tab.
3. Select the technology.
4. Select OK.

The component uses the selected technology. Media that do not use the selected technology are not detected and are ignored.

6.5.4 Determining the battery status

Components with a CR2 battery, e.g. digital cylinders, transmit only "ok" or "BatLow" as battery status.

The battery status of the components can be checked under the following requirements:

- In a wireless environment.

  In case of a query through the system software, the battery status along with the information is sent to the gateway.
- With programmer 1460 (directly on the component).

  The battery status in the programmer can be read out via the "Actuator info" menu. If a traceback is read out and the programmer is connected to the KEM, the battery status can be read out under the 'Actuators' tab in the info bar of the component.
- In a CardLink environment.

  The battery status of the component is transferred with the protocol data of the user medium.

6.5.5 Migrate components with V3 to V4

The advanced functions Time profile V2, TimePro 'Day/Night drive' and S-module are no longer supported after migrating.

Requirements

- The hardware components support V4.
- The master media for V4 are registered in the project.
- The time profiles for V4 are registered in the project.
- Only supported time profiles are copied.
- The properties and functions are transferred to the same properties and functions of V4.
- The existing authorisations are retained.

Conversion with context menu

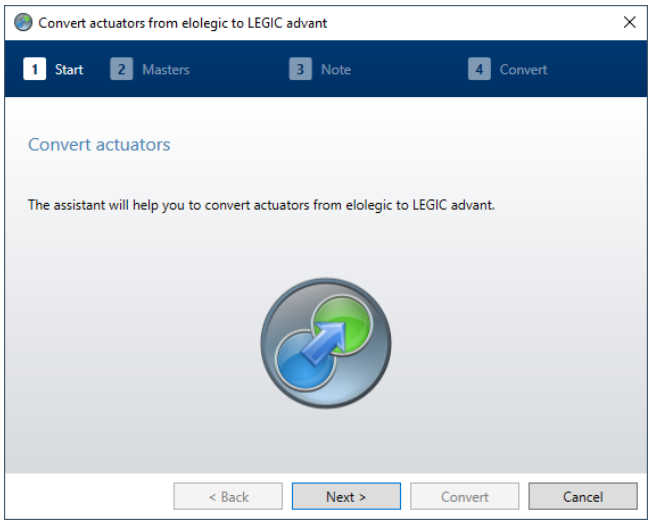
Conversion cannot be undone.
We recommend creating a backup copy of the existing project prior to conversion.

1. In the 'View' toolbar, open the 'Basics' menu.
2. Go to the 'Actuators' tab.
3. Select all or individual components.

4. Open the context menu.
5. Select the menu item 'Convert, elolegic to LEGIC advant".

Not all components can be converted and some individual components cannot be converted. That is, for example, elolegic cylinders **cannot** be converted to digital cylinders or c-lever.

6. Follow the wizard.
   The number of steps depends on the type of component.



7. After conversion, click the 'Close' button.

6.6 Door groups

Door groups are registered for easier management of door authorizations.

Door groups are only available in the CardLink authorization type.

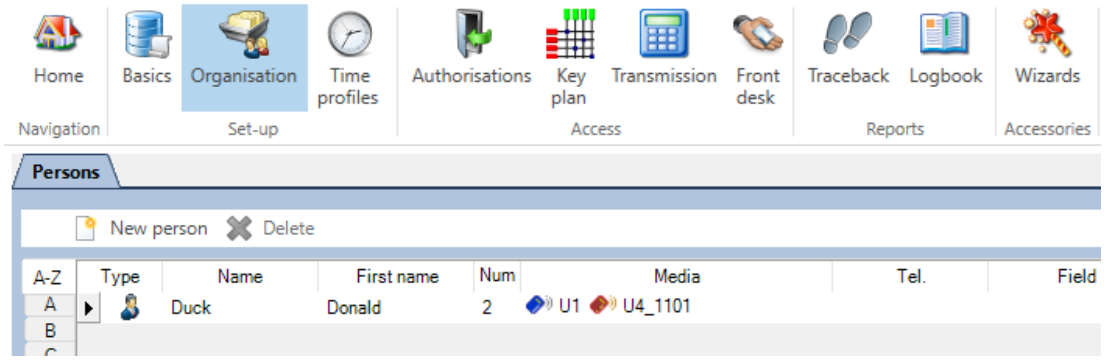
6.7 Persons

Creating multiple persons with the same name can lead to problems if the personal name of one person is to be deleted.

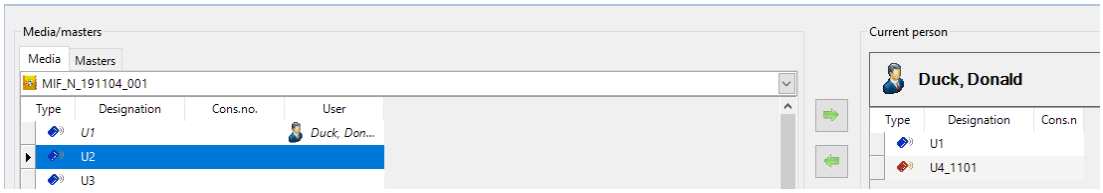
- If there are multiple persons with the same name, the names of all these persons will be deleted from the logbook, protocol list and traceback.

A staff list containing the media assigned to these persons is kept for the purpose of media management.

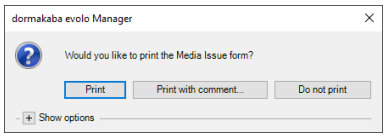
1. Open the 'Organisation' menu from the Navigator toolbar.
2. Use the 'New person' button to add a new user.



3. Assign media to the persons from the list:
   -- Highlight the person to whom a medium is to be assigned in the list. The name will appear in the area at the bottom right.
   -- Use the arrow button (in the middle) to move a selected medium from left to right or drag and drop from left to right.



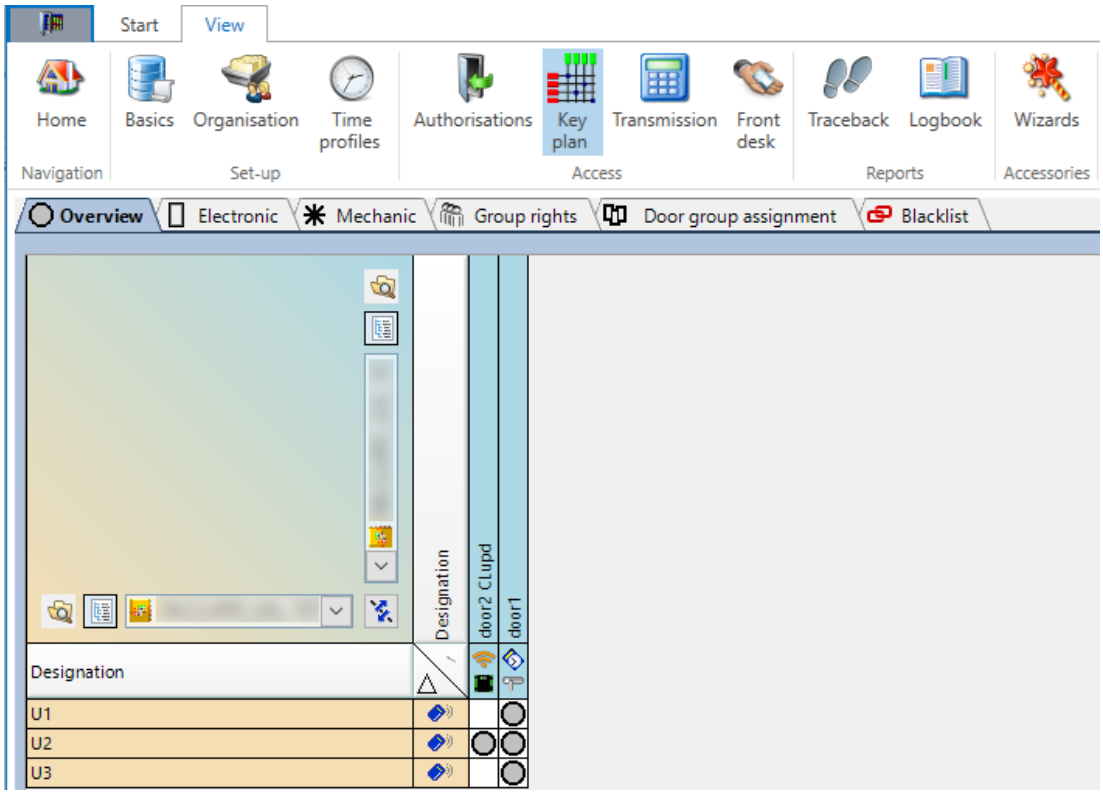
4. In the Print dialogue, choose whether the output form should be printed with or without commentaries.



6.8 Key plan

The authorisations are presented clearly in the matrix of a key plan.

Using the context menu of a matrix dot, you can call up the 'Export key plan to Excel...' function. The key plan will be exported to an Excel file.



Overview	• Authorisations of all media at components • Authorisations at mechanical components • Editing not possible
Electronic CardLink/ whitelist	• Authorisations of the electronic media at components • Editing possible
Mechanical	• Authorisations at mechanical components • Editing possible
Group rights (CardLink)	• Door group authorisation of the electronic media • Editing possible

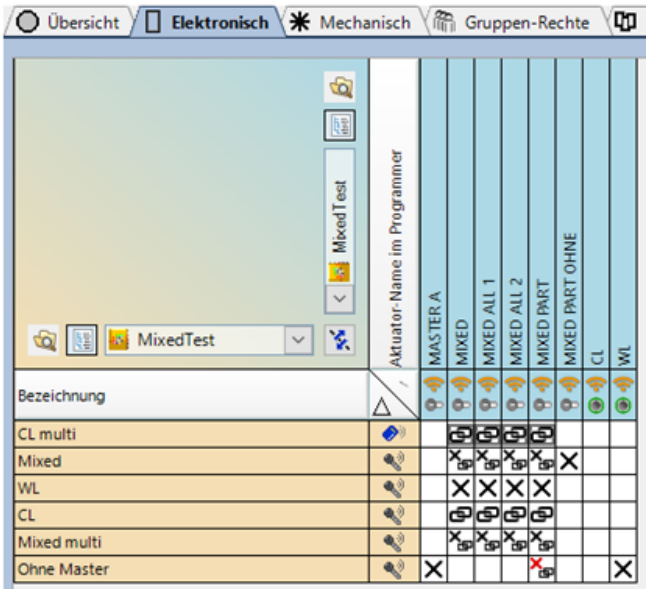
Door group assignment (CardLink)	• Door group assignment for electronic media • Editing possible

Explanation of symbols in the matrix:

Symbol	Description
	Authorisation set Under the "Overview" tab, it is shown if an authorisation is set.
	Mechanical authorisation The 'Mechanical' tab shows whether an authorisation has been set.

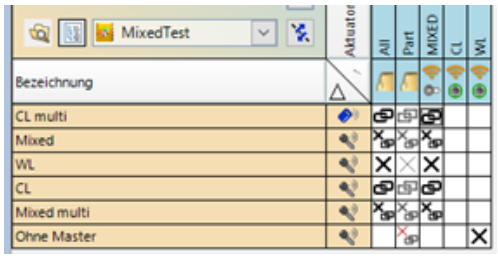
If you hover the mouse over a symbol, a tooltip will be displayed showing the values of the point in the authorisation matrix.

Electronic key plan 1:1



Symbol	Description
	No authorisation
	Whitelist authorisation has been set.
	Whitelist authorisation has been set, Master B missing.
	Whitelist and CardLink authorisation set (multiple reservations possible).
	Whitelist authorisation with missing Master B and CardLink authorisation set (multiple reservations possible).
	CardLink authorisation has been set.
	Multiple reservations set (at least 2).

Electronic key plan n:n



Symbol	Description
	No authorisation
	Whitelist authorisation set
	Whitelist authorisation partly set
	Whitelist authorisation set, Master B missing.
	At least one whitelist authorisation with missing Master B.
	Whitelist and CardLink authorisation (multiple reservations possible)
	Whitelist and CardLink or/and Mixed authorisation partly set.
	Whitelist authorisation with missing Master B and CardLink authorisation (multiple reservations possible)
	Master B missing from at least one whitelist authorisation. Partial whitelist and CardLink or/and mixed authorisation
	CardLink authorisation set.
	Multiple reservations made (at least 2).

6.9 Authorisations

Various authorisation structures are possible in the KEM software. A distinction is made between the CardLink authorisation type and the whitelist authorisation type.

CardLink authorisation	The access authorisations are saved to the media.
Blacklist (CardLink)	If a user medium needs to be disabled within the validity period, then it should be entered onto the blacklist. This removes authorisation from this user medium.
Whitelist authorisation	A whitelist is the set of media entered into the component's memory that are authorised to access that component or access manager.
Free choice with whitelist	This function can only be configured in connection with cabinet lock 21 10.
Free locker selection with CardLink	This function can only be configured in connection with cabinet lock 21 10.

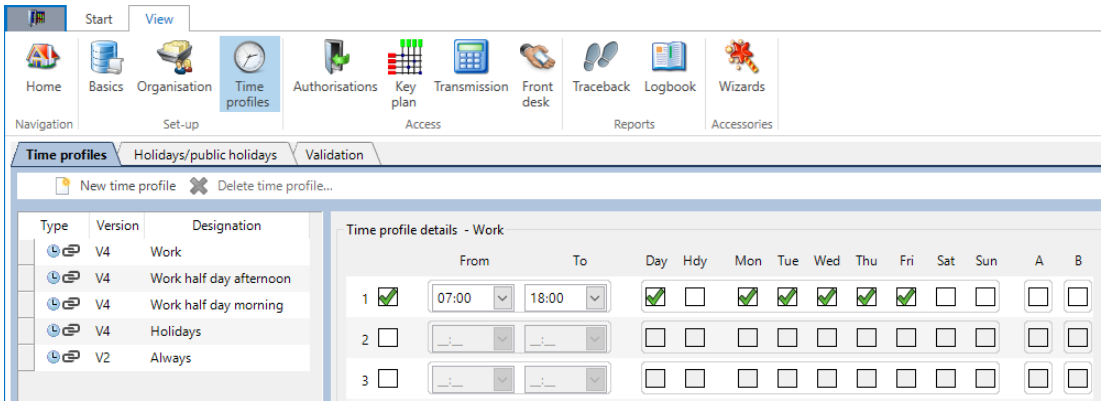
Note: Changes to the time profiles must be transferred to the components using a programmer or wirelessly. [▸ 6.10]

6.9.1 Setting up whitelist authorisation

Requirements and background information on the access manager can be found in the Access manager chapter.

Set up time profiles

1. In the 'View' toolbar, open the 'Time profiles' area.
2. Go to the 'Time profiles' tab.
3. Click the button 'New time profile' and create a new profile.
4. Select the time profile type.
5. Enter the name for the time profile into the "Name" field, e.g. 'Work week'.
6. Activate the corresponding checkboxes with the desired time profile details.

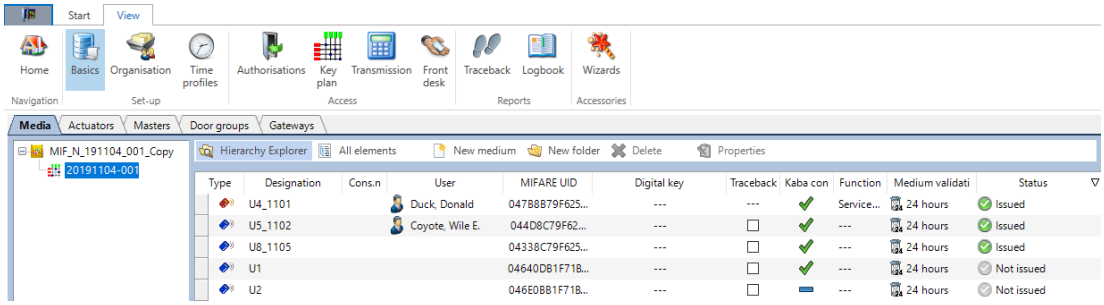


For more information, see chapter Access Manager.

Reading in/importing media

Media can be registered manually via the 'New medium' dialogue. It is possible to import a media list.

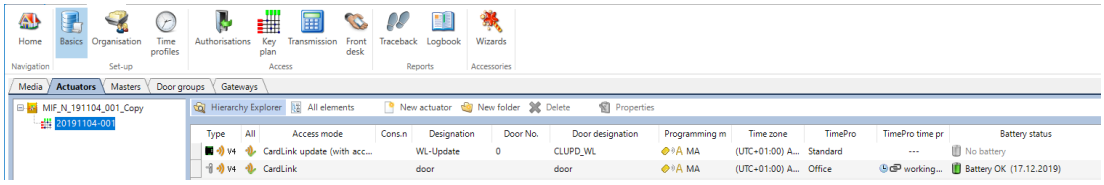
1. Open the 'Basic settings' menu from the Navigator toolbar.
2. Navigate to the 'Media' tab.
3. Place the medium on the desktop reader.
4. Fill in the 'Designation' and 'Cont. no.' fields.
   If necessary, enter the 'Card ID' as well.
5. Click on the 'Save' button.
6. Click on the 'Close' button.



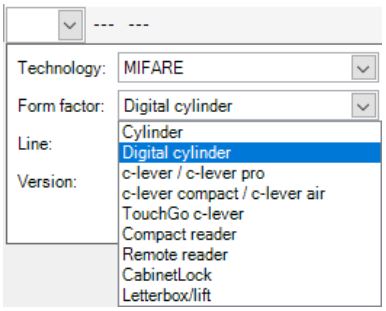
Create component and assign master

It is preferable that the components are imported using a KIF file.
Procedure if no KIF file is available:

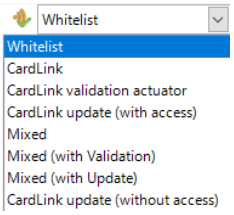
1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Actuators' tab.



3. Click on the 'New actuator' button.
4. In the "Type" column, select technology, form factor, line and version from the list.



5. Click on the 'OK' button.
6. Select the access mode from the list.



7. Fill out the "Ser. no.", "Designation" and "Door no." fields.
8. Assign a programming master to the component.

Letterbox/lift

This component has up to 49 connected outputs. These must then be configured in the properties.
Selecting this type is only possible for projects with V4.

Create main device and switch outputs:

1. Click 'Create new actuator'.
2. For form factor, select 'Letterbox/lift'.
3. Select the line 'E305' (standalone) or 'E345' (mobile with Bluetooth).
   ⇨ Version should be set to "V4".
   ⇨ The access mode should be set to 'Whitelist'.
4. Click 'OK'.
   ⇨ The main device has been created.
5. Enter or select serial number, name, door number, door name, programming master, time zone.
   Note: Access mode, TimePro and time profiles cannot be configured for the main device.
   ⇨ The device has been configured. Now, parametrise the number and name of the switch outputs.
6. Select the component.
7. Open the context menu.
8. Select the properties.
9. Select the property 'Letterbox/lift'.
10. In the selection menu, select the number of switch outputs.
    Note: select "0" from the list for components without an output up to "49" for components with 49 outputs.
11. Enter the names of the individual outputs in the details.
    Note: TimePro and time profiles can be separately configured for any output.
12. Click 'OK'.

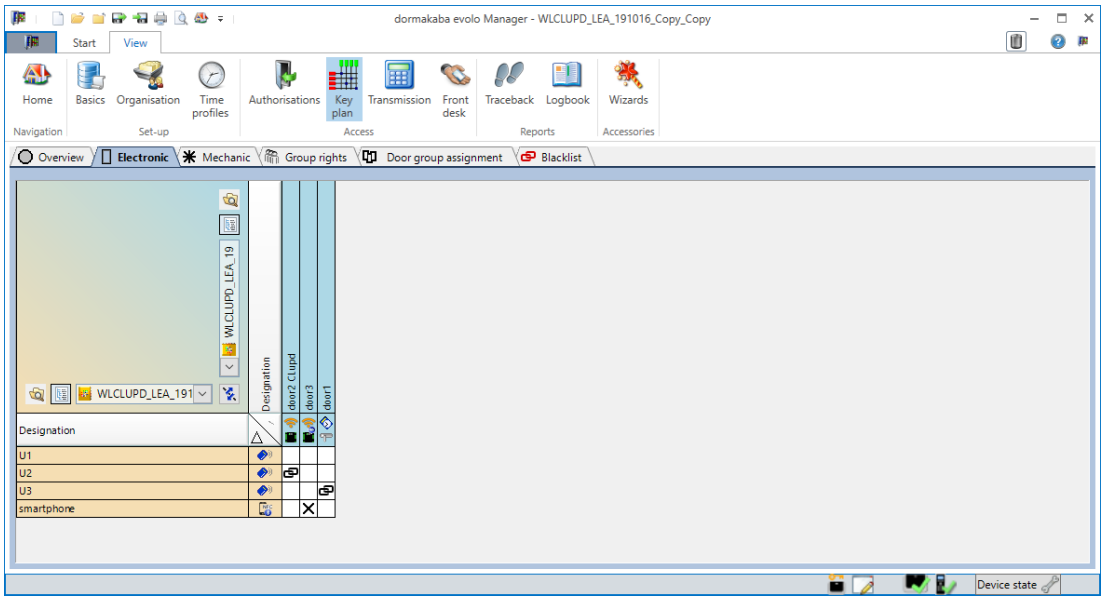
⇨ The outputs have been configured and authorisations can be assigned to the individual outputs.

Assign media (with time profile)

Using the 'Authorizations' button on the 'View' toolbar, media can be assigned to the components.

1. In the 'View' toolbar, open the 'Key plan' area.
2. Go to the 'Whitelist' or 'Electronic (CardLink)' tab.
3. The desired assignment is activated using the matrix.

4. Assign a time profile to the selected intersection.
5. Click on the 'OK' button.



For clarification of the symbols in the matrix, see section [▶ 6.8].

Prepare media in Whitelist for CardLink

If a project is created with Whitelist authorisation, the user media can be prepared for a later project with CardLink authorisation. The CardLink authorisations will already be saved to the media and do not need to be activated when switching the actuators to CardLink.

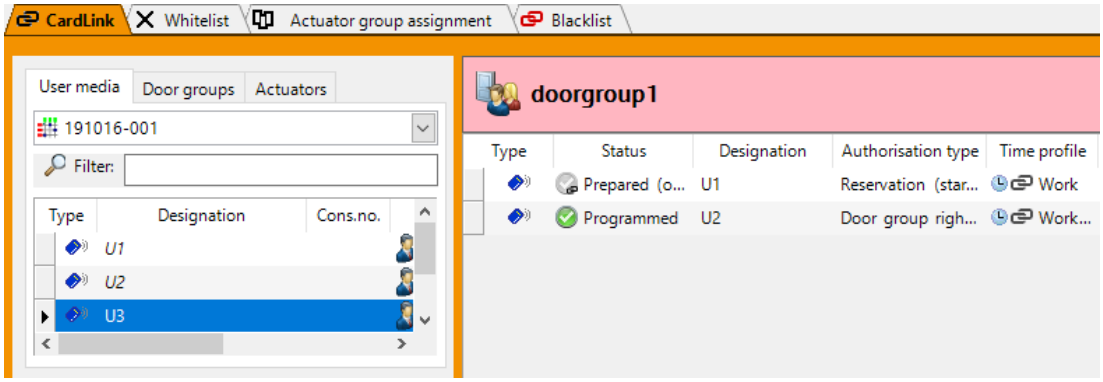
It is also possible to switch from a project with Whitelist authorisation to a project with CardLink authorisation retrospectively.

Requirements in the project properties (F4):

- The project must have been created fully in Whitelist mode.
- Access technologies:
  - elolegic
  - LEGIC advant
  - MIFARE
- Access mode
  - Whitelist and CardLink
- Security card
  - The security card exists or has already been read into the project.

Prepare for CardLink

1. Open project properties (F4).
2. Switch access mode to "Whitelist and CardLink mode."
3. Read in security card if it is not yet available in the project.
4. Close project properties.
5. In the 'View' toolbar, open the 'Authorisations' area.
6. Go to the 'CardLink' tab.
7. Go to the 'User media' subtab.

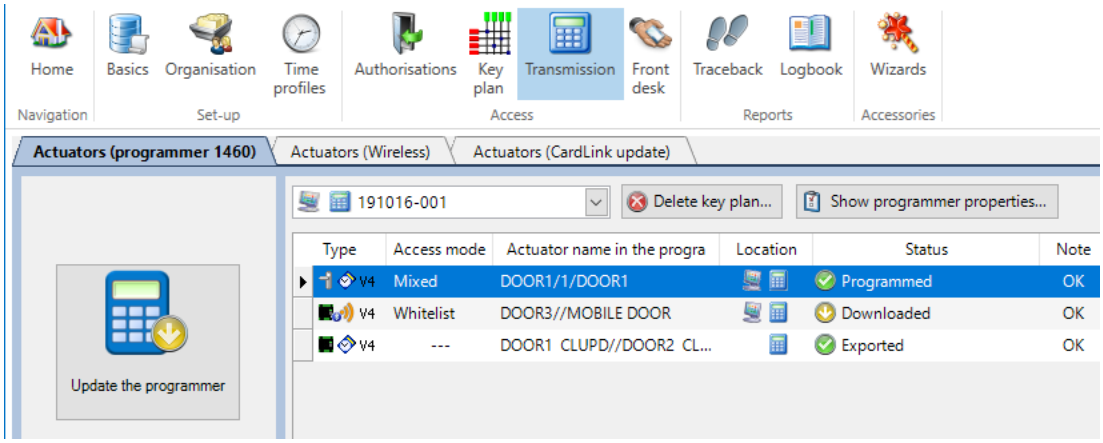


8. Drag the individual user media from the list in the left window and drop them into the top right window. The user medium will appear in the window.
9. Select the authorisation type and the time profile.
10. Go to the 'Actuators' subtab.
11. Drag the individual components from the list in the left window and drop them into the large right window.
    The newly assigned components will appear highlighted in grey if they are not yet in CardLink mode.
12. Put the corresponding user medium onto the desktop reader and program it. The user media are now prepared for CardLink.

Program the components

1. Connect the programmer and the computer with a USB cable.
   ⇨ The programmer appears in the status bar.

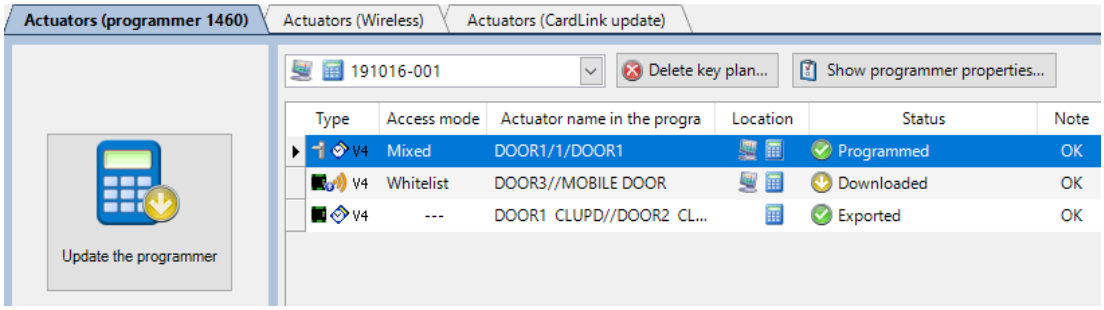
2. In the 'View' toolbar, open the 'Transmission' area.
3. Select the locking plan from the list.
4. Click the 'Update programmer' button.
   ⇨ The data are loaded onto the programmer.



5. Disconnect the programmer from the computer.
6. Transfer the data to the individual components using the programmer.

Confirm programming

1. Connect the programmer and the computer with a USB cable.
2. In the 'View' toolbar, open the 'Transmission' area.
3. Select the locking plan from the list.



⇨ The data are automatically updated. In the 'Status' column, the programmed components are marked with the status "Current".

Do not disconnect the programmer during data transfer: otherwise, data are not transferred or are transferred incompletely.

6.9.2 Setting up CardLink authorisation

If authorisation logging is activated, all authorisation-relevant activities are logged in a CardLink system.

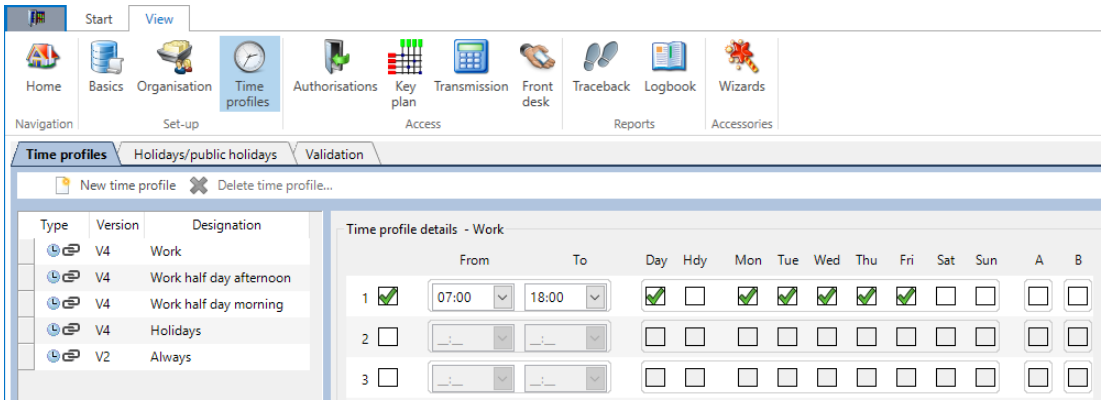
- To switch logging on or off, see section [▸ 6.2.2.1].
- For viewing/exporting the protocols, see section.

Information on the technologies

- dormakaba evolo supports CardLink.
- Kaba elolegic supports CardLink only with U-Line components.
- Kaba elostar does not support CardLink.

Setting up time profiles for door groups

1. Open the 'Time profiles' menu from the Navigator toolbar.
2. Navigate to the 'Time profiles' tab.
3. Click on the 'New time profile' button and register a new profile.
4. Enter a name in the Designation field.
5. Activate time profile details.



Set up validation times

1. In the 'View' toolbar, open the 'Time profiles' area.
2. Go to 'Validation' tab.
3. Change the type "end time" or the modifiable types. Change options are listed in the table.

⇨ The set validation times can now be used to set time profiles for components and media in the 'Basics' area.

Validations not modifiable	24 hours
Validations not modifiable	"Always" (unrestricted)
Validation with adjustable clock time	End time (only whole hours)

5x validation with adjustable duration	Days and hours

For validations with adjustable clock time and duration, the name field can be filled out with a user-defined name.

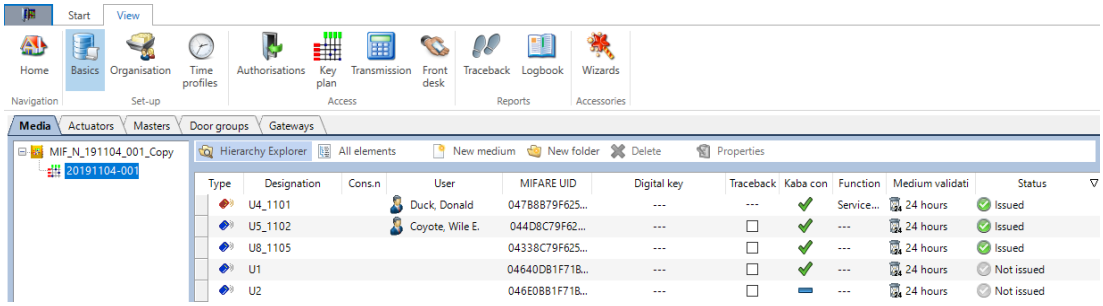
The set time profiles and validation dates can be applied to the individual components and media in the 'Basics' area:

- In the 'Actuators' tab in the fields
  - TimePro
  - TimePro time profile
- In the 'Media' tab in the fields
  - Medium validation

Reading in/importing media

elostar and elolegic media are read in using Programmer 1364. The desktop reader can also be used for LEGIC media.

1. Open the 'Basic settings' menu from the Navigator toolbar.
2. Navigate to the 'Media' tab.



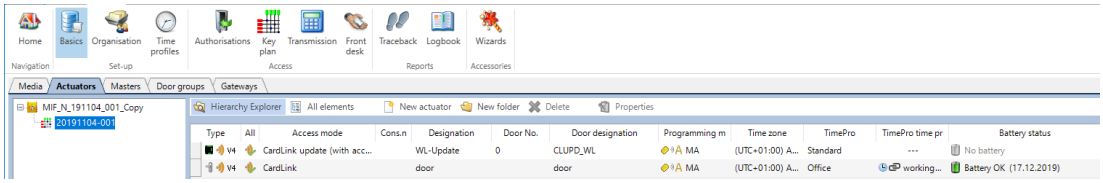
3. Select the key plan to which the media are to be read in.
4. Place a medium on the desktop reader.
5. Fill in the 'Designation', 'Cont. no.' and 'Users' fields.
6. Click on the 'Save' button.

Media can be registered manually by selecting the 'New medium' button. A media list can also be imported. [▶ 12.1]

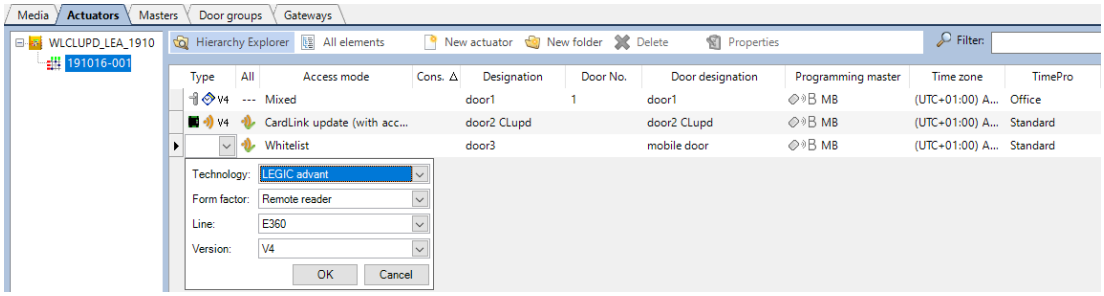
Create component and assign master

Procedure

1. In the 'View' toolbar, open the 'Basics' menu.
2. Go to the 'Actuators' tab.



3. Create the component with the "New actuator" button.
4. In the 'Type' field, select suitable values from the lists Technology, Form factor, Line and Version.



5. In the 'Access mode' field, select the mode for the selected type.
6. Fill out the fields Ser. no., Name, Door no.
7. Select a profile type in the TimePro field.
8. Press OK to confirm.
9. Select the programming master from the list under programming master.

It is preferable that the components be imported using a KIF file.

Determine components for validation

In LEGIC advant projects, the component for validation must be activated with the C2 security card.

Write authorisation for LEGIC advant

Procedure

1. Present the master medium to initialise programming.
2. Present the security card C2 for 20 seconds to activate write authorisation. The component LED lights up green during the process.
3. After 3 beeps, the green LED turns off and the process ends.

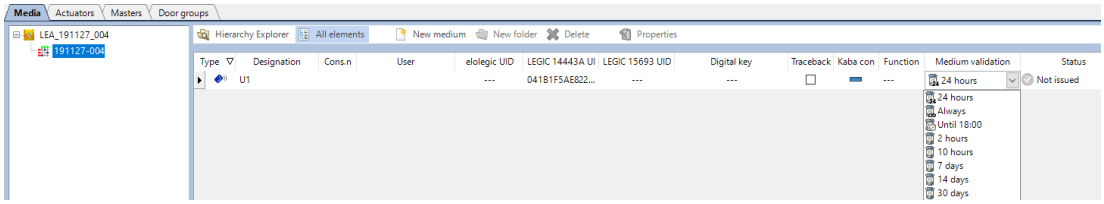
The authorisation data are deleted after an INI reset.
Carry out authorisation again.

1. In the 'View' toolbar, open the 'Basics' page.
2. Go to the 'Actuators' tab.
3. Select the validation mode from the list.
4. Select the media or components.

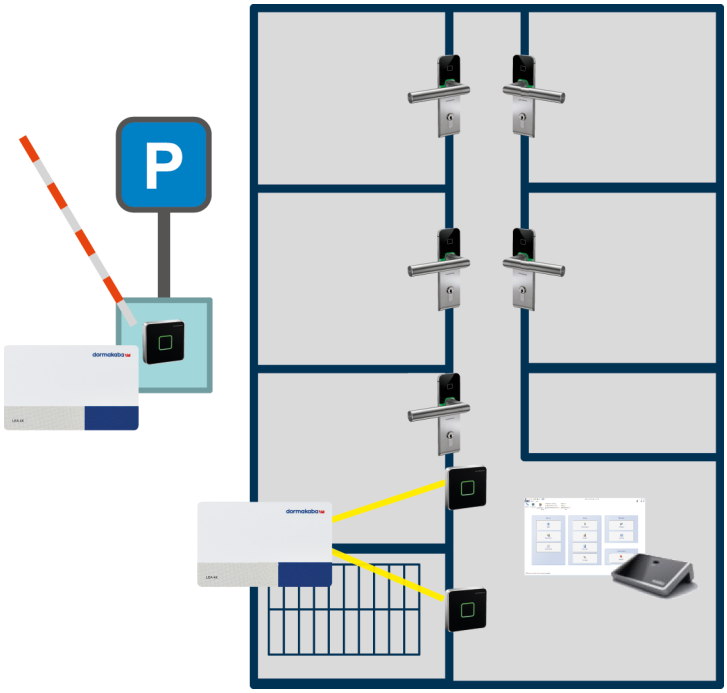
Define validation time for medium or component.

Procedure

1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Actuators' tab.
3. Select the entry desired for validation time from the list under "Actuator validation".

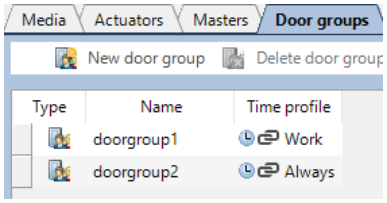


Example:
Validation in the building is written onto the media with the validation components, e.g. validation time one day. This way, a medium is only valid for one day. In case a user is absent for a long period of time, for the expired medium to still receive access at the parking gate, the component at the parking gate (arm) is set to validation mode 'Actuator 120 days'. If the user is absent for more than 120 days, even access to the car park is no longer possible.



Setting up door groups

1. Open the 'Basic settings' menu from the Navigator toolbar.
2. Navigate to the 'Door groups' tab.
3. Click on the 'New door group' button.
4. Register a new group.
5. Enter a name for this door group in the 'Name' field.
6. Select a time profile for this door group from the list under 'Time profile'.

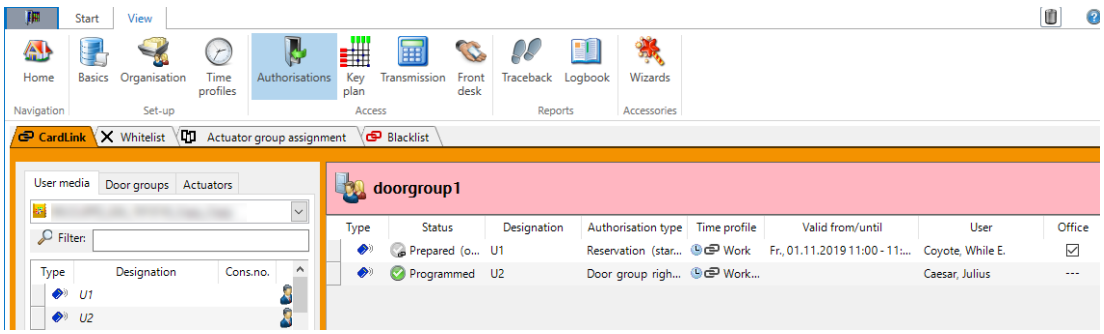


Group assignment of components (assigned to the door groups)

Door groups can also be created using the “Create new door groups” wizard.

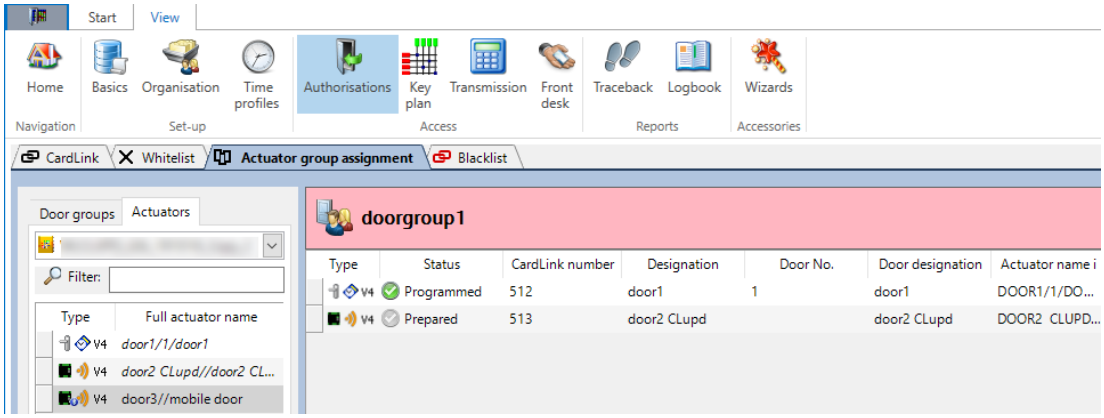
Procedure

1. In the 'View' toolbar, open the 'Authorisations' area.
2. Go to the 'Actuator group assignment' tab.
3. Go to the 'Door groups' subtab.
4. Select the door group from the list.
5. Drag and drop the door group into the top right window. The selected door group appears in the window.



6. Go to the 'Actuators' subtab.

7. Drag the desired components from the list in the left window and drop them into the right window (Door group...)

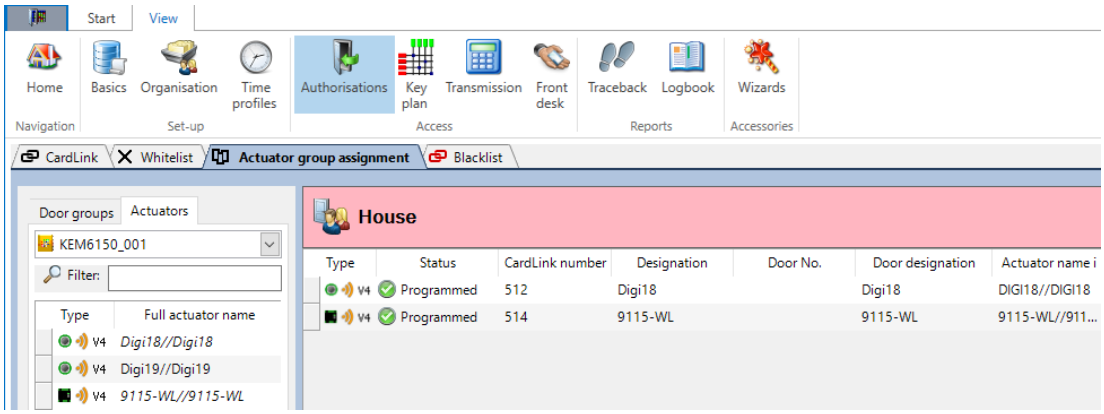


Multiple different door groups can be assigned to one component.

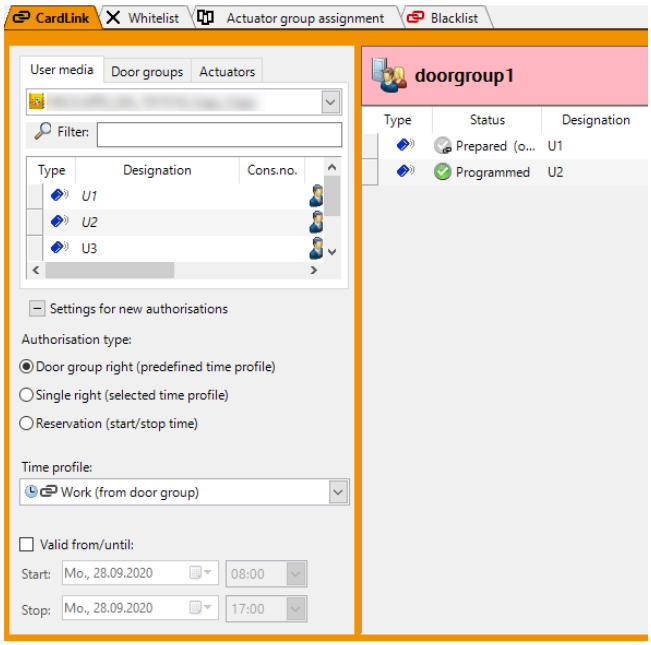
Create CardLink authorisation

Procedure

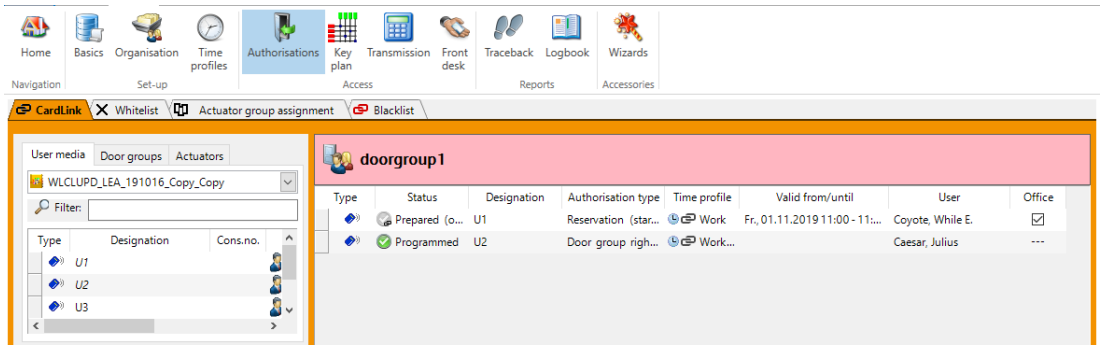
1. In the 'View' toolbar, open the 'Authorisations' area.
2. Go to the 'CardLink' tab.
3. Go to the 'Door groups' subtab.
4. Select a door group from the list.
5. Drag and drop the selected door group into the top right window.
   ⇨ The selected door group appears in the window.
6. Go to the 'User media' subtab.



7. Drag the selected user media from the list in the left window and drop them into the right window.
8. The CardLink authorisation properties are displayed.
9. Click the 'OK' button.
   ⇨ The user medium or the selected user media appear in the window.



10. Put a user medium onto the desktop reader and program it.
11. Program the components at the doors with a programmer or wirelessly.

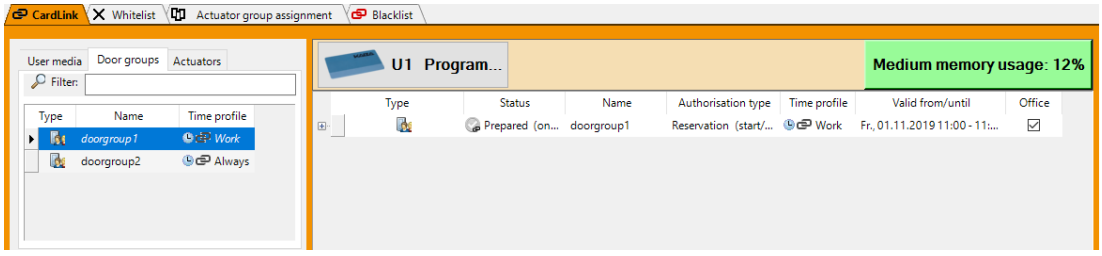


Programming media

Media can also be programmed via the 'Reception' or 'Key plan' menus.

Procedure

1. Open the 'Authorisations' menu from the Navigator toolbar.
2. Navigate to the 'CardLink' tab.
3. Navigate to the 'User media' sub-tab.
4. Drag the properties 'Group right', 'Individual right' or 'Reservation' and drop in the top right-hand window.
5. Place the medium to be programmed on the desktop reader.
6. Click on the 'Programming (media name)...' button.



Program actuators

- LEGIC advant and MIFARE components are programmed with Programmer 1460.

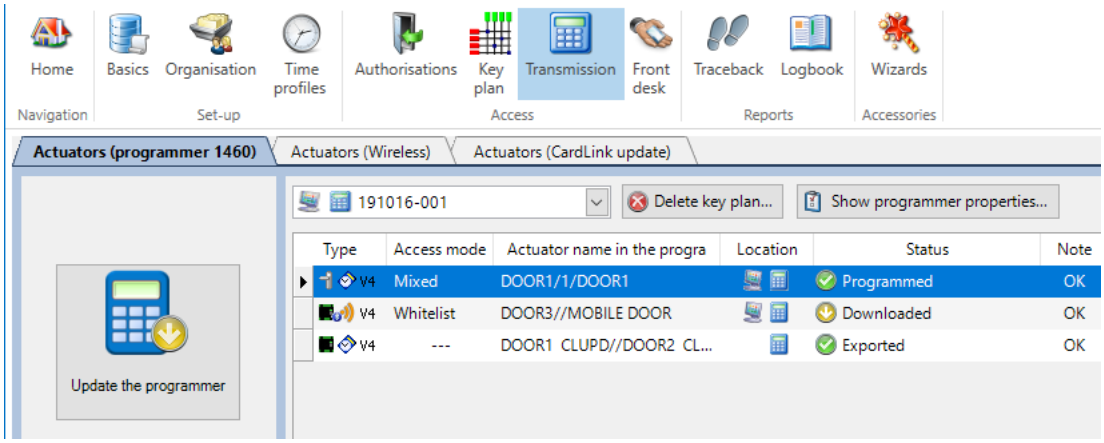
- elolegic and elostar components are programmed with Kaba elo Programmer 13 64.

If project components have different technologies, e.g. LEGIC advant and elolegic or elostar, both programmer types are needed. These are each shown in their own tabs.

Procedure

1. Connect the programmer and the computer with a USB cable.
   ⇨ The programmer appears in the status bar.

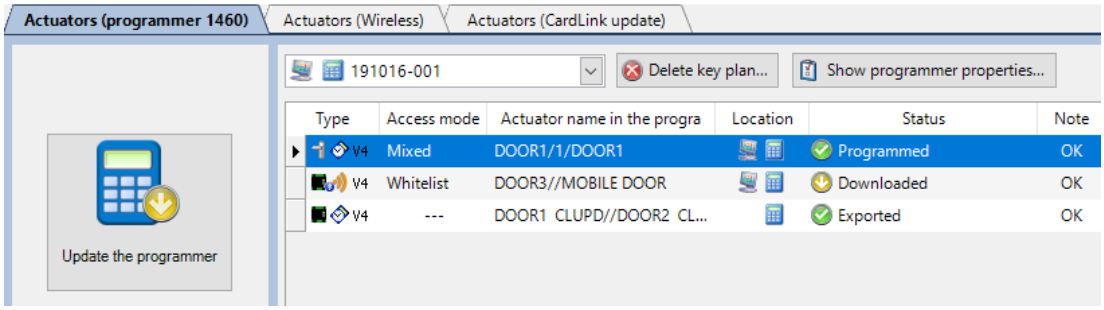
2. In the 'View' toolbar, open the 'Transmission' area.
3. Select the locking plan from the list.
4. Click the 'Update programmer' button.
   ⇨ The data are loaded onto the programmer.



5. Disconnect the programmer from the computer.
6. Transfer the data to the components using the programmer.

Confirm programming

1. Connect the programmer and the computer with a USB cable.
2. In the 'View' toolbar, open the 'Transmission' area.
3. Select the locking plan from the list.



   ⇨ The data are automatically updated. In the 'Status' column, the programmed components are marked with the status "Current".

Do not disconnect the programmer during data transfer: otherwise, data are not transferred or are transferred incompletely.

6.9.3 CardLink update with standalone components

Transferring a large number of data records can take some time.

The CardLink update function is used to update validations and authorisations on user media. This chapter contains information about the standalone version without a wireless gateway. A remote reader 91 15 with extension module 90 43 is used for the standalone version. This is then referred to as a CardLink update reader.

The components must have the following firmware versions or higher:

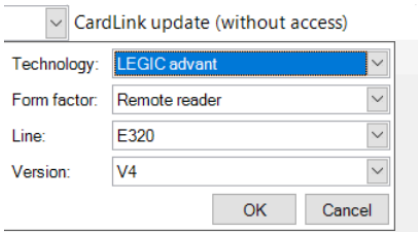
- Programmer 1460: 1.36
- Remote reader 91 15 with extension module 90 43 42.40

Carry out write authorisation when using under LEGIC at remote reader.

Requirements

Settings of a reader used:

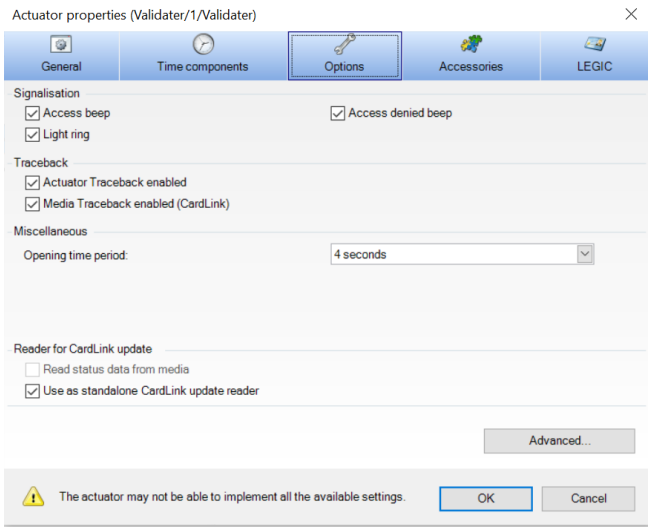
Components/devices used for the CardLink update must have the following parameter settings:



- The actuator type is a remote reader E320, 360 (wireless)
- One of the following access modes is selected in the basic information:
  - CardLink (with update)
  - Mixed (with update)
  - Update

Settings in the remote reader properties

The 'Reader for CardLink update' checkbox is activated: CardLink update data is transferred to the component via programmer 1460.



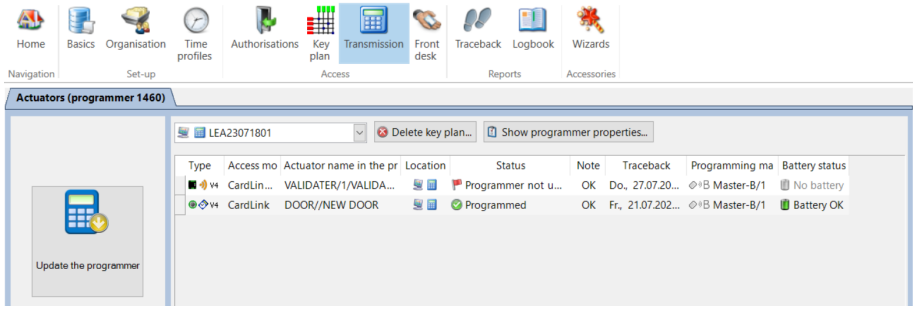
- 'Use as a standalone CardLink update reader' is selected

Updating the data records on the CardLink update reader

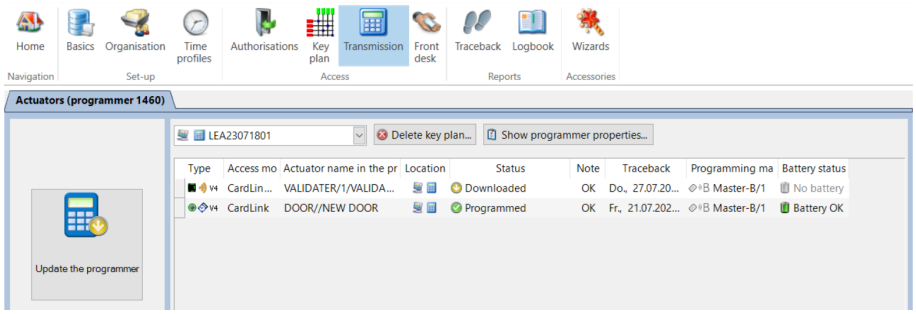
Transferring a large number of data records can take some time.

Procedure

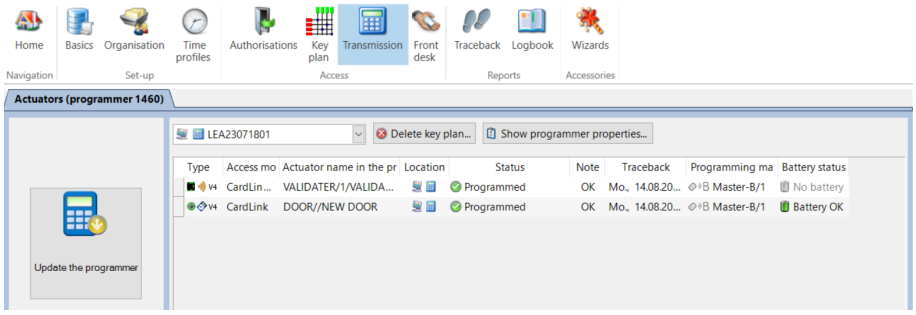
1. Navigate to the 'Transfer' menu.
2. Navigate to the 'Actuators (programmer 1460)' tab.



3. Click the 'Update programmer' button.



4. Take the programmer to the CardLink update reader.
5. Log in to the device using the master.
6. Select 'Update configuration' on the programmer.
   - ⇨ The changed data is uploaded to the component.
   - ⇨ New access rights and validations will be transferred to the medium the next time the relevant medium is presented.
   - ⇨ CardLink update feedback can be transferred to the programmer. For a description, see the section 'Retrieving CardLink update feedback with the programmer'.
7. Connect the programmer to KEM.
8. In the 'Transfer' menu, navigate to the 'Actuators (programmer 1460)' tab.
   - ⇨ Feedback from the update process transferred to the programmer is automatically transferred to KEM.

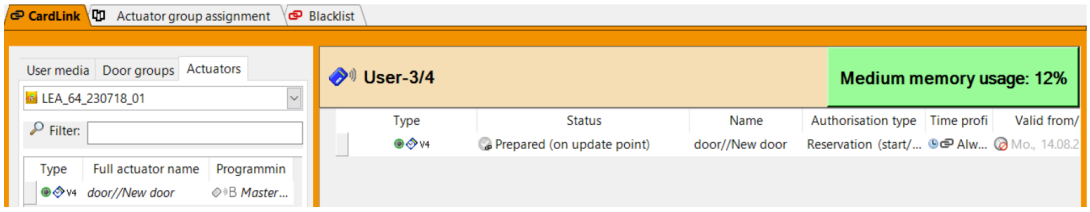


Retrieving CardLink update feedback with the programmer

Feedback concerning whether a user has retrieved their authorisations from the CardLink update reader is transferred to KEM via the programmer. To do this, take the programmer to the CardLink update reader.

Requirements

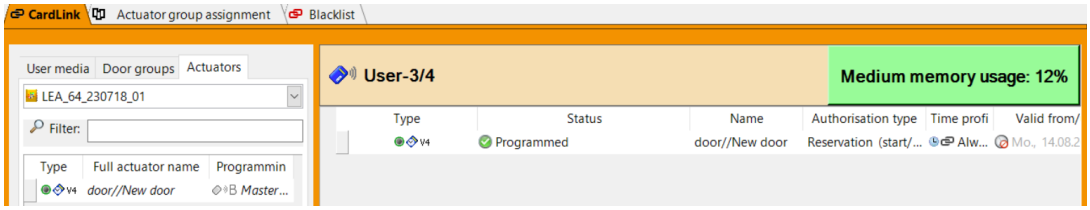
- The user's changed authorisations have been transferred to the CardLink update reader.



- Programmer 1460
- Master medium (for logging in to the component)

Procedure

1. Take the programmer to the CardLink update reader.
2. Log in to the device using the master.
3. On the programmer, select the menu item 'CardLink update' from the 'Read actuator' menu.
   ⇨ Once the data has been read, the programmer reports 'Read successfully'.
4. Connect the programmer to KEM.
5. Navigate to the 'Transfer' menu.
   ⇨ The data is automatically synchronised with KEM.
   ⇨ In 'Authorisations/CardLink', the user media in question is shown as being 'Current' if the assigned authorisations have been retrieved from the CardLink update reader.

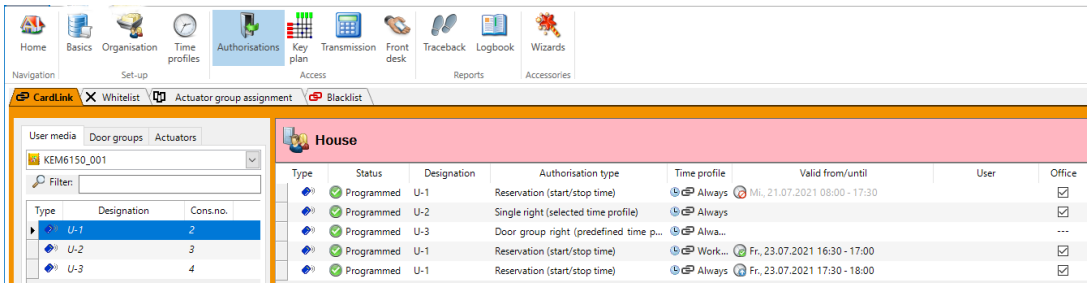


6.9.4 Reservation

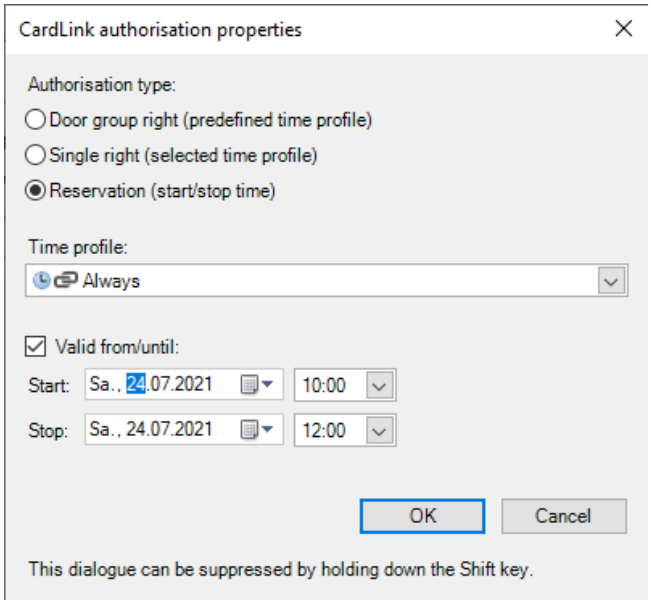
This section describes the assignment of rights for single doors or door groups for one or several periods of time. The function is only available with CardLink.

6.9.4.1 Create

Create single reservation



1. Open the 'Navigator/Authorisations' menu.
2. Select the 'CardLink' tab.
3. Select the medium to be programmed in the 'User media' tab.
4. Drag the selected medium to the right with the mouse and drop it into the bar at the top.
5. Move the door or door group to the right in the lower field to adjust the parameters.

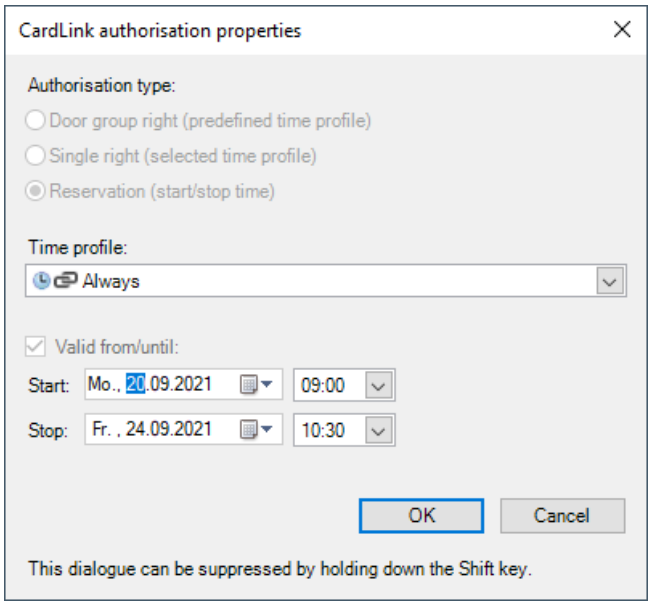


6. Select the reservation settings.
7. Click 'OK'.
   ⇨ The data is prepared and must still be written to the medium.
   ⇨ Repeat the process to create additional reservations.

Limited reservations

If 2 reservations have already been created or expired reservations have not been removed, the following configuration options are available for creating further reservations:

- Select the time profile for the reservation.
- Specify the validity period.



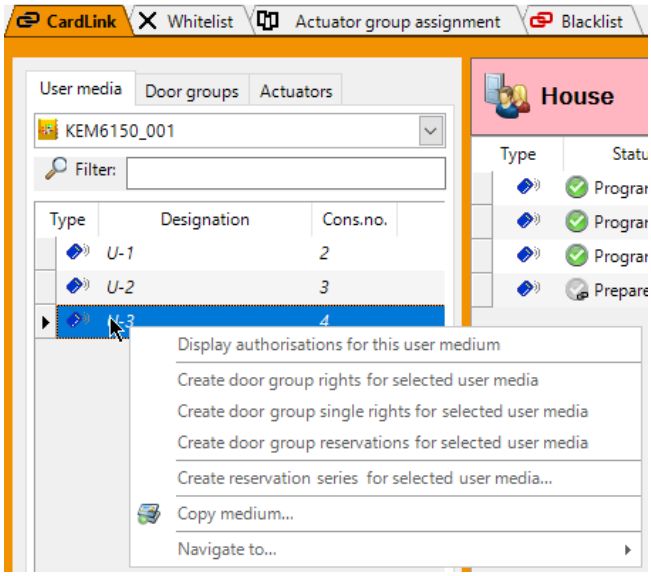
6.9.4.2 Create a reservation series

In the case of recurring events, a series of reservations is created for a medium and the corresponding validity period. The user of the medium therefore receives access to the displayed door or door group for the period at the specified times and days of the week.

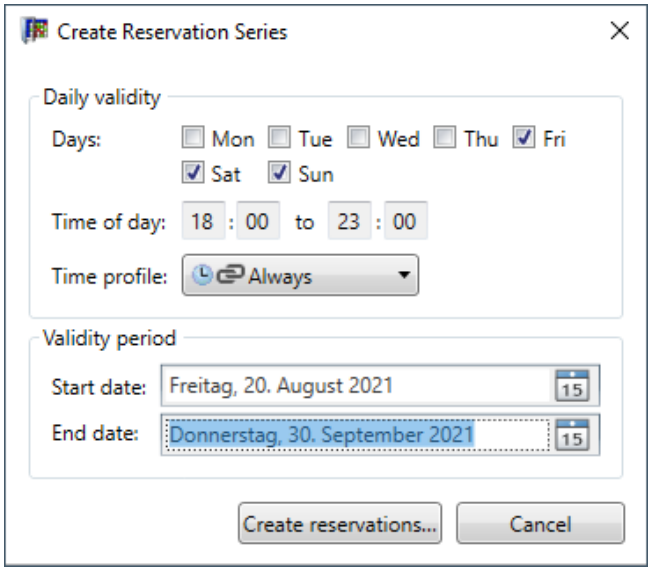
A maximum of 100 reservations can be created, depending on the available space on the medium.

Procedure

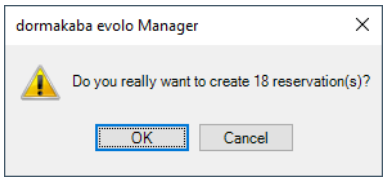
1. Open the 'Navigator/Authorisations' menu.
2. Select the 'CardLink' tab.
3. Select an item in the 'Door groups' or 'Actuators' tab.



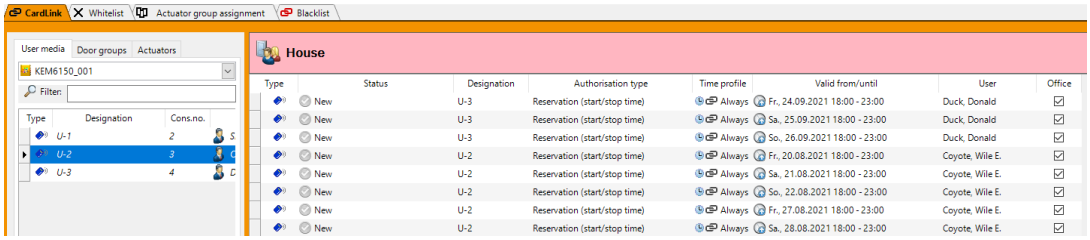
4. Drag the selected element to the right with the mouse and drop it into the bar at the top.
   ⇨ The actuator or door group for the reservation series is selected.
5. In the 'Media' tab, select the medium for which you want to create a reservation series.
6. In the context menu of the medium, select the entry 'Create reservation series'.



7. Select the settings.
8. Click 'Create reservations'.



9. Click 'OK'.
   ⇨ The data is prepared and must still be transferred to the medium.
10. Transfer the data to the medium.
    ⇨ Write the CardLink data to the user medium.
    ⇨ Download the CardLink data to the CardLink update point, e.g. wireless reader or terminal. See section.



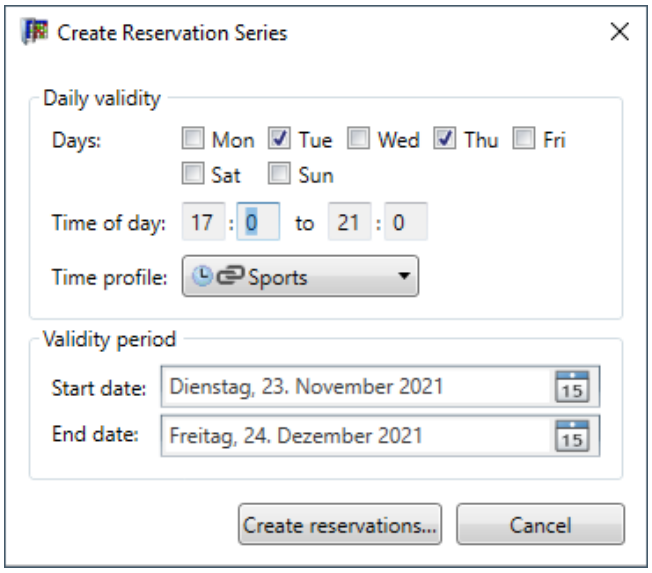
Example:
A sports club has planned fixed training times for its training groups for the winter season in the local sports hall, for which access is required for each of them. Games take place on Saturdays or Sundays.

Training Group	**Training Times**		
Group 1: Gymnastics	Monday 18:00 to 20:00 Changing rooms 1 and 2	Wednesday 18:00 to 20:00 Changing rooms 1 and 2	Friday 18:00 to 20:00 Changing rooms 1 and 2
Group 2: Football	Monday 20:00 to 22:00 Changing rooms 3 and 4	Thursday 20:00 to 22:00 Changing rooms 3 and 4	
Group 3: Hockey	Tuesday 19:00 to 21:00 Changing rooms 1 and 2	Friday 20:00 to 22:00 Changing rooms 3 and 4	
Matches	Saturday 14:00 to 18:00	Sunday 14:00 to 18:00	

Management of the hall access is implemented using CardLink. The administrator creates the required accesses as a series of reservations on the basis of the schedule. Trainers and group participants have media on which the series of reservations are stored. Each training group gets 2 changing rooms assigned to a door group and hall access during their time range.

The matches are managed in a separate group.

For example, in the KEM, for the Group 1 media, the following is entered in the menu for creating a series of reservations:



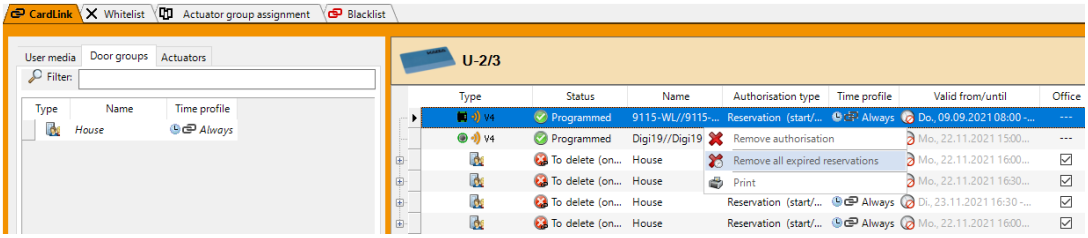
Series of reservations are also created for the other groups.

6.9.4.3 Delete

Procedure for deleting old or expired reservations.

1. Open the 'Navigator/Authorisations' menu.
2. Select the 'CardLink' tab.
3. Select the 'User media' tab.

4. Select the user medium.
5. Drag the selected user medium to the right to the top bar.
6. In the right-hand field, select the reservation/authorisation to be deleted.



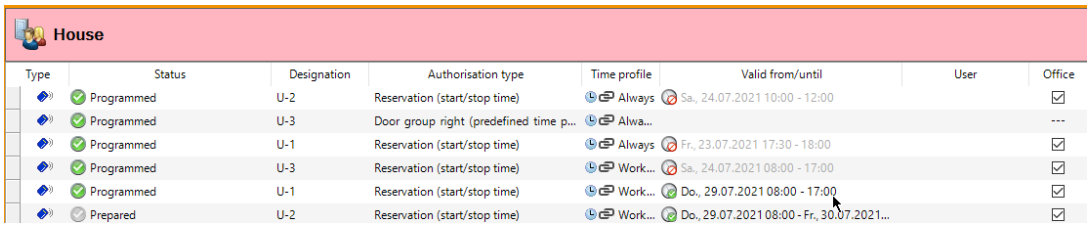
7. In the context menu, select:
   'Remove authorisation'
   'Remove all expired reservations'
   ⇨ The entry is prepared for deletion.
8. Transfer the modification to the medium.
   ⇨ Program the medium with the desktop reader.
   ⇨ Send the data to the CardLink update reader. See section.

6.9.4.4 Adjust

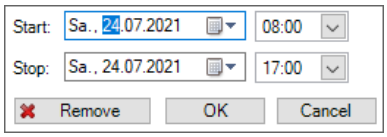
Adjust the validity for a displayed door group in the 'Valid from/to' field.

Procedure

1. Open the 'Navigator/Authorisations' menu.
2. In the 'Door groups' or 'Actuators' tab, select an item to display.



3. In the 'Valid from/to' column, select the entry to be adjusted.



4. Adjust the data of the selected entry.
5. Click 'OK' to confirm the adjustments.
   Click 'Remove' to remove the entry.
   ⇨ The data is prepared and must still be transferred to the medium.

6.9.5 Mixed mode

In mixed mode, CardLink or whitelist authorisations are saved on a medium. If the medium is held up to a component configured in mixed mode, the component first checks for a whitelist authorisation. If no authorisation is found, the component checks for a CardLink authorisation. The component opens if the medium is authorised in one of these authorisation types.

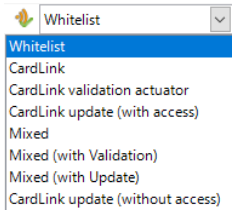
If the medium is found in both authorisation types but classified as "not authorised" in one of the authorisation types, the medium is denied.

Example: The component will not open if the medium has a valid CardLink authorisation but there is also a whitelist authorisation for the medium with a time profile that is outside of the validity period.

Set up

Mixed mode via wireless is not yet supported by the wireless gateway.

Mixed mode is selected under the 'Actuators' tab in the 'Basics' menu for access mode.



6.9.6 Copy authorisations from media and components

Media or components can be copied with their authorisations using this function.
The following is possible:

- Copying within the locking plan of a project.
- Copying to other locking plans of a project.
- Copying to one or more media.
- Copying to one or more components.

Prerequisites

- Media and components from a project can be copied with whitelist or CardLink.

- All authorisations from whitelist and/or CardLink are copied.

Copy media
Copy media by using the 'Wizards' button, or the 'Copy medium' function in the 'Authorisations' area. Select a medium as a reference and copy it to one or more target media.

The modified components must be updated with the programmer or wirelessly. Media with a CardLink authorisation must be updated with a desktop reader or a terminal.
PIN or door codes can only be copied to or from existing readers or antennas.

Procedure

1. In the 'View' toolbar, open the 'Wizards' area.
2. Click the 'Copy medium' button.
3. Follow the wizard.
4. After copying, click the 'Close' button.

Copy components
The components can be copied with the 'Wizards' button or from the authorisations using the context menu 'Copy actuator'. PIN-code readers or antennas can only be copied from other PIN-code readers or antennas.

The modified components must be updated with the programmer or wirelessly. Media with a CardLink authorisation must be updated with a desktop reader or a terminal.

1. In the 'View' toolbar, open the 'Wizards' area.
2. Click the 'Copy actuator' button.
3. Follow the wizard.
4. After copying, click the 'Close' button.

viber

6.10 Transfer

Transfer involves the exchange of data between the KEM software, the programmer and/or the gateway (GW) for the wireless option with the components.

Alongside the Type, Designation, User etc. fields, the 'Path' field can also be activated. The current path of a key plan, including sub-folders, is displayed under 'Path'. The path can be sorted.

Wireless
Components with the wireless option are shown as inactive in the 'Actuators (wireless)' tab as long as the commissioning of these components (connected to the GW) [▶ 11.3] has not yet been completed. The components must be programmed once with programmer 1460 prior to commissioning the wireless option. After wireless commissioning and transferring data from programmer 1460 to the software, the components automatically appear as active in the 'Actuators (wireless)' tab. In this tab, you can query various properties, load traceback and update the parameter setting. The component then no longer needs to be searched with the programmer.

Standalone

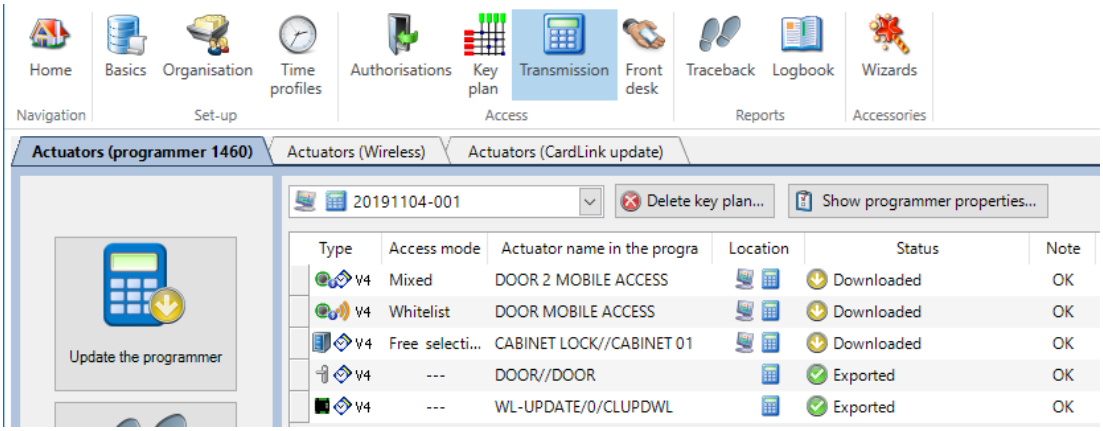
Programmer 1460

LEGIC advant and MIFARE components are programmed with Programmer 1460.

1. Connect the programmer to the computer using a USB cable.
2. Select the locking plan from the list.
3. Click the 'Update programmer' button.

⇨ The data are loaded onto the programmer.

All commands are in reference to the selected locking plan.



Update the programmer	The current data of the components are loaded onto the programmer.
Update traceback	The current traceback data are loaded by the programmer into the KEM software.
Delete all files	All component data are deleted on the programmer.

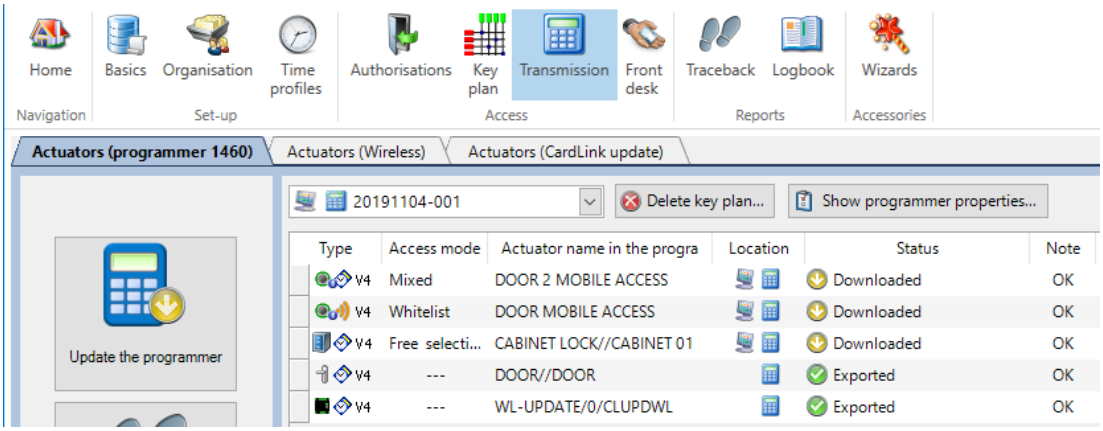
Do not disconnect the programmer during data transfer: otherwise, data are not transferred or are transferred incompletely.

Programmer 1364

The Kaba elolegic and Kaba elostar components are programmed with Kaba elo Programmer 1364.

1. Connect the programmer 1364 to the computer using a USB cable.
   ⇨ The programmer appears in the status bar.
2. Select the locking plan from the list.
3. Click the 'Update programmer' button.

⇨ The data are loaded onto the programmer.



Update the programmer 1364	The current component data are loaded onto the programmer 1364.
Load status of all actuators	The status of all components is loaded onto the programmer 1364.

Update traceback	The current traceback data are loaded from the programmer 1364 onto the KEM software.

Do not disconnect the programmer during data transfer: otherwise, data are not transferred or are transferred incompletely.

6.10.1 Data fault

If 'Data error' is displayed in the "Status" field, the component entry must be revised.
To display a more specific error description, place the mouse cursor over the term 'Data error'. Wait until the error description is displayed in the tooltip.

The following table shows the possible error descriptions.

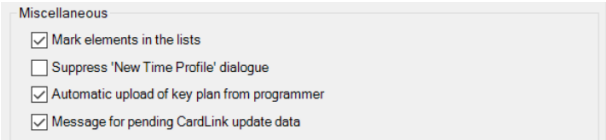
Error mes-sage	Description	Solution
Data error	The actuator has not yet been assigned a programming master.	Assign a master to the component or read a master into the project and assign it to the component.
	The assigned programming master does not have a valid UID.	Check the UID of the programming master.
	The access mode has not yet been set.	Assign the access mode.
	TimePro has not yet been assigned a time profile.	Create and/or assign a time profile.
	The time profile used by TimePro is incorrect.	Check and correct the time profile.
	One of the time profiles used is incorrect.	Check and correct the time profile.
	One of the user media used has an incorrect UID.	Check UID of the user media.
	One of the user media used has an incorrect CID.	Check CID of the user media.
	No Master B has been assigned yet for an authorization.	Assign a Master B to the component or read a Master B into the project and assign it to the component.
	One of the Master Bs used has an incorrect UID.	Check/add UID of the Master B used.
	The 'Active LEGIC advant Technologies' selection in the project properties has been set to 'Manual'. For this actuator, however, there are user media authorized that do not support the desired technology.	Check technology selection/project properties. Check user media and authorizations.

After correcting the error, 'Data error' no longer appears.

6.11 CardLink update data

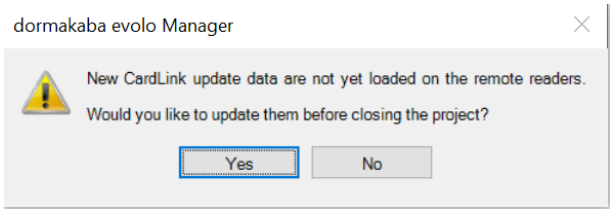
If CardLink update data has not yet been transferred, the user is informed of this when closing a project and can decide whether they now want to carry out the update.

Requirements



- The option 'Message for pending CardLink update data' is switched on (default).
- A remote reader with the CardLink update function is available.
- New update data for the remote reader has not yet been transferred.

Behaviour



- The dialogue window opens if CardLink update data has not yet been transferred.
- Click 'Yes' to transfer this data before closing the project. The user is directed to the 'Transfer' menu and can transfer the data.
- Click 'No' to close the project without transferring the data.

6.12 Traceback

The traceback function makes it possible to track activities. The traceback data can be transferred from the user medium or the component to the system software to be displayed.

You have the following options available:

- Transfer traceback data from the component.
- Transfer traceback data from the medium.
- Receive traceback data wirelessly.
- Transfer traceback data from the Access Manager
- Transfer traceback data from the terminal

After selecting the method, proceed as follows:

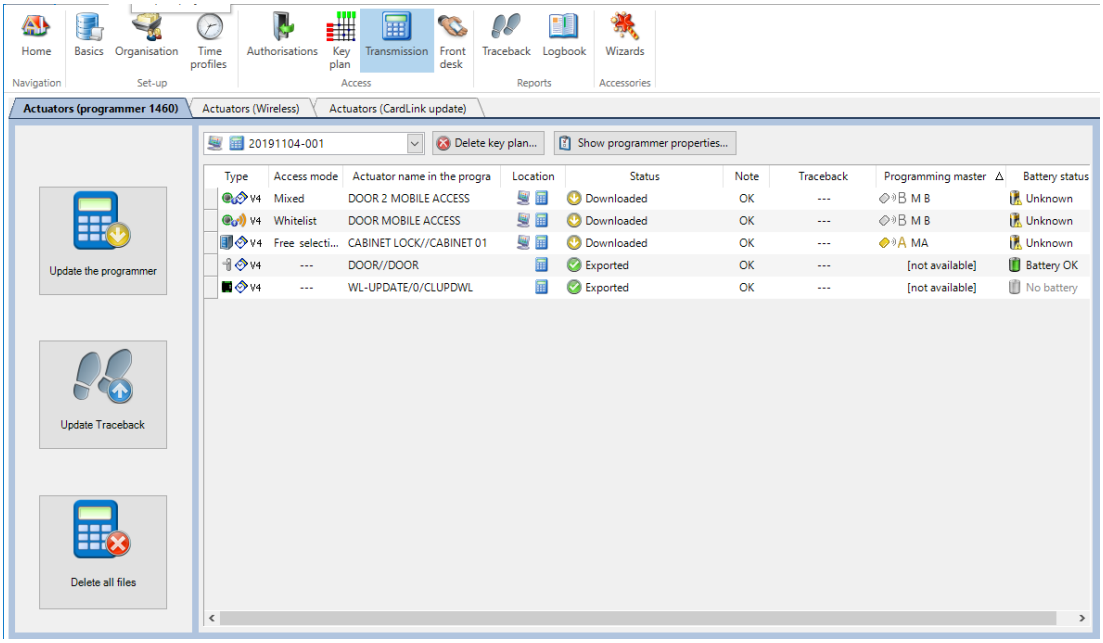
Transfer traceback data from the component

The traceback data is stored in the component's memory. When needed, the data is read using the programmer and transferred to the system software.

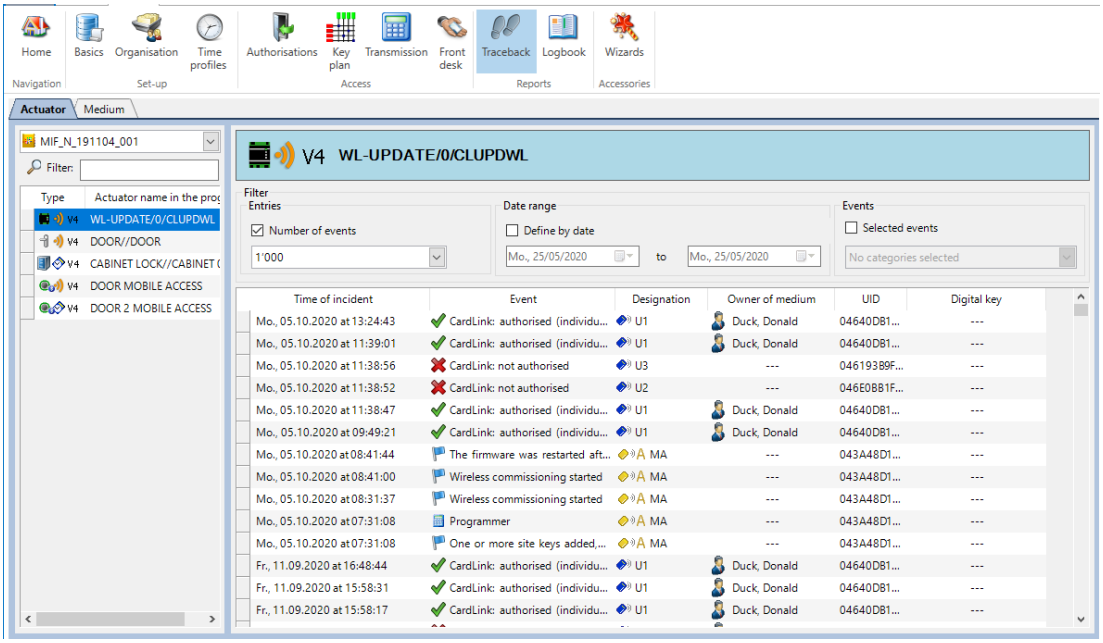
Requirement: The component's traceback data have been read out with the programmer.

Procedure

1. Connect the programmer to the computer using a USB cable.
2. In the 'View' toolbar, click on the 'Transfer' button.
3. Select the key plan from the list.
4. Click on the 'Update traceback' button.
   ⇨ The data are loaded by the programmer into the system software.



5. In the 'View' toolbar, click on the 'Traceback' button.
6. Go to the 'Actuator' tab.
7. If the key plan is not selected, select a key plan.
8. On the list, select the component by double-clicking on it. Alternatively, drag the list item and drop it into the bar at the top right.

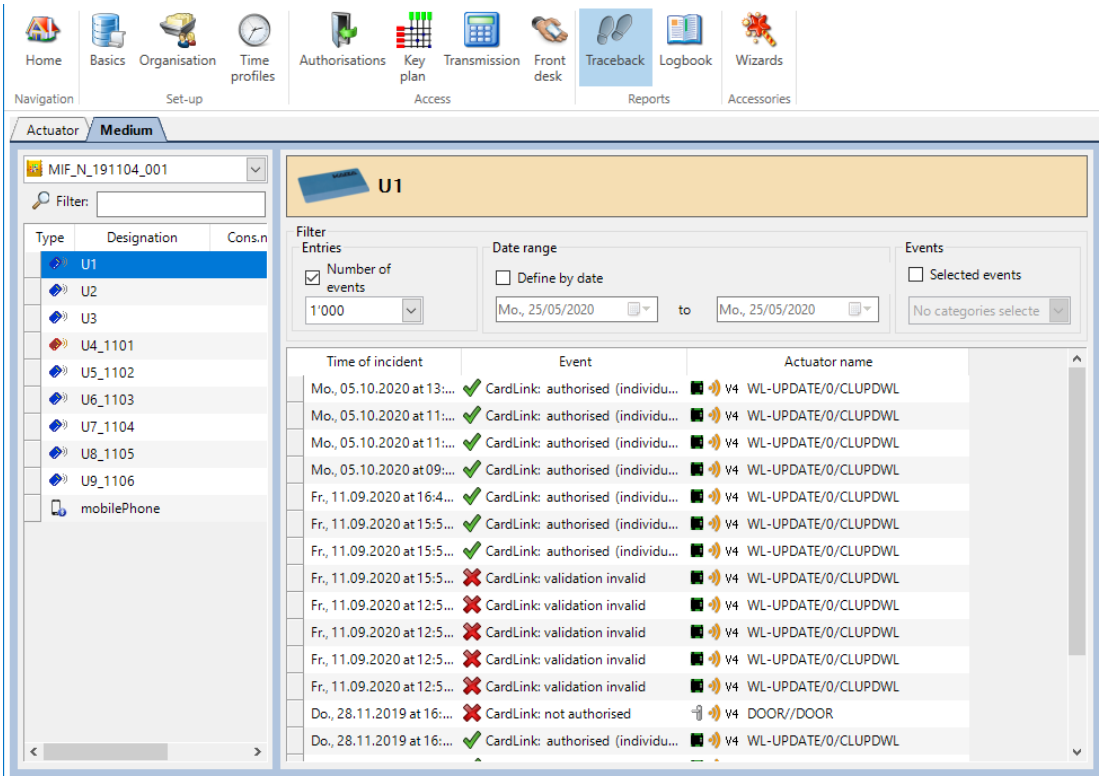


Transfer traceback data from the medium

The component writes the traceback data on the medium presented to it. These traceback data can be transferred to the system software using the desktop reader. This function can be activated in the project properties.

Procedure

1. In the 'View' toolbar, click on the 'Traceback' button.
2. Go to the 'Medium' tab.
3. Place the medium on the desktop reader.
4. Click on the 'Read in (media name) traceback...' button.



Receive traceback data wirelessly

Traceback data of components that are connected wirelessly can be received using the wireless gateway.

Procedure:

1. In the 'Transfer' menu, select the components for transfer.
2. Click on 'Load traceback'.
   - ⇨ The query is sent to the gateway and transferred to the components.
   - ⇨ The data are transferred from the components to KEM via the gateway.
   - ⇨ If the current time stamp of the query appears under "Traceback status", the transfer is completed.

Table of traceback codes

The following table explains the meaning of the read-out traceback data.

#	Traceback codes Event	Clarification/rectification
01	Access granted	The presented medium is authorised.
02	Access denied (no authorisation)	The presented medium has no authorisation.
03	Access denied (incorrect time)	The medium was presented outside of the time window.
04	Access granted (emergency power supply)	Replace batteries. See Service section in the component manual.
05	Master A/B	Start manual programming (keys)
06	Programmer	Start programmer access
07	Clock set	The clock has been set. A correctly set clock ensures the correct function of time-bound functions of the component.
08	Mode module (external)	(elolegic)
09	Open TimePro Office	
0A	Close TimePro Office	
0B	Access denied (incorrect TwinTime)	(elolegic)
0C	Access denied (incorrect SPC)	(elolegic)

#	Traceback codes Event	Clarification/rectification
0D	Does not couple with digital cylinder	(elolegic) Check mechatronic unit and electronics.
0E	Access denied (TwinTime error)	(elolegic)
0F	Close open mode	(only for remote reader and compact reader)
10	The firmware was restarted after successfully modifying actuator configuration	
11	Access granted (visitor authorisation)	(elolegic)
12	Locking module fault	Could not be closed.
13	Locking module fault rectified	Closing attempt was successful.
14	Coupling position warning	only for digital cylinder
15	Coupling position correct	only for digital cylinder
16	No configuration after FW update	The configuration has been lost and must be retransferred.
19	Open TimePro Day/Night	The component opens at the set time.
1A	Close TimePro Day/Night or Office (time expired)	The component closes at the set time.
1B	Open pass mode	The component is opened via pass mode.
1C	Close pass mode	The component is closed via pass mode.
20	One or more site keys have been added, changed or deleted.	
21	Not all site keys could be read out from the master.	
22	Access denied (no mobile authorisation)	(elolegic) The component is not configured for Mobile Access. Check: • Requirements for Mobile Access
23	Access denied (incorrect time)	(elolegic)
2B	Access denied (incorrect TwinTime)	(elolegic)
30	Launched	only LEGIC advant/prime: The component has been granted write authorisation with the security card C2.
31	Decommissioned	only LEGIC advant/prime: The write authorisation has been withdrawn from the component with the security card C2. The write authorisation must be re-granted e.g. after an INI reset.
32	Access denied (incorrect time)	(elolegic)
33	Access denied (incorrect time)	(elolegic)
35	VCP ok.	Successful VCP configuration of components. VCPs contain the cryptographic key for Mobile Access.
36	VCP error: general error	
37	VCP error: incorrect password	Check password.
38	VCP error: incorrect custom data format	Incorrect length, formatting.
39	VCP error: keystore full	All 128 memory cells for virtual keys are occupied.
3A	VCP error: incorrect KeySet project ID	KeySet project ID does not match the project ID from the database.
3B	Access rejected VCP error: incorrect VCP key	(elolegic) incorrect time in TwinTime (evolo) VCP from another Legic Connect company
3D	VCP error: admin is already set	
3E	VCP error: no admin set	

#	Traceback codes Event	Clarification/rectification
3F	VCP error: incorrect LEGIC chip ID	
40	S-Module (Start open mode)	The component has been opened with the S-Module.
41	S-Module (Start closed mode)	The component has been closed with the S-Module.
42	S-Module (Start 'Any medium' mode)	
43	S-Module (Start standard mode)	The S-Module is out of operation. The component works normal again.
44	S-Module (power failure end)	(elolegic)
45	S-Module (no access because in closed mode)	The component is closed via the S-Module. The medium is not authorised.
46	S-Module (Access granted)	
47	S-Module (Start mode: Authorised medium)	
48	S-Module (Switch off Start TimePro)	
50	Modification successfully executed	
56	Modification failed (whitelist full)	(elolegic) Whitelist: The maximum number of users for the whitelist operation of this component has been reached.
57	Modification failed (blacklist full)	CardLink: The maximum number of entries on the blacklist of the component has been reached.
58	Modification failed (general error)	
59	Validation update successful	The medium validation was successful.
5A	Validation update failed (unauthorised)	
5B	Validation update failed (incorrect time)	
5C	Validation update failed (validation expired)	
5D	CardLink update completed	
5E	CardLink update failed	The CardLink data could not be saved in the component.
60	CardLink: not authorised	
61	CardLink: validation invalid	
62	CardLink: incorrect administration area	
63	CardLink: incorrect time	
64	CardLink: error in validation update	(elolegic)
65	Blocked medium, validation deleted	CardLink: blacklisted medium in the validation actuator: header deleted
6A	CardLink: authorised (individual right)	
6B	CardLink: authorised (door group right)	
6C	CardLink: authorised (reservation)	
6D	Access denied (incorrect HW)	not authorised, incorrect connection
6E	Access rejected	not authorised, file faulty
70	Access granted (manually opened)	(elolegic) Lockerlock/CabinetLock: manually opened (without medium, UID=0)
71	Access granted (with administration medium)	Locker lock/CabinetLock: open/close with maintenance medium
72	Maximum occupancy time exceeded	(elolegic) Lockerlock: maximum occupancy time exceeded
73	No free locker selection segment or no place	Locker lock/CabinetLock: file/segment not present or no space free

#	Traceback codes Event	Clarification/rectification
74	Locking error (CabinetLock)	Cabinet lock: blocking unit activation switch
75	Alarm triggered (CabinetLock)	Cabinet lock: alarm triggered
76	Manual locking without medium (CabinetLock)	Cabinet lock: manually locked without medium
80	RCID: Access granted	
81	RCID: not authorised	
82	RCID: validation invalid	
83	RCID: incorrect time	
85	RCID: medium on blacklist	
8A	Wireless commissioning started	The component tries to connect to a wireless gateway on which wireless commissioning is enabled.
8B	Wireless commissioning successful	The component could successfully connect to a wireless gateway on which wireless commissioning is enabled.
8C	Wireless commissioning failed	The component could not connect to a wireless gateway. Check: • The component is configured for wireless operation. • Wireless commissioning on the gateway has started. • The wireless gateway for the commissioning is in range.
8D	Wireless disconnected	
90	Pass-Lock activated	Anti-terror: panic mode activated
91	Pass-Lock deactivated	Anti-terror: panic mode deactivated
95	Escape return activated	The door can be opened from outside without using any medium. Click on the door button to close or to switch mode
96	Escape return: closing with button	The door can only be opened from outside using a valid medium. Click on the door button to open or to switch mode.
97	Closing authorised	
98	Always open authorised	
9A	Remote access: opened	
9B	Remote access: access control	
9C	Remote access: blocked	
9D	Remote access: normal operation	
9E	Remote access: opened once	
9F	Access denied (blocked)	Remote unauthorised because in 'Shutdown' mode
B0	Door broken open	Door broken open (door status monitoring)
BB	Access denied (incorrect TwinTime)	(elolegic)
C2	Access denied (incorrect SPC)	(elolegic)
C3	Access denied (incorrect SPC)	(elolegic)
C4	Licence update from SL1 to SL2	Configuration through upgrade medium.
C5	Licence update from SL1 to SL3	Configuration through upgrade medium.
C6	Licence update from SL2 to SL3	Configuration through upgrade medium.

#	Traceback codes Event	Clarification/rectification
C7	Licence update from SL4 to SL3	Configuration through upgrade medium.
C8	Licence update on Bluetooth	Bluetooth configuration through upgrade medium.
D0	Battery change (triggered by special medium)	
D1	Battery change (triggered by programmer 1460)	
D2	Battery change (automatically detected)	
D3	Battery change (triggered by wireless gateway)	
D5	Switch off optimised low battery detection	
D6	Activate optimised low battery detection	
D7	Deactivate optimised low battery detection	
E2	Access denied (segment reading error)	(elolegic) Medium defect. Replace the medium.
E3	Access denied (segment reading error)	(elolegic) Medium defect. Replace the medium.
EB	Access denied (segment reading error)	(elolegic) Medium defect. Replace the medium.
F0	Access denied (medium on the blacklist)	CardLink/AoC/OSS/MobileLink: Media listed on the blacklist are invalid.
F2	Access denied (medium on the blacklist)	(elolegic) Media listed on the blacklist are invalid.
F3	Access denied (medium on the blacklist)	(elolegic) Media listed on the blacklist are invalid.
FB	Access denied (medium on the blacklist)	(elolegic) Media listed on the blacklist are invalid.
FF	Access granted (group authorisation)	(elolegic)
100	Traceback requested wirelessly	The connected gateway has requested the traceback data for the component wirelessly.

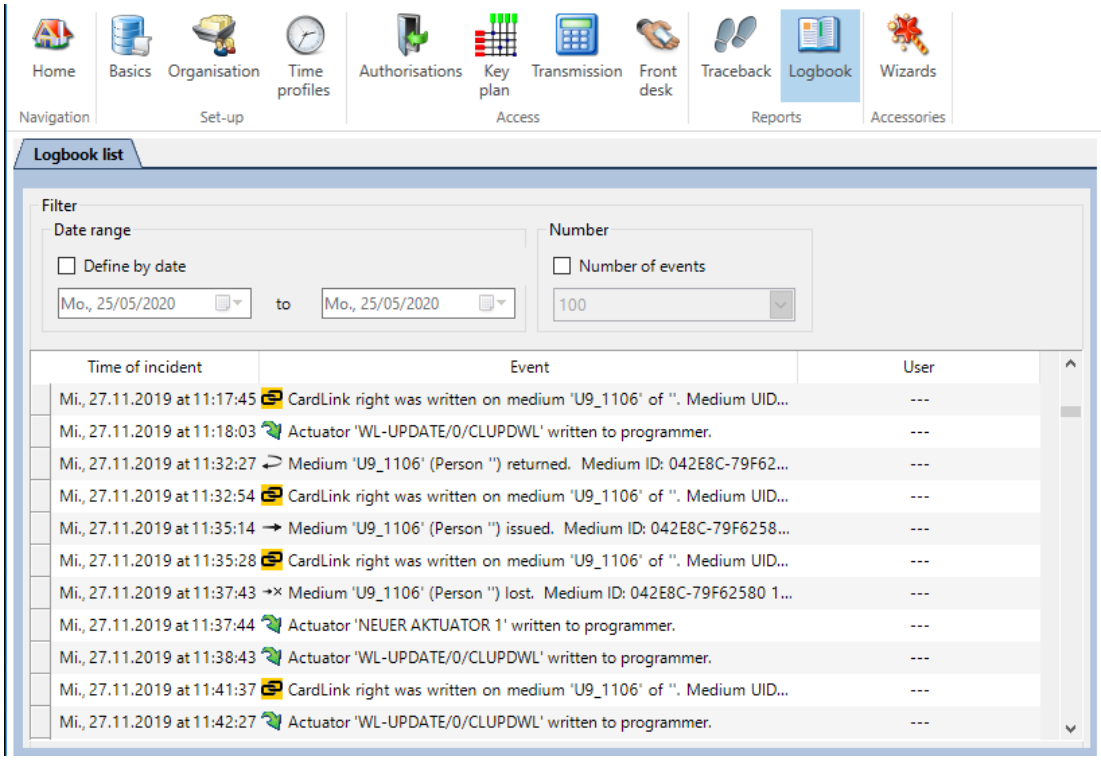
6.13 Logbook

6.13.1 Logbook list

The logbook function of the system software registers time and user for the following events:

- A project has been
  - Opened
  - Closed
  - Exported
  - Imported
- A download or upload of data from the programmer has taken place.
- A download or upload of data from the component has taken place.
- Media have been
  - Issued
  - Returned
  - Registered as lost
- Traceback data have been read.

The logbook list view can be restricted by activating filters.


Home
Basics
Organisation
Time profiles
Authorisations
Key plan
Transmission
Front desk
Traceback
Logbook
Wizards
Navigation
Set-up
Access
Reports
Accessories
Logbook list
Filter
Date range
Define by date
Mo., 25/05/2020
to
Mo., 25/05/2020
Number
Number of events
100
Time of incident
Event
User
Mi., 27.11.2019 at 11:17:45 CardLink right was written on medium 'U9_1106' of ''. Medium UID... ---
Mi., 27.11.2019 at 11:18:03 Actuator 'WL-UPDATE/0/CLUPDWL' written to programmer. ---
Mi., 27.11.2019 at 11:32:27 Medium 'U9_1106' (Person '') returned. Medium ID: 042E8C-79F62... ---
Mi., 27.11.2019 at 11:32:54 CardLink right was written on medium 'U9_1106' of ''. Medium UID... ---
Mi., 27.11.2019 at 11:35:14 Medium 'U9_1106' (Person '') issued. Medium ID: 042E8C-79F6258... ---
Mi., 27.11.2019 at 11:35:28 CardLink right was written on medium 'U9_1106' of ''. Medium UID... ---
Mi., 27.11.2019 at 11:37:43 Medium 'U9_1106' (Person '') lost. Medium ID: 042E8C-79F62580 1... ---
Mi., 27.11.2019 at 11:37:44 Actuator 'NEUER AKTUATOR 1' written to programmer. ---
Mi., 27.11.2019 at 11:38:43 Actuator 'WL-UPDATE/0/CLUPDWL' written to programmer. ---
Mi., 27.11.2019 at 11:41:37 CardLink right was written on medium 'U9_1106' of ''. Medium UID... ---
Mi., 27.11.2019 at 11:42:27 Actuator 'WL-UPDATE/0/CLUPDWL' written to programmer. ---

6.13.2 Protocol list

Activating the protocol list can generate large amounts of data.

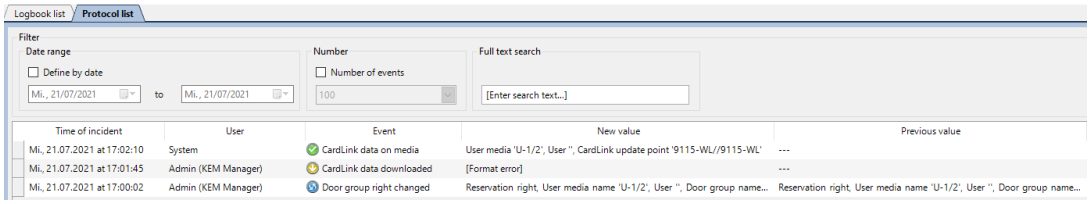
The time of and user who made authorisation-relevant modifications are recorded in the protocol list.

To activate or deactivate the protocol list, see section [▶ 6.2.2.1].

The following data is recorded:

- Time of the action
- Registered user
- Type of event
- The values before the modification
- The values after the modification

The protocol list view is restricted by activating filters.



The list can only be printed out after it has been exported to an external program.

The corresponding rights are required to execute the export functions.

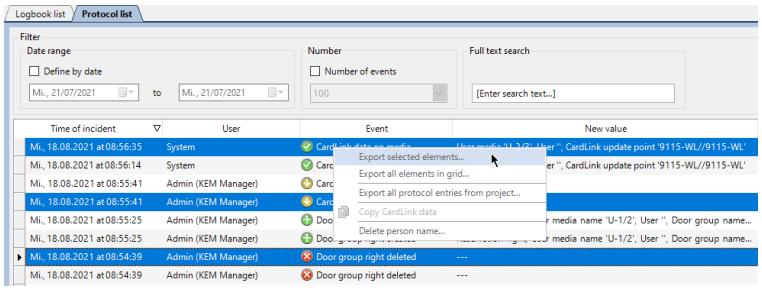
- The registered user needs to have the right to export data.

Additional functions are available via the context menu:

- Export selected entries. See section [▶ 6.13.2.1]
- Export all entries in the protocol list. See section [▶ 6.13.2.2]
- Export all protocol entries of the project. See section [▶ 6.13.2.3]
- Copy CardLink data to the clipboard. See section [▶ 6.13.2.4]
- Delete personal name. See section [▶ 6.13.2.5]

6.13.2.1 Export selected entries in the protocol list

The function exports selected entries to a CSV file.



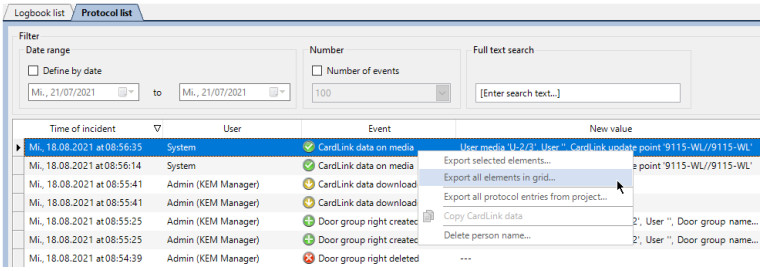
Procedure

1. Select the desired entries.
2. If several entries are selected, right-click on one of the entries to open the context menu.
3. Select the entry 'Export selected entries'.
4. Select the storage location and assign the file name.

5. Click 'Save'.
   ⇨ The selected entries are saved.

6.13.2.2 Export all entries in the protocol list

The function exports all entries of the protocol list displayed in the KEM to a CSV file.

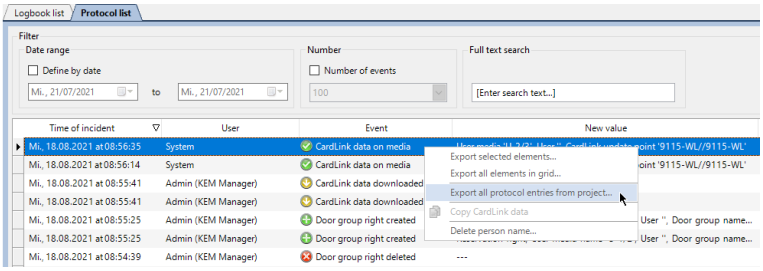


Procedure:

1. Open the context menu using the right mouse button.
2. Select the entry 'Export all elements in grid'.
3. Select the storage location and assign the file name.
4. Click 'Save'.
   ⇨ The entries are saved.

6.13.2.3 Export all protocol entries of the project

The function exports all entries in the project protocol list to a CSV file. Entries that are not displayed in the KEM are also exported.



Procedure:

1. Right-click on one of the entries to open the context menu.
2. Select the entry 'Export all protocol entries of the project'.
3. Select the storage location and file name.
4. Click 'Save'.
   ⇨ The entries are stored in a CSV file.

6.13.2.4 Copy CardLink data to the clipboard

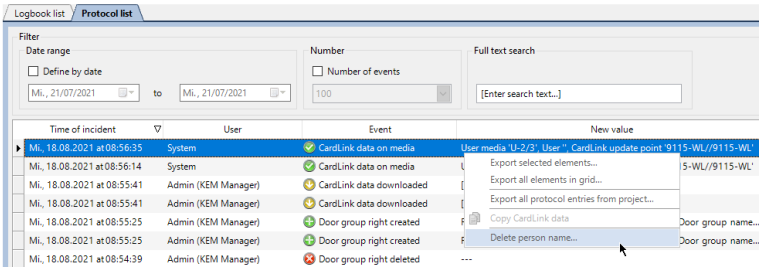
The function copies the CardLink data of the selected entry to the clipboard if CardLink data exists for the entry.

The function is used in cooperation with Support, for example, to analyse CardLink data of a user medium.

6.13.2.5 Delete personal name

The registered user needs to have the right to delete personal names.

The wizard deletes the name of a person from the protocol list. See section [▶ 17.1]. 'Name deleted' is displayed instead of the user name.



7 Mobile Access

Setting up of components and media for Mobile Access in KEM.

NOTICE

The existing digital key of evolo smart is overwritten in the Mobile Access app.

Authorisations of the evolo smart system are lost.

A digital key of a KEM system overwrites a digital key of an evolo smart system saved in the Mobile Access app. The authorisations of evolo smart are lost as a result of this. The user is then authorised in the KEM system but not in evolo smart.

- Users of the Mobile Access app, who already have a digital key from evolo smart or another KEM system, do not need any new key, rather they can use the existing key in KEM.
- The users send the existing digital key to the KEM administrator.

⇨ The authorisations for evolo smart are retained.

⇨ The user is also authorised in KEM.

Only the additional steps and options required for setting up the Mobile Access in KEM are described in this section.
Mobile Access only works with components that support it.

7.1 Requirements

For the project:

- V4
- Whitelist or CardLink and whitelist

For the components:
These components support Mobile Access:

- c-lever pro
- c-lever air
- c-lever compact
- digital cylinder
- Compact reader
- Remote reader

The components must meet the following requirements:

- Minimum SL2. More information about SL can be found in the evolo system description.
- Line E300, E320 or E321 for firmware version 42.32 or higher (only for NFC)
- Line E340, E360 or E361 (for NFC and Bluetooth).
- The operation is only possible with whitelist or in the mixed mode (authorisations in the whitelist). CardLink is not supported.

For management:

- A smartphone with an Android or iOS operating system is available.
- The VCP Installer app is installed on the smartphone.
- Mobile Access is possible on the respective components.
- Digital keys are available.

For the user:

- A smartphone with an Android or iOS operating system is available.
  - Android: Bluetooth and/or NFC

  - iOS: Bluetooth
- The dormakaba mobile access app is installed on the smartphone.

7.2 Setting up smartphone in KEM as a medium

NOTICE

The existing digital key of evolo smart is overwritten in the Mobile Access app.

Authorisations of the evolo smart system are lost.

A digital key of a KEM system overwrites a digital key of an evolo smart system saved in the Mobile Access app. The authorisations of evolo smart are lost as a result of this. The user is then authorised in the KEM system but not in evolo smart.

- Users of the Mobile Access app, who already have a digital key from evolo smart or another KEM system, do not need any new key, rather they can use the existing key in KEM.
- The users send the existing digital key to the KEM administrator.

⇨ The authorisations for evolo smart are retained.

⇨ The user is also authorised in KEM.

Only whitelist authorisations are supported. CardLink is not possible.

Users and authorisations can be assigned after setting up the smartphone as a medium.

Requirements

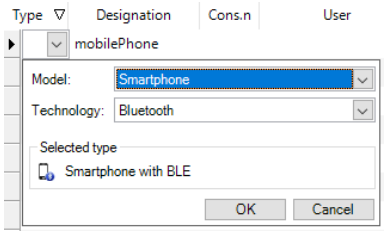
- A smartphone is available.
- A digital key is available.

The digital key consists of 20 hexadecimal characters and is shown on the DIGITAL KEY VOUCHER under Mobile ID (1).

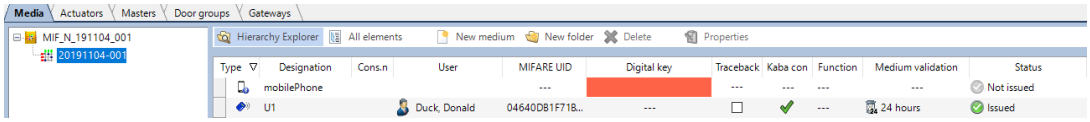
Example:

Procedure

1. Select the 'Media' tab under 'Basics'.
2. Create a new medium.



3. Select 'Smartphone' as a media type.
4. Select the Bluetooth and/or NFC technology as per the options on the smartphone.



5. Insert the digital key.
   ⇨ For information on importing digital keys, see.

⇨ Assign Mobile Access function to the smartphone as a medium of a component.

7.3 Importing digital keys

NOTICE

The existing digital key of evolo smart is overwritten in the Mobile Access app.

Authorisations of the evolo smart system are lost.

A digital key of a KEM system overwrites a digital key of an evolo smart system saved in the Mobile Access app. The authorisations of evolo smart are lost as a result of this. The user is then authorised in the KEM system but not in evolo smart.

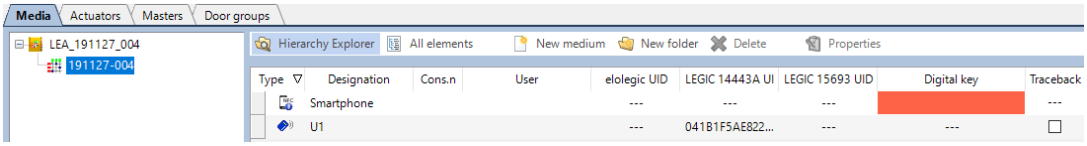
- Users of the Mobile Access app, who already have a digital key from evolo smart or another KEM system, do not need any new key, rather they can use the existing key in KEM.
- The users send the existing digital key to the KEM administrator.

⇨ The authorisations for evolo smart are retained.

⇨ The user is also authorised in KEM.

Digital keys are entered in the KEM in different ways:

- Manual entry
- Copy and paste
- In a media list.
- Import from one or more voucher PDF files.



7.3.1 Manual entry

The digital key is provided electronically as text in an email or in a PDF.

Enter using the keypad

Requirements

- The 'Basics/media' page is open.
- A smartphone is created as a user medium.

Procedure

1. From the list, select the smartphone to which the key should be added.
2. Enter the digital key for the selected smartphone in the 'Digital key' field using the keypad.

Enter by copying and pasting

Requirements

- The 'Basics/media' page is open in KEM.
- A smartphone is created as a user medium.

Procedure

1. Open the document with the digital key.
2. Select and copy the digital key.
3. Switch to KEM 'Basics/media'.
4. From the list, select the smartphone to which the key should be added.
5. Insert the entry in the 'Digital key' column.

7.3.2 Import from file

Import a media list

The smartphone and digital key data is recorded in a media list. The media list is imported into the project via the 'Start/import' menu.

Import from PDF voucher

One or more digital keys are recorded in a voucher document. These are then imported into KEM using a wizard.

Voucher composition

- Vouchers are searchable PDF documents.
- Scanned image PDF documents will be rejected as invalid.
  This is usually the case if the PDF has been printed out and scanned again. In this case, enter the key(s) using the keypad as described in 'Manual Entry' [▶ 7.3.1].

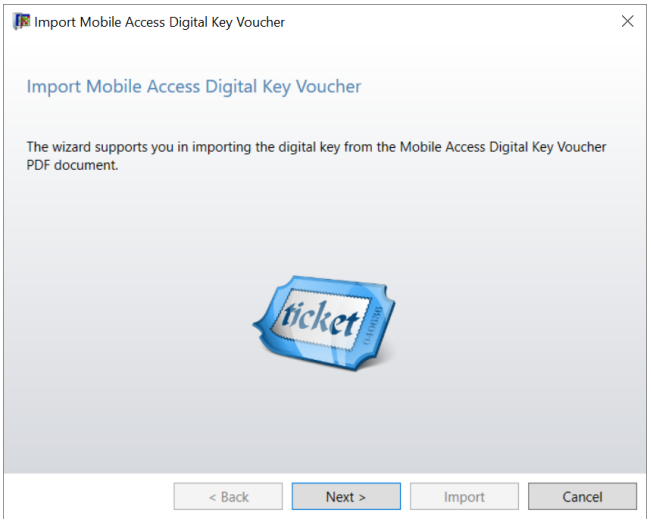
Starting points for the wizard

The wizard can be started from different points in KEM:

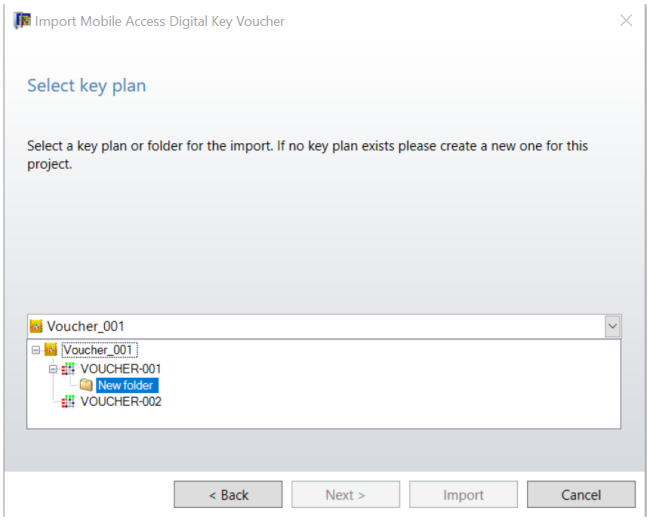
- From the 'Import' menu on the start screen.
- From 'Navigator/Wizards'.
- From the context menu of a Mobile Access medium (smartphone) in 'Navigator/Basics/Media'.

Procedure

1. Start the wizard.



2. Click 'Next'.
3. If a project contains several key plans or folders:
   Select the key plan or folder to which the imported digital keys should be assigned.
   ⇨ If the project only contains one key plan, this step is skipped.



4. Select the folder that contains the voucher documents.
5. Click 'Next'.
6. Use the checkboxes to select the digital keys to import.

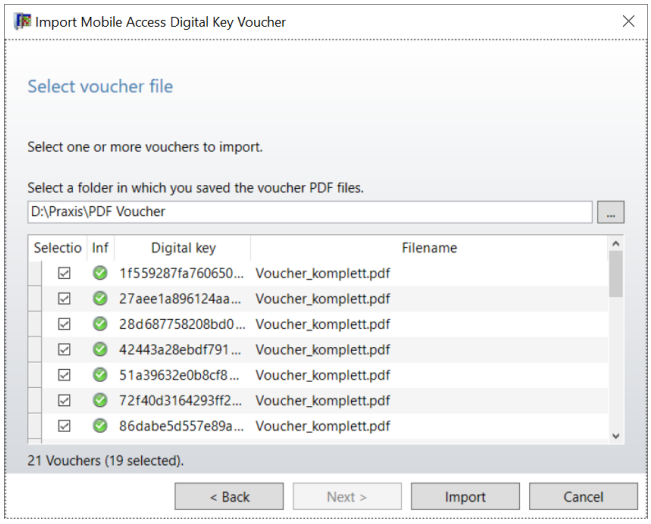
⇨ All valid keys within the folder are selected by default. Keys that have already been imported are displayed as invalid.

⇨ The 'Info' column shows whether a key is valid or invalid.

⇨ Invalid keys cannot be imported.

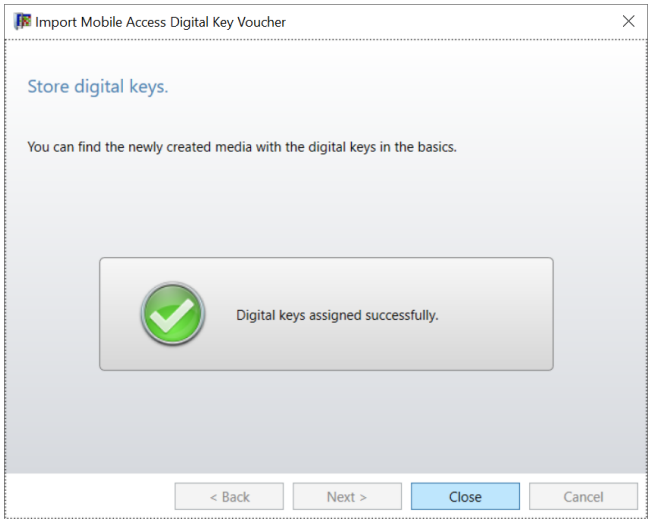
⇨ Keys can only appear once in a project.

7. Click on 'Import'.



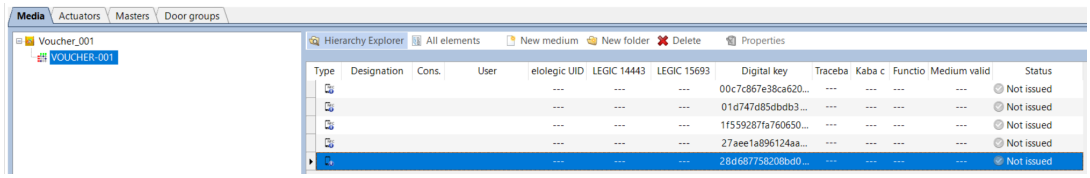
⇨ The import process is carried out.

8. Click 'Close'.



⇨ The wizard closes.

⇨ A Mobile Access medium (smartphone) has been created for every digital key in the 'Media' tab.



7.3.3 Import vouchers to a Mobile Access medium

If a smartphone is created as a user medium in KEM, the digital key from the voucher file can be imported to this medium.

Voucher composition

- Vouchers are searchable PDF documents.

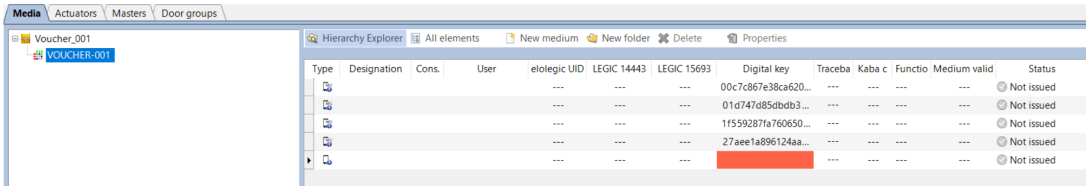
- Scanned image PDF documents will be rejected as invalid.
  This is usually the case if the PDF has been printed out and scanned again. In this case, enter the key(s) using the keypad as described in 'Manual Entry' [▶ 7.3.1].

Requirement

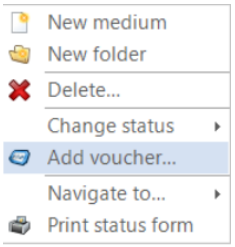
- The user medium is created as a smartphone.

Procedure

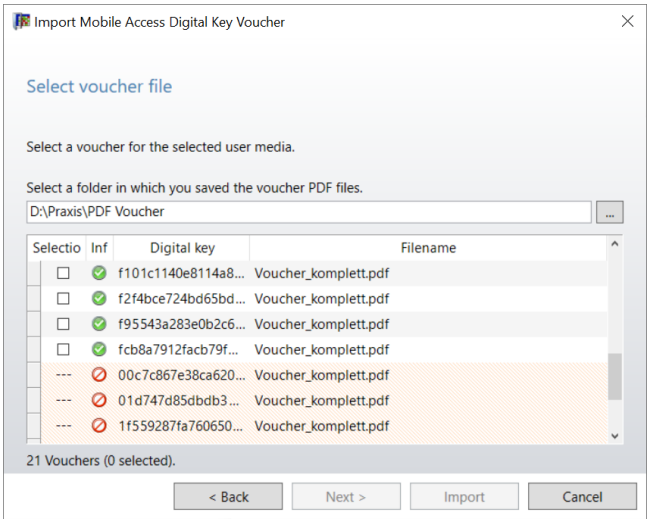
1. Navigate to 'Navigator/Basics/Media'.



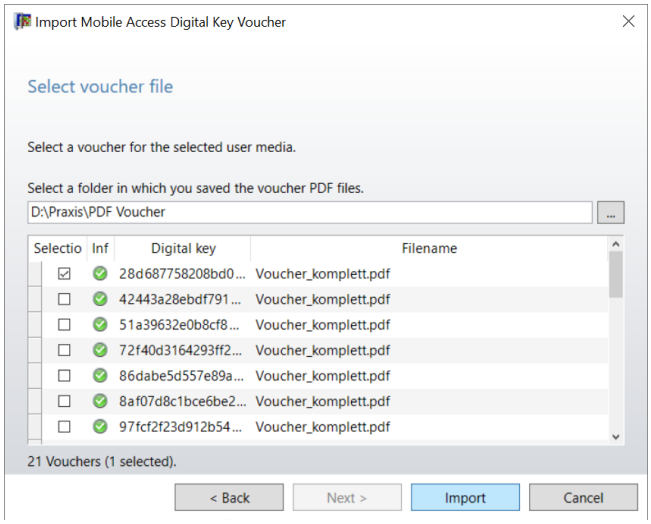
2. Use the right mouse button to open the context menu of the Mobile Access medium (smartphone) to which a digital key is being added.



3. Select 'Add voucher'.
   ⇨ The wizard starts.
4. Select the folder that contains the voucher documents.
5. Use the checkbox to select the digital key to import.

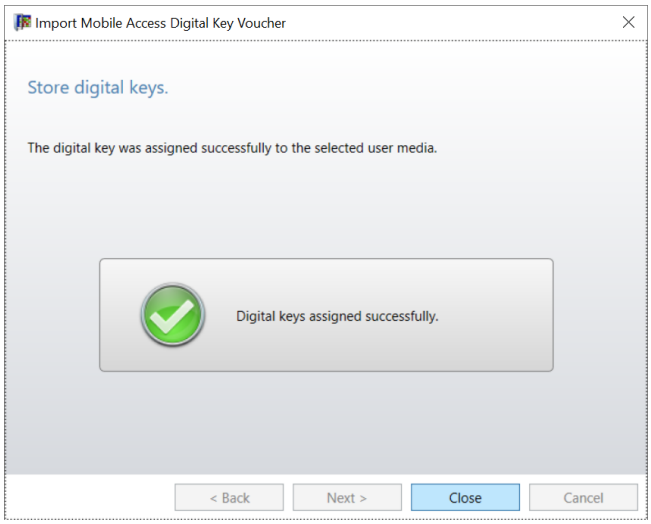


   ⇨ No keys are selected within the folder as default.
   ⇨ Only one key can be selected.
   ⇨ The 'Info' column shows whether a key is valid or invalid. A valid key can be selected. Keys that have already been imported are displayed as invalid.
   ⇨ Invalid keys cannot be selected or imported.
   ⇨ Keys may only appear once per project.
6. Click on 'Import'.



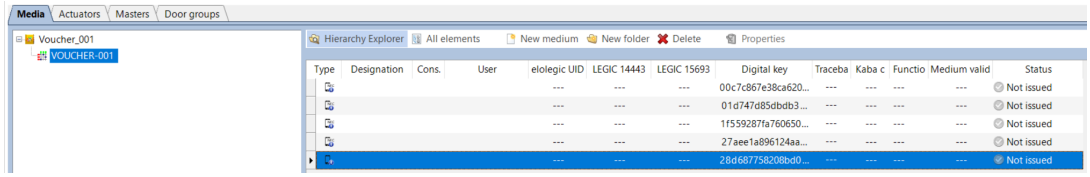
⇨ The import process is carried out.

7. Click 'Close'.



⇨ The wizard closes.

⇨ The digital key has now been added to the Mobile Access medium.



7.4 Authorisations

If smartphones and components are set up for Mobile Access, authorisations are assigned to components as in the case of other media types, as described in section.

7.5 Setting up components for Mobile Access

If the requirements for Mobile Access are met, a component can be configured in KEM as usual.

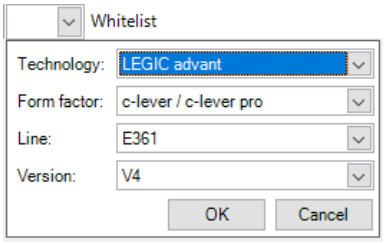
1 Configure components in KEM

2 Prepare the components with the VCP Installer app for Mobile Access.
VCPs contain the cryptographic key.

3 Transfer the configuration data from KEM to the component.

7.5.1 Creating components in KEM

Components for Mobile Access are created in the project of a master key system under basics/actuators.



When creating the component under Line for Mobile Access, select from these points:

- Line E3xx: Mobile Access (only NFC)
- Line E340: Mobile Access (NFC and Bluetooth)
- Line E360: wireless and Mobile Access
- Line E361: wireless with door monitoring and Mobile Access

Mobile Access is possible for firmware version 42.32 or higher.

7.5.2 Requesting LEGIC configuration package.

If the desired VCP file is not available, it must be requested from dormakaba. See separate description at https://www.dormakaba.com/en/software-downloads/downloads-kem-software

7.5.3 Initialising Mobile Access in the component

After an INI reset, the LEGIC configuration package is removed from the component.

Requirements

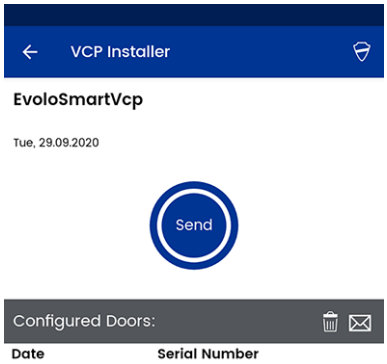
Smartphone
- The VCP Installer app is installed and the registration process with the telephone number is completed.
  The registration code received via SMS is entered.
- Access to the Internet is possible (WLAN or mobile data).
- Name and password for the LEGIC configuration package are known.
  Name and password for the package are shared by dormakaba after the registration process.

Component
- The component is ready for operation.
- There is a master medium available.

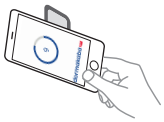
Procedure

LEGIC configuration package is transferred to the component

- Hold the master medium up to the antenna for approx. 1 second.
- Start the VCP installer on the smartphone.
- Selecting the LEGIC configuration package.
- Tap on 'Send'.



- Enter the password for the LEGIC configuration package.



- Hold the smartphone up to the component.

Signal/display		
	Component/registration unit	**Smartphone**
During data transmission:	• Green glows.	
After successful initialisation:	• Three signals are sounded.	• Green • Serial number of the component
The component is initialised.		
After unsuccessful initialisation:	• 1 brief acoustic signal sounds. • Red glows briefly. • 1 long acoustic signal sounds. • Red glows briefly. • 1 brief acoustic signal sounds.	• Red

7.6 Transfer

Components that receive the Mobile Access authorisations must be initialised with the VCP Installer app prior to the first usage of the authorisations.

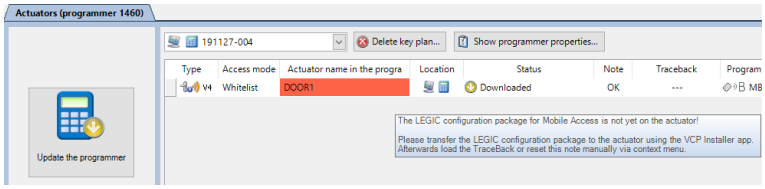
Mobile Access data cannot be processed if the initialisation of the components through the VCP Installer app has not been carried out.

The authorisations saved in KEM are transferred with the programmer or wirelessly.

7.6.1 Confirming VCP Installer

In order to use Mobile Access, the component must be initialised with the VCP Installer app for this purpose.

In the transfer menu, the actuator name is highlighted in red if the component has not yet received the LEGIC configuration package. The tooltip contains a warning.



The warning can be turned off in two ways:

- Automatic (recommended)
- (Relaisbetätigung manuell)

Automatic confirmation

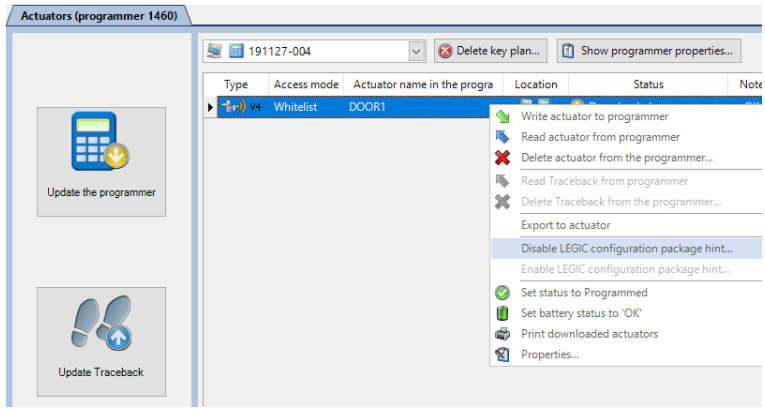
The warning is turned off automatically when the traceback of the component is loaded and updated in KEM after the component is initialised through the VCP Installer app.

Information about loading traceback data is described in section [▶ 6.12].

Procedure:

1. On the component, carry out the initialisation with the VCP Installer app. See section [▶ 7.5.3].
2. Load the traceback of the component with the programmer or wirelessly.
3. Update the traceback in KEM.
   ⇨ The warning is disabled, and the actuator name is no longer displayed in red.

Manual confirmation



1. On the component, carry out the initialisation with the VCP Installer app. See section [▶ 7.5.3].
2. Select the respective component.
3. Open the context menu with the right mouse button.
4. Select the 'Disable LEGIC configuration package hint...' menu option.
   ⇨ The warning is disabled, and the actuator name is no longer displayed in red.

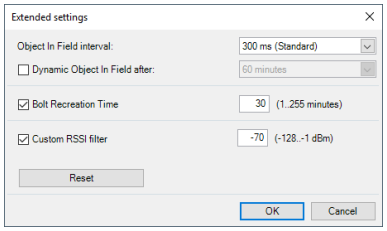
7.7 Properties

This section only describes the properties relevant to Mobile Access.

7.7.1 Actuator properties

Enabling Tap Go on an actuator is only effective if the user's Mobile Access credential on their smartphone was issued after January 1, 2026. Credentials issued before this date do not support Tap Go and must be reissued. If a user's phone does not respond to Tap Go despite it being enabled on the actuator, ask them to refresh their Mobile Access credentials in the app.

7.7.1.1 RSSI filter



The RSSI filter determines the threshold value for the signal strength and distance beyond which a smartphone will be detected.

Change the settings, only after consulting with Support, if it is absolutely required for reliable differentiation between several components.

Additional information can be found in PG Mobile Access.

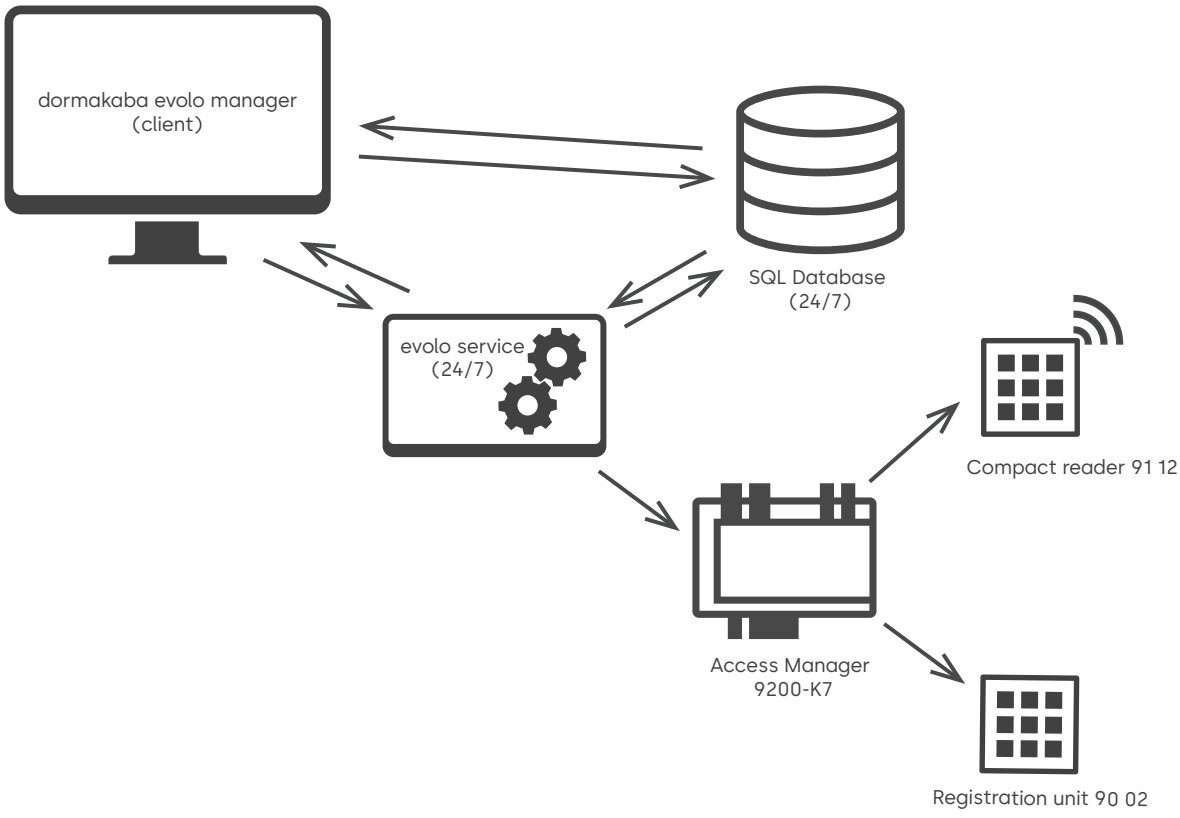
8 PIN-code-enabled devices

Introduction

This chapter describes how to integrate, configure, and use the PIN- and door-code-enabled devices dormakaba 90 02 registration unit and the dormakaba 91 12 compact reader within dormakaba's evolo manager (KEM). It contains an overview of the communication architecture, supported hardware, licensing information, credential handling, and tracing capabilities. Using the PIN code devices extends traditional credential-based access control by integrating PIN and door code functionality into the KEM environment.

Overview

The PIN code readers are connected to an Access Manager 92 00-K7 B-Client AC30, which makes access decisions locally (that is, offline). The Access Manager communicates with KEM through the evolo Service, which acts as a middleware component installed either locally or on a remote machine. KEM centrally manages users, credentials, and authorizations, while the evolo Service securely transfers this data (via HTTPS) to the Access Manager and returns status and event information to the KEM database. This approach ensures centralized management with decentralized, offline-capable access decisions at the Access Manager level.



In everyday practice, when a user enters a PIN, presents a LEGIC or MIFARE medium, or uses mobile access, the reader forwards the data to the Access Manager, which checks its stored whitelist authorisations or records and time profiles. If their authorization is valid, the corresponding output is triggered and the entry point opens to the user. If not, access is denied. All events are logged and synchronized back to KEM for traceback.

8.1 Communication concept and security

The PIN-capable readers are not connected directly to KEM. Instead, communication is handled through the evolo Service, which acts as middleware between KEM and the Access Manager. The communication workflow operates as follows:

- Configuration and authorization changes are created in KEM.
- The evolo Service detects and transfers these updates.

- The Access Manager stores the received data locally.
- When a credential is presented, the Access Manager locally decides whether to allow or deny access to the user.
- Event data and status information are returned to the dormakaba evolo Service and stored in the SQL database.

In cases when the network connection to KEM is temporarily unavailable, access decisions continue to function because they are made locally within the Access Manager. This means that users still receive access even when the device does not have an active connection to KEM.

Security model
All communication between the dormakaba evolo Service and the Access Manager is secured by using HTTPS. This ensures encrypted transmission of configuration and authorization data. The default used ports are HTTP: 8085 and HTTPS: 8086. In practice, most installations are configured to use HTTPS only.

8.2 Supported devices

The hardware components that support PIN functionality within KEM system are the following:

dormakaba Registration Unit 90 02
The Registration Unit 90 02 functions primarily as an antenna device. It is suitable for installations where Mobile Access is not required. User access is enabled using:

- Media access
- PIN access

Compact Reader 91 12
The Compact Reader 9112 extends the above-mentioned feature set. If smartphone-enabled access is a necessity, it is the only applicable option. User access is enables using:

- Media access
- PIN access
- Mobile Access via smartphone.

Access Manager 92 00 K7 B-Client AC30
The Access Manager 92 00 K7 B-Client AC30 is the central field controller in the PIN reader concept. It acts as the decision-making unit that stores authorizations locally and evaluates credentials without requiring a permanent connection to KEM. Functionally, the device:

- Receives configuration and authorization data from KEM via the evolo Service using HTTPS communication
- Stores whitelist entries
- Controls connected devices such as antennas and readers
- Logs granted and denied access events, and synchronizes them back to KEM.

8.3 Licensing

Licensing defines the operational boundaries of each Access Manager. It determines how many devices and credentials can be handled. Each Access Manager license specifies:

- Maximum number of antennas/readers
- Maximum number of whitelist entries (master records)

The master record limit is typically between 8,000 and 10,000 entries and is rarely a practical limitation. The device limit, however, is significantly more restrictive and must be considered during system planning. The system interface displays the license coverage to ensure transparency during configuration.

Each Access Manager operates under license-defined device limits. For KEM 7.2 these are:

- You can use a maximum of four devices per one Access Manager, if the device licence allows this number of devices.
- The supported hardware configurations can include two 90 02 devices as antennas (A and B), and up to two RS485 readers.

8.4 Access methods

KEM supports multiple access technologies, allowing flexible use depending on the security requirements of the project. The supported methods are:

- **Personal PIN**

  Assigned to an individual user and is invisible to other users, including in the KEM user interface.

- **Door code**

  A door code differs from a personal PIN in that it is assigned to one or more readers rather than to a person, and can be shared among personnel. For example, door codes can be convenient for cleaning staff, facility rooms, or parking areas.

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

  These credential technologies ensure compatibility with existing installations.

- **Mobile credentials (compact reader 91 12 only)**

All access methods can be restricted using time profiles.

MIFARE deployments require site keys to be stored in the reader. These keys are not automatically transferred by the Access Manager. Proceed as follows:

- Open the transmission view in KEM.
- Select the tab *Actuators (Access Manager)*.
- Select antenna or reader want to sent site key to, open the context menu, and select *Send site key ...*.
- When prompted, present the Security Card C to the desktop reader.

⇨ If a project includes MIFARE readers but no master credential, commissioning issues might occur.

Time Profiles and Operating Modes

All access methods can be restricted using configurable time profiles. Additionally supported are:

- Office mode
- Day/night mode
- Project-specific time zone configurations

8.5 Setting up KEM to use PIN-code-enabled devices

To use PIN-code-enabled devices, follow these steps in the described order.

Installing evolo Service

The evolo Service is required as middleware component that enables communication between KEM and the Access Manager. If not already present, proceed as described in section Install evolo Service [▸ 3.5]. You can install the evolo Service on the same machine as KEM, or on a separate machine within the same network. The choice depends on the infrastructure and security requirements of the specific project.

Configuring the evolo Service

After the service is installed, proceed as described in Set up the evolo Service to use the Access Manager [▶ 10.3].

Adding the Access Manager

The next step of the procedure is adding a new Access Manager to your project.

1. Starting from the KEM user interface, navigate to *View*, then *Basics*, *Access Managers* tab, and click *Add new Access Manager...*. When the wizard appears, click *Next*.

If the RF configuration of the Access Manager is not available, click *Add anyway*.

2. Enter the IP address and name of the new access manager, then click *Next*.
3. The next step automatically checks the availability of the new Access Manager. Once confirmed, click *Next*.
   ⇨ The subsequent automatic configuration may take up several minutes.
4. Click *Done* to complete the procedure.

Adding antennas and readers to the Access Manager

1. Open the properties of the newly added Access Manager.
2. In the *Common* properties tab, choose a time zone. For LEGIC projects, also choose which LEGIC technologies you want to use.
3. Configure each antenna and reader, depending on the allowance of your license. From the drop-down lists, choose the reader type, physical signal input and output of the device, designation to distinguish the device, and door number and designation. Note the instruction about setting correctly the rotary switch on the back side of the physical device.

Use the DIP switch on the compact reader to select MIFARE and LEGIC technologies and the RS-485 topologies (bus system or star topologies).

Use the rotary switch to set the internal address of the device. To set it up to communicate with the correct antenna, use position *3* for Reader 1, and position *4* for Reader 2.

The antennas are connected directly to *Ant. A* or *Ant. B* on the Access Manager. No additional configuration is required.

Enabling user access

Users are granted access to doors, actuators, or components by allowing their media in the project, whether it is a PIN code, door code, or a mobile device. To enable users, proceed as follows:

1. From the KEM user interface, navigate to *Media*.
2. In the *Hierarchy explorer* of the project, click *New medium*.
3. Choose the model and type of medium. For example, choose *Code* or *PIN* from the appropriate drop-down lists. After it is created, edit the PIN or code by double-clicking in the *Designation* column for the new PIN or code. For example, type *PIN code*.
4. In the *User* column, open the drop-down list and choose the user you want to grant access via this PIN.

For door codes: you cannot assign door codes to specific users.

5. Optionally, you can change the PIN or door code to one of your choice, or to an automatically generated one.
6. Authorize the PIN code for use. Navigate to the *Authorizations* view, and double-click on the *PIN code* media you just created in the left-hand side list. This opens a view that lists the actuators that this media is enabled for. For new projects, it currently be empty.
7. From the *Actuators* list on the left-hand side of the user interface, drag and drop the actuators you want to use with the *PIN code* media. For example, drag one antenna and one reader. Then wait for the devices to be automatically programmed and available for the media.

⇨ The user that has the particular *PIN code* media type is now enabled for the selected PIN-code-enabled devices, granting them access to the gateways they operate.

8.6 User process of accessing PIN-enabled components or entry points

1. When the user approaches the door they need access to, they provide the identification means assigned to them. For example, they want to use their PIN code.
2. They input the PIN code on the reader. If the code is correct, access is granted to them and the door opens. This is also denoted by a brief audio signal and a blinking green notification light on the device.

9 Terminal

From KEM V7.1, only 9600-K6 and 9600-K7 terminals are supported.

evolo Service must be installed before using a terminal for the first time.

- Install evolo Service [▶ 3.5]

9.1 Function

In a CardLink environment, a terminal can be used to centrally assign access rights and validate user media. Validation and access rights are configured in the system software. When a user medium is presented, the terminal retrieves the access rights from the KEM database and writes them to the medium or deletes them from there. The medium is validated.

The database and evolo Service must always be available for the terminal, otherwise CardLink updates cannot be provided. In this case, only existing user media with validation data stored on the terminal can still be validated. The number of validation data records that can be stored in the terminal depends on the scope of the purchased terminal licence.

Detailed information on assembly and further installation instructions for the terminal can be found in the terminal installation instructions.

9.2 Set up

The following steps must be completed before terminals can be used in KEM:

1. Install evolo Service [▶ 3.5].
2. Enable the use of terminals [▶ 9.2.1].
3. Add the terminal to the project [▶ 9.2.2].

9.2.1 Activate terminals

Before terminals can be used in KEM, the system must be prepared for using terminals.

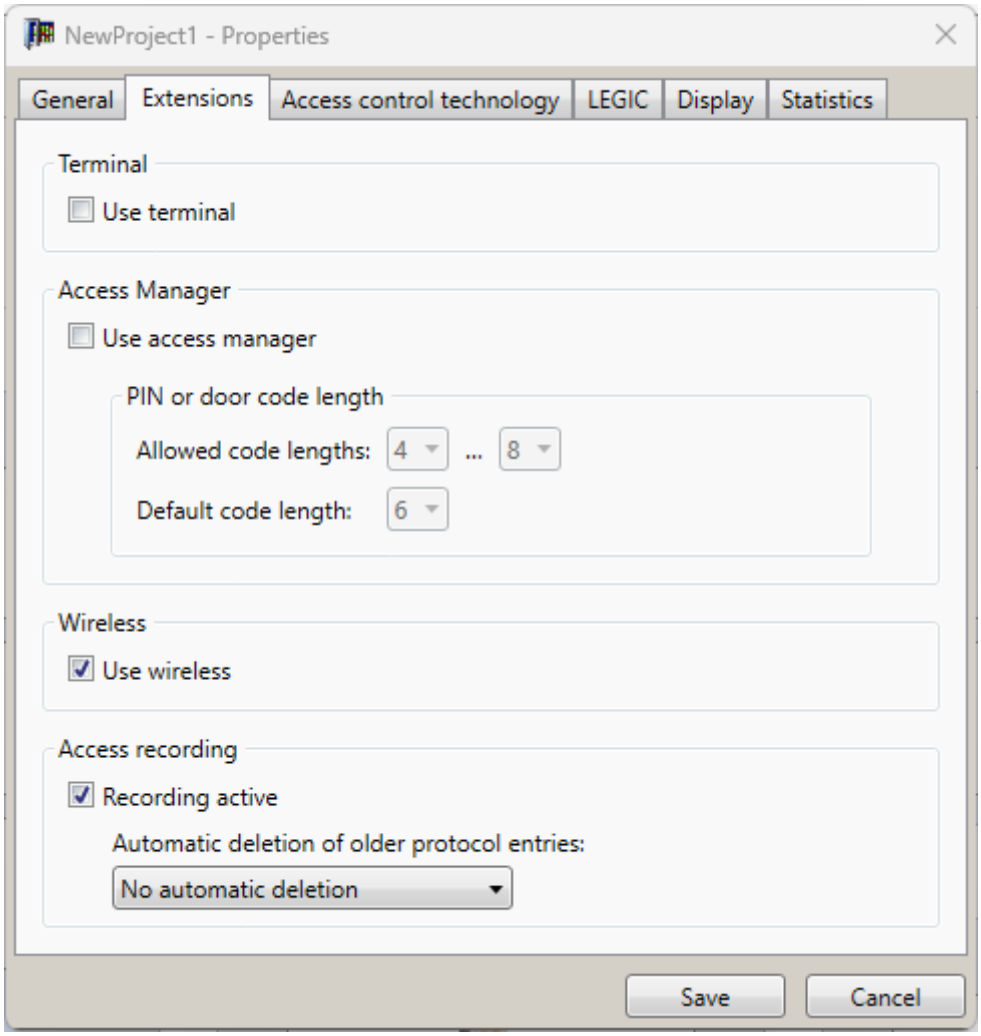
Terminal usage is only activated in the project properties once the wizard has been successfully executed.

Start KEM as an administrator if evolo Service is installed on a remote computer. This is only necessary for setup purposes.

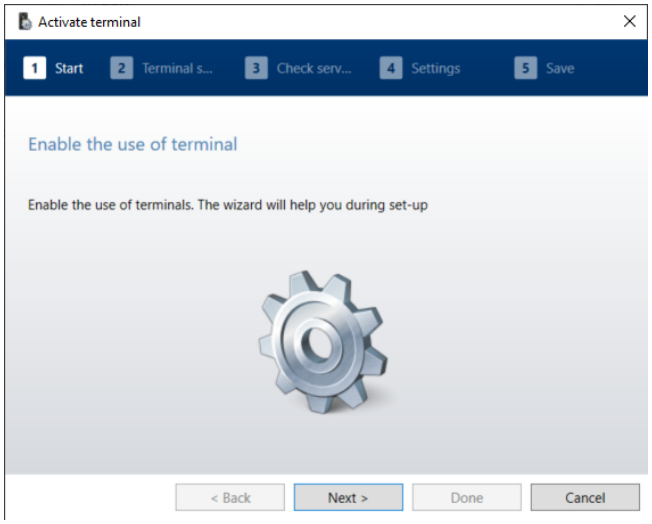
The user needs administrator rights on the computer to configure the ports in the firewall. This is only necessary for setup purposes.

Activation procedure

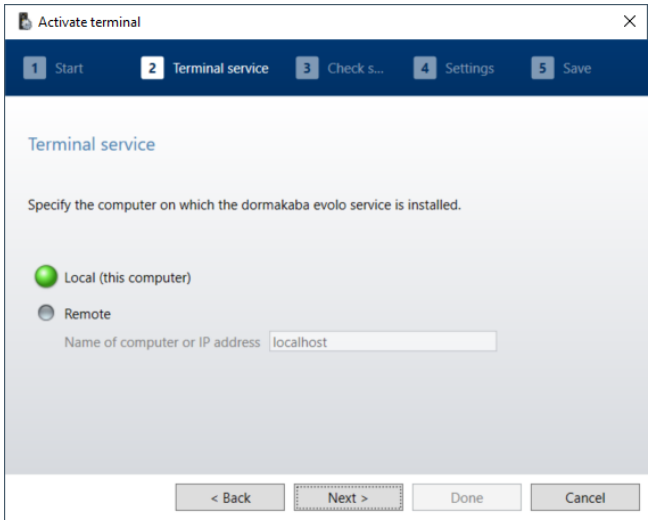
1. Open the project properties (F4).
2. In the 'Extensions' tab, tick the checkbox 'Use terminal'.
   ⇨ The wizard for setting up terminal use in KEM is started.



3. Follow the wizard.



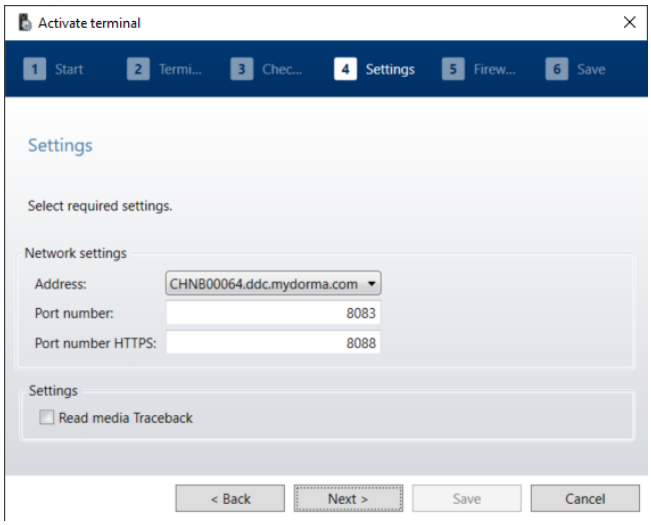
4. In step 2, specify the computer on which evolo Service is installed.



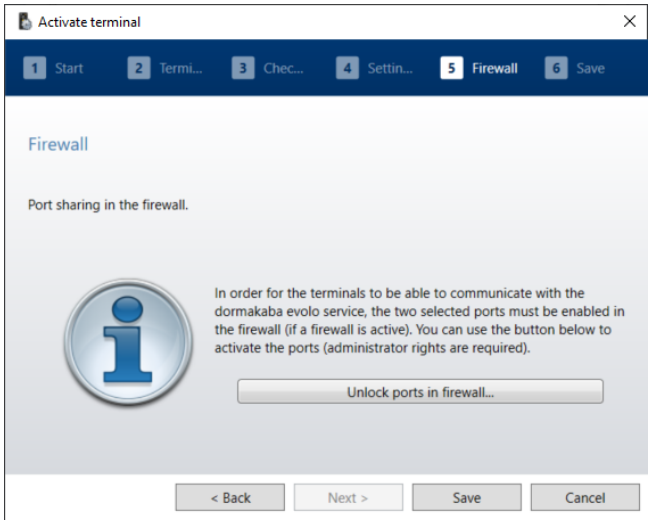
⇨ Local: evolo Service is installed on the computer on which KEM is also installed.

⇨ Remote: evolo Service is installed on a different computer than KEM. Specify the name or IP address of the other computer.

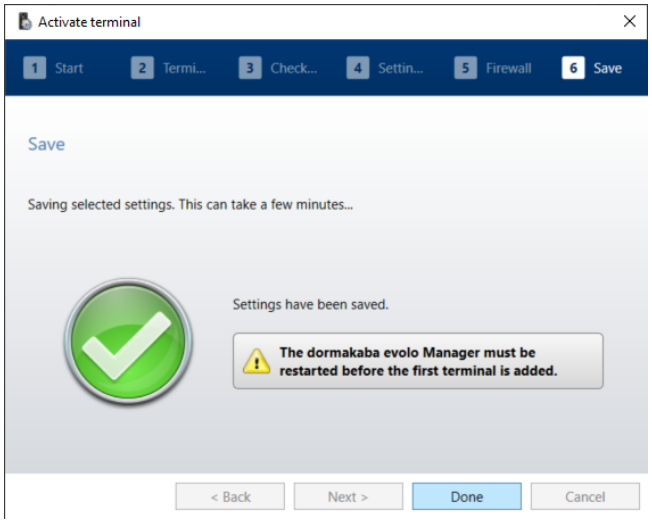
5. Click 'Next'.
6. In step 4, select the IP address or computer name of the computer on which evolo Service is installed.
   To do this, specify the port number. Port 8083 is used as the default setting. If the port is already occupied, the port number can be changed.
   Enter the HTTPS port number. The default port for HTTPS is 8084.
   Reading the media traceback log can be optionally enabled.



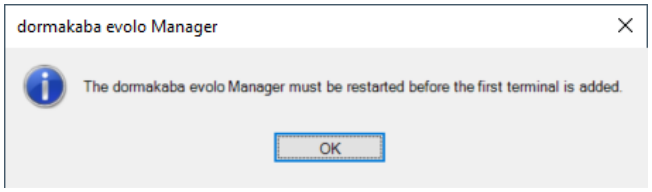
7. Click 'Next'.
   ⇨ If a firewall is activated on the computer, the desired ports in the firewall must still be enabled. The wizard does this for the user. The user requires administrator rights on the computer.



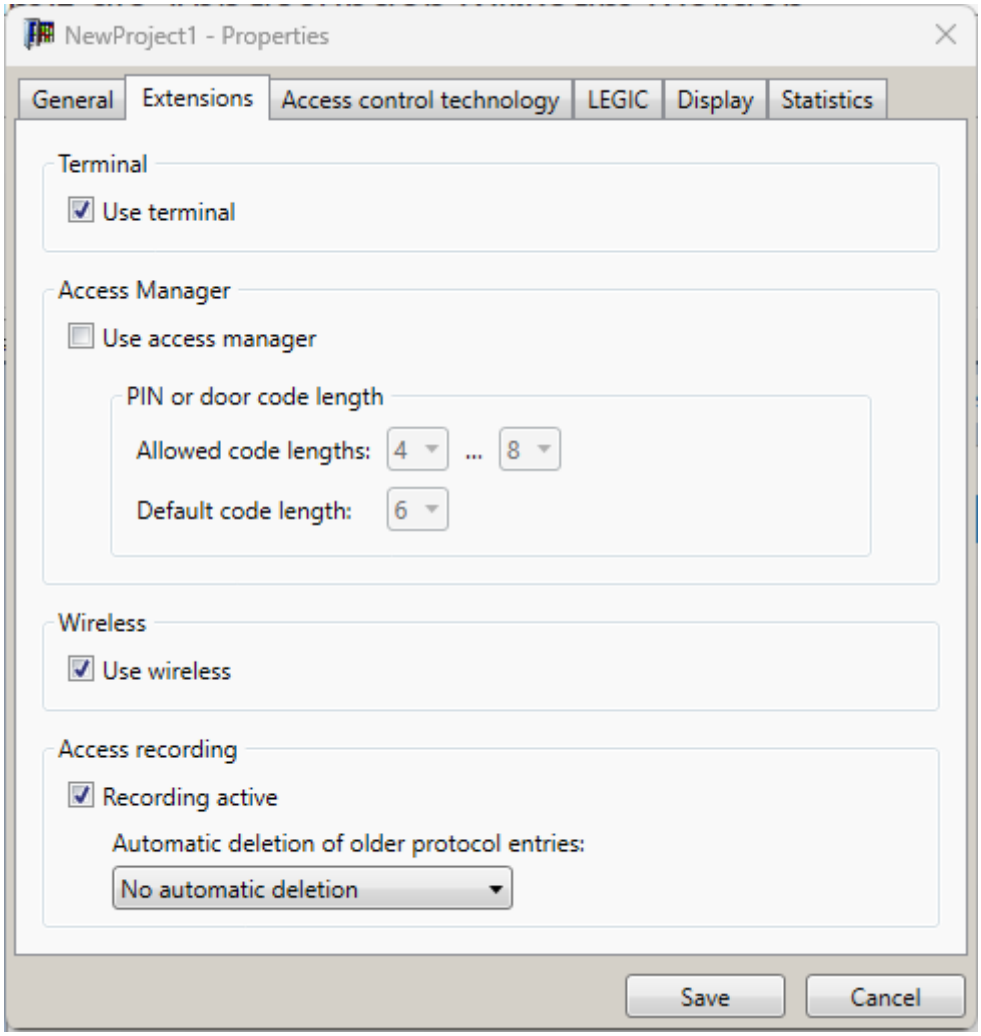
8. Click 'Enable ports in firewalls'.
   ⇨ The ports are enabled using a Windows command prompt. Press any key to close the window once the ports have been enabled.
9. Click 'Save'.
   ⇨ The settings are saved in KEM.
10. Click 'Finish'.



   ⇨ Before putting the first terminal into operation, close the evolo Manager and restart it to allow the changes to take effect.



   ⇨ The 'Use terminal' checkbox is activated in the project properties.



11. Click 'Save'.

⇨ The 'Terminals tab' is added to the 'Basics' area.

⇨ Terminals can now be [▸ 9.2.2] added in 'Basics/Terminals'.

9.2.2 Adding a terminal

Information and requirements

Terminals cannot be used in different projects in the system software. Previous configurations for other projects will then be overwritten, and it will no longer be possible to use the terminal in the previous project.

Terminals must be connected to the network.

The use of terminals in the project has been set up.

New terminal in the network

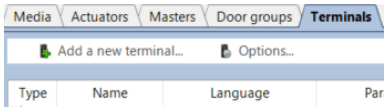
An unconfigured 9600-K6 or 9600-K7 terminal shows the following on the screen when it is connected to the network and switched on:

- Its own serial number
- Its own IP address
- 'Waiting for registration'

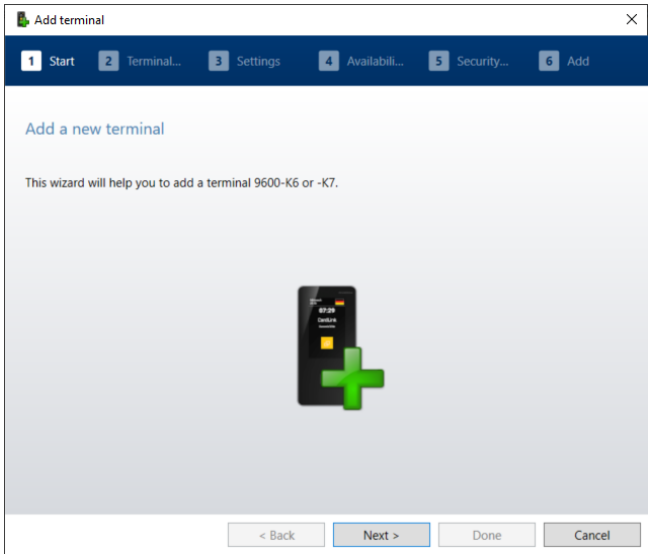
The terminal is ready for configuration.

Procedure

1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Terminals' tab.
3. Click 'Add new terminal'.



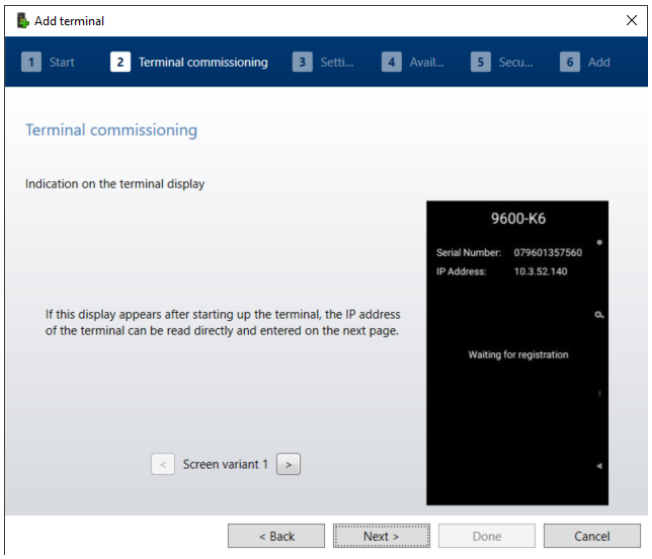
4. Follow the wizard.

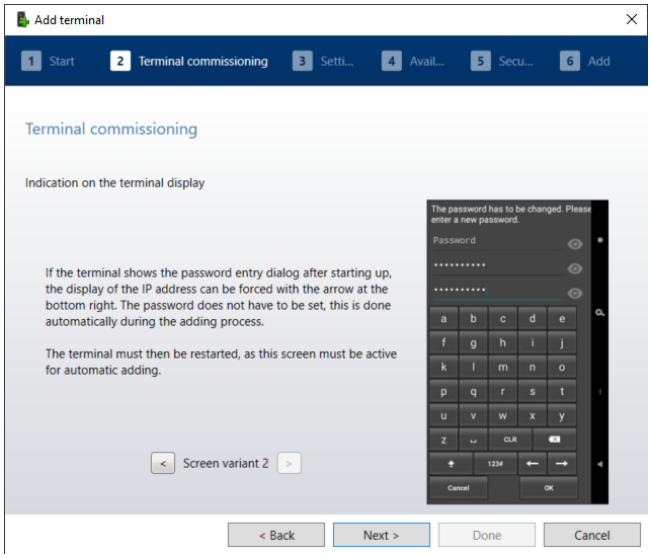


⇨ **Note:** If the security card for this project has not been scanned, you must confirm that you wish to continue without scanning the security card.

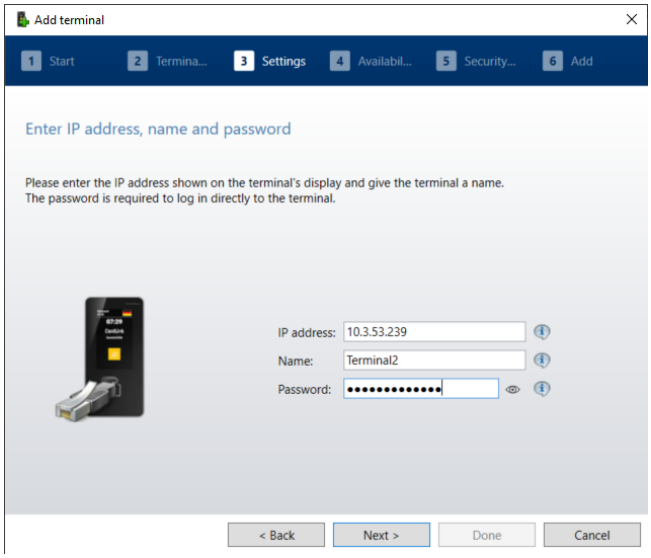
5. Click 'Next'.

⇨ Read the IP address needed for the next step from the terminal and note it down.

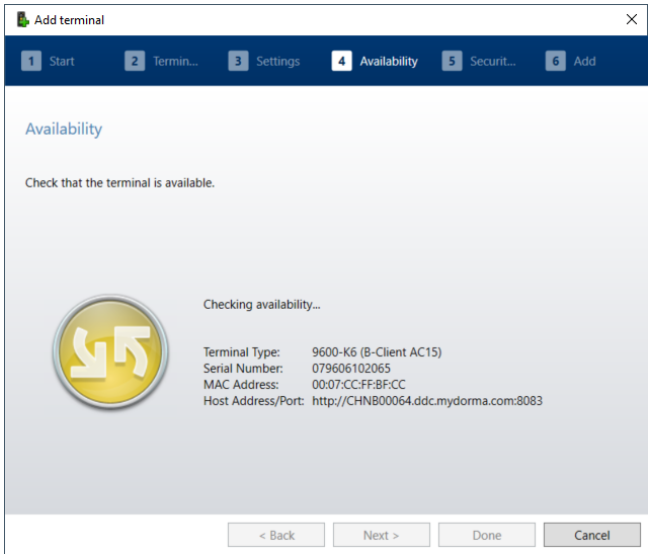


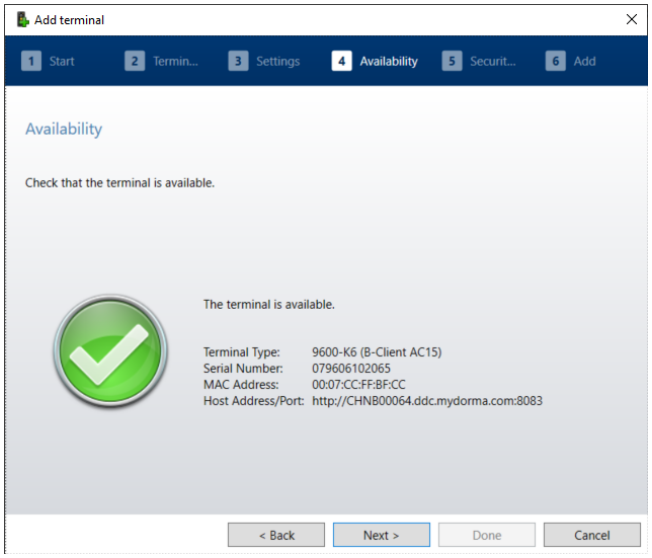


6. In step 3, enter the IP address of the terminal, enter a name and assign a password for the terminal.

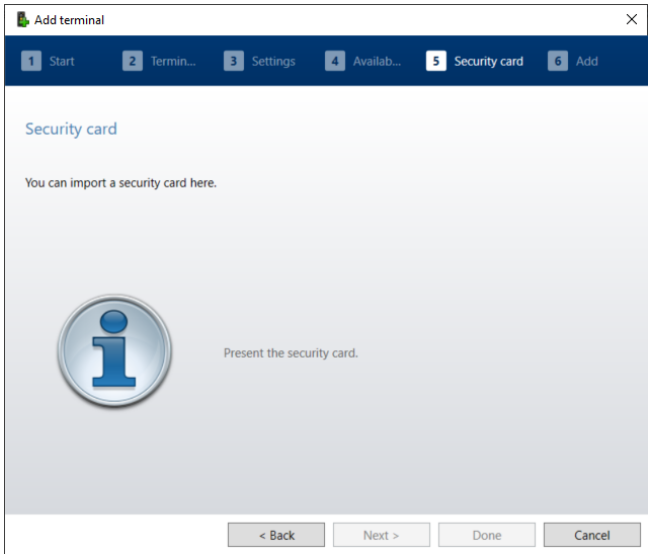


7. Click 'Next'.
   ⇨ KEM checks whether the specified terminal is available in the network.

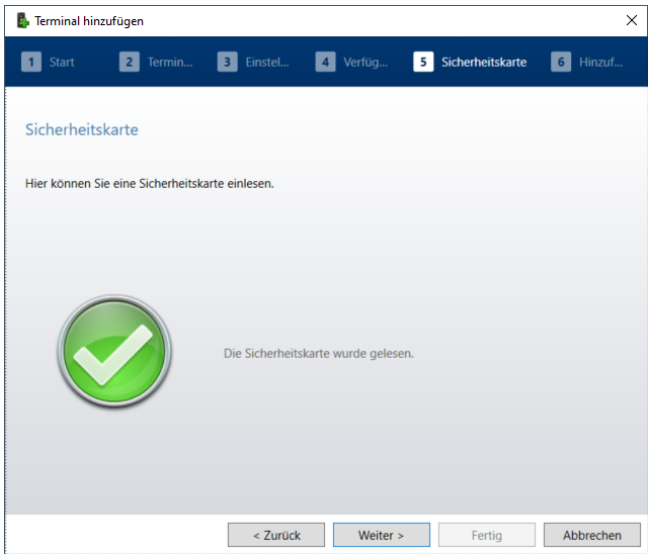




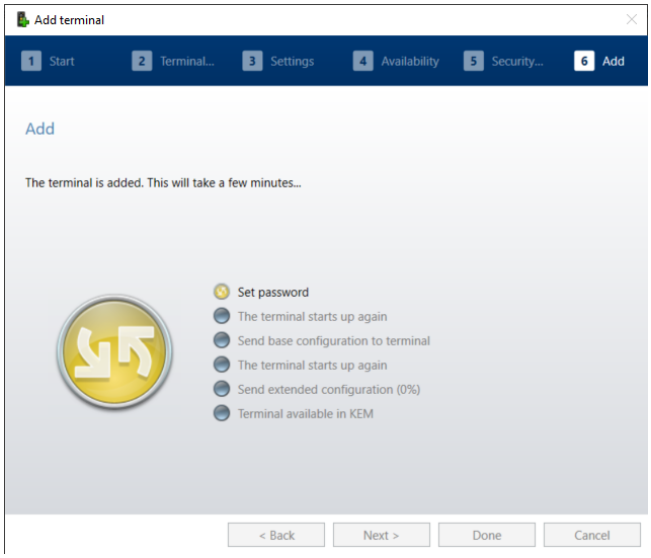
8. Click 'Next'.



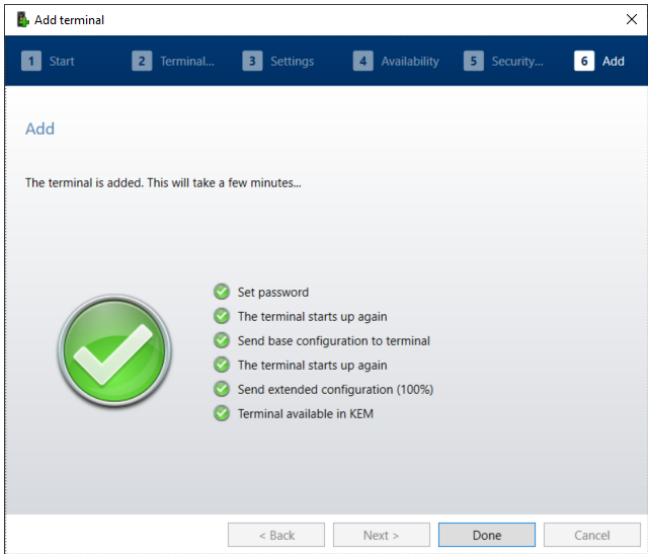
9. Scan the security card if it is configured for the project.



10. Click 'Next'.



⇨ The terminal is configured for use in KEM. This can take a few minutes. This process cannot be cancelled or paused.



11. Click 'Finish'.

⇨ The terminal has now been added to the project.

⇨ The wizard closes.

For information on operating the terminal, see.

Only for LEGIC projects

In LEGIC projects, the terminal must still be launched using a C2 security card to activate write authorisation.

To grant write authorisation, visit each terminal and present a C2 security card.

9.2.3 Reset/remove terminal

Process for removing a terminal from a project.

Requirements

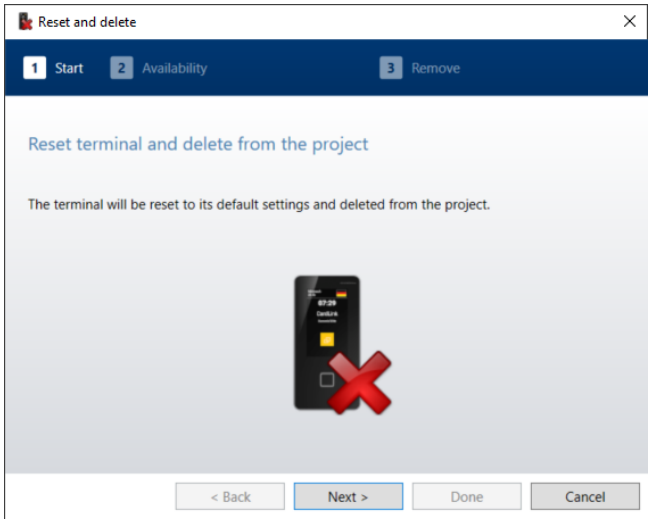
- The terminal is accessible in the project. The terminal can be reset and removed from the project (recommended).

- The terminal is not accessible in the project. The terminal can only be removed from the project.

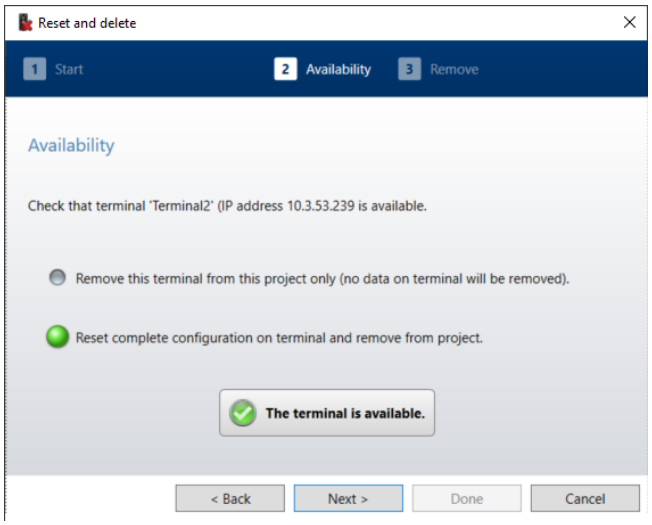
Procedure

1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Terminals' tab.
3. From the list, select the terminal being removed.
4. Right-click to open the context menu of the terminal entry.

5. Select the menu item 'Reset terminal and delete from project'.
   ⇨ The terminal removal wizard will start.

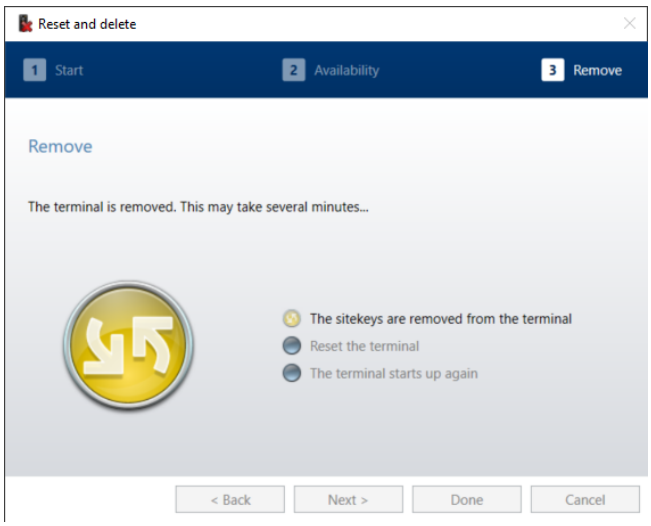


6. Click 'Next'.
   ⇨ The wizard checks whether the terminal can be reached.

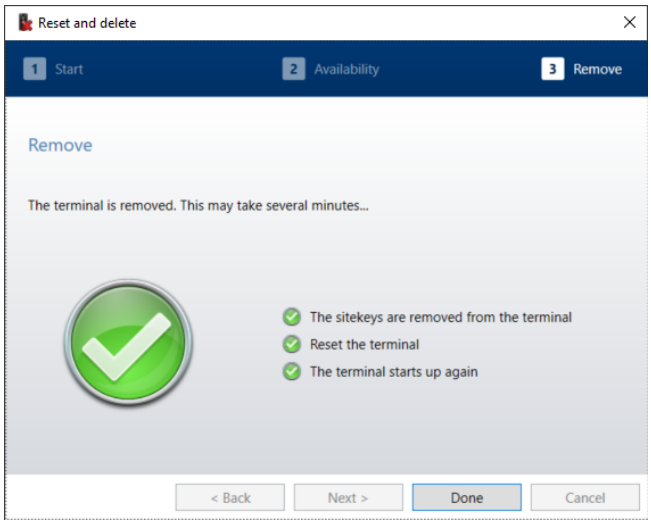


7. Choose whether the terminal should only be removed from the project or whether the terminal should also be reset. When a terminal is reset, all data saved on the terminal is lost and the terminal can then be integrated into another project.

8. Click 'Next'.



⇨ The process cannot be cancelled.
The wizard removes the relevant MIFARE or LEGIC project data from the terminal.



9. Click 'Finish'.
⇨ The terminal is removed, and the wizard closes.

9.3 Operation

9.3.1 Programming media

Before using the terminal in operation, all user media belonging to the project must be programmed for use with the terminal.

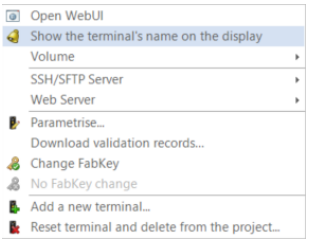
If the media are not supplied pre-programmed, they must be programmed once using KEM.

9.3.2 Volume

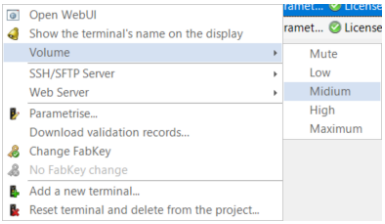
The terminal offers acoustic signalling options. The volume can be set using the context menu of the relevant terminal. The volume can be adjusted to 5 levels. The volume must be adjusted separately on each terminal.

Procedure

1. In 'Basics/Terminals', select the terminal whose volume is being adjusted.
2. Open the context menu with the right mouse button.



3. Expand the 'Volume' menu item.
4. Select the desired volume in the range from 'Mute' to 'Maximum'.



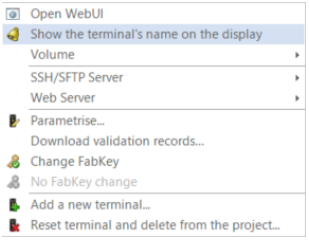
⇨ The terminal will play 4 tones at the selected volume.

9.3.3 SSH/SFTP server

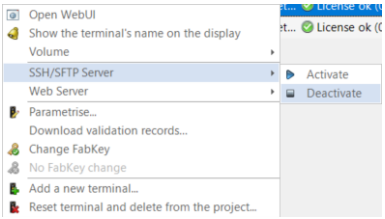
The terminal's SSH/SFTP server can be activated or disabled. After being configured for KEM, the server is deactivated by default and can be activated/disabled manually here.

Procedure

1. In 'Basics/Terminals', select the terminal whose SSH/SFTP server is being activated or disabled.
2. Open the context menu with the right mouse button.



3. Expand the 'SSH/SFTP server' menu item.



4. Select 'Activate' or 'Deactivate'.
   ⇨ It is disabled as default

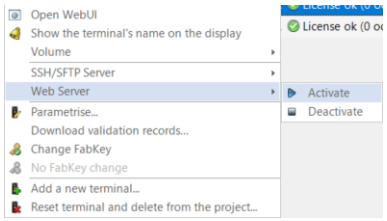
9.3.4 Web server

The terminal's web server can be activated or disabled. It can be used to access the web interface of the terminal. After being configured for KEM, the server is activated by default.

Procedure

1. In 'Basics/Terminals', select the terminal whose web server is being activated or disabled.
2. Open the context menu with the right mouse button.

3. Expand the 'Web server' entry.



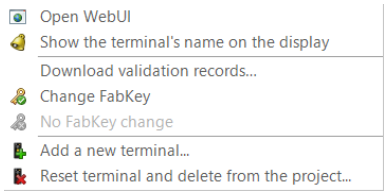
4. Select 'Activate' or 'Deactivate'.
   ⇨ It is activated as default.

9.3.5 Validation data records

The validation data records are required to validate media on the terminal. When the terminal is initialised, existing validation data is downloaded. The data is automatically updated by KEM during operation. The process can also be initiated manually. This may be necessary, for example, if the terminal has been unavailable for a longer period of time.

Procedure

1. In the 'Basics/Terminals' menu, right-click to open the terminal's context menu.



2. Select the menu item 'Download validation records'.
   ⇨ The validation records are loaded and saved on the terminal.

Online/offline

In online mode, the terminal has an active connection to evolo Service.

- evolo Service and the database are in operation.
- KEM is not needed.
- Current access data is available and can be written to the user medium.
- User media can be validated.

The terminal is not connected to the database in offline mode

- evolo Service is not in operation.
- KEM is not needed.
- Access data on user media cannot be updated.

- User media can be validated.

The maximum number of media that can be validated offline depends on the scope of the licence purchased for the terminal.

- If the licence does not have sufficient scope, a warning will be displayed in KEM.
- Only media whose data records are stored in the terminal can be validated.

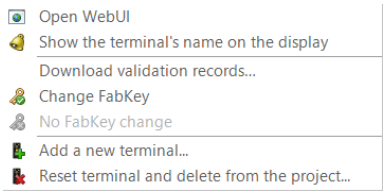
⇨ Recommendation: Choose a terminal licence with a scope that is suited to the number of media being validated.

9.3.6 Fabrication key changes

Only in MIFARE projects.

Media written by third-party companies receive a fabrication key for this production step. This key is used to programme the media. To allow the medium to be used by an end user, the fabrication key is replaced with an application key a single time. Every piece of device software on a medium has its own fabrication key that is replaced by a separate application key during this exchange. This replacement function can be activated for the connected terminals in the context menu. The function is disabled by default.

If the function is activated, the keys are replaced the first time the medium is presented.



Activate

1. Navigate to 'Basics/Terminals'.
2. Select one or more terminals.
3. Open the context menu with the right mouse button.
4. Select the menu item 'Fabrication key change active'.
   ⇨ The function is activated for all terminals.

Deactivate

1. Navigate to 'Basics/Terminals'.
2. Select one or more terminals.
3. Open the context menu with the right mouse button.
4. Select the menu item 'No FabKey change'.
   ⇨ The function is disabled for all terminals.

9.3.7 Parameterising

Information and requirements

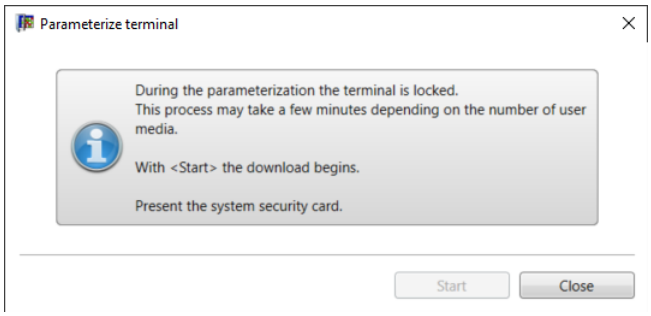
The security card of the technology used has been scanned.

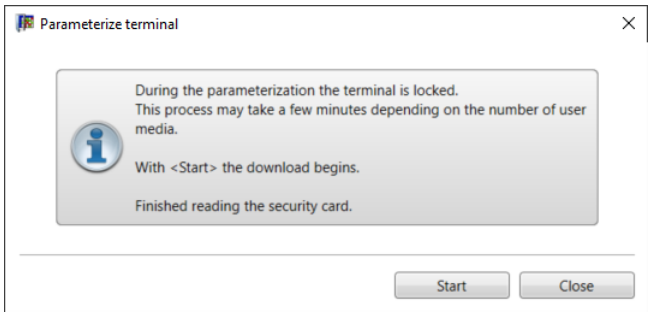
The terminal has been installed but the parameters not yet set.

Procedure

1. Navigate to 'Basics/Terminals'.
2. Select a terminal.
3. Open the context menu with the right mouse button.

4. Click 'Parameter settings...'
5. Only for MIFARE: Place the system's security card on the desktop reader.





6. Click 'Start'.
   ⇨ Data will be transferred The duration of the transfer depends on the number of pieces of configured user media.
7. The wizard guides you through the parameter setting process.
   ⇨ In the last step of the process, the terminal restarts. This procedure can take a few minutes.
   ⇨ The terminal's parameters are now set and it is available in the software.

In LEGIC projects, the terminal must still be launched using a C2 security card to activate write authorisation.

8. Present the security card C2 to the terminal and wait for the signals (1 tone, then 3 tones after 20 s).
   ⇨ The terminal now has write authorisation (has been launched) and can be used in the project.
   MIFARE projects do not require this step.

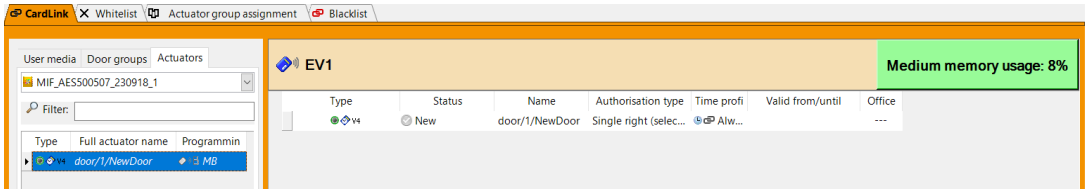
9.4 CardLink authorisations

In the CardLink authorisation type, the authorisations and validation data for a user medium are stored on the database server. They are retrieved from the terminal as necessary when the corresponding user medium is presented.

Once the CardLink data has been transferred to the database server, KEM is no longer needed.

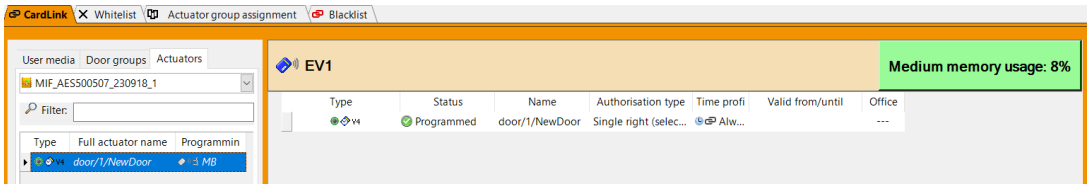
Procedure (example)

1. Go to 'Authorisations/CardLink'.
2. Select the 'User media' tab.
3. Drag and drop the medium into the top right field.
   ⇨ The medium then receives its new authorisations from the terminal.



4. Select the ‘Door groups’ or ‘Actuators’ tab.
5. Drag and drop a door group or an actuator into the right-hand field.
   ⇨ After being entered, the data record has the status 'New'. The data is transferred directly to the database. During operation, KEM is not required to collect data from the user. If the user media has retrieved its access authorisation from the terminal, the status in KEM changes to 'Current' after the next synchronisation.

If media traceback is enabled, the traceback data is transferred to KEM and can be viewed.



9.5 Project migration from V7.0

From V7.1, new terminals can only be commissioned using SSH/SFTP and https. The required certificate is provided by KEM. In addition, the port for secure communication must be defined and enabled in the firewall. The wizard helps you to do this. This chapter describes the process of migrating a terminal project created in V7.0 to the current version from V7.1. Older terminal projects with old terminals cannot be migrated.

Requirements

- The user requires administrator rights on the computer to install evolo Service and KEM.
- In V7.0, the terminals of the relevant project are correctly installed and active.
- The installation files (msi) for evolo Service from V7.1 are available.
- The installation files (msi) for evolo Manager from V7.1 are available.

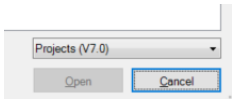
evolo Manager 7.0 and evolo Manager from V7.1 can be installed in parallel.
evolo Service may only be present and activated once on a computer.

Procedure

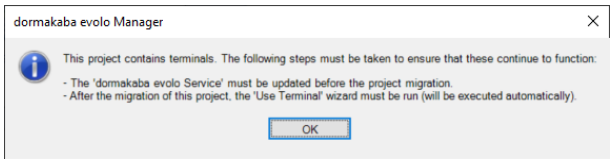
1. Update evolo Service to the current version.
2. Install evolo Manager version V7.1 or higher.
   ⇨ If the versions of evolo Service and KEM do not match, an error message is displayed.

Migration

1. Start the current evolo Manager.
2. Open the project to be migrated.
   ⇨ Filter the project selection for projects from V7.0.

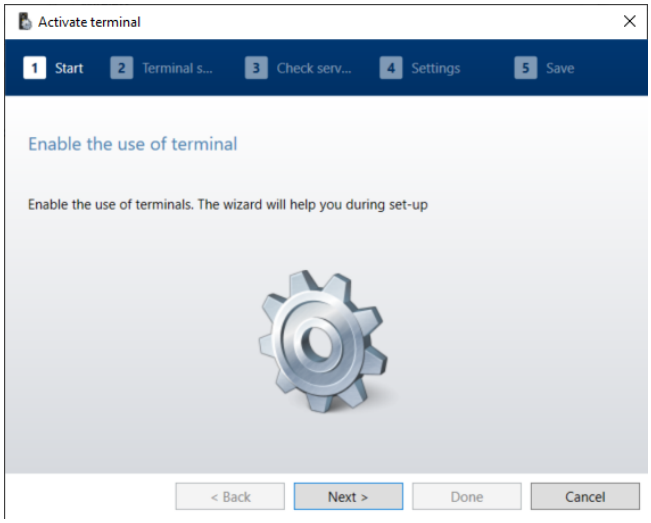


3. Select the project to be migrated.
   ⇨ KEM recognises the older project.

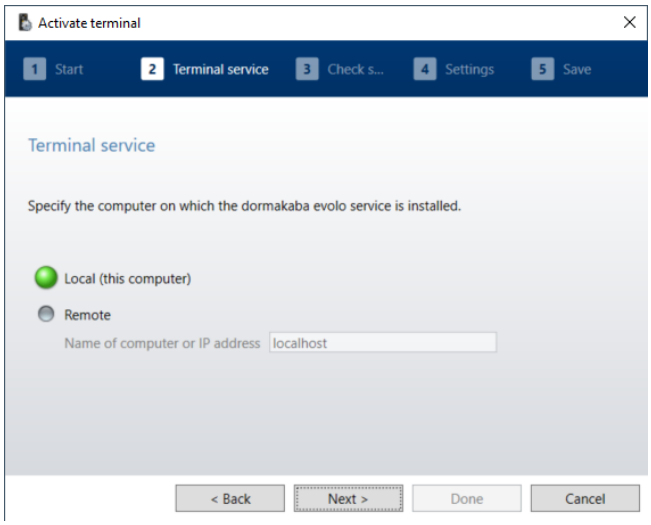


4. Click ‘OK’.

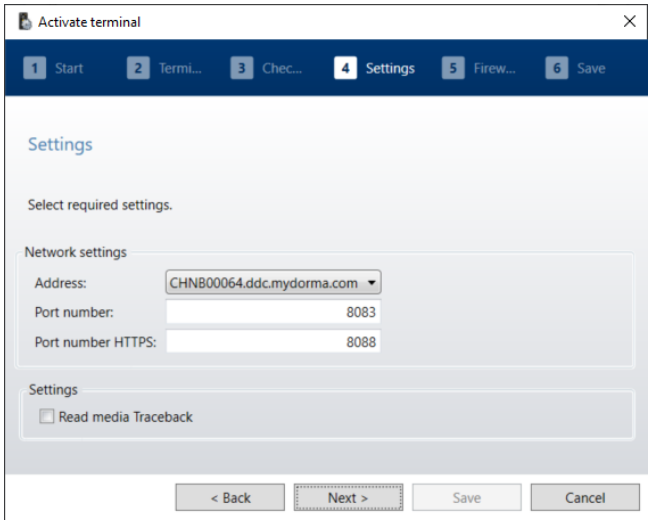
5. Click 'Yes' and migrate the project.
   ⇨ KEM switches to the 'Activate terminal' wizard after the migration. The newly required information is then collected and saved.
6. Follow the wizard's instructions.



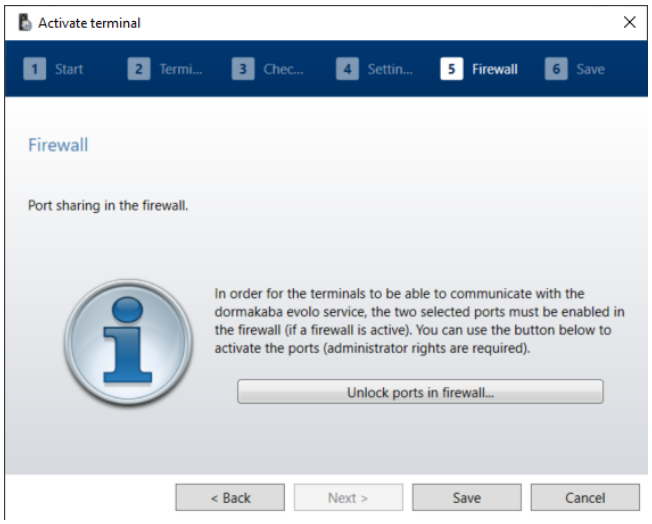
7. In step 2, specify the computer on which evolo Service is installed.



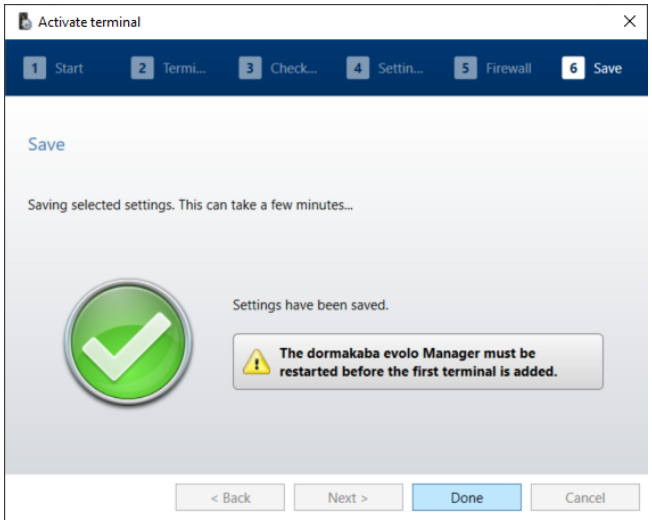
   ⇨ Local: evolo Service is installed on the computer on which KEM is also installed.
   ⇨ Remote: evolo Service is installed on a different computer than KEM. Specify the name or IP address of the other computer.
8. Click 'Next'.
9. In step 4, select the IP address or computer name of the computer on which evolo Service is installed.
   To do this, specify the port number. Port 8083 is used as the default setting. If the port is already occupied, the port number can be changed.
   Enter the HTTPS port number. The default port for HTTPS is 8084.
   Reading the media traceback log can be optionally enabled.



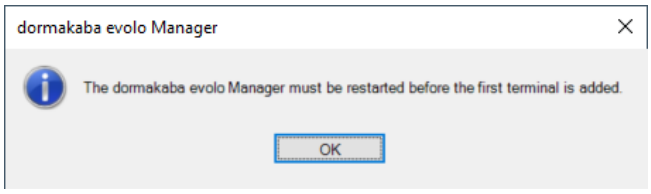
10. Click 'Next'.
    ⇨ If a firewall is activated on the computer, the desired ports in the firewall must still be enabled. The wizard does this for the user. The user requires administrator rights on the computer.



11. Click 'Enable ports in firewalls'.
    ⇨ The ports are enabled using a Windows command prompt. Press any key to close the window once the ports have been enabled.
12. Click 'Save'.
    ⇨ The settings are saved in KEM.
13. Click 'Finish'.



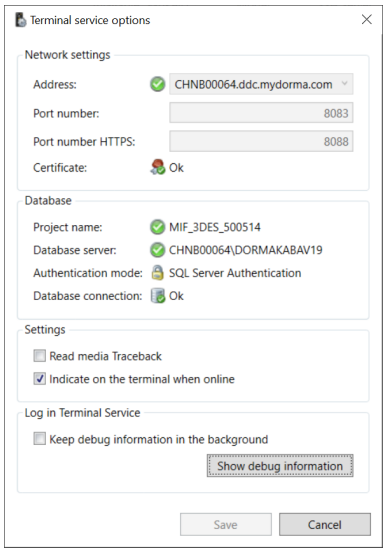
⇨ Before putting the first terminal into operation, close the evolo Manager and restart it to allow the changes to take effect.



⇨ The project is opened.

⇨ Check the results of the migration.

In the 'Terminals' tab of the options, check whether the set HTTPS port and the certificate are configured.



10 Access Manager

The evolo Service must be installed to use an Access Manager. See Install evolo Service [▶ 3.5].

The dormakaba Access Manager 92 00 K7 is a hardware access control device designed for commercial and industrial security systems. It is a network-connected access controller that is crucial to a physical security system connecting readers, doors, and management software. Its core function is to serve as an access control terminal that checks whether a media or credential (security card or smartphone via Mobile Access) has the required permissions, and if authorized, releases access to the user.

10.1 Prerequisites

To include an Access Manager in a project, the following conditions must be met:

- the evolo Service must be installed and configured, since it is required for communication between KEM and the Access Manager. See section Install evolo Service [▶ 3.5]. The version of the evolo Service that you install must match the KEM version.
- Network connectivity must be in place, including correct IP configuration and open ports (e.g., HTTPS 8086), so the device can be reached and verified.

  The Access Manager must be reachable and compatible, meaning firmware and communication checks must pass during setup.
- A valid license must exist for the Access Manager 92 00 K7 B-Client AC30, as this defines how many readers and antennas can be added.

10.2 Operation

An Access Manager unit must be implemented in your hardware landscape. To learn more about the physical on-site installation of an Access Manager, go to to https://portal.dormakaba.com/, section *Downloads*, and search for *Access Manager technical handbook*, where the process is described in detail.

Procedure

The main operation of an Access Manager is to connect readers, doors, and management software. You have to set it up and add it for your project as described in sections Set up the evolo Service to use the Access Manager [▶ 10.3] and Setting up KEM to use PIN-code-enabled devices [▶ 8.5].

Also see about this

Setting up KEM to use PIN-code-enabled devices [▶ 144]

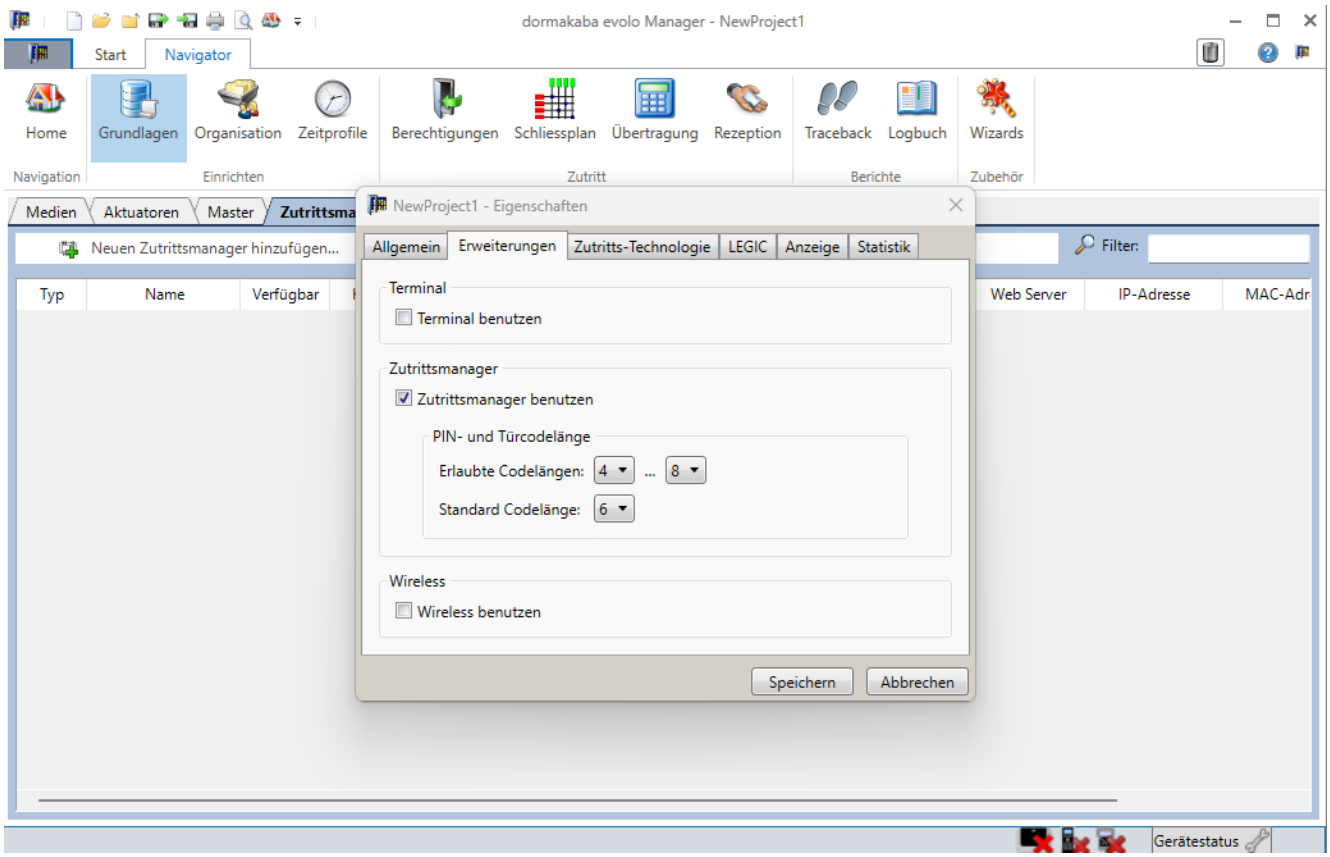
10.3 Set up the evolo Service to use the Access Manager

For more information, see chapter Access Manager.

To employ PIN-code-enabled devices in your project, you have to set up the evolo Service to use the Access Manager.

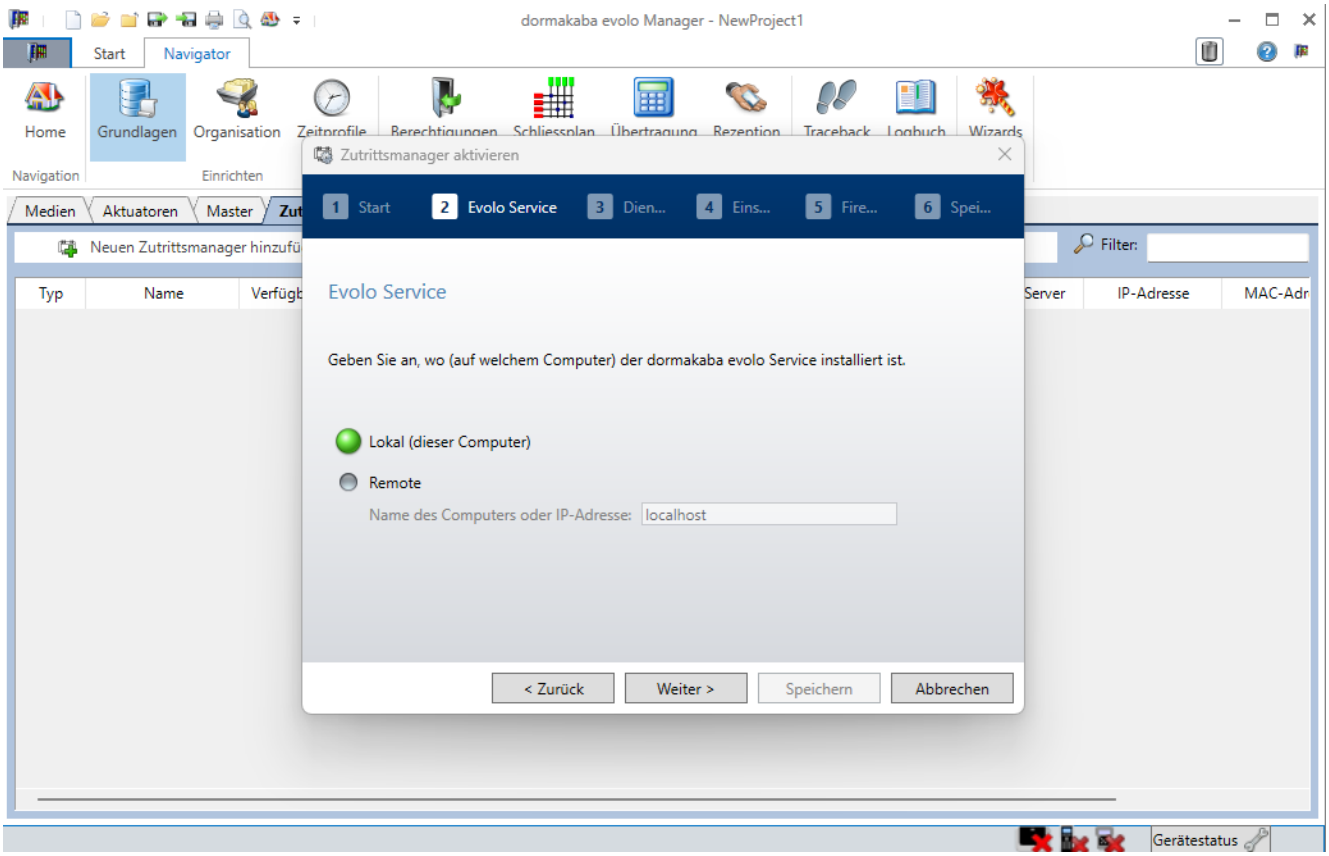
Start by creating a new device in KEM and entering its IP address, so that the system can locate it on the network. KEM then automatically checks communication with the evolo Service and verifies device compatibility, including firmware status. Once successful, the Access Manager is integrated and starts its initial synchronization, which may take a few minutes before it is ready for use.

Procedure

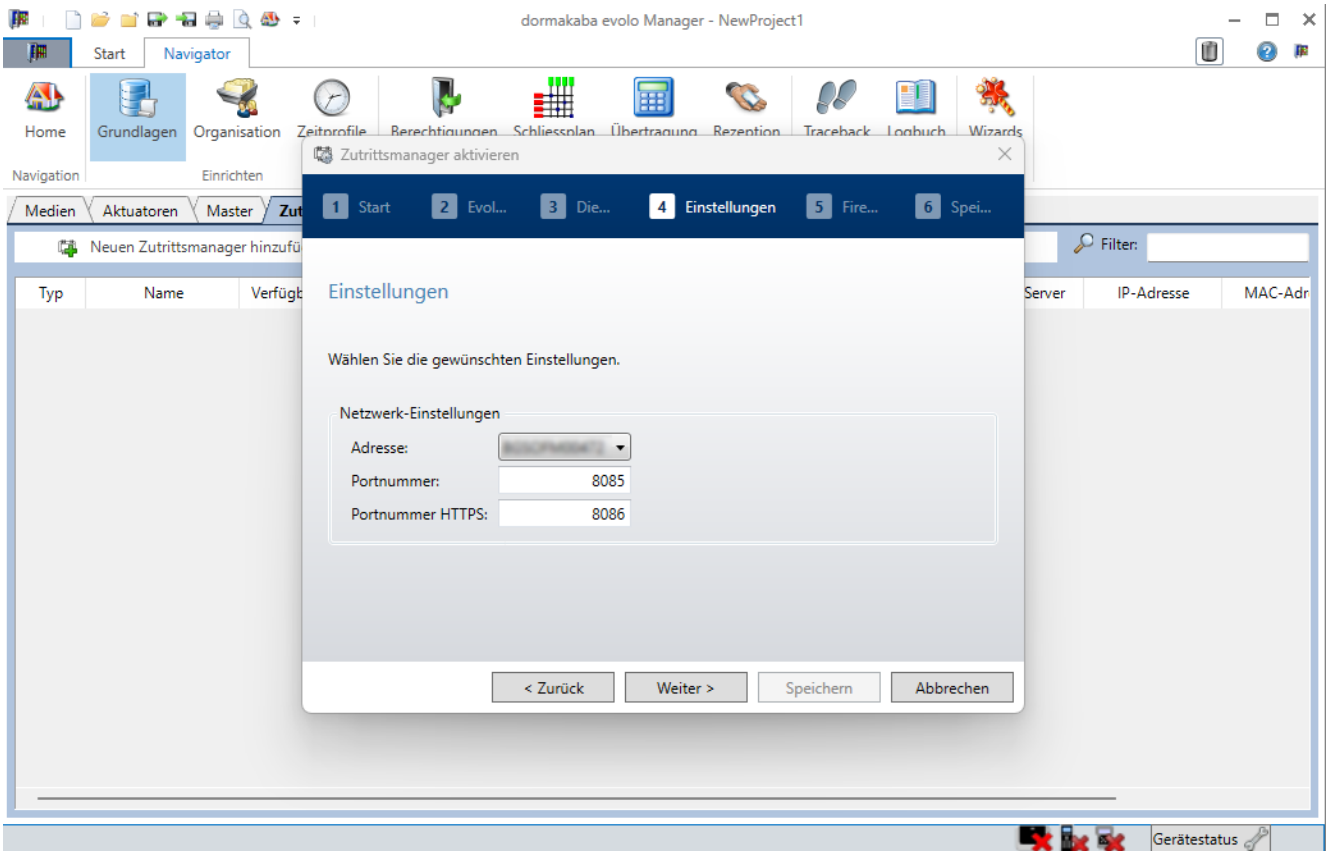


1. Starting from the KEM UI, press F4 to open the project properties and switch to the *Extensions* tab.
2. Enable the *Use access manager* checkbox. This triggers the *Activate access managers* wizard. Click *Next*.

In MIFARE projects, you must also add site keys when adding the Access Manager.



3. Specify where the evolo Service is installed. If it is remote, specify the hostname or IP address, and click *Next*.
   ⇨ A check for the presence and activation of the service takes place. When it completes, click *Next*.



4. Provide the network settings and parameters for the evolo Service. Add the address, and HTTP and HTTPS ports.

5. When prompted, unlock the ports in the firewall. You can use the provided option, which triggers a script that adds a rule in the firewall. Once you complete this step, click *Save*. This triggers a restart of the evolo service, which is necessary for operation.
6. Restart KEM for the changes to take effect.
7. **Optional:** After the Access Manager is set up, you are returned to the *Extensions* tab. At this time, you can also edit the minimum and maximum door code length and the default code length using the respective drop-down menus. You can also do this at a later time.
8. Click *Save* to close the changed project properties.

⇨ The Access Manager is now ready for use. If needed, you can proceed to add it to a project as described in Setting up KEM to use PIN-code-enabled devices [▶ 8.5].

Also see about this

Setting up KEM to use PIN-code-enabled devices [▶ 144]

11 Wireless

This section describes how to set up wireless components and put them into operation.
You can find additional information about using wireless here:

- Programmer 1460 user manual
- Wireless gateway 90 40 technical manual
- PG wireless planning guideline

11.1 Integrating a wireless gateway

If a gateway has already been configured for a project, it can be used in another project only after an INI reset.

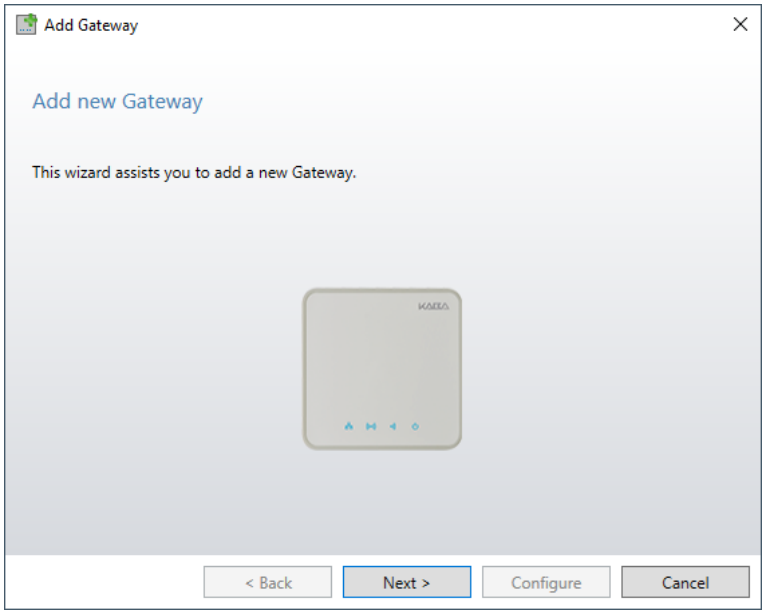
Prepare KEM:

1. Start the KEM software.
2. In the KEM software, open 'Project properties' (F4).
3. In the 'Extensions' tab, tick the checkbox 'Use wireless'.
4. Save the setting.
   ⇨ The tab 'Gateways' is added to the basics.
   ⇨ The menu 'Transmission' is added to the tab 'Actuators (wireless)'.

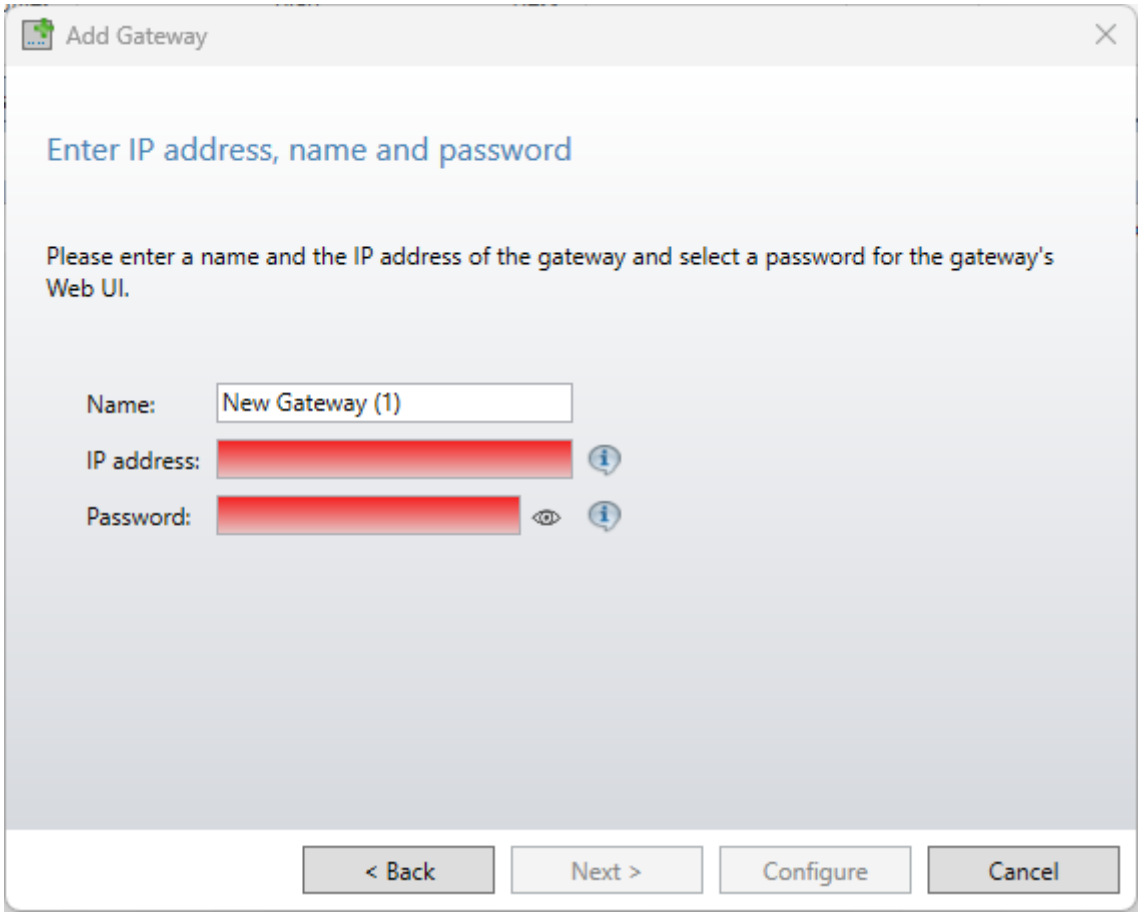
Add gateway to KEM:

✓ The IP address of the gateway is known.

1. Go to 'Gateways' tab.
2. Click on the 'Add new gateway' button.



3. Follow the wizard.



Enter the wired IP address of the gateway here.
If it is not possible to assign a fixed IP address to the wireless gateway, then the DHCP server must be parametrised so as to always have the same IP address assigned to a wireless gateway upon every network connection.

4. Parametrise the gateway.
   ⇨ The view in the 'Transmission' menu and 'Programmer 1460' tab changes to the 'Actuators (wireless)' tab.

11.2 Editing wireless components

Mixed mode via wireless is not yet supported by the wireless gateway.

11.2.1 Configuring components

Configuring components with the wireless option is similar to the configuration of standalone components.

In addition, please note:

- Wireless can only be selected for components that are operated in V4 mode.
  – In the 'Actuators' tab, in the 'Type' field, select E32x from the list.
- Allow wireless to be activated
- To use the CardLink update function via a remote reader, select 'CardLink update' from the 'Access mode' column.
  Under Legic, the remote reader must be given write authorisation to write the data to the media. See Issuing write authorisation (launching) [▶ 11.2.2]

11.2.2 Issuing write authorisation (launching)

(Only LEGIC)

A write authorisation is required in the following cases:

- Validating write-protected CardLink segments for CardLink applications.

Requirement

- A C2 security card is required for write authorisation.
- The component is in standard operation and is waiting for RFID input.

Procedure

1. Present the programming master.
2. Present the C2 security card for approx. 15 seconds.
   - ⇨ Lights up green during the process.
   - ⇨ Signal if successful: 3x beep
     If write authorisation has already been issued before with the same C2 security card, this is signalled immediately with 3 beeps.
   - ⇨ No signal: write authorisation has **not** been issued.
     Possible reasons
     - The C2 security card was removed too early from the RFID field.
3. The C2 security card was removed from the field.

11.2.3 S-Module, Pass-Lock or Escape-Return via wireless

Requirements
You must have at least the following firmware versions to be able to use the S-module, Pass-Lock or Escape-Return functions via wireless:

Component:	42.38
Wireless gateway:	4.10.0

The functions are configured in the properties of the component under 'Accessories'. See section.

11.3 Putting wireless components into operation

This chapter describes how wireless components can be put into operation and parameterised using the wireless gateway.

Action steps need to be performed at the components and at the gateway in order to put the components into operation.

11.3.1 Starting wireless commissioning

Start the wireless commissioning of the gateway.

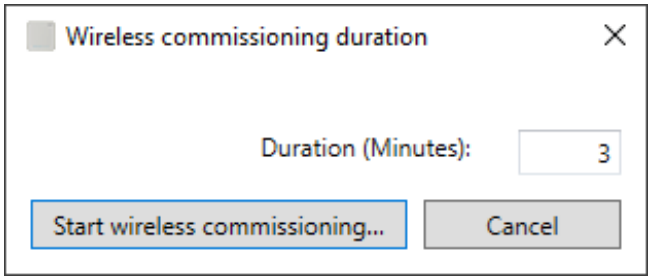
So that the components can be connected with the gateway, wireless commissioning must be started in the gateway. Commissioning can be started as follows:

- With the KEM system software
- In the web interface of the gateway

For operation with multiple gateways, always start wireless commissioning on only one gateway.
The components could connect with an unwanted gateway.

Commissioning with KEM

1. Start the KEM system software.
2. Go to the 'Gateways' tab in the 'Basics' section.
3. Select the gateway.
4. Open the context menu of the selected gateway.
5. Activate 'Start wireless commissioning...'.



6. Set duration of commissioning (in minutes).
   Time necessary for adding/commissioning the components.
   ⇨ The components can be connected to the gateway during this relevant period.
7. 'Start wireless commissioning...'
   ⇨ The component must be connected to the gateway within the set relevant period.
8. Connect the component using the programmer [▸ 11.3.2] within the set relevant period.

If it was not possible to commission all the necessary components within the relevant period set, the process can be repeated.

Commissioning via web interface

The web interface of the gateway can be started via the file manager or via KEM.

In the file manager, the gateway must be listed under network.

1. Select the gateway for commissioning the file manager.
2. Start the web interface of the gateway.

⇨ The web interface of the gateway is started.

The gateway is created and configured in KEM:

1. Select the gateway for commissioning in KEM.
2. With right-click, open the context menu of the selected gateway.
3. Select the "Open WebUI" entry.

⇨ The web interface of the gateway is started.

After starting the web interface of the gateway:

1. Login to the gateway as administrator.
2. Call up the 'Wireless commissioning' function.
3. Set the relevant period for commissioning.
   ⇨ The components can be connected to the gateway during this relevant period.
4. Start wireless commissioning.
5. Connect the component using the programmer [▸ 11.3.2] within the set relevant period.

If it was not possible to commission all the necessary components within the relevant period set, the process can be repeated.
Components already connected to the gateway remain connected.

11.3.2 Connecting wireless components

Connecting wireless components with a wireless gateway:

Prerequisites

- The component is parametrised for wireless functionality.
- The wireless gateway is parametrised in the system software.
- The wireless gateway is connected to the system software.

Procedure

1. Start wireless commissioning [▶ 11.3.1] in the gateway.
   ⇨ The following steps have to take place within the time period set there:
2. Find the component to be connected to the programmer.
3. Log onto the component with the programming master.
4. Select the 'Actuator/wireless' menu in the programmer.
5. Select the 'Connect' menu item.
6. Start the connection process with 'Enter'.
   ⇨ These steps then run:
   - Look for network...
   - GW found
   - Commissioning...
   - Connected to GW
7. Check connection status in the 'Wireless' menu.

⇨ Wireless commissioning is complete and the component can be operated wirelessly by the system software.

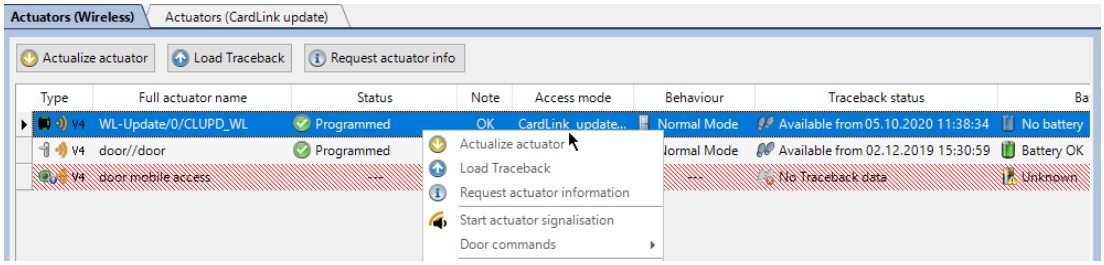
11.4 Updating wireless components

The component is initialized and connected wirelessly.

Procedure

1. In the 'View' menu, select the 'Transfer' area.
2. Go to the 'Actuators (wireless)' tab.
3. Select the component to be updated.
4. Select 'Update actuator' in the context menu.

⇨ The selected component is updated.



11.5 Downloading traceback of wireless components

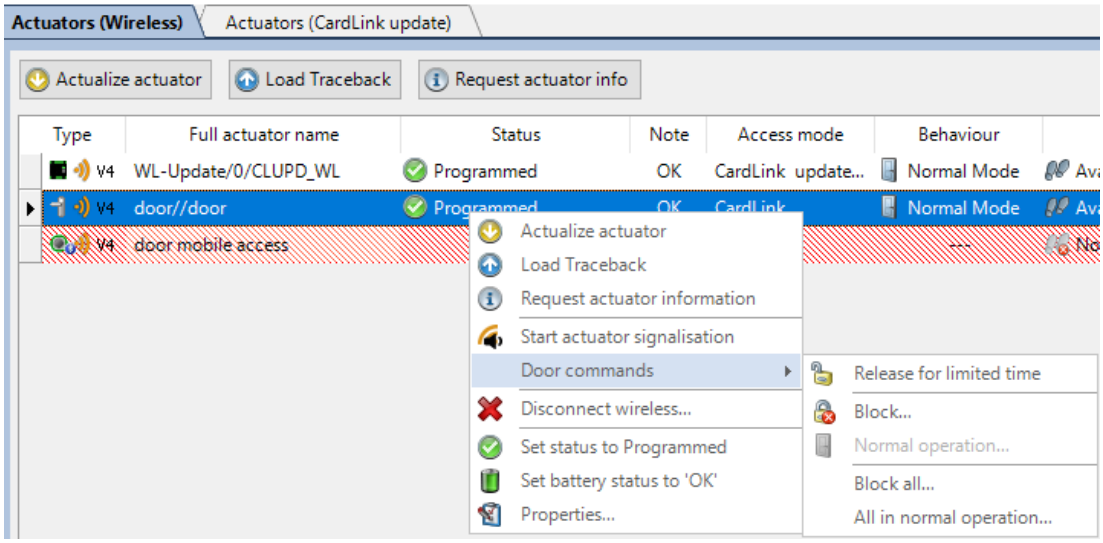
The components save their traceback data in the internal memory.

In the 'Transfer' view, you can transfer the traceback data to the KEM software. See [▶ 6.12]

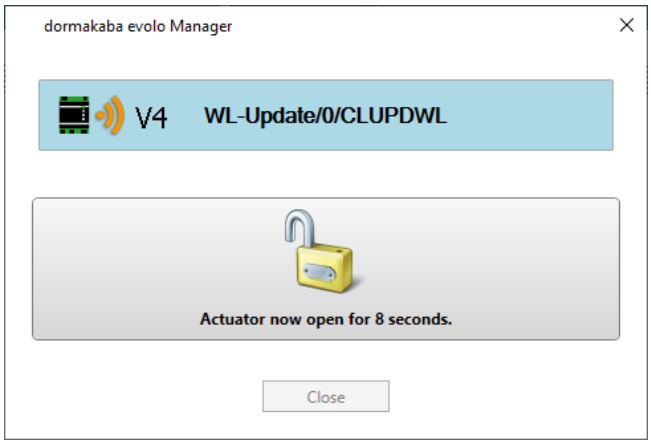
11.6 Opening and closing components via wireless

11.6.1 Releasing components with a time limit

1. In the 'View' toolbar, open the 'Transmission' area.
2. Go to the 'Actuators (wireless)' tab.
3. Select the component.
4. Open the context menu.
5. Open the 'Door commands' menu item.



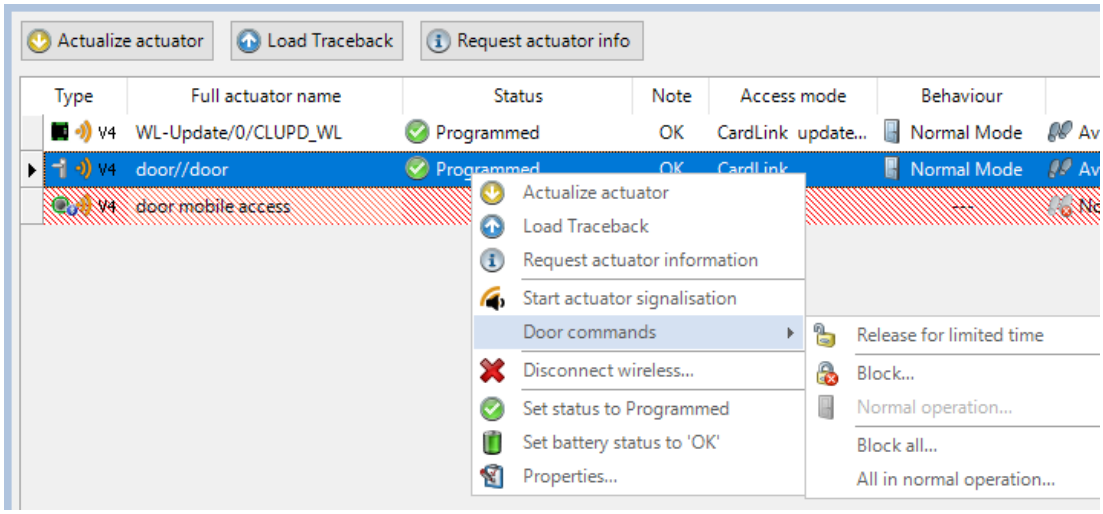
6. Select the menu item 'Release for limited time'.
   ⇨ The command is sent to the component.
   ⇨ The component opens for 10 seconds.



7. Carry out the action at the component. After the set time interval expires, the component reverts to standard operation.

11.6.2 Blocking components

1. In the "View" toolbar, open the 'Transmission' area.
2. Go to the 'Actuators (wireless)' tab.
3. Select the component.
4. Open the context menu.
5. Open the 'Door commands' menu item.

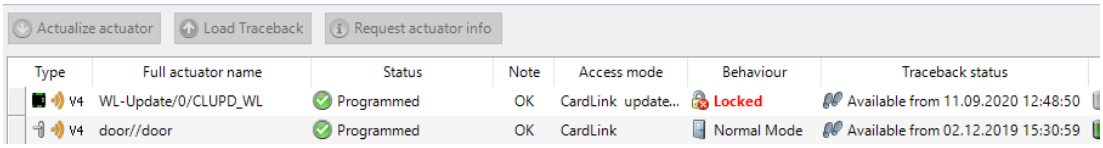


6. Select the menu item 'Lock ...'

⇨ The request is sent to the component.

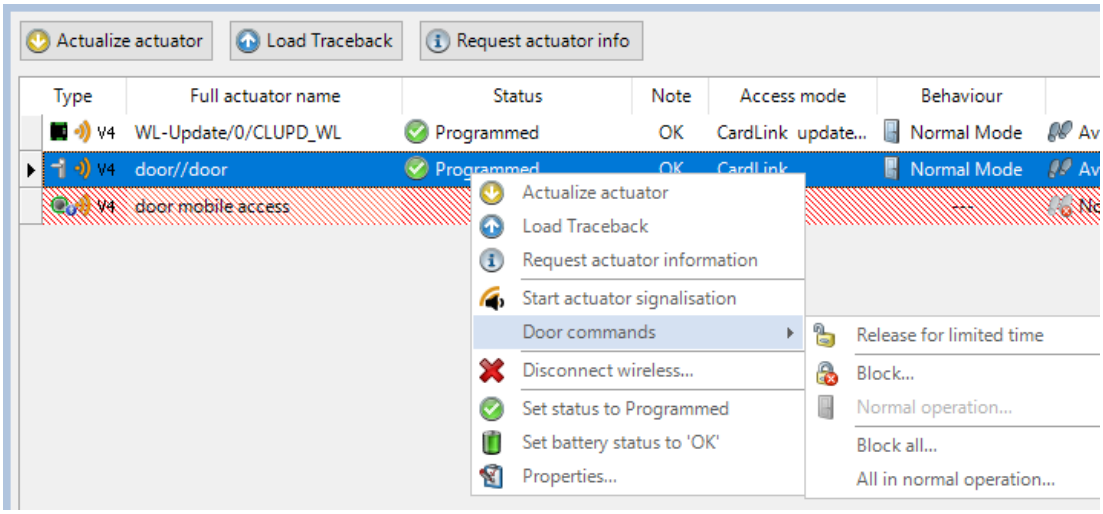
⇨ The component is locked.

To unlock, consult the following section [▶ 11.6.3].



11.6.3 Setting components to normal operation

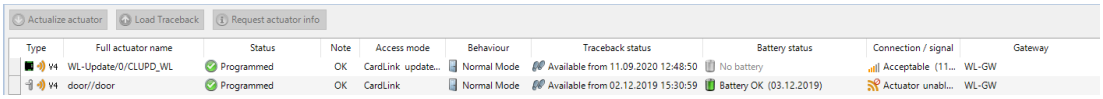
1. In the "View" toolbar, open the 'Transmission' area.
2. Go to the 'Actuators (wireless)' tab.
3. Select the component.
4. Open the context menu.
5. Open the 'Door commands' menu item.



6. Select the menu item 'Standard operation ...'

⇨ The request is sent to the component.

⇨ The component goes into standard operation.



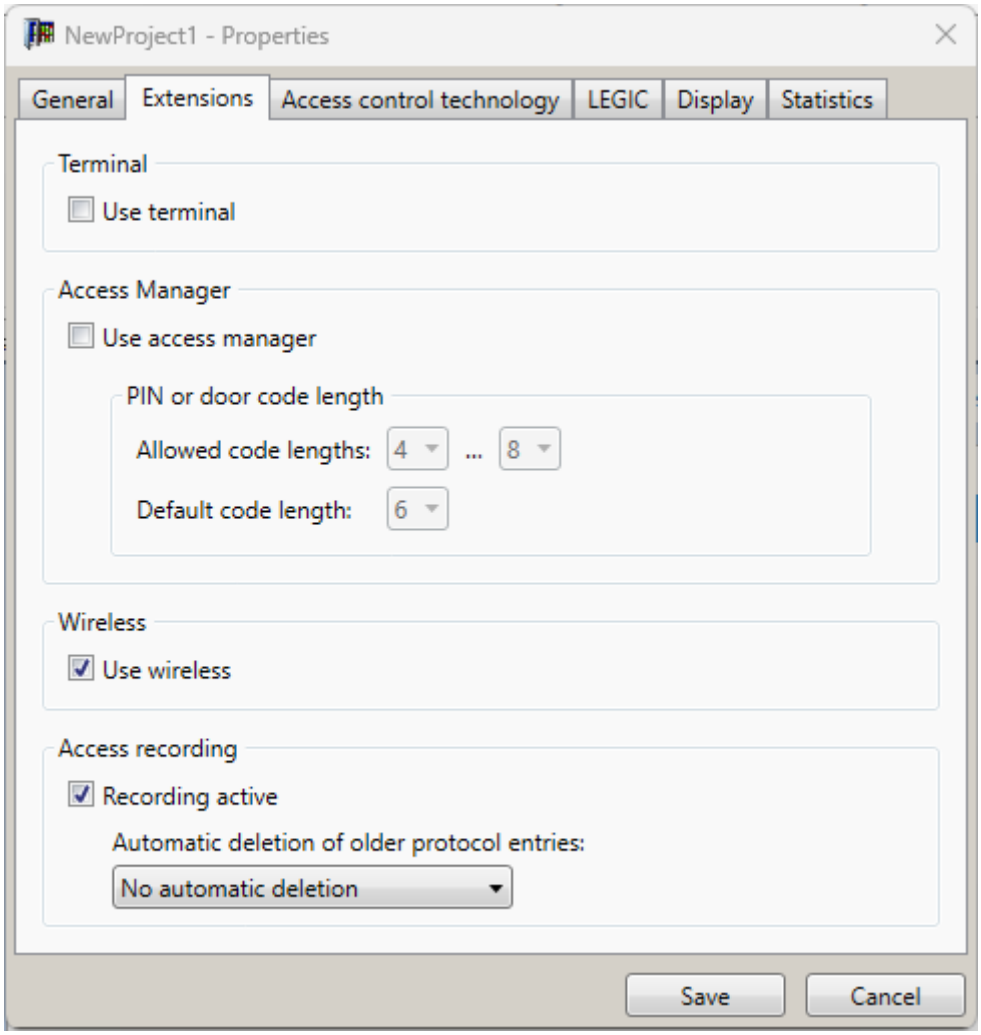
11.7 CardLink update

Mixed mode via wireless is not yet supported by the wireless gateway.

The CardLink update function can be used wirelessly to update validations and authorisations on user media.
This should be done using a remote reader with wireless function. This reader is then referred to as a wireless update reader.

Carry out write authorisation when using under LEGIC at remote reader.

Requirements
The following settings apply in the project properties:



Settings of a reader used:

Components/devices used for the CardLink update must have the following parameter settings:

- 'Actuator type' is remote reader E320 (wireless)
- Allow wireless to be activated
- One of the following access modes is selected:
  - CardLink update with access
  - CardLink update without access (with validation)
- The component is connected via a wireless gateway as described under Wireless.

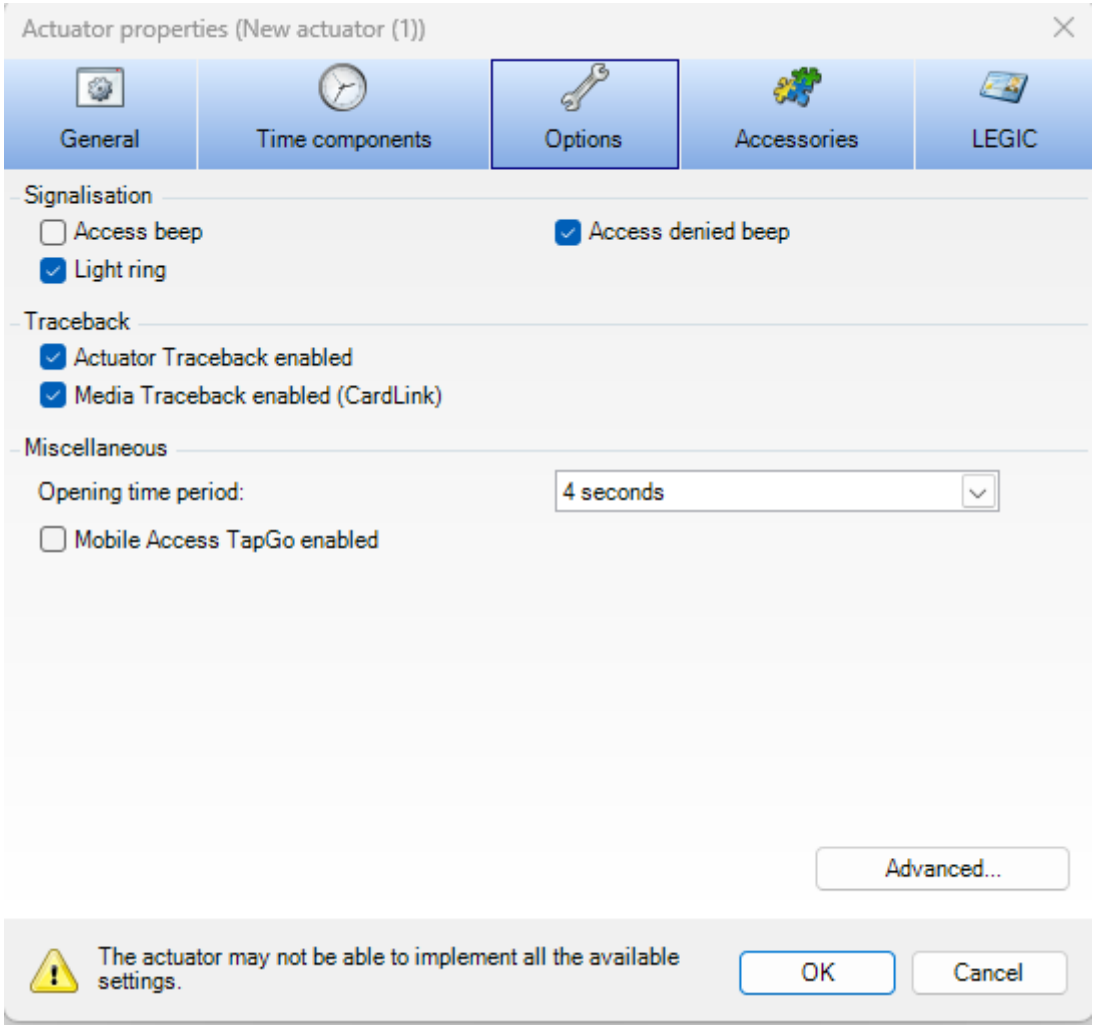
The selection of the behaviour in case of a connection interruption has the following meaning:

- CardLink update always active:
  Prepared rights can always be picked up.
- If there is no connection, the CardLink update becomes inactive after the selected time:
  Prepared rights can still be picked up until the set time has expired.

The corresponding CardLink data must have been fully transferred to the update reader at the time the connection was interrupted.

Settings in the properties of the component

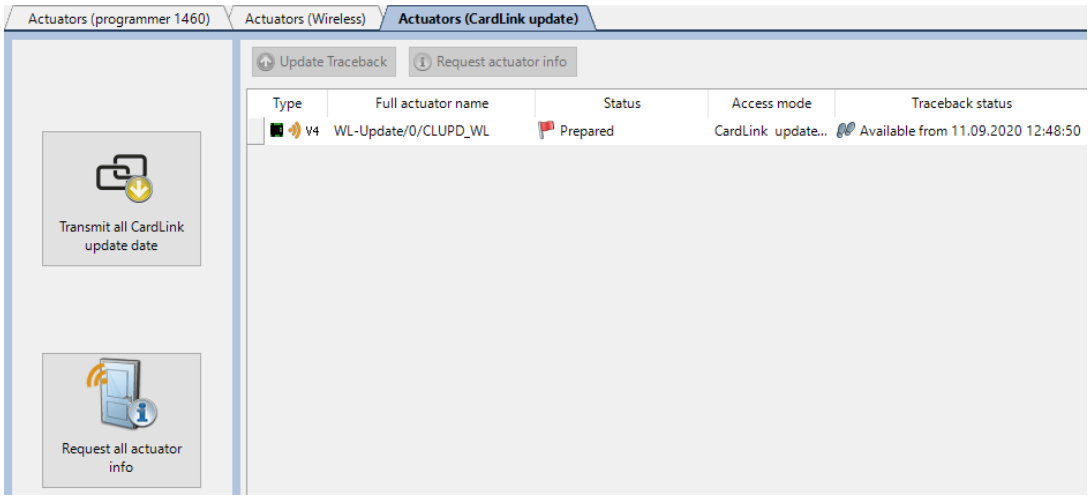
The 'CardLink update reader' checkbox is activated: the component reads back the status data of the visited component from the user media.



Updating the data records on the wireless update reader

A maximum of 3500 data records of user media can be sent to a CardLink update reader.

1. In the view, go to the 'Transfer' menu.
2. Go to the 'Actuators (CardLink update)' tab.
   ⇨ This window only shows the components used for the CardLink update.



3. Click the 'Update all CardLink update data' button.

⇨ After completing the transfer activities, the message 'On the reader' is displayed.

A connected terminal (not wireless) must be updated separately, as described in the Terminal section.

11.8 Wireless firmware update

The wireless firmware update enables a firmware update/downgrade of one or more components using the wireless gateway.

The components must be connected to the KEM via a wireless gateway.

Requirements

Each component must meet the requirements.
Components that do not meet these requirements will not be included in the wireless firmware update.

- Firmware version of the wireless gateway: 4.8.1 and higher
- Firmware version of the component: 42.34 and higher
- 'Battery Low' is not indicated.
- 'Allow wireless' is activated.
- The component is connected to the wireless gateway.
- New firmware files are available and the path is known.

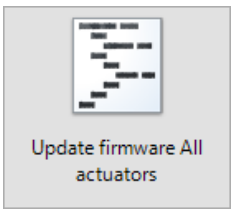
Symbols used
Symbols used in the update wizard summary:

Symbol	Meaning
	OK Update possible
	OK No update necessary
	Downgrade A previous firmware version is being used
	Update not possible

11.8.1 Update wizard

The update wizard is started from the 'Transfer/Actuators (wireless)' or 'Transfer/Actuators (CardLink update)' menu. The wizard assists with the selection of the firmware files and with transferring the files to the wireless gateway.

Updating the firmware of all components:

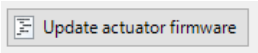


This button launches the update wizard for all displayed components. There is no need to select the components.

After starting, follow the update wizard's instructions.

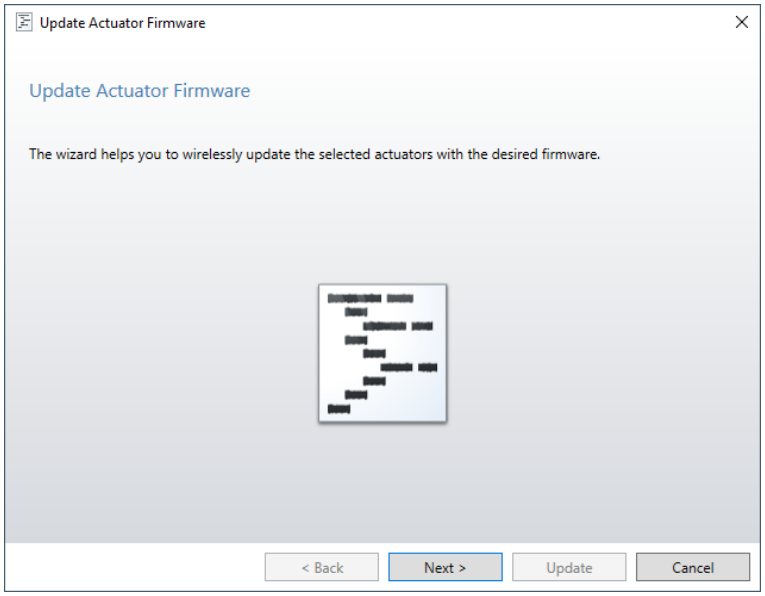
Update the firmware with component selection and Multiselect:
In the 'Transfer/Actuators (wireless)' or 'Transfer/Actuators (CardLink update)' menu, select the components with firmware that needs updating.

- After selecting the components, select the 'Update actuator firmware' button to launch the update wizard.

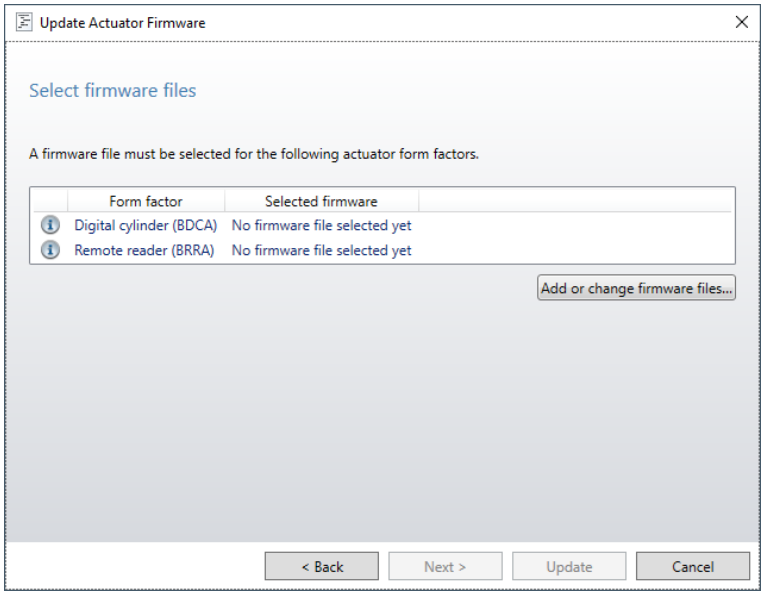


This button launches the update wizard for one or more selected components

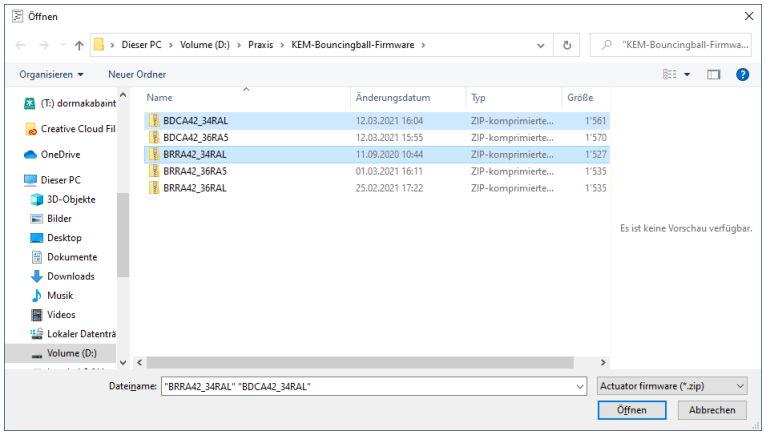
Follow the wizard's instructions.



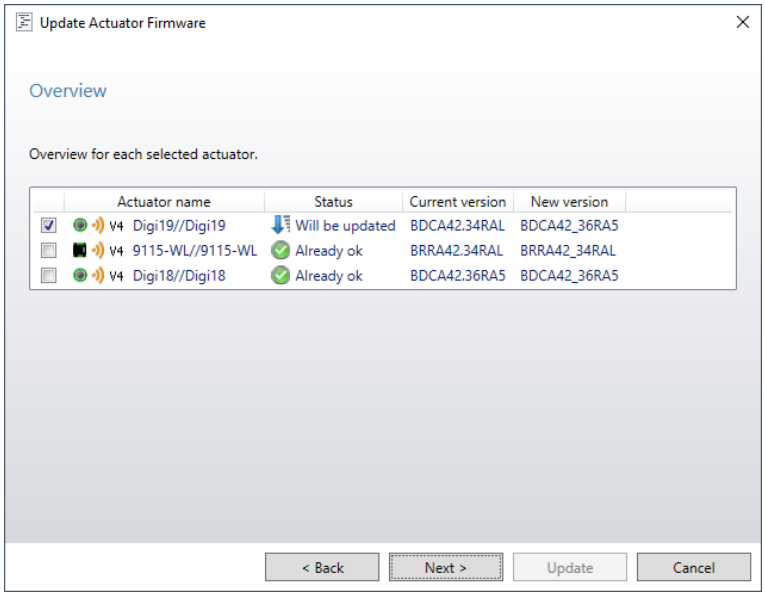
Select firmware files
Select the new firmware files for the components.
Several components with the same form factor are grouped together in one row.



A firmware file must be selected for each form factor in the list.



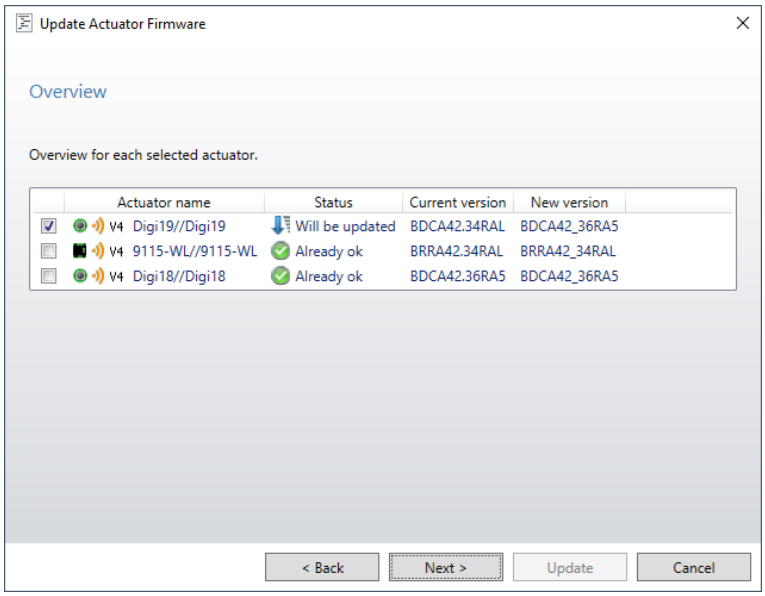
If all firmware files for all form factors are in the same folder, multiple selections are possible.

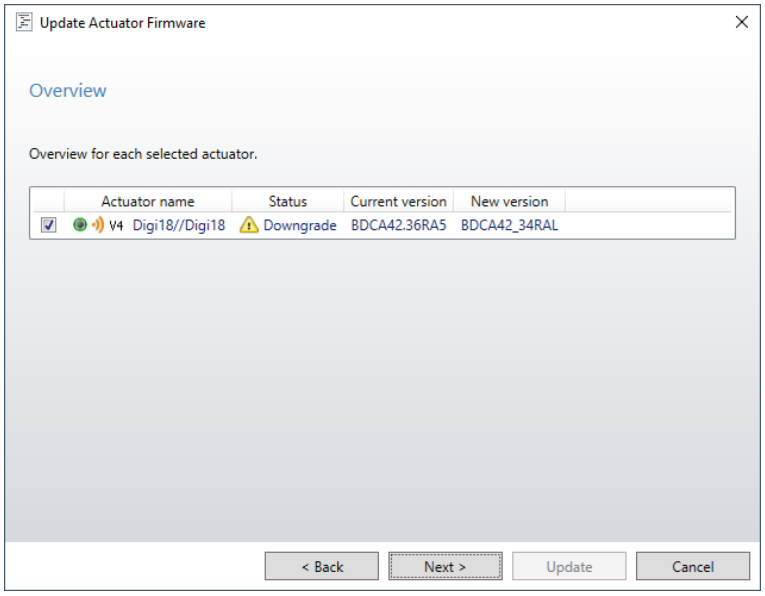


Overview/Control

This step provides an overview of all selected components with their current firmware version and the firmware version to be installed. The checkbox in front of the component shows whether this component will be considered in the subsequent firmware update.

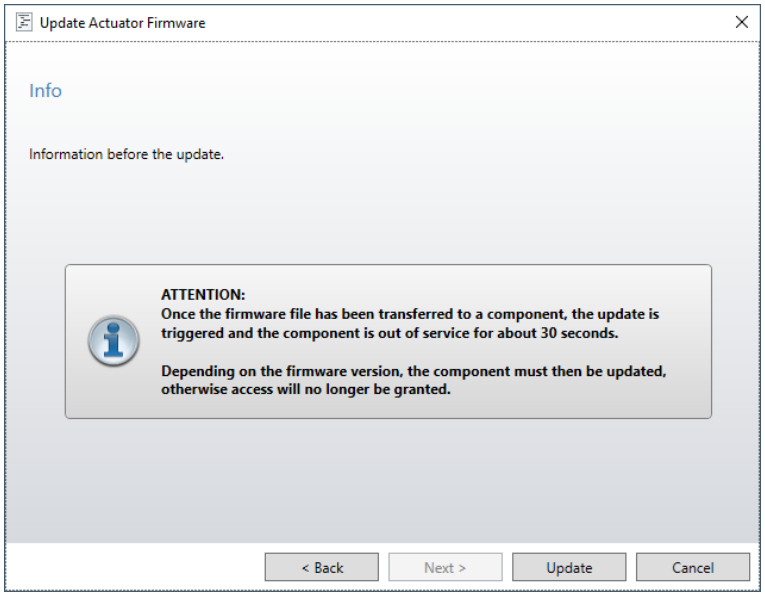
All checkboxes are activated by default. To exclude a component from the update, deactivate the checkbox.





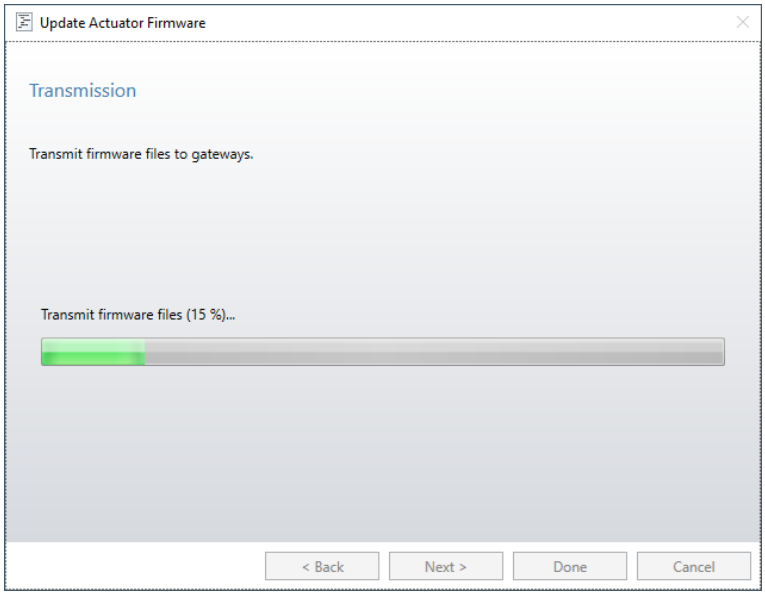
Components whose checkbox is not activated will not be considered during the update.

Important information before starting the update

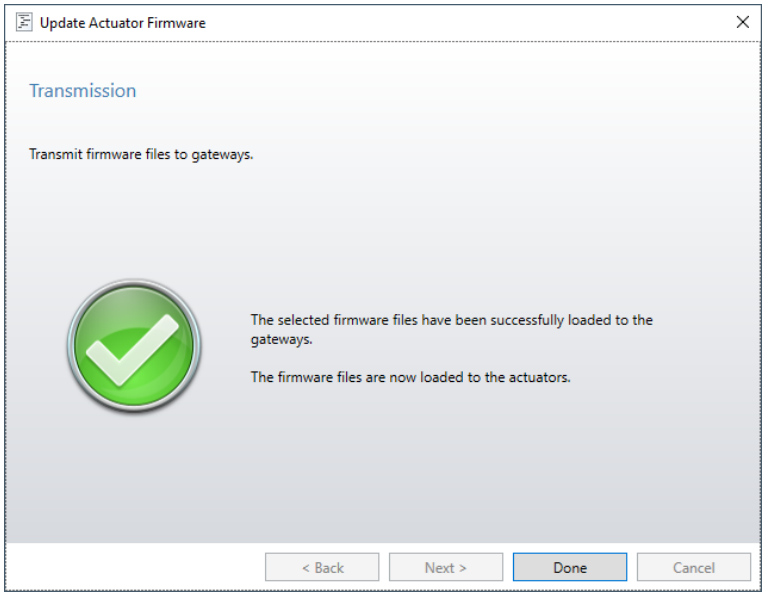


Once the update process has started, it can only be cancelled in the KEM using the component's context menu.

Selecting the 'Update' button starts the update process.



The transfer of files to the wireless gateway cannot be cancelled.



Depending on the firmware used, the configuration data/write authorisation in the component will be lost. The component must then be reconfigured by the KEM after the update.

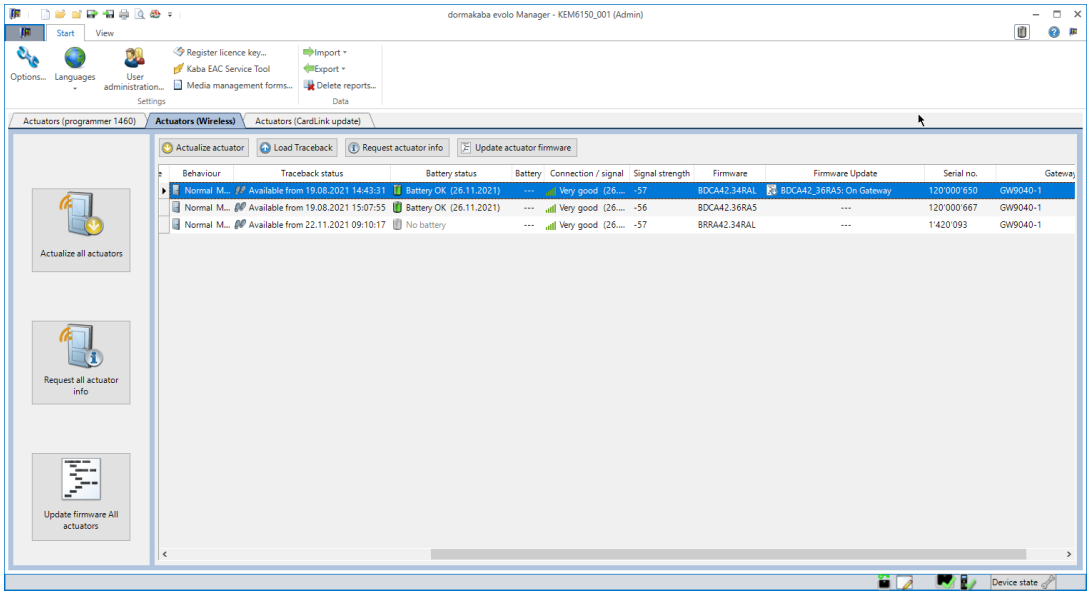
Transferring the firmware files from the wireless gateway to the component takes some time.

Installing the firmware on the component sets the component out of service for approximately 30 seconds.

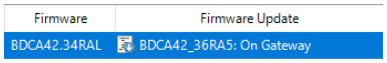
- The transfer and installation of the firmware files to the components is displayed in the KEM in the 'Transfer/Actuators (wireless)' menu.
- You can use the component's context menu to cancel the update process for that component at any time.

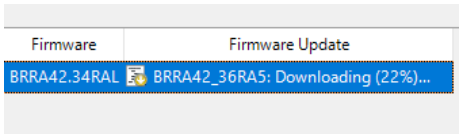
After the complete transfer to the wireless gateway, the files are distributed and installed on the components. The update wizard is no longer required for this. Select 'Finish' to exit the wizard.

Progress bar/information about the firmware

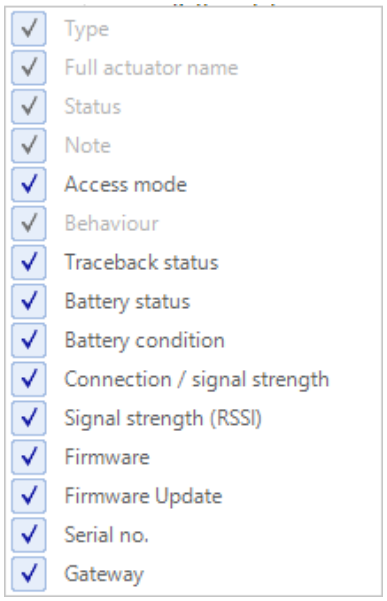


In the 'Transfer/Actuators (wireless)' or 'Transfer/Actuators (CardLink update)' menu, information on the current firmware, the new firmware and the firmware update status is displayed in the 'Firmware' and 'Firmware update' columns.





If the 'Firmware update' column is not visible, then select the column via the context menu of the column headings to display. Right-click in a column heading to display the context menu.



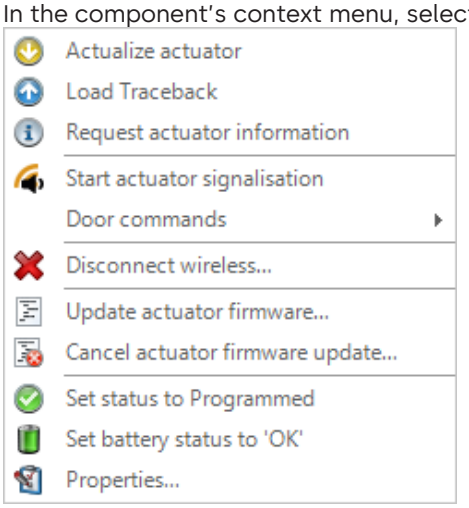
If a component is not reached by the wireless gateway within 24 hours, the update must be initiated again.

Cancel firmware update

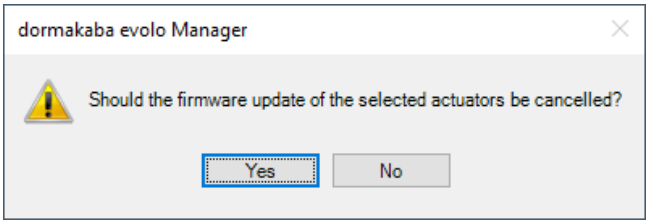
Options for cancelling the firmware update:

- Cancelling in KEM in the 'Transfer/Actuators (wireless)' or 'Transfer/Actuators (CardLink update)' menu:

– In the component's context menu, select the entry 'Cancel actuator firmware update'.



– Confirm the cancellation.



– The transfer of the firmware to the component is cancelled and the new firmware is not installed.
No modifications are made to the component.

12 Data

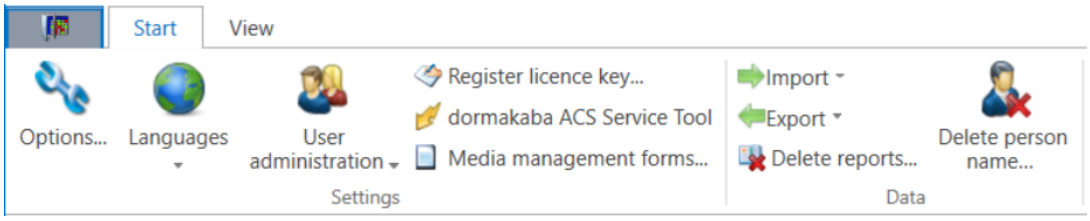
12.1 Importing and exporting data

The following options are available for the exchange of system data.

Import	
Import project	Imports a KEM project file.
Kaba import file (.kif)	System file which can be requested from dormakaba. It saves registering the installed components manually in a master key system.
Media list (.txt)	Media data imported from a text file
Actuators list (.txt)	Actuator data imported from a text file
Staff list (.txt)	Staff data imported from a text file
Calendar data (.txt)	Calendar data imported from a text file
Digital keys	Imports digital keys from voucher documents (PDF). To do this, a wizard is started that assists with the import process. For further information, see Importing digital keys.
Export	
Export project	Exports the KEM project file.
Export anonymised project	Anonymises and exports the KEM project file. Additional information Export anonymised project [▶ 12.2].
Media list (.txt)	Media data exported as a text file
Actuators list (.txt)	Actuator data exported as a text file
Staff list (.txt)	Staff data exported as a text file
Calendar data (.txt)	Calendar data exported as a text file

Importing example

1. In the 'Start' toolbar, open the 'Import data' menu.
2. Select e.g. 'Media list...' from the list.



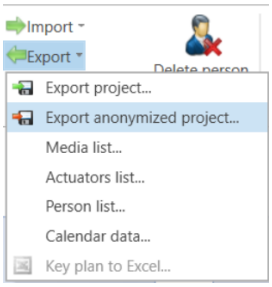
3. Select the key plan with the media via the drop-down menu.
4. Click the 'OK' button.
5. Search for the media list on the corresponding drive and import it.

Tip:

If the import format is not clear, first carry out an export to analyse the format.

12.2 Export anonymised project

The wizard anonymises a project and exports it to a specified target folder. The project in KEM will not be changed.
This function can be helpful for Support, for example.



The following will be deleted or replaced:

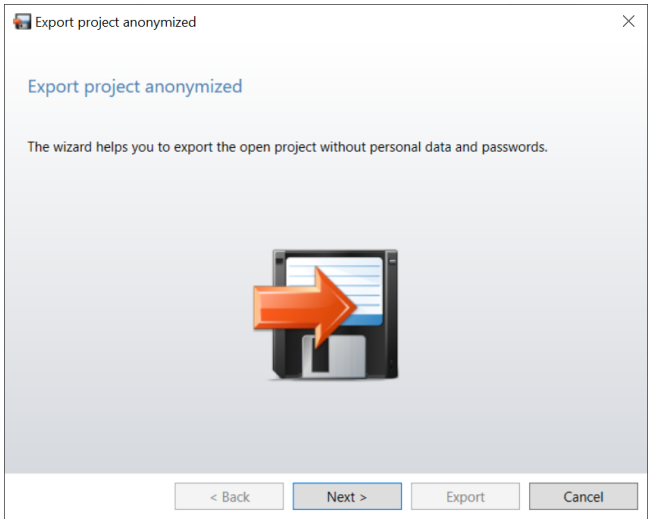
- User management is deleted.
- Gateway passwords are deleted.
- Personal names of persons are replaced with the database ID.
- Staff data (e.g. additional fields, telephone numbers) will be deleted.
- Personal names in log data are replaced with 'Deleted'.
- Personal names in protocol data are replaced with 'Deleted'.
- Personal names in traceback data are replaced with 'Deleted'.

Requirement

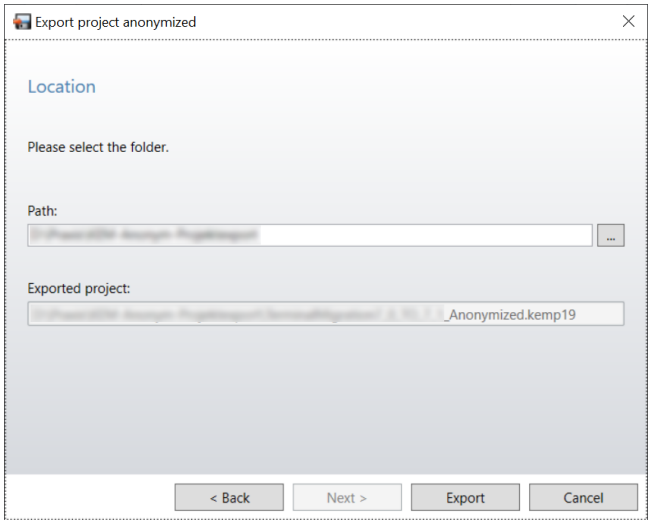
- If user administration is active, the user is registered as an administrator.
- If user administration is not active, the function is available.
- The project to be exported is open.

Procedure

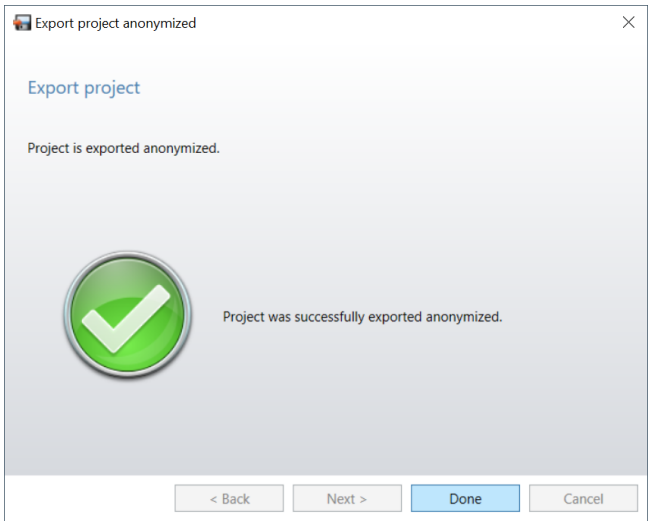
1. Click 'Export' in the 'Start' menu.
2. Click 'Export anonymised project'.
   ⇨ The wizard launches.



3. Click 'Next'.



4. Select the path to the target folder.
   ⇨ The file name of the exported project is displayed in 'Exported project'.
5. Click 'Export'.
   ⇨ The project is exported.



6. Click 'Finish'.
   ⇨ The wizard closes.

12.3 Adjusting properties after migration to the project

Various functions are no longer available after migration of projects or have modified properties. For existing projects, a copy is always made. The copied project file is then called "ProjectName_Copy".

The following generally applies:
• The information on the time zones must be reassigned. (The time zone set on the computer is used as the "default" time zone.)
For version KEM 4.4, the following applies:
• New temporary master Bs cannot be created. The existing temporary master Bs can continue being used and updated.
For version KEM 3.2, the following applies:
• The OKS functions, such as modifications, TwinTime, TwinTime Terminal, are no longer supported.
• Manual programming can no longer be turned off for individual components. It can only be set in the project properties. After migration, "Disable keys" is deactivated for all components.
• Passive components are no longer supported.

12.4 Delete reports

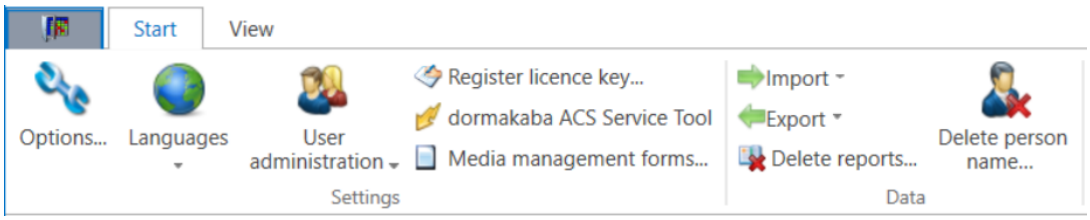
Delete logbook and traceback entries.

All entries with the displayed date and older entries are permanently deleted. In the interest of security, we recommend creating a security copy of the project before issuing this command.

Export the KEM project before deletion.

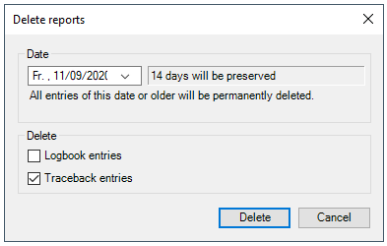
Example:
In this example, the older traceback entries including the entries from 09/03/2017 must be deleted.

1. In the 'Start' toolbar, open the 'Delete reports' menu.



2. Select the date.
3. Activate the tick in the traceback entries checkbox.
4. Click on the 'Delete' button.

⇨ The traceback entries with this date and older entries are deleted.



13 KEM operator

The KEM operator is a simplified user interface for the KEM software. However, this also means there are some limitations in terms of functionality.

13.1 Limitations

Restrictions to functions	
Access mode	The access mode for all components applies to the entire CardLink or whitelist project.
Locking plan	Projects with multiple locking plans are not supported.
Mechanical system	Projects having only mechanical components are not supported.
Time profiles	Only strictly V4 projects (MIFARE or LEGIC advant) are supported.
User administration	Not provided.
Front desk	Not provided.
Logbook	Not provided.
Traceback	Not provided.
Organisation	Persons can be registered and used with surname and first name. Other personal information is not provided.
Holidays/special days	Cannot be changed.
Validation	The following validation types can be used: – Duration in days and hours – 24 hours (one day) – End time – “Always”

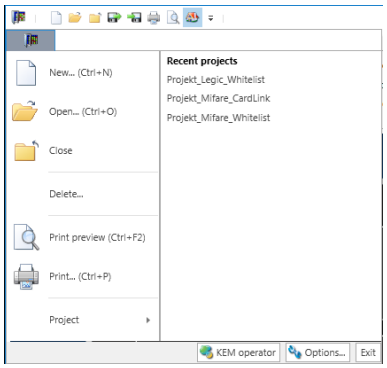
13.2 Creating a project

Security cards must be read in for a Whitelist project with CID (Card ID) to be created or a CardLink project.
These cards are as follows depending on the media type used:

- Security card C for use with MIFARE media
- Security card C1 or C2 for use with LEGIC media.

Procedure

1. Open the context menu in the toolbar on the left next to the '**Start**' tab.
2. Click on the 'KEM operator' button.



3. Open the context menu next to the 'Start' tab.
4. Open the 'New...' menu. (Ctrl + N).
5. Follow the instructions in the wizard.
6. In step 2, select the project type.
7. Follow the instructions in the wizard.
8. Conclude the process by clicking on 'Finish'.

⇨ The project has been created.

⇨ The wizard closes.

13.3 Creating a programming master

A programming master is needed for administrator access to standalone components (actuators). [▶ 6.3.2.1]

13.4 Wizards

Update programmer

	Wizard for transferring the key plan data to the programmer.

Lost media

	This wizard helps you take the necessary steps to keep the site secure. **Note:** The key plan/project must already be present on the programmer.

Reconfirm service medium

	Status data of the components are read into the project by the service medium using the wizard.

Add media

	This wizard helps you add additional media.

Edit components

	With this wizard, the user can - See the list of components - Edit the list of components - Add new components

Time profiles

	This wizard helps you create, modify or delete a time profile.

Create new service medium

	The wizard helps create a service medium for CardLink. The service medium is needed to disable individual IDs at certain components.

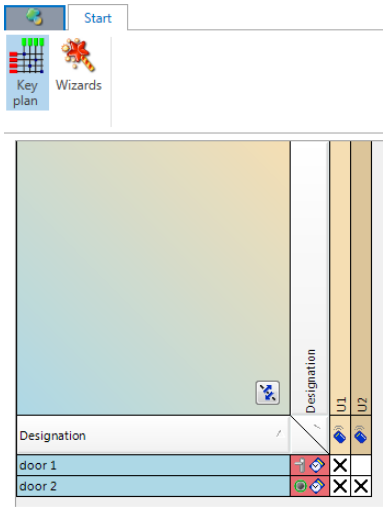
Configure CardLink

	This wizard helps define the basic configuration for CardLink. **Note:** The components must already have been created in the project. - Define validation-authorised components - Define the validation period

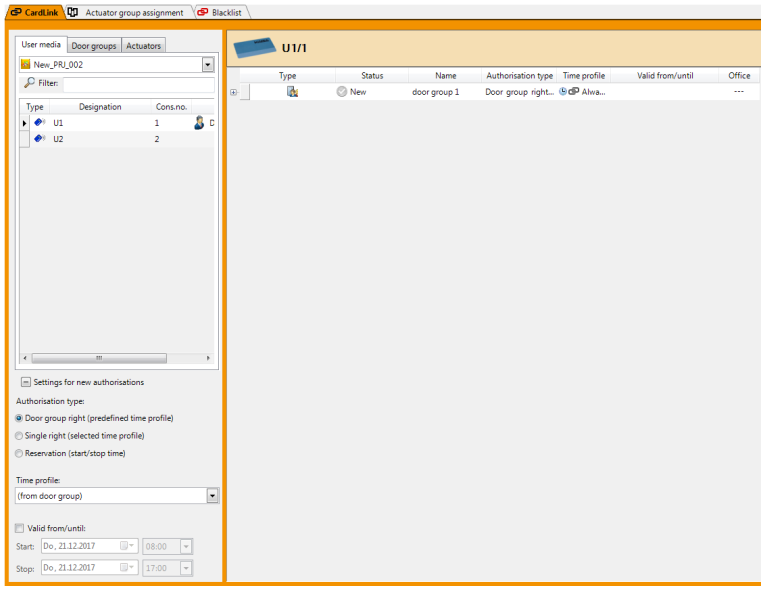
13.5 Operation

Procedure

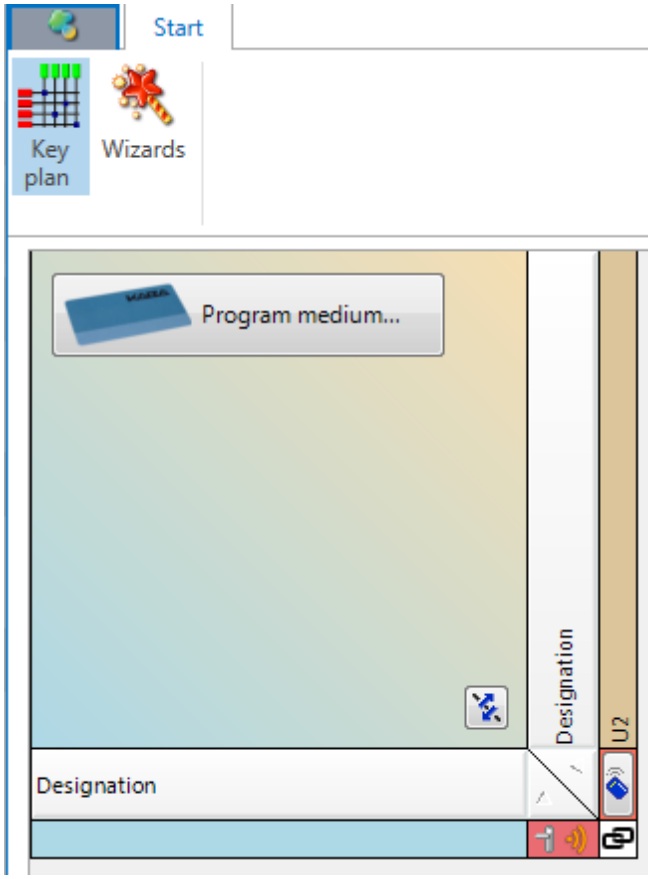
1. Activate the desired assignment by clicking the corresponding grid.



2. Assign the authorisation type and the time profile.
3. Click on the 'OK' button.



4. Place a medium on the desktop reader.

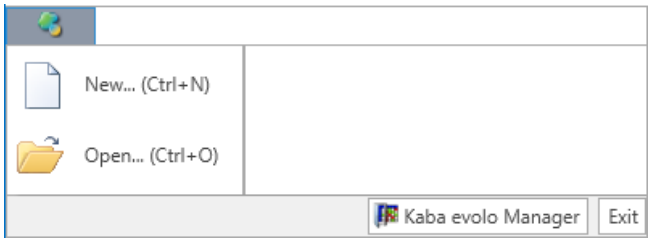


5. Click on the 'Program medium...' button.
   ⇨ The authorisations are written onto the medium.

After the first configuration of the KEM software, as well as upon changes to the time profiles and components, the updates must be transferred. With the **Update programmer** wizard [▸ 13.4], the changed data are transferred to the programmer. Next, the components are updated with the programmer.

Switch from the KEM Operator to KEM software or quit the program

1. Clicking the 'dormakaba evolo Manager' button in the 'File' menu changes the view to the start screen of the KEM software.
2. The 'Exit' button closes the KEM software.



14 Reception

The Front Desk function facilitates the assignment of individual authorisations. These are assigned to individual or multiple media. The process is not connected to the user. Prepared rights for selecting components and door groups are transferred onto the medium with a selected time profile.

The Front Desk function is available for CardLink and for Whitelist.

14.1 Process with CardLink

In just a few steps, media can be programmed and issued or returned.

Media issue

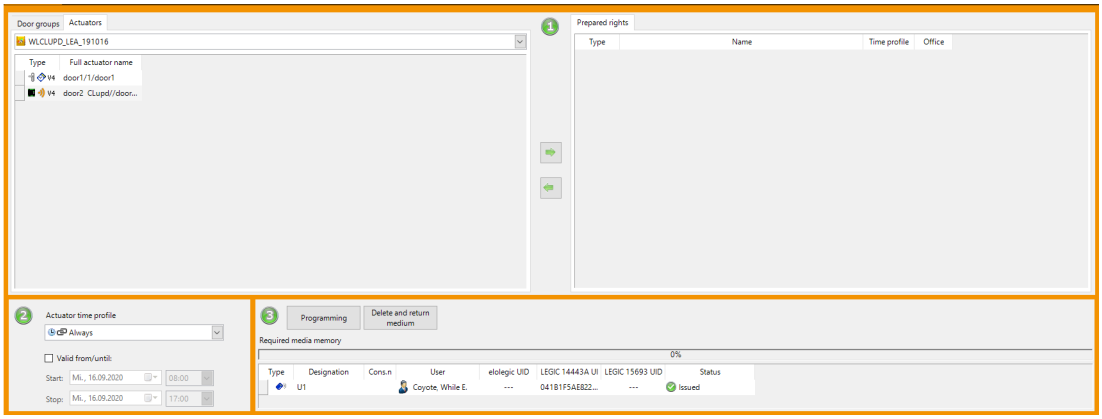
1. Move the door groups and/or components to the “Prepared rights” tab using the “Arrow” button (in the middle).
2. Assign a time profile and/or a validity period.
3. Place the medium onto the desktop reader and click on “Program”.

⇨ The data are written onto the medium.

Media return

1. Place the medium on the desktop reader.
2. Click the ‘Delete and return’ button.

⇨ The access authorisations of the medium are deleted.



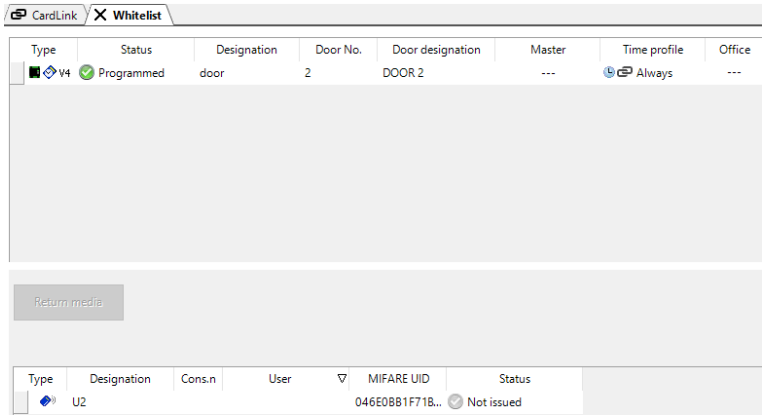
14.2 Process with Whitelist

Requirements

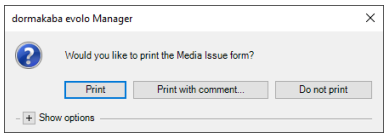
- The authorisations of the media are preconfigured.
- The persons to whom media are to be assigned must be added to the staff list.

Issuing media

An unassigned medium is placed on the desktop reader.



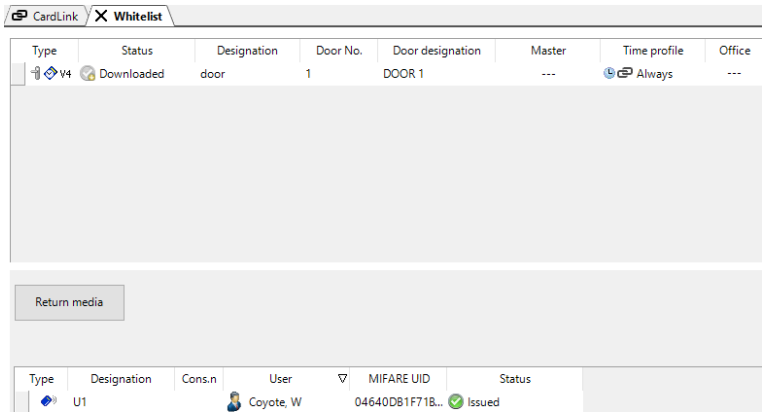
1. Select the person to whom the medium will be assigned from the list under 'Users'.
2. Print the issue ticket in the following dialogue.



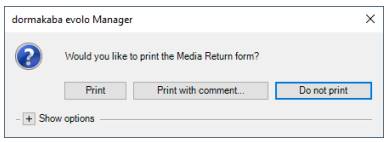
Returning media

Media return is only enabled if a medium has been assigned to a user and this medium is placed on the desktop reader.

A medium placed on the desktop reader is assigned to a person.



1. Click on the 'Media return' button.
   ⇨ The assignment to a person on the medium is deleted.
2. Print the return ticket in the following dialogue.



⇨ The authorisations assigned to the medium remain unaffected.

⇨ The medium can be assigned to another person with the same authorisations.

15 dormakaba CheckIn

The dormakaba CheckIn is a compact and comfortable management program for the check-in and check-out process. It can be used to manage access authorisations of guests and personnel for small hotels, guest houses and boarding houses.

15.1 Creating project for dormakaba CheckIn

Requirements

The following points are to be considered when creating a project for dormakaba CheckIn:

- dormakaba CheckIn can only be used with CardLink authorisations.
- All doors and, if necessary, the relevant door groups must be included in the project.
- In the KEM software, in the **Actuators** and **Door groups** tabs, the column 'CheckIn' must be visible.
- The programming of the components must be up to date.
- A block-key (service key) needs to have been created.

1. Start the KEM software.
2. Create a new project or open an existing project.

User (administration)

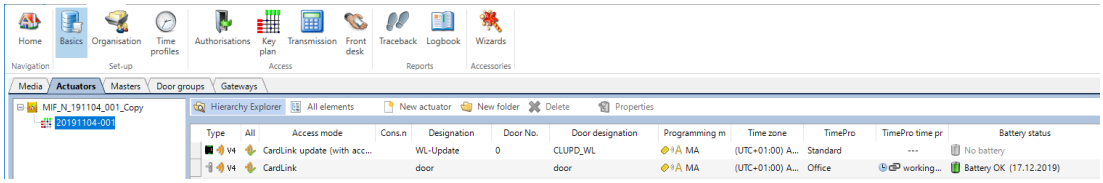
The users of the program must be registered and created to use dormakaba CheckIn. To do so, a user with the role of 'Administrator' and at least one user with the role of 'dormakaba CheckIn user' are needed.
Users can be created immediately upon starting the CheckIn wizard as well as in the settings of user administration.

15.2 Registering a dormakaba CheckIn project in KEM

15.2.1 Reading in/importing media

- Set up media with CardLink authorisation. [▶ 6.9.2]

15.2.2 Create component and assign master



- Set up components in the 'Actuators' tab [▶ 6.9.2].

Components with an entered door no. and ticked-off checkbox in the CheckIn column are available for rooms in the check-in view. If the checkbox is not ticked off in the column, the components are not displayed in the CheckIn view.

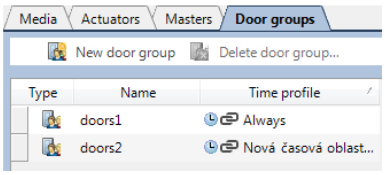
15.2.3 Setting up door groups

Procedure

1. Set up door groups. [▶ 6.9.2]

Other access points, like for an underground garage, lift, restaurant and wellness and fitness area etc. can be summarised into door groups. To display them in dormakaba CheckIn, they must be marked accordingly in the KEM tab Door groups in the CheckIn column.

2. Select one of the following options in the 'CheckIn' column:
   a) Not used
   b) Used
   c) Used, preselected



15.2.4 Programming doors with the programmer

- Program the components. [▸ 6.9.2]

15.3 Configuring and activating dormakaba CheckIn

Requirement
The project is fully registered in KEM.

Procedure
The following steps must be taken for configuration and activation.

1. In the 'View' toolbar, click on the 'Wizards' button.
2. Start the CheckIn wizard.
3. Follow the wizard's instructions.
4. Individual requirements can be defined in the dormakaba CheckIn standard data.

If a user profile has been created, the project can only be opened with the corresponding user name and relevant password. The user name determines whether dormakaba CheckIn or the KEM software should be opened.

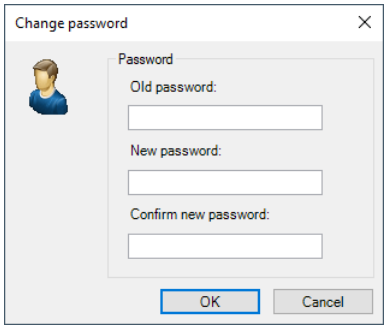
Modifying the background image
Modify the background image in the CheckIn view.

Supported image formats: PNG, JPG, BMP

- Select the background image in step 4 of the CheckIn wizard.

15.3.1 Registering users in user administration

1. Select the 'User administration' area from the Start toolbar.
2. Click on the 'New' button.
   ⇨ A new user is added on the left side.
3. Register the user properties on the right side.
4. Activate the 'dormakaba evolo Manager password' option.
5. Click on the 'Change' button to open the password dialogue.
6. Register the password.
7. Click on the 'OK' button.



   ⇨ User authentication with password is activated.
   ⇨ The administrator within the user rights option is activated.

If only one user is registered, the Admin [Administrator] user right cannot be changed.

8. Exit the user administration by clicking on the 'Close' button.

Delete user

1. Select the 'User administration' area from the Start toolbar.

2. Select the user to be removed.
3. Click on the 'Delete' button.
   ⇨ The user is deleted.
4. Click on the 'Close' button.

When the last user (**Admin**) is deleted, the user administration is disabled.

Change the user password

1. Select the 'User administration' area from the Start toolbar.
2. Select the user.
3. Navigate to the 'Authentication' area.
4. Click on the 'Change' button.
5. Register the password and click on the 'OK' button.
6. Click on the 'Close' button.

15.4 Operation

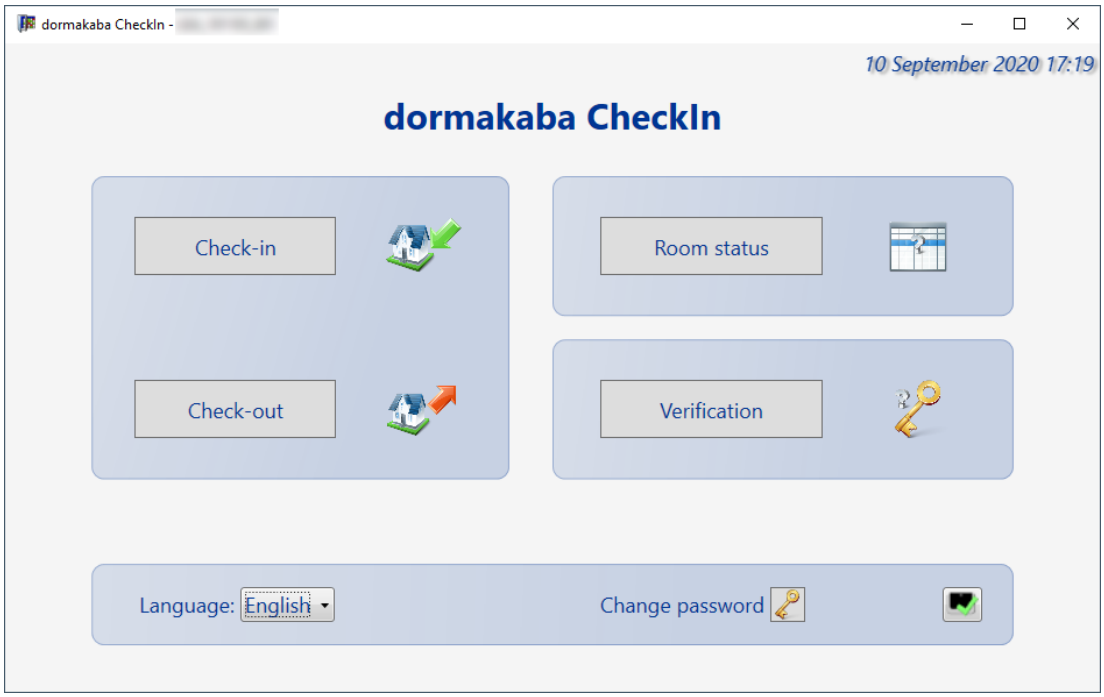
15.4.1 Opening CheckIn

1. Launch the dormakaba evolo Manager (KEM) software.
2. Select one of the following options:
   a) Create a new project:
   - Register a new project in KEM in full.
   - Configure and activate a CheckIn project. The rest of the process continues as described in .
   b) Open a project with CheckIn (existing project):
   - Select CheckIn project.
   - Enter the user name and password for the respective CheckIn project.
   - Click on the 'OK' button.
   c) Open a project without CheckIn (existing project):
   - Open CheckIn project in KEM.
   - Enter the user name 'Admin' and the password for the respective KEM project.
   - Click on the 'OK' button.

15.4.2 Arrival (check-in)

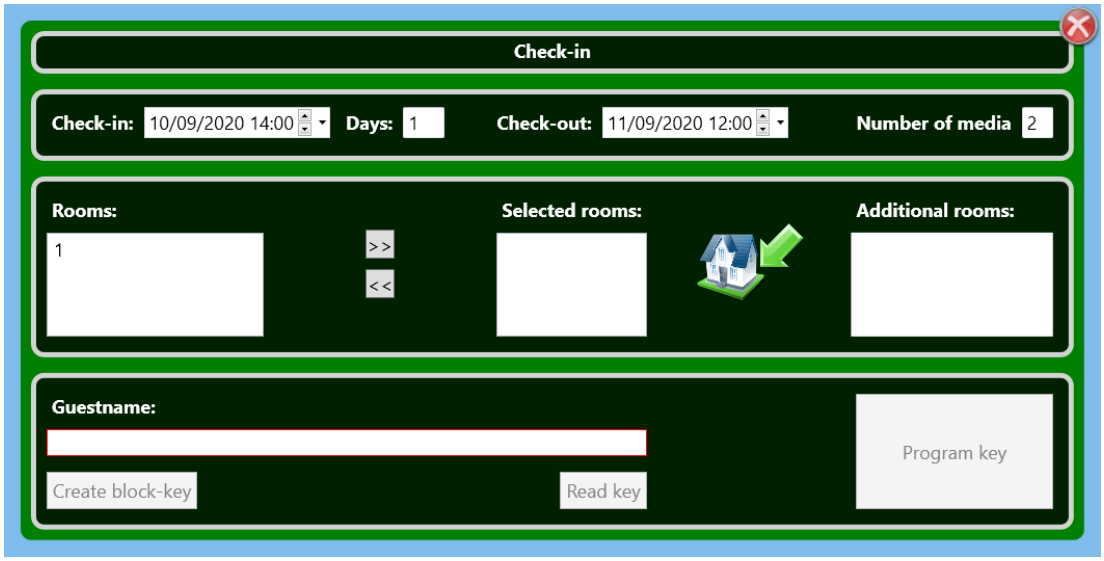
dormakaba CheckIn is opened.

1. Click on the 'Check-in' button.



2. Place a blank medium on the desktop reader.

3. Check or modify the check-in date and time.
4. Enter the number of days or check-out date (departure).
5. Check or modify the check-out date and time.
6. Modify the number of keys being issued.
7. Select the room under 'Rooms' and activate by moving to 'Selected rooms'.
8. Activate other access points, e.g. for the spa or fitness centre.
9. Enter the name of the guest.
10. Finish the process by clicking on the 'Program key' button.



15.4.3 Generating a block-key

'Create block-key' creates a block-key, with which keys, for instance a lost key, can be blocked.

Requirement

- dormakaba CheckIn is opened.
- A service medium is configured.

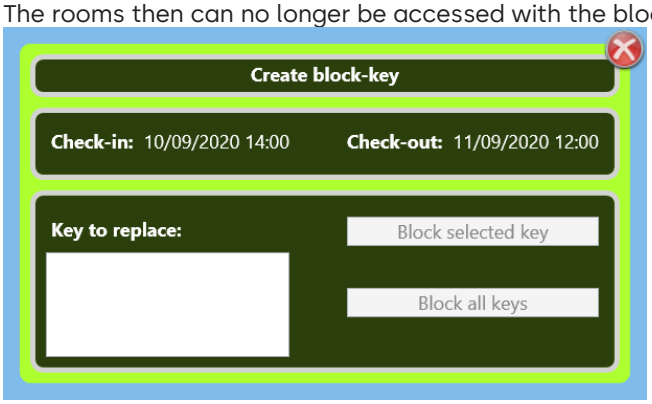
Procedure

1. Click Check-in.
2. Place the block-key (service medium) onto the desktop reader.
3. Select one or more rooms under rooms.

If multiple rooms need to be blocked, multiple rooms can be selected and collectively transferred to the block-key. Every time a block-key is created, the previous block-key on this medium is deleted.

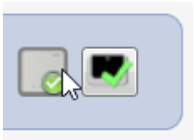
4. Click on the 'Create block-key' button.
5. Select the key to be blocked.
6. Click on the 'Block selected key' or the 'Block all keys' button.
   ⇨ The block-key is created.
7. Present this block-key to the components of the affected rooms. For each component, wait for confirmation/signals (one long acoustic signal and one green visual signal).

⇨ The rooms then can no longer be accessed with the blocked medium.



With gateway and wireless update reader:

The gateway also transfers the blacklist to the wireless components in parallel to the creation of the block-key on the service medium.

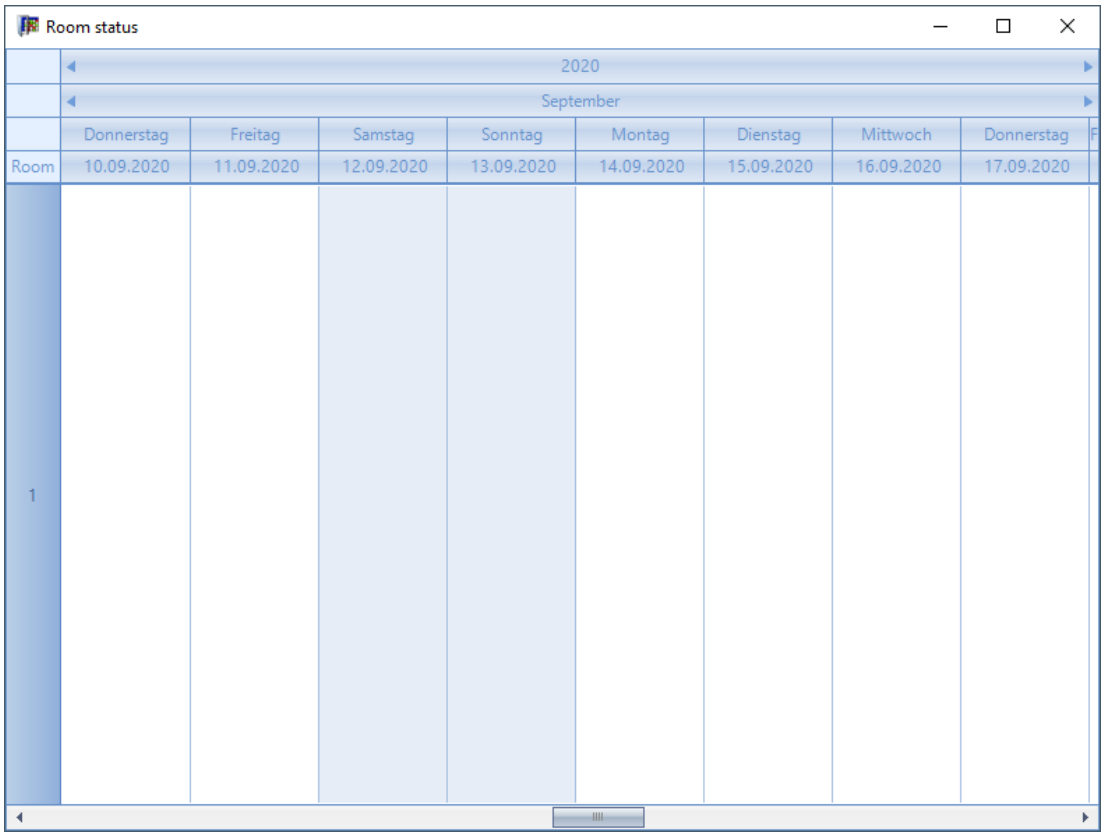


Status indication of the gateway icon on the start screen:

Transmission OK	
Transfer data	The blacklist is transferred to the wireless components via gateway.
Transfer error	Log into KEM as an administrator to be able to show details.

15.4.4 Room status

The 'Room status' is an overview of the current room occupations.



15.4.5 Departure (check-out)

dormakaba CheckIn is opened.

1. Place the guest's medium on the desktop reader.

2. Complete the process by clicking on the 'Check-out' button.

⇨ The check-out process is completed and the authorisations on the medium are deleted.

15.4.6 Verification

Verification provides the option to check the data that is on the presented key, such as on a key that has been found.

1. Place the key or block-key on the desktop reader.
2. The current data is displayed.

15.4.7 Switching from CheckIn to KEM

1. Quit the CheckIn program using “ESC”.
2. With the user name, such as "Hotel Taube" and the password, open KEM.

16 Lost medium

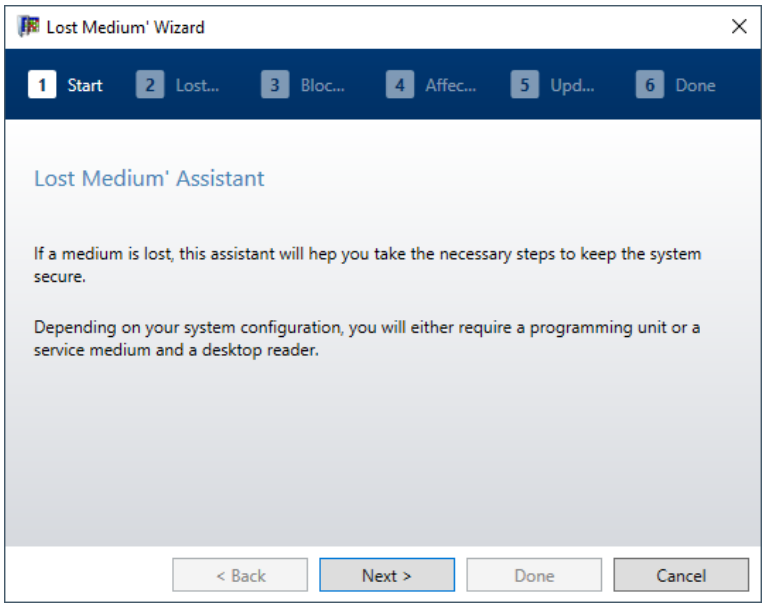
The access authorisations for lost media must be revoked.

16.1 Block/replace medium with wizard

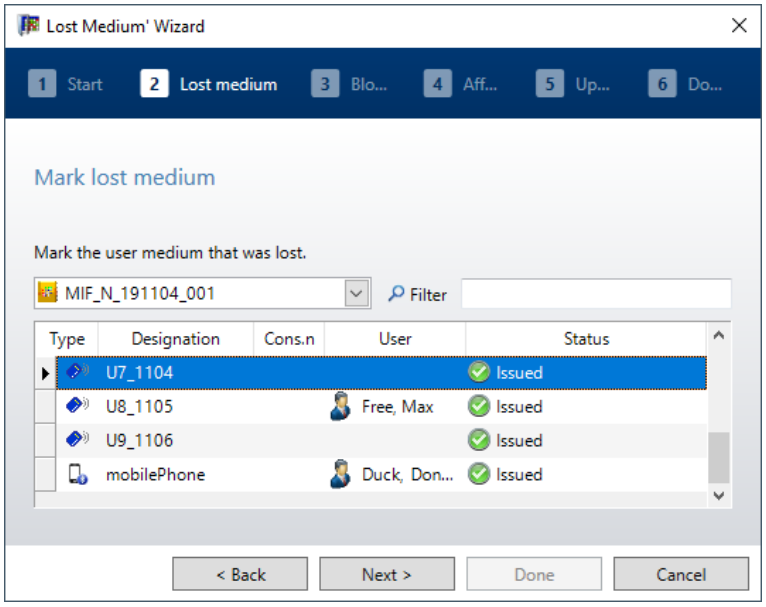
Lost media wizard
This wizard helps you to block lost media. These media can then no longer be validated or used at a component. Blocked media are rejected as unauthorised.

Procedure for blocking a medium:

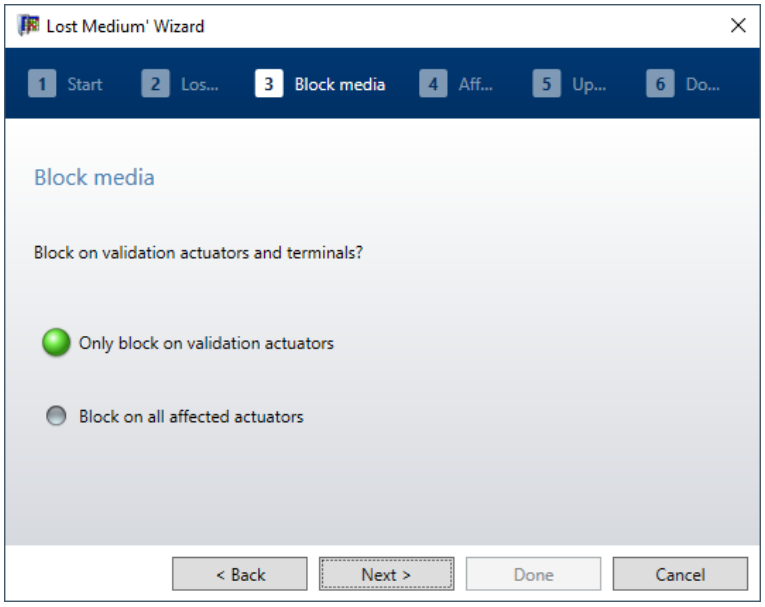
1. Select the "Wizards" menu.
2. Start the "Lost media" wizard.



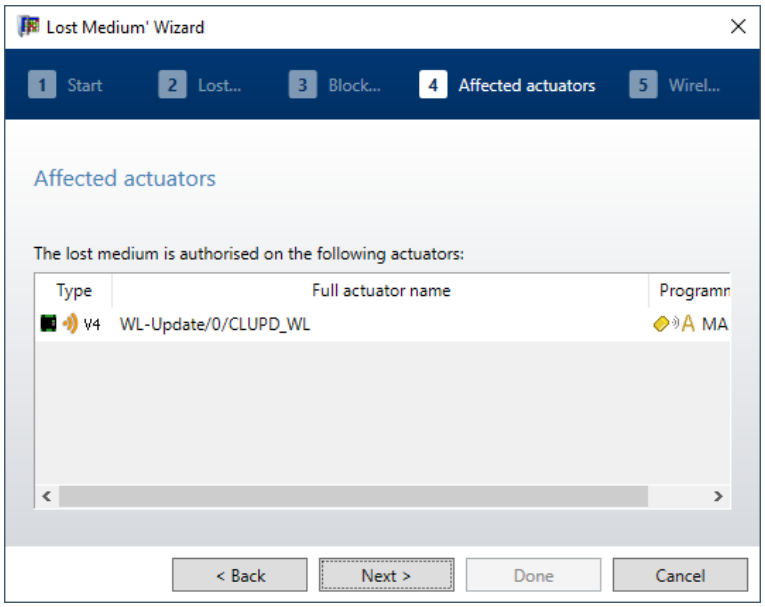
3. Select the affected medium from the media list.



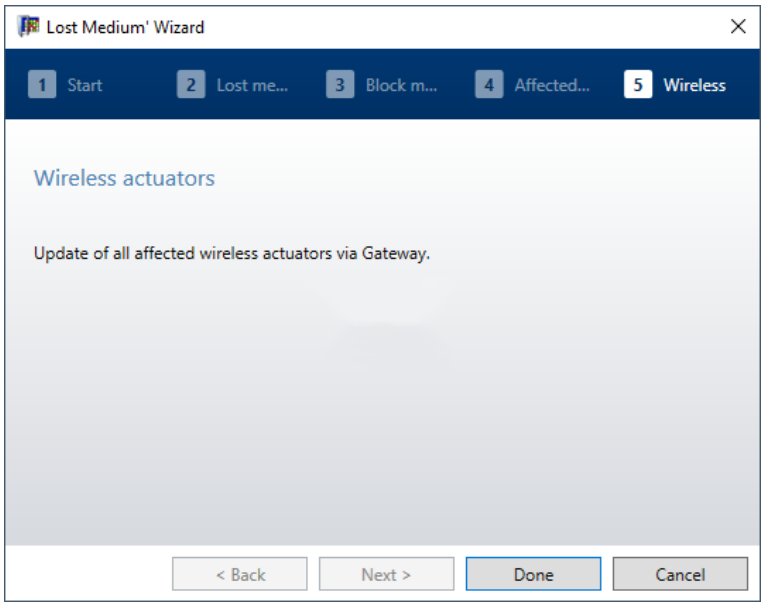
4. Select the type of blocking.



5. Select the affected components.



6. Select how the block should be transferred.



The blocking of the medium is effective only after the data has been transferred to the affected components.

Replacement badge wizard
This wizard helps you to transfer the authorisations of the existing or lost medium to a new medium. The existing or lost medium is blocked.

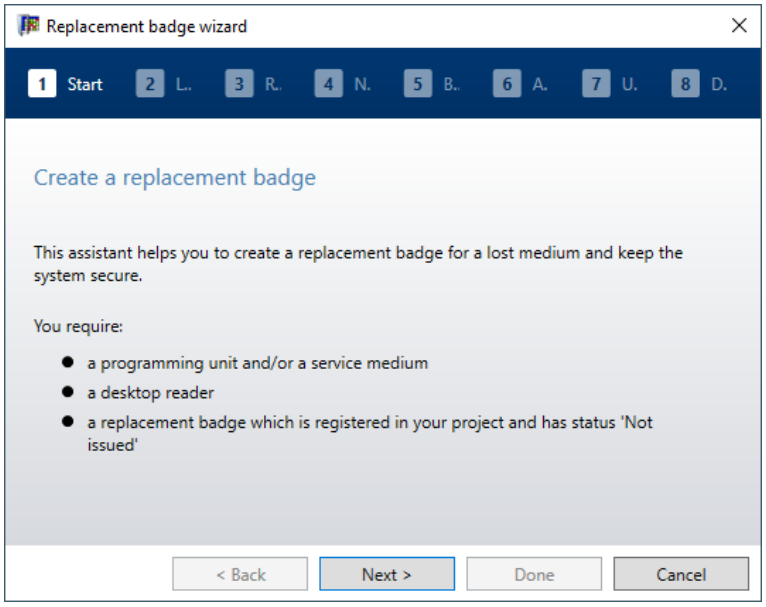
The wizard starts with the active project in the selection menu. Replacement badges can also be created for other projects.

Requirements:

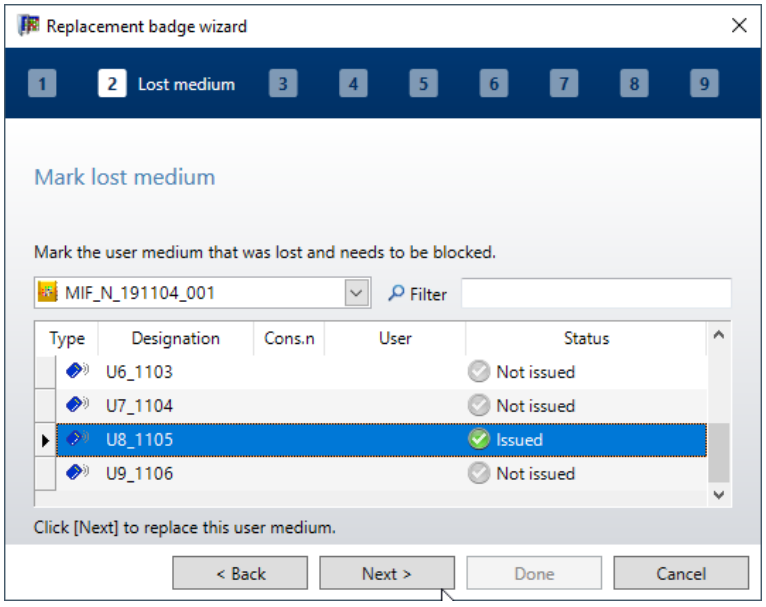
- A programmer 1460. The programmer is not required if the service medium is being used.
- A service medium. The service medium is required if no programmer is available.
- A desktop reader
- A replacement medium. The replacement medium must be read in the project. The replacement medium is not issued.

Procedure:

1. Select the Wizards menu in KEM.
2. Select the 'Replacement badge' wizard.



3. Select the lost medium of the user.



4. Follow the wizard's instructions.

The lost medium is blocked and the authorisations of the user are transferred to a new medium.

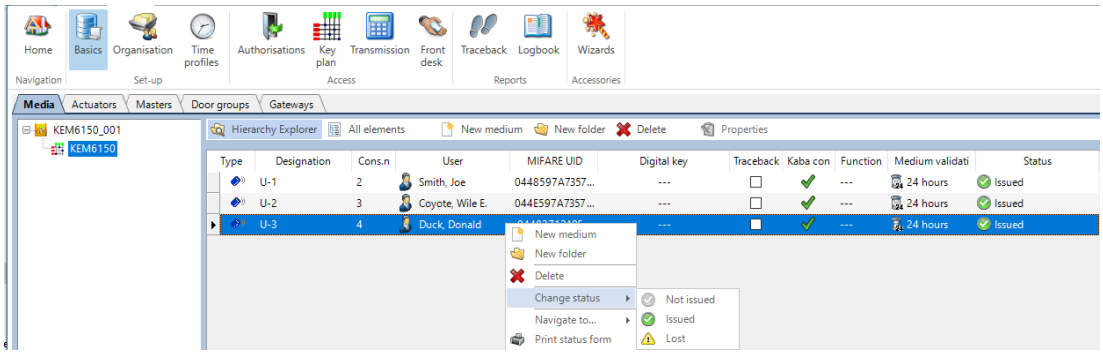
After transferring the block to the components, the lost medium can no longer be used.

16.2 CardLink

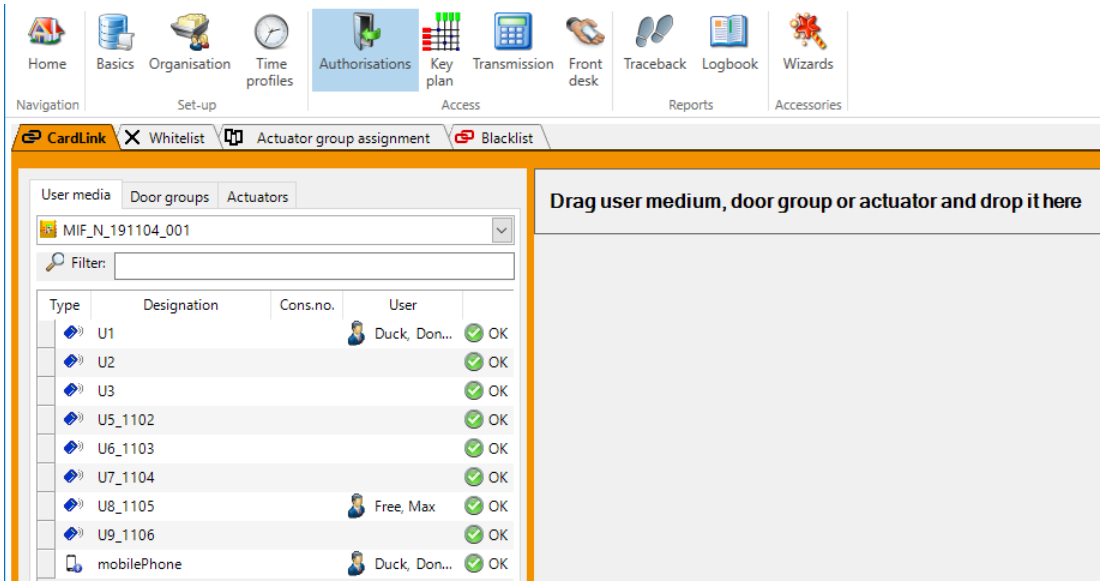
- The validation is not renewed for lost user media. As a result, these user media become invalid and access is blocked.
- If a user medium must be blocked within the validity period of a validation, blocking must be carried out on all affected components.

Procedure

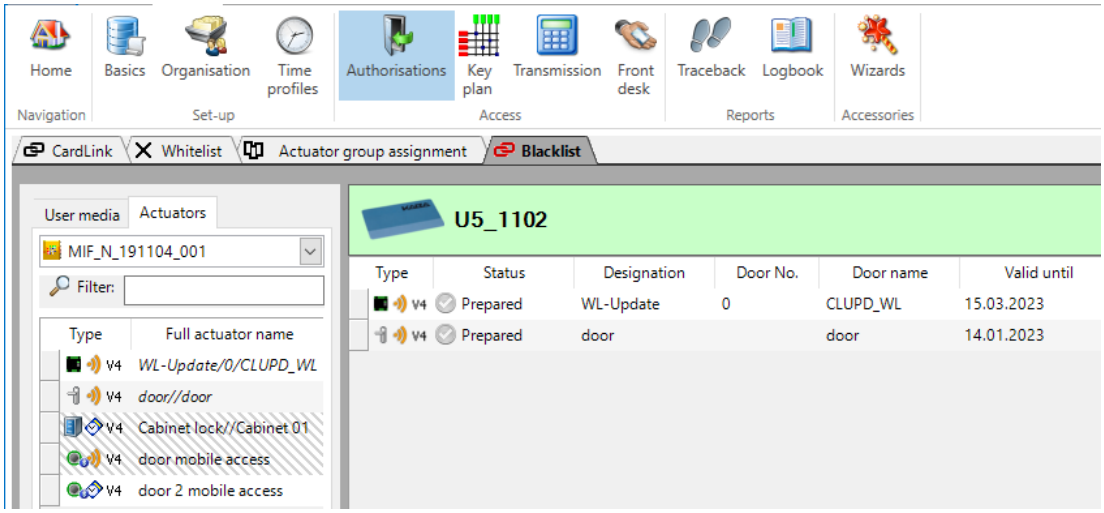
1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the Media tab.
3. Select all media or a single lost medium.
4. Open the context menu.
5. Go to 'Change status'.



6. Select the status 'Lost'.
7. If needed, a form can be printed out.
8. In the 'Navigator' menu bar, open the 'Authorisations' area.



9. The affected components that need to be updated are displayed in the blacklist.
10. Program the component. [▶ 6.9.2]
11. Confirm the programming. [▶ 6.9.1]



The blacklist is only available in the CardLink authorisation type.

- When operating with validation components, the user medium must be entered in the blacklist. The lost medium can then no longer be validated. The medium only becomes invalid after the validation period has elapsed.
- When operating with standalone components, the medium must be entered in the blacklist (CardLink) and then transferred to all standalone components of the respective system using the programmer or the service medium.
- All media that are entered in the blacklist are blocked for the corresponding components.

16.3 CardLink with terminal

In terminal mode, the medium is assigned the 'Lost' status in the KEM software. The medium is no longer validated by the terminal.

16.4 Whitelist

- If a medium is lost, it is important to revoke the authorisations from this medium.
- In operation with non-wireless standalone components, the current list of authorised media is transferred to all standalone components using the programmer.

  In operation with wireless standalone components, the current list of authorised media is transferred to all standalone components using a gateway.

  A lost medium is then no longer found on this list.

Procedure

1. In the 'View' toolbar, open the 'Basics' area.
2. Go to the 'Medium' tab.
3. Select the lost medium. If multiple media need to be entered as lost, select these.
4. Open the context menu.
5. Go to 'Change status'.
6. Select the status 'Lost'.
7. If needed, a form can be printed out.
8. Program the components. [▸ 6.9.1]
   For wireless, start the transfer via the gateway.
9. Confirm programming. [▸ 6.9.1]

17 Delete personal name

This function removes a person's name from the project. A distinction is made between persons (media users) and KEM users (user administration).

If user administration is active, the user requires the 'Delete personal names' right to be able to call up the function. This can be activated in the roles in user administration. The 'Administrator' role has this right by default.
If user administration is not active, only personal names can be deleted.

Effect of deleting a personal name

- The person is deleted from the organisation.
- Protocol entries are not removed.
  The name is replaced with 'Name deleted'.
- Logbook entries are not removed.
  The name is replaced with 'Name deleted'.
- Traceback entries are not removed.
  The name is replaced with 'Name deleted'.
- Media assigned to the person are set to 'Not issued'.
  The status 'Lost' is retained.

Effect of deleting a user name

- The user is not deleted from user administration.
  The user must be separately removed from user administration.
- Protocol entries are not removed.
  The name is replaced with 'Name deleted'.
- Logbook entries are not removed.
  The name is replaced with 'Name deleted'.

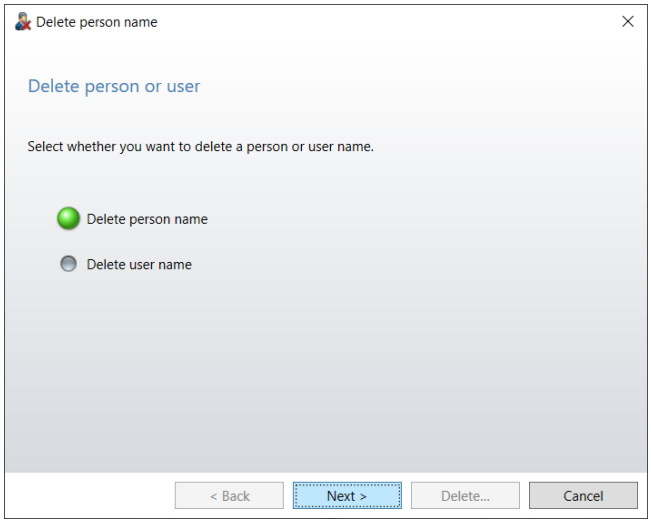
The 'Delete personal name' wizard can be called up from various menus:

- Start/Delete personal name
- Navigator/Organisation/Persons
- Navigator/Traceback
- Navigator/Logbook

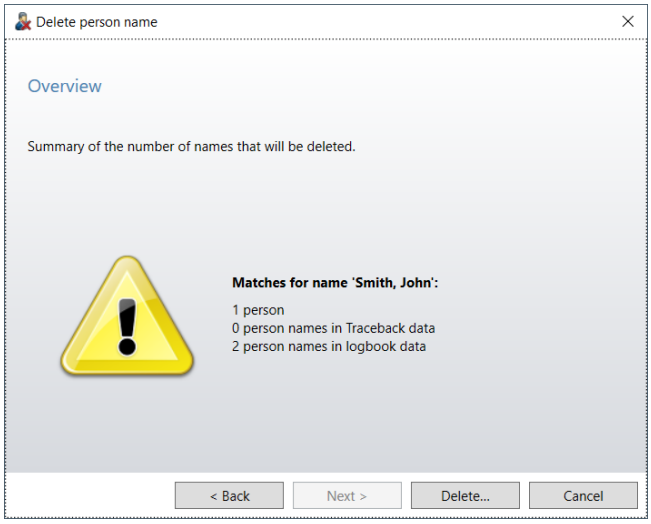
17.1 Delete personal name wizard

The action can be cancelled at any time before the wizard is completed.
Once the wizard has been run, the 'Undo' function can no longer be used.

1. Click 'Delete personal name'.
2. Enter the password.
   ⇨ A password is not required if user administration is not active.
3. Choose whether a personal name or a user name is to be deleted.
   If user administration is not active, only personal names can be deleted.



4. Select the name from the list or enter it into the field.
5. Click 'Next'.



   ⇨ The overview contains information concerning how often the name occurs in the affected ranges.

6. Click 'Delete'.
   ⇨ The name will be removed from the lists in the ranges.
   ⇨ The entries are retained.

If multiple persons with identical names are present in the system, the names of all those persons will be deleted.
Users must be removed from user administration separately.

18 Care and maintenance

18.1 Data security

A sudden system crash can corrupt data on a computer. It is important to regularly save data to external media and to keep these in a secure location (e.g. safe or safe deposit box).

A security back-up can be automated in the project properties .

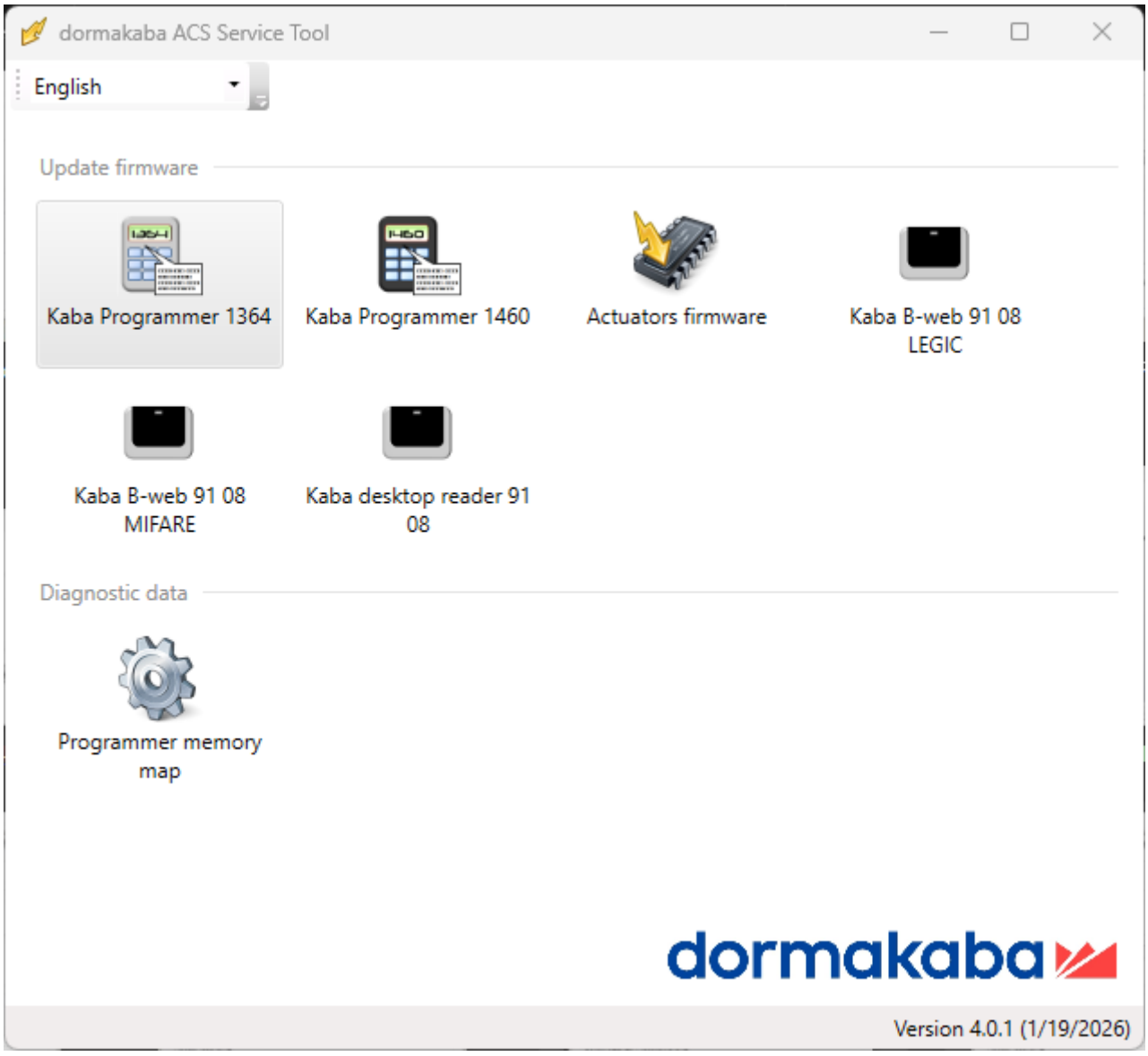
18.2 Updating dormakaba evolo Manager

An update can be purchased via the distribution channel. All updates within a major version (e.g. 7.0 to 7.2) are free of charge. The installation should be carried out as described in the Installing software chapter.

19 dormakaba ACS Service Tool

The dormakaba ACS Service Tool is an auxiliary program for updating firmware data and for conducting diagnoses.

You can also start the tool directly, that is, the system software does not need to be running. Navigate to *Start menu -> Programs -> Kaba -> dormakaba ACS Service Tool* to run it.



Programmer 1364	Wizard for updating the programmer firmware.
Programmer 1460	Wizard for updating the programmer firmware.
Actuators firmware	Wizard for transferring the firmware for the components to the programmer.
Desktop reader 91 08 LEGIC/MIFARE/MRD	Wizard for updating the desktop reader firmware for the selected technology.

Programmer 1460 memory image	Wizard for creating a ZIP file with the memory content of the programmer. A tool for problem-solving in support cases.

The firmware must be downloaded from the internet/extranet onto a local hard disk before updating.

Programmer 1364 is no longer available or supported. Latest downloadable firmware: 1.38

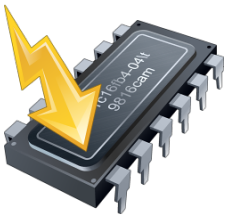
19.1 Programmer 1460 – Updating the firmware

1. Start the 'ACS Service Tool' auxiliary program.
2. Connect the programmer to the computer.
3. Click on the 'Programmer 1460' button.
4. Follow the wizard's instructions.
5. Select the current firmware file and click 'Next'.
   ⇨ The programmer will be updated.
6. Click the 'Finish' button.

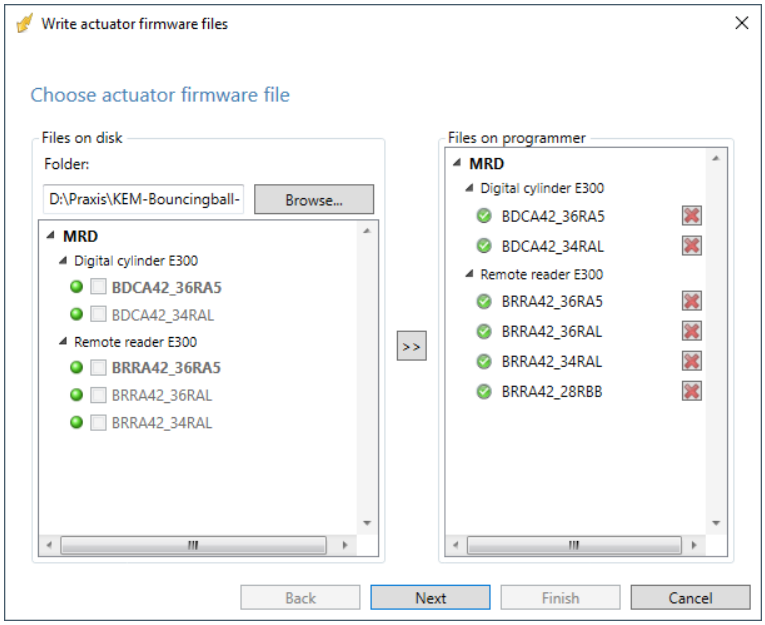
19.2 Programmer 1364 – Updating the firmware

1. Start the 'ACS Service Tool' auxiliary program.
2. Connect programmer 1364 to the computer.
3. Click on the 'Programmer 1364' button.
4. Follow the wizard's instructions.
5. Select the current firmware file and click 'Next'.
   ⇨ The programmer will be updated.
6. Click the 'Finish' button.

19.3 Actuators – Updating the firmware



1. Start the 'ACS Service Tool' auxiliary program.
2. Connect the programmer to the computer.
3. Click on the 'Actuator firmware' button.
4. Follow the wizard's instructions.
5. Select the current firmware file.
   Note: Files which are displayed as inactive are already on the programmer. The current files are marked with a green thumbtack.
6. Transfer the selected files to the programmer page using the 'arrow' button (in the middle).
7. Click on the 'Next' button.
   ⇨ The selected firmware files are transferred to the programmer.



Multiple firmware files can also be copied directly to the "Files on the programmer" folder from the explorer.

8. Click on the 'Finish' button.

⇨ The firmware files are now on the programmer and can be used for a firmware update. The firmware update is described in the user manual for the programmer 1460.

19.4 Updating the desktop reader 91 08

MIFARE/LEGIC desktop reader

1. Start the 'ACS Service Tool' auxiliary program.
2. Connect the desktop reader to the computer.
3. Click on 'Desktop reader 91 08 <selected technology>'.
4. Follow the wizard's instructions.
5. Select the current firmware file.
6. Click 'Next'.
   ⇨ The desktop reader is updated.
7. Click on "Finish".

MRD desktop reader

1. Start the 'ACS Service Tool' auxiliary program.
2. Connect the desktop reader to the computer.
3. Click on 'Desktop reader 91 08'.
   ⇨ The additional tool "LEGIC Flasher Pro" is launching.
4. In the 'File' menu, select the firmware file for the update.
5. Click on 'Download'.
   ⇨ The desktop reader is updated.
6. Exit the additional tool.

19.5 Creating a memory image of the programmer

The memory image can only be created with the programmer 1460.

1. Start the 'ACS Service Tool' auxiliary program.
2. Connect the programmer to the computer.
3. Click on 'Programmer memory image'.
4. Follow the wizard's instructions.
5. Select the storage location.
6. Enter the file name.
7. Click 'Next'.
   ⇨ The memory image is created.
8. Click 'Finish'.

Glossary

Access rights

An access right is the 'right' to open a door or door group under certain conditions.

Actuator traceback

An actuator traceback is an events log of all authorisations (activated and transferred), access attempts and successful accesses. It is updated automatically and saved to the actuator's memory (if this is supported). It can be read at any time and transferred to the control centre.

Actuators

Actuators are components installed in doors or door frames and opened by authorised media.

Blacklist

With CardLink authorisation, the actuators are provided with a list of media that are no longer authorised for access. Media will only be granted access if they are not included in the actuator's blacklist.

CardLink

CardLink is a system for storing access authorisations on media. This enables access authorisations to be managed centrally and media to be programmed centrally.

Components

All actuators, media and parts of the tool chain are referred to as components. Components differ in both form and function.

Door group

In a door group, a number of persons or doors are grouped together to form a door group. The door group is stored in the actuators to serve as identification, and a time profile is assigned to the door group.

KEM software

Management and configuration software for access systems.

Master A

A Master A is the highest-level programming medium in an A/B structure. The Master A can only program Master B media or CardLink.

Master B

A Master B is the programming medium that follows a Master A in an A/B structure. In a B structure, it represents the highest-level programming medium. In both types of structure (A/B), a Master B programmes the user media of each master key system.

Master T

The temporary master is a special type of programming media for standalone components. These are only valid for a certain period of time and have limited functionality.

Media

Generic term for security cards, master media (programming media) and user media.

Media applications

Media applications are defined segments on the media, such as for CardLink. To be able to use applications and other applications, media applications are needed on the user media.

Media traceback

A media traceback is an event log that can be stored in the user media. This data can be read by the desktop reader or the terminal and transferred to dormakaba evolo Manager software.

Pass mode

The function that makes it possible for the c-lever to be manually set to the open position.

Reset

The components' electronics modules can be re-initialised. In this process, all the data (authorisations and traceback) is deleted and the electronics are reset to their factory settings.

RTC

The components have a built-in electric real-time clock (RTC).

Safe UID

Safe UID is a security function for MIFARE. With Safe UID, the unique number (UID) undergoes additional encryption and is then saved to the media memory. The UID is only recognised as valid if the data in the user media matches.

Security card C, C1 and C2

A locking system can be initialised with the individual key using a security card. An individual security card is needed for every locking system.

Site key

The site key is a specific key that is assigned on an individual basis to each individual master key system. This key is produced automatically by a security chip. This additional security chip is integrated in every component and, once it has been initialised, it manages the individual encoding and decoding of all data that the system writes to the user media.

Site key

The site key (MIFARE) is a specific key that is assigned on an individual basis to each individual master key system. This key is produced automatically by a security chip. This additional security chip is integrated in every component and, once it has been initialised, it manages the individual encoding and decoding of all data that the system writes to the user media.

Special days

Individual time window for selected special days. For special days, two different days – Special Day A and Special Day B – can be created. This makes it possible to create two time windows.

Stamp

The stamp (LEGIC) is a specific key that is assigned on an individual basis to each individual master key system. At the same time, the user media are also initialised.

Standalone

This is the term used to denote actuators that are not linked with the central software, but make their own decisions regarding access authorisation.

Standalone validation actuator

The standalone actuators can also be used as validation actuators.

Time profile

A time profile is the definition of an authorisation pattern in relation to time. It is used to define from when, until when, and during which period of time a medium is to be permitted access to an actuator. Time profiles can be defined in advance or set up before authorisations are granted.

Time window

A time window defines a slot of time (in relation to holidays, special days, weekdays, etc.) in which access is permitted. When several time windows are combined, they form a time profile.

Unique number (UID)

Every medium has a unique medium identification number. This number is assigned by the manufacturer of the media and cannot be changed.

Validation

Validation (time stamp on user media) is the activation of an access authorisation.

Whitelist

The whitelist is a list of authorised media that is maintained in the actuators. A medium will only be granted access if it is included in the actuator's whitelist. Authorisation is withdrawn from a medium by removing it from the whitelist.

www.dormakaba.com

dormakaba Schweiz AG
Mühlebühlstrasse 23
8620 Wetzikon
Switzerland
T: +41 (0)44 931 61 11

www.dormakaba.com