ENiQ AccessManagement Manual

1.24 — Last update: 8 May 2025

DOM Group

Table of Contents

1. ENiQ AccessManagement – General information

Notes on the instructions and the manufacturer

These operating instructions will help you to use the following softwares in a correct manner:

- ENiQ AccessManagement
  (hereafter: “ENiQ Software”)

- ENiQ DeviceManagement

These instructions are intended for persons who perform the following activities with the software:

- Create devices
- Program devices
- Manage devices
- Create transponders
- Program transponders
- Manage transponders
- Manage locking authorizations
- Create persons
- Manage persons

Each of these persons must have read and understood the contents of these instructions. Following the instructions in this manual will help you to use the software as intended.
The persons must have basic computer knowledge and be proficient in using Microsoft Windows®.

Keep manual available

This manual is part of the software. Keep these instructions at the workstation where the software is used. Ensure that the manual is available to the operator. Include this manual if you sell or otherwise distribute the software.

This manual can be opened from the software using the *F1* shortcut key.

1.1. Content format

Formatted content

Various elements of this guide have specific format.
This allows you to easily distinguish the following elements:

```
Normal text
```

```
"Designation of buttons"
```

```
•  First level enumeration
   - Enumeration of the second level
```

```
1. Action step
2. Action step
3. Action step
```

Tips: You will receive useful tips for handling the software.

Risks on system damage

These hints warn about situations that could lead to unexpected behavior, problems in operation and property damage.

1.2. Information

Supplied documents

Further notes, instructions and information on the devices used in the system can be found in the associated instructions from the manufacturers.

Manufacturer address

> DOM Sicherheitstechnik GmbH & Co. KG
> Wesselinger Street 10-16
> D-50321 Brühl

Contact

> Phone: +49 (0) 2232 704-0
> E-Mail: dom@dom-group.eu
> Internet: www.dom-group.eu

Intended use

With the ENiQ Access Management and the ENiQ Device Management you manage, program and operate the devices of the DOM Mifare product range.

1.3. Technical data

Technical data for ENiQ Access Management

Supported devices:
Management of all DOM devices with Mifare 13.56 MHz technology:

- ENiQ Pro, ENiQ Pro V2 (BLE).
- ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S
- ENiQ AccessManager / Terminal / ITT V1 + V2 (BLE)
- ENiQ RF NetManager V1 + V2 (BLE)
- ENiQ Protector
- ENiQ LoQ
- No support of ELS 125 kHz terminals

Supported transponders:

- Mifare transponder (supported types depending on operation mode, see below).

System architecture:

- Web application (ASP.NET)
- Platform-independent client access via web browser without client installation
- Web server used: Microsoft IIS

Operation modes:

Offline “conventional” Data on Device (DoD):
UID of the transponder is stored in the device:

- Wireless communication with terminal devices via radio (868 MHz) or BLE (2.4GHz) via USB radio stick
- Use of the software with laptop as programming medium

Offline “intelligent” Data on Card (DoC):
Operation as virtual network (“intelligent DataOnCard transponder”):

- Writing of authorizations on transponders via DOM desk reader
- Validity extension of the transponder by means of ENiQ AccessManager Terminal

Online ‘conventional’ (DataOnDevice):
This concept is intended for objects in which authorizations change frequently or system events have to be displayed directly for security reasons.

- Ethernet network (TCP/IP)
- Authorization changes are carried out by the software and sent online to the end devices such as ENiQ AccessManager or ENiQ Guard®.
  Changes become effective immediately.
- Immediate door opening via ENiQ AccessManagement
- Activation of special functions via ENiQ AccessManagement

Online “intelligent” (DataOnCard) or mixed:
In addition, transponder authorizations can be rewritten or extended online via ENiQ AccessManager ITT.

Mobile mode:
(e.g. with a laptop)

If the server database is available
(stand-alone installation or available connection to the server):

- Availability of the web application on site
- Modification of all data possible on site

Without connection to the server database:

- Windows application “ENiQ DeviceManagement” with simple functionally and user interface without changes of (authorization) data
- Synchronization of data with the server database

User interface (GUI):

- Comfortable and powerful user interface
- Customizable to a person role via fixed profiles
- Languages: German, English, French, Dutch, Spanish and Italian

Modules:

Standard module:	Devices	Transponder
• Module S	max.25	max.100
• Module M	max.125	max.500
• Module L	max.750	max.3000

• Module XL	max.9.500	max.32.000
• Module XXL	<9.500	max.100.000

Module Intelligent (DataOnCard) Transponders:

- (additional) management and programming of intelligent (DataOnCard) transponders or virtual networks

Module Online

- (additional) administration and programming of DOM devices via Ethernet and RF NetManager (radio nodes).
- Modules available for the following numbers of devices: 5, 10, 25, 50, 100, >100

Data Sheet

German:

ENiQ AccessManagement Software Datasheet DE

English:

ENiQ AccessManagement Software Datasheet EN

1.4. Terms used

Term	Explanation
Administrator	Operator role with extended rights (e.g. create new operators, set system parameters etc.)
Operator	An operator is a person who can manage the ENiQ software. In the operator administration the operator rights can be assigned in the form of roles.
Operator interface	Interface between operator and the ENiQ software
Operator administration	In the operator administration of the ENiQ software, the assigned rights of operators are defined and administrated. With a role you can assign certain rights to operators.
Authorization period	You can assign an authorization period as from-to interval to the authorization of a transponder defined via a weekly schedule. This applies to both conventional (DataOnDevice) and intelligent (DataOnCard) transponders. By creating several data records consisting of a weekly schedule and the associated authorization period, you can also use this to pre-program future authorizations that deviate from the actual time (see also: Validity, Extension interval).
Area	Devices can be managed in the ENiQ software in an area hierarchy. Each main area as well as each sub-area is assigned an area ID.
Area authorization	An authorization assigned for an area (via an area ID) is called an area authorization (see also: Device authorization).
Event	The devices save processes as events with a time stamp. You can display and review these in the ENiQ software.
Device	The following are summarized under the collective term “device”: • ENiQ Pro, ENiQ Pro V2 (BLE) • ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S • ENiQ AccessManager / Terminal / ITT V1 + V2 (BLE) • ENiQ RF NetManager V1 + V2 (BLE) • ENiQ Protector • ENiQ LoQ
Device Authorization	An authorization assigned to a device via a device ID (see also: Area Authorization).
Device weekly schedule	Special function that activates a weekly schedule for a device. This device weekly schedule is then evaluated during the authorization check of a transponder, access is only granted if both the device weekly schedule and the transponder-specific weekly schedule are valid.
Validity	You can define a validity period for a transponder. Outside this time validity, the transponder is unauthorized. This applies regardless of other settings.
Main area	Main area in the top level of the area hierarchy of the ENiQ software.

Intelligent Transponder (Data on Card (DoC))	Store authorization data for areas and devices on the transponder. The authorizations are defined via the areas or the transponder groups which are provided with a weekly schedule. Renewal intervals are possible but not mandatory.
Conventional (DataOnDevice) transponder (Data on Device (DoD))	With conventional (DataOnDevice) transponders, authorization data is stored in the devices.
Person	Authorizations can be assigned to a person and locking media can be allocated
Person group	Persons who are to receive identical authorizations can be assigned to a person group and the corresponding authorizations can be assigned to the person group. If persons are assigned to an existing person group, they automatically inherit its authorizations.
Role	With the role you can assign specific user rights to operators.
Daily schedule (DS)	A daily schedule (DS) specifies the time-based definition of an authorization in the form of 15-minute intervals. It is part of a weekly schedule. In the ENiQ software as well as in the devices you can define or store 256 daily schedules each.
Subarea	All areas below the top level of the area hierarchy of the ENiQ software. Subareas always belong to a main area.
Weekly schedule (WS)	A weekly schedule (WS) specifies the temporal definition of an authorization for 7 weekdays plus 3 special days. For this purpose it refers to 10 daily schedules. You can define and save 256 weekly schedules in the ENiQ software as well as in the devices. The following definitions are possible: • WS=0 no access (unauthorized) • WS=1 access unlimited in time, special functions active • WS=2 to 254 freely definable • WS=255 access unlimited in time, special functions inactive. You can define a so-called fire department transponder via weekly schedule 255. With this transponder access is always possible

2. Notes on the ENiQ software

General information

This chapter contains basic information about the ENiQ software and the included programs.

- System Overview
- Access Management
- Device Management
- Intelligent (DataOnCard) and Conventional (DataOnDevice) Devices and Transponders

2.1. System description

Basic information on the ENiQ locking system.

The ENiQ software is composed of the following components:

- ENiQ Access Management (web application)
- ENiQ Device Management
- Database Server
- DB Manager

The components can be installed together on one computer or distributed on several computers.
A Windows operating system is mandatory for this purpose

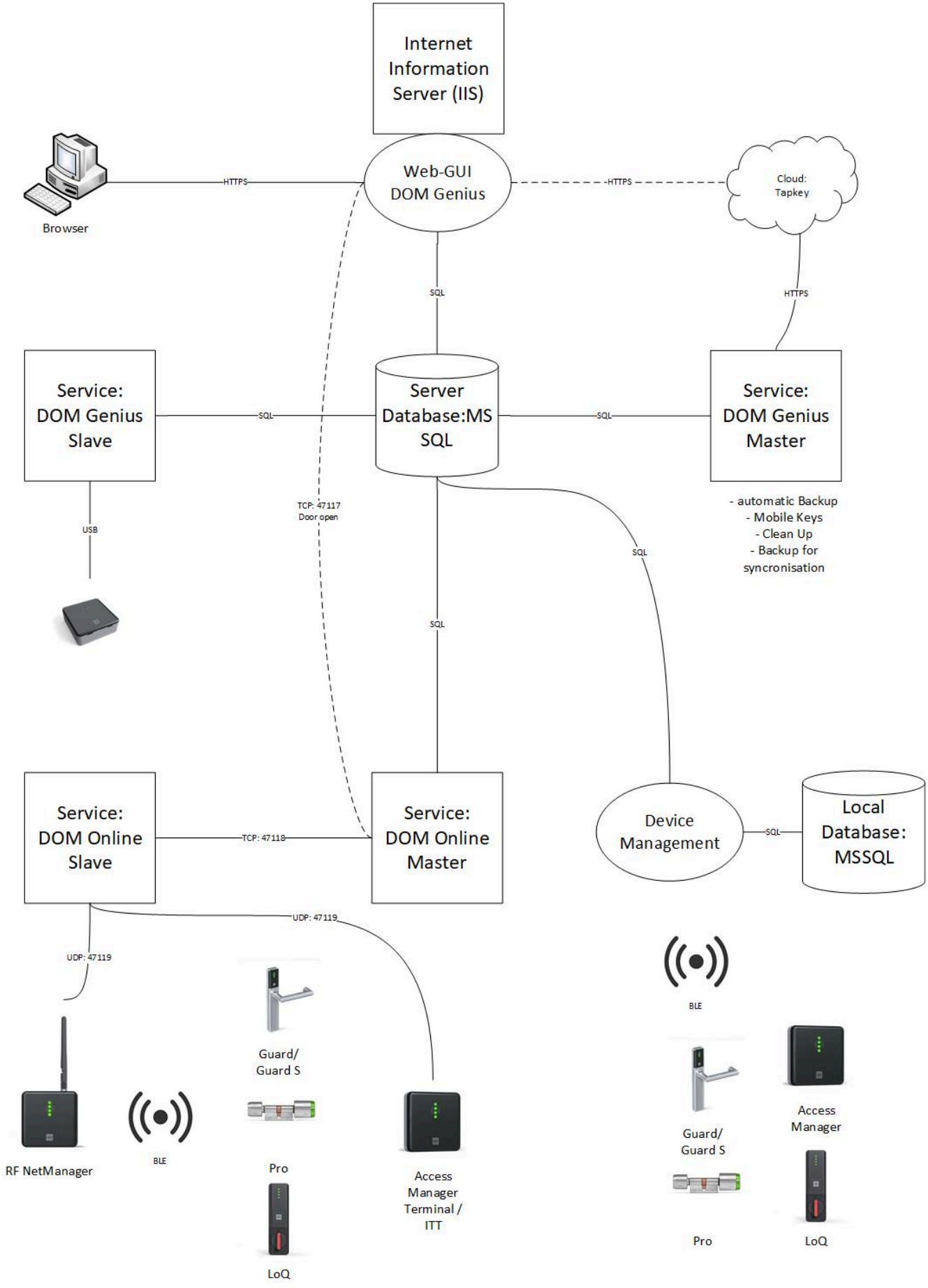
2.1.1. Basic information on the ENiQ locking system

Device	Explanation/ Purpose
ENiQ PRO, ENiQ Pro V2 (BLE) (mechatronic knob cylinder)	Locking and unlocking doors. It incorporates an electronic access control system.
ENiQ Guardian / ENiQ Guardian S / ENiQ Guard / ENiQ Guard S (electronic hardware reader)	Open and close doors. It includes an electronic access control system.
ENiQ AccessManager V1 + V2 (BLE)	When the transponder is presented, an authorization check is performed. If the check is successful, the relay on the AccessManager is switched.
ENiQ AccessManager Terminal V1 + V2 (BLE)	When the transponder is presented, the authorization is checked. If the check is successful, the authorizations present on the transponder are extended by a specified time interval. Subsequently, the relay on the AccessManager is switched.
ENiQ AccessManager ITT V1 + V2 (BLE) (Intelligent (DataOnCard) Transponder Terminal)	In addition to the DOM ACM Terminal function, when an authorized transponder is presented, the current authorizations and weekly schedules are stored on the transponder. E.G.: A person is authorized at an area A. However, he should also be able to open devices in area B. The operator assigns the authorization and the weekly schedule for area B to him. The next time the transponder is presented at the ACM ITT, the person can also open devices in area B.
ENiQ RF NetManager V1 + V2 (BLE)	The ENiQ RF NetManager is a communication module connected to the software and database via Ethernet. It transmits data to and from the ENiQ access control devices on the doors via radio – 868 MHz – (for V1) or Bluetooth low Energy – BLE – 2.4 GHz (for V2). It is suitable for Data on Device – Online operating mode.
ENiQ LoQ	Mechatronic access control for your furniture
Transponders e.g. transponders, cards	The transponders contain authorizations of the person to open doors.
Desk Reader V1 + V2	Read and program transponders.
USB wireless stick	Communication interface between devices and ENiQ Device Management.

The Mifare system operates at a frequency of 13.56 MHz.

! Managing and operating devices with a frequency of 125 kHz is not possible with the ENiQ software. (No support of ELS 125 kHz terminals).

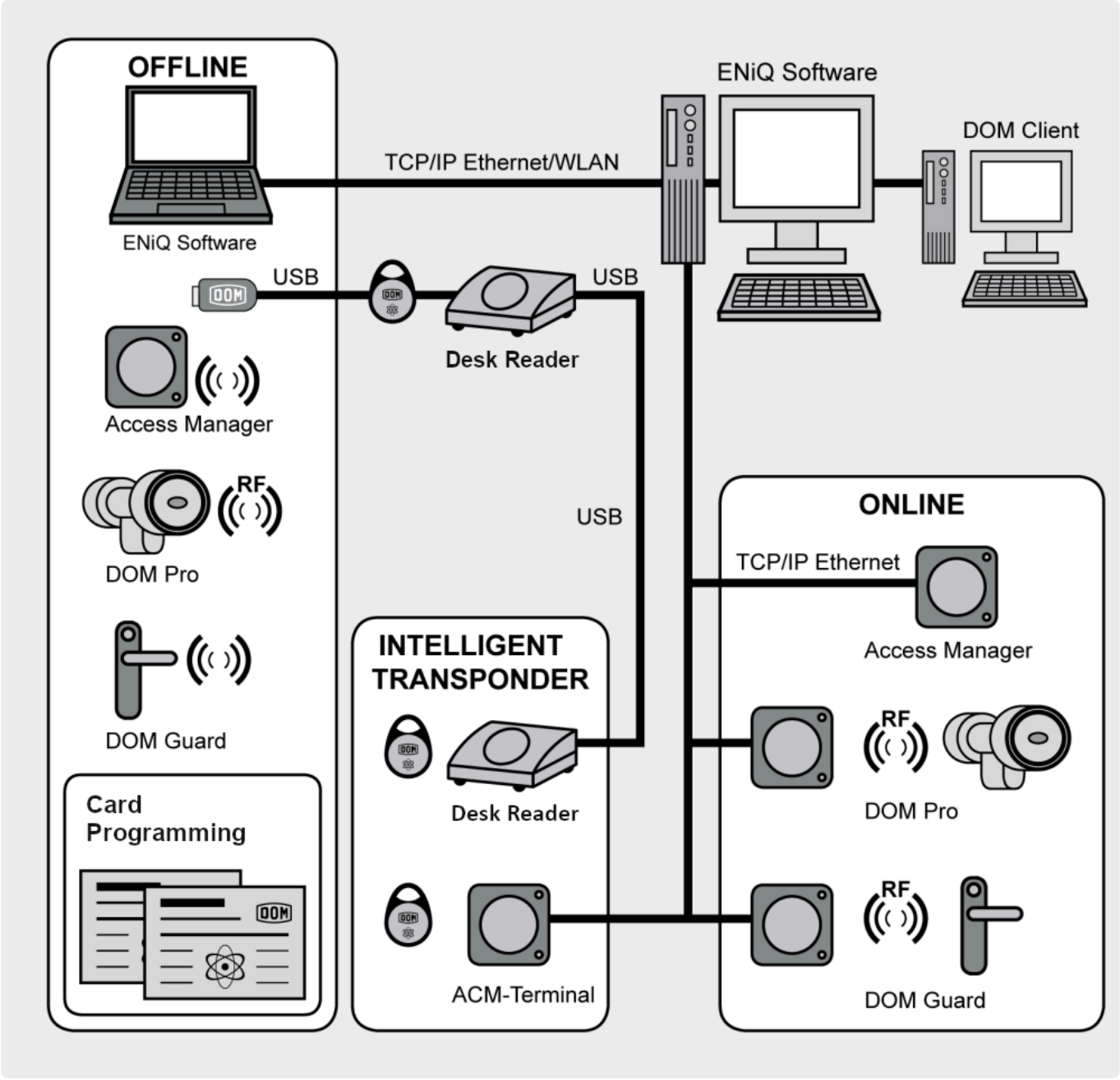
For further notes, instructions and information on the devices used in the system, please refer to the corresponding manuals of the manufacturers.
The data is stored centrally in an SQL database. During installation, Microsoft SQL Server Express Edition is installed as the default database.
Alternatively, databases that offer an ADO.NET data provider can be used.



You can read and program different device data offline. To do this, you need a pre-

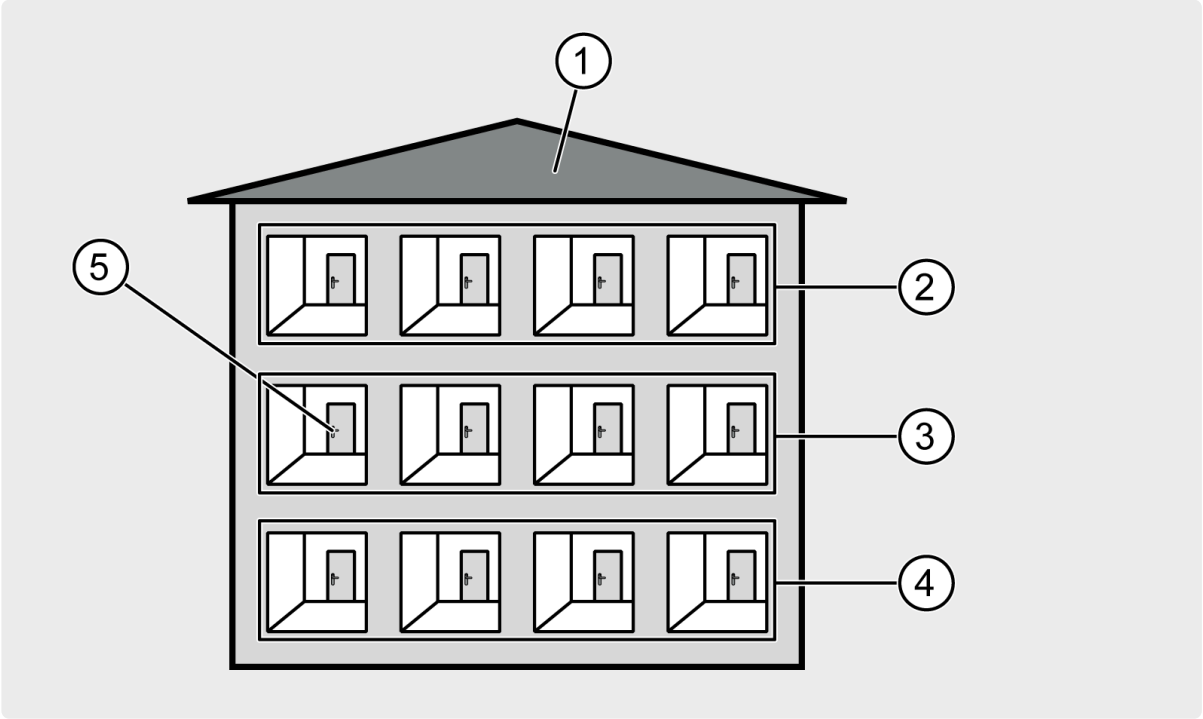
installed ENiQ Device Management software and the USB wireless stick, which can communicate wirelessly with your devices. A device is recognized by the ENiQ Device Management Software as soon as you hold an RF wake-up card in front of the device.

To read and write transponders locally via the USB interface of your computer, use a desk reader. You can either write the transponders “intelligently” (DataOnCard) or create them “conventionally” (DataOnDevice) in the database. With intelligent (DataOnCard) transponders, the authorizations are stored directly on the transponder. When the transponder comes into contact with a device, the authorizations are transmitted to the device. Intelligent (DataOnCard) transponders can exchange data with the device when used and can be programmed that way.

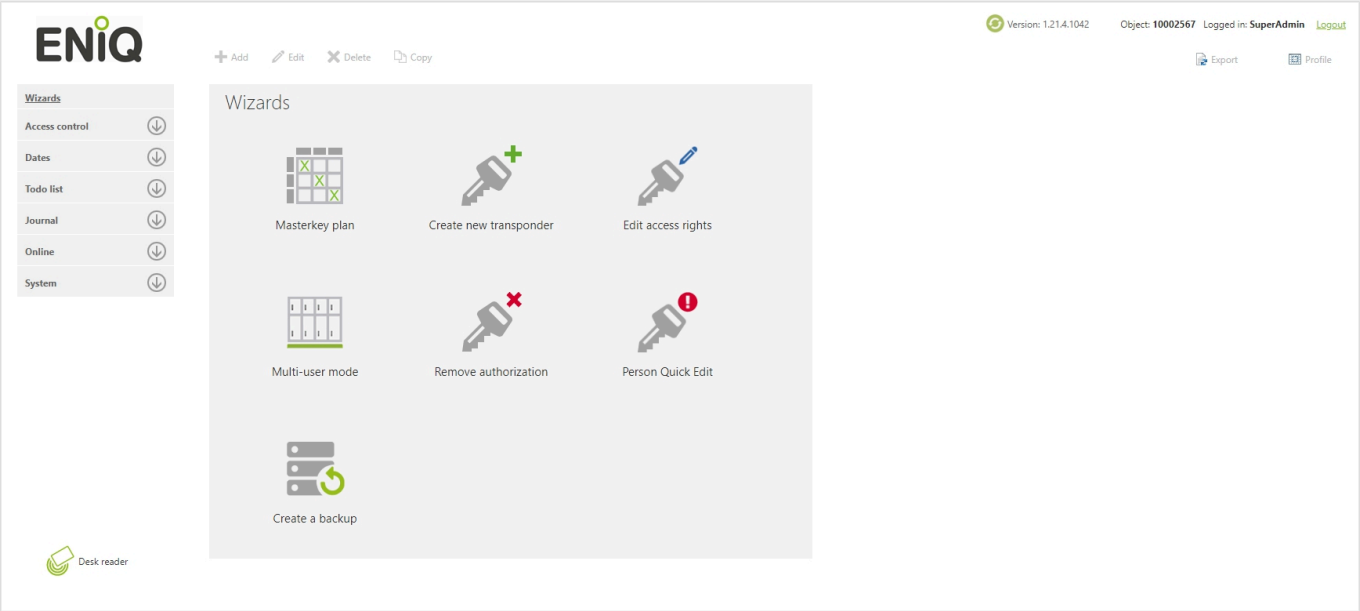


The task of the ENiQ software shall be explained by an example. You want to define the access authorizations to a building, its floors and rooms. For this you have to clarify in advance e.g. who should have access, when should access be granted and when not.

If this is clarified, you can create the building as an area (1) with the ENiQ Access Management Software.
In the first sub-area level (2, 3, 4) you create the floors.
In the second sub-area level (5), create the rooms present on the floors.
Doors are provided for access to the building, floors and rooms. The doors are equipped, for example, with ENiQ cylinders. You read the data of the ENiQ cylinders into the database using the ENiQ Device Management desktop software. You assign the ENiQ cylinders to the corresponding doors using the ENiQ Access Management software. You define the times for access and which persons are authorized for access. You program the devices and transponders with the defined authorizations.



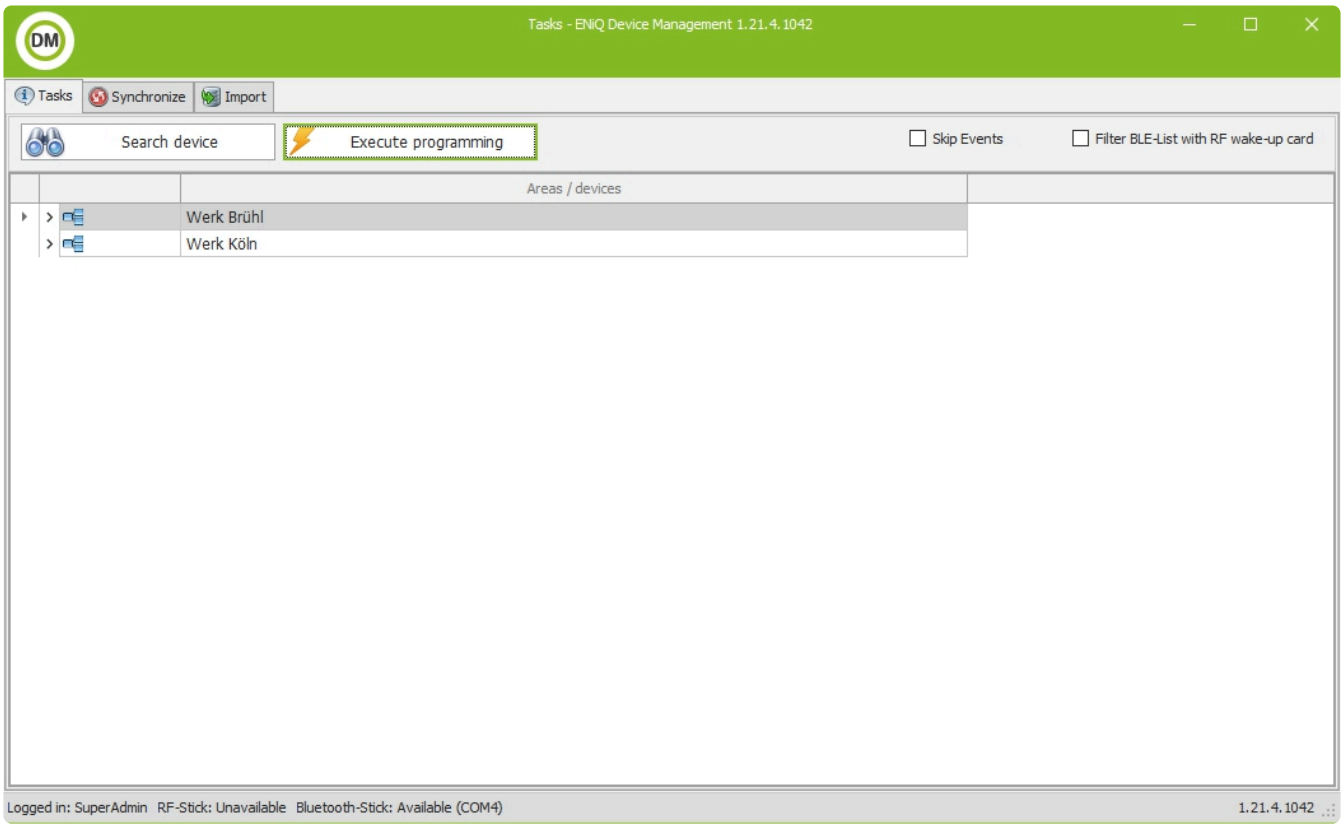
2.1.2. ENiQ Access Management



With the ENiQ Access Management software, you can perform the following, for example:

- Create areas
- Assign devices to areas
- Create a person
- Create schedules
- Enter mastercard data
- Assign authorizations (devices, areas, transponders, person)
- Block lost transponders*

2.1.3. ENiQ Device Management

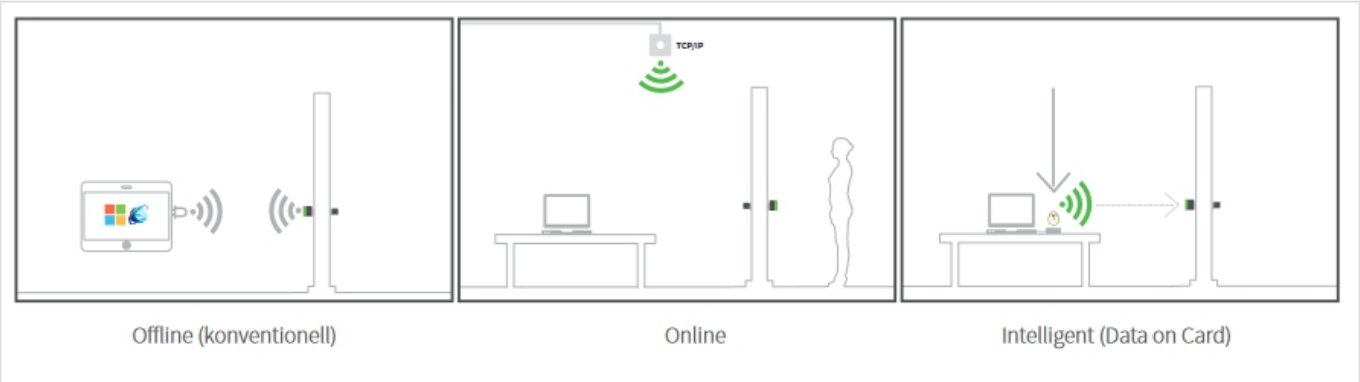


With the ENiQ Device Management software, you can:

- Add new devices
- Program devices (transfer settings from ENiQ Access Management software)
- Read out events
- Read out status information, e.g. battery status
- Import device data
- Import person/ transponder data

2.1.4. Operating modes Offline (DoD) / Online / Intelligent (DoC)

Our operating modes represent different ways of managing your user rights and operating your DOM products.
The user authorizations are either in the end device or on the locking media (transponder, ISO check card transponder, smartphone, etc.). User authorizations can be managed by programming cards, app or software.
You can choose from the following operating modes for your DOM digital locking systems:



OFFLINE (DATA ON DEVICE)
In the offline operating modes, the terminal devices are programmed from close range (0.5 cm – 3 m). So one goes with the programming medium from terminal device to terminal device. Programming a terminal device means the following actions:

- Initial connection of the Mastercard (highest administration card and proof of ownership in the system) and/or with an app/software terminal device.
- Initialization of an electronic product for the first time
- Creation of up to 5 programming cards
- Creation/authorization and deletion of locking media
- Assign authorizations with time limits and program them into the devices
- Reading out events on the terminal device
- etc.
  The user authorizations are stored in the terminal device.

CARD PROGRAMMING OFFLINE MODE:

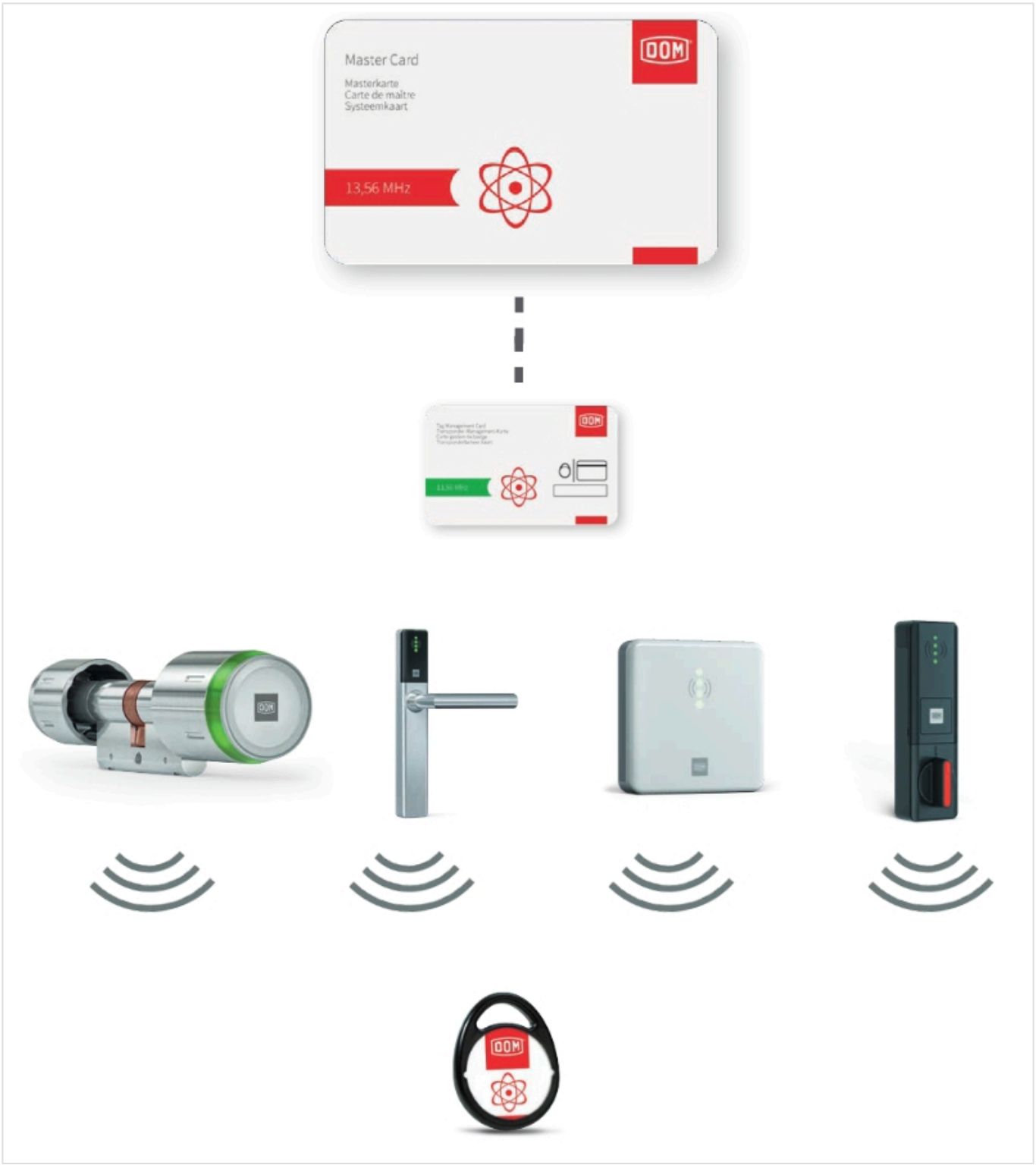
In the card programming offline mode, two different cards are available. The Mastercard, which is the highest authorized card in the hierarchy of your entire system, is primarily used to assign the terminal devices to your system. After that, your terminal devices will only work in your system. The Mastercard can then be used to authorize up to 5 programming cards on the terminal devices.

The Mastercard:
It is primarily used to assign the terminal devices to your system. It can be used to create up to 5 programming cards at the terminals and to assign the software to the system. Since the Mastercard is also the only card that can be used to remove terminal devices from your system, delete all user data

(including programming cards) and provide proof of ownership, it should be stored in a safe place, e.g. a safe, as soon as possible afterwards.

The programming card:
You can now use the programming card to permanently authorize or delete locking media, such as transponders and check card transponders, on the terminal devices. If a transponder is lost, you can now delete all locking media that are authorized at the end device. Those that are to be reused afterwards must be authorized again. The operating mode “Card Programming – Offline” works with all current ELS® (125 kHz) and ENiQ® (Mifare 13.56 MHz) products from DOM.

CARD PROGRAMMING – OFFLINE



SOFTWARE PROGRAMMING – OFFLINE

In this operating mode, you use software for efficient management of your digital locking system. With its help you can, for example, authorize persons temporally. The locking media of the persons carry a unique number (UID) and, if necessary, further individual data, which are unique and different for each transponder. This number can be used to identify each transponder in your locking system. The authorizations of the persons are in the terminal devices. These are then only compared with the UID and the data of the relevant transponder by the terminal devices when the transponder is presented. With the help of, for example, a laptop running the software and a wireless stick (V1) or a USB BLE stick (V2), terminal device is then programmed from a maximum distance of three meters and receives, for

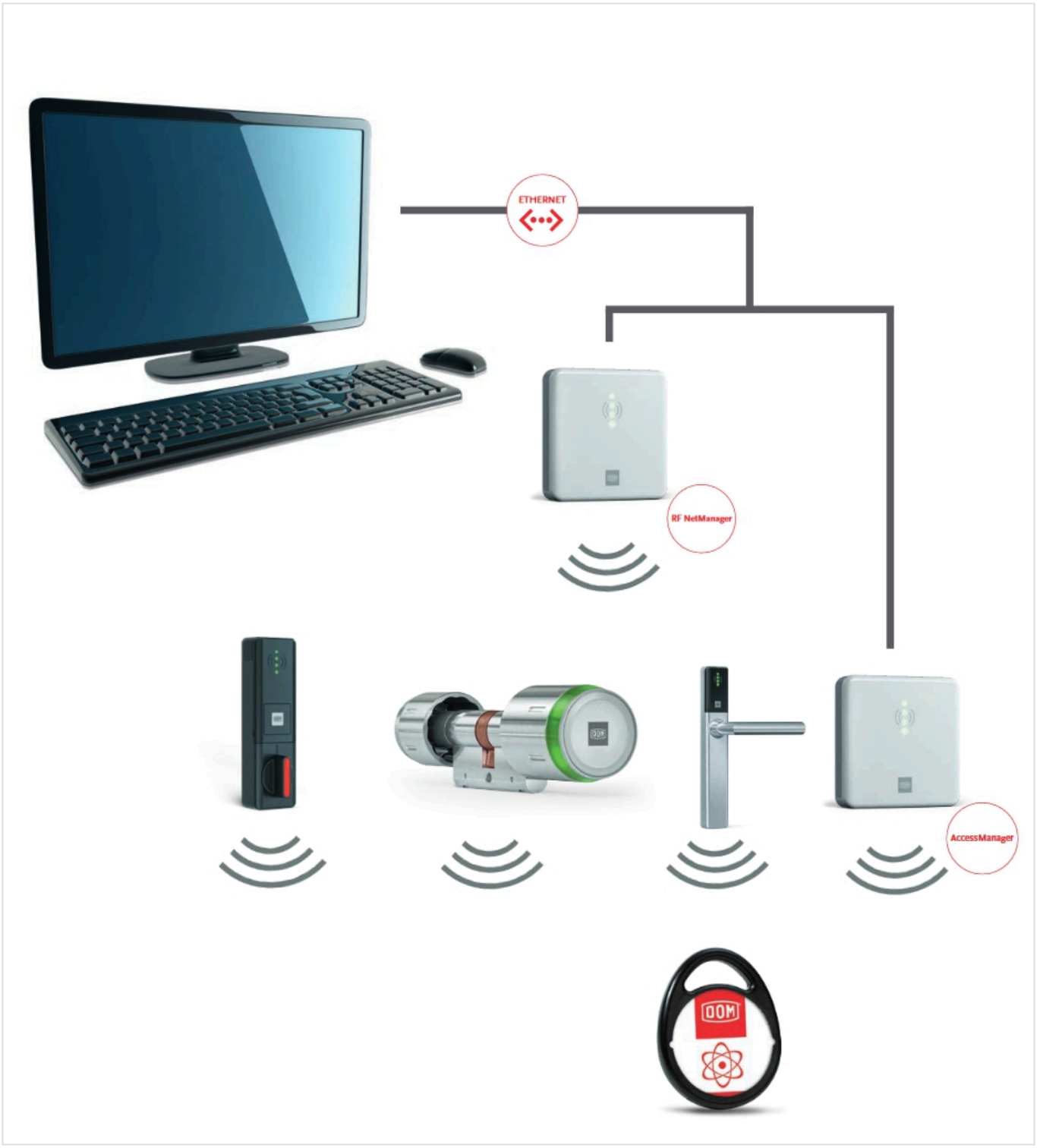
example, the authorizations of the locking media. The locking media themselves are read into the software via a so-called desk reader. The software database does not necessarily have to be on the same device that is used to manage and program the system. You can also use a client-server solution in the Software programming offline operating mode. The “Software Programming Offline” mode works with all current ELS® (125 kHz) and ENiQ® (Mifare 13.56 MHz) products from DOM.

SOFTWARE PROGRAMMING – ONLINE:

In the online operating mode, the terminal devices are programmed with the help of so-called communication devices via a network connection. This means that you do not go from terminal device to terminal device with the programming medium as in the offline operating modes, but program the

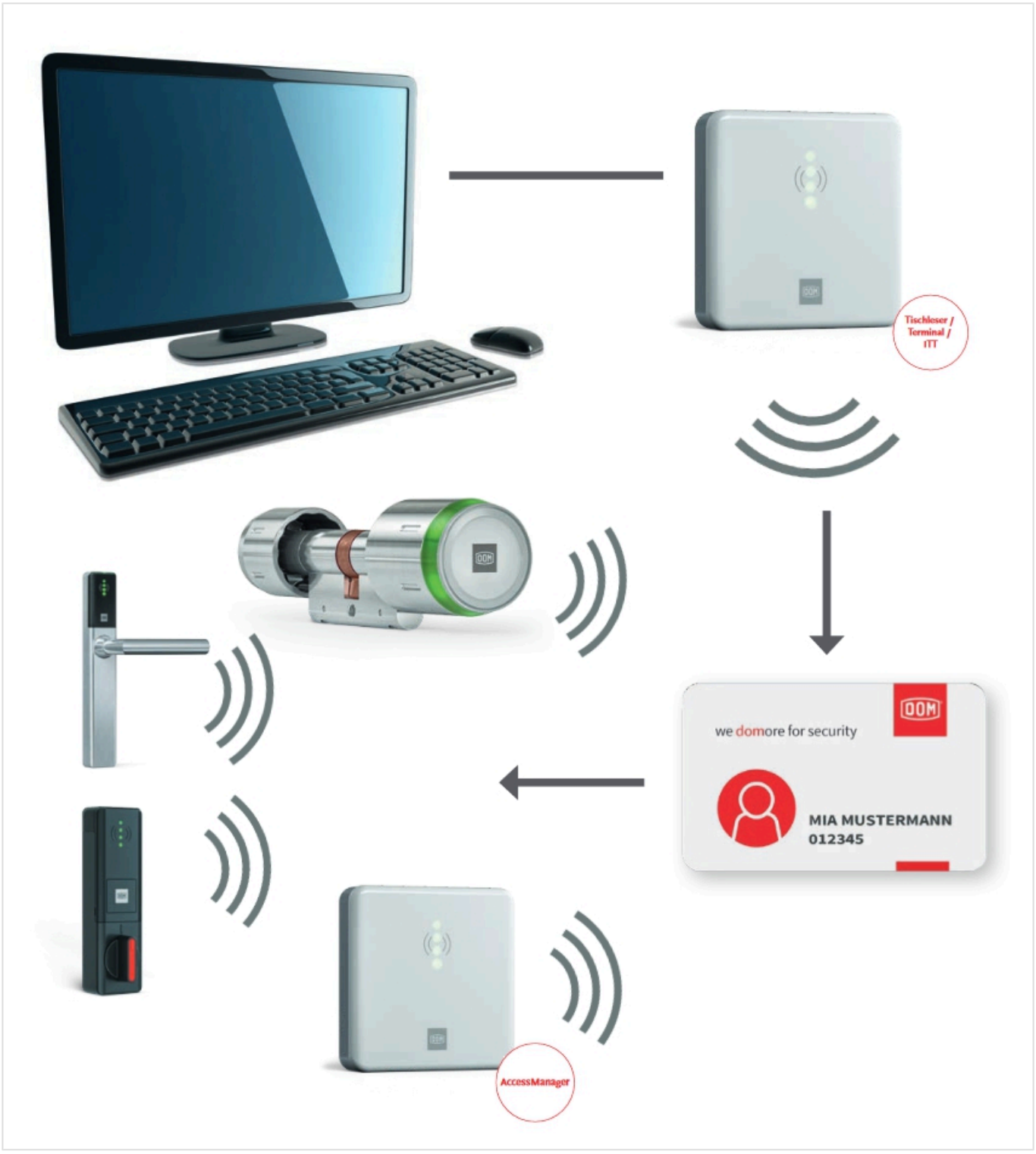
devices via the network connection and communication devices connected to the network.

As with software programming offline, using software gives you many additional features to make efficient use of your equipment. But now you can also program the terminal devices from the comfort of your office. Our digital cylinders and fittings are programmed with the help of a so-called RF NetManager. The RF NetManager is connected to your software via Ethernet and transmits the received data via radio (868 MHz (V1 devices) /2.4 GHz (BLE – V2 devices)) to the end devices. Our wall readers are directly connected to the Ethernet and thus to the software. Your changes made in the software, are then transmitted to the end devices in the shortest possible time. In addition, the terminal devices transmit to the software the events performed on them, such as the presentation of a transponder with time and date. The locking media are read into the software via a desk reader.



SOFTWARE PROGRAMMING – INTELLIGENT (DATA ON CARD):

The transponders are read into the software via a desk reader. When a transponder is read in, a person is created at the same time. The administrator can then define the authorizations for areas and according to times and store them on the transponder. It is also possible to create so-called groups of persons. This is very convenient if you need to create a large number of transponders (incl. associated person) with the same or similar authorizations. The persons can now simply be assigned to this person group and automatically take over the authorizations of their person group. Validity extensions of transponders can also be defined in the software. After the validity has expired, the transponder can no longer be used to open the door until the validity has been extended. The employee collects the validity extension, for example, once a day at a so-called terminal. When it comes to authorization changes, a so-called AccessManager ITT can be used. The AccessManager ITT can transmit authorization changes in addition to validity extensions. The “Software Programming Intelligent (DataOnCard)” operating mode can also be combined with, for example, the “Software Programming Offline” and “Online” operating modes. In such a system, all accesses to a building are programmed Offline or Online. The indoor areas are operated Intelligently (DataOnCard). This has the advantage that, for example, if a transponder is lost, only all terminal devices of the outer shell (building accesses) have to be reprogrammed directly. The finder of the transponder can now no longer enter the building. Unauthorized transponders are placed on a so-called blacklist for the intelligent (DataOnCard) area, which is written to all transponders with the desk reader or the AccessManager ITT. The transponders, in turn, now bring the blacklist to all end devices, so that the blocked transponders no longer function in the intelligent (DataOnCard) areas. Locking devices battery statuses can also be carried by transponders to the Software, when read by AccessManager ITT or Desk Reader (see Battery status collected by transponders).


Tischleser /
Terminal /
ITT
we domore for security
DOM
MIA MUSTERMANN
012345
AccessManager

2.1.5. Transponder

The ENiQ® system family can be operated with different transponder types (Mifare Classic, Mifare Desfire EV1,2,3, Mifare Ultralight/Ultralight C, Mifare Plus) and designs. We present a selection of the most common ones here. We offer individual transponder on request.

1. ENiQ® STANDARD TAG
The tag is available in black, red, green, white, blue or yellow. Also available with individual company imprint and as combination transponder (Hitag-Mifare).

2. ENiQ® PREMIUM PLUS TAG (13.56 MHz only)

3. ENiQ® ISO CHECK CARD TRANSPONDER
A very common transponder design. Areas of application for “ISO check card” transponders are time recording or accounting systems as part of employee management systems. Of course, “ISO check card” transponders can be printed individually and are available as combination transponders.

4. ENiQ® CLIP TAG

A real DOM innovation. The clip tag combines mechanical locking technology with digital access control. Thus, all conventional (DataOnDevice) systems of the RS series and all reversible key systems of the IX series can be integrated or retrofitted into the clip tag. In this way, a single transponder is used for both worlds of mechanics and electronics – and the size of the keychain is reduced.

With the Clip Tag, DOM-Sicherheitstechnik offers the possibility to use only one transponder when combining mechanical and digital locking systems.

MASTER CARD

The Mastercard is the most important card in your system. It serves as proof of ownership and you can use it to add or remove digital terminals from your facility. The Mastercard can also be used to authorize transponders and programming cards. After using the Mastercard, it should be stored in a safe place, e.g. in a safe.

PROGRAMMING CARD

The programming card is the second most important card in DOM digital locking systems. Up to 5 programming cards can be stored per terminal device. It can be used to create transponders, delete individual transponders in case of physical presence or reset all authorizations of transponders in end devices.

RF WAKE-UP CARD

The RF wake-up card is used to activate the radio interface in the terminal devices in order to communicate wirelessly with the terminal device by means of software. An additional component (e.g. USB radio stick) may be required for wireless communication. This enables battery-saving operation.

RF ONLINE CARD

The RF-Online card is used to establish the connection between RF NetManager and battery powered device.

PERMANENTLY-OPEN CARD

The permanently-open card can be used to set a terminal device to the so-called “permanently-open” mode, as well as back to the initial state. If this “permanently-open” mode is active, the terminal device can be accessed at any time without authorization check. This is done e.g. during business hours with many visitors at main entrance doors, when a reception desk is permanently occupied behind them.

PERMANENTLY-CLOSED CARD

The permanently-closed card can be used to set a terminal device to the so-called “permanently-closed” mode, as well as back to the initial state. In this mode the authorization check is deactivated and the device can be accessed only with specially authorized transponders. This mode is used, for example, to block entry into a building while the alarm system is armed.

INSPECTION CARD

The inspection card is a special card for the ENiQ LoQ. It is used to perform maintenance, inspection

and emergency opening in multi-user mode.

BATTERY CHANGE CARD

With an authorized battery change card, you confirm at the end device that the battery has been changed. The card must be previously authorized at the end device via card programming or software.

SERVICE MAINTENANCE CARD

DOM terminal devices can also be used to equip escape and rescue routes. Escape and rescue routes according to DIN EN 179 and 1125 must be maintained regularly. This maintenance must be legally recorded. By holding the service maintenance card, the event “Maintenance performed” is stored on the terminal device and forwarded to the software. The event is then legally logged and stored for you in the database.

INSTALLATION CARD

For functional testing of devices in installation situation, before a Mastercard or software has been created.

TRANSPONDER MANAGEMENT CARD

The transponder management card is only available in a 1:1 ratio with a transponder. The transponder management card contains the information about the associated transponder. With the help of the transponder management card and a Mastercard/programming card, it is possible to create and delete exactly this transponder, in case of physical absence. When a transponder management card is held directly on a terminal device, the terminal device displays the authorization status of the associated transponder. It is not possible to close with the transponder management card, the cards themselves have no authorizations.

The transponder management card is available for the operating mode Card Programming Offline with EasyFlex and only for the ENiQ (Mifare 13.56 MHz) system world

3. Installation

This chapter describes an initial installation of the ENiQ software on a system on which an older version has not yet been installed.

Before you start the installation, check if your PC meets the necessary system requirements.
Please refer to the technical data sheet.

It is generally possible to update from earlier versions to the current ENiQ version.

The installation CD contains all files necessary for the installation of the ENiQ software as well as the SQL OEM version.
Normally the installation program starts automatically when you put the CD into the drive.
If this is not the case, you have to start the program manually.

> ! Attention. Close all programs before you start the installation.
> If any error messages appear, follow the instructions.

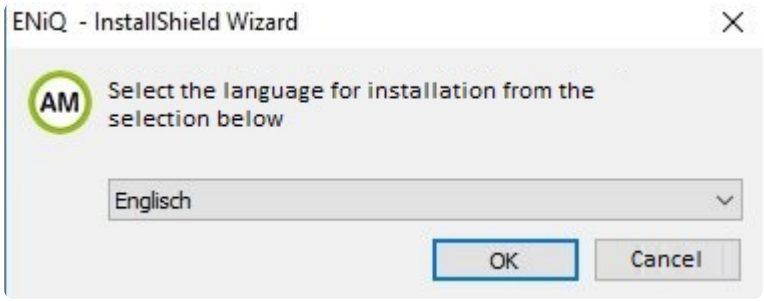
> ✻ Please note that the installation can be performed only on Windows 10/11 computers

> ! Windows 8 and older versions are no longer supported!

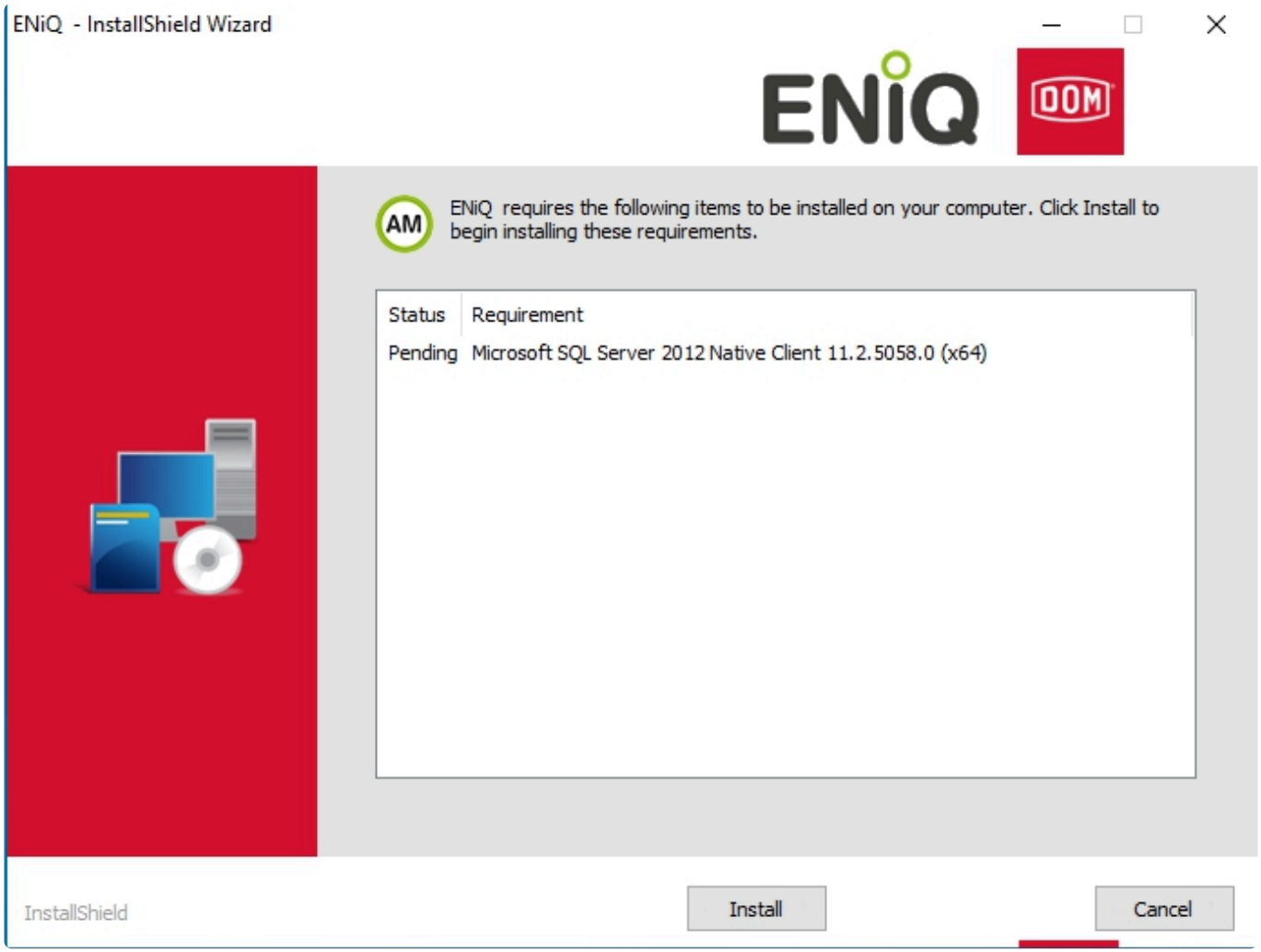
3.1. Standard installation of the ENiQ software

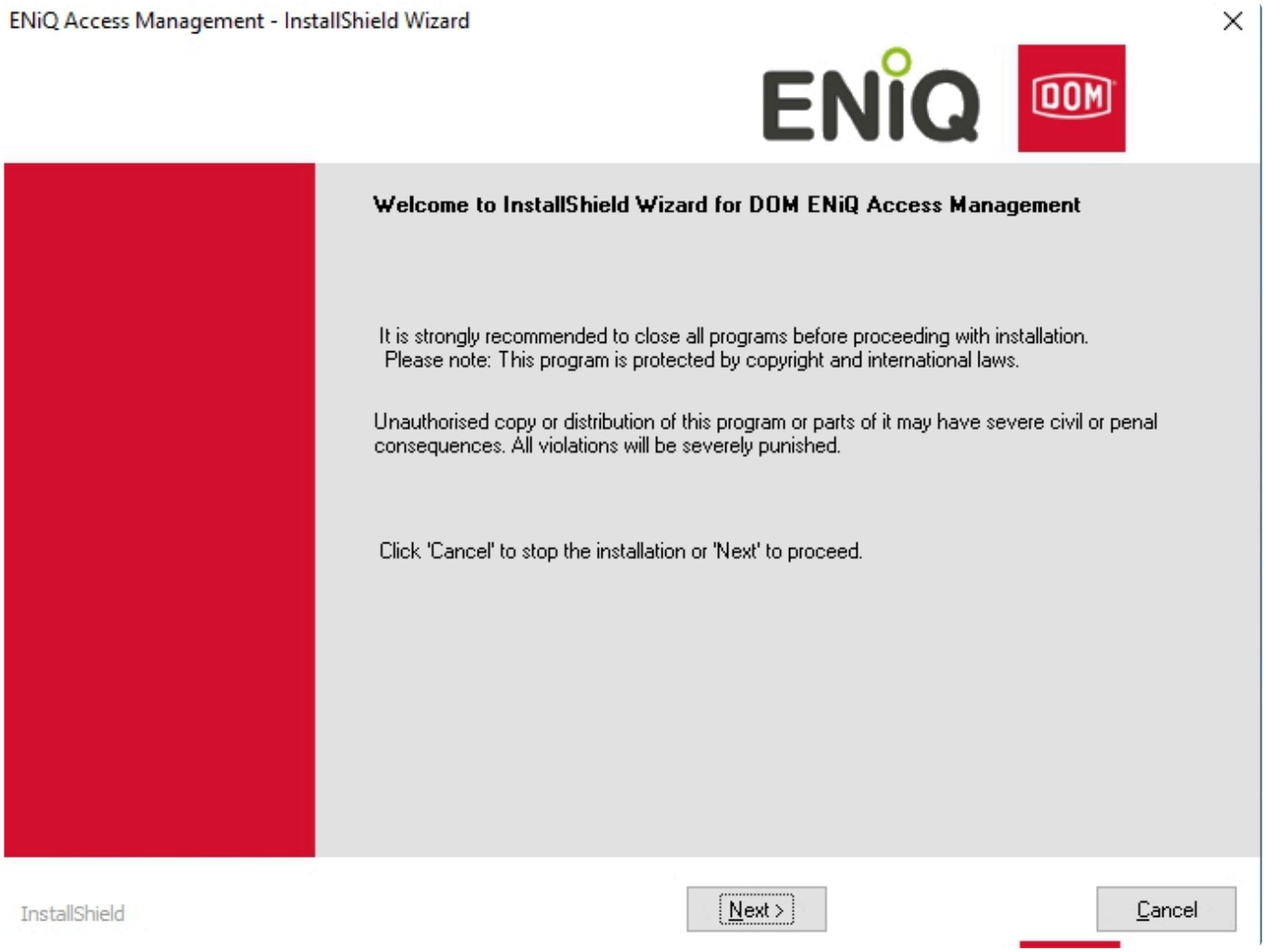
In this variant of the installation you receive the full functional range of the software on a central computer.
The complete ENiQ software, the database and the drivers for the desk reader and the RF radio stick are combined on this computer.
This type of installation is suitable for smaller objects without an own server in the data center.

START THE INSTALLATION
Insert the CD into your PC or start the setup program from your local folder.
After a short loading pause a dialog box opens where you can select your preferred installation language:



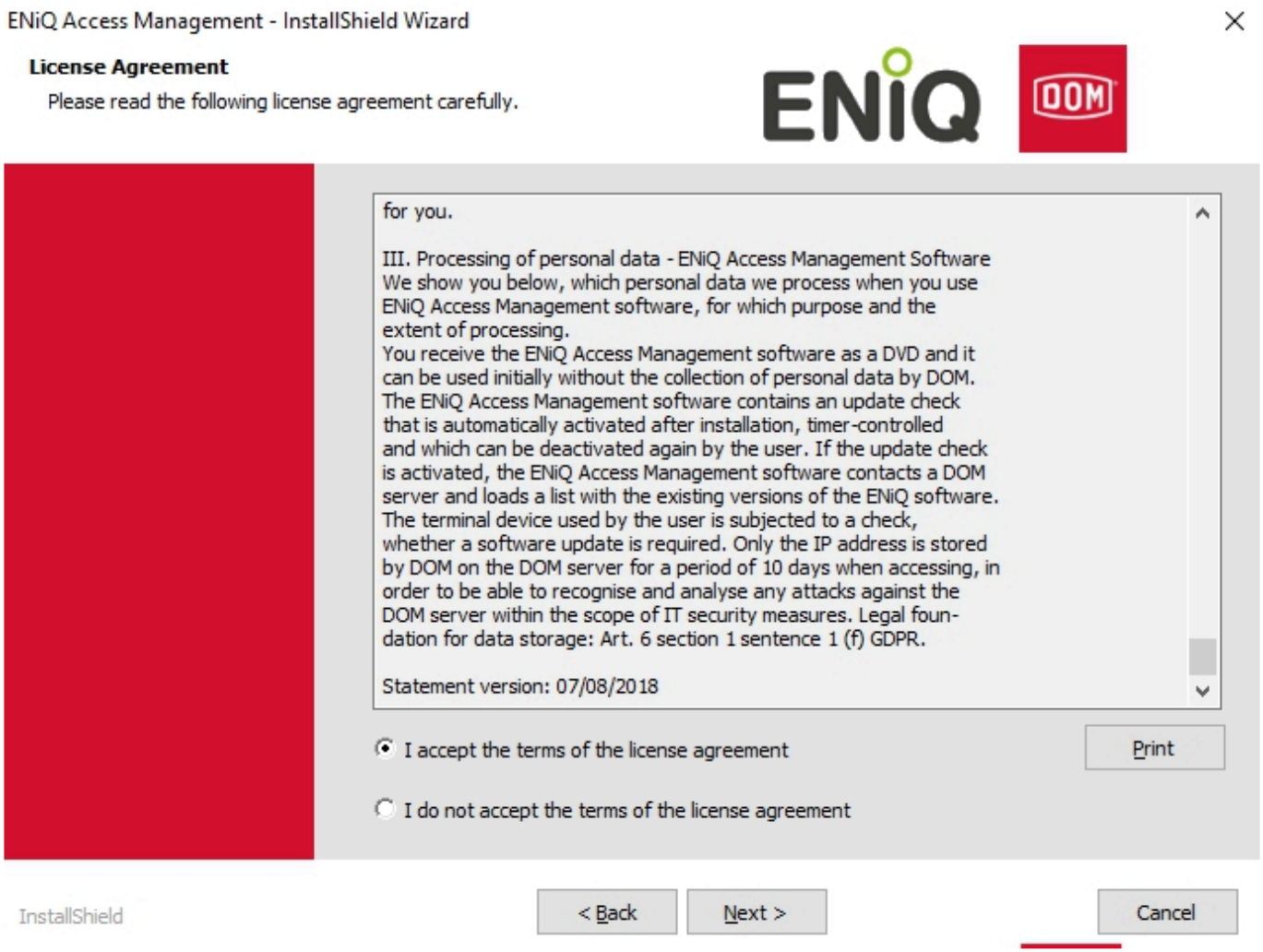
The next dialog shows you which elements are still needed to install ENiQ.


ENiQ - InstallShield Wizard
ENiQ
DOM
AM
ENiQ requires the following items to be installed on your computer. Click Install to begin installing these requirements.
Status
Requirement
Pending
Microsoft SQL Server 2012 Native Client 11.2.5058.0 (x64)
InstallShield
Install
Cancel

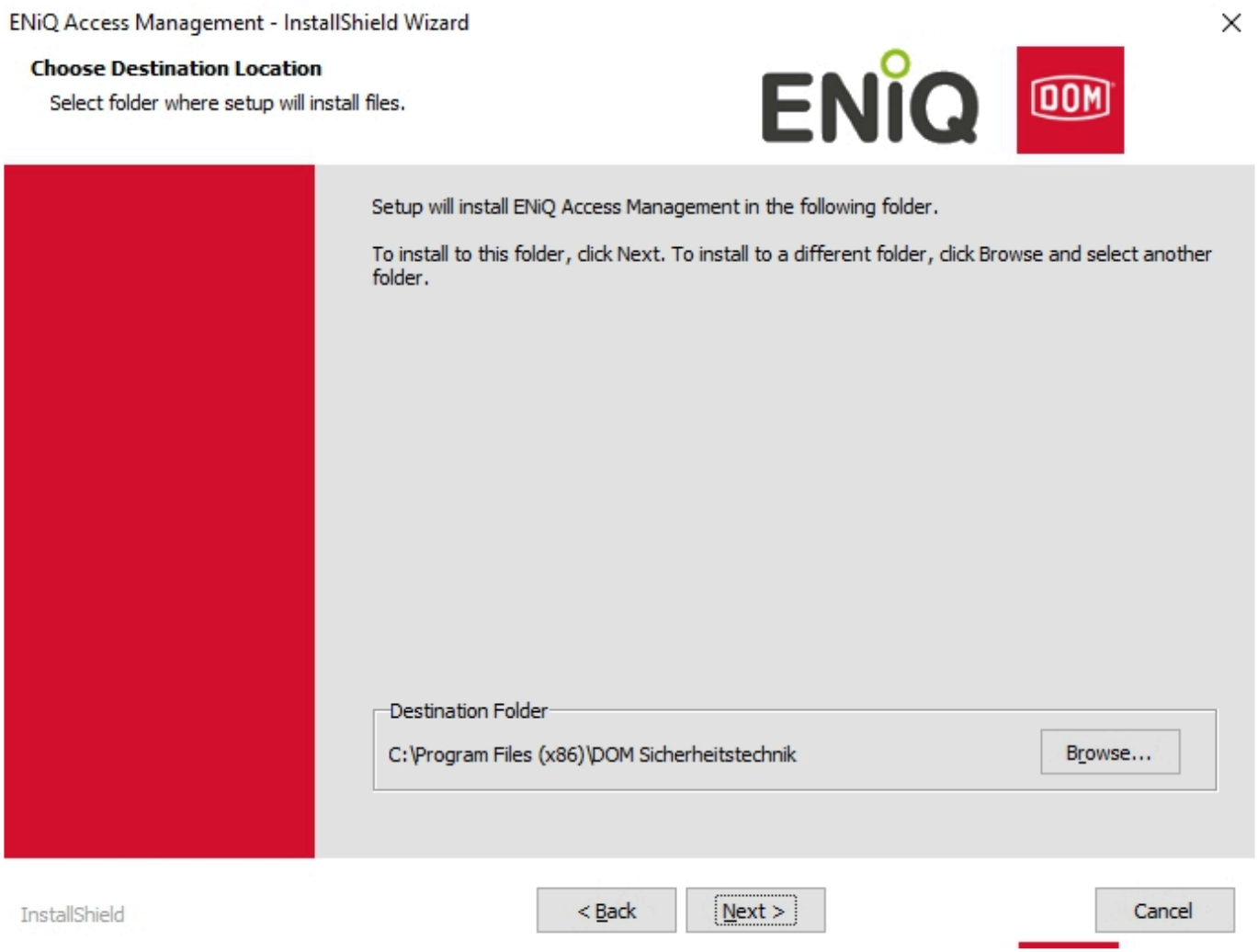


In this dialog you get your computer configuration. If problems occur during the installation, this information can be helpful.

License agreement:

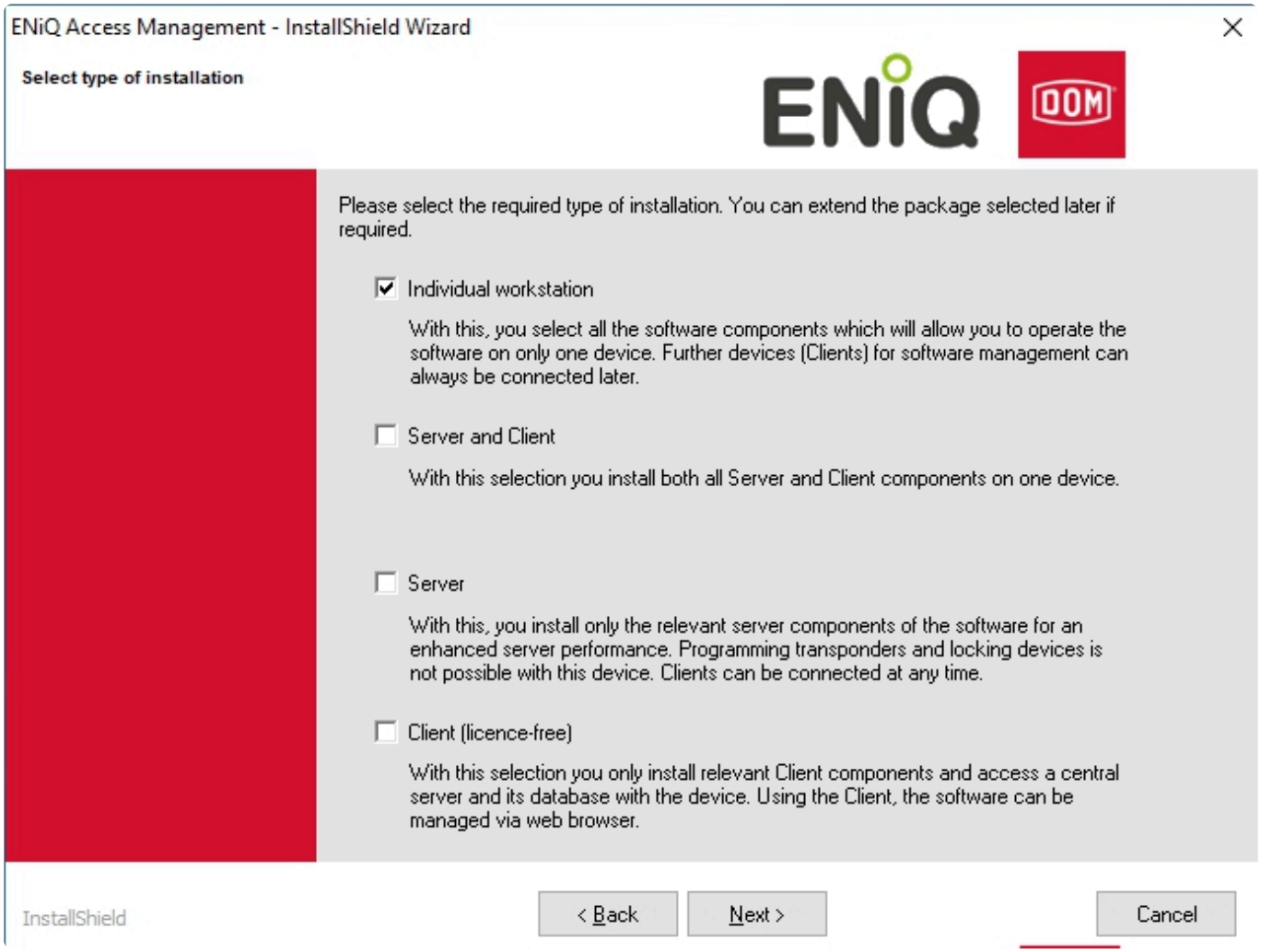


Now specify the target directory of your installation.
Normally you should use the suggested path:



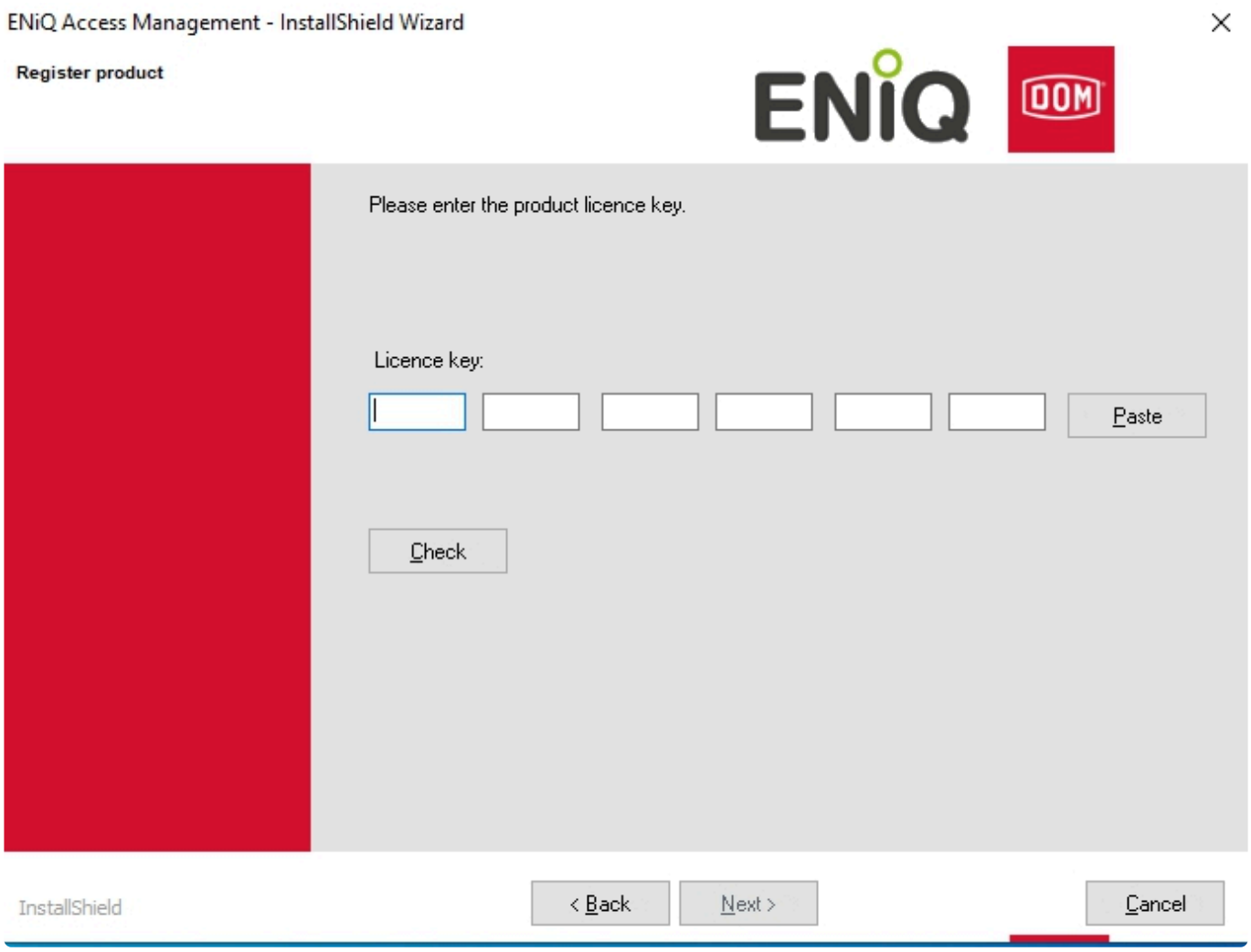
PRODUCT REGISTRATION/LICENSING

Select the desired installation type that is included in your package.



You can also expand the package selection (license) later if needed.

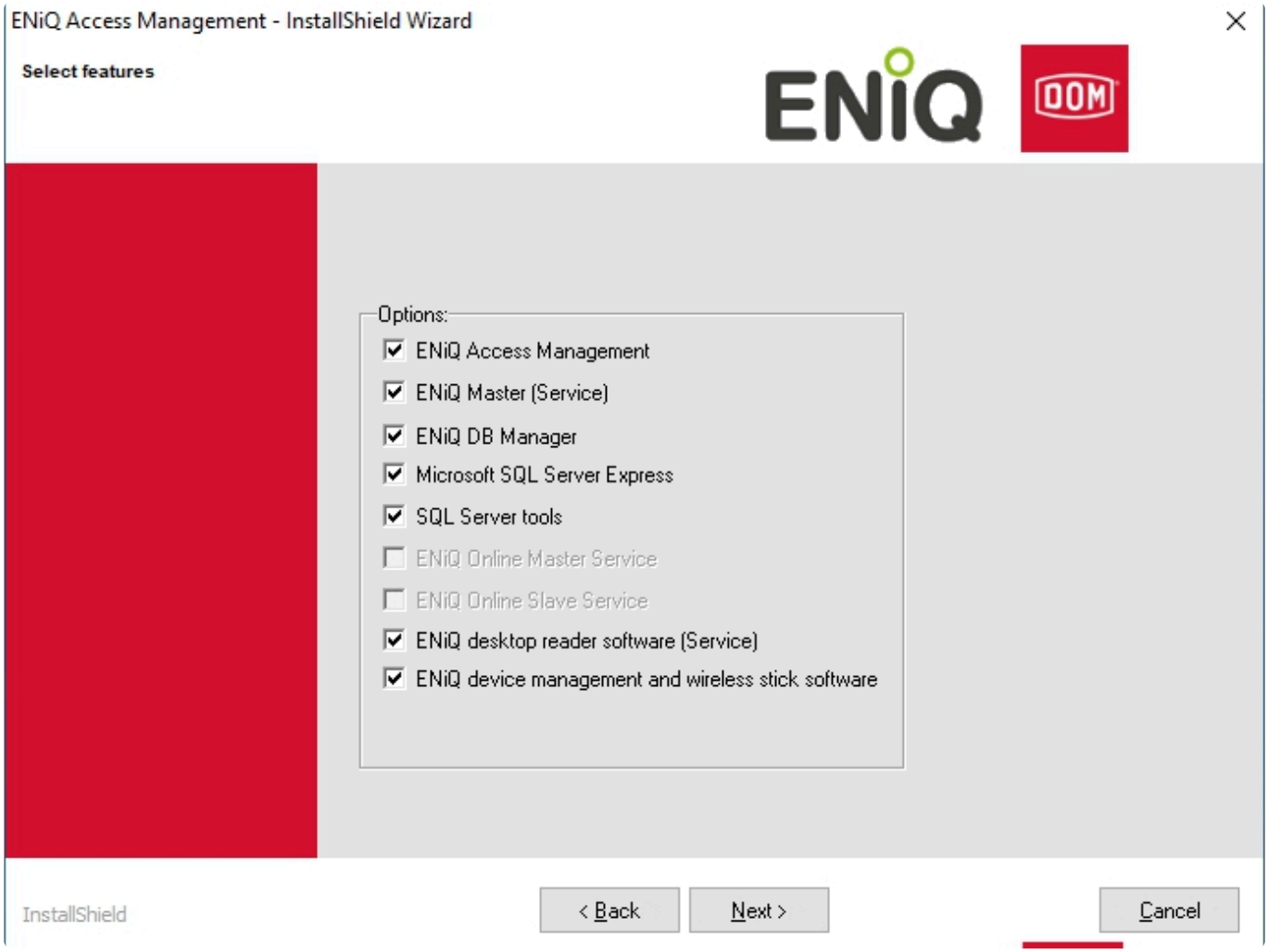
Fill in the fields here. The license key can be copied from another source (e.g. email) and inserted into the fields using the “Paste” button.



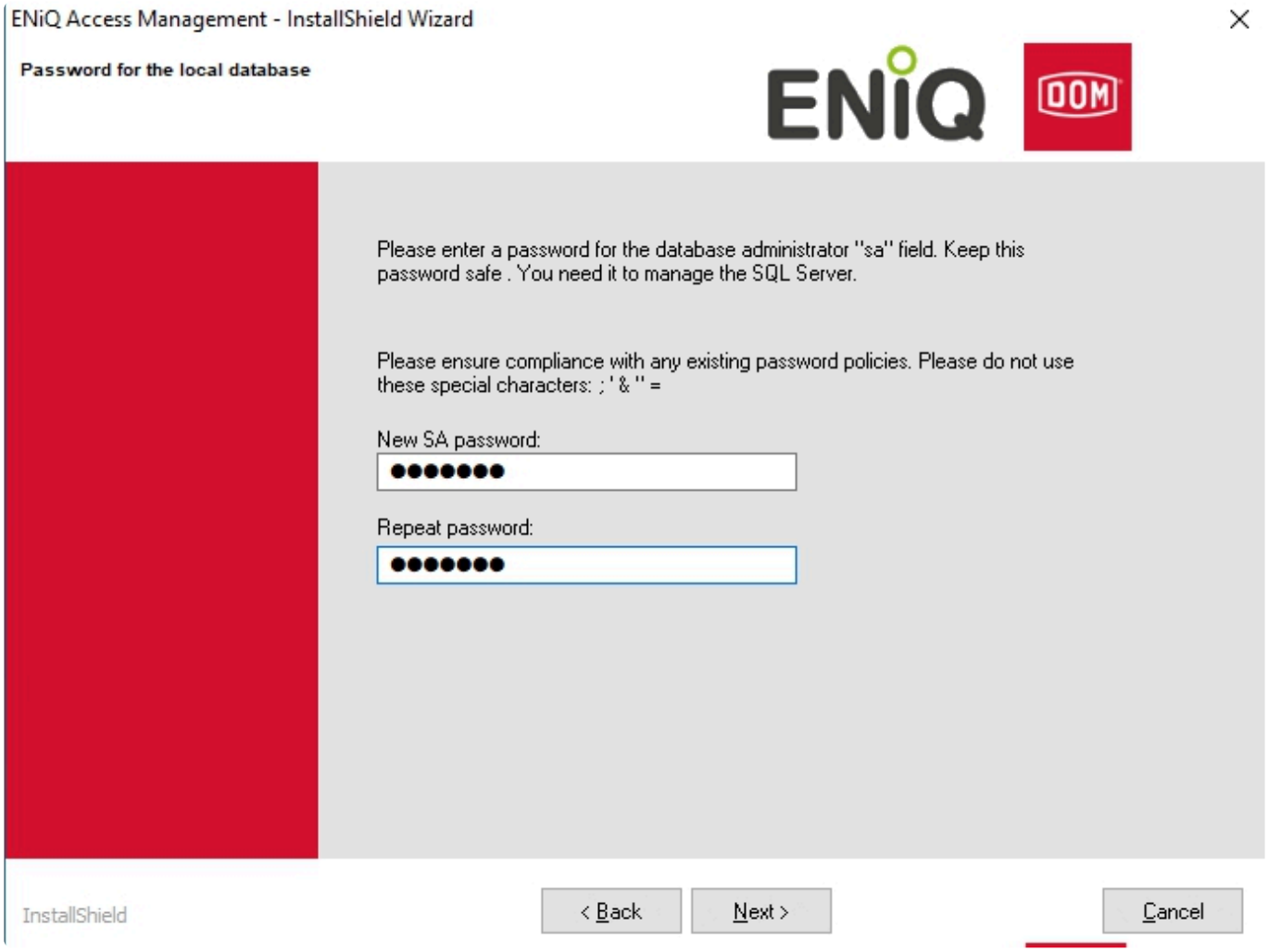
Click once on the button “Check” to validate the correctness of the key.

If you want to perform a client installation, select the checkbox “license-free …. only”. In this case you don’t need another license number, because the product is already registered via the server (see document Client Installation).

For the standard installation, select all options.
If you have additionally purchased an online license, the options “Online Master” and “Online Slave” are preselected.



MS SQL-SERVER INSTALLATION



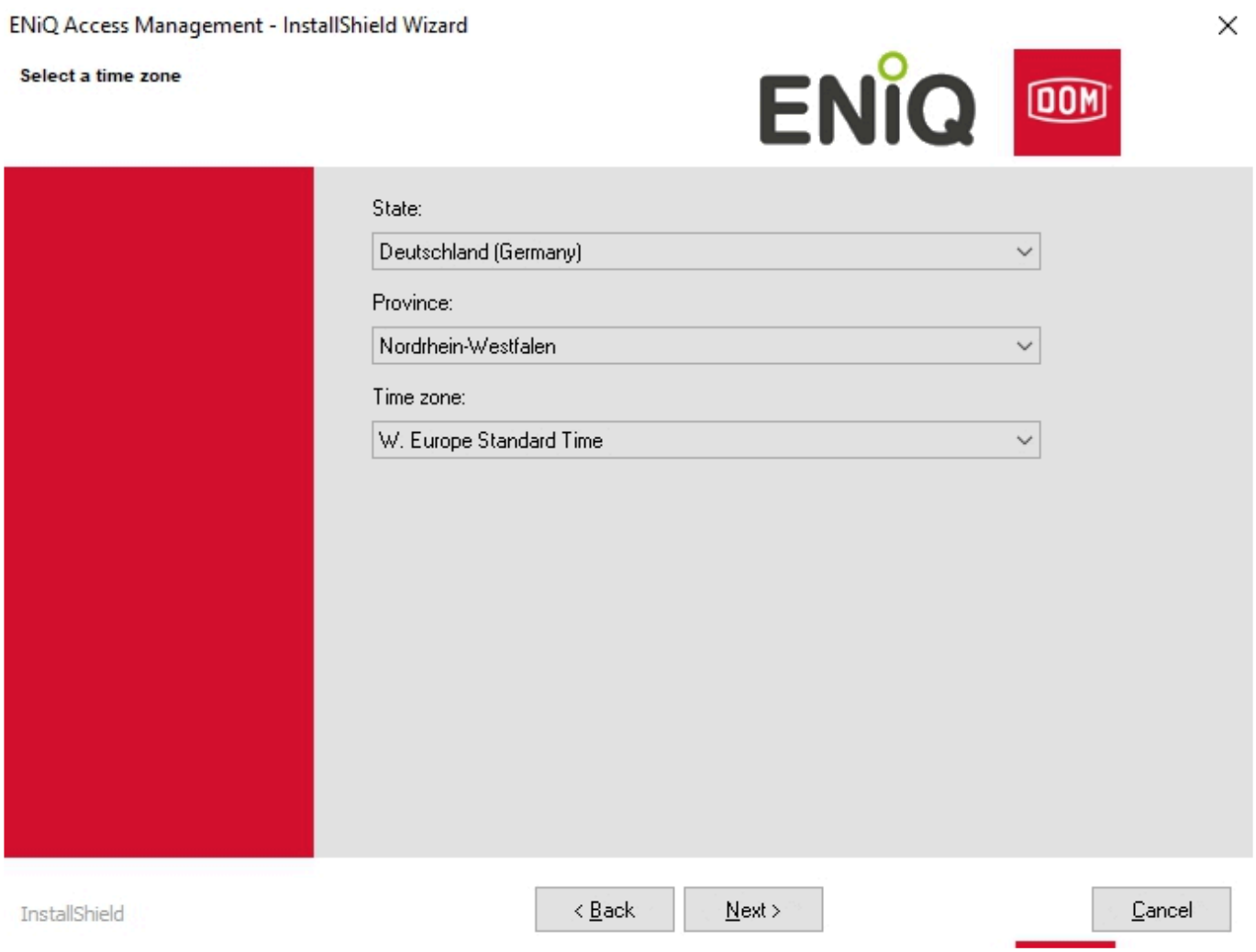
The installation software now tries to install a database server. For this purpose the main password of the database is requested.
Please enter a “complex” password, which contains at least 6 letters, 2 numbers and one special character.

> ! Please do not use “&”, quotation mark or apostrophe!

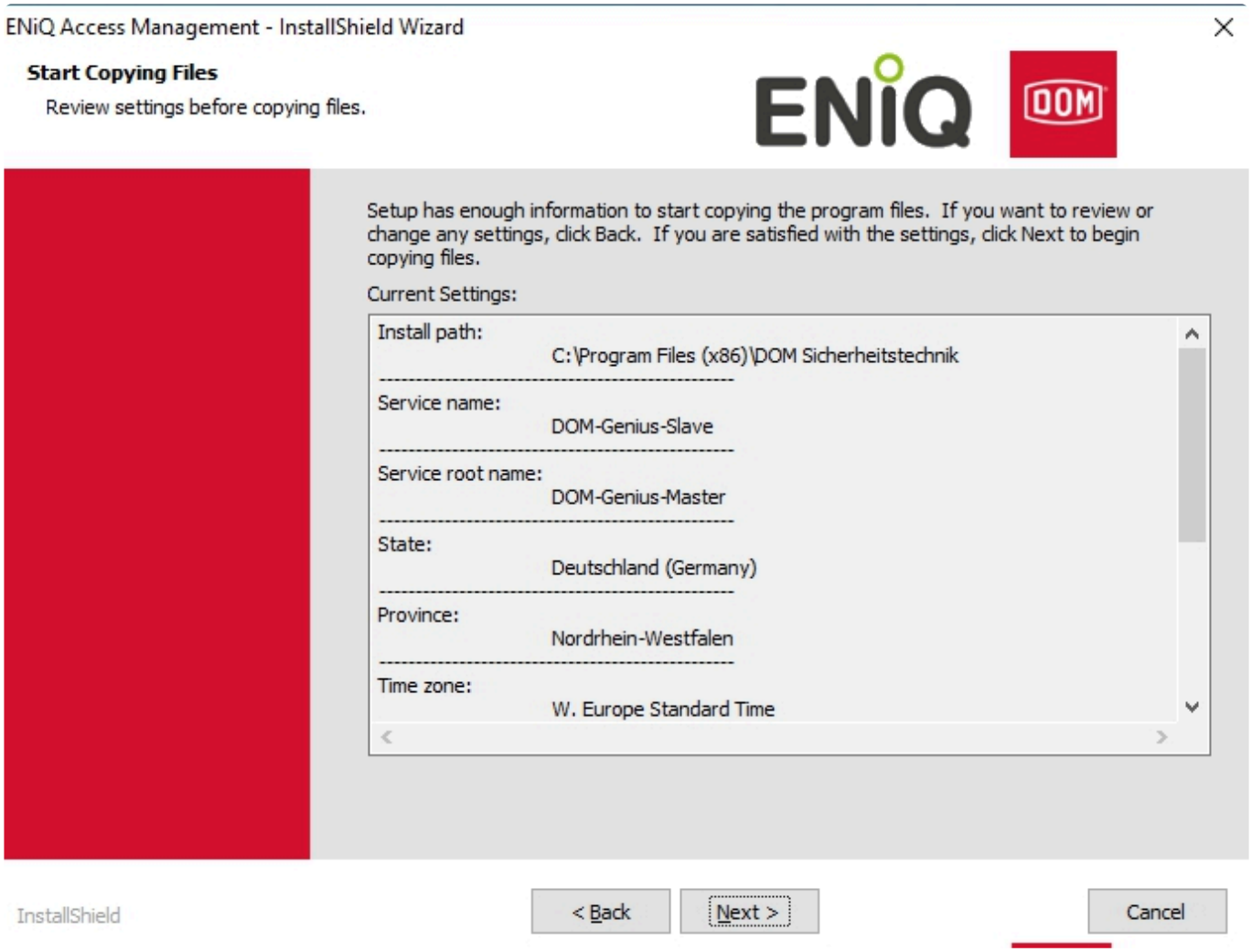
> ! If your computer works in a network, then follow the password policy specified there.

Keep the password safe – in case of database recovery, the password will be needed.

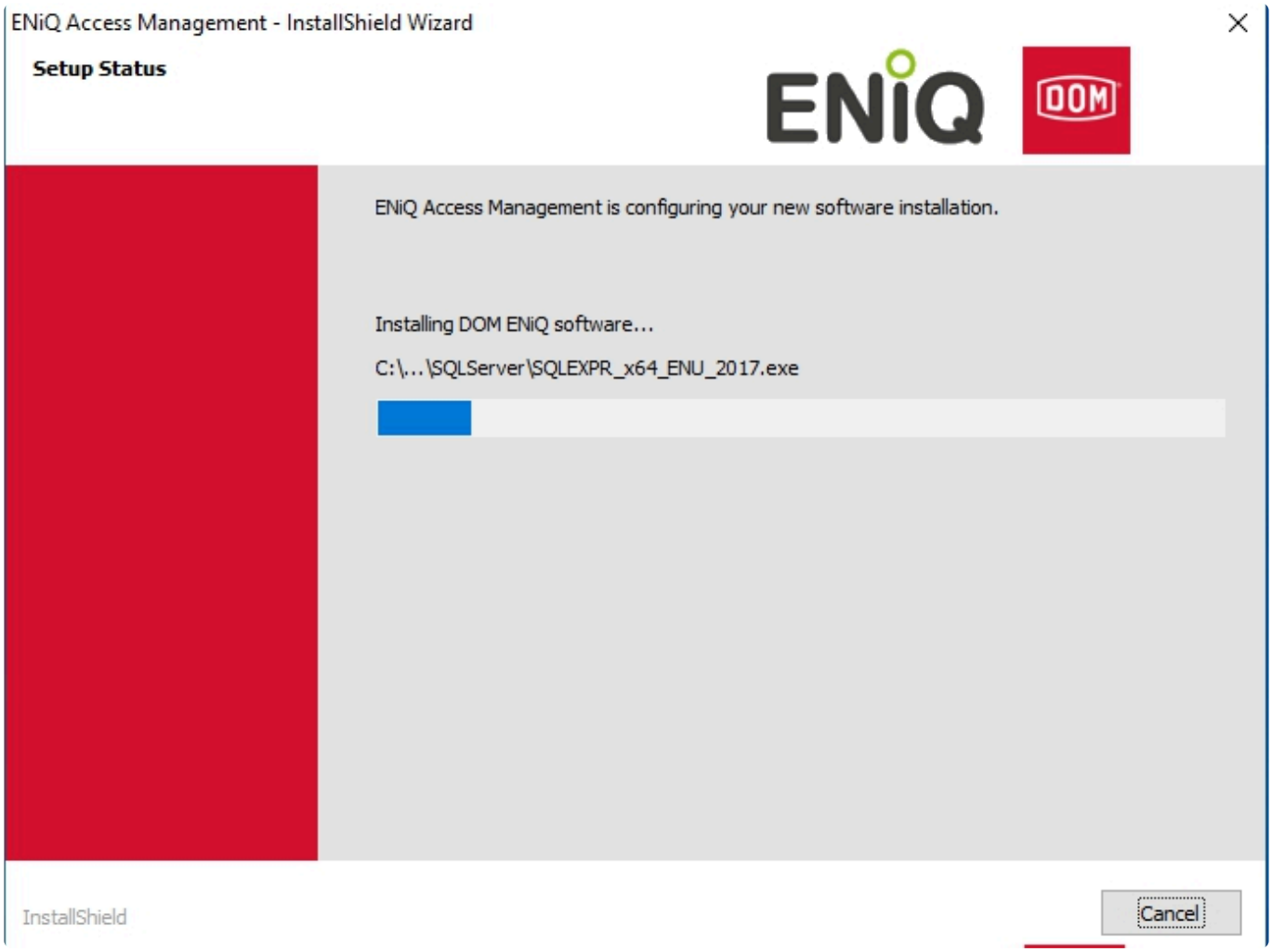
Select your local zone:



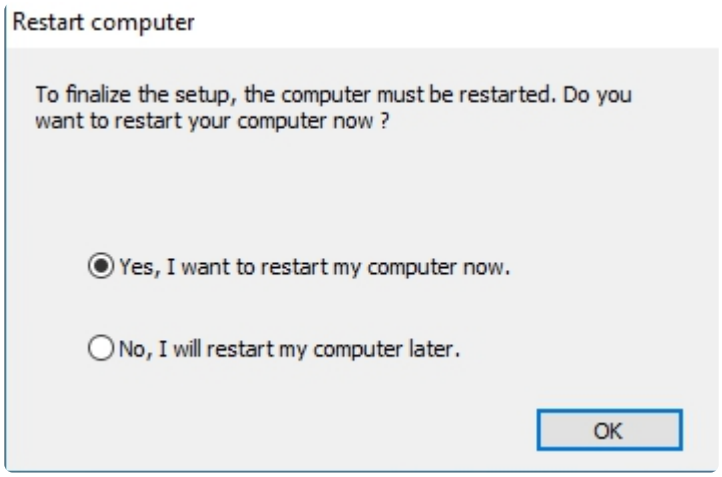
Afterwards you will see an overview of the installation.



Start the automatic installation process by clicking on continue:



Finally a restart of the computer is necessary.



After the restart you can use your ENiQ AccessManagement software.

At the first start after the installation the ENiQ software reacts a little bit delayed, because files are still updated in the background

4. Set up

This chapter describes how to set up the software

- Set up administrator
- Set up operator
- Managing passwords
- Assigning roles
- Getting familiar with the user interface
- Device management
- Integrate desk readers

4.1. Launch ENiQ Access Management

Prerequisites
To use the software, the following requirements must be met:

- Complete installation of the program on the computer
- Database available
- Desk reader connected, for information on how to integrate the desk reader into the software, see “Integrating desk readers”
- Service DOM-Master Service started (the icon shown below in the taskbar shows green)
- DOM-Slave Service started (the icon shown below in the task bar is green)

Start software

> The ENiQ software has a web interface. When you start the software, it will be displayed in the default web browser.

To be able to work with the software, you have to start it on your computer.

- Double click on the corresponding icon on the desktop.

- The software will start.

> For certain operations it is necessary to switch from the ENiQ Device Management software to the ENiQ software or vice versa.
> In such cases, start the ENiQ Device Management software and the ENiQ software in parallel.

4.2. Admin/ Operator setup

Create operator profile

The ENiQ software can be used by several operators. For this purpose, you as the system administrator must create the corresponding operator profiles in the software.
To create an operator profile, proceed as follows:

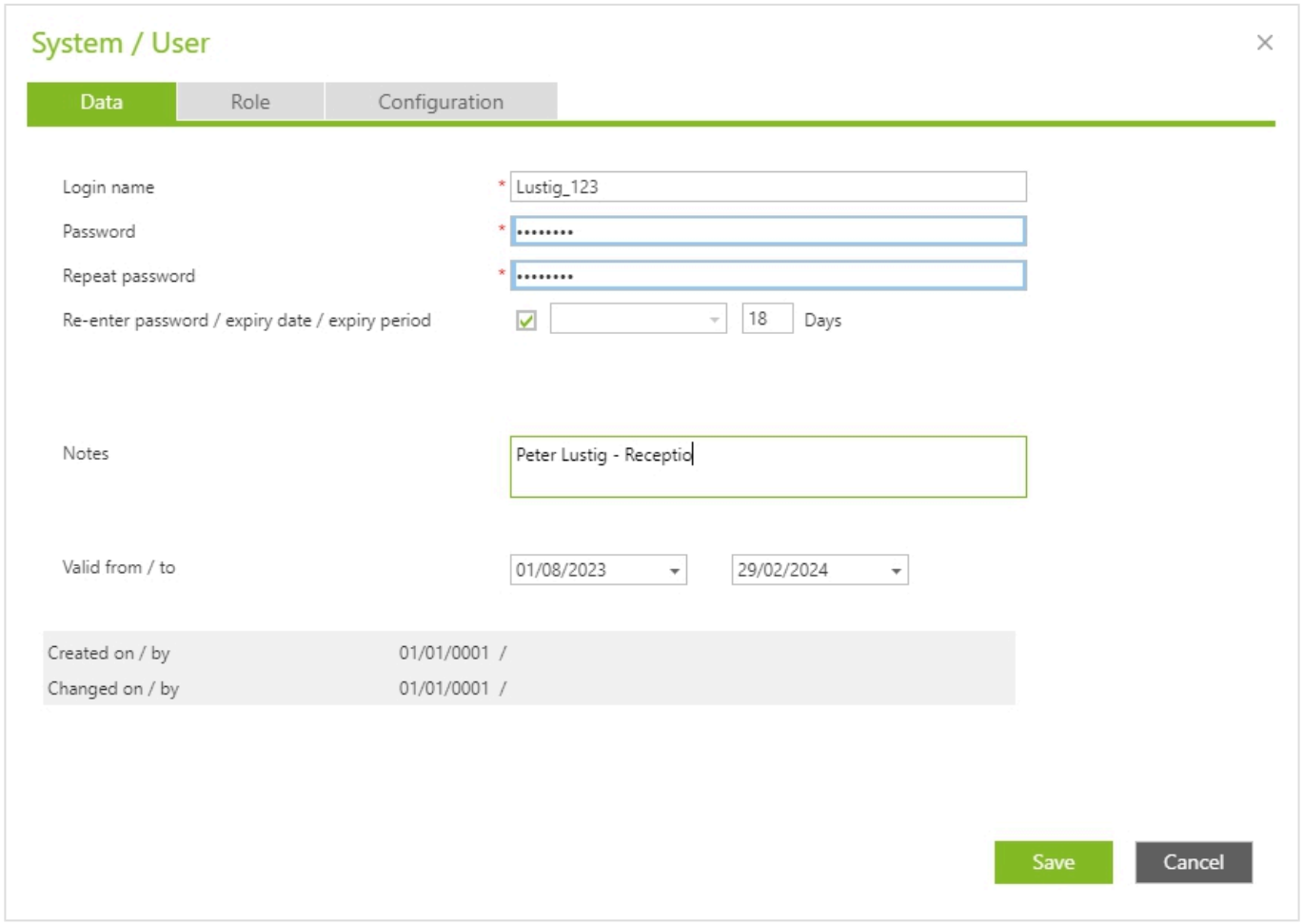
- Click on “System” in the navigation bar.
- Select the “User” menu item.

The “System / User” menu opens.

- Click on the “Add” button.

The “System / User” menu opens. The “Data” tab is displayed.

- Enter the desired login name for the new operator.
- Enter the password for the new operator in the “Password” field.
- Repeat the password entry in the “Repeat Password” field.
- Password guideline: At least 6 characters (at least 1 uppercase letter, at least 1 lowercase letter, at least 1 digit).



You can set a time limit for the password for the person profile. To do this, you can either specify a date on which the password expires. You can also specify an interval after which a new password must be assigned. To do this, proceed as follows:

- Select the “Re-enter password.” radio button.
- Enter the desired expiration date for the password.
- If desired, enter the time interval after which a new password must be assigned.

You can now save additional properties in the person profile.

- If desired, enter a comment for the operator profile.

If you want to set a time limit for the operator profile, proceed as follows:

- Enter the date from which the operator profile is active.

If you do not enter a date here, the operator profile is active immediately.

- Enter the date until which the operator profile is active.

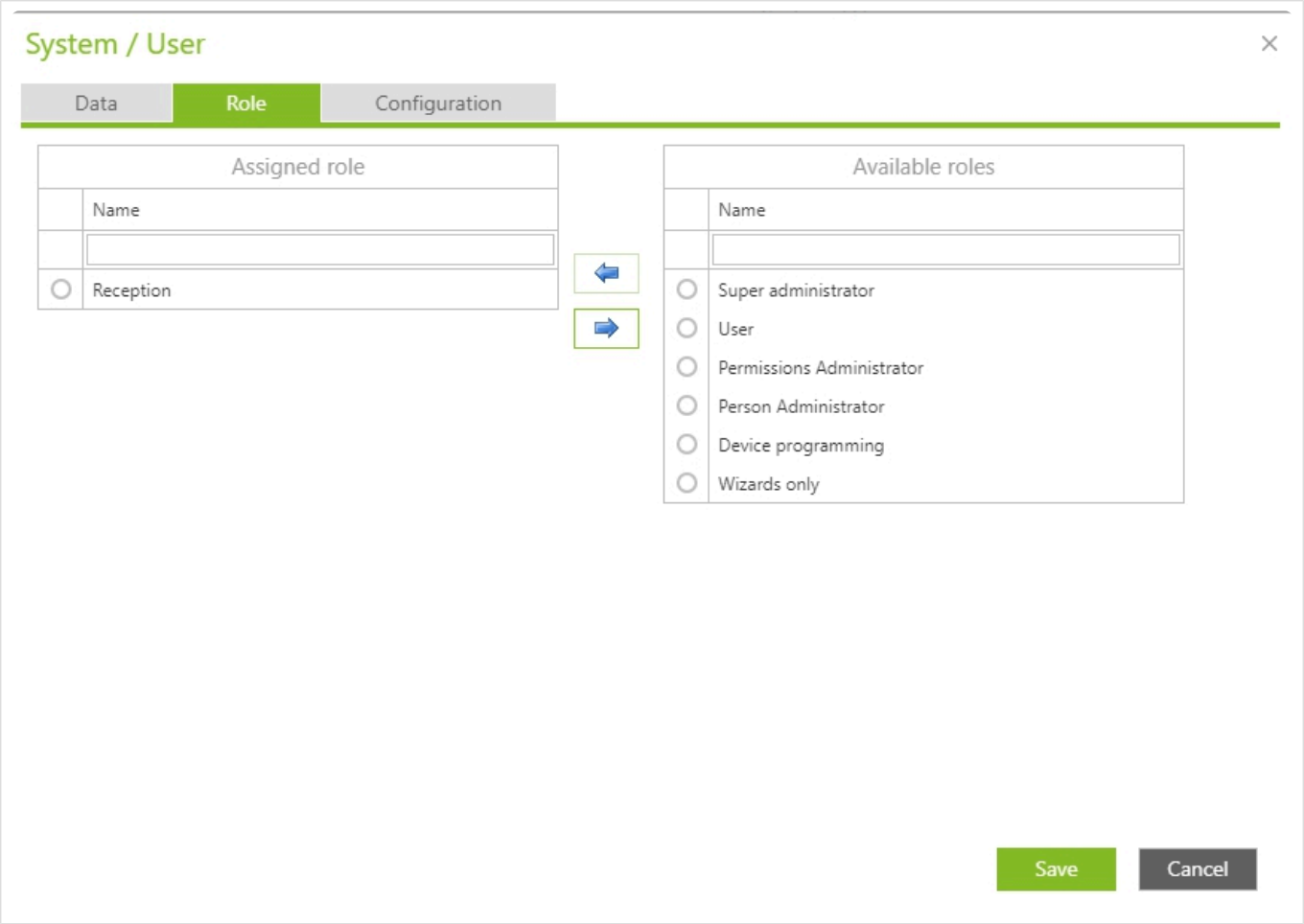
If you do not enter a date here, the operator profile is permanently active.
In the lowest lines you can see which person created the operator profile and when or by whom it was changed.

- If you want to discard the entries, click the “Cancel” button.
- Save the settings.

To assign operator rights to the new operator, you must now assign a role to the operator profile. Information on this can be found in the following section.

Assign operator rights

You must assign operator rights to an operator profile via so-called “roles”. Several roles are predefined in the program for this purpose. Depending on the assigned role, the operator profile has certain operator rights.



To assign a role, proceed as follows:

- Make sure that the desired operator is created in the system, as described in the previous section.
- Switch to the “Roles” tab.
- Enter the desired operator name in the “Name” field.
- In the “Available Roles” area, select the radio button for the role you want to assign to the operator.
- Click “Add.”

The selected role is added to the “Assigned Roles” area.

- To discard the entries, click the “Cancel” button.
- Save the settings.

The operator now has the operator rights associated with the selected role.

See all the available operator roles in the Operator section.

4.3. ENiQ DeviceManagement

Prerequisites

To use the software, the following requirements must be met:

- Complete installation of the program on the computer
- Database available
- USB wireless stick connected
- ENiQ-Master Service started (the icon shown below in the task bar shows green)
- ENiQ-Slave Service started (the icon shown below in the task bar shows green)

Start software

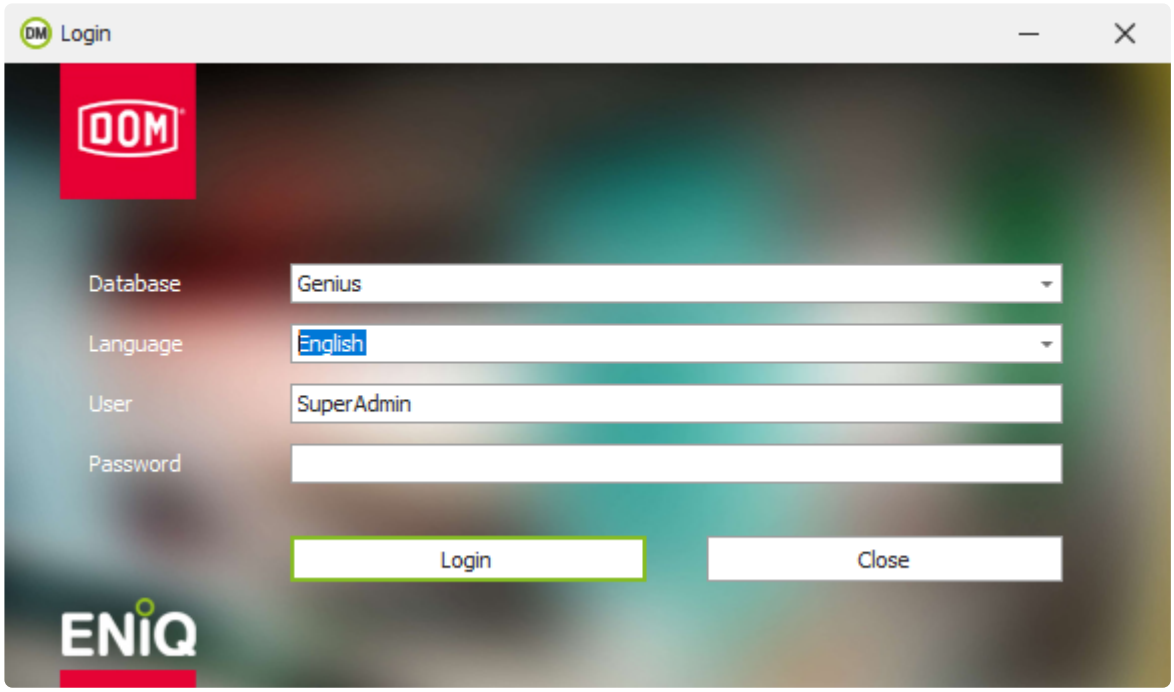
To be able to work with the software, you have to start it on your computer.

- Double click on the corresponding icon on the desktop.

- The software will start.

For certain operations it is necessary to switch from the ENiQ Device Management software to the ENiQ software or vice versa.
In such cases, start the ENiQ Device Management software and the ENiQ Access Management software in parallel.

Login
After the program start you will see the displayed screen:



To log in to the program as administrator, proceed as follows:

- Select the desired language in the selection window.
- Click into the input field “Password”.

As password use the identical password that you use in ENiQ AccessManagement.

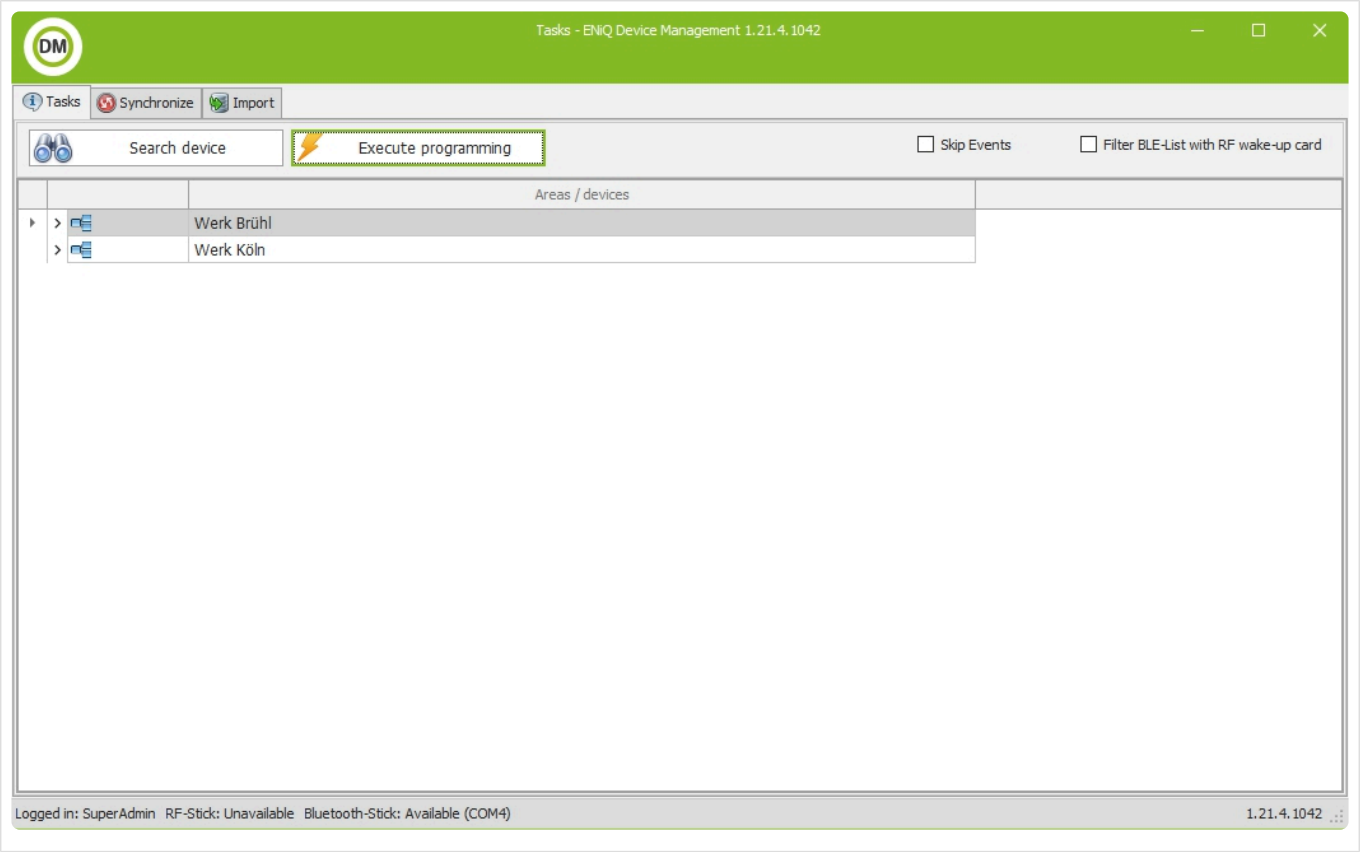
- Enter the password.
- Click on “Login” or press the “Enter” key.

The program opens and the program interface is displayed.

To log in to the program as a different operator, proceed as follows:

- Select the desired language in the selection window.
- Click in the “User” input field.
- Enter the desired operator name.
- Click in the “Password” input field.
- Enter the password.
- Click on “Log in” or press the “Enter” key.

The program opens and the program interface is displayed.



If the “Search Devices” button is grayed out, you have not connected the USB wireless stick.

- Exit the ENiQ Device Management software.
- Connect the USB radio stick.
- Restart the ENiQ Device Management software

4.4. DOM Service app

The DOM Service app can be used to synchronise offline devices.

Prerequisites

To use the software, the following requirements must be met:

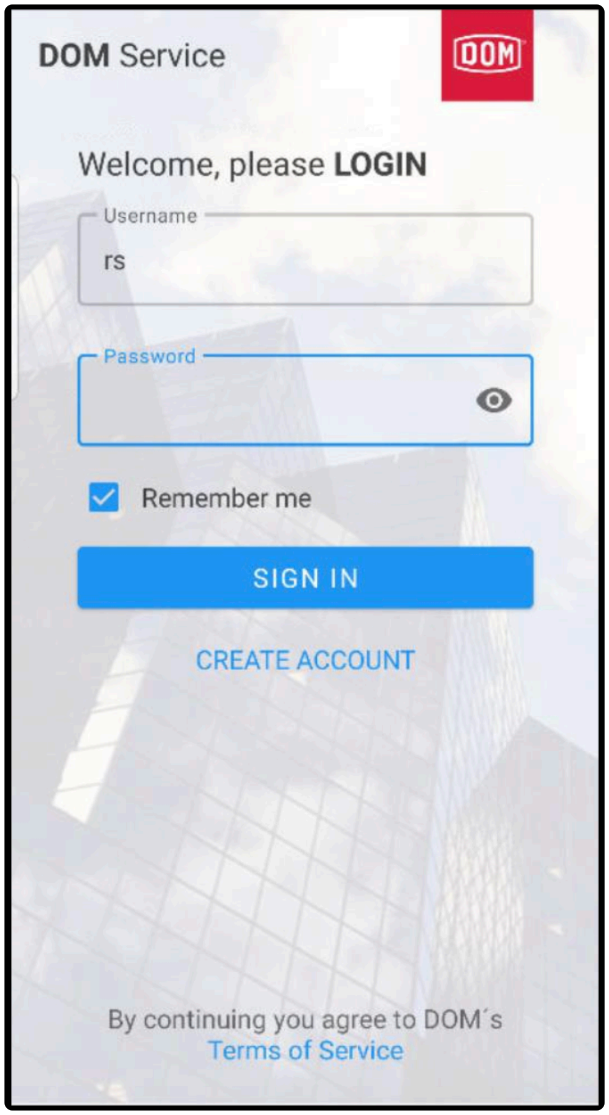
- Complete installation of the program on the computer
- Database available
- The DOM Service app can access the network of the ENiQ AccessManagement software

> To synchronise the ENiQ AccessManagement software and the DOM Service App, both components
> must be in the same network (Wifi or LTE/VPN).

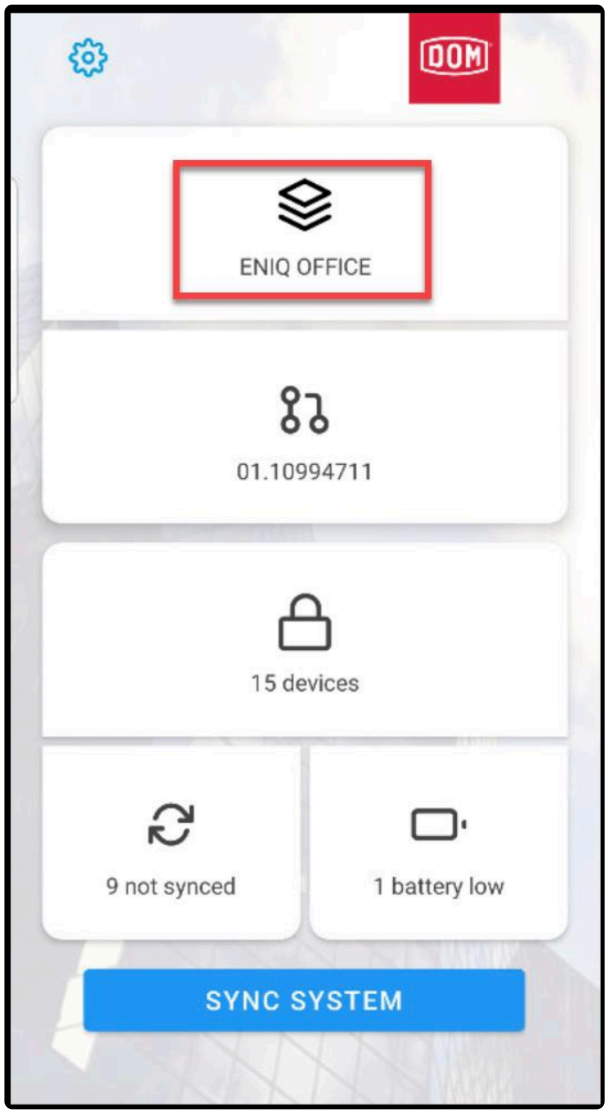
Setup DOM Service app

- Download the DOM Service app from Google Playstore or Apple App Store

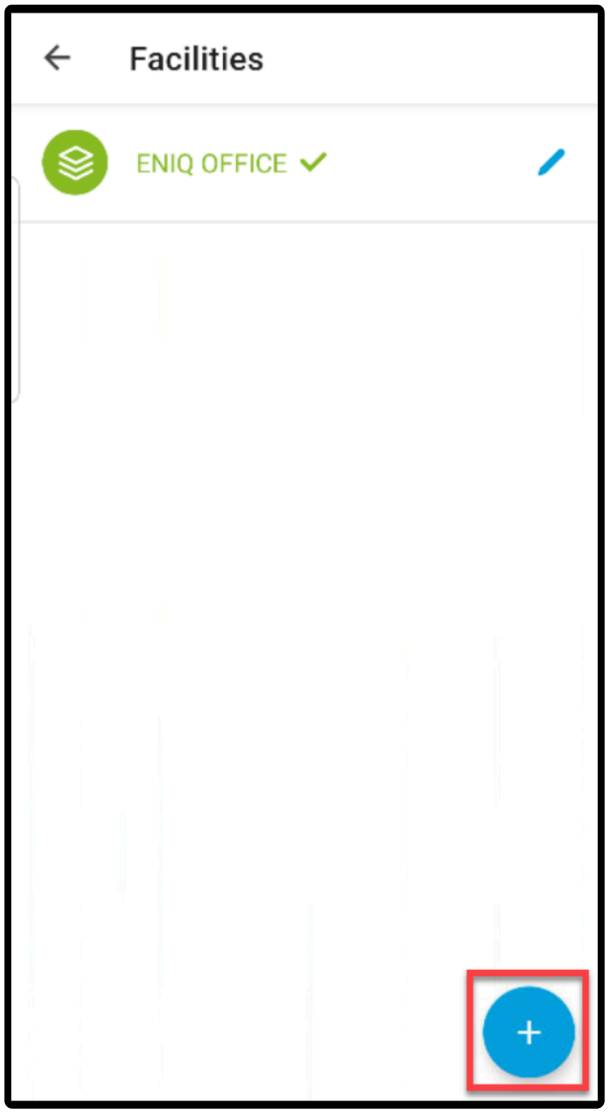
- Open the app, create an account, then sign in.



- Tap on “Facility”

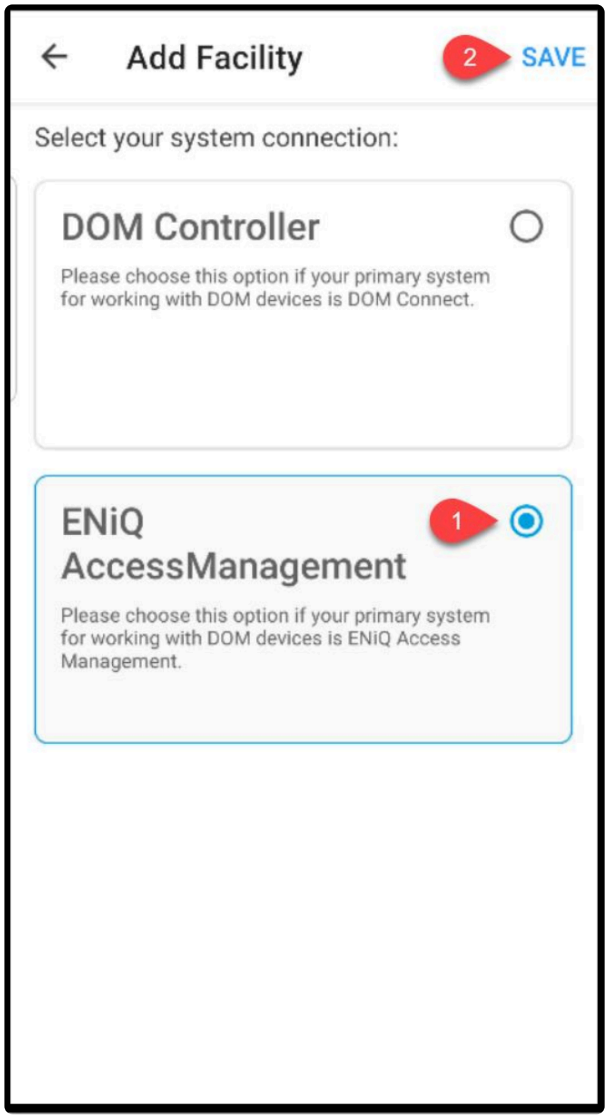


- Tap on “Add a facility”

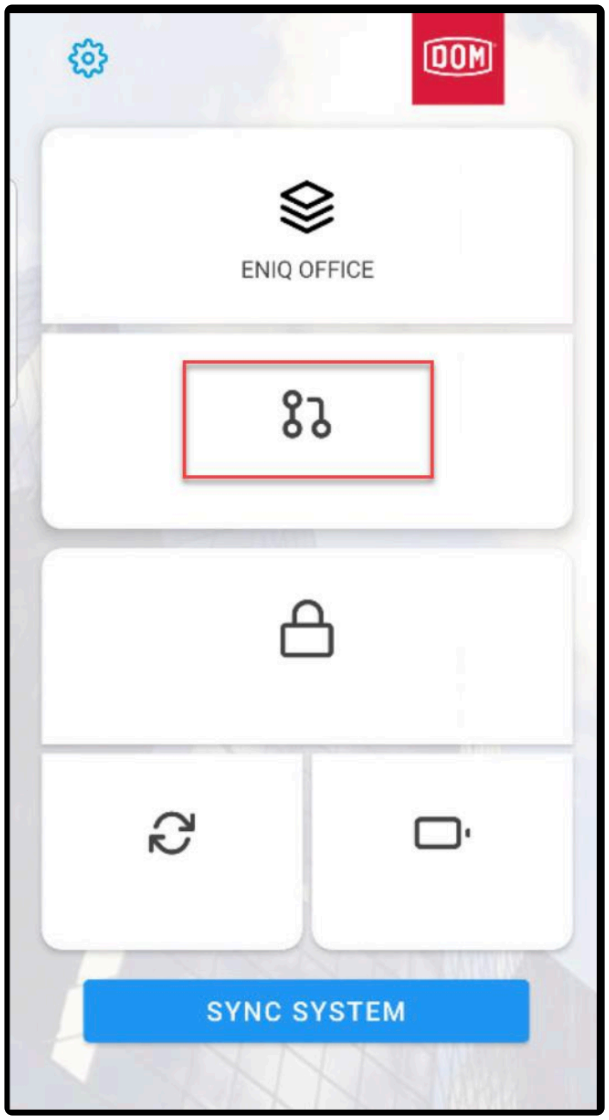


- Enter a facility name, an optional description, then tap “Save”

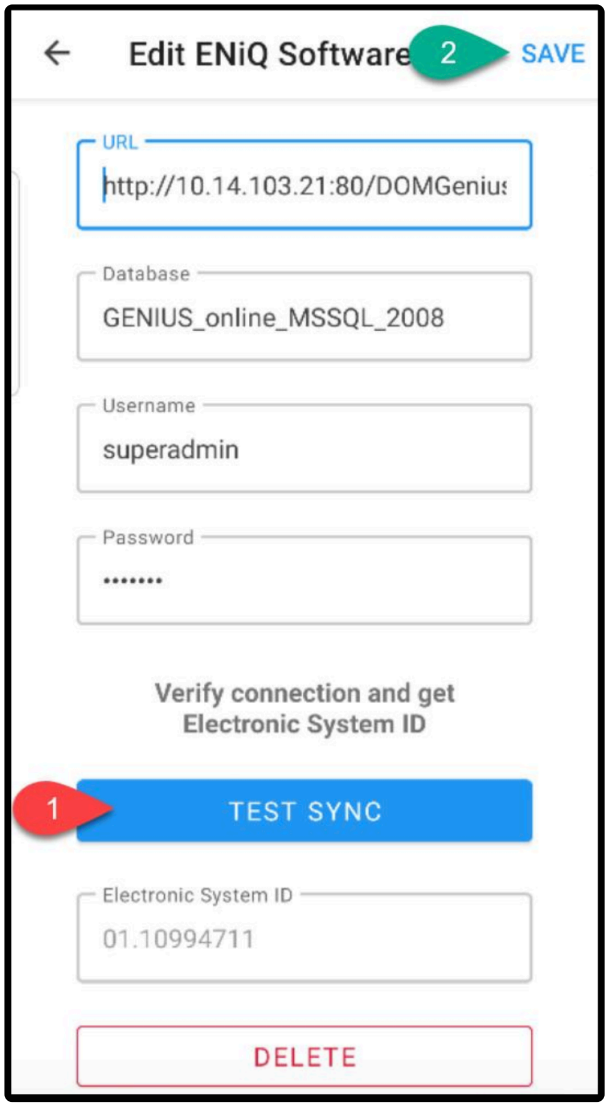
- Select the “ENiQ AccessManagement” type, then tap “Save”



- Tap on “Configuration”

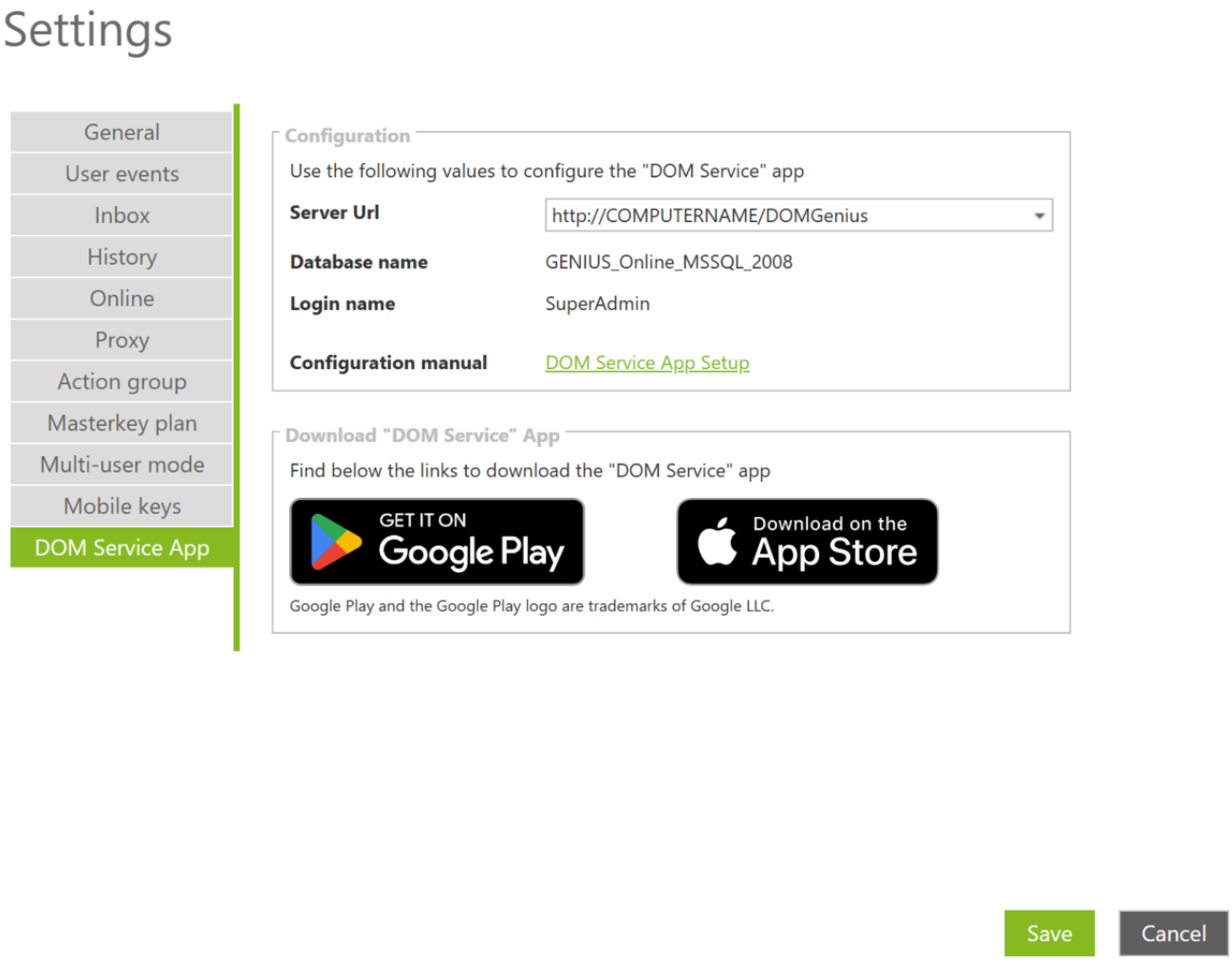


- Enter the connexion details, test the connexion (this can take a few seconds), then tap “Save”. On next section is described how to get the connexion details.



Connexion details

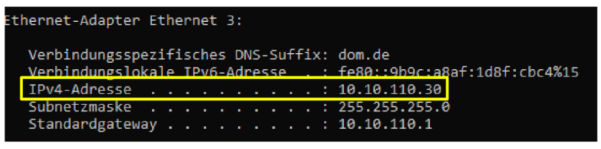
All configuration parameters can be found in ENiQ Software System / Settings / DOM Service app:



You can also find all parameters manually:

- You need the IP address of the server on which the login page of the ENiQ AccessManagement software
  is located. Type “Win” + R.

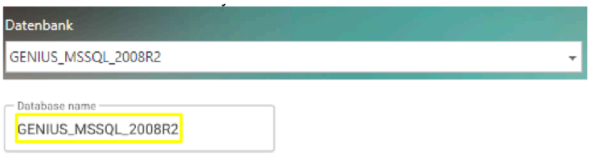
- In the column “Execute”, type “cmd”
- In the “Console window” type ipconfig
- You will now find the IP address



- Enter the IP address in the URL field. Alternatively, you can also enter the “/DOMGenius” if DNS is active in the network.

We recommend to set up the SSL. Instructions can be found on the Service Page. In this case type in the URL as follows:

- Enter the database name of your software



- Finally, enter the username and password of the user of ENiQ AccessManagement.

The user needs to be granted the permission to use the DOM Service app for offline synchronisation. To do so, go to “System” -> “User” -> “Configuration”, and make sure the option “Enable app synchronisation for users” is enabled. By default, all users with roles “Superadmin”, “User” and “Device Programmer” are allowed. Other user roles are not allowed by default.

4.5. Connect desk reader

Prerequisites:

- Desk reader is connected
- Desk reader shows red light

Assign desk reader to an operator

If this is the first time you have logged into the program, you must assign a desk reader to the operator.

To assign the desk reader to an operator, proceed as follows:

- Click on “System” in the navigation bar.
- Select the “User” menu item.

The “System / User” menu opens.

- Select the operator to whom the desk reader is to be assigned.
- Click on the “Edit” button or double click on the corresponding entry of the operator.

The “System / User” window opens.

- Select the “Configuration” tab.
- Open the “Assigned desk reader” drop-down menu.
- Select the desk reader entry to be assigned to the operator.

The serial number of the desk reader can be found on the bottom of the desk reader.

- Click on “Save”.
  The desk reader is assigned to the operator and is available for use.

4.6. Activate and deactivate transponder templates

A transponder template divides the memory available on a transponder to store area and device authorizations.

✻ Transponder templates are necessary only in an intelligent (DoC) as well as mixed system

✻ Define the transponder template for your use case at the beginning. Only one template can be assigned in a locking plan.

Authorizations for areas and for devices can be stored on a transponder (Data on Card).

Select the template to be used for the transponders according to the answers to the following questions:

- How much memory of the transponder do I want to use?
- How many area/device authorizations are needed?
- Will the facility continue to grow? Will I need more area/device authorizations in the future?
- Will other applications (time recording, canteen accounting, etc.) be managed with the transponder?

The following combinations (templates) are available for selection for a DESIFire 8K transponder:

- 160 device authorizations and 256 area authorizations (free memory 5920 bytes)
- 224 device authorizations and 2048 area authorizations (free memory 3872 bytes)
- 832 device authorizations and 256 area authorizations (free memory 3872 bytes)
- 1408 device authorizations and 2048 area authorizations (free memory 256 bytes)
- 2048 device authorizations and 256 area authorizations (free memory 416 bytes)

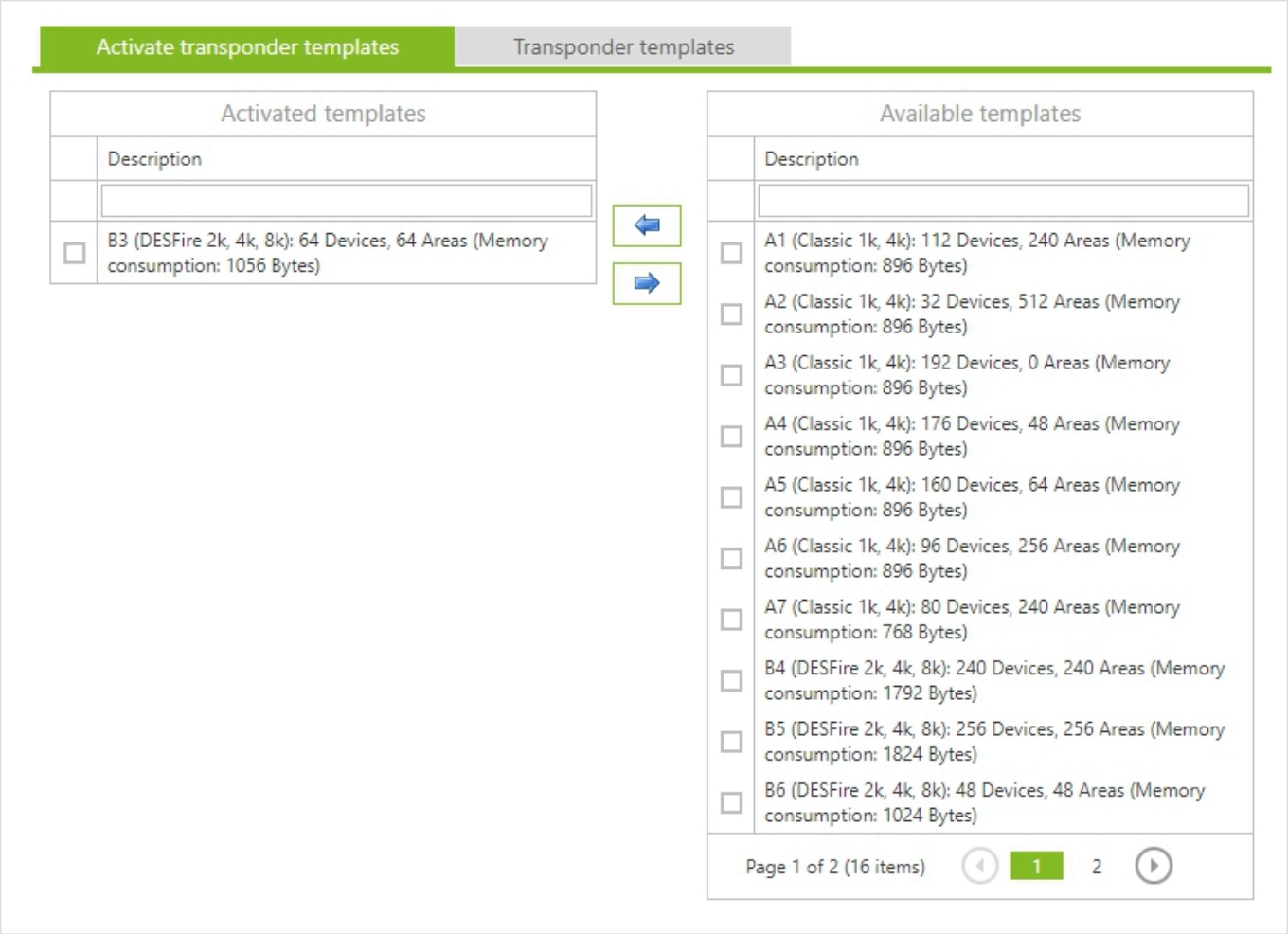
You can assign one template per locking plan. This allows you to define the allocation of memory space on the transponders.
Assigning a transponder template to a transponder activates the transponder template.

If a transponder template is already activated, you can add new templates only with the following properties:

- The new template must have the same number of areas as the existing template.
  Or:
- The new template must not be created with areas.

To activate a transponder template, do the following:

- Click on “System” in the navigation bar.
- Select the “Transponder templates” menu item.



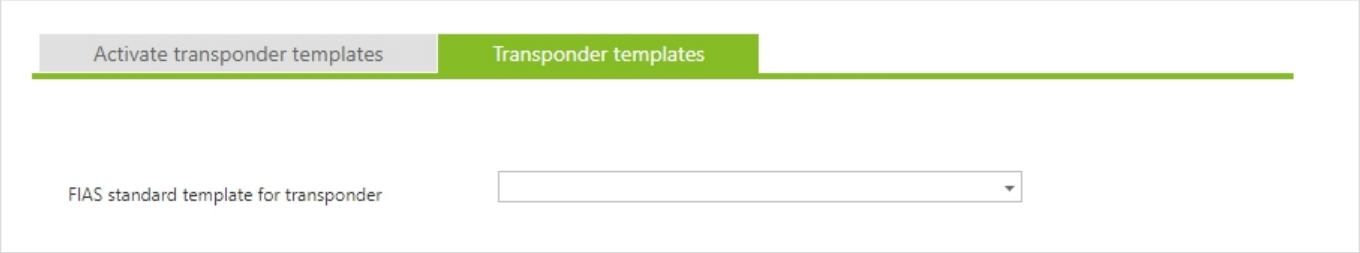
The “Activate transponder templates” tab opens.

- In the “Available templates” area, select the template to be used in the system.
- Click the “Add” button.

The selected template will be added to the “activated templates” area.

You only need the FIAS Standard template for a FIAS connection.
To check which FIAS Standard template is used for new transponders, do the following:

- Click on “System” in the navigation bar.
- Select the menu item “Transponder templates”.



The “Activate transponder templates” tab is displayed.

- Switch to the “Transponder templates” tab.
  The FIAS standard template for new transponders is displayed here.

- Select the desired type.

The selection will be applied directly.

> You can only deactivate templates that are not in use. If the template is already in use, the template cannot be deactivated.

To deactivate a transponder template, proceed as follows:

- Click on “System” in the navigation bar.
- Select the “Transponder templates” menu item.

The “Activate transponder templates” tab is displayed.

- In the “Activated templates” area, select the template that you want to deactivate.
- Click the “Remove” button.

The selected template is removed from the “activated templates” area.
A deactivated template can be reactivated at any time

5. First steps

This chapter describes the First Steps of the ENiQ software on your system.

- First login
- User interface and functions
- Setting up a person
- Create locking system

5.1. First login

Prerequisites
To use the software, the following requirements must be met:

- Complete installation of the program on the computer.
- Database available
- Desk reader connected, for information on how to integrate the desk reader into the software, see “Connect desk reader”.
- DOM-MasterService service started (the icon in the taskbar shown below is green)
- DOM-SlaveService service started (the icon in the taskbar shown below is green)

Start software

> The ENiQ software has a web interface. When you start the software, it will be displayed in the default web browser.

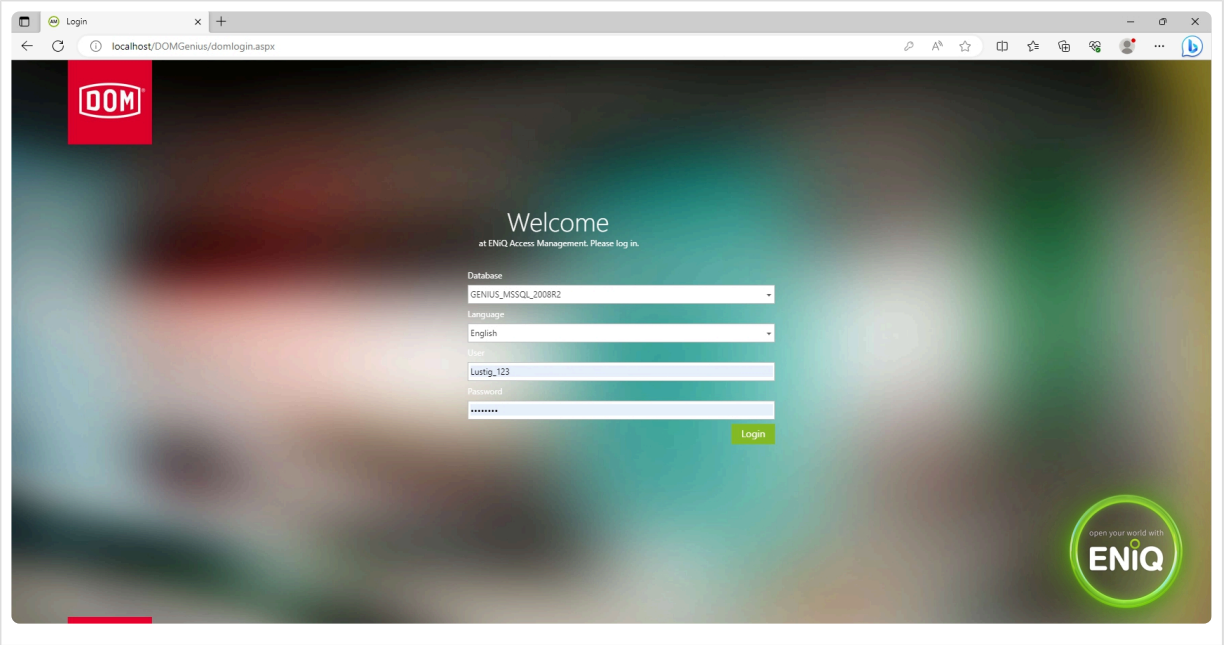
To be able to work with the software, you have to start it on your computer.

- Double click on the corresponding icon on the desktop or visit http://localhost/DOMGenius in the browser.

- The software will be launched.

> For certain operations it is necessary to switch from the ENiQ Device Management software to the ENiQ software or vice versa.
> In such cases, start the ENiQ Device Management software and the ENiQ software in parallel.

Login
After the program start you will see the displayed screen:



To log in to the program as administrator, proceed as follows:

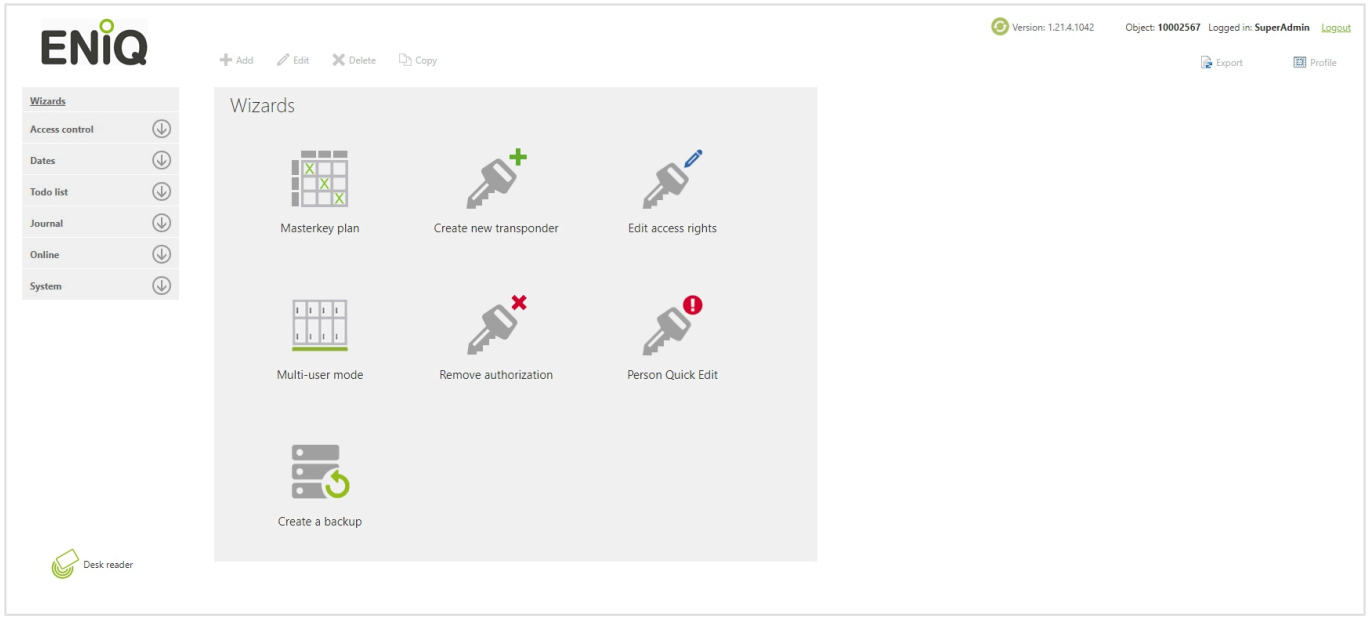
- Select the desired language in the selection window
- Click in the “Password” input field

> *The factory default password is “superadmin”.*

- Enter the password
- Click on “Login” or press the “Enter” key
- The program will open and the program interface will be displayed

To log in to the program as another operator, proceed as follows:

- Select the desired language in the selection window
- Click in the “User” input field
- Enter the desired operator name
- Click in the “Password” input field
- Enter the password
- Click on “Login” or press the “Enter” key
  The program will be opened and the program interface will be displayed


ENiQ
Version: 1.21.4.1042
Object: 10002567 Logged in: SuperAdmin Logout
Add
Edit
Delete
Copy
Export
Profile
Wizards
Access control
Dates
Todo list
Journal
Online
System
Wizards
Masterkey plan
Create new transponder
Edit access rights
Multi-user mode
Remove authorization
Person Quick Edit
Create a backup
Desk reader

5.2. Set up locking system

Procedure for implementing a locking system

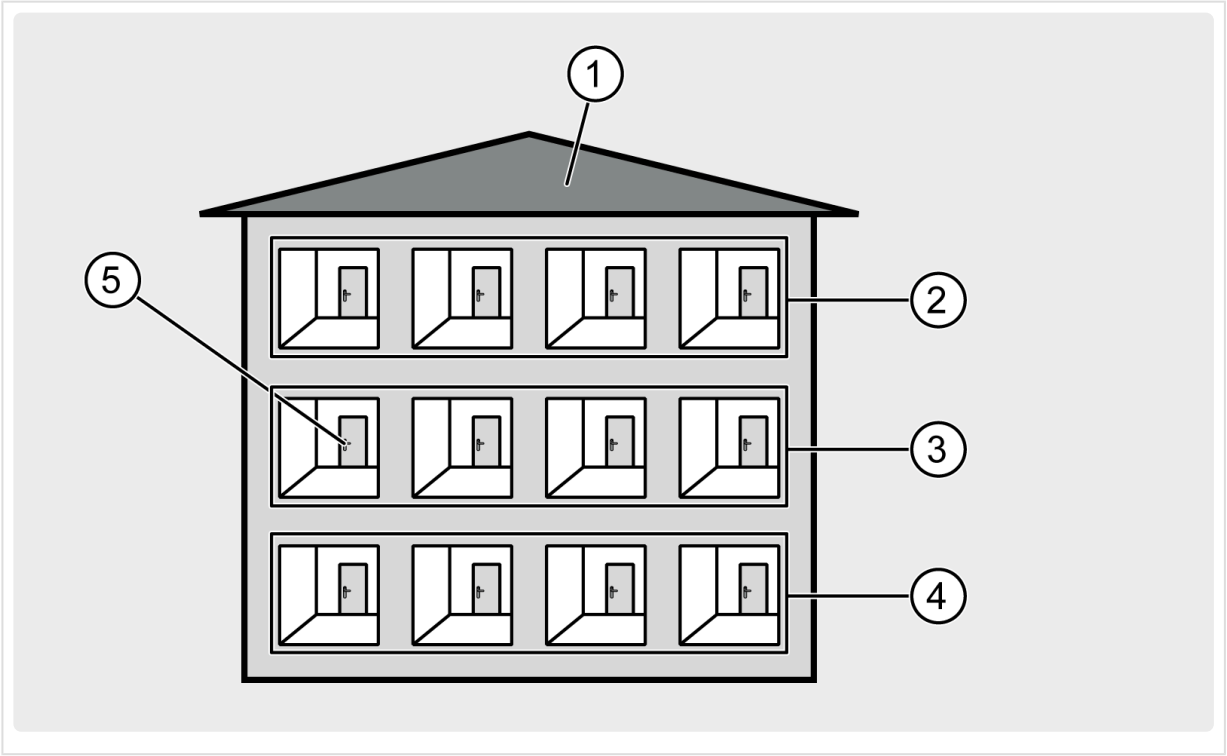
There are several ways to implement the locking system desired by the operator in the ENiQ software. If you have no or little experience with the software, use the following sequence as a guide.

- Start the ENiQ AccessManagement.
- For intelligent (DataOnCard) systems: select the transponder template corresponding to your needs.
- Read the Mastercard into the software
- Create a separate operator account for each operator in the software
- Create the desired schedules
- Create the desired area structure
- Create the desired groups of persons
- Assign authorizations to the groups of persons in the desired areas via the locking plan
- Include the transponders in the software
- Couple the devices via ENiQ Device Management

5.2.1. Create area

Create areas

Devices with the same access authorizations are assigned to an area. The areas can contain sub-areas so that the area structure can be clearly mapped. Depending on the scope of the locking system, an area (1) can represent a building, for example. In the first sub-area level (2, 3, 4) you can, for example, create the existing floors within the building. In the second sub-area layer (5) you can e.g. create the rooms on the floors.



In the case of extensive locking systems, the areas can represent federal states, for example. In the first sub-area level, e.g. locations can be created. In the second sub-area level, for example, buildings can be created, and so on. Any number of sub-areas can be added.

The properties and authorizations assigned in the areas are inherited by the sub-areas. When planning the locking system, take into account that the inheritance of authorizations can be changed in the ENiQ software. Then there is no automatic transfer of properties and authorizations from the parent area. Exceptions to this are the inheritance of state, province and whether an area is intelligent (DataOnCard).

For larger locking systems, it is advisable to create a main area for each federal state, as the assignment to a federal state also means that the public holidays and vacation dates are inherited.
This means that access authorization on public holidays and during vacations can be automatically taken into account for each location when assigning rights. This provides a geographically organized hierarchy in which the devices or sub-areas can be easily located.
To do this, one follows the hierarchy path from the state to the city to the desired building.

An area can be created either intelligently (DataOnCard) or conventionally (DataOnDevice). If a device or a sub-area is added to an area, the property “intelligent” (DataOnCard) or “conventional”

(DataOnDevice) is automatically inherited. If you set up the system “intelligently” (DataOnCard), the access rights are on the transponder. With “conventional” (DataOnDevice), the access rights are in the device.
It is not possible to mix intelligent (DataOnCard) and conventional (DataOnDevice) systems within an area. If intelligent (DataOnCard) and conventional (DataOnDevice) systems are required simultaneously in a locking plan, at least two main areas must be set up. Depending on the size of the locking system, several areas can also be created for intelligent (DataOnCard) or conventional (DataOnDevice) devices.

This section describes how to define and manage areas.
You can assign properties and authorizations in the created areas. You can assign devices to the corresponding areas.

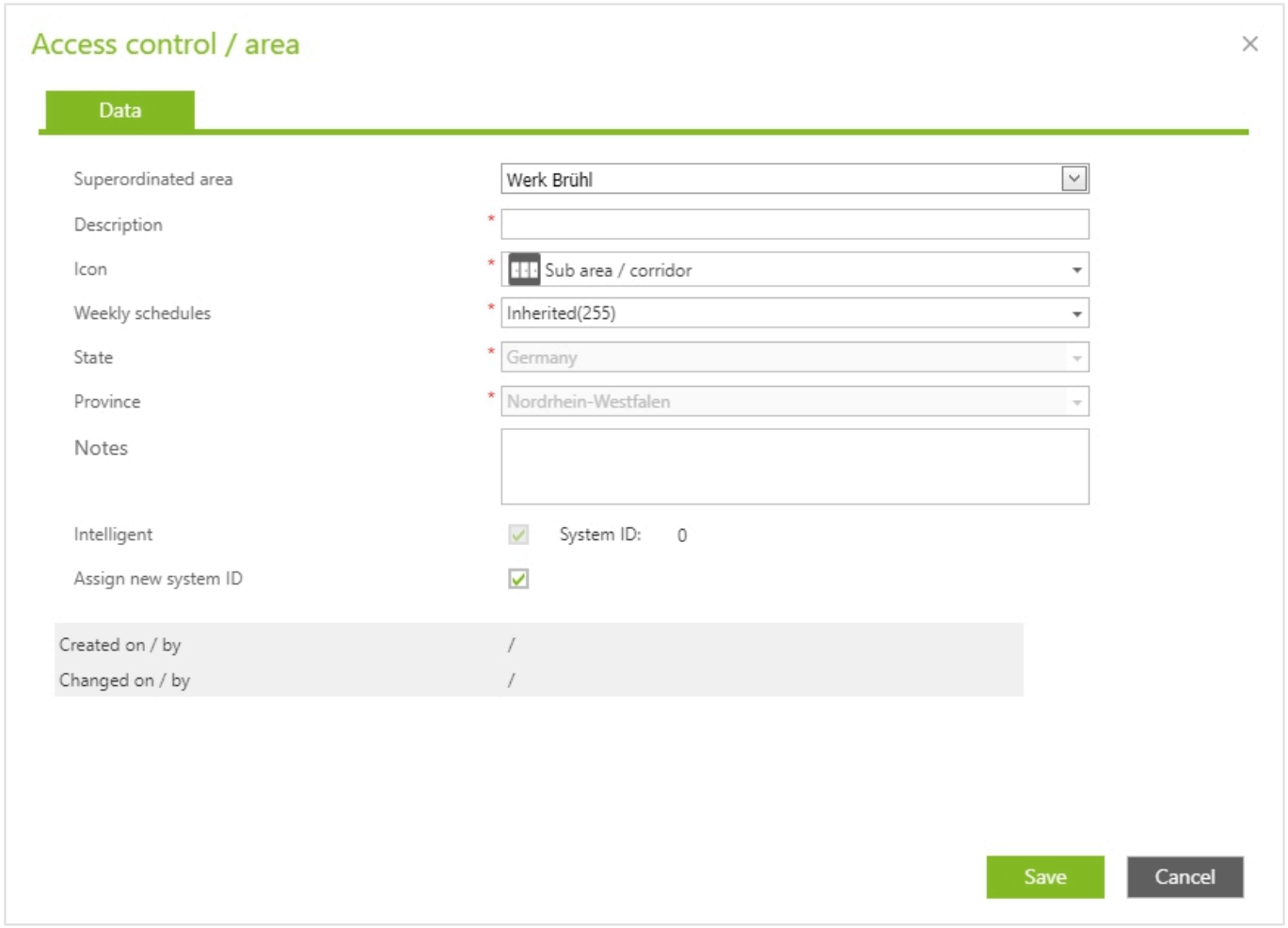
To create an area or sub-area, proceed as follows:

- Click on “Access control” in the navigation bar.
- Select the “Areas” menu item.

The “Access Control/Areas” menu opens.

- Click on the “Add” button.

The “Access Control/Area” menu, will open.



The contents of the “Data” tab will be displayed. You can now define the basic settings for the new area.

If you want to create a child area you have to select a parent area in the “parent area” field.

- Select a parent area from the drop-down menu.

The information or settings from the parent area will be inherited.
You must fill in the mandatory fields marked with an asterisk.
Fields not marked as mandatory can be left blank.

- Enter a name for the new area.
- Select a weekly schedule from the drop down menu.
- Select a state from the drop down menu.
- Select a province from the drop down menu.

You can set up the area as “intelligent” (DataOnCard) or as “conventional” (DataOnDevice). In “intelligent” (DataOnCard) areas, the access rights are on the transponder. If you want to change authorizations on devices, the transponder must be programmed. It is not necessary to make any changes on site. In “conventional” (DataOnDevice) areas, you must program the devices. If you want to change authorizations, you must do so on site.

- To set up the new area as a “Intelligent (DataOnCard)” area, check the checkbox.
- If you want to cancel the operation without saving, click “Cancel”.
- Click on “Save”

5.2.2. Create person

Persons can be created via:

- the “Create new transponder” wizard, by reading in a transponder via the desk reader button
- the menu item Access control/ Person

> If you want to create a person directly with transponder, use the “Create new transponder” wizard

To create a person via the “Create new transponder” wizard, proceed as follows:

- Click on “Wizards” in the navigation bar.

Overview of the wizards opens.

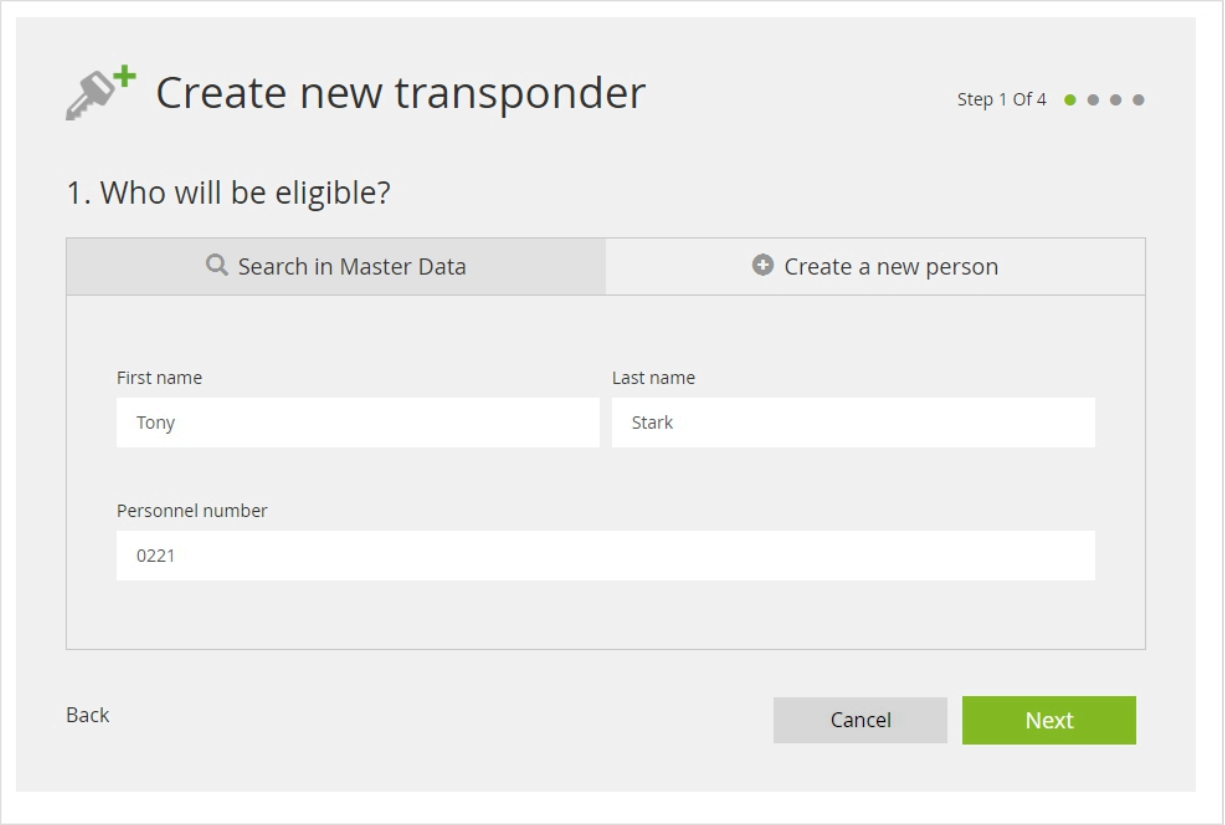
- Select the “Create new transponder” button

The wizard menu “How would you like to define the access rights?” opens.

- Select one of the three possible authorization types

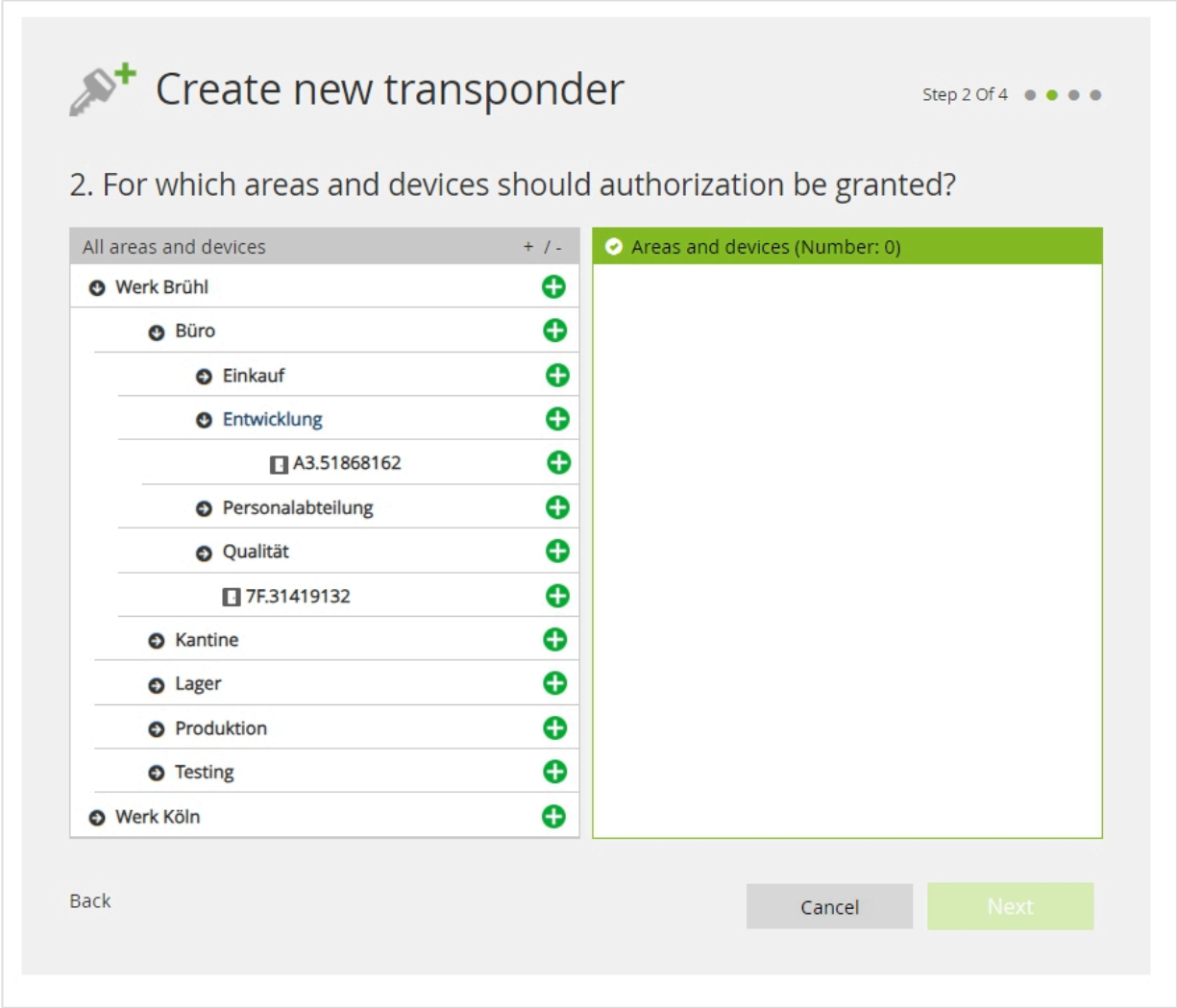
“Assign authorization” assigns rights to the person which can be single and individual
“Copy access rights of another person” copies the access rights of another person and takes them over
“Add person to a group” assigns the person to a person group who already have access rights.

- The selection opens the first window



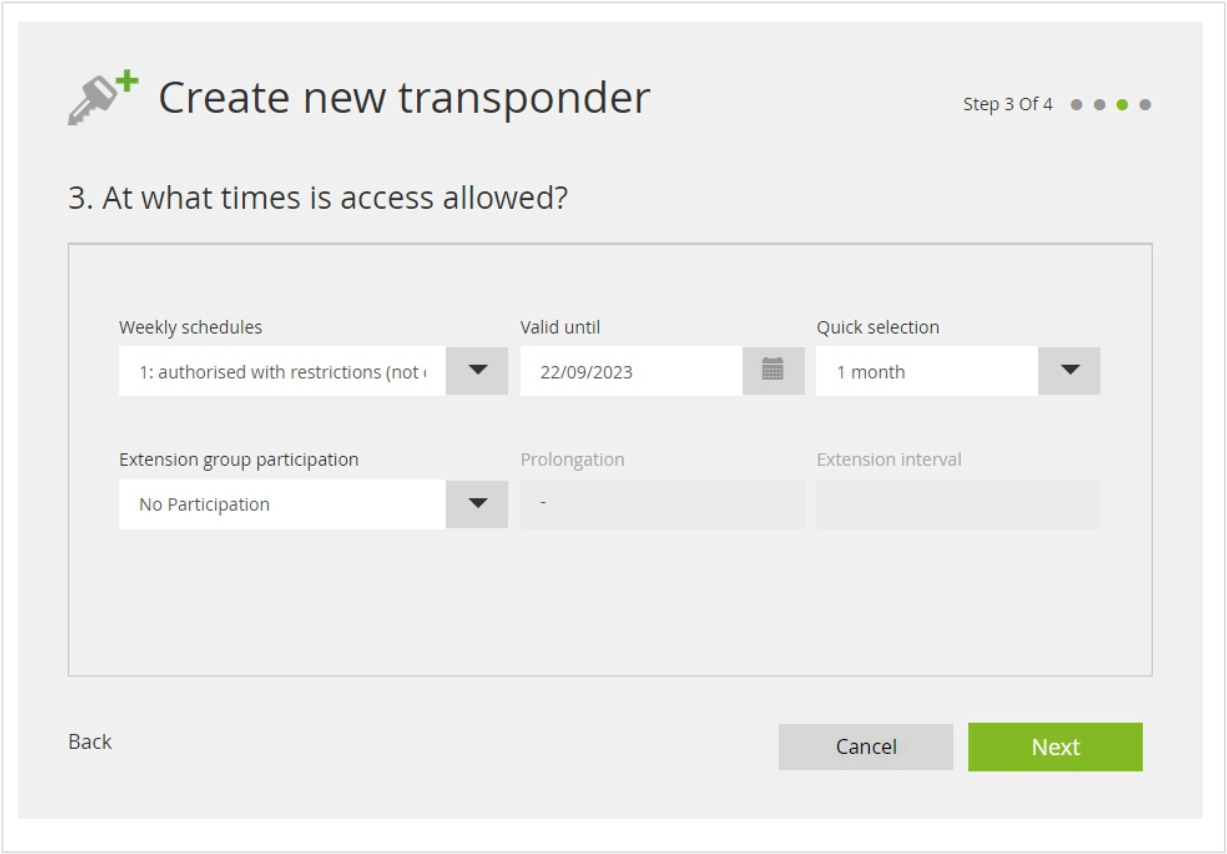
The menu of the "Who should be authorized?" wizard opens.

- Here click on the button "Create new person".
- Now enter the first name, last name and, if you wish, the personnel number
- Confirm your input by clicking on "Next



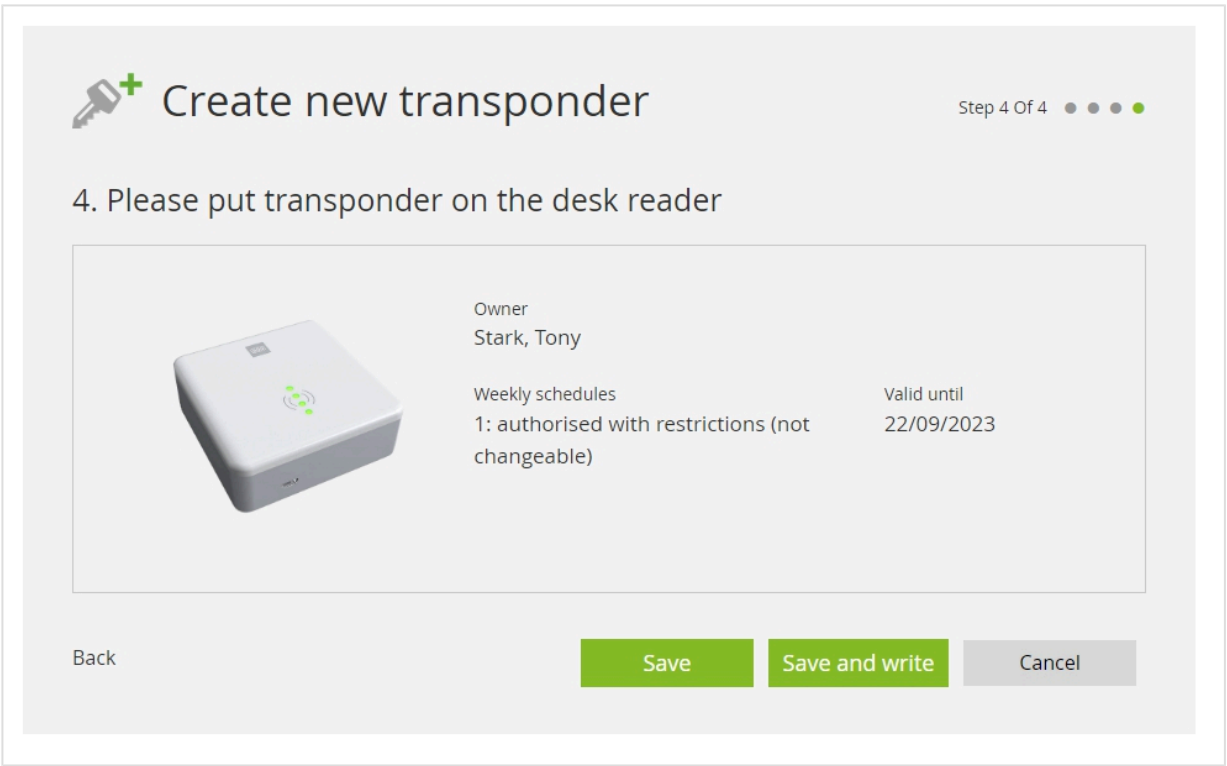
The second page “For which areas and devices should be the authorization be granted?” opens.

- Authorize the person by adding the devices/areas.
- Confirm your entry by clicking on “Next”.



The third page "At what times is access allowed?" opens.

- If already available select the desired weekly schedule
- Assign the validity of the person either over the "Quick selection" or to an exact date with "Valid to".
- Confirm your input by clicking on "Next".



The fourth page “Please put transponder on the desk reader” opens.

- Now select how you want to authorize the person:

1. Conventional (DataOnDevice) “Save” (data will be stored in the database).
2. Intelligent (DataOnCard) “Save and write” (data is written directly to transponder)

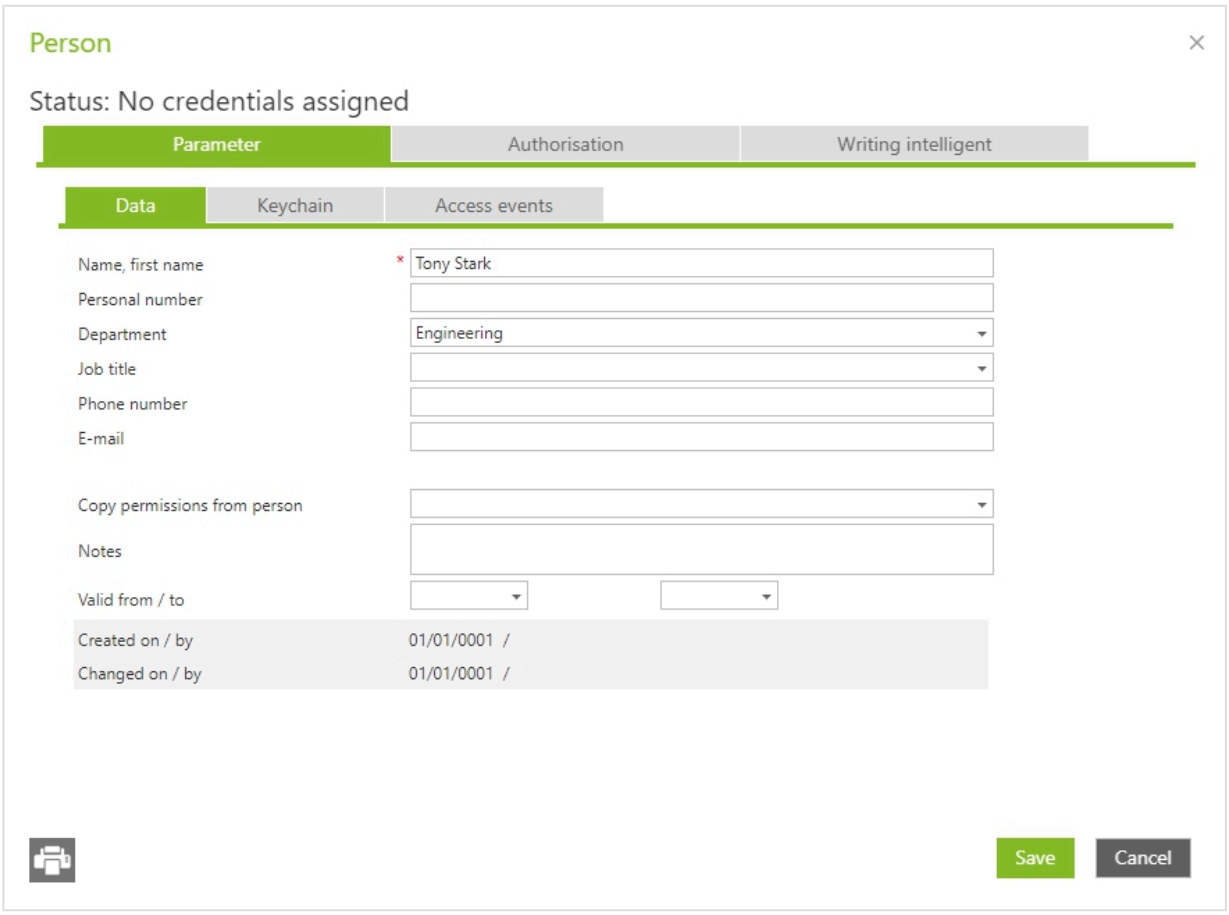
- Place the transponder on the desk reader
- Click on “Save” or “Save and Write” to add the New Person

To create a person via the “Access control”, proceed as follows:

- Click on “Access Control” in the navigation bar.
- Select the “Person” menu item

The “Access Control/Person” menu opens.

- Click on the “Add” button



The “Data” tab is displayed.

- Enter a unique designation for the person.
- If desired, enter a comment text.
- If desired, set the validity period for the person’s authorization.

After the validity period has expired, the person’s rights are automatically revoked.

This person can now either be assigned an existing transponder, or a new one can be read in and assigned via the “Keychain” tab.

- If you want to cancel the process without saving, click on “Cancel”.
- To accept the entries, click on “Save”

5.2.3. Assign authorizations

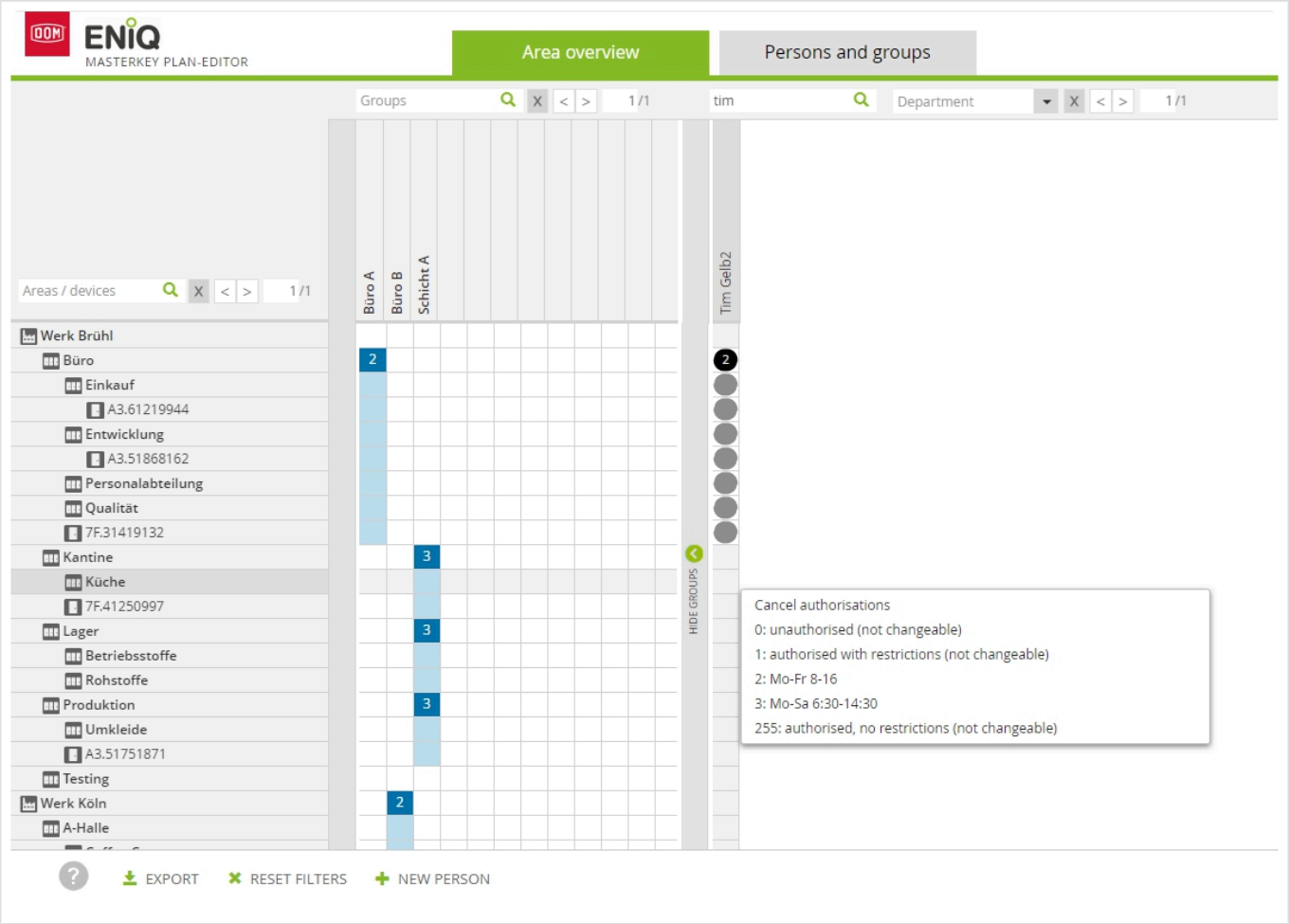
Give authorizations

In order for persons to gain access to devices, they must first be authorized.
You can do this using the “Masterkey plan”, “Persons Quick Edit” and “Edit access rights” wizards and the Access control menu item.

Masterkey plan

To authorize a person, proceed as follows:

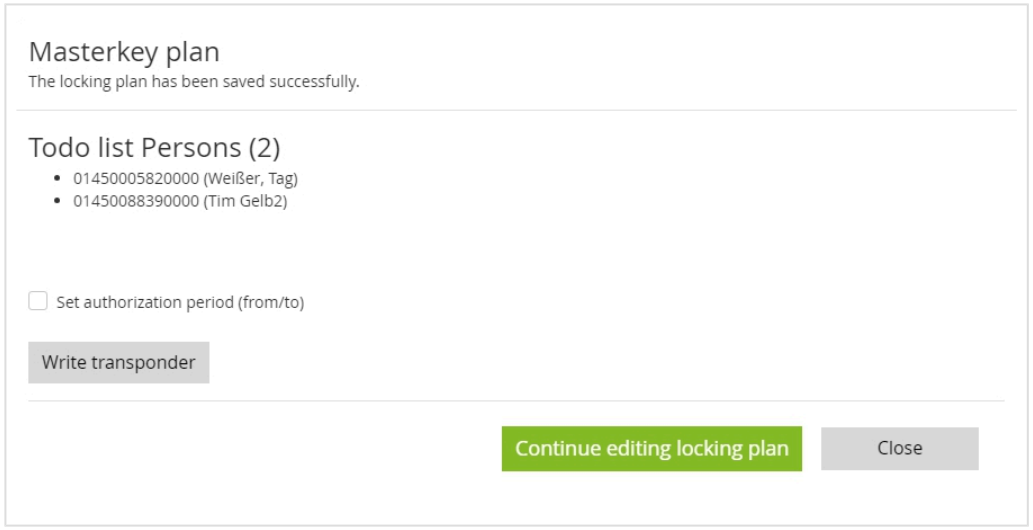
- Click on “Wizards” in the navigation bar.
- Select the “Masterkey plan” button



Masterkey plan is displayed

> Pay attention to the highlighting of the boxes to select the correct area.

- Move the cursor to the appropriate box and right-click to select the weekly schedule
- Click Save

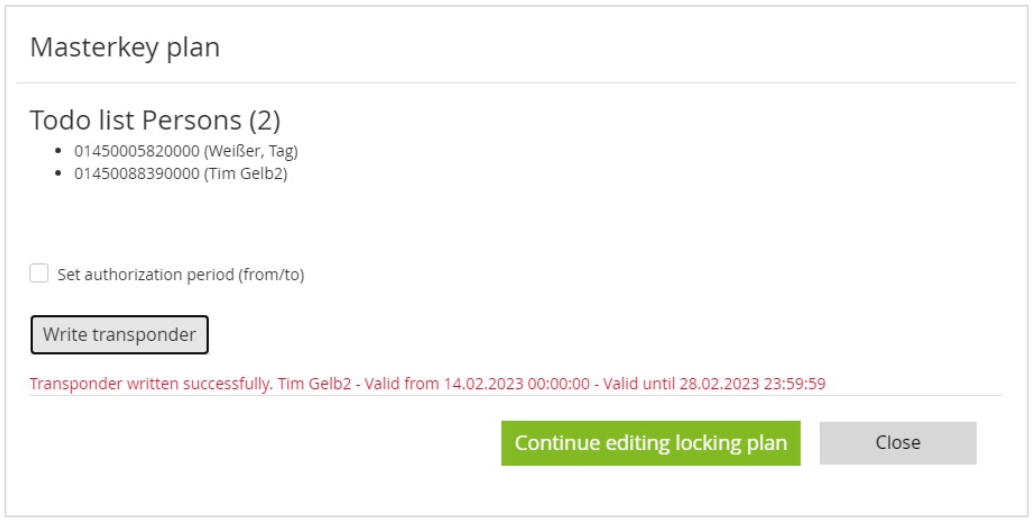


Pop-Up Masterkey plan

If the person has an Intelligent (DataOnCard) Transponder a ToDo is created

You can program intelligent (DataOnCard) transponders directly via “Write transponder”.

- To do this, place the transponder on the desk reader and select “Describe transponder



Success message “Write transponder”

After successful describing you receive the completion message

Edit access rights wizard

To change a person’s authorization, proceed as follows:

- Click on “Wizards” in the navigation bar.
- Select the “Edit access rights” button

Edit access rights step 1 of 4 opens

- Select the person manually or
- Read the transponder
- Confirm by clicking “Next”

Edit access rights step 2 of 4 opens

- Select the areas that should be assigned
- Confirm your selection by clicking on “Next”

Edit access rights step 3 of 4 opens

- Select the corresponding weekly schedule
- Set the validity of the person
- Confirm by clicking “Next”.

Edit access rights step 4 of 4 opens

- Now select how you want to authorize the person:

1. Conventional (DataOnDevice) “Save” (data will be stored in the database).
2. Intelligent (DataOnCard) “Save and write” (data will be written directly to transponder)

- Place the transponder on the desk reader
- Click on “Save” or “Save and Write” to save or program the authorizations to the transponder.

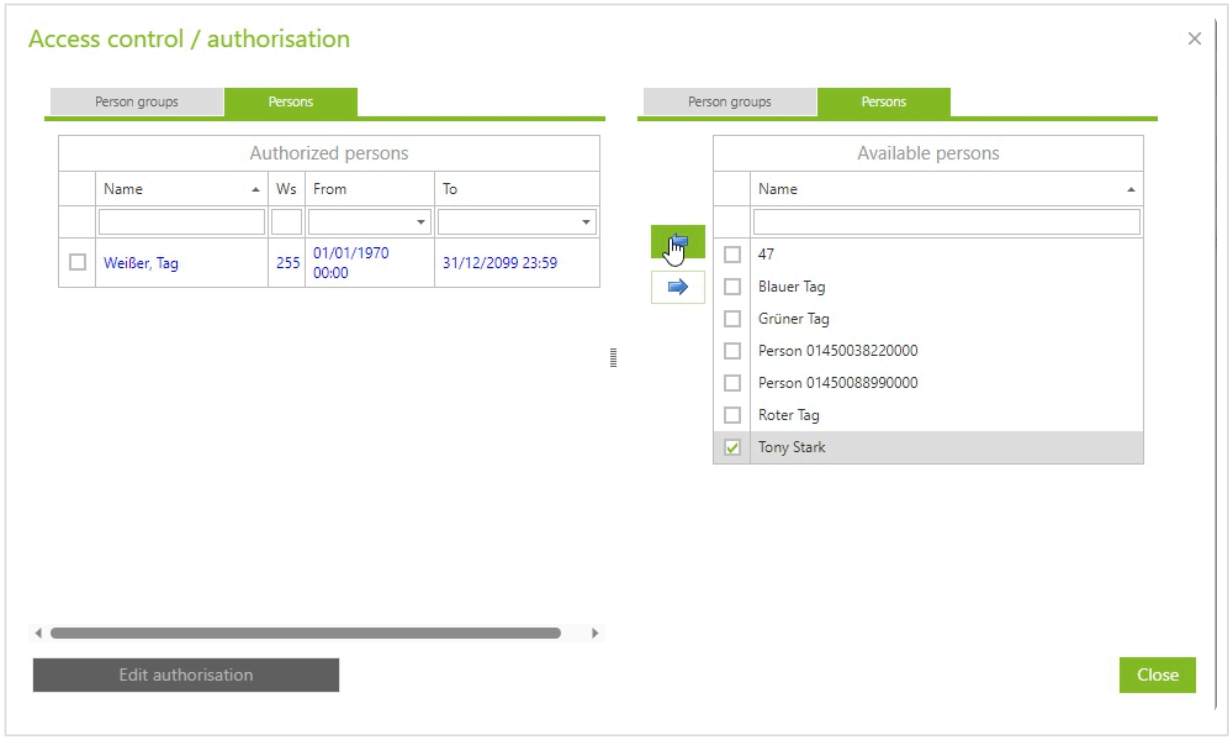
Access control

To authorize a person, proceed as follows:

- Click on “Access control” in the navigation bar.
- Select the “Area” menu item

The “Access Control / Area” menu opens

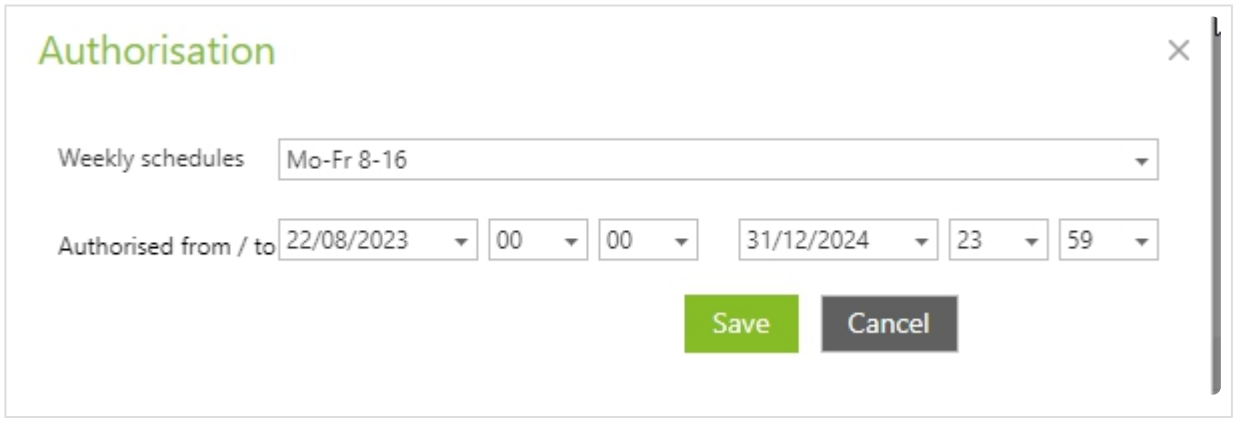
- In the area tree, select the area for which you want to assign authorizations.
- Click on “Assign authorization



The “Access Control Authorization” tab will be displayed

To assign a person to an area, proceed as follows:

- On the “Person” tab, in the “Available persons” area, select the person you want to assign to the area.
- Click on the left arrow to authorize the person(s)



The weekly schedule menu will be displayed

Select a weekly schedule for the person from the drop down menu in the Authorizations window.

- If you want to cancel the process without saving, click “Cancel”.
- To accept, click on “Save”.

To unassign a person, do the following:

- On the “Person” tab, in the “Authorized persons” area, select the desired person to be removed from the area.

- Click the “Remove” button

The assignment of the person is cancelled

- To accept the entries, click on “OK”.

To assign a person group to an area, proceed as follows:

- Switch to the “Person group” tab.
- On the “Person group” tab, in the “Available person groups” area, select the desired person group to be assigned to the area.
- Click on the “Add” button

- Select a weekly schedule for the person group from the drop down menu in the Permissions window.
- If you want to cancel the operation without saving, click on the “Cancel” button.
- To accept the entries, click on “Save”.

To cancel the assignment of a person group, proceed as follows:

- On the “Person Group” tab, in the “Authorized Person Group” area, select the desired person group to be removed from the area.
- Click the “Remove” button.

The assignment of the person group is removed

- To accept the entries, click on “OK”

5.2.4. Couple and program devices

Start ENiQ Device Management Software
In order to work with the software, you need to start it on your computer.

- Double click on the corresponding icon on the desktop.

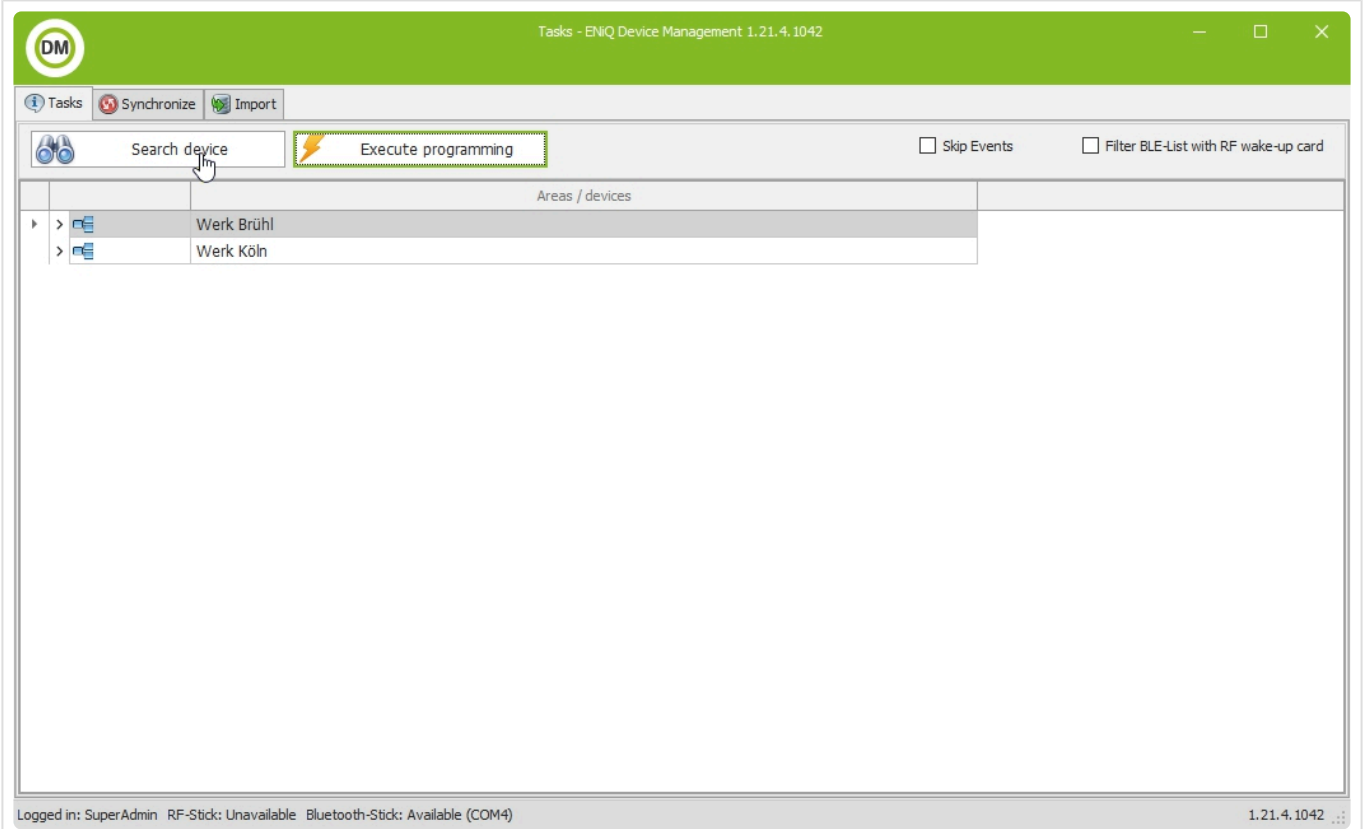
The software will be started

For certain operations it is necessary to switch from the ENiQ Device Management software to the ENiQ software or vice versa.
In such cases, start the ENiQ Device Management software and the ENiQ software in parallel.

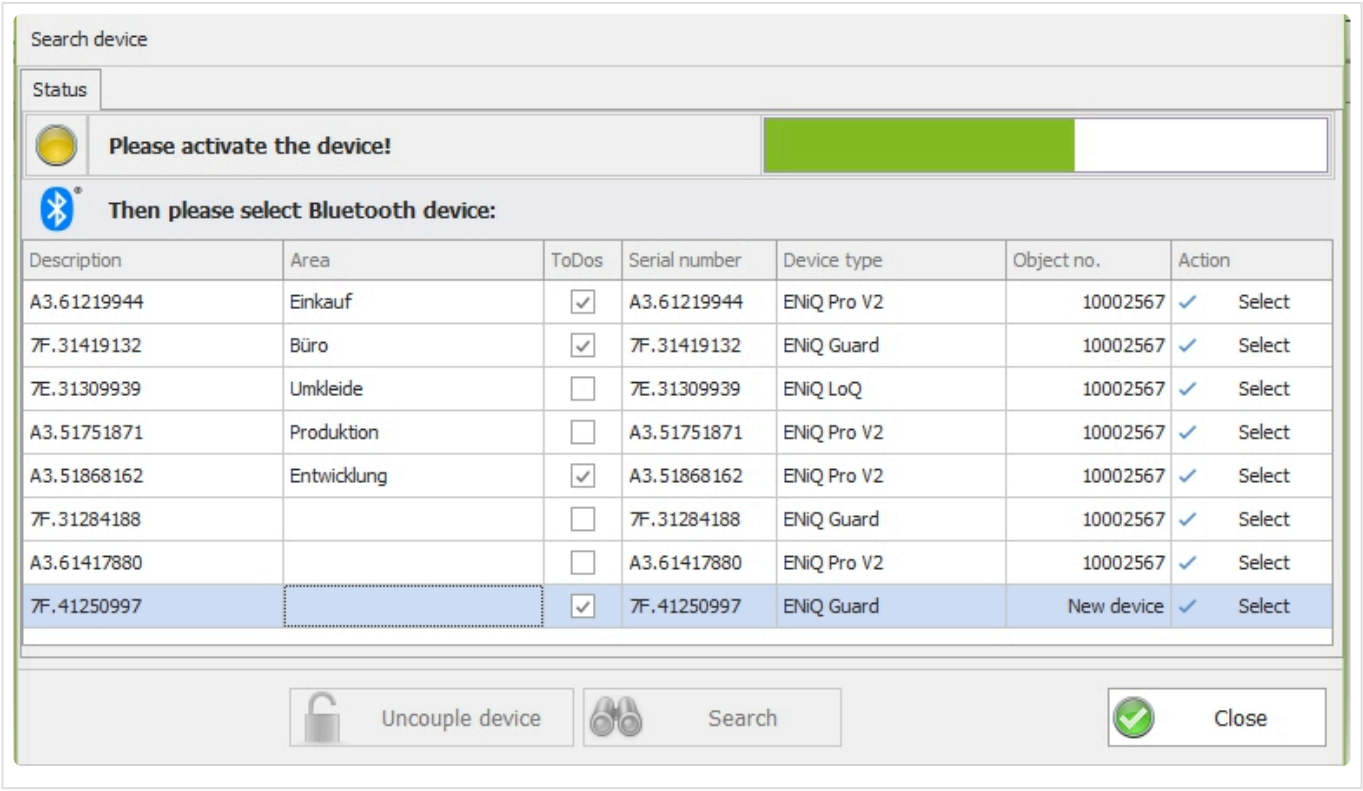
Couple device

To couple a device, proceed as follows:

- Click on the “Search device” button.

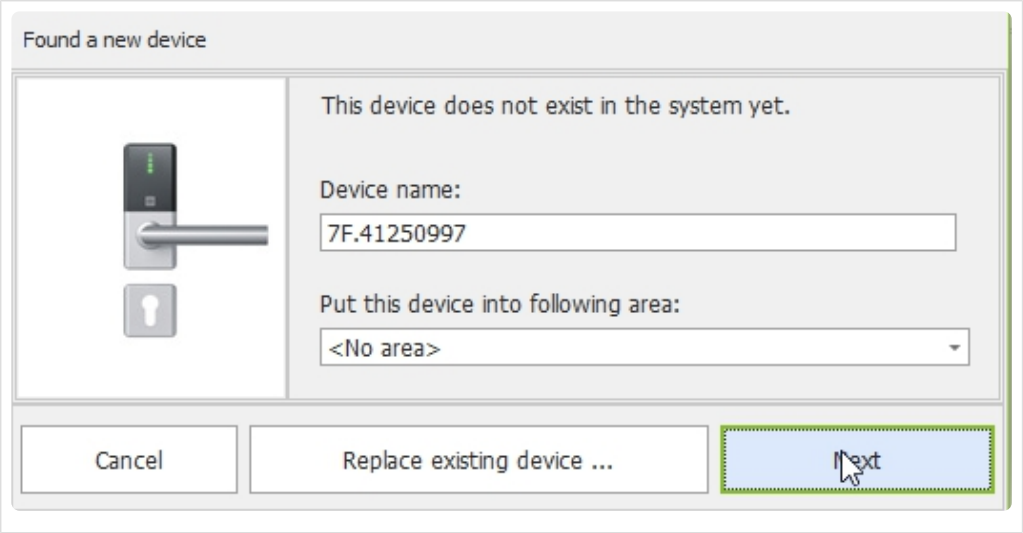


The “Search device” window opens.



You will be prompted to hold the RF wake-up card in front of the device to be coupled.

- Hold the RF wake-up card in front of the device to be coupled
- Select the device you want to couple and confirm with a double click



In this window you can assign an individual name and directly an area to the device.

- Enter a designation for the device.

This can be, for example, the description of the associated door.

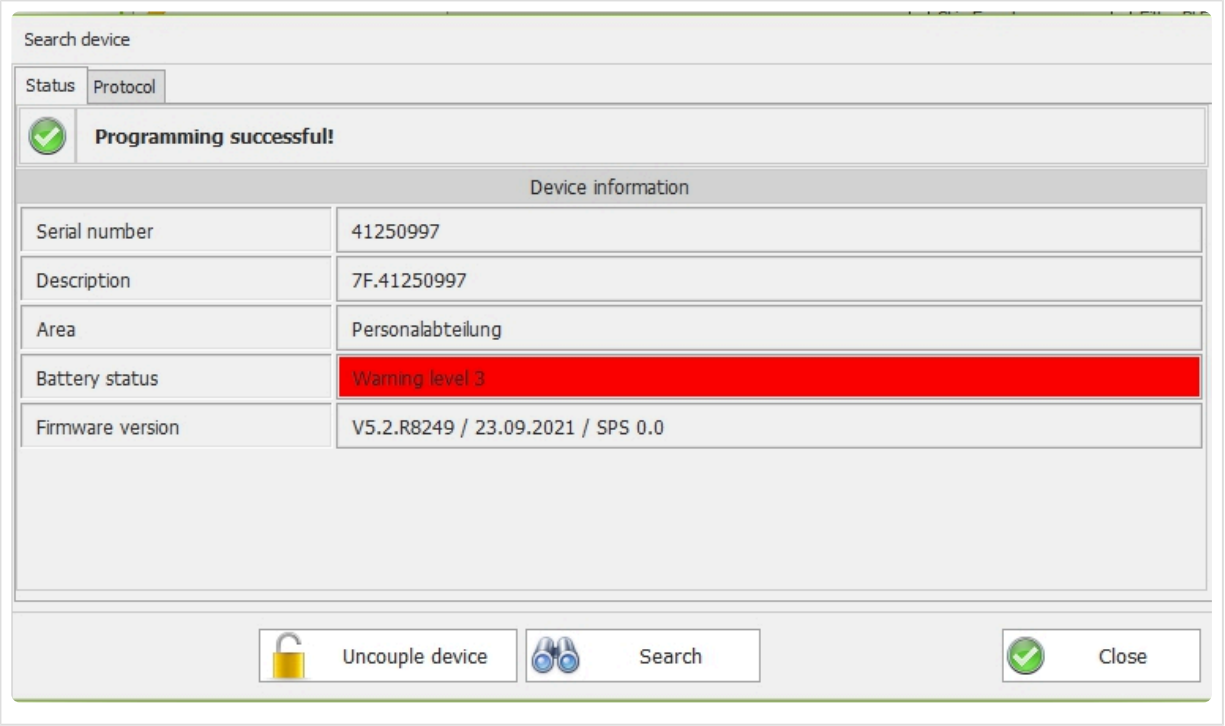
- Click Next if you want to create the device as New

> ! If the device is to replace an existing one, select “Replace existing device”.

- Select the device to be replaced from the list (double-click to confirm).
- Click the “Create device” button

Now a query window will open asking you to couple and program the device

The coupling of the device is executed.



You will see a closed padlock in the window at the bottom center-left.
The device information is displayed. The device is coupled.

- Click on the “Close” button

If the closed padlock is not displayed, you will need to repeat the coupling process.

Decouple device

To decouple a device, proceed as follows:

- Click the “Search Device” button.

You will be prompted to hold the RF wake-up card in front of the device you want to decouple.

- Hold the RF wake-up card in front of the device to be read in.
- If the device is displayed in the list, select it by double-clicking on it.

The window “A device has been found” is displayed

- Click on Next
- Confirm the query with “No”
- Click on the “Decouple device” button or use F8

Decoupling of the device is executed

The device is decoupled. The “Decouple device” button is grayed out.

Program device

If the device is coupled and you have defined the device and area authorizations in the ENiQ software, you can program the device. Here, the defined authorizations are made available to the device via the USB radio stick. You can only program one device at a time.

To program a device, proceed as follows:

- In the “Tasks” tab, click the “Execute Programming” button.

You will be prompted to hold the RF wake-up card in front of the device to be programmed.

- Hold the RF wake-up card in front of the device.

The programming is executed

The device is programmed

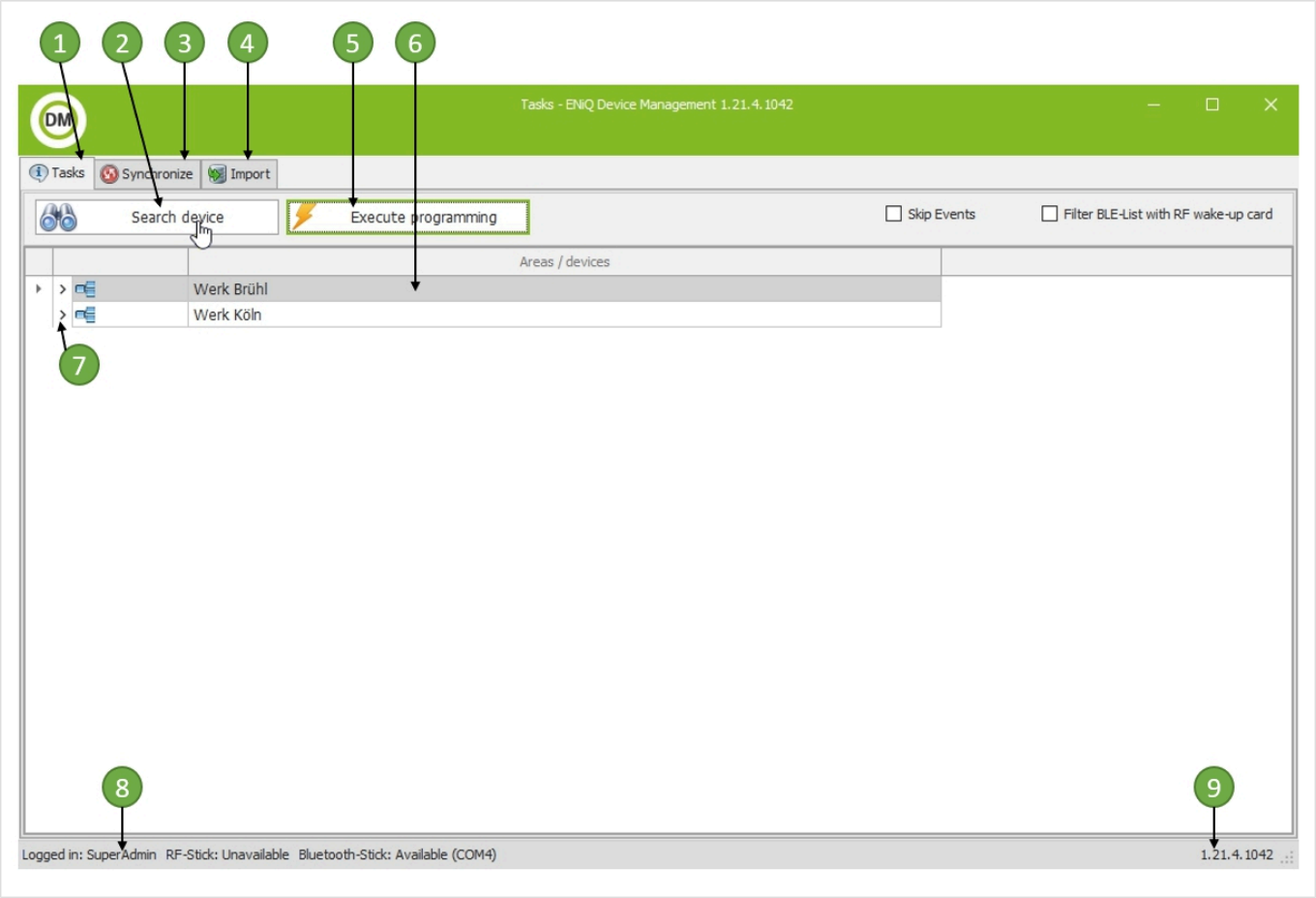
6. Basic functions

6.1. Use Device Management

Description of the ENiQ Device Management Software

Here you get an overview of the program interface and the functions of the program.

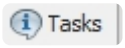
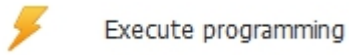
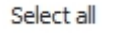
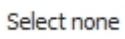
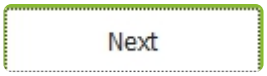
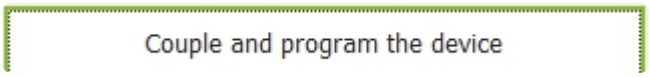
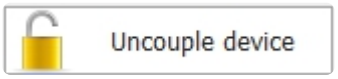
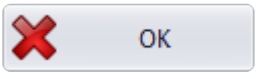
Elements of the program interface



No.	Explanation
1	Tasks tab Here you can search devices and program devices.
2	“Search devices” button The “Search Devices” window opens.
3	“Synchronize” tab Here you can synchronize the database.
4	“Import” tab Here you can import files.
5	“Execute programming” button A device is programmed.
6	Display of existing areas and devices

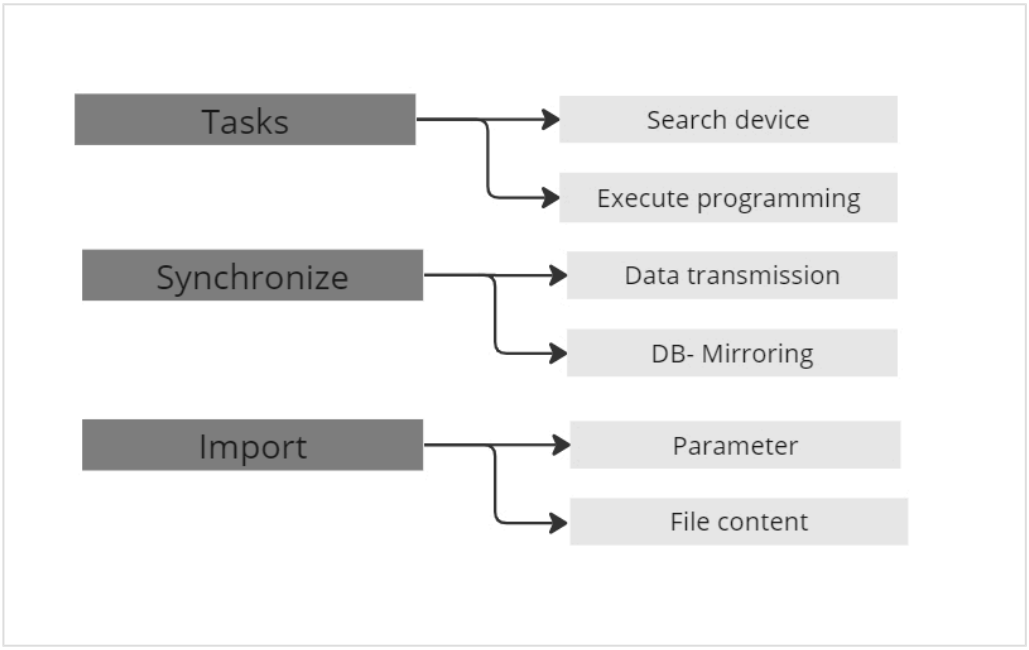
7	Software version
8	Logged in operator
9	Expand display

The following elements are available on the program interface. They are displayed case by case.

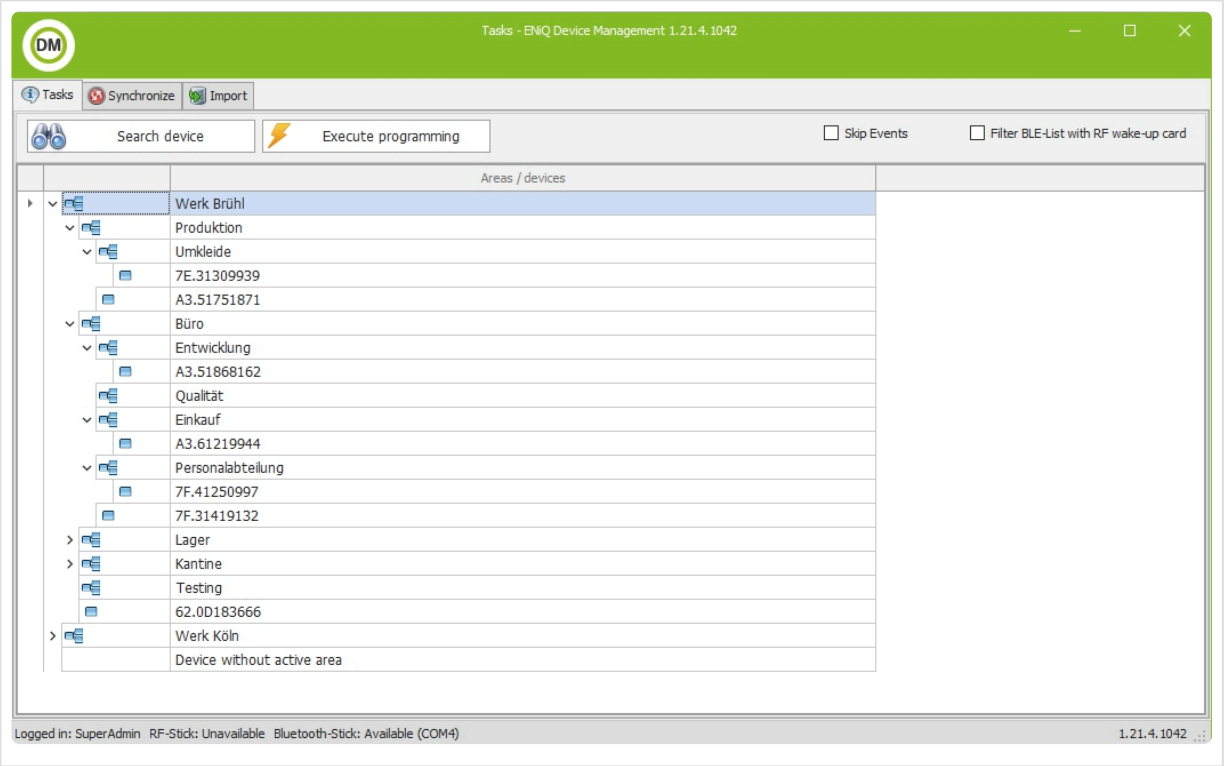
Icon	Explanation
	Open a menu that allows you to access the “Login” and “Exit” items.
	Show tabs “Search devices” and “Execute programming”.
	Start a search process for devices, e.g. ENiQ PRO or ENiQ Guard®.
	Program devices
	Synchronize database entries.
	Start synchronization.
	Read CSV file.
	Select all lines of the CSV file.
	Deselect all contents of the CSV file.
	Go to the next window.
	Couple devices. The device is coupled when the button is grayed out.
	Decouple devices. The device is not coupled if the button is grayed out.
	Search for a device.
	Confirm input.
	Expand table entries.
	Collapse table entries.
	Select CSV file.

	Select one of several options.
	Here you can switch options on or off.
	Adjust the size of the window areas.
	Import selected file contents into the database.
	On some screen pages you have to select drop-down menus. You can recognize a drop-down menu by a small arrow on the right side. You can select an entry from a list or enter a search term in the input field.

Menu structure

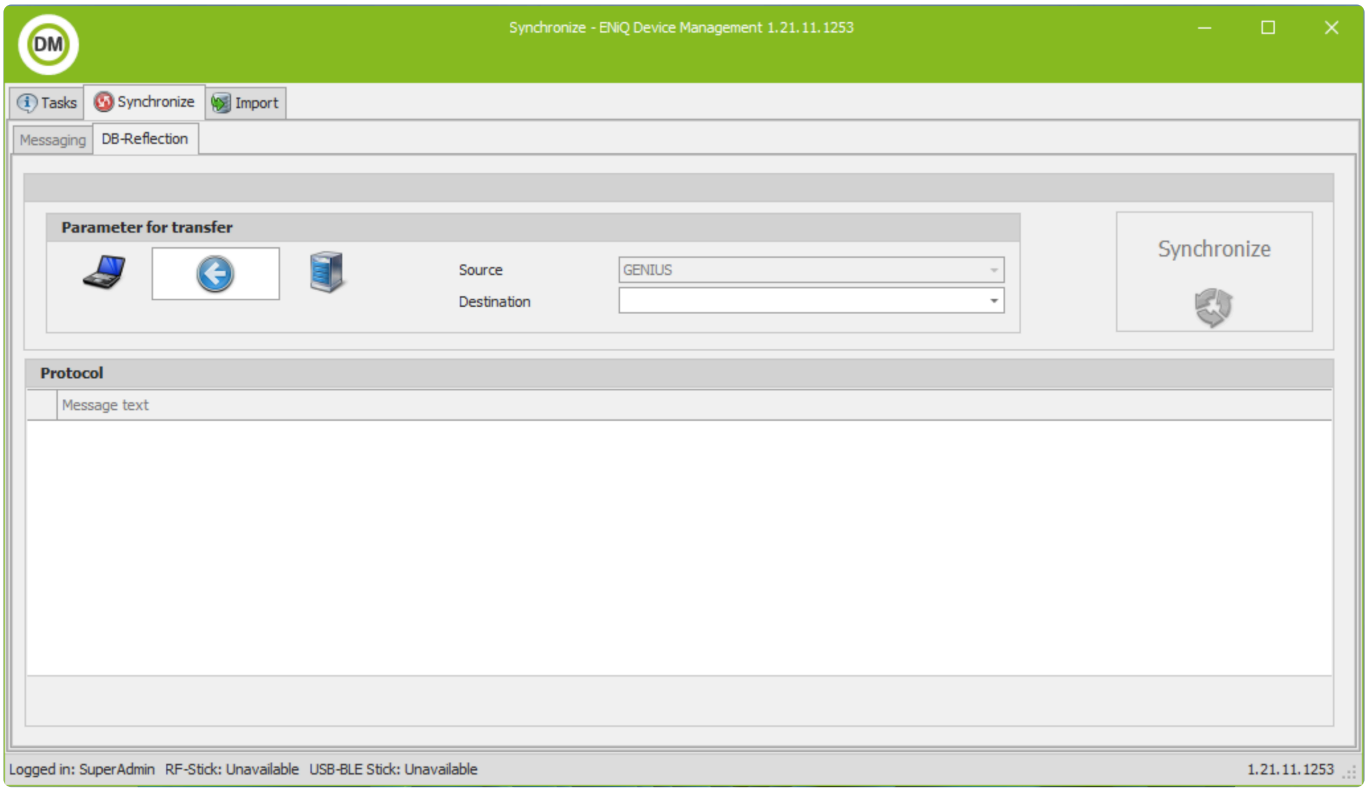


Tasks tab



Here you can search for existing devices (e.g. ENiQ Pro) and add them to the database. You can replace existing devices with new ones. You can program devices with settings e.g. permissions that you have previously made in the ENiQ software.

Synchronize tab



Here you can transfer the current authorization data from the server to a mobile computer. With the mobile computer you can program the devices e.g. ENiQ Pro offline on site. A connection to the main database is not required.

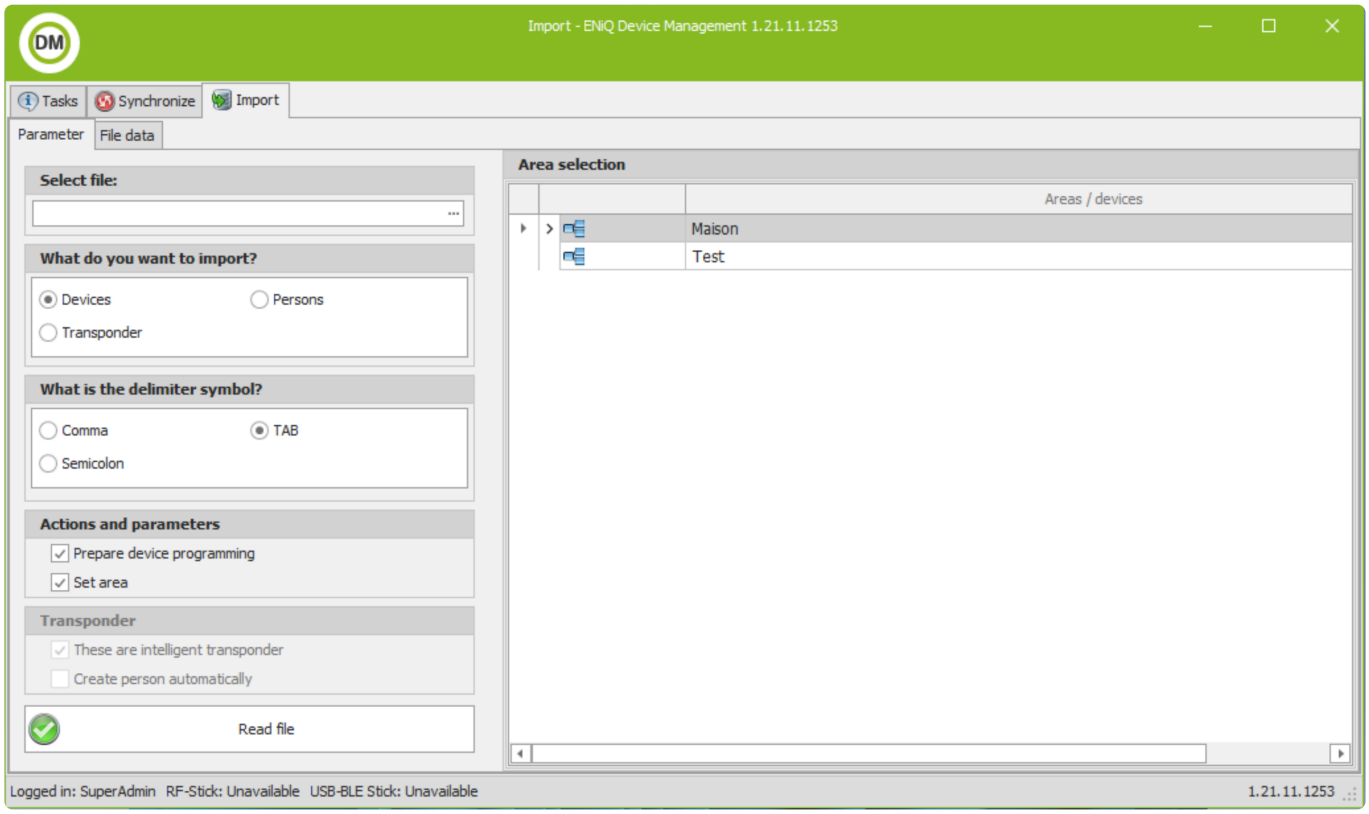
After programming, access events are automatically read from the devices and stored on the mobile computer. When the mobile computer is subsequently “synchronized” with the server (via LAN/WLAN), this data is transferred to the main database.

“Import” tab

You can store information on devices, transponders or persons in a CSV file. The Import tab allows you to import content from a CSV file into the database. The data in the CSV file must be in a certain format to allow importing.

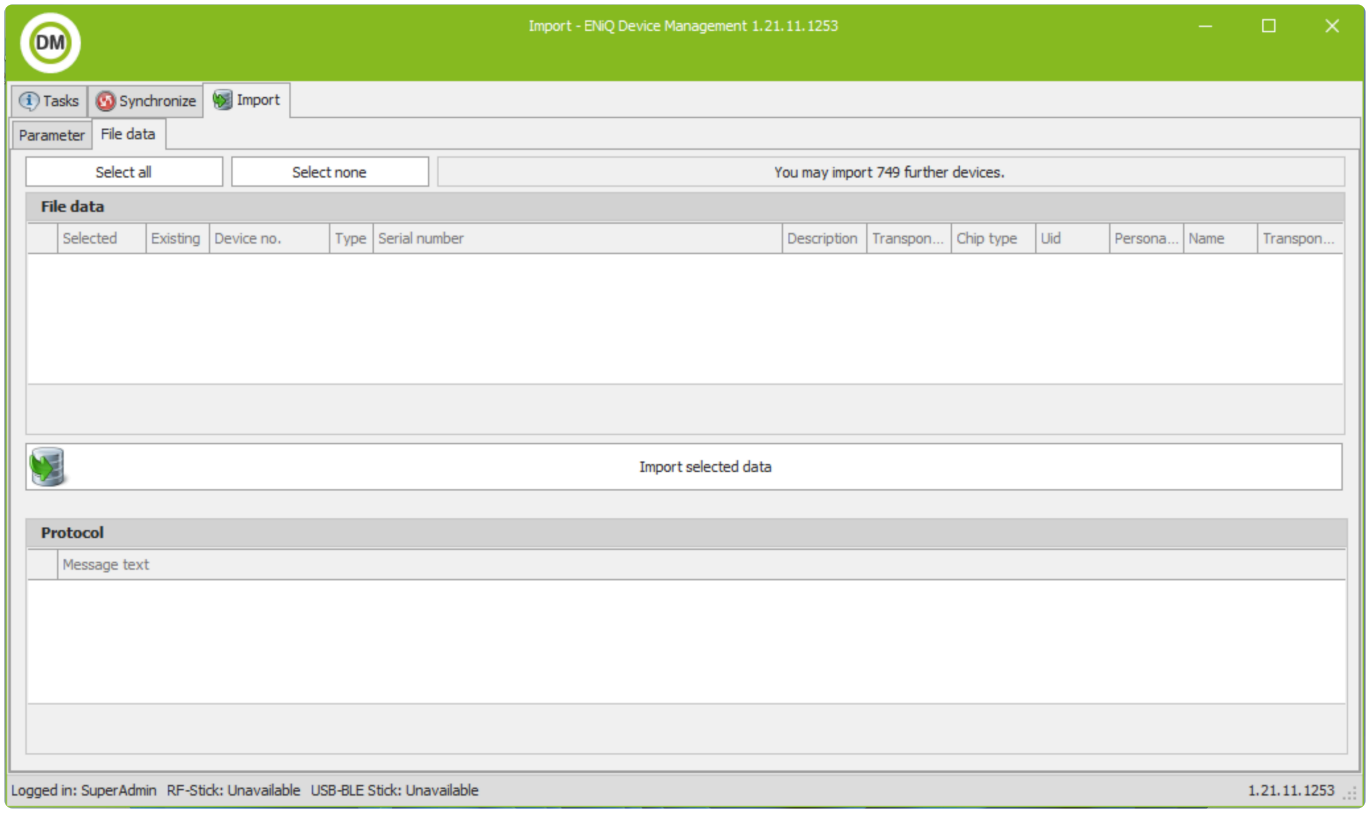
The CSV file for devices and transponders must be ordered with the order. The CSV file for persons is stored here: C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop\Templates (if the standard installation path has been selected).

Parameter



Here you can select parameters for importing a CSV file e.g. what should be imported or which separators were used in the CSV file.

File content



After importing the CSV file, you can check here if the data is mapped correctly. You can select lines and then import them. After the import you will see a log. The imported data is available in the database

6.1.1. Read device data into the database

Read device data into the database

To read device data into the database, proceed as follows:

- Click on the “Search devices” button in the “Tasks” tab.

The “Search devices” window opens.

You will be prompted to hold the RF wake-up card in front of the device to be read in.

- Hold the RF wake-up card in front of the device to be read in.
- Enter a name for the device

> This can be, for example, the description of the associated door.

- If a new device is to be created, go to “next”.
- If the device is to replace an existing one, select “replace existing device”
- To discard entries, click on the “Cancel” button
- Next, select the “Couple & program device” button

- To read in another device, click on the “Start search” button

6.1.2. Couple device

Couple device

To couple a device, proceed as follows:

- Click the “Couple & Program Device” button.

You will be prompted to hold the RF wake-up card in front of the device to be coupled.

- Hold the RF wake-up card in front of the device to be read in. This is not mandatory for BLE (V2) devices.

The coupling of the device is executed.

You will see a closed padlock in the top right window.
The device information is displayed. The device is coupled.

- Click on the “OK” button

If the closed padlock is not displayed, you must repeat the coupling process.

6.1.3. Decouple device

Decouple device

To decouple a device, proceed as follows:

- Click on the “Search devices” button in the “Tasks” tab.

The “Search devices” window opens.

You will be prompted to hold the RF wake-up card in front of the device to be coupled.

- Hold the RF wake-up card in front of the device to be read in. This is not mandatory for BLE (V2) devices.

- Select the device you wish to decouple in the list.

The device information is read, and a window with device name and area is displayed.

- Click on “Next” button

You will be asked if you wish to program the device. Click on “No”.

- Click on the “Decouple device” button.

A confirmation prompt is displayed

- If you do not want to decouple the device, click on the “No” button
- If you want to decouple the device, click on the “Yes” button.

You will be prompted to hold the RF wake-up card in front of the device you want to decouple. This is not mandatory for BLE (V2) devices.

- Hold the RF wake-up card in front of the device to be read in.

The decoupling of the device is executed.

The device is decoupled. The “Decouple device” button is grayed out

6.1.4. Program device

Program device

You can program offline devices also with the DOM Service app

If the device is coupled and you have defined the device and area authorizations in the ENiQ software, you can program the device. Here, the defined authorizations are made available to the device via the USB radio stick. You can only program one device at a time.

To program a device, proceed as follows:

- In the “Tasks” tab, click the “Execute Programming” button.

You will be prompted to hold the RF wake-up card in front of the device to be programmed. This is not mandatory for BLE (V2) devices.

- Hold the RF wake-up card in front of the device.

The programming is executed.

The device is programmed

6.1.5. Import/export data

6.1.5.1. Import and export persons

The import and export tools allow to easily create, update or delete a batch of persons.

Persons can be imported using an Excel or CSV file. However, the file should have a specific format. Templates can be found by clicking on ENiQ Device Management / “Import” tab / “Open template folder”: Import_Persons.csv, Import_Persons.xlsx, Import_Persons_Testfile.csv and Import_Persons_Testfile.xlsx. Test files contain 1 line of test data.

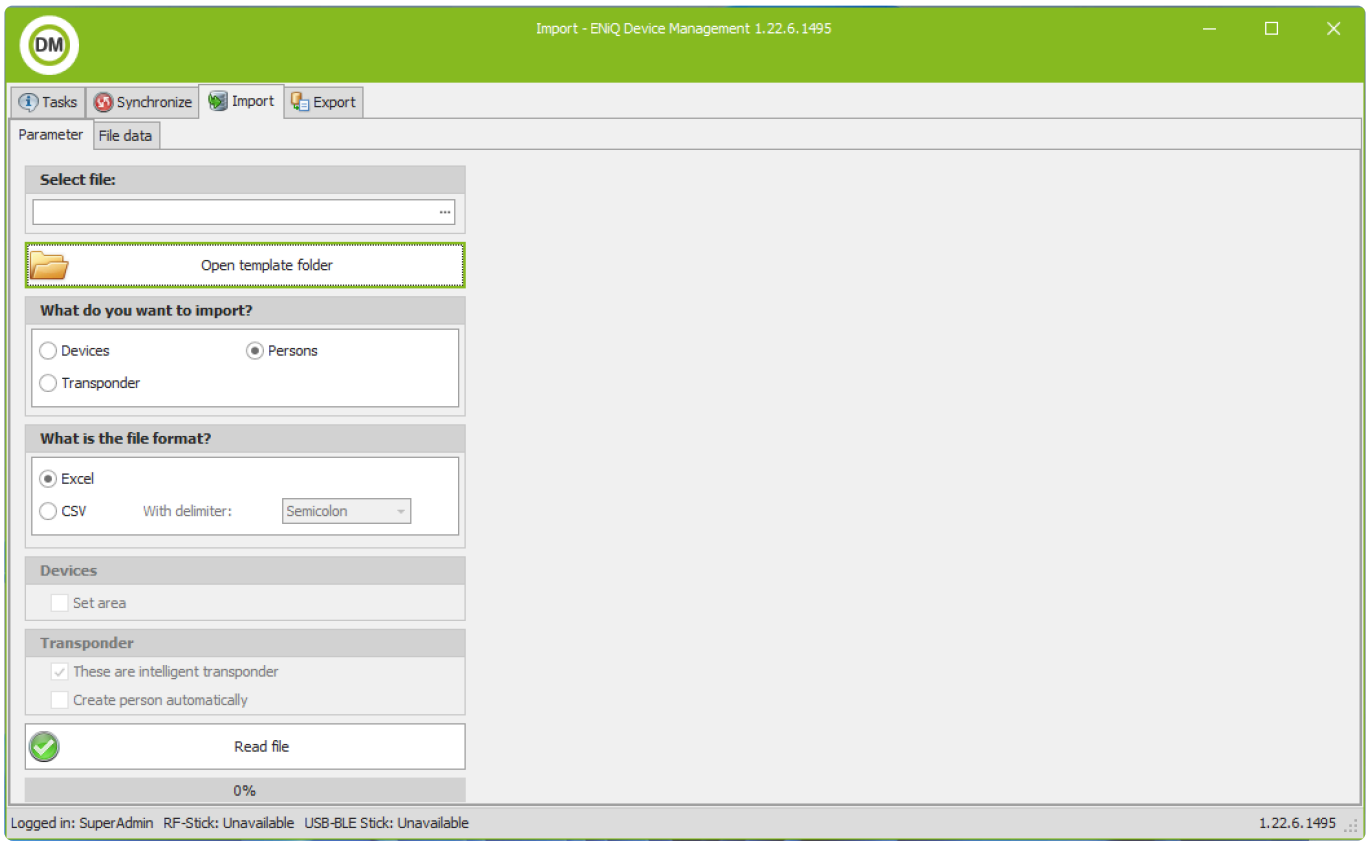
Description of import/export attributes

Attribute	Description
GUID	Identifier for the existing persons. **Required** if the person should be edited. If the row has no GUID, it will be considered as a new person, and will be created upon import.
Full Name	Full name for the person, as it is displayed in ENiQ AccessManagement. For new persons, it is a **mandatory** attribute if “First Name” and “Last Name” attributes are empty.
First Name	First name for the person. It is a **required** attribute if “Full Name” is empty. After import, “Full Name” will be generated by combining “First Name” and “Last Name”, as “First Name, Last Name”.
Last Name	Last name for the person. It is a **required** attribute if “Full Name” is empty. After import, “Full Name” will be generated by combining “First Name” and “Last Name”, as “First Name, Last Name”.
Personal Number	Personal number for the person (optional). Should be unique.
Department	Department for the person (optional).
Job Title	Job Title for the person (optional).
Phone Number	Phone Number for the person (optional). Not related to “Mobile Keys” attribute
Email	Email for the person (optional).
Person Groups	All Person Groups (Names) for the person, separated by a semicolon ‘;’ (optional). If the Person Group does not exist, it will be created when importing. This field is case insensitive.
Transponders	All Transponders (Type.UID, eg. “45.043513EA561278”) for the person, separated by a semicolon ‘;’ (optional). If the Transponder does not exist, it will be created.
Mobile Keys	All Mobile Keys (Phone Numbers, eg. “+33123456789”) for the person, separated by a semicolon ‘;’ (optional). When importing, all new assigned Mobile Keys will be created automatically.
Valid From	Valid From date for the person (optional). The date format is “DD/MM/YYYY HH:MM”

Valid Until	Valid Until date for the person (optional). The date format is “DD/MM/YYYY HH:MM”
Note	Note for the person (optional).
Delete?	Marker if the person should be deleted (only for existing persons, having a GUID). If the person should be deleted, set it as “Yes”. Otherwise, leave it empty (default).

Import new persons

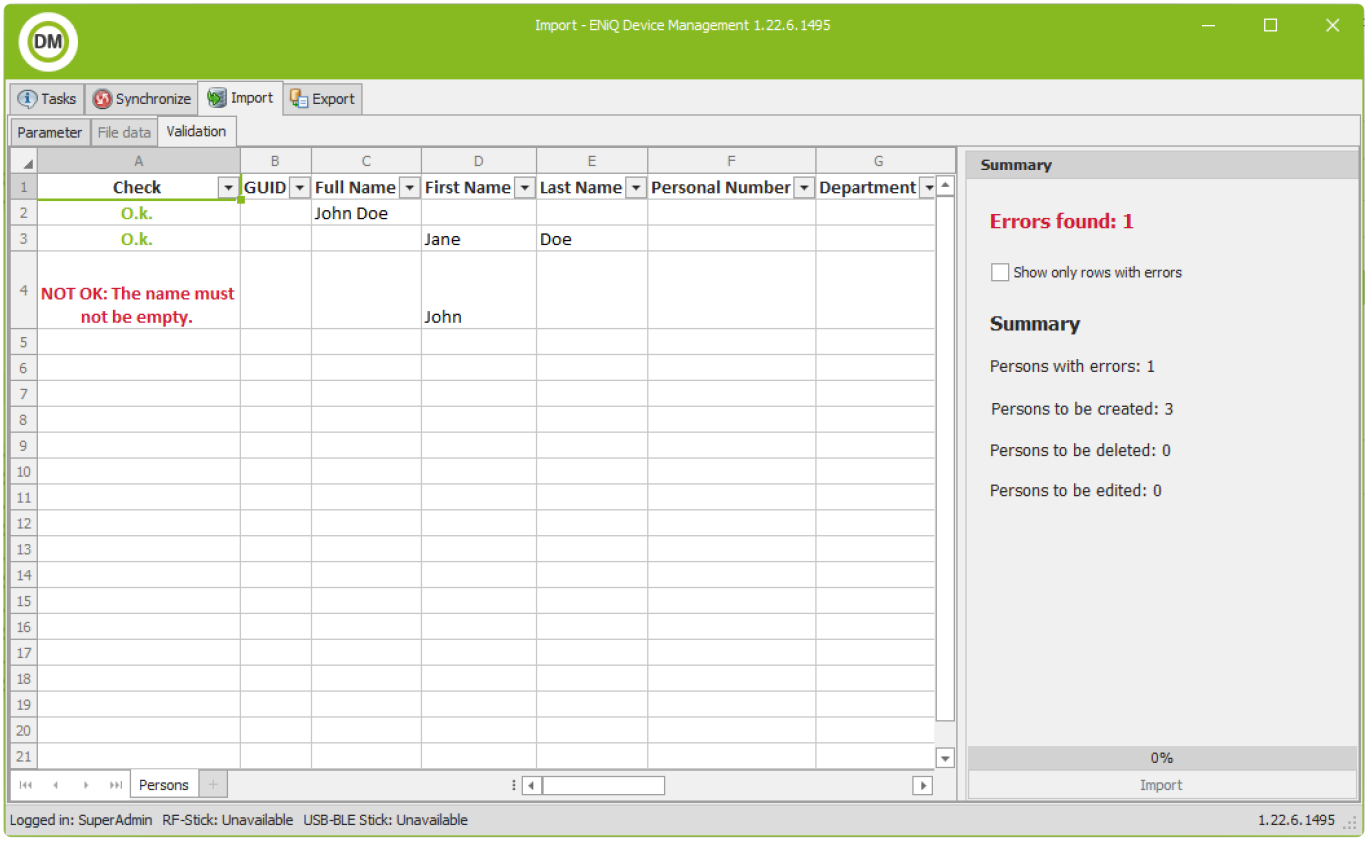
- Open “ENiQ Device Management” software, and sign in as an authorised user
- Go to the “Import” tab



- Select the file to import
- Select “Persons”
- Select the file format: CSV or Excel

> When importing data with CSV file, the attributes having multiple values (“Person Groups”, “Transponders” or “Mobile Keys”), have to be escaped with “”. Example: if the person should be in groups “Group1” and “Group2”, the attribute for “Person Groups” in the CSV file should be “Group1;Group2”.

- Click “Read file”. This can take a while, depending on the size of the file.
- The “Validation” tab will open, with a summary of the scanned import file.



A “Check” column indicates if the row has any error. A “summary” panel on the right lists all errors and actions that will be done: creations, updates, deletions.

> ✻ The preview is read-only. The original file should be edited and read again until all errors are fixed.

- When the import file contains no errors, click on “Import” button on the bottom-right corner. All persons will be created.

Export persons

- Open “ENiQ Device Management” software, and sign in as an authorised user
- Go to the “Export” tab
- Select “Persons”
- Click “Export data”. All persons will be exported.

Batch update persons

- First export all persons from ENiQ AccessManagement (see “export persons”)
- Open exported Excel file, and remove all the rows of persons you do not wish to update
- On the remaining person rows, update the needed attributes.

> ! When importing existing persons, all the person attributes will be overwritten. It is not possible to **only fill** the attributes you wish to update, otherwise all other attributes will

be cleared. That is why it is important to always do an export of the persons you wish to update.

When removing Person Groups, Mobile Keys, or Transponders from a person, those objects will be unassigned from the person when importing.

- When all needed attributes are updated, go to “ENiQ Device Management / Import” tab
- Select the exported and modified file
- Select “Persons”
- Select the “Excel” file format
- Click on “Read file”
- On the “Validation” tab, check that there is no errors. Otherwise, fix the original file and read it again from “Import” tab
- When the import file contains no errors, click on “Import” button on the bottom-right corner. All persons will be updated.

6.2. Use Access Management

Prerequisites
To use the software, the following requirements must be met:

- Complete installation of the program on the computer
- Database available
- Desk reader connected, for information on how to integrate the desk reader into the software, see “Integrating desk readers”
- Service DOM-Master Service started (the icon shown below in the taskbar shows green)
- DOM-Slave Service started (the icon shown below in the task bar is green)

Start software

> The ENiQ software has a web interface. When you start the software, it will be displayed in the default web browser.

To be able to work with the software, you have to start it on your computer.

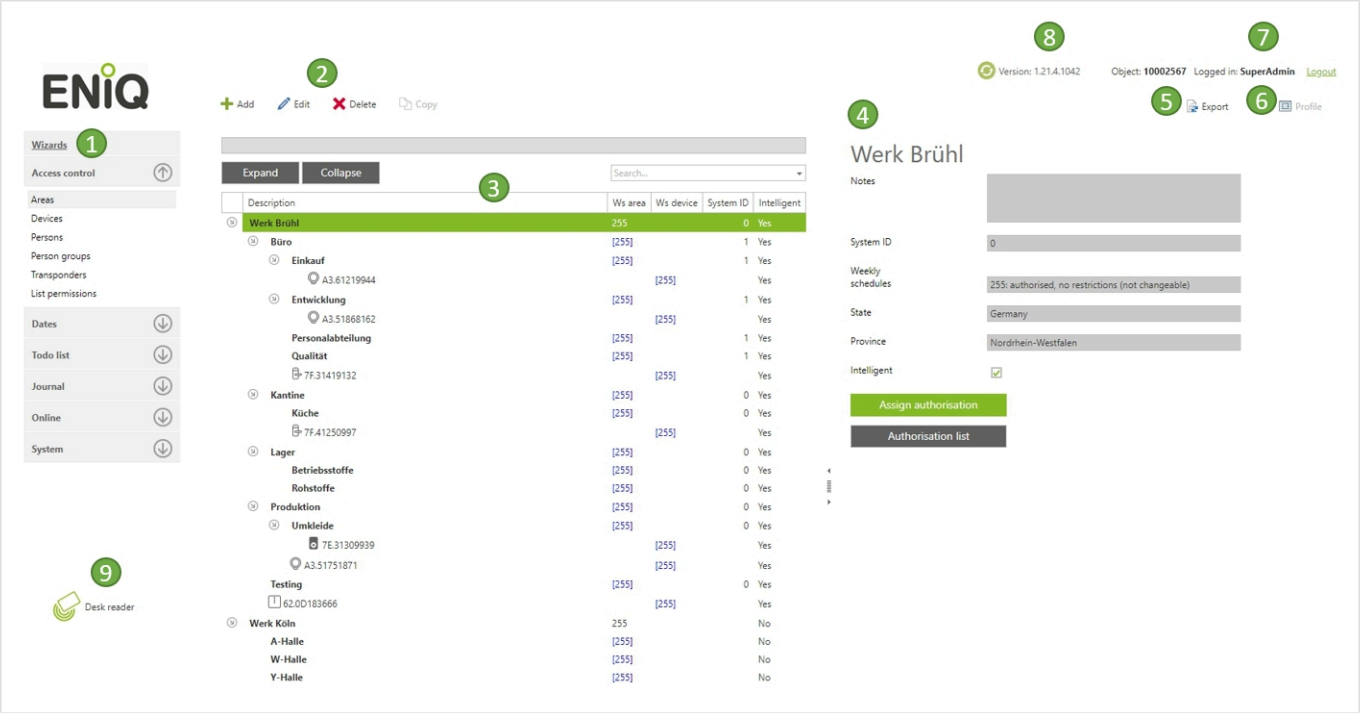
- Double click on the corresponding icon on the desktop.

- The software will start.

> For certain operations it is necessary to switch from the ENiQ Device Management software to the ENiQ software or vice versa.
> In such cases, start the ENiQ Device Management software and the ENiQ software in parallel.

Here you get an overview of the program interface and the functions of the program.

If you have logged in successfully, the program interface will be displayed.



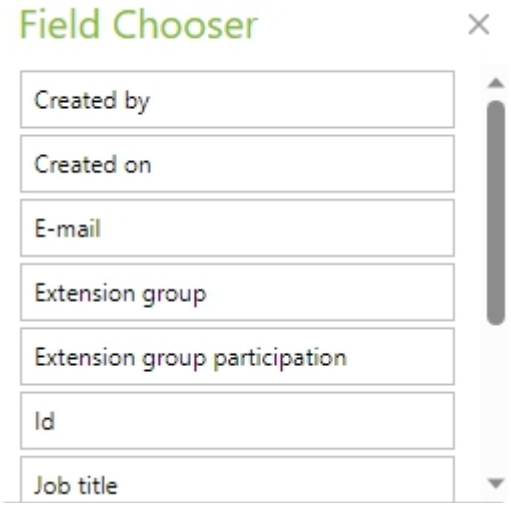
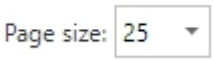
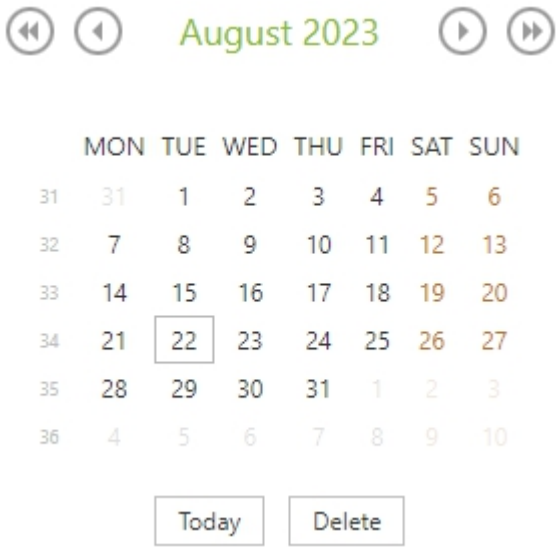
No.	Explanation
1	Navigation bar
2	Editing bar
3	Area tree
4	Detailed information about the selected area
5	Export button – Exports content to different file formats e.g. PDF, XLS, CSV, RTF
6	Button “Profile” – Opens a sub-menu to customize the program interface. Here you can influence the number of columns and arrangement of lists. Furthermore you can manage the profile data.
7	Name of the logged in operator
8	Version of the program
9	Button for using the desk reader

The following elements are available on the program interface. They are displayed case by case.

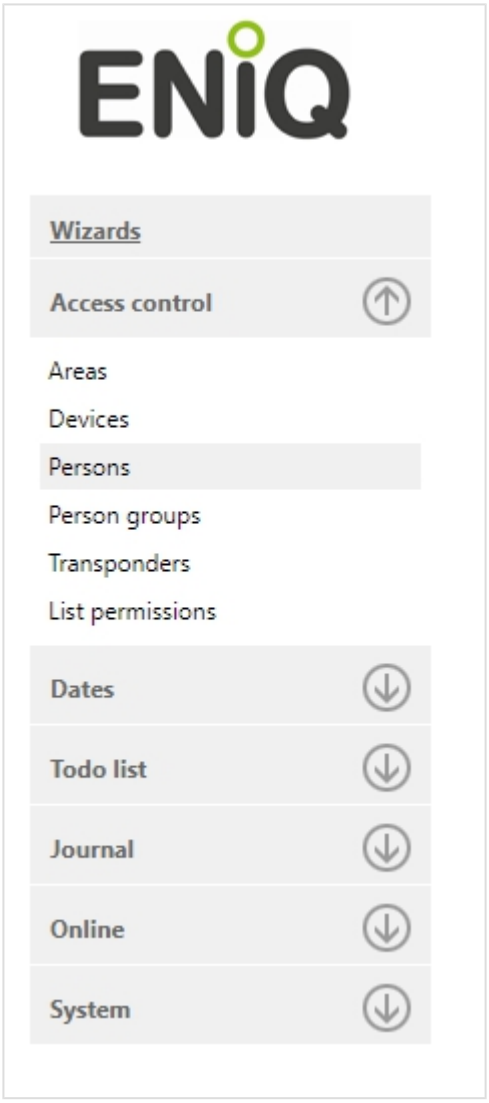
Symbol	Explanation
	Expand sub-elements of the navigation bar.
	Close sub-elements of the navigation bar.
	Expand sub-elements in the area tree.
	Close sub-elements in the area tree.
	Add content.

 Edit	Edit content.
 Delete	Delete contents.
 Copy	Copy contents.
	Navigate one page backwards.
	Navigate one page forward.
 Export	Select different options Show file formats for export.
 PDF	Export content as PDF file.
 XLS	Export contents as XLS file.
 RTF	Export contents as RTF file.
 CSV	Export contents as CSV file.
 Profile	Opens a sub-menu for customizing the program interface. Here you can influence the number of columns and the arrangement of lists. Furthermore you can manage the profile data.
 Select columns	Opens a sub-menu with column headers. In this sub-menu you can add or remove column headers from your current list by holding down the mouse button.
 Save settings	Saves the new column view of your list.
 Add	Add new profile data.
	Save new profile data.
	Cancel operation and go to the previous screen.
 Edit	Edit existing profile data.
 Delete	Delete profile data.
	Apply profile data.
	Apply profile data and switch to the previous screen.

×	Close window.
Logout	Log off from the program interface.
 Desk reader	Activate desk reader.
Save	Save entries and go to the previous screen page.
Cancel	Cancel operation and go to the previous screen.
OK	Save entries and go to the previous screen page.
Save	Accept entries and make further settings on this screen page.
Remove all authorisations	Remove all permissions.
	Here the receipt printout is started (a listing of the authorization for the person/transponder)
	Here you can enable or disable options.
Expand	Expand the structure of the area tree and view it completely.
Collapse	Close structure of the range tree.
	On some screen pages you have to select entries. This is done with drop down menus. You can recognize a drop down menu by a small arrow on the right side. You can select an entry from a list or enter a search term in the input field.
Assign authorisation	Access control / Authorization menu.
Authorisation list	Open the authorization list.
Access events	Retrieve access events from devices.
Export	Export data.
Clear filter	Reset input.
Save and write	Save and write entries to a transponder.

	Adjust the size of the window areas.
	Add columns to a list or remove existing ones.
	Set the number of entries to display per page.
	Select calendar dates, e.g. to define authorization periods.
	Add entries from one list to another list.
	Remove entries from a list.

Navigation bar



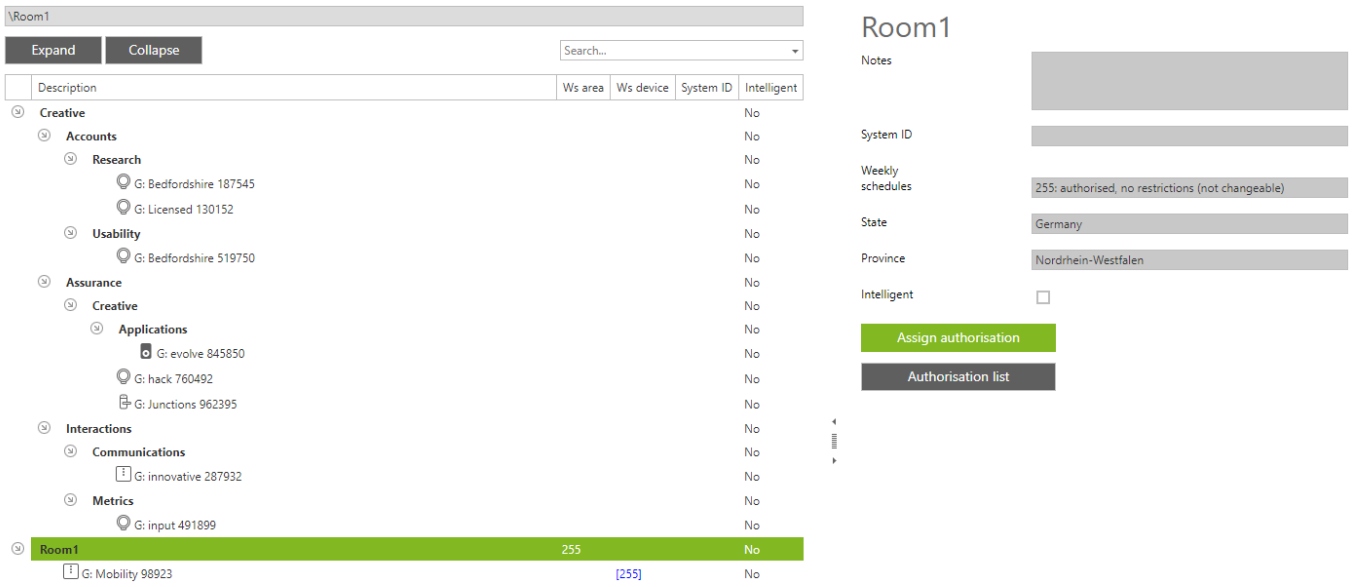
You can open the entries in the navigation bar with a mouse click. Explanations to the main entries can be found in the basic functions.

Edit bar

The four buttons in the edit bar are available for list entries.
The following functions can be executed:
* Add entries
* Edit entries
* Delete entries
* Copy entries

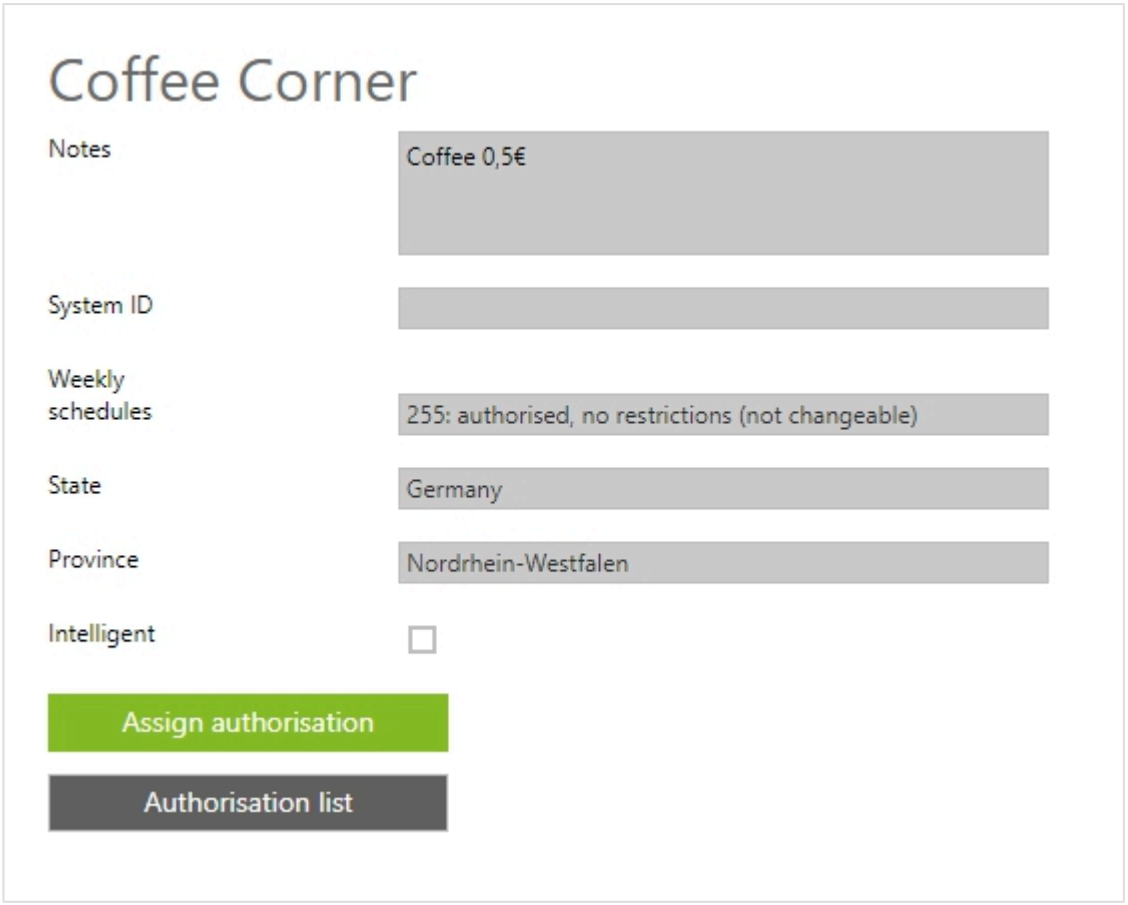
Not all functions are always available. Functions that are not available are grayed out.

Area tree



In the area tree the structure of the object existing in the database is displayed. Here you can create, change the structure of the object, add devices, etc.

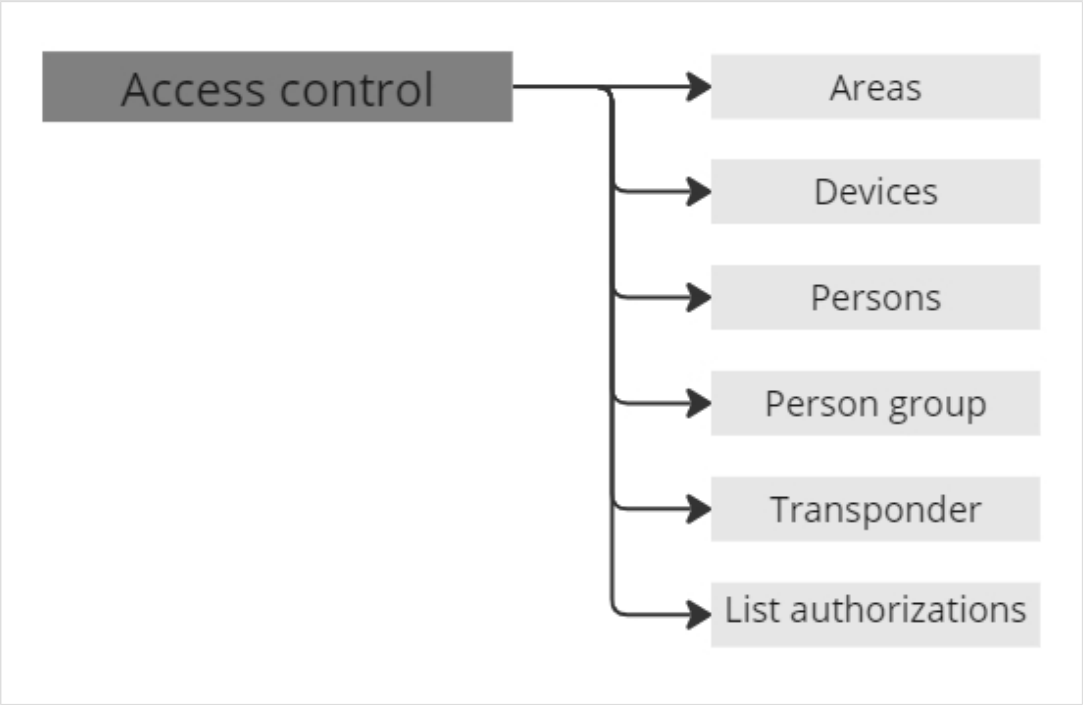
Detailed information



Here you can see detailed information about a marked entry in the area tree. The “Assign authorization” and “Authorization list” buttons take you to menus. In the menus, you can assign authorizations or display existing authorizations In the case of devices, you can also open the access events

6.2.1. Menu structure

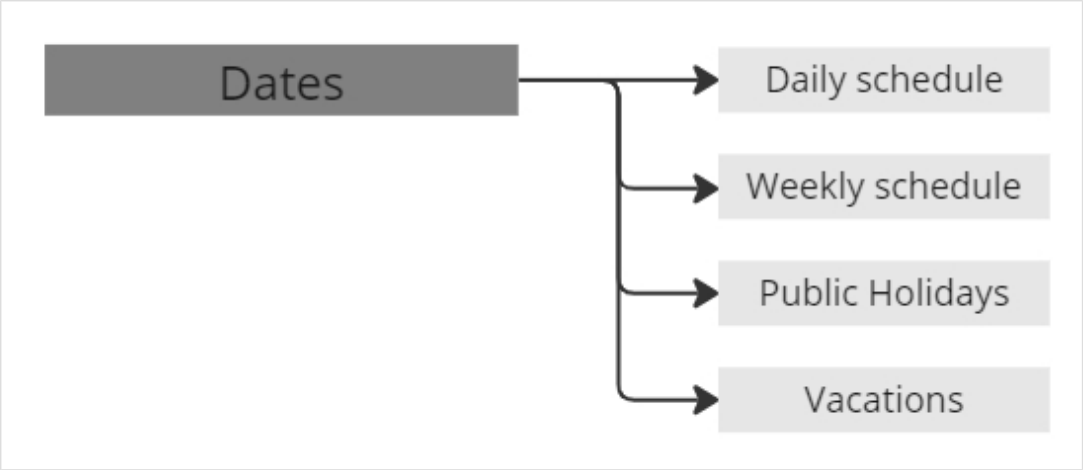
Explanation of the menu items



“Access control” menu

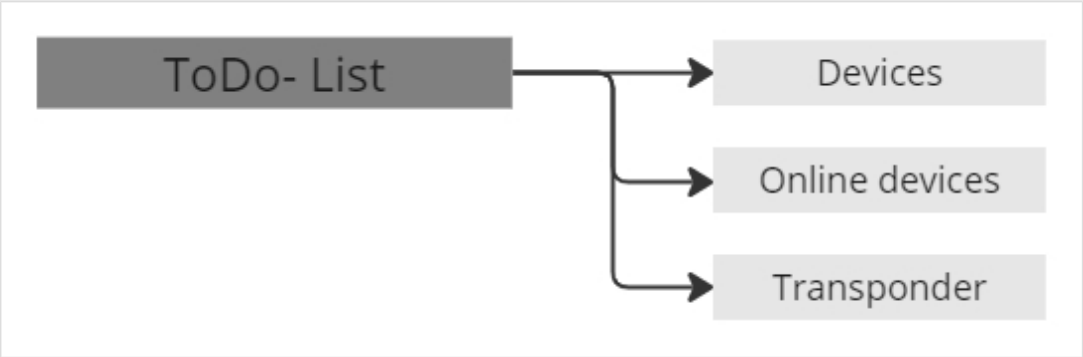
Entry	Explanation/ Function
Areas	Open overview. Assign areas to the object in the database, e.g. a building, e.g. individual rooms.
Devices	Manage and configure devices and assign them to areas.
Persons	Add, edit and delete persons.
Person Group	Assign persons with identical authorizations to a person group, e.g. cleaning staff.
Mobile Keys	Manage, add and edit mobile keys.
Transponder	Manage, add and edit locking media.

List Authorizations	View all assigned authorizations. You can filter the generated list and export it as an XLS file.



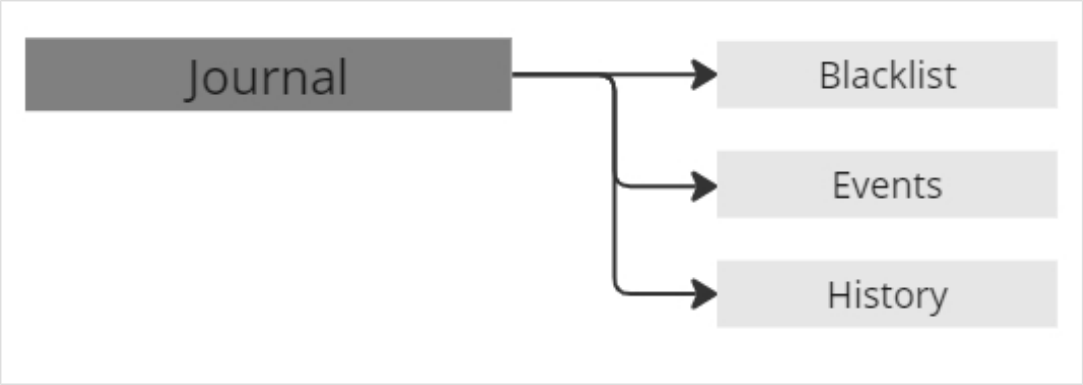
“Dates” menu

Entry	Explanation/ Function
Daily schedule	Create a daily schedule for access in 15 minute intervals.
Weekly schedule	Create a weekly schedule for access from one or more daily schedules.
Public Holidays	Enter specific holidays for each state.
Vacations	Enter vacation dates specifically for each state.



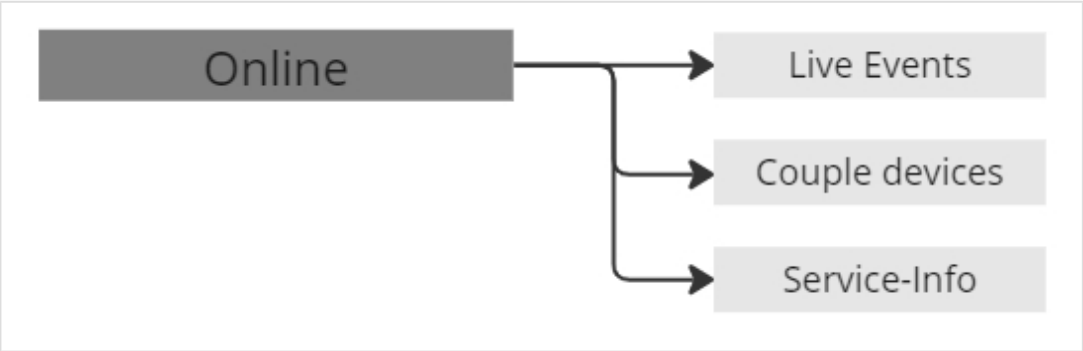
“ToDo List” menu

Entry	Explanation/ Function
Devices	List information about devices to which an action must be made, such as transferring a changed weekly schedule to the device.
Online devices	List information about online devices to which an action must be made, such as transferring a changed weekly schedule to the device.
Transponder	List information about transponders to which an action must be made, such as transferring changed authorizations to the transponder.
Mobile Keys	List information about mobile keys to which an action must be made, such as transferring changed authorizations. These tasks are performed automatically by the software at regular intervals, provided that an Internet connection is available.



“Journal” menu

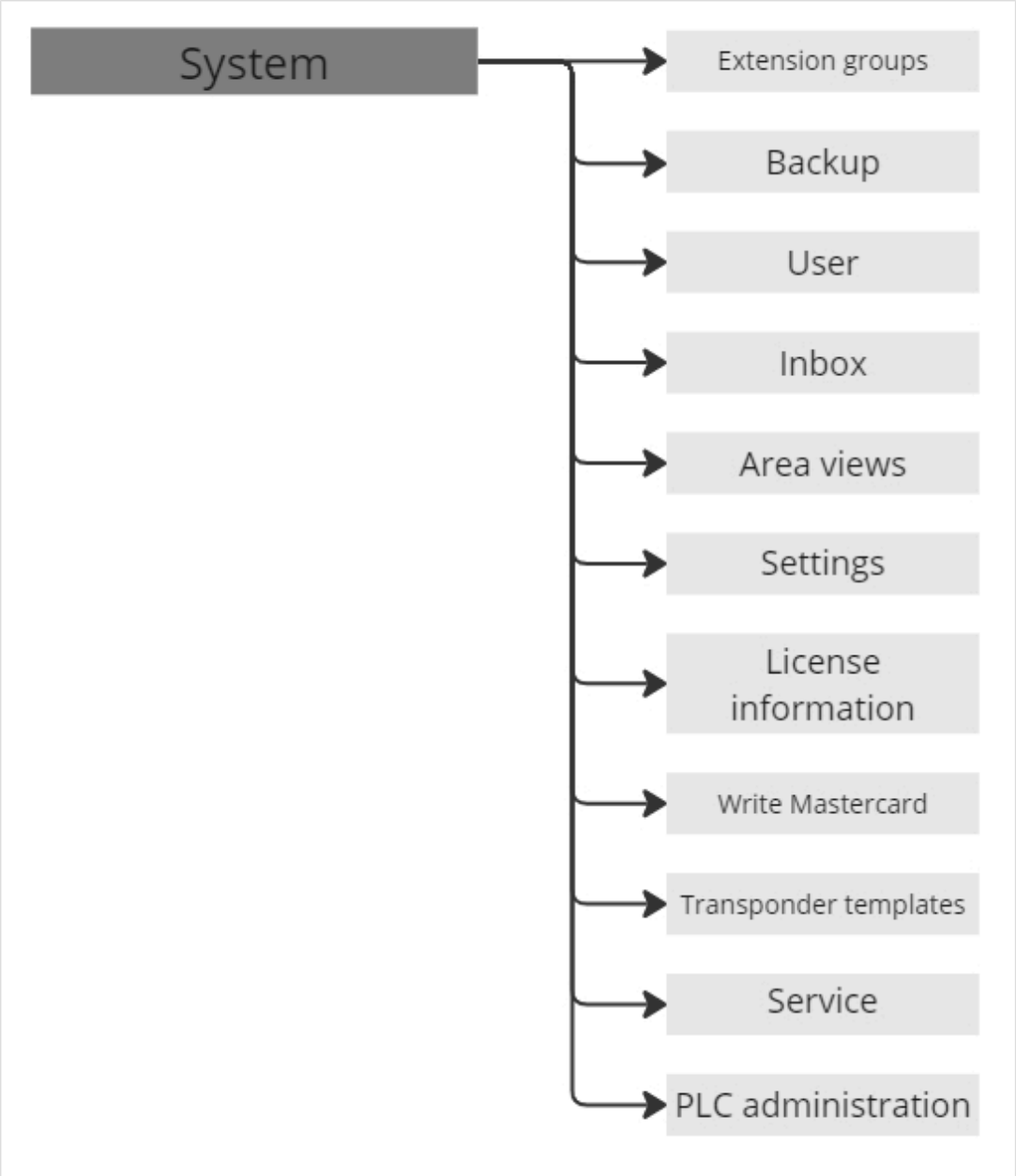
Entry	Explanation/ Function
Blacklist	List with information about blocked transponders.
Events	List events of the devices available in the system chronologically, e.g. the use of the RF wake-up card.
History	All events that you have made as a user are listed here. For example, add/edit/delete persons/ groups of persons.



“Online” menu

You can only access this menu if a valid online license is activated in the system.

Entry	Explanation/ Function
Live events	Display a list containing all events of different online devices. These are e.g.: Accesses, use of unknown transponders, and many more. These events are generated in real time.
Couple devices	During the automatic creation of DOM Online devices (Plug & Play), this menu item displays the devices that have registered for coupling (via Ethernet or radio). Via the button “Couple devices” you can have the selected device automatically coupled so that you can use it in the ENiQ software for access control. Coupled devices are then removed from the list.
Service Info	Add and configure e.g. online services, IP addresses, ports, DNS etc.



“System” menu

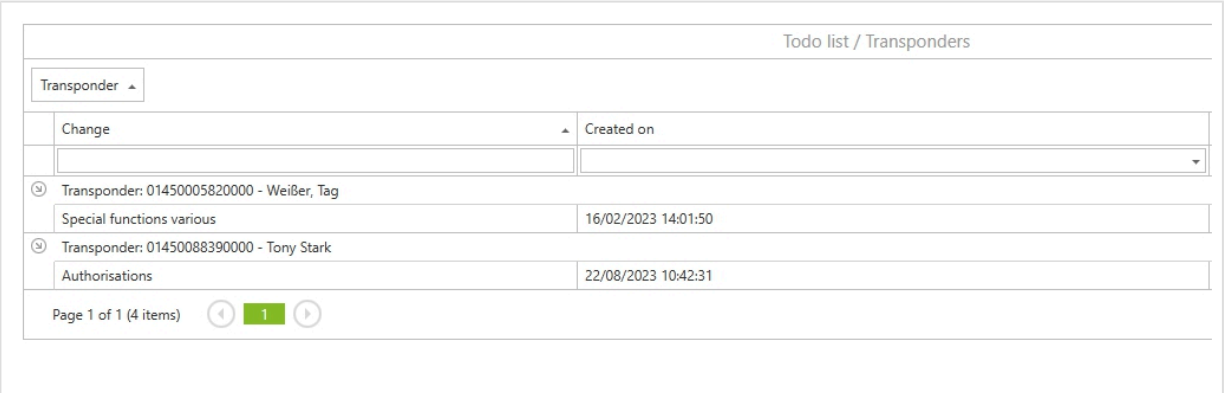
Entry	Explanation/ Function
Extension groups	Overview of available extension groups.
Backup	Create a backup of the database.
Users	Retrieve and change information about operators of the system. New operators can be created or added. Manage existing operators.
Inbox	Inbox where you can get information about new features in the software.
Area Views	Overview for creating area views for operators.
Settings	Here you can make settings regarding history, online and MuM and many more.
License Information	Get license information about the program. Furthermore you can extend the license.

Write Mastercard	Provide an unwritten Mastercard with the object keys of the database. Afterwards you can create and couple new devices manually with this card. Keep this card protected from unauthorized access.
Transponder templates	View and activate the available transponder templates. A transponder template divides the memory space available on a transponder. The maximum number of areas and devices is defined in the selected template.
Service management	View system information.
PLC Administration	Overview of PLC files.
Update Information	Information current version and available updates.

6.2.2. Standard tables – representation and functions

Group lists by column headers

To group the contents of your current list view by a column header, do the following:



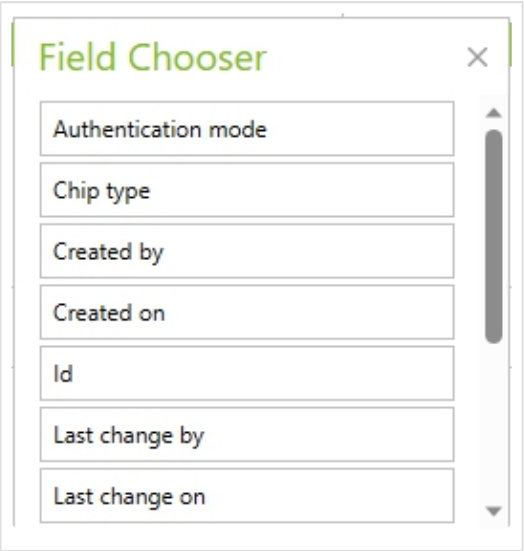
- Click on a column header and drag it to the area above while holding down the mouse button.
- Release the mouse button when you see the gray marker arrows

The contents of the list will automatically be sorted by the column header.

Add column headers to lists

To add more columns to your current list view, do the following:

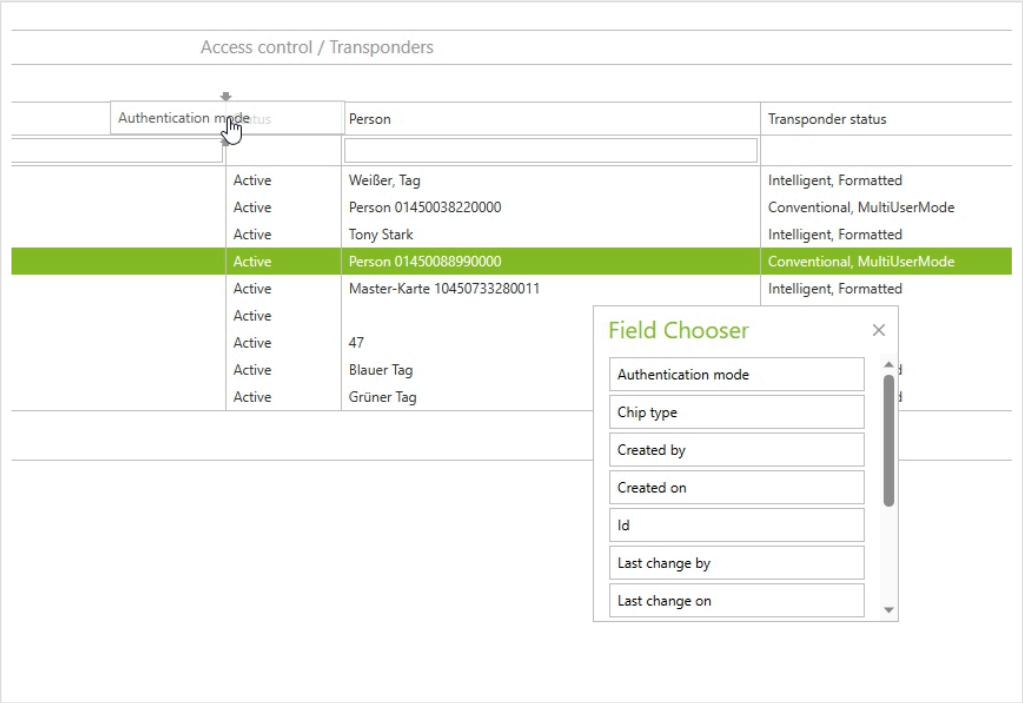
- Click the Profile button, then click Select Columns.



The “Field selection” window opens.

- In the list, select the column header you want to add to your current list view.
- Drag your selected column header into the current list view with the mouse button held down.

- Release the mouse button when you see the gray marker arrows



The new column will be added.

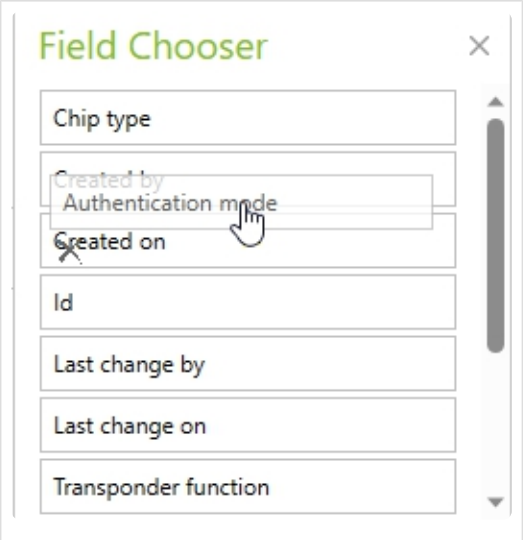
Delete column headers in lists

To remove columns from your current list view, do the following:

- Click the “Profile” button.

A “Field Selection” window will open. In the list, locate the column header you want to remove from your current list view.

- Drag your selected column header into the “Field Selection” window while holding down the mouse button.
- Release the mouse button when a small cross appears behind your selection.



The column header will be removed from the list.

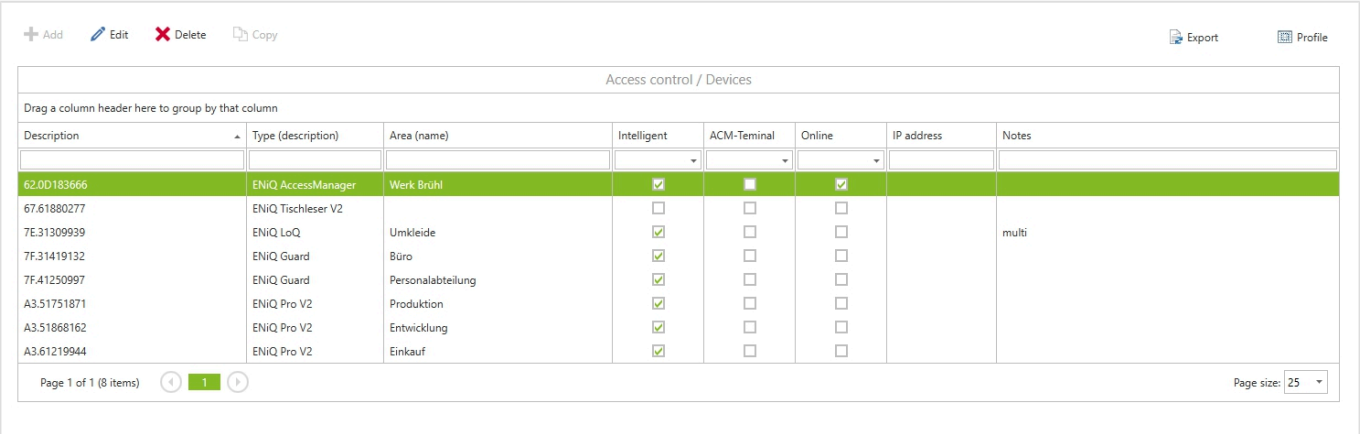
6.2.3. Set properties of a device

This section provides information on how to assign the following properties to a device:

- Assign the device to an area
- Assign a weekly schedule to the device
- Assign special properties to the device using weekly schedules
- Set a wait time for the second temporary release for the device.

To assign a device that exists in the system to an area, do the following:

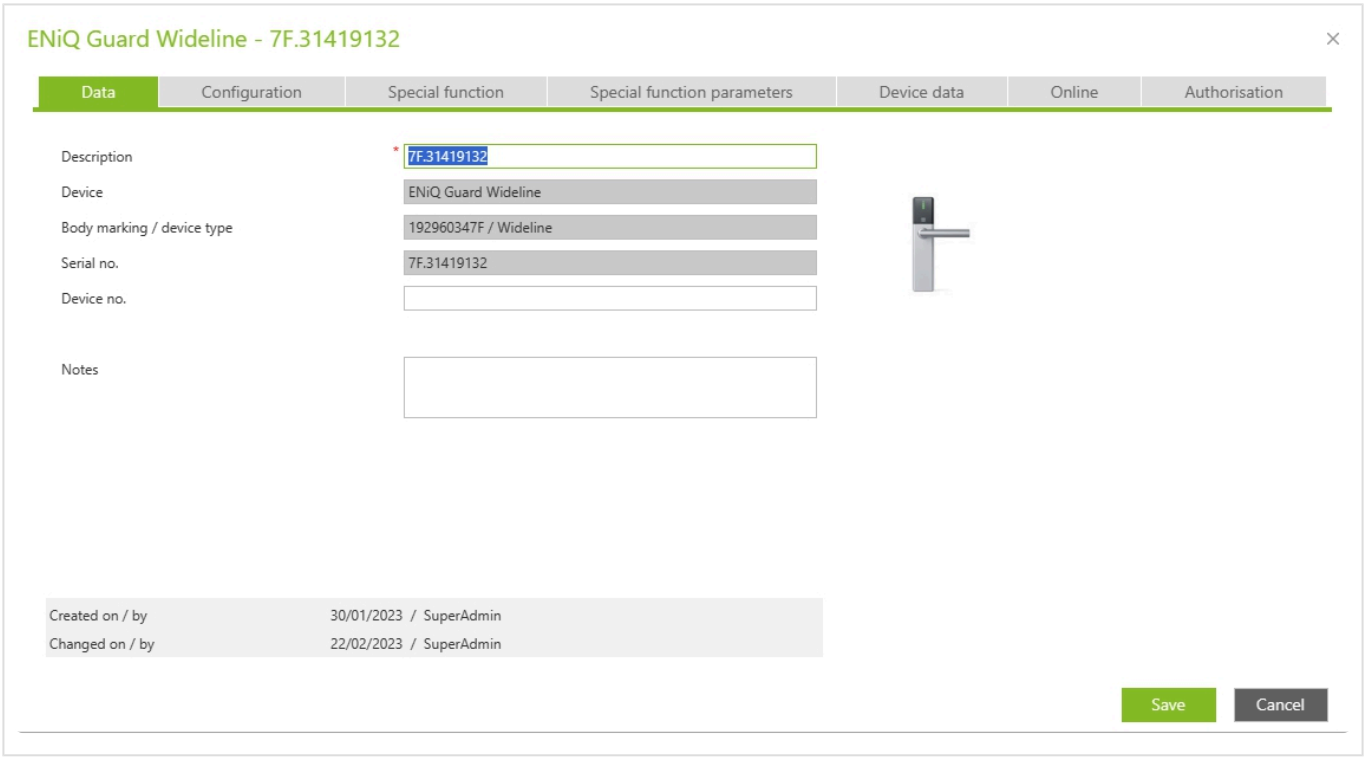
- Click on “Access Control” in the navigation bar.
- Select the “Devices” menu item



The “Access Control/Devices” menu opens.

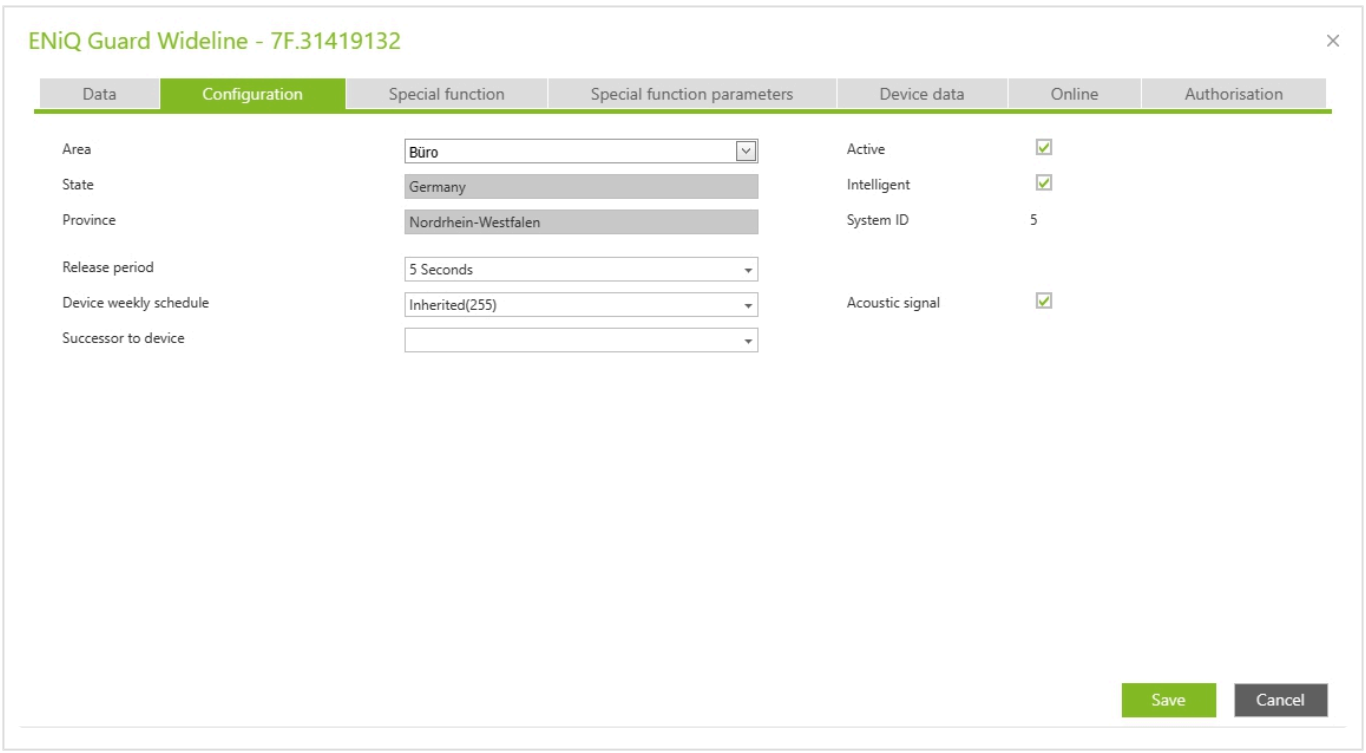
- Highlight the desired device in the list.
- Click the “Edit” button

> Alternatively, double-click on the highlighted device.



The menu of the selected device will be opened. The available device information is displayed on the “Data” tab.

- Switch to the “Configuration” tab
- Select the desired area from the drop-down menu



The mandatory field information is entered here from the area and inherited. They can be changed manually afterwards.

- Select a device weekly schedule from the drop-down menu.

- Enter the desired activation period in seconds.
- State and province are automatically selected based on the area.

> If you are using the new device to replace an existing device, select the device to replace from the drop-down menu.

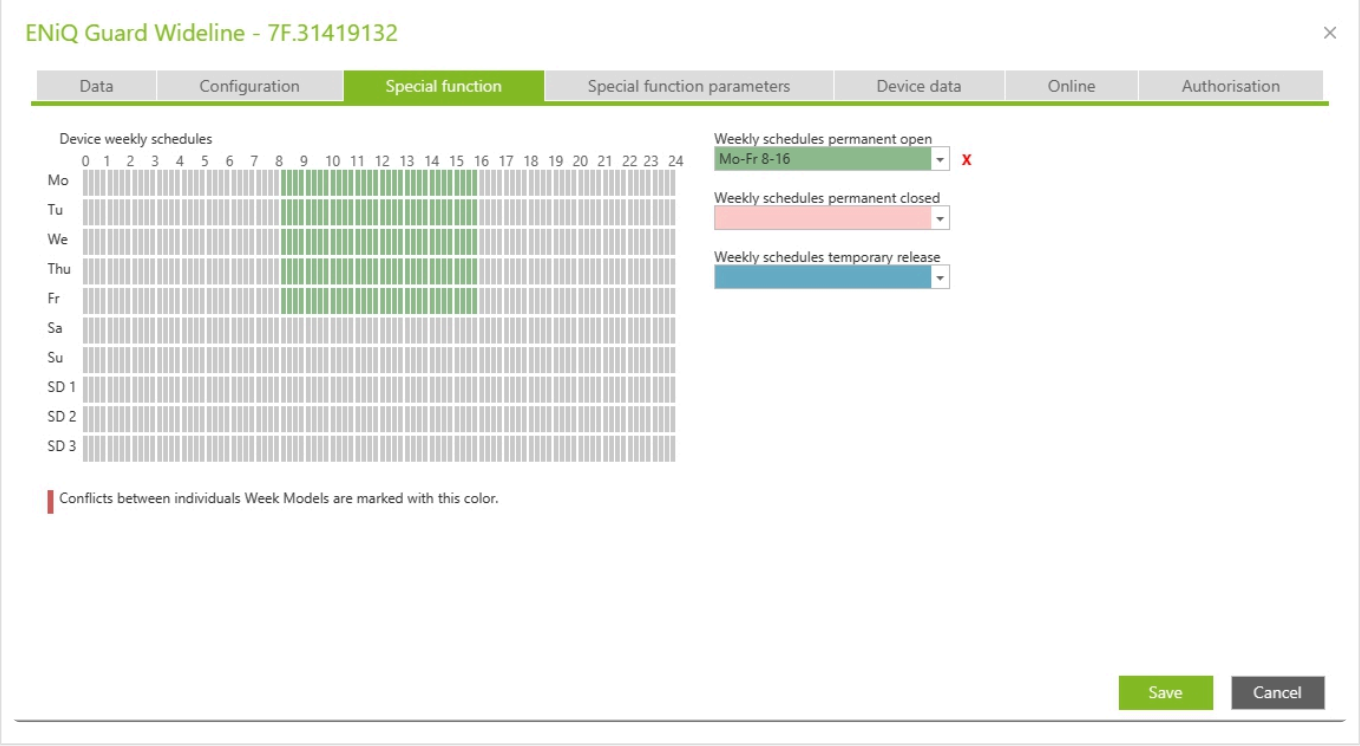
- If you want to create the device as “intelligent” (DataOnCard), set the checkmark in the “Intelligent (DataOnCard)” radio button.

If the area is already set as intelligent (DataOnCard), the device will automatically be set as intelligent (DataOnCard) as soon as it is assigned to the area.

- If you want to cancel the operation without saving, click “Cancel”.
- Click on “Save”.

To assign the special functions Permanently Open, Permanently Closed, Temporary Release, Access Repeat Lock (only for ENiQ AccessManager HiSec) or Multi-User Mode (only for ENiQ LoQ) to the device, proceed as follows:

- Switch to the “Special function” tab.
- Select the corresponding weekly schedule



- If you want to cancel the operation without saving, click “Cancel”.
- Click on “Save”.

- Switch to the “Special function parameters” tab.

Here you can enter a time in seconds. This defines the waiting time between the first and the second

presentation of the transponder. This setting is important for the double show for a temporary release.

- Enter the desired time
- If you want to cancel the operation without saving, click on “Cancel”.
- Click “Save”

To enable the device for online access and make the appropriate settings, proceed as follows:

- Switch to the “Online” tab.

- Activate the Online checkbox
- Use the arrow keys to enter a value for the desired “Alivetime”

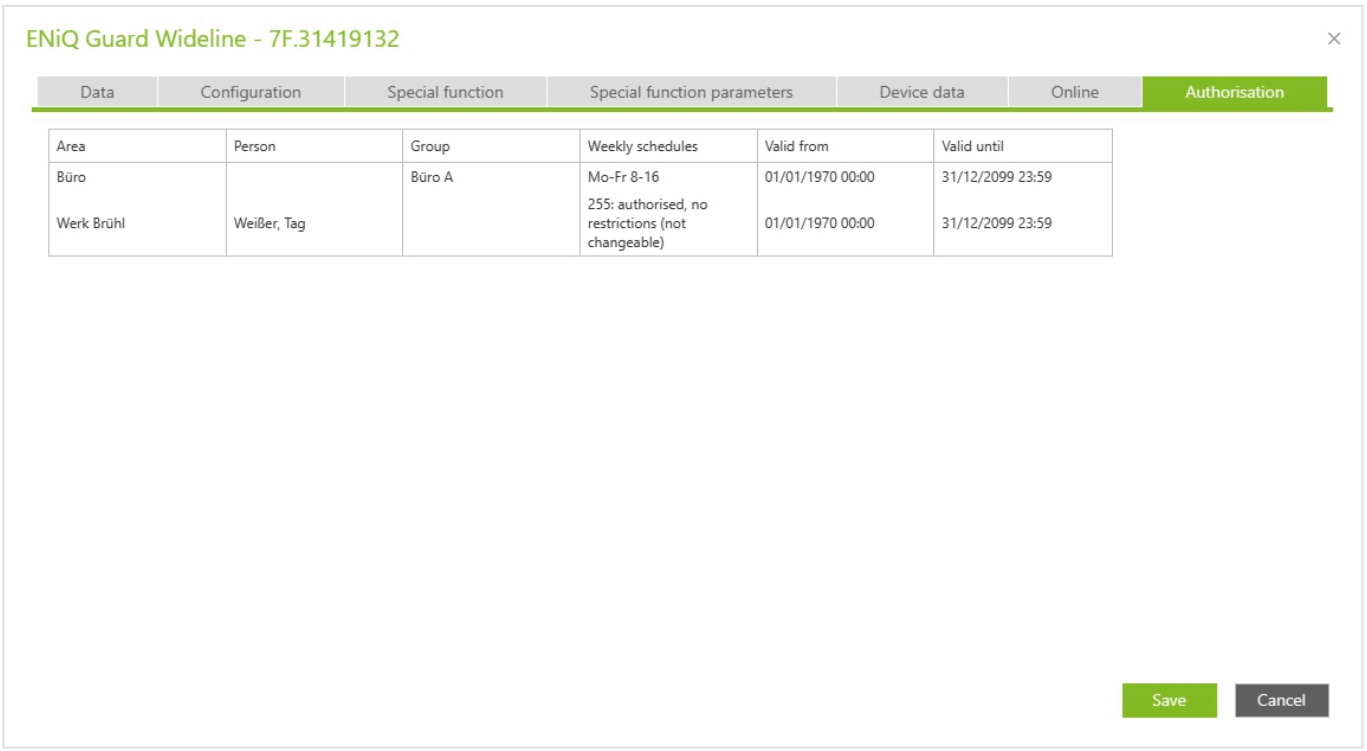
Use the “Alivetime” setting to specify the time interval at which the online device reports to the software to exchange information.

- Select the assigned slave service from the drop-down menu
- Select the assigned RF NetManager from the drop-down menu

- If you want to cancel the operation without saving, click on “Cancel”.
- Click “Save”

If you want to view information about the permissions assigned in the system, do the following:

- Go to the “Authorization” tab.



- If you want to cancel the operation without saving, click “Cancel”.
- To save the displayed selection, click on “Save”.

6.2.3.1. Eco Mode

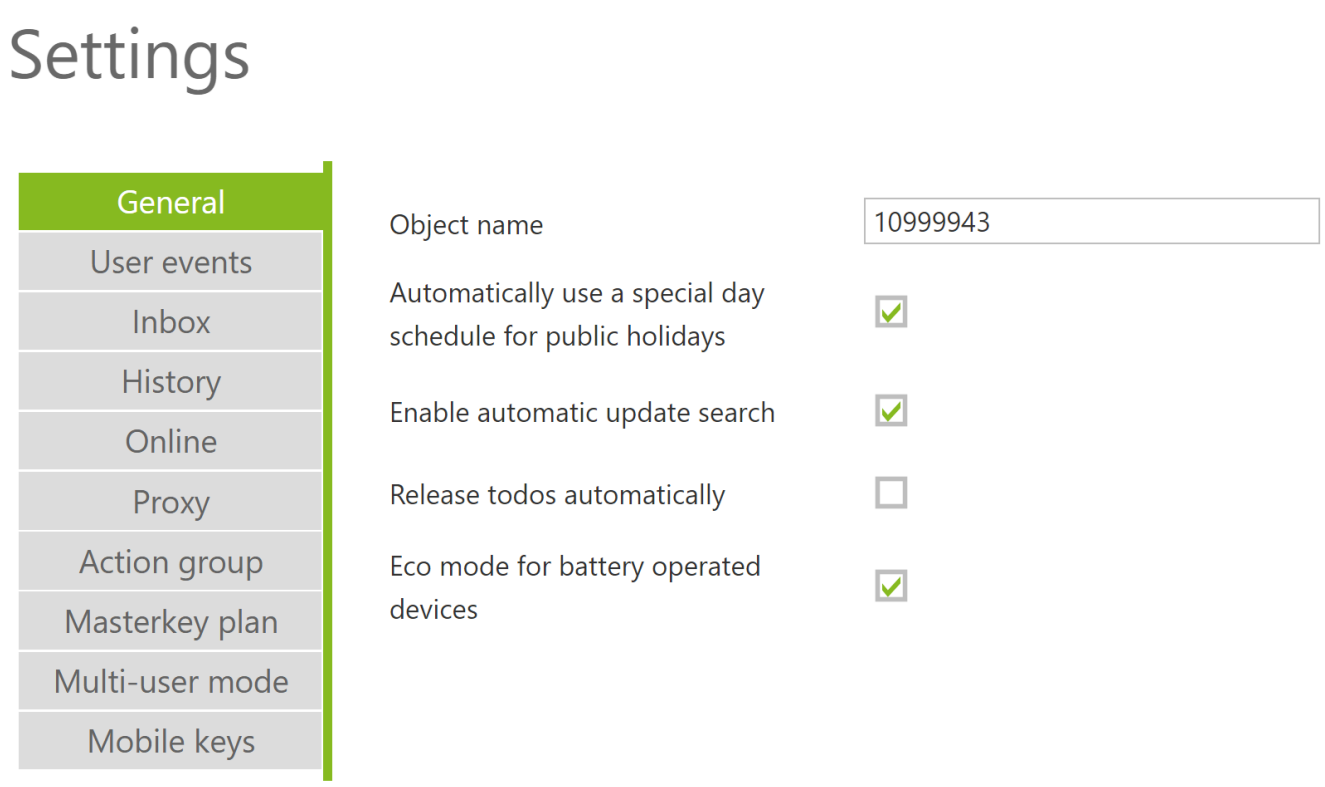
General information and setting up Eco mode

All ENiQ devices send a so-called advertisement after commissioning.
This means that the Bluetooth interface is permanently switched on and automatically sends the Bluetooth signal at regular intervals for communication.
However, the Bluetooth interface is not required for normal operation. The Bluetooth interface is only required to synchronize the devices with ENiQ Device Management.

If this is not required, the Bluetooth interface can be deactivated. This results in a longer battery life. Deactivating the Bluetooth interface is referred to as “Eco mode”.

To activate Eco mode, proceed as follows:

- System -> Settings -> General
- Activate the “Eco mode for battery-operated devices” checkbox



All battery-operated devices now have to be synchronized, to apply those changes.
By activating the checkbox, all battery-operated devices will use the Eco mode (idle Bluetooth interface)
.
To synchronize with ENiQ Device Management, activate the Bluetooth interface by holding up the RF wake-up card or a transponder.

Note
Eco mode is deactivated again when using online mode or the Mobile Key functionality for the

corresponding device.

6.2.4. Manage transponders/persons

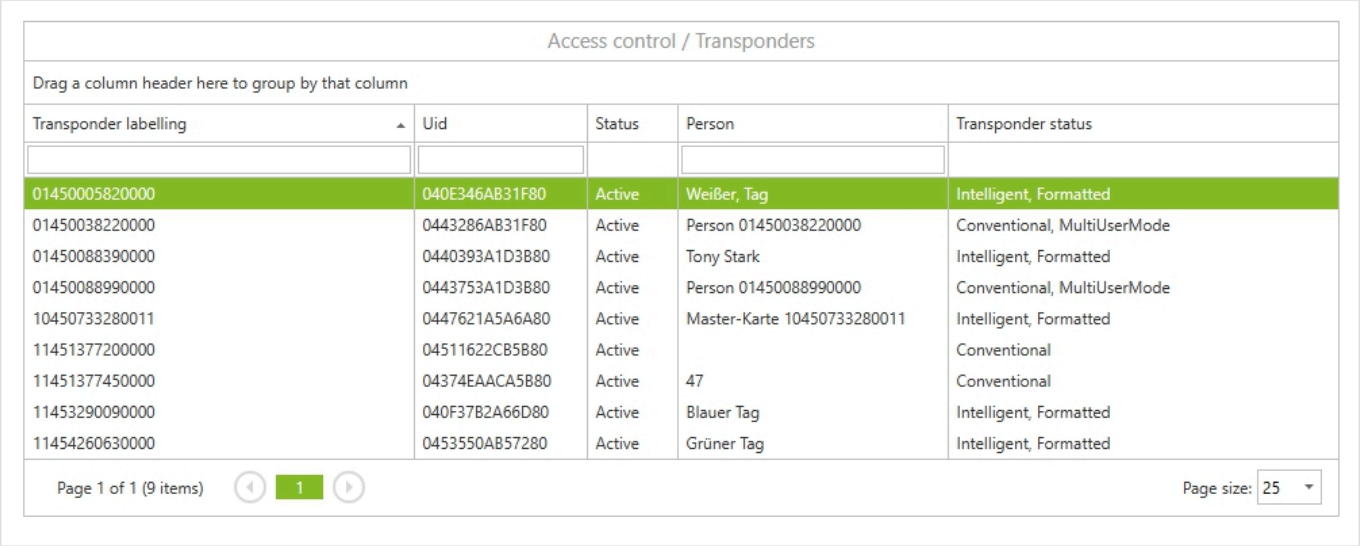
Manage transponders/persons

A transponder receives authorization for a device from a person by assigning the person to the device. If several people are to be given the same authorization for a device, these people can be assigned to a person group. You can then assign the authorization to the person group.
If the authorization of the person or person group is not assigned for a device but for an area or sub-area, the authorization is inherited by all sub-areas and devices contained in this area or sub-area by inheriting the assigned authorizations.
Transponders can be assigned to persons and thus receive their authorizations.

To create a person with a transponder, use the desk reader. The procedure is described in chapter Creating a person.

To manage a transponder, proceed as follows:

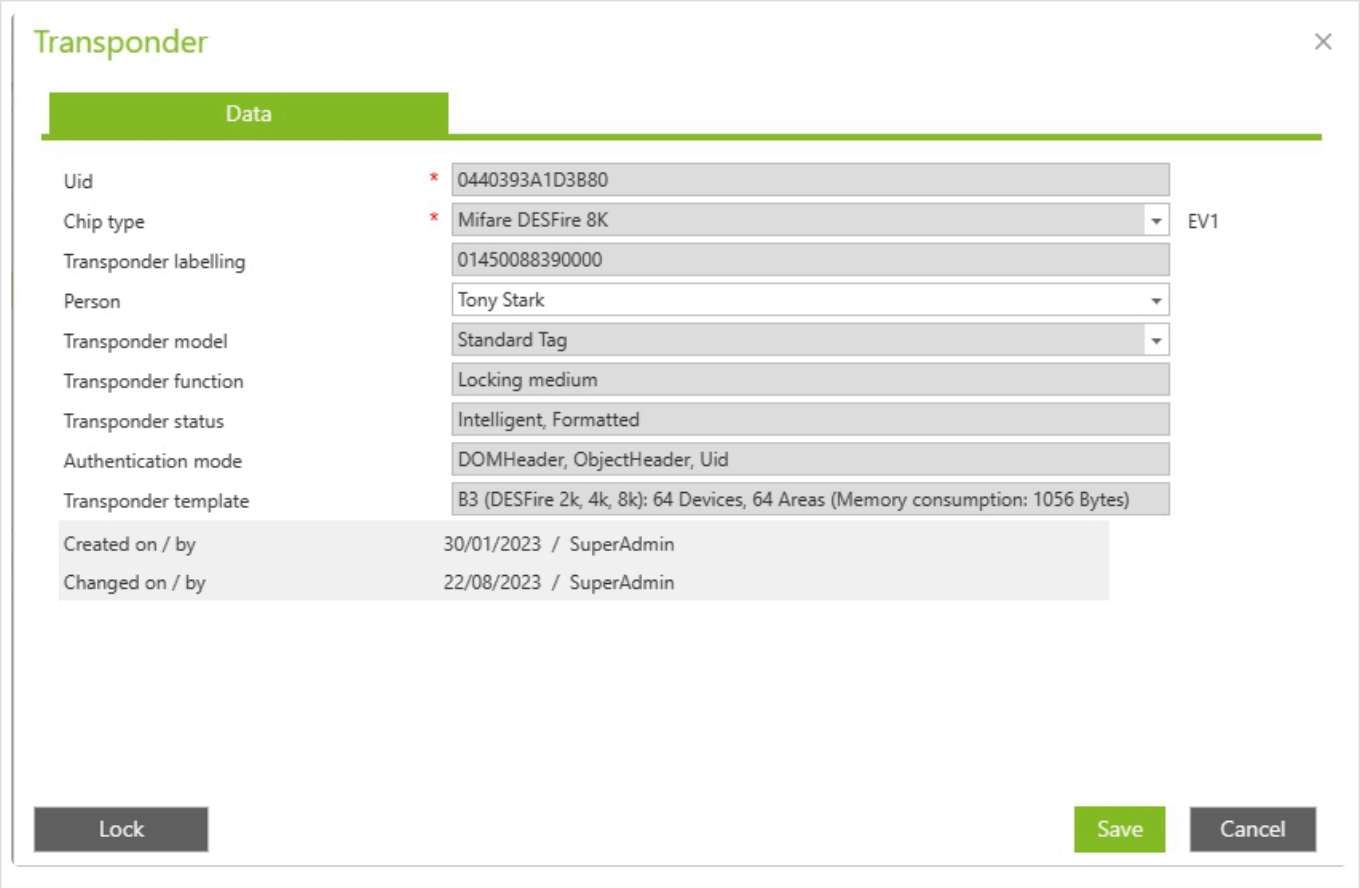
- Click on “Access control” in the navigation bar.
- Select the menu item “Transponder”.



The “Access control / Transponder” menu opens.

- Select the desired transponder

- Click on the “Edit” button

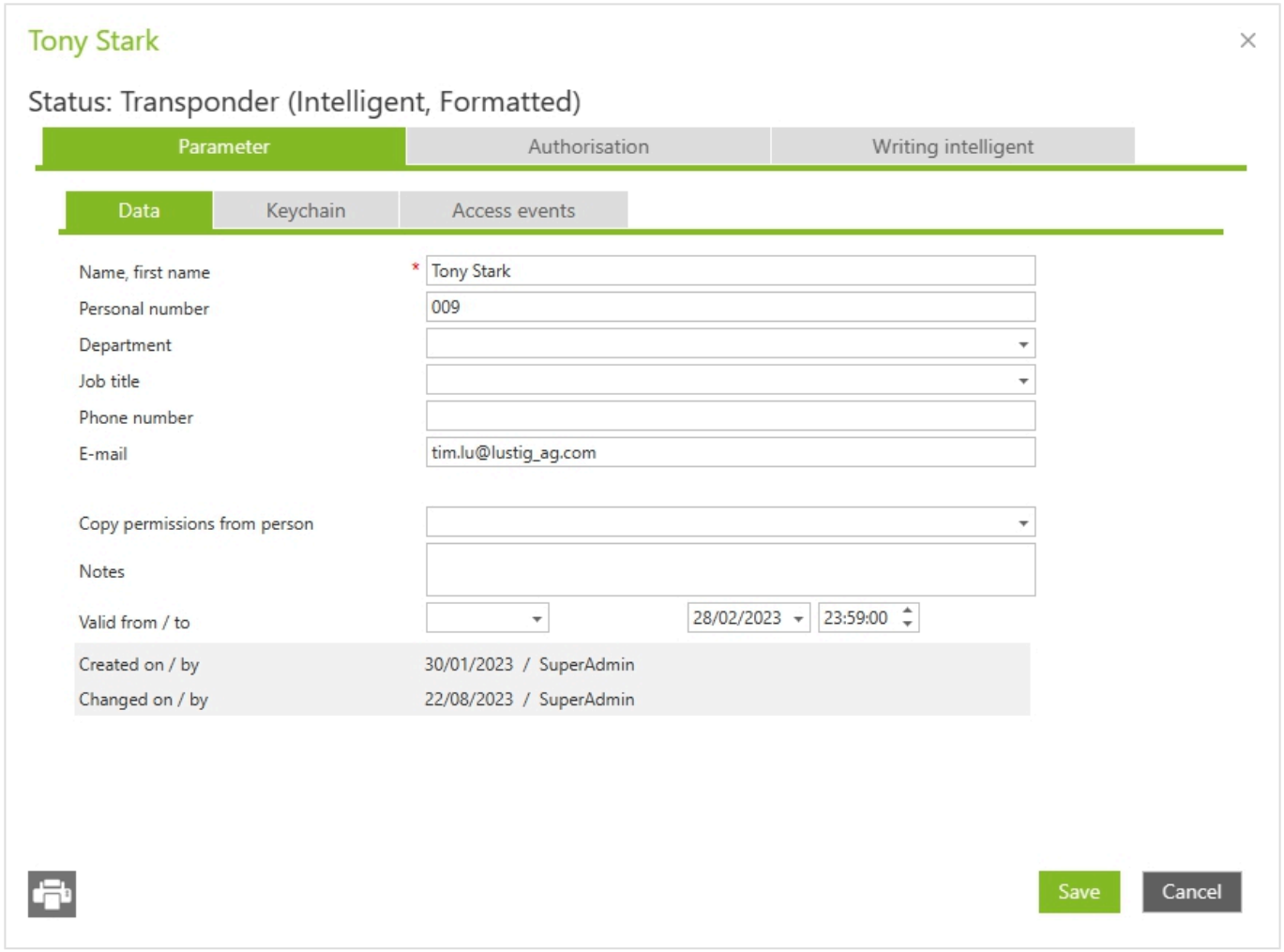


The “Transponder/Data” menu opens. The available information about the transponder is displayed.

- If desired, enter further information about the transponder.
- If you want to discard the entries, click on “Cancel”.
- To accept the entries, click on “Save”.

- To view the authorization for a transponder, switch to the “Persons “ menu item.

- Select the desired person and click on Edit



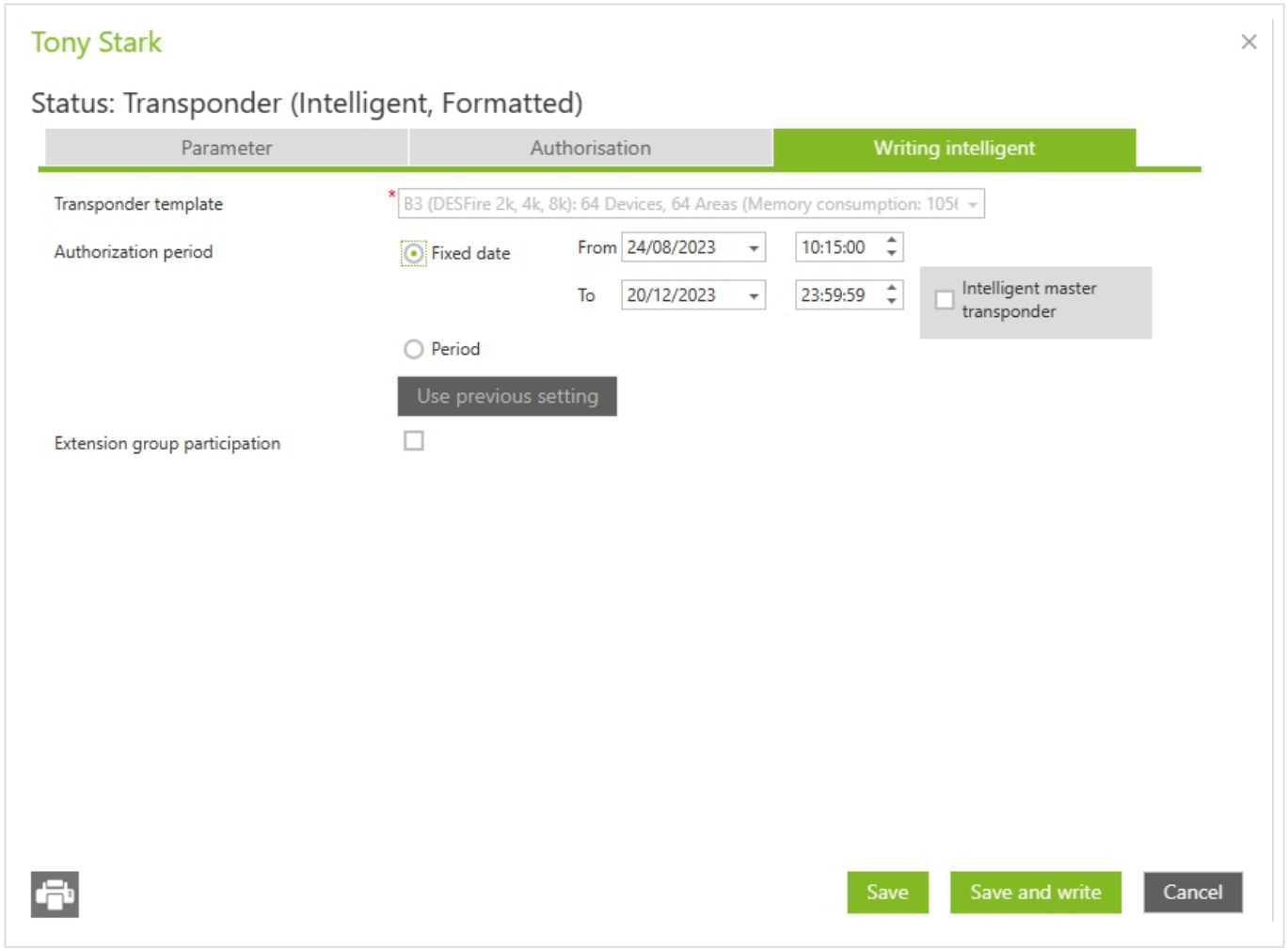
The overview of the person opens

- To view the authorization for a person, switch to the “Authorization” tab in the “Person” menu.

- To view the set authorizations of the transponder, switch to the “Authorization (read)” tab. The list of permissions assigned for the transponder will be displayed. You can sort the list.

- To remove all authorizations, click on “Remove all authorizations”.
- If you want to cancel the operation without saving, click “Cancel”.
- To apply the changes, click “Save”.

To use the transponder as a “intelligent” (DataOnCard) transponder, proceed as follows:



- Switch to the “Writing intelligent” (DataOnCard) tab.
- Select a transponder template in the “Transponder template” drop-down list, if none is selected by default.

Specify an authorization period.

- To activate the transponder for a fixed date interval, select the “Fix date” radio button.
- Select the desired date
- To activate the transponder for a period of time, select the “Period” radio button.

The period determines the duration of the authorization. It is specified as a number and as a time unit. You can specify both.

- Enter the desired number
- Select the unit of the set time in days, weeks or months
- If the transponder is to participate in the ACM terminal, check the “Extension group participation” option
- To transfer the set properties to the transponder, place it on the desk reader
- If you want to cancel the operation without saving, click on “Cancel” button

- Click on “Save and Write”

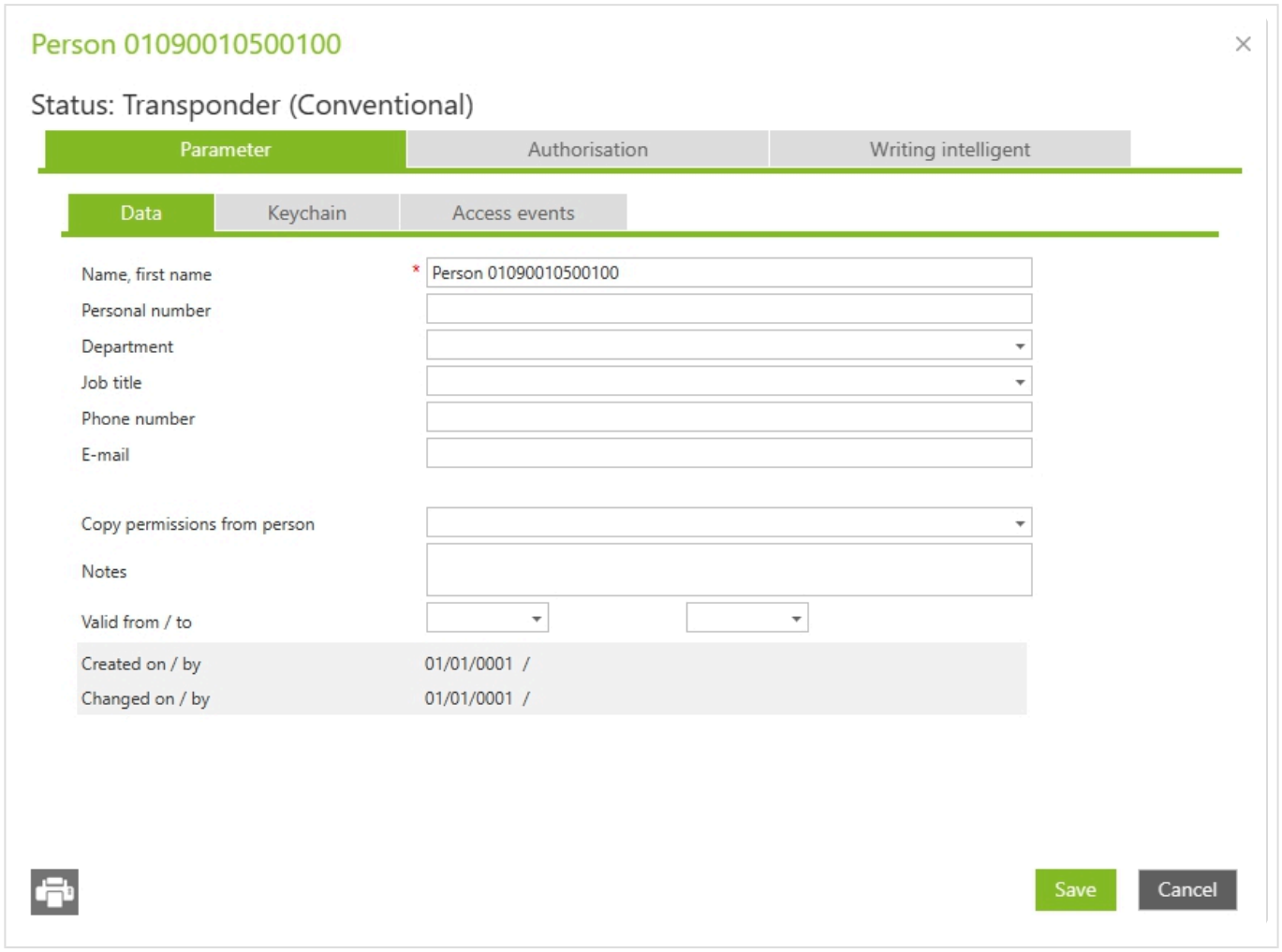
6.2.5. Read and write transponders with the desk reader

To add a transponder with the desk reader, proceed as follows:

- Place the transponder on the desk reader.
- Click on the “Desk reader” button.

> You can also open the Desk reader by pressing the *F4* shortcut key.

The transponder is read in and the corresponding person menu is displayed. If the transponder is read in for the first time, a new person is created. The transponder is automatically assigned to the person in the “keychain”.



The “Person/Parameter/Data” menu is opened. The read out data are displayed.
A temporary name for the person has been assigned automatically. To identify the person well, you should assign a unique designation.

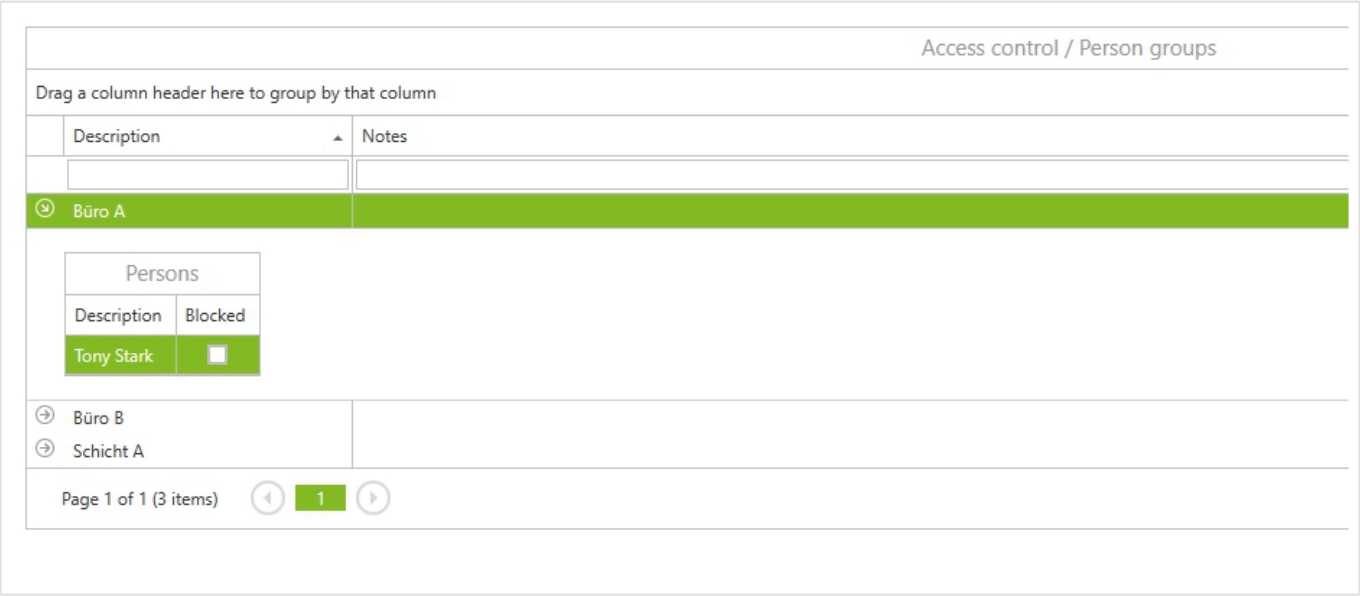
- Enter a designation
- If necessary, change more settings, see chapter Manage transponders/persons described
- If you want to cancel the process without saving, click on “Cancel”.
- Click on “Save”

6.2.6. Create group of persons

You can combine persons with identical permissions in a person group. If persons are assigned to an already existing person group, they automatically inherit the permissions of the person group.

To create a person group, proceed as follows:

- Click on “Access control” in the navigation bar.
- Select the menu item “Person groups”.



The “Access Control / Person groups” menu opens.

- Click on the “Add” button

The “Data” tab is displayed.

- Enter a name for the person group
- Enter a comment text if desired

- If you want to cancel the process without saving, click on “Cancel”.
- To create the person group, click on “Save”

6.2.7. Create schedules

The times at which you are authorized to enter a particular room are defined in daily and weekly schedules. In addition, different authorizations can be assigned for public holidays and vacations.
The daily schedules are the basis for building the weekly schedules. The weekly schedules are transferred to the devices and transponders. As a result, access is only granted at the times specified in the weekly schedules. Access is denied at all other times.

Daily schedule

A daily schedule covers a period of 24 hours. The 24 hours are divided into intervals of 15 minutes. In these intervals, access can be granted or denied during the day.
A total of 256 daily schedules are possible, three of which are predefined and cannot be changed. The remaining 253 daily schedules can be freely defined.

The following daily schedules are predefined and cannot be changed:

Plan	Explanation
Daily schedule 0:	no access (unauthorized)
Daily schedule 1:	access unlimited, special functions active, but restrictions via special functions possible
Daily schedule 255:	Unlimited access, special functions inactive. Via the weekly schedule 255 you can define a so-called fire department transponder. With this transponder, access is always possible.

Weekly schedule

On the basis of the daily schedules, the weekly schedule is compiled. Here you can either assign a daily schedule to each weekday or make an assignment over time periods:

- Monday to Friday
- Saturday + Sunday
- Monday to Sunday

In addition to the weekdays Monday to Sunday, 3 special days (SD 1 to SD 3) are available. You can use the special days, for example, for company vacations or public holidays on which different authorizations apply.

You can enter public holidays and vacation dates in the system and assign them to a state/province and one of the three special days. In the weekly schedules, you can then assign the desired daily schedule for the special days. For example, access can be denied on a holiday if that holiday falls on a weekday when access would otherwise be possible.

The weekly schedules only represent the time-based division of access authorizations, regardless of whether these are later used for areas, devices or transponders. Thus, once a weekly schedule is created, it can be used for one area. At the same time, it can be assigned to a device in another area. Similarly, a daily schedule can be assigned to Saturday in one weekly schedule, for example, and at the same time to a special day for holidays in another weekly schedule.
As with the daily schedules, a total of 256 week plans are available, three of which are predefined and cannot be changed.

Plan	Explanation
Weekly schedule 0:	no access (unauthorized)
Weekly schedule 1:	access unlimited, special functions active, but restrictions via special functions possible
Weekly schedule 255:	Unlimited access, special functions inactive. Via the weekly schedule 255 you can define a so-called fire department transponder. With this transponder, access is always possible.

In addition, special functions can be set up via weekly schedules:

Special function	Explanation
Permanently Open	The device automatically switches to permanently open mode within the selected weekly schedule.
Permanently Closed	The device automatically switches to permanently closed mode within the selected weekly schedule.
Office function (Temporary release)	By showing an authorized transponder twice, the device is set to release mode or the release mode is cancelled. After the weekly schedule has expired, the release status is also canceled.
Access repeat blocking	The access repeat blocking function is only active within the selected weekly schedule. The access repeat block function is only available with the AccessManager HiSec.
Multi User Mode	The Multi User Mode function is only active within the selected weekly schedule. The Multi User Mode function is only available with the LoQ.

The authorizations assigned for an area via weekly schedules are inherited to the sub-area as an area weekly schedule or to the device as a device weekly schedule when a sub-area or new device is created.
If a different weekly schedule than the inherited one is required, then the inheritance can be interrupted and a different weekly schedule can be assigned. If the inheritance is interrupted for a sub-area, the

newly defined weekly schedule is inherited by all lower elements of the hierarchy. That is, subordinate sub-areas and devices that have inherited the weekly schedule from the parent sub-area. Lower-level elements for which the inheritance was interrupted and for which a weekly schedule was already directly defined retain this weekly schedule. For example, when a store’s hours change, employee access times can be adjusted by assigning a new weekly schedule to the area or sub-area through which the store is managed, while extended access times for the store manager are retained.

The following sections provide information on creating daily and weekly schedules and defining vacations and holidays in the system.

To do this, proceed in the following order:

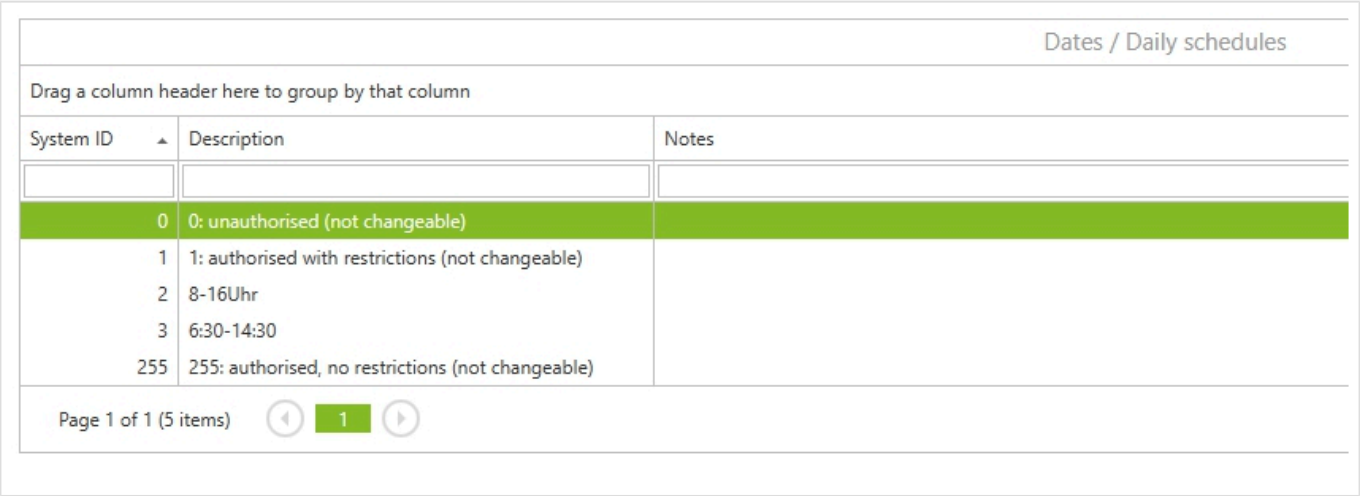
- First create a daily schedule or several daily schedules.
- Then create a weekly schedule
- Assign the desired daily schedules to the weekly schedule
- Define the desired holidays and vacations in the system

6.2.7.1. Create daily schedule

Create daily schedules

To create a daily schedule, proceed as follows:

- Click on “Dates” in the navigation bar.
- Select the “Daily schedules” menu item.



The “Dates/Daily schedules” menu will open.

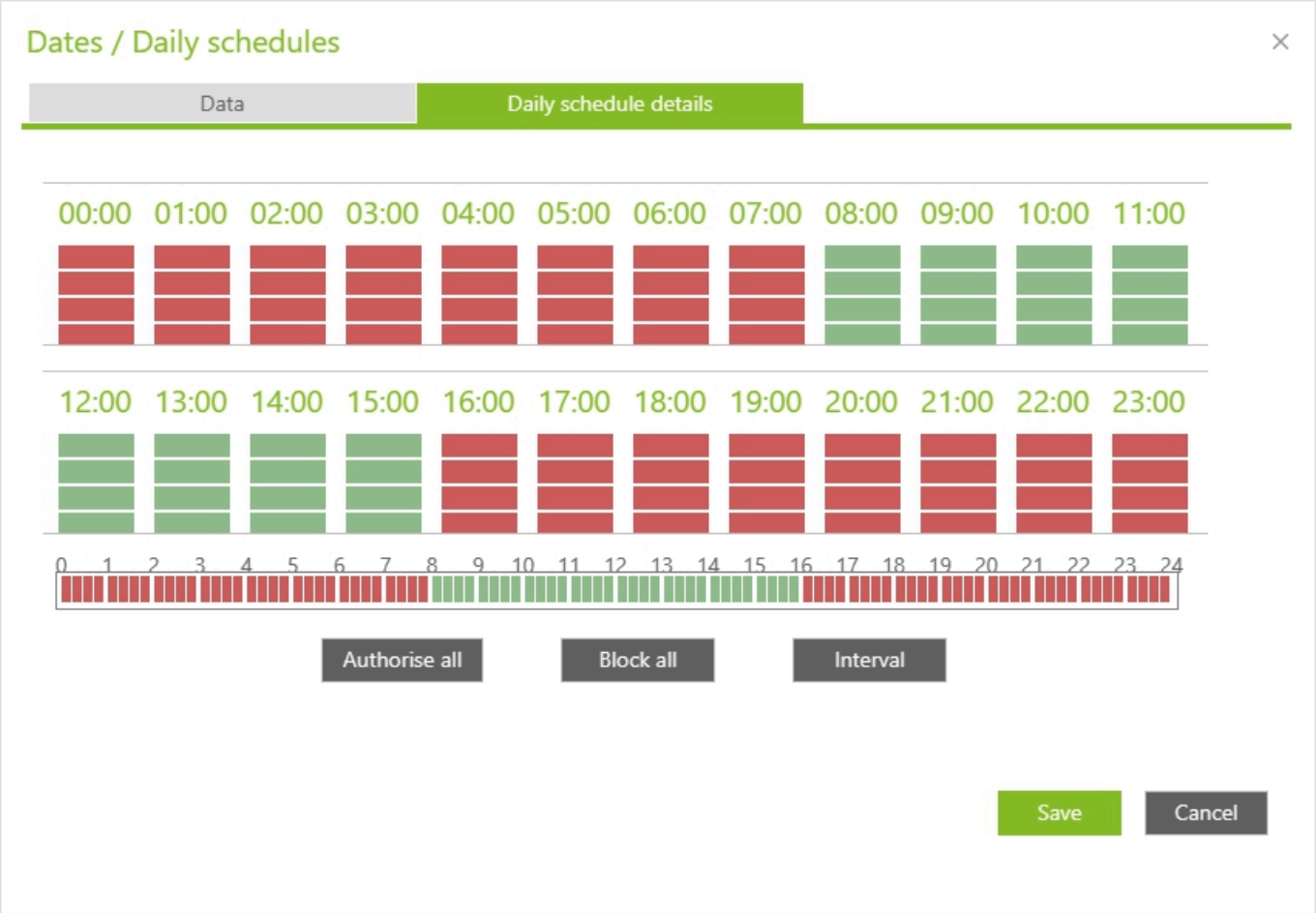
- Click on the “Add” button.

The “Dates/Daily schedules” sub-menu opens. The “Data” tab is displayed.

The “System ID” field is automatically filled in by the system. Do not enter any data here.

- Enter a unique name for the new daily schedule.
- Enter a comment text if desired
- If you want to cancel the operation without saving, click on “Cancel”.

- Switch to the “Daily schedule details” tab.



Daily schedule Details tab will be displayed.

An hourly representation and a daily overview are displayed. In these displays, each hour is divided into blocks. Each block is a quarter hour interval. If a block is marked red, there is no authorization in that interval. If a block is marked green, there is an authorization in this interval. You can also mark all blocks as “authorized” or as “blocked”.

- To lock all blocks of a daily schedule, click on the button “Block all”.
- To unlock all blocks of a daily schedule, click the “Authorized all” button.
- To change the current state for a single block, click on the block’s representation.

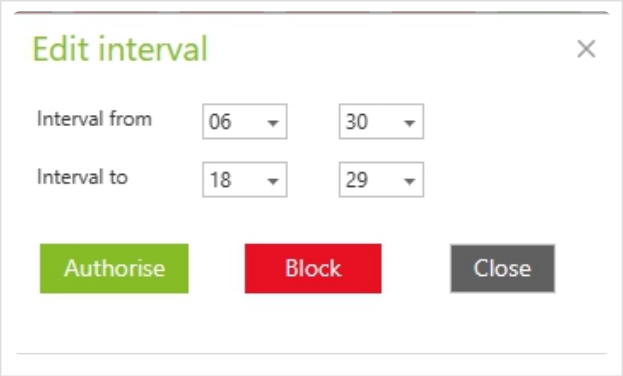
The color of the block will change.

A Daily Schedule can contain a maximum of 4 time intervals.

You can also edit all blocks within a time interval.

For example, if you want to directly set a time interval between 08:00 and 16:00, proceed as follows:

- Click on the “Interval” button.



The “Edit Interval” menu will open.

- Set the time span of the interval by clicking the drop-down menus and selecting the entries from the list.
- Click the “Authorize” button so that the selected time interval is marked as an authorization.
- The “Interval to” is specified as 14, 29, 44, 59. This means that the interval is authorized until XXh : 14/29/44/59min : 59s.

All other blocks remain marked in red. You can also use this function in the opposite way.

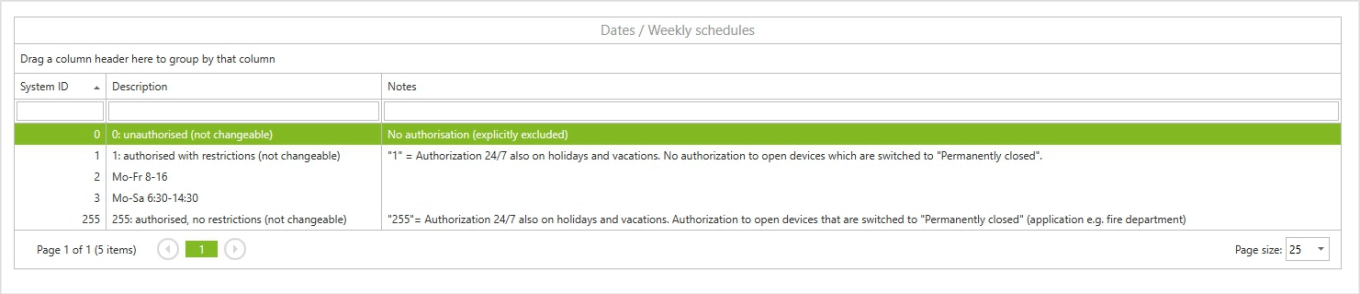
- To lock all blocks of the selected interval, click on the “Block” button.
- If you want to cancel the operation, click on “Cancel”.

- Click on “Save”

6.2.7.2. Create weekly schedules

To create a new weekly schedule, proceed as follows:

- Click on “Dates” in the navigation bar.
- Select the menu item “Weekly schedules”.



- Click on the “Add” button

The “Dates/Weekly schedules” tab “Data” menu will open.

The system ID for the weekly schedule is generated automatically. Do not enter anything in the “System ID” field.

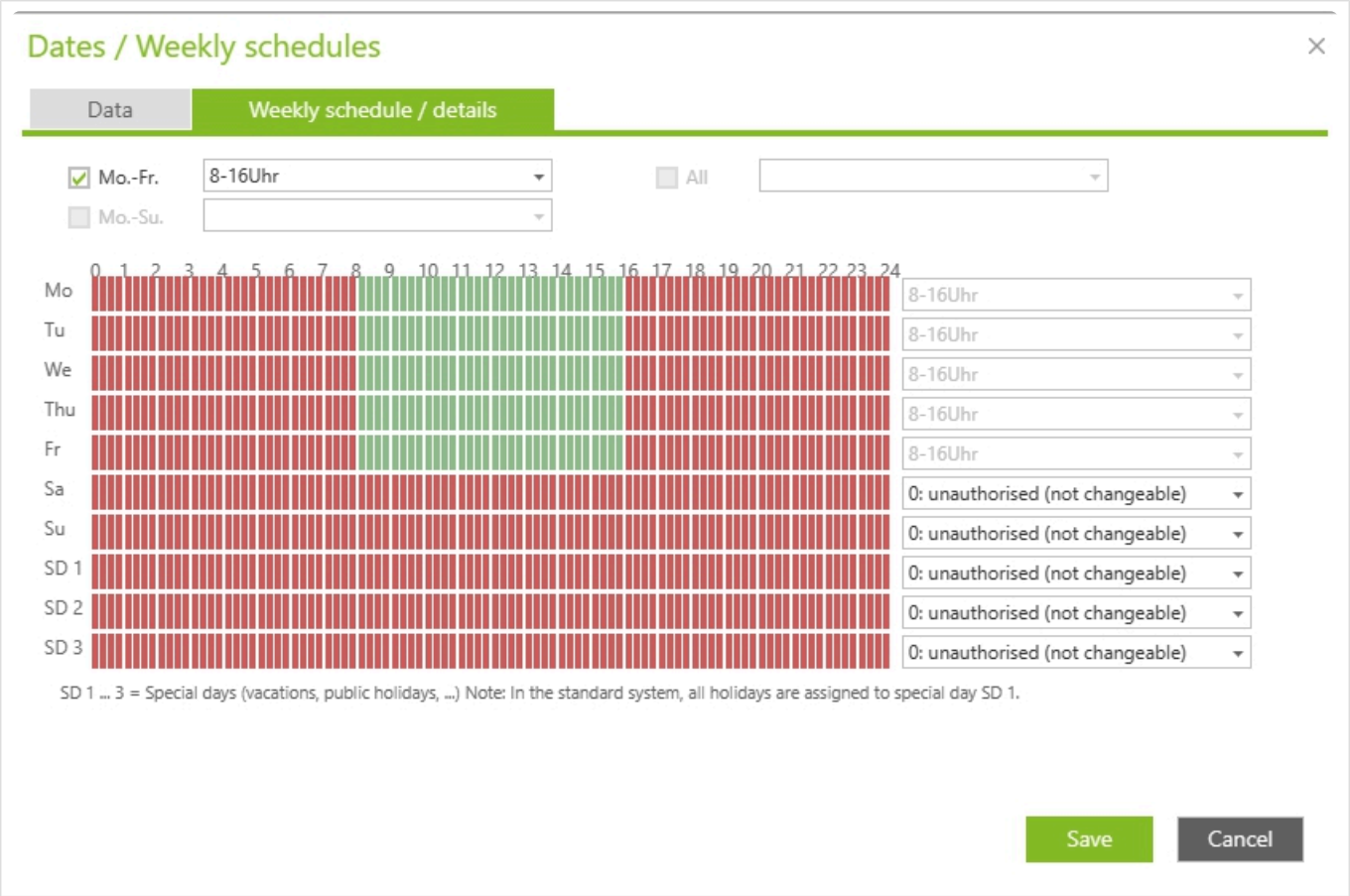
- Enter the desired name of the weekly schedule in the “Name” field.
- Enter a remark text if desired.
- If you want to cancel the operation without saving, click on “Cancel”.

You must now assign one or more daily schedules to the weekly schedule.

- Switch to the “Weekly schedule details” tab.

> In order to assign self-created daily schedules to a weekly schedule, you must create them beforehand. The creation of daily schedules is described in the previous section.

This is how you can assign individual daily schedules to a weekly schedule:



The overview of the current settings is displayed.
With the drop-down menus to the right of each weekday, you can assign a daily schedule to the weekdays.

- Select a daily schedule in the desired drop-down menu.
  The overview will be updated.

You can also assign a daily schedule to multiple days in a weekly schedule. Alternatively, you can select the following options:

- Option “Mo.-Su.”: all days except “special days”.
- Option “Mo.-Fr.”: all weekdays
- Option “All”: all days, including those defined as special days.

Proceed as follows:

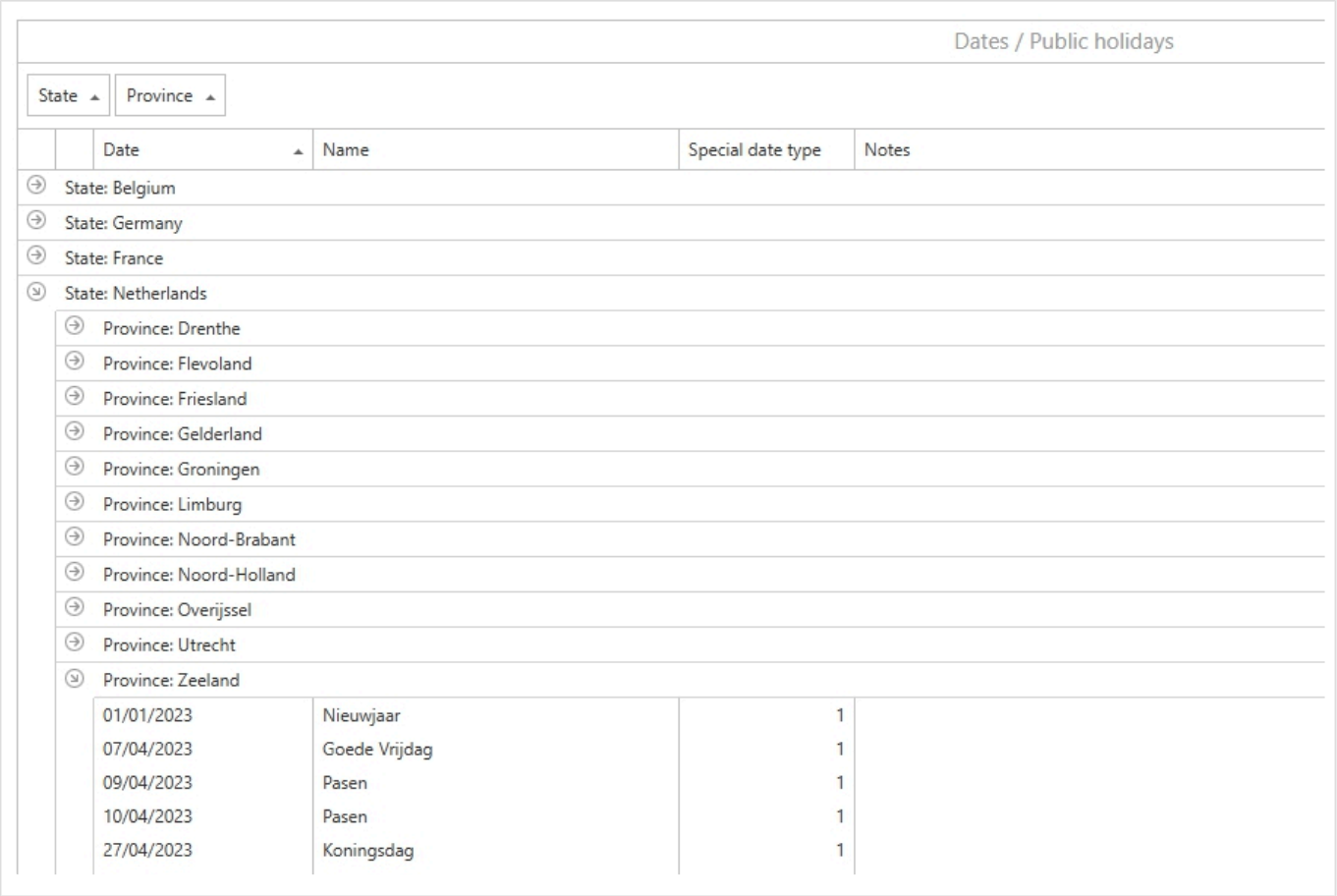
- Place a check mark in the desired option field.
- Click on the drop-down menu located to the right of each time period
- Select the desired day schedule from the list
- If you want to cancel the operation without saving, click on “Cancel”].

- Click on “Save”

6.2.7.3. Create public holidays

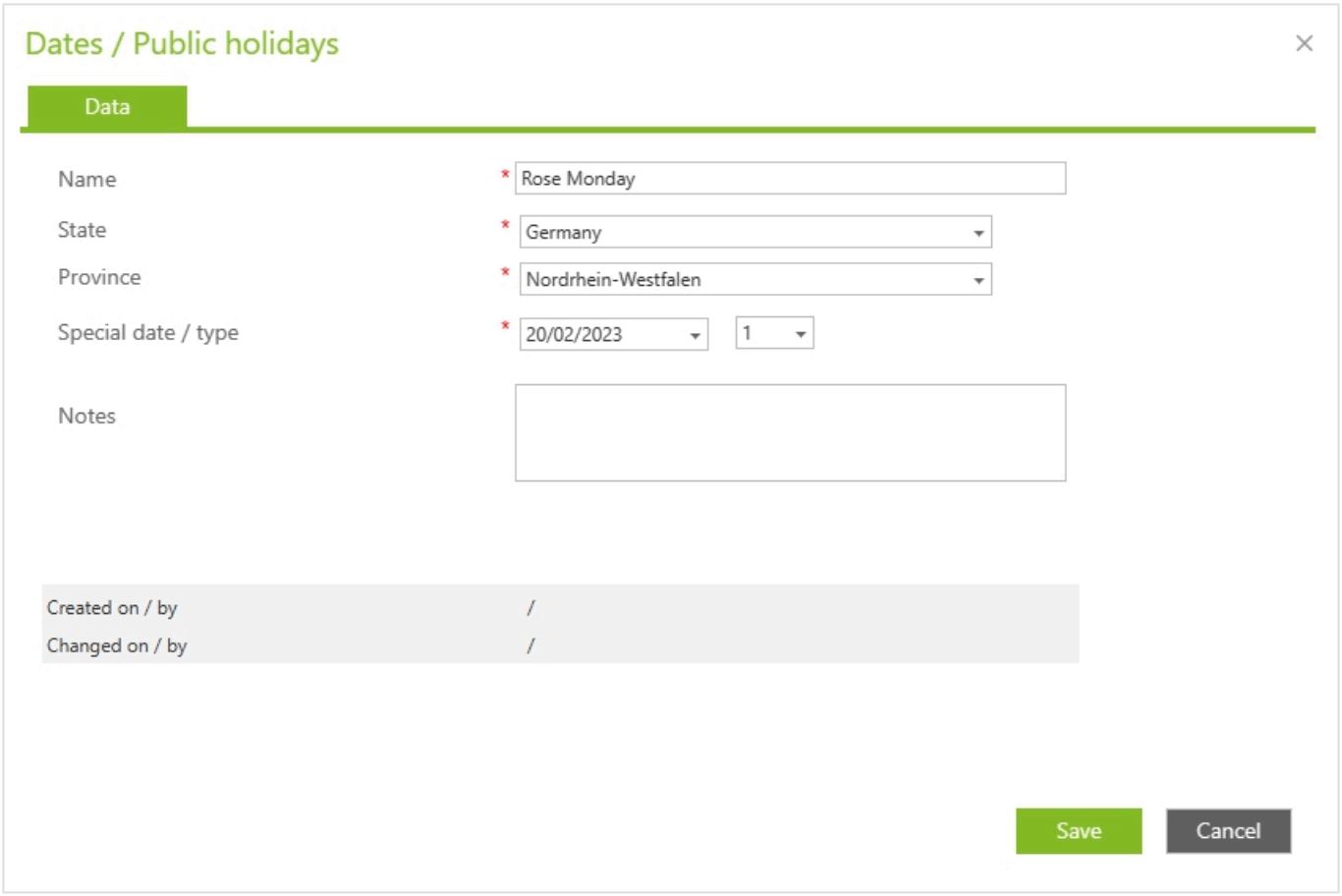
To create data for a holiday, proceed as follows:

- Click on “Dates” in the navigation bar.
- Select the menu item “Public holidays”.



The “Dates/Public holidays” menu will open.

- Click on the “Add” button



The “Data” tab will be displayed.

- Enter a descriptive name for the holiday definition.
- Select the desired state from the “State” drop-down menu.
- In the “State” drop-down menu, select the desired state.
- In the “Special date” drop-down menu, select the desired date.
- In the “Type” drop-down menu, select the desired type.
- Enter a comment text if desired.

- Click on “Save”

6.2.7.4. Create vacations

To create dates for vacations, proceed as follows:

- Click on “Dates” in the navigation bar.
- Select the menu item “Vacations”

The “Dates/Vacations” menu will open.

- Click on the “Add” button

The “Data” tab will be displayed.

- Enter a meaningful name for the definition of the vacation.
- Select the desired state in the “State” drop-down menu
- Enter the desired dates in the drop-down menus “Vacation start” and “Vacation end
- Enter the school year if desired
- Select the desired type in the drop-down menu “Special date type
- Enter a comment text if desired
- If you want to cancel the operation without saving, click on “Cancel”.

- Click on “Save”

6.2.8. Create special cards

Write Mastercard

With this function you can save all object keys of the database to an undescribed “Mastercard”. You can then use the Mastercard to manually create new devices and connect (“couple”) them to the system.

To couple the devices, you must use the “ENiQ Device Management Software” program. (See chapter Coupling and programming devices)

> ! Keep the Mastercard protected from unauthorized access.

The Mastercard provides full access to the system. All devices and settings can be manipulated.

To create a Mastercard, do the following:

- Click on “System” in the navigation bar.
- Select the menu item “Write Mastercard”.
- Place an unwritten Mastercard on the desk reader.

The Mastercard is written.

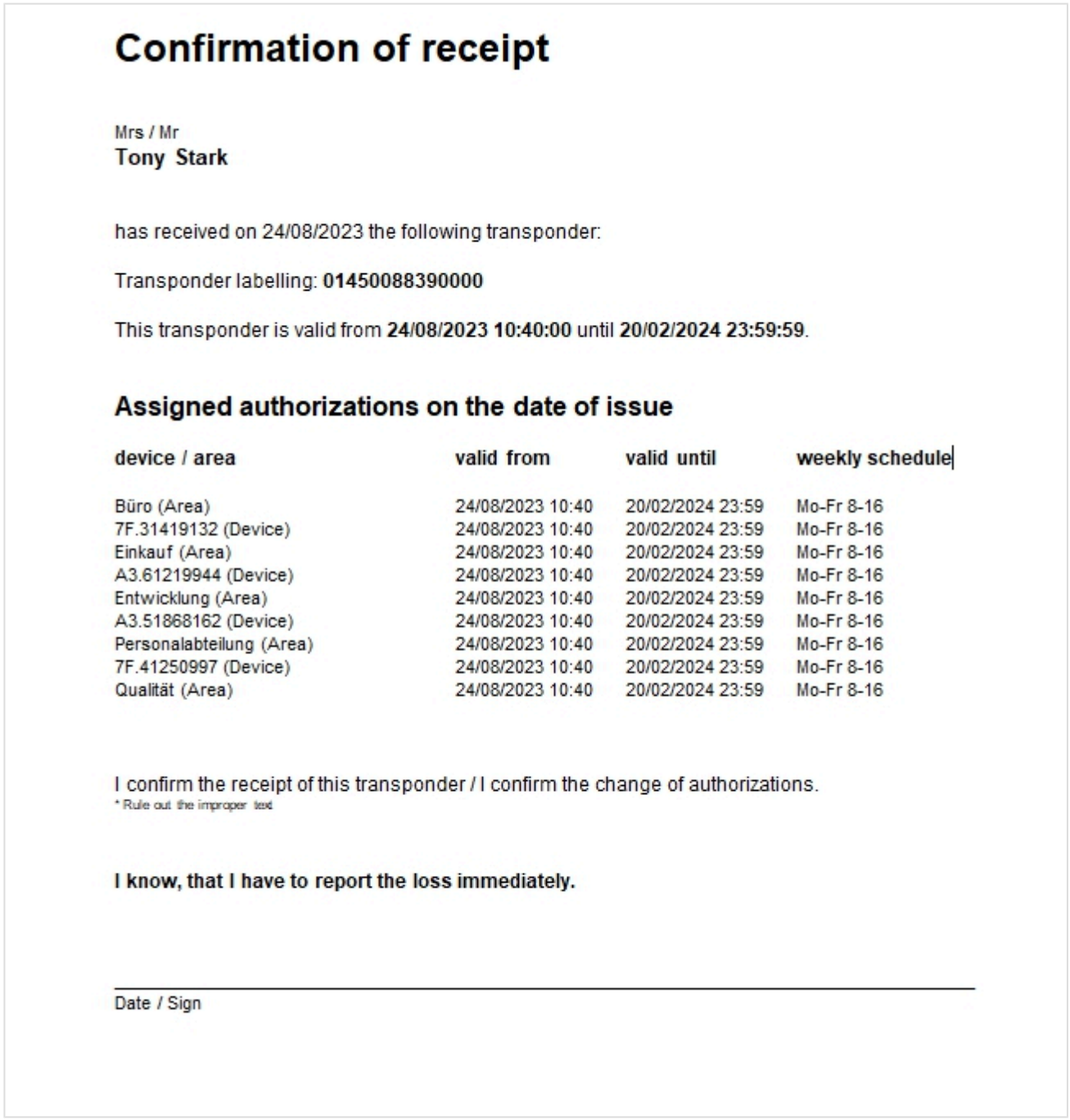
Further special cards

All other special cards are recorded in the same way as personal transponders.
Please refer to the chapter “Read and write transponders with the desk reader”.

6.2.9. Receipt printing

A listing of the information for this person

- A list of authorization for this person
- Authorization period with weekly schedule, if applicable
- Transponder labeling



Confirmation of receipt

Mrs / Mr
Tony Stark

has received on 24/08/2023 the following transponder:

Transponder labelling: **01450088390000**

This transponder is valid from **24/08/2023 10:40:00** until **20/02/2024 23:59:59**.

Assigned authorizations on the date of issue

device / area	valid from	valid until	weekly schedule
Büro (Area)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
7F.31419132 (Device)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
Einkauf (Area)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
A3.61219944 (Device)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
Entwicklung (Area)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
A3.51868162 (Device)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
Personalabteilung (Area)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
7F.41250997 (Device)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16
Qualität (Area)	24/08/2023 10:40	20/02/2024 23:59	Mo-Fr 8-16

I confirm the receipt of this transponder / I confirm the change of authorizations.
* Rule out the improper text

I know, that I have to report the loss immediately.

Date / Sign

The receipt printout can be printed for the person via the receipt print button.
The receipt printout can be customized.

6.2.10. Delete transponder

To delete a transponder, proceed as follows:

- Click on “Access control” in the navigation bar.
- Select the “Transponders” menu item

The “Access control / Transponders” menu opens

- Select the transponder you want to delete
- Click on the “Delete” button

A message window opens

- If you want to delete the transponder from the system, click the “Delete” button

The transponder will be deleted from the system. In the case of intelligent (DataOnCard) systems, it is placed on the blacklist. If the transponder is used for an access attempt, access will be denied. With conventional (DataOnDevice) systems, you can create the transponder again as a new transponder in the system. In this way, you can continue to use a transponder that has been found again.

To do this, the corresponding transponder must be re-read via the desk reader and the devices reprogrammed via the Device Management software.

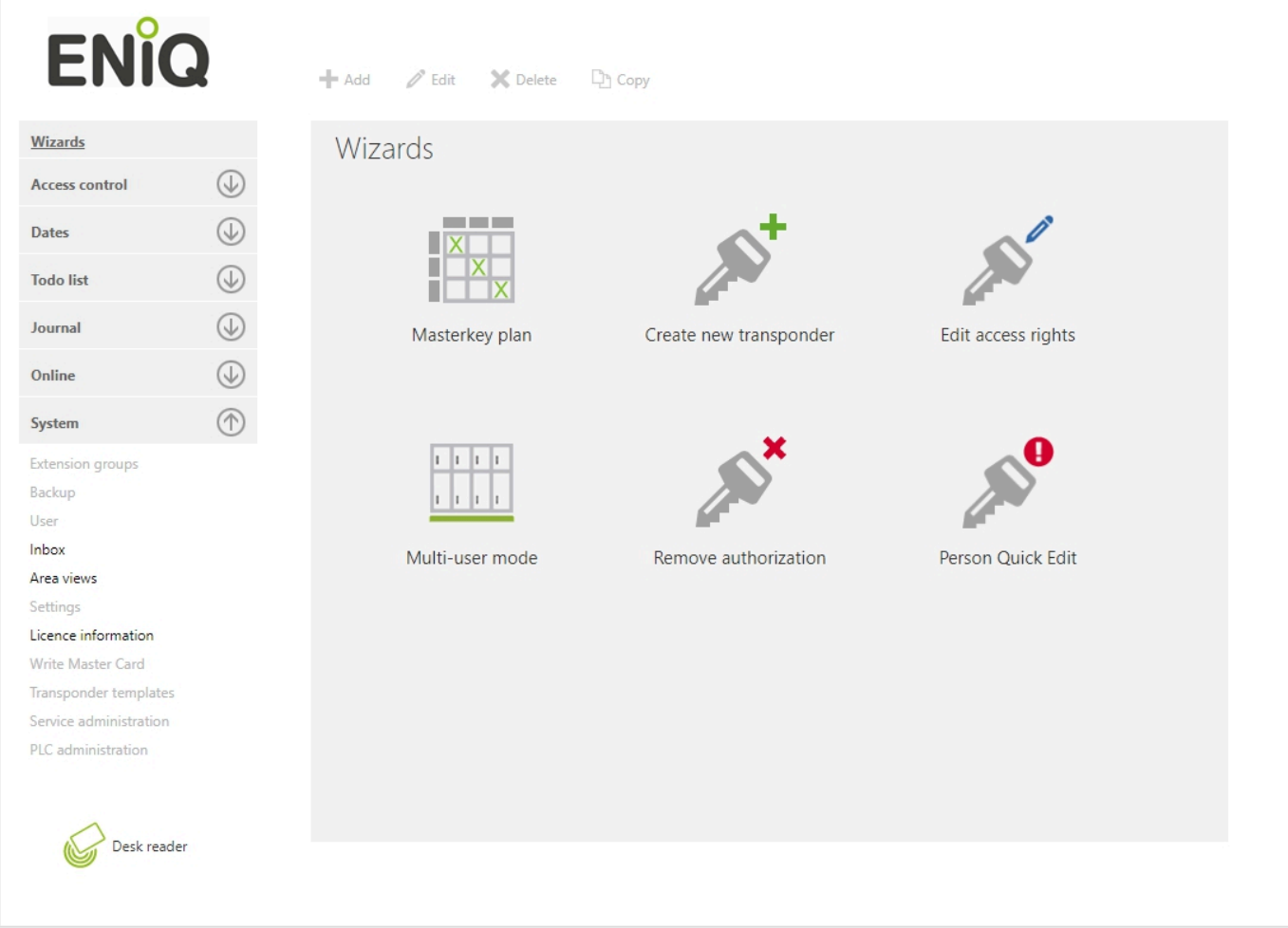
- If you do not want to delete or lock the transponder, click on the « Cancel » button.

6.2.11. Operator

The following operator roles are available:

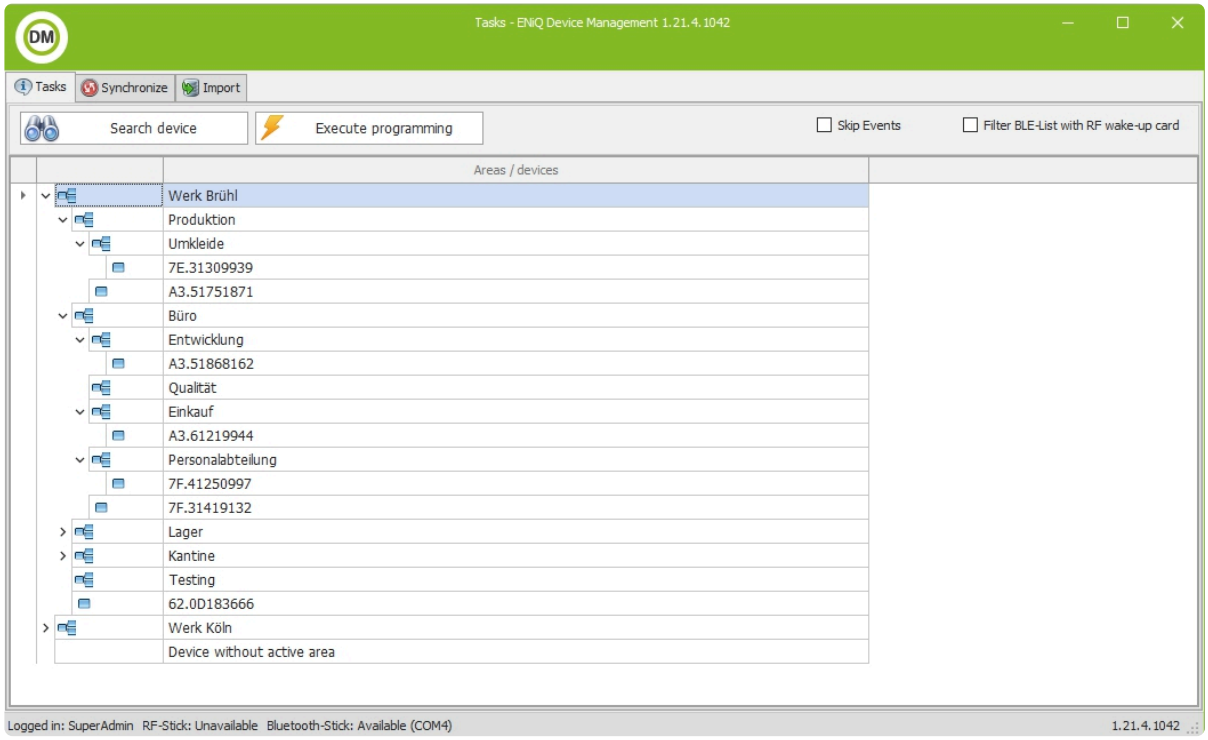
Operator role:	Functions:
Superadmin	No restrictions in the software

Operator role:	Functions:
User:	Can perform all functions in both systems except - Manage extension groups - Create backup - Create operator - Make settings - Write Mastercard - Manage transponder templates - Manage service - SPS administration

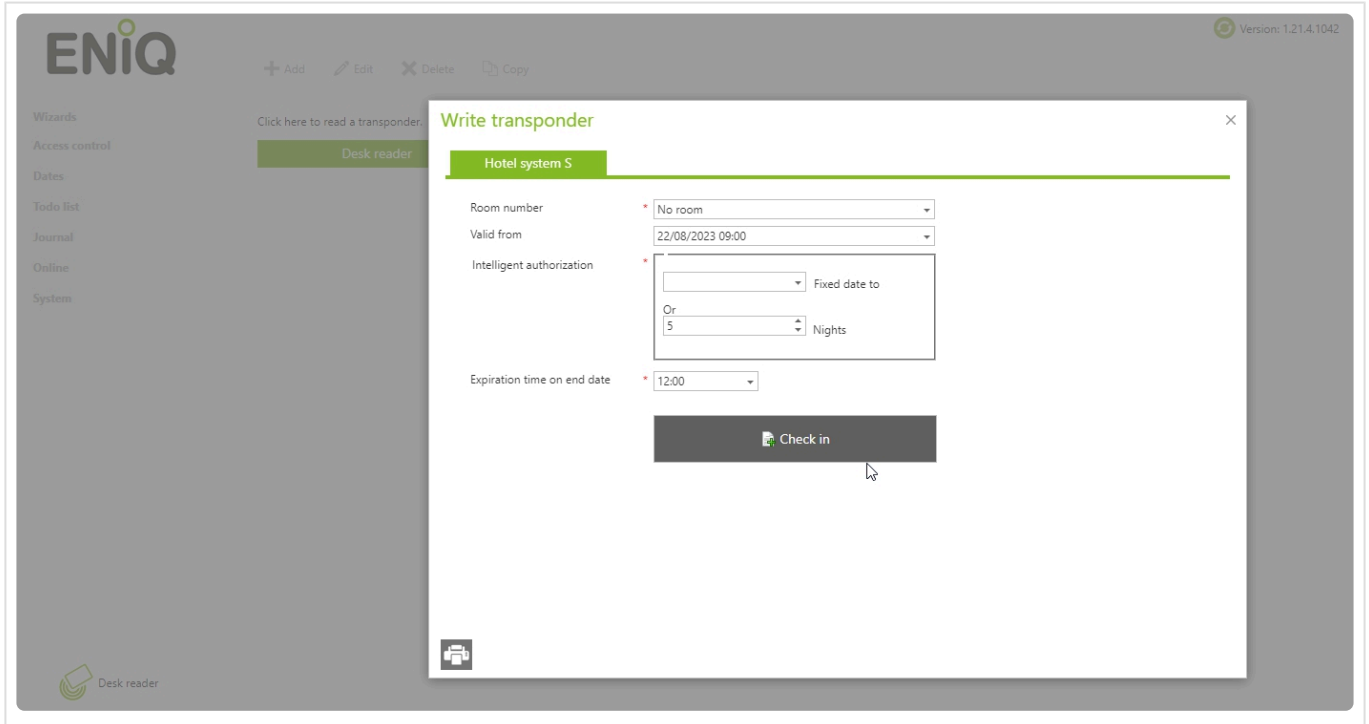


Operator role:	Functions:

Device Programmer	Can only open ENiQ Device Management or use DOM Service app - Device Programming - Synchronize database

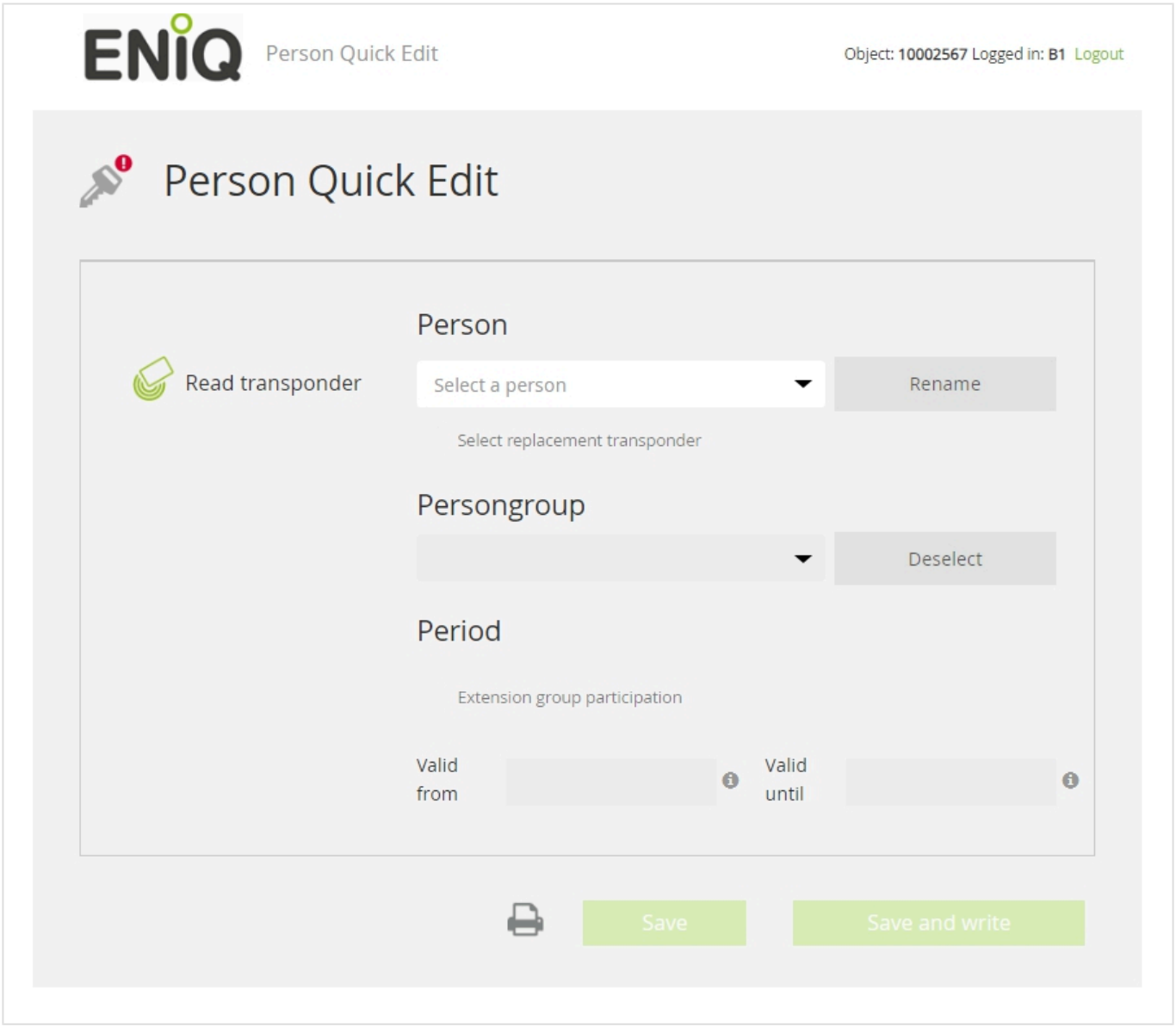


Operator role:	Functions:
Reception	Can only open ENiQ Access Management - Has only one mask in the software - Can only program transponders

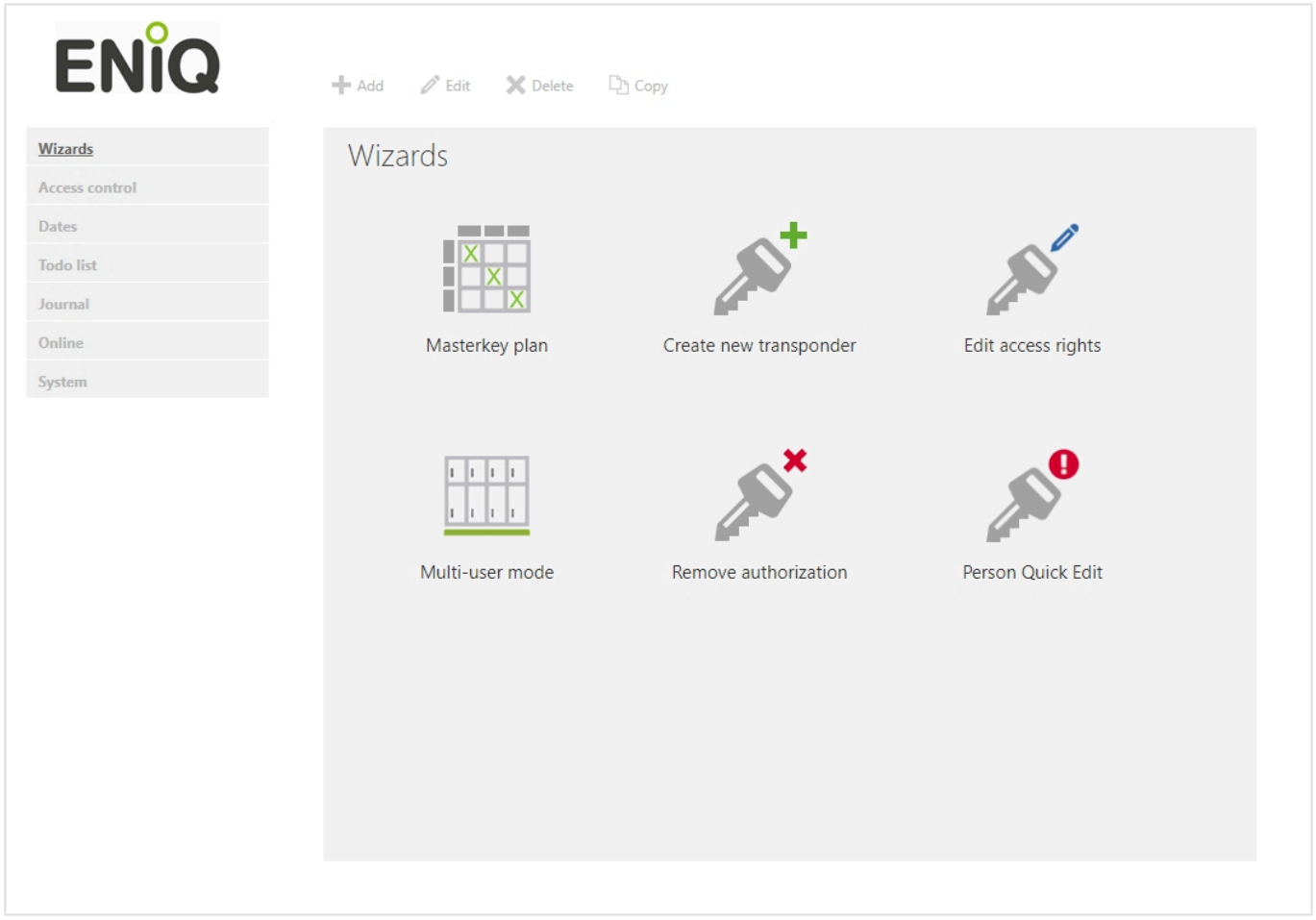


Operator role:	Functions:
Permission Administrator	Can only open ENiQ Access Management - Can authorize transponders or persons in assigned areas

Operator role:	Functions:
Person Administrator	Can only open ENiQ Access Management - Can only authorize persons via the wizard Persons Quick Edit



Operator role:	Functions:
Wizards only	Can only open ENiQ Access Management - Can edit locking plan - Can create transponders - Can edit access rights - Can manage multi-user mode - Can revoke authorizations - Can use the People Quick Edit


ENiQ
Add
Edit
Delete
Copy
Wizards
Access control
Dates
Todo list
Journal
Online
System
Wizards
Masterkey plan
Create new transponder
Edit access rights
Multi-user mode
Remove authorization
Person Quick Edit

6.2.11.1. Permission Administrator

This chapter describes the configuration and operation of the Permission Administrator role within the ENiQ Access Management Software. There is also a tutorial that shows the steps to set up an Permission Administrator.

Operators of this function are mainly large customers where sub-areas of a facility need to be managed by different people. In the following, administrators of sub-areas are referred to as Permission Administrator.

Functions
In this section the basic structure of the new functionality and its individual components are explained in more detail.

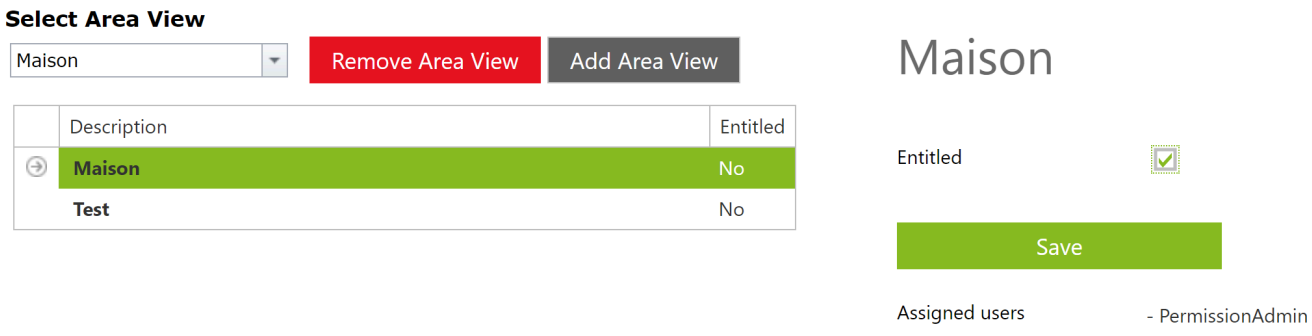
Structure

The ENiQ Access Management Software offers the possibility to create single operators with the role Permission Administrator. A Permission Administrator has the possibility to manage a sub-area of a system. In this sub-area he can assign authorizations for users. In addition, the authorizations and events associated with the sub-area can be displayed in a separate list.
To use the Permission Administrator function, a separate operator must be created. The role Permission Administrator is assigned to this operator. So-called AreaViews are used to define which areas are visible to this operator.

After the setup, the Permission Administrator can log in. A newly designed view opens in which the authorizations for the areas visible to him can be assigned. In addition, this operator can view the authorization and event lists. In these lists, however, only those areas and devices are available which have been enabled for him via the AreaView.

AreaView configuration

AreaViews can be managed via System -> AreaViews. You define the visibility of areas for Permission Administrators.

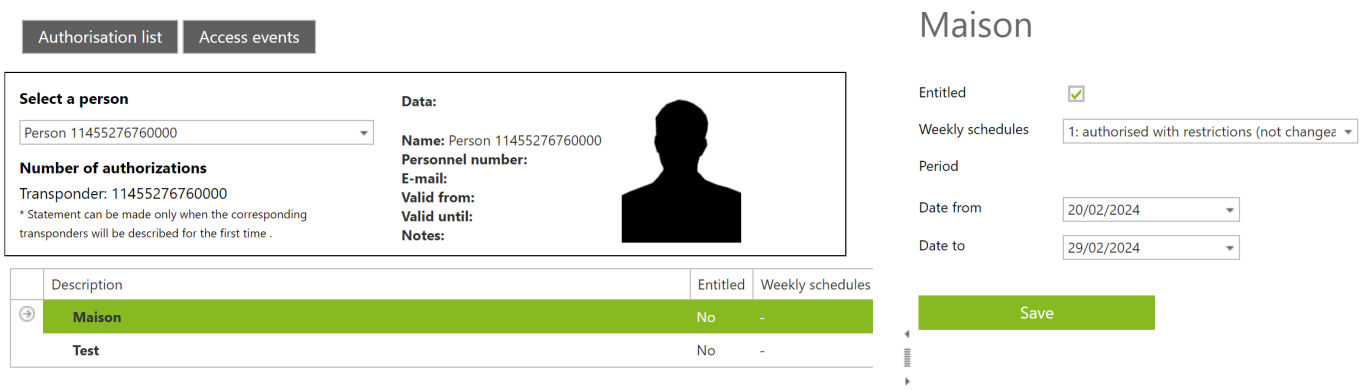


As soon as an area is marked as visible for an AreaView, all areas below it will automatically become visible as well. Explicit hiding of individual sub-areas is not possible. Individual devices cannot be

explicitly marked as visible via an AreaView either.
Exactly one AreaView can be assigned to each Permission Administrator. If no AreaView is assigned to a Permission Administrator, no areas are visible for this operator. An AreaView can be assigned to one or more Permission Administrators.
After selecting an AreaView in the upper combo box of the AreaView Configurator, the views for the respective areas appear in the area tree. In addition, the right side shows which operators are assigned to this AreaView.

Permission Administrator

The role of the Permission Administrator allows the main administrator of the system to grant individual operators access to sub-areas of the system. The Permission Administrator is only shown the part of the system that is visible to him. In addition, he can use the buttons in the upper part of the screen to access the list of authorizations and events. In these lists he is granted access to the sub-areas visible to him.



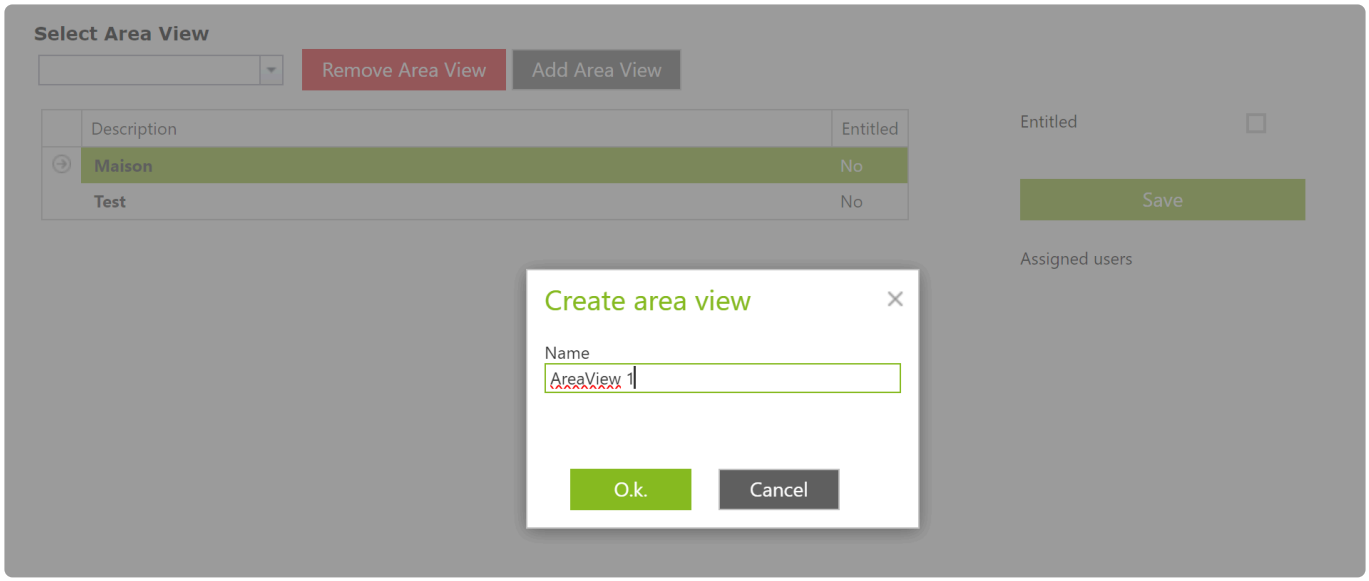
Operation
In this section, the prerequisites and operation of the function are explained in more detail with the help of a setup tutorial.

Configuration

At least one single license is required for operation.
With the first license, a standard single-user installation of the ENiQ Access Management Software is performed, so that a running ENiQ software is already fully functional on the PC and the system has been put into operation.

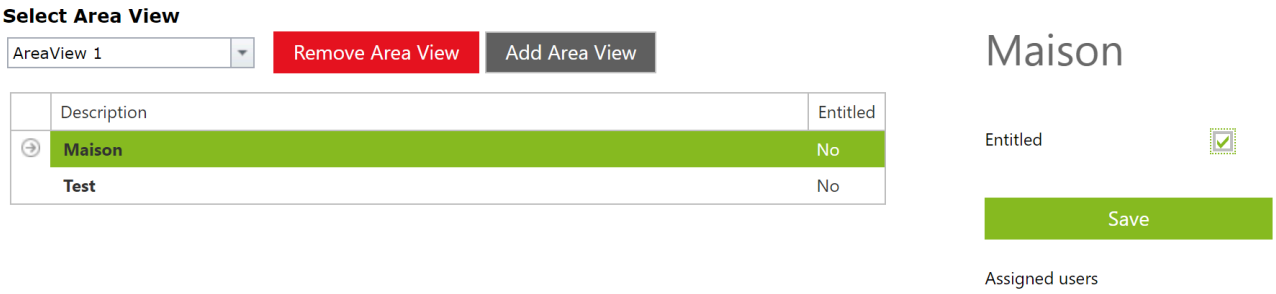
Tutorial – Setup of the Permission Administrators

Step 1 – Create AreaView: The visibility of sub-areas of the system for Permission Administrators are defined via so-called AreaViews. Via System -> AreaViews you get to the configurator of the AreaViews. Here you can create a new AreaView by clicking on Create AreaView. After that you have to enter a meaningful name for the AreaView and confirm the entry with OK.

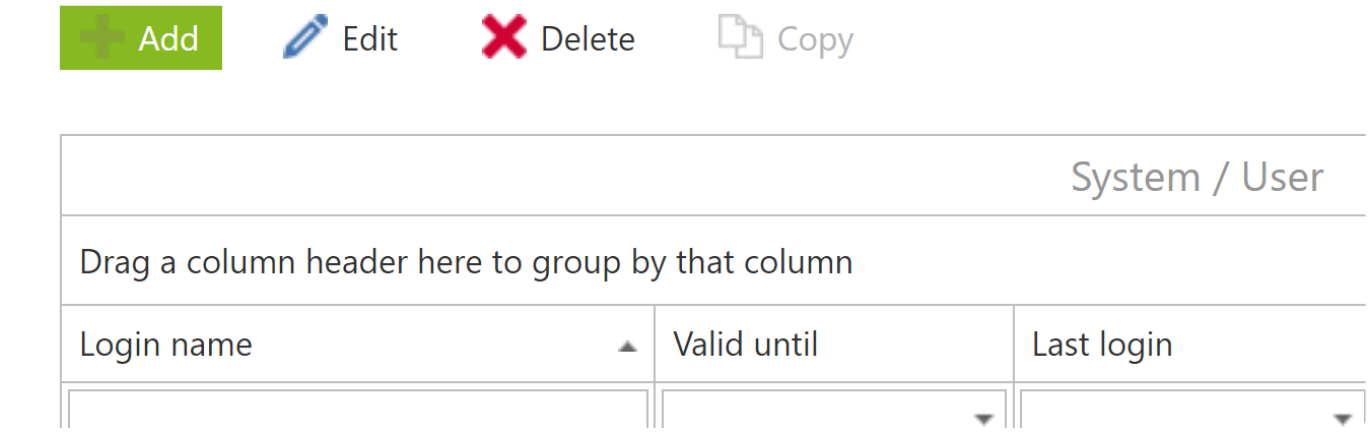


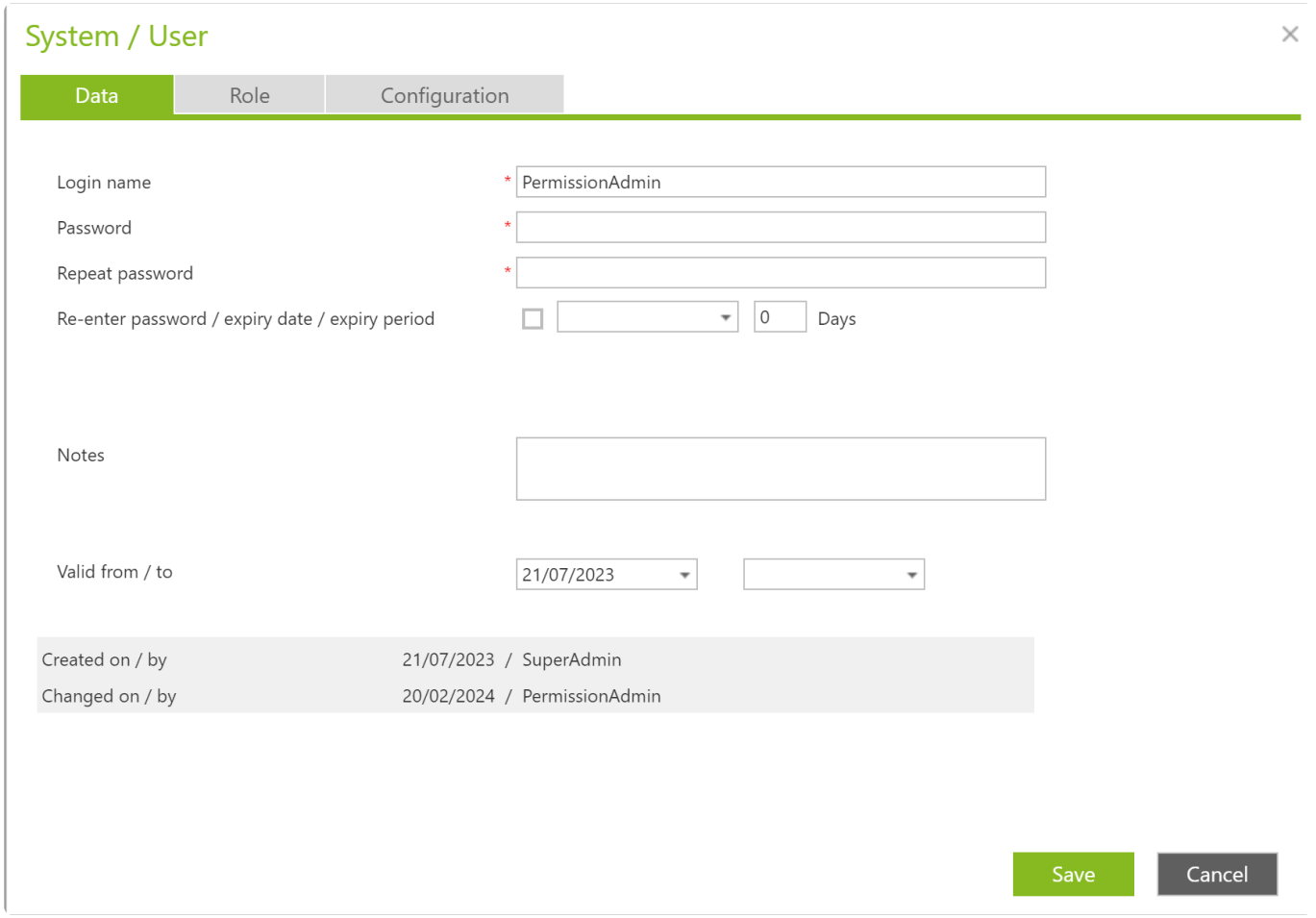
Step 2 – Define AreaView: After creating the AreaView, select the corresponding entry from the combo box in the upper area. After this is selected, you can define which sub-areas are visible for this AreaView. For this purpose, select an area from the area tree and then set the checkmark on the right side at the item Authorized.

With the button Save you can confirm your input. Repeat this step as often as you like for the respective areas. In this step you have to consider that for one operator all hierarchically subordinated areas will be visible as well. In the case example, for example, area B would be visible as soon as area A is switched as visible. The assignment of visibility for individual devices is not possible here.

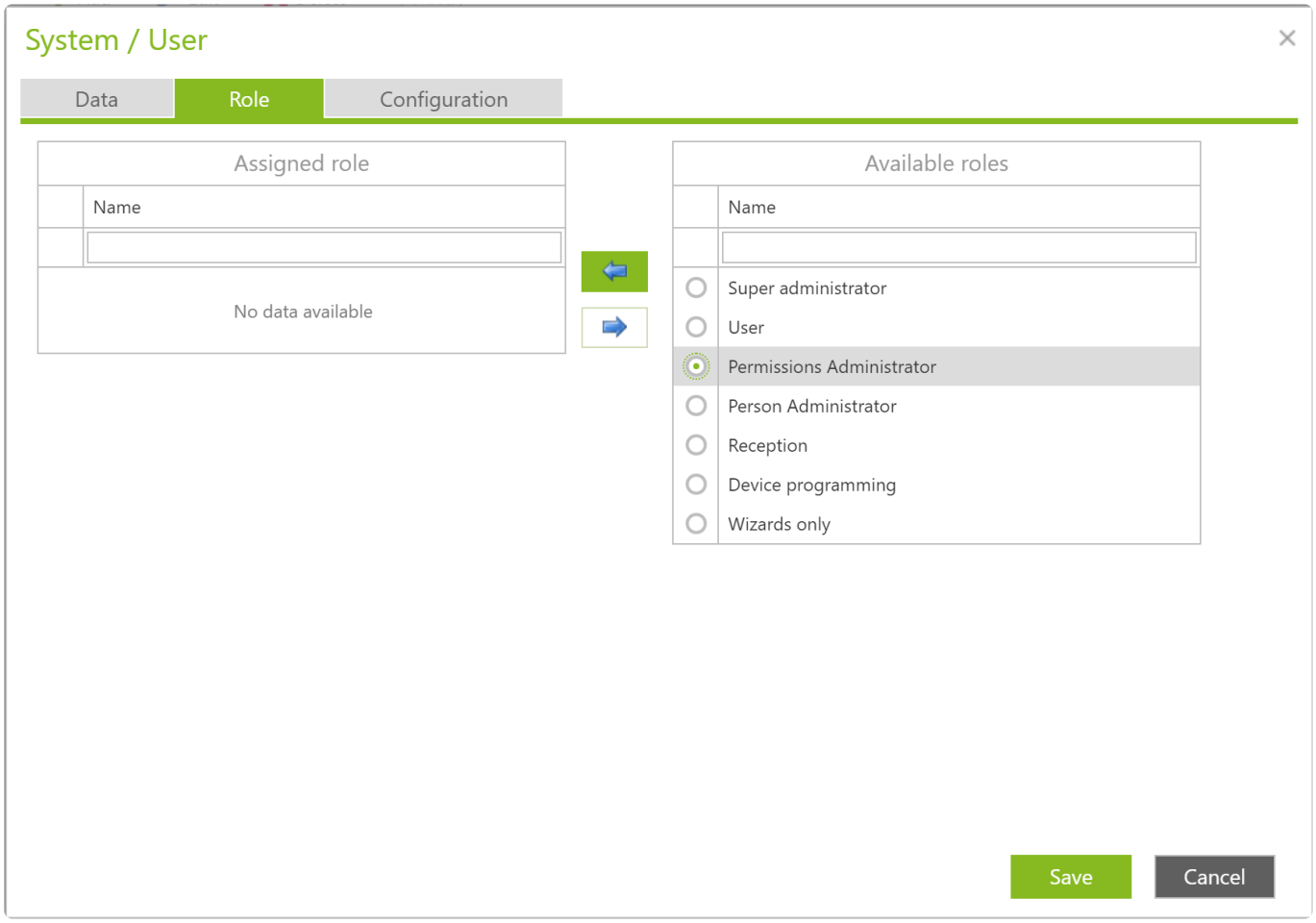


Step 3 – Create operator: If you have not done so yet, you must now create a new operator. Navigate to System -> Operator and click on the Add button at the top. Assign at least a name and password.

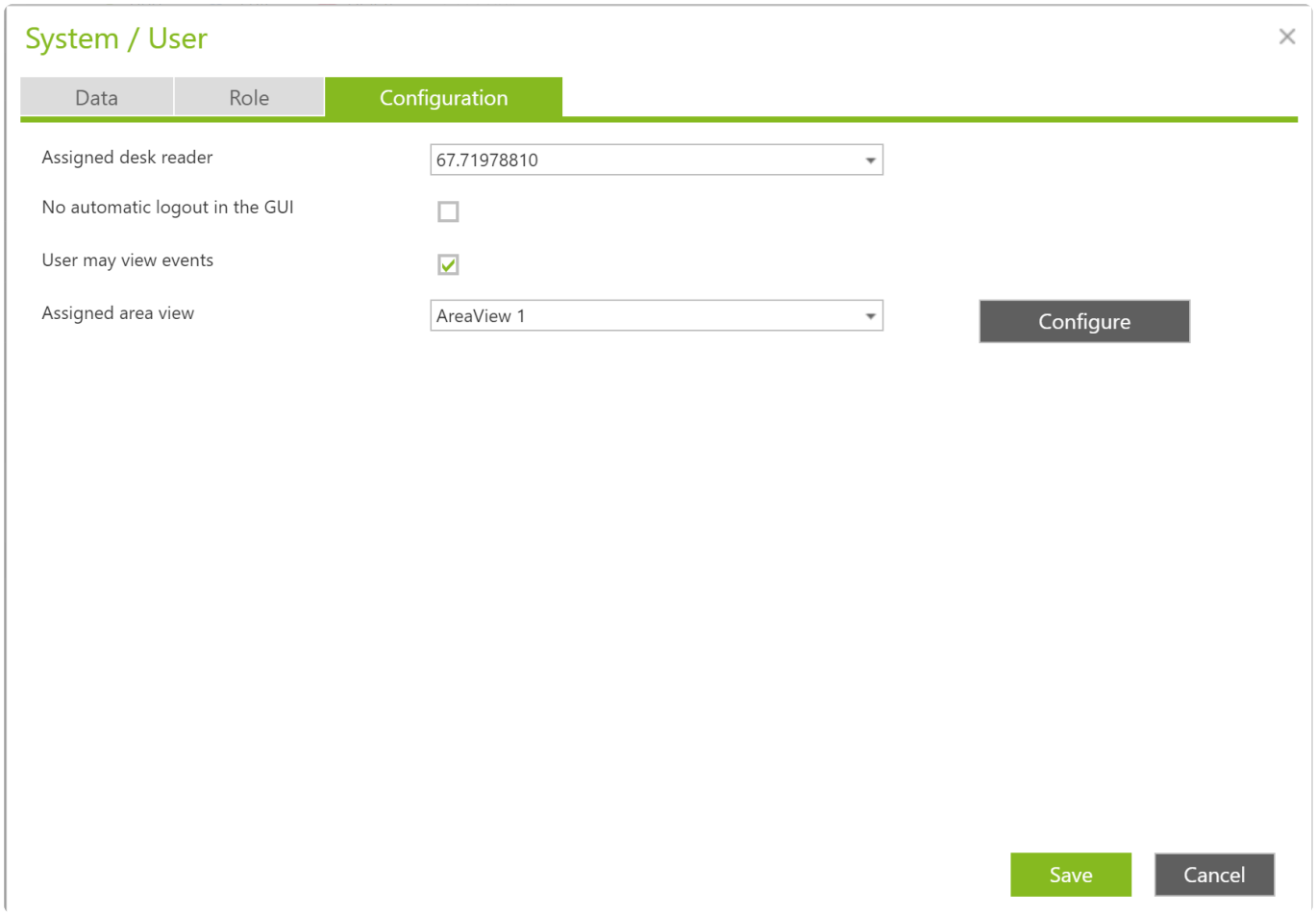




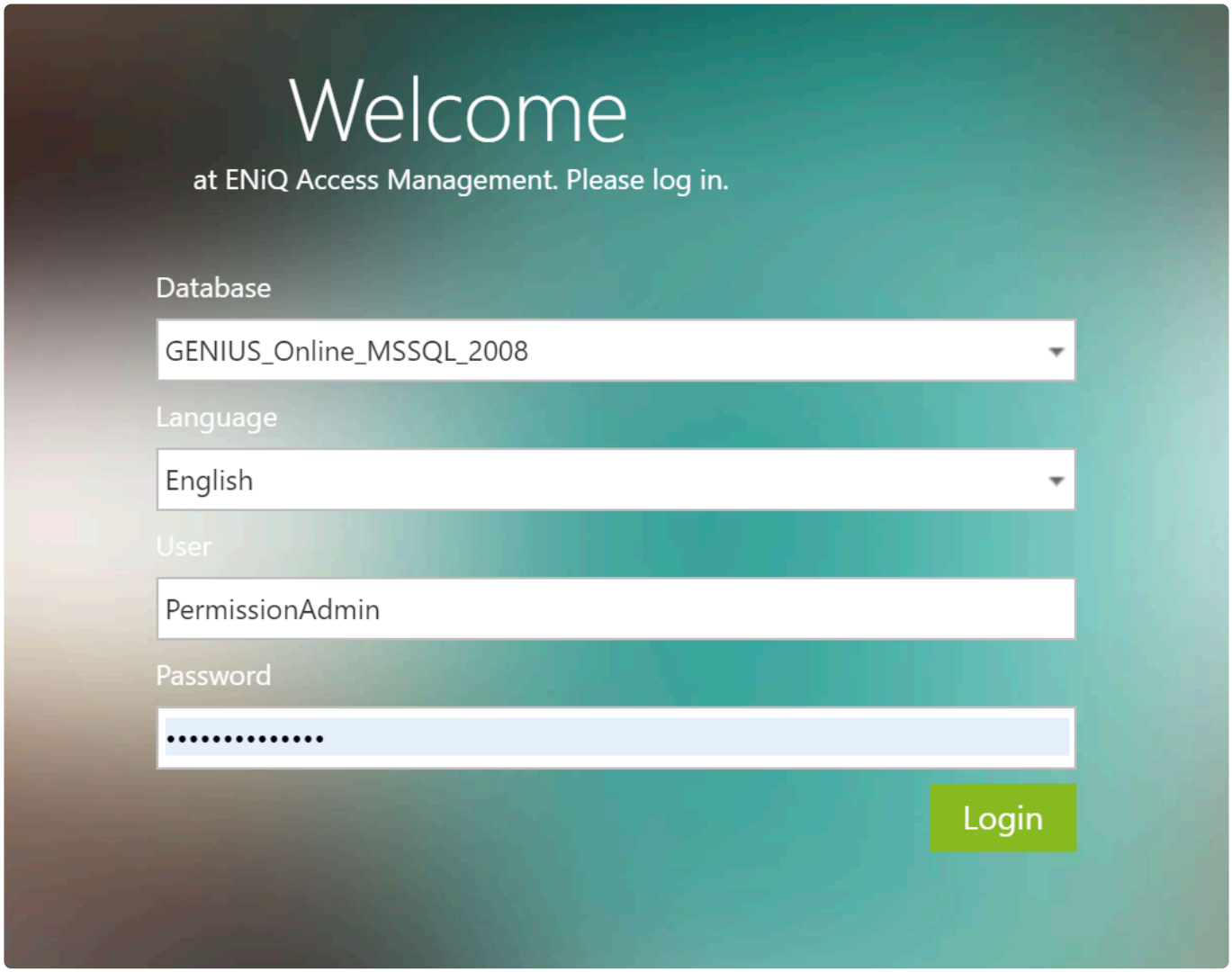
Step 4 – Assign role: The operator must now be assigned the role Permission Administrator. This leads to the fact that one can limit the view of the areas for this operator to a clearly defined area.



Step 5 – Assign AreaView: Once the role assignment has been made, the AreaView created in steps 1 and 2 can be assigned to the operator. To do this, switch to the Configuration tab in the operator detail view. Then select the correct AreaView from the Assigned AreaView item. Please note that an AreaView can be assigned to multiple permission admins.

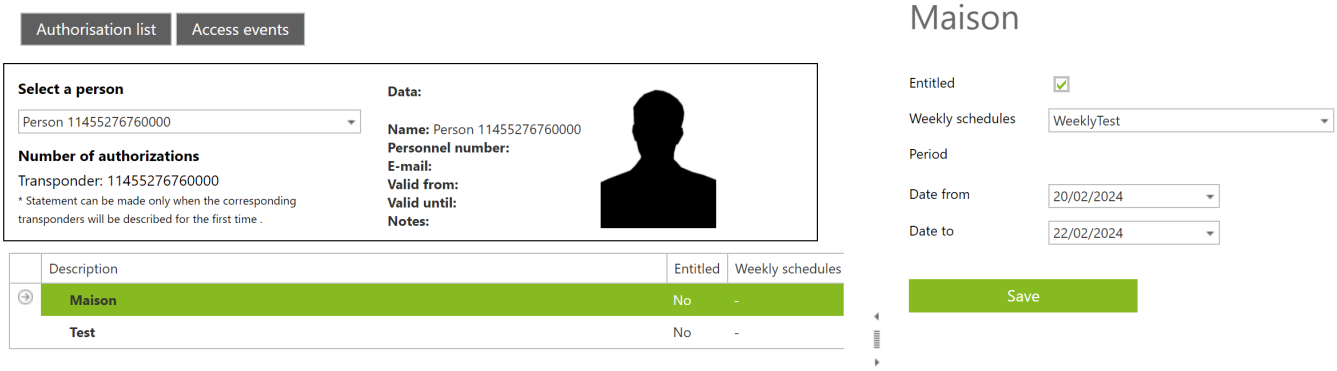


Step 6 – Using the Permission Administrator: After the complete configuration of the Permission Administrator, the newly created operator can log in using the usual login mask.



Step 7 – View of the Permission Administrator: Immediately after the successful login, the Permission Administrator sees his sub-areas assigned by the AreaView in a tree structure. In the upper area he can now select a user for whom he wants to assign a permission. In order to assign an authorization, he has to select an area and set the checkmark on the right side at the item Authorized and determine an associated weekly schedule.

The authorization for the selected area can then be confirmed with the Save button. Under the selection of the user, it is also displayed here how many area and device authorizations have already been assigned. If the maximum number of authorizations for one of the two authorization types is exceeded, there is a warning message. The maximum number of authorizations is defined by the transponder template that the system administrator activated after commissioning. If this is exceeded, an error may occur when writing to the affected locking medium. The names of the locking media affected by this are listed under the number of authorizations.



Restrictions

Current restrictions:

- Currently, only personal authorizations can be assigned. No locking media can be authorized directly.
- Authorization changes of locking media can only be written via an ACM terminal or an ACM-ITT. Locking media cannot be written directly via desk reader.
- No support of Person Groups
- Visibility can only be permitted for areas and not for individual devices
- In an allowed area, a sub-area cannot be explicitly blocked.
- No ACM extension group setting possible on the person (is set during SM import).
- No validity restriction possible (each authorization is infinite or not valid at all).
- No receipt printing possible

7. Operation

7.1. Journal

Display permissions and events

You can display information about events in the system in various menus.

You can view the following information:

- Access events of a transponder/person (in the “Person/Parameters” menu on the “Access events” tab)
- List of authorizations of a transponder/person (in the “Person/Authorization” menu on the “Authorisation (read only)” tab)
- Detailed list of authorizations of a person/transponder for areas and devices (in the “Person/Authorization” menu on the “Authorization List” tab)
- All assigned authorizations (in the “Access control” menu in the “List permissions” sub-menu)
- Authorizations filtered by properties (from the main menu using the “Go to Authorization List” button)
- List of all device events (from the “Journal/Events” menu)
- Display list of all current device data (in the “Access Control/Devices” menu on the “Device Data” tab)
- Display license information (in the “System” menu in the “License information” sub-menu)

7.1.1. Blacklist

Block transponder (blacklist)

> The blacklist function can be used in conventional (DataOnDevice) systems during device programming or in intelligent (DataOnCard) systems with an ENiQ ACM terminal or ITT, e.g. at the main access.

Transponders that have been lost, for example, can be locked out of the locking system using the blacklist function. The blacklist entry is programmed on each transponder using the desk reader or the ENiQ ACM ITT. The transponders bring the information to the devices by holding it on the terminal device. For offline devices, the blacklist entry can also be programmed to the device via the Device Management. For online devices, the blacklist entry is distributed to the devices via the network.

If an attempt is made to gain access with a blacklisted transponder, the transponder is permanently turned unusable. This ensures that even the devices that do not yet have any information about the blacklist entry can no longer be opened.
If you delete the transponder from the system, access will be denied if the transponder is used for an access attempt.

To blacklist a transponder, proceed as follows:

- Select the person who lost the transponder. In the “Person/Keychain” menu, select the lost transponder and go tor “Replace transponder”. Now you can read in a new transponder, the lost one will be blacklisted.
- Place a new transponder on the desk reader.
- Read the transponder
  The new transponder is now assigned to the person, the lost transponder is placed on the blacklist.

- Switch to the “Writing intelligent” (DataOnCard) tab.
- Click on “Save and write”

The transponder will be written with the appropriate permissions including the blacklist entry information.

To propagate the blacklist entry information in the system, do the following:

- Go to the existing offline devices with the transponder and show the transponder.

The information about the blacklist entry will be transmitted to the device.

- If an ACM-ITT is available, show the transponder there.

If the blacklisted transponder is now used, access is denied and the transponder becomes unusable.

7.1.1.1. Replace transponder

To replace the transponder of a person, proceed as follows:

- Click on “Access control” in the navigation bar.
- Select the “Persons” menu item

The “Persons” menu opens.

- Here you select the person who is to receive a successor transponder.
- Select the person and click on Edit

The “Data” tab opens

- Now switch to the “Keychain” tab

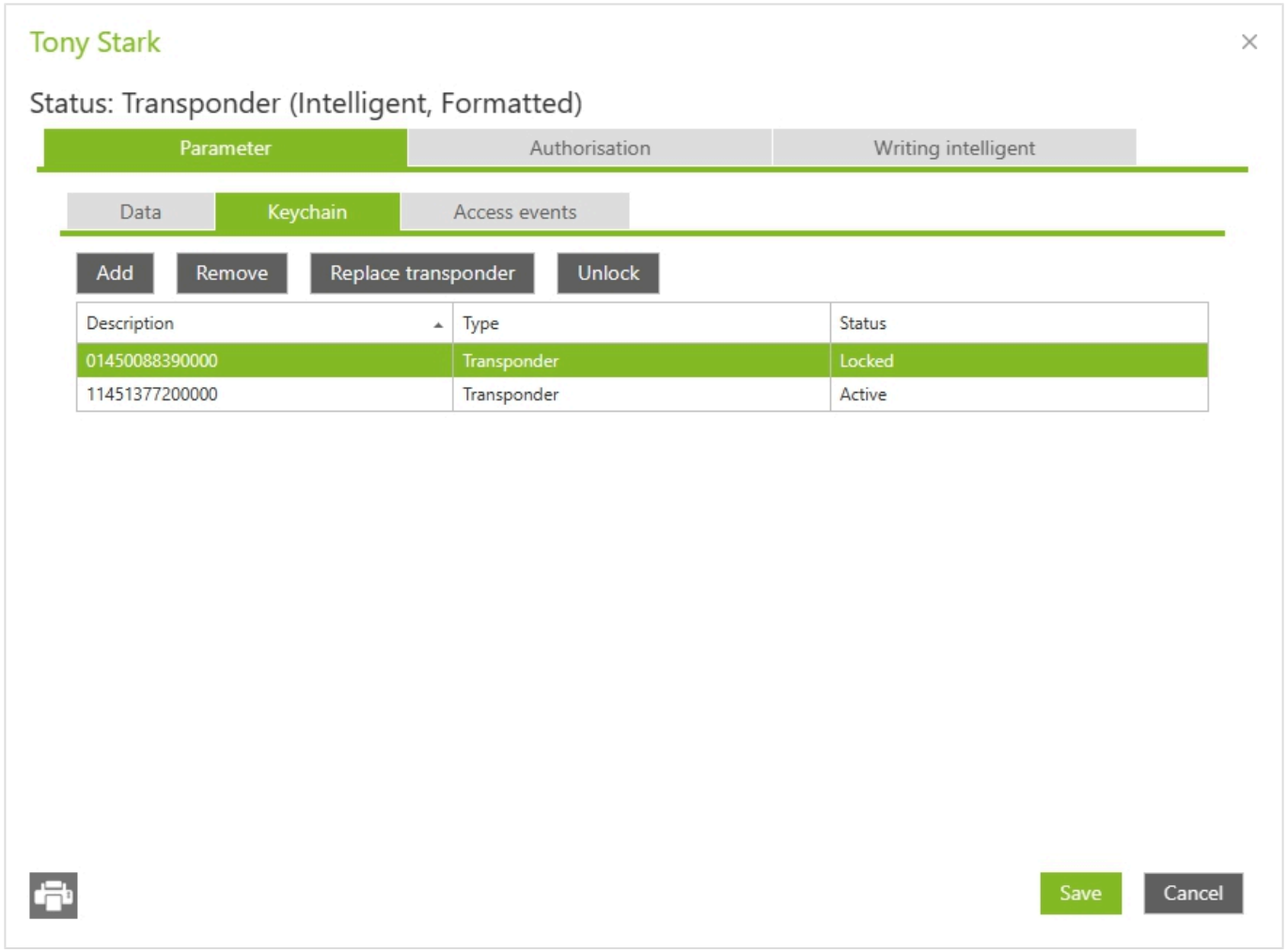
- Here you can see all the assigned locking media, e.g. transponders or mobile keys.

- Select the locking medium and click on the “Replace transponder” button.

The “Replace transponder” menu opens up

- Here you can assign an existing transponder, which is not yet assigned to a person, or assign a new transponder to the person.

- For an existing transponder use the drop-down menu and select the transponder
- To create a new transponder use the desk reader button and place a new transponder on the desk reader



The previous transponder is now deleted and blacklisted and the new one is active

For offline systems remember to program the associated devices

7.1.2. Events

Display and output event list for devices

This function allows you to display a list of events for all devices.
You can use the filter functions in the upper area of the menu to find specific information about devices or locking media. You can also rearrange the fields of the filter functions by moving them with the mouse.

To list the existing events of all the devices, proceed as follows:

- Click on “Journal” in the navigation bar.
- Select the “Events” menu item

The “Journal / Events” menu opens.

To show the events for a specific device, proceed as follows:

- Select the device in the top “Device” dropdown list.
- Tap “Search” button

The associated events are listed.

To export the list, proceed as follows:

- Click on the “Export” button.
- Select the desired file format from the drop-down menu.

The data is exported

7.1.3. History

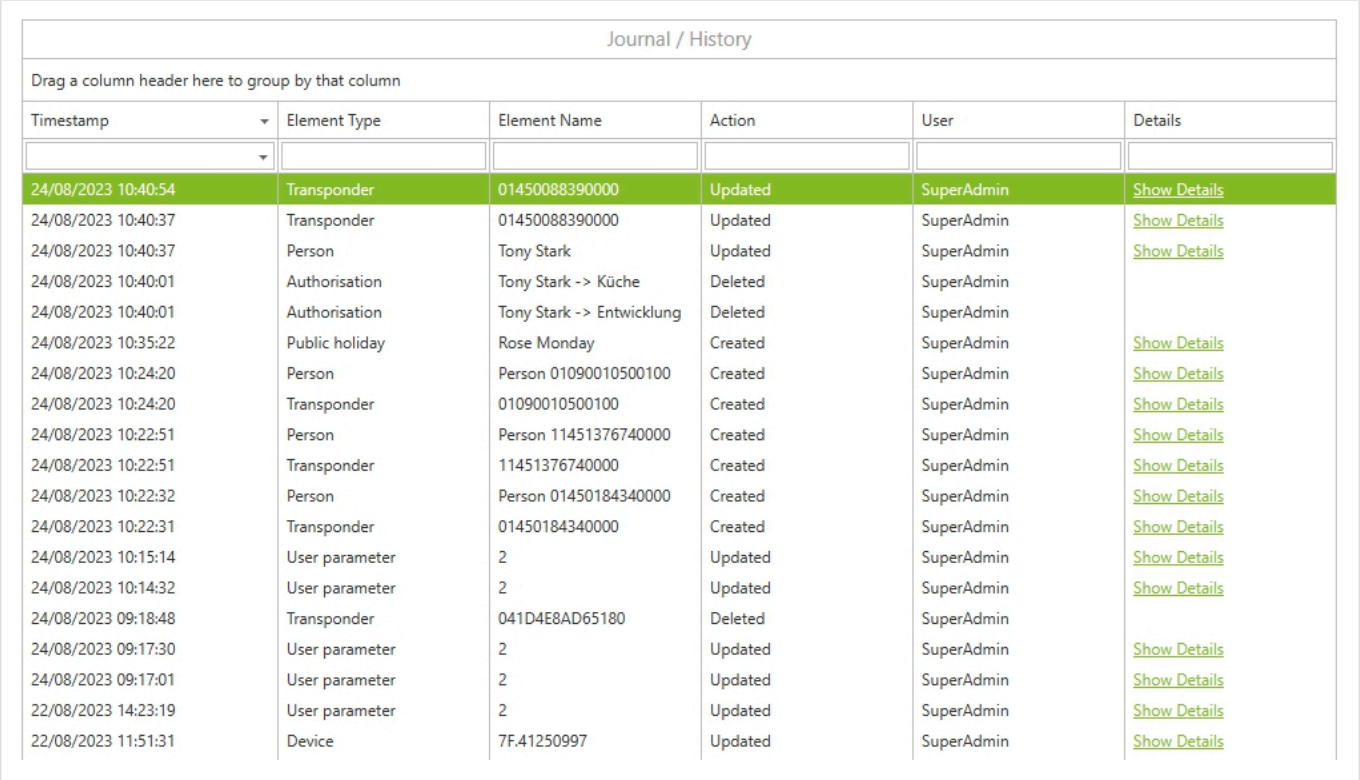
Display and output event list of the software

With this function you can display a list of all events that have been made generated by ENiQ AccessManagement.
You can use the filter functions in the upper part of the menu to find specific information about devices, persons and transponders. You can also rearrange the fields of the filter functions by moving them with the mouse.

To list the existing events, proceed as follows:

- Click on “Journal” in the navigation bar.
- Select the “History” menu item

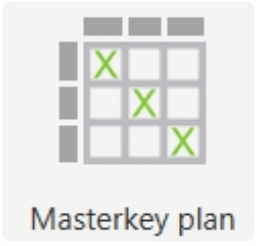
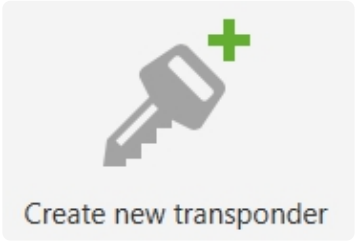
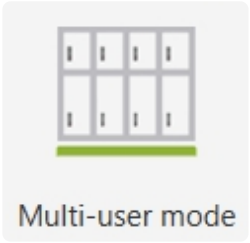
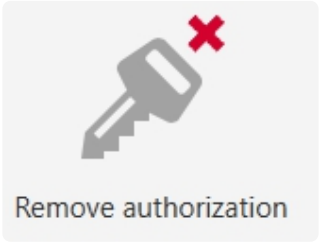
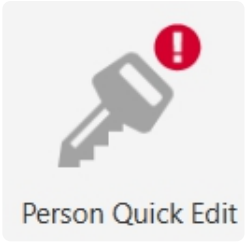
The “Journal / History” menu opens.

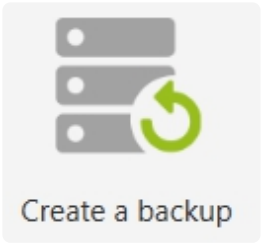


7.2. Assistants

7.2.1. Wizards description

Overview of the wizards and explanation of the functions

Assistant	Explanation/ Function
	The Masterkey plan editor provides you with a user-friendly way of displaying and editing authorizations. Especially in small and medium-sized systems, it gives you a good overview of all persons with access authorization in the system.
	This wizard is ideal for quickly creating and authorizing people with transponders. It also allows assignment to a Person group (It should be noted that the wizard supports only one group assignment for ease of use).
	If you need to make changes to the permissions, please use this wizard.
	This wizard will help you to use LoQs in multi-user mode. You can create new visitor transponders or read and display the status of an existing transponder.
	If a transponder is lost or an authorization is to be revoked, this wizard is an efficient solution to complete this task quickly.
	This wizard allows you to authorize all people and transponders on a static page. It offers an efficient and time-saving solution. In addition, this wizard is also available as an operator role (person administrator). When an operator logs in with this role, only this wizard page is displayed to him. This is particularly useful for certain functions such as reception.

	If you want to create a backup quickly, please use this wizard.

7.2.2. Masterkey plan

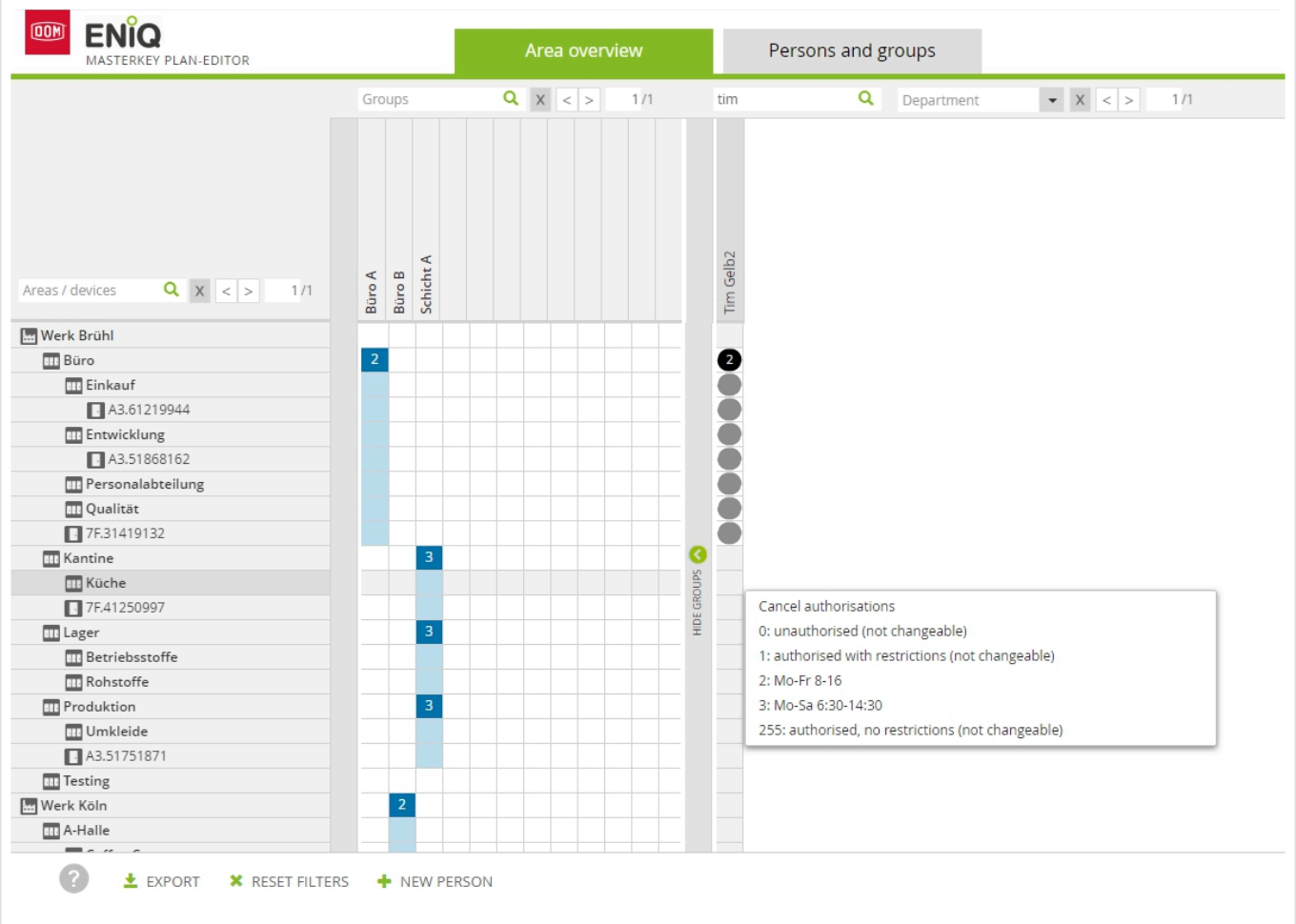
Allocate authorizations

Before you program the devices available in the system, you must assign the authorizations.
You can do this using the “Masterkey plan editor”, the wizards: “Quick Edit” and “Edit access rights” and the menu item Access control.

Masterkey plan

To authorize a person, proceed as follows:

- Click on “Wizards” in the navigation bar.
- Select the “Masterkey plan” button



Masterkey plan is displayed

> Pay attention to the highlighting of the boxes to select the correct area.

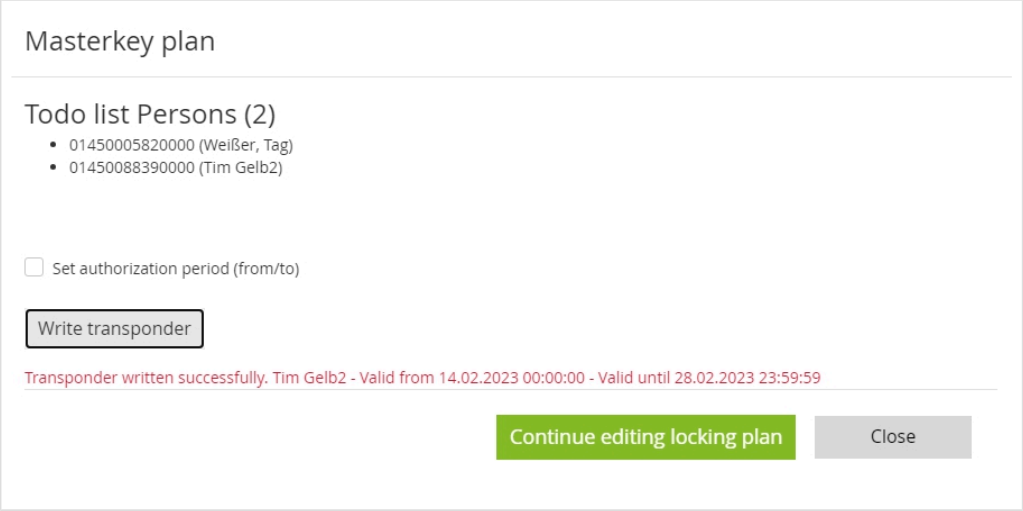
- Move the cursor to the appropriate box and right-click to select the weekly schedule
- Click Save

Pop-Up Masterkey planan

> If the person has an Intelligent (DataOnCard) Transponder a ToDo is created

You can update intelligent (DataOnCard) transponders directly via “Write to transponder”

- To do this, place the transponder on the desk reader and select “Write to transponder”



Success message “Write transponder”

After successful describing you receive the completion message

7.2.3. Backup

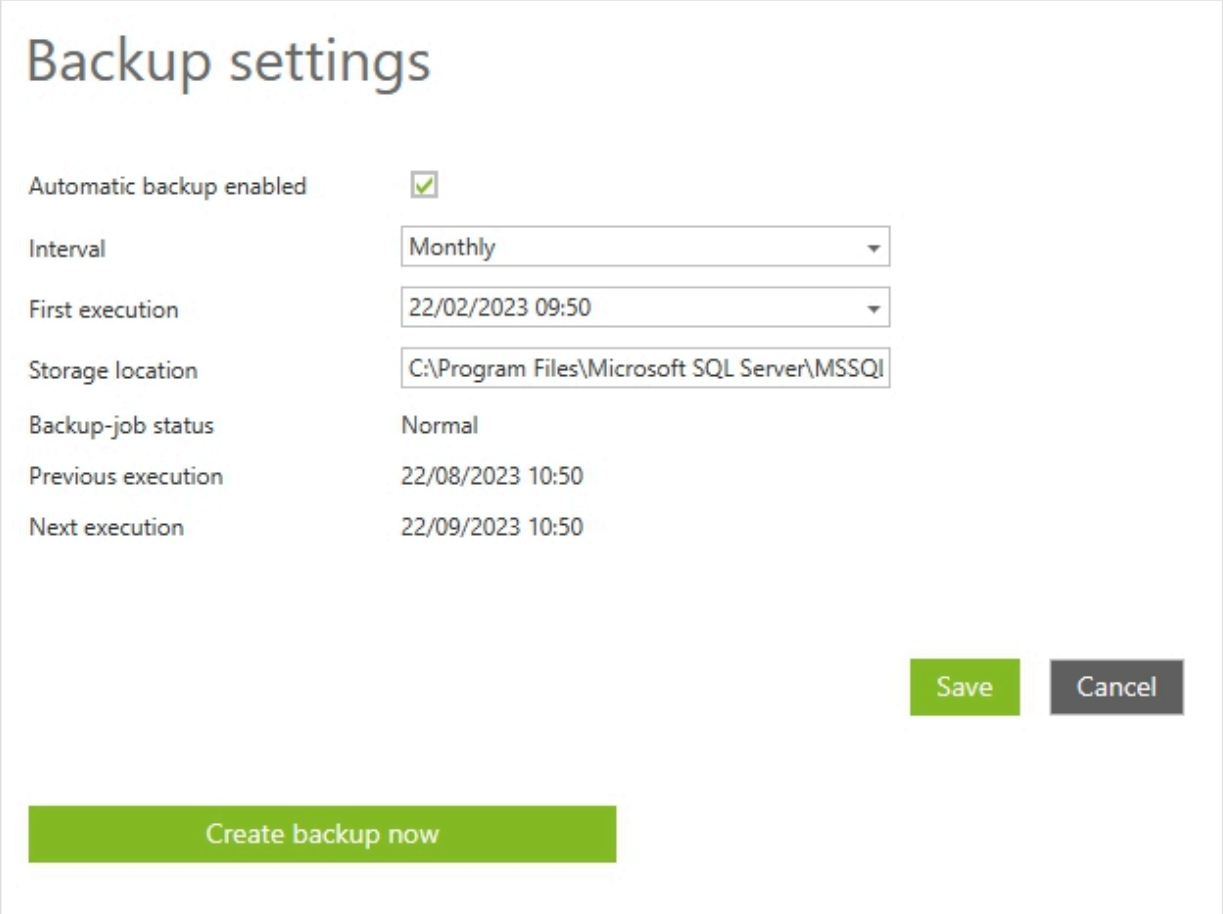
Use backup function

This function allows you to create a backup copy of the entire system.

Importing a backup may only be done by the system administrator.

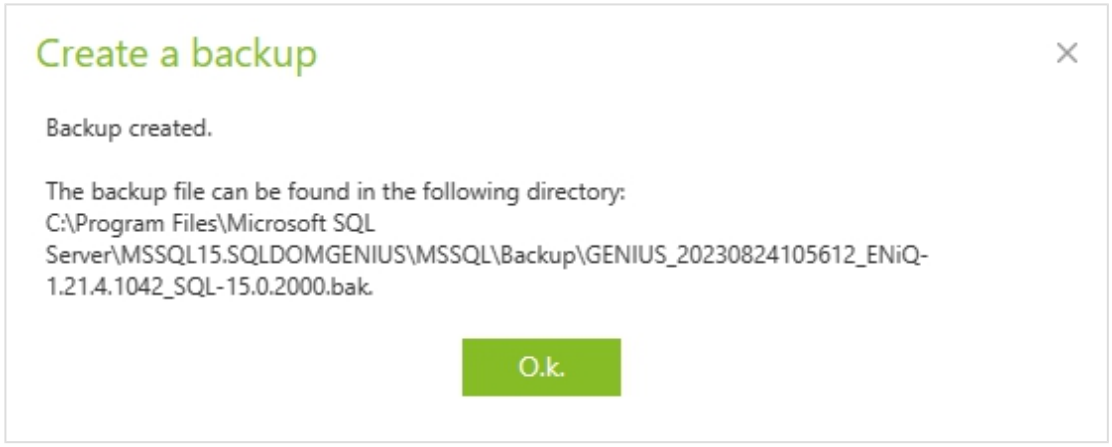
To create a backup of the database, proceed as follows:

- Click on “Wizards” in the navigation bar.
- Select the “Create a backup” menu item



The “Create Backup” button will be displayed.

- Click the “Create backup now” button.



A backup of the database will be created.

After successful completion, you will be shown the file path to the backup file location.

- Take note the location

To load a backup file, notify the appropriate database administrator. See more at Tools/DB-Manager/Backup/Restore

To schedule a regular backup of the database, do the following:

- Click on “System” in the navigation bar.
- Select the “Backup” menu item

Here you can set the regularity and location of the backup.

*Click Save to apply the settings

7.3. ToDo list

The “ToDo list” menu shows you whether there are still tasks to be completed after changing authorizations. This can be the programming of devices or the updating of transponders. The system and its devices and locking media are only up to date when no more entries are displayed in the ToDo list.

There is a ToDo list for each of the following system components:

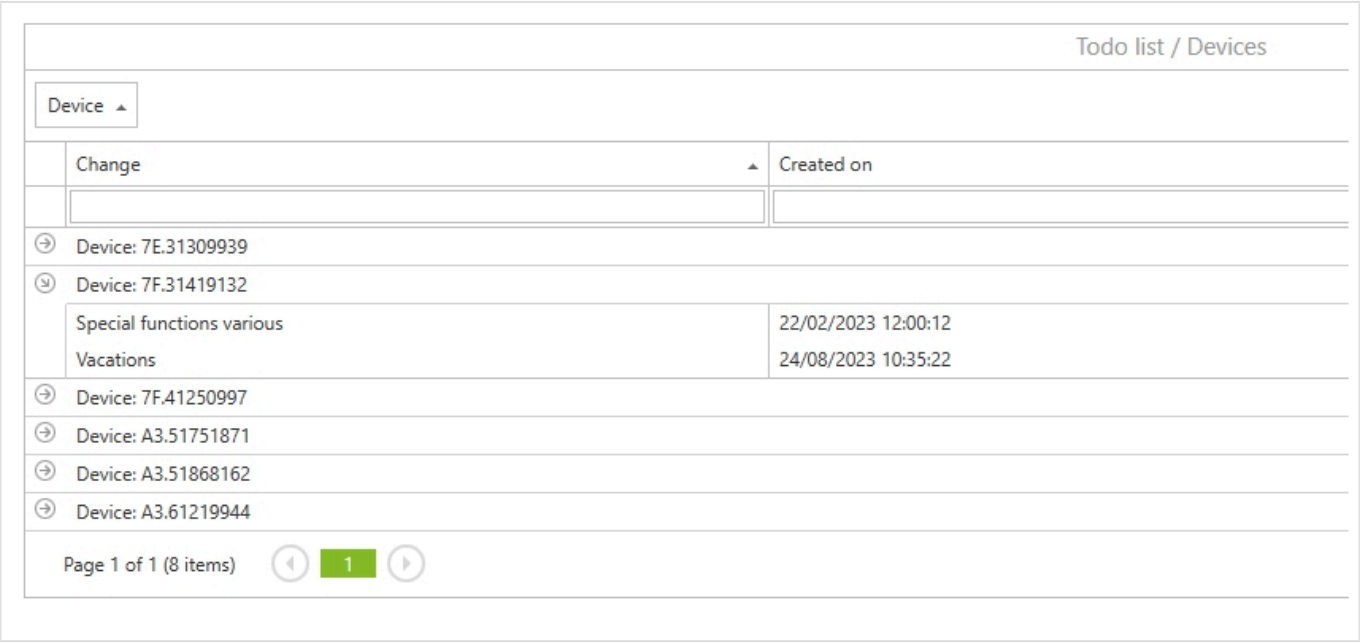
- To-do list for devices
- To-do list for online devices
- To-do list for transponders
- To-do list for MobileKeys

By default, the ToDos are released automatically, but you can decide to release the ToDos manually from *System/Settings/General/Release Todos automatically*. If this setting is disabled, a “Release all” button is available below the ToDos list.

Display ToDo list for devices

To display the ToDo list for devices, proceed as follows:

- Click on “ToDo List” in the navigation bar.
- Select the menu item “Devices”



The “ToDo List/Devices” menu opens.

- To update the displayed devices, perform a programming of the devices.

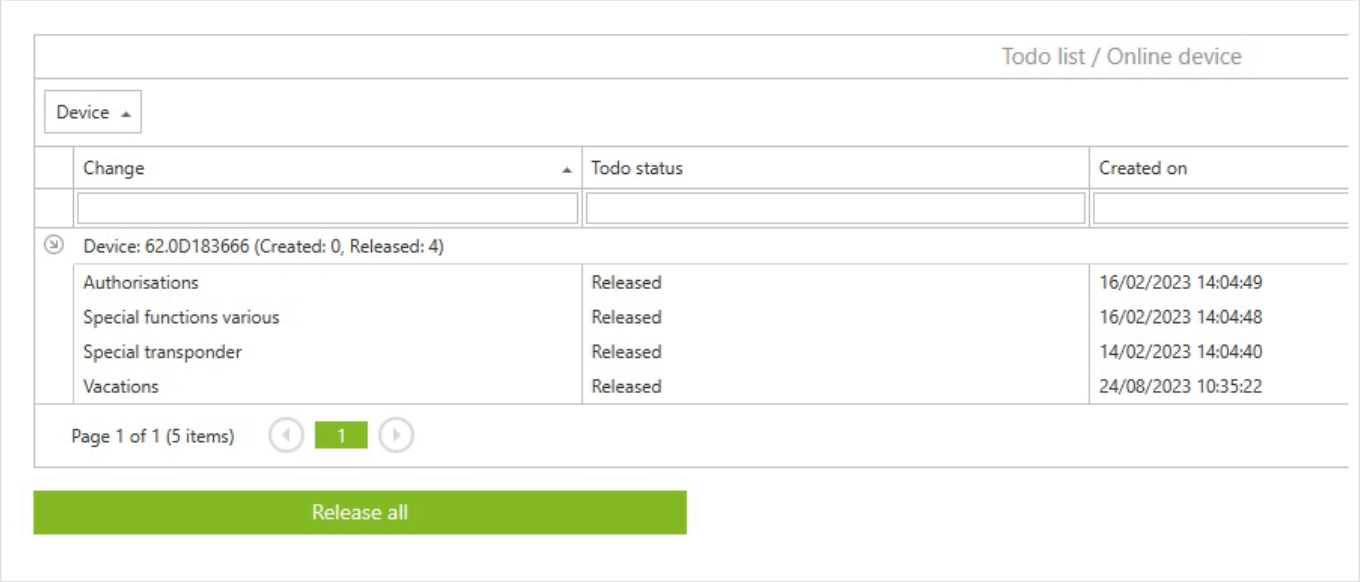
You have to perform the programming of the devices in the program “ENiQ Device Management software” or with the DOM Service mobile app. Information about this can be found in the chapter

Programming devices.

Display ToDo list for online devices

To view the ToDo list for online devices, do the following:

- Click on “ToDo List” in the navigation bar.
- Select the “Online devices” menu item



The “ToDo List/Online Devices” menu opens.

- The displayed devices will be automatically programmed with the next “Alive” when connected online. You can trigger the process manually by clicking on “Release all”.

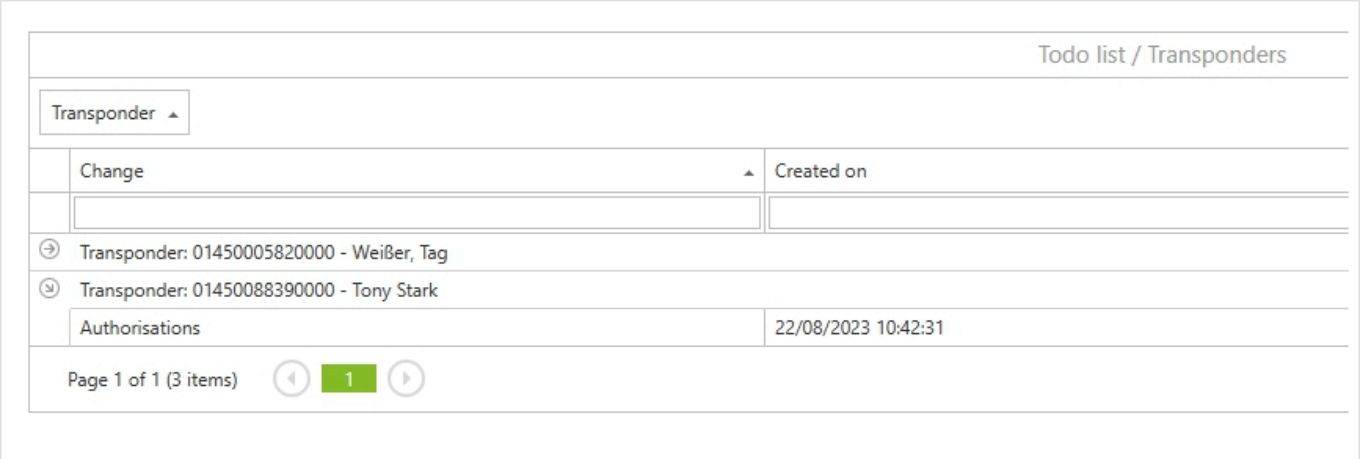
It is no longer necessary to program the devices via the ENiQ Device Management software.

The devices are now automatically programmed via the network connection.

Display ToDo list for transponders

To display the ToDo list for transponders, proceed as follows:

- Click on “ToDo list” in the navigation bar.
- Select the “Transponders” menu item



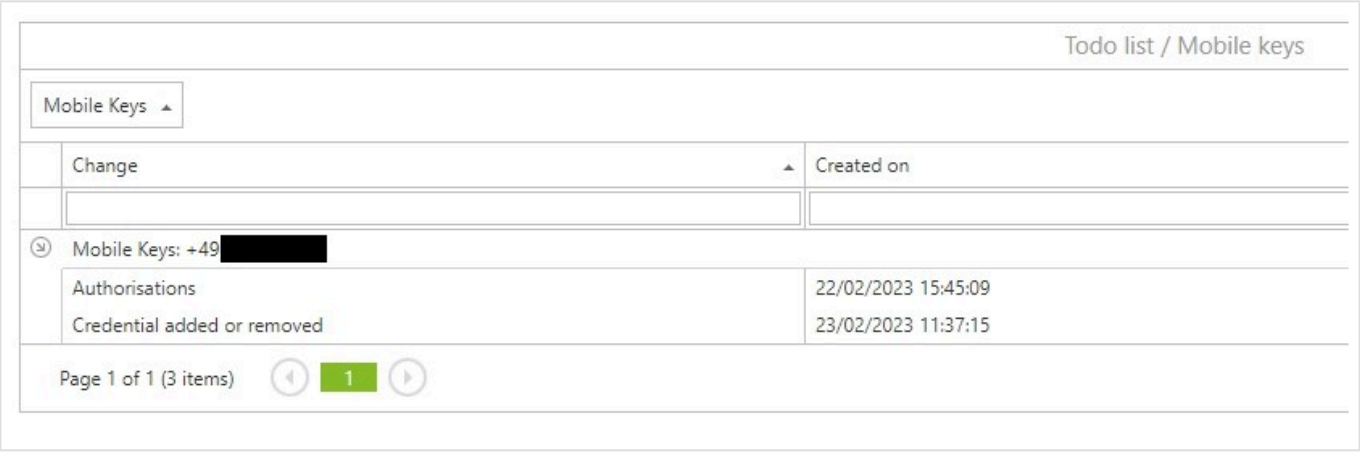
The “ToDo List/Transponders” menu opens.

- To update the displayed intelligently (DataOnCard) managed transponders, perform a programming of the transponders with the desk reader or on the ENiQ Access Manager ITT.

Displaying the ToDo List for Mobile Keys

To display the ToDo list for Mobile Keys, proceed as follows:

- Click on “ToDo List” in the navigation bar.
- Select the menu item “Mobile Keys



The menu “ToDo List/Mobile Keys” opens.

- The mobile keys are automatically synchronised in the cloud.

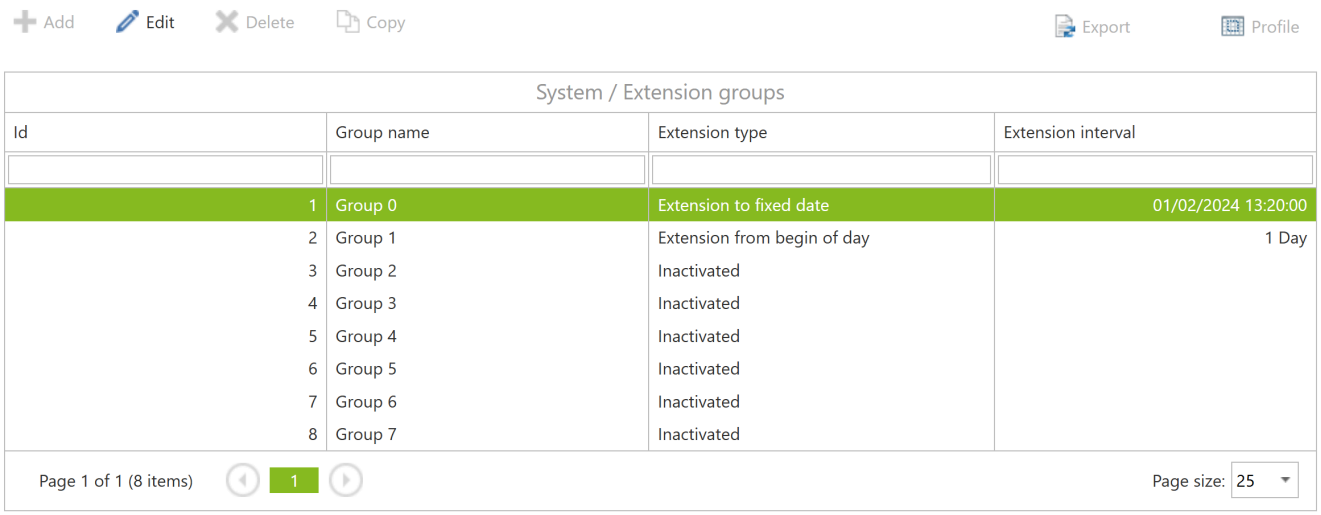
7.4. Extension groups

Extension Groups are used to extend the validity of transponders using ENiQ ACM Terminal or ITT. For example, you can define that a transponder is only valid for 24h, and needs to be extended everyday by presenting it to the ACM Terminal or ITT.

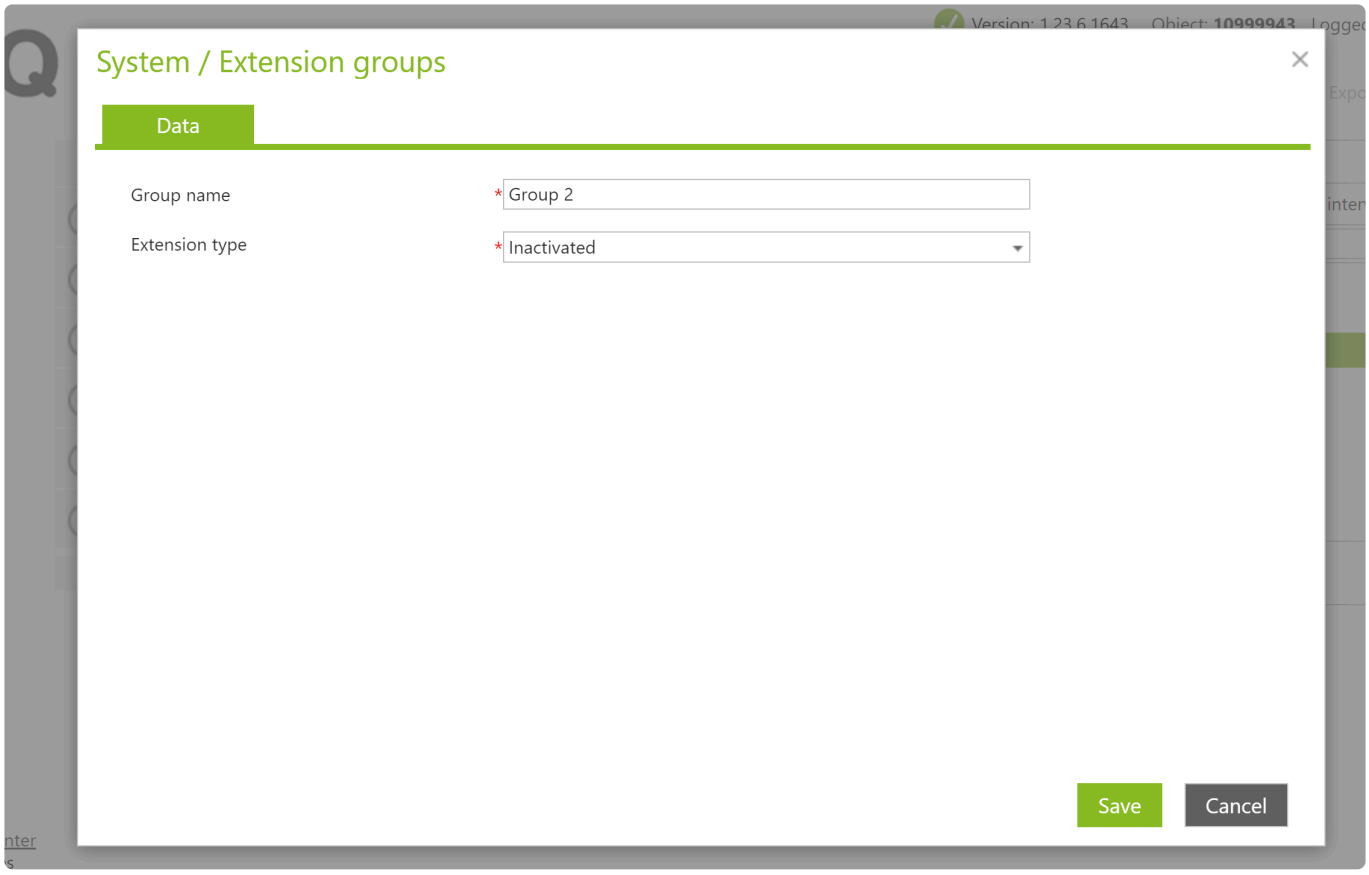
The benefit of Extension Groups is that you are in control of the maximum validity of transponders. If a transponder needs to be presented each day to an ACM Terminal or ITT in order to get its validity extended, it means that if the transponder is marked as lost (blacklisted), then it will maximum be valid until the end of the day. In that case the blacklist does not need to be transmitted to all the system devices, as the transponder will be invalidated at the end of the day.

Activate an Extension Group

Extension Groups can be activated in “System” / “Extension groups”. A maximum of 8 Extension Groups can be activated.



- Select and click “Edit” (or double-click) on an “inactived” Extension Group, then define the name and type of the group.



Here are the details of each available Extension Group type:

Extension Group Type	Description	Example
Extension to fixed date	Each time the transponder is presented to the ITT, the validity end of the transponder will be set to the specified date and time. Start of the validity will be set to the current time when transponder is presented to the ITT.	Date is defined as “25/02/2025 – 10h30”. Transponders associated to this Extension Group will get their validity end set to “25/02/2025 – 10h30” each time they are presented to the ITT. The fixed date for the Extension Group can be changed anytime to match the current needs.
Extension from current time	Each time the transponder is presented to the ITT, the validity end of the transponder will be set to “current date and time + specified interval”. Start of the validity will be set to the current time when transponder is presented to the ITT.	Extension interval is defined as “1 day – 0 hours – 0 minutes”. Transponders associated to this Extension Group will get their validity end set to the next day at the current time when it is presented to the ITT. If the transponder is presented at 16:00 to the ITT, it will be valid until next day at 16:00
Extension from begin of day	Each time the transponder is presented to the ITT, the validity end of the transponder will be set to “current day at 00:00 + specified interval”. Start of the validity will be set to the current time when transponder is presented to the	Extension interval is defined as “1 day – 6 hours – 0 minutes”. Transponders associated to this Extension Group will get their validity end set to the next day at 06:00, each time they are presented to the ITT.

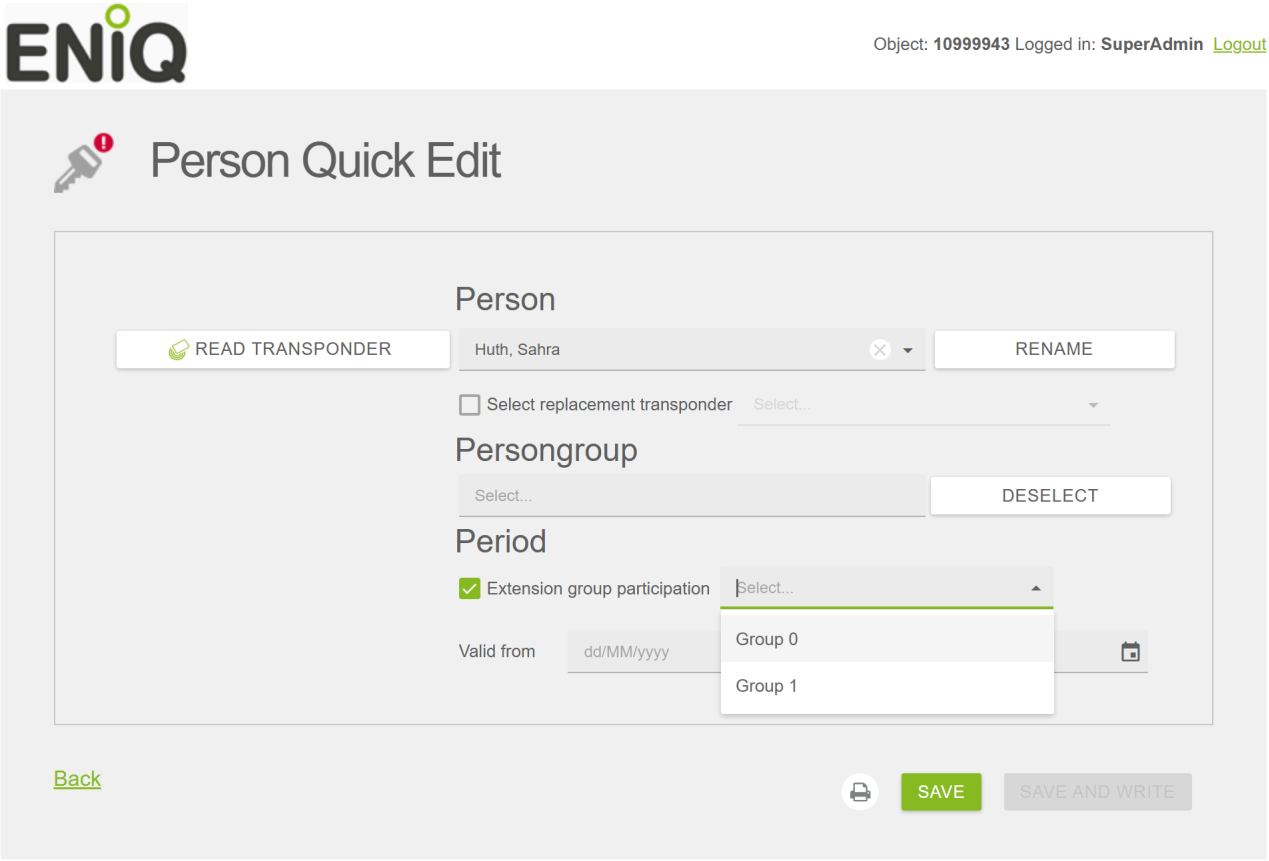
	ITT.	

- Once a new Extension Group is enabled or changed, ACM Terminals need to be synchronised (see Offline Synchronisation). ACM ITTs will be automatically synchronised with the online system.

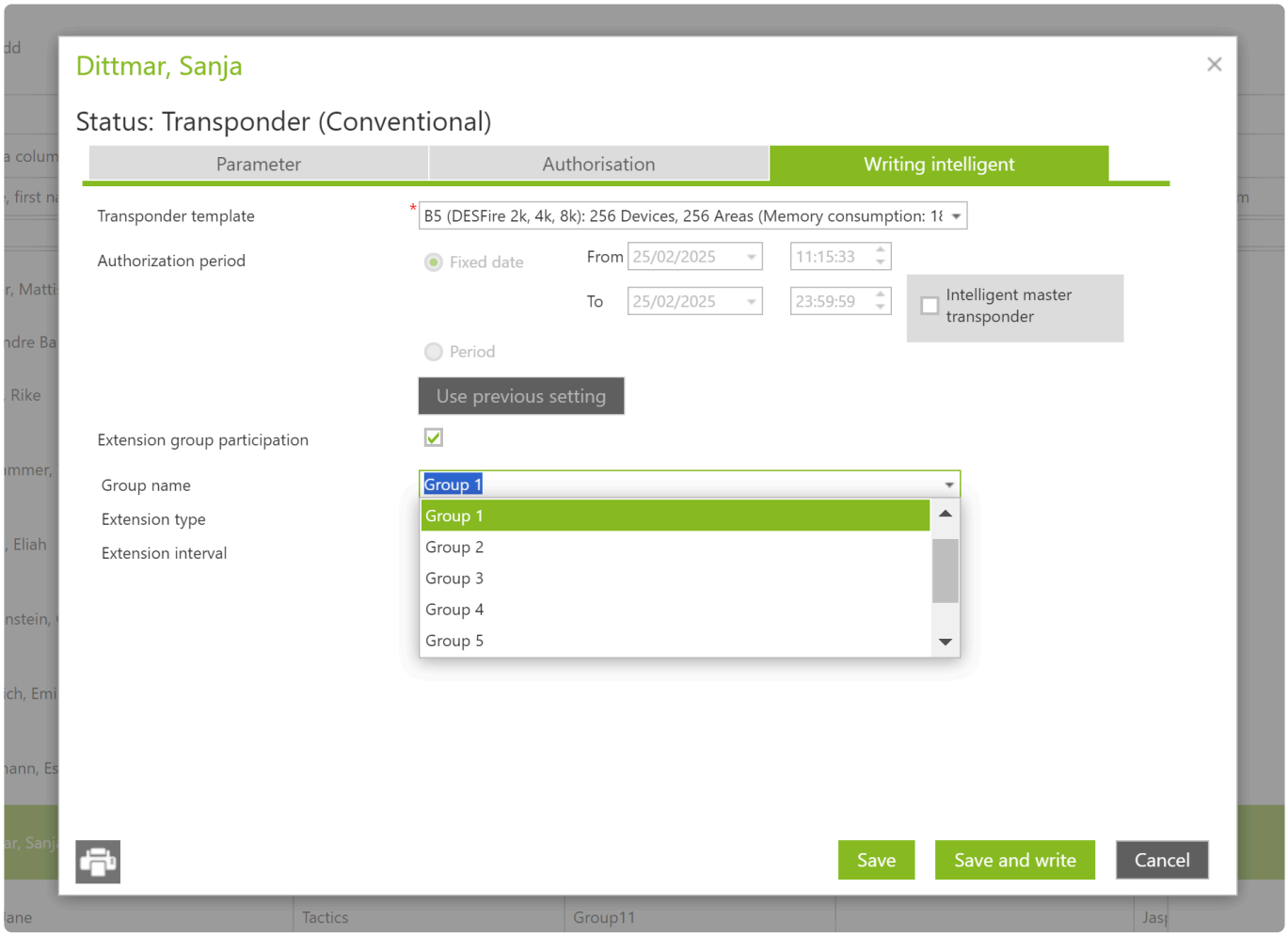
Assign an Extension Group to a transponder

Extension Groups can be assigned to transponders in multiple ways:

- With the Person Quick Edit wizard: Select a Person or read a transponder, select an Extension Group, then click “Save and write” to write the transponder.



- On the Person details: Open the Person details in “Access Control” / “Persons”, go to the “Writing intelligent” (DataOnCard) tab, select the “Extension group participation”, then click “Save and write” to write the transponder.


Dittmar, Sanja
Status: Transponder (Conventional)
Parameter
Authorisation
Writing intelligent
Transponder template
B5 (DESFire 2k, 4k, 8k): 256 Devices, 256 Areas (Memory consumption: 1
Authorization period
Fixed date
From 25/02/2025 11:15:33
To 25/02/2025 23:59:59
Intelligent master transponder
Period
Use previous setting
Extension group participation
Group name
Extension type
Extension interval
Group 1
Group 1
Group 2
Group 3
Group 4
Group 5
Save
Save and write
Cancel
Tactics
Group11

7.5. Action groups

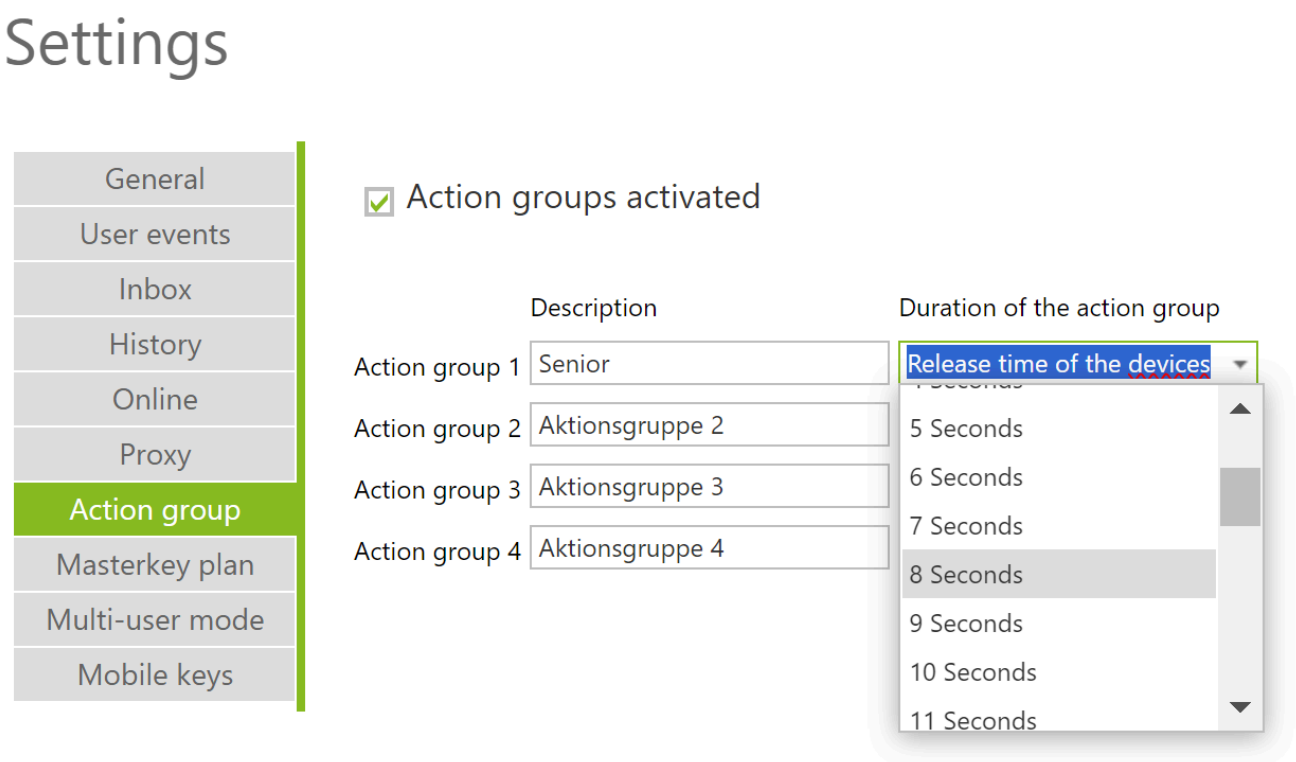
Overview of the action groups and corresponding explanations

With the help of the action groups, people can be granted different activation periods on the same end device.
To illustrate this, you can imagine a retirement home:

By default, staff are granted an activation time of 5 seconds at the entrance door.
Senior citizens have an extended activation time at the entrance door via the action group.

Procedure for setting up:

- System -> Settings -> Action group
- Activate the “Action groups activated” checkbox
- Assign a name
- Select an activation duration for the devices



Then assign the action group to the corresponding person

All devices that are opened by this person open with the activation duration of the action group.

7.5.1. 4-Eyes Principle

The “4-eyes principle” (or “2-persons principle”), is useful when the access to a room should require to present 2 different transponders, one after the other. This can be required to add security on accessing a critical room or area, that would require the authorisation of 2 different persons.

In ENiQ AccessManagement, this feature is configured using the Action Groups (see Action groups), so that 2 transponders belonging to an Action Group are required to unlock a device.

> All transponders belong by default to Action Group #1.

When 4-eyes principle is enabled on a locking device, it will require that 2 transponders are presented, one after the other.
Any combination of Action Groups are allowed, **expect “1 with 1”**:

- 1 with 2, 1 with 3, 1 with 4
- 2 with 1, 2 with 2, 2 with 3, 2 with 4
- 3 with 1, 3 with 2, 3 with 3, 3 with 4
- 4 with 1, 4 with 2, 4 with 3, 4 with 4

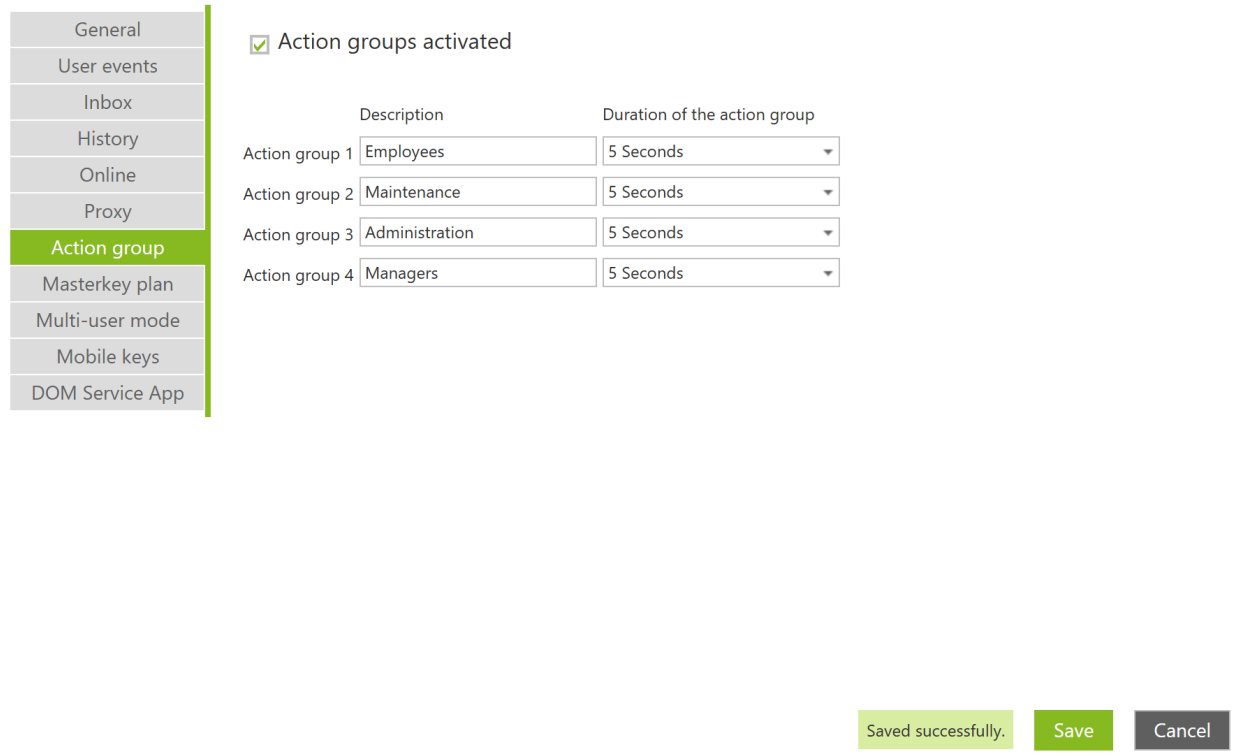
> This means that by default, when enabling 4-eyes principle on a locking device, 2 transponders with default Action Group 1 won’t be able to unlock the device. It will require that a transponder with a “higher” Action Group is presented, before or after.

Requirements

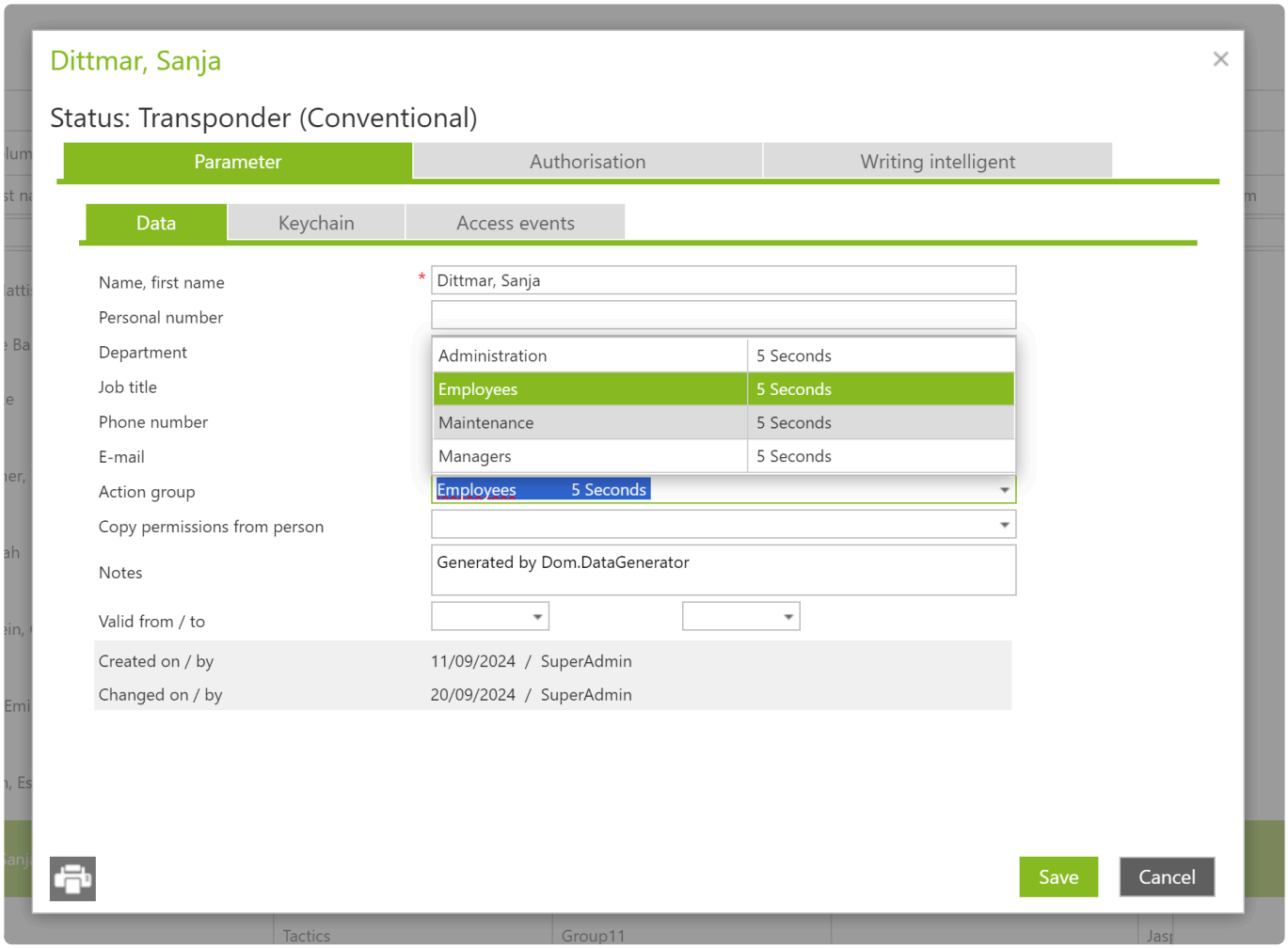
- Minimum firmware v5.4 on targeted ENiQ locking devices
- ENiQ AccessManagement v1.24

Configuration

- Activate the Action Groups: Go to “System” / “Settings” / “Action group”, enable the feature by clicking the checkbox, and rename the Action Groups you wish to use:

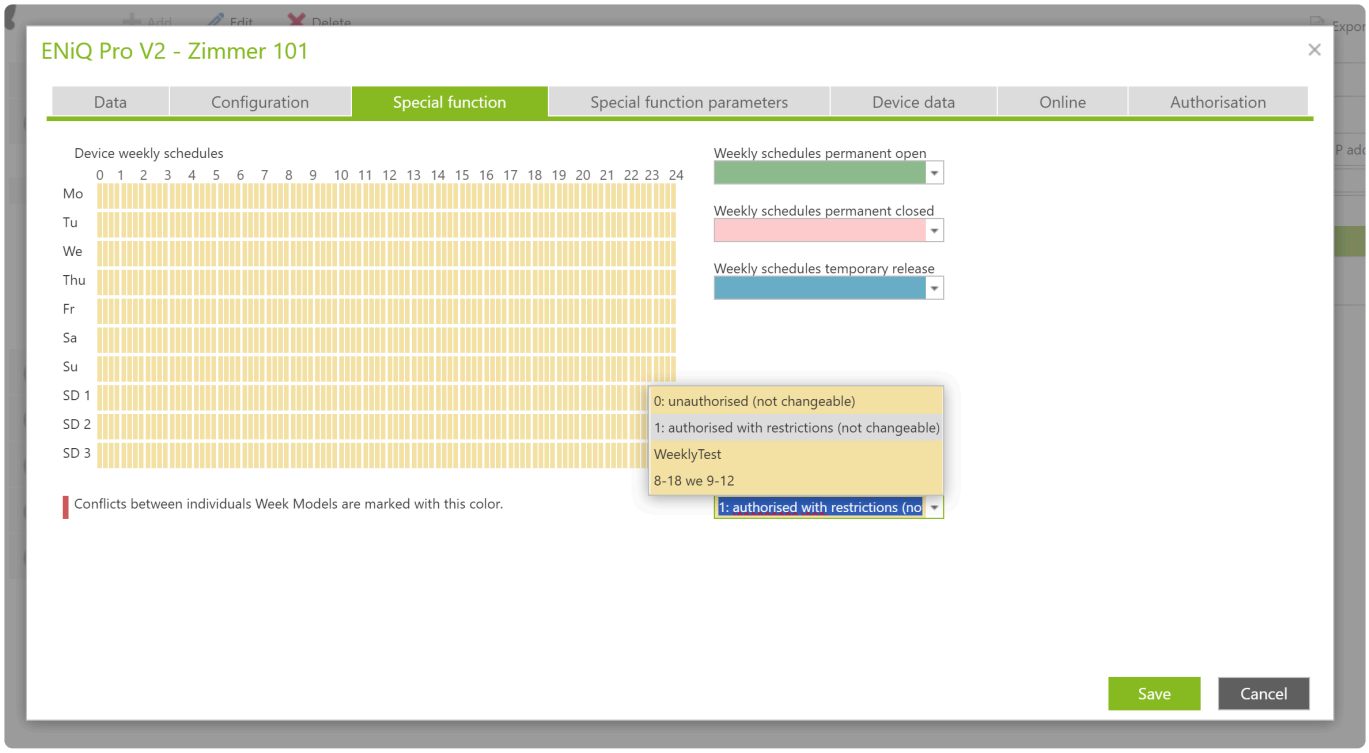


- Assign Action Groups to transponders: By default, all transponders belong to Action Group #1. This can be changed from the Person details (“Access Control” / “Persons”):



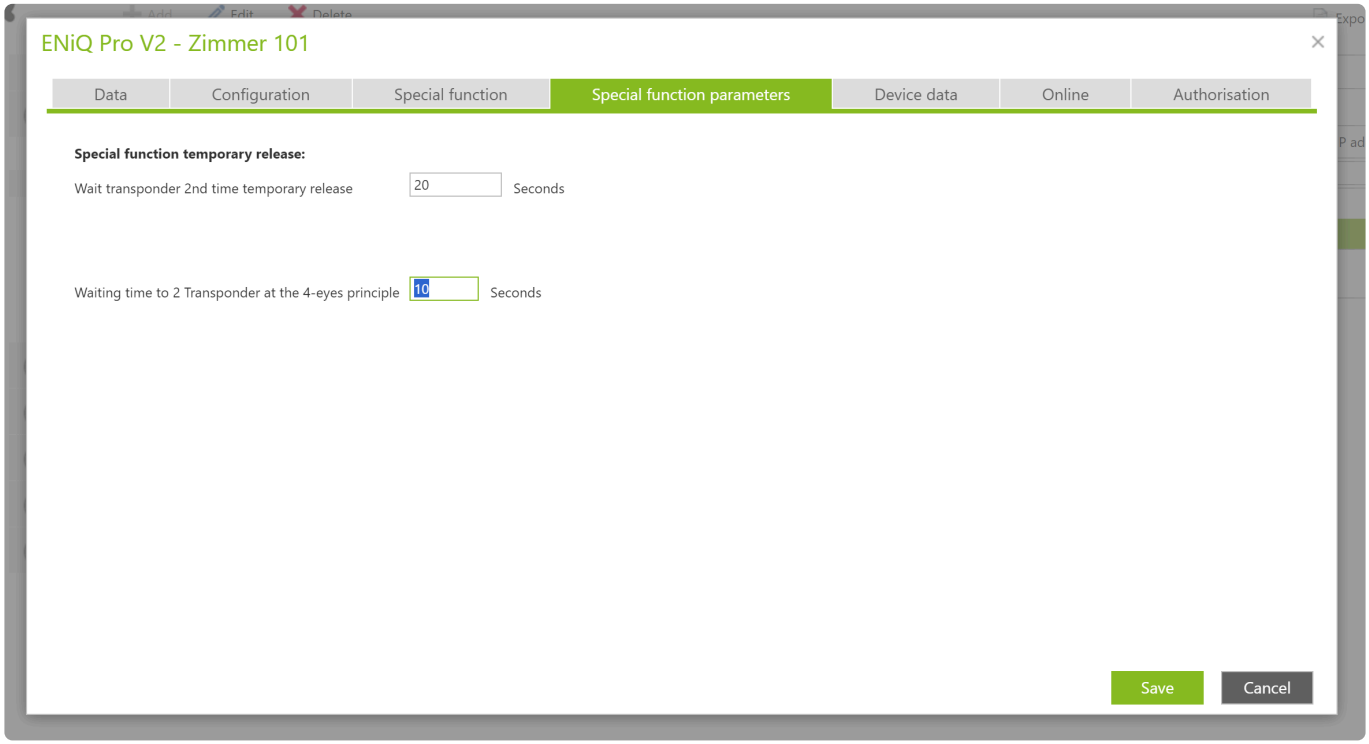
As an example, you can assign an Action Group higher than #1 to all Persons that have higher level permissions, or should be needed to unlock special doors.

- Enable 4-eyes principle on the required locking devices: Define which locking devices require an extra level of security, by enabling 4-eyes principle from Device details (“Access Control” / “Devices”), in the “Special function” tab:



If you wish that the locking device always requires that 2 transponders are presented, you can select the Weekly Schedule “1 – Authorised”. Otherwise, you can select any custom Weekly Schedule (see Create Weekly Schedules)

By default, the time allowed between the 2 transponders being presented is maximum of 20 seconds. This can be configured per locking device, on the Device details (“Access Control” / “Devices”), in the “Special function parameters” tab:



! After changing the Action Group of a transponder, in Data on Card (intelligent) systems, it needs to be synchronised. After enabling and configuring 4-eyes principle on a locking device, it needs to be synchronised.

8. Other settings and functions

8.1. System settings

This section describes all the settings and options available under “System” / “Settings”.

General

Setting	Description
Object name	The name of the system. By default, the value is the Electronic System ID (Object ID)
Automatically use a special day schedule for public holidays	If disabled, no public holidays or vacations are written to the devices. Also the menu items for “Public holidays” and “Vacations” are hidden.
Enable automatic update search	By default, ENiQ Software automatically searches for software updates. Learn more
Release todos automatically	When the configuration of devices or transponders change, ToDos are “Created”. When using Device Management, DOM Service, or Desk Reader to update the devices or transponders, only the “Released” ToDos are sent. By default, all “Created” ToDos are “Released”, and made available to Device Management, DOM Service and Desk Reader. This option allows to manually release the created ToDos, for having more control on what is written on devices and transponders
Eco mode for battery operated devices	If this is not required, the Bluetooth interface can be deactivated. This results in a longer battery life for battery operated devices. By default, “Eco mode” is disabled. Learn more
Transport battery warnings via transponder	Battery warning from offline devices can be transported by the transponders until the software. Learn more

User events

Setting	Description
User events enabled	By default, events generated by devices from user actions are collected and displayed in the software, in “Journal” / “Events”. User events collection can be disabled globally.
Cleaning type	By default, the user events are not deleted automatically. “Keep for [X] days” will delete all user events older than X days (X defined in setting below “Number of days”). “Delete completely after [X] days” will delete all user events each X days.

Number of days	Value to configure the [X] of the setting “Cleaning type”.
Current number of entries	Count of all user events stored.
Delete user events	Deletes all user events stored

Inbox

Setting	Description
Cleaning type	Inbox contains messages for software updates and system errors. By default, the Inbox messages are not deleted automatically. “Keep for [X] days” will delete all Inbox messages older than X days (X defined in setting below “Number of days”). “Number of entries” will only keep the latest Y Inbox messages. (Y defined in setting below “Number of entries”). “Number of days and entries” will both delete all Inbox messages older than X days and also will only keep the latest Y Inbox messages.
Number of days	Value to configure the [X] of the setting “Cleaning type”.
Number of entries	Value to configure the “Number of entries” cleaning type.
Current number of entries	Count of all Inbox messages stored.

History

Setting	Description
History enabled	By default, each modifications done in ENiQ Software by a user generates an History item, and is displayed in the software, in “Journal” / “History”. History collection can be disabled globally.
Cleaning type	By default, the History items are not deleted automatically. “Keep for [X] days” will delete all History items older than X days (X defined in setting below “Number of days”). “Number of entries” will only keep the latest Y History items. (Y defined in setting below “Number of entries”). “Number of days and entries” will both delete all History items older than X days and also will only keep the latest Y History items.
Number of days	Value to configure the [X] of the setting “Cleaning type”.
Date of	Date of the oldest History entry stored.

the first entry	
Number of entries	Value to configure the “Number of entries” cleaning type.
Current number of entries	Count of all History items stored.

Online

Setting	Description
Alive time of the online services (in minutes and seconds)	Delay between each check of the availability of the Online services (Slave and Master). Learn more
Maximum deviation of the device time to automatic reprogramming (in minutes and seconds)	The clock inside online locking devices can deviate of a few seconds over time. This settings forces the re-synchronisation of the online devices clocks if the clock deviate of more than MM:SS. By default, set to 00:05 (5 seconds).

Proxy

Setting	Description
Use proxy server	Possibility to enable and configure the ENiQ Software online connection through a proxy server. Disabled by default.
Use https protocol	Proxy is configured by default to use HTTP.
Address of the proxy server	IP or URL of the proxy server
Port of the proxy server	Port used for the proxy server
Use the default credentials for the proxy server	By default, no specific credentials are used, and depends on the user system. Disabling this option allows to specify the credentials to be used.
Login name for the proxy server	“login” name for proxy server connection
Password for the proxy server	“password” for proxy server connection

Action group

Setting	Description
Action groups activated	Activation and configuration of action groups. Learn more

Masterkey plan

Setting	Description
Show Inheritance	When a permission to a Person for an Area, this Person automatically gets the same permission for all Devices and Areas included in that Area. By default, the inheritance is displayed in the Masterkey plan using a special color.
Show Inherited Weekly Schedule	When inherited permissions are displayed with a special color (“Show inheritance” setting), it is also possible to show the Weekly Schedule number that is inherited.
Display symbols in the area tree	Displays an icon of the item type in front of each area/device.
Show devices as a door	The icon in front of devices changes from “device” to “door” type.
Number of columns for person groups	Maximum number of columns displayed for Person Groups. Default is 20. Pagination is used to view the rest of Person Groups.
Number of columns for persons	Maximum number of columns displayed for Persons. Default is 20. Pagination is used to view the rest of Persons.
Number of rows for areas / devices	Maximum number of columns displayed for Areas / Devices. Default is 20. Pagination is used to view the rest of Areas / Devices.
Defaults	Reverts the number of columns and rows of Person Groups, Persons, and Areas / Devices to the default value.

Multi-user mode

Setting	Description
Mifare Classic Sectors	2 sectors will be used by the Multi-User mode on visitor transponders. Default sectors are 2 and 3. Those sectors can be changed if already used by another application.

Mobile keys

Setting	Description

Automatic configuration	Choose which devices should be configured for Mobile Keys automatically. “Do not configure devices” – No devices will be configured automatically. Each device should be configured individually and manually. “Configure ACMs only” – Only ACM devices will be configured automatically. “Configure all devices” – All existing and new devices will be configured automatically. Default value is “Do not configure devices”.
Auto configuration interval (minutes)	Time interval in minutes for which the devices in the category selected above are configured automatically for Mobile Keys. Default value is 10 minutes.
Todos synchronisation interval (minutes)	Time interval in minutes for which the Mobile Keys ToDos are sent to the Cloud. It represents the maximum time for Mobile Keys permission changes to be effective on the end-users’ DOM Key application. Default value is 1 minute.
Clean-up interval (minutes)	Time interval in minutes for the Clean up Job. The job cleans up the binding states and synchronizes the sytem. Default value is 10 minutes.
Battery warning fetching interval (hours)	Time interval in which the software connects to the Mobile Keys Cloud in order to fetch the latest battery warnings retrieved from devices by the DOM Key mobile app. Default value is 6 hours.
Fetch Battery States now	Forces the retrieval of the latest battery states from Mobile Keys Cloud, that were retrieved from devices when using the DOM Key mobile app.
Mastercard number	Mastercard used to first register with Mobile Keys. Even if the Mastercard of the system changed since the Mobile Keys were enabled, still the first Mastercard is displayed here.
MobileKey Account ID	ID of the Mobile Keys Cloud account, for service purposes.
Update Mobile Keys Cache	Updates the local Mobile Keys cache and recovers the status from the Cloud. To be used in case the Mobile Keys are unstable.

8.2. Mobile Keys

Requirements

- A Mobile Keys license should be active in the system
- The webserver should be connected to the Internet
- Mobile Keys are compatible with all DOM ENiQ locking device that are BLE-compatible and have firmware version v5.4 or higher
- A Mastercard is registered to the system. To register a Mastercard, follow instructions here: Create special cards
- The firewall should allow ENiQ Software to connect to the following URLs: https://identitytoolkit.googleapis.com/ ; https://securetoken.googleapis.com/ ; https://login.tapkey.com/ ; https://my.tapkey.com/

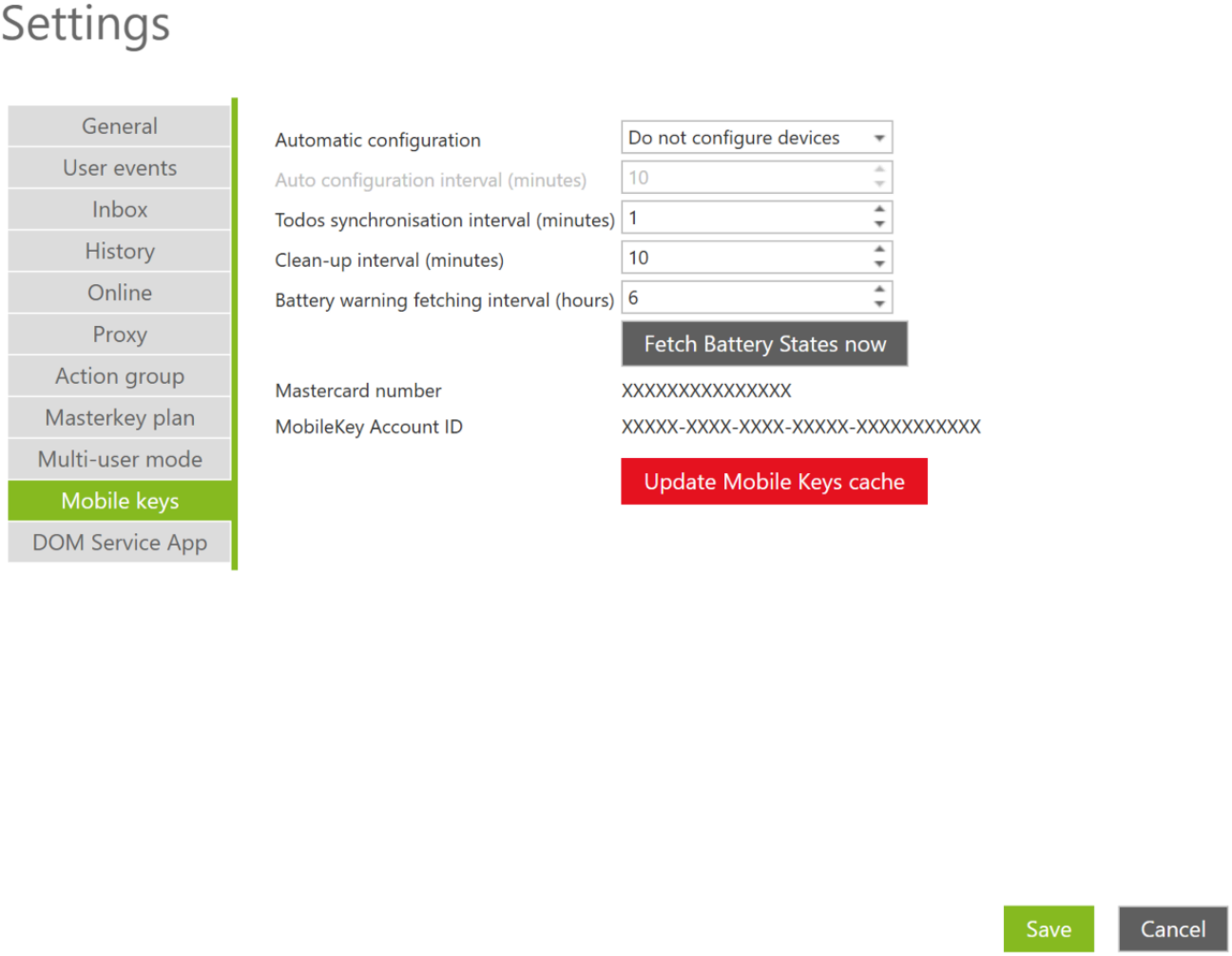
! Only with a valid mobile key license is it possible to set up mobile keys. For Mobile Keys, after the license has been updated in *System/License information*, the ENiQ AccessManagement Server needs to be restarted.

! To use the Mobile Keys functions, the web server must be connected to the Internet.

Enable mobile keys in the system

To activate Mobile Keys in the system, proceed as follows:

- Click on “System” in the navigation bar.
- Select the menu item “Settings”
- Under the tab “Mobile Keys” the settings appear



You can adjust the settings here:

Automatic configuration:

- You have the option of configuring no devices, only AccessManager or all devices. If you have selected “Configure all devices” or “Configure ACMs only”, you do not need to make any further settings on the devices. If “Do not configure devices” is selected, the devices must still be configured manually when using Mobile Keys (see below).
- Once you have adjusted all the settings, press the “Execute sign up” button
- After a successful message, a success text appears in the text field below the button
- If you receive an error message, please see what is missing or still needs to be configured
- Click on “Save” to complete the process

Auto-configuration interval (minutes):

- Time interval in which the system checks whether new devices can be bound to the cloud (default is 10 minutes).

Todos synchronisation interval (minutes):

- Time interval in which the system checks whether new information (e.g. new authorizations) is

available for the cloud (default is 1 minute).

Clean-up interval (minutes):

- Time interval in which it is checked whether devices in the cloud can be decoupled if they have only been deleted from the database but not decoupled via Device Management (default is 10 minutes). This process allows devices that have only been decoupled with the Mastercard to be added to the cloud again (e.g. in another system)

Battery warning fetching interval (hours):

- Time interval in which the software connects to the Mobile Keys cloud in order to fetch the latest battery warnings retrieved from devices by the DOM Key mobile app (default is 6 hours). This allows that the device battery warnings are automatically retrieved and displayed in the software, simply by users unlocking doors with the DOM Key app. You can also force fetch the latest battery warnings by clicking on “Fetch Battery States now” button.

Update Mobile Keys cache:

- The cache is a mirror database of the cloud so that synchronizations can be carried out more quickly. If problems occur during synchronization, the button can be pressed and the mirror database is deleted and recreated. After pressing the button, it cannot be pressed again for 2 hours.

If you have the impression that changes have not been synchronized to the cloud, please check the ToDo list “Mobile Keys” or the “Inbox” to see whether actions are still being carried out.

Prepare devices for Mobile Keys

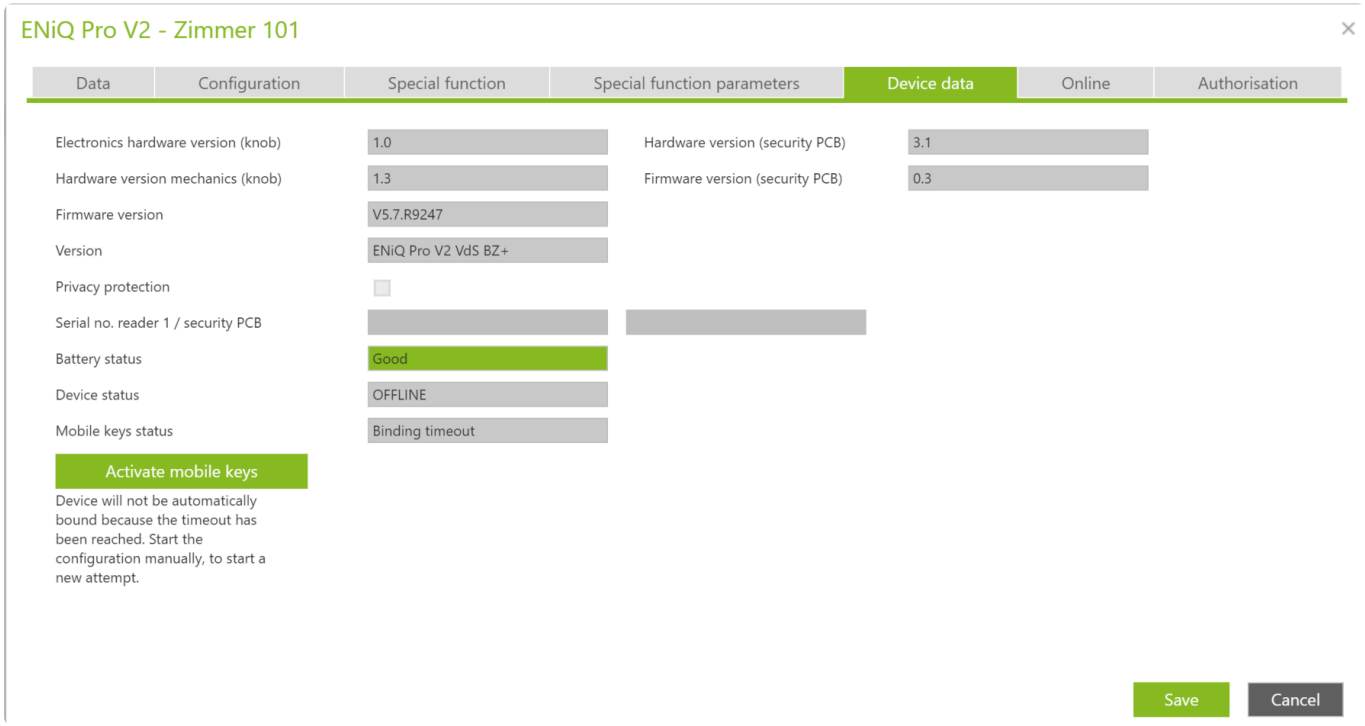
- Click on “Access control” in the navigation bar
- Select the “Devices” menu item

The Devices menu opens

- Select the desired device and click on Edit

The Data tab opens

- Switch to the “Device data” tab



- Here you click on the button “Activate Mobile Keys”

After that you will get a success message or a hint what still has to be set up

- Finally click on Save
- Afterwards the configuration of the mobile keys must be programmed to the devices within 7 days.

Create Mobile Keys

To create and assign mobile keys, proceed as follows:

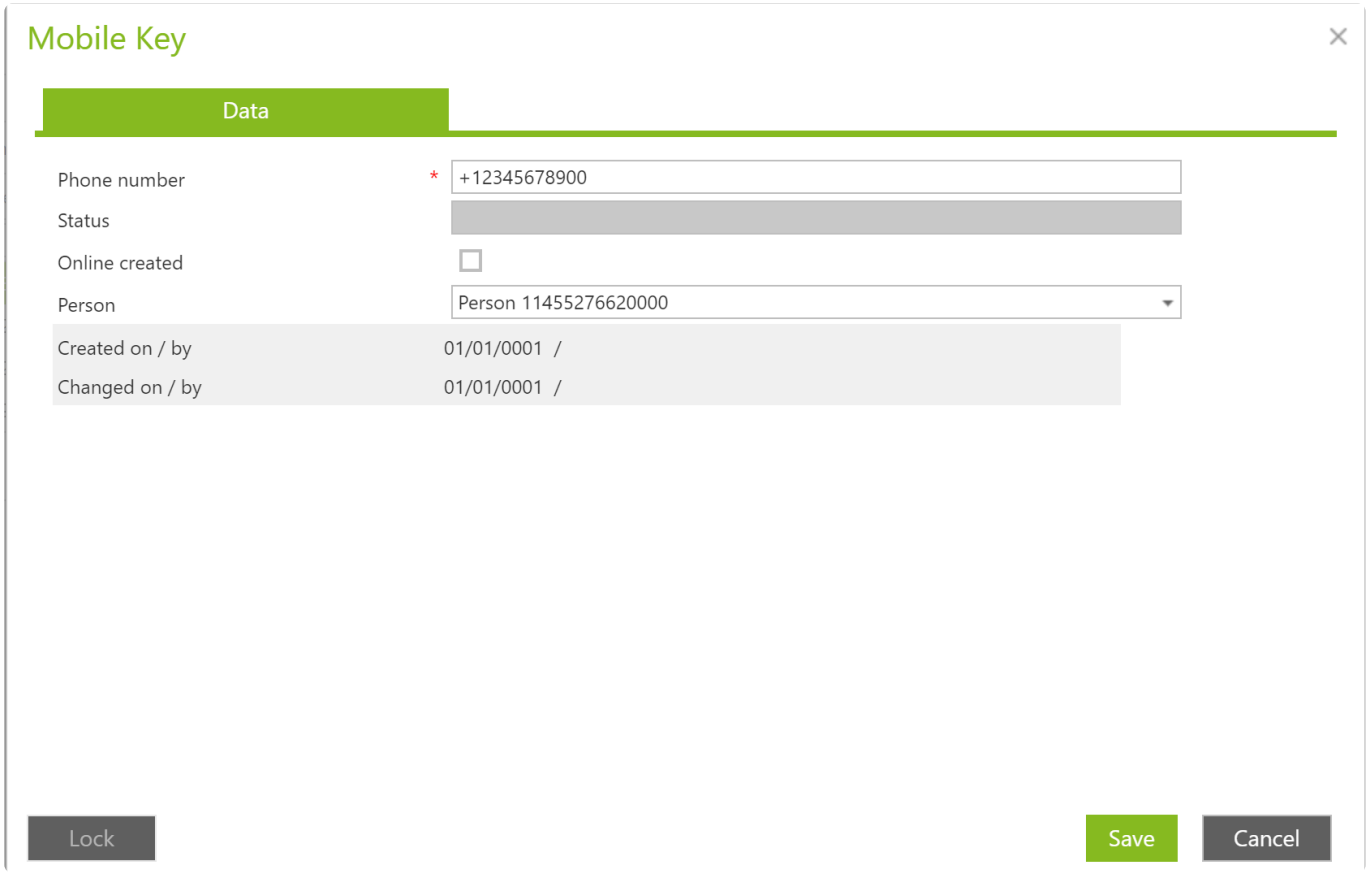
- Click on “Access control” in the navigation bar.
- Select the “Mobile Keys” menu item

The Mobile Keys menu opens

- Click on “Add”

The Mobile Key tab opens

- Now enter the phone number here
- Then select the person who should be assigned a mobile key



- Finally click on Save

A Mobile Key works like a data on card transponder.

8.3. Offline Synchronisation

Synchronization is performed using the ENiQ Device Management software or the DOM Service mobile application.
The ENiQ Device Management program is installed on a laptop. The ENiQ Device Management software or the DOM Service mobile application are synchronized with the central database.
The laptop or smartphone can then be disconnected from the network, and offline devices can be programmed locally according to the task list.
During the programming process, device data (events/status) are also automatically read.
This data can then be imported back into the central database via ENiQ Device Management or the DOM Service application.

8.3.1. Configuration

SET UP PROGRAMMING CLIENT (ENiQ DEVICEMANAGEMENT)

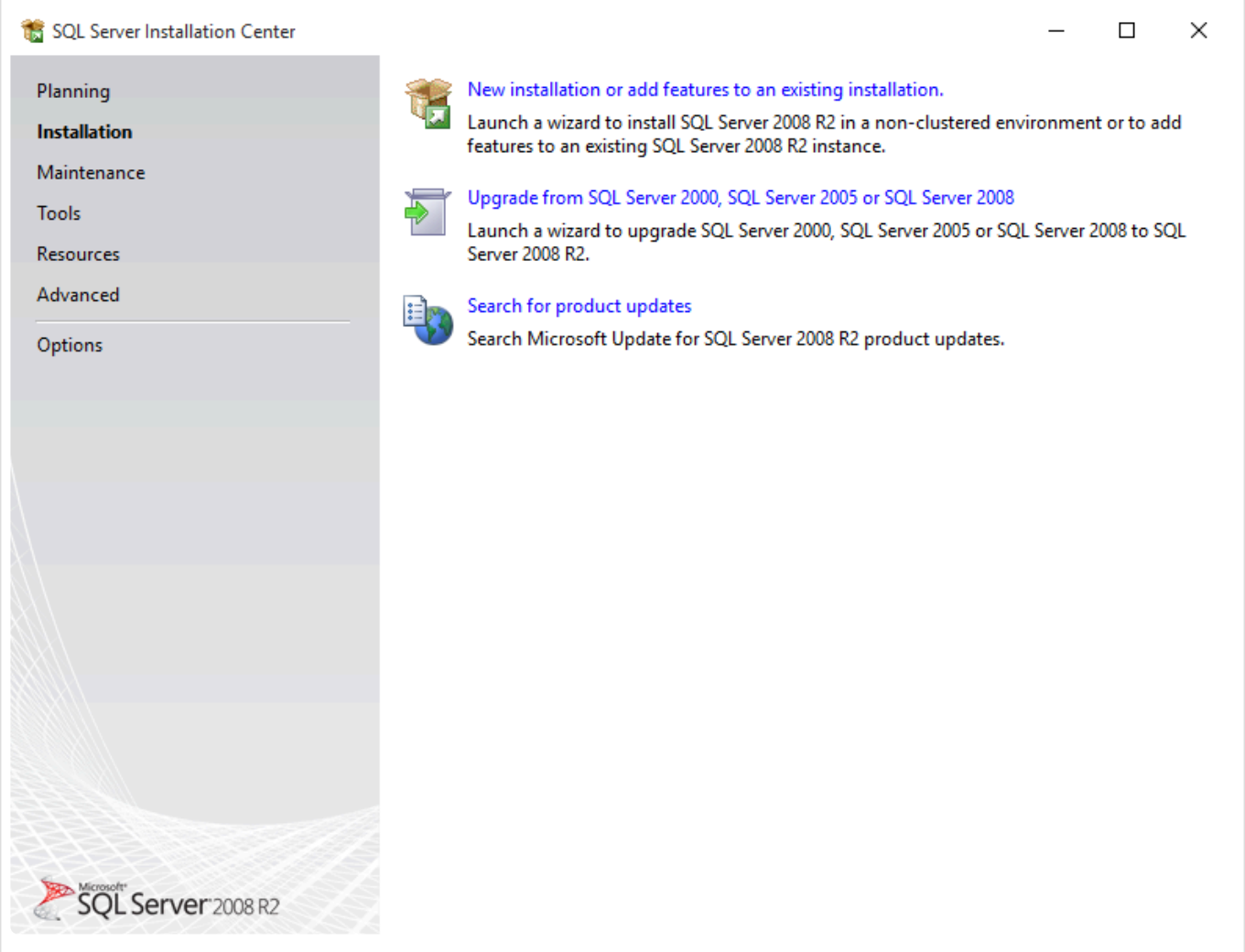
To enable offline synchronization in an installed ENiQ DeviceManagement, the following manual installation steps must be performed:

An instance of SQLServer Express 2008 R2 or 2012 32bit must be installed that uses the same database name (default is: GENIUS) as the server version.
This database must be made known to ENiQ DeviceManagement by entering the connection strings in its configuration.

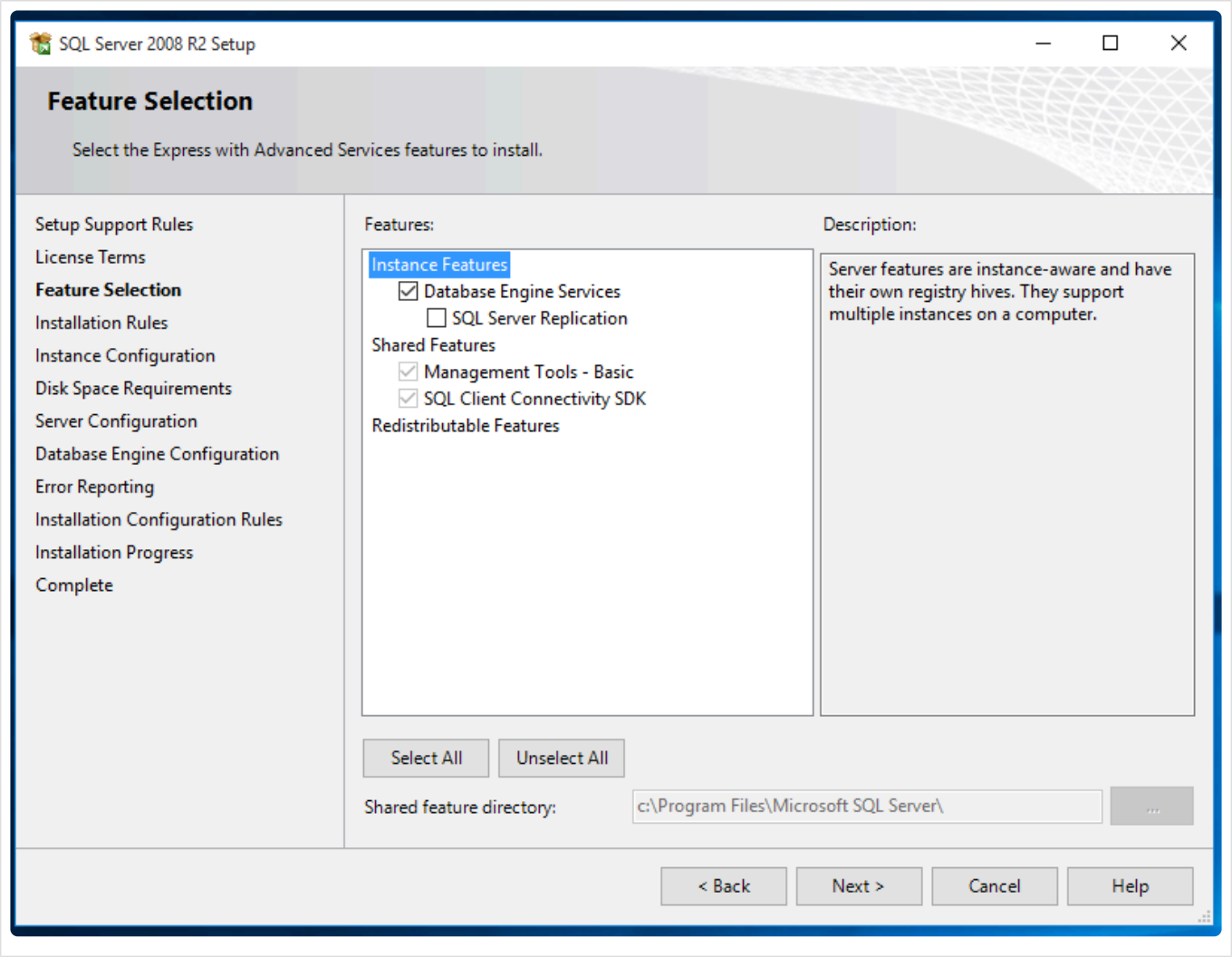
INSTALLATION OF THE SQL SERVER INSTANCE

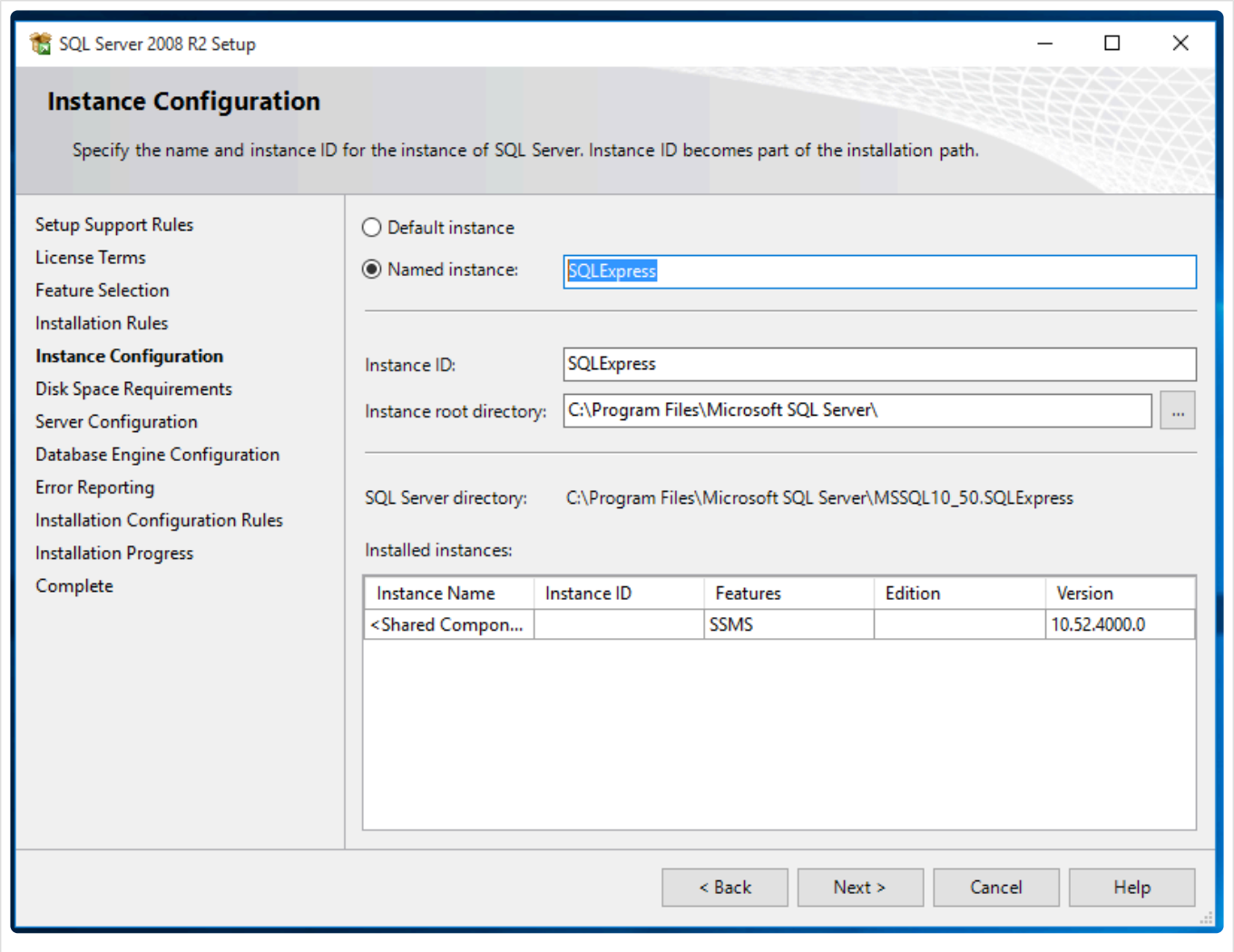
If you have already installed the ENiQ software, the SQL Server 2008 R2 32Bit Installer is located in the directory of the ENiQ software:
(Default: C:\Program Files\DOM Sicherheitstechnik\SQLServer or C:\Programs Files(x86)\DOM Sicherheitstechnik\SQLServer).

After running the MS-SQL installer, select the item
“New installation or add features to an existing installation.”

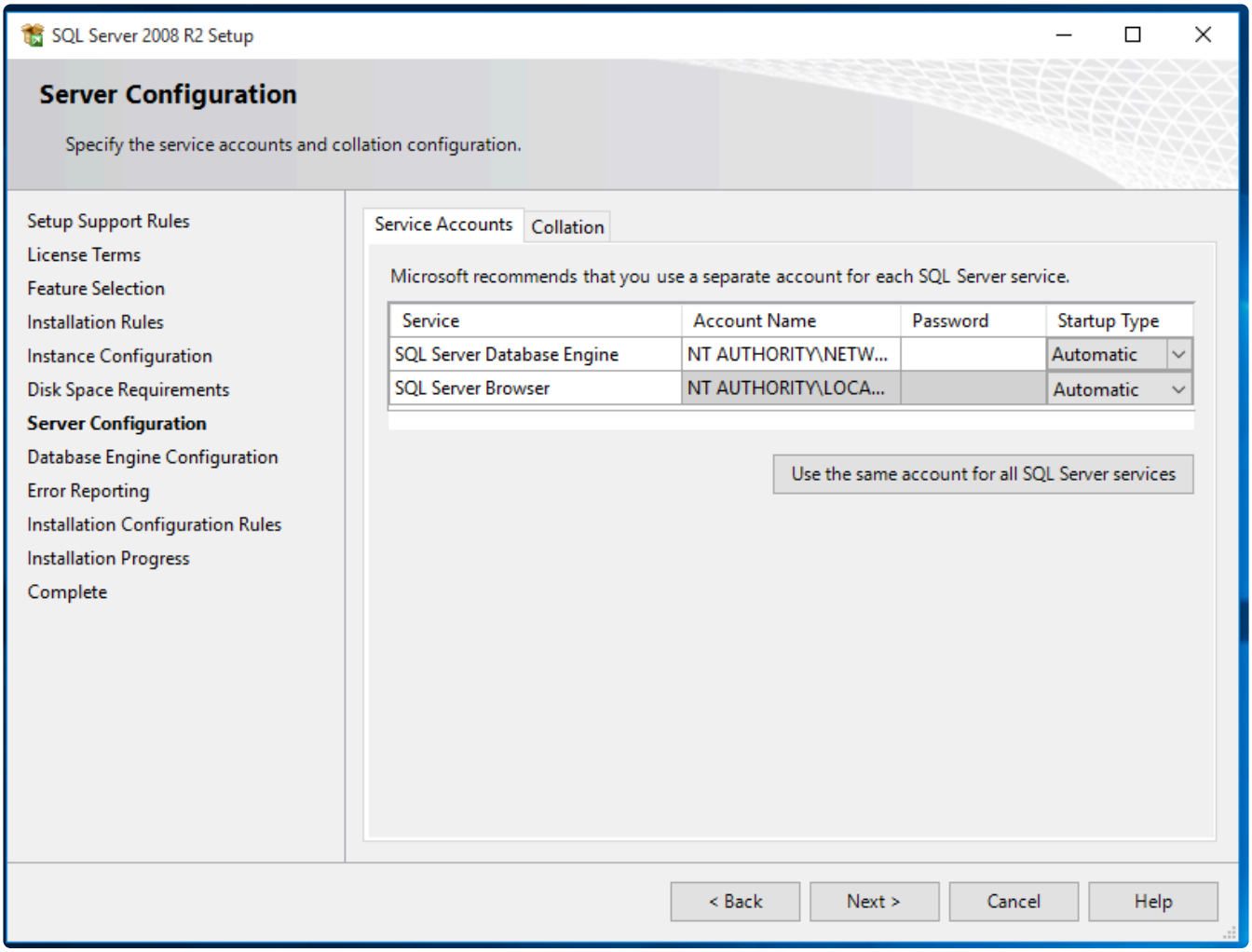


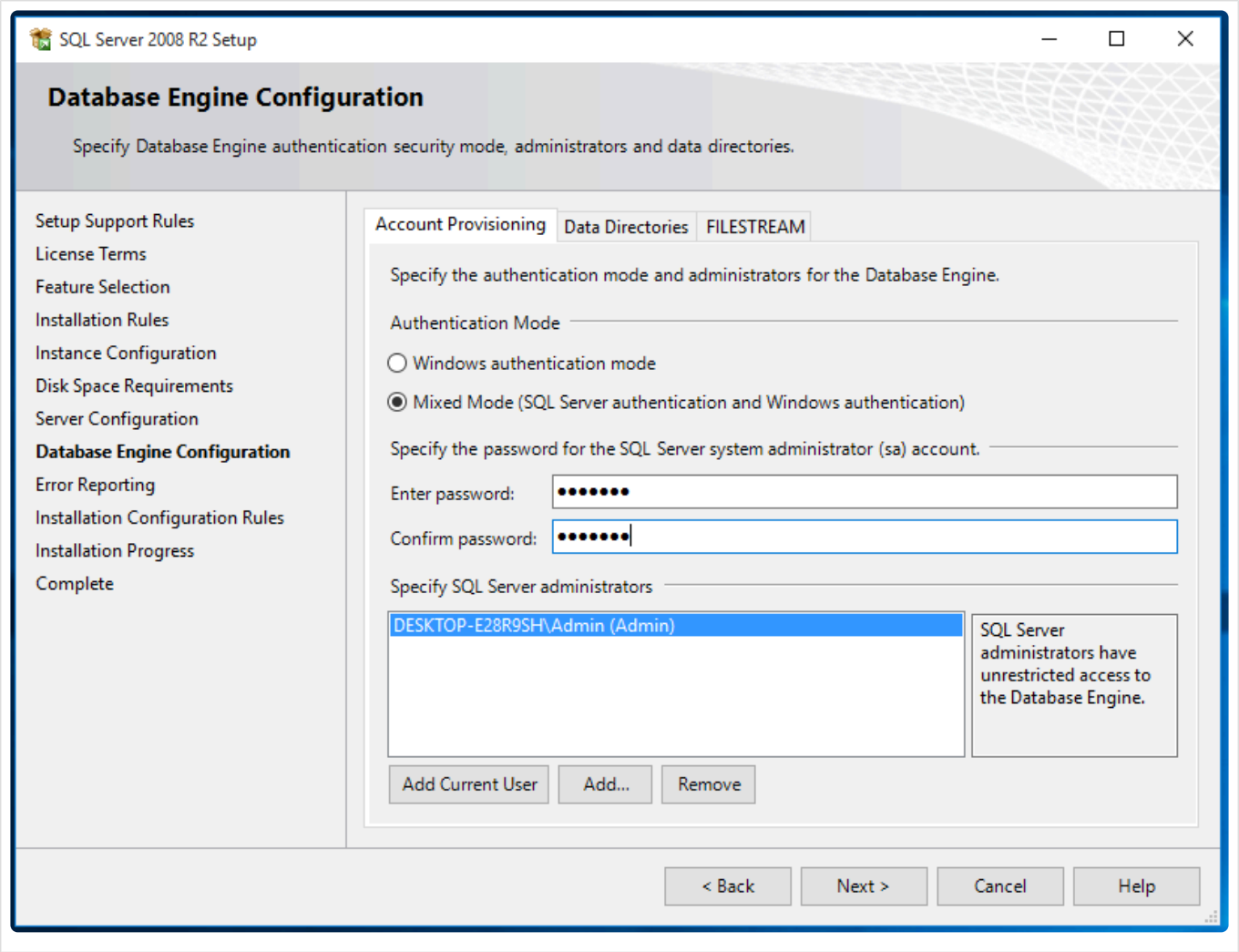
Select the combo boxes according to the image and continue the installation by clicking “Next”. In the next window fill in the field “Named instance” with a freely selectable instance name and continue the installation by navigating to the next window.





The following two steps will complete the MS SQL Server installation. First set the server configuration to “Automatic” as shown in the picture, then in the next window set the Authentication Mode to “Mixed Mode” and choose a password for the “sa” user.
This password can be independent of the server installation.


SQL Server 2008 R2 Setup
Server Configuration
Specify the service accounts and collation configuration.
Setup Support Rules
License Terms
Feature Selection
Installation Rules
Instance Configuration
Disk Space Requirements
Server Configuration
Database Engine Configuration
Error Reporting
Installation Configuration Rules
Installation Progress
Complete
Service Accounts
Collation
Microsoft recommends that you use a separate account for each SQL Server service.
Service
Account Name
Password
Startup Type
SQL Server Database Engine
NT AUTHORITY\NETW...
Automatic
SQL Server Browser
NT AUTHORITY\LOCA...
Automatic
Use the same account for all SQL Server services
< Back
Next >
Cancel
Help



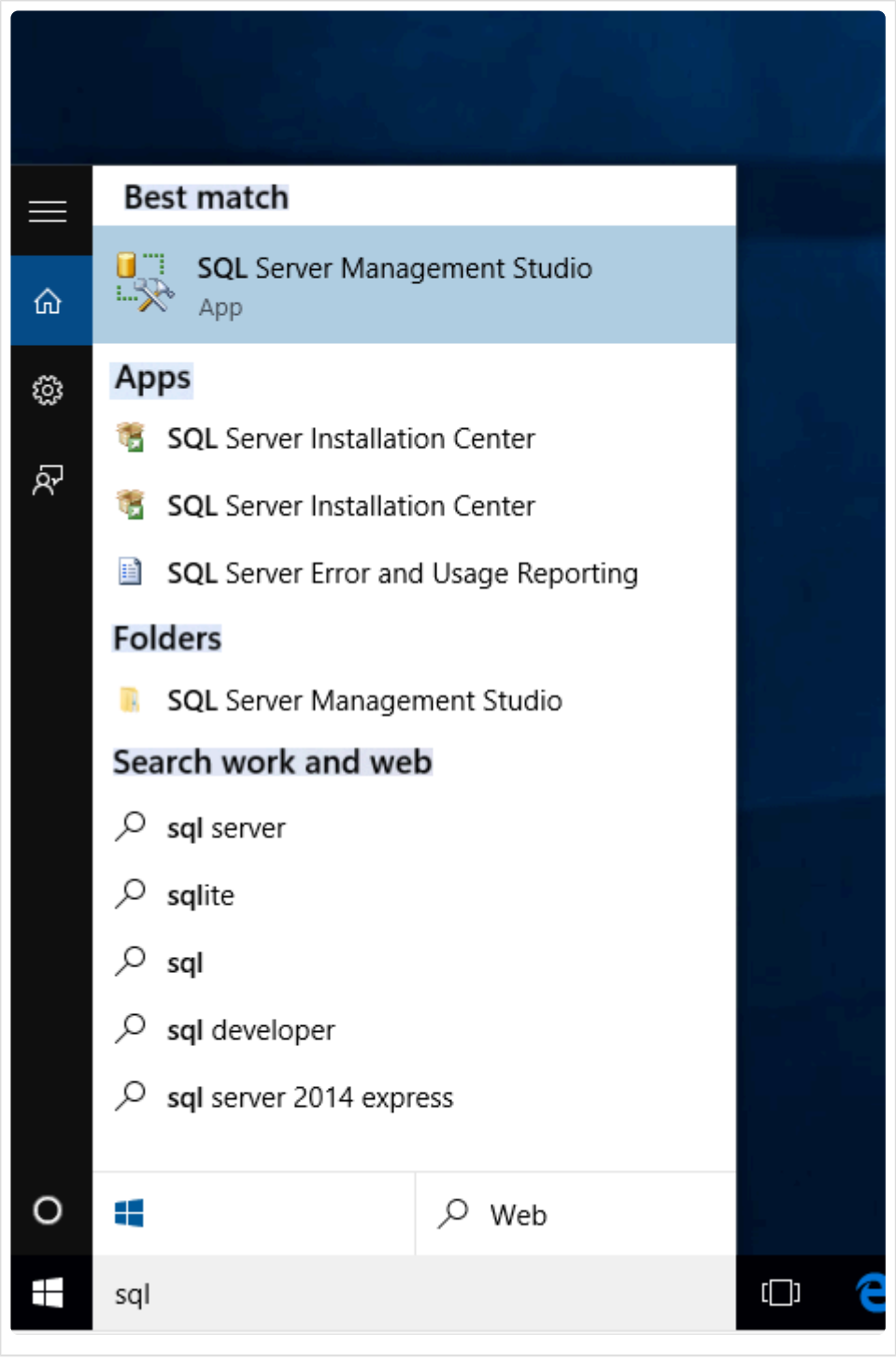
ENTER THE DATABASE CONNECTION DATA INTO THE CONFIG FILE OF THE ENiQ DEVICEMANAGEMENT :

Open “DOMGeniusDesktop.exe” under C:\Program Files\DOM Sicherheitstechnik\DOM Genius Software\Desktop
(or C:\Program Files(x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop).
There you will find an encrypted ConnectionString.

Now add the following string one line below this ConnectionString:

add name=“Genius-Offline_Online_MSSQL_2008” connectionString=“Data source=(local)\INSTANCENAME;user id=sa;password=MYPASSWORD;initial catalog=Genius; Persist Security Info=true;” providerName=“MSSqlServer”

Replace the words INSTANCENAME and MYPASSWORD with the instance name and password chosen during installation.
“Catalog” corresponds to the database name. This must match the database name of the Genius database on the server installation. By default, this is “Genius”.
The editor can now be closed.
Then an empty GENIUS database must be created via SQL Server Management Studio.

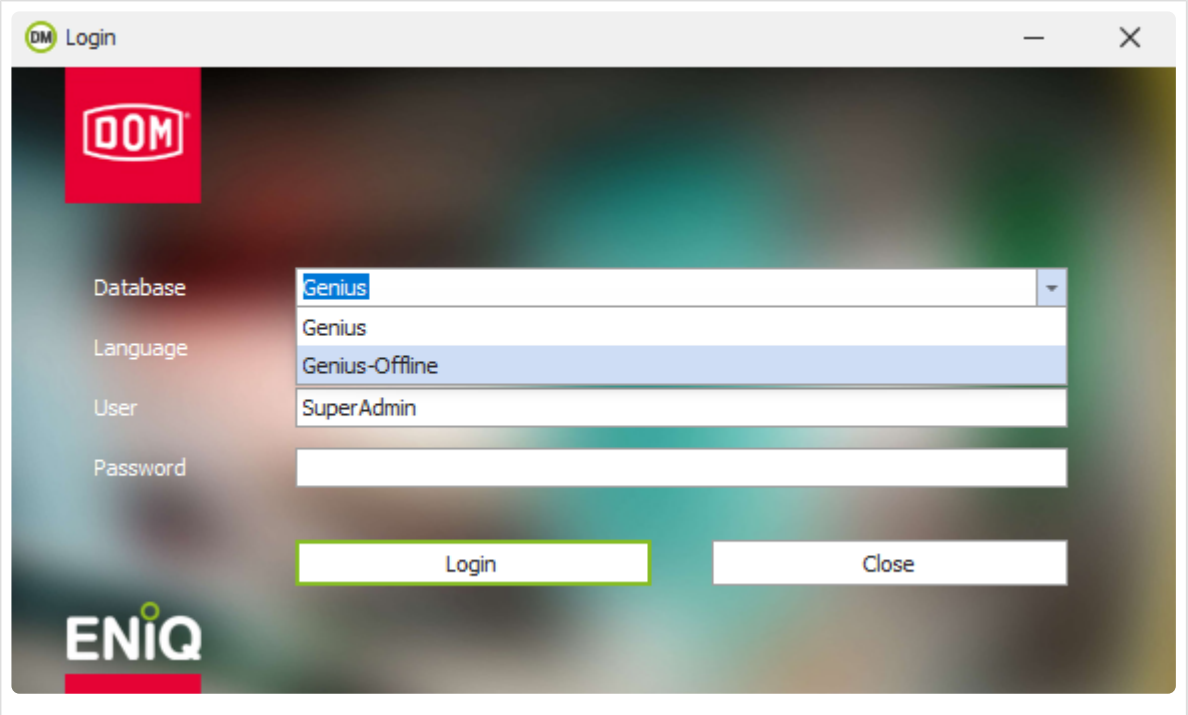


To do this, open the SQL Server Management Studio. After successful login, right-click on “Database” and then on “New Database”.

Enter GENIUS in the “Database Name” field and finish the process by clicking “OK”.

START AND TEST THE ENiQ DEVICEMANAGEMENT – CLIENT

In ENiQ DeviceManagement the additional entry “Genius-Offline” now appears under Database.



Genius is the “Online” server instance;
Genius-Offline is the local “Offline” server instance

8.3.2. Implementation

ENiQ DEVICEMANAGEMENT: PERFORMING OFFLINE SYNCHRONIZATION

Offline synchronization is necessary to synchronize DOM devices that are not permanently connected to the server (i.e. do not have an online connection).
This document contains step-by-step instructions on how to perform offline synchronization. The prerequisite for this is that you have successfully set up offline synchronization.

DATA SYNCHRONIZATION

Please start the ENiQ DeviceManagement.

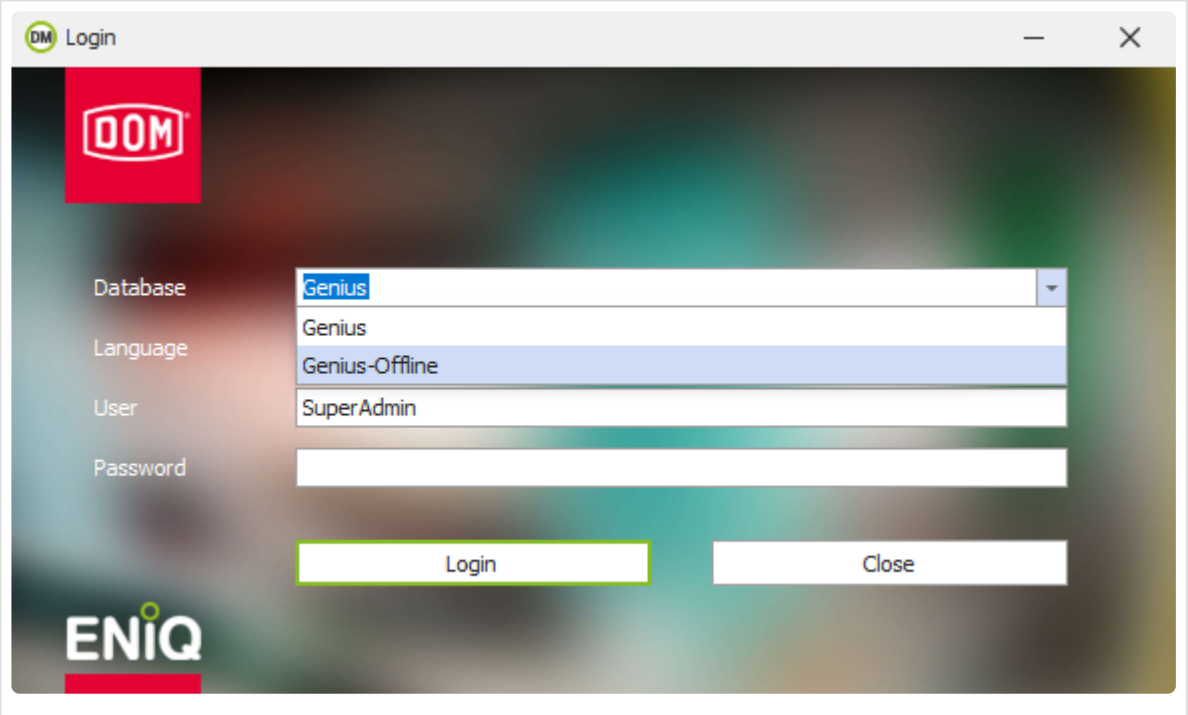
DATA SYNCHRONIZATION OFFLINE-CLIENT

To use the ENiQ Device Management client offline without an active database connection the following steps have to be done:

- Start the ENiQ Device Management with a server database connection and synchronize the database.
- After synchronization restart the ENiQ Device Management client and connect to the offline database.
- Program the devices
- When you have an active database connection again, restart the ENiQ Device Management client and connect to the server database. now synchronize the data.

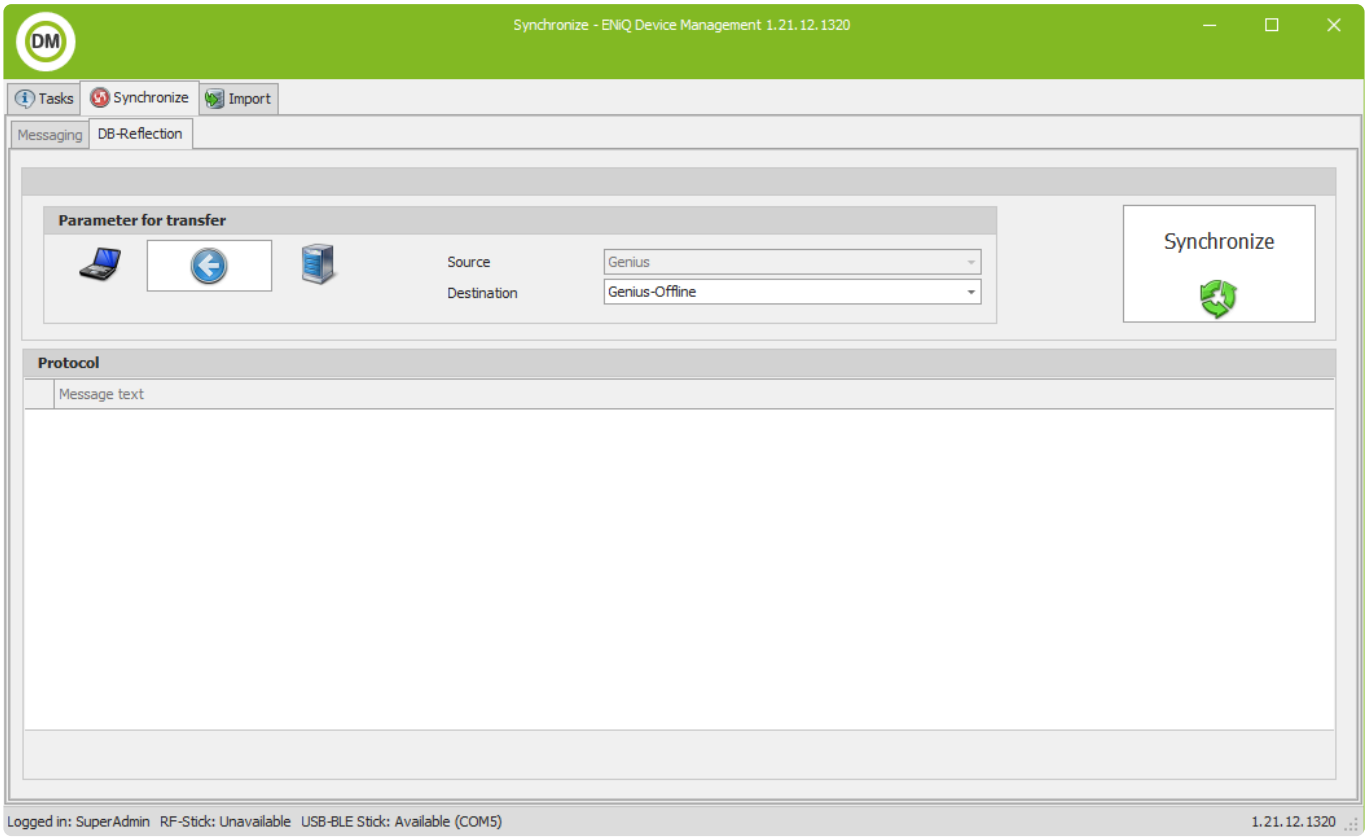
ENiQ DEVICEMANAGEMENT-CLIENT FOR OFFLINE SYNCHRONIZATION

start ENiQ DeviceManagement-Client select database “Genius”.



Click on the “Synchronize” tab. The field Target must contain “Genius-Offline”. Press the Synchronize button.

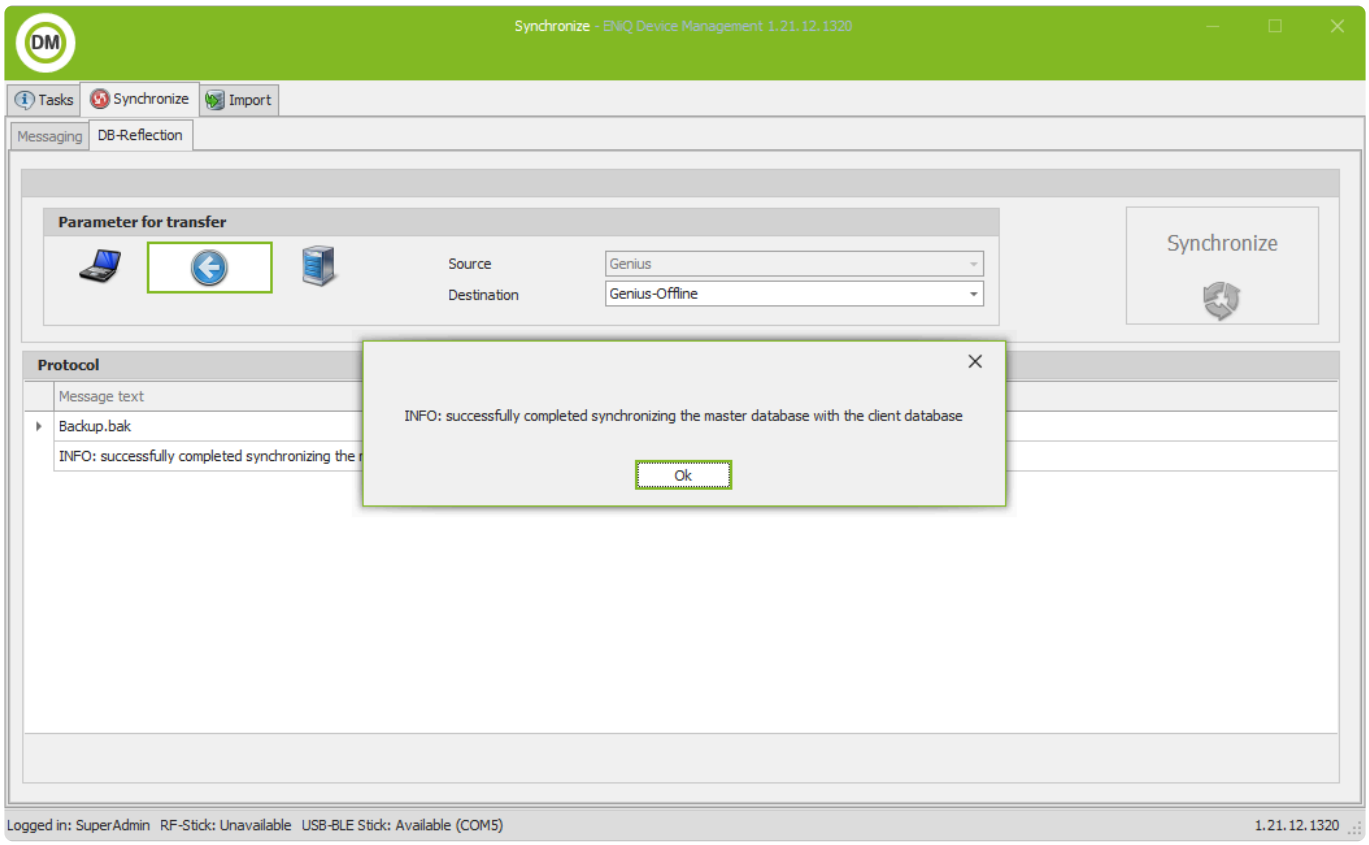
|



A field will appear showing the progress.
Depending on the size of the database and the network speed, synchronization will take time.

If no error message appears in the tip text, the synchronization was successful.

This means that the synchronization is complete.



USE ENiQ DEVICE MANAGEMENT OFFLINE

Start ENiQ Device Management and select the database “Genius-Offline”

Then program the devices as usual.

ENiQ DEVICE MANAGEMENT: SYNCHRONIZE OFFLINE DATA BACK TO SERVER

Start ENiQ Device Management and select the database “Genius”.

Click on the “Synchronize” tab. The field Target must contain Genius-Offline. Press the Synchronize button.
The arrow between the laptop computer icons now briefly changes direction and points to the computer instead of the laptop.

Depending on the size of the database and the network speed, the synchronization will take some time.
If no error message appears in the message text, the synchronization was successful.

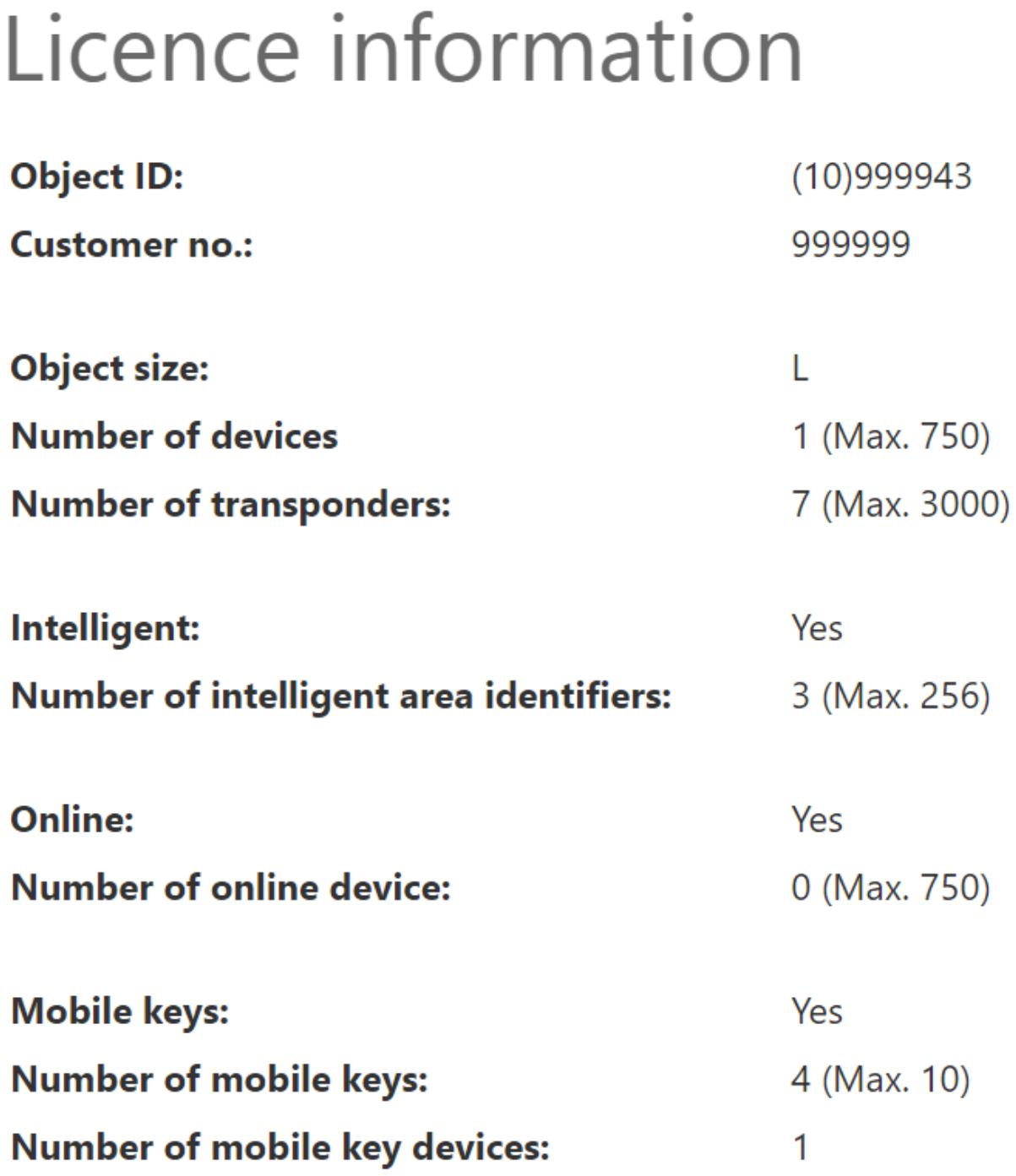
This means that the synchronization is completed

8.4. Extend license

Display license information

To view the license information, do the following:

- Click “System” in the navigation bar.
- Select the menu item “License Information”.



The current license information will be displayed.

In this sub-menu you can also extend the program with additional functions. For this purpose you can activate the corresponding functions by entering a license key.

To activate additional functions, proceed as described in the “Extend license” section.

Extend license

The modules of the software differ mainly in the number of devices and transponders to be managed. By extending the license, you can increase the number of devices and transponders that can be managed.

Standard module	Number of devices	Number of transponders
Module S	max. 25	max.100
Module M	max. 125	max.500
Module L	max. 750	max. 3000
Module XL	max. 9500	max. 32.0000
Module XXL	>9.500	100.000

In the menu item “License information” you can extend the existing scope of the software. For this you need an appropriate license key.

To extend the license, proceed as follows:

- Click on “System” in the navigation bar.
- Select the menu item “License information”.

The current license information will be displayed.

- Enter the license key received from the manufacturer.
- Click on the “Activate” button.
- Exit the program.
- Start the program again.
- Log in again.

The extended license is now available.

When decreasing the Mobile Keys license, the number of currently assigned Mobile Keys should not be superior to the new license. An error message will be displayed asking to unassign additionnal Mobile Keys.

8.5. Online commissioning

Prerequisites:

- Installed ENiQ AccessManagement Software

> ! For the operation of an online system an online license is mandatory.

General notes

- Port 47119 must be released in the firewall. Please discuss this with your system administrator.
- If VMWare is used, a port forwarding from 47119 to 47119 must be set up under Edit ␣ Virtual Network Editor for NAT.

General settings

- First check if your ENiQ software license allows online operation. To do this, open the following menu in the ENiQ AccessManagement:
  “System” -> “License information”
- In the list there must be a “Yes” at the item “Online”. The number of possible online devices corresponding to your license is also displayed there.
- If you need a license extension, please contact your dealer or the manufacturer.
- Install services OnlineMaster and OnlineSlave

These services are two new ENiQ Windows services that must be installed in addition to the existing ENiQ Windows services.
The services are either copied to the PC automatically during the ENiQ installation, or in case of an older installation the files are copied to the PC via ENiQ Updater.

The service DOM.OnlineMaster must be installed on the same computer as the ENiQ web user interface.
The service DOM.OnlineSlave must be installed on a PC that is accessible via network for the devices and the ENiQ software. This can also be one and the same PC. (1-PC installation)

The services are both installed according to the same pattern:

So the following steps have to be executed only if this does not work:

1. Open the folder containing the OnlineMasterService or OnlineSlaveService programs:

- Online Master Service:
  “C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\OnlineMasterService \”

- Online slave service:
  “C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\OnlineSlaveService\”

2. Then run the program (DOM.OnlineMasterService.exe or DOM.OnlineSlaveService.exe) as administrator.
   (Right click -> Run as administrator)

3. Please answer the question whether the program should be installed as a service with “Yes”.

Service setup

If you want to perform a manual installation (i.e. without ENiQ installer), then you have to make the following adjustments:

1. In the Genius directory (C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software) under Web, the web.config file must be opened in the editor.

2. Here you have to search for the line that starts with

3. The encrypted connection string that is in the quotes after ConnectionString must be copied to the clipboard. Example:
   connectionString=“TheCopyHere”

4. Now must be changed into the directory OnlineMasterService and open here the file DOM.OnlineMasterService.exe.config in the editor.

5. Now here must again the line, which begins with
   must be searched for.

6. The content that was copied before must now completely replace the content between the quotes:
   connectionString=“HereReplace”

7. Save the file afterwards!

Enter slave service in the ENiQ software

In the ENiQ AccessManagement every slave service must be entered.

1. For this purpose create a new service in the menu under Online -> Service info. (Add)

2. Enter a name under Description.

3. Under IP address, the IP address of the computer on which the slave is running must be entered. If this is the same computer as the master, then 127.0.0.1 must be entered.

4. As external IP address the address must be entered under which the devices can reach the online slave service.

5. DNS name can be left blank. Here the name of the computer could be used.

6. Port is the port under which the service can be reached. If the configuration was not changed, this is 47118.

7. Then save.

It may take a moment for the master to connect to the slave service, as this only happens at regular intervals.

Set up ACMs / RF-NetManager

Prerequisite: The devices should already be included and coupled via desktop software.

On the device's page under the Online tab, the Online checkbox must be set. If the tab is not visible, the license may not be correct.

1. This will make the Online Programming button visible.

2. In addition, the status of the device is queried regularly.

Make settings on the Online tab.

1. The Alivetime is the time how often the device reports automatically. This can simply be left at the default.

2. Set IP address of the device

3. Set the subnet mask of the device. (Default: 255.255.255.0)

4. Specify default gateway of the device.

5. Save

Transmit settings to the device via radio.

1. Open ENiQ DeviceManagement.

2. Execute programming.

3. The device can then be pinged under the set IP address.

Set up ENiQ Pro / Guard / Guard S / LoQ

Prerequisite: The ENiQ cylinder should already be found and coupled with the desktop software. There should already be an RF NetManager in the system.

1. Open the ENiQ Pro in the ENiQ AccessManagement under Access control ▭ Devices.

2. On the Online tab, set the Online checkbox.

   - The Alivetime is the time how often the device reports automatically. This can simply be left at the default. For the ENiQ cylinder this should be 15 minutes.

   - Assigned RF NetManager: Here you have to select the RF NetManager which should be used by the ENiQ Pro.

   - Save afterwards.

3. The ENiQ Pro and the RF NetManager must be programmed afterwards

8.5.1. Online functions

Use online functions

This menu is only available if you have activated a valid online license in the system.

Display live events

Here you can view the online live events in the system.

To view a list of live events, proceed as follows:

- Click on “Online” menu in the navigation bar.
- Select the “Live Events” menu item

The “Live Events” list will open in a new window.

- To close the “Live Events” list, close the window

Open door
If you select a device in the area tree that is switched online, you can see a button “Open door”, which can be used to unlock the device. The ACM receives the command directly over the network. The battery powered devices receive the command by radio from the RF NetManager, which receives it directly via the network.

Todo List / Online Programming
If an ENiQ software operator changes an authorization, for example, this change is listed in a todo list. There is a special todo list for the online devices. If you have activated the option “Release todos automatically” in the online settings, then you can see in this todo list which tasks are waiting to be executed. If you have not activated this option, you will have to release the waiting tasks on the page using the “Release all” button. This will allow you to collect changes and transfer them afterwards.

Configure settings for online functions

To view the “Online Settings” options, do the following:

- Click on “System” in the navigation bar.
- Select the “Settings” menu item
- Select the “Online” tab

The available options will be displayed.

- If you activate the option “Release todos automatically”, any changes made to the permissions will automatically be transferred to the devices with the next Alive
- Under “Alivetime of the online services” you can set the time interval at which the system should automatically report to you

- Under “Maximum deviation of the device time to automatic reprogramming” you can set a tolerance value for the deviation of the device clock time from the system clock time

Service info

Here you can configure and add the following:

- Online services
- IP addresses
- Ports
- DNS

- Click on “Online” menu in the navigation bar.
- Select the “Service information” menu item

The “Online/Service information” menu opens.

- Click on the “Add” button

The “Data” tab opens.

- Enter a designation
- Enter the IP address if desired
- Enter a DNS name if desired
- Enter the corresponding port

Under “Version” you will see the current version.
Under “Last Alive on” you will see when the device last reported an alive in the software.
Under “Status of slave” you will see if the assigned device is online or offline.

- If you want to cancel the process without saving, click on “Cancel”.
- To accept the entries, click on “Save”.

- Switch to the “Assigned devices” tab.
  Here you can display the assigned devices.

- Click on “Save”.
- If you want to cancel the process without saving, click on “Cancel”.

8.5.2. Use online plug & play

Basics

In order to use the Online Plug & Play in a meaningful way, a DHCP server should be installed in the system, which automatically assigns an IP address to devices in the network. Otherwise the devices would report their default IP address (192.168.47.11) (but after the second device there would be IP address conflicts).

Power-connected devices (e.g. RF-NetManager) report directly to the system at regular intervals (default: once per minute) and are thus immediately recognized and displayed by the software.

RF Online Card (for V1 devices)
The RF Online card is intended to connect battery-powered terminal devices (e.g. ENiQ Pro) to an RF-NetManager. Internally, data about the cylinder is stored in the RF-NetManager. (assignment, key).

The card must first be read into the software using a desk reader. The locking media dialog opens which you simply confirm with “Save”. Then all devices must be programmed once so that the card is made known to all devices.

In the uncoupled state of the RF-NetManager, it is possible to measure the radio quality of the radio link. In addition, the card functions for simple opening (building locking) in the case of uncoupled cylinders. When the RF-NetManager is coupled, a permanent connection is established between the RF-NetManager and the cylinder.

A battery-operated terminal device (e.g. ENiQ Pro) will first be shown the RF-Online card after the RF-Online card has previously been shown to the RF-NetManager (via which the respective device is to connect to the ENiQ software).

The battery-powered device then performs various device checks and is finally “switched online”. From this point on it also sends regular life signals (“Alives”) (default: every 15 minutes) to the system and is thus displayed on the device coupling page.

RF Online Card (for V2 BLE devices)

The RF online card does not have to be created in the software. By holding the card on the battery-powered devices, the BLE and online interface is permanently activated. The devices report via an RF NetManager V2 (BLE) in the system and appear in the sub-menu “Online / Couple devices”.

Couple devices menu

In the ENiQ-AM software there is a menu item “Couple devices” in the Online menu. Here all new devices are displayed, which have been detected automatically by the system (via radio or Ethernet). At this point, important data (such as the design or the external and internal length) of the new devices are queried and displayed.

On this page, the automatic coupling and programming of the device can be triggered by selecting the

respective device and clicking the “Couple device” button.

This process takes place in several steps (9 in total). The page does not refresh automatically, but by clicking on Reload page the current status of the process is queried and displayed.

License checks are also performed during this process. Coupling will not be performed if there are any license violations (e.g. trying to use more online devices than the license size allows).

In addition, please note that before battery-powered end devices are coupled, the assigned RF-NetManager must first be coupled. A message will appear if an attempt is made to couple a device that is reporting via an RF NetManager that has not yet been coupled.

After the process is completed, the device is no longer displayed on the “Couple devices” page. It is now coupled and programmed and therefore ready for use. Changes affecting the device will be programmed into the device via the online ToDos from this point on.

Note: By showing the wake-up card to online devices, the device reports to the ENiQ-AM software via Alive, thus individual processes can be accelerated or continued (e.g. the processing of ToDos only happens when the device reports via Alive or the online commissioning is continued when the device reports via Alive)

8.6. Server & Client Installation

8.6.1. Client Installation

This chapter is intended to help the administrator to install and configure the ENiQ software as a client on the target computer.
A client can be installed in three variants:

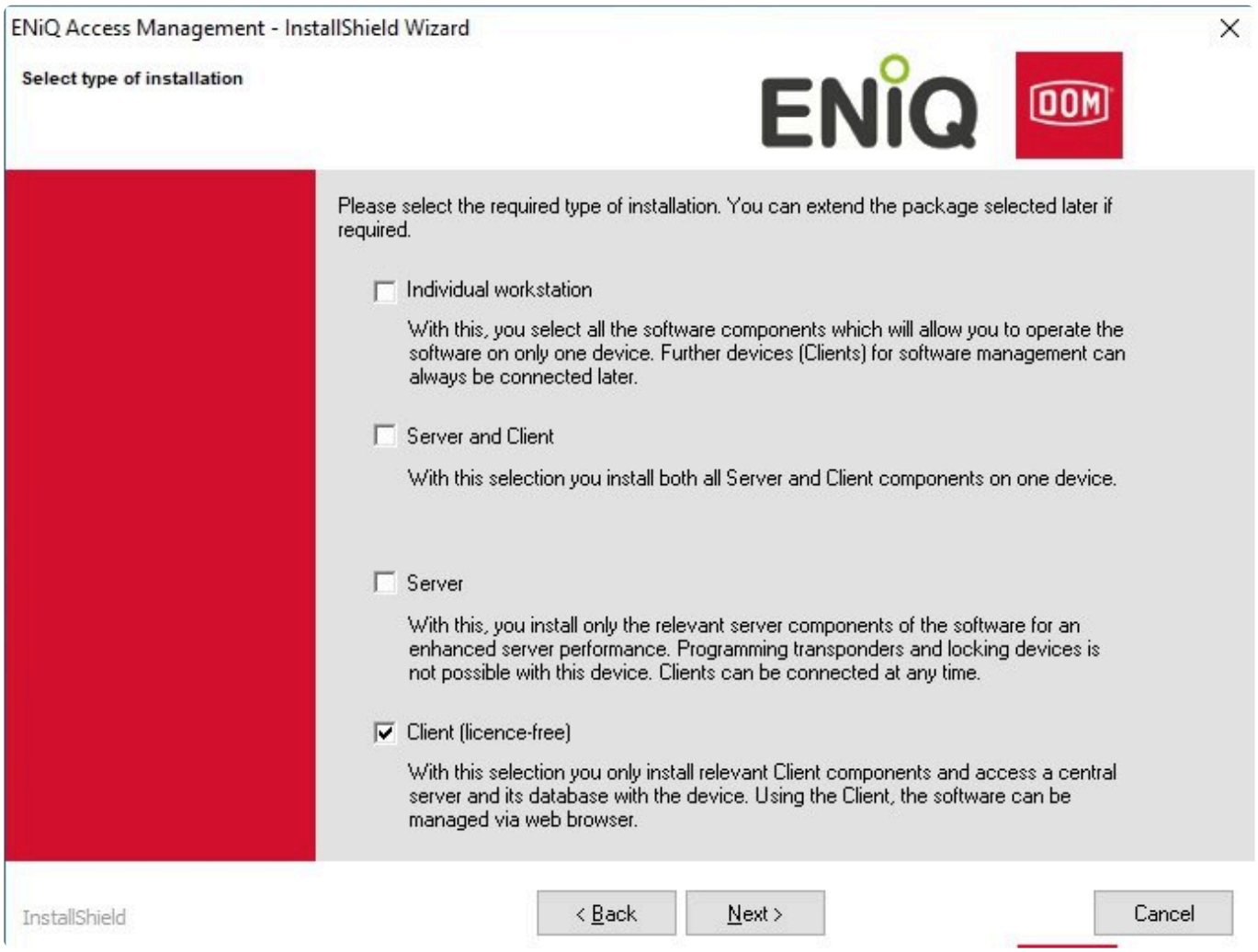
1) Only authorization management of users and transponders. For this you only need a web browser with a local connection to the server. This variant does not need to be installed.

2) Only authorization management additionally with a desk reader. Transponders can be read and written by the client. This variant must be installed.

3) Offline device management with ENiQ Device Management: Program authorizations or retrieve events from the connected devices.
(2 and 3 can be combined)

CLIENT INSTALLATION

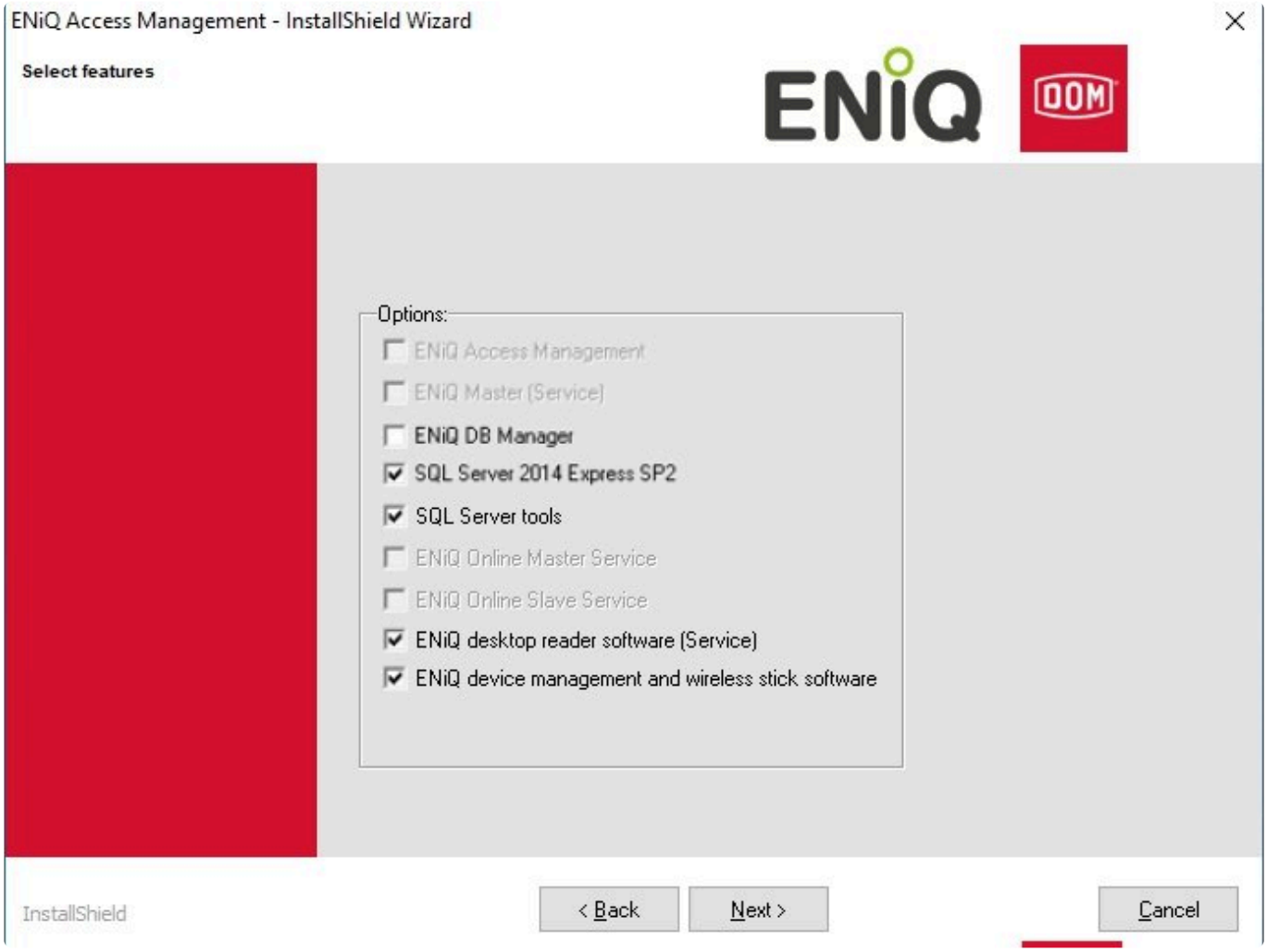
No license key is required for client installation. Check the box “Client (license free)” and click on “Next”.



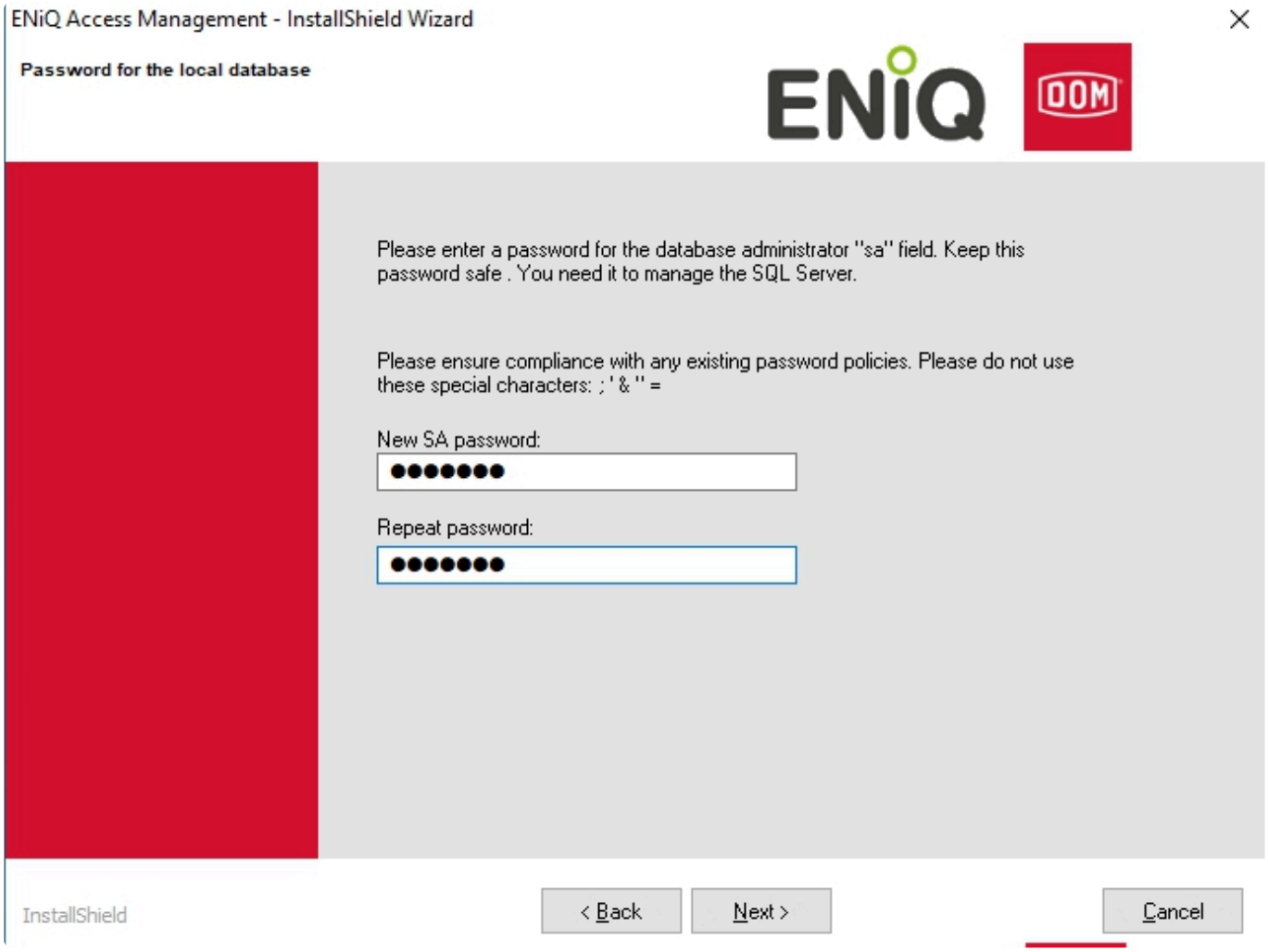
At the selection screen the necessary features for a client installation are selected:

These include the features

- SQL Server 2014 Express SP2
- SQL Server Tools
- ENiQ desk reader software (service)
- ENiQ Device Management and Wireless Stick Software

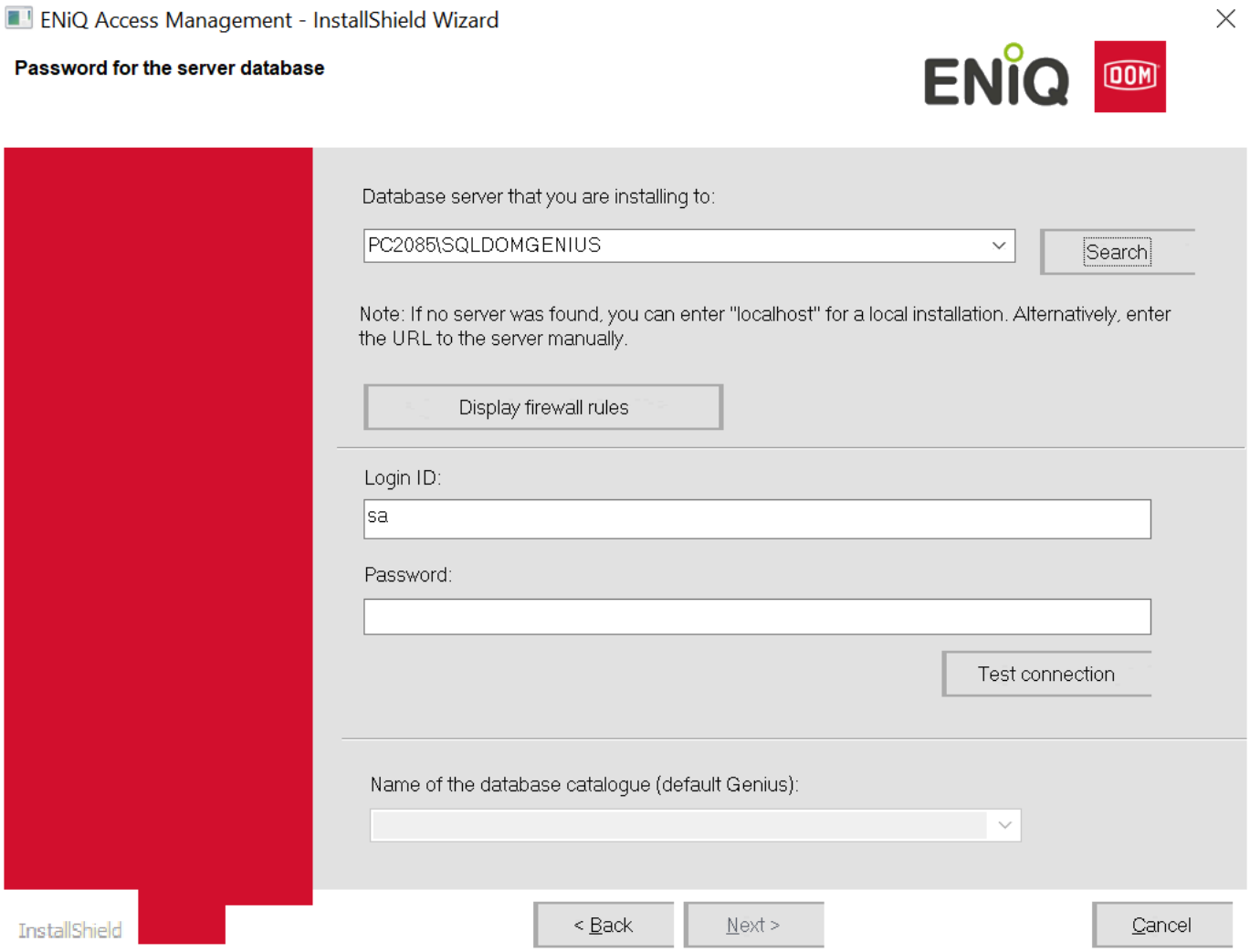


If “SQL Server 2014 Express SP2” was selected in the last step, the password for the local database will be requested in the next step.



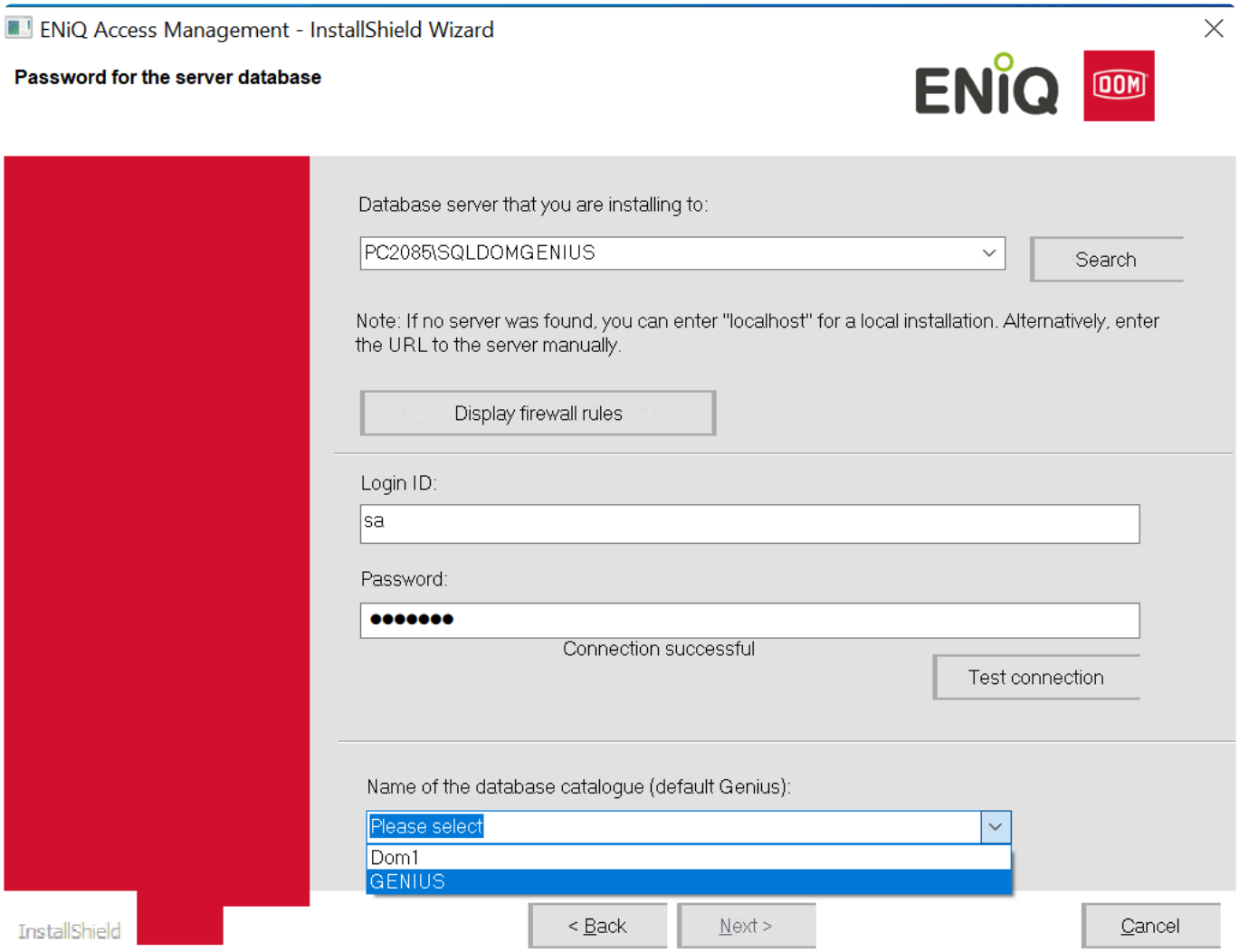
After that the database selection dialog appears. Here you have to enter the credentials for the database connection:

If you click on the upper “Search” button, a window appears with all available SQL database servers – among them should be our DB server.



After selecting it and entering the SQL Server authentication data (“SA” and the password) from the server installation, clicking the “Test Connection” button will display a message indicating a successful or failed connection.

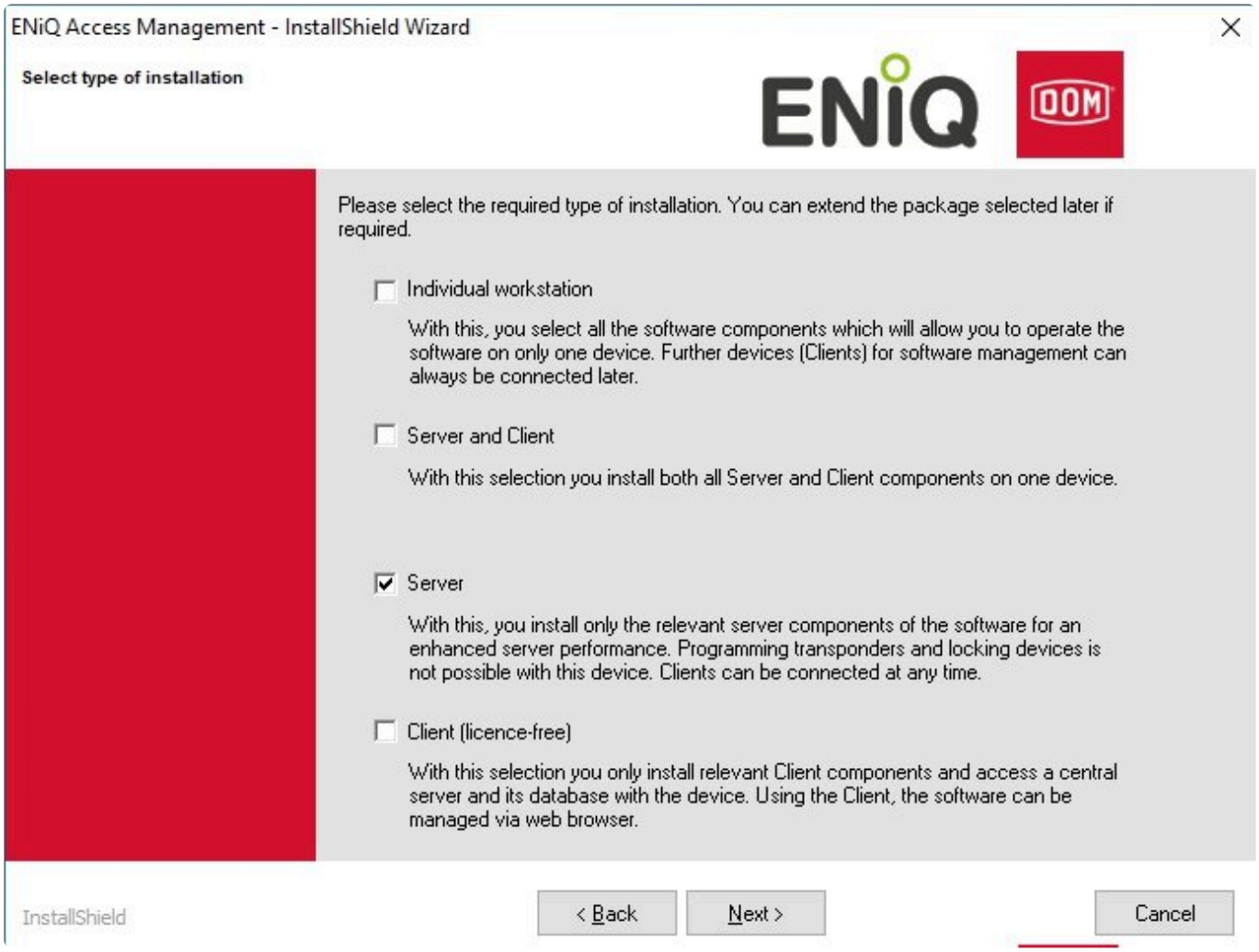
In the next step, if the connection is successful, select the window with all databases of the SQL Server instance. Select the “GENIUS” database. In case of incorrect login data, no instances are listed for selection.



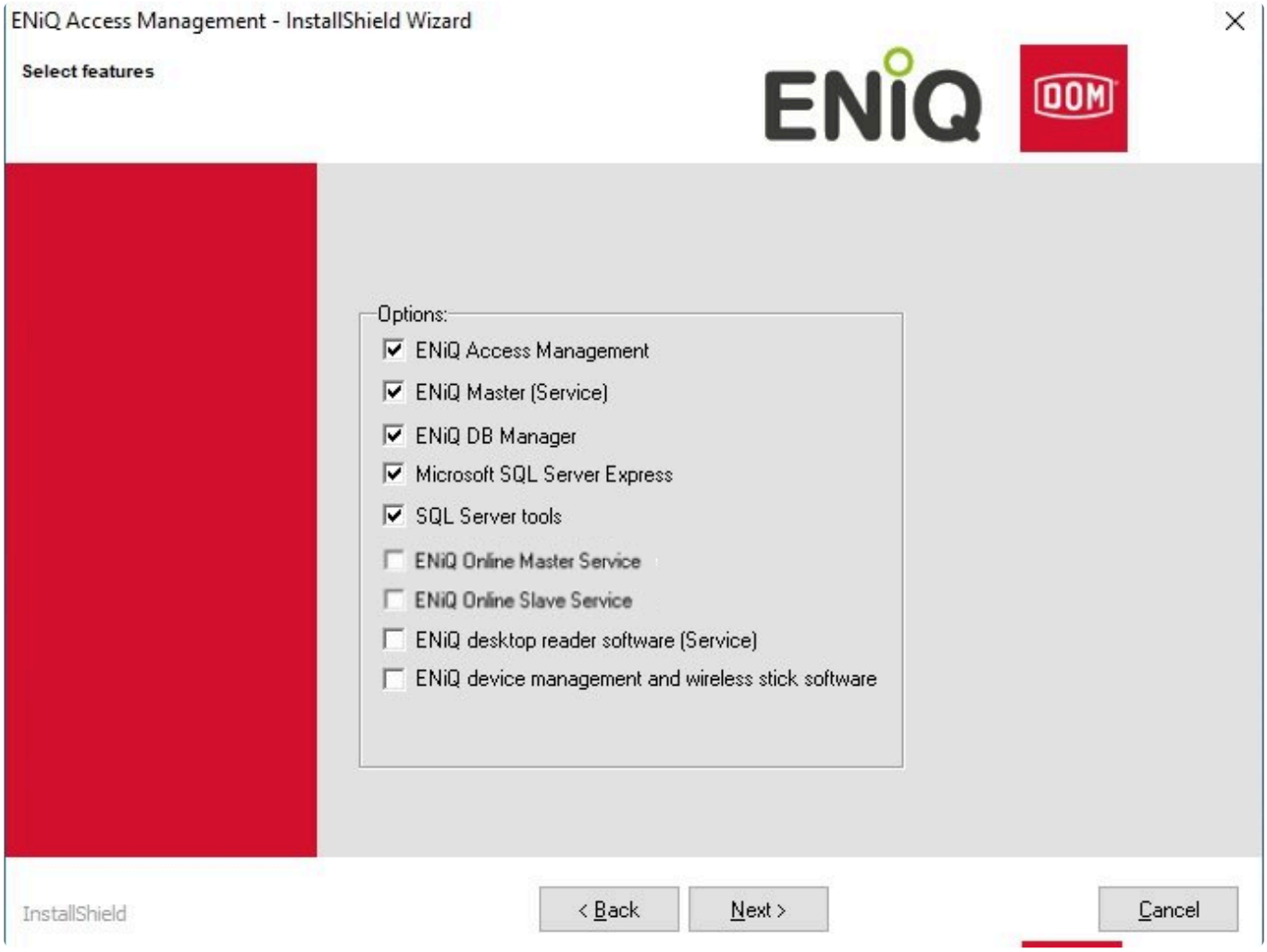
The remaining steps are identical to the standalone installation.

8.6.2. Server Installation

A pure server installation of the ENiQ AccessManagement does not require any directly connected programming devices (desk reader / RF radio stick for device programming via radio).
For a pure server installation please select the installation type “Server” and click Next.



In case of a server installation the following features should be selected:

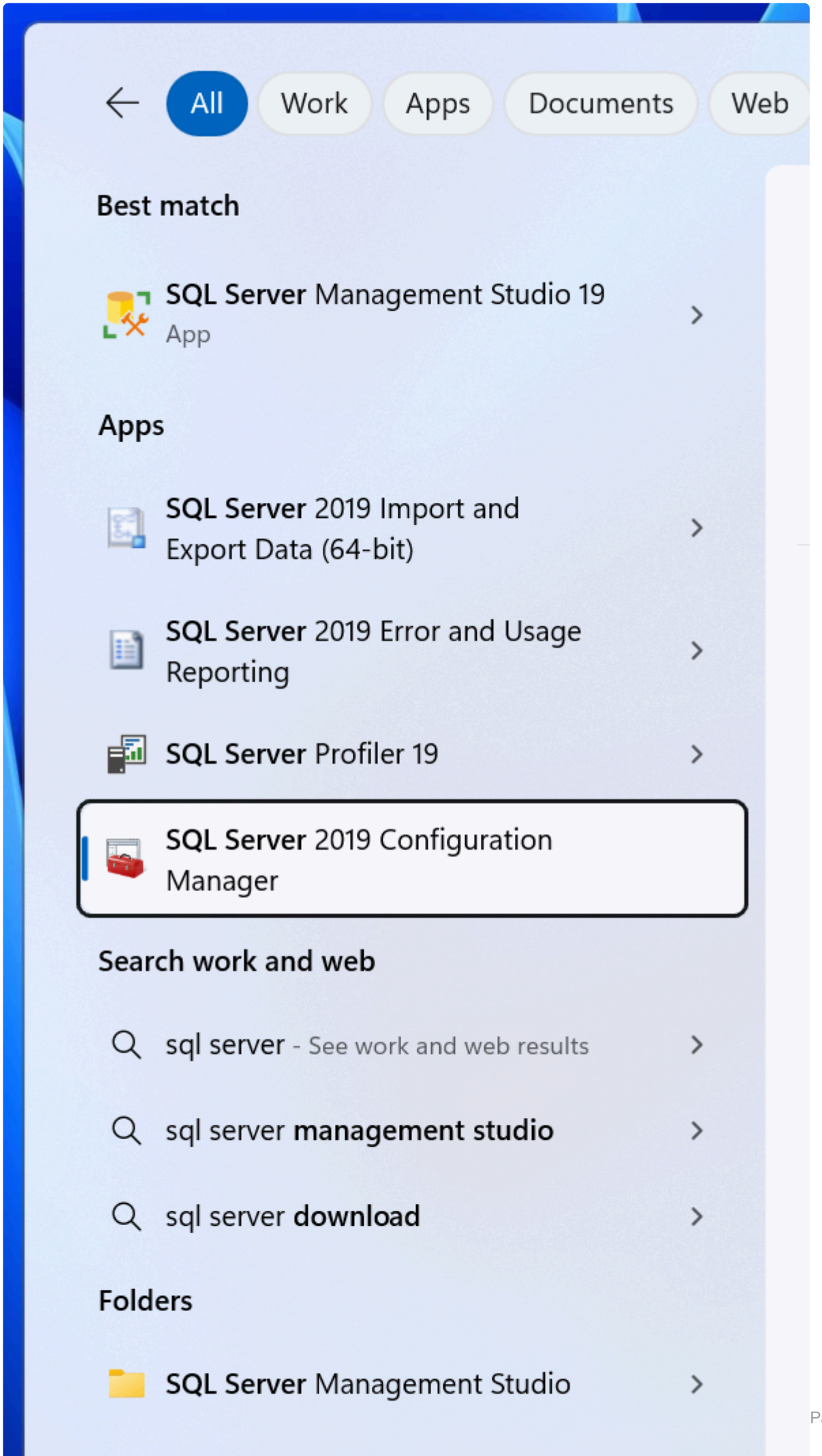


Then proceed as for a standard installation.

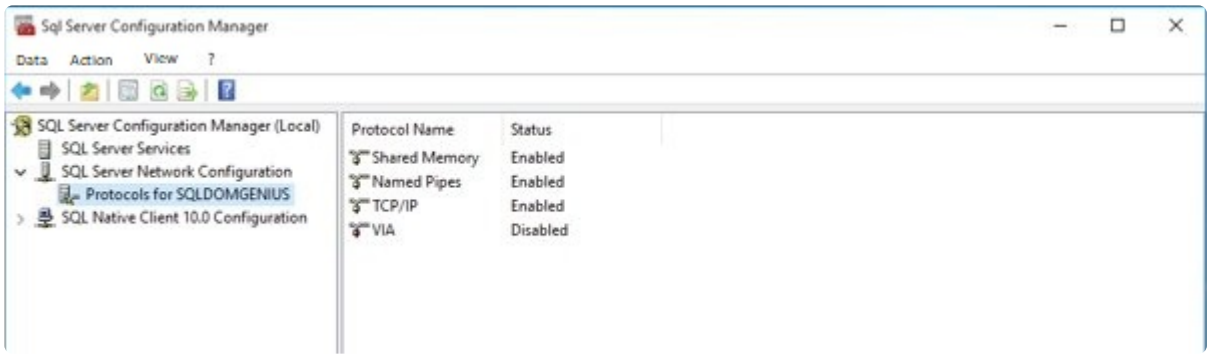
Checking the availability of the server

After the installation, it should be checked if the database and the website are reachable from another computer in the network.

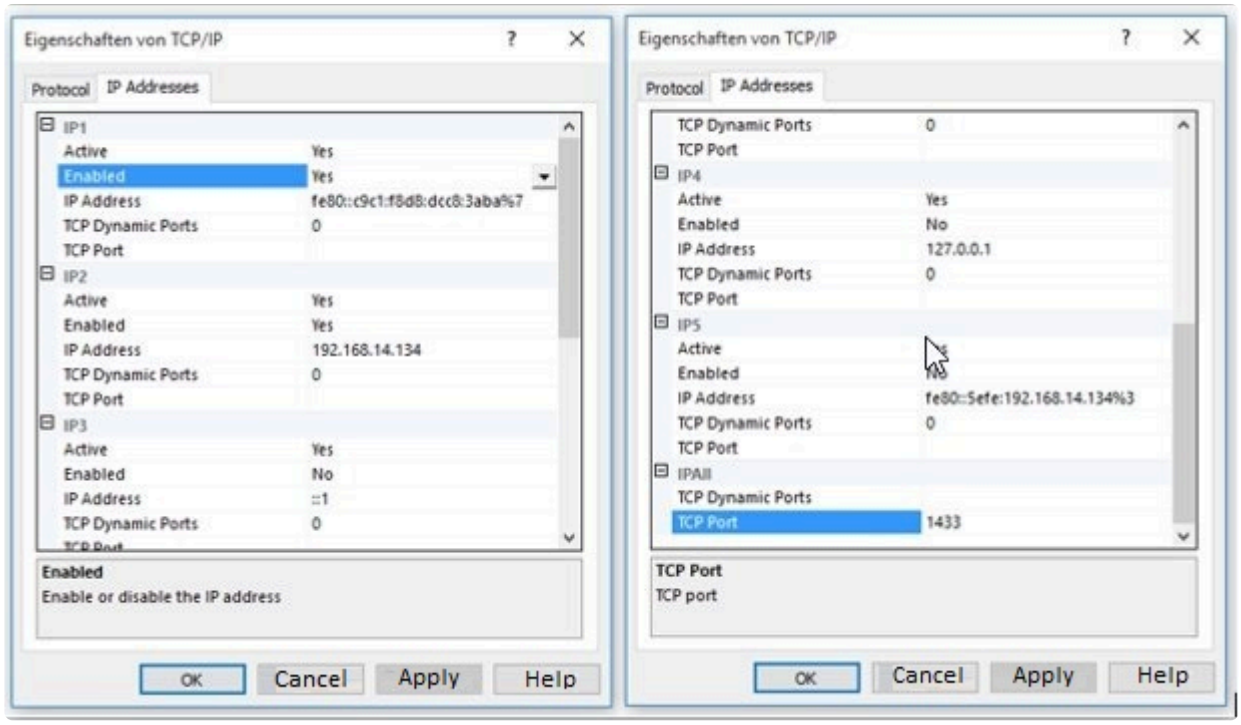
The following steps are necessary for this:
In the start menu under SQL Server 2008R2 —> Configurations Tools call the “SQL Server Configuration Manager”.


All
Work
Apps
Documents
Web
Best match
SQL Server Management Studio 19
App
Apps
SQL Server 2019 Import and Export Data (64-bit)
SQL Server 2019 Error and Usage Reporting
SQL Server Profiler 19
SQL Server 2019 Configuration Manager
Search work and web
sql server - See work and web results
sql server management studio
sql server download
Folders
SQL Server Management Studio

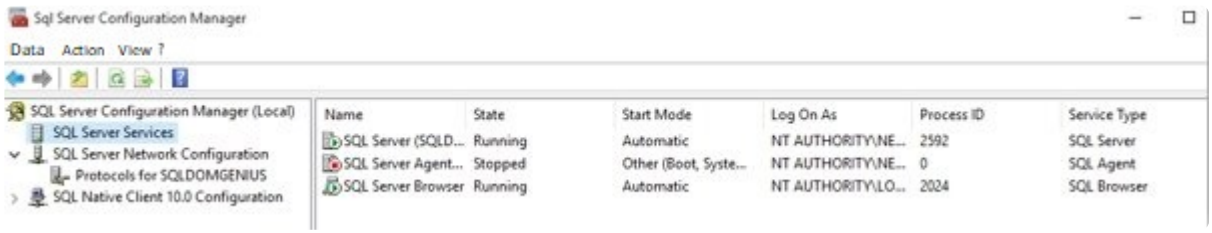
To do this, set the “TCP/IP” option in the Configuration Manager to “Enabled”:



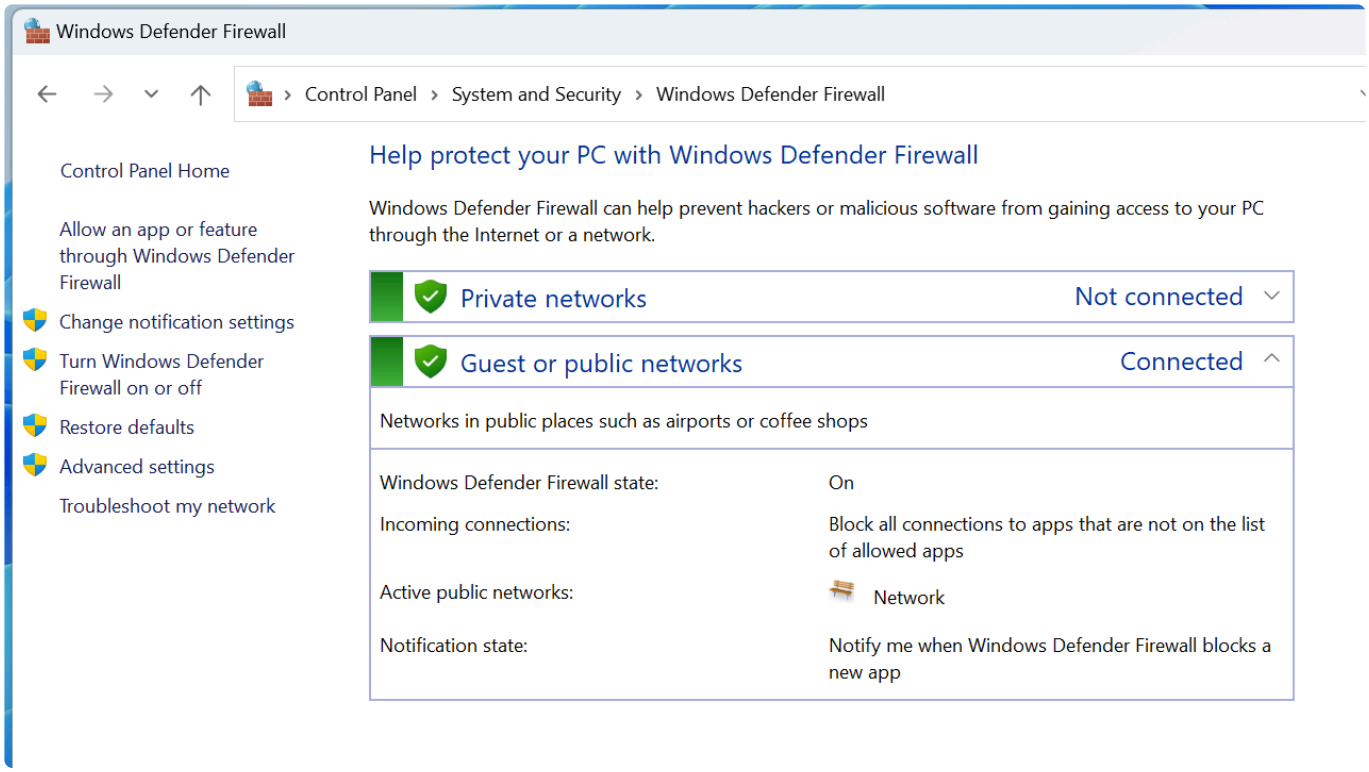
Then open the properties of TCP/IP (right click TCP/IP) and switch to the tab IP Address. Apply the settings as shown in the following picture:



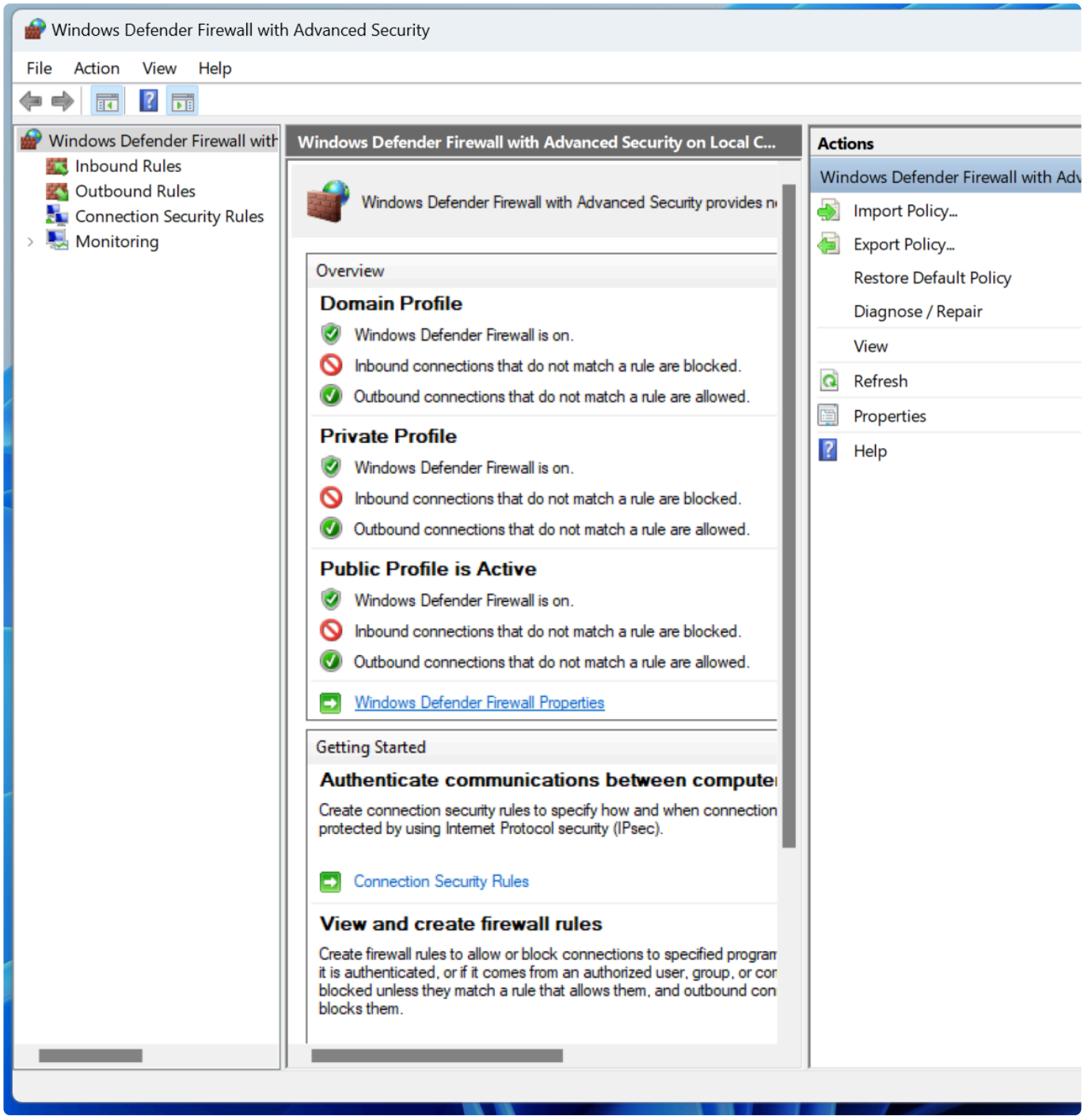
Then restart the SQL Server (SQLDomGenius) under SQL Server Services.
If the “SQL Server Browser” service is not running, it must also be started.



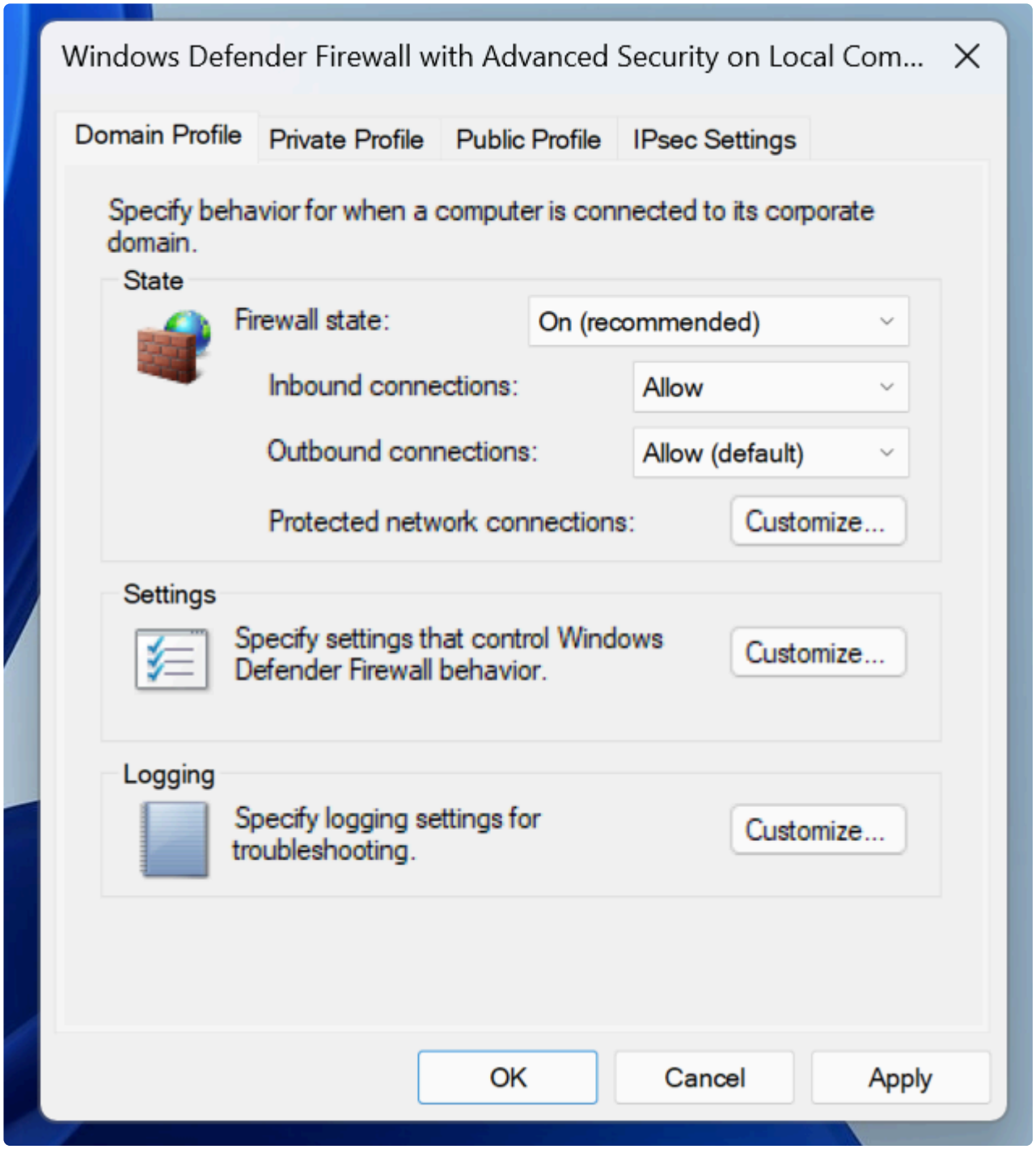
Set the following changes in the firewall only if the access to the SQL Server is denied:
Under Control Panel —> Windows Firewall —> Advanced Settings, access the Windows Firewall with Advanced Security.



There in the main window “Overview” click on “Windows Firewall Properties”



In the opened dialog under the corresponding network profiles (mostly “Private Profile” and “Domain Profile”) set “Allow incoming connections” to “Allow”.



Then the web server and the database should be reachable in the network.

8.6.3. SQL Server

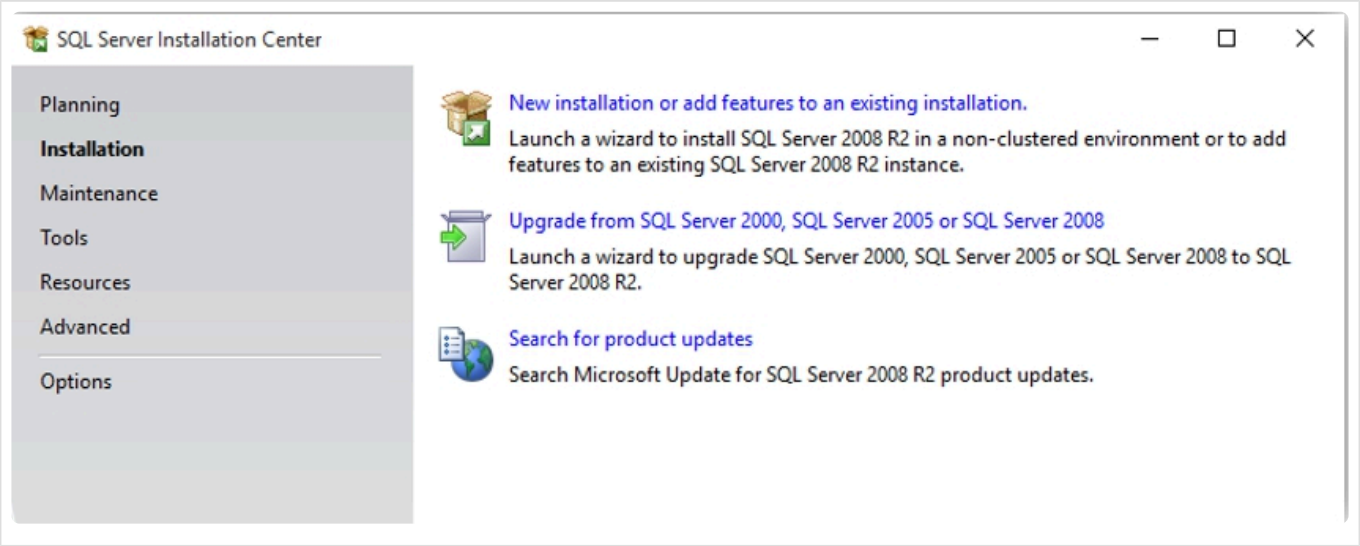
To use a different MS-SQL server than the one included in the setup, 2 steps are necessary:

1. Installation and setup of the server instance
2. Selection of the server instance during ENiQ installation

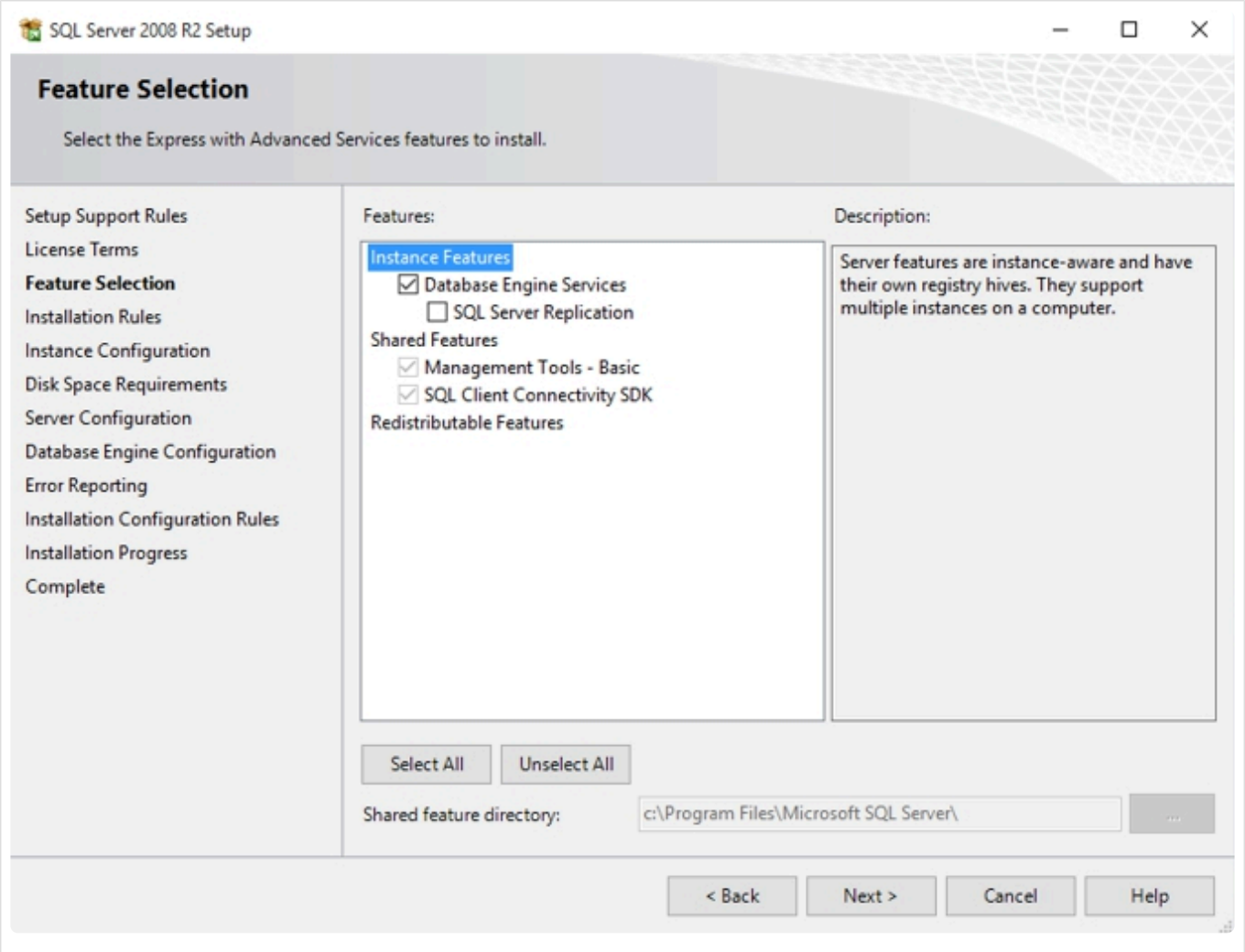
Installation and setup of the SQL Server instance

> ! If an already installed SQL Server is to be used, make sure that the installation steps have been performed as described.

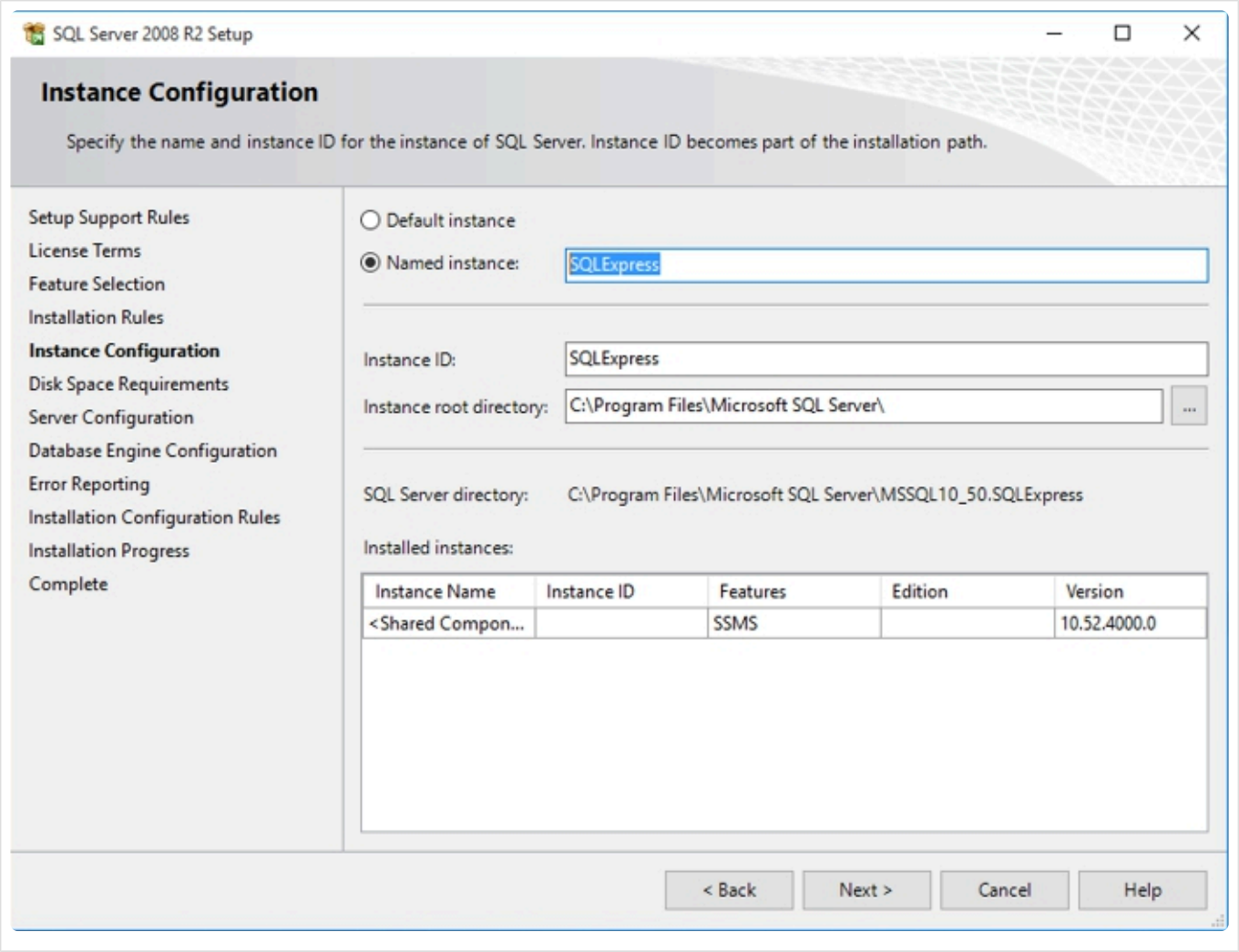
After running the MS-SQL installer (select “Custom installation” if necessary), select the item: “New installation or add features to an existing installation”.



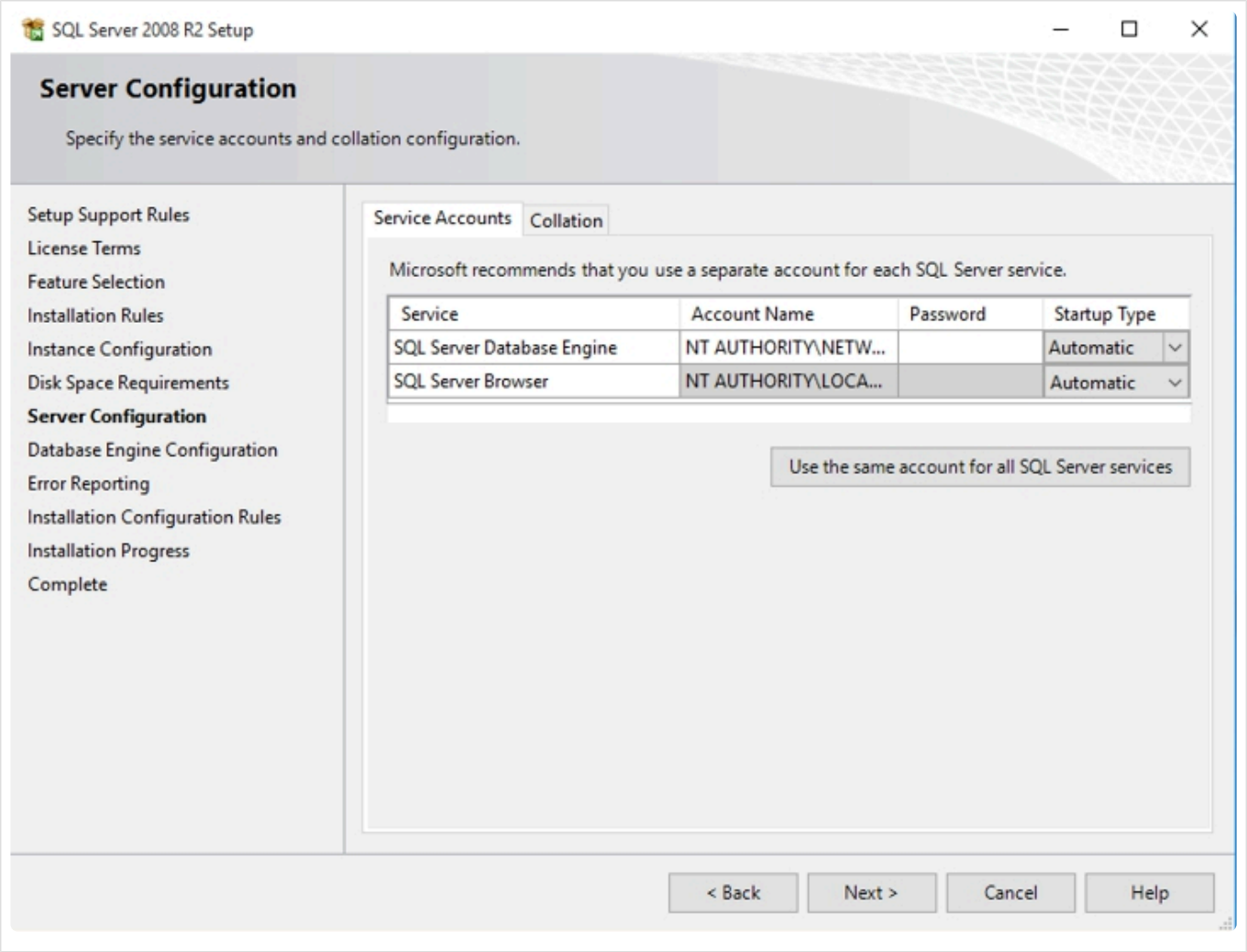
Select the checkboxes according to the image and continue the installation by clicking “Next”.



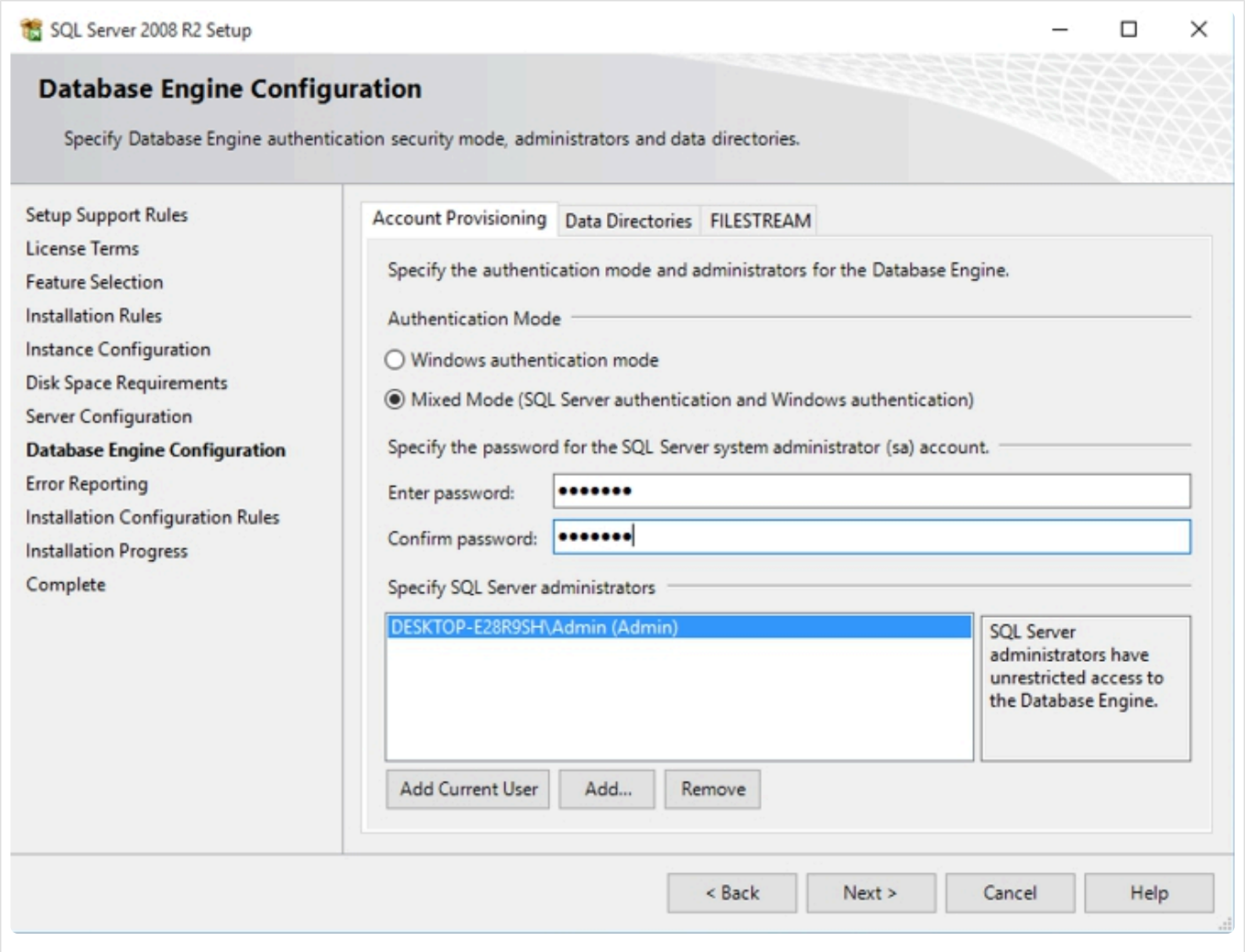
In the next window, fill in the “Named instance” field with an instance name of your choice and continue the installation by navigating to the next window.



The following two steps will complete the MS SQL Server installation. First set all server configuration to “Automatic” as shown in the picture.



Then in the next window set the Authentication Mode to “Mixed Mode” and choose a password for the “sa” user.
This password can be independent of the server installation.



Check/enter the database connection data into the config file of the ENiQ DeviceManagement:

Open “DOMGeniusDesktop.exe” under C:\Programme\DOM Sicherheitstechnik\DOM Genius Software\Desktop
(or C:\Programme (x86)\DOM Sicherheitstechnik\DOM Genius Software\Desktop).
There you will find an encrypted ConnectionString as shown in the image.

Now add the following string one line below this ConnectionString:

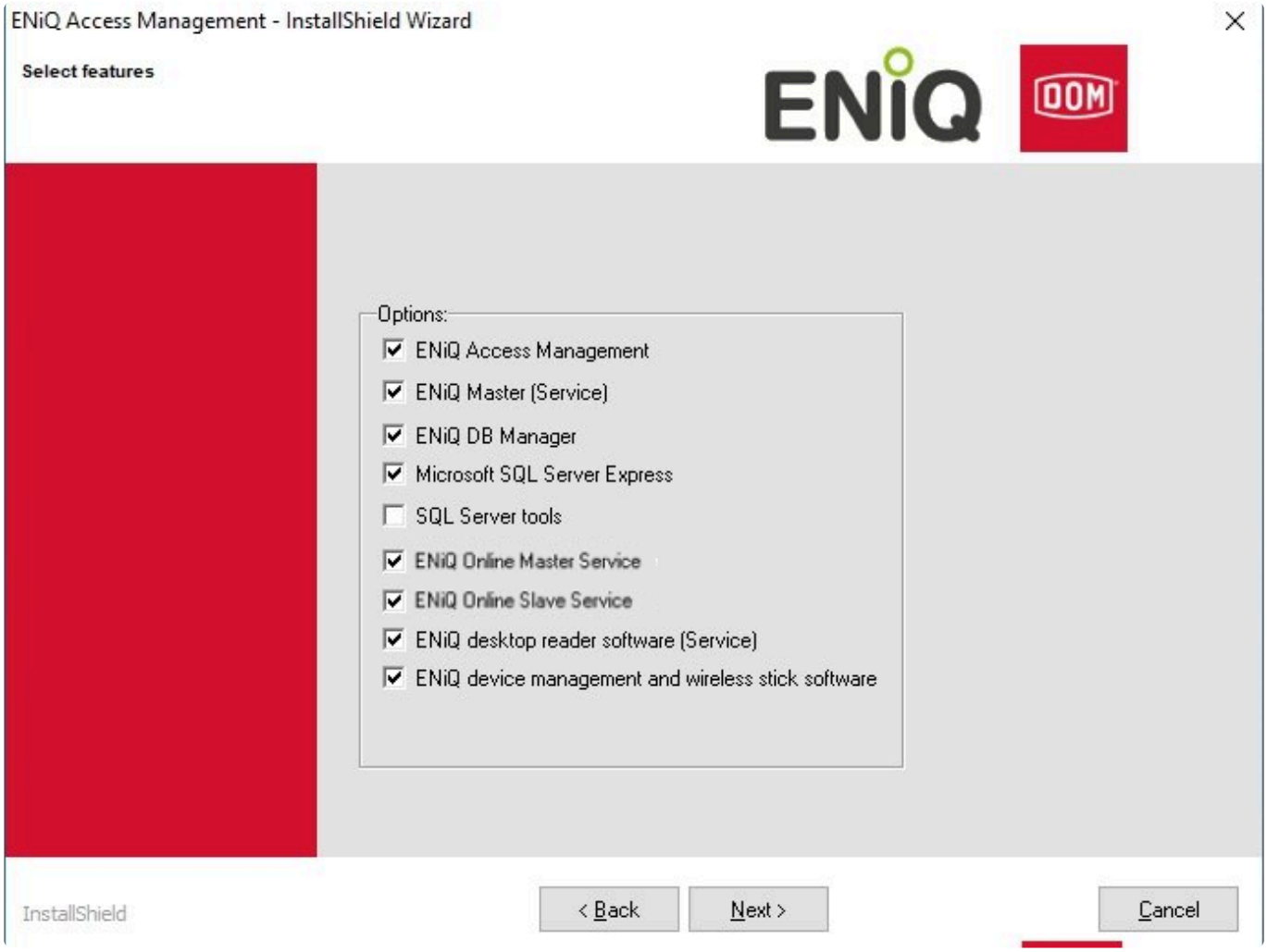
“add name=“Genius-Offline_Online_MSSQL_2008” connectionString=“Data source=(local)\MYINSTANCENAME;user id=sa;password=MYPASSWORD;initial catalog=Genius; Persist Security Info=true;” providerName=“MSSqlServer”

The image shows an example of how it could look like:

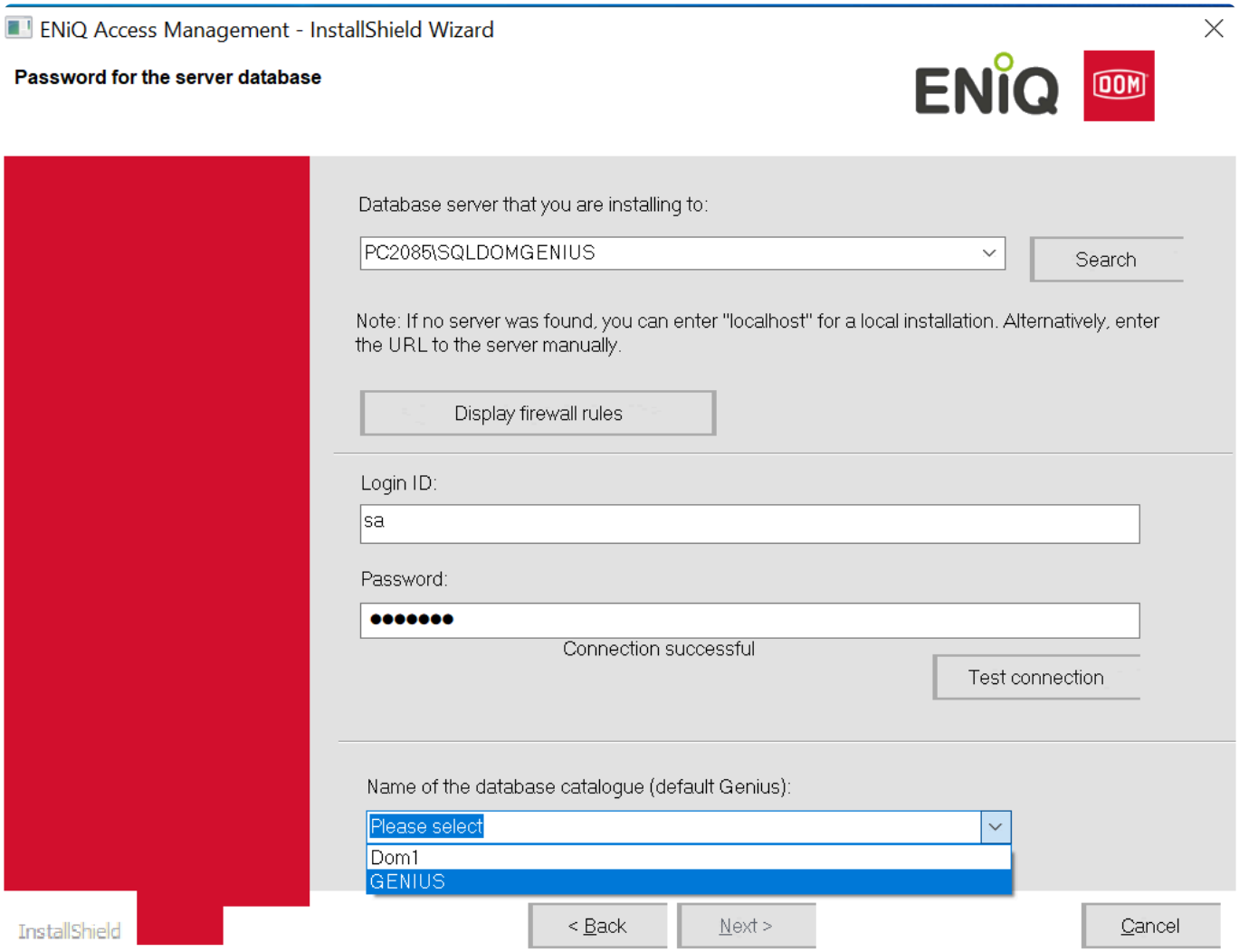
Replace the words MYINSTANCENAME and MYPASSWORD with the instance name and password chosen during installation.
“Catalog” corresponds to the database name. This must match the database name of the Genius database on the server installation. By default, this is “Genius”.
The editor can now be closed.

Installation of ENiQ AccessManagement

Follow the standard installation up to the feature selection and uncheck there the installation option “SQL Server 2014 Express SP2”.



After that the database selection dialog appears. Here you have to enter the credentials for the database connection as follows:
If you click on the upper “Search” button, a window appears with all available SQL database servers – among them should be your database server.



After selecting it and entering the SQL Server authentication data (“sa” and the password set accordingly) from the server installation, clicking the “Test Connection” button will display a message indicating a successful or failed connection.
If the connection is successful, type a name (e.g. “GENIUS”) into the “Database catalog name” field and click “Next”.

The remaining steps are identical to the standalone installation.

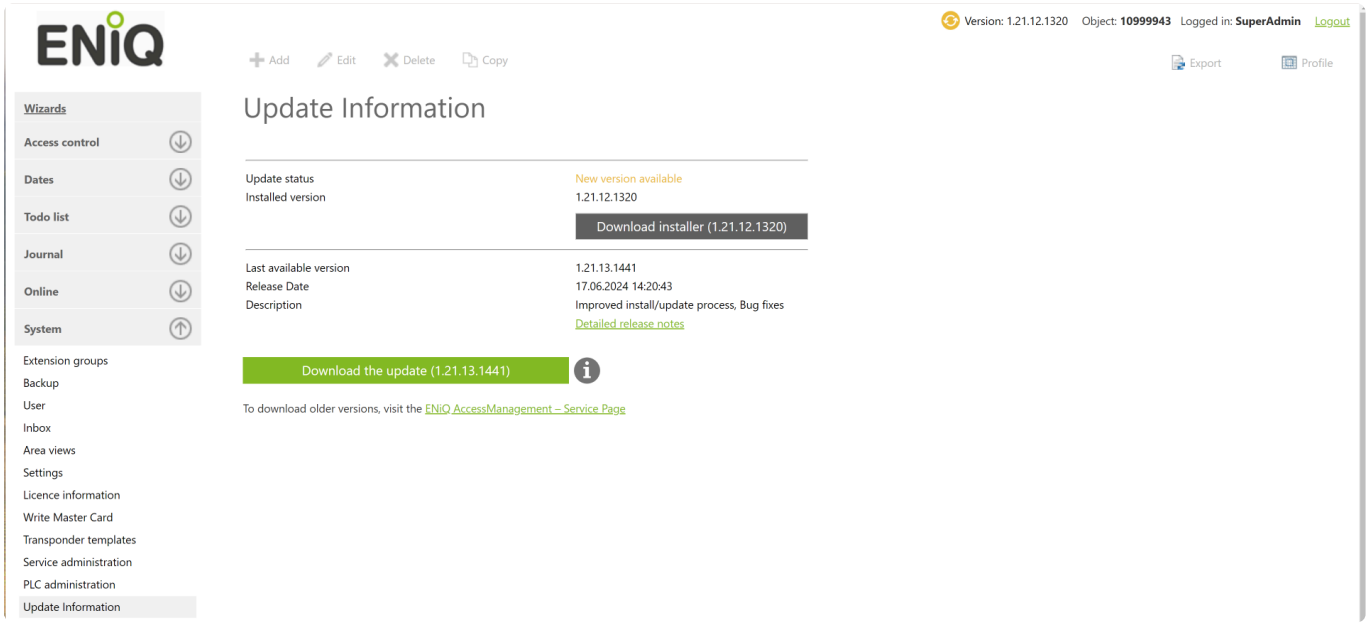
8.7. Server & Client Update

This chapter describes how to update the version of the server or client software.

> ! Before proceeding to update the server version, it is recommended to backup the system. See details here: Operation – Backup

Update status

In order to check whether there is a newer version of the software, you can visit the “Update Information” settings page in “System / Update Information”

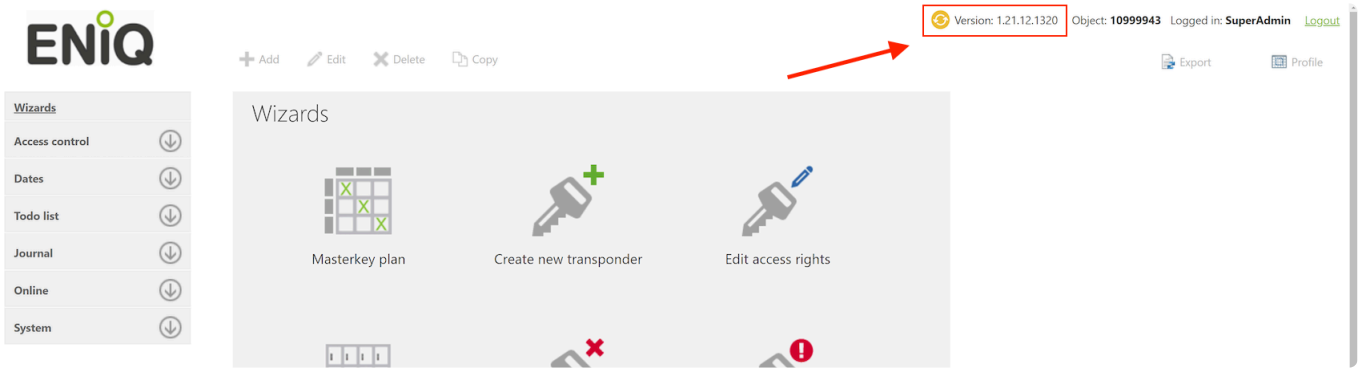


On this page you can download the Updater for the new version

You can also download the Installer for the currently installed version, to install new clients.

> ! The version of the clients should always match the version of the server.

This “Update Information” page can also be reached from the shortcut on the top-right of the page:



Updating the server or client version

- First make sure a recent system backup has been made. Read more here: Operation – Backup
- In order to update the server version, download the updater file and open it.
- Follow instructions until the server version is updated.

> The clients can also be updated without using the update wizard, by launching the Update file from command line, with option "——*client*". This command will launch the client update in the background, without requiring any further interactions, saving some time for the operator.

8.8. Battery status collected by transponders

With version 1.24 of ENiQ AccessManagement, the battery statuses of intelligent (DataOnCard) locking devices can be retrieved by intelligent (DataOnCard) transponders, and delivered back to the software using AccessManager ITT or Desk Reader.

Description

When presenting an intelligent (DataOnCard) transponder to a locking device, the battery status of that device is collected and stored on the transponder. The next time this transponder is read by an AccessManager ITT, or written by a Desk Reader, this battery status is sent to ENiQ AccessManagement.

Battery statuses are retrieved by the Desk Reader only when the intelligent (DataOnCard) transponder is written, not when it is just read.

Only transponders configured as “intelligent” (Data On Card) can retrieve the battery statuses from the devices.

Battery statuses are displayed in the “Access Control” / “Devices” list, when the columns “battery status” or “battery warning level” are added (see Standard tables – representation and functions), or in the device details window, on the “Device data” tab.

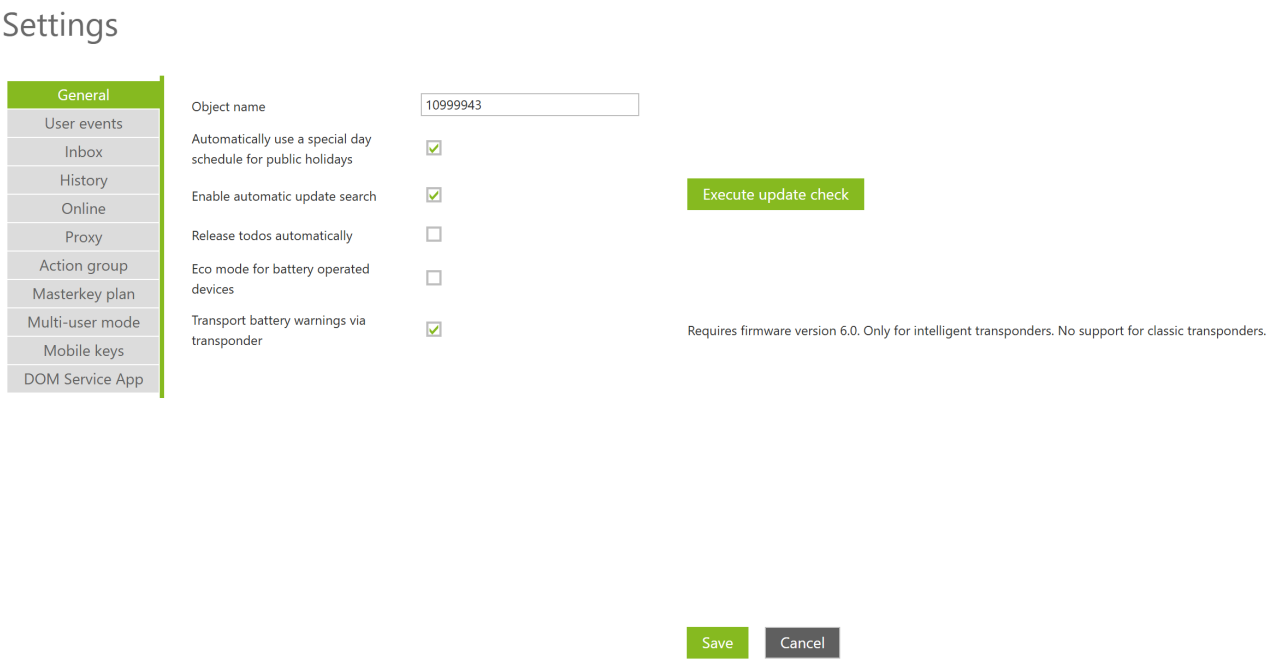
Requirements

- Locking devices on firmware v6.0 or later
- ENiQ AccessManagement v1.24
- Regular use of AccessManager ITTs (preferred) or Desk Readers
- “Intelligent” (Data On Card”) license module (see Operating modes)
- Transponders need an additional 128B of available memory space in order to store the battery statuses. This space is not included in the “transponder template” memory consumption.

Only Mifare DESFire Transponders are supported. No support for Mifare Classic.

Setup

- Enable the feature from “System” / “Settings” / “General”, with the checkbox “Transport battery warnings via transponder”, then click “Save”:



- Configure the locking devices as “intelligent” (DataOnCard) (see Set properties of a device), then synchronise those devices.
- Configure the transponders as “intelligent” (DataOnCard) (see Manage transponders/persons)
- Transponders need to be written once (by AccessManager ITT or Desk Reader), so they are configured to store the battery statuses.

The locking devices will then start storing the battery status changes on the presented transponders.

> In order to fully benefit from this feature, we suggest to force the update of transponders daily by using Extension Groups and setting up an AccessManager ITT for entering (and even exiting) the facility.

Disabling the feature

To disable that behavior, you can proceed as follows.

- Disable the feature from “System” / “Settings” / “General”, with the checkbox “Transport battery warnings via transponder”, then click “Save”.
- Transponders need to be written once (by AccessManager ITT or Desk Reader), so they are configured to stop storing the battery statuses.

> Disabling this feature does not free up the 128B of allocated memory on the transponders, for storing the battery statuses. Even when unused, this space will remaining reserved.

The locking devices will then stop storing the battery status changes on the transponders.

9. Tools

9.1. DB-Manager

This chapter describes the features of the ENiQ DB Manager software, and how to use it. For this purpose, the application scenario for which the ENiQ DB Manager software was developed is first described.

Configuration
At least one single license is required for using it.

With the first license, a standard single user installation of the ENiQ software is performed, so that a running ENiQ software is already available on the PC.

Commissioning
Neither installation nor configuration of the ENiQ DB-Manager software is required.

The ENiQ DB-Manager software can simply be copied into any directory of the PC and started directly. When the software is started for the first time, it automatically searches for the required configuration data in the installed ENiQ software and adopts them for future use in the ENiQ DB Manager configuration.

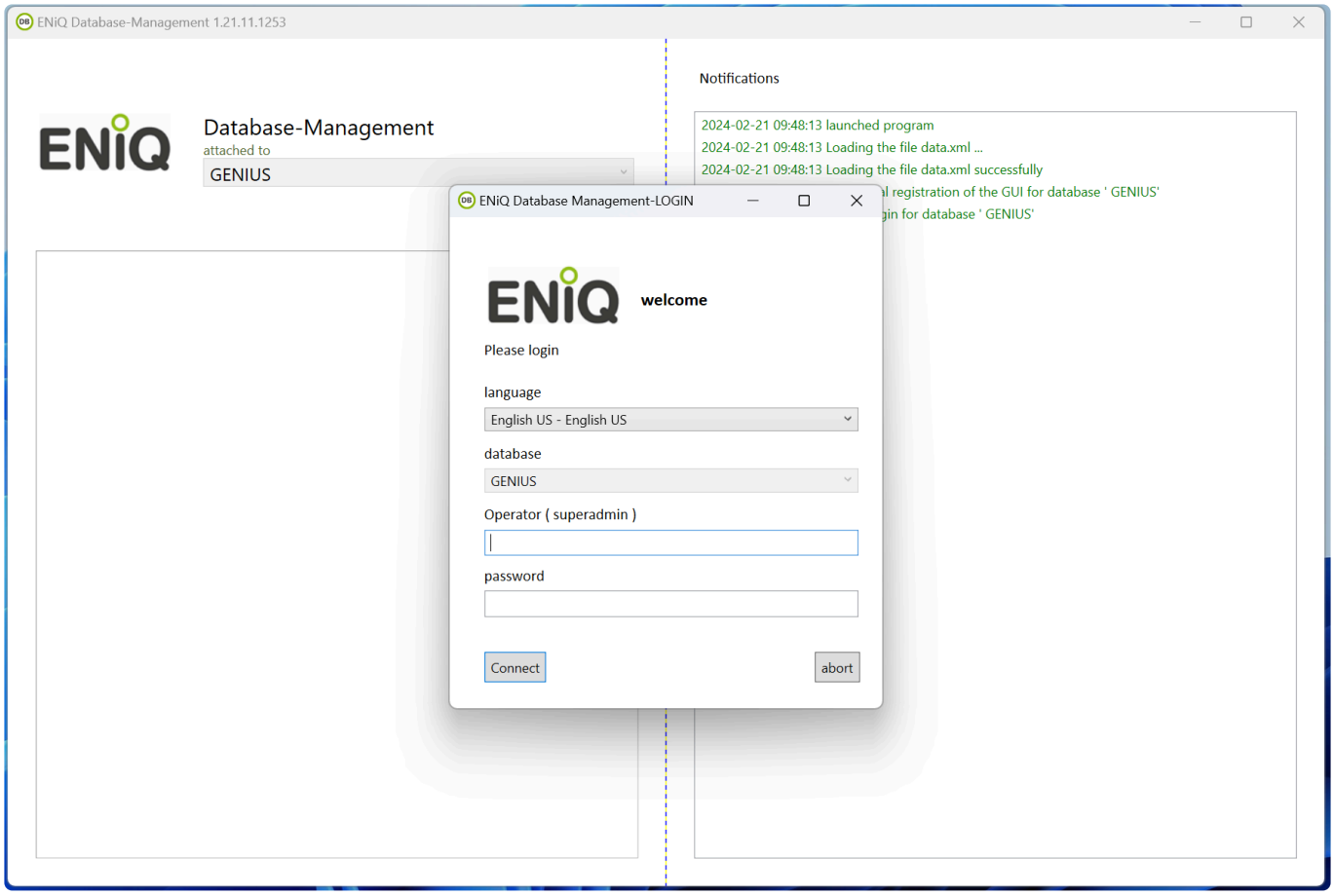
Thus the ENiQ DB-Manager software is already ready for operation after the first start.

Update

The software is part of the ENiQ AccessManagement installation.
When the installation is updated, the ENiQ DB Manager software is also updated.

User interface

When starting the ENiQ DB-Manager software, the operator must first authenticate himself as a valid operator of the active ENiQ database.
This operator must be assigned the role “SuperAdministrator” in the ENiQ software.



The user interface is divided into two areas:

Information area

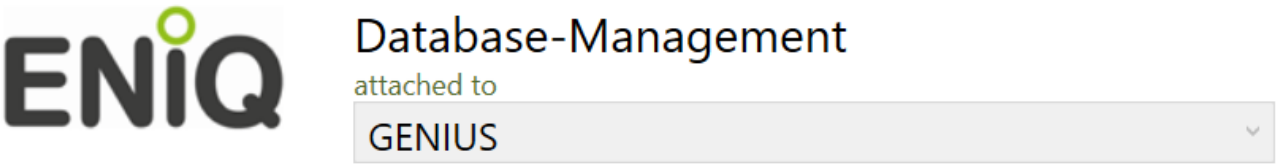
The left side contains the work area and the right side contains the information area.

In the right part titled “Notifications”, the information area, all actions performed by the software are documented and also any error messages are displayed.

The left part is divided into a header and workspace area.

Header area

In the header area the currently active database is displayed.
All actions that are triggered in the workspace area are performed in this database. Thus, the active database is always visible, even after switching between the individual function blocks in the workspace area.

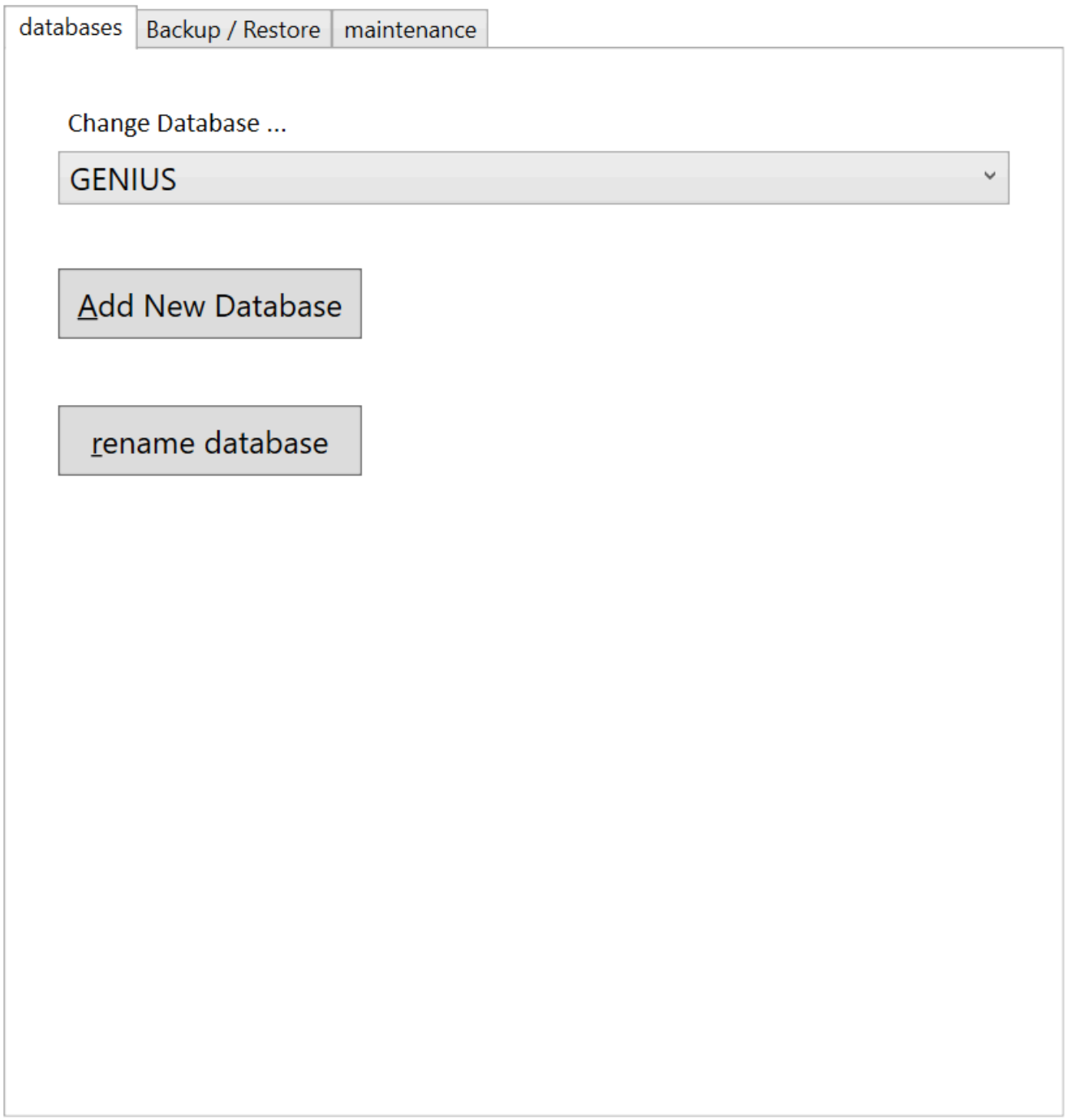


Workspace area

In the workspace area, the individual function groups are made available in separate tabs.

Currently the following function groups are available:

- Databases – Administration of databases
- Backup / Restore
- Maintenance



After logging in, the following functions are available:

- Databases – database management
- Creating a new database.
- Change the active database.
- Rename database.

- Backup / Restore
- Create a backup file of the active database.
- Restoring the active database from a backup file.

- Maintenance
- Creating archives in the database.

- Database maintenance

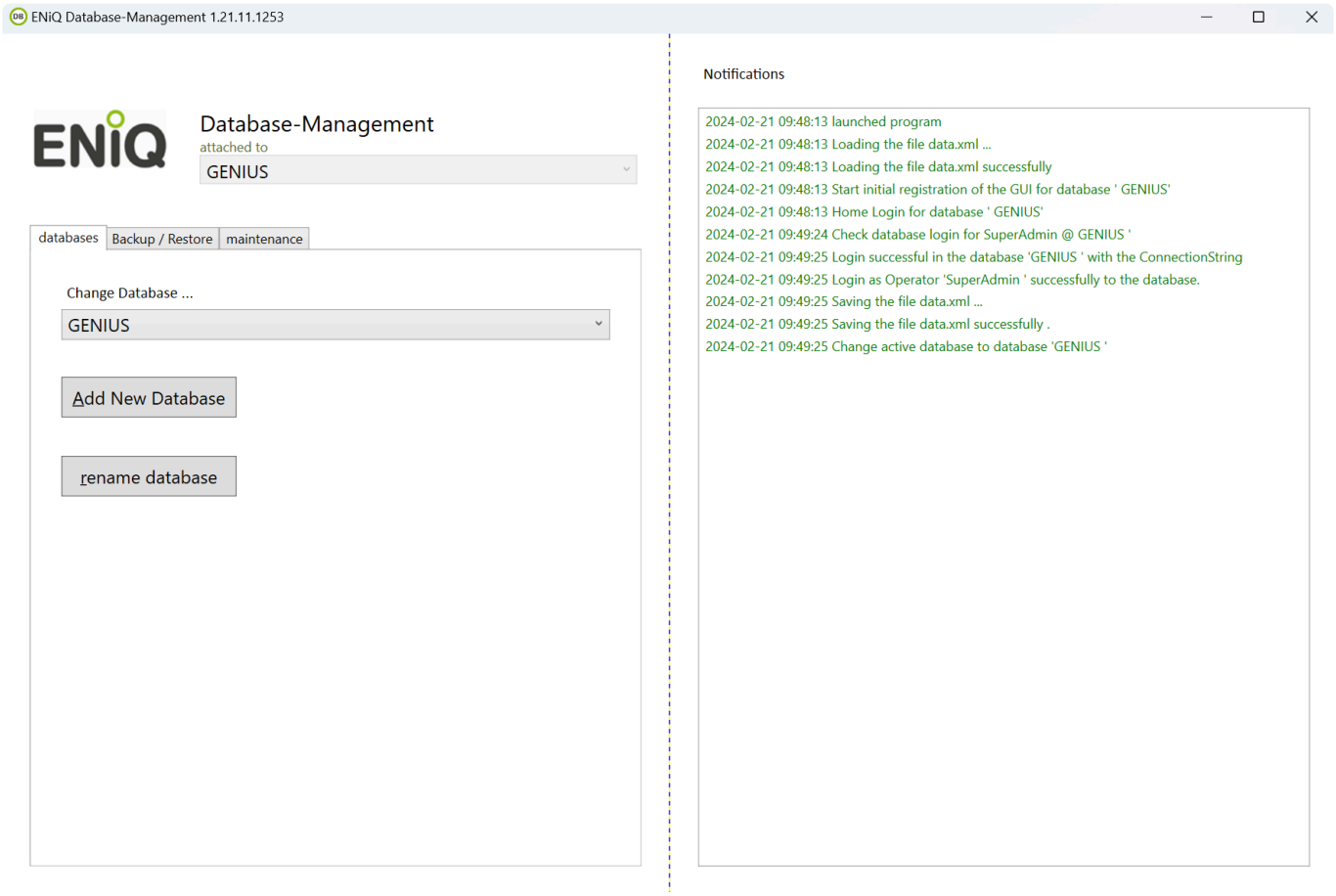
9.1.1. Functions

Functions

Functions are grouped into function groups according to related application scenario:

- Databases – database management
- Backup / Restore
- Maintenance

Database

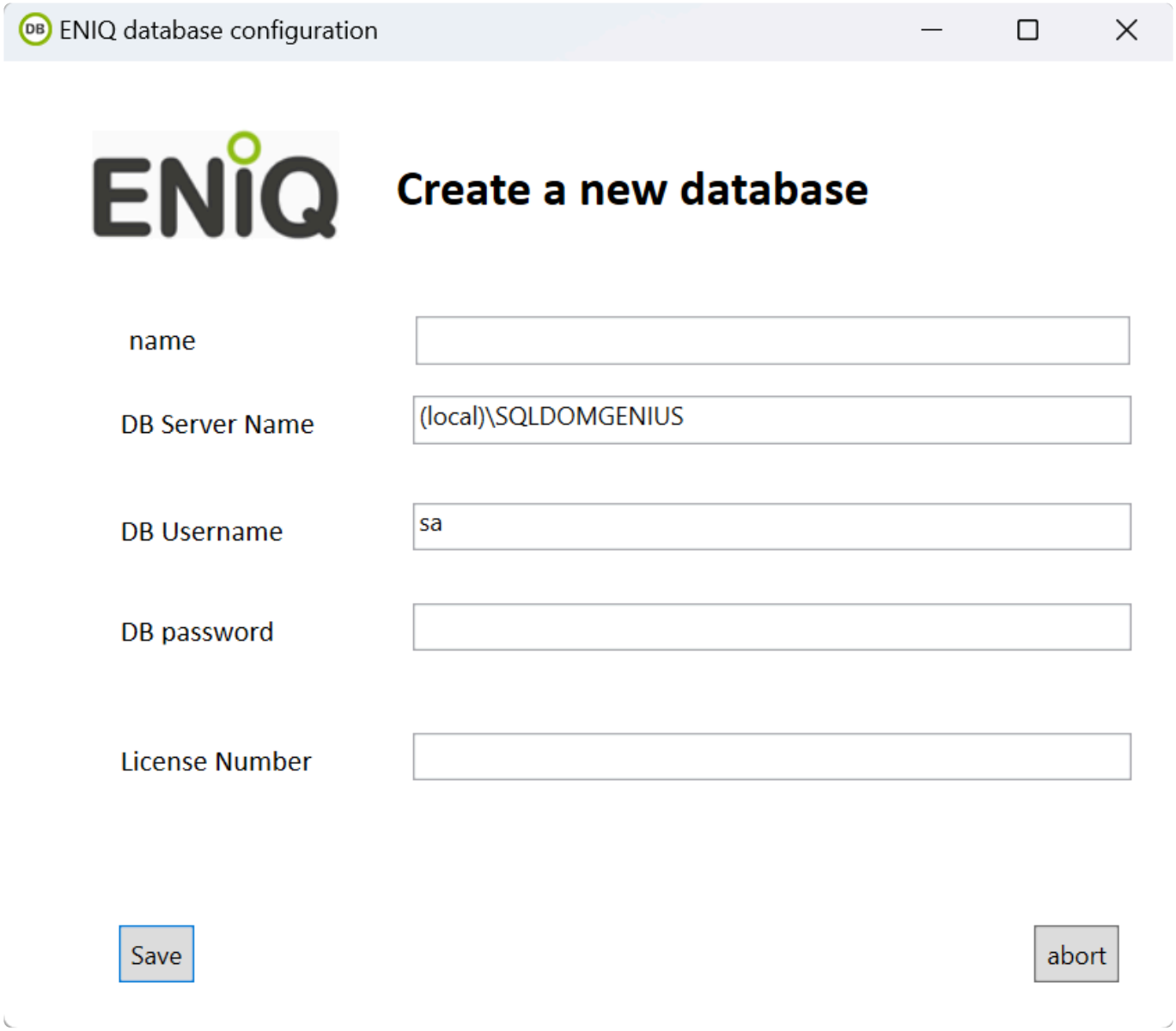


Here are the functions for managing a multi-DB system

Create a new database

Here you can add more databases to the list of managed databases.

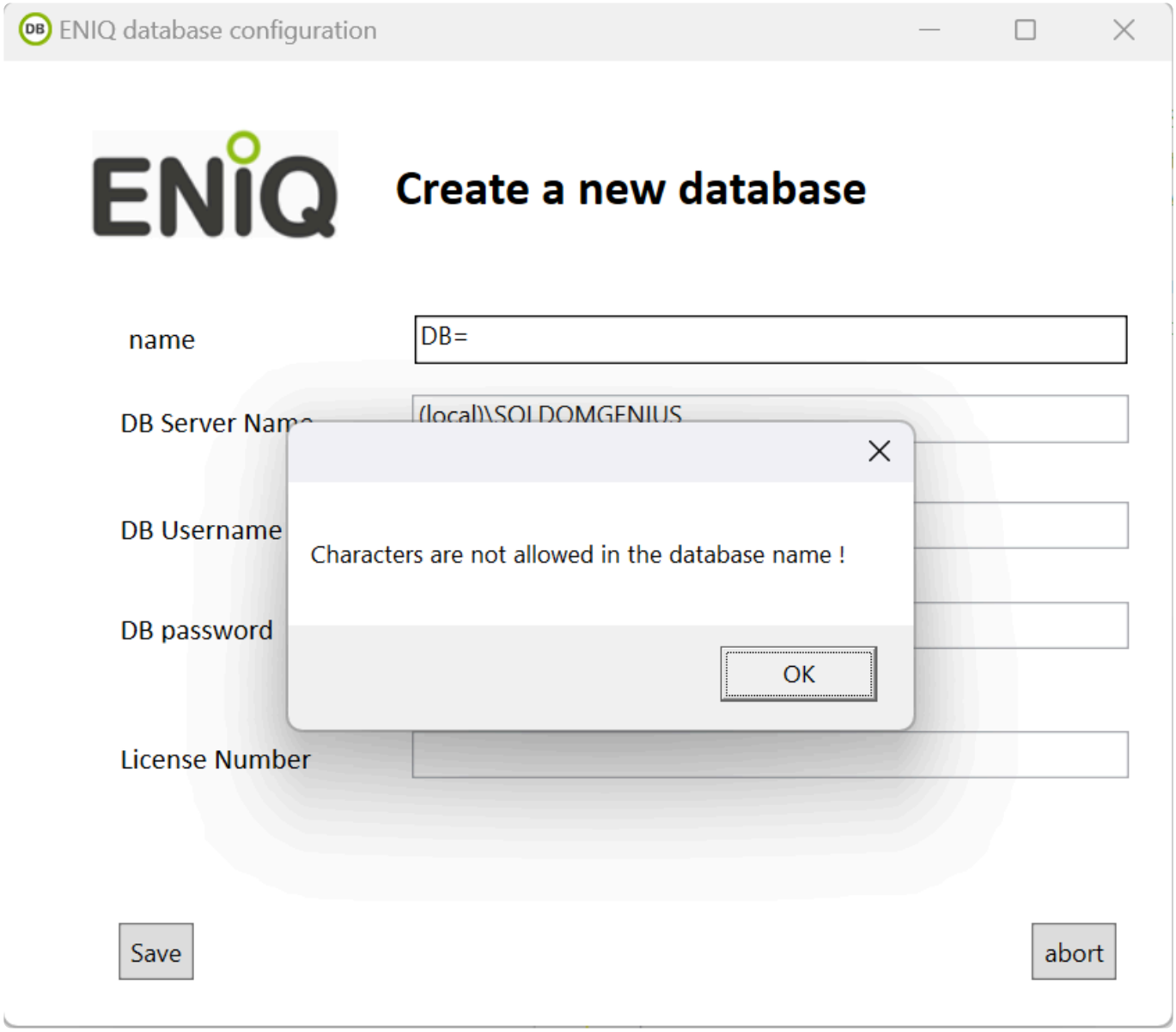
After pressing the “Add database” button, the window for entering all the relevant information needed to generate another database will open.



The name is used to give a title to the entry in the list of all databases. Also, this name is used to create a database instance on the database server that uses the same name.

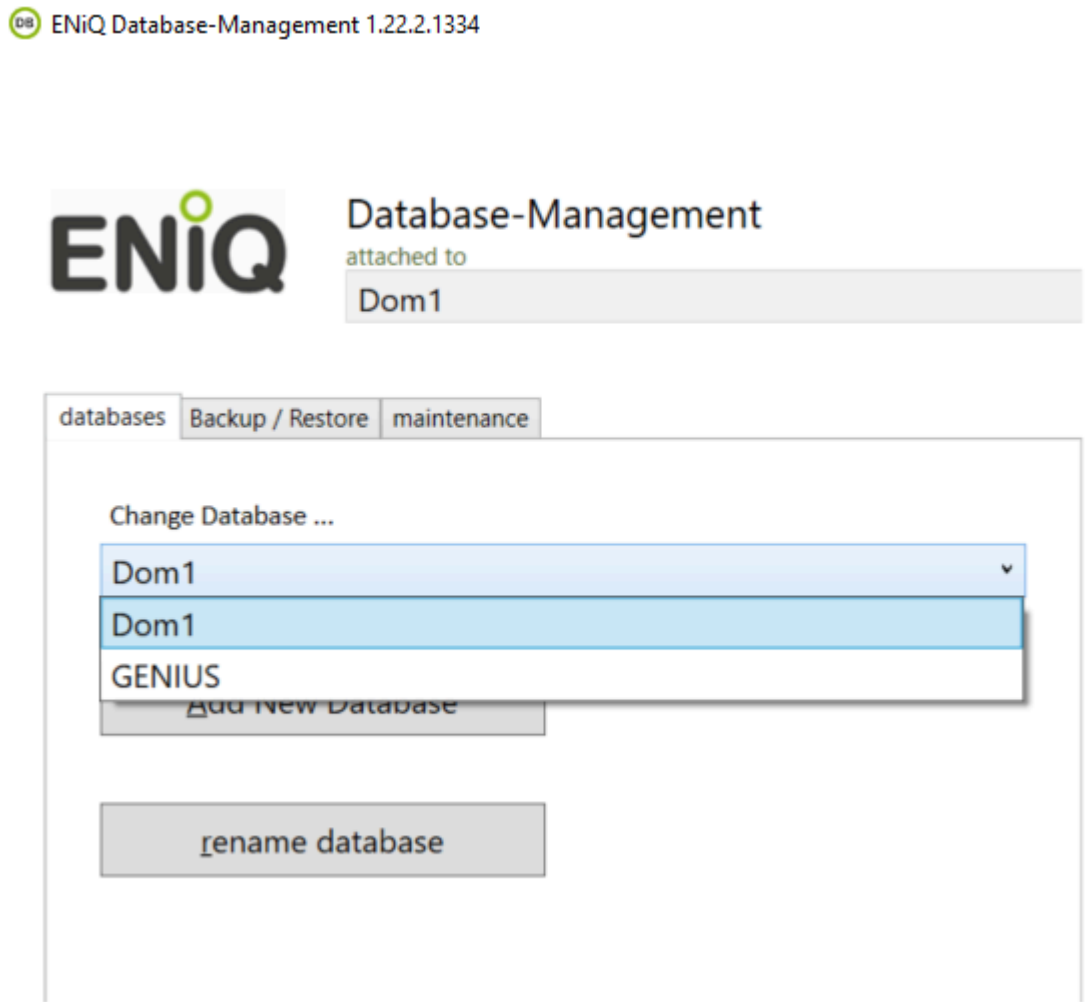
The database must be assigned a unique name that no other database has.

Only letters and numbers are allowed in the name. All special characters and the space character are not allowed.



Changing the active database

By selecting a database in the selection box, it is possible to switch between databases.

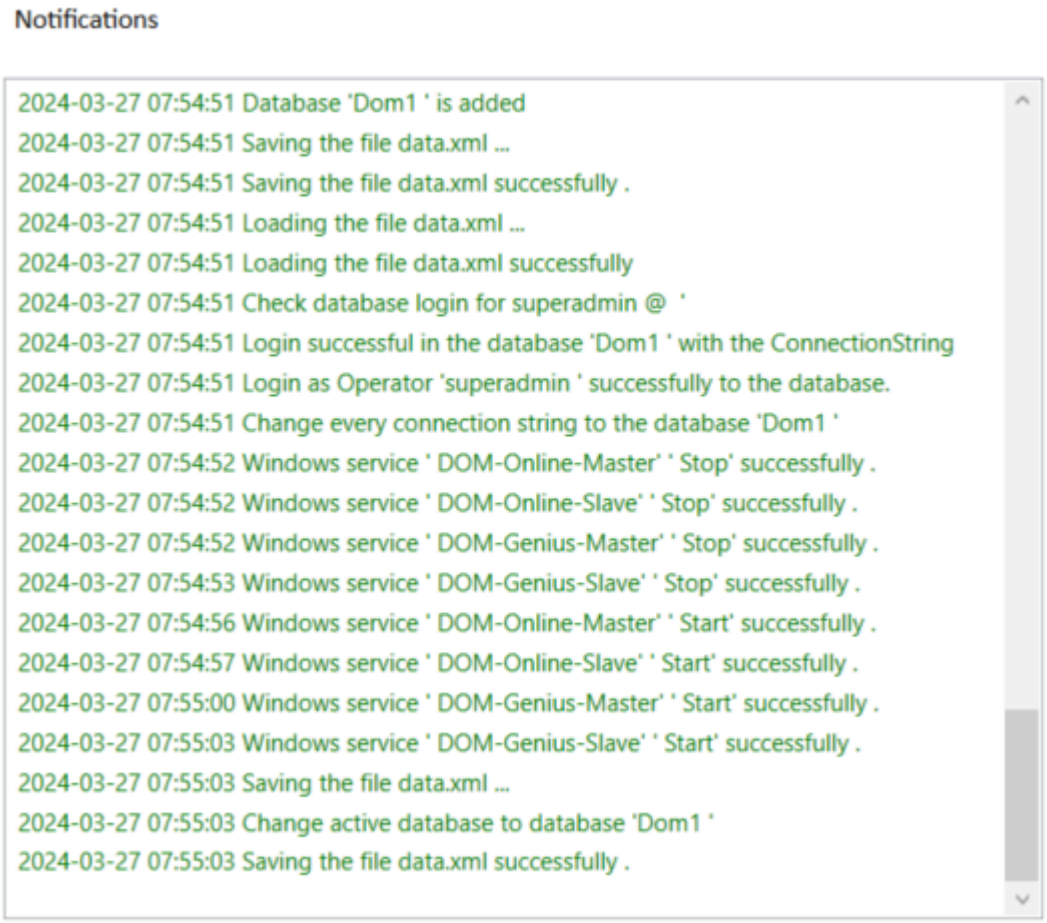


After selecting another database, the operator will be asked to authenticate with an operator name and password of an operator of the new database (who has the “SuperAdmin” role). This will determine whether the operator of the DB Manager software actually has the rights to work in this database.

If the operator does not have the rights, the system falls back to the last active database. Thus the selection has not executed any change.

After a positive validation of the operator, the following actions are automatically executed by the software and displayed in the information area of the progress:

- Stop any running ENiQ Device Management software.
- Stop all active ENiQ Windows services on this PC
- Adjust the configuration file with current connection string and license number (Web-Config)
- Adjust configuration file with current connection string, if available (ENiQ Windows services DOM-Genius-Master, DOM-Genius-Slave, DOM-Online-Master and DOM-Online-Slave)
- Start all previously stopped ENiQ Windows services



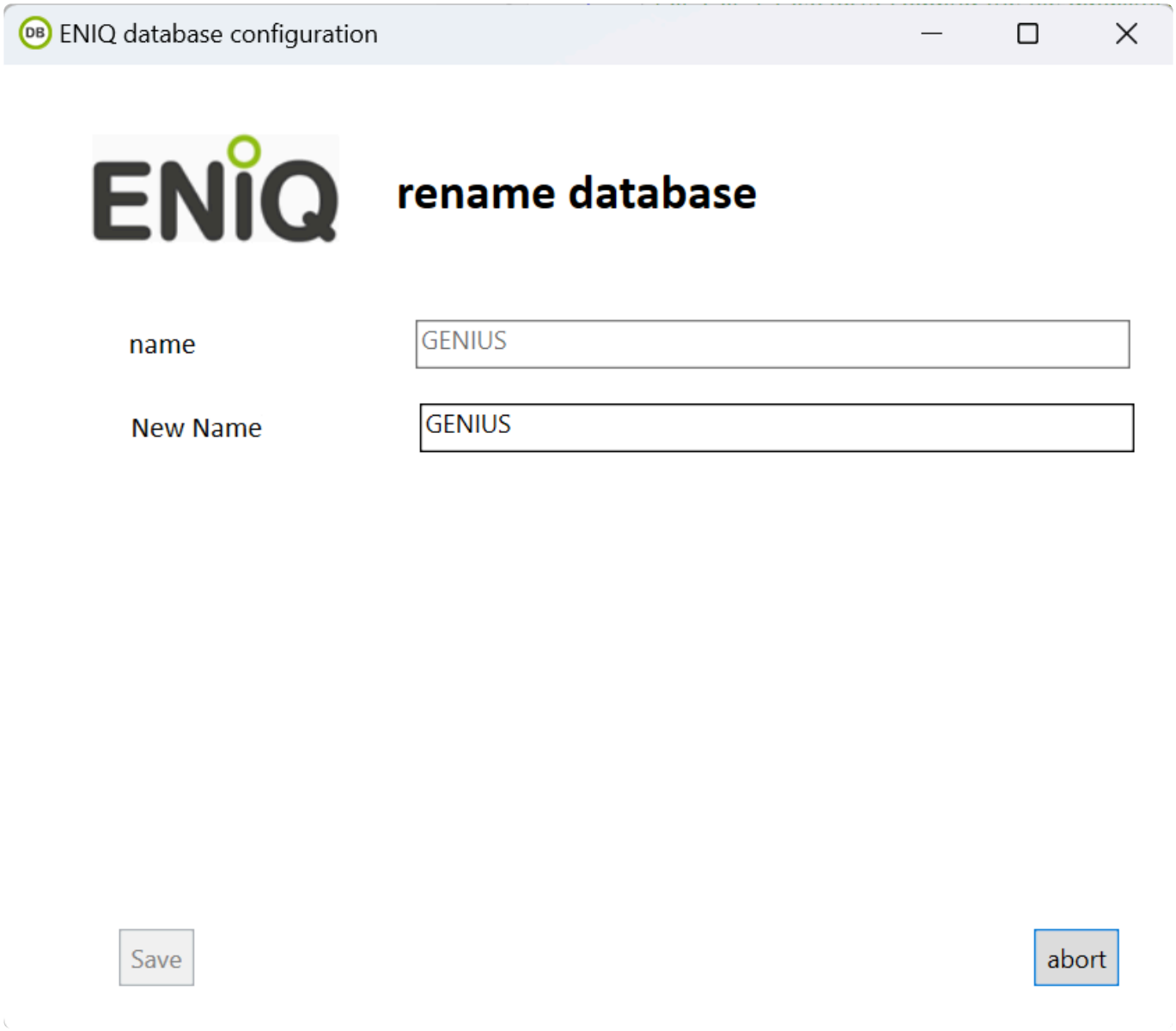
p(banner tip). The software finds all installed ENiQ software products on the PC automatically.

Rename database

With the button “Rename database”, the currently active database can be renamed.

After pressing the button, the input mask for the database name opens. The name input is checked according to the same rules as for a new database.

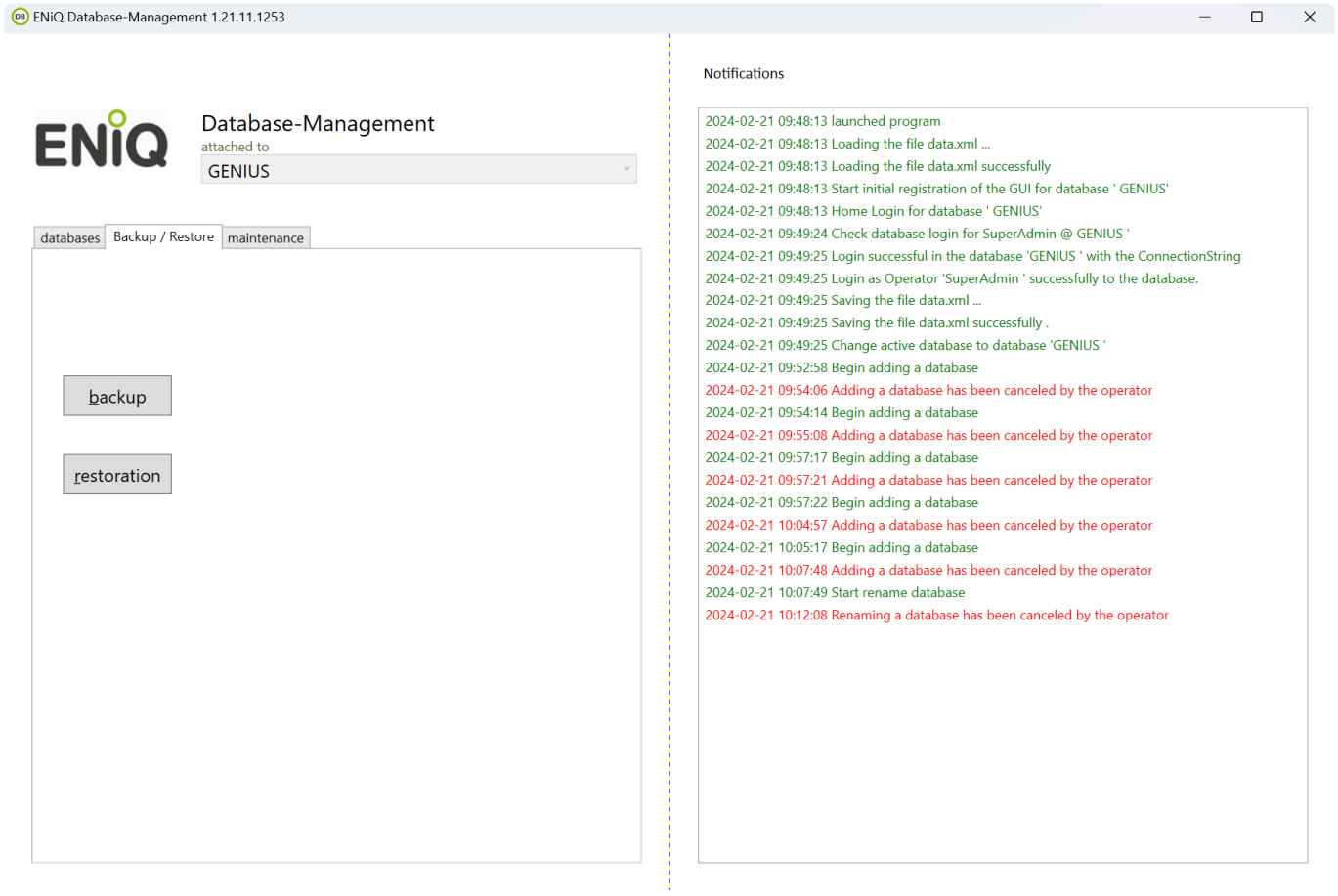
Only letters and numbers are allowed in the name. All special characters and spaces are not allowed.



Since renaming also renames the instance on the SQL Server, this action takes a few seconds.

9.1.2. Backup/ Restore

Backup / Restore



This area contains the functions for backing up and restoring the respective database instance.

Caution: By creating a backup, only the data backup for the currently active database is performed. For multi-DB systems
a backup must be performed separately for each database.

Backup – Create a backup file of the active database

This button creates a backup file of the SQL Server instance for the currently active database. This can be done at any time while the ENiQ Access Manager software is running without any interference.

The created backup files always get automatically a name with the current timestamp (e.g. “GENIUS_2015_07_31_11_17_42.bak”).
Thus, an already existing backup file will not be overwritten.

Restore – the active database from a backup file

This button, restores a SQL Server instance from a backup file for the currently active database.

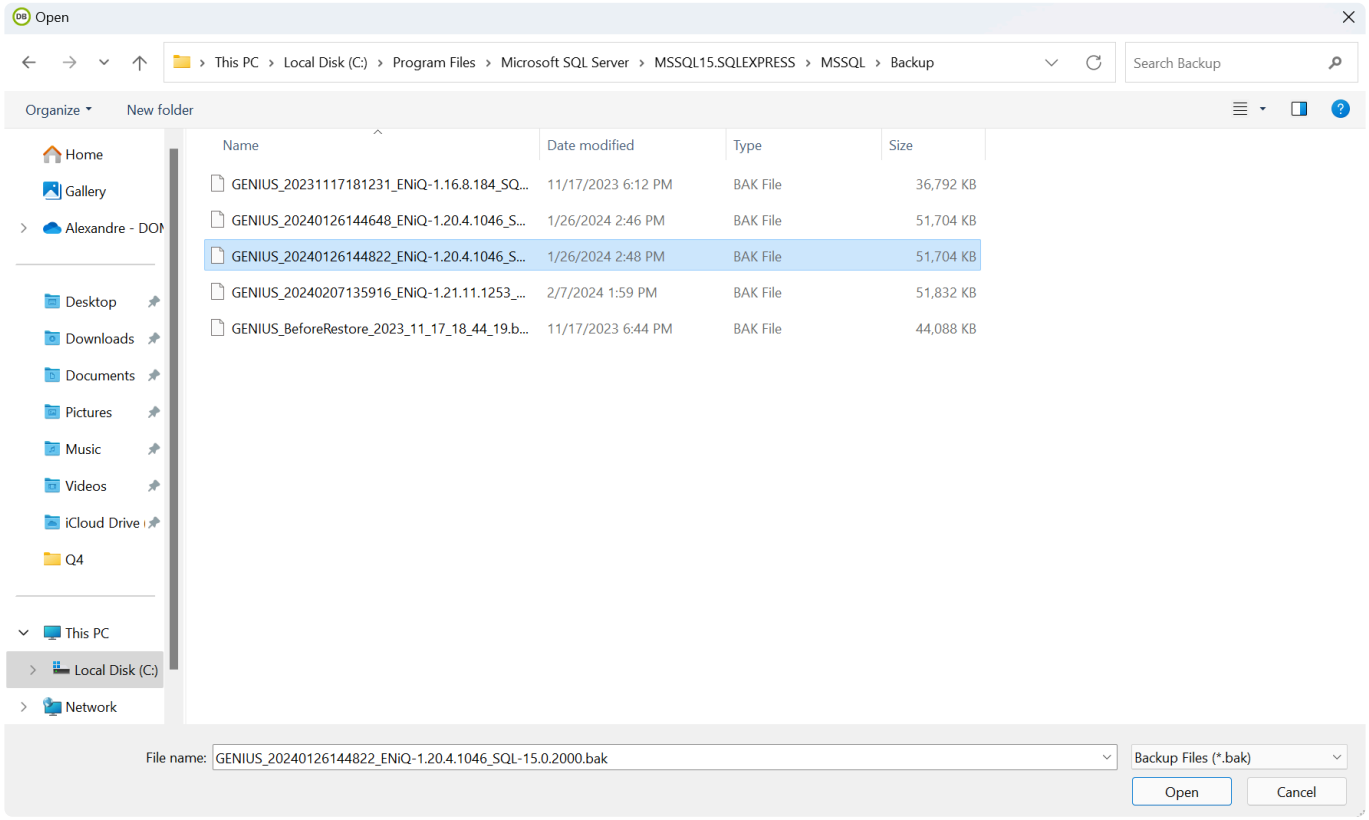
A warning will be displayed if the backup file name indicates it comes from a version lower than the actual installed ENiQ Software. This could lead to data incompatibility.

It is not supported to restore a backup from a version higher than the actual installed ENiQ Software.

A restore cannot be performed while the ENiQ Access Management Software is running, because all connections to the old database are interrupted before the restore is started. The system can be used again only after the recovery has been completed.

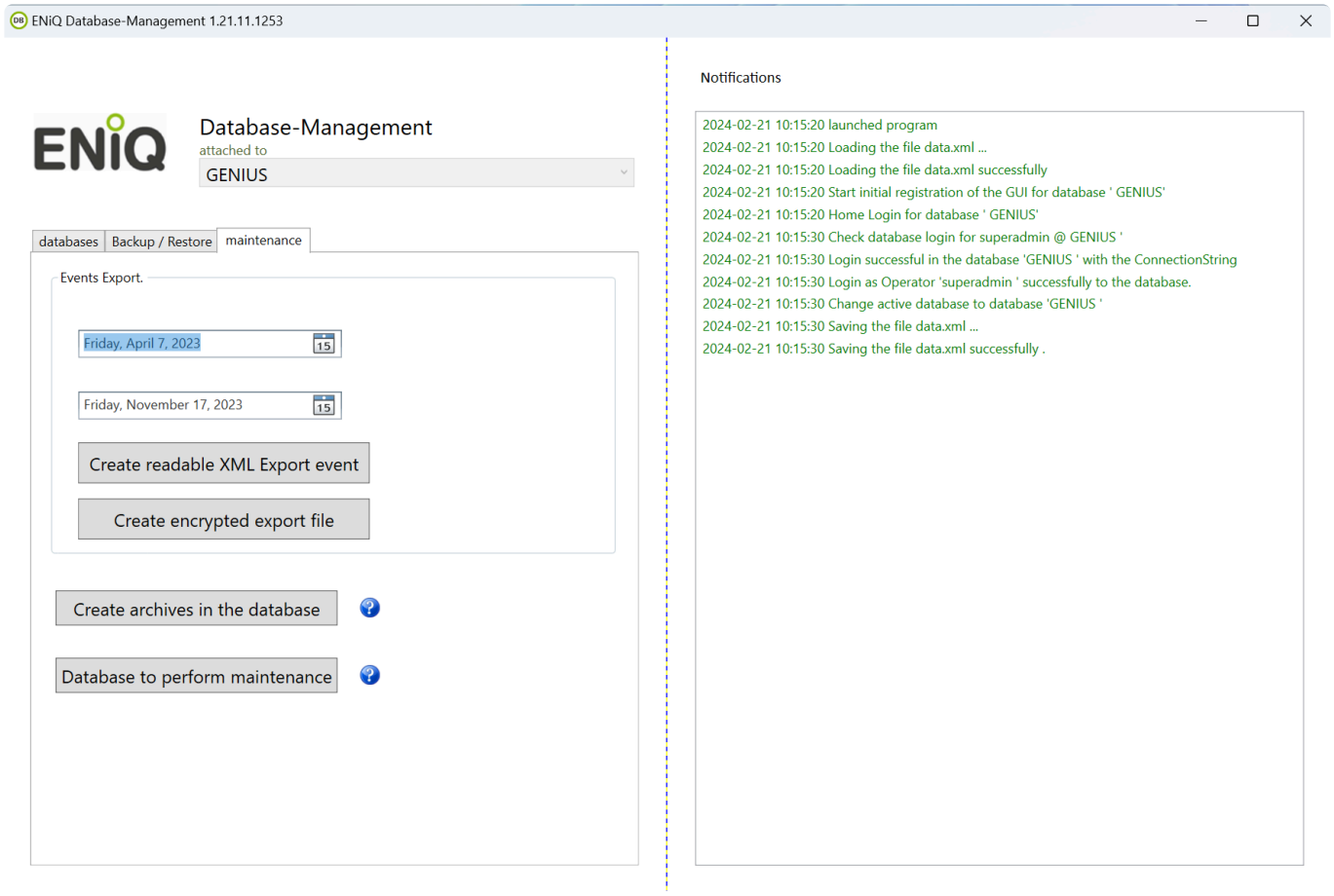
After pressing this restore button, the file selection window opens to select the desired backup file for the restore.

Please make sure that the selected file in the DB Manager is also accessible for the SQL Server, because it must be able to open the file to restore the database. There is no client/server function in this DB Manager version for this function.



9.1.3. Maintenance

Maintenance



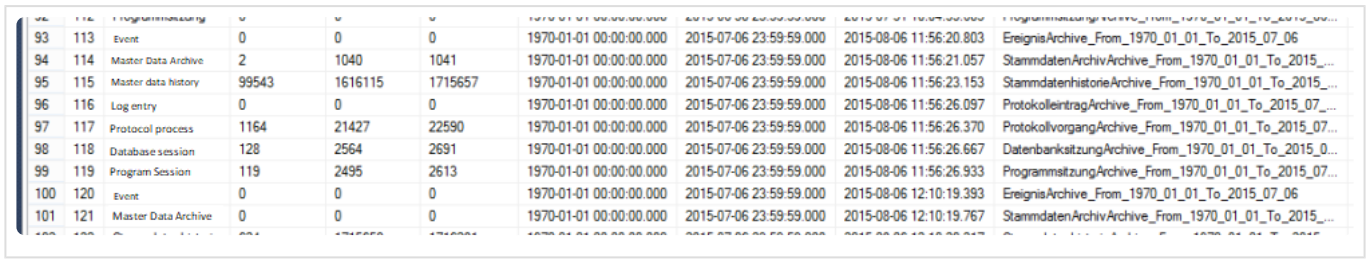
Here is a summary of the event export and database maintenance functions.

Create archives in the database

With this button, old and no longer needed data from the active tables of the selected database are exported and compressed in ENiQ archive files. After archiving, the corresponding records are deleted from the original database table.

This significantly accelerates the database working speed without losing any data. The ENiQ Archive files are saved back to the active database after export and compression. The “ArchiveFileElement” table then contains the following information: Archive record and number of elements per archive record.

The archive files can also be read by future software versions.



93	113	Event	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:20.803	EreignisArchive_From_1970_01_01_To_2015_07_06
94	114	Master Data Archive	2	1040	1041	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:21.057	StammdatenArchivArchive_From_1970_01_01_To_2015_...
95	115	Master data history	99543	1616115	1715657	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:23.153	StammdatenhistorieArchive_From_1970_01_01_To_2015_...
96	116	Log entry	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.097	ProtokolleintragArchive_From_1970_01_01_To_2015_07_...
97	117	Protocol process	1164	21427	22590	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.370	ProtokollvorgangArchive_From_1970_01_01_To_2015_07...
98	118	Database session	128	2564	2691	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.667	DatenbanksitzungArchive_From_1970_01_01_To_2015_0...
99	119	Program Session	119	2495	2613	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 11:56:26.933	ProgrammsitzungArchive_From_1970_01_01_To_2015_07...
100	120	Event	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 12:10:19.393	EreignisArchive_From_1970_01_01_To_2015_07_06
101	121	Master Data Archive	0	0	0	1970-01-01 00:00:00.000	2015-07-06 23:59:59.000	2015-08-06 12:10:19.767	StammdatenArchivArchive_From_1970_01_01_To_2015_...

The function “Create archives in the database” automatically selects all records of the stored tables to be archived in order to archive and delete them.

Only with the events, for security reasons, the events of the last 30 days remain in the database table and are therefore not archived.

In the following tables the records are stored in ENiQ archive files and deleted from the corresponding tables:

- Event
- Master data archive
- History
- Log entry
- Protocol process
- Database session
- Program session

Database Maintenance

This function is a combination of “Create archives from database” and the subsequent shrinking of the real database files on the SQL Server hard disk.

Shrinking the real database files on the server hard disk significantly speeds up the offline synchronization of the ENiQ Access Management software used today.

9.1.4. Explanations

Explanations

Offline synchronization
The operator must have his database stored on the laptop with which he wants to synchronize the devices offline.

Database backup

The database backups can be created per object. However, it is recommended that the operator regularly creates complete backups of his entire database system and keeps it in a safe place. Otherwise, the loss of a notebook with many databases could have fatal consequences.

Not a server solution

The Multi-DB concept is not a multi-server solution. Only one database can be selected and operated at a time. (see above)

ENiQ Software Update

With an ENiQ software update not only program files are updated, but also the database structures/ contents are adapted. This is no problem for the ENiQ software version open DB-Manager software.

An update of the ENiQ DB-Manager software to a multi-DB system can be done at any time. The ENiQ Access Management Software update will update all program parts of the ENiQ DB-Manager Software and after restarting the ENiQ services will automatically update the currently active database.

Note: The update is completed only after the first login to the web interface of the corresponding system.

After an update of the ENiQ software, the individual databases will be updated accordingly after the first activation in the DB Manager.

9.2. PLC management

What are PLC?

PLC programs are small software programs that can be loaded into the ENiQ AccessManager or RF-NetManager. Their purpose is to enable specific behavior of the AccessManager depending on different input configurations and the status of transponders or radio-connected devices such as the ENiQ Pro cylinder.

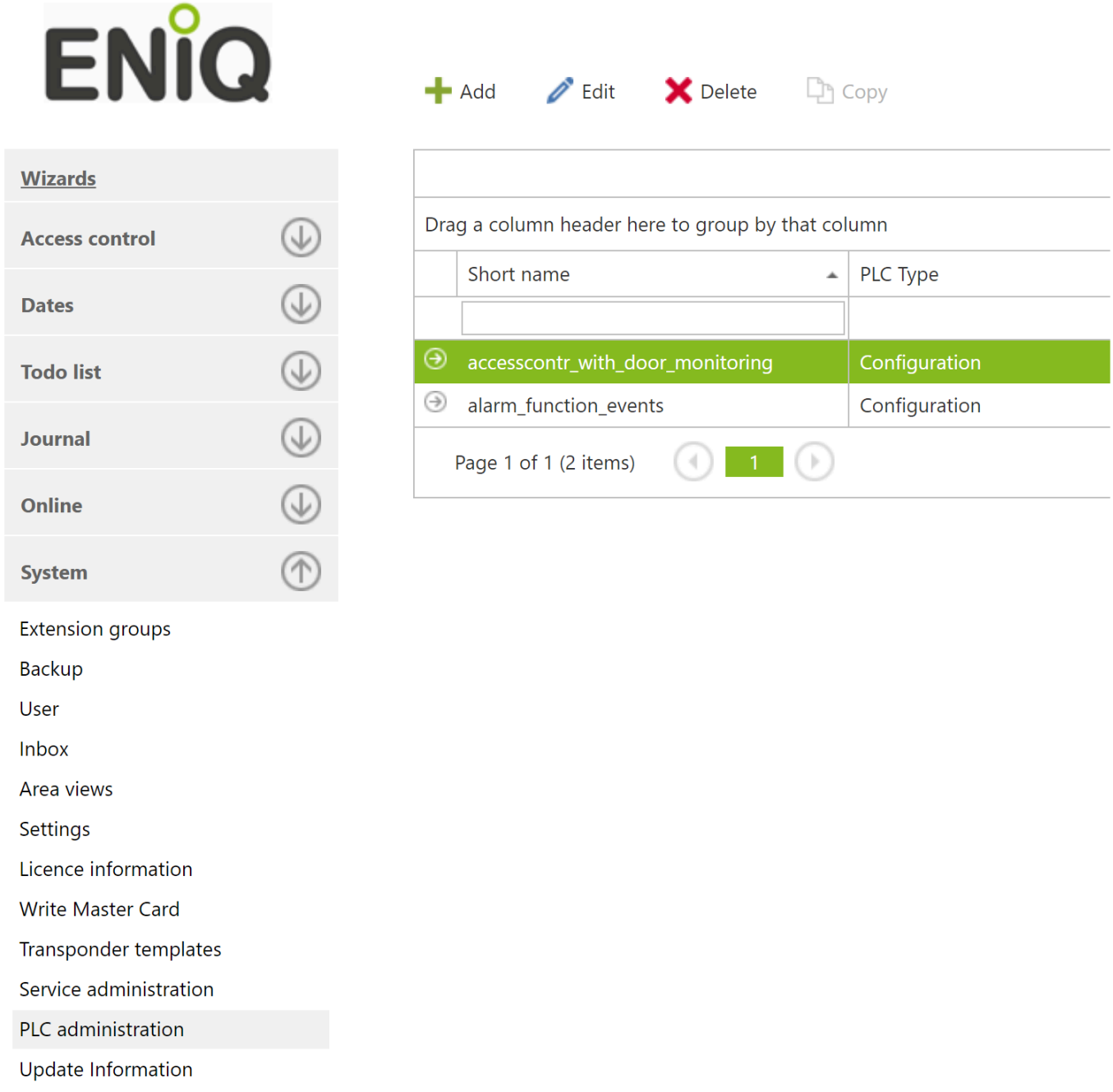
When installing the ENiQ software, 10 pre-configured PLC configurations are supplied as standard. These can be found in the standard installation under the following path:

C:\Program Files (x86)\DOM Sicherheitstechnik\DOM Genius Software\Web\SPS-Presets\

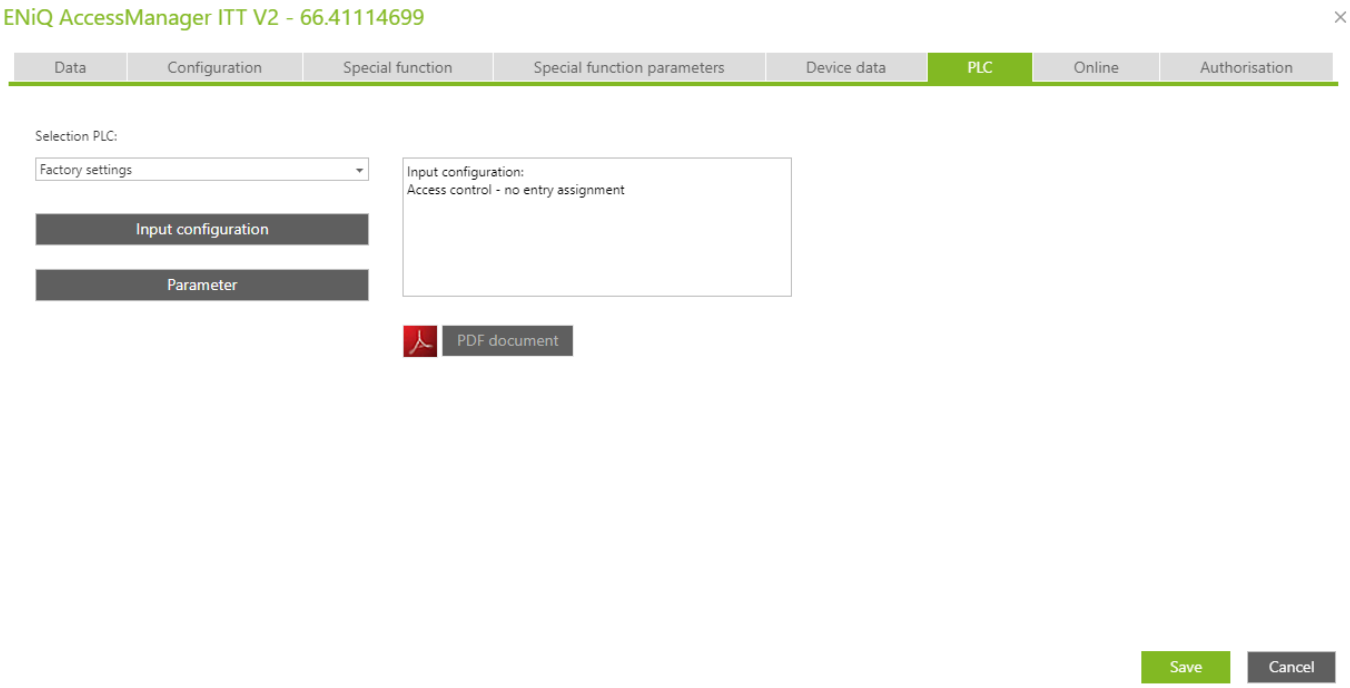
Name	Device	Function
accesscontrol_with_door_monitoring	RF-NetManager	With the PLC ‘access control with door open time monitoring’ access can be monitored and controlled via the input contacts of the controller.
alarm_function_events	RF-NetManager	With the PLC ‘Alarm function events’ the output of the controller is switched depending on the event ‘No release’. The output of the controller can be used to control the sensor e.g. video surveillance, alarm system etc.
burgler_alarm_system	Accessmanager	Control of an intrusion detection system
permanent_closed	Accessmanager	With the PLC ‘Permanently closed’, the AccessManager can be set to the functional state ‘Permanently closed’ via the input contact of the control unit.
permanent_closed_with_feedback	RF-NetManager	With the PLC ‘Permanently closed with feedback’ the actuator can be set to the function state ‘Permanently closed’ via the input contact of the control system.
permanent_open	Accessmanager	With the PLC ‘Permanently open with feedback’ the actuator can be set to the function state ‘Permanently open’ via the input contact of the control system.
permanent_open_with_feedback	RF-NetManager	With the PLC ‘Permanently open with feedback’ the actuator can be set to the function state ‘Permanently open’ via the input contact of the control system.
sluice_function_v3	Accessmanager	The PLC ‘Sluice’ is used to control the transition between two areas by means of a double access

		(e.g. 2 doors), where only one access may have the open state.
weekplanchange	Accessmanager	With the PLC ‘weekplanchange’ a change of the locking media authorization can be made via the input contact of the controller.
weekplan_change_with_feedback	RF-NetManager	The PLC ‘weekplanchange’ can be used to change the locking media authorization via the input contact of the controller.

PLC management can be used to transfer PLC programs to the ENiQ software.



Only PLCs that have been successfully loaded into the PLC management can subsequently be activated in the device configuration of the AccessManager.



Instructions for input configuration and parameters can be found in the corresponding PDF document (see button).

10. Appendix

10.1. Help & Contact

If you have not found the right answer for you here, please contact a specialized store near you or send us a message.

Contact

> +49 2232 704 0
> dom@dom-group.eu
> +49 2232 704 375

Address

> Wesselinger Str. 10-16
> 50321 Brühl
> Germany
> Directions