HÄFELE

ZN 6.162.000.90g

732.29.430

SOFTWARE MANUAL
Dialock 2.0 access control system
Version 8.4

Dialock CONTROL
Dialock HOTEL
Dialock PROFESSIONAL

Access control with experience

HDE 20.12.2023

HÄFELE

Contents

732.29.430

HDE 20.12.2023

732.29.430
HDE 20.12.2023

Key

 Update page immediately

 Page update status indicator

 Create data record

 Select data record

 Select data records which are not available in the system

 Edit data record

 Access authorisation

 Restricted offline authorisation

 Resource group authorisation

 Group authorisation

 Print

 History, audit trails

 Upload / import

 Download

 Calendar selection

 Delete

 Save

 Activate search filter

 Reset and hide search filter

 Extended search filter, evaluations

 Sorting direction

 Reload table

 Display valid only

 Update / reset / execute / generate / restore / bootstrap page area / parametrise MDU

 Generate configuration overview / PIN code / start


Describe transponder / select transponder identification source


Read transponder


Register MDU / find encoder / search for terminal


Install client


Create group


Create time model


Create guest option


Create room plan


Create person


Access matrix, assign authorisation, specify password


Create new segment


Delete segment


Search for time model


Search for person


Display information


Logout

Preface

This software manual is a guideline for users of Dialock software.

The installation and start-up of the Dialock software is generally carried out by a Dialock engineer.

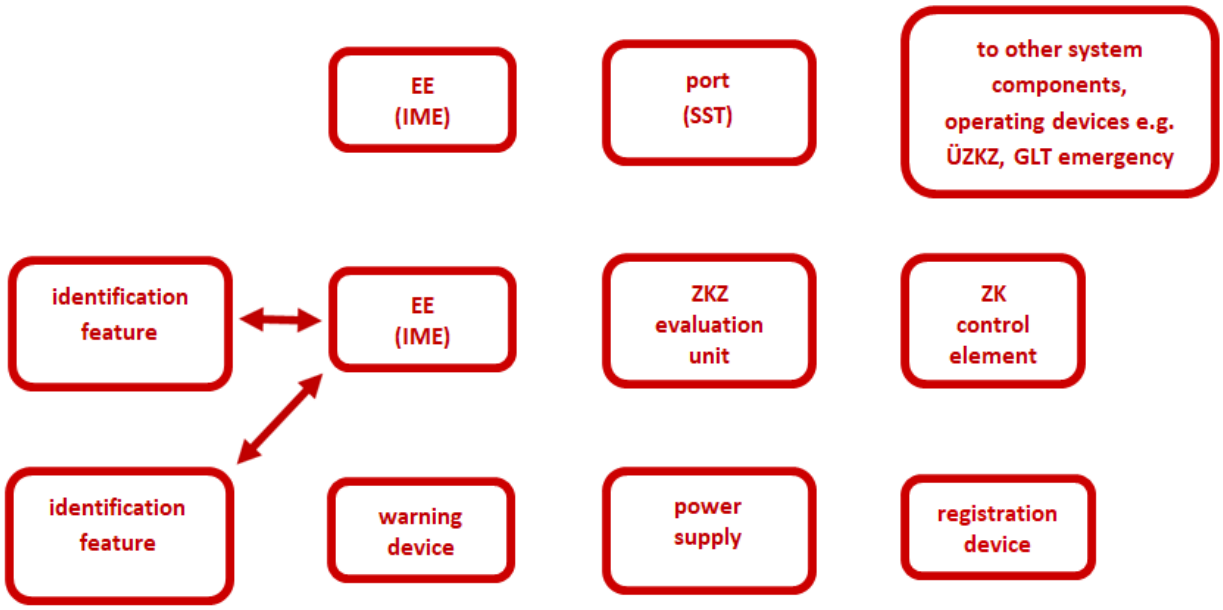
1. General access control

Access control systems are an important topic in the security area, and are networked with different systems such as alarm systems (burglar and fire alarms), emergency exit door controllers, video technology and other building management systems. For large building complexes, access control is often integrated into a graphical control station.

However, an access control system should always be considered in the context of other security alarm systems such as burglar protection, CCTV, fire alarm etc. A good security concept considers all of these aspects and takes the necessary interaction with the adjacent systems into account.

An access control system such as Dialock has the task of controlling and monitoring access to building sections and rooms that need protection and save occurring events and alarms in chronological order so that they can be evaluated at any time.

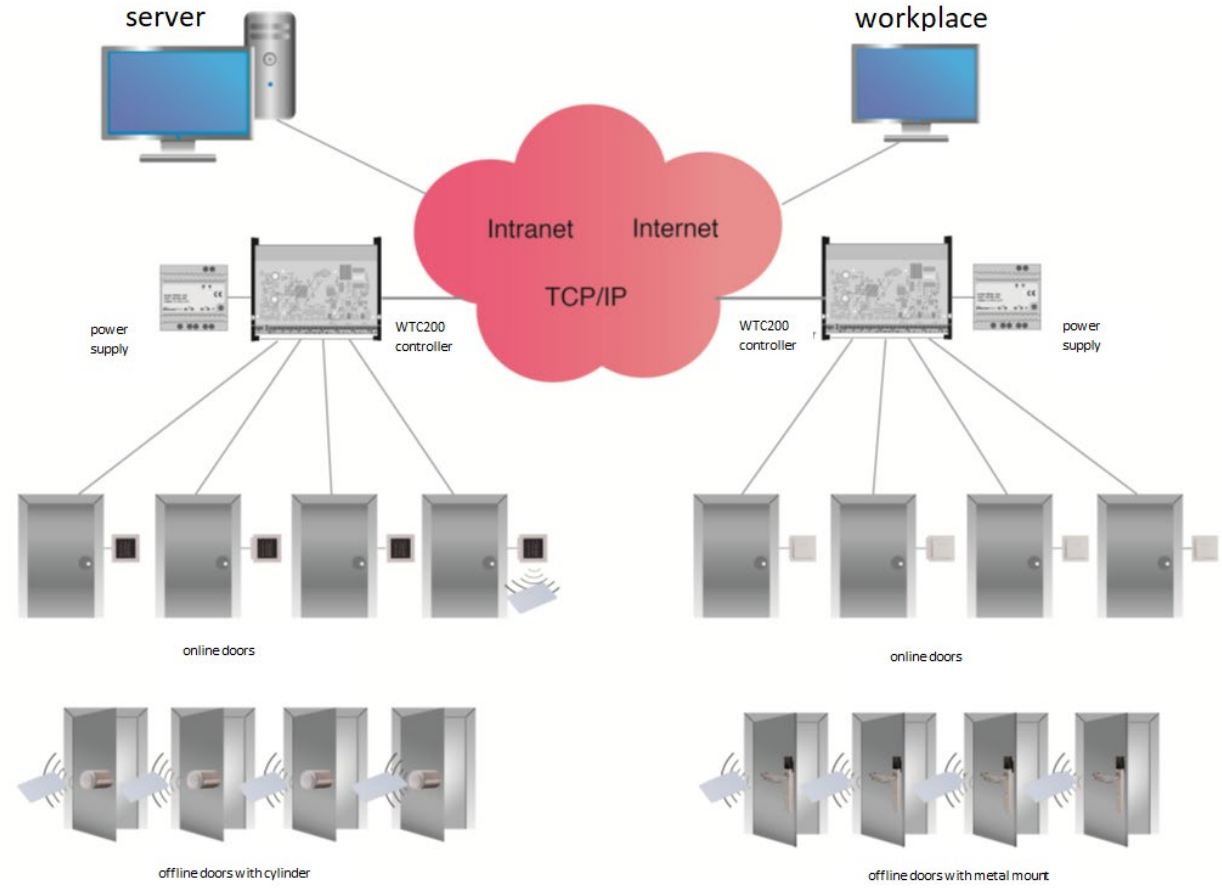
Professional access control systems should include the following function units (source: VdS):



EE = Input device
IME = Identification characteristic acquisition unit
ZKZ = Access control centre
ÜZKZ = Superior access control centre (server)

1.1. Dialock system philosophy

Dialock is based on a modular system concept. It is characterised by its freely scalable hardware and software architecture, its innovative ergonomic user concept as well as simple handling for installation.



1.2. The system overview of Dialock

The modern system architecture of Dialock consequently uses TCP/IP based Internet communication.
Accordingly, the connection from client to server is established (Internet compliant). Thus, installation is very easy and user-friendly. The software concept is characterised by its freely scalable software architecture.

Dialock includes extensive functions - from simple access control equipment up to large company solutions - for all professional applications.

The user carries out reoccurring tasks via appropriate workflow processes which systematically support him in the set-up and administration of the respective logically sequential processes. The operator always administers and maintains all relevant access control data in logical and related dialogue steps. Misuse is prevented by appropriate assistance to the greatest possible extent.

Dialock is characterised by its simple and intuitive user guidance, which makes it easy for the user to implement and administer even complex requirements in the system. Ergonomic and uniform structures of the operating procedures as well as logical automatism are crucial for the convenient operation of Dialock, which eliminates erroneous input or misinterpretation of data to the greatest possible extent. Dialock is characterised by the most advanced technologies and the highest safety standards. Logical links and intelligent plausibility checks in the background simplify the everyday processes.

With Dialock, all online locking points as well as all offline locking points e.g. in the form of Dialock door terminals and Dialock electronic cylinders, are set up and administered.

The solution is rounded off by the hardware platform of the WTC 200 (wall terminal controller). The WTC 200 controller supports all access functions around a door with interior and exterior readers using the currently available transponder technologies.

The Dialock software is web-client based and supports current operating systems as well as tablet PCs and smartphone platforms.

1.2.1. Important core functions of Dialock

1.2.1.1. Validation function

Validation of access media is a very powerful function for increasing security in an integrated access control system. When doing this, access authorisation for **offline access points** is provided for a limited time, but if the user is valid according to the access control centre database, the access authorisation is renewed at regular intervals at a validation terminal on the transponder medium.
The validation terminal is a specially configured online access control terminal which transfers the central or self-saved authorisation data of a user for the offline terminal on this access medium or updates this data on the medium.

In this way, offline authorisation can be restricted to one day so that the employee must always carry out a new validation in the morning.

If a key is then reported lost or stolen, it is automatically no longer valid at any offline terminal the next day. If loss or theft is reported, the validation terminal is notified of this by the administration; if this key is now presented at the validation terminal, no validation takes place and an appropriate alarm message can be sent to the control centre.

A possible security gap at the offline access points is therefore limited to the time between the loss of the medium and reporting to access management.

If a person is moved to another job in a different part of the system, the associated access authorisations for this new job are updated immediately for the affected offline access control terminals during the next validation process.

The key validation concept contributes to maximum operating convenience and maximum security of the system at the same time, and there is no need for a centrally established programming process.

1.2.1.2. Allocation of access authorisations according to groups and / or organisational units

The group authorisation concept rationalises the system and allocation of access authorisations considerably. To do this, one-time access authorisations are determined for a certain user group, e.g. for the persons in accounting. Then, the affected persons are assigned to this “Accounting” group and therefore automatically receive the authorisation profile of the “Accounting” group. In this way, new persons can even be given complex access profiles by assigning them to a group with no effort.

A group can also be a logical summary of access points, e.g. all access points on a certain floor in a building, such as a hotel corridor. The designation could be “Second floor”. Then, this group can be allocated to the relevant persons of the cleaning team, e.g., who receive the access authorisations they require to work on the floors.

Groups can be freely defined and set up, but are often already present as an **organisational unit** of the company (such as “Accounting”, “Development” etc.) and can be directly accepted for access control. The access authorisations are immediately assigned when a new employee joins the organisational unit.

Allocation of access authorisations is simplified enormously by using group authorisation assignment. At the same time, the system becomes comprehensible and easy to display, so that even security-related evaluations are possible, unlike the situation when countless individual access rights are allocated.

1.2.1.3. Client capability

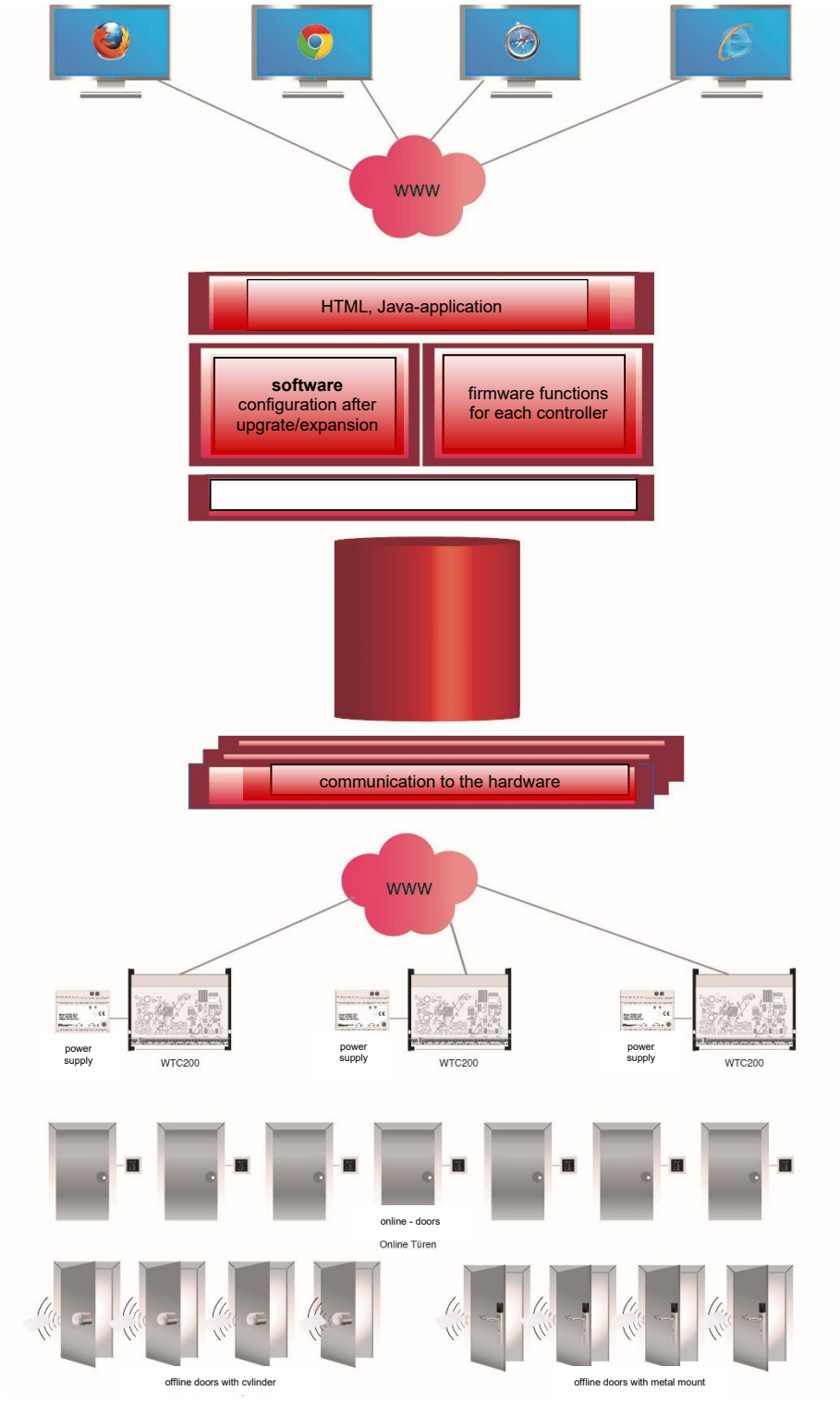
It is possible to administer clients as standard in Dialock PROFESSIONAL. Sensible use can always be made of client management if several parties in a building such as different companies are to be managed individually. When doing this, each client organises and manages its own access authorisations independently. This can be in an office building in which different companies are renting, or in entire office parks. Each client receives the necessary resources assigned to them and can use them as requested and invisibly to other clients.

The advantages of Dialock client management are clear subdivision of access areas and a considerable cost saving compared to individual separate system installations (hardware and software!) and licensing.

Shared use of data in multi-party buildings such as main and secondary entrances, car parks and lifts (overlaps) can be achieved without a great deal of effort.

The more clients share a Dialock system, the quicker the costs are redeemed.

Up to **50** clients can be set up (**5.7.11** *Client management*).


WWW
HTML, Java-application
software
configuration after
upgrate/expansion
firmware functions
for each controller
communication to the hardware
WWW
power
supply
WTC200
power
supply
WTC200
power
supply
WTC200
online - doors
Online Türen
offline doors with cylinder
offline doors with metal mount

1.3. Prerequisites

1.3.1. General

The different operating systems make different demands of the computer.

With Dialock, the user is essentially independent of the operating systems. Internet or Intranet access to the web server is required.

Transactions take place at the access points via the corresponding acquisition units such as readers or access terminals.

1.3.2. System requirements

Detailed information about the system requirements can be found in the separate document "**System Requirements**" / Dialock 2.0 Access control system (732.29.431).

1.3.3. Conditions for secure operation of Dialock

The conditions are requirements of the operational environment of Dialock. The security of Dialock can only take effect if the conditions are fulfilled accordingly.
The requirements that are made of the operational environment which are described in this user manual are both the responsibility of the operator of the server system on which Dialock is running and the responsibility of the user of the web browser on the client system.

1.3.3.1. Secure operation of the server system

The following components are installed on the server system:

- Dialock CONTROL, HOTEL, PROFESSIONAL
- Database
- Application server
- Message queue

1.3.3.2. Physical conditions

Physical access
Physical access to the server system and all of the necessary Dialock operating material is protected by means of suitable organisational measures in order to make unauthorised physical access difficult.

Protection from modifications

All server system components which are critical for the implementation of security, are physically protected from unauthorised modification by potential attackers.

1.3.3.3. Personnel conditions

Competent administrator
At least one competent administrator is responsible for the installation and ongoing administration of the server system and that the systems are installed and administered correctly. The administrator is responsible for regular monitoring of the data.

Minimum allocation of authorisations
The users are set up by the administrator so that they only have the rights that are needed for their tasks.

Trusted administrator and user
Both the administrator and the users must be trustworthy and sufficiently trained so that they are in a position to carry out their tasks properly.

1.3.3.4. Conditions for Internet connections

Encrypted connections only
Only encrypted https connections from the Internet to the web server may be set up. It must not be possible for an attacker to read or manipulate the data traffic.

Secure encryption algorithm
For encrypted connections, a sufficiently strong encryption algorithm must be used which is not vulnerable within a reasonable time. Non-secure encryption algorithms whose key length is too short or that have design weaknesses must not be used.

Connection establishment only with valid certificate
In order to establish an encrypted connection, a valid certificate from an accredited certification authority must be used so that a user can verify the authenticity of the server and establish a connection.

In the case of an SSL installation of Dialock, the SSL certificate used by the web server can be downloaded and installed directly on the login page using a hyperlink.

Suitable content filtering system
Systems must be installed upstream of the web server that repel attacks via the web interface in an appropriate way. This can take place by means of a combination of an Intrusion Detection System (IDS), Intrusion Prevention System (IPS) and a reverse proxy.

1.3.3.5. Conditions for system management

Data protection concept
A data protection concept must be available and in operation for securing the data in order to prevent data loss.

Protection of the network interface
The network interface of the server system must be sufficiently protected against attacks (e.g. firewall).

Current software
After release by Häfele, the software used on the system must be updated to the latest version regularly and promptly.

1.3.4. Secure operation of the client system

The client system is responsible for data inputs and outputs. The following conditions must therefore be realised so that the system can provide adequate protection against different types of attacks:

1.3.4.1. Physical conditions

Spatial boundaries

Access to the client systems must only be possible for permitted users.

1.3.4.2. Personnel conditions

User training

The number of authorised users must be numerically limited.

All users must be appropriately trained so that they can operate Dialock properly.

1.3.4.3. Conditions for Internet connections

Checking the secure connection
The user must be sufficiently sensitised to check the security certificates that are transmitted by the https protocol when establishing a connection to Dialock.

Tightening of the network interface

The network interface must be adequately secured against wilful intrusion from outside, e.g. by switching off network services or setting up a firewall.

1.3.4.4. Conditions for system management

Current software
The software installed on the system must be regularly updated to the latest version so that possible security gaps can be closed. The web browser must also be updated regularly.

Virus protection

An up-to-date virus scanner must be used regularly so that viruses and other malware can be detected and removed.

2. The Dialock software versions

In order to optimally fulfil the different requirement of possible application areas from small operations to the hotel industry all the way to administrative bodies and industrial companies, Dialock is available in different functional versions.

Depending on the version which is used, different functions appear greyed out in the software and can therefore not be selected.

The expansion options for persons and / or access points are recorded in the software via a separate license key and allow an appropriate increase in the number of persons and / or terminals.

Detailed information about the Dialock software can be found at: www.hafele.com

2.1. Dialock CONTROL

Dialock CONTROL is access control software for locking map with simple time profiles for small to medium-sized companies.

The solution is rounded off by the hardware platform of WTC 200 (wall terminal controller). The WTC 200 supports all access functions around a door with interior and exterior readers. An authorisation writing terminal (validation terminal) can also be realised with the WTC 200 and a WRU 200 / WRU 400 reader, with which access authorisations for offline locking points can be updated at regular intervals.

2.2. Dialock HOTEL

Dialock HOTEL is the modern access control software for small, medium-sized and even large hotels. With interfaces for all common hotel management system solutions, Dialock HOTEL not only supports the creation of guest keys, it also controls access to other operator services such as use of wellness areas, the car park or the underground garage.

The solution is rounded off by the hardware platform of WTC 200 (wall terminal controller). The WTC 200 supports all access functions around a door with interior and exterior readers. An authorisation writing terminal can also be realised with the WTC 200 and a WRU 200 / WRU 400 reader, with which access authorisations for offline locking points can be updated at regular intervals.

The standard licence packages of Dialock HOTEL range from 20 people / 20 access points (20/20) to 500 people / 500 access points (500/500) and can be extended even further.

2.3. Dialock PROFESSIONAL

Dialock PROFESSIONAL is the modern access control software for small, medium-sized and even large access control systems in authorities, administration, education providers, hospitals or industrial companies. The solution is ideally suited for projects that require increased security, organisational efficiency, flexibility and operating convenience.

Dialock PROFESSIONAL supports the creation and administration of locking media for persons for the online and offline access points of the system.

Dialock PROFESSIONAL also makes it possible to administer clients (**5.7.11** *Client management*).

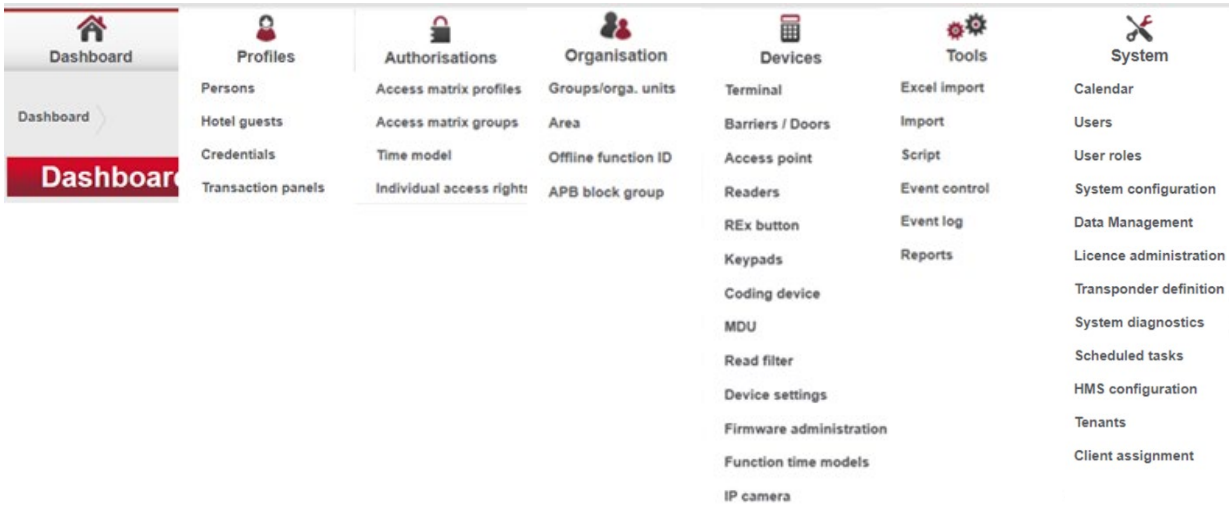
The solution is rounded off by the hardware platform of WTC 200 (wall terminal controller). The WTC 200 supports all access functions around a door with interior and exterior readers. An authorisation writing terminal (validation terminal) can also be realised with the WTC 200 and a WRU 200 / WRU 400 reader, with which access authorisations for offline locking points can be updated at regular intervals.

Note:

The number of encoders (ES 110) is generally unlimited with Dialock. However, the number of encoders with the Dialock **HOTEL** and Dialock **PROFESSIONAL** software variants is limited for the HMS Interface. Individual licences can be extended at any time.

3. The structure of Dialock

3.1. Overview of the modules in the dashboard



**Display is project-specific and dependent of the user authorisation*

The dashboard represents the highest level of the software operation. All main menus are set up here. The corresponding submenus appear as drop-down menus in the main menu.

The structure of Dialock is orientated to the user's tasks.

Profiles
Persons (such as employees), hotel guests, transponders and the transaction panel are depicted with profiles. Central administration of personnel data and log entries take place here. Under HOTEL GUESTS, the room name and the current reservation as well as the assigned transponder can be depicted. Administration of the associated data for the hotel room takes place in the HMS software.

Authorisations
All access authorisations are administered according to location and time here.

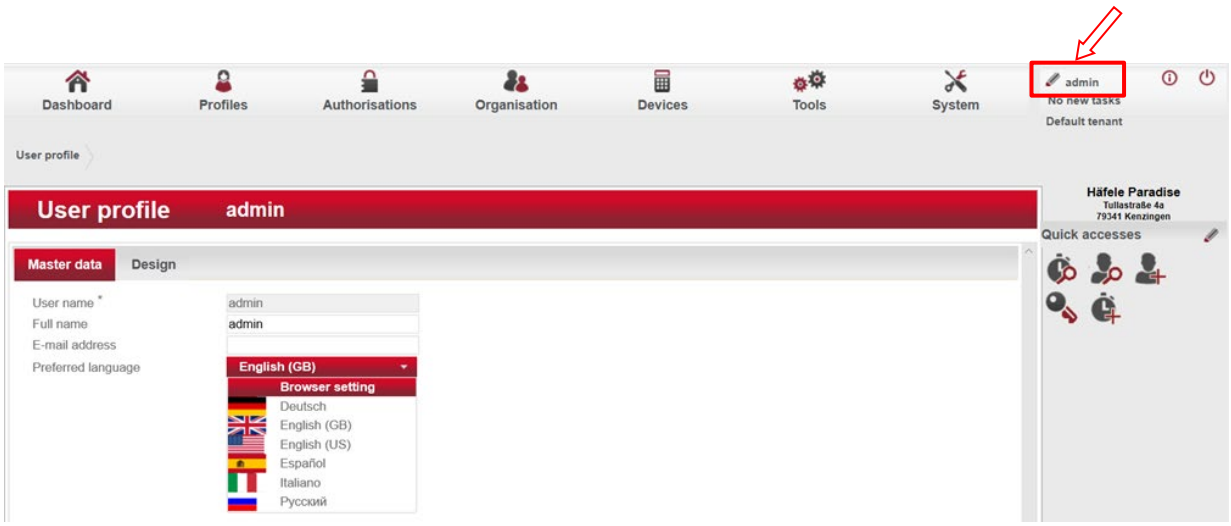
Organisation
In this area, organisational units of employees and access areas (access points such as doors etc.) are summarised in order to efficiently organise subsequent editing.

Devices
The hardware structure of the access control system is administered here, together with all of the associated parameters.

Tools
Under this menu item, special functions such as data import/export as well as automatic event control are defined and terminal event logs and user list reports are displayed.

System
In this menu item, all parameters for the software system are administered.

Language
The language of the software is automatically displayed and adjusted in your browser as “preferred language”. If this language version is not available, the English version is used. However, the logged-in user can set the language via “Change user profile”, regardless of the browser setting.



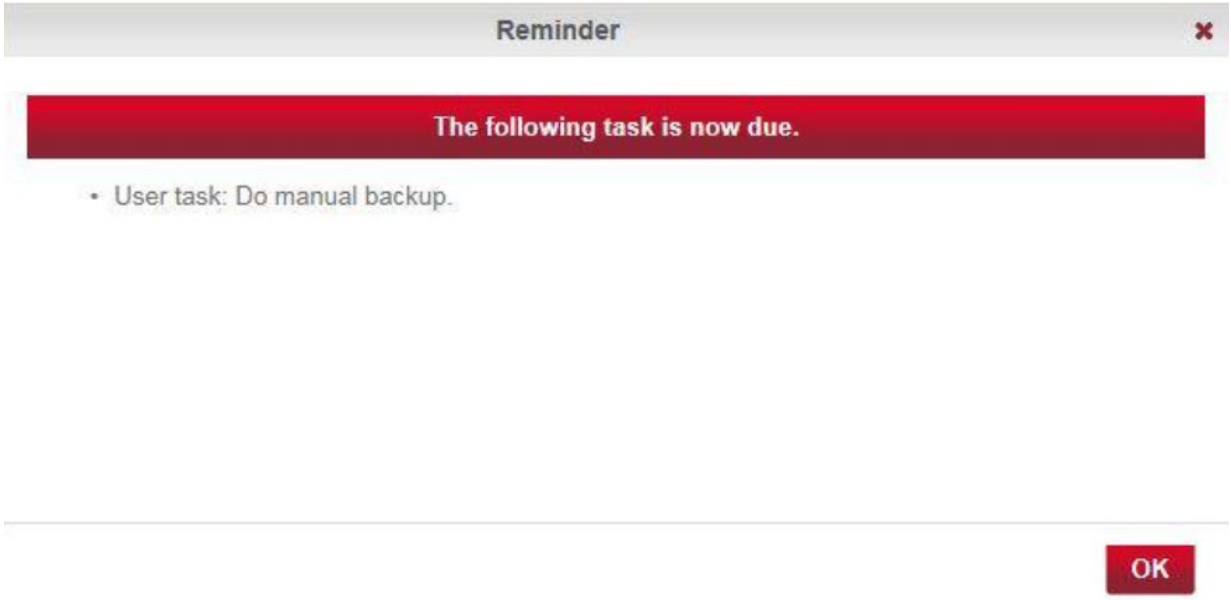
The Dialock software is currently available in German, English (GB/US), Spanish, Italian and Russian.

4. Working with Dialock

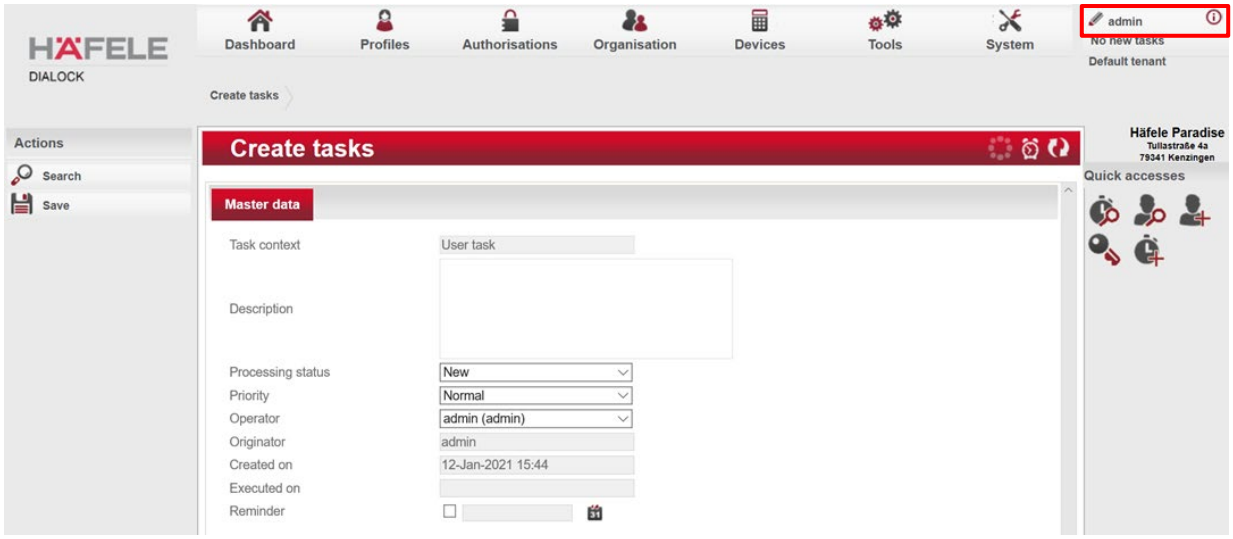
4.1. Tasks

As soon as data that concerns peripheral devices, for example, is modified in Dialock (e.g. time periods that are saved in Offline devices), Dialock automatically creates a task for the relevant user. The changes are usually made using a programming unit or programming transponders which are connected at the workplace and programmed.

Another example (see below) for automatic creation of a task is changing the SD card, which is signalled automatically in the system.



By clicking on “x **new task**(s)” or “**no new tasks**” at the top right below the user name, you can also create these for yourself and other users manually.



732.29.430
HDE 20.12.2023

In the **Description** field you can note down the task and details concerning it.

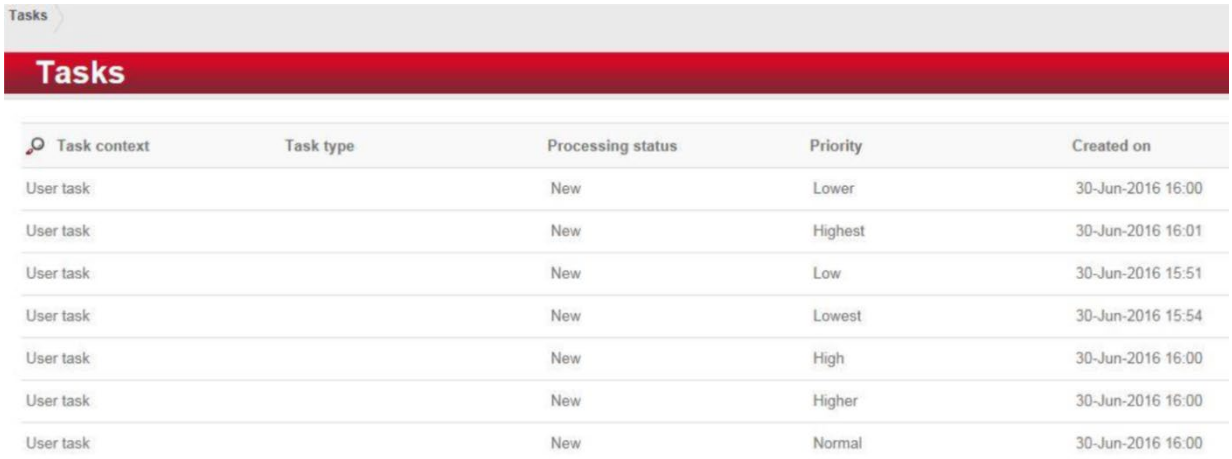
Under **Processing status** you can select between “New”, “Aborted”, “Completed” and “In progress”.

If required, you can classify the task with an appropriate **Priority**.

If you wish to assign the task to another user, then select the relevant **Operator** from the drop-down menu.

Define the date and time under **Reminder**.

As soon as the task has been defined as “Completed”, for example, and saved, the storage date and time appear in the field **Executed on**.



Task types:

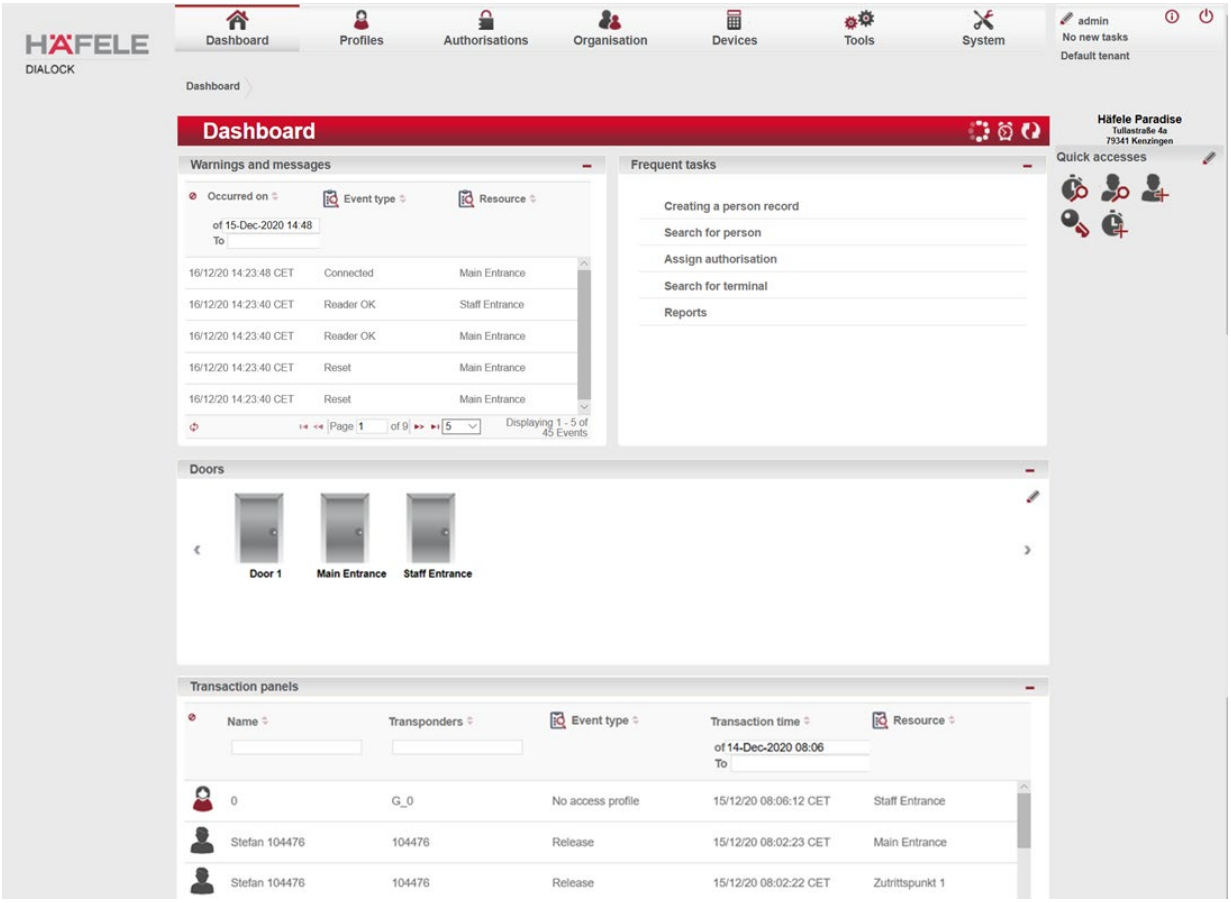
Dialock assigns the task type automatically, depending on the task.

User defined:	manual recording
SD card:	an SD card has been replaced at the controller and has to be checked prior to activation.
Offline hardware:	the parameters of the offline system must be modified here.

5. The modules

5.1. The dashboard

The dashboard is freely definable for each user and clearly represents all of the system data and function modules that are important for the user depending on the arrangement.



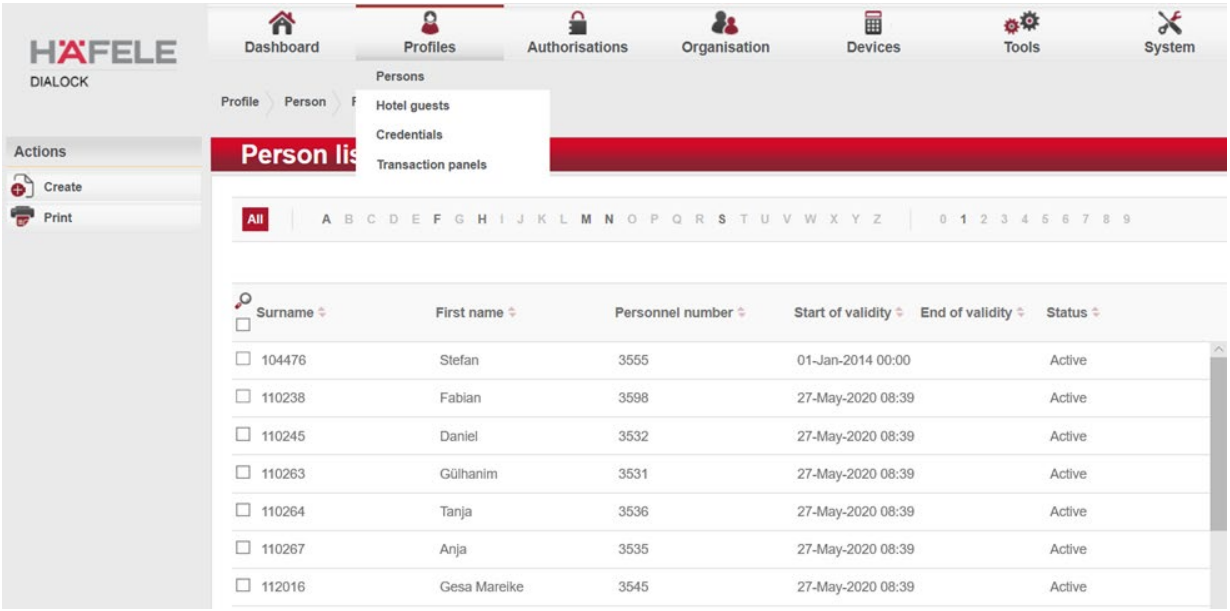
Among other things, the dashboard also represents the system events that are important for the user. A navigation aid for all of the system-related administration areas is also present.

5.2. Profiles

The persons to be created in the access control system, including the associated different authorisations, identifiers (PIN codes and transponders), events and group memberships are managed in this module. The transaction panel can also be found here (**5.2.4** *Transaction panel*)

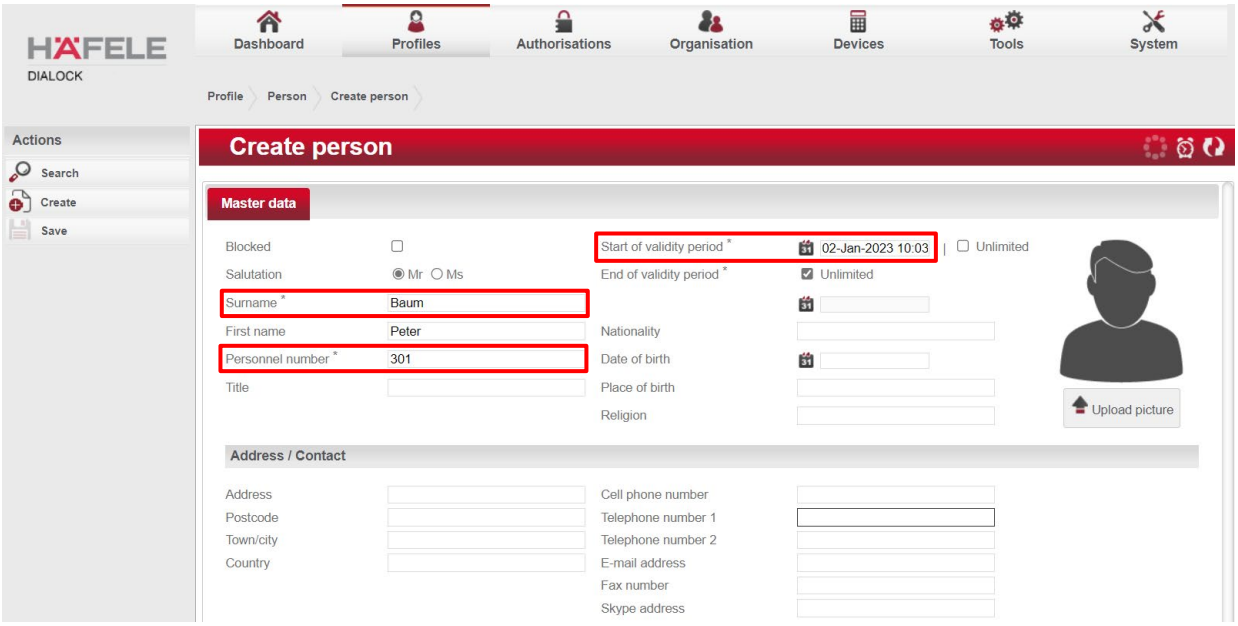
5.2.1. Persons

Personnel data maintenance is a main constituent of the software, and is located in the "**Profiles / Persons"** module. All of the users that are created are listed in the **Person list**. The personnel data can be updated by selecting a user.



5.2.1.1. Create person

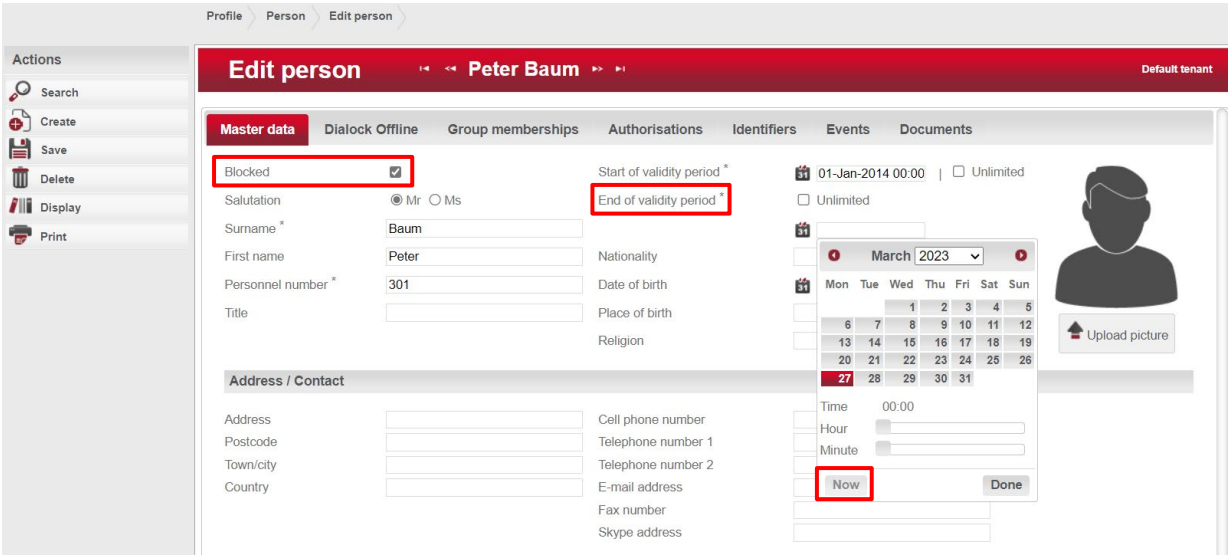
You can create new persons using the “**Create**” button in the left-hand action bar and assign at least the mandatory **(*)** “**Surname**, **Personnel number** and the **Start of validity** (of master record)” fields to them in the **Master data** tab.



If no **personnel number** is entered, Dialock automatically provides a consecutive number, if this has been activated (**5.7.4.1** *System*).

The validity range limits the duration of all assigned person authorisations. Dialock automatically sets the **Start of validity** to the input date and the **End of validity** to “unlimited”.

Block a person by setting “**End of validity”** to **“Now”,** if you wish to remove their access authorisation immediately. Deactivate the “Unlimited” check box beforehand (remove tick mark).

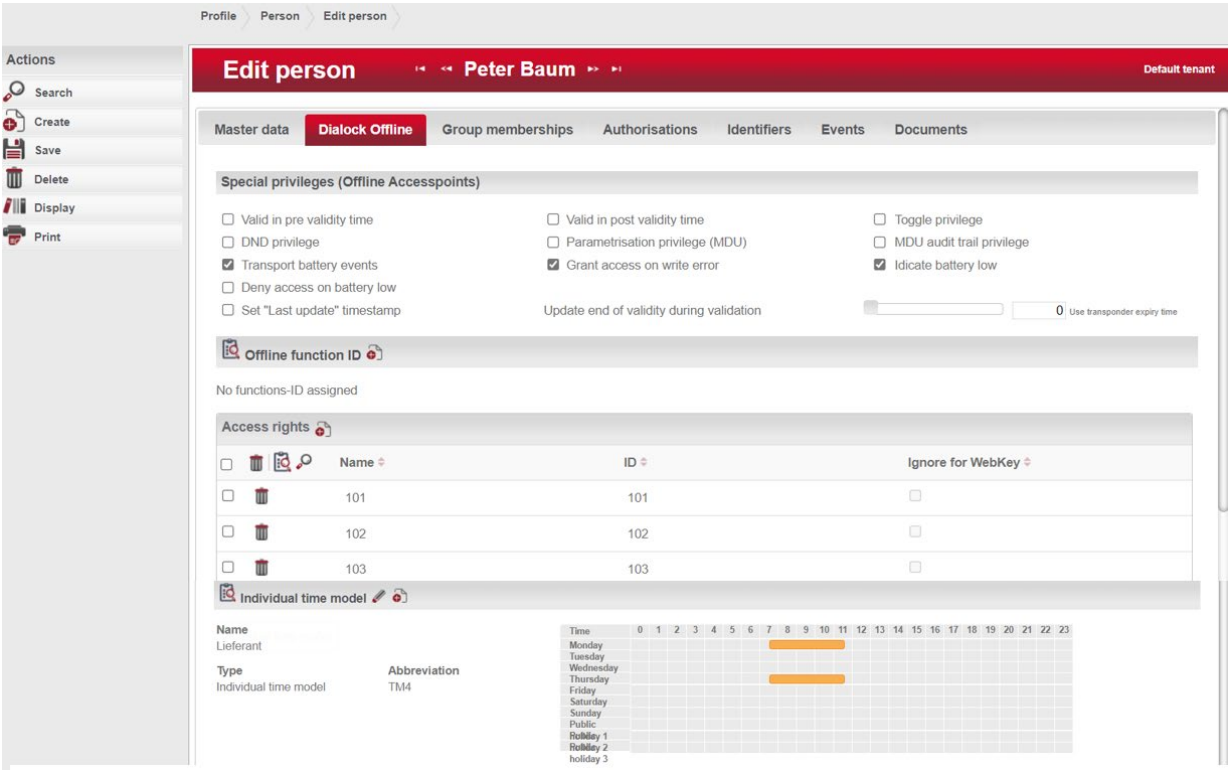


Enter further information depending on requirements.

Then save the data. 

5.2.1.2. Dialock Offline

A list of the offline authorisations of the selected person is displayed in the **Dialock Offline** tab. Here, you can change settings for the offline areas, and assign individual access rights and time models.



Valid in pre validity time:
The activation causes the time validity to be extended accordingly if a defined pre validity time is parametrised at an offline access point.

Valid in post validity time:
The activation causes the time validity to be extended accordingly if a defined post validity time is parametrised at an offline access point.

Toggle privilege:
If this privilege is set, an authorised person may operate this transponder terminal in toggle mode, i.e. open / close.
This option is effective if the toggle mode is activated during a corresponding time period within a time model or by holding up the transponder for a long time.

DND privilege:
If the “Do Not Disturb” function is activated at an offline terminal, this status can be overridden by the transponder which is assigned to this person. Example: Management key in a hotel.

Parametrisation privilege (MDU):
This authorises a person to make changes to the configuration of the offline terminals using the MDU data transfer unit 110 (Mobile Data Unit 110).

MDU audit trail privilege:
This authorises a person to read the access logs of the offline terminals using the MDU 110.

Transport battery events:
If this option is set, battery messages from the offline components are sent back into the system via this person’s transponders.

Grant access on write error:
If this option is set, this person is also granted access if the writing of the battery message to the transponder fails.

Low battery indication:
If this option is activated, the locking components acoustically and visually signal whether the battery is low to the person when they enter.

Deny access on battery low:
If this option is activated, this person can no longer access doors whose locking components have detected a weak battery.

Set “Last update” time stamp:
If this option is set, the “Last update” time stamp of the transponder is set to the current time during validation by the authorisation writer (validation terminal). The offline terminal settings decide the maximum amount of time since the last update before the transponder becomes invalid.

Update end of validity during validation:
If a user books at an authorisation writer (validation terminal), the end of validity for offline terminals is changed according to these settings:

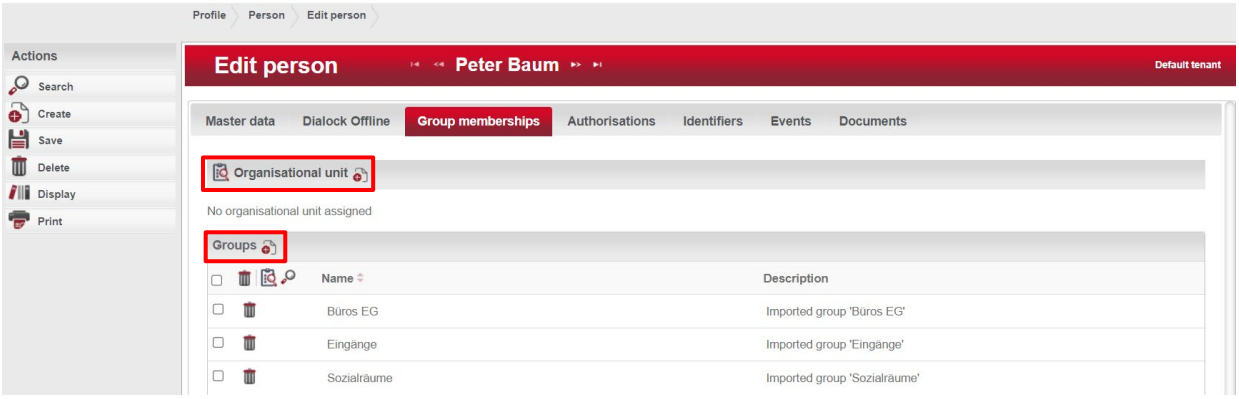
- With a value of 0, the transponder is not modified and uses the general validity of the transponder (see “Identifiers” tab).
- With a value of 1 to 9000 hours, the transponder’s time period is set to the specified value in the future
  (e.g. value set to 24: end of validity on offline terminals = current time + 24h)

5.2.1.3. Group memberships

In the “**Group memberships”** tab, you can then assign the person an **organisational unit** from the drop-down menu.

You can also assign this person to one or more **groups**. The person automatically receives the rights for this organisational unit or group.

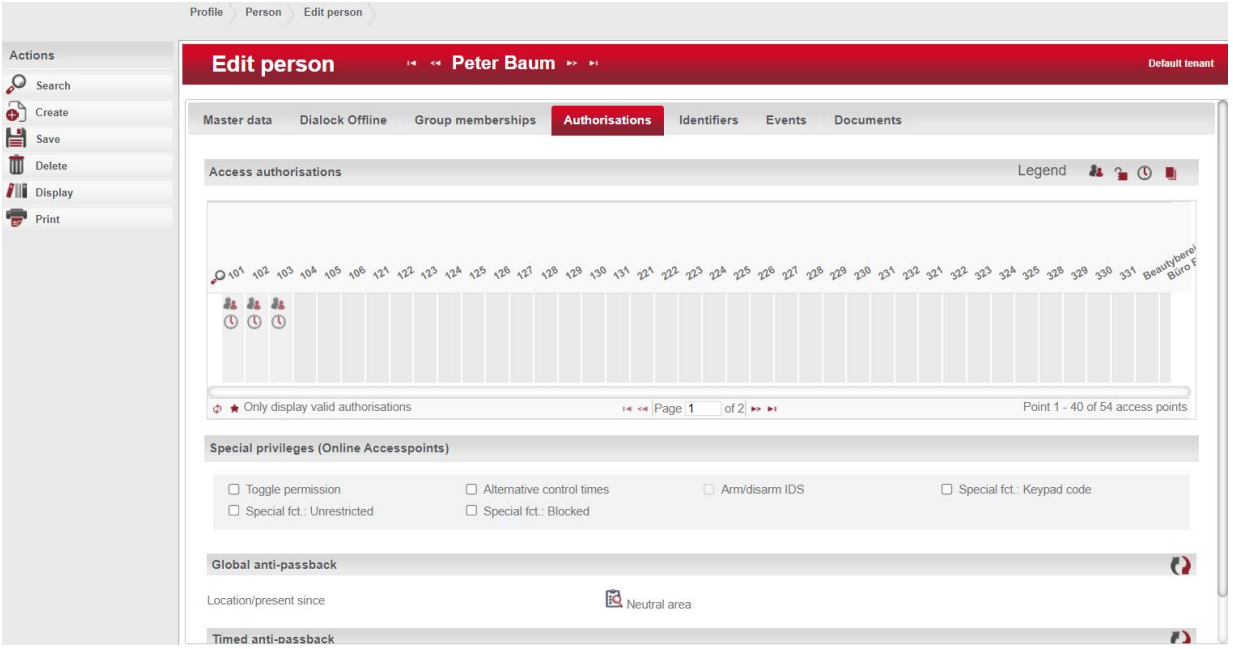
A person may belong to only <u>one</u> organisational unit, but <u>several</u> groups.



5.2.1.4. Authorisations

This is where the authorisations of the selected person are displayed and edited. You can assign the created time models individually in the “**Authorisations”** tab.

In the following example, you can see that individual time models have been assigned to person “**Peter Baum**”.



5.2.1.5. Identifiers

You can create, edit or delete personnel transponders under **Transponder** in the “**Identifiers”** tab. PIN codes can also be generated here.

A person must be assigned at least one identifier, so that they can be identified at an access point and permitted access.

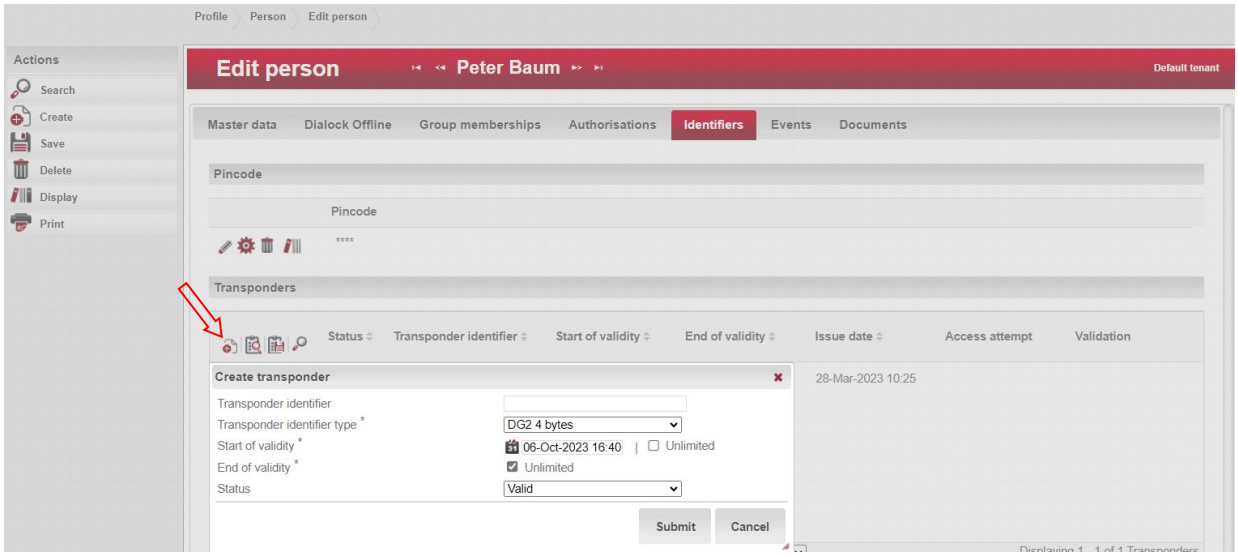
Transponder identification:

To create a transponder, click on the symbol and enter the **transponder identifier** of the respective identification characteristic in Dialock.

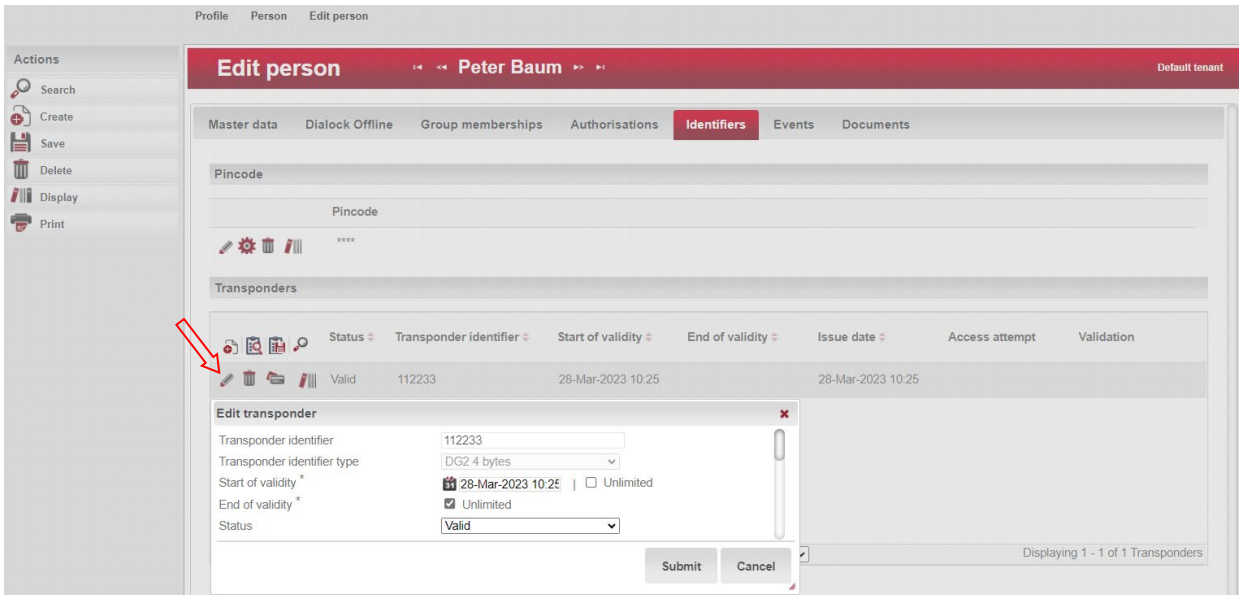
Dialock automatically sets the **Start of validity** to the current date. The **End of validity** is automatically set to “unlimited” if the end of validity of the person master record is set to unlimited.

Otherwise, Dialock automatically takes over the end of validity entered into the person master record.

Activate or deactivate a transponder in Dialock via the **Status** drop-down field. **Valid** status means that the transponder is active. All other statuses (locked, missing, forgotten) result in the deactivation of the transponder in Dialock. Save your entries.



To **Edit,** i.e. to change the validity range and the status of the transponder, click on the pencil icon.

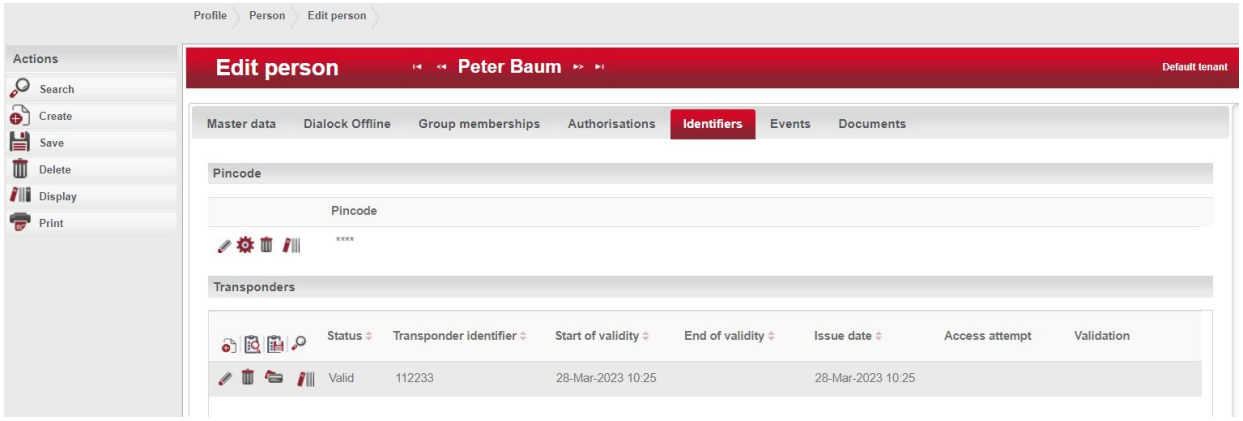


The transponder is **deleted** by clicking on the symbol. However, this only works if the transponder does not yet have any bookings.

On the basis of the **History** you can see which processing steps have already been taken with this transponder.

Notes:

1. The validity range of the person in the master data is of overriding importance to the validity range of the transponder.
2. One person can be assigned multiple transponders.
3. The maximum validity of the transponder is limited to the validity range of the person.
4. A transponder is only loaded in the peripherals (hardware) if it has been assigned access authorisation. The transponder data is only transmitted to those controllers to which an access point that is authorised for the transponder is connected.



You can list the history of when a transponder was last edited, which status was changed when, who the owner of the transponder is, and the start and end of validity etc. using the Info button.

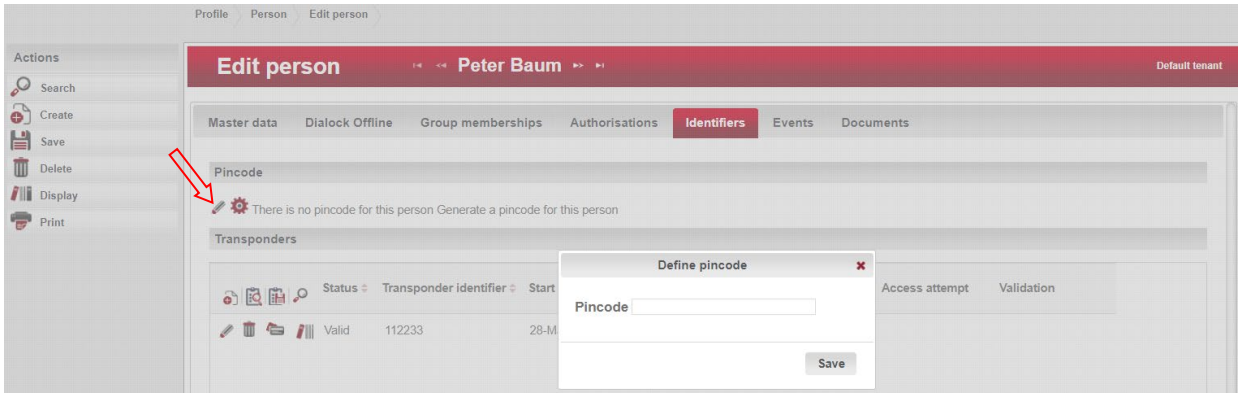
PIN code identification:

A prerequisite for PIN code identification is the use of a wall reader with a keypad and the “PIN Code” licence option.

A transponder must also be created in order to use a **PIN code** as a unique identification characteristic. This does not have to be physically coded or output, but is only used for logging the booking history. For this reason, when a data import is carried out using the Import function, the transponder ID and the transponder type must generally be specified (**5.6.1** *Excel Import*).

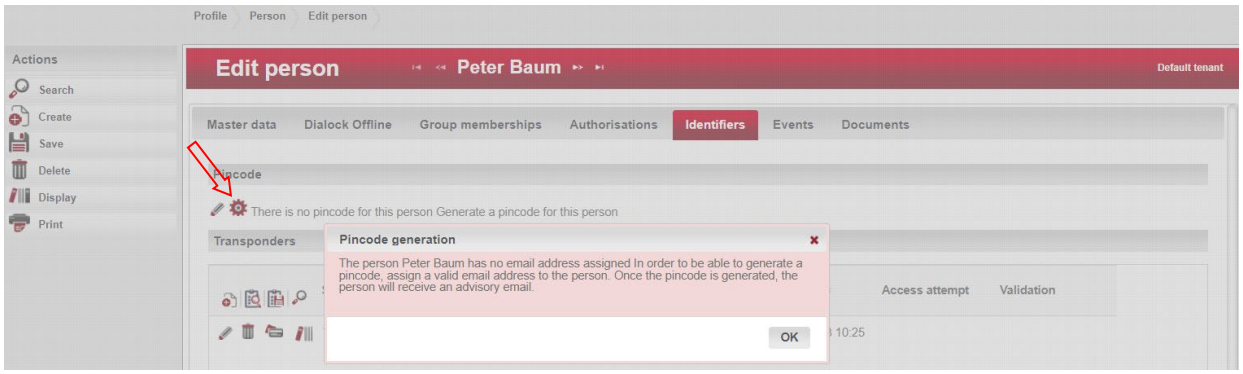
In other words, create a transponder as described above and then generate a **PIN code**.

Manual PIN code generation:
Issue a PIN code using the symbol, and forward this to the relevant person manually.



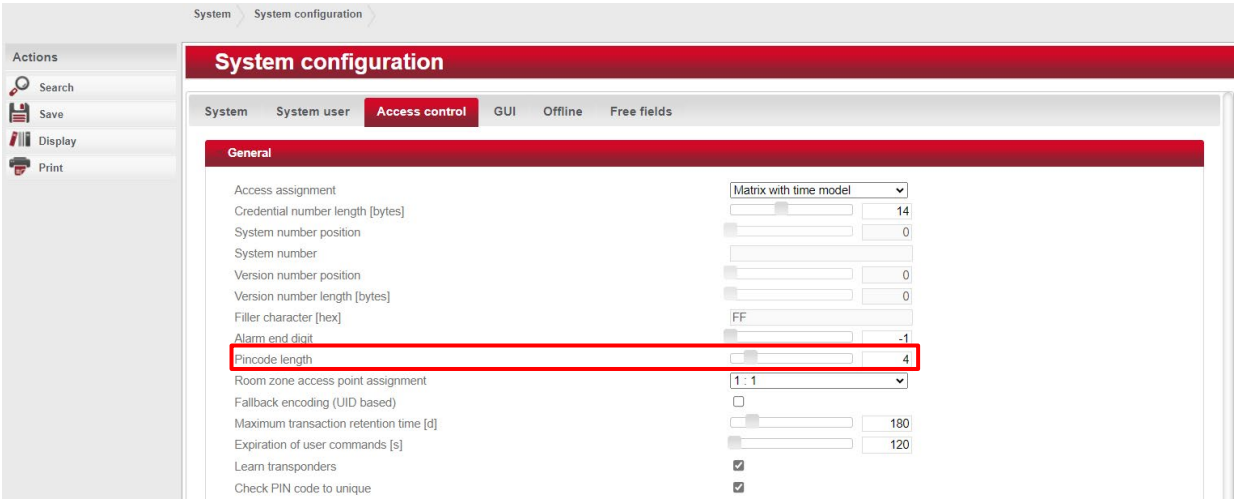
Automatic PIN code generation:
Have a PIN code generated automatically using the symbol.

A prerequisite for this is an existing e-mail address in the master data of the person concerned, and the setting up of the e-mail function in the Dialock system (**5.7.4.1** System).



The automatically generated PIN code is then forwarded to the specified e-mail address of the relevant person by Dialock.

The **PIN code length** defines the number of digits and can be set in the **Access Control** tab in the **System / System Configuration** menu.

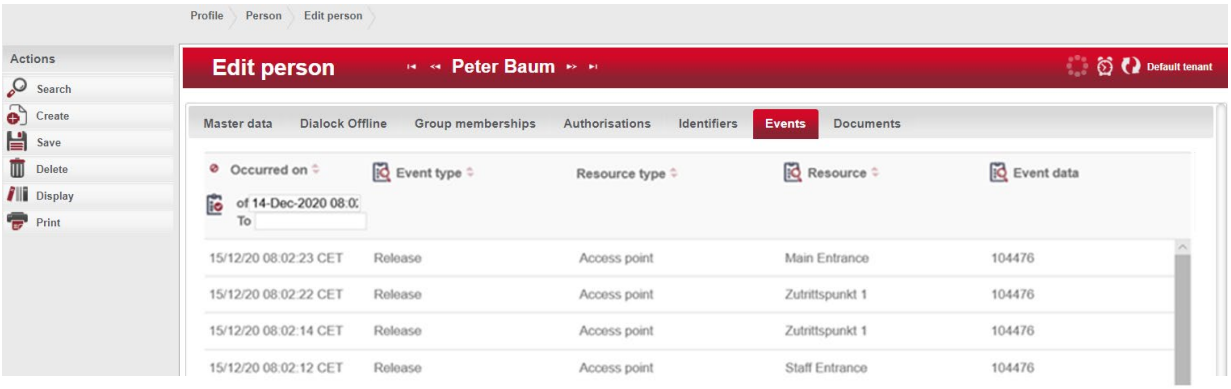


Note:

This setting also relates to length of the door code. (**5.5.6** *Keypads (PIN-Code reader).*

5.2.1.6. Events

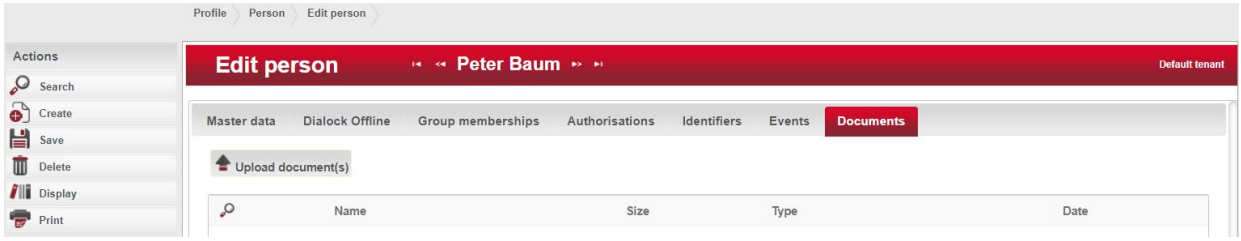
All events are listed that have been triggered by the person concerned within the set time period.



Events at offline terminals must be read out beforehand with the MDU 110, “Terminal>Logs” menu and imported into the software using menu item “Organisation>Area>Edit area” and action “Import logs”.

5.2.1.7. Documents

The documents that are associated with the selected person and are saved in the system are listed in this tab. The relevant document is opened and displayed by clicking on the **File name**. Documents are associated with the person using **Upload document(s)**.



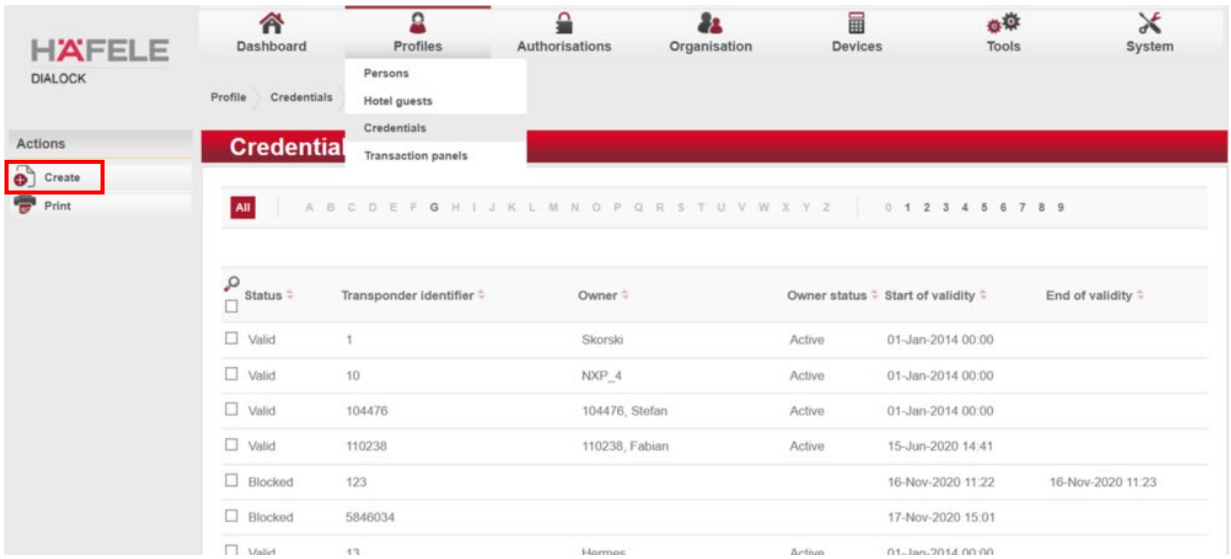
5.2.2. Hotel guests

Hotel guests are only displayed in the system for information and analysis only, but cannot be managed.

5.2.3. Credentials

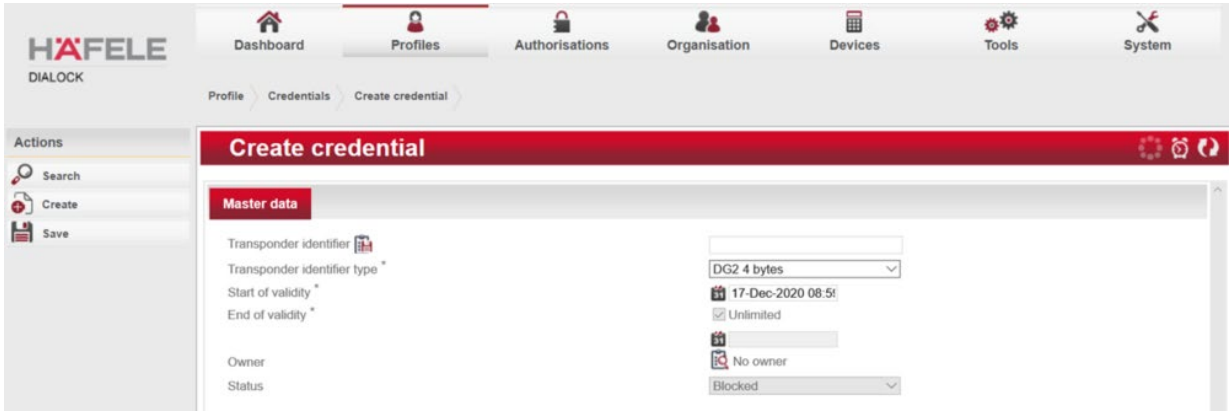
5.2.3.1. Credential list

By selecting **Profiles / Credentials**, the **Credential list** appears, containing all transponders that are in the system.



5.2.3.2. Create credential

With “**Create**” in the left-hand action menu, you can create a new transponder with the respective **master data**.



Under “**Transponder identifier**”, you can give the transponder an appropriate name or designation.

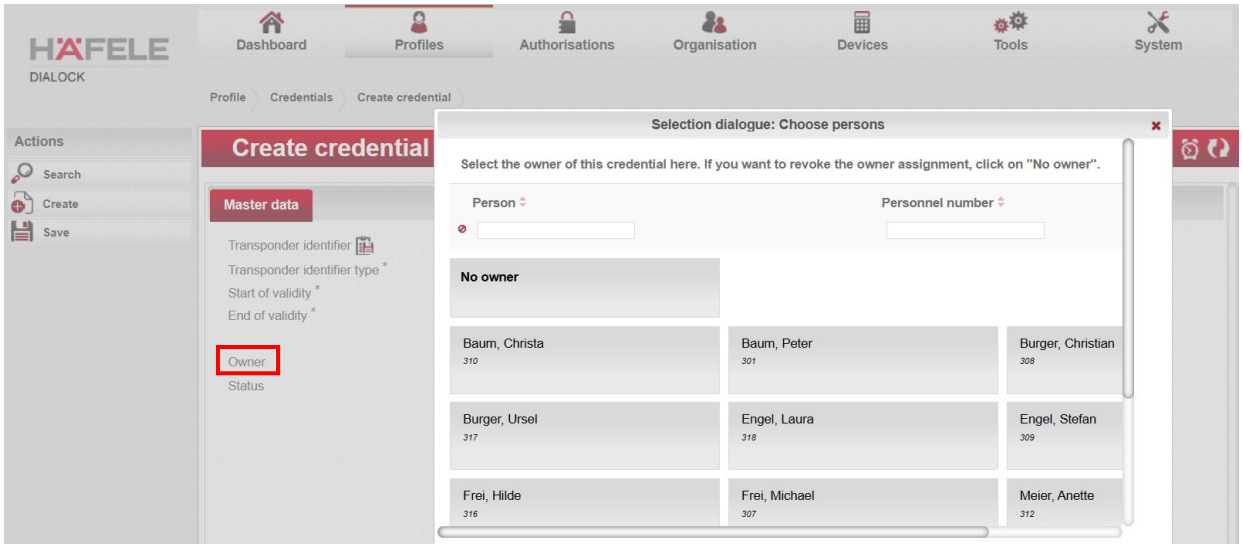
The “**Transponder identifier type**” is pre-set via the licence.

The **UID** is automatically entered when the transponder is programmed.

The **Start of validity** is usually the creation date of the transponder, but can be changed if required.

The **End of validity** is set to “unlimited” as standard, but can be changed if required.

Under “**Owner**” you can assign the transponder with the symbol to a specific person.

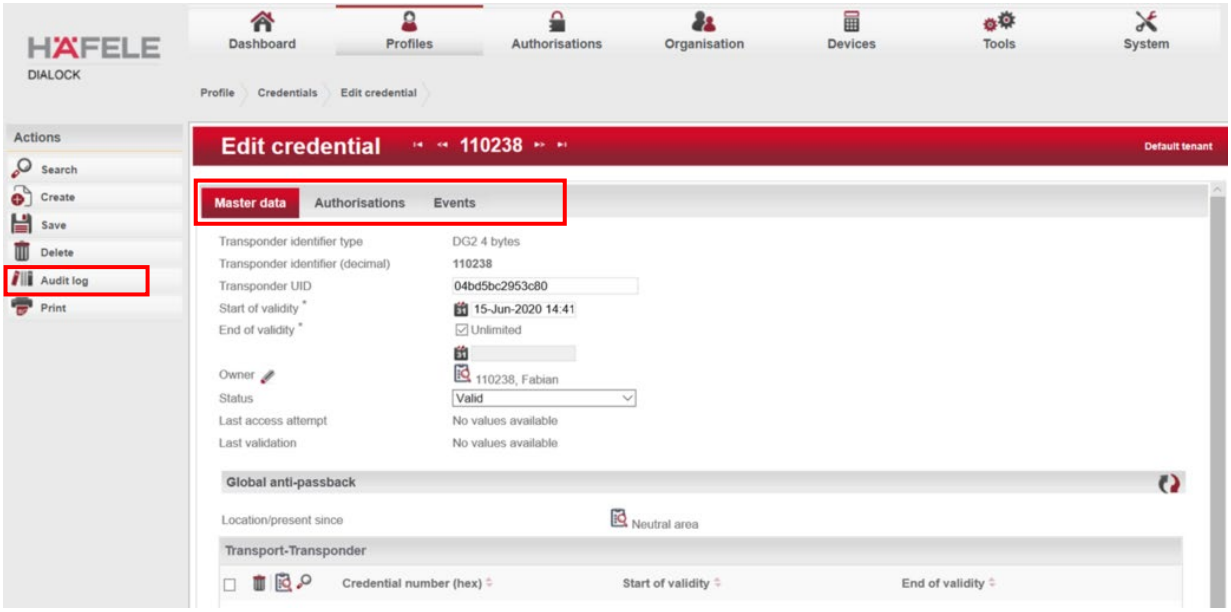


The **Status** displays the current usage status.

5.2.3.3. Edit credential

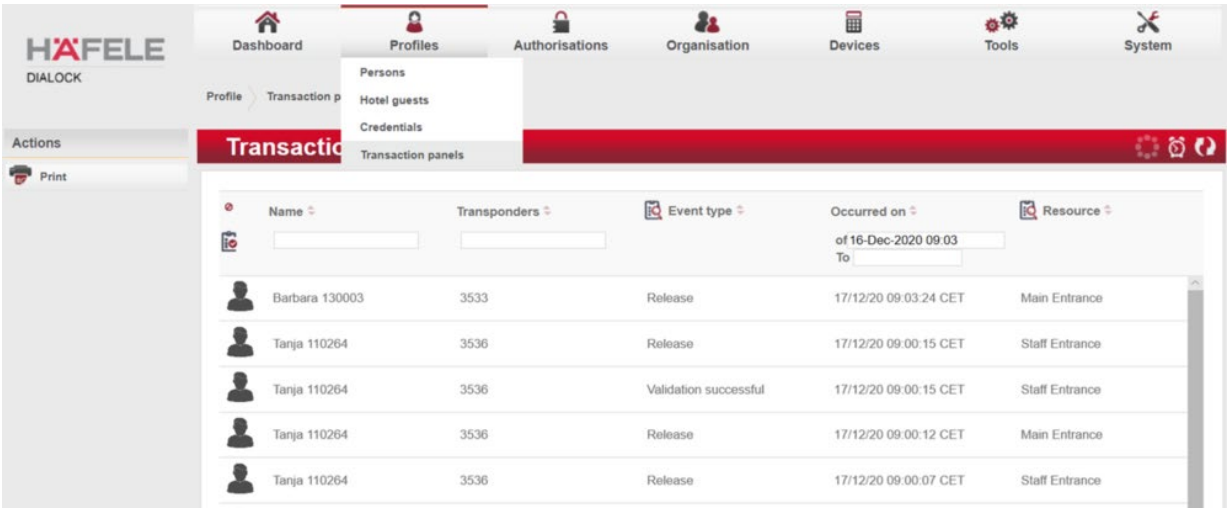
If you click on a transponder, the Edit window opens. Here, you can edit the **Master data**, issue **authorisations** or view the registered **events** of the transponder concerned.
The history can also be retrieved for each transponder (who had the transponder and when) in the left-hand action menu under “**Audit log**”.

732.29.430
HDE 20.12.2023



5.2.4. Transaction panel

Profile / Transaction panel lists all recorded events. The events are filtered according to name, transponder, event type, transaction time or resource.



Attention:
All changes, new entries etc. that are made and other input screens are taken over by confirming them using Save in the left-hand action bar.

Note:
Transponders are managed independently of the master data and can be assigned to individual persons.

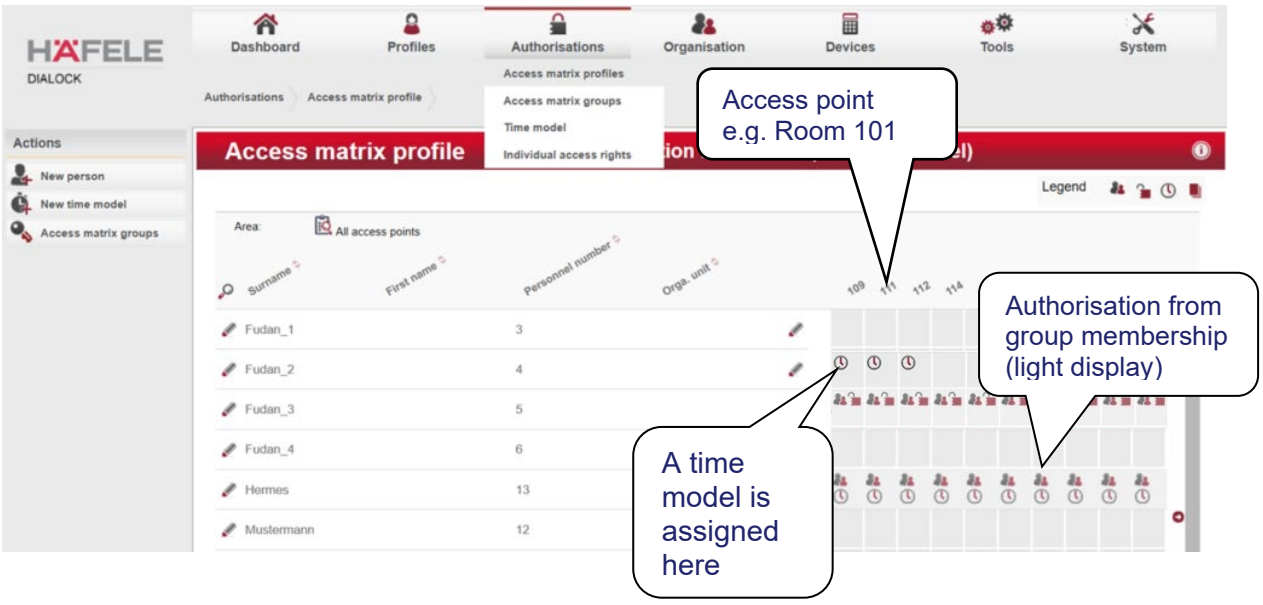
5.3. Authorisations

The access authorisations are issued to individual persons and groups in main menu item **Authorisations**.

5.3.1. Access matrix profiles

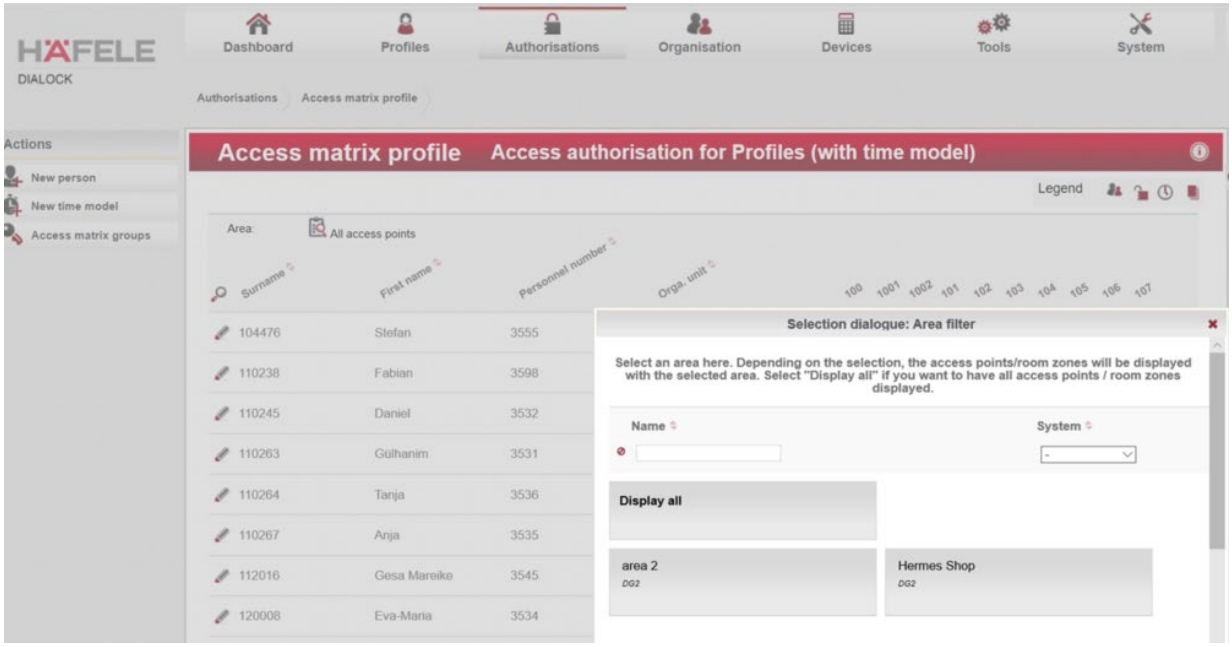
Via the **Authorisations/Access matrix profiles** and **Authorisations / Access matrix groups** menu, you are taken to the access matrix, which is both person-related and group-related. A person can be authorised individually as well as via groups or organisational units.

In the access matrix, you have the option to create, edit and delete the access authorisations of individual **Persons** with their **Personnel number** in a comprehensible way.



Furthermore, depending on the setting (**5.7.4.3** *Access control*), the matrix also gives you an extensive overview of all access authorisations.
In other words, you can see, **who** has **which** access authorisation, **where** and **when**.

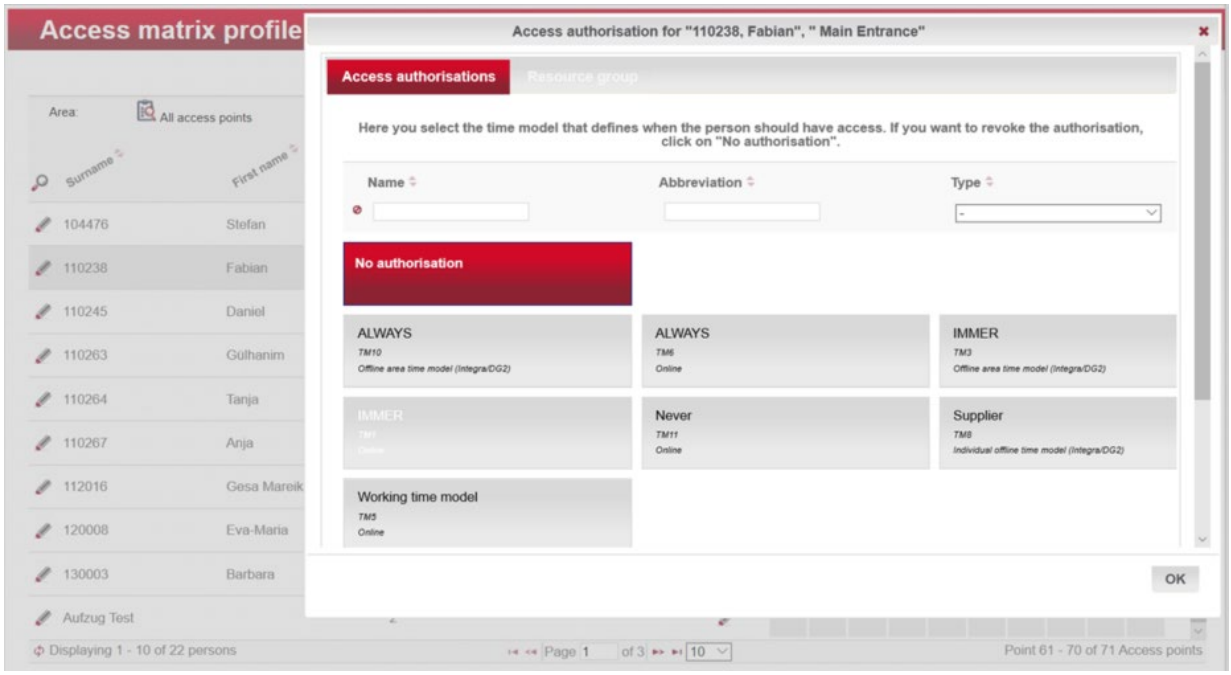
Select the desired **Areas** via the symbol. Now only the authorisations of the selected area are displayed in the matrix.



5.3.1.1. Allocation of authorisations in the access matrix for an online access point

In order to grant a person access authorisation for an online access point, assign a previously defined time model to it (**5.3.3** *Time model*)
In the matrix, click in the row of the desired person and in the column of the desired access point, in order to select the desired time model from the following selection screen.

In order to delete a person's access authorisation to an online access point, proceed as described above, but click on "**Not authorised**" on the selection screen.



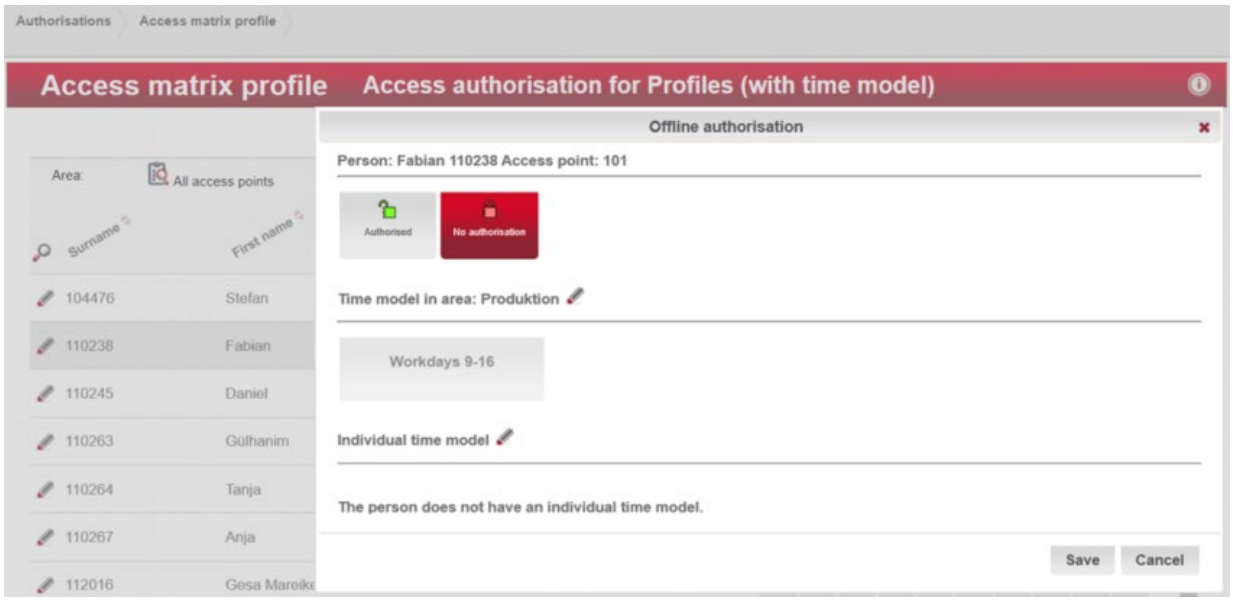
5.3.1.2. Batch processing when issuing authorisations in the access matrix for an online access point

In order to grant a person the rights for several access points, click on the symbol (edit) in the row of the person and select the desired access point in the menu that opens.

5.3.1.3. Allocation of authorisations in the access matrix for an offline access point

In order to grant a person offline access authorisation, click the row of the desired person and the column of the desired access point in the matrix.

To delete a person's offline access authorisation, proceed as described above.



5.3.1.4. The time models in the access matrix

After right-clicking on a field in the matrix, you can obtain a display of the authorisation overview for this access point.

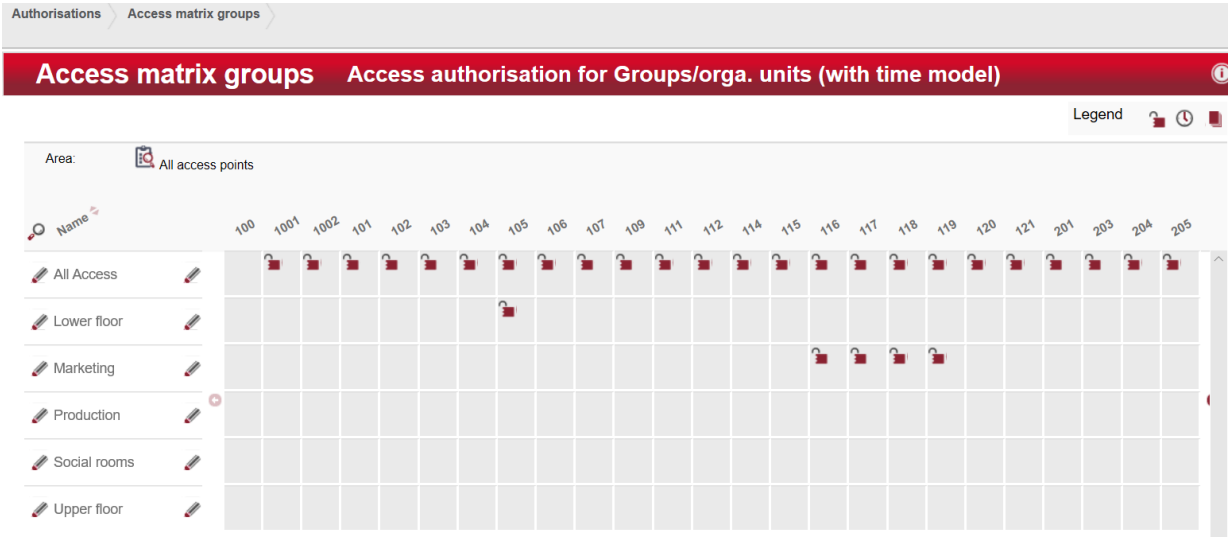
Details of the time model can be obtained by selecting "View time model".

The time model can be edited directly from the matrix by clicking on the Edit symbol.

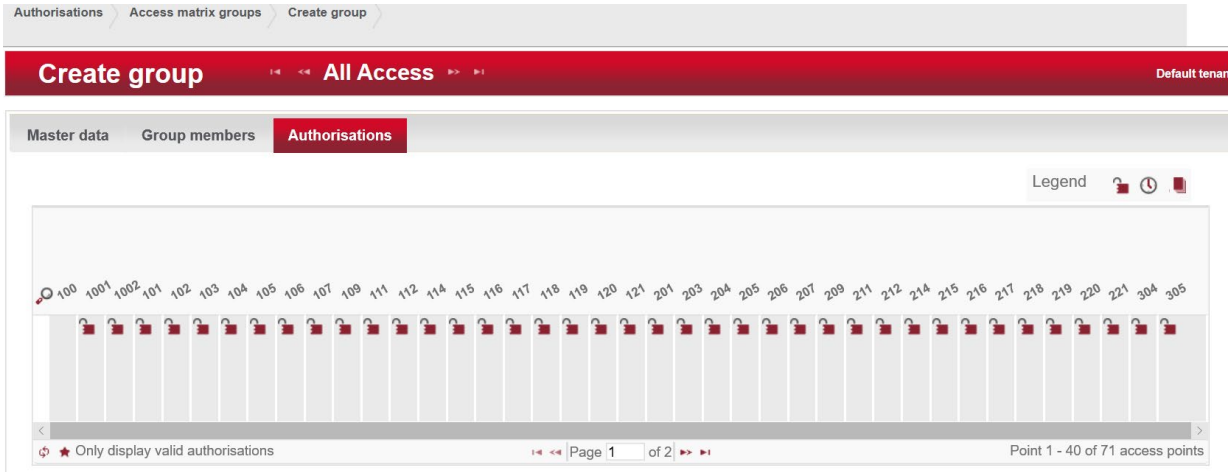
5.3.2. Access matrix groups

Additionally, or alternatively to the “Organisation>Groups>Organisational units” module, access authorisations can also be issued in the “Authorisations > Access matrix groups” module.

Editing in module “Authorisations > Access matrix group”



Editing in module “Organisation>Groups>Organisational units”



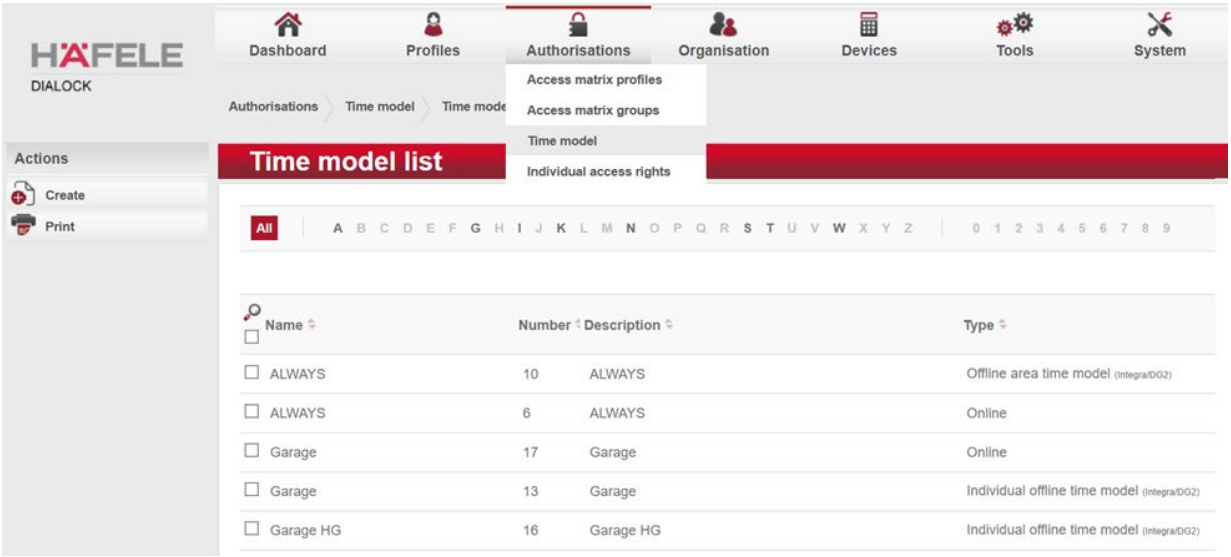
5.3.3. Time model

In the **Authorisations > Time model** menu, all online and offline time models are recorded.

Dialock creates two time models with the name “ALWAYS”, one for “offline” and one for “online” as standard.

“ALWAYS” means that the time model is valid on all days (incl. special days) around the clock. We recommend that these default values are not changed.

The offline time models are suitable for e-cylinders, door terminals etc. which do not have a fixed connection to the database. Online devices can process far more complex and more extensive time models. For example, the WTC 200 controller can process up to 2,048 different time models which can be changed at any time online.

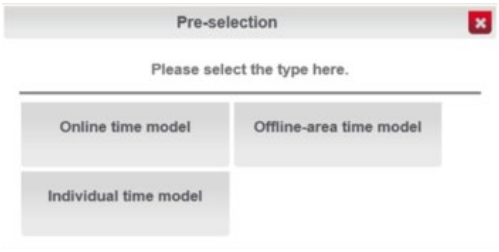


5.3.3.1. Create / edit online time models

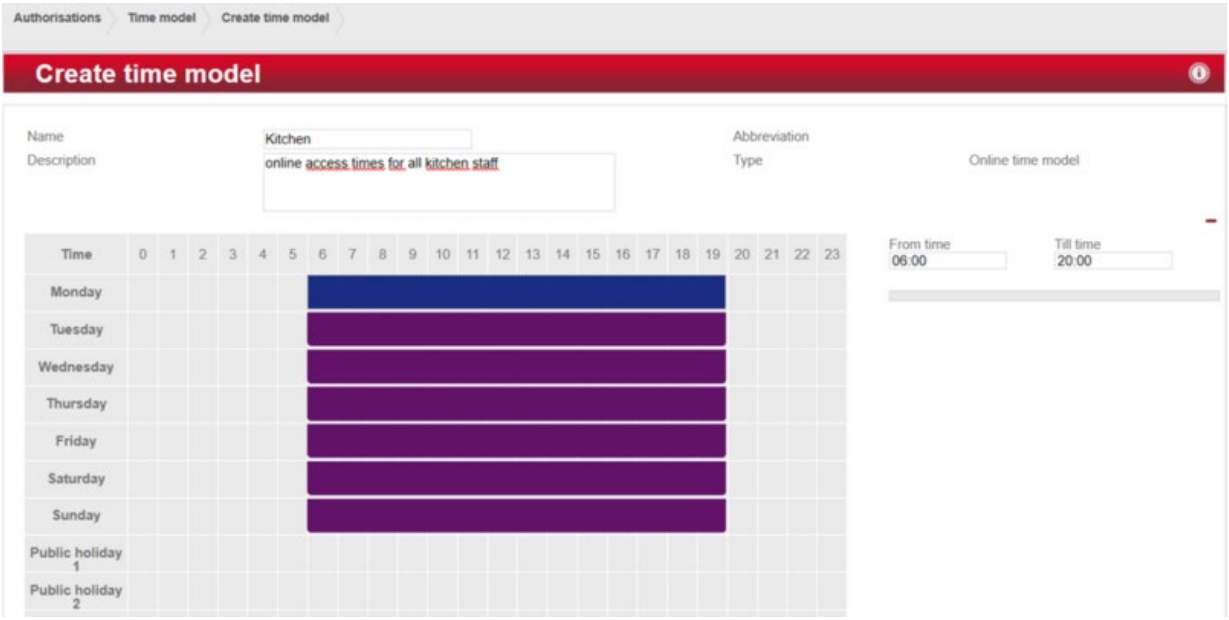
A new time model can be created using the “**Create**” button in the left-hand action bar. Make the choice between an online and offline time model here, such as in the example mentioned in the following – depending on the equipment of the doors at which the time model will be used later.

Notes:

1. Assignment to the relevant doors (access points) takes place later via the access matrix.
2. If you would like to use the same time model for an online and offline access point, it is necessary to create one online time model and one offline time model.



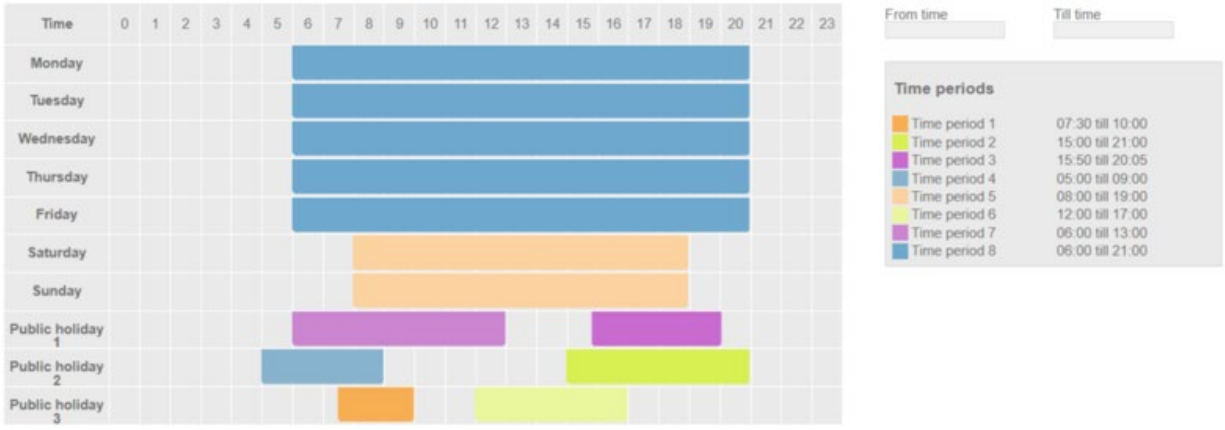
Specify a **Name** for the new time model and, if you wish, a **Description**. You can find the time model in other overviews using the name.



In order to set the time, double-click the line of the desired day and then the field of the desired start time (the exact time can still be set in the **From time** and **Till time** fields). The marked time is now highlighted. As soon as the cursor moves to the edge of the highlighted time, the appearance of the arrow changes. You can now drag the highlighted bar to the till time in 5 minute steps.

Copy function:
You can use the copy function for repeated time periods by moving the cursor to the lower edge of the bar and dragging the changed arrow downwards.

Alternatively, the time can also be set to the minute via a drop-down field (see above).



Online time models can contain eight (8) different time periods per model. Dialock automatically differentiates between the different time periods and uses a different colour for each one automatically.

A time period is **deleted** by highlighting it and then deleting it using the “Delete” key.

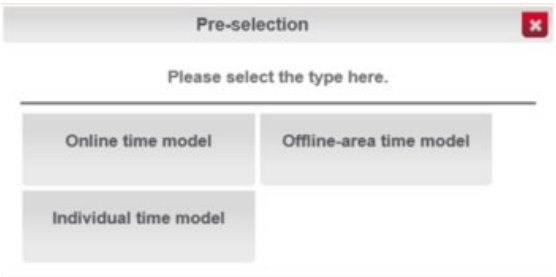
5.3.3.2. Offline time models

Offline access points can be opened at any time with a valid transponder. Offline time models are used to limit the access authorisation times at offline access points.

In order to create an offline time model, navigate via the **Authorisations / Time model** menu to the overview of the existing time models (please also note chapter **5.3.3.1** *Create / Edit online time models*).

To create a new offline area time model, click “**Create**” on the left-hand sidebar.

The following pre-selection appears:



Offline area time model:
An offline terminal can save up to 16 offline area time models each with max. 8 time periods which are available in an access control system area at all offline terminals. Changes to the offline area time models can be transferred with the MDU (Mobile Data Unit) to the offline terminals.

If a person is authorised at an offline access point, a time restriction can be defined by assigning offline area time models in the access matrix. In order to save memory on the transponders, only the assignment of the user to the time models is saved on the transponder. This assignment can be updated at any writing (hold the transponder at an authorisation writer).

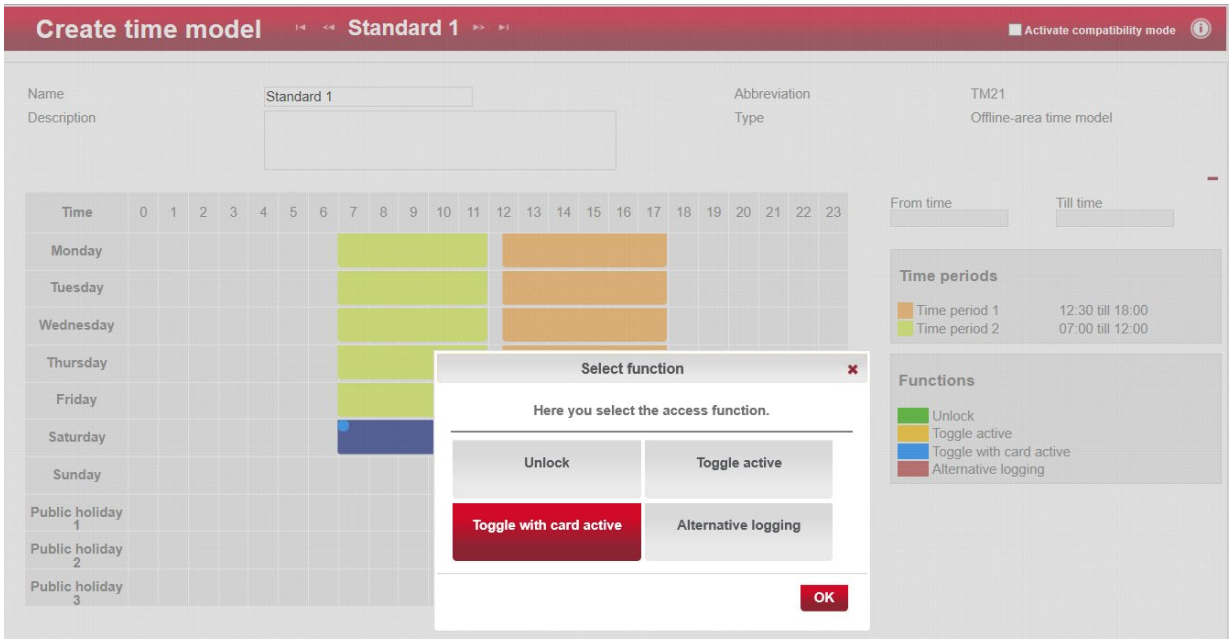
Individual offline time model:
The individual offline time models are saved on the transponder. The functionalities of the individual time models are minimised for memory reasons. Only one time period is recorded with individual offline time models.

Note:
The individual offline time model can be changed in the software and is then readjusted the next time writing takes place (hold the transponder at an authorisation writer).

5.3.3.3. Create / edit offline area time model

After selecting the offline area time model, you arrive at the input screen shown below. Assign a **Name** for the time model and a **Description**, if necessary. Define the desired time period by double-clicking and dragging the areas as described in chapter (**5.3.3.1** *Create / edit online time models)*.

Add one or more of these listed **Functions** by right-clicking on the desired time period.



Unlock:
Automatically opens at the start time (from time) and automatically locks at the end time (till time) of the time period.

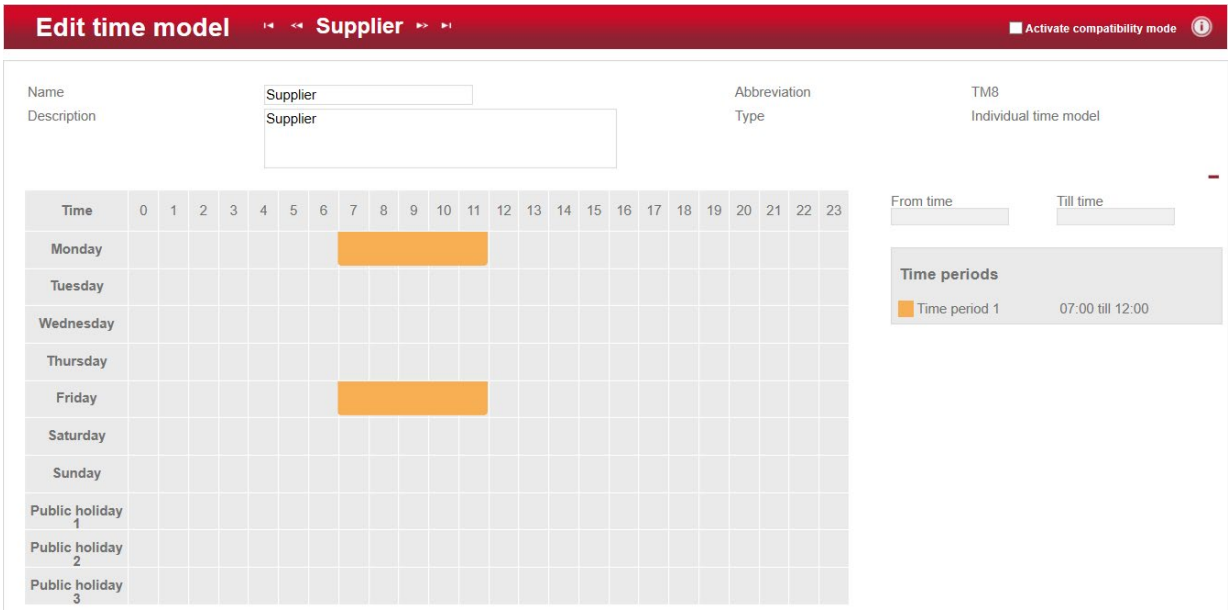
Toggle active:
When presenting a valid identification medium (transponder), the state of the access point changes from “Locked” to “Unlocked” or vice-versa and remains in this state.

Toggle with card active:
The combination of the “Toggle active” and “Unlock” functions correspond to the functionality of “Toggle active”. An open door/barrier is also automatically locked at the end time of the time period, in order to make sure that, for example, an office door is locked at the end of the working day.

Alternative logging:
Activate this function if no logging must take place at a certain door/barrier, e.g. as determined by the works council. The underlying alternative logging is individually defined by a trained technician.

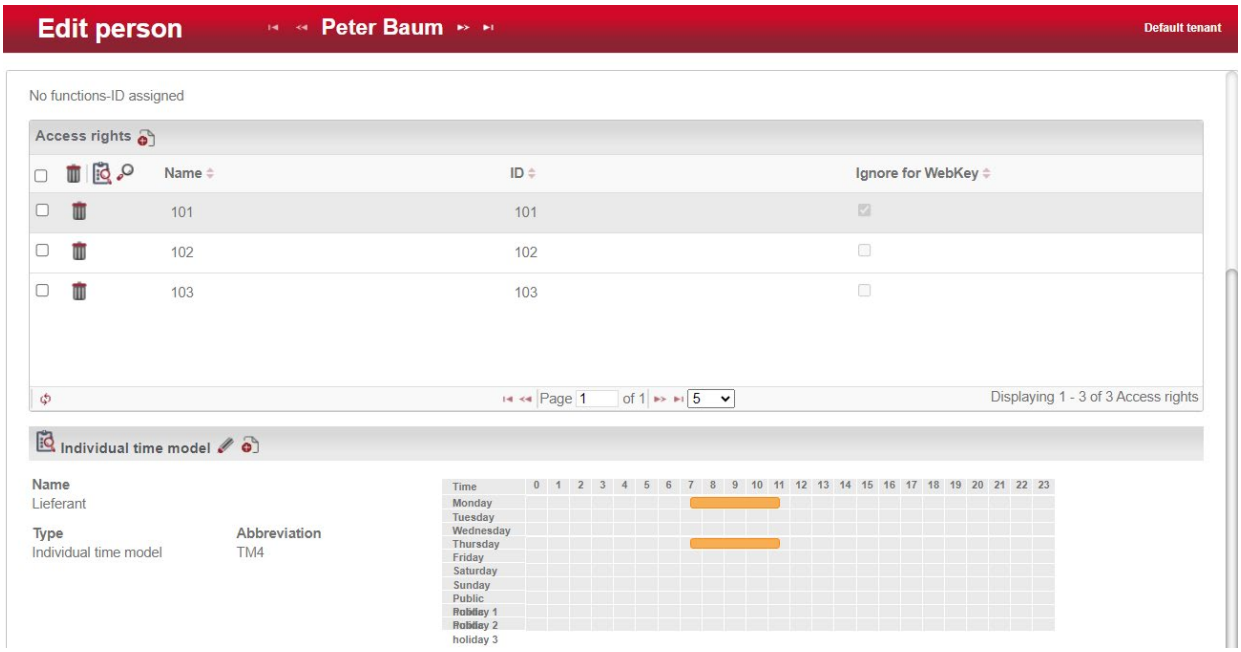
5.3.3.4. Create / edit individual offline time models

Give the individual time model a corresponding **Name** and write a **Description**, if necessary. Define the desired time period by double-clicking and dragging the areas as described in chapter (**5.3.3.1** *Create / edit online time models)*.



5.3.3.5. Assign individual offline time models to a person

The individual offline time model is assigned to a person in the "**Dialock Offline**" tab in **Profile/Person** menu by clicking on the symbol and then saving.



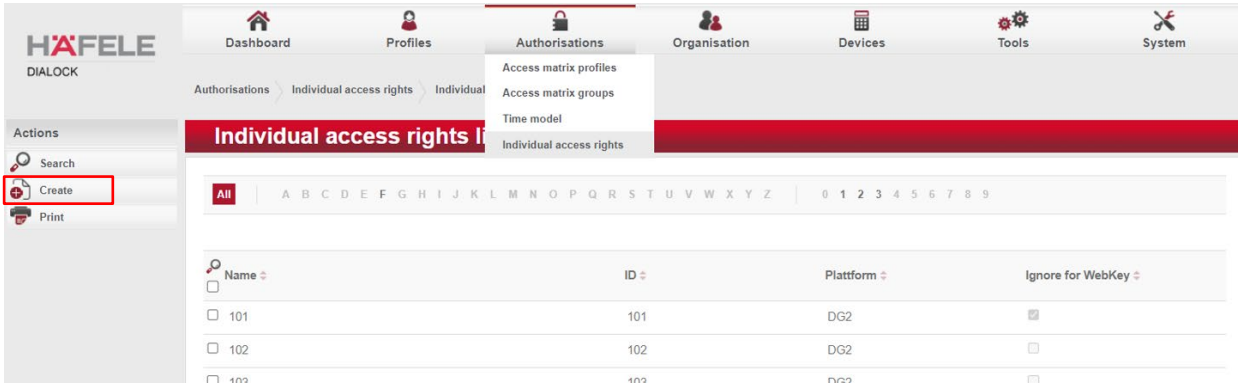
5.3.4. Individual access rights

An individual access right is a locking authorisation at an access point which is assigned to no room zone.

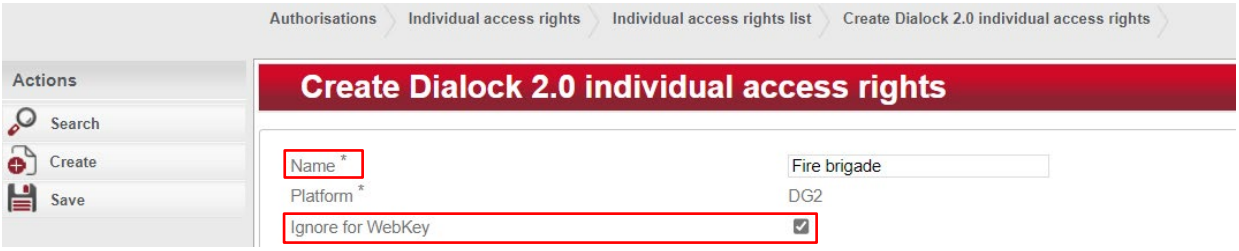
Note:
Dialock can administer a total of 65.535 individual access rights. Max. 5 individual access rights can be saved on one transponder. Up to 400 individual access rights can be saved in an offline terminal.

5.3.4.1. Create / edit individual access rights

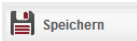
In order to **Create** individual access rights, navigate via the **Authorisations/ Individual access rights** menu to the individual access rights overview.



Click on "**Create**" in the left-hand side menu and assign a name for the **Individual access right.**

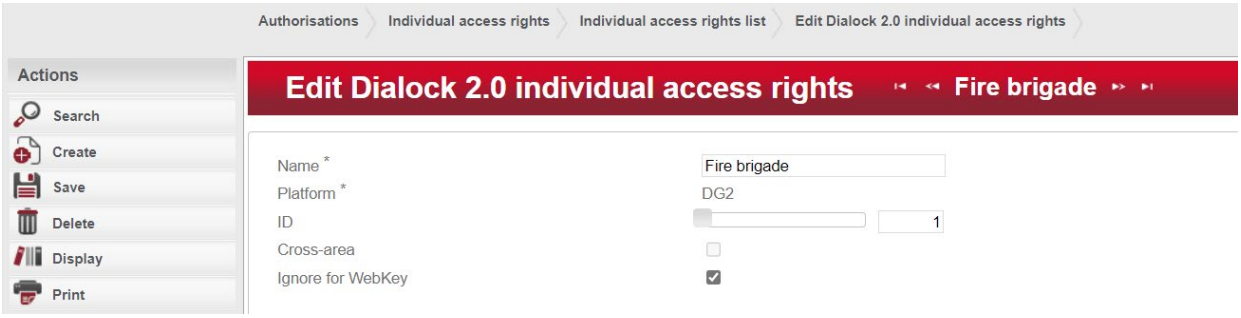


In order to use a standardized user key for emergencies (fire brigade, emergency or other helpers in emergencies) with Dialock 2.0, an appropriate individual locking authorisation must be created and stored at all access points. In order to ensure that this special individual locking authorisation does not affect queries from the PWA Checkin and REST-API areas, the "**Ignore with WebKey**" option must be activated.

Then save your entry with 

.

The individual locking authorisation can subsequently be edited by selecting it in the individual locking authorisation overview list.



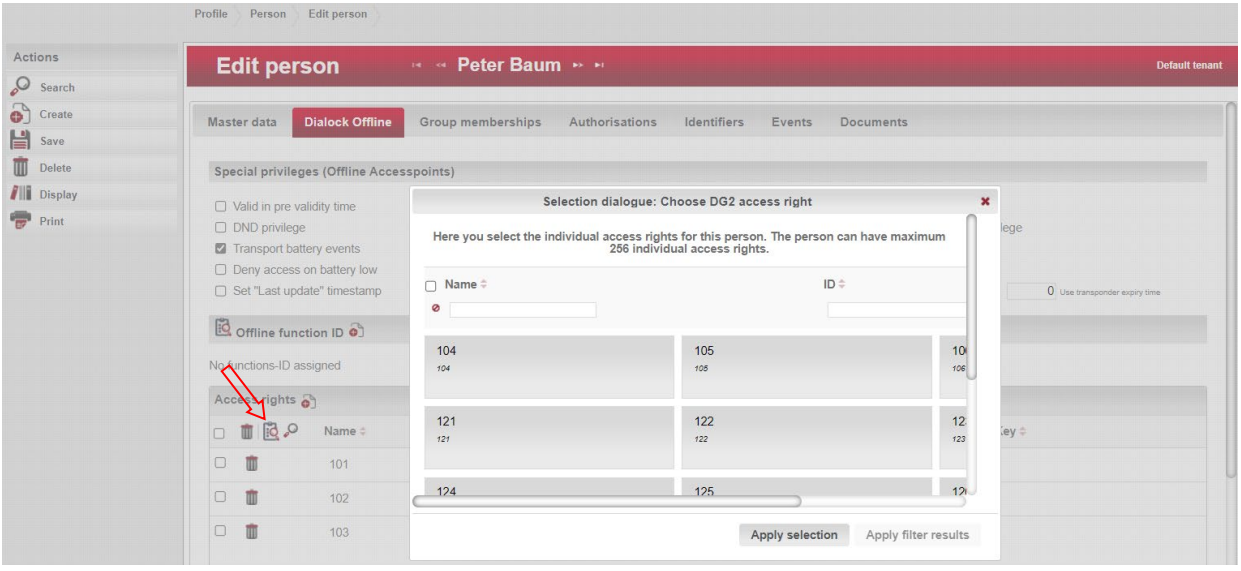
The ID can be adjusted if necessary (e.g. room number in hotel).

Note:
To become effective, the individual access rights must be assigned to the offline terminals at which they are to be valid (**5.5.1.2.1** *Offline terminal / Assign individual access rights*).

The individual access rights must also be assigned to the persons for which they are to be valid (see following).

5.3.4.2. Assign individual access rights to a person

Individual access rights are assigned to a person in the "**Individual access rights**" tab of the **Profiles / Person / Edit person** menu by clicking on the symbol .

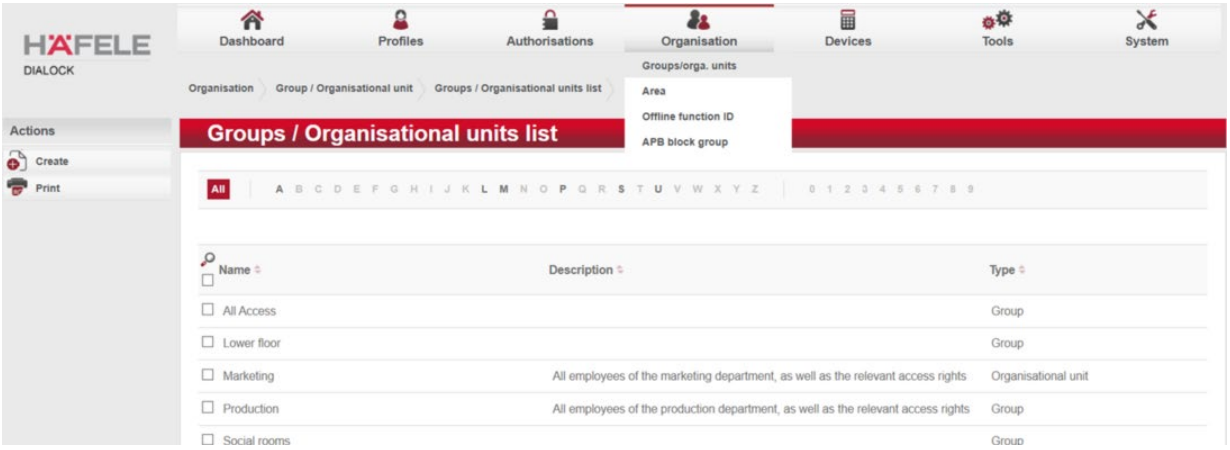


The settings are accepted with "Save". Save

5.4. Organisation

The **Groups / organisational units** are edited in main menu item "**Organisation**".
In order to edit a group / organisational unit, it must first be selected.

732.29.430
HDE 20.12.2023



5.4.1. Groups / organisational units

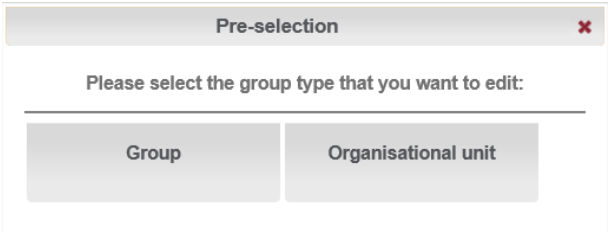
Groups / organisational units summarise selected persons. This means that access authorisations can be simply allocated later by assigning to authorised groups / organisational units.

Groups are project groups or work groups, for example. With **organisational units**, you are usually creating departments or other hierarchical units.
(**1.2.1.2** *Allocation of access authorisations according to groups and / or organisational units).*

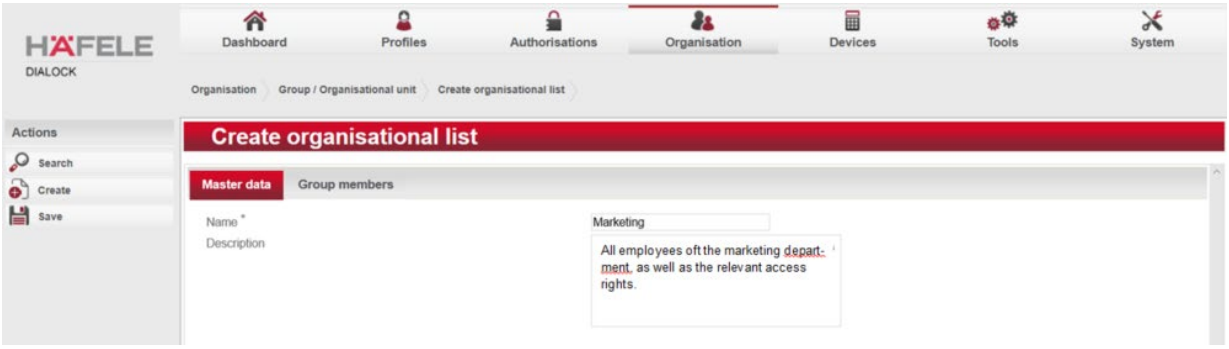
5.4.1.1. Create group / organisational units

Create your groups and organisational units by clicking on “**Create**” in the left-hand action menu under **Organisation/Groups/Organisational units**.

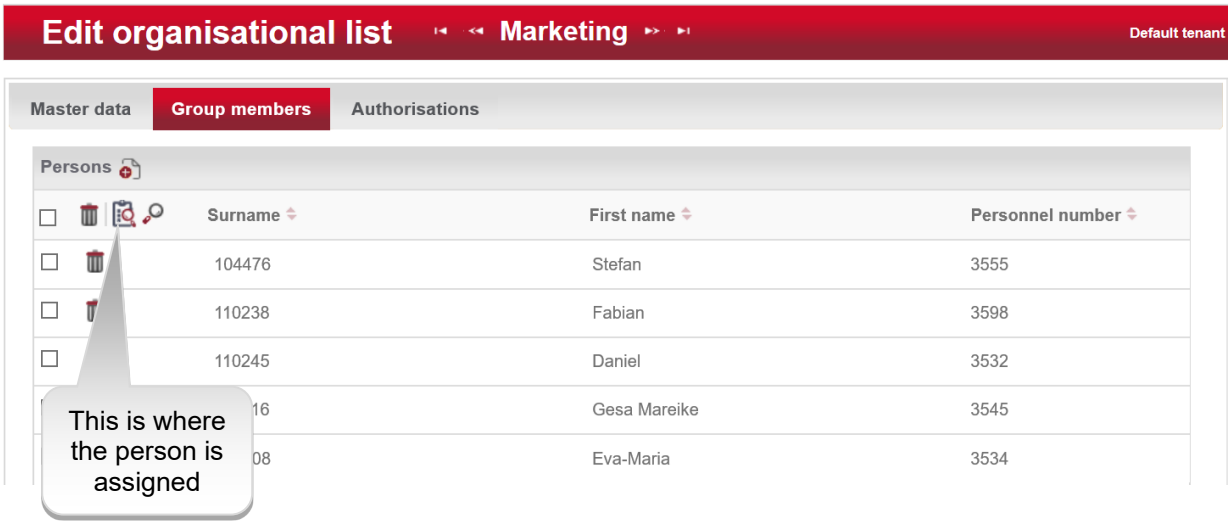
You first choose between “group” and “organisational unit”.



Give the group or organisational unit a name under **Name** and write a **Description** if necessary.

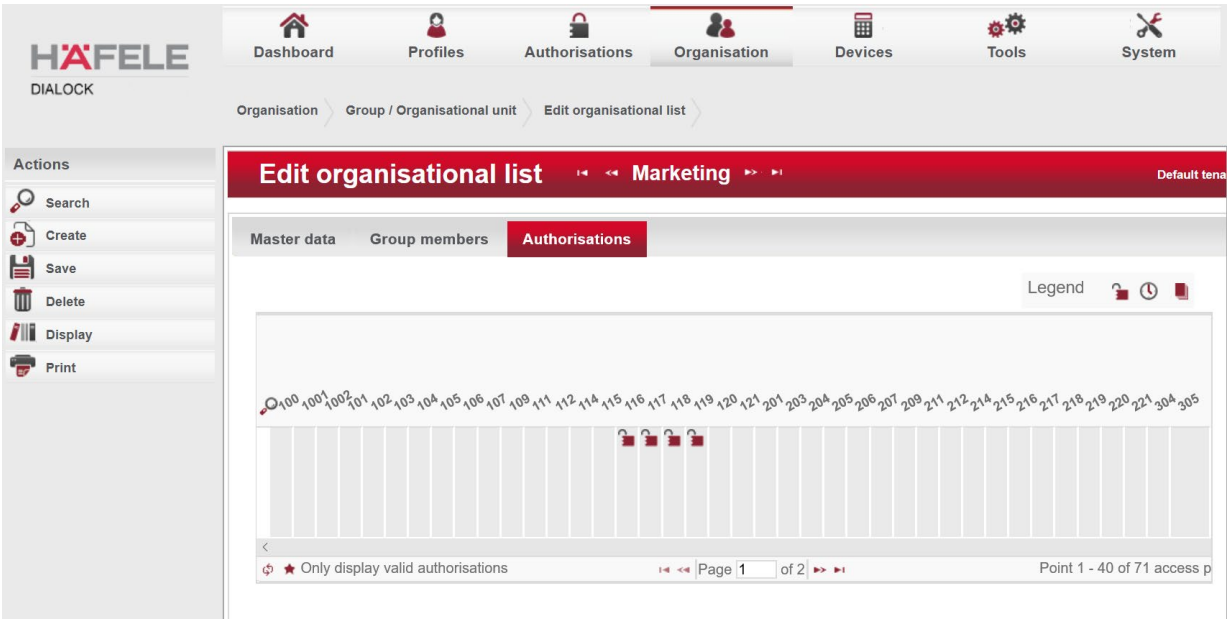


If a personnel master record has already been set up, people can now be assigned to the groups or the organisational unit under the “**Group members**” tab.



5.4.1.2. Assign authorisations for groups / organisational units

In the “**Authorisations**” tab, you will find a selection of possible barriers / doors with the associated access points.
Assign the **Authorisations** for your group and organisational unit here.
Click on the symbol in order to assign access rights to this group or organisational unit.

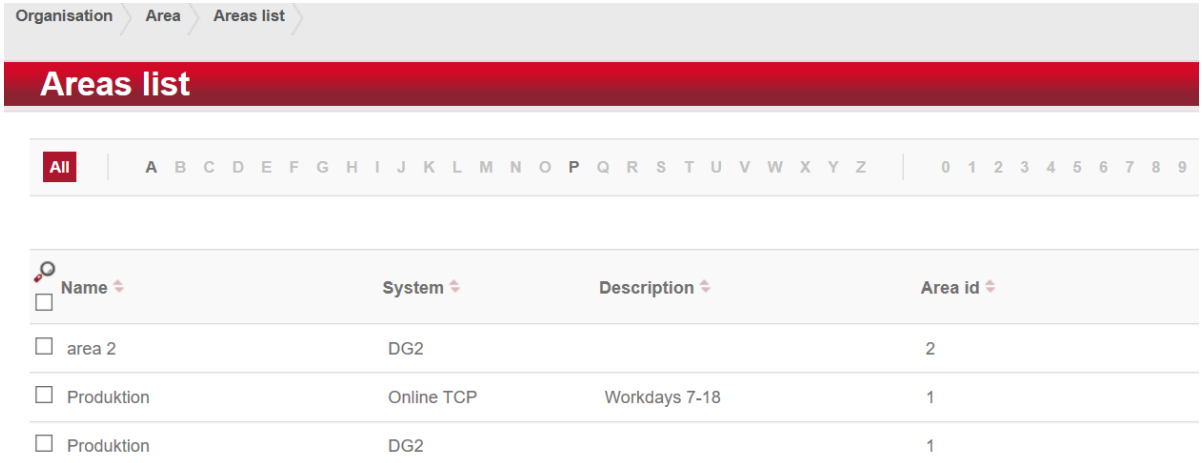


5.4.2. Area

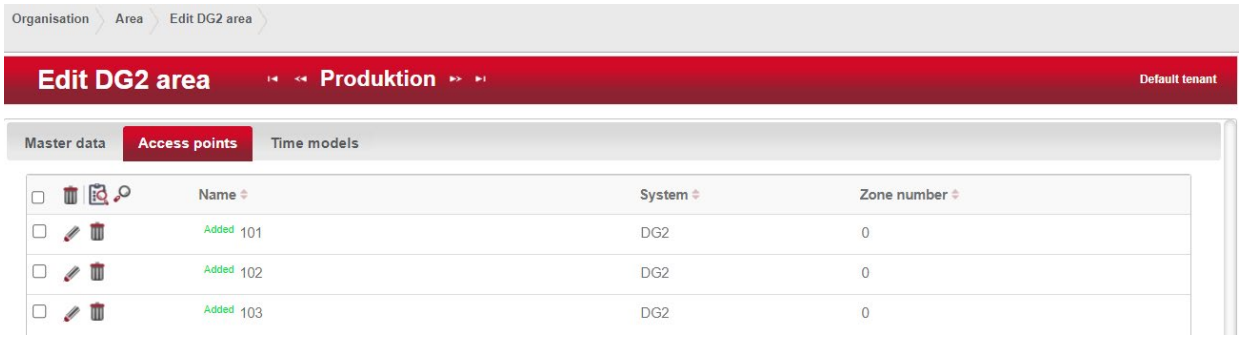
In order to have a better overview of the access control system and efficient organisation of access authorisations, it is recommended to combine related access points into logical zones, and combine these zones into areas. These can be individual departments, buildings, building complexes or locations, for example.

5.4.2.1. Create / edit online areas

To do this, create an online area in the **Organisation / Area** menu (preselect Dialock) and give the area a **Name** and a **Description** if necessary.



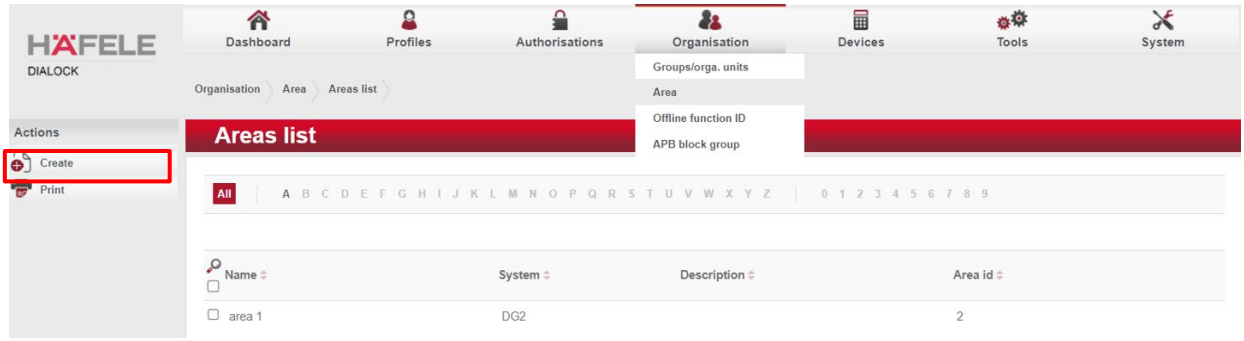
Now assign the associated access points to the area under the “Access points" tab with .



5.4.2.2. Create / edit offline areas

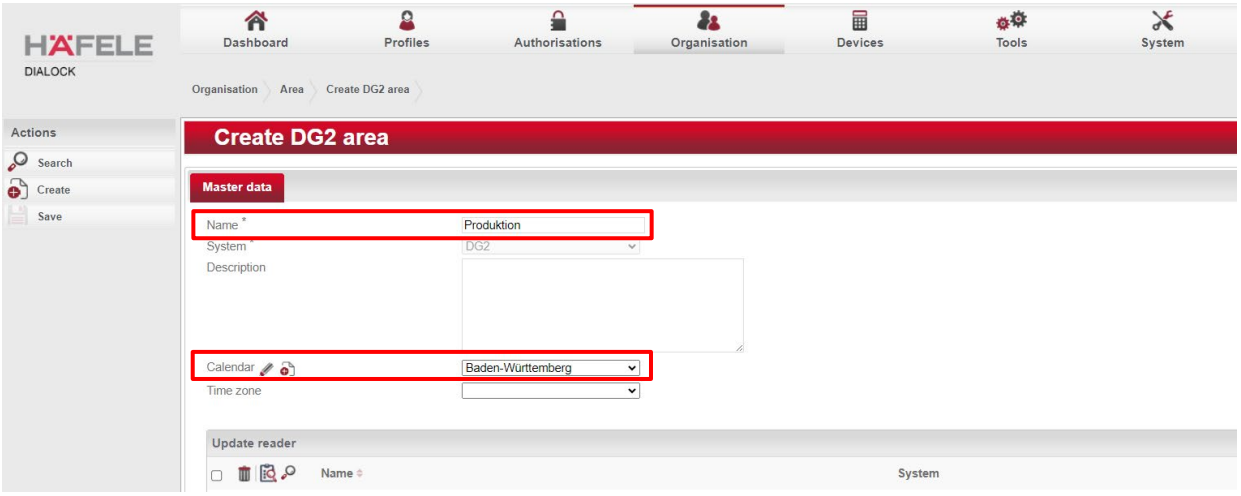
A maximum of 255 offline areas can be created per system.

Create an offline area in the **Organisation > Area** menu for this.



A pre-selection window can be opened using the "**Create**" action in the left-hand sidebar. Select the **DG2 (Häfele Offline)** option.

Give the area a **Name** as well as a **Description**, if necessary, and select the associated **Calendar** which is to be valid in this area.



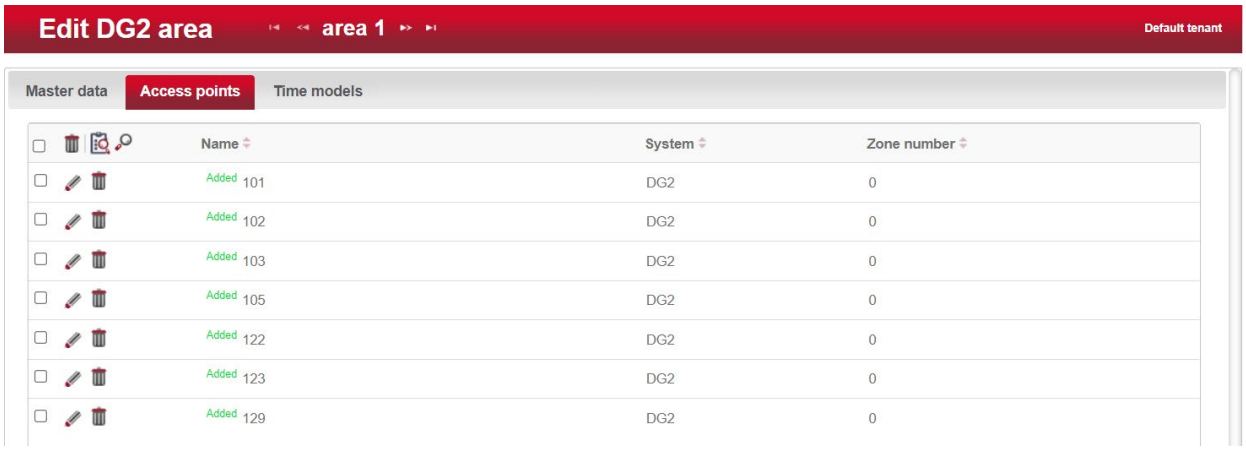
Save your selection. 

Authorisation writers are online terminals that write the currently valid offline access authorisations on the transponder or extend already entered authorisations for an authorisation period.
If you have already created an online reader, after saving it you can assign it to the current offline area as an authorisation writer by clicking on the symbol.

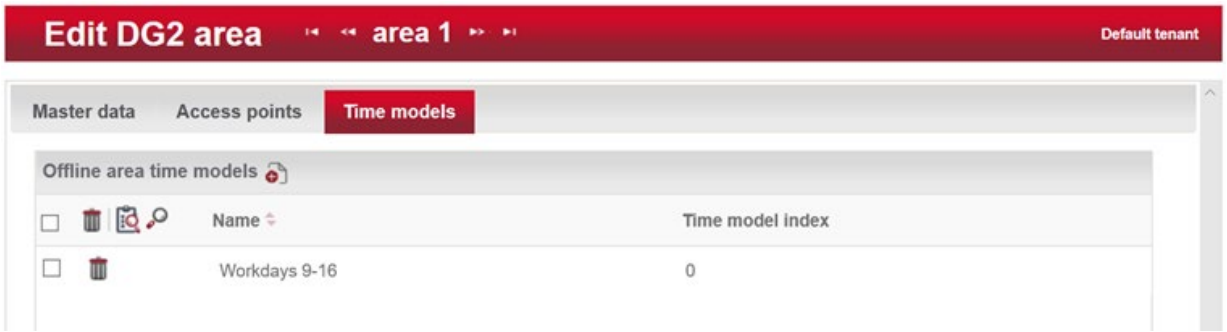
The authorisation writer is often referred to as a validation terminal.

732.29.430
HDE 20.12.2023

Under **Access points**, assign one or more corresponding online and/or offline access points to the offline area by clicking on the symbol.

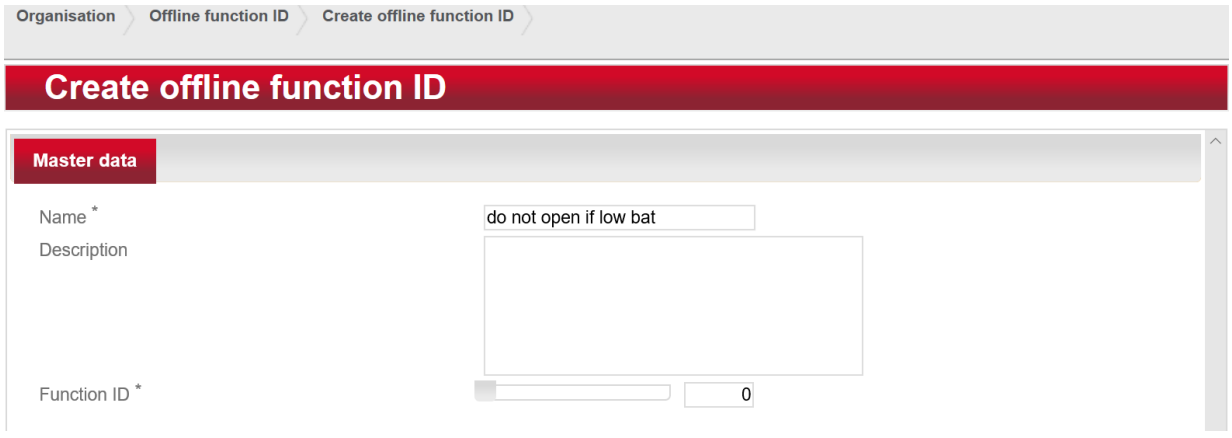


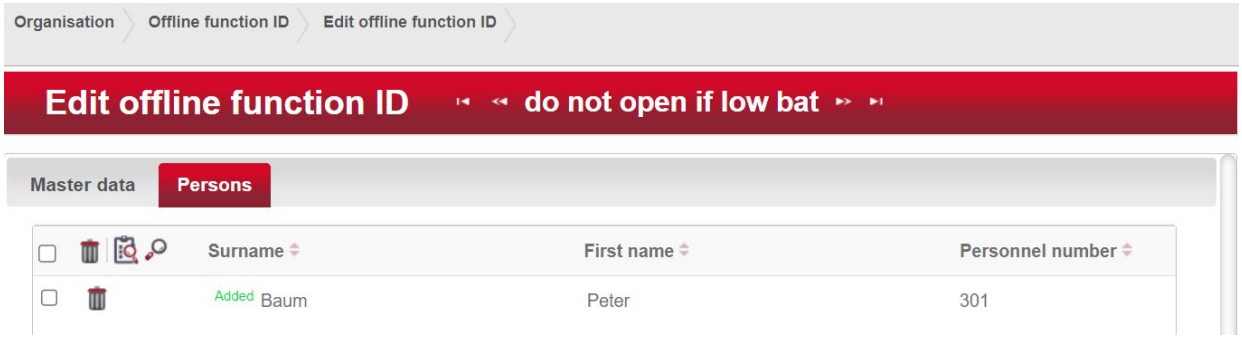
You can also assign one or more appropriate offline time models to the offline area under **Time model** by clicking on the symbol.



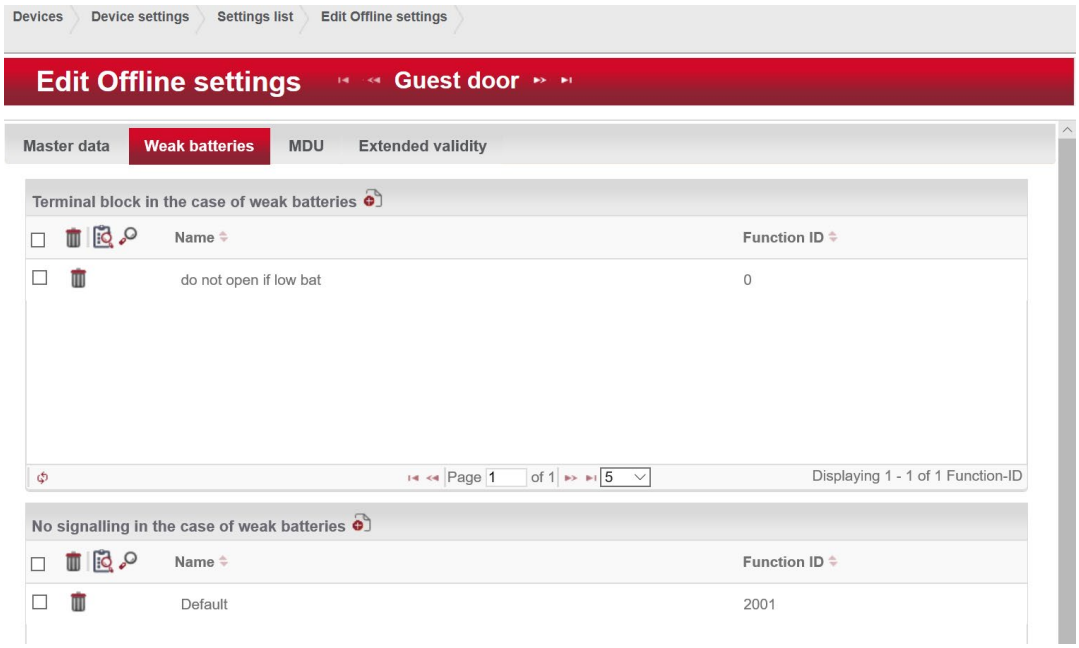
5.4.3. Offline function ID

This identifier is a number between 0 and 2,000. Then certain functions at offline terminals are assigned to the function identifier such as the suppression of certain signalling or “Do not open if low bat” as the highest signalling to the hotel employees. Then the ID can be assigned to a person. A person can be assigned one Offline function ID. However, a specific Function ID can be assigned to any number of people.





The setting of the function takes place in the **Devices / Device settings** menu and by selecting the relevant terminal type. When this terminal is configured, the function is also transferred.



5.4.4. APB block group

The APB blocking group is used for the Anti-Passback Block (APB) option. The latter is only visible if the option has been activated.

The Anti-Passback Block, abbreviated as APB, is used to prevent the misuse of access by passing on a transponder to a third party.

The classic application for an APB is an event (e.g. concert, theatre, sporting event etc.). The visitors purchase tickets in advance in the form of transponders which are valid for the duration of the event. After being permitted access to the event, visitors may now put their transponder in a suitable location in an unprotected area, giving access to another person who has not purchased a ticket (transponder) of their own.

To prevent this misuse, the option APB block group option can be created in Dialock 2.0, which groups access points into a unit. If a person with a transponder enters an access point of the APB block group, this information is shared with all access points in the group. The responsible terminal then starts a timer which blocks access with this transponder for an adjustable period of time (in this example, the entire duration of the event).

In order to defuse the working principle somewhat, the *Change of direction* option can be activated. This operates in combination with an exit reader. If this exit reader is used, all access points involved are notified and the timer deleted again. This allows someone to go to a toilet which is outside the secured area, for example, and then enter the event again.

Notes:

APB control elements:
If all associated control elements are triggered, i.e. the door contact, the latch contact and the passage contact, the anti-passback block is active and the access points of the APB block group will refuse the attempt to re-enter.

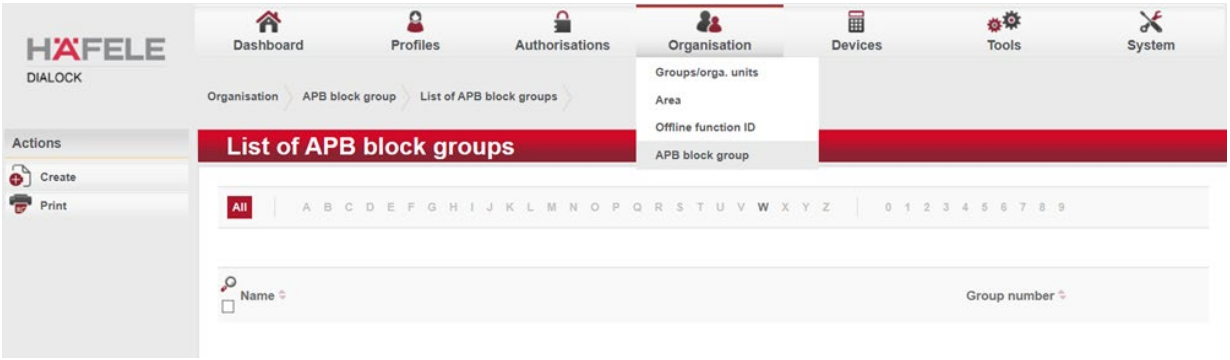
APB without opening:
If a person is registered at an APB access point and an available control element is not triggered (e.g. if the associated door contact does not open), the APB block which took place previously is cancelled after the release time. Once the release time has run out, access is possible again because there is no anti-passback block.

APB in the event of attempted misuse:
If someone registers at one of the APB access points while the anti-passback block is active (attempted misuse), the door is not opened and a so-called APB transaction takes place.

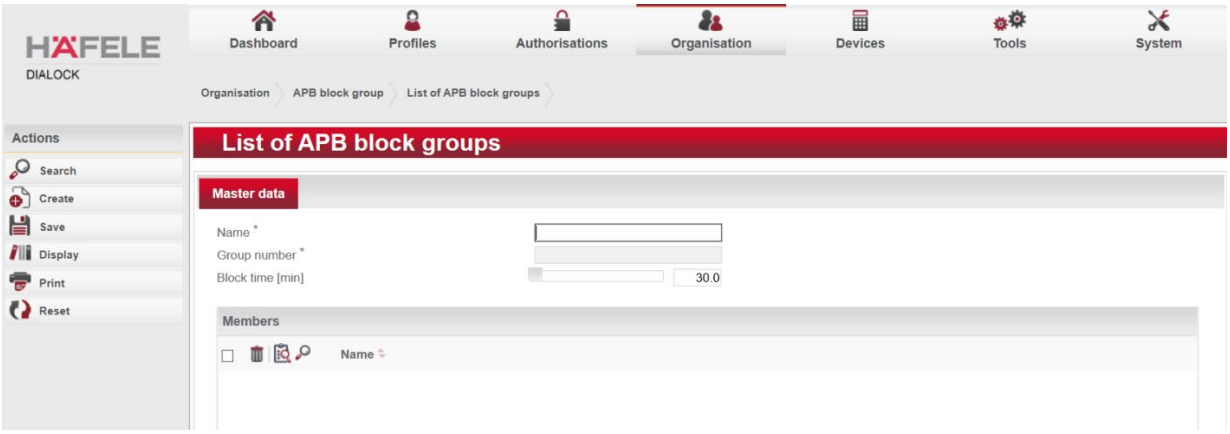
Manual reset of anti-passback block:
A reset is person-related, i.e. if a person has multiple transponders, resetting deactivates all active anti-passback blocks for that person.

5.4.4.1. Create APB block group

The list of APB block groups can be accessed in the **Organisation / APB block group** menu.

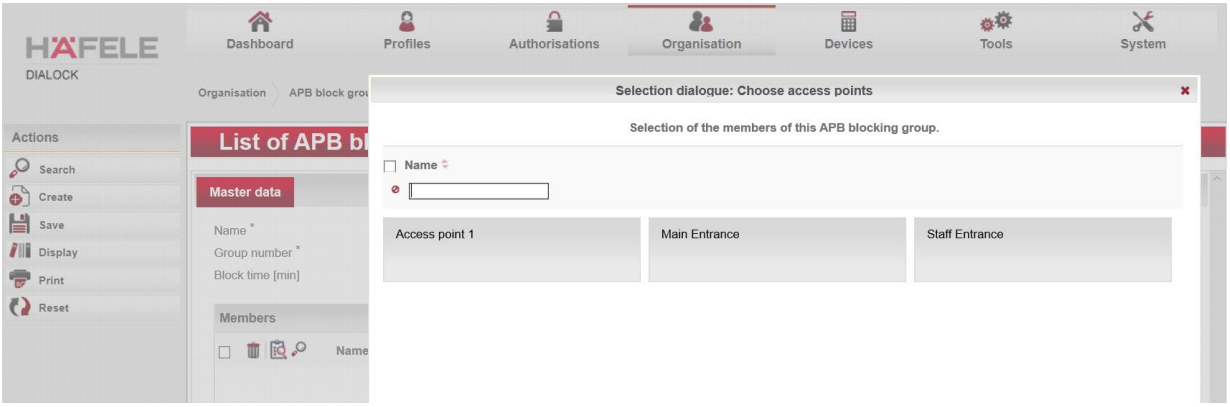


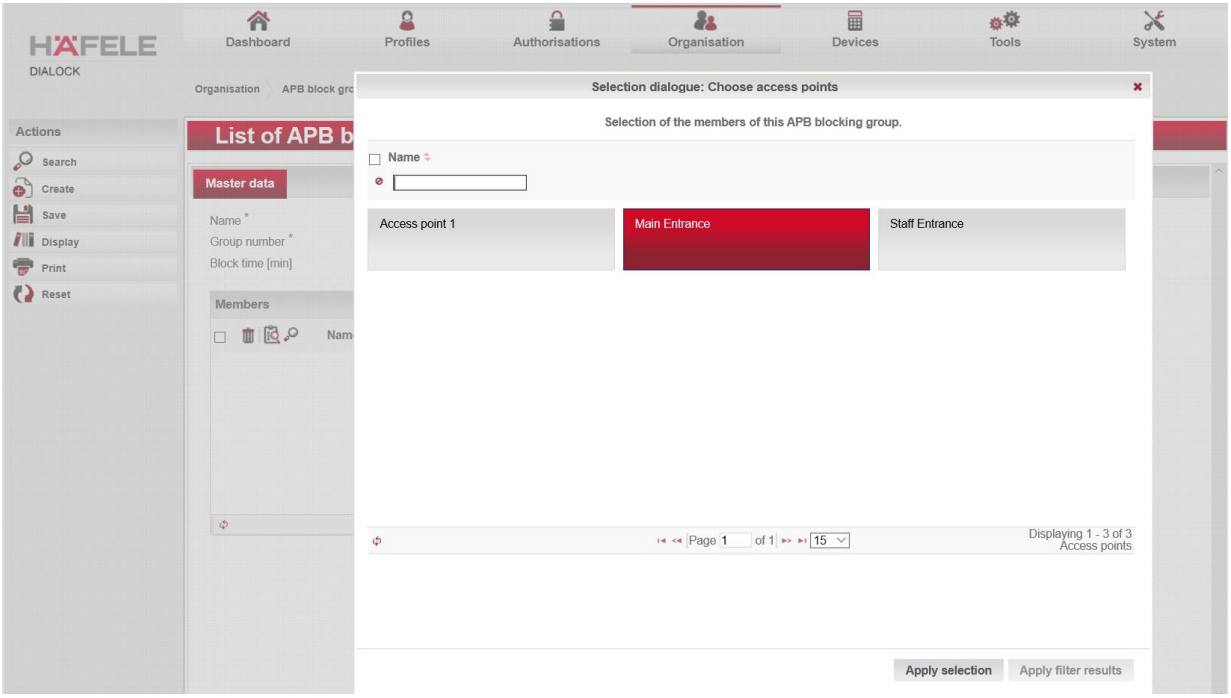
The master data of the APB block group is accessed using “**Create**” in the left-hand action menu.



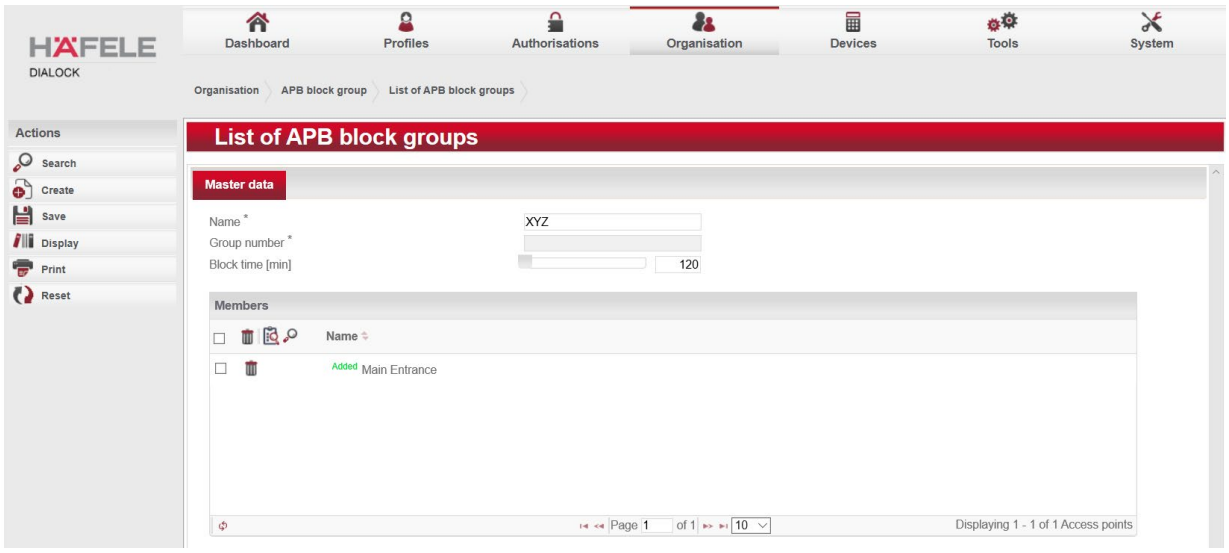
Provide a **Name** for the new group. The group number is automatically allocated by the system, and is unique within the system.

Specify a time period for the **Block time** in minutes. Repeated attempts to access the access points are not allowed during this time. Under “**Members**”, select the access points concerned with  and assign them to this APB block group.

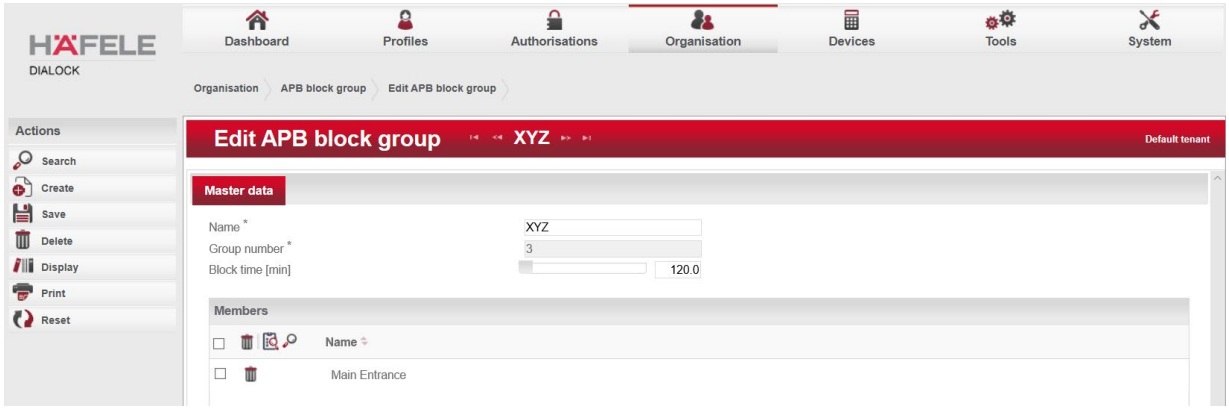




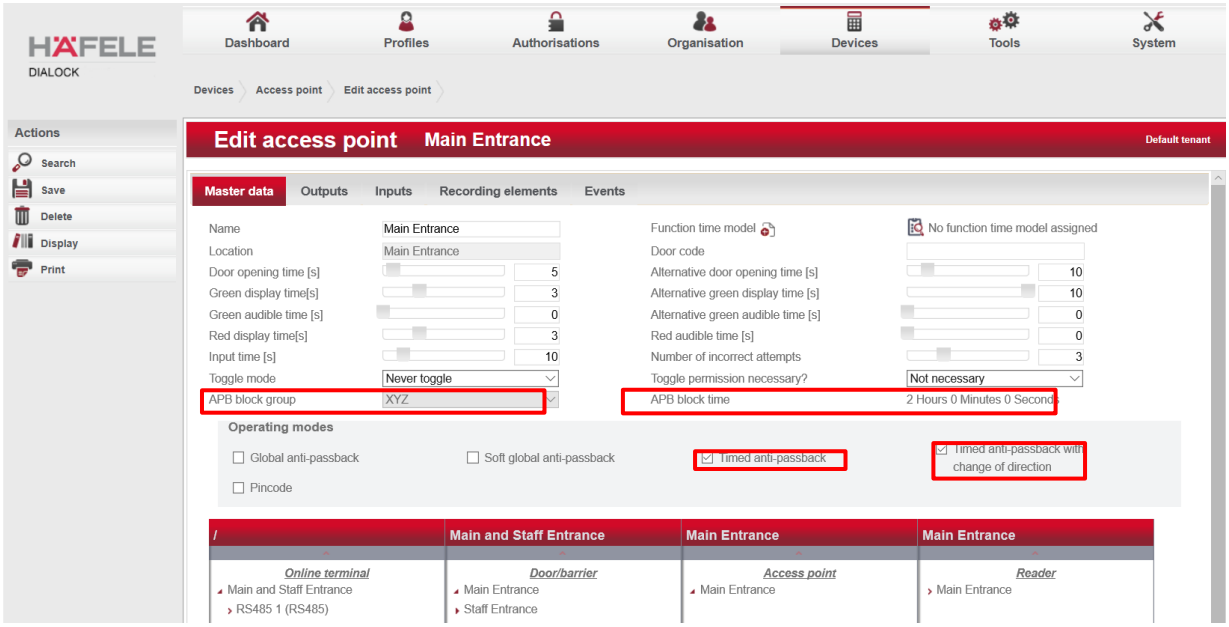
Then confirm your selection with “**Apply selection**”.



Save the procedure in the left-hand action menu with 

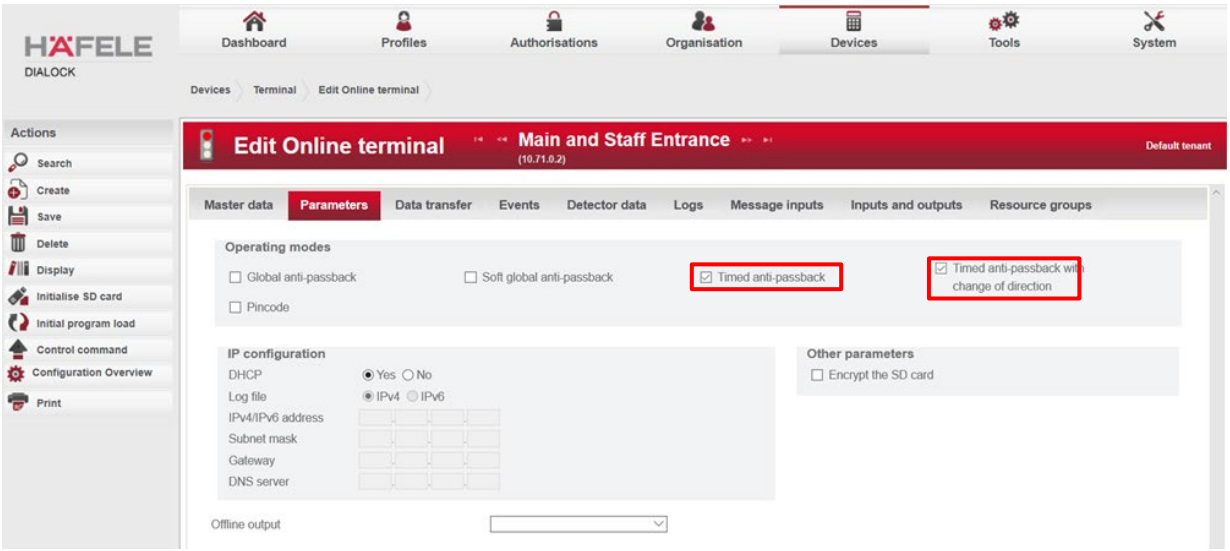


You have added access points to the APB block group and therefore created an APB block group.
At the same time, the **Anti-passback block** and **Timed anti-passback with change of direction** operating modes are automatically activated at the access points added to the APB block group. The relevant **APB block group** and the **APB block time** are also stored there.



5.4.4.2. Activating the anti-passback block in the terminal

Switch to the **Device / Terminal** menu and select the terminal which you have assigned to the APB block group.

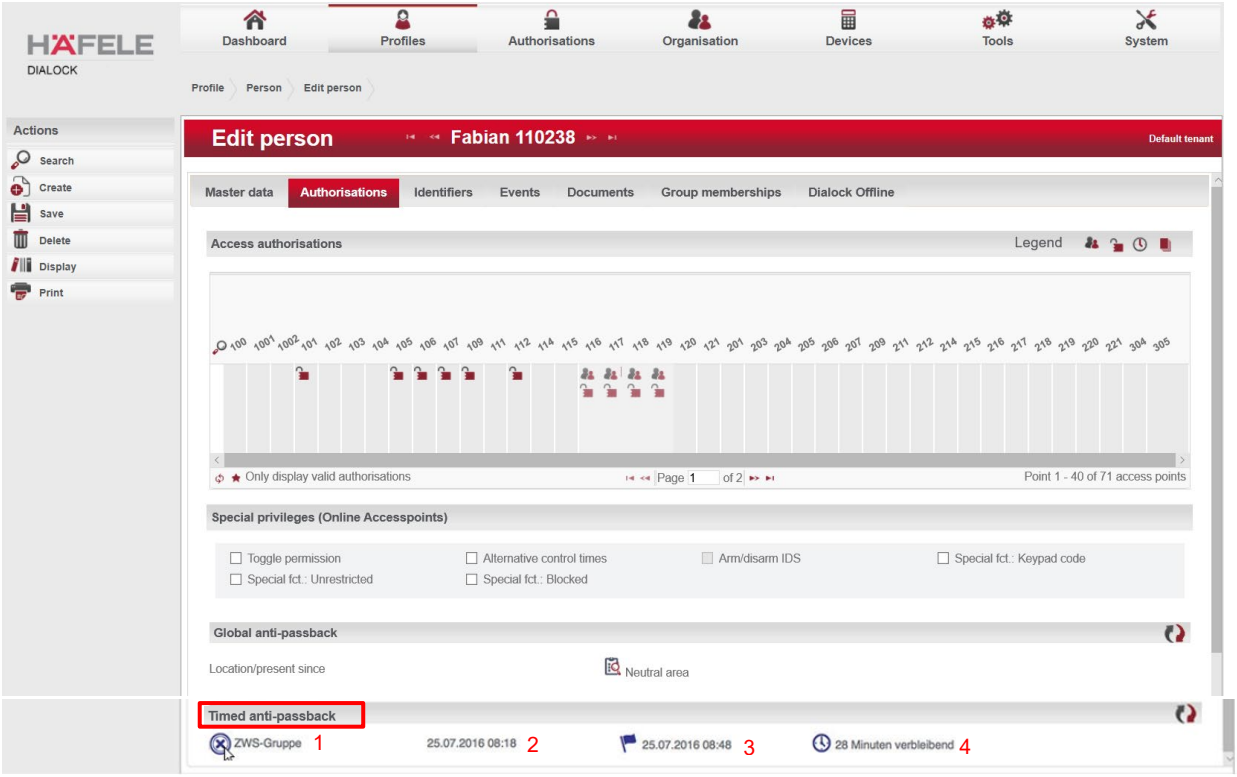


Select the “**Parameter**” tab and activate the “**Anti-passback block**” check box.

If the “**Timed anti-passback with change of direction**” is required, activate this check box as well.

5.4.4.3. Display status of a person's anti-passback block

The overview of all created persons is accessed via the "**Profiles / Persons**" menu. Select the required person and switch to the "**Authorisations**" tab. Scroll all the way down to the bottom to the "**Anti-passback block**" section.



The status of the anti-passback block is displayed here.

Functions:

1: Display APB block group. The person has registered at one of the access points of the specified APB block group

2: Date and time of transaction, i.e. the start of the anti-passback block

3: End of anti-passback block. Specification in date and time

4: Display remaining block time

5.4.4.4. Reset a person's anti – passback block

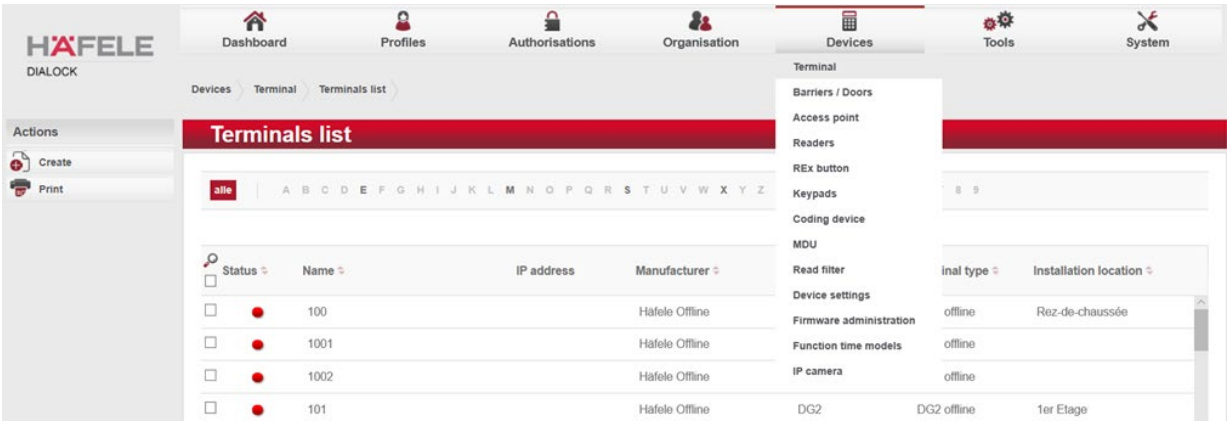
Click on the delete symbol for the APB block group (1).

You have reset the *Anti-passback block* for the selected *Person*. Resetting is displayed on the dashboard with **Name**, **Transponder**, **Event type** and **Transaction time**. The user who caused the reset is logged under **Resource**. This reset is person-related, i.e. if this person has multiple transponders, resetting deactivates all active anti-passback blocks for this *person*.

5.5. Devices

First, create the devices in your system such as terminals, barriers/doors, access points, readers, REx buttons, keypads and encoding devices as follows:

5.5.1. Terminal

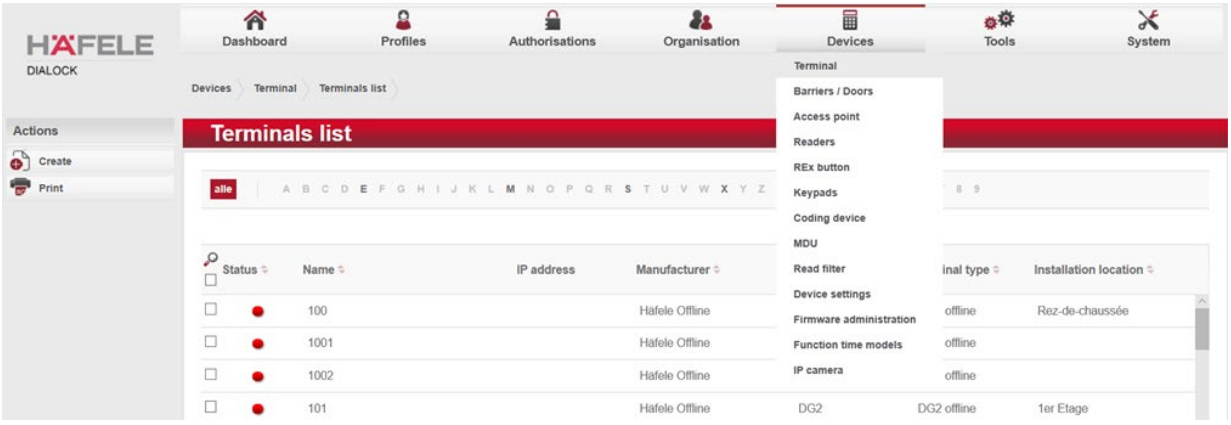


5.5.1.1. The online terminal

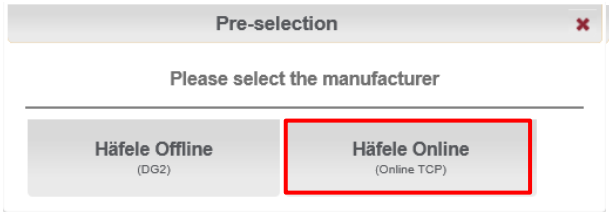
In order to establish a connection between the online terminal (WT 200) and the Dialock software, the user programs an SD card at his PC workplace for each WTC 200 controller. This card contains the configuration data that has been selected for the respective controller and the relevant communication parameters. No more settings then need to be made at the WTC 200 controller, provided that you work with the default values.

5.5.1.1.1. Create online terminal / master data

To create an online terminal such as the WT200, select **Device / Terminal** in the menu.

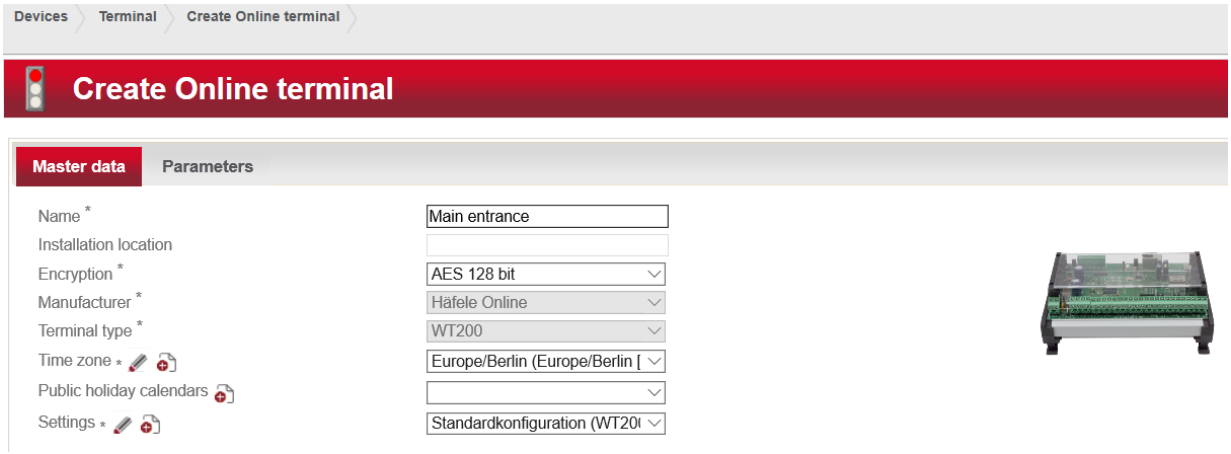


Selecting the “**Create**” action in the left-hand action bar opens a pre-selection window. Select **Häfele Online (Online TCP)** for an WT 200 online terminal**.**



Give the terminal a suitable **Name**.

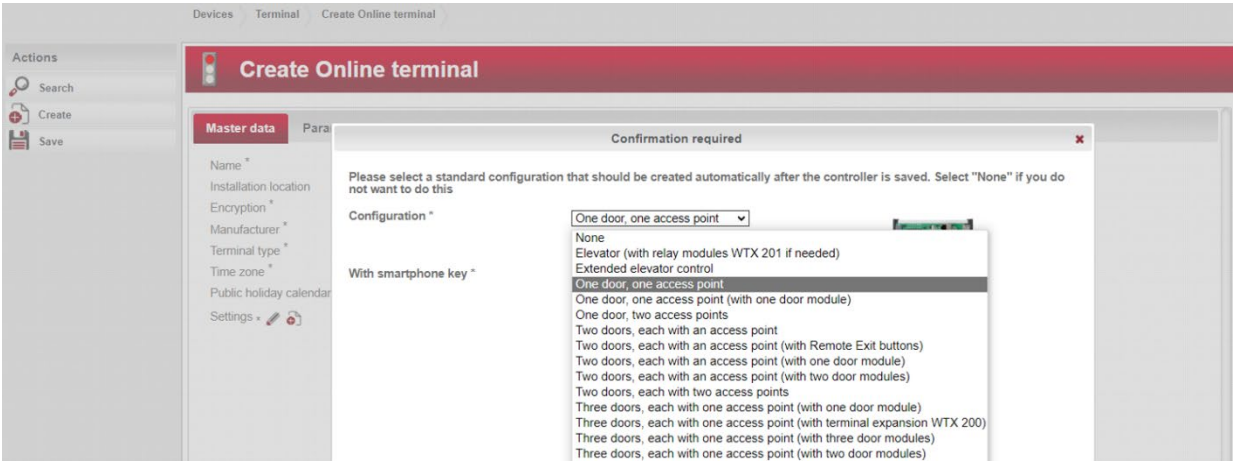
Note
This name is entered into the root directory of the SD card later and is used for correct assignment of the SD card to the WTC 200 controller.



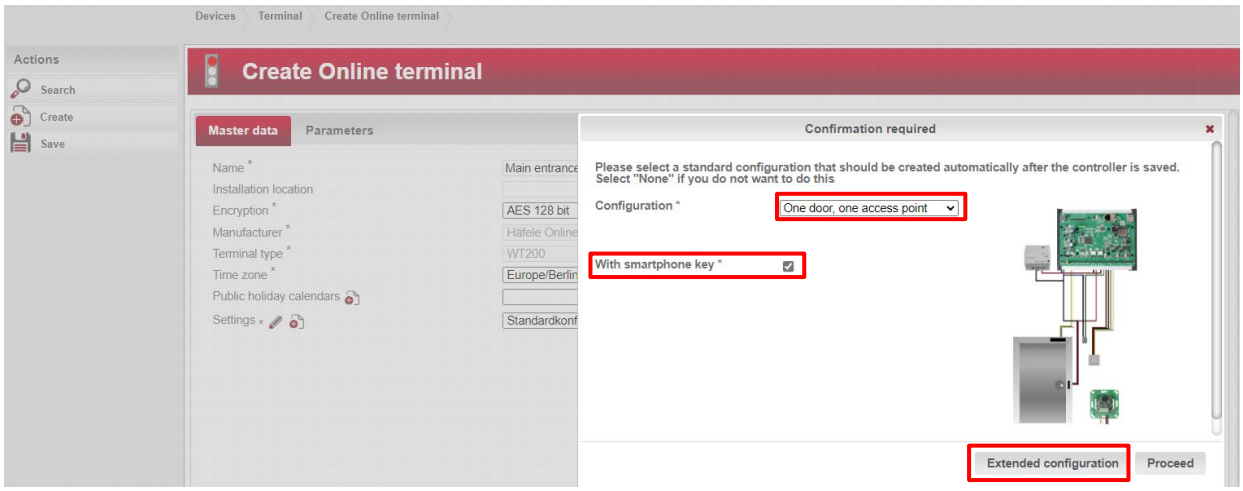
You can also describe the **Installation location** of the terminal, assign a previously defined **Public holiday calendar** to it, and assign the **Time zone** that is valid at the installation location to the terminal.

With regard to **Encryption** and **Settings** it is advisable to take over the suggested default values. Changes in this area should only be made by a trained technician.

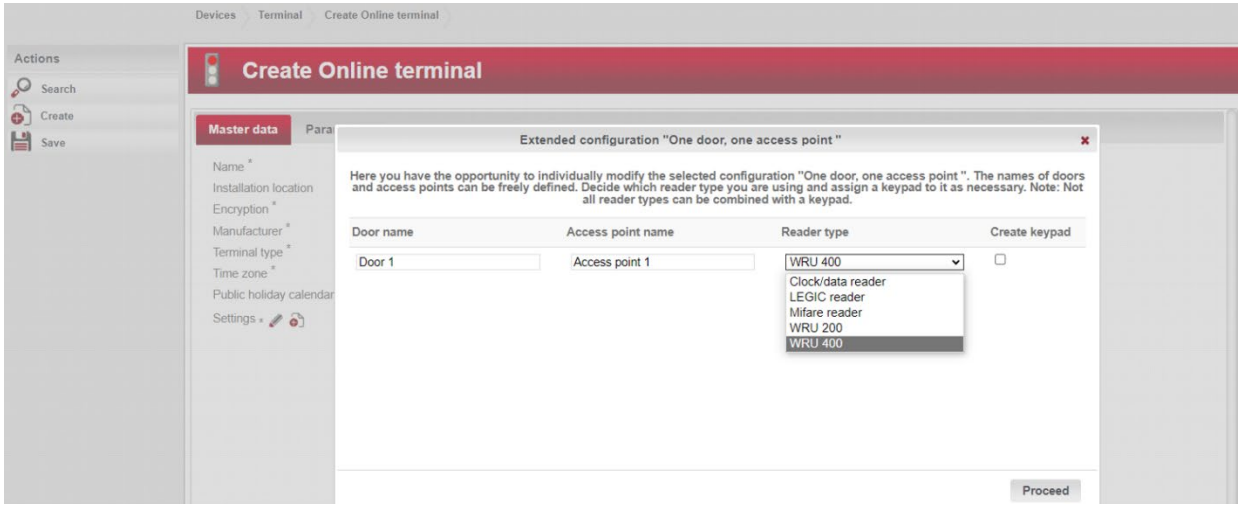
After saving, you are taken to the configuration selection.



The drop-down menu contains well-tried standard configurations which you can modify as required. However, it is advisable to keep to the standards, since all other parameters are created on this basis. If you create a manual configuration, all other parameters have to manually adapted.
You are now presented with a graphical display of the selected configuration.

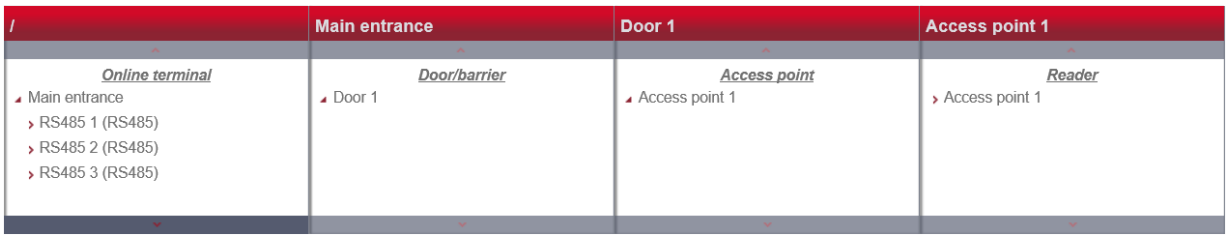


The WRU 200 reader type is generally stored in the standard configuration. Depending on the application, the reader type can be adapted to requirements accordingly under "**Extended Configuration**". If the "**With Smartphone Key**" option is activated, the preselection automatically changes to the WRU 400 reader type, since this is equipped with the Bluetooth (BLE) interface which is required for this.



If the reader type is modified at a later date, the entire reader must be deleted and re-created with the required reader type (**5.5.4.1** *Edit reader master data*).

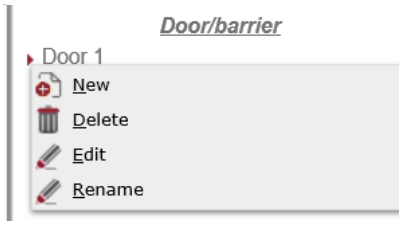
After saving, the associated system parameters are automatically set within Dialock, i.e. the associated elements such as doors, access points and readers are created in the system in accordance with the selected configuration (resources are defined).



The peripherals can be viewed from left to right in a hierarchy structure, and created, edited or deleted by right-clicking.

By clicking on the symbol ▸ you can obtain a display of the columns for the associated doors/barriers, access points etc. or hide them if you wish.

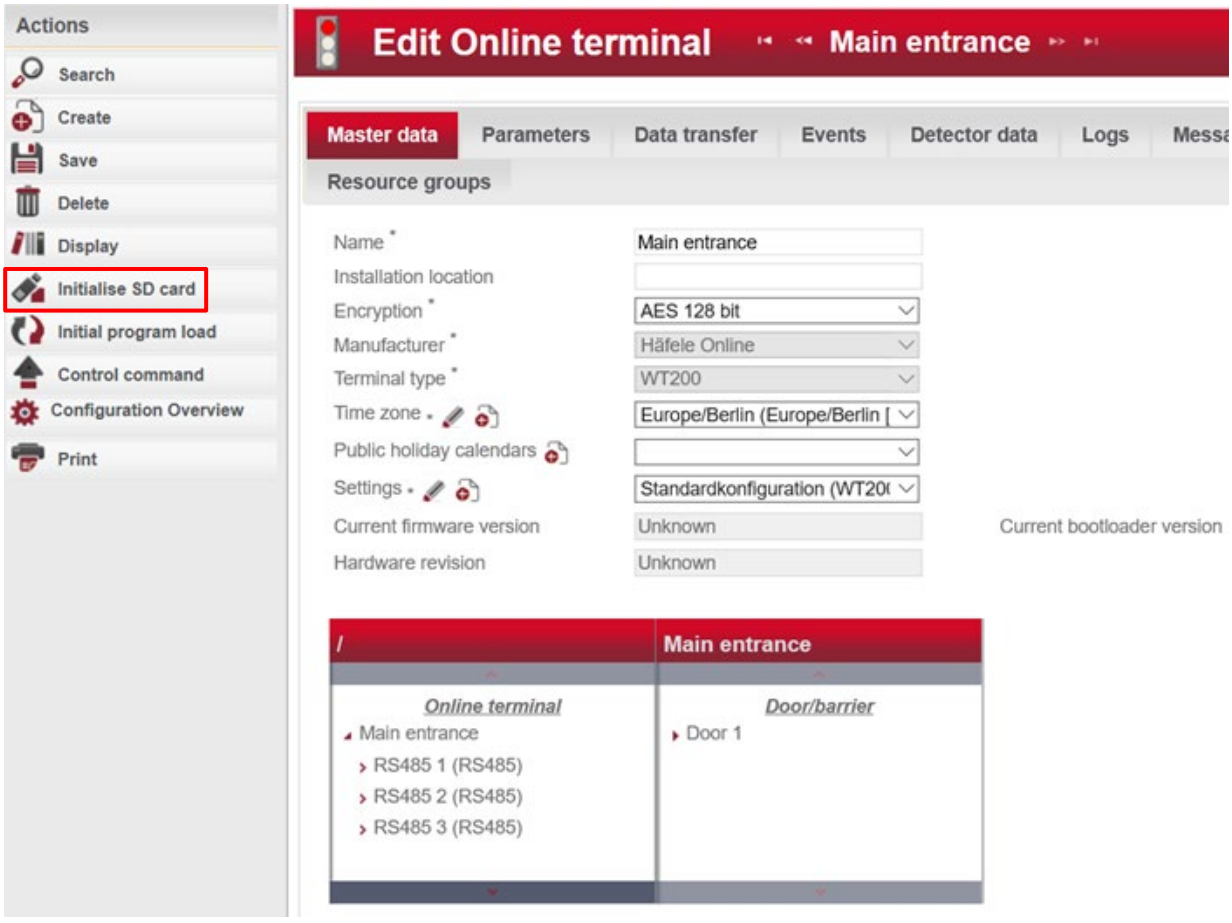
Right click to edit or delete parameters.



Initialisation of SD cards / Commissioning of a controller

In order to start up a WTC 200 controller, the SD card needs to be initialised. Always use the Micro SD card that was supplied with the WTC 200 controller. Ensure that you are at a workplace with an appropriate SD card reader and insert the SD card there.

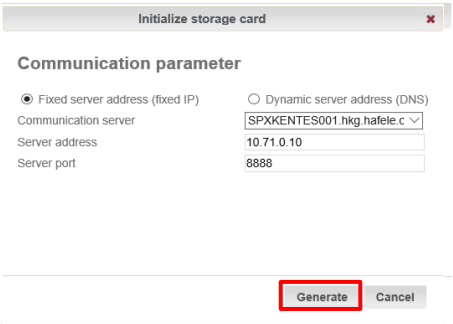
Then click on “Initialise SD card”.



Enter the relevant communication parameters.

The IP address is entered automatically by the system, as is TCP port 8888. If this port is not free, select another suitable port.

The DNS name is also entered automatically by the system and can be changed if required. However, it is advisable to use the default values if possible.



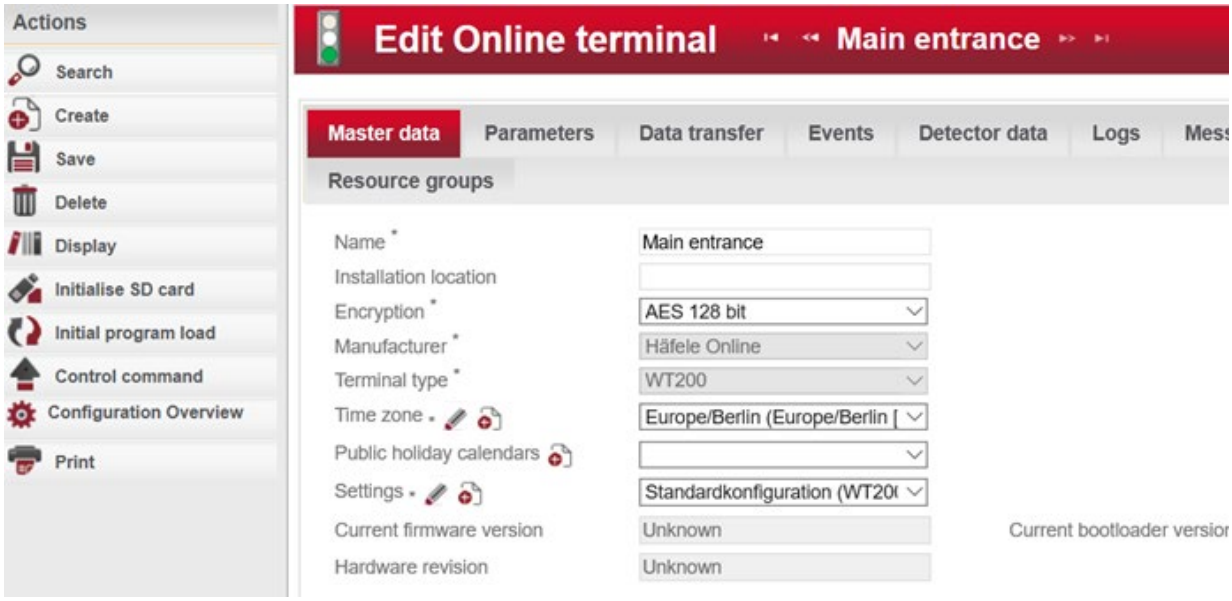
Click on Generate.

Unzip the .zip file contents onto the SD card.

Attention:
Before inserting the SD card into the card holder of the controller, ensure that the power supply is active and the 3 LEDs 15, 16 and 17 are illuminated in green. LED 6 must flash rapidly in green (no SD card present).

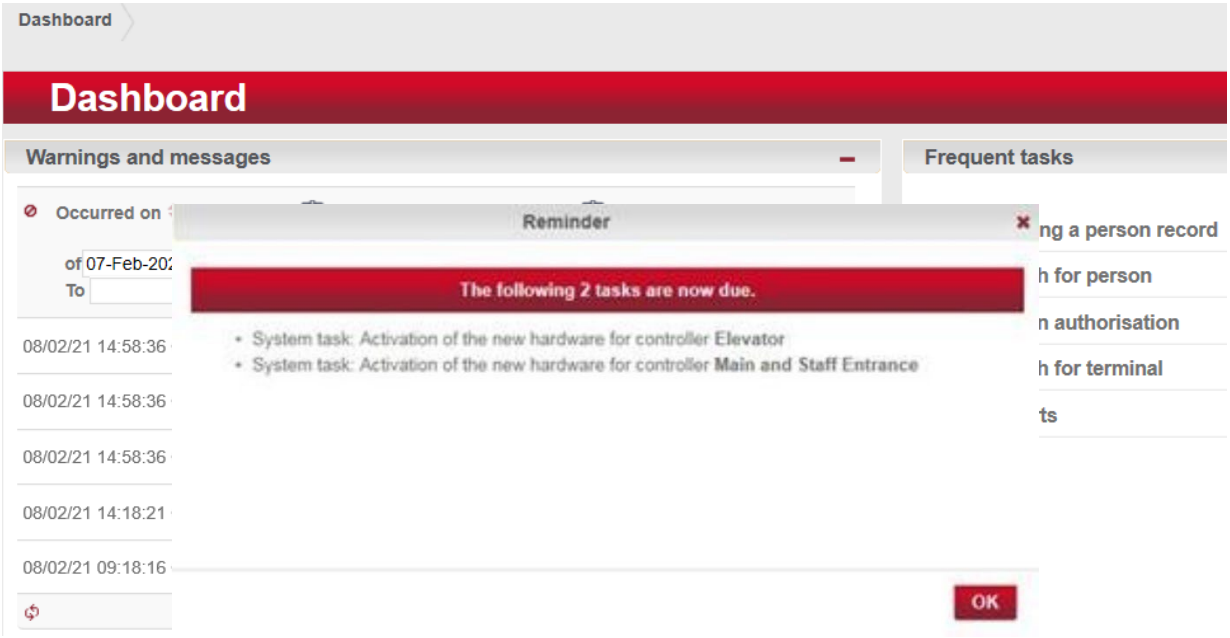
Now establish the network connection by inserting the network cable into the provided slot of the controller. The yellow LED at the network connection must flash slowly if the link to the network exists.
Now insert the SD card into the card holder of the controller. LED 6 will first flash in green, and then in white.

As soon as the connection between the WTC 200 controller and the host has been established, LED 6 goes off and the traffic light icon in Dialock changes from red to green.



As soon as the SD card was inserted into the controller, it is uniquely linked with the hardware of this controller. The WTC 200 controller is then ready for operation.

From now on, a change of SD card is only possible if confirmation from an authorised user is provided in Dialock. If no confirmation is received, the controller communicates with Dialock but the access control functions are not available until confirmation has been received.



Confirm any SD card change by clicking on “**Run**” in the left-hand action menu.

The **Bootstrap** function in the left-hand action menu represents an emergency function in the event of data inconsistency, e.g. after reconfiguring an access point in the software. Bootstrapping causes all Dialock data to be re-written to the SD card in the controller.

The selection dialogue shown in the following is accessed using the **Control command** function in the left-hand action menu.

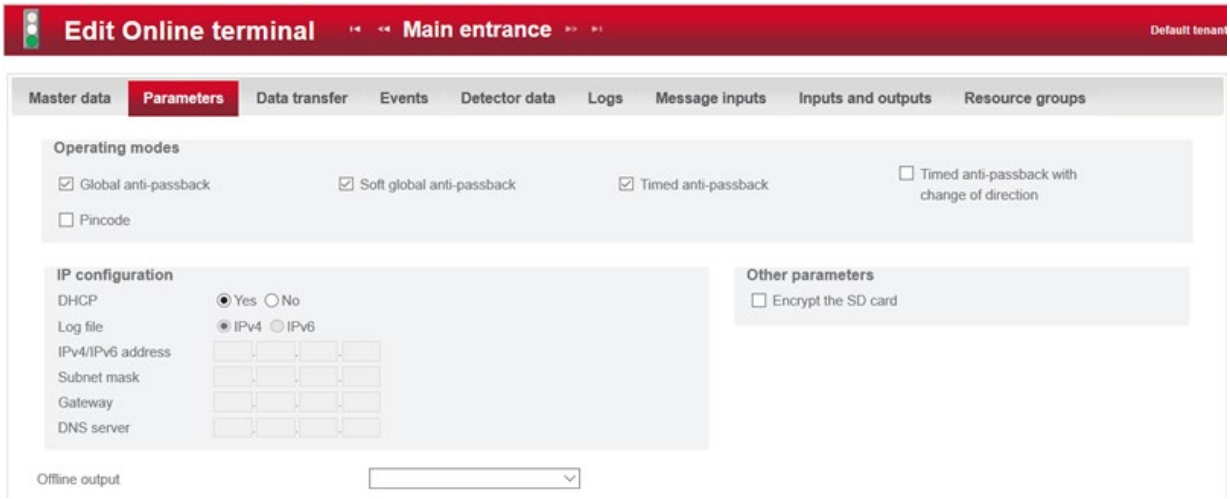
The controller is reset using **Restart**.

Delete permanent memory should only be carried out after explicit instructions from a responsible technician.

Check SD card is used to check the SD card for errors.

5.5.1.1.2. Online terminal / parameter settings

In the “**Parameter”** tab, you can set various operating modes (**Global anti-passback, Soft global anti-passback, Timed anti-passback and Timed anti-passback with change of direction, PIN code**).



Depending on the available options, one of the following operating modes can be selected:

Global anti-passback
This prevents access to a neighbouring area if the person with the access authorisation is not listed as present in the area that he is currently in. A person can only leave an area that they have entered beforehand. A prerequisite for a global anti-passback is the presence of an interior reader and an exterior reader at the relevant access points. If a person is not registered in the relevant area, the transponder is invalid for exiting from this area. An appropriate alarm is generated and the door is not released.

Soft global anti-passback
In the event of a global anti-passback error, the door to be unlocked is unlocked in spite of this. As a result, an access control error transaction is sent to the system.

Anti-passback block
Activation of the anti-passback block prevents a repeated access attempt at a door in the same timed anti-passback group within an adjustable time.

Timed anti-passback with change of direction
As above, but a door can always be opened from the other side/direction.

PIN code
Activate the PIN code check box if a wall reader with a keypad is going to be operated at this terminal. The PIN code must be generated for every person in the person master record.

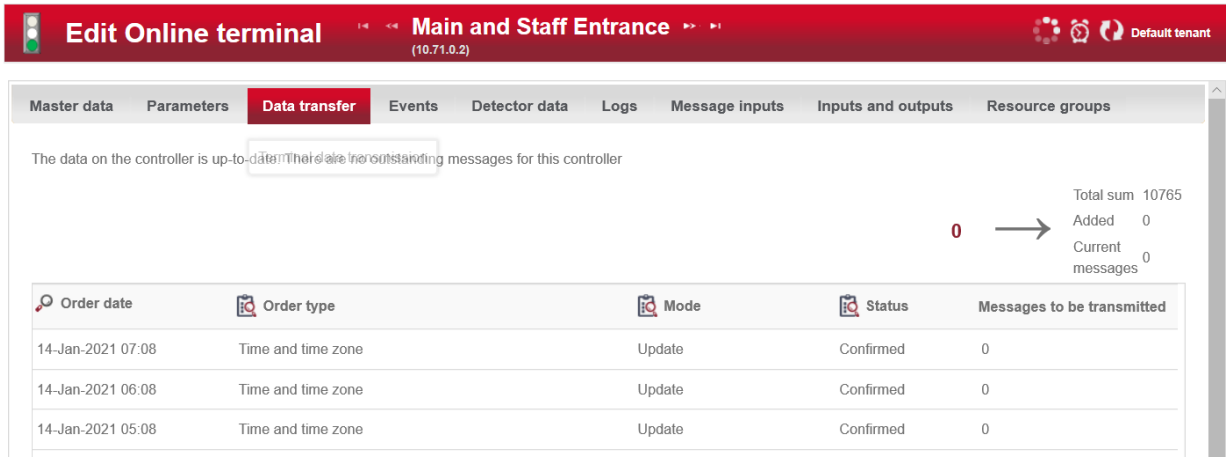
IP configuration
If DHCP is marked with “Yes”, no more entries need to be made here. If you do not use DHCP, please make the relevant entries in accordance with your IT administration. This information must be set in accordance with the specification of your department so that the terminal can communicate with the server.

SD card encryption
If the check box is checked, apart from the log files, the transaction files (parameter has to set separately) and the communication parameters, all other data on the SD card of the WTC 200 controller is encrypted with AES128. This check box should be activated if all access-related data on the SD card of the controller is to be saved in encrypted format.

Note:
The use of encryption slows down the reaction time of the controller slightly.

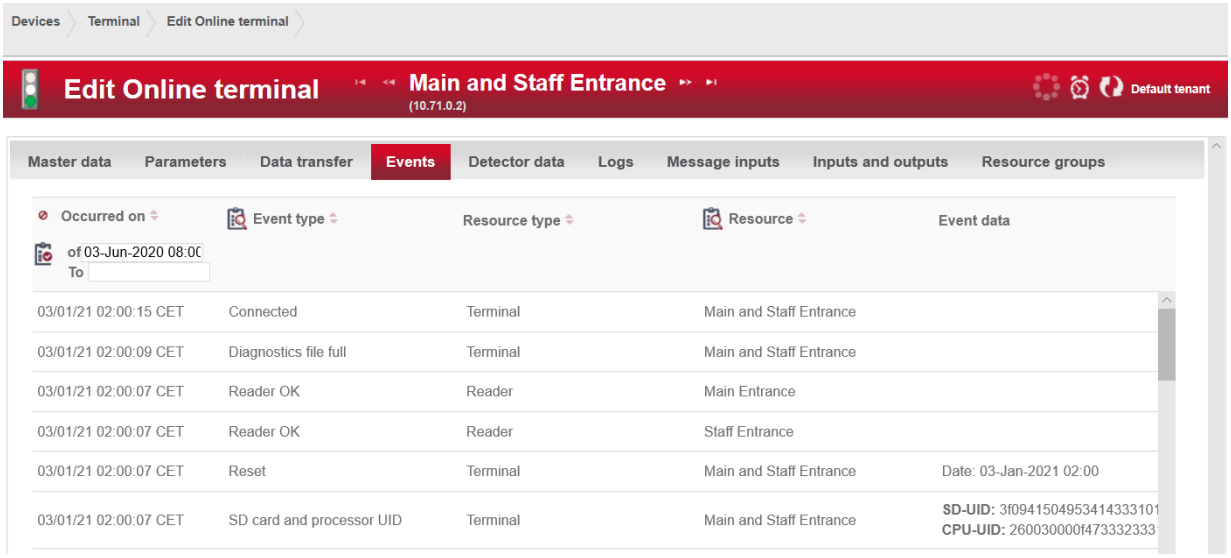
5.5.1.1.3. Online terminal / data transfer

The “**Data transfer**” tab displays the difference from the target/actual comparison of the data to be transferred. All data packages that are pending for transfer can be found here.
The newest logs are at the top.



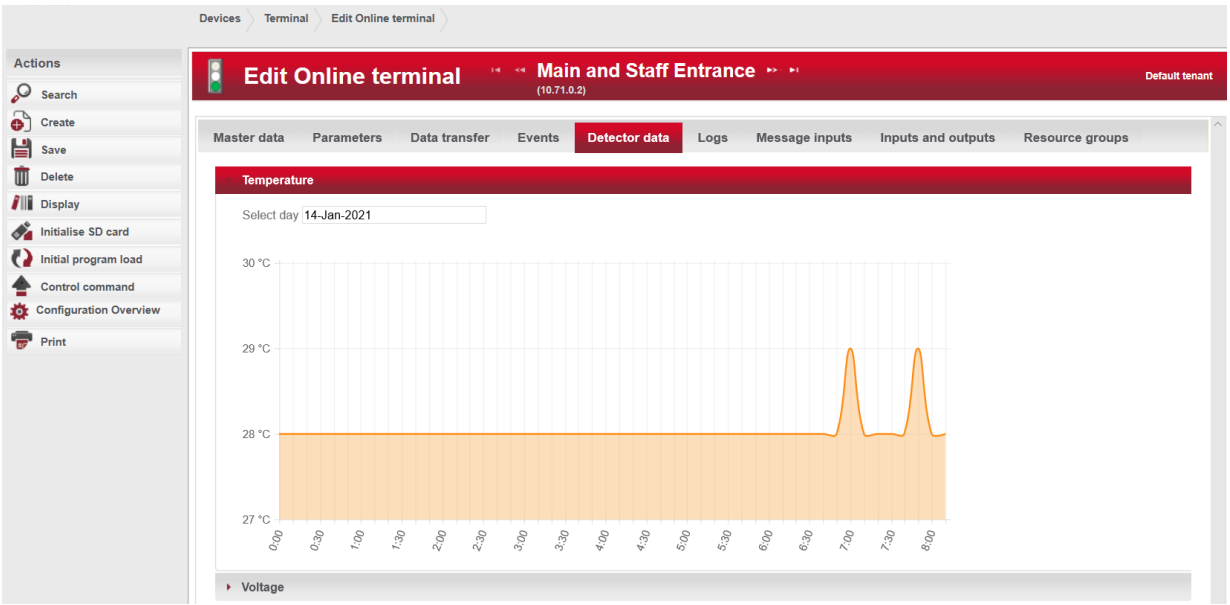
5.5.1.1.4. Online terminal / events

Under the “**Events**” tab you will find the events that have been sent by the terminal and can be selected according to event type, date and resource.



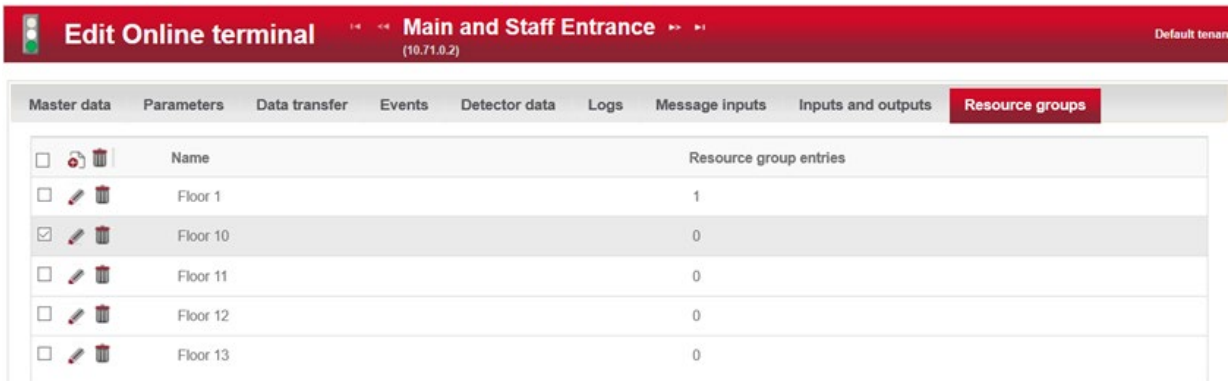
5.5.1.1.5. Online terminal / detector data

In the “**Detector data**” tab of the **Devices / Terminal menu** of the selected terminal, the temperature and voltage values of the last 7 days can be queried. The values are displayed graphically and can be shown for each day provided that the display thereof has been activated previously in the “**Transactions**” tab in the Devices/Device settings menu of the required terminal.



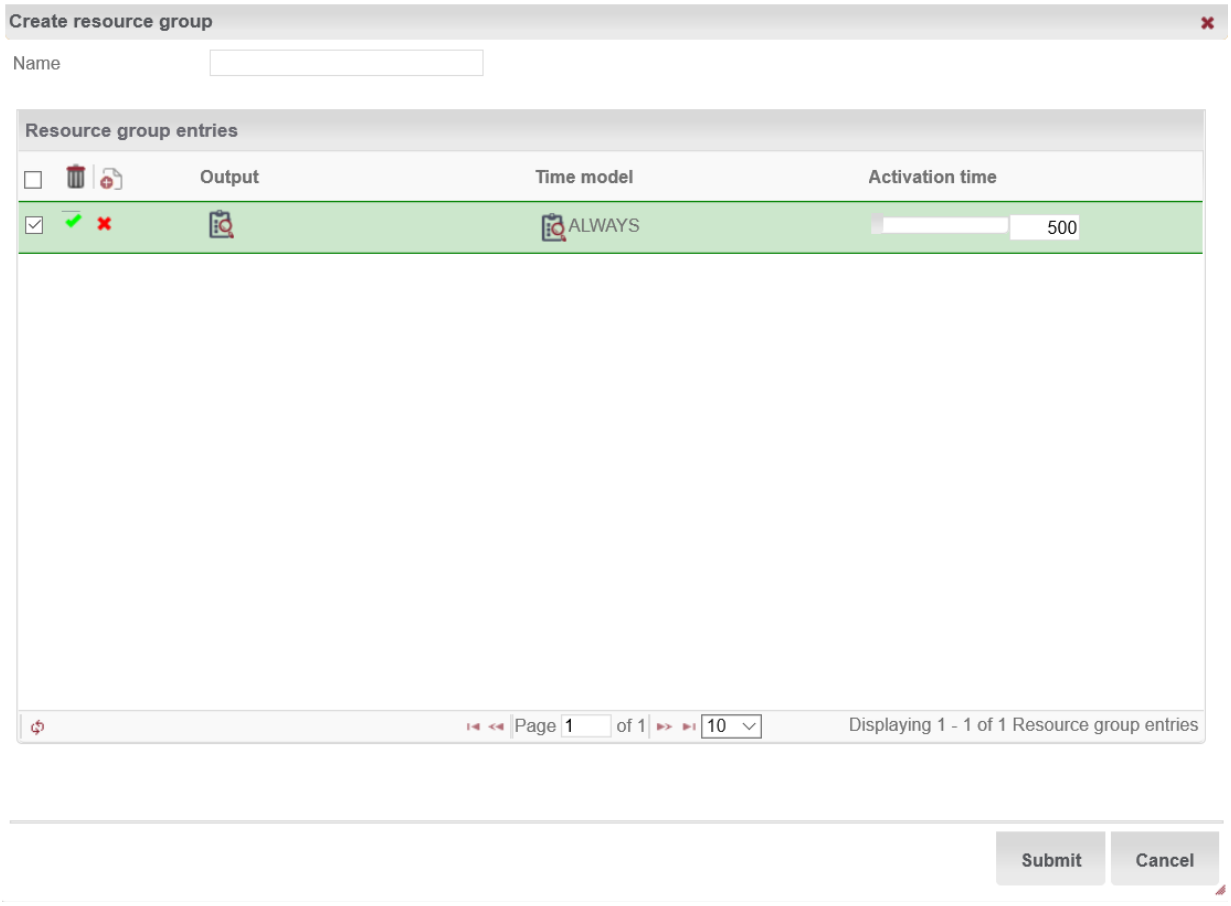
5.5.1.1.6. Online terminal / resource groups

In the “**Resource groups**” tab, individual or multiple outputs of an online terminal can be selected, which can then be authorised for a person at an access point in an authorisation matrix, individually as a resource group.



Click on the symbol  “**Create new data record**” to create a new resource group.

The “**Create resource group**” window will open.
Give the resource group a name and click on the symbol “Create new data record” under “**Resource group entries**”.

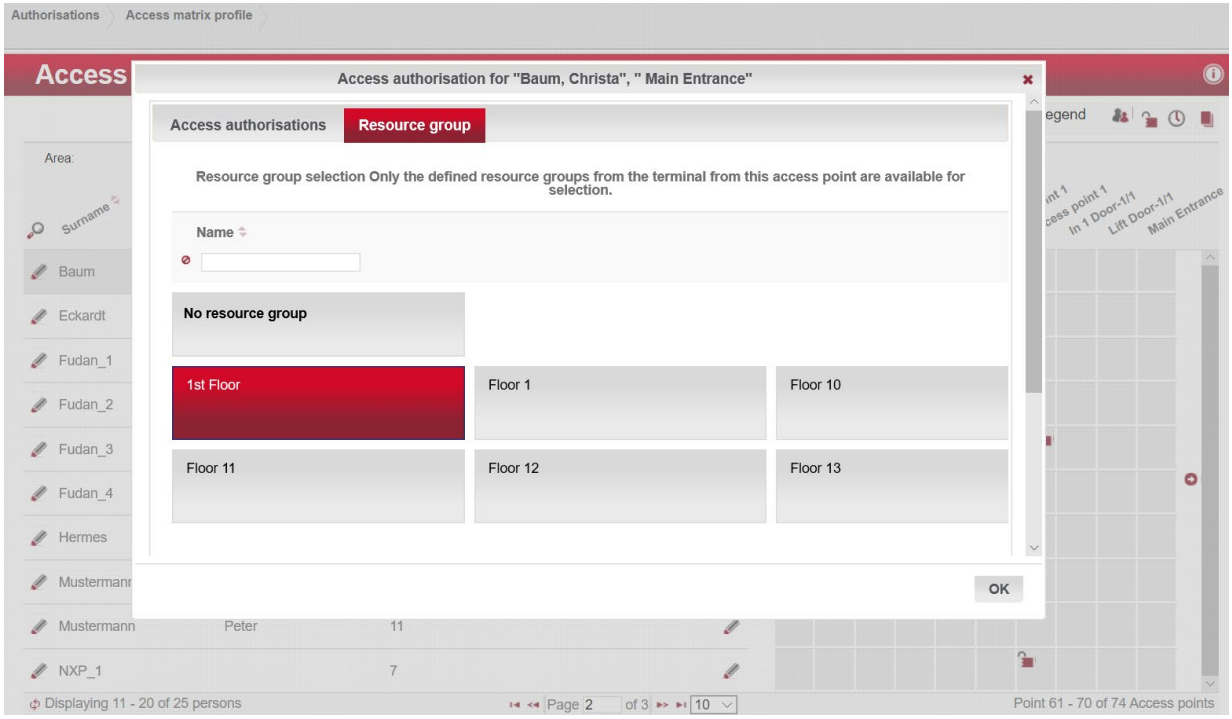


You can now enter the required output, the time model that you require for it and the activation time in the event of authorisation in the line marked in green.

Then click on the green check mark to save this resource group entry.
You can now create other entries as well.

When you have finished, click on “Save” at the bottom right.

Then save the terminal again.



The “**Resource group**” tab can now be selected in the same window in an access matrix after a person has been granted an authorisation at this online access point.

Choose the resource group which you created there.

The person is now authorised at this access point for the outputs defined in the resource group entries.

5.5.1.1.6.1. Online terminal / lift control

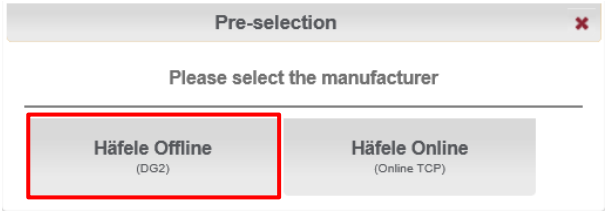
If you select (extended) lift control when an online terminal is being created and define the number of floors, a resource group (**5.5.1.1.6** *Online terminal / resource groups*) is automatically created for every floor (exit) with the relevant resource group entry.

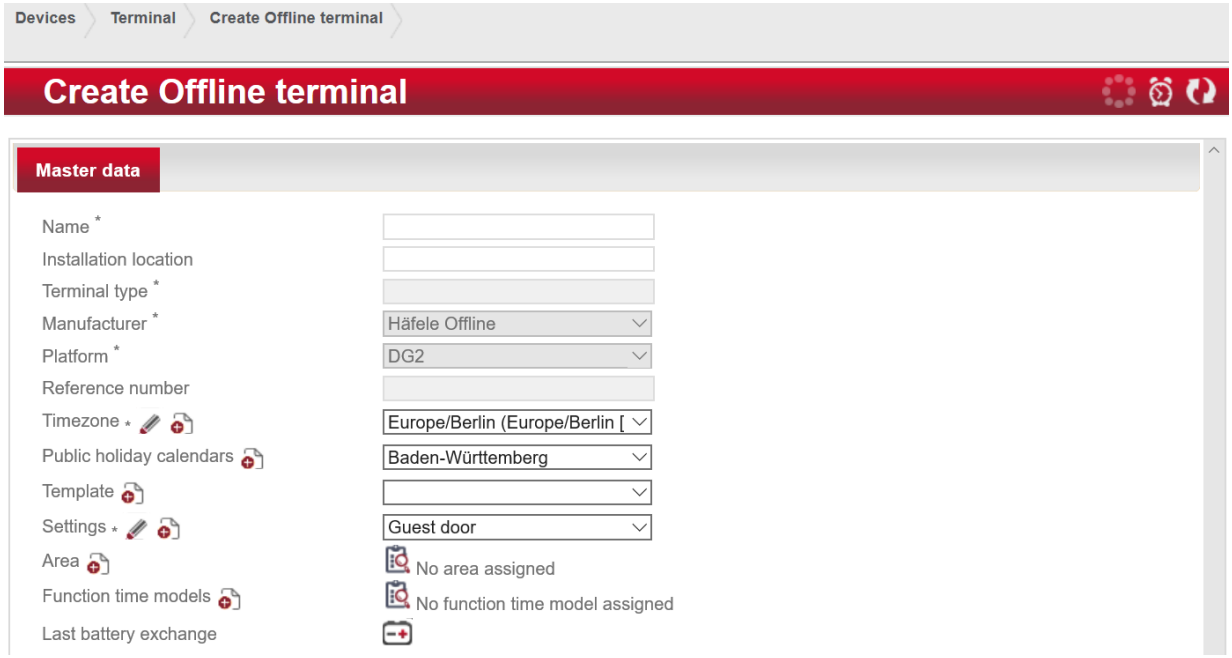
5.5.1.2. The offline terminal

You can create a new terminal using the **Devices / Terminal** menu.

Selecting the “**Create**” action in the left-hand action bar opens a pre-selection window.

Select the **Häfele Offline** option here.





Enter the designation of the access point that will subsequently also be displayed in the access matrix as “**Name**”.
The designation must correspond to the Windows folder naming conventions (no special characters and spaces).

Additional information concerning the installation location of the terminal can be entered under **Installation location** if required.

The **Terminal type** is set automatically by the system to suit the **Template** selection.

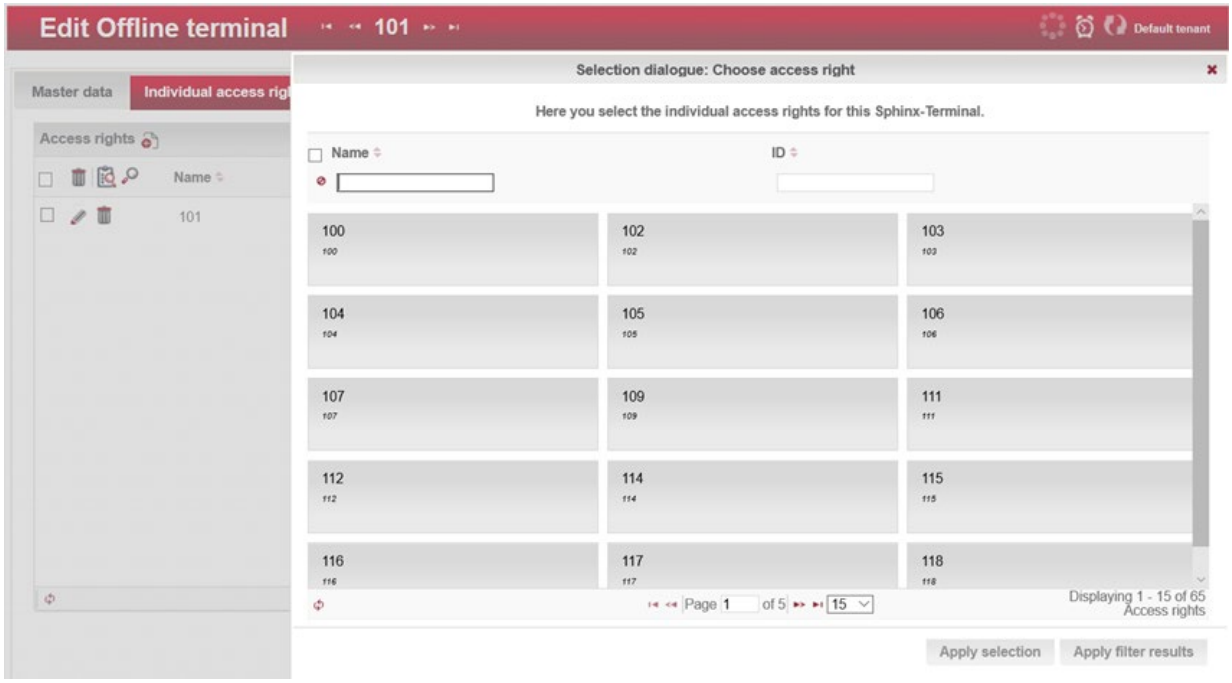
If you have already defined **Areas**, here you can assign the required offline area to the terminal (**5.4.2.2** *Create / edit offline areas*).

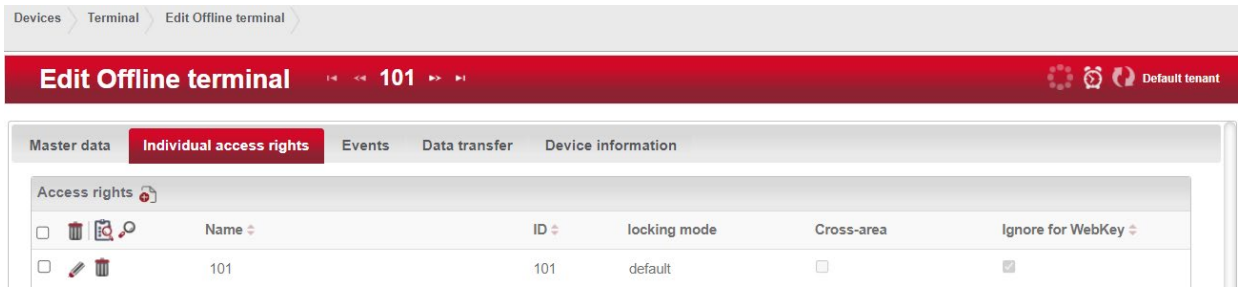
If **Function time models** have already been defined which will be used for this terminal, they can be assigned here.

Last battery exchange shows the date of the last completed battery change.

5.5.1.2.1. Offline terminal / Assign individual access rights

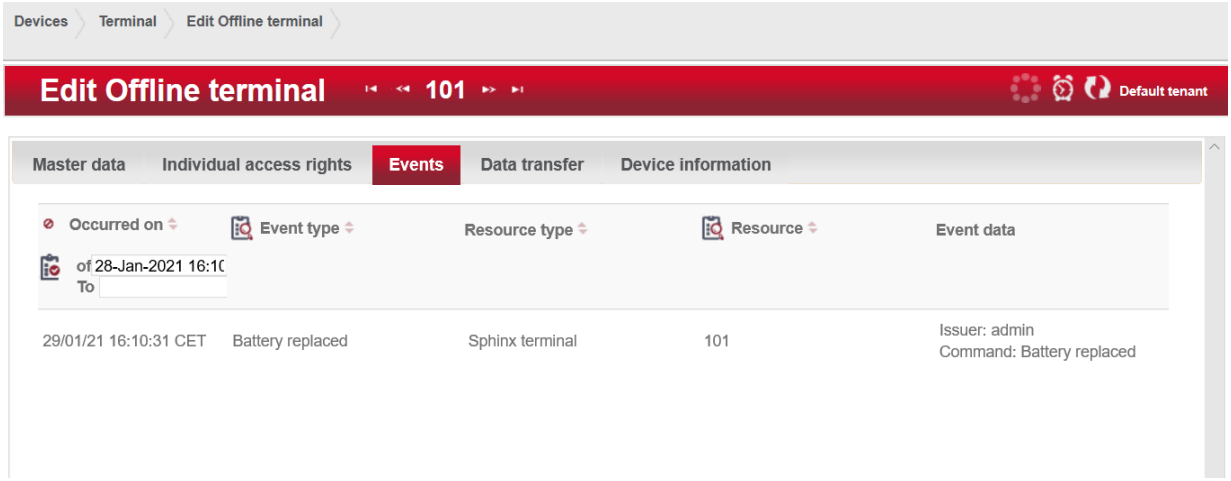
You can assign the individual access rights to the offline terminals in the “**Individual access rights**” tab of the **Devices > Terminal** menu.



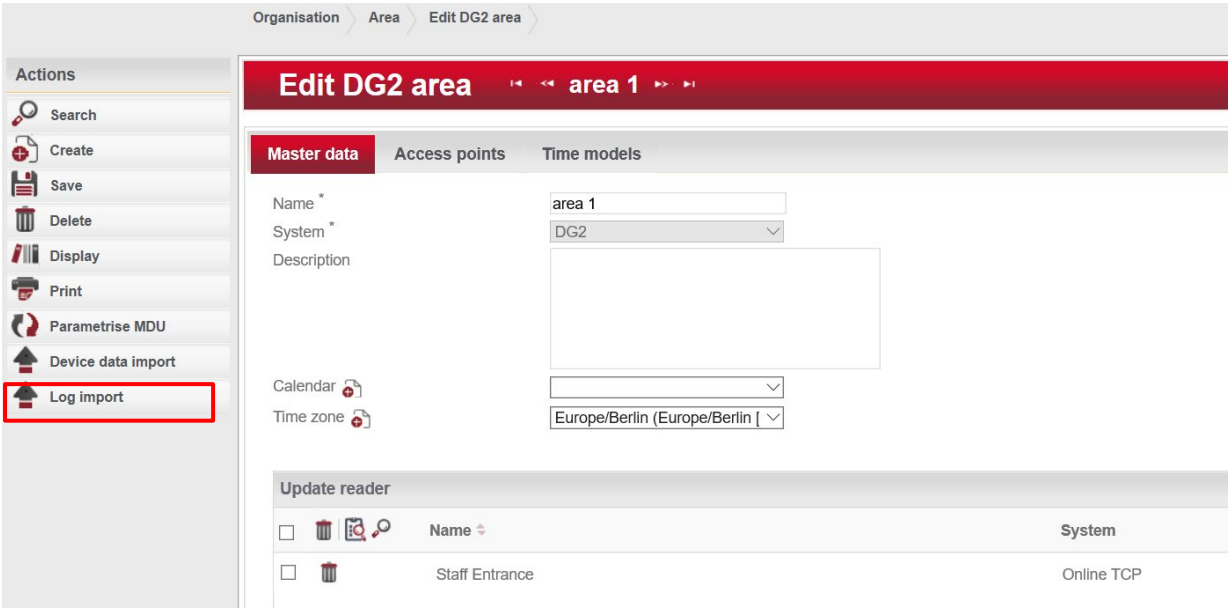


5.5.1.2.2. Display offline terminal / events

A Dialock offline terminal can save at least 1,000 events. These events can be displayed if they have been read out of the terminal beforehand with the MDU 110 and imported into the Dialock software.

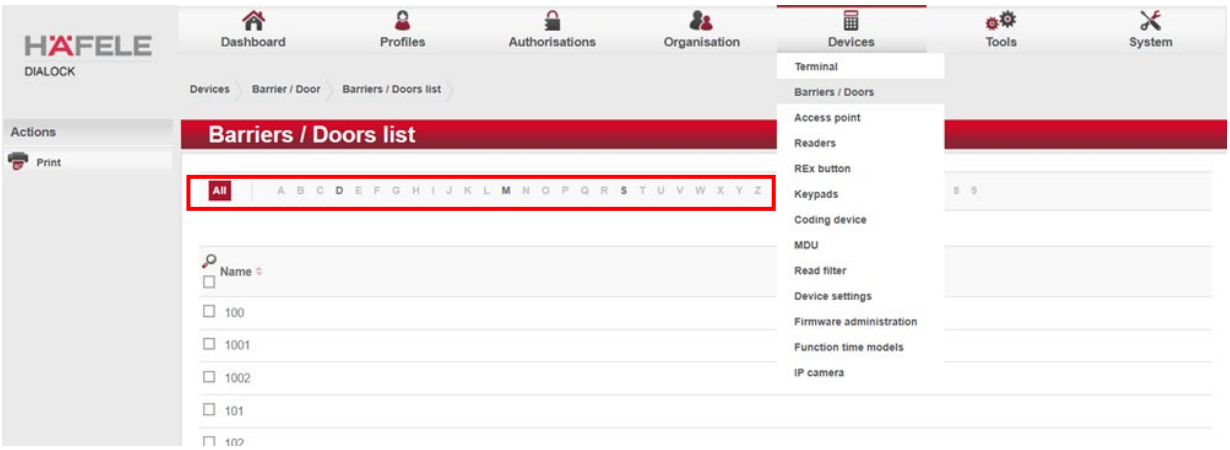


Events at offline terminals can be read out with the MDU 110 using the "**Terminal>Logs**" menu and imported into the software using menu item "**Organisation>Area>Edit area**" and action "**Log import**".

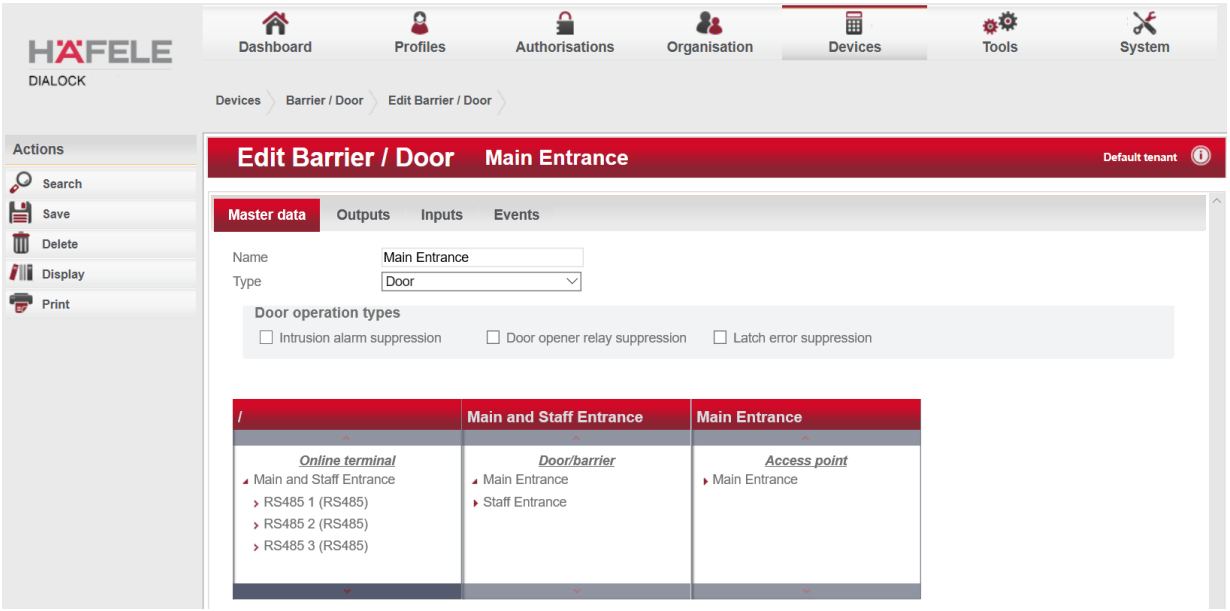


5.5.2. Barriers / doors

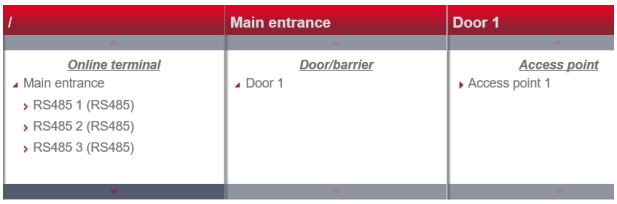
The **Devices-> / Barriers / doors** menu takes you to a overview of the barriers or doors. All barriers / doors are displayed using the "**All**" filter. However, you can obtain a display of specific barriers / doors via the alphanumeric search list.



If you select a barrier / door, the editing screen opens.

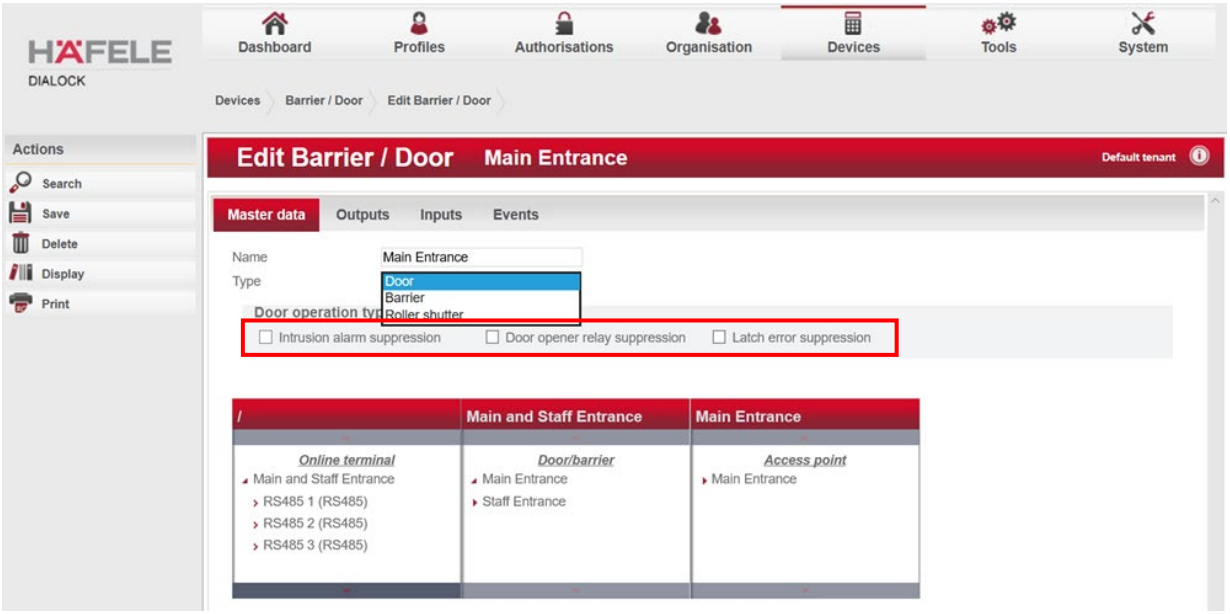


Alternatively, the editing screen for the required barriers/doors can be accessed when creating online terminals by right clicking on symbol ▸, then “**Edit**”.



5.5.2.1. Edit the barrier / door master data

Give the door a meaningful **Name** in order to be able to clearly identify and assign it later. For **Type** you can choose between “Door”, “Barrier” or “Roller shutter”.



Select the required special control type for your doors / barriers from the door operating modes.

Intrusion alarm suppression
If this door operating mode is activated, intrusion alarms are suppressed at this door. This setting is recommended if the door has neither a reader nor a REx button on the inside, and the door is only opened using a handle. Opening using a handle would signal a door break-in.

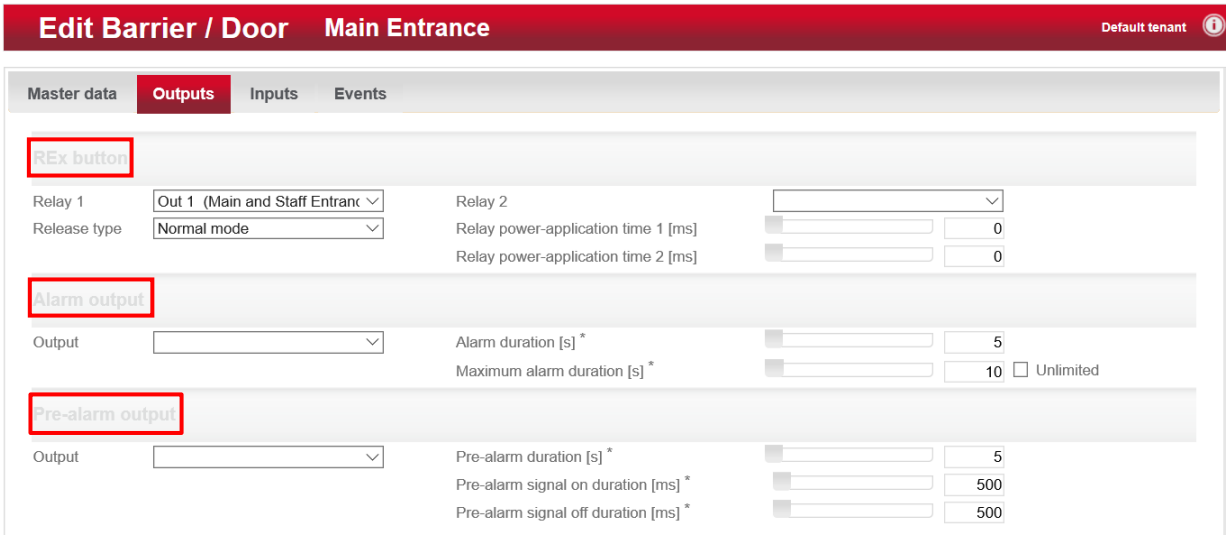
Door opener relay suppression
Activate this door operating mode if pressing the REx button should not energise the door opener relay. This check box is required if the door is opened from the inside via the handle with an integrated handle contact.

Latch error suppression

If this door operating mode is activated, a latch error alarm is suppressed at this door. This setting may be useful in certain situations (e.g. maintenance work). Or if it is known that the latch is temporarily not working properly, but there is no actual security risk.

5.5.2.2. Edit outputs of the barriers / doors

In the “**Outputs**” tab of the **Devices / Barriers / Doors** menu, the existing outputs of the terminal are led to the relevant functions.



REx button:

Relay 1: Select the required relay 1.

Lock release type: Normal mode
(Relay 2 does not matter here, and no details for the relay actuation time are needed.)
The other selection options of the drop-down menu are special settings. These are needed if automatic doors, turnstiles etc. are to be controlled.

Alarm output:

Output: Select the required relay output for controlling the alarm here.

Alarm duration: The alarm duration represents the actuation time of the alarm relay.

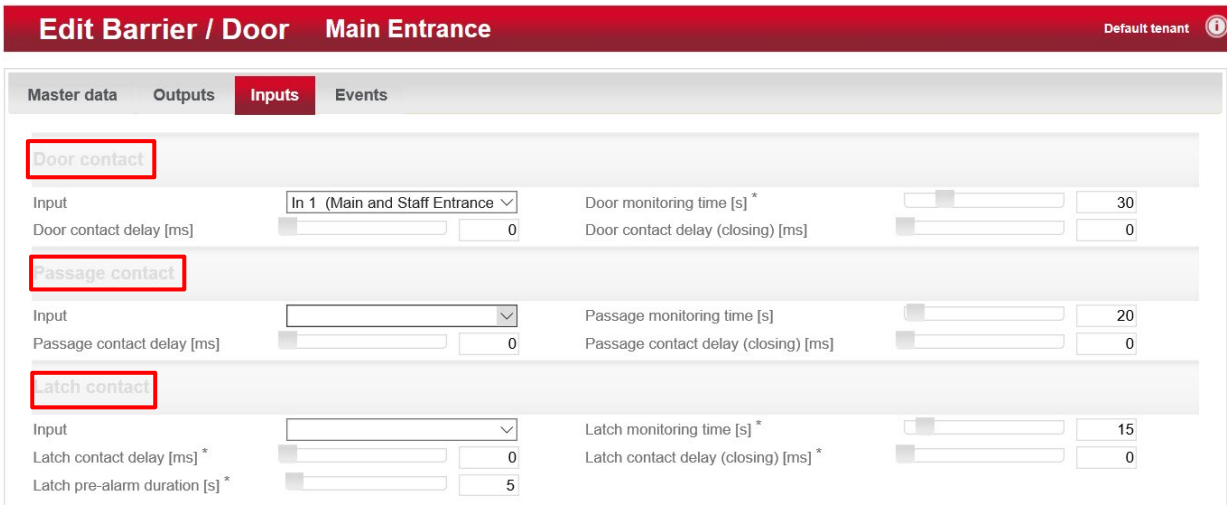
Pre-alarm output:

Output: Select the required relay output for controlling the pre-alarm here.

Pre-alarm duration: The pre-alarm duration is the time for which the pre-alarm is triggered before the alarm. The time for which a pre-alarm is triggered before the actual alarm, e.g. door monitoring max. door opening time 20 sec. pre-alarm = 5 sec., i.e. pre-alarm triggered at 15 sec. You now have 5 seconds before the main alarm is triggered.

5.5.2.3. Edit inputs of the barriers / doors

In the “**Inputs**” tab of the **Devices / Barriers / Doors** menu, the existing inputs of the terminal are linked to the relevant functions.



Door contact:

Entrance: Select the required input for door monitoring from the drop-down menu.

Door monitoring time: This the length of time for which the door may remain open without the door alarm being triggered.

Door contact delay: This is needed in special cases such as automatic doors and turnstiles.

Passage contact:

Entrance: Select the required input for the passage contact.
In addition to the door opening action, the passage of a person is also registered with this function, e.g. for global anti-passback.

Passage monitoring time: This is the duration for which passage through the door is monitored with the aid of the passage contact signal.

Passage contact delay: This describes the time by which the passage contact can be activated with a delay.

Latch contact:

Entrance: The latch contact is required if the latch of a lock is to be monitored.

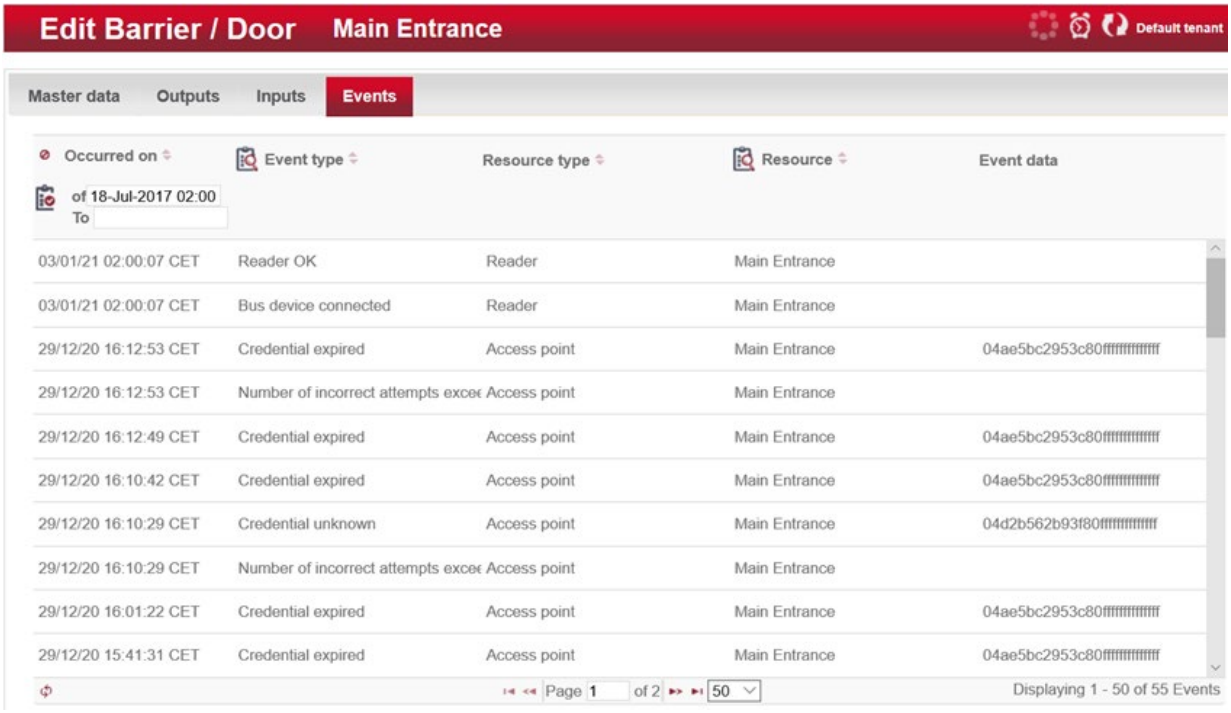
Latch monitoring time: This represents the duration for which the latch may not be extended without the door alarm being triggered.

Latch pre-alarm duration: This represents the delay before an alarm is triggered.

Latch contact delay: This describes the time by which the contact can be activated with a delay.

5.5.2.4. Events on barriers / doors

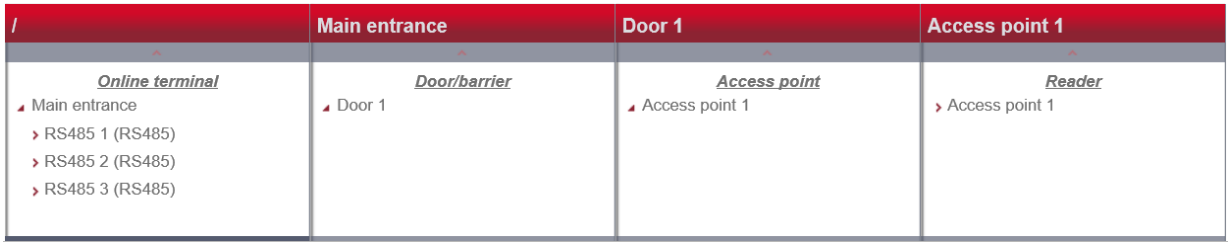
In the “**Events**” tab of the **Devices / Barriers / Doors** menu, events that have occurred at the barriers/doors can be filtered and listed according to date, event type and on the basis of resources.



5.5.3. Access point

The **Devices / Access point** menu takes you to the access point editing screen.

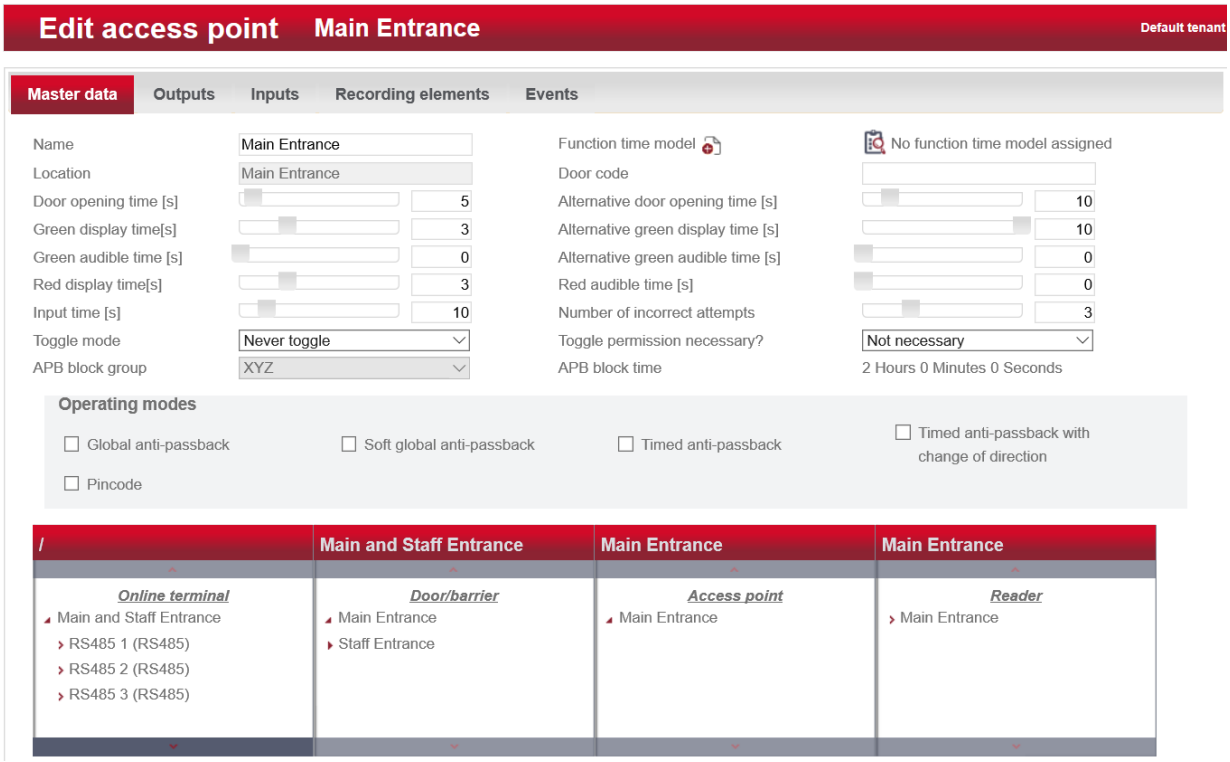
Alternatively, the editing screen for the required access point can be accessed when creating online terminals by right clicking on symbol ▸, then “**Edit**”.



732.29.430
HDE 20.12.2023

5.5.3.1. Edit the master data of an access point

Give the access point a meaningful **Name** in order to be able to clearly identify and assign it later.



It is also advisable to leave the default values set. If necessary, select a previously created **Function time profile** and a door code, if there is one.
Select the **operating modes** (**5.5.1.1.2** *Online terminal parameter settings*)

5.5.3.2. The outputs of an access point

In the “Global anti-passback” tab of the **Devices / Access point** menu, the parameters for the outputs of an access point are defined.

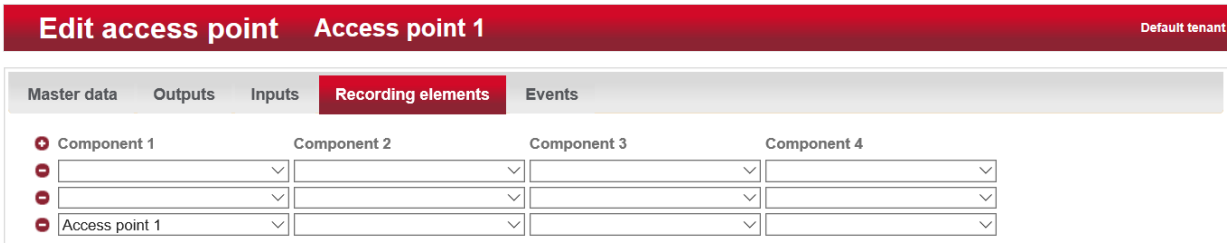
Attack output:
This function can only be used if a PIN or door code keypad is available. The output that is selected here is activated when an attack code is entered at the relevant keypad.

Output
Select the output for the attack alarming here.

Attack duration
This parameter represents the actuation time of the output relay.

5.5.3.3. Recording elements of an access point

The parameters for the recording elements of an access point are defined in the "**Recording elements**" tab of the **Devices/Access point** menu.



Dialock can be configured to only allow a door to be opened using several **Components** (up to four horizontal components).

Example:
Component 1 = reader
Component 2 = keypad
The door therefore only opens if a valid transponder and a valid code have been recorded.

A biometric system could be added as the 3rd component, for example. In this case the door would not open unless all 3 components were correctly operated.

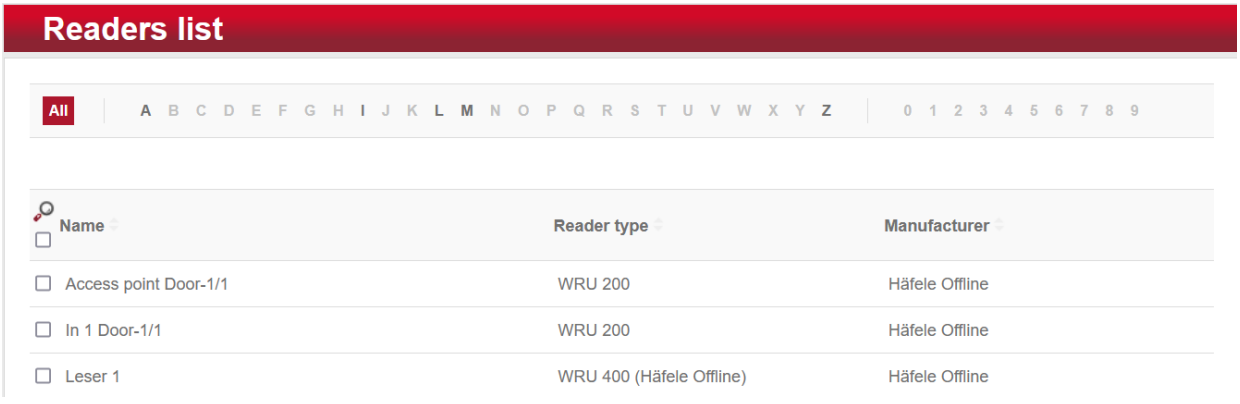
In the **Vertical**, **"OR" components** can be inserted, i.e. a door would only open if a valid transponder or a valid code was entered.

5.5.3.4. Events at an access point

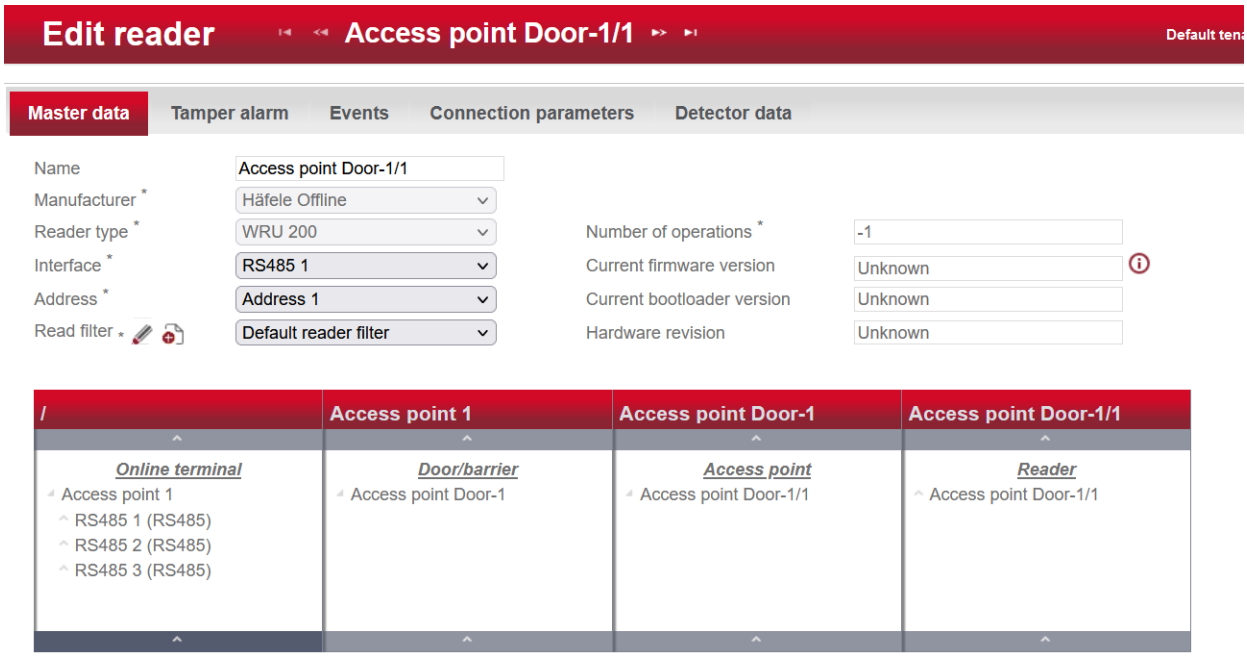
In the "**Events**" tab of the **Devices / Access point** menu, events that have occurred at the access point can be filtered and listed according to date, event type and on the basis of resources.

5.5.4. Readers without / with smartphone key

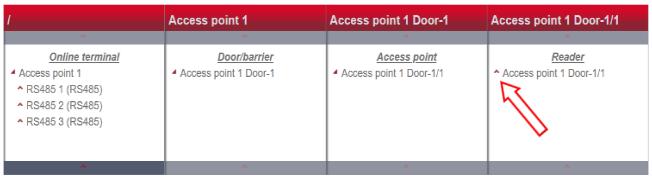
The **Devices / Readers** menu takes you to the **Readers list**. All registered readers are visible here.



Selecting a reader takes you to its editing screen.

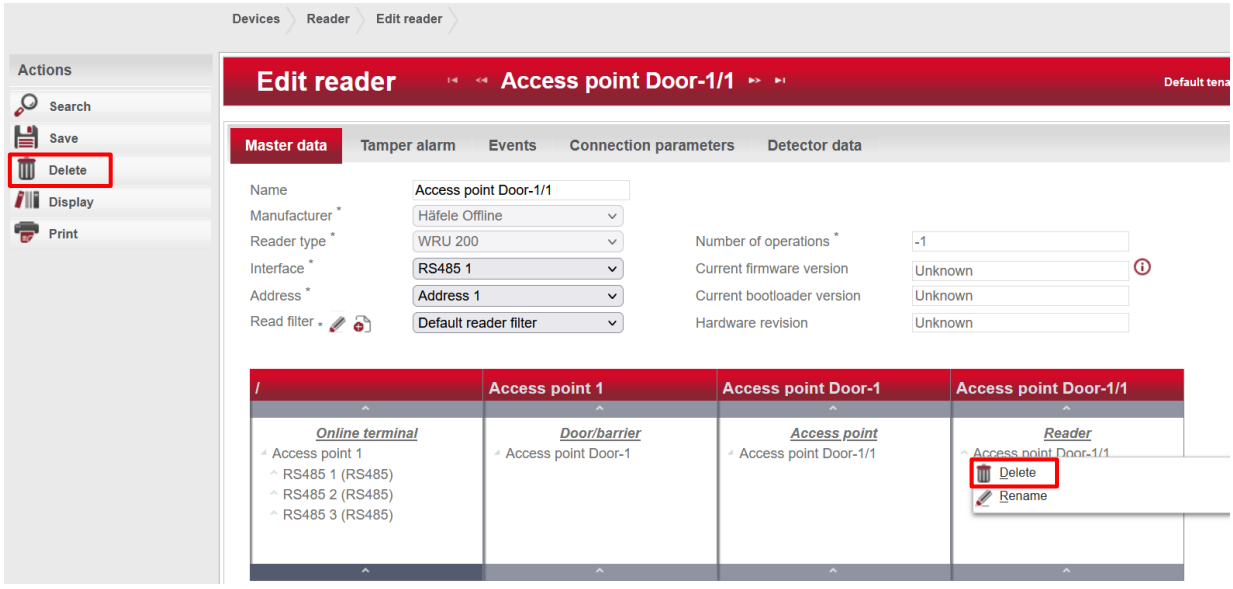


Alternatively, the editing screen for the required reader can be accessed when creating online terminals (in the hierarchy structure) by right clicking on symbol ▸, then **“Edit”**.

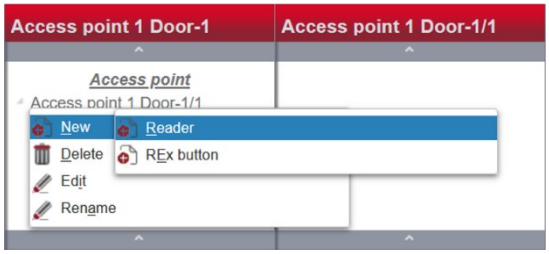


5.5.4.1. Edit the master data of the readers

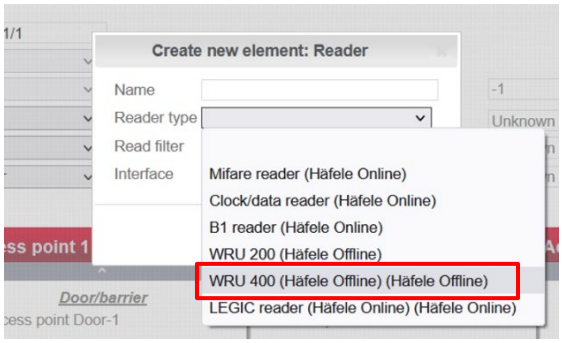
Give the reader a meaningful **Name** in order to be able to clearly identify and assign it later. The **Manufacturer** and the **Reader type** have already been defined during terminal creation. In order to **Modify** the reader type, the entire reader must be deleted (via the action menu on the left-hand side of the screen or by right-clicking on the reader in the hierarchy structure) and a new reader with the desired reader type created.

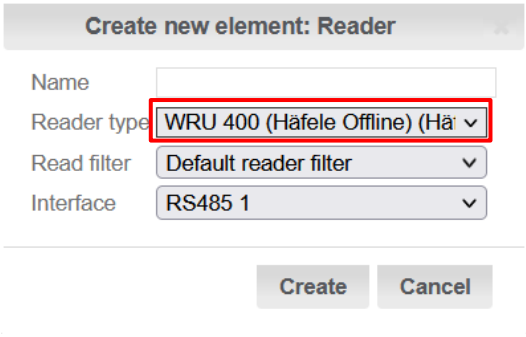


You can create a new reader by right-clicking on the access point.



The input field "**Create new element: Reader**" opens.





If a reader is to be used with an electronic key via smartphone (smartphone key), alternatively to the transponder, the reader "WRU 400" has to be selected in the drop-down list of the **Reader type** field. Only this reader has a Bluetooth (BLE) interface, which is required for this function.

Note:
BLE = Bluetooth Low Energy

The "**smartphone key function**" also has to be activated in the "Connection parameters" tab. (**5.5.4.4** *Connection parameters of the readers)*

Select the required **Interface** from the drop-down menu.

If several readers are connected to the same interface, the **address** of the respective reader must be coordinated with the interface. The default address is address 1.

The **read filter** defines how the read data of the medium is composed into a transponder ID (**5.5.9** *Read Filter)*

5.5.4.2. Tamper alarm signal for readers

In the "**Tamper alarm signal**" tab of the **Devices / Readers menu**, you determine the **Output** from the drop-down menu for the tamper alarm signal and determine the **Alarm duration**.

5.5.4.3. Events at readers

In the "**Events**" tab of the **Devices / Readers** menu, events that have occurred at the access point can be filtered and listed according to date, event type and on the basis of resources.

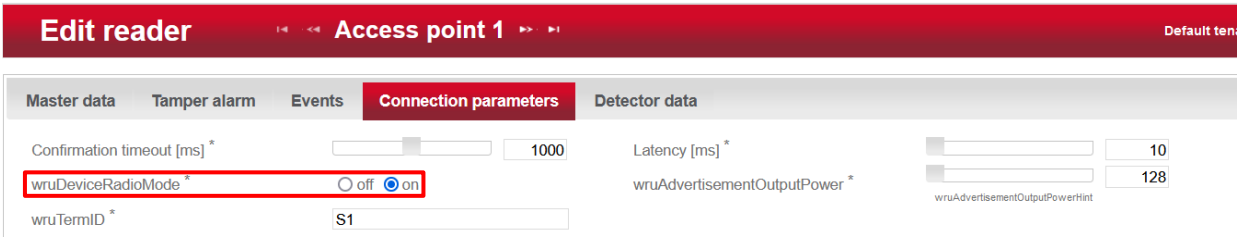
5.5.4.4. Connection parameters of the readers

The parameters for the connection between the reader and the online terminal are defined in the “**Connection parameters**” tab of the **Devices / Readers** menu.

Confirmation timeout determines the time for which the online terminal waits for the response from the reader in milliseconds.

The **Latency** in milliseconds describes the delay until the controller processes the next address on the interface. This delay is used to distribute the performance of the WTC 200 on the interface.

If you want to use the **smartphone key function**, select the button “on”.
This setting activates the smartphone key function with Häfele SDK.



If this option is not displayed, the wrong reader type has been stored. In this case, the reader must be completely deleted and re-created.

The **output power** of the Bluetooth advertisement can be set here. It is preset to the highest range at 128.

You enter a designation (max. 20 characters) for the Bluetooth identifier under **TermID (advertisement)**.

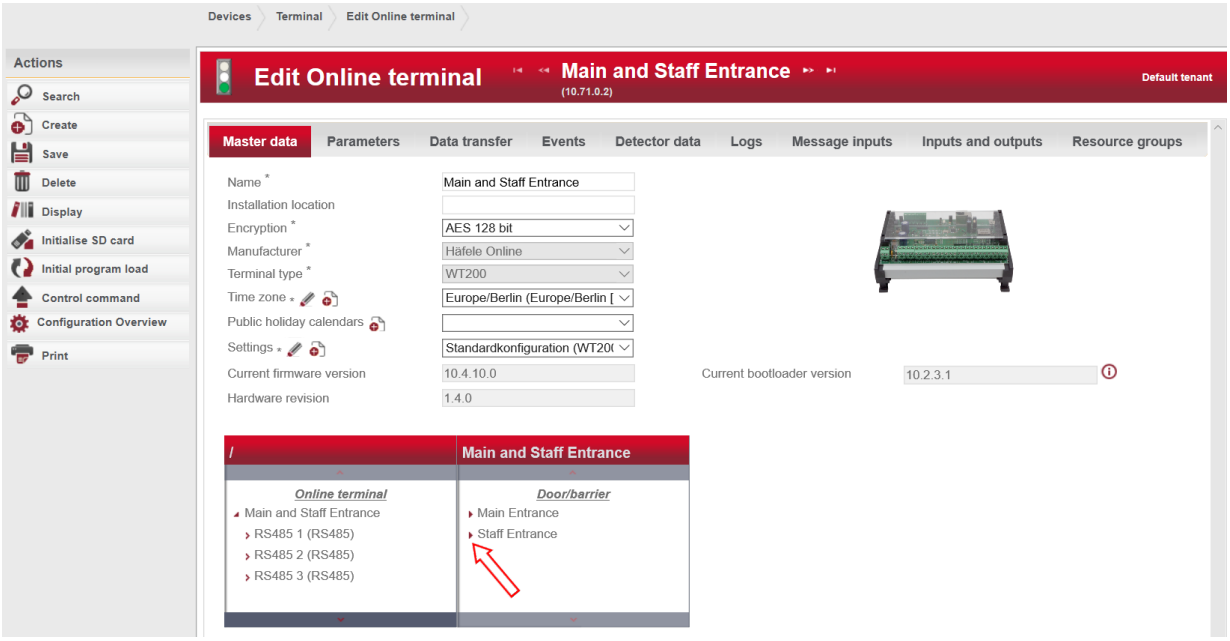
5.5.4.5. Reader detector data

The temperature and voltage values of the last 7 days can be queried in the “**Detector data**” tab of the **Devices / Readers** menu. The values are graphically displayed and can be displayed per day. Provided that the display thereof has been activated previously in the “**Transactions**” tab in the **Devices / Device settings** menu of the required terminal.

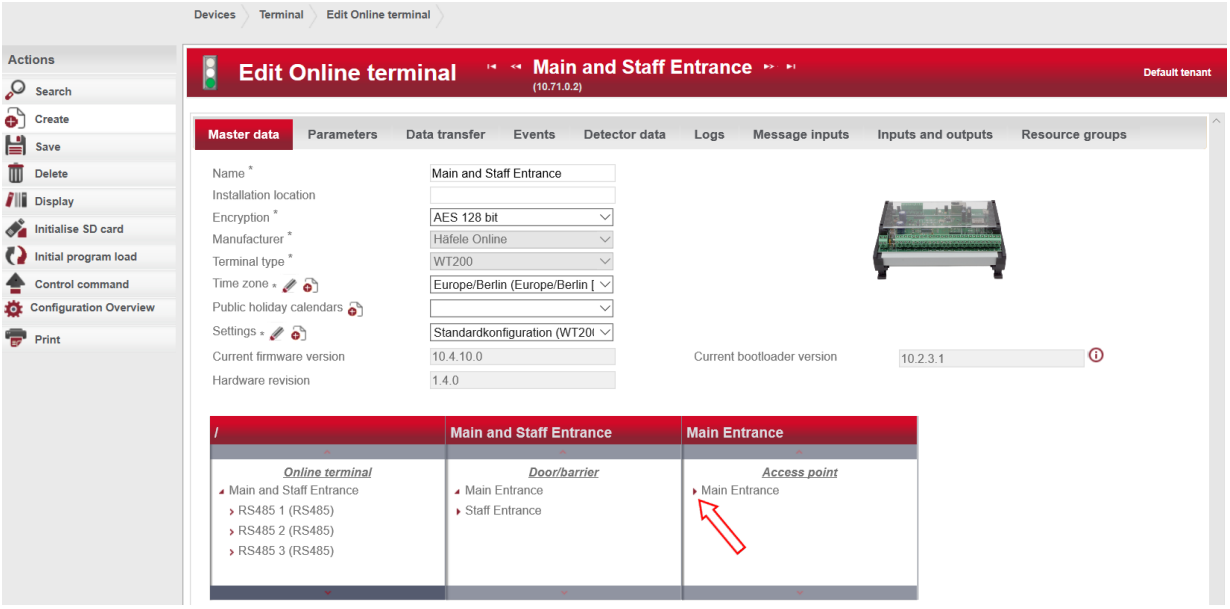
5.5.5. REx button

The **Devices / REx button** menu takes you to a list of created REx buttons.

To create a REx button, select the relevant online terminal in the **Device / Terminal** menu and access the editing window.



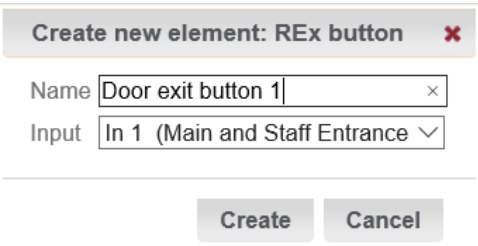
In the **Door / Barrier** window, the other **Access point** window is opened by clicking on the symbol ▸.



By **right clicking** on the symbol ▸ and selecting **NEW / REx button**, you can now create a REx button.

732.29.430
HDE 20.12.2023

The input field opens
“Create new element: REx button”

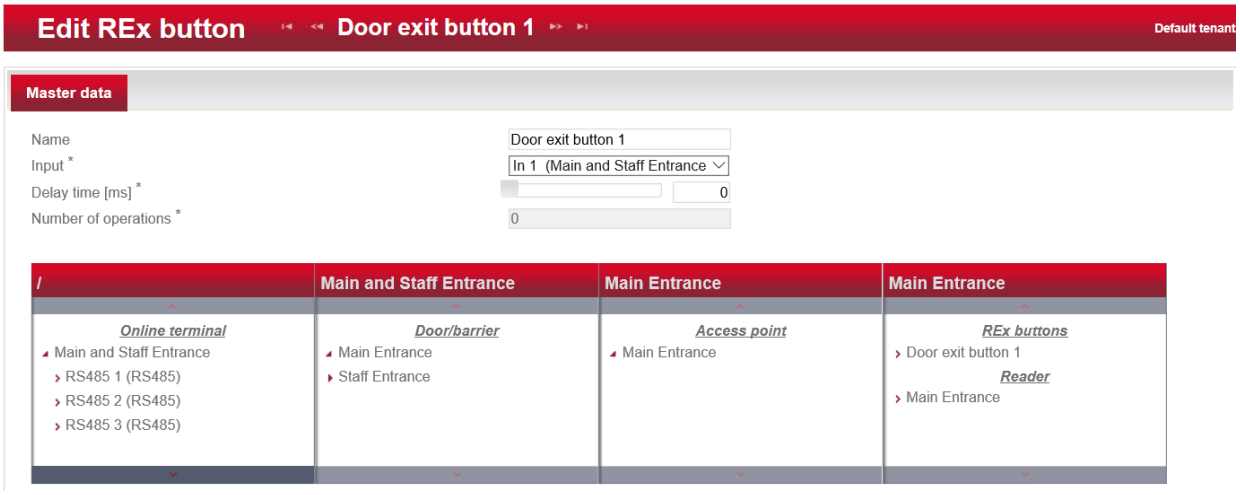


Give the REx button a meaningful **Name** in order to be able to clearly identify it later. Select the **Input** of the controller to which the REx button is connected using the drop-down menu.

By selecting the REx button in the **REx button list** in the **Device / REx button** menu, the REx button can be edited.

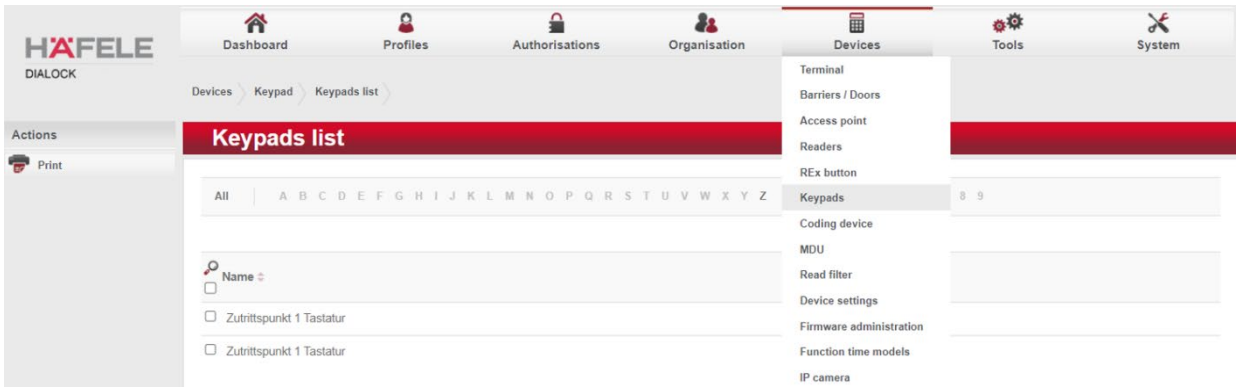
If necessary, you can set a delay for switching the REx button under a **Delay time**, for example.

The **Number of operations** shows how often the REx button has been used (numeric).

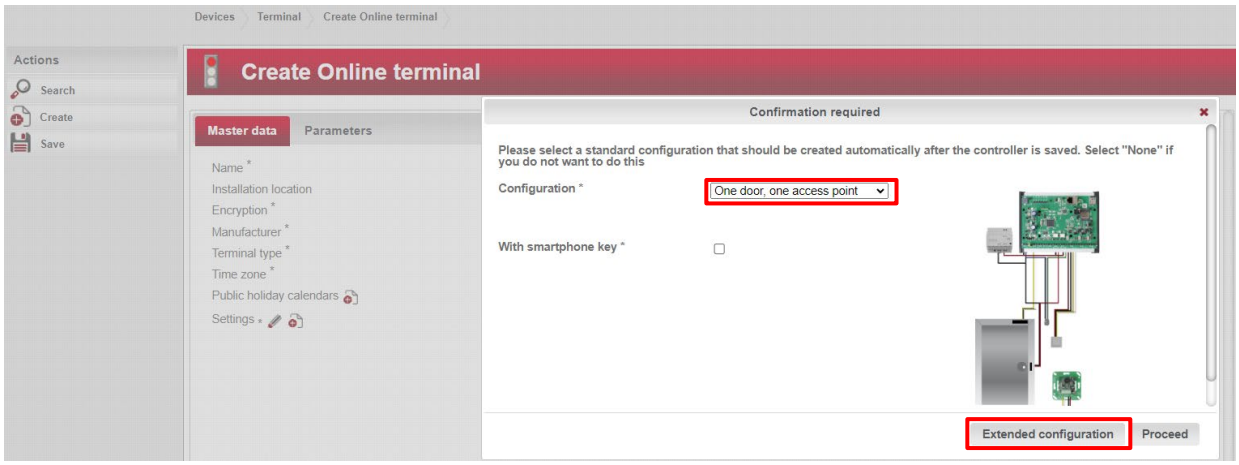


5.5.6. Keypads (PIN-Code reader)

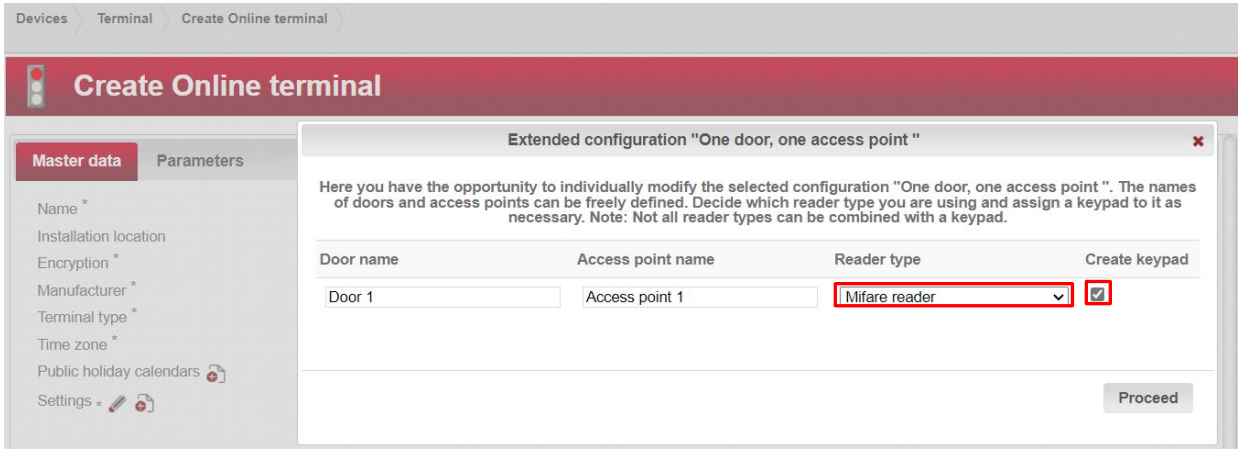
The **Keypad List** is accessed using the **Devices / Keypad menu**. All recorded keypads are visible here.



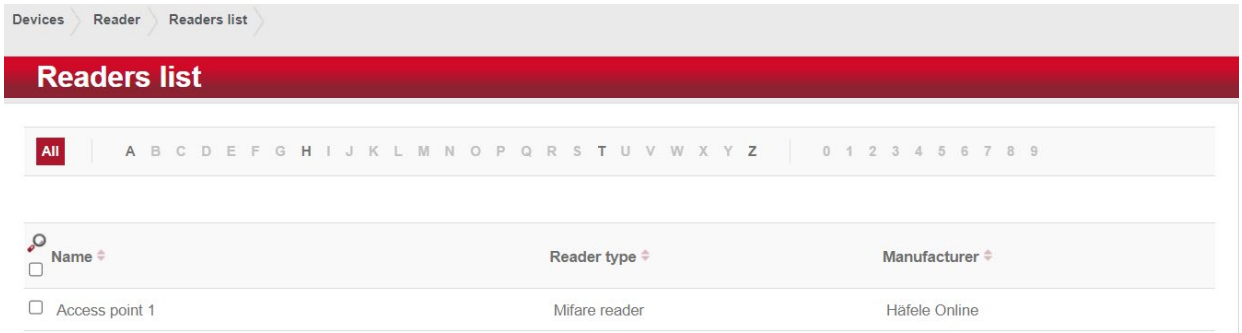
To create a keypad, proceed as described in **5.5.1.1.1** .*Record Online Terminal / Master Data*.



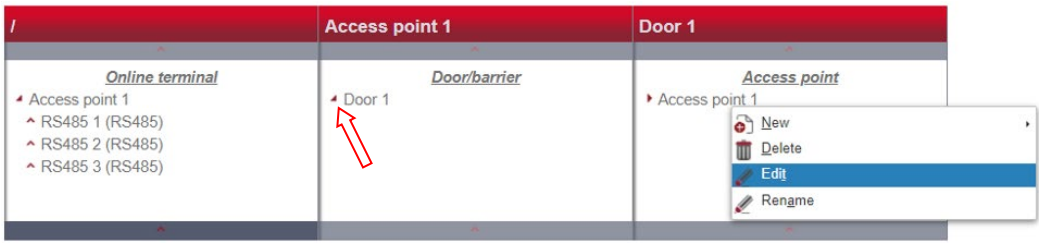
After selecting the required configuration, select the reader type “**Mifare Reader**” that is required for a keypad under “**Extended Configuration**” and activate the check box for “**Create Keypad**”.



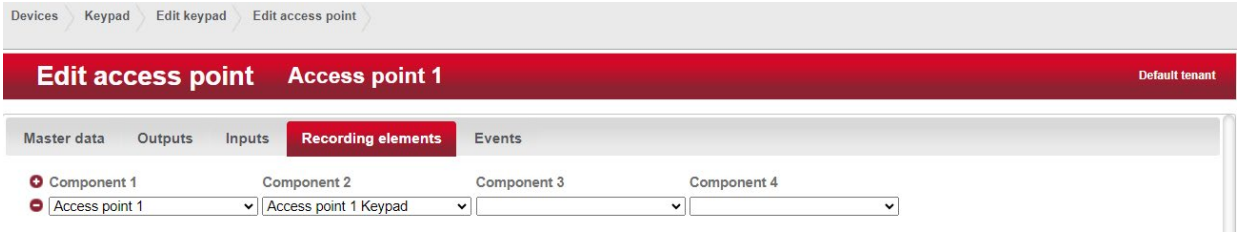
Complete the procedure with "**Done**”. The keypad is now visible in the keypad list.



Now open the hierarchy structure by clicking on the ▸ symbol until the access point can be selected.

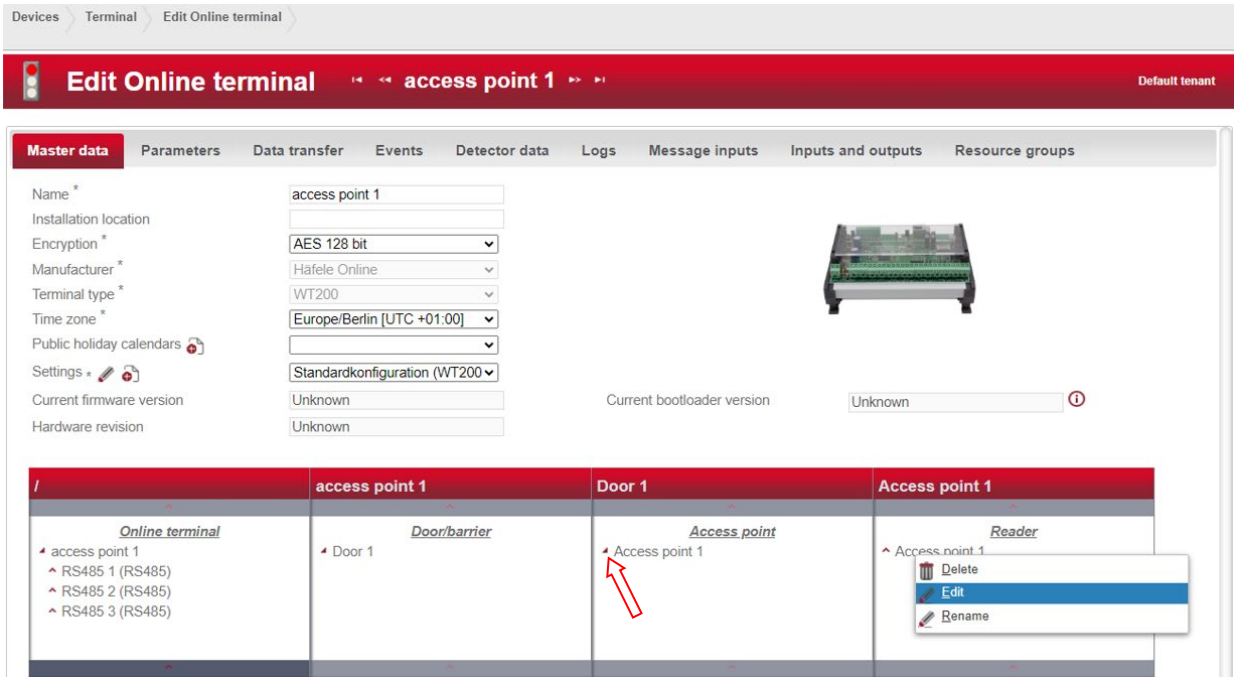


The access point can be edited by right clicking on it. Select the “**Recording Elements**” tab.



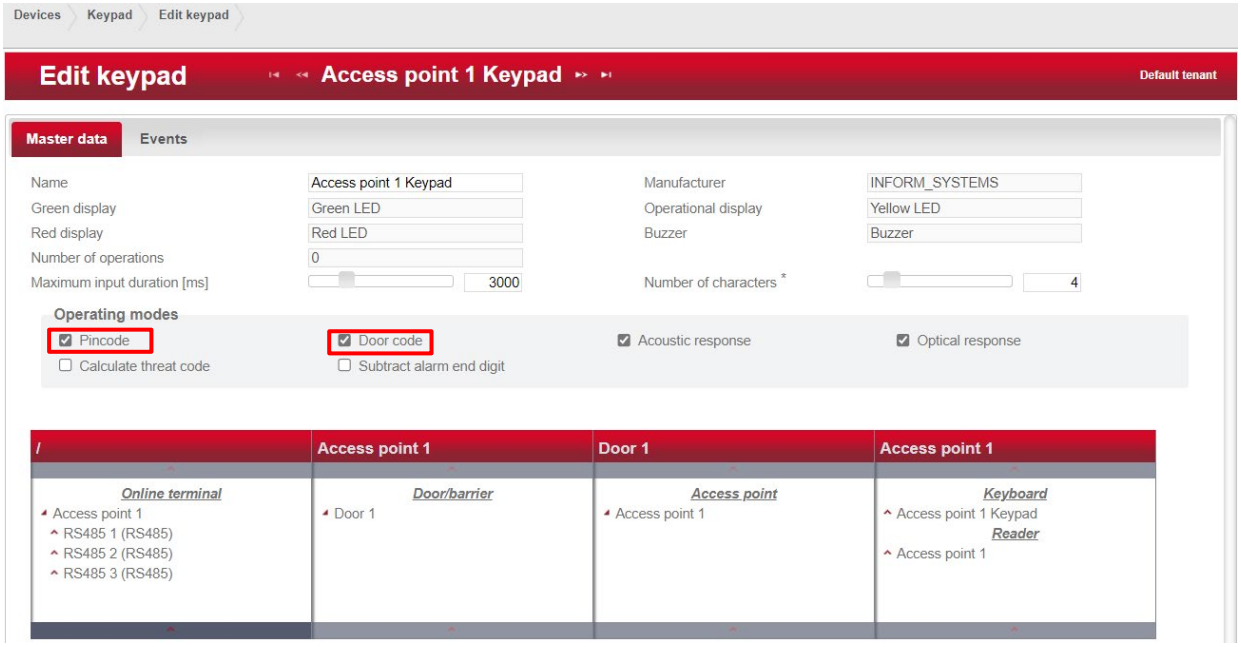
The components that are used (reader / keypad) and the order for performing the authentication can be selected here.

Now open the hierarchy structure further by clicking on the ▸ symbol until the keypad can be selected.



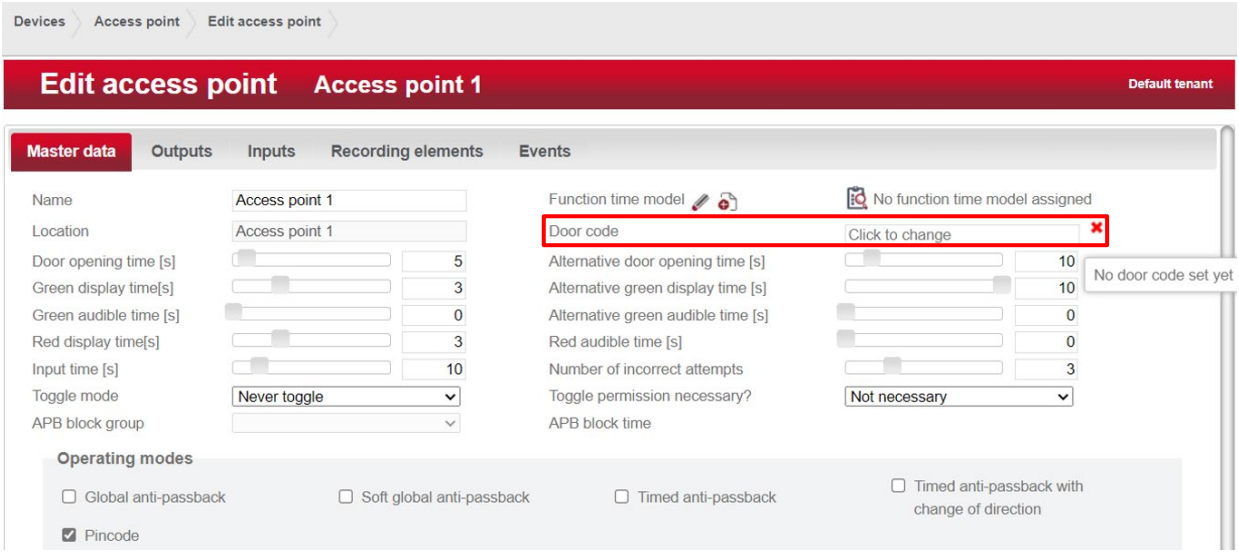
The keypad can be edited by right clicking on it.

You can set the operating modes for the keypad in the keypad master data.



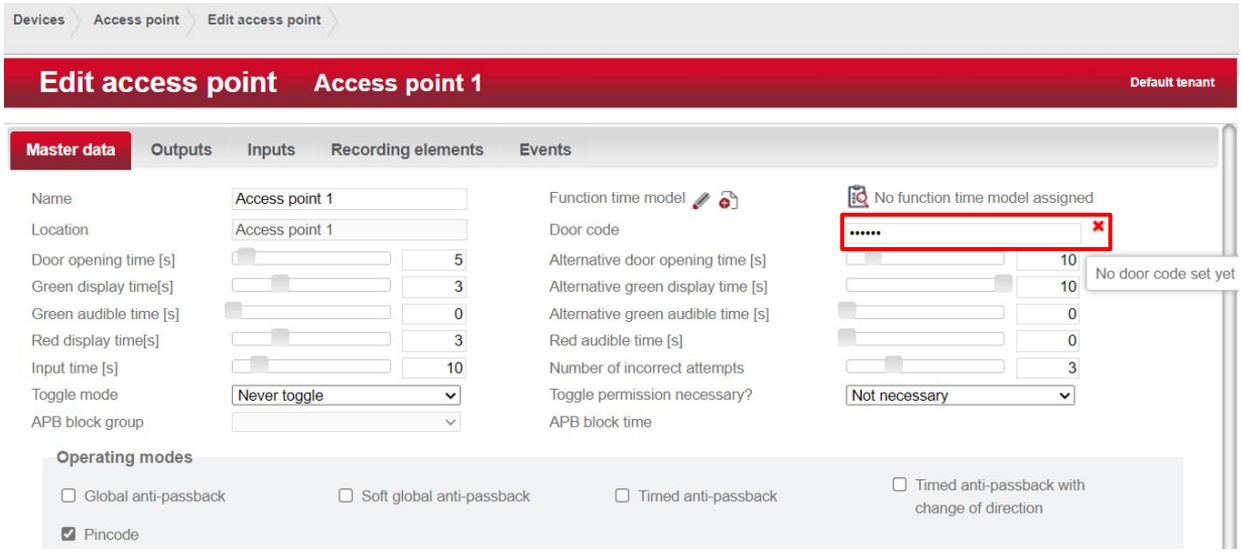
The **PIN Code** is person-specific, and is generated for the person in the **Profiles / Persons** menu in the "**Identification Characteristics**" tab (**5.2.1.5** *Identification Characteristics*).

The **Door Code** is valid for all persons who use the door and is allocated in the master data of the access point.

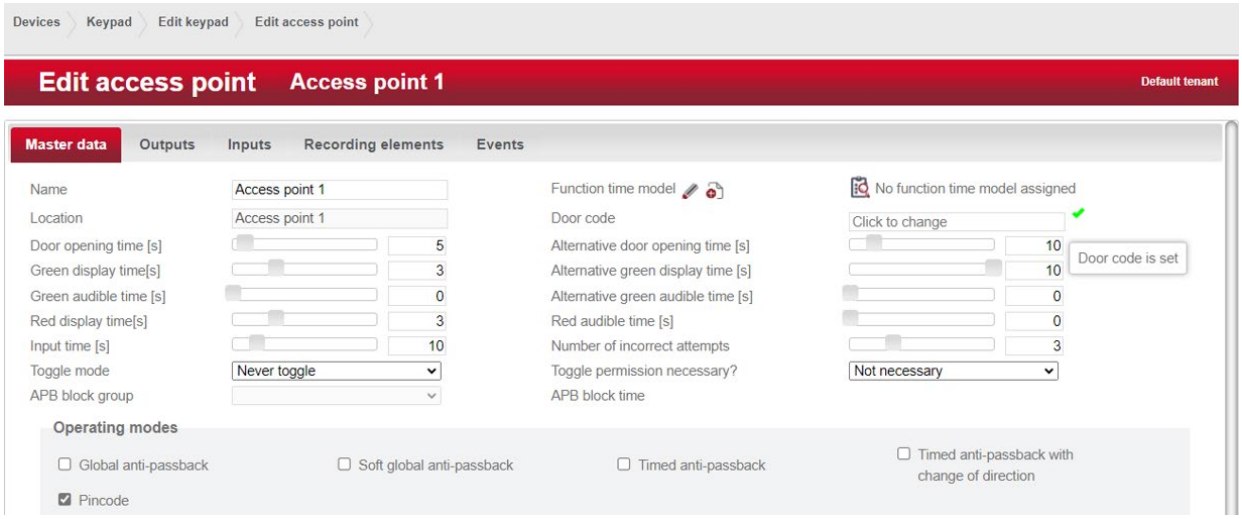


A door code can be defined by clicking in the relevant field and entering a sequence of digits.

732.29.430
HDE 20.12.2023



The door code is set by saving in the action field on the left. This must be forwarded to the persons manually.



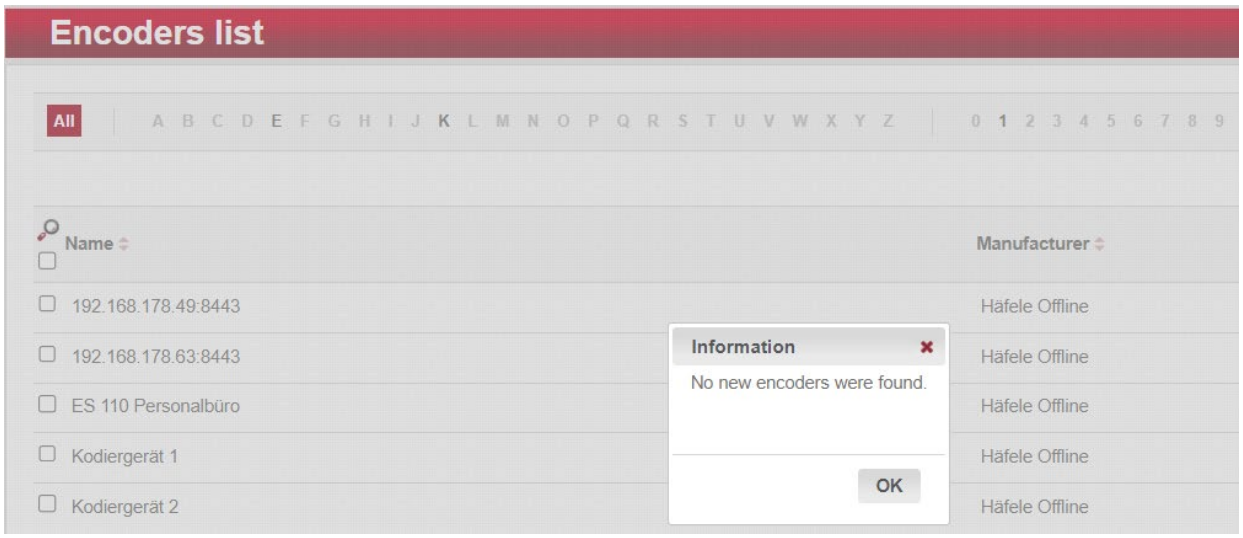
When a new digit is entered and then saved, an existing door code can be overwritten.

The length of the door code can be set in the **System / System Configuration** menu in the **Access Control** tab (**5.2.1.5** *Identification Characteristics*).

5.5.7. Encoding device (Encoder ES 110)

The **Devices > Enoding device** menu takes you to the encoding devices. To create a new encoding device, click on “**Create**” on the left-hand side of the screen.

To link to a connected encoding device, click on “**Find encoder**”.

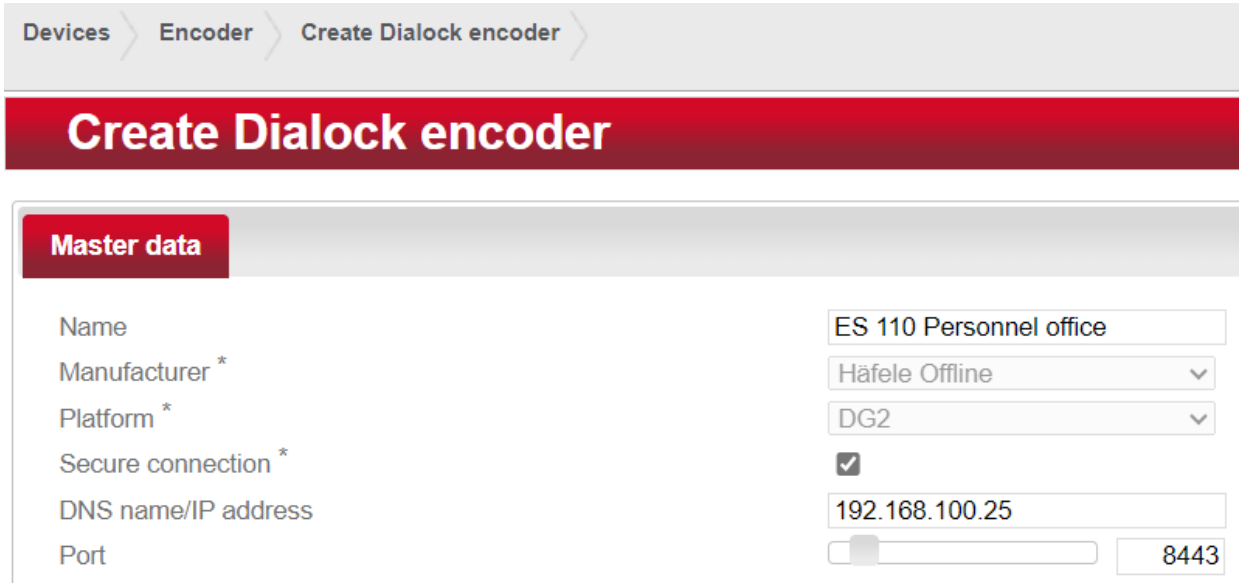


Give the encoding device a unique **Name** in order to be able to clearly identify it later.

The “**Secure Connection**” option is preset for security reasons.

In the “**DNS name/IP address**” field, specify the DNS name that is valid for the PC or the IP address of the encoder.

The associated port number should be entered in the “**Port**” field, and for a secure connection the default port “**8443**” should be used.



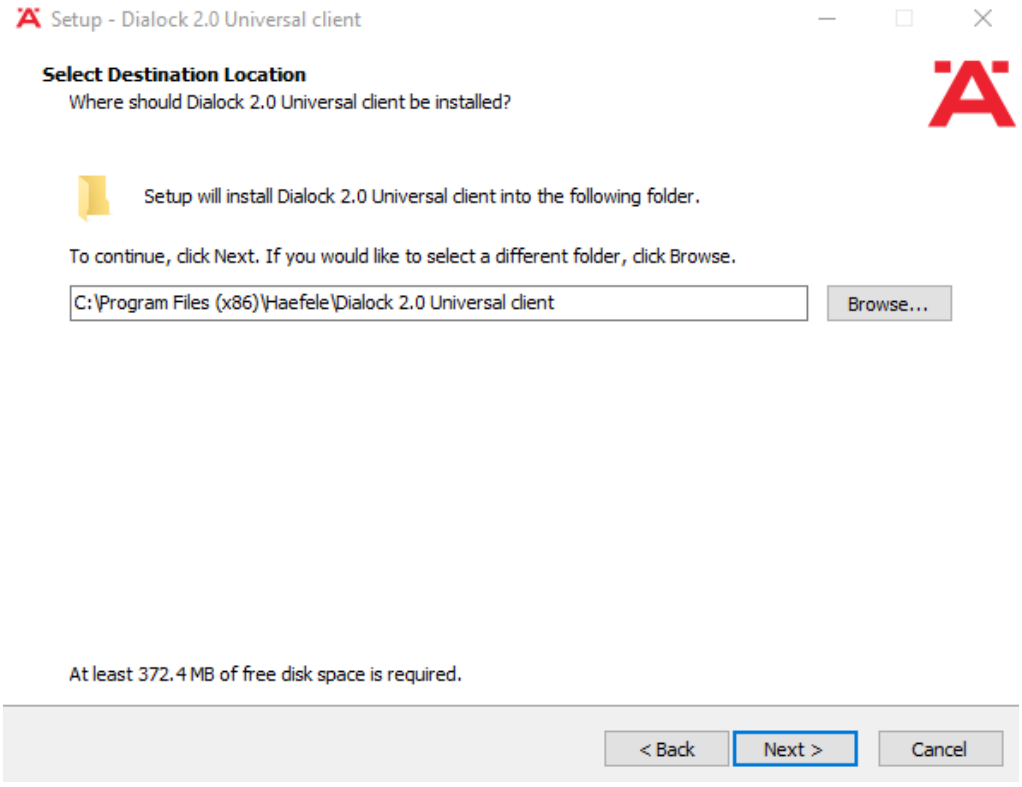
The encoding device is now ready to write the authorisations of a person to a transponder.

5.5.8. MDU 110 / Universal Client

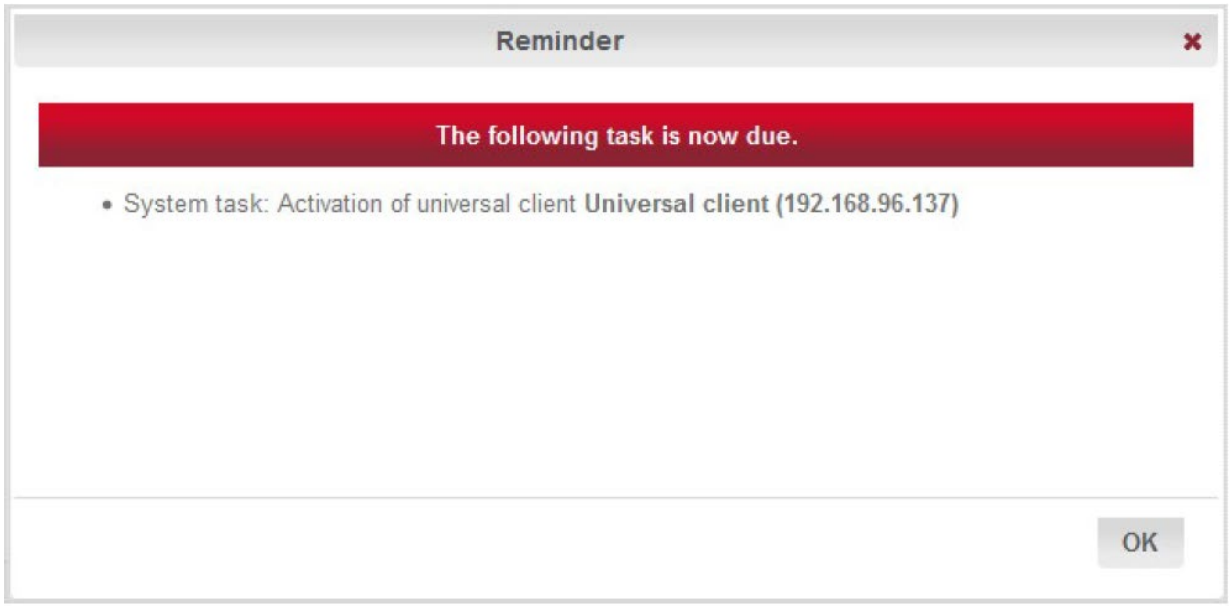
For exchanging data between Dialock 2.0 and the MDU 110, a dedicated program with a set-up has been created which can be downloaded via the web interface and installed.

The set-up programme for installing the client software can be downloaded directly on the MDU list screen in Dialock 2.0 by clicking on the “Install client” button. Since the programme has to be provided with parameters and packed by the system, the download can take several seconds.

The ZIP archive must be extracted into a temporary folder in order to then execute the setup.exe program. The set-up checks whether a 32-bit Java run-time environment is available and installs it if necessary. Then the Dialock 2.0 Universal Client software is installed, which runs in the background without a user interface.

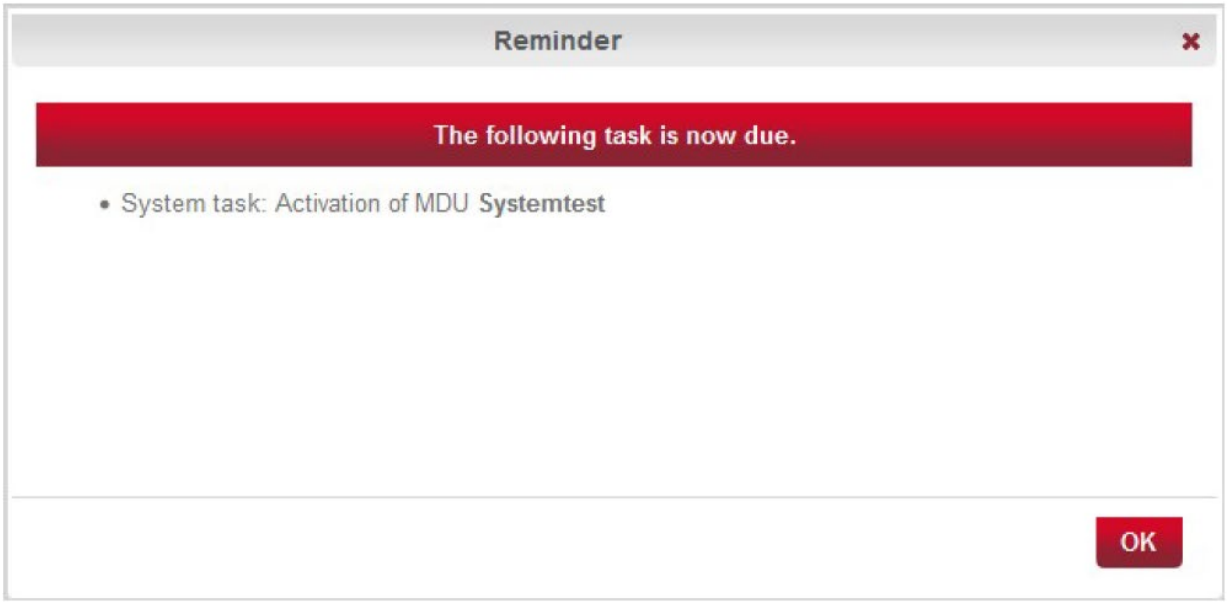


When installation is complete, the Universal Client registers itself with Dialock 2.0 and is blocked to begin with. The system creates a user task for activating the client services, similar to activating replaced hardware or a new SD card for a terminal. Only when this task has been carried out and the Universal Client has been unlocked, can it be used in the system.



The Universal Client is designed to search for any MDU 110 that is connected to your computer. No coupling to a specific MDU 110 takes place!
In other words, if you connect an MDU 110 to the computer on which you have installed the Universal Client, it will detect it after a short time. If the MDU 110 is still unknown to the system (serial number and / or public key unknown), a system task for activating this MDU 110 will also be generated. This is intended to prevent arbitrary devices from being used as an MDU 110 on the system.

Perform the task to make the MDU 110 available.

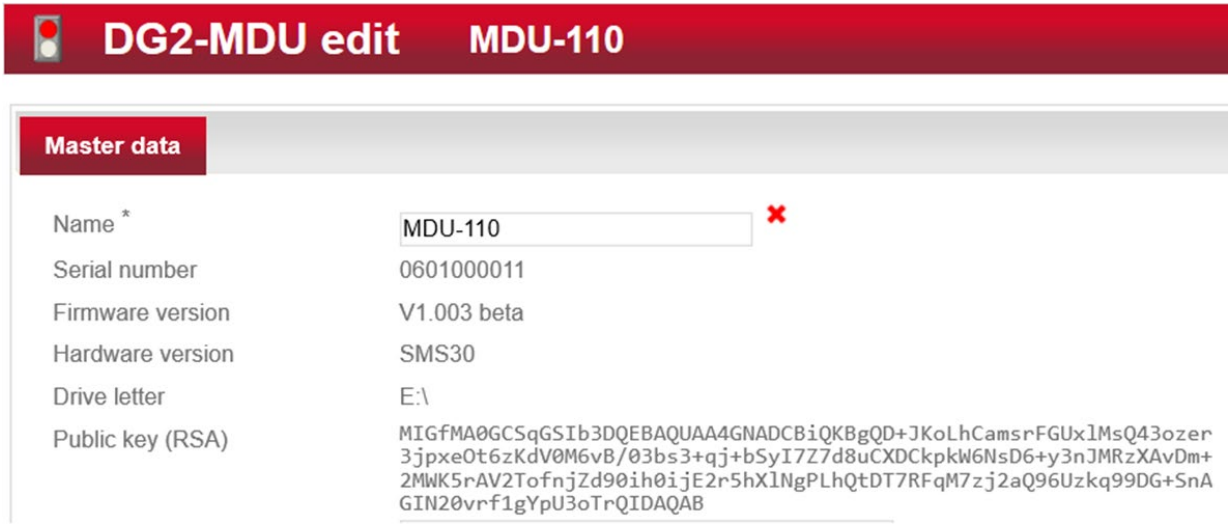


732.29.430
HDE 20.12.2023

The MDU 110 appears in the MDU list after it has been recognised, regardless of whether you have already enabled it or not.

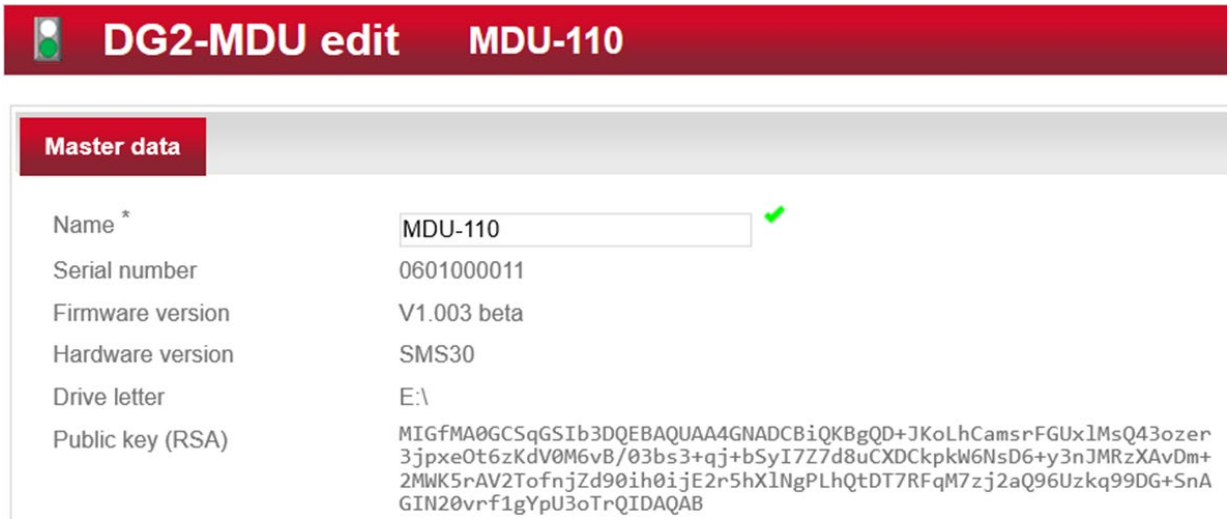
Call up the data record to find out more details about the MDU 110.
The traffic light icon in the header line of the MDU screen shows the status of the connection to the client software.

A red traffic light signals that the client software is not connected to the server or the MDU 110 is not connected.



In this case, check whether the Windows Services has been started and an MDU 110 is connected.

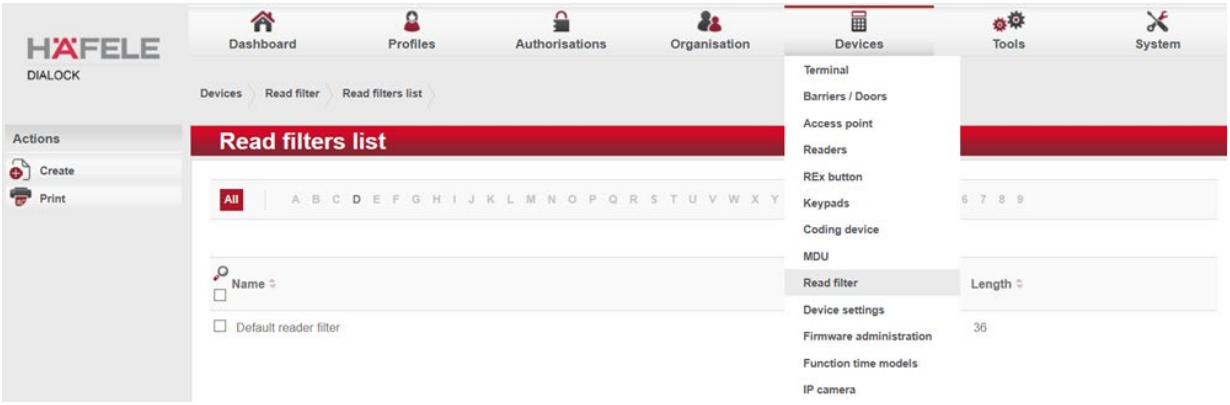
A green traffic light indicates that everything is running properly and the relevant MDU 110 can be addressed correctly. This means that you can use it immediately.



You can immediately see whether an MDU 110 has already been activated/unlocked or not via the information icon behind the device designation (red cross or green tick).
When you have carried out the task which activates the MDU 110, these are displayed differently accordingly.

5.5.9. Read filter

In the **Devices/read filters menu**, you can call up and edit the read filters in a **Read filter list**.

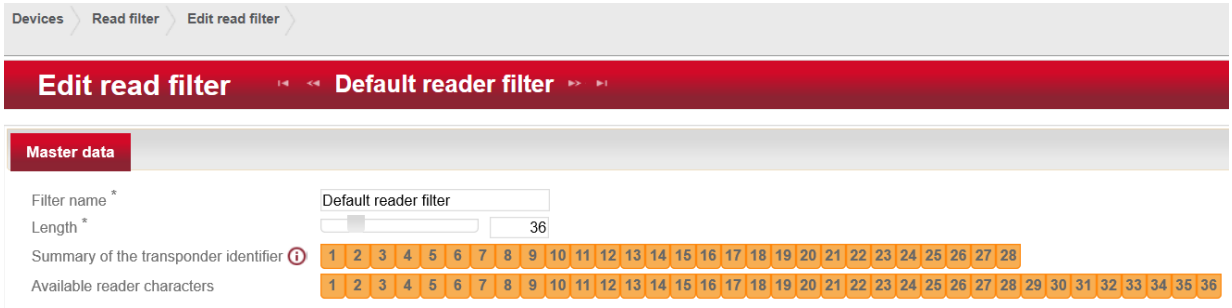


You can create new read filters using the “**Create**” button in the left-hand action bar.

Give the read filter a meaningful **Name** in order to be able to clearly identify and assign it later.

You can individually determine the **transponder number composition** from a defined group of numbers. This is determined using the **Length** field. The group of numbers and the available reader characters are graphically displayed under **Available reader characters**.

In order to now assign these to the required area of the transponder, drag the required number from "**Available reader characters**" with the mouse button held down to the required location of the **transponder composition**. Please note that all locations of the transponder composition have to be occupied.



Note:
These settings are only made when using systems from other providers, and must be made by trained technicians.

Reader buffer
This represents the storage space that is reserved for the group of numbers to be read out.

The **Number of operations** shows how often the reader has been used (numeric).

5.5.10. Device settings

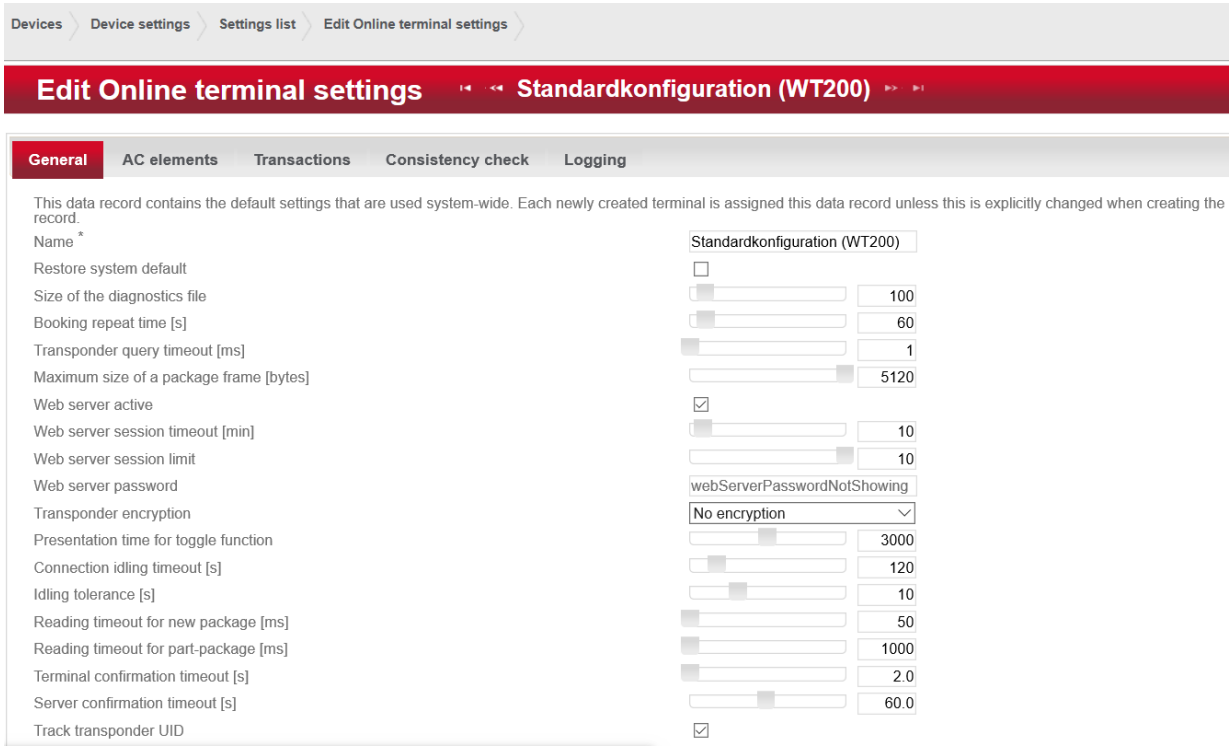
The setting list is accessed via the **Devices > Device settings** menu.
When one of the terminals listed here is selected, its settings can be edited.

Attention: These default settings must only be changed by a system specialist.

Online terminal

5.5.10.1. Online terminal / general

Here you can make your own settings which differ from the standard terminal settings and save them individually.
To do this, click on the "**Create**" button in the left-hand action bar.



Name:
Enter the name that you require for the settings here.

Restore system default:
Activate this check box and click on “Save” to restore the system defaults.

Size of the diagnostic file:
This parameter is used to define the size of the two diagnostic files. System diagnosis messages and notes are saved on the SD card in the diagnostic file (diag1.txt). Dialock manages up to two files. If the first file reaches its maximum size, it is renamed diag2.txt and a new diag1.txt file is created. This means that two diagnostic files are always available for system analysis.

Booking repeat time:
This is the waiting time for confirmation from the host system during TCP/IP communication for a transmitted data record.

Transponder query timeout:
Currently not used.

Maximum size of a package frame:
The length of the communication package between the terminal and the host can be set here. 5120 bytes is recommended as the optimum size.

Web server active:
The web server in the WTC200 can be activated here. Then the device can be accessed directly via a web browser for diagnosis purposes.

Web server session timeout:
The session is terminated automatically after this time in minutes.

Web server session limit:
This is the maximum number of sessions that can be connected simultaneously. The recommended minimum number of sessions that can run simultaneously is two.

Web server password:
This is the password with which the user can communicate with the terminal from the browser.

Transponder encryption:
This specifies the type of authentication. 3DES encryption is only possible in combination with the TIKS card. (Telekom Internal Key Service, future option).

Presentation time for toggle function
This value determines the time for which a transponder must be held in front of the terminal for it to permanently change its status from locked to unlocked or unlocked to locked.
If the time is set to 0, the function is disabled.

Connection idling timeout:
Determines the time after which the connection to the terminal is recognised as “In idle mode” if no messages have been sent from either side (terminal or server). It forces the server to send a message to the terminal so that the connection remains open.

Idling tolerance:
The terminal to server connection works using the idling principle are both ends. Since the server requires a little time to generate the Keep Alive message and send it to the terminal, the time specified here is added to the idling time at the terminal end.

Reading timeout for new package:
Time for which the terminal is in listening mode for incoming useful data telegrams. Once this time runs out, pending telegrams are transmitted to the server. This parameter influences the “graininess” of the communication.

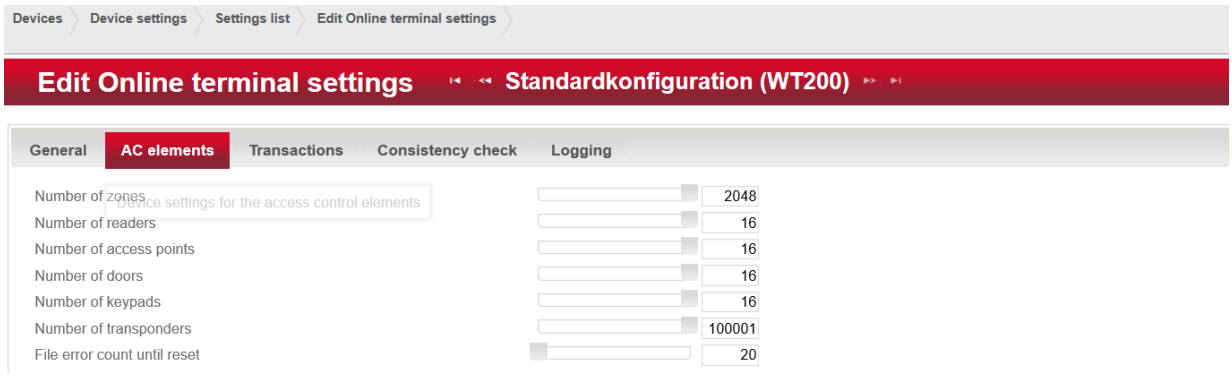
Reading timeout for part-package:
Time after which reception is regarded as failed when waiting for characters from the server

Terminal confirmation timeout:
Time for which the terminal waits for a response from the remote station after sending a package. After the time has elapsed, the package is re-transmitted.

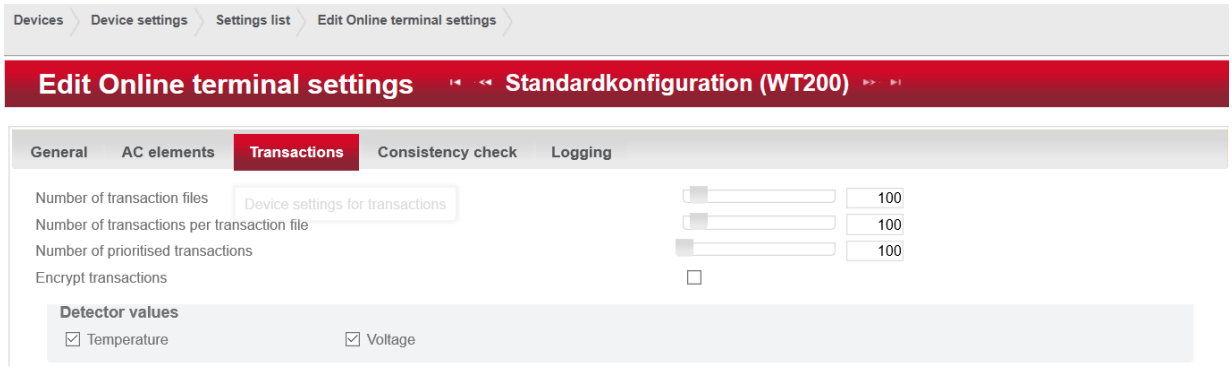
Server confirmation timeout:
Time for which the communication server waits for confirmation from the remote station after sending the package. After the time has elapsed, the package is re-transmitted.

5.5.10.2. Online terminal / AC elements

The maximum values that can be set here are licence-dependent and exclusively relate to the selected terminal. The terminal reserves its memory in accordance with these specifications, which you can change here at your discretion.



5.5.10.3. Online terminal / transactions



Number of transaction files:
The terminal always saves the transactions in several files. If the value of the transaction file is set to 0, transactions are neither logged nor forwarded. The number of transactions multiplied by the number of transactions per transaction file results in the maximum number of transactions saved in the terminal (maximum 1 million).

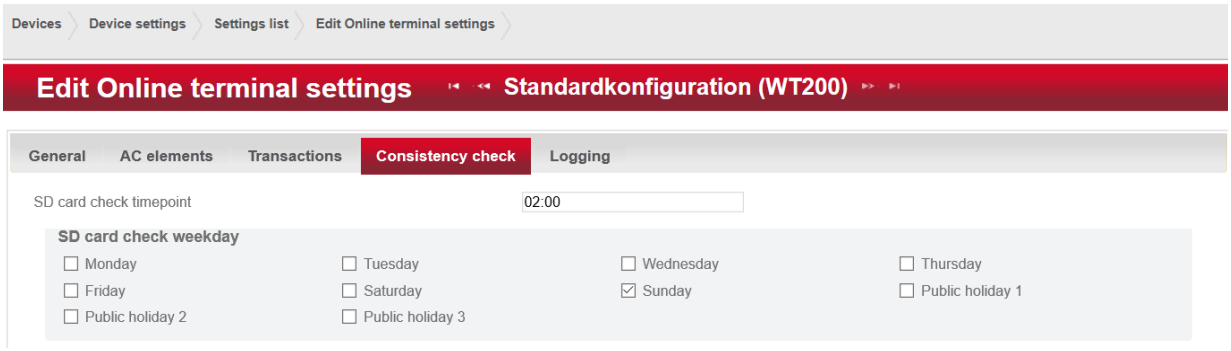
These values are used to define how many transactions are to be saved in the terminal. This is important for the offline case, when the terminal does not have a connection to the host system.

Number of prioritised transactions:
Prioritised transactions are transactions that must be sent before any others. Prioritised transactions are, for example, global anti-passback transactions, timed anti-passback transactions and system error messages.
The prioritised transactions are saved in a separate log file. The parameter specifies how many transactions are to be temporarily saved. If this parameter is set to 0, there are no prioritised transactions.

Encrypt transactions:
Activate the check box if you wish to encrypt transactions. However, encryption only takes place if the check box for "Encrypt SD card" has been activated in the “Parameters” tab of the “Devices/Terminal” menu.

Detector values:
Activate this check box if you would like to send the temperature and voltage values to the host. These values are always logged in the terminal.

5.5.10.4. Online terminal / consistency check



Time / weekday SD card check:
The days and times when the terminal (WT 200) performs an automatic check of the SD card are set here. It is advisable to enter days and times that are not during the general usage times of the device here.

Attention:
During the consistency check of the SD card the terminal cannot perform any access checking. This check can take several seconds to several minutes. If an error is found, the terminal tries to rectify it automatically. If this is not possible, the SD card may be formatted. In this case, all data would be lost. The terminal then requests a new configuration from the host system. If no host connection is available when this occurs, terminal operation is not possible.

5.5.10.5. Online terminal / logging

Here you can set which events are to be logged.

Offline terminal

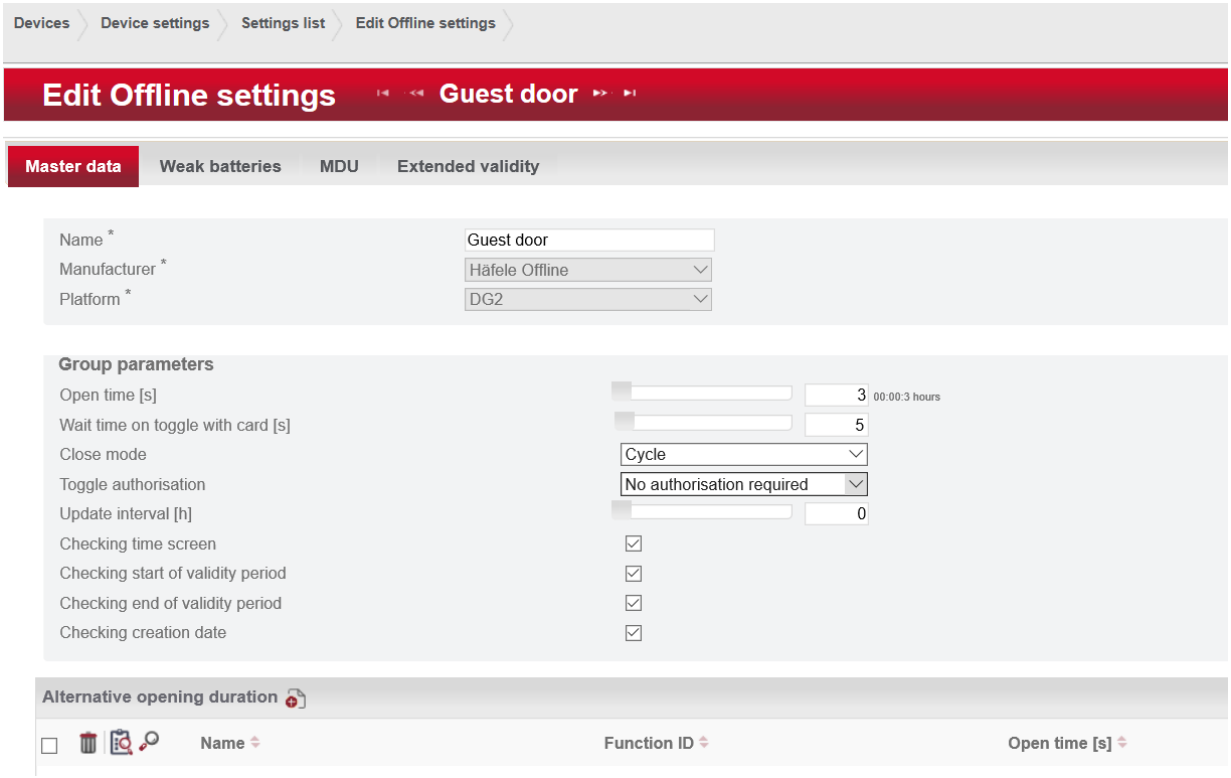
5.5.10.6. Offline terminal / master data

Clicking on the pencil icon next to parameter “**Settings**” on the “**Edit offline terminal**” screen takes you the setting level shown in the following.

Attention: These default settings must only be changed by a system specialist.

Here you can make your own settings which differ from the standard terminal settings and save them individually. To do this, click on the “**Create**” button on the left-hand side of the screen.

First select the **Manufacturer** and the **System platform**.



Open time
This corresponds to the door opening time in online mode and represents the period of time during which the door can be opened after the lock has been released using the transponder.

Wait time on toggle with card (transponder)
This value determines the time for which an identifier (**transponder**) must be held in front of the terminal for it to permanently change its status from locked to unlocked or unlocked to locked.
If the time is set to 0, the function is disabled. The toggle function corresponds to the “Latch lock” function.

Close mode
The close mode can be set to “Toggle” (latch lock function) or “Cycle” mode, i.e. lock cycle mode (spring bolt lock function). With “Toggle with card” the function can be initialised using privileged **transponders**.

Toggle authorisation
“**Unlocking and locking**”, “**Unlocking only**” or “**No authorisation required**” can be selected for the toggle authorisation.

Update interval
Here you can set the update interval for the authorisations to the nearest hour. If this is set to 0, no checking of the update interval takes place. If the last time the transponder was held in front of the authorisation writer was longer ago than the update interval, access is refused.

Checking time screen
If this option is activated, the validity of the individual time model of the transponder is checked.

Checking start of validity period
If this option is activated, the terminal checks the start of validity that is programmed for the transponder.

Note:
This option cannot be combined with the checking of the update interval.
(see above).

Checking end of validity period
If this option is activated, the expiry of the transponder is checked. This time can be specified in steps of one minute (up to max. year 2032) for the transponder.

Note:
Transponders that have already expired are only cleared out of the Blacklist (list of blocked **transponders** in the terminal) if necessary if the expiry time checking has been activated.

Checking creation date
The checking of the transponder creation date can be activated or deactivated in this way.

5.5.10.7. Weak batteries

The settings governing the terminal's behaviour in the event of weak batteries can be changed here, as well as the standard settings.

5.5.10.8. MDU 110

In addition to the standard settings, settings relating to MDU authorisations can be changed here.

5.5.10.9. Extended validity

The pre and post validity time for start and end of transponder validity can be defined here. This affects whether transponders are accepted at the terminals before or after their defined validity.

5.5.11. Firmware administration

During initial installation it is not normally necessary to specify **Firmware**, since the new devices are usually up to date.

If an update is required, download the new firmware in the **Devices / Firmware management** menu.

To do this, click on “**Create**” in the overview. In the master data of the new firmware, assign a new **Designation**.

In the drop-down menu **Type** select whether it is a firmware or bootloader version.

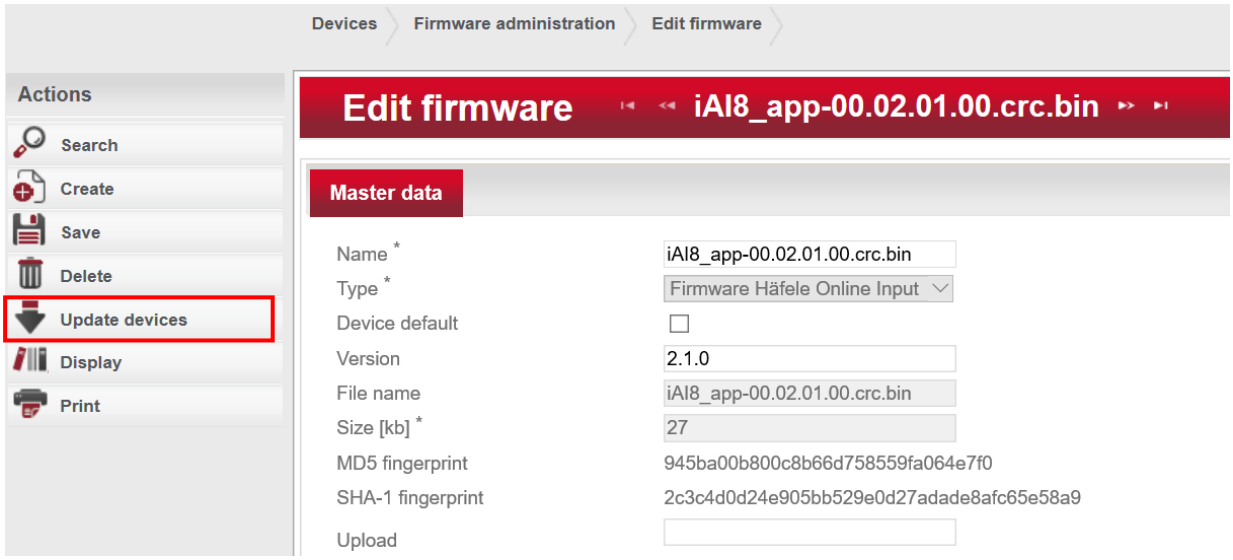
If this version is to be loaded as standard for new devices when firmware updates take place, activate the check box next to **Device default**.

Enter the new version designation under **Version**.

Dialock also assigns a unique **File name** and maps the **Size** of the firmware file.

Clicking on **Upload** takes you to the Explorer / Finder in order to select the file to be uploaded.

Save the information. Save

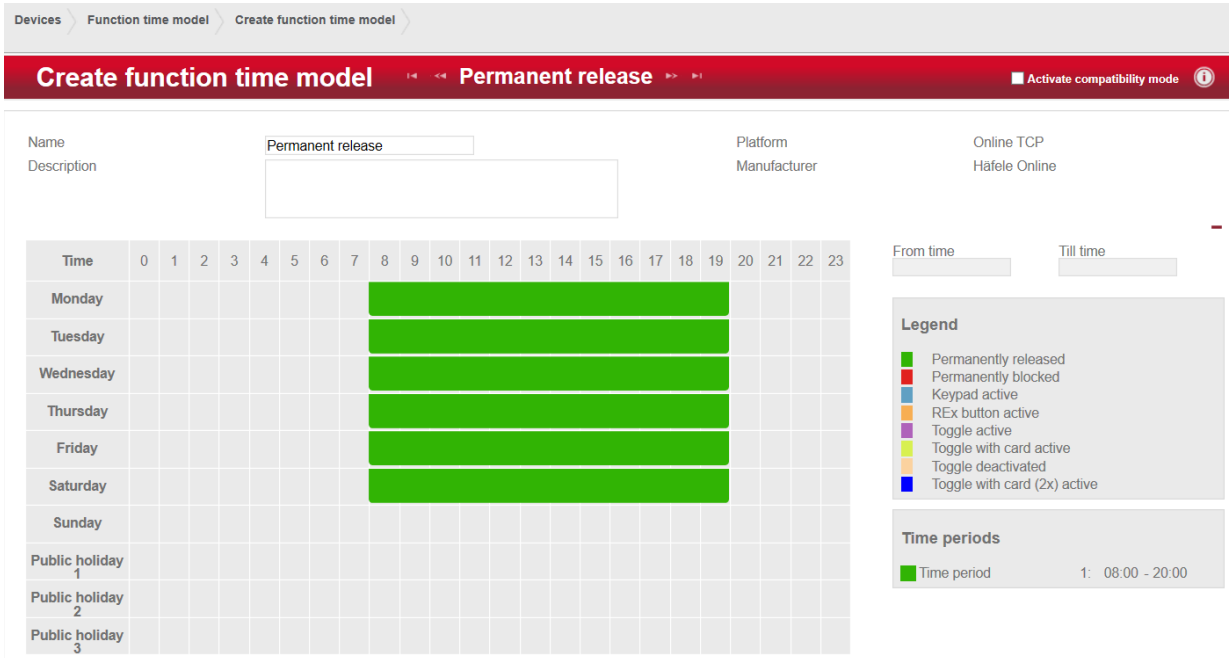


With **online terminals**, new firmware versions can be loaded into the required devices using the “**Update devices**” function.

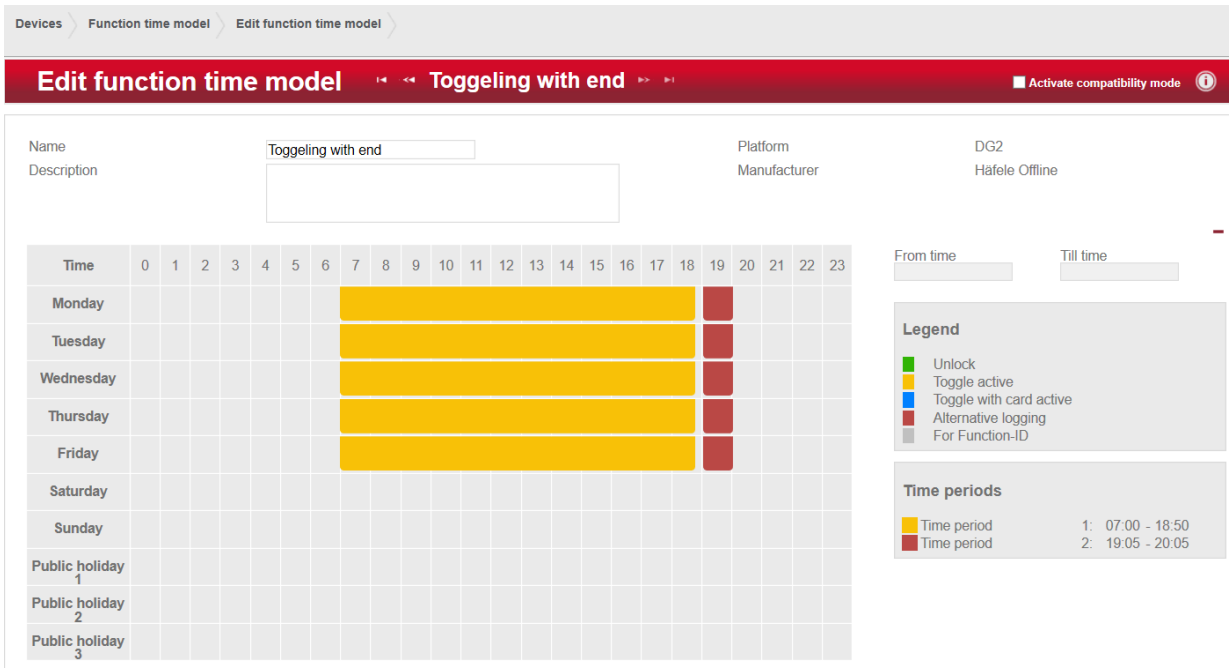
5.5.12. Function time model

You can create and edit the device-related time models in the **Devices / Function time model** menu. With function time models, a terminal automatically switches over to statuses such as unrestricted for a door/barrier at the specified point in time. This means that the terminal automatically switches on the release relay during the set time period or a keypad is activated in addition to the reader.

Select between online and offline function time model for each device during creation. Online function time models are created in the same way as online time models (**5.3.3.1**). The recording and editing of offline function time models also work in the same way as they do for the offline time models **(5.3.3.2)**.



Online function time model:



Offline function time model:

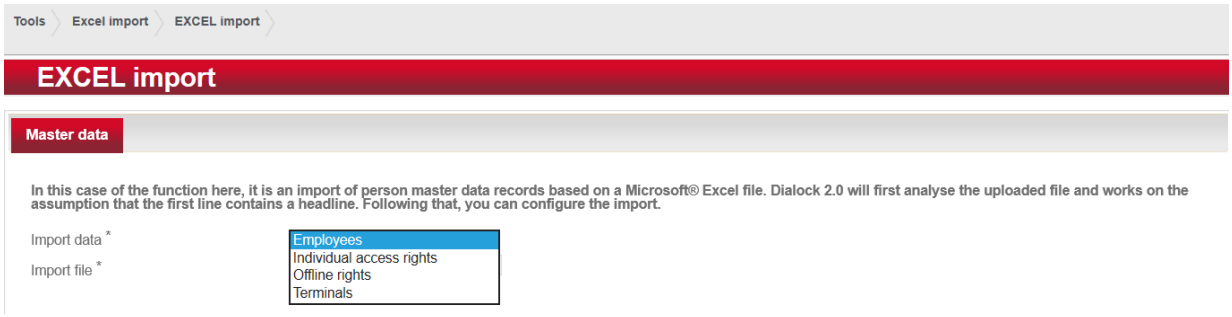
5.5.13. IP camera

Is not currently supported.

5.6. Extras

5.6.1. EXCEL® import

The import function makes it possible to transfer prepared person lists, terminal lists or authorisations to the system. Good preparation can make it considerably easier to configure the system.



Choose the required type of import data and then the Import (Excel) file.

A	B	C	D	E	F	G
Personal No	Name	Given Name	Gender	valid from	valid until	Groups
301	Baum	Peter	Mr	1.1.14 0:00		all doors
302	Müller	Hans	Mr	20.4.14 0:00	31.12.16 23:59	all doors
303	Meier	Klaus	Mr	21.4.14 0:00	31.12.16 23:59	all doors
304	Schulze	Albert	Mr	22.4.14 0:00		1st floor
305	Schmidt	Heinrich	Mr	23.4.14 0:00		1st floor
306	Schneider	Erwin	Mr	24.4.14 0:00		1st floor
307	Frei	Michael	Mr	25.4.14 0:00		1st floor
308	Burger	Christian	Mr	26.4.14 0:00		all doors
309	Engel	Stefan	Mr	27.4.14 0:00		2nd floor
310	Baum	Christa	Mrs	28.4.14 0:00		2nd floor
311	Müller	Andrea	Mrs	28.4.14 0:00		2nd floor
312	Meier	Anette	Mrs			2nd floor
313	Schulze	Lisa	Mrs			2nd floor
314	Schmidt	Maria	Mrs			lower flor, upper flor, 1st floor, 2nd floor
315	Schneider	Gudrun	Mrs			lower flor, upper flor, 1st floor, 2nd floor
316	Frei	Hilde	Mrs			lower flor, upper flor, 1st floor, 2nd floor
317	Burger	Ursel	Mrs			lower flor, upper flor, 1st floor, 2nd floor
318	Engel	Laura	Mrs			lower flor, upper flor, 1st floor, 2nd floor

Example of an employee list

Import of Offline Terminals

No. (not imported)	Area	Installation Location	Terminal ID (Only integra: max. 6 digits for MDU) possible signes: a-z, A-Z, 0-9, - _ No blanks are allowed!	Name Dialock 2: Maxium 20 digits for MDU 110	Firmware	Settings (Parameter) empty = default Terminal Parameter, New describtion = will be added to the system	Function time model (optional) Assignment according to describtion new describtion = will be added	Room zones (optional) 1 : 1: not imported will be assigned automatically n : m: values sperated by Comma	Individual Access Rights (optional) seperated by Comma	Remarks (Only informativ)
16	1	GF		130	DT 7xx DND default init.tlv	Guestroom			130	
17	1	GF		131	DT_700_DND	Guestroom			131	
18	1	1st FL		221	DT_700_DND	Guestroom			221	
19	1	1st FL		222	DT_700_DND	Guestroom			222	
20	1	1st FL		223	DT_700_DND	Guestroom			223	
21	1	1st FL		224	DT_700_DND	Guestroom			224	
22	1	1st FL		225	DT_700_DND	Guestroom			225	
23	1	1st FL		226	DT_700_DND	Guestroom			226	
24	1	1st FL		227	DT_700_DND	Guestroom			227	
25	1	1st FL		228	DT_700_DND	Guestroom			228	
26	1	1st FL		229	DT_700_DND	Guestroom			229	
27	1	1st FL		230	DT_700_DND	Guestroom			230	
28	1	1st FL		231	DT_700_DND	Guestroom			231	
29	1	1st FL		232	DT_700_DND	Guestroom			232	
30	1	2nd FL		321	DT_700_DND	Guestroom			321	
31	1	2nd FL		322	DT_700_DND	Guestroom			322	
32	1	2nd FL		323	DT_700_DND	Guestroom			323	
33	1	2nd FL		324	DT_700_DND	Guestroom			324	
34	1	2nd FL		325	DT_700_DND	Guestroom			325	
35	1	2nd FL		328	DT_700_DND	Guestroom			328	
36	1	2nd FL		329	DT_700_DND	Guestroom			329	
37	1	2nd FL		330	DT_700_DND	Guestroom			330	
38	1	2nd FL		331	DT_700_DND	Guestroom			331	
39	1	LF		Storage		Staff				
40	1	GF		Office		Staff				
41	1	GF		Wellness		General				

Example of an offline terminal list

Import Online Terminals												
Name of Terminal	Configuration	Installation location	DHCP	Protocoll	IP-Adresse	Subnetmask	Gateway	DNS-Server	Door-Name	Access püoint-Name	Reader type	Tastatur
Terminal 1	1	GF	true	IPv6					Door 1	AP 1		
Terminal 2	2	1st floor	true	IPv4					Door 1	AP 1, AP 2		
Terminal 3	3	2nd floor	true	IPv4					Door 1, Door 2	AP 1, AP 2		
Terminal 4	4	3rd floor	false	IPv4	192.168.96.166	255.255.254.0	192.168.96.254		Door 1, Door 2	AP 1, AP 2, AP 3, AP4		
Terminal 5	5	4th floor	true	IPv4					Door 1, Door 2, Door 3	AP 1, AP 2, AP 3		
Terminal 6	6	5th floor	true	IPv4					Door 1, Door 2, Door 3	AP 1, AP 2, AP 3		

Example of an online terminal list

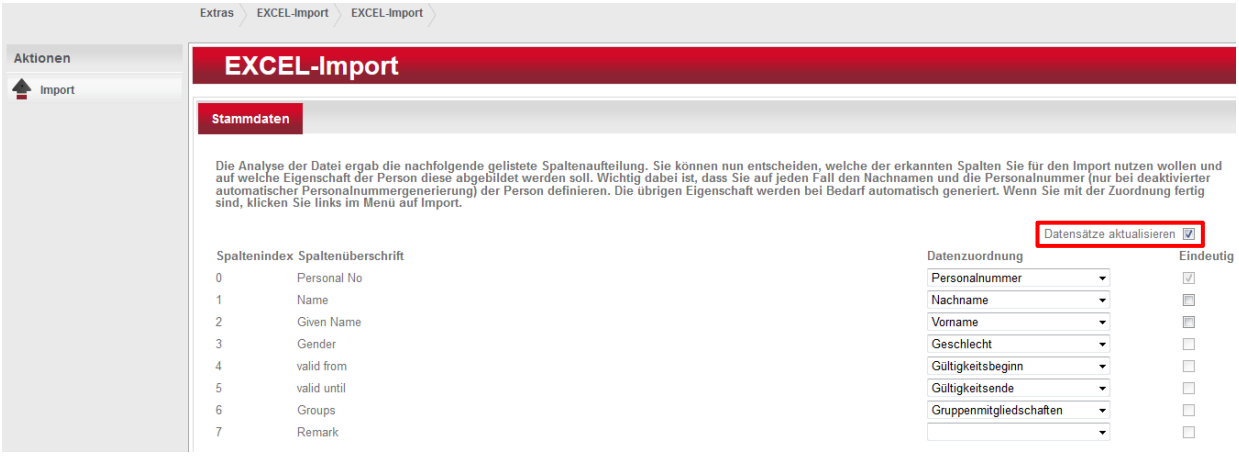
Import Offline Rights							
Row No. (is not imported)	Area	Personal No. (Only already defined persons can be imported)	Name No Import ! (Only helps for better Edition)	Given Name No Import ! (Only helps for better Edition)	Room zones (Hotel: start from 25) Values seperated by Comma	Individual Access Rights maximum 3! Seperated by Comma	Remarks (only Informativ)
1	1	301	Müller		25,29,31,33,35,37,39	101,102,103	(only Informativ)
2	1	302	Meier		25		
3	1	303	Schulze		26		
4	1	304	Schmidt		27		
5	1	305	Hoffmann		28	106	
6	1		...				
7	1						
8	1						
9	1						
10	1						

Example of an offline authorisation list

Import of Individual Rights Dialock2 (Hotel)			
Row Nn. (not imported)	Individual Access Right ID.	Name	Remarks (Only Informativ)
1	101	101	
2	102	102	
3	103	103	
4	104	104	
5	105	105	
6	106	106	
7	121	121	
8	122	122	
9	123	123	
10	124	124	

Example of an individual rights list

If the import file has been selected, you are forwarded to this page.
Assign the respective data (right) to the column headers (left).



Importing data records: Basically, only new data records are created.
Existing data records are not updated. If an existing data record is overwritten by a new data record, i.e. it is going to be updated, the "**Update Data Records**" function must be activated. In this case, the data record is updated with the new data from the Excel® file. The "Unique" function can be used to determine individual fields which are not updated when doing this.

Now click on Import.

The progress and the number of successfully and unsuccessfully imported rows are displayed to you.

Note:

Since a transponder for logging the booking history is required for using the PIN code as a unique identification characteristic, the transponder ID and the transponder type must generally be specified when a data import is carried out using the Import function. (**5.2.1.5** *Identification Characteristics*).

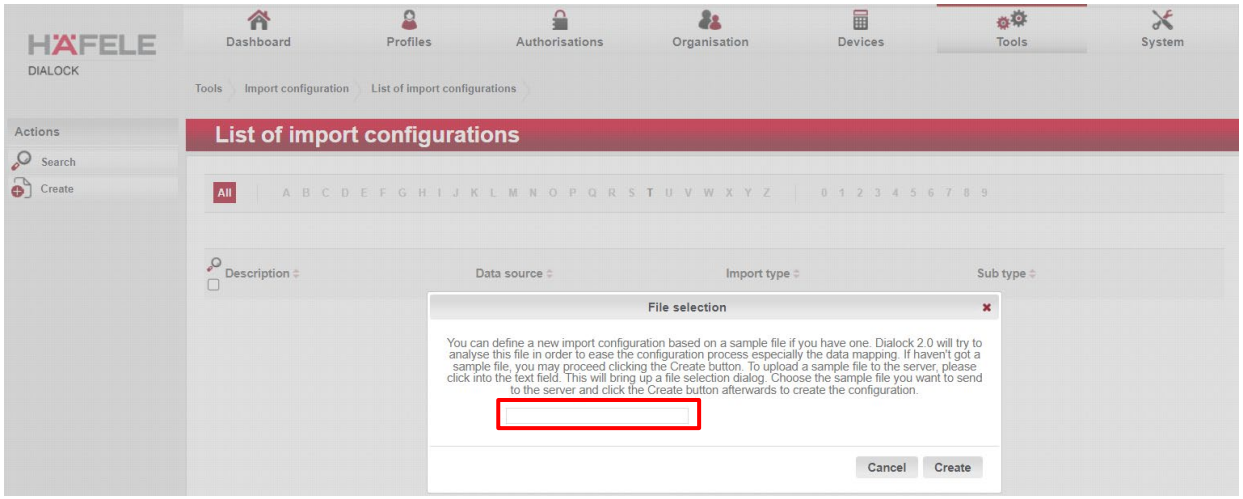
5.6.1.1. Time triggered import

Description of function

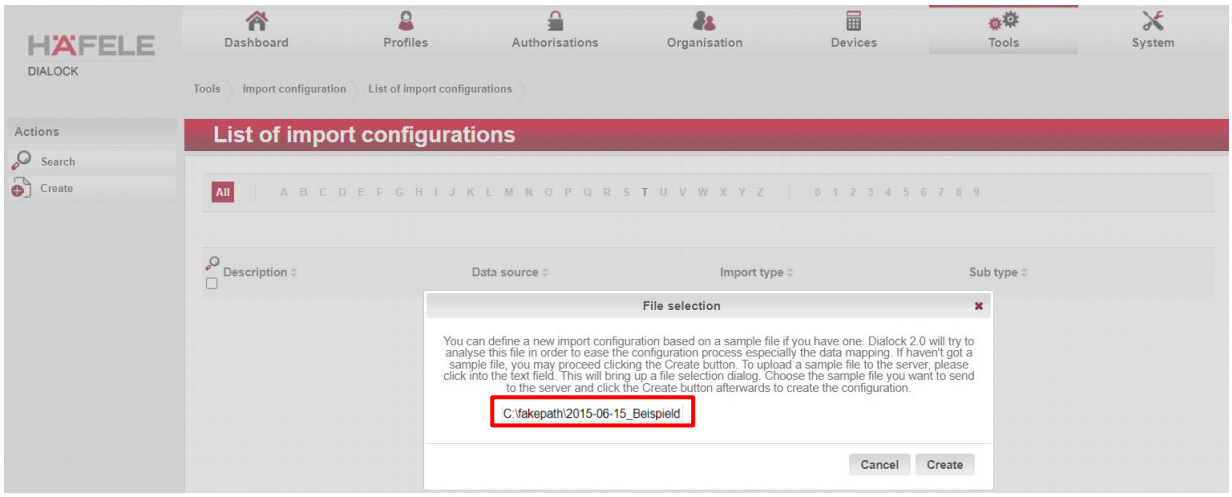
With this function it is possible to extend the automatic import to include the master records which **cannot** be imported using the current Excel import function. Only personnel records can be imported via the import function.

5.6.2. Import configuration

The configuration of the import is defined in menu item **Options -> Import configuration**. Clicking on Create opens a dialogue window.

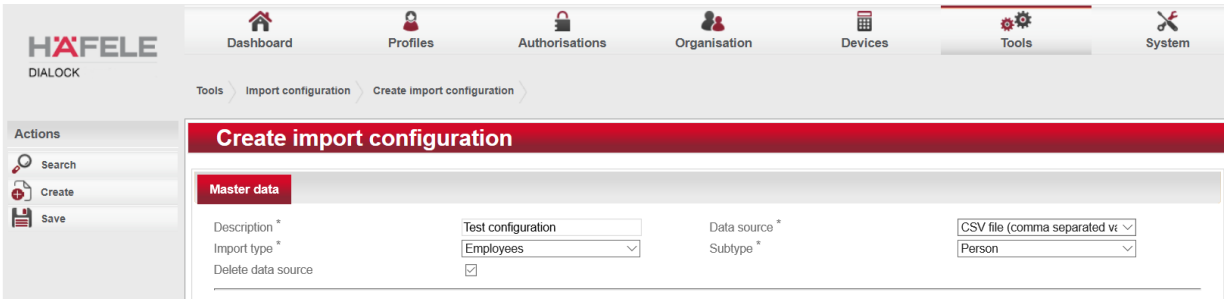


By clicking in the empty field, you can make an example file from your PC available for the configuration.



The software will then analyse this and attempt to determine the header and the column names. The example file does not have to be specified. In both cases, finish by clicking on the "**Create**".

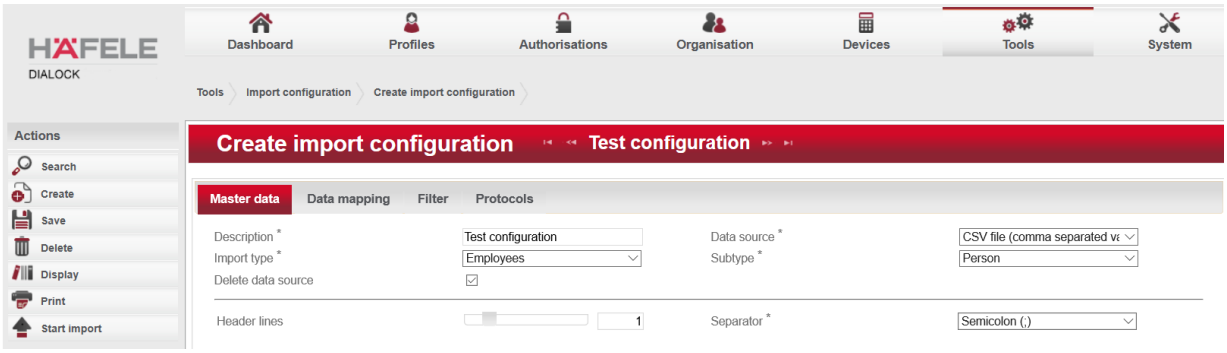
A form for the import configuration then appears.



Firstly, enter a name for the import. Then choose the format of your import file from the sources which are supported (currently EXCEL and CSV). Then define which type of data you would like to import using Import type and Subtype selection fields.

The Delete data source option is pre-selected. This means that imported files are automatically deleted from the directory. You should not change this setting unless you know exactly why you do not want it. If the file stays in the directory, the data that is received during every time-controlled run of the import will be transferred into the system again.

Now save the configuration 



After the first save, three more tabs appear (data mapping, filters and logs). However, first you will see that more input fields have appeared on the Master data tab. If you have selected an example file, the number of header lines is already set, and if not you should now set the number of header lines. These lines are skipped during the import.

If you have selected EXCEL as the import source, and several tables / worksheets are present in your import file, you can select which worksheet is imported using the name of the worksheet. Otherwise the Dialock software always uses the first worksheet.

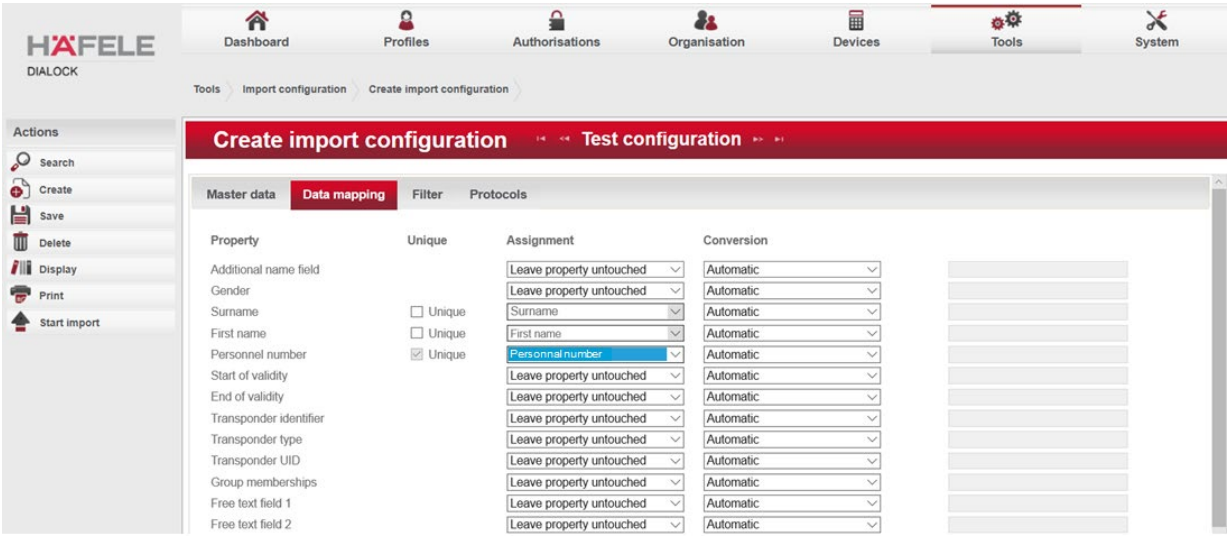
Data mapping

Now switch to the **Data mapping** tab. Here you can see all of the properties that are available for the selected import type in tabular format. However, you do not need to map all of the properties to carry out an import.

For each property that you would like to import, you should now define a column assignment so that the software can determine which column is mapped onto which property during the import procedure. If you have selected an example file, the designations of the header line are available in the selection fields. Otherwise the columns in CSV files are numerically numbered and Microsoft EXCEL files are alphanumerically numbered (A, B, C, ... X, Y, Z, AA, ...) and you must carry out the assignment in accordance with the column number.

Some properties can be marked as **unique**. This comes to bear if a follow-up import takes place or several records with the same properties are imported. The properties marked as unique identify the record to be updated in the Dialock software database.

If no record with the relevant values is found, a new record is created. Otherwise, the record which has been found is updated with the values from the import file. Certain characteristics are inherently unique, and must also be unique when they are entered via the import. The personnel number, for example.



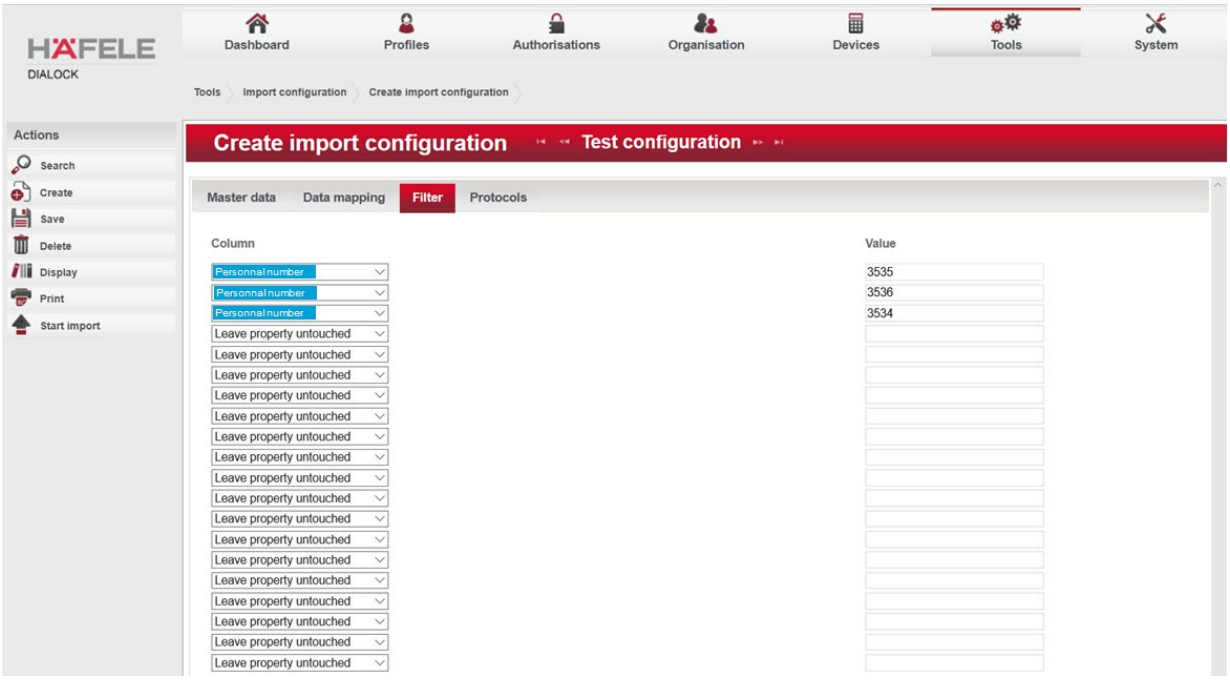
The **Conversion** column must be regarded as an expert function. Since import files initially only contain text, the values from the individual columns must be converted into the internal data types in the database. This is usually carried out by the software automatically. However, you can influence a conversion using various conversion functions, e.g. if you use an unusual data format or would like to only import part of a column value. For example, the software can also import personal portraits in HEX ASCII-i or Base 64 format with the new import functionality.

732.29.430
HDE 20.12.2023

Convertion	Explanation	Examples
Date format	Imports a date and expects a Java-compliant date pattern	yyyy-dd-MM HH:mm -> (2018-02-06 10:45) MMM d, ``yy h:mm a -> (Feb 6, '18 10:45 AM)
Number format	Imports a number and expects a Java-compliant number pattern	# , ## 0.0 # -> 12.354,0 -> 27,14
Regular expression	A regular expression with grouping. All groups are combined into the result.	([^ |] +) (? : \ | ([^ |] +)) -> Group 1 | Group 2 | Group 3
Base64 - Coding	Binary data in Base64 encoding	No format required
Hex-Ascii-Coding	Binary data in hex-ascii format	No format required

Filter

The data to be imported from the file can be defined in the **Filter** tab. If no filter is defined, the software imports all rows. The following example defines a filter for the "***Personnel number***" column. This means that only the rows with a value of 2535 or 3536 or 3534 in the "Personnel number" column are imported.



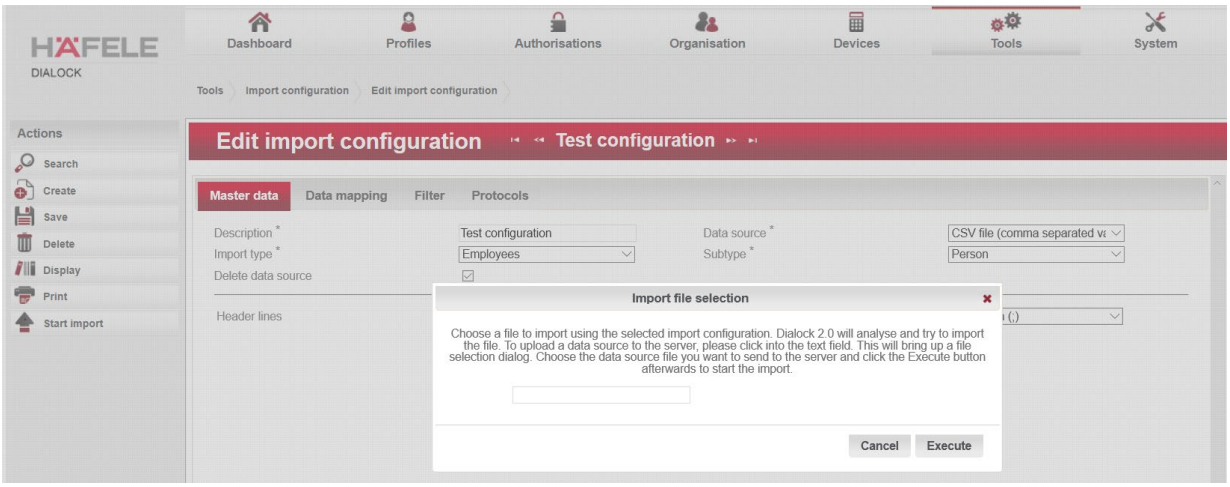
5.6.2.1. Carrying out an import

You now have a total of three ways of triggering an import procedure:

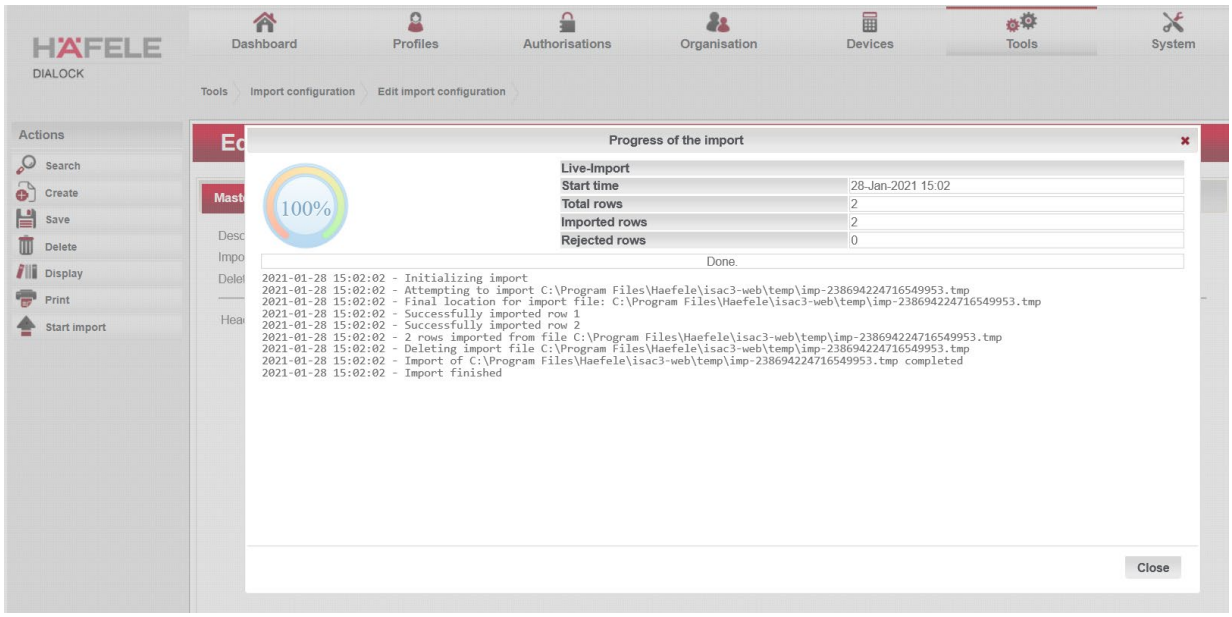
1. Start the import directly via file upload
2. Start a scheduled task directly
3. Configure a (cyclic) scheduled task for the import

5.6.2.2. Import via direct start

If you only want to carry out the import once in order to initialise the database, use this version. To do this, click on the Start import button in the action menu of your import configuration. In the dialogue that opens, select the file that you would like to import by clicking in the empty text field like you did at the beginning, and select the file.



Then start the import by clicking on the **Run** button.
During the import procedure, a progress dialogue is displayed which notifies you of the progress and the result of the import. The import log is displayed in the bottom area. This makes errors easier to spot (as in this example, where a CSV file has been selected instead of an EXCEL file):



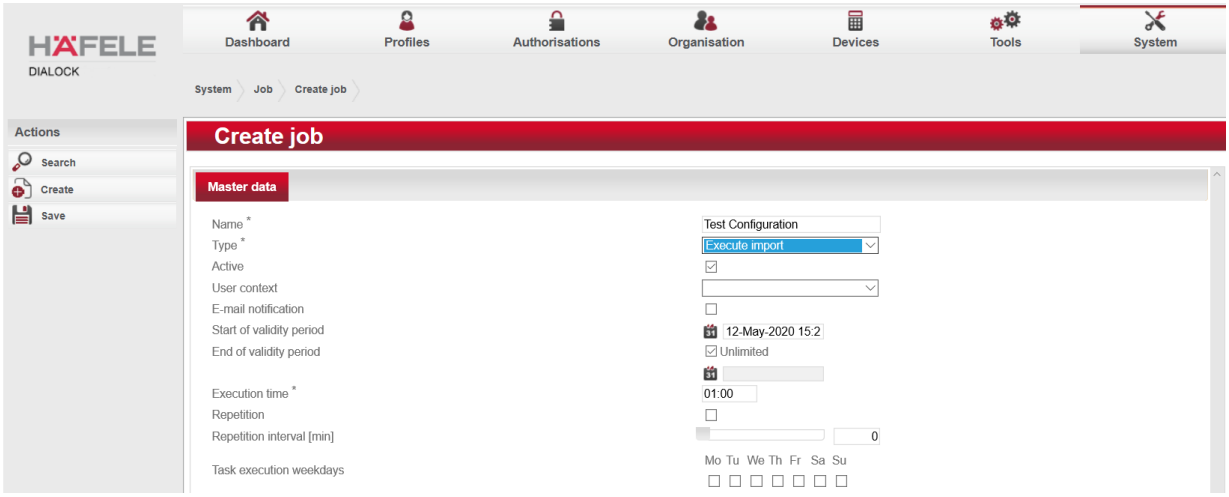
At the end of the import, close this dialogue using the **Close** button. Unlike the previous import functionality, the logs are not volatile but are stored in the database. This means that you have access to them at all times, and you can also check an overnight import procedure on the following morning. In order to this, you switch to the Logs tab. Clicking on the button with the magnifying glass opens the log, which is also displayed in the progress dialogue. You can delete the logs at any time using the button with the trash can.

5.6.2.3. Import via scheduled task

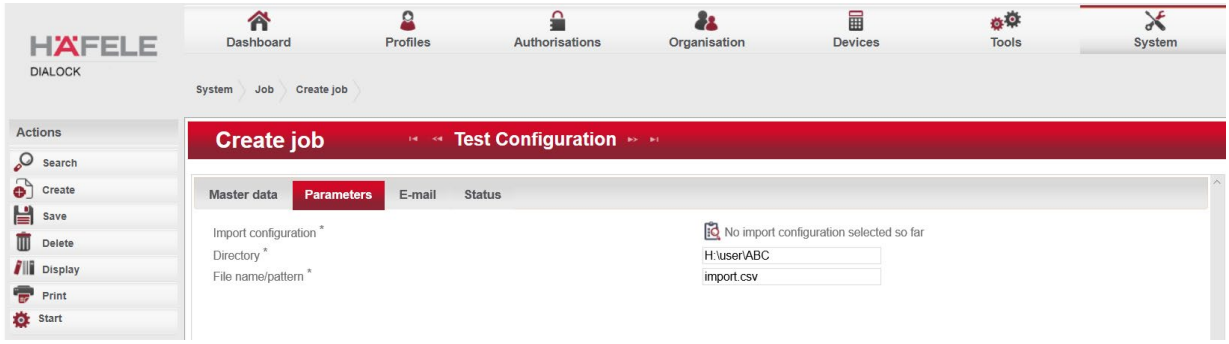
Particularly if the master data (particularly the personnel master data) has to be synchronised from an external system in the Dialock software by means of a regular data transfer, a time triggered import can be used. Imports such as this are usually carried out within a time window when the system is not being used, such as at night.

To start an import under time control, switch to **System->Scheduled task** and generate a new job by clicking on the Create button. Enter a name and select Execute import from the type list.

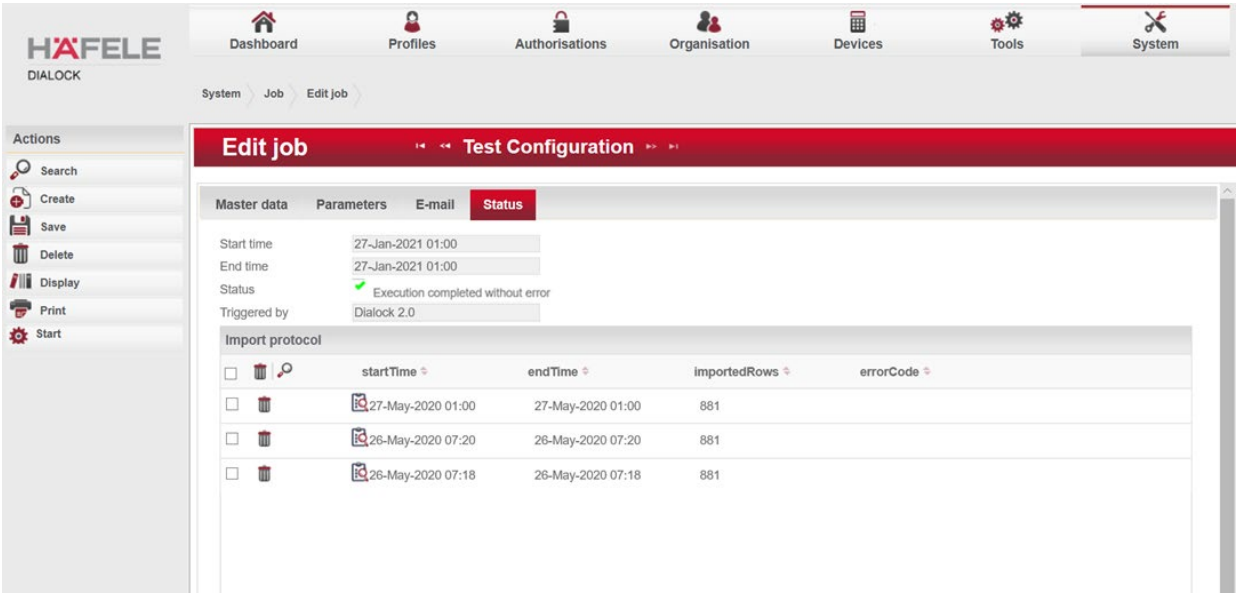
Now configure the job in accordance with your requirements like you do for any job type, and then click on Save.



Switch to the Parameters tab and select the import configuration to be run using the selection dialogue. Since interaction with a scheduled task is not possible, you must also define the directory and the file or a file name which defines the files to be imported. **The directory is a folder on the server** on which the Dialock 2 software is installed, not on your computer. The file name can contain * as a placeholder character in order to realise file selection in a more dynamic way (e.g. person-*.xlsx).



As soon as you click on Save, the job is planned by the scheduler component of the software and run at the next defined point in time. You can view the status of the job and the logs of the assigned import configuration on the Status tab.

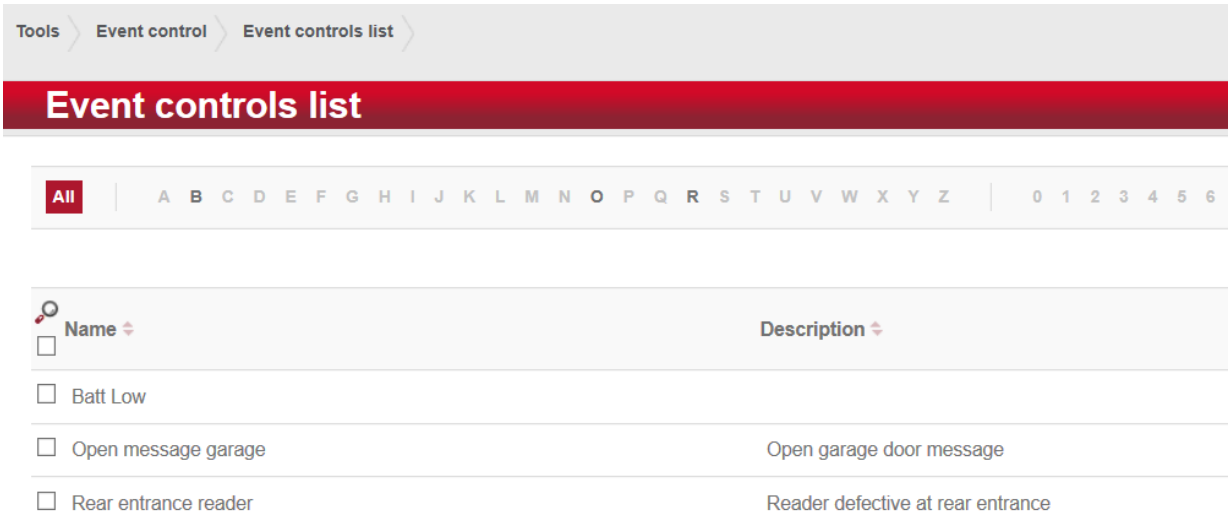


5.6.3. Script

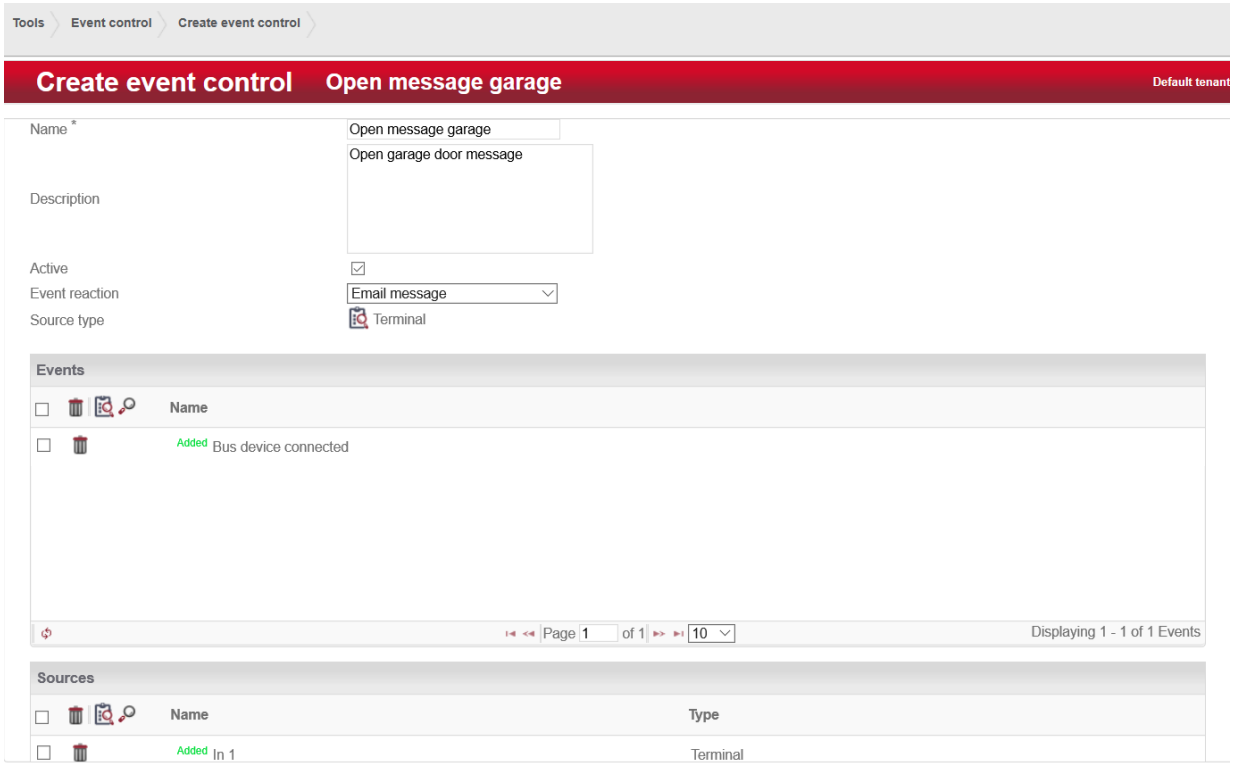
Allows the definition or incorporation of scripts for special functions.

5.6.4. Event control

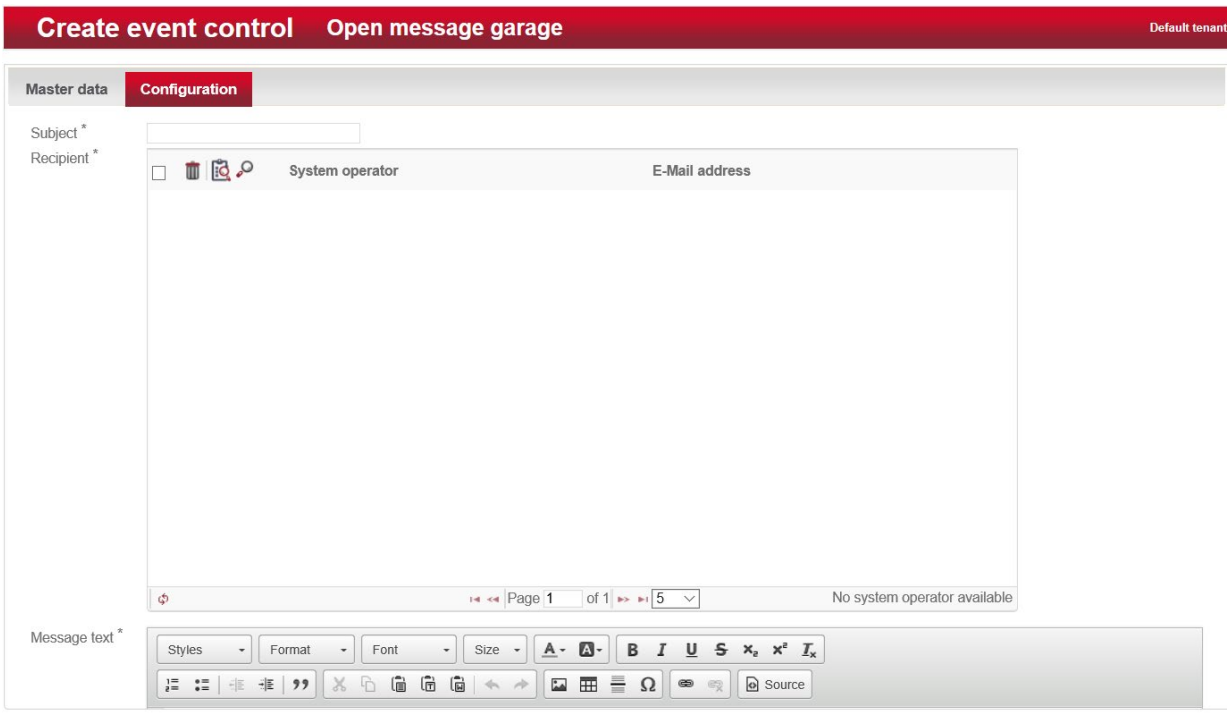
With the aid of event control it can be defined that the system sends a predefined e-mail to a selected user or executes a so-called script if a certain event or combination of events occurs.



In order to create an event control, issue a **Name** for it and a **Description**. If the event control is to be temporarily set to inactive, deactivate the check box next to “**Active**”. Define the required **Event reaction** and the **Source type**.

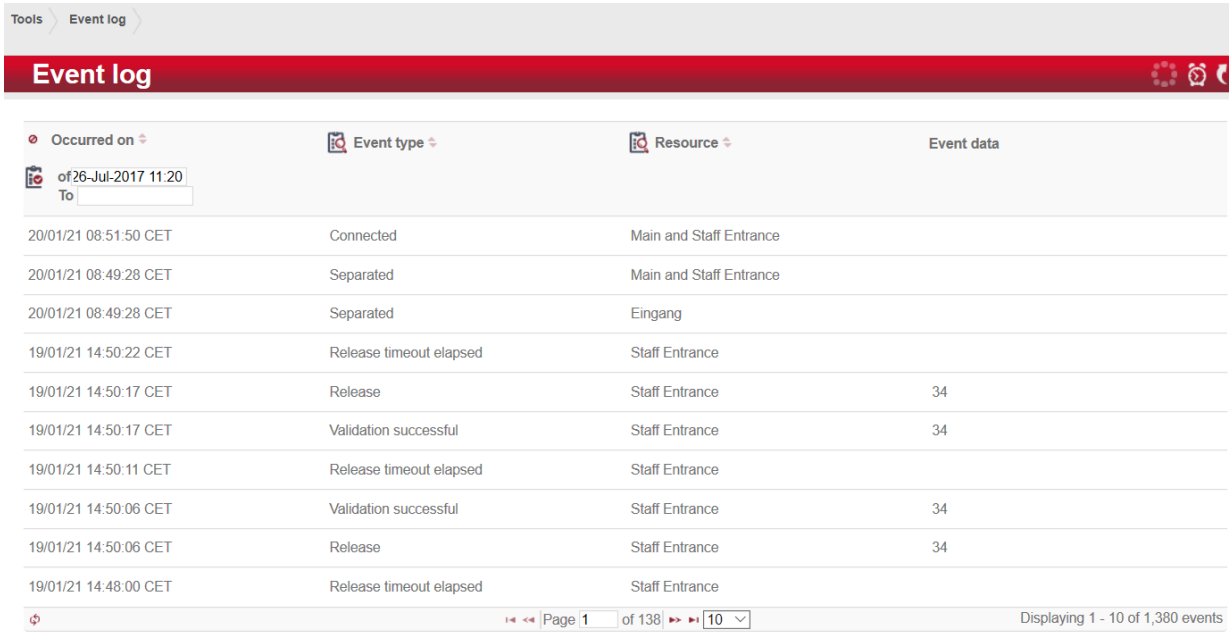


Then make a selection in the “**Configuration**” tab to configure the e-mail function or select the script that should be used for this event control. To do this, drag the required script from the list “**Available scripts**” to the list “**Selected scripts**”. Save your information.



5.6.5. Event log

The event log lists all events that have occurred during the selected time period at the system components.



It is possible to sort the events for reporting according to time, event type or resource.

List of Dialock event messages (**ID = Transponder**)

Designation	Description
Alarm reset due to release	Door alarm reset by another release.
Anti-passback block still active	Timed anti-passback still active for this ID.
Area change	Message concerning area change of an ID.
Area change error	ID causing error during area change.
Authentication error	ID could not be correctly authenticated.
Bus subscriber connected	Bus subscriber accessible.
Bus subscriber disconnected	Bus subscriber no longer accessible.
Connected	Controller connected to host again.
Contact to card aborted	Card or transponder removed during processing.
Data error	Maximum value exceeded or minimum value undershot when transferring data from table ...
Diagnostic file full	The diagnostic file is full. It will be renamed and the old backup file deleted.
Disconnected	Communication between host and controller disconnected.
Door locked	The door is locked.
Door locked again after error	Door has been locked after a procedural error.
Door not unlocked after release	Door has not been unlocked in spite of release.
Door open	Door is unlocked.
Door open too long	Door has been open for too long.
Door release by host	Door has been directly released by host.
Door unlocked without permission	Door unlocked without permission, without prior release.
Encryption error (SD card)	SD card has unexpected data encryption. Affected files will be deleted.
Entry time expired	Entry time between two keypad digits exceeded, input deleted.
Entry time expired	Release of access point / door took place without door being opened.
Entry time overwritten	Entry time between two identification characteristics was too long. The entries have been deleted.
ID expired	Access denied because validity has expired.
ID index re-created	Internal ID index file re-created due to file error.
ID query	Not yet implemented.

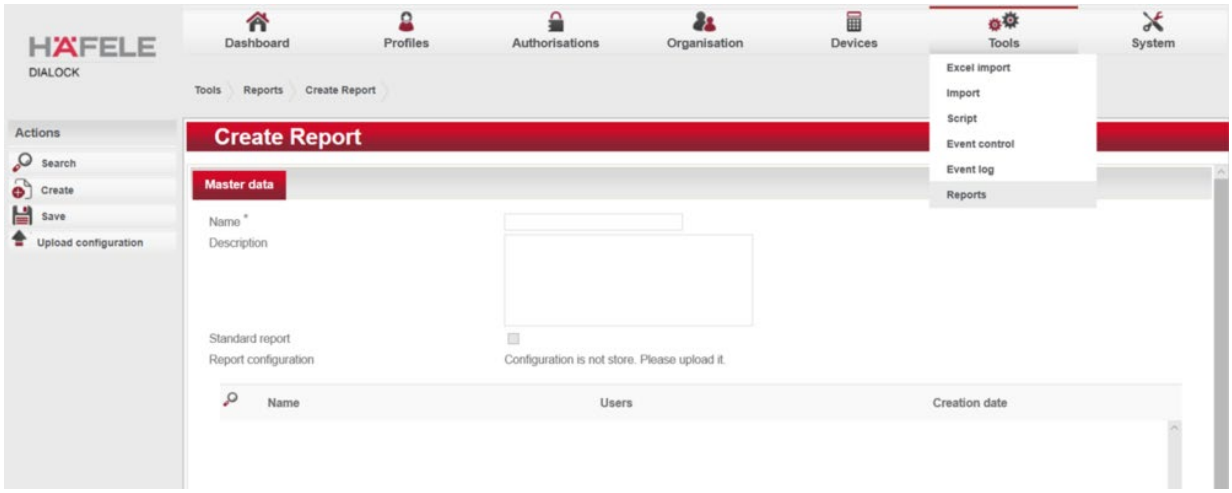
ID unknown	ID unknown in controller.
Incorrect door code	The door code entered was incorrect.
Incorrect PIN code	The PIN code entered was incorrect.
Input interruption	Signal input interrupted.
Input off	Signal input open.
Input on	Signal input closed.
Input short-circuit	Signal input short-circuited.
Keypad active	Automatic zone for keypad active.
Keypad inactive	Automatic zone for keypad inactive again.
Latch closed	Latch is closed.
Latch error: Break-in	Door open although latch is closed.
Latch error: Latch closed/door open	Door still open although latch is already closed.
Latch error: Latch open/door closed	The latch has been open for too long after the door was closed.
Latch open	Latch is open.
Name index re-created	Internal ID name index file re-created due to file error.
New SD card accepted	SD card in controller saved as the valid card.
No access profile	No suitable access profile on ID.
No ID for PIN code	Unable to find ID for PIN code. Only for keypad without reader.
No output voltage	Output voltage of serial interface is too low.
No passage	Passage contact not triggered, no passage took place.
Normal situation	Access point in normal condition.
Number of failed attempts exceeded	Maximum number of non-permitted access attempts reached at this access point.
Operating mode configuration error	Selected operating mode of access point is incorrect.
Output off	Not yet implemented.
Output on	Not yet implemented.
Output voltage OK	Output voltage of serial interface is OK again.
Passage	The passage contact has triggered, a passage has taken place.
Permanently free	Access point permanently unlocked.
Permanently locked	Access point permanently locked.
PIN code change	PIN code changed to ---.
Pre-alarm triggered	Pre-alarm (advance warning) for a door or latch too long.
Read error	Error occurred when reading card or transponder.
Reader defective	Reader sabotaged.
Reader ID data	Card information transaction --> bit information that was read via a CI / Da or Wiegand interface. (between iTCRIF and iTC).
Reader OK	Reader OK (again).
Release	Access point released by ID.
Release aborted	Release of access point / door aborted by another access action.
Release by means of door code	Access point was released by entering door code.
Reset	Controller has carried out a reset.
Resource list changed	Number of system resources changed.
Resource signalling value	Resource signalling the following value: ---
Result of SD check	Result of checkdisk on SD card was:---
REx button active	Automatic zone for REx button active.
REx button actuated	Access point has been released by pressing the REx button.
REx button inactive	Automatic zone for REx button inactive again.
Sabotage contact OK	Reader sabotage contact OK.
Sabotage contact triggered	Reader sabotage contact triggered.
SD card defect	Defective SD card.
SD card formatted	SD card has been formatted.
Silent alarm	Attack signalled using code keypad.
Table deleted	Format table ... false. Controller has deleted table.
Toggle activated by ID	Access point switch to toggled permanently free using an ID.
Toggle deactivated by ID	Toggled permanently free disabled using an ID.
Toggle status: Permanently free	Access point is in toggled permanently free status.
UID of SD card and processor	Both UIDs are reported.
UID of unauthorised SD card	SD card invalid at this controller and has UID of: --
UID processor	Processor UID is: ---
UID SD card	SD card UID is: ---
Unknown	Event type unknown to host.
Write error	Error occurred when writing to card or transponder.

5.6.6. Reports

In order to manage reports, go to menu **Tools \ Reports**.
In order to create reports, click on “**Create**” in the menu on the left-hand side and give the new report a **Name** and a **Description** if required.

The check box next to **Standard report** indicates whether it is a report that was supplied with the system. In this case the check box is activated. If it is a report that you have generated, the check box remains deactivated.

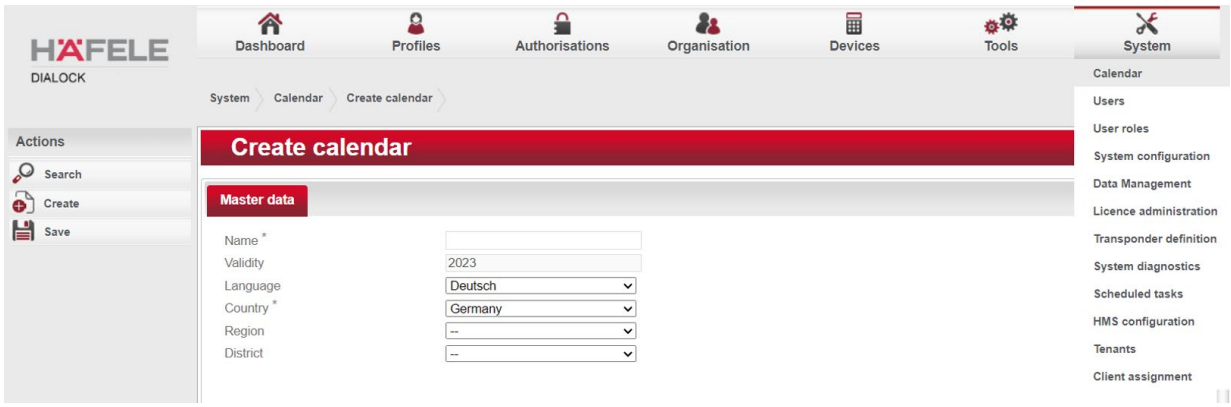
If no **Report configuration** has been saved, click on “**Upload configuration**” in the menu on the left-hand side to upload your report. Save this.



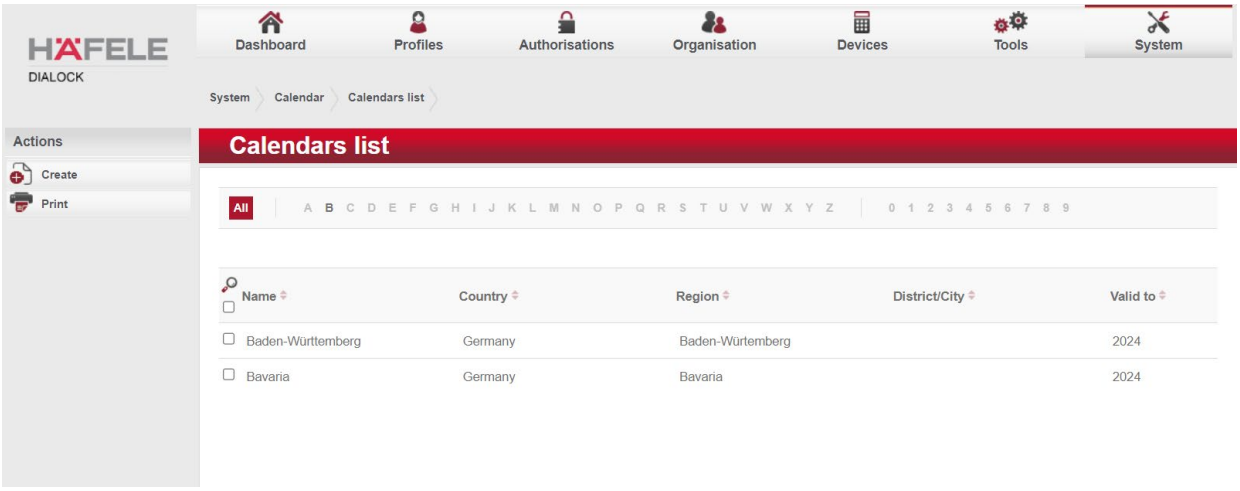
5.7. System

5.7.1. Calendar

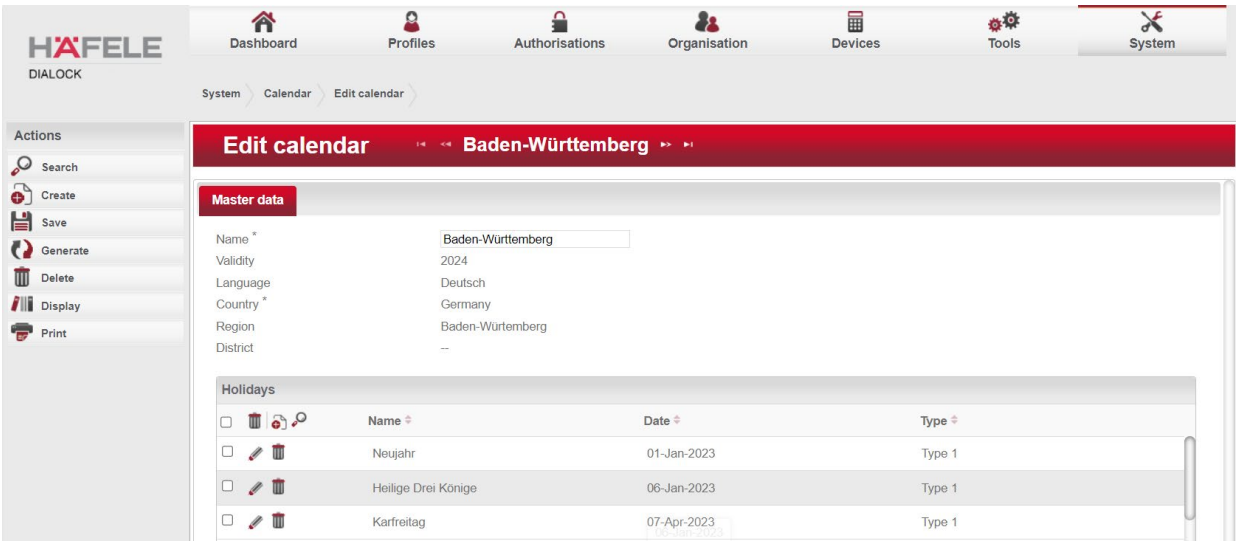
The public holiday calendar of the required country can be loaded using the “**Create calendar**” function and identified with a name.



After a **Saving** has taken place, the calendar is visible in the **Calendars list** and can be selected for processing.



Dialock has a facility for creating your own additional public holidays for the calendars that have been created. This is useful if different access authorisations are to apply for company holidays, for example. In order to do this you create an appropriate time model for public holiday type 2 and assign it to the persons concerned.
In order to create an additional public holiday, click on the plus symbol and enter the **Name**, the **Date** and choose between **Type** 1, 2 or 3. Public holidays can also be deleted from the calendar.



Click on “**Ok**” and save the results of this action.

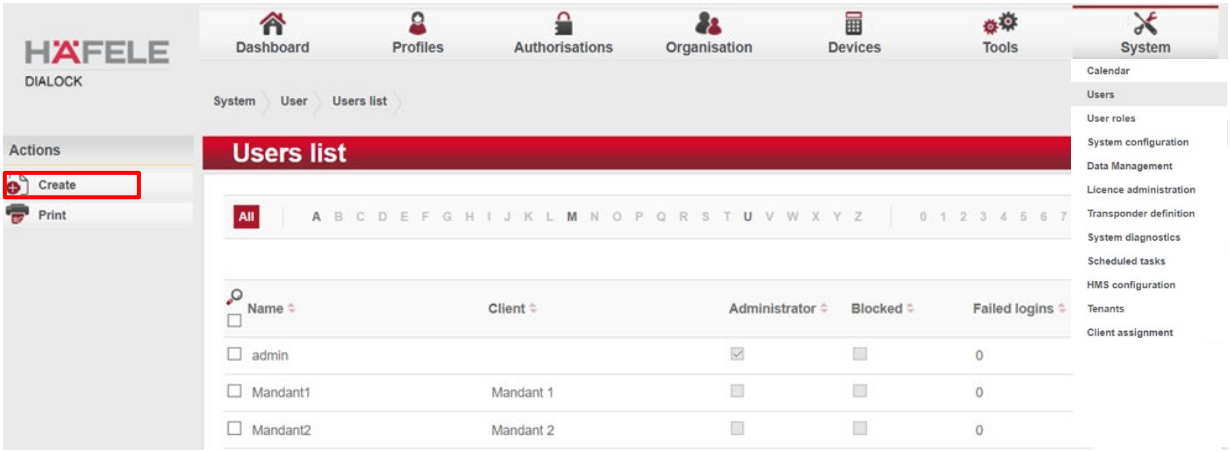
5.7.2. User

Dialock is supplied with the user “**admin**” and the password “**admin@dialock**” as standard. We recommend that the administrator password as well as the user passwords are changed on a regular basis for security reasons.

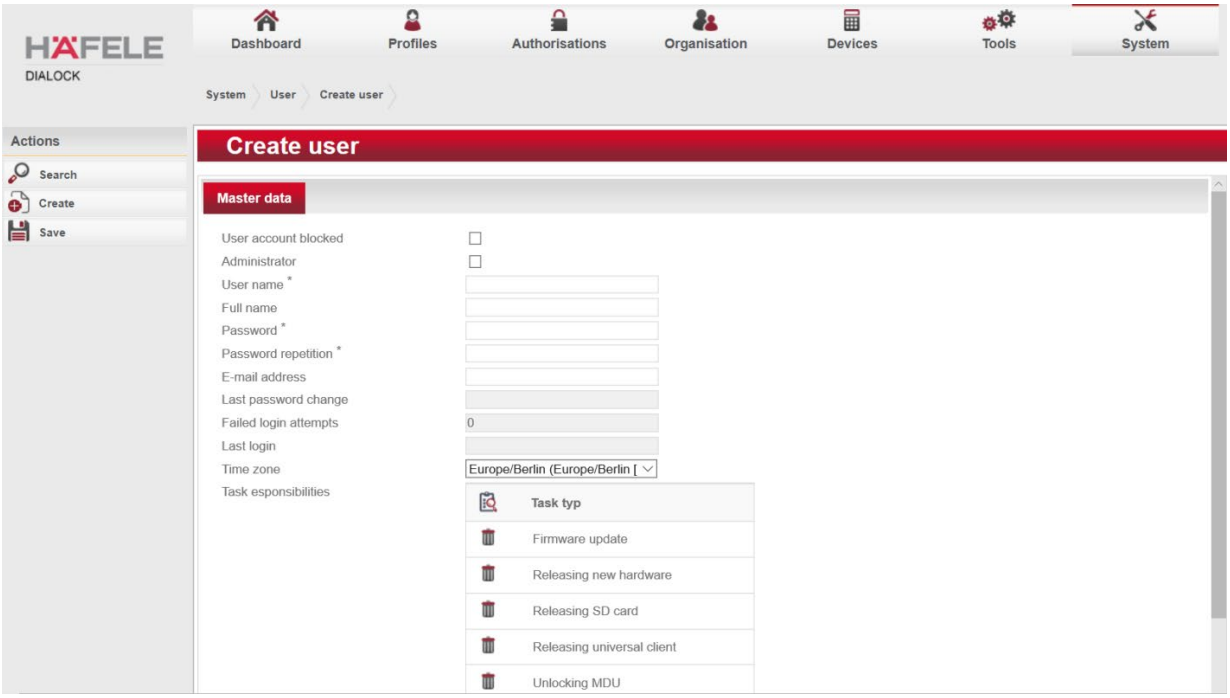
The administrator (admin) has the right to create other users.

5.7.2.1. Enter / block user

An overview of the current system users can be found in the **User list** in the **System \ User** menu.



More users can be created by clicking on “**Create**” in the left-hand action bar.



Block the user account immediately with “**User account blocked**” if the user concerned should no longer have authorisation to use Dialock.

If you create a user as an **Administrator**, it is not necessary to assign further authorisations. An administrator automatically has all authorisations.

Enter a **Username** and a **Password**. The user can change these here himself later.

Enter the **E-mail address** of the user and specify the **Time zone** that the user is assigned to.

You can also determine the **Task types** (4.1 *Tasks*) for which the user is to be authorised.

A user without administrator rights should have user roles with different authorisations assigned to him.

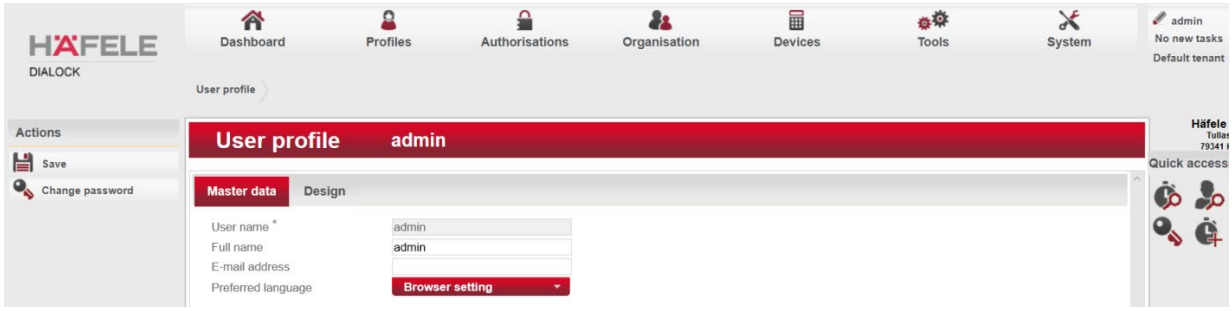
5.7.2.2. User customisations

Each user can make individual adjustments via the pencil icon on the right side of the screen.

The following changes can be carried out here:

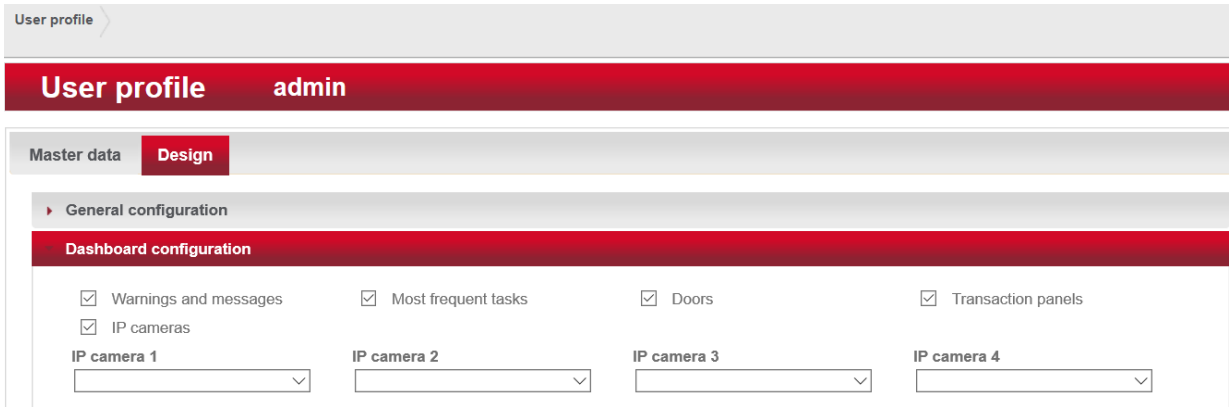
5.7.2.3. Change / edit user profile

Via the pencil icon (alternatively also via the menu item **System > User**), you can access your own profile. You have the option to change your user name and your e-mail address here.



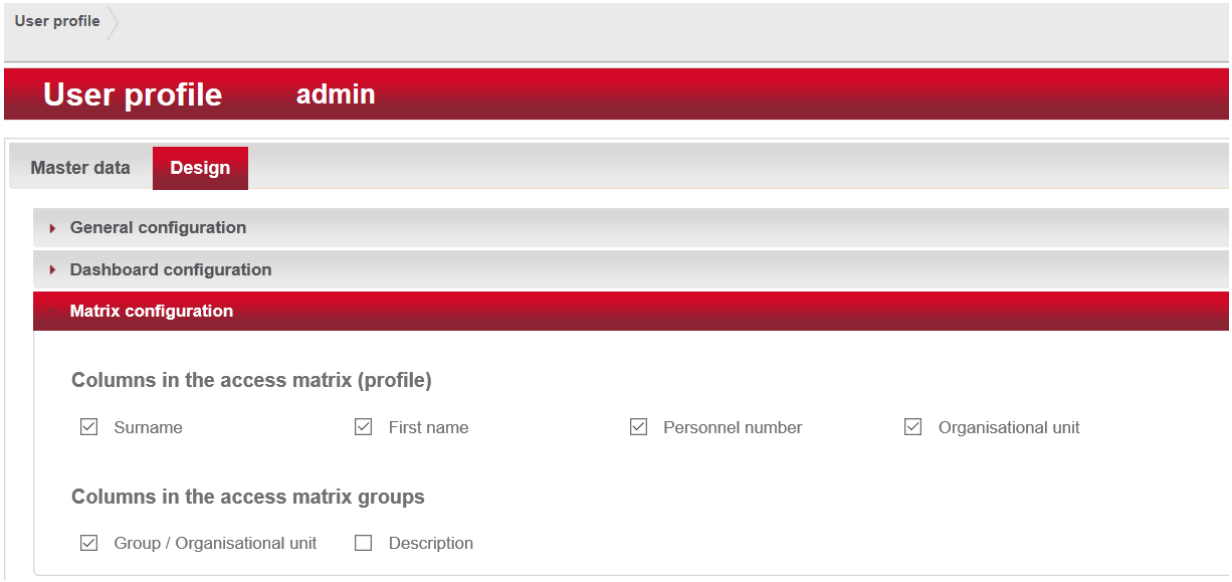
5.7.2.4. Dashboard display (dashboard configuration)

Under **Dashboard configuration** in the **System > User** menu of the “**Design**” tab, “**Warnings and messages**”, “**Frequent tasks**”, “**Doors**”, “Transaction panel” and “**IP cameras**” are available for selection. Activate that which should be displayed in your personal dashboard.



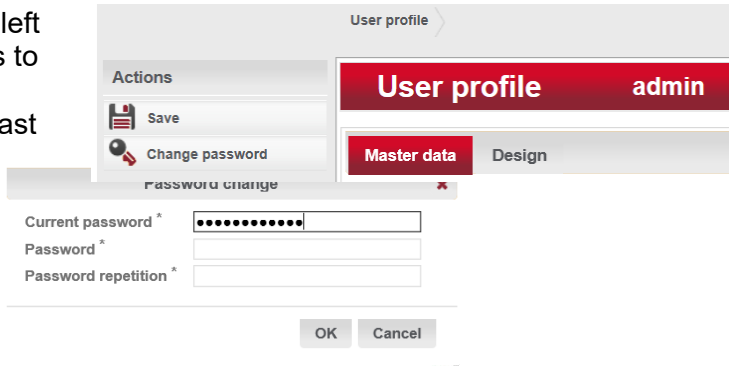
5.7.2.5. Matrix configuration

You can adapt the tasks which should be displayed in the access matrix of the profiles and the groups in the “**Design**” tab of the **System > User** menu in the “Matrix configuration” bar.



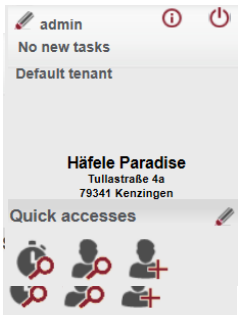
5.7.2.6. Password change

Click on “**Change password**” on the left sidebar and fill out the specified fields to create a new password.
Choose a secure password with at least 8 characters.

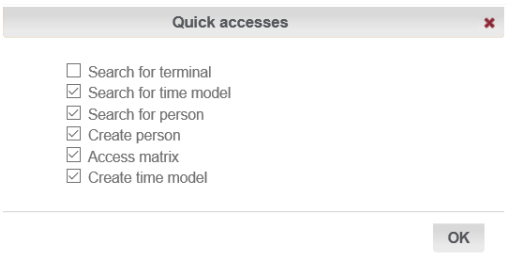


5.7.2.7. Quick access settings

Quick accesses are set up using the pencil icon on the right-hand sidebar.



Select the desired modules you would like to have quick access to.

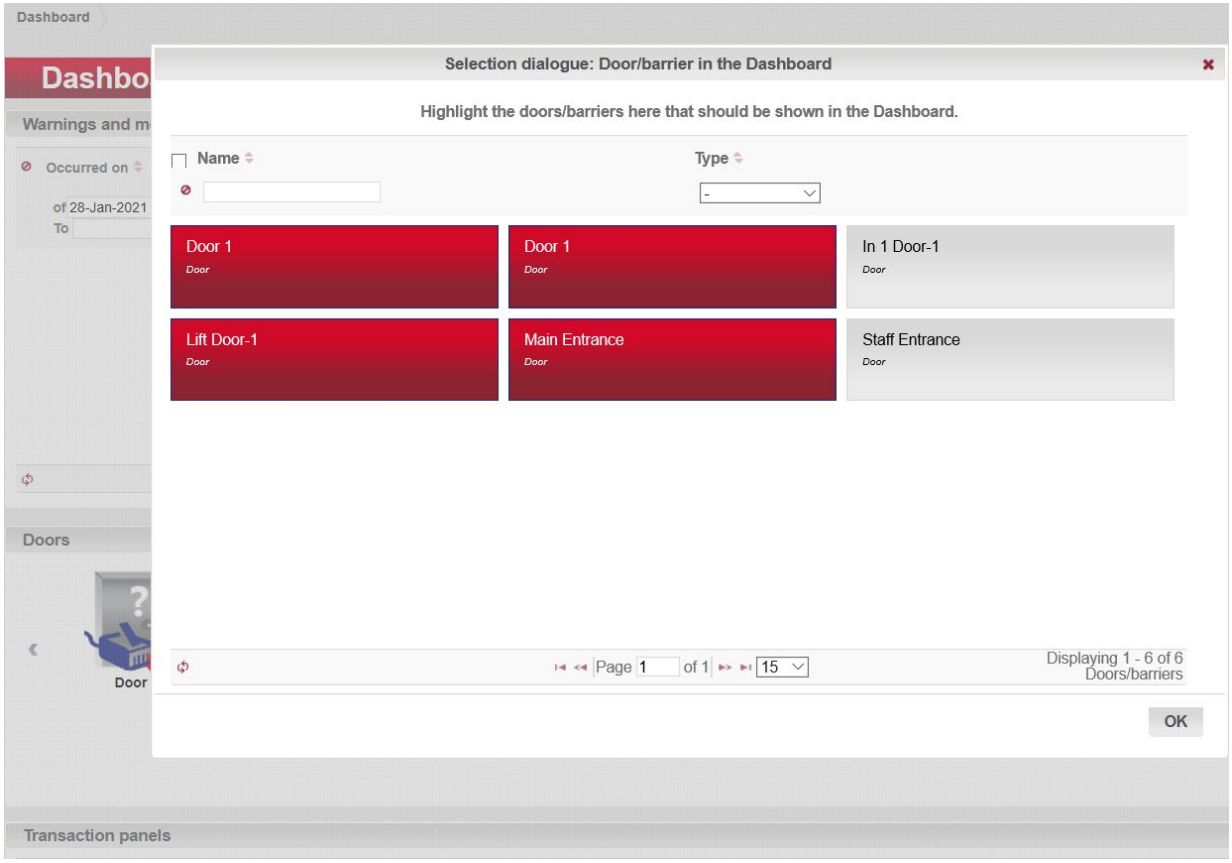


5.7.2.8. Arrangement in the dashboard

You can change the arrangement of the function groups in the dashboard using drag & drop by clicking with the mouse button on the upper bar containing the headings and dragging to the desired location.

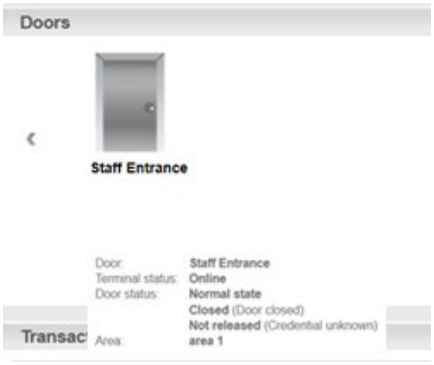
5.7.2.8.1. Individual display of doors in the dashboard

Click on the pencil icon on the right-hand edge of the doors screen. Mark the desired door(s) or barrier(s) which should be displayed in your dashboard.



Clicking on the respective door icon during your everyday work takes you directly to the editing screen of menu item **Devices > Edit barrier / door**.

Move the cursor to a door or a barrier in order to display data as shown on the right-hand side of the screen.



By right-clicking on the desired door, it can be actuated directly or the associated events can be displayed.

5.7.3. User roles

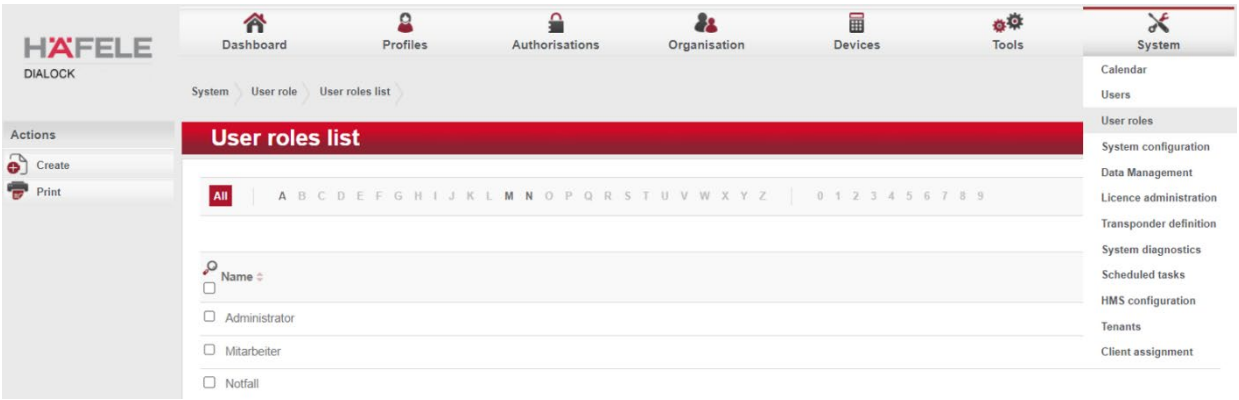
Users can be assigned different **user roles** and therefore receive the respective access rights to the different modules using the “**User roles**” function.

Multiple assignments of user roles are possible.

Numerous *detailed* user roles can be created using the user role system of Dialock 2.0. In order to avoid the tiresome repeated work that is required to create comparable roles in every system, Dialock creates the **Employee**, **Administrator** and **Emergency** roles automatically.

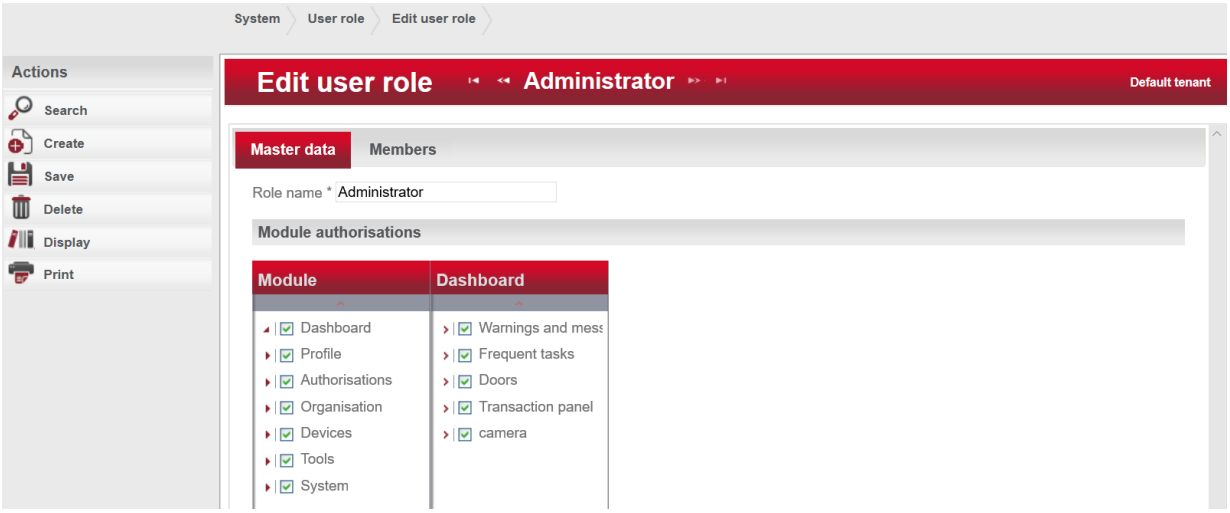
5.7.3.1. Edit user role

You can obtain a display of the assigned user roles in the “**User role list**” via the “**System \ User roles**” menu item.

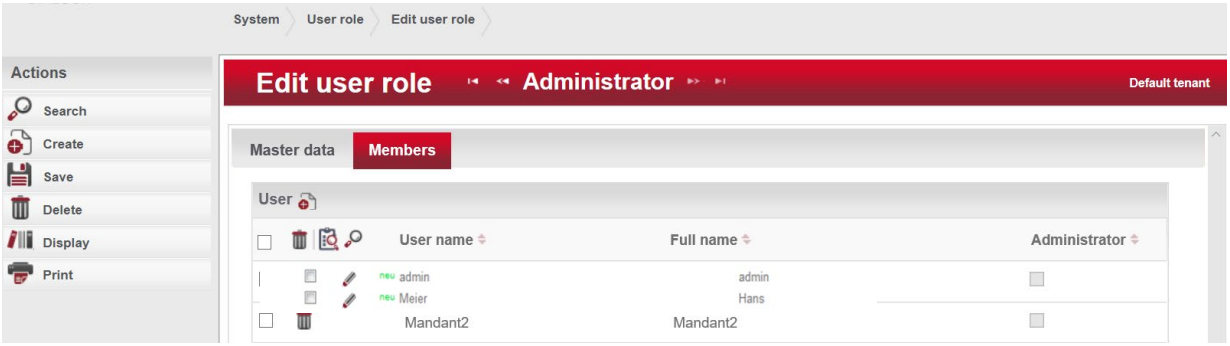


When a user is selected, the authorisations in connection with the respective role are assigned using “**Edit user role**”.

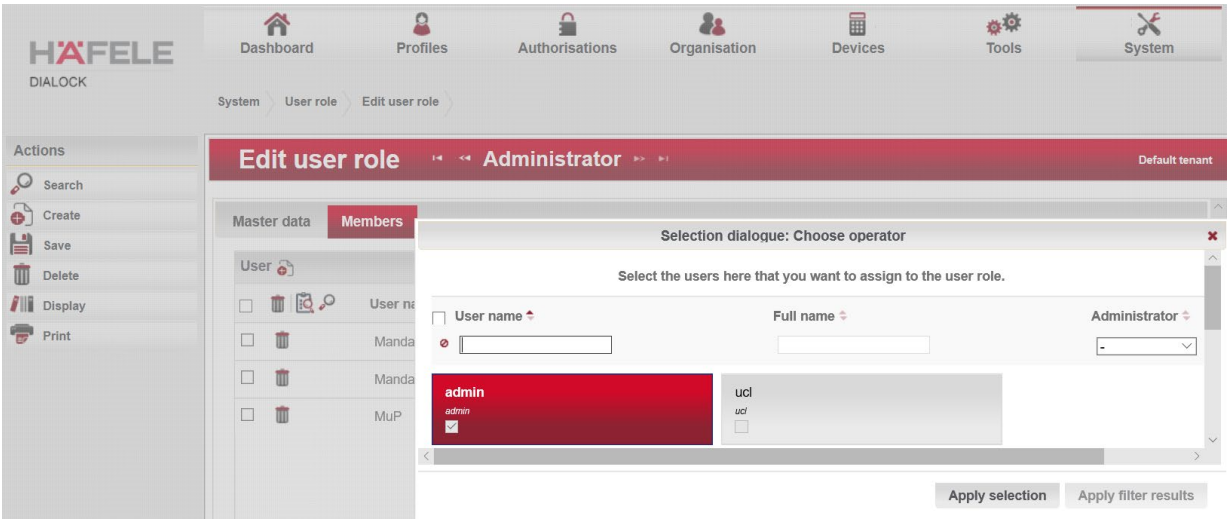
In “**Module authorisations**”, the main menu structure is depicted which can be individually authorised here by activating the selection.



The employees which have this role and the associated right are displayed under **Members**.

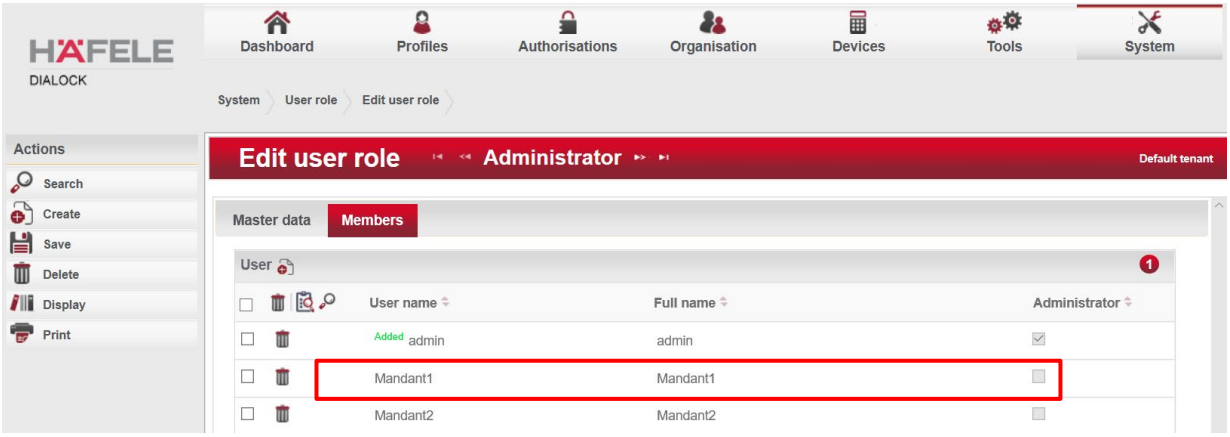


You can select and add more employees to this user role by clicking on the  symbol.



Click on “**Accept Selection**” and save your selection. 

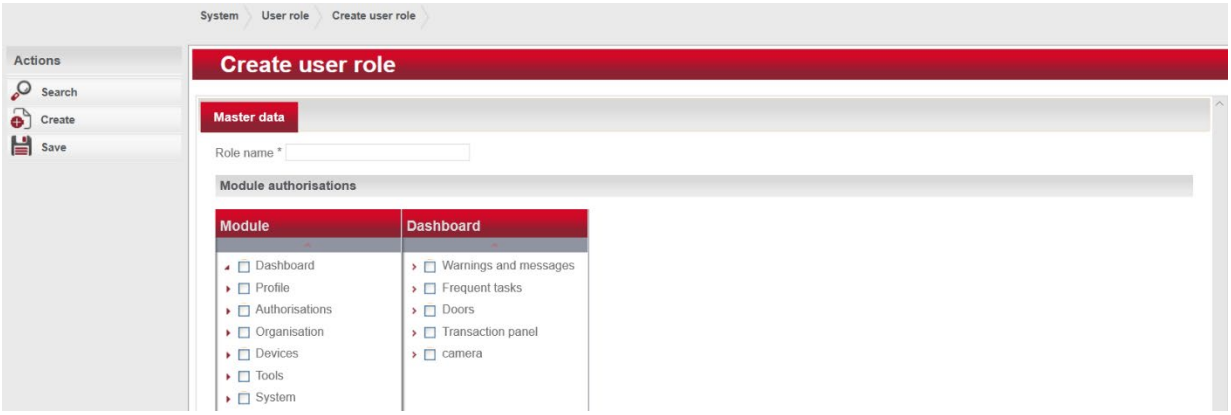
732.29.430
HDE 20.12.2023



The employee is assigned to the user role.

5.7.3.2. Create user role

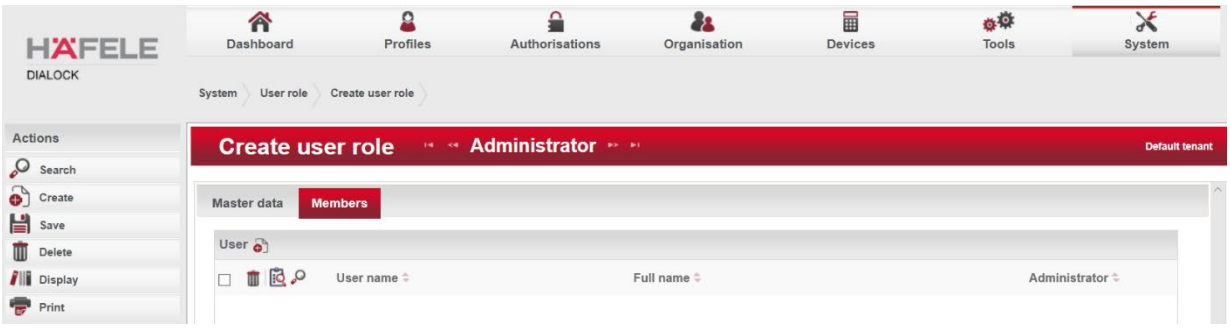
You can also create new user roles. To do this, click on “**Create**” in the list of user roles under “**System \ User role”**.



Here you issue a name for the **Role name** and the authorisations for the users who are assigned this role.

Save your selection. 

Under “**Members**” you can now assign the users for this user role again (as described in the previous chapter).

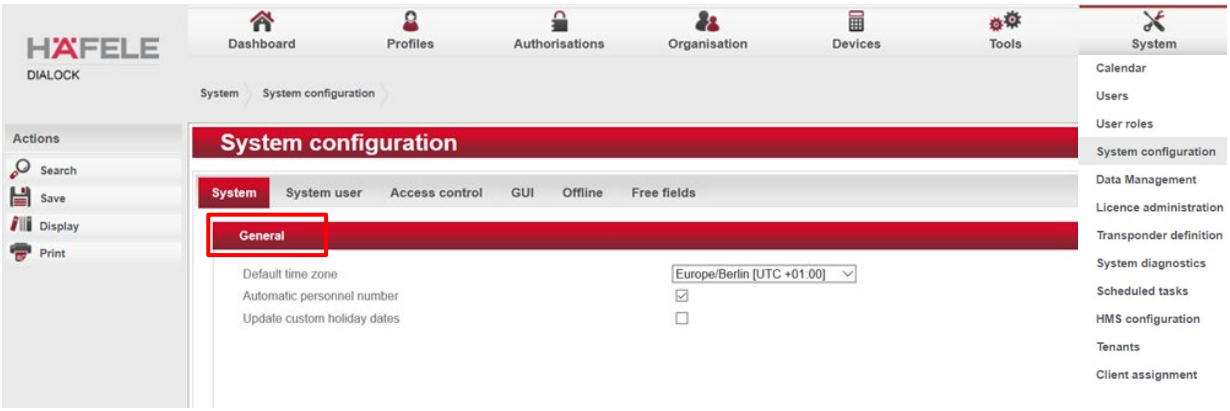


5.7.4. System configuration

The configuration of the Dialock software is accessed using **System > System configuration**.

5.7.4.1. System

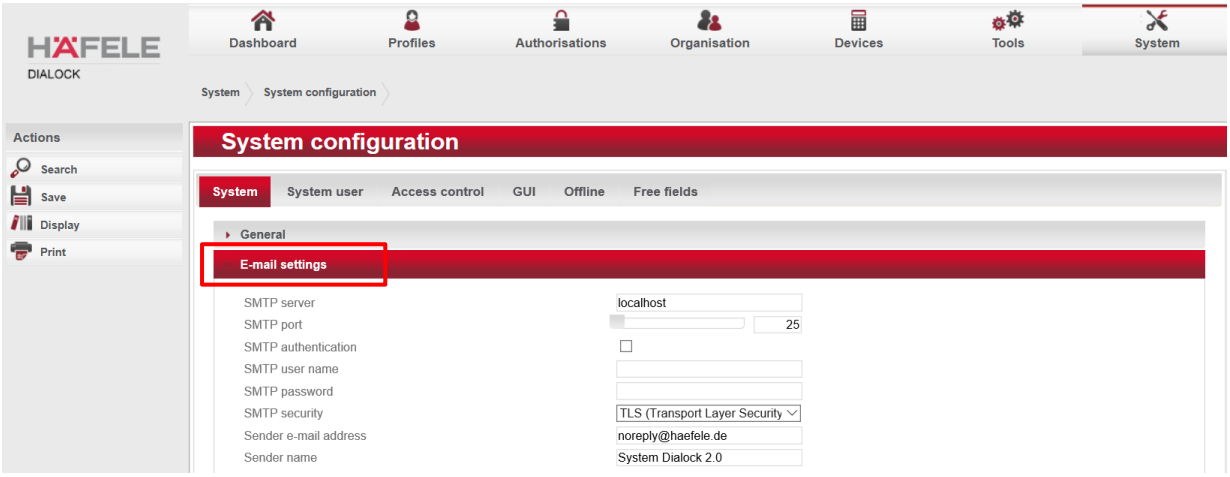
In the “**System**” tab under **General** you determine the **Time zone** to be used by Dialock by default by selecting from the drop-down menu.



If the personnel number is to be allocated automatically when recording personnel data, activate “**Automatic personnel number**”.

Update custom holiday dates must be used if self-defined holidays are repeated annually on the same date.

Enter the e-mail send parameter to be used by the system here under “**E-mail settings**”. This address is used by the system for sending e-mail messages.



5.7.4.2. System user

The password prerequisites are defined in the “**System user**” tab of the **System / System configuration** menu.

Here you determine the minimum **Length** and duration of the **Validity** of a **Password**.

Here you define the maximum number of **Login attempts** that a used can make before he/she is blocked.

Under **Password guidelines** you define how a user has to create his/her password.

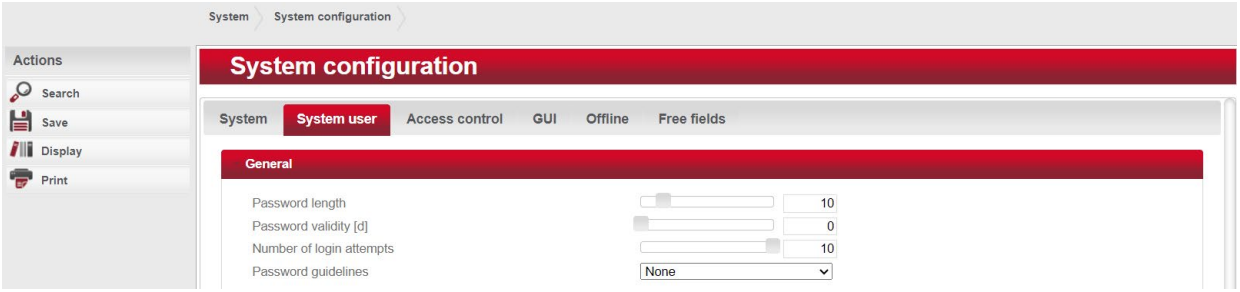
None:
The user can enter a password with any format.

Limited:
The password must be alphanumeric.

Strict:
The password must contain alphanumeric characters, special characters and upper and lower case.

The name of a system user is generally excluded by Dialock, also as part of a password.

The values in the following illustration represent the default setting of the Dialock Software 2.0 (from Version 8.4) in a new installation. These values are not changed during updates to existing systems.

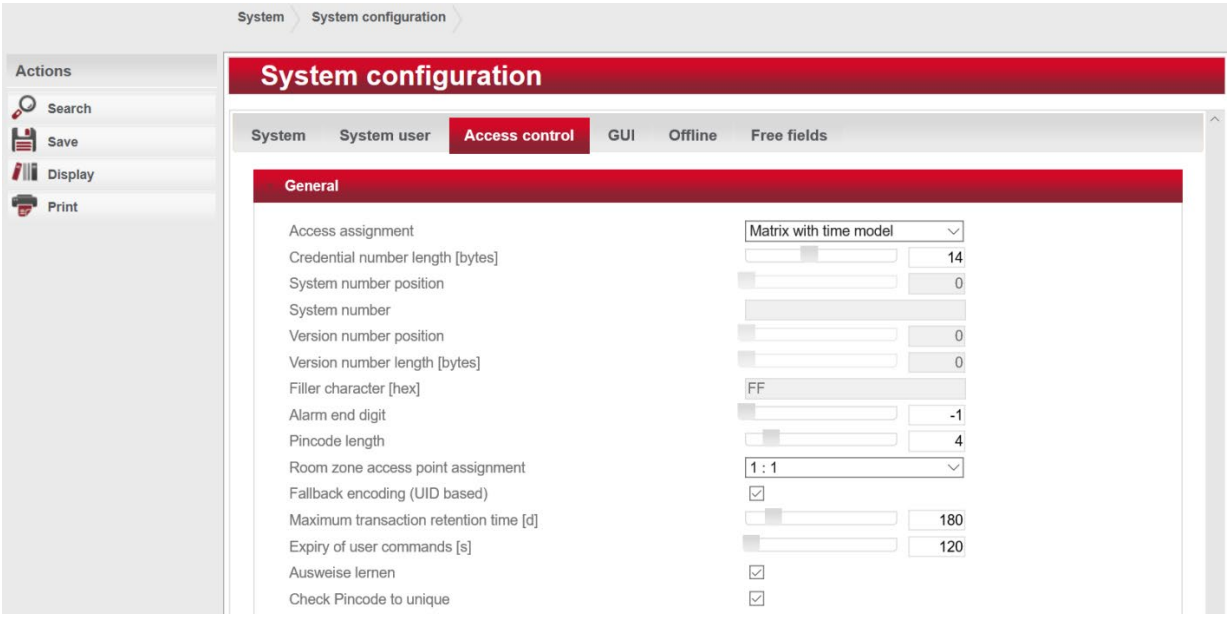


5.7.4.3. Access control

Basic parameters for access control are defined in the “**Access control**” tab in **System/System configuration**.

The possibility of allocating authorisations is set under “**Access assignment**”. Changes are only possible within the scope of the licence and should only be made by trained personnel.

Note:
Dialock is not downwards compatible. Once the access allocation **n to m** has been set, it cannot be changed back.



The global length of the transponders in bytes in the system is defined under **Transponder identifier length**.

The position of a fixed system number in the transponder is set under **System number position**.

Specify the **System number** here that you will use if necessary.

The position of a fixed version number in the transponder is set under **Version number position**.

Under **Filler character** you define a character with which transponder IDs that are too short will be padded out to the defined length.

The **Alarm end digit** specifies a number that can be added at the end of the PIN code in the event of an attack. A value of -1 deactivates this function.

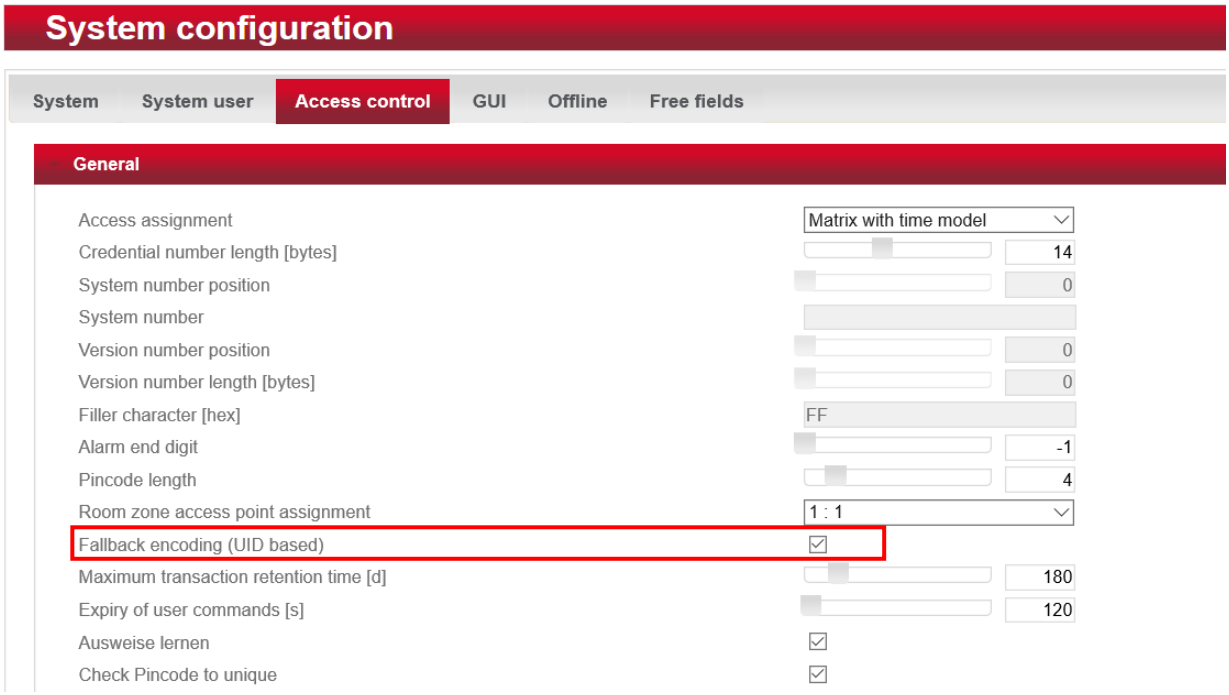
The number of digits in the PIN code is defined in **PIN code length**.

Room zone access point assignment
The number of authorisations per access point is specified with the setting “1 to 1”. The "n to m" setting makes it possible to assign access points via room zones which can then be authorised.

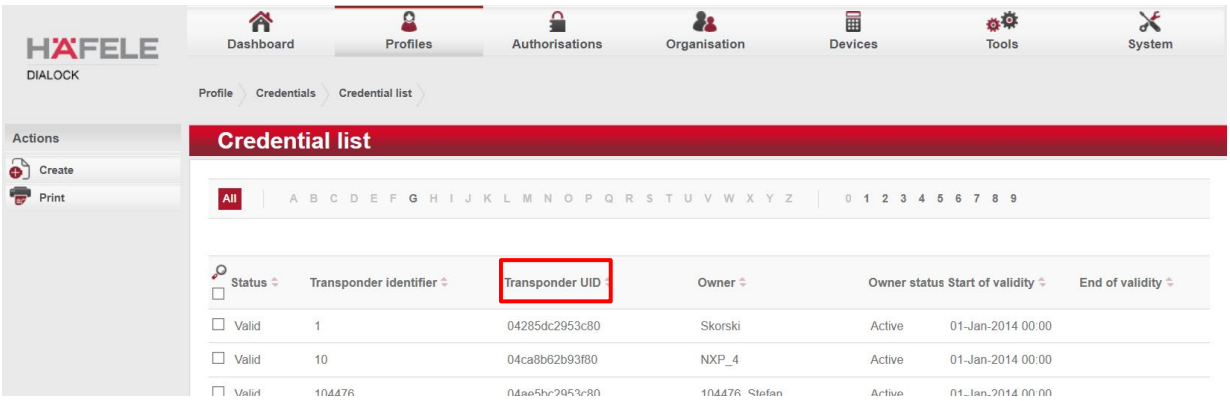
Note:
If the “**n to m**” setting is activated, you cannot change back to “1 to 1” assignment.

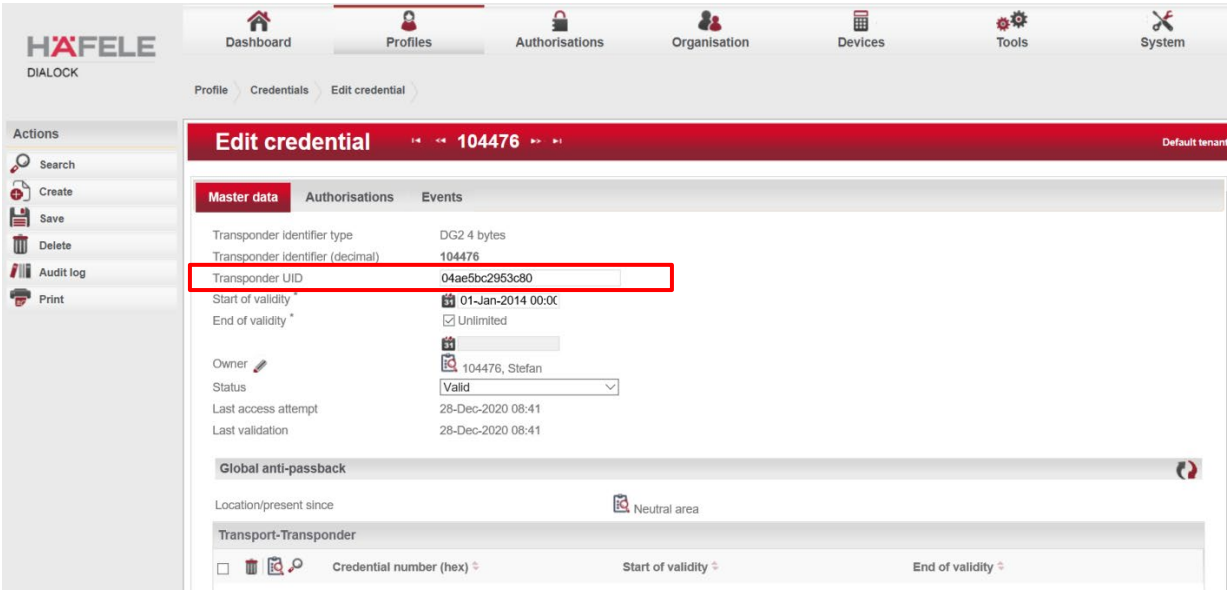
If **Fallback encoding** is activated, after a failed attempt to read the token, the online reader will determine the UID of the transponder and use it to create the assignment to the person and therefore their authorisations, and transfer all of this data to the transponder again.

The function of the fallback encoding is activated globally in the system configuration.



If the relevant option is active, an additional input field for the transponder UID is also displayed in the relevant locations, and also made visible in the search list





Under **Maximum transaction retention time** you set the number of days for which Dialock should save the transactions. 0 means that the transactions are never deleted.

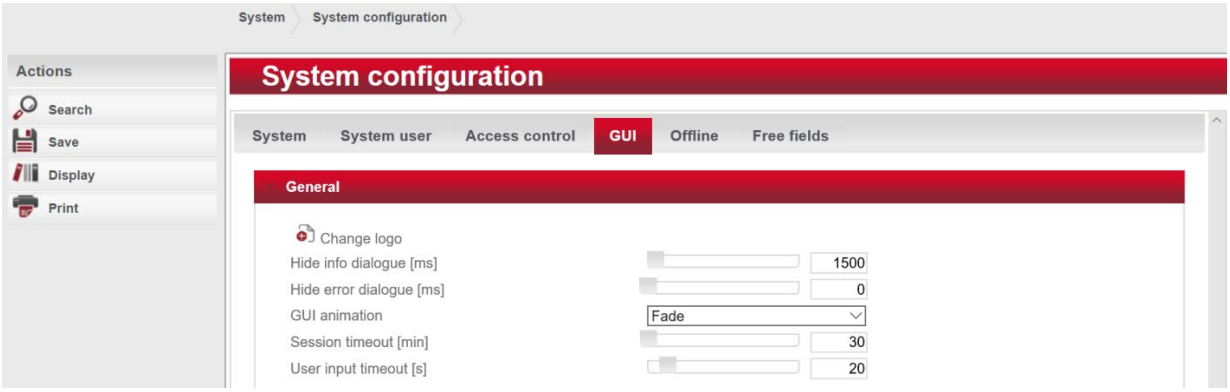
Under **Expiry of user commands**, the user can transmit telegrams to a terminal in different locations. It is pointless executing or transmitting certain telegrams if they could not be executed / transmitted for a long period because the device was disconnected, for example. You can therefore define here how “old” telegrams such as this are allowed be before they are no longer processed. A value of “0” deactivates the check.

If the **Learn IDs (transponder)** option is selected, when a transponder from another system is presented, an entry is generated in the database which allows the transponder to be directly added to a person.

Selecting **Check Pincode to unique** prevents the same PIN codes from being assigned to several persons.

5.7.4.4. GUI

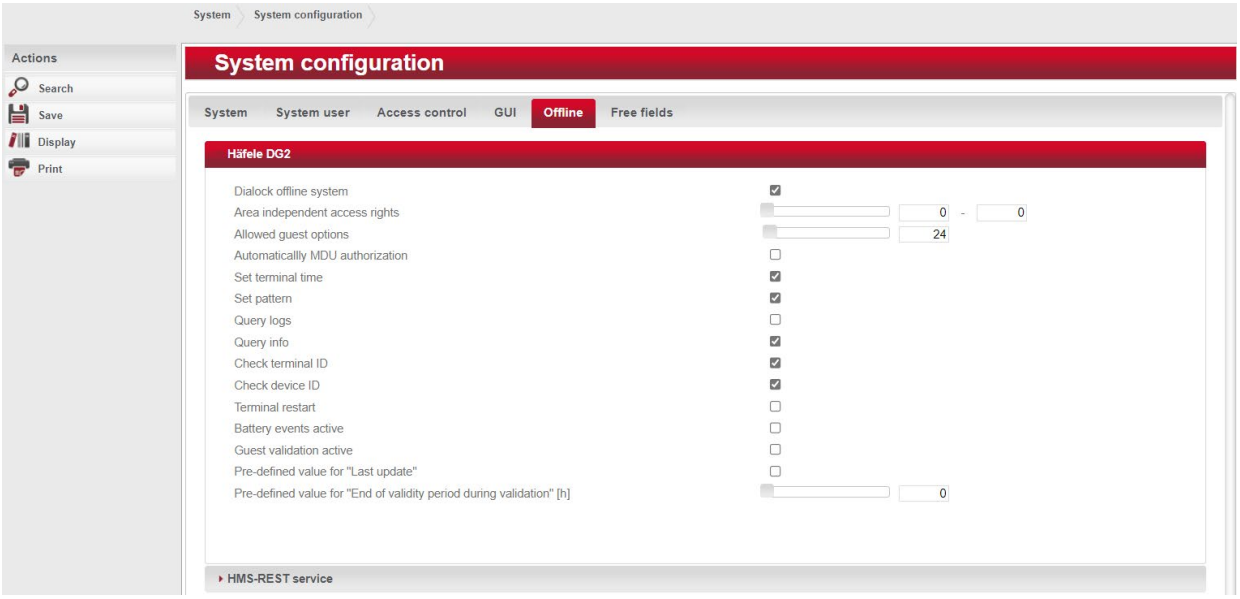
The parameters for the GUI design are defined in the “**GUI**” tab of the **System/System configuration** menu.



Here you can **Change the logo** and determine the duration for which **Info and error dialogues** are displayed. Select the required **GUI animation** in the drop-down menu and determine the time after which a user is logged out by the system in **Session time-out**.

5.7.4.5. Offline

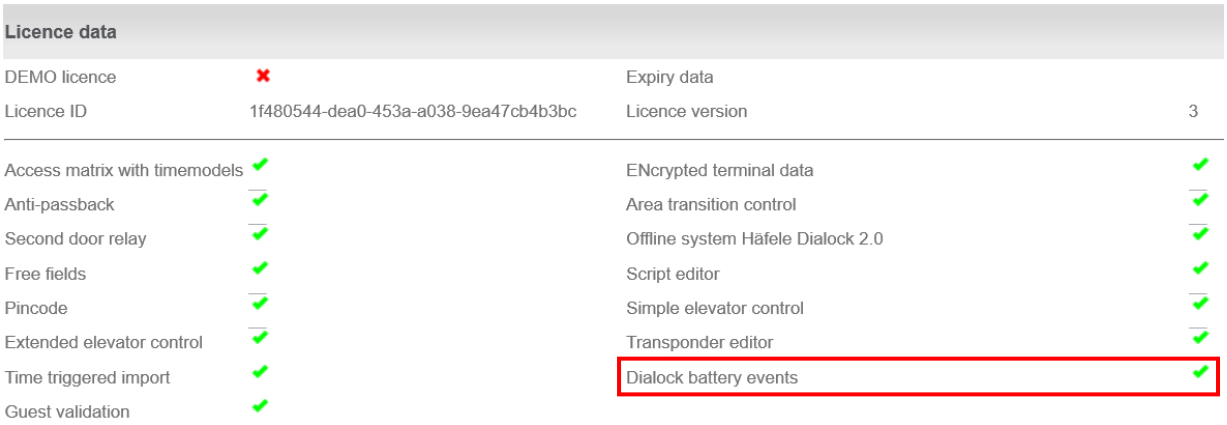
In the **Offline** tab of the **System / System configuration** menu, on the **Häfele DG2** screen you can activate/deactivate the **Dialock offline system** and set associated parameters.



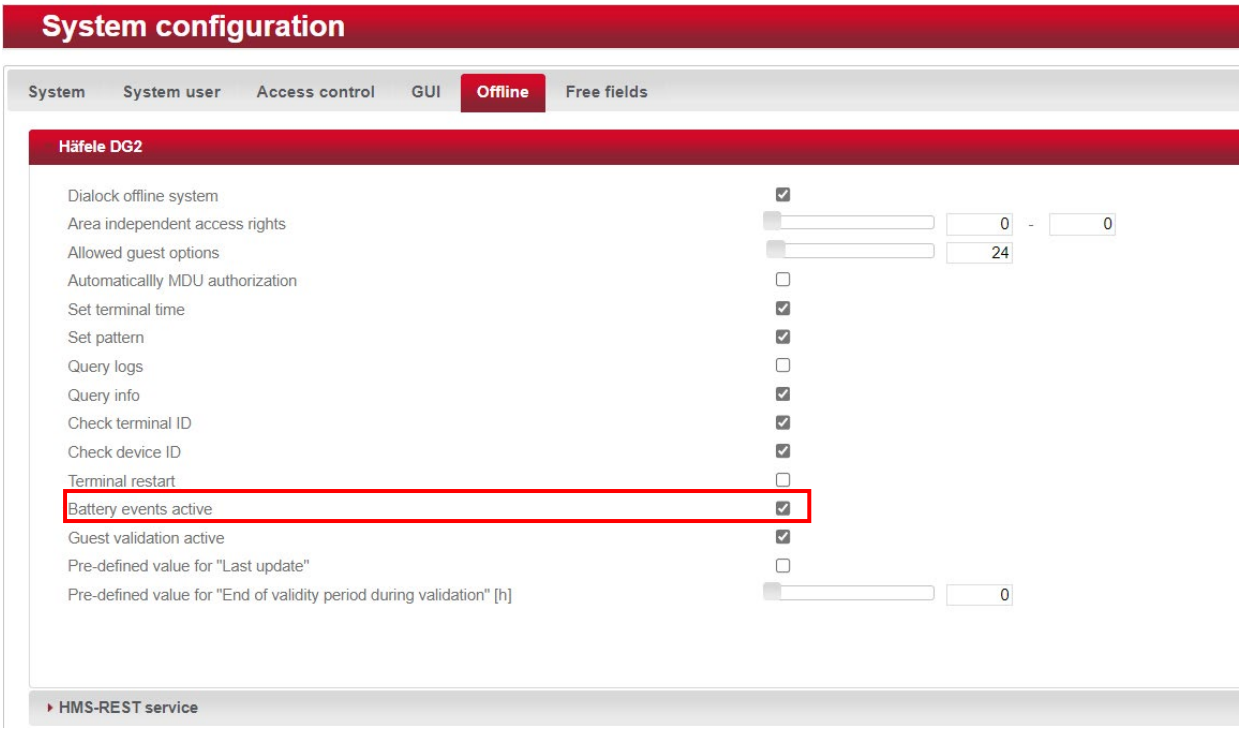
Note:
Some of the changes that are possible here can lead to malfunctions in a system that is already operational.

If **Battery events** is activated, these can be copied back into the system via the transponder during validation at the online terminals.

Configuration:
The battery status events function is an option that requires a licence, and requires the **Dialock battery events** licence option. Activation should only be carried out by trained personnel.

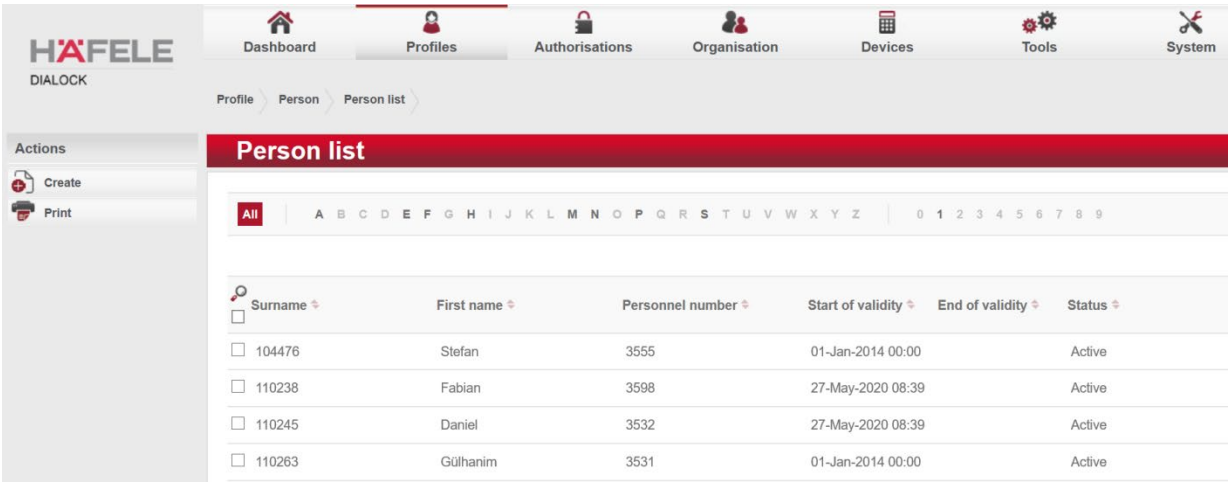


The function itself is activated globally in the system configuration.



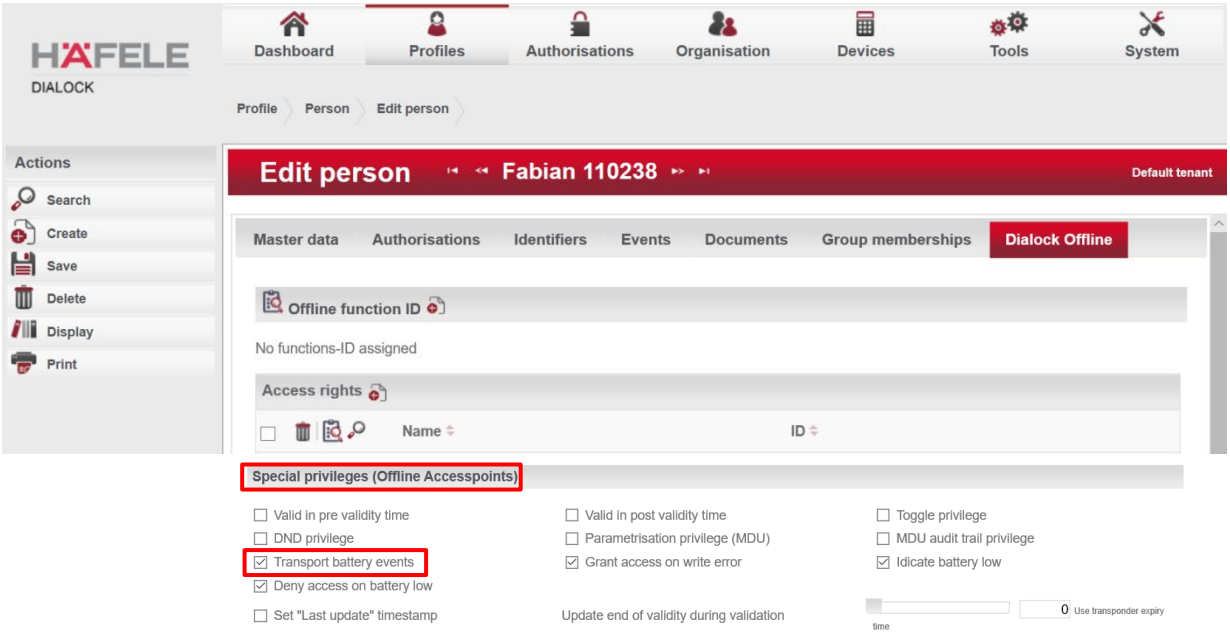
To activate this function, the “**Transport battery events**” setting must **also** be set for those persons who are to transport the messages.

The person list is accessed via the **Profiles / Persons** menu.



After selecting the required person, I can use “**Edit person**” to make person-related settings.

The setting can be made in the “**Dialock Offline**” tab under **Special privileges** (scroll all the way down).



Please select the “**Transport battery events**” setting here.

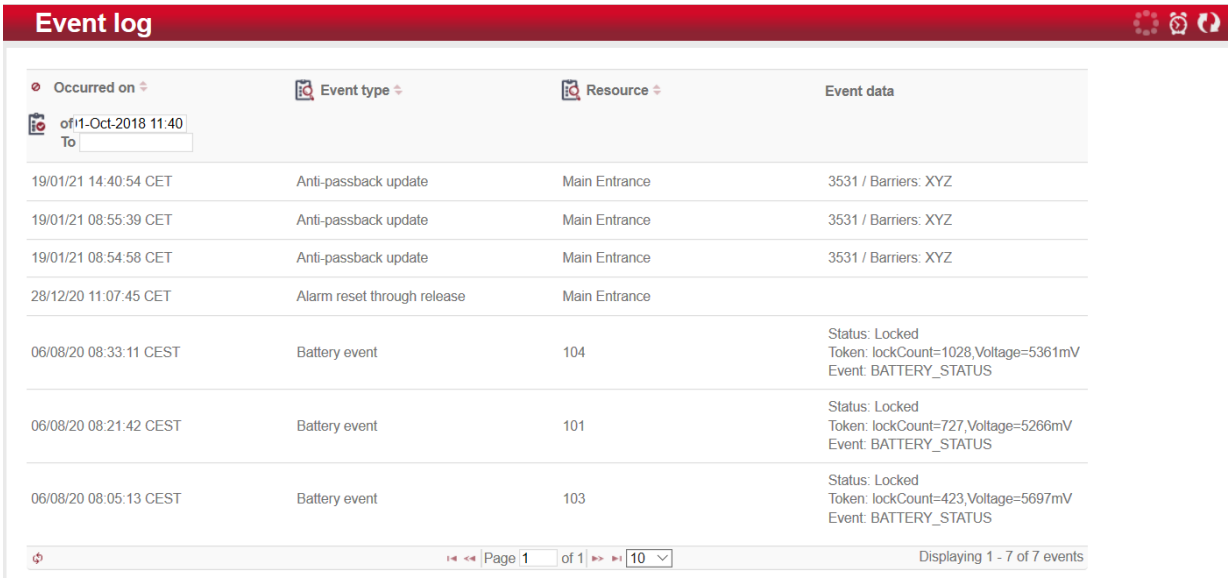
The battery events to be transported back into the system via the user transponder are entered into the event table, where they can be evaluated like any other transaction or reacted to with an event control. The “**Occurred on**” date is the date on which the offline component wrote the message to the transponder (Write Time).

The individual battery status values are translated into the following event types:

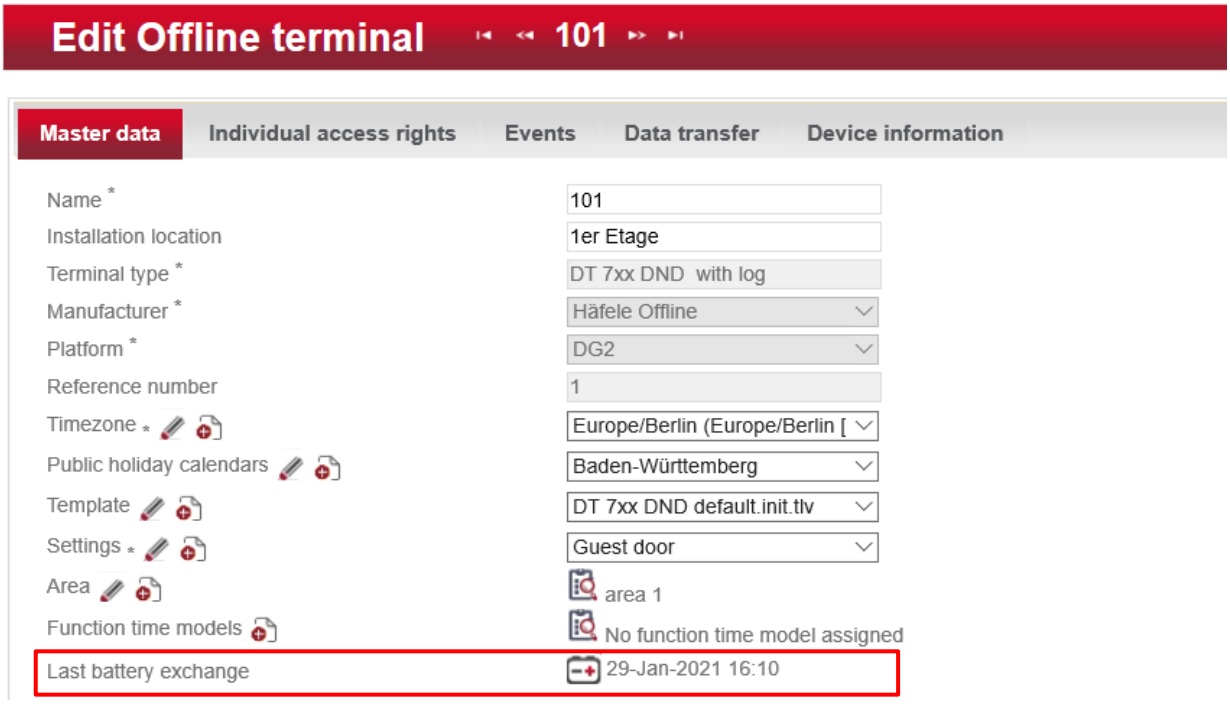
Battery status value	Event type
0	Battery OK
1	Battery low
2	Battery very low

With the audit trails, the following additional information is displayed in addition to the event type:

1. Name of area to which the offline component is assigned.
2. Date when the component detected the reported battery condition.
3. Use counter since the detection date.
4. Remaining battery capacity in percentage of anticipated maximum charge



If the battery of an offline component is changed, the system user of Dialock 2.0 can log this on the master data page of the respective offline terminal. The date of the last logged battery change is also displayed there.
If you click on the battery symbol a dialogue appears which indicates to the user that the logging of a battery change leads to all battery status events with a date older than the point in time of logging the change being ignored, i.e. discarded. if the user confirms with “yes”, the battery change is noted.



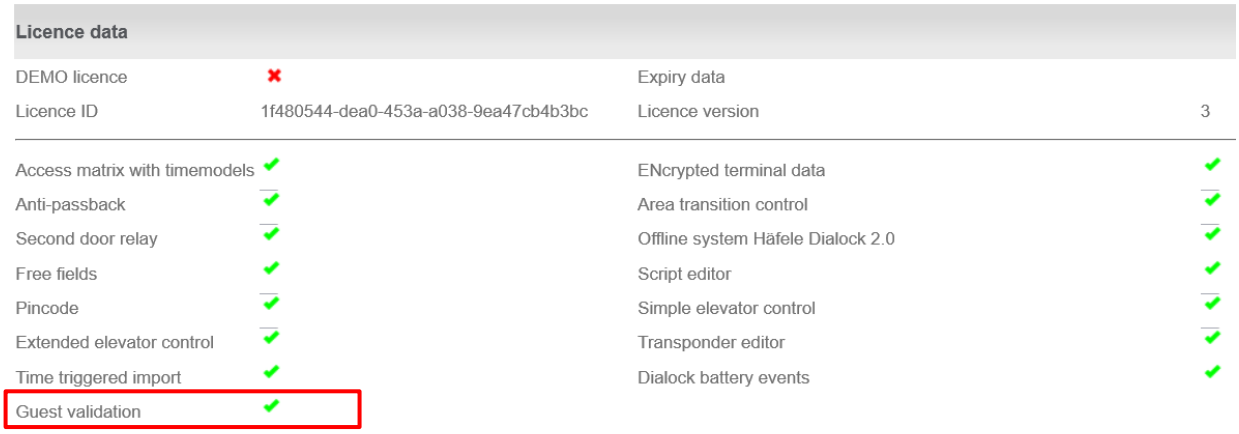
This logging is entered into the audit trail together with the relevant system user when the “**Battery replaced**” transaction takes place.

When **Guest validation active** is activated, the validation of hotel guest transponders at the configured validation readers is activated.

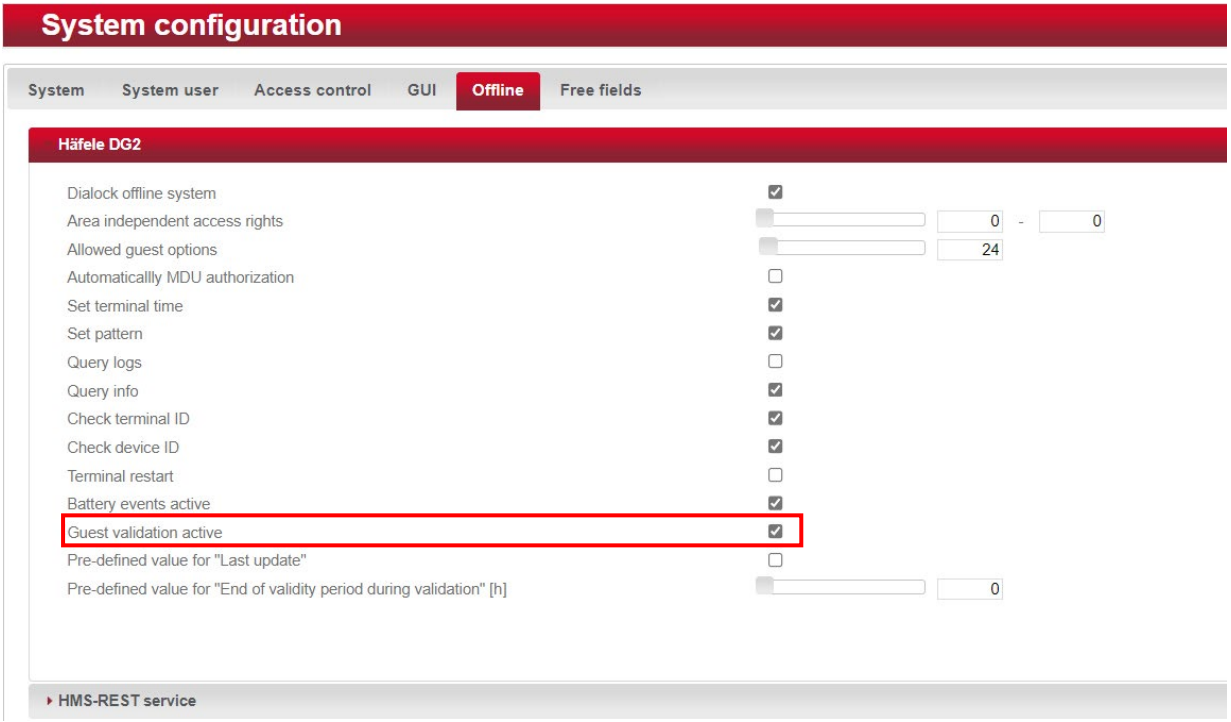
The transponders of hotel guests can be coded via the validation function of the DG2 validation readers.

Functionality:
If Dialock 2.0 is notified of a check-in via the HMS interface, in addition to his basic rights and booking options, the hotel guest who is created is also assigned the individual access right for the relevant room. This makes it possible to write the complete offline authorisations to a guest transponder at the validation reader.

Configuration:
The function is an option that requires a licence and requires the **Guest validation** licence option.
The activation should only be carried out by trained personnel.



The function itself is activated globally in the system configuration.



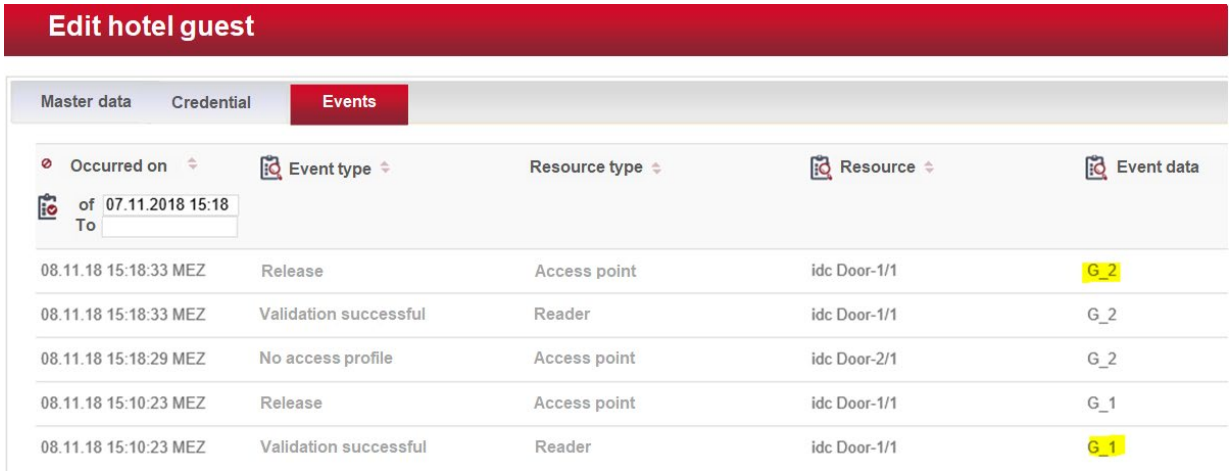
Of course, the guest must have an appropriate authorisation at the validation reader to validate the guest keys.

Once the **Guest validation** option has been activated, the following scenarios are possible:

Room move

In the event of a room move, the guest would like to change room before or during his stay. The HMS sends an RM (room move) command with the new room number. When guest validation is active, the previous hotel guest is retained and receives an additional transponder with the new token and the individual access right to the new room.

The previous transponder remains valid but is validated in an identical way to the new one. This means that when the old transponder is used for the first time at a validation terminal, the new information (token, creation time stamp and rights) are updated on the transponder and the old transponder is therefore recoded. This procedure can be seen in the audit trail, since a last successful validation is recorded. From this time forward, the old transponder identifier can no longer appear in the system.



In the above-mentioned example, the hotel guest was rebooked from room 1 to room 2. The same physical transponder was used for the transactions. During the first validation after the room move, the transponder is still recognised as **G_1** but is recoded to **G_2** with the successful validation. Subsequent access attempts are therefore registered in the system as **G_2**.

Stay extended (extended stay)

In the event of a “Stay extended”, the guest would like to extend the duration of his stay. This can take place before the check-in or while the guest is already in the hotel. This special case is dealt with via the RM (room move) command, whereby the room numbers (old and new) are identical. When this takes place, the modified check-out date is exclusively applied to the guest and his identifier.

Because of the guest validation at the online terminals, the Dialock Application Container (DAC) with the HostKey application is also automatically written again, and the modified validity is therefore also activated for the offline terminals.

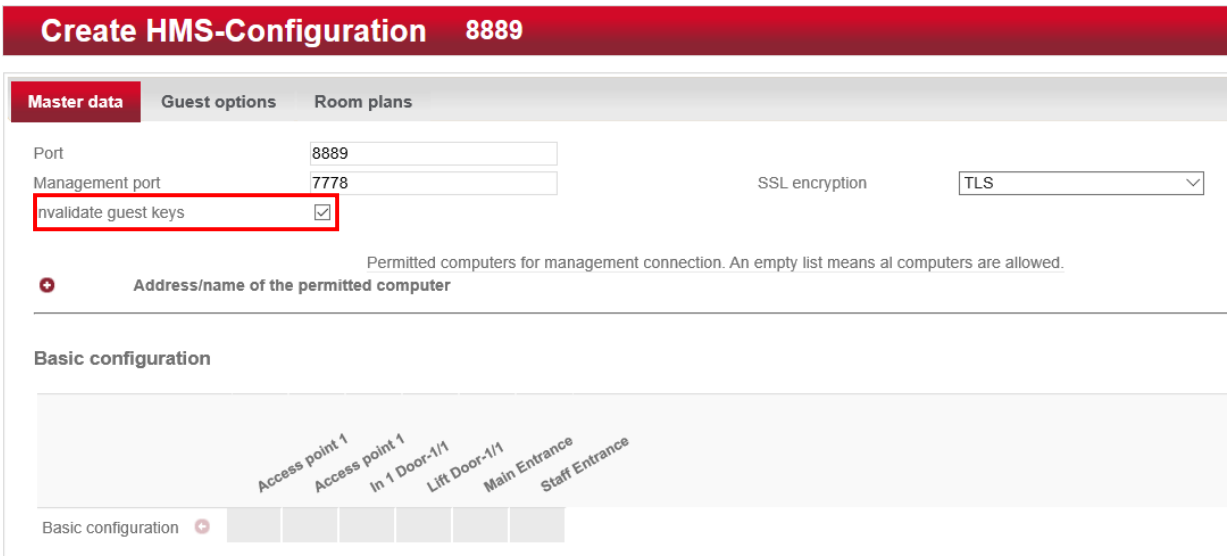
Key deletion (replacement transponder)

If a hotel guest loses his transponder or it becomes defective / destroyed, the guest is issued with a new transponder. This scenario corresponds to a new check-in to this guest’s room.

732.29.430
HDE 20.12.2023

Previously, this case resulted in the authorizations of the previous guest being downgraded to the authorisations defined in the basic configuration of the HMS configuration, but the transponder therefore remained valid, particularly as far as the offline data for the Dialock system is concerned.

In order to increase the security of the overall system, this case can now be modified by setting the “Invalidate guest keys” parameter in the HMS configuration.



This affects the scenario by also downgrading the authorisations to the basic configuration. However, it is not the defined time model from the matrix of the basic configuration that is used for the authorisation, but a time model that is temporally invalid (NEVER). This has the effect that the transponder does not gain access at the online reader, but is still validated. The offline authorisations are removed as a result of this validation.

IMPORTANT:

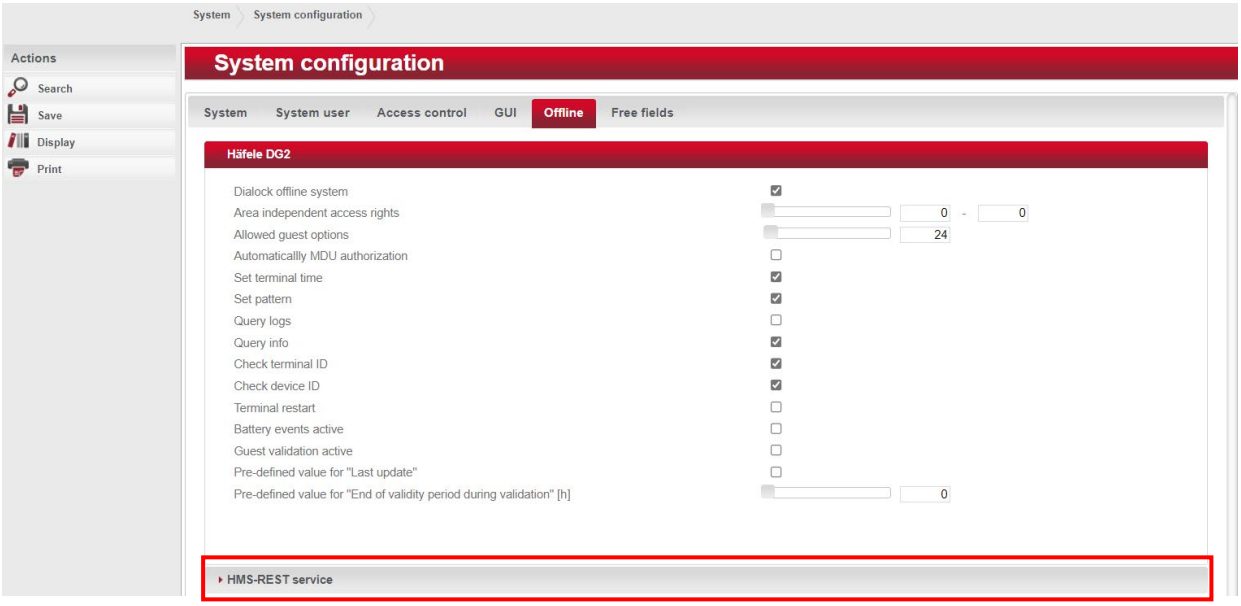
1. THE BASIC CONFIGURATION MUST INCLUDE THE VALIDATION READER

2. THIS CHANGE DOES NOT JUST AFFECT THE SPECIAL CASE OF REPLACEMENT TRANSPONDERS, BUT ALSO ANY CHECK-IN OF A SUBSEQUENT GUEST. UNFORTUNATELY, NO DISTINCTION CAN BE MADE BETWEEN THESE CASES ON THE BASIS OF THE HMS DATA.

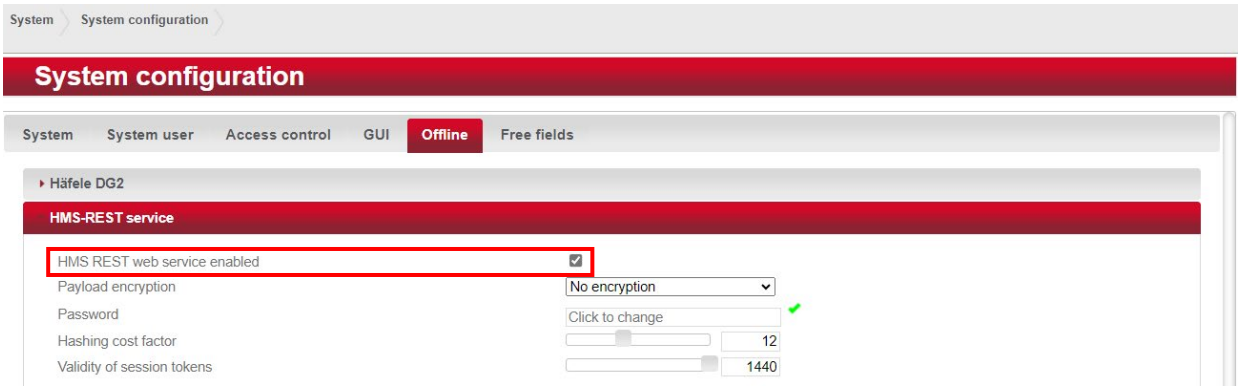
HMS-REST Service

This is a communication interface for supporting web-based apps (PWA).
The HMS-REST service is used for data communication between the Dialock Software 2.0 and the HMS. This makes it possible to query the terminal list with the individual locking authorisations and options in the Dialock Software 2.0.

To configure the REST interface, scroll down to the bottom and select the “**HMS-REST Service**” sub-menu.



Note:
If PWA keys are being used, the HMS-REST service must be activated.



The "**HMS RESET WebService**" service can be deactivated using this option.
With subsequent queries the message "404 – Not found" will appear.

Additional data encryption in the request and response body can be activated using "**User Data Encryption**". This setting is also binding for the client. If must then process all queries accordingly.

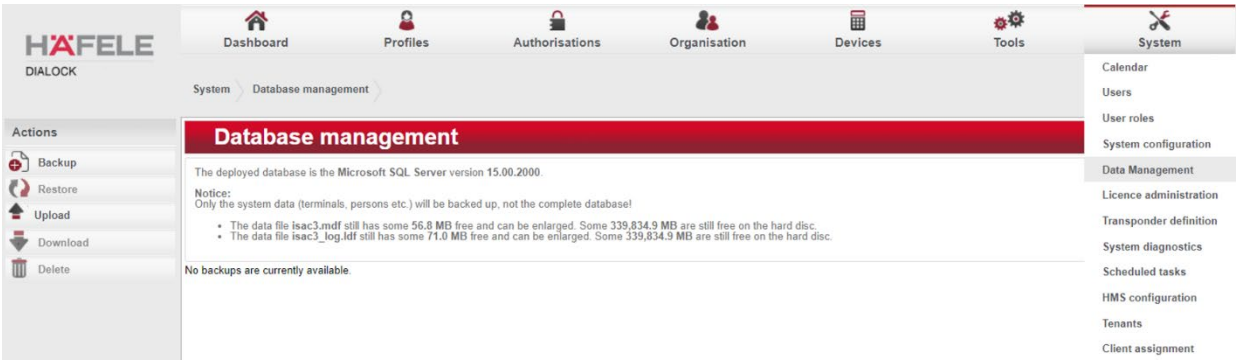
To issue new authentication tokens, the server and the client use a common "**Password**".

The issuing of the tokens is also influenced by the "**Hashing Cost Factor**". The server and client use a cost factor. This must be identical. The amount of the cost factor is determined using this option. The duration of the derivation key increases with the amount of the factor.

The duration of validity of the authentication token is defined under "**Validity of the Session Key**".

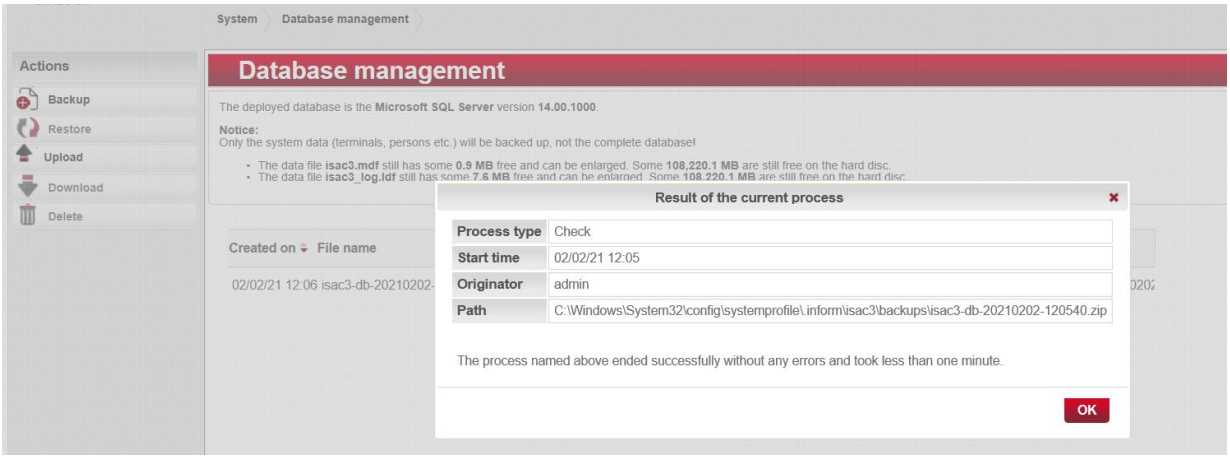
5.7.5. Data Management

In order to create a backup of the database or restore a previous backup, go to menu **System \ Database management**.



Basic & important note:
The database management is administered on a project basis. These are abstract objects which are database-independent. In this way, they can be migrated from one database to another. The events are not backed up.
In other words, conventional backups still need to be taken!
The overall database must be backed up independently by the IT administration.
Each operator is responsible for backing up the database at IT level!

Click on “**Save**” in the menu on the left-hand side to back up your current database.

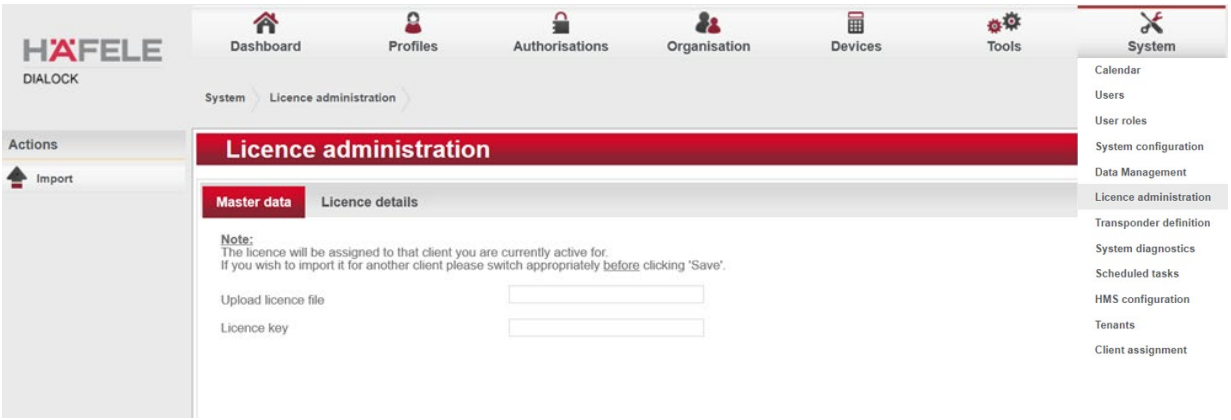


Dialock indicates the progress of the backup and notifies you of the result of the data backup in another dialogue.
The last file to be backed up is shown at the top of the list according to the default setting.

If a backed-up database is restored again, mark the required backup in the list and select “**Restore**” from the menu on the left-hand side. Once the restore is complete, you are automatically logged off by Dialock. Here too, the progress of the restore is indicated.

5.7.6. Licence administration

You upload the licence file that you have purchased under **System \ Licence management**. This file contains all licence-related settings such as the maximum number of master personnel records, access points, time models etc.

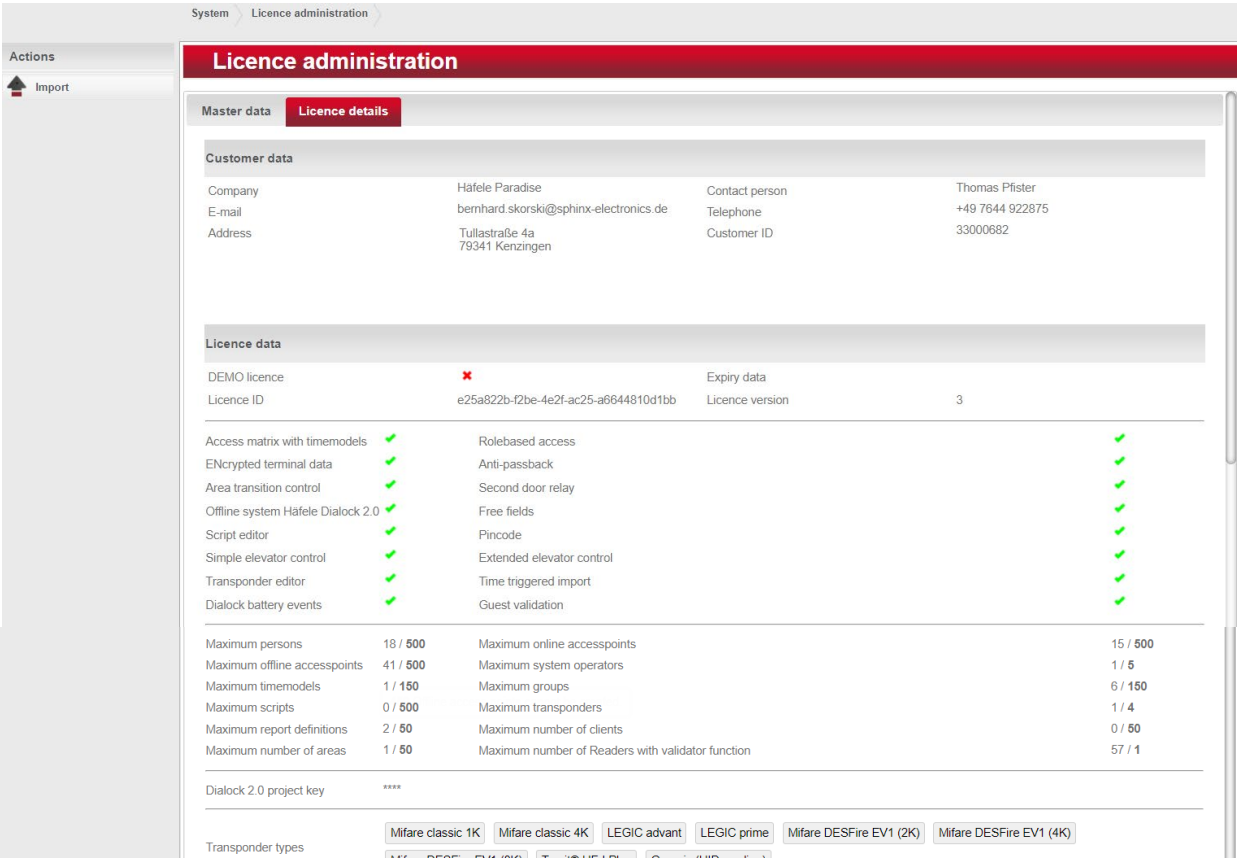


Click in the “**Upload licence file**” input field to upload your licence file and enter the associated licence key in the “**Licence key**” field.

Then click on “**Import**” in the left-hand action menu.

Save the results of this action. Save

The system then has all of the performance features in accordance with the software version that you have purchased, which you can call up under “**Licence details**”.



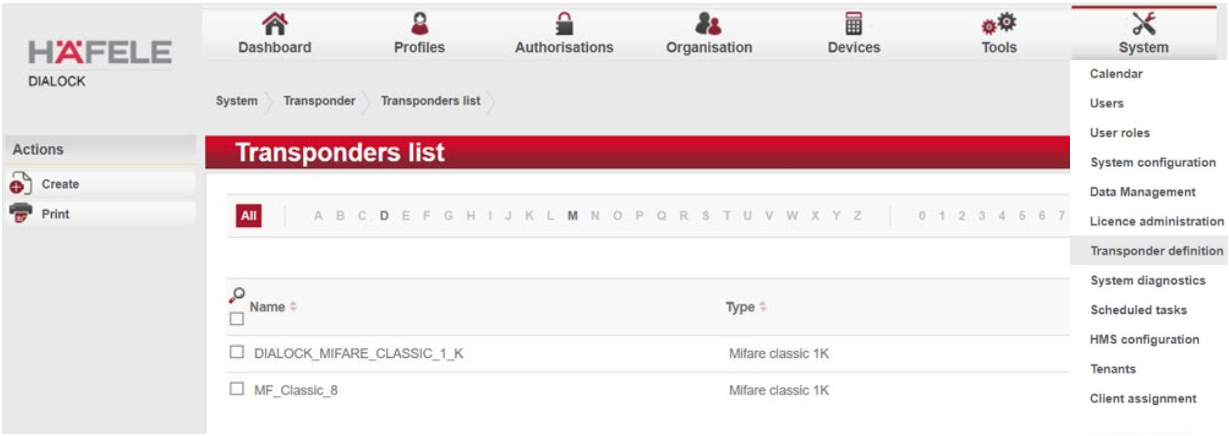
732.29.430
HDE 20.12.2023

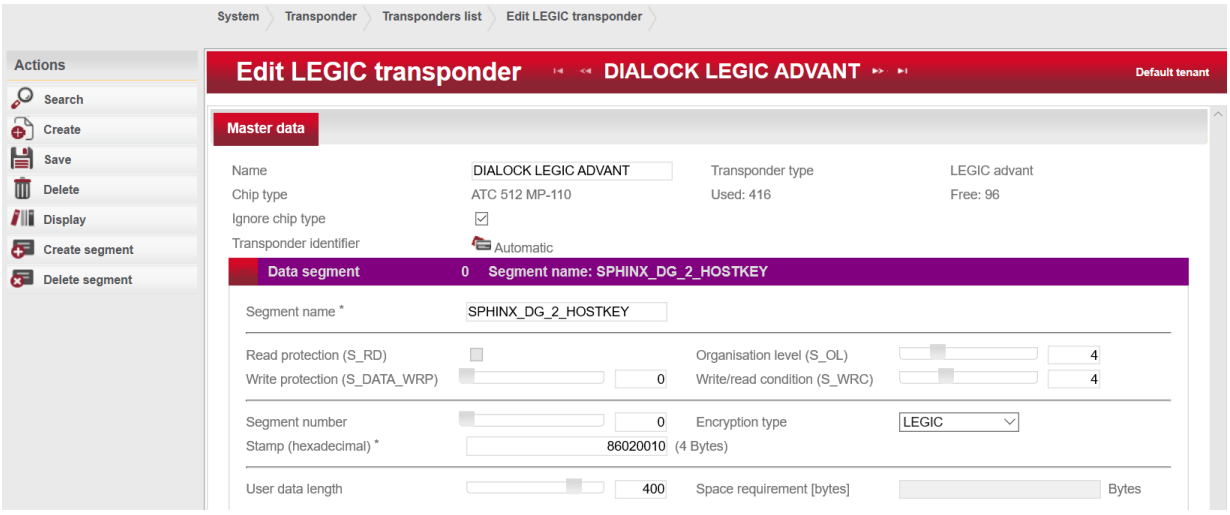
5.7.7. Transponder definition

Information about the **Transponders** that are available in the system is recorded in the **System / Transponder definitions** menu. The transponders are created when the licence is imported.

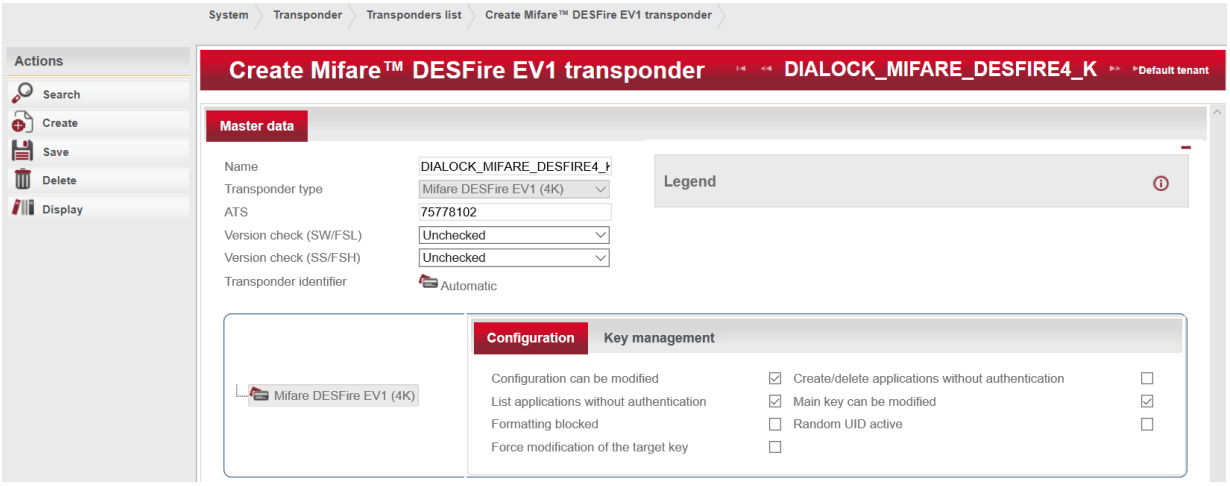
Note:
Changes are only possible within the scope of the licence and should only be made by trained personnel.

Some of the changes that are possible here can lead to malfunctions.

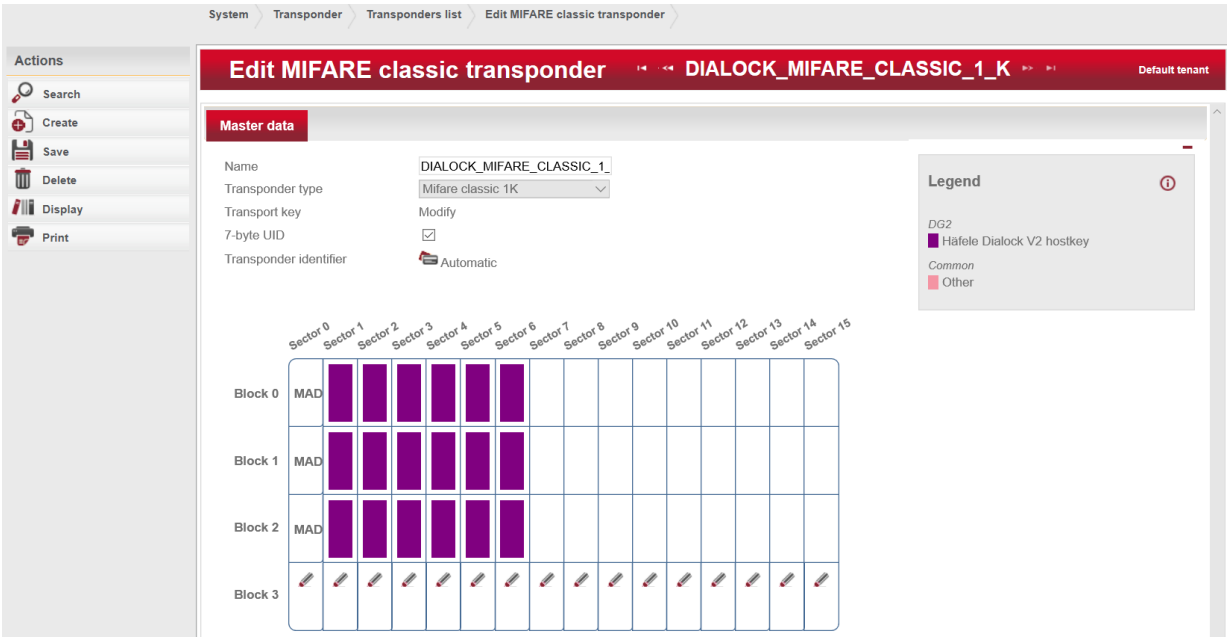




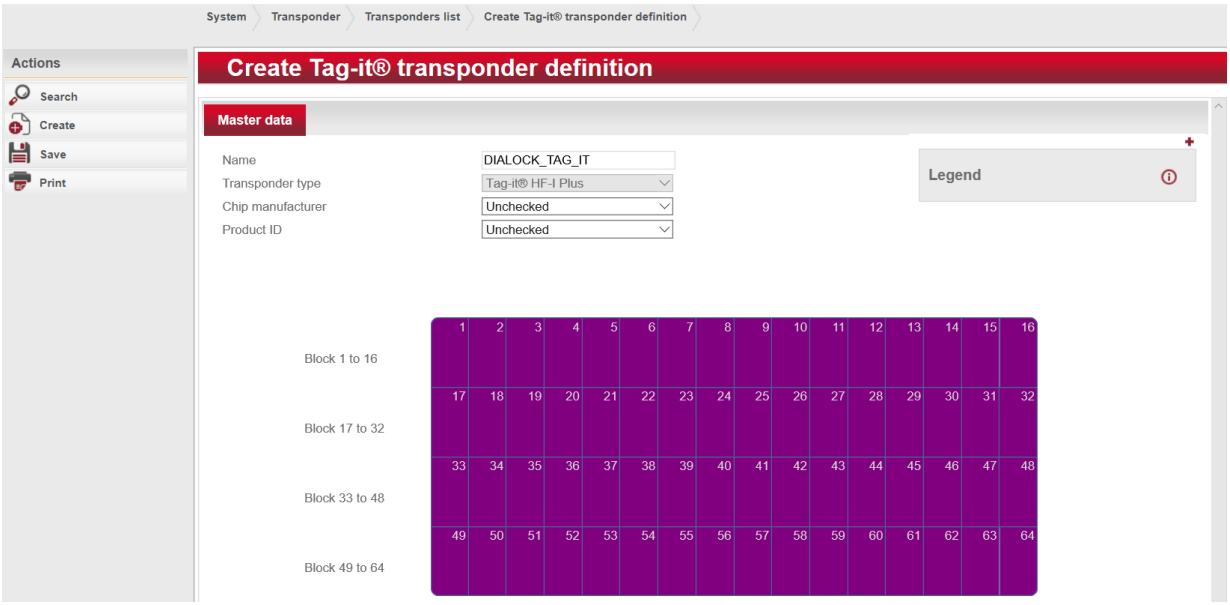
Example of Legic Advant transponder definition



Example of Mifare DESFire transponder definition



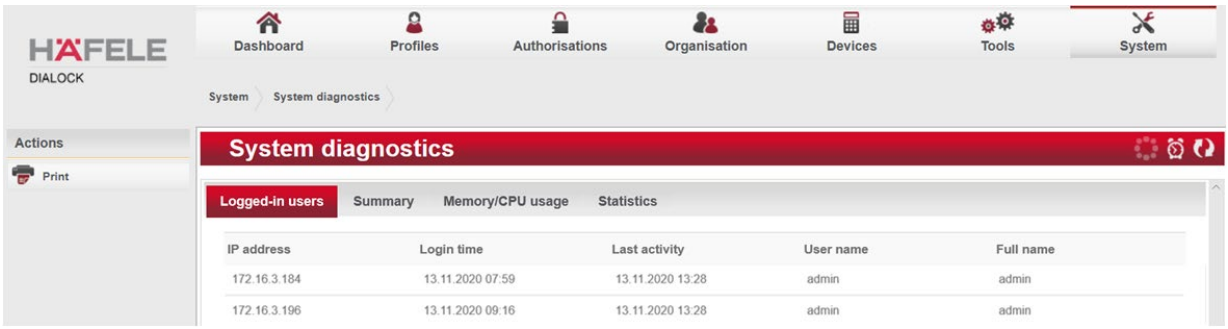
Example of Mifare classic transponder definition

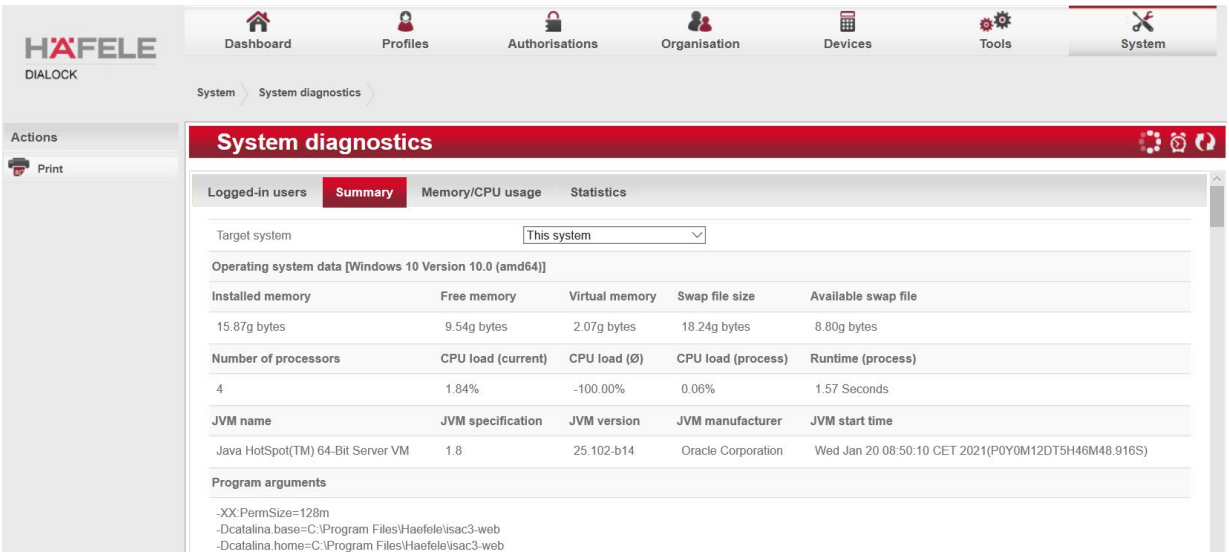


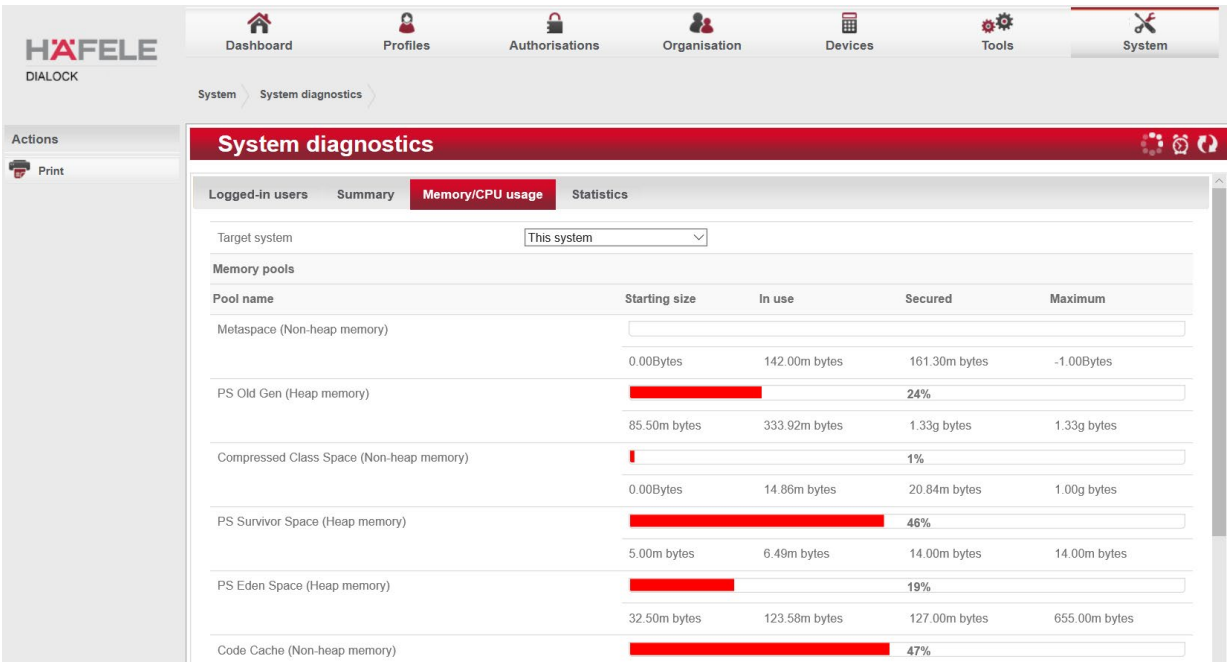
Example of Tag-it transponder definition

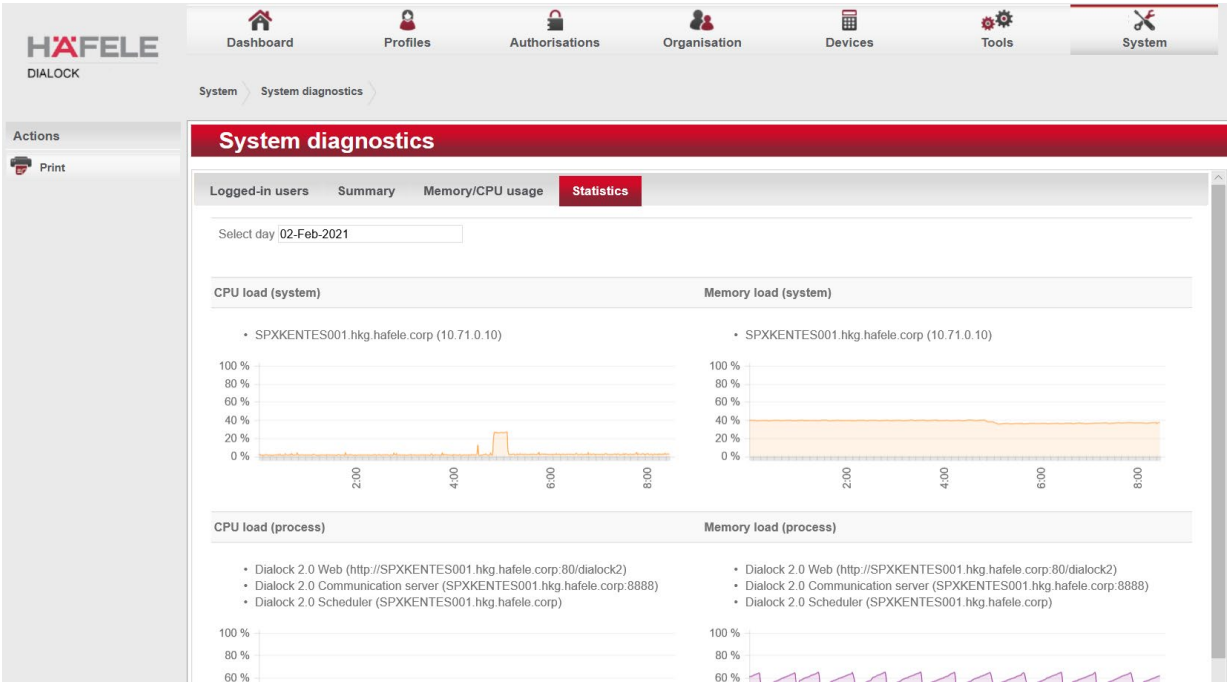
5.7.8. System diagnostics

Allows diagnostic data and statistics to be called up.









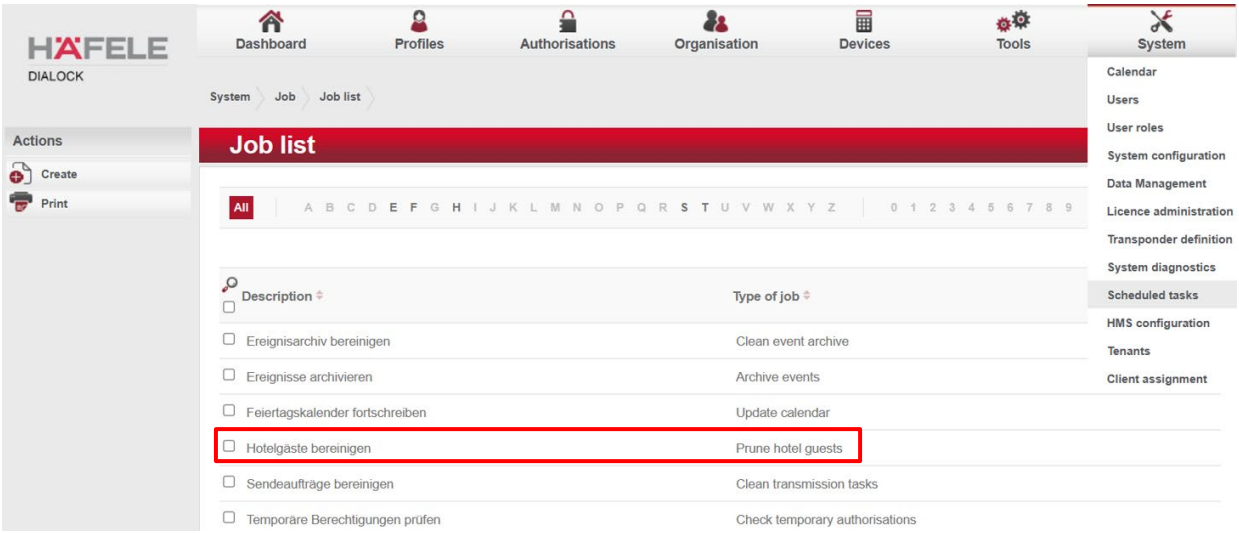
5.7.9. Scheduled tasks

Scheduled tasks are used to automatically carry out certain jobs once at certain times or at regular time intervals.

Certain job types are stored in the Dialock software 2.0 as standard.

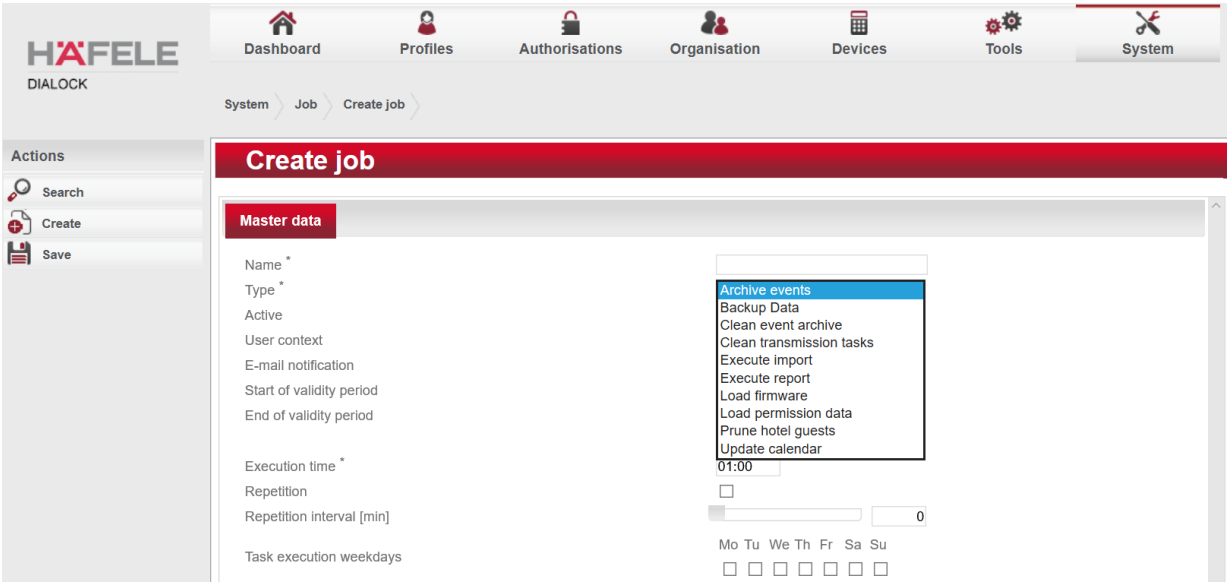
The **Job list** is accessed via the **System / Scheduled task** menu. This is where new jobs can be created or existing ones edited.

An existing job can be edited by selecting it.



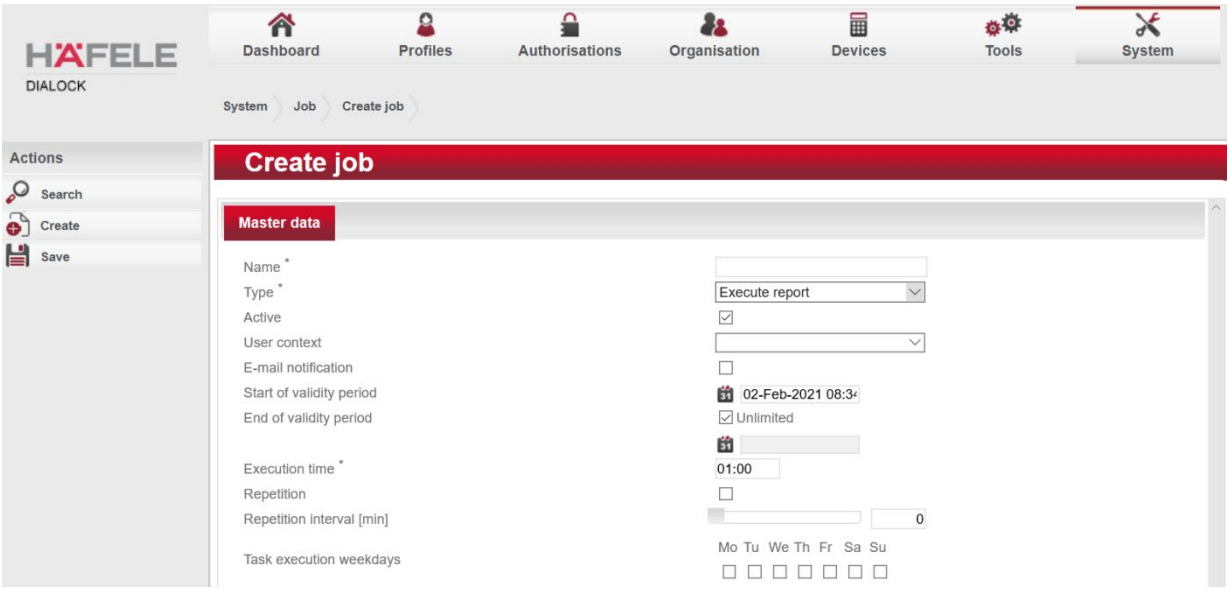
5.7.9.1. Create job master data

To create a job, click on “**Create**” on the left-hand action bar of the scheduled task list. This takes you to the job creation screen.



Give the new job a **Name**.

Select the required **Type** of the job from the drop-down menu.



Deactivate the “**Active**” check box if you would like to deactivate the job temporarily or permanently.

If you would like to receive a confirmation e-mail after a job has been carried out, activate the “**E-mail notification**” check box.

The **Start of validity** and the **End of validity** can be defined exact to the day or minute.

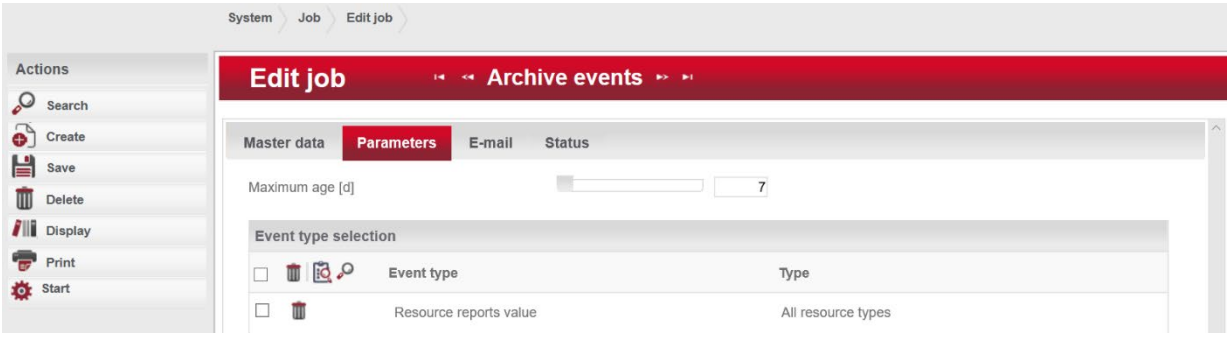
The **Execution time** determines the time when the job is to be executed.

If the job is to be executed every 10 minutes, for example, the “**Repetition**” must be activated and the “**Repetition interval**” set to 10 using the regulator.

If a job is to be executed on certain days, activate the relevant check box for “**Task execution weekdays**”.

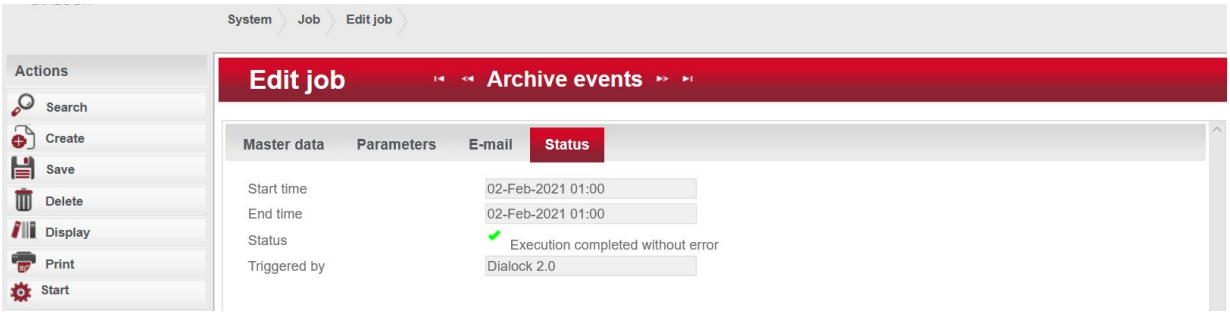
5.7.9.2. Managing the “Archive events” parameter

In the “**Parameters**” tab of the **System \ Scheduled task** menu you can also define after how many days the events are to be archived. You can also select which events are **NOT** archived but are to be deleted immediately.



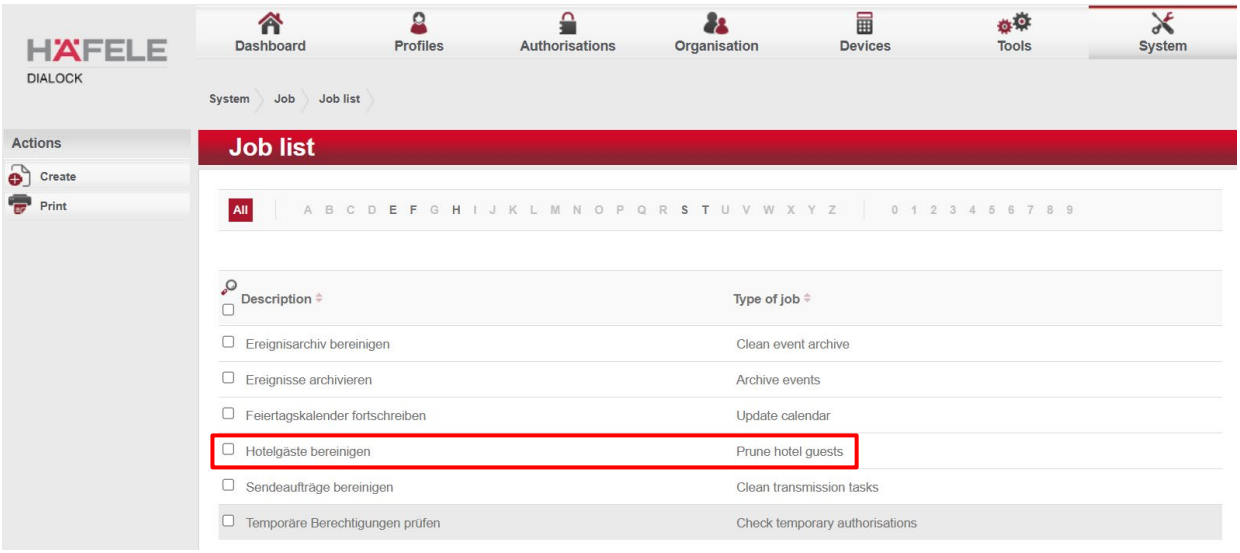
5.7.9.3. Status of jobs

In the “Status” tab of the **System \ Scheduled task** menu, you can see the **Start time**, the **End time** and the **Status** of the selected job. “0” means that the job has been executed as planned. The “**Triggered by**” field shows who started the job.



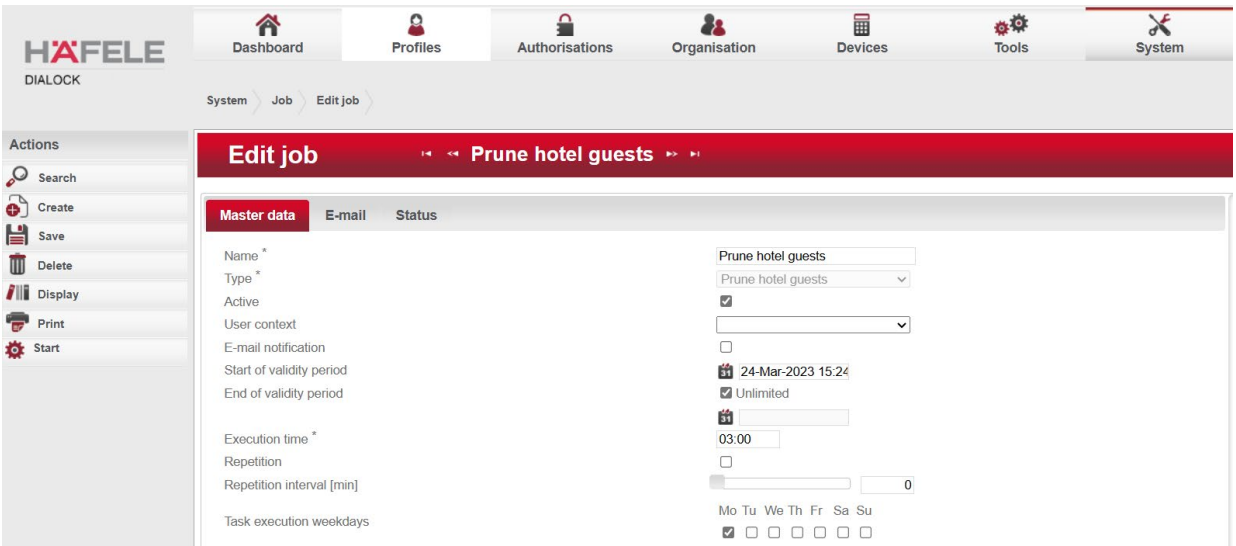
The “**Status**” tab depends on the selected **Type** in the master data tab of the job and is therefore not always available.

5.7.9.4. Example: “Prune hotel guests”



Experience from practice has clearly shown that the check-out function is not used in the majority of hotels, or not used in a reliable way. There is no problem with regard to authorisation, since the authorisations of the hotel guests are basically only valid for a limited time until the end of the stay. However, this data is then not deleted. Neither from the database of the Dialock 2.0 nor the internal memories of the online terminals.

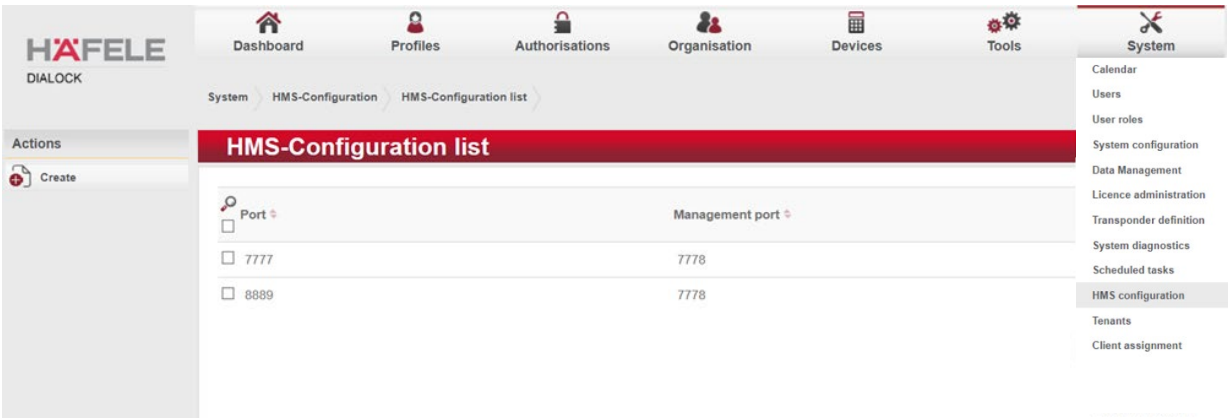
In order to solve this latent problem, a new scheduled task type has been created. This is created automatically by Dialock 2.0 after an update, and is set up in such a way as standard that all expired and/or blocked hotel guests are deleted from the database on Monday morning at 3am, and therefore also from the memories of the online terminals.



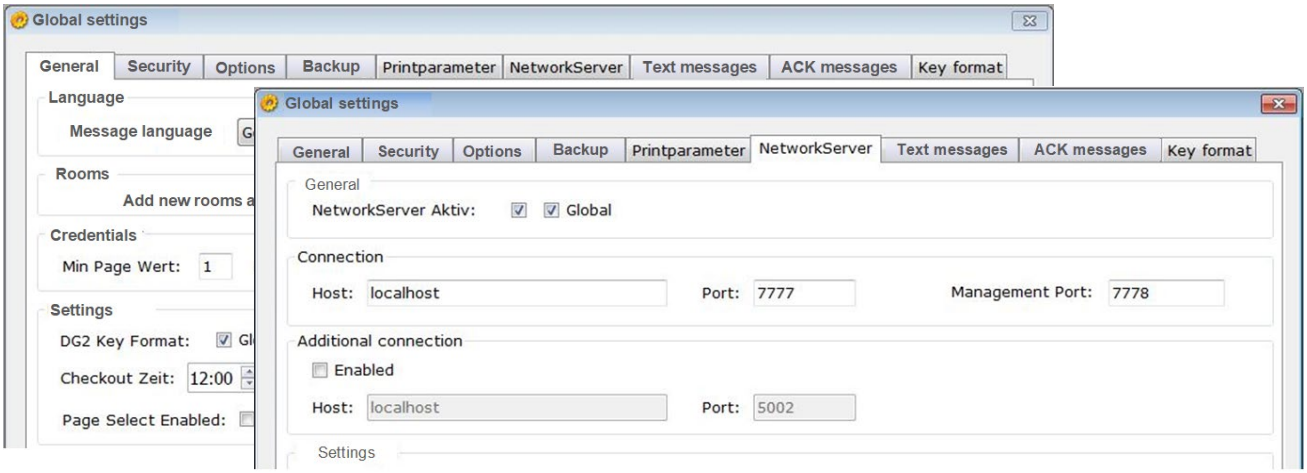
These parameters are freely adjustable, meaning that this task can run in the background without interfering with the procedure in the hotel.

5.7.10. HMS configuration

The parameters for communication between the guest key system (HMS interface) and Dialock can be set in the **System / HMS Configuration** menu.

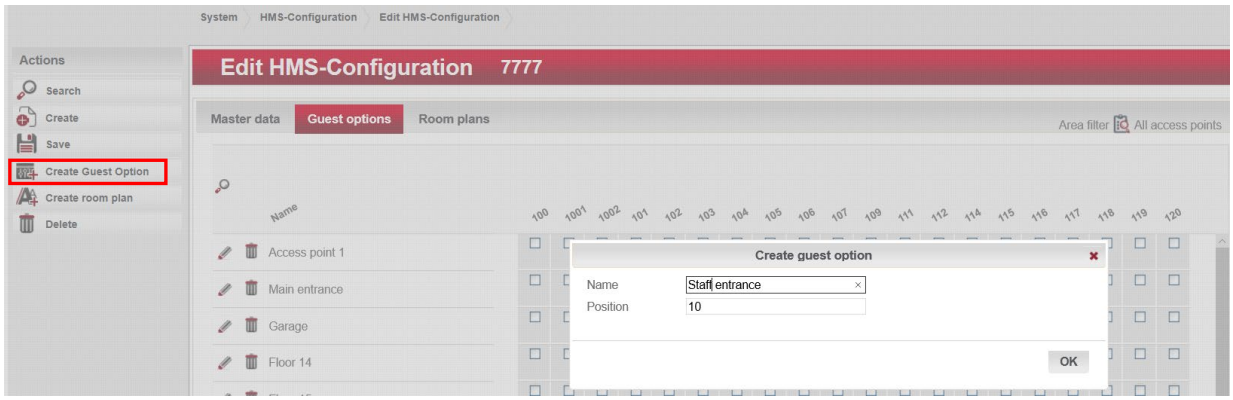


The pre-set ports (default 7777 / 7778) must correspond with the "Network Server" port in the HMS administration.

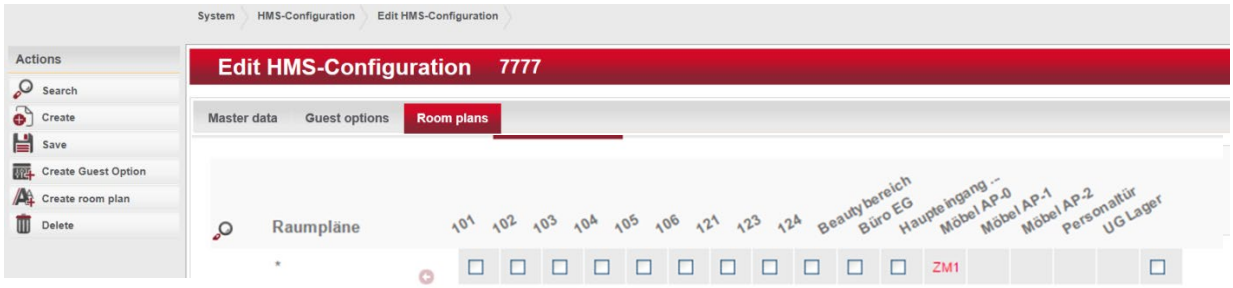


Settings for the HMS interface communication
If the “DG2 Key Format” has been selected in the HMS Interface Administration, the set ports (default 7777 / 7778) can be adapted if necessary in the “Network Server” tab.

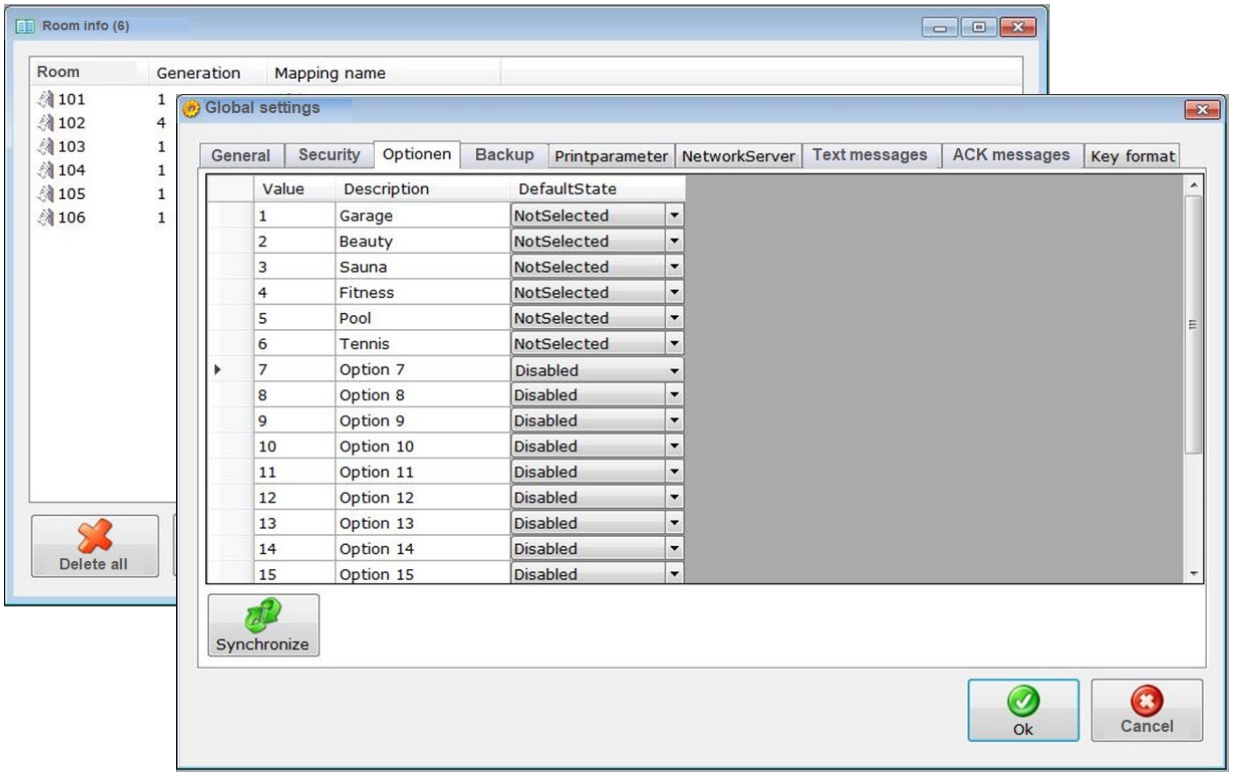
Definition of guest (visitor) options
A new option can be created by clicking on the “Create guest option” button  Create Guest Option
When the option has been named and saved, authorisations can be assigned to it.



Definition of access authorisations to "General doors"
The access authorisations for all valid guest keys can be issued in the room plan “*”. Authorisations for the guests in certain rooms can also be created using other room plans which must be defined manually.



Importing / synchronising rooms and options in the HMS interface
The room numbers or room designations to be used in the HMS Interface are imported in menu item “**Room info**”, and the options to be used are imported in menu item “**Global settings > Options”** using the “**Synchronize**” button.



5.7.11. Client management

It is possible to manage a client as standard in Dialock PROFESSIONAL. The client management can optionally be extended to as many as **50** clients.
Sensible use can always be made of client management if several parties in a building such as different companies are to be managed individually.

The advantages of Dialock client management:

Every client can be licensed. This makes it possible for the client to create his own configurations and embed his own logo.
Because of the advantageous structuring of the database, considerable costs for database licences and computer hardware can be avoided. Shared use of data in multi-party buildings such as main and secondary entrances, car parks and lifts (overlaps) can be achieved without a great deal of effort.

Client-capable data:

1. Terminals
2. Barriers/doors
3. Access points (online/offline)
4. Reader
5. Persons
6. Groups and organisational units
7. Identification characteristic (transponders, PIN codes)
8. Scripts
9. Transponder definition
10. Reports

Note!

Client-capable data:
In this context, client-capable means “manageable using a client”. "Client-capable data" is data which is individually manageable for each client.

Not client-capable data:
The definition of the length of the transponder segments cannot be individually managed. The length of the segments cannot be different for individual clients.
The room zone access point assignment is also not client-capable.

Client authorisations can be used to authorise system users who can see the data of other clients, edit it and / or delete it.
The actions of a system user, i.e. creation, editing and deleting of data records are assigned to the active client. New data records can always only be created for a client that is assigned to the system user. A system administrator can create new data records for every client.
System users whose main client is the default client can switch between clients. System users whose main client is not the default client can only see the data records of their main client in accordance with the client authorisations and edit them or delete them depending on the authorisation.

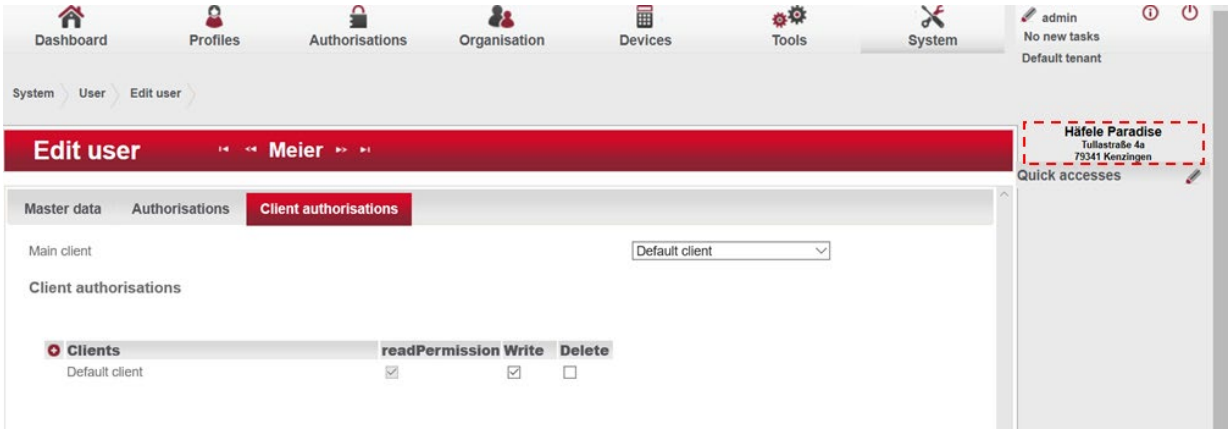


Fig: Client authorisations

In practice there are always three types of use in the Dialock operating concept:

1. System administrators

An administrator is a system user with Dialock administrator rights. Assigning the main client to the system client guarantees that this system user (Dialock Administrator) has the authorisation to work in different clients. This makes him a system administrator in Dialock. In practice, this authorisation level would be assigned to the owner of the building, for example. System administrators have unrestricted access to all modules of the Dialock system. They can decide which client they want to work in.

2. Client administrators

A client administrator is a system user with Dialock administrator rights. If the main client is assigned to a different client than the default client, the administrator only has the rights for the client that has been assigned to him. A client administrator cannot change the active clients. These authorisation levels would be assigned in practice e.g. to the administrator of a rental unit. Client administrators have unlimited access to all Dialock system modules within their clients.

3. Standard users

Standard users have no Dialock administrator rights. They are only assigned a client like client administrators and cannot change the active clients. Standard users can view and have rights to the Dialock system modules as per their assigned user roles. In practice, standard users are operators of the Dialock system of a rental unit, a building with limited access authorisations to the Dialock system modules within their clients.

6. Glossary

AbP	Amtliches bauaufsichtliches Prüfzeugnis (Official technical test certificate). The AbP certifies the usability of a fitting on a fire protection or smoke control door and describes the installation conditions and precautions that must be complied with.
Access regulation	See Access control
Access right	See Access authorisation
Administrator	The administrator of an access control system is the person who has the authorisation to install and configure access control system software, configure terminals, create room zones, areas, area groups and time models and modify them. The administrator is given exclusive access to the system using his own ID medium. The administrator can create other users with administrator rights.
AES	Advanced Encryption Standard Modern encryption system, successor to DES and 3DES.
Anti-Pass-Back	See Double usage monitoring
AP	Access Point. Location that is equipped with an access control device and at which access to a furniture item, room, area, building, site etc. is possible as per the authorisation.
Area	Collection of room zones for managing access rights.
Area group	Collection of several areas for organising access rights.
Area time model	A time model that applies to an area (see above) of an access control system.
Audit trail	Entry of all reading and unlocking procedures and special events (e.g. configuration, battery change, emergency opening operation at a door terminal etc.) together with a time stamp in a non-volatile memory of a terminal.
Authorisation group	Group of persons who are authorised for the same procedures in the software or at access points in an access control system.
Authorisation updating	Procedure in which an authorisation writer/validation terminal updates the offline authorisations on a transponder for the duration of the defined authorisation period / validation period.
Authorisation writer	Online wall terminal at an access point that can perform both an authorisation check and an update of the offline authorisation on the transponders.
Authorisation writer	Device at an access point that reads the usage authorisation on a key, checks it and depending on the result of the check, unlocks the access point or also only re-writes offline access rights. In order to do this the terminal communicates with the access control server in which the authorisations are saved.
Authorised person(s)	Person(s) who is (are) authorised for procedures in the software or at access points in an access control system.
AWE Evaluation unit	Device or part of a device that checks the access authorisation and allows access depending on the result of the check. See also door terminal, wall terminal
Balancing	Calculation of the number of persons that are inside an access control system or an access control system area. In order to do this, it must only be possible to exit areas/zones with keys at online access points (evaluation unit).
Black List	List of keys (UID or key number) in an evaluation unit that are blocked at this unit. See “Blocking list”
Block lock	The block lock is used in a burglar warning system as a locking device that activates the burglar alarm system control centre when the protected area is exited. All alarms that are triggered after activation trigger an alarm. However, activation can only take place if the compulsory conditions have been fulfilled, i.e. all alarms are in the passive state. The burglar alarm system is also deactivated via the block lock.

Block lock function	A WT 200 wall terminal can take over a partial block lock function by receiving an appropriate signal from the burglar alarm system when it is activated and then deactivates all readers in the protected area, and activates them again when the burglar alarm system is deactivated.
Block lock function	The block lock function ensures that the readers belonging to an area that is protected by an alarm do not read access media after the burglar alarm system has been activated and therefore prevent access to the area. The activation and deactivation of the burglar alarm system can also take place via a reader connected to the WTC 200. Activation can only take place if all doors belonging to the protected area are locked.
Blocking element	Electro-mechanical component for controlled blocking and opening of an access point within an access control system (doors, gates, locks, furniture flaps etc.).
Blocking key	Special key that is used to block a key that has been lost, for example, at offline terminals.
Blocking list	List of keys (UID or key number) in an evaluation unit that are blocked at this unit. See "Black List"
Dashboard	The Dashboard is the top level of the graphical user interface of Dialock 2.0. All main functions and function groups are displayed and selectable in this.
Deletion key	Special transponder that is used to delete keys that are to be invalidated at an offline terminal.
DES	Date Encryption Standard. For a long time this was the encryption algorithm used in IT. No longer considered to be secure.
DHCP	The Dynamic Host Configuration Protocol (DHCP) is a communications protocol in computer engineering. It makes it possible to assign the network configuration to clients by a server.
Door alarm	The door alarm is triggered if the door is not closed after expiry of the door opening time.
Door monitoring time	This the length of time for which the door may remain open without the door alarm being triggered.
Door opening time	The door opening time is the time for which a door may remain open before the door alarm is triggered.
Door release time	See Open time
Door terminal	Electromechanical access control unit that is fitted to a door. It contains the key reader, the evaluation unit and the electrically controlled locking element. The power is usually supplied using batteries.
Double usage monitoring	Function of an access control system that ensures that access at an access point can only take place in one direction, and that prevents a key from being used two or more times in the same direction. It is therefore not possible for an authorised person to pass back their key to another person after entering in order to give them access.
EE Input device	Device or part of a device that reads the authorisation data from the identification data media that are used and forwards it to the evaluation unit. (reader, reader head)
EMA	Burglar alarm system
Emergency authorisation system	Offline terminal operating mode in which the teaching in of keys using a programming and deletion key is assigned in the event of a system failure
Emergency opening	Opening of an access point in the event of evaluation unit or input device failure. An emergency opening device must always be planned and installed.
Encoding device	Technical device for writing data onto transponder media, triggered by an authorised user.
End date	Date after which a time-based/area-based access authorisation becomes invalid.

End of validity	Point in time to which a transponder is valid. This point in time is independent of group or individual access rights and time models.
End time	Time after which a time-based/area-based access authorisation becomes invalid.
Event log	This log book lists all event data coming from the access points centrally in the server. It also contains events that occur because of configuration changes on the server.
Fire protection, smoke control door	See Fire protection door, see Smoke control door
Four eyes principle	Authorisation procedure in which two different valid keys are required to allow access or carry out other terminal actions. Emergency authorisation e.g. in standalone systems.
FSA Fire protection door	Fire protection doors are self-closing doors and other self-closing closures (e.g. flaps, roller shutters, gates) that are intended to block the passage of a fire through openings in walls and ceilings when they are installed. Def. in accordance with DIN 4102
Furniture terminal	Electronic offline access control unit, designed for installation in furniture. The locking element is usually an electric furniture lock that is actuated by the furniture terminal. A furniture terminal can have additional digital signal inputs and relay outputs.
Group authorisation	Collection of several individual authorisations for a group of persons, e.g. for a department.
Guest key	Transponder for the guest of a hotel or similar accommodation. Normally valid for the duration of the booked stay.
Identification media	Transponders that contain information that can be read from an input device in the sense of identification characteristics. QSEC
Individual access right	Access authorisation for a single access point without assignment to a room zone
Integrated access control	Access control system consisting of access control components that are used in online operation and access control components that are operated offline. The configuration of the access control components and the administration of the access authorisations takes place centrally.
Key	Transponder medium as key onto which the access authorisations for an evaluation unit can be saved in a readable format, and onto which the evaluation unit can deposit operating information.
Key card	Version of a transponder key in credit card format in accordance with ISO 7810. Other designs are key tags and wrist band transponders, for example.
LE Reader unit, reader	A reader unit takes the identification characteristic of the ID, converts them into electrical signals and sends them to the evaluation unit.
Licence file (Dialock)	File in which the object key, the functional scope and the scaling values of the Dialock software are saved in a customer-related way. This file is accessed during the installation of the software in order to install and adjust the relevant resources. The licence file is encrypted in the as-delivered condition.
Licence key (Dialock)	A 16-digit licence key for decoding the licence file. Sent to the customer or the installer using a different delivery method from the Dialock software and the licence file for security reasons.
Location	Top spatial level of the access control system topology.
Locking cycle	Operating mode in which a barrier is opened for the period that is defined as the open time whenever an access authorisation is detected.
Locking group	Access right for a group of terminals (1 to n terminals)
Login key	Key for authentication as an authorised user of the DIALOCK software at workplaces with an encoding device
Login right	Authorisation to use the Dialock software. Part of the graduated authorisation concept.
Macro (program)	Additional programs that are saved in the non-volatile memory of Dialock terminals to supplement the basic functionality.

Master data	Data record with which an object belonging to an access control system is described. This could apply to persons, groups, users, transponders, terminals, areas, readers, encoding devices etc.
MDU (Mobile Data Unit) 110	Portable device for transmitting terminal parameters and terminal configurations data to and reading out terminal logs and operating data from the offline terminals.
Offline function ID	This identifier is a number between 0 and 2000. Then certain functions at offline terminals are assigned to the function identifier such as the suppression of certain signalling or "Do not open if low bat" as the highest signalling to the hotel employees. Then the ID can be assigned to a person. A person can only have one offline function ID assigned to them, but a particular function ID can be assigned to any number of people.
Offline terminal	Device at an access point that reads the usage authorisation on a key, checks it and depending on the result of the check, unlocks the access point. This is done without the terminal communicating with any other component of the access control system.
Online terminal	Device at an access point that reads the access authorisations on a key, checks them and depending on the result of the check, unlocks the access point. In order to do this the terminal communicates with the access control server in which the authorisations are saved.
Open time	Time for which the locking element at an access point is unlocked for opening. The default open time is defined as a parameter for the terminals. A deviating open time can be defined on the key as a person-related parameter.
Parametrisation	Setting of operating parameters at access control terminals such as: Room number, date, open time, operating mode etc. The parameters are transmitted via the network in the case of online terminals, and via MDU 110 in the case of offline terminals.
Passage contact	Contact, switch or reader with which the actual passage through a door is monitored within the door opening time.
Passage monitoring time	This is the duration for which passage through the door is monitored using the passage contact signal.
Person master record	This data record is created for each person before granting access rights. Among other things, it contains information such as name and surname, e-mail address and personnel number (this comes from the system) and specification of the duration of validity of the transponder or key. Person master records can be imported from existing personnel systems as an Excel file.
PIN	Numeric code as access authorisation (**P**ersonal **I**dentification **N**umber)
Pre-alarm	The pre-alarm is triggered a certain adjustable time before the door alarm is triggered. This makes it possible to request closing of the door before the main alarm is triggered.
Privileged key	Transponder with special authorisations at offline terminals. Privileged keys can authorise one or more functions such as configuration with MDU, reset, protocol audit trail, override “Do not disturb” etc.
Programming key	Special transponder in standalone mode, used to assign authorised keys to offline terminals in standalone mode and also takes over additional functions of the “Privileged keys”.
Protected area	A self-contained object or sub-area thereof (room, building, site) that is monitored by an access control system.
Resource	In a Dialock access control system, a resource describes a device that transmits messages such as event messages, status messages or error messages to the server.
Room group	See Room zone
Room zone, zone	Sub-areas of a protected area consisting of one or more rooms with one or more entrances and/or exits.
Route monitoring	Recording of the route of a person in a system by recording the use of the key at access control readers.

Sabotage contact, tamper switch	Electric contact or switch that generates an alarm signal if a device is opened.
Signalling	Visual or acoustic indication of an operating status or the test result of an access control input device.
Smartphone key	Function for operating a reader with an electronic key via smartphone (alternatively to transponder)
Stand-alone operation (SA mode)	Simplest operating mode in a Dialock system. This is preset in the factory. With this operating mode, a terminal can be started up immediately after installation by teaching in the master key (programming and deletion key).
Start date	Date from which a time-based/area-based access authorisation becomes valid.
Start of validity	Point in time from which a transponder is valid. This point in time is independent of group or individual access rights and time models.
Start time	Time from which a time-based/area-based access authorisation becomes valid.
Student key	Individual key that has been created for a student.
System code	Unique identifier of an object (project code or Legic system code).
Tag, key tag	Transponder medium in the form of a key ring.
Terminal configuration	Terminal ID, date and time, terminal parameters (e.g. operating mode, open time, locking groups, system code, audit trail options, time models, …)
Terminal parameters	Settings for an access point in the access configuration software resulting from the configuration of a terminal.
Time mask	Time stamp on the key for defining the duration of validity of the key.
Time model	Collection of several (8) time stamps consisting of a start time and an end time for different days of the week. In the offline access point, defines periods for autonomous functions or authorisations, for example.
Time stamp	In the time model, a time stamp consists of the start time and end time for different days of the week. In the audit trail, the time stamp is the value that assigns an event to a certain point in time.
Time zone	Selection or definition of the valid time at the respective location (CET etc.)
Toggle mode	Operating mode in which the status of a barrier changes whenever a spatial/chronological access authorisation is detected. The toggle function can be fixed or also be configured for certain keys only.
Token	General term for an identification data medium.
Transaction	Term taken over from time & attendance for the recording of the COMING or GOING of a user. In access control it corresponds to the access event.
Transaction panel	Tabular display of the saved access events in the DIALOCK 2.0 GUI (dashboard).
Transaction record	Data record consisting of all data of an access event, such as the transponder number, the transaction time and the terminal action.
Triple DES, 3DES	Encryption algorithm in which the DES procedure is used three times. Has now been superseded by AES.
UID	Unique Identifier Number. Globally unique 4-10 byte number that is saved in transponders when they are manufactured.
Updating interval	The updating interval for offline authorisations can be set to the nearest hour here. If this has been set to 0, the updating interval is not checked by the authorisation writer. If the last time the transponder was held in front of the authorisation writer was longer ago than the update interval, access is refused.
Usage frequency	Frequency with which an access point in a building is used, in relation to a certain period of time (week, day, hour).
User	Person, who has rights for using the Dialock software.

Validation	Procedure in which a validation terminal/authorisation writer updates the offline authorisations on a transponder for the duration of the defined authorisation / validation period.
Validation terminal	Online wall terminal at an access point that can perform both an authorisation check and an update of the offline authorisation on the transponders.
Visitor management	(IT) device for recording visitor data and creating visitor transponders. Balancing!
Wall terminal	Electronic access control unit without an actual mechanical actuator. It consists of a reader, which is typically mounted in or on the wall, the evaluation units which interprets the data that is read in, and a series of digital signal inputs and relay outputs. Signal inputs are used to process signals such as buttons for door opening, door monitoring contacts or the like. Relay outputs are used to actuate electric actuators or signal generator. The power is supplied by a power supply.
WebKey	digital UserKey for Progressive Web App (PWA)
White List	List of keys (UID or key number) in an evaluation unit that are authorised at this unit.
ZK Access control	Access control controls the access to areas, buildings, plots and rooms via a “WHO−WHEN−WHERE” regulation so that only authorised persons are given access to the area for which they are authorised. Access authorisations can be time-limited (day of week, date, time). In electronic access control, the access authorisation of electronic evaluation units is checked on the basis of identification data media.
ZKA	Access control system. System for regulation and automatic checking of access authorisations, control of locking elements and registration of transactions (VdS).
ZKS Access control system	The access control system includes all structural, media and organisational circumstances that are needed for access control. QSEC
ZKZ Access control centre	The unit in an access control system that decides whether an access request is granted or denied. In a door terminal, the access control centre is integrated in the terminal.
Zone	See Room zone

Copyright

Exclusion of liability

Häfele SE & Co KG compiles the contents of this document with the utmost care and ensures that they are updated regularly. Häfele SE & Co KG does not accept any liability for the up-to-dateness, correctness or completeness of the information on these pages.

Häfele SE & Co KG
Adolf-Häfele-Str. 1
D-72202 Nagold
Germany

Phone: +49 (0)74 52 / 95 - 0
Fax: +49 (0)74 52 / 95 - 2 00
E-mail: info@haefele.de

Dialock hotline: +49 (0)74 52 / 95 - 1930

Subsidiaries of Häfele:

www.hafele.com

732.29.430

HDE 20.12.2023