HÄFELE

Version 02.06.2016

SOFTWARE MANUAL
Access control system

Dialock CONTROL
Dialock HOTEL
Dialock PROFESSIONAL

Access control with experience

Copyright

Exclusion of liability

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

Key


Activate/deactivate update


Perform update now


Update progress


Edit/change


Assign authorisation


Create data record


Add/assign data record


Print


Re-enter person


Search for person


Search (fade-in search filter)


Exit program


Reset search filter


Terminal connected and ready for use


Terminal offline


Terminal search


Operate transponder with authorisation of an employee


Open up submenu (right mouse button)


Edit access authorisation

Contents

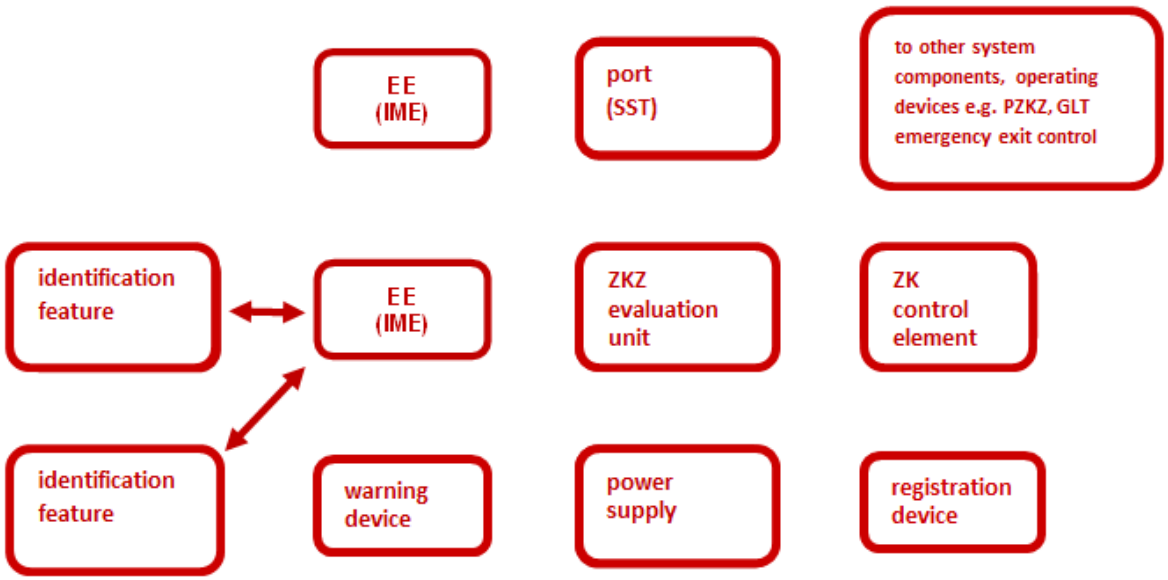
1. General access control

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.

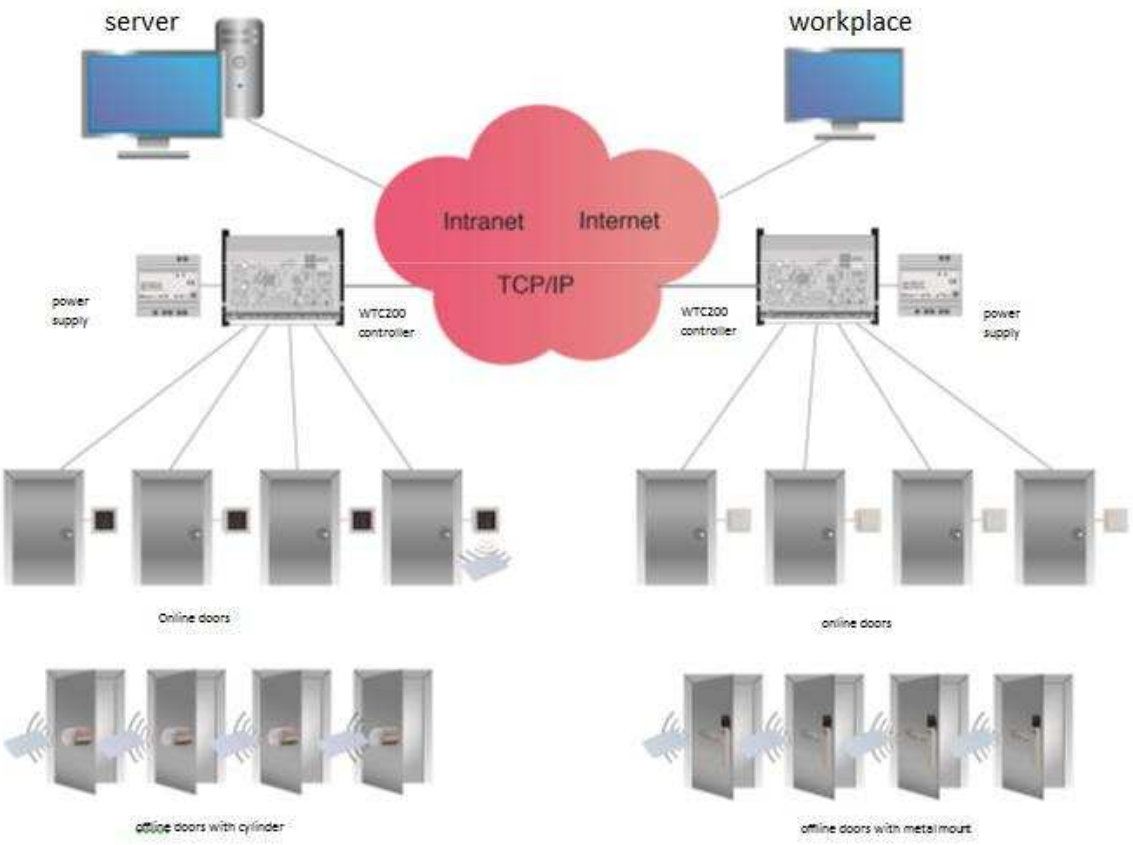
Professional access control systems should include the following function units (source: VdS):



EE	= input device
IME	= Identification feature detection unit
ZKZ	= central access
ÜZKZ	= parent access controller (server)
ZK	= access control
SST	= interface

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.



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 PC’s and smartphone platforms.

1.1.1. Important core functions of Dialock

1.1.1.1. 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 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 an employee 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.

1.1.1.2. 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 accounting employees. Then, the affected employees are assigned to this “Accounting” group and therefore automatically receive the authorisation profile of the “Accounting” group. In this way, new employees 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 cleaning team employees 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.

1.1.1.3. Allocation of rights using role models

The establishment and allocation of role-based access authorisation to employees is another powerful function of the Dialock PROFESSIONAL, software which strongly rationalises the organisation of the access control:

The bigger an organisation is, the more comprehensive the property and the greater the number of persons, and the more difficult it is to ensure that data storage is consistent throughout the organisation. The restructuring that is taking place all the time, particularly in large, dynamically expanding companies, and project-related, time-limited team structuring therefore require higher-order, functional authorisation control.

In this case, role-based concepts are then taken as a basis for the allocation of authorisations. When doing this, authorisations are no longer assigned directly to each individual person, but to a **role**, i.e. a **task** or a **process**. The employees can then have one or more of the defined roles assigned to them.

The advantage of the role concept lies in the additional transparency when allocating authorisations, greater proximity to the processes and simpler work steps because they are not person-related if many adaptations are required.

The creation of the roles and the associated authorisations requires in-depth knowledge of company processes and also detailed knowledge of the performance capability and requirements of the system components which carry out the authorisation queries. There is also the organisationally difficult question of who is allowed to change and allocate roles, and under which conditions.

However, help is at hand with the function for creating different administrator profiles in the Dialock system and the consistent possibility of **traceability** of all administration procedures.

When the decision is made to allocate access authorisations using role models, it is essential to ensure that it is **not** possible to retrospectively change the system in order to use the group authorisation concept on the basis of the structure of the automatically created database. The system has to be reinstalled to make this kind of change.

In other words, when the access control system is being designed it must be decided whether the allocation is going to be organised in a role-based way or according to group authorisations.

1.1.1.4. Client capability

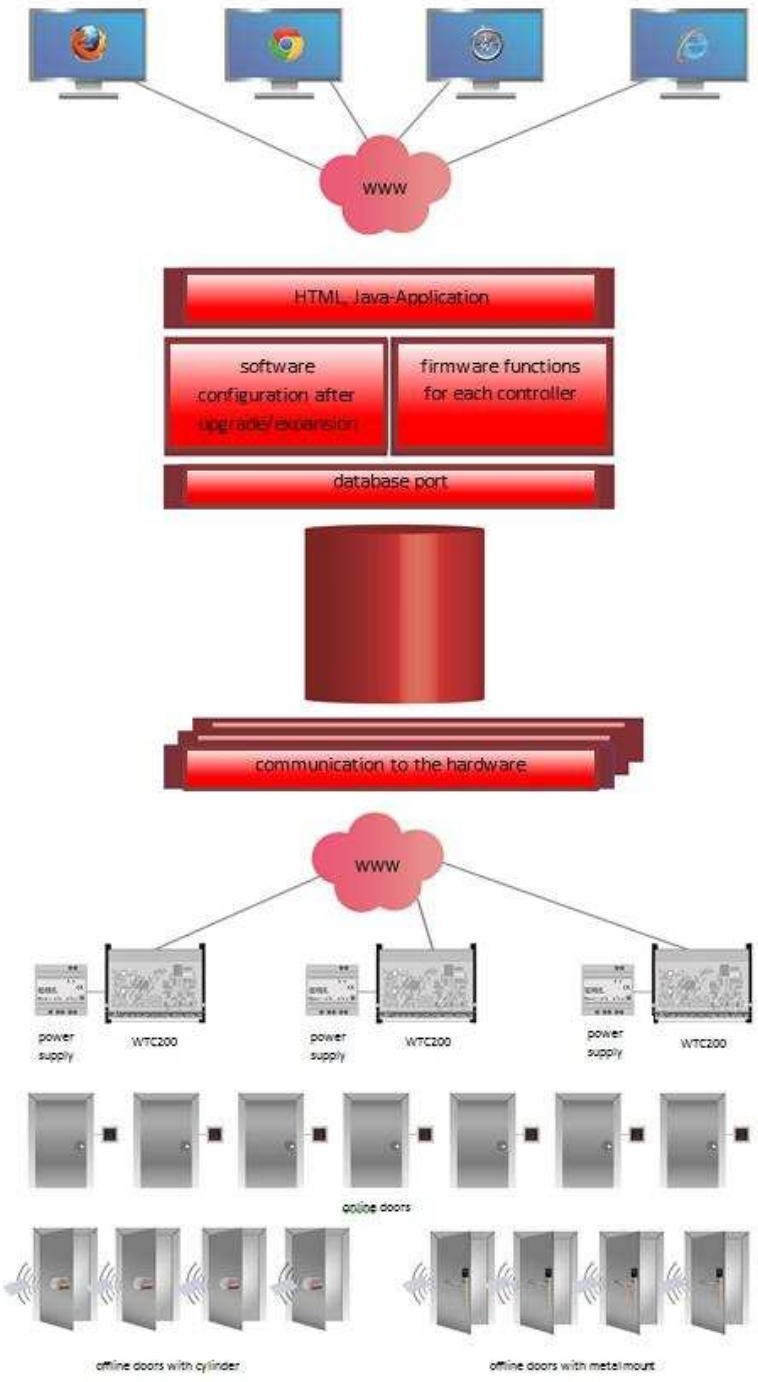
It is possible to administer clients as standard in Dialock PROFESSIONAL. Sensible use can always be made of client management if several parties in a building such as different companies are to be managed individually. When doing this, each client organises and manages its own access authorisations 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 10,000 clients can be set up.


www
HTML, Java-Application
software configuration after upgrade/expansion
firmware functions for each controller
database port
communication to the hardware
www
power supply
WTC200
power supply
WTC200
power supply
WTC200
online doors
offline doors with cylinder
offline doors with metal mount

1.2. Prerequisites

1.2.1. Miscellaneous

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.

1.2.2. Browser settings

The operator software (client) can be operated in the following web browsers, independent of the operating system:

- Microsoft Internet Explorer from version IE 11
- Mozilla Firefox from version 36
- Google Chrome from version 42
- Safari from version 8.0.4

Recommended monitor: Resolution 1680 x 960 pixel min.

1.2.3. Java compatibility

Server:
Installation with Java 1.8 or higher

Client:
During the configuration of the system, for certain operating procedures (e.g. MDU data transfer or saving of the network configuration of the WTC) hardware needs to be connected via USB. A suitable Java version is needed for the browser that is used (32 bit or 64 bit) on these clients.

1.2.4. System requirements

Dialock provides an automatic setup program for installation that is intended for systems on which none of the components mentioned in the following are installed:

If an SQL server has already been installed, a specially adapted installation must be performed.

The server operating systems supported for the setup program are (server installation):

- Windows 2008 Server SP2 (64-Bit)
- Windows 2008 Server R2 SP1 (64-Bit)

- Windows 2012 Server
- Windows 2012 R2 Server

Installation on a computer with a desktop operating system is generally possible, but the performance and availability may be restricted. The following are possible:

- Windows 7 Pro SP1 (64-Bit)
- Windows 8.1 Pro (64-Bit)
- Windows 10 Pro (64-Bit)

It is not advisable to use the server as a workplace PC as well.

The hardware requirements (server) are

- RAM: Min. 4 GB, 8 GB recommended
- Hard disk space: Min. 15 GB, 50 GB recommended
- Processor: Min. Dual Core 2 GHz, Quadcore 2 GHz recommended (e.g. Intel Core i3 or better)

Note:

The following manufacturer's conditions also apply to the Microsoft Server 2012 Express SQK database installation:

http://www.microsoft.com/de-de/download/details.aspx?id=29062

http://msdn.microsoft.com/library/ms143506(v=SQL.110).aspx

1.2.5. 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.

1.2.5.1. Secure operation of the server system

The following components are installed on the server system:

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

1.2.5.2. 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.

1.2.5.3. 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.

1.2.5.4. 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.

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.

1.2.5.5. 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.

1.2.6. 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:

1.2.6.1. Physical conditions

Spatial boundaries

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

1.2.6.2. 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.

1.2.6.3. 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.

1.2.6.4. 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 the number of persons and/or the number of 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 on the system.

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 reader, with which access authorisations for offline locking points can be updated at regular intervals.

Dialock CONTROL is scalable from 20 people and 30 access points up to 500 people and 500 access points and 2 encoding stations. Extensions can also be installed.

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 reader, with which access authorisations for offline locking points can be updated at regular intervals.

Dialock HOTEL is scalable from 30 people and 30 access points up to 500 people and 500 access points and 16 encoding stations or authorisation writing terminals (the authorisation writer is often known as the validation terminal).
Extensions can also be installed.

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 locations that require increased security, organisational efficiency, flexibility and operating convenience. Dialock PROFESSIONAL supports the creation and administration of locking media for employees for the online and offline access points of the system.

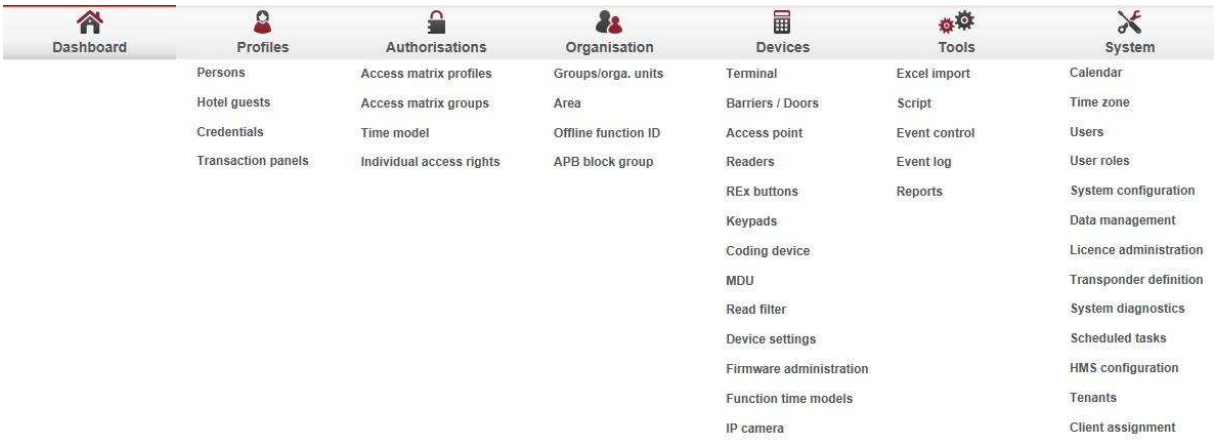
The establishment and allocation of role-based access authorisation for employees is a particularly powerful function which rationalises the organisation of access control considerably. (see also 1.2.1.3)

Dialock PROFESSIONAL also makes it possible to administer clients. (see also 1.2.1.4)

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 reader, with which access authorisations for offline locking points can be updated at regular intervals.

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
People (such as employees), hotel rooms, transponders and the transaction panel are depicted with profiles. Central administration of personnel data and log entries take place here. Under HOTEL ROOM, 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 language can also be set independently of the browser setting.

The Dialock software is currently available in German, English and Spanish.

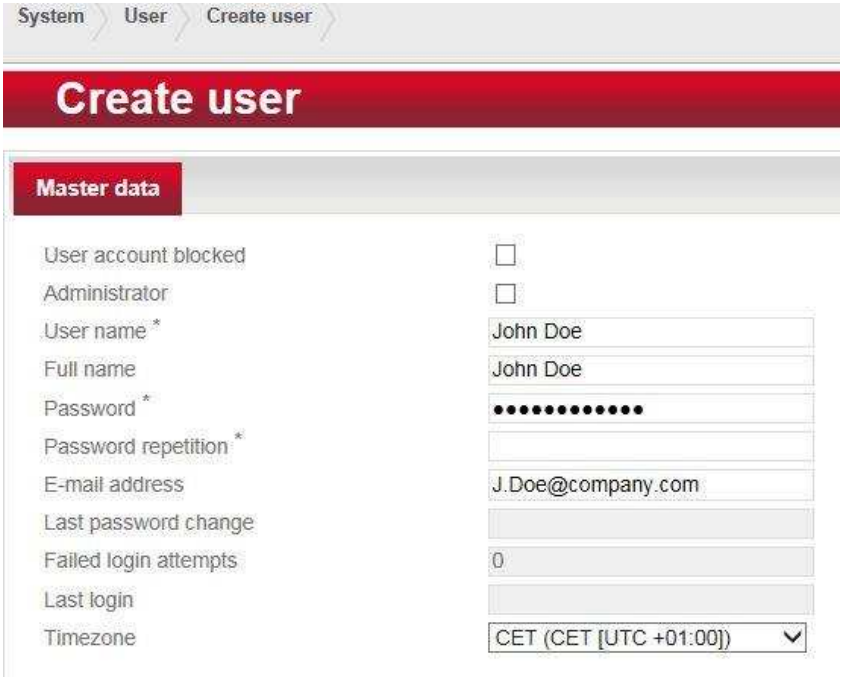
4. Quickstart for access allocation with/without time model

4.1. Enter/block 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. To do this, he assigns an appropriate user name and password in the **System > User** menu via the **Create** side-menu item. 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.

Block the user account immediately 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.

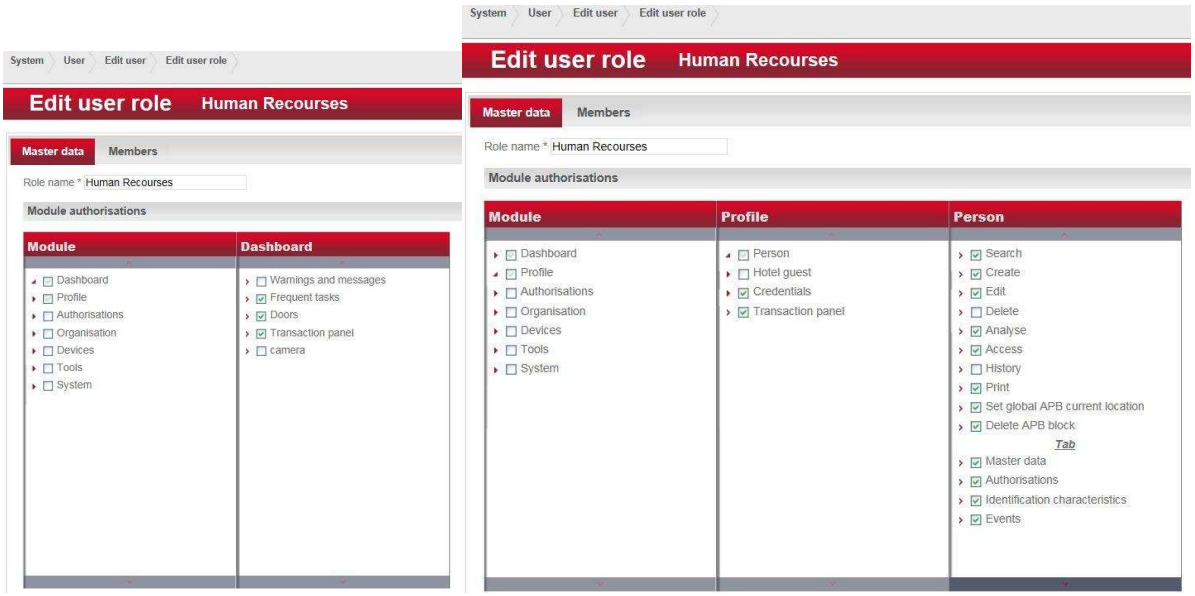
A user without administrator rights should have user roles with different authorisations assigned to him.

4.2. Creating user roles

The individual access authorisations of the users to the different modules are assigned in the **System > User roles** menu.

Multiple assignments of user roles are possible.

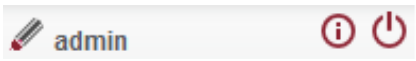
Via the menu item **System > User roles**
or via the **Authorisations** tab in the **System > Users** menu (of an existing user), you can create a new valid user role for this user by clicking on the symbol.



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

4.3. 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:

4.3.1. Change/edit user profile

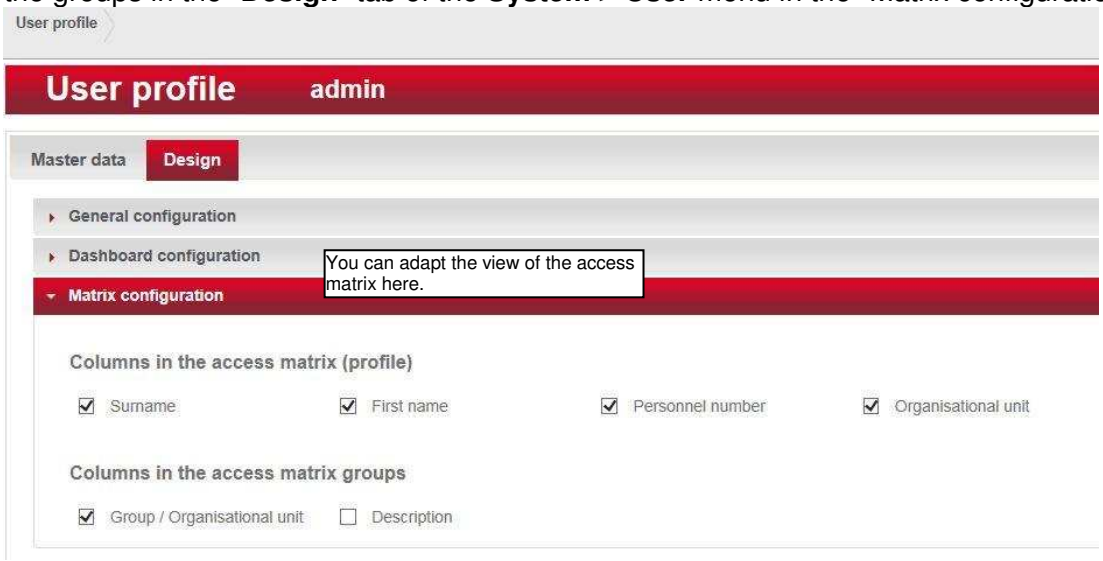
Via the pencil icon (alternatively also via the menu item **System > User**), you can access your own profile. You have the option to change your user name and your e-mail address here.

4.3.2. Dashboard display (dashboard configuration)

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

4.3.3. 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.

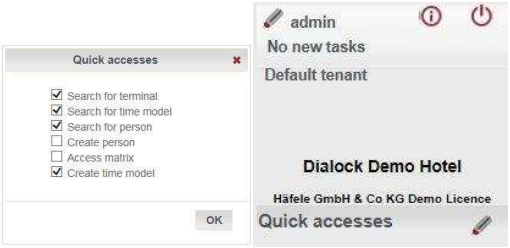


4.3.4. Password change

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

4.3.5. 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.

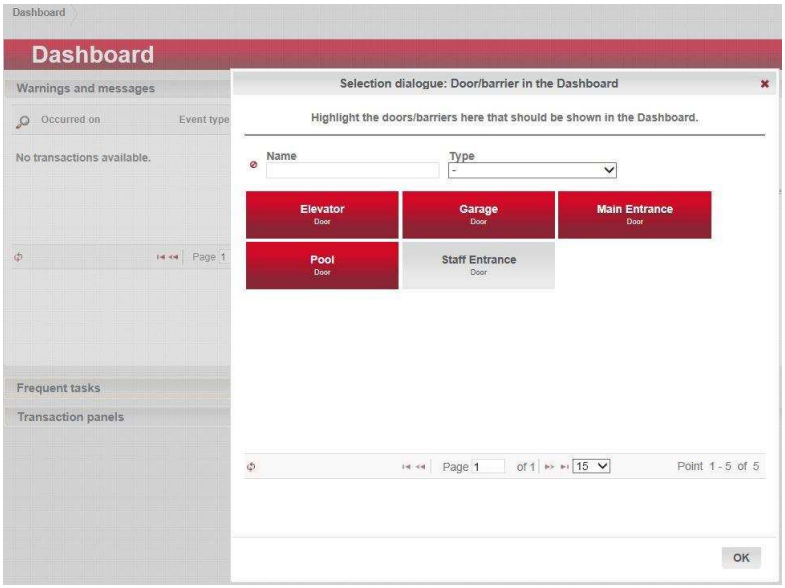


4.3.6. Arrangement in the dashboard

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.

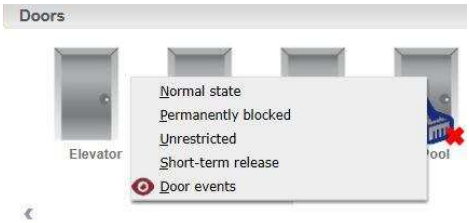
4.3.6.1. Individual display of doors in the dashboard

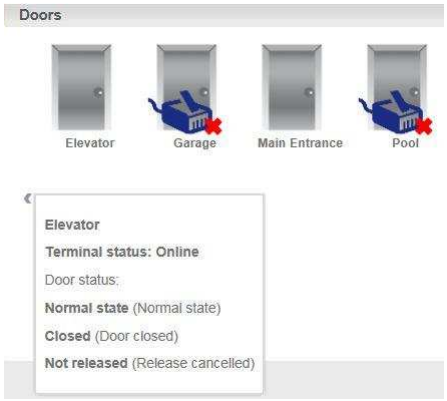
Click on the pencil icon on the right-hand edge of the doors screen. Mark the desired door(s) or barrier(s) which should be displayed in your dashboard.



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.

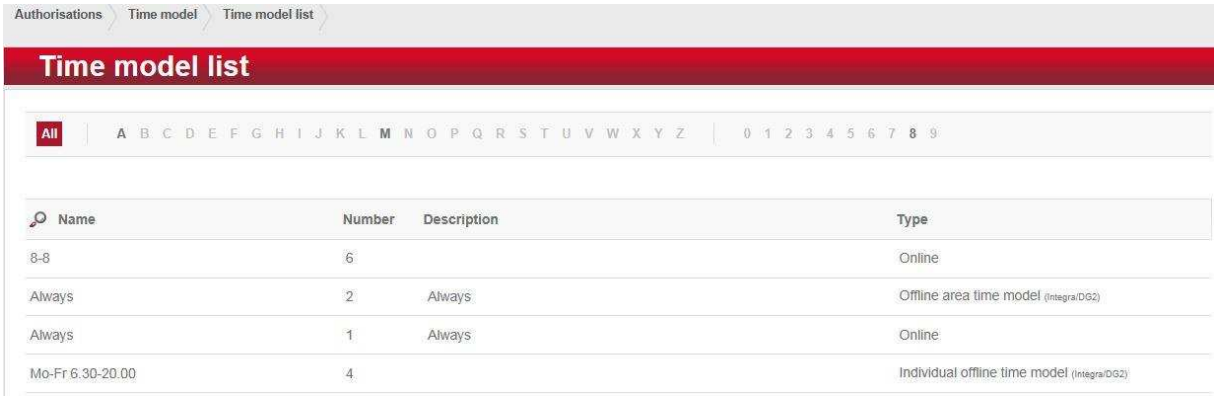
4.4. Time models

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.

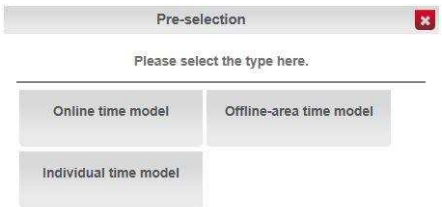


4.4.1. Create/edit online time models

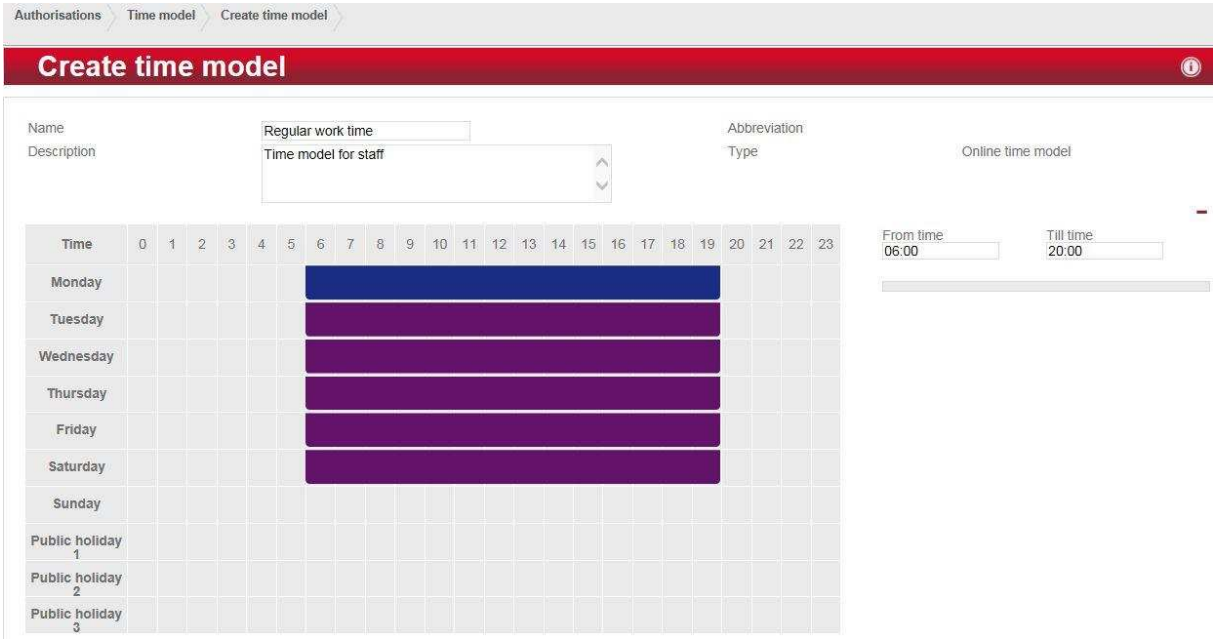
A new time model can be created via the “**Create**” action on the left-hand sidebar. Make the choice between an online and offline time model here, such as in the example mentioned in the following – depending on the equipment of the doors at which the time model will be used later.

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.

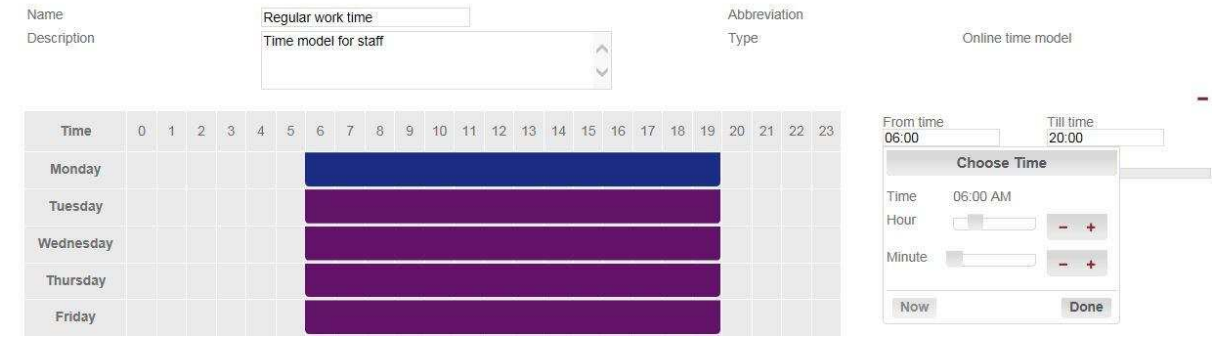


Specify a **Name** for the new time model and, if you wish, a **Description**. You can find the time model in other overviews using the name.

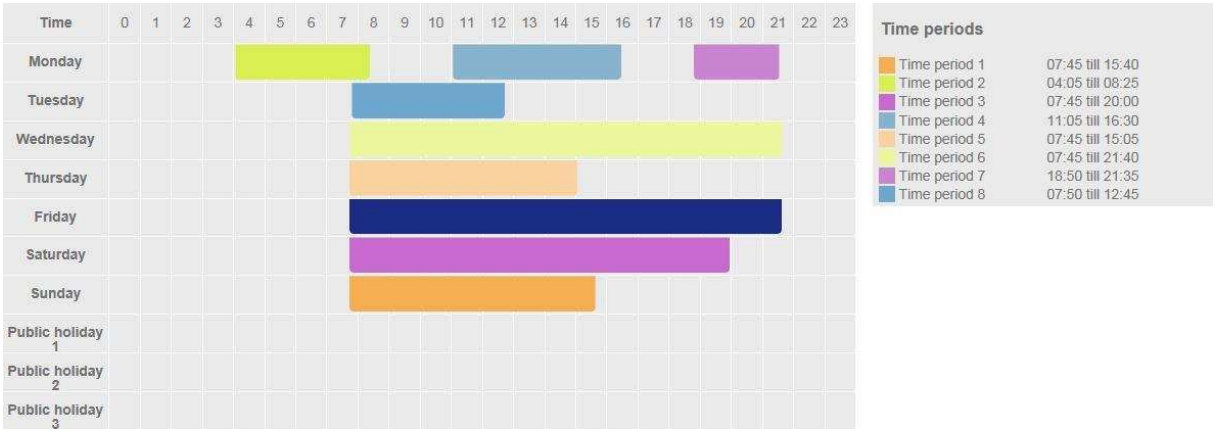


In order to set the time, double-click the line of the desired day and then the field of the desired start time (the exact time can still be set in the **From time** and **Till time** fields). The marked time is now highlighted. As soon as the cursor moves to the edge of the highlighted time, the appearance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

4.4.2. Offline time models

Offline access points can be opened at any time with a valid ID. 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 4.4.1 “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 IDs, only the assignment of the user to the time models is saved on the pass. This assignment can be updated at any writing (hold the ID at an authorisation writer).

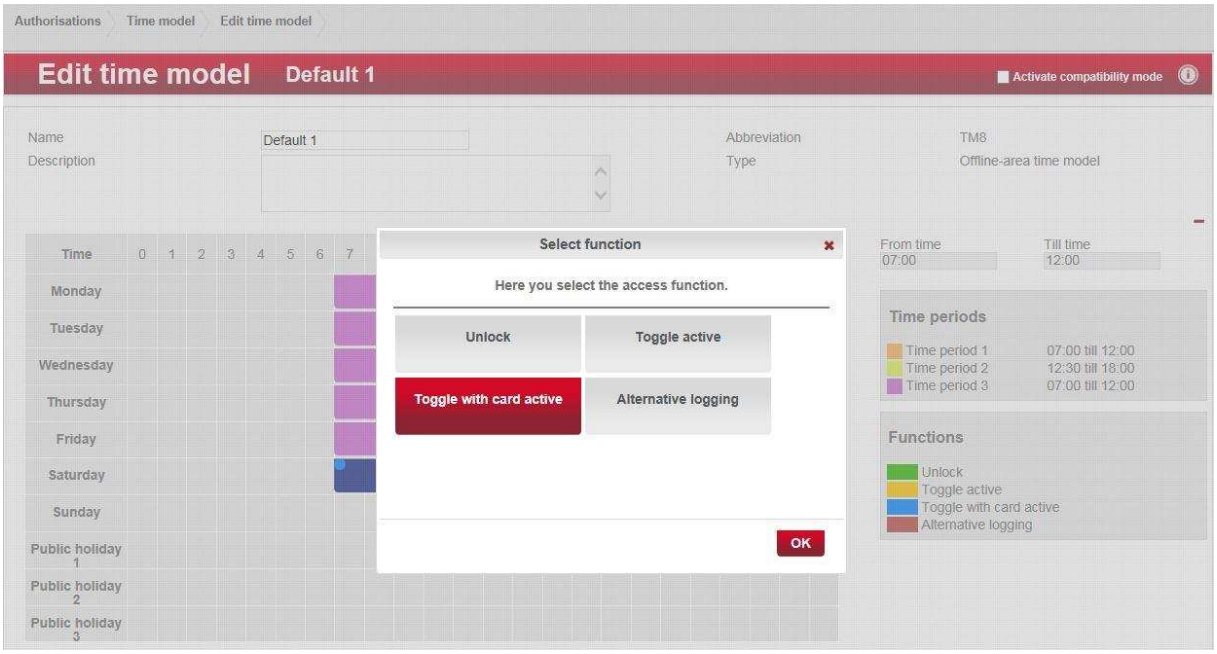
Individual offline time model:
The individual offline time models are saved on the card. The functionalities of the individual time models are minimised for memory reasons. Only one time period is recorded with individual offline time models.

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

4.4.3. Enter/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 4.4.1.

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.

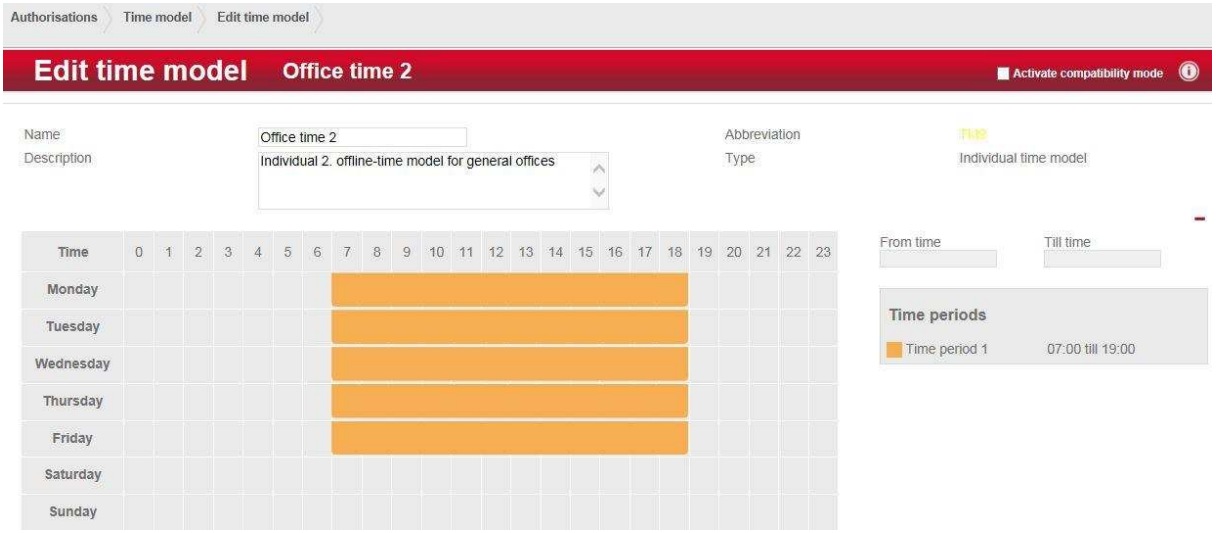
Toggle active:
When presenting a valid identification medium (e.g. ID card), the state of the access point changes from “Locked” to “Unlocked” or vice-versa and remains in this state.

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.

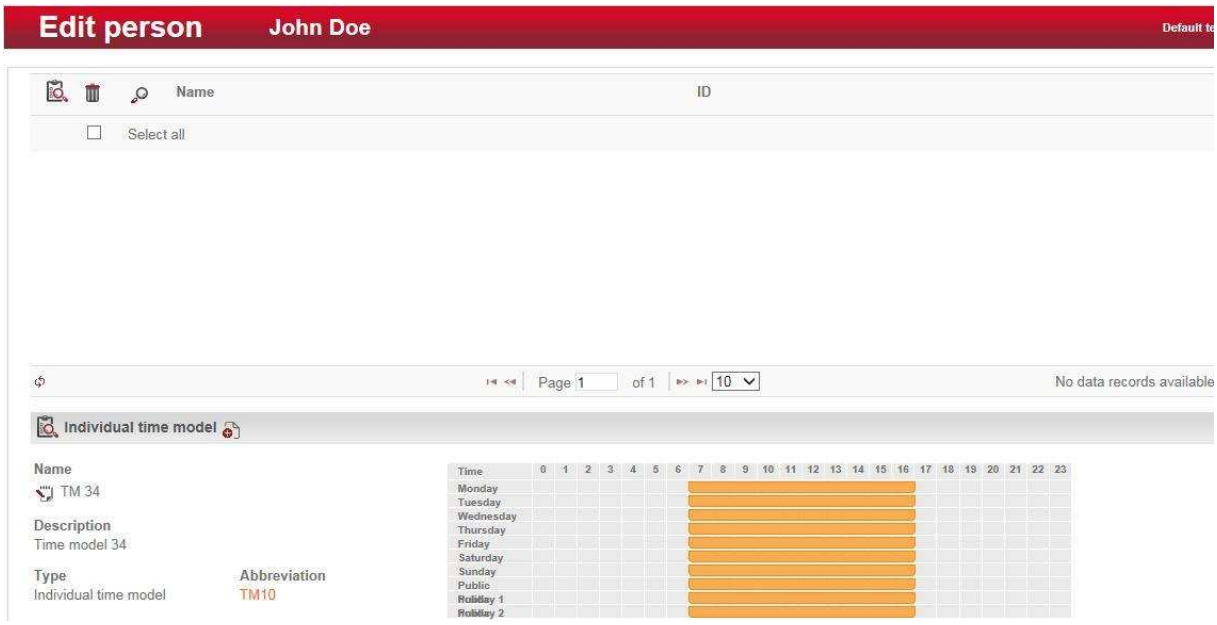
4.4.4. Enter/edit individual offline time models

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 4.4.



4.4.5. 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.



4.5. Group/organisational units

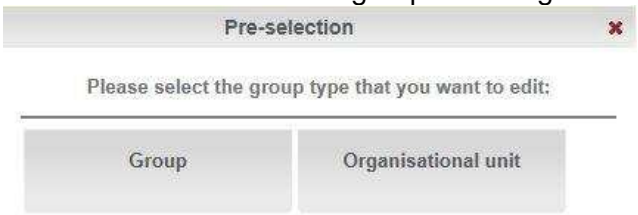
Groups/organisational units summarise selected person ranges. This means that access authorisations can be simply allocated later by assigning to authorised groups/organisational units.

Groups are project groups or work groups, for example. **Organisational units** usually represent departments or other hierarchical units. See 1.2.1.2.

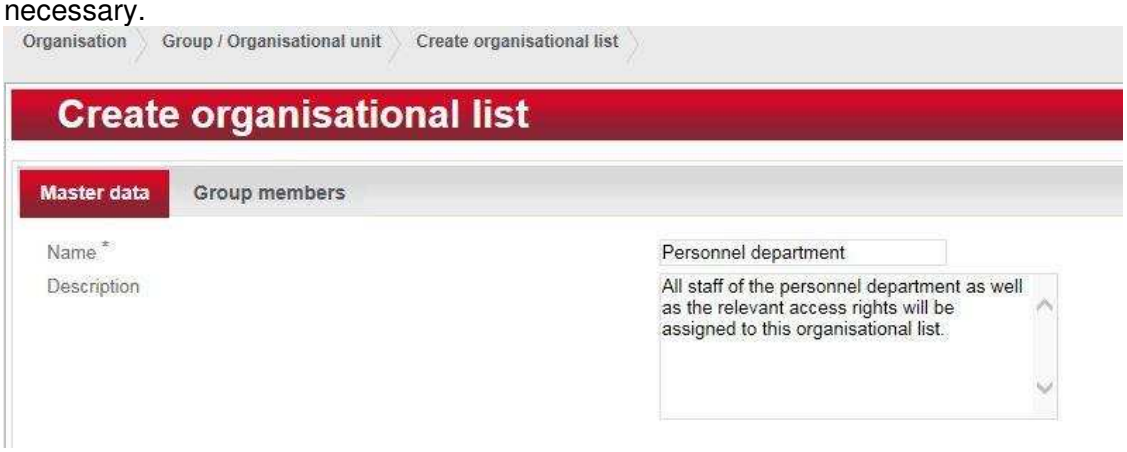
4.5.1. Enter group/organisational units

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.

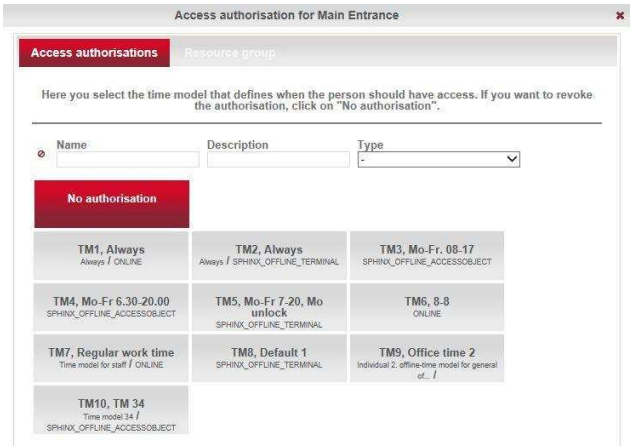


If a personnel master record has already been set up, people can now be assigned to the groups or the organisational unit under the “**Group members**” tab.

4.5.2. Assign authorisations for groups/ Organisational units

In the “**Authorisations**” tab in the **Organisation/Group/Organisational unit** menu, 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.

As shown below, all existing time models that are available are displayed. Mark the desired time model for the access point which is valid for this group or organisational unit.

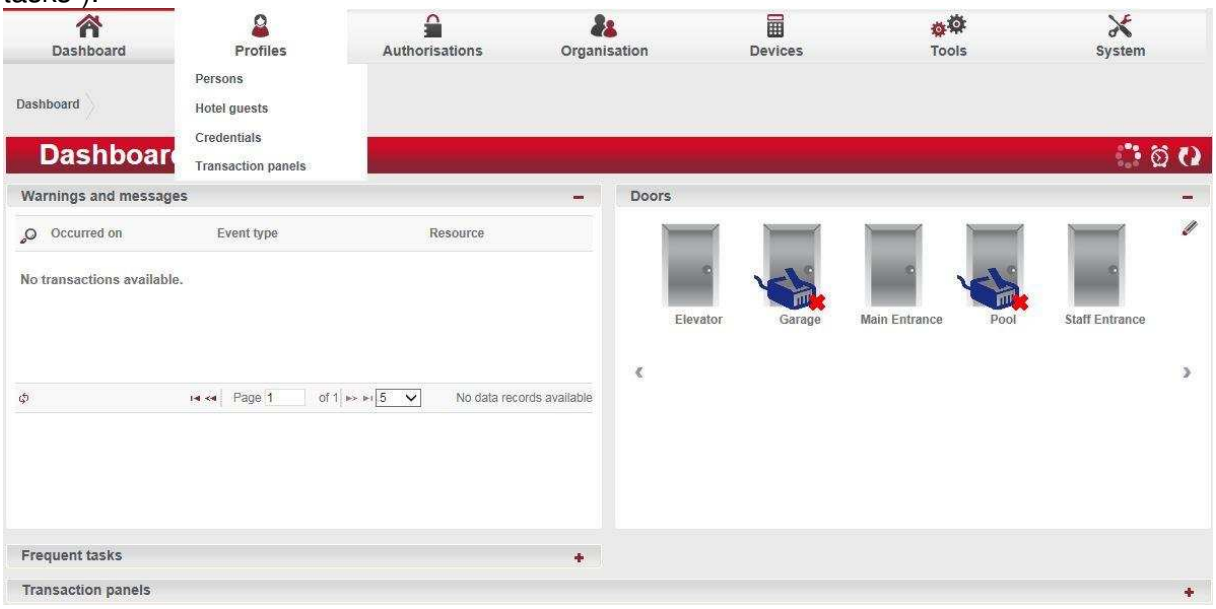


Save your selection 

4.6. The persons

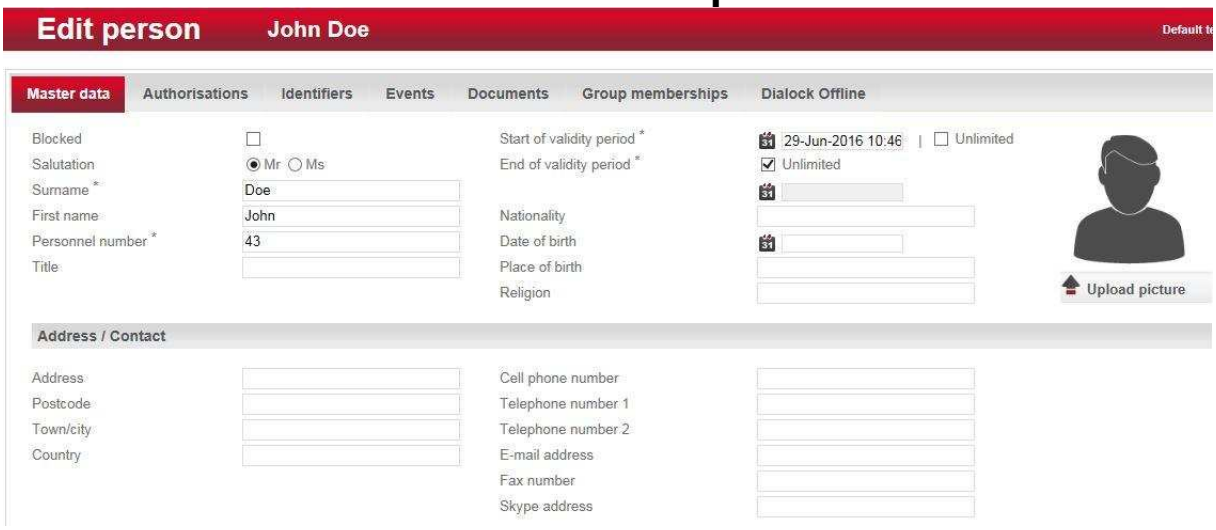
Now create the persons with their master data.
You have the following 3 options for this:

1. Via main menu navigation **Profile**/**Person**,
2. Via one of the definable **Quick accesses** in the right-hand sidebar,
3. Via "**Frequent tasks"** (provided that this has been assigned as one of your "Frequent tasks").



With options 2 and 3, you arrive directly at the creation screen; with option 1, you first select "**Create**" via the left hand sidebar.

4.6.1. Enter the master data for persons



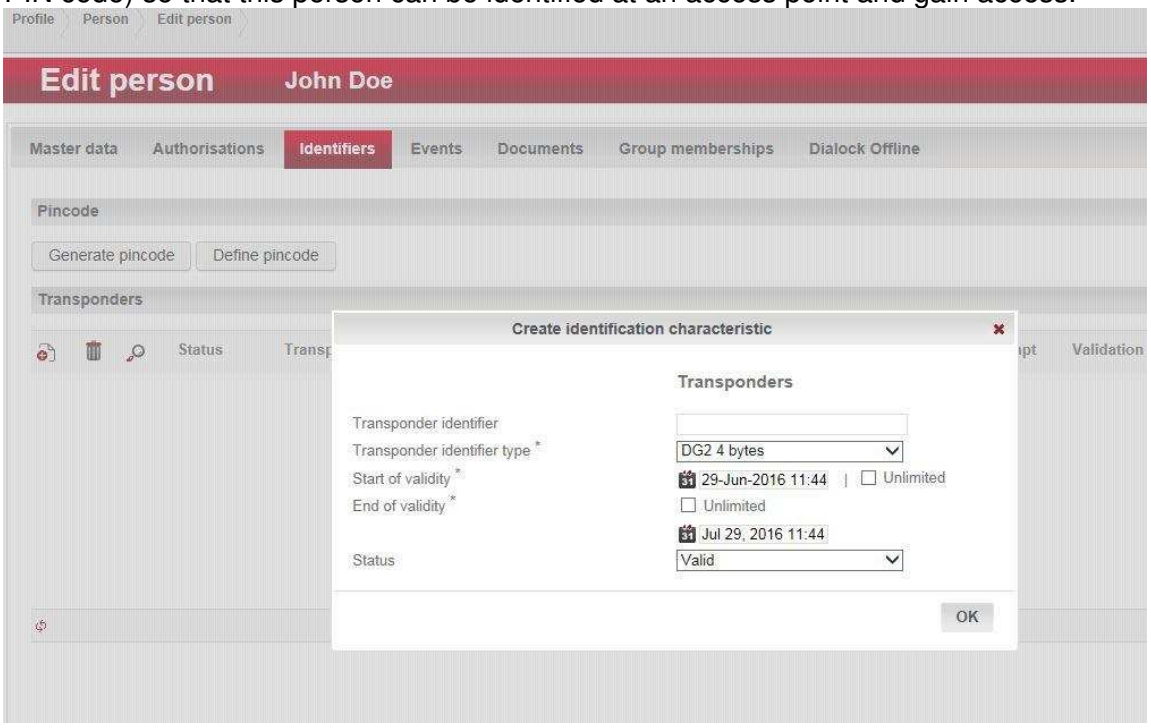
Enter the data for your new employee here. There are three mandatory fields:
Surname, start of validity and personnel number.

Enter the **Surname** of the employee.
If no **Personnel number** is entered, Dialock automatically assigns a successive number if this has been activated as described in chapter 11.1.
The validity range limits the duration of all assigned employee authorisations. Dialock automatically sets the **Start of validity** to the input date and the **End of validity** to “unlimited”.
Block an employee by saving an **End of validity**, if you wish, so that they do not have access authorisation immediately.
Enter further information depending on requirements.

4.6.2. Create/assign identification characteristic

In the “**Identifiers”** tab in the **Profile**/**Person** menu, you can create, edit or delete employee IDs. PIN codes are also generated here.

In this step, you assign the employee an identification characteristic (e.g. Transponder and/or PIN code) so that this person can be identified at an access point and gain access.



Generate a **PIN code**, if you are using a reader with a keypad, which requires a personnel code. Dialock sends the person the generated PIN code by e-mail.
Note: To do this, an e-mail address must be entered into the master data (see chapter 4.3.1.).

To create an ID, click on the symbol  and enter the **Transponder identifier** of the respective identification characteristic into 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 accepts the end of validity entered into the person master record.
Activate or deactivate an ID in Dialock via the **Status** drop-down field. **Valid** status means that the ID is active. All other status’ (locked, missing, forgotten) result in the deactivation of the ID in Dialock. Save your entries.

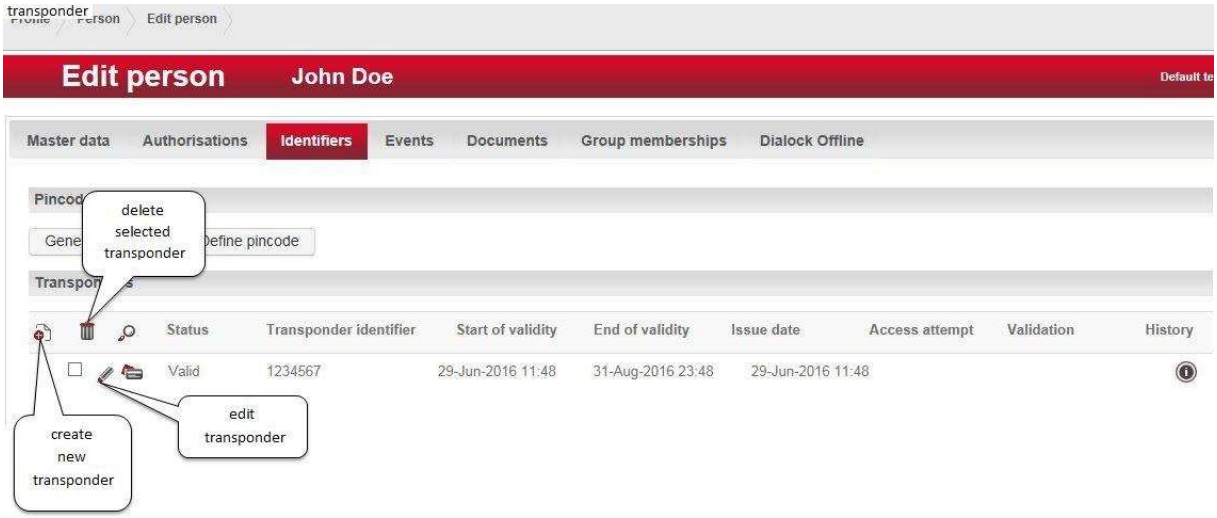
To **Edit,** i.e. to change the validity range and the status of the IDs, click on the pencil icon.

Delete the ID by marking it with a cross and clicking on the “waste bin” symbol. However, this only activates if the ID does not yet have any transactions.

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

Notes:

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

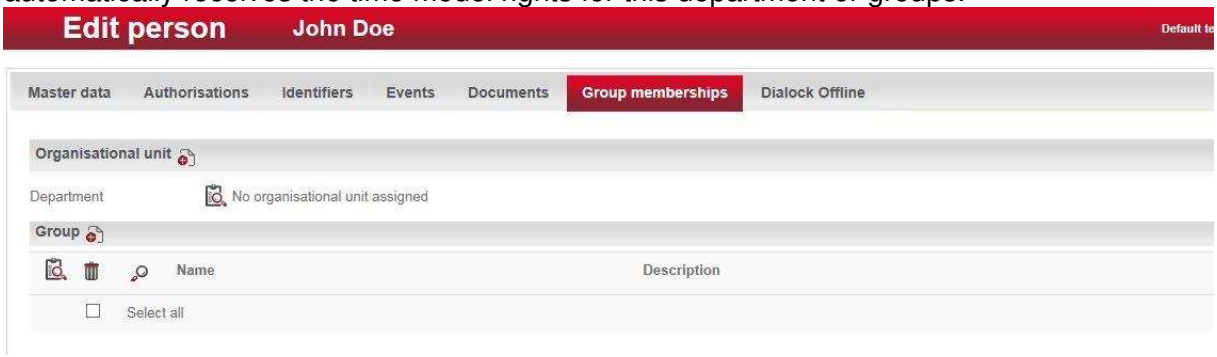


You can list the history of when a transponder was last edited, which status was changed when, who is the owner of the transponder, and the start and end of validity etc. using the Info button.

4.6.3. Assign groups/organisational units

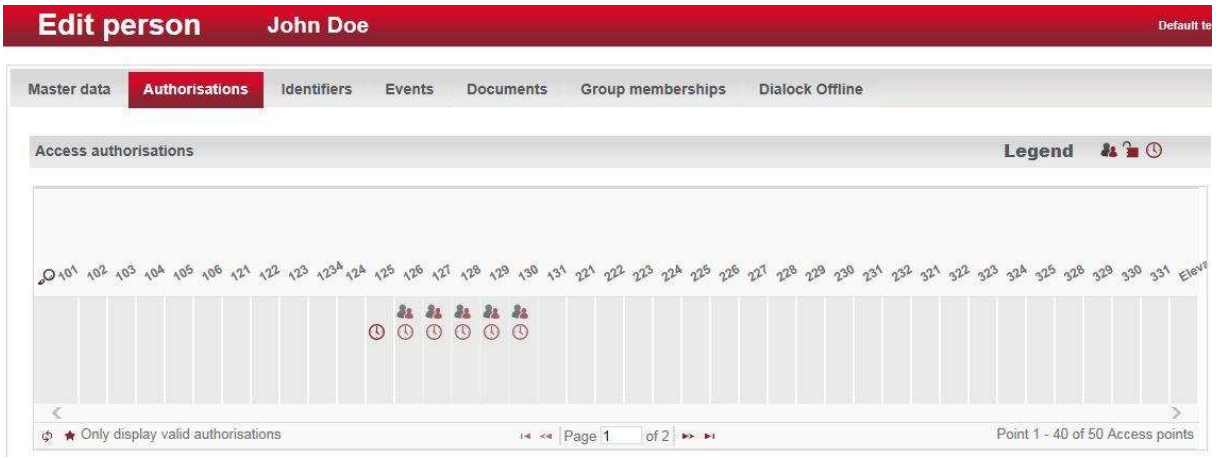
In the “**Groups/Organisational units**” tab under the **Profile/Persons** menu item, assign the person an **Organisational unit** from the drop-down menu.

You also have the option of assigning a person to one or more **Groups**. The person automatically receives the time model rights for this department or groups.



4.6.4. Assign individual authorisations

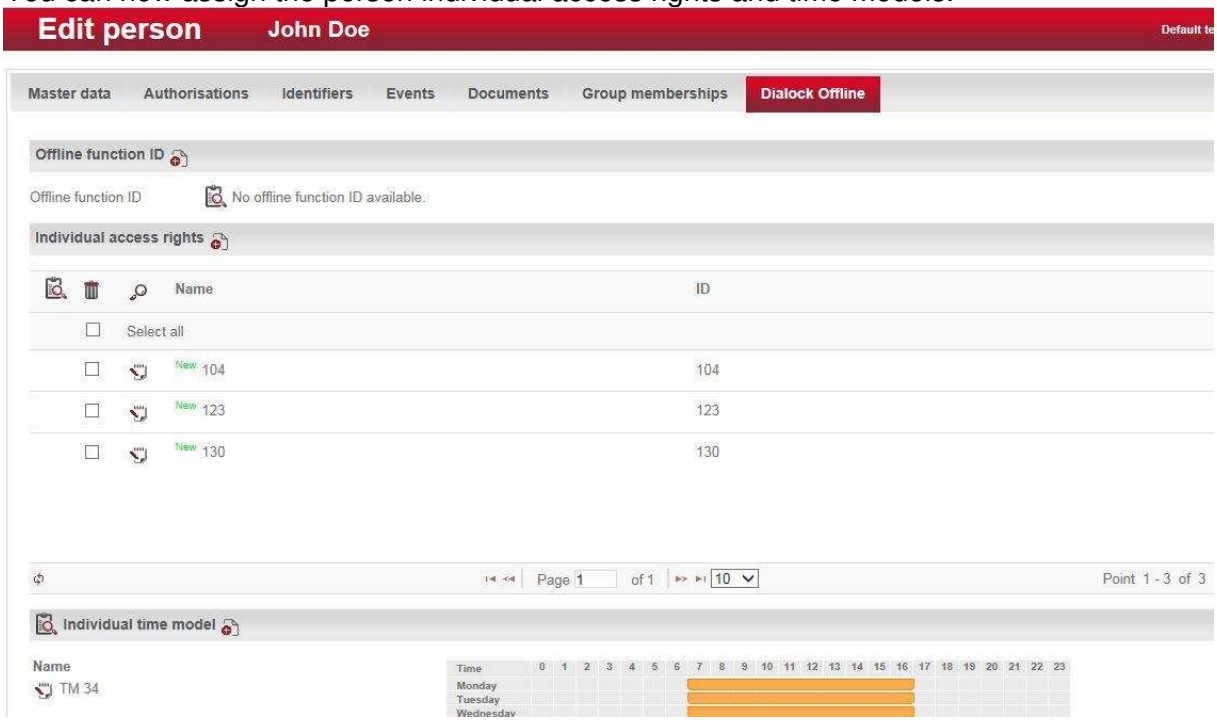
In the “**Authorisations**” tab under the **Profile/Persons** menu item, assign the previously set up time models individually. Click on the symbol in the column of the authorisations.
In the following example, you can see that time models have been assigned to person “John Doe”. The time model and the description of the access point can be displayed by moving the cursor over the time model symbol.



4.6.5. Adjust/edit offline parameters for persons

In order to make settings for a person who has access to offline areas, select the "**Dialock Offline**" tab in the **Profile**/**Person** menu.

You can now assign the person individual access rights and time models.



Special privileges:

Parametrisation privileges (MDU):
These are used to authorise a user to make changes to the configuration of the offline terminals and read out their logs using the data transfer unit MDU (Mobile Data Unit).

Door opening time, open time (sec):
This is the duration in seconds which a locking element is opened at an access point after a valid ID is held up to the access reader.
If it is set to 0, the standard opening time of the terminal is used. With all other values, a valid, differing time is set for this person.

Override “Do-Not-Disturb” status:
If the “Do-Not-Disturb” function has been activated at an offline terminal, this status can be overridden by the IDs which are assigned to this person. Example: Management key in a hotel.

Toggle rights by group locking rights:
If this tick mark is set in the special privileges, the ID that is assigned to this person may operate a terminal that is in toggle mode, i.e. unlock/lock.
This option is effective if the toggle mode is activated during a corresponding time period within a time model or by holding up the ID for a long time.

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 ID 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:

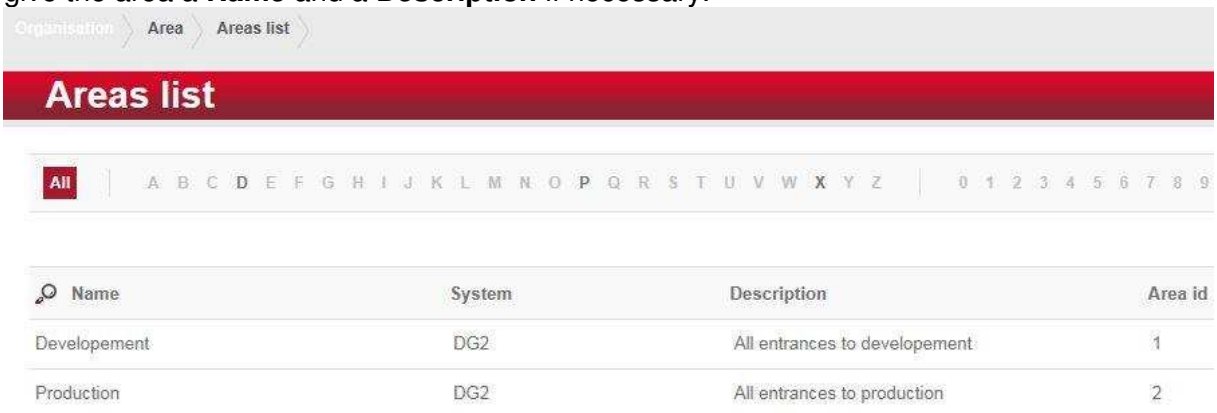
- With a value of 0, the transponder is not modified and uses the general validity of the transponder (see “Identifiers” tab).
- With a value of 1 to 9000 hours, the transponder’s time period is set to the specified value in the future
  (e.g. value set to 24: end of validity on offline terminals = current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

4.7. The areas

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.

4.7.1. 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.

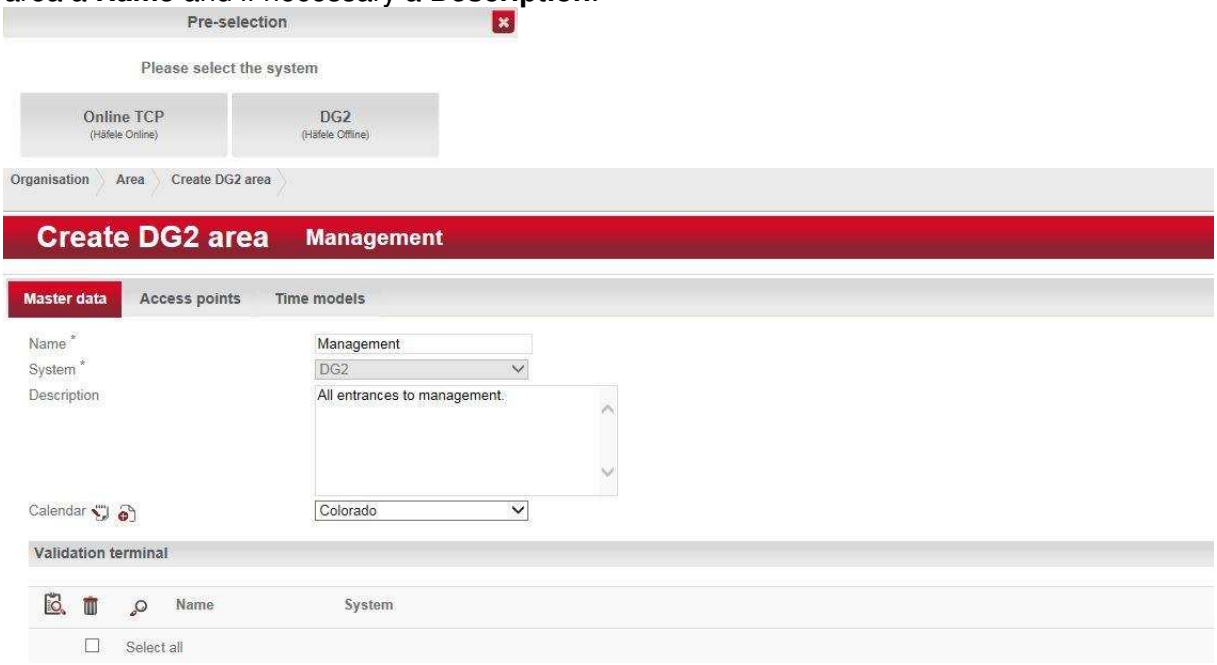


Now assign the associated access points to the area under the "**Access points**" tab with 

4.7.2. Create/edit offline areas

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

Create an offline area in the **Organisation > Area** menu (select Häfele offline) and give the area a **Name** and if necessary a **Description**.

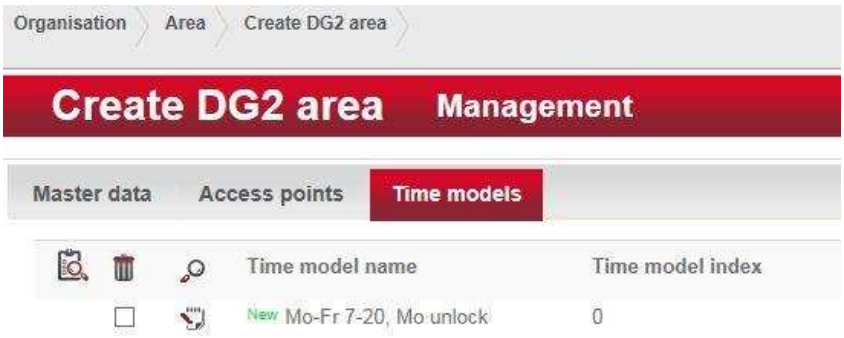


Select the associated **Calendar** which should be valid in this area.

Authorisation writers are online terminals that write the currently valid offline access authorisations on the ID 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.)

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 .



4.8. The 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 32,000 individual access rights. Max. 3 individual access rights can be saved on one card. Up to 400 individual access rights can be saved in an offline terminal.

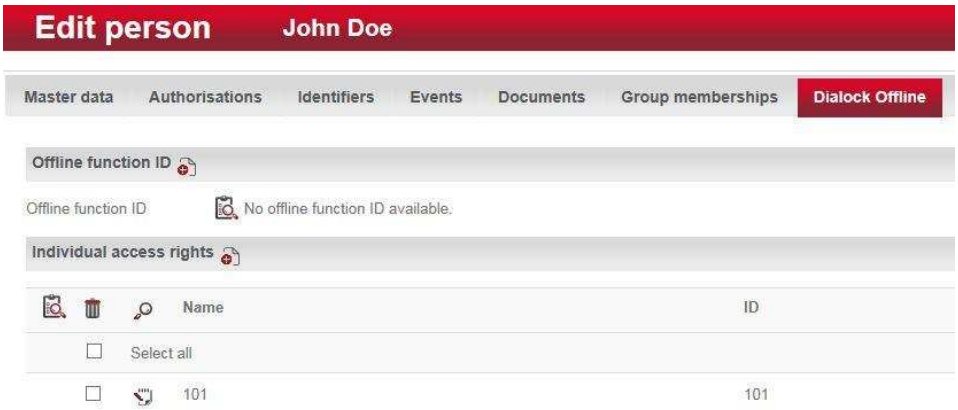
4.8.1. Create/edit individual access rights

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, assign a name for the **Individual access right** and adapt the ID if necessary (e.g. room number in the hotel).
Save.

Note:
In order to become effective, the individual access rights must be assigned to the offline terminals at which they are to be valid (see Chapter 6.2 Assign individual access rights in the offline terminal). The individual access rights must also be assigned to the persons for which they are to be valid (see below).

4.8.2. 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 .

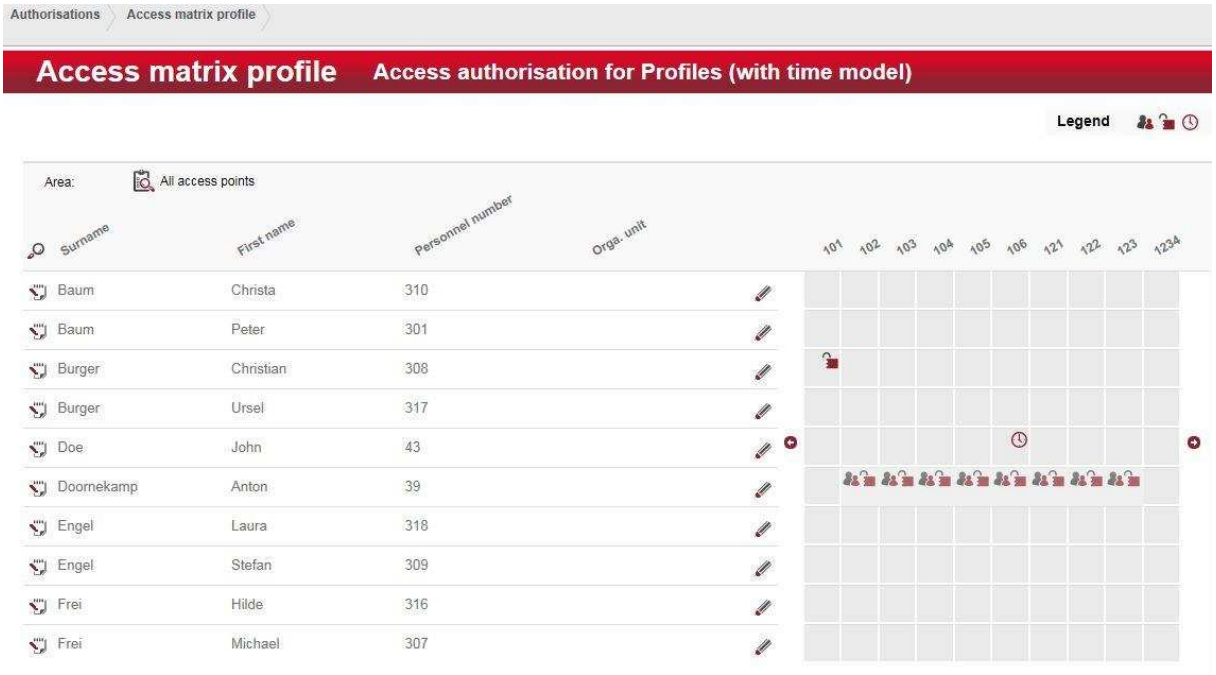


The settings are accepted with "Save".

4.9. The access matrix

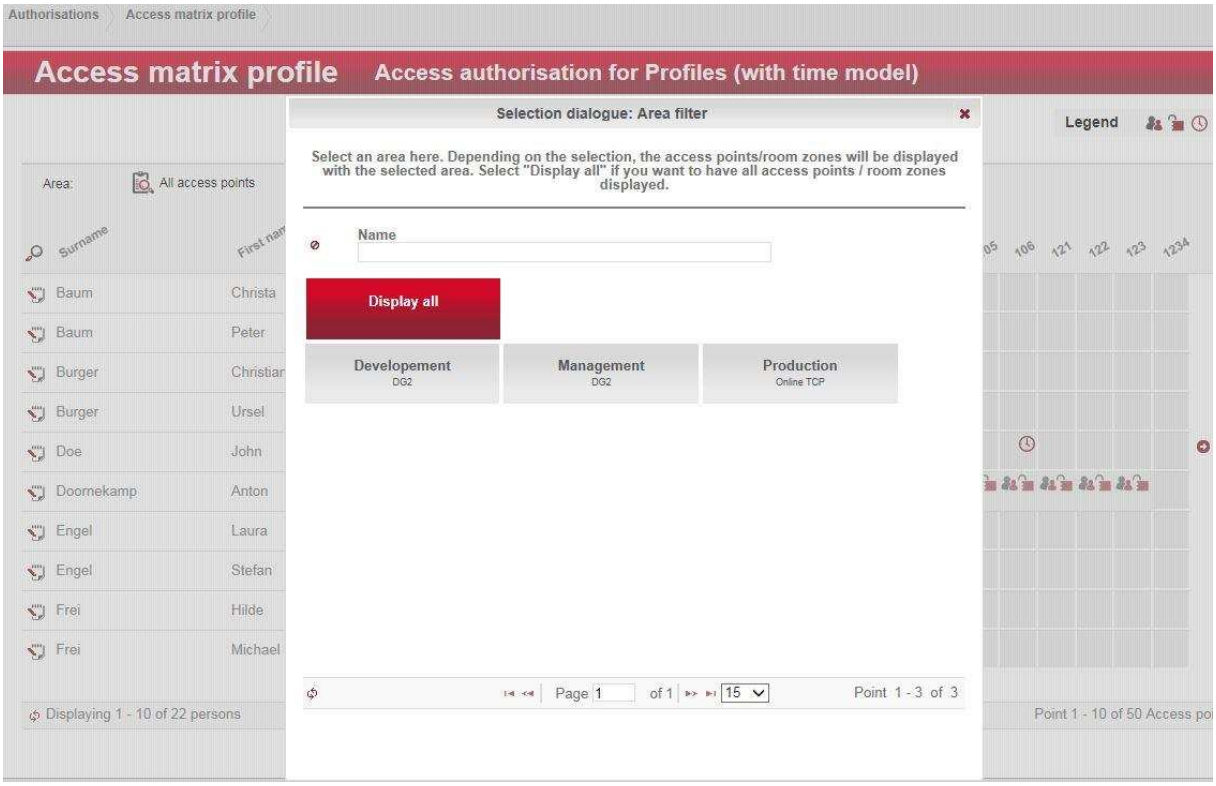
Via the **Authorisations**/**Access matrix profiles** and **Authorisations**/**Access matrix groups** menu, you are taken to the access matrix, which is both person-related and group-related. A person can be authorised individually as well as via groups or organisational units.

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 (see Chapter 4.3.3 “Matrix configuration”), 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**.

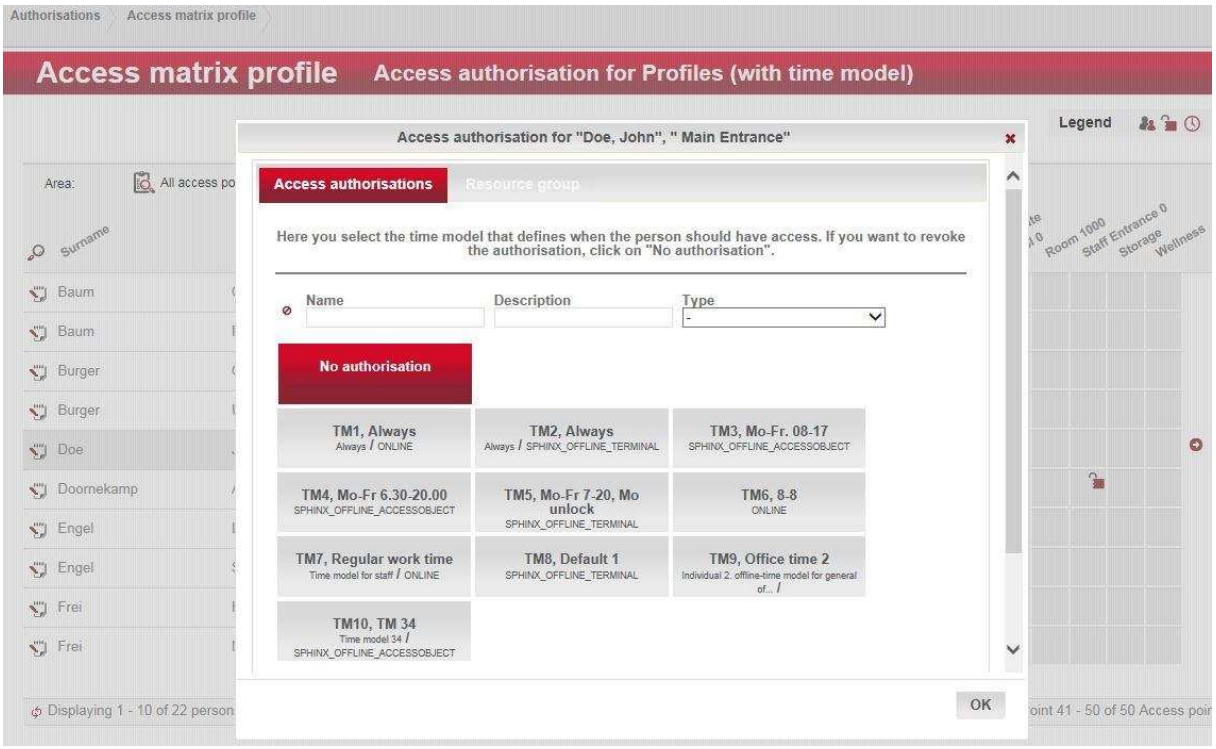
Select the desired **Areas** via the symbol . Now only the authorisations of the selected areas are displayed in the matrix.



4.9.1. 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 (see chapter 0).
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 "No authorisation" on the selection screen.



4.9.2. 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. With online terminals, select the associated time model in the additional menu that opens.

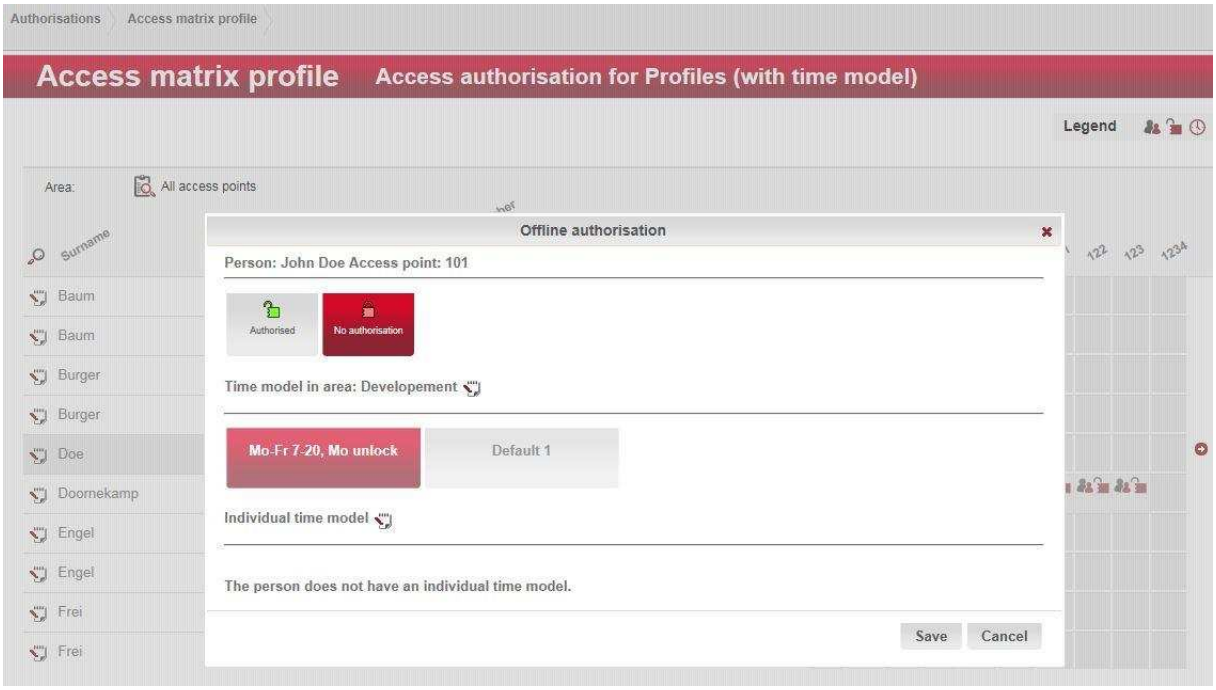
4.9.3. Allocation of authorisations in the access matrix for an offline access point

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. Select “**Authorised**” and save your selection.

In order to delete a person from offline access authorisation, proceed as above by clicking on “**No authorisation**” in the selection screen. Save your selection.

Furthermore, you have the option of setting a time limit for access authorisations by selecting one or more **Offline area time models**. Select the required time model(s) here. Save your selection.

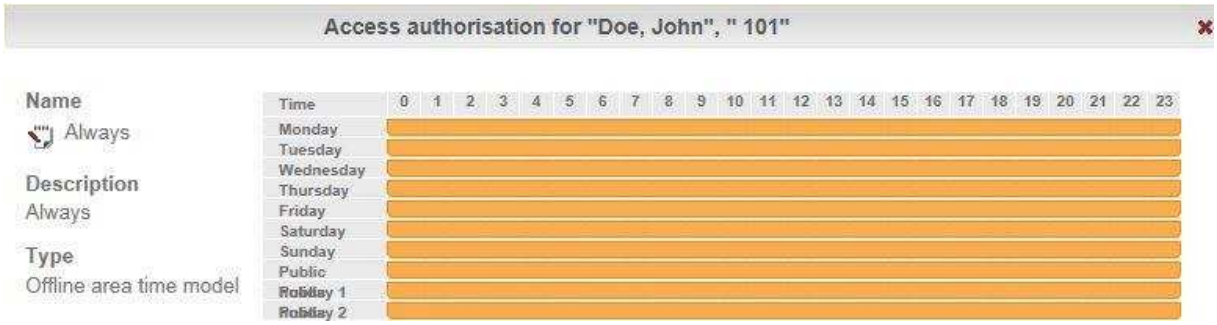
Note:
This change has an effect on the authorisation on all offline components that are assigned to the same area.



4.9.4. 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. Create devices (online hardware installation)

First, create the devices in your system such as terminals, barriers/doors, access points, readers, door release buttons, keypads and coding device as follows:

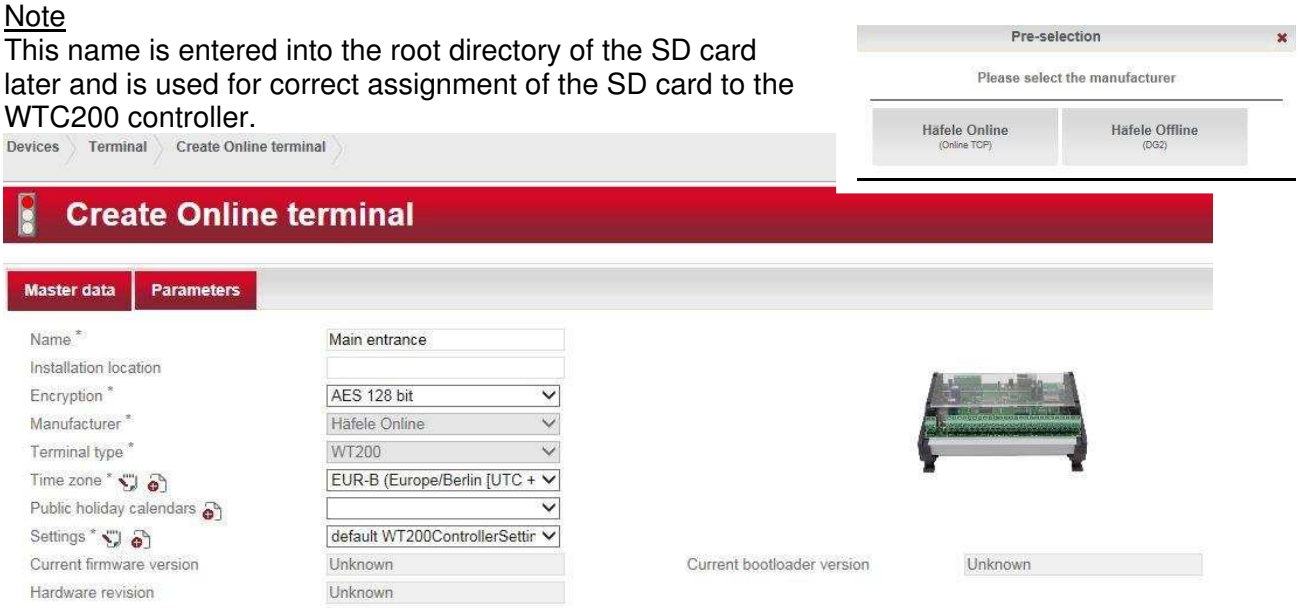
5.1. The online terminal

In order to establish a connection between the online terminal (WT200) and the Dialock software, the user programs an SD card at his PC workplace for each WTC200 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 WTC200 controller, provided that you work with the default values.

5.1.1. Enter online terminal master data

In order to create an online terminal such as the WT200, in menu **Devices/Terminal** select "**Create**" in the left-hand action menu. In the menu that now appears, click on "**Online TCP**" for a WT200 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 WTC200 controller.

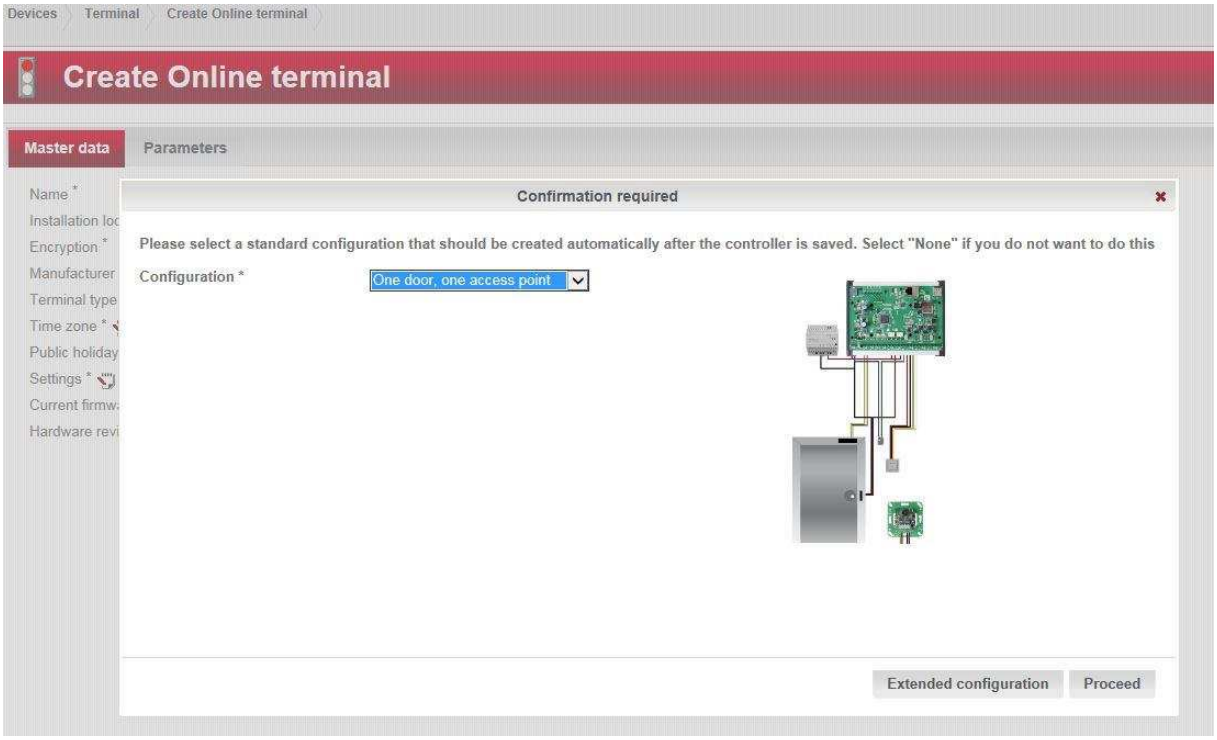


You can also describe the **Installation location** of the terminal, assign a previously defined **Public holiday calendar** to it, and assign the **Time zone** that is valid at the installation location to the terminal.

The current version numbers are specified under **Current firmware version** and **Current bootloader version**. You can call up the latest version by clicking on the Info button. If the loaded version matches the current version, the field flashes in green. If the version is not the latest version, the field flashes in red. You can find out how to update the firmware version or the bootloader version in Chapter 9 (firmware management).

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. More information about settings can be found in 7.

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.

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.

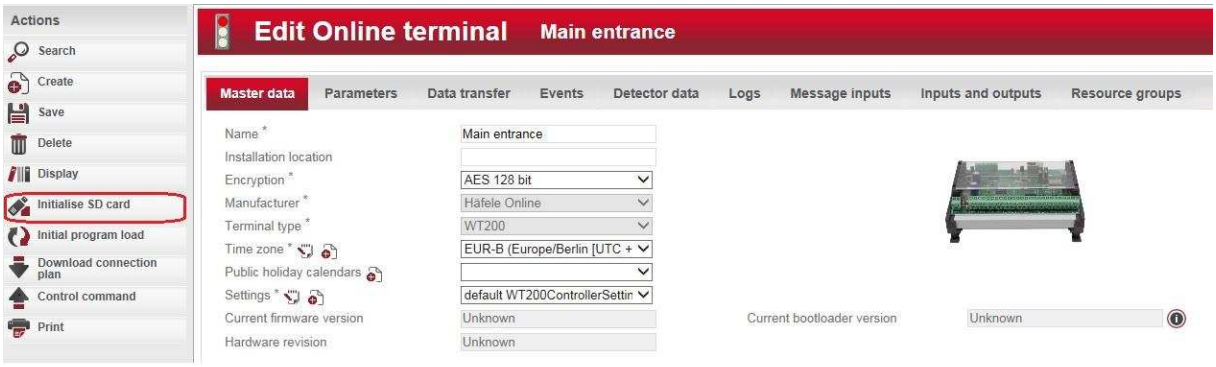
By clicking on the symbol ▸ you can obtain a display of the columns for the associated doors/barriers, access points etc. or hide them if you wish.

Right click to edit or delete parameters.

Initialisation of SD cards / Commissioning of a controller

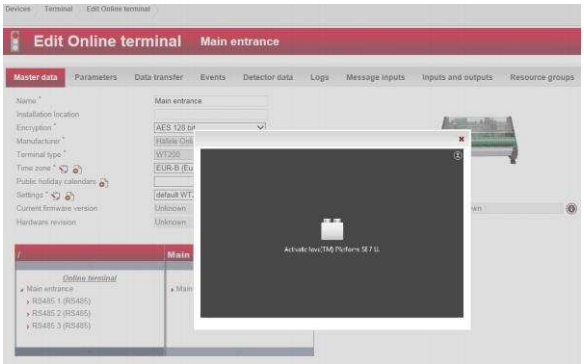
In order to start up a WTC200 controller, the SD card needs to be initialised. Always use the Micro SD card that was supplied with the WTC200 controller. Ensure that you are at a workplace with an appropriate card reader and insert the card there.

Then click on “Initialise SD card”.



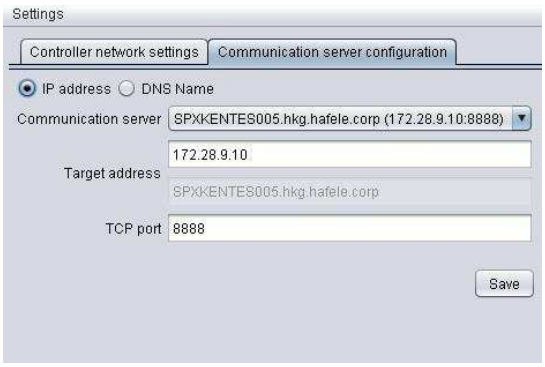
A Java applet is now activated so that the browser software can access the SD card slot of your PC. Click on “Activate Java applet” and “Run”.

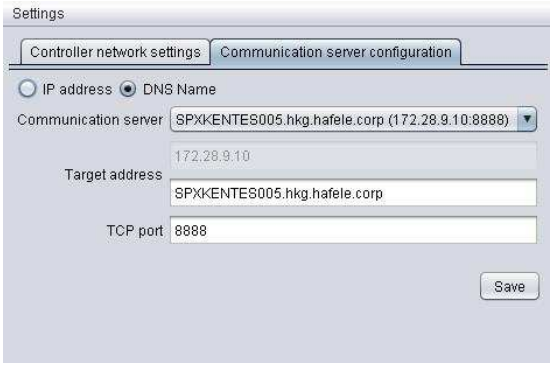
Note:
Different dialogue windows appear depending on the security settings. If your Java version is not up to date, you are automatically taken to the Java download page on the Internet http://java.com/en/download. You can download the latest Java version here. Follow the relevant installation instructions.



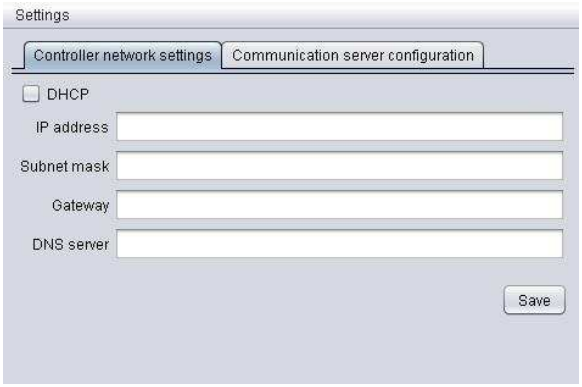
Ensure that you are in the “Settings” window after installing the latest Java software.

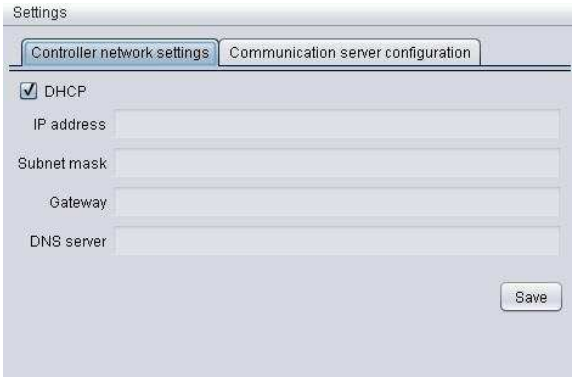
The IP address is entered automatically by the system, as is TCP port 8888. If this port is not free, select another suitable port.
The DNS name is also entered automatically by the system and can be changed if required. However, it is advisable to use the default values if possible.





If you use DHCP, nothing else needs to be entered in the “Controller network settings” tab. If you do not use DHCP, enter the data provided by your system administrator in the fields.





Click on Save and select the volume of the SD card as the storage location.

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).

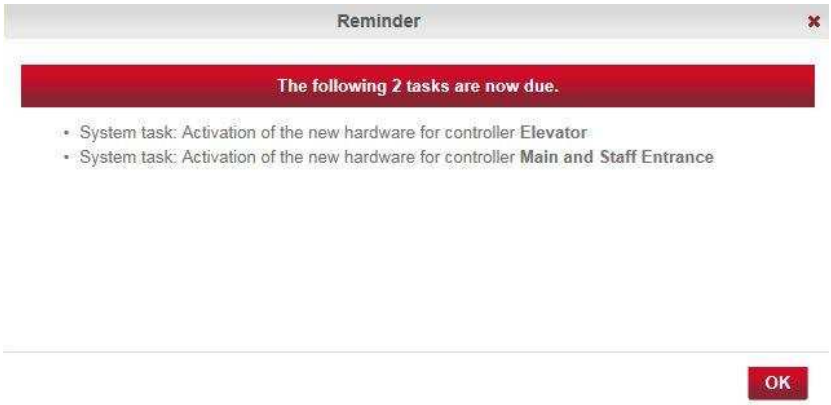
Now establish the network connection by inserting the network cable into the provided slot of the controller. The yellow LED at the network connection must flash slowly if the link to the network exists.

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 WTC200 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 WTC200 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**.

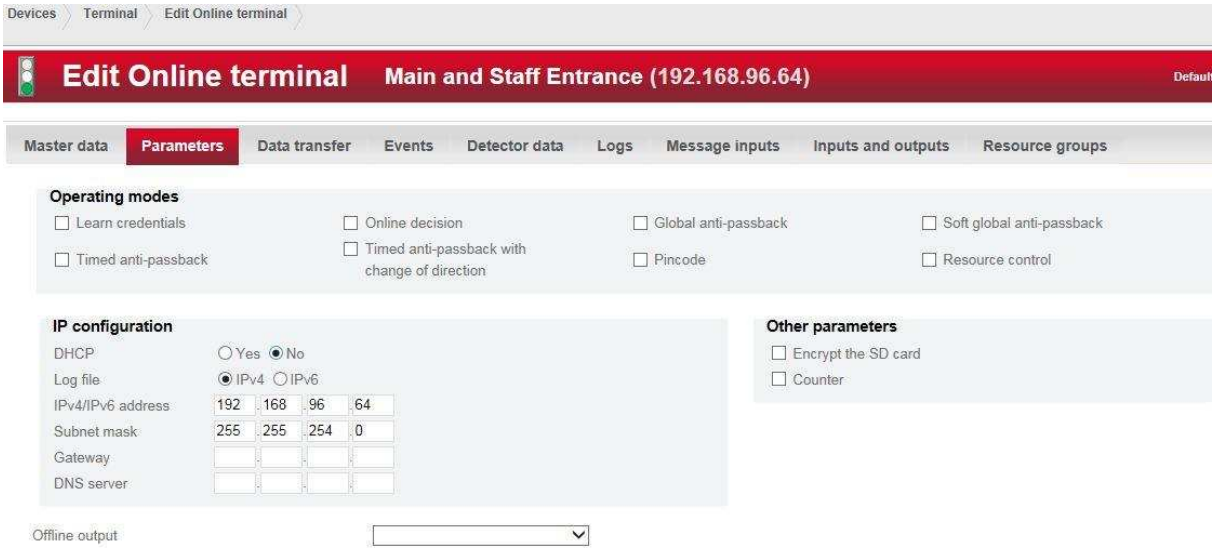
Delete permanent memory should only be carried out after explicit instructions from a responsible technician.

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

5.1.2. Online terminal parameter settings

(this area requires expert knowledge)

The different operating modes are set in the “**Parameters**” tab. The operating modes “Learn credentials”, “Online decision”, “Global anti-passback”, “Soft global anti-passback”, “Timed anti-passback” and “Timed anti-passback with change of direction” are currently still in the planning.



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

Learn credentials
The terminal sends an enquiry to the system about an unknown ID. If the ID is authorised, the unknown ID is included in the list of valid IDs.

Online decision
The terminal makes a decision online concerning an access permission and transmits this to the system, which confirms or revises it.

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 card 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.

Timed anti-passback
Activation of the timed anti-passback 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 reader with a PIN code keypad is going to be operated at this terminal. The PIN code must be generated for every person in the person masterrecord.

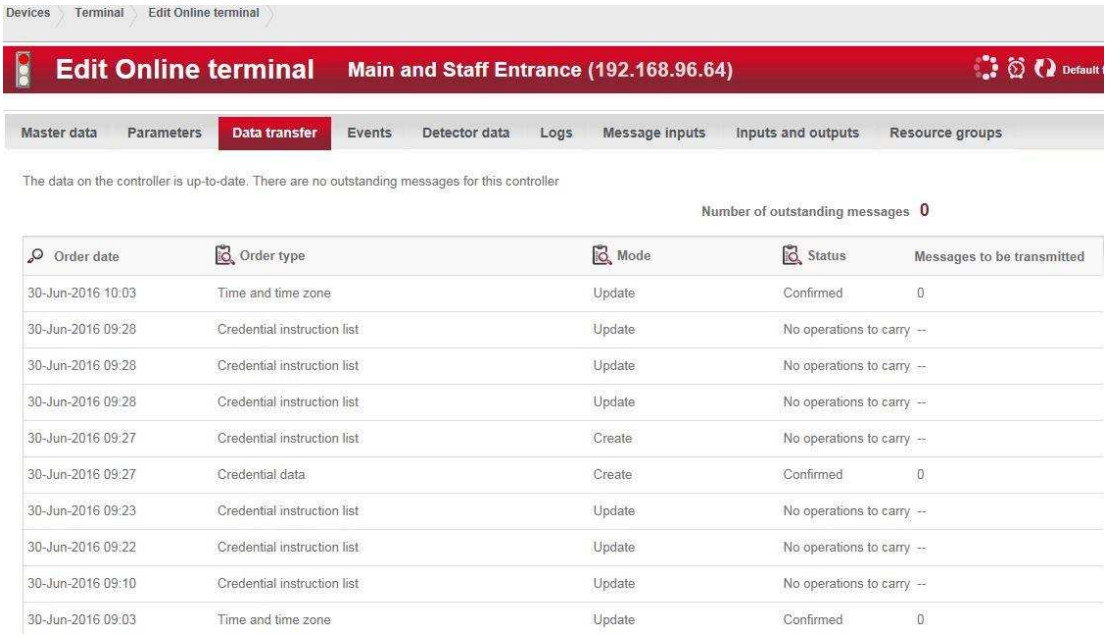
IP configuration
If DHCP is marked with “Yes”, no more entries need to be made here. If you do not use DHCP, please make the relevant entries in accordance with your IT administration. This information must be set in accordance with the specification of your department so that the terminal can communicate 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 WTC200 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.

5.1.3. The data transfer in the online terminal

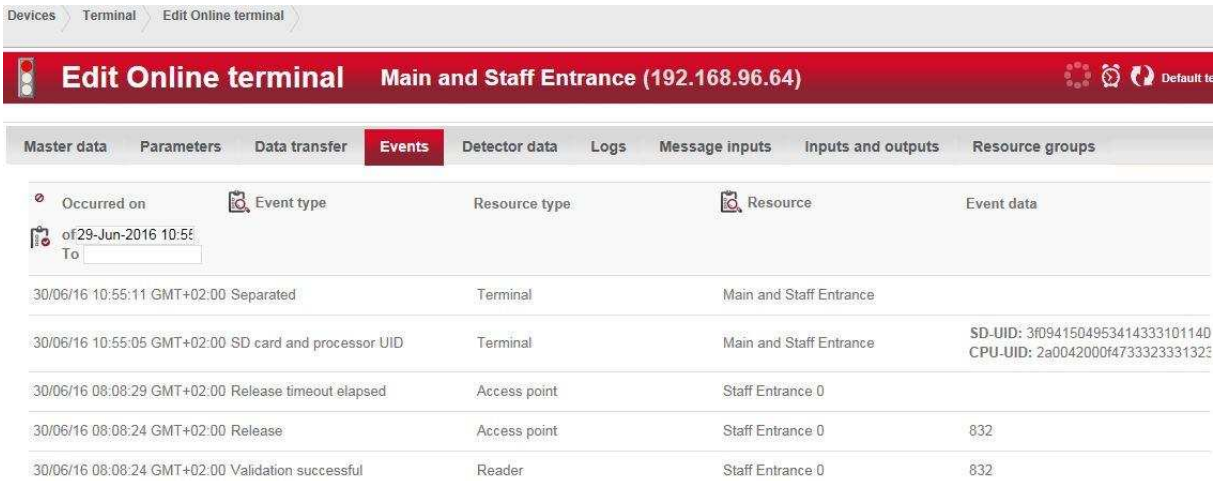
The “**Data transfer**” tab displays the difference from the target/actual comparison of the data to be transferred. All data packages that are pending for transfer can be found here.
The newest logs are at the top.



5.1.4. The events in the online terminal 1

(this area requires expert knowledge)

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.



5.1.5. The events in the online terminal 2

(this area requires expert knowledge)

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.

5.2. Edit barriers/doors

The **Devices/Barriers/Doors menu** takes you to the editing screen of the barriers or doors.

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

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.

Alarm control
The signalling of a door alarm is set by default. This door alarm lasts for as long as the “Alarm duration” (see tab “**Outputs**” in the **Devices/Barriers/Doors** menu) is set, but no longer than 3,600 seconds, i.e. 1 hour.
Activate this check box if the alarm is to last for as long as the door is open (feedback contact). The alarm time, which is a maximum of 3,600 seconds, starts when the door is locked. This means that the alarm relay is activated during the entire door opening time plus the alarm time.

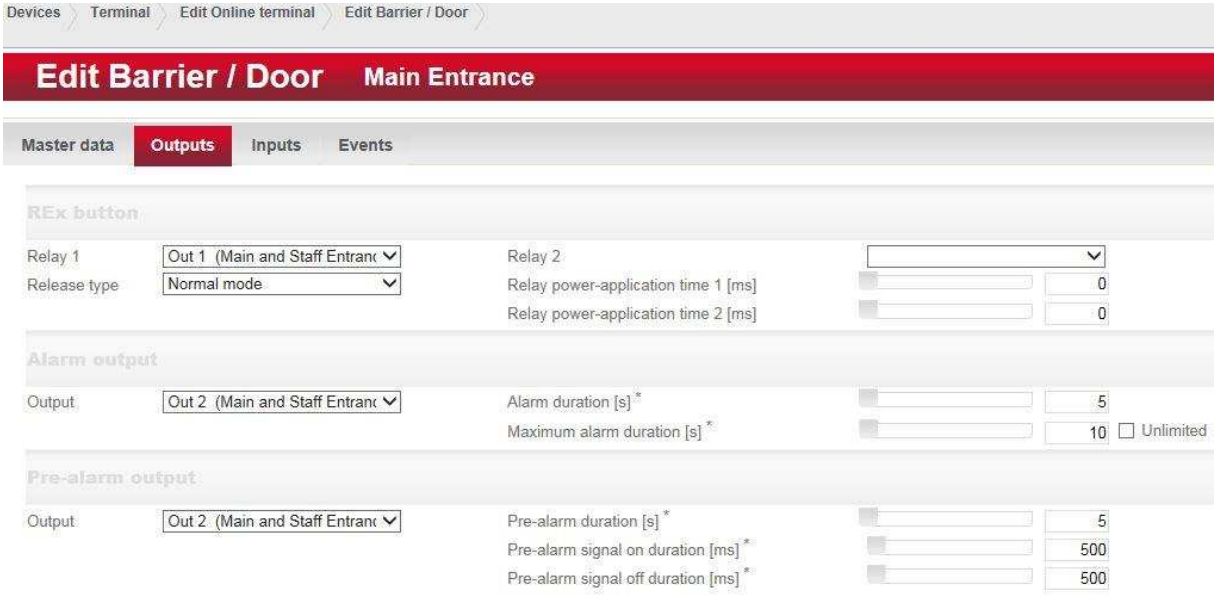
Intrusion alarm suppression
If this door operating mode is activated, intrusion alarms are suppressed at this door. This setting is recommended if the door has neither a reader nor a door release button on the

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 door opener 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.

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.



Door opener:
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.

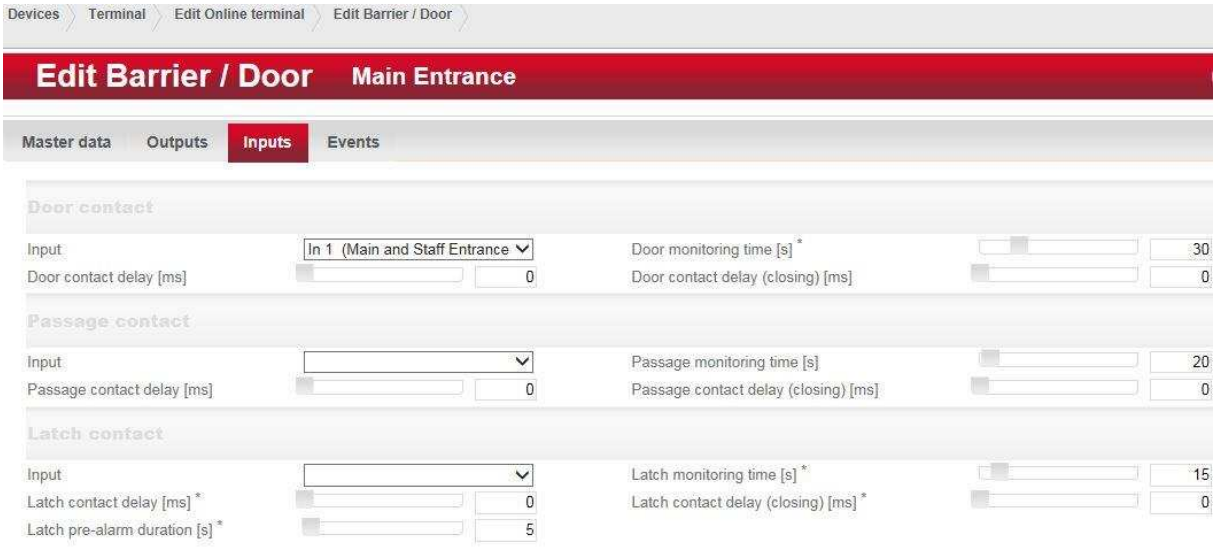
Alarm duration:
The alarm duration represents the actuation time of the alarm relay.

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.

5.2.3. 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:
Input:
Select the required input for door monitoring from the drop-down menu.

Door monitoring time:
This represents the duration 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:
Here you define the input that is used 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 monitoring delay:
This describes the time by which the passage contact can be activated with a delay.

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

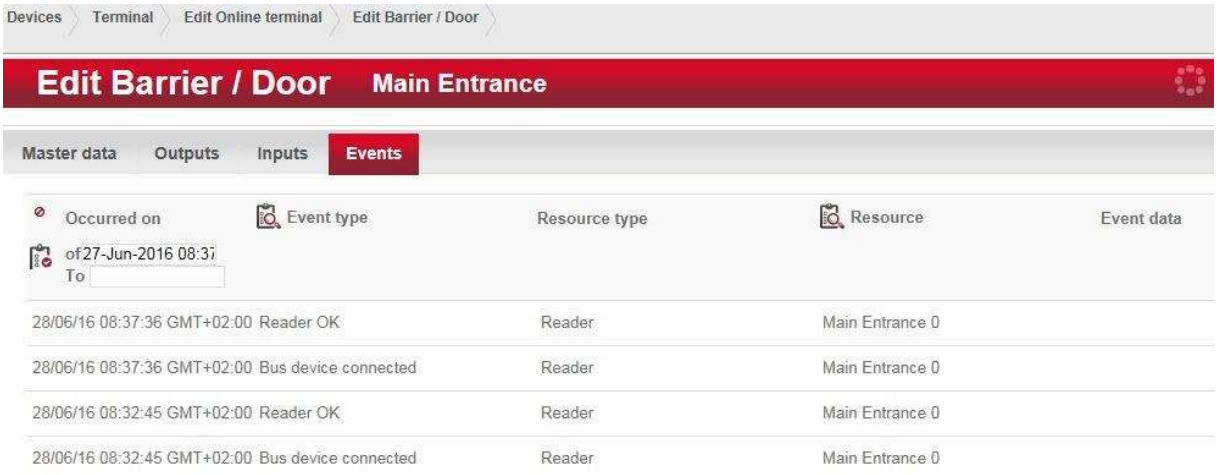
Latch monitoring time:
This represents the duration for which the latch may not be extended without the door alarm being triggered.

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.

5.2.4. 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.



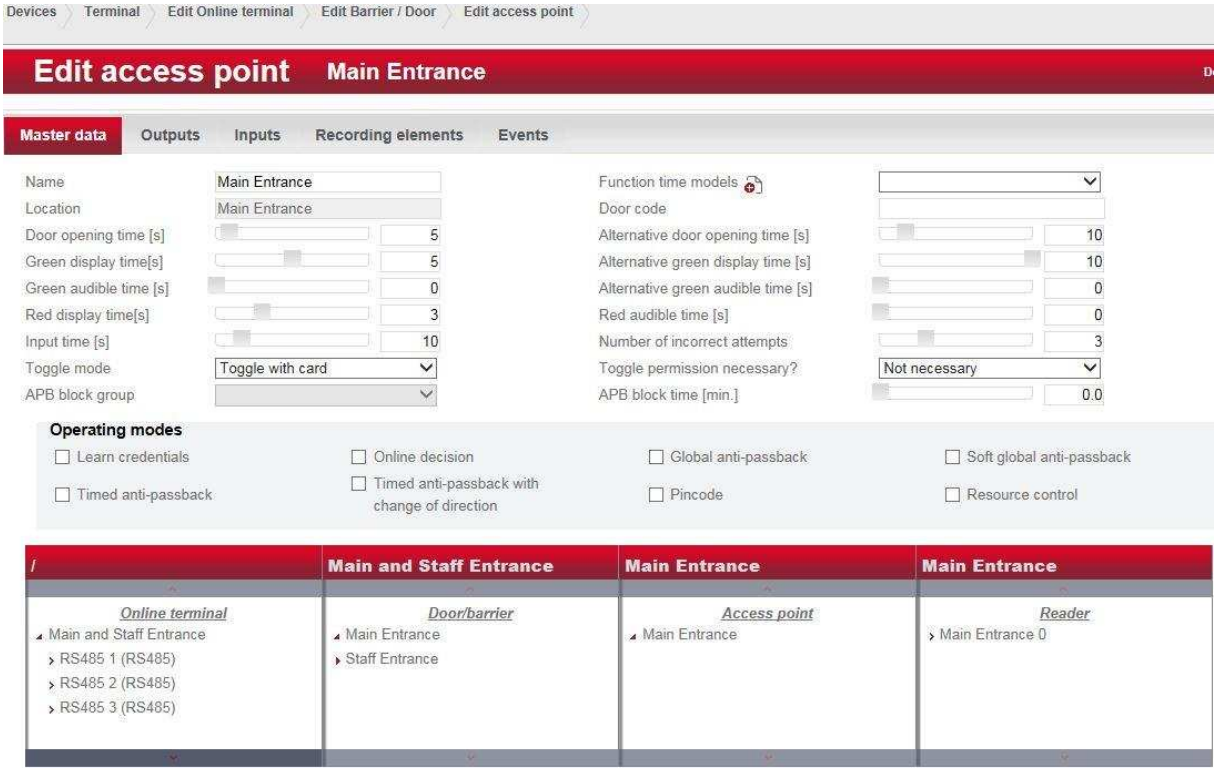
5.3. Edit access points

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**”.

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** as shown in chapter 5.1.2 “Online terminal parameter settings”.

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.

5.3.3. 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 card 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 card or a valid code was entered.

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.

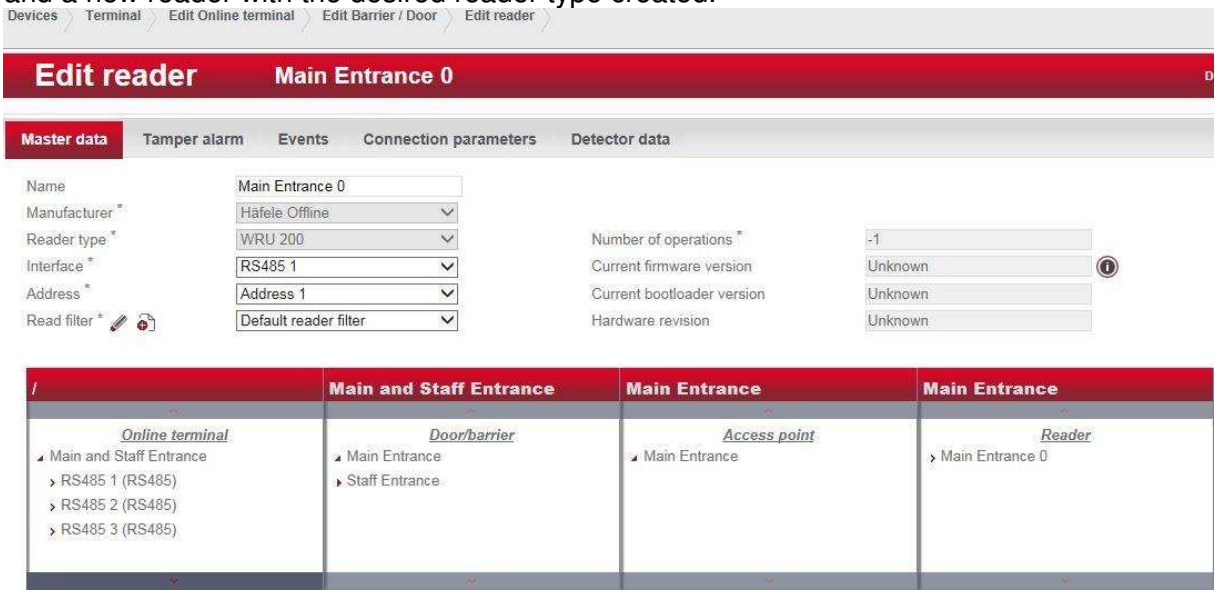
5.4. Edit reader

The **Devices**/**Readers** menu takes you to the reader editing screen.

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

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.



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.

5.4.1.1. Elaboration: Create/edit reader filters

(this area requires expert knowledge)

Clicking on the create or edit symbol in the “**Master data**” tab in the **Devices**/**Readers** menu takes you to the editing/creation of **Reader filters.** The reader filters can also be called up using the **Devices**/**Reader filters** menu.

You can individually determine the **ID 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 ID, drag the required number from "**Available reader characters**" with the mouse button held down to the required location of the **ID composition**. Please note that all locations of the ID 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).

5.4.2. 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**.

5.4.3. 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.

5.4.4. Connection parameters of the reader

(this area requires expert knowledge)

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.

5.4.5. Reader detector data

(this area requires expert knowledge)

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.

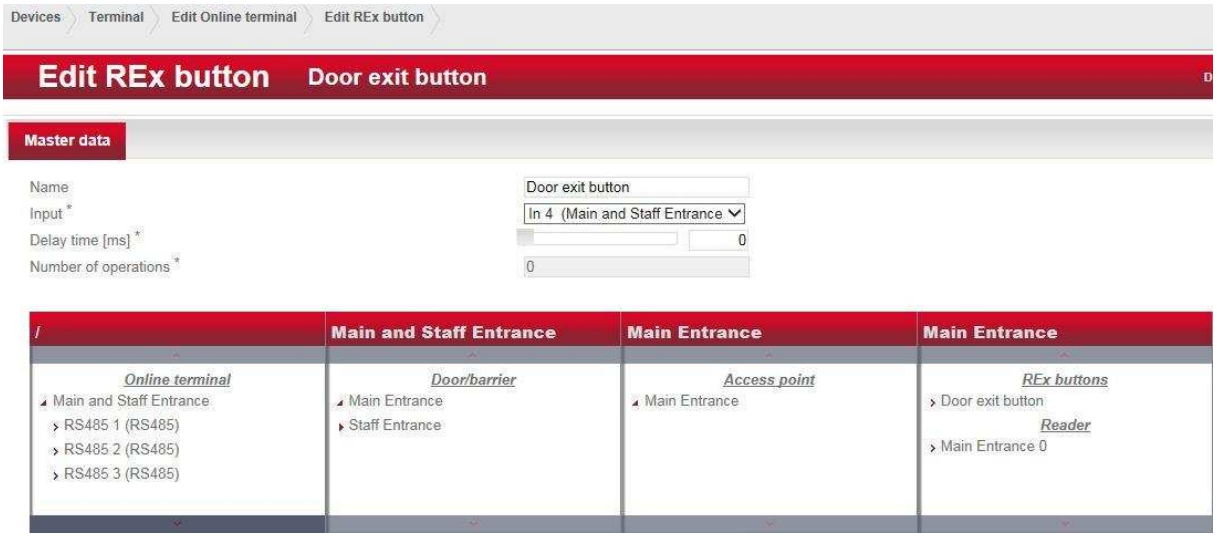
5.4.6. Edit door release button

The **Devices/Door release button** menu takes you to the reader editing screen.

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

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

If necessary, you can set a delay for switching the door release button under **Delay**. The **Number of operations** shows how often the door release button has been used (numeric).

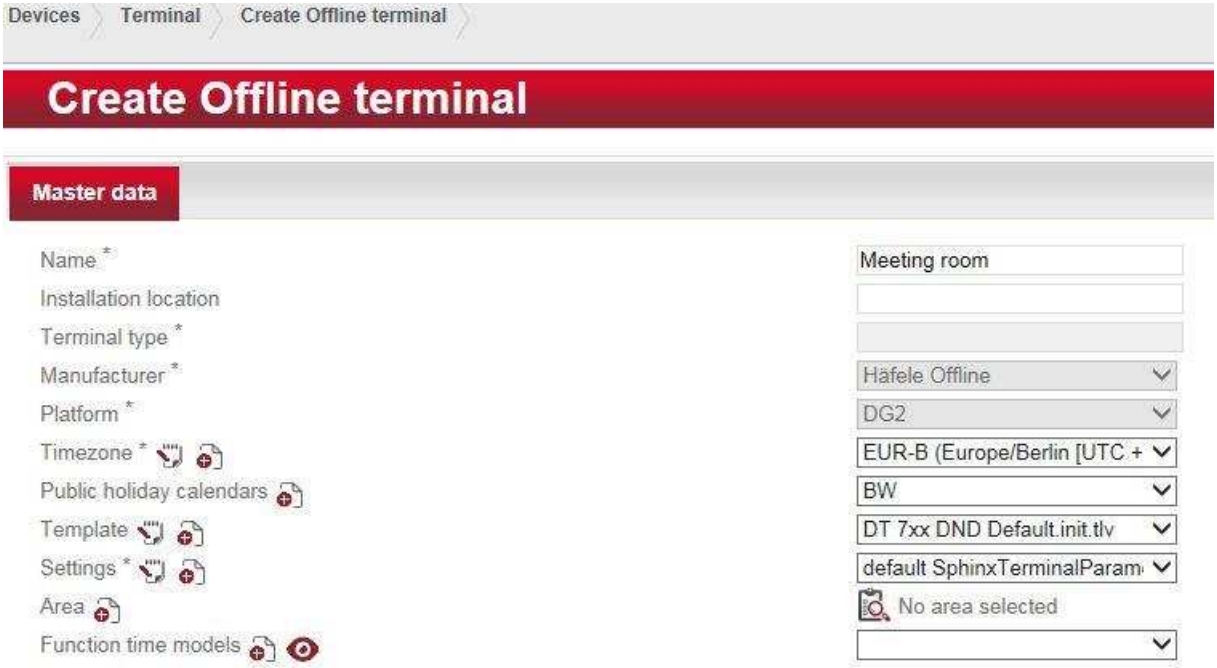


6. Create devices (offline hardware installation)

6.1. The offline terminal

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

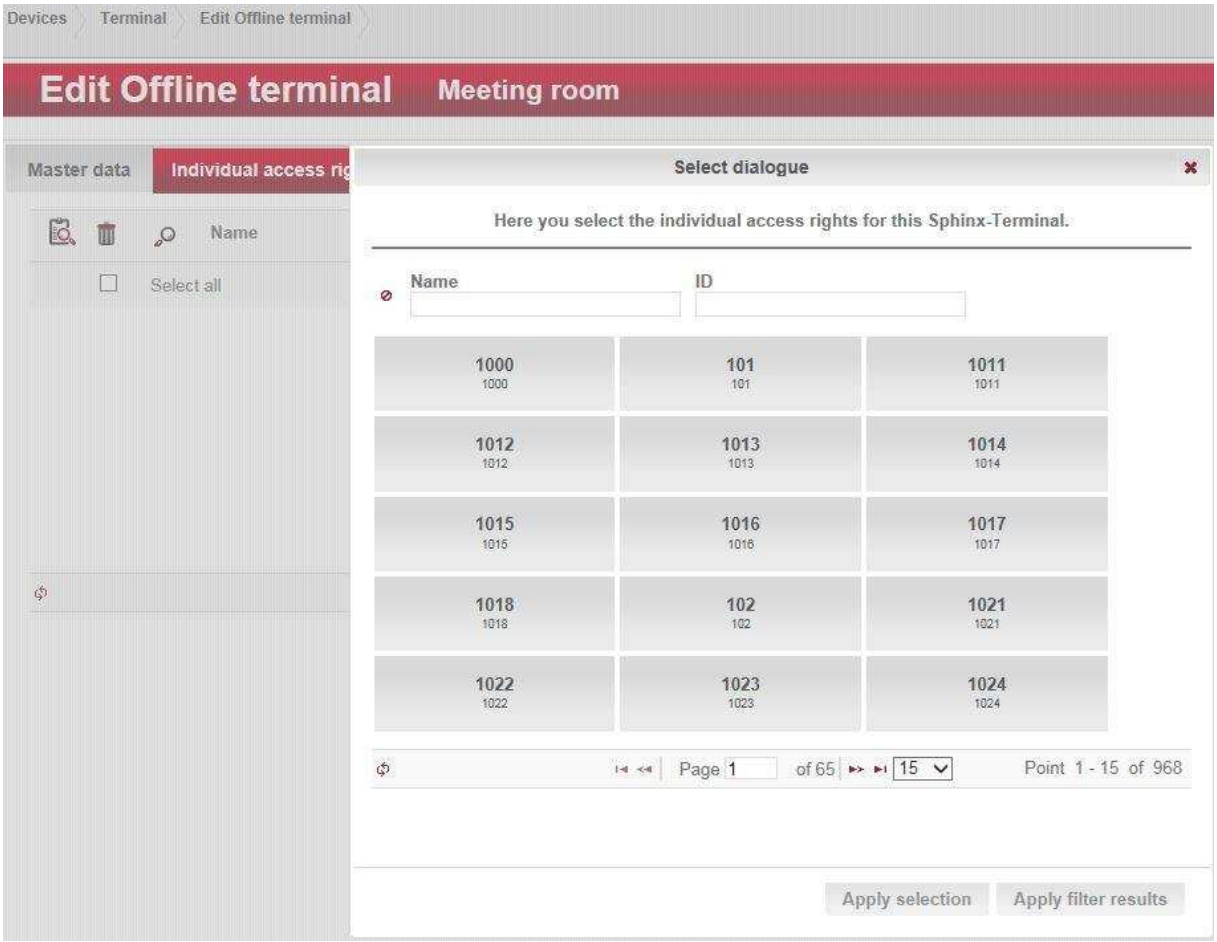
Here you can choose between Häfele online terminals and Häfele offline terminals. In this case, select **Häfele Offline.**



Enter the designation of the access point that will subsequently also be displayed in the access matrix as “**Name**”.
The “**Short name**” will appear later in the MDU data transfer unit (i.e. Mobile Data Unit). Use a maximum of 6 characters for this.
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 (see Chapter 4.7 “The areas”).

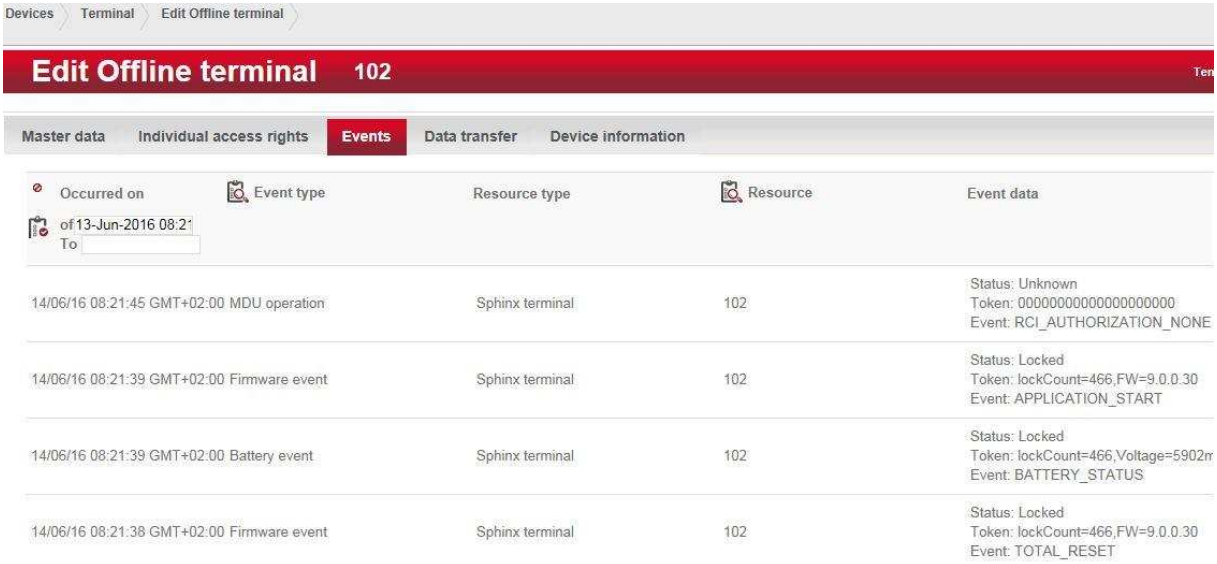
6.2. Assign individual access rights in the offline terminal

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

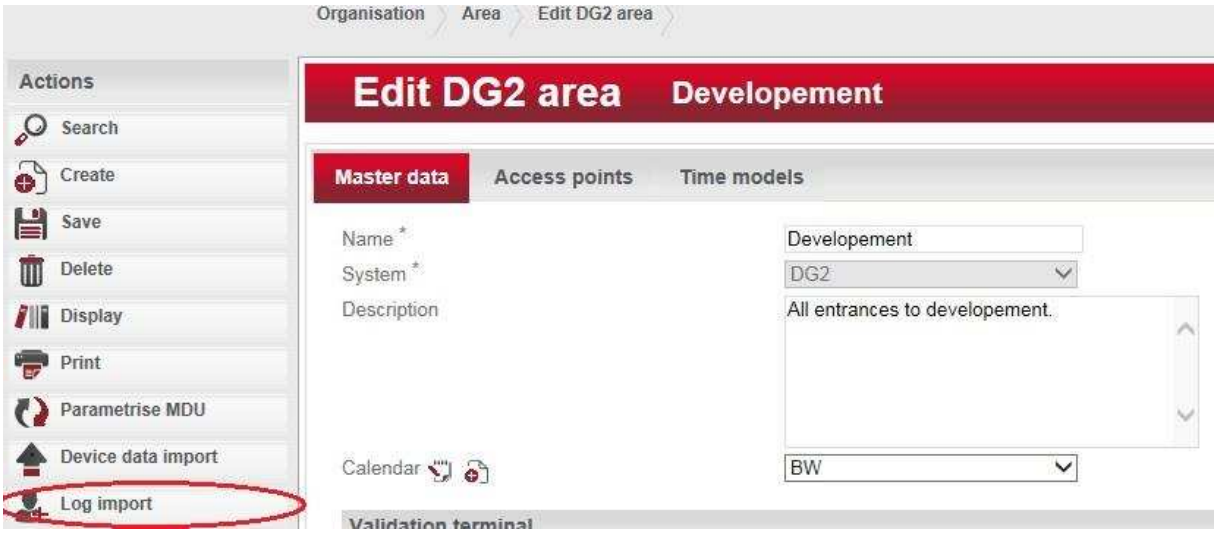


6.3. Show offline terminal events

A Dialock offline terminal can save at least 1000 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.

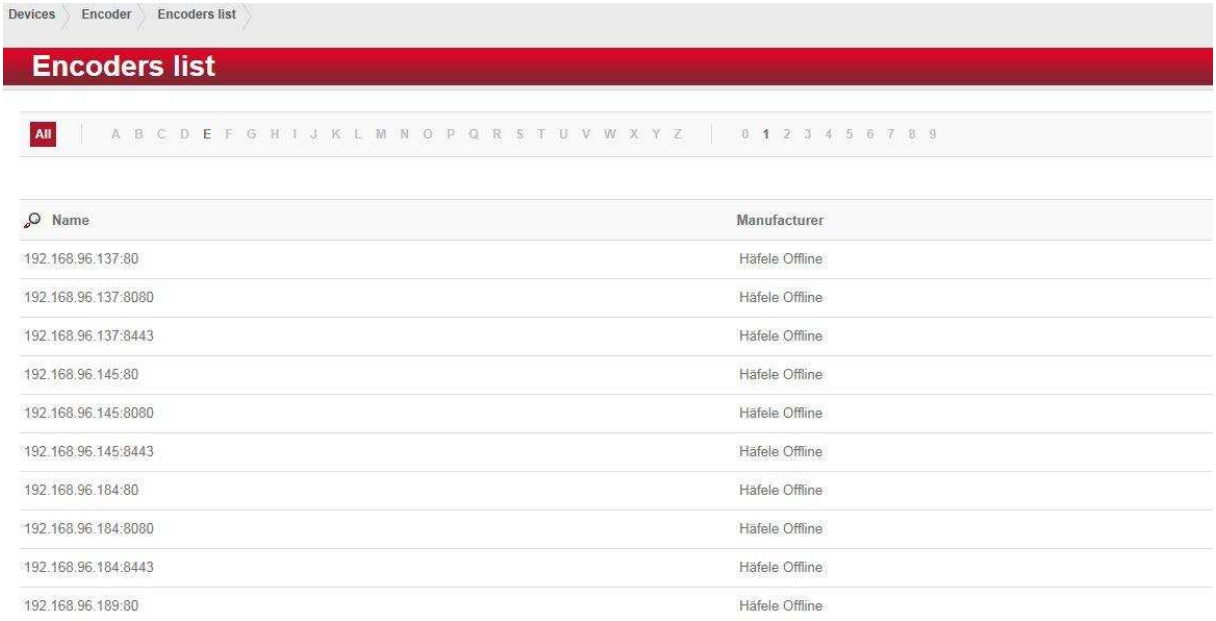


Events at offline terminals can be read out with the MDU using the "**Terminal>Logs**" menu and imported into the software using menu item "**Organisation>Area>Edit area**" and action "**Log import**".

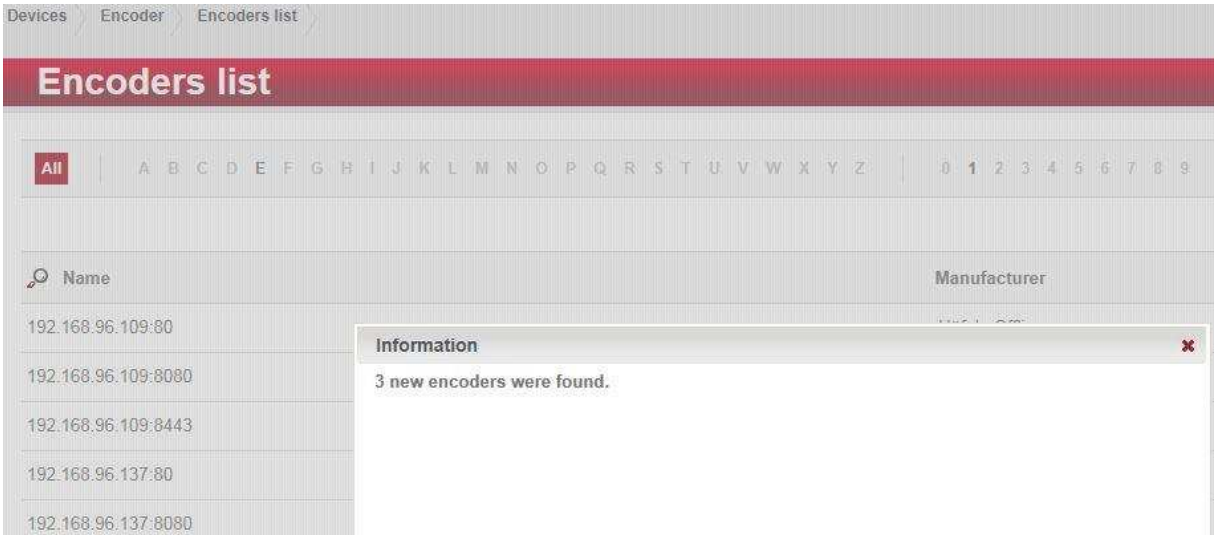


7. Dialock coding device (Encoder ES 110)

The **Devices > Coding device** menu takes you to the coding devices. To create a new coding device, click on “**Create**” on the left-hand side of the screen. Then select the associated manufacturer.



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



Give the coding device a unique **Name** in order to be able to clearly identify it later.
If the coding device operates with an encrypted connection, activate the check box for “**Secure connection**”.
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 “**COM-Port**” address is needed for the web service call. This is where you enter the COM port address of the destination PC to which the coding device is linked. This can be found in the Windows device manager.

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

7.1. Dialock MDU 110

The **Devices > MDU** menu takes you to the MDU. In order to create a new MDU 110 in the system, connect the MDU to the system using USB. If all drivers have been correctly installed, a drive with the designation “MDU” should now be available on the PC.
Now click on “**Register MDU**” on the left-hand side of the screen.

All registered MDUs will be displayed in the **DG2 MDU List**.

The transmission of data to/from the MDU takes place for the terminals of an offline area in the respective area of the **Organisation > Areas** menu.

8. Device settings

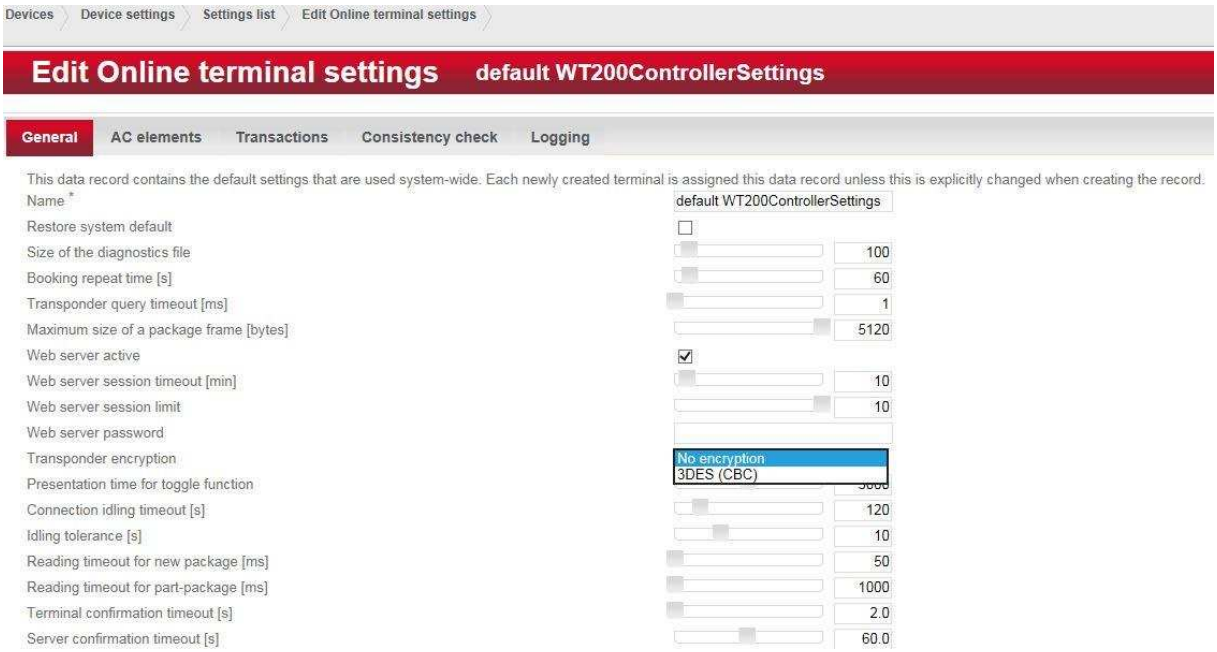
8.1. General settings for online terminals

(this area requires expert knowledge)

By selecting a terminal using **Devices > Device settings**, you are taken to the relevant settings level.

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.



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.

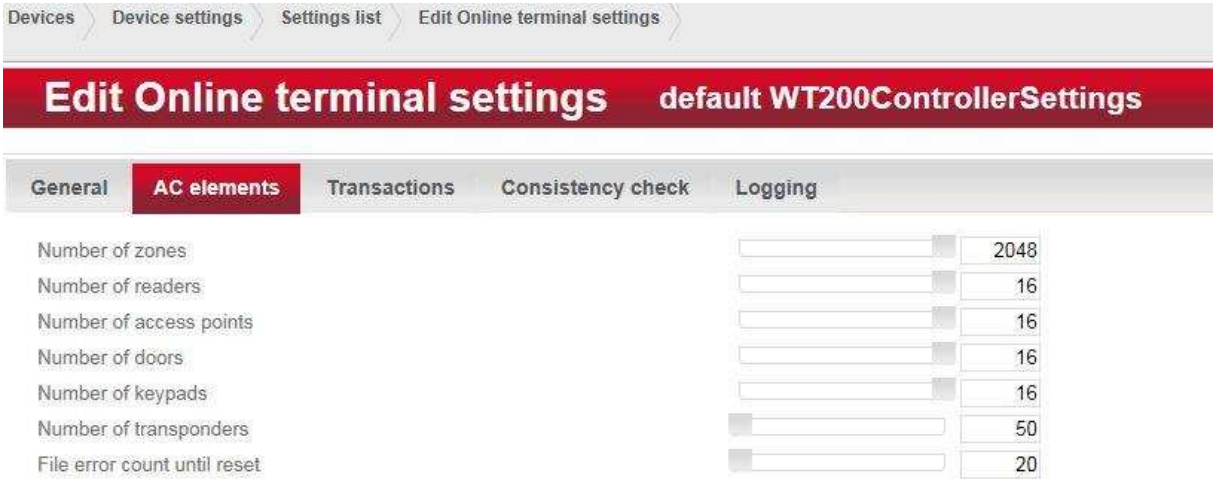
Transponder encryption:
This specifies the type of authentication. 3DES encryption is only possible in combination with the TIKS card. (Telekom Internal Key Service, future option).

Presentation time for toggle function
This value determines the time for which an ID 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.

8.2. Access control elements of the online terminal settings

(this area requires expert knowledge)

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.



8.3. Transactions in the online terminal

(this area requires expert knowledge)

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.

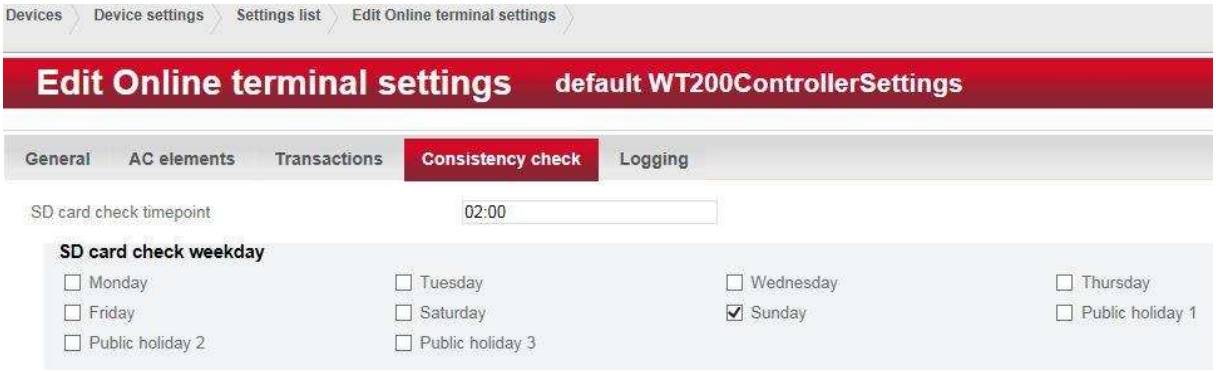
Number of prioritised transactions:
Prioritised transactions are transactions that must be sent before any others. Prioritised transactions are, for example, global anti-passback transactions, timed anti-passback transactions and system error messages.
The prioritised transactions are saved in a separate 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.

8.4. Online terminal consistency check

(this area requires expert knowledge)



Time/weekday SD card check:
The days and times when the terminal (WT200) 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.

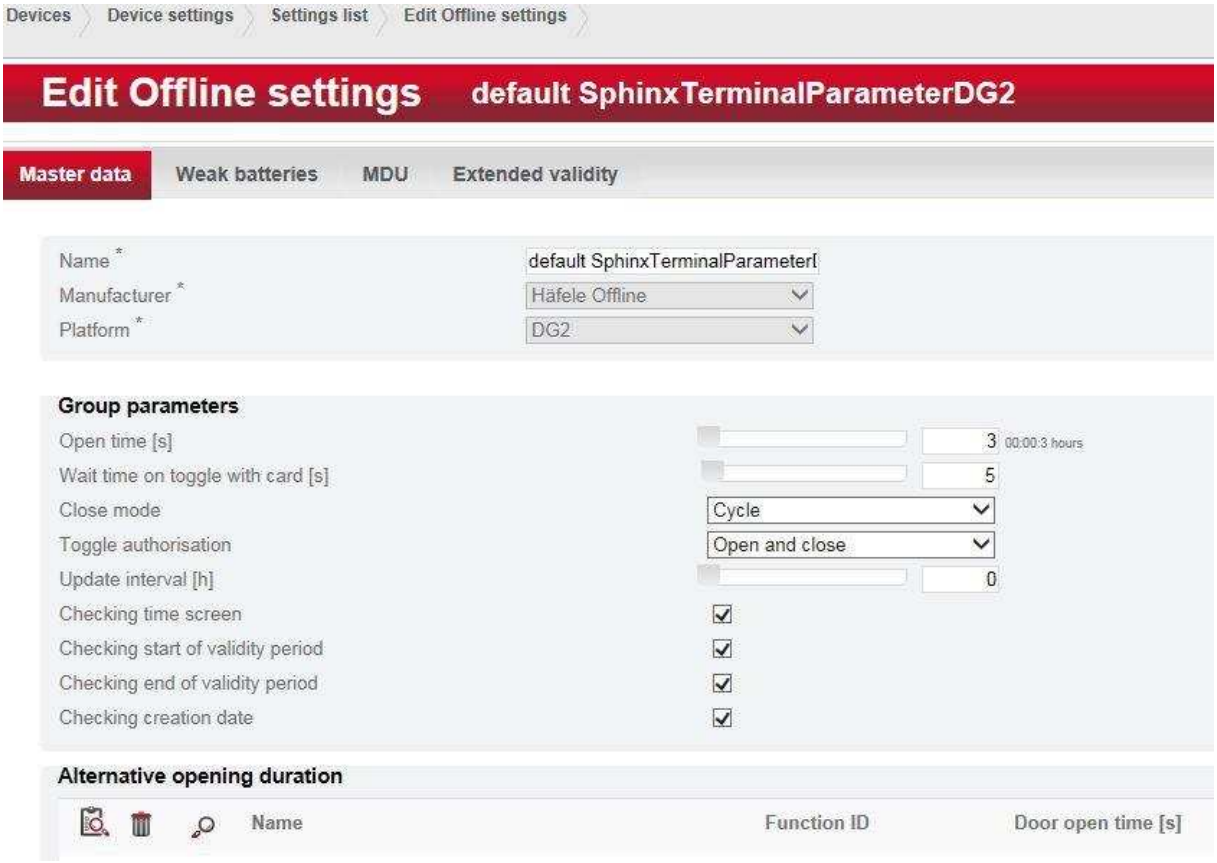
Attention:
During the consistency check of the SD card the terminal cannot perform any access checking. This check can take several seconds to several minutes. If an error is found, the terminal tries to rectify it automatically. If this is not possible, the SD card may be formatted. In this case, all 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.

8.5. General settings for offline terminals

Clicking on the pencil icon next to parameter “**Settings**” on the “**Edit terminal Sphinx**” 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 ID.

Wait time on toggle with card
This value determines the time for which an ID 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 cards.

Toggle authorisation
Unlocking and locking, unlocking only or without authorisation 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 ID 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 ID is checked.

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

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 ID is checked. This time can be specified in steps of one minute (up to max. 2032) for the ID.

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

9. 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.

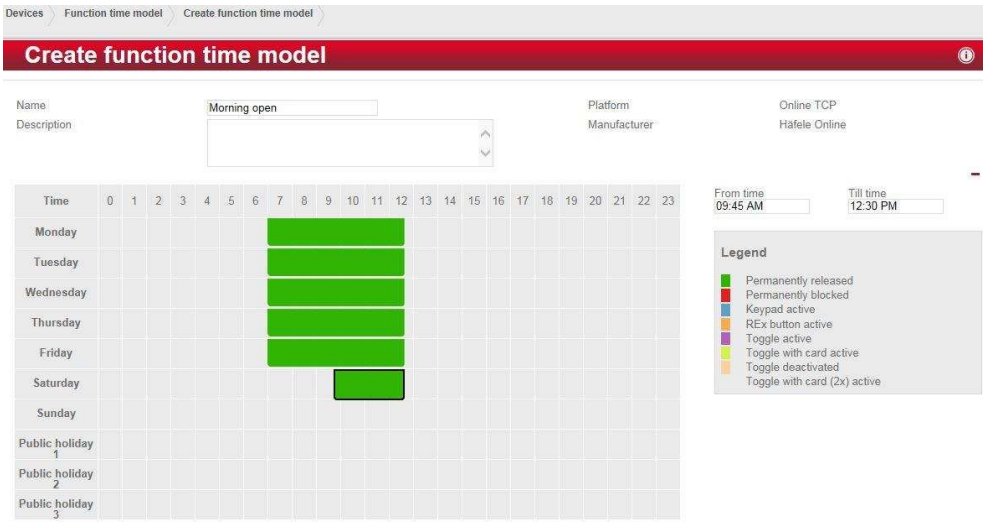
You can load a new firmware version into the required devices using the “Update devices” function.

10. Function time models

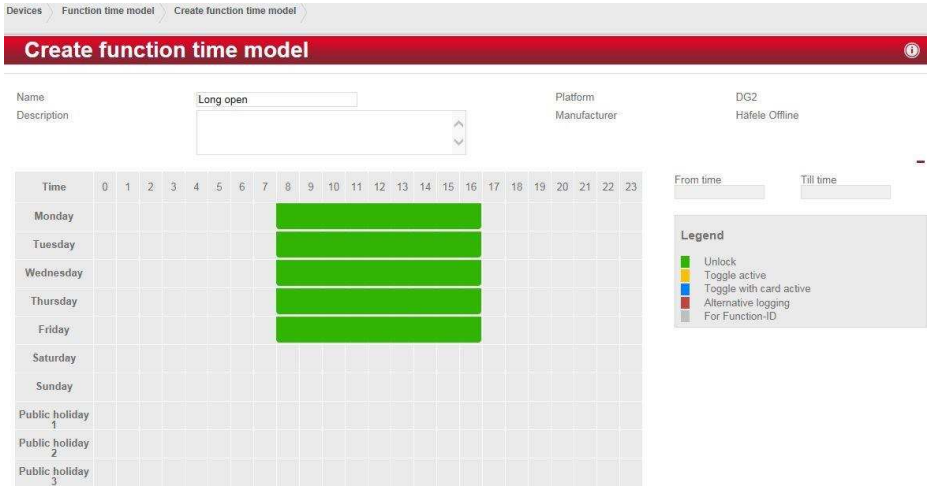
You can create and edit the device-related time models in the **Devices**/**Function time model** menu. With function time models, a terminal automatically switches over to statuses such as unrestricted for a door/barrier at the specified point in time. This means that the terminal automatically switches 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, see Chapter 4.4. The recording and editing of offline function time models also work in the same way as they do for the offline time models, see Chapter 4.4.2.

Online
Function time model



Offline
Function time model

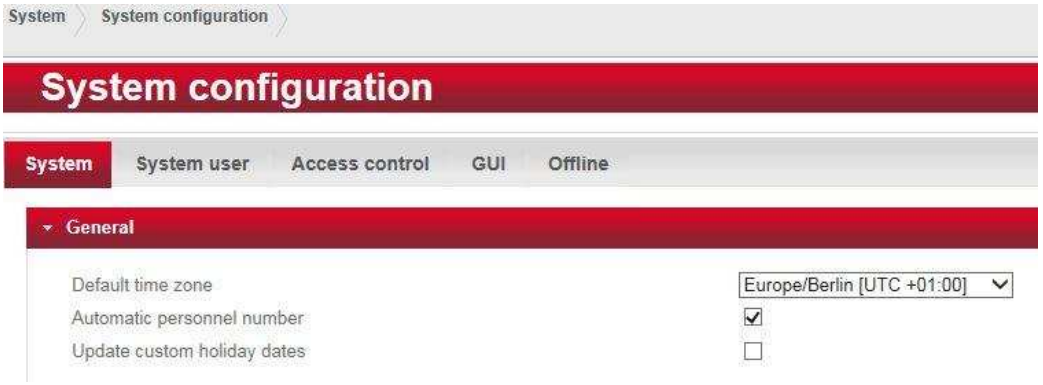


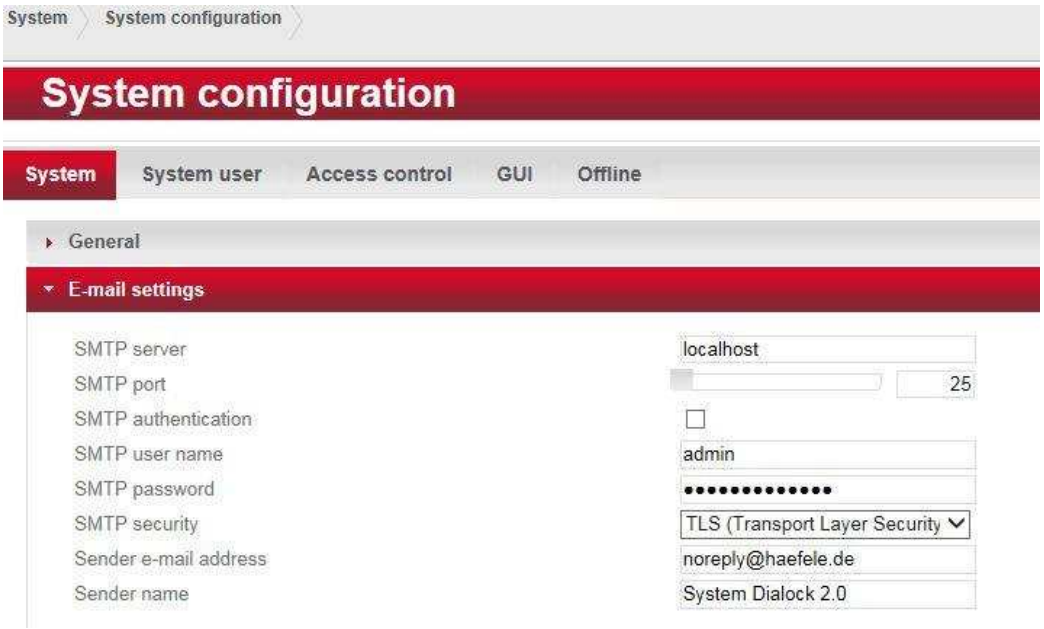
11. System configuration

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

11.1. Configuration of the 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.



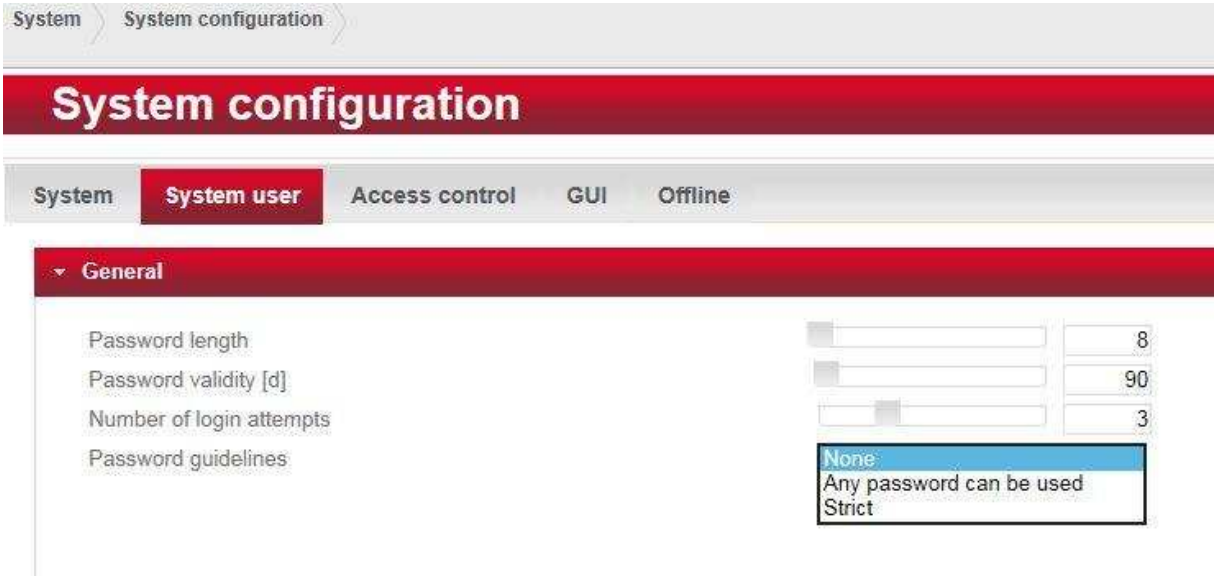


Enter the e-mail send parameter to be used by the system here.

11.2. 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.

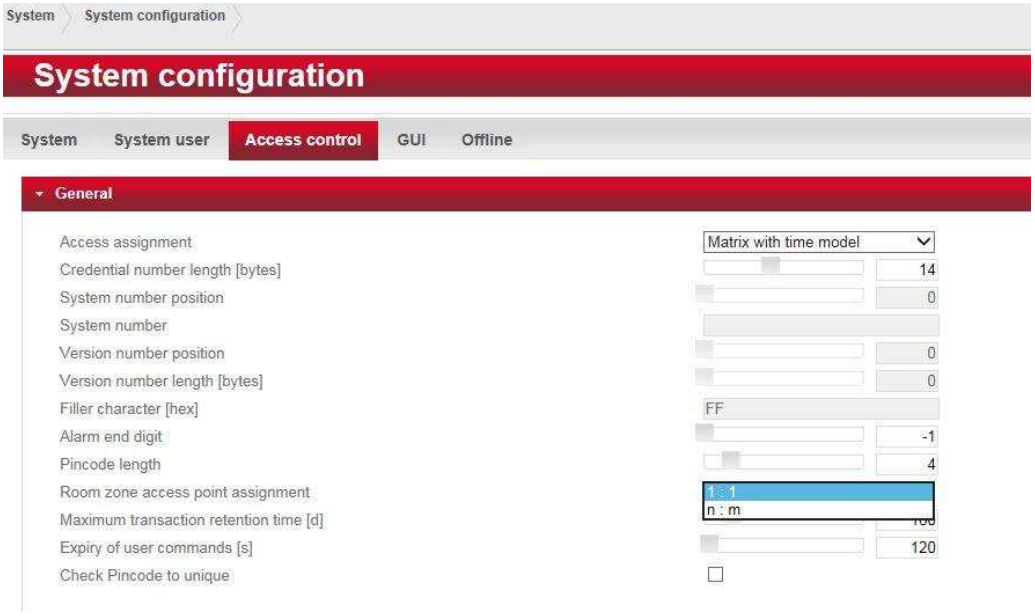
Under password guideline you define how a user has to create his/her password.
None: The user can enter a password with any format.
Any password can be used: The password must be alphanumeric.
Strict: The password must contain alphanumeric characters, special characters and upper and lower case.



11.3. System configuration: Access control

Basic parameters for access control can be defined in the “**Access control**” tab of the **System/System configuration** menu.
The possibility of allocating authorisations is set under access allocation. Changes are only possible within the scope of the licence and should only be made by trained personnel.

Note:
Dialock is not downwards-compatible. If the **Role-based** or **n to m** function has been selected for access allocation, it cannot be undone.



The global length of the passes in bytes in the system is defined under **Credential number length**.
The position of a fixed system number in the ID 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 ID is set under **Version number position**.
Under **Filler character** you define a character with which IDs that are too short will be filled.
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.

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.

11.4. System configuration: GUI

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

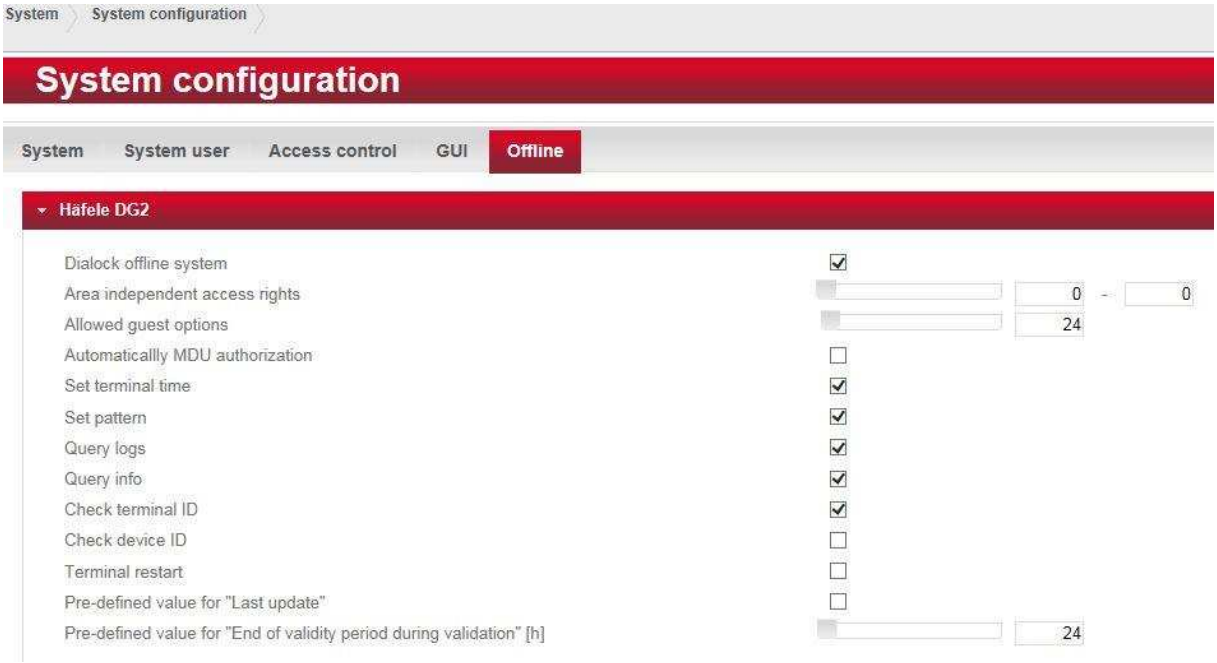
Here you can **Change the logo** and determine the duration for which **Info and error dialogues** are displayed. Select the required **GUI animation** in the drop-down menu and determine the time after which a user is logged out by the system in **Session time-out**.

11.5. System configuration: Offline

In the **Offline** tab of the **System/System configuration** menu, on the **Häfele DG II** screen you can set parameters of the **Offline system**.

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

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



12. Licence administration

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

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

13. Transponder

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

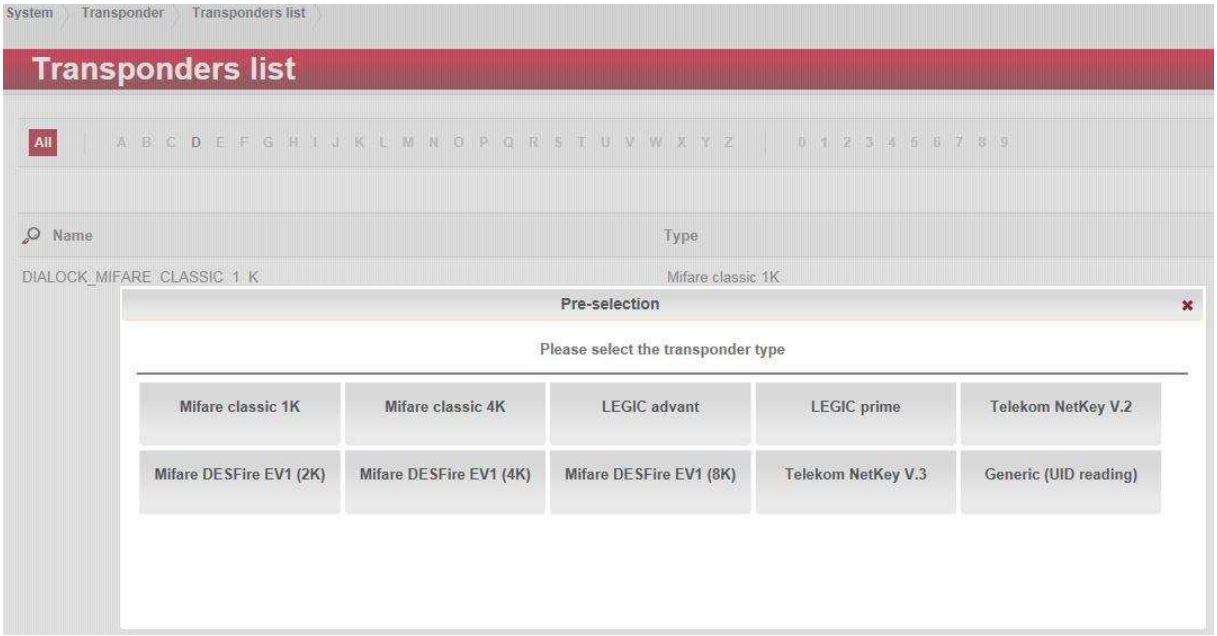
Changes are only possible within the scope of the licence and should only be made by trained personnel.

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

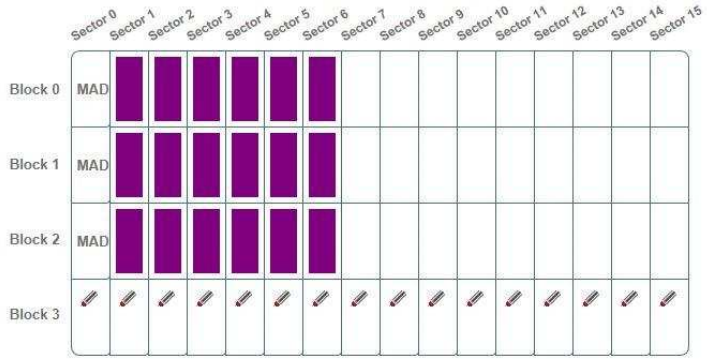
13.1. Organise transponder

(this area requires expert knowledge)

Select the required **Technology** here and the associated **Chip type** and assign a name to this transponder.



In the **System/Transponder** menu you can **Create a new segment** by making the relevant selection on the left-hand side of the screen.



You can edit the **Segment name**.
Activate the "**Read protection**" option if the entire area of this segment is to be read-protected.

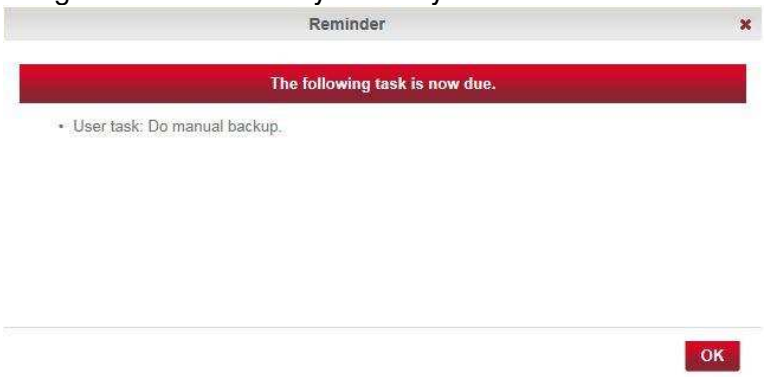
Note:
The write/read condition must be ≥ 1.

Under "**Write protection**" you define the length of the write-protected area.
With "**Organisation level**" you define the size thereof and therefore the length of the stamp.

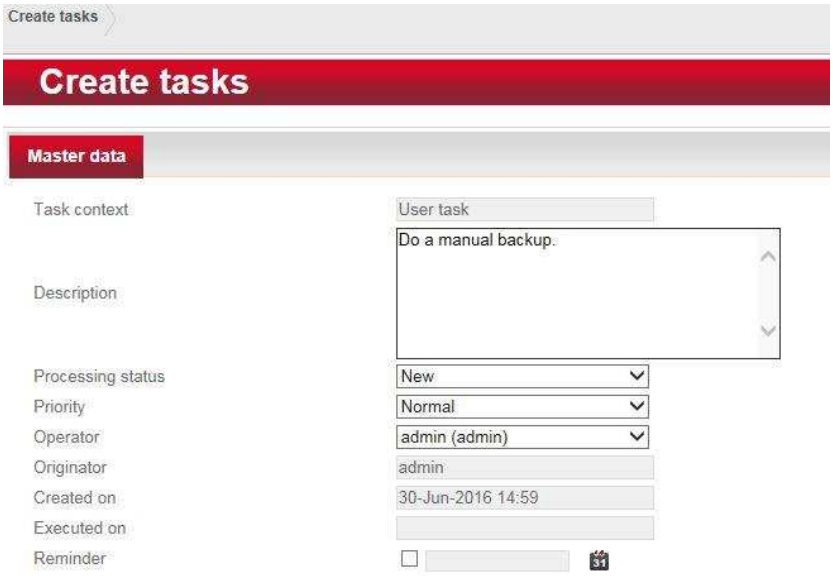
14. Working with Dialock

14.1. Tasks

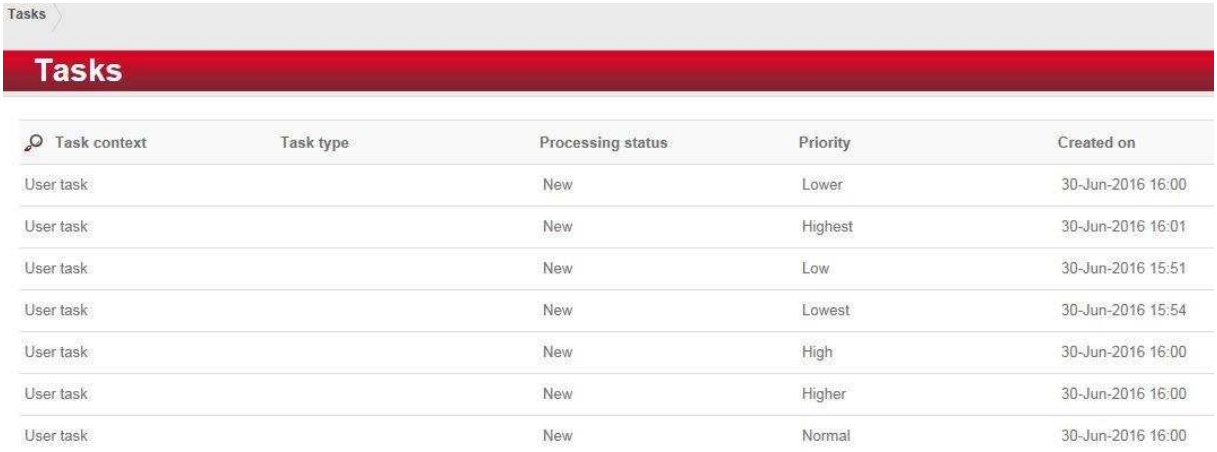
As soon as data that concerns peripheral devices, for example, is modified in Dialock (e.g. time periods that are saved in Offline devices), Dialock automatically creates a task for the relevant user. The changes are usually made using a programming unit or programming cards which are connected at the 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 “**Tasks**” you can also create these manually for yourself and other users.



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

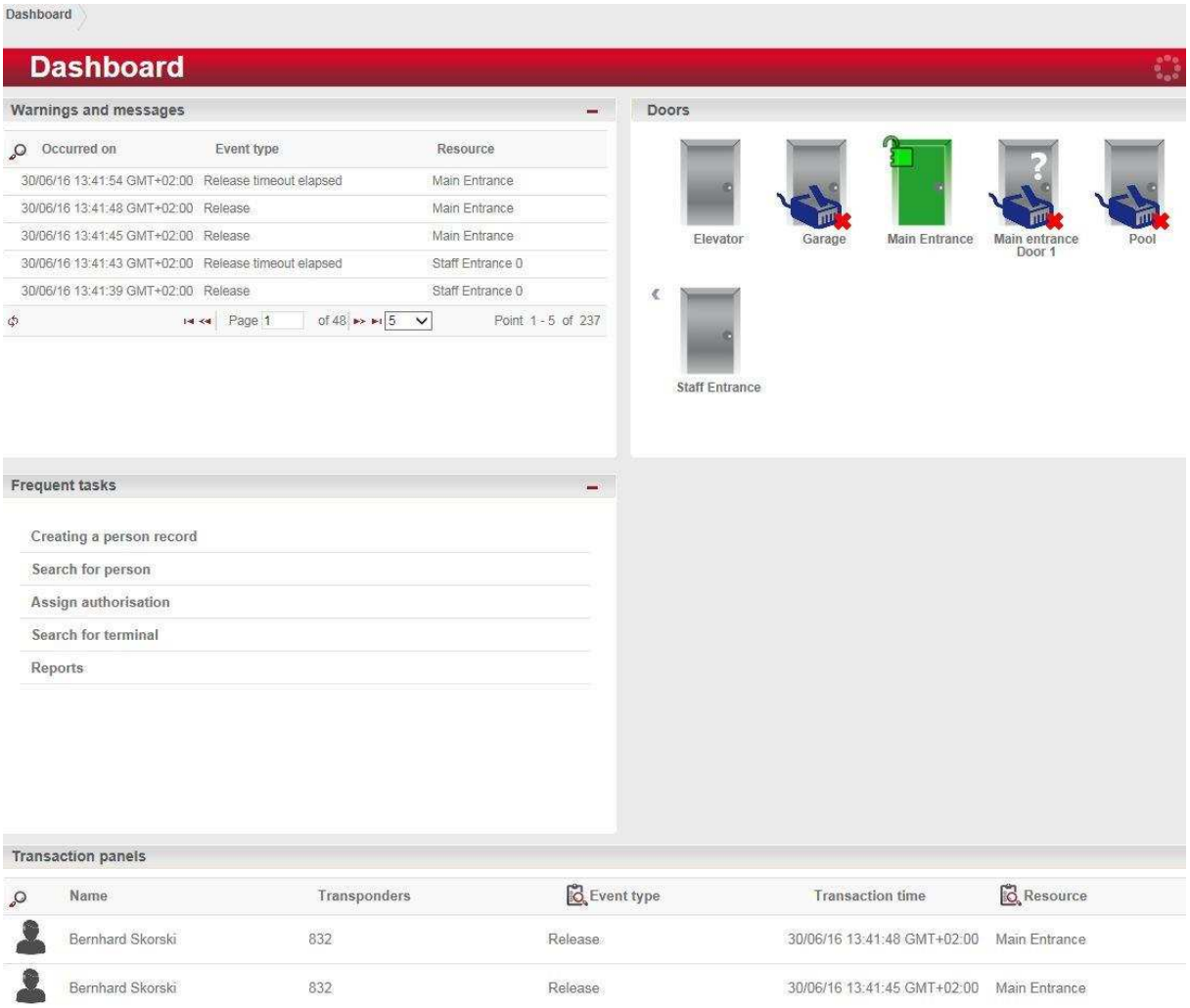
SD card: an SD card has been replaced at the controller and has to be checked prior to activation

Offline hardware: the parameters of the offline system must be modified here

15. The module

15.1. 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.

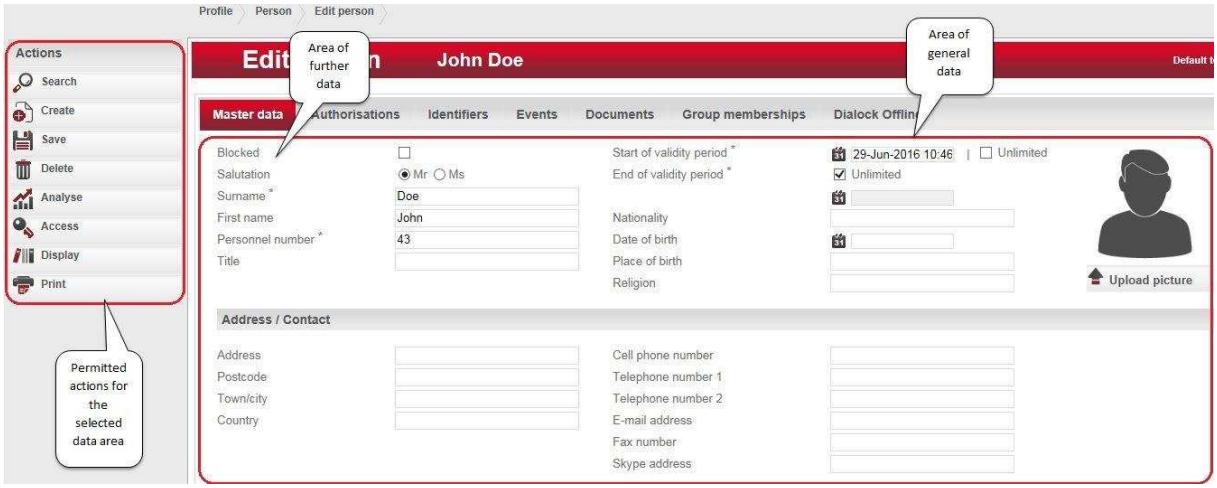
15.2. Profiles

Looking after the personnel data is an important part of the software. This takes place in the **PERSONS** module.

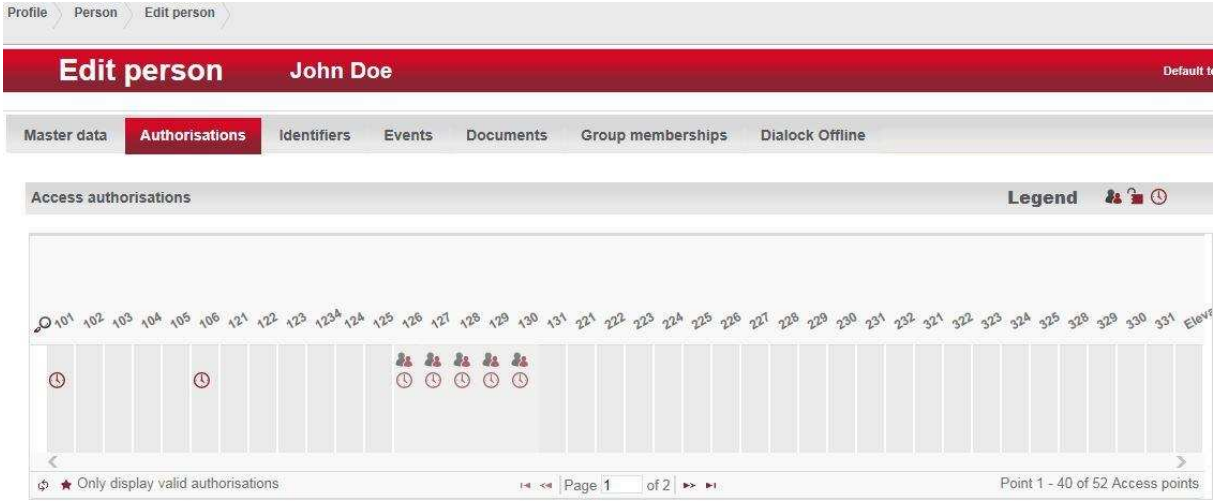
15.2.1. PERSONS

15.2.1.1. Master data

This is where you assign at least the must-enter fields of surname, personnel number and the start of validity (of the master record) to the employee.

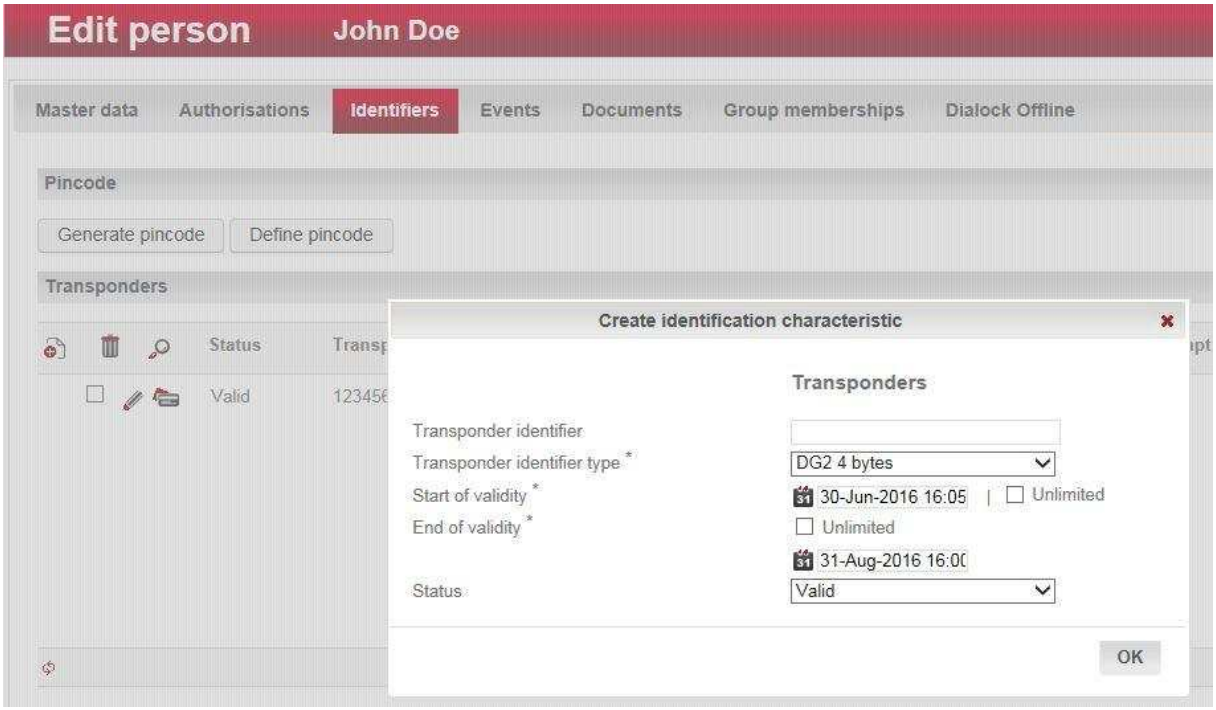


15.2.1.2. Authorisations



This is where the authorisations of the selected person are displayed and can be edited.

15.2.1.3. Identification characteristic

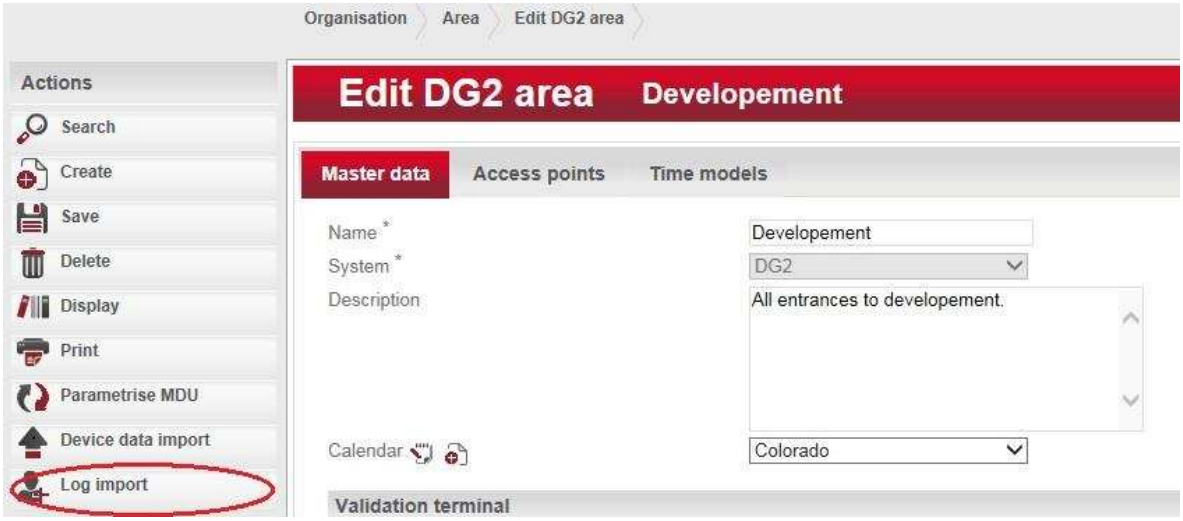


In the **Identification characteristic** form, at least one means of identification via which access can be controlled (such as a transponder) must be assigned.

15.2.1.4. Events

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

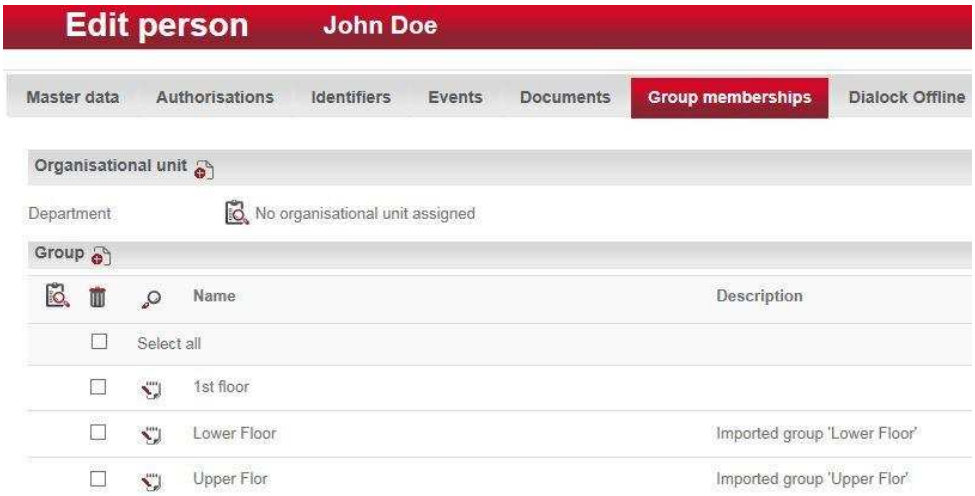
Events at offline terminals must be read out beforehand with the MDU “Terminal>Logs” menu and imported into the software using menu item “Organisation>Area>Edit area” and action “Log import”.



15.2.1.5. Documents

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

15.2.2. Group memberships



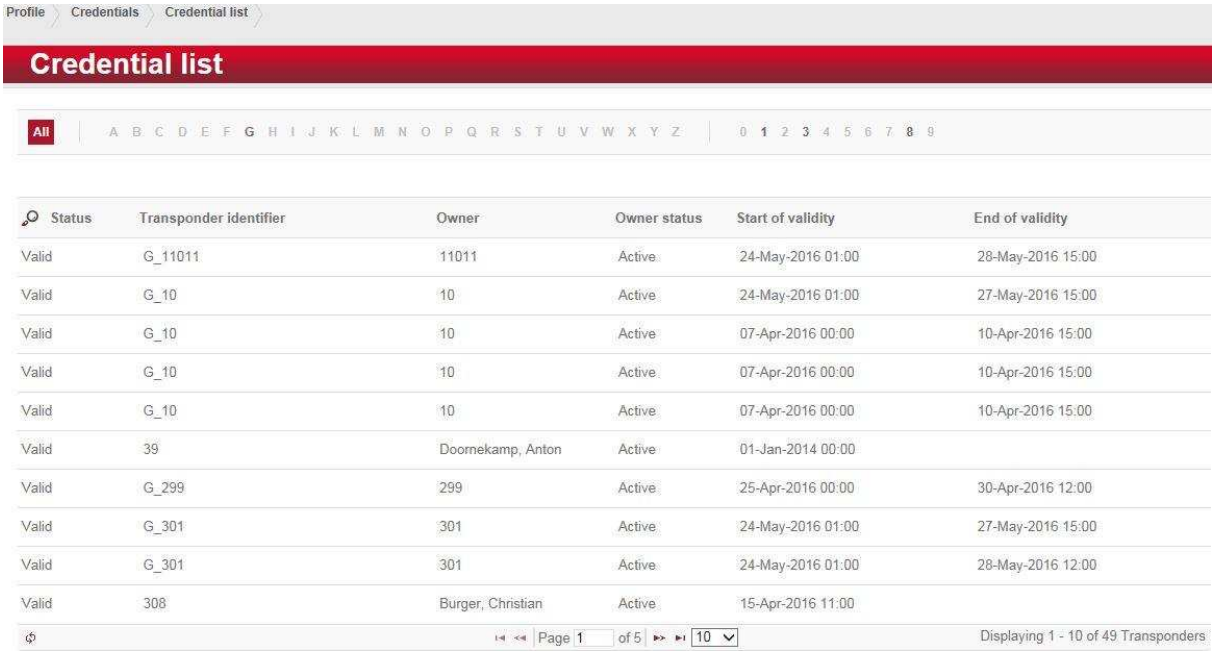
The group memberships of the selected person are displayed in this module.

15.2.3. Dialock Offline

A list of the offline authorisations of the selected person is displayed in the **Dialock Offline** module.

15.3. Transponder

15.3.1. Transponder list

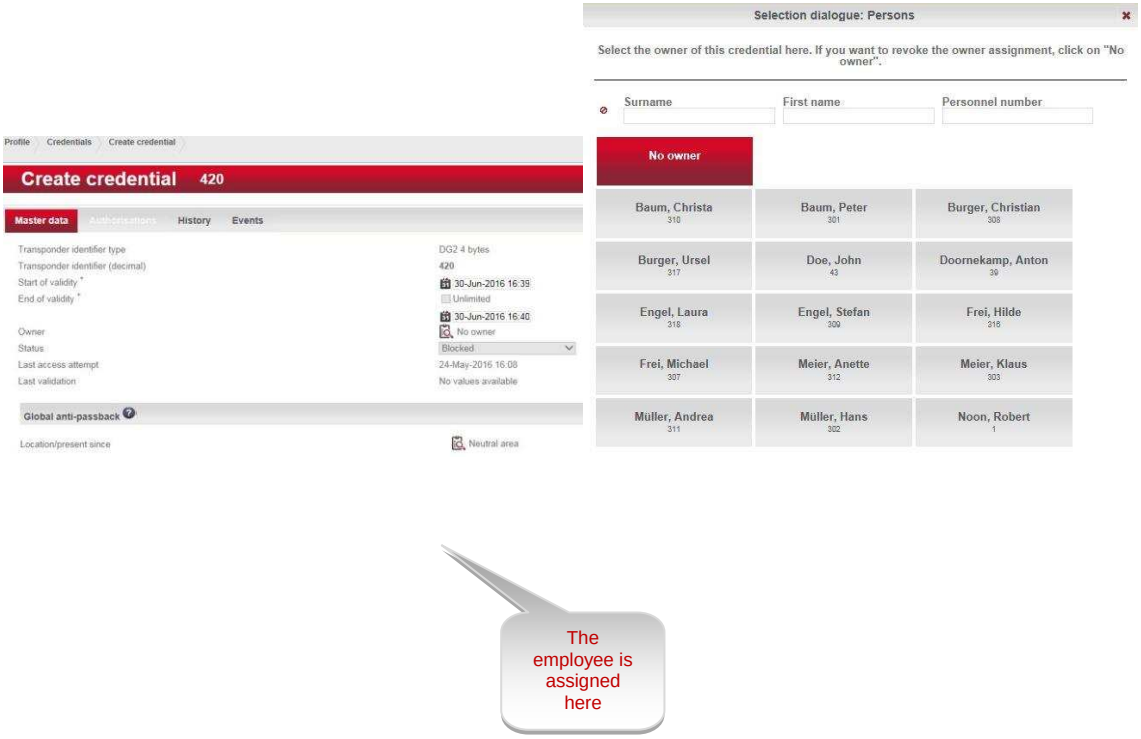


The list of transponders in the system is called up by selecting Profile/Transponder.

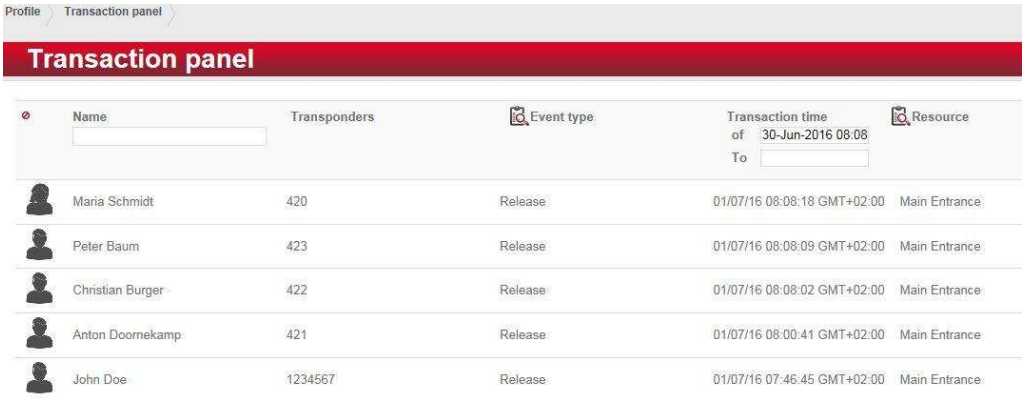
If you double-click on a transponder identifier, the relevant transponder is displayed and can be edited. The authorisations, the editing history and registered events can be displayed.

15.3.2. Edit / register transponder

In the “Transponder” sub-menu item the transponder is registered (manually or via a USB reader), searched for or assigned to an employee. The history can also be retrieved for any pass using the “History” tab of the same name (who had the transponder ID and when).



15.4. 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 with 

in the left-hand.

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

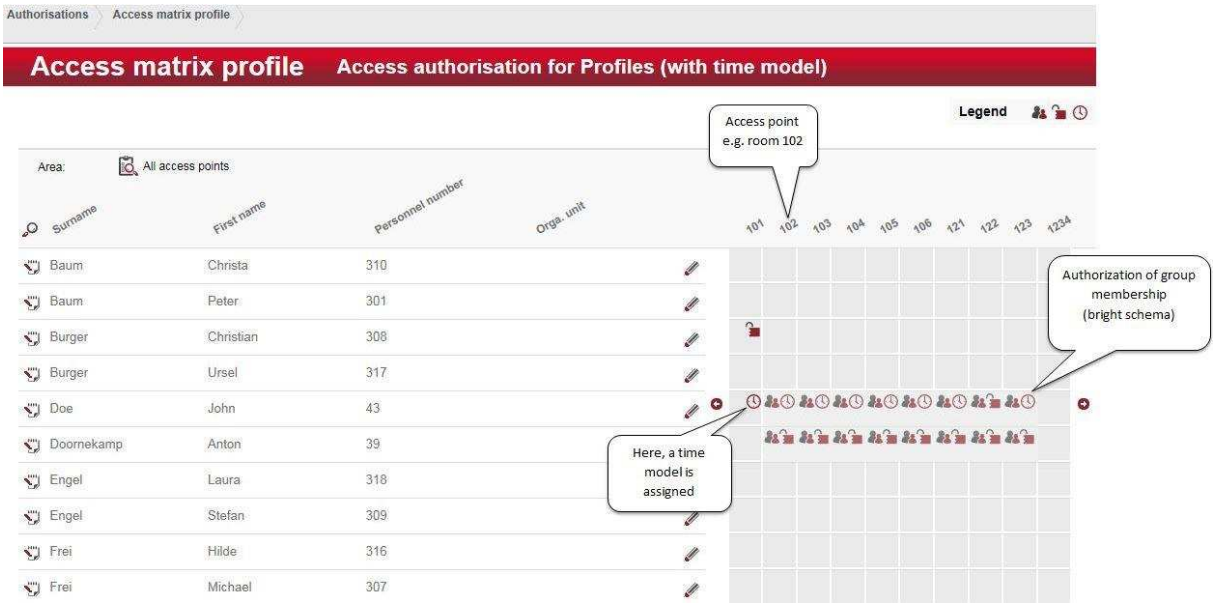
15.5. Authorisations

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

15.5.1. The access matrix

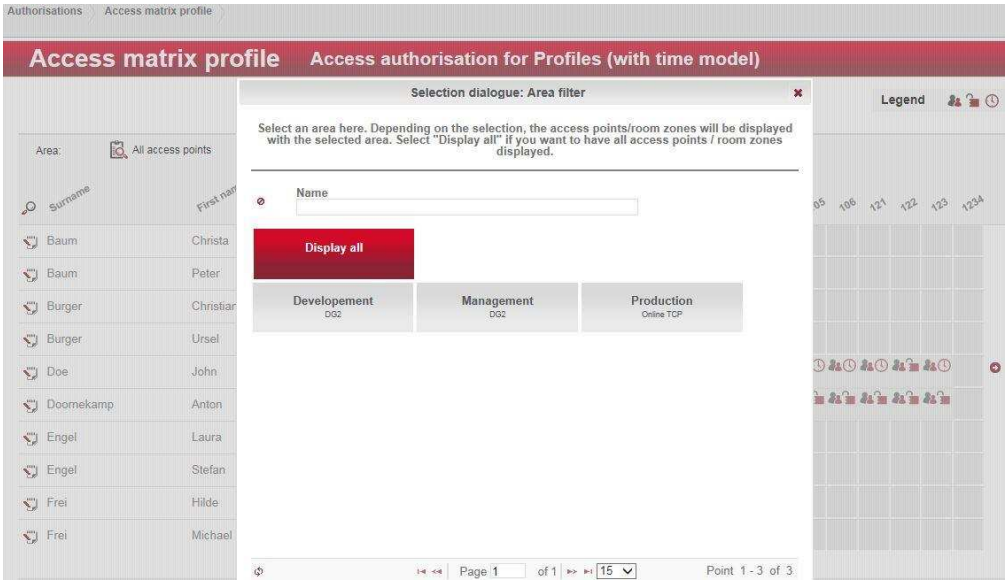
Via the **Authorisations/Access matrix profiles** and **Authorisations/Access matrix groups** menu, you are taken to the access matrix, which is both person-related and group-related. A person can be authorised individually as well as via groups or organisational units.

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 (see Chapter 4.3.3 “Matrix configuration”), 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**.

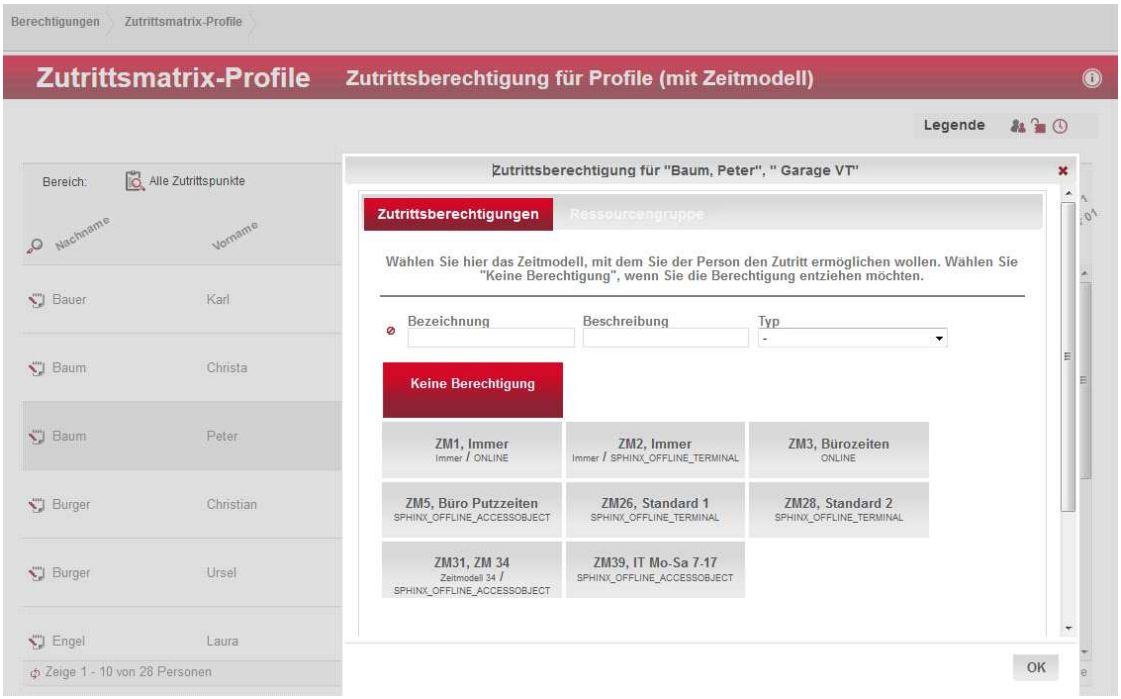
Select the desired **Areas** via the symbol . Now only the authorisations of the selected area are displayed in the matrix.



15.5.2. 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 (see chapter 0).
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 "No authorisation" on the selection screen.



15.5.3. 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. With online terminals, select the associated time model in the additional menu that opens.

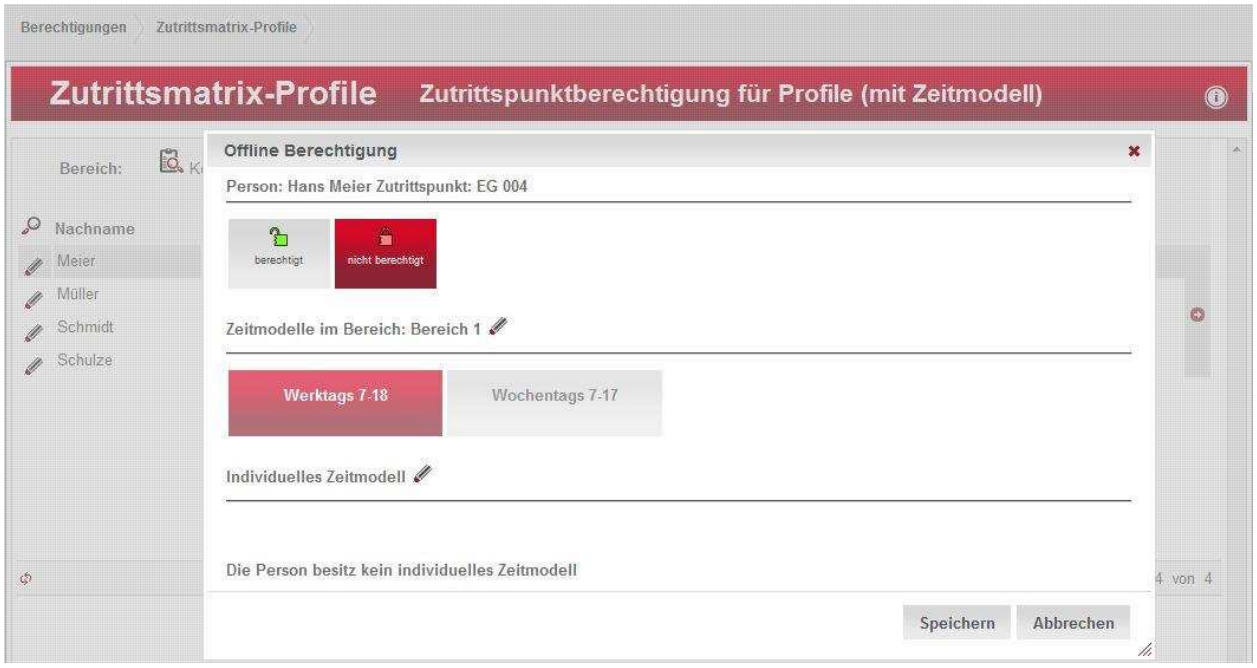
15.5.4. Allocation of authorisations in the access matrix for an offline access point

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. Select “**Authorised**” and save your selection.

In order to delete a person from offline access authorisation, proceed as above by clicking on “**No authorisation**” in the selection screen. Save your selection.

Furthermore, you have the option of setting a time limit for access authorisations by selecting one or more **Offline area time models**. Select the required time model(s) here. Save your selection.

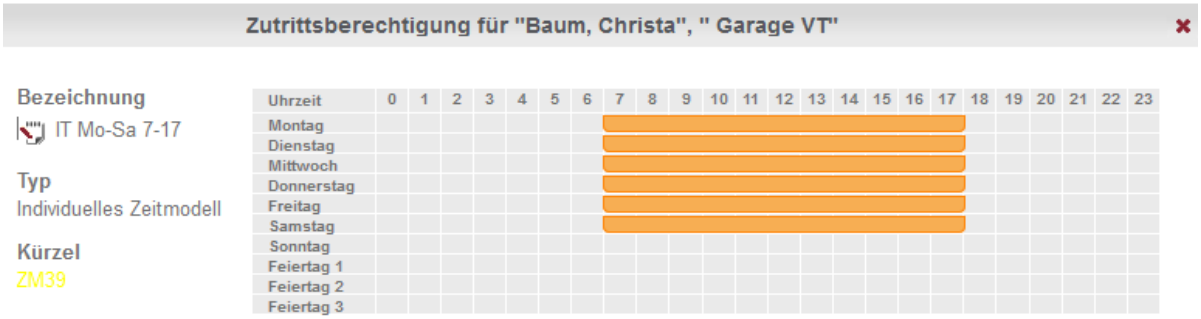
Note:
This change has an effect on the authorisation on all offline components that are assigned to the same area.



15.5.5. 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”.

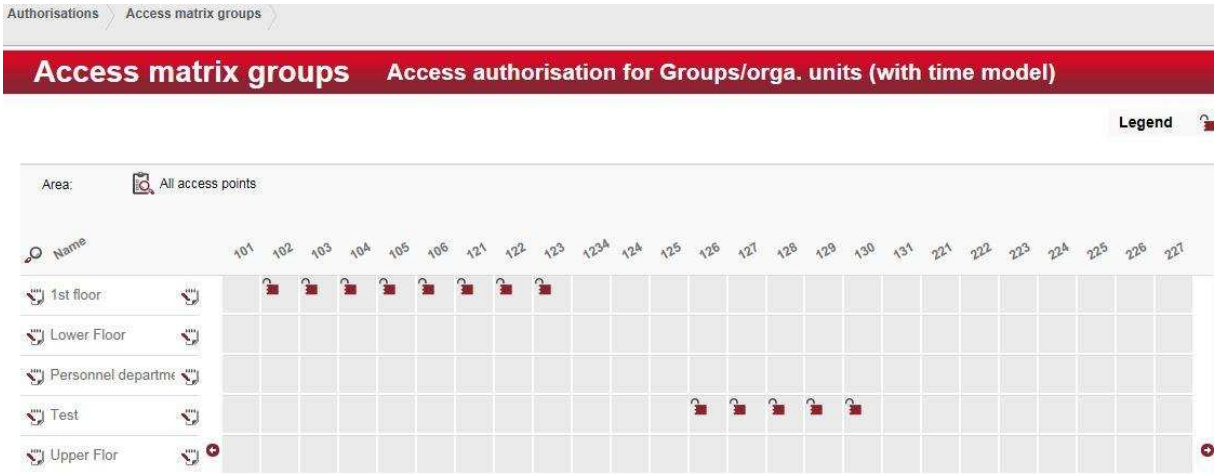


The time model can be edited directly from the matrix by clicking on the Edit symbol.

15.6. 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”

15.7. Organisation

The group is edited in main menu item “Organisation”. In order to edit a group, it must first be selected by double clicking.

15.7.1. Group / organisational unit

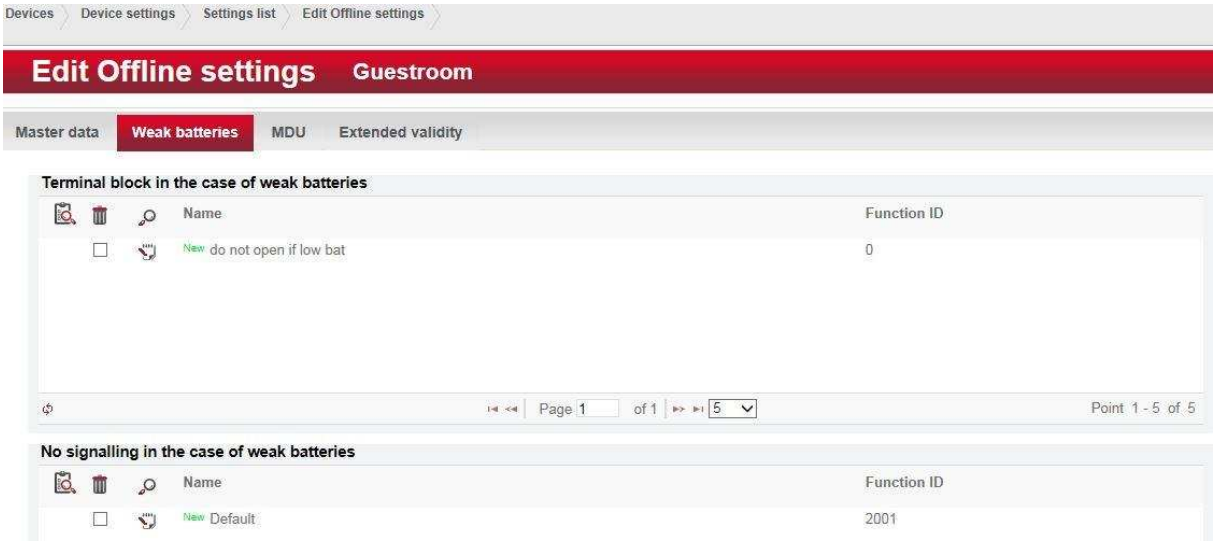
Employees or access points can be combined into groups. These groups can be used to simplify the issuing of access authorisations. Authorisations can also be issued to groups. Individual authorisations can also be issued to the employees. Both authorisations are complementary.

The employee is assigned here

15.8. Offline function ID

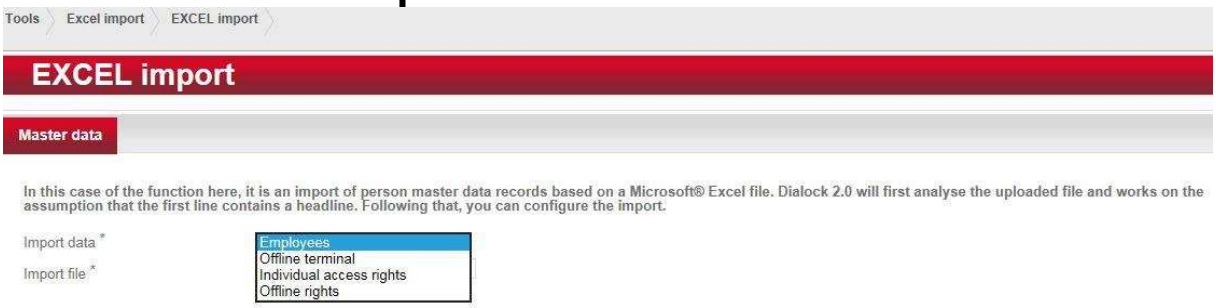
This identifier is a number between 0 and 2000. Then certain functions at offline terminals are assigned to the function identifier such as the suppression of certain signalling or “Do not open if low bat” as the highest signalling to the hotel employees. Then the ID can be assigned to a person. A person can only have one offline function ID assigned to them, but a particular function ID can be assigned to any number of people.

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.



15.9. Tools

15.9.1. 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.

Personal No	Name	Given Name	Gender	valid from	valid until	Groups	Remark
301	Baum	Peter	Herr	1.1.14 0:00		Lower Floor, Upper Flor	frühester Startzeitpunkt (1.1.2014) Uhrsetzen mit MDU
302	Müller	Hans	Herr	20.4.14 0:00	31.12.16 23:59	Lower Floor, Upper Flor	
303	Meier	Klaus	Herr	21.4.14 0:00	31.12.16 23:59	Lower Floor, Upper Flor	
304	Schulze	Albert	Herr	22.4.14 0:00		Lower Floor, Upper Flor	
305	Schmidt	Heinrich	Herr	23.4.14 0:00		Lower Floor, Upper Flor	
306	Schneider	Erwin	Herr	24.4.14 0:00		Lower Floor, Upper Flor	
307	Frei	Michael	Herr	25.4.14 0:00		Lower Floor, Upper Flor	
308	Burger	Christian	Herr	26.4.14 0:00		Lower Floor, Upper Flor	
309	Engel	Stefan	Herr	27.4.14 0:00		Lower Floor, Upper Flor	
310	Baum	Christa	Frau	28.4.14 0:00		Lower Floor, Upper Flor	
311	Müller	Andrea	Frau	28.4.14 0:00		Lower Floor, Upper Flor	
312	Meier	Anette	Frau			Lower Floor, Upper Flor	
313	Schulze	Lisa	Frau			Lower Floor, Upper Flor	
314	Schmidt	Maria	Frau			Lower Floor, Upper Flor	
315	Schneider	Gudrun	Frau			Lower Floor, Upper Flor	
316	Frei	Hilde	Frau			Lower Floor, Upper Flor	
317	Burger	Ursel	Frau			Lower Floor, Upper Flor	
318	Engel	Laura	Frau			Lower Floor, Upper Flor	

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	Terminal type - Only for Dialock Integra Dialock 2: Is automatically assigned for standard template	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)
22	1	1st FL		225		Guestroom			225	
23	1	1st FL		226		Guestroom			226	
24	1	1st FL		227		Guestroom			227	
25	1	1st FL		228		Guestroom			228	
26	1	1st FL		229		Guestroom			229	
27	1	1st FL		230		Guestroom			230	
28	1	1st FL		231		Guestroom			231	
29	1	1st FL		232		Guestroom			232	
30	1	2nd FL		321		Guestroom			321	
31	1	2nd FL		322		Guestroom			322	
32	1	2nd FL		323		Guestroom			323	
33	1	2nd FL		324		Guestroom			324	
34	1	2nd FL		325		Guestroom			325	
35	1	2nd FL		328		Guestroom			328	
36	1	2nd FL		329		Guestroom			329	
37	1	2nd FL		330		Guestroom			330	
38	1	2nd FL		331		Guestroom			331	
39	1	LF		Storage		Staff				
40	1	GF		Office		Staff				
41	1	GF		Wellness		General				

Example of an offline terminal list

Import Offline Rights							
Row No. (is not imported)	Area	Personal No. (Only alreads 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						
11	1						
12	1						

Script

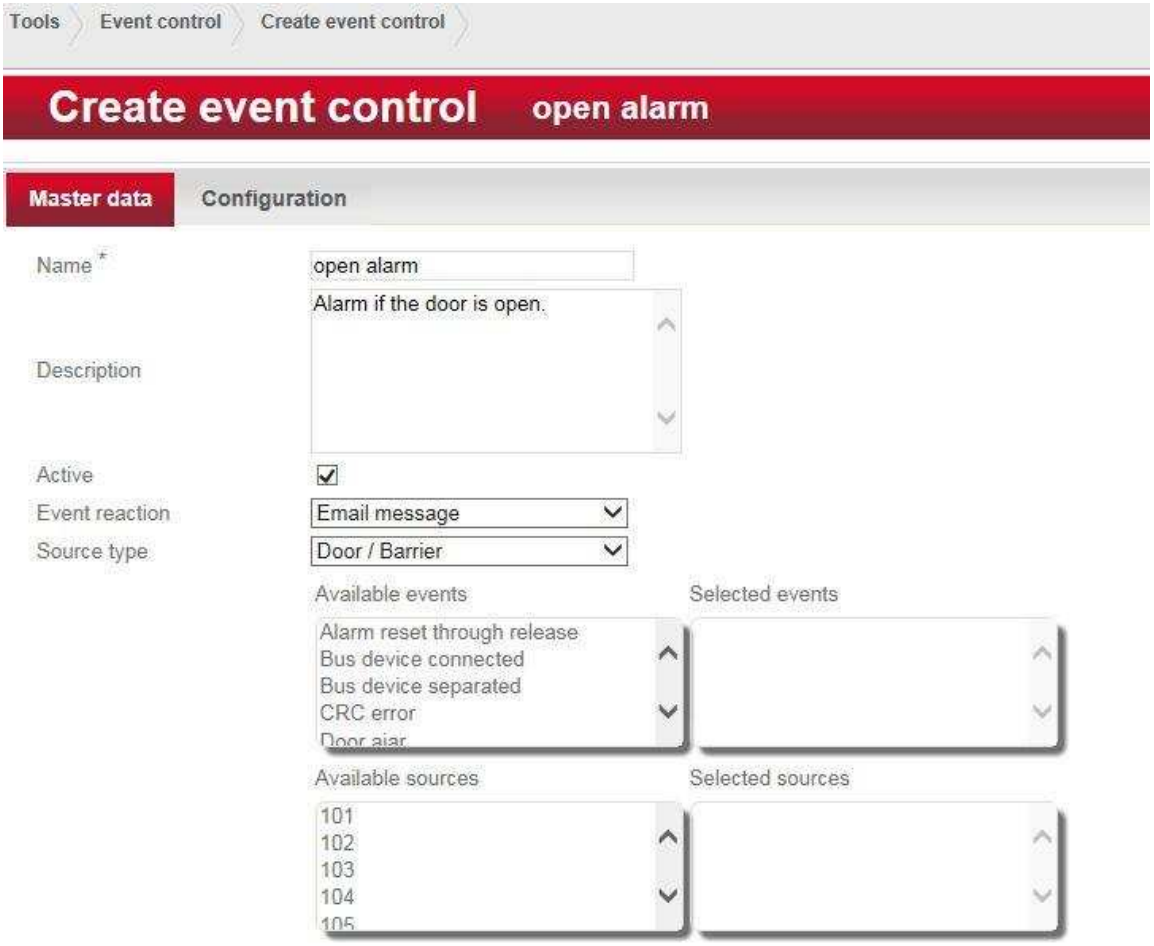
Example of a list with offline authorisations.

Lists must be always created using these specified formats so that are read in correctly.

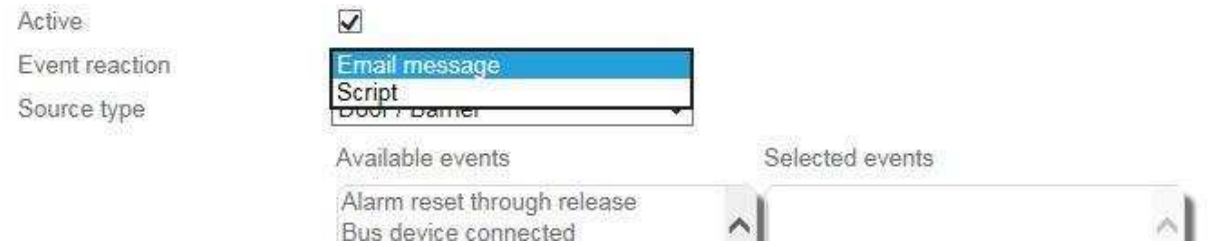
15.9.2. Event control

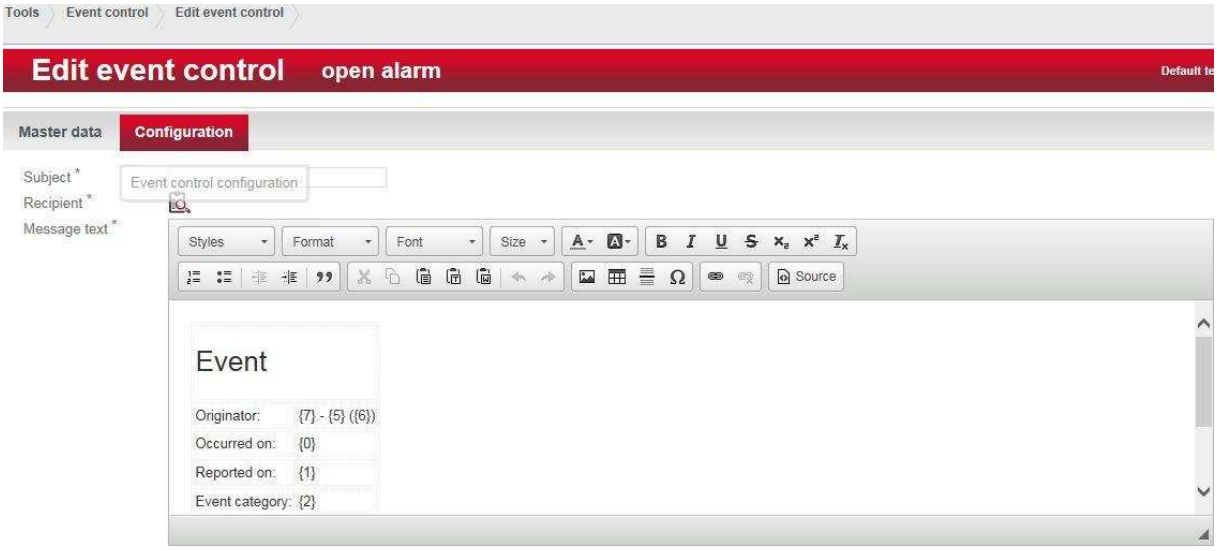
With the aid of event control it can be defined that the system sends a predefined e-mail to a selected user or generates a so-called script if a certain event or combination of events occurs.

List of saved event controls



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**.
In order to determine the events for which an e-mail is generated or a script should react (bottom selection menu), drag the required events from "**Available events**" to the "**Selected events**" field using the mouse pointer. Multiple choice is possible.

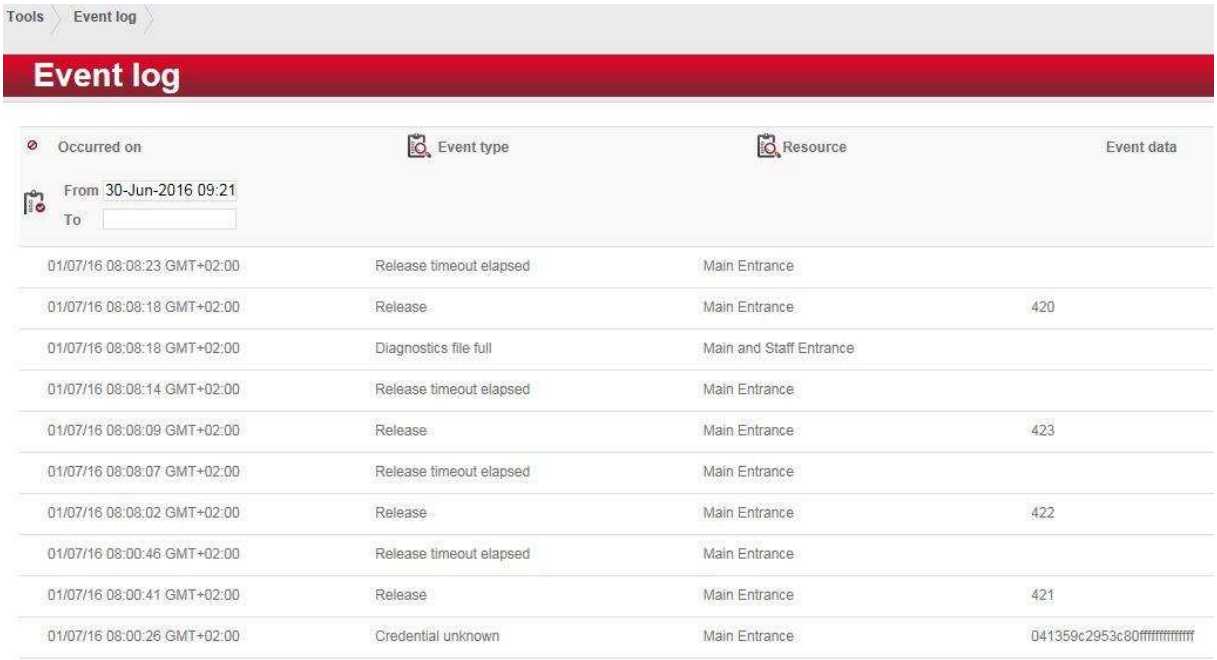




Then make a selection in the "**Configuration**" tab to configure the e-mail function or select the script that should be used for this event control. To do this, drag the required script from the list "**Available scripts**" to the list "**Selected scripts**". Save your information.

15.9.3. 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

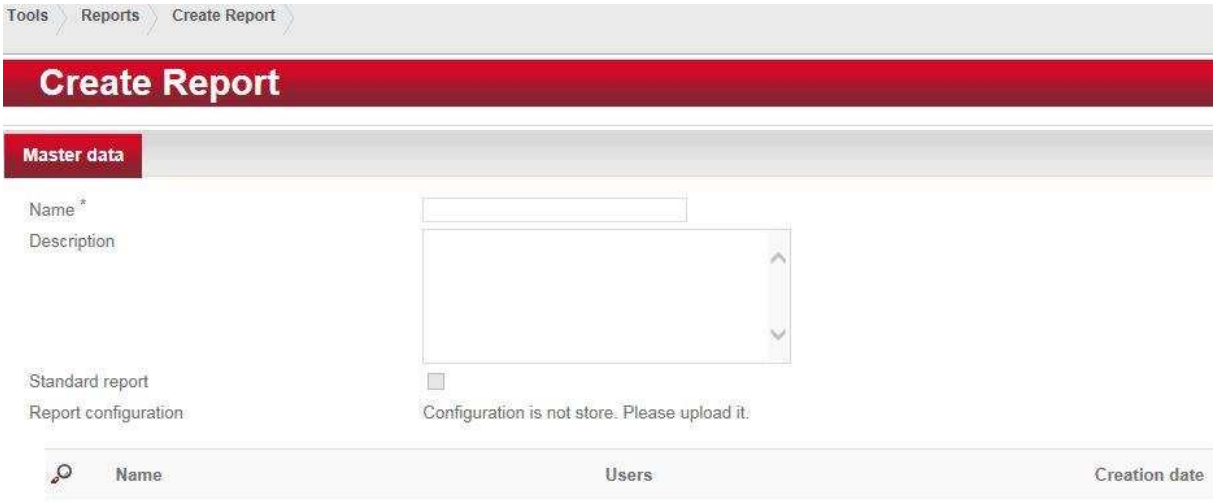
Designation	Description
Alarm reset due to release	Door alarm reset by another release.
Number of failed attempts exceeded	Maximum number of non-permitted access attempts reached at this access point.
Output on	Not yet implemented.
Output off	Not yet implemented.
Output voltage OK	Output voltage of serial interface is OK again.
ID expired	Access denied because validity has expired.
ID unknown	ID unknown in controller.
ID query	Not yet implemented.
ID index re-created	Internal ID index file re-created due to file error.
Authentication error	ID could not be correctly authenticated.
Area change	Message concerning area change of an ID.
Area change error	ID causing error during area change.
Bus subscriber disconnected	Bus subscriber no longer accessible.
Bus subscriber connected	Bus subscriber accessible.
Data error	Maximum value exceeded or minimum value undershot when transferring data from table ...
Permanently free	Access point permanently unlocked.
Permanently locked	Access point permanently locked.
Diagnostic file full	The diagnostic file is full. It will be renamed and the old backup file deleted.
Passage	The passage contact has triggered, a passage has taken place.
Entry time expired	Entry time between two keypad digits exceeded, input deleted.
Entry time overwritten	Entry time between two identification characteristics was too long. The entries have been deleted.
Input off	Signal input open.
Input on	Signal input closed.

Input short-circuit	Signal input short-circuited.
Input interruption	Signal input interrupted.
Result of SD check	Result of checkdisk on SD card was:---
Incorrect PIN code	The PIN code entered was incorrect.
Incorrect door code	The door code entered was incorrect.
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.
Entry time expired	Release of access point / door took place without door being opened.
Disconnected	Communication between host and controller disconnected.
No ID for PIN code	Unable to find ID for PIN code. Only for keypad without reader.
No passage	Passage contact not triggered, no passage took place.
No access profile	No suitable access profile on ID.
No output voltage	Output voltage of serial interface is too low.
Operating mode configuration error	Selected operating mode of access point is incorrect.
Contact to card aborted	Card or transponder removed during processing.
Read error	Error occurred when reading card or transponder.
Reader defective	Reader sabotaged.
Reader OK	Reader OK (again).
Reader ID data	Card information transaction --> bit information that was read via a CI / Da or Wiegand interface. (between iTCRIF and iTC).
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.
Normal situation	Access point in normal condition.
PIN code change	PIN code changed to ---.
Reset	Controller has carried out a reset.
Resource signalling value	Resource signalling the following value ---
Resource list changed	Number of system resources changed.
Latch open	Latch is open.
Latch closed	Latch is closed.
Latch error: Break-in	Door open although latch is closed.
Latch error: Latch open/door closed	The latch has been open for too long after the door was closed.
Latch error: Latch closed/door open	Door still open although latch is already closed.
Sabotage contact triggered	Reader sabotage contact triggered.
Sabotage contact OK	Reader sabotage contact OK.
Write error	Error occurred when writing to card or transponder.
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.
Keypad active	Automatic zone for keypad active.
Keypad inactive	Automatic zone for keypad inactive again.
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.
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 unlocked without permission	Door unlocked without permission, without prior release.
Door locked	The door is locked.
Door open too long	Door has been open for too long.
Door release by host	Door has been directly released by host.
Door opener active	Automatic zone for door release button active.
Door opener actuated	Access point has been released by pressing the door release button.
Door opener inactive	Automatic zone for door release button inactive again.
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: ---
UID of SD card and processor	Both UIDs are reported.
Unknown	Event type unknown to host.

Connected	Controller connected to host again.
Encryption error (SD card)	SD card has unexpected data encryption. Affected files will be deleted.
Pre-alarm triggered	Pre-alarm (advance warning) for a door or latch too long.
Timed anti-passback still active	Timed anti-passback still active for this ID.

15.9.4. Reports

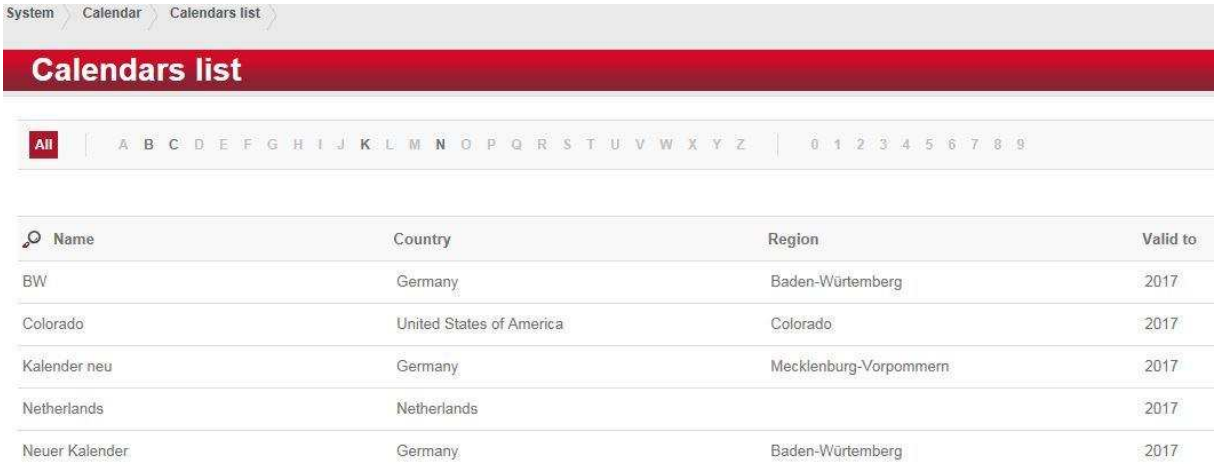
In order to manage reports, go to menu **Tools\Reports**. In order to create reports, click on “Create” in the menu on the left-hand side and give the new report a **Name** and a **Description** if required. The check box next to **Standard report** indicates whether it is a report that was supplied 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.



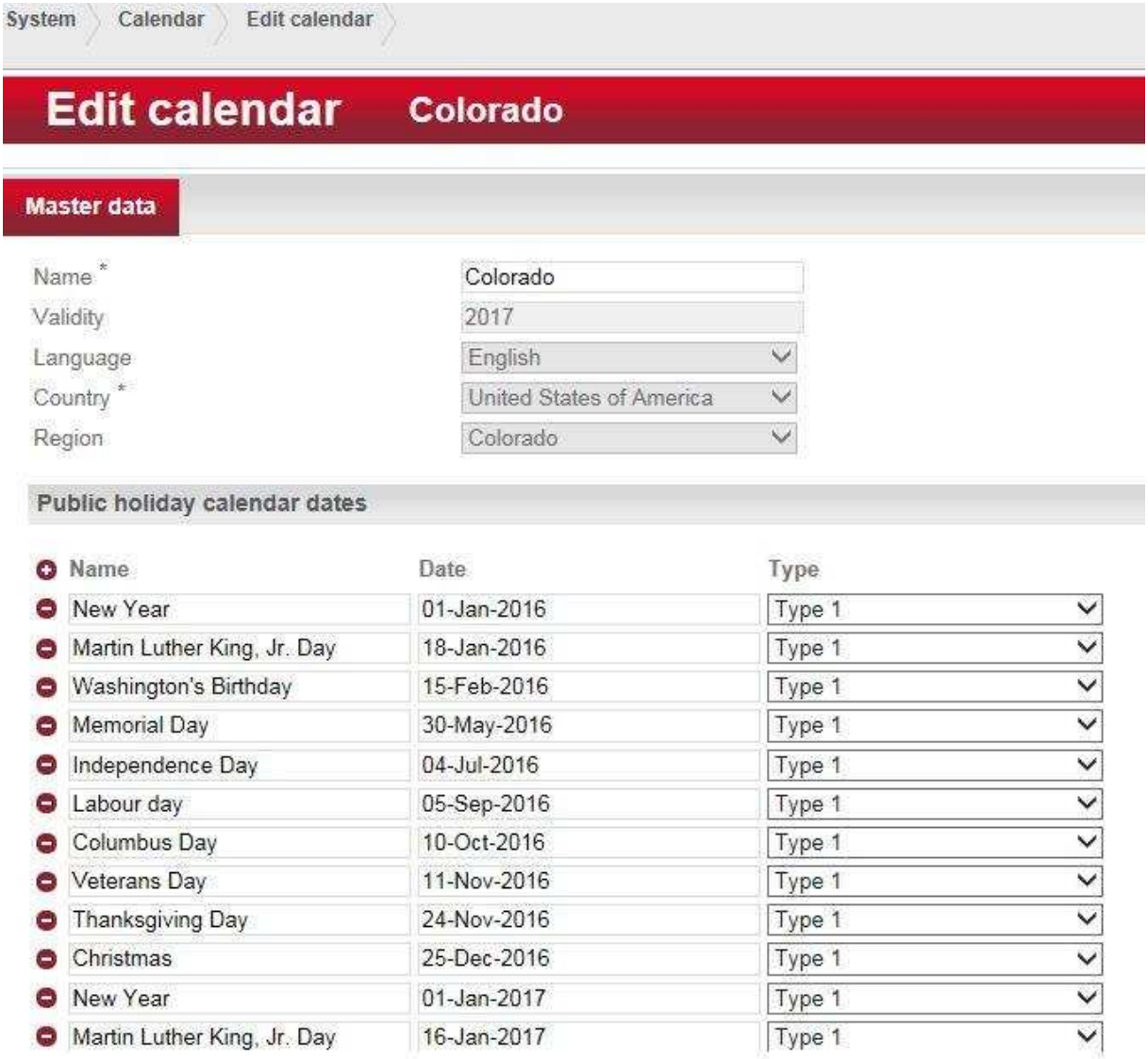
15.10. System

15.10.1. 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.

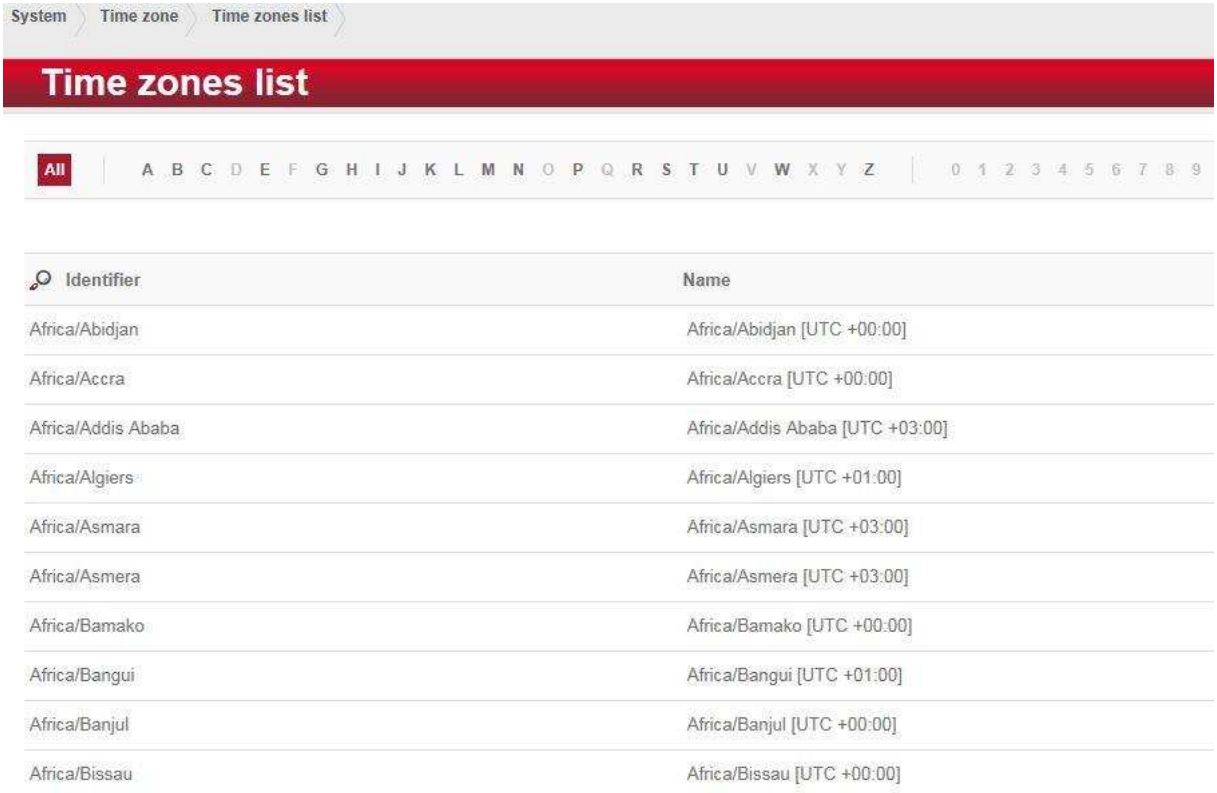


Dialock has a facility for creating your own additional public holidays for the calendars that have been created. This is useful if different access authorisations are to apply for company holidays, for example.
In order to do this you create an appropriate time model for public holiday type 2 and assign 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.

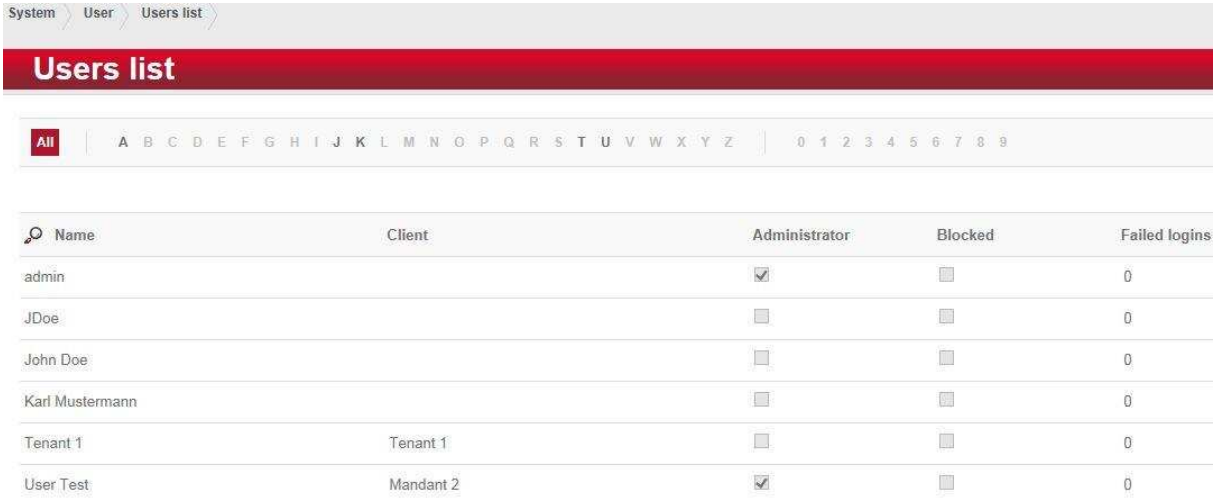
15.10.2. Time zone



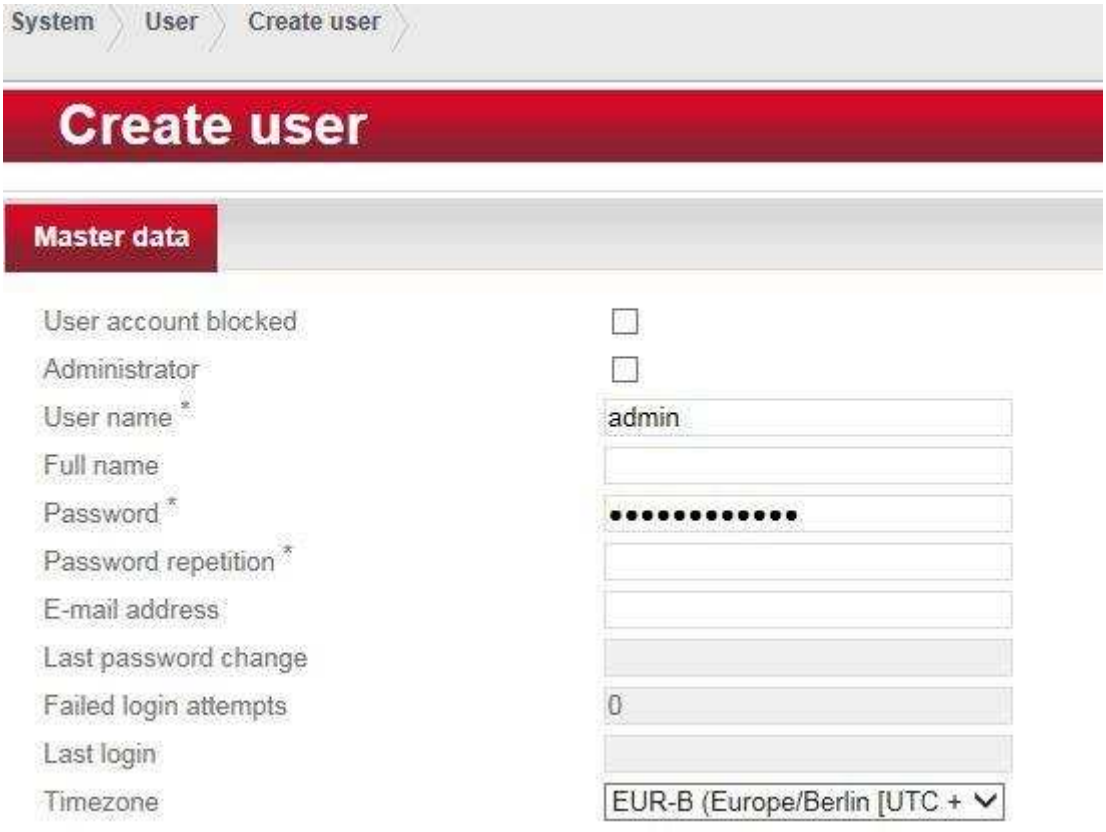
The time zones list represents all international time zones. The time zone for your own region can be selected and edited in this list:

After making changes, the time zone can be saved under its own time zone abbreviation. The time zones are used when the **Devices**/**Terminals** are being adjusted.

15.10.3. User



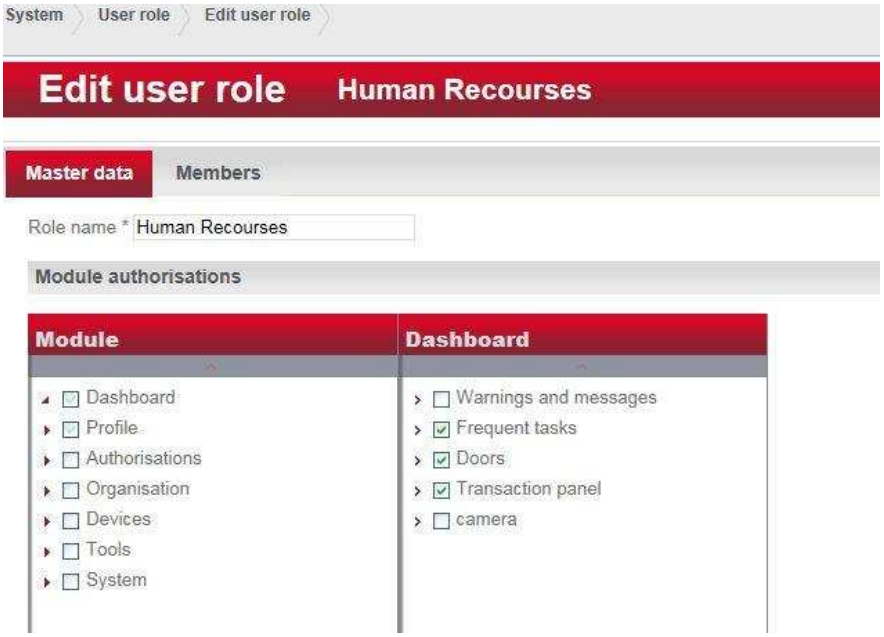
The **System\User** menu shows an overview of the current users of the system.



Additional users are created in the User sub-menu.

15.10.4. User roles

The user roles list represents the created user roles of the system.



Database management

Licence administration

Transponder definition

System diagnosis

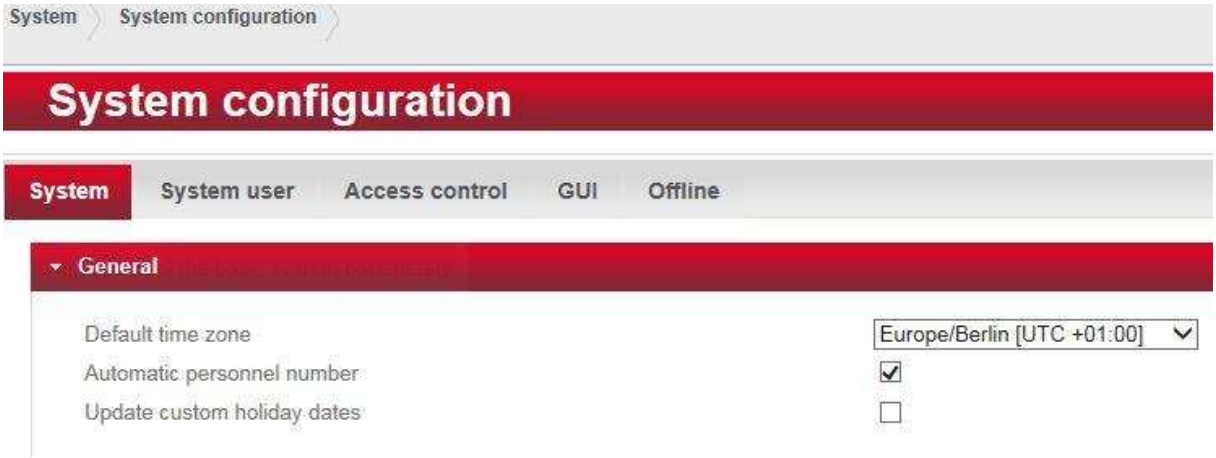
The assignment of the permissions in connection with the respective role takes place in **Edit user role.**

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

15.10.5. System configuration

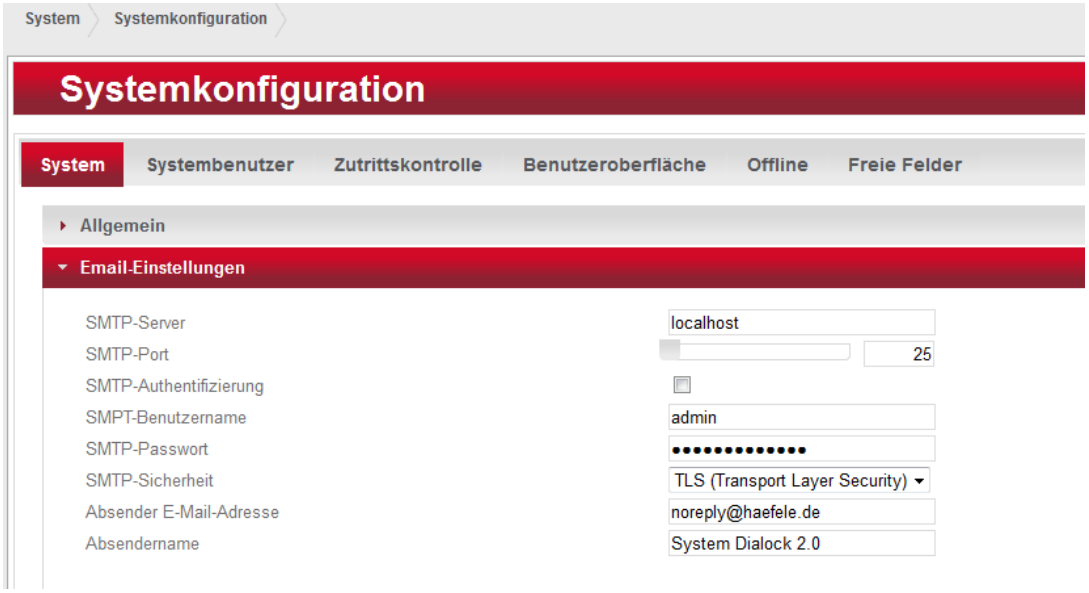
15.10.5.1. Miscellaneous

The configuration of the Dialock software is accessed using **System > System configuration**. In the "**System**" tab under **General** you determine the **Time zone** to be used by iSAC-3 by default by selecting from the drop-down menu.



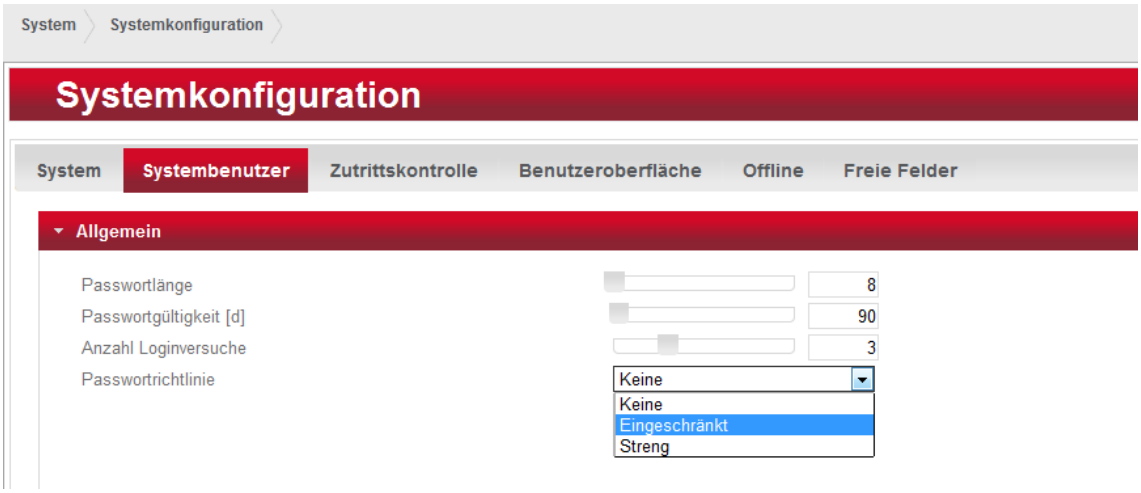
If the personnel number is to be allocated automatically when recording personnel data, activate "**Automatic personnel number**".
Update custom holiday dates must be used if self-defined holidays are repeated annually on the same date.

15.10.5.2. E-mail settings



Enter the e-mail send parameter to be used by the system here. This address is used by the system for sending e-mail messages.

15.10.5.3. System user



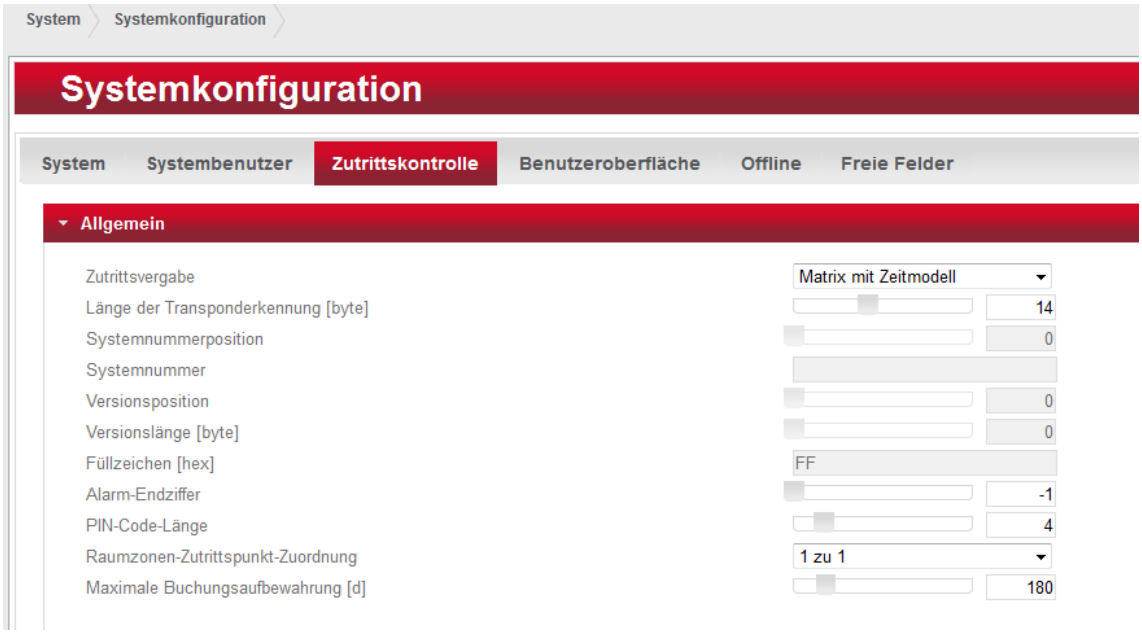
The password prerequisites are defined in the “**System user**” tab of the **System/System configuration** menu. Here you determine the minimum **Length** and duration of the **Validity** of a **Password**. Here you define the maximum number of **Login attempts** that a used can make before he/she is blocked.

Under **Password guideline** you define how a user has to create his/her password:
None: The user can enter a password with any format.
Any password can be used: The password must be alphanumeric.
Strict: The password must contain alphanumeric characters, special characters and upper and lower case.

15.10.5.4. 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 allocation.

Note:
If the role-based function has been selected for access allocation, it cannot be undone.



The global length of the IDs in bytes in the system is defined under **Transponder identifier length**.
The position of a fixed system number in the ID 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 ID is set under **Version number position**.
Under **Filler character** you define a character with which IDs that are too short will be filled.
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.

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.

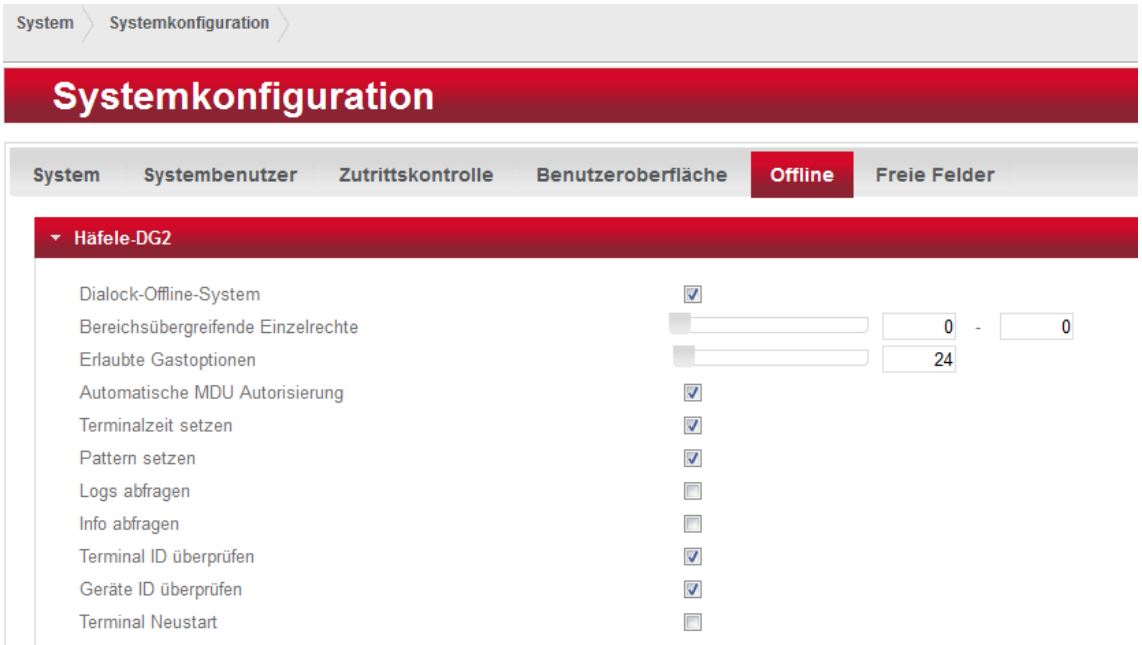
15.10.5.5. GUI

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**.

15.10.5.6. 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.

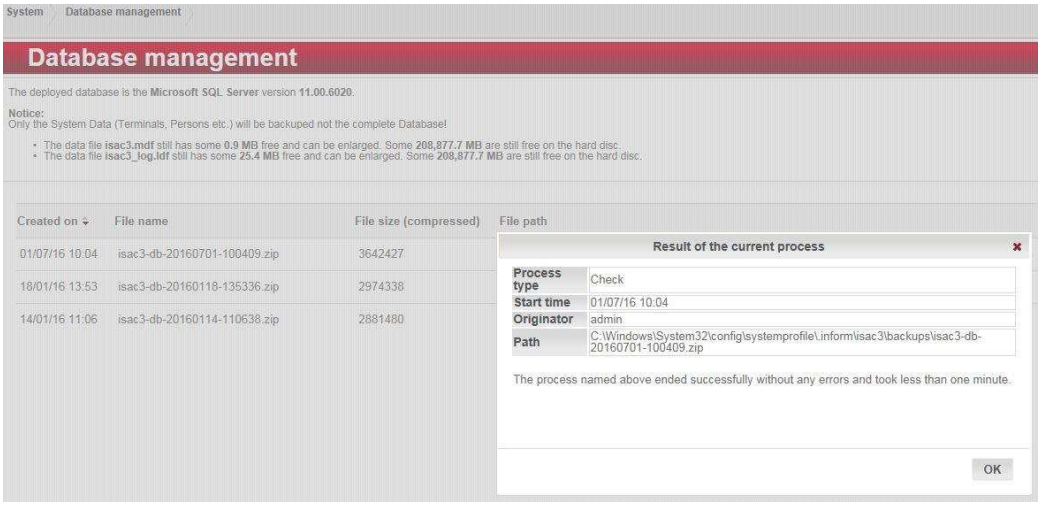


15.10.6. Database management

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

Basic important note:
Database management takes place on an object 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 “**Backup**” 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.

15.10.7. 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 and access points.

Click in the input field to select your licence file in order to then import it by clicking on “Import” in the menu on the left-hand side.

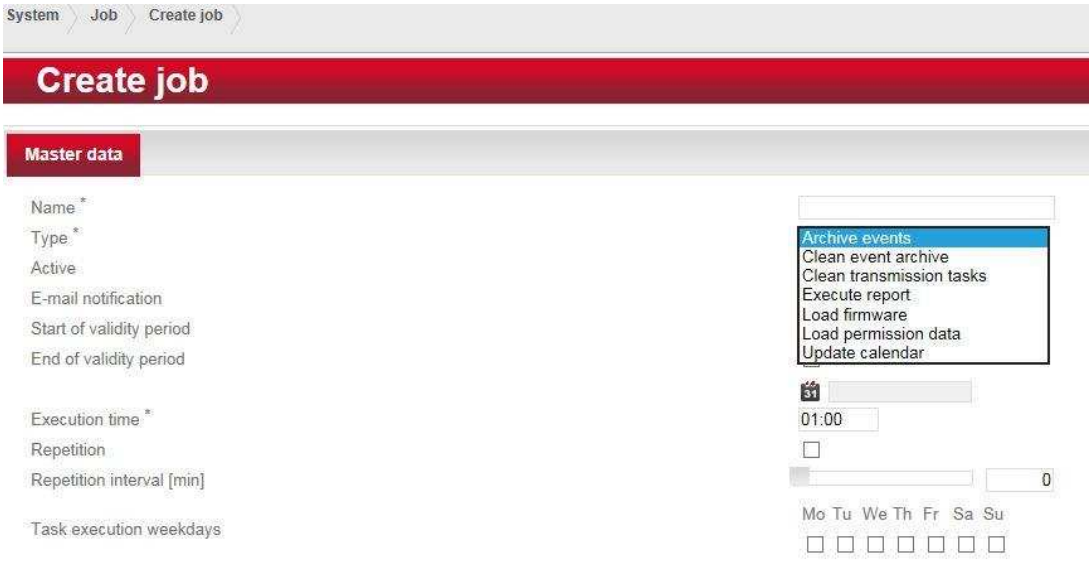
Save the results of this action.

The system then has all of the performance specifications in accordance with the software version that you have purchased.

15.10.8. Job

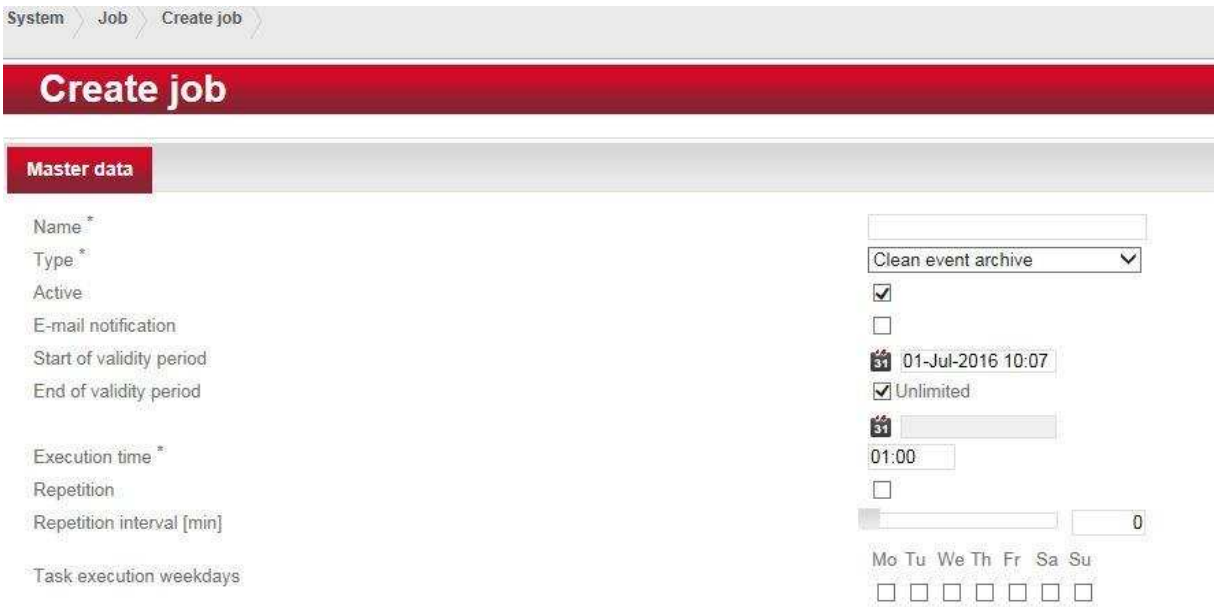
Jobs are used to automatically carry out certain jobs once at certain times or at regular time intervals.

15.10.8.1. Management of job master data



In order to create or manage a job, go to the **System\Job** menu.

Give the new job a **Designation**. The types contained within the following drop-down menu are available for selection as possible job types.
Select the required **Type**.



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.

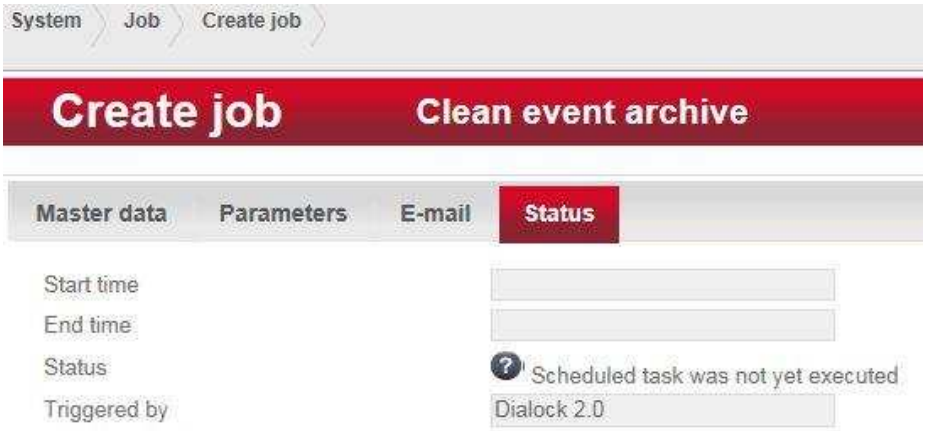
The **Start of validity** and the **End of validity** can be defined exact to the day or minute.
The **Execution time** determines the time when the job is to be executed.
If the job is to be executed every 10 minutes, for example, the "**Repetition**" must be activated and the "**Repetition interval**" 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**".

15.10.8.2. Managing the "Archive events" parameter

In the "Parameters" tab of the **System\Job** 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.

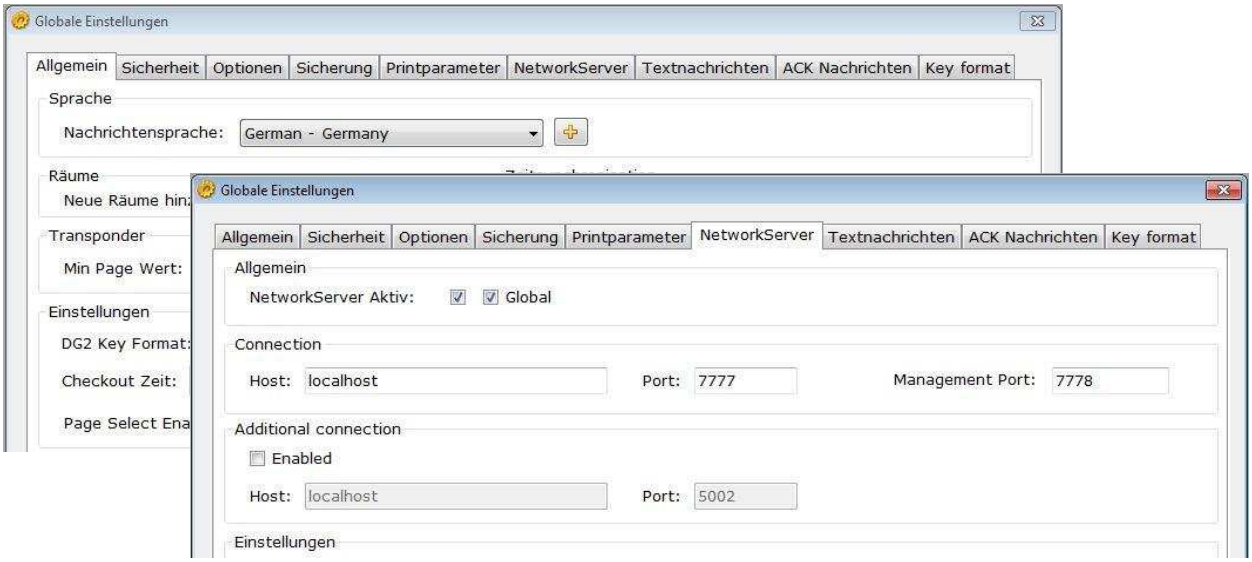
15.10.8.3. Status of jobs

In the "**Status**" tab of the **System\Job** 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.

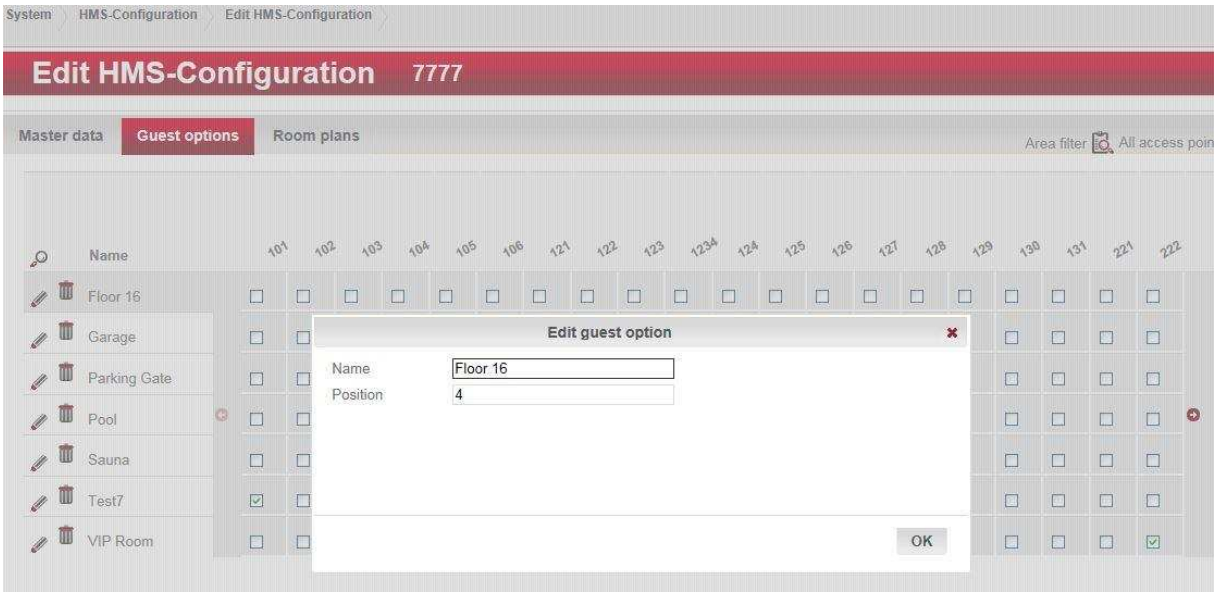


15.10.9. HMS configuration

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.

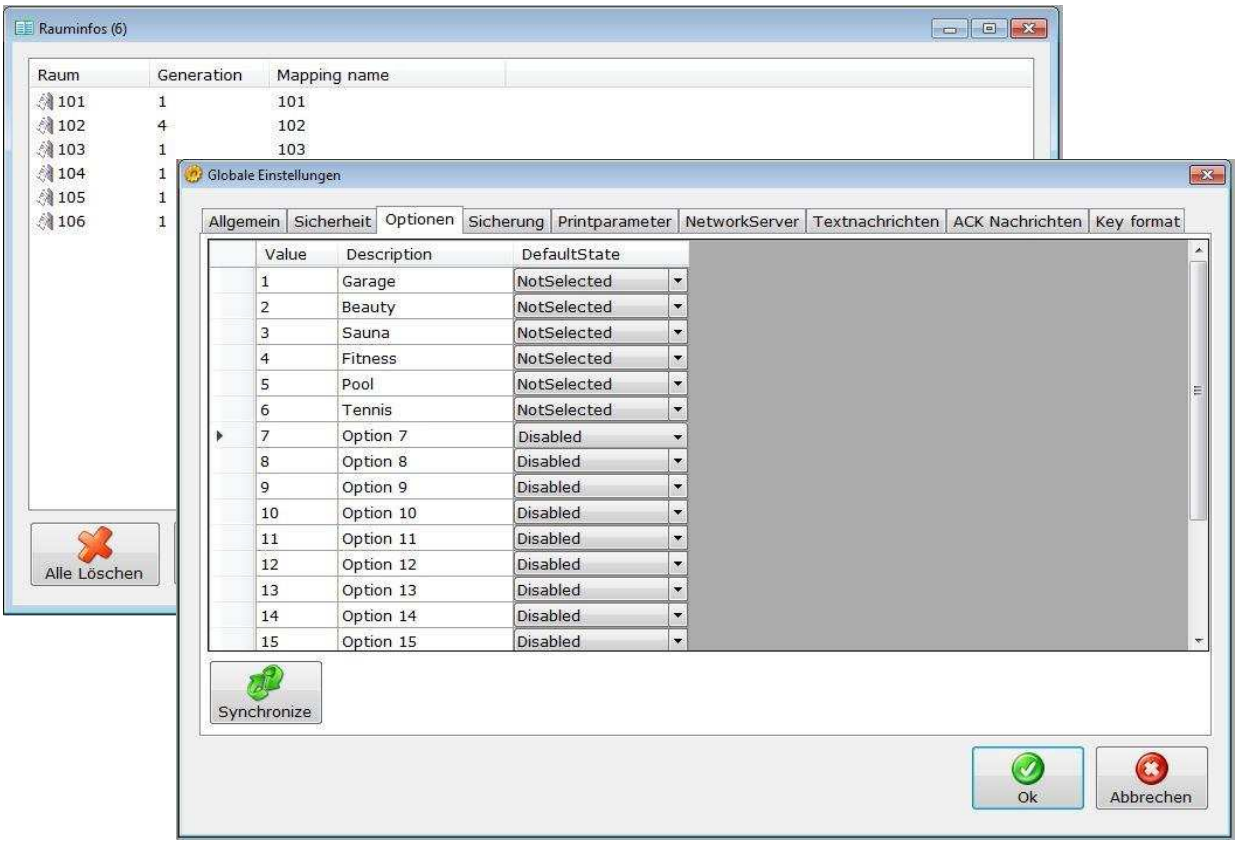


Settings for the HMS interface communication
If the “DG2 Key Format” has been selected in the HMS Interface Administration, the set ports (default 7777 / 7778) can be adapted if necessary in the “Network Server” tab.



Definition of guest (visitor) options
A new option can be created by clicking on the “Create guest option” button. 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.

15.10.10. 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 10,000 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.
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. Time models (online/offline)
5. Reader
6. Persons
7. Groups and organisational units
8. Identification characteristic (transponders, PIN codes)
9. Scripts
10. Transponder definition
11. Reports

Note!
Definition of “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 (Fig. ❶) can be used to give system users the authority to see the data of other clients (Fig. 1- 2), edit it (Fig. ❸) and/or delete it (Fig. ❹).
The actions of a system user, i.e. creation, editing and deleting of data records are assigned to the active client (Fig.❺). 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 (Fig. ❻) can switch between clients (Fig. ❺). 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 (Fig. ❸) or delete them (Fig. ❹) depending on the authorisation.

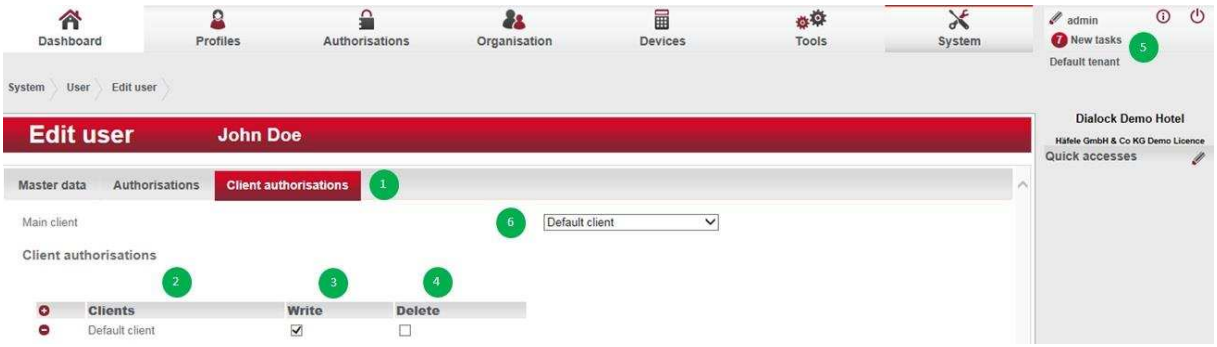


Fig: Client authorisations

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 (Fig. 6) 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 (Fig. 5).

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 (Fig. 2- Fig. 4) for the client that has been assigned to him (Fig. 2). A client administrator cannot change the active clients (Fig. 2). 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 (Fig. 5). 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.

16. 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.
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.
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 that the ID was held in front of the authorisation writer is longer ago than the updating interval, access is refused.
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.
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
Construction site lock	former SA mode. Simplest, temporary operating mode in a Dialock system. This is set in the factory. Keys can be taught in with this with the programming key immediately after installing a terminal, after the programming key and the deletion key have been created. When a software-programmed key is used for the first time, this operating mode is permanently disabled and the associated keys become invalid.
User	Person, who has rights for using the Dialock software.
Authorisation updating	Procedure in which an authorisation writer/validation terminal updates the offline authorisations on an ID for the duration of the defined authorisation period / validation period.
Authorised person(s)	Person(s) who is (are) authorised for procedures in the software or at access points in an access control system.
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 writer	Online wall terminal at an access point that in addition to performing the authorisation check, can also update the offline authorisation on the IDs.
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.
Visitor key	“Individual key that has been created for a visitor. The validity thereof is limited to the duration of the visit”.
Visitor management	(IT) device for recording visitor data and creating visitor IDs and keys. Balancing!
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.
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 record	Data record consisting of all data of an access event, such as the ID number, the transaction time and the terminal action.
Transaction panel	Tabular display of the saved access events in the DIALOCK 2.0 GUI (dashboard).
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.
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.
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.
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.
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.
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.
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)
Individual access right	Access authorisation for a single access point without assignment to a room zone
EMA	Burglar alarm system
End date	Date after which a time-based/area-based access authorisation becomes invalid.
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
Release time	Time for which the locking element at an access point is released for opening. See also open time
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
Guest key	Key for the guest of a hotel or similar accommodation. Normally valid for the duration of the booked stay.
Generation	Incremental index on a key that is always incremented at the point in time of key programming. A DIALOCK terminal uses the generation index to distinguish a key from a replacement key that has been created later (after loss or theft) which otherwise has identical data. Replaced with “Time stamp created” in Dialock
Group authorisation	Collection of several individual authorisations for a group of persons, e.g. for a department.
Start of validity	Point in time from which an ID is valid. This point in time is independent of group or individual access rights and time models.
End of validity	Point in time to which an ID is valid. This point in time is independent of group or individual access rights and time models.
Means of identification	ID cards and tags that contain information that can be read from an input device in the sense of identification characteristics. QSEC
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.
Coding device	Technical device for writing data onto transponder media, triggered by an authorised user.
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.
Login key	Key for authentication as an authorised user of the DIALOCK software at workplaces with an encoding station
Login right	Authorisation to use the Dialock software. Part of the graduated authorisation concept.
Deletion key	Special key that is used to delete keys that are to be invalidated at an offline terminal.
Macro (program)	Additional programs that are saved in the non-volatile memory of Dialock terminals to supplement the basic functionality.

MDU Mobile Data Unit	Portable device for transmitting terminal parameters and terminal configurations data to and reading out terminal logs and operating data from the offline terminals.
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.
Emergency authorisation system	Offline terminal operating mode in which the teaching in of keys using a programming and deletion card 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.
Usage frequency	Frequency with which an access point in a building is used, in relation to a certain period of time (week, day, hour).
Object key	
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.
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.
One Shot Key	Key with an access right that can be used once only. The key becomes invalid after use.
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.
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 in the case of offline terminals.
Patient key	Individual key that has been created for a patient.
Person master record	This data record is created for each employee 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 ID or key. Person master records can be imported from existing personnel systems as an Excel file.
PIN	Person Identification Number
Privileged key	Key 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 key in standalone mode, used to assign authorised keys to offline terminals in standalone mode and also takes over additional functions of the “Privileged keys”.
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.

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.
Role model	_____
SA Mode	“Stand Alone Mode”. Operating mode of an offline terminal in which the authorised key is not assigned using access control system software but authorised directly at the terminal using the programming key.
Sabotage contact, tamper switch	Electric contact or switch that generates an alarm signal if a device is opened.
Locking group	Access right for a group of terminals (1 to n terminals)
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.
Access right	See Access authorisation
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.
Protected area	A self-contained object or sub-area thereof (room, building, site) that is monitored by an access control system.
Signalling	Visual or acoustic indication of an operating status or the test result of an access control input device.
Locking element	Electromechanical component that performs reliable locking and controlled unlocking of the passages at the access points of an access control system (doors, gates, turnstiles, 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”
Master data	Data record with which an object belonging to an access control system is described. This could apply to persons, groups, users, IDs, terminals, areas, readers, coding devices etc.
Location	Top spatial level of the access control system topology.
Start date	Date from which a time-based/area-based access authorisation becomes valid.
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.
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.
Triple DES, 3DES	Encryption algorithm in which the DES procedure is used three times. Has now been superseded by AES.
Door alarm	The door alarm is triggered if the door is not closed after expiry of the door opening time.
Door release time	See Open time
Door opening time	The door opening time is the time for which a door may remain open before the door alarm is triggered.

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.
Door monitoring time	This the length of time for which the door may remain open without the door alarm being triggered.
UID	Unique Identifier Number. Globally unique 4-10 byte number that is saved in transponders when they are manufactured.
Validation	Procedure in which a validation terminal/authorisation writer updates the offline authorisations on an ID 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 ID's.
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.
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.
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.
Route monitoring	Recording of the route of a person in a system by recording the use of the key at access control readers.
White List	List of keys (UID or key number) in an evaluation unit that are authorised at this unit.
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	Defined time interval within which an access authorisation to a room, a room zone or an area exists. Designation from Dialock 1; in Dialock : Time model
ZKA	Access control system. System for regulation and automatic checking of access authorisations, control of locking elements and registration of transactions (VdS).
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.
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
Access regulation	See Access control

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

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

Catalogue number 732.29.116
Drawing number 6.162.90a