Access PE - Offline Locking System

BOSCH

en Installation Manual

Table of contents

1 Overview

The Access Professional Edition System (hereunder referred to as **Access PE)** provides a self-contained access control for small and medium sized companies. It consists of several modules:

- LAC Service: a process which is in constant communication with the LACs (Local Access Controllers – hereafter referred to as Controllers). AMCs (Access Modular Controllers) are used as Controllers.
- Configurator
- Personnel Management
- Logviewer
- Alarm Management
- Video Verification

The modules can be divided into server and client modules.
The LAC service needs to remain in constant contact with the controllers because firstly it constantly receives messages from them regarding movements, presence and absence of cardholders, secondly because it transmits data modifications, e.g. assignment of new cards, to the controllers, but mainly because it carries out meta-level checks (access sequence checks, anti-passback checks, random screening).
The Configurator should also run on the server; however it can be installed on client workstations and operated from there.
The modules Personnel Management and Logviewer belong to the Client component and can be run on the Server in addition, or on a different PC with a network connection to the server.
The following Controllers can be used.

- AMC2 4W (with four Wiegand reader interfaces) - can be extended with an AMC2 4W-EXT
- AMC2 4R4 (with four RS485 reader interfaces)

2 General

2.1 User Login

The following applications are available. The the respective User manuals for details:

Personnel Management

Configurator

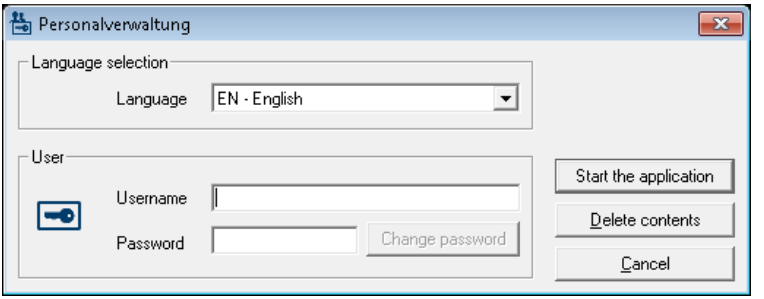
Logviewer

Map and Alarm Management

Video Verification

The system's applications are protected from unauthorized use.
The **default passwords** on first usage are:

- Username: **bosch**
- Password: **bosch**

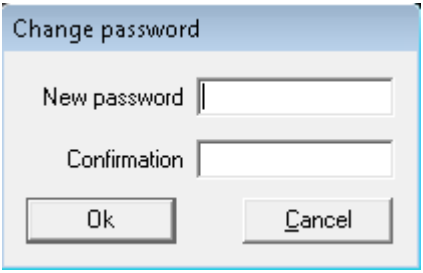


The upper drop-down list can be used to select the desired interaction **language**. The default is that language which was used to install the application. If there is a change of user without restarting the application then the previous language is retained. For this reason it is possible for a dialog box to appear in an undesired language. In order to avoid this, please log in to Access PE again.
Access PE applications can be run in the following languages:

- English
- German
- French
- Japanese
- Russian
- Polish
- Chinese (PRC)
- Dutch
- Spanish
- Portuguese (Brazil)

Notice!
All facilities such as device names, labels, models and user-rights schemes are displayed in the language in which they were entered.Similarly buttons and labels controlled by the operating system may appear in the language of the operating system.

If a valid username/password pair are entered then the button **: Change Password** appears. This can be used to start a new dialog to change the password.



Notice!
Do not forget to change the password!

The button **Start the application** checks the user's privileges and, based on these, starts the application. If the system is unable to authenticate the login then the following error message appears**: Wrong username or password!**

3 Offline Locking System

The offline locking system is a **PegaSys** system from **Normbau** (hereafter referred to as the "locking system" or "offline system"). This is used to secure objects that cannot, should not or must not be monitored online.
Offline systems are normally used where non-real-time data transfer means that high availability of individual components is not necessary, where the infrastructure does not permit a direct connection (e.g. cabling for installations set up at a considerable distance) or where the installation of online components is too expensive. In comparison with conventional locking systems (security locks with specially manufactured keys), the advantage of offline systems is that significant investment costs are only incurred when installing or extending the system. Locks and keys do not need to be updated or replaced (e.g. in the event of loss or theft), as the software can deactivate the units concerned (cards) and therefore render them unusable.
Suitable objects for offline systems are generally installations with a number of individual areas to secure, such as hotels, student residences and hospitals.
PegaSys components are integrated into the Access PE access control system and managed from there.

3.1 Explanation of terms

In order to differentiate between the individual access control components, the following terms are used for the various components:

- **Access control system**
  This refers to the online components
  These include
-
  - The data recording level (dialog system, database, logbook etc.) i.e. top level
  - Controllers, which take decisions regarding access on the basis of data they receive from the top level.
  - Readers, which read the code data from the cards and forward it to the controllers.
- **Locking system**
  This includes the offline system elements
-
  - Cards, which contain the authorization data.
  - Door terminals, which take decisions regarding access on the basis of the authorization data that is read.

The locking system as an integrated unit also makes partial use of the dialog system and the access control system's controllers and readers.

3.2 Special features of the locking system

In access control systems (for example, the Access PE) code data is read off the card and stored in the database in combination with the personnel data and access authorizations. When scanned at an access control reader, the code number is read again and compared with the stored data. If this check is positive, the person in question is granted access.
A connection to a data storage element of the system (= online system) is therefore essential.

With offline systems, access authorizations for certain doors are stored on the card. [The locking system variants for which authorizations are stored in the door terminal (armature or cylinder) are not described here.] When scanned, these authorizations are read and a check is carried out to ascertain whether or not the card contains the identification for the door concerned and has up-to-date data.

The offline variant poses a basic security risk, as it is essentially impossible to prevent misuse in the event of loss or theft. In access control systems, cards of this kind can be blocked, deleted or assigned a validity expiration date, whereas offline systems offer no means of direct intervention. However, in order to keep the risk of misuse as low as possible, the authorizations are assigned an expiration date/time. If this deadline elapses, the authorizations are no longer valid. In order to reactivate them, the validity period must be extended. This is carried out via a special reader with write capability (e.g. DELTA 7020). If the authorizations have not been deleted or blocked in the meantime, they are extended or renewed when the card is scanned at this online reader.

3.3 Locking system components

When the offline system is installed, the following necessary applications and extensions are set up:

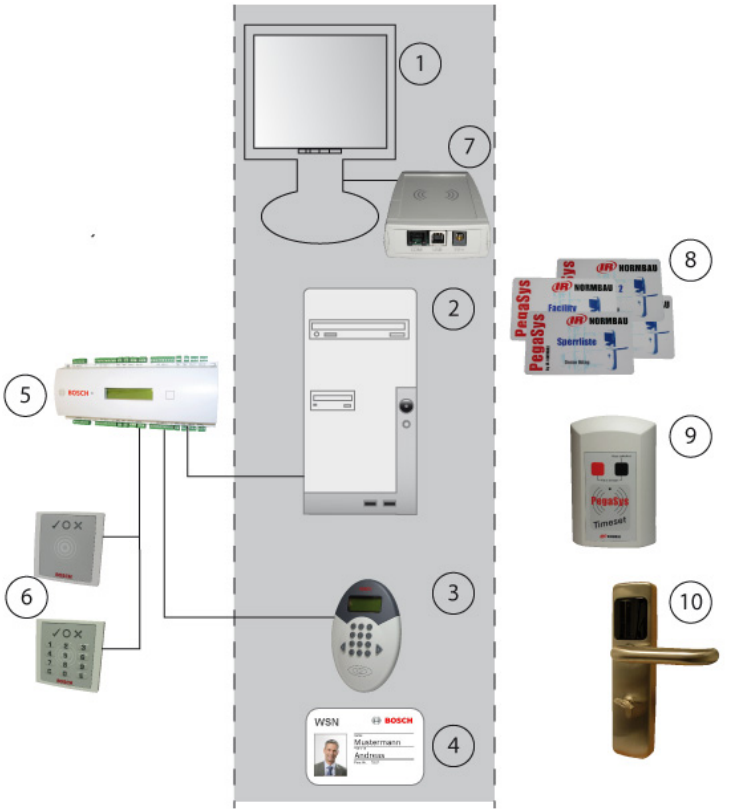
- **Software**
-
  - Configurator > **Offline locking system**
    This application is used to set up the features and make all the general settings, create time models, and configure doors and door groups.
  - Configurator > **Entrances**

When setting up entrances, write capability can be activated and configured for the readers.

- Personnel Management > **Personnel data**
  This dialog contains (after initialization with a facility card) another tab called **Offline Access Authorizations**; this is where you can allocate authorizations and record cards for the locking system.

- **Hardware**
-
  - **System cards**
    System cards are used to initialize the door terminal and to update data (e.g. blacklists).
  - A **read-write device** for user cards and system cards must be connected to the workstation(s) at which offline system data is processed.
  - A **mobile read-write device** (timesetter) which updates door and time model initialization cards, which in turn are used to update/initialize the door terminals (optional).
  - **Terminals** to read the user and system cards at the doors in the locking system.
  - At least one write-capable reader for distributing and extending access authorizations for the locking system.

3.4 System Overview



When the locking system is integrated into the Access PE access control system, certain components are used by both systems. The gray area in the diagram above contains the system components that are used by both the access control system and the locking system. The items on the left are purely access control installations and the items on the right belong only to the locking system.

1. Workstation
2. Server with configuration application and database

3. Access control reader with write unit ("write-capable reader")
4. Card - for both systems
5. AMC2 4R4 Access Control Panel
6. Access control readers
7. Dialog read-write unit for online and offline system data
8. Various system cards for the locking system
9. Mobile read-write units for date/time stamping
10. Door terminal with read unit

3.4.1 Description of system components

The following sections describe the components listed above for both systems, focusing mainly on the function of the common elements.

Workstation

The same dialog interface [**1**] is used to create personnel data for the access control system and for the locking system. Only a single step is required to allocate both access authorizations for the Access PE and access rights for the offline system.
Lists outlining the status of authorization allocations for the locking system can be called up via the same menu items as used for access control.

Server

The software for the access control system and the locking system run on this computer [**2**]. The Access PE Configurator is also used to configure the readers [**3**] for the locking system. Data for the offline system is managed in special tables of the Access PE database.

Write-capable readers

At least one reader of this type [**3**] must be available. Ideally, these are placed at entrances used on a frequent basis (e.g. the main entrance) so that authorization for the locking system is extended at the same time as access is granted to the secured facility.

However, it is also possible to install these readers at special locations, independently of the access control system, so that rights are not extended automatically but have to be specifically obtained.

An RS485 reader is configured on an AMC2 4R4 with L-bus protocol for setup.

Notice!

Don’t activate Videoverification to this reader.

This reader type cannot be used for arming/disarming (DM 10 and 14).

Card

No special cards [**4**] are required for the offline system. The data required for the locking system is written to separate sectors of the access control card.

Notice!

For the offline system, only a person's card 1 can be used.

AMC2 4R4 Controller

An AMC2 4R4 L bus [**5**] (= access control panel with RS485 reader interface) is required for the write-capable reader [**3**] that is used as a read-write unit for the locking system.

The readers dedicated solely to access control [**6**] can use any protocols and read procedures, and can be operated with any AMC2 variant.

Access control readers
These readers [**6**] have nothing to do with the locking system; they simply regulate access requests in the Access PE system. Card holders who are able to use the doors in the locking system [**9**] can also have authorizations for doors in the access control system.

Dialog read-write unit
This device [**7**] is connected directly to the workstation computer via a USB interface and is used to transfer authorizations to user cards and system-related data (e.g. door and time initialization data) to special system cards [**8**]. It is also used to enroll online cards.

System cards
Different system cards [**8**] (time, door and facility cards) are required for the locking system to transfer relevant data — e.g. initialization data — to the door terminals [**9**].

Mobile read-write units (optional) - timesetter
In order for the terminals to be updated, current terminal initialization data is written to door and time model initialization cards via this unit.

PegaSys - door terminal
This read unit uses the individual door identification or its own door group identification to check the access rights for the card holder.
The access rights on the card must be continually updated via special readers with write capability [**3**].

If an emergency opening is required, e.g. if the electronics fail, the terminals have mechanical cylinder locks.

3.4.2 System limits

The following values apply as the upper limits for individual installations in the locking system.

Entrances (doors)	There are no restrictions governing the creation and configuration of entrances. The number that can be allocated as individual door authorizations depends on the length of the datasets ordered; see , *page 17*.
Door groups	The maximum number depends on the length of datasets for the offline data; see , *page 17*.
Time models	15
Periods/Time model	4
Holidays	10

Door groups **Individual doors**	**256**
2	48

Table 3.1: The figures refer to the dataset length in bytes.

Notice!
When **Hitag1** cards are used, only 2 individual doors can be created; similarly, only 240 (instead of the specified 256) door groups can be created — no other formats are possible here.

The dataset length should be selected in line with current requirements. Do not order storage space in anticipation of possible requirements. As data is written to all enabled sectors, increasing the storage space can significantly lengthen the time required for extending or renewing authorizations.

3.5 Access PE - Configurator

Special write-capable readers are required to extend and renew access authorizations for the locking system.
These readers with write capability are created as access control readers and are usually also assigned door control functions. However, they can also be used purely as "rechargers" for offline system authorizations.

3.5.1 Adding hardware components

In the Access PE access control system, no specific reader types are selected when hardware components are added; the appropriate protocol used by the AMCs is selected for each reader.
To add and configure the locking system components, please carry out the following steps:

- Start the Access PE **Configurator**.
- Switch to the **Settings** tab.
-
  - Add an **AMC2 4R4 L-Bus**.
- Switch to the **Entrances** tab.
-
  - Add an entrance with any door model (except DM 10 and 14) and one or two **RS485** readers. There must be at least one write-capable reader at this entrance.
  - For the write-capable reader, select **read/write** in the **Write access** field.
  - Confirm the new entry with **OK** to close the dialog.

– For the reader options, set the **Grant access on write error** and **Write without access rights** parameters if these apply to your system.

3.5.2 Configuring the write-capable reader

If this reader is also used as an access control reader and the settings are different to the default settings, configure it according to your requirements. For further information about the parameters in question, please see the section on adding entrances.

Notice!
Don’t activate Videoverification to this reader.
This reader type cannot be used for arming/disarming (DM 10 and 14).

The following parameters are of importance for the locking system.

Write access	**read only** This reader is purely an access control reader and is not part of the locking system. **read/write** This reader has access control functions and is also activated for the locking system.
Grant access on write error	Access checking and safeguarding (in the online system) does not depend on the success of the locking system write process. The door is released following several unsuccessful write attempts. **Deactivated** (unchecked): If it is not possible to write to the card, access is also denied. **Activated** (checked): The write process has no impact on the access check.
Write without access rights	Rights for the locking system will only be written to the card if the card holder has (online) access authorization for the entrance. **Deactivated** (unchecked): Data is only written to the card if valid authorization is present. **Activated** (checked): Data is always written to the card.

Notice!
If the parameter is deactivated, the write process will be prohibited even if the authorizations are only temporarily invalid (e.g. if time models are used).

3.5.3 Switching the reader protocol

As a rule, readers with write capability are installed at central entrances (e.g. as the entry reader at the main entrance), so that when personnel enter the site in the morning, the access rights for the locking system are automatically updated.
When subsequently setting up the offline system, at least one reader in the facility must be replaced with a write-capable reader. If this involves adding an entrance again, the existing entrance would be deleted and would need to be added again with the write-capable reader.
If the existing entrance was deleted, this entrance would also be removed from all access authorizations. All authorizations would therefore need to be added to the new entrance.
To avoid this laborious process, which could lead to errors, the AMC in question can be reconfigured.

- Go to the **Settings** tab in Access PE Configurator.
- Select the relevant AMC from the list field.
- Click the  button to open the Edit dialog.
-
  - In the **Device type** field, select the **AMC2 4R4 L-Bus** entry.
  - Test the AMC so that the new software is downloaded and confirm the changes with **OK**.
- Save the changes  and send them to the LAC Service process  .

Notice!

Other readers on this AMC must also understand this protocol.
If necessary, these readers must also be replaced.
If you have changed the device type from AMC2 4W to AMC2 4R4 L-Bus, the AMC must also be replaced.

3.6 Configurator - Offline Locking System

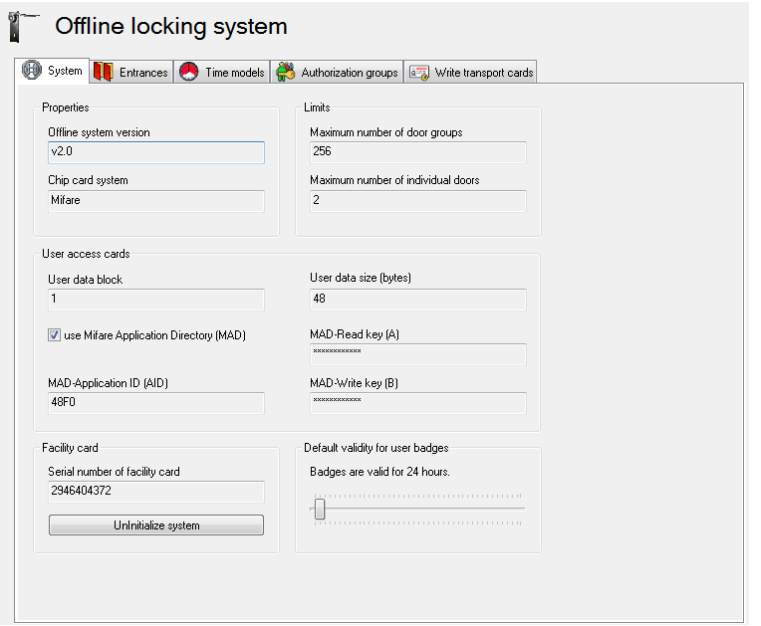
In this dialog, which is accessed by clicking the  button in the Configurator toolbar, the necessary locking system settings are configured on five different tabs. In the interests of user-friendliness, the tabs for configuring the locking system have the same names and icons as the corresponding access control dialogs. Insofar as this was possible given the specific data structure of the offline system, the structure and data processing characteristics of the online configuration process were also used.

The individual tabs are used to manage the following data:

- **System**
  Special offline system data, such as system limits, keys and serial numbers.
- **Entrances**
  As in the dialog of the same name in the access control system, this is where the entrances are managed, but in this case the locking system entrances.
- **Time models**
  As the offline system cannot use the access control time models, these must be set up separately for the locking system, if required.
- **Authorization groups**
  As with the dialog of the same name in the access control system, this tab is also used for combining a number of entrances in the locking system into authorization groups.
- **Write transport cards**
  In order to receive updated data on the locking system installations, individual entrances and time models can be written to transport cards. These are read by the terminals.

3.6.1 Offline locking system: System

When the locking system is purchased, one of the items the customer receives is a "facility card". This contains details of the system settings that the customer specified on the manufacturer's order form.
All of the fields on this page are read-only fields and cannot be overwritten. Their content is read from the facility card and entered into the corresponding fields.
Before the locking system is set up, the **Facility card** dialog field at the bottom of the page contains the **Initialize system with facility card** button. The system data is transferred and set when the facility card is placed on the dialog reader for the offline system and the button is clicked.



Properties dialog field

– **Offline system version**

Locking system software version — only Version V2.0 functionalities are used in Access PE.

– **Chip card system**
  Displays the card technology — MIFARE classic and Hitag1 can be used for Access PE.

Limits dialog field

– **Maximum number of door groups**
  Maximum possible number of access authorization groups.
– **Maximum number of singular door permissions**
  Maximum possible number of individual door authorizations.

These entries correlate with one another and define the available dataset lengths [= User data size (bytes)] on the cards — see also , *page 17*.

User access cards dialog field

– **User data block**
  Details on the card sector in which the offline data write process begins.
– **User data size (bytes)**
  Length of the datasets — this also determines the maximum values for the authorizations.

Notice!
If using Hitag1, these values should be checked when a system is set up for the first time, as these card types do not have a function to prevent areas that are already in use from being unintentionally overwritten.

Data is only written to the following four fields if the MAD has been activated in the MIFARE card technology.

– **use Mifare Application Directory (MAD)**
  If this check box is activated (checked), data for the other MAD fields will also be displayed.

When the MAD is activated, the user data block is simply the default sector and is dynamically defined for each user card if the specified block is occupied.

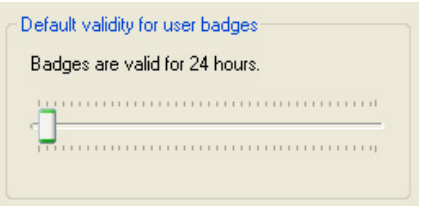
- **MAD-Application ID (AID)**
  Identification number for the MAD of this system.
- **MAD-Read key (A)**
  Read key for this system.
- **MAD-Write key (B)**
  Write key for this system.

Facility card dialog field

- **Serial number of facility card**
  Serial number of the facility card that has been read in — if this serial number is saved, the facility card cannot be overwritten.

Dialog field **Default validity for access cards**

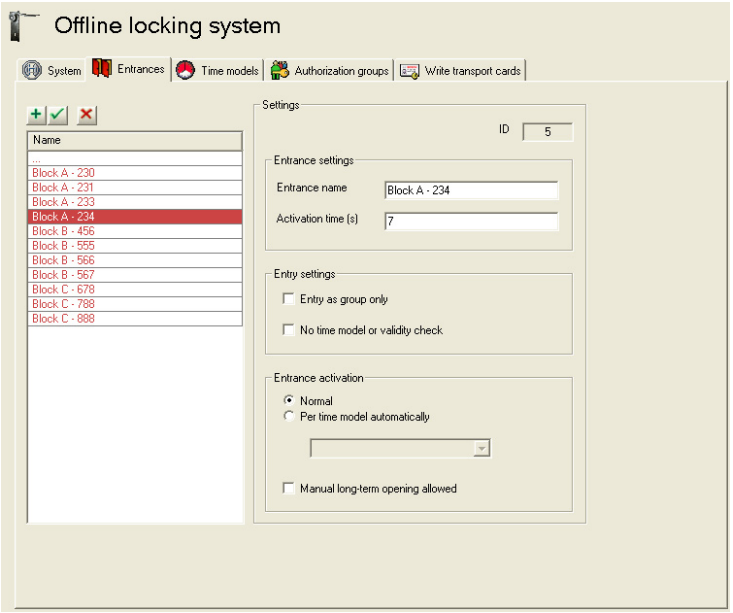
- Use the slider to set the default validity period in hours for the offline system's access cards. Values from 1 to 1000 can be used. First hold the left mouse button and slide to set an approximate value, then use the arrow keys to set values exact to the hour.



Immediately after initialization, the offline locking system is activated within the displayed limits. The **Offline Access Authorizations** tab is now displayed in Personnel Management.

3.6.2 Offline locking system: Entrances

A list entry must be created and configured in this dialog for each door terminal in the locking system. These can then be assigned to certain door groups.



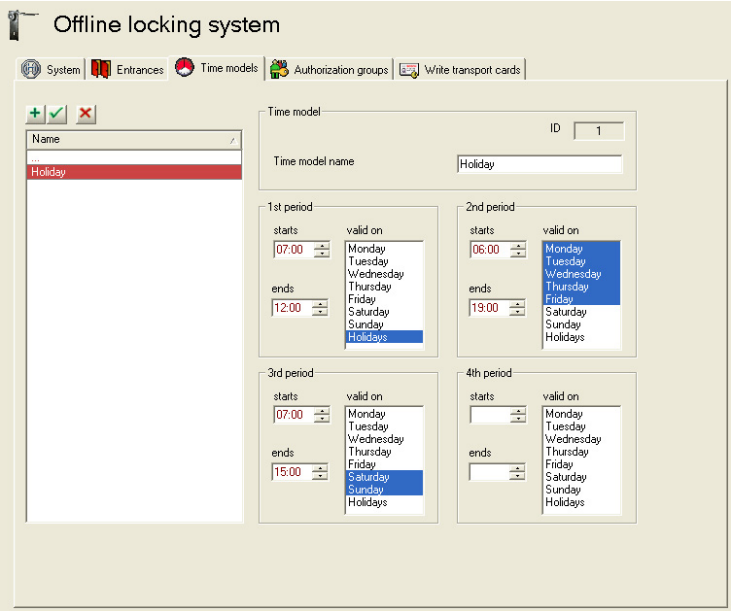
The list field contains all entrances that have been set up and are fitted with locking system terminals. The button above the list enables new list entries to be created, and existing entries to be edited or deleted.
The parameters for the entrance selected in the list are displayed in the fields to the right, where they can be entered and edited.

Parameter	Description
ID	Assigned by the system when the list entry is created and cannot be edited. Sequential number that uniquely identifies the dataset.
Entrance settings	
Entrance name	The entrance can be specified more precisely via the name. Max. 29 characters
Activation time (s)	Entry in seconds defining how long the door remains unlocked after a positive check. Default = 7
Entry settings	
Entry as group only	A group is defined as two people. This ensures the dual control principle is used, as it is always necessary for two authorized people to scan their cards at these entrances for the door to be opened. Offers added security.
No time model or validity check	When this option is activated, only the general authorization for this entrance is checked — any restrictions such as time models or expiration dates are ignored. Offers reduced security.
Entrance activation	

Parameter	Description
Normal	Each authorized person is permitted to open the door for access purposes. If the **Manual long-term opening allowed** parameter is set and the card holder has the relevant authorization, long-term unlock is also possible.
Per time model automatically	Outside the time model = normal operation Within = long-term unlock For automatic locking, only the end times of the periods are set.
Manual long-term opening allowed	It is only possible to unlock the door on a long-term basis if this parameter is set and the card holder is authorized for this feature. A card with authorization must also be held to the door terminal reader for 5 seconds.

3.6.3 Offline locking system: Time models

The list field contains all time models that have been set up. The buttons above the list can be used to create further list entries , edit existing entries  or deleted them  .
The parameters for the entrance selected in the list are displayed in the fields to the right, where they can be entered and edited.



Parameter	Description
Time model	
ID	Assigned by the system when the list entry is created and cannot be edited. Sequential number that uniquely identifies the dataset. A maximum of 15 time models can be defined for the locking system.
Time model name	The time model can be specified more precisely via the name. Max. 29 characters
1. 1st period to 4th period	

Parameter	Description
starts ... ends	Start and end time of the period concerned. If only end times are specified, these time models can be used for automatic door locking.
valid on	Days of the week on which the period is valid are selected. Entries are selected by clicking on them with the mouse — selected days are shown in blue. Clicking again removes the selection.

Holidays

Holidays and special days are taken from the list in the online system.

In the **Special days** dialog, up to ten holidays can be selected for the offline system by activating the **active for offline locking system** parameter. Irrespective of the category given to the holiday for the online system or its activation status in that system, it can be used as a holiday in the offline system.

An activation for the locking system is independent of the use of the holiday in the access control system — this means that holidays deactivated for the online system can nevertheless be activated for the offline system.

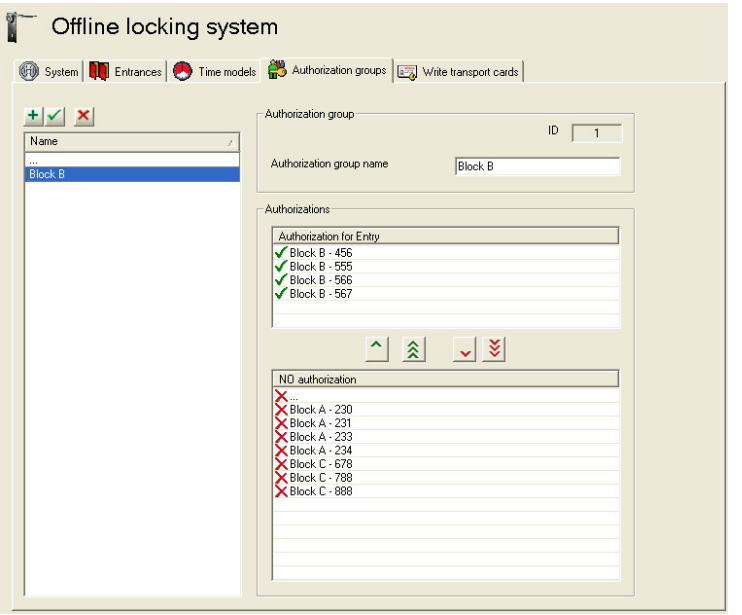
Time model vs time period

A time model can contain up to four time periods in one 24 hour day. Defining start and end times of a period means that a different regulation applies in this period (e.g. long-term door unlock) compared with the rest of the day. The periods can be as long as necessary and can overlap. If only end times are specified, this can be used for automatic door locking, but when allocated to specific persons, they have no access at all.

Each period can be allocated to any day of the week or holiday. The user is thereby responsible for ensuring that the period limits are set and allocated to the days in a logical and consistent manner.
The entirety of all time periods and their allocations to days makes up the time model, which can be used as an entity in the system.

3.6.4 Offline locking system: Authorization groups

The list field contains all authorization groups that have been set up. The buttons above the list can be used to create further list entries  , edit existing entries  or delete them  .
The parameters for the entrance selected in the list are displayed in the fields to the right, where they can be entered and edited.



Parameter	Description
Authorization group	
ID	Assigned by the system when the list entry is created and cannot be edited. Sequential number that uniquely identifies the dataset. The number of door groups that can be created is determined by the data size (, *page 17*) and corresponds to the data for **Maximum number of door groups** on the **System** tab.
Authorization group name	The authorization group can be specified more precisely via the name. Max. 29 characters
Authorizations	
Authorization for Entry	All entrances, allocated from the bottom list, for which access authorization has been granted.
NO authorization	All doors in the offline system that have been defined on the **Entrances** tab but have not been transferred to the top list.

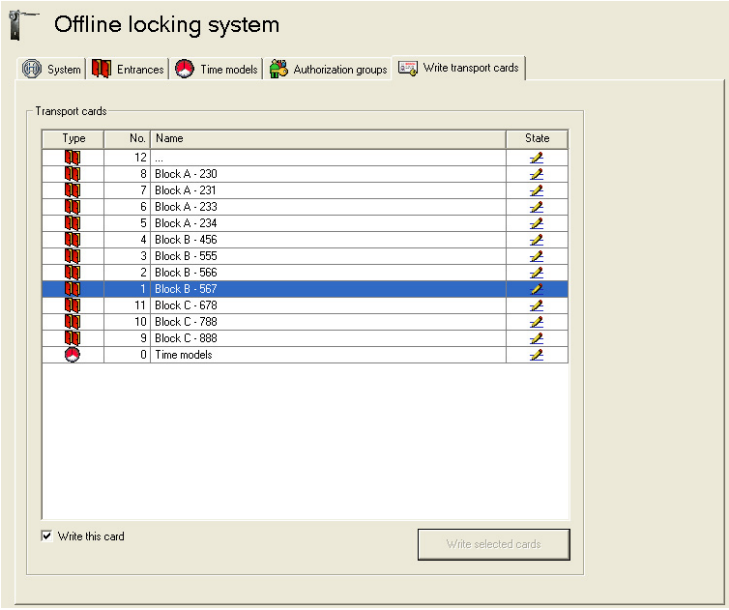
Individual selected entries can be added to ⌃ or removed from ⌄ the top list using the arrow keys between the two list fields; it is also possible to transfer all entries from one list to the other ⌃⌃ or ⌄⌄.

Notice!

The segmentation of cards allows only a relatively low allocation of individual doors in comparison with door groups. However, given that individual door authorizations are only used in special circumstances, that authorizations for certain doors are usually allocated by combining a number of doors together into a door group, and that it is also possible to form a door group containing only one door, the number of permitted individual door authorizations is sufficient.

3.6.5 Offline locking system: Write transport cards

In contrast to the online system, configuration data in the offline systems cannot be distributed via system components and transmitted to the relevant installations; instead, it must be brought to the devices via another route. In *System Overview, page 12*, various system cards have already been mentioned, including **door initialization** and **time model** cards, to which door parameter settings and time models are written and which are scanned at the door terminals.



Transport cards for doors (door initialization cards)
The list field on the **Write transport cards** dialog page contains one entry for each individual configured door. To facilitate selection and for the purposes of carrying out the write process, the doors for which transport cards need to be written are highlighted in the list after configuration. If the appropriate list entry is selected and the **Write this card** check box is activated (or if the list entry is double-clicked), these entries are assigned the icon in the **State** column and are therefore selected for the next write process. In addition to this identification mark, doors that have not been selected are shown grayed out.
The **Write selected cards** button is used to activate the dialog reader; this writes **a separate transport card for each door**.

Notice!
Please ensure that the necessary number of transport cards is available for the selected number of doors.

A dialog box prompts you to place the card in position and then shows the progress of the write process.
If door data has been written to the transport card that is currently in position, the user will be prompted to place a new card in position for the next dataset.

Notice!
Door data also contains information about the authorization groups to which this door belongs.

If several door initialization cards are used these should be clearly marked, so that data is assigned to the correct door. For this reason, the data on the card is deleted once the door initialization card has been scanned at the relevant terminal.

Transport cards for time models (time model cards)
There is also a list entry for the time model; this is always added to the end of the list. In contrast to the doors, the time models are combined together and all of them—up to 15—are written with the current time to a single card.
Accordingly, **all** time models are also scanned at **all** door terminals.

Checking the card type
Before the current card is written, the system checks whether it is actually a door initialization card. If the card has already been encoded in a different way (e.g. as a user or facility card), a warning to this effect is displayed.

3.6.6 Updating the date and time

In addition to the door and time model data, the current time stamp (date/time) is also written to the transport cards. Depending on the size of the facility being secured, there is a certain time delay before the cards can be scanned at the doors. The time delay will increase significantly with the number of doors to configure, particularly in the case of time model cards. In order to gain the most precise time data, above all for when cards are scanned, a **mobile read-write device** (timesetter) should be used. This unit allows the times to be updated on the transport cards immediately before scanning at the terminal, to ensure that the time delay remains within the tolerable limits.

Scanning the system card

1. The timesetter must first be initialized with the facility-specific data. To achieve this, it must be "christened" with a facility card once.
2. In addition to the door and time model data, the transport cards described above (door initialization and time model cards) also contain the current system time. These can be used to provide the timesetter with the time data.
3.
   - Place the system card (facility or transport card) on the read head of the device (gray field).
   - Press **1**.
   - Hold down **1** and press **2**.

Writing to the transport cards

Immediately before the transport cards are scanned, their time data should be updated — door and time model data remain unaffected.

- Place the transport card (door initialization or time model card) on the read head of the device (gray field).
- Press **2**.

Notice!
The write and read process is indicated by an LED display. For details on what the color sequences mean, please see *LED display signals, page 54*.

3.6.7 Booking cards

In addition to the transport cards for the doors and time models, other special cards are also used for data transfer in the offline system. These are called access or booking cards; these are used to copy recordings of access attempts from the door terminals and transfer them to the management system. Successful and unsuccessful opening attempts are saved in the door terminals. The last 800 bookings are saved in a ring buffer. These can be retrieved with special booking cards and entered in the database.
The different card types allow varying numbers of bookings to be written to one card: Hitag1 holds 32, MIFARE classic holds 244. You must therefore create sufficient booking cards and set up appropriate retrieval deadlines.

Reading the bookings on the terminal
The system card is held to the read unit of the corresponding terminal. While the LED shows orange, the terminal is writing data to the booking card. When the LED flashes green three times, the bookings have been successfully written to the card. If the booking card is removed during the terminal is writing, the data transfer will be interrupted.

Scanning booking cards
The cards with the transferred bookings are then scanned via the dialog reader and displayed in the **LogViewer** dialog.
The messages are automatically transferred to the log file and can be retrieved at any time in the same way as the online messages.

As the offline messages are listed together with the online messages in the standard view, a predefined filter in the toolbar of the  dialog can be used to restrict the view to just the offline messages.

Notice!
The data is deleted from the transferring unit:
When the terminal is read, its memory is erased.
When the booking card is scanned at the workstation, the card is erased.

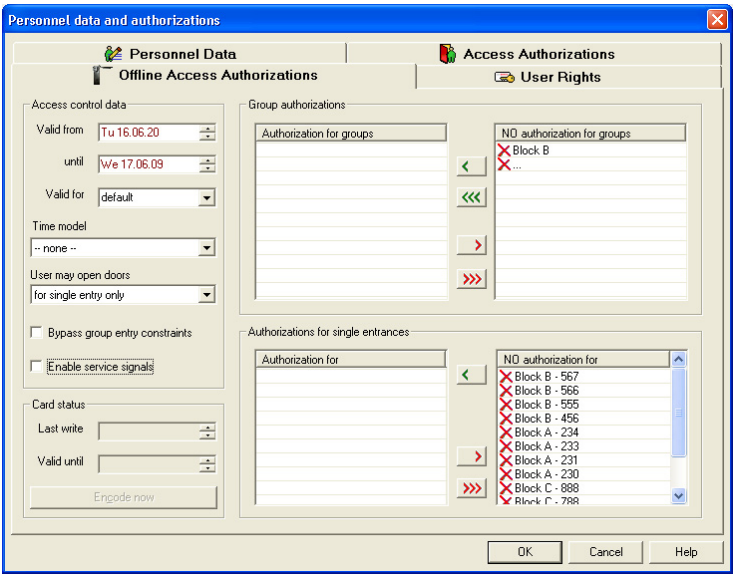
3.7 Managing Personnel Data

The database of the Access PE access control system is used to store personnel data for the offline system as well.
Accordingly this data is entered via the access control system dialogs.

Notice!
Each card holder for the offline system requires a valid card for the access control system (online system).

3.7.1 Description of dialogs

When the offline system is active (after the facility card has been scanned), the dialog for entering personnel and card data contains the additional page **Offline Access Authorizations**.
Here all personnel-related settings are configured for the locking system.



The four list fields on the right of the dialog are used to assign **Group authorizations** (top list fields) and **Authorizations for single entrances** (bottom list fields). The process of assigning and withdrawing authorizations is the same as the process for online access authorizations.

Notice!
Individual authorizations can only be assigned in line with the data size. The maximum number for each locking system can be found in the system data in Access PE Configurator.

Other settings for the offline cards are configured to the left of the list fields for access authorizations.
Access control data dialog field
– **Valid from ... until**

The card's general duration of use can be defined here. Extensions (Valid for) can be set up for no longer than the specified "until" date. The start date (Valid from) can be set as a date in the future, in which case the set extensions are only written to the card on this date.
If no entries are made, the card is valid indefinitely from the time of encoding.
The validity of assigned access authorizations, however, is regulated by the settings in the **Valid for** field. Only when the **end of validity** entry has been selected here is the "until" date also applied to the access authorizations.

- **Valid for**
  This field is used to define the extension periods for authorizations. It contains a list of predefined periods for quick selection, but other time data can also be entered. [Depending on the time unit, time periods of up to four years can be defined. If necessary, time data can be expressed in larger units, e.g. 14 days as 2 weeks].
  In addition to the time periods 1 hour, 1 day, 1 week, 1 month and 1 year, the list also contains the entries **default** and **end of validity**.
-
  - Default
    This is a predefined entry and corresponds to an extension period of two days.
  - End of validity
    This is used to extend the period to the general card validity period ("until" date) during the encoding process or the initial write process.
    Note: If no end date is set for use of the card, the card is extended indefinitely.
- **Time model**
  Selecting a time model restricts the use of the card to the defined time periods.

The only time models that can be selected are those that have been created in the dialog of the same name for the offline locking system in Access PE Configurator. Time models for access control (online system) cannot be used here.

- **User may open doors**
-
  - **for single entry only**
    Corresponds to a normal access authorization — depending on the authorization, the card holder may or may not open the door.
  - **long-term only**
    The standard access authorization does not apply for this card holder. He can only open correspondingly configured doors (**Manual long-term opening allowed** parameter) on a long-term basis by briefly presenting his card to the door terminal reader.
  - **both**
    Depending on his authorizations the card holder is able to unlock the door either long-term (by presenting his card to the reader for 5 seconds, provided the door in question has been configured appropriately) or for a single entry (by presenting the card briefly i.e less than 5 seconds).
- **Bypass group entry constraints**
  With this authorization selected, a card holder can access doors configured with **Entry as group only** on his own, i.e. override the group requirement.
- **Enable service signals**
  When the battery status at the door terminal is low, optical signals will only be displayed for users for whom this option is activated. This also allows the signaling to be restricted to people who are responsible for system repairs and maintenance.

Card status dialog field

– **Last write**
  The date and time of the last extension is displayed on the encoding reader of the workstation or on the write-capable reader.
– **Valid until**
  Expiration date (date/time) for access authorizations based on the last extension.
– **Encode now**
  Data for the locking system can be written to the user card via a connected encoding reader (Interflex - RWD).
  If the card is not available when setting up or changing the offline settings, the card will be rewritten the next time it is scanned at a write-capable reader.

3.7.2 Adding personnel data

People to be granted access authorizations for the locking system (offline system) must be added as records in the access control system (online system).
As the same card is used for both systems and access authorizations are extended for the offline system via (write-capable) readers (e.g. DELTA 7020) in the online systems, card holders must also have valid access authorizations for the access control system, in line with the **Write without access rights** parameter setting.

Prerequisites

In order to encode the cards at the workstation, you require an appropriate **dialog read-write unit**. This is connected directly to the workstation computer and set up via **Access PE Personnel Management**.

1. Connect the reader to the workstation.
2. Open **Access PE Personnel Management**.
3. In the **Tools** menu, use the **Properties** function to openthe **Change configuration** dialog.

4. Activate the **Dialog reader** check box.
5. In the **Reader** field, select the **Interflex USB Hitag, Mifare (IFRW)** entry.
6. Click **OK** to close the dialog.

You also require a write-capable reader (e.g. DELTA 7020) to extend the offline authorizations. This reader can be installed as an access control reader in the online system, e.g. at frequently used entrances (main entrance), and can be configured at the same time with write capabilities for the locking system; see also *Configuring the write-capable reader, page 19*.

Online data

For people who have not yet been created in the system, a record must first be added. To add personnel data and to assign authorizations for the access control system, follow the steps below:

1. Open **Personnel Management**.
2.
   - To add a new dataset, click  or open the **Persons > New person ...** menu and then go to the **Personnel data and authorizations** dialog.
   - On the **Personnel Data** tab, complete at least the mandatory fields with the data for the person in question.
   - Assign a card to the person.
3. Switch to the **Access Authorizations** tab.
4.
   - Assign the person the necessary access authorizations for the online system.

– If the **Write without access rights** (*Configuring the write-capable reader, page 19*) parameter is not activated for the write-capable reader, the access authorization for this entrance must also be assigned.

You can distribute the offline access authorizations immediately, without closing the dialog.

Offline data

If you wish to add to offline data for an existing dataset, or if you have closed the creation dialog when setting up a new dataset, you can open it either by double-clicking the relevant entry in the list of available items or by selecting the entry and clicking the  button.

Notice!

Only people with a valid card for the access control system (online system) can be assigned authorizations for the locking system (offline system).

1. Switch to the **Offline Access Authorizations** tab.
2. Assign the person the necessary authorization groups and individual authorizations.
3. Enter any use restrictions (validity dates, validity period, time model etc.).
4. Place the card on the dialog reader.
5. Click the **Encode now** button to encode the card.
   The **Last write** and **Valid until** fields are populated with the relevant dates.
   [If the physical card is not available, encoding is automatically carried out the next time it is scanned at a write-capable reader].
6. Once encoding has been successfully completed, click **OK** to close the dialog.

Data check during write process

When the **Encode now** button is clicked, a dialog box appears prompting you to place the card on the read-write unit.

The following circumstances result in error messages and in the termination of the write process.

– No card is place on the unit or the code data cannot be read.
– The card is not a user card.
– The card does not belong to the selected person.

Display of the validity period indicates that the write process has been successful.

3.7.3 Changing data

Any changes made to offline data (extensions or reductions of access authorizations, new extension cycles etc.) are distributed to the controllers, as with online data. The next time the card is scanned at a write-capable reader, the changed data is transferred to the card.

Notice!

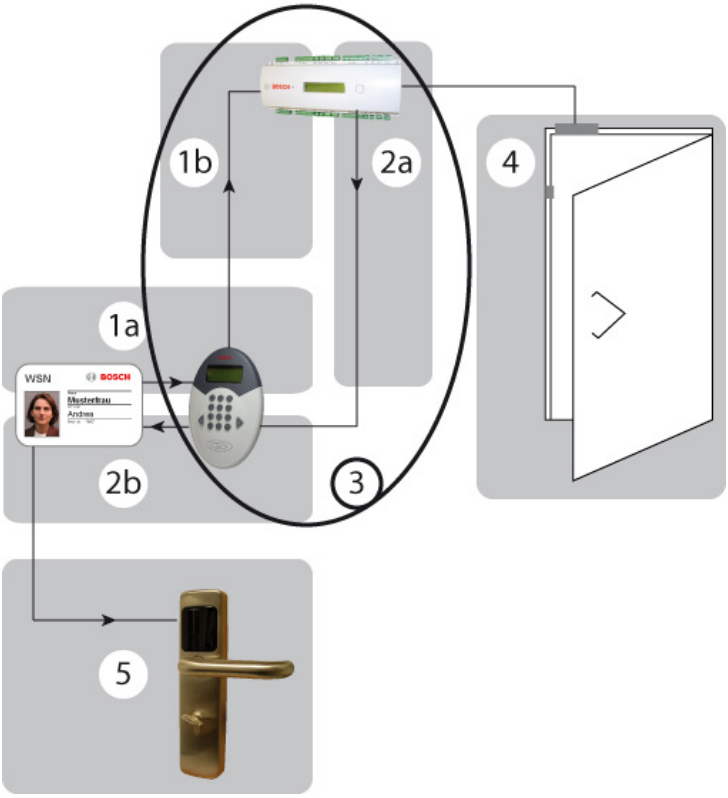
Certain online data can also have an impact on offline authorizations.

For people who are blocked in the online system, all offline data will be deleted from the card during the next read/write process.

3.8 Description of Procedures

The following procedural descriptions are intended to provide a brief overview of the required steps and processes, with a view to demonstrating and explaining the peculiarities of offline systems — in particular in connection with access control systems (online).

3.8.1 Access



1a Card read

1b Card number sent to the AMC

2a Current data shared with the reader

2b Current data written to the card

3 For details on the checking and write process on the AMC, please see the flow diagram in *Write process, page 48*.

4 Door release for the online system (if configured)

5 Authorization check at door terminals

3.8.2 Write process

In the majority of cases write processes are used to extend access authorizations by the amount of time specified.
For this reason, the last write date is also stored in the database. The need for extension is determined by means of a comparison with the current date or the current time. However, as this would mean that expiration data would be updated every time the card is scanned, a write process would also need to be carried out each time. To avoid unnecessary waiting times and delays at read-write units, a validity period is used to determine a point in time until which the card data is considered valid. Data is only updated when a third of the validity period has expired.

Example
Validity period: 1 day = 24 hours
1/3 of the validity period: 8 hours
If a card holder scans the card when he starts work and his expiration date is updated, he can pass the read-write unit during the subsequent eight hours without a new write process being triggered — the data is only updated at the end of the eight hours.
Tip: If the validity period in the example above is doubled (= 48 hours), the updating period increases accordingly (= 16 hours). This ensures that the validity period is only updated once a day.

3.9 Application Examples

The following examples demonstrate how the system can be set up for special requirements or events via the relevant parameter settings. The examples are restricted to one specific element. Other variations can occur when a combination of parameter settings is used. The examples can also be combined with each other accordingly.

Access control reader and/or write-capable reader?
The decision regarding the way in which the write-capable reader is used depends on a number of different factors; it can make sense not to integrate the reader into the access control system (online).

- Is there an entrance (e.g. main entrance) that must be passed by most of the card holders?
-
  - **Yes**: A write-capable reader with simultaneous access control function for the online system is recommended.
  - **No** (There are a number of possible entrances, for example): The use of write-capable readers at each entrance would not be recommended for cost reasons. In this case, the reader (or possibly two readers) should be installed in the most frequented area as a simple recharging station.
- Should extensions of authorizations be possible at all times?
-
  - **Yes**: We recommend the use of a write-capable reader (with or without access control function) in the most frequented area.
  - **No** (As a rule, fixed expiration dates are used): If the read-write unit at the operator workstation is not enough, any write-capable reader will suffice for these special extensions.

Example 1: Read-write unit only
Ideally a hotel should be accessible to everyone, at least as far as the reception desk. For this reason, access control readers are predominantly installed at doors that require particular security, in the event that the settings in the second example in *Single doors or door groups?, page 52* are not sufficient.

Accordingly, the write-capable reader is not linked with access control functions; instead, it is configured purely as a read-write unit for the offline system.

Requirements:

The **Reader function** reader parameter must be set to **Write locking system** and the **Only write card** parameter is activated (= checked).

The write-capable reader need only be installed in a central location for hotel personnel, so that their rights can be updated and extended. If possible, choose a position that all relevant people pass on a regular basis, e.g. staff room.

For hotel guests, authorization for the hotel room door is assigned in accordance with the room booking and written to the card via a write-capable reader at reception. Authorizations do not normally need to be changed, but this is carried out at reception if required; the reader does not need to be installed in a freely accessible area.

Example 2: Read-write unit with access control function

Student residences: Here, only residents must be allowed access. One access control reader for the main entrance can secure the building against unauthorized access. One write-capable reader can update and extend rights for the locking system for authorized people at the same time.

Requirements:

The **Reader function** reader parameter must be set to **Write locking system** and the **Only write card** parameter is deactivated (= unchecked).

If the **Write without access rights** parameter is not set (checked), only people with access authorization (online) for the main entrance will have their offline rights updated and extended.

Single doors or door groups?
Each door created in the system can be assigned as an individual authorization and belong to any number of door groups. The following examples are intended to demonstrate how these two types of authorization should be handled.

Example 1: Hotel
At reception, the validity period for the room in question is assigned as an **individual authorization** in accordance with the booking. It is also possible, for example, to assign another door group containing all general-use areas (restaurant, breakfast room, sauna, sports facilities etc.), provided that these areas are secured by terminals.
In contrast, hotel personnel are assigned a **door group** containing all (or at least most) doors.
Requirements:
The **Check door groups** parameter must be selected.
Procedure:
The guest can open the door to his room, in line with the assigned individual authorization, and can also open all doors in the door group. Hotel personnel are able to open all doors in the assigned door group, which also includes all doors to the guest rooms.

Example 2: Areas within the offline system that are subject to increased security requirements and may only be accessed by certain people.
The authorized people are assigned these doors as individual authorizations. It is irrelevant whether these doors belong to door groups and it is also irrelevant to whom these door groups have been assigned.
Requirements:
The **Check door groups** parameter must be cleared (unchecked).
Procedure:

Only individual authorizations are accepted at the doors. People who are only assigned door group authorizations for these doors will not be granted access.

Normal or long-term unlock
If the card is valid, the LED on the terminal flashes green three times. The door is unlocked for a set door opening time (the default is 3 seconds). If the door is in **Long-term unlock** mode, the LED again flashes green three times when a valid card is presented.
A card with permission for **single entry** can only open the door for single entry. A card with **long-term unlock** function immediately activates long-term unlock (no five second presentation necessary). Cards that are authorized for **both** can be used for normal opening if the card is removed during the three flashes. If, instead, the card continues to be presented to the terminal's read unit (> five seconds), a continuous green signal is displayed and the door remains unlocked until a card with **long-term unlock** [**both**] authorization is presented to the terminal (for at least five seconds). The door is then locked; i.e. access is only possible with authorized cards.
Requirements:
The **long-term unlock (Toggle)** parameter must also be selected (checked) for the terminal.

By time model:
The same function can be controlled via a time model. A time model is selected for the **Opening time model** door parameter and the door is unlocked ("from time") or locked ("until time") on a long-term basis in line with the specified time periods. Time models containing only "until times" can be used to lock doors which have been unlocked long-term.

Notice!
Unlocks governed by time models always contain the risk that unsupervised areas could be made freely accessible.

Examples: Office buildings with public access

1. **Manual long-term unlock/lock**
   The office is unlocked each morning using the long-term unlocking function and made accessible to the public. When the office closes, long-term locking is carried out, meaning that only people with a valid card can access the office during this time.
2. **Long-term unlock/lock controlled via a time model**
   If the public visiting hours are not the same as the staff hours, door opening and closing can also be controlled via a time model.
   Personnel hours: 8:00-12:00 and 13:00-17:00
   Public visiting hours: 9:00-11:00 and 14:00-16:00
   To correctly comply with the hours and avoid the need for manual unlocking/locking, a time model can be used with two periods that correspond to the public visiting hours.
3. **Long-term locking controlled via time model**
   The office is unlocked manually each morning by the first associate to arrive, using the long-term unlocking function. A time model without start times is used to initiate long-term locking at a certain point in time.

3.10 LED display signals

Signals for user cards

Door opened with single-unlock function

Meaning	The door is unlocked with a single-unlock card. This message also appears if the door is already unlocked on a long-term basis.
Booking entry	**access, single door permission** or **access, door group permission**

Door opened with long-term unlock function

Meaning	The door has been unlocked by long-term unlock card, or by time model.
Booking entry	**Door unlocked**

Door closed with long-term unlock function

Meaning	The door has been locked by long-term unlock card, or by time model.
Booking entry	**Door in normal mode**

Battery change request

Meaning	Red LED signal of one to three seconds' duration. As long as the battery is not completely empty, a card-specific signal will follow. If the batteries are empty, no further signal will be displayed and no bookings will be possible. The battery change request is only displayed for user cards.
Booking entry	The **battery voltage too low** entry is shown after every 25 bookings.
Solution	Replace batteries.

Special signals

Read-write confirmation for system cards

Meaning	A system card was successfully read or written.
Booking entry	**Initialization**

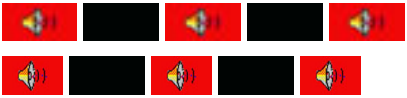
No card in range

Meaning	The electronics have been activated, however no card was recognized in front of the reader.
Booking entry	<No entry made>
Solution	Present the card to the reader again.

Read/write error

Meaning	It was not possible to read or write to a system card successfully.
Booking entry	<No entry made>
Solution	Present the system card to the reader again.

Invalid authorization

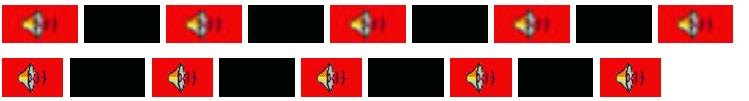


Meaning	The card has no valid authorization.
Booking entry	**Access denied, card status blocked**, **Not authorized**, **Access denied, card expired** or **Access denied, outside time model**
Solution	If necessary, change the authorization for this card.

Time invalid

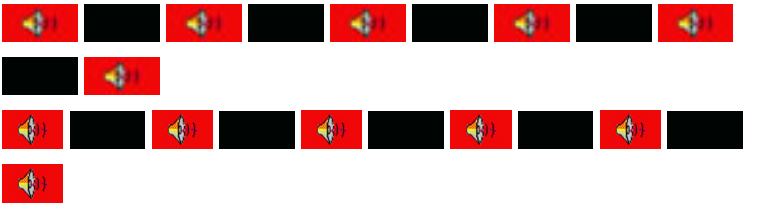
Meaning	The terminal does not know the current time.
Booking entry	<No entry made>
Solution	A time initialization card must be created and scanned at the terminal.

Door initialization missing



Meaning	The terminal has not been initialized.
Booking entry	<No entry made>
Solution	A door initialization card must be created and scanned at the terminal.

Facility data missing



Meaning	The terminal has not been initialized for this facility.
Booking entry	<No entry made>
Solution	The terminal must be initialized with a facility card.

Data transmission

Meaning	The LED lights up orange while data is being exchanged between a system card and a terminal. The duration depends on the volume of data to be transferred. The read/write process is then signaled.

LED displays for mobile read-write device

Write-confirmation for time model cards

Meaning	Data has been successfully written to time model card.

Read-confirmation for the time model card

Meaning	The time model card has been successfully read.

Read-confirmation for facility card

Meaning	The facility card has been successfully read.

Read/write error

Meaning	It was not possible to read or write to the system card successfully.
Solution	Hold the system card to the reader again.

Facility data missing

Meaning	The timesetter has not been initialized for this facility.
Solution	The timesetter must be reinitialized with the facility card.

Time invalid

Meaning	The timesetter does not know the current time.
Solution	An appropriate time initialization card must be created and the timesetter must be synchronized.

Key:

- LED signal lasting one second.

- LED signal lasting up to three seconds.

- green LED

- red LED

- orange LED

- additional acoustic signal

- additional acoustic signal

- signal interrupted

Bosch Access Systems GmbH
Charlottenburger Allee 50
52068 Aachen
Germany
www.boschsecurity.com