Access Engine (ACE)

en Operation Manual

Table of contents

1 Introduction

1.1 Foreword

In its capacity as an access control system, the Access Engine provides dialogs for data acquisition and data modification as well as the necessary features for ID card creation and individual layout presentation. In addition to this, the Access Engine also controls and monitors its own system components. These different tasks and activities can be carried out on specially set up workstations independently of the actions of other users.

1.2 How to use this Help File

This help file will assist you with the Access Engine operation. The following information explains how to use this help file.

Tool bar buttons

Button	Function	Description
	Hide	Click this button to hide the navigation pane (Contents, Index, Search, and Favorites tabs). leaving only the help pane visible.
	Show	When the Hide button is clicked it is replaced by the Show button. Click this button open the Navigation pane.
	Back	Click this button to move back through the chain of topics most recently viewed.
	Forward	Click this button to move forward again through the same chain of topics
	Print	Click this button to print. Choose between “Print the selected topic,” and “Print the selected heading and all subtopics”.

Tabs

Contents Tab: This tab displays the help file topics in a book-oriented table of contents format. Click a book icon to open it and then click on a topic icon to view the topic.

Index Tab: This tab displays the index terms in alphabetical order. Select a topic from the list or type in a keyword to find the topic(s) containing that keyword.

Search Tab: Use this tab to find a keyword. Enter a keyword in the field and then click the **List Topics** button to display topics that contain the specified keyword.

Favorites Tab: Use this tab to maintain a list of your favorite topics for quick access. Click the Add button to add the current topic to the list. Select a list item and click Remove to remove the item from the list.

Links

Jump Link: This link type brings you to a new topic page. For example, click this link to learn to create personnel data.

Help Window Dimensions

Adjust the size of the help window by dragging the corner or edge of the window to the desired size.

Using the Online Help

In addition to the standard delivery, the access control system Access Engine can be extended by numerous modules which can be activated according to customer requirements. The Online Help therefore describes all orderable extensions as well as the standard delivery dialogs and equipment.

Depending on the components installed and the user's rights not all extensions described may be accessible in the dialog system

Division capability

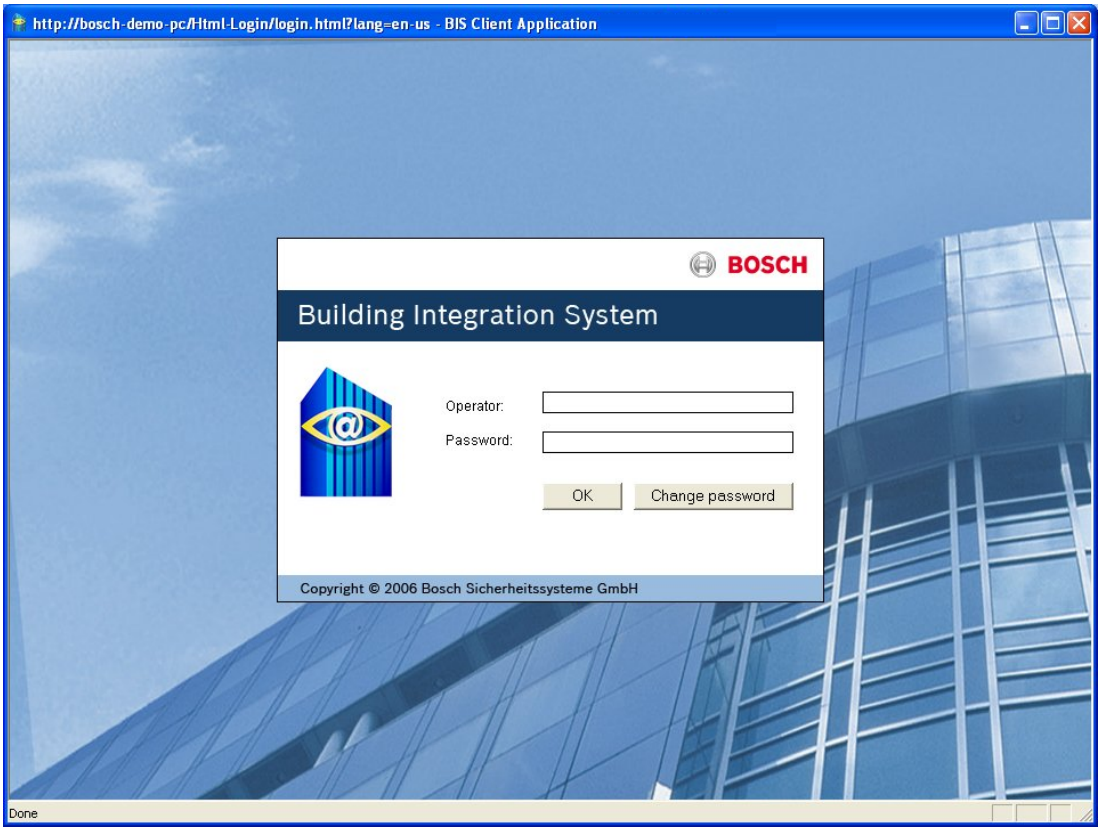
Although the division capability is shared by many dialogs it is not described there but in a separate chapter (see “Technical Data”) for the following reasons:

– Depending on license keys divisions may be disabled. In this case the division controls are not shown in the dialogs.
– Because the capability is shared it is best documented centrally to avoid describing the same functionality for each dialog.
– The divisions topic is complex and would affect readability of dialog documentation if included there.

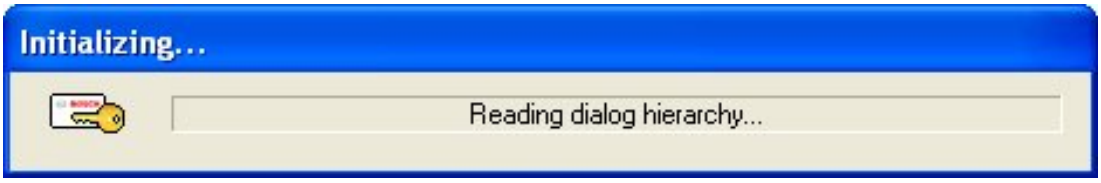
2 Starting the system

2.1 Starting the workstation

The Access Engine dialogs and reports are available via the BIS client application. Run the BIS client by opening the address **http://<servername>** in an Internet Explorer window, where <servername> is the computer name of the BIS Login Server.
If necessary, the BIS client installs or updates its internal components on the local workstation. Then it shows the BIS logon dialog.



Log on with an authorized operator's name and password. The main page of the BIS client will appear
To open the dialog manager of the access control system, just click the Access Engine button. Permissions are checked briefly and the dialogs are grouped together using the user and workstation profiles. The dialog manager then makes the menus and dialogs available.

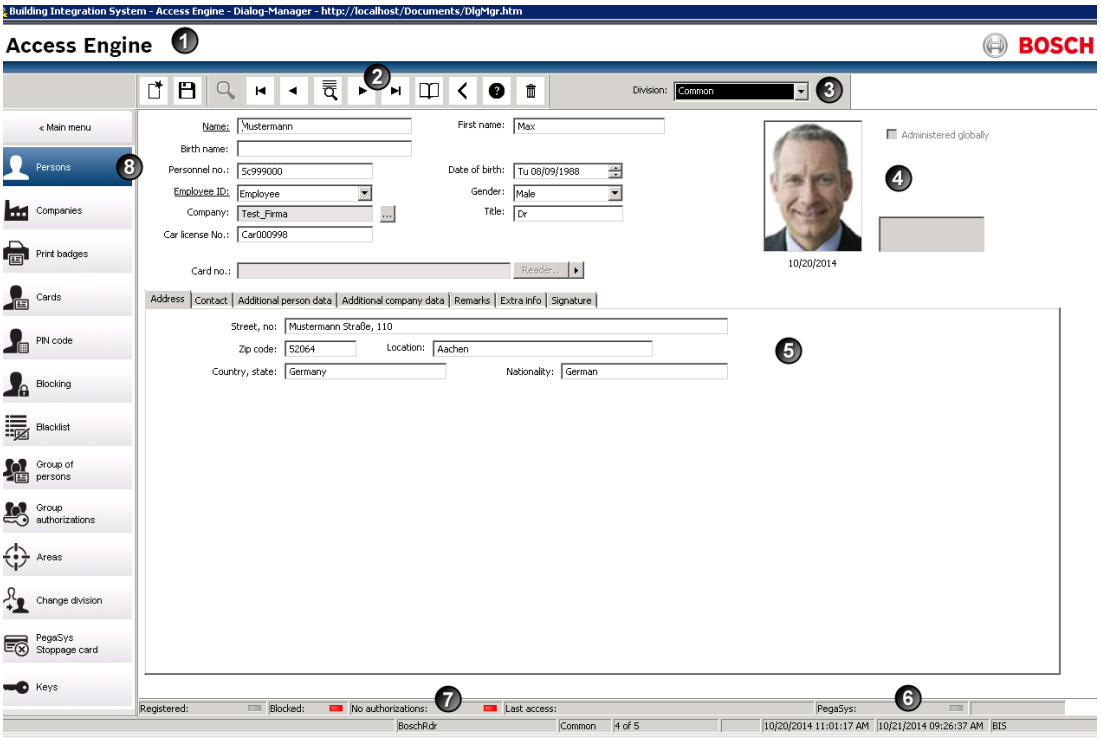


3 Operating the system

3.1 General creation and editing of data

3.1.1 Construction of the dialog system

The following figure is an example for an application of the dialog manager with running dialog.



Item	Description
1	Title Bar
2	Toolbar
3	Division Selection
4	Dialog header
5	Dialog field
6	Stautsbar
7	Statusbar
8	Dialog bar

The biggest part of the window of the dialog manager takes in the dialog field in which only one subordinated dialog may be displayed in each case. With the aid of the  -button in the title bar the dialog manager is closed.
The lower status bar in the lower part of the dialog mask is used for the representation of different information:

1. Displays of the selected **type** for data capture
2. Only if division mode is active: displays the selected **division**
3. **Current number** of the displayed record in the search list
   Number of selected records which the search list contains
4. "**Changed**", if an input has taken place
5. **Date** and **Time** of generation of the displayed record
6. **Date** and **Time** of the last change of the displayed record
7. Last **Editor**

The status bar above is only displayed in the personnel data dialogs.

3.1.2 The toolbar

The toolbar contains various buttons that offer shortcuts to most of the menu functions. The above figure shows the standard buttons that feature in most dialogs

Icon	Function	Description
	New	Removes current data from the dialog to prepare the dialog for the entry of new datasets or new search criteria.
	Save	Saves the data entered by the user when changing an existing dataset or creating a new one.
	Search	Searches for data. To use this function, any existing data must first be removed using the **New** button. Click the **Search** icon. A list will appear containing the records that have been found. The first of its datasets will be shown in the dialog.
	First	Jumps to the first record in the search list.
	Previous	Jumps to the previous record in the list.
	Search list	Opens the search list that was previously created using the **Search** command. The user can double-click each entry in the search list to open that record.
	Next	Jumps to the next record in the list.
	Last	Jumps to the last record in the list.

	Back	Returns to the dialog that was displayed before the current dialog. When clicked repeatedly, this takes the user back through each individual dialog.
	Help	Opens help files.
	Delete	Removes the record from the database.

The following are additional buttons that are only used in a few dialogs:

Icon	Function	Description
	Copy function	Copies the current record to a new record.
	Event log	The data of the selected person are send to the Event log as predefined filter criteria.
	Preview	Displays the print view of a report.
	Print	Prints a report or a visitor certificate.

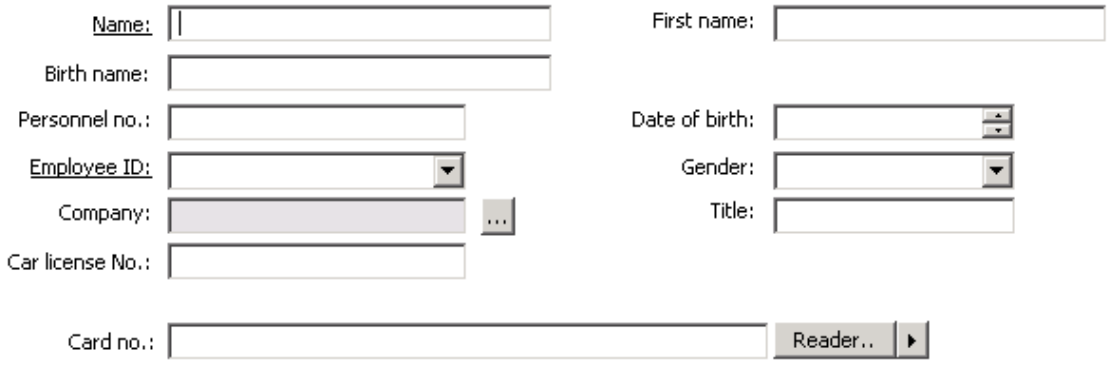
3.1.3 Behavior of data fields in the dialog manager

Three different procedures must be taken into account with data processing:

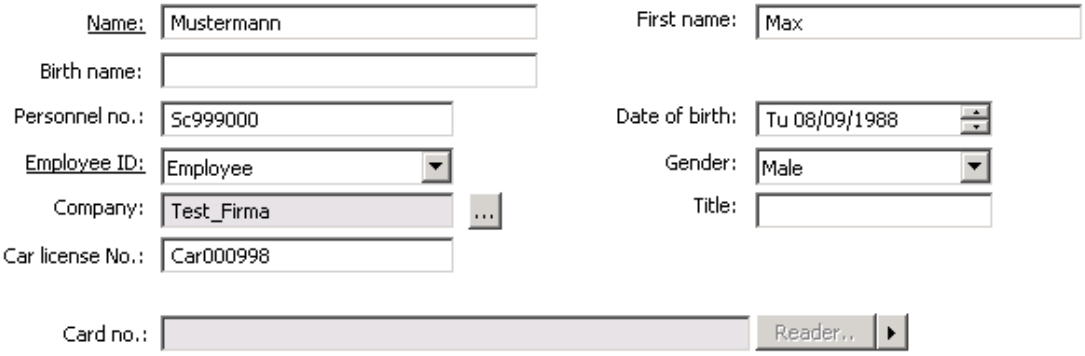
1. Selecting saved datasets
2. Changing an existing dataset
3. Creating a dataset

Data selection

A saved dataset may only be selected with cleared masks. This status is reached by clicking the  button in the toolbar. Search criteria can be entered in all fields with **blue** labeling.



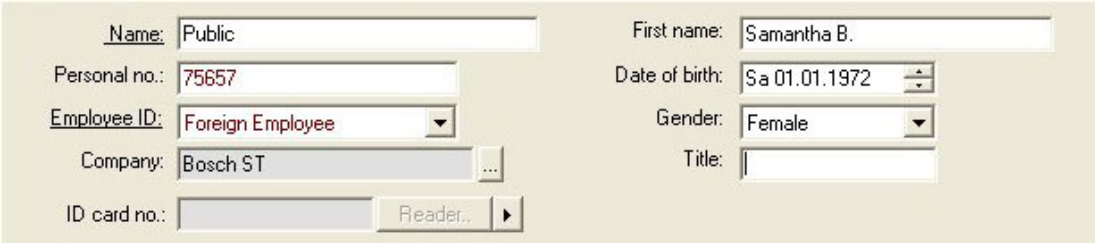
The search process is started by clicking the  button in the toolbar or by pressing the ENTER key. The first dataset that fits the search criteria is set. If more than one dataset is found, the search list is also shown automatically to select the desired dataset.



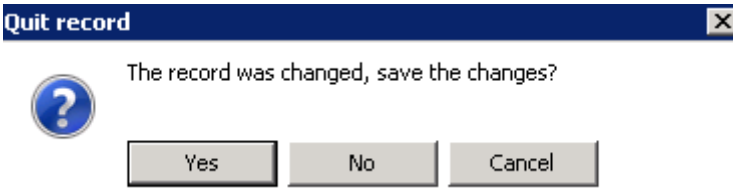
Data changing

If an **existing record is changed**, the dialog manager and the input fields behave as follows:

– the labeling of the input fields is **black**
– all changed data are marked in **red**



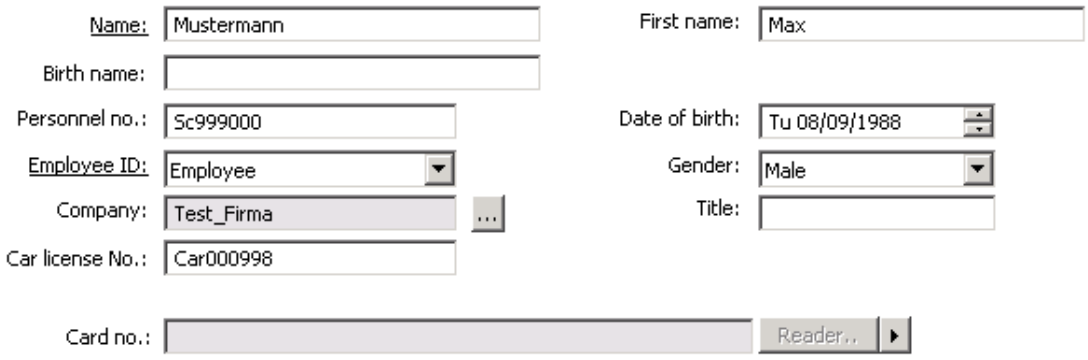
If an attempt is made to switch the dataset or dialog without saving the changes, the dialog manager asks for the changed dataset to be dealt with.



A choice can be made between saving the changes (Yes), discarding the changes (No) or canceling the switch to another dataset or dialog (Cancel).

New data record

It is also only possible for new records to be created with cleared masks  . In contrast to the searching process, data may be entered in all activated fields - independent of the labeling color (the field ID card no. in the personnel data dialogs is an exception - see Creating new data section). At least the underlined fields must contain entries.
All data that has not yet been saved is marked in **red** - as when changing data.



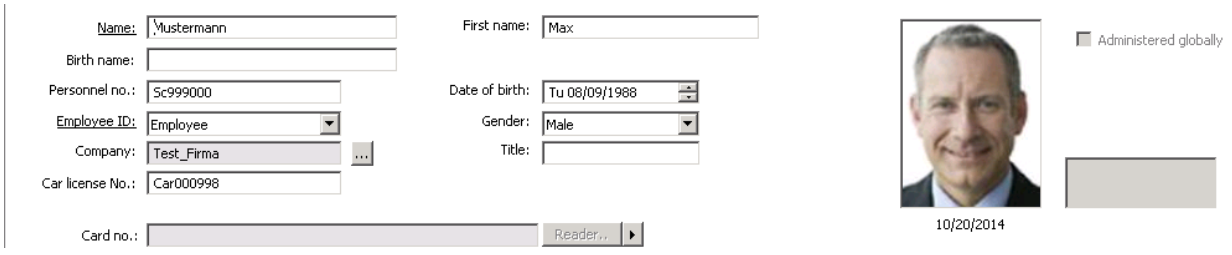
The entries **must** be saved by clicking the  button - pressing the ENTER-key activates the search function and the following message would be displayed:

Notice!

After clicking the  button, it is possible to select saved datasets and create new ones in the dialog manager. Since the default setting activates the search function, failure to save a new dataset is not registered if fewer than three fields have been changed. The dialog manager switches to another dataset or dialog without notification and all data that has been entered is lost as a result.

3.1.4 Person-related dialogs

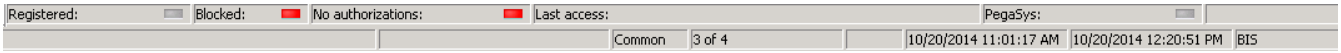
In addition to the general dialog elements of the toolbar, dialog bar and status bar, all person-related master data dialogs are made up of three other dialog elements.
In the common upper area (dialog header) are general declarations to the person as for example last name, first name and date of birth. Data that has been selected once is transferred from the other dialogs to the personnel data dialogs, which therefore allows a dataset to be processed completely and continuously.



The following dialogs use this dialog header, which enables them to transfer selected personnel data including the search list:

- Menu Personnel data
- Persons
- Print Badge
- Cards
- PIN Code
- Locking
- Area
- Black List

A variable part (dialog field) follows which offers other input options (e.g. recording ID cards or setting blocks) depending on the dialog functionality.
In addition to the general status bar, there is another status bar in the lower area in which current data concerning the person displayed is shown. The image below shows a view of the status bar with a selected person.



This shows the following information at a glance:

- This person has been assigned a card and is therefore **registered** or unregistered, i.e. this person does not own an ID card.
- The person is **blocked** otherwise
- The person's access authorizations are either **currently not valid**, i.e. the access authorizations have not yet begun or they have **expired**, i.e. the valid-until date has passed - active access authorizations: .
- The person was specified for **random screening** (flashing), otherwise - at the same time a block entry is generated and the **blocked** label is set to red.
- The date and time of the person's last access, i.e. the last ID card identification by a card reader is additional information that can be configured to appear:

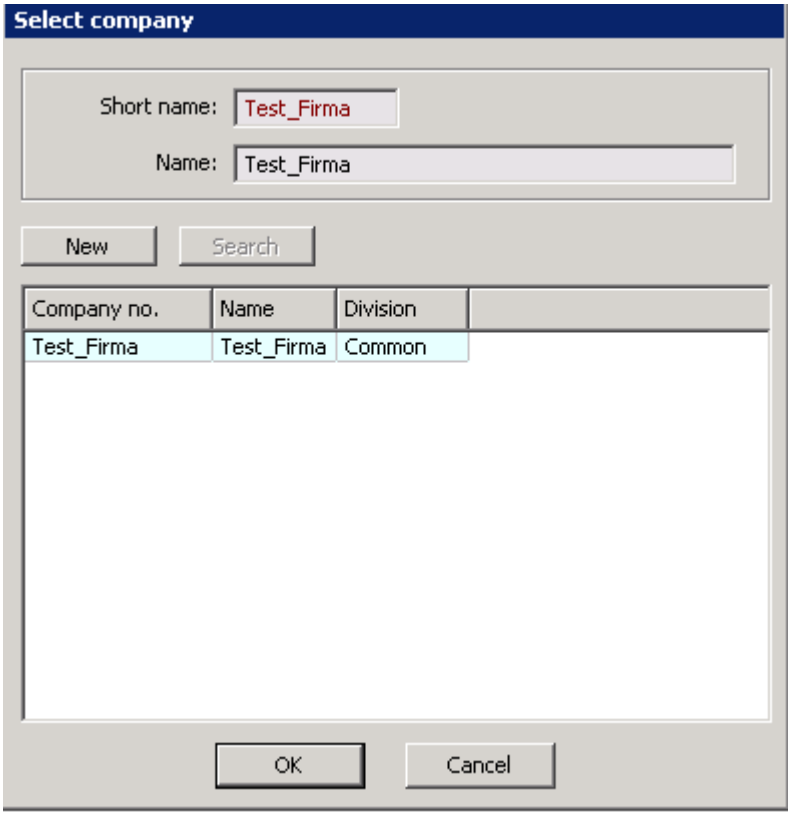
  Last Access: 22.06.2006 10:50:13

3.1.5 Company selection in the personnel data dialogs

Depending on the size of the system the selection of company datasets may be set up differently. The standard delivery offers a selection dialog to guarantee a quick Search especially for many data records.
In this case, the company entry field is grayed out

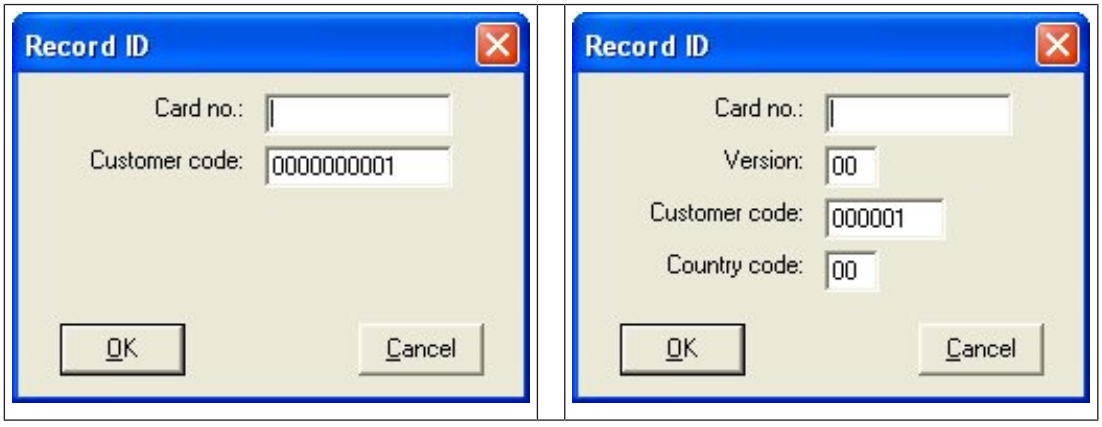
and the selection is made by clicking the 

button on the right-hand side of the display field in the dialog header. Once the search criteria has been entered in the **short name** and/or **name** fields and the **Search** button has been clicked, a selection box will open displaying a list of the appropriate existing datasets from the database. The desired dataset is selected in the list and transferred to the display field in the dialog header by clicking the **OK** button.



3.1.6 Selection Using ID Card Number

An assigned ID card number may also be used as a selection criterion. This requires a workstation that is equipped with a card reader or configured to allow entering the card data manually. Click the Reader button to the right of the ID card no. field and scan the card at the card reader to quickly find the holder of that card. Alternatively, if the workstation is configured for entering card data manually, one of the following dialogs appears - the dialog variant displayed depends on the ACE card definition being used.



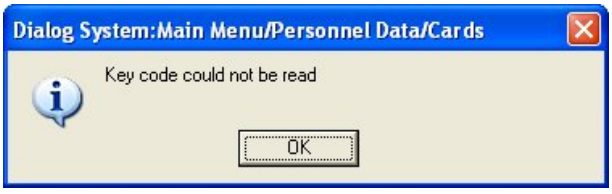
Using the card number data, the relevant dataset can now be selected. To do this, the numbers printed on the card can be entered without the preceding zeros. Other than the version number, the other data does not need to be adapted as a rule.
At dialog stations with ID card readers, another button is located next the **Reader...** button. This allows you to switch from manually inputting the card number to using the connected reader, so that the user can also initiate a person search by scanning an ID card.

Notice!
In contrast to the manual input the automatically selection needs the physical card in present. If the card isn't present, the user can always switch to manual input.

If the appropriate reader type is selected, the switch also appears in the lower status bar.

The **Reader** button is clicked to open the following dialog. The ID card must be held close to the reader and card holder data appears in the dialog mask described above.

The progress bar shows how much longer the ID card must be held near the reader. If the time passed without the ID card being read, the following note appears:



3.1.7 Editing Personnel Data

By clicking the button, the entries are saved in the relevant database tables and can also be used immediately in other dialogs.
All changes to this personnel data and the deletion of a person-related dataset can only be performed in this dialog, because in contrast to the other personnel data dialogs, the input fields remain active after the selection. The and buttons in the other dialogs, which transfer the personnel data, therefore also only relate to the contents of the dialog fields or to connections of personnel data with system data, but not to the personnel data itself.

Persons created via the Persons and Visitors dialogs can be selected in all dialogs with the dialog header and then transferred as described in construction of the personnel data dialogs section.
To select certain persons or person groups by means of entries in one or several input fields, any existing entries must be deleted by clicking the  button. At the same time, the input fields are activated and new entries are enabled (the dialog fields are active the first time the dialog is opened). This allows every single field input or any possible combination to be selected.
Except for the **Employee ID**, **Company** and **Gender** fields, which are list fields and therefore offer a choice of possible inputs, it is sufficient to enter partial data in the other input fields (e.g. one or several letters of a name, single figures from the personnel or card number etc.).
Once the selection criteria have been defined, the  button is clicked or the enter key pressed to start the search process. The first dataset that fits the specifications is entered. The number of other available datasets is displayed in the lower status bar and the list of persons can be called up via the  button.

Notice!
The maximum number of selected data records is limited to 1000. If you can't find the expected dataset in the search list, repeat the search with other or more criteria.

3.1.8 Selecting data in the dialogs

Single and multiple selection

Single selection		Single left-click
Multiple selection	consecutive elements	Hold the **Shift** button down and left-click the first and the last list entry of the selection.
	multiple non-consecutive elements	Hold the **Ctrl** button down and left-click the desired elements.

Assignment and reassignment
Some dialogs contain two columns, one with items that are available for assignment, and one with items currently assigned. Double-click items in either list to transfer them to the other list.

Sorting
Click any column header to sort the table by that column.
Click the header again to reverse the order of sorting.

Date (cur. year)	Description	Day model
Mon 25.12.2006	Christmas Day	DMAC-Holiday
Mon 09.10.2006	Columbus Day	DMAC-Holiday
Tue 04.07.2006	Independence Day	DMAC-Holiday
Mon 04.09.2006	Labor Day	DMAC-Holiday
Mon 16.01.2006	Martin Luther King Jr. Day	DMAC-Holiday
Mon 29.05.2006	Memorial Day	DMAC-Holiday
Sun 01.01.2006	New Year	DMAC-Holiday
Mon 20.02.2006	Presidents' Day	DMAC-Holiday
Thu 23.11.2006	Thanksgiving Day	DMAC-Holiday
Sat 11.11.2006	Veterans' Day	DMAC-Holiday

Date (cur. year)	Description	Day model
Sat 11.11.2006	Veterans' Day	DMAC-Holiday
Thu 23.11.2006	Thanksgiving Day	DMAC-Holiday
Mon 20.02.2006	Presidents' Day	DMAC-Holiday
Sun 01.01.2006	New Year	DMAC-Holiday
Mon 29.05.2006	Memorial Day	DMAC-Holiday
Mon 16.01.2006	Martin Luther King Jr. Day	DMAC-Holiday
Mon 04.09.2006	Labor Day	DMAC-Holiday
Tue 04.07.2006	Independence Day	DMAC-Holiday
Mon 09.10.2006	Columbus Day	DMAC-Holiday
Mon 25.12.2006	Christmas Day	DMAC-Holiday

3.1.9 Saving, editing and deleting personnel data

By clicking the  button, the entries are saved in the relevant database tables and can also be used immediately in other dialogs.

Special behavior of the ACE database

Each data record, which is saved in the database, gets an identification number (ID) from the system. This ID is built with the current date and time stamp and guarantees that the data record is unique. Deleting a record and recreating it with the same data creates a new record that has a new ID and is unrelated to the deleted record.

Example:

A dialog user with the user name Smith will be determined in the system by his unique ID, only. All message belonging to this user will be managed using the user ID. If the user Smith is deleted and will be created new, the new one gets his own unique ID and is a new record in the system. Messages belonging to the old user cannot be displayed to the new one.

3.1.10 Behavior of Time models

Time models related to persons will be checked only if the default state of the reader parameter **Check time model upon access** didn't change.

Because time models can be assigned to several system components, it is possible that two or more time models working together. Therefore note the following rules working with time models:

– If a person gets authorizations with time models for certain entrances, the time model will be ignored.

Example:

A person gets the following authorizations:

– Entrances A, B, C, and D with a time model valid from 9 a.m. until 5 p.m..
– Entrance B and D without time model.

The person gets access for the entrances A and C between 9 a.m. and 5 p.m. and for the entrances B and D without a limit.

– If a person gets with the same entrances but different time models the sum of the time models will be used.

Example:

A person gets the following authorizations:

– Entrances A, B, C, and D with a time model valid from 7 a.m. until 1 p.m..
– Entrances B, D, E, and F with a time model valid from 9 a.m. until 17 p.m..

The person gets access for the entrances A and C between 7 a.m. and 1 p.m., for the entrances B and D between 7 a.m. and 5 p.m., and for the entrances E and F between 9 a.m. and 5 p.m..

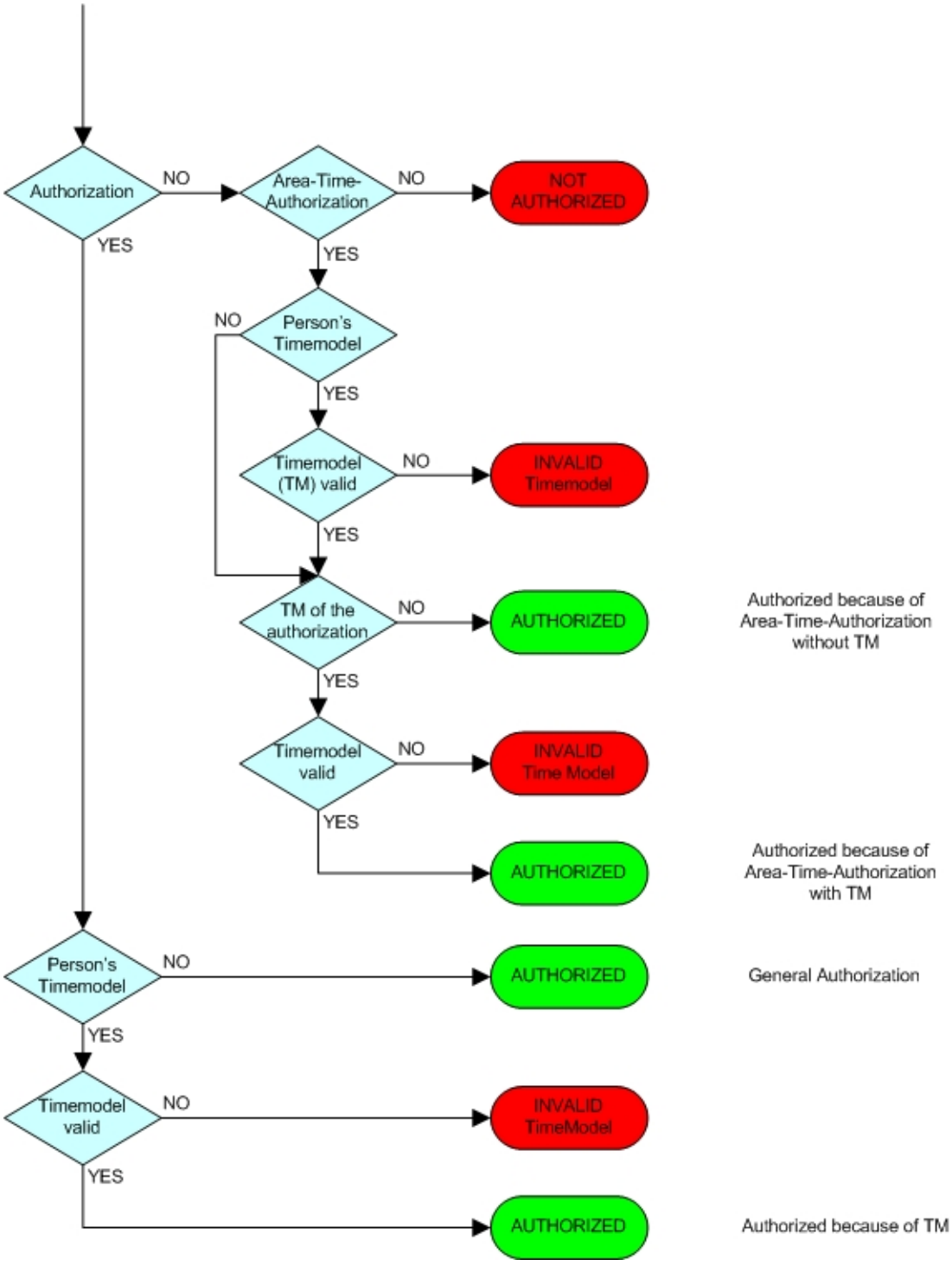
– If a person gets authorizations and an additional time model for the general use of the card, the intersection of the time intervals will be created.

Example:

A person gets the following authorizations:

– Entrances A, B, C, and D with a time model valid from 7 a.m. until 1 p.m..
– Entrances B, D, E, and F with a time model valid from 9 a.m. until 5 p.m..
– A time model valid from 11 a.m. until 7 p.m..

The person gets access for the entrances A and C between 11 a.m. and 1 p.m. and for the entrances B, D, E, and F between 11 a.m. and 5 p.m..



3.2 Common operator tasks

3.2.1 Creating Time Models

Prerequisite

Time models are created from existing day models and defined holidays.

Dialog path

ACE Client > **System data** > **Calendar**

AMS Client > Main menu > **System data** > **Calendar**

1. Clear the input fields by clicking the **New** button
2. Assign a unique time model and an optional description.
3. Define the **period number**, i.e. enter of the number of days included in the time model, after which the model will start again.
4. Define a **reference date**; this date determines the start of the first period.
   Usually you will want the time model to start on a certain weekday, like Monday, so be sure to select a reference date that falls on this weekday.
5. By default, holidays as defined in the Special Days dialog will always be treated as if they had the “Holiday” day model, no matter which day model is specified in the time model. If you want to change this, activate the **Ignore special days** check box.
6. Assign the desired day model to every period day in the upper list field. Double-click in the **day model** column to open a selection list with available day models.
7. Save.
8. Optional - but recommended: saved time models can be tested before being used. To do this, click the **Preview** button to open a dialog that offers the option of testing the time model on certain calendar days. By setting a maximum time period of 90 days in the date fields and then clicking the **Calculate** button, you can check whether the correct days have been assigned and whether holidays have been taken into account.

3.2.2 Creating Personnel Data

All personnel data - except for the visitor data - is created exclusively in the Persons dialog.
To create new data,

1. click the **New** button to clear the input fields
2. enter the desired personnel data in the corresponding fields:
3. enter the most essential master data in the dialog header,
4. supplementary data can be entered in the fields of the tabs. (These tabs can have up to ten freely definable additional fields for entering information that does is not covered by the standard fields).
5. click the Save button to save the data. If you navigate to a different person or dialog without saving the data that has been entered is lost

Further steps:

– Assign access authorizations
– Create access authorizations
– Create card
– Assign card

3.2.3 Assigning cards

Use the **Cards** dialog to assign one or more cards to a person (except for visitors, see below). This requires a workstation that is equipped with an enrolment reader or is configured for manual input of card data.

– Select the person
– Optionally assign access authorizations
– Read in or enter the card data
– Save

3.2.4 Temporary cards

Introduction

A temporary card is a temporary replacement for a card that has been misplaced by a regular cardholder. It is a duplicate that contains all the authorizations and limitations of the original, including rights for offline doors.

To prevent abuse, the system can optionally block one or all of the cardholder's other cards for a limited period, or until unblocked manually.

Temporary cards are therefore **unsuitable** for use as visitor cards.

Prerequisites

- The operator has access to an enrollment reader configured on their workstation.
- A suitable physical card is available for enrollment in the system as a temporary card.

Dialog path

ACE client: **Personnel data** > **Cards**

Procedure: Assigning temporary cards

1. Load the required personnel record into the **Cards** dialog
2. In the list of cards, select the card or cards that require a temporary replacement
3. Click **Change card**
4. In the **Change card** popup window, select **Temporary card**
5. In the **Period** list, select one of the options:
   - **Today**
   - **Today and tomorrow**
   - **Enter number of days**
6. In the case of the last option, enter an integer for number of day in the box.
   Note that in all three cases the **Period** always expires at midnight on the relevant day.
7. If required, select the check box **Deactivate all cards now**.
   - If selected, all cards belonging to this cardholder will be blocked.
   - If cleared, only the card selected above will be blocked.
8. If required, select the check box **Activate card(s) automatically after period**.
   - The blocked cards will be unblocked automatically when the **Period** defined above expires.
9. Place the temporary card on the enrollment reader
10. Click **OK**
    The badge ID is recorded by the enrollment reader.
    - The temporary card appears as active ✓ in the list of cards, along with its validity period and code data.
    - The other card or cards appear as blocked ×, depending on the setting made above: **Deactivate all cards now**.
11. (Optional) In the list of cards, click the column **Collecting date** for the temporary card, and set a date for retrieving it from the cardholder.
    The default value is **Never**.

Procedure: Deleting temporary cards

When the misplaced original card is found, delete the temporary card as follows:

1. Load the required personnel record into the **Cards** dialog.
2. In the list of cards, select the temporary card.
3. Click **Delete card**
   The temporary card is deleted from the list, and the card or cards that it replaced are unblocked immediately

Procedure: Removing temporary blocks on cards

If the blocking of the original card is no longer required, delete the block as follows:

1. Navigate to the **Blocking** dialog: **Personnel data** > **Blocking**.
2. In the list of cards, select the personal card marked as blocked in the **Lock(s)** column.
3. Click **Release temporary lock**
   Note that removing **Blocking** does not remove temporary cards. Temporary cards will expire naturally after their validity periods. If required, delete them manually.

Notes on temporary cards

- The system does not allow temporary cards themselves to be replaced by temporary cards.
- The system does not allow a personal card to have more than one temporary card.
- To see a quick summary of all the cards held by a cardholder, mouse over the leftmost small pane, labeled **Registered,** in the status bar of the main dialog window.

3.2.5 Assigning access rights to personnel

Use the **Cards** dialog to assign access rights to all persons except visitors (for visitors use the Visitor dialog):

- Select the person in the dialog
- Assign authorizations, either by selecting a preconfigured access profile or by picking authorizations individually from the “Available authorizations” box
- Optionally edit date and time values to restrict the validity period of assigned authorizations
- Save changes

In the **Visitor** dialog, only access profiles marked as visitor profiles can be selected.
Person types can be configured to have a default access profile. Any person created with such a type (employee ID) will automatically be assigned the default profile.
The default profile may also be made mandatory. In this case the dialog will show the authorizations but will not allow to change them.

3.2.6 Granting access to persons

The following steps are necessary to register a person to be able to use the access control system with an access card.

Dialog path

Main menu > **Personnel data** > <sub-dialogs>

Overall Procedure

1. In the **Persons** sub-dialog enter the person’s ID data.
2. In the **Cards** sub-dialog:
   - assign access profiles or individual access authorizations.
   - assign a time model, if required.
   - assign the card.
3. In the **PIN-Code** sub-dialog: assign a PIN-Code, if required.
4. In the **Print Badges** sub-dialog, print the card.

For **Visitors,** proceed as follows:

- Enter the personal data in the **Visitors** dialog of the **Visitors** menu and assign an escort (attendant), if required.

Notice!
ID cards and access authorizations do not have to be assigned at the same time. It is therefore possible to assign ID cards to persons without assigning access authorizations or vice versa. However, all access is denied to these persons in both cases.

The process of scanning cards.
When cards are scanned at readers, the reader carries out a number of checks:
- Is the card valid and registered on the system?
- Is the cardholder currently blocked (disabled in the system)?
- Does the card holder have the access authorization for entering in this direction?
- Is the access authorization an area-time authorization? If so, is the scanning time within the periods set by the time model?
- Is the access authorization active, i.e. neither **expired** nor **blocked** (disabled)?
- Is the cardholder subject to a time model? If so, is the scanning time within the defined intervals?
  Prerequisite: Time model checks must be enabled at the reader concerned.
- Is the cardholder in the correct location according to Access sequence monitoring ?
  Prerequisite: Access sequence monitoring is enabled at the reader concerned.
- Has a maximum number of persons been defined for the destination area of this reader, and has this number already been reached?
- In the case of Access sequence monitoring, including anti-passback : Is this card being scanned at a reader before the blocking time set by anti-passback has elapsed?
- Is an additional PIN code required? **Prerequisite**: the reader has a keyboard.
- If a threat level is in operation, does the **Person security profile** of the cardholder have a **security level** that is at least equal to the security level of the reader at this threat level?

3.2.7 Create cards / Print badges

Prerequisites
- The personnel record for the new cardholder should already exist in the system.
- A workstation with the following hardware connected, typically via USB:
  - A badge printer
  - A camera for capturing ID photos.

Procedure:
Dialog path
ACE client: **Personnel data** > **Print badges**
1. Load the personnel record for which the card is to be printed.
2. In the **Layout** pull-down menu, select the desired card layout from the stored layouts.
3. Obtain an ID photo by one of the following methods:
   - Click the **Capture** button and select the desired camera from the list of connected cameras.
   - Click the **Import picture** button and use the cropping frame to select the part of the photograph to be printed on the card.
4. Click **Preview** to ensure that the correct data will appear in the correct layout on the badge.
5. Click **Print** to print the badge.

Supported Cameras
All USB devices that the operating system recognizes as a camera.

3.2.8 Creating Access Authorizations

Dialog path

Main menu > **System data** > **Authorizations**

Procedure

1. Clear the input fields by clicking the **New**  in the toolbar.

   Alternatively, click **Copy**  to create a new authorization based on an existing one.
2. Enter a unique name for the authorization
3. (Optional) Enter a description
4. (Optional) Select a time model to govern this authorization
5. (Optional) choose an **Inactivity limit** from the list.
   This is a timed period of between 14 and 365 days. If an assignee of this authorization fails to use it within the defined period, then he will lose it. Each time the assignee uses the authorization, the timer restarts from zero.
6. (Mandatory) Assign at least one **Entrance**.
   The existing entrances are listed on different tabs, depending on their door models. (Generic) **Entrance**, **Time management**, **Elevator**, **Parking lot**, **Arming Intrusion detection**.
   Select individual entrances from the lists on the various tabs, as described below. Alternatively, use the **Assign all** and **Remove all** buttons on each tab.
   - on the **Entrance** tab select an entrance by selecting one or both check boxes for **In** or **Out**
   - on the **Time management** tab (for time and attendance readers) select one or both check boxes for **In** or **Out**
   - on the **Elevator** tab select the various floors
   - on the **Parking lot** tab by selecting a parking-lot and a parking zone
   - on the **Arming Intrusion detection** tab by selecting **Armed** or **Disarmed**.
7. Select the appropriate MAC from the list
8. Click save  to save the authorization.

Notice!
If you edit an authorization, the changes will immediately affect persons who already have that authorization.

3.2.9 Creating Access Profiles

Access profiles combine multiple access authorizations so that they can be assigned together. Use the **Access Profiles** dialog in the System Data menu to create an access profile:
To create an Access Profile proceed as follows:

1. Clear the input fields by clicking the **New** button in the toolbar, or
2. Select a profile with similar properties and use the **Copy function**.
3. Enter a unique profile **name**
4. Enter a **description** - optional
5. Mark the profile as a **visitor profile** - optional
6. Optionally enter the default duration of validity by selecting the number of days, months, and years
7. Select available authorizations for inclusion in this profile
8. Save the changes.

Modifying Access profiles in a running system
Later modifications to an access profile normally have no effect on persons to which the access profile has already been assigned. In this case an access profile just a convenient means to assign multiple access authorizations at once
However, if a Person type and an Access profile are locked together (Profile locked), then modifications to the profile need to be propagated to all persons of that type.

Notice!
If a Person type is locked to an Access profile, and the Person type contains many persons, then any modifications to that Access profile may take considerable time to propagate to all those persons.
In such cases, plan modifications to the Access profile for times when a large propagation will have least impact to the system.

Refer to
– *Dialog: Person Types, page 107*

3.2.10 Configuring random screening

Random screening is a common method of enhancing site security by selecting personnel randomly for additional security checks.

Prerequisites:
– The entrance should be of the man-trap or turnstile type to prevent one person's "tailgating" another without presenting his own ID.
– A card reader must be present for the at least one of the directions of passage.
– The readers must be configured for normal access control.
– The randomizer can be configured separately for each reader.
– There should be a workstation in the immediate vicinity for releasing any blocks set by the system.

Procedure
1. Locate the desired reader in the device editor DevEdit
2. On the **Settings** tab, select the **Random screening** check-box.
3. In the **Screening percentage** box, enter the percentage of persons to be screened.
4. Save your settings.

The random screening process
1. A cardholder presents his card to a reader configured for random screening.
   Note
   Only persons authorized to pass through the entrance in the defined direction can be randomly selected. As authorizations are checked before random screening takes place any unauthorized person will immediately be barred, and will not be included in the selection process.
2. If the randomizer selects this person for screening his or her card will be blocked throughout the whole system.
   – The event is recorded in the system event log.
   – The **Blocking** dialog receives an entry of unlimited duration marked **Random screening**. [Figure below - number 1]

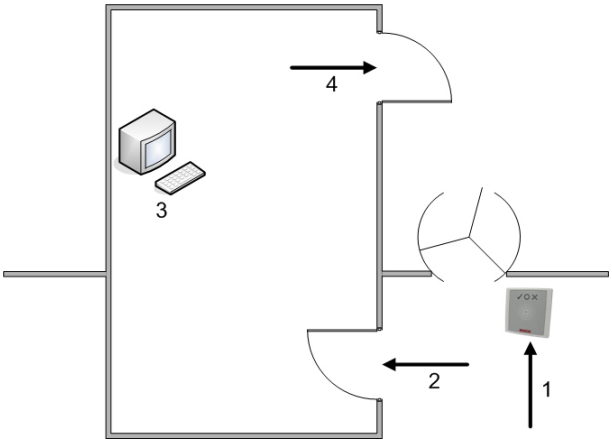
– The status bar of the personnel data dialogs displays the "LEDs" Blocked (red) and with it Random screening (flashing violet).

Notice!
Persons for whom the parameter **Excluded from random screening** has been set (in the **Cards** dialog, **Other data** tab) are not included in the screening process.

3. The randomly selected person is invited for further checks in a separate security booth.
4. After carrying out these checks the security guard resets the block in the **Blocking** dialog as follows:
   – Select the appropriate block in the list control **Blocking** list.
   – Click the **Delete** button.
   – Confirm the deletion by clicking **Yes**.

The randomly screened person can now use his card again at all readers for which he is authorized.

Example room layout for random screening



1 = Present card - screening - system-wide block
2 = Cardholder enters security booth
3 = Cardholder is searched and the block then removed from his/her card via the dialog box.
4 = Cardholder leaves the security booth, without presenting the card to the reader again.

Notice!
The screening percentage is achieved cumulatively over time. For instance, at 10% random screening there is still a possibility (1 in 100, that is 1/10 x 1/10) that two consecutive persons be selected.

3.2.11 Creating visitor data

Visitors have a special status in access control and are kept separate from other personnel data. For this reason, visitor data is created and maintained in separate dialogs.
Use the **Visitor** dialog in the Visitors menu to maintain visitor data:

1. Click the **New** button to clear the input fields.
2. Enter the visitor data and select an attendant, if necessary.
3. Save

3.2.12 Assigning visitor cards

As a rule, a pool of cards is maintained for exclusive use by visitors. For the duration of the visit, a visitor is assigned a card from the pool, after which the card is dissociated from the visitor and returned to the pool.

Use the Visitor Cards dialog to add a card to the pool:

- Click the Register card button
- Scan the card using an enrolment reader
- Alternatively, enter the card data manually

Use the **Visitor** dialog to assign a card from the pool to a visitor:

- Select or enter the visitor data
- Optionally assign the access rights
- Scan a free card from the pool or enter the card data manually

Use the **Visitor** dialog to return a card to the pool after use:

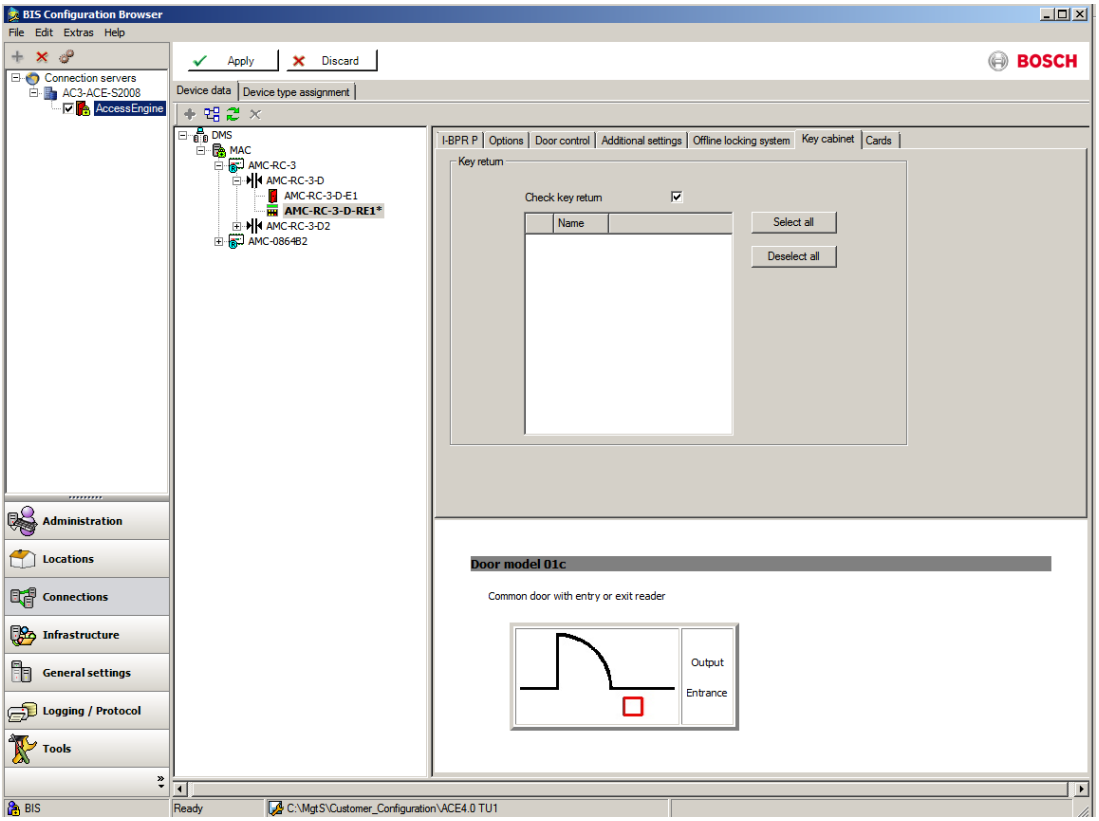
- Select the visitor data
- Select the card in the visitor's card list
- Click the Withdraw card button

3.2.13 Printing visitor certificates

The toolbar of the **Visitors** dialog contains an additional button  for printing out a visitor certificate. Among other things, the person receiving the visitor can use this visitor certificate to confirm if and when the visitor arrived and left.

3.2.14 Configuring usage of key cabinets

The following dialog in the Configuration Browser tracks the return of keys to the key cabinet:

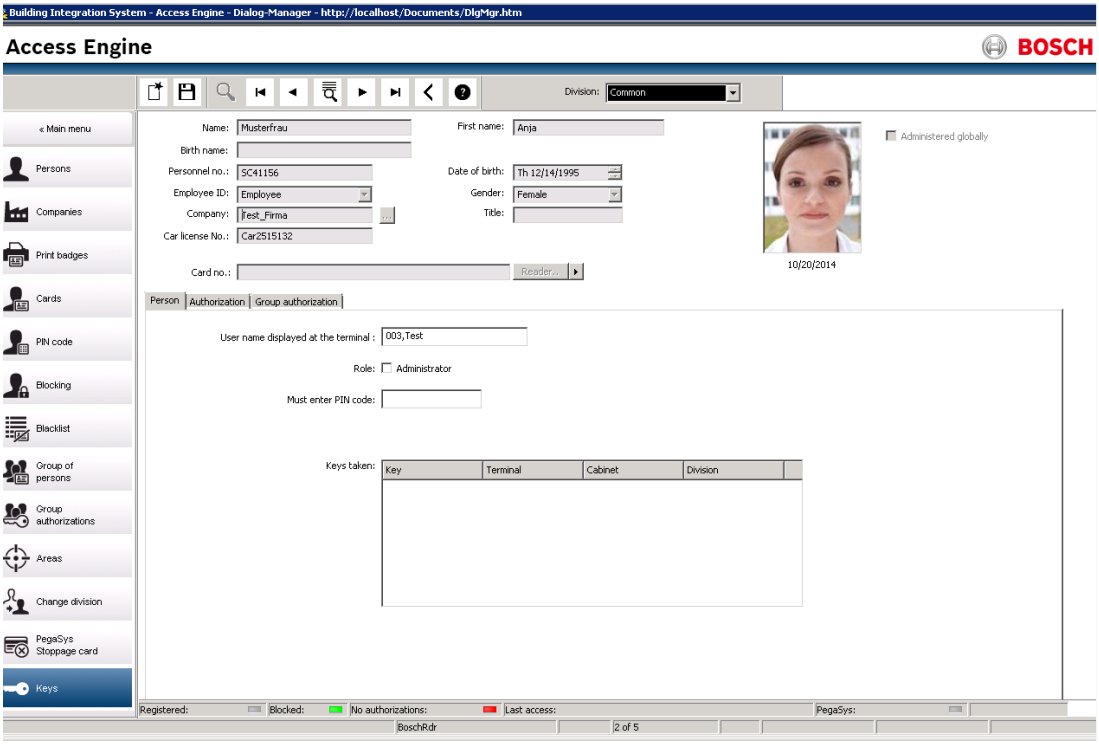


1. Select an acces, e.g. „I-BPR 0101_01“ as in the example shown.

2. Activate the field **Check Return of Keys**.
3. Select at least on key cabinet from the list.

The error message as in the example above will show if no key cabinet was selected.

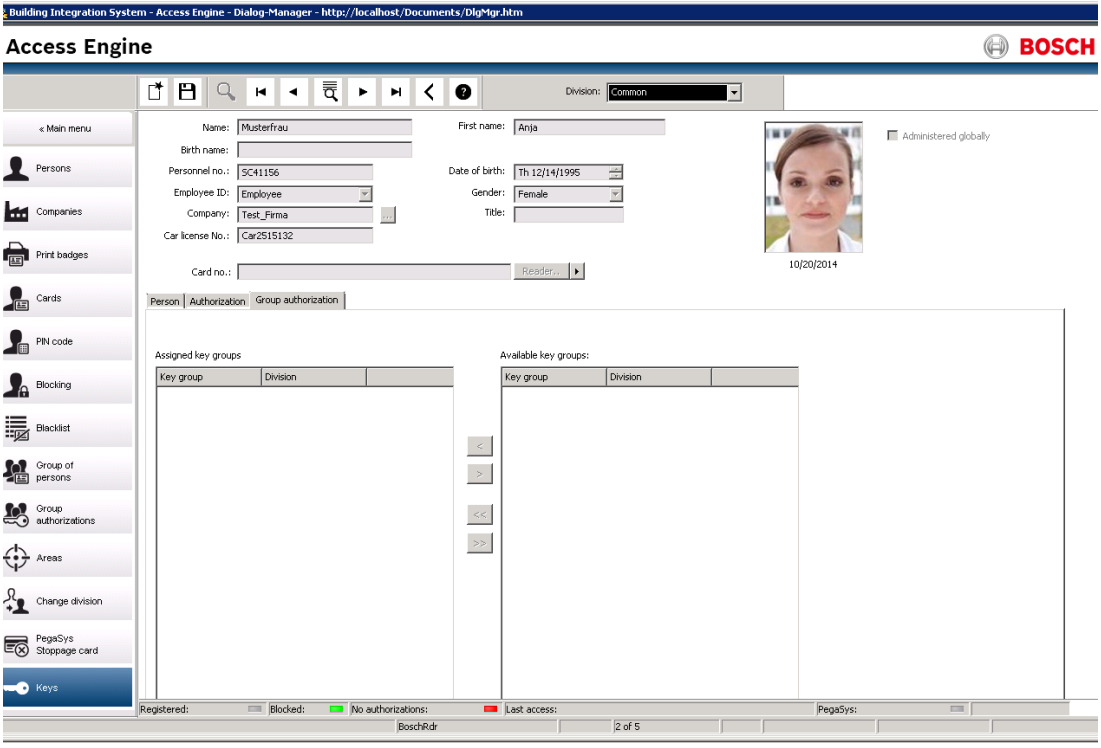
Keys



By clicking the **Key** file a list with 4 columns is displayed:

- **Key:** Number of the key.
- **Terminal:** At which terminal is the key used
- **Cabinet:** Description of the respective key cabinet.
- **Client:** Name of the client.

Key Groups



By clicking the **Key groups** file a list with 2 columns is displayed:

- **Key group:** Description of the key group
- **Client:** Name of the client

3.3 Time and authorization profiles

3.3.1 Day Models

Day models help to manage a fictitious daily routine. Independent of a particular weekday a day model specifies which times of day access shall be granted or not.

Thus different day models must be created for different daily routines.

Three intervals with starting and ending time can be used each day model. The defined intervals activate the corresponding function depending on the usage.

Two day models are predefined: “None” and “Holiday”. By default, both have no active time interval.

Day models are used to construct time models which can be assigned to card holders, access authorizations etc. to restrict access to certain times.

3.3.2 Special days

When used in the time models, the days defined in this dialog should be given a temporal regulation that deviates from the weekday on which they fall. The day model assigned to the holiday is used instead of the day model for the weekday.

The preconfigured list can be changed and supplemented at will. Holidays that are not needed can be removed from the list, so that the normal day model of the respective day is valid for these days. Holidays that are not already available - mainly customer-specific holidays - can be added and defined individually.

Thus, time models periods remain small and contain only those days that follow a different sequence. This allows the calendar to be updated from period to period and year to year. Without holidays, the entire year would have to be defined in the time models and updated every year.

3.3.3 Time Models

Time models restrict the general access at the assigned entrances to certain times of day. This allows assigned authorizations to be withdrawn or to be permitted only in conjunction with additional control procedures, e.g. during the night or at weekends.
Time models can be used in several situations in the access control system Access Engine.
In connection with:

- Access authorizations:
  Time models can be assigned to certain access authorizations, so that the use of entrances included in these authorizations is only allowed at the times enabled in the time model. Access authorizations without temporal restriction can be used at the same time.
- Persons:
  Time models assigned to persons restrict the general use of the ID card to the enabled times.
- AMCs:
  The activation of input and output signals can also be managed via time models.
- Doors:
  Time models can also control door opening times.
- Readers:
  also includes a membership check, i.e. a check to verify that the credential presented to the reader belongs to the customer’s system at all.
- PIN-Code:
  As with the general requirement, PIN code entry can also only be requested as an additional control feature at the times defined in the time model.
- Reader block:
  When a time model is assigned, readers may be blocked at the times declared in the time model.

Time models must be created differently according to their application, since the defined times activate the respective function.

Example:
If time models are used for access authorizations or persons, and if they are set up to prohibit access on weekdays from 7 a.m. to 7 p.m. and at weekends, 2 day models are required:

- One with the interval from 7 p.m. to 7 a.m..
- One without time specifications.

If, however, a time model is set up that makes it necessary to enter a PIN code outside the given weekday times, the day models for this time model must be set up as follows:

- One with the intervals 0 a.m. to 7 a.m. and 7 p.m. to 12 p.m..
- One with the interval from 0 a.m. to 12 p.m.

Notice!
Where necessary, if time models are being used, the intersections of the given times must also be defined where several time models meet.
Regarding the example above, a person or access authorization may not be given a time model if the PIN code input is wanted at the defined times.
However: If authorizations exist containing the same entrances and both variants are assigned to a person, the general authorization is will apply, i.e. the time model is ignored in this case.

–

3.3.4 Authorizations

To use an ID card, the relevant person must be given authorizations at certain entrances. Access is granted to the person if the assigned authorizations contain the relevant entrances. It is possible to assign up to 1024 authorizations per each MAC
Since in the access control system Access Engine it is not possible to assign particular entrances to persons, these must be summarized in authorizations. An authorization must be created even if only a single entrance is to be assigned. However, because as a rule several entrances are assigned which belong, for example, to a complex of buildings, the assignment of the authorizations is simplified by combining them. This way, the number of access authorizations can be kept clearly arranged, even in large plants with several hundred entrances.
In the dialog **Cards** or **Visitors** the adjusted authorizations are assigned to the relative persons.

3.3.5 Access Profiles

This simplifies the assignment of access authorization - also of a large number of authorizations. Access profiles ensure that no access authorization are forgotten or added too much at the assignment.
By selecting an access profile in the **Cards** or **Visitors** dialogs, the contained access and area-time authorizations are assigned. Here the profile serves only as a help for the assignment and as a selection criterion - it is not saved with the personnel data (Exception: **Profile locked**).
Access profiles are particularly suitable for visitors:

- They must be marked as visitor profiles, in order to be used for this purpose.
- This ensures that visitors are not granted access to special areas.
- By the specification of a default validity access authorizations become automatically invalid after the expiration of the given term - this also applies if the visitor fails to return the card.

Notice!
This assignment can be changed by adding or removing single authorizations. Selecting another access profile replaces the assignment made before - you can only select one access profile for each person. By default, all assignments are replaced by the authorizations in the new profile. However, you have an option to keep the old assignments in addition to the new ones.

3.3.6 Secured Facilities

Secured facilities can be divided into Areas for which special control functions can be implemented, for example:

– The localization of individual persons within the secured area.
– The estimation of the number of persons within a given area, in the case of an emergency.
– Limiting the number of persons or vehicles in an area:
  When the predefined population limit is reached further admissions are rejected until persons or vehicles leave the area.
– Implementing access sequence control and/or anti-passback
  Access is denied if a person tries to scan a card at a location to which he has not been tracked. This situation can arise if the person does not scan the card correctly at the entrance to each area he passes through.

Areas can be of any size: one or several buildings, single floors or even single rooms.
The definition and administration of the areas is performed in the BIS Configuration Manager.
Entrances are assigned a location area and a destination area in the Device Editor. When someone scans a card at a reader belonging to a certain entrance, his new location becomes the destination area of that entrance.
Areas can be defined for both persons and vehicles (i.e. parking-lot areas). These are stored separately and can be created and modified in the Areas dialog. When a card is scanned at a reader leading to a parking-lot area, the location is registered for the person's vehicle. Scannings of cards at readers for all other areas are registered for the person.

Notice!
Access sequence control and anti-passback require the existence of both ingress and egress readers at the areas' entrances.
Turnstile-type entrances are strongly recommended to prevent accidental or deliberate "tailgating", i.e. following a cardholder through an entrance without scanning one's own card

3.4 Using the personnel data dialogs

Introduction
Before a person can get access authorizations, he or she must be registered in the acces control system with personal information and one or more credentials of identity:
– Physical credentials such as cards or tokens
– Intellectual credentials such as identification PINs
– Biometric credentials such as fingerprints
– Combined credentials such as cards with verification PINs

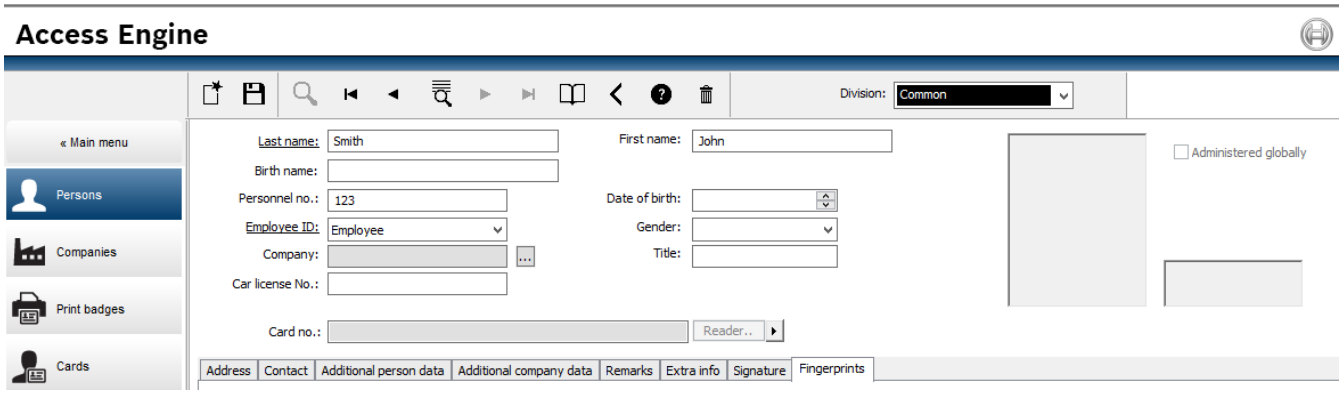
The various tabs of the **Persons** dialog serve to record these credentials, and any other information that your security policy requires. All data is optional except where the labels for the field are underlined, for example, **Last Name** and **Employee ID**.
The **Persons** dialog is used to record data about persons with long-term access to your site. These are usually employees, but can also be external, temporary or contracted staff.
Note that visitor data is handled entirely separately, in the **Visitors** menu.

Refer to
– *Visitor Management, page 58*

3.4.1 Persons

The Persons dialog

Note that the toolbar of this dialog contains an additional button  - which invokes the BIS Event log with the personnel data currently displayed, so that you can quickly find system events involving this person.



Tabs and fields for recording personnel data

The following table lists the data that is displayed by default in the **Persons** dialogs. The dialogs are highly customizable. See section **Custom fields for personnel data**.

Nearly all fields are optional. Mandatory fields are clearly marked with underlined labels in the user interface.

Tab	Field name
Dialog header	Name
	First name
	Birth name (called maiden name in some cultures)
	Personnel no.
	Date of birth
	Employee ID (also known as Person type)
	Gender
	Company
	Title
	ID card no.
	Car license no.
Address	Zip code (called postal code in some cultures)
	Street, no.
	Country, state
	Nationality
Contact	Phone other

	Company phone
	Company fax
	Mobile phone
	Phone
	E-Mail
	Web page address
Additional Person Data	Patronymic (an additional name used in many cultures)
	Birthplace
	Marital status
	Official identity card
	Identity card no.
	Valid until
	Height
Additional Company Data	Department
	Location
	Cost center
	Job title
	Attendant (Escort)
	Reason for visit
	Remarks
Remarks	(Provides a free-form text field for notes and remarks about the person.
Extra Info	10 user-definable fields
Signature	Capture, re-record and delete signatures
Fingerprints	Capture, re-record, delete, and test fingerprints as biometric credentials. Designate certain fingerprints to signal duress.

3.4.2 Recording user-defined information

Use the **Extra info** tab to define additional fields that are not provided on other tabs. If no additional fields have been defined the tab remains empty.

3.4.3 Recording signatures

Recording signatures with the Signature tab

Prerequisite

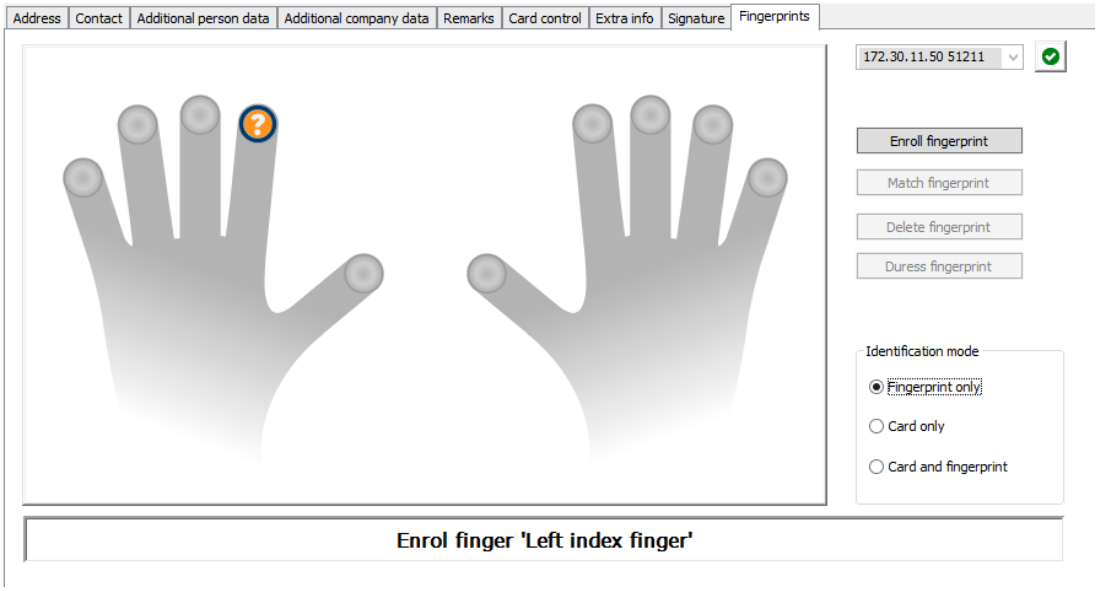
A signature capture pad from the signotec company must be connected and configured in the system in order to capture signatures. Consult your system manager if in doubt.

1. Click the **Signature** tab
2. Click the **Capture Signature** button to record a new signature.

3. Sign directly on the capture pad using its special stylus.
4. Click the check-mark button on the capture pad to confirm.
   The new signature is now displayed on the screen (Click the signature for an enlarged view).

Related procedures:
- Click the **Capture Signature** button to overwrite an existing signature.
- Click the **Delete Signature** button to delete an existing signature.

3.4.4 Enrolling fingerprint data



Prerequisites:
- One or more fingerprint readers must be configured at the entrances, in order to perform biometric access control.
- IMPORTANT: These readers periodically receive and store card and fingerprint data from the servers. The settings on the individual reader ultimately decide which credentials are accepted. They override any settings made here for the person.
- In order to use fingerprints as a verification for (or alternative to) card-based authentication, all cardholders must have their fingerprints scanned.
- The enrollee is in front of a fingerprint reader that is connected to and configured for your workstation. This fingerprint enrollment reader must **not** be an access reader.
- As the operator you are communicating directly with the enrollee, that is, with the person whose fingerprints are to be recorded as biometric credentials for access.
- You have familiarized yourself with how to present your finger repeatedly at the particular reader used, to allow it to capture fingerprints efficiently.

Procedure for enrolling a fingerprint for access
1. Navigate to the fingerprints dialog: **Personnel data** > **Persons** > tab:**Fingerprints** and create or find the enrollee in the database.
2. Ask the enrollee which finger they wish to use for regular access at the fingerprint reader.
3. Select the corresponding finger in the hands diagram.
   Result: The fingertip is marked with a question mark.
4. Click the **Enroll fingerprint** button.

5. Give the enrollee instructions for presenting their finger at the reader.
   Example instructions can be read from the dialog pane below the hands diagram, but different reader types may require slightly different procedures.
6. If the fingerprint is successfully enrolled, a confirmation window will appear.
7. Select an **Identification mode**; this determines what credentials a fingerprint reader will demand of the enrollee when they request access. Note that the mode set here will only take effect if the reader parameter **Person-dependent verification** has been selected.
   The options are:
   - **Fingerprint only** - Only the fingerprint scanner in the reader is used
   - **Card only** - Only the card scanner in the reader is used
   - **Card and fingerprint** - both scanners in the reader are used. The enrollee will have to present both card and chosen finger at the reader, to obtain access.
8. Click **Accept** to store the fingerprint and identification mode for the enrollee.

Notice!
Reader settings override person settings
Note that the identification mode chosen in the fingerprint dialog will only operate if the fingerprint reader itself is configured with the option **Person-dependent verification** in the device editor. If in doubt, consult your system administrator.

Procedure for enrolling a fingerprint to signal duress

Prerequisites:
- Fingerprint readers can only send duress signals if they are configured in the **Device Editor** with the following setting
  Network & Operation modes tab > **Templates on server** > **Card and fingerprint**
- At least one fingerprint of the enrollee has already been successfully enrolled and stored.
- The fingerprint reader is online. In offline mode the reader, of course, cannot send a duress signal to the system.

1. Ask the enrollee to choose a finger they wish to use to signal duress, that is, in case forced by an unauthorized person to use the fingerprint reader.
2. Repeat the fingerprint enrollment procedure, described above, for that finger.
3. When the second fingerprint is successfully enrolled, select it in the hands diagram and click the **Duress finger** button.
   The designated duress finger is marked with an exclamation mark in the hands diagram.

If the enrollee subsequently uses the duress finger at a fingerprint reader, and the reader is not offline, the system will signal duress to the operator, using a popup window.

Procedure for testing stored fingerprints

1. In the hands diagram, select the fingerprint you wish to test.
2. Instruct the enrollee to place that finger on the reader.
3. Click the **Match fingerprint** button
   Result: a popup window will confirm whether or not the stored fingerprint matches that placed on the reader. Note that this procedure may need to be repeated to reduce the likelihood of a false alarm.

Procedure for deleting stored fingerprints

1. In the hands diagram, select the fingerprint you wish to delete.

2. Click the **Delete fingerprint** button
3. Await confirmation of the deletion.

Biometric verification
Biometric verification means allowing a cardholder to enter only after they present biometric proof that they are the true owner of the ID card (or equivalent credential).

3.4.5 Enrolling palm vein data

Biometric verification
Biometric verification means allowing a cardholder to enter only after they present biometric proof that they are the true owner of the ID card (or equivalent credential).

Enrolling a palm vein pattern for ID verification

Prerequisites:
– The palm vein reader is configured on your operator workstation.
– The palm vein reader is powered on and connected to the network.
The palm vein reader is presenting constant blue lights.
– You are acquainted with the manufacturer's instructions for the enrollment process with your palm vein reader.
– The enrollee has already been defined as a cardholder in the system.

Procedure
1. Start the ACE client (Dialog Manager), or close and restart if already running.
2. Navigate to **Personnel data** > **Persons** > tab:**Palm vein**
– The green tick icon, next to the **Enroll palm veins** button, means that the palm vein reader is connected.
3. Load the required cardholder's record in the main dialog.
4. Ask the enrollee which palm they wish to use at the palm vein reader.
5. Select the corresponding palm in the hands diagram.
The palm is marked with a question mark.
6. Give the enrollee instructions for presenting their palm at your model of the palm vein reader. (The following steps may be require some modification depending on make and model).
7. Click the **Enroll palm veins** button.
The palm vein reader's lights change to indicate readiness to read.
– Place the palm on the palm vein reader.
– Wait until the reader lights flash
– Remove the palm from the reader for approximately one second, and replace it again.
– If the reader lights flash again, repeat the previous step until the reader shows either constant green or red lights.
  – **Green**: The palm vein pattern has been enrolled successfully.
  – **Red**: The palm vein pattern has not been enrolled. Verify that the enrollee followed the manufacturer's instructions and repeat the procedure.
8. When the palm vein pattern is successfully enrolled, the question mark icon in the hands diagram turns into a green tick icon.
9. Click  (Save) to store the read palm vein pattern.

Testing a stored palm vein pattern

1. Navigate to **Personnel data** > **Persons** > tab: **Palm vein**
2. Load the required cardholder's record in the main dialog.
3. In the hands diagram, select the hand you wish to test.
4. Click the **Compare palm veins** button.
   The palm vein reader's lights change to indicate readiness to read
– Place the palm on the palm vein reader.
– Wait until the reader shows either constant green or red lights.
  – **Green**: The palm vein pattern matches the pattern stored.
  – **Red**: The palm vein pattern does not match the pattern stored for you.
    Verify that the enrollee followed the manufacturer's instructions and repeat the procedure if necessary.

Deleting a stored palm vein pattern

1. Navigate to **Personnel data** > **Persons** > tab: **Palm vein**
2. Load the required cardholder's record in the main dialog.
3. In the hands diagram, select the hand whose palm vein pattern you wish to delete.
4. Click the **Delete palm veins** button.
5. Await a dialog box confirming the deletion.

Using a palm-vein reader at an entrance

Notice!
Reader offline
If the palm vein reader is flashing blue lights, then the reader is not connected to the network, and will not function. Inform the security staff.

1. Present your card to the card reader.
   If verification by palm vein pattern is required, the palm vein reader now signals readiness to read.
2. Hold your palm over the palm vein reader until it displays either green or red lights.

– **Green**: The palm vein pattern matches the pattern stored for you. Access granted.
– **Red**: The palm vein pattern does not match the pattern stored for you. Access denied.

LED light signals

Note that light signals may vary depending on make and model.

– **Blue (flashing):** The device is powered on but not connected to the network.
– **Blue (constant):** The device is powered on and connected to the network.
– **Blue and pale (constant):** The device is ready to read a palm vein pattern.
– **Flashing under the enrollee's palm**: Signal to remove the palm from the reader for approximately one second, and replace it again.
– **Green (constant):** The palm vein pattern has been recognized.
– **Red (constant):** The palm vein pattern has not been recognized.

3.4.6 Authorizing persons to set Office mode

Introduction

The term Office mode describes the suspension of access control at an entrance during office or business hours. The entrance remains unlocked for these hours, to allow unhindered public access. Outside of these hours Normal mode applies, that is, access is granted only to persons who present valid credentials at the reader.
Office mode is a typical requirement of retail, educational and medical facilities.

Prerequisites

For office mode to operate, the following requirements must be met:
In the configuration (device tree)

– One or more entrances must be configured to allow extended unlocked periods.
– At least one keypad reader must be used at the entrance.

In the client (Persons dialogs)

– One or more cardholders must be authorized to put the entrance in and out of office mode.
– Their cards must be valid and allow access to the entrance outside of office mode hours.

Procedures for authorizing persons to set office mode
Procedure for individual cardholders

1. Navigate to: **Personnel data** > **Cards** > tab:**Other data** and create or find the designated cardholder in the database.
2. Select the check box **Permission to unlock doors**.
3. Click the diskette icon  to save the cardholder's data.

Procedure for groups of cardholders

1. Navigate to: **Personnel data** > **Groups of persons** and use the filter criteria to assemble a list of cardholders in the list window.
2. From the dropdown list **Field to change** select **Unlock doors**
3. Select the check box **Unlock doors**.
4. Click the **Apply changes** button to save the cardholders' data.

Instructing the cardholder how to start and stop office mode

To start or stop office mode at an entrance, the cardholder presses the number *3* on the keypad, and then presents their specially authorized card at the reader.
The entrance remains unlocked until an authorized cardholder presses *3* and presents the card again.
Note that guards with guard cards can stop office mode in the same way, without special permission.

Notice!
Office mode and device parameters for Door
Office mode overrides the **Unlock door** parameter in the **Options** tab of a door in the Device Editor, allowing only **0 Normal mode** and **1 Unlocked.**

3.4.7 Companies

Introduction to the Companies dialog.

- This dialog can be used to create new companies and modify or delete existing company data.
- The company's name and short name must be entered. The short name must be unique.
- If the entry of a company is mandatory in the **Persons** dialog, create the company in this dialog before attempting to create personnel records for that company.
- Companies cannot be deleted from the system if personnel records are still assigned to them.

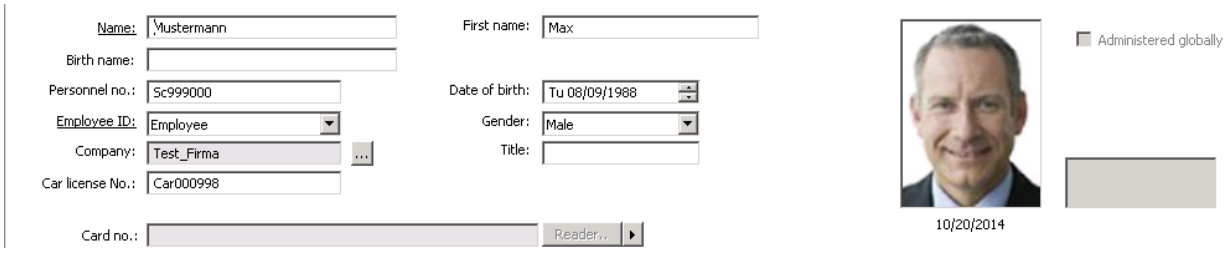
3.4.8 Print Badges

Dialog path

Client main menu > **Personnel data** > **Print badges**

Procedure

1. Create or find the relevant cardholder in the database.
2. Click the **Import picture** button
3. Select the correct photo from the file system.
4. Click **Open** to choose the file.
5. If required, adjust the cropping frame to select only a part of the photo.
6. Click the **OK** button to finalize the selection.
   The selected area appears in the photo frame on the dialog.



Capturing ID photos on the dialog

Prerequisite: A USB camera is connected at the current workstation, and directed at the face of the person in question.

1. Navigate to **Personnel data** > **Print badges**
2. Select the personnel record of the person to be photographed.
3. Click the arrow button next to the **Capture** button and select a camera from the list of connected cameras.
4. Click the **Capture** button.
   A photograph is taken and displayed in a preview window with a cropping frame.
5. If required, adjust the cropping frame to select only a part of the photo.
6. Click the **OK** button to finalize the selection.
   The selected area appears in the photo frame on the dialog.

Printing a badge

Prerequisites:

- At least one badge layout has been created and saved (with the command **Save to gallery**) in the **ACE Badge Designer** tool, invoked from the BIS Configuration Browser. This tool has its own online help.

Note that badge layouts can be single or double sided. Layouts that are activated for use by the **Print badges** dialog are stored on the server in the folder *…\Mgts\AccessEngine\AC\Layouts*

– A suitable badge printer is connected to the workstation.

Procedure

1. Navigate to **Personnel data** > **Print badges**
2. Select the personnel record of the person to be photographed.
3. Select a layout from the **Layout** drop-down list.
4. Click the **Print** button.
   A preview of the badge appears, instantiated with the personnel data and ID photo of the current
5. Verify that the data are correct, and click the **Print** or the **Cancel** button.

Printing forms

ACE provides template forms for printing records of personnel data.
To print a form, proceed as follows:

1. In the ACE Client navigate to **Personnel data** > **Print badges**
2. Select the required personnel record.
3. Select a layout from the **Form** drop-down list.
4. Click the **Print form** button.
5. Select a printer from the list of those available to your system.
   The form is instantiated with the personnel data of the current personnel record, and sent to that printer directly.

3.4.9 Cards

The purpose of this dialog is to assign **cards**, **access authorizations**, or bundles of access authorizations called **access profiles** to personnel records.
Access authorizations and profiles are assigned to persons, not to cards.
New cards that are assigned to a person receive the access authorizations already assigned to that person.

Note: Using access profiles to bundle authorizations

For consistency and convenience, access authorizations are not assigned singly, but typically bundled into **Access profiles** and assigned as such.

– ACE Client: **System data** > **Access profiles**

The card list

A list of cards owned by the selected person is displayed in the Cards dialog. Among the attributes shown in the list are:

– The card usage type.
– A flag whether the card can be used for a configured offline locking system.
– Whether the card is blocked due to the repeated use of invalid PINs. This state is specially highlighted.
– The creation date of the card
– An expiry date (Collecting date) of the card.
  Note: If a motorized card reader is in use, it can physically withhold an expired card. Otherwise the card is simply invalidated.

– The date when the card was last printed, and the number of cards printed.
– Details of the code data.

Option **Administered globally**
The data of persons who have the setting **Administered globally** (check box beside the photo frame) can be only be edited by operators who have the additional right **Global Administrator**. The following data are read-only for operators who do not have this right:
– All data of the dialog **Persons**, except the tabs **Remarks, Extra info** and custom fields.
– All data of the dialog **Cards**.
– All data of the dialog **PIN Code**.

This **Global Administrator** right can be assigned in the in the following check box:
– BIS Configuration Browser menu: **Adminstration** > **Operators** > tab: **ACE operator settings** > check box: **Global Administrator**.

3.4.9.1 Authorizations tab

Assigning authorizations bundled as Access profiles
The most convenient and flexible way to assign authorizations to cardholders is to bundle them first into Access profiles, and then assign the profile.
– For creating Access profiles see the section Creating access profiles
– To assign an Access profile to this cardholder, select a defined profile from the **Access profile:** list

Assigning access authorizations directly
On the **Authorizations** tab:
All access authorizations that have already been assigned to the person appear in the list on the left.
All access authorizations that are available for assignment appear in the list on the right.
Select items and then click the buttons between the lists to move items from one list to the other.

 assigns the selected item.

 unassigns the selected item.

 assigns all available items.

 unassigns all assigned items.

Option: **Keep authorizations assigned**
The effect of assigning an access profile to a person depends on the check box **Keep authorizations assigned**:
– If the check box is cleared, any selection made before this and any access authorizations that have already been assigned are **replaced** when the profile is assigned.
– If the check box is selected, the authorizations of the profile are **added** to the assigned authorizations.

Limiting the time-span of authorizations

Use the date fields **Valid from:** and **until:** to limit the start and end times of the authorizations and profiles. If no values are set then the authorization is valid immediately and of unlimited duration.

Click  to open a dialog to set durations for individual authorizations.

Displaying the entrances of an authorization

Right-click an authorization in either list to display a list of the entrances that belong to it.

Locations tracking for persons and vehicles

ID card readings at parking lot readers are assigned to an ID card holder's vehicle. Detailed car data is stored along with the card holder's access rights for parking lot areas. A person's current whereabouts therefore include the locations of both car and person. A location record is created each time the ID card is scanned. When the card is read by the parking lot's exit reader, the final record is created.

Example A person with authorizations for parking lot area A and building II scans his ID card at the reader in parking area A. A record is created, specifying that this person is in "parking lot area A". If the person subsequently scans his card at other readers, e.g. a reader at an entrance to building II, another location record is saved. This location record is updated at each subsequent reader until the card is once again scanned at the reader in parking lot area A.**:**

Recording Card Data

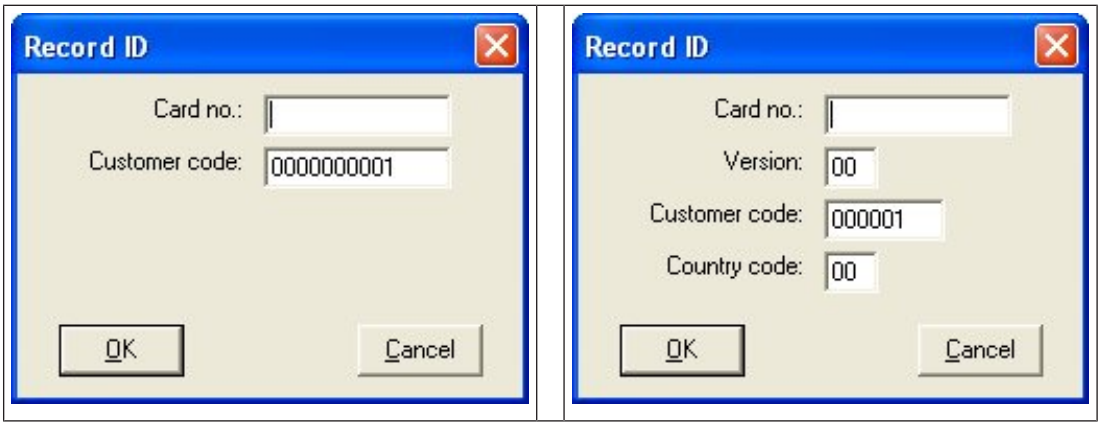
Every person under access control requires a card or other electronic credential, which is assigned to its holder in this dialog.

Reader registrations cannot be done using the Persons dialog. Registrations can only be assigned to the person when his data is linked to the ID card via this dialog.

According to the settings of the system the card number can be assigned by manual input or automatic capture.

Manual Data Input

Click the **Record card** button to assign an ID card to a person. The **Record ID** dialog mask appears. One of these two input dialogs will appear, depending on the type of card and the controllers and readers in use.



Manually enter the number printed on the ID card - card numbers are automatically padded with zeros so that they are always stored as 12 digits. In some systems, no new ID card numbers will be assigned if an ID card is lost; instead the same ID card number is issued, but with a higher version number. The national index number and the customer code are provided by the manufacturer and must be entered in the registration file of the Access Engine system. After checking that the ID card is not already in use by the system, it can be assigned to the person. Successful assignment is confirmed by a pop-up window.

Data capture by reader

Personnel data can be read from ID cards.

1. Click the ▸-button on the right-hand side of the **Record card** button to select a configured card reader.
2. Click the **Record card** button. Depending on the type of reader you can now enter card details in a dialog box, or read data from the card by presenting it to the reader.

Changing Cards

By clicking the **Change card** button the following dialog is brought up if Dialog reader is selected. Otherwise the **Read card** window is shown as seen above:

Deleting ID Cards

Click the **Delete card** button to remove a person's assignment to a card. If you delete a cardholder’s last card then the person's status changes to **unregistered** (red label next to **Registered** in status bar).

3.4.9.2 Other data tab

On the Other data tab you can set additional options for cards.

Assigning a time model:

Use the **Time model** list box to specify the card holder’s daily hours of access, that is, the periods in which the cardholder’s credentials will grant access.

Excluding persons from random screening

Select the check box **Excluded from random screening** to exempt them from being randomly selected for inspections at entrances and exits.

Exclude persons from PIN-code checks

Select the check box **Disable PIN code check** to exempt them from having to enter their PIN codes at PIN-code readers outside of normal working hours.

Notice!

Exclusion from PIN-code checks affects the whole system.
For example, because the PIN codes of these persons are not checked, they will also be unable to arm or disarm alarms at entrances in door model 10.

Extending the door opening time

Select the check box **Extended door opening time** to give persons with disabilities more time (default is 3x) to pass through an entrance before the state **Door open too long** is generated.
Note: The default extension factor can be reset in the properties of the MAC in the Device Editor.
Select **Global Access Settings** > **Time factor for handicapped persons**

Tour monitoring

A **Tour** or **Route** is a strict sequence of readers that is defined in the Client menu:
Tour monitoring > **Define routes** dialog.
To assign a tour to a cardholder, select the **Tour monitoring** check box, and select a defined tour from the drop-down list. If no tours have been defined the check box will be inactive.
When assigned to a cardholder a **Tour** becomes activated as soon as the cardholder scans their card at the first reader in the sequence. After that all the readers in the sequence must be used in order, until the tour is completed. Typical uses are to enforce strict access sequences in industrial clean environments, hygienically controlled, or high-security areas.

Permission to unlock doors

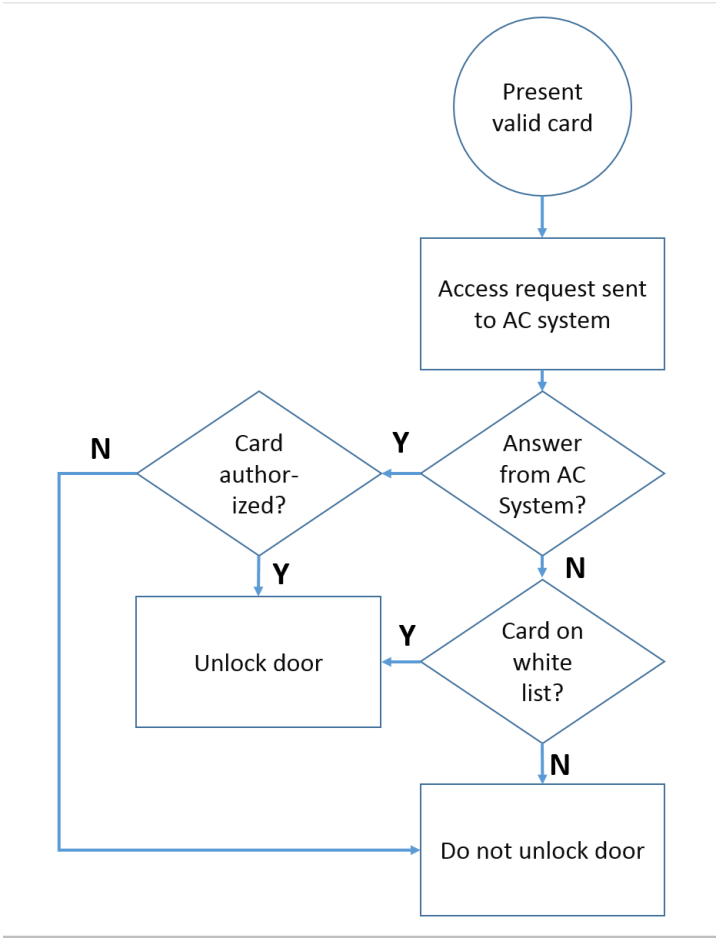
Select the check box to allow the cardholder to unlock doors for an extended period, see **Office mode**.

3.4.9.3 SmartIntego tab

SmartIntego locking systems

Introduction

The SmartIntego card reader first tries to authorize access via the main access control (AC) system. If connection fails it searches its stored whitelist for the card number.



Access authorizations for the SmartIntego locking system are assigned in much the same way as any other access authorizations.

Prerequisites

- A SimonsVoss SmartIntego locking system has been configured within your access control system. See the configuration guide for instructions.
- The cardholders are using MIFARE Classic or MIFARE Desfire cards.
  SmartIntego uses the Card Serial Number (CSN).

The assignment procedure

The following procedure describes how to add a card number to a SmartIntego whitelist , in addition to any authorizations that are already assigned via the main access control system. Whitelists are stored locally on the SmartIntego doors, so that a reader can grant access to the whitelisted card numbers even when the connection to its MAC is broken.
Additions to and deletions from the whitelists are transmitted to the SmartIntego readers as soon as the cardholder data is saved, and a connection is available.

1. In the ACE client menu select **Personnel data** > **Cards**
2. Select the person to receive SmartIntego authorizations
3. Select the **SmartIntego** tab**.**
4. Make the assignments:
   - All access authorizations that have already been assigned to the person appear in the list on the left.
   - All access authorizations that are available for assignment appear in the list on the right.

Select items and then click the buttons between the lists to move items from one list to the other.

 assigns the selected item.

 unassigns the selected item.

 assigns all available items.

 unassigns all assigned items.

3.4.9.4 Alert card tab

This section describes how to create an Alert card that can be used to trigger a threat level

Introduction

An alert card is a card that triggers a particular threat level when presented to a reader. A threat level cannot be cancelled by an alert card, but only through the access control software.

Prerequisites

– An enrollment reader is configured on your system.
– At least one threat level has been defined in the system.

Dialog path

Main menu > **Personnel data** > **Cards** > **Alert card**

Procedure

1. Load the Person record of the person to whom the Alert card will be assigned
2. On the Alert card tab, click Record card
   – A popup window appears: **Select threat level**
3. In the popup window, select the desired threat level and click **OK**
   – A popup window appears: **Recording badge ID**
4. Enter the usual card data corresponding to your site installation, and click **OK**
   – The Alert card that you have recorded appears in the list on the **Alert card** tab.

3.4.10 Permitting access by PIN alone

Background

Keypad readers can be configured to allow access by PIN alone.
When readers are so configured, the access control operator can assign individual PINs to selected personnel. In effect, these personnel receive a "virtual card" that consists solely of a PIN. This is called an Identification PIN . By contrast a Verification PIN is a PIN used in combination with a card, to enforce greater security.

The operator can enter PINs for personnel manually, or assign to them PINs generated by the system.
Note that the same personnel can continue to access using any physical cards that are also assigned to them.

Notice!
This feature is only available to operators with the special permission to assign virtual cards. Please contact your system administrator if you lack permission.

To allow a cardholder to access at a keypad reader by PIN alone, proceed as follows.
Path

Procedure

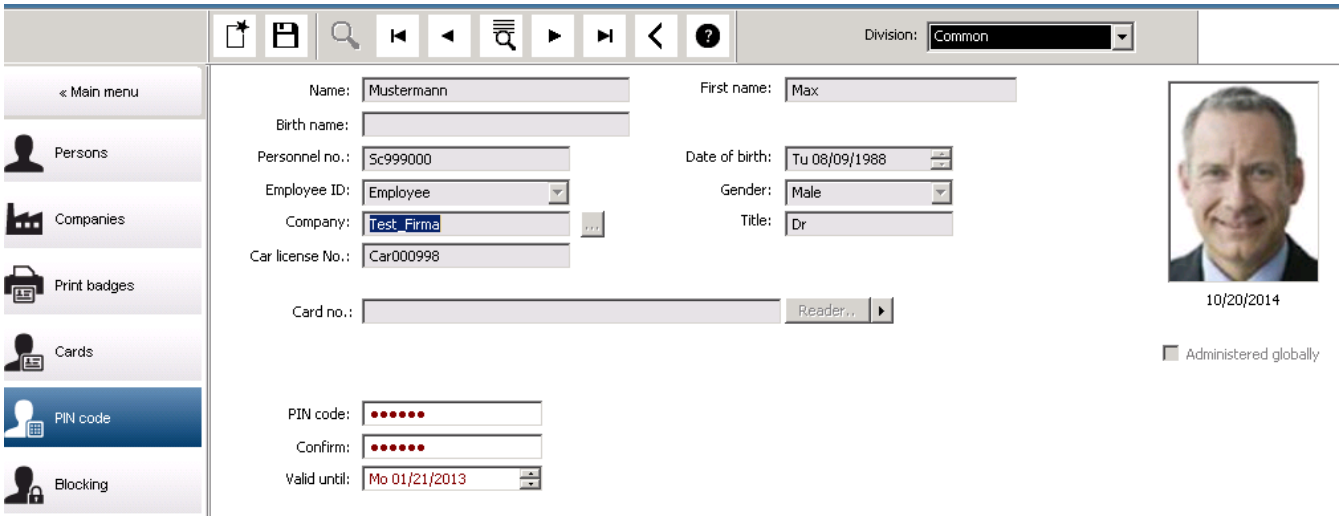
1. Select the cardholder for whom you wish to permit access by PIN alone.
2. Click the arrow button to the right of the **Record Card** button.
3. Select a reader of type **Dialog Enter PIN** or **Dialog Generate PIN**.
   If there are none of these available, please contact your system administrator.
4. Depending on the type of reader, proceed as follows:
   – If the reader is of type **Dialog Enter PIN** then enter a PIN in the text box and click **OK.**
     Note that the system may reject PINs that do not conform to system parameters or standard security regulations. In this case please use a different PIN.
   – If the reader is of type **Dialog Generate PIN** then click the button **Generate PIN** and click **OK**.
     Note that you may click the button repeatedly until a PIN is shown that is acceptable to the cardholder.
5. When the PIN has been accepted, a new line appears in the list of cards for the selected cardholder. The line represents the PIN as a virtual card with the word **PIN** in the **Card no.** column.
6. Click the diskette button to save the cardholder data.

3.4.11 PIN Code

Dialog: PIN-Code

For access to zones with higher safety requirements, access authorization may not be sufficient. Here a PIN code must also be entered. Each person or ID card can have a PIN code, which is valid for all areas. The system prevents the use of very simple codes (e.g. 123456, or palindromes like 127721). Validity can be restricted and is specified for each person in the dialog.
If a PIN code is blocked or has expired, access to the area requiring the code is denied, even if the ID card is still valid for all other areas.

If an incorrect code is entered three consecutive times (default setting - this can be configured between 1 and 99), this card is blocked, i.e. access is denied to all areas. A card blocked in this way can only be unblocked via the Blocking dialog.



Enter a new PIN code in the **PIN-Code** input field and confirm by re-typing. The length of the PIN code (between 4 and 9, default value 6) is configured by the system administrator.

Notice!
How cardholders enter identification PINs at card readers depends the kind of readers configured in your system. For example:
At RS485 card readers the cardholder enters: **4 #** *<the PIN>*
At Wiegand and other card readers the cardholder enters: *<the PIN>* **#**
Be sure to inform cardholders how to enter their PINs. If in doubt, consult your system administrator.

PIN-Code for arming intrusion detection systems (IDS)
Input of a 4 to 8 digit PIN (default = 6 - the same length as the verification PIN). This PIN will be used to arm an IDS.
The display of this fields can be parametrized. Only if the control **separate IDS PIN** is activated the control are available.
– Configuration Browser > **Infrastructure** > **System configuration** > **ACE PIN-Codes**
Select an expiration date if required.
If the input fields to enter the IDS PIN are not available, the verification PIN can be used to arm and disarm the IDS too. But, if the input fields are shown in this dialog, the arming PIN can be used for IDS, only.
Default setting: The input fields for the PIN Code Arming are invisible.

Alarm (Duress) PINs
Persons under duress may trigger a silent alarm via a special PIN code. Because the silent alarm needs to remain unnoticed by the aggressor, access is granted, but the system operators are alerted to the duress.
Two variants are available which are activated at the same time and the person being threatened can choose between them:
– Inputting the PIN code in reverse order (321321 instead of 123123).

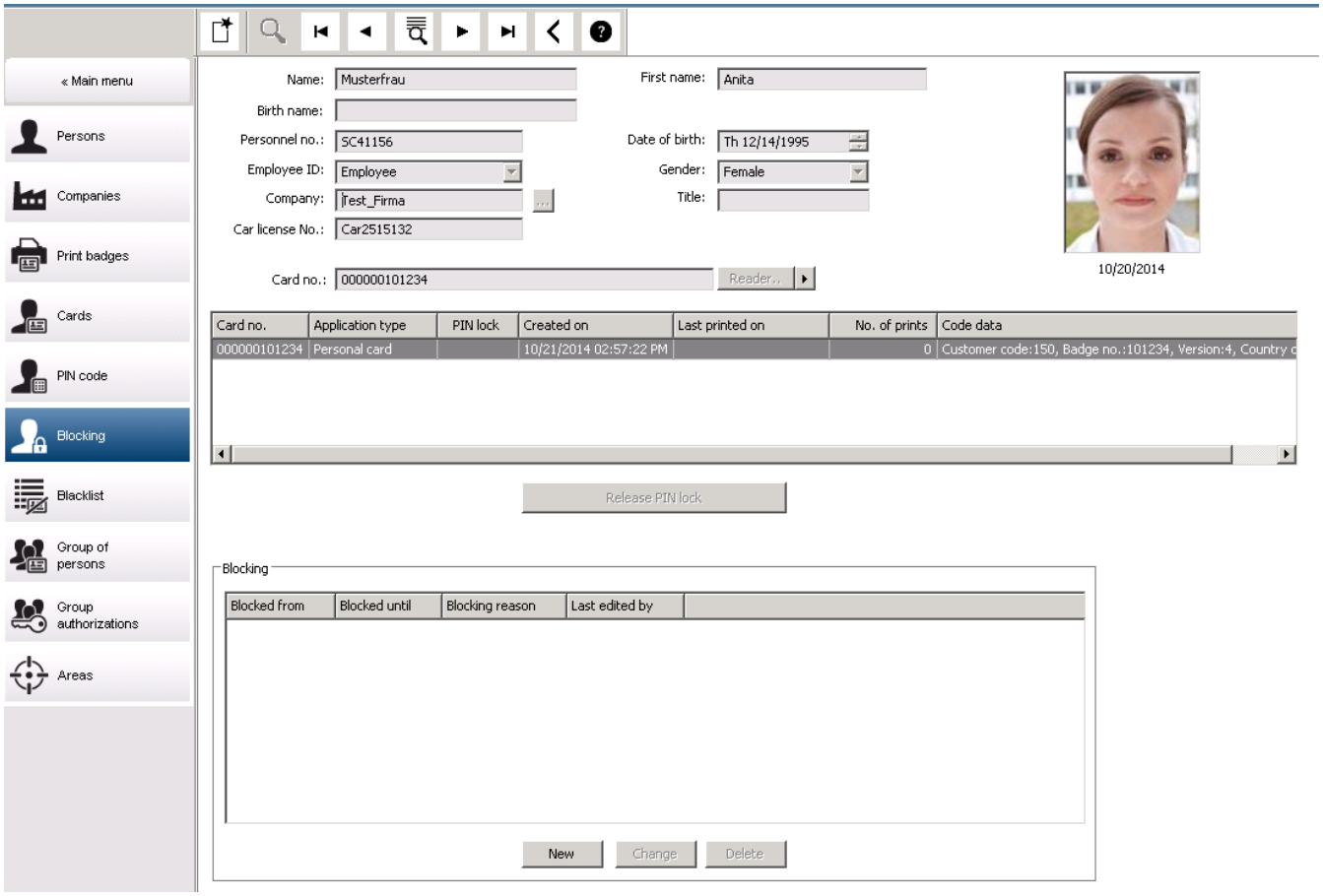
– Incrementing the PIN by 1 (for example: 123124 instead of 123123). Note that if the last digit is 9 then the PIN is still incremented, so PIN 123129 would have a duress PIN of 123130.

3.4.12 Blocking

Dialog: Blocking

In certain situations it is necessary to deny access to a Person temporarily, or to remove a block imposed by the MAC, e.g. due to incorrect PIN codes being entered three times, or to random screening.

Blocking means that all access is denied for this person, regardless of the credential used.



1. Select the person as usual.
2. In the Blocking pane, click **New** or to create a block for the currently selected person.
3. Enter additional information in the popup dialog:
   – **Blocked from / until**: (If no end time period is specified, the person is blocked until the block is lifted manually.)
   – **Block type:**
   – **Blocking reason:** (For the person's record, if the block type is `Manual`)
4. Click **Save** in the popup to save the block.

– If required, select a block from the list and click **Change** or **Delete** to change or delete it.

If **Manual lock** is chosen as the block type enter a **Blocking reason** for the person's record.

Notice!
The block applies to the person not to a particular credential. It is therefore not possible to cancel or avoid the block by allocating a new ID card.

3.4.13 Blacklisting

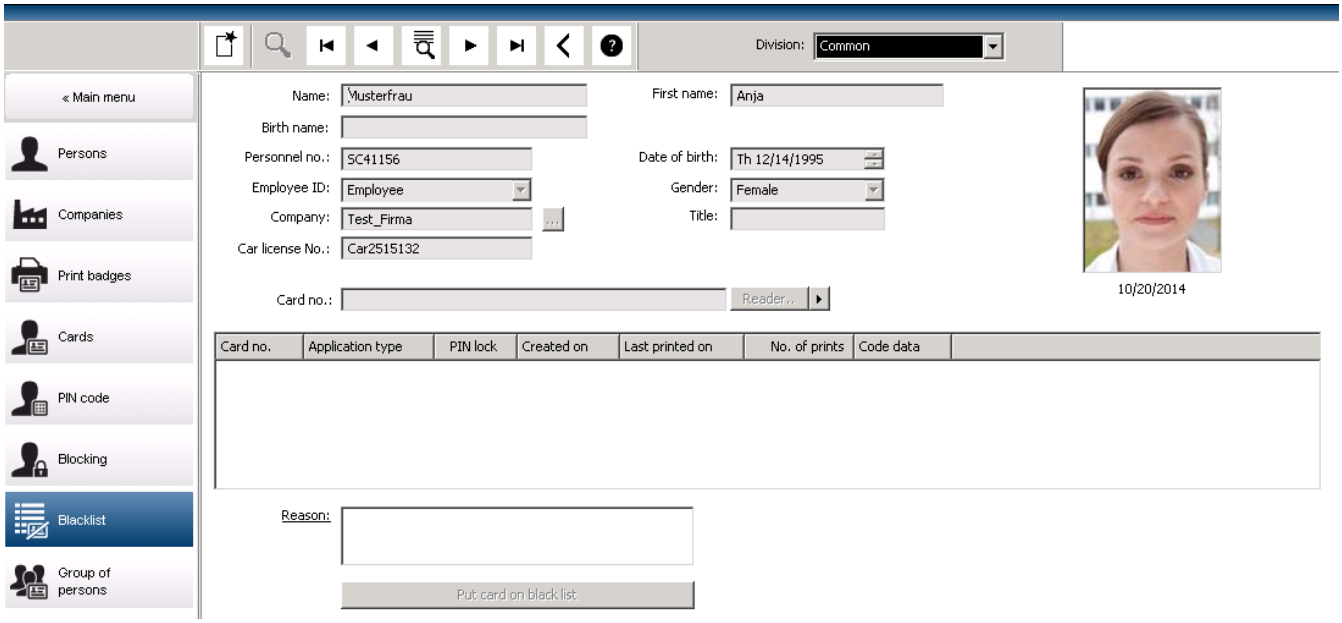
Dialog: Blacklist

Any cards that must never be used again are, for example stolen or lost cards, are entered into a blacklist table.

Note that the credential is blacklisted, not the person.

Notice!
The process is irreversible. Cards on the blacklist can never be unblocked, but must be replaced instead.

Blacklisted cards do not grant access. Instead the attempted use is recorded in the log file, and an alarm is generated.



Main menu > **Personnel data** > **Blacklist**

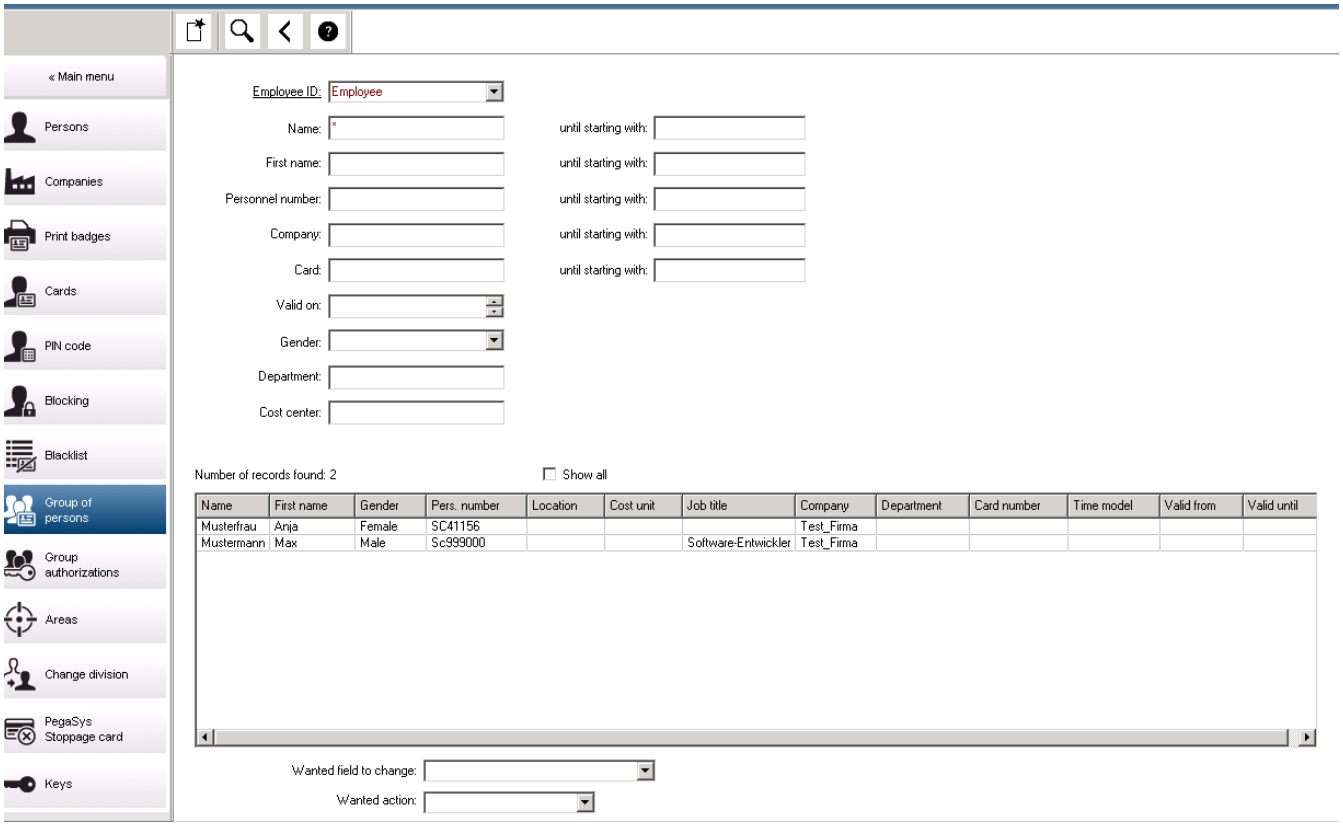
1. Select the person whose ID card is to be put on the blacklist.
2. If more than one card is assigned to this cardholder, select the card in the list **ID card No**.
3. Enter the reason for blacklisting this card in the **Reason** input field.
4. Click the **Blacklist this card** button.
5. Confirm the blacklisting in the popup window.

The card is blacklisted with immediate effect.

Notice!
Blacklisting affects cards, **not** cardholders.
Non-blacklisted cards belonging to the same cardholder are not blocked.

3.4.14 Dialogs for editing multiple persons simultaneously

Group of Persons



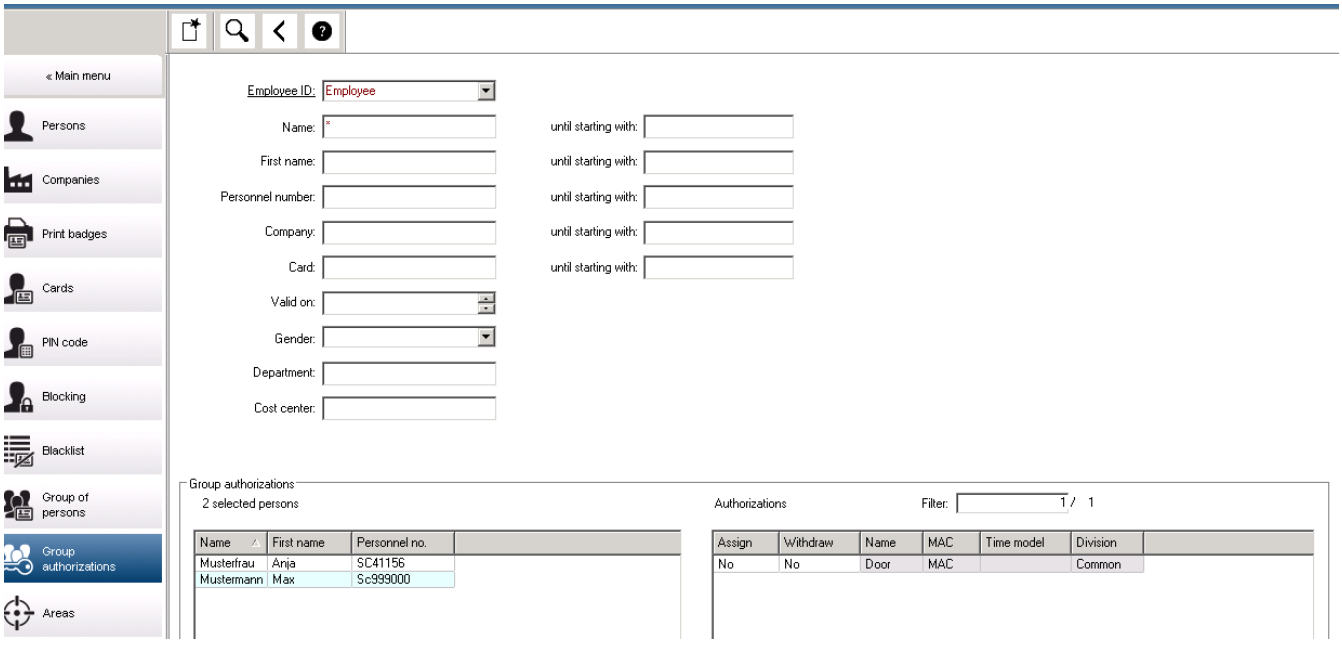
Another dialog selects a group of persons to which group modifications can be defined. To keep control over the selected group of persons the first ten persons are listed with names and real data form the database (real data: if “ST-AC” is selected as a department, then e.g. “ST-ACS” and “ST-ACX” will be displayed). In addition, the number of persons of the selected group is displayed.
After the group of persons has been selected the following entries can be selected:

- Employee ID
- Name
- First name
- Personnel number
- Company
- Card
- Valid on
- Gender
- Department
- Cost unit
- Reserve fields if defined

Then the modification option can be selected:
- Field to be changed
- Desired action
- Old value
- New value.

Thus the designed values are entered into the field **Old value** or **New value** respectively. By selecting a button **Apply changes** and confirming the safety request **apply changes for all selected persons?** the action will be completed, i.e. the dialog cannot be used while the action is ongoing. Actions triggered by the fields *1 to *4 will probably take more time than the other fields (without a star), and not all modifications are allowed. Thus, for instance, **Desired action** cannot be compared with **New value**, as these inputs are not covered by the standard product. The **Old value** and **New value** fields can also vary respectively.

Group Authorization



In the menu item **[Group Authorization]** the following search criteria are supported:
- Employee ID
- Name
- First name
- Personnel number
- Company
- Card
- Valid on
- Gender
- Department
- Cost unit
- Reserve fields if defined

After this, a list shows in the lower part of the dialog which displays all selected persons (with name, first name, and personnel no.). All authorizations with description of the authorization are listed on the bottom right, with description of the authorization, time model, and the columns **[Assign]** and **[Withdraw]**. When the authorization list opens the current authorizations are not shown, and the columns **[Assign]** and **[Withdraw]** are preset to “No”. Now, the individual authorizations can be assigned by double clicking the field in either column, which converts the “No” to a “Yes” entry or vice versa. Clicking Execute changes all authorizations assigned with “Yes” are added to all selected persons, or withdrawn, respectively. All other authorizations for the persons remain unchanged, as usually the selected persons don’t have completely identical authorizations.

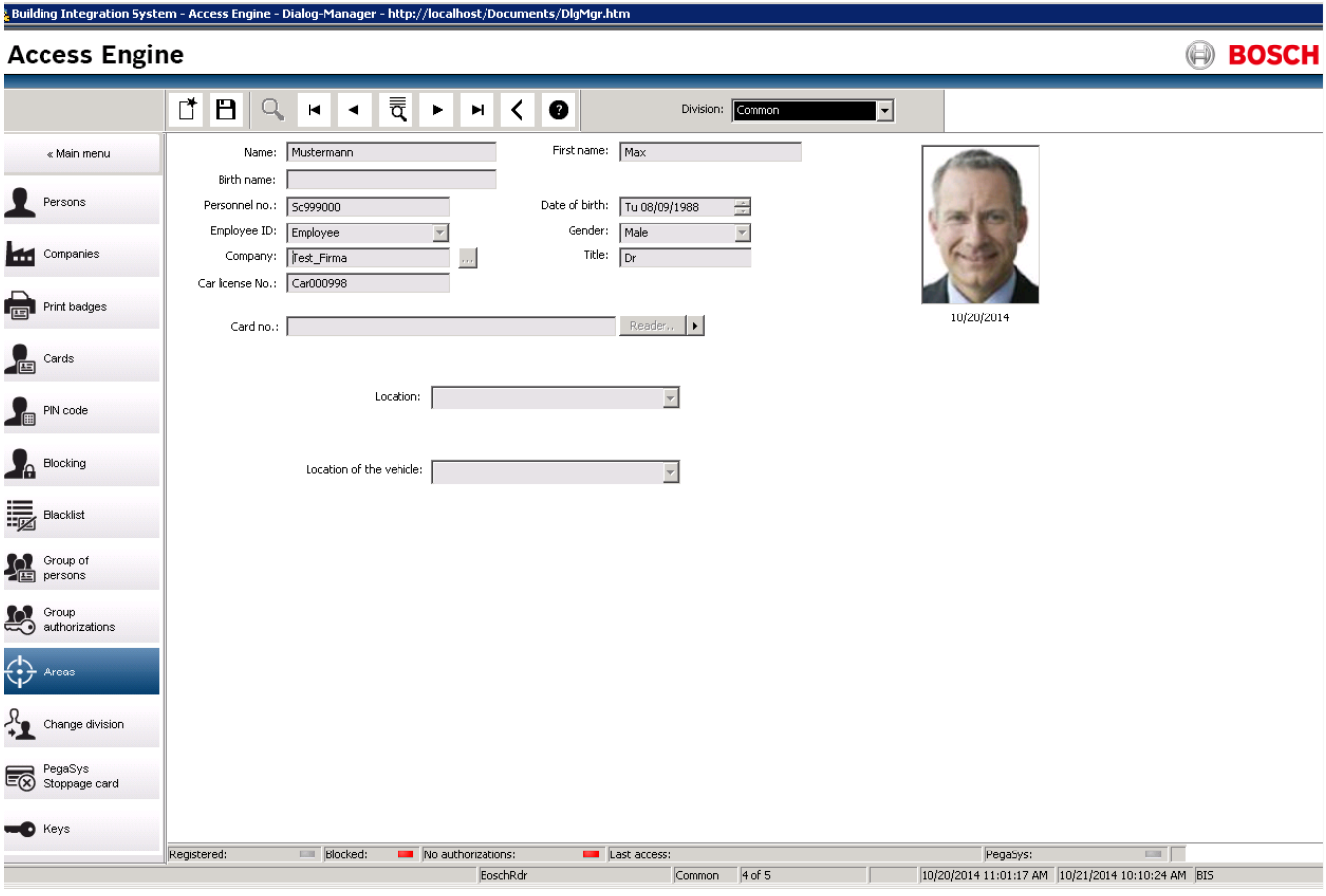
3.4.15 Areas

Dialog: Areas

The system can automatically trace a person's whereabouts. If, for one reason or another (e.g. fire alarm exercise), the trace is lost, the person's location can be set manually in the system. If, for example, access sequence check is activated and a person passes an ID card reader without using his ID card, the system will not be aware of the person's change in location. At the next ID card reader, what the system considers to be the wrong location can lead to the person being denied access. In these cases, the location must be corrected manually. The same applies to vehicles.

Dialog path

Main menu > **Personnel data** > **Areas**



1. Select the person from the database as usual
2. Select a new location from the pull-down lists Location or Location of the vehicle
3. Click  to save the correction.

General reset of locations

Note that corrections made in the **Personnel data** > **Areas** dialog affect only the location of the selected person or the vehicle.

To reset the locations of all persons/cars *UNKNOWN* in, for example, after an evacuation drill, use the dialog:

Main menu > **System data** > **Reset Areas Unknown** dialog.

4 Visitor Management

4.1 Visitor Data

Introduction

The system supports the quick and easy administration of visitor data. Data for visitors who are already known can therefore be entered and access authorizations set before the visitor arrives. When the visitor arrives, only the card has to be assigned. At the end of the visit, when the card is returned, the connection between the ID card and the person is deleted again and the authorizations are automatically withdrawn.

If the visitor's data is not deleted by the user, this is done by the system at the end of the configured amount of time (default value 6 months) after the ID card was returned for the last time.

There are two dialogs for the administration of external visitors.

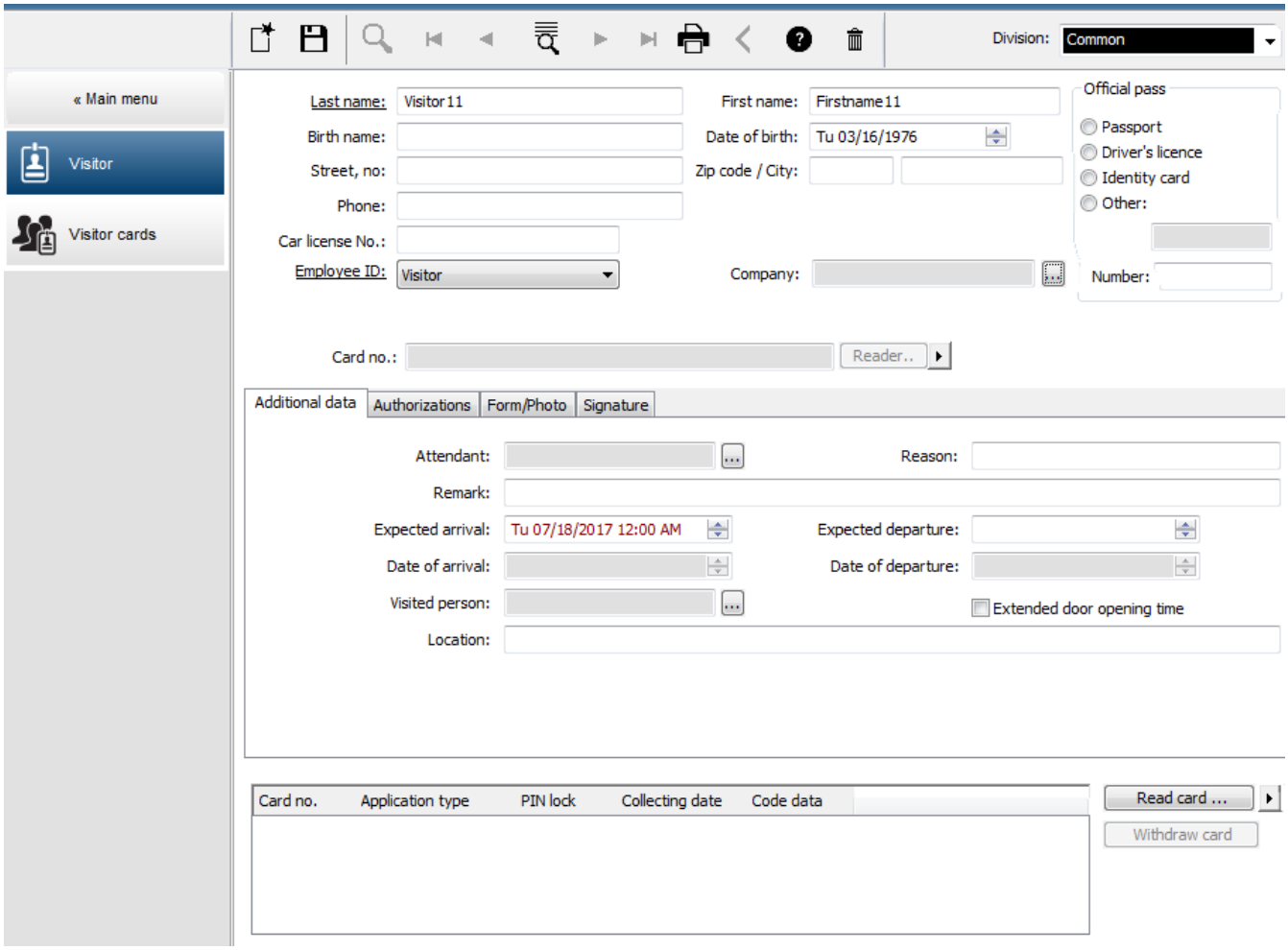
– The **Visitors** dialog is used for entering visitor data and visitor access authorizations.
– The **Visitor cards** dialog regulates the registration and deletion of visitor cards.

Dialog: Visitors

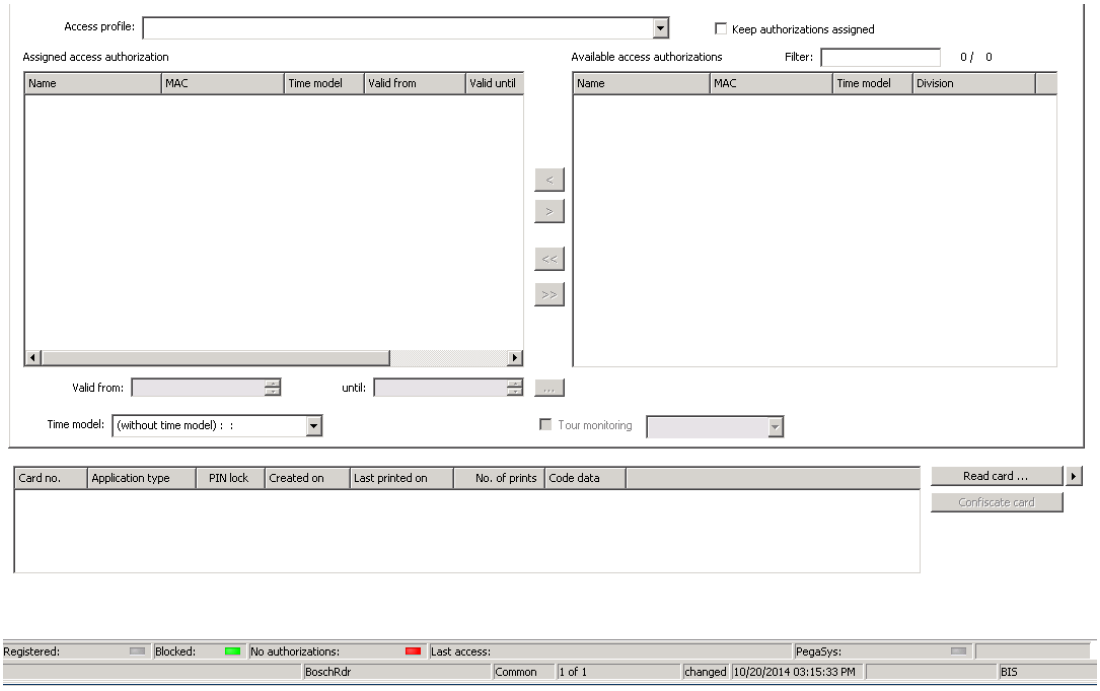
Visitors have a strictly separated status from other persons and are therefore processed in a separate dialog. Persons with **visitor** identification can neither be created in the **Persons** dialog nor have ID cards recorded for them in the dialog for that purpose.

Among other things, there is no **Employee ID** input field in the **Visitors** dialog. Since there is a separate database table for visitors, persons created in the dialog described here are automatically identified as visitors. This therefore means that no persons other than visitors can be created here. Accordingly, selections are only made in this dialog in the relevant database table. In contrast, all persons registered on the system can be selected in the other personnel data dialogs, but may not always be able to be used for visitors (the **Cards** dialog).

Where known, visitor data can be completely or partially entered in the system before the visitor arrives. This provides a minimum of waiting times for visitors whose data have already been recorded.



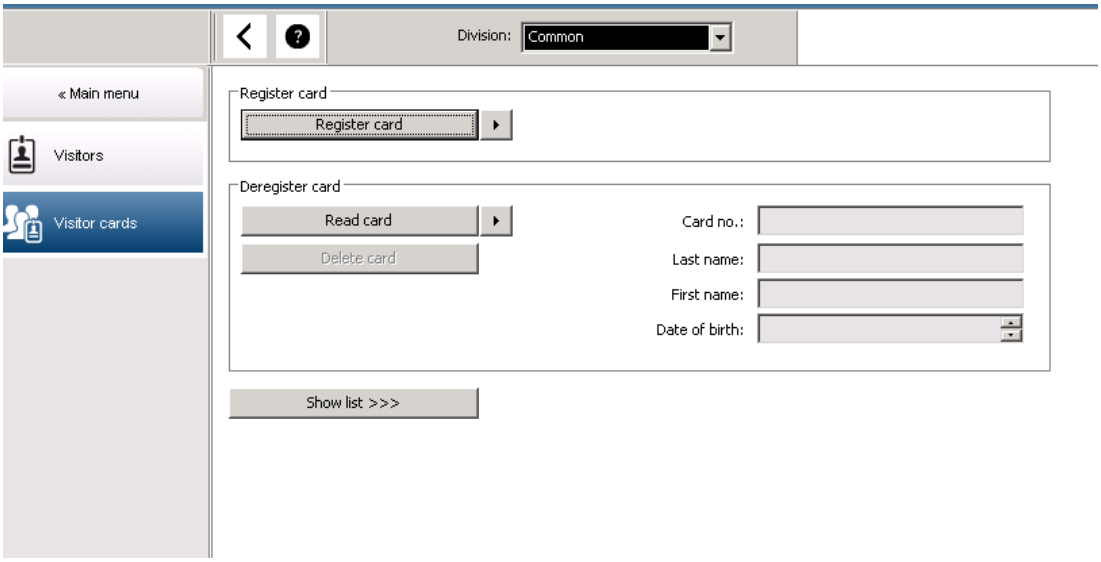
The **Reason** of the visit, the **Location** the visitor visits and a **Remark** may be entered in the input fields below.
If you choose to enter data in the **expected arrival** and **expected departure** fields, these dates will then also appear in the **valid from** and **until** fields.
The relevant dates are entered in the **Date of arrival** and **Date of departure** fields by the system when visitor data is respectively assigned to and separated from a visitor ID card.
As with the **Cards** dialog, there is also the possibility of assigning visitors extended door opening times" to ensure easier access, e.g. for disabled persons.



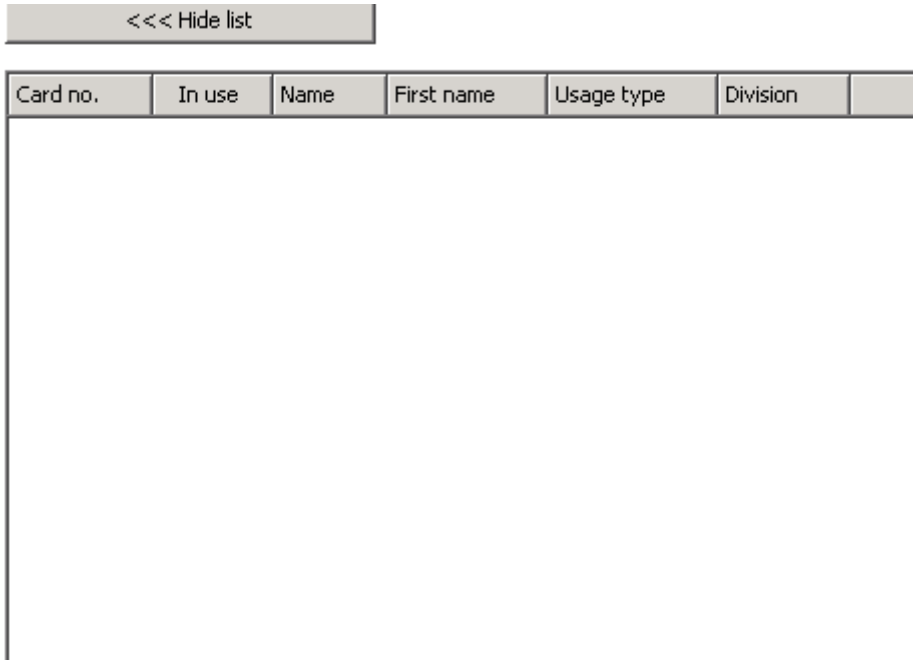
In the **Assign authorization** dialog field an existing visitor profile can be selected in the homonymous selective list, or single access authorizations from the **Available access authorization** list can be selected in the **Assigned access authorization** list on the left by marking and transferring them from the right list.
Only Access profiles which are marked as Visitor profiles can be selected in this dialog. Thereby it shall be avoided that visitors get access to special areas by the allocation of general authorizations.
The validation of access authorizations can also be set for each authorization by themselves.
If the card reading has got an error, the ID card number may also be given manually. The current date is stored as arrival date simultaneously.
After the visit the visitor returns his ID card. While this ID card is read in a card reader or the ID card number is entered manually, the associated person is selected and his data are displayed on the screen.
The operator confirms the return of the card. The association between the ID card and the visitor is removed by clicking the **Confiscate card** button. The date and time of this action are stored as departure date.

Dialog: Visitor Cards
Some cards in the system are reserved as visitor cards. Normally a visitor card is assigned to an incoming visitor and returned when that visitor leaves. Then the card can be reused. Such cards need to be registered as visitor cards in this dialog before they can be assigned to visitors:

Notice!
In general, visitor ID cards are created without a name or photo, to make them reusable.



Click **Register ID card** button for the registration.
The input procedure described previously (sections **Persons** and **ID cards** in the **Personnel data** chapter) is then used with the ID card number in order to detect the ID card. This allows the system to recognize the ID card as a visitor ID card and it can then be applied within the scope of the following dialogs.



To make the assignment of visitor ID cards quicker, it is advisable to scan all existing ID cards, so that these cards can be assigned to the respective visitors in the next dialog.
At the end of the visit, the visitor returns the ID card. By scanning this ID card at a dialog reader or by entering the ID card number, the person to whom the card is assigned is selected and this person's data is displayed on the screen. [For inputting the ID card number manually and switching to the use of readers, please see the descriptions in the **Dialog: Cards** and **Dialog: Visitors**.] The user confirms the return of the ID card. The connection between the ID card and the personnel data of the visitor is removed using the button. The current date is stored as the departure date.

Printing a Visitor form

The toolbar of the **Visitors** dialog contains an additional button  for printing out a visitor certificate. Among other things, the person receiving the visitor can use this visitor certificate to confirm if and when the visitor arrived and left.

Visitor pass

Entry	Exit

First- and lastname
Steven Visitor

Company

☐ Proof of authority for plant area

Registration plate

Passed card

Contact person | Phone | Department

Reason of visit

Visit appointment
☐ Yes ☐ No

Type of official
Passport

Number of offical document

I accept the terms and conditions overleaf

Location, date

Sign of visitor

Identy card with photo seen ?
☐ Yes ☐ No

Sign of plant protective force

To complete from visited person

Arrival at _____
Departure at _____

To sign on visited person

4.2 Visitor too late

The view **Visitor too late** enables an operator to check the location of visitors on the premises, and see whether they have overstayed their scheduled departure time.

– To view the html page, authorized operators need to have its link configured on their start screen.
– It is possible to create an alarm trigger in the BIS to respond to the **Visitor too late** message. The trigger can then open the html page with the visitor's data.

Events that lead to the message Visitor too late:

When a card is assigned to a visitor the operator enters the expected time of departure. When the visit ends the visitor returns the card to the reception desk where an operator cancels the card.

Alternatively a motorized card reader can be used as an exit reader for visitors, and configured to retain the visitor's card when they leave the premises.

If a visitor fails to return the card before the prearranged time of departure, regardless of whether the visitor is still on the premises, a **Visitor too late** message is generated by the system.

This check for overdue card returns is executed at regular intervals (e.g. every minute). A **Visitor too late** message will be generated by each check until the card is returned. The time interval can be configured in the server's registry under: *HKLM\Software\Micos\SPS\Default\VLDP\Interval*

Notice!

The generation of this message can be deactivated in the server's registry under: *HKLM\Software\Micos\SPS\Default\VLDP\Active*

This feature enables the customer to detect any visitor who doesn't meet the designated officer or doesn't report back at the reception or exit gate after meeting the officer in the given time frame.

It is checked:

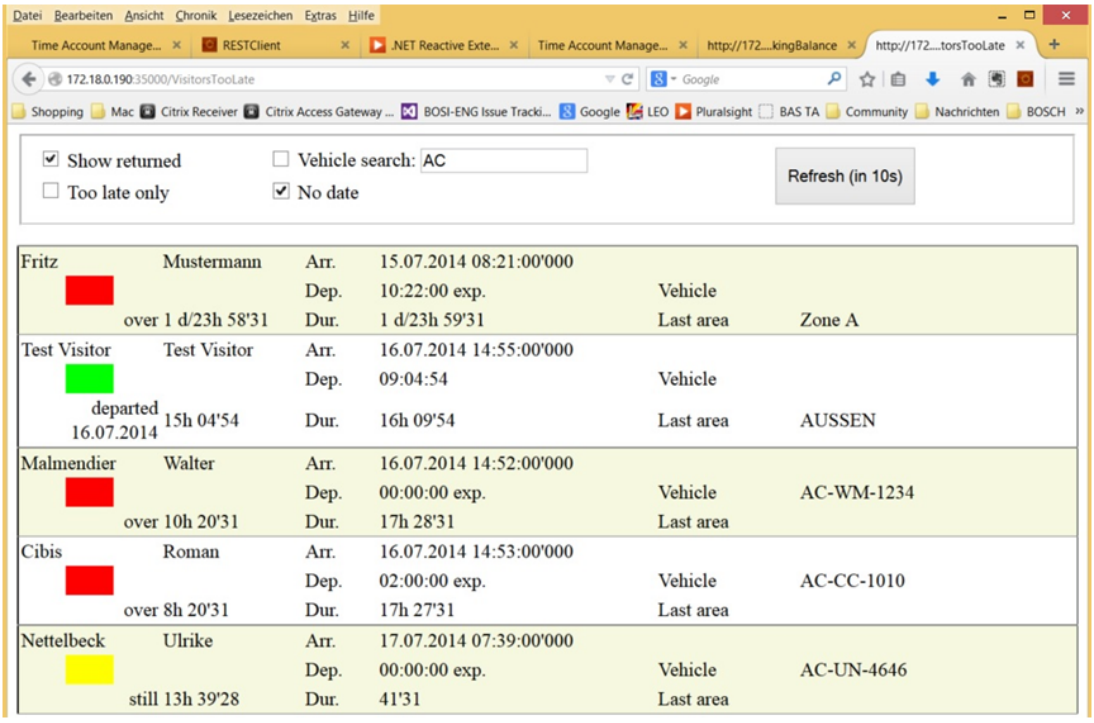
– Which is the last used area for the visitor's building access tag,
– If the visitor has drawn back the building access tag,
– If the visitor has drawn back the vehicle tag, if applicable.

A **Visitor too late** and **Vehicle too late** report are generated.

If not returned, the current area of the tag could be printed in the 'visitor too late' report.

The visitor status is displayed on the website with colored bars::

– **Green**: The visitor has returned all access cards.
– **Yellow:** The visit is not yet finished and the time has not yet expired.
– **Red:** The visit is not yet finished and the time has expired, i.e. **Visitor too late**.



The page does an automatic refresh every 30 seconds. The refresh time is configurable inside the webpage. In addition the operator's view can be adjusted using the filters **Show returned**, **Too late only**, and **Vehicle search**.

5 Car Park Management

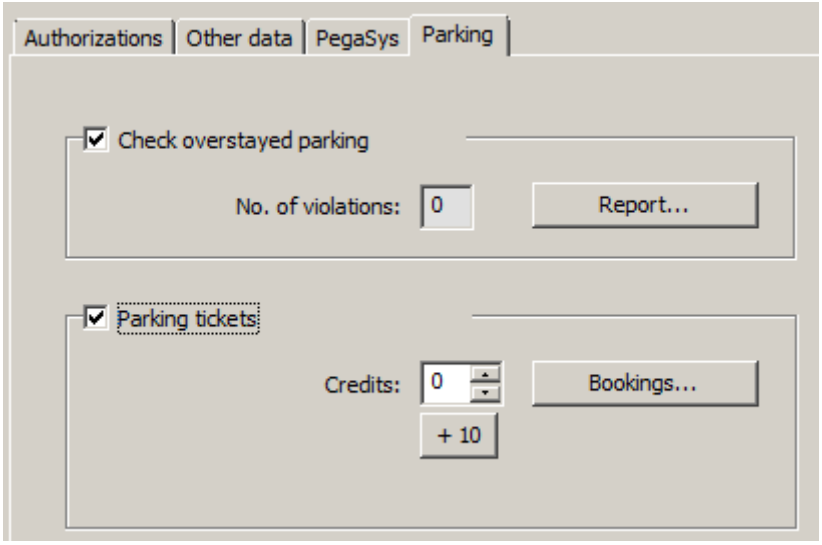
5.1 Overstayed Parking

This feature enables the operator to do the following:
- Detect overstayed parkers,
- Show violations on the terminals of the car parking management,
- Allow the exit of an overstayed parker only after manual release,
- Keep a log of violations,
- Check for overstayed parkers at selected readers,
- Exempt selected persons from checks on overstayed parking.

The car park management feature can detect users who leave their vehicle on the car park for 24 hours or more.

If the maximum period is exceeded, however, the barrier will remain closed when the card is presented, and exit will be denied. A message appears on the workstations of the car park operator. An operator must accept the message, which automatically activates a live video image of the exit concerned. The operator is shown the telephone number of the exit, and can contact the driver directly.

After contacting and checking the driver, the operator can manually release the barrier via his interface but has to provide a comment. The incident will be recorded with time of entrance, time of exit, and the comment.



Detection and handling of overstayed parking

The system records the entry and exit times of each vehicle, as long as the complete system is online. If the LAC is offline it will allow or deny entry depending on its stored data.
- If the driver is exempt from checks on overstayed parking, the MAC allows the exit through the barrier in any case.
- If the driver is not exempt the exit time is compared with the last-recorded entry time of the vehicle.
  - If the complete stay is less than the maximum allowed, the exit will be allowed.
  - If not, the barrier will remain closed and the driver will need to contact the parking lot supervisor to open the barrier manually.

Statistics about overstayed parking

This feature provides an overview of how many overstayed vehicles are in the parking lot.

5.2 Parking Tickets

This feature enables the customer to issue multi-park tickets for a defined number of single parking procedures (configurable).
The authorized user gets a parking ticket that allows him to enter one of the assigned car parks.
Prior to admitting the access to a car park the system checks if there is still a minimum of one parking procedure left on the ticket.

- If this is the case, the access will be permitted and the assets on the ticket reduced by one
- If this is not the case, the access will be denied.

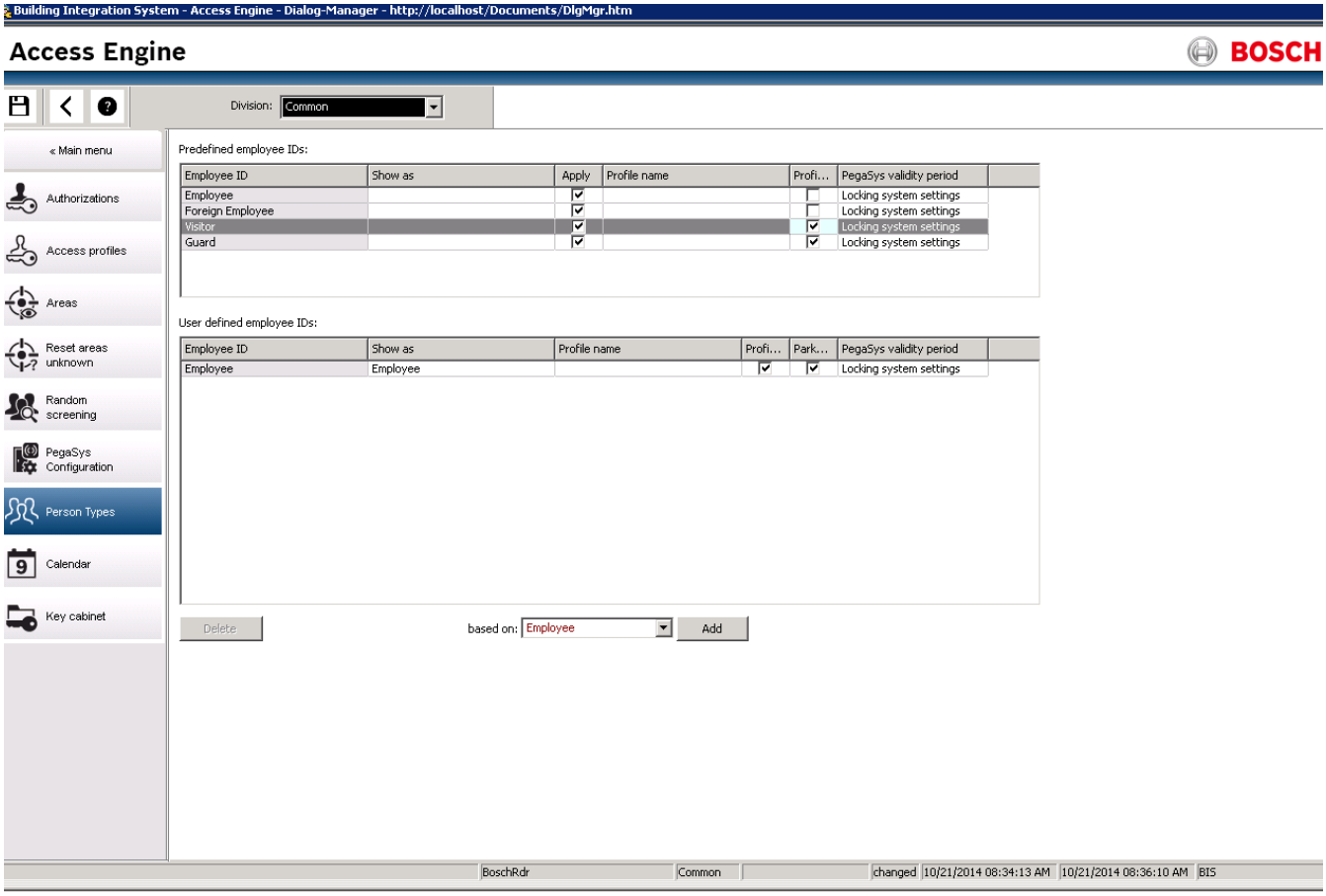
When entering the car park, a time interval will be defined in which the ticket owner is allowed to enter and leave the car park at will. This interval has the same length as the maximum parking period (default: 24 hrs).
Owning a parking ticket means to have permission to use any of the permitted parking zones for one day (24 hrs). Within this period of time it is also possible to change the parking zone or the car park

- If the owner of a multi-park ticket exceeds the maximum parking period, the assets on the park ticket will be reduced accordingly. This can also lead to negative assets! In this case the same rule applies as for overdue parking: the exit must be released manually and the incident will be logged..
- If the owner of a multi-park ticket exceeds the initial time interval (e.g. by repeatedly entering and leaving) without exceeding the maximum parking period, the assets will be reduced by 1, and exit will be permitted.

Assignment of Multi-Park Tickets

For the assignment of multi-parking tickets the following applies:

- Only persons with certain, specified personnel classes are authorized to have a multi-park ticket. This can be parameterized in the **Person Types** dialog.



– If the assets on a ticket falls below an adjustable value (default = 4) the owner will be automatically informed by email.

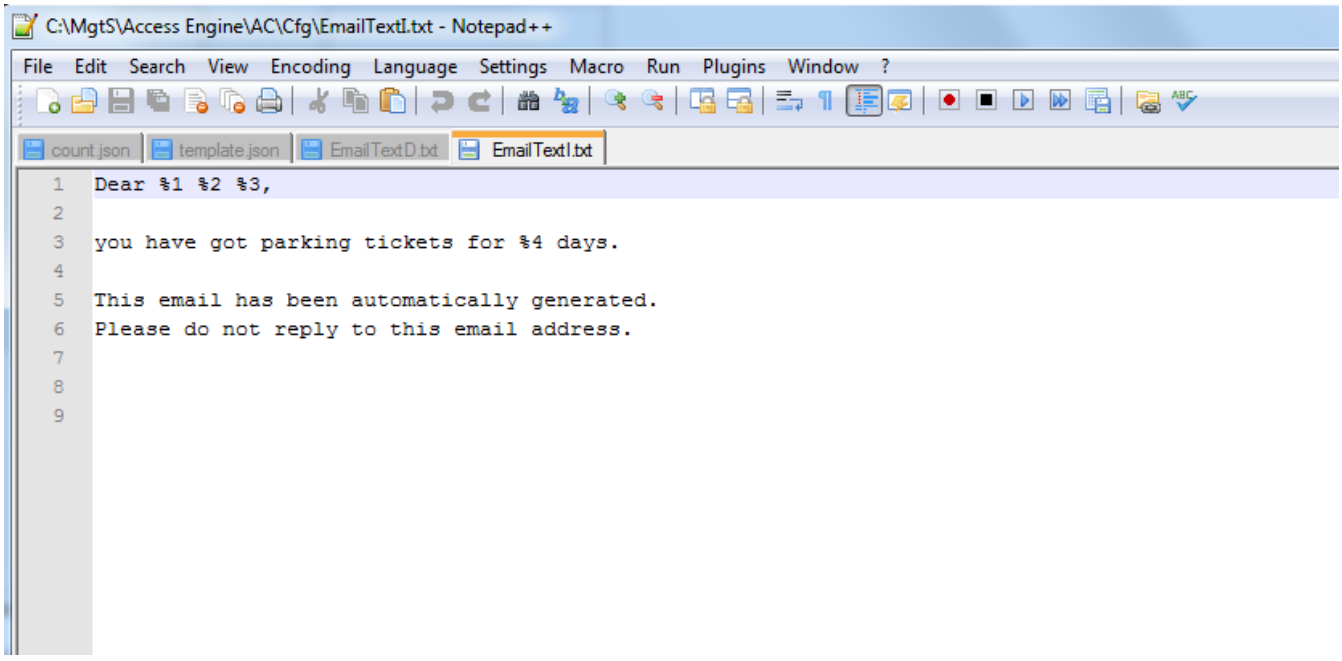
The operator can check the assets of a ticket owner at any time and make corrections if necessary. All corrections will be logged and saved into the database.

The system allows to increase the assets for complete personnel groups by a value of x. The owners will be informed by email.

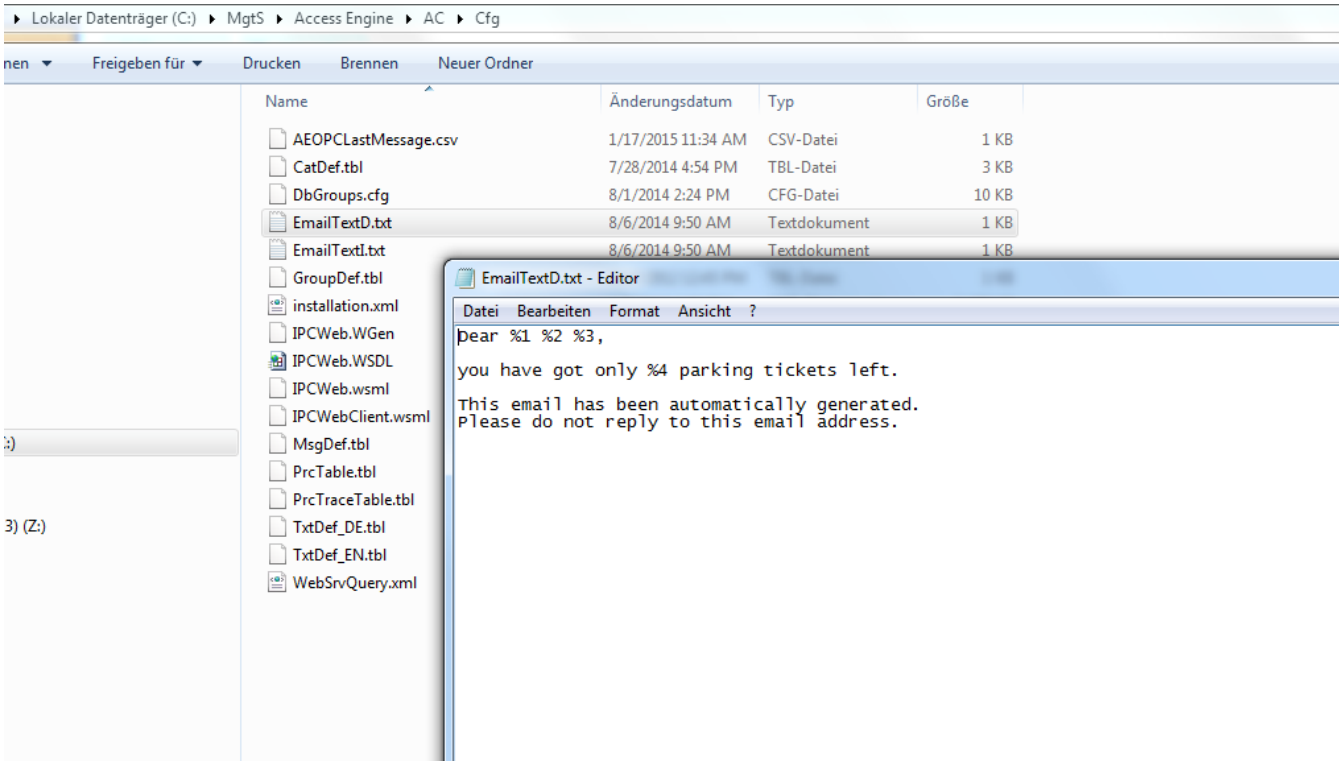
To configure the email message go to your installation directory of the BIS ACE. Select the directory: **<Your path to the installation>\MgtS\AccessEngine\AC\Cfg.**

In this directory you have two choices:

– Edit **EmailTextI.txt** to create a message text that the ticket account has been increased:

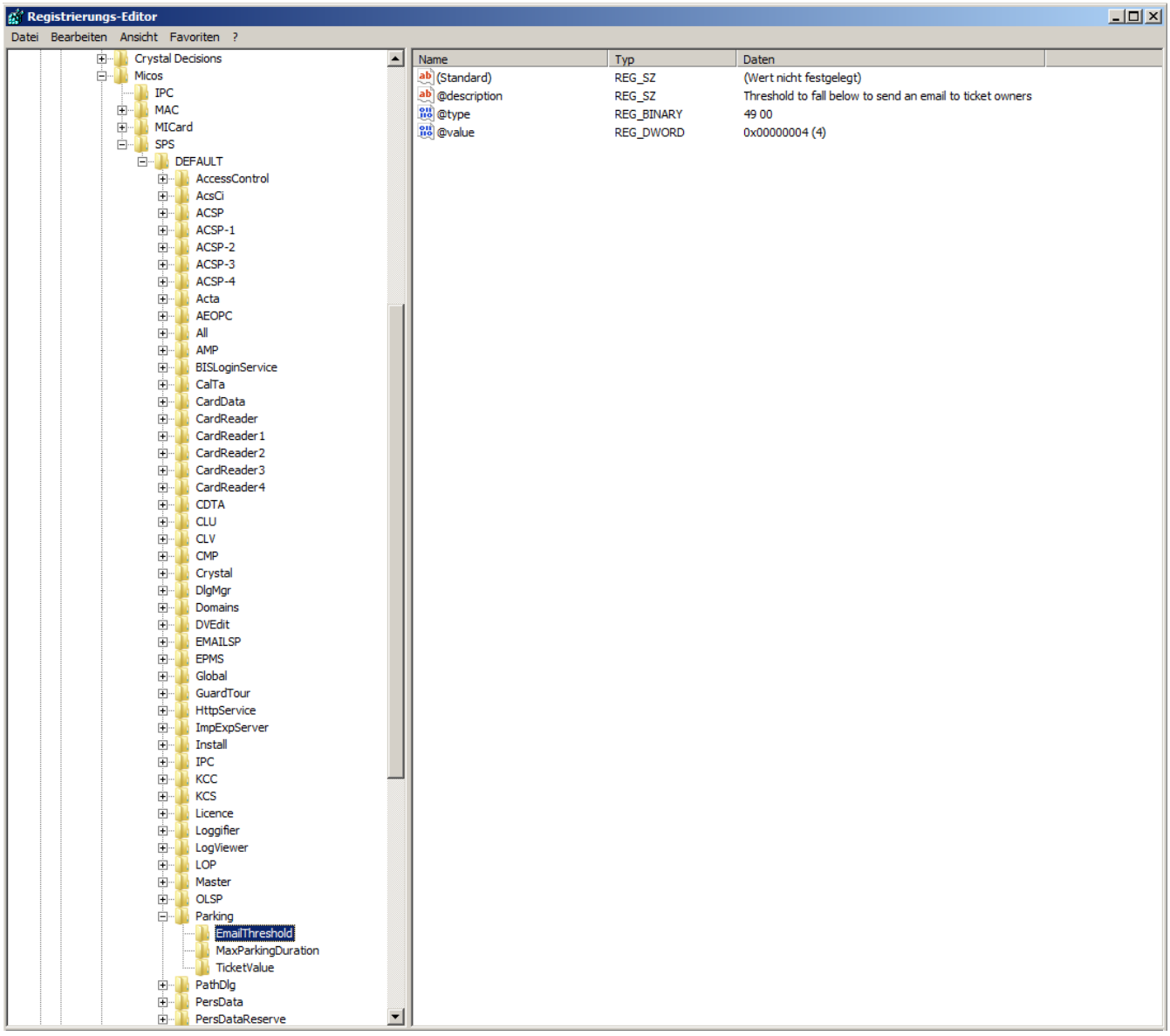


– Edit **EmailTextD.txt** to create a message text that the configured Email threshold has been reached (4 in the example):



Notice!
The wildcards %1, %2, and %3 in the first line of the messages refer to the addressing of the user and will be filled in with the respective card, e.g. “Mr. Henry Average,”.

The limit value itself can be set in the Parking Registry under **Micos\SPS\DEFAULT\Parking \EmailThreshold:**



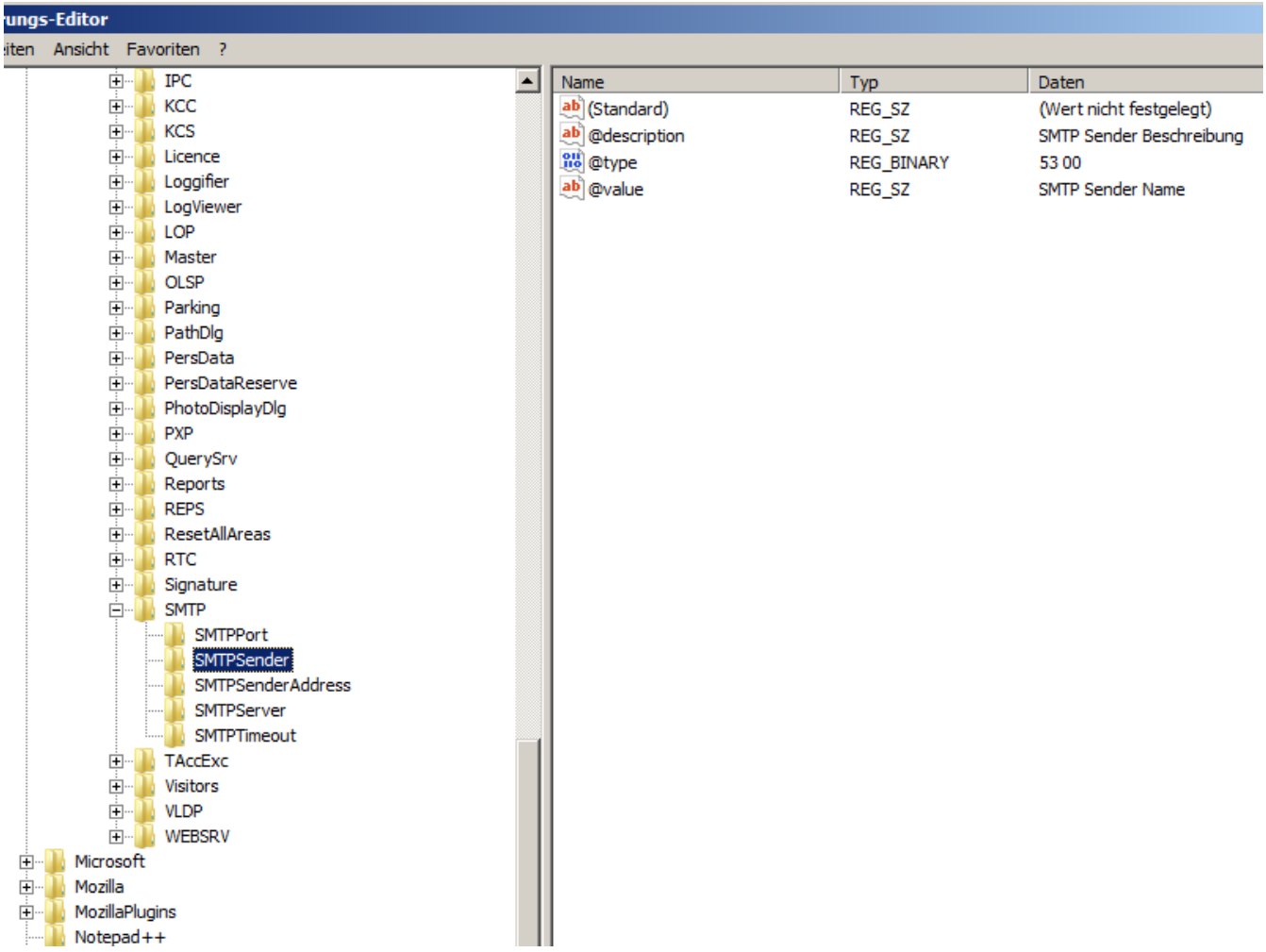
The example shows the default setting of 4.

In likewise manner the two other features under **Parking** can be set:

- **MaxParkingDuration**: Default setting is 23:59 hrs
- **TicketValue**: Default setting 10 parkings.

SMTP Settings

Use the registration editor to configure your **SMTP settings**: for using Email in the context of the car park management



Administration of ticket credits

The current assets of a person gets saved to the database for the owners of multi-park tickets. An entry field **Parking credits** in the **Cards** dialog shows the current value and can be edited. Modifications in this field are logged and saved into the database.

The parking credits can only be edited if the operator has a special permission for the cards dialog (see **Dialog Permission** in the Configuration Browser).

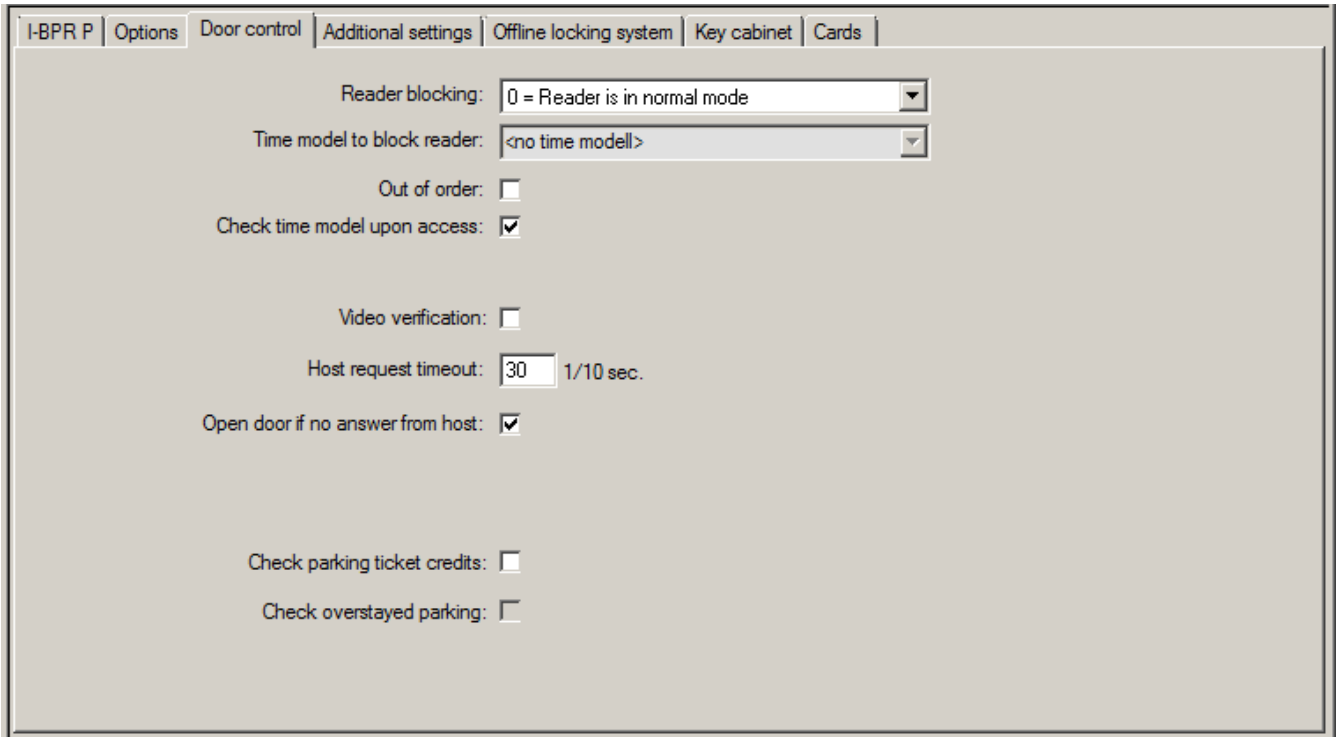
The same special permission is required to use the mass data dialog for this purpose.

Notice!

Several cards per cardholder are possible. The parking assets are saved person related, so a card change will do not lead to a problem for the assets counting.

Credits updated on access

On access of a multi-park ticket owner the system checks the ticket for reduction of the assets. If the assets is 0 or less the access will be denied.



– To configure the ticket check, activate the check box **Check parking ticket credits.**
– **To check for overstayed parking activate the check box Check overstayed parking.**

Prior to admitting the access to a car park the system checks if there is still a minimum of one parking procedure left on the ticket.

– If this is the case, the access will be permitted and the assets on the ticket reduced by one, unless it is a park zone change within the allowed period of time (24 hrs).
– If this is not the case, the access will be denied.

Email notice if fallen below minimum assets

If the assets on a ticket falls below a certain set value (e.g. 4) the ticket owner will automatically be informed by email.

If the email cannot be shipped to the ticket owner, an error message will be sent to the BIS.

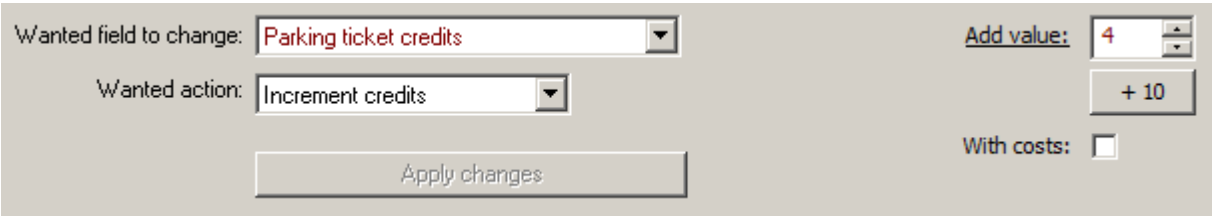
Ticket credits

The personal assets of a multi-park ticket owner is displayed in a field in the Master Data dialog under **Parking ticket credits**.

The operator can edit the value of the ticket assets at any time. Any modification will be logged and put into the database.

The ticket assets can also be modified for whole groups of persons. For this, the entry field **Parking ticket credits** is available in the **Mass Data** dialog. A group of persons is selected via filter functions in the **Mass Data** dialog. Then a delta value (e.g. “n”) is entered in the field **Parking tickets credits**.

This increases the value of parking assets by the value „n“, and the involved persons get an Email which informs them about this.



If the email cannot be shipped to the ticket owners, error messages will be sent to the BIS. All modifications of the parking assets will be collected in the ACE database and provided as report in the dialog under **Parking ticket credits**.

5.3 Export of parking-lot utilization figures

This feature enables the operator to evaluate the utilization of parking lots statistically. The access control system exports parking lot utilization figures to a CSV file at predefined by the operator.
The Export into the CSV file contains data about the utilization of all car parks by the various classed of card owners - i.e. personnel classes. The values are taken in periodical, settable intervals with a length of max 15 minutes.
The data for any point in time are:

- Date
- Time
- Car Park
- Number of parkers, subdivided in:
  - parking zones
  - user groups (personnel classes)

Notice!
If individual card holders change the personnel class, report data from an earlier period will still show the old allocation.

The export path can be set in the system parameter editor under **Default\TAccExc\PB-Dir. As soon as a valid directory was entered one capacity per car park will be exported.**

5.4 Export Mobile Validity check

Prerequisite
This feature requires a separate license.

Overview
This feature enables the operator to check the parking authorizations of vehicles on the parking lot.
A CSV file is generated in regular intervals which contains all ticket owners together with additional information about the car park zones. .
For configuration select the system parameter editor under **Default\PXP\Task0001...** and switch on the export path, file name, and export explicitly (or off respectively).

The export is performed at configurable intervals. The exported data are:

- Validity of the card (entry field **valid until** in **AC Persons**)
- Name of the authorized person
- Car registration number
- Registered card numbers
- Phone number
- Card status
- Name of the car park or parking zone if applicable
- Reserve fields (optional if configured)

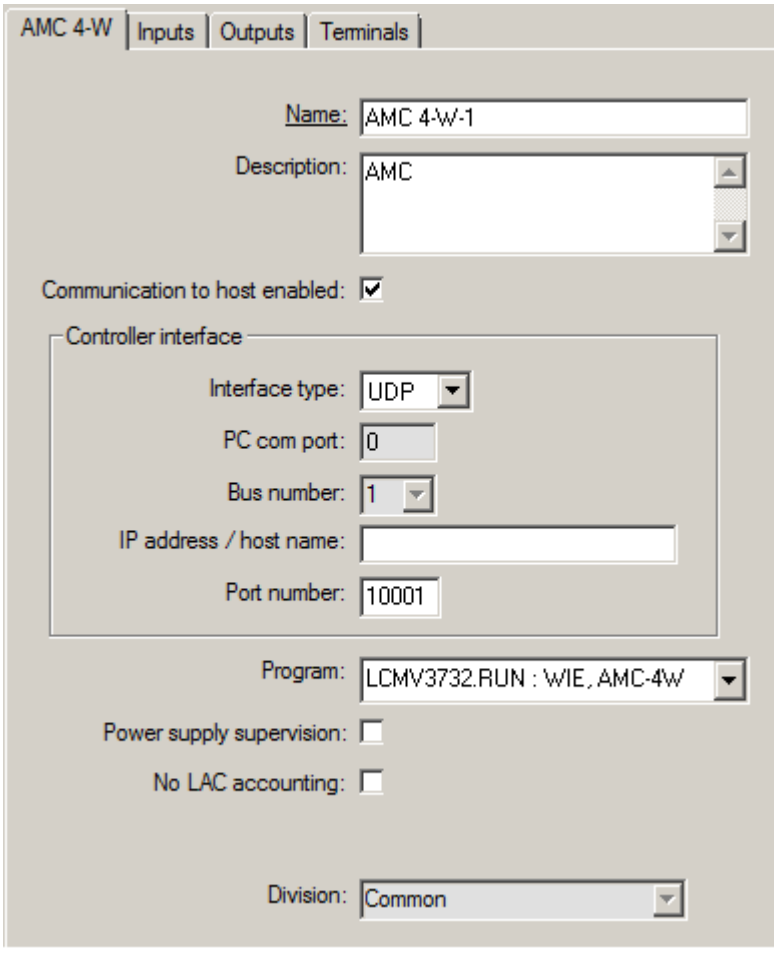
5.5 Authorizations for several park zones

Some car parks have zones for handicapped and non-handicapped drivers. In this case the following rules apply:

– Owners of season tickets are only allowed to drive in as long as there are still parking bays for non-handicapped persons available.
– Handicapped persons are allowed to drive in as long as there are still parking bays for handicapped or non-handicapped persons available.

Notice!
This presupposes that the ticket owners follow the rules. This especially means that:
Non-handicapped persons do not park on a parking bay for the handicapped
Handicapped persons use the parking bays for the handicapped as long as they are available

A person who has several authorizations can access both, if handicapped or not. The AMC tries to book in the person in according to the configured sequential order of parking zones. In case one zone is full, the search for the next authorized and free zone will proceed.
Counter calculation in MAC and AMC:
1) One AMC controls all entrances and exits of a car park:
=> The AMC counts on its own and can be corrected by the MAC when going online.
2) Entrances and exits of one car park are divided up onto different AMCs:
=> The MAC counts for the AMC in case of online operation. When operating offline, the AMCs permit the access (if configured accordingly) but don’t count.
If several AMCs control one car park, activate the checkbox **No LAC accounting**.in the AMC configuration



5.6 Parking lot report

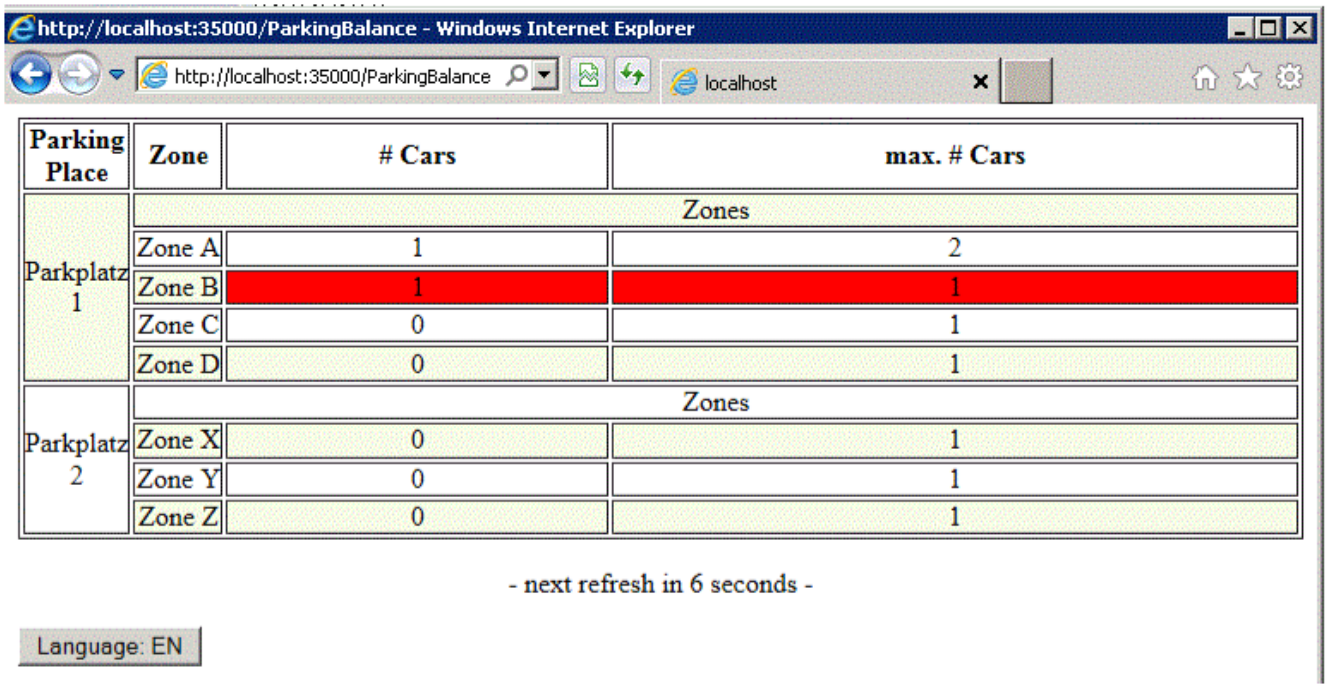
This report shows the current occupancy of areas that are designated as parking areas. Select **Parking lot occupancy** from the list of layouts.

Dialog path
Reports > **Reports system data** > **Areas**

Parking lot list Date 08.11.2013 , 14:51:23 Page 1

Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

A second example **Parking Balance** shows what is possible with the web server. All parking places are shown including the current usage counters for all parking zones. Furthermore the example contains a language selection button to show how easy the language could be toggled between German and English. The localization is only done inside the web page only.



5.7 Extended parking-lot management

Introduction

The operator can adjust the number of parking spaces in a parking area in order to compensate for vehicles of non-standard sizes, for example:

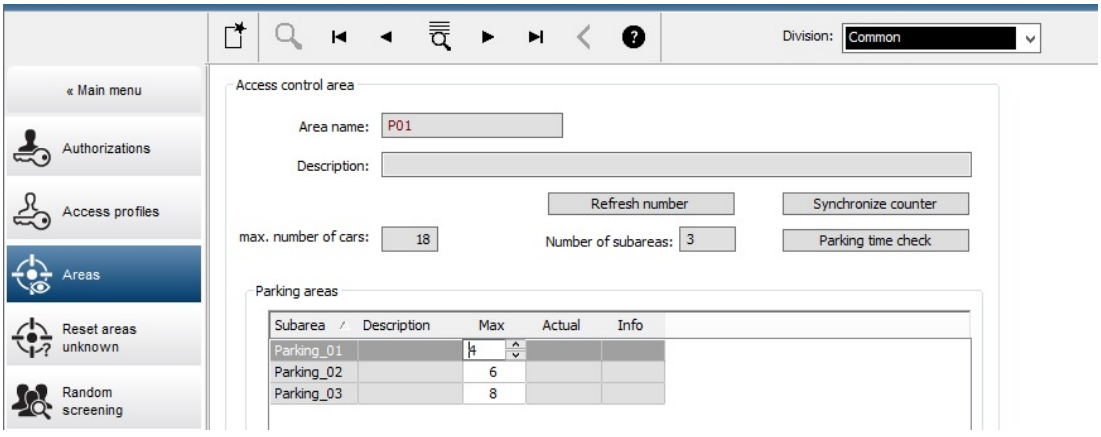
- Trucks
- Handicapped access
- Motorcycles

Dialog path

Main menu > **System data** > **Areas**

Procedure

1. Select a parking area
2. In the **Parking areas** pane, adjust the value in column **Max** to the new number of parking spaces for that area.



Notes:

- Settings made in the **Max** column override the settings made in the **Areas** configuration. See **Configuring areas for vehicles** at the link below.
- A zero *0* in the **Max** column means Unlimited; all vehicle counting is switched off.

6 Offline doors - Managing Personnel Data

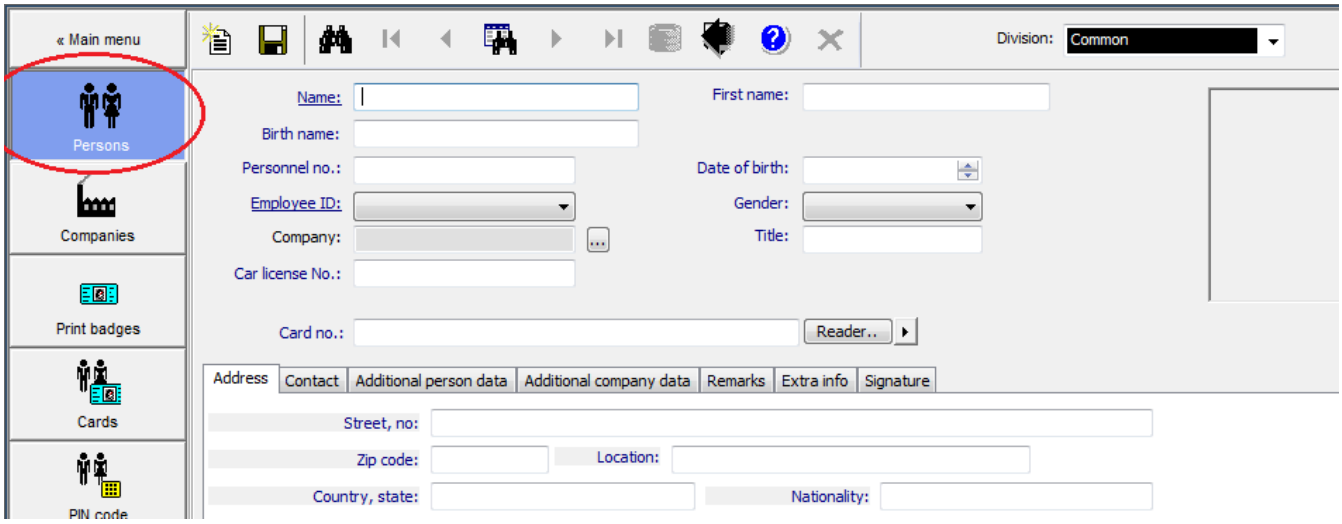
The database of the main access control system is used to store personnel data for the offline system as well.
Accordingly this data is entered via the access control system dialogs, and each cardholder for the offline system requires a valid card for the online access control system

6.1 Adding personnel data

Online data

To add personnel data and assign online authorizations, follow the steps below:

1. Switch to the dialog manager of the main access control system.
2. Open the dialog the **Personnel data** > **Persons**
3. Enter at least the mandatory data for the person.
4. Save the new record.



5. Create a badge in the **Print badges** dialog, if there is not one available yet.
6. Switch to the **Cards** dialog.
7. If an **enrollment reader** is already configured in the system, select it.
8. Press the **Record card** button to register the card in the system.

Offline data

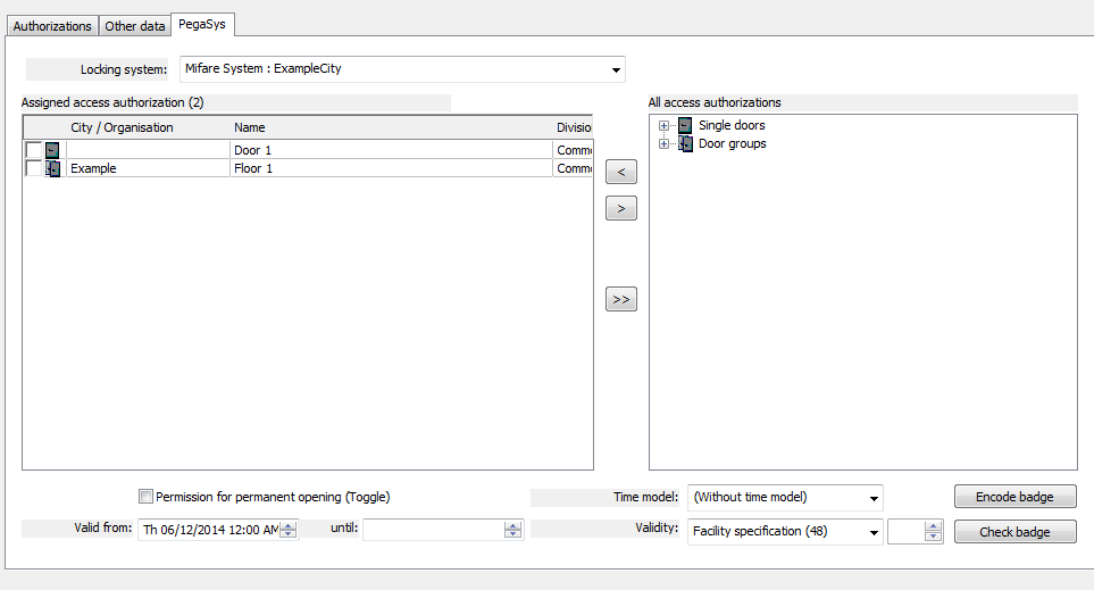
The corresponding authorizations for the locking systems are allocated separately.

1. In the **Cards** dialog, switch to the **PegaSys** tab with the selected personnel data.
2. Select the relevant locking system from the upper drop-down list - the doors and door groups set up for this system are displayed in the **Available access authorizations** list field.
3. Double-click to add individual entries or select several list entries and press the left arrow button to add the required doors and door groups. Repeat steps 2 and 3 for other systems - the selections made previously are retained. The authorizations for a maximum of three systems can be saved onto one (HITAG) card.
4. If necessary, overwrite the parameter values (validity dates, time model, etc.) if you do not wish them to have default values.
   - **Permission for extended unlocking (toggle)**:
     If the parameter **Extended unlocking (toggle)** is set on the door, then the cardholder can unlock that door for extended periods by presenting his badge at the read terminal for three seconds.
   - **Valid from:**

This field contains the current date and time by default, but these can be overwritten with future dates.

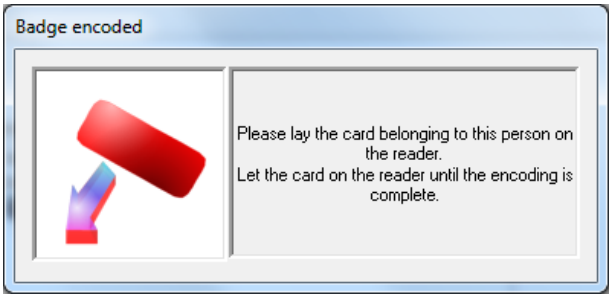
- **Valid until:**
  A date that specifies an absolute validity period for rights can be entered in this field - e.g. calendar year.
  Any date entered here supersedes information in the **Validity** field.
- **Time model:**
  One of the offline time models can restrict use of the badge to the times defined by the parameters.
  [time model no. 1 is not included in the selection list. It cannot be assigned to personnel.]
  The **Time check** parameter must be selected for the terminal.
- **Validity:**
  The default value specified when the system was configured is displayed in the default settings. This value can be modified individually for each cardholder.
  The validity period can be defined in different ways and on different levels - see also *Special settings, page 84*.

5. Writing to the card
6. Choose one of the following options:
   - Place the badge on the read-write unit at the workstation and press the **Encode card** to initiate the write process. [The system automatically activates the dialog reader for the offline system without you having to select it beforehand.]
   - Alternatively, the badge can also be encoded on one of the online readers (DELTA 7020/1000/1010).



Notice!
The validity limits of the online access control system apply to the offline system and take precedence in case of conflict.

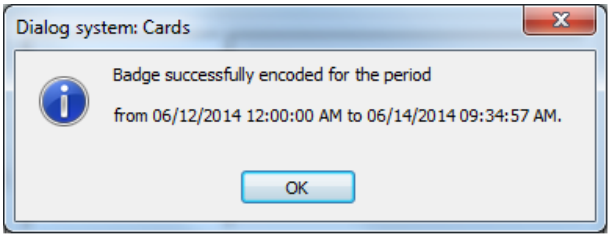
Data check during write process
When the Encode card button is clicked, a dialog box appears prompting you to place the card on the read-write unit.



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

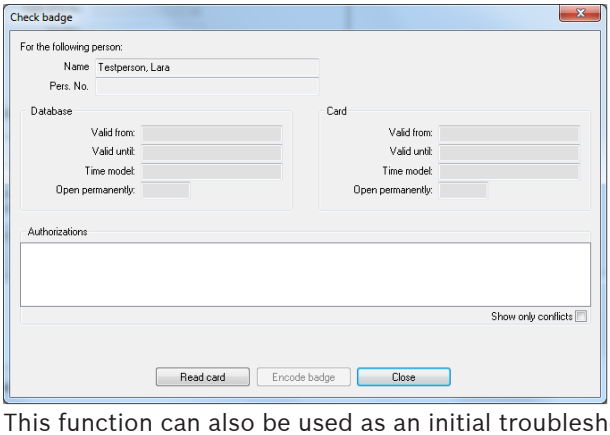
– No card is place on the unit or the code data cannot be read.
– The card is not a user card.
– The card does not belong to the selected person.

Display of the validity period indicates that the write process has been successful. The current date and time of 00:00 are used as a start time to ensure access even to terminals showing the incorrect time.



Validating cards

Pressing the **Validate card** button opens a dialog that validates the authorizations just encoded on the card by comparing them with the database.



This function can also be used as an initial troubleshooting measure, for example if a card does not work. One reason for malfunctions is data conflicts between card and database.

1. Select the relevant record from the database using the search fields in the dialog header.
2. Press the **Validate card** button on the **PegaSys** tab to open the **Check authorizations** dialog.
   Data for the selected person is entered in the **Name** and **Pers. no.** fields as well as the fields in the **Authorizations in the database** dialog field.
3. Place the badge on the dialog reader for the workstation.
4. Now press the **Read card** button at the bottom of the dialog.
5. Compare the **Authorizations in the database** with the **Authorizations on the card**.

If the comparison reveals differences in the dates, the badge should be encoded again. The displayed dates do not have to match exactly. Rather the dates on the badge should fall completely within the validity period in the database.

6.2 PegaSys - Blocked cards

If the dialog authorization is valid, the **PegaSys Blocking** dialog appears in the **Personnel data** menu. When the locking system is selected, a list of currently invalid user cards is displayed on the right.

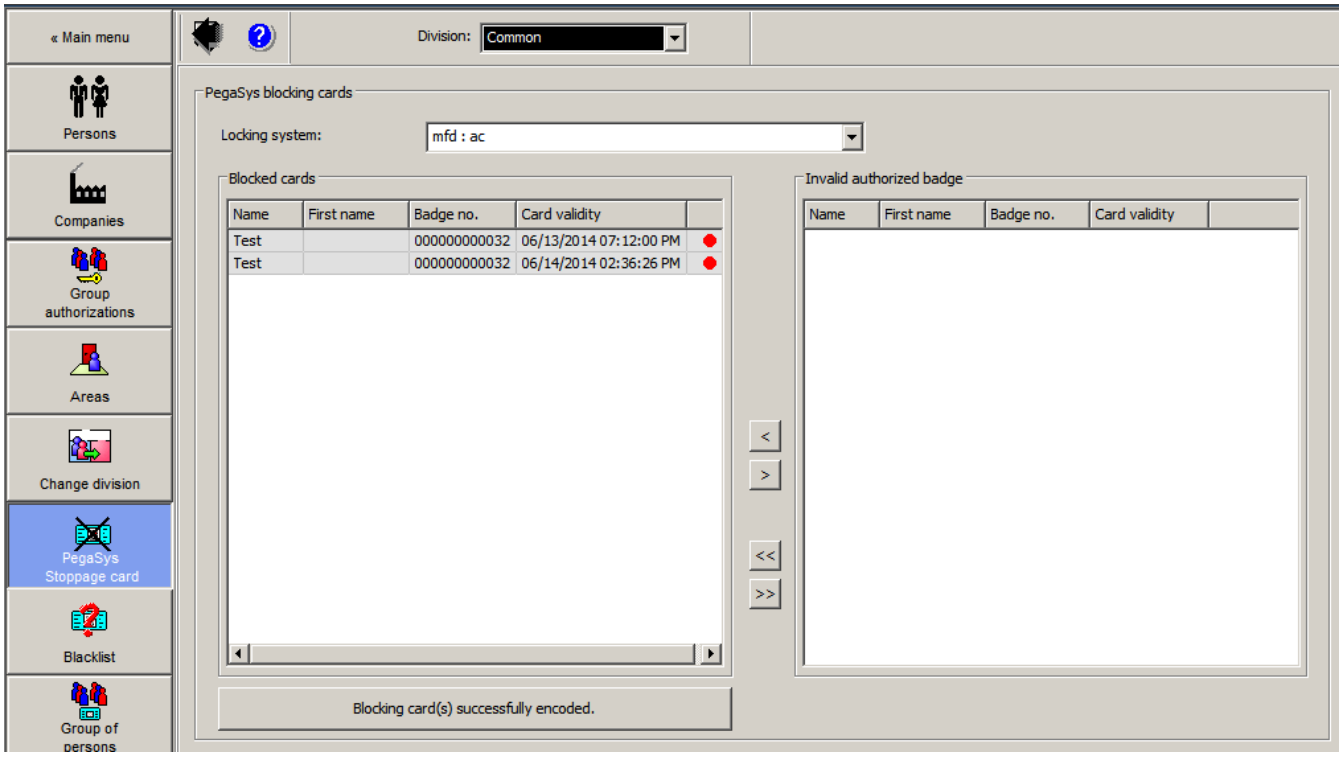
Currently invalid means:

– Personnel who have been actively blocked but whose cards still have active authorizations.

– Personnel whose card's validity has been terminated online but where the cards themselves still have active authorizations.

The offline terminals only have a limited memory for the entries in the blocked cards list. Therefore user cards that are to be blocked must be selected manually.

The expiry date of the user card is displayed in the **Card validity** column. Entries in the **Invalid authorized badge** list can be added to the Blocked cards list using the arrow buttons.



Pressing the **Encode** button adds the entries to so-called Blocking Cards. These encoded Blocking Cards must then be read into the offline terminals. Only then it is no longer possible to use these badges on these terminals.

The left list also provides an overview of which badges are currently on the PegaSys blocked list. A green/red lamp indicates whether or not the relevant entry can be removed from the list again.

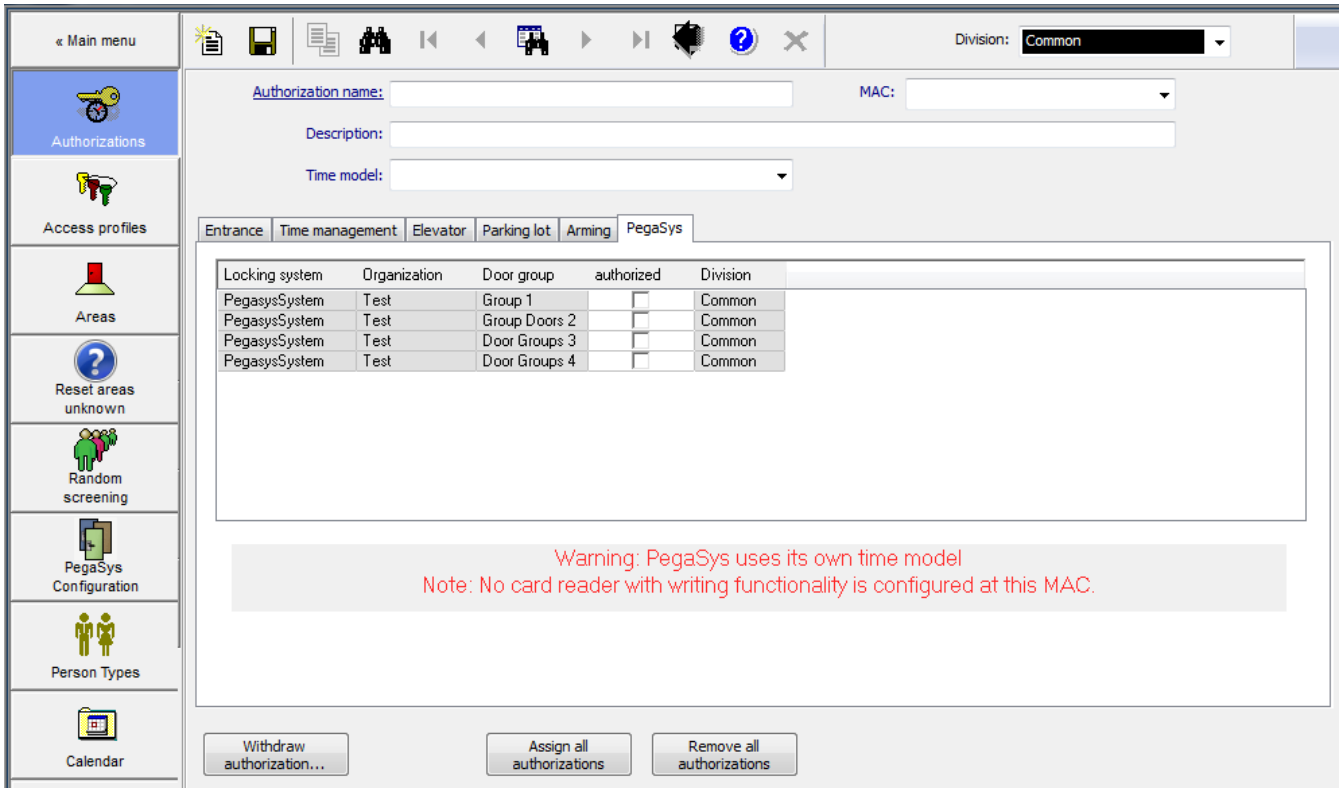
– Red
  Card should be blocked.

– Green
  Card either re-authorized or expired and therefore no longer active.

The green entries are removed automatically the next time the blocking cards are encoded.

6.3 Online/offline access authorizations

The **Access authorizations** and **Room/time authorizations** dialogs in the **System data** menu contain a tab named **PegaSys**. All defined door groups (not individual doors) are listed in this tab.



Door groups of the offline locking system can be assigned to any access authorization in the online system. In order for the cardholder to access the door group, their card must be re-encoded.

Door groups that were assigned as a result of the access authorizations cannot be removed in the **Cards** dialog.

This also applies for the room/time authorizations, even though the time models for the online system do not apply to offline installations. This is highlighted in a message under the list field: **Note: PegaSys uses its own time models]**. In terms of offline authorizations, there is no difference between access authorizations and room/time authorizations - online room/time authorizations and offline authorizations are grouped together here.

6.4 Offline data on Temporary cards

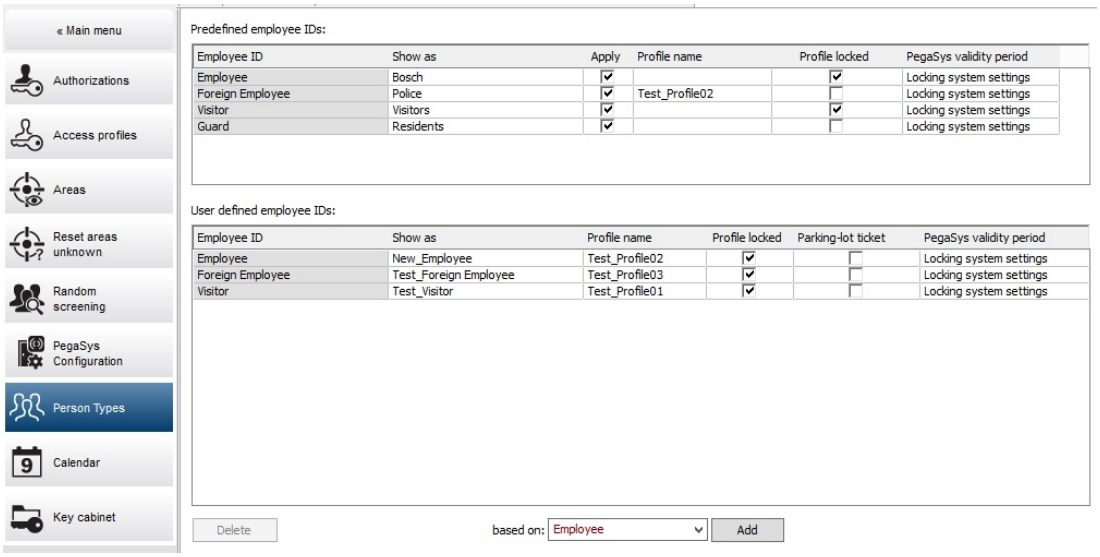
Avoid putting offline data on temporary cards

Online access control systems can generate temporary replacements for cards, potentially including cards containing offline data. The offline data will remain valid on the card even when the online data has expired.

To prevent possible security breaches, it is safest to ensure that you do not generate temporary cards for cards containing offline data.

6.5 Personnel classes - Validity period

If software for the offline locking system is installed, the additional column **PegaSys validity period** is displayed in the two list fields in the **Personnel classes** dialog.
If the relevant personnel class is selected when creating new personnel records in the **Persons** dialog, the validity period specified here is assigned to the offline authorizations. This validity period supersedes the default validity period that can be set when the offline locking system is configured.
The validity period can be defined in different ways and on different levels - see also *Special settings, page 84*.



Clicking the corresponding line in the **PegaSys validity period** column opens a dialog for selecting and setting a new value.

6.6 Status bar in main access control system

In addition to the displays for the access control system (Known, Blocked, Currently not valid and Random screening) the status bar also contains a colored visualization of the authorizations for the offline system (PegaSys).
This display and varying captions indicate the following states according to the processing state of the offline data.

LED	Caption	Meaning
	PegaSys	This card is not defined for the offline system.
	Encoded	A card with valid authorizations was encoded.
	Expired	The validity period for the offline system has been exceeded.
	Not current	The validity period for the offline system has not yet started - the start time is in the future.

6.7 Lists for offline data

The **Reports > Reports master data** menu in the main access control system has been extended to include the **Persons PegaSys** dialog, which allows users to print offline data.

Filter options

- **Personnel data**
  Individual people or groups (e.g. all personnel from a company/department) can be filtered out using the input fields.
- **Offline elements**
  - Locking system
  - Door groups
  - Doors
  - Organization (= grouping door groups)
  - Area (= area where door is located)
- All filters can be combined with one another.

Layout selection

The layout determines how the search results are displayed and which information is included. Four predefined list layouts are available.

Persons with doors/groups	Every person who has been assigned authorizations is listed together with the most important access control data. A system, location, and doors/door groups are listed for each person.
Doors with persons	The persons authorized for each door are listed and sorted according to the system.
Door groups with persons	The persons authorized for each door group are listed and sorted according to their offline systems.
Crosstab persons	Table view. The columns contain the designations of the doors and door groups (G), while the lines contain the names of the persons from the offline system. A cross (X) at the intersection of a column and a row indicates an existing authorization.
Event log by doors	All bookings (containing personnel information) at these terminals are listed according to their respective doors.
Logbook by person	All doors at which persons have booked are listed by person.

Blocked cards	List of all PegaSys cards that will be blocked or unblocked by the next encoding process.

6.7.1 PegaSys data in online reports

The reports

- Access authorization for each person
  with a display of PegaSys authorizations in the form:
  - Individual door, location, system
  - Door group, organization, offline system
- Access authorizations and room/time authorizations
  with a display of PegaSys authorizations in the form:
  - Door group, offline system

contain information about the PegaSys system.

6.8 Special settings

Unlike online systems, authorizations for offline locking systems are only allocated for relatively short periods and must be renewed and extended at regular intervals. The validity period can be defined in three different ways and on three different levels.

1. Individual setting for each person.
   See *Offline data, page 77*.
2. Assignment via personnel class.
   See *Personnel classes - Validity period, page 82*.
3. Specification of a default validity period for the entire locking system.
   See .

The sequence specified reflects the relative importance of the information. An individual setting supersedes personnel class assignments and settings of the locking system. Personnel class assignments supersede settings of the locking system.

7 Offline doors - Description of Procedures

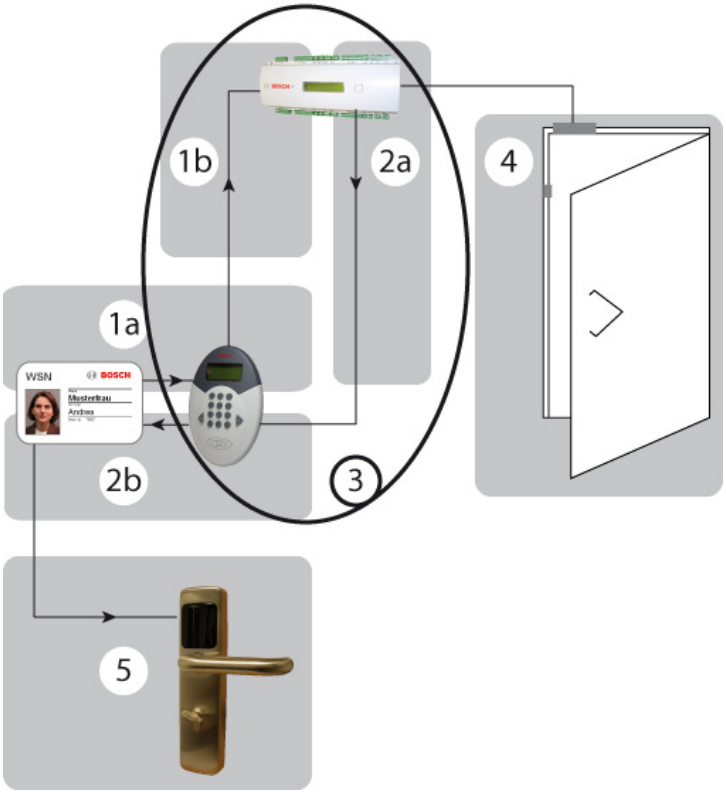
The following procedures for offline / online hybrid systems differ from those for pure online systems.

7.1 Data creation

The following procedure is recommended for new objects.

1. Definition of door groups
2. Definition of time models
3. Definition of terminals (doors)
4. Management of Personnel Data
   - Adding personnel data
   - Authorization allocation - online (optional)
   - Card allocation - online
   - Authorization allocation - offline
   - Card encoding - offline

7.2 Access



1a Read card

1b Card number sent to the AMC

2a Current data shared with the reader

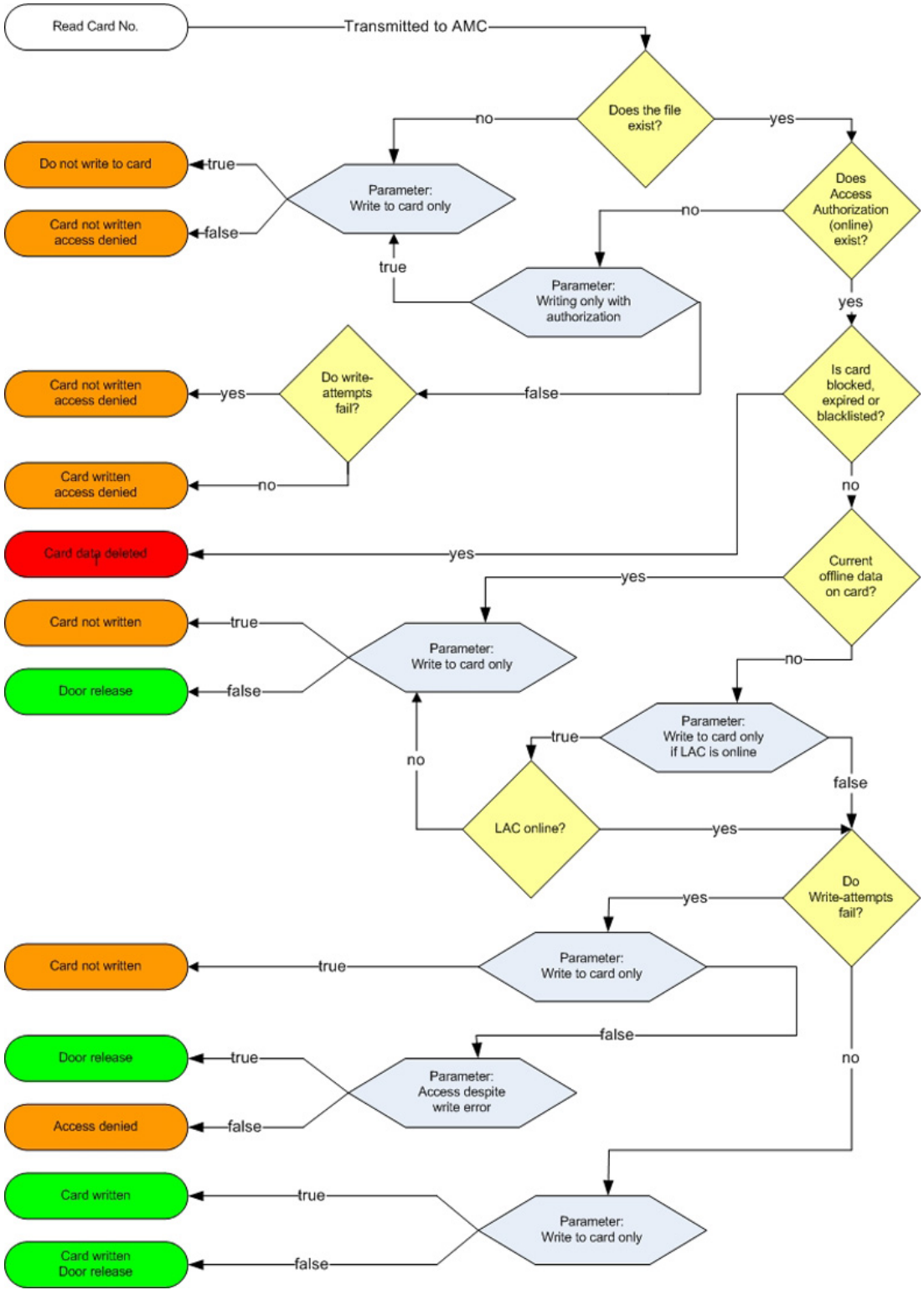
2b Current data written to the card

3 For details on the validation and write process on the AMC, please see the flow diagram in *Write process, page 86*.

4 Door release for the online system (if configured)

5 Authorization check at door terminals

7.2.1 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 and the preset writing rules (see also Configuring the read-write unit) are used to determine a point in time until which the badge data is considered valid.
In the default setting, the data is only updated when two-thirds of the validity period have expired.

Example of default writing rules
Validity period: 1 day = 24 hours
2/3 of the validity period: 16 hours
If a cardholder scans the card when he starts work and his expiration date is updated, he can pass the read-write unit for the rest of the day without a new write process being triggered - the data is only updated after sixteen hours.
This ensures that the validity period is only updated once a day, for example.

8 Offline doors - Application Examples

The following examples demonstrate parameter settings for special requirements. Each example deals with one specific parameter.
Other variations can be produced by combining parameter settings. Hence the examples can also be combined with each other.

Access control reader and/or write-capable reader?
The decision regarding the way in which the DELTA 7020 is used depends on a number of different factors; it can make sense to omit the reader from the access control system (online).

- Is there an entrance (e.g. main entrance) that must be passed by most of the cardholders?
  - **Yes**: A DELTA 7020 with simultaneous access control function for the online system is recommended.
  - **No** (There are a number of possible entrances, for example): The use of DELTA 7020 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 DELTA 7020 (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 DELTA 7020 will suffice for ad hoc extensions.

Example 1: Read-write unit only
Ideally a hotel should be accessible to everyone, at least as far as the reception desk. Therefore, access control readers are mainly installed at doors that require particular security, in the event that the settings in the **Example 2** in Single doors or door groups (see below)are not sufficient.
Accordingly, the DELTA 7020 is not linked with access control functions; instead, it is configured purely as a read-write unit for the offline system.
Condition:
The **Reader function** parameter in BIS Configuration Browser > Connections > ... > Offline locking system must be set to **Write locking system** and the **Write to card only** check box is selected.
The DELTA 7020 needs only to be installed in a central location for hotel personnel, so that their authorizations can be updated and extended. If possible, choose a location that all affected persons pass on a regular basis, e.g. staff room.
For hotel guests, authorization for the hotel room door is assigned at check-in, and written to the card via a DELTA 7020 at reception. Authorizations normally need not be changed, but this can be carried out at reception if required. Hence the reader need not 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 DELTA 7020 can simultaneously update and extend locking system rights for authorized persons.
Condition:
The **Reader function** parameter must be set to **Write locking system** and the **Write card only** check box is cleared.

If the **Write without access rights** check box is not selected, then 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 as well as belonging 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.

Condition:

The **Check door groups** parameter must be selected (checked).

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.

Condition:

The **Check door groups** check box must be cleared.

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

More holidays per year

The maximum limits for holidays (= 10) and holiday periods (= 2) are based on the permitted volume of data that can be saved simultaneously in the terminals via initialization cards.

It is possible e.g. to define more holidays and holiday periods throughout a period of one year, albeit with a slight increase in the administrative workload.

Example

At the end of 2007, the dates of ten holidays for the 2008 calendar year were stored in the terminals. At the start of April 2008, the holidays that have already passed (e.g. New Year's Day, Good Friday, Easter Monday) can be deleted and replaced with three new dates.

This new list must be distributed back to the terminals via the time initialization cards.

Normal or extended unlock

If the badge is valid, the LED on the terminal flashes green three times. The door may be opened within a predefined unlocking pulse of 3 seconds (default value). If the door is in **extended unlock** mode, the LED also flashes green three times when a valid badge is presented.

A card with the **Permission for extended unlocking (Toggle)** unlocks the door normally if the card is removed during these three flashes. If, instead, the card is held to the terminal's read unit for longer than 3 seconds, then a continuous green signal is displayed and the door remains unlocked until a card with extended unlock authorization is held to the terminal again for at least three seconds. The door is then locked; i.e. access is only possible with authorized badges.

Condition:

The **Extended unlock (Toggle)** check box must also be selected for the terminal.

By time model:

The same function can be controlled via a time model. A time model is selected for the **Opening hours model** door parameter and the door is unlocked between the "from" time and the "until" time.

Time models with the same "from" and "until" times can be used to lock doors that are in extended unlock mode.

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 extended unlock/lock**
   The office is unlocked each morning using the extended unlocking function and made accessible to the public. When the office closes, extended locking comes into effect. Thereafter only people with a valid card have access.
2. **Extended unlock/lock controlled via a time model**
   If the public visiting hours are not the same as the staff hours, door locking and unlocking 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. **Extended locking controlled via time model**
   The office is unlocked manually each morning by the first staff member to arrive, using the extended unlocking function. A time model with identical "from" and "to" times is used to perform extended locking and unlocking at those times.

Refer to

– *Single doors or door groups, page 89*

9 Guard tours and Patrols

Introduction to Guard tours

A **Guard tour** is a route around the premises, punctuated by card readers, where persons of employee-type **Guard**, must present a special guard card to prove that they have physically visited the reader.

Guard cards do not open entrances, but are used solely for tracking. To open entrances the guard requires an access card in addition.

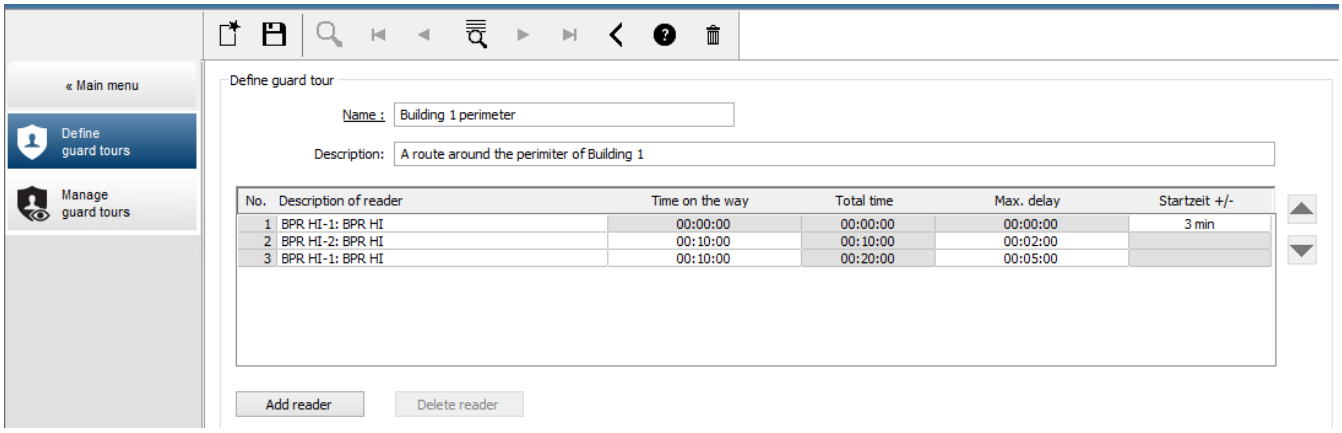
The Guard tour consists of a series of readers with the approximate walking times in between. The maximum tolerable delay between readers, and the tolerable deviation (+/-) from the start time, are also attributes of the Guard tour. Deviations outside of these defined tolerances can potentially trigger alarms, and are recorded in **Patrols**.

Introduction to Patrols

A **Patrol** is the traversal of a Guard tour at a particular date and time. Each patrol is created and recorded as a unique entity in the system, for forensic purposes.

9.1 Defining guard tours

Select **Guard tours** > **Define guard tours**

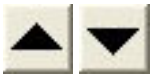


- In the text field **Name**, enter a name for the Guard tour
- In the text field **Description**, enter a more detailed description of the route (optional).

Adding readers to the guard tour:

1. Click the **Add reader** button.
   A line is created in the table.
2. In the **Description of reader** column, select a reader from the drop-down list.
3. Enter values for tolerable deviations:
   - If this is the first reader in the sequence, under **Start time +/-** enter a number of minutes earlier or later that would still be tolerable as start time for a patrol on this guard tour.
   - If this is **not** the first reader in the sequence, under **Time on the way** enter the time (hh:mm:ss) required for the guard to travel between the previous reader and this one.
     The total time for the tour, excluding delays, is accumulated in the **Total time** column.

4. Under **Max. delay** enter the maximum amount of additional **Time on the way** that is still tolerable without causing a patrol to be marked **Delayed**.
5. Add as many readers as required. Note that the same reader can occur more than once if the guard tour passes it multiple times, or returns to it.

– To delete a reader from the sequence, select the line and click the **Delete reader** button.
– To change the position of a reader in the sequence, select the line and click the up/down  buttons.

9.2 Managing patrols

Select **Guard tours** > **Manage guard tours**

Scheduling a new patrol

To schedule a patrol along a particular guard tour proceed as follows:

1. Ensure that you have the desired guard card for the patrol, and access to a configured access card reader or directly connected enrollment reader.
2. In the **Guard tours** column, select one of the guard tours that have been defined.
3. Click the **New patrol...** button.
   A pop-up window appears.
4. In the pop-up window, if desired, change the guard tour in the drop-down list.
5. If the patrol is to have a predefined start time, select the check box **Set start time:**
   – Enter the start date and time.
   – If desired, click the spin box **Start time +/-** to adjust the tolerance for late or early starts.
6. Click the right arrow and select the reader that you want to use to register the guard card. Note that the reader must be already configured in the system before it will appear here for selection.
7. Click the green plus button to start reading the guard card, present the card at the reader and follow the popup-instructions.
   The guard card is recorded for use in the patrol.
8. Repeat the previous step to record alternative guard cards for this patrol. Note however that the first card to be presented during the patrol must be used at all the readers during that patrol.
9. Click **OK**. The selected guard tour will be marked as **planned** in the list.

Tracking a patrol

All planned and active patrols move to the top of the list. If multiple patrols are planned or active, the selected patrol is framed in red. Click on the frame to get further information.
A patrol starts when the guard presents his guard card at the first reader in the guard tour. This card must be used for the rest of the patrol, even if alternative cards were defined for the patrol.
The **State** of the patrol changes to **Active**.
Every reader that is reached on schedule receives a green check mark - ✔. The scheduled and actual times between readers in the currently selected patrol are displayed in the lower half of the dialog window.
Every reader that is reached later than the scheduled time plus **Max. delay** receives a red mark. The patrol is marked as **Delayed.**

In this case the guard calls the operator to confirm that there is no problem. The operator then clicks the **Resume patrol** button. The reader receives a green check mark with an additional "c" -  . The guard can now continue the patrol at the next reader.
If there is an unforeseen but harmless delay in an active patrol, the guard can call the operator to adjust the schedule. Enter the minutes of delay in the **Delay (min)** spin box and click the **Apply** button.
If a patrol cannot be completed as scheduled, the operator can abort it by clicking the **Interrupt** button. The **State** of the patrol changes to **Aborted**, and it drops below the planned and active guard tours in the list.

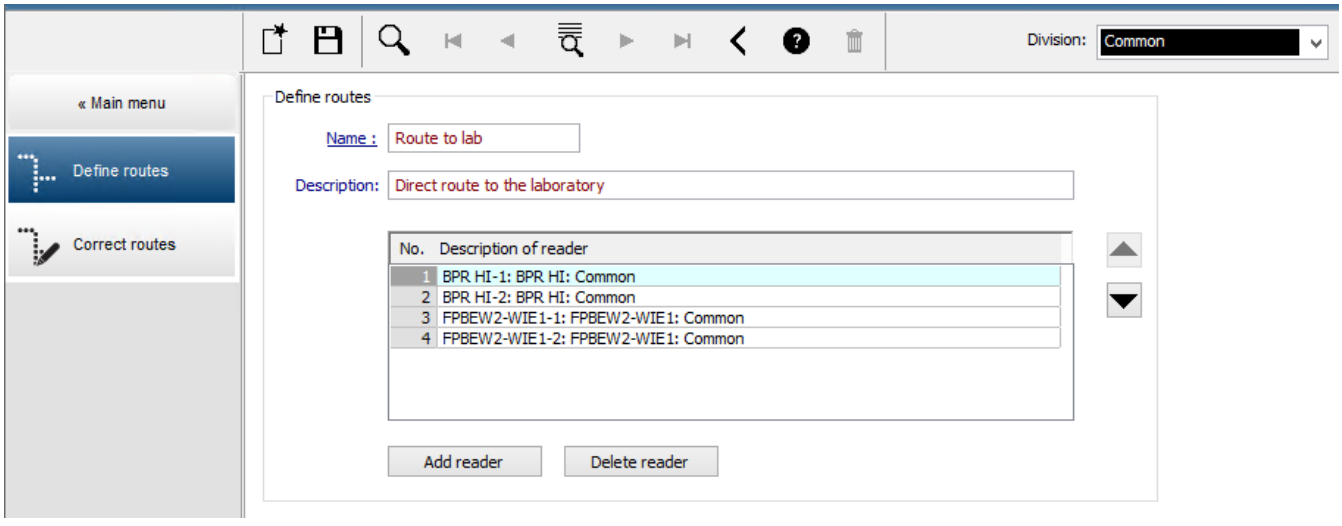
9.3 Tour monitoring (formerly Path control)

Introduction

A Route (or Tour) is a predefined sequence of readers that can be imposed on Persons defined in the access control system, to direct their movements on the premises, regardless of the person's authorizations.
Typical uses are to enforce strict access sequences in industrial clean environments, hygienically controlled, or high-security areas.

Defining routes

1. In the Main menu select **Tour monitoring** > **Define routes**
2. Enter a name for the route (up to 16 characters)
3. Enter a more detailed description (optional)
4. As with Guard tours, click the **Add reader** button to create a sequence of readers. Use the arrow buttons to change the position of a reader in the sequence, and the **Delete reader** button to remove it.



Assigning a route to a person

To assign a route to a person proceed as follows:

1. In the Main menu click **Personnel data** > **Cards**
2. Load the personnel record of the person to be assigned
3. In the **Other data** tab select the check box **Tour monitoring**
4. From the drop-down list next to it, select a defined route (for defining a route, see the previous section).

5. Save the personnel record.

The route is activated when the person assigned presents their card at the first reader on the route. The other readers on the route must now be used in sequence, that is, only the next reader in the sequence will grant access. After the route has been traversed completely, the person may book at any other reader within their authorizations.

Correcting and monitoring routes

1. In the main menu select **Tour monitoring** > **Correct routes**
2. Load the personnel record of the person assigned to the route.
3. To locate that person on the route, click the **Determine location** button.
4. The readers that have already been passed successfully receive a green check mark ✔ in the list.
5. To reset or correct the location of a person on the route, click the **Set location** button.

10 Operating Threat Level Management

This section describes the various ways to trigger a threat level and cancel it. For background information see section Configuring Threat Level Management

Introduction

A threat level is activated by a threat alert. A threat alert can be triggered in one of the following ways:

– By a command in the software user interface
– By an input signal defined on a local access controller, for instance a push button.
– By swiping an Alert card at a reader

Note that threat alerts can be cancelled by the UI command or hardware signal, but not by alert card.

10.1 Triggering a threat alert via hardware signal

This section describes how to send a hardware input signal to trigger a threat alert.

Prerequisites

– At least one threat level has been defined
– At least one entrance has been configured in the device tree.
– Hardware signals have been defined on an AMC, and a device has been connected to the correct terminal on that AMC, that will deliver a signal to it. If required, click the link at the end of this section for instructions on how to configure the input signal, or contact your system administrator.

Procedure

Activate the device, typically a push button or hardware switch, that is connected to the AMC. To cancel the threat alert, activate the device that sends the input signal defined as **Threat level: Deactivate**.

10.2 Triggering a threat alert via Alert card

This section describes how to trigger a threat alert via an Alert card.

Prerequisites

– At least one threat level has been defined
– At least one entrance has been configured in the device tree.
– An alert card has been created for a particular cardholder. If required, click the link at the end of this section for instructions on how to create an alert card, or contact your system administrator.

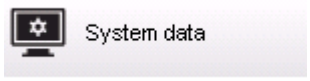
Procedure

1. The cardholder presents their special alert card at any **non-fingerprint** reader the site.
   – The threat level that was defined for that card is activated.
2. When the treat has passed, cancel the threat level via UI command or hardware switch. By design it is no possible to cancel a threat level via an alert card.

11 Using system dialogs

11.1 System Data

All the authorizations and criteria that can be selected in the person-related dialogs are defined in the System Data dialogs.

If you open the 

menu item from the main menu, the following dialogs will be available:

11.1.1 Access Authorizations

Dialog: Access authorizations

Access Authorizations are bundles of access rights for one or more entrances. Access authorizations can be assigned to persons directly, or can be bundled into **Access profiles** and assigned as such.

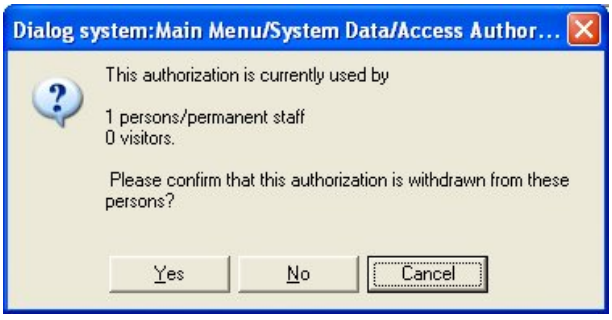
- The authorizations are assigned to a MAC which must be selected
- The selection of a time model is optional.
- Each access authorization is specified by a unique name in the **Authorization name** field.
- The **Description** field is for an optional description of the access authorization.
- The **Time model** field allows the selection of a certain time model.

– The **Inactivity limit** field is a means to withdraw an authorization from a person if the person does not use the authorization within the selected time period (“use it or lose it”). Select **(No entry)** if you want to set no inactivity limit.

Notice!
Subsequent changes to authorizations will affect existing assignees, unless the governing profile is locked.
Example: If an Inactivity limit of 60 days is reduced to 14 days, then the authorization will be lost to all persons who have not used that authorization in the past 14 days.
Exception: If an authorization is part of an access profile that is **locked** to an Employee ID (Person type), then persons of that type are not affected by inactivity limits on the authorization. Profile locks can be set with the following check box.
Main menu > **System data** > **Person Types** > table: **Predefined Employee IDs** > check box: **Profile locked**

Notice!
The uniqueness of the naming also refers to the area-time authorizations. Both types of access authorization are managed in one database table and must therefore be given unique names.

For better orientation all existing entrances, which were created in the **Device Editor**, are subdivided into five categories.
– Entrance
– Time management (time and attendance)
– Elevator
– Parking lot
– Arming intrusion detection
Each access authorization can consist of entrances of multiple categories.
By clicking the **Assign all** button, all doors (for all configured directions), elevators and their levels, parking lots and arming authorizations are assigned to this access authorization.
Click the **Remove all** button to revoke all assigned entrances from the authorization so that new assignments can be carried out.
If access authorizations become completely invalid or should no longer be applied for whatever reason, they can be revoked in one action from all persons who use them. To do this, the respective authorization is first selected and when the **Withdraw authorization** button is clicked, a message appears with the indication about the number of persons currently using this authorization and the explicit request for authorizations to be withdrawn.



If this is confirmed and the access authorization is withdrawn, access will be denied at all entrances concerned to those persons who use this authorization. If this authorization was the only one being used by this person, he will no longer be granted any access until he is assigned a new authorization.

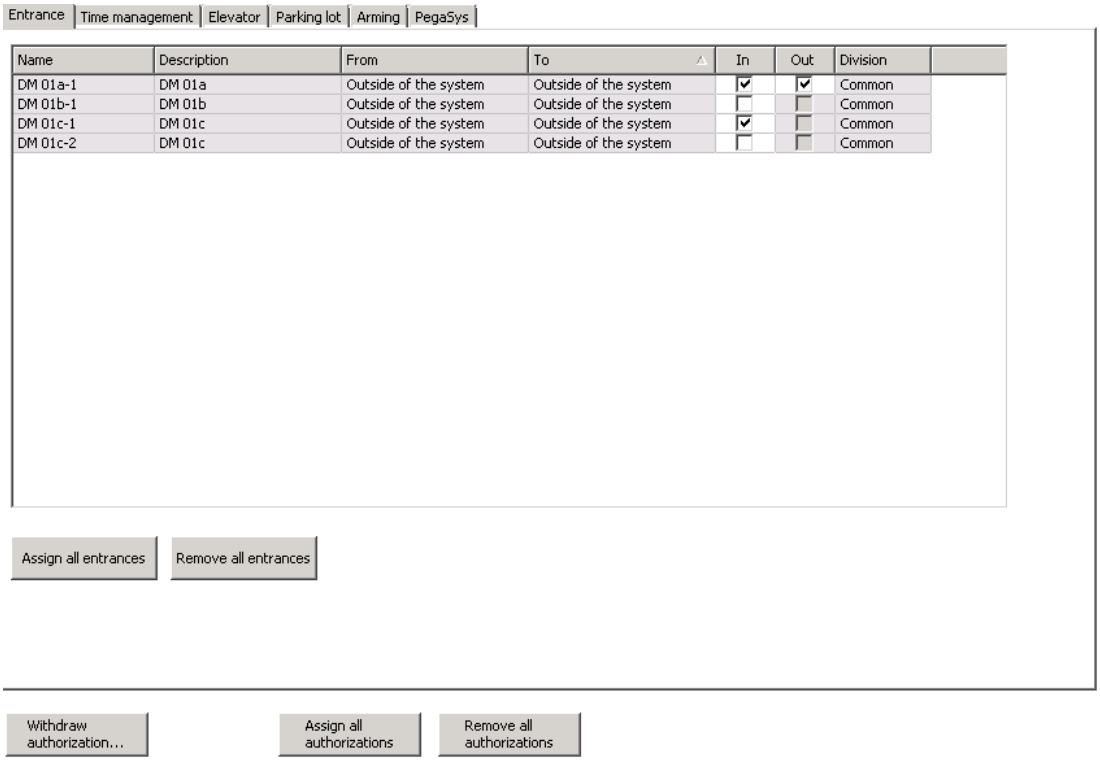
However, the withdrawn authorization remains in the system and can be reused at any time. If the authorization is to be deleted entirely, it must first be withdrawn from all users. Only after it has been withdrawn can it be deleted definitely via the tool button.
The display showing the number of persons currently using the authorization can also be used for system maintenance; individual authorizations are selected and, by clicking the **Withdraw authorization** button, the above message can be used to check the extent to which the authorization is currently being used. By rejecting the prompt for authorizations to be withdrawn or canceling the message, current status is retained.
For authorizations that are not in use, a message appears to that effect. Unused authorizations can be deleted to reduce clutter in the system.

Access Authorizations for Entrances
On the first tab of the dialog, all entrances other than time-management readers, parking-lots, elevators or arming readers.
In addition to the name and the description of the entrances, the respective locations and destinations and the configured entry direction are displayed. The list entries can be sorted according to each column so that, for example, all selectable entry or exit directions can be displayed one below the other.
The **In** and **Out** columns contain check boxes that indicate which entry direction can be selected and which has been selected:

☐	Configured and selectable entry direction
☑	Entry direction assigned to this authorization
☐	Not configured and non-selectable entry direction

Selectable entry directions are activated with a click of the mouse and assigned to the access authorization. A further mouse click deactivates the selection made previously.
For quick processing - including with long lists all selectable entry directions in this list can be activated by clicking **Assign all Entrances**; this way, only individual entry directions have to be deactivated again where necessary.
For a subsequent change of access authorizations, all activations can first be withdrawn by clicking **Remove all Entrances** and then new assignments can be selected individually.

Notice!
Special features of door model 14:
In addition to the normal access regimentation which also relates to the other door models, this model can also be used to arm and disarm a connected alarm system. Unlike door model 10 (= arming the alarm system using a PIN code), here the system is armed or disarmed with a button and by means of special authorizations.
When an access authorization is assigned for an entrance in door model 14 on this tab, entrance is only granted in one of the activated directions. Authorization for arming or disarming must be assigned separately on the **Arming** tab.

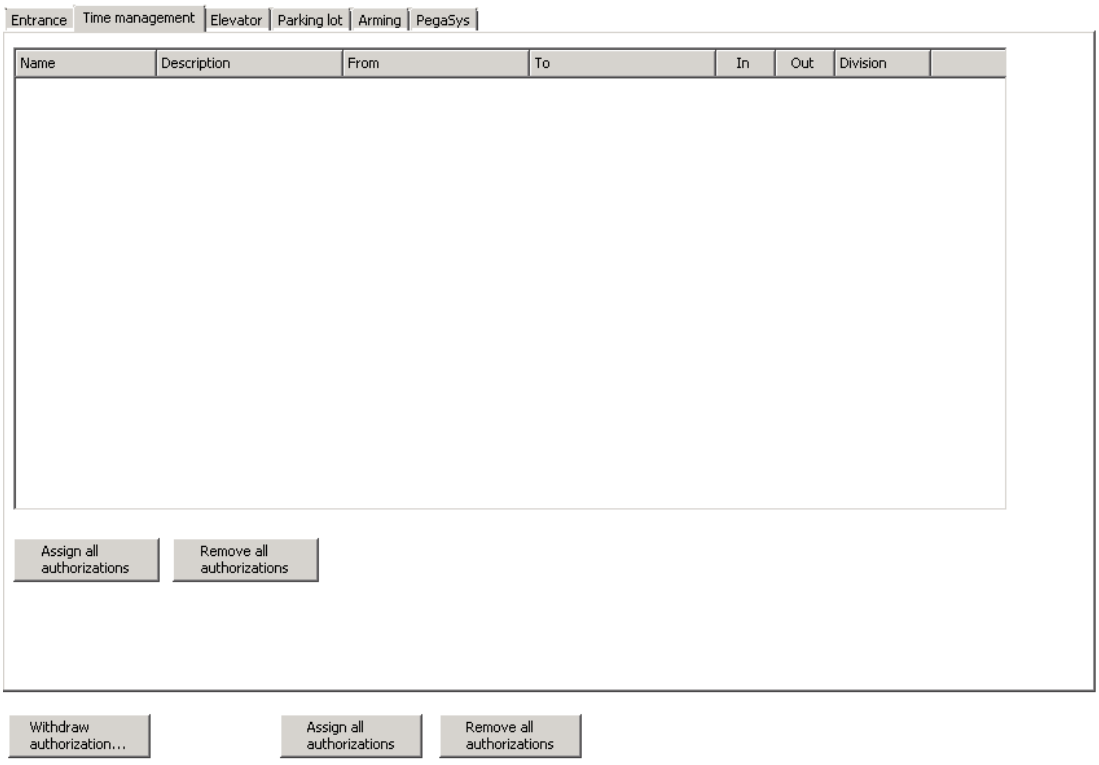


Access authorization for time management

This tab lists those readers created with door model 06. These readers collect time and attendance data; they are not connected with doors, i.e. they give no access authorizations as such.

Here too the detection of cardholders' directions of movement can be activated on an individual basis and the directions recorded. Time management readers can be configured so that they function in one direction only. This makes it possible differentiate between entrance and exit areas.

The list is structured and can be edited in the same way as described for the Entrance tab.



Access Authorizations for Elevators

This tab contains the two list fields **Elevators** and **Floors**. The floors set up for the selected elevator are indicated in the lower list.

In addition to the name and description (and also the location and destination for floors) the lists contain the **Status** column. In contrast to the entrances, no entry directions can be defined for the elevators; however, floors that can be reached with this access authorization are activated.

Notice!

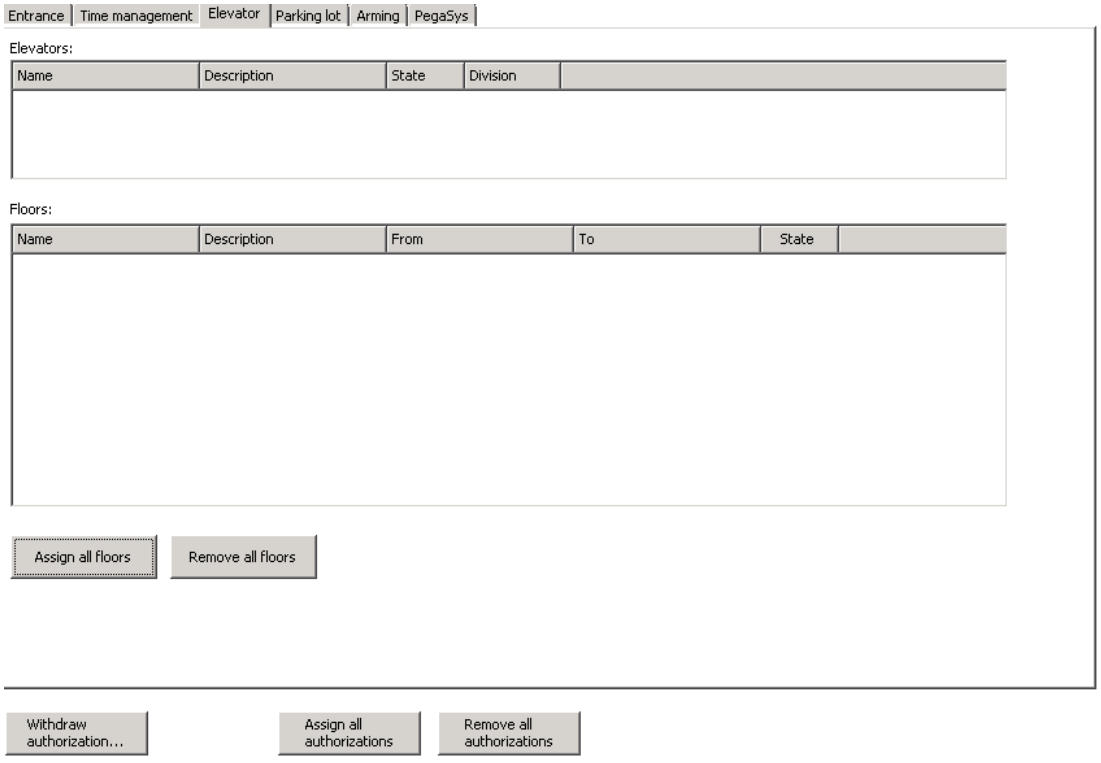
One list entry in the Floors list does not necessarily mean that only one floor is activated. Floor areas can also be defined in the Device Editor, so that several floors can be activated by selecting one entry.

Processing notes

The check boxes in the **Elevators** list **cannot** be activated or deactivated directly; they serve only to show which elevators are contained in the selected access authorization. Activation only occurs when the relevant floors are selected.

The desired elevator is selected from the **Elevators** list. Then the floors configured for this elevator appear in the **Floors** list. In this list the floors that are to be assigned with the access authorization, are then activated. If at least one floor is selected, the status display in the **Elevators** list changes when the elevator is activated.

All floors of **all** lifts can be assigned using the **Assign all floors** button. Accordingly, all activations are withdrawn by clicking **Remove all floors**.

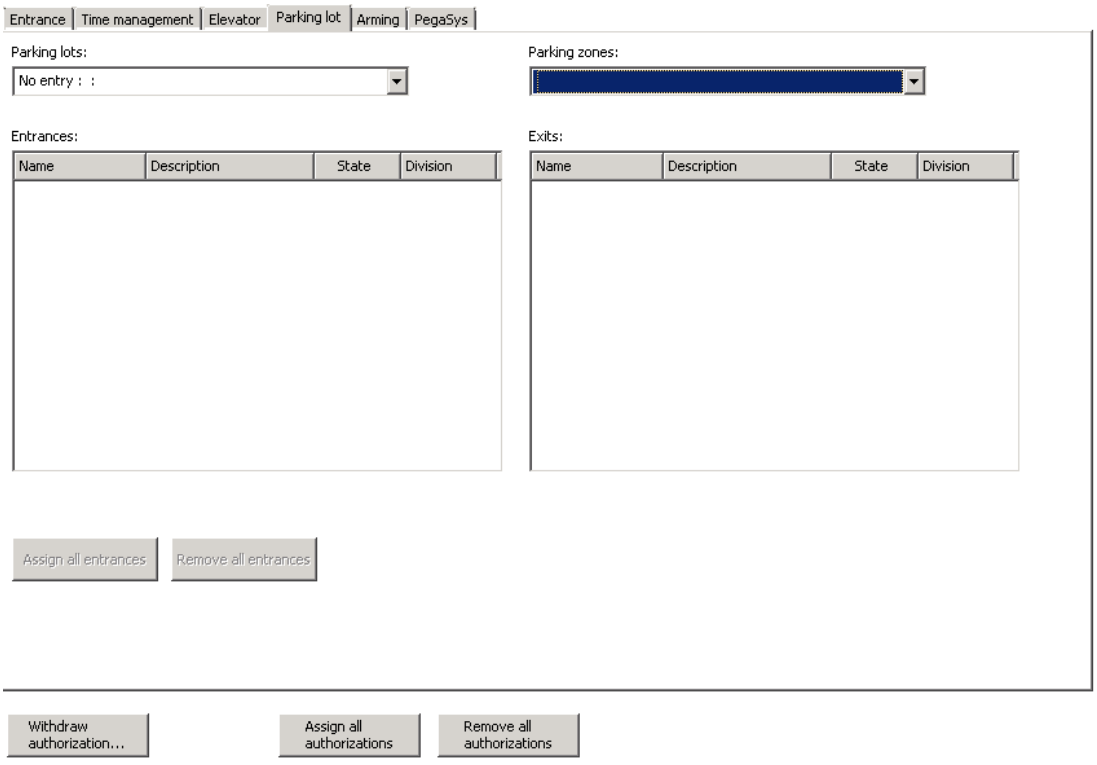


Access Authorizations for Parking-Lots

This tab contains a selection list fields for **parking lots** and **parking zones**. When a parking lot is selected, the second list is filled with the parking zones that belong to it and the first entry in the list is set. At the same time, the entrances and exits that have been set up appear in both list fields.

Notice!

By default, no parking lot is assigned to the access authorization. But if the buttons **Assign all entrances** or **Assign all authorizations** are used the first configured parking lot and the depending first parking zone will be chosen.



Access Authorizations for Arming intrusion detection

This type of access authorization only contains entries if entrances with door model 14 are configured. In addition to the normal access regimentation which also relates to the other door models, this model can also be used to arm and disarm a connected alarm system. Unlike door model 10 (= arming the alarm system using a PIN code), here arming or disarming happens by means of special authorizations.

The list field contains all arming and disarming authorizations that have been set. Because of the fact that for each door model 14 a separate arming and disarming authorization is created, the check boxes in the Armed and Disarmed column only display two statuses - there is no “not configured” status (= gray check box) here:

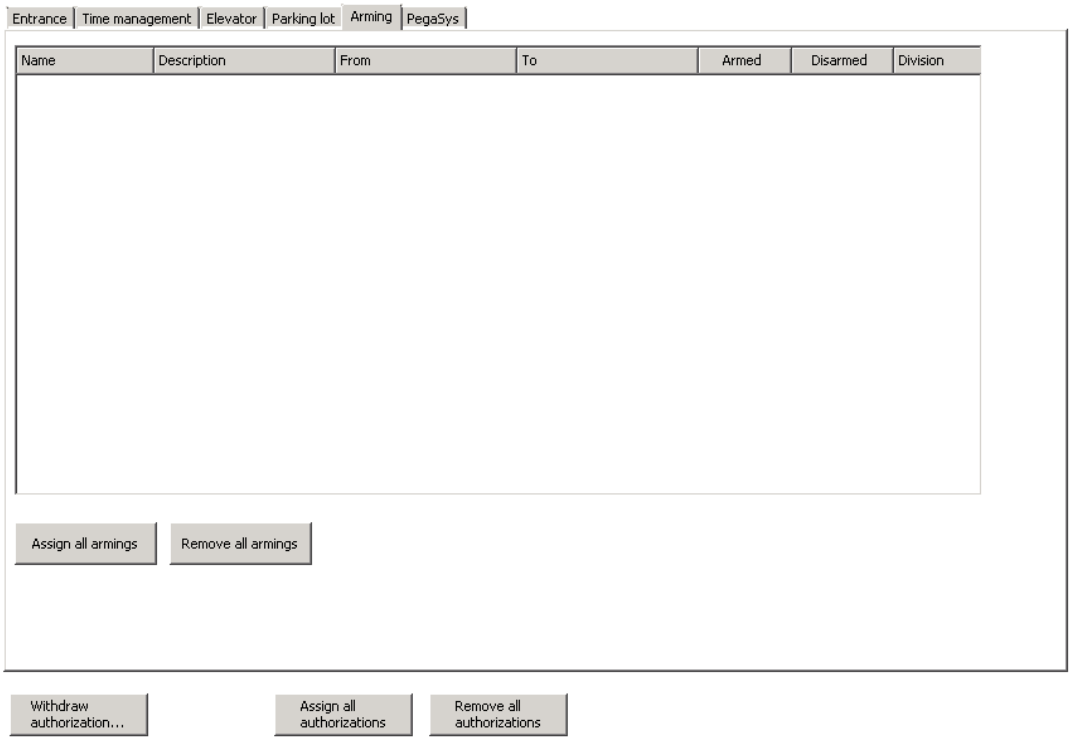
☐	Selectable authorization
☑	Assigned authorization

The arming authorization can be separated from the disarming authorization and can therefore be assigned to different access authorizations and persons.

Notice!

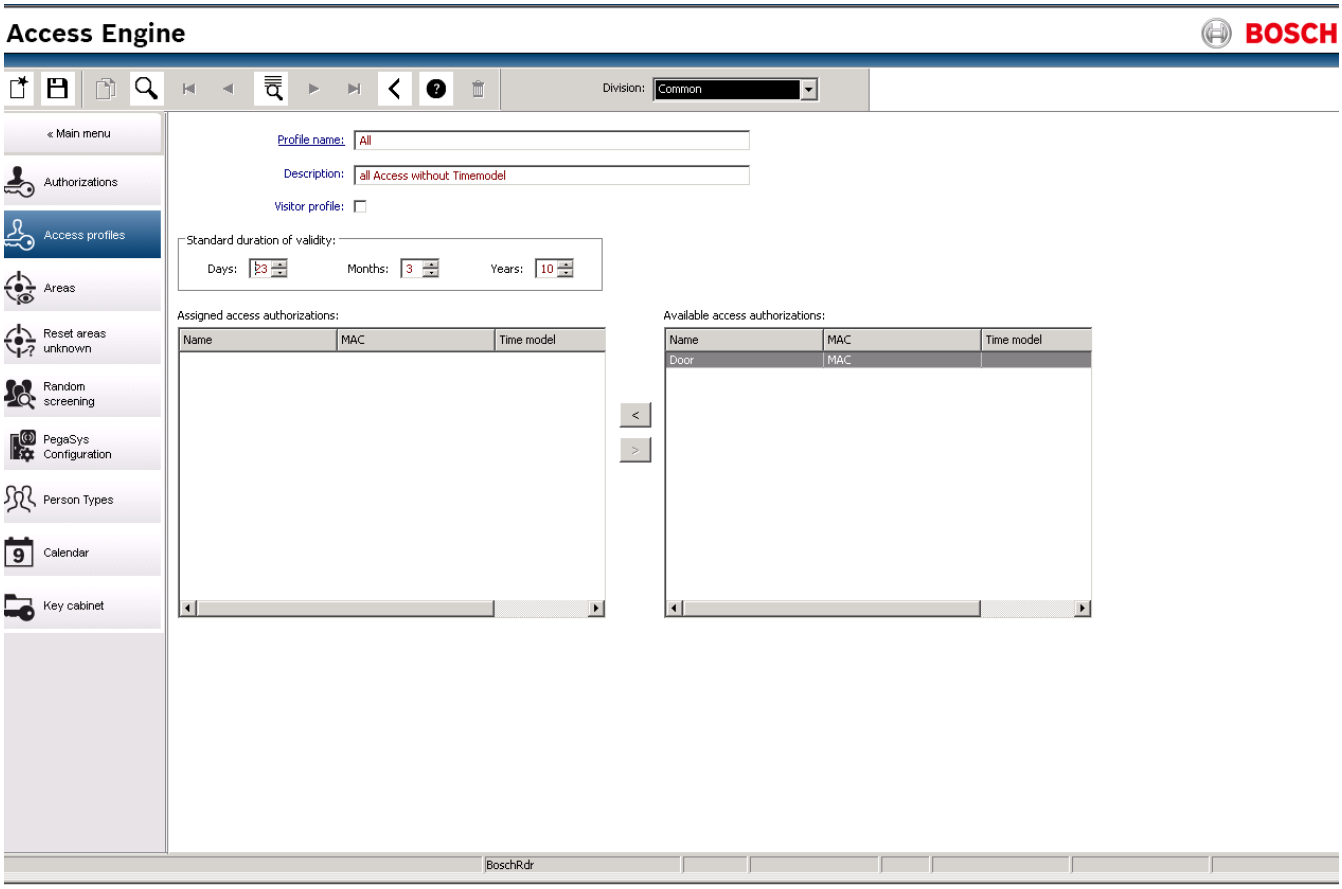
The assignment of arming or disarming authorizations is not connected to the access authorization for passage through the entrance concerned.

If the access authorization is also to authorize passage through the entrance, the desired entry direction must also be activated on the Entrance tab.

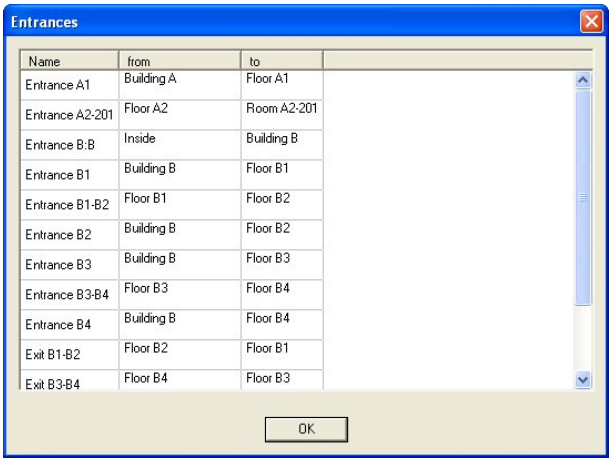


11.1.2 Dialog: Access Profiles

Individual access authorizations and area-time authorizations can be grouped into an access profile, making it easy to assign frequently used rights to employees and visitors.



To create an access profile, the user must enter a unique name for the profile in the **Profile name** field.
Checking the **visitor profile** check box for certain profiles allows that profile to be selected in the Visitors dialog. Since all profiles are available in the **Cards** dialog, it is recommended to give visitor profiles a special name and description to avoid any potential misunderstandings.
An area-time authorization can be recognized by the fact that a time model has been assigned.
The Assigned access authorizations list on the left contains the rights belonging to the corresponding access profile. Access authorizations can be transferred from one list to the other by double-clicking or selecting the authorization and then using the < and > buttons to transfer it.
To quickly check which entrances each of the authorizations contain, the relevant authorization can be selected from one of the lists and a button as shown below activated by right-clicking (as shown below):
Clicking this button opens a dialog with this authorization's entrances.



Notice!
In contrast to access authorizations, changes made to access profiles only apply to future operations. Profiles that have already been assigned will not be affected by this change.

A validity period can be specified for the access profile in the **Days**, **Months** and **Years** fields located above these two lists. If the profile is now selected for a person, the access authorizations of the profile are valid from the current date for the given profile validity period. This means that if the validity was limited to one day, the authorization would expire at the end of the day it was assigned.
According to the validity period requirements, when the profile is selected in the **Cards** or the **Visitors** dialog, dates are entered in the **Valid from** and **until** fields - starting from the current date. If the validity period of the access authorization expires, the person is marked with a yellow block next to **Expired** in the status bar.

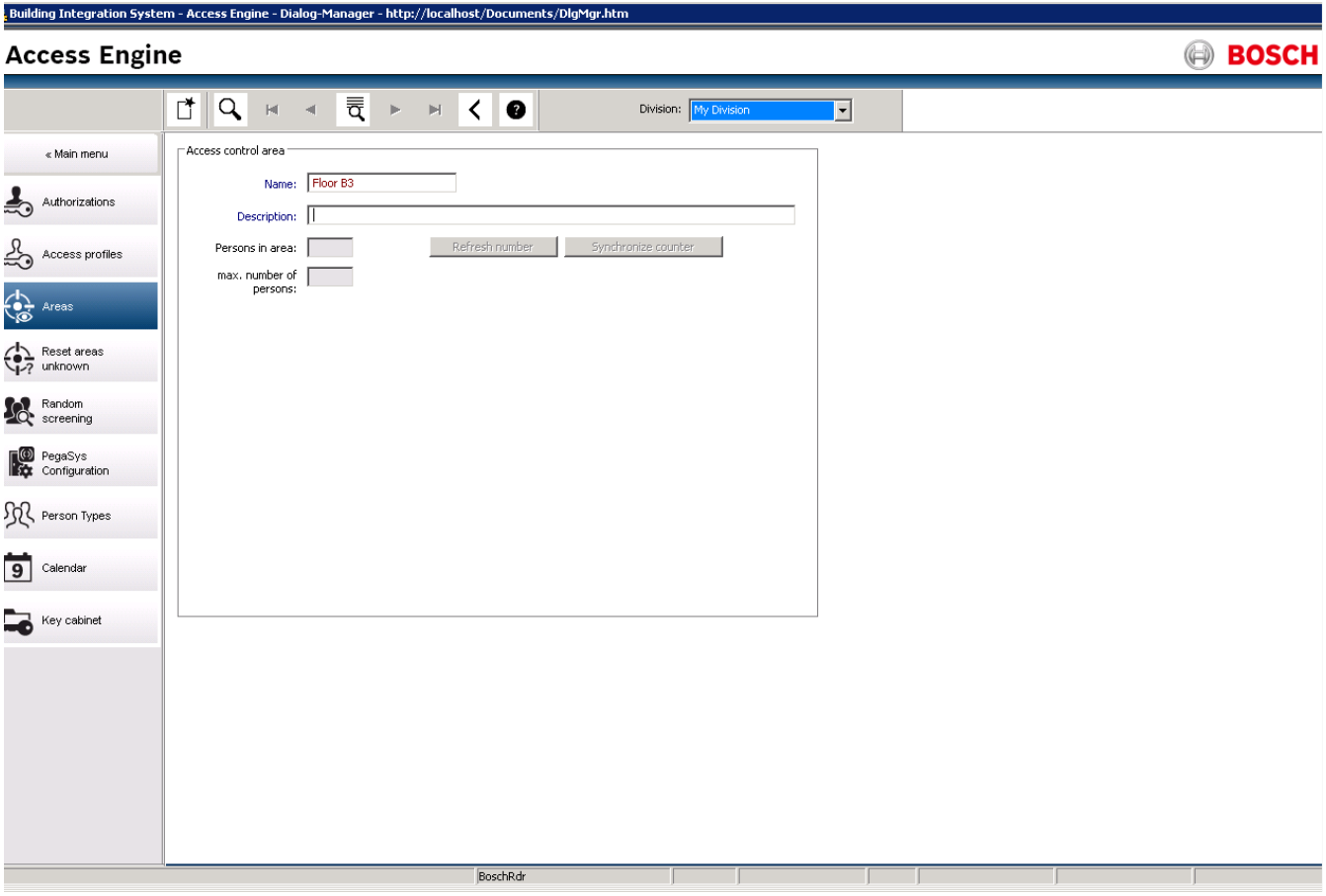
If no validity period is given, no end point is specified for the validity when the profile is assigned; rather, only the day of assignment is entered as the **Valid from** date.

11.1.3 Dialog: Areas

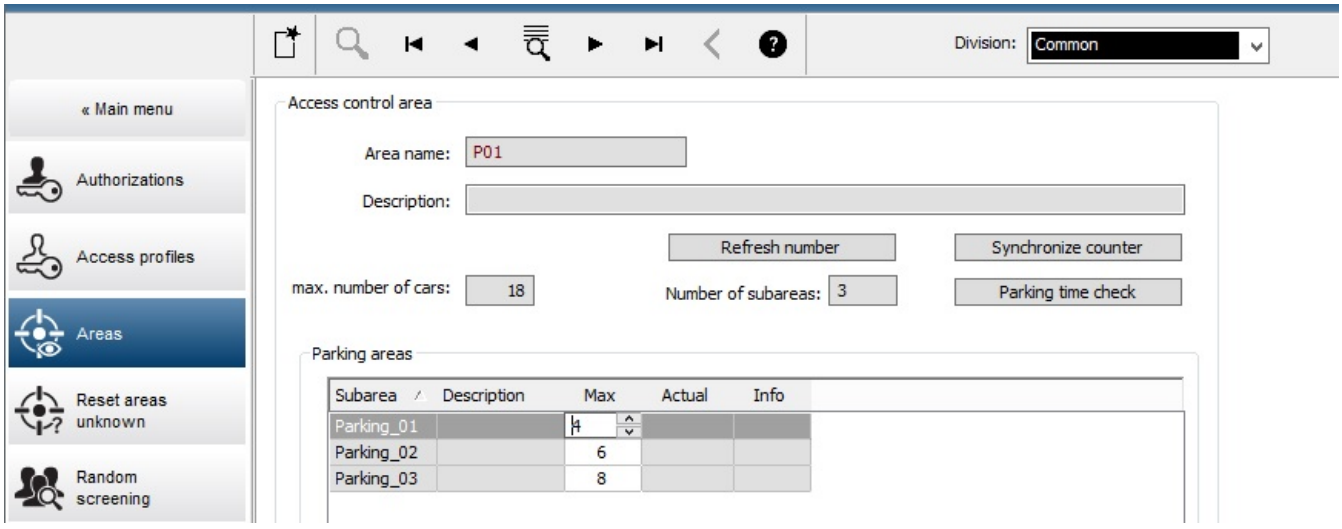
This dialog is used to check the locations where access rights will apply. The areas which are created by the BIS Configuration Browser Dialog **ACE Areas** can be selected here to prove the capacity of the single areas.

The system provides the possibility to define and differentiate two types of areas.

- Areas for persons
- Areas for cars (parking lots)

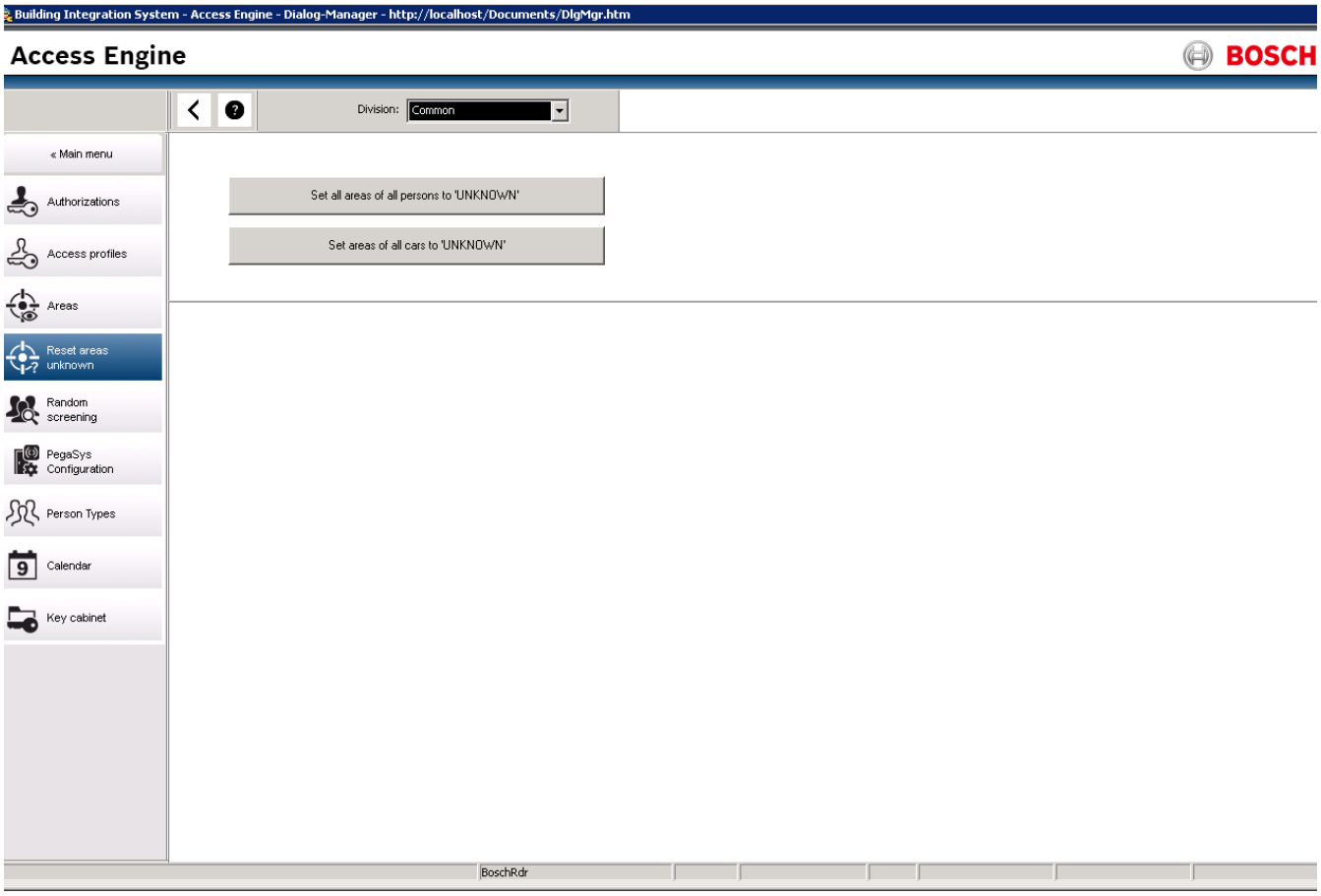


The dialog box is given additional controls if a parking lot area is selected.



11.1.4 Dialog: Reset Areas Unknown

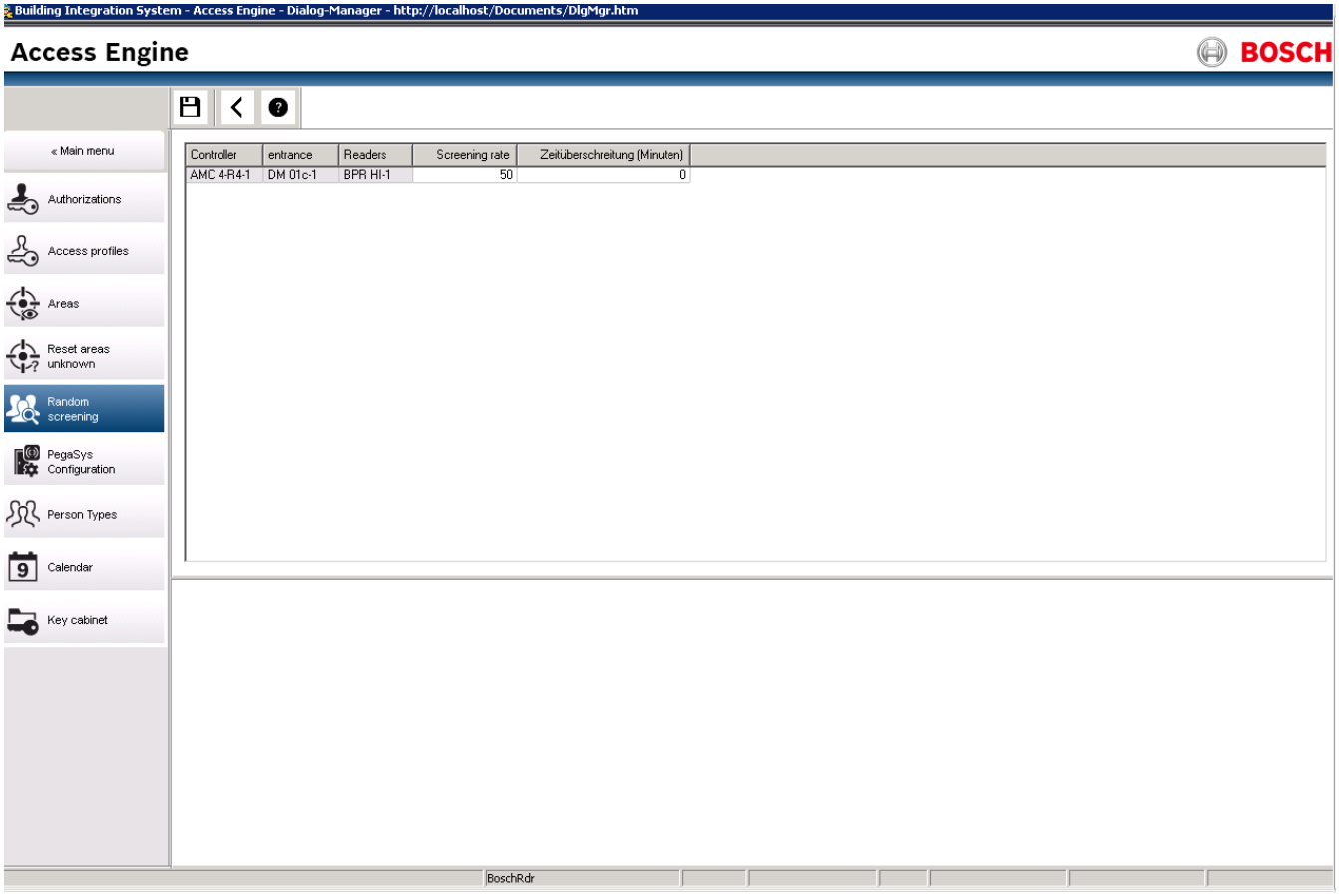
In the case of an event like evacuation or fire exercise, it's recommendable to set the location of all persons and/or cars to unknown, using the corresponding buttons. As all persons will leave unchecked, no one would be allowed to return. Setting all person and/or cars to "unknown", lets persons check in again and thus re-establishing a valid status and a known location. This does not apply to persons outside, as they are not registered anyway.



Notice!
Persons and vehicles with the location OUTSIDE are not switched as they are not in the plant and are therefore not subject to access sequence check.

11.1.5 Dialog: Random Screening

The list field of this dialog shows all readers (and the corresponded controllers and entrances) parametrized for random screening. The column **Rate** displays the current screening rate. Additional to the overview of the defined random screening readers and their actual screening settings the rate of each reader can be changed directly. So it is possible to react to special events or different frequencies at the entrances - e.g. reducing the rate at the start of work to avoid waiting times and lines in the security booth.



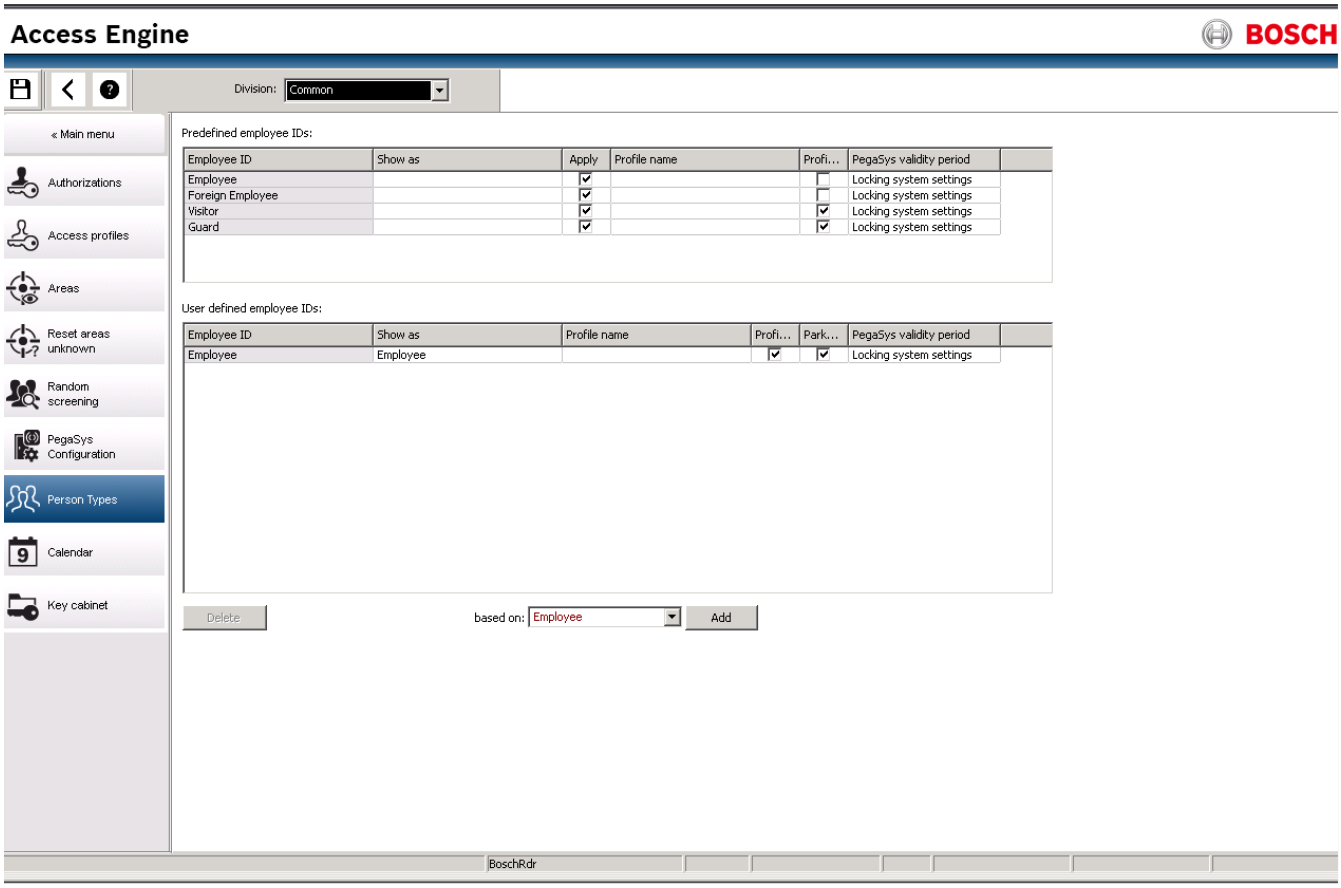
Click into the corresponded cell of the column **Rate** to activate the edit mode. Then enter the new screening rate using the keyboard. The possible value range is 1 to 100.

Notice!
Selection is at random. It is therefore possible, e.g. with a screening percentage of 10%, for the next person entering also to be selected. The configured screening percentage is achieved gradually as the number of bookings increases.

See also the notes to configure random screening.

11.1.6 Dialog: Person Types

The dialog consists of two lists: **Predefined Employees IDs** and **User defined Employees IDs**



Predefined Person Types (Employee ID)

The following Person types are system defaults and cannot be deleted, though their appearance and behavior can be modified.

Employee	Persons of these types can be added and edited only in the dialog **Persons**.
External personnel (formerly Foreign employee)	
Guard	Persons of this **Person Type** are also added in dialog **Persons**. In the **Cards** dialog, assign a card to a person of this Person type. Note that the tab **Authorizations** in that dialog will not allow you to assign access authorizations to the card. Guard cards are used only for **Guard tours**, where they signal that the guard has reached a certain reader during a particular patrol. A guard who requires access authorizations must receive an additional and separate definition in the **Persons** dialog, either as **Employee** or **External personnel**.
Visitor	Persons of this **Person Type** can be added and edited in the dialog **Visitors** only.

The list of **Person Types** contains the following columns:

Employee ID (Person Type)	

Show as	Enter the name of the person type as it should appear in the user interface.
Apply (check box)	Disable unused Person types by clearing this check box. They will no longer appear in the **Employee ID** list.
Profile name (drop-down list)	The name of an **Access profile** that may be locked to this Person type
Profile locked (check box)	Select this check box to lock this person type to the access profile in the previous column.
Security profile name	Select a **Person security profile** from the list. These profiles are defined in their own dialog and determine the person's **Security level** and **Screening rate**.

User-defined Person Types
The lower list includes user-defined Person types.
To create customized Person types, first select one of the default types from the upper list as a template. Click the button **Add** for a new list entry based on the selected template Person type. Modify its properties as desired to customize your new Person type.
Use the **Show as** column to give to user-defined Person types a distinctive name in the system UI. The default name is that of the parent **Person type**.
User-defined person types inherit properties from their parent type. For example types based on the **Guard** template are likewise unable to have access authorizations.

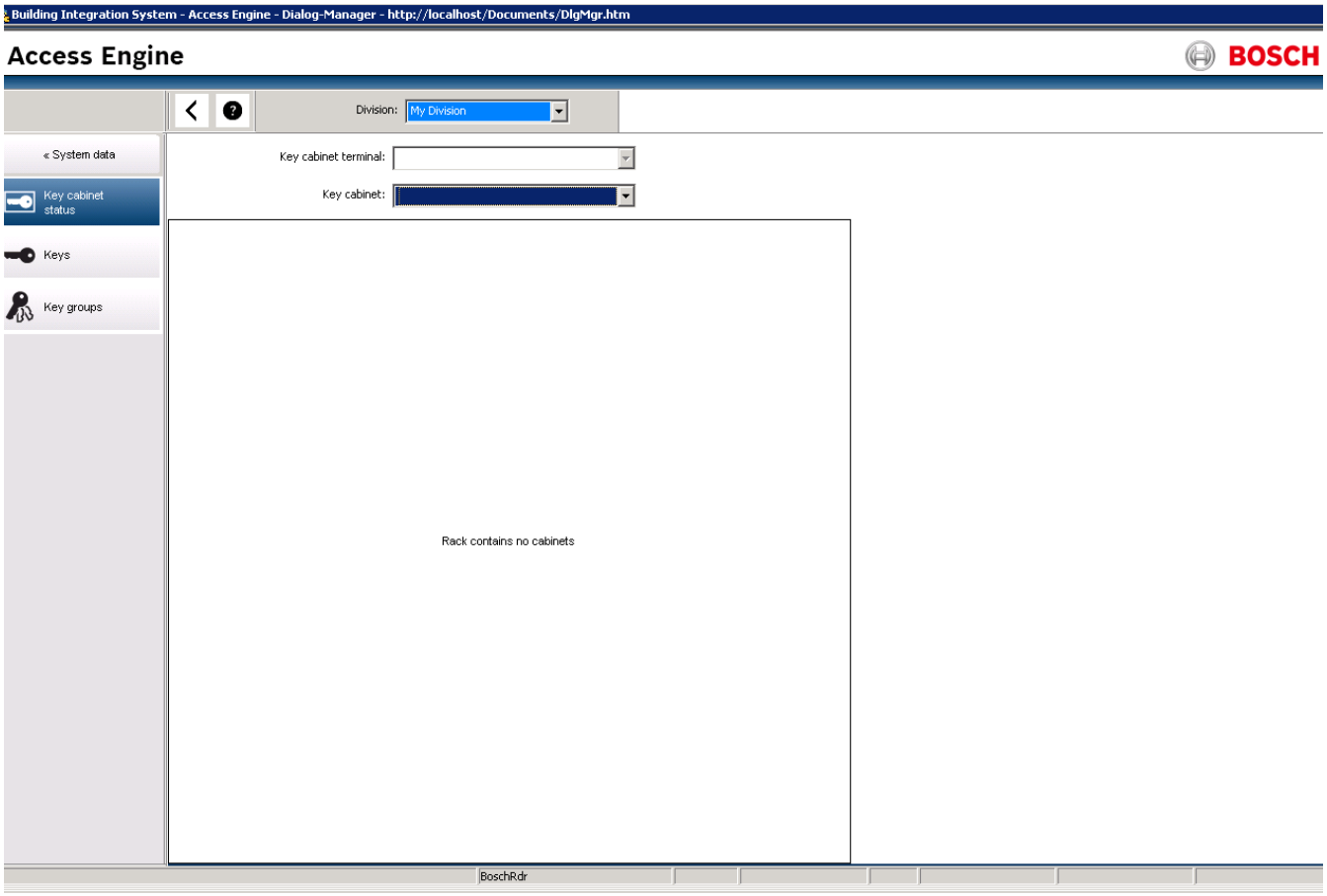
Profile locked
Select the check box **Profile locked** to lock a **Person Type** (Employee ID) to the **Access profile** that is named in the column **Profile name**. When this option is set, all cardholders that are assigned to this Person Type automatically inherit their Access authorizations from the named Access profile.
This has advantages for ensuring consistency of cardholder data, nevertheless all modifications to the profile need to be propagated to all persons of that type.

Notice!
If a Person type is locked to an Access profile, and the Person type contains many persons, then any modifications to that Access profile may take considerable time to propagate to all those persons.
In such cases, plan modifications to the Access profile for times when a large propagation will have least impact to the system.

Refer to
– *Guard tours and Patrols, page 91*

11.1.7 Dialog: Status Key Cabinet

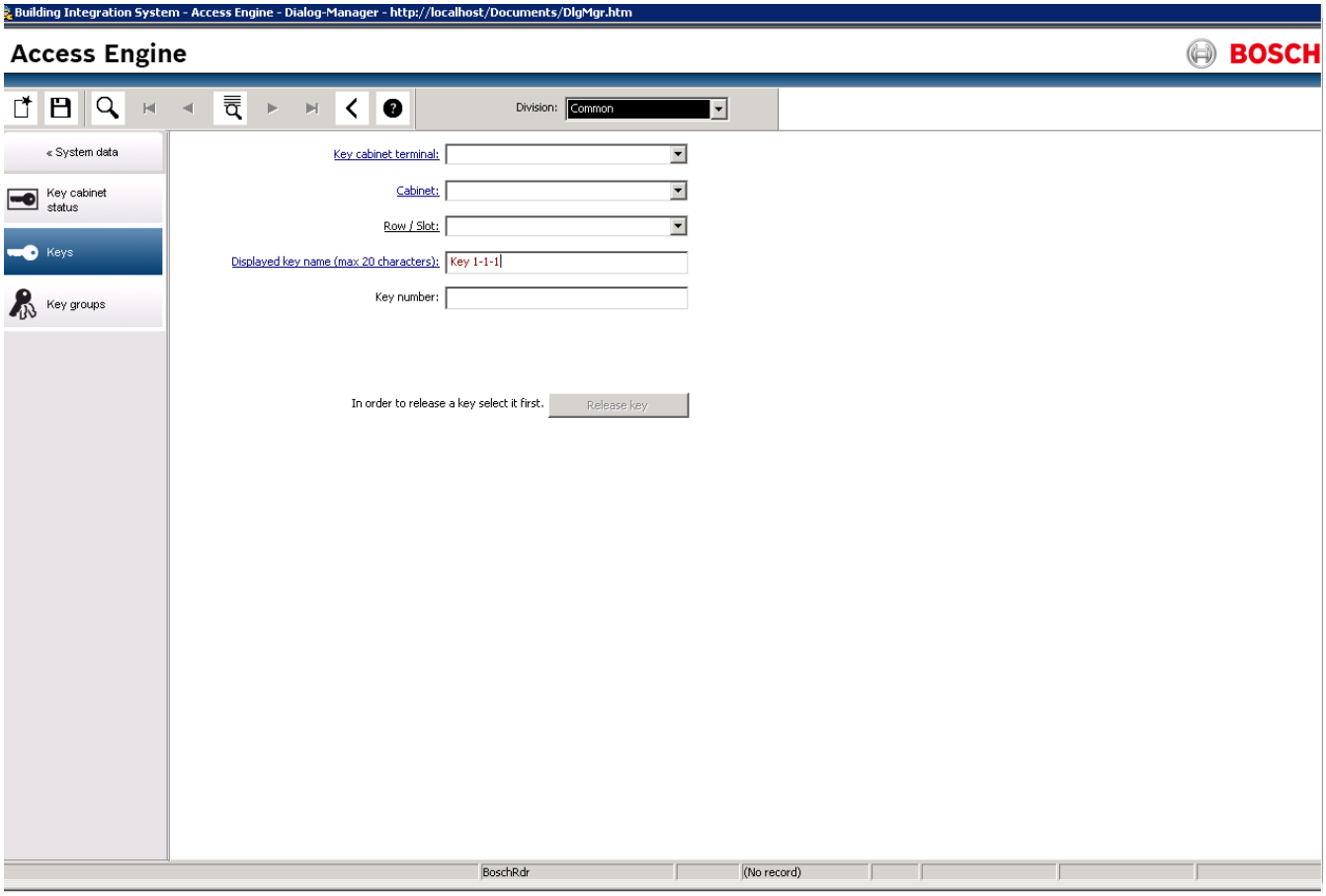
Click onto **Status key cabinet** to display this Dialog:



- **Division:** Name of the division.
- **Key Cabinet Terminal:** the terminal at which the key is used.
- **Key cabinet:** Selection of the key cabinet.

11.1.8 Dialog: Key

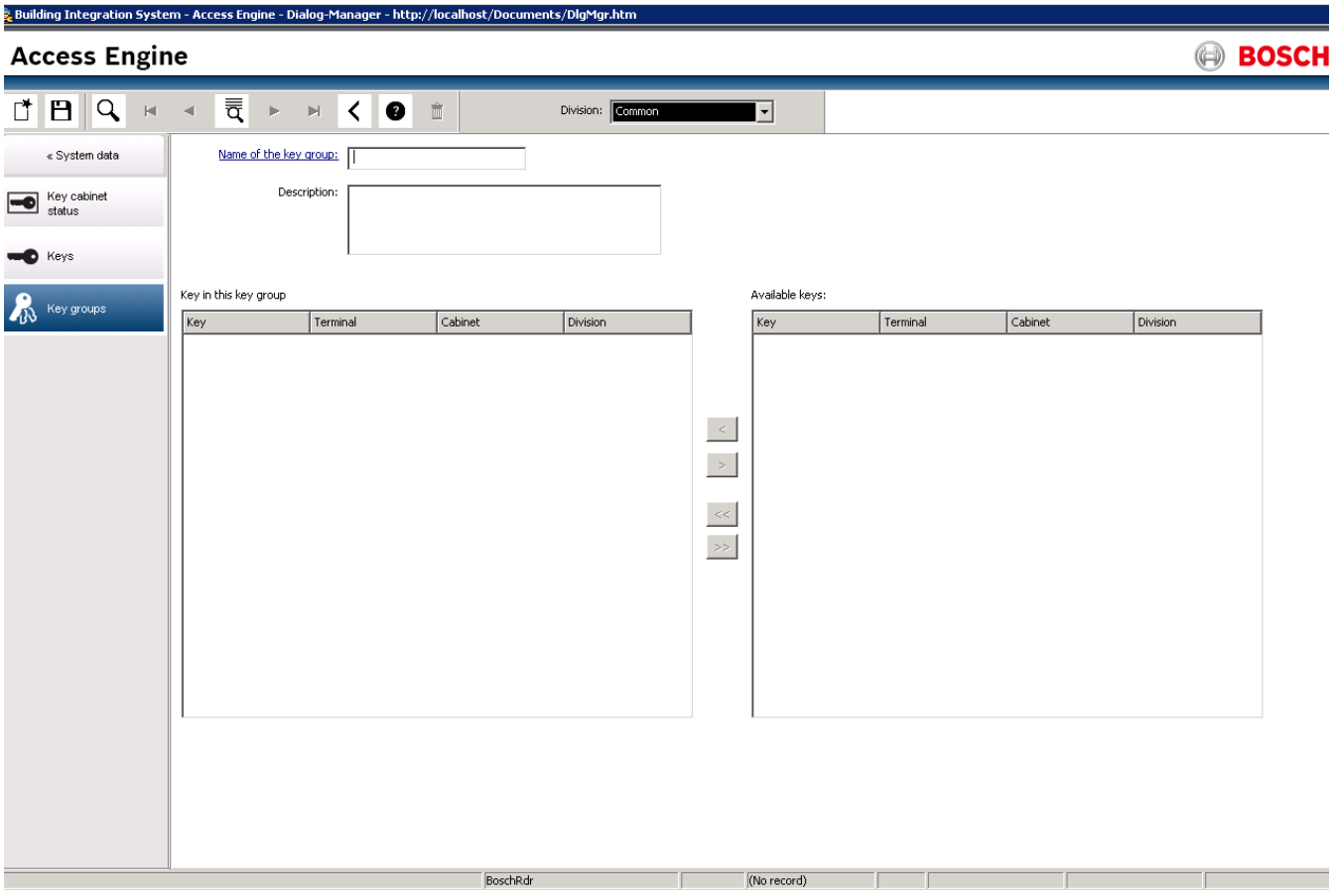
Click onto **Key** to show this Dialog:



- **Division:** Name of the division
- **Key cabinet Terminal**: Selection of the terminal
- **Cabinet**: Selection of the cabinet
- **Row/Slot**: Selection of the individual position in the rack
- **Displayed key name:** Designation of the key (max. 20 digits)
- **Key number:** display of the key code
- **Release key:** Push to release the selected key

11.1.9 Dialog: Key Group

Click onto **Key Groups** to show this Dialog:



Enter the adequate name into the field **Name of Key Group**. A List with 4 columns opens:

- **Key:** Key number
- **Terminal:** The terminal where the key is used
- **Cabinet:** Name of the respective key cabinet
- **Division:** Name of the division

11.2 Calendar

11.2.1 Calendar

The scheduling of access control activities is governed by **time models**.

A **time model** is an abstract sequence of one or more days, each of which is described by a **day model**.

Time models control activities when they are applied to the underlying **calendar** of the access control system.

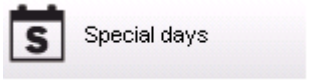
The calendar of the access control system is based on the calendar of the host computer's operating system, but amplifies it with **special days** that are freely defined by the administrator of the access control system.

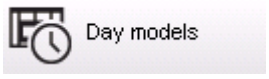
Special days can be fixed to a particular date in the calendar or defined relative to a cultural event, such as Easter. They can be recurring or not.

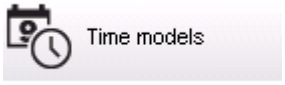
The configuration of an effective calendar for your access control system consists of the following steps.

1. Define the **special days** of the calendar that applies to your location.
2. Define **day models** that describe the active and inactive periods of each type of day. For instance, the day model for a public holiday will be different from that of a normal working day. Shift work will also effect the type and number of day models you require.

3. Define **time models** consisting of one or more day models.
4. Assign time models to cardholders, authorizations and entrances.

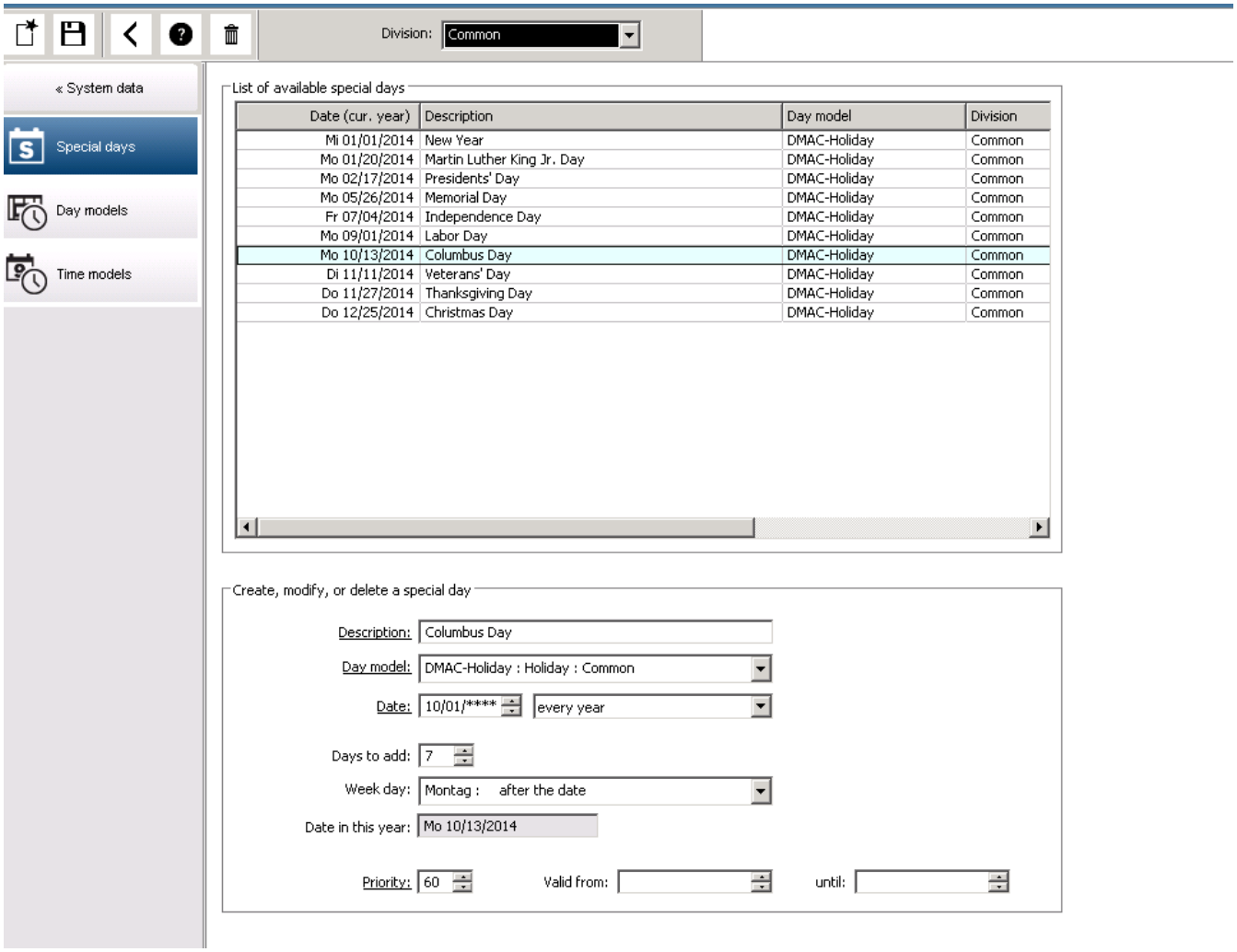






11.2.2 Dialog: Special Days

When this is opened, a list appears in the top list field of the dialog containing all specified holidays. Please note that all holiday dates shown relate only to the current year. However, the calendar is updated from year to year in accordance with the data entered.
Beneath the list there are different dialog fields for the creation of new special days and for the change or deletion of existing special days. To add a new special day, at least three of these input fields must contain data. First a **description** and a **date** must be entered in the respective fields. Thirdly the **class** to which this special day belongs must be selected from the appropriate selective list.



The date is specified in several steps. First of all, a base date is entered in the **Date** field. At this point the date describes an event in the current year. If the user now specifies the frequency of a periodic return in the selection list next to the date field, the parts of the date set by the periodicity are replaced by "wildcards" (*).

once	__.__.____
once per year	__.__.****
once per month for a period of a year	__.**.____
once per month in every year	__.**.****
depending on Easter	**.**.****

Holidays that depend on Easter are not specified with their date, but with the difference in days from Easter Sunday. The date of the Easter Sunday in the current year is indicated in the **Date within this year** field , and the variance of this date is entered or selected in the **Days to add** field. The maximum number of days is 188, so with adding or subtracting you can define every day of the year.

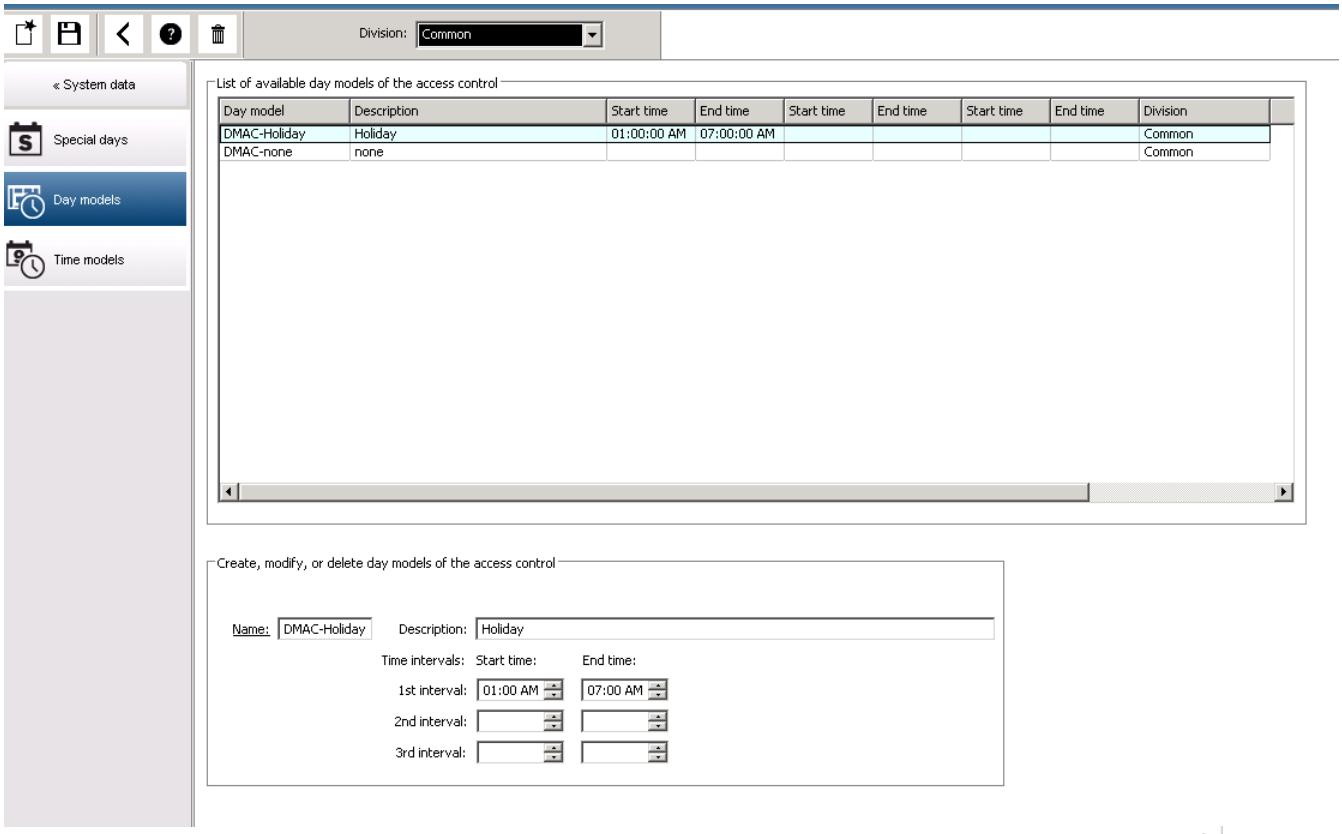
The other data, e.g. the **week day** of the holiday, are optional. Please note that the week day list is determined by the regional settings of the operating system (OS). This leads unavoidably to mixed-language displays where the languages of the access control system and the OS differ.

The assignment of a **validity period** is also optional. If no duration is specified, the default settings make validity unlimited from the input date.
A **priority** can also be set. The priority, rising from 1 to 100, defines which holiday shall be used. If two holidays fall on the same date, the holiday with the higher priority ranges first. In case of equal priorities it is undefined which holiday will be used.
Holiday with the priority “0” are deactivated and will not be used.
The dialog **Time Models** displays only the active holidays, i.e. with a priority greater than 0.

Notice!
A time model of the division “Common” can only use holidays which are assigned to the division “Common”.
A time model of a specific division “A” can only use holidays which are assigned to the division “A”.
It is not possible to mix holidays between divisions, i.e. every division can use only the specific holidays which are assigned to it in its specific time model.

11.2.3 Dialog: Day Models

Day models define a pattern for any day. They can have up to three time intervals.
Once the dialog is started, all existing day models are displayed.



Use the dialog to define or modify model name, descriptions and intervals. The  icon starts a new model.

Start and End times for an interval are entered in hours and minutes. As soon as such a time is reached the interval is activated or deactivated respectively. In order to mark these times more clearly as delimiters, the list pane displays them with seconds (always 00). For example, an authorization in a time model which contains an interval from 8:00 AM to 3:30 PM allows access from 8:00 AM to 3:30 PM but prevents access at 3:30:01 PM.
Start and end times are subjected to logical checks when they are entered, for instance a start time must be smaller than its corresponding end time.
One consequence of this is that no interval may extend over midnight, but has to be split at that point:

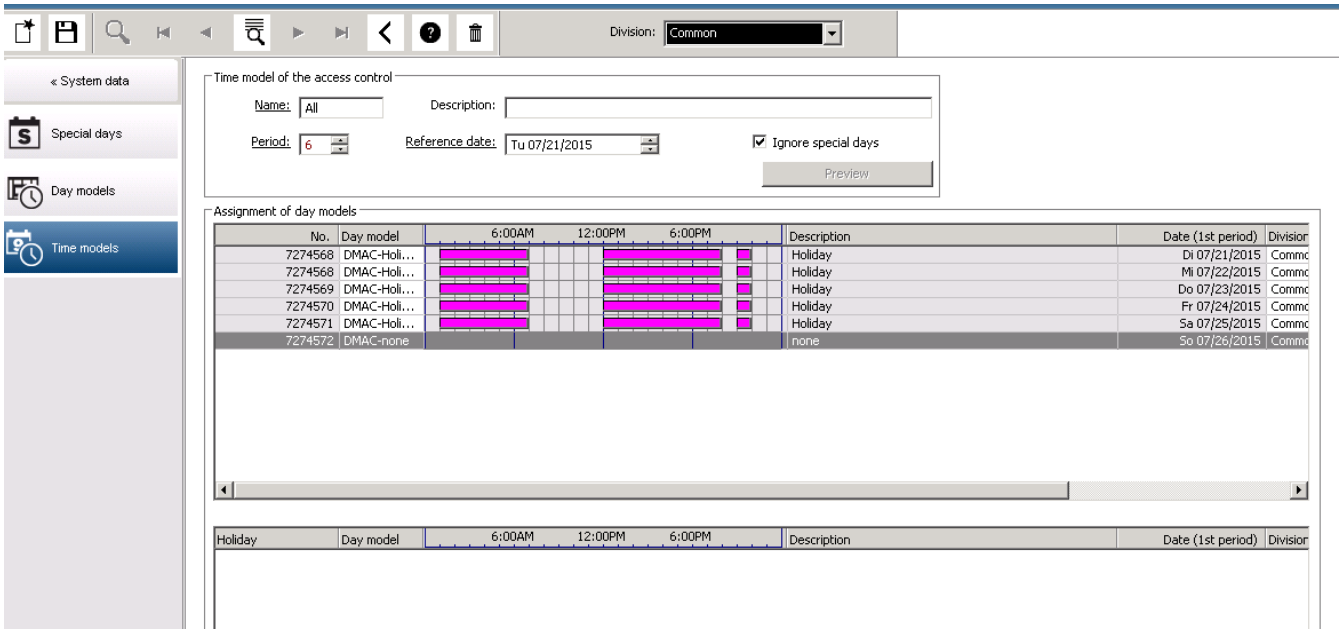
1st Interval	from:	...	to:	12:00 AM
Following Interval	from:	12:00 AM	to:	...

With the exception of midnight (12:00 AM) no overlaps are allowed between the interval delimiters of a single day model. Note, this precludes the entering of the same time for the end of one and the beginning of the next interval.
Exception: A 24 hour interval nevertheless has start and end times both set to 12:00 AM.

Notice!
Tip: You can check intervals by viewing them in the Time models dialog: First create a day model containing those intervals (System data > Calendar > Day models). Then assign this day model to a dummy time model with a period of one day (System data > Calendar > Time models). The intervals are then illustrated in the bar graphic.
Exit the Time models dialog without saving the changes.

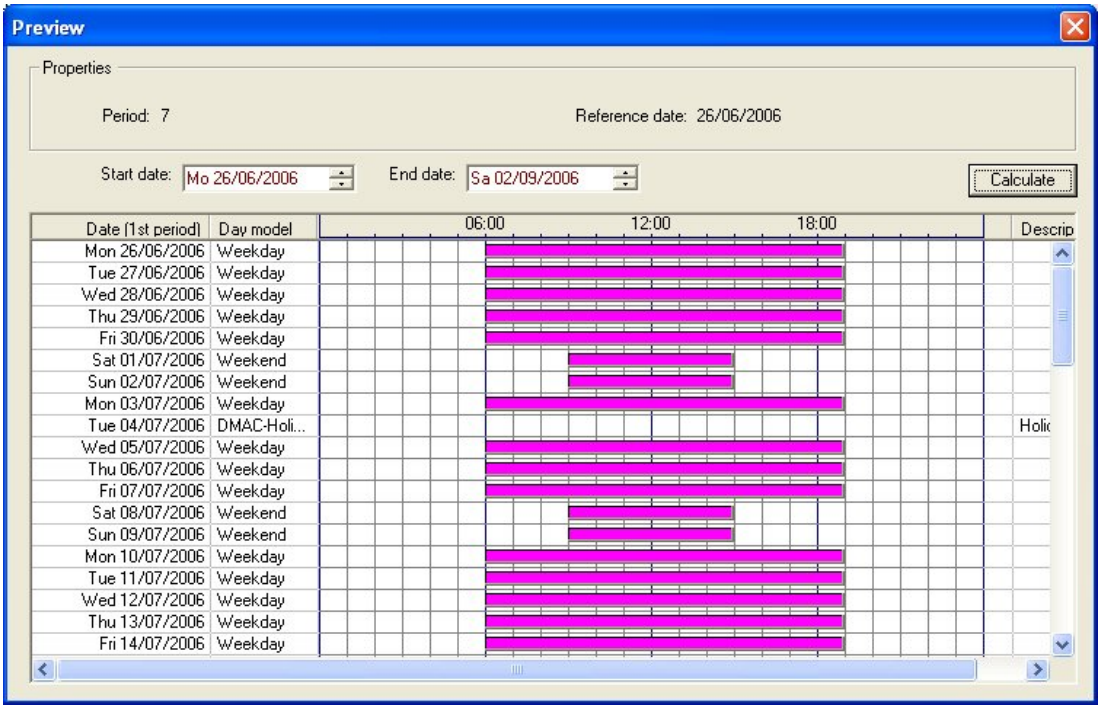
A day model can only be deleted if it has not been assigned to a special day and is not being used in a time model.

11.2.4 Dialog: Time Models

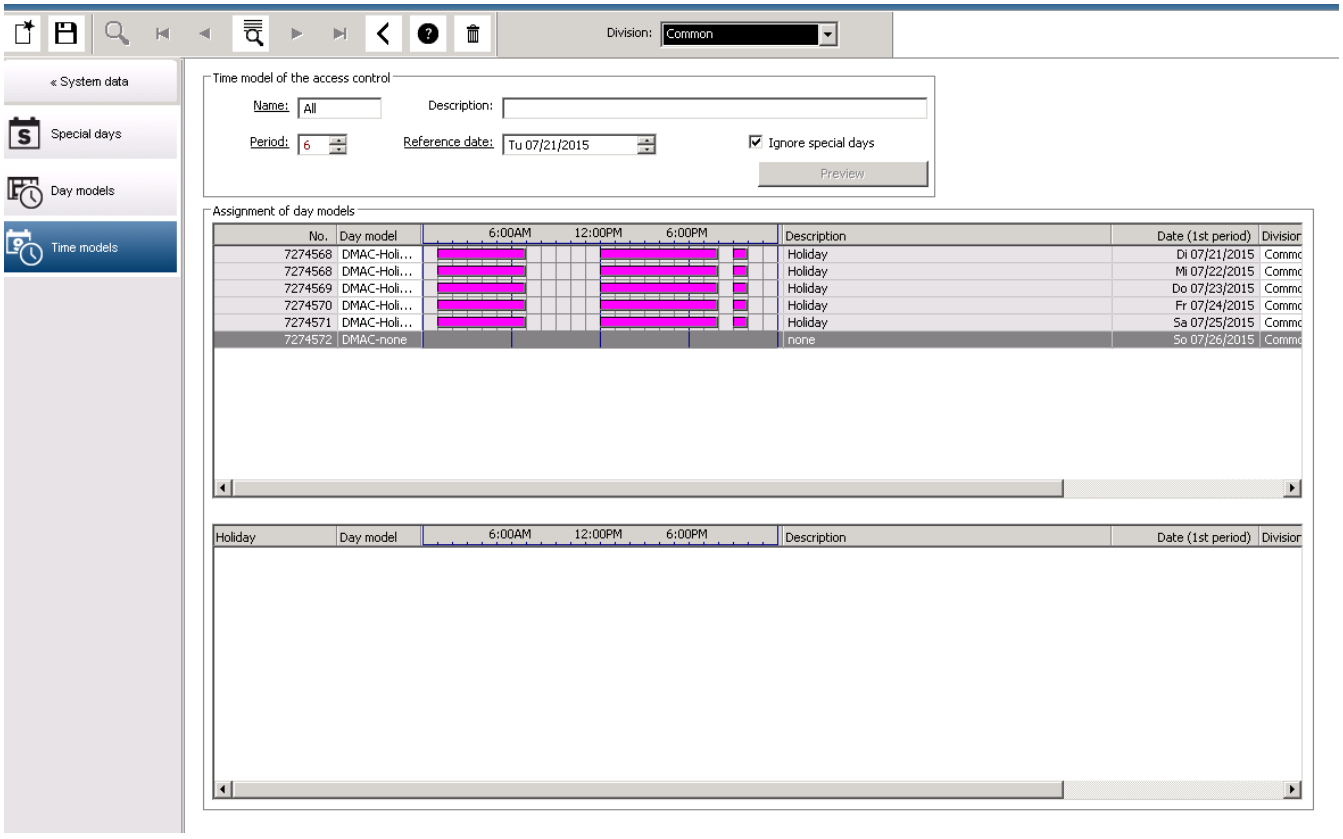


Existing time models can be selected from the search list and their details displayed in the dialog fields. Any processing is carried out in line with the procedure for creating new time models.

If the mask is empty, time models can be created from scratch. To do this, you must enter a **name** and the number of days in the **period** and select a starting or **reference date**. When this data is confirmed (**Enter**), a list appears in the **Assignment of day models** dialog field below it. The number of lines in this list corresponds to the number of days set above, and the columns already contain a progressive number and the dates for the period, beginning with the start date selected.
Only entries of the column **"Name"** can be changed or inserted by the user in this list - as already mentioned, the entries in the columns **“No”** and **“Date”** arise from the declarations of the dialog head; the column **"Description"** is filled out by the system with the choice of a day model and the explanations done in this dialog.
By double-clicking in the relevant line of the **Day model** column, a selection list field is activated. One of the existing day models can be selected from this list. In this way, a specific day model can be assigned to each day of the period. When the user switches to another line, an existing description of the selected day model is indicated by the system in the **Description** column.
The predefined **holidays** with the relevant day models are shown in the lower list field for navigation and checking purposes. For the selected or newly created time model, the assignment of day models to certain holidays can be changed. However, these changes will only apply to this particular time model - general changeovers that are to apply to all existing and future models can only be performed in the Holidays dialog. In line with these settings, the week days are then given the assigned day models, in consideration of the holidays.
Then appropriately to these settings the weekdays are faced with the assigned day models under consideration of the special days. To quickly check that day models are have been used and assigned correctly - particularly on holidays - this dialogue contains a **preview** that shows the day allocation of certain periods.
Finally, a separate dialog box is opened by clicking the **Preview** button and a time period of up to 90 days can be specified, including holidays. When the **Calculate** button is clicked, the report is composed and displayed as shown below - this process can take a few seconds depending on the size of the interval.



In the default setting the special days are applied to the time models according to their definitions. Should the special days find, however, exceptionally no consideration, this can be caused by the choice of the option **Ignore special days**. Simultaneously the entries from the two lower lists are deleted, so that it is evident to the user immediately that the special days and day classes find no use in this model.



11.3 Reports

11.3.1 Reports

This section describes a collection of report functions that can be used to filter system and event log data, and to present it in clear formats.

Dialog path

Main menu > **Reports**.

A choice of reports is available:

- **Master Data**
- **System Data**
- **Authorizations**

Using the reports toolbar

Click  to display a preview before printing.

The preview has its own toolbar:

- Click ✕ to exit the preview without printing.

– Use the arrow keys |◀ ◀ 2 of 17 ▶ ▶| in the preview toolbar to browse back and forth, or to select individual pages by page number.
– Click  to print immediately, using your default printer
– Click  to print via a Print Setup dialog, which allows further print options.
– Click  to export the report to a selection of file formats, including PDF, RTF and Excel.
– The numbers on the right of the toolbar represent:
  – The total number of existing database entries that correspond to the filter criteria.
  – The percentage of those database entries that are displayed in the preview.

Applying sort criteria

The sort criteria that are currently applied appear on the left, and available criteria on the right.

The sort criteria on the left are applied in order, top to bottom.

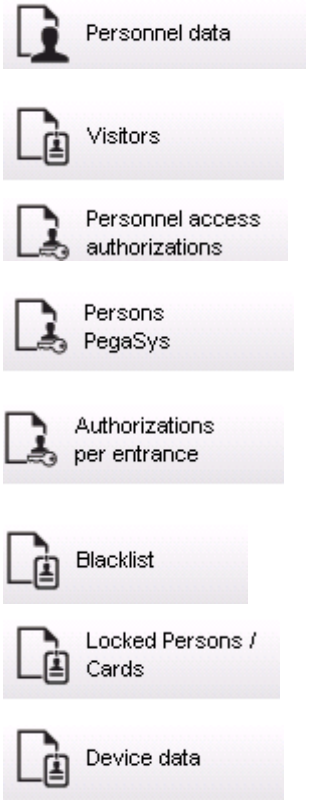
Use the arrow buttons  and  to add or remove criteria, and to change the order of the criteria on the left.

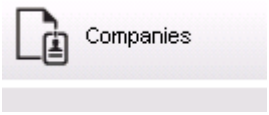
Click **Default** to restore the default sort settings.

11.3.2 Master Data

Reports overview - Master Data

The Master Data reports includes all reports concerning persons, visitors, cards and their access authorizations. Futhermore the device data and company data can be displayed.





Report: Personnel Data
Two filters can be applied when creating reports.
Person filter: Here, the operator filter based on the usual personnel data fields.
Access card filter: Here, the operator can filter based on the card numbers, ranges of numbers, the status, and the blocking status.

Report: Visitors
Similarly to the personnel data, reports of visitors can be created here. In doing so, it is still possible to access all created visitor data, i.e. even visitors who have yet to arrive but who were already registered can be selected.

Report: Personnel Access Authorizations
This report gives an overview of the access authorizations registered on the system and also shows the persons to whom these authorizations have been assigned.
In terms of filters, personal data and the selection of certain authorizations can be used:
– Personnel data: Surname, first name, personnel no.
– Validation of all authorizations.
– The name of the authorization the entrance is included.
– The name of the time model - if exists.
– Direction for the entrance.
– Validation of the special authorization.

Report: Blacklist
In this dialog, a list can be printed detailing all or a desired selection of ID cards that have been put on the blacklist for various reasons.

Report: Blocked Persons/Cards
This dialog can be used to create reports containing data about all blocked persons.
Use dates to find blocks within specified time periods.

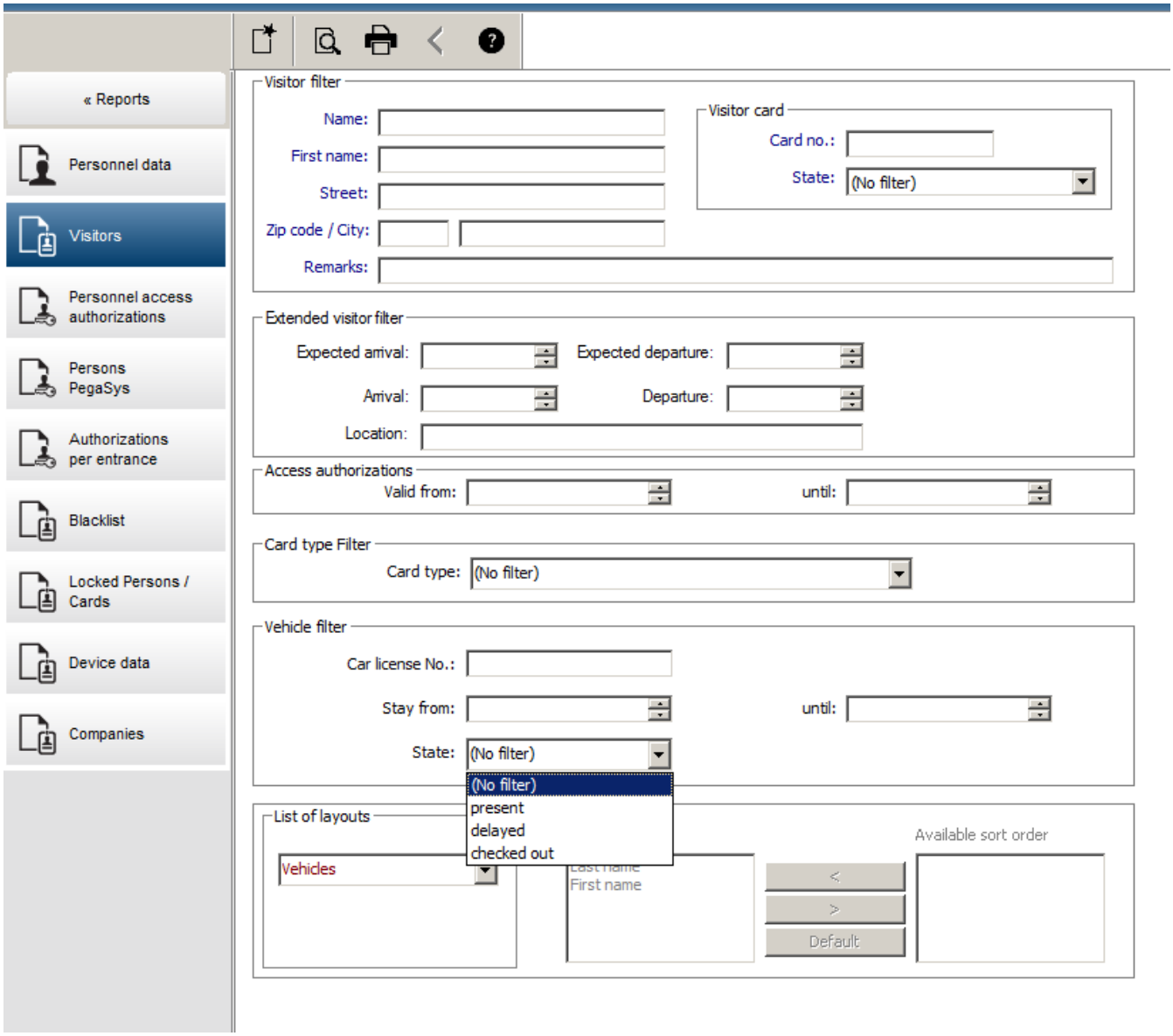
Report: Device Data
The dialog can be used to create reports based on device data, e.g. device name or device type.

Report: Companies
The Companies report dialog is used to collate company data in a list.
Use asterisks, for example, to find companies that begin with a certain letter.

11.3.3 Report for vehicles

In the dialog **Reports > Visitors** it is possible to select **Vehicles** from the layout list. Once **Vehicles** is selected the dialog area **Vehicle filter** is activated and can be used by the operator to filter out vehicles and their status.
The status is displayed as follows:
– Present: Visit not yet finished and time not yet expired.

- Delayed: Visit not yet finished, but time expired,
- Checked out: Visitor has returned all access cards.



The **Report for vehicles** only is available for visitors because the expected arrival date, expected departure date, arrival date and departure date are only available for visitors in the database table **Visitors**.

The report only lists the vehicle numbers which are stored in the database table **Persons**. So once a vehicle number has been changed, the report will provide other results.

The duration will be calculated as follows:

- if the visitor already checked out, the difference between arrival and departure in minutes will be displayed.
- if the visitor has not checked out yet, the time from arrival in minutes until now will be displayed

Access Engine

Vehicle

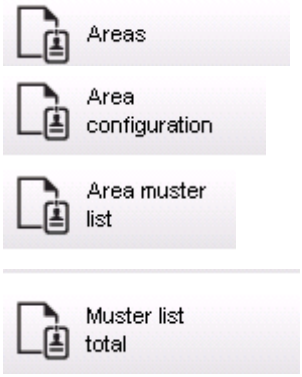
Datum 02.07.2014 , 14:26:14
Seite 1

Lastname	Firstname Status	Arrival Departure Duration	Vehicle Last area	Person Last area
Neuer Besucher mit Langem Namen	**Vorname** present	02.07.2014 14:21 02.07.2014 14:30 0h 5'	AC BB 5678 parkplatz_01	ASB
Test	**Visitor** too late	01.07.2014 09:10 02.07.2014 12:00 29h 16'	AC AA 1234 parkplatz_01	ISB
Testbesucher mit sehr lagem Namen	**Besucher mit gaaaaaanz langem namen** departed	01.07.2014 07:30 01.07.2014 12:00 4h 30'	AC AA 2345 AUSSEN	AUSSEN

11.3.4 System Data

Reports - System Data

In contrast to the master data, the system data is information that is assigned to the system and is not person, ID card or company-related. These reports are explained in more detail below.



Report: Areas

This dialog can be used to collate the locations in a report. The dialog contains only one area filter, which offers the various buildings and other zones for selection.
The area concerned is selected via a left mouse click. The user can view the report on the screen using the **Preview** button before he starts the printing process with **Print**.
There are two layouts available.

	Standard	Persons present in the location - no parking lots
	Parking lot occupancy	Persons present in the location - only parking lots

To check that the datasets displayed are up to date, the last card scannings for the areas are also listed.
Reliable information about the locations of persons can therefore be given for various events.

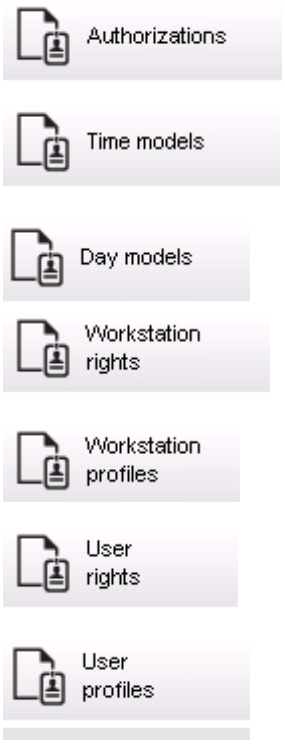
Report: Areas Configuration
Defined areas and their subareas with a flag signed parking lots and maximum number of persons or cars.

Report: Area Muster List
As well as being listed according to purely numerical data, the persons in an area can also be listed by name.
With the scanning times for the individual areas, these reports also contain the times for each individual person.

Report: Muster List Total
In principle, the muster lists correspond to the **Areas** report dialog; however, they offer lists for the specific zones, which provide information about the number of persons currently in that area according to access control.

11.3.5 Authorizations

Overview
In this menu item, a summary is provided of the various authorizations given in the corresponding dialogs:



Report: Authorizations
This dialog can be used to display the access authorizations defined in the system. The entrances belonging to the individual access authorizations are listed. The name of the selected time model is displayed. In addition, this report shows the number of persons to whom the authorization is assigned.

Report: Time Models
This report can be used to display the time models defined in the system, as selected. This report displays all data associated with the model as well as the number of the persons to whom the model.

Report: Day Models
This report displays all defined day models with their names, descriptions, and the intervals they contain.

Report: Workstation Rights
This dialog can be used to display the workstation rights assigned to the workstations defined in the system.

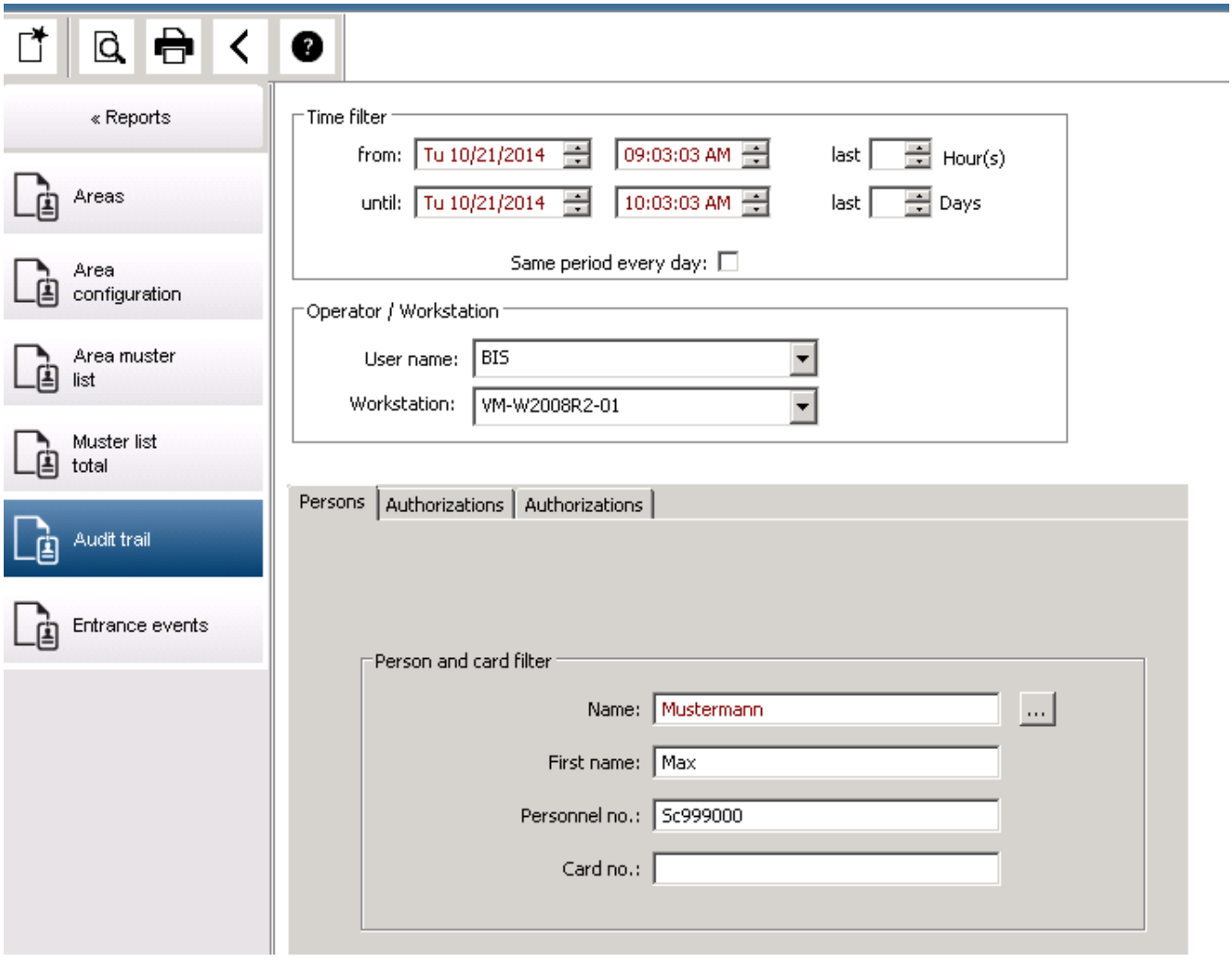
Report: Workstation Profiles
This dialog can be used to display the workstation profiles defined in the system; this allows the system operations that are possible on the individual workstations to be presented in a clear format.

Report: User Rights
This dialog can be used display the assigned user profiles for users defined in the system.

Report: User Profiles
This dialog can be used to display the assigned dialogs and dialog rights for the user profiles defined in the system.

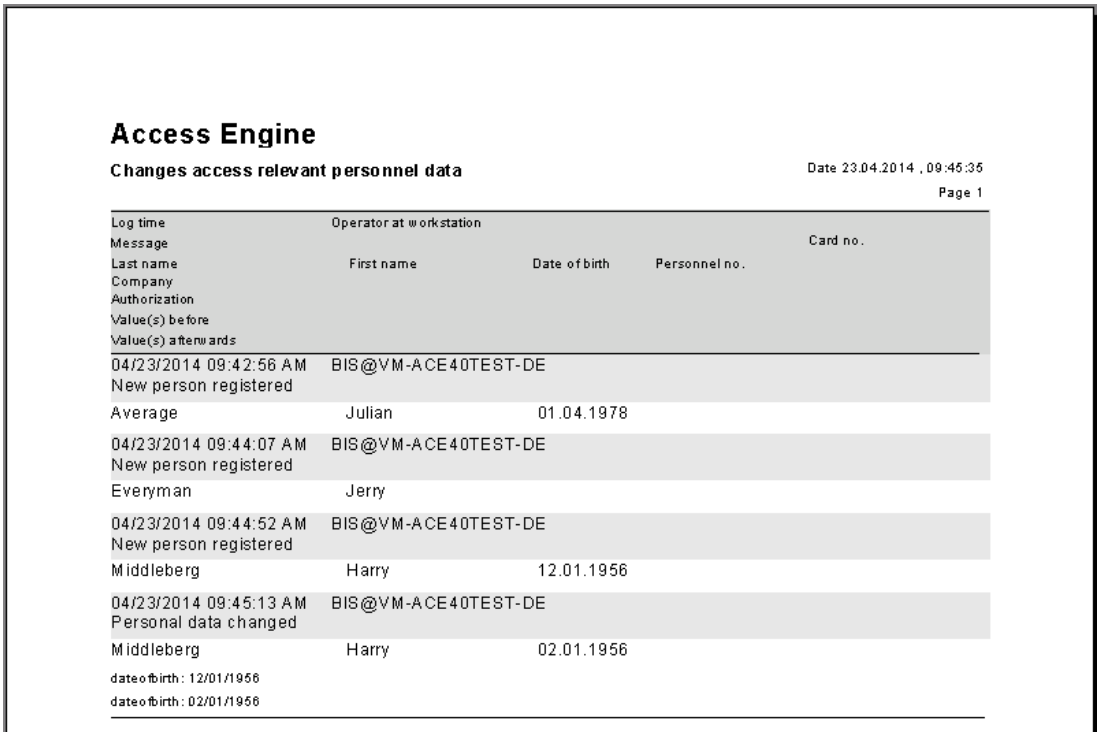
11.3.6 Report Audit trail

The Audit log Report uses the system event log to select the actions of operators for the last 30 days (default). The default value is low because activity is typically high, which causes large volumes of data.



The following images show examples of the various templates:

Template Personal Related Data:



Access Engine

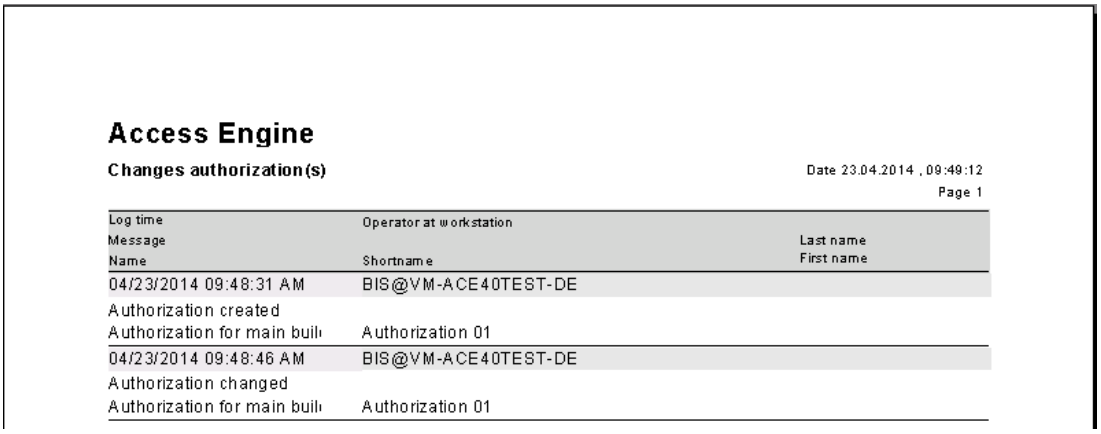
Changes access relevant personnel data

Date 23.04.2014 , 09:45:35

Page 1

Log time Message Last name Company Authorization Value(s) before Value(s) afterwards	Operator at workstation First name	Date of birth	Personnel no.	Card no.
04/23/2014 09:42:56 AM New person registered	BIS@VM-ACE40TEST-DE			
Average	Julian	01.04.1978		
04/23/2014 09:44:07 AM New person registered	BIS@VM-ACE40TEST-DE			
Everyman	Jerry			
04/23/2014 09:44:52 AM New person registered	BIS@VM-ACE40TEST-DE			
Middleberg	Harry	12.01.1956		
04/23/2014 09:45:13 AM Personal data changed	BIS@VM-ACE40TEST-DE			
Middleberg	Harry	02.01.1956		
dateofbirth: 12/01/1956 dateofbirth: 02/01/1956				

Template Authorization Changes:



Access Engine

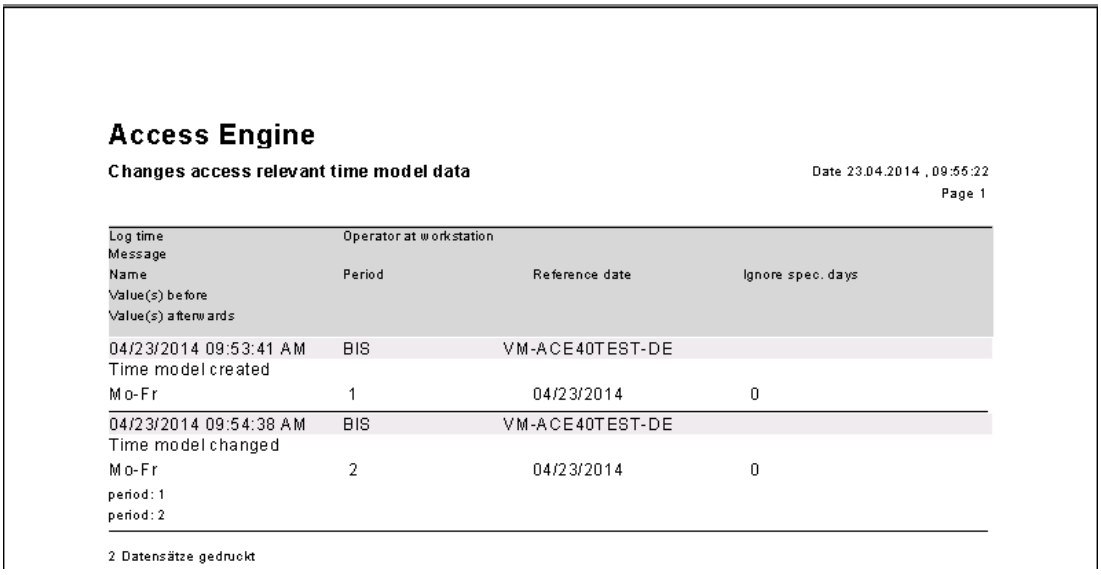
Changes authorization(s)

Date 23.04.2014 , 09:49:12

Page 1

Log time Message Name	Operator at workstation Shortname	Last name First name
04/23/2014 09:48:31 AM	BIS@VM-ACE40TEST-DE	
Authorization created Authorization for main buil	Authorization 01	
04/23/2014 09:48:46 AM	BIS@VM-ACE40TEST-DE	
Authorization changed Authorization for main buil	Authorization 01	

Template Time Models:



Access Engine

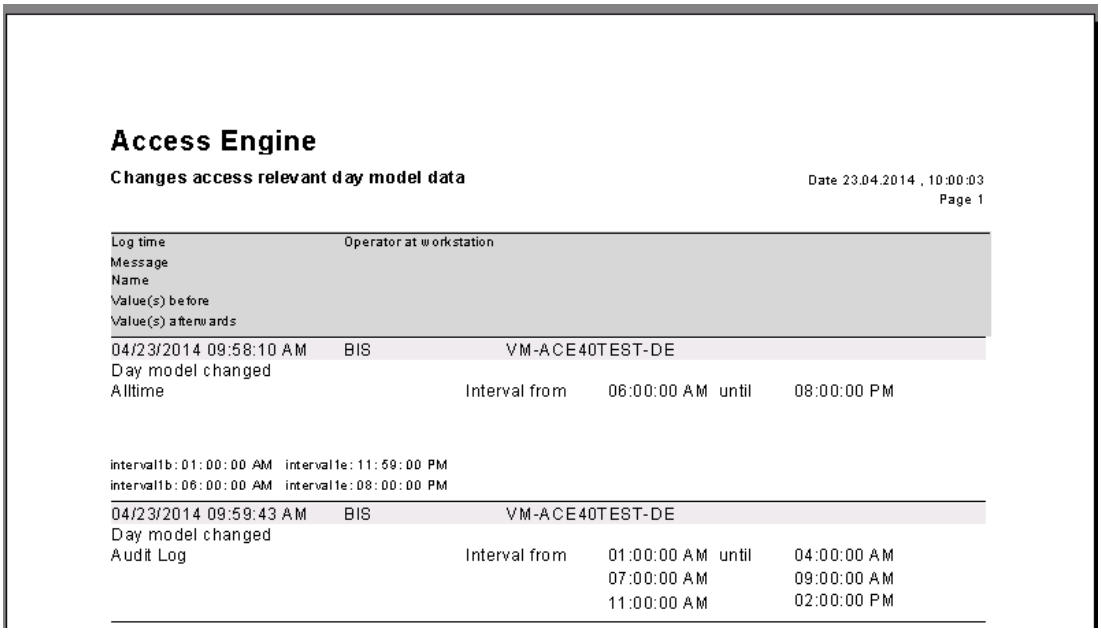
Changes access relevant time model data

Date 23.04.2014 , 09:55:22
Page 1

Log time	Operator at workstation		
Message			
Name	Period	Reference date	Ignore spec. days
Value(s) before			
Value(s) afterwards			
04/23/2014 09:53:41 AM	BIS	VM-ACE40TEST-DE	
Time model created			
Mo-Fr	1	04/23/2014	0
04/23/2014 09:54:38 AM	BIS	VM-ACE40TEST-DE	
Time model changed			
Mo-Fr	2	04/23/2014	0
period: 1			
period: 2			

2 Datensätze gedruckt

Template Day Models:



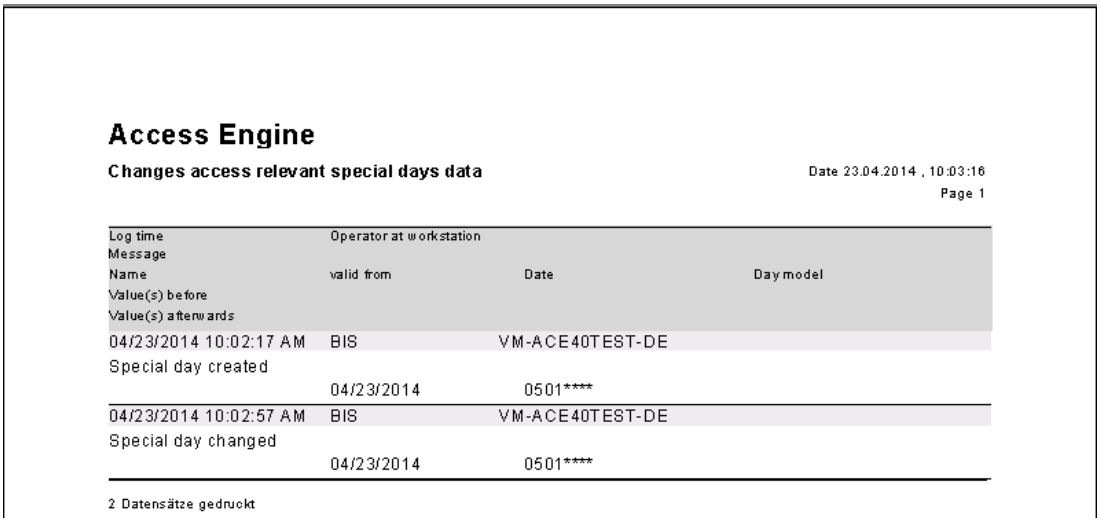
Access Engine

Changes access relevant day model data

Date 23.04.2014 , 10:00:03
Page 1

Log time	Operator at workstation				
Message					
Name					
Value(s) before					
Value(s) afterwards					
04/23/2014 09:58:10 AM	BIS	VM-ACE40TEST-DE			
Day model changed					
Alltime		Interval from	06:00:00 AM	until	08:00:00 PM
interval1b: 01:00:00 AM interval1e: 11:59:00 PM					
interval1b: 06:00:00 AM interval1e: 08:00:00 PM					
04/23/2014 09:59:43 AM	BIS	VM-ACE40TEST-DE			
Day model changed					
Audit Log		Interval from	01:00:00 AM	until	04:00:00 AM
			07:00:00 AM		09:00:00 AM
			11:00:00 AM		02:00:00 PM

Template Special Days:



Access Engine

Changes access relevant special days data

Date 23.04.2014 , 10:03:16
Page 1

Log time Message Name Value(s) before Value(s) afterwards	Operator at workstation valid from	Date	Day model
04/23/2014 10:02:17 AM Special day created	BIS 04/23/2014	VM-ACE40TEST-DE 0501****	
04/23/2014 10:02:57 AM Special day changed	BIS 04/23/2014	VM-ACE40TEST-DE 0501****	

2 Datensätze gedruckt

11.4 Divisions

11.4.1 Introduction

The BIS system is designed so that the data of several clients can be managed independently of each other in a database and via one dialog system.
It is therefore possible, for example, to manage buildings or entire plants which are used by several independent companies with one access control system. Here, personnel data as well as system data and devices are assigned to a certain division and can only be seen and processed by workstation users with respective rights.
This module, which can be ordered as a software extension, already forms the basic system in every Access Engine access control system. In the standard delivery, all datasets are given the **Common** division. If new divisions are set up - this also applies if carried out at a later date - new datasets can be created under these divisions without being accessible from Common. Existing data that was previously Common can be moved to the new division or another division.
When the system is installed, the afore-mentioned **Common** division is created. When ordering the **Division** software extension, the number of additional divisions is activated in accordance with the licenses. Because this setup is valid throughout the system, creation and configuration are carried out via the BIS manager.
Each division is identified by a **separate color** in the list.

11.4.2 User Disposition

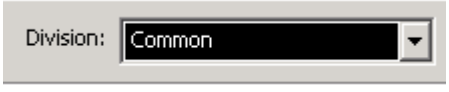
BIS system users are set up via the BIS manager. In addition, these users are given specific rights for the Access Engine access control system. In the dialogs for dialog authorization, which can be called up via the BIS configuration manager, the users that have been set up are given processing rights for access control data through the assignment of user profiles. The rights for division-oriented data are also assigned there at the same time.
A user can be given processing rights for several divisions. Every user has implicit access to data for the **Common** division.
In the **Divisions** select the location where the data should be saved.
While a dialog is being processed, users can only see and process datasets for one division (+ the Common data). A selection list in the toolbar can be used to switch to other divisions, provided that the user is permitted to be active for several divisions.

If the multi-client system is activated, data is subdivided into two categories:
– Not division-specific (= Common)
– Division-specific
Data that belongs to the **Common** category can be seen by all dialog operators of all divisions and processed by them - provided that they have the relevant rights. Data that belongs to specific divisions can only be selected and processed by dialog operators who have authorization for this division.

Notice!
In every system there will be a user with general rights who is automatically given processing rights for all existing and future divisions and for the Common category.
This setup is necessary for there to be a central office that can work throughout system.

11.4.3 General Data Processing

If the multi-client system is activated, data is subdivided into two categories:
– Not division-specific (= Common)
– Division-specific
Data that belongs to the **Common** category can be seen by all dialog operators of all divisions and processed by them - provided that they have the relevant rights. Data that belongs to specific divisions can only be selected and processed by dialog operators who have authorization for this division.
The toolbar contains an additional selection list field: **Division**. This list contains the divisions for which the operator who is logged on possesses the processing rights, and the entry **Common**. The divisions are sorted alphabetically in this list At the start of the dialog manager, the first division in the list other than Common is set.



In addition, the selected division will be displayed in the lower status bar:

When selecting datasets, only data is selected that belongs to the set division and the **Common** category. When the **Common** category is selected, only datasets from this category are selected - no division-specific datasets.

Notice!
Only one entry can be selected from the Division list at any time.

Notice!
With the exception of personnel and device data (device data via the BIS user interface), the affiliation to a division **cannot** be changed for all other data. This applies to preconfigured datasets as well as newly created datasets.

The following access control data can be division-specific. The dialogs concerned contain the **Division** selection list field and any existing list fields are given the additional column **Division** - the dialog and menu titles concerned are given here:

- Persons
- Visitors
- Companies
- Access Authorizations
- Area-Time Authorizations
- Access Profiles
- Day Models
- Holidays
- Time Models
- Guard Tour
- Path Control
- Reports

Notice!
Persons who belong to the Common category can be given data from other divisions. For example, these persons can be given access authorizations belonging to a specific division.

Creating new records
Newly created datasets are assigned to the currently selected division.

Notice!
Once a dataset has been saved with the assignment to a division, this can no longer be changed.
Exception:
Personnel Data - a special dialog exists for changing the division for personnel.

11.4.4 Special Data Processing

Persons can belong to specific divisions or to the **Common** category.
The search for datasets selects data from the division that is currently set and from the Common category. If the search takes place in the **Common** setting, only datasets belonging to this category are selected.

Dialog: Cards
With regard to **path control**, the following special features apply on the **Other data** tab:
Paths of other divisions are indicated in an explanatory note to ensure that these are not accidentally overwritten.
Example:
If an operator has, for example, the processing rights for division "A" datasets and can therefore select data for this client and for the Common category, and a selected person from the Common category has been given a division "B" path, this path is grayed out (i.e. not cannot be selected or processed) and displayed with the explanatory note, **External division**.

Dialog: Set area
The operator can only see the areas that belong to the division for which he has processing rights. If the selected person is in another division's area, this is indicated with the entry **External division**.

Dialog: Register/Deregister Visitor Cards
The registration occurs when the ID card is assigned to the currently selected division. Only ID cards registered as Common can be used for Common visitors or division-specific visitors.

Notice!
Each visitor ID card can only be registered once. A decision must therefore be made as to whether each division has its own pool of visitor ID cards or whether these are registered as Common ID cards and are therefore available for all clients.

Dialog: Visitors
Only persons from the currently set division and the Common category can be selected as an **attendant** and **visited person**.
This also applies to the assignment of the ID card: only cards registered for the division to which the visitor is also assigned (or Common), can be assigned.

Dialog: Define Paths
Every operator can define paths that contain readers belonging to the division for which he possesses processing rights and which belong to the Common category.
The operator with general rights can access all readers and is able to define paths containing readers that belong to several divisions.
Example:
A path must be defined for the cleaning staff which includes the Common areas as well as those belonging to divisions A, B and C. A path is defined in the Common category that contains Common, division A, division B and division C readers. Now this path can be used by operators of all three divisions; however, operators who do not possess processing rights for all of these divisions are unable to see the path.

Dialog: Define Guard tours
Each operator can define guard tours that contain readers belonging to the division for which he possesses processing rights and those belonging to the Common category.
The operator with general rights can access all readers and is able to define guard tours containing readers that belong to several divisions.
Example:
A tour must be defined for a patrol which includes the Common areas as well as those belonging to divisions A, B and C. A tour is defined in the Common category that contains Common, division A, division B and division C readers. Now this guard tour can be used by operators of all three divisions; however, operators who do not possess processing rights for all of these divisions are unable to see the tour.

Dialog: Manage Guard tours
The division-specific operator can only see guard tours that belong to his division or the Common category. He can also only use ID cards for a patrol that are assigned to that division and the Common category.

11.4.5 Changing the Division for persons

Introduction
Change division is a powerful dialog for changing the Division of a set of personnel records in the system.

Notice!
Use this feature with great care!
A change in Division has far-reaching consequences for the personnel records that you change.

Prerequisites

The operator who changes the Division of personnel records, must have authorizations to edit those persons and both the divisions concerned.

Dialog path

Main menu > **Personnel data** > **Change division**

Procedure

1. In the **Filter persons** pane, enter filter criteria in one or more of the following fields:

Filter	Remarks / Description
Last name	Use a single asterisk to match all persons, or letters **without** asterisks
Personnel no. from/ to	Use both fields to define a range of values
Employee ID (Employee type)	Select from the list
Division	The Apply filter button shows only persons from this Division
Company	Select from available companies
Department	
Card no. (from/to)	Use both fields to define a range of values

2. Click **Apply filter**
   All persons that match the filter are displayed in the **Selected persons** list**.**
3. To further refine the set of selected persons click one or more lines in the **Selected persons** list and then click the **Remove** button. Use the Ctrl and Shift keys to select multiple records at once.
   – **IMPORTANT:** Before proceeding, make sure that the **Selected persons** list contains only persons for which you want to change the Division.
4. In the **New division** list, select the destination Division for the selected persons.
5. Click **Change division of persons**
   ALL the persons in the **Selected persons** list are moved to **New division**.

Effects of changing from one division to another

Persons

– Access authorizations and path control
– Links to the previous division are deleted.
– Links to data of the category Common are retained.

Companies

– Links to companies of the previous division are deleted.

Effects of changing from Common to another division

– Access authorizations and path control
– Links to Common and the new division are retained.
– Links to other division are deleted.

Effects of changing from one division to Common

All links are retained.

Bosch Security Systems B.V.
Torenallee 49
5617 BA Eindhoven
Netherlands
www.boschsecurity.com

202105212011