



MATRIX

Access

User Documentation

1073G-00-B1a -Version 3.7

EN

dormakaba 

dormakaba EAD GmbH

Albertistrasse 3

78056 Villingen-Schwenningen

Germany

www.dormakaba.com

Copyright © dormakaba 2020

All rights reserved.

This documentation must not be reproduced or used in any way without the written permission of dormakaba Holding.

All names of products are brands of the respective companies.

Subject to technical modifications.

Contents

1 Introduction	6
2 Getting started	7
2.1 Creating a new access system	7
3 Working with MATRIX	9
3.1 Access control instructions	9
3.1.1 ▶ Set up Mobile Access	10
3.1.2 ▶ Add a door	13
3.1.3 ▶ Create a door opening with keyboard input	14
3.1.4 ▶ Set up access control for two persons	17
3.1.5 ▶ Set up office release	18
3.1.6 ▶ Work with visitor administration	20
3.1.7 ▶ Set up visitor administration with QR codes	23
3.1.8 ▶ Set up a keyboard reader for duress alarm	25
3.1.9 ▶ Work with AccessOnCard AoC (for XS/evolo components)	27
3.1.10 ▶ Create a lift control	30
3.1.11 ▶ Set up an IDS connection	33
3.1.12 ▶ Configure the counting information option	35
3.1.13 ▶ Work with video surveillance	37
3.1.14 ▶ Monitor doors with manual image comparison	44
4 Dialogs in the Access module	45
4.1 Person administration	46
4.1.1 Persons	46
4.1.2 Departments	60
4.1.3 Access profiles	61
4.1.4 VBI permissions	64
4.1.5 IDS profiles	65
4.1.6 Priority circuits	66
4.1.7 Access weekly profiles	68
4.1.8 Access daily times	71
4.1.9 Reasons for blocking person	73
4.1.10 Search profiles	74
4.2 External company administration	76
4.2.1 External company employees	76
4.2.2 External companies	85
4.3 Visitor administration	86
4.3.1 Overview of visits	86
4.3.2 Visitor reservations	92
4.3.3 Visitors	96
4.4 ID card administration	98
4.4.1 ID cards	99
4.4.2 Priority circuits	106
4.4.3 Reasons for blocking ID card	109
4.5 Room administration	110
4.5.1 Reservations	110
4.5.2 Rooms	113

4.6 Area/door administration	114
4.6.1 "Security areas - Doors" dialog - Security area	114
4.6.2 Counting groups	131
4.6.3 Door weekly profiles	132
4.6.4 Door daily times	135
4.6.5 Security area weekly profile	139
4.6.6 Security area daily programs	141
4.7 Calendar administration	142
4.7.1 Calender	142
4.7.2 Additional options (calendar)	146
4.8 Locking plan administration	155
4.8.1 Locking plan	156
4.8.2 Person groups	161
4.8.3 Door groups	162
4.9 Additional functions	163
4.9.1 Corrections	164
4.9.2 Interlocks	165
4.9.3 Lifts	167
4.9.4 Intruder detection systems	169
4.10 Area monitoring	188
4.10.1 Security areas	188
4.10.2 Set persons	189
4.11 Door monitoring	191
4.11.1 Status display	191
4.11.2 Allocate door selectionAllocate door selection	195
4.11.3 Door selection	196
4.12 Patrol	197
4.12.1 Status display	198
4.12.2 Patrols	199
4.12.3 Patrol definitions	201
4.12.4 Patrols log	203
4.13 Attendance display (access)	205
4.14 Reports (access)	210
4.14.1 Person access report	211
4.14.2 Reader events report	212
4.14.3 Reader locations	213
4.14.4 Access times	215
4.14.5 Access profiles	216
4.14.6 Display access permissions overview	218
4.14.7 Person access permissions	220
4.14.8 Door access permissions	223
4.14.9 Room zone access permissions	224
4.14.10 ID card history	226
4.14.11 Blocked AoC ID cards	227
4.14.12 Blocks	230
4.14.13 Attendance report	230
4.14.14 Visits	232
4.14.15 External company employee	235

4.14.16 Booking evaluation for person	238
4.14.17 Smart phone status	241
4.14.18 Time-controlled reports	242
4.14.19 Print system data	245
4.15 Special reports	247
5 Glossary	248
6 Index	250

1 Introduction

This user documentation describes and explains the operation of the access module of dormakaba MATRIX.

In the first part you will find examples and procedures for the most common tasks. The main body of the documentation is based on the menu structure of the access module.

Note: The dialogs displayed in the user documentation contain all available options of the system. Depending on the licence and the activated options your dialogs may differ from the descriptions.

For detailed and basic operating instructions see the user documentation of the basic module.

2 Getting started

Note: Setup, commissioning and maintenance of a MATRIX system must be performed by trained expert personnel.

If you have no experience with the access module of dormakaba MATRIX, this section provides information on the necessary steps for creating a new access system.

For general operating instructions and information on the user interface see the user documentation of the basic module.

Tip: The menu structure of all modules in the system is set up in such a way that when you create a new system, you always work "from bottom to top". In this way, you form the structure of your data from the bottom upwards.

2.1 Creating a new access system

The procedure for creating a new access system consists of four steps:

- I. Creating and defining the hardware components (devices) in dormakaba MATRIX, so that the system can recognise them.
- II. Transferring the configuration data to the hardware components.
- III. Defining possible access times to the doors.
- IV. Defining the access permissions for persons.

You do not have to perform all of the aforementioned steps for existing systems with existing records.

I. Creating hardware components

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. Create the installed hardware components in the device tree according to their physical positions.

Note: The ID card types and device classes required for your devices were set up when the system was installed. If you need new ID card types or classes for new devices, you have to create them first as described in the relevant sections of the user documentation.

II. Transferring the configuration data to the hardware components

1. Click **Devices** in the menu bar, then **Load/display terminal** in the menu tree.
2. Select the devices whose data you would like to load by activating the corresponding checkboxes.
3. In the toolbar, click **Edit selected search results** or click **Edit all search results** if you want to load all records. The selected records open in the dialog **Load data**.
4. If you only want to transfer some of the data, activate the **Expert mode** checkbox. In expert mode, you can select all the configuration data and application data to be loaded individually.

Note: The application data is transferred automatically when it is created for the first time.

5. Click the **Transfer data** button.

Note: You can find information on transferring data to the XS/evolo offline components using XS Manager in the separate user documentation on XS Manager.

III. Defining access permissions for the doors

1. In the menu bar, click **Access** and open **Calendar administration** in the menu tree.
2. Create at least one **Calendar** that is used as the basis for the time-based access control.

Note: The submenu **Additional options** provides access to the definitions of the weekdays, bank holidays, special days and day types. As these are already pre-installed, you do not have to make any changes here to create a new calendar.

3. Open the menu item **Room zone/door administration**.

Note: Depending on the system settings, this menu item can have various names:

Security areas – doors, if security areas are activated.

Room zones/doors, if only room zones are activated and not security areas.

Doors, if no security areas or room zones are activated.

4. Click **Door daily times** and define the access times.
5. Click **Door weekly profiles** and assign the door daily times to the days of the week.
6. Click **Room zones – doors** or **Doors** and illustrate the local structures.
7. Define the room zones. This step does not apply if you control access permissions directly using the reader.
8. Define all **Doors** that have a reader.

IV. Define access permissions for persons

1. Open **Person administration** in the **Access** module.
2. Click **Access daily times** and define the access times for the person groups.
3. Click **Access weekly profiles** and assign the door daily times to the days of the week.
4. Click **Access profiles** and connect the access weekly profiles to the room structures.
5. Click **Departments** and illustrate your company's organisational structures. This step is optional.
6. Click **Persons** and create the persons with the relevant access permissions.

3 Working with MATRIX

This section provides support for setting up and maintaining your MATRIX system.

The "How to" instructions are grouped by the MATRIX modules.

3.1 Access control instructions

This section will help you to configure the access functionalities.

- ▶ [Set up Mobile Access](#)
- ▶ [Add a door](#)
- ▶ [Create a door opening with keyboard input](#)
- ▶ [Set up access control for two persons](#)
- ▶ [Set up office release](#)
- ▶ [Work with visitor administration](#)
- ▶ [Set up visitor administration with QR codes](#)
- ▶ [Set up a keyboard reader for duress alarm](#)
- ▶ [Work with AccessOnCard AoC \(for XS/evolo components\)](#)
- ▶ [Work with OSS](#)
- ▶ [Create a lift control](#)
- ▶ [Configure the counting information option](#)
- ▶ [Monitor doors with manual image comparison](#)
- ▶ [Work with video surveillance](#)

3.1.1 ▶ Set up Mobile Access

Mobile Access functions allow all person groups (persons, external company employees, visitors) to perform access bookings using smartphones.

Note: A requirement for using Mobile Access is that the function must be enabled in MATRIX. Ensure that the system parameter Access 150 is set to 1.

When using Mobile Access, access permissions for persons are granted in the same way as access permissions via RFID card. A connection is required between MATRIX and a Mobile Access Connector (LEGIC Connect) in order to be able to use permissions on a smartphone. For this purpose, the **dormakaba mobile access** app must be installed on the smartphone, which will be used to receive the access permissions.

As soon as an e-mail address and a Mobile Access device number are saved in the record, the person (visitor, external company employee) receives an e-mail notification prompting them to download the app from the App Store. E-mail dispatch must be configured for automatic notifications to work.

Users can also read their own bookings and the status of components via smartphone using the **dormakaba mobile access** app. To be able to do this, history logging must be activated in the class and system parameter Access 155 must be enabled.

Important note: If you wish to use Mobile Access in conjunction with RFID ID cards, the ID card administration level "Several ID cards per person" (2) must be set in step 5 ("ID cards"). Otherwise, the master ID card type will be set to Mobile Access and will apply to all ID cards.

Mobile Access can be used both with LEGIC and with MIFARE DESFire.

Permission models

There are two different permission models in Mobile Access:

A. Permission via Infinilink:

- This permission type is only supported by standalone components.
- Infinilink permissions are encrypted and stored on the smartphone.
- Infinilink permissions can only be read by the component.

B. Permission via Infini-ID:

- This permission type is supported by standalone and wireless components.
- Permissions are transferred to the components.
- A virtual ID card number (= Infini-ID) is encrypted and stored on the smartphone.

Perform the following steps to set up Mobile Access:

I. Activate Mobile Access in the terminal class

The type and parameters of the Mobile Access communication technology are specified in the terminal class. Communication can be established via NFC and/or BLE.

1. Select the menu item **Class administration** from Device management.
2. Select the evolo terminal class from **Classes**.
3. In the **Bluetooth and Mobile Access parameters** area, enable the use of Mobile Access by activating one of the two checkboxes, regardless of which communication technology (NFC or BLE) is going to be used. You can also use both communication technologies in parallel.
4. If necessary, adjust the scan duration and power level (RSSI filter) to meet your requirements.

II. Create LEGIC Mobile Access Connector

The end-to-end management service LEGIC Connect is used to connect to smartphones. The connection between the MATRIX server and LEGIC Connect is established via the LEGIC Mobile Access Connector.

1. Switch to the **Devices** dialog, select the appropriate node and click **Create new record**.
2. Select the LEGIC Mobile Access Connector and enter the LEGIC Connect data.

III. Connect KCP reader via Mobile Access

The ID card number is transmitted from the smartphone to a MATRIX terminal via the KCP interface. For this purpose, a KCP reader (e.g. compact reader 91 12) with Mobile Access capabilities must be created below an AM TP4 terminal (e.g. AM 92 00).

1. Go to the AM TP4 terminal that will be used for Mobile Access in the device tree.
2. Click **Create new record** and select the KCP reader.
3. Configure the KCP reader using the LEGIC configuration packages.

Note: The ID card number allocated to the smartphone is transferred to the terminal along with the employee record.

IV. Activate Mobile Access (Infinilink) identifier for components

The Mobile Access component connection must be specified in device configuration.

1. Click the components in the device tree for which you wish to enable Mobile Access.
2. In device configuration, activate the **Mobile Access (Infinilink)** checkbox to grant access permissions to the components directly on the smartphone without needing to update the components using the programmer (in the same way as for AoC functions).

Note: If this option is not set, and if a smartphone is permitted for the components, the smartphone can be used as a substitute ID card medium in evolo offline/whitelist mode (using Infini-D).

3. Configure the components using a LEGIC configuration package.

V. Enable Mobile Access and access permissions for the person

LEGIC Mobile Access Connector must be able to identify the smartphone uniquely to be able to send access permissions to a smartphone. Mobile Access uses the telephone number of the smartphones in the same way as the ID card number is used for RFID ID cards.

The telephone number must be entered in the person's employee record as a Mobile Access number to enable bookings to be made via smartphone. The procedure depends on the ID card administration level.

Access permissions are granted using the same procedure as for RFID ID cards. The procedure for blocking persons or ID cards is also the same as the existing process. When blocking ID cards of the Mobile Access type, the validity period stated in the system parameter Access 151 is evaluated to determine the blocking/expiry date.

ID card administration level 1:

As each person can only be allocated one ID card in ID card administration level 1, booking using RFID ID cards is no longer possible for the person in question once Mobile Access is set up.

Note: Note: Set the system parameter "ID card type master ID card" (system parameter System 74) to the value 3 (Mobile Access) to be able to use Mobile Access in ID card administration level 1.

1. Switch to the main **Access** menu and click **Person administration** in the menu tree.
2. Click **Persons** and open the appropriate employee record of the person for whom access via Mobile Access is being set up.
3. Enter the telephone number of the smartphone the tab in the **Mobile Access device number** input field on the **Access** tab. The Mobile Access number requires the prefix "phone#", e.g. "phone#+4917256889755".
4. Assign access permissions for the person's bookings via Mobile Access on the **Permissions** tab.

ID card administration level 2:

As multiple ID cards can be allocated to each person in ID card administration level 2, Mobile Access can be used in addition to booking via one or more RFID ID cards.

1. Switch to the main **Access** menu and click **Person administration** in the menu tree.
2. Click **Persons** and open the appropriate employee record of the person for whom access via Mobile Access is being set up.
3. Add the smartphone to the **ID cards** table on the **Access** tab. To do this, click **New entry**, select the **ID card type** "Mobile Access" and enter the telephone number of the smartphone in the field **Mobile Access device number**. The Mobile Access number requires the prefix "phone#", e.g. "phone#+4917256889755".
4. Assign access permissions for the person's bookings via Mobile Access on the **Permissions** tab.

ID card administration level 3:

As multiple ID cards can be allocated to each person in ID card administration level 3, Mobile Access can be used in addition to booking via one or more RFID ID cards.

1. Switch to the main **Access** menu and click **ID card administration** in the menu tree.
2. Click **ID cards** and select **Create new record**.
3. Enter an ID card number, e.g. the telephone number in numeric format (4917256889755) and select the person to whom this ID card will be allocated.
4. Select the **ID card type** "Mobile Access" from the **General** tab and enter the telephone number of the smartphone in the **Mobile Access device number** field. The Mobile Access number requires the prefix "phone#", e.g. "phone#+4917256889755".
5. Assign access permissions for the person's bookings via Mobile Access on the **Permissions** tab.
6. Assign the ID card to a person.

3.1.2 ▶ Add a door

If changes are made to a building or organisation in an existing infrastructure, it may be necessary to add additional doors or readers to the system.

The new components need to be added to device administration as well as to the access system. Afterwards, the data for the devices concerned needs to be synchronised once.

To create an additional door proceed as follows:

1. First create the reader in device administration.
2. If the door creates a new room zone, create the new room zone in the **Access** module under **Room zones/Door**.
3. Now create the door record and assign it a reader and access functions.

Note 1: If the new reader is a standalone component, you must synchronise the data with the evolo Programmer or the XS Manager.

Note 2: When commissioning a new system or if you wish to set up multiple standalone components, use the [XS/evolo offline doors wizard](#).

3.1.3 ▶ Create a door opening with keyboard input

Usually, access bookings are performed using an ID card. In addition, dormakaba MATRIX provides the possibility to open doors via keypad.

For doors with very low security requirements, you can assign a terminal-specific door opening code or, for higher security requirements, you can assign a person-related identification code that is treated like an ID card number.

For the terminal-specific door opening code you do not need to assign access permissions, in this case a door opening event is recorded without reference to a person. For the personal identification code, you must define a door and assign the corresponding access permissions. In this case, the door openings will be recorded and processed like bookings.

Note: To enter the door opening code or identification you need a keypad or alternatively a keypad reader. In either case, you must set the device as a keypad reader in the Devices main group. Only a reader with defined characteristics such as door unlocking pulse lengths and controlled outputs can be connected to a door.

Door opening with door opening code

To set up a door with a door opening code, you must carry out the following steps:

I. Create a terminal class for door opening

1. In the menu bar, click **Devices**. In the menu tree click **Class administration** and then on **Classes**.
2. In the selection, click the **TP4 LAN Access** class to use this class as a template.
3. In the **Edit Class** dialog, click in the toolbar on **Copy** to create a copy for the new class.
4. Enter a new description for the class and select the **Offline parameters** tab.
5. Enter the terminal-specific door opening code in the **Comparison value door opener code** field in the **Door settings** area.
6. In the toolbar, click **Save** to save the class.

II. Create terminal

1. Select **Devices** from the menu and click the **Server** main node in the device tree.
2. Click **Create new record** in the toolbar.
3. In the device selection, click the terminal to which the keypad or keypad reader is connected.
4. On the **General** tab in the **Terminal class** selection field, select the previously created class.
5. Enter a description and in the toolbar click **Save** to save the terminal.

III. Create and load keypad reader

1. Highlight the terminal to which you wish to assign a keypad reader in the **Devices** dialog in the device tree and then click **Create new record** in the toolbar.
2. In the device selection click the desired keypad reader. Even if you are using a keypad, you must select a keypad reader.
3. In the **General** tab, enter the corresponding parameters.
4. Enter a name and click **Save**. Other necessary settings for the device are specified during saving and the **Device group** tab is activated.
5. On the **Device group** tab in the **Booking instructions** selection field, select the booking instruction **31 Access door code** and save the change.
6. In the menu tree, click **Load/display terminal** and click the new terminal.
7. In the **Load data** dialog, activate the **All configuration data** checkbox and click **Transfer data** to load the terminal.
8. To open the door with the door opening code you must enter the code and confirm the entry with the **#** key.

Note: No access permissions are required for the new keypad reader.

IV. Create door

1. In the menu bar, click **Access**. In the menu tree click **Door administration** and then on **Doors**.

Note: Depending on the options activated, this menu item may also be displayed as area/door administration or room zone/door administration.

2. In the tree structure, click the node to which you wish to allocate the new door.
3. Click **Create new record** in the toolbar, then **Door** in the selection dialog to create a new door.
4. Complete the input fields and assign the previously created reader to the door.
5. In the toolbar, click **Save** to save the door.

Door opening with identification code

To set up a door with a personal identification code, you must carry out the following steps:

I. Create terminal

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, click the **Server** main node and then **Create new record** in the toolbar.
3. In the device selection, click the terminal to which the keypad or keypad reader is connected.
4. In the **Devices** dialog, enter a name and complete the required fields.
5. In the toolbar, click **Save** to save the terminal.

II. Create keypad reader

1. Highlight the terminal to which you wish to assign a keypad reader in the **Devices** dialog in the device tree and then click **Create new record** in the toolbar.
2. In the device selection click the desired keypad reader. Even if you are using a keypad, you must select a keypad reader.
3. In the **General** tab, enter the corresponding parameters.
4. Enter a name and click **Save**. Other necessary settings for the device are specified during saving and the **Device group** tab is activated.
5. On the **Device group** tab in the **Booking instructions** selection field, select the booking instruction **32 Access ident code** and save the change.
6. In the menu tree, click **Load/display terminal** and click the new terminal.
7. In the **Load data** dialog, activate the **All configuration data** checkbox and click **Transfer data** to load the terminal.

III. Create door

1. In the menu bar, click **Access**. In the menu tree click **Door administration** and then on **Doors**.

Note: Depending on the options activated, this menu item may also be displayed as area/door administration or room zone/door administration.

2. In the tree structure, click the node to which you wish to allocate the new door.
3. Click **Create new record** in the toolbar, then **Door** in the selection dialog to create a new door.
4. Complete the input fields and assign the previously created reader to the door.
5. In the toolbar, click **Save** to save the door.

IV. Assign access permissions

1. In the menu tree, click **Person administration** and **Access profiles**.
2. In the **Selection Access profiles** dialog, click the access profile to which you want to assign permissions, or click **Create new record** in the toolbar if you want to create a new access profile.
3. Make the assignment for the new door/new reader and click **Save**.
4. If you created a new access profile, you must assign it to the required persons as a permission or special permission.

Note: Alternatively, you can directly assign the access permissions for the door/reader to the persons as a special permission.

5. You can assign another ID card number to the person as well, if the system option **Several ID cards** is active.
6. Then the ID card number is used as a personal identification code. Accordingly, the ID card number must be entered with the keypad during the booking. Input is confirmed and ended by pressing the **#** button, e.g. on DP1 readers, or the **E** button, e.g. on 91 xx-series readers.

3.1.4 ▶ Set up access control for two persons

When using the "Access control for two persons" function, the door is only released if two authorised persons present their ID cards to the reader or readers within a predefined time frame.

This is generally to ensure that at least two persons always enter the room.

The function can be implemented with the aid of one or two access readers at the entrance to a security area. The configuration with two readers is the most secure. In this case, the readers are arranged so that it is impossible for one person to present two ID cards to the two readers within a predefined time span.

I. Set up terminal

1. Switch to the **Devices** main menu.
2. In the menu tree, click **Devices** and then click the **Server** node in the device tree.
3. Click **Create new record** in the toolbar.
4. In the device selection click the terminal you want to use.
5. Enter all required details for the terminal and click **Save** in the toolbar to save the terminal.

II. 1. Set up readers

1. Stay on the newly created terminal and in the toolbar click **Create new record**.
2. In the device selection click the reader you want to use.
3. Enter the general information for the reader.
4. Switch to the **Reader function** tab and enter the time frame in which booking must be carried out.
5. Go to the **Device group** and enter the variable booking instruction **35 Access SecondSetOfEyes**.
6. Save the reader.

III. 2. Set up readers

1. Stay on the newly created terminal and in the toolbar click **Create new record**.
2. In the device selection click the reader you want to use.
3. Enter the general information for the reader.
4. Switch to the **Reader function** and enter the same detail as for the first reader.
5. Go to the **Device group** and enter the variable booking instruction **35 Access SecondSetOfEyes**.
6. Enter the first reader in the terminal function unit 2.
7. Save the reader.
8. In the device tree, click the first reader which you created in step II and go to the **Device group** tab.
9. Enter the second reader in the terminal function unit 2 and save the entry.

IV. Create room zones and doors

1. Create the room zones for the access control for two persons.
2. Under the new room zone, create the door for the access control for two persons.

V. Allocate permissions

The access permissions for the reader can be allocated via all known access permissions.

3.1.5 ▶ Set up office release

In addition to access control, dormakaba MATRIX also provides an office release option. During the office release periods, persons with access permission can activate the office release by means of bookings. When office release is activated, no access bookings are required at the door. Office release ends on departure from the room with a booking, or automatically at the end of an office release period.

Note: The office release function is supported by all doors that are connected to evolo or XS components (wireless or standalone) or a reader on a TP4 terminal.

To set up office release for a door, proceed as follows:

I. Set up variable booking instructions for online components

If you wish to set up office release for a door with an offline component, you do not need to make any changes to the reader in the **Devices** main menu.

If the door is set up with a reader that is connected with a TP4 terminal online, the variable booking instruction for the reader must be changed, so that the two bookings performed within a short time interval are evaluated as office release bookings.

1. Select **Devices** in the **Devices** main menu.
2. In the device tree, click the reader connected to the door for which you wish to set up office release.
3. Switch to the **Reader function** tab and select the door relay that opens the door, unless a relay has already been entered.
4. Go to the **Device group** tab and enter the variable booking instruction **5 Access with office release**.
5. In the toolbar, click **Save** to save the changes.

II. Set up door daily times

The time intervals for the office release are defined in the door daily times that are allocated to the door via the door weekly profile.

1. Go to the **Access** main menu and select **Area/door administration**.

Note: Depending on the options activated, this menu item may be displayed as area/door administration or room zone/door administration.

2. Then click the **Door daily times** menu item.
3. Click the door daily times you would like to define office release intervals for in the Selection dialog.
4. Enter the office release time intervals in the **Office release allowed** row on the **General** tab. Up to four time intervals can be defined.

Note: The maximum office release duration can be individually restricted for each entered time interval on the **Extended time ranges** tab.

5. In the toolbar, click **Save** to save the changes.

III. Assign permission for office release

Permission for office release is assigned directly to the person. If you have activated ID card administration level 3, permission is assigned for the ID cards.

1. In the menu tree, click **Person administration** and then **Persons**.
2. In the selection dialog, click the person to whom you wish to assign permission for office release.
3. On the **Permissions** tab, use the **Office release** selection field to select whether you wish to grant office release for all doors or just a selection of doors.

Note: If you select **all doors**, office release can be activated for all doors for which the person has access permission.

In the **Selection** option, a table appears from which you must select the doors for which office release is to be allowed and for which the person has access permission.

4. Table of doors for office release.
In this table, you can individually authorise for office release all doors connected with an offline component and for which access permission exists.
Doors that have a reader with an online connection to a TP4 terminal are grouped under the **All online doors** option and can only be authorised together. Permission cannot be granted for individual online doors.
5. When you have granted permission for office release for all the desired doors, click **Save** in the toolbar.

3.1.6 ▶ Work with visitor administration

Visitor administration offers a series of dialogs for maintaining visitor data and maintaining and managing individual visits.

The data of every visitor is recorded and managed in a separate record. When planning a visit, these visitor records are transferred to a visitor reservation along with the date and time of the visit. The visitor reservations are provided to reception on the day of the visit. The receptionist must activate the visit as soon as the visitor arrives.

Only certain users can access visitors via Self Service. If the user role does not have the "Show all visitors" permission, permission can be controlled for individual users via the organisational structure. If a user has neither of these permissions, they can only use self service to view the visitors that have been created for them or that they have created themselves.

Information on using QR code ID cards can be found under ▶ [Set up visitor administration with QR codes](#).

Visitor administration is a component of the Mobile Access functions in MATRIX. This means that visitors can also be granted access via their smartphone (for more information, see ▶ [Set up Mobile Access](#)).

The following steps must be performed to manage visitors:

I. Create visitors

The person-related data of all visitors is only recorded once and can then be used for repeat visits from the same visitor. Visitors can be created at any time, even before a definite visit has been planned.

1. Click **Access** in the menu bar and open **Visitor administration** in the menu tree.
2. Click the **Visitors** menu item to open the **Selection Visitor** dialog.
3. In the toolbar, click **Create new record** to create a new visitor, or click an existing record to edit the record.
4. Enter the visitor's data. Enter the Mobile Access device number if the visitor is to be granted access via smartphone.

Note: The Mobile Access device number is a mandatory field if using Mobile Access and ID card administration level 1.

5. Click **Save** in the toolbar to save the visitor.

II. Create visit appointments via visitor reservations

Visitor reservations are used to schedule visitor appointments.

1. Click **Access** in the menu bar and then on **Self Service**.
2. Click **Visitor reservations** in the menu to open the **Selection Visitor reservation** dialog.
3. Click **Create new record** in the toolbar to create a new visitor reservation or click an existing record to edit it. Alternatively, click the **Create new record** symbol in the table to create a copy of the appropriate visitor reservation.
4. Select a visitor from the list.

Note: Enter their name if the visitor has not yet been created in the system. A visitor record is automatically created after saving the visitor reservation. It is vital to check the existing entries in the **Visitors** selection report to prevent undesired duplicate records being generated.

5. Enter the data for the visit such as date, time and purpose of the visit.
6. To save the visitor reservation, click **Save** in the toolbar.
7. To log in a visitor for multiple visits, click the **New advance reservation for this visitor** button. Change the date and any other details and then click **Save** again.

III. Activate, interrupt and end visits

Visits are usually handled by reception staff within the company.

The **Visitor overview** dialog displays all visits for the current day. Every visit is activated on the visitors' arrival and ended after completion using the action buttons. Active visits can be interrupted, e.g. if the visitor leaves the building during a lunch break.

Note: Mobile Access: When a visit is activated, the ID card number is suggested from the range of virtual ID card numbers. You can change the number manually. The visit is authorised using an access profile.

Proceed as follows to activate a visit:

1. Click **Access** in the menu bar and open **Visitor administration** in the menu tree.
2. Click the **Overview of visits** menu item.
3. When a visitor arrives, click the **Activate** action button. The **Edit visit** dialog will open.
4. Select a free visitor ID card from the **ID card** selection. An ID card number is automatically suggested when using Mobile Access.
5. You must also select an access profile when using Mobile Access.
6. Click **Save**. The visit is displayed with the status "Active"(green) in the **Overview of visits** dialog.

Proceed as follows to interrupt and restart a visit:

1. Click the **Interrupt** action button. The visit is displayed with the status "Interrupted" (yellow).
2. To continue the visit, click the **Activate** button again.

Note: If the visitor ID card is no longer available, you can issue a new ID card. Click the interrupted visit and enter the new ID card number in the **Edit visit** dialog.

Proceed as follows to end a visit:

1. Click the **End** action button. The visit is displayed with the status "Ended" (grey).

Note: A visit that has been ended cannot be restarted.

Setting up Mobile Access for visitors

The **dormakaba mobile access** app must be installed for access using a smartphone. This app is available from the AppStore.

A Mobile Access device number must be saved for a visitor to allow you to enable the user for Mobile Access.

Proceed as follows to store a Mobile Access device number for a visitor:

1. Switch to the main **Access** menu and click **Visitor administration** in the menu tree.
2. Click **Visitor** and enter the telephone number of the smartphone in the **Mobile Access device number** input field in the **Edit visitor** dialog. The Mobile Access number requires the prefix "phone#", e.g. "phone#+4917256889755".

As soon as an e-mail address and a Mobile Access device number have been saved in the record, the visitor receives an e-mail notification prompting them to download the **dormakaba mobile access** app from the App Store. E-mail dispatch must be configured for automatic notifications to work.

Notes on ID card administration level 1

Setup: As each person can only be allocated one ID card in ID card administration level 1, booking using RFID ID cards is no longer possible for the person in question once Mobile Access is set up. In this case, it is mandatory for all visitors to enter a Mobile Access device number.

Notes on ID card administration level 2

As multiple ID cards can be allocated to each person in ID card administration level 2, Mobile Access can be used in addition to booking via one or more RFID ID cards. Visitors cannot combine access via smartphone and via an RFID ID card. If a visitor is to be allowed to use both options, a second visitor record must be created.

Notes on ID card administration level 3

As multiple ID cards can be allocated to each person in ID card administration level 3, Mobile Access can be used in addition to booking via one or more RFID ID cards.

A virtual ID card with the ID card type "Mobile Access" must be created and given the appropriate permissions in ID card administration in order to use Mobile Access. The Mobile Access device number is assigned to the visitor's ID card when the visit is activated.

3.1.7 ▶ Set up visitor administration with QR codes

QR codes can be sent to a visitor by e-mail in advance of their visit:

- To simplify registration at the reception/gate (QR code without access function) or
- To grant access at a few safety-relevant access-control points, such as the entrance to the visitor car park (QR code with access function)

Note: As QR codes are sent via e-mail, an e-mail server must be configured in the system and an e-mail address saved for the visitor in question.

General information on creating visitors and visits can be found under ▶ [Work with visitor administration](#).

Using QR codes for simplified registration with access function

Note: The system parameter Access 73 "With QR code" must have the value "1" to enable this function to be used.

Perform the following steps to use QR codes for simplified registration:

I. Assign an access profile and send the QR code

Access profiles with QR code activation are allocated in Visitor reservations and the QR code is sent to the visitor.

1. Click **Access** in the menu bar and then **Self Service**.
2. Click the **Visitor reservation** menu item.
3. Open the appropriate visitor reservation or create a new one.
4. Choose the appropriate access profile from the **QR access profile** selection list.
5. Save the visitor reservation. After saving, an e-mail containing a generic QR code is sent to the stated e-mail address and the visit is shown with the status "Pre-activated".

Note: E-mail template 13 "Visitor access with QR code" is used.

If an arriving visitor registers at the gate using the QR code that they received, the associated visitor reservation is opened directly in the **Visitor overview** dialog and the visit can be activated.

Using QR codes with access function

Note: The system parameter Access 73 "With QR code" must have the value "2" to enable this function to be used.

For reasons of security, this function should only be set up for access at a few safety-relevant access control points, such as the visitor car park entrance. Once the visit has been activated at reception/the gate, the visitor receives a regular access ID card.

Note: As soon as a visit is activated in the **Visits overview** dialog, the QR code ID card is replaced with the new ID card.

Perform the following steps to use QR codes with access functions.

I. Creating a QR code reader

Wiegand readers are used as QR code readers.

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. Click a 92 30 AM controller in the device tree and create a new Wiegand reader.
3. Select the ID card type "QR code" from the **General reader info** tab.
4. Save the QR code reader.

II. Setting up access profiles

Activation using QR codes must be enabled in the access profile.

1. In the menu bar, click **Access** and open **Person administration** in the menu tree.
2. Click the **Access profiles** menu point.
3. Open the appropriate access profile or create a new one.
4. Activate the **Relevant for pre-activation with QR code** checkbox.
5. Save the access profile.

III. Assign an access profile and send the QR code

Access profiles with QR code activation are allocated in Visitor reservations and the QR code is sent to the visitor.

1. Click **Access** in the menu bar and then **Self Service**.
2. Click the **Visitor reservation** menu item.
3. Open the appropriate visitor reservation or create a new one.
4. Choose the appropriate access profile from the **QR access profile** selection list.
5. Save the visitor reservation. After saving, an e-mail containing a generic QR code is sent to the stated e-mail address and the visit is shown with the status "Pre-activated".

Note: E-mail template 13 "Visitor access with QR code" is used.

Note: The period during which the QR code is valid before the visit appointment actually begins is determined using the system parameter Access 74 "QR code validity period before visit".

3.1.8 ▶ Set up a keyboard reader for duress alarm

When the PIN code input is activated, the input of a duress PIN code can be activated in addition. A silent duress alarm is triggered during the input and the door opening is acknowledged positive. The duress PIN code is the PIN code stored in the employee master record with the last position incremented or decremented by 1 whereby 0 becomes 9 and 9 becomes 0.

Note: You need a keypad reader to enter the PIN code. Only a reader with defined characteristics such as door release pulse length and the outputs to be controlled can be connected to a door and the duress alarm.

You need to perform the following steps to set up the input of a duress PIN code with duress alarm:

I. Create terminal

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, click the **Server** node and then **Create new record** in the toolbar.
3. In the device selection, click the terminal to which the keypad or keypad reader is connected.
4. In the **Devices** dialog, enter a name and complete the required fields.
5. In the toolbar, click **Save** to save the terminal.

II. Create keypad reader

1. Click **Create new record** in the toolbar of the **Devices** dialog.
2. In the device selection click the desired keypad reader.
3. Enter a name and select the corresponding parameters in the **General reader**
4. In the **Device group** tab in the **Booking instructions** selection field, select the booking instruction **33 Access threat code** and save the change.
5. In the menu tree, click **Load/display terminal** and click the new terminal.
6. In the **Load data** dialog, activate the **All configuration data** checkbox and click **Transfer data** to load the terminal.

III. Create door

1. In the menu bar, click **Access**. In the menu tree click **Door administration** and then on **Doors**.

Note: Depending on the options activated, this menu item may be displayed as area/door administration or room zone/door administration.

2. In the tree structure, click the node to which you wish to allocate the new door.
3. Click **Create new record** in the toolbar, then **Door** in the selection dialog to create a new door.
4. Complete the input fields and assign the previously created reader to the door.
5. In the toolbar, click **Save** to save the door.

IV. Assign access permissions

1. In the menu tree, click **Person administration** and **Access profiles**.
2. In the **Selection Access profiles** dialog, click the access profile to which you want to assign permissions, or click **Create new record** in the toolbar if you want to create a new access profile.
3. Make the assignment for the new door/new reader and click **Save**.
4. If you created a new access profile, you must assign it to the required persons as a permission or special permission.

Note: Alternatively, you can directly assign the access permissions for the door/reader to the persons as a special permission.

5. Enter the desired PIN code for the persons.
Before entering the duress PIN code, the person needs to book with a valid ID card allocated to them.

Note: Do not enter the duress PIN code for the person because it is calculated from the PIN code.

3.1.9 ▶ Work with AccessOnCard AoC (for XS/evolo components)

The AccessOnCard (AoC) option dormakaba MATRIX offers you the ability to save access permissions on an ID card and to use this information when performing a booking at an AoC reader.

Note: The AoC option is only available with the corresponding license. If the AoC option has not been activated, the following steps cannot be carried out.

As a basic prerequisite for AoC, you will need the appropriate ID cards, an AoC station and one or more AoC readers.

AoC ID cards are ID cards on which AoC data is written on the AoC stations during the loading process. The AoC data on the ID card is read when booking at the AoC readers and is used to evaluate access permissions.

An AoC station is a computer on which the AoC manager software is installed and to which a PC reader is connected that can read and write to the AoC ID cards. Alternatively, an AoC station can be a TP4 terminal with a suitable reader that is configured as an AoC writer.

Note: You find the appropriate AoC Manager software for the AoC station on the dormakaba MATRIX installation CD.

Install the software by starting the file "Desktop_Reader_Manager_windows_setup_x_x_x" (where x_x represents the version number).

Any component identified in the device definition as an AoC reader can be used as an AoC reader.

For security reasons, the AoC data on the ID card is generally valid for one day only. If the ID card is locked, it is already invalid on the day after the data was loaded.

An AoC ID card does not offer much space for access data. For this reason, the various time frames for access from all access daily times needed for one person are combined into a blanket interval. Exceptions to this rule are possible using the special identification "AoC special interval".

Note: When planning the access daily times, you should bear in mind that these programs are combined into a blanket interval in AoC. Special intervals require a great deal of space on the ID card. As the number of special intervals grows, the time required for writing and reading AoC ID cards increases significantly. Therefore, it is recommended to keep the number of special intervals per ID card to a minimum.

Perform the following steps to set up the system for AoC:

I. Activate the AoC option in the system parameters

1. In the menu bar, click **System**. In the menu tree, click **Administration** and then on **System parameters**.
2. Open system parameter **30 AoC function** under the **Access** node and enter the value 1 to enable AoC functions.
3. Next, click **Save** and log in to MATRIX again.

Ila. Create an AoC station based on the Desktop Reader Manager

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, select the main node **Server** and in the toolbar click **Create new record**.
3. Select the device type "AccessOnCard station".
4. Enter the appropriate data in the device configuration dialog.
5. Enter a name and click **Save** to save the device.
6. In the menu tree, click **Load/display terminal** and click the new AoC station.
7. Click the **Transfer data** button to load the AoC station.

Note: The AoC station must be active to load the data to the station properly.

IIb. Create an AoC station with a TP4 terminal

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, select the main node **Server** and in the toolbar click **Create new record**.
3. In the device selection, click a TP4 terminal such as, for example, an L6L or M6L.
4. Enter a relevant name and number for the terminal.
5. Select the class "TP4 LAN AoC" from the **Terminal class** selection field on the **General** tab.

Note: Class TP4-LAN-AoC is designed for terminals with additional memory. If a terminal without additional memory is used, the number of persons and the number of AoC readers must be reduced to 500 at any one time.

6. Switch to the **General reader** tab and activate the **AoC writer** checkbox.
7. Switch to the **Device group** tab and select the command "34 AoC load data" from the **Variable booking instruction** field.
8. Save your input.
9. In the menu tree, click **Load/display terminal** and click the new terminal.
10. Click the **Transfer data** button to load the terminal.

III. Assign booking permissions for an AoC station

Assigning booking permissions for an AoC station is no different to the general procedure for assigning access permissions, apart from the fact that no door needs to be created for an AoC station.

How to assign the booking permissions for an AoC station in an access profile:

1. In the menu tree, click **Person administration** and then on **Access profiles**.
2. In the selection dialog, click the access profile to which you wish to add the booking permission.
3. Allocate the required AoC station to the access profile and then click **Save**.

How to assign the booking permission directly to a person:

1. Click **Persons** in **Person administration**.
2. In the selection dialog, click the person to whom you wish to allocate the booking permission on an AoC station and then open the **Permissions** tab in the **Edit Persons** dialog.
3. Add the AoC station to the special permissions for **Doors/readers** and click **Save**.

IV. Create an AoC reader

1. In the menu tree, click **Devices**.
2. In the device tree, select the node under which you want to create the AoC reader and click **Create new record** in the toolbar.
3. Click an offline component in the device selection.
4. Complete the appropriate fields in the dialog for the component and activate the **AoC reader** checkbox.
5. Enter a description and click **Save** to save the entries.

Note: Triggered by the new component, the system indicates in the info centre that XS/evolo components still need to be synchronised with the XS Manager. However, synchronisation is not necessary at this point, because more settings still need to be transferred to the AoC Reader.

V. Allocate access permissions

The allocation of access permissions for AoC Readers does not differ from that for other readers. Before you allocate access permission for the new component, you must assign it to a door.

1. In the menu bar, click **Access**, followed by **Door administration** in the menu tree and then on **Doors**.

Note: Depending on the options activated, this menu item may be displayed as area/door administration or room zone/door administration.

2. In the tree structure, click the node to which you wish to allocate the new door.
3. Click **Create new record** in the toolbar, then **Door** in the selection dialog and set up the new door.

Note: If you activate the **AoC Special interval** checkbox, this door is not included in the calculation of the blanket interval but saved with the access ranges as a special interval on the ID card.

Special intervals correspond exactly to the access intervals from the access daily times applied to the ID card through its access permissions.

The blanket interval is used for permissions if the checkbox is not activated. The blanket access range is determined by taking the earliest start point from all access intervals of the access daily times as the start point and accordingly the latest end point from all access intervals of the access daily times as the end point. The calculation is made individually for each ID card based on the assigned access permissions. Please note that more space is needed to save special intervals on the ID card.

Note: The control for special intervals can also be saved in the room zone if necessary if the door is assigned to a room zone.

4. After the new component has been assigned to a door, you can allocate the access permissions for the door.
The access permission can be assigned via access profiles or directly to the person as a special permission.
5. To allocate the permission to an access profile, click **Person administration** in the menu tree and click **Access profiles**.
6. In the selection dialog, click the required **Access profile** to which you wish to assign the new component.
7. Allocate the AoC reader to the access profile and then click **Save**.
8. Click **Persons** in **Person administration**.
9. Click the person whose AoC settings and permissions you wish to edit.
10. If you wish to assign the access permission for the AoC reader to the person as a special permission, open the **Permissions** tab and enter the AoC reader in the special permissions for **Doors/readers**.
11. To edit the AoC settings, open the **AoC** tab.
12. In the **AoC validity** field, enter the number of validity days for the AoC permissions on the ID card. Usually this is 1 day.
In the table, you can check for each day which permissions have been written on the ID card. Without any special interval assigned to the person, the table is empty and only displays the blanket interval.
13. Click **Save** in the toolbar to save the entries.

Note: After all AoC entries have been made, you must synchronise the AoC components with the evolo Programmer and the XS Manager.

3.1.10 ▶ Create a lift control

In addition to access control, dormakaba MATRIX provides the possibility to allocate and manage access permissions for a lift with individual floors.

You use room zones to assign access permissions to the floors because each floor is represented by a room zone. You can specify the allocation of the floors to the room zones in the **Edit Lift** dialog.

To set a lift control you need:

- A TP4 terminal of type B6L 19" or B6L-WM which detects the access permissions for the elevator and the floors.
- One or more output modules depending on the floors for permissions.
- A reader located in the lift. The bookings for using the lift are carried out at this reader.

Note: To perform the following steps you need the rights for creating devices and for the access menu.

To set up the system for lift control, you must carry out the following steps:

I. Create a terminal for floor release

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, select the main node **Server** and in the toolbar click **Create new record**.
3. In the device selection, click on the B6L 19" or the B6L-WM to transfer the device to the dialog for editing.
4. Change the number of the device and enter a description of the device and an IP address or a host name.
5. Select **Inputs/Outputs** and in the **Number of relays for lift** field enter the number of floors to be managed.
6. In the **Lift output devices** selection field, select the terminal outputs and the output modules connected to the lift control. The following rule applies:

You can use the internal terminal outputs and the output modules (input/output modules).

Output modules must be located at the first possible address in the respective bus.

For DCS output modules, this is the DCW address 0.

For DP1 output modules, this could be the address 17 or 25 in the DP1 bus, depending on the device.

The following table displays details regarding module selection.

Value	Bus	Module	Max. no. of modules	Total number of relays depending on the number of the local relays (+free relay)		
				2	5	8
0		Local relays		2	5	8
1	DCW	4 x I/O modules from DCW module address 68 (DIP switch 0)	4	16	16	16
2		Local relays + 4 x I/O modules from DCW module address 68 (DIP switch 0)	4	18	21	24
3		15 x O modules from DCW module address 84 (DIP switch 0)	4	60	60	60
4		Local relays + 15 x O modules from DCW module address 84 (DIP switch 0)	4	62	64 (+1)	64 (+4)
5		Door modules from DCW module address 76 (DIP switch 0)	4	8	8	8
6		Local relays + door modules from DCW module address 76 (DIP switch 0)	4	10	13	16
7	DP1	4 x I/O modules from DP1 address 17	15	60	60	60
8		Local relays + 4 x I/O modules from DP1 address 17	15	62	64 (+1)	64 (+4)
9		15 x O modules from DP1 address 17	5	64 (+11)	64 (+11)	64 (+11)
10		Local relays + 15 x O modules from DP1 address 17	5 or 4	64 (+13)	64 (+1)	64 (+4)
11		Door modules from DP1 address 17	15	30	30	30
12		Local relays + door modules from DP1 address 17	15	32	35	38
13		4 x I/O modules from DP1 address 25	7	28	28	28
14		Local relays + 4 x I/O modules from DP1 address 25	7	30	33	36
15		15 x O modules from DP1 address 25	5	64 (+11)	64 (+11)	64 (+11)
16		Local relays + 15 x O modules from DP1 address 25	5 or 4	64 (+13)	64 (+1)	64 (+4)
17		Door modules from DP1 address 25	7	14	14	14
18		Local relays + door modules from DP1 address 25	7	16	19	22

Selection example:

You use only the DCW 15x output module, then select 3.

You can connect a total of four modules.

You use the internal outputs on the terminal and DP1 4x input/output modules, then select 8.

You can connect a total of 15 DP1 4x input/output modules.

7. Click **Save** in the toolbar to save the entries.

II. Create output modules

1. In the **Devices** dialog for the newly created terminal, click **Create new record** in the toolbar.
2. In the device selection, click the output module type that you want to use for the lift control.
3. In the dialog for the device, complete the corresponding fields.
4. Click **Save** in the toolbar to save the entries.
5. If required, repeat steps 1 to 4 until all output modules are created.

Note: You can only use output or input/output modules of the same type. It is not possible to mix 15-way output modules with 4-way input/output modules, for example.

III. Create lift readers

1. In the **Devices** dialog for the newly created terminal, click **Create new record** in the toolbar.
2. In the device selection, click the required reader to transfer it to the dialog for editing.
3. In the **General** tab, enter the corresponding parameters.
4. Enter a name and click **Save**. Other necessary settings for the device are specified during saving and the **Device group** tab is activated.
5. On the **Device group** tab in the **Booking instructions** selection field select the booking instruction **21 Access Elevator** and save the change.
6. In the menu tree, click **Load/display terminal** and in the selection click the new terminal to open the **Load data** dialog.
7. Click the **Transfer data** button to load the terminal.

IV. Generate room zones for access-controlled floors and set up lift door

You need a room zone for each floor to which you want to give access permission.

1. In the menu bar, click **Access**. In the menu tree, click **Area/door administration** and then **Room zones/doors**.

Note: Depending on the options activated, this menu item may also be displayed as "Area/door administration".

2. Click the node in the tree structure to which you wish to allocate the new room zone.
3. Click **Create new record** in the toolbar, then **Door** in the selection dialog and set up the new door.
4. Complete the input fields and assign the reader to the lift door.
5. Go to the tree structure and click the node to which you wish to allocate the new room zone. This should be the same node as under IV.2.
6. Click **Create new record** in the toolbar, then on **Room zone** in the selection dialog and set up the new room zone.
7. In the toolbar, click **Save** to save the room zone.
8. Repeat steps 5 to 7 until you have created all room zones for the floors.

V. Create lift

1. In the menu tree, click **Additional functions** and then on **Lifts**.
2. In the toolbar, click **Create new record** to create a new lift.
3. Enter a description and a short description for the lift.
4. Select the terminal that is to manage the lift control.
5. Select the reader for the lift control and select the number of floors.
6. To each floor in the table, assign the corresponding room zone. Floors that cannot be accessed with the lift or that are always accessible do not require a room zone.
7. Click **Save** in the toolbar to save the entries.

VI. Assign access permissions for the lift

1. In the menu tree, click **Person administration** and then on **Access profiles**.
2. In the selection dialog, click the access profile that you want to assign permissions to or click **Create new record** in the toolbar, if you want to create a new access profile.
3. Make the assignment for the new reader in the lift and the required room zones (floors) and click **Save**.

Note: You can assign the access permissions directly to the persons, of course. Be sure though to remember the access right for the reader in the lift. Without access rights at this reader a person cannot make a booking in the lift and activate the floor selection based on the access rights granted.

4. If you created a new access profile you must assign it to the required persons as a permission or special permission.

3.1.11 ▶ Set up an IDS connection

Intruder detection systems (IDS) block access at times of day during which no employees are present in an area.

dormakaba MATRIX allows an intruder detection system to be easily connected to a TP4 controller via inputs and outputs.

The IDS is armed and disarmed by a TP4 access reader. evolo wireless components can also be actuated.

If you want to prevent the monitored area from being accessed after it has been armed, you can disable the readers allocated to the terminal that controls the IDS connection.

Note: You must create a reader with the number 16 if you use a B6L-RR-15 for the IDS connection. This reader will be automatically configured as activation reader for the IDS connection. The following inputs and outputs for the B6L-RR-15 are permanently set as defaults for the IDS connection:

Internal input 2: Condition of the IDS armed/disarmed

Internal input 3: IDS readiness to be armed

Internal output 2: Arm/disarm IDS

The internal input 2 is evaluated for deactivating readers.

Simple IDS connection

Perform the following steps to set up a simple connection to an intruder detection system:

I. Create terminal

1. Select **Devices** in the menu and click the **Server** node in the device tree.
2. Click **Create new record** in the toolbar.
3. Click a device type of the B6L family in the device selection.
4. Enter a description and select a B6L class on the **General** tab in the **Terminal class** selection field.
5. Fill in all other mandatory fields and in the toolbar click **Save** to save the terminal.

II. Create activation reader

1. Click **Create new record** on the toolbar in the **Devices** dialog.
2. In the device selection click the desired reader. If you use a B6L-RR-15, this must be the reader featuring the physical address 16.
3. Enter a description and fill in all mandatory fields in the **General** tab. Click **Save**.

III. Create additional readers

If you want to set up an IDS connection with reader shutdown, you must create the corresponding readers at the terminal which you have created beforehand, because reader activation and inactivation can only be controlled by the terminal for the IDS connection.

1. Click **Create new record** on the toolbar in the **Devices** dialog.
2. In the device selection click the desired reader.
3. Enter a description and fill in all mandatory fields in the **General** tab. Click **Save**.
4. Repeat steps 1 to 3 until you have created all readers.

IV. Load data

1. In the menu tree, click **Load/display terminal** and click the new terminal to open the **Load data** dialog.
2. Click the **Transfer data** button to load the terminal.

V. Create door for reader

1. Go to the **Access** main menu. In the menu tree click **Door administration** and then **Doors**.

Note: Depending on the options activated, this menu item may be displayed as area/door administration or room zone/door administration.

2. In the tree structure, click the node to which you wish to allocate the new door.
3. Next, click **Create new record** in the toolbar, followed by **Door** in the selection dialog to create a new door.
4. Complete the input fields and assign the reader for the IDS connection.
5. In the toolbar, click **Save** to save the door.

VI. Set up the IDS connection

1. In the menu tree, click **Additional functions** and then on **Intruder detection systems**.
2. Click **Create new record** in the toolbar.
3. Select **IDS Standard** in the selection dialog if you do not prefer reader shut down or **IDS for reader shut down**, if you want to inactivate the readers in the IDS area when the IDS is armed. The relevant **Edit Intruder detection system** dialog will open up.
4. Enter a number. It is recommended that you specify a name and short name.
5. From the selection select the terminal previously created for the IDS connection and then the previously created reader.
6. Use the other selection fields to select the inputs and outputs connected to the IDS according to the description.
7. If you have chosen an IDS connection with reader shut down, select the readers in the **Available readers** selection report and assign them by clicking the arrow.
8. Next, click **Save** in the toolbar to save the entries.

VII. Assign access permissions for the IDS reader

1. In the menu tree, click **Person administration** and then on **Access profiles**.
2. In the selection dialog, click the access profile that you want to assign permissions to or click **Create new record** in the toolbar, if you want to create a new access profile.
3. Add the reader with IDS connection and click **Save**.

Note: Of course, you can assign the access permission also directly to the persons.

4. If you have created a new access profile, you must assign it to the required persons as a permission or special permission.

3.1.12 ▶ Configure the counting information option

dormakaba MATRIX features a counting information option that allows you to monitor the number of persons present in a security area.

Note: The counting information option is only available in conjunction with the security areas option and with an appropriate licence. If the options are not activated, you cannot carry out the following steps.

As a basic requirement, you need an entrance and an exit reader for a security area, positioned on the security area's connecting door.

To set up the system for counting information, you must carry out the following steps:

I. Enable the security areas and counting information in the system parameters

1. In the menu bar, click **System**. In the menu tree, click **Administration** and then on **System parameters**.
2. Click the **Security areas** system parameter and enter the value 1 to activate the Security areas option.
3. Click the **Counting information** system parameter and enter the value 1 to activate the Counting information option.
4. Then click **Save**.
5. Log out of dormakaba MATRIX, then log in again.

II. Set up readers

Only online readers on a TP4 terminal can be used for counting information.

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. In the device tree, select the **Server** node under which you want to set up the terminal and the readers, and click **Create new record** in the toolbar.
3. In the device selection, click a TP4 terminal.
4. Fill in the fields for the terminal in the dialog and save your entries.
5. Click **Create new record** in the toolbar.
6. In the device selection click the desired reader.
7. Fill in the general fields for the reader and change to the **Device group** tab.
8. Enter the variable booking instruction **3 Access with ITK SA** and save the entries.
9. Repeat steps 5 to 8 for the second reader.
10. In the menu tree, click **Load/display terminal** and click the new terminal.
11. In the **Load data** dialog, activate the **All configuration data** checkbox and click **Transfer data** to load the terminal.

III. Set up booking types

For the counting functions to become effective, the access bookings of the relevant readers must be linked to the corresponding user programs and functions.

1. Click the **Administration** menu item in the **System** menu bar and then the **Application** menu item.
2. Click **Booking types**, then select the booking type **1 Successful access**.
3. For the user program, select **10001 Security area: counting information** and save the entries.
4. Click **Booking type allocations** in the menu, enter the **1 Successful access** booking type under **TP4 booking code 3** and save the input.
5. Click the **Class administration** menu item in the **Device administration** main menu followed by the menu item **Class settings**.
6. In the menu tree, click **Function assignments** and under **Access cancellation notification**, enter the user program **10002 Security area: cancellation notification**.
7. Save the entry.

IV. Set up counting groups and attendance recording

If counting groups are to be shown for a security area, attendance recording must be enabled for this security area and the relevant persons must be assigned to the counting groups. Only if attendance recording is enabled will the persons present in the security area be recorded. If attendance recording is disabled for a security area, counting is performed anonymously and only the number of persons present in the security area is recorded.

The counting groups are set up as follows:

1. In the **Access** main menu, click **Area/door administration**, then **Counting groups**.
2. Click **Create new record** in the toolbar.
3. Give the counting group an appropriate name and save the entry.

How to assign persons to a counting group:

1. In the menu tree, click **Person administration** and then **Persons**.
2. In the selection dialog, click the person whom you would like to assign to a counting group.
3. On the **Access** tab, select the desired group in the **Counting group** selection field and save your entry.

How to enable attendance recording for the security area:

1. Click **Area/door administration** and then **Security areas - doors**.
2. Click the security area for which you want to enable attendance recording.
3. On the **Counting information** tab, activate the **Attendance recording** checkbox and save the entry.

V. Monitor security areas

In the **Area monitoring/security areas** dialog, the number of persons present in the security area can be monitored and if necessary corrected or recalculated. A recalculation is always performed for the selected security area and for all enclosed security areas. Depending on the number of bookings and employees, the recalculation may take some time.

Note: To recalculate the counting values, you need the corresponding rights.

How to monitor a security area:

1. In the **Access** main menu, click **Area monitoring**.
2. Click the **Security areas** menu item to open the new window for monitoring the security areas.
3. In the tree structure, select the security area that you wish to monitor.

If attendance recording is not enabled for the security area, the number of persons present can be changed in this dialog.

If attendance recording is activated, the correction must be made by setting the person as present in the security area.

3.1.13 ▶ Work with video surveillance

You can integrate video cameras using the floor plan in Alarm management. The cameras are created in Device management and can then be positioned on a floor plan. Clicking a camera symbol in the Alarm monitor floor plan calls up the camera popup containing the camera's live stream. It can display multiple live streams simultaneously. The live stream is also displayed immediately if a door alarm has been triggered (e.g. forced entry).

In addition to these options in the Alarm monitor, the live stream can also be displayed via the Door status dialog.

PTZ-capable cameras can be remotely controlled, swivelled and zoomed (pan, tilt and zoom) within MATRIX.

The current versions of the following browsers support video surveillance functions in MATRIX:

- Microsoft Edge
- Google Chrome
- Mozilla Firefox

Internet Explorer version 11 does not provide full support.

3.1.13.1 Technical information on video surveillance

The following sections provide technical insight into video surveillance using MATRIX.

Architecture overview

The connection of video surveillance cameras involves two functions:

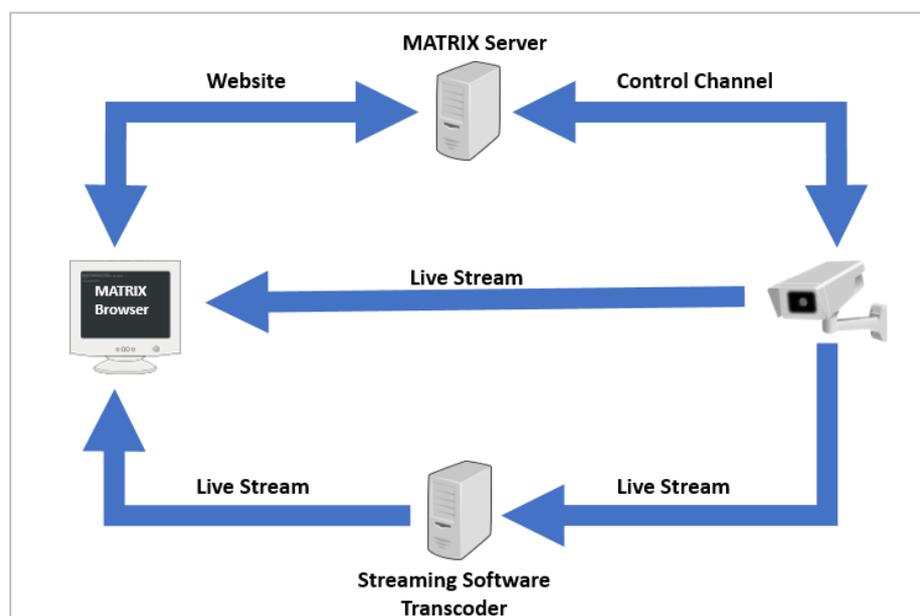
- Displaying the camera's live stream (possibly including audio).
- Optional PTZ control (pan, tilt and zoom) of the camera via a control channel.

All communication channels in which the MATRIX server or the MATRIX client (browser) participate can and must be encrypted using HTTPS. Please also read the documentation of the respective camera to see whether the camera also supports encryption.

There are basically two methods for feeding the live stream from a camera to the MATRIX client:

- Direct route from the camera to the MATRIX client (browser).
- Indirect route via streaming software.

The following illustration shows an overview of the architecture.



The live stream is never diverted via the MATRIX server. A live stream displayed in the MATRIX client either comes directly from the actual camera or from streaming software upstream from the camera. The MATRIX server only informs the MATRIX client of where and how the appropriate live stream can be accessed. This keeps the MATRIX system scalable and means that an increased number of network cameras has no negative impact on the MATRIX server.

Using streaming software can provide the following advantages:

- Relieves the load on the camera if multiple persons call up the live stream simultaneously. In cases such as these, the streaming software acts as a multiplier. Only the streaming software accesses the camera whilst providing the live stream to many clients.
- Conversion of the camera streaming protocol into a protocol that can be processed by the browser, conversion of RTSP/RTP into MPEG-DASH. This process is known as transcoding.
- Authentication for the camera.

Note: The MATRIX IP installation CD also contains streaming software called Camera Connector that supports authentication (see below). If you wish to use third-party streaming software, the customer is responsible for its installation and maintenance.

An outstanding feature of streaming software is the ability to transcode an RTSP/RTP stream from a camera into MPEG-DASH that MATRIX can display in the browser. Please note that transcoding causes lag, i.e. the image is displayed to the observer with a delay of a few seconds. The extent of this latency depends significantly on the streaming software in use or its configuration.

Optional PTZ camera control is performed by the MATRIX server via the control channel (see illustration). In contrast to live streams, the MATRIX server only sends small data packets to a camera for controlling the camera. This is performed via HTTP or HTTPS. The MATRIX server must usually authenticate itself to the camera in order to be able to control a camera. MATRIX transmits the login data (user name and password) required for authentication to the camera in a secure manner (in line with the ONVIF standard). This sensitive login data is not transmitted to the user's browser for reasons of security. This does not apply when commissioning a camera. During commissioning, the administrator must create the login data in MATRIX device management.

MATRIX IP Camera Connector additional component

The MATRIX IP Camera Connector is provided as a separate component on the MATRIX DVD (Windows Installer).

The MATRIX IP Camera Connector is streaming software that allows MATRIX to access password-protected images from cameras.

You will require administrators' rights to install it. During installation, you must define a port via which MATRIX can access the IP Camera Connector later on. MATRIX IP Camera Connector is installed as a Windows service that starts automatically. It requires no further configuration, such as which cameras are to be activated, and it does not save any passwords or other similar data.

MATRIX communicates directly with the IP Camera Connector and at the same time transfers the authentication data for the snapshots in line with HTTP Basic Authentication. The connector forwards the request to the camera and finally returns the result to MATRIX.

Different cameras can be activated via different IP camera connectors, for instance separate connectors can be used for each site or each building.

Streaming technologies for displaying live streams

If a camera, possibly connected via streaming software, is to be used exclusively to display a live stream, the camera or the streaming software must only provide a stream that MATRIX can process. Therefore, it is not necessary for the camera or streaming software to fulfil the ONVIF standard in order to display the live stream.

MATRIX only uses HTML standards to display live streams and does not require the client to install any additional software.

MATRIX supports the following three streaming technologies. All of these streaming technologies are based on the HTTP protocol. It is therefore not usually necessary to make any adjustments to firewalls. The streaming technology to be used is defined for each camera. Different cameras can use different streaming technologies.

The following streaming technologies are supported:

- JPEG snapshots:** Just about every network camera provides the option of requesting an up-to-date snapshot as a JPEG image. If the quantity of snapshots is high enough, the observer sees the images as a continuous film. The frequency with which snapshots are requested from cameras is defined separately for each camera in MATRIX.
 In principle, MATRIX permits up to 25 images per second if both the network to camera route and the camera itself respond quickly enough. However, the more frequently snapshots are requested, the higher the network load. Even more expensive and faster cameras can hardly return more than 5 or 10 JPEG snapshots per second. Please note that you may be able to positively affect the size and compression of JPEG snapshots, possibly using the configuration tool or the camera's web interface.
- Motion JPEG (MJPEG):** Many network cameras provide MJPEG streams via HTTP. The logic of MJPEG streams is, so to speak, the reverse of JPEG snapshot logic. MATRIX actively requests the images when using JPEG snapshots. In contrast, when using MJPEG streams, the cameras automatically deliver the images as a package. So, the camera determines how many images it delivers per second and how much load it places on the network. Please note that you can usually also positively influence MJPEG stream settings using the configuration tool or the camera's web interface.
- MPEG-DASH:** MPEG-DASH requires significantly less bandwidth than the two streaming technologies named above and also supports audio. MPEG-DASH is the standard choice for streaming (live) video via the Internet. However, network cameras do not support this type of streaming (at least not yet) and so streaming software (transcoder software) is required. When using streaming software, please pay attention to the level of latency it produces (delay before the observer receives the image).

Ensure live stream security

All transfer routed must be encrypted to ensure secure video surveillance. It is also crucial whether a live stream password is protected or not. Due to the fact that the live stream is transmitted directly from the camera or from the streaming software to the MATRIX client (browser), the MATRIX client must also authenticate itself to the camera or the streaming software using the correct user data. The following options can often be configured in the cameras or streaming software:

- The live stream is not password protected. Other protective mechanisms are used instead.
- The live stream is password protected. User name and password or other authentication data are stored in the URL as parameters, example:
<http://mycamera.example.com/stream?user=<user>&password=<password>>
- The live stream is password protected. User name and password are transferred in line with the HTTP Basic Authentication standard.

Password protection is possible or not possible depending on type of streaming technology. This is shown in the following table.

User data	JPEG stream	MJPEG stream possible	MPEG DASH stream possible
<none>	Yes	Yes	Yes
URL parameter	Yes	Yes	Yes
HTTP basic auth.	Yes, see following	No	No

User data	JPEG stream	MJPEG stream possible	MPEG DASH stream possible
	options 1 to 3		

Option 1: Password-protected JPEG snapshots directly from the camera

MATRIX supports HTTP basic authentication for JPEG snapshots. This requires the camera to support the cross-origin resource sharing standard (CORS) and be appropriately configured. Cameras of this kind can be used directly. To use a camera of this kind, you must only enter the user name and password for the snapshots in Device management.

The MATRIX client must authenticate itself to the camera using the login data. Therefore, the login data must be transferred to the MATRIX client. This means that the login data could theoretically be viewed in the browser by a third party. For this reason, we recommend creating a separate user in the camera that has a separate password, can only view the live stream and that has no further control over the camera. Save this user and password in MATRIX camera configuration for the selected streaming technology.

Option 2: Password-protected JPEG snapshots and using the MATRIX IP Camera Connector

The MATRIX IP Camera Connector allows password-protected access to the JPEG snapshots from a camera. This tool does not perform transcoding of any kind, which makes it fast and very simple. After installing the software on one or more computers (but not on the MATRIX server itself to prevent excessive load), you only need to adjust the camera's snapshot URL in Device management.

Option 3: Password-protected JPEG snapshots and deactivated CORS standard

Browsers follow the CORS standard to protect against malware. This standard is irrelevant to cameras. If you transmit the correct user name and associated password to the camera, you will usually receive the requested data.

You can deactivate compliance with the CORS standard in Google Chrome. This allows the login data to be transferred to the camera even if the camera does not support CORS. To do so, Chrome must be started with the following command line parameters:

```
chrome.exe --disable-web-security --user-data-dir="D:\temp\chrome"
```

(whereby any directory is entered as the `--user-data-dir` (empty at first). This entry must not point to the normal Chrome installation directory. Chrome then fills this directory with internal data.)

Important information

- An instance of Chrome started in this way warns the user that security may be compromised.
 - An instance of Chrome started in this way must only be used for accessing MATRIX and not for accessing any web pages.
 - The question of whether this function will be removed from Chrome at some time in the future is a decision to be made by Google, the browser manufacturer.
-

Option 4: No password protection and use of IP address filters

Almost all cameras feature an IP address filter. This means that a camera only issues the live stream if the requesting IP address is on a whitelist (or not on a blacklist). You can usually either configure multiple separate IP addresses or IP address ranges as follows:

- The live stream (e.g. MJPEG) is not password protected. The camera can of course be a native camera in an internal and protected network.
- The live stream is only transferred from the camera to known IP addresses.
- The MATRIX client has a corresponding IP address and so receives the live stream from the camera.
- All communication can optionally be secured via HTTPS so that the live stream can only be viewed by the actual recipients.

Option 5: Use third-party streaming software

In contrast to browser applications, streaming software provides the option of covering all protocols with all possible authentication procedures. This enables you to create the following configuration:

- The camera live stream is password protected.
- The streaming software receives the live stream from the camera and transcodes it as necessary. Both the camera and the streaming software can of course be native components in an internal and protected network.
- The streaming software delivers the live stream, transcoded as necessary.
- The streaming software can control access to the live stream using IP address filtering, URL parameters or HTTP basic authentication (including CORS) for JPEG snapshots.

PTZ camera control

Only cameras that support **ONVIF Profile S** can be PTZ-controlled from within MATRIX. ONVIF stands for Open Network Video Interface Forum, a collaboration between renowned companies for standardising the connection of video cameras (see www.onvif.org). The ONVIF protocol uses HTTP(S) as a transport protocol, which means that firewalls usually require no adjustment.

When commissioning a PTZ-capable camera, the camera data can be requested from the MATRIX Device management dialog using the ONVIF standard, which simplifies camera configuration.

3.1.13.2 ▶ Set up video surveillance

If you are working with video cameras and MATRIX video surveillance for the first time, please first read the [Technical information](#).

Further information on the individual functions can be found in the respective dialog descriptions. Click the Help button in the dialog.

The procedure for setting up video surveillance involves creating the cameras in Device management. The further procedure depends on whether video surveillance will be based on floor plans in the Alarm monitor or based on door monitoring.

Note 1: If you wish to use streaming software, install it first on a separate computer; if possible, not one that is used as a MATRIX server. For example, use the MATRIX IP Camera Connector included on the MATRIX DVD to access password-protected JPEG snapshots from a camera.

Note 2: Alarm management must be enabled in MATRIX to allow video surveillance to be used. Ensure that system parameter 230 (System) is activated.

I. Create video camera

Each video camera must be created as a device in the device tree.

1. Click **Devices** in the menu bar, then **Devices** in the menu tree.
2. Select the node where the camera is to be created, click **Create new record** and select the device type "Video camera".
3. Enter a name and the communication data in device configuration.
4. Enter the user name and password for accessing the camera.
5. Select the streaming technology and enter the URL or the path to the live stream. This can be a camera URL or a previously installed streaming software.

Note: additionally, when using a MATRIX IP camera connector, the snapshot URL must be prefixed to the address of the IP camera connector.

Example:

`http://myconnector.example.com:9000/snapshot/http://mycamera.example.com/snapshot.jpg`

In this example, "http://mycamera.example.com/snapshot.jpg" is the snapshot URL and

"http://myconnector.example.com:9000/snapshot" is the URL of the MATRIX IP camera connectors.

6. Further input is required when using JPEG snapshots.
7. Enter the camera control (PTZ) data if the camera supports this function.
8. Then click **Save**.
9. Click the **Show camera** button to test the configuration. The live image is displayed in the camera popup.

IIA. Set up video surveillance using floor plans

To do this, first position the video cameras in the floor plans. The camera images can then be displayed using the floor plans in the Alarm monitor.

I. I. Add video cameras to the floor plans

1. In the menu bar, click **System**. In the menu tree, click **Administration** and then on **Alarm administration**.
2. Click **Floor plans** and select the appropriate floor plan.
3. Select a video camera from the **Devices** window and drag it to the respective position in the floor plan with the mouse key held down.
4. Then click **Save**.
5. Click a camera in the floor plan to call up the live image in the camera popup.

II. Display camera images

1. In the menu bar, click **System** and select **Alarm monitor** from the menu tree.
 - If an alarm has occurred at a door with an installed camera, click the notification. The live image from the camera will be displayed in miniature in the Details window. Click a live image to open it in a camera popup.
 - If you wish to display live images from cameras and no alarm has been triggered, activate the **Keep details open** checkbox. The **Floor plans** window will be displayed. Click a camera in the selected floor plan. The camera popup containing the live image from the camera will be opened.

Information on data group rights

Data group rights can be allocated to floor plans depending on system configuration. Proceed as follows if you have selected an alarm whose path from the root plan to the alarm trigger contains a plan in which the data group permission is missing:

If the system parameter 171 is set to the value 0 (greyed out) in the data group display options, the corresponding plan is shown in the floor plan tree with a crossed-out eye icon. The node can be selected but no floor plan will be displayed (notification: "No floor plan available").

If system parameter 171 is set to the value 1 (hide), no floor plan tree and no floor plan will be displayed (notification: "No floor plan available").

IIB. Set up video surveillance using door cameras

Video cameras must be allocated to doors in Door administration. The camera images (live streams) are called up using the Door monitoring status display. If an alarm occurs on a door with an installed camera, a miniature live image from the camera is automatically displayed in the Alarm monitor. Click a live image to open it in a camera popup.

I. Assign doors

Multiple video cameras can be created for each door. A single video camera can also be assigned to multiple doors, e.g. if a video camera covers two doors.

1. In the menu bar, click **Access** and open **Area/door administration** in the menu tree.

Note: Depending on the options activated, this menu item may be displayed as Area/door administration, Room zone/door administration or Door administration.

2. Highlight the door that you wish to add to the video camera and click **Create new record**.
3. Click the video camera in the **Create new element** dialog.
4. All available video cameras will be displayed. Select the appropriate video camera and click **Save**.

Note: If multiple cameras are defined for a door, the camera type determines the order in which the cameras are displayed in the Details window of the Alarm monitor. They are sorted in the order: Identification, foreground, background. This means that a camera with the type "Identification" would be displayed first and the other below this one. If multiple cameras of the same type have been assigned to a door, the camera number is used as a further sorting criteria.

II. Display camera images

1. In the menu bar, click **Access** and open **Door monitoring** in the menu tree.
2. Open the status display. A camera symbol is displayed for doors on which video cameras are installed.
3. Click on the camera icon to open the current camera image in a popup dialog. If multiple cameras are assigned to a door, a separate popup dialog is opened for each camera.

As the live streams are opened in separate popup dialogs, you can monitor multiple cameras simultaneously by arranging the camera popups side by side

3.1.14 ▶ Monitor doors with manual image comparison

Manual image comparison enables the photo stored in dormakaba MATRIX for the respective ID card to be displayed on a MATRIX client, e.g. at the gate, during access bookings. The images from one or more video cameras assigned to the door can be displayed at the same time.

A delay time for automatic door opening can be set for door monitoring at the gate. Permissions for online bookings are granted using buttons.

The system is operated via the status display in MATRIX door monitoring. A separate popup dialog is opened for each door. A user can open any number of doors in parallel. One and the same door can be opened by different users at the same time.

The function can be limited to a single entrance or monitoring workstation via the user role.

Overview of options:

- Manual image comparison without a video camera with or without approval
- Manual image comparison with a video camera with or without approval

Set up manual image comparison

The basic requirements are that the system parameter must be enabled and the rights must be authorised for the appropriate user role. All doors to be monitored must be allocated in Door monitoring.

1. Open the **System parameters** dialog and set the parameter Access 120 "Manual image comparison" to 1. Save your input and log back in to MATRIX.
2. Open the **Edit user role** dialog for the relevant user role and activate the change rights under Access > Door selection > Status display > Manual image comparison.
3. If you wish to specify a delay for door opening with approval, open the **Manual image comparison** dialog, activate the **Automatically allow access after seconds** checkbox and enter a delay value in seconds.
4. If manual image comparison will be performed using a video camera, create a new video camera and allocate it to the door as described below.
5. Edit the door selection and assign the selection to be displayed in the status display.

Set up a video camera for manual image comparison

I. Set up the variable booking instruction on the terminal

The terminal to which the video camera is connected must be configured using the variable booking instruction "9 Access with Video."

1. Select the terminal to which the video camera is connected in the **Devices** dialog.
2. Ensure that "Access" or "Time and access" is selected in the **Allocation** field in the **General reader** tab.
3. Select "9 Access with Video" in the **Variable booking instruction** field in the **Device group** tab.

II. Set up the video camera

Each video camera must be created as a device in the device tree.

1. Select the node under which the camera is to be created in the **Devices** dialog and create a new video camera.
2. Enter the access data in device configuration.
3. Then click **Save**.

III. Assign the camera to the door

Each video camera must be linked to the door (reader) to which it is attached in dormakaba MATRIX.

1. In the menu bar, click on **Access** and select the door to which the camera is attached from **Room zone/door administration** or Area/door administration.
2. Click on **Create new record** and then click on the camera previously configured in the device tree.
3. Select the camera type **Identification** and click on **Save**.

4 Dialogs in the Access module

Use the **Access** module to completely configure access control.

In Person administration, you manage person data and the person-related access permissions such as access profiles, access weekly profiles and set up access programs.

In External company administration, you can maintain the data for external companies and their employees.

In Visitor administration, you manage your visitors and their visits; in Room administration you can coordinate the room reservations.

In ID card administration, you can maintain ID cards for employees, external company employees and visitors.

In Area/Door management, you can map your security areas, room zones and doors. Area/Door management also contains the dialogs for the doors and their time-related control unit, such as door daily times and door weekly profiles.

Note: Depending on the options activated, this menu item may also be displayed as Room zone/door administration or Door administration.

The calendar administration offers calendars, bank holidays and special days, allowing you to specify dependencies on the date in the various daily programs.

The locking plan administration offers special access control functions.

Additional functions of Access control relate to the interlock control, lifts and the connection of intruder detection systems.

The control functions include area monitoring and counting values as well as door monitoring, which allows you to monitor the status of doors centrally. Here you can also control a door remotely using simple commands.

You can show or change the attendance status of persons in the attendance display.

Use the **Person administration** menu to manage the persons and the required master data for the access permissions.

Use the **External company administration** menu to manage external companies and their employees.

Use the **Visitor administration** menu to manage your visitors and their visits.

Use the **ID card administration** to manage the ID cards in your system.

Use the **Room administration** menu to manage rooms and associated reservations.

Use the **Area/door administration** menu to manage the security areas, room zones and doors and the time-related controls.

Use the **Calendar administration** menu to manage the calendars with special days and the necessary configuration data.

Use the **Locking plan administration** menu to manage the locking plans and their configuration.

Use the **Additional functions** menu contains special functions and applications for the access system.

Use the **Area monitoring** menu to view the security areas, with the option of correcting the counting values.

Use the **Door monitoring** menu to view the status display for the doors and to control the doors remotely.

Use the **Patrol** menu to manage and monitor the patrols.

Use the **Attendance display** menu item to open the configured popup dialogs belonging to the attendance display.

Use the **Reports** menu provides access to the different reports in the access system.

4.1 Person administration

In the **Person administration** menu you manage all persons and the master data required to allocate the access permissions; these include items such as access profiles, access weekly profiles and access daily times for granting access permissions

Access profiles are a combination of several access permissions. An individual access right is a combination of a room zone or a door/reader and an access weekly profile.

An access weekly profile determines for each day of a week which access daily time is used. In the access daily times you determine to the minute when a person has access permission, and you can use substitute programs to control the calendar dependency.

Functions for maintaining blocking reasons for persons and setting up departments and search profiles are also provided to help you manage Person administration.

Use the **Persons** menu item to manage the person records of all persons with access permission in your system.

Use the **Departments** menu item to manage all departments that you can allocate to persons.

Use the **Access profiles** menu item to manage the access profiles that control access permissions of persons.

Use the **VBI permissions** menu item to manage VBI permissions. VBI permissions can be allocated to persons to limit their booking options.

Use the **IDS profiles** menu item to manage permissions for arming/disarming IDS security areas.

Use the **Priority circuits** menu item to manage the priority settings which allow you to partially or fully override access checks for selected groups of persons.

Use the **Access weekly profiles** menu item to manage the access weekly profiles that are required to define the access profiles.

Use the **Access daily times** menu item to manage the access daily times that are required to define the access profiles.

Use the **Reasons for blocking person** menu item to manage the reasons for blocking which you can use to block and clear access for persons without deleting the employee master record.

Use the **Search profiles** menu item to manage the search profiles which you can use in selection dialogs, with corrections and in reports for searching persons.

4.1.1 Persons

For each person with access permission, you have to create an employee record in your system. This is the basis of the employee records transferred to the terminal peripherals, enabling performing the access validations during a booking.

In addition to the settings relevant for access, the employee record also includes organisational elements and current information on the bookings performed and the control functions for the AoC permissions.

For the individual assignment of permissions and special permissions, the employee record provides extensive input options.

Delete persons

Persons can be deleted regardless of data housekeeping limits. Dependent data is also deleted, where possible.

This is not possible for:

- Incomplete workflows
- Incomplete visits
- Incomplete patrols
- Incomplete room reservations
- Incomplete corrections

After deleting a person, their access bookings are neutralised by removing the link to the deleted person. This prevents the adulteration of access information at access points. The access bookings are retained without reference to persons.

Note: Please bear in mind that the default data housekeeping limit for personal records that are marked as Blocked or Former Employee is 60 days. These records will be deleted once this period has expired.

"Selection persons" dialog

The **Selection Persons** dialog lists all employee records in the system along with filter criteria, such as department, ID card number and work schedule. Select individual or multiple employee records for editing.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Note: The search fields and columns of the table may contain different fields depending on the employee record configuration selected.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Selection Persons

Last name

First name

Department

Employee number

ID card number

ID card label

Ignore date of joining

Ignore date of leaving

Start search

<input type="checkbox"/>	Last name	First name	Department	Employee number	ID card number	ID card label	Blocked	Delete
<input type="checkbox"/>	Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>	
<input type="checkbox"/>	Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>	
<input type="checkbox"/>	Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>	
<input type="checkbox"/>	Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>	
<input type="checkbox"/>	Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>	
<input type="checkbox"/>	Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Leroy	Fabienne	1 - Administration	4	9011	011	<input type="checkbox"/>	
<input type="checkbox"/>	Martin	Eric	1 - Administration	2	9002	002	<input type="checkbox"/>	
<input type="checkbox"/>	Matrino	Johanna	1 - Administration	3			<input checked="" type="checkbox"/>	
<input type="checkbox"/>	Meunier	Catherine	2 - Production	8	8204	204	<input type="checkbox"/>	

Number of records: 10

Note: When the **Several ID cards per person** option is active, an individual record is displayed in the table for each of the person's ID cards.

Last name column:

Contains the last name of the person.

First name column:

Contains the first name of the person.

Department column:

Contains the department to which the person belongs.

Employee number column:

Contains the unique employee number.

ID card number column:

Contains the unique ID card number of the allocated ID card.

Work schedule column:

Contains the person's allocated work schedule.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit persons" dialog

Use the **Edit Persons** dialog to create new persons and edit existing persons.

Note: The tabs in this dialog may contain different fields depending on the employee record configuration.

Dialog header**Last name** input field:

Contains the last name of the person. This field is mandatory. Enter the person's last name.

First name input field:

Contains the first name of the person. Enter the person's first name.

Department selection field:

Contains the department to which the person belongs. Select the relevant department from the list.

Note: The department cannot be changed if the person is included in time management. In this case, the department change is subject to correction in the time system.

Employee number input field:

Contains the unique employee number. This field is mandatory. Enter the relevant employee number for new records. This cannot be changed at a later stage.

Note: If the **Automatic generation of employee numbers** option is activated in the system parameters, no employee number can be entered.

ID card number input field:

Contains the ID card number, which clearly identifies the ID card across the company.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Encode and print ID card button:

If a PC reader is configured as an ID card creation system, the ID card can be encoded directly using this button. You can encode and print the ID cards simultaneously using a MAGiCARD printer.

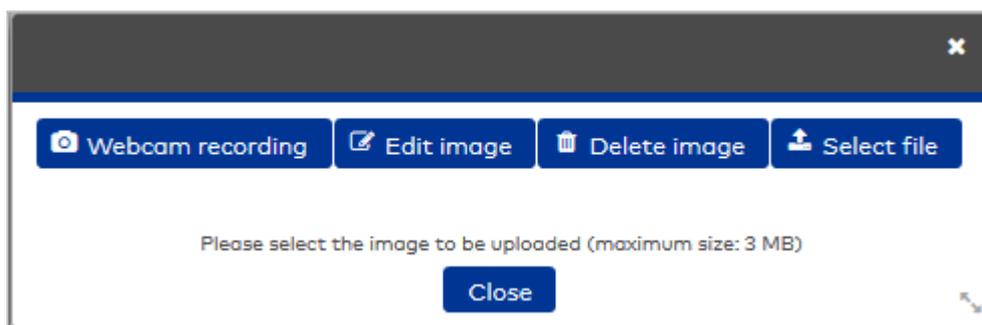
ID card label input field:

Contains the label visible on the ID card. This can be any text or a printed or handwritten number.

Note: The ID card administration options are only available when using simplified ID card administration (ID card administration level 1).

**Photo frame**:

Opens a pop-up dialog in which you can add, change or delete the person's profile photo. Click in the frame.

**Webcam recording** button:

Opens a connected webcam to take a profile photo directly. The following requirements must be fulfilled in order to be able to use this function:

- Connected webcam
- MATRIX must use an HTTPS connection
- The website requires permission to use the browser

Edit image button:

Opens the photo in a simple image editor. The available editing functions allow you to crop, flip and rotate your images.

Note: Webcam recording and image editing are not supported by Internet Explorer 11.

Delete image button:

Removes an existing image from the record. The image is immediately deleted and cannot be restored.

Select file button:

Opens a search dialog. Switch to the directory where the image file is saved, select the file and then click **Open**.

Close button:

Accepts the changes and closes the pop-up dialog.

"Access" tab

The **Access** tab contains the person's general access data and displays the bookings that have been made.

Mobile Access device number input field:

If using the Mobile Access via smartphone function, enter the telephone number.

The system automatically adds the prefix (phone#) if the Mobile Access device number (e.g. +49123456789) is entered.

Note: This option is only available if the Mobile Access via smartphone function is enabled (system parameter Access 150, value 1) and the ID card administration level is 1.

Attendance display field:

Contains the current attendance status of the person.

Possible status values:

- Unknown: The attendance status of the person cannot be determined as no access bookings are available to set the attendance status.
 - Present: The person is listed in the system as present.
 - Absent: The person is listed in the system as absent.
-

Note: If you have set up an attendance display in your system, you can also call up the attendance status of a person in the attendance display.

Reason for blocking selection field:

Contains the reason for blocking a blocked person. Select a reason for blocking if the person is not authorised to perform access bookings but is not to be deleted from the system. You can remove the reason for blocking at any time.

Options:

- All reasons for blocking created in the system.

VBI permission selection field:

Contains the VBI permission if the booking options available to the person are to be restricted.

Options:

- All VBI permissions created in the system.

PIN code input field:

Contains the PIN code that the person has to use as authentication on a reader with a keypad in addition to the ID card. Enter the relevant PIN code.

Value range for the PIN code: 1-999999.

If no value is entered, the PIN code is not requested from this person as long as the terminal configuration is set in line with the employee record settings.

Note: If the terminal is configured for PIN code input only, persons for whom no PIN code is specified cannot make a successful access booking.

Duress PIN code input field:

Contains an individual duress PIN code. This must only be entered if the +1/-1 logic in the variable booking instruction is to be overwritten. The duress PIN code replaces the calculated duress PIN if a VBI duress PIN does not equal 0.

Note: The duress PIN code field is only visible if the system parameter Access 21 "Individual PIN codes" is activated.

Note: You can use system parameter Access 22 "PIN code display in plain text" to specify whether the PIN code is displayed in plain text or is hidden and replaced with asterisks.

Counting group selection field:

Contains the counting group for the person. If counting information is enabled, all persons in a counting group appear as a distinct counting value in the monitoring dialog of the security areas.

Options:

- All counting groups created in the system.
-

Note: The "Counting information" option is only present if the system parameter Access 92 is enabled.

No accounting checkbox:

Indicates whether the person is excluded from the counting information.

Options:

- Activated: the person is not included in the counting information if the **Accounting according to employee record** checkbox is activated in the security area at the same time.
- Not activated: the person is included in the counting information.

Note: The next three fields for selecting IDS profiles and the IDS PIN code are only active if the system parameter Access 130 "Intruder Detection Systems" is set to 2 and system parameter Access 21 "Individual PIN codes" is set to 1.

IDS profile selection field:

Contains the IDS profile for arming/disarming IDS security areas.

Options:

- All IDS profiles created in the system.

IDS activation PIN code input field:

Contains the PIN code for arming IDS security areas.

Value range: 4 digits (numerical)

IDS deactivation PIN code input field:

Contains the PIN code for disarming IDS security areas.

Value range: 4 digits (numerical)

Enter in blocked list button:

Blocks the person with the reason for blocking "Blocked list" and creates a corresponding blocked list candidates. If a blocked list candidate of the same name already exists, a query will be displayed. You can decide whether to create the blocked list entry based on the existing entry (block based on *number*) or to generate a new blocked list candidate entry (block based on *new blocked list entry*).

Note: You require the appropriate user role rights to be able to make or cancel block list entries.

Tables:**ID cards:**

This table displays the ID cards allocated to the person.

Note: The ID card administration table is only available when using ID card administration level 2.

ID card number column:

Contains the encoded ID card number for the company ID card/access ID card, which uniquely identifies the ID card across the company (e.g. 508123).

Encode and print ID card button:

If a PC reader is configured as an ID card creation system, the ID card can be encoded directly using this button. You can encode and print the ID cards simultaneously using a MAGiCARD printer.

ID card label column:

Contains the printed label on the company ID card/access ID card (such as 123), if available.

Reason for blocking column:

Contains the reason for blocking for an ID card if a reason for blocking has been set for the ID card.

ID card type column:

Contains the type of the ID card that essentially determines the reading technology and the evaluation of the internal ID string.

Mobile Access device number column:

Enter the smartphone telephone number using the Mobile Access function.

Enter using the format "phone#+4917256889755".

Note: This column is only available if the Mobile Access function is enabled (system parameter 150) and the ID card administration level is 2. This field can only be edited for ID cards with the ID card type "Mobile Access".

Bookings:

This table displays the access bookings of a person on a daily basis. In the case of two-person access, the ID number of the second ID card is displayed in a tooltip.

Date display: Displays the date of the access log. Click the left arrow to move the date back by one day. Click the right arrow to move the date forward by one day. You can also enter a date or select one in the calendar.

Time column:

Displays the time of a booking on the selected date.

Booking type column:

Displays the type of booking, such as access, office release and so on.

Door column:

Displays the name in the respective language for the door where the booking took place.

Reader column:

Displays the name in the respective language for the reader on which the booking took place.

"Permissions" tab

Use the **Permissions** tab to create the various access permissions for the person. As an additional option to general access permissions, special permissions enable you to define advanced access rights that will only apply for a certain period, for example.

Note: The **Permissions** tab is not available if ID card administration is set to type 3 in the system parameters. In this case, access permissions are issued with the ID cards.

Access calendar »

Offline employee record

Office release

Priority settings »

AoC tracking

TMS door release

TMS alert resetting

TMS special function 3

Access valid from 📅

until 📅

Office release for door/reader

Door/reader ▲ New entry

55 XS 5(55 Development) ✎ 🗑

Permissions

Display current and future entries only

Access profiles	Access profile ▲	Valid from	Valid until			
	1 - Chief executive			✎	🗑	New entry

Special permissions New room zone permission New door/reader permission

Access via locking plan

Person group

Locking plan number	Name	Door number	Name	Permission	
1	Visitor centre	G:1	G:London-NewYork	<input checked="" type="checkbox"/>	- All - ▼
1	Visitor centre	101	Reception B5	<input checked="" type="checkbox"/>	
1	Visitor centre	102	Paris room	<input checked="" type="checkbox"/>	
1	Visitor centre	104	Berlin room	<input checked="" type="checkbox"/>	
1	Visitor centre	105	Rome room	<input checked="" type="checkbox"/>	

Access calendar selection field:

Contains the access calendar for access control.

Access valid from date field:

Contains the date from when the ID card access permission is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit in the past if the field is empty.

Access valid until date field:

Contains the date until when the access permission of the ID card is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit and is valid indefinitely if the field is empty.

Offline employee record checkbox:

Indicates an employee record which acts as an "emergency employee record" to enable door opening if a terminal fails. This employee record is loaded into the relevant components during initialisation and/or commissioning.

Bürofreigabe selection field:

Enables the person to activate an office release.

Options:

- No doors - the person is not allowed to activate an office release.
- All doors - the person is allowed to activate office release for all doors for which the person has access permission, provided the door supports the function.
- Selection - enables a person to allocate doors on an individual basis for which the person is allowed to activate the office release if they have access permission. The **Office release** table is displayed.

Office release for door reader table:

Use this table to enable office release on doors for which the person has access permission.

Doors with XS/evolo offline components can be release individually. Online doors can only be released individually if the system parameter (access) 141 is activated. AoC doors can only be released collectively.

Door/reader column:

Contains the door with number and name as well as the reader with number and name.

Priority settings selection field:

Priority settings can be used to override various checks for a booking.

Note: Priority settings are part of the person administration if ID card administration level 1 or 2 is activated. If ID card administration level 3 is enabled, the priority settings are part of the ID card administration.

Options:

- All priority settings created in the system.

AoC tracking checkbox:

Indicates that a booking log record is always created for this employee record, even if this is suppressed by the door daily time.

Note: You have access to the following three fields only if the **TMS connection** option is active. Special function 1, special function 2 and special function 3 can be equipped in TMS Software with different commands or logic links. Please note: Only special function 3 can be activated in addition to a TMS function.

TMS door release selection field:

Contains the selection for the door release of a TMS-secured door.

Values:

- Short - The door may be briefly unlocked
- Long - The door can be unlocked for an extended period
- Permanent - The door can be unlocked without time restriction
- Short long permanent - The door can be unlocked for a short or long time or permanently
- Special function 1 - The door's special function 1 may be used
- Special function 2 - The door's special function 2 may be used

TMS alert resetting checkbox:

Enables a person to acknowledge an alarm. Deselect the checkbox if you want to prevent the person from acknowledging an alarm.

TMS special function 3 checkbox:

Enables a person to initiate TMS special function 3. Deselect the checkbox if you want to prevent the person from using the TMS special function 3.

Permissions:**Display current only** checkbox:

Restricts the selection of the individual permissions displayed to the current values. Select the checkbox if you do not want to display any individual permission already expired. Deselect the checkbox to display all the individual permissions created.

Access profiles table:

Use this table to display and edit additional access tables.

Access profile column:

Contains the number and the name of the access profile.

Valid from column:

Displays the validity start date of the access profile.

Valid until column:

Displays the validity end date of the access profile.

Special permissions:**Room zones** table:

Use this table to display and edit special permissions for room zones. When a room zone permission is transferred, a check is performed to establish whether further related room zones have been defined for the room zone. Further related room zones are entered automatically.

Room zone column:

Displays the room zone to which the special permission applies.

Access weekly profile: column:

Displays the access weekly profile to which the room zone applies.

Valid from column:

Displays the validity start date of the special permission for the room zone.

Valid until column:

Displays the validity end date of the special permission for the room zone.

Door/reader table:

Use this table to display and edit special permissions for doors/readers.

Door (Reader) column:

Displays the door/reader to which the individual permission applies.

Access weekly profile: column:

Displays the access weekly profile that applies for the door/reader.

Valid from column:

Displays the validity start date of the special permission for the door/reader.

Valid until column:

Displays the validity end date of the special permission for the door/reader.

Access via locking plan:

As well as options for assigning access permissions via access profiles and special permissions, the person can also be allocated to one or more locking plans.

Provided the person is not yet allocated to a locking plan, the table with the access permissions from the locking plans is replaced by the selection field for the allocation.



The screenshot shows a rectangular box containing the text "No access via locking plan!" in blue. To the right of the text is a white input field with a blue dropdown arrow on its right side.

An individual can be allocated to one or more locking plans or allocated indirectly via a person group.

Options:

- Locking plan (individual), all locking plans
- Locking plan, select from all existing locking plans.
- Person groups, select from all existing person groups.

Person group selection field:

Contains the options for the person group. These options are used to allocate the person to the person group. The person then receives the corresponding access permissions for the person group from the locking plans.

Locking plan selection field:

Contains the options for the locking plan with the permissions displayed in the subsequent table.

Locking plan table:

Depending on the selected locking plan, the table displays all doors that can be given permissions using the selected locking plans. The table can also be used to edit the permissions. For locking plans with single time profiles, the permission is activated via a checkbox; for individual access, the corresponding access weekly profile has to be selected.

Locking plan number column:

Contains the number for the locking plan.

Name column:

Contains the name for the locking plan.

Door number column:

Contains the number for the door of the locking plan.

Name column:

Contains the name for the door of the locking plan.

Permission column:

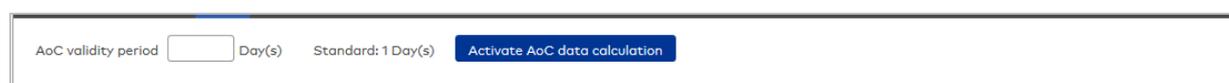
Contains the permission from the locking plan depending on the setting as a checkbox for **single time profiles** or as a selection field for the access weekly profile for **individual** access.

"AoC" tab

The **AoC** tab contains the settings of the person for participating in AoC (Access on Card). The table displays the AoC data for the selected date. In addition to the blanket interval, the access spectrum for special intervals is shown with the access permissions.

Note: The **AoC** tab is only available if the AoC function is activated in the system parameters and ID card administration level 1 or 2 is activated.

If ID card administration level 3 is active, this tab is part of the ID card administration.



The screenshot shows a form with the following elements: "AoC validity period" followed by an input field containing "1", "Day(s)", "Standard: 1 Day(s)", and a blue button labeled "Activate AoC data calculation".

AoC validity period input field:

Determines the length of time for which the data on the AoC ID card is valid. Usually the AoC data are calculated for one day and written on the ID card.

Activate AoC data calculation button:

Click this button to activate the calculation of the AoC data. The AoC data is shown in the tables below.

AoC data for date selection:

Here the date is selected for which the AoC data are displayed. Both future and past dates can be selected. Enter a date or click the calendar icon and select a date.

Blanket interval**Blanket interval of** display field:

Displays the calculated blanket interval for the date selected.

Blanket interval table:**Reader** column:

Displays the reader to which the blanket interval applies.

Special intervals**Special intervals** table:

Displays the calculated special intervals for the selected date. If the AoC validity is longer than 1 day, the output starts with the selected date.

Reader column:

Displays the reader to which the special interval applies.

Access column:

Displays the start and end of the special interval.

Valid on column:

Display of the data to which the special interval applies.

"Official data" tab

The **Official data** tab contains official contact data and additional information on company affiliation and function. All fields on this tab are optional; you do not have to enter any data.

Day of joining date field:

Contains the date from which the person is employed in the company. Enter a date or click the calendar icon and select a date.

Place of employment input field:

Contains the place of employment to which the person is allocated, such a subsidiary or branch office.

Phone input field:

Contains the business phone number of the person.

Mobile phone input field:

Contains the business mobile phone number of the person.

E-mail input field:

Contains the business e-mail address of the person.

Date of leaving the company date field:

Contains the date from which the person has left/will leave the company.

If the set leaving date is in the past, the blocking reason "Former employee" will be set immediately. If the person is assigned as a user, this authorisation will also be blocked.

If the set leaving date is in the future, background tasks ensure that the blocking reason is set starting on the day after the leaving date. The time zone of the respective person is taken into consideration.

Function input field:

Contains the function of the person within the company.

Identifier input field:

For specifying additional attributes, such as the company car LPN.

Comment input field:

Free text field for specifying additional comments.

"Personal information" tab

The **Personal information** tab contains personal data and additional information on the person. All fields on this tab are optional; you do not have to enter any data.

Number or Name/Street	<input type="text"/>	Title	1 - Dr. 
Town/ Postcode	<input type="text"/>	Date of birth	06/12/1957 
Phone	0453/362332	Sex	1 - male 
Mobile phone	0175/44556677	Marital status	2 - Married 
E-mail (private)	t.ackreiter@provider.com	Comment	<input type="text"/>

Number or Name/Street input field:

Contains the street and street number where the person is registered.

Town/Postcode input field:

Contains the postcode and city where the person is registered.

Phone input field:

Contains the private phone number of the person.

Mobile phone input field:

Contains the private mobile phone number of the person.

E-mail input field:

Contains the private e-mail address of the person.

Title selection field:

Contains the academic title of the person. Select a title from the list.

Date of birth date field:

Contains the date of birth of the person. Enter a date or click the calendar icon and select a date.

Sex selection field:

Contains the gender of the person. Select a gender from the list.

Marital status selection field:

Contains the marital status of the person. Select a marital status from the list.

Comment input field:

For specifying additional comments.

"Other" tab

The **Other** tab contains two input fields in which you can save additional comments and information.

The screenshot shows a tab labeled "Other" with a dark header. Below the header, there are two text input fields. The first is labeled "Comments" and the second is labeled "Additional information". Both fields are empty and have a light gray border.

"Documents" tab

The **Documents** tab contains all the documents saved for the respective person.

Note: This tab is only present if documents have been imported for this person.

Name	File name	File size	Created by	Creation date	Download	Delete
Annual statement	7.pdf	18 kb	Import	07/06/2020 13:00:56		
NDA	7.pdf	66 kb	Import	07/06/2020 13:09:39		

Number of records: 2

Click the symbols to download or delete any of the saved documents. Documents can be added to employee records using the [Document import interface](#).

"Login" tab

The **Login** tab contains the necessary information on the login into the system. In addition to the operators who administrate the system, people who carry out visitor reservations, perform room administration or carry out web bookings, for example, also require a user ID for logging in.

Note: This tab is mainly used to display the associated user data. You can use the **Details** symbol to switch directly to the **Edit user** dialog and edit the user data there.

The screenshot shows the "Login" tab interface. At the top, there is a "User ID" field with the value "ackreiter" and a dropdown arrow. Below this, there are two sections: "User information" and "Workflow settings". Under "User information", there is a field for "Employee record dialog allocation" with a dropdown menu showing "13 - Employee time allocation". Under "Workflow settings", there is a field for "Organisational unit" with a dropdown menu showing "1 - Management". At the bottom, there is a section for "Allocated user roles" with a table:

Number	Name
10	Superior

User ID field:

Displays the system-wide unique user name. You can use the **Details** symbol to open the **Edit user** dialog, where you can create or edit the user record.

Allocate employee record configuration:

For the maintenance of employee master data, you must select a configuration for the employee record dialog for every user.

If the selection is empty, but the user has access permissions for person maintenance, a corresponding message appears when person maintenance is opened from the menu.

Note: The selections are only active with the relevant licence.

Person administration time selection field:

Determines the employee record dialog for opening the employee master data from the **Access** menu.

Options:

- All employee record dialogs created in the system.

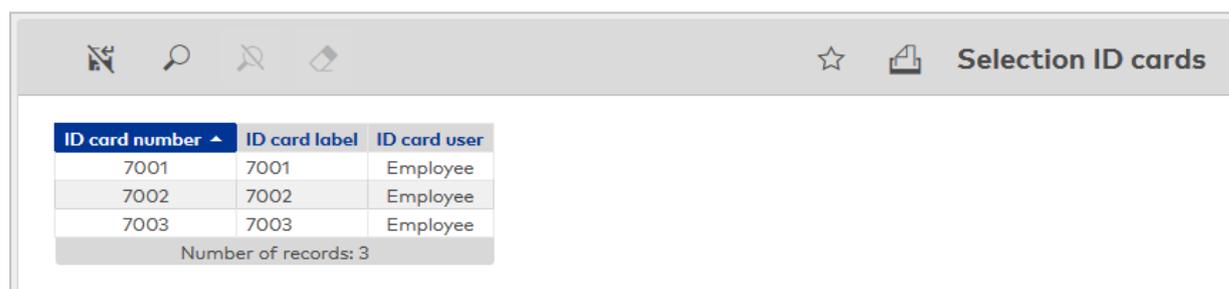
Allocated user roles table:

Contains the user roles allocated to the user, in which the access permissions for the dialogs are specified.

"Selection ID cards" dialog

Use the **Selection ID cards** dialog to search for ID cards that have not yet been allocated and transfer them directly to the invoking dialog.

Note: When selecting ID cards as replacement ID cards, only ID cards of the same ID card type as the ID card to which the replacement ID card is to be allocated will be considered. This applies also to combi ID cards if they have an ID string with the same ID card type.



ID card number	ID card label	ID card user
7001	7001	Employee
7002	7002	Employee
7003	7003	Employee

Number of records: 3

Click an entry to directly apply the corresponding record.

"Selection forms" dialog

Use the **Selection Forms** dialog to select the forms to be printed out.

Note: The selection dialog is not displayed if only one form is present and if the form does not require a signature.



Number	Name	Short name
1	Visit - info	
8	ID card handover (with signature pad)	

Number of records: 2

Print selection

Sign

All existing forms are displayed in the table. Highlight a form and start printing by pressing the **Print selection** button.

Sign button:

This opens the form in a popup dialog. It can be read and signed in this dialog. The forms are subsequently saved in MATRIX or can be output as PDFs or as hardcopies using a printer.

Note: This button is only present if a form requires a digital signature. A device providing a touchscreen or signature pad must be connected in order to use this function.

4.1.2 Departments

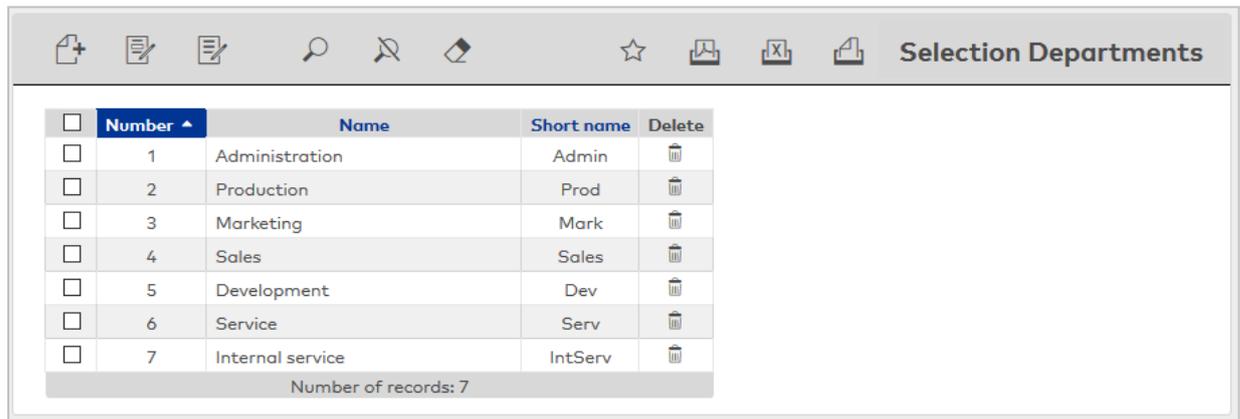
The departments allow you to map your company's organisational structure. The departments created can then be allocated to persons.

Creating departments is optional, although it is recommended for larger companies. Employee records, annual overviews, bookings and evaluation reports can be filtered using the departments.

"Selection departments" dialog

The **Selection Departments** dialog displays all created departments.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number	Name	Short name	Delete
<input type="checkbox"/>	1	Administration	Admin	
<input type="checkbox"/>	2	Production	Prod	
<input type="checkbox"/>	3	Marketing	Mark	
<input type="checkbox"/>	4	Sales	Sales	
<input type="checkbox"/>	5	Development	Dev	
<input type="checkbox"/>	6	Service	Serv	
<input type="checkbox"/>	7	Internal service	IntServ	

Number of records: 7

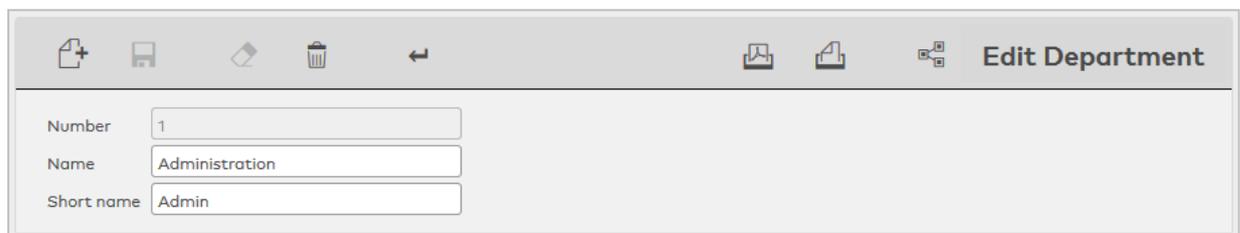
Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit department" dialog

Use the **Edit Department** dialog to create new departments and edit existing department records. Each department requires a unique number; it is recommended that you specify a name and a short name.

Departments are used to allocate person records to organisational units.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Number:

Name:

Short name:

Number input field:

Contains the department's unique number. When you create a new record, the number increases

automatically by an increment of one. However, you can also enter your own number between one and six digits (1–999999).

Name input field:

Contains the department's name. When you enter a new name, you can enter any combination of figures and letters. This field is language-dependent.

Short name input field:

Contains the department's short name. When you enter a new short name, you can enter any combination of figures and letters. This field is language-dependent.

4.1.3 Access profiles

Access profiles are groups of access permissions. An access permission consists of an allocation of a door (reader) or a room zone to an access weekly profile. The doors/readers and the room zones determine the local specifications and the access weekly profiles determine the time specifications.

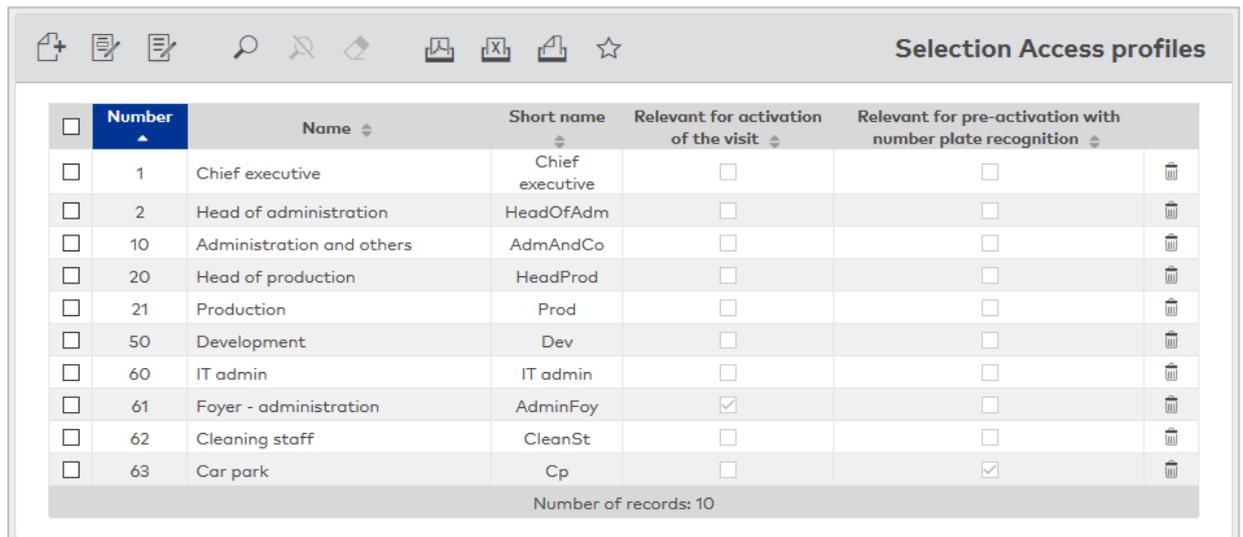
You can define several access permissions for each access profile. You can allocate room zones or door/reader may to several access profiles.

Further information on the use of access profiles can be found in the section "Getting started" under "[Create a new access system](#)".

"Selection access profiles" dialog

The **Selection access profiles** dialog displays all access profiles created for access control.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.



<input type="checkbox"/>	Number	Name	Short name	Relevant for activation of the visit	Relevant for pre-activation with number plate recognition	
<input type="checkbox"/>	1	Chief executive	Chief executive	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	2	Head of administration	HeadOfAdm	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	10	Administration and others	AdmAndCo	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	20	Head of production	HeadProd	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	21	Production	Prod	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	50	Development	Dev	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	60	IT admin	IT admin	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	61	Foyer - administration	AdminFoy	<input checked="" type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	62	Cleaning staff	CleanSt	<input type="checkbox"/>	<input type="checkbox"/>	
<input type="checkbox"/>	63	Car park	Cp	<input type="checkbox"/>	<input checked="" type="checkbox"/>	

Number of records: 10

Note: The **Relevant for ...** columns are only present if the relevant functions are enabled.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit access profile" dialog

Use the **Edit access profile** dialog to create new access profiles and edit existing access profiles.

You can allocate several room zones or readers and an access weekly profile to each access profile. Access profiles are assigned to persons in person administration.

Use the additional **Cross table for access permissions** button in the toolbar to configure the access weekly profile for one or more access profiles by selection in a cross table.

Edit Access profile

Number: 10

Name: Administration and others

Short name: AdmAndCo

Relevant for activation of the visit:

Relevant for pre-activation with QR Code:

Permissions

Door (Reader) ^	Room zone/range	Access weekly profile			New entry
	1 - Foyer - administration	10 - Administration			
	3 - Administration and others	10 - Administration			

Number of records: 2

Persons with this access profile

Last name ^	First name	Department	Employee number	ID card number	ID card label
Leroy	Fabienne	Administration	4	9011	011
Martin	Eric	Administration	2	9002	002

Relevant for activation of the visit checkbox:

Indicates if the access profile can be used for visitors in the visitor administration.

Options:

- Activated: The access profile can be used for visitors.
- Not activated: The access profile cannot be used for visitors.

Note: The checkbox is only present if the system parameter Access 70 "Visitor administration" is activated.

Relevant for pre-activation with QR code checkbox:

Indicates if the access profile can be used in visitor administration for access with QR code ID cards.

Options:

- Activated: The access profile can be used for access with QR code ID cards.
- Not activated: The access profile cannot be used for access with QR code ID cards.

Note: The checkbox is only present if the system parameter Access 70 "Visitor administration" is activated and the system parameter Access 73 "With QR code" has the value "2".

Relevant for pre-activation with LPN recognition checkbox:

Identifier indicating whether the access profile can be used for LPN recognition access in visitor administration.

Options:

- Activated: The access profile can be used for LPN recognition access.
- Not activated: The access profile cannot be used for LPN recognition access.

Note: The checkbox is only present if the system parameter Access 76 "With number plate recognition" is activated.

Permissions table:

Contains the allocated access permissions.

Door (Reader) column:

Contains the unique number of the door/reader and the name in the respective language to which the access permission applies.

Room zone/range column:

Contains the unique number of the room zone and the name in the respective language to which the

access permission applies. When a room zone permission is transferred, a check is performed to establish whether further related room zones have been defined for the room zone. Further related room zones are entered automatically.

Access weekly profile: column:

Contains the unique number for the allocated access weekly profile and the name in the respective language.

Persons with this access profile table:

Displays all persons to whom the access profile is allocated.

"Edit access profile permission" dialog

Use the **Edit Access profile permissions** dialog to configure permissions for one or more access profiles using a cross table.

Use the buttons in the toolbar to save or reject changes to the record or print the cross table from a PDF file. Use the **Back to selection** button to return to the selection dialog.

10 Administration and others	
Room zone - 1 - Foyer - administration	10 - Administration
Room zone - 2 - Chief executive	
Room zone - 3 - Administration and others	10 - Administration
Room zone - 4 - Head of administration	1 - Always
Room zone - 5 - Development	

The magnifier opens the **Selection Folder** dialog, which you can use to select the folder for which you wish to edit the permissions for doors/readers or room zones.

Note: This option is only available when folders are created in the room zone/door administration.

The left-hand column in the table shows all readers and room zones in the selected folder or, if no folders have been added, all available readers and room zones.

The selection is displayed for each access profile in another column. Use the selection field to allocate access weekly profiles.

Note: The number of table rows and columns displayed on a page can be limited using the system parameters Access 63 (number of rows) and Access 64 (number of columns). Use the arrow buttons to navigate forwards and backwards if more records are present than rows and columns per page.

"Selection folders" dialog

The **Selection Folder** dialog displays all folders created in the room zone/door administration.

You can use the buttons in the toolbar to apply a highlighted folder to the selection or return to the calling dialog without applying a folder.

Use the search function to search for individual folders using their number, name or short name.



To select a folder, highlight it and click **Edit selected search results** in the toolbar.

4.1.4 VBI permissions

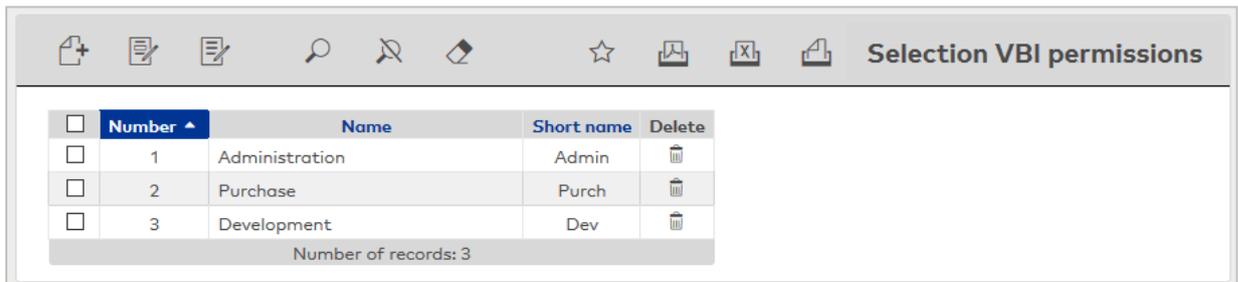
Use the VBI permissions to specify which variable booking instructions can be executed by a person. The VBI permissions are allocated to a person using the employee record.

The variable booking instructions are used for terminals with booking keys.

"Selection VBI permissions" dialog

The **Selection VBI permissions** dialog displays all VBI permissions created.

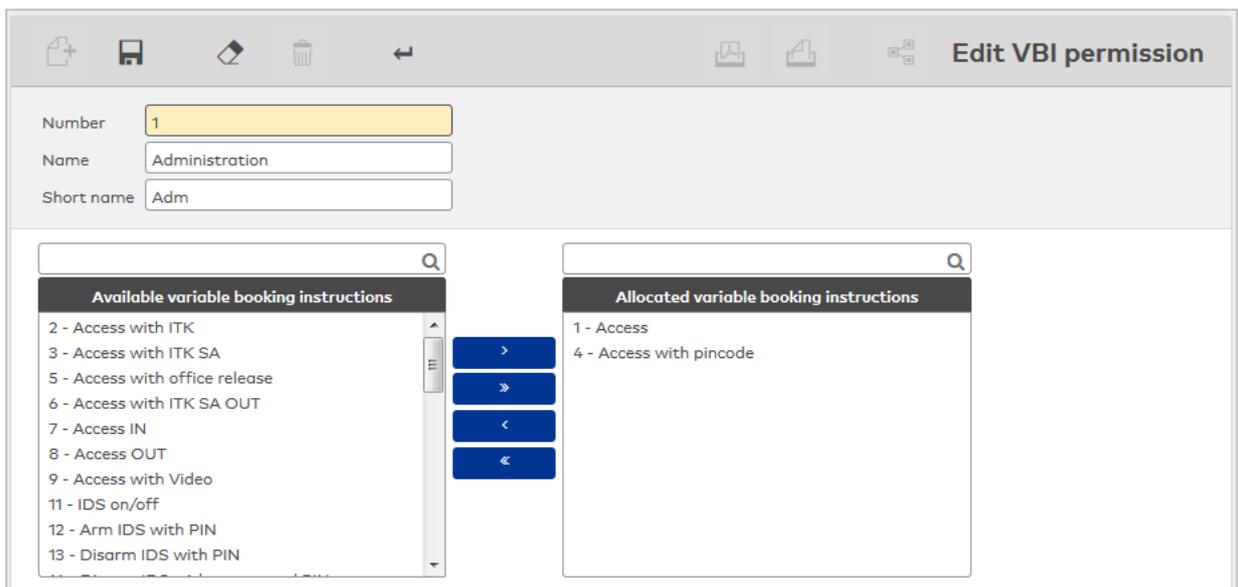
The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit VBI permission" dialog

Use the **Edit VBI permission** dialog to create new VBI permissions and edit or delete existing VBI permissions.



Use the selection report to allocate all required booking commands to the VBI permissions.

4.1.5 IDS profiles

Use an IDS profile to authorize persons to arm or disarm IDS areas. The profile contains a list of IDS areas. A permission for arming, disarming or both can be issued for each IDS area.

The profiles are allocated to persons in person administration.

"Selection IDS profiles" dialog

The **Selection IDS profiles** dialog displays all created IDS profiles.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

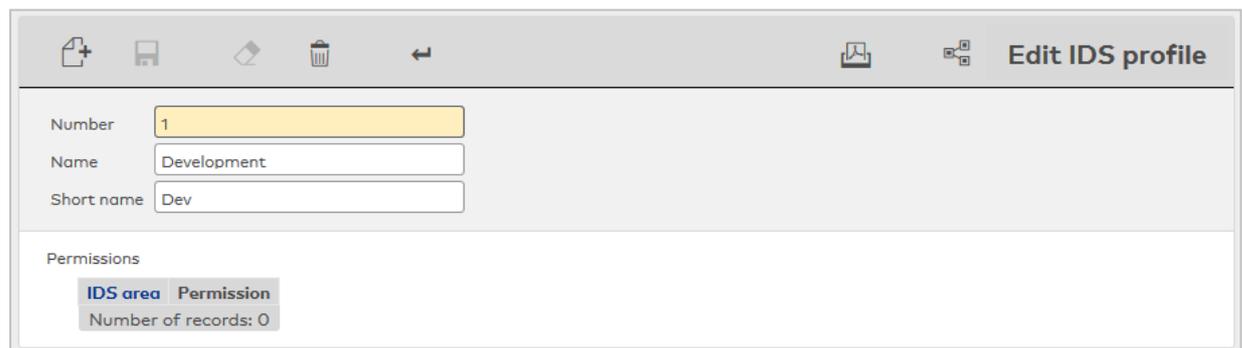


Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit IDS profile" dialog

Use the **Edit IDS profile** dialog to create new IDS profiles and edit or delete existing IDS profiles. Each IDS profile requires a unique number; it is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Permissions table:

The table contains the IDS areas with their relevant permissions.

IDS area column:

Contains the IDS area for the permission.

Options:

- All IDS areas created in the system.

Permission column:

Contains the permission for the IDS area.

Options:

- Arming only: the IDS area can only be armed.
 - Disarming only: the IDS area can only be disarmed.
 - Arming/disarming: the IDS area can be armed and disarmed.
- Default value: Arming only.

4.1.6 Priority circuits

Priority settings can be used to override various checks for a booking.

This means that a positive access booking can be enabled for specific persons even when access is not possible due to, for example, a door daily time.

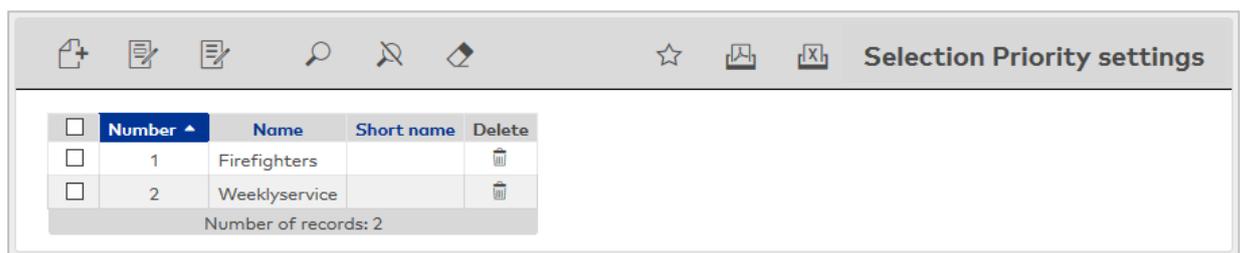
Note on counting information: Persons who are granted access via the priority circuit are included in the counting information.

Note: Priority settings are part of the person administration if ID card administration level 1 or 2 is activated.
If ID card administration level 3 is enabled, the priority settings are part of the ID card administration.

"Selection priority settings" dialog

The **Selection Priority settings** dialog displays all priority settings created in the access system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit priority settings" dialog

In the **Edit Priority settings** dialog, you can create new priority settings and edit existing priority settings. Each priority setting requires a unique number. It is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number

Name

Short name

No access restriction through a door program

No PIN code check

No repeated access lock check

No hard anti-passback

No area-to-area movement control

No check of number of persons

No attendance control for two persons

No access control for two persons

No monitoring of duration of stay

No check for activated IDS

No access restriction through a door program checkbox:

Indicates whether the door daily time's checks are to be performed. Switching off the check makes a positive access booking possible even during time ranges or under conditions when the door program's check would prevent this.

Options:

- Activated: for an access booking, door programs are not taken into account by the check.
- Not activated: door programs are included in the access check.

Default value: Not activated

No PIN code check checkbox:

Indicates whether the PIN code check is to be switched off. If the check is switched off, entry of a PIN code is not necessary.

Options:

- Activated: no PIN code check is performed.
- Not activated: a PIN code check is performed if this is required by other configuration settings.

Default value: Not activated

No attendance control checkbox:

Indicates whether attendance control is to be switched off. Switching off the check makes a positive access booking possible even if the person is not listed as present in the specified area.

Options:

- Activated: access control is not checked.
- Not activated: access control is checked.

Default value: Not activated

No timed anti-passback checkbox:

Indicates whether the timed anti-passback is to be switched off. Switching off the check makes a positive access booking possible even if the person makes a booking within the time frame for the timed anti-passback.

Options:

- Activated: the timed anti-passback is not checked.
- Not activated: the timed anti-passback is checked.

Default value: Not activated

No hard anti-passback checkbox:

Indicates whether the hard anti-passback is to be switched off. Switching off the check makes a positive access booking possible even if the person is still listed as present in the area to which they would like to gain access.

Options:

- Activated: the hard anti-passback is not checked.
- Not activated: the hard anti-passback is checked.

Default value: Not activated

No area-to-area movement control checkbox:

Indicates whether the area-to-area movement control is to be switched off. Switching off the check makes

a positive access booking possible even if the person is not listed as present in the specified area.

Options:

- Activated: area-to-area movement control is not checked.
- Not activated: area-to-area movement control is checked.

Default value: Not activated

No access control for two persons checkbox:

Indicates whether the access control for two persons is to be switched off. Switching off the check makes a positive access booking possible for one person even if two bookings are stipulated.

Options:

- Activated: the access control for two persons is not checked.
- Not activated: the access control for two persons is checked.

Default value: Not activated

No attendance control for two persons checkbox:

Indicates whether the attendance control for two persons is to be switched off. Switching off the check makes a positive access booking possible for one person even if no second person is booked as present in the area.

Options:

- Activated: the attendance control for two persons is not checked.
- Not activated: the attendance control for two persons is checked.

Default value: Not activated

No monitoring of duration of stay checkbox:

Indicates whether the monitoring of duration of stay is to be switched off. Switching off the check makes a positive access booking possible for one person even if the duration of stay has been exceeded and/or the blocking time for a booking has not yet expired.

Options:

- Activated: monitoring of duration of stay is not checked.
- Not activated: monitoring of duration of stay is checked.

Default value: Not activated

No check for armed IDS checkbox:

Indicates whether the check for armed IDS is switched off. Switching off the check makes a positive access booking possible for one person even if the IDS is armed.

Options:

- Activated: armed IDS are not checked.
- Deactivated: armed IDS are checked.

Default value: Not activated

4.1.7 Access weekly profiles

An access weekly profile determines for each day of a week which access daily time is used. The access weekly profiles thus form the time-related component for the access permissions.

"Selection Access weekly profiles" dialog

The **Selection Access weekly profiles** dialog displays all access weekly profiles created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Number	Name	Short name	Delete
1	Always	Always	
2	Head of administration	HeadOfAdm	
3	Head of production	HeadProd	
10	Administration	Admin	
11	Production	Prod	
12	Development	Dev	
13	Cleaning staff	CleanSt	

Number of records: 7

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Access weekly profile" dialog

Use the **Edit Access weekly profile** dialog to create new access weekly profiles and edit existing access weekly profiles. Each access weekly profile requires a unique number. It is recommended that you specify a name and a short name.

In an access weekly profile, an access daily time is allocated to each calendar day in a week.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

"Access weekly profile" tab

This tab is used to assign access weekly profiles.

Day	Access Profile	Dropdown	Next
Monday	3 - Full (7-18)	▼	▶
Tuesday	3 - Full (7-18)	▼	▶
Wednesday	3 - Full (7-18)	▼	▶
Thursday	3 - Full (7-18)	▼	▶
Friday	3 - Full (7-18)	▼	▶
Saturday	2 - Never	▼	▶
Sunday	2 - Never	▼	▶

Access daily time for Monday: to Sunday selection fields:

Contain the number and name of the access daily time used on a particular day. You must select an entry for each weekday.

"evolo time profile" tab

Note: The tab is only present if evolo components are used.

If evolo components are used in the system, the time frame is mapped from the assigned access daily times to the evolo time profile for use in the evolo components. The mapping is displayed on this tab for checking.

evolo time profiles consist of a report of time ranges during which the component allows access. A time range can be valid for one or more weekdays, on holiday days, or on the two special day types A or B.

Access weekly profile		evolo time profile										
From	To	Day	Ho	Mo	Tu	We	Th	Fr	Sa	Su	A	B
06:00	20:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>				
06:00	14:00	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

The resulting time frames from the access daily times are displayed in the table. Changes cannot be made directly. They must be made in the corresponding access daily times.

Note: Holiday days are weekday-dependent, whereas special days are independent of the day of the week. This means that a time range for a holiday Monday does not necessarily need to apply for a holiday Tuesday. For special days, it is not possible to distinguish between weekdays.

From/To columns:

Contain the time interval for access.

Day column:

Identifier for access on the set weekdays (Mo to Su).

Ho column:

Identifier for access on a bank holiday.

Mo, Tu, We, Th, Fr, Sa, Su column:

The columns contain the identifiers for the weekdays from Monday to Sunday.

Column **A**:

Identifier for the day type A.

Column **B**:

Identifier for the day type B.

Convert an access weekly profile

The conversion of the access weekly profile into the evolo time profile takes place as follows:

Firstly, the "access" time ranges of each access daily time used are carried over to the time profile and a tick placed in the "Day" column for the corresponding weekday.

Next, the system runs through the access daily time substitute programs:

- If no substitute program is defined for the access daily time, it will also apply on holiday days and all special days.
- If there is a substitute program for the holiday day type, the time ranges of this substitute program are carried over to the time profile and a tick placed for Holidays and the corresponding weekday.
- If a substitute program is available for a day type with the special day identifier A, the time ranges are transferred and a tick entered in column A. The same applies to type B.

Optimise by combining time ranges

Finally, as evolo components only allow a maximum of 12 time ranges per time profile, the system attempts to combine time ranges.

Conditions for combining rows:

1. The time frame is the same for both "From" and "To".
2. If both Day and Holidays are ticked, the rows can be combined by linking the ticks for the weekdays and special day type using an OR function.
3. If a row only applies for special days, i.e. has no tick for Day and Holidays, and there is the same time range in the time profile, the rows can be combined by simply placing a tick additionally for the corresponding special day in the other time range.

Validation

An access daily time cannot always be converted to an equivalent time profile. The following validations will appear in the interface with corresponding messages:

1. Maximum 12 time ranges. If more time frames were generated during the conversion, a message to this effect appears.
2. Because substitute programs depend on the time profile for evolo components, only one substitute program may be allocated to a day type. If different substitute programs are allocated to a day type, a message to this effect appears.

Note: If no substitute program is assigned to a day type, the same daily program applies on special days, i.e. the substitute program is the same as the program, so to speak. It is therefore not possible for e.g. evolo components to use two daily programs and specify special days but not assign a substitute program to either.

3. If substitute programs are defined for day types that are marked as neither a special day nor a holiday day, these are ignored in evolo components. A corresponding notification is output in the access weekly profile on the **evolo time profile** tab.

4.1.8 Access daily times

Use the access daily times to define for each day the time intervals when a person with an authorised ID card is granted access.

Access daily times are a basic part of the access control and are combined into one week to determine the access weekly profiles.

Substitute door daily times can be used to allocate a separate access daily time to each day type, such as bank holidays or special days. As a prerequisite, the day types must have been entered in the calendar and respective substitute door daily times must have been defined in the access daily time for the respective day type.

For example, access may be permitted for weekdays in the time from 10:00 h to 18:00 h.

If the weekday coincides with a bank holiday on which no access is supposed to be possible, a substitute access daily time must be entered for the respective day type which does not contain a time frame for the access.

"Selection Access daily times" dialog

The **Selection Access daily times** dialog displays all access daily times created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Number	Name	Short name	Delete
1	Always	Always	
2	Never	Never	
3	Head of administration	HeadOfAdm	
4	Head of production	HeadProd	
10	Administration - complete day	AdminCD	
11	Administration - half day	AdminHD	
20	Production - complete day	ProdCD	
21	Production - half day	ProdHD	
50	Development	Dev	
60	Cleaning staff	CleanSt	

Number of records: 10

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Access daily time" dialog

Use the **Edit Access daily time** dialog to create new access daily times and edit existing access daily times. Each access daily time requires a unique number; it is recommended that you specify a name and a short name.

For each access daily time you can define up to four time periods for the access. If you enter a time interval, you must include a start and an end value.

Use **Substitute programs** to allocate a substitute daily program to each day type.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

From	Until	From	Until	From	Until	From	Until
Access	08:00	17:00					
Substitute programs							
Day type				Substitute programs			
3 Bank holiday				2 - Never			

Access input fields:

Contain the time intervals in which access booking is possible with the relevant ID card.

Substitute programs table:

Contains substitute programs that you can define for individual day types.

Day type column:

Contains the unique number and language-dependent name of the day type. The day types are determined using the calendar, which is connected by permissions to the access weekly profile.

Substitute programs column:

Contains the selected substitute daily program. Select the relevant substitute daily program from the list. This field remains empty if the original access daily time is always used for a day type.

4.1.9 Reasons for blocking person

In this area you can maintain the reasons for blocking persons. They can then be allocated to the persons in person administration. This procedure allows persons to be simply blocked or cleared without losing the person master data. Blocked persons cannot perform any bookings. A blocking reason for a person applies at the same time also for all ID cards allocated to the person. In addition to default blocking reasons, you can also create additional blocking reasons.

"Selection reasons for blocking person" dialog

The **Selection Reasons for blocking person** dialog displays all reasons created for blocking persons.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number	Name	Short name	Relevant for AoC back lists	Delete
<input type="checkbox"/>	1	Blocked	B	<input type="checkbox"/>	
<input type="checkbox"/>	2	Works ban	WB	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	3	Former employee	L	<input type="checkbox"/>	

Number of records: 3

Relevant for AoC black lists column:

Contains the identifier indicating whether the reason for blocking is relevant to the AoC black lists.

Note: This column is only available if the AoC function is activated in the system parameters.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit reason for blocking persons" dialog

Use the **Edit Reasons for blocking person** dialog to create new blocking reasons persons and edit existing blocking reasons. Each reason for blocking requires a unique number; it is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number	<input type="text" value="1"/>
Name	<input type="text" value="Blocked"/>
Short name	<input type="text" value="B"/>
Relevant for automatic deletion	<input type="checkbox"/>
Relevant for AoC black list	<input type="checkbox"/>

Relevant for automatic deletion checkbox:

Indicates whether persons with this reason for blocking are automatically deleted via the **Blocked persons** data housekeeping limits. Activate this checkbox if persons with this reason for blocking are to be deleted via the data housekeeping limits.

Relevant for AoC black list checkbox:

Identifier indicating that the reason for blocking affects the AoC black list. Activate the checkbox if a blocked ID card with the reason for blocking shall be included in the AoC black list.

Note: The checkbox is only present if the AoC function is activated in the system parameters.

If you block an ID card with a reason for blocking relevant to AoC black list, blocking only becomes effective after a synchronisation with the AoC readers.

Changes do not affect existing blocks.

4.1.10 Search profiles

Search profiles always apply to the respective person group and are accordingly available in either person administration, external company employee administration or visitor administration. They can be used by opening the advanced search function (double magnifying glass) provided in the selection dialogs.

Search profiles enable users to display or edit persons, visitors or external company employees with corresponding characteristics. All elements with direct relationships to a person group can be included in the selection process. The selected set can be specified precisely using linkable search criteria and used in all person-related dialogs.

Search profiles also play an important role in the output of person-related reports. The group of persons for the report is determined by a search profile. Likewise, the period for the search for data with time reference and the output period are defined by the search profile.

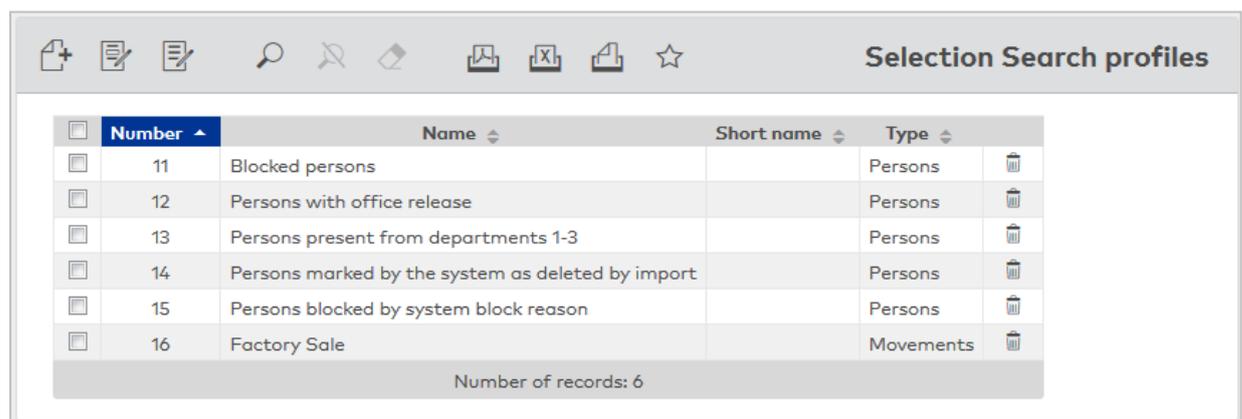
If the search profile requires parameters to be entered, parameter input is automatically activated when opening the report.

"Selection search profiles" dialog

All search profiles created in the system are displayed in the **Selection Search profiles** dialog.

The search profiles are available from the person administration, external company administration and visitor administration dialogs for advanced search functions.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



The screenshot shows the 'Selection Search profiles' dialog with a toolbar at the top containing icons for adding, editing, deleting, searching, and other actions. Below the toolbar is a table with the following data:

<input type="checkbox"/>	Number	Name	Short name	Type	<input type="checkbox"/>
<input type="checkbox"/>	11	Blocked persons		Persons	<input type="checkbox"/>
<input type="checkbox"/>	12	Persons with office release		Persons	<input type="checkbox"/>
<input type="checkbox"/>	13	Persons present from departments 1-3		Persons	<input type="checkbox"/>
<input type="checkbox"/>	14	Persons marked by the system as deleted by import		Persons	<input type="checkbox"/>
<input type="checkbox"/>	15	Persons blocked by system block reason		Persons	<input type="checkbox"/>
<input type="checkbox"/>	16	Factory Sale		Movements	<input type="checkbox"/>

At the bottom of the table, it says: Number of records: 6

Type display field:

Contains the data type on which the search profile is based and for which it is used.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit search profiles" dialog

Use the **Edit Search profile** dialog to create new search profiles and edit existing search profiles. Each search profile requires a unique number; it is recommended that you specify a name and a short name.

The search profile fields present in the **Edit Search profile** dialog depend on the data type.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Data types: persons, external company employees, visitors

Criterion	Value range		
Department	1;2;3		
Attendance	1		

Table:

The table contains the conditions of the search profile.

Criterion selection field:

Contains the search element for the search condition.

Value range input field:

Contains the value or value range describing your search quantity.

Possible parameters:

- The parameters depend on the selected criterion. A tooltip in the opened input line shows all possible values and operators for the criterion.
- Use the wildcard @EMPTY if you wish to search for missing or empty fields.
- Use the wildcard @NOTEMPTY if you wish to search for arbitrary values.
- To keep the value range flexible, use wildcards of the type @1, @2, @3 etc., where 1 stands for the first parameter, 2 stands for the second parameter etc. Specific values will be queried if a search profile is used.
- An OR operator can be created within a row using a semicolon ;

"Apply filter" dialog

If a search profile containing wildcards is used, specific values will be queried in the **Apply filter** dialog.

Input fields:

The input fields are determined by the search profile. All fields from the search profile that contain a wildcard will be displayed.

Cancel button:

Cancels the input and returns to the invoking dialog without evaluating the search profile.

Next button:

The search is carried out using the specified search criteria. The following selection dialog contains all persons (or visitors, external company employees) that match the search criteria.

4.2 External company administration

Use the **External company administration** menu to manage all companies and their employees who work in your company on a regular basis and generally have an ID card for the access system.

Use the **External company employees** menu item to manage the employees of the external companies who work in your company on a regular basis.

Use the **External companies** menu item to manage companies with the key contact details.

4.2.1 External company employees

External company employees are persons who work for external companies and are regularly present in your company.

For each person with access permission, you have to create an employee record in your system. This is the basis of the employee records transferred to the terminal peripherals, enabling performing the access validations during a booking.

The same applies to the external company employees. Therefore, you must create each external company employee in the system. The external company employees form their own number range.

Delete external company employees

External company employees can be deleted regardless of data housekeeping limits. Dependent data is also deleted, where possible.

The access booking is neutralised by removing the link to the deleted external company employee. This prevents the adulteration of access information at access points even after an external company employee has been deleted. In this way, the access booking is retained without a reference.

"Selection External company employees" dialog

The **Selection External company employees** dialog displays all external company employees created.

Note: If the **Several ID cards per person** option is active, an individual record for the external company employee is displayed in the table for every ID card issued.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Selection External company employee

Last name ID card number Ignore date of joining
 First name ID card label Ignore date of leaving
 External company

Start search

<input type="checkbox"/>	Last name	First name	External company	ID card number	ID card label	Blocked	Delete
<input type="checkbox"/>	Schilling	Wolfgang	ACME	19001	ACME 19001	<input type="checkbox"/>	
<input type="checkbox"/>	Schmitz	Peter	ACME	19002	ACME 19002	<input type="checkbox"/>	

Number of records: 2

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit External company employee" dialog

Use the **Edit External company employee** dialog to create new external company employees and edit existing external company employees. Each external company employee requires a unique employee number and at least the name.

Note: The tabs in this dialog may contain different fields depending on how the system is integrated in your company.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Edit External company employee

Last name ID card number

First name ID card label

External company

Dialog header

Last name input field:

Contains the last name of the person. This field is mandatory.

First name input field:

Contains the first name of the person.

Company selection field:

Contains the company to which the person belongs.

ID card number input field:

Contains the ID card number, which clearly identifies the ID card across the company.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Encode and print ID card button:

If a PC reader is configured as an ID card creation system, the ID card can be encoded directly using this button. You can encode and print the ID cards simultaneously using a MAGiCARD printer.

ID card label input field:

Contains the label visible on the ID card. This can be any text or a printed or handwritten number.

Note: The ID card administration options are only available when using simplified ID card administration (ID card administration level 1).

Access

The **Access** tab contains the person's general access data and displays the bookings that have been made.

Attendance display field:

Contains the current attendance status of the person.

Possible status values:

- Unknown: The attendance status of the person cannot be determined as no access bookings are available to set the attendance status.
- Present: The person is listed in the system as present.
- Absent: The person is listed in the system as absent.

Enter in blocked list button:

Blocks the external company employee with the reason for blocking "Blocked list" and creates a corresponding blocked list candidate. If a blocked list candidate of the same name already exists, a query will be displayed. You can decide whether to create the blocked list entry based on the existing entry (block based on number) or to generate a new blocked list candidate entry (block based on new blocked list entry).

Note: You require the appropriate user role rights to be able to make or cancel block list entries.

Reason for blocking selection field:

Contains the reason for blocking a blocked person. Select a reason for blocking if the person is not authorised to perform access bookings but is not to be deleted from the system. You can remove the reason for blocking at any time.

VBI permission selection field:

Contains the VBI permission with the permitted bookings on the terminal.

Options:

- All VBI permissions created in the system.

Default: No selection.

PIN code input field:

Contains the PIN code that the person has to use as authentication on a reader with a keypad in addition to the ID card. Enter the relevant PIN code.

Value range for the PIN code: 1–999999.

If no value is specified for the PIN code, the PIN code is not requested for this person provided that the terminal configuration is set to request the PIN code according to the employee record settings.

Note: If the terminal is configured for PIN code input always, persons for whom no PIN code is specified cannot make a successful access booking.

Counting group selection field:

Contains the counting group for the generation of counting values for person groups.

Options:

- All counting groups created in the system.

Default: No selection.

Tables:

Note: The ID card administration table is only available when using ID card administration level 1.

ID cards:

This table displays the ID cards allocated to the person.

ID card number column:

Contains the encoded ID card number, which clearly identifies the ID card across the company.

ID card label column:

Contains the printed label of the ID card, if available.

ID card type column:

Contains the ID card type. The ID card type specifies the medium from which a reader or terminal reads or determines the ID card number.

Bookings:

This table displays the access bookings of a person on a daily basis.

Date display: Displays the date of the access log. Click the left arrow to move the date back by one day. Click the right arrow to move the date forward by one day. You can also enter a date or click the calendar icon and select a date.

Time column:

Contains the time of a booking on the selected date.

Booking type column:

Contains the type of the booking, such as access, office release and so on.

Door number column:

Contains the unique number of the door where the booking took place.

Door column:

Contains the name for the door where the booking took place in the respective language.

Reader number column:

Contains the unique number of the reader where the booking took place.

Reader column:

Contains the name for the reader where the booking took place in the respective language.

Permissions

Use the **Permissions** tab to create the various access permissions for the person. As an additional option to general access permissions, special permissions enable you to define advanced access rights that will only apply for a certain period, for example.

Note: The **Permissions** tab is not available if ID card administration is set to type 3 in the system parameters. In this case, access permissions are issued with the ID cards.

The screenshot shows a configuration form with the following elements:

- Access calendar:** A dropdown menu with a right-pointing arrow.
- Access valid from:** A date input field with a calendar icon.
- Access valid until:** A date input field with a calendar icon.
- Offline employee record:** A checkbox.
- Office release:** A dropdown menu with a right-pointing arrow, currently set to "No doors".
- Priority settings:** A dropdown menu with a right-pointing arrow.
- AoC tracking:** A checkbox.
- TMS door release:** A dropdown menu, currently set to "Short-term door release".
- TMS alert resetting:** A checkbox.
- TMS special function 3:** A checkbox.
- Permissions:** A section with three sub-sections:
 - Access profiles:** A button labeled "New access profile permission".
 - Special permissions:** Two buttons labeled "New room zone permission" and "New door/reader permission".
 - No access via locking plan!:** A dropdown menu.

Access valid from date field:

Contains the date from when the ID card access permission is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit in the past if the field is empty.

Access valid until date field:

Contains the date until when the access permission of the ID card is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit and is valid indefinitely if the field is empty.

Access calendar selection field:

Contains the calendar for the access control.

Bürofreigabe selection field:

Enables the person to activate an office release. Please make a selection for the office release

Values:

- No doors - the person is not allowed to activate an office release.
- All doors - the person is allowed to activate the office release for all doors for which the person has access permission, provided the door supports the function.
- Selection - enables an individual allocation of the doors for which the person is allowed to activate the office release. The **Office release** table is displayed next to the selection field.

Office release table:

Use this table to enable office release on doors for which the person has access permission.

Doors with XS/evolo offline components can be released individually; online doors can only be released collectively ("All online doors" selection).

Door - reader column:

Contains the door with number and name as well as the reader with number and name.

Offline employee record checkbox:

Indicates an employee record which acts as an "emergency employee record" to enable online door opening if a terminal fails. When online fittings are initialised or put into operation, this employee record is loaded in the fitting.

AoC tracking checkbox:

Indicates that a booking log record is always created for this employee record, even if this is suppressed by the door daily time.

Note: You have access to the following three fields only if the **TMS connection** option is active. Special function 1, special function 2 and special function 3 can be equipped in TMS Software with different commands or logic links. Please note: Only special function 3 can be activated in addition to a TMS function.

TMS door release selection field:

Contains the selection for the door release of a TMS-secured door.

Values:

- Short – The door may be briefly unlocked
- Long – The door can be unlocked for an extended period
- Permanent – The door can be unlocked without time restriction
- Short long permanent – The door can be unlocked for a short or long time or permanently
- Special function 1 – the door's special function 1 may be used
- Special function 2 – The door's special function 2 may be used

TMS alert resetting checkbox:

Enables a person to acknowledge an alarm. Deselect the checkbox if you want to prevent the person from acknowledging an alarm.

TMS special function 3 checkbox:

Enables a person to initiate TMS special function 3. Deselect the checkbox if you want to prevent the person from using the TMS special function 3.

Permissions:**Display current only** checkbox:

Restricts the selection of the individual permissions displayed to the current values. Select the checkbox if you do not want to display any individual permission already expired. Deselect the checkbox to display all the individual permissions created.

Access profiles table:

Use this table to display and edit additional access profiles.

Access profile column:

Contains the number and the name of the access profile.

Valid from column:

Displays the validity start date of the access profile.

Valid until column:

Displays the validity end date of the access profile.

Special permissions:**Room zones** table:

Use this table to display and edit special permissions for room zones.

Room zone column:

Displays the room zone to which the special permission applies.

Access weekly profile: column:

Displays the access weekly profile to which the room zone applies.

Valid from column:

Displays the validity start date of the special permission for the room zone.

Valid until column:

Displays the validity end date of the special permission for the room zone.

Door/reader table:

Use this table to display and edit special permissions for doors/readers.

Door (Reader) column:

Displays the door/reader to which the individual permission applies.

Access weekly profile: column:

Displays the access weekly profile that applies for the door/reader.

Valid from column:

Displays the validity start date of the special permission for the door/reader.

Valid until column:

Displays the validity end date of the special permission for the door/reader.

Access via locking plan:**Locking plan** selection field:

Contains the options for the locking plan with the permissions displayed in the subsequent table.

Locking plan table:

Depending on the selected locking plan, the table displays all doors that can be given permissions using the selected locking plans. The table can also be used to edit the permissions. For locking plans with single time profiles, the permission is activated via a checkbox; for individual access, the corresponding access weekly profile has to be selected.

Locking plan number column:

Contains the number for the locking plan.

Name column:

Contains the name for the locking plan.

Door number column:

Contains the number for the door of the locking plan.

Name column:

Contains the name for the door of the locking plan.

Permission column:

Contains the permission from the locking plan depending on the setting as a checkbox for **single time profiles** or as a selection field for the access weekly profile for **individual** access.

AoC

The **AoC** tab contains the settings of the person for participating in AoC (Access on Card). The table displays the AoC data for the selected date. In addition to the blanket interval, the access spectrum for special intervals is shown with the access permissions.

Note: The **AoC** tab is only available if the AoC function is activated in the system parameters and ID card administration level 1 or 2 is activated.

If ID card administration level 3 is active, this tab is part of the ID card administration.

AoC validity period Day(s) Standard: 1 Day(s) [Disable AoC data calculation](#)

AoC data for   

Blanket interval of 00:00 - 00:00 Special intervals

Reader	Access	valid at
<input type="checkbox"/>	<input type="checkbox"/>	

AoC validity period input field:

Determines the length of time for which the data on the AoC ID card is valid. The AoC data is usually calculated for one day and written on the ID card.

AoC data for date field:

Here the date is selected for which the AoC data are displayed. Both future and past dates can be selected. Enter a date or click the calendar icon and select a date.

Blanket interval:

Blanket interval of display field:

Displays the calculated blanket interval for the date selected.

Blanket interval table:**Reader** column:

Displays the reader to which the blanket interval applies.

Special intervals:**Special intervals** table:

Displays the calculated special intervals for the selected date. If the AoC validity is longer than 1 day, the output starts with the selected date.

Reader column:

Displays the reader to which the special interval applies.

Access column:

Displays the start and end of the special interval.

Valid on column:

Display of the data to which the special interval applies.

Employee details

The **Employee details** tab contains official contact data and additional information on the person's company affiliation and role. All fields on this tab are optional; you do not have to enter any data.

Place of employment	<input type="text" value="Bonn"/>	Function	<input type="text" value="Berater"/>
Phone	<input type="text"/>	Identifier	<input type="text" value="FFM00102"/>
Mobile phone	<input type="text"/>		
E-mail	<input type="text" value="Schillingw@acmedemo.com"/>		

Place of employment input field:

Contains the place of employment to which the person is allocated, such a subsidiary or branch office.

Phone input field:

Contains the business phone number of the person.

Mobile phone input field:

Contains the business mobile phone number of the person.

E-mail input field:

Contains the business e-mail address of the person.

Day of joining date field:

Contains the date from when the person joined the company. Enter a date or click the calendar icon and select a date.

Function input field:

Contains the function of the person within the company.

Identifier input field:

For specifying additional attributes, such as the company car LPN.

Comment input field:

Free text field for specifying additional comments.

Other

The **Other** tab contains two input fields for additional comments and information.

Comments

Additional information

"Selection ID cards" dialog

Use the **Selection ID cards** dialog to search for ID cards that have not yet been allocated and transfer them directly to the invoking dialog.

Note: When selecting ID cards as replacement ID cards, only ID cards of the same ID card type as the ID card to which the replacement ID card is to be allocated will be considered. This applies also to combi ID cards if they have an ID string with the same ID card type.

Selection ID cards

ID card number	ID card label	ID card user
7001	7001	Employee
7002	7002	Employee
7003	7003	Employee

Number of records: 3

Click an entry to directly apply the corresponding record.

"Selection forms" dialog

Use the **Selection Forms** dialog to select the forms to be printed out.

Note: The selection dialog is not displayed if only one form is present and if the form does not require a signature.

Selection Forms

<input type="checkbox"/>	Number	Name	Short name
<input type="checkbox"/>	1	Visit - info	
<input type="checkbox"/>	8	ID card handover (with signature pad)	Sign

Number of records: 2

All existing forms are displayed in the table. Highlight a form and start printing by pressing the **Print selection** button.

Sign button:

This opens the form in a popup dialog. It can be read and signed in this dialog. The forms are subsequently saved in MATRIX or can be output as PDFs or as hardcopies using a printer.

Note: This button is only present if a form requires a digital signature. A device providing a touchscreen or signature pad must be connected in order to use this function.

4.2.2 External companies

External companies are companies such as service providers and suppliers whose employees visit your company regularly or for longer periods.

The company data is entered into dormakaba MATRIX along with the most important details and central contacts and allocated to every external company employee.

"Selection External companies" dialog

The **Selection External companies** dialog displays all external companies created in the system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Company number ▲	Company name	Company short name	Delete
<input type="checkbox"/>	1	ACME	acme	

Number of records: 1

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit External company" dialog

Use the **Edit External company** dialog to create new external companies and edit existing external companies. Each external company requires a unique number. It is recommended that you specify a company name and a company short name.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Company number:

Company name: Data group 1:

Company short name:

Town/ Postcode:

Street/Number:

Telephone number:

Fax:

E-mail:

Contact Name:

Contact First name:

Comments:

Company number input field:

Contains the unique number of the company. When you create a new record, the number increases

automatically by an increment of one. However, you can also enter your own number using between 1 and 4 digits (1-9999).

Company name input field:

Contains the name of the company. When you enter a new name, you can enter any combination of figures and letters. This field is language-dependent.

Company short name input field:

Contains a short name for the company. When you enter a new short name, you can enter any combination of figures and letters. This field is language-dependent.

Town/Postcode input field:

Contains the postcode and the location of the company.

Number or Name/Street input field:

Contains the street and street number of the company.

Phone input field:

Contains the central telephone number of the company.

Fax input field:

Contains the central fax number of the company.

E-mail input field:

Contains the central e-mail address of the company.

Contact person:

Contains details on the contact person of the company.

Last name input field:

Contains the last name of the contact.

First name input field:

Contains the first name of the contact.

Comments input field:

Free text field for additional details regarding the company.

4.3 Visitor administration

Use the **Visitor administration** menu to manage visitor records and visitor reservations.

Visitor administration is a Mobile Access function component. This means that visitors can be granted access via smartphone by stating their Mobile Access device number.

 see also: [▶ Work with visitor administration](#); [▶ Set up visitor administration with QR codes](#)

Use the **Visits overview** to access the current visits. You can activate and end visits here.

Use the **Visitor reservations** menu item to register planned visits.

Use the **Visitors** menu item to record person-related visitor data.

4.3.1 Overview of visits

All registered visits for the current day are shown in the Visit overview along with their status.

Visits can be activated, interrupted or terminated. Unannounced visits can also be set up directly, if required.

Note: When a visit is activated, the average number of visits per month is checked distributed over the last six months. This is because the number of possible visits depends on the licence.

"Visitor overview" dialog

The **Visitor overview** dialog displays all visits for the current day and allows them to be activated and ended. Visits can also be interrupted.

A red and white QR code in the toolbar indicates that Visitor administration with QR code is activated. If the QR code in the toolbar is grey, this function is inactivated.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

This dialog allows you to search using the name, ID card or company and also provides further filter options.

Hide terminated visits checkbox:

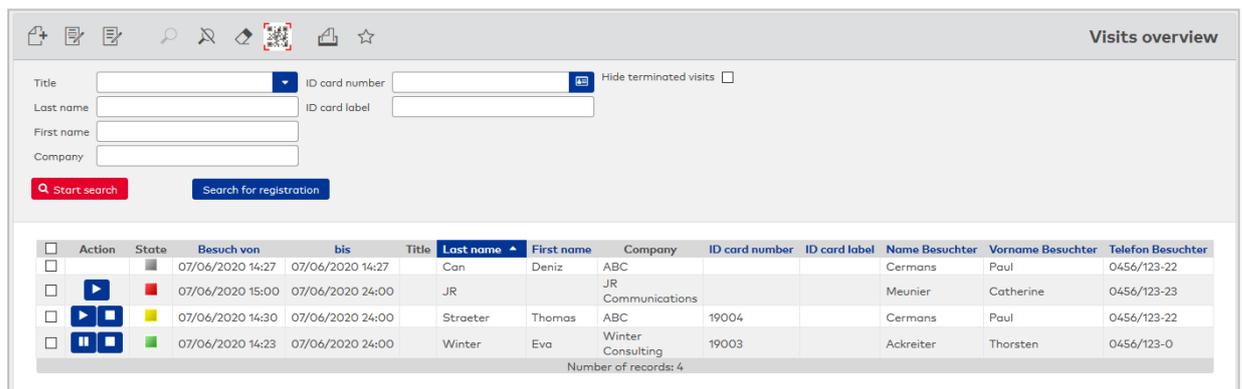
When activated, visits that have already been ended are no longer displayed.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Search for registration button:

In contrast to the **Start search** button, which only searches records from the current day, this search also takes past visits into account. A visit from the past, future or the current day is displayed for each visitor and person visited pair.



The screenshot shows the 'Visits overview' dialog with search filters and a table of visits. The search filters include Title, Last name, First name, Company, ID card number, and ID card label. There are buttons for 'Start search' and 'Search for registration', and a checkbox for 'Hide terminated visits'. The table below shows the results of the search.

Action	State	Besuch von	bis	Title	Last name	First name	Company	ID card number	ID card label	Name Besucher	Vorname Besucher	Telefon Besucher
	■	07/06/2020 14:27	07/06/2020 14:27		Can	Deniz	ABC			Cermans	Paul	0456/123-22
	■	07/06/2020 15:00	07/06/2020 24:00		JR		JR Communications			Meunier	Catherine	0456/123-23
	■	07/06/2020 14:30	07/06/2020 24:00		Straeter	Thomas	ABC	19004		Cermans	Paul	0456/123-22
	■	07/06/2020 14:23	07/06/2020 24:00		Winter	Eva	Winter Consulting	19003		Ackreiter	Thorsten	0456/123-0

Number of records: 4

Table:

The table displays visits from the current day that correspond to the search parameters entered.

Action column:

You can activate, interrupt or end the visit in this column depending on the current status of the visit.

State column:

Contains the current state of the visit.

Possible display:

■	Visit is reserved
■	Visit is pre-activated
■	Visit is active
■	Visit is interrupted
■	Visit is finished

Title column:

Contains title of the visitor.

Last name column:

Contains the last name of the visitor.

First name column:

Contains the visitor's first name.

Company column:

Contains the company where the visitor is employed.

ID card number column:

Contains the ID card number if the visitor has been issued an ID card.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Name Person visited column:

Contains the name of the person visited.

First name Person visited display field:

Contains the first name of the person visited.

Phone column:

Contains the phone number of the person visited.

Visit from column:

Contains the time and date the visit starts.

Visit until column:

Contains the time and date the visit ends.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit visit" dialog

Use the **Edit Visit** dialog to activate visits, create new visits and edit or delete existing visits.

Only the end time can be changed for visits that have already been activated.

Only the ID card number can be edited for visits that have been interrupted.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Edit Visit

Visitors

Visitor Winter, Eva (Winter Consulting) ▼ 🔍

Title ▼

Last name Winter

First name Eva

Company Winter Consulting

Mobile Access device number phone#+15369652687

Additional visitor details

Phone E-mail

Person visited

Person visited 5 - Hochmeyer, Gertrud ▼ 🔍 Department 2 - Production ▼

Employee number 5 Function

Last name Hochmeyer Phone 0456/123-20

First name Gertrud

Visit

Active

ID card number 19006 🔍

ID card label

Visit from 01/14/2021 📅 Time

until 📅 Time

Access profile ▼ ➤

Purpose

Comment

Header:

Contains information on the visitor.

Selection field for the visitor.

The visitor is shown in the display fields once selected or applied.

Note: Use the magnifier  to open the selection dialog for visitors to select the visitor or, if necessary, change the visitor.

Title display field:

Contains the visitor's title if available.

Name display field:

Contains the visitor's last name.

First name display field:

Contains the visitor's first name.

Company display field:

Contains the company where the visitor is employed.

Additional visitor information

Phone input field:

Free text for the visitor's phone number.

E-mail input field:

Free text for the visitor's e-mail address.

Person visited**Person** selection field:

Once selected or applied, the person is shown in the display fields.

Note: Use the magnifier  to open the selection dialog for Persons. This allows you to change the person visited if necessary.

Employee number display field:

Contains the employee number of the person visited.

Name display field:

Contains the name of the person visited.

First name display field:

Contains the first name of the person visited.

Department display field:

Contains the department of the person visited.

Function display field:

Contains the role of the person visited.

Phone display field:

Contains the phone number of the person visited.

Visit

Note: The displayed fields depend on the selected ID card administration level. Access permissions are conferred via the access profile in ID card administration level 1 and 2. In ID card administration level 3, access permissions are conferred via the visitor ID access permissions.

Active checkbox:

Sets the visit status to active.

ID card number input field:

Contains the allocated visitor ID card if ID card assignment is activated for visitor administration.

Note: You can allocate ID card numbers freely in ID card administration level 1 and 2. Pre-authorized ID cards are used for ID card administration level 3.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

ID card label column:

Contains the printed label on the company ID card/access ID card (such as 123), if available.

Visit from date field:

Contains the time and date the visit starts.

Visit until date field:

Contains the time and date the visit ends.

Access profile selection field:

Contains the access profile with the access permissions.

Note: The selection field is only present for ID card administration levels 1 and 2.

Options:

- All access profiles approved for visitor administration.

Purpose input field:

Information on the purpose of the visit.

Comment input field:

Free text field for additional details on the visit.

"Selection Visitor" dialog

Use the **Selection Visitor** dialog to search for visitors and directly apply them to the invoking dialog; if required, you can also create new visitors.

Select one or more entries and click **Apply selected search results** in the toolbar.

<input type="checkbox"/>	Title	Last name	First name	Company	Delete
<input type="checkbox"/>		Can	Deniz	ABC	
<input type="checkbox"/>		Winter	Eva	Winter Consulting	

Number of records: 2

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.

Last name	First name	Department	Employee number	ID card number	ID card label	Blocked
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

"Selection ID cards" dialog

Use the **Selection ID cards** dialog to search for ID cards that have not yet been allocated and transfer them directly to the invoking dialog.

Note: When selecting ID cards as replacement ID cards, only ID cards of the same ID card type as the ID card to which the replacement ID card is to be allocated will be considered. This applies also to combi ID cards if they have an ID string with the same ID card type.



ID card number	ID card label	ID card user
7001	7001	Employee
7002	7002	Employee
7003	7003	Employee

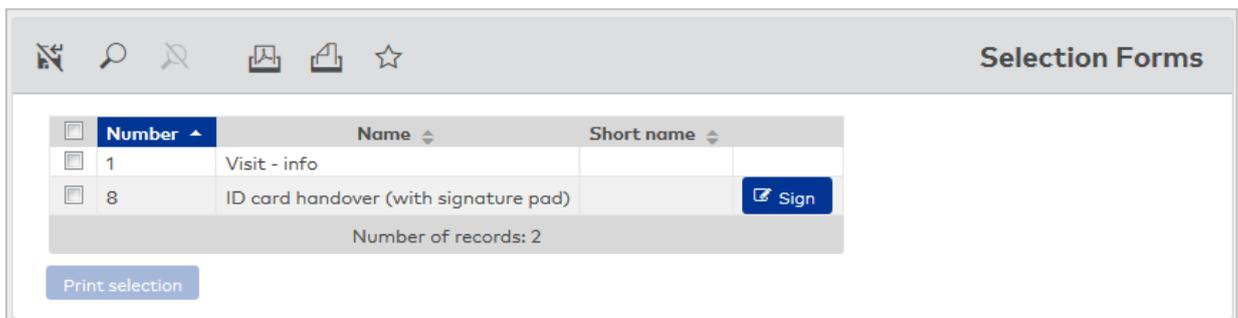
Number of records: 3

Click an entry to directly apply the corresponding record.

"Selection forms" dialog

Use the **Selection Forms** dialog to select the forms to be printed out.

Note: The selection dialog is not displayed if only one form is present and if the form does not require a signature.



Number	Name	Short name
1	Visit - info	
8	ID card handover (with signature pad)	

Number of records: 2

Print selection

All existing forms are displayed in the table. Highlight a form and start printing by pressing the **Print selection** button.

Sign button:

This opens the form in a popup dialog. It can be read and signed in this dialog. The forms are subsequently saved in MATRIX or can be output as PDFs or as hardcopies using a printer.

Note: This button is only present if a form requires a digital signature. A device providing a touchscreen or signature pad must be connected in order to use this function.

4.3.2 Visitor reservations

Every company employee can make reservations for visitors with the relevant permission. In reception areas, visitor reservations are provided in the visitor overview dialog and provide support when processing visitors.

For recurring visitors, you can use visitor reservations that have already been created as a template for a new visit. In general, it is then sufficient to enter only the dates of the current visit.

The globally created visitor reservations that are visible to the individual users in the Self Service area depend on the organisational unit. Rights are granted in user administration.

"Selection visitor reservation" dialog

The **Selection Visitor reservations** dialog displays all visitor reservations created along with their state.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Selection Visitor reservations

Title

Last name

First name Visit from until

Company

Start search

<input type="checkbox"/>	State	Title	Last name	First name	Company	Visit from	until	Purpose	Name of visited person	First name of visited person	Delete
<input type="checkbox"/>			Bob	Bob							
<input type="checkbox"/>			Winter	Eva							

Number of records: 2

Visitor reservations table:

The visitor reservation table contains all active visitor reservations and all ended visitor reservations.

New column:

Click the **New** icon in the table row to use a visitor reservation as a template for a further reservation. This function is independent of the visitor status.

State column:

Contains the current state of the visit.

Possible display:

	Visit is reserved
	Visit is pre-activated
	Visit is active
	Visit is interrupted
	Visit is finished

"Edit visitor reservation" dialog

Use the **Edit visitor reservation** dialog to create new visitor reservations and edit or delete existing visitor reservations.

Use the buttons in the toolbar to navigate between records, create, copy and delete a record, and save or discard changes to the record. Use the **Back to selection** button to return to the selection dialog.

Edit Visitor reservation

Visitors

Visitor: Winter, Eva (Winter Consulting)

Title:

Last name: Winter

First name: Eva

Company: Winter Consulting

Mobile Access device number: phone#+0125893546

Additional visitor details

Phone: E-mail:

Person visited

Person visited: 5 - Hochmeyer, Gertrud

Visit

Visit from: 06/24/2020 09:00 Time

until: 06/24/2020 18:00 Time

Purpose:

Comment:

Licence plate number: HH-W100

LPN access profile: 63 - Car park

Visitors

This area contains information on the visitor.

Visitor selection field:

Selection field for the visitor. The visitor's contact data is shown in the display fields once selected or applied.

Note: Use the magnifier  to open the selection dialog for visitors to select the visitor or, if necessary, change the visitor. You can use the central toolbar to create a new visitor and then apply if the visitor has not yet been created in the system.

New advance reservation for this visitor button.

This button creates a new visitor reservation for the displayed visitor.

As a general rule, the only further information required is the details on the time of the visit.

Note: Unlike the central toolbar used to enter new entries, this button does not create any new visitors; it simply generates a new visitor reservation.

Additional visitor information

Additional details about the visitor can be entered, e.g. telephone number and e-mail address, depending on the configuration of the visitor dialog.

Person visited

This area contains information on the person visited.

Selection field:

Selection field for the person visited. The official data of the person visited is shown in the display fields once selected or applied.

Note: Use the magnifier  to open the selection dialog for persons to select or, if necessary, change the person visited.

Visit

This area contains information on the visit appointment.

Visit from column:

Contains the time and date the visit starts according to the schedule.

Visit until column:

Contains the time and date the visit ends according to the schedule.

Purpose column:

Contains the reason for the visit.

Comment input field:

Free text field for additional details on the visit.

Available fields if QR code access is activated:**QR access profile** selection field:

Used to select an access profile for pre-activation using QR codes with access function.



Button:

Pressing the button sends an e-mail containing a generated QR code to the stated e-mail address. Please note that, if an e-mail address and access profile have already been set, an e-mail is sent automatically when the visitor is saved.

Note: E-mail template 13 "Visitor access with QR code" is used.

Available fields if LPN recognition access is activated:**Licence plate number** input field:

Contains the licence plate number (LPN) of the visitor.

LPN access profile selection field:

Used to select an access profile for pre-activation using LPN recognition.

Note: Pre-activation using a QR code or LPN recognition: The system parameter Access 74 "Access validity period before visit" defines the period during which the visitor can enter the car park before the beginning of the visit appointment. During this period, the visit has the status "Pre-activated".

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.

Last name	First name	Department	Employee number	ID card number	ID card label	Blocked
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

"Selection Visitor" dialog

Use the **Selection Visitor** dialog to search for visitors and directly apply them to the invoking dialog; if required, you can also create new visitors.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

	Title	Last name	First name	Company	Delete
<input type="checkbox"/>		Can	Deniz	ABC	
<input type="checkbox"/>		Winter	Eva	Winter Consulting	

Number of records: 2

Select one or more entries and click **Apply selected search results** in the toolbar.

4.3.3 Visitors

Visitors are all external persons who are to be granted access one or more times. The person-related data of a visitor is created a single time. You can then access this data when making visitor reservations, which means you do not have to reenter the data for every following visit.

Note: Visitor files that no longer contain a reference to a reservation, a visit or a booking are automatically deleted after the data housekeeping limit has expired. The default value for this period is 60 days. If you also wish to store more infrequent visitors for retrieval, it is advisable to increase the data housekeeping limit.

"Selection Visitor" dialog

The **Selection Visitor** dialog displays all personal records created in the visitor administration.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Selection Visitors

Title ▼

Last name

First name

Company

🔍 Start search

<input type="checkbox"/>	Title	Last name ▲	First name	Company	Delete
<input type="checkbox"/>		Can	Deniz		
<input type="checkbox"/>		Winter	Eva	Winter Consulting	

Number of records: 2

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit visitor" dialog

Use the **Edit visitor** dialog to create new visitors and edit or delete existing visitors.

Every visitor created must contain at least a last name as the minimum entry.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Edit Visitors

Title ▼

Last name

First name

Company

Mobile Access device number

Additional visitor details 2

Comment Phone

E-mail

Title selection field:

Contains the visitor's title, if available.

Last name input field:

Contains the visitor's last name.

First name input field:

Contains the visitor's first name.

Company input field:

Contains the company where the visitor is employed.

Mobile Access device number input field:

Enter the smartphone telephone number using the Mobile Access function.

The prefix requires "phone#+" for Mobile Access device numbers. Example: phone#+49123456789

Note: This is a mandatory field if Mobile Access (system parameter access 150) and ID administration level 1 (system parameter basis 120) are activated.

Create blocked list candidate button:

Creates a blocked list candidate using the entered data. If a blocked list candidate of the same name already exists, a query will be displayed. You can decide whether to create the blocked list entry based on the existing entry (block based on *number*) or to generate a new blocked list candidate entry (block based on new blocked list entry).

Additional visitor information

Different fields for additional information about the visitor can be set up, depending on the configuration for visitor dialogs.

Comment input field:

Free text field for additional comments.

Phone input field:

Contains the visitor's phone number.

E-mail input field:

Contains the visitor's e-mail address.

4.4 ID card administration

Use the ID card administration to manage all ID cards in the system.

Note: ID card administration must be activated via a system parameter. The appropriate licence is required for the activation.

With ID card management, dormakaba MATRIX allows you to keep person data maintenance and ID card management separate. This is usually the case if these tasks are carried out by different organisations. T

his separation is also related to the task of issuing access permissions. When using ID card administration, access permissions are granted in the ID card dialog and not in the person data dialog.

Additional criteria and options for ID card administration are:

- ID card user: Identifier indicating to which organisational ID card user types the ID card can be assigned (persons, external company employees, visitors, LPN)
- ID card type: Identifies personalised and non-personalised ID cards for better handling and selection during allocation
- Replacement ID card concept with replacement ID cards and original ID cards
- Multiple ID cards for a single user using identical or different reader technologies
- Simplified handling of combi ID cards
- Reasons for blocking ID cards

Use the **ID card administration** to manage the ID cards in your system.

Use the **Priority circuits** menu item to manage the priority settings which allow you to partially or fully override access checks for selected groups of persons.

Use the **Reasons for blocking ID card** menu item is used to manage the reasons for blocking ID cards, which you can allocate to ID cards in order to block them.

4.4.1 ID cards

You can maintain your company's ID cards in this area. The ID cards created can be allocated to the ID card users in ID card administration or person administration.

In addition to access-relevant settings, the ID card contains organisational elements and control functions.

For organisational purposes, ID cards can not only be assigned to the various ID card user types, such as employees, visitors and external company employees, they can also be linked to vehicle number plates.

Extensive options are available for the individual issuance of access permissions and special access permissions of the ID cards.

An original ID card can only be allocated to one ID card user. Replacement ID cards are allocated to an original ID card. An original ID card cannot be issued as replacement ID card. Access permissions can only be issued for original ID cards. Replacement ID cards inherit access permissions from the allocated original ID card.

Information on encoding ID cards can be found in the section "Working with Matrix", under the heading .

"Selection ID cards" dialog

The **Selection ID cards** dialog displays all ID cards created. If the ID card is allocated to a person, it is also displayed along with the name and employee number.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

The ID card search function provides numerous filtering options. If a PC reader is configured, you can also use the **Apply ID card number** button to scan the ID card directly.

Selection ID cards

ID card number	<input type="text"/>	Employee number	<input type="text"/>	<input checked="" type="checkbox"/> Allocated ID cards	<input checked="" type="checkbox"/> Free ID cards
ID card label	<input type="text"/>	Last name	<input type="text"/>	<input checked="" type="checkbox"/> Personalised ID cards	<input checked="" type="checkbox"/> ID cards not personalised
ID card user	<input type="text"/>	First name	<input type="text"/>	<input checked="" type="checkbox"/> Original ID cards	<input checked="" type="checkbox"/> Replacement ID cards
		End of validity period	on <input type="text"/>	<input checked="" type="checkbox"/> ID cards not blocked	<input checked="" type="checkbox"/> Blocked ID cards

Start search

	ID card number	ID card label	ID card user	Access valid until	Personalised	Replacement ID card	Blocked	Person	Employee number	Delete
<input type="checkbox"/>	8201	201	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Hochmeyer, Gertrud	5	
<input type="checkbox"/>	8202	202	Employee		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Legrand, Marc	6	
<input type="checkbox"/>	8203	203	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cermans, Paul	7	
<input type="checkbox"/>	8204	204	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Meunier, Catherine	8	
<input type="checkbox"/>	8205	205	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Kamp, Karsten	9	
<input type="checkbox"/>	8206	206	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Leconte, Sandra	10	
<input type="checkbox"/>	9001	001	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Ackreiter, Thorsten	1	
<input type="checkbox"/>	9002	002	Employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Martin, Eric	2	
<input type="checkbox"/>	9011	011	Employee		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Leroy, Fabienne	4	
<input type="checkbox"/>	19001	ACME 19001	External company employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Schilling, Wolfgang	102	
<input type="checkbox"/>	19002	ACME 19002	External company employee		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Schmitz, Peter	101	
<input type="checkbox"/>	50010	Besucher 010	Visitor		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	789789789	Besucher 112	Visitor		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			
<input type="checkbox"/>	6917529063640863760	HH-W100	LPN	06/24/2020 18:00:00	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Winter, Eva	1	
<input type="checkbox"/>	6917531131597362323	EN-DK-123	LPN		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Kamp, Karsten	9	

Number of records: 15

Note: You cannot delete an ID card if it still contains history entries. This is normally the case if the ID card is still allocated to a person or bookings still exist in the system for the ID card. The same applies to replacement ID cards if they are still allocated to an ID card.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit ID cards" dialog

Use the **Edit ID cards** dialog to create new ID cards and edit existing ID cards. Each ID card requires a unique ID card number. This is normally the internal identification number of the ID card.

If you have one, PC reader you can read the ID card number with the help of the PC readers.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Note: You cannot delete an ID card if it still contains history entries. This is normally the case if the ID card is still allocated to a person or bookings still exist in the system for the ID card. The same applies to replacement ID cards if they are still allocated to an ID card.

ID card number display field:

Contains the internal identification number of the ID card. This field can only be edited when creating a new ID card.

Apply ID card number button:

If a PC reader is configured, you can also use the button to scan the ID card number directly.

Encode and print ID card button:

If a PC reader is configured as an ID card creation system, the ID card can be encoded directly using this button. You can encode and print the ID cards simultaneously using a MAGiCARD printer.

ID card label input field:

Contains the label visible on the ID card. This can be any text or a printed or handwritten number.

Replacement ID card checkbox:

Identifier indicating whether this is a replacement ID card. A replacement ID card can only be allocated to another ID card. It cannot be allocated to a person. Access permissions can only be issued for original ID cards. Replacement ID cards inherit the access permissions from the respective original ID card.

Employee number input field:

Contains the unique employee number. To allocate an ID card to a person, enter the employee number or click the **Search** button to select a person.

Note: If the ID card is assigned to a person, the last name and first name of the person are shown below the employee number. Click the names to open the **Edit persons** dialog.

In addition to the general information for the ID card, the access permissions are also linked to the ID card.

General

The **General** tab contains the general information on the ID card.

Settings	Replacement ID card allocation
ID card type <input type="text"/>	Replacement ID card <input type="text"/>
ID card version <input type="text"/>	<input type="button" value="Find"/>
ID card user <input type="text" value="1 - Employee"/>	ID card label <input type="text"/>
Licence plate number <input type="text"/>	Valid from <input type="text"/>
Personalised <input type="checkbox"/>	until <input type="text"/>
ID card blocking reason <input type="text"/>	
Mobile Access device number <input type="text"/>	

Settings

ID card type selection field:

Contains the ID card type of the ID card which essentially determines the reading technology and the evaluation of the internal ID string.

ID card version input field:

Contains the version of the ID card. The ID card does not have an ID card version if the field is empty.

ID card user selection field:

Contains the organisational ID card user types.

Options: Employee, visitor, external company employee, LPN

Licence plate number input field:

This field is only present if LPN recognition devices are used in the system. The field is active and is a mandatory field if the value "LPN" has been selected in the **ID card user** field.

Note: When saving a new LPN ID card, the ID card number is calculated on the basis of the licence plate number and entered automatically. If the field **ID card label** is empty, the licence plate number is also entered in this field automatically.

Personalised checkbox:

Identifier indicating whether the ID card is personalised. Personalised ID cards normally contain the imprint of the ID card user name and a photo.

Reason for blocking ID card selection field:

Contains the reason for blocking an ID card. This ID card can no longer be used for booking if a reason for blocking has been set. There is no reason for blocking if the field is empty.

Reason for blocking person display field:

Contains the reason for blocking a person if the ID card has been allocated to a person who is blocked by a reason for blocking. A reason for blocking a person also applies to all ID cards allocated to the person. The reason for blocking the person cannot be cancelled or modified in ID card administration. This can only be done in person administration. No reason for blocking the allocated person exists if the field is empty or the ID card is not allocated to any person.

Mobile Access device number input field:

Enter the smartphone telephone number using the Mobile Access function. The value "Mobile Access" must be selected in the **ID card type** field.

The prefix "phone#" is automatically added to the telephone number, e.g. "phone#+4917256889755".

Note: This option is only available if the Mobile Access function is enabled (system parameter 150).

Replacement ID cards

Replacement ID card input field:

Contains the ID card number of an allocated replacement ID card. No replacement ID card is allocated to the ID card if the field is empty. Enter the ID card number of the replacement ID card or click the magnifier  to open the **Selection Replacement ID card** dialog to search for and load replacement ID cards.

ID card label display field:

Contains the ID card label of the allocated replacement ID card.

Valid from date field:

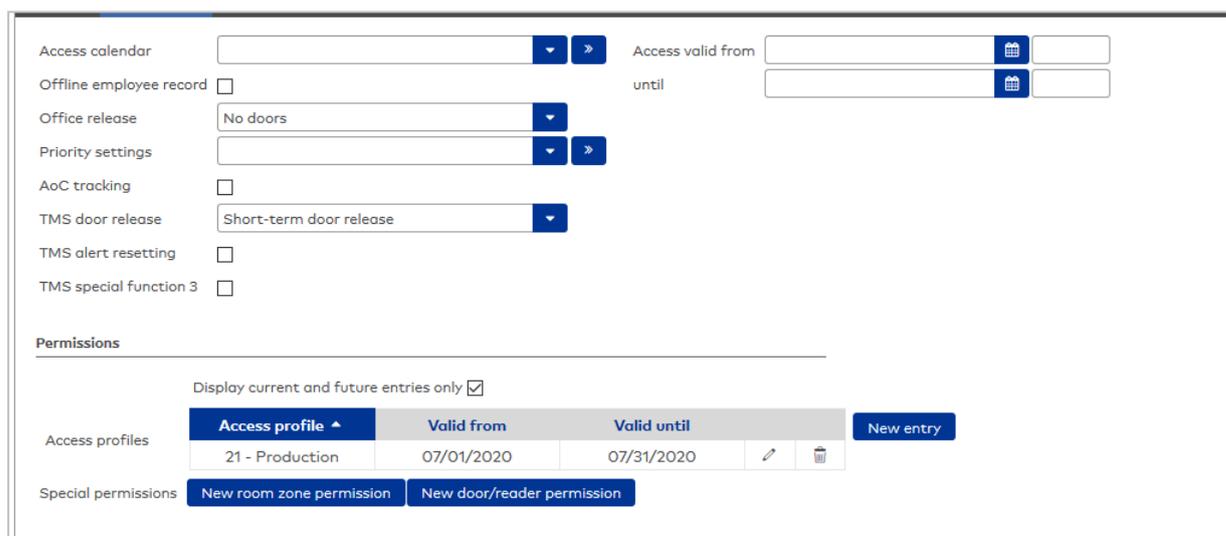
Contains the date from which the replacement ID card has been allocated. Enter a date or click the calendar icon and select a date. The replacement ID card has no limit in the past if the field is empty.

Until date field:

Contains the date until which the replacement ID card is granted access. Enter a date or click the calendar icon and select a date. The replacement ID card has no limit and is valid indefinitely if the field is empty.

Permissions

Use the **Permissions** tab to create the various access permissions for the person.



Access calendar   Access valid from  until 

Offline employee record

Office release 

Priority settings  

AoC tracking

TMS door release 

TMS alert resetting

TMS special function 3

Permissions

Display current and future entries only

Access profile	Valid from	Valid until		
21 - Production	07/01/2020	07/31/2020		

Special permissions

Access valid from date field:

Contains the date from when the ID card access permission is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit in the past if the field is empty.

Access valid until date field:

Contains the date until when the access permission of the ID card is valid. Enter a date or click the calendar icon and select a date. The ID card has no limit and is valid indefinitely if the field is empty.

Access calendar selection field:

Contains the access calendar for access control.

Offline employee record checkbox:

Indicates an employee record which acts as an "emergency employee record" to enable online door opening if a terminal fails. When online fittings are initialised or put into operation, this employee record is loaded in the fitting.

Bürofreigabe selection field:

Enables the person to activate an office release. Please make a selection for the office release

The following types are available for selection:

- No doors; the person is not allowed to activate an office release.
- All doors; the person is allowed to activate office release for all doors for which the person has access permission, provided the door supports the function.
- Selection; for the individual allocation of the doors where the person is allowed to activate the office release. In this selection, the table for the allocation of the doors for the office release is displayed next to the selection field.

Office release table:

Use this table to enable office release on doors for which a person has access permission.

While doors with XS/evolo offline components can be enabled individually, there is only the 'All online doors' selection for online doors.

Door - reader column:

Contains the door with number and name as well as the reader with number and name.

AoC tracking checkbox:

Indicates that a booking log record is always created for this employee record, even if this is suppressed by the access daily time.

Note: You have access to the following three fields only if the **TMS connection** option is active. Special function 1, special function 2 and special function 3 can be equipped in TMS Software with different commands or logic links. Please note: Only special function 3 can be activated in addition to a TMS function.

TMS door release selection field:

Contains the selection for the door release of a TMS-secured door.

Values:

- Short – The door may be briefly unlocked
- Long – The door can be unlocked for an extended period
- Permanent – The door can be unlocked without time restriction
- Short long permanent – The door can be unlocked for a short or long time or permanently
- Special function 1 – The door's special function 1 may be used
- Special function 2 – The door's special function 2 may be used

TMS alert resetting checkbox:

Enables a person to acknowledge an alarm. Deselect the checkbox if you want to prevent the person from acknowledging an alarm.

TMS special function 3 checkbox:

Enables a person to initiate TMS special function 3. Deselect the checkbox if you want to prevent the person from using the TMS special function 3.

Permissions**Display current only** checkbox:

Restricts the selection of the individual permissions displayed to the current values. Select the checkbox if you do not want to display any individual permission already expired. Deselect the checkbox to display all the individual permissions created.

Access profiles table:

Use this table to display and edit additional access tables.

Access profile column:

Contains the number and the name of the access profile.

Valid from column:

Displays the validity start date of the access profile.

Valid until column:

Displays the validity end date of the access profile.

Special permissions:**Room zones** table:

Use this table to display and edit special permissions for room zones. When a room zone permission is transferred, a check is performed to establish whether further related room zones have been defined for the room zone. Further related room zones are entered automatically.

Room zone column:

Displays the room zone to which the special permission applies.

Access weekly profile: column:

Displays the access weekly profile to which the room zone applies.

Valid from column:

Displays the validity start date of the special permission for the room zone.

Valid until column:

Displays the validity end date of the special permission for the room zone.

Door/reader table:

Use this table to display and edit special permissions for doors/readers.

Door (Reader) column:

Displays the door/reader to which the individual permission applies.

Access weekly profile: column:

Displays the access weekly profile which applies to the door (the reader).

Valid from column:

Displays the validity start date from when the special permission for the door (the reader) is valid.

Valid until column:

Displays the validity end date of the special permission for the door (the reader).

AoC

The **AoC** tab contains the ID card settings for participating in AoC (Access on Card). The table displays the AoC data for the selected date. In addition to the blanket interval, the access spectrum for special intervals is shown with the access permissions.

AoC validity period Day(s) Standard: 1 Day(s) [Activate AoC data calculation](#)

AoC validity period input field:

Determines the length of time for which the data on the AoC ID card is valid. Usually the AoC data are calculated for one day and written on the ID card.

Activate AoC data calculation button:

Click this button to activate the calculation of the AoC data. The AoC data is shown in the tables below.

AoC validity period Day(s) Standard: 1 Day(s) [Disable AoC data calculation](#)

AoC data for   

Blanket interval of 00:00 - 00:00 Special intervals

Reader	Access	valid at

AoC data for date selection:

Here the date is selected for which the AoC data are displayed. Both future and past dates can be selected. Enter a date or click the calendar icon and select a date.

Blanket interval**Blanket interval of** display field:

Displays the calculated blanket interval for the date selected.

Blanket interval table:**Reader** column:

Displays the reader to which the blanket interval applies.

Special intervals**Special intervals** table:

Displays the calculated special intervals for the selected date. If the AoC validity is longer than 1 day, the output starts with the selected date.

Reader column:

Displays the reader to which the special interval applies.

Access column:

Displays the start and end of the special interval.

Valid on column:

Display of the data to which the special interval applies.

Create ID card

When the ID card creation system interface is activated, the **Create ID card** tab also appears in the dialog. Based on an ID card creation system running in the background, it is possible to personalise ID cards directly from ID card administration.

Note: To use the ID card creation system interface, it must be possible to access the path /matrix-
<versionnumber>/I without logging in.

Last name	<input type="text" value="Leroy"/>	 <input type="button" value="Create image with ID card"/> <input type="button" value="No connection"/>
First name	<input type="text" value="Fabienne"/>	
Company	<input type="text"/>	
Print layout	<input type="text" value="Employee ID card"/>	
Last created on	<input type="text"/>	
State	<input type="text" value="Not yet created"/>	
<p>??BAS_BADGEPROD_LBL_badgePreview??</p> 		

Print layout selection field:

Select the print layout for creating the ID card.

Options:

- All print layouts created in the system.

Last created on selection field:

Shows the date and time of the last ID card creation.

State display field:

Contains the status in relation to the ID card creation.

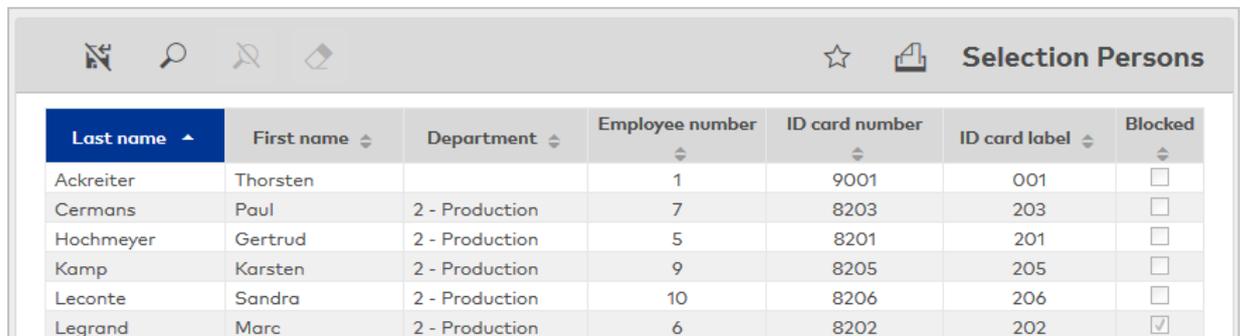
No connection display area:

If there is no connection to the IDCardConnector, this is shown in the display area of the dialog.

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.



Last name	First name	Department	Employee number	ID card number	ID card label	Blocked
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

"Selection ID cards" dialog

Use the **Selection ID cards** dialog to search for ID cards that have not yet been allocated and transfer them directly to the invoking dialog.

Note: When selecting ID cards as replacement ID cards, only ID cards of the same ID card type as the ID card to which the replacement ID card is to be allocated will be considered. This applies also to combi ID cards if they have an ID string with the same ID card type.



ID card number	ID card label	ID card user
7001	7001	Employee
7002	7002	Employee
7003	7003	Employee

Number of records: 3

Click an entry to directly apply the corresponding record.

4.4.2 Priority circuits

Priority settings can be used to override various checks for a booking.

This means that a positive access booking can be enabled for specific persons even when access is not possible due to, for example, a door daily time.

Note on counting information: Persons who are granted access via the priority circuit are included in the counting information.

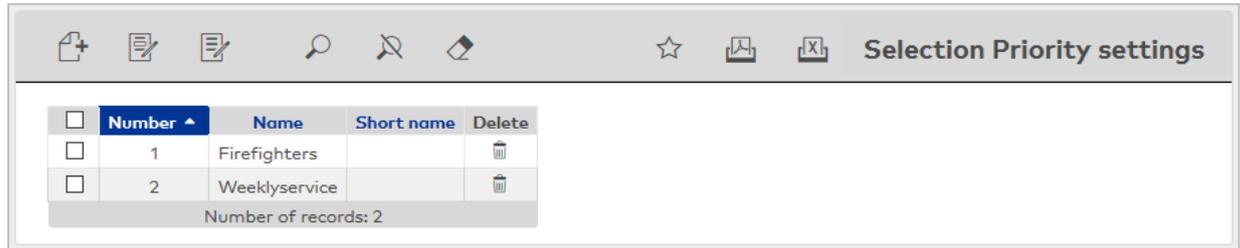
Note: Priority settings are part of the person administration if ID card administration level 1 or 2 is activated.

If ID card administration level 3 is enabled, the priority settings are part of the ID card administration.

"Selection priority settings" dialog

The **Selection Priority settings** dialog displays all priority settings created in the access system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit priority settings" dialog

In the **Edit Priority settings** dialog, you can create new priority settings and edit existing priority settings. Each priority setting requires a unique number. It is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number:

Name:

Short name:

No access restriction through a door program
 No PIN code check
 No repeated access lock check
 No hard anti-passback
 No area-to-area movement control
 No check of number of persons
 No attendance control for two persons
 No access control for two persons
 No monitoring of duration of stay
 No check for activated IDS

No access restriction through a door program checkbox:

Indicates whether the door daily time's checks are to be performed. Switching off the check makes a positive access booking possible even during time ranges or under conditions when the door program's check would prevent this.

Options:

- Activated: for an access booking, door programs are not taken into account by the check.
- Not activated: door programs are included in the access check.

Default value: Not activated

No PIN code check checkbox:

Indicates whether the PIN code check is to be switched off. If the check is switched off, entry of a PIN code is not necessary.

Options:

- Activated: no PIN code check is performed.
- Not activated: a PIN code check is performed if this is required by other configuration settings.

Default value: Not activated

No attendance control checkbox:

Indicates whether attendance control is to be switched off. Switching off the check makes a positive access booking possible even if the person is not listed as present in the specified area.

Options:

- Activated: access control is not checked.
- Not activated: access control is checked.

Default value: Not activated

No timed anti-passback checkbox:

Indicates whether the timed anti-passback is to be switched off. Switching off the check makes a positive access booking possible even if the person makes a booking within the time frame for the timed anti-passback.

Options:

- Activated: the timed anti-passback is not checked.
- Not activated: the timed anti-passback is checked.

Default value: Not activated

No hard anti-passback checkbox:

Indicates whether the hard anti-passback is to be switched off. Switching off the check makes a positive access booking possible even if the person is still listed as present in the area to which they would like to gain access.

Options:

- Activated: the hard anti-passback is not checked.
- Not activated: the hard anti-passback is checked.

Default value: Not activated

No area-to-area movement control checkbox:

Indicates whether the area-to-area movement control is to be switched off. Switching off the check makes a positive access booking possible even if the person is not listed as present in the specified area.

Options:

- Activated: area-to-area movement control is not checked.
- Not activated: area-to-area movement control is checked.

Default value: Not activated

No access control for two persons checkbox:

Indicates whether the access control for two persons is to be switched off. Switching off the check makes a positive access booking possible for one person even if two bookings are stipulated.

Options:

- Activated: the access control for two persons is not checked.
- Not activated: the access control for two persons is checked.

Default value: Not activated

No attendance control for two persons checkbox:

Indicates whether the attendance control for two persons is to be switched off. Switching off the check makes a positive access booking possible for one person even if no second person is booked as present in the area.

Options:

- Activated: the attendance control for two persons is not checked.
- Not activated: the attendance control for two persons is checked.

Default value: Not activated

No monitoring of duration of stay checkbox:

Indicates whether the monitoring of duration of stay is to be switched off. Switching off the check makes a positive access booking possible for one person even if the duration of stay has been exceeded and/or the

blocking time for a booking has not yet expired.

Options:

- Activated: monitoring of duration of stay is not checked.
- Not activated: monitoring of duration of stay is checked.

Default value: Not activated

No check for armed IDS checkbox:

Indicates whether the check for armed IDS is switched off. Switching off the check makes a positive access booking possible for one person even if the IDS is armed.

Options:

- Activated: armed IDS are not checked.
- Deactivated: armed IDS are checked.

Default value: Not activated

4.4.3 Reasons for blocking ID card

In this area you can maintain the reasons for blocking ID cards. They can then be allocated to the ID cards in ID card administration. This procedure allows ID cards to be simply blocked or cleared without losing the ID card master data. A reason for blocking an ID card does not simultaneously also apply to the person to whom the ID card is allocated.

Creating reasons for blocking ID cards is optional. However, it is recommended for larger corporate structures since this allows, for example, to search for blocked ID cards.

"Selection reasons for blocking ID card" dialog

The **Selection Reasons for blocking ID card** dialog displays all created reasons for blocking ID cards.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number	Name	Short name	Relevant for AoC back lists	Delete
<input type="checkbox"/>	1	Blocked list	B	<input checked="" type="checkbox"/>	
<input type="checkbox"/>	2	Return	R	<input type="checkbox"/>	

Number of records: 2

Relevant for AoC black lists column:

Contains the identifier indicating whether the reason for blocking is relevant to the AoC black lists.

Note: This column is only available if the AoC function is activated in the system parameters.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit reasons for blocking ID cards" dialog

Use the **Edit Reasons for blocking ID cards** dialog to create new blocking reasons for ID cards and edit existing blocking reasons.

Reasons for blocking are allocated to ID cards if the ID cards may no longer be used for booking. You can determine, depending on the reason for blocking, whether blocking shall affect the AoC black list.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

The screenshot shows a dialog box titled "Edit Reasons for blocking ID cards". At the top is a toolbar with icons for adding, saving, deleting, undo, and printing. Below the toolbar are four input fields: "Number" (value: 1), "Name" (value: Blocked list), "Short name" (value: B), and "Relevant for AoC black list" (checkbox checked).

Relevant for AoC black list checkbox:

Identifier indicating that the reason for blocking affects the AoC black list. Activate the checkbox if a blocked ID card with the reason for blocking shall be included in the AoC black list.

Note: The checkbox is only available if the AoC function is activated in the system parameters.

If you block an ID card with a reason for blocking relevant to AoC black list, blocking only becomes effective after a synchronisation with the AoC readers.

4.5 Room administration

Use the **Room administration** menu to manage rooms and the associated reservations.

Use the **Reservations** menu item to display an overview of the existing reservations. You can create new reservations or edit or delete existing reservations.

Use the **Rooms** menu item to manage the rooms of your company.

4.5.1 Reservations

Reservations can be used to plan room occupancies on a specified date. Further participants can be entered for every reservation. Participants are then automatically granted access permission to the reserved room on the specified date.

All authorised persons can make reservations independently in the self-service area.

In addition, room management in the Access menu can be used to grant selected persons access permission to all reservations. This allows reservations of persons to be changed or deleted by third parties in special cases, such as sickness or absence of persons.

"Selection Reservations" dialog

The **Selection Reservations** dialog displays all existing reservations for rooms for each day along with the date, time and responsible person.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Date	From time	Until time	Room	Person	Department	Phone
Jun 12, 2017	19:00	24:00	Seminar room	Hochmeyer, Gertrud	Sales	0456/123-20
Jun 13, 2017	10:00	24:00	Seminar room	Hochmeyer, Gertrud	Sales	0456/123-20

Number of records: 2

"Edit Reservation" dialog

Use the **Edit Reservations** dialog to create new room reservations and edit existing reservations.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Room selection field:

Selection of the room to be reserved.

Reserved from date field:

Contains the date when the reservation starts. Enter a date or click the calendar icon and select a date.

Time input field:

Contains the time when the reservation starts. Enter the appropriate time.

Reserved until date field:

Contains the date when the reservation ends. Enter a date or click the calendar icon and select a date. The field may remain empty for one-day reservations. The date is then automatically adopted from the **Reserved from** field.

Time input field:

Contains the time when the reservation ends. Enter the appropriate time. If you do not specify a time, it is set to 23:59.

Reserved by:

Contains the person who has reserved the room. When creating a new reservation the registered person is entered here. The person reserving can be changed if required.

Note: Use the magnifier  to open the selection dialog for Persons.

Employee number display field:

Contains the employee number of the person making the reservation.

Name display field:

Contains the last name of the person making the reservation.

First name display field:

Contains the first name of the person making the reservation.

Department display field:

Contains the department of the person making the reservation.

Phone display field:

Contains the phone number of the person making the reservation.

Participants table:

The table contains the participants to whom the necessary access rights are assigned during the reservation.

Note: Use the magnifier  to open the selection dialog for Persons.

Person column:

Contains the last name and the first name of the invited person.

Department column:

Contains the department of the invited person.

Phone column:

Contains the phone number of the invited person.

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.

Note: Persons who have left the company are not included in this selection.

Last name ▲	First name ⇅	Department ⇅	Employee number ⇅	ID card number ⇅	ID card label ⇅	Blocked ⇅
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

4.5.2 Rooms

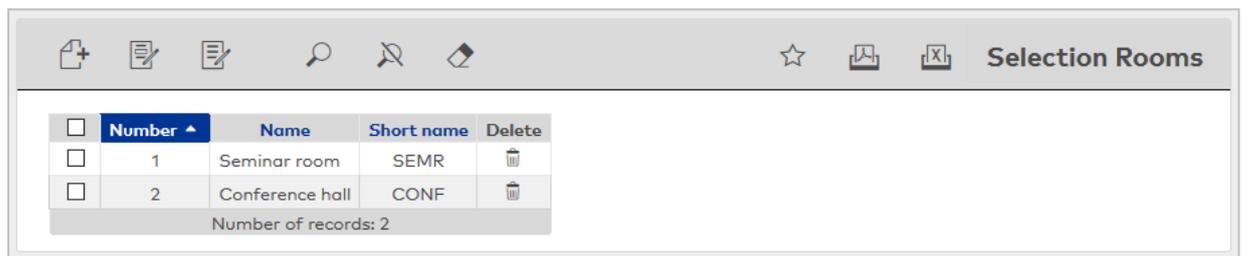
Rooms are a prerequisite for the room administration. A room is a physically enclosed area that consists of one or more access points with allocated readers.

The room reservation requires the relevant access permissions for the time period of a reservation. By defining a room, it is precisely specified which doors and thus which readers have to be authorised for access.

"Selection Rooms" dialog

The **Selection Rooms** dialog displays all rooms created.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



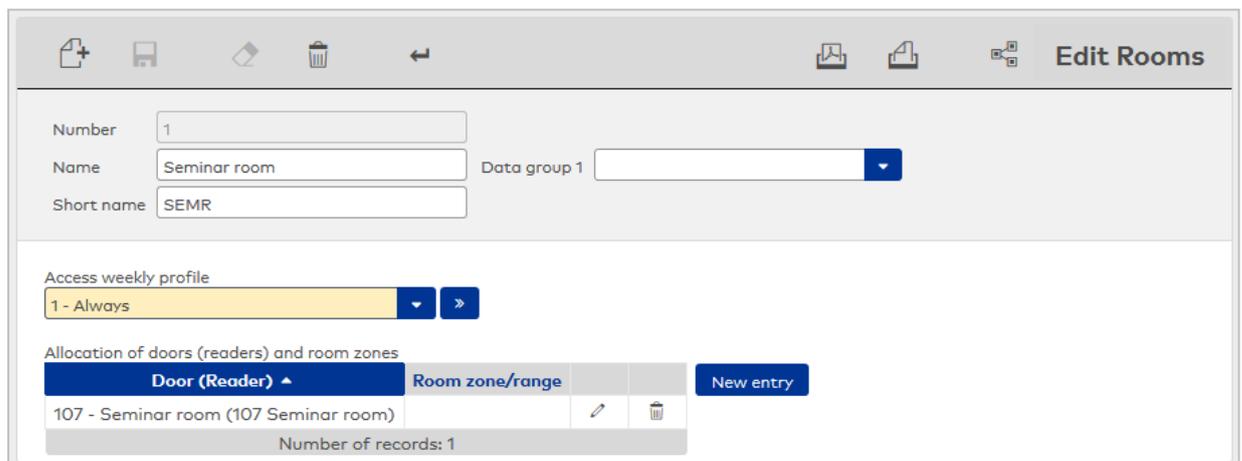
Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Rooms" dialog

Use the **Edit Rooms** dialog to create new rooms and edit or delete existing rooms. Each room requires a unique number; it is recommended that you specify a name and a short name.

Room are physically delimited areas. When you assign such areas a name, you should base the names on your company's local or organisational structure.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Access weekly profile selection field:

Contains the access weekly profile which is required for assigning access permissions during the reservation.

Allocation of doors and room zones table: Specify a door or a room zone.

Door (reader) selection field:

Select the door of the room.

Room zone/range selection field:

Select the room zone to which the room belongs.

4.6 Area/door administration

Use the **Area/door administration** menu to manage all security areas, room zones, doors and the required door control master data.

Note: Depending on the options activated, this menu item may be displayed as Area/Door administration, Room zone/door administration or Door administration.

Door daily times form the basis for timed door control. In these time plans, the time intervals for door target statuses are defined to the minute. The calendar specifics are defined via substitute door programs.

Use the **Security areas – doors** or **Room zones – Doors** menu item to define the security areas, room zones and doors.

Use the **Counting groups** menu item to define the person groups for which counting information is recorded in the security areas.

Use the **Door weekly profiles** menu item to determine which door daily time is used for each individual day of a week.

Use the **Door daily times** menu item to manage the controller time intervals for every door.

4.6.1 "Security areas - Doors" dialog - Security area

Note: Depending on the options activated, the menu item may also be displayed as Room zone/door administration or Door administration.

All local and room components in the access system are displayed in a tree structure to conform to the hierarchical structures. The tree structure can also be adapted to organisational conditions or other factors using folders.

The local and room elements include:

- Folders: support the mapping of the organisational and local conditions.
- Security areas: are the top-level organisational units of the room zones. Each room zone can only be allocated to one security area.
Access control functions such as hard anti-passback or timed anti-passback are associated with the security areas. Moreover, security areas offer counting functions and advanced access functions, such as two-person attendance control or attendance control based on minimum and maximum values, which are drawn from counting values.

Note: Security areas are only available when the security areas option is activated. When security areas are activated, access functions no longer apply to the room zones, since they become an integrated part of the security area.

- Room zones: each room zone is based on a system of several doors.
A room zone is a physically enclosed area that consists of one or more access points with assigned readers. Access functions can be associated with a room zone; their properties are defined using access

parameters.

Note: Room zones are only available if the room zones option is activated in the system parameters.

- Doors: Basic doors, usually with a reader for access control.
- Cabinet doors: Doors that are used in connection with the device type "Cabinet lock". Cabinet doors can also be allocated to room zones if no advanced room zone functions are configured. They can also be used in access profiles and locking plans.
- Connecting doors: Doors that connect two room zones.
- Emergency exit doors: Doors that are managed by a TMS control room.

Note: Emergency exit doors are only available with an appropriate licence; additionally, the TMS option must be activated in the system parameters.

- Monitoring doors: Doors without readers that can only be monitored and for which no access permission can be granted.
- Readers: Various parameters for door control and door monitoring such as door release pulse length or alarm are defined via the readers.

"Security areas - doors" dialog

Use the **Security areas - Doors** dialog to create all local and room elements of the access system and to edit or delete existing elements.

Note: Depending on the options activated, the dialog may also be displayed as Security areas - Doors, Room zones - doors or Doors.

All elements in the access system are displayed in a tree structure to conform to a hierarchical structure. The tree structure can also be adapted to organisational conditions or other factors using folders.

Each element requires a unique number; it is recommended that you specify a name and a short name.

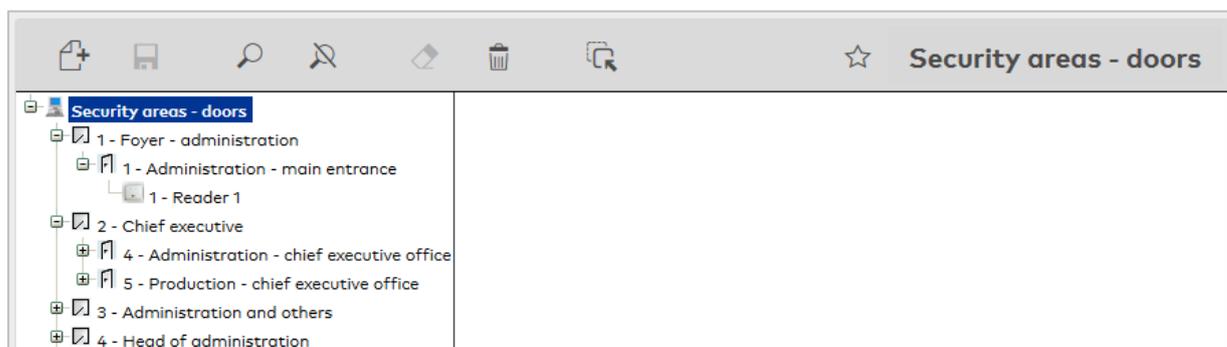
Use the search function to search for individual elements or a group of elements by number, name, short name and item type.

Note: In addition to the elements that can be displayed and edited in the tree, you can also search for readers. When searching for readers, the edit dialog opens for the door to which the reader is allocated.

Click the plus sign in front of a node to expand this part of the structure tree.

Click an element in the tree to open the associated edit dialog with the element definitions. This appears in the right-hand section of the window, where it can be edited.

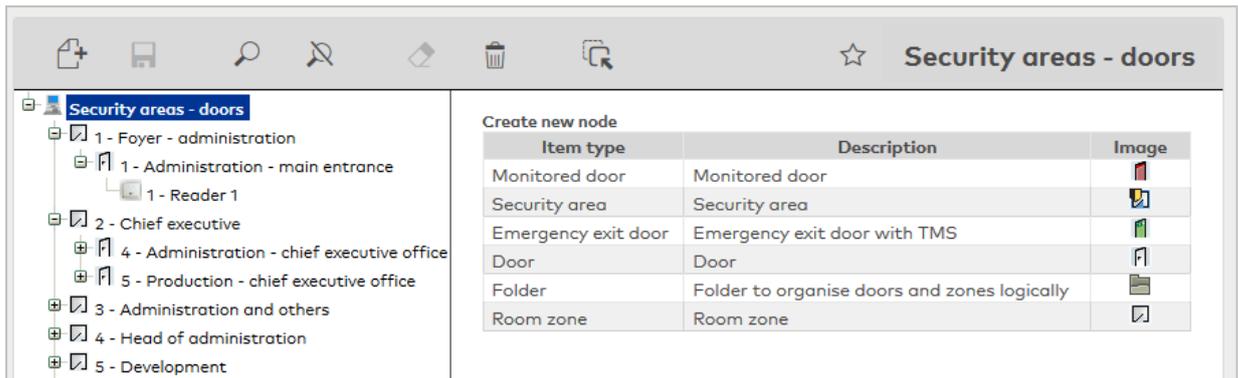
Note: The various item types such as security areas, room zones and doors each have their own number ranges.



For a description of the elements with their specific properties see the relevant components.

Create new node

Click **Create new record** in the toolbar to open the **Create new node** dialog. Click an element to insert it at the activated position in the tree.



Item type column:

Displays the element.

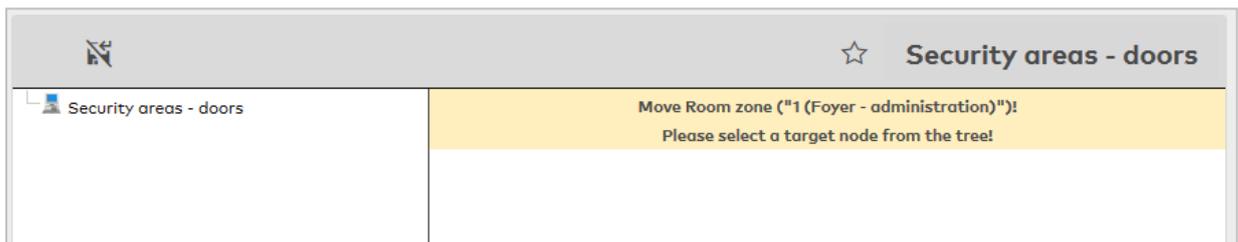
Description column:

Contains the name for the element.

Illustration column:

Contains an image of the element.

Move elements



Now click the element or the node in the tree into which you want to move the element. The tree only displays possible destinations for the copy process at this time.

The dialog description for the elements provides more information about the specific parameters.

"Security areas - doors" dialog - Emergency exit door

An emergency exit door is monitored by a TMS control room. Like any other door, the emergency exit door requires a calendar and door weekly profile for controlling the door functions.

Note: You can only set up emergency exit doors if the TMS connection option is activated and the TMS software is installed.

Number	<input type="text" value="3"/>	
Name	<input type="text"/>	
Short name	<input type="text"/>	
Emergency exit door		
TMS control room	<input type="text"/>	<input type="button" value="v"/>
Calendar	<input type="text"/>	<input type="button" value="v"/>
Door weekly profile	<input type="text"/>	<input type="button" value="v"/>

TMS control room selection field:

Contains the TMS control room which monitors and controls the door.

Options:

- All TMS control rooms set up in the system.

Calendar selection field:

Contains the calendar for the calendar specifics for door and access control.

Options:

- All calendars created in the system.

Default value: No selection.

Door weekly profile selection field:

Contains the door weekly profile for door and access control.

Options:

- All door weekly profiles created in the system.

"Security areas - Doors" dialog - Reader

The readers on a door define various specific properties for the door. The release duration and door open time can be defined, and the alarm preset for each reader.

Note: The various properties are adopted from the reader definition by the device administration, where the settings can also be changed by users with the appropriate permission.

Number	<input type="text" value="1"/>	
Name	<input type="text" value="Reader 1"/>	
Short name	<input type="text"/>	
		S6 - reader
		Data group 1 <input type="text"/>
Door release pulse length (DRP)	<input type="text" value="5"/>	Seconds
Door open time (DOT)	<input type="text"/>	Seconds
Alarm duration	<input type="text"/>	Seconds
Alarm delay time	<input type="text"/>	Seconds
Door monitoring alarm type	Default <input type="button" value="v"/>	
Pre-alarm duration	<input type="text"/>	Seconds
Pre-alarm type	Main alarm following pre-alarm (<input type="button" value="v"/>)	
Booking cancellation	<input checked="" type="checkbox"/>	

Number display field:

Contains the unique number for the reader.

Name display field:

Contains the name for the reader.

Short name display field:

Contains a short name for the reader.

Door release pulse length (DRP) input field:

Contains the duration of the door release pulse for the door opening in seconds. If the value = 0, the door relay is not activated even if the access check is positive.

Value range: 0-999

Default value: 3 seconds

Note: The door release pulse length must be at least 3 seconds for XS components.

Door open time (DOT) input field:

Contains the time that the door can be open in seconds before an alarm is triggered. An alarm is triggered when this time is exceeded. When door open time = 0, the door status contact is not monitored.

Value range: 0-999

Default value: 0 seconds (no door open time monitoring)

Alarm duration input field:

Contains the alarm duration in seconds.

Value range: 0-999

Default value: 0 seconds, no alarm duration.

Alarm delay time input field:

Contains the alarm delay in seconds. The alarm is triggered when this time is exceeded.

Value range: 0-999

Default value: 0 seconds, no alarm delay.

Door monitoring alarm type selection field:

Selection of the alarm at the door if the door open time is exceeded. The door monitoring alarm type determines whether a pre-alarm is triggered when the door open time (DOT) is exceeded and how long the alarm output is activated in case of forced entry or the DOT being exceeded.

Options:

- Standard. Alarm output activated if door opening time is exceeded, door is forced entry or an invalid door opening code is entered
- Main alarm depending on alarm duration
- Main alarm until door closed
- No alarm activation
- Pre-alarm until DOT The pre-alarm is ended by closing the door. Booking, pressing the door key switch, entering the door opener code or permanent door opening when door open time monitoring or the pre-alarm is running does not reset DOT monitoring or the pre-alarm.
- Main alarm according to alarm duration or until door closing
- Pre-alarm for DOT with resetting the DOT in case of door action The pre-alarm is ended by closing the door. Re-releasing the door by booking, pressing the door key switch, entering the door opener code or permanent door opening when door open time monitoring or the pre-alarm is running resets DOT monitoring or the pre-alarm and restarts DOT monitoring. No further door opening, opening time or pre-alarm activation messages are subsequently generated.

Default value: Default

Pre-alarm duration input field:

Contains the pre-alarm duration in seconds. If the reason the alarm removed during the pre-alarm, the pre-alarm is ended and the alarm is not triggered.

Value range: 0-99

Default value: 0 seconds (no pre-alarm)

Pre-alarm type display field:

Selection of the pre-alarm type for pre-alarm behaviour in relation to the main alarm.

Options:

- Main alarm following pre-alarm (according to alarm duration)
- Main alarm after pre-alarm (until door closed)
- Main alarm after pre-alarm (according to alarm duration/door closing)
- Main alarm after forced entry (according to alarm duration)
- Main alarm after forced entry (until door closed)
- Main alarm after forced entry (according to alarm duration/door closed)

Default value: Main alarm following pre-alarm (according to alarm duration)

Booking cancellation checkbox:

Indicates whether a successful access booking is cancelled if a door is not opened. In the event of a cancellation, the internal employee record fields "Last access time", "Actual room zone" and "Actual security area" are reset in the terminal to the values prior to the access booking and the counting information is also corrected. The terminals are also automatically notified of the cancellation by update packets.

Options:

- Not activated: No cancellation is triggered.
- Activated: A booking cancellation is implemented.

Default value: Activated.

"Security areas - Doors" dialog - Room zone

Room zones are physically delimited areas. When you assign such areas a name, you should base the names on your company's local or organisational structure.

Room zones are used for the assignment of access permissions. The access permission for a room zone automatically contains the access permissions for all doors that are allocated to the room zone.

The screenshot shows the configuration interface for a room zone. At the top, there are input fields for 'Number' (3), 'Name' (Administration and others), and 'Short name' (AdmAndCo). To the right is a 'Room zone' icon. Below this is a section for 'AoC special interval' with a checkbox and a table of 'Approving persons' (Cermans, Paul (cermans)) with edit and delete icons, and a 'New entry' button. The bottom section is divided into two panes: 'Available room zones' and 'Allocated room zones'. The 'Available room zones' pane lists: 1 - Foyer - administration, 2 - Chief executive, 4 - Head of administration, 5 - Development, 6 - Server room, 7 - Production, 8 - Head of production, and 9 - Material stores. The 'Allocated room zones' pane is currently empty. Navigation arrows are placed between the two panes.

Note: The access functions of timed anti-passback, hard anti-passback and anti-passback room control are only available for the room zones if no security areas are activated in the system. If the 'Security areas' option is activated, the access functions are part of the security areas.

Input field Timed anti-passback:

Contains the time in minutes an ID card is locked for repeated access to the room zone. If the ID card is subsequently used to access a different room zone, the timed anti-passback for this room zone is

removed.

Value range:

0 = the timed anti-passback is inactivated.

1-99 = timed anti-passback in minutes

Default value: 0

Note: If an individual value is entered into a subordinate reader, this overrides the global room zone setting.

Hard anti-passback checkbox:

Creates a block that prevents multiple access to the room zone by a person. Select the checkbox to determine that persons can only enter the room zone if they have previously left this room zone, that is, were registered as present in a different room zone.

Options:

- Activated: The hard anti-passback is activated.
- Not activated: The hard anti-passback is inactivated.

Default value: 0

Anti-passback room control checkbox:

Permits extended access control. Select the checkbox if persons may only enter the room zone, if they were previously registered as present in the neighbouring room zone.

Options:

- Activated: Anti-passback room control is activated.
- Not activated: Anti-passback room control is inactivated.

Default value: 0

Note: This function of the anti-passback room control is only ensured if all doors of the room zones are equipped with entry and exit readers.

AoC special interval checkbox:

Select this checkbox to save the permissions for the doors/readers in this room zone in AoC as special intervals on the ID card.

Special intervals correspond exactly to the access intervals from the access daily times applied to the ID card through its access permissions.

The blanket interval is used for permissions if the checkbox is not activated. The blanket access range is determined by using the earliest start pointing from all access intervals of the access daily times as the starting point and accordingly the latest end point from all access intervals of the access daily times as the end point. The calculation is made individually for each ID card based on the assigned access permissions.

Options:

- Activated: The AoC permissions are written as special intervals.
- Not activated: The blanket interval is used.

Default value: Not activated.

Note: The **AoC special interval** checkbox is only available if the AoC function is activated in the system parameters.

Approving person table:

The table contains the approving person for the access permissions.

Note: The button is only available when the option workflow administration is activated.

Approving person column:

Contains the approving person's first and last name for the approval of access requests for this room zone.

Further related room zones area:

Further related room zones make operation easier when assigning access permissions, for example if other room zones need to be crossed first to reach a particular room zone.

Note: This area is only visible if system parameter **93 Further related room zones** is activated.

Available room zones report:

Contains all room zones that can be allocated to the current room zone.

Allocated counting groups report:

Contains all further related room zones allocated to the current room zone.

"Security areas – Doors" dialog – Security area – Cabinet door

Only one reader can be allocated to each cabinet door (cabinet lock). The cabinet lock does not support TimePro functions (Day/Night and Office).

The screenshot shows a configuration dialog for a cabinet door. It has the following elements:

- Number:** Input field containing '3'.
- Name:** Input field containing 'Cabinet 24'.
- Short name:** Empty input field.
- Cabinet door icon:** A simple icon of a door with two handles.
- Cabinet lock number:** Input field containing '24'.
- AoC special interval:** A checkbox that is currently unchecked.
- Reader table:**

Reader		
26 - Cabinet Lock 24		
- New entry:** A blue button to add a new reader.

Locker lock number input field:

Enter a unique locker lock number when using cabinet doors in Free Selection Mode. This field is only available if the option **Free Selection Mode** is selected as the evolvo terminal class on the **Cabinet lock** tab. Value range: 0–999999999

AoC special interval checkbox:

Select this checkbox to save the permissions for the doors/readers in AoC as special intervals on the ID card.

Special intervals correspond exactly to the access intervals from the access daily times applied to the ID card through its access permissions.

The blanket interval is used for permissions if the checkbox is not activated. The blanket access range is determined by taking the earliest start point from all access intervals of the access daily times as the start point and accordingly the latest end point from all access intervals of the access daily times as the end point. The calculation is made individually for each ID card based on the assigned access permissions.

Note: The **AoC special interval** checkbox is only available if the AoC function is activated in the system parameters.

Table:

Reader column:

Contains the allocated cabinet lock.

Calendar column:

Contains the calendar allocated to the cabinet door.

"Security areas - Doors" dialog - Security area

Security areas are usually based on room zones and are therefore physically delimited areas. When you assign such areas a name, you should base the names on your company's local or organisational structure.

Security areas offer more extensive access functions and counting functions than room zones.

The functions are divided between the **General** and **Counting information** tabs.

"General" tab

This tab contains the general information on the security area and the associated access functions.

Timed anti-passback input field:

Contains the time in minutes an ID card is blocked for repeated access to the room zones of the security area. If the ID card is subsequently used to access a different security area, the timed anti-passback for this security area is removed. Enter the time in minutes.

Value range: 0–99

Default: 0 = timed anti-passback inactivated.

Note: If an individual value is entered into a subordinate reader, this overrides the global security area setting.

Hard anti-passback checkbox:

Creates a block that prevents multiple access to the same security area by a person. If the hard anti-passback is activated, the person must leave the security area and be registered as present in another security area.

Options:

- Activated: The hard anti-passback is switched on for the security area.
- Not activated: The hard anti-passback is switched off.

Default value: Not activated.

Area-to-area movement control checkbox:

Indicates if the control of area-to-area movements is set for the security area. If the area-to-area movement control is activated, persons may only enter the security area if they are registered as present in

a neighbouring security area.

Options:

- Activated: The control of area-to-area movements is activated for the area.
- Not activated: The control of area-to-area movements is inactivated for the area.

Default value: Not activated.

Motion recording off checkbox:

Indicates if motion data for the security area is created and sent to the application.

Note: If attendance control for two persons is activated, it is not possible to specify a minimum number of persons.

Options:

- Not activated: Motion data is created and sent to the application
- Activated: Recording of motion data for the security area is switched off. In this case, the settings in the door daily time determine if motion data is generated.

Default value: Not activated.

Block on incorrect PIN code checkbox:

Indicates if access is to be blocked if an incorrect PIN code is entered several times.

Options:

- Activated: Access blocked if incorrect PIN code is entered several times.
- Not activated: No blocking.

Default value: Not activated.

Monitoring of duration of stay area:

Duration of stay monitoring determines the time a person is allowed to stay in a particular security area and the length of the blocking period until they can enter the area again.

Terminal selection field:

Contains the terminal for monitoring of duration of stay. Selecting the terminal determines the possible exits that are available in the other selection fields.

Options:

- All terminals created in the system.

Activate output selection field:

Contains the exit that is activated if the maximum duration of stay is exceeded.

Options:

- All exits controlled by the selected terminal.

For x seconds input field:

Contains the time in seconds the exit is activated.

Value range:

0 = until the person has left the security area.

1-99 seconds

Default value: 0

Maximum duration of stay input field:

Defines the maximum duration in minutes. If this time is exceeded, a message is created.

Value range: 0-1440 minutes

Default value: 0, no monitoring of duration of stay

"Counting information" tab

This tab contains the counting groups and control functions.

Counting information

Accounting according to employee record

Attendance recording

Attendance control

Attendance control for two persons

Minimum number of persons

Maximum number of persons

Counting groups

Available counting groups

1 - Counting Production

Allocated counting groups

2 - Counting Administration

Counting information checkbox:

Indicates if counting information is activated for the security area.

Options:

- Activated: the counting values are displayed.
- Not activated: no counting values are displayed.

Default value: Activated

Counting information according to employee record checkbox:

Indicates whether counting information is controlled separately by the settings in the employee record.

Options:

- Activated: employee record configuration determines whether a person is included in the counting information.
- Not activated: all persons are included in the counting information.

Attendance recording checkbox:

Indicates if attendance recording is switched on for the security area. This checkbox is only available if counting information is activated.

Options:

- Activated: The attendance recording is switched on.
- Not activated: The attendance recording is not switched on.

Default value: Not activated.

Attendance recording

The following parameters define the attendance control of the security area.

Attendance control for two persons checkbox:

Indicates if attendance control for two persons is switched on for the security area.

Note: If attendance control for two persons is activated, it is not possible to specify a minimum number of persons.

Options:

- Activated: Attendance control for two persons is switched on.
- Not activated: Attendance control for two persons is not switched on.

Default value: Not activated.

Minimum number of persons input field:

Number of persons who must be in the security area. If this number is reached, exit bookings are rejected. Special case: If the minimum number of persons is 2 and the attendance control for two persons is activated for the exit reader, access control for two persons is implemented for the last two persons in the security area. It is assumed that both persons leave the security area.

Value range: 0–9999

Default value: 0 = no restriction on the minimum number of persons.

Maximum number of persons input field:

Maximum number of persons allowed in the security area. If this number is reached, access bookings are refused.

Note: Persons granted access by a priority circuit are also included in the counting information. The priority circuit only overrides the access verification checks, not the counting information.

Value range: 0–9999

Default value: 0 = no restriction on the maximum number of persons.

Counting groups

Use the report fields to allocate counting groups to the security area.

Note: The report fields are only available if the security area is not a lower-level area of another security area. Lower-level security areas cannot be allocated counting groups, even if they are themselves at the same time higher-level security areas. Lower-level security areas adopt the counting groups from the top-level security area.

Available counting groups report:

Contains all counting groups that can be allocated to the security area.

Allocated counting groups report:

Contains all counting groups that are allocated to the security area.

Control functions

Depending on the security area's specific counting information counter, this area can be used to activate an exit if a pre-set condition is fulfilled.

Control functions

Terminal ▼

Counting action if ▼ and

activate output ▼ for Seconds (0 = unlimited)

Intruder detection systems

IDS activation via counting information

IDS area

Security area weekly program ▼

Calendar ▼

Terminal selection field:

Contains the terminal for the control function. Selecting the terminal determines the selection of the possible exits.

Options:

- All terminals created in the system.

Counting action if selection field:

Defines the condition required to activate the exit.

Options:

- 0 – No action
- 1 – If the counting value 1 is reached, the specified exit is activated.
- 2 – If the counting value falls below the counting value 1, the specified exit is activated.
- 3 – If the counting value 1 is exceeded, the specified exit is activated.
- 4 – If the counting value is in a range between the counting value 1 and counting value 2, the specified exit is activated.
- 5 – If the counting value is not in a range between the counting value 1 and counting value 2, the specified exit is activated.

Default value: 0 – No action

Counting value 1 and counting value 2 input fields:

Counting values that are used to evaluate the counting action. Depending on the condition, one or two values are required.

Value range: 0–999999

Default value: 0

Activate output selection field:

Contains the exit that is activated if the pre-set condition is met.

Options:

- All exits controlled by the selected terminal.

For x seconds input field:

Contains the time in seconds the exit is activated.

Value range:

0 = for as long as the set condition is met.

1–99 seconds

Default value: 0

Intruder detection systems

Activated counting information can be used for arming the area.

IDS arming via counting information checkbox:

Indicates if the IDS is to be armed via the counting information.

Options:

- Activated: IDS arming via counting information is used.
- Not activated: IDS arming via counting information is not used.

Default value: Not activated

IDS area:

Contains the configured IDS area. If this checkbox is activated, the IDS area that is armed is determined automatically based on the reader location (the security area must match the activation area).

Security area weekly profile selection field:

If a security area weekly profile is selected, this can be used for time-dependent control of IDS arming via counting information.

Options:

- All security area weekly profiles created in the system.

Calendar selection field:

Contains the calendar to be used.

Options:

- All calendars created in the system.

"Security areas – doors" dialog – Folder

You can map your organisational and room dependencies using folders.

Folders can be placed anywhere in the tree. The only place where folders are not possible is underneath doors.

Apart from header data, no other information is required for folders.

"Security areas - Doors" dialog - Door

Each door is controlled by at least one reader and one door weekly profile. In combination with a calendar, calendar-specifics can be taken into account to ensure, for example, stricter access checks on bank holidays or even prevent access on bank holidays.

Reader	Calendar	Door weekly profile	evolo TimePro
1 - Reader 1	1 - Default	1 - Always	

AoC special interval checkbox:

Note: The **AoC special interval** checkbox is only available if the AoC function is activated in the system parameters.

Select this checkbox to save the permissions for the doors/readers in this room zone in AoC as special intervals on the ID card.

Special intervals correspond exactly to the access intervals from the access daily times applied to the ID card through its access permissions.

The blanket interval is used for permissions if the checkbox is not activated. The blanket access range is determined by using the earliest start pointing from all access intervals of the access daily times as the starting point and accordingly the latest end point from all access intervals of the access daily times as the end point. The calculation is made individually for each ID card based on the assigned access permissions.

Options:

- Activated: The AoC permissions are written as special intervals.
- Not activated: The blanket interval is used.

Default value: Not activated.

Reader table:

Contains the readers with the calendar and the door weekly profile allocated to the door.

Reader table

Contains the readers of the door.

Calendar column:

Contains the calendar allocated to the reader.

Weekly profile column:

Contains the door weekly profile allocated to the reader.

evolo TimePro column:

If an evolo reader is allocated to a door, the door weekly profile is then no longer a mandatory field.

If one of the TimePro options is selected, the weekly profile becomes a mandatory field again and serves as the basis for the release mode.

Options:

- No selection, the door weekly profile is then not a mandatory field in this case.
- Permanent release: Door permanently opened in line with the weekly profile
- Office mode: If the door is opened by a short booking using an authorised ID card, it is kept open until it is closed again by a further booking. Short-term opening is not possible.
- Office release: If the door is opened by a short booking using an authorised ID card, the door is opened only briefly. If the ID card is presented for a longer time or presented twice in quick succession, the door is opened permanently until the office release expires or until the release is ended by performing a new booking using an ID card.

Note: This column is only present if one of the evolo system parameters 17 or 18 is active.

"Security areas – doors" dialog – Monitored door

Monitoring doors are monitored in the system only to detect unauthorised opening. A virtual reader is required to determine the required door status contact.

If the monitoring door can also be opened with a door key switch, you must allocate a door daily time and a calendar to the virtual reader, otherwise the terminal refuses door opening via the door key switch.

Access permissions cannot be assigned to the door.

Reader selection field:

Contains the reader allocated to this door.

Options:

- All available readers

Note: Although the reader does not need to be physically present, it is necessary to create the reader in device administration.

Calendar selection field:

Contains the calendar applicable for this door.

Options:

- All available calendars

Door weekly profile selection field:

Contains the door weekly profile applicable for this door.

Options:

- All available door weekly profiles

"Security areas - doors" dialog - Connecting door

Connecting doors connect two room zones. A connecting door therefore requires at least two readers which are each allocated to one room zone.

Each reader is assigned a door weekly profile for time-related control of the door functions. In combination with a calendar, calendar-specifics can be taken into account to ensure, for example, stricter access checks on bank holidays or even prevent access on bank holidays.

Note: In the tree, connecting doors are displayed for both room zones. The exit room zone is also displayed after the connecting door.

Number

Name

Short name



Connecting door

AoC special interval

Enter entrance room zone

with the readers	Reader	Calendar	Door weekly profile	evolo TimePro			
	3 - Reader 3	1 - Default	10 - Administration and others		✎	🗑️	New entry

Enter exit room zone ▼ ▶

with the readers	Reader	Calendar	Door weekly profile	evolo TimePro			
	2 - Reader 2	1 - Default	20 - Production		✎	🗑️	New entry

AoC special interval checkbox:

Select this checkbox to save the permissions for the doors/readers in AoC as special intervals on the ID card.

Special intervals correspond exactly to the access intervals from the access daily times applied to the ID card through its access permissions.

The blanket interval is used for permissions if the checkbox is not activated. The blanket access range is determined by taking the earliest start point from all access intervals of the access daily times as the start point and accordingly the latest end point from all access intervals of the access daily times as the end point. The calculation is made individually for each ID card based on the assigned access permissions.

Note: The **AoC special interval** checkbox is only available if the AoC function is activated in the system parameters.

Entrance room zone

Contains the room zone for the readers of the following table. The entrance room zone is automatically defined by the position in the tree structure when the connecting door is created under a room zone.

Reader table:

Contains the readers with the allocated calendar and the door weekly profile allocated to the door. The readers are allocated to the entrance room zone.

Reader column:

Contains the readers of the door to be allocated to the entrance room zone.

Calendar column:

Contains the calendar allocated to the reader.

Weekly profile column:

Contains the door weekly profile allocated to the reader.

evolo TimePro column:

If an evolo reader is allocated to a door, the door weekly profile is then no longer a mandatory field.

If one of the TimePro options is selected, the weekly profile becomes a mandatory field again and serves as the basis for the release mode.

Options:

- No selection, the door weekly profile is then not a mandatory field in this case.
- Permanent release: Door permanently opened in line with the weekly profile
- Office mode: If the door is opened by a short booking using an authorised ID card, it is kept open until it is closed again by a further booking. Short-term opening is not possible.
- Office release: If the door is opened by a short booking using an authorised ID card, the door is opened only briefly. If the ID card is presented for a longer time or presented twice in quick succession, the door is opened permanently until the office release expires or until the release is ended by performing a new booking using an ID card.

Note: This column is only present if one of the evolo system parameters 17 or 18 is active.

Exit room zone

Contains the room zone for the readers to be allocated to the exit room zone.

Options:

- All room zones created in the system.

Reader table:

Contains the readers with the allocated calendar and the door weekly profile allocated to the door. The readers are allocated to the exit room zone.

Reader column:

Contains the readers of the door to be allocated to the exit room zone.

Calendar column:

Contains the calendar allocated to the reader.

Weekly profile column:

Contains the door weekly profile allocated to the reader.

evolo TimePro column:

If an evolo reader is allocated to a door, the door weekly profile is then no longer a mandatory field.

If one of the TimePro options is selected, the weekly profile becomes a mandatory field again and serves as the basis for the release mode.

Options:

- No selection, the door weekly profile is then not a mandatory field in this case.
- Permanent release: Door permanently opened in line with the weekly profile
- Office mode: If the door is opened by a short booking using an authorised ID card, it is kept open until it is closed again by a further booking. Short-term opening is not possible.
- Office release: If the door is opened by a short booking using an authorised ID card, the door is opened only briefly. If the ID card is presented for a longer time or presented twice in quick succession, the door is opened permanently until the office release expires or until the release is ended by performing a new booking using an ID card.

Note: This column is only present if one of the evolo system parameters 17 or 18 is active.

"Room zone - doors" dialog - Video camera

Each camera installed for video surveillance must be assigned to the door or reader to which it is connected in area/door management.

Video cameras may only be added beneath doors.

Number	<input type="text" value="85"/>	 Video camera
Name	<input type="text" value="Camera Main entry"/>	
Short name	<input type="text"/>	
IP address	<input type="text"/>	
Camera type	<input type="text" value="Identification"/> ▼	

IP address display field:

Displays the IP address of the video camera.

Camera type selection field:

To specify the type of camera use.

Values:

- Identification: For cameras with facial recognition and manual image comparison.
- Foreground: For surveillance cameras in the foreground without image comparison.
- Background: For surveillance cameras in the background without image comparison.

The selection determines the position and sequence in which the camera images are displayed. The image from the identification camera is displayed in the upper section, next to the employee record data and photo. This is followed by the images from the foreground camera and finally the images from the background camera.

4.6.2 Counting groups

Using counting groups you can create counting values for person groups to be displayed in the overview of the security areas. The counting values are created for each group for the security areas with a counting function.

You allocate counting groups to a person in person administration.

"Selection Counting groups" dialog

The **Selection Counting groups** dialog displays all counting groups created.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Selection Counting groups				
<input type="checkbox"/>	Number ▲	Name	Short name	Delete
<input type="checkbox"/>	1	Medical service		
Number of records: 1				

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Counting group" dialog

Use the **Edit Counting group** dialog to create new counting groups and edit existing counting groups. Each counting group requires a unique number. It is recommended that you specify a name and a short name.

Use the buttons in the toolbar to navigate between records, create or delete a record and save or discard changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number input field:

Contains the unique number for the counting group. When you create a new record, the number increases automatically by an increment of one. However, you can also enter your own number using up to 16 digits.

Name input field:

Contains the name for the counting group. When you enter a new name, you can enter any combination of figures and letters. This field is language-dependent.

Short name input field:

Contains the short name for the counting group. When you enter a new short name, you can enter any combination of figures and letters. This field is language-dependent.

4.6.3 Door weekly profiles

Door weekly profiles are based on the door daily times and are allocated to each door. A 7-day cycle applies to the door weekly profile, corresponding to a calendar week.

Note: The door weekly profile refers only to the door and not to the rights of the persons who make bookings at the door.

"Selection Door weekly profiles" dialog

The **Selection Door weekly profile** dialog displays all door weekly profiles created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Number	Name	Short name	Delete
1	Always	Always	
10	Administration and others	AdmAndCo	
20	Production	Prod	
21	Sales - customers	SalesCust	

Number of records: 4

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Door weekly profile" dialog

Use the **Edit Door weekly profile** dialog to create new door weekly profiles and edit existing door weekly profile records. Each door weekly profile requires a unique number. It is recommended that you specify a name and a short name.

A door weekly profile is allocated to each calendar day in a week.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



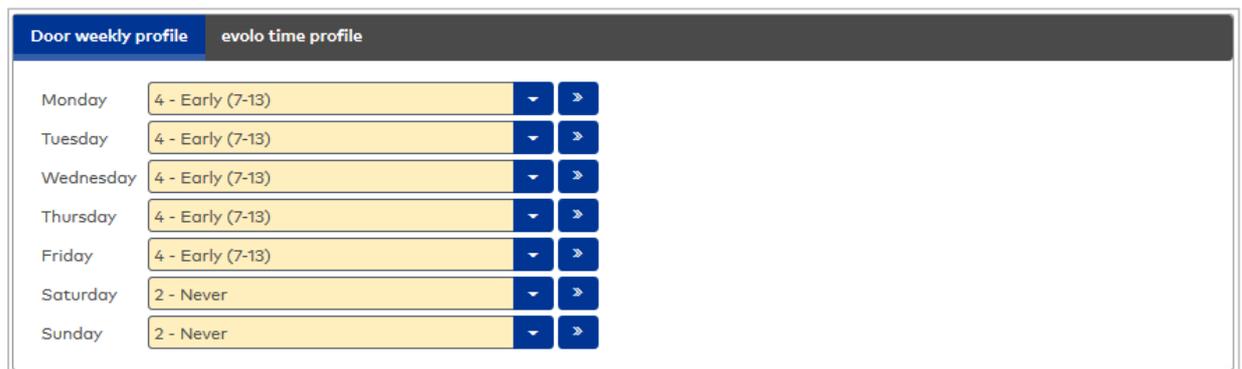
Number

Name

Short name

"Door weekly profile" tab

This tab is used to assign the door daily times.



Day	Selection
Monday	4 - Early (7-13)
Tuesday	4 - Early (7-13)
Wednesday	4 - Early (7-13)
Thursday	4 - Early (7-13)
Friday	4 - Early (7-13)
Saturday	2 - Never
Sunday	2 - Never

It contains the selection fields **Monday:** to **Sunday:**

Contain the number and name of the access daily time used on a particular day. You must select an entry for each weekday.

"evolo time profile" tab

Note: The tab is only present if evolo components are used.

If evolo components are used in the system, the time frames are mapped from the allocated door daily times to the evolo time profile for use in the evolo components.

The mapping is displayed on this tab for checking.

The time profile, which is calculated from the door weekly profile, can be assigned to the evolo components via the area/door tree, either as a profile for the permanent release times or as a profile for the possible office release times.

evolo time profiles consist of a report of time ranges during which the component allows access. A time range can be valid for one or more weekdays, on holiday days, or on the two special day types A or B.

Note: Holiday days are weekday-dependent, whereas special days are independent of the day of the week. This means that a time range for a holiday Monday does not necessarily need to apply for a holiday Tuesday. For special days, it is not possible to distinguish between weekdays.

Door weekly profile		evolo time profile										
evolo time profile for office release												
From	To	Day	Ho	Mo	Tu	We	Th	Fr	Sa	Su	A	B
evolo time profile for permanent release												
From	To	Day	Ho	Mo	Tu	We	Th	Fr	Sa	Su	A	B

The resulting time frames from the door daily times are displayed in the table. Changes cannot be made directly but must be made in the corresponding door daily times.

From/To columns:

Contain the time interval for access.

Day column:

Identifier for access on the set weekdays (Mo to Su).

Ho column:

Identifier for access on a bank holiday.

Mo, Tu, We, Th, Fr, Sa, Su column:

The columns contain the identifiers for the weekdays from Monday to Sunday.

Column **A**:

Identifier for the day type A.

Column **B**:

Identifier for the day type B.

Convert a door weekly profile

For the conversion of the door weekly profile, two evolo time profiles are generated, one of which applies to the permanent release intervals and one of which defines the intervals in which an office release is possible.

It is possible to assign only one time profile to a component and then define this as either a permanent release or office release time profile, but since a door weekly profile can be used differently on different components, both time profiles are generated.

The conversion of the door weekly profile into the evolo time profile for permanent release takes place as follows:

First, the "Permanent release" time ranges of each door daily time used are carried over to the time profile and a tick placed in the "Day" column and the corresponding weekday.

The system then runs through the access daily time substitute programs:

- If no substitute program is defined for the access daily time, it will also apply on holiday days and all special days.
- If there is a substitute program for the holiday day type, the time ranges of this substitute program are carried over to the time profile and a tick placed for Holidays and the corresponding weekday.
- If a substitute program is available for a day type with the special day identifier A, the time ranges are carried over with a tick in column A. The same applies to type B.

The time profile for office release is generated in the same way. In this case, the time ranges for office release are taken from the daily program instead of the permanent release time ranges.

Optimisation

Finally, as evolo components only allow a maximum of 12 time ranges per time profile, the system attempts to combine time ranges.

Conditions for combining rows:

1. The time frame is the same for both "From" and "To".
2. If a tick is placed for both Day and Holidays, the rows can be combined by linking the ticks for the weekdays and special day type with an "OR" function.
3. If a row only applies for special days, i.e. has no tick for Day and Holidays, and there is the same time range in the time profile, the rows can be combined by simply placing a tick additionally for the corresponding special day in the other time range.

Validation

A door daily time cannot always be converted to an equivalent time profile. The following validations will appear in the interface with corresponding messages:

1. Maximum 12 time ranges. If more time frames were generated during the conversion, a message to this effect appears.
2. Because substitute programs depend on the time profile for evolo components, only one substitute program may be allocated to a day type. If different substitute programs are allocated to a day type, a message to this effect appears.

Note: If no substitute program is assigned to a day type, the same daily program applies on special days, i.e. the substitute program is the same as the program, so to speak. It is therefore not possible for e.g. evolo components to use two daily programs and specify special days but not assign a substitute program to either.

3. If substitute programs are defined for day types which are marked as neither a special day nor a holiday day, these are ignored in evolo components. A corresponding notification is output in the door weekly profile on the **evolo time profile** tab.

4.6.4 Door daily times

A door can have different target statuses over the course of a day and handle different functions. You can use up to four time intervals to control to the minute if a door can be opened with a valid ID card, for example, or to define the period in which a door is permanently open.

Door daily times are a fundamental component of access control and are required for defining the door weekly profiles.

Note: Not all door daily times functions may be supported depending on the components used and the firmware installed.

You can use substitute door daily times to assign a separate door daily time to each day type, such as weekdays, bank holidays or special days. As a prerequisite, the day types must have been entered in the calendar and respective substitute door daily times defined in the door daily time for the respective day type.

For example, a door daily time for weekdays can switch the door as permanently open in the time from 10:00 h to 12:00 h.

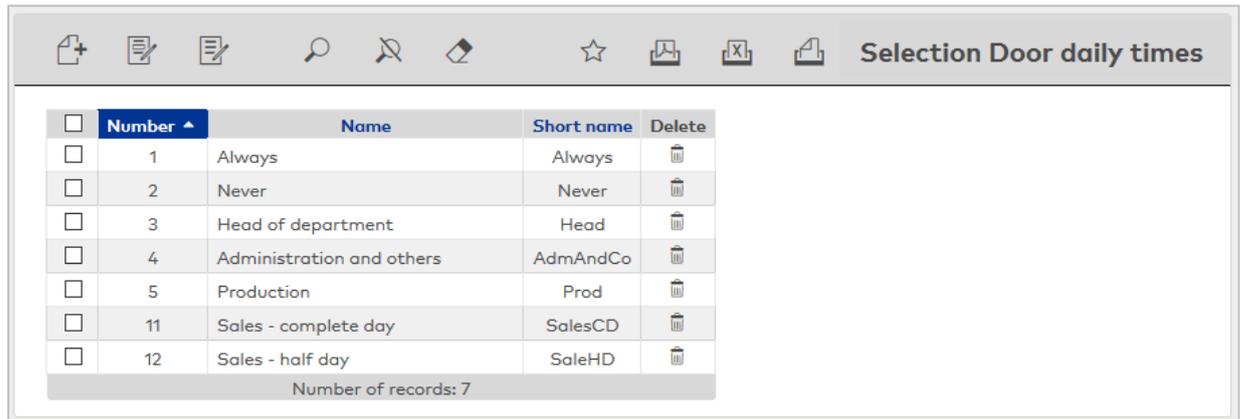
If the weekday coincides with a bank holiday on which the door is not to be open, you must enter a substitute door daily time for the respective day type which does not contain a time frame for the permanent opening.

Note: The door programs override the individual door commands when a time for a change is reached. This removes the status of the door that was set "manually". This procedure is necessary to ensure that the intended normal status of a door is reached even if the manual input was forgotten.

"Selection Door daily times" dialog

The **Selection Door daily times** dialog displays all door daily times created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number	Name	Short name	Delete
<input type="checkbox"/>	1	Always	Always	
<input type="checkbox"/>	2	Never	Never	
<input type="checkbox"/>	3	Head of department	Head	
<input type="checkbox"/>	4	Administration and others	AdmAndCo	
<input type="checkbox"/>	5	Production	Prod	
<input type="checkbox"/>	11	Sales - complete day	SalesCD	
<input type="checkbox"/>	12	Sales - half day	SaleHD	

Number of records: 7

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Door daily time" dialog

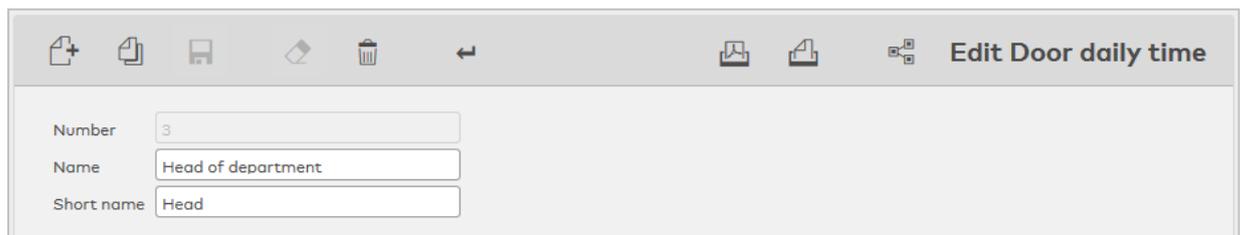
Use the **Edit Door daily time** dialog to create new door daily times and edit existing door daily times. Each door daily time requires a unique number; it is recommended that you specify a name and a short name.

For each door daily time you can define up to four periods with different functions. If you enter a time interval, you must include a start and an end value.

In the **Substitute programs** table, you can allocate a substitute daily program for each day type.

Note: This table is only available if calendars with special days are defined in your system.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Number: 3

Name: Head of department

Short name: Head

"General" tab

This tab contains the access-relevant time frame and the table with the substitute programs for door daily times.

Note: OSS components only support the "Office release" access function.

General		Advanced time ranges							
		from	until	from	until	from	until	from	until
Access:		04:00	23:00						
Permanent opening:									
Office release allowed:									
Motion recording off:									
PIN code check off:									
Substitute programs									
		Day type		Substitute programs					
		3 Bank holiday		<input type="text"/> <input type="button" value="▼"/> <input type="button" value="▶"/>					

Access input fields:

Contain the time intervals for electronically secured access. In the specified interval, access booking is possible with a valid ID card.

Permanent opening input fields:

Contain the time intervals in which the door is permanently open and access is possible without electronic authentication.

Office release allowed input fields

Contain the time intervals in which a person with corresponding permission can manually switch a door to "Permanent opening" using special bookings. Enter the times here for which a person such as the office owner can release this office for permanent opening.

Note: If the time frame for an office release starts at the end of the previous interval, the office release ends at the end of the first interval. However, this is not the case if the two intervals end and start exactly at the date limit.

Note: The maximum office release duration can be individually restricted for each entered time interval on the **Extended time ranges** tab.

Motion recording off input fields:

Contain the time intervals when the bookings should not be logged. For example, motion recording may not be required during regular business hours.

PIN code check off input fields:

Contain the time intervals when a PIN code does not have to be entered during booking. This option is only relevant to readers with a keypad. Enter the time intervals during which PIN code input should be inactivated, for example during regular business hours. Outside of these times, a PIN code must be entered.

Substitute programs table:

Contains substitute programs that you can define for individual day types.

Day type column:

Contains the unique number of the day type and the name in the respective language.

Substitute programs column:

Contains the selected substitute daily program. Select the relevant substitute daily program from the list. This field remains empty if the original door daily time should be used for a day type.

"Extended time ranges" tab

This tab can be used to define additional time frames for special uses. Up to four time intervals can be saved for each function.

General	Advanced time ranges	Emergency exit doors						
	from	until	from	until	from	until	from	until
No door open time monitoring:	<input type="text"/>							
Additional permanent opening:	<input type="text"/>							
Door key switch off:	<input type="text"/>							
Door status contact off:	<input type="text"/>							

No door open time monitoring input fields:

Time intervals during which door open time monitoring is deactivated.

Additional permanent opening input fields:

Additional time intervals during which the door is permanently open and access is possible without electronic authentication.

Door key switch off input fields:

Time intervals during which the door key switch is not activated. Opening the door with the door key switch is therefore not possible in this time range.

Door status contact off input fields:

Time intervals during which the door status contact is not evaluated.

Defaults area:

This area can be used to define time intervals with deviating VBI terminal texts.

Defaults			
from	until	Terminal text:	LED colour:
<input type="text"/>	<input type="text"/>	<input type="text"/>	Off <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Off <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Off <input type="button" value="v"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	Off <input type="button" value="v"/>

From ... to input fields:

Comply with the time intervals for deviating defaults.

Terminal text input fields:

Number of the terminal text displayed as preselection text in the display of the terminal or reader at the stated interval.

Refer to the device administration under class setting in the text number allocation for the required text numbers.

LED colour selection fields:

Colour of the ID card reader LED in the stated interval.

Maximum office release duration area

This area can be used to individually restrict the maximum time intervals for all office release durations specified on the **General** tab.

Maximum office release duration	
Interval 1 max.	<input type="text"/> Minutes
Interval 2 max.	<input type="text"/> Minutes
Interval 3 max.	<input type="text"/> Minutes
Interval 4 max.	<input type="text"/> Minutes

Interval max. __ minutes input fields

Value range: 0–1440 minutes

Note: If the field is empty, no restrictions are imposed and the office release applies until the end of the stated interval.

Output actuation area

This area can be used to define time intervals for deviating output actuation.

Output actuation

from	until	Output device number
<input type="text"/>	<input type="text"/>	<input style="width: 95%;" type="text"/> ▼
<input type="text"/>	<input type="text"/>	<input style="width: 95%;" type="text"/> ▼
<input type="text"/>	<input type="text"/>	<input style="width: 95%;" type="text"/> ▼
<input type="text"/>	<input type="text"/>	<input style="width: 95%;" type="text"/> ▼

From ... to input fields:

Comply with the time intervals during which the specified exit is to be activated.

Output device number selection fields:

Specifies the exit selected in the time ranges. All connected exits are available for selection.

"Emergency exit doors" tab

This tab contains the time frames for emergency exit doors.

Note: The tab is only available if the TMS connection option is activated.

	General	Advanced time ranges	Emergency exit doors				
		from	until	from	until	from	until
Access:		<input type="text" value="00:00"/>	<input type="text" value="24:00"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
Permanent opening:		<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
PIN code check off:		<input type="text" value="00:00"/>	<input type="text" value="24:00"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

Access input fields:

Contain the time intervals for access. In the specified interval, access booking is possible with a valid ID card.

Permanent opening input fields:

Contain the time intervals in which the door is permanently open and access is possible without authentication.

PIN code check off input fields:

Contain the time intervals when a PIN code does not have to be entered during booking. This option is only relevant to readers with a keypad. Enter the time intervals during which PIN code input should be inactivated, for example during regular business hours. Outside of these times, a PIN code must be entered.

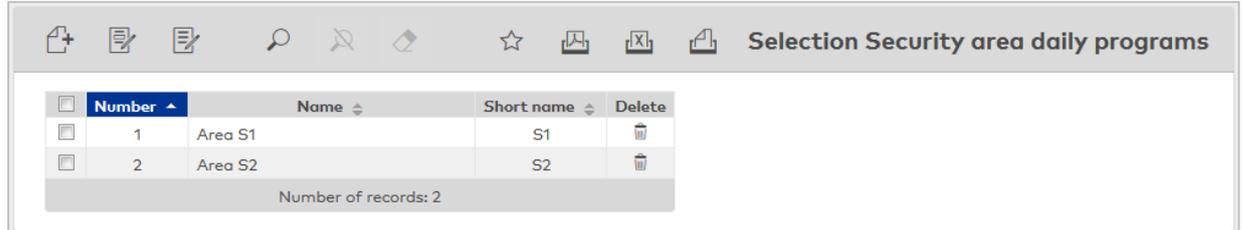
4.6.5 Security area weekly profile

The security area weekly profiles are based on the security area daily programs and are allocated to the security areas for IDS arming. A 7-day cycle applies to the security area weekly profile, corresponding to a calendar week.

"Selection Security area weekly profiles" dialog

The **Selection Security area weekly profiles** dialog displays all security area weekly profiles created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



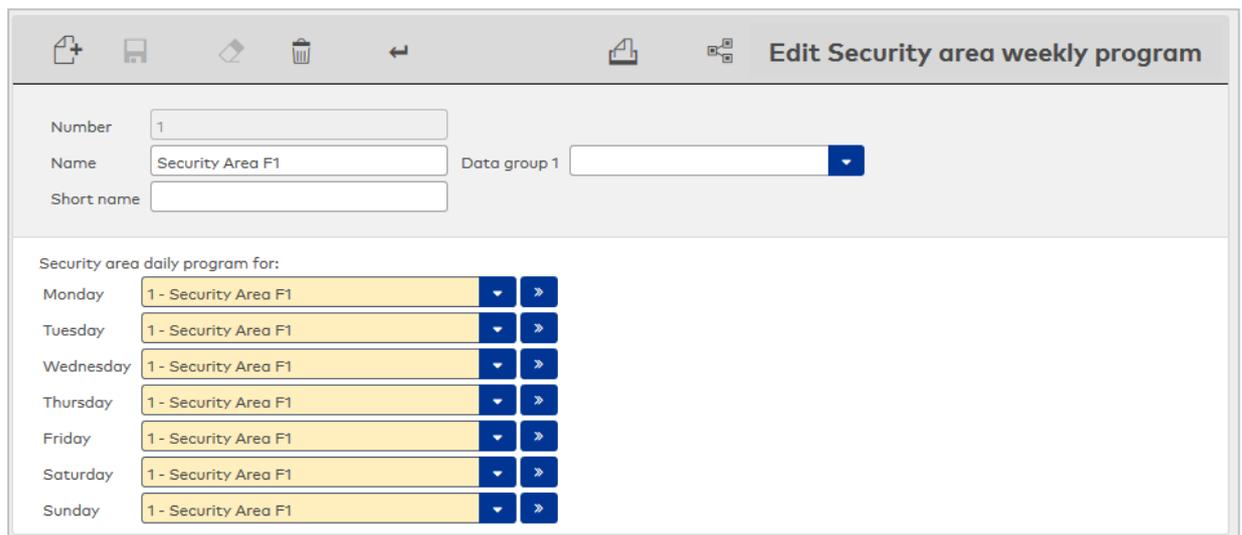
Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Security area weekly profile" dialog

Use the **Edit Security area weekly profile** dialog to create new security area weekly profiles and edit existing security area weekly profile records. Each security area weekly profile requires a unique number. It is recommended that you specify a name and a short name.

A security area weekly program is allocated to each calendar day in a week.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Selection fields **Door daily time for: Monday to Sunday** selection fields:

Contains the security area daily program to be used for each day of the week. You must select an entry for each day.

Options:

- All security area daily programs created in the system.

4.6.6 Security area daily programs

In the security areas, the IDS can be armed via counting information. This can be enabled/disabled at up to four intervals over the course of one day.

"Selection Security area daily programs" dialog

The **Selection Security area daily programs** dialog displays all security area daily programs created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number	Name	Short name	Delete
<input type="checkbox"/>	1	Security Area F1	SA F1	
<input type="checkbox"/>	2	Security Area F2		

Number of records: 2

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Security area daily program" dialog

Use the **Edit Security area daily program** dialog to create new security area daily programs and edit existing security area daily programs. Each security area daily program requires a unique number; it is recommended that you specify a name and short name.

For each security area daily program, you can define up to four periods in which IDS arming is disabled. If you enter a time interval, you must include a start and an end value.

In the **Substitute programs** table, you can allocate a substitute daily program for each day type.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number: 1 Data group 1: [dropdown]

Name: Security Area F1

Short name: SA F1

IDS activation via counting information disabled: [from] [until] [from] [until] [from] [until] [from] [until]

Day type	Substitute programs
3 Bank holiday	[dropdown]

Disable IDS arming via counting information input fields:

Contain the time intervals without IDS function.

Substitute programs table:

Contains substitute programs that you can define for individual security area daily programs.

Day type column:

Contains the unique number of the day type and the name in the respective language.

Substitute programs column:

Contains the selected substitute daily program. Select the relevant substitute daily program from the list. This field remains empty if the original door daily time should be used for a day type.

4.7 Calendar administration

On the **Calendar administration** menu you can define any number of calendars that you can use to take different company and regional bank holiday and special day regulations into account.

A distinction is made between different day types (such as weekdays, weekends and bank holidays) in each calendar. These day types and country-specific bank holiday templates are pre-installed with the system. However, you can use the dialogs in the **Additional options** sub-menu to change this, if different regulations apply in your company.

A calendar must be allocated to every person and every door (or every reader) when they are activated for access control.

Use the **Calendar** menu item to define a specific calendar.

In the **Additional options** sub-menu you can define company-specific special regulations.

Use the **Holidays** menu item to define ranges as holidays.

Use the **Manual special days** menu item to set up individual or recurring company-specific special days.

Use the **Bank holiday templates** menu item to define the templates for regional bank holidays. The system already contains a number of predefined bank holiday templates. You can use these directly; you do not need to enter them.

Use the **Bank holidays** menu item to define all fixed and floating bank holidays. All official bank holidays and a number of additional bank holidays are predefined in the system. You can use these directly; you do not need to enter them.

Use the **Weekdays** menu item to allocate a day type to each weekday. You can define a name, a short description and a colour for the calendar overview for each weekday in the calendar. All weekdays are predefined in the system. Editing is only required if you want to display them differently. If you want to display the weekdays differently in different calendars, you can create additional weekday records.

Use the **Day types** menu item to define the day types that can be used. These represent a group of days that should be handled in the same way. For example, all weekdays are grouped into the type "Weekdays" and bank holidays such as New Year's Eve and New Year's Day into the type "Bank holidays".

4.7.1 Calendar

The calendar forms the basis of the company- and regional-dependent definition of bank holidays and manual special days such as company holidays. Each day is allocated to a specific day type which has specific access programs defined.

The calendar, which can be displayed as a year or a month overview, gives an overview of all bank holidays and special days. You can maintain special days individually. The standard day assignment (Monday to Sunday) is calculated automatically using the defaults.

To take regional- and company-specific differences into account, you can save several calendars.

"Selection calendar" dialog

The **Selection Calendar** dialog displays all calendars created in the system.

You need at least one calendar to which you allocate bank holidays and manual special days according to your company's regional and operational specifications.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



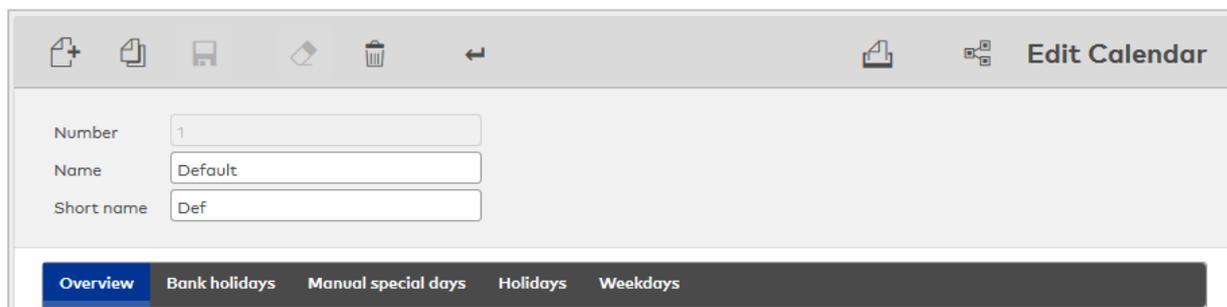
Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit calendar" dialog

Use the **Edit Calendar** dialog to create new calendars and edit existing calendar records. Each calendar requires a unique number; it is recommended that you specify a name and a short name.

Use the relevant tabs to allocate bank holidays or bank holiday templates, manual special days and weekdays.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Overview

On the **Overview** tab, you can display the calendar as a yearly overview or a monthly overview.

Apply to this calendar button:

Click this button to apply the selected bank holiday template. This allocates the bank holidays from the selected template. The bank holidays are set up in the calendar after saving.

Available bank holidays report:

Contains all bank holidays created in the system. Click a bank holiday to select it and then click the arrow pointing right. This adds the selected day to the calendar.

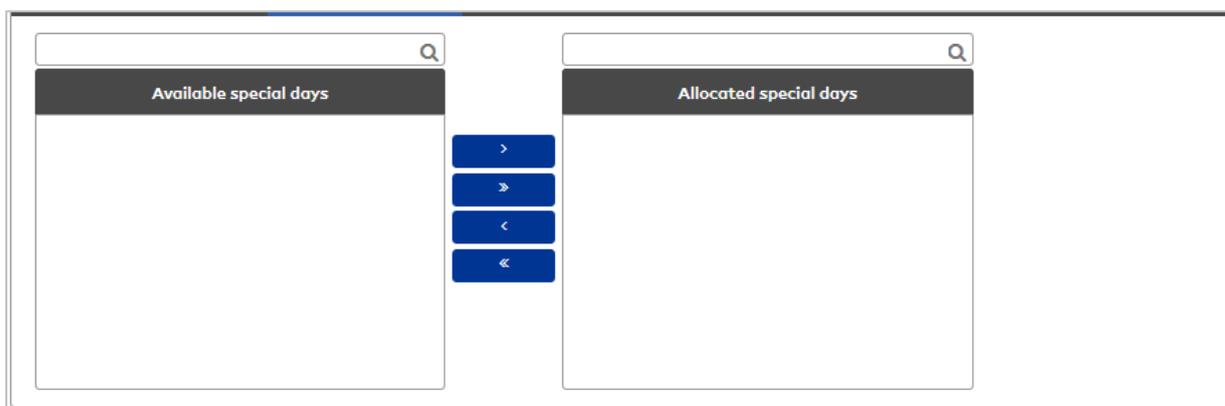
Allocated bank holidays report:

Contains all bank holidays that are allocated to the calendar. Click a bank holiday to select it and then click the arrow pointing left to remove this day from the calendar.

Note: Select multiple bank holidays simultaneously by holding down the Ctrl key as you click them.

Manual special days

Use the **Manual special days** tab to allocate the created manual (company) special days to the calendar.

**Available special days** report:

Contains all manual special days that are created in the system. Click a special day to select it and then click the arrow pointing right. This adds the selected day to the calendar.

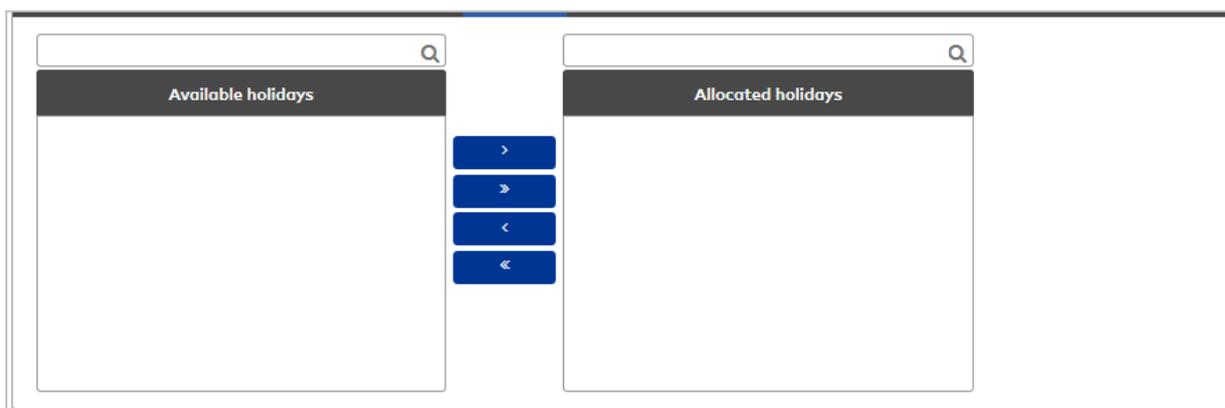
Allocated special days report:

Contains all the special days that are allocated to the calendar. Click a special day to select it and then click the arrow pointing left to remove this day from the calendar.

Note: You can select several bank holidays simultaneously by holding down the Ctrl key as you click them.

Holidays

Use the **Holidays** tab to allocate the created holidays to the calendar.



Available holidays report:

Contains all holidays created in the system. Click an entry to select it and then click the arrow pointing right. The selected holidays will be added to the calendar.

Allocated holidays report:

Contains all holidays that are allocated to the calendar. Click an entry to select it and click the arrow pointing left to remove the holidays from the calendar.

Weekdays

Use the **Weekdays** tab to allocate weekdays to the calendar. The allocated weekdays determine how the weekday is displayed in the calendar.

Note: By default, the pre-installed weekdays are already selected. You only need to change the selection if you have created additional weekdays.

Monday	1 - Monday	▼	»
Tuesday	2 - Tuesday	▼	»
Wednesday	3 - Wednesday	▼	»
Thursday	4 - Thursday	▼	»
Friday	5 - Friday	▼	»
Saturday	6 - Saturday	▼	»
Sunday	7 - Sunday	▼	»

Monday – Sunday selection fields:

Contain the allocated weekday.

Options:

- All weekdays created in the system.

4.7.2 Additional options (calendar)

The additional options for calendar administration can be used to make individual adjustments to bank holidays, special days and weekdays for the calendar display.

In addition, holiday days, manual special days, bank holidays, bank holiday templates, weekdays and day types can be defined.

4.7.2.1 Holidays

In addition to special days and bank holidays, holidays are a range of special days in the calendar on which abnormal conditions have to be taken into account. Holidays are intrinsically linked to the special day type "Holidays". If this day type is not present in the system, no holidays can be defined.**Note.** During evaluation of holidays, they are overwritten by manual special days and bank holidays.

"Selection holidays" dialog

The **Selection Holidays** dialog displays all holidays created in the system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number ▲	Name	Short name	Delete
<input type="checkbox"/>	1	Summer		
<input type="checkbox"/>	2	Winter		

Number of records: 2

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit holidays" dialog

Use the **Edit Holidays** dialog to create new holidays and edit existing holidays. Holidays require a unique number; it is recommended that you specify a name and a short name.

Holidays are defined as a range and are always intrinsically linked to the day type "Holidays".

Note: If the day type "Holidays" is not present in the system, no holidays can be defined.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number: 1

Name: Summer

Short name:

Data group 1:

Holidays from: 07/01/2017

Holidays until: 08/16/2017

Colour:

Day type: 6 - Holidays

Holidays from date field:

Contains the first day of the holidays.

Holidays until date field:

Contains the last day of the holidays.

Colour field:

Contains the colour for the calendar display. Click the **Colour** button to change the colour. The colour chart is opened.

4.7.2.2 Manual special days

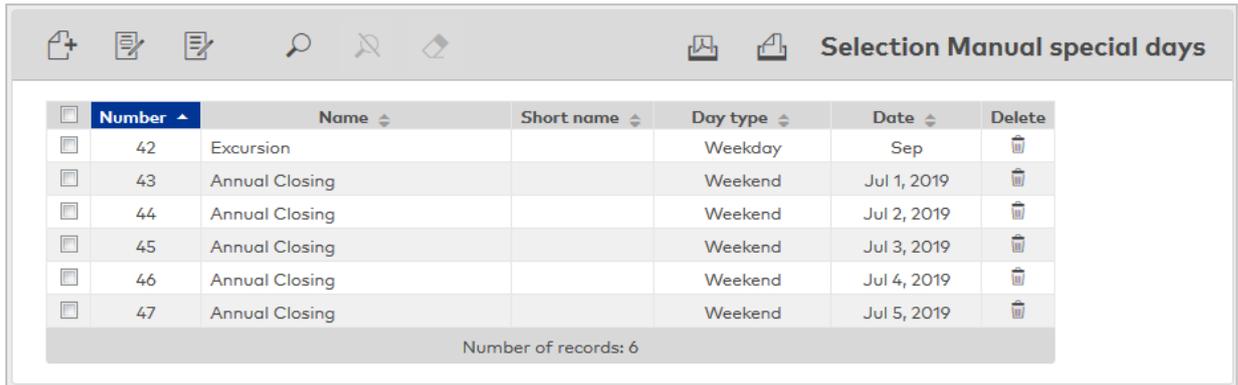
Manual special days refer to special days within the company. These can be individual days, annually-recurring days or periods such as company holidays.

"Selection Manual special days" Dialog

The **Selection Manual special days** dialog displays all company special days that can be used for calendar definition.

A period is always displayed in the form of individual days.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number	Name	Short name	Day type	Date	Delete
<input type="checkbox"/>	42	Excursion		Weekday	Sep	
<input type="checkbox"/>	43	Annual Closing		Weekend	Jul 1, 2019	
<input type="checkbox"/>	44	Annual Closing		Weekend	Jul 2, 2019	
<input type="checkbox"/>	45	Annual Closing		Weekend	Jul 3, 2019	
<input type="checkbox"/>	46	Annual Closing		Weekend	Jul 4, 2019	
<input type="checkbox"/>	47	Annual Closing		Weekend	Jul 5, 2019	

Number of records: 6

Day type column:

Contains the day type that is allocated to the special day.

Date column:

Contains the date of the special day.

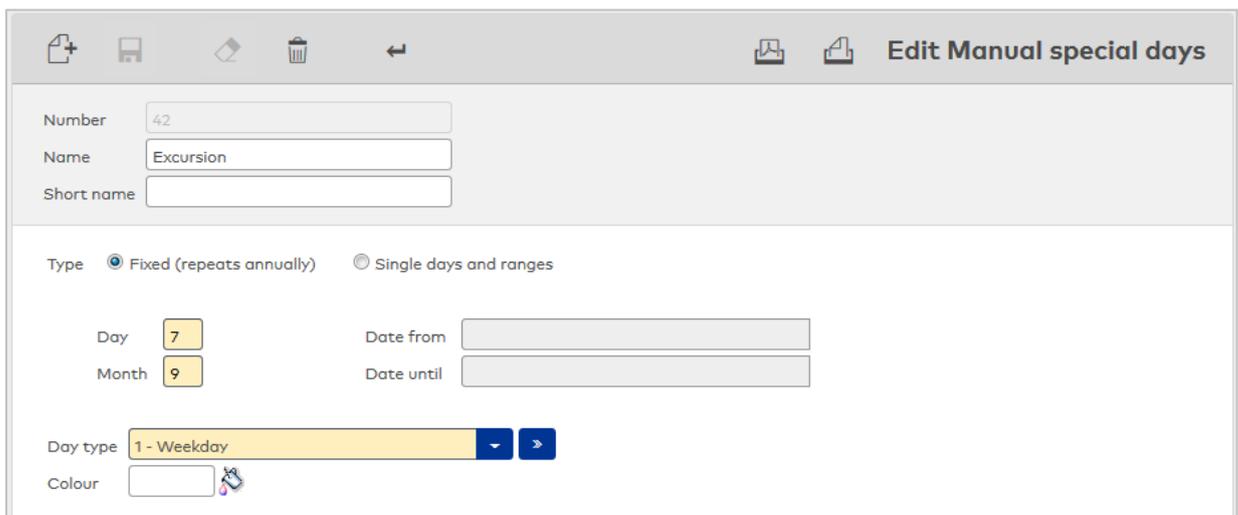
Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Manual special days" dialog

Use the **Edit Manual special days** dialog to create company special days and edit existing special day records. Each record requires a unique number; it is recommended that you specify a name and a short name.

You can create fixed, annually-recurring special days as well as individual events or even time periods (ranges). For ranges, individual special days are created according to the information you specify; they can then be edited individually.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Number:

Name:

Short name:

Type: Fixed (repeats annually) Single days and ranges

Day: Date from:

Month: Date until:

Day type:

Colour:

Fixed radio button:

Defines a fixed special day that is repeated annually.

Single days and ranges radio button:

Defines a single special day or a single period. Select this option if you want to specify company holidays for

your company in the calendar. When you specify a range, individual special days are generated for the period.

Day date field:

Contains the day of a date specification as a two-digit number. This field is only active for the **Fixed** option.

Month date field:

Contains the month of a date specification as a two-digit number. This field is only active for the **Fixed** option.

Date from field:

Contains the date of an individual special day or the start date for a period. This field is only active for the **Single days and ranges** option. Enter a date, or click the calendar icon and select a date.

Date until date field:

Contains the end date for a period. This field is only active for the **Single days and ranges** option. Enter a date, or click the calendar icon and select a date.

Day type selection field:

Contains the day type that should be allocated to the special day. Select a day type.

Colour field:

Contains the colour for the calendar display. Click the **Colour** button to change the colour. The colour chart is opened.

4.7.2.3 Bank holiday templates

To make bank holidays easy to use, the system provides country-specific bank holiday templates enhanced with a template containing all bank holidays, and a template containing no bank holidays.

You can adapt these templates according to your company's local specifications, or create additional templates on the basis of existing ones by copying them. There is no function for replacing the original templates with ones that have changed.

Note: Changes to the template do not affect the existing calendar as the template is only used when a calendar is created. When it is allocated, the bank holidays it contains are simply copied to the calendar.

"Selection bank holiday templates" dialog

The **Selection Bank holiday templates** dialog displays all bank holiday templates that can be used for the calendar definition.

By default, a series of bank holiday templates are pre-installed in the system. You can create as many of your own bank holiday templates as you like according to your company's regional and operational specifications.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

	Number	Country code	Name	Short name	Delete
<input type="checkbox"/>	0	XX	No bank holidays	No	
<input type="checkbox"/>	2	DE	Baden-Württemberg	BW	
<input type="checkbox"/>	3	DE	Bavaria	BY	
<input type="checkbox"/>	4	DE	Berlin	BE	
<input type="checkbox"/>	5	DE	Brandenburg	BB	
<input type="checkbox"/>	6	DE	Bremen	HB	
<input type="checkbox"/>	7	DE	Hamburg	HH	
<input type="checkbox"/>	8	DE	Hesse	He	
<input type="checkbox"/>	9	DE	Mecklenburg-Western Pomerania	MV	

Country code column:

Contains a country code for the bank holiday template.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit bank holiday template" dialog

Use the **Edit Bank holiday template** dialog to create new bank holiday templates and edit existing bank holiday template records. Each bank holiday template requires a unique number and a country code; it is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Edit Bank holiday template	
Number	<input type="text" value="11"/>
Name	<input type="text" value="North Rhine-Westphalia"/>
Country code	<input type="text" value="DE"/>
Short name	<input type="text" value="NW"/>
<div style="border: 1px solid gray; padding: 5px;"> <p>Available bank holidays</p> <ul style="list-style-type: none"> 2 - Epiphany 3 - Carnival Monday 4 - Shrove Tuesday 13 - Assumption Day 15 - Reformation Day 17 - Penance Day 18 - Christmas Eve 21 - New Year's Eve 22 - Eighth of May 23 - Seventeenth of May </div>	<div style="border: 1px solid gray; padding: 5px;"> <p>Allocated bank holidays</p> <ul style="list-style-type: none"> 1 - New Year 5 - Good Friday 6 - Easter Sunday 7 - Easter Monday 8 - 1st of May 9 - Ascension Day 10 - Whit Sunday 11 - Whit Monday 12 - Corpus Christi 14 - German Unification Day </div>

Country code input field:

Contains the bank holiday template's country code. In the selection field of the bank holiday templates, the country code appears in front of the name in the calendars. Bank holiday templates with the same country code are therefore grouped in the selection field which makes them easier to identify
Value range: 2 characters.

Available bank holidays report:

Contains all bank holidays created in the system. Click a bank holiday to select it and then click the arrow pointing right. This adds the selected day to the bank holiday template.

Allocated bank holidays report:

Contains all the bank holidays that are allocated to the bank holiday template. Click a bank holiday to select it and then click the arrow pointing left to remove this day from the bank holiday template.

Note: You can select several bank holidays simultaneously by holding down the Ctrl key as you click them.

4.7.2.4 Bank holidays

In addition to manual (business) special days, bank holidays are special days in the calendar, on which unusual conditions have to be taken into account.

Fixed bank holidays take place every year on the same date. Floating bank holidays have a calendar reference and can be calculated by the system.

To make it easier to use, the system provides bank holiday templates that take country-specific differences in bank holidays into account. You can also create individual templates in the dialog for bank holiday templates. You do not need to maintain the bank holidays every year as the system updates them independently.

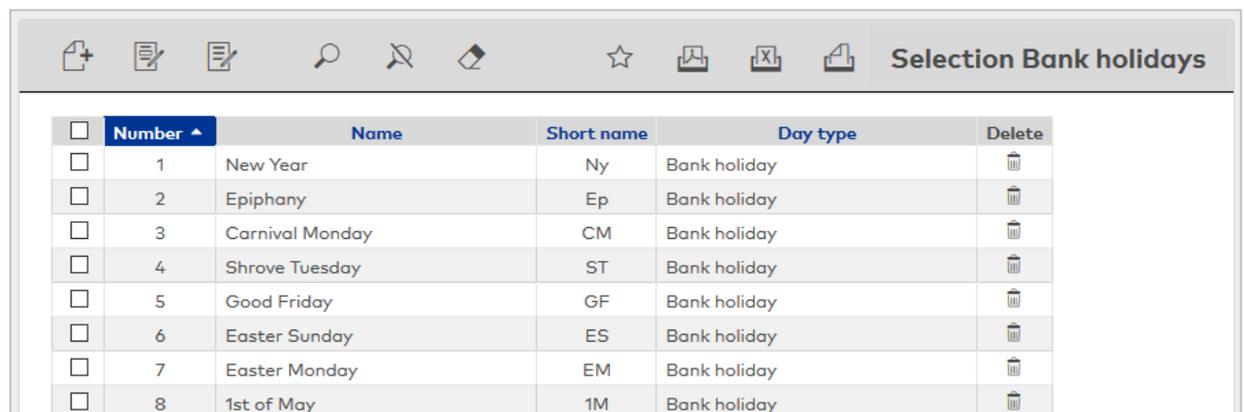
To take regional differences in bank holidays into account, you can easily enter or edit them in the system.

"Selection bank holidays" dialog

The **Selection Bank holidays** dialog displays all bank holidays that can be used to create the bank holiday templates.

By default, a series of bank holidays are pre-installed in the system. You can create as many additional bank holidays as you like according to your company's regional specifications.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number ▲	Name	Short name	Day type	Delete
<input type="checkbox"/>	1	New Year	Ny	Bank holiday	
<input type="checkbox"/>	2	Epiphany	Ep	Bank holiday	
<input type="checkbox"/>	3	Carnival Monday	CM	Bank holiday	
<input type="checkbox"/>	4	Shrove Tuesday	ST	Bank holiday	
<input type="checkbox"/>	5	Good Friday	GF	Bank holiday	
<input type="checkbox"/>	6	Easter Sunday	ES	Bank holiday	
<input type="checkbox"/>	7	Easter Monday	EM	Bank holiday	
<input type="checkbox"/>	8	1st of May	1M	Bank holiday	

Day type column:

Contains the day type that is allocated to the bank holiday.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit bank holiday" dialog

Use the **Edit Bank holiday** dialog to create new bank holidays and edit existing bank holiday records.

Bank holidays can be fixed, that is, tied to a fixed calendar day, or dynamic, that is, they take place on a different calendar day each year.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

The screenshot shows the 'Edit Bank holiday' form. At the top is a toolbar with icons for adding, saving, deleting, navigating back, printing, and a 'Back to selection' button. The form fields are as follows:

- Number:** 1
- Name:** New Year
- Short name:** Ny
- Type:** Fixed (selected), Dynamic
- Day:** 1
- Month:** 1
- Formula:** (empty)
- Day type:** 3 - Bank holiday
- Colour:** Red

Fixed radio button:

Defines a fixed bank holiday. Select this option if the bank holiday is on the same date each year.

Dynamic radio button:

Defines a floating bank holiday. Select this option if the bank holiday is on a different date each year.

Day date field:

Contains the day of a date specification as a two-digit number. This field is only active for the **Fixed** option.

Month date field:

Contains the month of a date specification as a two-digit number. This field is only active for the **Fixed** option.

Formula selection field:

Contains the formula for calculating a dynamic bank holiday. The formulas are specified by the system. This field is only active for the **Dynamic** option.

Day type selection field:

Contains the day types. This is usually the entry **Bank holiday** or **Half bank holiday** (e.g. for New Year's Eve and Christmas Eve if these days generally count as half bank holidays in your company.) However, you can also allocate any other day types you like.

Colour field:

Contains the colour for the calendar display. Click the **Colour** button to change the colour. The colour chart is opened.

4.7.2.5 Weekdays

Weekdays form the basis of automatic calendar generation and define the layout of a calendar week.

The system specifies seven weekdays that cannot be deleted. You can change the day type and the colour in which the weekdays are displayed in the calendar.

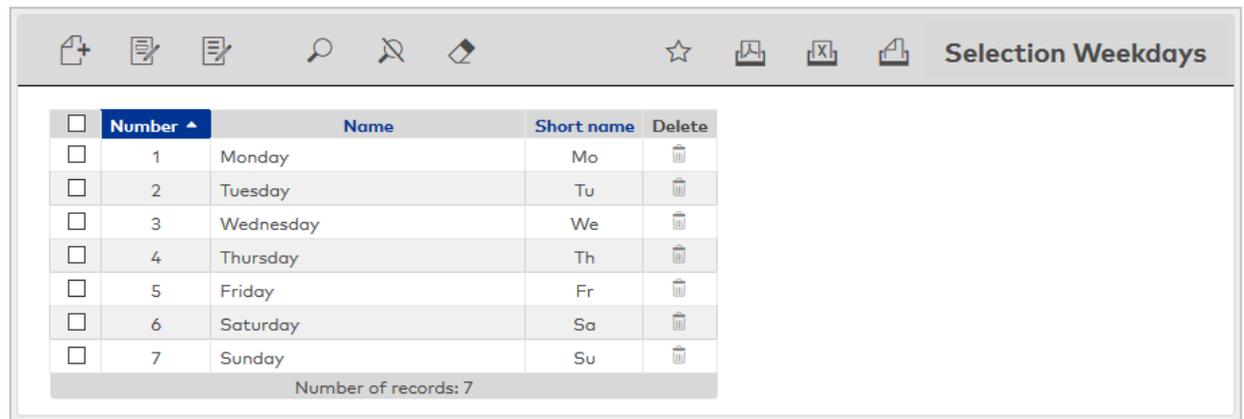
If you want to maintain different calendars with different day types or display the weekdays in different colours, you can create additional weekdays and edit them accordingly.

"Selection weekdays" dialog

The **Selection Weekdays** dialog displays the weekdays contained in the calendar.

The weekdays are created with their name and the usual short name. You can change this information, although we do not recommend this.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

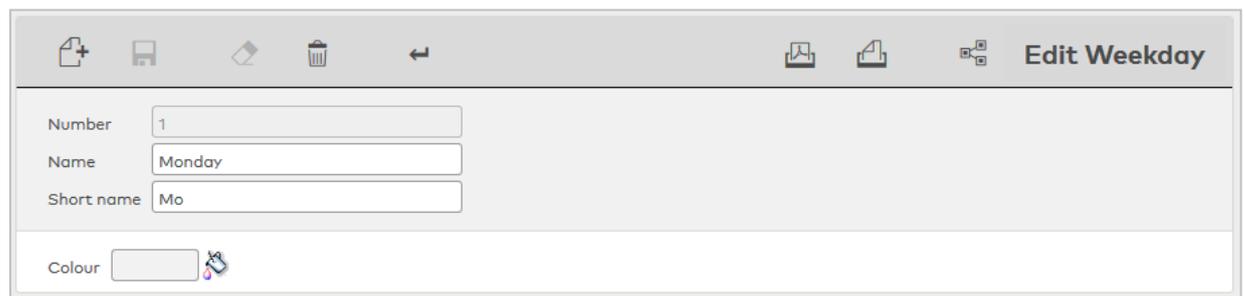


Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit weekday" dialog

Use the **Edit Weekday** dialog to change the colour in which the weekday is displayed in the calendar and the allocation of the day type.

You can use the buttons in the toolbar to navigate between records, to save or reject changes made to the record, or to print a record. Use the **Search** button to return to the selection.



Number input field:

Contains the weekday's unique number.

Name input field:

Contains the weekday's name. This field is language-dependent.

Short name input field:

Contains the weekday's short name. This field is language-dependent.

Colour field:

Contains the colour for the calendar display. Click the **Colour** button to change the colour. The colour chart is opened.

4.7.2.6 Day types

Day types make up groups of days to which the same processing rules apply. This significantly reduces the amount of effort needed to maintain the calendar.

The system specifies the following day types:

- Week day, Wd
- Weekend, We
- Bank holiday, BH
- Special bank holiday, SBH
- Half bank holiday, HBH

You can also create additional day types.

Note: You can only delete day types if there are no references to them in the system.

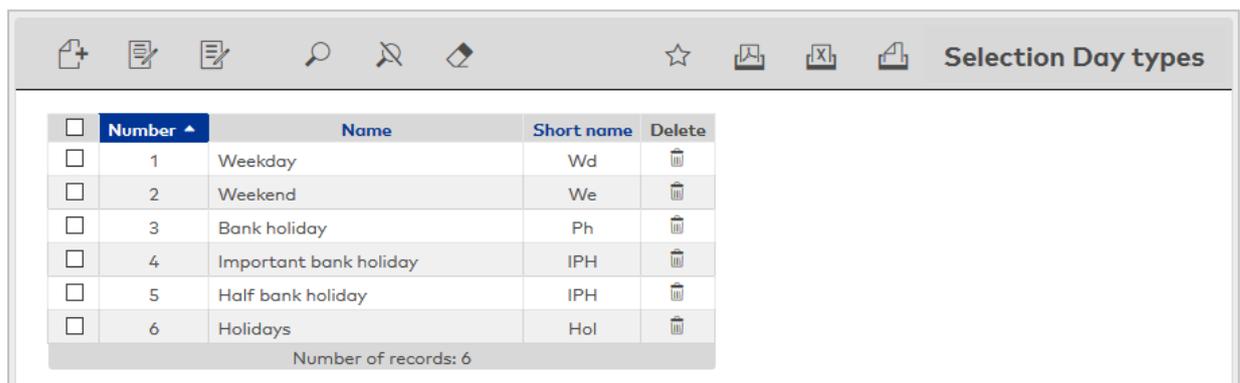
The calendar-related substitute program handles the special days on the basis of the allocated day types. Day types are used internally as the link between the special days and substitute programs.

"Selection day types" dialog

The **Selection Day types** dialog displays all day types that can be used for calendar definition.

By default, the following day types are pre-installed: week day, weekend, bank holiday, special bank holiday and half bank holiday.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number ↑	Name	Short name	Delete
<input type="checkbox"/>	1	Weekday	Wd	
<input type="checkbox"/>	2	Weekend	We	
<input type="checkbox"/>	3	Bank holiday	Ph	
<input type="checkbox"/>	4	Important bank holiday	IPH	
<input type="checkbox"/>	5	Half bank holiday	IPH	
<input type="checkbox"/>	6	Holidays	Hol	

Number of records: 6

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit day type" dialog

Use the **Edit Day type** dialog to create new day types and edit existing day type records. Each record requires a unique number; it is recommended that you specify a name and a short name.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Number input field:

Contains the unique number for the day type. When you create a new record, the number increases automatically by an increment of one. However, you can also enter your own number using between 1 and 4 digits (1–9999).

Name input field:

Contains the name for the day type. When you enter a new name, you can enter any combination of figures and letters. This field is language-dependent.

Short name input field:

Contains the short name for the day type. When you enter a new short name, you can enter any combination of figures and letters. This field is language-dependent.

Note: The two fields below are present if the system parameters 17 or 18 for evolo devices are activated for evolo devices.

Holidays checkbox:

Indicates whether this day type is used for holiday days. The identifier "Holidays" can only be assigned for one day type.

Options:

- Active: The day type is used for holiday days.
- Not activated: The day type is not used for holiday days.

Default: Not activated.

evolo special day type selection field:

Selection of the day type for use in the evolo components.

Options:

- No selection for the special day type
- Type A
- Type B

Default value: No selection.

4.8 Locking plan administration

Use the **Locking plan administration** menu to manage locking plans.

A locking plan is used to grant access permissions via tables. Permissions can be granted to individual persons, person groups, individual doors and door groups.

Use the **Locking plans** menu item to manage the locking plans.

Use the **Person groups** menu item to combine persons into person groups.

Use the **Door groups** menu item to combine doors into door groups.

4.8.1 Locking plan

The locking plan is a simple way of assigning access permissions. It is displayed in a table. The table columns contain the doors and the rows contain the persons to be granted permissions. The access permissions are set at the intersections of the columns and rows.

The basic prerequisite for the locking plan is the door. No distinction is made as to whether one or more readers are connected to the door. The side of the door on which the reader is located or whether readers are located on both sides of the door is also irrelevant. The access permission always applies to all the door's readers.

You can group persons in person groups and doors in door groups to keep the table simple.

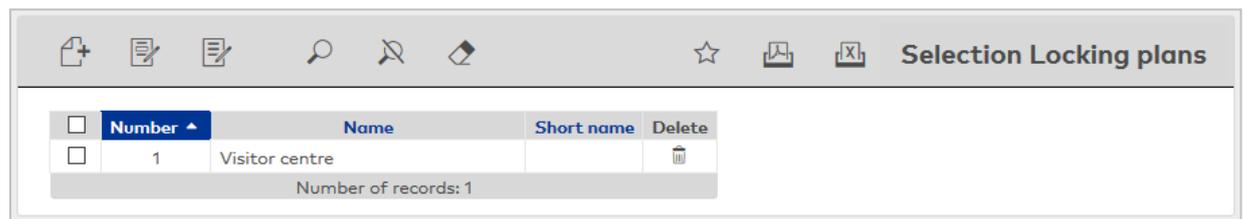
The basic version of the locking plan does not include any time-related components for access permissions. Calendar-dependent, time-related components that limit access permissions to a specific time frame by using access weekly profiles and access programs can be connected with an extended locking plan.

A distinction is made between locking plans that use single time profiles and those that use individual allocation of access weekly profiles. In the case of the locking plans with single time profile weekly profiles, the access weekly profile is allocated once in the locking plan; in the case of individual locking plans, allocation occurs at the intersection in the table by selecting the access weekly profile.

"Selection locking plans" dialog

The **Selection Locking plans** dialog displays all locking plans created in the access system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit locking plan" dialog

The **Edit Locking plan** dialog is used to assign access permissions for persons and doors. All created persons and doors together form the matrix for the locking plan in the form of a table.

Access permissions can be assigned using single time profiles in which the same access weekly profile applies to all person/door combinations. Alternatively, individual access weekly profiles can be selected for every person/door combination.

If the locking plan contains many doors and persons, you can use the search function (magnifying glass) to search for specific persons/person groups and doors/door groups.

The persons and doors for which actions are still required are in the first position in the table. The column and row headers for such items are also displayed in red. Persons highlighted in red have no access permissions.

Doors may be marked red for two reasons:

- The doors have no access permission or
- the doors are equipped with XS/evolo offline components which have not yet been synchronised.

Single time profile checkbox:

Indicates if the same access weekly profile is used for all access permissions or if individual allocation of an access weekly profile is possible.

- Activated: The same access weekly profile applies to all access permissions in the table. The table is a simple matrix in which access permission is granted for person–door combinations by ticking the boxes.
- Not activated: Allows access weekly profiles to be individually allocated for every person–door combination using the selection fields in the table.

Note: When you change the checkbox you must save the changes so that they are included in the display of the locking plan.

If you change from a locking plan with individual weekly profile to a locking plan with single time profile, the individual weekly profiles are replaced by the single time profile weekly profile. This change can **not** be reversed after saving.

Configure persons/person groups button:

Opens [Configure persons/person groups dialog](#) for selecting persons and person groups.

Configure doors/door groups button:

Opens [Configure doors/door groups dialog](#) for selecting doors and door groups.

Button :

Enlarges the view of the locking plan to fit the browser window. The **Embedded view** button sets the browser window back to the normal display.

Note: The number of table rows and columns displayed on a page can be limited using the system parameters Access 63 (number of rows) and Access 64 (number of columns). Use the arrow buttons displayed to navigate forwards and backwards if more records are present than rows and columns per page.

Locking plan with single time profile

If a single time profile is activated, the access permissions are set using a simple checkbox at the intersections in the table.

	104 Berlin room	G:00001 London-NewYork	102 Paris room	101 Reception B5	105 Rome room
Ackreiter, Thorsten (1)	<input checked="" type="checkbox"/>				
Administration (G:1)	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Cermans, Paul (7)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Hochmeyer, Gertrud (5)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Kamp, Karsten (9)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Leconte, Sandra (10)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Legrand, Marc (6)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Meunier, Catherine (8)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Access weekly profile selection field:

Select the access weekly profile for access permissions in a single time profile. This access weekly profile applies to all access permissions in the table.

Table:

The table contains the checkboxes for the access permissions. Activate the checkbox for the person/door combination at the intersections for which access permission shall be granted.

Locking plan with individual access weekly profiles

In a locking plan with individual access weekly profiles, the access weekly profiles for access permissions are selected from the intersections of the table. No access permissions apply to the person/door combination if no access weekly profile is selected.

	104 Berlin room	G:1 London-NewYork	102 Paris room	101 Reception B5	105 Rome room
Ackreiter, Thorsten (1)	1 - Always	1 - Always	1 - Always	1 - Always	1 - Always
Administration (G:1)	10 - Administration	10 - Administration	10 - Administration	1 - Always	10 - Administration
Cermans, Paul (7)	12 - Development			1 - Always	1 - Always
Hochmeyer, Gertrud (5)	12 - Development	12 - Development		1 - Always	1 - Always
Kamp, Karsten (9)			11 - Production	1 - Always	1 - Always
Leconte, Sandra (10)	11 - Production		11 - Production	1 - Always	1 - Always
Legrand, Marc (6)			12 - Development	1 - Always	1 - Always
Meunier, Catherine (8)	10 - Administration		10 - Administration	1 - Always	1 - Always

Table:

The table contains the selection fields for the access weekly profiles. Select the appropriate access weekly profile at the person/door combinations. Leave the selection for the access weekly profile blank for the person/door combinations for which you do not want to grant any access permissions.

Tip: Proceed as follows to set up a locking plan with individual access weekly profiles that contains many access permissions with the same access weekly profile:

1. First, create a locking plan with a single time profile and select the favoured access weekly profile.
2. Set access permission for the selected access weekly profile for all required person/door combinations and save the locking plan.
3. Next, deactivate the single time profile and save it again. All previously selected table intersections: now contain the favoured access weekly profile.
4. Now, just change the access permissions where a different access weekly profile is to be used.

"Configure persons/person groups" dialog

Use the **Configure persons/person groups** dialog to specify the persons and person groups managed in the locking plan.

Use the buttons in the toolbar to apply or discard the selection. Use the **Cancel** button to return to the locking plan.

Persons/person groups selection report:

Use the selection reports to allocate persons and person groups to the locking plan. You can recognise person groups by the **G:** identifier.

"Configure doors/door groups" dialog

Use the **Configure doors/door groups** dialog to specify the doors and door groups managed in the locking plan.

Use the buttons in the toolbar to apply or discard the selection. Use the **Cancel** button to return to the locking plan.

Doors/door groups selection reports:

Use the selection reports to allocate the doors and door groups to the locking plan. All doors are available which have not yet been added to another door group, do not belong to a room zone and for which no permissions or special permissions were allocated.

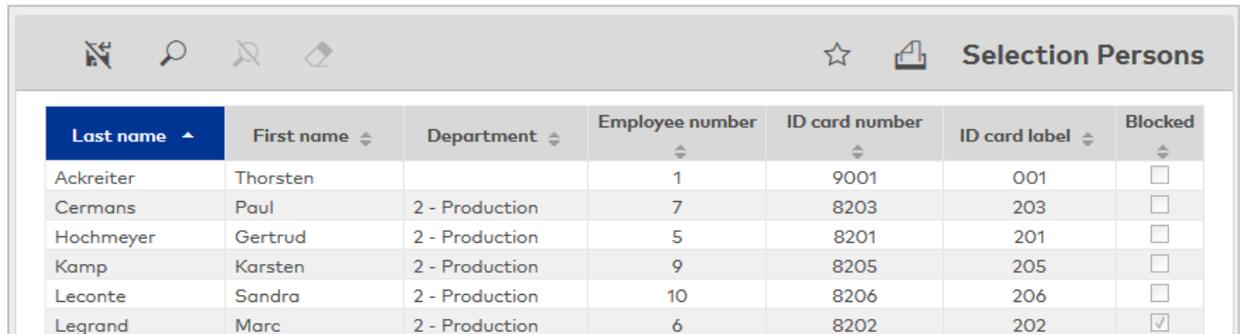
You can recognise door groups by the **G:** identifier.

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.

Note: Persons who have left the company are not included in this selection.



Last name	First name	Department	Employee number	ID card number	ID card label	Blocked
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

"Selection Person groups" dialog

The **Selection Person groups** dialog displays all person groups allocated to the locking plan.

You can use the buttons in the toolbar to search for individual person groups by number, name or short name.

The table displays the corresponding search results. Click a column header to sort the report by a characteristic in ascending or descending order. Click an entry to directly apply the corresponding record to the invoking dialog.



	Number	Name	Short name
<input type="checkbox"/>	1	Administration	A

Number of records: 1

"Selection Doors/Readers" dialog

The **Selection Doors/Readers** dialog displays all doors/readers which have been created and allocated to the locking plan.

You can use the buttons in the toolbar to search for individual doors by number, name or short name.

The table displays the corresponding search results. Click a column header to sort the report by a characteristic in ascending or descending order. Click an entry to directly apply the corresponding record to the invoking dialog.

<input type="checkbox"/>	Door number ▲	Door name	Door short name
<input type="checkbox"/>	101	Reception B5	R B5
<input type="checkbox"/>	102	Paris room	Pr
<input type="checkbox"/>	104	Berlin room	Be
<input type="checkbox"/>	105	Rome room	Ro

Number of records: 4

"Selection Door groups" dialog

The **Selection door groups** dialog displays all door groups allocated to the locking plan.

You can use the buttons in the toolbar to search for individual door groups by number, name or short name.

The table displays the corresponding search results. Click a column header to sort the report by a characteristic in ascending or descending order. Click an entry to directly apply the corresponding record to the invoking dialog.

<input type="checkbox"/>	Number ▲	Name	Short name
<input type="checkbox"/>	1	London-NewYork	

Number of records: 1

4.8.2 Person groups

Persons with the same properties with respect to access permissions are combined in the person groups. Grouping allows the locking plan to be displayed in a compact format and simplifies the assignment of access permissions.

"Selection Person groups" dialog

The **Selection Person groups** dialog displays all person groups created in the access control system for the locking plan administration.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number ▲	Name	Short name	Delete
<input type="checkbox"/>	1	Administration	A	

Number of records: 1

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit person group" dialog

Use the **Edit person group** dialog to create new person groups and edit existing person groups for locking plan administration. Each person group requires a unique number; it is recommended that you specify a name and a short name.

Use the buttons in the toolbar to navigate between records, create or delete a record and save or discard changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Available persons report:

Contains all persons not allocated to a person group. Click a person to select the entry and then click the right arrow to allocate the person to the group.

Allocated persons report:

Contains all persons allocated to the person group. Click a person to select the entry and then click the left arrow to remove this person from the group.

Note: To select several entries simultaneously press the Ctrl key while clicking.

Note: Persons who have left the company are not included in this selection.

4.8.3 Door groups

You combine doors with the same properties with respect to access permissions in the door groups. Grouping allows the locking plans to be displayed in a compact format and simplifies the assignment of access permissions.

"Selection Door groups" dialog

The **Selection door groups** dialog displays all door groups created in the access control system for locking plan administration.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

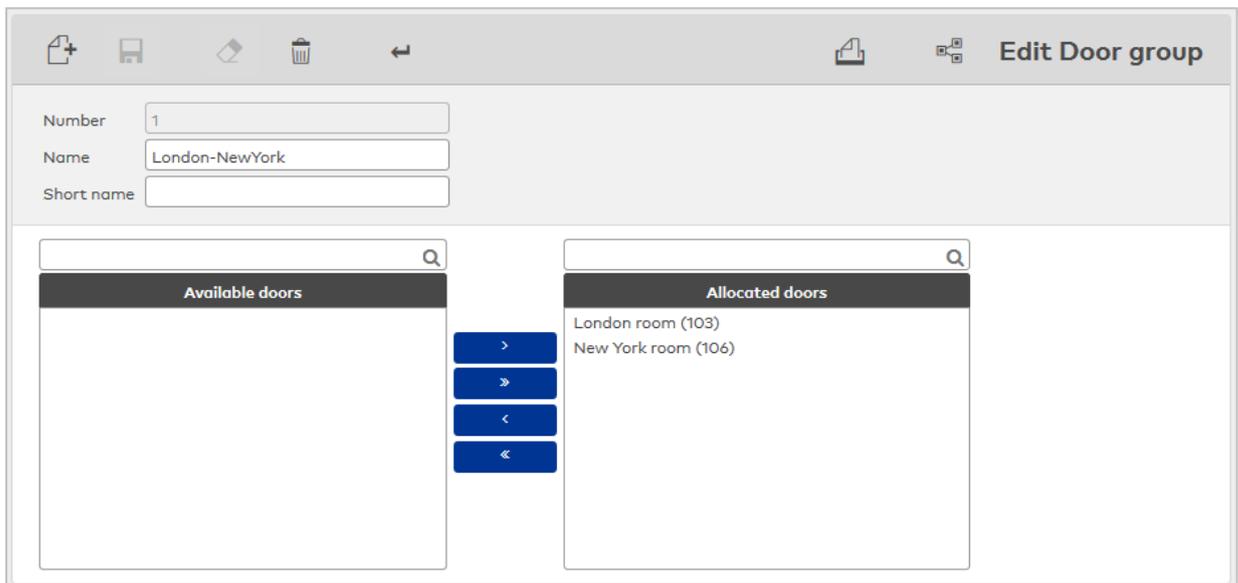


Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Door group" dialog

Use the **Edit Door group** dialog to create new door groups and edit existing door groups for the locking plan administration. Each door group requires a unique number; it is recommended that you specify a name and a short name.

Use the buttons in the toolbar to navigate between records, create or delete a record and save or discard changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Available doors report:

Contains all doors that can be allocated to the door group. All doors are available which have been assigned a reader, have not been added to another door group, do not belong to a room zone and for which no permissions or special permissions have been allocated. Click a door to select it and then click the right arrow to allocate the door to the group.

Allocated doors report:

Contains all doors allocated to the door group. Click a door to select it, then click the left arrow to remove the door from the group.

Note: To select several entries simultaneously press the Ctrl key while clicking.

4.9 Additional functions

This menu contains additional functions and applications for the access system.

Use the **Corrections** menu item to make corrections to employee master data and access profiles.

Use the **Interlocks** menu item to manage the interlocks.

Use the **Lifts** menu item to manage the lifts.

Use the **Intruder detection systems** menu item to manage the intruder detection systems.

4.9.1 Corrections

Changes can be made to the master data records using corrections. The dialog is designed to make many different types of corrections and also allows you to enter many corrections at the same time. The dialog provides a generating function and a related searching procedure for applying the same corrections to different master data. Input entries in the dialog interface are saved as correction records in the database and processed in a correction process. Corrections are applied directly to the master data and are valid immediately.

"Edit corrections" dialog

Use the **Edit Corrections** dialog to record the various corrections and display incorrectly processed correction records for revision. The input fields are located in the upper section of the dialog and the corrections already recorded or incorrectly processed are displayed in the lower section.

Use the buttons on the toolbar to save and discard the correction inputs and start processing corrections or print or delete the displayed records. You can display the progress of correction processing by clicking the **Refresh** button.

Correction type	Number/name	Valid from	Valid until	Parameter	Error message
Person - change office release	5 - Hochmeyer, Gertrud			Office release = 1	
Person - change office release	9 - Kamp, Karsten			Office release = 1	
External company employee - change master data	102 - Schilling, Wolfgang			Field name=E-mail, Value=ps@schilling.de	

Number of records: 3

Corrections are recorded or edited in the input line. The composition of the line matches the correction type selected.

Correction type selection field:

Selecting the correction type determines the master data reference and the parameter fields in the input line.

Search button (magnifier):

Opens a selection dialog that is based on the correction types. One or more records can be chosen from this dialog. If you select multiple records, an * is displayed into the input field.

If a correction type for which a correction filter has been stored is selected, you can use the magnifier to open a filter criteria input dialog for flexible searching.

Other **selection and input fields**:

The other selection and input fields relate to the correction type selected.

Apply button:

Use this button to create the correction records and transfer them into the table. One correction record is generated for each master data record.

Corrections () progress display

After startup, the number of corrections is displayed with the current status. These are updated at time intervals of 2 seconds in order to show the progress.

Total	Number of corrections in the table
Open	Corrections that must still be processed
Failed	Corrections that could not be completed; the entries remain in the table where they can be corrected or deleted.
New	Newly entered corrections for which correction processing has not yet been triggered

Table:

The table displays all correction records that have been newly created but not yet processed. The correction records can be deleted or modified. Click the **Change line** button of a correction record. The entry will then be loaded into the input line and can be directly altered.

Correction type column:

Displays the type of correction for the correction record.

Number/name column:

Displays the number and name of the master data records to which the correction is applied.

Valid from/valid until column:

Enter a start and end date for validity.

Parameter column:

Displays the parameters required for correction. The master data reference and the new value are displayed, respectively.

Error message column:

Displays a message if a correction record could not be processed.

4.9.2 Interlocks

The system provides interlock control for the controlled transition between rooms. Contact mats, motion detectors or buttons can act as sensors.

To set up an interlock, allocate an interlock function to the doors or readers and specify the inputs and outputs of the connections for the sensors. The interlock is then controlled using the reader definition.

Three additional inputs are provided for the interlock control to include additional functions and conditions in the interlock control.

The three inputs can be used as follows:

- Contact mats
- Motion detectors
- Emergency override switch

"Selection Interlocks" dialog

The **Selection Interlocks** dialog displays all interlocks created in the access system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Interlock" dialog

Use the **Edit Interlock** dialog to create new interlocks and edit existing interlocks. Each interlock requires a unique number; it is recommended that you specify a name and a short name.

You must allocate to an interlock the required doors and their readers as input or output reader. As the terminals control the interlocks, an interlock can only be mapped by doors with readers and inputs/outputs controlled by a terminal.

You can use the buttons in the toolbar to navigate between records, to create a new record, to copy, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Door number	Door name	Mandatory passage complete	Reader number	Reader name	Reader location
71	Interlock 1	<input type="checkbox"/>	71	Sluice 1	<input type="radio"/> Not <input checked="" type="radio"/> Inside <input type="radio"/> Outside
72	Interlock 2	<input type="checkbox"/>	72	Sluice 2	<input type="radio"/> Not <input type="radio"/> Inside <input checked="" type="radio"/> Outside
73	Stores P8	<input type="checkbox"/>	73	Reader Depot P8	<input checked="" type="radio"/> Not <input type="radio"/> Inside <input type="radio"/> Outside

Terminal selection field:

Contains the terminal that controls the interlock. When the terminal is selected, the table displays the readers connected to the terminal. At the same time, the choice of terminal determines which input and output can be used for the interlock.

Motion detector selection field:

Contains the input for the motion detector. Select from the list the input to which the motion detector is connected. The selection depends on the terminal that is selected.

Contact mat selection field:

Contains the input for the contact mat. Select from the list the input to which the contact mat is connected. The selection depends on the terminal that is selected.

Emergency override switch selection field:

Contains the input for the interlock opening. Select from the list the input to which a button for opening the interlock is connected. The selection depends on the terminal that is selected.

Note: This button opens the interlock without checking the conditions.

Table:

Door number column:

Displays the unique number of the door that is controlled by the selected terminal.

Door name column:

Displays the name for door in the respective language.

Mandatory passage complete column:

Defines the door as a mandatory passage complete. A mandatory passage complete can only be passed in one direction, that is, you cannot leave using the door through which you entered.

Reader number column:

Displays the unique number of the reader that is allocated to the door. If several readers are allocated to one door, the door number and door name fields are displayed only for the first reader.

Reader name column:

Displays the name of the reader.

Reader location column:

Allocates the reader to the interlock. Select the **Internal** option for an output reader. Select the **External** option for an input reader. With the **Not** default option, the reader is not part of the interlock.

4.9.3 Lifts

The system provides a lift control for the controlled use of lifts. In addition to the general use of the lift, you can assign rights for individual floor levels, where each floor level is represented by a room zone.

Rights allocation is connected with a room zone and corresponds with the access permissions for that room zone.

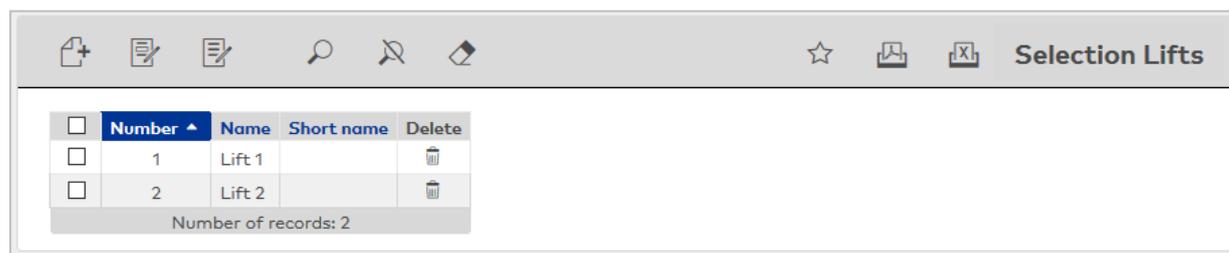
Further information on integrating lifts into access control systems can be found in the section "Work with the system" under [►Create a lift control](#)".

"Selection Lifts" dialog

The **Selection Lifts** dialog displays all lifts created in the access system. Each lift is represented by a unique number, a name and a short name.

Use the buttons on the toolbar to create new lifts, edit selected lifts or print a report containing records displayed. Use the search function to search for individual lifts using their number, name or short name.

The table displays the corresponding search results. Click a column header to sort the report by a characteristic in ascending or descending order. Click an entry to open the relevant record.



<input type="checkbox"/>	Number ▲	Name	Short name	Delete
<input type="checkbox"/>	1	Lift 1		
<input type="checkbox"/>	2	Lift 2		

Number of records: 2

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

Number column:

contains the unique number for the lift.

Name column:

Contains the name for the lift in the respective language.

Short name column:

Contains the short name for the lift in the respective language.

Delete column:

Deletes the record. Before the record is finally deleted, the system displays a confirmation request. If you click **OK**, the record is irrevocably deleted and cannot be recovered.

"Edit Lift" dialog

Use the **Edit Lift** dialog to create new lifts and edit existing lifts.

The lift control requires a terminal and a reader. Entering the number of floor levels sets the lines in the table. Each line corresponds to one floor level. Because access to a floor level is assigned by room zones, you have to allocate a room zone to each floor level to provide access.

Floor	Description	Room zone		
1	A1, 1F	3 - Administration and others		
2	A1, 1F	3 - Administration and others		
3	A1, 1F	3 - Administration and others		

Terminal selection field:

Contains the terminal that controls the lift. Only terminals not allocated to a lift control are available.

Reader selection field:

Selection of readers located in the lift. All readers managed by the terminal are displayed.

Note: If the terminal is changed, all floor level allocations are lost.

Table:

The table contains the floors with the allocated room zones.

Only the last line of the table can be deleted to prevent gaps in the floors.

Note: If the data groups option is activated, you cannot edit floors that refer to a room zone to which the user does not have access.

Floor column:

Contains the floor number.

Description column:

Free text field with the description for the floor.

Room zone column:

Selection of room zones representing the floors.

4.9.4 Intruder detection systems

MATRIX allows simple IDS applications or VdS-compliant applications for more stringent requirements to be integrated into the system.

Note: This function is only available if the system parameter "Access 130" is activated.

The following applications are supported:

- Standard IDS: Simplest form of the connection of an intruder detection system via inputs and outputs.
- IDS with reader blocks: Simple form of connecting an intruder detection system via inputs and outputs with the option of reader shut down in the IDS security area.
- IDS Comfort with reader blocking: Extended dialog interface with additional settings and options.
- Comfort IDS (VdS-compliant): The VdS-relevant fields are greyed out and are for information only.
- Comfort IDS with OII: Intruder detection system with integration via Open Intrusion Interface.
- Comfort IDS with OII (VdS-compliant): VdS-compliant integration of an intruder detection system with Open Intrusion Interface.

The assignments of rights for arming/disarming an intruder detection system is based on access permissions and can be assigned to the activation reader of the intruder detection system as well as to any other reader in the access system.

It is also possible to switch off readers or assign additional functions to readers. Please note the following:

- All terminals must be LAN terminals (2-wire terminals are not allowed).
- The number of terminals is limited to a maximum of 10.
- The terminals must be in one communication zone (inter-terminal communication).
- evolo wireless components can be inactivated or blocked by arming the IDS but cannot arm or disarm the system themselves.

Further information on integrating intruder detection systems can be found in the section "Work with the system" under [► Set up an IDS connection](#).

Arming via counting information

In addition to manual arming via an arming reader, areas can also be armed via the counting information if the counting information counter for an area is "0". This function is enabled in the **Security areas – doors** dialog in the **Counting information** tab.

"New intruder detection system" dialog

The **New intruder detection system** dialog displays the available templates for intruder detection system types. Select a template to transfer the standard settings for this connection to the **Edit Intruder detection system** dialog. The configurable parameters depend on the connection of the intruder detection system.

Use the **Back to selection** button in the toolbar to return to the selection dialog.

← Intruder detection systems type	
Name	Description
Standard IDS	Most basic integration of an intruder detection system via inputs and outputs.
IDS with reader blocks	Simple integration of an intruder detection system via inputs and outputs including the possibility to disable readers in the IDS area.
IDS Comfort with reader blocking	Easy integration of an intruder detection system via inputs and outputs including the possibility to disable readers in the IDS area.
Comfort IDS (VdS-compliant)	VdS-compliant integration of an intruder detection system.
Comfort IDS with OII	Intruder detection system with integration via Open Intrusion Interface
Comfort IDS with OII (VdS-compliant)	VdS-compliant integration of an intruder detection system with Open Intrusion Interface

Standard IDS:

Simplest way of connecting an intruder detection system via inputs and outputs on a reader.

IDS with reader blocks:

Simple way of connecting an intruder detection system via inputs and outputs on a reader with the additional option of reader shut-down in the IDS area.

IDS Comfort with reader blocking:

Convenient connection of an intruder detection system via inputs and outputs with the option of reader shut down in the IDS area and other options:

- An area can be armed or disarmed via several readers.
- There can be readers to arm an area and other readers to disarm the area, or readers which can do both.
- A terminal can manage up to four security areas.
- Configurable reader block display for the readers.
- Configuration block for the terminal: Changes to the terminal configuration are not permitted, if an IDS is armed. The terminal accepts no orders while the IDS is armed.
- Configurable IDS activation duration. This is the maximum time between the request to arm the IDS and the response from the IDS that it is ready to be armed.
- Tampering monitoring: for arming. No activation, if one of the anti-tamper switches monitored by the terminal reports tampering. This also affects the anti-tamper switches of all readers connected to the terminal.

VdS-compliant IDS:

VdS-compliant intruder detection system connection which also meets further requirements for the IDS Comfort:

- At least two activation areas.
- Configuration block is always active when the IDS is armed. This setting cannot be changed in the configuration and is only displayed for information.
- This reader block is not indicated by the LED of the readers. This setting cannot be changed in the configuration and is only displayed for information.

Comfort IDS with OII:

Intruder detection system with integration via Open Intrusion Interface.

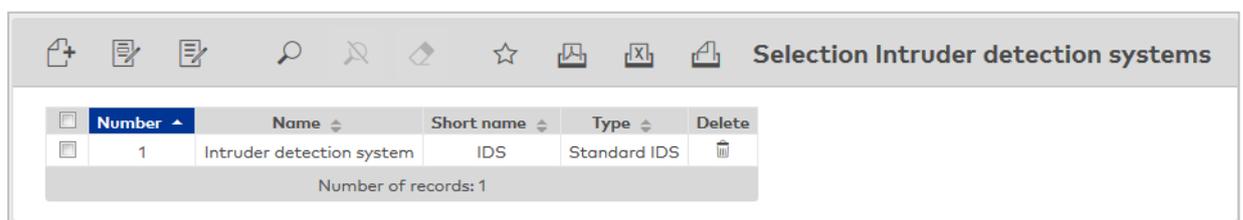
Comfort IDS with OII (VdS compliant):

VdS-compliant integration of an intruder detection system with Open Intrusion Interface.

"Selection intruder detection systems" dialog

The **Selection Intruder detection systems** dialog displays all intruder detection systems created in the access system.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

**Type** column:

Contains the selected intruder detection system types.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit intruder detection system" dialog

Use the **Edit Intruder detection system** dialog to create new intruder detection systems and edit existing intruder detection systems. Each intruder detection system requires a unique number. It is recommended to specify a name and a short name.

A terminal, a reader and the corresponding inputs and outputs are required as a minimum to connect an intruder detection system.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

The dialog contains different fields and options depending on the selected IDS type. The header data are the same for all IDS types.

IDS type display field:

Contains the IDS type selected for the new entry.

Standard IDS

Standard IDS is the simplest type of IDS connection with only one reader.

Terminal selection field:

Contains the terminal for connection of the intruder detection system. Only terminals not allocated to an IDS are available.

Reader selection field:

Selection of the reader for arming/disarming the intruder detection system. All readers managed by the terminal are displayed.

IDS switch output; arm or disarm selection field:

Specification of an output on which the intruder detection system is armed/disarmed. All outputs available to the terminal are displayed.

IDS input "ready to be armed" status selection field:

Selection of the input on which the intruder detection system indicates the readiness to be armed. All inputs available to the terminal are displayed.

IDS input status; armed or disarmed selection field:

Selection of the input on which the intruder detection system indicates that it is armed. All inputs available to the terminal are displayed.

IDS with reader blocks

In addition to the standard fields for the connection of an intruder detection system, an additional input for the reader shut-down is required. You can include all readers controlled by the selected terminal in the reader shut-down.

The screenshot displays a configuration interface for an Intruder Detection System (IDS). At the top, there are several dropdown menus for selection:

- Terminal:** 1200 - B6L-4P Terminal
- Reader:** 7 - Reader 7
- IDS switch output; arm or disarm:** (empty)
- IDS input "ready to be armed" status:** (empty)
- IDS input status; armed or disarmed:** (empty)
- Input for reader shut down:** (empty)

Below these fields is the **IDS area shut down** section, which contains two panels:

- Available readers:** A list showing "8 - Reader 8" and "9 - Reader 9".
- Allocated readers:** An empty list.

Between the two panels are four blue arrow buttons: a right-pointing arrow (>), a double right-pointing arrow (>>), a left-pointing arrow (<), and a double left-pointing arrow (<<), used for moving readers between the available and allocated lists.

Terminal selection field:

Contains the terminal for connection of the intruder detection system. Only terminals not allocated to an IDS are available.

Reader selection field:

Selection of the reader for arming/disarming the intruder detection system. All readers managed by the terminal are displayed.

IDS switch output; arm or disarm selection field:

Specification of an output on which the intruder detection system is armed/disarmed. All outputs available to the terminal are displayed.

IDS input "ready to be armed" status selection field:

Selection of the input on which the intruder detection system indicates the readiness to be armed. All inputs available to the terminal are displayed.

IDS input status; armed or disarmed selection field:

Selection of the input on which the intruder detection system indicates that it is armed. All inputs available to the terminal are displayed.

Input for reader shut down selection field:

Select the input used to shut down the selected reader. All inputs available to the terminal may be selected.

IDS area shut down selection reports:

Use the selection reports to assign which readers are to be shut down.

Comfort IDS with reader blocking

Reader locations and security areas affected by the IDS are configured for the selected terminal. Signals can be assigned to additional inputs/outputs for each security area using the advanced input/output definition settings.

Terminal	1200 - B6L-4P Terminal
Configuration blocked when IDS is activated	<input checked="" type="checkbox"/>
Tampering monitoring	<input checked="" type="checkbox"/>
Number of IDS security areas	2

Terminal selection field:

Contains the terminal for connection of the intruder detection system.

Options: Only terminals that are linked to the IDS and to which no intruder detection system has yet been connected are available for selection.

Configuration blocked when IDS is activated checkbox:

If the configuration block is activated, the terminal will cease to accept any configuration data as soon as the IDS is armed.

Note: The configuration block will not become active until each IDS security area has been successfully armed and disarmed once.

Tampering monitoring checkbox:

Determines the behaviour of the terminal with a monitored anti-tamper switch. Activate the tampering monitoring if the terminal should not be armed while an anti-tamper switch is still reporting tampering. Tampering monitoring is related to the anti-tamper switches in all devices connected to the terminal, such as readers, I/O modules and MUX, irrespective of whether they are linked to the activation area or not.

Options:

- Activated: the terminal cannot be armed if there is a tamper message.
- Not activated: the terminal is armed without taking the anti-tamper switches into account.

Default value: Not activated.

Number of activation areas selection field:

Determines the number of security areas which are managed by the terminal in connection with the IDS. Depending on the number, further area blocks will be shown in the dialog and can be used to configure each security area separately.

Options:

1-4 areas

Default value: 1

"General" tab

This tab contains the IDS security areas to be monitored and the settings for the readers managed by the terminal.

General
Further input/output definitions

Area 1

IDS switch output; arm or disarm

IDS input "ready to be armed" status

IDS input status; armed or disarmed

Access block signalling

Max. activation duration (seconds)

TMBasic program

TMBasic start parameter

Terminal	Reader	Reader action	IDS security area
1200 AM 92 00 - Terminal	7 Reader 7	Activate IDS	Area 1
1200 AM 92 00 - Terminal	8 Reader 8	Block reader when IDS is activated	Area 1
1200 AM 92 00 - Terminal	9 Reader 9	Custom function	

Add further readers from terminal

Add further readers from gateway

Areas 1–4:

1, 2, 3 or 4 blocks are displayed, depending on the configured number of areas.

IDS switch output; arm or disarm selection field:

Specification of an output on which the intruder detection system is armed/disarmed. All outputs available to the terminal are displayed.

IDS input "ready to be armed" status selection field:

Selection of the input on which the intruder detection system indicates the readiness to be armed. All inputs available to the terminal are displayed.

IDS input status; armed or disarmed selection field:

Selection of the input on which the intruder detection system indicates that it is armed. All inputs available to the terminal are displayed.

Access block signalling checkbox:

Indicates if the readers signal that they are armed.

- Activated: A red LED on the reader indicates that it is armed.
- Not activated: the readers do not indicate that they are armed.

Note: The setting depends on the reader and cannot be changed.

Max. activation duration input field:

Contains the maximum time in seconds which may pass after the IDS arming signal is activated until the IDS armed signal is activated by the IDS. If the IDS does not activate after this interval, the security area is not armed.

Value range: 1-99

TMBasic program selection field:

Contains an additional program for the terminal which is started when the security area is armed/disarmed.

Options:

- Blank field.
- All TMBasic programs available in the system.

Default value: Blank

TMBasic parameter input field:

Contains the start parameter for the TMBasic program. This depends on the selected TMBasic program.

Table:

The table contains all terminals and readers. For each individual reader, you can determine which functions are to be adopted for arming/disarming the IDS and to which IDS security area each reader belongs.

Terminal column:

Contains the terminal with number and name.

Reader column:

Contains the reader with number and name.

Reader action column:

The selected option determines which action the reader can trigger and how the reader should behave.

Options:

- No action: the reader is not used for the IDS.
- Block reader: the reader is blocked when the IDS is armed.
- IDS arming: the IDS can be armed via the reader.
- IDS disarming.
- IDS disarming with access.
- IDS reverse.
- IDS reverse with access.
- Individual function: This option allows to manually allocate a variable booking instruction to the reader. This function is used, for instance, when reader are to perform differing functions.
- IDS function via shortcut. This option is only available for key pad readers and allocates a shortcut to the reader which can be used to select the action.

Note: This option is only available if a keypad is allocated to the reader.

Add further readers from terminal selection field:

Used to select the readers that are to be assigned a function. The available selection contains all TP4 terminals that are present in the same communication zone as the terminal selected above. The communication zone is determined in the infrastructure nodes of the device tree.

Add further readers from gateway selection field:

Used to select the evolo wireless components that are to be assigned a function. The available selection contains all evolo wireless gateways.

Apply buttons:

These buttons enter the selected readers into the table.

"Further input/output definitions" tab

This tab contains additional inputs and outputs for the forwarding signal, the ready to be armed signal and the arming signal for each security area. 1, 2, 3 or 4 areas are shown, depending on the configured number of areas.

General		Further input/output definitions	
	Area 1		Area 2
Forwarding signal input 1	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 1	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 2	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 2	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 3	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 3	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 4	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 4	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 5	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 5	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 1	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 2	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 3	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 4	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 5	<input type="text"/>	▼	<input type="text"/>
Activation signal 1	<input type="text"/>	▼	<input type="text"/>
Activation signal 2	<input type="text"/>	▼	<input type="text"/>
Activation signal 3	<input type="text"/>	▼	<input type="text"/>
Activation signal 4	<input type="text"/>	▼	<input type="text"/>
Activation signal 5	<input type="text"/>	▼	<input type="text"/>

Forwarding signals:

Five inputs and five outputs are provided for forwarding signals. The output is activated when an input is activated.

Forwarding signal input 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Forwarding signal output 1-5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Ready to be armed signals:

Once all arming signals have been activated, these inputs need to be activated within the IDS activation duration.

Ready to be armed signal 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Arming signals:

The outputs are activated during arming.

Arming signal 1–5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Comfort IDS (VdS-compliant)

Reader locations and security areas affected by the IDS are configured for the selected terminal. Signals can be assigned to additional inputs/outputs for each security area using the advanced input/output definition settings.

Terminal	1200 - B6L-4P Terminal
Configuration blocked when IDS is activated	<input checked="" type="checkbox"/>
Tampering monitoring	<input checked="" type="checkbox"/>
Number of IDS security areas	2

Terminal selection field:

Contains the terminal for connection of the intruder detection system.

Options: Only terminals that are linked to the IDS and to which no intruder detection system has yet been connected are available for selection.

Configuration blocked when IDS is activated checkbox:

If the configuration block is activated, the terminal will cease to accept any configuration data as soon as the IDS is armed.

Note: The configuration block will not become active until each IDS security area has been successfully armed and disarmed once.

The setting is predefined for this type and cannot be changed.

Tampering monitoring checkbox:

Contains the setting determining the behaviour of the terminal with a monitored anti-tamper switch. If tampering monitoring is activated, the terminal will not be armed as long as a tamper switch still reports a tampering event.

Note: The setting is fixed for this type and cannot be changed.

Number of activation areas selection field:

Determines the number of security areas which are managed by the terminal in connection with the IDS.

Depending on the number, further area blocks will be shown in the dialog and can be used to configure each security area separately.

Options: 2–4 areas
Default value: 2

"General" tab

This tab contains the IDS areas to be monitored and the settings for the readers managed by the terminal.

General
Further input/output definitions

Area 1
Area 2

IDS switch output; arm or disarm

IDS input "ready to be armed" status

IDS input status; armed or disarmed

Access block signalling

Max. activation duration (seconds)

Terminal	Reader	Reader action	IDS security area
2000 AM 92 00 Sluice	71 Sluice 1	No action, reader not allocated to IDS	<input type="text"/>
2000 AM 92 00 Sluice	72 Sluice 2	No action, reader not allocated to IDS	<input type="text"/>
2000 AM 92 00 Sluice	73 Reader Depot B5	No action, reader not allocated to IDS	<input type="text"/>

Add further readers from terminal

Add further readers from gateway

Areas 1–4:

1, 2, 3 or 4 blocks are displayed, depending on the configured number of areas.

IDS switch output; arm or disarm selection field:

Specification of an output on which the intruder detection system is armed/disarmed. All outputs available to the terminal are displayed.

IDS input "ready to be armed" status selection field:

Selection of the input on which the intruder detection system indicates the readiness to be armed. All inputs available to the terminal are displayed.

IDS input status; armed or disarmed selection field:

Selection of the input on which the intruder detection system indicates that it is armed. All inputs available to the terminal are displayed.

Access block signalling checkbox:

Indicates if the readers signal that they are armed.

- Activated: A red LED on the reader indicates that it is armed.
- Not activated: the readers do not indicate that they are armed.

Note: The setting depends on the reader and cannot be changed.

Max. activation duration input field:

Contains the maximum time in seconds which may pass after the IDS arming signal is activated until the IDS armed signal is activated by the IDS. If the IDS does not activate after this interval, the security area is not armed.

Value range: 1-99

Table:

The table contains all terminals and readers. For each individual reader, you can determine which functions are to be adopted for arming/disarming the IDS and to which IDS security area each reader belongs.

Terminal column:

Contains the terminal with number and name.

Reader column:

Contains the reader with number and name.

Reader action column:

The selected option determines which action the reader can trigger and how the reader should behave.

Options:

- No action: the reader is not used for the IDS.
- Block reader: the reader is blocked when the IDS is armed.
- IDS arming: the IDS can be armed via the reader.
- IDS disarming.

- IDS disarming with access.
- IDS reverse.
- IDS reverse with access.
- Individual function: This option allows to manually allocate a variable booking instruction to the reader. This function is used, for instance, when reader are to perform differing functions.
- IDS function via shortcut. This option is only available for key pad readers and allocates a shortcut to the reader which can be used to select the action.

Note: This option is only available if a keypad is allocated to the reader.

Add further readers from terminal selection field:

Used to select the readers that are to be assigned a function. The available selection contains all TP4 terminals that are present in the same communication zone as the terminal selected above. The communication zone is determined in the infrastructure nodes of the device tree.

Add further readers from gateway selection field:

Used to select the evolo wireless components that are to be assigned a function. The available selection contains all evolo wireless gateways.

Apply buttons:

These buttons enter the selected readers into the table.

"Further input/output definitions" tab

This tab contains additional inputs and outputs for the forwarding signal, the ready to be armed signal and the arming signal for each security area. 1, 2, 3 or 4 areas are shown, depending on the configured number of areas.

	Area 1	Area 2
Forwarding signal input 1	<input type="text"/>	<input type="text"/>
Forwarding signal output 1	<input type="text"/>	<input type="text"/>
Forwarding signal input 2	<input type="text"/>	<input type="text"/>
Forwarding signal output 2	<input type="text"/>	<input type="text"/>
Forwarding signal input 3	<input type="text"/>	<input type="text"/>
Forwarding signal output 3	<input type="text"/>	<input type="text"/>
Forwarding signal input 4	<input type="text"/>	<input type="text"/>
Forwarding signal output 4	<input type="text"/>	<input type="text"/>
Forwarding signal input 5	<input type="text"/>	<input type="text"/>
Forwarding signal output 5	<input type="text"/>	<input type="text"/>
Ready for activation signal 1	<input type="text"/>	<input type="text"/>
Ready for activation signal 2	<input type="text"/>	<input type="text"/>
Ready for activation signal 3	<input type="text"/>	<input type="text"/>
Ready for activation signal 4	<input type="text"/>	<input type="text"/>
Ready for activation signal 5	<input type="text"/>	<input type="text"/>
Activation signal 1	<input type="text"/>	<input type="text"/>
Activation signal 2	<input type="text"/>	<input type="text"/>
Activation signal 3	<input type="text"/>	<input type="text"/>
Activation signal 4	<input type="text"/>	<input type="text"/>
Activation signal 5	<input type="text"/>	<input type="text"/>

Forwarding signals:

Five inputs and five outputs are provided for forwarding signals. The output is activated when an input is activated.

Forwarding signal input 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Forwarding signal output 1-5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Ready to be armed signals:

Once all arming signals have been activated, these inputs need to be activated within the IDS activation duration.

Ready to be armed signal 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Arming signals:

The outputs are activated during arming.

Arming signal 1-5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Comfort IDS with OII

Reader locations and security areas affected by the IDS are configured for the selected terminal. Signals can be assigned to additional inputs/outputs for each security area using the advanced input/output definition settings.

The screenshot shows a configuration panel with the following elements:

- Terminal:** A dropdown menu with the selected value "1200 - B6L-4P Terminal".
- Configuration blocked when IDS is activated:** A checked checkbox.
- Tampering monitoring:** A checked checkbox.
- Number of IDS security areas:** A dropdown menu with the selected value "2".

Terminal selection field:

Contains the terminal for connection of the intruder detection system.

Options: Only terminals that are linked to the IDS and to which no intruder detection system has yet been connected are available for selection.

Configuration blocked when IDS is activated checkbox:

If the configuration block is activated, the terminal will cease to accept any configuration data as soon as the IDS is armed.

Note: The configuration block will not become active until each IDS security area has been successfully armed and disarmed once.

Tampering monitoring checkbox:

Determines the behaviour of the terminal with a monitored anti-tamper switch. Activate the tampering

monitoring if the terminal should not be armed while an anti-tamper switch is still reporting tampering. Tampering monitoring is related to the anti-tamper switches in all devices connected to the terminal, such as readers, I/O modules and MUX, irrespective of whether they are linked to the activation area or not.

Options:

- Activated: the terminal cannot be armed if there is a tamper message.
- Not activated: the terminal is armed without taking the anti-tamper switches into account.

Default value: Not activated.

Number of activation areas selection field:

Determines the number of security areas which are managed by the terminal in connection with the IDS. Depending on the number, further area blocks will be shown in the dialog and can be used to configure each security area separately.

Options:

1-4 areas

Default value: 1

"General" tab

This tab contains the IDS security areas to be monitored and the settings for the readers managed by the terminal.

The screenshot shows the 'General' tab of a configuration window titled 'Further input/output definitions'. It contains several input fields and a table.

Fields include:

- Host name/IP (text input)
- Port (text input)
- User ID (text input)
- Password (text input)
- Area 1 and Area 2 sections, each containing:
 - Area SIID (text input)
 - Access block signalling (checkbox)
 - Max. activation duration (seconds) (text input)
 - TMBasic program (dropdown menu)
 - TMBasic start parameter (text input)

Below these fields is a table with the following structure:

Terminal	Reader	Reader action	IDS security area
1300 AM 92 00 Elevator	11 Reader Elevator	No action, reader not allocated to IDS	
1300 AM 92 00 Elevator	12 Reader Depot A4	No action, reader not allocated to IDS	

At the bottom, there are two rows of controls:

- Add further readers from terminal (dropdown menu) and Apply button
- Add further readers from gateway (dropdown menu) and Apply button

Host name/IP input field:

Contains the name or IP of the host.

Port input field:

Contains the port for the host.

User ID input field:

Contains the ID of the user.

Password input field:

Contains the password for the user.

Areas 1-4:

1, 2, 3 or 4 blocks are displayed, depending on the configured number of areas.

Area SIID input field:

To specify the SIID for the area.

Access block signalling checkbox:

Indicates if the readers signal that they are armed.

- Activated: A red LED on the reader indicates that it is armed.
- Not activated: the readers do not indicate that they are armed.

Note: The setting depends on the reader and cannot be changed.

Max. activation duration input field:

Contains the maximum time in seconds which may pass after the IDS arming signal is activated until the IDS armed signal is activated by the IDS. If the IDS does not activate after this interval, the security area is not armed.

Value range: 1-99

TMBasic program selection field:

Contains an additional program for the terminal which is started when the security area is armed/disarmed.

Options:

- Blank field.
- All TMBasic programs available in the system.

Default value: Blank

TMBasic parameter input field:

Contains the start parameter for the TMBasic program. This depends on the selected TMBasic program.

Table:

The table contains all terminals and readers. For each individual reader, you can determine which functions are to be adopted for arming/disarming the IDS and to which IDS security area each reader belongs.

Terminal column:

Contains the terminal with number and name.

Reader column:

Contains the reader with number and name.

Reader action column:

The selected option determines which action the reader can trigger and how the reader should behave.

Options:

- No action: the reader is not used for the IDS.
- Block reader: the reader is blocked when the IDS is armed.
- IDS arming: the IDS can be armed via the reader.
- IDS disarming.
- IDS disarming with access.
- IDS reverse.
- IDS reverse with access.
- Individual function: This option allows to manually allocate a variable booking instruction to the reader. This function is used, for instance, when reader are to perform differing functions.
- IDS function via shortcut. This option is only available for keypad readers and allocates a shortcut to the reader which can be used to select the action.

Note: This option is only available if a keypad is allocated to the reader.

Add further readers from terminal selection field:

Used to select the readers that are to be assigned a function. The available selection contains all TP4 terminals that are present in the same communication zone as the terminal selected above. The communication zone is determined in the infrastructure nodes of the device tree.

Add further readers from gateway selection field:

Used to select the evolo wireless components that are to be assigned a function. The available selection contains all evolo wireless gateways.

Apply buttons:

These buttons enter the selected readers into the table.

"Further input/output definitions" tab

This tab contains additional inputs and outputs for the forwarding signal, the ready to be armed signal and the arming signal for each security area. 1, 2, 3 or 4 areas are shown, depending on the configured number of areas.

General	Further input/output definitions	
	Area 1	Area 2
Forwarding signal input 1	<input type="text"/>	<input type="text"/>
Forwarding signal output 1	<input type="text"/>	<input type="text"/>
Forwarding signal input 2	<input type="text"/>	<input type="text"/>
Forwarding signal output 2	<input type="text"/>	<input type="text"/>
Forwarding signal input 3	<input type="text"/>	<input type="text"/>
Forwarding signal output 3	<input type="text"/>	<input type="text"/>
Forwarding signal input 4	<input type="text"/>	<input type="text"/>
Forwarding signal output 4	<input type="text"/>	<input type="text"/>
Forwarding signal input 5	<input type="text"/>	<input type="text"/>
Forwarding signal output 5	<input type="text"/>	<input type="text"/>
Ready for activation signal 1	<input type="text"/>	<input type="text"/>
Ready for activation signal 2	<input type="text"/>	<input type="text"/>
Ready for activation signal 3	<input type="text"/>	<input type="text"/>
Ready for activation signal 4	<input type="text"/>	<input type="text"/>
Ready for activation signal 5	<input type="text"/>	<input type="text"/>
Activation signal 1	<input type="text"/>	<input type="text"/>
Activation signal 2	<input type="text"/>	<input type="text"/>
Activation signal 3	<input type="text"/>	<input type="text"/>
Activation signal 4	<input type="text"/>	<input type="text"/>
Activation signal 5	<input type="text"/>	<input type="text"/>

Forwarding signals:

Five inputs and five outputs are provided for forwarding signals. The output is activated when an input is activated.

Forwarding signal input 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Forwarding signal output 1-5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Ready to be armed signals:

Once all arming signals have been activated, these inputs need to be activated within the IDS activation duration.

Ready to be armed signal 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Arming signals:

The outputs are activated during arming.

Arming signal 1–5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Comfort IDS with OII (VdS-compliant)

Reader locations and security areas affected by the IDS are configured for the selected terminal. Signals can be assigned to additional inputs/outputs for each security area using the advanced input/output definition settings.

Terminal	1200 - B6L-4P Terminal
Configuration blocked when IDS is activated	<input checked="" type="checkbox"/>
Tampering monitoring	<input checked="" type="checkbox"/>
Number of IDS security areas	2

Terminal selection field:

Contains the terminal for connection of the intruder detection system.

Options: Only terminals that are linked to the IDS and to which no intruder detection system has yet been connected are available for selection.

Configuration blocked when IDS is activated checkbox:

If the configuration block is activated, the terminal will cease to accept any configuration data as soon as the IDS is armed. **Note:** The configuration block will not become active until each IDS security area has been successfully armed and disarmed once.

The setting is predefined for this type and cannot be changed.

Tampering monitoring checkbox:

Contains the setting determining the behaviour of the terminal with a monitored anti-tamper switch. If tampering monitoring is activated, the terminal will not be armed as long as a tamper switch still reports a tampering event.

Note: The setting is fixed for this type and cannot be changed.

Number of activation areas selection field:

Determines the number of security areas which are managed by the terminal in connection with the IDS.

Depending on the number, further area blocks will be shown in the dialog and can be used to configure each security area separately.

Options: 2–4 areas Default value: 2

"General" tab

This tab contains the IDS areas to be monitored and the settings for the readers managed by the terminal.

General
Further input/output definitions

Host name/IP

Port

User ID

Password

Area 1

Area SIID

Access block signalling

Max. activation duration (seconds)

Area 2

Area SIID

Access block signalling

Max. activation duration (seconds)

Terminal	Reader	Reader action	IDS security area
1300 AM 92 00 Elevator	11 Reader Elevator	No action, reader not allocated to IDS ▼	<input style="width: 50px;" type="text"/> ▼
1300 AM 92 00 Elevator	12 Reader Depot A4	No action, reader not allocated to IDS ▼	<input style="width: 50px;" type="text"/> ▼

Add further readers from terminal ▼ Apply

Add further readers from gateway ▼ Apply

Host name/IP input field:

Contains the name or IP of the host.

Port input field:

Contains the port for the host.

User ID input field:

Contains the ID of the user.

Password input field:

Contains the password for the user.

Areas 1–4:

1, 2, 3 or 4 blocks are displayed, depending on the configured number of areas.

Area SIID input field:

To specify the SIID for the area.

Access block signalling checkbox:

Indicates if the readers signal that they are armed.

- Activated: A red LED on the reader indicates that it is armed.
- Not activated: the readers do not indicate that they are armed.

Note: The setting depends on the reader and cannot be changed.

Max. activation duration input field:

Contains the maximum time in seconds which may pass after the IDS arming signal is activated until the IDS armed signal is activated by the IDS. If the IDS does not activate after this interval, the security area is not armed.

Value range: 1-99

Table:

The table contains all terminals and readers. For each individual reader, you can determine which functions are to be adopted for arming/disarming the IDS and to which IDS security area each reader belongs.

Terminal column:

Contains the terminal with number and name.

Reader column:

Contains the reader with number and name.

Reader action column:

The selected option determines which action the reader can trigger and how the reader should behave.

Options:

- No action: the reader is not used for the IDS.
- Block reader: the reader is blocked when the IDS is armed.
- IDS arming: the IDS can be armed via the reader.
- IDS disarming.
- IDS disarming with access.
- IDS reverse.
- IDS reverse with access.
- Individual function: This option allows to manually allocate a variable booking instruction to the reader. This function is used, for instance, when reader are to perform differing functions.
- IDS function via shortcut. This option is only available for key pad readers and allocates a shortcut to the reader which can be used to select the action.

Note: This option is only available if a keypad is allocated to the reader.

Add further readers from terminal selection field:

Used to select the readers that are to be assigned a function. The available selection contains all TP4 terminals that are present in the same communication zone as the terminal selected above. The communication zone is determined in the infrastructure nodes of the device tree.

Add further readers from gateway selection field:

Used to select the evolo wireless components that are to be assigned a function. The available selection contains all evolo wireless gateways.

Apply buttons:

These buttons enter the selected readers into the table.

"Further input/output definitions" tab

This tab contains additional inputs and outputs for the forwarding signal, the ready to be armed signal and the arming signal for each security area. 1, 2, 3 or 4 areas are shown, depending on the configured number of areas.

General		Further input/output definitions	
	Area 1		Area 2
Forwarding signal input 1	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 1	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 2	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 2	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 3	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 3	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 4	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 4	<input type="text"/>	▼	<input type="text"/>
Forwarding signal input 5	<input type="text"/>	▼	<input type="text"/>
Forwarding signal output 5	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 1	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 2	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 3	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 4	<input type="text"/>	▼	<input type="text"/>
Ready for activation signal 5	<input type="text"/>	▼	<input type="text"/>
Activation signal 1	<input type="text"/>	▼	<input type="text"/>
Activation signal 2	<input type="text"/>	▼	<input type="text"/>
Activation signal 3	<input type="text"/>	▼	<input type="text"/>
Activation signal 4	<input type="text"/>	▼	<input type="text"/>
Activation signal 5	<input type="text"/>	▼	<input type="text"/>

Forwarding signals:

Five inputs and five outputs are provided for forwarding signals. The output is activated when an input is activated.

Forwarding signal input 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Forwarding signal output 1-5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Ready to be armed signals:

Once all arming signals have been activated, these inputs need to be activated within the IDS activation duration.

Ready to be armed signal 1-5 selection fields:

Contains the assignment of an input.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

Arming signals:

The outputs are activated during arming.

Arming signal 1–5 selection fields:

Contains the allocation of an output.

Options:

- Blank field
- All inputs managed by the terminal.

Default value: Blank

4.10 Area monitoring

Use the **Area monitoring** menu to monitor the security areas and correct the counting values. There are also functions available for placing an employee in a specific security area or room zone.

Note: Security area monitoring is only available if the security areas option and counting information option are active.

Further information can be found in the section "Working with Matrix" under the heading [► Configure the counting information option](#).

Use the **Security areas** menu item to monitor the security areas, if they are activated.

Use the **Set persons** menu item to place persons into specific room zones.

4.10.1 Security areas

The status display shows the counting values for the security areas created in area/door administration.

"Security areas" dialog

The **Security areas** dialog displays all security areas of area/door administration in a tree structure with their counting values.

Additional identifiers for the security areas provide information on the current status of the counters. The counting values can be changed or recalculated, if required.

The status display is updated depending on the update interval set in the system parameters.

You can use the buttons in the toolbar to update the status display, save the changes or recalculate the counting values.

Note: If the values are recalculated, the number of persons in the selected security area is set to 0 and then recalculated based on the bookings saved in the system.

When updated, only the current counter readings from the database are displayed.

Hierarchical representation of the security areas:

The security areas are displayed in the tree structure with their number and name as well as the counting values (in brackets).

The counting values consist of:

- the value for security area itself,
- the total value of the lower-level security areas.
- the total of the security area and the lower-level security areas.

Status symbols:

Show the current status of the security area counting value.

	No counting information
	Unknown, if no information is available from the terminals yet
	Error, if a terminal is offline, for example

Detailed view

The details of the activated area are displayed in the right-hand section of the dialog.

Persons present input field:

Contains the number of persons currently listed as present in the security area. This entry can be overwritten to correct the value. The affected terminal peripheral device is updated on saving.

4.10.2 Set persons

Use this function to set persons as present in a security area or in a room zone. This can be required in the case of incorrect bookings. For instance, when a person has not entered the security area or room zone despite making a booking, or if an area has been exited without a booking.

"Set person selection" dialog

The **Set person selection** dialog displays all persons created in the system. Click a person to open their details in the **Set person** dialog.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Note: Persons who have left the company are not included in this selection.

🔍 ✂️ 📄
☆ 📄 **Select Set persons**

Last name Employee number

First name ID card number

Department ID card label

Start search

Last name	First name	Department	Employee number	ID card number	ID card label
Akreiter	Thorsten		1	9001	001
Cermans	Paul	2 - Production	7	8203	203
Hochmeyer	Gertrud	2 - Production	5	8201	M201
Kamp	Karsten	2 - Production	9	8205	205
Leconte	Sandra	2 - Production	10	8206	206
Leroy	Fabienne	1 - Administration	4	9011	011
Martin	Eric	1 - Administration	2	9002	002
Meunier	Catherine	2 - Production	8	8204	204
Schilling	Wolfgang		102	19001	ACME 19001
Schmitz	Peter		101	19002	ACME 19002
			Number of records: 10		

"Set person" dialog

Use the **Set person** dialog to set a person in the security area or room zone in which they are actually present. With this manual intervention you can correct incorrect bookings.

Note: If security areas are activated in the system, the person is placed in the selected security area. If no security areas are activated, the person is placed in the specified room zone.

Use the button in the toolbar to return to the selection.

←
📄 📄 **Set person**

Last name Employee number

First name

Department



Select the room zone, if no security areas are activated.

Available room zones Q Set in room zone

Available Room zones selection field:

Select the room zone in which the person should be placed.

Options:

- All room zones created in the system.

Set in room zone button:

Places the person in the room zone. Click this button to set the person as present in the selected room zone.

Select the security area, if security areas are activated.

Available security areas Q Set in security area

Available security areas selection field:

Select the security area in which the person should be placed.

Options:

- All security areas created in the system.

Set in security area button:

Places the person in the security area. Click this button to set the person as present in the selected security area.



The screenshot shows a user interface element with a dropdown menu labeled 'Available security areas' containing the text 'Unknown security area'. To the right of the dropdown are two small icons: a downward arrow and a magnifying glass. Below the dropdown is a 'Present' label followed by a small square checkbox. To the right of these elements are two blue buttons: 'Set in security area' and 'Set attendance status'.

Present checkbox:

Indicates the presence status of a person for an unknown security area or an unknown room zone. You can use this option to set a person as "Present" without stating a room zone or security area. The current room zone or current security area is set for this person at the next authorised access booking.

Default value: Deactivated (absent).

Set attendance status button:

Sets the attendance status in line with the **Present** checkbox.

4.11 Door monitoring

The **Door monitoring** menu allows central control and monitoring of individual doors or door groups, if they are connected as online components to a terminal.

Use the **Status display** menu item to monitor access to doors and open and close them centrally.

Use the **Allocate door selection** menu item to allocate door selections to the status display.

Use the **Door selection** menu item to group the doors to be monitored for the selection in the status display.

4.11.1 Status display

The status display enables users, such as gatekeepers, to monitor the status of all created doors or change them manually using buttons.

The following manual status changes are possible:

- Short-term opening
- Permanent opening with limitation
- Permanent opening
- Lock

Changes can be made for individual doors or all doors. Exception: Short-term opening can only be implemented for individual doors.

Note: Permissions for changing statuses depend on the rights of the assigned user role (see: dialog **Edit User role** > Access > Door monitoring > Status display).

If manual image comparison is set up, the photo stored in MATRIX for the respective ID card can be displayed in a separate popup window during access bookings. The images from a video camera assigned to the door can be displayed at the same time (previously: video verification).

"Status display" dialog

The **Status display** dialog displays all doors in the allocated door groups with their actual status and target status. The buttons can be used to activate or end permanent opening or a block for all doors or for individual doors.

Press the image comparison symbol to display images of the booking persons stored in MATRIX.

Press the video symbol to display the camera footage from the installed video cameras (video surveillance).

Note: When it is necessary to use proxy servers or load balancers, these must be WebSocket capable to ensure that the dialog is displayed correctly.

The status display condition will be updated as soon as the assigned terminal reports a change of status.

Note: The short-term opening of the door by a booking is not displayed.

The "Permanent opening with limitation" function is not possible using all devices and firmware versions.

Use the buttons in the toolbar to update the status display manually.

The screenshot shows the 'Status display' dialog with a toolbar at the top containing icons for refresh, star, and a lock symbol. Below the toolbar, there are five buttons: 'Permanent opening with limitation', 'Permanently open', 'End permanent opening', 'Lock', and 'Cancel locking'. The main area contains a table with the following columns: Number, Name, Action, Target status, Different status, Image comparison, and Video. The table lists six doors with their respective statuses and actions.

Number	Name	Action	Target status	Different status	Image comparison	Video
101	Reception B5	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	[Video icon]
102	Paris room	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	
103	London room	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	
104	Berlin room	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	
105	Rome room	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	
106	New York room	[Icons: Lock, Open, Limit, Brief, Lock, Open, Refresh]	Unknown status		[Image comparison icon]	

Number of records: 6

Permanent opening with limitation button:

Activates immediate permanent opening of all doors displayed. Click this button to open all displayed doors immediately for all persons. The permanent opening is closed again at the end of the next permanent opening interval.

Permanently open button:

Activates immediate permanent opening of all doors displayed. Click this button to open all displayed doors immediately for all persons. The permanent opening must be ended using the **End permanent opening** button.

End permanent opening button:

All manually opened doors are immediately closed. Click this button to end the centrally-initiated permanent opening of individual or all doors. The doors return to the target status defined in door administration.

Lock button:

Immediately locks all doors displayed. Click this button to lock all displayed doors immediately for all persons. End the lock using the **Cancel locking** button. The buttons for the actions "Open briefly", "Permanent opening with limitation" and "Permanently open" are inactivated during locking.

Cancel locking button:

Immediately releases all manually locked doors. Click this button to end the centrally-initiated locking of individual doors or all doors. The doors return to the target status defined in door administration. This does

not end locking that was initiated due to an activated intruder detection system. All permanent openings that were active before a block are inactivated once the block is revoked.

Table:

Number column:

Contains the unique number for the door.

Name column:

Contains the name for door in the respective language.

Action column:

Enables individual doors to be opened and closed centrally.

 Open briefly	Opens an individual door for the period of the door release pulse length.
 Permanent opening with limitation	Opens an individual door permanently until the end of the next permanent opening interval, regardless of the target status.
 Permanently open	Opens an individual door permanently, regardless of the target status. Permanent opening must be ended centrally.
 End permanent opening	Resets the individual door back to the target status after manual permanent opening.
 Lock	Locks an individual door immediately, regardless of the target status. Locking must be ended manually.
 Cancel locking	Resets the individual door back to the target status after manual locking.

Target status column:

Displays the target status of the door defined in door administration.

 Permanently open	Door is unlocked due to permanent opening.
 Office release	Door is opened with office release.
 No access	Access is not possible.
 Access	Door is closed, access only possible with access permission.
 Office release possible	Door is closed, office release is possible.

Different status column:

Displays the current status if it deviates from the target status. Critical status messages are displayed with a flashing icon:

 Manual permanent opening	The door is open and differs from the target status.	Click End permanent opening to return the door to the target status.
 Door manually locked	The door is locked contrary to the target status.	Click Cancel locking to return the door to the target status.
 Unknown (flashing)	Warning: The door status is unknown!	Check the status of the door.
 Open (flashing)	Warning: The door was not closed after it was opened and the door open time has expired!	Check the status of the door.

 Forced entry (flashing)	Warning: The door was opened without a booking!	Check the status of the door.
 Door offline (flashing)	Warning: There is no connection to the terminal!	Check that the terminal is available.

Image comparison column:

If no cameras are configured for the door, the persons symbol will be displayed. The camera symbol is displayed for doors at which manual image comparison using video surveillance has been set up. Clicking on the symbol opens image comparison in a separate popup dialog. You can monitor multiple doors simultaneously by arranging the windows side by side.

Video column:

A camera symbol is displayed for doors on which video cameras are installed. Clicking on the camera icon opens the current camera image in a separate popup dialog. You can monitor multiple cameras simultaneously by arranging the windows side by side.

Popup dialog "Manual image comparison"

The popup dialog is an access control component of MATRIX. It is opened from the door monitoring status display by clicking on a symbol in the **Image comparison** column.

Note 1: An open popup dialog keeps the browser session open. If a user has opened a popup dialog, the MATRIX session will not time out, even if no other user activities take place.

Note 2: A user can open any number of doors in parallel. One and the same door can be opened by different users at the same time.



 Sound on booking


Reception B5

Booking time **1/14/2021 14:59**

Last name **Gert Hochmeyer**

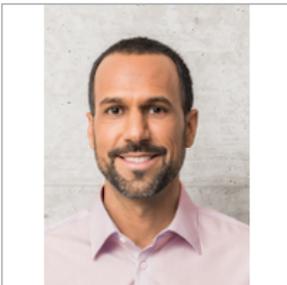
Department/company **Production**

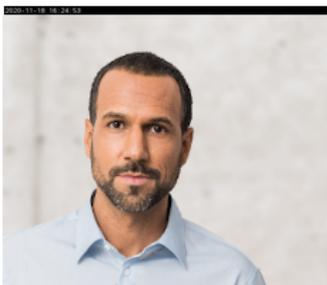
ID card number **8201**

Allow access

Deny access

Remaining time 0







Toolbar

Checkbox **Sound on booking:**

Specifies whether every booking should be signalled by a booking sound.

Buttons **Small/medium/large:**

Specifies the size of the displayed photos and camera images. This always applies to the current popup dialog.

Name:

Shows the name of the door.

Dialog header

The dialog header shows the booking time, name, department or company and the ID card number of the person currently booking.

Additional permission buttons are shown during online bookings.

Permit access button:

Allows access through the door.

Deny access button:

Denies access through the door.

Remaining time counter:

If access is not allowed, it will be automatically denied once this time has elapsed.

Note: It is possible for multiple users to have the same door open in manual image comparison at the same time. In this case, the first action will always be performed. The user name is logged.

Main window

Top left image:

Shows the picture of the currently booking person that is stored in MATRIX. The image is updated with every new booking.

Top right camera image:

Shows the image from a identification camera installed at the door, if present.

Bottom additional camera image:

Shows the image from a background camera installed at the door, if present. If multiple background cameras are installed, multiple camera images are shown side by side.

Camera control:

Hovering the mouse over the camera images opens the PTZ controls of the ONVIF camera. The PTZ controls can be operated directly from this dialog.

4.11.2 Allocate door selection

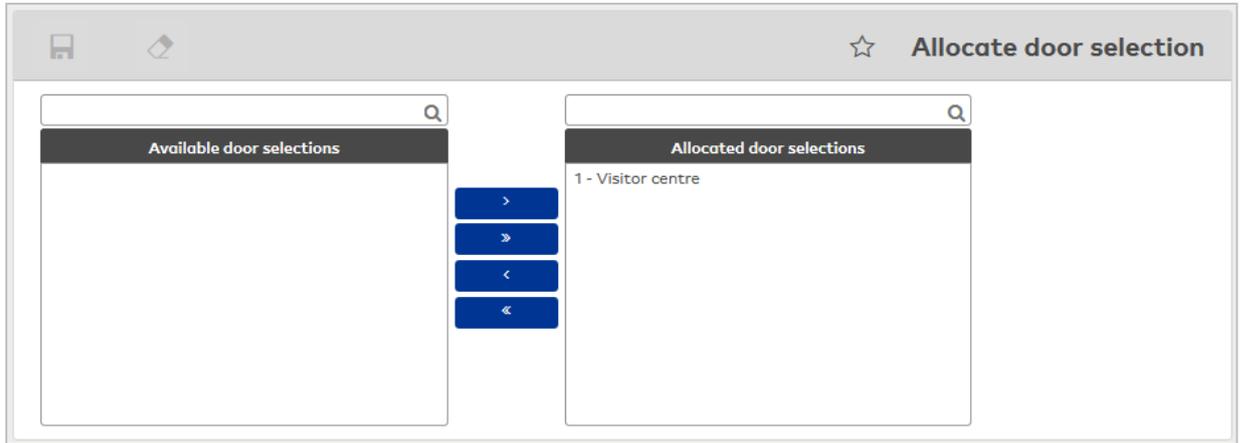
You must allocate door selections to the status display for the display. Using the door selections the status display can quickly be switched between different monitoring areas.

"Allocate door selection" dialog

Use the **Allocate door selection** dialog to determine the door selections that are to be monitored in the status display.

The selection is saved in the user profile and is reopened each time the user logs in.

Use the buttons in the toolbar to save or discard the selection. Use the **Search** button to return to the status display.



Available door selections report:

Contains all door selections created. Click a door selection to select it and then click the right arrow. All doors in the selected door selection are displayed in the status display.

Allocated door selections report:

Contains all door selections that are displayed in the status display. Click a door selection to select it and then click the left arrow to remove this door selection from the status display.

Note: To select several entries simultaneously press the Ctrl key while clicking.

4.11.3 Door selection

The door selection enables grouping doors to simplify the selection of the doors to be monitored in the status display.

"Selection door selection" dialog

The **Selection Door selection** dialog displays all door selections created.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit door selection" dialog

Use the **Edit Door selection** dialog to create new door selections and edit existing records. Each door selection requires a unique number; it is recommended that you specify a description and a short description.

Doors are grouped into door selections not necessarily using physically delimited areas; instead, they comprise doors that have to be monitored together. When you assign such areas a name, you should base the names on your company's local or organisational structure.

You can use the buttons in the toolbar to navigate between records, to create, delete or print a record and to save or reject changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Available doors report:

Contains all doors created (only online components) that can be allocated to the door selection. Click a door to select it and then click the right arrow. The selected door is added to the door selection.

Allocated doors report:

Contains all doors allocated to the door selection. Click a door to select it, then click the left arrow to remove this door from the door group.

Note: To select several doors simultaneously press the Ctrl key while clicking.

4.12 Patrol

Each patrol consists of a report of readers which have to be passed in a specified order. If necessary, you can monitor the time for the stage between two readers.

Note: The following online components are available as checkpoints for the patrol.

A security guard is managed in the system like any other person. The only difference is the allocation of a patrol and a security guard ID, which is part of the employee record. You can use the security guard allocation to allocate a security guard to a patrol. The patrol is activated by the booking at the first reader of the patrol, and time control is started if a patrol time has been set.

Use the **status display** menu item to monitor the active patrols.

Use the **Patrols** menu item to assign patrols to the security guards.

Use the **Patrol definitions** menu item to manage the patrol definitions to determine the patrols and, if required, the maximum times required by the security guards between the checkpoints.

Use the **Patrols log** menu item to view the finished patrols and control when particular security guards reported at a checkpoint.

4.12.1 Status display

Use the status display to monitor and check the active patrols.

As this dialog is merely for monitoring, it is displayed as a pop-up dialog.

The display is updated in accordance with the system parameter for the update interval.

"Status display" dialog

The **Status display** dialog displays all active patrols and their current status.

The status display is updated depending on the update interval set in the system parameters.

You can use the buttons in the toolbar to update the status display manually.

Action	State	Number	Name	Start	Security guard	Last reader	Next reader	Booking no later than
	Active	2	Ronde 2	Jan 5, 2016 4:05:32 PM	2 Martin, Eric		2 Reader 2	Jun 12, 2017 12:17:52 PM
	Failed	1	Ronde 1	Jan 5, 2016 4:06:34 PM	7 Cermans, Paul		1 Reader 1	Jan 5, 2016 4:36:34 PM
Number of records: 2								
Last update: 06/12/2017 11:48:01								

Action column:

You can use the symbols in this column to finish, interrupt or resume the patrol manually.

Possible actions depending on the status:

Status	Possible actions
Active	Interrupt or finish
Interrupted	Resume or finish
Failed	Finish

Note: A patrol is no longer displayed once it is completed.

State column:

Displays the current state of the patrol.

Possible state values:

- Planned: the patrol is planned, but not yet started.
- Active: the patrol has started and is within the specified time.
- Failed: the booking was late.
- Interrupted: the patrol was manually interrupted.
- Finished: the patrol is finished.

Number column:

Contains the unique number for the patrol.

Name column:

Contains the name for the patrol in the respective language.

Start column:

Contains the time when the patrol was started.

Security guard column:

Contains the last and first names of the security guard who carries out the patrol.

Last reader column:

Contains the reader on which the most recent booking took place.

Next reader column:

Contains the reader on which the next control booking should take place.

Booking no later than:

Contains the remaining time in which the next control booking should take place.

4.12.2 Patrols

To activate a patrol, you have to allocate the patrol to a security guard. When a booking is made to the first reader on the patrol it is listed as active in the table.

You can select a security guard for the patrol in the **Edit Patrol** dialog.

"Selection Patrols" dialog

The **Selection Patrols** dialog displays all patrols created. The status and the allocated security guard of active patrols are also displayed. Active patrols can be ended or interrupted using the action buttons. Patrols can be activated in the **Edit Patrol** dialog by allocating a security guard.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Action	State	Number	Name	Short name	Start time	Security guard	Action
		1	Patrol 1				
		2	Patrol 2				
		3	Patrol 3				

Number of records: 3

Action column:

You can use the symbols in this column to finish, interrupt or resume the patrol manually.

Possible actions depending on the status:

Status	Possible actions
Active	Interrupt or finish
Interrupted	Resume or finish
Failed	Finish

Note: If a patrol was terminated, only the patrol definition for the allocation of a new security guard is displayed.

State column:

Displays the current state of the patrol.

Possible state values:

(empty)	The patrol is planned, but has not yet been started.
Active	The patrol has been started and is within the specified time.
Interrupted	The patrol was manually interrupted.
Failed	The booking was late.

Number column:

Contains the unique number for the patrol.

Name column:

Contains the name for the patrol in the respective language.

Short name column:

Contains the short name for the patrol in the respective language.

Start time column:

Contains the date and time the patrol was started.

Security guard column:

Contains the allocated security guard.

Action column:

The action allows a planned patrol to be deleted before activation. Patrols to which no security guard is allocated and active patrols cannot be deleted.

"Edit Patrol" dialog

Use the **Edit Patrol** dialog to allocate a security guard to the patrol.

When a security guard is allocated to a patrol, the patrol is activated and shown in the status display, provided a patrol time has been defined for the route to the first door/reader.

If no patrol time is defined, the patrol has the status 'ready'. In this case, the patrol is initiated by the booking at the first door/reader.

Note: Once the allocation has been saved, an active patrol can no longer be changed.

Use the buttons in the toolbar to navigate between records, create or delete a record and save or discard changes made to the record. Use the **Back to selection** button to return to the selection dialog.

Checkpoint	Door (Reader)	Patrol time (minutes)
	1 Administration - main entrance (1 Reader 1)	5
	2 A-P connecting door (2 Reader 2)	5
	2 A-P connecting door (3 Reader 3)	5
	8 Production - rolling gate (8 Reader 8)	

Number display field:

Contains the unique number for the patrol.

Name display field:

Contains the name for the patrol.

Short name input field:

Contains the short name for the patrol.

Allocated security guard:

You can use the search function  to open the security guard selection dialog for allocating a security guard to the patrol.

Employee number display field:

Contains the employee number of the allocated security guard.

Name display field:

Contains the last name of the allocated security guard.

First name display field:

Contains the first name of the allocated security guard.

Comment display field:

Contains remarks and information on the patrol, provided these have been entered in the patrol definition.

Access profile display field:

Contains the access profile required for the patrol. By allocating a security guard to a patrol, the specified access profile is allocated to the security guard so that he has the necessary access permissions for the patrol.

Checkpoint table:

The table displays the checkpoints of the patrol.

Reader column:

Contains the reader that represents the checkpoint.

Patrol time column:

Contains the time required by the security guard to reach this checkpoint.

"Selection persons" dialog

Use the **Selection Persons** dialog to search for persons and directly apply them to the invoking dialog.

Note: When the **Several ID cards per person** option is active, an individual record for the person is displayed in the table for every ID card.

      Selection Persons 						
Last name ▲	First name ⇅	Department ⇅	Employee number ⇅	ID card number ⇅	ID card label ⇅	Blocked ⇅
Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>

Click an entry to directly apply the corresponding record.

4.12.3 Patrol definitions

Use the patrol definitions to describe the patrols for your company's security guards. A patrol is based on the doors/readers which a security guard must pass. If required, you can specify the time required by the security guard for the stage between two doors/readers. If this time is exceeded, the deviation is shown on the status display and in the selection dialog.

"Selection Patrol definitions" dialog

The **Selection Patrol definitions** dialog displays all patrol definitions created.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

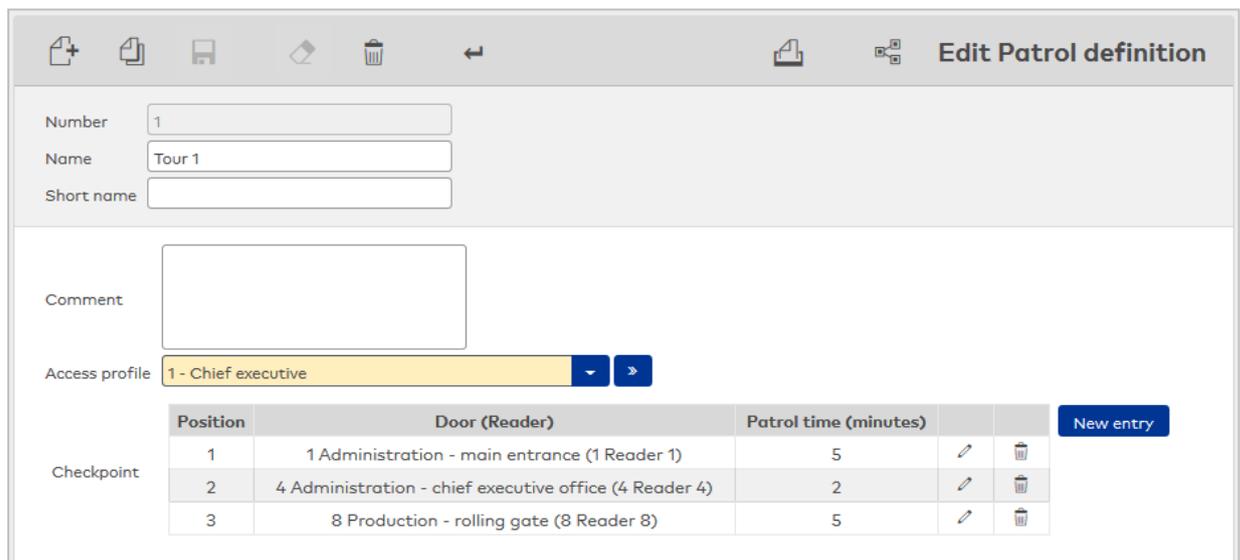


Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Patrol definition" dialog

Use the **Edit Patrol definition** dialog to create new patrol definitions and edit existing patrol definitions. Each patrol definition requires a unique number. It is recommended that you specify a name and a short description.

Use the buttons in the toolbar to navigate between records, create or delete a record and save or discard changes made to the record. Use the **Back to selection** button to return to the selection dialog.



Comment input field:

Free text field for comments on the patrol definition.

Access profile selection field:

Contains the allocation for the required access profile for the patrol.

Options:

- All access profiles created in the system.

Table:

This table defines the stages of the patrol. Every stage is defined by a reader and, optionally, by the time required for the stage. The first reader in the table represents the start of the patrol. Each additional reader represents the start of a stage and also the end of the previous stage.

Position input field:

Contains table position, which is the same as the order of the sections.

Reader selection field:

Contains the readers for the patrol. All online readers are available. Offline readers cannot be used.

Options:

- All online readers

Travelling time input field:

Contains the maximum time in minutes required for this stage of the patrol. If the time expires, it is shown as failed in the status display. If a booking is not made before the time has expired, this booking is marked accordingly in the log.

Value range: 0, 1–99 minutes

Default value: 0 no patrol time default

4.12.4 Patrols log

Every patrol is logged, including all bookings and manual interventions. The log contains the following information:

- Who performed the patrol.
- When was the patrol started.
- When were the various positions reached.
- When was the patrol finished.
- What special issues arose.

"Selection Patrols log" dialog

The **Selection Patrols log** dialog displays all patrols carried out.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number	Name	Date ↑	Start ↑	End	Security guard
<input type="checkbox"/>	1	Ronde 1	01/05/2016	4:06:34 PM	11:49:32 AM	7 Cermans, Paul

Number of records: 1

Date column:

Contains the start date of the patrol.

Start column:

Contains the time when the patrol started.

End column:

Contains the time when the patrol ended.

Security guard column:

Contains the employee who carried out the patrol along with the employee number, last name and first name.

"Patrol log" dialog

The **Patrol log** dialog displays the details of security guard patrols. All surveillance bookings, including the reader and time, as well as manual interventions during the patrol, are displayed in chronological order.

You can use the buttons in the toolbar to navigate between data records or to print the current log. Use the **Back to selection** button to return to the selection dialog.

←
🖨️
📄
Patrol log

Number

Name

Short name

Start

End

Employee number

Last name

First name

Comment

	Booking time	Target time	Door (Reader)	Comment
Checkpoint	4:06:48 PM			Interrupted (admin)
	11:47:52 AM			Resumed (admin)
	11:51:25 AM			Finished (admin)
		12:17:52 PM		2 Porte entre gest-prod (2 Reader 2)

Start display field:

Contains the start of the patrol with the date and time. If a patrol time is defined for the first reader of the patrol, the start corresponds to the time at which the patrol was saved. Otherwise the start is the time when the booking is made to the first reader of the patrol.

End display field:

Contains the end of the patrol with the date and time.

Employee number display field:

Contains the employee number of the security guard who carried out the patrol.

Name display field:

Contains the name of the security guard who carried out the patrol.

First name display field:

Contains the first name of the security guard who carried out the patrol.

Comment display field:

Contains special incidents and remarks on the patrol, if these have been entered.

Checkpoint table:

The table displays the control bookings of the patrol in chronological order.

Note: Irregularities of the patrol, such as late bookings or missed bookings, are displayed in red, including the target time, the checkpoint, the door and the reader.

Booking time column:

Contains the time when the booking was carried out.

Target time column:

Contains the time until when the booking should have been carried out.

Door (Reader) column:

Contains the checkpoint and specifies the door and the reader.

Comment column:

Contains manual interventions in the patrol such as interruptions or manual cancellation of the patrol.

4.13 Attendance display (access)

The attendance display popup dialog allows the user to view the attendance status of the allocated persons at any time. The popup dialog can also be used to change the attendance status of a person, where necessary.

The attendance display is user-specific. Every user can be assigned a global configuration. In addition, every user can create their own, individual configurations. The attendance display in the Access area also allows the use of configurations based on folders or security areas. Nested security areas are also recognised, although persons in lower-level areas are displayed without separate identifiers.

The **Selection Configurations** dialog displays all configurations that the user can view. If only one configuration is present, the respective attendance display will be opened directly in the popup dialog. If multiple configurations are present, they can be opened in parallel.

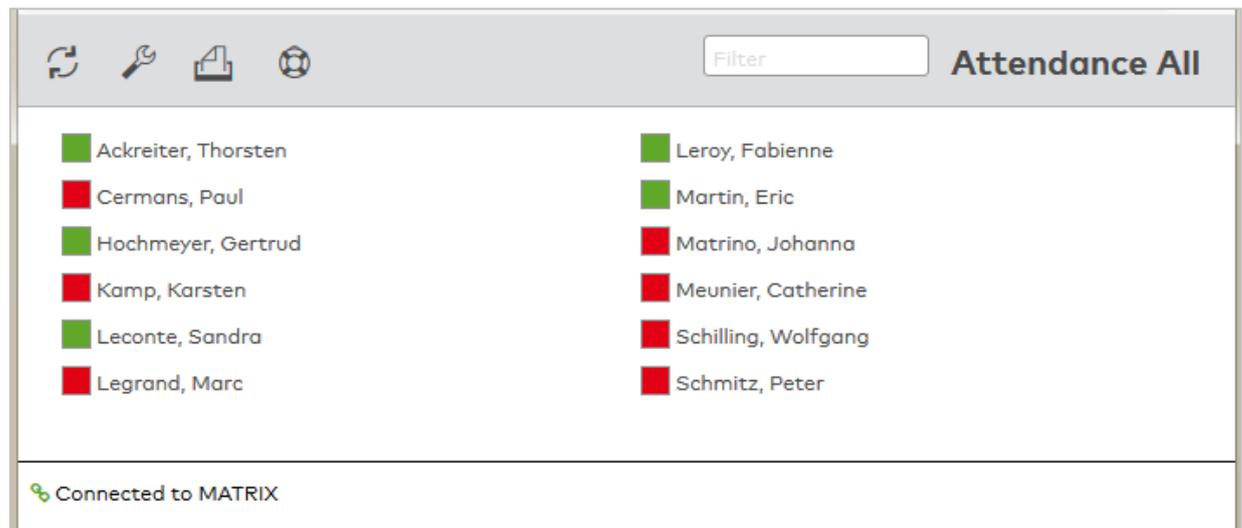
Note: The attendance display requires doors with two readers: one for entering and one for exiting. The entrance reader is assigned the variable booking instruction **7 - Access IN** and the exit reader the variable booking instruction **8 - Access OUT**.

"Attendance display" dialog

The **Attendance display** popup dialog displays the current attendance status of persons.

You can change the attendance status if necessary, for instance, if a person has forgotten a booking. To do so, click on the person in question.

Use the toolbar to update, print or filter the display. Use the **Configure** button to call up the **Edit Configuration** dialog for the respective attendance display. The name of the configuration is shown in the toolbar on the right.



Display:

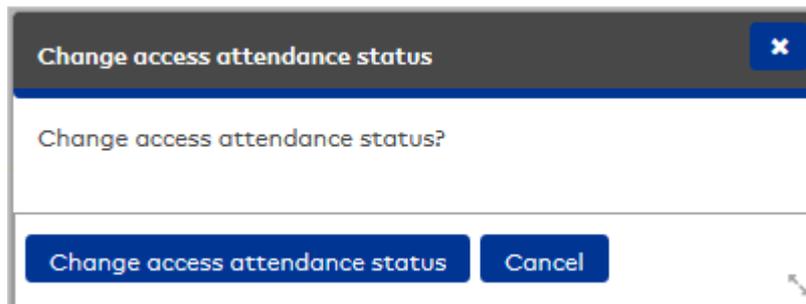
Displays the current attendance status as symbol and with the name of the person. Further details can also be displayed, depending on the configuration.

Status:

 Unknown	The attendance status of the person is not known, for example because the person has not yet performed a booking.
 Absent	The person is currently listed with the attendance status set to "absent".
 Present	The person is currently listed with the attendance status set to "present".

Edit status display:

Click on the status symbol of the person whose attendance status you want to change.



The change is applied after confirming the prompt and the new status is displayed.

The attendance status changes according to the following rules:

	Changes to
 Unknown	 Present
 Absent	 Present
 Present	 Absent

Note: All changes of the attendance status are executed as bookings and displayed in the bookings log of the person.

"Selection configurations" dialog

The **Selection Configurations** dialog displays all attendance display configurations available to the user.

Click on **Create new record** to create your own user-specific configurations.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Click on an attendance display to open it.

"Edit Configuration" dialog

The **Edit Configuration** dialog is used to create and edit user-specific configurations for the attendance display. Each configuration requires a unique number. It is recommended that you specify a name and a short name.

Use the buttons on the toolbar to create new records, delete records, save changes made to a record or discard changes made to a record. Use the **Back to selection** button to return to the selection dialog.



Attendance display (access) configuration

"Persons" tab

The persons to be displayed are defined on this tab.



Persons checkbox:

Display all entries from the "Persons" person group. If the checkbox is activated, a selection field is shown that can be used to define further criteria.

Visitors checkbox:

Display all entries from the "Visitors" person group. Only present if visitor administration is activated.

External company employee checkbox:

Display all entries from the "External company employee" person group. Only present if external company administration is activated.

Disable limitation by data groups checkbox:

As default, user authorisations for data groups are taken into account in the attendance display (inactivated). If the checkbox is activated, the existing user authorisations are not taken into account. The user is shown all records.

Person selection

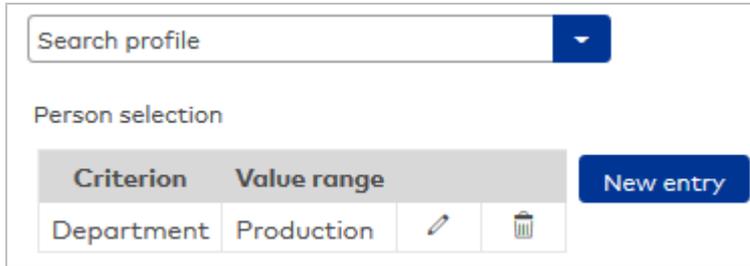
All persons selection:

All persons present in the system are shown in the attendance display.



Search profile selection:

For configuring a selection of persons using defined criteria.


Person selection table:

The Person selection table contains the criteria for the search. Within a row, an OR link can be created with a semicolon (;).

Criterion selection field:

Contains the search element for the search condition.

Value range input field:

Contains the value or value range describing your search quantity.

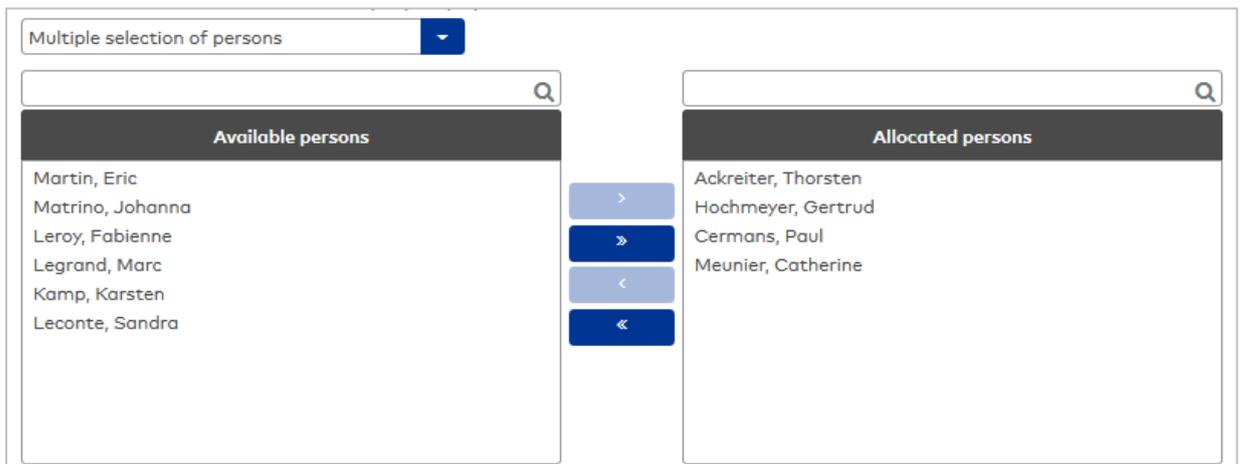
If you want to search for missing or empty fields, use the wildcards @EMPTY or @NOTEMPTY for fields which contain any value.

Note: Other wildcards are not allowed in this search.

The employee record fields, which are enabled for use in the search profiles, are available for selection. If no person search is specified for the configuration, users can determine the persons directly using the **Attendance display** dialog.

Multiple selection of persons selection:

For configuring a selection of persons using a list.


"Area" tab

This tab allows users to select a folder or security area. The tab is only available if folders or security areas are defined in the system.

If a setting is made here, persons who are not present in the folder or security area are no longer displayed.

Persons **Area** Display Additional info

Note: If you select an area, the following limitations apply:

- Present persons only are displayed.
- You cannot select a search profile.
- Display, Sorting and Additional information will support the Last name, First name, Employee number, ID card number and ID card label fields only.

Folder

Security area

Folder selection field:

This limits the attendance report to persons who are present in the selected folder.

Options: All folders created in the system.

Security area selection field:

This limits the attendance report to persons who are present in the selected security area.

Options: All security areas created in the system and for which attendance recording is activated.

Note: This option is only available if security areas and counting information are activated in the system.

"Display" tab

This tab is used to define the details of the display, such as fields to be displayed and sorting.

Persons Area **Display** Additional info

Animated status change

Display

Position	Employee record field	New entry	
1	Last name		
2	First name		

Sorting

Position	Sorting criterion	Sorting	New entry
----------	-------------------	---------	-----------

Animated status change checkbox:

Indicates whether a status change is animated in a pop-up dialog.

Options:

- Activated: Every status change is animated using a fading effect.
- Not activated: The display is switched over without any additional effects when the status changes.

Default: Activated.

Display table:

The details of the person are defined in this table.

Position column:

Contains the position specification for the table:

Value range: 1–9999

Employee record field column:

Contains the employee record field to be displayed.

Sorting table:

All fields used in the search can be used for sorting of persons in the display.

Position column:

Contains the position specification for the table:
Value range: 1–9999

Sorting criterion column:

Contains the sorting criterion and specifies the sorting sequence and the field name. If multiple fields are specified, the first sorting uses the first field.

Sorting column:

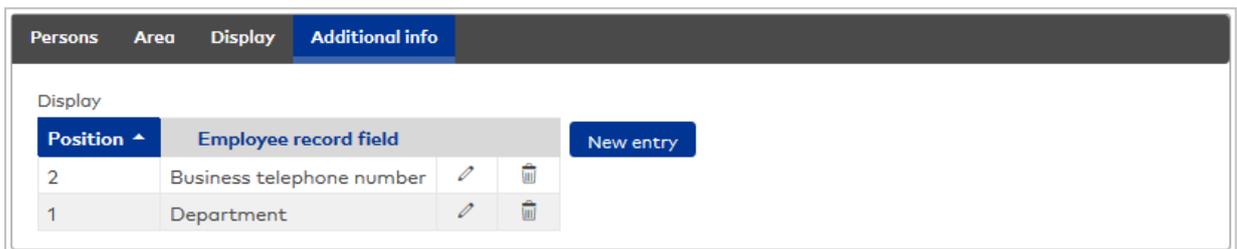
Specifies how the data is sorted.

Options:

- Ascending – The records are sorted in ascending order, starting with the smallest value.
- Descending – The records are sorted in descending order, starting with the greatest value.

"Additional info" tab

This tab is used to configure data that is displayed as additional information when the mouse cursor is hovered over a person in the display (tooltip).

**Display** table:

The details of the person are defined in this table.

Position column:

Contains the position specification for the table:
Value range: 1–9999

Employee record field column:

Contains the employee record field to be displayed.

Note: If a folder or security area is indicated on the **Area** tab, the only attributes that can be chosen are name, first name, ID card number and ID card name.

4.14 Reports (access)

The **Reports** menu provides various reports that you can use to query the various access permissions and access bookings that have taken place.

The **Person access report** dialog contains all bookings of a person within a specified period.

The **Reader events report** contains all bookings and events from a reader within a specified period.

The **Reader locations** allow you to open a report of the readers with their allocated doors and room zones.

The **Access times** report contains an overview of the access time frames for the selected access weekly profiles, including the replacement day programs.

The **Access profiles** report contains an overview of the access profiles with the possible access permissions including the allocated access weekly profiles.

The **Access permissions overview** contains all the access permissions allocated to a person in a tree structure based on the doors, including up to the time frames for access.

Use the **Person access permissions** entry to output a report of all access permissions for selected persons or all persons.

Use the **Door access permissions** entry to output a report of all access permissions for selected doors or all doors.

Use the **Room zone access permissions** entry to output a report of all persons with access permission for each room zone with detailed information on employee category, ID card and type of permissions.

Use the **ID card history** entry to output a report with the information when a particular ID card was or is still allocated to a person.

Use the **Blocked AoC ID cards** entry to output a report of all ID cards that are currently blocked. This report is available only if the AoC function is active.

The **Blocks** report contains all blocked persons and specification of the reason for blocking.

Use the **Attendance report** entry to query a report of all persons listed as present.

Use the **Visits** menu item to access terminated or active visits.

Use the **Smart phone status** entry to display all available smartphones along with their access permission transfer statuses.

Use the **Time-controlled reports** entry to execute dynamic reports at configurable times.

Use the **Print system data** entry to print the most important system data in a report.

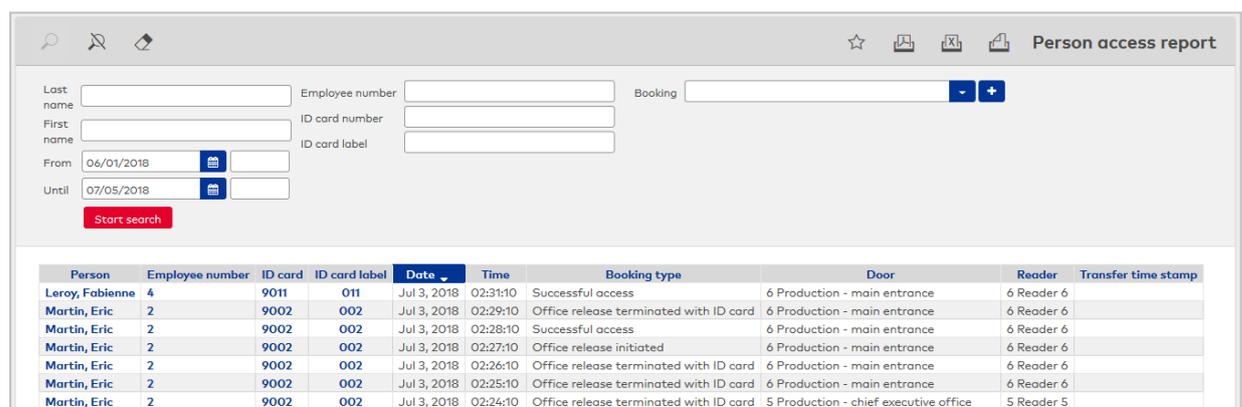
4.14.1 Person access report

The **Person access report** contains information on which person made an access booking at a particular time and at which doors.

"Person access report" dialog

The **Person access report** dialog displays all bookings of persons within a selected period along with the date, time and door.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



Person	Employee number	ID card	ID card label	Date	Time	Booking type	Door	Reader	Transfer time stamp
Leroy, Fabienne	4	9011	011	Jul 3, 2018	02:31:10	Successful access	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:29:10	Office release terminated with ID card	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:28:10	Successful access	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:27:10	Office release initiated	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:26:10	Office release terminated with ID card	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:25:10	Office release terminated with ID card	6 Production - main entrance	6 Reader 6	
Martin, Eric	2	9002	002	Jul 3, 2018	02:24:10	Office release terminated with ID card	5 Production - chief executive office	5 Reader 5	

Table:

Person column:

Contains the name and first name of the person.

Employee number column:

Contains the unique employee number of the person.

Type column:

Contains the person group identifier; Per = personnel/employee, Vis = visitor, Ext = external company employee.

ID card column:

Contains the unique ID card number.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Date column:

Contains the date of the booking.

Time column:

Contains the time of the booking.

Booking type column:

Contains the type of booking. In the case of two-person access, the ID number of the second ID card is displayed in a tooltip.

Door column:

Displays the name in the respective language for the door that corresponds with the booking

Reader column:

Contains the number and name in the respective language for the reader that corresponds with the booking

Media column:

An icon indicates if a recording has been saved for a booking with video verification. Click the icon to open the recording in a media viewer. Windows Media Player Version 11 or higher must be installed to play the recording.

Transfer time stamp column:

Contains the transfer time of the booking.

4.14.2 Reader events report

The **Reader events report** contains the events that have occurred on a reader.

The events include access bookings with information on who made an access booking at a particular time and notifications generated by the components.

"Reader events report" dialog

The **Reader events report** dialog displays all bookings and notifications from a component within a selected period along with the date, time, name and ID card number of the respective person.

The Search function can be used to search by Reader number, Reader name or r ID card and filter the results by desired periods.

Use multiple selection to select specific bookings or notifications for the search.

Note: Specifying a particular booking only affects the bookings. It does not affect the filter for the notification. The same applies in reverse for notifications, which do not affect the filter for the bookings.

Use the buttons in the toolbar to print selected records or all records or to open the search function.

The table displays the corresponding search results.

Reader	Door	Date	Time	Booking/notification	ID card	ID card label	Person	Employee number	Transfer time stamp
6 Reader 6	6 Production - main entrance	Jul 3, 2018	02:31:10	Successful access	9011	011	Leroy, Fabienne	4	
7 Reader 7	7 Salesroom - customers	Jul 3, 2018	02:30:10	Office release initiated	9011	011			
6 Reader 6	6 Production - main entrance	Jul 3, 2018	02:29:10	Office release terminated with ID card	9002	002	Martin, Eric	2	
6 Reader 6	6 Production - main entrance	Jul 3, 2018	02:28:10	Successful access	9002	002	Martin, Eric	2	
6 Reader 6	6 Production - main entrance	Jul 3, 2018	02:27:10	Office release initiated	9002	002	Martin, Eric	2	
6 Reader 6	6 Production - main entrance	Jul 3, 2018	02:26:10	Office release terminated with ID card	9002	002	Martin, Eric	2	

Table:**Column Reader:**

Contains the number and the name of the component where the booking was executed or where an event was reported.

Date column:

Contains the date of the booking.

Time column:

Contains the time of the booking.

Booking/notification column:

Contains the type of booking or notification. In the case of two-person access, the ID number of the second ID card is displayed in a tooltip.

ID card column:

Contains the unique ID card number.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Person column:

Contains the name and first name of the person.

Employee number column:

Contains the unique employee number of the person.

Type column:

Contains the person group identifier; Per = employee, Ext = external company employee.

Transfer time stamp column:

Contains the transfer time of the booking.

4.14.3 Reader locations

The **Reader locations** report contains the readers with their allocated doors and room zones.

The details view provides you with an overview of the time intervals for the time daily programs concerned, including the substitute day programs.

"Reader locations display" dialog

The **Reader locations display** dialog shows all existing readers with their door allocation, room zone allocation and the parent folder.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Reader locations display

Reader number <input type="text"/>	Room zone number <input type="text"/>
Reader name <input type="text"/>	Room zone name <input type="text"/>
Door number <input type="text"/>	
Door name <input type="text"/>	

Start search

<input type="checkbox"/>	Reader ▲	Door	Room zone	Folder
<input type="checkbox"/>	1 - Reader 1	1 - Administration - main entrance	1 - Foyer - administration	
<input type="checkbox"/>	2 - Reader 2	2 - A-P connecting door	7 - Production	
<input type="checkbox"/>	3 - Reader 3	2 - A-P connecting door	3 - Administration and others	
<input type="checkbox"/>	4 - Reader 4	4 - Administration - chief executive office	2 - Chief executive	
<input type="checkbox"/>	5 - Reader 5	5 - Production - chief executive office	2 - Chief executive	
<input type="checkbox"/>	6 - Reader 6	6 - Production - main entrance	7 - Production	
<input type="checkbox"/>	7 - Reader 7	7 - Salesroom - customers	7 - Production	

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Reader location details display" dialog

The **Reader locations details display** dialog shows the time intervals for the different functions in the door daily times grouped according to readers for each weekday in the door weekly profile. If a substitute program is specified, this is also shown.

Display Reader location details

Reader: 1 - Reader 1, Door: 1 - Administration - main entrance, Reader location details: 1 - Always

Day	Function	Interval 1	Interval 2	Interval 3	Interval 4	Interval 5	Interval 6	Interval 7	Interval 8	Substitute programs
Monday	Access	00:00 - 24:00								
	Permanent opening									
	Office release									
	Motion recording off									
	PIN off									
Tuesday	Access	00:00 - 24:00								
	Permanent opening									
	Office release									
	Motion recording off									
	PIN off									

Table:

This table displays the time intervals indicated in the allocated door daily times for the weekdays. If a substitute program is specified, this is also shown.

Day column:

Contains the weekday.

Function column:

Contains the access function for which the following intervals are valid.

Interval 1 - 4 column:

Contains Time Intervals 1 to 4 for the access functions.

Substitute program column:

Contains the day type and the name for the substitute program which is valid on days corresponding to the day types concerned.

Substitute programs table:

The **Substitute programs** table displays the time intervals for the featured door daily times.

Door daily time column:

Contains the number and name of the door daily time.

Function column:

Contains the function for which the following intervals are valid.

Interval 1 - 4 column:

Contains Time Intervals 1 to 4 for the functions.

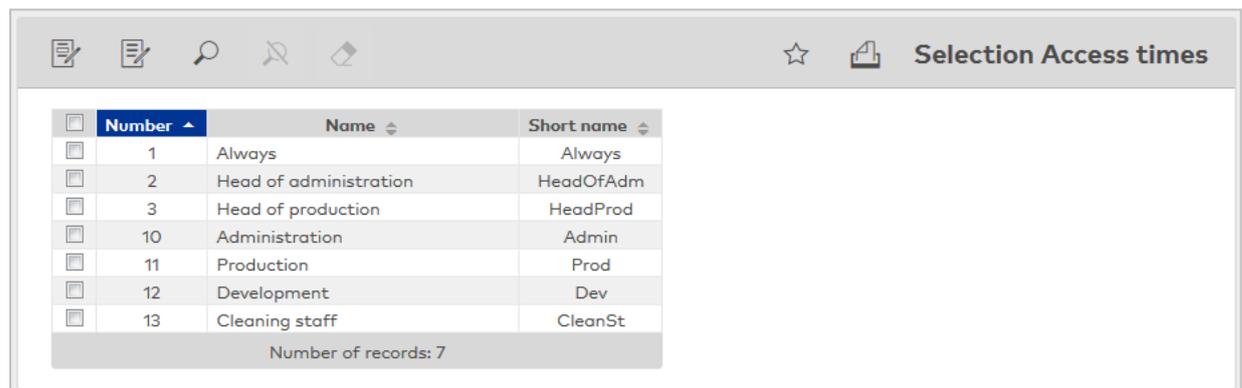
4.14.4 Access times

The **Access times** report groups the time intervals for access indicated in the respective access daily times, including substitute daily programs, according to the selected access weekly profiles.

"Selection access times" dialog

The **Selection Access times** dialog displays all access weekly profiles created for access.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.



<input type="checkbox"/>	Number ▲	Name ▲	Short name ▲
<input type="checkbox"/>	1	Always	Always
<input type="checkbox"/>	2	Head of administration	HeadOfAdm
<input type="checkbox"/>	3	Head of production	HeadProd
<input type="checkbox"/>	10	Administration	Admin
<input type="checkbox"/>	11	Production	Prod
<input type="checkbox"/>	12	Development	Dev
<input type="checkbox"/>	13	Cleaning staff	CleanSt

Number of records: 7

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display access times" dialog

The **Display Access times** dialog groups the time intervals for access indicated in the allocated access daily times, including substitute programs, according to the access weekly profiles.

←   Display Access times					
Access weekly profile: 1 - Always					
Day	Interval 1	Interval 2	Interval 3	Interval 4	Substitute programs
Monday	00:00 - 24:00				
Tuesday	00:00 - 24:00				
Wednesday	00:00 - 24:00				
Thursday	00:00 - 24:00				
Friday	00:00 - 24:00				
Saturday	00:00 - 24:00				
Sunday	00:00 - 24:00				
Access weekly profile: 2 - Head of administration					
Day	Interval 1	Interval 2	Interval 3	Interval 4	Substitute programs
Monday	06:00 - 22:00				Bank holiday: Never
Tuesday	06:00 - 22:00				Bank holiday: Never
Wednesday	06:00 - 22:00				Bank holiday: Never
Thursday	06:00 - 22:00				Bank holiday: Never
Friday	06:00 - 22:00				Bank holiday: Never
Saturday	06:00 - 22:00				Bank holiday: Never
Sunday					

Tables for Access weekly profiles:

These tables display the time intervals for the allocated access daily times. If a substitute program is specified, this is also shown.

Day column:

Contains the weekday.

Interval 1 - 4 column:

Contains time intervals 1 to 4 for access.

Substitute program column:

Contains the day type and the name for the substitute program which is valid for the day types concerned.

Substitute programs table:

The **Substitute programs** table displays the time intervals for the featured access daily times.

Access daily time column:

Contains the name of the access daily time.

Interval 1 - 4 column:

Contains time intervals 1 to 4 for access.

4.14.5 Access profiles

In the **Access profiles** report, you will find information about which room zones and doors are included in the access profiles and their allocated access weekly profiles.

"Selection access profiles" dialog

The **Selection Access profiles** dialog displays all access profiles created for access control.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Number	Name	Short name
1	Chief executive	Chief executive
2	Head of administration	HeadOfAdm
10	Administration and others	AdmAndCo
20	Head of production	HeadProd
21	Production	Prod
50	Development	Dev
60	IT admin	IT admin
61	Foyer - administration	AdminFoy
62	Cleaning staff	CleanSt

Number of records: 9

Relevant for visitors column:

Indicates if the access profile can be used for visitor administration.

Note: The column is only available, if the visitor administration option is active.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display Access profiles" dialog

The **Display Access profiles** dialog displays the previously selected access profiles with the allocated doors or room zones and the access weekly profile.

Type	Description	Access weekly profile
1 Chief executive		
Door/reader	11 - Lift	1 - Always
	12 - Stores A4	1 - Always
	71 - Interlock 1	1 - Always
	72 - Interlock 2	1 - Always
	73 - Stores P8	1 - Always
Room zone/range	1 - Foyer - administration	1 - Always
	2 - Chief executive	1 - Always
	3 - Administration and others	1 - Always
	4 - Head of administration	1 - Always
	5 - Development	1 - Always
	6 - Server room	1 - Always
	7 - Production	1 - Always
	8 - Head of production	1 - Always
	9 - Material stores	1 - Always

Number and name display:

Contains the number and name of the access profile.

Table:

The table displays the doors and room zones permitted for every access profile along with the allocated access weekly profiles.

Type column:

Displays the permission type.

Description column:

Shows the permitted doors and/or room zones.

Access weekly profile: column:

Shows the allocated access weekly profile.

4.14.6 Display access permissions overview

In the Access permissions overview, all access permissions relating to doors are structured starting from a person and extending as far as the time frames for access. Since the door control is also taken into account, information is available showing why a person is allowed to access a door or not.

"Selection access permissions overview" dialog

The **Selection Access permissions overview** dialog lists all existing employee records.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Type	Last name ▲	First name	Department	Employee number	ID card number	ID card label	Blocked
<input type="checkbox"/>	Per	Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
<input type="checkbox"/>	Per	Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
<input type="checkbox"/>	Per	Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
<input type="checkbox"/>	Per	Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
<input type="checkbox"/>	Per	Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
<input type="checkbox"/>	Per	Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Per	Leroy	Fabienne	1 - Administration	4	9011	011	<input type="checkbox"/>
<input type="checkbox"/>	Per	Martin	Eric	1 - Administration	2	9002	002	<input type="checkbox"/>
<input type="checkbox"/>	Per	Matrino	Johanna	1 - Administration	3			<input checked="" type="checkbox"/>
<input type="checkbox"/>	Per	Meunier	Catherine	2 - Production	8	8204	204	<input type="checkbox"/>
<input type="checkbox"/>	Ext	Schilling	Wolfgang		102			<input type="checkbox"/>
<input type="checkbox"/>	Ext	Schmitz	Peter		101			<input type="checkbox"/>

Number of records: 12

Type column:

Contains the person group identifier; Per = personnel/employee, Vis = visitor, Ext = external company employee.

Last name column:

Contains the last name of the person.

First name column:

Contains the first name of the person.

Department column:

Contains the department to which the person belongs.

Employee number column:

Contains the unique employee number.

ID card number column:

Contains the company ID card/access ID card number of the person.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Blocked column:

Displays whether the employee is blocked and therefore does not have access.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display access permissions overview" dialog

The **Display Access permissions overview** dialog displays all access permissions for pre-selected persons. The doors with access permission and all components leading to the access permissions are also taken into account.

The day-related display of the access-relevant time frames from the door control and the person's access permissions are part of the dialog. They are displayed in the header of the dialog. Using the scrolling function by day or a direct date specification, a determination for each day can be made as to when a permission or permission with PIN code is possible and whether the person has access permission for these times.

The screenshot shows the "Display Access permissions overview" dialog. At the top, there are input fields for "Last name" (Hochmeyer), "First name" (Gertrud), and "Employee number" (5). Below these is a date selector for "06/12/2017". A time bar shows the day from 00:00 to 24:00 with markers at 06:00, 12:00, 18:00, and 24:00. Below the time bar, there are four rows of colored bars representing different access types: "Access" (green), "PIN code check" (blue), "Permanent opening" (grey), and "Access permission" (green). Below the time bar, there is a list of doors and their access profiles. The selected door is "Door:8 Production - rolling gate / 9 Reader 9". The list includes:

- Hochmeyer, Gertrud
 - Door:2 A-P connecting door / 2 Reader 2
 - Door:6 Production - main entrance / 6 Reader 6
 - Door:7 Salesroom - customers / 7 Reader 7
 - Door:8 Production - rolling gate / 9 Reader 9**
 - Door control:
 - Access permission:
 - Access profile: - 21 Production
 - Room zone: - 7 - Production
 - Access weekly profile: - 11 - Production
 - Door:8 Production - rolling gate / 8 Reader 8
 - Door:59 Salesroom - employees / 59 Air 9
 - Door:60 Head of production / 60 Air 10
 - Door:61 Material stores / 61 Air 11
 - Door:101 Reception B5 / 101 Reception B5
 - Door:104 Berlin room / 104 Room Berlin
 - Door:107 Seminar room / 107 Seminar room
 - Door:107 Seminar room / 107 Seminar room

Name display field:

Contains the last name of the person.

First name display:

Contains the first name of the person.

Employee number display:

Contains the unique employee number of the person.

Time bar display:

The top section shows the time frames of the door daily time program of the respective door. Possible time ranges for access permission, access with PIN code checks and time ranges for permanent opening are also shown for the selected date. Output starts with the current date.

In the lower section, all time ranges from all the person's access permissions for the door are displayed depending on the selected date. In this way, potential conflicts are identified quickly.

Access time bar:

Displays time ranges when access bookings are possible via the door daily time.

PIN code check time bar:

Displays time ranges when access bookings with PIN code check are possible via the door daily time.

Permanent opening time bar:

Displays the time ranges in which the door is unlocked via the door daily time.

Access permission: time bar:

Displays the time ranges in which the person has access permission.

Bookings table:

This table displays the person's access bookings for the selected date.

Time column:

Displays the time of a booking on the selected date.

Booking type column:

Displays the type of booking, such as access, office release and so on.

Door number column:

Contains the unique number of the door where the booking took place.

Door column:

Displays the name in the respective language for the door where the booking took place.

Reader column:

Displays the name in the respective language for the reader on which the booking took place.

Tree structure display:

Based on the person, the first node of the tree contains the systems. If no systems are created in the system or if the displayed doors are not allocated to any system, the systems' node is omitted.

The door control and the access permissions are located beneath the node of the doors on the same level. Calendar, door weekly profiles and door daily times for weekdays are part of the door control. The time frames are located beneath the door daily times. The substitute door programs with the respective time frames are displayed beneath the day types if there are day types for the door daily time which derive from the associated calendar.

The access permissions are listed depending on their association. The access permissions from locking plans, access profiles and special permissions are located on the same level. Each permission then follows the access weekly profile with access daily times. This contains the time frames for access and for access with a PIN code.

If an access permission is subject to a validity it is displayed in the access permission's node. The substitute access door programs with the respective time frames are displayed beneath the day types if there are day types for the door access daily time which derive from the associated calendar.

4.14.7 Person access permissions

The **Person access permissions** contain information on the doors for which a person has access permission. The access permissions are broken down with information about their origin such as access profile, special permission or locking plan.

"Selection person access permissions" dialog

The **Selection Person access permissions** dialog lists all existing person records.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Type	Last name	First name	Department	Employee number	ID card number	ID card label	Blocked
<input type="checkbox"/>	Per	Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>
<input type="checkbox"/>	Per	Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>
<input type="checkbox"/>	Per	Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>
<input type="checkbox"/>	Per	Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>
<input type="checkbox"/>	Per	Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>
<input type="checkbox"/>	Per	Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>
<input type="checkbox"/>	Per	Leroy	Fabienne	1 - Administration	4	9011	011	<input type="checkbox"/>
<input type="checkbox"/>	Per	Martin	Eric	1 - Administration	2	9002	002	<input type="checkbox"/>
<input type="checkbox"/>	Per	Matrino	Johanna	1 - Administration	3			<input checked="" type="checkbox"/>
<input type="checkbox"/>	Per	Meunier	Catherine	2 - Production	8	8204	204	<input type="checkbox"/>
<input type="checkbox"/>	Ext	Schilling	Wolfgang		102			<input type="checkbox"/>
<input type="checkbox"/>	Ext	Schmitz	Peter		101			<input type="checkbox"/>

Number of records: 12

Type column:

Contains the person group identifier; Per = personnel/employee, Vis = visitor, Ext = external company employee.

Last name column:

Contains the last name of the person.

First name column:

Contains the first name of the person.

Department column:

Contains the department to which the person belongs.

Employee number column:

Contains the unique employee number.

ID card number column:

Contains the company ID card/access ID card number of the person.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Blocked column:

Indicates if the person is blocked and therefore has no booking permissions.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display person access permissions" dialog

The **Display Person access permissions** dialog lists all access permissions for the selected persons; a differentiation is made between access permissions granted via an access profile, via special permissions or via the locking plan.

Display Person access permissions				
Status: June 3, 2017 9:22:43 AM				
Last name: Ackreiter, Thorsten				
Employee number: 1				
Number ▲	Door name	Short name	Access weekly profile	Source
1	Administration - main entrance	A-001	1 - Always	Access profile 1
2	A-P connecting door	A-010	1 - Always	Access profile 1
4	Administration - chief executive office	A-011	1 - Always	Access profile 1
5	Production - chief executive office	P-001	1 - Always	Access profile 1
6	Production - main entrance	P-002	1 - Always	Access profile 1
7	Salesroom - customers	P-003	1 - Always	Access profile 1
8	Production - rolling gate	P-004	1 - Always	Access profile 1
11	Lift	Elev	1 - Always	Access profile 1
12	Stores A4	L-A4	1 - Always	Access profile 1
51	Administration	A-002	1 - Always	Access profile 1
52	Head of administration	A-003	1 - Always	Access profile 1
53	Marketing	A-004	1 - Always	Access profile 1
54	Sales	A-005	1 - Always	Access profile 1
55	Development	A-006	1 - Always	Access profile 1
56	Server room	A-007	1 - Always	Access profile 1
57	Office stores	A-008	1 - Always	Access profile 1
58	Meeting room	A-009	1 - Always	Access profile 1
59	Salesroom - employees	P-005	1 - Always	Access profile 1
60	Head of production	P-006	1 - Always	Access profile 1
61	Material stores	P-007	1 - Always	Access profile 1
71	Interlock 1	Slu1	1 - Always	Access profile 1
72	Interlock 2	Slu2	1 - Always	Access profile 1
73	Stores P8	L-P8	1 - Always	Access profile 1
101	Reception B5	R B5	1 - Always	Locking plan 1
102	Paris room	Pr	1 - Always	Locking plan 1
103	London room	Lo	1 - Always	Locking plan 1
104	Berlin room	Be	1 - Always	Locking plan 1
105	Rome room	Ro	1 - Always	Locking plan 1
106	New York room	NY	1 - Always	Locking plan 1
Number of records: 1				

Status display:

Displays the date and time when the query was generated.

Name display:

Contains the name and first name of a person.

Employee number display:

Contains the record number.

A table displays the access permissions for each person selected.

Number column:

Contains the unique number for the door.

Door name column:

Contains the name for door in the respective language.

Short name column:

Contains the short name for door in the respective language.

Access weekly profile: column:

Contains the allocated access weekly profile.

Source column:

Contains the access profile, the locking plan or specification of the special permission from which the access permission originates.

Note: A note is displayed if no access permissions exist for a person.

4.14.8 Door access permissions

The **Door access permissions** contain information on which persons have access permission for a door. The access permissions are broken down with information about their origin such as access profile, special permission or locking plan. The list always applies to the current day.

"Selection door access permissions" dialog

The **Selection door access permissions** dialog lists all existing door records.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

📄 📄 🔍 🗑️ ✏️

☆ 🖨️ 📄 📄

Selection Door access permissions

Door number

Door name

Door short name

Reader number

Reader name

Reader short name

Start search

	Number	Name	Short name	Reader number	Reader name	Reader short name
<input type="checkbox"/>	1	Administration - main entrance	A-001	1	Reader 1	
<input type="checkbox"/>	2	A-P connecting door	A-010	2	Reader 2	
<input type="checkbox"/>	2	A-P connecting door	A-010	3	Reader 3	
<input type="checkbox"/>	4	Administration - chief executive office	A-011	4	Reader 4	
<input type="checkbox"/>	5	Production - chief executive office	P-001	5	Reader 5	
<input type="checkbox"/>	6	Production - main entrance	P-002	6	Reader 6	
<input type="checkbox"/>	7	Salesroom - customers	P-003	7	Reader 7	

Reader number column:

Contains the device's unique number.

Reader name column:

Contains the device's name.

Reader short name column:

Contains the short name of the device.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display door access permissions" dialog

The **Display Door access permissions** dialog lists all persons who have an access permission for the selected doors. You can see where the permission originates by adding the access weekly profile and the source.

Note: The **Door access permissions** list is updated every day. Blocked persons/ID cards or persons whose access validity period has expired or not yet begun on the current day are not displayed.

Display Door access permissions						
Status: June 3, 2017 9:25:00 AM						
Door: 1 Administration - main entrance (1 Reader 1)						
Last name	First name	Type	ID card number	Access weekly profile	Source	
Ackreiter	Thorsten	Per	9001	Always 1	Access profile 1	
Leroy	Fabienne	Per	9011	Administration 10	Access profile 10	
Martin	Eric	Per	9002	Administration 10	Access profile 10	
Door: 2 A-P connecting door (2 Reader 2)						
Last name	First name	Type	ID card number	Access weekly profile	Source	
Ackreiter	Thorsten	Per	9001	Always 1	Access profile 1	
Cermans	Paul	Per	8203	Production 11	Access profile 21	
Hochmeyer	Gertrud	Per	8201	Production 11	Access profile 21	
Kamp	Karsten	Per	8205	Production 11	Access profile 21	
Leconte	Sandra	Per	8206	Production 11	Access profile 21	
Meunier	Catherine	Per	8204	Production 11	Access profile 21	

Status display:

Displays the date and time when the query was generated.

Door display:

Contains the number and language-dependent name of the door. A table displays the access permissions for each door selected.

Last name column:

Contains the last name of the person with access permissions.

First name column:

Contains the first name of the person with access permissions.

Type column:

Contains the person group identifier; Per = employee, Ext = external company employee.

ID card number column:

Contains the ID card number for the ID card with access permissions.

Access weekly profile: column:

Contains the allocated access weekly profile.

Source column:

Contains the access profile, the locking plan or specification of the special permission from which the access permission originates.

Note: A note is displayed if no access permissions for a door exist.

4.14.9 Room zone access permissions

The **Room zone access permissions** report contains the persons who have access to selected room zones. These can be employees, external company employees or visitors. The list always applies to the current day.

"Selection room zone access permissions" dialog

The **Selection Room zone access permissions** dialog lists all existing room zone administration records.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

Selection Room zone access permissions

Room zone number	<input type="text"/>	Reader number	<input type="text"/>
Room zone name	<input type="text"/>	Reader name	<input type="text"/>
Room zone short name	<input type="text"/>	Reader short name	<input type="text"/>

Start search

<input type="checkbox"/>	Room zone number ▲	Room zone name	Room zone short name
<input type="checkbox"/>	1	Foyer - administration	AdmFoy
<input type="checkbox"/>	2	Chief executive	Chief executive
<input type="checkbox"/>	3	Administration and others	AdmAndCo
<input type="checkbox"/>	4	Head of administration	HeadOfAdm
<input type="checkbox"/>	5	Development	Dev
<input type="checkbox"/>	6	Server room	Server
<input type="checkbox"/>	7	Production	Prod
<input type="checkbox"/>	8	Head of production	HeadProd
<input type="checkbox"/>	9	Material stores	MatStock

Number of records: 9

Room zone number column:

Contains the number of the room zone.

Room zone name column:

Contains the name for the room zone in the respective language.

Room zone short name column:

Contains the short name for the room zone in the respective language.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display Room zone access permissions" dialog

The **Display Room zone access permissions** dialog lists all persons with access permissions for the current day, including detailed information on employee category, ID card and type of permission for each selected room zone.

Note: The **Room zone access permissions** list is updated every day. Blocked persons/ID cards or persons whose access validity period has expired or not yet begun on the current day are not displayed.

Display Room zone access permissions						
Status: July 5, 2018 2:49:07 PM						
Room zone : 7 Production						
Last name	First name	Type	ID card number	Access weekly profile	Source	
Ackreiter	Thorsten	Per	9001	Always 1	Access profile 1	
Cermans	Paul	Per	8203	Production 11	Access profile 21	
Hochmeyer	Gertrud	Per	8201	Production 11	Access profile 21	
Kamp	Karsten	Per	8205	Production 11	Access profile 21	
Leconte	Sandra	Per	8206	Production 11	Access profile 21	
Meunier	Catherine	Per	8204	Production 11	Access profile 21	
Number of records: 6						
Room zone : 8 Head of production						
Last name	First name	Type	ID card number	Access weekly profile	Source	
Ackreiter	Thorsten	Per	9001	Always 1	Access profile 1	
Cermans	Paul	Per	8203	Production 11	Access profile 21	
Hochmeyer	Gertrud	Per	8201	Production 11	Access profile 21	
Kamp	Karsten	Per	8205	Production 11	Access profile 21	
Leconte	Sandra	Per	8206	Production 11	Access profile 21	
Meunier	Catherine	Per	8204	Production 11	Access profile 21	
Number of records: 6						

Status display:

Displays the date and time of the query.

Room zone display:

Displays the number and name of the room zone.

A table displays the access permissions for each room zone selected.

Last name column:

Contains the last name of the person.

First name column:

Contains the first name of the person.

Type column:

Contains the person group identifier; Per = employee, Ext = external company employee.

ID card number column:

Contains the number of the allocated ID card.

Access weekly profile: column:

Contains the applicable access weekly profile.

Source column:

Contains the access profile, the locking plan or specification of the special permission from which the access permission originates.

4.14.10 ID card history

The ID card history report displays the allocation of ID cards to persons. New entries are added to the ID card history when the allocation is removed.

Using the ID card history allows allocating bookings to a person after the removal of an ID card from a person record. This usually occurs for bookings at XS/evolo offline components if the bookings are read out from the components at greater time intervals only.

"ID card history" dialog

The **ID card history** dialog displays all changes in the allocation of ID cards to persons. This provides information on when a particular ID card was allocated to a person.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

The screenshot shows the 'ID card history' dialog with the following search filters:

- ID card number:
- Employee number:
- ID card label:
- Last name:
- from:
- First name:
- until:

A red 'Start search' button is located below the filters.

The results table is as follows:

ID card number	ID card label	Employee number	Person	Type	from	until
157852		3	Tamaira, Dallas	Vis	06/12/2017 11:02:51	

Number of records: 1

ID card number column:

Contains the unique ID card number.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Employee number column:

Contains the unique employee number of a person.

Person column:

Contains the name and first name of a person.

From column:

Contains the date from which the ID card was allocated to the person.

Until column:

Contains the date until when the ID card is allocated to the person. If the date is not present, the allocation is still valid.

Type column:

Contains the identifier of the group to which the person belongs.

Possible display:

- Per - persons, employees
- Ext - external company employees
- Vis - visitors

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

4.14.11 Blocked AoC ID cards

AoC Blocked ID cards contains all ID cards with a reason for blocking which is relevant for the AoC function.

Blocking reasons with AoC relevance are normally set if there is a risk that a person will find the ID card and thus be able to perform an access booking on an AoC reader. Because the ID card contains the access permissions, you must include this ID card in the list of blocked ID cards for the AoC validity.

Note 1: To enable the AoC readers to reject a blocked ID card you must synchronise the report manually with the AoC offline components.

Note 2: This list is only available if the AoC function is activated.

"Blocked AoC ID cards" dialog

The **Blocked AoC ID cards** dialog displays all ID cards that are currently blocked with an AoC-relevant blocking reason.

Use the toolbar buttons to add new ID cards to the list of blocked AoC ID cards.



ID card number	ID card version	ID card label	ID card type number	ID card type	Employee number	Last name	First name	Expiration date	
8204		204			8	Meunier	Catherine	Jun 10, 2017	

Number of records: 1

ID card number display field:

Contains the blocked ID card number.

ID card version display field:

Contains the version of the ID card.

Note: The **ID card version** column is only visible if **ID card administration level 3** is set in the system parameters.

ID card label display field:

Shows the label of the blocked ID card, if available.

Employee number display field:

Displays the unique employee number last assigned to the ID card.

Last name display field:

Displays the last name of the person with the employee number shown.

First name display field:

Displays the first name of the person with the employee number shown.

Expiration date display field:

Displays the date until which the ID card is blocked. This date corresponds with the AoC data on the ID card. The AoC data on the ID card is no longer valid after the date when the ID card expires; the ID card is then deleted from the system and can be allocated again.

Delete column:

Removes the ID card from the list of the blocked AoC ID cards. Before the record is finally deleted, the system displays a confirmation request.

Note: After the ID card is removed from the list of blocked ID cards, you must synchronise the XS/evolo offline components manually to make a booking with the ID card possible before the AoC validity expires. Synchronisation is not necessary if the AoC validity has already expired.

"Edit Blocked ID card" dialog

Use the **Edit blocked ID card** dialog to add further ID cards to the list of blocked ID cards.

ID card number  [Check data relating to ID card number](#)
 ID card version

ID card number	ID card version	ID card label	ID card type number	ID card type	Employee number	Last name	First name
9002		002			2	Martin	Eric

Number of records: 1

ID card number input field:

Contains the ID card number. Enter the ID card number you want to block.

Button :

Click the button to search for an ID card.

ID card version input field:

Contains the ID card version for the blocked ID card.

Note: The ID card version column is only visible if **ID card administration level 3** is set in the system parameters.

Check data related to ID card number button:

Click the button to display additional information on the selected ID card.

Table:**ID card number** column:

Contains the ID card number.

ID card version column:

Contains the ID card version, if available and if ID card administration level 3 is set in the system parameters.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Employee number column:

Contains the unique employee number if the ID card is allocated to a person.

Last name display field:

Contains the last name of the person if the ID card is allocated to a person.

First name display field:

Contains the first name of the person if the ID card is allocated to a person.

4.14.12 Blocks

All blocked persons are displayed in the Blocks report

"Display blocks" dialog

The **Display Blocks** dialog displays all blocked persons.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Blocking reason	Name	First name	Type	Time of blocking
1 - Blocked	Matrino	Johanna	Per	
1 - Blocked	Legrand	Marc	Per	

Number of records: 2

Reason for block column:

Contains the reason for blocking the person.

Last name column:

Contains the person's last name.

First name column:

Contains the first name of the person.

Type column:

Contains the person group identifier; Per = personnel/employee, Vis = visitor, Ext = external company employee.

Time of blocking column:

Contains the date on which the block was entered.

4.14.13 Attendance report

The attendance report displays all persons listed as present.

Note: An attendance report can only be maintained if access bookings are recorded as incoming and outgoing bookings.

If you work with folders in your system, you have the option to select a folder for report preparation before calling the report.

"Selection folders" dialog

The **Selection Folder** dialog lists all existing folders, for which you can generate an attendance report.

Note: Folders can only be selected if folders have been created in Area/Door management.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Number	Name	Short name
0	No folder	
1	Administration Building	B1
2	Production 1	P1
3	Production 2	P2

Number of records: 4

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Attendance report" dialog

The **Attendance report** dialog lists all persons recorded as present according to the selection.

Note 1: An attendance report can only be maintained if access bookings are recorded as incoming and outgoing bookings.

Note 2: The **Back to Selection** button is only available if folders are defined in your system.

Last name	First name	Employee number	Type	ID card number	ID card label	Folder
Ackreiter	Thorsten	1	Per	9001	001	No folder
Cermans	Paul	7	Per	8203	203	No folder
Hochmeyer	Gertrud	5	Per	8201	201	No folder
Leconte	Sandra	10	Per	8206	206	No folder
Meunier	Catherine	8	Per	8204	204	No folder

Number of records: 5

Last name column:

Displays the last name of the person.

First name column:

Displays the first name of the person.

Employee number column:

Displays the unique employee number.

Type column:

Contains the identifier of the group to which the person belongs.

Possible display:

- Per - persons, employees
- Ext - external company employees
- Vis - visitors

ID card number column:

Displays the ID card number of the ID card allocated to the person.

Note: If several ID cards are allocated to a person, a separate line is displayed for each ID card number.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Folder column:

Displays the folder in which the person is listed as present.

4.14.14 Visits

The **Visits report** gives you a quick overview of active or completed visits.

Note: This list is only available if Visitor administration is activated.

"Selection visits" dialog

The **Selection visits** dialog lists all existing visits within a selected period.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

State	From	Until	Last name	First name	Company	ID card	ID card label	Person visited - last name	Person visited - first name	Person visited - department
Green	6/12/2017 11:02	6/12/2017 03:00	Tamaira	Dallas	FFD	157852		Cermans	Paul	2 Production
Red	6/12/2017 07:00	6/12/2017 11:59	Lindsay	Joe	FFD			Hochmeyer	Gertrud	4 Sales

Number of records: 2

State column:

Contains the current state of the visit.

Possible display:

	Visit is reserved
	Visit is pre-activated
	Visit is active
	Visit is interrupted
	Visit is finished

From column:

Contains the date and time for the start of the visit.

Until column:

Contains the date and time for the end of the visit.

Last name column:

Contains the person's last name.

First name column:

Contains the first name of the person.

Company column:

Contains the name of the company for which the person works.

ID card number column:

Contains the number of the ID card that was used during the visit.

ID card label column:

Contains the label of the ID card that was used during the visit.

Person visited - last name column:

Contains the name of the person visited.

Person visited - first name column:

Contains the first name of the person visited.

Person visited - department column:

Contains the department to which the visited person belongs.

Open a record by clicking it.

"Show visit" dialog

The **Show visit** dialog displays the details of a visit. Changes cannot be made.

←
📄 Show visit

Title

Last name

First name

Company

Additional visitor details

Phone E-mail

Person visited

Employee number Department

Last name Function

First name Phone

Visit

Active

ID card number

Visit from Time

until Time

Access profile

Purpose

Comment

activated by: Administrator (admin)

Bookings and events

Visitor:

Contains information on the visitor.

Title display field:

Contains the visitor's title if available.

Name display field:

Contains the visitor's last name.

First name display field:

Contains the visitor's first name.

Company display field:

Contains the company where the visitor is employed.

Additional visitor details:

Contains additional information on the visitor.

Phone display field:

Free text for the visitor's phone number.

E-mail display field:

Free text for the visitor's e-mail address.

Person visited:

Contains the information on the person visited.

Employee number display field:

Contains the employee number of the person visited.

Name display field:

Contains the name of the person visited.

First name display field:

Contains the first name of the person visited.

Department display field:

Contains the department of the person visited.

Function display field:

Contains the role of the person visited.

Phone display field:

Contains the phone number of the person visited.

Visit:

Contains information on the visit.

Active display checkbox:

Indicates whether the visit has been set to active.

ID card number display field:

Contains the allocated visitor ID card if ID card assignment is activated for visitor administration.

Visit from display field:

Contains the time and date when the visit started.

Visit until display field:

Contains the time and date when the visit ended.

Access profile display field:

Contains the allocated access profile if ID card assignment is activated for visitors and the access permissions are associated with an access profile.

Purpose display field:

Contains information on the purpose of the visit.

Comment display field:

Contains additional information on the visit.

4.14.15 External company employee

The attendance times of external company employees are calculated using the Access IN and Access OUT access bookings of the external company employee at a reader/registration unit. The report states the times per day and the sum totals.

The booking types specified for Arrive access and Leave access in device management function allocation are evaluated.

Note: This list is only available if External company administration is activated.

"Selection Booking evaluation for external company employees" dialog

The **Selection Booking evaluation for external company employee** dialog displays all external company employees created.

Note: If the **Several ID cards per person** option is active, an individual record for the external company employee is displayed in the table for every ID card issued.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Selection Booking evaluation for external company employee

Last name: ID card number:
 First name: ID card label:
 External company:

Start search

<input type="checkbox"/>	Last name	First name	External company	ID card number	ID card label	Blocked	Delete
<input type="checkbox"/>	Schilling	Wolfgang	ACME	19001	ACME 19001	<input type="checkbox"/>	
<input type="checkbox"/>	Schmitz	Peter	ACME	19002	ACME 19002	<input type="checkbox"/>	

Number of records: 2

Last name column:

Contains the last name of the external company employee.

First name column:

Contains the first name of the external company employee.

External company column:

Contains the company for which the external company employee works.

ID card number column:

Contains the unique ID card number of the allocated ID card.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Blocked column:

Indicates if the external company employee is blocked and therefore has no booking permissions.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display Booking evaluation for external company employees" dialog

The **Display Booking evaluation for external company employee** dialog displays booking pairs (Arrive and Leave) for the selected external company employee along with the resulting attendance times.

One booking pair is output per line along with the elapsed time. The daily elapsed time is displayed in the last row of a day. In addition, the elapsed time for the period is displayed in a separate total line for each external company employee.

The total elapsed time of all selected external company employees is output as a sum total for the period at the end of the report.

Clicking an entry transfers this to the **Booking corrections** dialog where it can be edited.

Note: Bookings are shown for the calendar day. Attendances that cross the date limit must be manually added using the **Booking corrections** dialog by making bookings with 24:00 set as the leaving time and 00:00 set for the arrival time.

Display Booking evaluation for external company employee										
Time range From: 10/26/2018 until 10/27/2018 Start search										
External company	First name	Name	ID card number	ID card label	Date	Wd	From	To	Time	Day
ACME	Wolfgang	Schilling	19001	ACME 19001	10/27/2018	Sat	08:10	16:15	8:05	
							16:15 COR	17:00 COR	0:45	8:50
									Total	8:50
ACME	Peter	Schmitz	19002	ACME 19002	10/26/2018	Fri	08:31	16:31	8:00	8:00
					10/27/2018	Sat	08:10	12:10	4:00	
							12:30	16:15	3:45	7:45
									Total	15:45
									Sum total	24:35

Number of records: 8

External company column:

Contains the company for which the external company employee works.

First name column:

Contains the first name of the external company employee.

Last name column:

Contains the last name of the external company employee.

ID card number column:

Contains the unique ID card number of the allocated ID card.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Date column:

Contains the date of the bookings.

Wd column:

Contains the weekday of the bookings.

From column:

Contains the time of the Arrive booking and, where relevant, the booking source if the booking is a correction booking.

Until column:

Contains the time of the Leave booking and, where relevant, the booking source if the booking is not a correction booking.

Time column:

Difference between the From and To times. If one of the two times is missing, no time is displayed.

Day column:

Elapsed time for the day as a total in the Time column for the day and as a total of all daily totals for external company employees.

Sum total row:

The elapsed time across all selected external company employees and all days in the selected time range.

"Edit Booking corrections" dialog

The **Edit Booking corrections** dialog can be used to add missing bookings and alter existing bookings. Correction bookings can also be deleted.

Date field:

Contains the date for display. Use the arrows to scroll backwards or forwards by one day.

Table:

The table displays bookings from the selected day. Use the **New entry** button to manually add further bookings. These are indicated with "COR" in the display dialog.

From column:

Time of the Arrive booking.

Until column:

Time of the Leave booking.

4.14.16 Booking evaluation for person

The attendance times of persons are calculated using the Access IN and Access OUT access bookings at a reader/registration unit. The report states the times per day and the sum totals.

The booking types specified for Arrive access and Leave access in device management function allocation are evaluated.

Note: This function is a component of the additional module external company administration. If the external company administration licence is not available, the special "Basic time recording" licence is required.

"Selection Booking evaluation for person" dialog

The **Selection Booking evaluation for person** dialog displays all persons created.

Note: If the **Several ID cards per person** option is active, an individual record is displayed in the table for every ID card issued to the person.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

	Last name	First name	Department	Employee number	ID card number	ID card label	Blocked	Delete
<input type="checkbox"/>	Ackreiter	Thorsten		1	9001	001	<input type="checkbox"/>	
<input type="checkbox"/>	Cermans	Paul	2 - Production	7	8203	203	<input type="checkbox"/>	
<input type="checkbox"/>	Hochmeyer	Gertrud	2 - Production	5	8201	201	<input type="checkbox"/>	
<input type="checkbox"/>	Kamp	Karsten	2 - Production	9	8205	205	<input type="checkbox"/>	
<input type="checkbox"/>	Leconte	Sandra	2 - Production	10	8206	206	<input type="checkbox"/>	
<input type="checkbox"/>	Legrand	Marc	2 - Production	6	8202	202	<input checked="" type="checkbox"/>	

Last name column:

Contains the last name of the person.

First name column:

Contains the first name of the person.

Department column:

Contains the department to which the person is allocated.

Employee number column:

Contains the person's employee number.

ID card number column:

Contains the unique ID card number of the allocated ID card.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Blocked column:

Indicates if the person is blocked and therefore has no booking permissions.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Display Booking evaluation for person" dialog

The **Display Booking evaluation for person** dialog shows the booking pairs for the selected persons and a specified period along with the resulting elapsed time on a day-by-day basis.

One booking pair is output per line along with the elapsed time. The daily elapsed time is displayed in the last row of a day. In addition, the elapsed time for the period is displayed in a separate total line for each person.

The total elapsed time of all selected persons is output as a sum total for the period at the end of the report.

Clicking an entry transfers this to the **Booking corrections** dialog where it can be edited.

Note: Bookings are shown for the calendar day. Attendances that cross the date limit must be manually added using the **Booking corrections** dialog by making bookings with 24:00 set as the leaving time and 00:00 set for the arrival time.

Display Booking evaluation for person											
Time range From <input type="text" value="10/26/2018"/> until <input type="text" value="10/27/2018"/> <input type="button" value="Start search"/>											
Department	Employee number	First name	Name	ID card number	ID card label	Date	Wd	From	To	Time	Day
2 - Production	7	Paul	Cermans	8203	203	10/26/2018	Fri	08:31	16:31	8:00	8:00
						10/27/2018	Sat	08:10	12:10	4:00	
								12:30	16:15	3:45	7:45
										Total	15:45
2 - Production	5	Gertrud	Hochmeyer	8201	201	10/26/2018	Fri	07:31	16:31	9:00	
								17:00 COR	17:45 COR	0:45	9:45
						10/27/2018	Sat	09:10	11:10	2:00	
								13:30	16:15	2:45	4:45
						Total			14:30		
										Sum total	30:15
Number of records: 10											

Department column:

Contains the department to which the person is allocated.

First name column:

Contains the first name of the person.

Last name column:

Contains the last name of the person.

ID card number column:

Contains the unique ID card number of the allocated ID card.

ID card label column:

Contains the label visible on the assigned ID card, if available.

Date column:

Contains the date of the bookings.

Wd column:

Contains the weekday of the bookings.

From column:

Contains the time of the Arrive booking and, where relevant, the booking source if the booking is a correction booking.

Until column:

Contains the time of the Leave booking and, where relevant, the booking source if the booking is a correction booking.

Time column:

Difference between the From and To times. If one of the two times is missing, no time is displayed.

Day column:

Elapsed time for the day as a total in the Time column for the day and as a total of all daily totals for the person.

Sum total row:

The elapsed time across all selected persons and all days in the selected time range.

"Edit Booking corrections" dialog

The **Edit Booking corrections** dialog can be used to add missing bookings and alter existing bookings. Correction bookings can also be deleted.

Date field:

Contains the date for display. Use the arrows to scroll backwards or forwards by one day.

Table:

The table displays bookings from the selected day. Use the **New entry** button to manually add further bookings. These are indicated with "COR" in the display dialog.

From column:

Time of the Arrive booking.

Until column:

Time of the Leave booking.

4.14.17 Smart phone status

The **Smartphone status** record contains all authorised persons and smartphones allocated to a person, an external company employee or a visitor along with the status of access permissions conferred.

Note: This list is only available if Mobile Access is activated.

"Selection Smart phone status" dialog

The **Status smartphone selection** dialog displays a list of all smartphones created in the system that are assigned to a person, an external company employee or a visitor and that have permissions. The displayed status is a compilation of the access permission transfers of all devices for which the smartphone is authorised. Click an entry to display the details of the individual access permissions.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

Person column:

Contains the last name and the first name of the person to whom the smartphone is allocated.

Employee number column:

Contains the employee number of the person to whom the smartphone is allocated.

ID card number column:

Contains the ID card number allocated to the smartphone.

Mobile Access device number column:

Contains the Mobile Access device number of the smartphone.

State column:

Displays the current transfer status of the smartphone. If access permissions are currently being transferred to a device, the status will be "Transferring" even if the access permissions have already been transferred to all other devices. The status is only changed to "Transfer complete" once all transfers have been completed.

	Transferring
	Transfer complete
	Transfer error
	Status unknown

"Display Smart phone status" dialog

The **Smartphone status display** dialog displays details of the individual access permissions for a smartphone.

**Transfer status:**

Displays the current transfer status of the smartphone. If access permissions are currently being transferred to a device, the status will be "Transferring" even if the access permissions have already been transferred to all other devices. The status is only changed to "Transfer complete" once all transfers have been completed.

	Transferring
	Transfer complete
	Transfer error
	Status unknown

4.14.18 Time-controlled reports

You can use the time-controlled reports to execute dynamic reports at configurable times. You can define daily, weekly, monthly or periodically recurring times. You can also specify flexibly recurring times using a Cron expression.

Time-controlled reports are saved as job definitions that are automatically executed at the defined times. The resulting reports are saved on the server in a directory that is only accessible to the current user, who can download the latest version to a workstation.

The report can be sent by e-mail in addition, provided that a mail server is configured. The sending of the e-

mail is not saved in the database, but directly executed. If it is not possible to connect to the mail server, a message to this effect is generated.

Note: Time-controlled reports are only available if the system parameter "210 Use time-controlled reports" is activated. System parameter "211 Target directory for time-controlled reports" defines the target directory in which the reports are saved.

"Selection Time-controlled reports" dialog

The **Selection Time-controlled reports** dialog displays all time-controlled reports created for the logged-in user.

The Search function can be used to limit the selection using a single filter criterion or a group of filter criteria.

<input type="checkbox"/>	Number [▲]	Name	Last execution time	Delete	Download
<input type="checkbox"/>	3	Daily data			Download report
<input type="checkbox"/>	4	Blocked Persons			Download report

Number of records: 2

Download report button:

Use this button to save the last report created from the server onto the workstation.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

"Edit Time-controlled report" dialog

You can use the **Edit Time-controlled report** dialog to create and edit time-controlled reports.

← 📄 📁 🗑️ 🔄 📄

Edit Time-controlled report

Number

Name

Short name

Active

Report » Export type

Search profile »

Cycle type

Shift days

Execution time

E-mail to address +

E-mail to user » +

Print output sorting

Position	Sort column	Sorting	Page break (PDF)		
1	Department	Ascending	<input type="checkbox"/>		
2	Last name	Ascending	<input type="checkbox"/>		
3	Work schedule	Ascending	<input type="checkbox"/>		

Number of records: 3

New entry

Last execution start time 16/1/2020 15:45:48

Last execution time 16/1/2020 15:45:55

Last execution state OK

File at ..\report\scheduledreports\admin\Daily Data

Run report
Download report
Send report

Active checkbox:

Indicates whether the time-controlled report is active.

Activated: Time-controlled report is active and executed reports are saved.

Not activated: Time-controlled report is not active and no reports are executed.

Report selection field:

Selection of the dynamic report that is to be created.

Options:

- All dynamic reports created in the system that do not require additional search parameters.

Export type selection field:

Selects whether the report is exported as a PDF or CSV file.

Cycle type selection field:

Selects the interval for executing the report.

Options:

- daily: Execution time = time in hh:mm format (24-hour format)
- weekly: Execution time = time in hh:mm format; allocation of one or more weekdays on which the report is to be generated
- monthly: Execution time = time in hh:mm format; allocation of one or more days of the month on which the report is to be generated
- periodically: Specification of an execution cycle in whole hours. Example: If the value "4" is entered in **Cycle (hours)**, the report is generated every 4 hours from the current time.
- Cron expression: manual input of a Cron expression. The **Show CRON syntax help** button displays a help text for a valid syntax in the dialog.

E-mail to address multiple input:

Contains an e-mail address to which the report will be sent. Multiple e-mail addresses can be specified, if necessary.

E-mail to user multiple selection:

Contains the user to whom the report will be sent. Multiple users can be specified, if necessary.

Print output sorting table:

All fields defined for person selection in the configured header data can be used for sorting the records in the report.

Note: The table is only present if fixed reports have been selected such as the "Yearly overview – Person" or the "Daily data" and "Monthly overview" from the Time module.

Position column:

Contains the table row. If the position is changed, all subsequent positions will be incremented by one position.

Sort column column:

Contains the sorting sequence which specifies the field name.

Sorting column:

Specifies how the data is sorted.

Options:

- Ascending: The records are sorted in ascending order, starting with the smallest value.
- Descending: The records are sorted in descending order, starting with the greatest value.

Execution time input field:

Specifies the time when the time-controlled report is to be created. Other fields may be displayed depending on the cycle type selected.

Last execution time display:

Contains the time when the report was generated.

Last execution state display:

Contains a status message for the last execution.

Run report button:

Immediately generates a report, regardless of the specified interval.

Download report button:

Downloads the last generated report from the server directory to the workstation.

Send report button:

Sends the report to the specified e-mail addresses. The mail server must be set up for this.

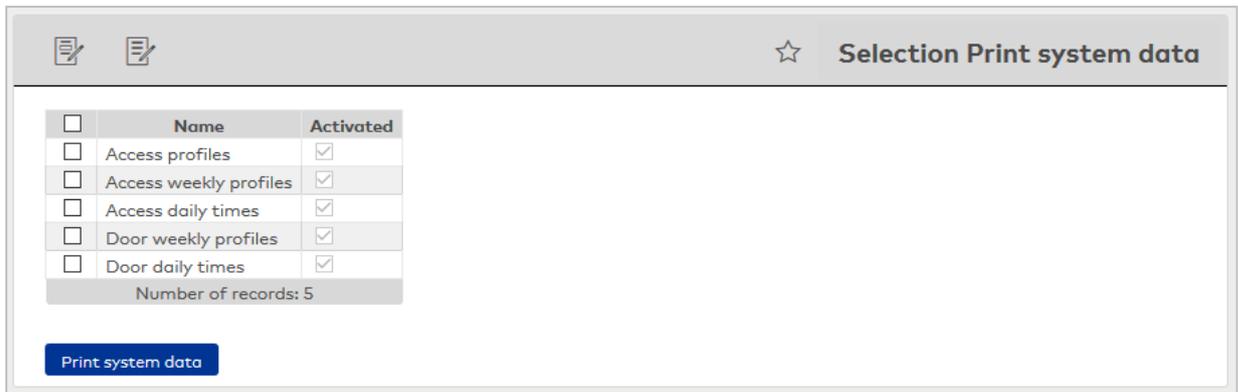
4.14.19 Print system data

You can use the system data printout to create a PDF file for printing the selected user data. In the configuration of the individual user data, you can specify the information content of the report according to your requirements.

"Selection print system data" dialog

The **Selection Print system data** dialog lists all existing user data in the access system. This data can be output as a PDF file.

Note: This dialog is only displayed if the system administration is activated in the system parameters and systems have been created.

**Name** column:

Contains the name of the user data.

Activated column:

Indicates if the user data are included in the PDF file.

Open a record by clicking it. Open multiple records by highlighting the records and clicking the **Edit selected search results** symbol.

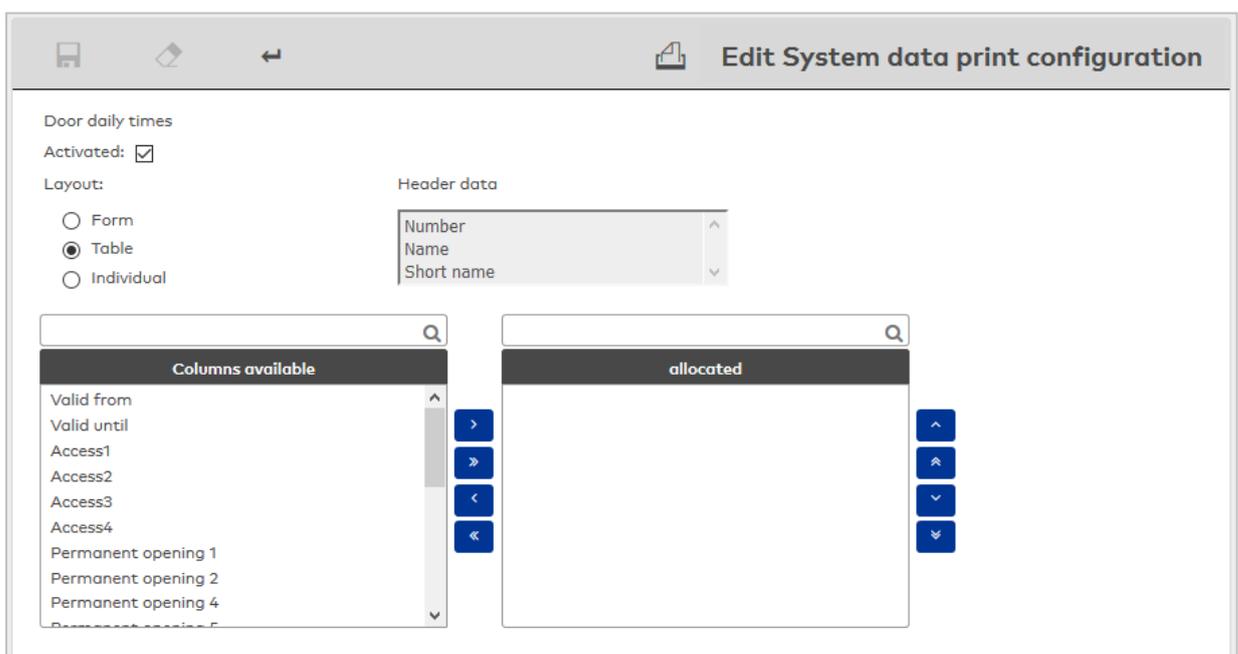
"Edit system data print configuration" dialog

Use the **Edit system data print configuration** dialog to specify the output format and the fields included in the output for different user data.

The configuration is the same for all user data and is comprised of the following:

- Layout
- Header data
- Columns containing the fields' content.

Note: Depending on the displayed user data, not all configuration options may be available. The possible columns correspond to input fields in the respective dialogs used to edit the relevant user data.

**User data** display:

Displays to which user data the configuration applies.

Activated checkbox:

Indicates if the user data are included in the PDF file. Deselect the checkbox to exclude the user data from the PDF file.

Layout selection:

The layout determines the display of the data.

Options:

- Table: The data are displayed as a table.
- Form: The data are displayed as a form.
- Individual: Each record is displayed on a separate page.

Header data display field:

Displays the header in the PDF file.

Available columns report:

Contains all columns which can be allocated to the printout. Click a column name to select it and then click the right arrow. The selected column is added to the printout.

Columns allocated report:

Contains all columns that are allocated to the printout. Click a column name to select it, then click the left arrow to remove the column from the printout.

4.15 Special reports

The **Special reports** menu lists all the created reports which are not included in the reports main menu **Reports**.

Click a report to call it up and display it. If the report is linked to a search profile that contains search wildcards, the corresponding search input fields are displayed. Once the search values have been entered, the search can be executed and the result is displayed in the report.

"Display Report" dialog

Use the **Display report** dialog to display the configurable reports. The dialog title contains the name of the report.

Example: Report with parameter input

Blocking reason ⓘ

Start search

Blocked persons

Department	Last name	First name	Blocking reason
1 - Administration	Matrino	Johanna	Blocked
2 - Production	Legrand	Marc	Blocked

Number of records: 2

Example: Fixed report without parameter input

The table contains the fields configured in the search profile report layout.

5 Glossary

A

Access daily time

Access daily times are used to define to the minute for each day the time intervals when a person with an authorised ID card is granted access.

Access profiles

You can form access profiles from any number of access permissions. An access permission consists of a door (reader) or room zones and an access weekly profile. The doors/readers and the room zones determine the local specifications and the access weekly profiles determine the time specifications.

Access weekly profile

An access weekly profile determines for each day of a week which access daily time is used. The access weekly profiles thus form the time-related component for the access permissions.

Anti-passback room control

The anti-passback room control specifies that a person may only enter the room zone, if they were previously registered as present in the neighbouring room zone

D

Digital Key

Simple mobile access solution with ID card number (mobile ID) using vouchers.

Digital Key Pro

Flexible mobile access solution with LEGIC Mobile Access Connector. Authorisation is granted via Infinilink or Infini-ID.

Door group

Door groups can be mapped using room zones (without movement control).

L

Locking plan

The locking plan is a simple way of assigning access permissions. It is displayed in a table. Permissions are activated using a checkbox at the intersections of the columns and lines.

O

Office release

Office release allows the manually-controlled permanent opening of a door, for example if you are in your office and you want everyone to have free access to your office during this period. The office release can be ended at any time, for example if you leave your office.

Offline door

Offline doors are doors with standalone components, i.e. components that are not connected wirelessly or by cables. Permissions or other alterations must always be transferred using XS manager or the evolo Programmer.

Online door

Online doors are doors with online or wireless components. This means that they are connected to a terminal either by a cable or wirelessly. Permissions and other alterations are exchanged directly between the components and MATRIX.

R**Room zone**

A room zone is a physically enclosed area that consists of one or more access points with assigned readers. Access functions can be associated with a room zone; their properties are defined using access parameters.

T**Timed anti-passback**

Prevents a person from entering a room zone again for a specified time.

6 Index

A

access 163

access control 163

Access control for two persons (how to) 17

Access daily times 71

access permissions

- access profile 62
- door 223
- person 220
- room zone 224

Access permissions overview 218

Access profiles 61, 216

access times

- persons 72

Access times 137, 215

Access via smartphone 10

Access weekly profiles 68

Add a door (how to) 13

anti-passback room control 120

AoC 121, 127, 129

AoC (how to) 27

AoC ID cards 227

AoC special interval 120

AoC tracking 53, 80, 103

Area monitoring 188

area/door administration 114

Attendance display (access) 205

Attendance report 230

B

Bank holiday templates 149

Bank holidays 144, 151

Blocks 230

Booking evaluation for person 238

C

cabinet door 121

Calendar 146

Calendar administration 142

Calender 142

company special days 147

connecting door 128

Corrections 164

Counting groups 131

Counting information (how to) 35

D

Day types 154

Departments 60

door administration 114

Door administration 114

Door daily times 135

Door groups 162

Door monitoring 191

Door opening

- with keyboard input 14

Door opening code 14

Door selection 195-196

Door weekly profiles 132

doors

- security areas 127

Duress alarm (how to) 25

Dynamic reports 247

E

emergency exit door 116
 evolo time profiles 70
 evolo time profiles in the door weekly profile 133
 External companies 85
 External company administration 76
 External company employees 76, 235

F

folders 126

H

hard anti-passback 120
 Holidays 146

I

ID card administration 98
 ID card history 226
 ID cards 99
 Identification code 15
 IDS 169
 Interlocks 165
 Intruder detection system 169
 Intruder detection system (how to) 33

K

Key codes (how to) 14

L

Lift control (how to) 30
 Lifts 167
 Locking plan 156

Locking plan administration 155

M

Manual image comparison (how to) 44
 Manual image comparison (popup dialog) 194
 manual special days 147
 Mobile Access (how to) 10
 monitoring doors 128
 Motion recording 137

O

office release
 activate 53, 80, 103
 Office release 137
 Office release (how to) 18
 Offline employee record 53, 80, 102

P

patrol
 log 203
 set up 199
 Patrol 197
 Patrol definitions 201
 patrols 199
 Permanent opening 137
 Permissions 52, 102
 Person access report 211
 Person administration 46
 Person groups 161
 Persons 46
 PIN code check 137, 139
 Print system data 245
 Priority circuits 66, 106

R

Reader events report 212
 Reader locations 213
 Reason for blocking ID card 101
 Reason for blocking person 101
 Reasons for blocking ID card 109
 Reasons for blocking person 73
 Replacement ID card 102
 Reports (access) 210
 reservation 110
 Room administration 110
 room reservation 110
 room zone
 security area 119, 121
 room zone/door administration 114
 Room zone/door administration 114
 Rooms 113

S

Search profiles 74
 Security area daily programs 141
 Security area weekly profile 139
 security areas 114, 122
 status display 188
 Set up IDS (how to) 33
 Smart phone status 241
 special days 147
 allocate 145
 status display
 doors 191
 substitute daily programs
 allocate 72, 137

T

Threat code (how to) 25
 Time-controlled reports 242
 timed anti-passback 119

V

VBI permissions 64
 video camera 130
 Video surveillance (how to) 37
 Video verification (how to) 44
 Visitor administration 86
 Visitor administration (how to) 20
 Visitor administration with QR codes (how to) 23
 Visitor overview 86
 Visitor reservations 92
 Visitors 96
 Visits 232

W

weekdays
 allocate 146
 Weekdays 152