



**BOSCH**

# **Access Management System**

AMS configuration and operation

**en**

Software Manual



## Table of contents

<b>1</b>	<b>Using Help</b>	<b>6</b>
<b>2</b>	<b>About this documentation</b>	<b>8</b>
<b>3</b>	<b>AMS System overview</b>	<b>9</b>
<b>4</b>	<b>Licensing the system</b>	<b>10</b>
<b>5</b>	<b>Configuring the calendar</b>	<b>11</b>
5.1	Defining Special days	11
5.2	Defining Day models	13
5.3	Defining Time models	14
<b>6</b>	<b>Configuring Divisions</b>	<b>17</b>
6.1	Assigning Divisions to devices	17
6.2	Assigning Divisions to operators	18
<b>7</b>	<b>Configuring the IP addresses</b>	<b>19</b>
<b>8</b>	<b>Using the device editor</b>	<b>20</b>
<b>9</b>	<b>Configuring areas of access control</b>	<b>22</b>
9.1	Configuring areas for vehicles	23
<b>10</b>	<b>Configuring operators and workstations</b>	<b>26</b>
10.1	Creating the workstations	26
10.2	Creating workstation profiles	27
10.3	Assigning workstation profiles	28
10.4	Creating user (operator) profiles	28
10.5	Assigning user (operator) profiles	29
10.6	Setting passwords for operators	30
<b>11</b>	<b>Configuring card codes</b>	<b>32</b>
<b>12</b>	<b>Configuring the controllers</b>	<b>35</b>
12.1	Configuring MACs and RMACs	35
12.1.1	Configuring a MAC on the DMS server	35
12.1.2	Preparing MAC server computers to run MACs and RMACs	36
12.1.3	Configuring a MAC on its own MAC server	37
12.1.4	Adding RMACs to MACs	38
12.1.5	Adding further MAC/RMAC pairs	40
12.1.6	Using the MAC installer tool	41
12.2	Configuring the LACs	42
12.2.1	AMC parameters and settings	44
<b>13</b>	<b>Configuring Entrances</b>	<b>60</b>
13.1	Entrances - introduction	60
13.2	Creating entrances	60
13.3	Additional I/O checks	64
13.4	Configuring AMC terminals	65
13.5	Predefined signals for door models	70
13.6	Special entrances	76
13.6.1	Elevators (DM07)	76
13.6.2	Door models with intruder alarms (DM14)	79
13.6.3	DIPs and DOPs (DM15)	82
13.6.4	Mantrap door models	83
13.7	Doors	85
13.8	Readers	88
13.8.1	Configuring random screening	98
13.9	Access by PIN alone	98

13.10	AMC extension boards	99
<b>14</b>	<b>Custom Fields for personnel data</b>	<b>103</b>
14.1	Previewing and editing Custom fields	103
14.2	Rules for data fields	105
<b>15</b>	<b>Configuring Milestone XProtect to use AMS</b>	<b>106</b>
<b>16</b>	<b>Configuring Threat Level Management</b>	<b>108</b>
16.1	Concepts of Threat Level Management	108
16.2	Overview of the configuration process	108
16.3	Configuration steps in the device editor	109
16.3.1	Creating a threat level	109
16.3.2	Creating a Door security profile	109
16.3.3	Creating a Reader security profile	110
16.3.4	Assigning door and reader security profiles to entrances	111
16.3.5	Assigning a threat level to a hardware signal	112
16.4	Configuration steps in System data dialogs	113
16.4.1	Creating a Person security profile	113
16.4.2	Assigning a Person security profile to a Person Type	113
16.5	Configuration steps in Personnel data dialogs	114
<b>17</b>	<b>Creating and managing personnel data</b>	<b>115</b>
17.1	Persons	115
17.1.1	Card control / building control options	117
17.1.2	Extra info: Recording user-defined information	117
17.1.3	Recording signatures	117
17.1.4	Enrolling fingerprint data	118
17.2	Companies	119
17.3	Cards: Creating and assigning credentials and permissions	120
17.3.1	Assigning cards to persons	120
17.3.2	Authorizations tab	122
17.3.3	Other data tab: Exemptions and special permissions	122
17.3.4	Authorizing persons to set Office mode	123
17.3.5	Smartintego tab	124
17.3.6	Creating an Alert card	126
17.4	Temporary cards	126
17.5	PIN codes for personnel	128
17.6	Blocking access for personnel	129
17.7	Blacklisting cards	130
17.8	Editing multiple persons simultaneously	132
<b>18</b>	<b>Defining access authorizations and profiles</b>	<b>135</b>
18.1	Creating access authorizations	135
18.2	Creating access profiles	135
<b>19</b>	<b>Managing visitors</b>	<b>137</b>
19.1	Visitor data	137
19.2	Visitor too late	142
<b>20</b>	<b>Managing parking lots</b>	<b>144</b>
20.1	Authorizations for several park zones	144
20.2	Parking lot report	145
20.3	Extended Car Park management	145
<b>21</b>	<b>Managing guard tours and patrols</b>	<b>147</b>
21.1	Defining guard tours	147

---






21.2	Managing patrols	148
21.3	Tour monitoring (formerly path control)	149
<b>22</b>	<b>Random screening of personnel</b>	<b>151</b>
<b>23</b>	<b>Using the Event Viewer</b>	<b>153</b>
23.1	Setting filter criteria for time relative to the present	153
23.2	Setting filter criteria for a time interval	153
23.3	Setting filter criteria irrespective of time	154
<b>24</b>	<b>Using reports</b>	<b>155</b>
24.1	Reports: master data	155
24.1.1	Reporting on vehicles	157
24.2	Reports: system data	158
24.3	Reports: authorizations	159
<b>25</b>	<b>Operating Threat Level Management</b>	<b>161</b>
25.1	Triggering and cancelling a threat alert via UI command	161
25.2	Triggering a threat alert via hardware signal	162
25.3	Triggering a threat alert via Alert card	162
<b>26</b>	<b>Backup and Restore</b>	<b>163</b>
26.1	Backup procedure	163
26.2	Restore procedure	164
	<b>Glossary</b>	<b>166</b>

---

# 1 Using Help




How to use this help file.

## Tool bar buttons

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

## Tabs

### Contents

This tab displays a hierarchical table-of-contents. Click a book icon  to open it  and then click on a topic icon  to view the topic.

### Index

This tab displays an index of terms in alphabetical order. Select a topic from the list or type in a word to find the topic(s) containing it.

### Search

Use this tab to find any text. Enter text in the field and then click button: **List Topics** to find topics that contain all the words entered.

## Resizing the help window

Drag the corner or edge of the window to the desired size.

## Further conventions used in this documentation

- Literal text (labels) from the UI appears in **bold**.  
E.g. **Tools, File, Save As...**
- Sequences of clicks are concatenated using the > character (the greater-than sign).  
E.g. **File > New > Folder**
- Changes of control-type (e.g. menu, radio-button, check box, tab) within a sequence are indicated just before the label of the control.  
E.g. Click menu: **Extra > Options > tab: View**
- Key combinations are written in two ways:

- Ctrl+Z means hold down the first key while pressing the second
- Alt, C means press and release the first key, then press the second
- The functions of icon buttons are added in square brackets after the icon itself.  
E.g. [Save]

## 2 About this documentation

This is the main software manual for the Access Management System.

It covers the use of the main dialog manager program, hereafter referred to as AMS

- The configuration of an access control system in AMS .
- The operation of the configured system by system operators.

### **Related documentation**

The following are documented separately:

- The installation AMS and its auxiliary programs.
- The operation of AMS - Map View.



### 3 **AMS System overview**

Access Management System is a powerful, pure access control system, which performs solo or in concert with BVMS, the Bosch flagship video management system.

Its power stems from its unique balance of leading-edge and proven technologies:

- Designed for usability: practical user interface with drag-and-drop Map View, and streamlined biometric enrollment dialogs.
- Designed for data security: supporting the latest standards (EU-GDPR 2018), operating systems, databases and encrypted system interfaces.
- Designed for resilience: middle-layer main access controllers provide automatic failover and replenishment of local access controllers in case of network failure.
- Designed for the future: regular updates and a pipeline full of innovative enhancements.
- Designed for scalability: offering low to high entry levels.
- Designed for interoperability: RESTful APIs, with interfaces to Bosch video management, event handling and specialized partner solutions.
- Designed for investment-protection: allowing you to build on, but boost the efficiency of, your installed access-control hardware.

## 4 Licensing the system

### Prerequisites

- The system has been installed successfully.
- You are logged onto the AMS server computer, preferably as Administrator.

### Procedure for purchased licenses

**Prerequisites:** You have purchased licenses based on the computer signature of this computer. Contact your sales representative for instructions.

Dialog path: **Configuration > Licenses**

1. Log onto AMS, the Access Management System.  
**Note:** If AMS is installed und the Windows Program Files folders, log on with Windows Administrator rights.
2. Navigate to **Configuration > Licenses**
3. Click **Start license manager**
4. In the **License Manager** window, select the check box of the base package that you have purchased.
5. In the **License Activation** popup window,
  - Paste the **Computer Signature** of the Access Manager server computer,
  - Paste the **License Activation Key** that you received for the base package,
  - Click **Activate...**
6. In the **License Manager** window, verify that the base package you have just licensed now has the status **Activation valid**.
7. In the **License Manager** window,
  - Click **Import Bundle Info** to browse to and activate any license bundles that you have purchased and received as files.
  - Click **Import License** to browse to and activate any individual licenses that you have purchased and received as files.
8. Click **Close** to close **License Manager**.
9. Back in the main **Licenses** dialog, verify that the features that you purchased are listed with the correct number of units.

### Procedure for Demonstration Mode

Demonstration Mode licenses all system features for a limited period. Use Demonstration Mode only in non-production environments to try out features before purchasing them.

1. Log onto the Access Manager
2. Navigate to **Configuration > Licenses**
3. Click the button **Activate Demo Mode**
4. Verify that the features are listed in the **Licenses** dialog window.

Demonstration mode is activated for 5 hours. Note that the expiration time is displayed near the top of the **Licenses** dialog, and in the title bar of most dialog windows.

## 5 Configuring the calendar

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

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

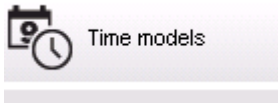
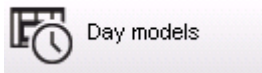
Time models control activities when they are applied to the underlying **calendar** of the access control system.

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

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

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

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



### 5.1 Defining Special days

When this is opened, a list appears in the top list field of the dialog containing all specified holidays. Please note that all holiday dates shown relate only to the current year. However, the calendar is updated from year to year in accordance with the data entered.

Beneath the list there are different dialog fields for the creation of new special days and for the change or deletion of existing special days. To add a new special day, at least three of these input fields must contain data. First a **description** and a **date** must be entered in the respective fields. Thirdly the **class** to which this special day belongs must be selected from the appropriate selective list.

Division: Common

« System data

**S** Special days

Day models

Time models

List of available special days

Date (cur. year)	Description	Day model	Division
Mi 01/01/2014	New Year	DMAC-Holiday	Common
Mo 01/20/2014	Martin Luther King Jr. Day	DMAC-Holiday	Common
Mo 02/17/2014	Presidents' Day	DMAC-Holiday	Common
Mo 05/26/2014	Memorial Day	DMAC-Holiday	Common
Fr 07/04/2014	Independence Day	DMAC-Holiday	Common
Mo 09/01/2014	Labor Day	DMAC-Holiday	Common
Mo 10/13/2014	Columbus Day	DMAC-Holiday	Common
Di 11/11/2014	Veterans' Day	DMAC-Holiday	Common
Do 11/27/2014	Thanksgiving Day	DMAC-Holiday	Common
Do 12/25/2014	Christmas Day	DMAC-Holiday	Common

Create, modify, or delete a special day

Description:

Day model: DMAC-Holiday : Holiday : Common

Date: 10/01/\*\*\*\* every year

Days to add: 7

Week day: Montag : after the date

Date in this year: Mo 10/13/2014

Priority: 60    Valid from:     until:

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

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

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

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

The assignment of a **validity period** is also optional. If no duration is specified, the default settings make validity unlimited from the input date.

A **priority** can also be set. The priority, rising from 1 to 100, defines which holiday shall be used. If two holidays fall on the same date, the holiday with the higher priority ranges first. In case of equal priorities it is undefined which holiday will be used.

Holiday with the priority "0" are deactivated and will not be used.

The dialog **Time Models** displays only the active holidays, i.e. with a priority greater than 0.

**Notice!**



A time model of the division "Common" can only use holidays which are assigned to the division "Common".

A time model of a specific division "A" can only use holidays which are assigned to the division "A".

It is not possible to mix holidays between divisions, i.e. every division can use only the specific holidays which are assigned to it in its specific time model.

## 5.2 Defining Day models

Day models define a pattern for any day. They can have up to three time intervals.

Once the dialog is started, all existing day models are displayed.

« System data

Special days

**Day models**

Time models

Division: **Common**

List of available day models of the access control

Day model	Description	Start time	End time	Start time	End time	Start time	End time	Division
DMAC-Holiday	Holiday	01:00:00 AM	07:00:00 AM					Common
DMAC-none	none							Common

Create, modify, or delete day models of the access control


Name:  Description:

Time intervals: Start time: End time:

1st interval:

2nd interval:

3rd interval:

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

Start and End times for an interval are entered in hours and minutes. As soon as such a time is reached the interval is activated or deactivated respectively. In order to mark these times more clearly as delimiters, the list pane displays them with seconds (always 00). For example, an authorization in a time model which contains an interval from 8:00 AM to 3:30 PM allows access from 8:00 AM to 3:30 PM but prevents access at 3:30:01 PM.

Start and end times are subjected to logical checks when they are entered, for instance a start time must be smaller than its corresponding end time.

One consequence of this is that no interval may extend over midnight, but has to be split at that point:

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

With the exception of midnight (12:00 AM) no overlaps are allowed between the interval delimiters of a single day model. Note, this precludes the entering of the same time for the end of one and the beginning of the next interval.

Exception: A 24 hour interval nevertheless has start and end times both set to 12:00 AM.

**Notice!**



Tip: You can check intervals by viewing them in the Time models dialog: First create a day model containing those intervals (System data > Calendar > Day models). Then assign this day model to a dummy time model with a period of one day (System data > Calendar > Time models). The intervals are then illustrated in the bar graphic.

Exit the Time models dialog without saving the changes.

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

### 5.3 Defining Time models

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

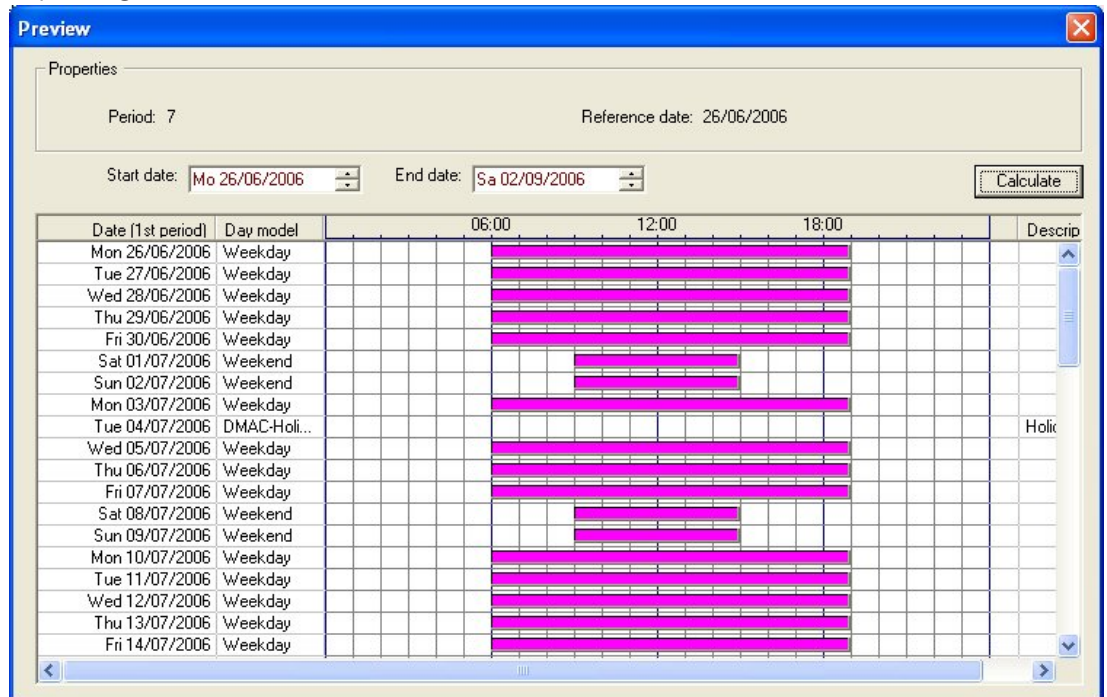
If the mask is empty, time models can be created from scratch. To do this, you must enter a **name** and the number of days in the **period** and select a starting or **reference date**. When this data is confirmed (**Enter**), a list appears in the **Assignment of day models** dialog field below it. The number of lines in this list corresponds to the number of days set above, and the columns already contain a progressive number and the dates for the period, beginning with the start date selected.

Only entries of the column **"Name"** can be changed or inserted by the user in this list - as already mentioned, the entries in the columns **"No"** and **"Date"** arise from the declarations of the dialog head; the column **"Description"** is filled out by the system with the choice of a day model and the explanations done in this dialog.

By double-clicking in the relevant line of the **Day model** column, a selection list field is activated. One of the existing day models can be selected from this list. In this way, a specific day model can be assigned to each day of the period. When the user switches to another line, an existing description of the selected day model is indicated by the system in the **Description** column.

The predefined **holidays** with the relevant day models are shown in the lower list field for navigation and checking purposes. For the selected or newly created time model, the assignment of day models to certain holidays can be changed. However, these changes will only apply to this particular time model - general changeovers that are to apply to all existing and future models can only be performed in the Holidays dialog. In line with these settings, the week days are then given the assigned day models, in consideration of the holidays. Then appropriately to these settings the weekdays are faced with the assigned day models under consideration of the special days. To quickly check that day models are have been used and assigned correctly - particularly on holidays - this dialogue contains a **preview** that shows the day allocation of certain periods.

Finally, a separate dialog box is opened by clicking the **Preview** button and a time period of up to 90 days can be specified, including holidays. When the **Calculate** button is clicked, the report is composed and displayed as shown below - this process can take a few seconds depending on the size of the interval.



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

Time model of the access control

Name: All Description:

Period: 6 Reference date: Tu 07/21/2015  Ignore special days

Assignment of day models

No.	Day model	6:00AM	12:00PM	6:00PM	Description	Date (1st period)	Division
7274568	DMAC-Holi...	[shaded]			Holiday	Di 07/21/2015	Commc
7274568	DMAC-Holi...	[shaded]			Holiday	Mi 07/22/2015	Commc
7274569	DMAC-Holi...	[shaded]			Holiday	Do 07/23/2015	Commc
7274570	DMAC-Holi...	[shaded]			Holiday	Fr 07/24/2015	Commc
7274571	DMAC-Holi...	[shaded]			Holiday	Sa 07/25/2015	Commc
7274572	DMAC-none				none	So 07/26/2015	Commc

Holiday	Day model	6:00AM	12:00PM	6:00PM	Description	Date (1st period)	Division



# 6 Configuring Divisions

## Introduction

The system may be licensed optionally to provide joint access control for a facility which is shared by any number of independent parties, called **Divisions**.

System operators can have one or more divisions assigned to them. Operators then see only the persons, devices and entrances of those divisions.

Where the **Divisions** feature is not licensed, all objects managed by the system belong to a single division called **Common**.



## Prerequisites

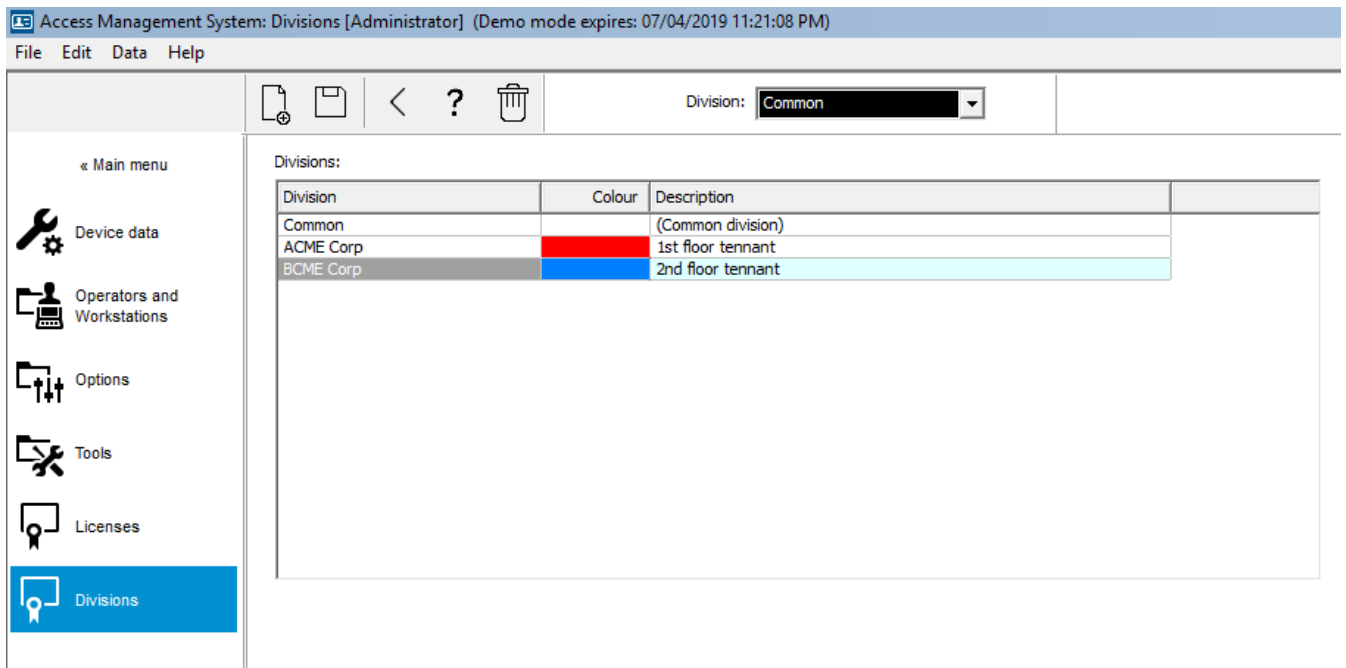
- The Divisions feature is licensed for your installation.

## Dialog path

- Main menu > **Configuration** > **Divisions**

## Procedure

1. Click  in the tool bar.
  - A new Division is created with a default name.
2. Overwrite the default name and (optional) enter a description for the benefit of other operators.
3. Click in the **Color** column to assign a color to help distinguish the division’s assets in the user interface.
4. Click  to save



## 6.1 Assigning Divisions to devices

Assign Divisions to devices in the Device editor

### Dialog path


Main menu > **Configuration** > **Device data**

**Prerequisites**

- Divisions are licensed and in operation
- At least one division has been created.

**Procedure**

1. In the Device tree, select the device for assignment.
  - The device editor appears in the main dialog pane.
2. From the Division list, select the new division for the device
  - The list box reflects the new division.

3. Click  (Save) to save

**Notice!**

All components of an entrance must belong to one division  
The system will not allow you to save an entrance until all its components belong to the same division.

## 6.2 Assigning Divisions to operators

Assign Divisions to operators in the **User rights** dialog

**Dialog path**


Main menu > **Configuration** > **Operators and workstations** > **User rights**

**Prerequisites**

- Divisions are licensed and in operation
- At least one division has been created.
- At least one operator has been created in the system

**Procedure**

1. In the **User rights** dialog, select the personnel record of the operator to be assigned.
2. On the **Divisions** tab, use the arrow keys to move divisions from the list of **Available divisions** to the list of **Assigned divisions** for this operator.

3. Click  (Save) to save

## 7 Configuring the IP addresses

The local access controllers on the network require a consistent scheme of IP addresses in order to participate in the access control system. The **AccessIPConfig** tool locates the controllers on the network and provides a convenient interface to administer their addresses and other network options centrally.

### Prerequisites

- The local access controllers are powered on and connected to the network.
- You have a scheme for the IP addresses of the controllers, and their passwords if required.

### Dialog path

**Main menu > Configuration > Tools**

### Procedure

1. Follow the dialog path above and click **Configuration AMC and fingerprint devices**  
The **AccessIPConfig** tool opens.
2. Click **Scan AMCs**  
The local access controllers that are available on the network are listed, each with the following parameters:
  - **MAC address:** The hardware address of the controller. Note, this is **not** the address of its Main Access Controller, which is called MAC only by coincidence.
  - **Stored IP address:**
  - **Port number:** The default is 10001
  - **DHCP:** The value is **Yes** only if the controller is configured to receive an IP address from DHCP
  - **Current IP address**
  - **Serial number**
  - Notes added by the network configuration team
3. Double-click an AMC in the list to change its parameters in a popup window. Alternatively, select the line of the desired AMC and click **Set IP...** Note that it may be necessary to enter a password, if one has been configured for the device.  
The modified parameters are stored as soon as you click OK in the popup window.
4. When you have finished configuring the IP parameters of the controllers, click **File > Exit** to close the tool.  
You will return to the main application.

For more detailed information, click **Help** in the **AccessIPConfig** tool to view its own help file.

## 8 Using the device editor

### Introduction

The Device Editor, **DevEdit**, is intended for adding and deleting small numbers of entrances and devices, or for adding, modifying, or deleting individual parameters.

For import of large, existing configurations use the **Configuration Import/Export** function under **Main menu > Configuration > Tools**

The Device Editor offers views corresponding to the following editable hierarchies:

- **Device configuration:** the electronic devices within the access control system.
- **Workstations:** the computers cooperating in the access control system.
- **Areas:** the physical areas into which the access control system is divided.

### Prerequisites











The system is correctly installed, licensed and on the network.




### Dialog path

- **Main menu > Configuration > Device data**


### Using the DevEdit toolbar

The DevEdit toolbar buttons have the following functions, regardless of which view is active, for example **Devices**, **Workstations** or **Areas**.

Button	Shortcut	Description
	Ctrl + N	Creates a new item below the selected node. Alternatively, right-click the node to invoke its context menu.
	Del	Deletes the selected item and all beneath it.
	Ctrl-Page up	First item in the tree
	Ctrl -	Previous item
	Ctrl +	Next item
	Ctrl-Page down	Last item in the tree
	Ctrl-A	Expands and collapses the tree.
	Ctrl-K	Refreshes the data by reloading them from the database. <b>All unsaved changes are discarded.</b>
	Ctrl-S	Saves the current configuration
	Ctrl-F	Opens a search window

		Open the <b>Device configuration</b> tree
		Open the <b>Workstations</b> tree
		Open the <b>Areas</b> tree

In all DevEdit views, start at the root of the tree and add items using the toolbar buttons, the menu or the context menu of each item (right-click to invoke it). To add sub-items to the tree, first select the item under which the sub-items should appear.

When you have finished adding items to the tree, click **Save**  to save the configuration. To close DevEdit, click **File > Exit**.

## 9 Configuring areas of access control

### Introduction to Areas

Secured facilities can be divided into Areas. Areas can be of any size: one or several buildings, single floors or even single rooms.

Some uses of Areas are:

- The localization of individual persons within the secured facilities.
- The estimation of the number of persons within a given area, in case of an evacuation or other emergency.
- Limiting the number of persons or vehicles in an area:  
When the predefined population limit is reached, further admissions can be rejected until persons or vehicles leave the area.
- Implementing access sequence control and anti-passback

The system distinguishes between two types of access-controlled areas

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

Each area may have sub-areas for finer granularity of control. Areas for persons may have up to 3 levels of nesting, and areas for parking lots only 2, namely the overall parking lot and parking zones, between 1 and 24 in number.

The default area, which exists in all installations, is called **Outside**. It serves as the parent for all user-defined areas of both kinds: person and parking lots.

An area is not usable unless at least one entrance leads into it.

Device Editor **DevEdit** can be used to assign a location area and a destination area to any entrance. When someone scans a card at a reader belonging to an entrance, the person's new location becomes the destination area of that entrance.



### Notice!

Access sequence control and anti-passback require both entrance and exit readers at the areas' entrances.

Turnstile-type entrances are strongly recommended to prevent accidental or deliberate "tailgating "

### Procedure for creating areas

#### Prerequisites

As a system operator you require an authorization from your system administrator to create areas.


#### Dialog path (AMS)

1. In the AMS dialog manager select **Main menu > Configuration > Device data**



2. Click Areas



3. Select the node **Outside**, or one of its children, and click  in the toolbar. Alternatively, right-click **Outside** to add an area via its context menu. All areas created initially receive a unique name of **Area** plus a numeric suffix.
4. In the popup window select its type, that is **Area** for persons or **Parking lot** for vehicles. Note that only **Outside** can have children of both types. Any sub-area of these children always inherits the type of its parent.
  - **Areas** for persons can be nested to three levels. For each area or sub area you can define a maximum population.
  - **Parking lots** are virtual entities consisting of at least one **parking zone**. If the population of a parking lot does not need to be limited by the system, 0 is displayed. Otherwise the maximum number of parking spaces per zone is 9999, and the parking lot main pane displays the sum of all the spaces in its zones.

**Procedure for editing areas**

1. Click an Area in the hierarchy to select it.
2. Overwrite one or more of the following attributes in the main pane of the dialog.

<b>Name</b>	The default name, which you may overwrite.
<b>Description</b>	A free-text description of the area.
<b>Maximum number of persons / cars</b>	Default value 0 (zero) for no-limit. Else, enter an integer for its maximum population.

**Notes:**

- An area cannot be moved by dragging and dropping to a different branch of the hierarchy. If necessary, delete the area and recreate it on another branch.

**Procedure for deleting areas.**

1. Click an area in the hierarchy to select it.



2. Click **Delete**  or right-click to delete via the context menu.

**Note:** an area cannot be deleted until all its children have been deleted.

## 9.1 Configuring areas for vehicles

**Creating areas for vehicles (parking lot, parking zone)**

If you select an area type of **Parking lot** a popup window appears.

Name	Count
Central parking_01	20
Central parking_02	15
Central parking_03	50
Central parking_04	100

1. Enter a name in the field **Name starts with** to create a trunk name for all its parking sub-areas or **parking zones**.  
Up to 24 **parking zones** can be created using the **Add** button, and each will have the trunk name plus a 2-digit suffix.
2. If the system is to limit the population of these areas, enter the number of parking spaces in the **Count** column. If no population limit is required, enter 0.

**Note:** The maximum population of the entire parking lot is the sum of these numbers. Only parking zones can contain parking spaces; the **parking lot** is only a virtual entity consisting of at least one **parking zone**. The maximum number of parking spaces per zone is 9999.

### Creating entrances for parking lots

As with normal areas, parking lots require an entrance. The appropriate door model is **Parking lot 05c**.

For monitoring the population of a parking lot 2 entrances with this door model are required on the same AMC, one for ingress and one for egress.

#### Prerequisite

Create a parking lot with at least one parking zone, as described above.

#### Dialog path

**Main menu > Configuration > Device data**



Click **LACs/Entrances/Devices**

#### Procedure

1. In the device hierarchy, create an AMC, or select an AMC that has no dependent entrances.
2. Right-click the AMC and select **New entrance**
3. In the **New entrance** popup window select Entrance model **Parking lot 05c** and add an inbound reader of the type installed at the parking lot entrance.
4. Click **OK** to close the popup window.
5. Select this newly created entrance in the device hierarchy.
  - Note that the system has automatically designated the reader as an Entry reader.
6. In the main editing pane, on tab **Parking lot 05c**, select from the **Destination** pull-down menu the parking lot that you created previously.
7. Right-click the AMC again, and create another entrance of type **Parking lot 05c** as above.
  - Note that this time you can only select an outbound reader.
  - Click **OK** to close the popup window.
8. Select this second newly created entrance in the device hierarchy



- Note that the system has automatically designated the second reader as an Exit reader.

## 10 Configuring operators and workstations

### Introduction to access-control administration rights

Administration rights for the access control system determine which system dialogs may be opened, and which functions may be performed there.

Rights can be assigned to both operators and workstations.

The rights of a workstation may temporarily restrict the rights of its operator, because security-critical operations should only be performed from workstations that are especially secure.

Rights are assigned to operators and workstations in bundles called **Profiles**. Each profile is tailored to the duties of one of a particular type of operator or workstation.

Each operator or workstation may have multiple authorization profiles.

### Overall procedure and dialog paths

1. Create the workstations in the Device Editor:



**Configuration > Device data > Workstations**

2. Create workstation profiles in the dialog:  
**Operators and workstations > Workstation profiles.**
3. Assign profiles to workstations in the dialog:  
**Operators and workstations > Workstation rights**
4. Create operator profiles in the dialog:  
**Operators and workstations > User profiles** dialog.
5. Assign profiles to operators in the dialog:  
**Operators and workstations > User rights** dialog

### 10.1 Creating the workstations

Workstations are the computers from which operators operate the access control system. First a workstation must be “created”, that is, the computer is registered within the access control system.

#### Dialog path

**Configuration > Device data > Workstations**

#### Procedure

1. Right-click **DMS** and select **New object** from the context menu, or click **+** on the toolbar.
2. Enter values for the parameters:
  - The **Name** of the workstation must match the computer name exactly
  - **Description** is optional. It can be used, for example, to describe the function and the location of the workstation
  - **Login via reader** Leave this check box clear unless operators are to log on to this workstation by presenting cards to an enrollment reader connected to this workstation. For details see the section 2-Factor Authentication
  - **Automatic logout after:** The number of seconds after a logon via enrollment reader is automatically terminated. Leave at 0 for unlimited time.

## 10.2 Creating workstation profiles

### Introduction to workstation profiles

Depending on its physical location, an access control workstation should be carefully configured regarding its usage, for example:

- Which operators may use it
- What credentials are necessary to use it
- What access control tasks may be performed from it

A workstation profile is a collection of rights that defines the following:

- The menus of the dialog manager and the dialogs which can be used at a workstation
- Which user profile(s) an operator must have to in order to log in at this workstation.



### Notice!



Workstation profiles override user profiles

An operator can employ only those of his user profile rights which are also included in the workstation profile of the computer where he is logged on. If the workstation and operator profiles have no rights in common, the user will lack all rights at that workstation.


### Dialog path

**Configuration > Operators and workstations > Workstation profiles**

#### Creating a workstation profile

1. Click  to create a new profile
2. Enter a profile name in the **Profile Name** field (mandatory)
3. Enter a profile description in the **Description** field (optional but recommended)
4. Click  or **Apply** to save your changes

#### Assigning execution rights for system functions


1. In the **Functions** list, select the functions that are to be accessible to this workstation and double-click them to set the value in the **Execute** column to **Yes**.
  - Likewise ensure that all the functions that are not to be accessible are set to **No**.
2. Click  or **Apply** to save your changes

#### Assigning User profiles to Workstation profiles

In the **User Profile** pane.

The **Assigned Profiles** list contains all user profiles authorized to log onto a workstation with this workstation profile.

The **Available Profiles** field contains all other profiles. These are not yet authorized to log onto a workstation with this workstation profile.

1. Click the arrow buttons between the lists to transfer selected profiles from one list to the other.
2. Click  or **Apply** to save your changes

**Notice!**

The default administrator profiles for the user (**UP-Administrator**) and the workstation (**WP-Administrator**) cannot be changed or deleted.

The profile **WP-Administrator** is irrevocably bound to the server workstation. This guarantees that there is at least one user who can log onto the server workstation.

**10.3****Assigning workstation profiles**

Use this dialog to manage the assignments of Workstation profiles to Workstations. Every workstation must have at least one workstation profile. If it has multiple profiles then all rights in those profiles apply simultaneously.


**Dialog path**

**Configuration > Operators and workstations > Workstation rights**

**Procedure**

The **Assigned Profiles** list contains all the workstation profiles that already belong to this workstation.

The **Available Profiles** list contains all workstation profiles that have not yet been assigned to this workstation.

1. In the list of workstations, select the workstation you wish to configure
2. Click the arrow buttons between the **Assigned** and **Available** lists to transfer selected profiles from one to the other.
3. Click  or **Apply** to save your changes

**Notice!**

The default administrator profiles for the user (**UP-Administrator**) and the workstation (**WP-Administrator**) cannot be changed or deleted.

The profile **WP-Administrator** is irrevocably bound to the server workstation. This guarantees that there is at least one user who can log onto the server workstation.

**10.4****Creating user (operator) profiles****Introduction to user profiles**

**Note:** The term **User** is synonymous with **Operator** in the context of User rights.

A user profile is a collection of rights that defines the following:


- The menus of the dialog manager and the dialogs which are visible to the operator.
- The capabilities of the operator in those dialogs, basically the rights to execute, change, add and delete the elements of those dialogs.


User profiles should be carefully configured, depending on the person's experience, security clearance and responsibilities:

**Dialog path**

**Configuration > Operators and workstations > User profiles**

**Procedure**


1. Click  to create a new profile
2. Enter a profile name in the **Profile Name** field (mandatory)

3. Enter a profile description in the **Description** field (optional but recommended)
4. Click  or **Apply** to save your changes

**Notice!**

Choose profile names that clearly and accurately describe the profile's capabilities and limitations.

**Adding editing and execution rights for system functions**

1. In the list pane, select the functions (first column) and the capabilities within that function (**Execute, Change, Add, Delete**) that are to be accessible to this profile. Double-click them to toggle their settings to **Yes**.
  - Likewise ensure that all the functions that are not to be accessible are set to **No**.
2. Click  or **Apply** to save your changes

**10.5****Assigning user (operator) profiles**

**Note:** The term **User** is synonymous with **Operator** in the context of User rights.

**Prerequisites**

- The operator who is to receive this user profile has been defined as a **Person** in the access control system.
- A suitable user profile has been defined in the access control system.
  - Note that it is always possible to assign the unrestricted user profile **UP-Administrator**, but this practice is deprecated for security reasons.

**Dialog path**

**Configuration > Operators and workstations > User rights**


**Procedure**

1. Load the personnel record of the intended user into the dialog.
2. If required, limit the validity of the user profile by entering dates in the fields **Valid from** and **Valid until**.

**Assigning User profiles to operators**

In the **User Profiles** pane:

The **Assigned Profiles** list contains all user profiles that have been assigned to this user. The **Available Profiles** field contains all profiles that are available for assignment.

1. Click the arrow buttons between the lists to transfer selected profiles from one list to the other.
2. Select the **Global administrator** check box to give this operator read+write access to those personnel records where the **administered globally** attribute is activated. The default operator access to such personnel records is read only.
3. Click  to save your changes.

**Assigning API usage rights to operators**


If configured and licensed, external program code can invoke features of the access control system via an Application Programming Interface or API. The external program acts through a proxy operator within the system. The **API usage** drop-down list controls the capabilities of the current operator if it is used as a proxy operator by external code.

#### **Configuration > Operators and workstations > User rights**

- Select a setting from the **API usage** list.

The choices are:

<b>No access</b>	The operator can not be used by the API to perform system functions.
<b>Read only</b>	The operator can be used by the API to read system data, but not to add, modify or delete it.
<b>Unlimited</b>	The operator can be used by the API to read, add, modify and delete system data.

- Click  to save your changes

## 10.6 Setting passwords for operators

How to set secure passwords for oneself and others.

### **Introduction**

The system requires at least one operator. The default operator in a new installation has username **Administrator** and password **Administrator**. The first step in configuring the system should always be to log on with those credentials and change the password for **Administrator**, in accordance with your organization's password policies.

After that you can add other operators, both privileged and unprivileged.

### **Procedure for changing one's own password.**

#### **Prerequisites**

You are logged onto the dialog manager.

#### **Procedure**

1. In the dialog manager, select menu: **File > Change password**
2. In the popup window, enter the current password, the new password, and the new password again to confirm.
3. Click **Change**.

Note that this procedure is the only way to change the Administrator password.

### **Procedure for changing the passwords of other operators.**


#### **Prerequisites**

To change the passwords of other users you must be logged onto the dialog manager using an account with Administrator privileges.

#### **Procedure**

1. In the main menu of the dialog manager, navigate to **Configuration > Operators and Workstations > User rights**
2. In the main dialog pane, use the tool bar to load the operator whose password you wish to change.
3. Click **Change password...**
4. In the popup window, enter the new password and the new password again to confirm.

5. In the popup window, enter the period of validity for the new password, either **Unlimited** or a number of days.
  - For production environments it is urgently recommended that you set a validity period.
6. Click **OK** to close the popup window.

In the main dialog window, click the  icon to save the user record.

Note that the date pickers **Valid from** and **Valid until**, below the **Change password...** button, refer to the validity of the user rights in this dialog, not the password.

#### **Further information**

Always set passwords according to the password policy of your organization. For guidance on creating such a policy you may consult, for example, the guidance provided by Microsoft at the following location.

<https://www.microsoft.com/en-us/research/publication/password-guidance/>

XREF to Creating new users

# 11 Configuring card codes

The coding of the access control cards ensures that all card data is unique.

## Dialog path

**Main Menu > Configuration > Options > Card coding configuration**

## Entering numbers in the dialog

To avoid errors in card-coding, all numbers can be entered in decimal or hexadecimal formats. Select the radio buttons **Hexadecimal** or **Decimal** according to the instructions of the cards' manufacturer. Any values already entered are automatically converted internally.

The main dialog pane is divided into two groups, which are described in more detail below:

- **Card default code data**
- **Check membership only values**

## Card default code data

Use these fields to define values for the **Version**, **Country code**, and the **Facility code** which are assigned to the card number when the card is enrolled in the system.

If the card is enrolled manually at an operator workstation, then a dialog appears displaying the default values which may be customized for each card.

<p><b>Code no. complete (default)</b></p>	<p>Only the facility code is entered (hex or decimal).</p> <div data-bbox="501 1008 1398 1229"> </div> <p><b>Entering encoding data:</b> The facility code is provided by the manufacturer as a decimal value: 56720 Select the radio button <b>Decimal</b> and enter the facility code. Click the Apply button to save the data.</p>
<p><b>Code no. split</b></p>	<p>Version, Country Code and Facility Code must all be entered as <b>decimal</b> values.</p> <div data-bbox="501 1451 1398 1655"> </div> <p><b>Entering code data:</b> The data are provided by the manufacturer as the following decimal values: Version: 2 Country code: 99 Facility code: 56720 Enter the data in the appropriate text boxes. Click the Apply button to store the data.</p>



**Notes on inputting default code data:**

The default data are stored in the registry of the operating system and each badge number is added at encoding time. Registration takes the form of an **8 digit hexadecimal** value with leading zeros as necessary.

If the code numbers are transferred completely then the system may convert from decimal to hex, pad to 8 places with leading zeros and save the appropriate system parameter.

- Example:
  - Input: 56720
  - Conversion: DD90
  - Saved as: 0000DD90

If the code numbers are transferred separately (split form) then only in **decimal** form. They are converted to a 10-digit decimal number which is constructed as follows:

- Version: 2 digits
- Country code: 2 digits
- Facility code: 6 digits
- If any of the 10 digits are still empty then they are padded with leading zeros
  - Example: 0299056720

This 10-digit decimal value is converted and stored as an 8 digit hexadecimal value.

- Example:
  - decimal: 0299056720
  - hexadecimal: 11D33E50

**Notice!**

The system validates hex values, in the case of split code numbers, in order to prevent the input of invalid country codes (above hex 63 or decimal 99) and invalid facility codes (above hex F423F or decimal 999,999)

**Notice!**

If the card capture occurs via a connected dialog reader then the default values are assigned automatically. It is not possible to override the defaults when capturing from a reader.

In order to do so the capture type should be switched to **Dialog**

Manual entry of the card number is in decimal format.

When saving the data a 10-digit decimal value (with leading zeros) is created, which is then converted to an 8 digit hexadecimal value. This value is now stored with the default code data as the 16-digit code number of the card.

- Example:
  - Input of the card number: 415
  - 10-digit: 0000000415
  - Converted to hexadecimal: 0000019F
  - Combined with the default Code data (see above) and saved as the code number of the badge: 11D33E500000019F

**Check Membership only values**

Checking for membership only means that the credential is checked only for membership of a company or organization, not to identify an individual. Therefore do not use the

**Membership check only** for readers that give access to high-security areas.

Use this options group to enter up to four company or client codes. The data can be entered as decimal or hexadecimal, but are stored as decimal values in the operating system's registry.



Check membership only values:

Hexadecimal

Decimal

1. value: 150

2. value: 0

3. value: 0

4. value: 0

Select the reader in the Device Editor, DevEdit, and activate the reader parameter **Membership check**.

Only the company or client codes within the card data are read and verified against the stored values.



**Notice!**

**Membership check** only works with card definitions predefined in the system (gray background), not with customized definitions.

# 12 Configuring the controllers

## Introduction

The controllers in the access control system are the virtual and physical devices that send commands to the peripheral hardware at entrances (readers and doors), and send requests from the readers and doors back to the central decision-making software.

The controllers store copies of some of the central software’s device and cardholder information, and if so configured, can make access control decisions even when temporarily isolated from the central software.

The decision making software is the Data Management System .

Controllers are of two kinds:

- Main access controller, known as the MAC s, and its redundant backup counterpart the RMAC .
- Local access controllers, known as LAC s or AMCs.

Controllers are configured in the device editor, DevEdit

## Dialog path to the device editor

Main menu > Configuration > Device data > Device tree



## Using the device editor, DevEdit

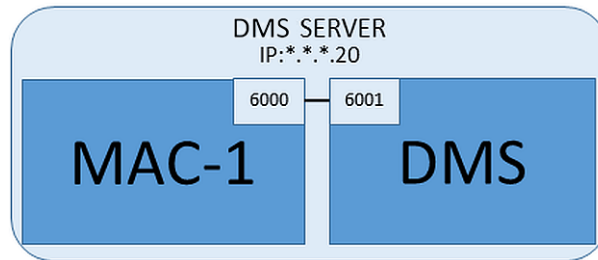
The basic usage of DevEdit is described in the section **Using the device editor**, at the link below.

## Refer to

- *Using the device editor, page 20*

## 12.1 Configuring MACs and RMACs

### 12.1.1 Configuring a MAC on the DMS server



For a minimal system configuration one MAC is required. In this case the MAC can reside on the DMS server.

## Procedure

On the DMS server open the Device Editor and create a MAC in the device tree as described in the section **Using the device editor**.

Select the MAC in the Device Editor. On the **MAC** tab, supply the following parameter values:

Parameter	Description
Name	The name that is to appear in the device tree, For example MAC-1.
Description	Optional description for the benefit of system operators
With RMAC (check box)	<Leave blank>

Parameter	Description
RMAC Port	<Leave blank>
Active (check box)	<b>Clear</b> this check box to suspend temporarily the real-time synchronization between this MAC and DMS. This is advantageous after DMS-updates on larger systems, in order to avoid restarting all the MACs at once.
Load devices (check box)	<b>Clear</b> this check box to suspend temporarily the real-time synchronization between this MAC and its subordinate devices. This shortens the time needed to open a MAC in the device editor.
IP address	localhost 127.0.0.1
Time zone	<b>IMPORTANT:</b> The time zone of the MAC and all its subordinate AMCs.
Division	(If applicable) The Division to which the MAC belongs.

Because this local MAC has no redundant failover MAC, it is not necessary to run the MACInstaller tool for it. Simply leave the two RMAC parameters on the **MAC** tab blank.

### 12.1.2

#### Preparing MAC server computers to run MACs and RMACs

This section describes how to prepare computers to become MAC servers.

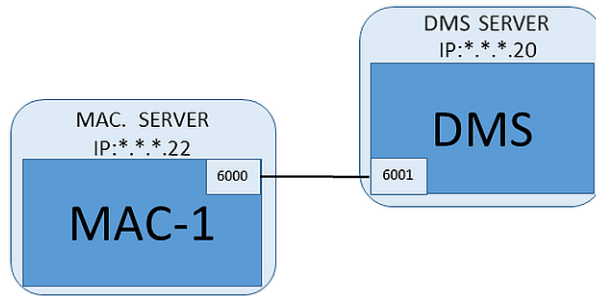
By default the first MAC in an Access Engine system runs on the same computer as its Data Management Server (DMS), however, for enhanced resilience, it is recommended that the MAC run on a separate computer, which can assume access control tasks if the DMS computer goes down.

Separate computers where MACs or RMACs reside, are known as MAC servers regardless of whether they host a MAC or an RMAC.

In order to provide failover capability, MACs and RMACs **must** run on separate MAC servers. Ensure that the following conditions are met on all participating MAC servers:

1. All servers have the same version of the same operating system as the DMS server, with the latest Windows updates.
2. The Administrator user on all servers has the same password
3. You are logged on as Administrator (if using MSTC, use only /Admin /Console sessions)
4. Disable IP V6. Note carefully the IP V4 address of each server.
5. Enable .NET 3.5 is on all participating computers.  
**Note:** On Windows 7 this is an installation. On Windows 10 and Windows Server operating systems it is enabled as a feature
6. Reboot the computer

### 12.1.3 Configuring a MAC on its own MAC server



- The MAC server computer has been prepared as described in the section Preparing MAC server computers to run MACs and RMACs
1. On the DMS server, deactivate the MAC by clearing the check boxes **Activate** and **Load devices** for this MAC in the device editor.
  2. On the MAC server, stop the MAC process using the Windows program `services.msc`.
  3. Start the `MACInstaller.exe`
    - For ACE this is found on the the BIS installation media  
`\AddOns\ACE\MultiMAC\MACInstaller` (see the section, Using the MACInstaller tool below).
    -
  4. Step through the screens of the tool, supplying values for the following parameters.

Screen#	Parameter	Description
1	<b>Destination Folder</b>	The local directory where the MAC is to be installed. Take the default wherever possible.
2	<b>Server</b>	The name or the IP address of the server where the DMS is running.
2	<b>Port (Port to DMS)</b>	The port on the DMS server which will be used to receive communication from the MAC. Use 6001 for the first MAC on the DMS, and increment by 1 for each subsequent MAC.
2	<b>Number (MAC System Number)</b>	Set 1 for this and all MACs (as opposed to RMACs).
2	<b>Twin (Name or IP address of partner MAC)</b>	Leave this field blank as long as this MAC is to have no RMAC.
2	<b>Configure Only</b> (radio button)	Do not select, because you are not configuring a MAC on the main DMS login server.
2	<b>Update Software</b> (radio button)	Select this option because you are configuring a MAC on its own computer (MAC server), not on the main DMS login server.

5. After completing the tool, reboot the MAC server or, alternatively, start the MAC process on the MAC server using the Windows program `services.msc`.
6. On the DMS server, select the MAC in the Device Editor.
7. On the **MAC** tab, supply values for the following parameters:

Parameter	Description
Name	The name that is to appear in the device tree, For example MAC-1.
Description	Optional description for the benefit of ACE operators
With RMAC (check box)	<b>&lt;Leave blank&gt;</b>
RMAC Port	<b>&lt;Leave blank&gt;</b>
Active (check box)	Select this check box now
Load devices (check box)	Select this check box now
IP address	The IP address of the MAC server computer.
Time zone	<b>IMPORTANT:</b> The time zone of the MAC and all its subordinate AMCs.
Division	(If applicable) The ACE Division to which the MAC belongs.

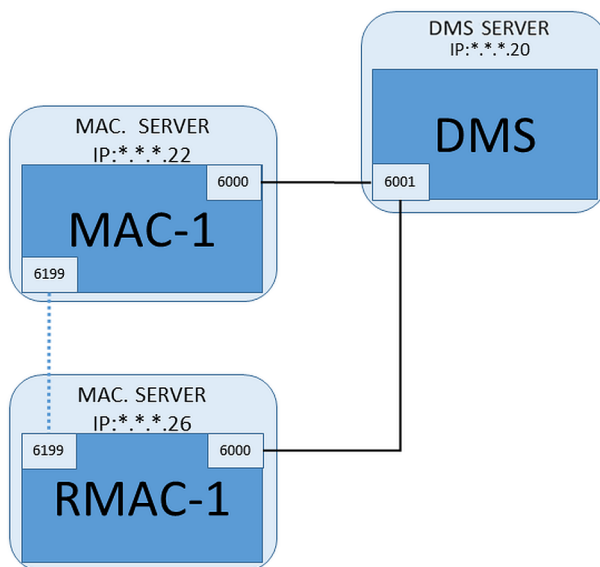
### 12.1.4 Adding RMACs to MACs



#### Notice!

Do not add RMACs to ordinary MACs until the ordinary MACs are installed and running correctly.

Data replication could otherwise be prevented or damaged.



- The MAC for this RMAC has been installed as described in the previous sections, and is running correctly.
- The MAC server computer for the RMAC has been prepared as described in the section Preparing MAC server computers to run MACs and RMACs

MACs may be twinned with redundant MACs (RMACs) to provide failover capability, and hence more resilient access control. In this case the access control data are replicated automatically between the two. If one of the pair fails, then the other takes control of the local access controllers below it.

#### On the DMS server, in the Configuration browser

1. In the Device Editor, select the MAC for which the RMAC is to be added.
2. On the **MAC** tab, change the values for the following parameters:

Parameter	Description
<b>With RMAC</b> (check box)	<b>Clear</b> this check box until you have installed the corresponding RMAC on the redundant failover connection server
<b>Active</b> (check box)	<b>Clear</b> this check box to suspend temporarily the real-time synchronization between this MAC and DMS. This is advantageous after DMS-updates on larger systems, in order to avoid restarting all the MACs at once.
<b>Load devices</b> (check box)	<b>Clear</b> this check box to suspend temporarily the real-time synchronization between this MAC and its subordinate devices. This shortens the time needed to open a MAC in the device editor.

3. Click the **Apply** button
4. Keep the Device Editor open as we will return to it presently.

**On the MAC server for the MAC**

To reconfigure the MAC to partner with an RMAC, proceed as follows.

- On the previously prepared MAC server computer, run the MACInstaller tool (see Using the MACInstaller tool) and set the following parameters:
  - **Server:** Name or IP address of the DMS server computer
  - **Port:** 6001
  - **Number:** 1 (all MACs have Number 1)
  - **Twin:** IP address of the computer where the RMAC will run.
  - **Update software:** Select this option, as you are configuring a MAC server, not the DMS server.

**On the MAC server for the RMAC**

To configure the RMAC, proceed as follows:

- On its own separate and prepared MAC server computer, run the MACInstaller tool (see Using the MACInstaller tool) and set the following parameters:
  - **Server:** Name or IP address of the DMS server computer
  - **Port:** 6001 (same as for the MAC)
  - **Number:** 2 (all RMACs have Number 2)
  - **Twin:** IP address of the computer where the twin MAC is running.
  - **Update software:** Select this option, as you are configuring a MAC server, not the DMS server.

**Return to the Device editor on the DMS server**

1. **IMPORTANT:** Ensure that both the MAC and RMAC, on their respective computers, are running and visible to each other on the network.
2. On the **MAC** tab, change the parameters as follows:

Parameter	Description
<b>With RMAC</b> (check box)	<b>Selected</b> A new tab labeled <b>RMAC</b> appears next to the <b>MAC</b> tab.
<b>RMAC Port</b>	6199 (the static default)

Parameter	Description
	All MACs and RMACs use this port to check whether their partners are running and accessible.
<b>Active</b> (check box)	<b>Selected</b> This enables synchronization between this MAC and its subordinate devices.
<b>Load devices</b> (check box)	<b>Selected</b> This shortens the time needed to open a MAC in the device editor.

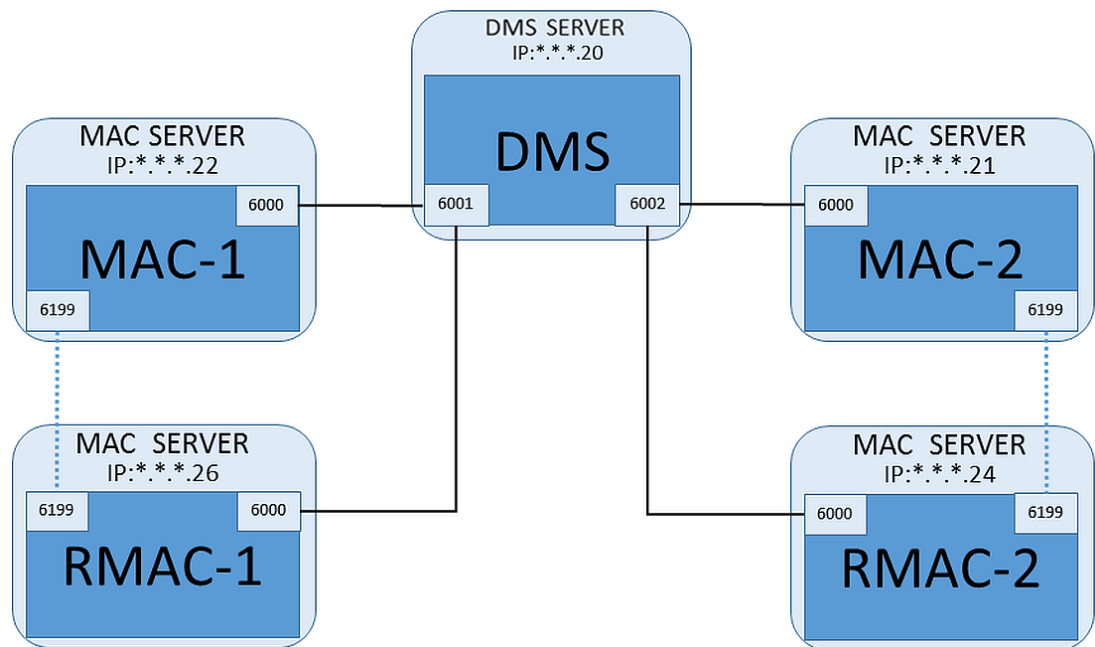
3. On the **RMAC** tab supply values for the following parameters:

Parameter	Description
<b>Name</b>	The name that is to appear in the device tree. For example, if the corresponding MAC is named MAC-01 then this RMAC could be named RMAC-01
<b>Description</b>	Optional documentation for ACE operators
<b>IP address</b>	The IP address of the RMAC
<b>MAC Port</b>	6199 (the static default) All MACs and RMACs use this port to check whether their partners are running and accessible.

### 12.1.5

#### Adding further MAC/RMAC pairs

Depending on the number of entrances to be controlled, and the degree of fault tolerance required, a large number of MAC/RMAC pairs can be added to the system configuration. For the exact number supported by your version, please consult the corresponding datasheet.



For each additional MAC/RMAC pair...



1. Prepare the separate computers for MAC and RMAC as described in the section Preparing MAC server computers to run MACs and RMACs
2. Set up the MAC as described in the section Configuring a MAC on its own MAC server
3. Set up the RMAC for this MAC as described in the section Adding RMACs to MACs

Note that each MAC/RMAC pair transmits to a separate port on the DMS server. Therefore, for the parameter **Port (Port to DMS)** in `MACInstaller.exe`, use:

- 6001 for both computers in the first MAC/RMAC pair
- 6002 for both computers in the second MAC/RMAC pair
- etc.

In the Device Editor port 6199 can always be used for the parameters **MAC Port** and **RMAC Port**. This port number is reserved for the “handshake” within each MAC/RMAC pair, whereby each knows whether its partner is accessible or not.



**Notice!**

Reactivating MACs after system upgrades

After a system upgrade MACs and their AMCs are deactivated by default. Remember to reactivate them in the configuration browser by selecting the relevant check boxes in the device editor.

**12.1.6**

**Using the MAC installer tool**

`MACInstaller.exe` is the standard tool for configuring and reconfiguring MACs and RMACs on their own computers (MAC servers). It collects parameter values for a MAC or RMAC, and makes the necessary changes in the Windows Registry.



**Notice!**

Because the tool makes changes to the Windows Registry, it is necessary to stop any running MAC process before reconfiguring it.

The MACInstaller tool can be found on the BIS installation medium under the following path:

```
\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe
```

Through a series of screens it collects values for the parameters below.

Screen#	Parameter	Description
1	<b>Destination Folder</b>	The local directory where the MAC is to be installed.
2	<b>Server</b>	The name or the IP address of the server where the DMS is running.
2	<b>Port (Port to DMS)</b>	The port number on the DMS server which will be used for communication between the MAC and the DMS. <b>See below for details.</b>
2	<b>Number (MAC System Number)</b>	Set 1 for all original MACs. Set 2 for all redundant failover MACs (RMACs).

Screen#	Parameter	Description
2	<b>Twin (Name or IP address of partner MAC)</b>	The IP address of the computer where the redundant failover partner for this MAC server is to run. If not applicable leave this field blank.
2	<b>Configure Only</b> (radio button)	Select this option if you are reconfiguring a MAC on the main DMS login server. <b>See below for details</b>
2	<b>Update Software</b> (radio button)	Select this option if you are installing or reconfiguring a MAC on its own computer (MAC server), not on the main DMS login server. <b>See below for details</b>

Port numbers have the following numbering scheme:

- In a non-hierarchical system, where only one DMS server exists, each MAC and its corresponding RMAC transmit from the same port number, usually 6000. The DMS can communicate with only one of each MAC/RMAC pair at a time.
- The DMS receives signals from the first MAC or MAC/RMAC pair on port 6001, from the second MAC or MAC/RMAC pair on port 6002, and so on.



#### Notice!

DMS receiver port in hierarchical systems

Note that the numbering scheme for DMS receiver ports is different in hierarchical systems. For details see MACs and RMACs in hierarchical topologies

This parameter is to distinguish original MACs from RMACs:

- All original MACs have the number 1.
- All redundant failover MACs (RMACs) have the number 2

Select this option to change the configuration of an existing MAC on the main DMS server, in particular to inform it of a newly installed RMAC on a different computer.

In this case, enter the IP address or hostname of the RMAC in the parameter **Twin**.

Select this option on a computer other than the main DMS server, either to install an RMAC or to change its configuration.

In this case, enter the IP address or hostname of the RMAC's twin MAC in the parameter **Twin**.

## 12.2

### Configuring the LACs

#### Creating an AMC local access controller

Access Modular Controllers (AMCs) are subordinate to Main Access Controllers (MACs) in the device editor.

To create an AMC:

1. In the Device Editor, right-click a MAC and choose **New Object** from the context menu or
2. Click the **+** button.
3. Choose one of the following AMC types from the dialog that appears:

- AMC 4W (default) with four Wiegand reader interfaces to connect up to four readers
- AMC 4R4 with four RS485 reader interfaces to connect up to eight readers

**Result:** A new AMC entry of the chosen type is created in the DevEdit hierarchy

<b>AMC2 4W</b>	<b>Access Modular Controller</b> with four Wiegand readers.	A maximum of four Wiegand readers can be configured to connect up to four entrances. The controller supports eight input and eight output signals. If needed, extension boards can provide up to 48 additional input and output signals.
<b>AMC2 4R4</b>	<b>Access Modular Controller</b> with four RS485 reader-interfaces	A maximum of eight RS485 readers can be configured to connect up to eight entrances. The controller supports eight input and eight output signals. If needed, extension boards can provide up to 48 additional input and output signals.
<b>AMC2 8I-8O-EXT</b>	Extension board for the AMC with eight input and output signals	Make additional signals available. Up to three extension boards can be connected to an AMC
<b>AMC2 16I-16O-EXT</b>	Extension board for the AMC with sixteen input and output signals	
<b>AMC2 8I-8O-4W</b>	Extension board for Wiegand AMC with eight input and output signals	

**Activation/Deactivation of controllers**

When first created, a new controller has the following option (check box) selected:

**Communication to host enabled.**

This opens the network connection between the MAC and the controllers, so that any changed or extended configuration data are propagated to the controllers automatically.

Deactivate this option to save network bandwidth, and so improve performance, while creating multiple controllers and their dependent devices (entrances, doors, readers, extension boards). In the device editor the devices are then marked with grayed icons.

**IMPORTANT:** Be sure to reactivate this option when the configuration of devices is complete. This will keep the controllers continually updated with any configuration changes made at other levels.

**Mixing controller types within one installation**

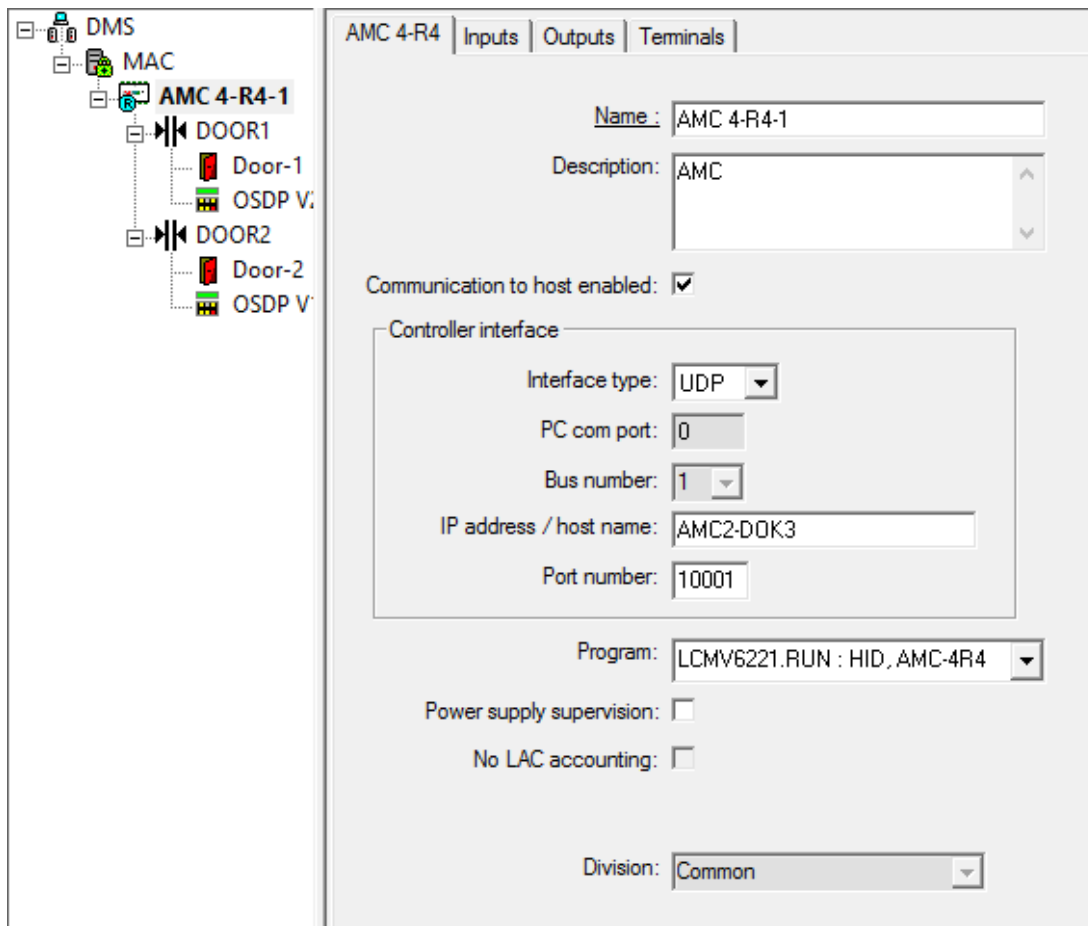
Access control systems are normally equipped with only one type of controller and reader. Software upgrades and growing installations can make it necessary to supplement existing hardware components with new ones. Even configurations combining RS485 variants (AMC 4R4) with Wiegand variants (AMC 4W) are possible, as long as the following caveats are heeded:

- RS485 readers transit a "telegram" which contains the code number as read.

- Wiegand readers transmit their data in such a way that they must be decoded with the help of the badge definition in order to preserve the code number in the correct form.
- Mixed controller operation can only function if both code numbers are constructed the same.






## 12.2.1 AMC parameters and settings


### General Parameters of the AMC



### Configuring AMC parameters

Parameter	Possible values	Description
Controller name	Restricted alphanumeric: 1 - 16 digits	ID generation (default) guarantees unique names, but these can be overwritten individually. If overwriting it is the user's responsibility to make sure the IDs are unique. We therefore recommend that Network connections to DHCP servers use the network name.
Controller description	alphanumeric: 0 - 255 digits	This text is displayed in the OPC branch.

<p>Communication to host enabled</p>	<p>0 = deactivated (check box is clear) 1 = activated (check box is selected)</p>	<p>Default value = active The check box displays the current setting and can also be used to change it. The status of the host connection is indicated by the following icons in the Explorer: Controller variant: active not active</p> <p>AMC2 4W  </p> <p>AMC2 4R4  </p> <p>Deactivation provides a means of creating and parameterizing devices to be included in the access control system at a later date. The devices should not be activated, and thus added to the host's database, until put into operation. This also reduces useless polling of the devices by the host.</p> <p></p> <p>For security reasons after a software upgrade all controllers are set offline (check box is clear). This ensures that the installation can continue running with the old software, and can be brought up to speed with the new software step-by-step. Include new controllers in the installation gradually by checking their respective boxes.</p>
<p>Controller Interface</p>		
<p>Interface Type</p>	<p>COM  UDP</p>	<p>COM where connection to the AMC is via one of the MAC COM ports. UDP (= user datagram protocol) where connection is by network. Where this connection type is selected, the parameters "host name" and "remote-controlled port" become settable.</p>

		 <p>With the interface type "UDP", DIP switch "5" <b>must</b> be set on the AMC. In addition, it is recommended to set switch "1" to ON.</p>
PC COM port	numeric: with COM-ports: 1 - 256 with UDP-ports: 1 - 65535	Number of the COM ports at which this AMC is connected to the MAC. For ethernet connections via converters, virtual COM-ports are generated and shown here. With type "UDP" enter the port via which the MAC will receive information from the AMC. If this port is unknown the field can be left empty and a free port will be selected automatically.
Bus number	numeric: 1 - 8	Using the interface adapter AMC-MUX up to 8 controllers can be configured on one COM port. In such cases enter the unique address of each AMC as given by its DIP switch.  <b>Note:</b> Switch 5 can be ignored here because only the first 4 switches are used for addressing. For UDP connections use the default setting (=0)
IP Address/ Hostname	Network name or IP address of the AMC	This input box is only settable if <b>UDP</b> is selected as the port type. If IP addresses are allocated by DHCP then the network name of the AMC should be provided so that the AMC can be located after a restart even if the IP address has changed. For networks without DHCP the IP address must be given.
UDP Port	numeric: 1 - 10001 - with default configuration	This input box is only activated if <b>UDP</b> is selected as port type. This is the AMC port which will receive the MAC-messages.
Further Parameters		

Program	alphanumeric	File name of the program to be loaded into the AMC. The available programs are located in the BIN-directory of the MAC, and can be selected from a list. For convenience the protocol and the description are also shown. This parameter is set automatically as programs are loaded automatically depending on which readers are connected, and the parameter is overridden in the case of a reader/program mismatch.
Power supply supervision	0= deactivated (check box is clear) 1= activated (check box is selected)	Supervision of the supply voltage. If the power supply drops then an informational message is generated. The supervision function assumes the prerequisite of a UPS (uninterruptible power supply), so that a message can be generated. 0 = no supervision 1 = supervision activated
No LAC accounting	0= deactivated (check box is clear) 1= activated (check box is selected)	Select this check box for AMC devices that work jointly to provide access to parking lots, where only the parent MAC keeps account of the number of units entering and leaving. <b>Note</b> that, if this option is selected and the AMC offline, the AMC will not be able to prevent access to overcrowded areas, as it has no access to the full population count.
Division	Default value "Common"	This is a read-only informational field. "Divisions" are a means of dividing an access control installation between multiple autonomous parties, created and maintained in the BIS Manager.

### Configuring AMC inputs

Name	Serial resistor	Parallel resistor	Time model	Messages
01, AMC 4-W-8	2K2	1K2	<No time model>	03, Open, close, Line cut, short circuit
02, AMC 4-W-8	1K5	1K	<No time model>	00,
03, AMC 4-W-8	none	none	<No time model>	00,
04, AMC 4-W-8	none	none	<No time model>	00,
05, AMC 4-W-8	none	none	<No time model>	00,
06, AMC 4-W-8	none	none	<No time model>	00,
07, AMC 4-W-8	none	none	<No time model>	00,
08, AMC 4-W-8	none	none	<No time model>	00,

Input type  
 Digital mode, single       Analog mode, 4 state

Events  
 Time model: <No time model> ▾  
 Open, close   
 Line cut, short circuit

Resistors  
 serial  
 none  
 1K  
 1K2  
 1K5  
 1K8  
 2K2  
 2K7  
 3K3  
 3K9  
 4K7  
 5K6  
 6K8  
 8K2  
 parallel  
 none  
 1K  
 1K2  
 1K5  
 1K8  
 2K2  
 2K7  
 3K3  
 3K9  
 4K7  
 5K6  
 6K8  
 8K2

This dialog is divided into four panes:

- List of the inputs by name
- The input types
- The events which will be signaled by the inputs
- The resistor types used with analog mode

### Parameters of inputs

The parameters of the AMC inputs are described in the following table:

Column name	Description
Name	Numbering of the input (from 01 to 08) and name of the appropriate AMC or AMC-EXT.
Serial resistor	Display of the set resistor value for the serial resistor. "none" or "---" = digital mode
Parallel resistor	Display of the set resistor value for the parallel resistor. "none" or "---" = digital mode
Time model	Name of the selected time model



Messages	Indenture number and designation of the messages which will be generated 00 = no messages 01 = if events <b>Open, close</b> were activated 02 = if events <b>Line cut, short circuit</b> were activated 03 = if both event options were activated
Assigned	Using Entrance Model 15 the signal name of the DIP is displayed.

Use the Ctrl and Shift keys when clicking to select multiple inputs simultaneously. Any values you change will apply to all the selected inputs.

**Events and Time models**

Depending on the operation mode, the following door states are detected and reported:

**Open, Closed, Line cut and Short circuit.**

Select their respective check boxes to enable the AMC to transmit these states as events to the overall system.

Select a **Time model** from the drop-down list of the same name to restrict the transmission of the events to the times defined by the model. For example, the **Open** event might only be significant outside of normal business hours.

**Input type**

The resistors can be operated in **Digital mode** or **Analog mode (4 state)**.

The default is **Digital mode**: only the door states **open** and **close** are detected.

In Analog mode the wire states **Line cut** and **Short** circuit are detected additionally.

Door open	sum of the serial ( $R_s$ ) and parallel ( $R_p$ ) resistor values: $R_s + R_p$
Door closed	is equal to the serial resistor values: $R_s$
Circuit break	sum of the serial ( $R_s$ ) and parallel ( $R_p$ ) resistor values approaching infinity.
Short-Circuit	sum of the serial ( $R_s$ ) and parallel ( $R_p$ ) resistor values is equal to zero.

**Resistors**

The resistors are set to "none" or "---" in the default **Digital mode**.

In **Analog mode** the values for the serial and parallel resistors can be set by selecting their respective radio buttons.

**none, 1K, 1K2, 1K5, 1K8, 2K2, 2K7, 3K3, 3K9, 4K7, 5K6, 6K8, 8K2** (in 100 ohm)

Depending on the resistor value selected, only restricted ranges are available for the corresponding resistor.

The following tables show in the left columns the selected values, and in the right columns the available ranges of the other resistor.

Serial	Range	Parallel	Range
"none" or "---"	1K to 8K2	"none" or "---"	1K to 8K2
1K	1K to 2K2	1K	1K to 1K8
1K2	1K to 2K7	1K2	1K to 2K7
1K5	1K to 3K9	1K5	1K to 3K3
1K8	1K to 6K8	1K8	1K to 3K9
2K2	1K2 to 8K2	2K2	1K to 4K7

2K7	1K2 to 8K2		2K7	1K2 to 5K6
3K3	1K5 to 8K2		3K3	1K5 to 6K8
3K9	1K8 to 8K2		3K9	1K5 to 8K2
4K7	2K2 to 8K2		4K7	1K8 to 8K2
5K6	2K7 to 8K2		5K6	1K8 to 8K2
6K8	3K3 to 8K2		6K8	1K8 to 8K2
8K2	3K9 to 8K2		8K2	2K2 to 8K2

**Configuring AMC Outputs - Overview**

This dialog page provides the configuration of each output on an AMC or AMC-EXT, and contains three main areas:

- list box with an overview of the parameter that is set for every output
- configuration options to the outputs selected in the list
- definition of conditions for the activation of the outputs

The screenshot shows the 'AMC 4-W' configuration window with tabs for 'Inputs', 'Outputs', and 'Terminals'. The 'Outputs' tab is active, displaying a table with columns: Output, Action type, Max. duration, Delay, Period, Pulsing, Duration, Count, Time model, and Message. Below this table is a detailed configuration area for 'Output data' with sections for 'State', 'Events', 'Behaviour', and 'Pulsing'. At the bottom, there is a table for selected outputs with columns: Output, Op1, Description, Param11, Param12, Op2, Description, and Parameter21.

Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Message
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	

Output	Op1	Description	Param11	Param12	Op2	Description	Parameter21
03		Door open	10b, DM 10b	NORMDOOR, Door-6			
03	OR	Door opened unauthorised	10b, DM 10b	NORMDOOR, Door-6			
05		Door open	01a, DM 01a-6	NORMDOOR, Door-7			
05	OR	Door opened unauthorised	01a, DM 01a-6	NORMDOOR, Door-7			

**Selecting AMC outputs in the table**

To configure output contacts, first select the corresponding line in the upper table. Use the Ctrl and Shift keys to select multiple lines, if required. Changes made in the lower part of the window will affect only the outputs that you select.

Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
05, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
06, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
07, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
08, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00

Lines whose outputs have already been assigned via a door model, or elsewhere, are shown in light gray with the information "used by an entrance!". Such outputs cannot be configured further.

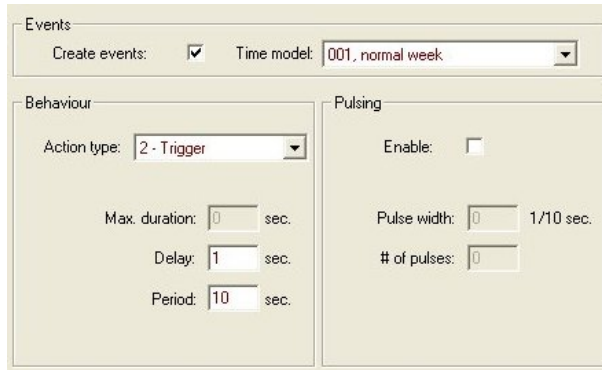
Lines selected by you are in dark grey.

**Parameters of AMC outputs**

Column name	Description
Output	current numbering of the exits at the respective AMC or AMC-EXT 01 to 08 with AMC and AMC_IO08 01 to 16 with AMC_IO16
Action type	indication of the selected action type 1 = Follow state 2 = Trigger 3 = Alternating
Max. duration	length in seconds the signal [1 - 9999; 0 = always, if the converse message fails to appear] - only with action type "1"
Delay	delay in seconds until the signal is given [0 - 9999] - only with action types "1" and "2"
Period	period in seconds the signal is given - only with action type "2"
Pulsing	activation of the impulse - otherwise the signal is given constantly
Duration	impulse length
Count	number of impulses per second
Time model	name of the selected time model
Messages	marking of the message activity 00 = no messages 03 = events are reported
Assigned	Using Entrance Model 15 the signal name of the DOP is displayed.

**Outputs: Events, Action, Pulsing**

All entries from the list above are generated by using the check boxes and input fields in the dialog areas **Events**, **Action**, and **Pulsing**. Selecting a list entry indicates the respective settings in these areas. This also holds for the multiple choice of list entries, provided that the parameters to all selected outputs are equal. Changes to the parameter settings are adopted for all entries selected in the list.



Select the check box **Create events** if a message should be sent for the output activated. If these messages are to be sent only during special periods, e.g. at night or at weekends, then assign a suitable **time model**.

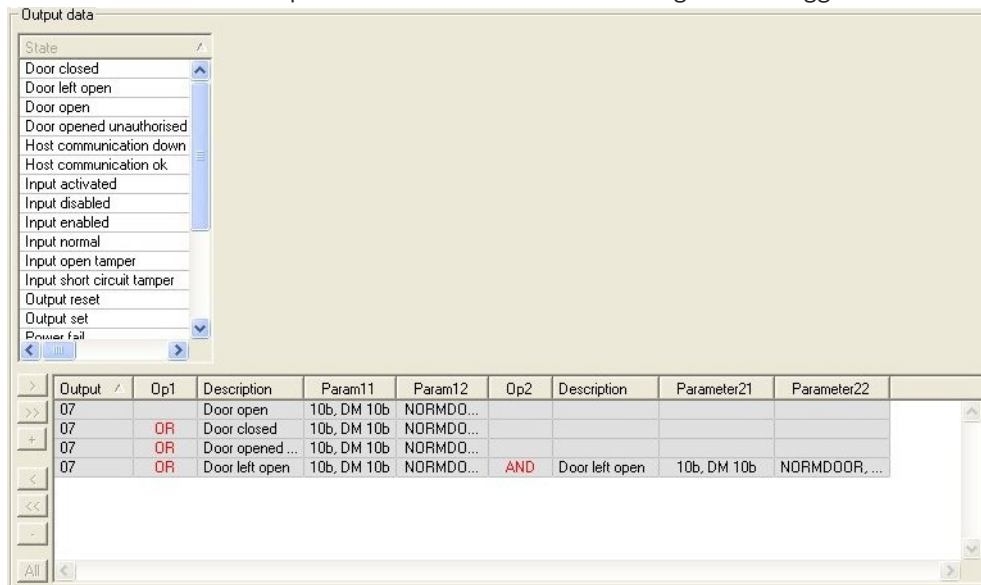
The following parameters can be set for the individual action types:

Action type	Max. duration	Delay	Period	Pulsing/Enable	Pulse width	Number of pulses
Follow state	0 = always 1 - 9999	0 - 9999	no	yes	1 - 9999	None
Trigger	no	0 - 9999	0 - 9999 if pulsing is <b>not</b> enabled	yes disables period	1 - 9999	1 - 9999
Alternating	no	no	no	yes	1 - 9999	no

### AMC output data



The lower part of the **Outputs** dialog contains:


- A list box with the **states** available for the selected outputs.
- A table with the outputs and the states that are configured to trigger them.





### Configuring states to trigger outputs


You can configure the outputs you have selected above to be triggered by individual states or logical combinations of states.

- Select one or several outputs in the upper list box.
- Select a State from the **State** list.
- If there are several devices or installations to a selected status which can transmit this state, the button  is activated beside the button .


Click  (or double-click the status) to create for each selected exit an entry of its status with the first device (for example, AMC, first entrance) and the installation (for example, first signal, first door).

Exit 	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2


By clicking , the selected status is transferred to the list and created together with an OR-shortcut for every installed device (for example, all AMC entrances).


Exit 	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 02, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 03, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 04, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 05, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 06, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 07, AMC 4-W-2
04	OR	Output set	00, AMC, AMC 4-W-2	Out, 08, AMC 4-W-2

- Several states can be assigned over one OR-shortcut.

Exit 	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

Shortcuts with AND are also possible:

- A status must already be assigned to which another condition is added by selecting it in an arbitrary column.
- Then another status is selected and connected to the marked status by clicking .


Exit 	Operand1	Description	Param11	Param12	Operand2	Description	Parameter21	Parameter22
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2				
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2				
04	OR	Door open	06a, Timemgm	<< !!! >>	AND	Door opened unauthorised	06a, Timemgm	<< !!! >>



**Notice!**

Up to 128 OR-shortcuts can be assigned to every output.  
To every assigned condition, **one** AND-short cut can be created.

After a status is assigned for a device or installation, this can also be assigned for all other existing devices and installations.

- Select the assigned entry in an arbitrary column.
- This status is created for all existing devices and installations by clicking .

### Modifying the parameters of outputs

List entries can be changed.

With several devices or installations to which the assigned status could match, the first devices and installations of this type are always set.

In the columns **Param11** and **Param21** (with AND-shortcuts) the devices (for example, AMC, entrance) are displayed. The columns **Param12** and **Param22** contain special installations (for example, input signal, door, reader).

If several devices (for example, I/O boards) or installations (for example, additional signals, readers) exist, the mouse pointer changes while pointing to this column.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>

A double-click on the column entry adds a button brings up a drop-down list of valid entries for the parameter.

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Input normal	00, AMC, AMC 4-W-2	01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	

01, AMC 4-W-2

02, AMC 4-W-2

03, AMC 4-W-2

04, AMC 4-W-2

05, AMC 4-W-2

06, AMC 4-W-2

07, AMC 4-W-2

08, AMC 4-W-2

Changing the entries in the columns **Param11** and **Param21** updates the entries in columns **Param12** and **Param22**:

Exit	Operand1	Description	Param11	Param12
04		Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
04	OR	Door open	06a, Timemgm	<< !!! >>
04	OR	Input normal	01, AMC_IO, AMC_IO16_002_1	In, 01, AMC_IO16_002_1



#### Notice!

This is only possible for columns **Param11**, **Param12**, **Param21** and **Param22**.

If there are no other options (for example, because only one entrance was configured), the mouse pointer does not change and all field are grey. If this entry is double-clicked, this is interpreted as a deletion command, and the message box for verifying the deleting appears.


### Deleting the states that trigger outputs

Selected assignments can be removed by clicking '<' (or by double-clicking the list entry). A message box will request confirmation for the deletion.

If several states have been associated with an output, then they can all be deleted together as follows:

- Select the first list entry (the one which has no entry in the column **Op1**) and then click the '<<' button .
- Alternatively, double-click the first entry.

- A popup window appears. Confirm or abort the deletion.
- If you confirm deletion then a second popup asks whether you wish to delete all associated entries (answer **Yes**), or only the selected entry (answer **No**).

To delete additional states that qualify the first state by an AND operator in column **Op2**, click anywhere in the line and then click the 'minus' button , which is only active if a qualifying AND state is present in that line.

#### State description

The following table provides an overview of all selectable states, their type number, and description.

The list field **State** contains these parameters as well - they are indicated by scrolling right on the list.

State	Type	Description
Input activated	1	Local input
Input normal	2	Local input
Input short circuit tamper	3	Local input with resistor configured
Input open tamper	4	Local input with resistor configured
Input enabled	5	Local input activated by time model
Input disabled	6	Local input deactivated by time model
Output set	7	Local output, not current output
Output reset	8	Local input, not current input
Door open	9	GID of the entrance, door number
Door closed	10	GID of the entrance, door number
Door opened unauthorized	11	GID of the entrance, door number, replaces "Door open" (9)
Door left open	12	GID of the entrance, door number
Reader shows access granted	13	Reader address
Reader shows access denied	14	Reader address
Time model active	15	Configured time model
Tamper reader	16	Reader address
Tamper AMC	17	---
Tamper I/O board	18	---
Power fail	19	for battery powered AMC only
Power good	20	for battery powered AMC only
Host communication ok	21	---
Host communication down	22	---
Reader Messages	23	(Details depend on the current software version)

LAC Messages	24	(Details depend on the current software version)
--------------	----	--

**Configuring outputs**

Beside the signal assignment with door models or with individual assignment, conditions can be defined for outputs which are not allocated yet. If these conditions occur, the output is activated corresponding to the set parameter.

You must decide what will be switched over the output. In contrast to the signals that can be associated to a specific door model, its doors, and readers, in this case the signals of all devices and installations connected to an AMC can be applied.

If, for example, an optic, acoustic signal or a message to the UGM is to be triggered by the input signals **Input short circuit tamper** and **Door opened unauthorized**, those input or inputs which can be considered are assigned to the corresponding destination output.

Example in which only one contact was selected in each case:

Exit	Operand1	Description	Param11	Param12
04		Input short cir...	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Door opened ...	06a, Timemgm	<< !!! >>

Example with all contacts:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOR, Revolving Door


Example with selected contacts:

A single entry is created for every contact by clicking or removing the not required contacts after assigning all contacts:

Exit	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	---
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOR, Revolving Door

The same conditions can be installed on several outputs if, for example, in addition to an optical you also need an acoustic signal, a message should be sent to the UGM at the same time:



Exit 	Operand1	Description	Param11	Param12
04		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
04	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
04	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
04	OR	Door opened unauthorised	03a, Entrance B:B	REVDOOR, Revolving Door
06		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2
06	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 08, AMC 4-W-2
06	OR	Door opened unauthorised	06a, Timemgm	<< !!! >>
07		Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 02, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 03, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 04, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 05, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 06, AMC 4-W-2
07	OR	Input short circuit tamper	00, AMC, AMC 4-W-2	In, 07, AMC 4-W-2

List of all existing states with the default values for the Parameter11/21 and 12/22:

Description	Param11	Param12
Input activated	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input normal	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input short circuit tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input open tamper	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input enabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Input disabled	00, AMC, AMC 4-W-2	In, 01, AMC 4-W-2
Output set	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Output reset	00, AMC, AMC 4-W-2	Out, 01, AMC 4-W-2
Door open	06a, Timemgm	<< !!! >>
Door closed	06a, Timemgm	<< !!! >>
Door opened unauthorised	06a, Timemgm	<< !!! >>
Door left open	06a, Timemgm	<< !!! >>
Reader shows access granted	---	TM-Reader IN
Reader shows access denied	---	TM-Reader IN
Time model active	---	000, <No time model>
Tamper reader	---	TM-Reader IN
Tamper AMC	---	---
Tamper I/O board	---	00, AMC, AMC 4-W-2
Power fail	---	---
Power good	---	---
Host communication ok	---	---
Host communication down	---	---

#### Defining signals on the Terminals tab

The **Terminals** tab lists the contact allocation on an AMC or AMC-EXT. Once entrances are created, signal assignments are indicated according to the door model selected.

You cannot make modifications on the **Terminals** tab of the controller or the extension boards. Edits are only possible on terminals tab of the entrance page. For this reason terminal settings are displayed on a gray background. Entrances which are displayed in red indicate the signal configurations of the respective outputs.

AMC 4-R4 | Inputs | Outputs | **Terminals**

Signal allocation of 'AMC 4-R4' with 12 signal pairing

Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

## 13 Configuring Entrances

### 13.1 Entrances - introduction

The term Entrance denotes in its entirety the access control mechanism at an entry point:

The elements of the entrance include:

- Access readers - between 1 and 4
- Some form of barrier, for example a door, turnstile, mantrap or boom-barrier.
- The access procedure as defined by predefined sequences of electronic signals passed between the hardware elements.

A Door model is a template for a particular kind of entrance. It describes the door elements present (number and type of readers, type of door or barrier etc.), and enforces a specific access control process with sequences of predefined signals.

Door models greatly facilitate the configuration of an access control system.

Door model 1	simple or common door
Door model 3	reversible turnstile for entrance and exit
Door model 5	parking lot entrance or exit
Door model 6	Inbound/Outbound readers for time & attendance
Door model 7	elevator control
Door model 9	vehicle boom barrier and rolling gate
Door model 10	simple door with IDS arming/disarming
Door model 14	simple door with IDS arming/disarming and special access rights
Door model 15	independent input and output signals

- Door models 1, 3, 5, 9 and 10 include an option for additional card readers on the inbound or outbound side.
- A local access controller that is used within door model 05 (parking lot) or 07 (elevator) cannot be shared with another door model.
- When an entrance has been configured with a door model and saved, the door model can no longer be swapped for another. If a different door model is required the entrance must be deleted and reconfigured from scratch.

Some door models have variants (a, b, c, r) with the following characteristics:

<b>a</b>	inbound <b>and</b> outbound readers
<b>b</b>	inbound reader and outbound push button
<b>c</b>	inbound <b>OR</b> outbound reader (not both - which would be variant <b>a</b> )
<b>r</b>	(Door model 1 only). one reader for the sole purpose of registering persons at an assembly point , for example in the case of an evacuation. No physical barrier is involved in this door model.

The **OK** button to conclude the configuration only becomes active when all mandatory values have been entered. For example, door models of variant (a) require inbound **and** outbound readers. Not until a type is selected for both readers can the entries be saved.

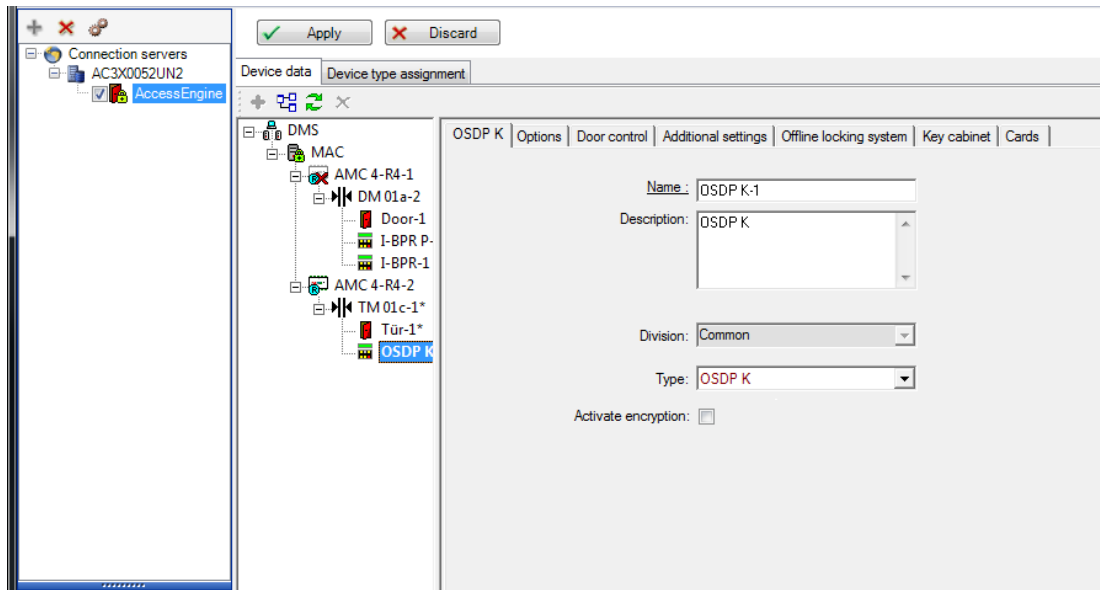
### 13.2 Creating entrances

The list of readers presented for selection will be tailored to the controller type you selected.

- For **AMC 4W** types only Wiegand-readers are available, both with and without keyboard.
- For **AMC 4R4** the readers in the following table are available. Do not mix protocols on the same controller.

Reader name	Wiegand-Protocol	BPR-Protocol	I-BPR-Protocol	HID-Protocol
WIE1	X			
WIE1K (Keyboard)	X			
BPR MF		X		
BPR MF Keyboard		X		
BPR LE		X		
BPR LE Keyboard		X		
BPR HI		X		
BPR HI Keyboard		X		
TA40 LE		X		
TB30 LE		X		
TB15 HI1		X		
INTUS 1600			X	
I-BPR			X	
I-BPR K (Keyboard)			X	
DT 7020			X	
OSDP				X
OSDP K (Keyboard)				X
OSDP KD (Keyboard +Display)				X
HADP				X
HADP K (Keyboard)				X
HADP KD (Keyboard +Display)				X
RKL 55 (Keyboard + LCD)				X
RK40 (Keyboard)				X
R40				X
R30				X
R15				X

In case of an **OSDP reader** the dialog appears as follows:



The following types of OSDP readers are available:

OSDP	OSDP standard reader
OSDP Keyb	OSDP reader with keyboard
OSDP Keyb+Disp	OSDP reader with keyboard and display

The following OSDP readers have been tested:

OSDPv1 - unsecure mode	LECTUS duo 3000 C - MIFARE classic LECTUS duo 3000 CK - MIFARE classic LECTUS duo 3000 E - MIFARE Desfire EV1 LECTUS duo 3000 EK - MIFARE Desfire EV1
OSDPv2 - unsecure and secure mode	LECTUS secure 2000 RO LECTUS secure 4000 RO LECTUS secure 5000 RO

**Notice!**

Caveats for OSDP



Do not mix product families, e.g. **LECTUS duo** and **LECTUS secure** on the same OSDP bus. A customer specific key is generated and used for encrypted data transmission to the OSDP reader. Ensure that system is properly backed up.

Keep the keys safe. Lost keys cannot be recovered; the reader can only be reset to factory defaults.

For security reasons do not mix encrypted and unencrypted modes on the same OSDP bus.

The screenshot shows a configuration window titled "DM 01a | Terminals". It contains the following fields:

- Entrance name:** A text input field containing "DM 01a".
- Entrance description:** A text area containing "DM 01a".
- Location:** A dropdown menu with "Outside" selected.
- Destination:** A dropdown menu with "Outside" selected.
- Division:** A dropdown menu with "Common" selected.

Parameter	Possible values	Description
<b>Entrance name</b>	Alphanumeric, between 1 and 16 characters	The dialog generates a unique name for the entrance, but that name can be overwritten by the operator who configures the entrance, if so desired.
<b>Entrance description</b>	alphanumeric: 0 to 255 characters	An arbitrary descriptive text for display in the system.
<b>Location</b>	Any defined area (no parking lots)	The named area (as defined in the system) where the reader is located. This information is used for access sequence control: If a person attempts to use this reader, but the current location of that person (as tracked by the system) is different from that of the reader, then the reader will deny access to the person.
<b>Destination</b>	Any defined area (no parking lots)	The named area, as defined in the system, to which the reader allows access. This information is used for access sequence control: If a person uses this reader their location will be updated to the value of <b>Desintation</b> .
<b>Waiting time external access decision</b>	Number of tenths of a second	The time for which access controller waits for a decision from the access control system. before making its own decision.

<b>Division</b>	A read-only field	The defined division to which the reader belongs. The default division is <b>Common</b> .
<b>Latency alarm device</b> (only for entrance models 10 and 14)	100 - 9999	The time span in which the door opener can be activated without an alarm being released. This is a reader parameter which is set and then sent to the readers. The unit of this parameter is one tenth (1/10) of a second.
<b>Arming Area</b> (only for entrance model 14)	One letter: A through Z	Entrances of an IDS group will be activated together by the activation of the area's readers.

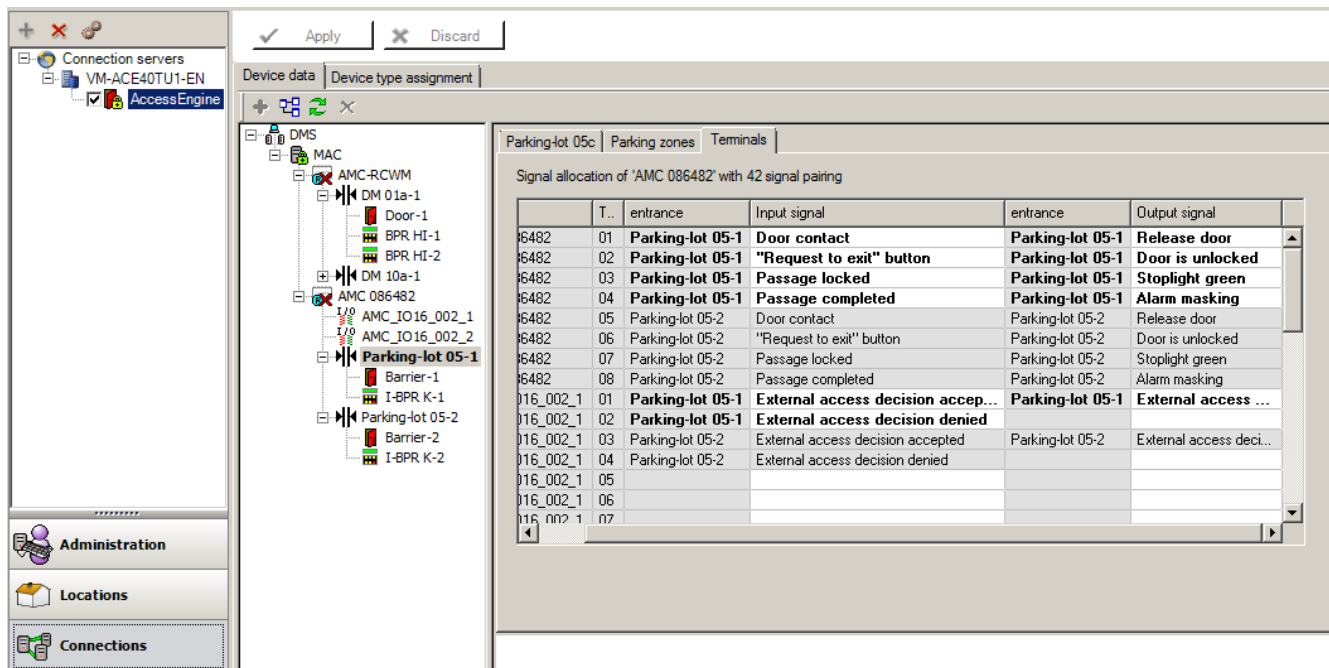
### 13.3 Additional I/O checks

Additional I/O checks can, for example, help identify a visitor based on Automated Number-Plate Recognition (ANPR).

The AMC gets 1 input via AMC I/O contact:

- Visitor authorized Additional I/O check

The AMC prevents access in the case of a 'not authorized' signal.



Card Status	Signal = 1:ANPR authorized	Signal = 0: ANPR not authorized
Card authorized	Access	Invalid vehicle number' event
Card on blacklist	Not authorized - blacklist	Not authorized - blacklist
Card expired	Not authorized - expired	Not authorized - expired
Card not authorized for this reader	Not authorized	Not authorized

It is possible to open the barrier manually even if the visitor is not recognized.

For that functionality a switch is connected to the AMC I/O contacts.

The AMC sets an output signal **Additional check active** before the input signal is analyzed.



If a new visitor is registered, the license plate info must be entered by the operator in the BIS (for reports) and in the ANPR system (for scanning). ANPR will recognize for a registered vehicle from its database.

### 13.4 Configuring AMC terminals

In its contents and structure, this tab is identical to the AMC **Terminals** tab.

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	<b>DM 01b</b>	<b>Door contact</b>	<b>DM 01b</b>	<b>Release door</b>
0	03	<b>DM 01b</b>	"Request to exit"...		
0	04				
0	05				
0	06				
0	07				
0	08				

Here, however, it is possible to make changes to the signal assignment for selected entrance model. Double-clicking in the columns **Output signal** or **Input signal** opens up combo-boxes.

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	<b>DM 01b</b>	<b>Door contact</b>	<b>DM 01b</b>	<b>Release door</b>
0	03	<b>DM 01b</b>	"Request to exit" ▾		
0	04		< not assigned >		
0	05		"Request to exit" button		
0	06		Bolt sensor		
0	07		Passage locked		
0	08		Sabotage		

Similarly it is possible to create additional signals for the respective entrance. Double-clicking in an empty line brings up the appropriate combo-box:

B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	<b>DM 01b</b>	<b>Door contact</b>	<b>DM 01b</b>	<b>Release door</b>
0	03	<b>DM 01b</b>	"Request to exit"...		
0	04	<b>DM 01b</b>	Bolt sensor ▾		
0	05				
0	06				
0	07				
0	08				

Signal assignments which are inappropriate for the entrance that you are editing are read-only, with a gray background. These can only be edited while the corresponding entrance is selected.

A similar gray background and pale foreground color is given to those outputs which were parameterized in the **Outputs** tab of the AMC.



**Notice!**

The combo-boxes are not 100% context-sensitive, therefore it is possible to select signals that will not work in real life. If you add or remove signals on the **Terminals** tab, test them to ensure that they are logically and physically compatible with the entrance.

**Terminal Assignment**

For each AMC and each entrance a **Terminal** tab lists all 8 signals for the AMC on 8 separate lines. Unused signals are marked white, and used ones are marked blue.

The list has the following structure:

- **Board:** numbering of the AMC Wiegand Extension (0) or the I/O extension board (1 to 3)
- **Terminal:** number of the contact on the AMC (01 up to 08) or the Wiegand extension board (09 to 16).
- **Entrance:** name of the entrance
- **Output signal:** name of the output signal
- **Entrance:** name of the entrance
- **Input signal:** name of the input signal

Board	T..	entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 01a	Door contact	DM 01a	Release door
AMC 4-R4	02				
AMC 4-R4	03				
AMC 4-R4	04				
AMC 4-R4	05				
AMC 4-R4	06				
AMC 4-R4	07				
AMC 4-R4	08				
BPR HI	01				
BPR HI	02				
BPR HI-1	01				
BPR HI-1	02				

**Changing the signal assignment**

On the terminal tabs of the controllers the assignment of the separate signals is only displayed (read-only). On the terminal tabs of the respective entrances, however, it is possible to change or reposition the signals of the selected entrances.

A double-click on the entry to be changed in the column **Output signal** or **Input signal** activates a drop-down list, so that a different value can be selected as the signal for the entrance model. If you select **Not assigned**, the signal is released and can be used for other entrances.

Thus you can not only change signals, but also assign signals to other contacts in order to optimize the use of the available voltage. Any free or freed contacts can be used later for new signals or as new positions for existing signals.



**Notice!**

In principle all input and output signals can be freely selected, but not all selections make sense for all door models. For example it would make no sense to assign IDS signals to a door model (e.g. 01 or 03) which does not support IDS. For more details see the table in section Assigning Signals to the Door Models.

**Assigning signals to door models**

In order to avoid incorrect parameterization the pull-down menus for assigning signals to doors models, the menus offer only those signals which are compatible with the selected door model.

**Table of input signals**

Input Signals	Description
Door sensor	
Request to exit button	Button to open the door.
Bolt sensor	Is used for messages, only. There is no control function.
Entrance locked	Is used to lock the opposite door in sluices temporarily. But can also be used for permanently locking.
Sabotage	Sabotage signal of an external controller.
Turnstile in normal position	Turnstile is closed.
Passage completed	A passage was completed successfully. This is a pulse of an external controller.
IDS: ready to arm	Will be set by the IDS, if all detectors are in rest and the IDS can be armed.
IDS: is armed	The IDS is armed.
IDS: request to arm button	Button to arm the IDS.
Local open enable	Will be used if a doorway arrangement opens the door without involving the AMC. The AMC sends no intrusion message but "door local open".
External access decision accepted	Signal is set, if an external system accepts access
External access decision denied	Signal is set, if an external system accepts access

**Table of output signals**

Output Signals	Description
Door opener	
Sluice: lock opposite direction	Locks the other side of the mantrap. This signal is sent when the door opens.

Alarm suppression	... to the IDS. Is set as long as the door is open, to avoid that the IDS creates an intrusion message.
Indicator green	Indicator lamp - will be controlled as long as the door is open.
Door open too long	Pulse of three seconds. If the door is open too long.
Camera activation	Camera will be activated at the beginning of a passage.
Open turnstile inbound	
Open turnstile outbound	
Door is permanent open	Signal to unlock a door for an extended period.
IDS: arm	Signal to arm the IDS .
IDS: disarm	Signal to disarm the IDS .
External access decision activated	Signal must be set to activate external access system

#### Mapping table of door models to input and output signals

The following table lists meaningful assignments of signals and door models.

Door Model	Description	Input Signals	Output Signals
01	Simple door with entry and exit reader Readers for time & attendance External access decision available	<ul style="list-style-type: none"> <li>- Door sensor</li> <li>- "Request to exit" button</li> <li>- Bolt sensor</li> <li>- Entrance locked</li> <li>- Sabotage</li> <li>- Local open enable</li> <li>- External access decision accepted</li> <li>- External access decision denied</li> </ul>	<ul style="list-style-type: none"> <li>- Door opener</li> <li>- Sluice: lock opposite direction</li> <li>- Alarm suppression</li> <li>- Indicator green</li> <li>- Camera activation</li> <li>- Door open too long</li> <li>- External access decision activated</li> </ul>
03	Revolving door with entry and exit reader Readers for time & attendance External access decision available	<ul style="list-style-type: none"> <li>- Turnstile in rest position</li> <li>- "Request to exit" button</li> <li>- Entrance locked</li> <li>- Sabotage</li> <li>- External access decision accepted</li> <li>- External access decision denied</li> </ul>	<ul style="list-style-type: none"> <li>- Sluice: lock opposite direction</li> <li>- Open turnstile inbound</li> <li>- Open turnstile outbound</li> <li>- Alarm suppression</li> <li>- Camera activation</li> <li>- Door open too long</li> <li>- External access decision activated</li> </ul>
05	Parking lot entrance or exit - maximum of 24 parking zones Readers for time & attendance External access decision available	<ul style="list-style-type: none"> <li>- Door sensor</li> <li>- "Request to exit" button</li> <li>- Entrance locked</li> <li>- Passage completed</li> <li>- External access decision accepted</li> </ul>	<ul style="list-style-type: none"> <li>- Door opener</li> <li>- Alarm suppression</li> <li>- Indicator green</li> <li>- Door open too long</li> <li>- Door is permanent open</li> <li>- External access decision activated</li> </ul>

		- External access decision denied	
06	Readers for time & attendance		
07	Elevator - maximum 56 floors		
09	Vehicle entrance or outgoing reader and push button Readers for time & attendance External access decision available	- Door sensor - "Request to exit" button - Entrance locked - Passage completed - External access decision accepted - External access decision denied	- Door opener - Alarm suppression - Indicator green - Door open too long - Door is permanent open - External access decision activated
10	Simple door with entry and exit reader and IDS arming/disarming Readers for time & attendance External access decision available	- Door sensor - "Request to exit" button - IDS: ready to arm - IDS: is armed - Sabotage - IDS: request to arm - External access decision accepted - External access decision denied	- Door opener - Camera activation - IDS: arm - IDS: disarm - Door open too long - External access decision activated
14	Simple door with entry and exit reader and IDS arming/disarming Readers for time & attendance	- Door sensor - "Request to exit" button - IDS: ready to arm - IDS: is armed - Sabotage - IDS: request to arm	- Door opener - Camera activation - IDS: arm - Door open too long
15	Digital contacts		

**Assigning signals to readers**

Serial readers (i.e. readers on an AMC2 4R4) and OSDP readers can be enhanced with local I/O signals. In this way additional signals can be made available and electrical paths to the door contacts shortened.

When a serial reader is created the **Terminals** tab of the corresponding entrance shows two input and two output signals for each reader below the controller and (if present) the extension board signals.



**Notice!**

These list entries are created for each serial reader regardless of whether or not it has local I/Os.

These reader-local signals can not be assigned to functions and parametrized like those of controllers and boards. They also do not appear on the **Input signal** and **Output signal** tabs, nor can they be used for elevators (e.g. to exceed the 56-floor limit). For this reason they are best suited for direct control of doors (e.g. door strike or release). This does however free up the controller's signals for more complex parametrized functions.

### Editing the signals

When an entrance is created the **Terminals** tab of the corresponding entrance shows two input and two output signals for each reader below the controller. The Board column displays the name of the reader. The standard signals for the entrance are assigned by default to the first free signals on the controller. In order to move these to the reader's own signals they first have to be deleted from their original positions. To do this select the list entry **<Not assigned>**

Double-click in the **Input signal** or **Output signal** column of the reader to see a list of possible signals for the chosen door model, and so reposition the signal. Like all signals these can be viewed on the **Terminals** tab of the controller, but not edited there.



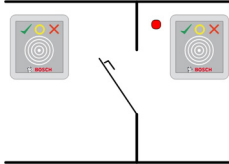
### Notice!

The status of reader signals can not be monitored. They can only be used for the door to which the reader belongs.

## 13.5

### Predefined signals for door models

#### Entrance Model 01



Model variants:

<b>01a</b>	Normal door with entry <b>and</b> exit reader
<b>01b</b>	Normal door with entry reader and push button
<b>01c</b>	Normal door with entry <b>or</b> exit reader

#### Possible signals:

Input signals	Output signals
Door sensor	Door opener
"Request to exit" button	Sluice: lock opposite direction
Sabotage	Indicator green
Local open enable	Camera activation
	Door open too long



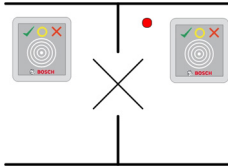
**Notice!**

Singling function, especially the lock of the opposite, can be parameterized with DM 03, only.

Alarm suppression is only activated when the alarm suppression time before door opening is greater than 0.

This entrance model can also be advantageous for vehicle entrances, in which case a secondary reader for trucks and cars is also recommended.

**Entrance Model 03**



Model variants:

<b>03a</b>	Reversible turnstile with entry <b>and</b> exit reader
<b>03b</b>	Reversible turnstile with entry reader and push button
<b>03c</b>	Turnstile with entry <b>or</b> exit reader

Possible signals:

Input signal	Output signals
Turnstile in normal position	Open turnstile inbound
"Request to exit" button	Open turnstile outbound
Sabotage	Entrance locked
	Camera activation
	Door open too long
Additional signals using <b>mantrap</b> option:	
Entrance locked	Sluice: lock opposite direction
	Alarm suppression

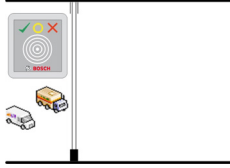
Configuration notes for mantraps:

When the turnstile is in normal position the first input signal of all connected readers is switched on. If a card is presented and if the owner has access rights for this entrance, then :

- If at the entrance reader the first output signal is set at the entrance reader for the duration of the activation time.
- If at the exit reader the second output signal is set at the exit reader for the duration of the activation time.

When the Request to Exit (REX) button is pressed then the second input signal and second output signal are set. During this time the revolving door can be used in the enabled direction.

### Entrance Model 05c



Model variant:

<b>05c</b>	Parking-lot access entrance <b>or</b> exit reader
------------	---

Possible signals for this entrance model:

Input signals	Output signals
Door sensor	Door opener
"Request to exit" button	Door is permanent open
Entrance locked	Indicator green
Passage completed	Alarm suppression
	Door open too long

Both the entrance and the exit of the parking lot must be configured on the same controller. If parking lot access has been assigned to a controller, then that controller can govern no other door models. For the entrance to the parking lot only an entrance reader (no exit reader) can be assigned. Once the entry has been assigned then selecting the door model again permits you only to define the exit reader. You can define up to 24 subareas to every parking lot, of which one must be contained in the card's authorizations in order for the card to work.

### Entrance Model 06



Model variants

<b>06a</b>	Entry <b>and</b> exit reader for time & attendance
<b>06c</b>	Entry <b>or</b> exit Reader for time & attendance

Readers which are created with this door model do not control access but are used exclusively for time & attendance purposes. They do not control the doors but only forward card data to the time & attendance system.

As a consequence, no signals are defined. These readers are usually installed within an already controlled area.





**Notice!**

In order that valid booking pairs (entry time plus exit time) can be created in the time & attendance system, it is necessary to parameterize two separate readers with door model 06: one for inbound clocking and one for outbound

Use variant **a** when entrance and exit are not separate. Use variant **c** if the entrance and the exit are spatially separate, or if you cannot attach the readers to the same controller. Make sure that you define one of the readers as inbound reader and one as outbound reader. As with any entrance it is necessary to create and assign authorizations. In Access Engine the **Time Management** tab in the dialogs **Access Authorizations** and **Area/Time Authorizations** lists all time & attendance readers which have been defined. Activate at least one reader in the inbound direction, and one reader in the outbound direction. Authorizations for time & attendance readers can be assigned along with other access authorizations, or as separate authorizations.

If more than one time & attendance reader exists for a given direction, then it is possible to assign certain cardholders to certain readers. Only the attendance times of assigned and authorized users will be registered and stored by the reader.



**Notice!**

Other access control features also affect the behavior of time & attendance readers. Hence blacklists, time models or expiry dates can also prevent a time & attendance reader from registering access times.

The registered entry and exit times are stored in a text file in the directory: C:\MgtS\AccessEngine\AC\TAEExchange under the name TAccExc\_EXP.txt and held pending export to a time & attendance system.

The booking data are transmitted in the following format:

ddMMyyyy;hhmm[s];Direction [0,1]; AbsenceReason; Personnel-Nr.

d=day, M=month, y=year, h=hour, m=minute, s=summertime (daylight saving), 0=outbound, 1=inbound

The export file is not sorted by person but contains all bookings in chronological order, as received by the administration module. The field separator in the file is a semicolon.

**Entrance Model 07 variants**



Model variants:

<b>07a</b>	Elevator with max. 56 floors
<b>07b</b>	Elevator with max. 56 floors

**Entrance Model 07a**

**Signals:**

Input signal	Output signals
	Release <name of the floor>

	One output signal per defined floor, with a maximum of 56.
--	--

Upon summoning the elevator the card owner can select only those floors for which his card is authorized.

The elevator door models can not be mixed with other door models on the same controller. Using extension boards up to 56 floors can be defined for each elevator on an AMC. The card's authorizations must contain the elevator itself and at least one floor.

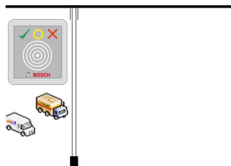
### Entrance Model 07c

#### Signals:

Input Signal	Output Signal
Input key <name of the floor>	Release <name of the floor>
For each defined floor an output and input entry exists - up to 56.	

Upon summoning the elevator and pressing a floor selector button (hence the need for input signals) the card's authorizations are checked to see whether they include the chosen floor. Moreover with this door model it is possible to define any floors served as **public access**, i.e. no authorization check will be performed for this floor, and any person may take the lift to it. Nevertheless public access may itself be governed by a **time model** which limits it to certain hours of certain days. Outside of these hours authorization checks will be performed as usual. The elevator door models can not be mixed with other door models on the same controller. Using extension boards up to 56 floors can be defined for each elevator on an AMC. The card's authorizations must contain the elevator itself and at least one floor.

### Entrance Model 09

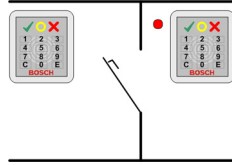


Possible signals:

Input signals	Output signals
Door sensor	Door opener
"Request to exit" button	Door is open long-term
Entrance locked	Traffic light is green
Passage completed	Alarm suppression
	Door open too long

For the barrier control, an underlying control (SPS) is assumed. In contrast to **door model 5c**, you can configure this entrance and exit on different AMCs. Moreover there are no subareas, but only a general authorization for the parking area.

**Entrance Model 10**



**Model variants:**

<b>10a</b>	Normal door with entry <b>and</b> exit reader <b>and</b> IDS (intrusion detection system) arming/disarming
<b>10b</b>	Normal door with entry, REX (request for exit) button and IDS arming/disarming
<b>10e</b>	Normal door with entry, REX button and decentral IDS arming/disarming

Possible signals:

Input signals	Output signals
Door sensor	Door opener
IDS: is armed	IDS: arm
IDS: ready to arm	IDS: disarm [only DM 10e]
"Request to exit" button	Camera activation
Bolt sensor	Door open too long
Sabotage	
IDS: request to arm button	



**Notice!**

This door model requires keypad readers. Cardholders require **PIN codes** to arm/disarm the IDS.

Different procedures are required depending on which readers are installed.

**I-BPR readers:** (e.g. DELTA 1010, INTUS 1600)

Arm by pressing key **7** and confirming with Enter (#). Then present the card, enter the PIN code and again confirm with the Enter (#) key.

Disarm by presenting the card, entering the PIN code, and confirming with Enter (#).

**BPR reader:** (including Wiegand)

Arm by pressing 7, presenting the card and entering the PIN code. There is no need to confirm using the Enter key.

Disarm by presenting the card and entering the PIN code. Disarming and door-release occur simultaneously.

**Special features of DM 10e:**

Whereas with door models 10a and 10b every entrance is its own security area, with 10e multiple entrances can be grouped into units. Any one reader in this group is capable of arming or disarming the whole unit. An output signal **Disarm IDS** is required to reset the status set by any of the readers in the group.

Signals:

- Door models 10a and 10b:
  - - Arming is triggered by a steady signal
  - - Disarming is triggered by the discontinuation of the steady signal.
- Door model 10e:
  - - Arming and disarming are triggered by a signal pulse of 1 second's duration.

[Using a bistable relay it is possible to control the IDS from multiple doors. In order to do this the signals of all doors require an OR operation at the relay. The signals **IDS armed** and **IDS ready to arm** must be replicated at all participating doors.]

## 13.6

## Special entrances

### 13.6.1

### Elevators (DM07)

#### General notes on Elevators (Entrance Model 07)

Elevators cannot be combined with other door models on the same AMC controller.

Elevators cannot be used with the reader options **Group access** or **Attendant required**

Up to 8 floors can be defined on one AMC. An AMC extension board offers 8 or 16 additional outputs per extension board.

Hence, using the maximum number of the largest extension boards it is possible to configure up to 56 floors with RS485 readers, and 64 floors with Wiegand readers, if a special Wiegand extension board is used in addition.

#### Differences between entrance models 07a and 07c

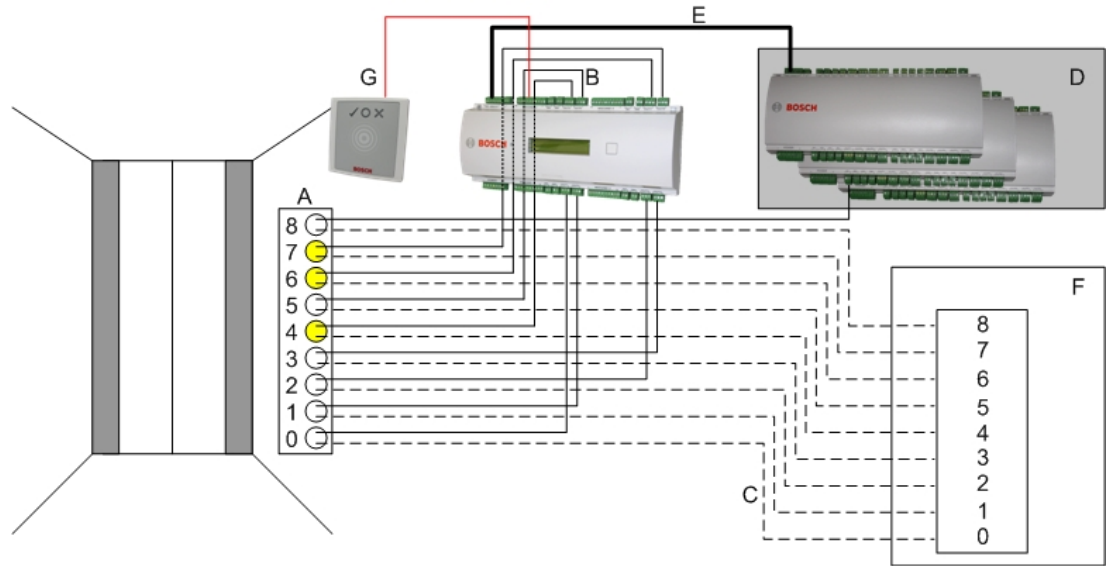
In the access authorization dialogs of the Access Engine System you can assign specific floors to the authorization of a person.

If the elevator was created using the entrance model **07a** a cardholder presents their ID card and the floors for which they have permission for become available.

With the entrance model **07c** the system checks the authorization for the selected floor after the person has chosen it. The marked floors **public** are available for each person regardless of authorization. Together with a time model the public function can be restricted to the specified time model. Outside this period the authorization will be checked for the selected floor.

#### Wiring scheme for elevators:

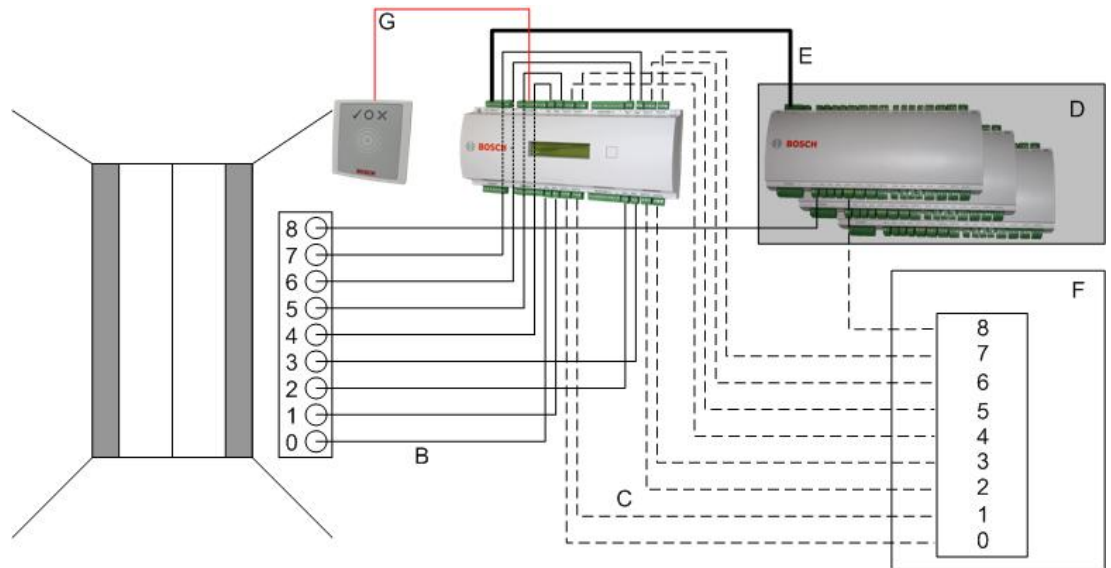
The following picture shows the connection scheme of an elevator using door model 07a.



Legend:

- A = Key board of the elevator
- B = (solid line) AMC-Output signals
- C = (broken line) Connection to the elevator controls
- D = up to three I/O-Boards can be connected to an AMC, if its own eight inputs and outputs are not sufficient.
- E = Data and Power supply from the AMC to the I/O-Boards
- F = The elevator's floor selector
- G = Reader. Two readers are configurable for each elevator.

The following picture shows the connection scheme of an elevator using door model 07c.



Legend:

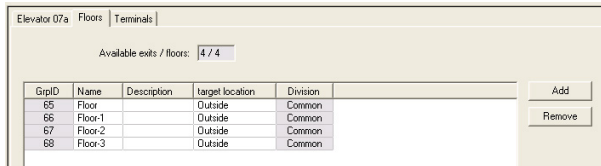
- B = (solid line) AMC-Output signals
- C = (broken line) Connection to the elevator controls
- D = up to three I/O-Boards can be connected to an AMC, if its own eight inputs and outputs are not sufficient.
- E = Data and Power supply from the AMC to the I/O-Boards
- F = The elevator's floor selector
- G = Reader. Two readers are configurable for each elevator.

Like parking lots, elevators have the parameter **Public**. This parameter can be set for each floor individually. If the parameter **Public** is activated access authorizations are not checked - so, any cardholder in the elevator can select the floor.

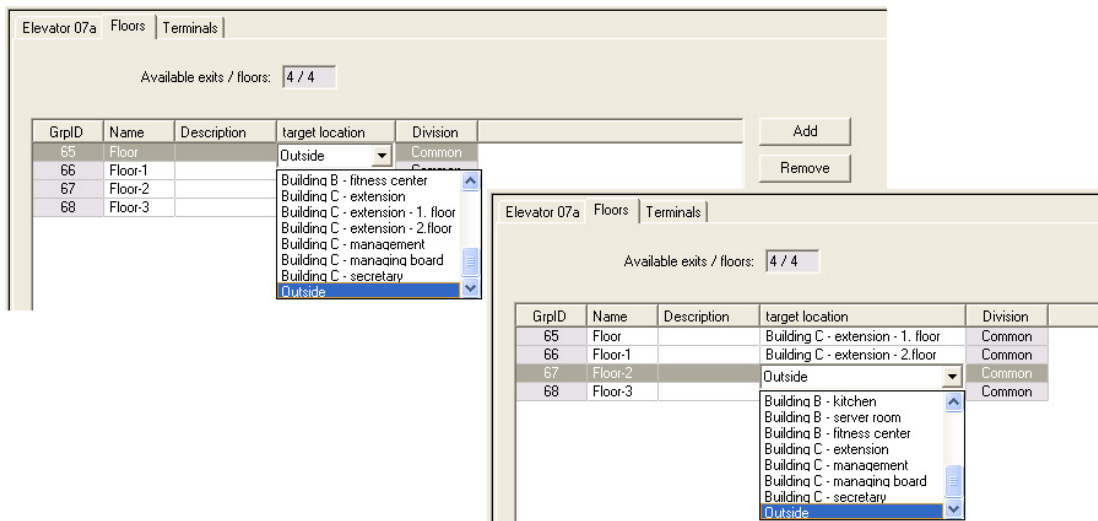
If desired, set a time model for the entrance model: Outside the defined time zones authorizations will be checked.

**Floors for entrance model 07**

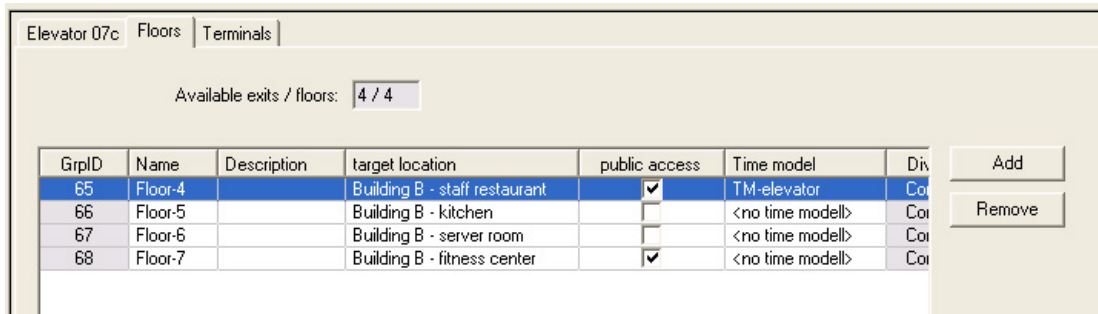
Use the **Floors** tab to add and remove floors for the elevator, using the **Add** and **Remove** buttons.



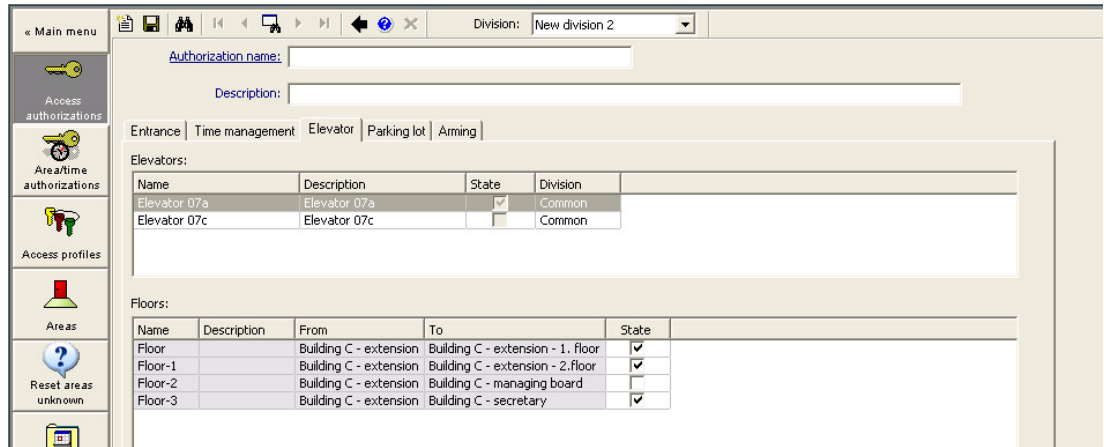
Target locations for a floor can be any **Areas** except parking lots and parking zones. Only one Area can be assigned to an individual floor. The choice of areas offered in the combo-boxes is therefore reduced after each assignment, thus preventing unintentional double-assignments.



When using entrance model 07a it is possible to make individual floors publicly accessible by checking the **Public access** box. In this case no checking of authorizations takes place. The additional assignment of a **Time model** would nevertheless restrict access to pre-defined periods.



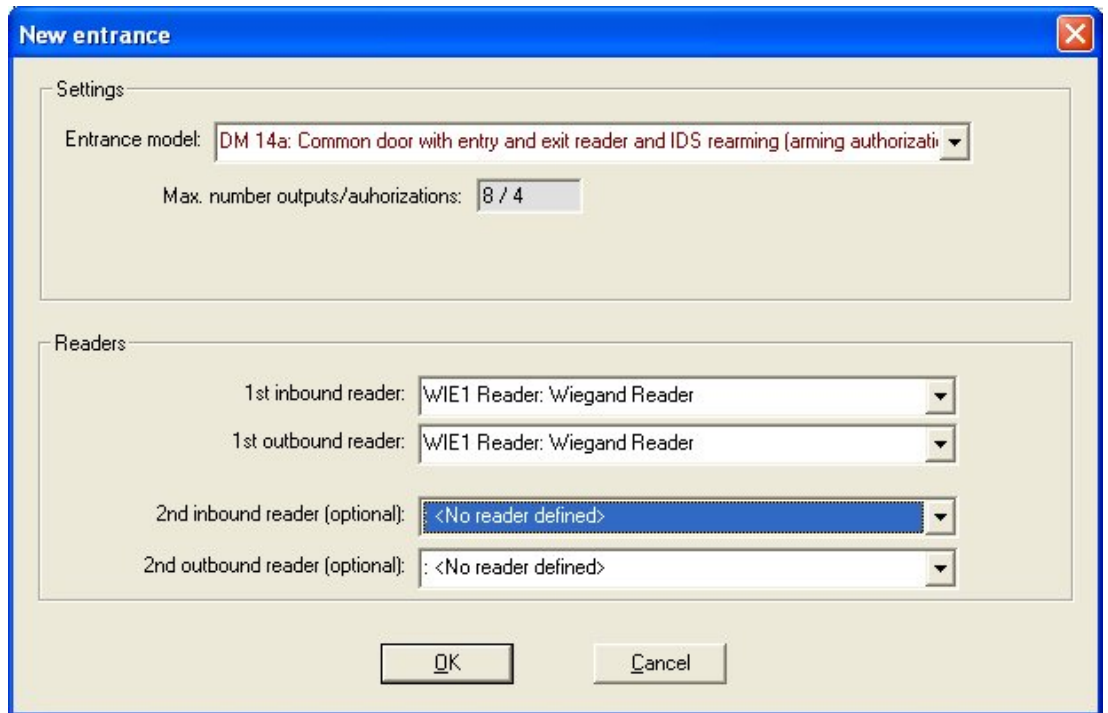
On the **Elevator** tab above the upper list box in the Access Engine dialogs **Access authorizations** and **Area/time authorizations** select first the required elevator and then, below, the floors to which the cardholder is permitted access.



### 13.6.2 Door models with intruder alarms (DM14)

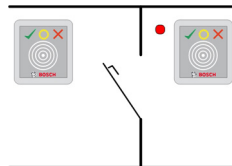
#### Arming and disarming intrusion detection systems - DM 14

In contrast to entrance model 10, DM 14 can be armed/disarmed.



An arming area is designated by a capital letter on the first page of the entrance. By assigning an entrance to an arming area, the arming at one reader will apply to all entrances of that area.

#### Entrance Model 14



Model variants:

<b>14a</b>	Normal door with entry and exit reader and IDS arming / disarming
------------	---

<b>14b</b>	Normal door with entry, push button and IDS arming / disarming
------------	--

Possible signals:

Input signals	Output signals
Door sensor	Door opener
IDS: is armed	IDS: arm
IDS: ready to arm	Camera activation
"Request to exit" button	Door open too long
Bolt sensor	
Sabotage	
IDS: request to arm button	

With door model 14 it is possible to form secured areas where the IDS (Intrusion detection system) can be armed from any reader in the area. In such a case the signals **IDS armed** and **IDS ready to arm** need to be replicated at each entrance.

In contrast to model 10 door model 14 can use readers with or without keypads. Another difference is the assignment of arming/disarming authorizations. Only card owners with the proper authorizations can arm/disarm.

In the case of keyboard readers, arming and disarming is performed as with door model 10. In the case of non-keyboard readers, arming is not achieved by entering the PIN code, but by using a switch near the reader which has the same function as key 7 of the keypad readers. After using this switch, the status of the alarm device is displayed by the reader's colored LEDs:

- Disarmed = alternating green and red light
- Armed = constant red light

Arm by presenting a properly authorized card.

Disarm by using the switch and presenting a properly authorized card.

Door-release is not automatic upon disarming, but requires the card to be presented again.

#### **Authorizations for arming with Entrance Model 14**

The first tab of the entrance 14 dialog contains an additional parameter for creating "Arming areas". Several model 14 Entrances can reference the same arming area, so that any reader in this area can arm or disarm the IDS (intrusion detection system).



DM 14a | Arming authorizations | Terminals

Name: DM 14a

Description: DM 14a

Location: Outside

Destination: Outside

Division: Common

Latency alarm device: 100 1/10 sec.

Arming area: A

In this case the signals **IDS armed** and **IDS ready to arm** need to be replicated on the inputs of the other entrances. When a second entrance model is created for the same arming area then the device editor does the replication for you. The description of the signal of the second door will be expanded by the signal no. of the corresponding signal of the first entrance model: e.g. 1:04 [= the fourth signal on board 1]

DM 14b | Arming authorizations | Terminals

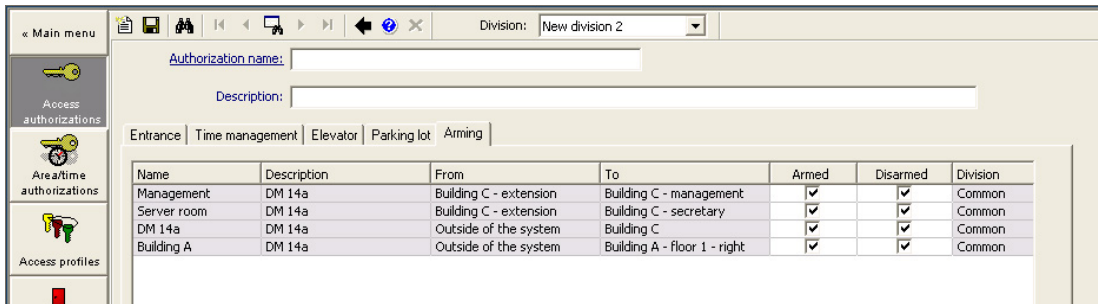
Signal allocation of 'AMC 4-R4' with 18 signal pairing

Board	T. entrance	Input signal	entrance	Output signal
AMC 4-R4	01	DM 14b Door contact	DM 14b	Release do
AMC 4-R4	02	DM 14b 1:04:IDS armed	DM 14b	Arming IDS
AMC 4-R4	03	DM 14b 1:05:IDS ready t...		
AMC 4-R4	04	DM 14b Arm IDS		
AMC 4-R4	05	DM 14b "Request to exit"...		
AMC 4-R4	06	DM 14b.1 Door contact	DM 14b.1	Release do

After creating an instance of entrance model 14 the additional tab **Arming authorizations** lists the authorizations generated by creating it. The user can freely choose names for the arming/disarming authorizations.



When collating authorizations, all created instances of entrance model 14 are listed on the tab **Arming** of the dialogs **Access authorizations** and **Area/Time Authorizations**. Authorizations for arming and disarming can be assigned separately.

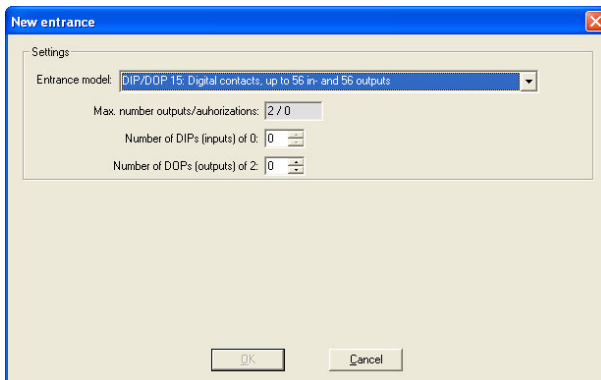


### 13.6.3

## DIPs and DOPs (DM15)

### Creating Entrance Model 15:

This entrance model offers independent input and output signals.



If all reader interfaces are taken only this entrance model becomes available. You can define this entrance model as long as there are at least two signals free.

To AMCs with elevators (model 07) or parking lots (model 05c) it is not possible to assign this entrance model.

**Entrance Model 15**

Possible signals: These default names can be overwritten.

Input Signal	Output Signal
DIP	DOP
DIP-1	DOP-1
...	...
DIP-63	DOP-63

Unlike other door models, entrance model 15 manages those inputs and outputs of a controller which are still free, and places them as generic inputs and voltage-free outputs at the disposal of the whole system.

Unlike the output contacts of other door models, those of entrance model 15 can be individually browsed in BIS's graphical user interface.

**Reinstating DOPs after restarts**

When a MAC or AMC is restarted, it normally resets the state values of its subordinate DOPs to the default value 0 (zero).

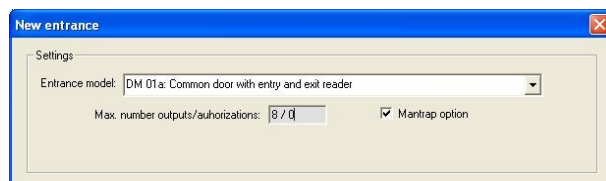
To ensure a restart always resets a DOP to last state that was manually assigned to it, select the DOP in the device tree, and select the check box **Keep state** in the main window.

**13.6.4**

**Mantrap door models**

**Creating a Mantrap**

Entrance models 01 and 03 can be used as "mantraps" for the singling of cardholder accesses. Use the check box **Mantrap option** to make the necessary additional signals available.

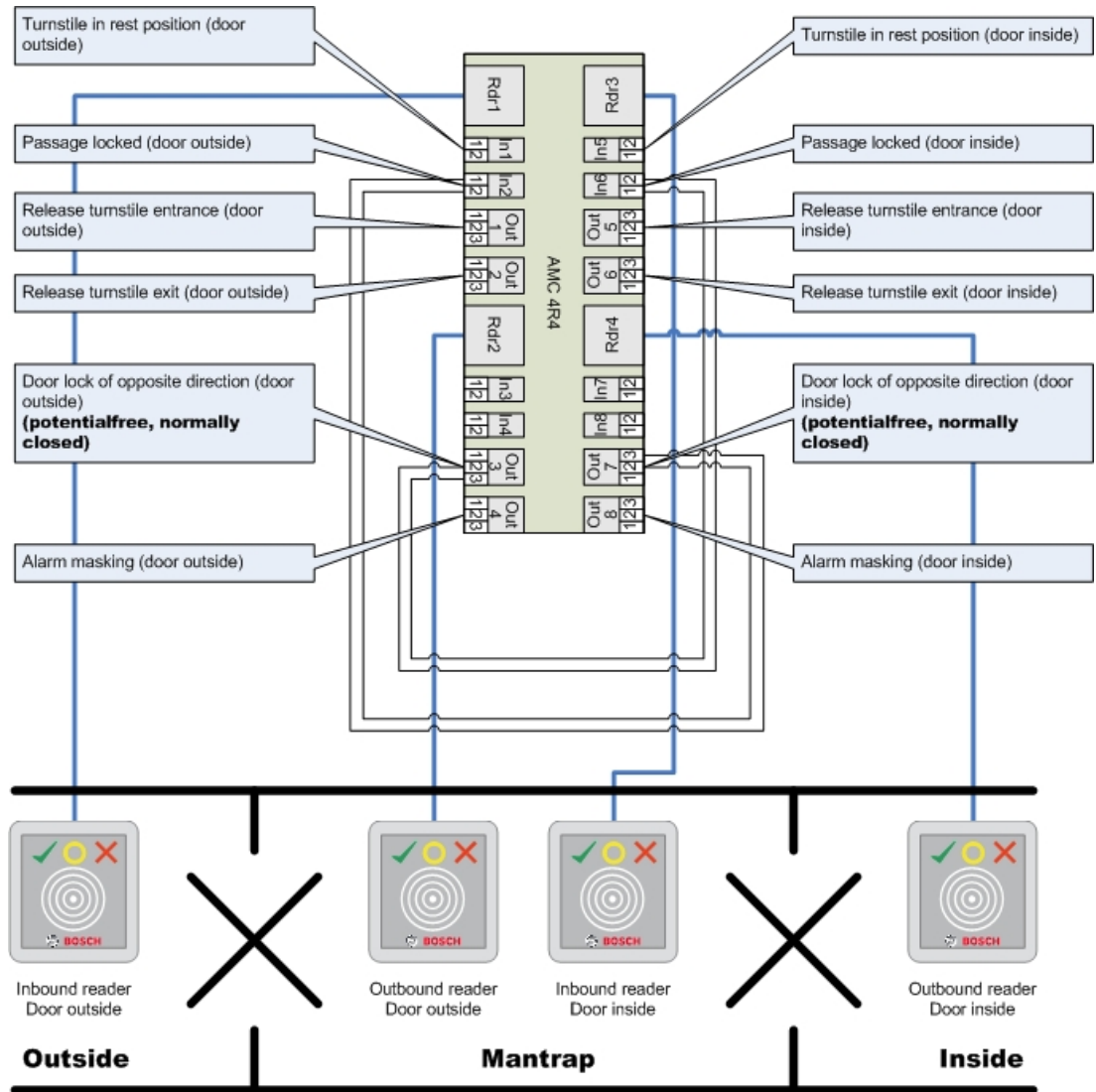


You can combine all model types 01 and 03, but set this option on both entrances belonging to the mantrap.

Along with the usual signal assignments for the door model, the mantrap option requires additional signal assignments of its own.

**Example: mantrap on one controller**

Turnstiles are the most common means of singling access by cardholders. In the following examples we have therefore used door model 3a (turnstile with entry and exit reader). Mantrap configuration with two turnstiles (DM 03a):



Connections to the door locks for the opposite direction ensure that only one of the turnstiles can be opened at any one time.

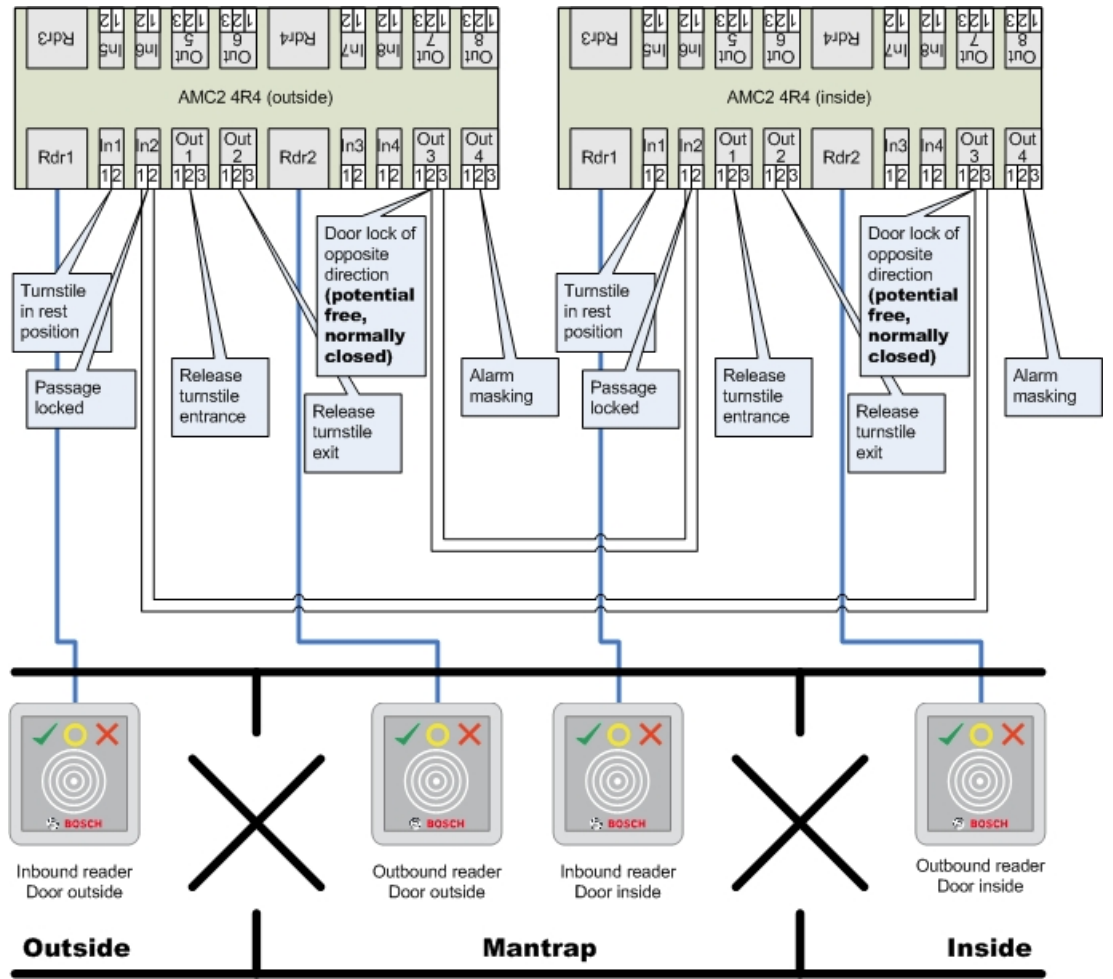


**Notice!**

The output signals (Out) 3 and 7 are to be set potential free (dry mode)  
 The signal "door lock of opposite direction" is active on the 0. It is to be used for outputs 3 and 7 "normally closed".

**Example: mantrap on two controllers**

Mantrap configuration with two turnstiles (DM 03a) which are distributed across two controllers:



Connections to the door locks for the opposite direction ensure that only one of the turnstiles can be opened at any one time.



**Notice!**

The output signal (Out) 3 is to be set potential free (dry mode)  
 The signal "door lock of opposite direction" is active on the 0. It is to be used for output 3 "normally closed".

**13.7**

**Doors**

**Configuring a Door: General Parameters**

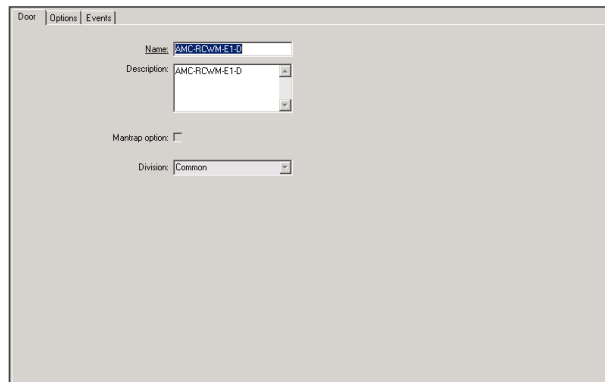
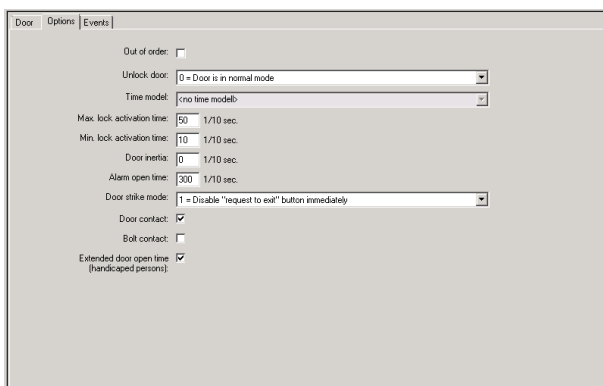


Figure 13.1:

Parameter	Possible values	Description
Name	Alphanumeric, up to 16 characters	The generated default value may optionally be replaced by a unique name.
Description	Alphanumeric, up to 255 characters	
Division	Default division is "Common"	This is a read-only field. Assignments to divisions are performed in the device editor DevEdit for each door in the device hierarchy
Only for door models 01 and 03 if a mantrap is configured:		
Mantrap option	0 = deactivated (check box is clear) 1 = activated (check box is selected)	A mantrap exists where two combined doors use door model 01 or 03. Activate the mantrap option for <b>both</b> doors. The doors will also require special physical wiring.

**Configuring a Door: Options**



Parameter	Possible values	Remarks
Manual operation	0 = check box is clear 1 = check box is selected.	0 = the door is in normal mode (default), that is, it is subject to access control by the overall system. 1 = door is excluded from the access control system. The door is not controlled and does not generate messages. It can only be locked or unlocked manually. All other parameters for this door are turned off. This parameter must be set for door and reader separately.
Unlock door	0 = Door is in normal mode  1 = Door is unlocked 2 = Door is unlocked depending on time model	0 = normal mode (default) - the door will be locked or unlocked depending on the access rights of the credentials. 1 = unlock for extended period - access control is suspended for the period. 2 = unlock for a time period defined by the time model. Access control is suspended during the period.

	<p>3 = Door is open depending on time model after first passing through</p> <p>5 = Door is blocked long-term</p> <p>6 = Door is blocked depending on time model</p>	<p>3 = locked as long as the time model is active until the first person gets access - then open as long as the time model is active.</p> <p>5 = blocked until manually unblocked.</p> <p>6 = locked as long the time model is active - there is no door control, the door cannot be used while the time model is active.</p>
Time model	one of the available time models	Time model for door opening times. If the door modes 2, 3, 4, 6, and 7 are selected the list box for the time models is available. The selection of a time model is required.
Max. lock activation time	0 - 9999	Time span for the activation of the door opener, in 1/10 of second - default: 50 for doors, 10 for revolving doors (03), and 200 for barriers (05c or 09c).
Min. lock activation time	0 - 9999	Minimum time span for the activation of the door opener, in 1/10 of a second. Electromagnetic locks need some time to de-magnetize - default: 10.
Door inertia	0 - 9999	After activation time has passed, door may be opened in this time span, without an alarm being issued, in 1/10 of second. Hydraulic doors need some time to built up pressure - default: 0.
Alarm open time	0 - 9999	If the door stays open after this time span, a message is issued (door open too long), in 1/10 of a second - default: 300. 0 = no time out, no message
Door strike mode	List box entry	0 = REX (request-to-exit) button is disabled after activation time 1 = REX (request-to-exit) button is disabled immediately (= default)
Door contact	<p>0 = deactivated (check box is clear)</p> <p>1 = activated (check box is selected)</p>	<p>0 = door has no frame contact</p> <p>1 = door has a frame contact. A closed contact usually means that the door is closed. (= default)</p>
Bolt contact	<p>0 = deactivated (check box is clear)</p> <p>1 = activated (check box is selected)</p>	<p>0 = door has no bolt contact (= default)</p> <p>1 = door has a bolt contact. A message is issued when the door is opened or closed.</p>

Extended door open time (handicapped persons)	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = the lock activation time is normal. 1 = the lock activation time is extended by the factor set in the system-wide EXTIMFAC parameter. This is to give disabled persons more time to pass through the door. (= default)
---	---	---

**Configuring a Door: Events**

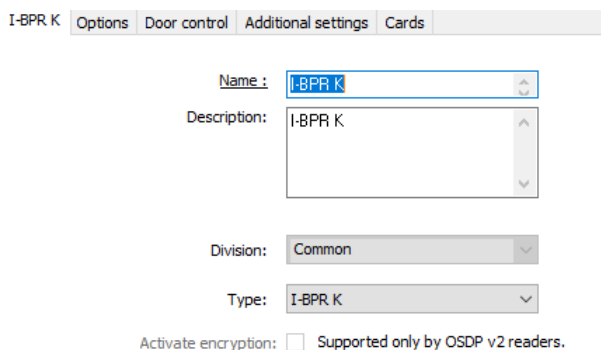


Parameter	Possible values	Remarks
Intrusion	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = no intrusion message. This is useful if a door can be freely opened from the inside. 1 = Upon unauthorized opening a message will be triggered. Another message will indicate the subsequent closure. (default)
Door state open/closed	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = no "door open" message is sent (default) 1 = a message is sent upon opening or closing.

**13.8**

**Readers**

**Configuring a Reader: General Parameters**



Parameter	Possible Values	Description
-----------	-----------------	-------------



Reader name	alphanumeric, restricted to between 1 and 16 characters	The default value can be replaced by a unique name.
Reader description	alphanumeric: 0 to 255 characters	A free text description.
Division	Default "Common" division.	Only relevant if Divisions are licensed and in use.
Type	alphanumeric, restricted to between 1 and 16 characters	Type of reader, or group of readers

**Configuring a Reader: Options**

I-BPR K | Options | Door control | Additional settings | Offline locking system | Key cabinet | Cards

PIN code required: 0 = PIN code turned c ▾

Time model for PIN codes: <no time modell> ▾

Access also by PIN code alone:

Reader terminal / bus address: 1 ▾

Attendant required:

Membership check: 0 - no check ▾

Membership time model: <no time modell> ▾

Group access: 1

Deactivate reader beep if access granted:


Deactivate reader beep if access denied:

VDS - Mode:

Max. time for arming: 50 1/10 Sec.

Parameter	Possible values	Description
PIN code required	0 = PIN code turned off - no input necessary (default) 1 = PIN code turned on - input always necessary 2 = PIN code controlled by time model - input only necessary if outside of time model	This field is only enabled if the reader has an input device.  Note that checks on the card, such as its authorizations and access sequence (if enabled), take precedence over the correctness of the PIN.

Time model for PIN codes	one of the available time models	The selection of a time model here is mandatory if the parameter <b>PIN code required</b> parameter is set to 2.
Access also by PIN code alone	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Determines whether this reader can also permit access based on a PIN alone, that is without a card, if the access control system is so configured. See Access by PIN alone
Reader terminal / bus address	1 - 4	For AMC 4W: Numbered corresponding to the Wiegand-Interfaces. For AMC 4R4: Numbered like the jumpered address of the reader.
Attendant required	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = visitor needs no attendant (default) 1 = the attendant must also use the reader
Membership check	List box entry	Membership check is typically used in the early phases before an access control system goes live. Here access is granted based on the generic company ID of the credential rather than its unique personal ID. <b>IMPORTANT</b> Membership check only works with physical credentials where the card definitions are predefined in the system (gray background), <b>not</b> with customized definitions or biometric credentials. <b>0 - no check</b> Membership check is off, but the card is checked for authorizations as normal (default) <b>1 - check</b> The card is checked only for company ID, that is for membership of the system. <b>2 - depending on time model</b> The card is checked for company ID (membership) but only during the period defined in the membership time model.
Membership time model	one of the available time models	The time model enables/disables the membership check. The selection of a time model is mandatory for <b>Membership check</b> option 2.
Group access	1 - 10	<b>For readers with keypad:</b> Minimum number of valid cards which must be presented to the card reader before the door is opened. The group can consist of

		<p>more cards than this number; in which case the ENTER/# key is used to signal that the group is complete. Thereupon the door is opened.</p> <p><b>For readers without keypad:</b> The exact number of valid cards which must be presented to the card reader before the door is opened. The default value is 1.</p>
Deactivate reader beep if access granted	<p>0 = deactivated (check box is clear) 1 = activated (check box is selected)</p>	If activated (1) the reader remains silent if an authorized user is granted access.
Deactivate reader beep if access not granted	<p>0 = deactivated (check box is clear) 1 = activated (check box is selected)</p>	If activated (1) the reader remains silent when an unauthorized user is denied access.
 <p>The “Deactivate Reader Beep” functions depend on the respective reader firmware. The firmware of some readers may not support this function.</p>		
VDS mode	<p>0 = deactivated (check box is clear) 1 = activated (check box is selected)</p>	If activated (1) the signalization of the of the reader is switched off.
Max. time for arming	1 - 100 [1/sec]	Maximum time for feedback from intrusion panel that arming is completed.

**Network and Operation modes**

This tab is only displayed for networked biometric readers.

**Templates** are stored patterns. They can be card data or biometric data.

Templates can be stored both on devices above the reader in the device tree, and on the reader itself. Data on the reader is periodically updated by the devices above it.

The reader can be configured to use its own templates when making access decisions, or only to use the templates from the devices above it.

Parameter	Description
IP address:	The IP address of this networked reader
Port:	The default port is 51211

Parameter	Description
<b>Templates on server</b>	
Card only	The reader reads card data only. It authenticates them against data from the overall system.
Card and fingerprint	The reader reads both card data and fingerprint data. It authenticates them against data from the overall system.
<b>Templates on device</b>	
Person dependent verification	The reader allows settings of the individual cardholder to determine which <b>Identification mode</b> it uses. The personnel data offers the following options: <ul style="list-style-type: none"> <li>- Fingerprint only</li> <li>- Card only</li> <li>- Card and fingerprint</li> </ul> These are described later in this table.
Fingerprint only	The reader reads fingerprint data only. It authenticates them against its own stored data.
Card only	The reader reads card data only. It authenticates them against its own stored data.
Card and fingerprint	The reader reads both card data and fingerprint data. It authenticates them against its own stored data.
Card or fingerprint	The reader reads either card data or fingerprint data, depending on which the cardholder offers first. It authenticates them against its own stored data.

**Configuring a Reader: Door Control**

I-BPR K
Options
Door control
Additional settings
Cards

Reader blocking: 0 = Reader is in normal mode v

Time model to block reader: <no time model> v

Office mode:

Manual operation:

Check time model upon access:

Additional verification:

Host request timeout: 330 1/10 sec.

Open door if no answer from host:

Parameter	Possible values	Remarks
-----------	-----------------	---------

Reader blocking	List box entry	0 = Reader in normal mode - no blockade (= default) 1 = Reader is permanently blocked - permanent blockade 2 = Reader is blocked depending on time model - blockade according to time model set with <i>Time model to block reader</i>
Time model to block reader	one of the time models defined in the system.	Blocks the reader according to the time model selected.
Office mode	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Allows this reader to be used in Office mode ,
Manual operation	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = reader in normal mode (= default)  1 = reader is effectively removed from the access control system, that is "out of order". No commands are received. All other parameters for this reader are turned off. The parameter must be set independently for both the reader and door.
Check time models upon access	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = Time models will not be checked. There is no time-restriction for access. 1 = If the cardholder has a time model assigned to it, either directly or as an area-time authorization, the time model will be checked. (= default)
Additional verification	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = host verification is not required  1 = host verification is required (default) <b>(IMPORTANT: Activation of this option is required for additional video verification by the operator of a BVMS or BIS system)</b>
Host request timeout	0 = deactivated	0 = AMC works without host verification (does not work with <i>Area Change</i> or <i>Person Countings</i> ). This control is only active if Host verification is deactivated (0) and <i>Open door if no answer from host</i> is activated (1) 1 to 9999 = using the reader requires a BIS inquiry. The inquiry has to be answered within the specified time span. If the time expires, the AMC checks the parameter <b>Open</b>

		<b>door if no answer from host</b> and decides for itself. Values are 1/10 of a second. (Default = 30)
Open door if no answer from host	0 = deactivated (check box is clear) 1 = activated (check box is selected)	This control is only active, if the parameter <b>Host verification</b> is set. 0 = does not open the door if a host decision is needed but cannot be retrieved (offline operation). 1 = opens the door after time out if it can be released from the AMC. (= default)
Check parking ticket credits	0 = deactivated (check box is clear) 1 = activated (check box is selected)	If activated (1) the parking ticket credits are checked.
Check overstayed parking	0 = deactivated (check box is clear) 1 = activated (check box is selected)	If activated (1) it is checked if the parking period was too long.

**Configuring a Reader: Additional Settings**

I-BPR K
Options
Door control
Additional settings
Cards

Access sequence check: 0 - Deactivated ▼

Time management:

Double access control

Enable:

Door group ID: ..

Anti-Pass-Back timeout: 5 minutes

Random screening

Random screening:


Screening rate:

Timeout random screening:  Minutes

REX button active when IDS armed:

Read permanently:

Parameter	Possible values	Remarks
-----------	-----------------	---------

<p>Access sequence check</p>	<p>0 - Deactivated                  1 - Activated; deactivate upon LAC malfunction                  2 - Activated; leave active upon LAC malfunction                  3 - Activated; use strict sequence checking even when LAC malfunctions (note: update person's location manually)</p>	<p>0 = reader takes no part in access sequence checking (= default)                  An activated sequence check can handle persons who are set UNKNOWN in the following ways:                  1 = The first reading of the card will be down without checking the location. All controllers must be online.                  2 = The first reading of the card will be down without checking the location.                  3 = Checking the location will be down for every reading the card during LAC malfunction.</p>
<div style="text-align: center;">  </div> <p>In the BIS platform there is a MAC command to activate or deactivate all access sequence checking generally.</p> <p>To deactivate access sequence checking for a time period, a value is given in minutes with a maximum of 2880 (= 48 hours). Setting the value "0" deactivates access sequence checking completely.</p> <p><b>Note:</b> This command can modify access sequence checking only for those readers where the parameter <b>Enable access sequence</b> is set. It does not deactivate/activate access sequence checking for <i>all</i> readers.</p>		
<p>Time Management</p>	<p>0 = deactivated (check box is clear)                  1 = activated (check box is selected)</p>	<p>In activated (1) the Ace process collects data for the time attendance system.</p>
<p><b>Double access control (anti-passback control)</b></p>		
<p>Enable</p>	<p>0 = deactivated (check box is clear)                  1 = activated (check box is selected)</p>	<p>0 = without double access control (= default)                  1 = with double access control                  Within the time span set by the <b>Duration</b> parameter, this reader and other readers in the group cannot be used with the same card.                  If this parameter is activated, a door group ID must be used, even if only one reader is used.</p>

Door group ID	Letters A - Z and a - z, and "-" 2 characters	Readers can be grouped using a Door group ID. Presenting a card at one reader will block subsequent bookings at all readers in the door group (Default = -- ) until the time out elapses.
Anti-passback time out	1 - 120	The reader can be used with the same card after this time span has elapsed. As soon as the card is used at a reader outside the group the blockade is lifted immediately. Values are minutes - default = 5.
Random screening	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = no random screening  1 = random screening according to the factor will have no admittance until unblocked by the dialog <b>Blocking</b> .
Screening rate	1 - 100	Percentage of random screening for an extended check. Available if random screening is activated.
Timeout random screening	1 - 120	With in the set time the user is subject to the random screening. Values are minutes - default = 5.
REX button active when IDS armed	0 = deactivated (check box is clear) 1 = activated (check box is selected)	For <b>DM10</b> and <b>DM14</b> only: REX push buttons are disabled by default when the IDS is armed. This would make it impossible to exit the monitored area. This new reader parameter enables the REX button even when the IDS is armed. This parameter also needs to be set where a reader is used instead of a push button.
Read permanently	0 = deactivated (check box is clear) 1 = activated (check box is selected)	The reader read permanently if the reader has the respective firmware of the manufacturer.



### Configuring a Reader: Cards

WIE1K Reader | Options | Door control | Additional settings | Offline locking system | Biometrics | Key cabinet | **Cards**

---

Card validation

Motorized card reader:

Withdraw card:

Triggering criteria:

Blocked card

Visitor card

Card is blacklisted

Invalid time model

Invalid area/time model

No authorization

Always collect

Collect visitor cards on collecting date

Collect visitor cards on last day of validity

Collect other cards (no visitor cards) on collecting date

Collect other cards (no visitor cards) on last day of validity

Time model defined and invalid, independent of access and reader parameters

Area/Time model defined and invalid, independent of access and reader parameters

Parameter	Possible values	Remarks
Motorized card reader	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Select this check box if a motorized card reader is used
Withdraw card	0 = deactivated (check box is clear) 1 = activated (check box is selected)	In the case of a motorized card reader Withdraw means physically retain the card. In the case of other card readers Withdraw means that the system makes the card invalid.
Triggering criteria	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Select from this list any criteria that should trigger the action <b>Withdraw card</b> .



**Notice!**

Motorized card readers can only be used with IBPR readers.

### 13.8.1 Configuring random screening

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

#### Prerequisites:

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

#### Procedure

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

## 13.9 Access by PIN alone

#### Background

Keypad readers can be configured to allow access by PIN alone.


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

The operator can enter PINs for personnel manually, or assign to them PINs generated by the system.

Note that the same personnel can continue to access using any physical cards that are also assigned to them.

#### Prerequisite authorization for Operators

Authorization for a cardholder to access by PIN alone is only grantable by operators with the special authorization to assign virtual cards. To give an operator this authorization, proceed as follows.

1. Navigate to Main menu > **Configuration** > **Operators and workstations** > **User profiles**
2. Select the User profile that is to receive the authorization:  
Either enter it in the text field **Profile name** or use the search facility to find the desired profile.
3. In the list of dialogs, click the cell containing **Cards**  
A popup window called **Special functions** appears near the bottom of the main window pane.
4. In the Special functions pane select the check box for **Assign virtual cards (PIN)**
5. Click  or **Apply** to save your changes

#### Setting the length of the Identification PIN for supported reader types

The length of manually entered or system-generated PINs is governed by the parameter set in the system configuration.

- Main menu > **Configuration** > **Options** > **PIN codes** > **PIN code length**

**Configuring a reader for access by PIN alone**



1. Navigate to Main menu > **Configuration** > **Device data** > **Workstations** tree
2. In the **Workstation** pane select the workstation to which the reader is physically connected.
3. Right-click the workstation and add a reader of type **Dialog Enter PIN** or **Dialog Generate PIN**.
4. Select the reader in the **Workstations** pane.  
A custom reader configuration pane appears to the right of the **Workstations** pane.
5. Verify that the drop-down list **Card usage default** contains the default value **Virtual card. Use PIN as card**.



6. Click  or **Apply** to save your changes



7. In the device editor DevEdit, navigate to the **Device configuration** tree
8. Select the reader at the entrance where you wish to configure access by PIN alone.
9. In the **Options** tab, select the check box **Access also by PIN code alone**.



10. Click  or **Apply** to save your changes

## 13.10 AMC extension boards

### Creating an AMC-I/O-EXT (I/O Extension Board)


Extension boards provide additional input and output signals, if the eight contacts located on the AMC are not sufficient for the connection of the necessary contacts (for example, with elevators).

These extensions are physically connected to the associated AMC and can be installed only below the respective AMCs in the Device Editor. The corresponding AMC entry is selected in the explorer for the creation of an AMC-EXT, and the entry **New Extension Board** is chosen in the context menu **New Object**.

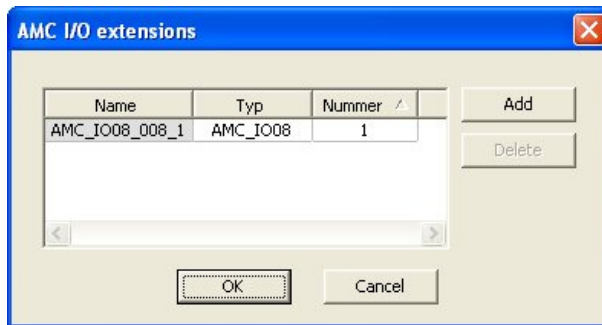


**Notice!**



Clicking the + button  in the toolbar of the Device Editor creates new entrances only. Extension boards can be selected using the context menu.

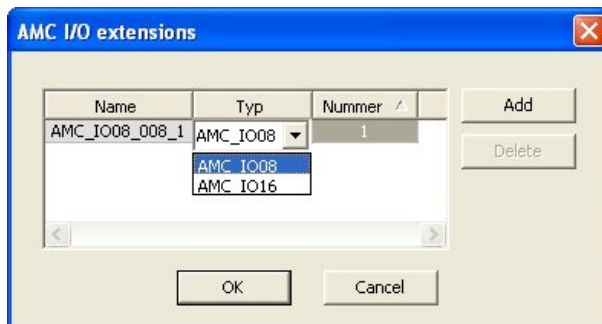
A selection dialog for the creation of the extensions appears.



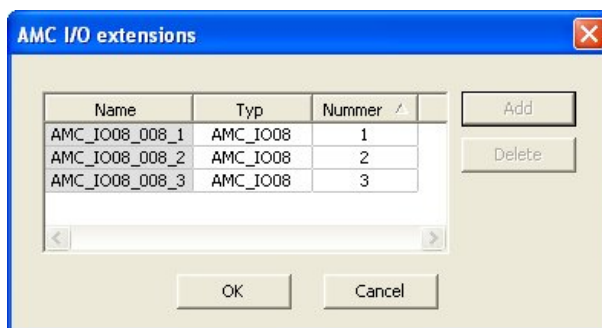
AMC-EXT is available in two variants:

- AMC\_IO08: with 8 inputs and 8 outputs
- AMC\_IO16: with 16 inputs and 16 outputs
- AMC\_4W extension: with 8 inputs and 8 outputs

The selection dialog contains an entry with an AMC\_IO08. By double-clicking the list box in the **Type** column, you can also place an AMC\_IO16.



You can connect up to three extensions to one AMC. A mix of the two variants is possible. Click **Add** to create more list entries. These can all the column entries can be customized.



Extension boards are numbered 1, 2 or 3 as created. The numbering of the signals begins for each board at 01. The signal number In combination with the board number provides a unique identification. The signals of the extension boards can also be seen on the tab of the AMC to which they belong.

Together with the input and output signals on the AMC up to 56 signal pairs can thus be provided.

Extension boards can be added as required individually or at a later date up to the maximum number (3 per AMC).

### Creating an AMC2 4W-EXT

It is possible to configure special extension boards (AMC2 4W-EXT) for controllers with Wiegand reader interfaces AMC2 4W). These modules provide an additional 4 Wiegand readers connections as well as 8 input and 8 output contacts each. Thus the maximum number of readers and doors connectable per AMC2 4W can be doubled to 8.



#### Notice!

The AMC2 4W-EXT can not be used as a standalone controller, but only as an extension to an AMC2-4W. The doors are controlled and the access control decisions are made only by the AMC2 4W.

The AMC2 4W-EXT can only be used in connection with an AMC2 4W. As it only has Wiegand reader interfaces it is not usable with the AMC variant AMC2 4R4.

Like the I/O extension boards (AMC2 8I-8O-EXT and AMC2 16I-16O-EXT) the AMC2 4W-EXT is connected via the extension interface of the AMC2 4W. The extension board has neither memory nor display of its own, but is controlled entirely by the AMC2 4W.

One AMC2 4W-EXT and a maximum of three I/O extensions can be connected to each AMC2-4W.

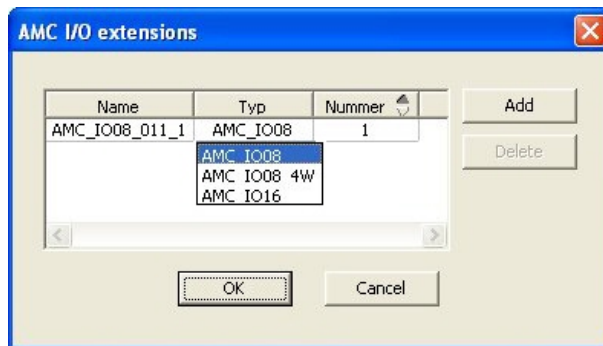
To create an AMC2 4W-EXT in the system right-click the desired parent AMC2 4W in the Explorer and select **New object > New extension board** from the context menu.



#### Notice!

The **+** button in the tool bar of the Device data editor can only be used for adding entrances. Extension boards can only be added via the context menu.

The same selection dialog appears as for creating I/O extensions, except that the list for an AMC2 4W contains the additional element AMC\_IO08\_4W.



The list entry AMC2 4W can only be added only once, whereas up to three I/O Extensions can be added.

The button **Add** adds new list entries. In the case of an AMC2 4W the maximum number is 4 whereby the fourth entry is created as an AMC2 4W-EXT board.

Extension boards are numbered according to creation order 1, 2 or 3. The AMC2 4W-EXT receives the number 0 (zero). The numbering of the signals for the AMC2 4W-EXT continues from that of the controller, namely 09 to 16, whereas for each I/O board the numbering begins with 01. The signals for all extension boards are also shown on the tab for the relevant AMC2 4W.

Together with the input and output signals of the AMC2 4W up to 64 signal pairs can be provided.

### Modifying and deleting extension boards


The first tab contains the following controls for configuring extension boards.

Parameter	Possible values	Description
Board name	Restricted alphanumeric: 1 - 16 digits	The default identification guarantees a unique name, but it can be overridden manually. Please ensure that the ID is unique. Network connections with DHCP servers should use the network name.
Board description	alphanumeric: 0 - 255 digits	This text is displayed in OPC branch.
Board number	1 - 3	Number of the board connected to the AMC. Display field, only.
Power supply	0= deactivated (check box is selected) 1= activated (check box is selected)	Supervision of the supply voltage. With voltage breakdowns a message is generated at the end of a delay. The supervision function assumes the use of a USV, so that a message can be generated. 0 = no supervision 1 = supervision activated
Division	Default value "Common"	This read-only field is only applicable where the Divisions feature is licensed and used.

The tabs Inputs , Outputs and Signal Settings have the same layout and function as the corresponding tabs for the controllers.

### Deleting extension boards

It is only possible to delete an extension board when none of its interfaces is occupied. The

associated signals must first be configured on a different board before the delete button  and the context menu option **Delete object** become usable.

### AMC2 4W-EXT

Because readers which occupy extension boards can not be removed or reconfigured singly, they need to be deleted along with their corresponding entrances. Not until then can the AMC2 4W-EXT be removed as well.

# 14 Custom Fields for personnel data

## Introduction

Data fields for personnel are customizable in many ways:

- Whether they are **Visible**, that is, whether they are displayed in the ACE client at all
- Whether they are **Required**, that is whether a data record can be stored without valid data in the field
- Whether the values they contain must be kept **Unique** within the system
- What data type they contain (text, date-time, integer etc.)
- Where (on which tab, in which column and in which row) in the ACE client they will appear
- How large they will appear
- Whether and where the data will be used in standard reports

It is of course still possible to define entirely new data fields with all the attributes listed here.

## 14.1 Previewing and editing Custom fields

### Dialog path

- Main menu > **Configuration** > **Options** > **Custom fields**

The main window is divided into two tabs

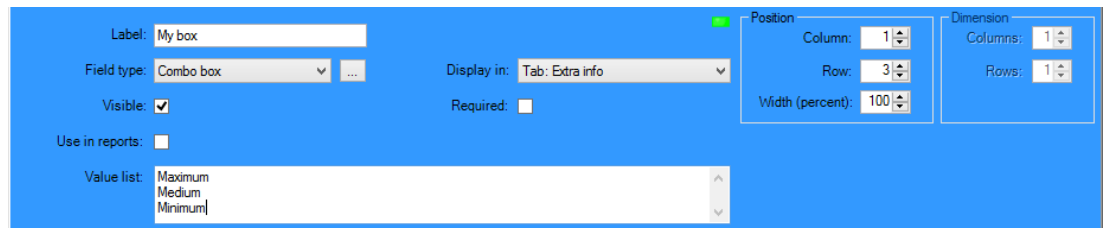
**Overview** This tab and its sub tabs (**Address, Contact, Additional person data, Additional Company data, Remarks, Card Control** and **Extra Info**) are read-only, and contain a roughly WYSIWYG overview of which data will appear on which tabs in the ACE Client.

**Details** This tab contains a list of editors, one for each predefined or user-defined data field.

### Editing existing data fields



On the **Custom fields > Details** tab each data field, predefined or user-defined, has its own editor window where its attributes can be modified.

Click in the editor of the field that you wish to modify. The active editor will be highlighted.



The editable attributes of custom fields are explained in the following table.

Label text	Description
<b>Label</b>	<b>Label</b> is the label of the data field as it appears in the client. It can be freely overwritten to reflect the terminology used on your site.
<b>Field type</b>	<b>Field type</b> is the type of the data, and determines the dialog control that the operator will use to make entries in the client. Each field type provides consistency checks for its particular input values, to ensure valid dates, times, text lengths and numerical limits.

Label text	Description
	<ul style="list-style-type: none"> <li>- <b>Text field</b> <ul style="list-style-type: none"> <li>- Click the ellipsis button next to it to specify the number of characters allowed.</li> </ul> </li> <li>- <b>Check box</b></li> <li>- <b>Date field</b></li> <li>- <b>Time</b></li> <li>- <b>Date-time field</b></li> <li>- <b>Combo box</b> <ul style="list-style-type: none"> <li>- Enter the valid values for your combo box in the text field provided. Separate them with commas or carriage returns.</li> </ul> </li> <li>- <b>Numerical input</b> <ul style="list-style-type: none"> <li>- Enter your minimum and maximum values for the numerical input in the spin boxes provided.</li> </ul> </li> <li>- <b>Building control 1</b> and <b>Building control 2</b> <ul style="list-style-type: none"> <li>- These are special controls that can be relabeled here (in the <b>Label</b> field) and linked to commands in the client UI. Thus you can give specific users permission, via their cards, to perform special operations within the site. Examples of such operations are the turning on of floodlights or the control of special equipment.</li> </ul> </li> </ul>
<b>Visible</b>	Clear this check box to prevent the data field from appearing in the client.
<b>Unique</b>	Select this check box to make reject data field contents that are not unique. For example, personnel numbers should be unique for all employees.
 	<p>The green light means that the data field is <b>not</b> currently used in the database.</p> <p>The red light means that the data field is currently used in the database.</p>
<b>Display in</b>	Use this drop-down list to select the client tab on which the data field should appear.
<b>Required</b>	<p>Select this check box to make the data field mandatory. For example, a surname is required for each personnel record. Without a surname the data record can not be stored.</p> <p>Note that the editor will not allow a required data field to be set invisible via the <b>Visible</b> check box.</p> <p>For ease of use in the client it is highly recommended that all required fields be placed on the first tab.</p>
<b>Position</b>	<p>Use the spin boxes for <b>Column</b> and <b>Row</b> to position the data field on the tab named in the <b>Display in</b> drop-down list.</p> <p>Note that the editor will not allow you to select a position that is already in use, or to overlay existing data fields.</p> <p>Use the <b>Width (percent)</b> spin box to set the size of certain resizable controls, such as text fields. 100% means that the control will occupy all of the slot that is not already occupied by the data-field label.</p>
<b>Dimension</b>	Use the spin boxes for <b>Column</b> and <b>Row</b> to specify the number of columns and rows to be occupied on the tab named in the <b>Display in</b> drop-down list. Note that the editor will not allow you to overlay existing data fields.



**Creating and editing new data fields**

On the **Custom fields > Details** tab each data field, predefined or user-defined, has its own editor pane where its attributes can be modified.

Click the **New field** button to create a new custom field with its own editor. The active editor pane will be highlighted.

The editor has the same dialog controls for editing existing data fields, see the table above, plus two extra:

<b>Use in reports</b> (check box)	Select this check box to enable the new data field to appear in standard reports.
<b>Sequence number</b> (spin box)	The sequence number determines the column that the data field will occupy in standard reports.



**Notice!**

Only sequence numbers 1..10 are currently addressable by **Badge Designer** and **Reports**.

**14.2**

**Rules for data fields**

- Location of data fields
  - Each field can only appear on one tab.
  - Each custom field can appear on any selectable tab.
  - Fields can be moved to other tabs by changing the entry in the **Display in** pull-down list.
- The label can contain any text: maximum length 20 characters.
- The custom text fields can contain any text: maximum length 2000 characters.
- Any field can be made a required field, but its **Visible** check box must be selected.



**Notice!**

Urgent recommendations before productive use

Agree and finalize the field types and their usage before using them to store persons' data:

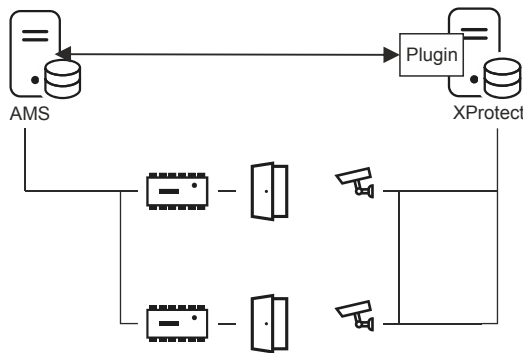
Each data entry field is assigned to a specific database field so that data can be located both manually and by report generators. Once data records from custom fields have been stored in the database, then these fields can no longer be moved or changed without risking data loss.

## 15 Configuring Milestone XProtect to use AMS

### Introduction

This chapter describes how to configure Milestone XProtect to use the access control features of AMS.

A plugin provided by AMS, but installed on the XProtect server, transmits events and commands to AMS, and sends results back to XProtect.



The configuration has 3 stages, which are described in the following sections:

- Installing the AMS public certificate on the XProtect server.
- Installing the AMS plugin on the XProtect server.
- Configuring AMS within the XProtect application.

### Prerequisites

- AMS is installed and licensed.
- XProtect is installed and licensed on the same computer or on its own computer.
- A network connection exists between both systems.

### Installing the AMS public certificate on the XProtect server

Note that this procedure is only required if AMS is running on a different computer.

1. Copy the certificate file from the AMS server  
`C:\Program Files (x86)\Bosch Sicherheitssysteme\Access Management System\Certificates\Access Management System Internal CA.cer`  
 to the XProtect server.
2. On the XProtect server, double-click the certificate file.  
 The Certificate wizard appears.
3. Click **Install Certificate...**  
 The Certificate Import Wizard appears.
4. Select **Local Machine** as the **Store Location** and click **Next**
5. Select **Place all certificates...**
6. Click **Browse...**
7. Select **Trusted Root Certification Authorities** and click **OK**
8. Click **Next**
9. Review the summary of the settings and click **Finish**

### Installing the AMS plugin on the XProtect server

1. Copy the setup file  
AMS XProtect Plugin Setup.exe  
from the AMS installation media to the XProtect server.
2. Execute the file on the XProtect server.  
The setup wizard appears.
3. In the setup wizard, make sure that the AMS XProtect Plugin is marked for installation, and click **Next**.  
The End User License Agreement is displayed. Click **Accept** to accept the agreement if you wish to continue.
4. The wizard displays the default installation path for the plugin. Click **Next** to accept the default path or **Browse** to change it before clicking **Next**.  
The wizard confirms that it is about to install the AMS XProtect plugin.
5. Click **Install**
6. Await confirmation of the completed installation and click **Finish**.
7. Restart the Windows service named **Milestone XProtect Event Server**.

### Configuring AMS within the XProtect application

1. In the XProtect management application, navigate to **Advanced Configuration > Access Control**
2. Right-click **Access Control** and select **Create new...**  
The plugin wizard appears.
3. Enter the following information in the plugin wizard:
  - **Name:** A description of this AMS-XProtect integration to distinguish it from other integrations on the same XProtect system
  - **Integration plug-in:** AMS - XProtect Plugin (This name will be available in the drop-down list after successful installation of the plugin)
  - **AMS API discovery endpoint:** https://<hostname of the AMS system>:44347/  
where 44347 is the default port selected when installing AMS API.
  - **Operator name:** The username of an AMS operator with at least permissions to operate the doors to which XProtect cameras will be mapped.
  - **Operator password:** the AMS password of that operator.
4. Click **Next**  
The AMS plugin connects to the AMS server that you have specified, and lists the access control elements that it discovers (doors, units, servers, events commands and states)
5. When the progress bar is complete, click **Next**  
The **Associate cameras** wizard page appears.
6. To associate cameras with doors, drag cameras from the **Cameras** list to access points in the **Doors** list.
7. When finished, click **Next**.  
XProtect saves the configuration and confirms when it has saved successfully.

## 16 Configuring Threat Level Management

### Introduction

The goal of threat level management is to respond effectively to emergency situations by making an instant change to the behavior of entrances throughout the affected area.

### 16.1 Concepts of Threat Level Management

- A **Threat** is a critical situation that requires an immediate and simultaneous response from some or all entrances in an access control system.
- A **Threat level** is the system's response to a foreseen situation. Each threat level must be carefully configured so that each of the MAC's entrances knows how to respond. Threat levels are completely customizable, for instance, typical high threat levels might be configured as follows:
  - **Lockout**: Only first responders, with high security levels, can enter.
  - **Lockdown**: All doors are locked. Both ingress and egress are denied to all credentials below a configured security level.
  - **Evacuation**: All exit doors are unlocked.
- Typical low threat levels might be configured as follows:
  - **Sports event**: Doors to sports areas are unlocked, all other areas are secured.
  - **Parents' evening**: Only selected classrooms and main entrance are accessible.
- A **Threat alert** is an alarm that triggers a threat level. Suitably authorized persons can trigger a threat alert with a momentary action, for example through the operator's UI, through a hardware signal (e.g. push button), or by presenting a special alert card at any reader.
- A **Security level** is an attribute of cardholders' and readers' **Security profiles**, expressed as an integer 0..100. Each threat level sets the readers of its Main Access Controller (MAC) to the appointed security levels. Then those readers grant access only to credentials of persons with an equal or greater security level in their security profiles.
- A **Security profile** is a collection of attributes that can be assigned to a **Person type** (**Person security profile**), to a door (**Door security profile**), or to a reader (**Reader security profile**). Security profiles govern the following access control behaviors:
  - **Security level**, as defined above, for person type, door or reader
  - **Screening rate**. The percentage probability that random screening will be triggered by this person type or reader.

### 16.2 Overview of the configuration process

Threat Level Management requires the following configuration steps, which are explained in detail after this overview

1. In the Device Editor
  - Define threat levels
  - Define Door security profiles
  - Define Reader security profiles
  - Assign Door security profiles to entrances
2. In the System data dialogs
  - Define Person security profiles
  - Assign Person security profiles to Person types
3. In the Personnel data dialogs
  - Assign Person types to Persons
  - Assign Person types to Groups of persons

When threat level management has been successfully configured, alarms and the device states of the MAC can be monitored and controlled from the Map view application. See the Map view online help for details.

## 16.3 Configuration steps in the device editor

This section describes the prerequisite configuration steps that are required in the device editor.



### Notice!

Device data cannot be modified in the device editor while a threat level is in operation.


### 16.3.1 Creating a threat level

This section describes how to create threat levels for use at your site. Up to 15 may be created.

#### Dialog path

- **Main menu > Configuration > Device data**

#### Procedure

1. Select sub-tab **Threat levels**
  - The Threat levels table appears. It may contain up to 15 threat levels, each with a name, a description and a check box with which to activate the threat level after it has been configured.
2. Click the line that reads **Please enter a name for the threat level**
3. Enter a name that will be meaningful to the system operators.
4. (optional) In the **Description** column, enter a fuller description of how the entrances will behave when this threat level is in operation.
5. Do **not** select the **Active** check box at this time. First complete all the other configuration steps for this threat level, as described in the following sections.
6. Click  (Save) to save the new threat level.

### 16.3.2 Creating a Door security profile

This section describes how to create security profiles for different types of door, and to define the state to which all doors of this profile will switch when a threat level comes into operation.

#### Dialog path


- **Main menu > Configuration > Device data**

#### Prerequisites

- At least one threat level has been defined
- At least one entrance has been configured in the device tree.

#### Procedure

1. Select sub-tab **Door security profiles**
  - The main dialog window divides into 2 panes: **Selection** and **Door security profile** (default name)
2. Click **New**

- A new Door security profile is created with a default name
  - The **Threat level** table in the **Door security profile** pane becomes populated with the threat levels that have already been created, along with a value of **undefined** for each in the **State** column.
3. In the **Door security profile** pane, enter a name for the type of door to which this profile will be assigned.
    - The new profile name appears in the **Selection** pane. If desired it can be deleted from the configuration by clicking **Delete** in that pane.
  4. (Optional) Enter a description of the profile, to help operators assign the profile correctly.
  5. If this profile is to be assigned to turnstiles, select the **Turnstile** check box.
    - This will provide extra options for the target state of the door at different threat levels, for instance, the options to permit ingress or egress alone, or both together.
  6. In the **State** column of the **Threat level** table, for each threat level select a suitable target state, for all doors of this profile, whenever that threat level is triggered.
  7. Click  (Save) to save the changes.

Repeat the procedure to create as many Door security profiles as there are types of door in your configuration. Typical door types might be:

- Main public door
- Evacuation access to outside
- Access to classrooms
- Public access to sports arena

### 16.3.3

#### Creating a Reader security profile

This section describes how to create security profiles for different types of reader. Reader security profiles define the following reader attributes **for each threat level**:

- The minimum security level required by a credential to gain access at the reader.
- The screening rate, that is, the percentage of cardholders that will be selected randomly for extra security screening.
  - **Note:** a screening rate that is set in a reader security profile overrides a screening rate set on the reader itself.

#### Dialog path


- **Main menu > Configuration > Device data**

#### Prerequisites

- At least one threat level has been defined
- At least one entrance has been configured in the device tree.

#### Procedure

1. Select sub-tab **Reader security profiles**
  - The main dialog window divides into 2 panes: **Selection** and **Reader security profile** (default name)
2. Click **New**
  - A new Reader security profile is created with a default name
  - The **Threat level** table in the **Reader security profile** pane becomes populated with the threat levels that have already been created, along with a default value of **0** for each in the **Security level** and the **Screening rate** columns.

3. In the **Reader security profile** pane, enter a name for the type of reader to which this profile will be assigned.
  - The new profile name appears in the **Selection** pane. If desired it can be deleted from the configuration by clicking **Delete** in that pane.
4. (Optional) Enter a description of the profile, to help operators assign the profile correctly.
5. In the **Security level** column of the **Threat level** table, for each threat level, select a minimum security level (integer 0..100) that an operator must have in order to operate a reader of this profile whenever that threat level is triggered.
6. In the **Screening rate** column of the **Threat level** table, for each threat level select the percentage of cardholders that will be selected randomly by the reader for extra security checks whenever that threat level is triggered.
7. Click  (Save) to save the changes.

### 16.3.4

#### Assigning door and reader security profiles to entrances

This section describes how to assign the door and reader security profiles to the doors and readers at particular entrances.

The first sub-procedure is to identify and filter out the set of entrances that you want to assign, and the second sub-procedure is to make the assignments.

In addition you can preview the states, security levels and screening rates of the selected entrances as they would be set by the various threat levels that you have defined.

##### Dialog path

- **Main menu > Configuration > Device data**

##### Prerequisites

- At least one threat level has been defined
- At least one entrance has been configured in the device tree.

##### Procedure

1. In the device tree select the **DMS** (the root of the device tree)
2. In the main dialog pane, select the tab **Threat level management**
  - The main dialog pane receives several sub-tabs.

##### Sub-procedure 1: Selecting entrances for assignment

1. Select sub-tab **Entrances**
  - The main dialog window divides into 2 panes: **Filter conditions** and a table of all the entrances that have been created in the system so far.
2. (Optional) In the **Filter conditions** pane enter criteria to restrict the set of entrances that appear in the table in lower half of the dialog, for example:
  - Select or clear the check boxes that determine whether **Inbound readers**, **Outbound readers** and/or **Doors** should appear in the table.
  - Enter strings of characters that must appear in the names of the entrances, areas, profile names or reader names of all entrances listed in the table.
  - Select or clear the check box that determines whether doors and readers that are not yet configured should also appear in the table
3. Click **Apply filter** to filter the Entrances list, or **Reset filter** to set the filter controls back to their default values.

##### Sub-procedure 2: Assigning security profiles to the selected entrances

Prerequisite: The entrances to be assigned have been identified and appear in the table in the lower half of the dialog.

Note that each entrance consists typically of a door or barrier plus one or more card readers. However, some specialized entrance types such as **Assembly points** may lack these.

1. In the column **Door or reader security profile**, click the cell corresponding to the door or reader you wish to assign.
2. Select a door or reader security profile from the cell's drop-down list.

#### (Optional) Previewing the behavior of doors and readers at threat levels

The columns on the right hand side of the table are read-only. They show what the lock status (**Mode**), **Security level** and **Screening rate** of the doors and readers in the table would be if the threat level selected in the **Select threat level for details** list were in operation.

Prerequisite: The entrances that you wish to preview have been identified and appear in the table in the lower half of the dialog.

- ▶ From the list **Select threat level for details** select the threat level that you wish to preview.
- ✓ The table displays the lock status (**Mode**) of the doors, and the **Security level** and **Screening rates** of the readers, as they would be if the selected threat level were in operation.

## 16.3.5

### Assigning a threat level to a hardware signal

This section describes how to assign a hardware input signal to trigger or cancel a threat alert.


#### Dialog path

- **Main menu > Configuration > Device data**

#### Prerequisites

- At least one threat level has been defined
- At least one entrance has been configured in the device tree.

#### Procedure

1. In the device tree select an **entrance** below the AMC controller whose input signals you want to assign.
2. In the main dialog window, select the **Terminals** tab.
  - The table of entrances and signals is displayed.
3. In the row of the signal that you want to assign, click the cell for **Input signal**.
  - The drop-down list contains a command **Threat level: Deactivate** plus a **Threat level: <name>** for each threat level that you have previously defined.
  - The command **Threat level: Deactivate** will cancel any threat level that is currently in operation.
4. Assign the commands to the desired input signals.
5. Click  (Save) to save the changes.



#### Notice!

Restriction for DM 15

Door model 15 (DIP/DOP) cannot currently be used to trigger a threat level.



## 16.4 Configuration steps in System data dialogs

This section describes how to create **Person security profiles** and assign them to **Person types**.

### 16.4.1 Creating a Person security profile



**Dialog path**

- **Main menu > System data > Person security profile**

**Prerequisites**

Person security profiles require careful planning and specification in advance, as they will have important consequences for the functioning of the system in critical situations.

**Procedure**

1. If the dialog already contains data, click  (New) to clear it.
2. Enter a name for the new profile in the text field Security profile name:
3. (Optional) Enter a description of the profile, to help operators assign the profile correctly.
4. Enter an integer between 0 and 100 in the **Security level** box.
  - Given that the cardholder is authorized to use an entrance, 100 is sufficient to gain access at any reader, even if its security level is also currently set to 100
  - Otherwise the security level in a cardholder’s Person security profile must be equal to or greater than the current security level of the reader.
5. Enter an integer between 0 and 100 in the **Screening rate** box.
  - **Note:** The screening rate of the person profile is secondary to that of the reader profile. The table below describes the interplay between the two profile screening rates.
6. Click  (Save) to save the changes.

**Interplay of screening rates for person and reader security profiles**

Screening rate (%) in Reader security profile <b>R</b>	Screening rate (%) in Person security profile <b>P</b>	Person selected for extra security checks?
0	Any	<b>No</b>
100	Any	<b>Yes</b>
1..99	0	<b>No</b>
1..99	100	<b>Yes</b>
1..99	1..99	<b>Possibly</b> Probability = MAX(R,P)


### 16.4.2 Assigning a Person security profile to a Person Type

**Dialog path**

- **Main menu > System data > Person Type**
- **ACE client > System data > Person Type**

**Procedure**

**Note:** for historical reasons, **Employee ID** is here a synonym for **Person type**

1. In either the **Predefined employee IDs** table, or the **User-defined employee IDs** table, select the cell in the **Security profile name** column that corresponds to the desired Person type.
2. Select a person security profile from the drop-down list.
  - Repeat this procedure for all person types that require a person security profile
3. Click  (Save) to save your assignments

## 16.5 Configuration steps in Personnel data dialogs

This section describes how new **Person** records that are created in the system, receive a **Person security profile** through their **Person type**.

### Dialog paths

- **Main menu > Personnel data > Persons**
- **Main menu > Personnel data > Group of Persons**

**Note:** for historical reasons, **Employee ID** is here a synonym for **Person type**

### Procedure

All **Person** records created in the system must have a **Person type**.

1. Ensure that system operators assign only **Person types** that have been linked to a **Person security profile** in the dialog **Main menu > System data > Person Type**
2. For details on the linking of **Person security profiles** and the creation of **Person** records, click the following links.

### Refer to

- *Assigning a Person security profile to a Person Type, page 113*
- *Creating and managing personnel data, page 115*

## 17 Creating and managing personnel data

### Dialog path

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

### Overall Procedure

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

For **Visitors**, proceed as follows:

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



### Notice!

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

### The process of scanning cards.

When cards are scanned at readers, the reader carries out a number of checks:

- Is the card valid and registered on the system?
- Is the cardholder currently blocked (disabled in the system)?
- Does the card holder have the access authorization for entering in this direction?
- Is the access authorization an area-time authorization? If so, is the scanning time within the periods set by the time model?
- Is the access authorization active, i.e. neither **expired** nor **blocked** (disabled)?
- Is the cardholder subject to a time model? If so, is the scanning time within the defined intervals?

**Prerequisite:** Time model checks must be enabled at the reader concerned.

- Is the cardholder in the correct location according to Access sequence monitoring ?  
**Prerequisite:** Access sequence monitoring is enabled at the reader concerned.
- Has a maximum number of persons been defined for the destination area of this reader, and has this number already been reached?
- In the case of Access sequence monitoring, including anti-passback : Is this card being scanned at a reader before the blocking time set by anti-passback has elapsed?
- Is an additional PIN code required? **Prerequisite:** the reader has a keyboard.
- If a threat level is in operation, does the **Person security profile** of the cardholder have a **security level** that is at least equal to the security level of the reader at this threat level?

### 17.1 Persons

The data of persons for whom the check box **Administered globally** has been selected can be edited only by operators with the additional right of **Global Administrator**. This right is set in the operator dialog of the BIS Configuration Browser.

Protected data are:

- All data of the dialog **Persons** except the tab **Remarks** and specially defined additional information fields on the **Extra Info** tab.
- All data of the **Cards** dialog.

- All data of the **PIN Code** dialog.
- All other data of these persons can be edited by any operator.

The following table lists the main kinds of data that may be recorded. Nearly all fields are optional. Mandatory fields are clearly marked with underlined labels in the user interface.

Tab	Field name
Dialog header	Name
	First name
	Birth name (called maiden name in some cultures)
	Personnel no.
	Date of birth
	Employee ID (also known as Person type)
	Gender
	Company
	Title
	ID card no.
	Car license no.
Address	Zip code (called postal code in some cultures)
	Street, no.
	Country, state
	Nationality
Contact	Phone other
	Company phone
	Company fax
	Mobile phone
	Phone
	E-Mail
	Web page address
Additional Person Data	Patronymic (an additional name used in many cultures)
	Birthplace
	Marital status
	Official identity card
	Identity card no.
	Valid until
	Height

Additional Company Data	Department
	Location
	Cost center
	Job title
	Attendant (Escort)
	Reason for visit
	Remarks
Remarks	(Provides a free-form text field for notes and remarks about the person.)
Extra Info	10 user-definable fields
Signature	Capture, re-record and delete signatures
Fingerprints	Capture, re-record, delete, and test fingerprints as biometric credentials. Designate certain fingerprints to signal duress.

### 17.1.1 Card control / building control options

### 17.1.2 Extra info: Recording user-defined information

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

### 17.1.3 Recording signatures

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

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

#### Related procedures:

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

## 17.1.4

## Enrolling fingerprint data

Address Contact Additional person data Additional company data Remarks Card control Extra info Signature Fingerprints

172.30.11.50 51211 ✓

Enroll fingerprint

Match fingerprint

Delete fingerprint

Duress fingerprint

Identification mode

Fingerprint only

Card only

Card and fingerprint

Enrol finger 'Left index finger'

## Prerequisites

- One or more fingerprint readers must be configured at the entrances, in order to perform biometric access control.
- **IMPORTANT:** These readers periodically receive and store card and fingerprint data from the servers. The settings on the individual reader ultimately decide which credentials are accepted. They override any settings made here for the person.
- In order to use fingerprints as a verification for (or alternative to) card-based authentication, all cardholders must have their fingerprints scanned.
- The enrollee is in front of a fingerprint reader that is connected to and configured for your workstation.
- As the operator you are communicating directly with the enrollee, that is, with the person whose fingerprints are to be recorded as biometric credentials for access.
- You have familiarized yourself with how to present your finger repeatedly at the particular reader used, to allow it to capture fingerprints efficiently.

## Procedure for enrolling a fingerprint for access

1. Navigate to the fingerprints dialog: **Personnel data > Persons > tab:Fingerprints** and create or find the enrollee in the database.
2. Ask the enrollee which finger they wish to use for regular access at the fingerprint reader.
3. Select the corresponding finger in the hands diagram.  
Result: The fingertip is marked with a question mark.
4. Click the **Enroll fingerprint** button.
5. Give the enrollee instructions for presenting their finger at the reader.  
Example instructions can be read from the dialog pane below the hands diagram, but different reader types may require slightly different procedures.
6. If the fingerprint is successfully enrolled, a confirmation window will appear.
7. Select an **Identification mode**; this determines what credentials a fingerprint reader will demand of the enrollee when they request access. Note that the mode set here will only take effect if the reader parameter **Person-dependent verification** has been selected.  
The options are:
  - **Fingerprint only** - Only the fingerprint scanner in the reader is used

- **Card only** - Only the card scanner in the reader is used
- **Card and fingerprint** - both scanners in the reader are used. The enrollee will have to present both card and chosen finger at the reader, to obtain access.

8. Click  (Save) to store the fingerprint and identification mode for the enrollee.

**Notice!**

Reader settings override person settings

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

**Procedure for enrolling a fingerprint to signal duress****Prerequisites:**

- At least one fingerprint of the enrollee has already been successfully enrolled and stored.
  - The fingerprint reader is online. In offline mode the reader, of course, cannot send a duress signal to the system.
1. Ask the enrollee to choose a finger they wish to use to signal duress, that is, in case forced by an unauthorized person to use the fingerprint reader.
  2. Repeat the fingerprint enrollment procedure, described above, for that finger.
  3. When the second fingerprint is successfully enrolled, select it in the hands diagram and click the **Duress finger** button.

The designated duress finger is marked with an exclamation mark in the hands diagram. If the enrollee subsequently uses the duress finger at a fingerprint reader, and the reader is not offline, the system will signal duress to the operator, using a popup window.

**Procedure for testing stored fingerprints**

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

**Procedure for deleting stored fingerprints**

1. In the hands diagram, select the fingerprint you wish to delete.
2. Click the **Delete fingerprint** button
3. Await confirmation of the deletion.

## 17.2

### Companies

- This dialog can be used to create new companies and modify or delete existing company data.
- The company's name and short name must be entered. The short name must be unique.
- If the entry of a company is mandatory in the **Persons** dialog, create the company in this dialog before attempting to create personnel records for that company.

- Companies cannot be deleted from the system if personnel records are still assigned to them.

## 17.3 Cards: Creating and assigning credentials and permissions

The purpose of this dialog is to assign **cards**, **access authorizations**, or bundles of access authorizations called **access profiles** to personnel records.

Access authorizations and profiles are assigned to persons, not to cards.

New cards that are assigned to a person receive the access authorizations already assigned to that person.

### **Note: Using access profiles to bundle authorizations**

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

- Main menu: > **System data** > **Access profiles**

### **The card list**

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

- The card usage type.
- A flag whether the card can be used for a configured offline locking system.
- Whether the card is blocked due to the repeated use of invalid PINs. This state is specially highlighted.
- The creation date of the card
- An expiry date (Collecting date) of the card.

**Note:** If a motorized card reader is in use, it can physically withhold an expired card. Otherwise the card is simply invalidated.

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

### Option **Administered globally**

The data of persons who have the setting **Administered globally** (check box beside the photo frame) can be only be edited by operators who have the additional right **Global Administrator**.

The following data are read-only for operators who do not have this right:

- All data of the dialog **Persons**, except the tabs **Remarks**, **Extra info** and custom fields.
- All data of the dialog **Cards**.
- All data of the dialog **PIN Code**.

This **Global Administrator** right can be assigned in the in the following check box:

- Main menu: **Configuration** > **Operators and workstations** > **User rights** > check box: **Global Administrator**.

### 17.3.1 Assigning cards to persons

#### **Introduction**

A persons under access control requires a card or other electronic credential, which is assigned to its holder in the Cards dialog.

Card numbers can be assigned manually or automatically through an enrollment reader.



**Dialog path**

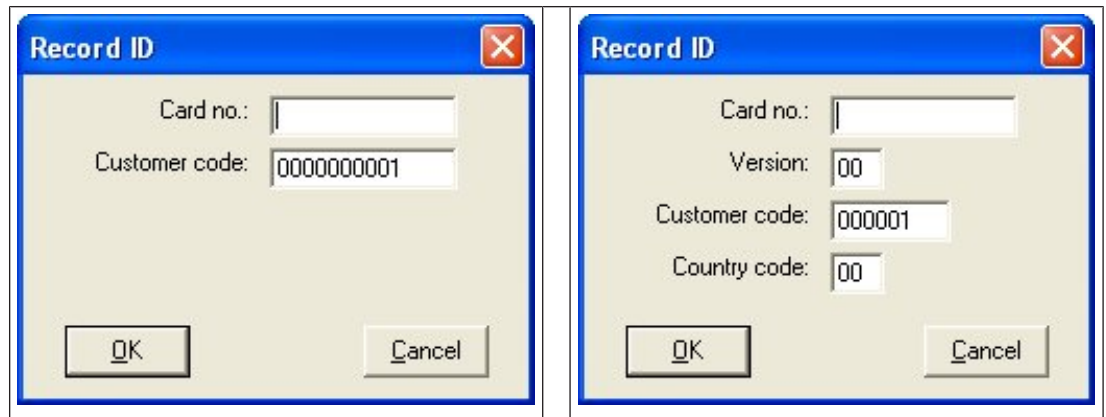
Main menu > **Personnel data** > **Cards**

**Prerequisite**

You have loaded the personnel record that is to receive the card in the header of the **Cards** dialog.

**Manual input of card data**

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




Manually enter the number printed on the ID card - card numbers are automatically padded with zeros so that they are always stored as 12 digits. In some systems, no new ID card numbers will be assigned if an ID card is lost. Instead, the same ID card number is issued, but with a higher version number. The country code and the customer code are provided by the manufacturer and must be entered in the registration file of the system.

If not already in use by the system, the card number is assigned to the person. Successful assignment is confirmed by a pop-up window.

**Using an enrollment reader****Prerequisite**

An enrollment reader has been connected to the workstation at which you are working.

**Procedure for enrollment**

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

**Procedure for changing cards**

1. Select a card from the list.
2. Click the **Change card** button
3. Edit the card data in the popup window and click OK to save.

**Deleting cards**

1. Select a card from the list.
2. Click the **Delete card** button to remove a person's assignment to a card.

**Note:** If you delete a cardholder's last card then the person's status changes to **unregistered** (red label next to **Registered** in status bar). That person is then longer subject to access control.

## 17.3.2

### Authorizations tab

#### Assigning authorizations bundled as Access profiles

The most convenient and flexible way to assign authorizations to cardholders is to bundle them first into Access profiles, and then assign the profile.

- For creating Access profiles see the section *Creating access profiles, page 135*
- To assign an Access profile to this cardholder, select a defined profile from the **Access profile:** list

#### Assigning access authorizations directly

On the **Authorizations** tab:

All access authorizations that have already been assigned to the person appear in the list on the left.

All access authorizations that are available for assignment appear in the list on the right. Select items and then click the buttons between the lists to move items from one list to the other.



assigns the selected item.



unassigns the selected item.



assigns all available items.



unassigns all assigned items.

#### Option: **Keep authorizations assigned**

The effect of assigning an access profile to a person depends on the check box **Keep authorizations assigned:**

- If the check box is cleared, any selection made before this and any access authorizations that have already been assigned are **replaced** when the profile is assigned.
- If the check box is selected, the authorizations of the profile are **added** to the assigned authorizations.

#### Limiting the time-span of authorizations

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

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

#### Displaying the entrances of an authorization

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

## 17.3.3

### Other data tab: Exemptions and special permissions

#### Assigning a time model:

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

#### **Excluding persons from random screening**

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

#### **Exclude persons from PIN-code checks**

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



#### **Notice!**

Exclusion from PIN-code checks affects the whole system.

For example, because the PIN codes of these persons are not checked, they will also be unable to arm or disarm alarms at entrances in door model 10.

#### **Extending the door opening time**

Select the check box **Extended door opening time** to give persons with disabilities triple the time to pass through an entrance before the state **Door open too long** is generated.

#### **Tour monitoring**

A **Tour** or **Route** is a strict sequence of readers that is defined in the Client menu:

**Tour monitoring > Define routes** dialog.

To assign a tour to a cardholder, select the **Tour monitoring** check box, and select a defined tour from the drop-down list. If no tours have been defined the check box will be inactive.

When assigned to a cardholder a **Tour** becomes activated as soon as the cardholder scans their card at the first reader in the sequence. After that all the readers in the sequence must be used in order, until the tour is completed. Typical uses are to enforce strict access sequences in industrial clean environments, hygienically controlled, or high-security areas.

#### **Permission to unlock doors**

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

## 17.3.4

### **Authorizing persons to set Office mode**

#### **Introduction**

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

Office mode is a typical requirement of retail, educational and medical facilities.

#### **Prerequisites**

For office mode to operate, the following requirements must be met:

#### **In the configuration (device tree)**

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

#### **In the client (Persons dialogs)**

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

### Procedures for authorizing persons to set office mode

#### Procedure for individual cardholders

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



3. Click the diskette icon to save the cardholder's data.

#### Procedure for groups of cardholders

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

### Instructing the cardholder how to start and stop office mode

To start or stop office mode at an entrance, the cardholder presses the number 3 on the keypad, and then presents their specially authorized card at the reader.

The entrance remains unlocked until an authorized cardholder presses 3 and presents the card again.

Note that guards with guard cards can stop office mode in the same way, without special permission.

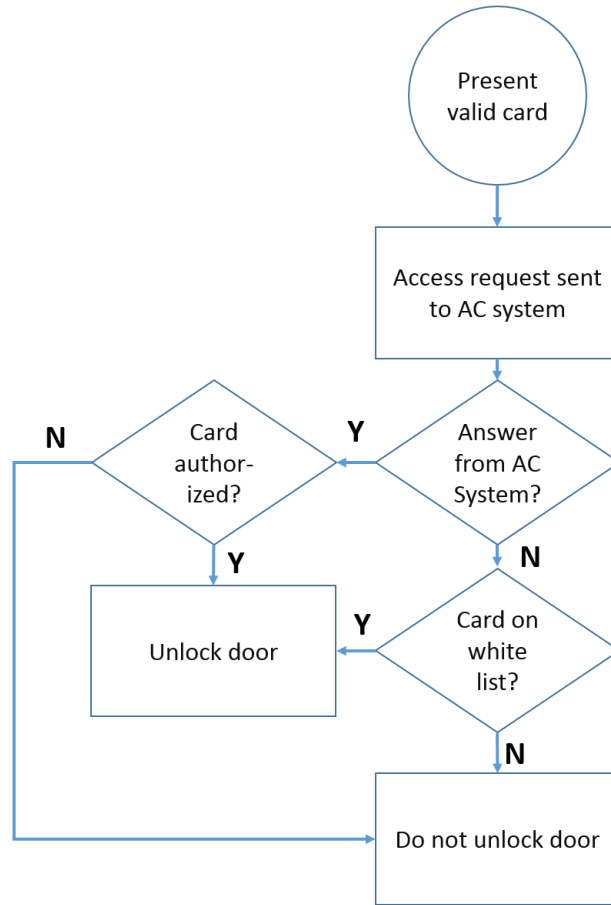
## 17.3.5

### SmartIntego tab

#### SmartIntego locking systems

##### Introduction

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



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

**Prerequisites**

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

**The assignment procedure**

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

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

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



assigns the selected item.



unassigns the selected item.



assigns all available items.



unassigns all assigned items.

## 17.3.6

### Creating an Alert card

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

#### Introduction

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

#### Prerequisites

- A dialog reader is installed on your system, for writing data to the card.
- At least one threat level has been defined in the system.

#### Dialog path

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

#### Procedure

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

## 17.4

### Temporary cards

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

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

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

#### Prerequisites

- The operator has access to an enrollment reader configured on their workstation.
- A suitable physical card is available for enrollment in the system as a temporary card.
- The recipient of the temporary card already has at least one other card.

**Main menu** > **Personnel data** > **Cards**

#### Procedure: Assigning temporary cards

1. Load the required personnel record into the **Cards** dialog
2. In the list of cards, select the card or cards that require a temporary replacement
3. Click **Change card**

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

#### Procedure: Deleting temporary cards

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

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

#### Procedure: Removing temporary blocks on cards

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

1. Navigate to the **Blocking** dialog: **Personnel data > Blocking**.
2. In the list of cards, select the personal card marked as blocked in the **Lock(s)** column.
3. Click **Release temporary lock**  
Note that the record in the **Blocking** list remains. The list contains only a history of all blocks for the current personnel record, past and present.

#### Notes on temporary cards

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

## 17.5 PIN codes for personnel

### Dialog: PIN-Code

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

If a PIN code is blocked or has expired, access to the area requiring the code is denied, even if the ID card is still valid for all other areas.

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

The screenshot displays the 'PIN-Code' dialog box. On the left is a navigation menu with options: Main menu, Persons, Companies, Print badges, Cards, PIN code (selected), and Blocking. The main area contains the following fields:

- Name: Mustermann
- First name: Max
- Birth name: [empty]
- Personnel no.: Sc999000
- Employee ID: Employee
- Company: Test\_Firma
- Car license No.: Car000998
- Date of birth: Tu 08/09/1988
- Gender: Male
- Title: Dr
- Card no.: [empty]
- PIN code: [masked with 6 red dots]
- Confirm: [masked with 6 red dots]
- Valid until: Mo 01/21/2013

On the right side, there is a photo of a man, the date 10/20/2014, and a checkbox labeled 'Administered globally'.

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

### Notice!

How cardholders enter identification PINs at card readers depends the kind of readers configured in your system. For example:

At RS485 card readers the cardholder enters: **4 #** <the PIN>

At Wiegand and other card readers the cardholder enters: <the PIN> **#**

Be sure to inform cardholders how to enter their PINs. If in doubt, consult your system administrator.

### PIN-Code for arming intrusion detection systems (IDS)

Input of a 4 to 8 digit PIN (default = 6 - the same length as the verification PIN). This PIN will be used to arm an IDS.

The display of this fields can be parametrized. Only if the control **separate IDS PIN** is activated the control are available.

– Main menu > **Configuration** > **Options** > **PIN codes**

Select an expiration date if required.



If the input fields to enter the IDS PIN are not available, the verification PIN can be used to arm and disarm the IDS too. But, if the input fields are shown in this dialog, the arming PIN can be used for IDS, only.

Default setting: The input fields for the PIN Code Arming are invisible.

### Alarm (Duress) PINs

Persons under duress may trigger a silent alarm via a special PIN code. Because the silent alarm needs to remain unnoticed by the aggressor, access is granted, but the system operators are alerted to the duress.

Two variants are available which are activated at the same time and the person being threatened can choose between them:

- Inputting the PIN code in reverse order (321321 instead of 123123).
- Incrementing the PIN by 1 (for example: 123124 instead of 123123). Note that if the last digit is 9 then the PIN is still incremented, so PIN 123129 would have a duress PIN of 123130.

## 17.6 Blocking access for personnel

### Dialog: Blocking

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

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

The screenshot shows the 'Blocking' dialog in the software. On the left is a navigation menu with options like 'Persons', 'Companies', 'Print badges', 'Cards', 'PIN code', 'Blocking', 'Blacklist', 'Group of persons', 'Group authorizations', and 'Areas'. The main area displays the profile of 'Musterfrau', Anita, with fields for birth name, personnel number (SC41156), employee ID, company (Test\_Firma), car license number, and card number (000000101234). A 'Reader...' button is next to the card number. A table below shows card details:

Card no.	Application type	PIN lock	Created on	Last printed on	No. of prints	Code data
000000101234	Personal card		10/21/2014 02:57:22 PM		0	Customer code:150, Badge no.:101234, Version:4, Country c

Below the table is a 'Release PIN lock' button. At the bottom, there is a 'Blocking' table with columns: 'Blocked from', 'Blocked until', 'Blocking reason', and 'Last edited by'. Below this table are 'New', 'Change', and 'Delete' buttons.

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

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

**Notice!**

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

## 17.7

### Blacklisting cards

**Dialog: Blacklist**

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

Note that the credential is blacklisted, not the person.

**Notice!**

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

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

Division: Common

< Main menu

Persons

Companies

Print badges

Cards

PIN code

Blocking

**Blacklist**

Group of persons

Name:

Birth name:

Personnel no.:

Employee ID:

Company:

Car license No.:

Card no.:

First name:

Date of birth:

Gender:

Title:

10/20/2014

Card no.	Application type	PIN lock	Created on	Last printed on	No. of prints	Code data

Reason:

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

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

The card is blacklisted with immediate effect.



#### **Notice!**

Blacklisting affects cards, **not** cardholders.

Non-blacklisted cards belonging to the same cardholder are not blocked.

## 17.8 Editing multiple persons simultaneously

### Group of Persons

Employee ID:

Name:  until starting with:

First name:  until starting with:

Personnel number:  until starting with:

Company:  until starting with:

Card:  until starting with:

Valid on:

Gender:

Department:

Cost center:

Number of records found: 2  Show all

Name	First name	Gender	Pers. number	Location	Cost unit	Job title	Company	Department	Card number	Time model	Valid from	Valid until
Musterfrau	Anja	Female	SC41156				Test_Firma					
Mustermann	Max	Male	Sc999000			Software-Entwickler	Test_Firma					

Wanted field to change:

Wanted action:

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

After the group of persons has been selected the following entries can be selected:

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

Then the modification option can be selected:

- Field to be changed
- Desired action
- Old value
- New value.

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

### Group Authorization

In the menu item **[Group Authorization]** the following search criteria are supported:

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

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

authorizations assigned with “Yes” are added to all selected persons, or withdrawn, respectively. All other authorizations for the persons remain unchanged, as usually the selected persons don’t have completely identical authorizations.

## 18 Defining access authorizations and profiles

### 18.1 Creating access authorizations


#### Dialog path

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

#### Procedure

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

Alternatively, click **Copy**  to create a new authorization based on an existing one.

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

#### Notice!

Subsequent changes to authorizations will affect existing assignees, unless the governing profile is locked.

**Example:** If an Inactivity limit of 60 days is reduced to 14 days, then the authorization will be lost to all persons who have not used that authorization in the past 14 days.

**Exception:** If an authorization is part of an access profile that is **locked** to an Employee ID (Person type), then persons of that type are not affected by inactivity limits on the authorization. Profile locks can be set with the following check box.

Main menu > **System data** > **Person Types** > table: **Predefined Employee IDs** > check box: **Profile locked**



### 18.2 Creating access profiles

#### Note: Using access profiles to bundle authorizations






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

- Main menu: > **System data** > **Access profiles**

### Prerequisites

Access Authorizations have already been defined in the system.

### Procedure

1. Clear the input fields by clicking **New**  in the toolbar.  
  
Alternatively, click **Copy**  to create a new profile based on an existing one.
2. Enter a unique name for the profile
3. (Optional) Enter a description
4. (Optional) Select the check box **Visitor profile** to limit this profile to visitors
5. (Optional) Set a value for **Standard duration of validity**.
  - If no value is set, then the profile will remain assigned indefinitely.
  - If a value is set, then it will be used to calculate the expiry date of any later assignment of the profile.
6. (Mandatory) Assign at least one **Authorization**:  
Authorizations that are available for assignment are listed on the right.  
Authorizations that are already assigned are listed on the left.  
Select items and then click the buttons between the lists to move items from one list to the other.
  -  assigns the selected item.
  -  unassigns the selected item.
7. Click save  to save the profile.



## 19 Managing visitors

Visitors have a special status in access control and are kept separate from other personnel data. For this reason, visitor data is created and maintained in separate dialogs.

### 19.1 Visitor data

#### Introduction

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

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

There are two dialogs for the administration of external visitors.

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

#### Dialog: Visitors

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

Among other things, there is no **Employee ID** input field in the **Visitors** dialog. Since there is a separate database table for visitors, persons created in the dialog described here are automatically identified as visitors. This therefore means that no persons other than visitors can be created here. Accordingly, selections are only made in this dialog in the relevant database table. In contrast, all persons registered on the system can be selected in the other personnel data dialogs, but may not always be able to be used for visitors (the **Cards** dialog). Where known, visitor data can be completely or partially entered in the system before the visitor arrives. This provides a minimum of waiting times for visitors whose data have already been recorded.

Division: Common

« Main menu

Visitor

Visitor cards

Last name:

Birth name:

Street, no.:

Phone:

Car license No.:

Employee ID: Visitor

First name:

Date of birth:

Zip code / City:

Company:

Official pass

Passport

Driver's licence

Identity card

Other:

Number:

Card no.:  Reader.. ▶

Additional data Authorizations Form/Photo Signature

Attendant:  ...

Remark:

Expected arrival:

Date of arrival:

Visited person:  ...

Location:

Reason:

Expected departure:

Date of departure:

Extended door opening time

Card no.	Application type	PIN lock	Collecting date	Code data

Read card ... ▶  
Withdraw card

The **Reason** of the visit, the **Location** the visitor visits and a **Remark** may be entered in the input fields below.

If you choose to enter data in the **expected arrival** and **expected departure** fields, these dates will then also appear in the **valid from** and **until** fields.

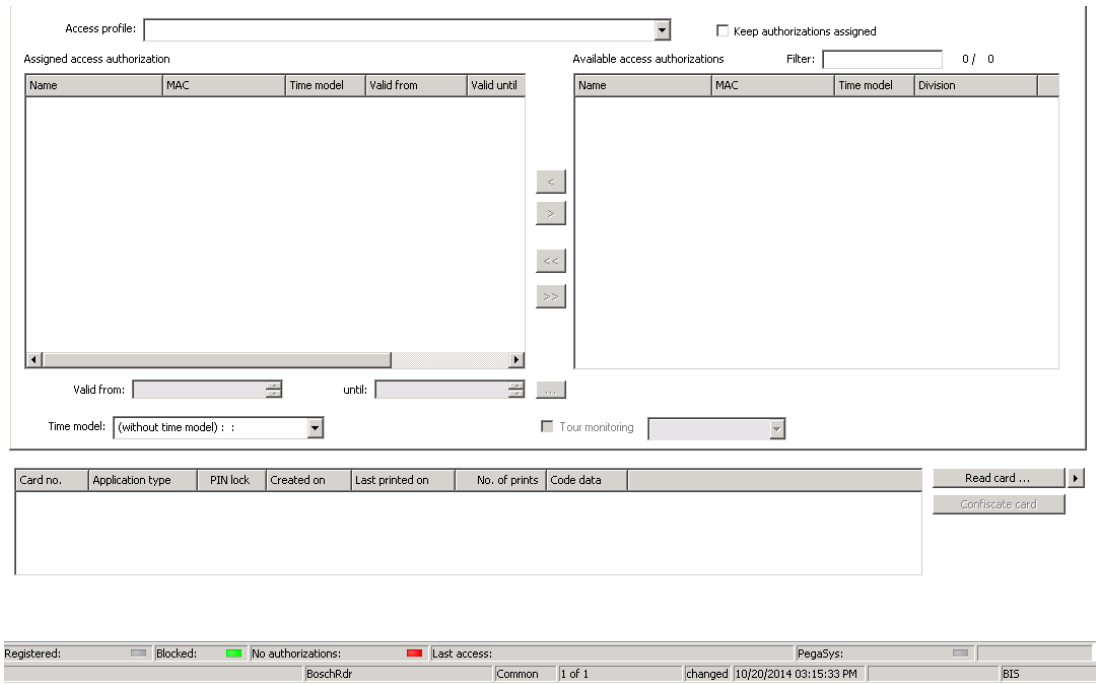
The relevant dates are entered in the **Date of arrival** and **Date of departure** fields by the system when visitor data is respectively assigned to and separated from a visitor ID card.

As with the **Cards** dialog, there is also the possibility of assigning visitors "extended door opening times" to ensure easier access, e.g. for disabled persons.

2019-08 | 2.0 |

Software Manual

Bosch Security Systems



In the **Assign authorization** dialog field an existing visitor profile can be selected in the homonymous selective list, or single access authorizations from the **Available access authorization** list can be selected in the **Assigned access authorization** list on the left by marking and transferring them from the right list.

Only Access profiles which are marked as Visitor profiles can be selected in this dialog. Thereby it shall be avoided that visitors get access to special areas by the allocation of general authorizations.

The validation of access authorizations can also be set for each authorization by themselves. If the card reading has got an error, the ID card number may also be given manually. The current date is stored as arrival date simultaneously.

After the visit the visitor returns his ID card. While this ID card is read in a card reader or the ID card number is entered manually, the associated person is selected and his data are displayed on the screen.

The operator confirms the return of the card. The association between the ID card and the visitor is removed by clicking the **Confiscate card** button. The date and time of this action are stored as departure date.

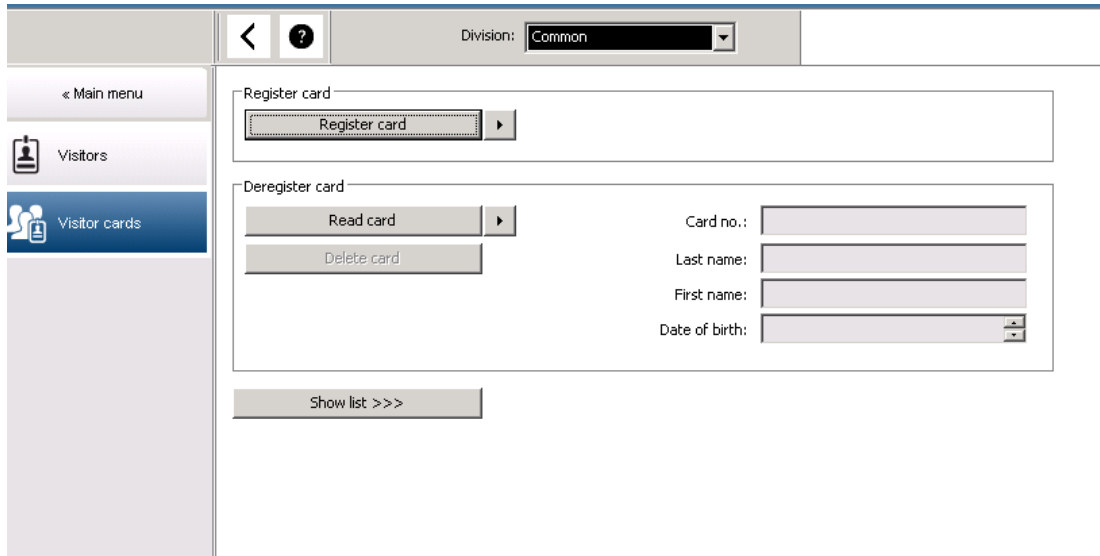
**Dialog: Visitor Cards**

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



**Notice!**

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



Click **Register ID card** button for the registration.

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



Card no.	In use	Name	First name	Usage type	Division	

To make the assignment of visitor ID cards quicker, it is advisable to scan all existing ID cards, so that these cards can be assigned to the respective visitors in the next dialog.

At the end of the visit, the visitor returns the ID card. By scanning this ID card at a dialog reader or by entering the ID card number, the person to whom the card is assigned is selected and this person’s data is displayed on the screen. [For inputting the ID card number manually and switching to the use of readers, please see the descriptions in the **Dialog: Cards** and **Dialog: Visitors.**] The user confirms the return of the ID card. The connection between the ID card and the personnel data of the visitor is removed using the button. The current date is stored as the departure date.

### Printing a Visitor form



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

<b>Visitor pass</b>	
Entry	Exit
First- and lastname Steven Visitor	Company _____
<input type="checkbox"/> Proof of authority for plant area	Registration plate _____
Passed card	
Contact person	Phone      Department
Reason of visit	Visit appointment <input type="checkbox"/> Yes <input type="checkbox"/> No
Type of official Passport	Number of official document
I accept the terms and conditions overleaf  <div style="display: flex; justify-content: space-between; width: 100%;"> <span>_____</span> <span>_____</span> </div> <div style="display: flex; justify-content: space-between; width: 100%; font-size: small;"> <span>Location, date</span> <span>Sign of visitor</span> </div>	
Identify card with photo seen ?  <input type="checkbox"/> Yes <input type="checkbox"/> No  _____ Sign of plant protective force	To complete from visited person  Arrival    at _____ Departure at _____  _____ To sign on visited person

## 19.2 Visitor too late

The view **Visitor too late** enables the customer to check where visitors stay within the location, and if they have possibly exceeded the expected time of departure.

The authorized BIS users need to have a link configured on their start screen so that they can view this website.

In addition it is possible to configure a trigger in the BIS to the DMS device so that in case of a Visitor too late message an alarm can be activated, which in turn opens the website and display only the respective person with the last known whereabouts.

[see screen website]

### Events that lead to the message Visitor too late:

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

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

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

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



### Notice!

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

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

It is checked:

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

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

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

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

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

Filter		Vehicle search: <input type="text" value="AC"/>		Refresh (in 10s)	
<input checked="" type="checkbox"/> Show returned	<input type="checkbox"/> Too late only	<input type="checkbox"/>	<input checked="" type="checkbox"/> No date		
Fritz	Mustermann	Arr. 15.07.2014 08:21:00'000	Dep. 10:22:00 exp.	Vehicle	Zone A
	over 1 d/23h 58'31	Dur. 1 d/23h 59'31		Last area	
Test Visitor	Test Visitor	Arr. 16.07.2014 14:55:00'000	Dep. 09:04:54	Vehicle	AUSSEN
	departed 15h 04'54 16.07.2014	Dur. 16h 09'54		Last area	
Malmendier	Walter	Arr. 16.07.2014 14:52:00'000	Dep. 00:00:00 exp.	Vehicle	AC-WM-1234
	over 10h 20'31	Dur. 17h 28'31		Last area	
Cibis	Roman	Arr. 16.07.2014 14:53:00'000	Dep. 02:00:00 exp.	Vehicle	AC-CC-1010
	over 8h 20'31	Dur. 17h 27'31		Last area	
Nettelbeck	Ulrike	Arr. 17.07.2014 07:39:00'000	Dep. 00:00:00 exp.	Vehicle	AC-UN-4646
	still 13h 39'28	Dur. 41'31		Last area	

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

## 20

### 20.1

## Managing parking lots

### Authorizations for several park zones

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

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



#### Notice!

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

A person who has several authorizations can access both, if handicapped or not. The AMC tries to book in the person in according to the configured sequential order of parking zones. In case one zone is full, the search for the next authorized and free zone will proceed.

Counter calculation in MAC and AMC:

1) One AMC controls all entrances and exits of a car park:

=> The AMC counts on its own and can be corrected by the MAC when going online.

2) Entrances and exits of one car park are divided up onto different AMCs:

=> The MAC counts for the AMC in case of online operation. When operating offline, the AMCs permit the access (if configured accordingly) but don't count.

If several AMCs control one car park, activate the checkbox **No AMC accounting**.in the AMC configuration



AMC 4-W | Inputs | Outputs | Terminals

Name: AMC 4-W-1

Description: AMC

Communication to host enabled:

Controller interface

Interface type: UDP

PC com port: 0

Bus number: 1

IP address / host name:

Port number: 10001

Program: LCMV3732.RUN : WIE, AMC-4W

Power supply supervision:

No LAC accounting:

Division: Common

## 20.2 Parking lot report

Parking lot list			Date 08.11.2013 , 14:51:23
			Page 1
Parking area	Zone	Vehicle count	State
<b>Main Park</b>		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
<b>Building A</b>		39	
	Zone A	30	full
	Zone B	9	--
<b>Building B</b>		39	
	Zone A	30	full
	Zone B	9	--

## 20.3 Extended Car Park management

### Introduction

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

- Trucks

- Handicapped access
- Motorcycles

### Dialog path

**Main menu > System data > Areas**

### Procedure

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

The screenshot displays the 'Areas' configuration page in the Access Management System. The interface includes a top navigation bar with a search icon, navigation arrows, and a 'Division' dropdown menu set to 'Common'. A left sidebar contains menu items: « Main menu, Authorizations, Access profiles, Areas (highlighted), Reset areas unknown, and Random screening. The main content area is divided into two sections: 'Access control area' and 'Parking areas'.

**Access control area**

Area name:

Description:

max. number of cars:       Number of subareas:

Buttons: Refresh number, Synchronize counter, Parking time check

**Parking areas**

Subarea	Description	Max	Actual	Info
Parking_01		4		
Parking_02		6		
Parking_03		8		

# 21 Managing guard tours and patrols

## Introduction to Guard tours

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

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

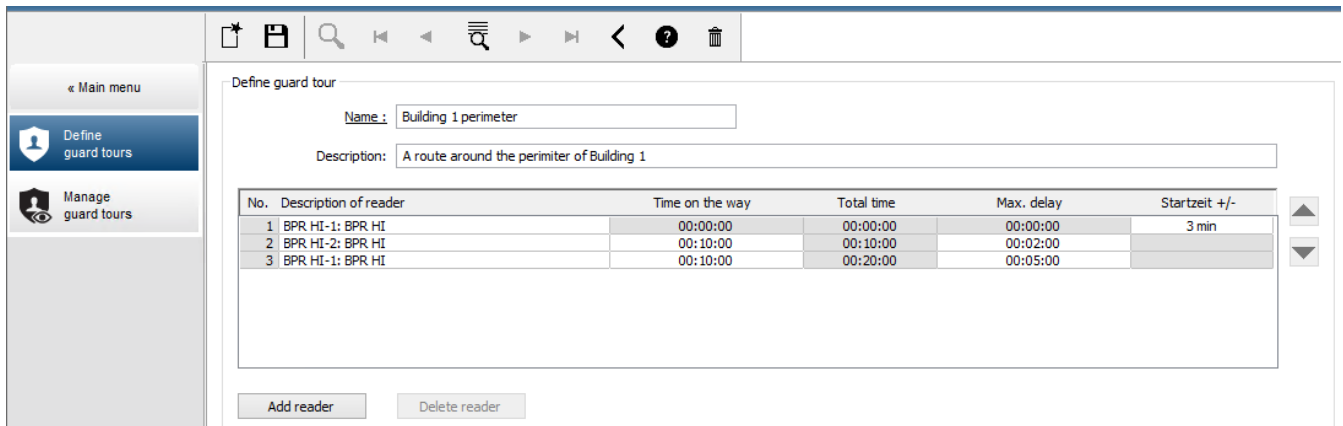
The Guard tour consists of a series of readers with the approximate walking times in between. The maximum tolerable delay between readers, and the tolerable deviation (+/-) from the start time, are also attributes of the Guard tour. Deviations outside of these defined tolerances can potentially trigger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

## Introduction to Patrols

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

## 21.1 Defining guard tours

Select **Guard tours > Define guard tours**



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

### Adding readers to the guard tour:

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

4. Under **Max. delay** enter the maximum amount of additional **Time on the way** that is still tolerable without causing a patrol to be marked **Delayed**.
5. Add as many readers as required. Note that the same reader can occur more than once if the guard tour passes it multiple times, or returns to it.
  - To delete a reader from the sequence, select the line and click the **Delete reader** button.
  - To change the position of a reader in the sequence, select the line and click the up/down



buttons.

## 21.2

### Managing patrols

Select **Guard tours > Manage guard tours**

#### Scheduling a new patrol

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

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


#### Tracking a patrol


All planned and active patrols move to the top of the list. If multiple patrols are planned or active, the selected patrol is framed in red. Click on the frame to get further information.


A patrol starts when the guard presents his guard card at the first reader in the guard tour.

This card must be used for the rest of the patrol, even if alternative cards were defined for the patrol.

The **State** of the patrol changes to **Active**.

Every reader that is reached on schedule receives a green check mark - . The scheduled and actual times between readers in the currently selected patrol are displayed in the lower half of the dialog window.

Every reader that is reached later than the scheduled time plus **Max. delay** receives a red  mark. The patrol is marked as **Delayed**.

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

## 21.3 Tour monitoring (formerly path control)

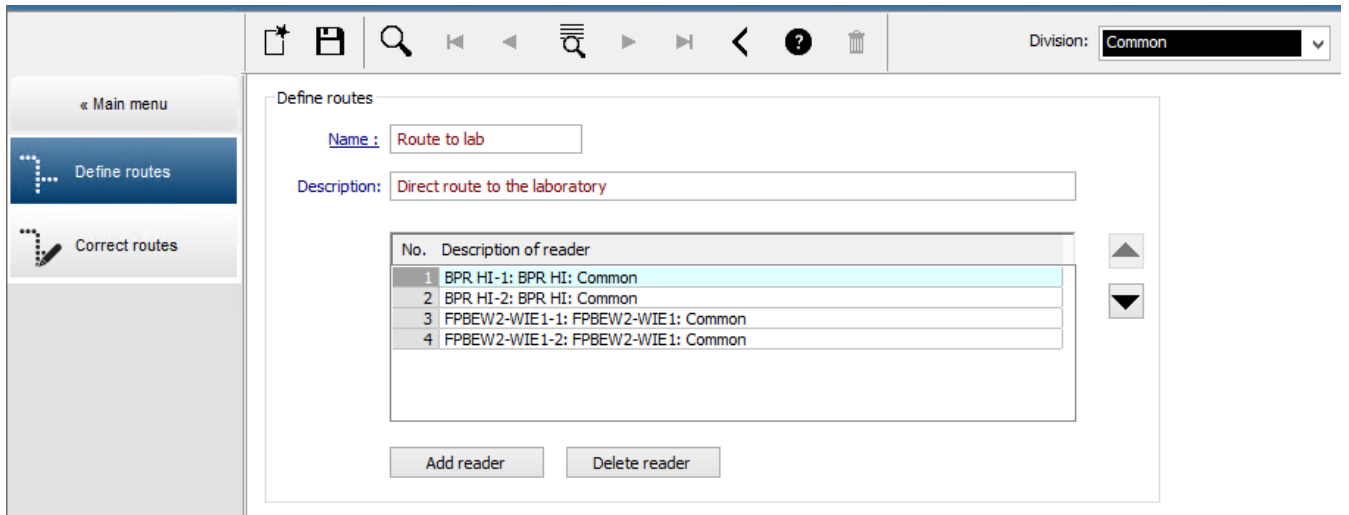
### Introduction

A Route (or Tour) is a predefined sequence of readers that can be imposed on Persons defined in the access control system, to direct their movements on the premises, regardless of the person’s authorizations.

Typical uses are to enforce strict access sequences in industrial clean environments, hygienically controlled, or high-security areas.

### Defining routes

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



### Assigning a route to a person


To assign a route to a person proceed as follows:

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

5. Save the personnel record.

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

#### **Correcting and monitoring routes**

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

## 22 Random screening of personnel

### The random screening process

1. A cardholder presents his card to a reader configured for random screening.

**Note**

Only persons authorized to pass through the entrance in the defined direction can be randomly selected. As authorizations are checked before random screening takes place any unauthorized person will immediately be barred, and will not be included in the selection process.

2. If the randomizer selects this person for screening his or her card will be blocked throughout the whole system.
  - The event is recorded in the system event log.
  - The **Blocking** dialog receives an entry of unlimited duration marked **Random screening**. [Figure below - number 1]
  - The status bar of the personnel data dialogs in Access Engine displays the "LEDs" Blocked (red) and with it Random screening (flashing violet).



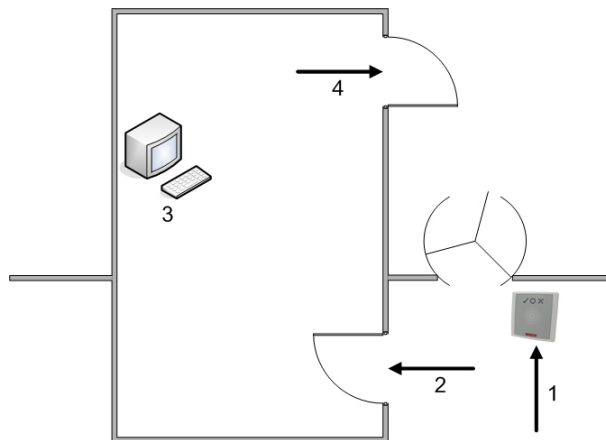
**Notice!**

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

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

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

### Example room layout for random screening



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



**Notice!**

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

---



## 23 Using the Event Viewer

### Introduction

The Event Viewer enables suitably authorized operators to examine events that were recorded by the system, and to produce reports, printed or on-screen.

To retrieve and display the desired records from the Event Log database, set filter criteria and

click **Refresh** .

Filter criteria can be set in different ways:

**Relative** To select events relative to the present time.

**Interval** To select events within a freely definable time interval

**Total** To select events irrespective of their time of occurrence





### Prerequisites

You are logged onto the dialog manager.

### Dialog path





Dialog manager main menu > **Reports** > **Event viewer**

### 23.1 Setting filter criteria for time relative to the present

1. Under **Time period**, select radio button **Relative**
2. In the box **Search within the last**, set the number time units to be searched, and choose which units to use, for example, weeks, days, hours, minutes, seconds.
3. In the **Event types** menu, select the category of events to be searched, and then the event types that interest you.
4. In the **Maximum number** menu, limit the number of events that the event viewer attempts to receive. For performance reasons it is **not** recommended to leave the value **(unlimited)**.
5. Specify other filter criteria that interest you:
  - Last name
  - First name
  - Personal number
  - Card number
  - User (that is, system operator)
  - Code data
  - Device name
  - Area name.
- Click **Refresh**  to start collecting events, and **Cancel** to stop.
- Click  to save the results, or  to print them.
- Click  to clear the results for another search.





### 23.2 Setting filter criteria for a time interval

1. Under **Time period**, select radio button **Interval**

2. In the date pickers **Time from**, **Time until** define the beginning and end of the period in which to search for events.
  3. In the **Event types** menu, select the category of events to be searched, and then the event types that interest you.
  4. In the **Maximum number** menu, limit the number of events that the event viewer attempts to receive. For performance reasons it is **not** recommended to leave the value **(unlimited)**.
  5. Specify other filter criteria that interest you:
    - Last name
    - First name
    - Personal number
    - Card number
    - User (that is, system operator)
    - Code data
    - Device name
    - Area name.
- Click **Refresh**  to start collecting events, and **Cancel** to stop.
  - Click  to save the results, or  to print them.
  - Click  to clear the results for another search.

## 23.3

### Setting filter criteria irrespective of time

1. Under **Time period**, select radio button: **Total**
  2. In the **Event types** menu, select the category of events to be searched, and then the event types that interest you.
  3. In the **Maximum number** menu, limit the number of events that the event viewer attempts to receive. For performance reasons it is **not** recommended to leave the value **(unlimited)**.
  4. Specify other filter criteria that interest you:
    - Last name
    - First name
    - Personal number
    - Card number
    - User (that is, system operator)
    - Code data
    - Device name
    - Area name.
- Click **Refresh**  to start collecting events, and **Cancel** to stop.
  - Click  to save the results, or  to print them.
  - Click  to clear the results for another search.


## 24 Using reports

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

### Dialog path



Main menu > **Reports**.




### Using the reports toolbar

Click  to display a preview before printing.

The preview has its own toolbar:



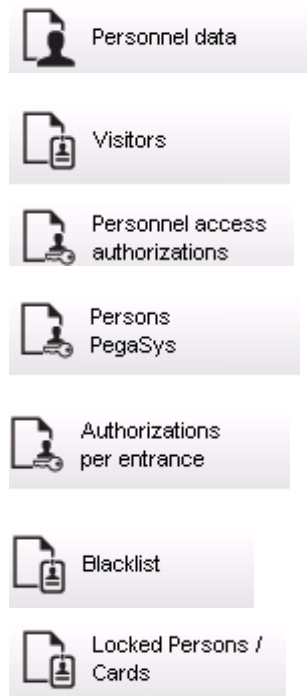
- Click **X** to exit the preview without printing.
- Use the arrow keys   in the preview toolbar to browse back and forth, or to select individual pages by page number.

- Click  to print immediately, using your default printer
- Click  to print via a Print Setup dialog, which allows further print options.
- Click  to export the report to a selection of file formats, including PDF, RTF and Excel.
- The numbers on the right of the toolbar represent:
  - The total number of existing database entries that correspond to the filter criteria.
  - The percentage of those database entries that are displayed in the preview.

### 24.1 Reports: master data

#### Reports overview - Master Data

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



**Report: Personnel Data**

Two filters can be applied when creating reports.

Person filter: Here, the operator filter based on the usual personnel data fields.

Access card filter: Here, the operator can filter based on the card numbers, ranges of numbers, the status, and the blocking status.

**Report: Visitors**

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

**Report: Personnel Access Authorizations**

This report gives an overview of the access authorizations registered on the system and also shows the persons to whom these authorizations have been assigned.

In terms of filters, personal data and the selection of certain authorizations can be used:

- Personnel data: Surname, first name, personnel no.
- Validation of all authorizations.
- The name of the authorization the entrance is included.
- The name of the time model - if exists.
- Direction for the entrance.
- Validation of the special authorization.

**Report: Blacklist**

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

**Report: Blocked Persons/Cards**

This dialog can be used to create reports containing data about all blocked persons.

Use dates to find blocks within specified time periods.

**Report: Device Data**

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

**Report: Companies**

The Companies report dialog is used to collate company data in a list.

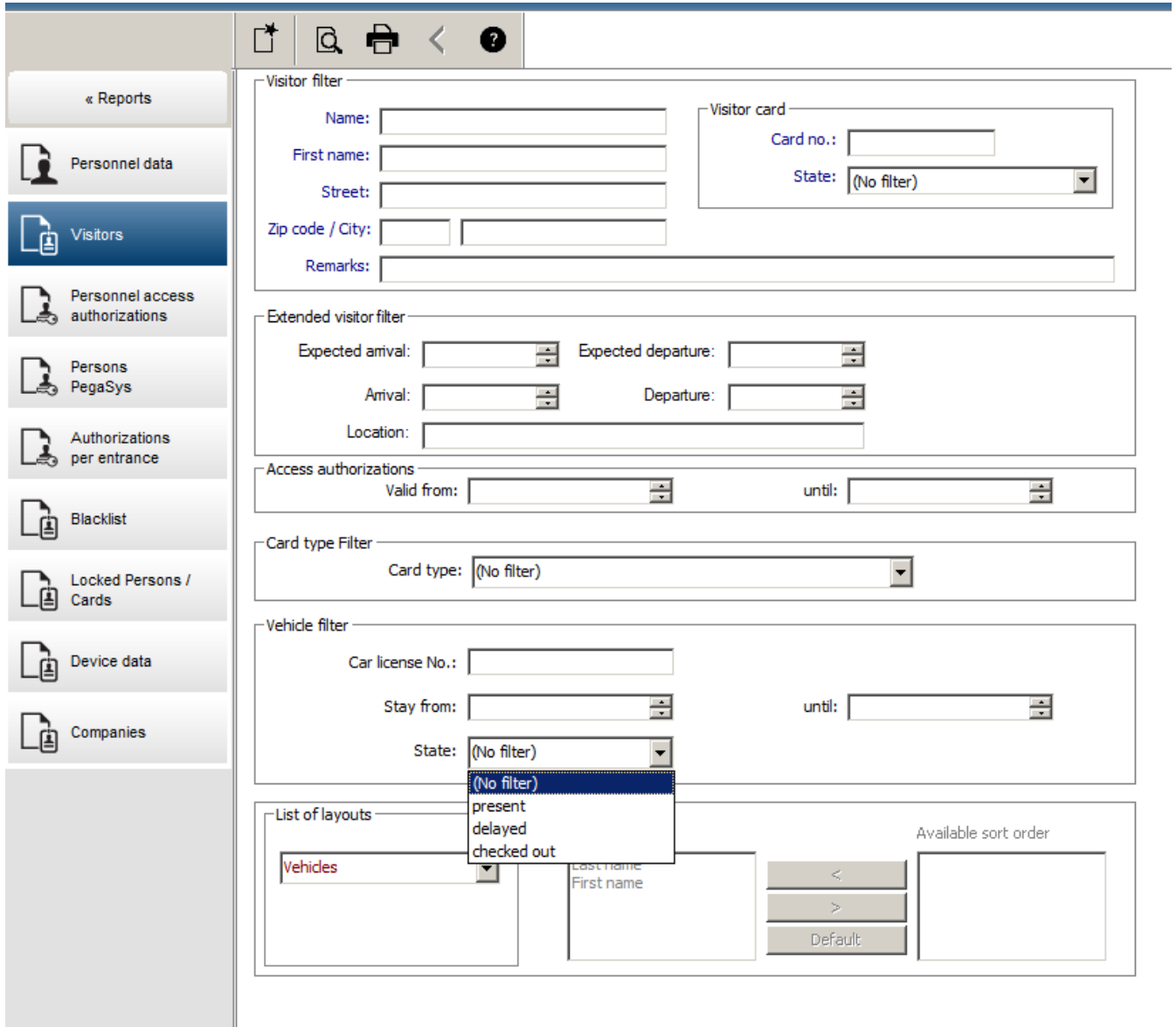
Use asterisks, for example, to find companies that begin with a certain letter.

### 24.1.1 Reporting on vehicles

In the dialog **Reports > Visitors** it is possible to select **Vehicles** from the layout list. Once **Vehicles** is selected the dialog area **Vehicle filter** is activated and can be used by the operator to filter out vehicles and their status.

The status is displayed as follows:

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



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

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

The duration will be calculated as follows:

- if the visitor already checked out, the difference between arrival and departure in minutes will be displayed.

- if the visitor has not checked out yet, the time from arrival in minutes until now will be displayed

## Access Engine

Vehicle Datum 02.07.2014 , 14:28:14  
Seite 1





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

## 24.2

### Reports: system data

#### Reports - System Data

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

-  Areas
-  Area configuration
-  Area muster list
-  Muster list total

#### Report: Areas

This dialog can be used to collate the locations in a report. The dialog contains only one area filter, which offers the various buildings and other zones for selection.

The area concerned is selected via a left mouse click. The user can view the report on the screen using the **Preview** button before he starts the printing process with **Print**.

There are two layouts available.

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

To check that the datasets displayed are up to date, the last card scannings for the areas are also listed.

Reliable information about the locations of persons can therefore be given for various events.

**Report: Areas Configuration**

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

**Report: Area Muster List**

As well as being listed according to purely numerical data, the persons in an area can also be listed by name.

With the scanning times for the individual areas, these reports also contain the times for each individual person.

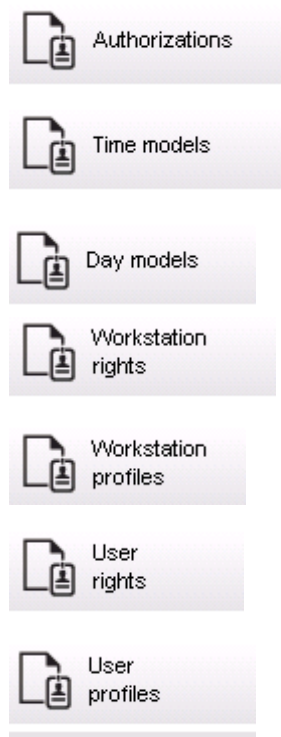
**Report: Muster List Total**

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

## 24.3 Reports: authorizations

**Overview**

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



**Report: Authorizations**

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

**Report: Time Models**

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

**Report: Day Models**

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

**Report: Workstation Rights**

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

**Report: Workstation Profiles**

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

**Report: User Rights**

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

**Report: User Profiles**

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



## 25 Operating Threat Level Management

This section describes the various ways to trigger a threat level and cancel it. For background information see section *Configuring Threat Level Management, page 108*

### Introduction

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

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

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

### Refer to

- *Configuring Threat Level Management, page 108*

### 25.1 Triggering and cancelling a threat alert via UI command

This section describes how to trigger a threat alert in AMS Map View.

#### Dialog path

- AMS Map view >  (Device tree)

#### Prerequisites

- At least one threat level has been defined
- At least one threat level has been marked with Active in the device editor.
- You as a Map View and AMS operator have the necessary permissions:
  - to operate Threat levels
  - to view the MAC or MACs in the Division where the threat alert is to be triggered.

#### Procedure to trigger a threat alert

1. In the device tree in AMS Map view, right click the MAC device where the threat alert is to be triggered.
  - A context menu appears, containing the commands that you are authorized to execute on that MAC
  - If no threat level is yet in operation, the menu will include one or more items labeled **Activate Threat level** '<name>', where is the name of the threat level defined in the device editor.
2. Select the threat level that you wish to trigger.
  - The threat level goes into operation.

#### Procedure to cancel a threat alert

Prerequisite: A threat level is already in operation.

1. In the device tree in AMS Map view, right click the MAC device where the threat alert is to be cancelled.
  - A context menu appears, containing the commands that you are authorized to execute on that MAC
2. Select **Deactivate Threat level**. From the context menu.
  - The currently threat level is deactivated.

## 25.2 Triggering a threat alert via hardware signal

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

### Prerequisites

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

### Procedure

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

**Threat level: Deactivate.**

### Refer to

- *Assigning a threat level to a hardware signal, page 112*

## 25.3 Triggering a threat alert via Alert card

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

### Prerequisites

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

### Procedure

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

### Refer to

- *Creating an Alert card, page 126*

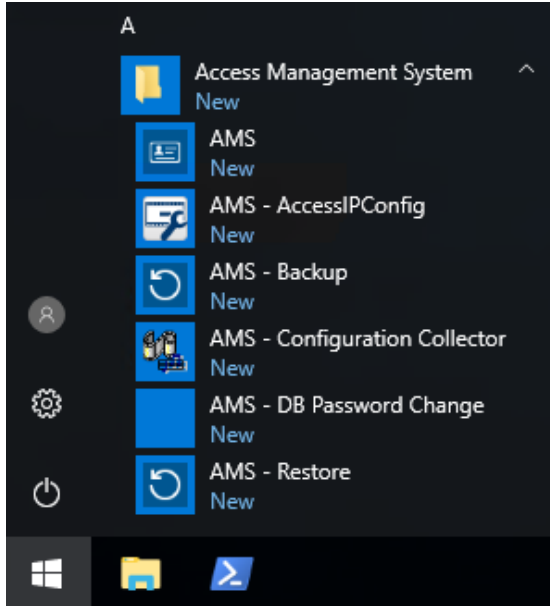
## 26 Backup and Restore

The **Backup & Restore** function enables you to reconstruct your installation on a different computer if the original computer fails.

**Backup and Restore** can only be started on the machine where the AMS server is installed.

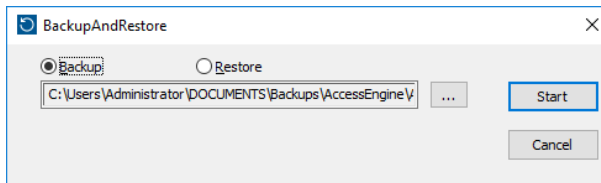
For convenience, two shortcuts are created:

- **AMS - Backup** for creating a backup
- **AMS - Restore** for restoring a backup:

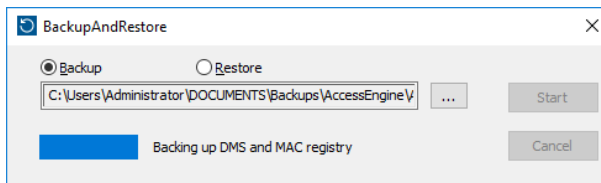


### 26.1 Backup procedure

1. Click the shortcut **AMS - Backup**.  
This will launch the **Backup and Restore** tool:

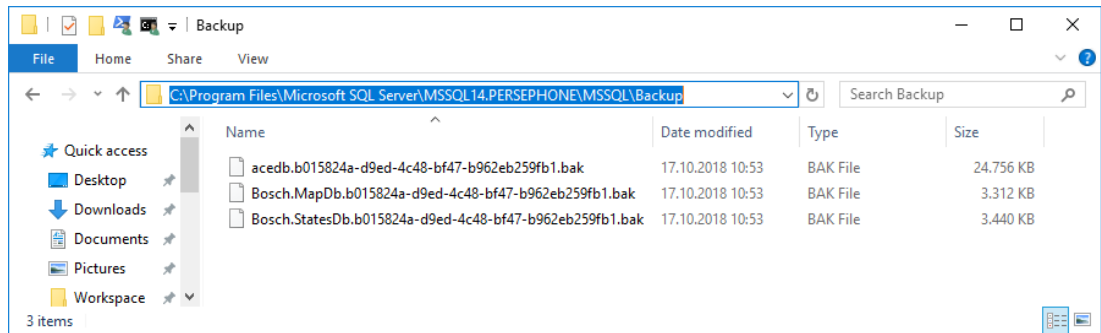


2. Enter a path where the GZIP file is to be saved.
3. Click **Start** to start the backup.  
A progress bar will be shown.  
Once it is completed the GZIP file will be created.



The location of the database backup depends on the version of SQL Server, and the name of the database instance.

For example, if the AMS SQL Server instance name is “PERSEPHONE”, the backup will be located in:



**IMPORTANT:** For data security, Bosch urgently recommends that you copy this folder and the GZIP file to a secure, remote location. Do not leave the only backup copy on the DMS server computer.



### Notice!

The event log is saved under the following default path (your installer may have chosen a different path):

C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\

## 26.2

### Restore procedure

#### Prerequisites

- The GZIP file that was created by the **Backup and Restore** tool
- The backup data created by SQL Server in the SQL Server backup folder.
- An SQL account with **sysadmin** rights, such as `sa`.

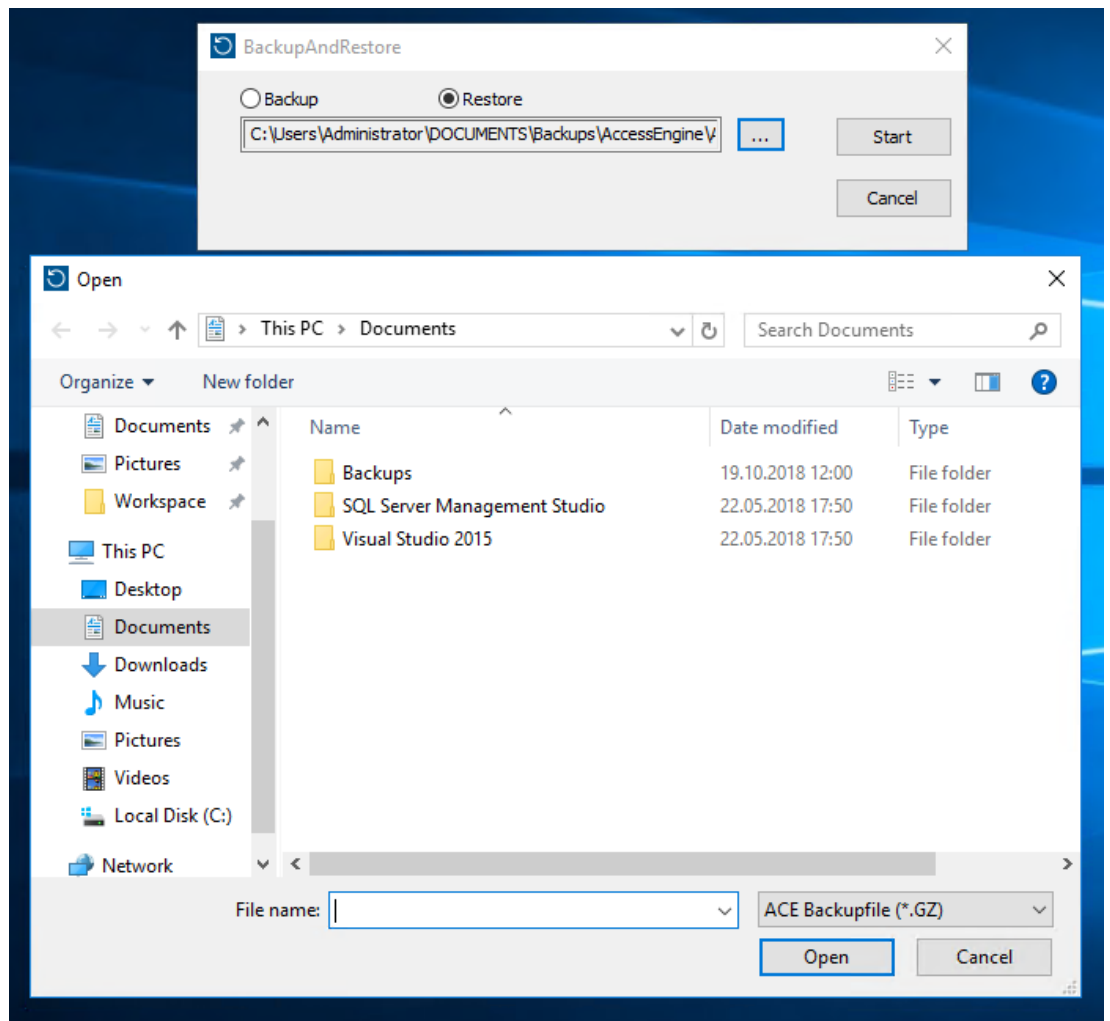
#### Notes on the target computer

- In order to run the restored configuration, the target computer (where you restore the backup) will require at least equivalent licenses to those on the computer where the backup was made.
- Any clients of the target computer will require the certificates generated by the installation on the target computer, not those generated by the installation on the original computer.

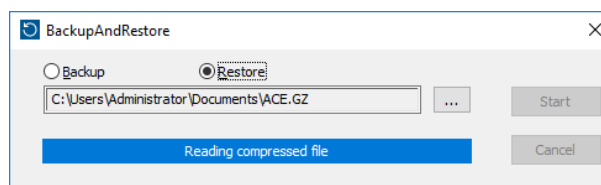
See the installation guide for installation of client certificates.

#### Procedure

1. In the AMS program click **File > Exit** to stop all running services.
2. When the program has terminated, run the Windows **Services** application and check that all *Access Engine* and *Access Management System* services have stopped.
3. Click Windows Start > **AMS - Restore**
4. Click the **[...]** button to locate and select the GZIP backup file.



5. Click **Start** to start the restore process.
6. Enter the **SQL sysadmin** login credentials.  
The restore process begins



7. When the restore process is completed, run the Windows **Services** application and check that all **Access Engine** and **Access Management System** services have restarted. If not, restart them manually.
8. Start **AMS Map View** from the desktop.
9. Locate and right click the MAC in Map View.
10. Execute the server setup program `AMS Server Setup.exe` as Administrator in order to resynchronize the data from the backup with the current system data.

# Glossary

## 1. MAC (first MAC)

The primary MAC (Master Access Controller) in a BIS Access Engine (ACE) or Access Manager (AMS) system. It can reside on the same computer as the DMS, but it can also reside, like a subsidiary MAC, on a separate computer known as a MAC server.

## Access Sequence Monitoring

The tracking of a person or vehicle from one defined Area to another by recording each scan of the ID card, and granting access only from Areas where the card has already been scanned.

## anti-passback

A simple form of Access Sequence Monitoring in which a cardholder is prevented from entering an Area twice within a defined time period, unless the card has been scanned to exit that Area in the meantime. Anti-passback deters a person from passing credentials back through an entrance for use by an unauthorized second person.

## Assembly point

a designated place where people are instructed to wait after evacuating a building.

## Automated number-plate recognition (ANPR)

The use of video technology to read and process number plates, typically of road vehicles.

## Data Management System (DMS)

A top-level process for managing access control data in Access Engine. The DMS supplies data to main access controllers (MAC), which in turn supply data to local access controllers (usually AMC).

## Data Management System (DMS)

A top-level process for managing access control data in Access Engine. The DMS supplies data to MACs, which in turn supply data to AMCs.

## Door model

A stored software template of a particular type of entrance. Door models facilitate the definition of entrances in access control systems.

## Entrance

The term Entrance denotes in its entirety the access control mechanism at an entry point: It includes the readers, some form of lockable

barrier and an access procedure as defined by sequences of electronic signals passed between the hardware elements.

## IDS

Intruder detection system, also known as a burglar alarm system.

## Local Access Controller (LAC)

A hardware device that sends access commands to peripheral access control hardware, such as readers and locks, and processes requests from that hardware for the overall access control system. The most common LAC is an Access Modular Controller or AMC.

## MAC (Main Access Controller)

In access control systems a server program that coordinates and controls the Local Access Controllers, usually AMCs (Access Modular Controller)

## Normal mode

In contrast to office mode, normal mode grants access only to persons who present valid credentials at the reader.

## Office mode

The suspension of access control at an entrance during office or business hours.

## Identification PIN

A Personal Identification Number (PIN) that is the sole credential required for access.

## Verification PIN

A Personal Identification Number (PIN) used in combination with a physical credential to enforce greater security.

## RMAC

A redundant main access controller (MAC) that is a synchronized twin of an existing MAC, and takes over management of its data if the first MAC fails or gets disconnected.

## MAC server

Hardware: A computer (other than the DMS server) in an Access Engine (ACE) or Access Management (AMS) System, where a MAC or an RMAC runs.

---

**SmartIntego**

---

A digital locking system from Simons Voss technologies. SmartIntego is integrated with some Bosch access control systems.

**tailgating**

---

Circumventing access control by closely following an authorized cardholder through an entrance without presenting one's own credentials.

**Threat alert**

---

an alarm that triggers a threat level. Suitably authorized persons can trigger a threat alert with a momentary action, for example through the operator's UI, through a hardware signal (e.g. push button), or by presenting a special alarm card at any reader.

**Whitelist (SmartIntego)**

---

A whitelist is a list of card numbers that is stored locally on the card readers of a SmartIntego locking system. If the reader's MAC is offline, the reader grants access for cards whose numbers are contained in its local whitelist.









**Bosch Security Systems B.V.**

Torenallee 49

5617 BA Eindhoven

Netherlands

**[www.boschsecurity.com](http://www.boschsecurity.com)**

© Bosch Security Systems B.V., 2020