



BOSCH

Access Managment System V5.5

Configuration and Operation

Table of contents

1	Security	7
2	Using Help	8
3	About this documentation	10
4	AMS System overview	11
5	Licensing the system	12
6	Configuring the calendar	13
6.1	Defining Special days	13
6.2	Defining Day models	15
6.3	Defining Time models	16
7	Configuring Divisions	19
7.1	Assigning Divisions to devices	20
7.2	Assigning Divisions to operators	20
8	Configuring the IP addresses	21
9	Using the Device Editor	22
9.1	Configuration modes and overrides	23
10	Configuring areas of access control	24
10.1	Configuring areas for vehicles	25
11	Configuring intrusion areas and panels	27
11.1	Installing the Intrusion RPS API on the RPS computer	28
11.2	Connecting the access control system to the intrusion panels	29
11.2.1	Step 1: Defining the connection to the RPS API	29
11.2.2	Step 2: Configuring the panel connections	29
11.3	Creating authorization profiles for panels	30
11.4	Assigning panel authorization profiles to cardholders	31
11.5	Controlling doors through B901 modules on intrusion panels	32
12	Configuring operators and workstations	33
12.1	Creating the workstations	33
12.2	Creating workstation profiles	34
12.3	Assigning workstation profiles	35
12.4	Creating user (operator) profiles	35
12.5	Assigning user (operator) profiles	36
12.6	Setting passwords for operators	37
13	Configuring cards	39
13.1	Card Definition	39
13.1.1	Active Card Types	39
13.1.2	Creating and Modifying	39
13.1.3	Activating / Deactivating card definitions	41
13.1.4	Creating card data in the dialog manager	41
13.2	Configuring card codes	42
14	Configuring the controllers	45
14.1	Configuring MACs and RMACs	45
14.1.1	Configuring MAC Global access settings	45
14.1.2	Configuring a MAC on the DMS server	46
14.1.3	Preparing MAC server computers to run MACs and RMACs	47
14.1.4	Configuring a MAC on its own MAC server	47
14.1.5	Adding RMACs to MACs	49
14.1.6	Adding further MAC/RMAC pairs	51
14.1.7	Using the MAC installer tool	52

14.2	Access control hardware devices	53
14.3	Configuring the LACs	53
14.3.1	AMC parameters and settings	55
15	Configuring DTLS for secure communication	70
15.1	Top-down DTLS deployment	72
16	Configuring Entrances	74
16.1	Entrances - introduction	74
16.2	Creating entrances	75
16.3	Additional I/O checks	79
16.4	Configuring AMC terminals	80
16.5	Predefined signals for door models	86
16.6	Special entrances	92
16.6.1	Elevators (DM07)	92
16.6.2	Door models with intruder alarms (DM14)	95
16.6.3	DIPs and DOPs (DM15)	100
16.6.4	Mantrap door models	101
16.7	Doors	103
16.7.1	REX shunt	107
16.7.2	Configuring doors to sound local alarms	108
16.8	Readers	109
16.8.1	Configuring random screening	120
16.9	Access by PIN alone	121
16.10	AMC extension boards	122
17	Custom reader configurations	127
17.1	Introduction	127
17.2	The reader property: Extended reader parameters	127
17.3	Importing a reader parameter set	127
17.4	Applying a parameter set to readers	128
17.5	Managing reader parameter sets	129
17.6	Deleting reader parameter sets	130
18	Custom Fields for personnel data	131
18.1	Previewing and editing Custom fields	131
18.2	Rules for data fields	133
19	Configuring Threat Level Management	135
19.1	Concepts of Threat Level Management	135
19.2	Overview of the configuration process	135
19.3	Configuration steps in the device editor	136
19.3.1	Creating a threat level	136
19.3.2	Creating a Door security profile	136
19.3.3	Creating a Reader security profile	137
19.3.4	Assigning door and reader security profiles to entrances	138
19.3.5	Assigning a threat level to a hardware signal	139
19.4	Configuration steps in System data dialogs	140
19.4.1	Creating a Person security profile	140
19.4.2	Assigning a Person security profile to a Person Type	141
19.5	Configuration steps in Personnel data dialogs	141
20	Configuring Milestone XProtect to use AMS	142
21	Integrating Otis Compass	144
21.1	Configuring a Compass system in the Device Editor	145

21.1.1	Tier 1: Setting up the Compass system	145
21.1.2	Tier 2: Elevator groups, DES and DER devices	146
21.1.3	Tier 3: DET devices	147
21.2	Configuring customized fields for Otis-specific properties of cardholders	150
21.3	Creating and configuring authorizations for Otis elevators	151
22	Configuring IDEMIA Universal BioBridge	153
22.1	Setting up BioBridge in the Bosch access control system	153
22.2	Selecting card technologies and formats	154
22.3	Selecting an identification mode	159
22.3.1	Card OR Biometry	159
22.3.2	Card AND Biometry	161
22.3.3	Biometry only	161
22.4	Setting up BioBridge in MorphoManager	162
22.4.1	Wiegand Profiles	162
22.4.2	Biometric Device Configuration	163
22.4.3	Biometric device	165
22.4.4	User Configuration	166
22.4.5	User Distribution Groups	167
22.4.6	Setting up ODBC for BioBridge	169
22.4.7	BioBridge System Configuration	173
22.5	Configuring the BioBridge Enrollment Client	176
22.5.1	Adding an enrollment operator to Morpho Manager	176
22.5.2	Configuring the MorphoManager client computers for enrollment tasks	176
22.5.3	Testing the enrollment client	182
22.6	Technical notes and limits	183
23	Achieving EN 60839	186
24	Defining access authorizations and profiles	187
24.1	Creating access authorizations	187
24.2	Creating access profiles	187
25	Creating and managing personnel data	189
25.1	Persons	189
25.1.1	Card control or Building control options	191
25.1.2	Extra info: Recording user-defined information	192
25.1.3	Recording signatures	192
25.1.4	Enrolling fingerprint data	192
25.1.5	Enrolling palm vein data	194
25.2	Companies	197
25.3	Cards: Creating and assigning credentials and permissions	197
25.3.1	Assigning cards to persons	198
25.3.2	Printing badges	200
25.3.3	Authorizations tab	200
25.3.4	Other data tab: Exemptions and special permissions	201
25.3.5	Authorizing persons to set Office mode	202
25.3.6	Smartintego tab	203
25.3.7	Creating an Alert card	205
25.4	Temporary cards	205
25.5	PIN codes for personnel	207
25.6	Blocking access for personnel	208
25.7	Blacklisting cards	209

25.8	Editing multiple persons simultaneously	211
25.8.1	Group authorizations	212
25.9	Changing the Division for persons	213
25.10	Setting the area for persons or vehicles	214
25.10.1	Procedure for resetting the location of all cardholders and vehicles	214
25.11	Customizing and printing forms for personnel data	215
26	Managing visitors	216
26.1	Visitor data	216
26.2	Visitor too late	221
27	Managing parking lots	223
27.1	Overstayed parking	223
27.2	Parking tickets	224
27.3	Export of parking-lot utilization figures	230
27.4	Export Mobile Validity check	230
27.5	Authorizations for several park zones	230
27.6	Parking lot report	232
27.7	Extended Car Park management	232
28	Managing guard tours and patrols	234
28.1	Defining guard tours	234
28.2	Managing patrols	235
28.3	Tour monitoring (formerly path control)	236
29	Random screening of personnel	238
30	Using the Event Viewer	240
30.1	Setting filter criteria for time relative to the present	240
30.2	Setting filter criteria for a time interval	240
30.3	Setting filter criteria irrespective of time	241
31	Using reports	242
31.1	Reports: master data	242
31.1.1	Reporting on vehicles	244
31.2	Reports: system data	245
31.3	Reports: authorizations	246
32	Operating Threat Level Management	248
32.1	Triggering and cancelling a threat alert via UI command	248
32.2	Triggering a threat alert via hardware signal	249
32.3	Triggering a threat alert via Alert card	249
33	Operating Swipe ticker	250
33.1	Special cases	251
34	Backup and Restore	253
34.1	Backing up the system	253
34.2	Restoring a backup	254
34.2.1	Restoring RMACs into a new installation	256
35	Configuration and usage of CEPAS cards	257
	Glossary	259

1 Security

Use latest software

Before operating the device for the first time, make sure that you install the latest applicable release of your software version. For consistent functionality, compatibility, performance, and security, regularly update the software throughout the operational life of the device. Follow the instructions in the product documentation regarding software updates.

The following links provide more information:






- General information: <https://www.boschsecurity.com/xc/en/support/product-security/>
- Security advisories, that is a list of identified vulnerabilities and proposed solutions: <https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html>

Bosch assumes no liability whatsoever for any damage caused by operating its products with outdated software components.




2 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]

3 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.

4 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 boost the efficiency of your installed access-control hardware.

5 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.

Activating the license

Path

- AMS dialog manager > **Main menu** > **Configuration** > **Licenses**

1. Click **License Manager**
The **License Manager** wizard opens.
2. Click **Save** to save your system information to a file.
3. Click **Continue**.
4. Log on to the remote portal remote.boschsecurity.com with your company credentials.
5. Select the product to license, and follow the instructions in the portal to generate and download your license file.
6. Return to **License Manager**.
7. Click **Continue**.
8. Click **Import** to locate the license file you downloaded, and add it to your system.
9. Click **Finish**.
10. Click **Restart of AMS Dialog Manager**.



Notice!

If you encounter any error messages during the process, contact Bosch support.



Notice!

Effects of hardware and software changes

Changes to the hardware of your server may invalidate your license and cause the software to stop functioning. Please check with technical support before making changes to the server.

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.

6 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**.

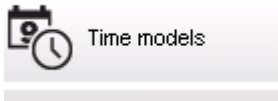
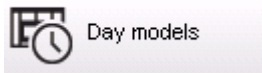
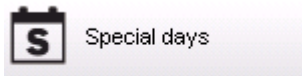
Time models control activities when they are applied to the underlying **calendar** of the access control system.

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.



6.1 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.

6.2 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: DMAC-Holiday Description: Holiday

Time intervals: Start time: End time:

1st interval: 01:00 AM 07:00 AM

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.

6.3 Defining Time models

The screenshot shows the 'Time models' configuration window. At the top, there's a toolbar with icons for search, navigation, and help. Below that, a 'Division' dropdown is set to 'Common'. The main area is divided into two sections:

- Time model of the access control:** Contains input fields for 'Name' (set to 'All'), 'Description', 'Period' (set to '6'), and 'Reference date' (set to 'Tu 07/21/2015'). There is a checked checkbox for 'Ignore special days' and a 'Preview' button.
- Assignment of day models:** A table with columns for 'No.', 'Day model', time slots ('6:00AM', '12:00PM', '6:00PM'), 'Description', 'Date (1st period)', and 'Division'. The table lists several 'DMAC-Holi...' entries with pink bars indicating active intervals, and a 'DMAC-none' entry at the bottom.

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.

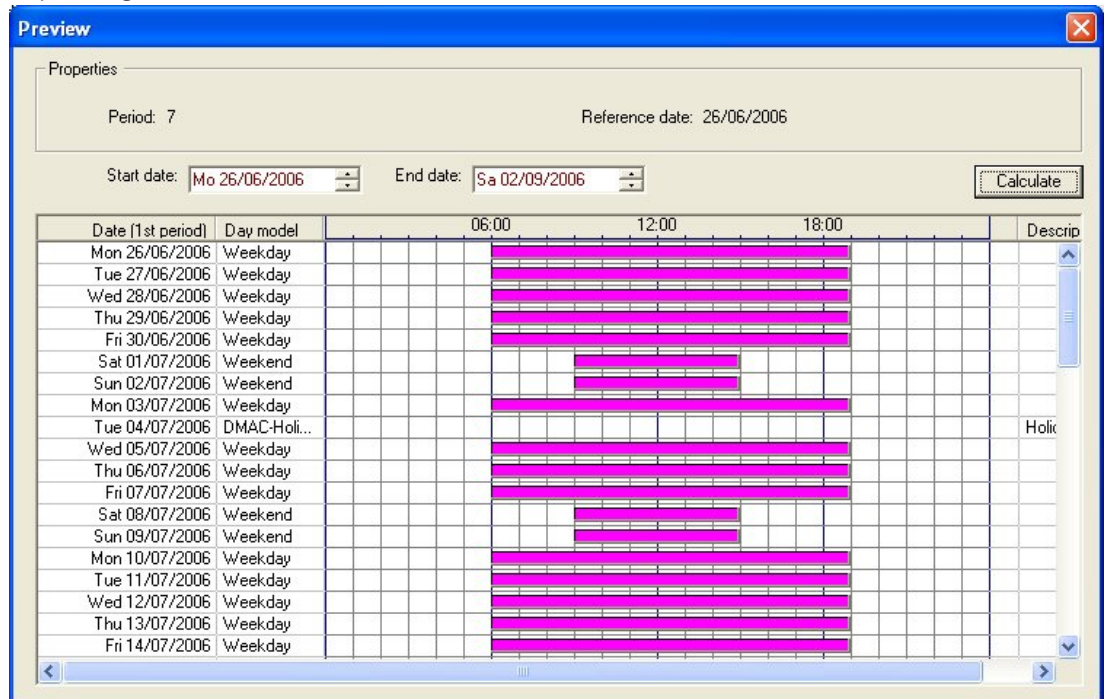
Only entries of the column **"Name"** can be changed or inserted by the user in this list - as already mentioned, the entries in the columns **"No"** and **"Date"** arise from the declarations of the dialog head; the column **"Description"** is filled out by the system with the choice of a day model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

Division: Common

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...				Holiday	Di 07/21/2015	Commc
7274568	DMAC-Holi...				Holiday	Mi 07/22/2015	Commc
7274569	DMAC-Holi...				Holiday	Do 07/23/2015	Commc
7274570	DMAC-Holi...				Holiday	Fr 07/24/2015	Commc
7274571	DMAC-Holi...				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

7 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

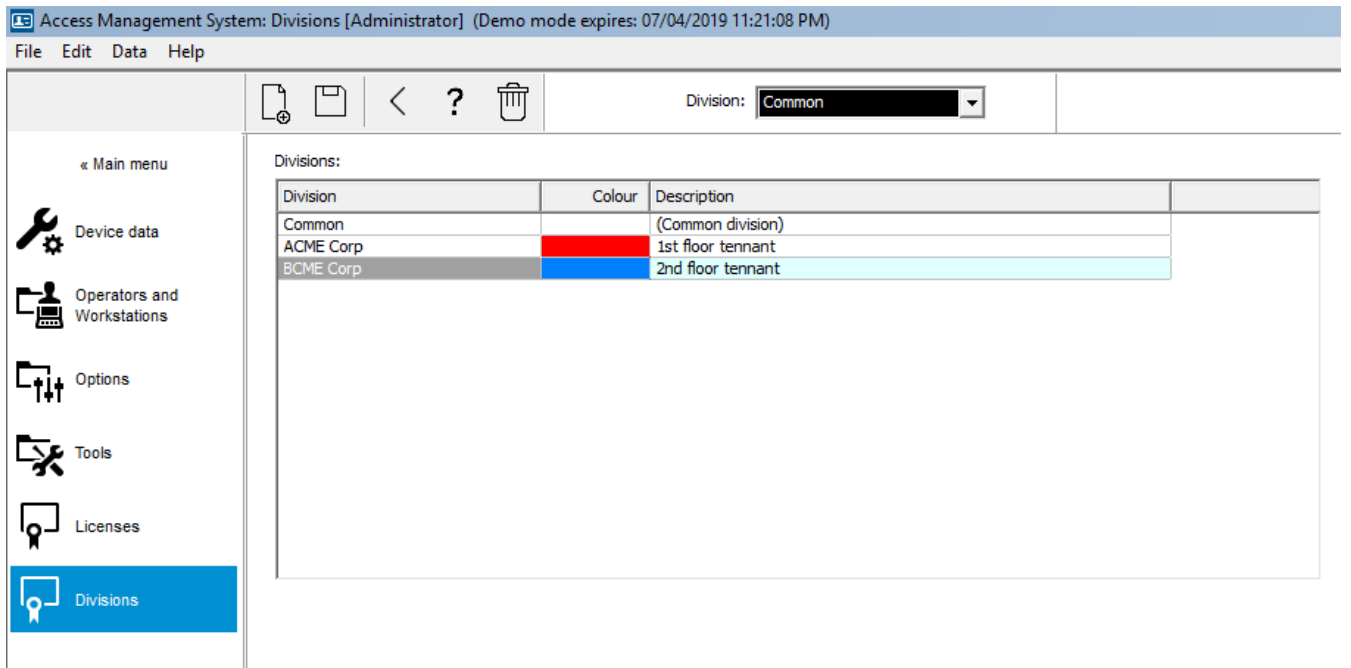
- The Divisions feature is licensed for your installation.

Dialog path

- Main menu > **Configuration** > **Divisions**
- BIS Configuration browser > **Locations** > **Divisions**

Procedure

1. Click the  button or right-click **Common** and select **Add new division** in the context menu.
2. Click  in the tool bar.
 - A new Division is created with a default name.
3. Overwrite the default name and (optional) enter a description for the benefit of other operators.
4. Click in the **Color** column to assign a color to help distinguish the division's assets in the user interface.
5. Click **Apply** to save
6. Click  to save



7.1 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.

7.2 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

8 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 **AMCIPConfig** 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**.
2. Click **Scan AMCIPConfig**
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 addresss**
 - **Serial number**
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 **Devices/Configure...** 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 **AMCIPConfig** tool to view its own help file.

9 Using the Device Editor

Introduction

The Device Editor is a tool for adding, deleting or modifying entrances and devices.

The Device Editor offers views for 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**
- **BIS Configuration browser > Connections > Device data**

Using the Device Editor toolbar

The Device Editor toolbar offers the following functions, regardless of which view is active: **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. All unsaved changes are discarded.
	Ctrl-S	Saves the current configuration
	Ctrl-F	Opens a search window
		Open the Device configuration tree

		Open the Workstations tree
		Open the Areas tree


In all Device Editor 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 a device, first select the parent device under which the sub-items should appear.

Copying and pasting AMC devices

To copy AMC devices from one part of the tree to another:

1. Right-click the AMC device and select **Copy** from the context menu.
2. Right-click on a suitable parent device elsewhere in the tree, and select **Paste** from the context menu.
 - The device is copied to the new location with its sub-devices and settings.
 - Device parameters such as **IP address** and **Name**, which must be unique, are **not** copied.
3. Enter unique values for those device parameters that require them. Until you do this you cannot save the device tree.

Saving your work

When you have finished adding and modifying items in the tree, click **Save**  to save the configuration.

To close the Device Editor, click **File > Exit**.

9.1

Configuration modes and overrides

Configuration mode is the default state of access control devices in the device editor. In configuration mode, an authorized user of AMS or BIS ACE can make changes to devices in the device editor, and the ACS propagates the changes immediately to subordinate devices. An operator can **override** configuration mode by sending commands directly to access control devices from outside the device editor. This is common, for example, when an operator is handling incoming messages and alarms. Until the operator sends the **Restore configuration** command, the device remains in Operation mode . If a configuration user selects a device in the device editor while it is in operation mode, then the main property page of the device displays the notification.

10 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.

Name	The default name, which you may overwrite.
Description	A free-text description of the area.
Maximum number of persons / cars	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.
- The **Division** field is read-only in this dialog. To change the Division of an area use the **Detector placement** dialog and select the area in the **Devices** pane.

Procedure for deleting areas.

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



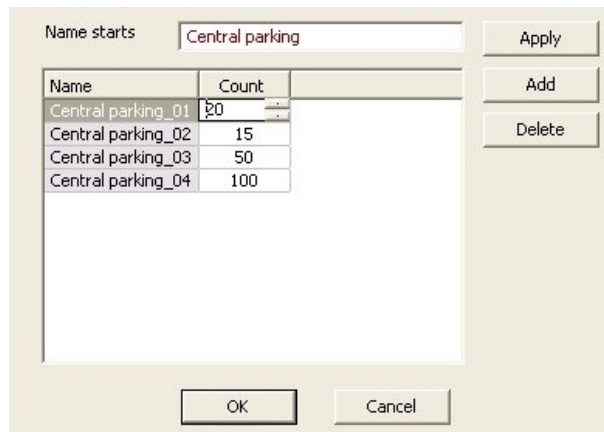
2. Click **Delete** or right-click to delete via the context menu.

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

10.1 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.



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.

11 Configuring intrusion areas and panels

Introduction

The access control system participates in the administration and operation of Bosch intrusion panels. Consult the datasheet of the access control system for details of the models that it supports. The access control system adds particular value in the administration of the intrusion panel **users**. These users are a subset of the cardholders of the overall access control system. Access control system administrators give these cardholders special authorizations to operate the intrusion panels through the ACE Dialog Manager.

The intrusion panels themselves are configured and updated as previously through their Remote Programming Software (RPS). ACE continually reads from the RPS, and displays the panels that are in it.

ACE contains dialogs to create and assign authorization profiles, and to the manage panel users on the RPS.

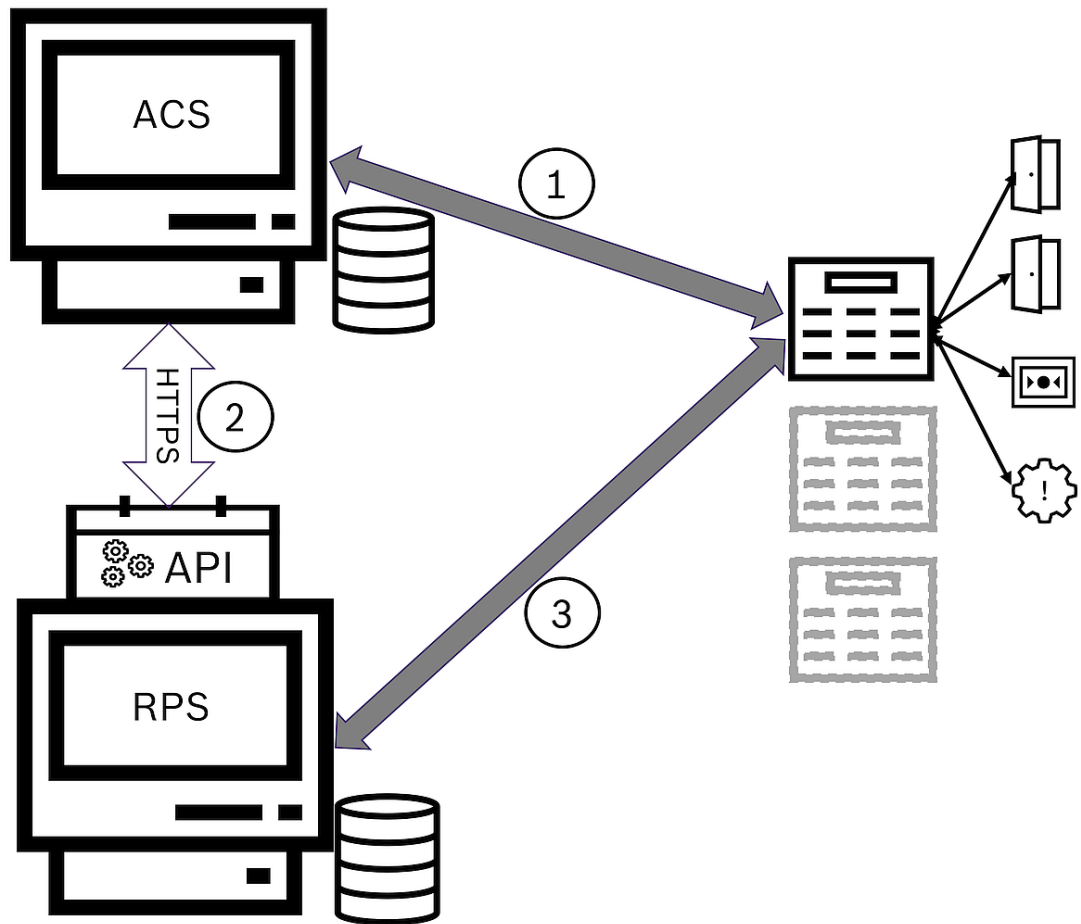


Figure 11.1: Simplified ACS-Intrusion system topology

ACS	The main Access Control System: AMS or BIS-ACE
API	The Application Programming Interface
RPS	Remote Programming System: The application for controlling Intrusion panels

1	ACS to panel: panel commands. Panel to ACS: events from intrusion points .
2	ACS to RPS: cardholder data
3	RPS to Panel: configuration settings

Prerequisites

- The RPS of supported Bosch intrusion panels is installed on a separate computer with a network connection to the ACE server, **not** on the ACE server itself. Consult the RPS installation guide for installation instructions.
- RPS has been configured with the intrusion panels that will belong to the ACE access control system. Consult the RPS user guide or online help for instructions.
- The clocks on the panels are within 100 days of the clock on the ACE server, to enable automatic synchronization.
- Mode 2 protocol is set on all participating panels.
- Cards with one of the following standard card definitions:
 - HID 37 BIT -> Intrusion 37 BIT with a facility/site code of 32767 or lower.
 - HID 26 BIT- > Intrusion 26 BIT
 - EM 26 BIT- > Intrusion 26 BIT

Overview

The configuration process consists of the following stages, described in the following sections in this chapter:

1. Installing the Intrusion RPS API on the RPS computer
2. Connecting the access control system to the intrusion panels.
 - Defining the connection to the RPS API.
 - Configuring the panel connections.
3. Creating panel authorization profiles that govern which functions of the connected panels can be used.
4. Assigning panel authorization profiles to cardholders.
 - These cardholders thus become operators for the intrusion panels.

11.1

Installing the Intrusion RPS API on the RPS computer

The Intrusion RPS API is the communication channel between the AMS and the RPS applications on their respective computers. You must first install the API on the RPS computer, then install the certificates that the setup generates on the AMS computer.

Procedure

1. Execute the RPS API setup file according to its own documentation.
 - The setup file and its documentation, are located on the AMS installation media:
AddOns\Intrusion-RPS-API\Bosch_RPS_API_Setup_v*.exe
AddOns\Intrusion-RPS-API\RPS-API_Application_note_v*.pdf
 - The setup program generates 2 certificates and saves them on the RPS computer:
%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.cer
%AppData%\Roaming\Bosch_RPS_API\BoschRpsAPI.pfx (requires you to set a password)
2. Copy the certificate files to the AMS computer.
3. On the AMS computer install the certificates to **Store location:** Local Machine,
Certificate store: Trusted Root Certification Authority.

11.2 Connecting the access control system to the intrusion panels

Introduction

This section describes how to view the intrusion panels and make them available for control through ACE client. The access control system connects via the API to the RPS on its network. Through the API it maintains an up-to-date internal list of the compatible intrusion panels that are available.

Two steps are necessary in AMS to connect it to intrusion panels:

- Step 1: Defining the connection to the RPS API
- Step 2: Configuring the panel connections

Dialog path

- Main menu > **Configuration** > **Panels** and subdialogs

11.2.1 Step 1: Defining the connection to the RPS API

Step 1 is to provide the RPS computer's address and administrator login information to the access control system.

Dialog path


Main menu > **Configuration** > **Panels** > **RPS API configuration**

Procedure

1. Enter the following information:

Information	Description
Host name / IP address	The HTTPS address of the computer on which the RPS is running, and the port number through which the RPS communicates. The use of <code>localhost</code> is not permitted. The default port number is <code>9000</code> .
User name	The user name of an RPS administrator user for the API.
Password	The password of the RPS administrator user.

2. Click the button **Test the connection** to ensure that the RPS is running, and that the user name and password are valid.

3. Click  (Save) to save the changes.


11.2.2 Step 2: Configuring the panel connections

Step 2 is to configure the amount of control that the access control system has over individual panels on the network.

Dialog path

Main menu > **Configuration** > **Panels** > **Panel administration**


The dialog maintains a list of the compatible intrusion panels that the RPS API has provided to the ACE.

The list is periodically updated in the background. After you open the dialog, click  occasionally, to force an immediate update manually.

The list is read-only, except for the controls described in the following section.

Procedure

1. Select a panel from the list
2. Use the controls below to define what the access control system can do on the selected intrusion panel.

List column User administration	Select the check box to ensure that the users of the intrusion panel in this row are maintained in the access control system and not on the panel itself. IMPORTANT: this setting causes all panel users that were created locally in RPS to be overwritten.
List column Map View	Select the check box to make this panel available for Command and Control through the ACE client .
Settings icon in the Access data column.  (cog)	If you selected the check box in the Map View column, click the icon to enter <ul style="list-style-type: none"> – an IP address – a port number (default 7700) – the passcode for the individual panel. The passcode is set in the RPS.
Button: Delete selected panel	If a panel has been deleted in RPS it appears with a status of Removed in the list. Select the panel and click this button to delete it completely from the database.

11.3

Creating authorization profiles for panels

Introduction


This section describes how to create panel authorization profiles.


A panel authorization profile is a custom set of authorizations to operate a custom set of intrusion panels. An ACE administrator can create multiple panel authorization profiles for the various responsibilities of various groups of cardholders.

Dialog path

- Main menu > **System data** > **Authorization profiles for intrusion panels**

Procedure

1. Click  to create a new profile
2. (Mandatory) Enter a name for the profile
3. (Optional) Enter a free-text description for the panel
4. Below the **Assigned panels** list, click **Add...** to add one or more panels from a popup list of panels available on the network.
Conversely, select one or more panels and click **Remove** to remove them from the list.
5. Click a panel in the **Assigned panels** list to select it.
 - In the **Authorizations** pane, a list appears containing all the intrusion areas that belong to the selected panel.
6. In the **Authorizations** list, in the column **Authority level**, select an authority level for each intrusion area of the panel that is to be included in this profile.
 - The authority levels are defined and maintained in RPS. They may be customized there also. Make sure you know the definition of the authority level in RPS before assigning it to a profile.
 - By default **L1** is the highest authority level, with **L2**, **L3** etc. increasingly restricted.

- If you leave a cell blank, then the recipient of this profile will have **no** authorization over the selected intrusion area of the selected panel.
7. Repeat this process for all the intrusion areas of all the panels to be included in this profile.
 8. (Optional) From the **User group** list, select a panel user group in order to restrict the authorizations to certain time periods.
 - The user groups are defined and maintained in RPS. They may be customized there also. Make sure you know the definition of the user group in RPS before assigning the user group to a profile.
 9. Click  (Save) to save the changes.

11.4 Assigning panel authorization profiles to cardholders

Introduction

This section describes how to assign different panel authorization profiles to different types or groups of cardholders.


Prerequisite


You have defined one or more panel authorization profiles in the access control system.

Dialog path

Main menu > **Persons** > **Cards**

Procedure

1. In the usual way, find and select the desired cardholder from the database.
2. Click the **Intrusion** tab.
3. On the **Intrusion** tab, select the check box **Panel user**.
4. (Mandatory) In the **Passcode** field, type a passcode through which this cardholder will operate the intrusion panels.
 - If required, use the button to generate an unused new passcode.
5. In the **ID card** list, select one of the access control credentials that is assigned to this cardholder.
6. (Optional) In the **Number of remote** field, enter the number that is printed on the cardholder's remote control device for intrusion panels.
7. In the **Language** list, select the language in which the cardholder prefers to read panel dialogs.
8. If the cardholder is to use the Bosch smartphone application for intrusion panels, select the **Remote access** check box.
9. From the **Authorization profile** list, select a suitable panel authorization profile for the cardholder.
10. Click  (Save) to save the changes.
 - This panel authorization profile, with all its panels and authorizations, is assigned to the cardholder. The cardholder thus becomes an operator for the intrusion panels.

Note that you can also use the data fields on this dialog with the  button to find cardholders in the database.

11.5 Controlling doors through B901 modules on intrusion panels

In AMS 4.0.1 and later, B901 Access Control Interface Modules can be controlled via the AMS Map View.

The B901 is a simple door controller that a system administrator connects to Bosch intrusion panels. You connect the corresponding intrusion panel to AMS as described in the previous sections.

You do not configure the B901 in the Device Editor.

The B901 can lock/unlock, secure/unsecure, and cycle doors, but it provides limited state information to the access control system. For example, it does not communicate whether a door was physically opened rather than just unlocked.

Like all other intrusion devices, In order to send commands to the B901 from AMS Map View, you must enable Map View for the corresponding panel in the AMS dialog:

Main menu > **Configuration** > **Panels** > **Panel administration**

Map View Swipe ticker and B901 doors

In order to provide correct information to the **Swipe ticker** app in AMS Map View, the IDs of B901 doors must match the IDs of their door points. That is, Door 1 must be assigned to Door Point 1, Door 2 to Door Point 2 etc.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SD12 (B901)	SD12 (B901)	SD12 (B901)	SD12 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms
Door Point	1	2	3	4

Make these assignments to the B901 door controller in the RPS tool that configures intrusion panels and controllers.

12 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

12.1 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 inactive time:** The number of seconds after which a logon session via enrollment reader is automatically terminated. Leave at 0 for unlimited time.

12.2 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.

12.3**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.

12.4**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

12.5

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:

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

- Click  to save your changes

12.6 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 to 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/>

13 Configuring cards

13.1 Card Definition

Use this dialog to activate, deactivate, modify or add the card definitions to be used by your access control system.

Dialog path

- Configuration Browser > **Infrastructure** > **ACE Card definition**
- AMS main menu > **Configuration** > **Options** > **Card definition**

The system is supplied with a set of predefined card types. The predefined card types are displayed with gray background in the table **Available card types** and cannot be modified. They can only be moved between the **Active Card types** and **Available card types**.

13.1.1 Active Card Types

The active card types are those types that the card readers in your access control system are to recognize and process. Up to 8 card definitions can be active simultaneously in one system except CEPAS cards.

CEPAS cards is an exclusive card type. Therefore, when using CEPAS cards, no other card types can be activated.

For readers with L-Bus or BG900 protocols the list entry **Serial Readers** must be added under **Active Card types** in the Configuration Browser (**Infrastructure** > **ACE Card definition**) in order to make the manual input mask Dialog (Bosch) available in Access Engine for manually entering card data.

13.1.2 Creating and Modifying

Click the **+** (green +) button above the right-hand list box to create a new list entry. In contrast to predefined card types the data of newly created types are freely editable.

Double-click the fields **Name**, **Description** and **Number of Bits** to edit them.

The name can have a maximum of 80 characters, and the description 255. The number of bits is limited to 64 (if a higher number is entered then this will be reset to the maximum as soon as the text field loses input-focus).



Notice!

Bit lengths are used to differentiate between Wiegand definitions. Therefore each new definition must have a unique bit length which has not been used by an existing definition.

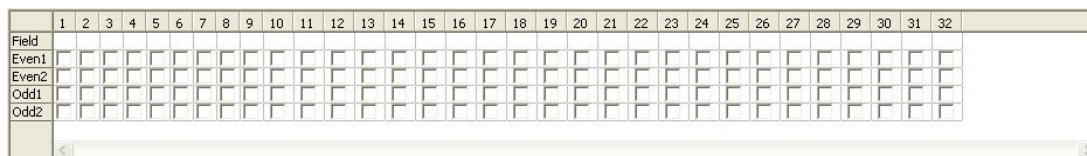
- ▶ To modify a data bit, double-click the relevant field. To delete it, first select the data bit then click the **X** (red x) button.



Notice!

Only card types that were created by the user can be modified or deleted.

When a single card type is selected (in left or right-hand lists) then its encoding is displayed in the lower part of the dialog. The display shows data bits in 5 rows, and as many columns as the number of bits in the definition.



Each column of the **Field** row can be given a label that determines how that part of the code is to be interpreted. The labels available are as follows:

F	Facility: marks the code part for facility affiliation	
C	Code no: code part containing the individual card number	
E1	Even 1: bit to balance the first Even Parity Mask	The declaration of these values activates the check box for the corresponding line.
E2	Even 2: bit to balance the second Even Parity Mask	
O1	Odd 1: bit to balance the first Odd Parity Mask	
O2	Odd 2: bit to balance the second Odd Parity Mask	
1	Fix bit values contained in the code	
0		

In the case of the labels E1, E2, O1 and O2 it is enough to select the check-box on the corresponding row. The box on the **Field** row will automatically be marked accordingly.

Explanation:

The signal sent by a reader when presented with a card is made up of a series of zeros and ones. For each card type the length of this signal (i.e the number of bits) is exactly defined. In addition to the actual user data, which are saved as code data, the signal also contains control data in order to a) identify the signal as a card signal, and b) verify correct transmission.

In general the fixed zeros and ones are useful for identifying the signal type.

The parity bits, which must yield either a zero (Even Parity) or a one (Odd Parity) as a checksum over selected bits of the signal, are used to verify correct transmission. The controllers can be configured so that they calculate one or two checksums for Even Parities and one or two checksums for Odd Parities.

In the list control, those bits can be marked in the respective lines for the parity checksums (Even1, Even2, Odd1 and Odd2) which should be included in the checksum. In the top line (Field) for every checksum used a bit is defined to balance the checksum according to the parity type. If a parity option is not used, the corresponding line simply remains empty.

13.1.3 Activating / Deactivating card definitions

Up to 8 card definitions can be active simultaneously, except CEPAS cards. The definitions to be activated must be moved to the left-hand list **Active Card Types**. This is done by (multi-)selecting one or more definitions on the right-hand side, and clicking the left arrow (<) button.

No more than eight definitions can be moved at once. Once eight definitions are in place then any surplus are discarded from the move. To add more definitions to **Active Card Types** it will be necessary to delete one or more of those present by (multi-)selecting and moving them to the right-hand side using the (>) button, thus deactivating them.



Notice!

To use readers with L-Bus or BG900 protocols, activate the card type **Serial Reader**. This makes the manual input dialog **Dialog Bosch** available to the dialog manager of the access control system.

13.1.4 Creating card data in the dialog manager

Manual data input

Different input methods are used for Wiegand and Bosch cards.

For all Wiegand definitions (HID 26, HID 35, HID 37 and 32 Bit CSN) the dialog box **Dialog (Wiegand)** allows you to enter **Customer code** and **Card no.** (card number).

For serial readers the dialog box **Dialog (Bosch)** contains additional fields for **Version** and **Country code**.

Data input by enrollment reader

In addition to manual data input, any workstation can be equipped with a dialog reader for collecting card data. Use a reader from the list in the following dialog:

- Configuration Browser > **Infrastructure** > **ACE Card Reader**.
- AMS main menu > **Configuration** > **Options** > **Card reader**

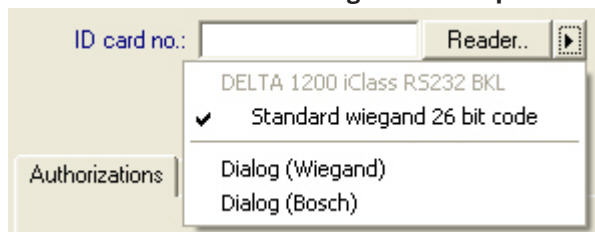
If the chosen reader is an input reader for Wiegand cards then all active Wiegand card types will be listed along with the reader

- Access Engine > **Personnel data** > **Cards** > Reader button > ► (right arrow).
- AMS main menu > **Personnel data** > **Cards** > Reader button > ► (right arrow)

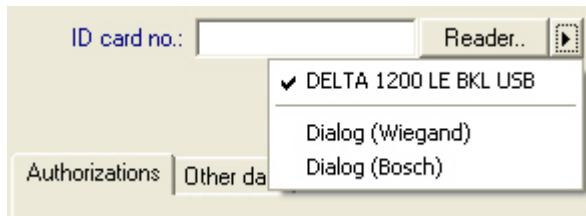
One of these card types must be selected in order to ensure the correct saving of the card encoding. That is, the reader itself cannot be selected directly but only indirectly via the choice of Wiegand definition.

If the required card type does not appear in the pull-down list, you must activate it in the card definition dialog.

- Configuration Browser > **Infrastructure** > **ACE Card definition**
- AMS main menu > **Configuration** > **Options** > **Card definition**



HITAG, LEGIC and MIFARE enrollment readers can be selected from the list directly.



13.2 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

Entering numbers in the dialog

For convenience, you can enter numbers in decimal or hexadecimal formats. Select the radio buttons **Hexadecimal** or **Decimal** according to the format specified by the cards' manufacturer.

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 text entry 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 fields are not writeable, then they are not relevant to any of the active card definitions. For Bosch code all fields are writeable.

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.

Card default code data

Hexadecimal
 Decimal

Version:

Country code:

Facility code:

Entering code data:

If the data are provided by the manufacturer as decimal values, select the Decimal radio button and enter the values provided, for example:

Version: 2

Country code: 99

Facility code: 56720

Click **Apply** to store the data.

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: 000000415
 - 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.

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.

14 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 22*

14.1 Configuring MACs and RMACs

14.1.1 Configuring MAC Global access settings

In the **Global access settings** tab is possible to set the values for the following parameters:

- Time factor for handicapped persons.
- Time limit for group access.
- Time limit for level keypad input.
- Area dwell time of person expires after.

To set the parameters, consider the following dialog path:

Main menu > Configuration > Device data > Device tree > DMS > MAC > Global access settings

For more information using the device editor, refer to *Using the Device Editor, page 22*.

Consider the following parameters:

- **Time factor for handicapped persons:**
 - Value "Max. duration of pulse to door strike" is multiplied by this factor (Doors->Tab: Options).
 - To mark a person as handicapped use.
- **Time limit for group access:**
 - Maximum time until the next card is read for Group access.
 - Value 0 -> switch off the time limit (infinite time).

- **Time limit for keypad input:**
 - Maximum time for input on the reader for each digit. (If you have a 4 digit PIN and the value for time limit is set to 50 [1s/10) you have 20 seconds (4 times 5 seconds) for the input. It does not matter if you wait longer than 5 seconds between two digits, as long as the total input time does not exceed 20 seconds (Values for the example with a 4digit Pin and time for keypad input 50 1s/10).
 - Value 0 -> switch off the time limit (infinite time).

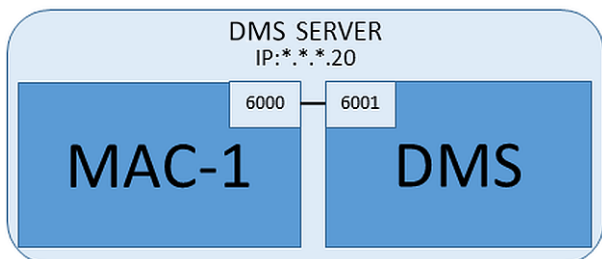
- **Area dwell time of person expires after:**
 - 0 = disabled the card check functionality (a person will stay in an area until he/she books at a reader to another area) -> no time limit, no automatic booking to outside.
 - Value between 0 and 168 possible.
 - 1-168: time in hours until the person will be set to outside, if there are no bookings of this person for that time.
 - Value 0 will set the area dwell time to infinity.

Refer to

- *Using the Device Editor, page 22*

14.1.2

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, page 22*.

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>
RMAC Port	<Leave blank>
Active (check box)	Clear 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.

Parameter	Description
Load devices (check box)	Clear 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	IMPORTANT: 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.

14.1.3

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 control 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.

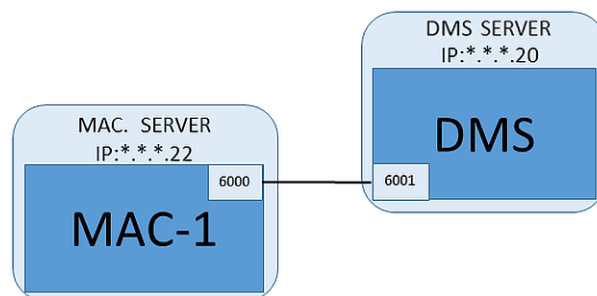
Separate computers where MACs or RMACs reside, are known as MAC servers regardless of whether they host a MAC or an RMAC.

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. The operating systems of all the MAC servers must be currently supported by Microsoft, and have the latest updates installed.
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 10 and Windows Server operating systems it is enabled as a feature.
6. Reboot the computer.

14.1.4

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 computer, in the device editor,
 - Right click the MAC and select **Disable all LACs**.
 - Deactivate the MAC by clearing the check boxes **Activate** and **Load devices** for this MAC.
2. On the MAC server computer, using the Windows program `services.msc`
 - Stop the MAC service **AUTO_MAC2**
 - Set the **Startup type** of this MAC service to **Manual**.
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).
 - For AMS this is found on the AMS installation media
`\AddOns\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
3	Destination Folder	The local directory where the MAC is to be installed. Take the default wherever possible.
4	Server	The name or the IP address of the server where the DMS is running.
4	Port (Port to DMS)	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.
4	Number (MAC System Number)	Set 1 for this and all MACs (as opposed to RMACs).
4	Twin (Name or IP address of partner MAC)	Leave this field blank as long as this MAC is to have no RMAC.

5. On the DMS server, select the MAC in the Device Editor.
6. 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 system operators
With RMAC (check box)	<Leave blank>
RMAC Port	<Leave blank>
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	IMPORTANT: The time zone of the MAC and all its subordinate AMCs.

Parameter	Description
Division	(If applicable) The Division to which the MAC belongs.

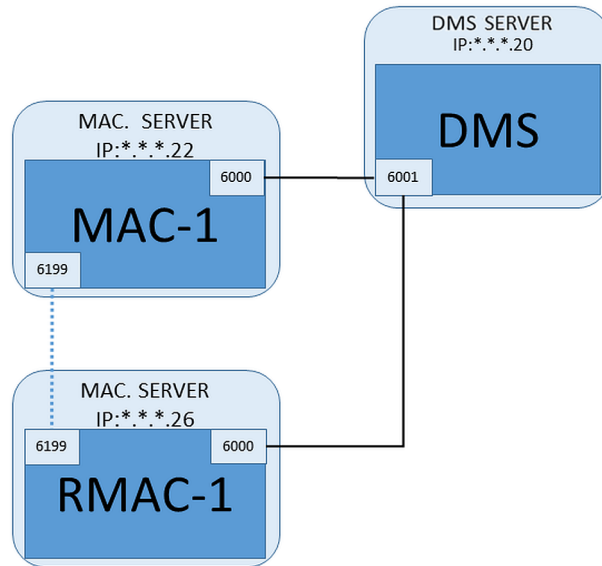
14.1.5 Adding RMACs to MACs



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
With RMAC (check box)	Clear this check box until you have installed the corresponding RMAC on the redundant failover connection server
Active (check box)	Clear 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.

Parameter	Description
Load devices (check box)	Clear 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 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.

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
With RMAC (check box)	Selected A new tab labeled RMAC appears next to the MAC tab.
RMAC Port	6199 (the static default) All MACs and RMACs use this port to check whether their partners are running and accessible.
Active (check box)	Selected This enables synchronization between this MAC and its subordinate devices.
Load devices (check box)	Selected 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
Name	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.
Description	Optional documentation for access control operators.
IP address	The IP address of the RMAC.

Parameter	Description
MAC Port	6199 (the static default) All MACs and RMACs use this port to check whether their partners are running and accessible.

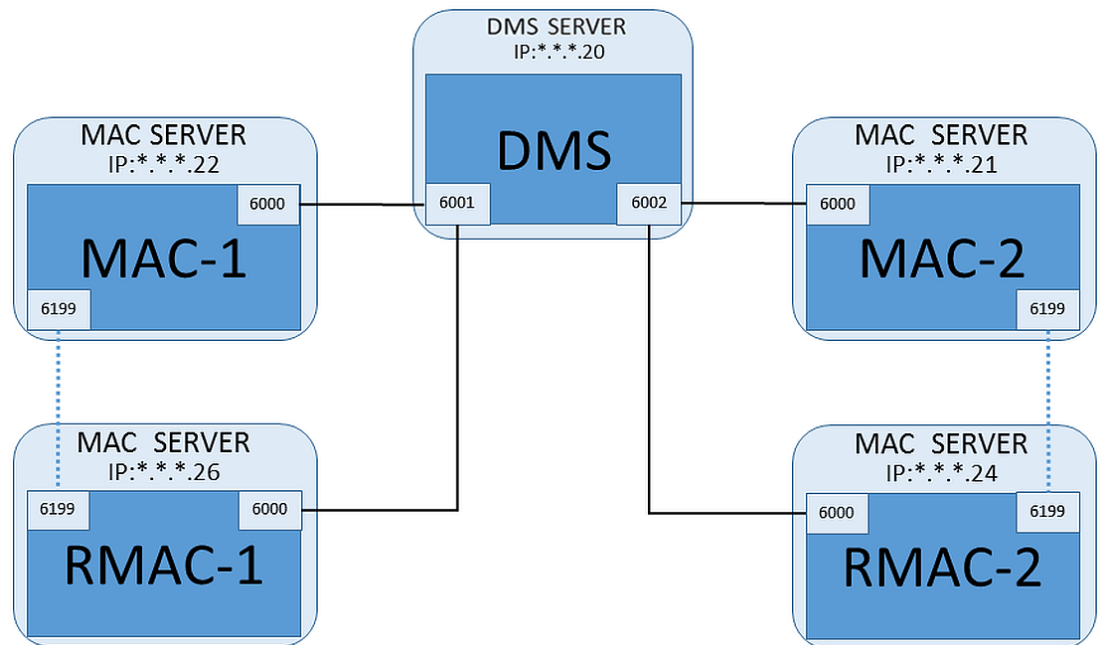
Refer to

- Using the MAC installer tool, page 52

14.1.6

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.

14.1.7**Using the MAC installer tool**

MACInstaller.exe is the standard tool for installing 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 installation medium under the following path:

- \AddOns\ACE\MultiMAC\MACInstaller.exe
- \AddOns\MultiMAC\MACInstaller.exe

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

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

Parameter: Port (Port to DMS)

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.

Parameter: Number (MAC System Number)

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

Parameter: Configure Only (radio button)

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**.

Parameter: Update Software (radio button)

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**.

14.2 Access control hardware devices

AMCs with DTLS-Support no longer support RS485 or RS232 connections between host (MAC) and AMC.

Disable or remove from configuration all AMCs that are configured on COM ports.

Otherwise, the device editor cannot finalize the migration. Therefore, the configuration remains unsaved.

With AMS 4.0 the bootloader has been updated to version 00.62 v02.30.00 LCM. AMCs will be updated automatically by AMS 4.0.

In order to update AMCs manually, the Bosch.AMCIPConfig-Tool must be used.

If the AMC has Bootloader V00.49 and earlier, first update to V00.61v01.47.00 and from this to 00.62 v02.30.00 LCM.

Firmware downgrades

In order to use an AMC that has been upgraded to BIS 4.9.1 or AMS 4.0 on an older access control system (ACE, AMS or APE), an AMC firmware downgrade is necessary.

Firmware versions V00.62 must first be downgraded to V00.61 before they can be downgraded to older versions.

14.3 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

AMC 4-W	Access Modular Controller 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.
AMC 2-W	Access Modular Controller with two Wiegand readers.	A maximum of two Wiegand readers can be configured to connect up to two entrances. The controller supports four input and four output signals.
AMC 4-R4	Access Modular Controller 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.
AMC_IO08	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
AMC_IO16	Extension board for the AMC with sixteen input and output signals	
AMC_IO84W	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

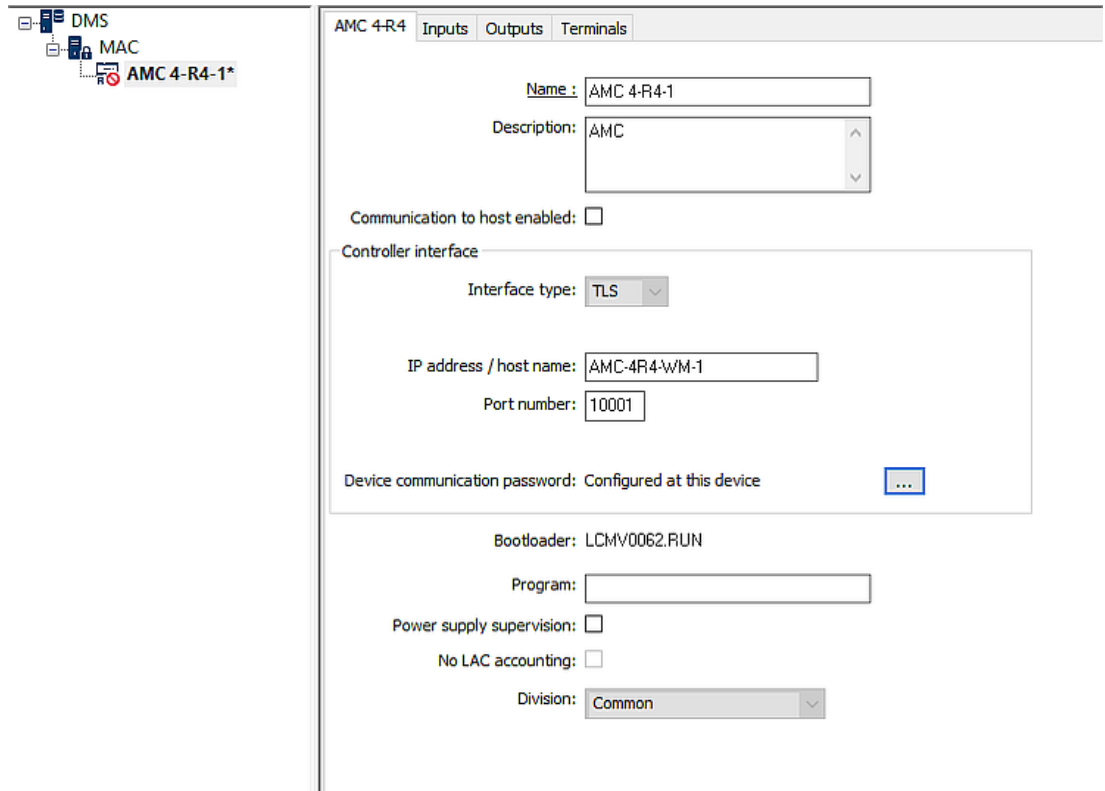
Access control systems are normally equipped with only one type of controller and reader. Software upgrades and growing installations can make it necessary to supplement existing hardware components with new ones. Even configurations combining RS485 variants (AMC 4R4) with Wiegand variants (AMC 4W) are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

14.3.1 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 users can overwrite them. If you overwrite a name you must make sure the IDs are unique.
Controller description	alphanumeric: 0 - 255 digits	Free text.
Communication to host enabled	0 = disabled (check box is cleared) 1 = enabled (check box is selected)	Default = enabled Overlay-icons on the controllers in the device tree indicate the status of the host connection (enabled/disabled). Clearing the check box temporarily takes the AMS offline, and is useful for reconfiguration and testing.

		<p>Updating the access control system to a new version clears the check boxes of all controllers automatically. Select and clear the check boxes of AMCs to test them individually in the updated software.</p>
		<p>Select the check box when using the device editor to set a DCP (device communication password) on the AMC during "top-down" implementation of DTLS. This opens a 15-minute time window to propagate the DCP down to the AMCs. Clear and select the check box to restart the time window.</p>
Controller Interface		
Interface Type	TLS	<p>TLS (=transport layer security): When you set a DCP (device communication password) for the AMC, the communication to the MAC is via DTLS with enhanced security.</p> <p>Make sure that the DIP switches 1 and 5 on the AMC are set to ON.</p>
IP Address/ Hostname	Network name or IP address of the AMC	<p>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 enter the IP address.</p>
Port number	numeric: 10001 (default)	This is the AMC port which will receive the MAC-messages.
Further Parameters		
Program	Alphanumeric	<p>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.</p>

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. Note 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"	Relevant only if the Divisions feature is licensed.

Configuring AMC inputs

AMC 4-W
Inputs
Outputs
Terminals

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

<p>serial</p> <ul style="list-style-type: none"> <input type="radio"/> none <input type="radio"/> 1K <input type="radio"/> 1K2 <input checked="" type="radio"/> 1K5 <input type="radio"/> 1K8 <input type="radio"/> 2K2 <input type="radio"/> 2K7 <input type="radio"/> 3K3 <input type="radio"/> 3K9 <input type="radio"/> 4K7 <input type="radio"/> 5K6 <input type="radio"/> 6K8 <input type="radio"/> 8K2 	<p>parallel</p> <ul style="list-style-type: none"> <input type="radio"/> none <input checked="" type="radio"/> 1K <input type="radio"/> 1K2 <input type="radio"/> 1K5 <input type="radio"/> 1K8 <input type="radio"/> 2K2 <input type="radio"/> 2K7 <input type="radio"/> 3K3 <input type="radio"/> 3K9 <input type="radio"/> 4K7 <input type="radio"/> 5K6 <input type="radio"/> 6K8 <input type="radio"/> 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 Open, close were activated 02 = if events Line cut, short circuit 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.

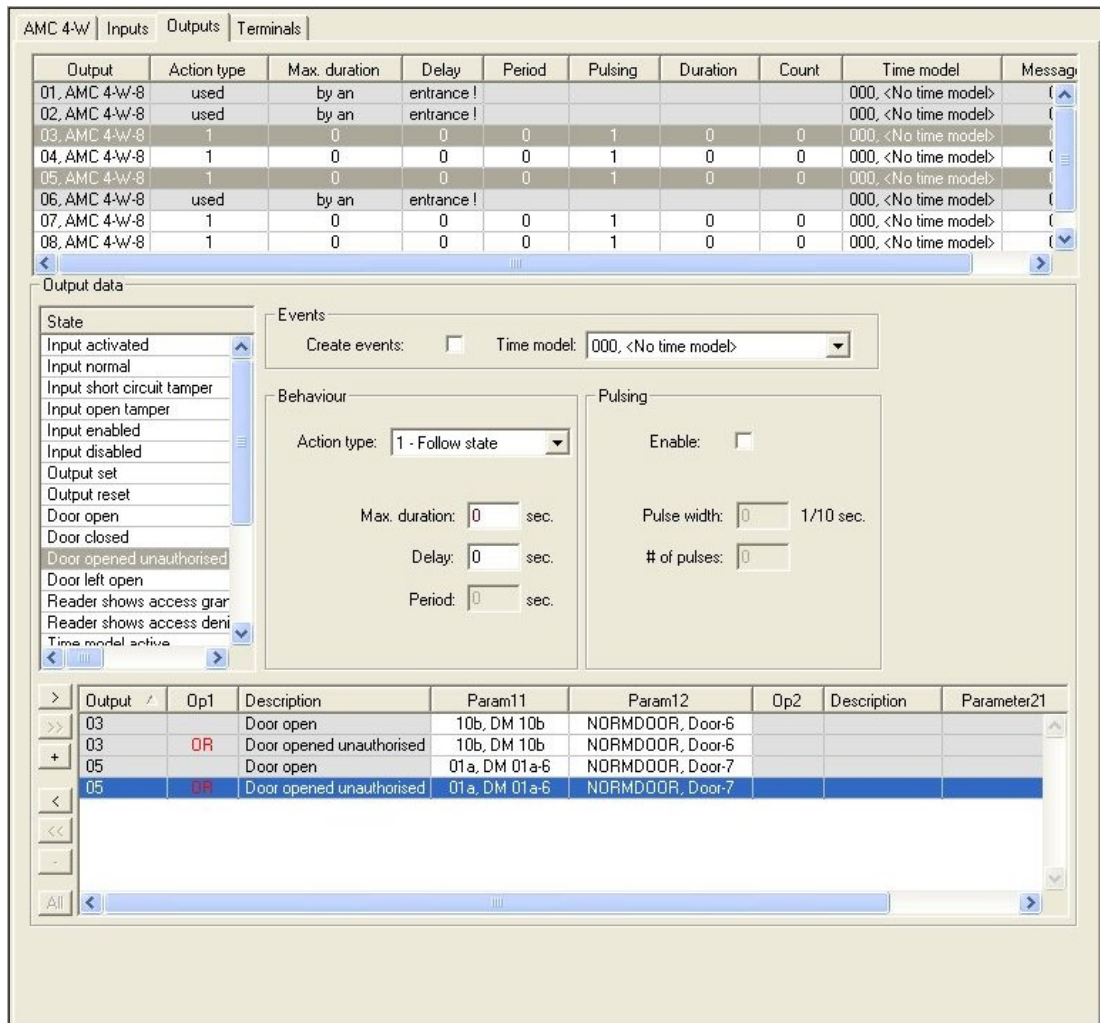
The following tables show in the left columns the selected values, and in the right columns the available ranges of the other resistor.

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



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 gray.

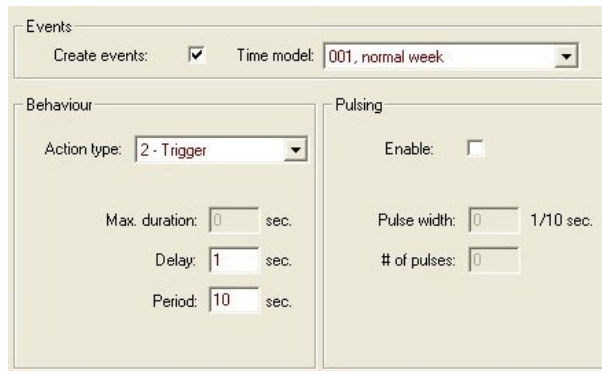
Parameters of AMC outputs

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:

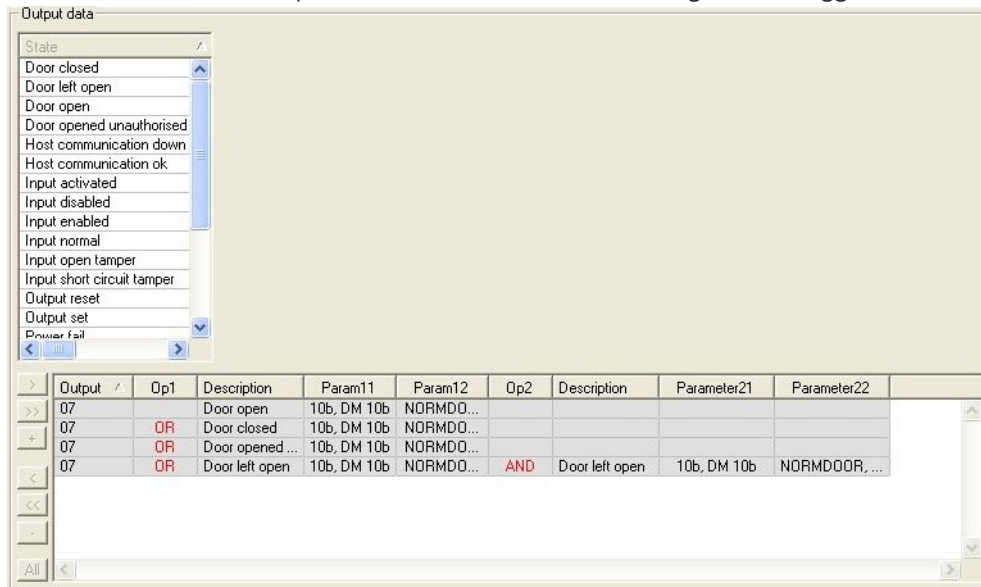
Action type	Max. duration	Delay	Period	Pulsing/ Enable	Pulse width	Number of pulses
Follow state	0 = always 1 - 9999	0 - 9999	no	yes	1 - 9999	None

Trigger	no	0 - 9999	0 - 9999 if pulsing is not 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 those outputs.



Configuring outputs to be triggered by certain states

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

- Select one or more 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 state) to create for each selected output an input with that state. 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 a

logical OR-operator 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 state must already be assigned to which another condition is added by selecting it in an arbitrary column.
- Then another state 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-conditions can be assigned to every output.
Each condition can have **one** AND-condition within it.

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

You can modify lines in the list



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_10, AMC_1016_002_1	In, 01, AMC_1016_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 disabled	5	Local input deactivated by time model
Input enabled	6	Local input activated 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	---
Message from reader	23	Reader address
Message from LAC	24	Board number
Card control	25	Reader address, card control function.


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 an external device 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	REVDOOR, 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	REVDOOR, 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 external device 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				

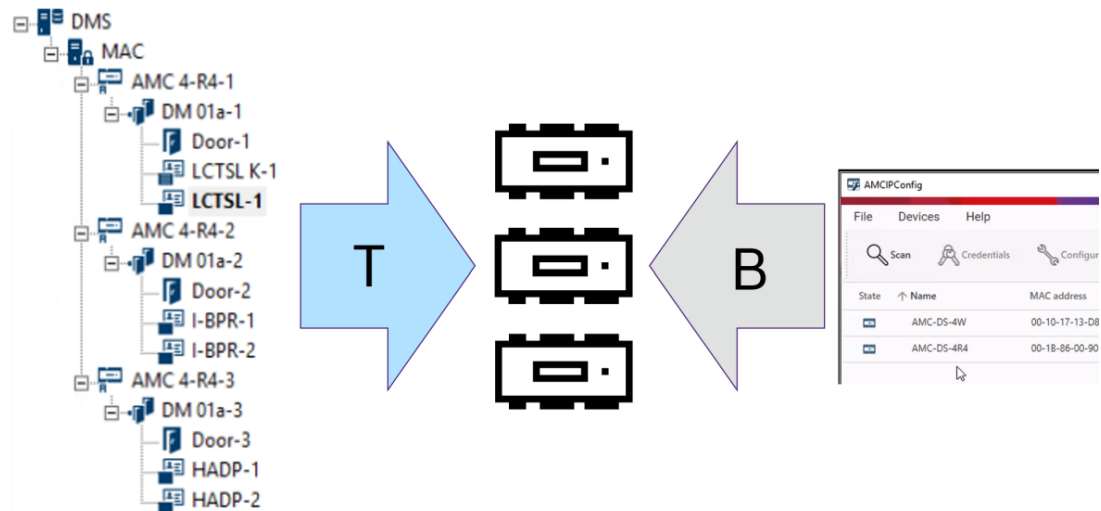
15 Configuring DTLS for secure communication

Introduction

The access control system (ACS) offers highly secure inter-device communication, protected by DTLS. There are two main ways to deploy DTLS communication between the devices in the ACS:

Top-down deployment (T) is done in the device editor in the ACS.

Bottom-up deployment (B) is done mainly in the AMCIPConfig tool, but requires the device editor for completion.



- (T) Top-down deployment can be done in two alternative ways in the device editor:
 - Using a single device communication password (DCP) at the DMS level for all AMCs,
 - Using multiple DCPs for different branches of the device tree, starting at their respective MACs or AMCs.
- (B) Bottom-up deployment can also be initiated in two alternative ways in the AMCIPConfig tool:
 - Using an AMC hardware key
 - Using a random LCD key

Notice!

Bottom-up deployment still requires the setting of DCPs in the device editor.

Bottom-up deployment allows you to set a DCP on the AMC device. You must nevertheless set the same DCP on the same AMC in the device editor also, to enable full DTLS communication between the MAC and AMC.



Summary of DTLS deployment options

	Short description	Advantages	Disadvantages
Top-down	The system administrator enters a strong password in the Device Editor . From this password, the system generates a Master key that it propagates top-down through the tree of access	Fast, simple, deployment.	During the propagation of the master key to the AMC door

	Short description	Advantages	Disadvantages
	control devices, from DMS through the MACs to the AMC door controllers. You can set one password for the entire device tree, or different passwords for different branches of the device tree.		controllers, device communication is not protected by DTLS.
Bottom-up using AMC hardware key	The system administrator uses the AMC IPConfig tool to deploy DTLS at the level of the AMC door controllers.	Greater differentiation and flexibility of deployment. This method avoids the main disadvantage of top-down deployment, namely sporadic unprotected communication of the master key. Nevertheless it requires that the connection from the AMCIPConfig tool to the AMC be secure when it sets the DCP.	During the time when the IPConfig tool sets the DCP on the AMC, you must ensure secure communication by other means. For example, connect the AMC directly to the computer where IPConfig is running. DCPs that you set in the IPConfig tool must also be set on the same AMCs via the device editor.
Bottom up using random LCD key		Greater differentiation and flexibility of deployment. Highest security, because the LCD key is not transmitted via the network at all; therefore the propagation of credentials is protected at all times.	More complicated and time-consuming deployment. You must transfer the 27-symbol random LCD key via some non-network means to the IP Config tool.
Details and instructions are found in the following sections of this chapter.			

DTLS terminology

DCP (Device Communication Password)

A single strong password from which the ACS generates an internal Master key. The password must be kept secure because it is not stored in the ACS.


Master key	A code that the system generates from the DCP, and uses to protect the access control devices. The Master key is never made visible to any user.
Random LCD key	A temporary alphanumeric code that the AMC generates afresh every time it boots. The key can be shown in the liquid crystal display (LCD) of the AMC and may be requested by software tools to authenticate network communication.
AMC hardware key .	An internal authentication code that the AMC generates from certain hardware parameters. It is not visible to the user.

15.1 Top-down DTLS deployment


Prerequisites


- AMS 4.0 or BIS-ACE 4.9.1 or later.
- The tree of access control devices from DMS to AMCs is physically set up, and connected to the network, but the AMCs are not enabled. Enabled means that the AMCs' check boxes **Communication to host enabled** are selected.
- DTLS has not already been configured on the AMCs by one of the bottom-up methods, via the IPConfig tool.

Procedure: One DCP for all

- In the ACS, start the Device Editor
 - BIS Configuration Browser > **Connections**
- AMS Main menu > **Configuration** > **Device data** > **Device tree** 
 - A dialog window appears, inviting you to enter a strong Device Communication Password (DCP).
- To set a single DCP for all the AMCs in the device tree, enter and confirm a strong password according to your local password policies.
 - The dialog gives feedback regarding the strength of the password, based on password entropy .
- Make careful note of the password, because it is not stored in the ACS.
- Click **OK** to close the dialog.

Alternative procedure: Multiple DCPs for different branches of the device tree

- In the ACS, start the Device Editor
 - BIS Configuration Browser > **Connections**
- AMS Main menu > **Configuration** > **Device data** > **Device tree** 
 - A dialog window appears, inviting you to enter a strong Device Communication Password (DCP).
- Click **Cancel** to set different DCPs on different branches of the device tree (MACs and AMCs).
 - A popup dialog advises how many AMCs in the system still have no DCP.

- The device tree opens in the Device Editor.
3. Unfold the device tree to select the MAC or AMC for which you want to set a DCP.
 - If you set the DCP at the level of a MAC, it is set for all the MAC's subordinate AMCs.
 - If you set the DCP at the level of an AMC, it is set for only that AMC.
4. Click the ellipsis button  beside the text field **Device communication password:**
5. Enter and confirm a strong password according to your local password policies.
6. Make careful note of the password and the branch to which it applies, because it is not stored in the ACS.
7. Repeat this procedure for every MAC or AMC for which you want to set a separate DCP.
8. Click **OK** to close the dialog.

Result of top-down deployment

The ACS uses the DCP or DCPs to generate internal keys for all the AMCs below the selected DMS or MAC.

You need not repeat this procedure unless you subsequently change the DCP on one or more AMCs using the AMC IPConfig tool (see "bottom-up" deployment). In that case you must immediately set the same DCP top-down on the same AMCs in the device editor.

If you later add devices in the device tree subordinate to DMSs and MACs that already have DCPs, then the new devices will automatically inherit the same DCP from their superordinate devices.

16 Configuring Entrances

16.1 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:

a	inbound and outbound readers
b	inbound reader and outbound push button
c	inbound OR outbound reader (not both - which would be variant a)
r	(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.

16.2 Creating entrances

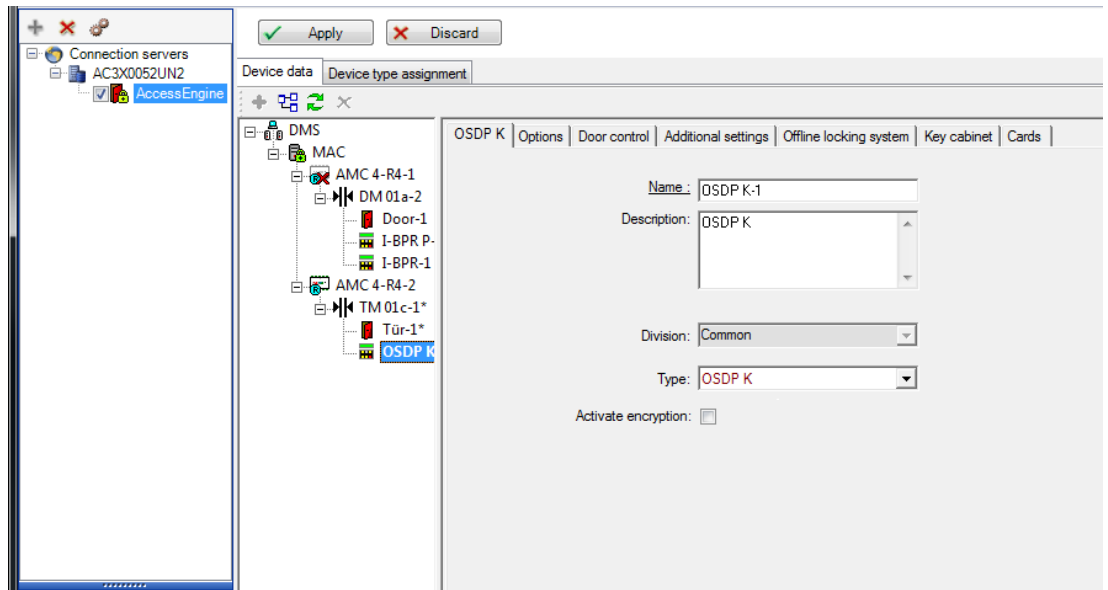
The list of readers presented for selection will be tailored to the controller type you selected.

- 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	OSDP-Protocol	Wiegand-Protocol	LBUS-Protocol	HADP-Protocol
Fingerprint reader BEW2	X	X		
EM Mini Mullion Reader		X		
HADP Reader	X			
HADP Reader, keyboard	X			
HADP Reader, keyboard, display	X			
HID Reader R15	X			X
HID Reader R30	X			X
HID Reader R40	X			X
HID Reader RK40, keyboard	X			X
HID Reader RKL55, keyboard and display	X			X
HID Mini Prox Reader		X		
HID Prox Pointplus Reader		X		
LECTUS duo Reader	X	X		
LECTUS duo Reader, keyboard	X	X		
LECTUS secure 1000 Reader	X	X		
LECTUS secure 2000 Reader	X	X		
LECTUS secure 4000 Reader	X	X		
LECTUS secure 5000 Reader	X	X		
LECTUS secure 9000 Reader		X		
LECTUS select reader	X			

LECTUS select reader with keypad	X			
Morpho Wave MDPI Reader	X	X		
OSDP Reader	X			
OSDP Reader, keyboard	X			
OSDP Reader, keyboard, display	X			
SIGMA Lite Bio/iClass/Prox/Multi Reader	X	X		
SIGMA Lite/Lite+iClass/Prox/Multi Reader	X	X		
STID Keyboard Reader	X	X		
STID Standard Reader	X	X		
STID Mullion Reader	X	X		
Vision Pass MDPI Facial Recognition	X	X		
Wiegand Reader		X		
Wiegand Reader, keyboard		X		
I-BPR Reader			X	
I-BPR Reader with write function			X	
I-BPR Reader, keyboard			X	
HADP				X
HADP K (Keyboard)				X
HADP KD (Keyboard + Display)				X

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



Secure communication with OSDP

By default, the **Activate encryption** check box is cleared. Select it if you are using readers with **OSDPv2 secure** support.

If you later deactivate encryption by clearing the check box, reset the reader hardware, according to the manufacturer's instructions.

As an additional security precaution, any attempt to exchange a configured OSDP reader unit with a different OSDP reader unit generates an alarm in the access control system. The operator can acknowledge the alarm in the client, and simultaneously give permission for the exchange.

Alarm message: **Exchange of OSDP reader refused**

Command: **Allow exchanging the OSDP reader**

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. If you deactivate encryption by clearing the check box on the OSDP tab of the reader in the Device Editor, then reset the reader hardware, according to the manufacturer's instructions.

The screenshot shows a configuration window titled "DM 01a | Terminals". It contains several input fields and dropdown menus:

- Entrance name:** A text box containing "DM 01a".
- Entrance description:** A text box 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
Entrance name	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.
Entrance description	alphanumeric: 0 to 255 characters	An arbitrary descriptive text for display in the system.
Location	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.
Destination	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 Destination .
Waiting time external access decision	Number of tenths of a second	The time for which an access controller waits for a decision from an external system or device that is connected to one of its inputs.
Division	The division to which the reader belongs. Default value is Common	Relevant only if the Divisions feature is licensed.
Arming Area (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.

16.3 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.

T..	entrance	Input signal	entrance	Output signal
#6482	01	Parking-lot 05-1 Door contact	Parking-lot 05-1	Release door
#6482	02	Parking-lot 05-1 "Request to exit" button	Parking-lot 05-1	Door is unlocked
#6482	03	Parking-lot 05-1 Passage locked	Parking-lot 05-1	Stoplight green
#6482	04	Parking-lot 05-1 Passage completed	Parking-lot 05-1	Alarm masking
#6482	05	Parking-lot 05-2 Door contact	Parking-lot 05-2	Release door
#6482	06	Parking-lot 05-2 "Request to exit" button	Parking-lot 05-2	Door is unlocked
#6482	07	Parking-lot 05-2 Passage locked	Parking-lot 05-2	Stoplight green
#6482	08	Parking-lot 05-2 Passage completed	Parking-lot 05-2	Alarm masking
016_002_1	01	Parking-lot 05-1 External access decision accep...	Parking-lot 05-1	External access ...
016_002_1	02	Parking-lot 05-1 External access decision denied	Parking-lot 05-1	External access ...
016_002_1	03	Parking-lot 05-2 External access decision accepted	Parking-lot 05-2	External access deci...
016_002_1	04	Parking-lot 05-2 External access decision denied		
016_002_1	05			
016_002_1	06			
016_002_1	07			

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 the vehicle owner and the license plate are as yet unknown to the access control system, the operator must record them now.

16.4 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	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"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	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"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:

DM 01b		Terminals			
Signal allocation of 'AMC 4-R4' with 8 signal pairing					
B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	DM 01b	Door contact	DM 01b	Release door
0	03	DM 01b	"Request to exit"...		
0	04	DM 01b	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 contact	
"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 long-term locking.
Tamper	Tamper 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.
Suppress alarm from unauthorized opening	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 denies access

Table of output signals

Output Signals	Description
Release door	
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.
Stoplight green	Indicator lamp - will be controlled as long as the door is open.
Max. door open time elapsed or Door security compromised	If the door is held open or open too long
Camera connecting	Camera will be activated at the beginning of a passage.
Release turnstile inbound	
Release turnstile outbound	
Door is unlocked	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"> - Door contact - "Request to exit" button - Bolt sensor - Entrance locked - Tamper - Local open enable - External access decision accepted - External access decision denied 	<ul style="list-style-type: none"> - Release door - Sluice: lock opposite direction - Alarm suppression - Stoplight green - Camera connecting - Max. door open time elapsed or Door security compromised - External access decision activated
03	Revolving door with entry and exit reader Readers for time & attendance External access decision available	<ul style="list-style-type: none"> - Turnstile in rest position - "Request to exit" button - Entrance locked - Tamper - External access decision accepted - External access decision denied 	<ul style="list-style-type: none"> - Sluice: lock opposite direction - Release turnstile inbound - Release turnstile outbound - Alarm suppression - Camera connecting - Max. door open time elapsed or Door security compromised - External access decision activated
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"> - Door contact - "Request to exit" button - Entrance locked - Passage completed - External access decision accepted - External access decision denied 	<ul style="list-style-type: none"> - Release door - Alarm suppression - Stoplight green - Max. door open time elapsed or Door security compromised - Door is unlocked - External access decision activated
06	Readers for time & attendance		
07	Elevator - maximum 56 floors		
09	Vehicle entrance or outgoing reader and push button	<ul style="list-style-type: none"> - Door contact - "Request to exit" button - Entrance locked 	<ul style="list-style-type: none"> - Release door - Alarm suppression - Stoplight green

	Readers for time & attendance External access decision available	- Passage completed - External access decision accepted - External access decision denied	- Max. door open time elapsed or - Door security compromised - Door is unlocked - 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 contact - "Request to exit" button - IDS: ready to arm - IDS: is armed - Tamper - IDS: request to arm - External access decision accepted - External access decision denied	- Release door - Camera connecting - IDS: arm - IDS: disarm - Max. door open time elapsed or - Door security compromised - External access decision activated
14	Simple door with entry and exit reader and IDS arming/disarming Readers for time & attendance	- Door contact - "Request to exit" button - IDS: ready to arm - IDS: is armed - Tamper - IDS: request to arm	- Release door - Camera connecting - IDS: arm - Max. door open time elapsed or - Door security compromised
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.



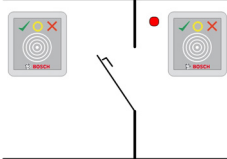
Notice!

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

16.5

Predefined signals for door models

Entrance Model 01



Model variants:

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

Possible signals:

Input signals	Output signals
Door contact	Release door
"Request to exit" button	Sluice: lock opposite direction
Tamper	Stoplight green
Suppress alarm from unauthorized opening	Camera connecting
	Max. door open time elapsed or Door security compromised



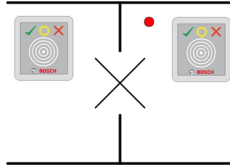
Notice!

Singling functions, especially the lock of the opposite direction, 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:

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

Possible signals:

Input signal	Output signals
Turnstile in normal position	Release turnstile inbound
"Request to exit" button	Release turnstile outbound
Tamper	Entrance locked
Suppress alarm from unauthorized opening	Camera connecting
	Max. door open time elapsed or Door security compromised
Additional signals using mantrap option:	
Entrance locked	Sluice: lock opposite direction
	Alarm suppression

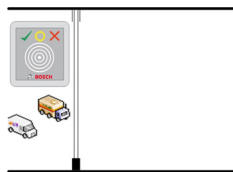
Configuration notes for mantraps:

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:

05c	Parking-lot access entrance or exit reader
------------	---

Possible signals for this entrance model:

Input signals	Output signals
Door contact	Release door
"Request to exit" button	Door is unlocked
Entrance locked	Stoplight green
Passage completed	Alarm suppression
	Max. door open time elapsed or Door security compromised

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

06a	Entry and exit reader for time & attendance
06c	Entry or exit Reader for time & attendance

Readers which are created with this door model do not control doors or barriers, but only forward card data to a time & attendance system. These readers are usually situated in places to which access has already been controlled. Therefore no signals are defined.



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. 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:

<SW_installation_folder>\AccessEngine\AC\TAExchange\

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 contains all bookings in chronological order. The field separator within the file is a semicolon.

Entrance Model 07 variants



Model variants:

07a	Elevator with max. 56 floors
07c	Elevator with max. 56 floors and time model

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

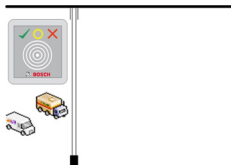
Signals:

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

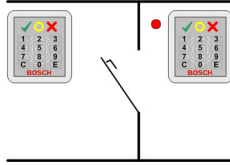


Possible signals:

Input signals	Output signals
Door contact	Release door
"Request to exit" button	Door is open long-term
Entrance locked	Traffic light is green
Passage completed	Alarm suppression
	Max. door open time elapsed or Door security compromised

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:

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

Possible signals:

Input signals	Output signals
Door contact	Release door
IDS: is armed	IDS: arm
IDS: ready to arm	IDS: disarm [only DM 10e]
"Request to exit" button	Camera connecting
Bolt sensor	Max. door open time elapsed or Door security compromised
Tamper	
Suppress alarm from unauthorized opening	
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.

Serial readers (including I-BPR, HADP and OSDP)

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 (#).

Wiegand readers (including serial BPR protocol)

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.]

Special entrances

For entrance-models with special features, such as:

- Elevators
- Intrusion detection
- Generic digital or binary switches
- Mantraps

refer to the dedicated chapter on Special entrances.

Refer to

- *Special entrances, page 92*

16.6

Special entrances

16.6.1

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

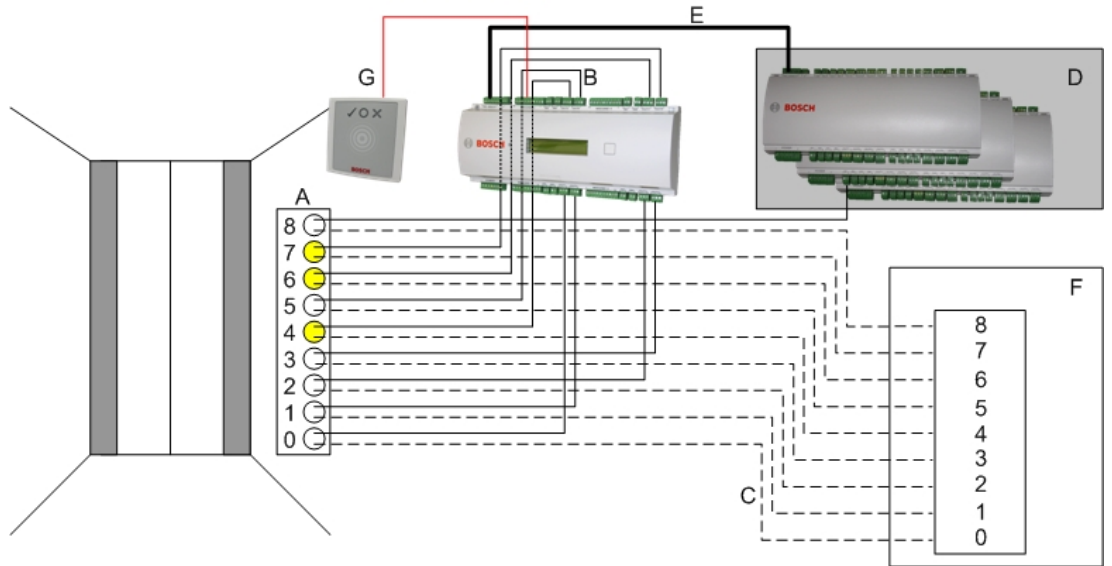
In the access authorization dialogs you can assign specific floors to the authorization of a person.

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:

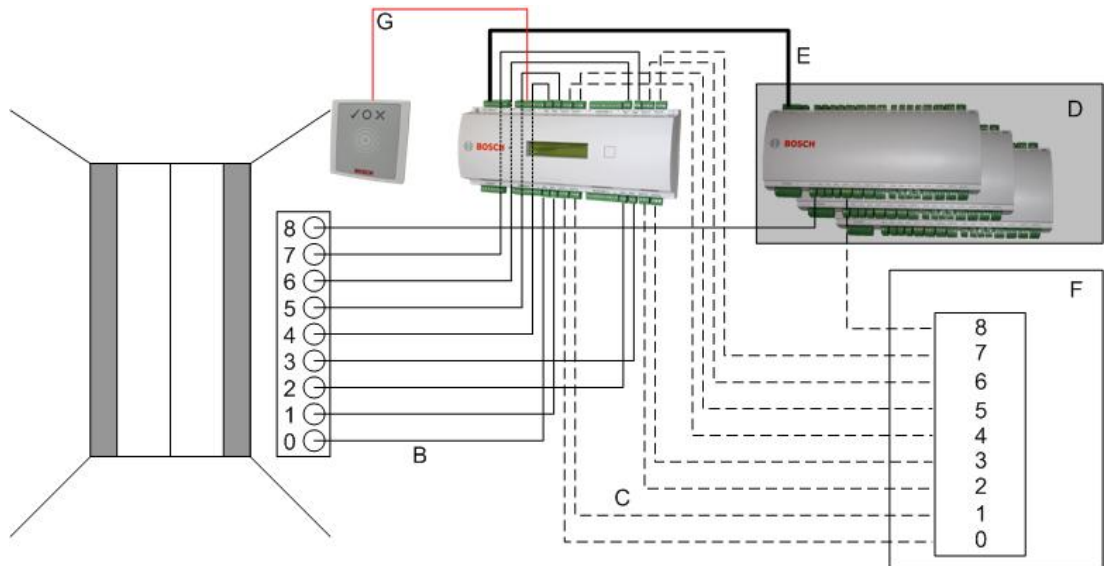
The following picture shows the connection scheme of an elevator using door model 07a.



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.l

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

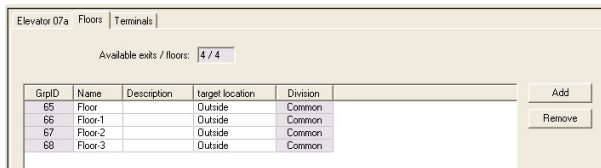
- D = up to three I/O-Boards can be connected to an AMC, if its own eight inputs and outputs are not sufficient.
- E = Data and Power supply from the AMC to the I/O-Boards
- F = The elevator's floor selector
- G = Reader. Two readers are configurable for each elevator.

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.

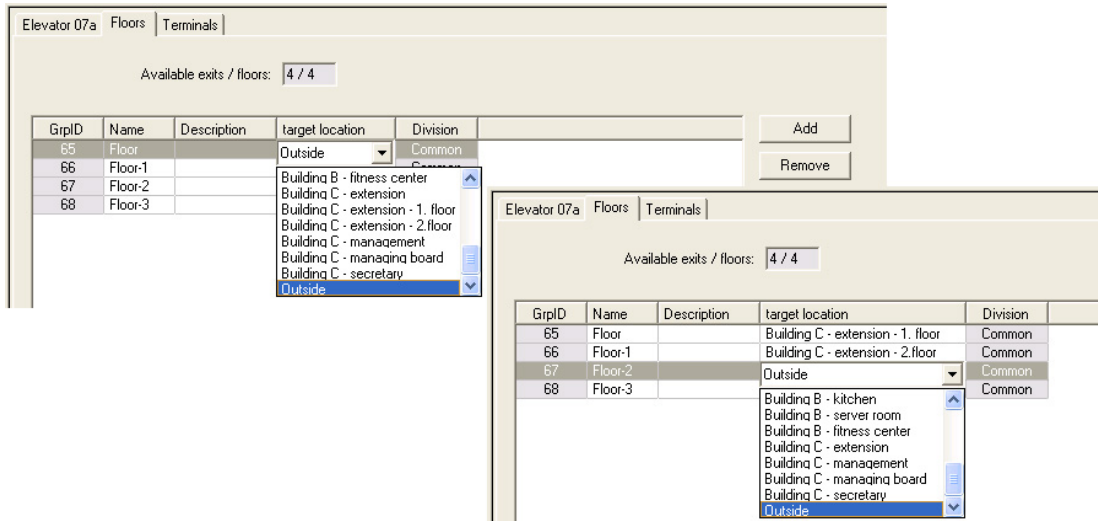
If desired, set a time model for the entrance model: Outside the defined time zones authorizations will be checked.

Floors for entrance model 07

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

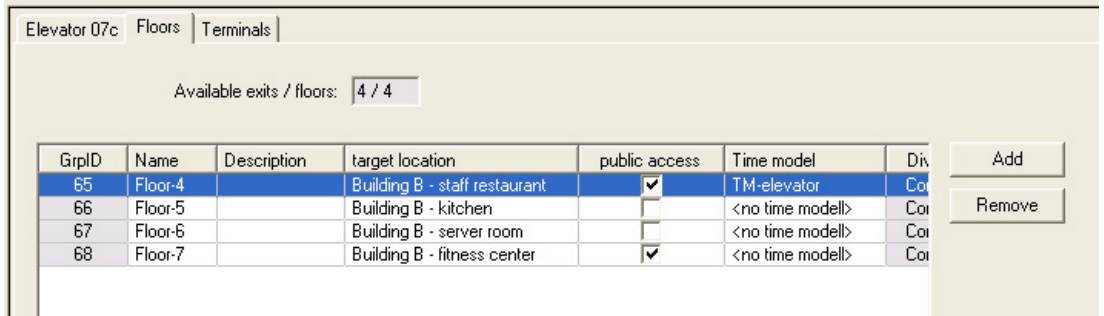


Target locations for a floor can be any **Areas** except parking lots and parking zones. Only one Area can be assigned to an individual floor. The choice of areas offered in the combo-boxes is therefore reduced after each assignment, thus preventing unintentional double-assignments.

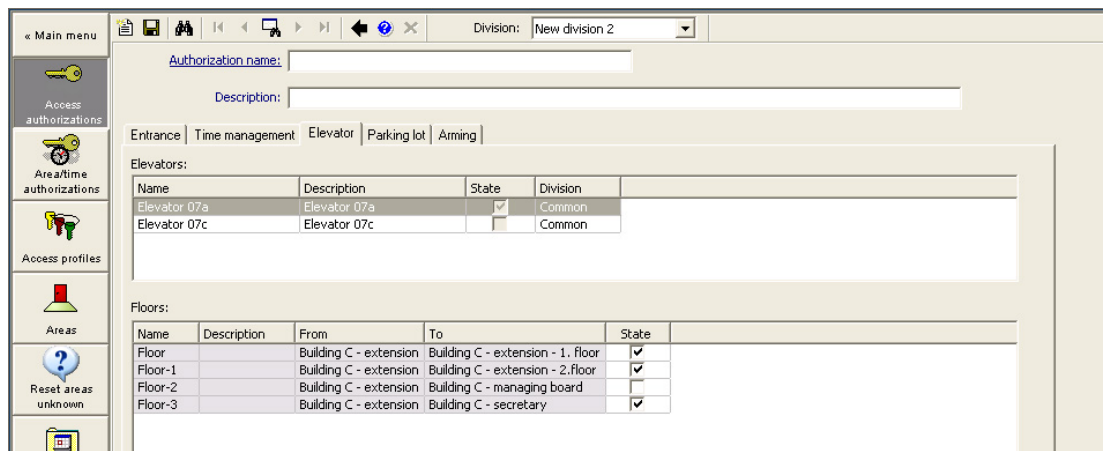


When using entrance model 07a it is possible to make individual floors publicly accessible by checking the **Public access** box. In this case no checking of authorizations takes place.

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 dialogs **Access authorizations** and **Area/time authorizations** select first the required elevator and then, below, the floors to which the cardholder is permitted access.



16.6.2 Door models with intruder alarms (DM14)

Introduction

In contrast to entrance model 10 (DM10), **DM14** can arm and disarm an intruder alarm system, or IDS for a particular Arming area . A DM14 entrance can also be configured to grant access to the cardholder who disarms from it, provided the cardholder has all other access permissions required.

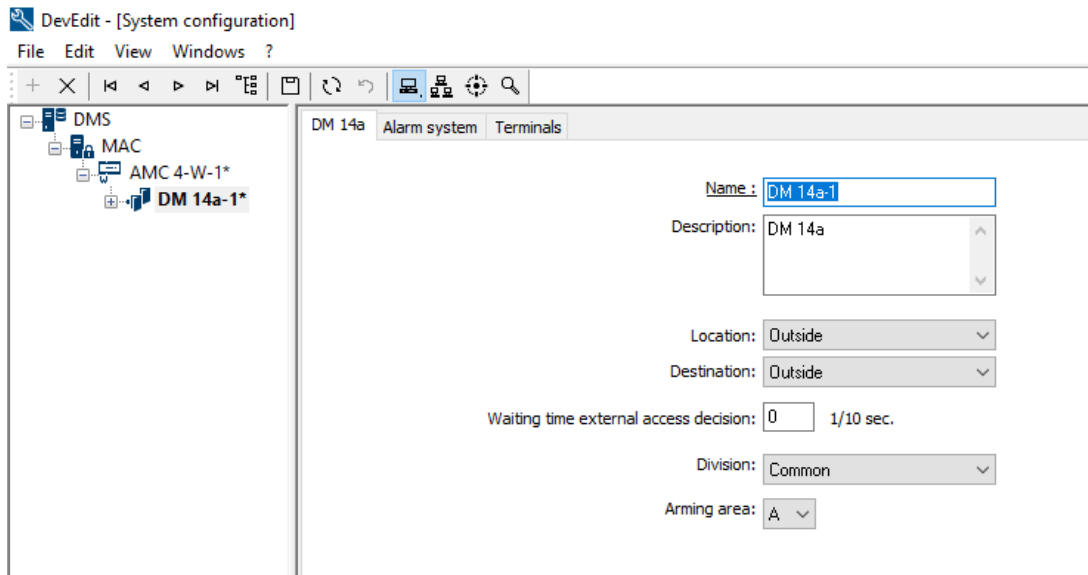
The configuration procedure for DM14 in the device editor and dialog manager includes these tasks:

1. Set general parameters to identify the entrance and its arming area.
2. Set specific parameters to set the exact procedure for disarming the area.
3. Define IDS-specific input and output signals on the terminals of the entrance's door controller.
4. Include arming/disarming permissions in the access authorizations of those cardholders that are to operate DM 14 entrances.

The tasks are described in the following sections.

General parameters

On the first tab, **DM14a** or **DM14b**, set the following parameters.



Parameter	Value type	Description
Name	Free text	The name of the entrance.
Description	Free text, optional	A description of the entrance.
Location	List of defined areas, if used	The access area where the entrance is located.
Destination	List of defined areas, if used	The access area to which the entrance leads.
Division	List of defined divisions, if used	The Division or tenant within the access control system to which the entrance belongs.
Waiting time external access decision	Tenths of seconds	If you have connected an external system to the terminals of the AMC, to make access decisions on its behalf, then this parameter limits the time to wait for a response from the external system. Note: the access decision requires the fulfilment of all conditions defined in the access control system, for example, access authorizations, time models and Divisions (if used). The default value is 0, that is, the parameter is ignored.

Parameter	Value type	Description
Arming area	List of capital letters A...Z	A letter by which to group DM14 entrances into Arming areas .

Alarm-system parameters

On the second tab, **Alarm system**, set the following parameters. These parameters govern the credentials and the procedure for disarming the IDS, and the disarming affects all entrances within the same arming area, as defined on the first tab.

DM 14b Alarm system **Terminals**

Authorizations

Name of disarming authorization: <input style="width: 90%;" type="text"/>	Name of the arming authorization: <input style="width: 90%;" type="text"/>
Description: <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	Description: <div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>

<p>Disarming</p> <p><input type="radio"/> By card alone</p> <p><input checked="" type="radio"/> With card and keypad</p> <ul style="list-style-type: none"> <input checked="" type="radio"/> Confirmation key + PIN code <input type="radio"/> By PIN code alone <input type="radio"/> By confirmation key alone <hr/> <p>Automatic door cycle: <input checked="" type="checkbox"/></p>	<p>Procedure</p> <p><small>With card and keypad</small></p> <ol style="list-style-type: none"> 1. Press confirmation key '7'. 2. Press confirmation key 'Enter' or #. 3. Present the card. 4. Enter PIN code. 5. Press confirmation key 'Enter' or #. 6. The alarm system is disarmed. 7. The door is cycled automatically. <p><small>Confirmation can also be given by an input signal (e.g. from a key switch).</small></p>
---	---

Arming and disarming

Output signal with a 1 sec pulse:

Parameter	Value type	Description
Authorizations pane		
Name of disarming authorization	Free text	A name to appear in protocols and reports when a cardholder disarms the IDS at this entrance.
Name of arming authorization	Free text	A name to appear in protocols and reports when a cardholder arms the IDS at this entrance.
Description (one for each authorization)	Free text, optional	Descriptions of the arming authorizations

Parameter	Value type	Description
Disarming pane		
By card alone	Radio button	Select this option to allow the IDS to be disarmed by presenting a card to the reader, without further authentication.
By card and keypad	Radio button	Select this option to allow the IDS to be disarmed by presenting a card to the reader and giving further authentication via the reader's keypad. The exact authentication and disarming procedure is determined by the following sub-parameters:
Confirmation key + PIN code	Radio button	Cardholders must authenticate themselves using a card, a confirmation key and a PIN code.
By PIN code alone	Radio button	Cardholders must authenticate themselves using a card and a PIN code.
By confirmation key alone	Radio button	Cardholders must authenticate themselves using a card and a confirmation key.
Automatic door cycle	Check box	Select this check box if you want to cycle the door lock upon disarming, to allow the cardholder to disarm and enter simultaneously. Note: the lock will only be cycled if the cardholder also has access permission for this door.
Procedure pane		
Depending on the parameters set in the Disarming pane, this pane shows a standard procedure for disarming the IDS. Communicate this procedure to the cardholders who will be using the DM14 entrances in this Arming area.		
Arming and disarming pane		
Output signal with a 1 sec pulse	Check box	Select this check box if you are using a Bosch B or G-Series intrusion panel. The effect is to send a single pulse signal to toggle the arming state of the entrance's intrusion area, rather than to set the signal to a constant 1 (arm) or 0 (disarm).

Door controller terminals

In order make arming and disarming possible with a DM14 entrance, you must define the IDS input and the output signals that you wish to use on the terminals of the entrance's door controller.

This step is required once for each controller that has DM14 entrances. All subsequent DM14 entrances that you define on the same controller and its extension boards will inherit the signals from the shared controller.

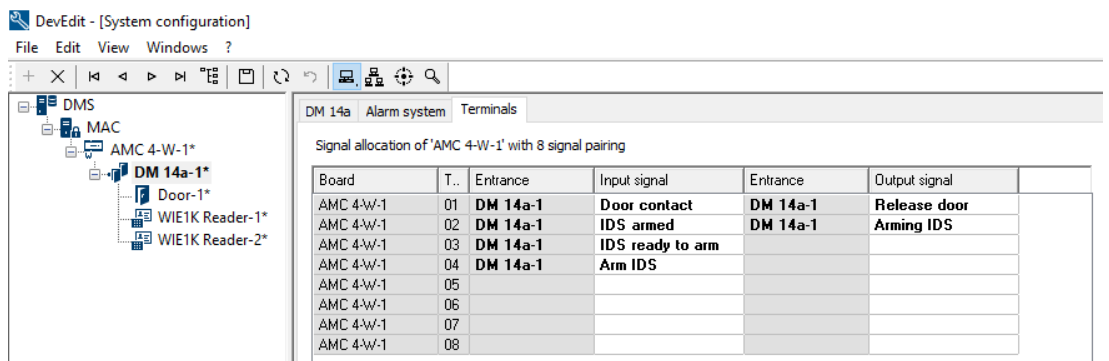
The default signals are described in the following table.

Signal	In/Out	Description
IDS armed	In	The IDS is armed for this intrusion area.

Signal	In/Out	Description
IDS ready to arm	In	No IDS points are in a faulted (open or unready) state.
Arm IDS	In	A request to arm the IDS.
"Request to exit" button (REX)	In	
Bolt sensor	In	A sensor is monitoring the door bolt.
Tamper	In	Tampering has been detected.
Suppress alarm from unauthorized opening	In	Suppress the alarm for a configured number of extra seconds if a REX signal has been given by a motion detector. See REX shunt feature for further details.
Release door	Out	Cycle the door's mechanism to unlocked and back to locked, to allow access.
Arming IDS	Out	Arm or disarm the IDS, depending on its current state (toggle).
Camera connecting	Out	Activate a camera connected to the entrance.
Max. door open time elapsed or Door security compromised	Out	The door is held open, or the system suspects a breach of security at the door.

Procedure to assign signals to terminals

1. Open the 3rd tab, **Terminals**.
 - The terminals of the door controller of this entrance, plus any extension boards that it may have, are displayed in a table.




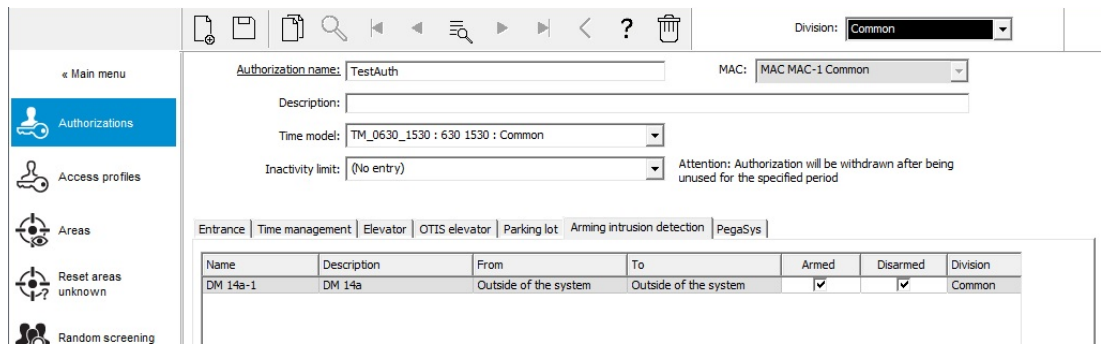
2. Select the line corresponding to the terminal that you want to use for the input signal.
3. In the corresponding cell, in the **Input signal** column, select the desired signal from the drop down list. Note that only hitherto unassigned signals appear in the list.


4. Repeat the previous steps to add any other input signals that you require for this entrance.
5. Repeat the procedure as often as necessary to add to the column **Output signal** any output signals that you require.

Defining authorizations to arm and disarm DM14 entrances

After you have created a DM14 entrance in the device editor, the entrance will be available for inclusion in access authorizations.

1. In the dialog manager, navigate to:
 - Main menu > **System data** > **Authorizations** > tab: **Arming Intrusion detection**
2. Load an existing access authorization into the dialog, or click  (New) to create a new one.
3. Locate the desired DM14 entrance in the list, and select the check boxes **Armed** and/or **Disarmed**.

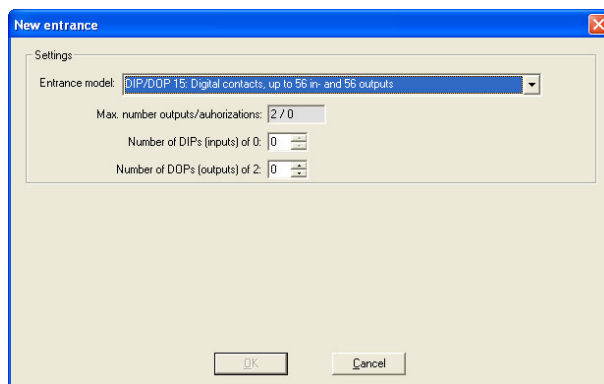


4. Click  (Save) to save the access authorization with the selected permissions.
5. Assign this access authorization to those cardholders that are to operate DM 14 entrances.

16.6.3 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 the device editor.

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).

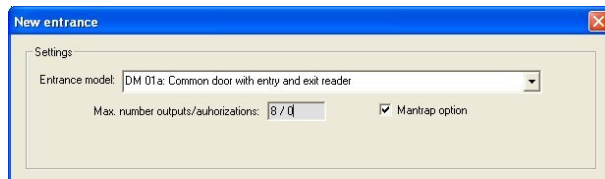
To ensure a restart always resets a DOP to last state that was manually assigned to it, select the DOP in the device tree, and select the check box **Keep state** in the main window.

16.6.4

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.



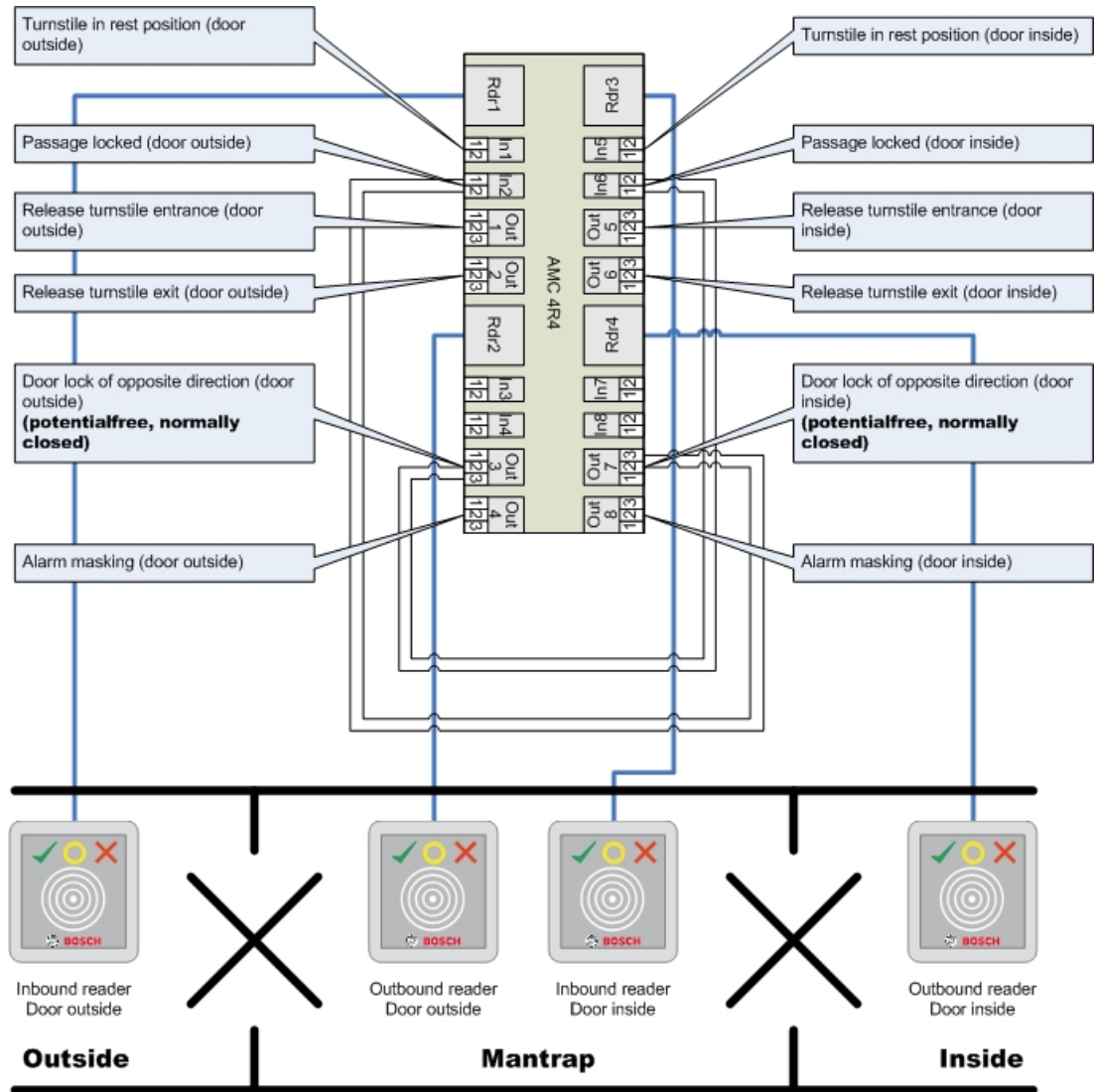
You can combine all model types 01 and 03, but set this option on both entrances belonging to the mantrap.

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.

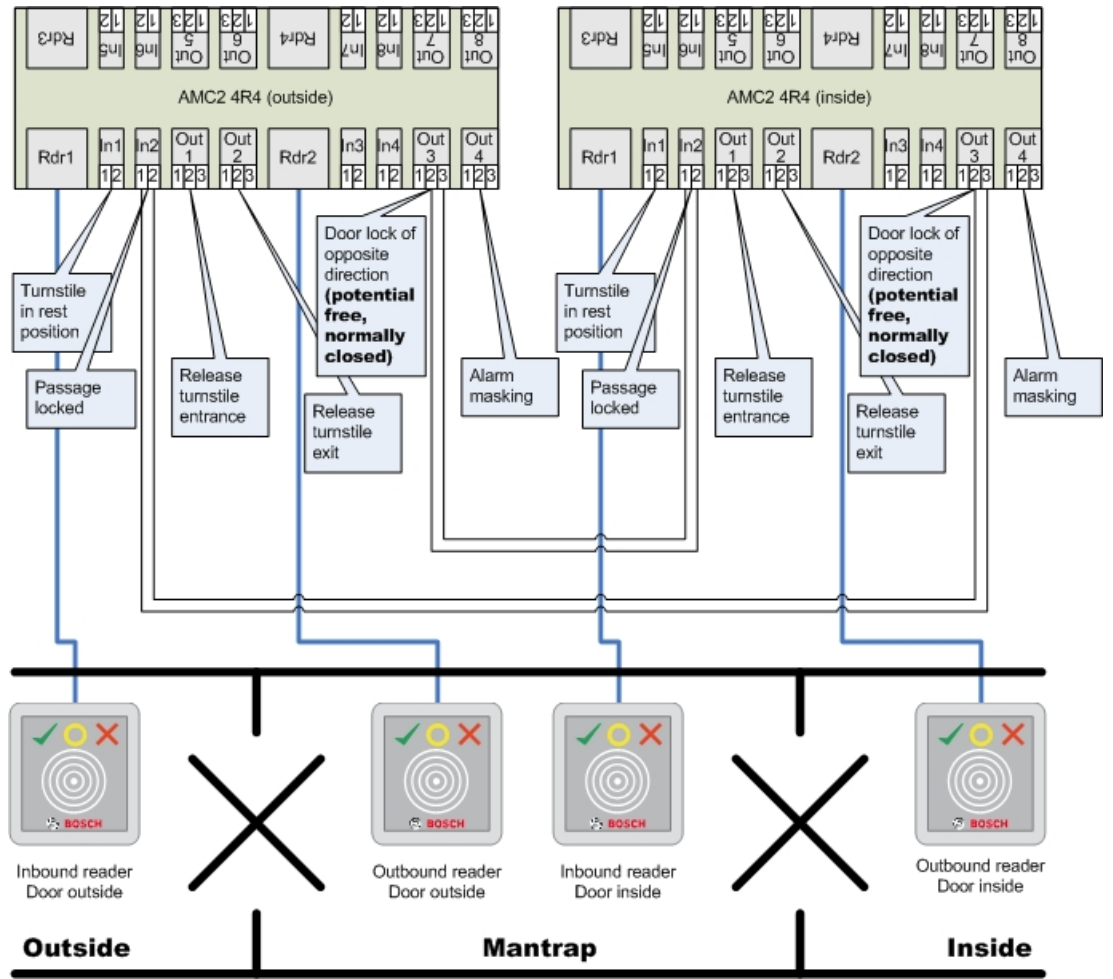


Notice!

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".

16.7

Doors

Tab: Door

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"	Relevant only if the Divisions feature is licensed.
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 both doors. The doors will also require special physical wiring.
----------------	--	--

Tab: Options

Parameter	Possible values	Remarks
Generate message for open/closed	0 = check box is clear 1 = check box is selected.	0 = No message is generated when the door is opened (at an angle to the door frame) or closed (fully latched within the door frame). 1 = the corresponding messages are generated in the event log.
Door set to manual	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.
Door mode	0 = Door is in normal mode 1 = Door is unlocked 2 = Door is unlocked depending on time model 3 = Door is open depending on time model after first passing through 5 = Door is blocked long-term 6 = Door is blocked 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. 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. 5 = blocked (excluded from access control system) until manually unblocked. 6 = blocked (excluded from access control system) as long the time model is active - there is no door control, the door cannot be used while the time model is active.
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. duration of pulse to door strike:	0 - 9999	Maximum duration of the unlock signal. Unit 1/10s. Default values: 50 for doors, 10 for revolving doors (door model 03), and 200 for barriers (door models 05c or 09c).
Min. duration of pulse to door strike:	0 - 9999	Minimum duration of the unlock signal in 1/10s. Default: 10.
Prefixed alarm suppression	0 - 9999	Additional alarm suppression before pulse to door strike. ($\$PARAMETER_WAITEMA$) In very rare cases where a door strike may react more slowly than an intrusion alarm, it is possible to suppress the alarm temporarily before sending the unlock signal to the door. Unit: 1/10 sec. Default 0. A value of 20, that is 2s, is normally sufficient for even very slow doors.
Suffixed alarm suppression	0 - 9999	Additional alarm suppression after pulse to door strike. ($\$PARAMETER_OPENINRT$) After the pulse to door strike (the unlock signal) has passed, the door can be opened within this timespan, without triggering an alarm. Unit: 1/10s. Default: 0.
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-frame sensor is present	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = door has no frame contact 1 = door has a frame contact. A closed contact usually means that the door is closed. (= default)
Bolt sensor is present	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 (default) = door has no bolt sensor 1 = door has a bolt sensor. A message is issued when the door is bolted or unbolted.
Extended door open time (handicapped persons)	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = The unlock signal has the standard duration, which is set on the door parameter "Max. lock activation time", that is, the duration of the pulse to the door strike. 1 (default) = the duration of the unlock signal is multiplied by the factor set on the MAC parameter " Time factor for handicapped persons " (tab: Global access)

		<p>settings). A value of 0 on that MAC parameter puts extended door open times out of operation.</p>
--	--	--

Tab: Door security

Parameter	Possible values	Remarks
Generate message for "Door forced open"	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 = (default) Upon unauthorized opening a message will be issued, followed by another message when the door closes.
Generate message for "Door held open" after:	0 - 9999	If the door stays open after this timespan, a message is issued, to warn that the door has remained open too long. Unit: 1/10s. Default: 300. 0 = No timeout, no message.
Extension of alarm suppression for "Door forced open"	0 - 9999	Used in the "REX shunt" feature: Unit = 1/10s. Default 0. After a REX signal from a motion detector, if the door closes again within this timespan then the usual message <code>Unauthorized opening of door N</code> is replaced by the message: <code>Door N opened (in alarm suppression mode)</code> where N is the number of the door.
Generate local alarm for "Door forced open"	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Prerequisite: the check box Generate message for "Door forced open" on this dialog is selected (see above). 0 = (default) the readers connected to this door do not sound a local alarm. 1 = the readers connected to this door sound a local alarm if the door is forced open.
Generate local alarm for "Door held open" after:	0 - 9999	If the door stays open after this timespan, then the readers connected to this door sound a local alarm. Unit: 1/10s. 0 = (default) No local alarm.

16.7.1 REX shunt

Introduction

At entrances where there is no security risk in opening a door manually from the inside, a motion detector often takes the place of a REX button, to unlock the door. For this common scenario, the ACS provides a simple means of extending the duration of the REX signal from the motion detector, while simultaneously shunting (suspending) the *Door forced open* alarm.

This feature is known as "REX shunt".

When the feature is in operation, cardholders leaving through the door within the duration of the shunt will generate the access event

Door N opened (in alarm suppression mode) rather than the event
Unauthorized opening of door N.



Notice!

REX shunt in combination with armed intrusion detector systems

The REX shunt feature suspends alarms for the duration set in the parameter:

Device Editor > ... > **Door** > tab: **Door security** > **Extension of alarm suppression for "Door forced open"**

regardless of whether that door is currently armed as part of a burglar alarm system.



Prerequisites

- Configured doors of the following types: 01a, 01b, 01c, 03a, 03b, 03c, 10a, 10b, 10e, 14a, 14b
- The physical door is fitted with a motion detector, rather than an REX button, to unlock the door. Set the duration of the signal from the motion detector to at least 1 second.

Dialog path

- **Main menu** > **Configuration** > **Device data**
- **BIS Configuration browser** > **Connections** > **Device data**

Procedure

1. In the device editor, navigate to the desired entrance (a direct child node of a door controller).
2. On the **Terminals** tab of the entrance create a new input signal of type:
Suppress alarm from unauthorized opening
3. Click  (Save) to save the changes.
4. Select the door that is within the desired entrance
5. On the **Door security** tab of the door, set a value for the parameter **Extension of alarm suppression for "Door forced open"**
 - The value is in tenths of a second.
 - The default value is 0. That is, by default there is no extension of alarm suppression after the cardholder leaves the sensitive area of the motion detector.
6. Click  (Save) to save the changes.

16.7.2 Configuring doors to sound local alarms

Introduction

For the following door states, the ACS provides a means of sounding the alarms in all the readers connected to the door.

State	Local alarm response
Door forced open	The alarm sounds for 17 seconds or until the door closes.
Door held open	The alarm sounds until the door closes.

Prerequisites

- The readers use either OSDP or Wiegand protocol
- Alarm sounders are present in the readers and electrically connected to the door controller.
- AMC firmware version 02.38 or later.

The following reader types are **not** supported:


- IDEMIA readers
- Suprema readers with Wiegand protocol
- LBUS readers
- BG900 readers

Dialog path

- **Main menu > Configuration > Device data**
- **BIS Configuration browser > Connections > Device data**


Procedure for Door forced open

1. In the device tree, select the door that you wish to configure.
2. On the **Door security** tab of the door, select the check box **Generate message for “Door forced open”**
3. Select the check box **Generate local alarm for “Door forced open”**
The default value is 0 (the check box is clear). This means that by default no local alarm is sounded.

4. Click  (Save) to save the changes.

Procedure for Door held open

1. In the device tree, select the door that you wish to configure.
2. On the **Door security** tab of the door, set a non-zero value for **Generate local alarm for “Door held open” after:**
 - The value is in tenths of a second.
 - The default value is 0. This means that by default no local alarm is sounded.

3. Click  (Save) to save the changes.

16.8 Readers

Configuring a Reader: General Parameters

I-BPR K Options Door control Additional settings Cards

Name : I-BPR K

Description: I-BPR K

Division: Common

Type: I-BPR K

Activate encryption: Supported only by OSDP v2 readers.

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:

Time model for PIN codes:

Access also by PIN code alone:

Reader terminal / bus address:

Attendant required:

Membership check:

Membership time model:

Group access:

Deactivate reader beep if access granted:


Deactivate reader beep if access denied:

VDS - Mode:

Max. time for arming: 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 PIN code required parameter is set to 2.
Access also by PIN code alone	0 = deactivated (checkbox is clear) 1 = activated (checkbox 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	<p>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.</p> <p>IMPORTANT Membership check only works with physical credentials where the card definitions are predefined in the system (gray background), not with customized definitions or biometric credentials.</p> <p>0 - no check Membership check is off, but the card is checked for authorizations as normal (default)</p> <p>1 - check The card is checked only for company ID, that is for membership of the system.</p> <p>2 - depending on time model The card is checked for company ID (membership) but only during the period defined in the membership time model.</p>
Membership time model	one of the available time models	<p>The time model enables/disables the membership check.</p> <p>The selection of a time model is mandatory for Membership check option 2.</p>
Group access	1 - 10	<p>For readers with keypad: Minimum number of valid cards which must be presented to the card reader before the door is opened. The group can consist of 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>For readers without keypad: 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	0 = deactivated (check box is clear) 1 = activated (check box is selected)	If activated (1) the reader remains silent if an authorized user is granted access.
Deactivate reader beep if access not granted	0 = deactivated (check box is clear) 1 = activated (check box is selected)	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	0 = deactivated (check box is clear) 1 = activated (check box is selected)	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
Templates on server	
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.
Templates on device	
Person dependent verification	The reader allows settings of the individual cardholder to determine which Identification mode it uses. The personnel data offers the following options:

Parameter	Description
	<ul style="list-style-type: none"> - Fingerprint only - Card only - Card and fingerprint 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 set an entrance to Office mode. The reader must have a keypad. When this parameter is activated, a suitably authorized cardholder switches office mode on and off by pressing key 3 before presenting their card. See <i>Authorizing persons to set Office mode, page 202</i>
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) (IMPORTANT: Activation of this option is required for additional video verification by the operator of a Bosch BVMS or Bosch access control system).
Host request timeout	0 = deactivated	0 = AMC works without host verification (does not work with <i>Area Change</i> or <i>Person Counting</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 x 1/10 of a second. (Default = 330 =33 seconds). The reader requests confirmation from the access control system. If the confirmation is not received within this time, the AMC checks the parameter Open door if no answer from host and grants or denies access accordingly.
Open door if no answer from host	0 = deactivated (check box is clear)	This control is only active, if the parameter Host verification is set.

	1 = activated (default) (check box is selected)	0 = does not open the door if the host system fails to confirm before timeout. 1 (default) = opens the door after time out if the host system fails to confirm before timeout.
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:

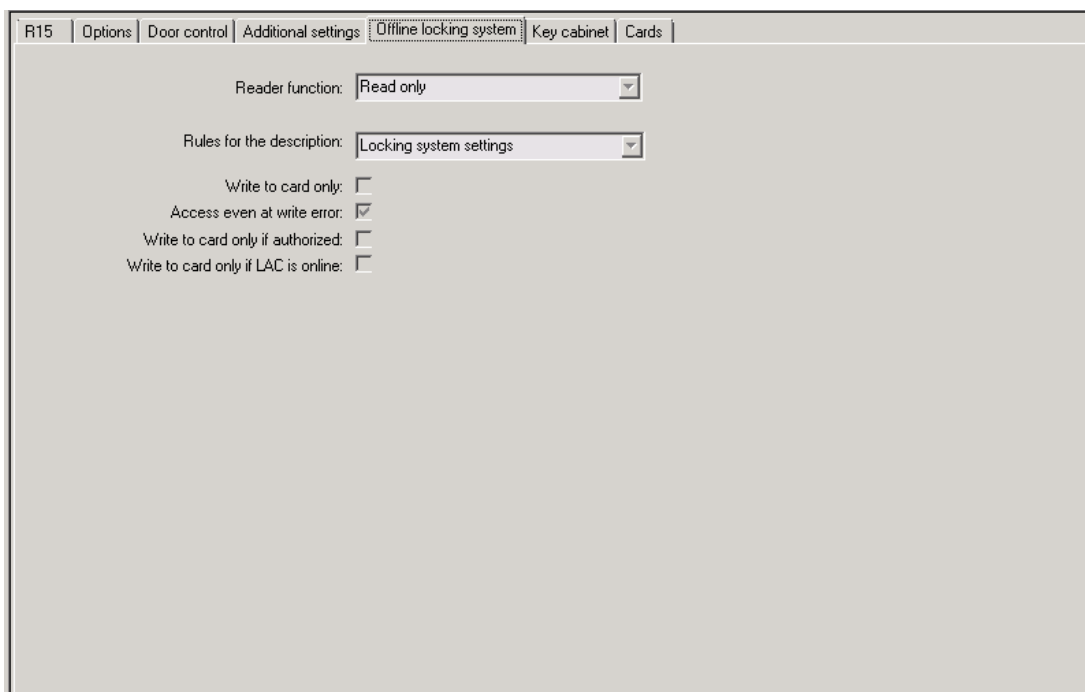
Read permanently:

Parameter	Possible values	Remarks
Access sequence check	0 - Deactivated 1 - Activated; deactivate upon LAC malfunction	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:

	<p>2 - Activated; leave active upon LAC malfunction</p> <p>3 - Activated; use strict sequence checking even when LAC malfunctions (note: update person's location manually)</p>	<p>1 = The first reading of the card will be down without checking the location. All controllers must be online.</p> <p>2 = The first reading of the card will be down without checking the location.</p> <p>3 = Checking the location will be down for every reading the card during LAC malfunction.</p>
		
<p>There is a MAC command to activate or deactivate all access sequence checking generally. 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>Note: This command can modify access sequence checking only for those readers where the parameter Enable access sequence is set. It does not deactivate/activate access sequence checking for <i>all</i> readers.</p>		
Time Management	<p>0 = deactivated (check box is clear)</p> <p>1 = activated (check box is selected)</p>	<p>If selected the access control system collects data for Time and Attendance management.</p>
<p>Double access control (anti-passback control)</p>		
Enable	<p>0 = deactivated (check box is clear)</p> <p>1 = activated (check box is selected)</p>	<p>0 = without double access control (= default)</p> <p>1 = with double access control</p> <p>Within the time span set by the Duration parameter, this reader and other readers in the group cannot be used with the same card.</p> <p>If this parameter is activated, a door group ID must be used, even if only one reader is used.</p>
Door group ID	<p>Letters A - Z and a - z, and "-"</p> <p>2 characters</p>	<p>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.</p>

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 Blocking .
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 DM10 and DM14 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.
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: Offline Locking System



R15 | Options | Door control | Additional settings | **Offline locking system** | Key cabinet | Cards

Reader function: Read only

Rules for the description: Locking system settings

Write to card only:

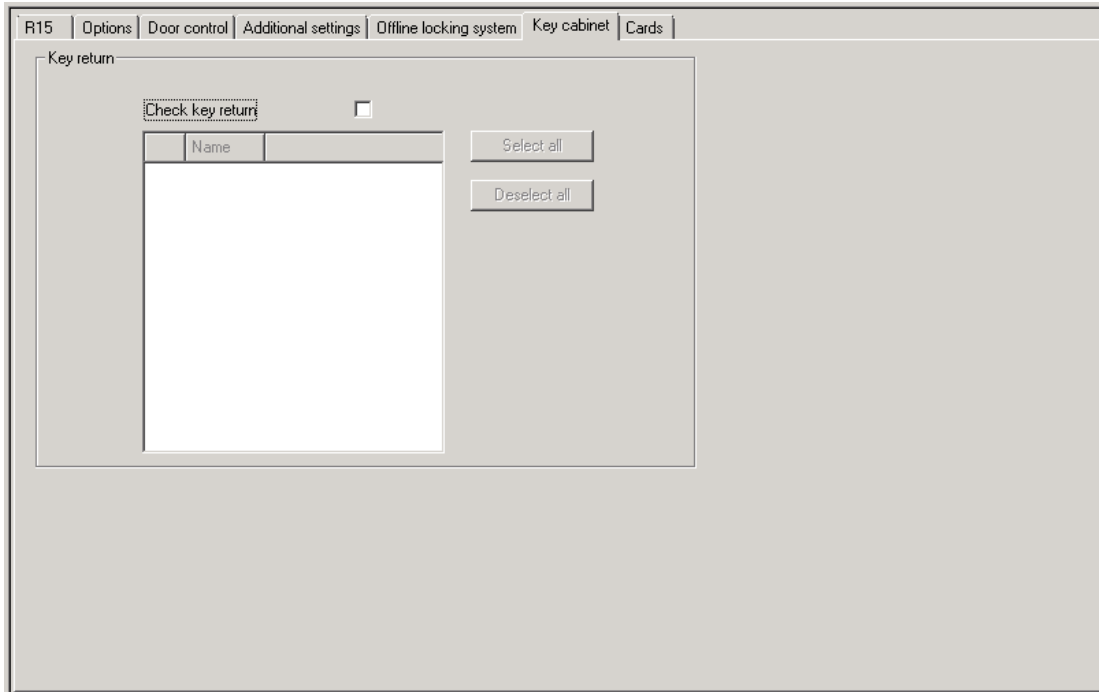
Access even at write error:

Write to card only if authorized:

Write to card only if LAC is online:

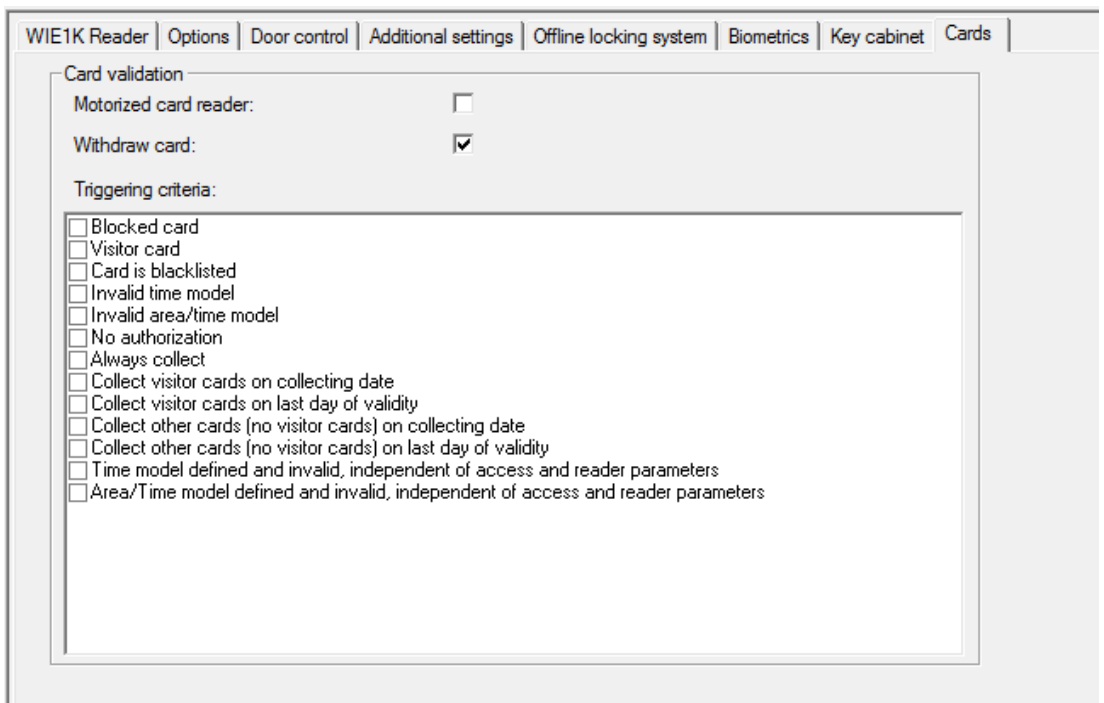
Parameter	Possible values	Remarks
Reader function		This box must be selected if a motorized card reader is used
Rules for the description		“Withdraw” means to make the card invalid.
Write to card only	0 = deactivated (check box is clear) 1 = activated (check box is selected)	
Access even on write error	0 = deactivated (check box is clear) 1 = activated (check box is selected)	
Write to card only if authorized	0 = deactivated (check box is clear) 1 = activated (check box is selected)	
Write to card only if LAC is online	0 = deactivated (check box is clear) 1 = activated (check box is selected)	

Configuring a Reader: Key cabinet



Parameter	Possible values	Remarks
Check key return	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Instructs the access control system to ensure that a key has been returned to a Kemas key cabinet before allowing the keyholder to leave the premises.

Configuring a Reader: Cards



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 Withdraw card .

**Notice!**

Motorized card readers can only be used with IBPR readers.

Refer to

- *Authorizing persons to set Office mode, page 202*

16.8.1**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.

16.9 Access by PIN alone

Background

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


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

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

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

Prerequisite authorization for Operators

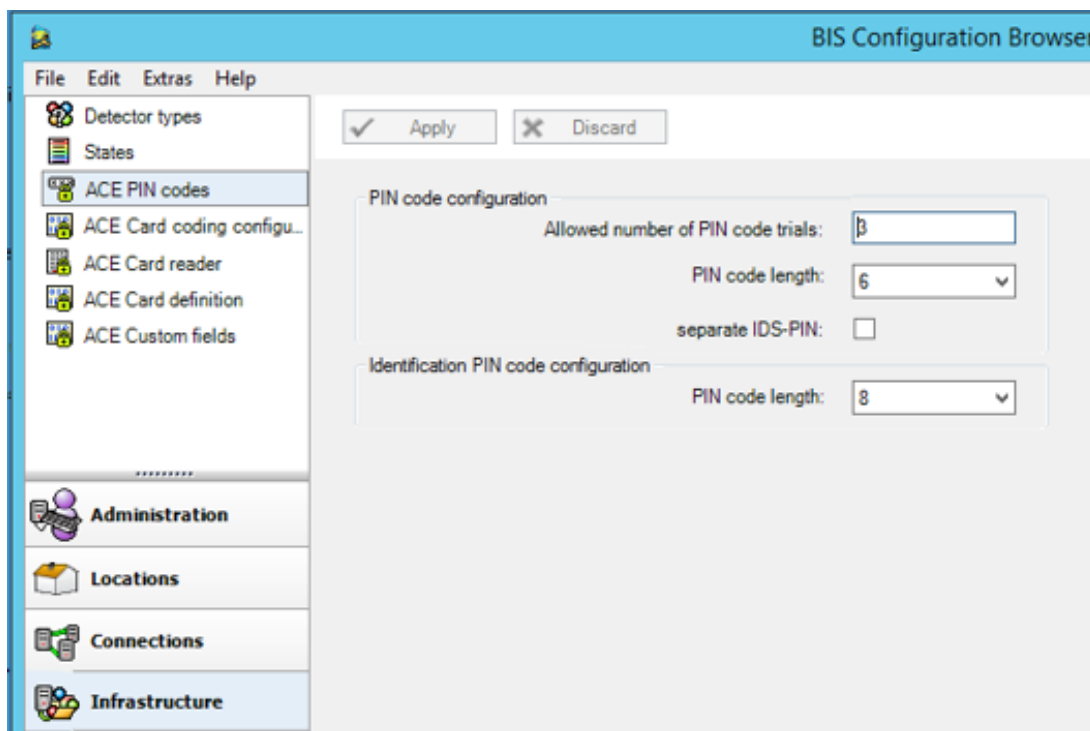
Authorization for a cardholder to access by PIN alone is only grantable by operators with the special authorization to assign virtual cards. To give an operator this authorization, proceed as follows.

1. In the BIS Configuration Browser navigate to **Administration > ACE User profiles**
2. Navigate to Main menu > **Configuration > Operators and workstations > User profiles**
3. 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.
4. 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.
5. In the Special functions pane select the check box for **Assign virtual cards (PIN)**
6. 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.

- BIS Configuration Browser dialog
Infrastructure > ACE PIN Codes > (the lower dialog pane)
Identification PIN code configuration > PIN code length
- Main menu > **Configuration > Options > PIN codes > PIN code length**



Configuring a reader for access by PIN alone

1. In the BIS Configuration Browser navigate to **Infrastructure** > **ACE Card reader**.
2. Navigate to Main menu > **Configuration** > **Device data** > **Workstations** tree 
3. In the **Workstation** pane select the workstation to which the reader is physically connected.
4. Right-click the workstation and add a reader of type **Dialog Enter PIN** or **Dialog Generate PIN**.
5. Select the reader in the **Workstations** pane.
A custom reader configuration pane appears to the right of the **Workstations** pane.
6. Verify that the drop-down list **Card usage default** contains the default value **Virtual card. Use PIN as card**.
7. Click  or **Apply** to save your changes
8. In the BIS Configuration Browser navigate to **Connections**.
9. In the device editor DevEdit, navigate to the **Device configuration** tree 
10. Select the reader at the entrance where you wish to configure access by PIN alone.
11. In the **Options** tab, select the check box **Access also by PIN code alone**.
12. Click  or **Apply** to save your changes

16.10

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**.

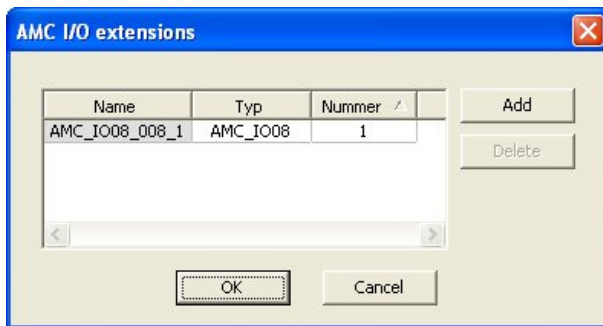


Notice!



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

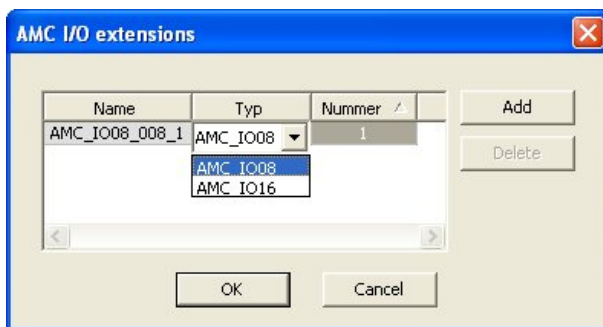
A selection dialog for the creation of the extensions appears.



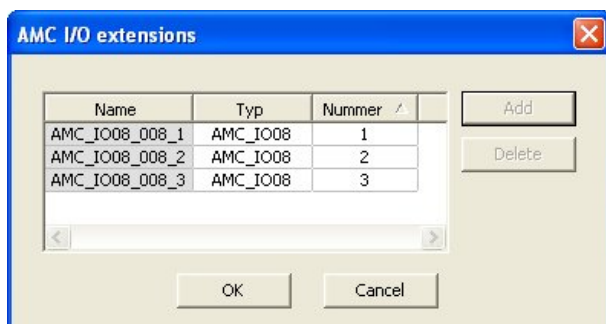
AMC-EXT is available in two variants:

- 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.

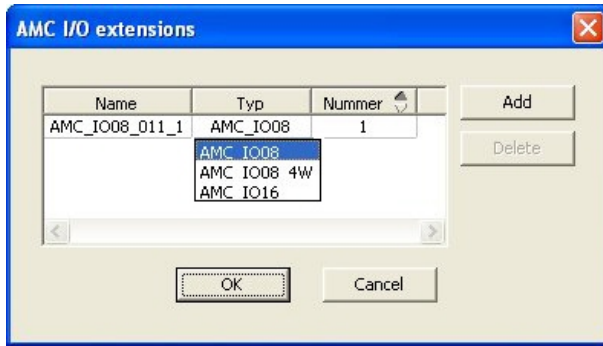
To create an AMC2 4W-EXT in the system right-click the desired parent AMC2 4W in the Explorer and select **New object > New extension board** from the context menu.



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 AMC 2 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	Relevant only where the Divisions feature is license.

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.

17 Custom reader configurations

17.1 Introduction

As of BIS 4.9, and AMS 4.0, Bosch access control systems allow the use of customized MIFARE DESFire settings. You can create encrypted parameter files by using the auxiliary tool `Bosch.ReaderConfigTool.exe`. This tool is included in the setups for BIS ACE 4.9, AMS 4.0 and later versions, with its own documentation. Consult that documentation for the current list of compatible readers

The following sections describe how to use the Device editor to import an encrypted parameter file and apply it to any or all compatible readers in the hierarchy of access control devices.

17.2 The reader property: Extended reader parameters

The available extended parameter sets for compatible readers are displayed on their property pages in the device editor under the label **Extended reader parameters**.

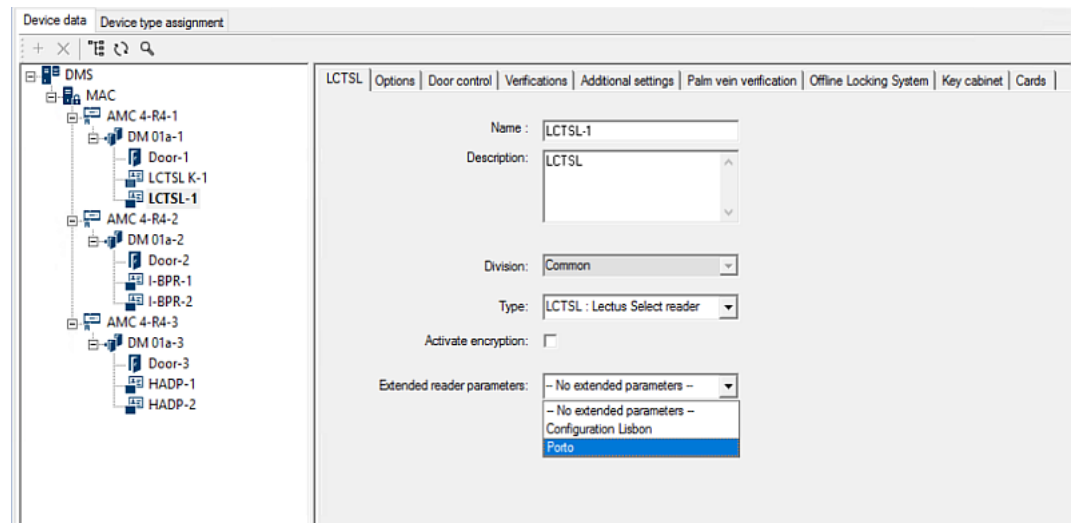


Figure 17.1: Extended reader parameters

The default value of the dropdown list is `No extended parameters`. This is the only possible value unless you import additional parameter sets.

Procedure

To apply an imported parameter set to a compatible individual reader:

1. In the Device editor, select the reader in the device tree
2. Select the first property tab
3. Select the required parameter set from the list **Extended reader parameters**

4. Click **Apply** or 

17.3 Importing a reader parameter set

You import and delete parameter files only at the DMS level of the device hierarchy.

Prerequisites

Access to an approved parameter file for your access control system. By default the file is of type `.ReaderConfigSave`

Procedure

1. In the Device Editor, right-click the DMS node and select **Import reader parameter sets** from the context menu.
The popup window **Import reader parameter sets** appears.
2. Click **File** and locate the parameter file by use of the file explorer.
3. When prompted, enter the password of the parameter file.
If the password is correct, the lower half of the popup window is populated with the following information:
 - A list of the reader types to which the parameter set applies.
 - The name of the parameter set. You can edit it in this dialog.
 - A free-text description, if the creator of the parameter set provided one. You can add or edit a description in this dialog.
4. Click **Import** to import the parameter set for possible future use by the access control system.
 - The parameter set is imported and stored in the access control system.
 - It is added to the list of available parameter sets at the top of the popup window.
5. Click **Exit** to exit the popup window **Import reader parameter sets**.

17.4**Applying a parameter set to readers****Introduction**

Importing a parameter set into the access control system stores it for future use, but does not apply it to readers in the system. Applying the parameter set is an extra step that you can perform at different levels in the device hierarchy:

- DMS
- MAC
- AMC

When you apply a parameter set at the DMS, MAC or AMC level, it can apply only to subordinate readers of reader types for which the set was created. All other subordinate readers remain unaffected.

Prerequisites

You have successfully imported a reader parameter set.

Procedure


1. In the Device editor, select right-click a reader or a device (DMS, MAC or AMC) whose readers you want to parameterize.
2. Select **Manage reader parameter sets** from the context menu.
3. In the upper list pane, **Parameter sets for reader types**, select the parameter set that you want to apply.
Applicable readers are listed in the bottom left pane: **Readers parametrizable with this parameter set**.
4. In the list **Readers parametrizable with this parameter set**, select those readers to which you want to apply the selected parameter set.
 - If the number of readers is large, use the drop-down lists to restrict the display to subordinates of a particular MAC or AMC.
5. Use the arrow buttons to move selected readers into the bottom right pane, **All readers parametrized with the selected parameter set**.

**Notice!**

Display of compatible readers

Only readers that are compatible with the parameter set will be listed. If you select the check box **Show all readers** then readers that have other parameter sets will also be displayed. These have a gray background to mark them as read-only for the selected parameter set.

6. Click **OK** to close the popup window.

7. Back in the Device editor, click **Apply** or 

The parameter set is applied to all the readers that you left in the list **All readers parametrized with the selected parameter set** in the popup.

17.5

Managing reader parameter sets

Introduction

You can change the application of parameter sets at different levels in the device hierarchy:


- DMS
- MAC
- AMC

Changes at the DMS, MAC or AMC level, can apply only to subordinate readers of reader types for which the set was created. All other subordinate readers remain unaffected.

Prerequisite

You have successfully imported a reader parameter set.

Procedure

1. In the Device editor, right-click a reader or a device (DMS, MAC or AMC)
2. Select **Manage reader parameter sets** from the context menu.
3. In the upper list pane, **Parameter sets for reader types**, select the parameter set that you want to apply.
 - Applicable readers are listed in the bottom left pane: **Readers parametrizable with this parameter set.**
 - Readers to which the parameter file has already been applied are listed in the bottom right pane: **All readers parametrized with the selected parameter set.**
4. Select readers in either list. Use the arrow keys to move readers into and out of the bottom right list, **All readers parametrized with the selected parameter set.**
 - IMPORTANT: Make careful note of readers that you take out of the list, for the last step in this procedure.
5. When you have completed your changes, click **OK** to close the popup window.
6. Back in the Device editor, click **Apply** or 
 - The parameter set is applied to all the readers that you left in the list **All readers parametrized with the selected parameter set.**
 - It is removed from the readers that you took out of this list.
7. Do one of the following to all the readers that you took out of the list:
 - Reset factory defaults by using the DIP switches in the reader hardware.
 - Apply a different parameter set to them.

**Notice!**

The deletion of a parameter set does not reconfigure the readers that used it. The deleted reader configuration will persist in the readers that used it until you reset the reader hardware, or apply a different parameter set.

17.6

Deleting reader parameter sets

You import and delete parameter files only at the DMS level of the device hierarchy.

Prerequisites

At least one parameter file has already been imported into your access control system.

Procedure

1. In the Device Editor, right-click the DMS node and select **Delete reader parameter sets** from the context menu.

The popup window **Delete reader parameter sets** appears.

2. In the **Parameter sets for reader types** list, select the parameter set that you wish to delete.
 - In the lower right of the popup window, a list appears of all readers that are currently parameterized (configured) with the selected parameter set.
 - Make careful note of these readers, they will require reset or reconfiguration after you delete the parameter set. See the last step in this procedure for details.
3. Click **Delete**
4. Click **Exit**

5. Back in the Device editor, click **Apply** or



6. Do one of the following to all the readers that were using the deleted parameter set:
 - Reset factory defaults by using the DIP switches in the reader hardware.
 - Apply a different parameter set to them.

**Notice!**

The deletion of a parameter set does not reconfigure the readers that used it. The deleted reader configuration will persist in the readers that used it until you reset the reader hardware, or apply a different parameter set.

18 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 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 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.

18.1 Previewing and editing Custom fields

Dialog path

- In the Configuration Browser, navigate to the **Infrastructure** menu > **ACE Custom fields**
- 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 client software.

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

Previewing

To preview in the Configuration Browser the effect of any change made in the **Details** tab, click the **Apply** button and go to the **Overview** tab.

To see in the ACE Client the effect of these changes, click the **Apply** button and open the relevant dialog in the ACE client. It is not necessary to reload the configuration or to restart the ACE client. However, if the modified dialog is currently open in the ACE client, it will be necessary to close and reopen that dialog.



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
Label	Label 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.
Field type	<p>Field type 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.</p> <ul style="list-style-type: none"> – Text field <ul style="list-style-type: none"> – Click the ellipsis button next to it to specify the number of characters allowed. – Check box – Date field – Time – Date-time field – Combo box <ul style="list-style-type: none"> – Enter the valid values for your combo box in the text field provided. Separate them with commas or carriage returns. – Numerical input <ul style="list-style-type: none"> – Enter your minimum and maximum values for the numerical input in the spin boxes provided. – Building control 1 and Building control 2 <ul style="list-style-type: none"> – These are special controls that can be relabeled here (in the Label 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.
Visible	Clear this check box to prevent the data field from appearing in the client.
Unique	Select this check box to ensure the uniqueness of values entered in this field. The system then rejects the input of any value that has already been stored for this field in the database. For example, personnel numbers should be unique to persons, and license plates to vehicles.
 	<p>The green light means that the data field is not currently used in the database.</p> <p>The red light means that the data field is currently used in the database.</p>
Display in	Use this drop-down list to select the client tab on which the data field should appear.
Required	<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 Visible 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>

Label text	Description
Position	Use the spin boxes for Column and Row to position the data field on the tab named in the Display in drop-down list. Note that the editor will not allow you to select a position that is already in use, or to overlay existing data fields. Use the Width (percent) 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.
Dimension	Use the spin boxes for Column and Row to specify the number of columns and rows to be occupied on the tab named in the Display in 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:

Use in reports (check box)	Select this check box to enable the new data field to appear in standard reports.
Sequence number (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**.

18.2

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.

19 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.

19.1 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.

19.2 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.

19.3 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.


19.3.1 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**
- **BIS Configuration browser > Connections > 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.

19.3.2 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**
- **BIS Configuration browser > Connections > 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

19.3.3 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**
- **BIS Configuration browser > Connections > 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.

19.3.4

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**
- **BIS Configuration browser > Connections > 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.

19.3.5

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**
- **BIS Configuration browser > Connections > 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.

19.4

Configuration steps in System data dialogs

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

19.4.1

Creating a Person security profile



Dialog path

- **Main menu > System data > Person security profile**
- **ACE client > 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 R	Screening rate (%) in Person security profile P	Person selected for extra security checks?
0	Any	No
100	Any	Yes
1..99	0	No
1..99	100	Yes
1..99	1..99	Possibly Probability = MAX(R,P)


19.4.2 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

19.5 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

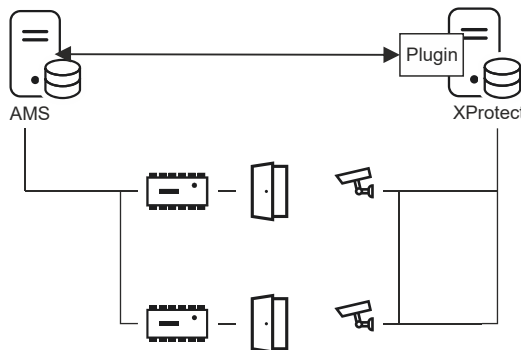
- *Assigning a Person security profile to a Person Type, page 141*
- *Creating and managing personnel data, page 189*

20 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.



Notice!

Potential incompatibility of plugins from different sources

Milestone XProtect plugins are not sandboxed, that is, they are not completely insulated from each other. For this reason, software errors may occur if you run multiple plugins with different versions of .NET and their dependencies on the same XProtect server. BOSCH can only guarantee the correct functioning of the AMS plugin if it is the only plugin installed.

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.
- FQDN installation is not supported by default. In case of installation in a domain environment, it is recommended to contact the support organization.

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\Bosch Security System Internal CA - BISAMS.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 matching the AMS version to be connected 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 Client, navigate to **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 server>:62904/` where `62904` 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.

21 Integrating Otis Compass

Introduction

Compass is a Destination Management System from the Otis Elevator Company. Its function is to manage multiple banks of elevators, dispatching elevators to passengers so that they can reach their destinations as efficiently as possible. To provide the necessary data, passengers no longer simply press **Up** or **Down** keys, but request their destinations at card-reader, touch-screen or keypad terminals.

Integration with Bosch access control systems adds security. Based on their credentials and the time models in operation, passengers are transported to their home floors and other authorized destinations efficiently. The system will not accept requests for floors that are not in the passenger's authorization profiles, or at a time of day that is outside the current time model.

Hardware topology of a Compass system

The hardware of a Compass system is configured top-down as a 3-tier hierarchy underneath a single MAC in the Device Editor.

	<p>First tier: (Otis Compass) The Destination management system. Each Compass system can govern up to 8 elevator groups (also known as elevator banks). Parameters: The range of floors, network addresses, port numbers and timeouts.</p>
<p>The hierarchy above shows:</p>	<p>Second tier: (Otis DES/DER) Up to 8 elevator groups, each managed by a logical Destination Entry Server (DES) consisting of 1 or 2 physical devices. In addition, this tier may have up to 2 optional devices for optimization, known as Destination Entry Redirectors (DER). Parameters: 1 group ID per elevator group. 1 IP address per device. The table of floors with elevator doors, and whether they are publicly accessible.</p>
<p>An Otis Compass system on a dedicated MAC A single elevator group governed by one DES A number of terminals (DET), each with a floor number from -2 to +7, and F or R referring to Front or Rear doors.</p>	<p>Third tier: Otis DET The Destination Entry Terminals (DET) Parameters: 1 IP address per terminal. Reachable floors with elevator doors for each terminal.</p>

Overview of integration in the access control system

Administrators of the access control system integrate Compass in the following stages, described in detail later in the chapter:

1. Configure the Compass hardware upon a single MAC in the Device Editor.
2. Configure customized fields for Otis-specific cardholder properties such as home floor.
3. Create Authorization profiles that govern access to specific elevator destinations.
4. Assign authorization profiles to the appropriate cardholders
 - (see the ACE operation guide for these standard procedures).

21.1 Configuring a Compass system in the Device Editor

This section describes the steps to configure an Otis Compass system in the device editor.

Dialog path

- **Main menu > Configuration > Device data**
- **BIS Configuration browser > Connections > Device data**

21.1.1 Tier 1: Setting up the Compass system


Procedure for Tier 1: Setting up the Compass system

1. Select the desired MAC in the Device editor tree view
2. Right-click and select **New Otis Compass**. The properties page has 2 tabs.
 - **Otis Compass**
 - **Floors**
3. On the **Otis Compass** tab the most important parameters to set are
 - **Name** (the name that should appear in the device tree)
 - **MAC IP-Address** (the callback IP address for the Compass system, on a dedicated network card, through which the Compass system communicates with the MAC).
NOTE: This is **not** the IP address of the MAC itself.
 - **Division** (if and only if Divisions are licensed and used in your installation)

Leave the rest of the parameters at their default values unless instructed to change them by expert technical support. They are briefly explained in the following table:

Parameter	Default value	Description
MC group address	234.46.30.7	IP address for the multicast group
MC port for DES/DER remote MC port for DES/DER local	48307 47307	Multicast ports
UDP port for DES/DER remote UDP port for DES/DER local	46303 45303	UDP ports for the DES and DER devices
UDP port for DET remote UDP port for DET local	45308 46308	UDP ports for the DET devices
Multicast time-to-live (TTL)	5 seconds	
Heartbeat interval	1 second	The amount of time between heartbeat signals. These signals show other devices that a device is "alive", that is functioning
Max. number of missed heartbeats	3	The number of heartbeats that can be missed before a device is considered "dead" (no longer functioning)
Message timeout	1 second	

Parameter	Default value	Description
Message retries	3	

1. On the **Floors** tab, click **Change floor range**
2. Enter the numbers of the lowest and highest floors to be served by all the elevator banks of the Otis Compass system.
 - The maximum range is -127 to +127
3. Click  (Save) to save the changes.

21.1.2

Tier 2: Elevator groups, DES and DER devices

Procedure for Tier 2: Setting up the elevator groups (DES/DER devices)

Introduction

The DES (Destination Entry Server) is the computer that manages an elevator group. If desired, two physical DES devices with separate IP addresses can be combined in a logical DES, with failover capability.

The DER (Destination Entry Redirector) connects elevator groups and allows DETs at a common entry point in the building, for example the Lobby, to accept destination requests for any floor in the building. The DER is not configured to act in a fail-over mode.

Creating DES devices in the device tree:

1. Select the desired Otis Compass in the Device editor tree view
2. Right-click and select **New Otis DES**. The properties page has 2 tabs:
 - **Otis DES**
 - **Floors**
3. On the **Otis DES** tab set the following parameters:
 - **Name:** the name that should appear in the device tree.
Use a systematic naming scheme that will provide clear orientation for configurers of DES and DET devices later in the configuration process.
 - **Description:** (optional) a free-text description of the device.
 - **Group:** an integer from 1 to 10. Make this integer unique among all the elevator groups (designated by their DES/DER devices) within this Otis Compass system. You will not be able to save your device edits if you use the same **Group** number more than once.
 - **1st IP address:** The IP address of this DES device.
 - **2nd IP address:** If this DES has a redundant twin, enter its IP address here.
 - **Division** (if and only if Divisions are licensed and used in your installation)

On the **Floors** tab the floors defined for Tier 1 (the Compass system) are presented as a table of editable cells.

Creating DER devices in the device tree:

DER devices are created in almost the same way as DES devices. The only difference is that a DER needs no fail-over device, so does not have a parameter for **2nd IP address**.

Example elevator group.

The example below shows the floors for a 10 floor elevator group, with front and rear doors, and publicly accessible ground and 6th floors.


OTIS DES Floors

Highest floor: 7

Lowest floor: -2

Change floor range

Floor number	Name	Description	Front door	Front door publicly accessible	Rear door	Rear door publicly accessible
7	VIP	CxO floor	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
6	Restaurant	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
5	Offices-4	Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
4	Offices-3	Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
3	Offices-2	Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	Offices-1	Staff	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
1	Conference	Invited visitors	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
0	Lobby	Public	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
-1	Maintenance	Restricted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
-2	Servers	Restricted	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

1. In the **Front door** column, select the check boxes of all floors where the elevator offers use of its front door.
2. Select the check boxes similarly for the **Rear door** column, if applicable.
3. For the column **Front door publicly accessible**, select the check boxes of those floors that are accessible to all elevator passengers without restriction.
4. Select the check boxes similarly for the **Rear door publicly accessible** column, if applicable.
5. (optional) Click **Change floor range** on this tab to further restrict the range of floors that was set at the **Otis Compass** level.
6. Overwrite the default names in the **Name** and **Description** columns with meaningful alternatives.
7. Click  (Save) to save the changes.

21.1.3 Tier 3: DET devices

Procedure for Tier 3: Setting up the terminals (DET devices)

Introduction:

A DET (also known as a DEC -- Destination Entry Computer) reads physical credentials or PIN codes. A DET can be located on a particular floor outside the front or rear door of an elevator, or inside the elevator cabin.

Creating DET devices in the device tree:

1. Select the desired Otis DES/DER device in the Device editor tree view.
2. Right-click and select **New Otis terminal**.
 - A popup window **Create Otis terminals** appears
3. Enter the number of terminals that you wish to configure on this DES/DER.
4. Accept the default values, or enter new starting values for the four octets of its IP address.

- For any octet, but typically for the 4th, select the check box **Automatic increment** if you wish the system to configure a unique IP address for each terminal by incrementing the octet.
5. Click **OK**.
 - The desired number of DET devices is created in the device tree.
 - Their IP addresses are incremented as determined in the previous step.

Configuring DET devices

The properties page for each DET has 2 tabs:

- **Otis terminal**
 - **Floors**
1. On the **Otis terminal** tab set the following parameters:
 - **Name:** The name that should appear in the device tree
 - **Description** (optional) a free-text description of the device.
 - **IP address** The IP address of this DET device
 - **Operational mode:** 1 . . 4

This determines how the terminal requests destinations from the elevator passenger, and passes the requests to the DES/DER for validation. The following table gives details:


Op. mode	Description	Behavior
1	Default floor	(The default operational mode) The passenger presents their credential, or enters a PIN code. If the credential or PIN is valid, and the passenger makes no further input, then the DET requests from the DES the passenger's default or "home" floor. If the passenger enters a different destination floor, then the DET requests that destination from the DES.
2	Access to authorized floors	The passenger presents their credential, or enters a PIN code, then enters a destination floor. The DET requests that destination from the DES. The access control system grants or denies access to the requested destination.
3	User entry of destination floor	The passenger enters a destination floor. If the destination is publicly accessible, then the DET requests the destination from the DES. Otherwise, the DET requests the passenger to present their credential for validation.
4	Default floor or User entry of destination floor.	The passenger presents their credential, or enters a PIN code. If the credential or PIN is valid, then the DET requests from the DES the passenger's default or "home" floor. Within a set timeout period the passenger may override the selection of the default floor and choose a different destination.

- **Audit records:** Select this check box to record passenger inputs at this terminal for the event log.
- **PIN code:** Select this check box to allow the use of an identification PIN code at this terminal as an alternative to physical credentials.
Note: Use enrollment readers of type **Dialog PIN card (enter)** to enroll PIN codes for use at Otis terminals.
- **Time models:** Select this check box to allow time models to restrict the times when this terminal can be used.
- **Division** (if and only if Divisions are licensed and used in your installation)

On the **Floors** tab of the **Otis terminal** properties page, the floors that you defined for Tier 2 (the DES/DER) are presented as a table of editable cells.

Note: The naming scheme defined for Tier 2 above should provide sufficient orientation. If not, we recommend saving your work and returning to Tier 2 to complete the naming scheme.

1. Select in turn each DET that you have just created in the device tree, and open the **Floors** tab.
 - The **Floors** table appears
2. In the **Front door** column, select the check box of every floor that is to be reachable from the current DET.
3. In the **Front door publicly accessible** column, select the check box of every front door that is to be publicly accessible, that is, without explicit authorization.
4. (optional) In the **Time model for front door** column, select a time model to restrict public access to the front door on that floor, if required. For example, the restaurant floor may be accessible only at certain times of the day.
5. Redo the previous steps, if necessary, for the columns **Rear door**, **Rear door publicly accessible** and **Time model for rear door**.

6. Click  (Save) to save the changes.

Example:

The example below shows the floors for a 10 floor elevator group, with those floors and doors reachable from the front elevator door in the lobby. Access to the restaurant floor, both front and rear elevator doors, is restricted by a time model.

OTIS terminal Floors

Highest floor: 7
 Lowest floor: -2

Change floor range

Floor number	Name	Front door	Front door publicly accessible	Time model for front door	Rear door	Rear door publicly accessible	Time model for rear door	Description
7	VIP	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		CxO floor
6	Restaurant	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mo_Fr_07-17	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Mo_Fr_07-17	Public
5	Offices-4	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Staff
4	Offices-3	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Staff
3	Offices-2	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Staff
2	Offices-1	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Staff
1	Conference	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Invited visitors
0	Lobby	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Public
-1	Maintenance	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input checked="" type="checkbox"/>	<input type="checkbox"/>		Restricted
-2	Servers	<input checked="" type="checkbox"/>	<input type="checkbox"/>		<input type="checkbox"/>	<input type="checkbox"/>		Restricted

21.2 Configuring customized fields for Otis-specific properties of cardholders

Introduction

This section describes how to create those custom fields where an operator can enter the Otis-specific properties for a cardholder, in particular the cardholder's "home" or default destination. This "home" must be defined by **three coordinates**:

1. Elevator group,
2. Floor
3. Door

Note that when specifying a home floor for a cardholder in the access control system client, an operator must enter data in the same order: elevator group, floor, door. For this reason the three custom fields should be positioned in reading order, preferably top to bottom.

Click **OK** to confirm any popup reminders that you must create all three coordinates.

Define the 3 necessary custom fields, plus any special Otis options you require, to appear on the **Elevators** tab of the access-control client interface.

For general information about configuring custom fields, see the ACE/AMS Configuration help for **Custom fields for personnel data**.

Dialog path

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

BIS Configuration browser > **Infrastructure** > **ACE Custom fields**

Procedure

On the **Custom fields** property page, select the **Elevators** tab.

First coordinate: Elevator group

1. Double-click in a cell on the tab and click **Yes** to create a new input field.
2. From the **Field type** list, select **Otis DES selection**.
3. In the **Label** field, enter `Elevator Group`
4. From the **Display in** list, select `Tab:Elevators`
5. In the **Position** group, select a unique location on the **Elevators** tab, where this custom field is to appear.

Second coordinate: Home floor

1. Click **New field**, to create a new custom fields
2. From the **Field type** list, select **Home floor**.
3. In the **Label** field, enter `Home floor`
4. From the **Display in** list, select `Tab:Elevators`
5. In the **Position** group, select a unique location on the **Elevators** tab, where this custom field is to appear. For ease of use by system operators, it should be below the previous coordinate.

Third coordinate: Exit door

1. Click **New field**, to create a new custom fields
2. From the **Field type** list, select **Exit door**.
3. In the **Label** field, enter `Exit door`
4. From the **Display in** list, select `Tab:Elevators`

- In the **Position** group, select a unique location on the **Elevators** tab, where this custom field is to appear. For ease of use by system operators, it should be below the previous coordinate.


Special Otis options for cardholders

Introduction

Eight Otis-specific binary options are provided in accordance with standard Otis functionality. If defined as custom fields on the **Elevators** tab, they appear as check boxes on the **Elevator data** tab of cardholders in the **Persons** dialog (Main menu > **Personnel data** > **Persons**). They can then be selected and cleared by operators of the access control system.

Configure these options only as instructed by your Otis representative.

Procedure

- Click **New field**, to create a new custom fields
- From the **Field type** list, select **Otis options**.
- In the **Label** field, enter your own label, for example `Otis flag 1` or according to Otis documentation.
- From the **Display in** list, select `Tab:Elevators`
- From the **Function type** list, select one of the options from `OTIS option 1` to `OTIS option 8`
- In the **Position** group, select a unique location on the **Elevators** tab, where this check box is to appear.
- Click  (Save) to save the changes.

21.3

Creating and configuring authorizations for Otis elevators

Introduction

This section describes how to include access rights for Otis elevator groups, floors and elevator doors in an **Authorization**.

Authorizations are assigned directly to cardholders or, more commonly, combined with other Authorizations into **Access profiles**, which are then assigned to cardholders.


Prerequisites


An Otis Compass system has been defined on a MAC in the device editor. It is complete with an elevator group (represented by its DES) and floor+door pairs (represented by their DETs).

Dialog path

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

Procedure

- In the **Authorization name** field, enter the name of an existing Authorization, or click  (New) to create a new Authorization.
- In the **MAC** list, select the name of the MAC upon which the Otis Compass system has been created.
- Click the **Otis elevator** tab
- In the **Otis elevators** list, select the DES/DER for the elevator group that you wish to add to the Authorization (Note that an Authorization can contain only one DES/DER).

- The floors of the selected elevator group are displayed in the **Floors** pane.
5. In the **Front door** and **Rear door** columns of the **Floors** pane, select the doors on those floors that are to be included in this Authorization.
 - Note that those floors and doors that were **not** selected for this elevator group, when it was defined in the device editor, will be grayed out and not selectable in this dialog.
 6. Alternatively, click the buttons **Assign all floors** and **Remove all floors** to select or clear all floors and doors at once.
 7. Click  (**Save**) to save the Authorization.

22 Configuring IDEMIA Universal BioBridge

This section describes the configuration of IDEMIA biometric devices to work with Bosch access control systems through **MorphoManager** and **BioBridge**.

The subsections cover the configuration tasks necessary in the following areas:

- The Bosch access control system
- MorphoManager
- The BioBridge enrollment client in MorphoManager
- Adaptations for various card technologies and formats

22.1 Setting up BioBridge in the Bosch access control system

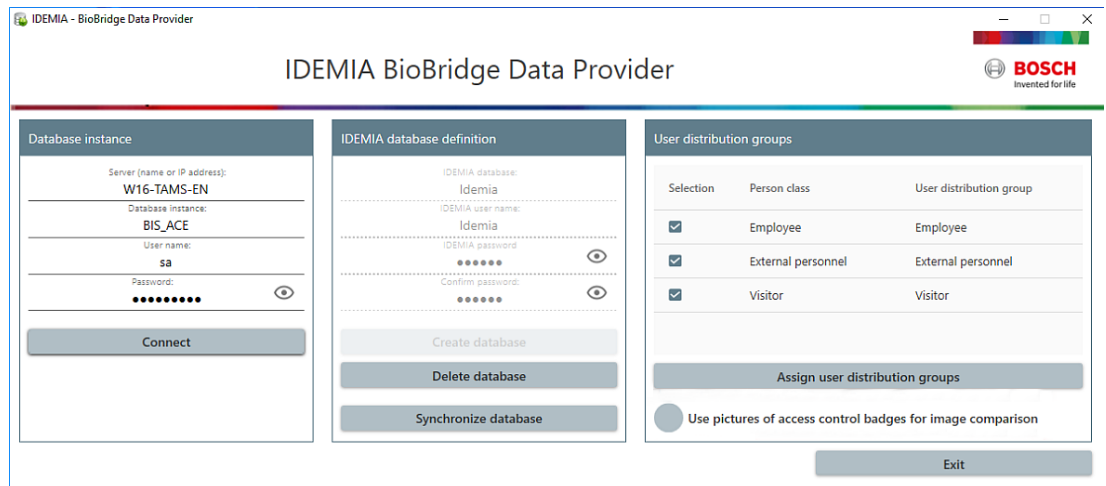
The following steps are performed in the ACS to create the database that links IDEMIA biometric devices to the Bosch access control system. The database maps the following database entities to each other:

- **Person class** (Bosch) and
- **User distribution group** (IDEMIA).

Dialog path

- BIS Configuration Browser > **Tools** > **ACE configuration IDEMIA database**
- AMS main menu > **Configuration** > **Tools** > **IDEMIA database configuration**

1. Click **Configuration IDEMIA database**
The **IDEMIA BioBridge Data Provider** dialog appears.



2. In the **Database instance** pane, enter the following information:
 - **Server:** The hostname or IP address of the computer where the ACS SQL Server database instance is running. This may be the local hostname, if the SQL Server is running locally.
 - **Database Instance:** The instance of the ACS (default **ACE**).
 - **Username:** The name of administrator account of the ACS database instance (default: **sa**)
 - **Password:** The password of the administrator account, as configured during the installation of the ACS .
3. Click **Connect** to test the connection. All other controls are disabled until you do this.

In the IDEMIA database definition pane

The first two fields are read-only:

- **Idemia database:** the name of the database that joins Bosch and IDEMIA data.
 - **Idemia username:** the name of the database user in whose name the software executes commands in the database.
1. Enter and confirm a strong password for **Idemia username**.
 2. Carefully note the password. It will be required in future configuration tasks, and cannot be restored if lost.
 3. Click **Create database**.
A message box will confirm if the creation was successful. Click **OK**
 4. When tests are successfully completed, click **Exit** to close the dialog.

In the User distribution groups pane

User Distribution Groups are MorphoManager objects that map users (credential holders) to groups of biometric readers or MorphoManager clients. We map them to the **Person Classes** of Bosch access control systems.

1. In the Select column, select the check box of each ACE **Person Class** that your installation uses.
 2. For each line you have selected, copy the name of that Person class to the corresponding cell in the **User distribution group** column.
- Note that the names of the **Person class** and the **User distribution group** must match exactly.
3. When your mapping is complete, click **Assign user distribution groups**.

Providing ID photos for VisionPass face recognition

To allow IDEMIA readers to perform VisionPass face recognition using cardholders' ID photos from the ACE database:

- ▶ Click **Use pictures of access control badges for image comparison** and confirm in the popup window.
The **IDEMIA BioBridge Data Provider** window confirms that synchronization is in progress.
Note that, depending on the amount of image data involved, the transfer may take considerable time.

22.2

Selecting card technologies and formats

Introduction

If you intend to use cards as well as biometric identification, you must create a profile (or "Wiegand profile") in MorphoManager that includes the format (or formats) of those access cards.

The following table gives an overview of supported formats. Note that for MIFARE technology only CSN identification is supported.

Card Family	HID Prox	HID Class	HID iClass Seos	MIFARE Classic	MIFARE DESFire EV0	MIFARE DESFire EV1
Card Variant	Prox	2k/2 16k/2 16k/16 32k(16k/2+16k/1) 32k(16k/16+16k/1)	Seos	1K 4-byte NUID 1k 7-byte UID 4k 4-byte NUID 4k 7byte UID	2k 4k 8k	2k 4k 8k

Figure 22.1: IDEMIA cards supported

General procedure

1. In MorphoManager navigate to **Administration > Wiegand Profile**
2. Click **Add** to create a custom Wiegand profile
3. In the related dialogs, enter the formatting information and the card technology that your system uses
4. In order to use your newly-defined Wiegand profile in the system, enter its name in the **Wiegand Profile** field of the following MorphoManager dialogs:
 - **Administration > Biometric Device profile**
 - **Administration > User policy**

Mifare Classic CSN

1. Add Wiegand Element `User CSN Element` and enter the following details
 - **Name:** CSN (for example)
 - **Length** 32
 - **Transformation mode:** `Reversed`
2. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box **MIFARE Classic**

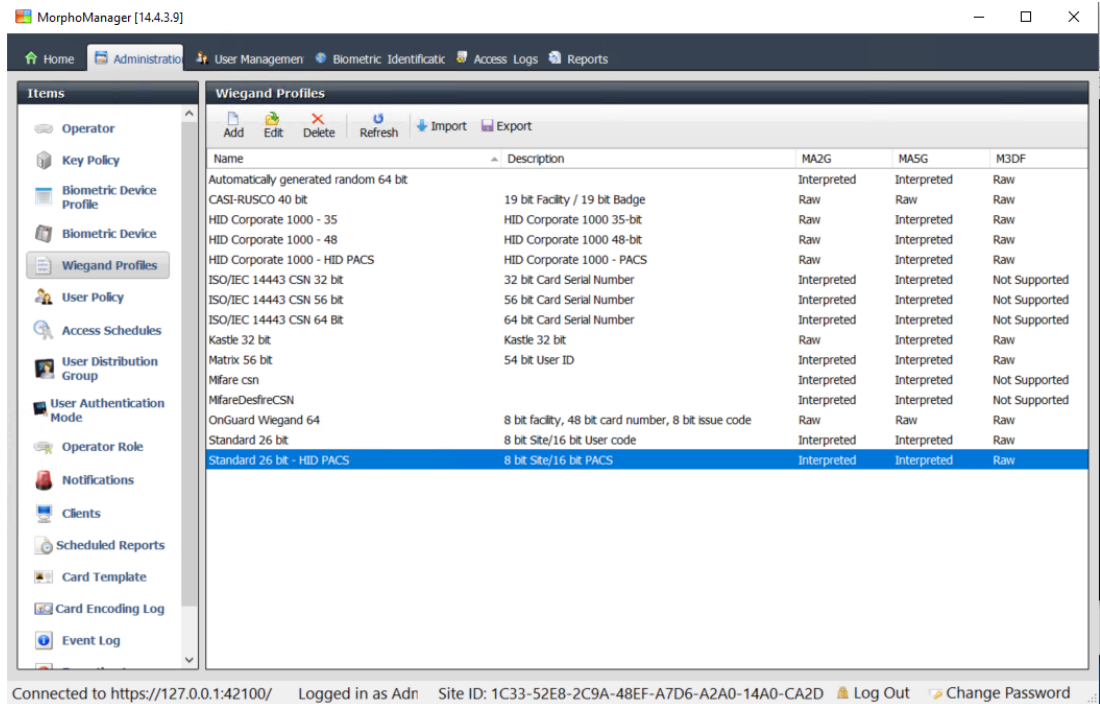
Mifare DESFire CSN

The configuration is identical to Mifare Classic except for the following details:

- **Length:** 56
- Add **Wiegand Element User CSN Element**
 - Enter a name under **Name:**
 - For **Length** enter 56
 - For **Transformation mode:** enter `Reversed`
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box **Mifare DESFire 3DES**

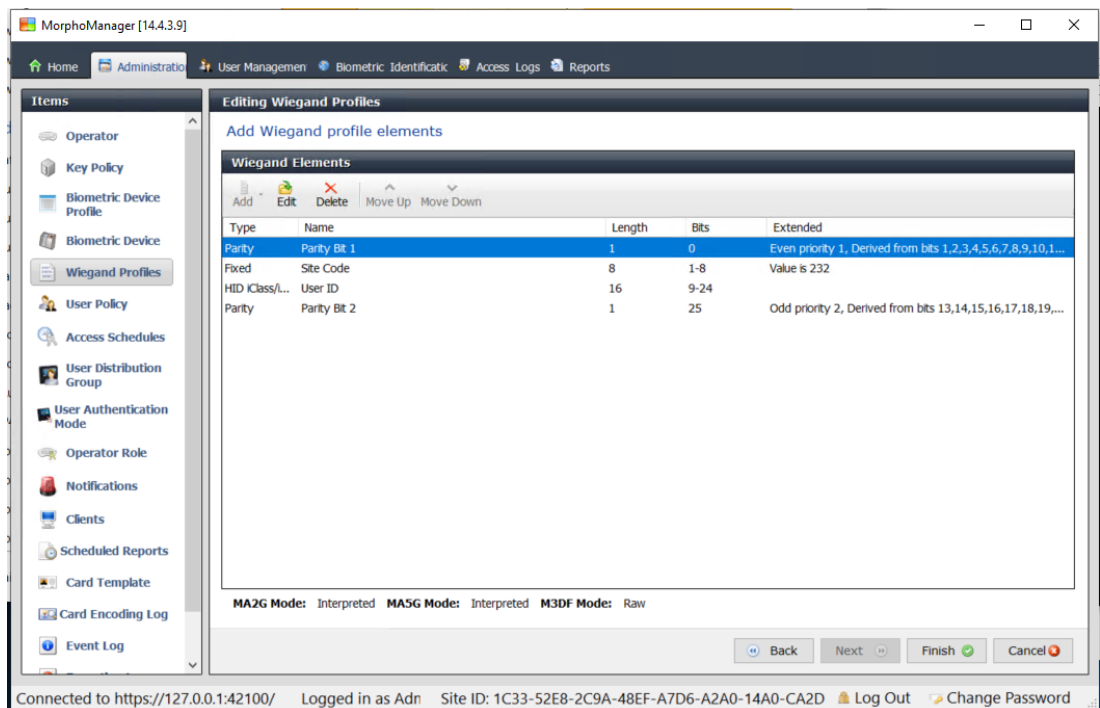
iClass 26 BIT

1. Select the predefined profile `Standard 26 bit-HID PACS`



Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

2. Click **Edit**
3. Click **Next**



Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

4. Click **Edit**
5. Delete the line Fixed Facility Code
6. Select the line HID iClass SEP User ID
7. Click **Edit**
8. Change the length of the User ID from 1..16 to 1..24
9. **Under Administration > Biometric Device profile**, on the Biometric Device Settings page, for Wiegand Profile select Standard 26 BIT-HID-PACS

10. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
11. Click **Next** until you reach the page **Custom Parameters**
12. Click **Add**
13. Add custom parameter (case-sensitive) `wiegand.site_code_propagation`
14. Set its value to 1
15. Click **Finish**.
16. Enter this completed Wiegand profile under **Administration > User policy**

iClass 35 BIT

1. Select the predefined profile `HID Corporate 1000 35 BIT`
2. Click **Edit**
3. Click **Next**
4. Select and delete the element line `Fixed Company ID`
5. Select and delete the element line `User Card ID Number`
6. Add the element line `HID iClass/iClass SE PACS Data` and in its element details, set the following:
 - Name: `Card ID Number`
 - Length: 32
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
- Click **Next** until you reach the page **Custom Parameters**
- Click **Add**
- Add custom parameter (case-sensitive) `wiegand.site_code_propagation`
- Set its value to 1
- Click **Finish**.
- Enter this completed Wiegand profile under **Administration > User policy**

iClass 37 BIT

- **Administration > Wiegand Profile**
 - Click **Add new profile**
 - **Length** 37
1. Add element Parity:
 - **Name:** (for example) `EvenParityBit 1`
 - **Priority:** 1
 - **Length:** 18
 - **Mode:** Even
 - **Basis bits:** `1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18`
 - Click **Next**
 2. Add element `User HID iClass/iClass SE PACS Data` and in its element details, set the following:
 - **Name:** `UserID`
 - **Length:** 35
 - Click **Next**
 3. Add element Parity:
 - **Name:** (for example): `Parity Bits 2`
 - **Priority:** 2
 - **Length:** 19
 - **Mode:** Odd

- **Basis bits:** 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36, 37
- Click **Next**
- **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
- Click **Next** until you reach the page **Custom Parameters**
- Click **Add**
- Add custom parameter (case-sensitive) `wiegand.site_code_propagation`
- Set its value to 1
- Click **Finish**.
- Enter this completed Wiegand profile under **Administration > User policy**

iClass 48BIT

1. Select the predefined profile `HID Corporate 1000 48 BIT`
2. Click **Edit**
3. Click **Next**
4. Select and delete the element line `Fixed Company ID`
5. Select and delete the element line `User Card ID Number`
6. Add the element line `HID iClass/iClass SE PACS Data` and in its element details, set the following:
 - Name: `User`
 - Length: 45
7. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check box `HID iClass`
8. Click **Next** until you reach the page **Custom Parameters**
9. Click **Add**
10. Add custom parameter (case-sensitive) `wiegand.site_code_propagation`
 - Set its value to 1
11. Click **Finish**.
12. Enter this completed Wiegand profile under **Administration > User policy**

HID Prox

1. Select the predefined profile `Standard 26 BIT`
2. Click **Edit**
3. Click **Next**
4. Delete the line `Fixed Facility Code`
5. Click **Edit**
6. Change the length of the User ID from `1..16` to `1..24`
7. **Under Administration > Biometric Device profile**, on the **Biometric Device Settings** page, for Wiegand Profile select `Standard 26 BIT`
8. **Under Administration > Biometric Device profile**, on the **Multi-Factor Mode Settings** page, select the check boxes:
 - **Biometry**
 - **Proximity card**
9. Click **Next** until you reach the page **Custom Parameters**
10. Click **Add**
11. Add custom parameter (case-sensitive) `wiegand.site_code_propagation`
 - Set its value to 1
12. Click **Finish**.
13. Enter this completed Wiegand profile under **Administration > User policy**

22.3 Selecting an identification mode

Introduction

Biometric readers can identify credential holders in different ways. These ways are known as Identification modes or Authentication modes.

- By **Card OR Biometry**, depending on what the credential holder presents to the reader
- By **Card AND Biometry**, that is the user must verify through biometric credentials that they are the true owners of the card.
- By **Biometry only**

This section describes how to set configure these modes in MorphoManager.

Note that wherever card credentials are involved, it is of course necessary to create a profile for the appropriate card technology and format.

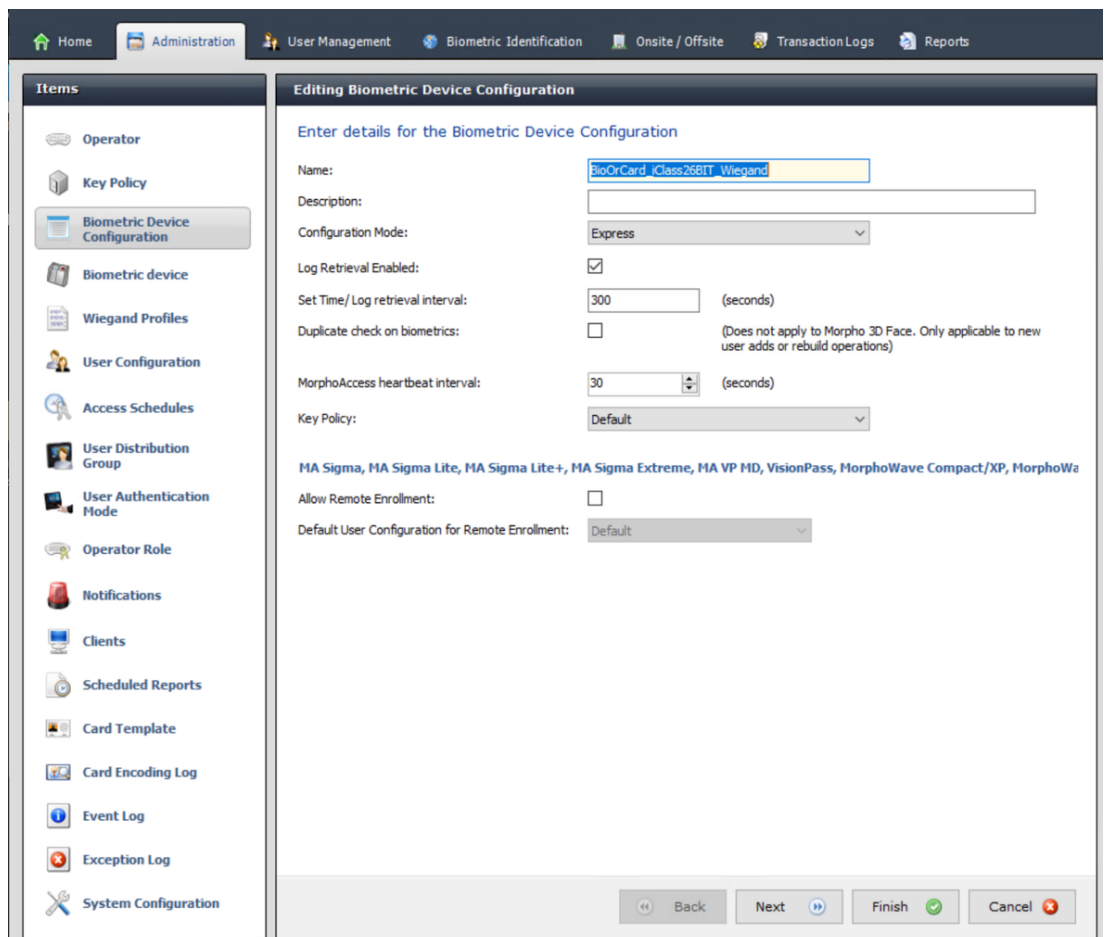
Dialog path

In MorphoManager **Administration** tab

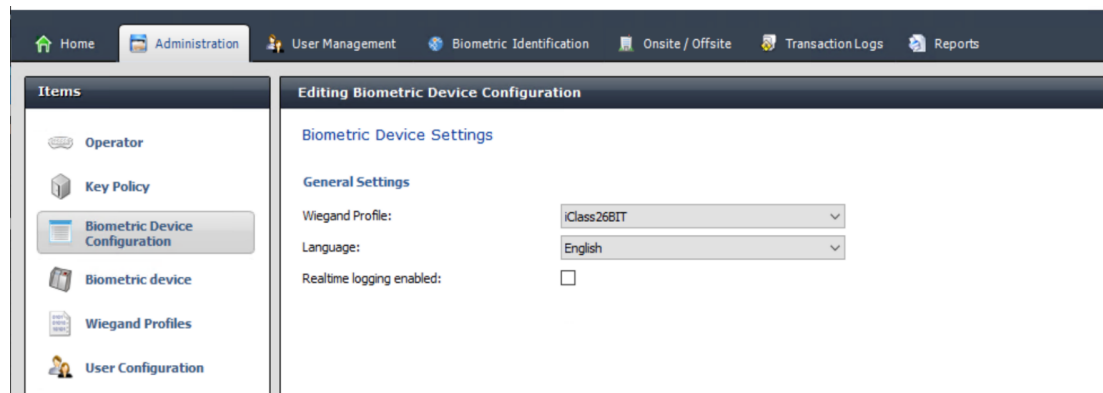
22.3.1 Card OR Biometry

Create this custom authentication mode if users are to identify themselves EITHER by card OR by biometric credentials.

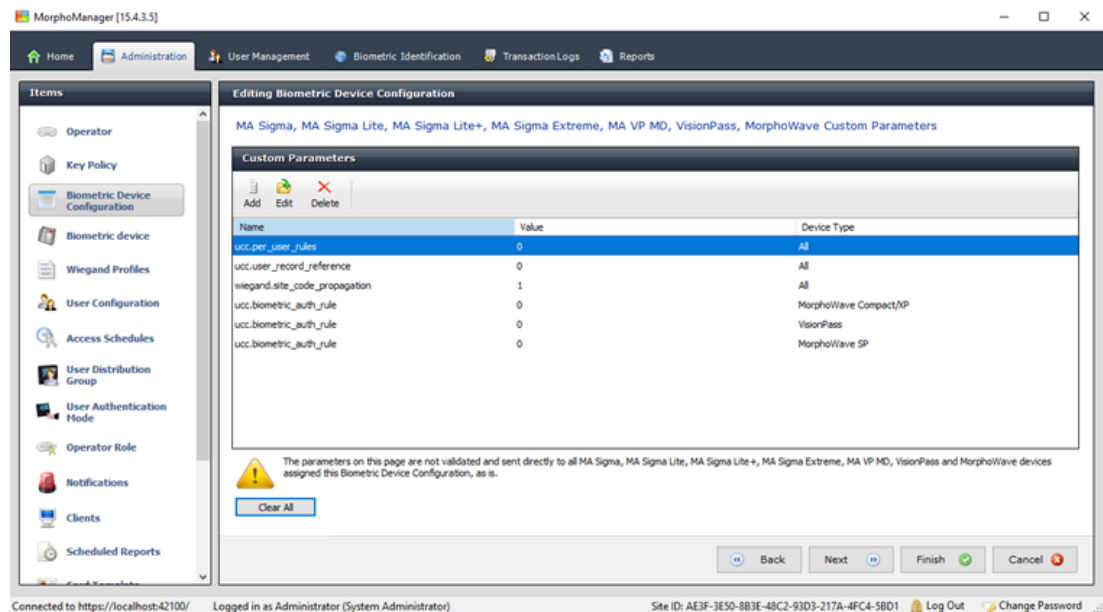
1. In MorphoManager, go to **Administration > Biometric Device Configuration**
2. Enter a name for this biometric device configuration, for example `CardORBiometric`



- Click **Next** until you reach the page titled **Biometric Device Settings**



- For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge.
- Click **Next** until you reach the dialog **Biometric Threshold settings**.
- Set the **Biometric Threshold** values according to your local conditions and the MorphoManager documentation. The default value is *Recommended*
- Click **Next** until you reach the **Multi Factor Mode Settings** screen.
- Select the **Biometric** check box, plus the check box of the card technology that your installation uses.
- Click **Next** until you reach the **Custom Parameters** screen



- For each device that you use:
 - Click **Add** to add two custom parameters.
(If these two parameters are set, the reader sends the card data directly to the AMC. The user does not need to be enrolled on the IDEMIA reader)
 - ucc.per_user_rules
 - ucc.user_record_reference
- For WAVE and VisionPass readers, add one more parameter:
 - ucc.biometric_auth_rule=0
 - In this case, select for **Device Type** MorphoWave Compact/XP or MorphoWave SP or VisionPass
- Click **Finish**

Assign this user authentication mode to the users

In the ACS you must assign a card with a valid card definition to each cardholder.

1. In MorphoManager, go to **Administration > User Authentication Mode**
2. Set the following attributes:
 - Set **Mode** to `Enabled`
 - Set the list **Template Location** to `Download to Device`
 - Select the check box **Allow Start by Biometric**
 - Select the check box **Allow Start by Contactless Card**
 - Disable **Require Template Match**
3. Go to **Administration > User Configuration**
4. Click **Add**
5. For **User Authentication Mode** select the name of the mode that you created above for Card OR Biometry.
6. Click **Finish**

Refer to

- *Selecting card technologies and formats, page 154*

22.3.2**Card AND Biometry**

Make the following settings if users must use a card AND biometric credentials, to verify that they are the owners of the card.

1. In MorphoManager, go to **Administration > Biometric Device Configuration**
2. Click **Next** until you reach the page titled **Biometric Device Settings**
3. For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge.
4. Click **Next** until you reach the page titled **Multi-Factor Mode Settings**
5. Select the check box of the card technology that your installation uses.
6. Click **Finish**

Assign this user authentication mode to the users

In the ACS you must assign a card with a valid card definition to each cardholder.

1. In MorphoManager, go to **Administration > User Configuration**
2. For **User Authentication Mode** select `Contactless Card ID + Biometric` from the list.
3. Click **Finish**.

Refer to

- *Selecting card technologies and formats, page 154*

22.3.3**Biometry only**

Make the following settings if users are to identify themselves by biometric credentials only.

1. In MorphoManager, go to **Administration > Biometric Device Configuration**
2. Click **Next** until you reach the page titled **Editing Biometric Device Configuration**
3. For **Wiegand Profile**, select the same profile that you defined for your biometric devices when setting up BioBridge
4. Click **Next** until you reach the page titled **Multi-Factor Mode Settings**
5. For **Multi-Factor Mode** select `Biometric only` from the list

6. Click **Finish**

Assign this user authentication mode to the users

In the ACS you must assign a card with a valid card definition to each cardholder.

1. In MorphoManager, go to **Administration > User Configuration**
2. For **User Authentication Mode** select `Biometric(1:many)` from the list.
3. Click **Finish**.

22.4

Setting up BioBridge in MorphoManager

Prerequisites

MorphoManager is installed on a MorphoManager server in your network. See the MorphoManager's own installation guide and online help.

Overview

To use the BioBridge interface between Bosch access control systems and Morphomanager, you need to configure the following in MorphoManager:

- **Biometric Device Configuration**
- **Biometric Device**
- **Wiegand Profiles**
- **User Configuration**
- **User Distribution Group**
- **User Authentication Mode**
- **System Configuration**

In addition, Open Database Connectivity (ODBC) must be set up for communication between Morphomanager BioBridge and the database it shares with the ACS.

All these configuration tasks are described in the following sections.

22.4.1

Wiegand Profiles



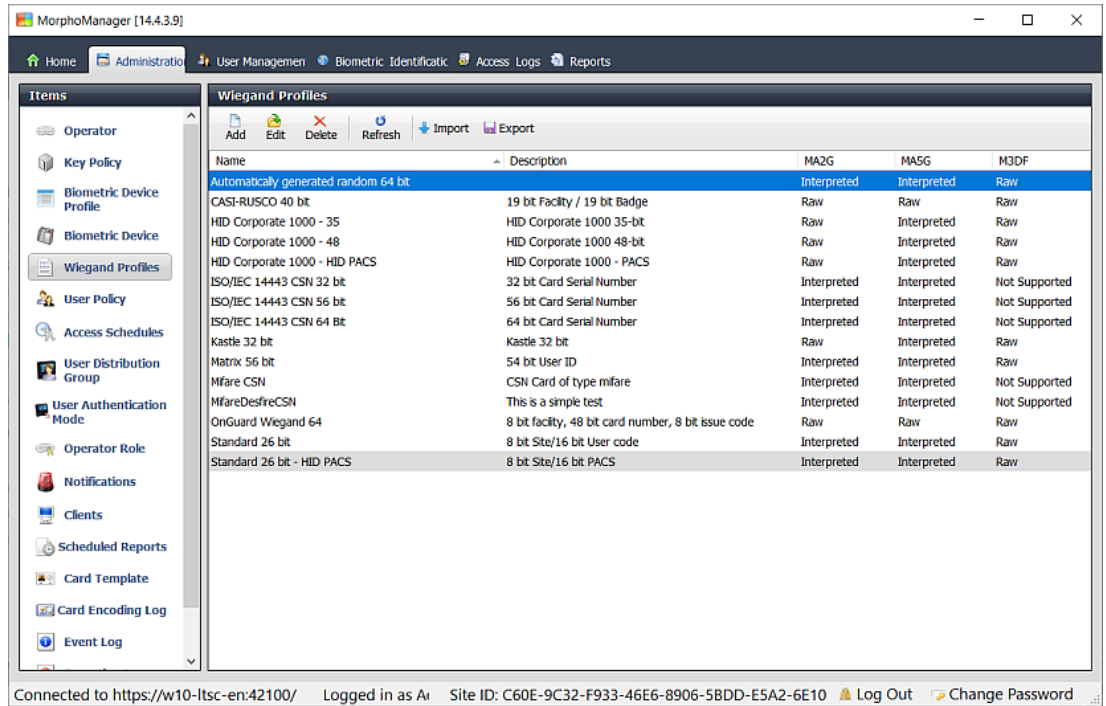
Notice!

Despite the name, Wiegand Profiles apply to all reader types, including OSDP readers.

Wiegand Profiles define what information the biometric devices output via their Wiegand Out interface, when they identify a user. This information goes to the Bosch access control system, which uses it to make an access decision.

Procedure:

1. In MorphoManager navigate to **Administration > Wiegand Profile**.
2. Select one of the predefined Wiegand profiles or click **Add** to create a custom profile. In general, all CSN profiles are suitable for use with Bosch access control systems, plus the standard 26 bit profiles. If your installer has provided a profile for your system, click **Import** to locate and import the file provided, and select it from the list.



3. In the dialog, enter the information that your access control system requires from the biometric devices.
4. Carefully note the name of the Wiegand profile that you select or create here. You must reference it in the MorphoManager configurations of **User Configuration** and **Biometric Device Configuration**.

Refer to

– *Selecting card technologies and formats, page 154*

22.4.2 Biometric Device Configuration

The Biometric Device Configuration defines common settings and parameters for one or more biometric devices. When you add biometric devices to the system later in the **Biometric Device** section of **Administration**, you apply a Biometric Device Configuration to them.

The following procedure assumes that you are deploying biometric readers from IDEMIA with additional card-reading technology.

Procedure:

1. In MorphoManager navigate to **Administration > Biometric Device Configuration**.
2. Click **Add** to create a new biometric device configuration.
3. On the next screen, enter a name for the profile and a description (optional). If you do not use the description field, we recommend a name that describes the type and the identification modes (biometry and/or card) of the group of readers.
4. Click **Next** until you arrive at the **Biometric Device Settings**
 - Select the Wiegand profile that you created previously for your installation.
5. Click **Next** until you arrive at the **Access Control Mode Settings** page.

At this point, the procedures for Wiegand and OSDP AMCs diverge. Follow the procedure below that corresponds to your AMC controller type:

For Wiegand AMCs

1. Set **Access Control Mode** to *Integrated by Wiegand*
2. Set **Panel feedback Mode** to *LED Feedback (2 wire)*
3. Click **Finish**

For OSDP AMCs

1. Set **Access Control Mode** to *Integrated by OSDP*
2. Set **Panel feedback Mode** to *LED Feedback (2 wire)*
3. Select the check box **OSDP Secure Channel**
4. Set baud rate 9600
5. For more details, see section **Biometric device**
6. Click **Finish** to exit MorphoManager.

Troubleshooting OSDP keys

If you cannot establish a secure connection to the OSDP reader, try resetting the base key as follows:

1. Start the separate program **MorphoBioToolBox (MBTB)**
2. In the MorphoBioToolBox program, go to **Device Settings > Reset**
3. Select the OSDP base key

4. Click **Reset cryptographic keys**
5. Exit MorphoBioToolBox

For more complex cases, contact IDEMIA technical support.

Refer to

- *Biometric device, page 165*

22.4.3

Biometric device

The biometric devices test whether the biometric credentials that they read match records in the database. They also keep a log of every usage event.

Procedure:

1. In MorphoManager navigate to **Administration > Biometric device**.
2. Click **Add** to create a new biometric device.
3. Enter at least the essential details for the device:
 - (from the list) **Hardware Family**
 - **Hostname\IP address**
 - (from the list) the **Biometric Device Configuration** that you defined earlier

4. Click **Finish**

The Biometric Device dialog now lists devices that are already configured:

The screenshot displays the MorphoManager [14.4.3.9] web interface. The navigation menu on the left includes: Home, Administration, User Management, Biometric Identification, Access Logs, and Reports. The main content area is titled 'Biometric Device' and contains a table with the following data:

Name	Description	Location	Biometric Dev...	Synchronizati...	Status	Tasks
MASigmaMulti			Express	Required Sy...	Online	4
VisionPassMDPI	Face Recognition	AC3	Default	Synchronized	Online	0

Below the table, the 'Details' tab is selected, showing the following information for the 'MASigmaMulti' device:

- Description:** MA SIGMA Multi WR
- Hardware Type:** 2019SMS0001431
- Serial Number:** 4.5.1
- Firmware version:** MASigmaMulti:11010
- Hostname\IP Address:** 0 / 5000
- User Slots:** (UTC+01:00) Amsterdam, Berlin, Bern, Rome, Stockholm, Vienna
- Time Zone:** Automatic
- Synchronization Mode:** Required Synchronization
- Synchronization Status:** Online
- Device Status:** Online

The status bar at the bottom indicates: Connected to https://127.0.0.1:42100/ Logged in as Adn Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

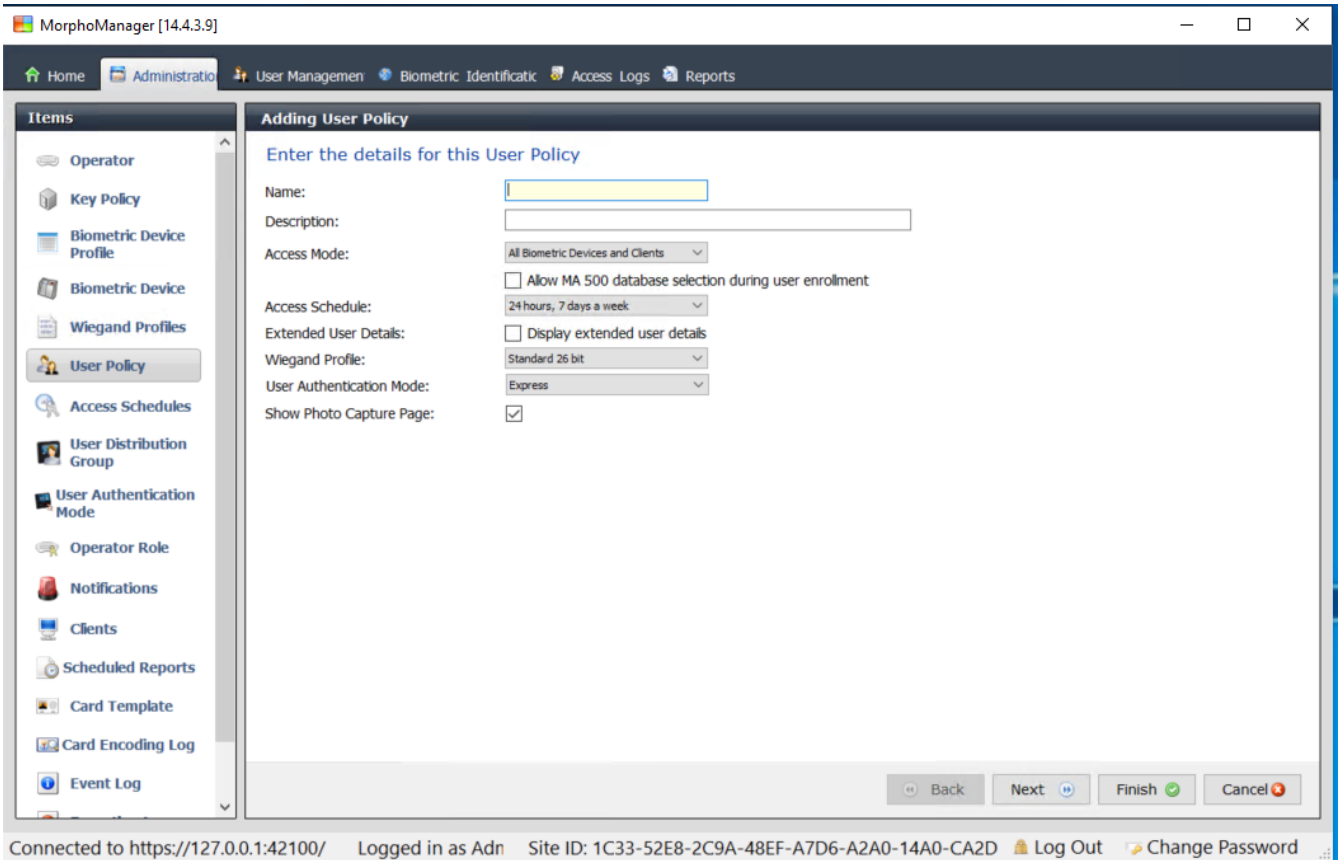
22.4.4

User Configuration

User configurations are bundles of access rights that you assign to users who have the same access requirements, that is, which biometric devices they are permitted to use in which modes and at what times.

Procedure:

1. In MorphoManager navigate to **Administration > User Configuration**
2. Click **Add** to create a new user configuration.



3. In the **Adding User Policy** dialog enter the following:
 - A **Name** for the User Policy and (optionally) a description
 - The **Access Mode** *Per User*
 - An **Access Schedule** governing the days and times when access is permitted
 - The same **Wiegand Profile** that you defined and used for the **Biometric Device Profile**.
 - A **User Authentication Mode**, depending on the ways in which the device users will use the devices (by fingerprint, finger, face, cards etc.). See section **Selecting an identification mode** for details.
 4. Click **Finish**
- The default User Policy will have a User Authentication mode of (1: Many). To utilize other authentication modes, create additional User Policies. Consult the MorphoManager User Manual for more detail on all the various properties that can be assigned to a User Policy.

Refer to

- *Selecting an identification mode, page 159*

22.4.5 User Distribution Groups

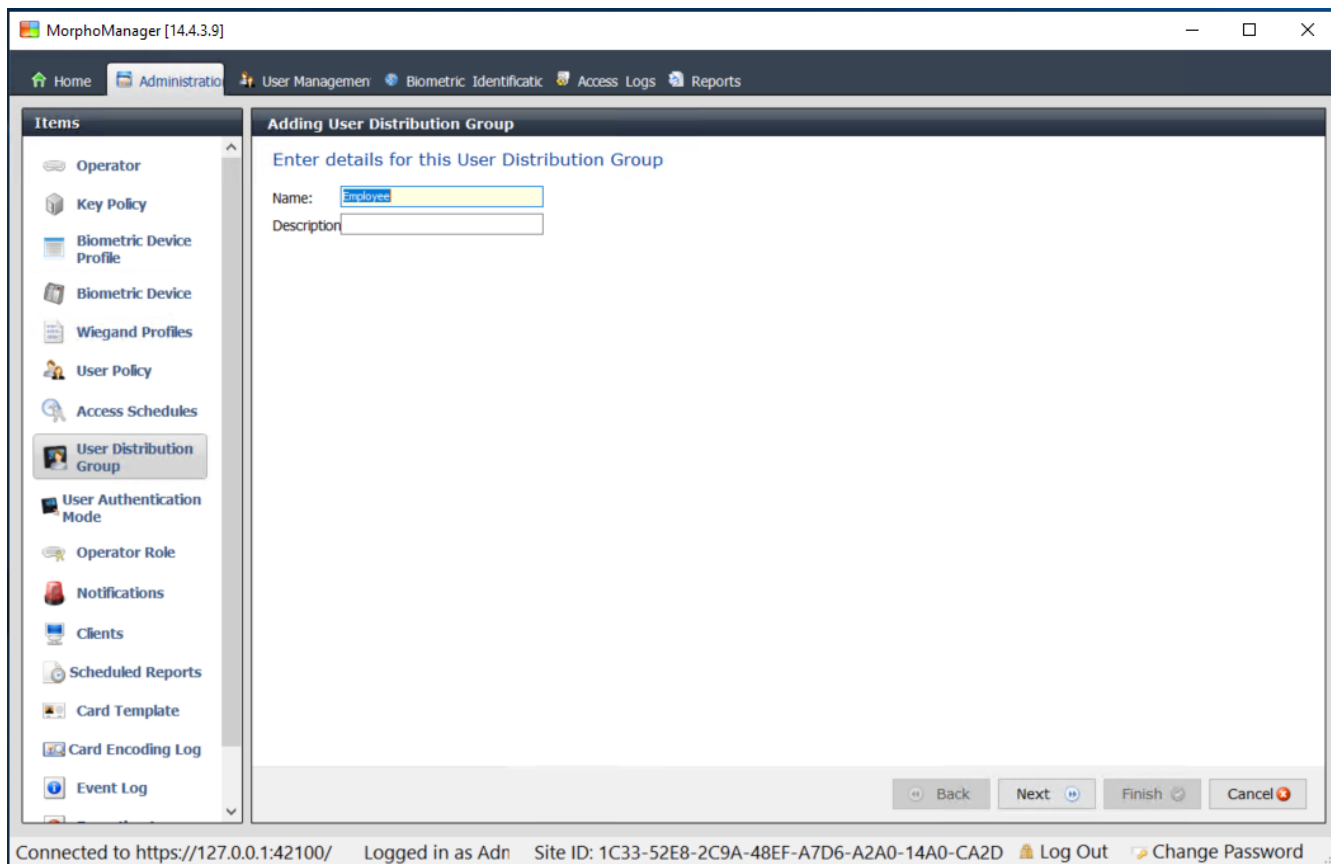
User Distribution Groups map users to groups of biometric readers or MorphoManager clients.

Prerequisites:

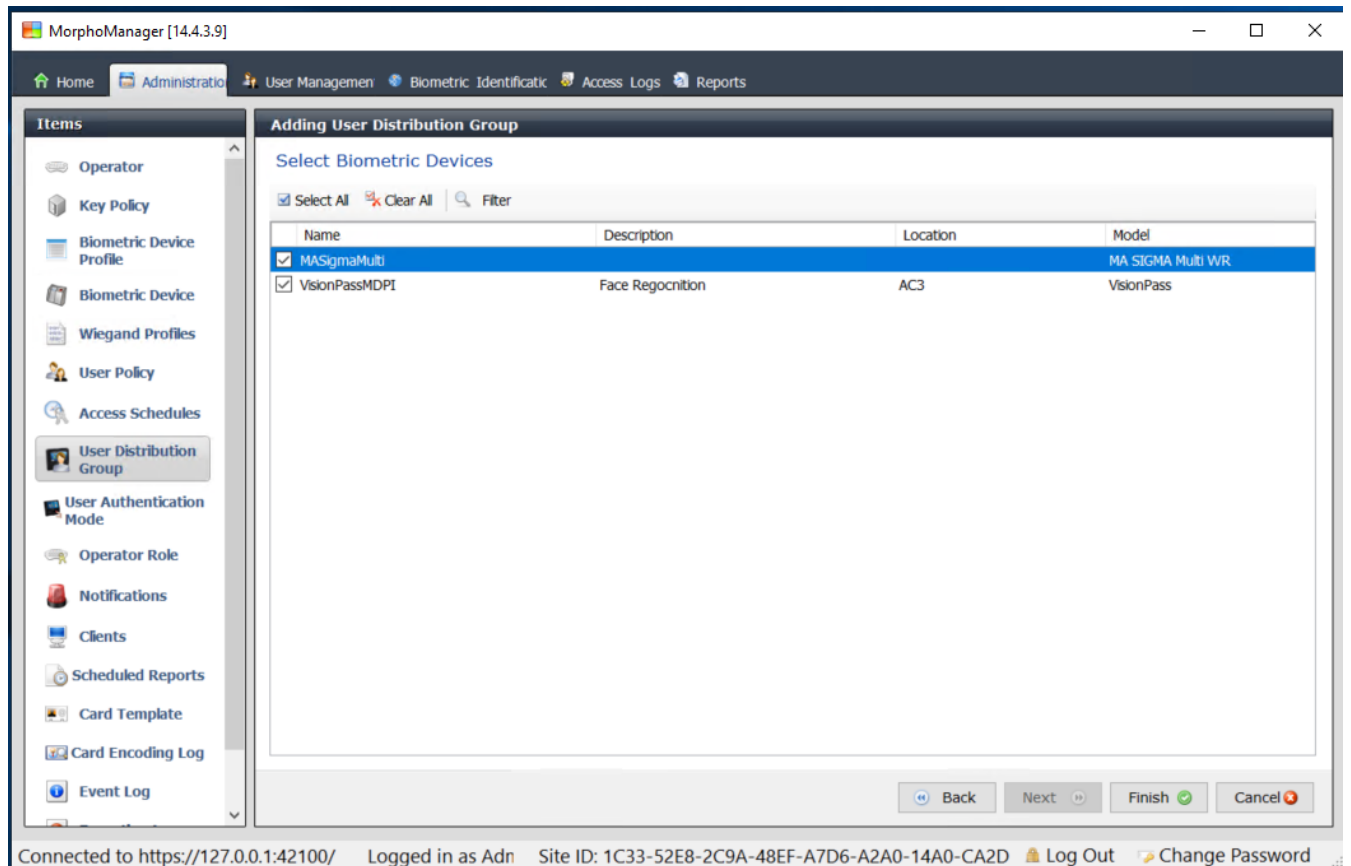
Each User Distribution Group must be mapped to at least one Person Class in the ACS . Therefore, create at least one User Distribution Group for each Person Class that you use.

Procedure:

1. In MorphoManager navigate to **Administration > User Distribution Group**.
2. Click **Add** to create a new User Distribution Group.



3. Click **Next** until you reach the page titled **Select Biometric Devices**.
4. Select the check boxes of those biometric devices that the persons of this User Distribution Group are to use.



5. Click **Finish**

22.4.6 Setting up ODBC for BioBridge

Introduction

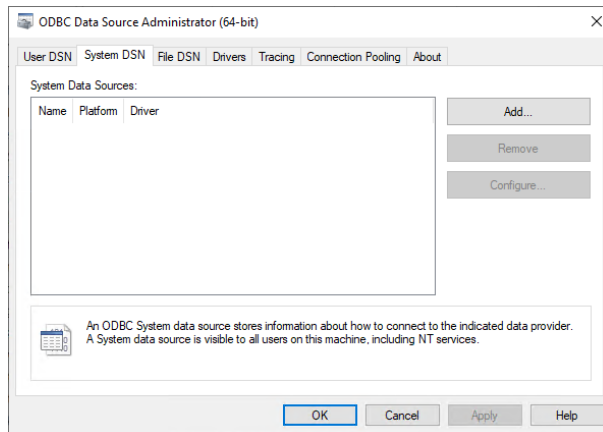
Open Database Connectivity (ODBC) is a prerequisite for use of MorphoManager BioBridge. ODBC is a standardized programming interface for accessing different databases. The recommended driver is `OdbcDriver17SQLServer`

- For BIS the driver is located on the BIS installation media at `BIS\3rd_Party\OdbcDriver17SQLServer`
- For AMS, download the driver from www.microsoft.com

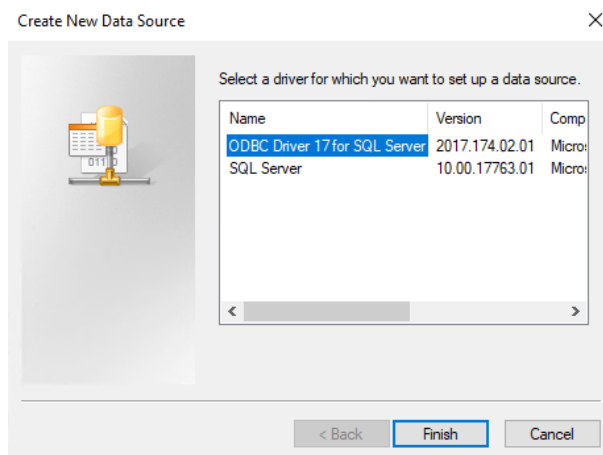
Creating a Data Source

Creating a Data Source name (DSN) for ODBC

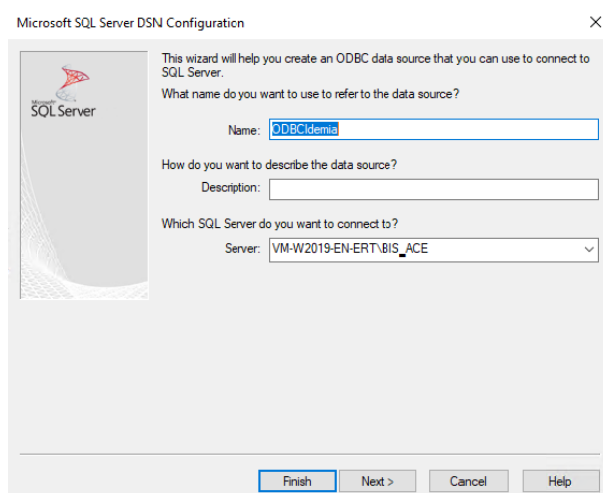
1. In the Windows Control Panel select **Administrative Tools**.
2. Select `ODBC Data Sources (64-bit)` from the list.
3. Select the **System DSN** tab.



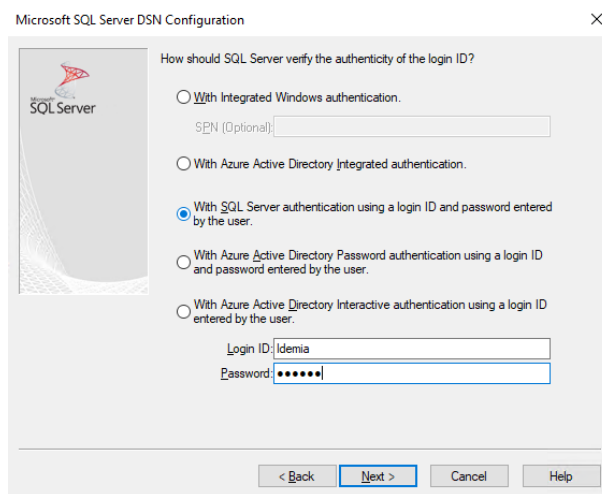
4. Click **Add** to select a driver.
5. Select ODBC Driver 17 for SQL Server as the driver, and click **Finish**.



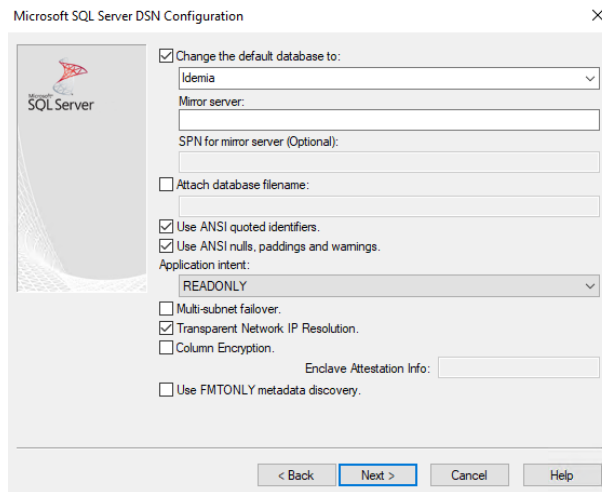
6. Enter the following details for the Data Source.
 - **Name:** a name for the data source
 - **Description** (optional)
 - **Server:** the name of the computer where the ACE database is installed, and the name of the database (default: <MyACS server>\ACE)



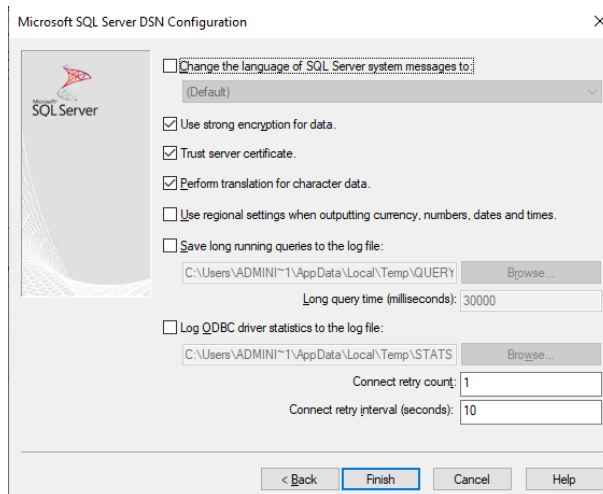
7. Click **Next >**
A dialog appears to collect login information



8. Select **With SQL Server authentication using a login ID...**
9. Enter the following information:
 - **Login ID:** The user name of the Idemia database user as configured in the ACS. This is always `Idemia`.
 - **Password:** The password that was set for the Idemia database user, when it was configured in the ACS.
10. Click **Next >**
11. In the next dialog, select the check boxes:
 - **Change the default database to:** and select `Idemia`
 - **Use ANSI quoted identifiers**
 - **Use ANSI nulls, paddings and warnings**
 - **Transparent Network IP Resolution**
12. Set **Application intent** to `READONLY`

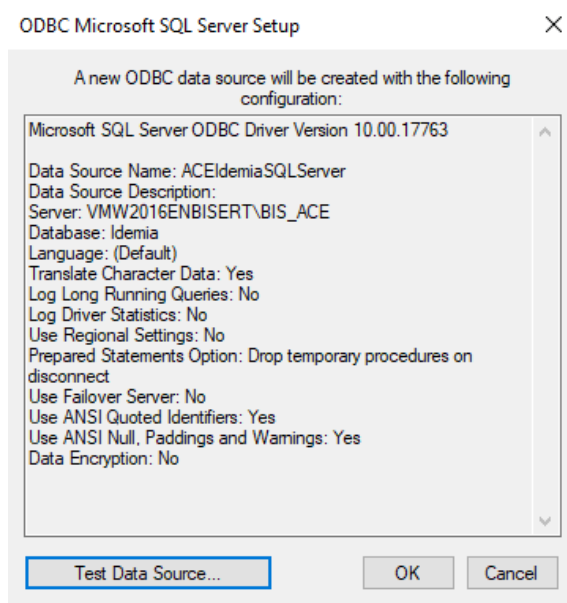


13. Click **Next >**
14. In the next dialog, select the check boxes
 - **Use strong encryption for data**
 - **Perform translation for character data**
 - **Trust server certificate**

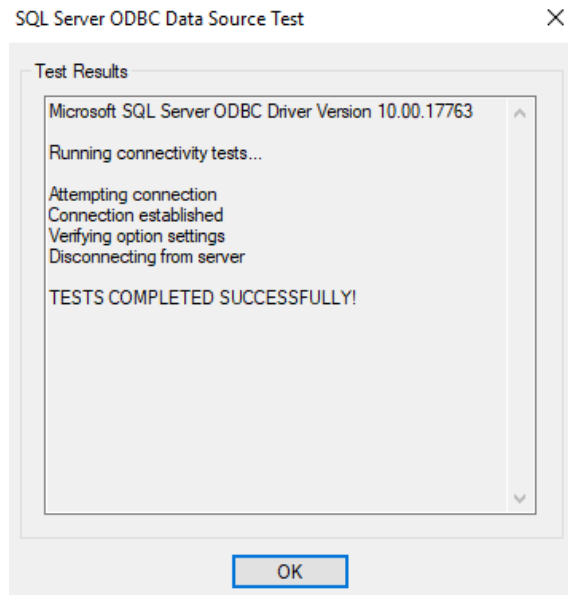


15. Click **Finish**

16. In the next dialog, review the summary data



17. Click **Test Data Source...** and ensure that the tests complete successfully



18. Save all changes and exit the ODBC setup wizard.

22.4.7

BioBridge System Configuration

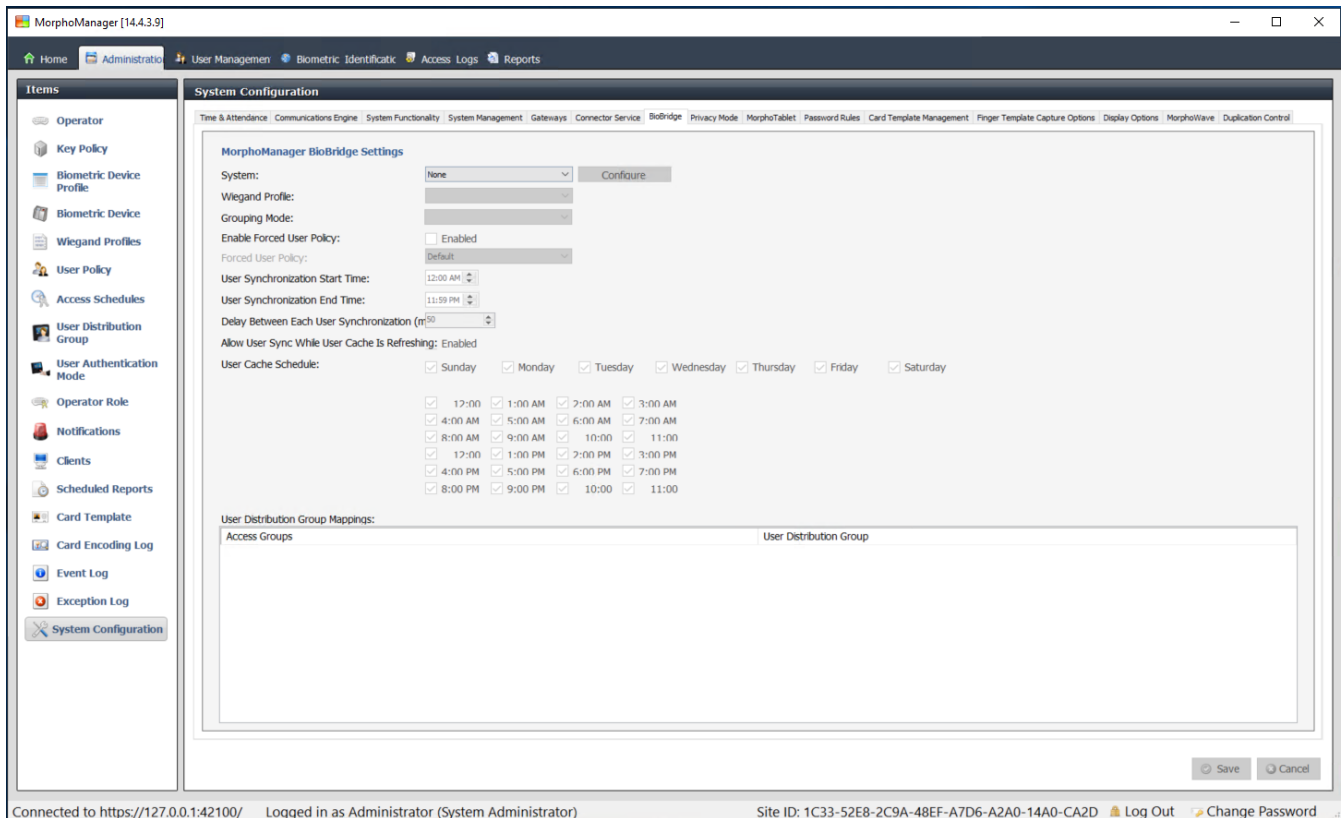
This section describe the remaining settings required for access control systems to use the BioBridge interface.

Prerequisite

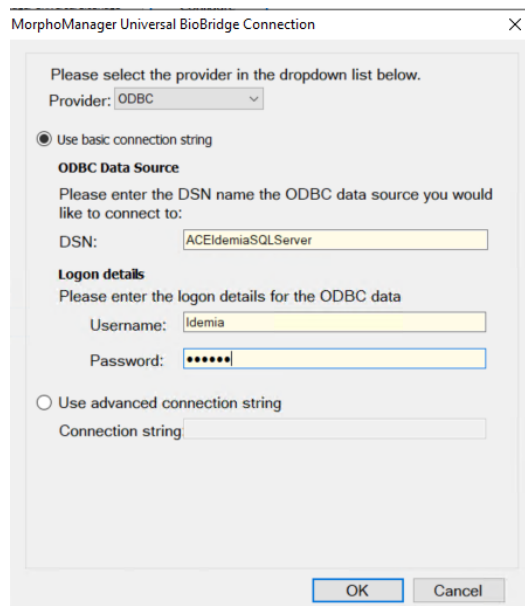
ODBC is set up for BioBridge. See *Setting up ODBC for BioBridge*, page 169

Procedure:

1. In MorphoManager navigate to **Administration > System Configuration**.
2. Select the **BioBridge** tab



- In the **System** drop-down list, select MorphoManager Universal BioBridge
- Click **Configure**
A popup dialog appears.



In the popup window

- In the **Provider** drop-down list, select ODBC
- Enter the DSN (Data Source Name) from the ODBC setup.
- Under **Logon details**, enter the username (Idemia) and password as defined in the ODBC setup.
- Click **OK** to return to the **System Configuration** dialog.

In the **System Configuration** dialog

1. For **Wiegand Profile**: select from the list the Wiegand profile that you defined earlier.

Grouping mode:

This setting determines how MorphoManager should map MM Universal BioBridge users to MorphoManager User Distribution Groups. Select one of the following:

- **Automatic**: This mode will automatically match **Access Level groups** from MM Universal BioBridge to MorphoManager **User Distribution Groups**, if they have the same naming convention.
- **Manual**: If the **Access Level groups** of MM Universal BioBridge and the **User Distribution Group(s)** of MorphoManager are not the same, then you can perform the mapping manually in **User Policy Mappings**.

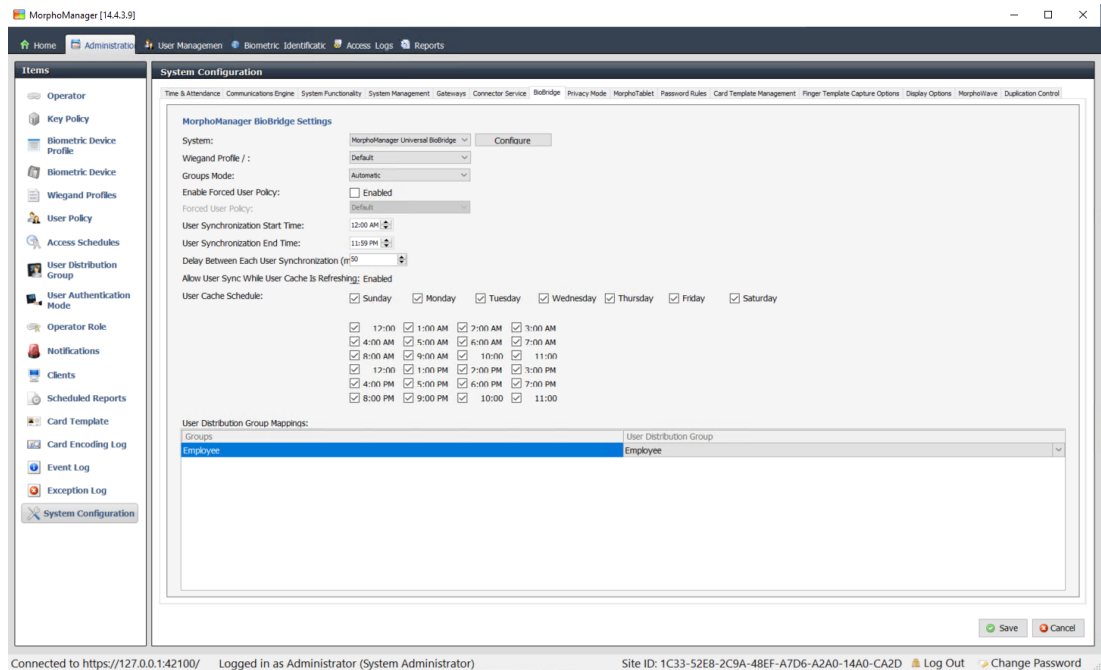
Other settings

In most cases the following settings can be left at their default values:

Enable Forced User Policy	When selected, all users that are enrolled in the BioBridge enrollment client will receive the User Policy that is selected from the adjacent list. If you select this check box, always use the User policy named <code>Per User</code>
User Synchronization Start Time and End Time	The user synchronization engine will only be permitted to run between these two times.
Delay between Each User Synchronization	The time interval between user synchronizations. Increasing the delay will save system resources, but increase the time for all the users to be updated.
Allow User Sync While User Cache Is Refreshing	When enabled, the User Synchronization engine will run in parallel to the User Cache Refresh. This is very taxing on system resources. It is recommended that you disable this setting when using large databases.
User Cache Refresh Schedule	The days and times when the user cache may be refreshed. For the highest accuracy, this should be at all times, but for the performance of systems with large databases, a compromise is required.

User Distribution Group mappings

- In the mappings table, ensure that all **Groups (Personnel classes** defined in the ACS) are mapped to **User Distribution groups** (defined MorphoManager).



22.5

Configuring the BioBridge Enrollment Client

Introduction

A BioBridge enrollment client is a computer at which you can create biometric records for users of the access control system. The setup of a BioBridge enrollment client has 3 parts:

- Adding an enrollment operator to MorphoManager
- Configuring the MorphoManager client computers for enrollment tasks
- Testing the enrollment client

Prerequisites

MorphoManager BioBridge is installed on every ACE workstation from which you perform biometric enrollment for IDEMIA systems.

22.5.1

Adding an enrollment operator to Morpho Manager

Procedure

Follow the instructions in the MorphoManager client installation guide.

Note: for security reasons, Active Directory user accounts are recommended.

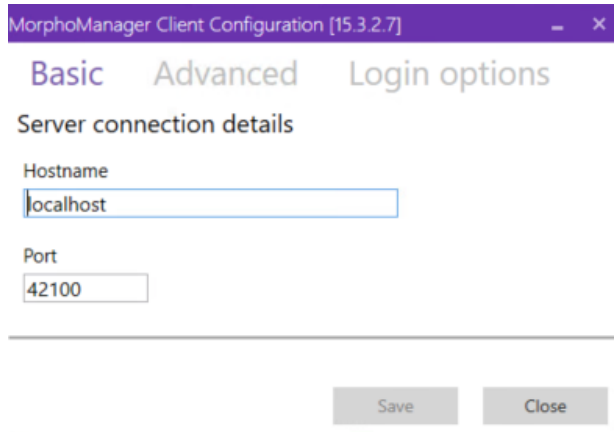
22.5.2

Configuring the MorphoManager client computers for enrollment tasks

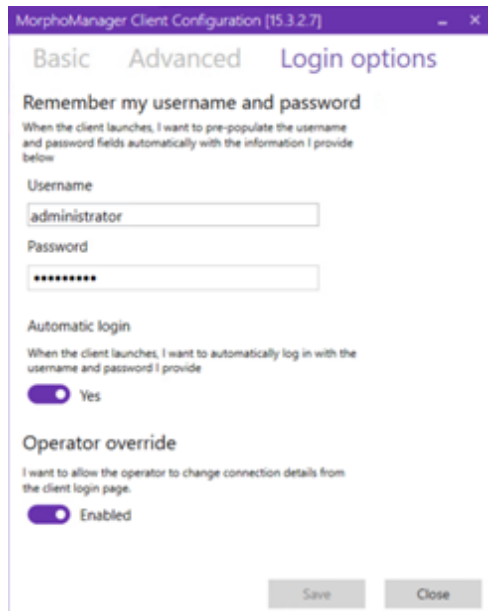
Perform this procedure on each computer that you wish to use for biometric enrollment.

Procedure

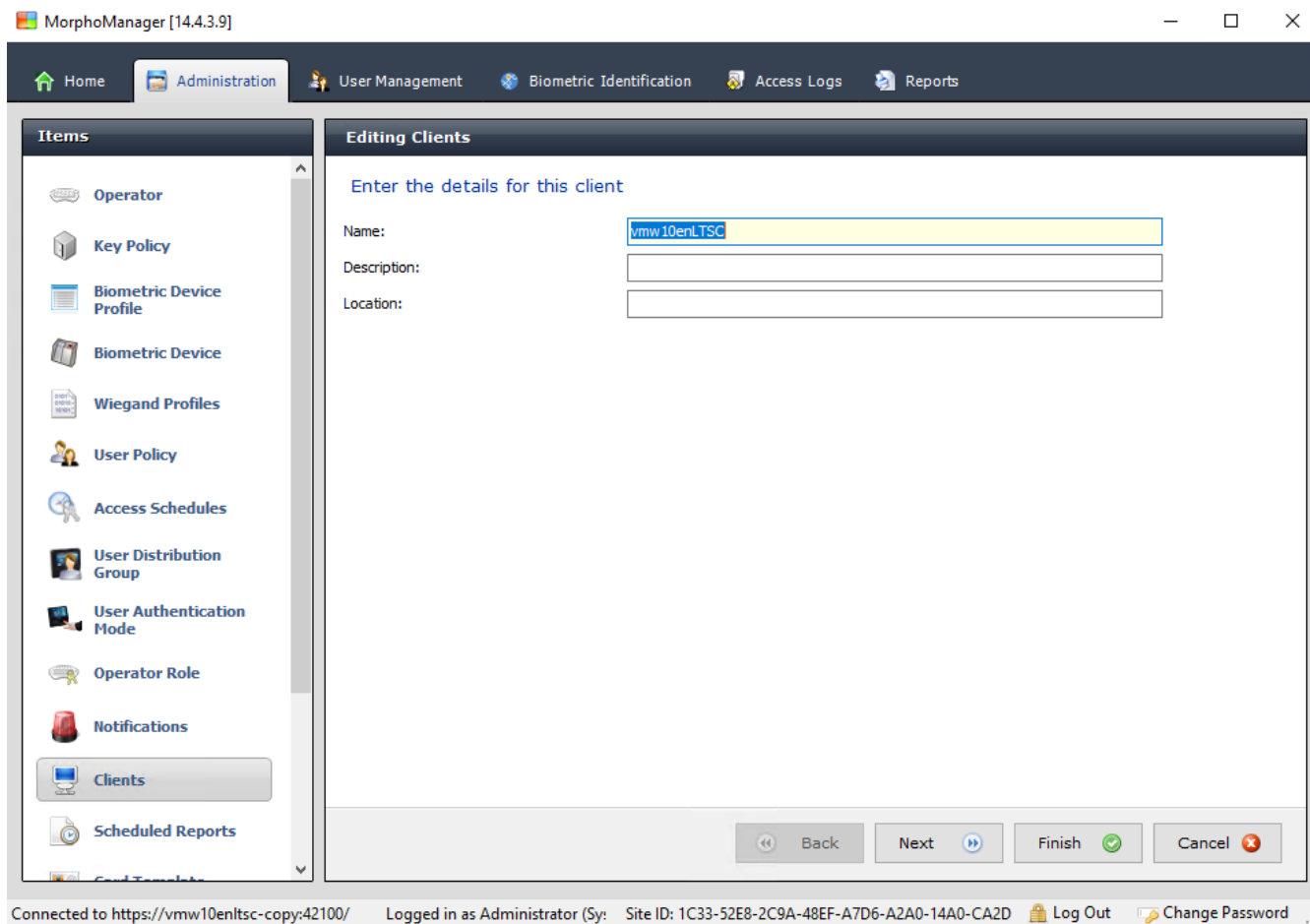
1. In the MorphoManager installation directory (default: `C:\Program,Files(x86)\Morpho\MorphoManager\Client\`) execute the file `ID1.ECP4.MorphoManager.AdvancedClientConfig.exe` as administrator



2. On the **Basic** tab, enter the Hostname of the Morpho server under **Hostname**.
3. For secure installations, use Active Directory or native username and password, as per the Morpho documentation.
4. Alternatively [NOT recommended for highly secure installations] on the **Login options** tab



- Enter the username and password that you entered for the enrollment operator in the previous section
 - Set the **Automatic login** switch to *Yes*
1. In the MorphoManager installation directory (default: `C:\Program Files (x86)\Morpho\MorphoManager\Client\`) execute the file `Start_ID1.ECP4.MorphoManager.Client.exe` as Administrator
 2. Navigate to **Administration > Clients**
 3. Select a client computer
 4. Click **Edit**



5. Enter the name of the intended enrollment client, and optionally the location and a description
6. Click **Next**

MorphoManager [14.4.3.9]

Home Administration User Management Biometric Identification Access Logs Reports

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role
- Notifications
- Clients
- Scheduled Reports

Editing Clients

Select the tabs displayed on this Client

Tab Name	
Administration	<input checked="" type="checkbox"/>
User Management	<input checked="" type="checkbox"/>
Reports	<input checked="" type="checkbox"/>
Access Logs	<input checked="" type="checkbox"/>
Onsite/Offsite	<input type="checkbox"/>
Biometric Identification	<input checked="" type="checkbox"/>

⚠ Changing the visibility of tabs requires a logout/restart of MorphoManager

Back Next Finish Cancel

Connected to https://vmw10enlts-cop:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D Log Out Change Password

7. Select the check boxes of the tabs that you want to display on the enrollment client:
 - **Administration,**
 - **User Management,**
 - **Reports,**
 - **Access Logs,**
 - **Biometric Identification**
8. Click **Next**

MorphoManager [14.4.3.9]

Home Administration User Management Biometric Identification Access Logs Reports

Items

- Operator
- Key Policy
- Biometric Device Profile
- Biometric Device
- Wiegand Profiles
- User Policy
- Access Schedules
- User Distribution Group
- User Authentication Mode
- Operator Role
- Notifications
- Clients
- Scheduled Reports

Editing Clients

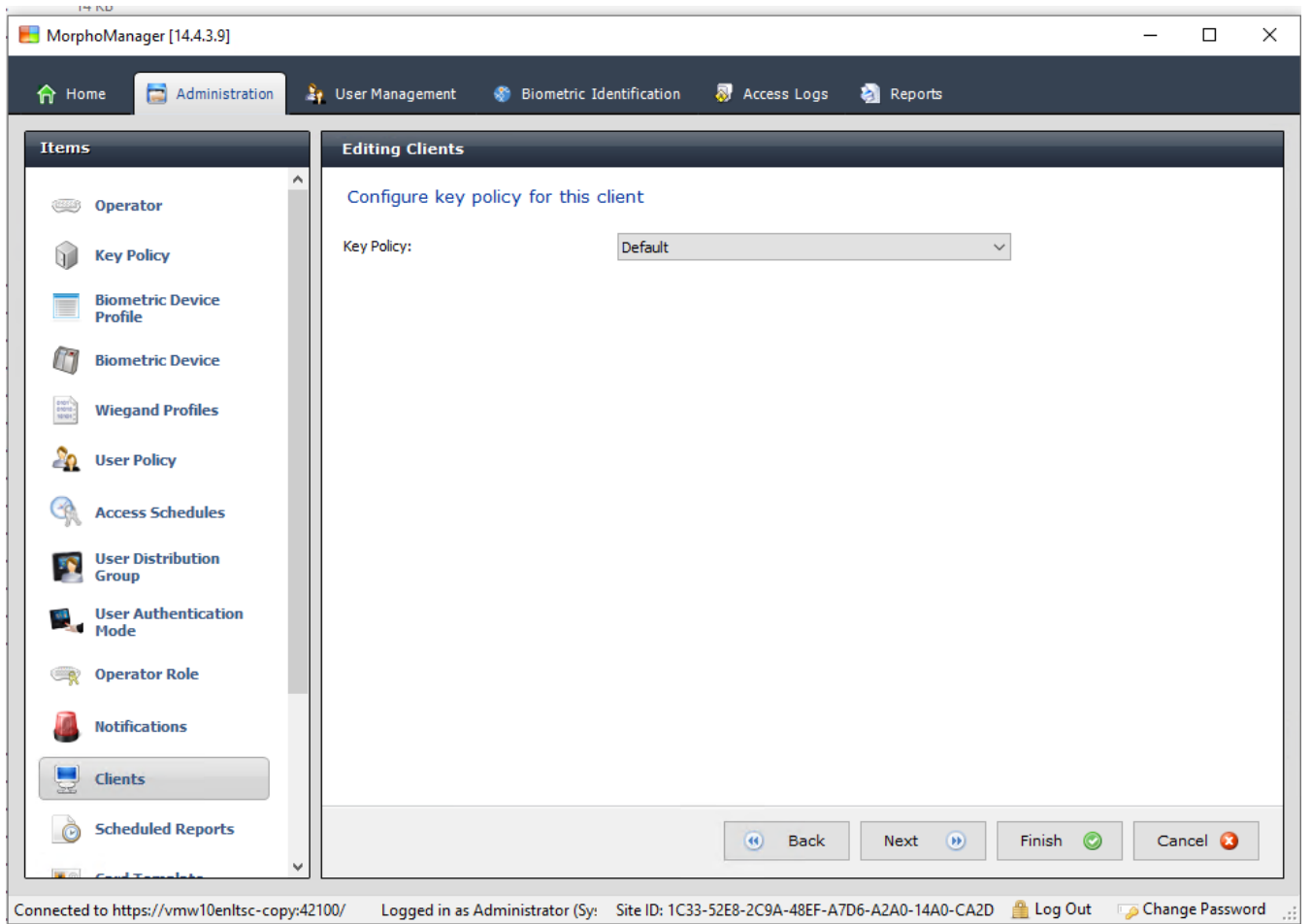
Configure Camera for this client

Camera: No Camera

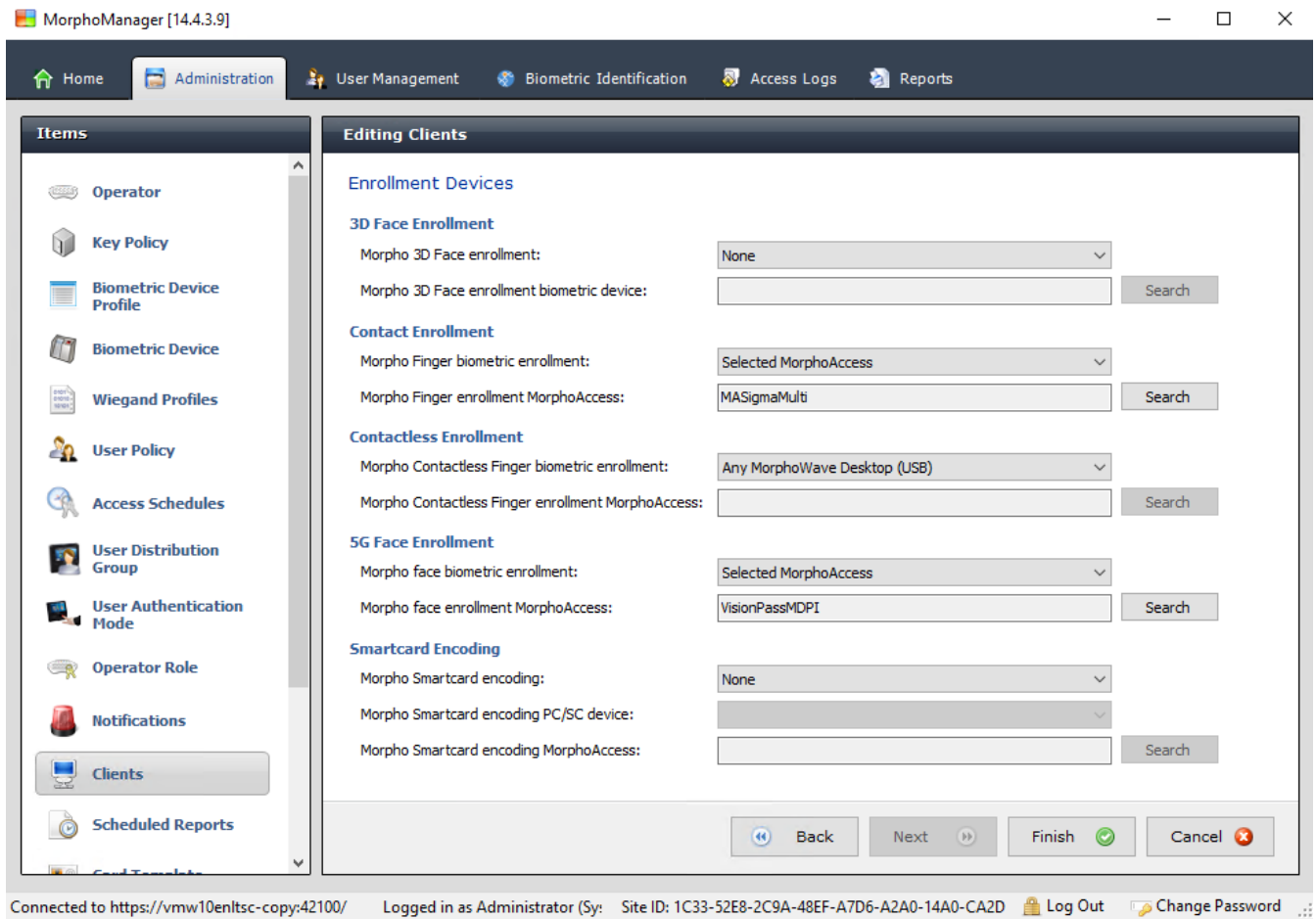
Back Next Finish Cancel

Connected to https://vmw10enlts-copy:42100/ Logged in as Administrator (Sy: Site ID: 1C33-52E8-2C9A-48EF-A7D6-A2A0-14A0-CA2D) Log Out Change Password

9. For **Camera:** select No camera from the list
10. Click **Next**



11. For **Key Policy** select `Default` from the list
12. Click **Next**



13. Select the biometric enrollment reader that you want to use on the enrollment workstation
14. Click **Finish**
15. Close the MorphoManager application

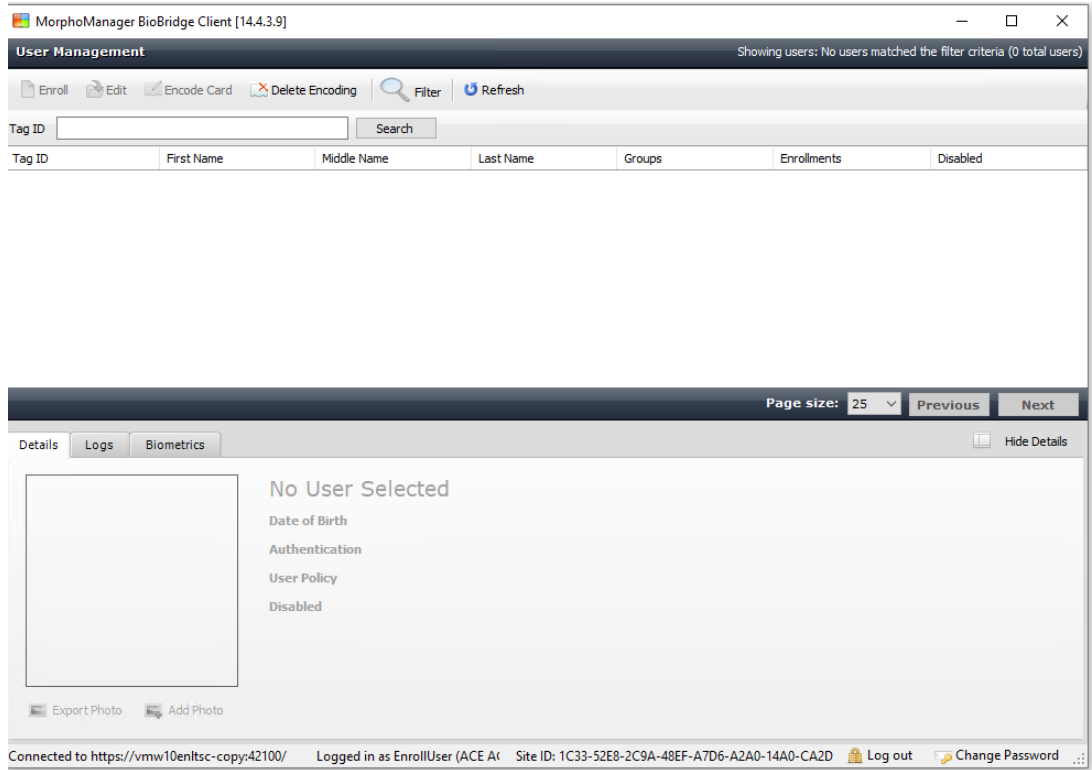
Refer to

- *Configuring the BioBridge Enrollment Client, page 176*

22.5.3

Testing the enrollment client

1. In the MorphoManager installation directory (default: C:\Program Files (x86)\Morpho\MorphoManager\Client\) execute the file `ID1.ECP4.MorphoManager.BioBridgeEnrollmentClient.exe`



1. Make sure that you can invoke the enrollment screen without having to enter the username and password of the enrollment operator.

22.6 Technical notes and limits

Officially supported windows operating systems

IDEMIA supports the same Windows 10 versions as the Bosch ACS.

Officially supported version of Microsoft SQL Server

The support version is SQL Server 2017

One IDEMIA system per Access System

A Bosch access control system can support only one IDEMIA system.

One IDEMIA card per cardholder.

Bosch access control systems support multiple cards per cardholder, but IDEMIA supports only one. Therefore, upon enrollment, and when synchronizing with BIS, the first valid card (that is, where status=1) of type “Access”, “Temporary” or “Parking” is assigned to IDEMIA. If the card is later blocked, its number is still transmitted and recorded in the event log.

Maximum number of IDEMIA cardholders

The BioBridge MorphoManager can handle up to 100,000 cardholders.

Maximum number of access groups

IDEMIA supports up to 5000 access groups (user distribution groups). These are mapped to **Person classes** in the Bosch access control system.

Performance of templates download

- 1000 templates to 1 device: Download takes under 1 minute.
- 1000 templates to 100 devices: Download in some minutes.

IDEMIA does not support Divisions

Where an IDEMIA system is integrated, an ACS system is not able to screen the cardholders of one Division reliably from the access control operators of another Division. If absolute privacy is mandatory between Divisions, do not integrate an IDEMIA system.

Virtual Cards / Access by PIN code alone.

IDEMIA does not support access by PIN code alone. A physical card is required.

IDEMIA duress-finger functionality

The IDEMIA duress finger functionality is currently not supported by AMC controllers.

Minimum set of identification criteria.

Enrollment in the IDEMIA system requires at least the following identification criteria:

- First name,
- Last name,
- Person class
- One physical card assigned to the cardholder.

States displayed on the readers

No reader state (e.g. "Device Blocked") is displayed on Wiegand and OSDP readers.

Backup and Restore

Before restoring a backup of with IDEMIA, delete and recreate the IDEMIA database using the IDEMIA DataBridge provider tool.

In the **Biometric device** dialog, make sure that all configurations were sent correctly to the IDEMIA readers. If one of the synchronization tasks has failed, rebuild the reader configuration:

1. In MorphoManager, go to **Biometric device**.
2. Select the affected device.
3. Click **Rebuild**.

Compatibility of ACS card functionalities with IDEMIA authentication modes:

Functionality	Mode: Card AND Bio	Mode: Card OR Bio
Access cards: Insert	OK	OK
Access cards: Update	OK	OK
Access cards: Delete	OK	OK
Access cards: Multiple cards	First card only	First card used for biometry.
Replacement card	OK	OK
Temporary card	OK	OK
Temporary card: Period only	OK	OK

Temporary card: Period deactivate all cards immediately	OK	OK
Temporary card: Activate cards automatically after set period	OK	OK
Temporary card: Deactivate cards and activate automatically	OK	OK
Alarm cards	Not supported	OK
Office mode	Not supported (*)	Not supported (*)
Visitor	Possible that biometric data of first visitor remain assigned to the card.	Possible that biometric data of first visitor remain assigned to the card.
Guard	Not supported	No biometry supported. Card works.
Parking Card	OK	OK
PIN code	Not supported (*)	Not supported (*)
3rd party validation	No PIN code (*)	No PIN code (*)
(*) IDEMIA reader not usable as a keypad reader		

23 Achieving EN 60839

Introduction

EN 60839 is a family of European international standards for the hardware and software of the following:

- alarm and electronic security systems
- electronic access control systems

To ensure compliance of your access control system with this standard, parts of the configuration may need to be adapted. The following list contains the most important parts. For a complete list, please consult the standard as adopted in your own country.

Requirements to use AMS 4.0 as an EN 60839 certified system, grade 2

- The system meets the requirements for Global anti-passback in terms of using one zone per MAC.
- The different useable times zones of the AMS system depends on the numbers of MACs. A separate time zone can be used for each MAC.
- The wiring of door contacts must not prevent the door's opening for an emergency evacuation triggered by a fire- or intrusion-prevention system.
- Only OSDP readers use encryption on the RS485 interface.
- Access to the configuration mode must be strictly controlled. This can be achieved, for instance, by locating the computers in secured areas, and by timeouts on login sessions, particularly timeouts for inactivity at application and operating system level.
- Network and electric cabling must be laid in a secure area or encased in pipes.
- Only the card readers may be mounted in non-secured areas; all other devices must be in secured areas.
- The minimum length of verification PINs for biometric or physical credentials must be set to at least 4.
- The minimum length of identification PINs must be set to at least 8.
- The main server computer, connection servers, MAC servers and clients must be synchronized with a network time server.
- Power monitoring must be enabled on local access controllers (e.g. AMCs).
- Offline functioning of local access controllers (e.g. AMCs) is only permitted during network failures. For example, the AMC parameter **Host timeout** must not be set to 0.

Rules for password strength

- The minimum length of the password must be at least 5 characters.

24

Defining access authorizations and profiles

24.1

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**



24.2

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.


- ACE Client: **System data > Access profiles**
- 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.

25 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?

25.1 Persons

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

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

Tab	Field name
-----	------------

Dialog header	Name
	First name
	Birth name (called maiden name in some cultures)
	Personnel no.
	Date of birth
	Employee ID (also known as Person type)
	Gender
	Company
	Title
	ID card no.
	Car license no.
	Address
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.

Refer to

- *Custom Fields for personnel data, page 131*

25.1.1

Card control or Building control options

Overview

Use the **Card control** tab to give cardholders the ability to activate 1 or 2 generic access controller outputs with their card. You assign the ability to a cardholder by selecting a **Building control** check box in the **Persons** dialog. The **Building control** (or **Card control**) check boxes are predefined custom fields that are visible on the Person's **Card control** tab by default, but can be positioned elsewhere.

There are two main tasks for a Building control option. They are described below:

- Configure the check box: Give it a suitable label, and (if desired) position it on a different tab of the **Persons** dialog.
- Assign the function to an output on an AMC access controller and a check box.

Prerequisites

- The access controller output is electrically connected to the device that is to be activated by the card.

Dialog path

- BIS Configuration browser > **Infrastructure** > **ACE Custom fields** > **Card control** tab
- AMS Main menu > **Configuration** > **Options** > **Custom fields** > **Card control** tab

Configuring the check boxes

1. On the **Custom fields** page, select the **Details** tab in the upper pane.
2. Locate the **Building control** function, 1 or 2, that you wish to use.
3. Overwrite the label with a suitable name (recommended). If desired, position the check box on a tab other than **Card control**. See section **Previewing and editing Custom fields** at the link below, for more detailed instructions.

Assigning the function to an output of the access controller and a check box

See section **AMC parameters and settings** at the link below.

1. In the **Device Editor**, in the device tree, select the AMC access controller whose output signal you want to use.
2. On the **Outputs** tab, upper pane, select the output that you wish to use.
3. In the middle pane, **Output data**, select type **25, Card control**
4. Click the > button to add the output to the lower pane.

5. In the lower pane, column **Param11**, select the label of the Building control function that you selected in the previous procedure **Configuring the check boxes**.
6. Save the device tree.

Refer to

- *AMC parameters and settings, page 55*
- *Previewing and editing Custom fields, page 131*

25.1.2 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.

25.1.3 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.


25.1.4 Enrolling fingerprint data

Prerequisites

- One or more fingerprint readers must be configured at the entrances, in order to perform biometric access control.

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

Procedure for enrolling a fingerprint for access

1. Navigate to the fingerprints dialog: **Personnel data > Persons > tab:Fingerprints** and create or find the enrollee in the database.
2. Ask the enrollee which finger they wish to use for regular access at the fingerprint reader.
3. Select the corresponding finger in the hands diagram.
Result: The fingertip is marked with a question mark.
4. Click the **Enroll fingerprint** button.
5. Give the enrollee instructions for presenting their finger at the reader.
Example instructions can be read from the dialog pane below the hands diagram, but different reader types may require slightly different procedures.
6. If the fingerprint is successfully enrolled, a confirmation window will appear.
7. Select an **Identification mode**; this determines what credentials a fingerprint reader will demand of the enrollee when they request access. Note that the mode set here will only take effect if the reader parameter **Person-dependent verification** has been selected.
The options are:
 - **Fingerprint only** - Only the fingerprint scanner in the reader is used
 - **Card only** - Only the card scanner in the reader is used
 - **Card and fingerprint** - both scanners in the reader are used. The enrollee will have to present both card and chosen finger at the reader, to obtain access.
8. Click **Accept** to store the fingerprint and identification mode for the enrollee.
9. 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:

- Fingerprint readers can only send duress signals if they are configured in the **Device Editor** with the following setting
Network & Operation modes tab > **Templates on server > Card and fingerprint**

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

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

Procedure for testing stored fingerprints

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

Procedure for deleting stored fingerprints

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

25.1.5 Enrolling palm vein data

Biometric verification

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

At least 2 biometric readers must be configured in the system, before biometric ID verification can be profitably used:

- A reader connected to an operator workstation for enrollment of biometric data.
- One or more readers at entrances to verify the identities of cardholders.

Prerequisites:

- The palm vein reader is licensed and configured in the software of the manufacturer. You have defined the following:
 - IP address of the reader
 - Reader ID (1 or 2) to distinguish between readers on the same biometric controller.
- You have carefully noted the reader's password, as provided by the installer of the reader.

Configuring the palm vein reader on an operator workstation

Dialog path

- BIS configuration browser > **Infrastructure** > **ACE Card reader**

Procedure

1. In the **Workstations** pane, select the workstation to which you want to connect the palm vein reader.
2. In the **Workstations** pane, click the green plus icon.
3. In the **Card reader** pane, enter the following data:
 - **Type:** Select **Palm vein sensor** from the drop-down list.
 - **IP address:** Enter the IP address of the palm vein reader controller.
 - **Reader ID:** Select the palm vein reader ID from the drop-down list.
 - **Password:** Enter the password that has been provided by the installer of the reader.
4. Click **Apply** to apply and save the changes, or click **Discard** to cancel the changes.

Creating a biometric controller in the device tree

Dialog path

- BIS Configuration Browser > **Connections**

Procedure

1. On the **Device data** tab, right-click a MAC device and select **New biometric controller** from the context menu.
2. In the PCS controller dialog, enter the required data:
 - **Name:** Enter the name of the controller.
 - **Description:** Enter a description.
 - **IP address:** Enter the IP address of the palm vein reader controller.
3. Click **Apply**, to apply and save the changes, or click **Discard** to cancel or remove the applied changes.

Adding a palm vein reader to a biometric controller

1. On the **Device data** tab, expand the device tree, right-click a **PCS controller device** and select **New palm vein reader** from the context menu.
2. In the PCS palm vein dialog, enter the required data:
 - **Name:** Enter the name of the palm vein reader.
 - **Description:** Enter a description (optional).
 - **Division:** Select a division.
 - **Reader terminal / bus address:** Enter the reader ID, 1 or 2.
 - **Number of retries:** Enter the maximum number of attempts allowed.
 - **Password:** Enter the password that has been provided by the installer of the reader.
3. Click **Apply**, to apply and save the changes, or click **Discard** to cancel or remove the applied changes.


Enrolling a palm vein pattern for ID verification

Prerequisites:

- The palm vein reader is configured on your operator workstation.
- The palm vein reader is powered on and connected to the network.
The palm vein reader is presenting constant blue lights.

- You are acquainted with the manufacturer’s instructions for the enrollment process with your palm vein reader.
- The enrollee has already been defined as a cardholder in the system.

Procedure

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

Testing a stored palm vein pattern

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

Deleting a stored palm vein pattern

1. Navigate to **Personnel data > Persons > tab: Palm vein**

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

LED light signals

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

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

Using a palm-vein reader at an entrance



Notice!

Reader offline

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

1. Present your card to the card reader.
If verification by palm vein pattern is required, the palm vein reader now signals readiness to read.
2. Hold your palm over the palm vein reader until it displays either green or red lights.
 - **Green:** The palm vein pattern matches the pattern stored for you. Access granted.
 - **Red:** The palm vein pattern does not match the pattern stored for you. Access denied.

25.2

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.

25.3

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.

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

- BIS Configuration Browser menu: **Administration > Operators > tab: ACE operator settings > check box: Global Administrator**.
- Main menu: **Configuration > Operators and workstations > User rights > check box: Global Administrator**.

25.3.1

Assigning cards to persons

Introduction

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

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

Dialog path

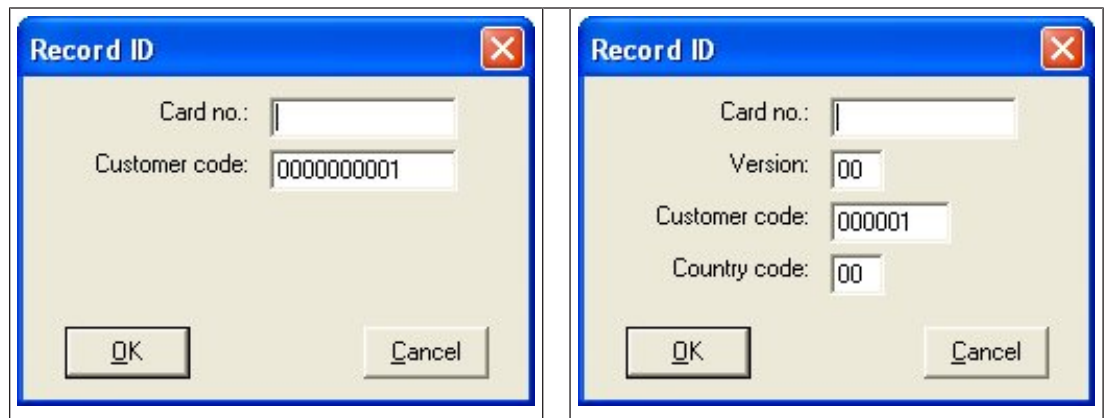
Main menu > **Personnel data > Cards**

Prerequisites

- 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 is configured on your workstation.

Procedure for enrollment

1. Click the  button on the right-hand side of the **Record card** button to select a configured enrollment reader.
- Note that to change the selection of enrollment reader you need to be logged on to the ACE dialog manager as Administrator.
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. In the popup window
 - Select **Replace card** if the original is permanently lost or damaged.
 - Select **Temporary card** if the original has been mislaid or left at home, and only a temporary replacement is required.
 - Enter a validity period for the temporary card.
 - Select if you want to deactivate all other cards now.

- Select if the original cards should be reactivated automatically when the temporary card expires.
4. 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.

25.3.2

Printing badges

Prerequisites

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

Procedure

Dialog path

AMS client: **Personnel data > Print badges**

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

Supported Cameras

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

25.3.3

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 187*
- 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.

25.3.4

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 more time (default is 3x) to pass through an entrance before the state **Door open too long** is generated.

Note: The default extension factor can be reset in the properties of the MAC in the Device Editor.

Select **Global Access Settings > Time factor for handicapped persons**

Tour monitoring

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

Tour monitoring > Define routes dialog.

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

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

Permission to unlock doors

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

Refer to

- *Authorizing persons to set Office mode, page 202*

25.3.5

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 **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.

Office mode is only supported with physical cards.



Notice!

Office mode and device parameters for Door

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

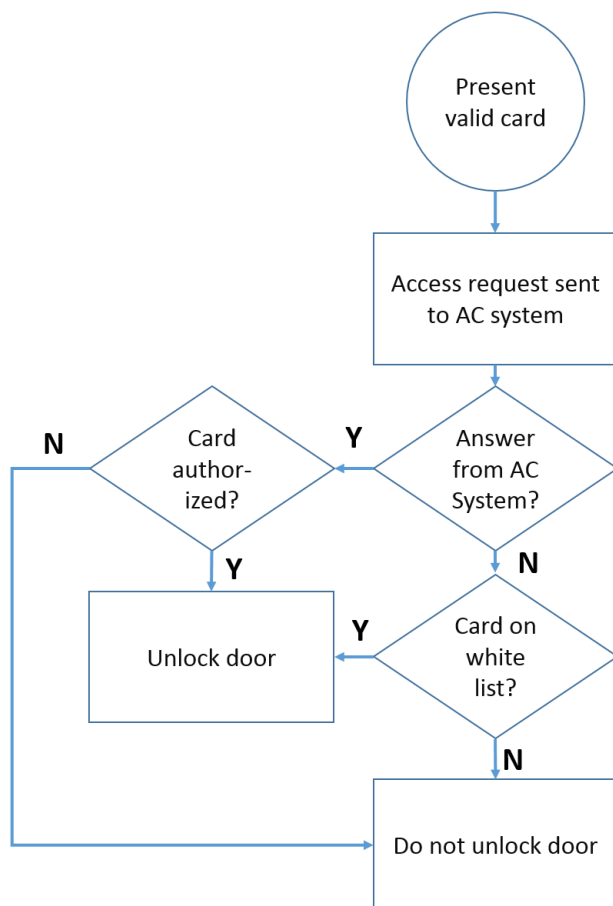
25.3.6

SmartIntego tab

SmartIntego locking systems

Introduction

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



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

Prerequisites

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

The assignment procedure


The following procedure describes how to add a card number to a SmartIntego whitelist, in addition to any authorizations that are already assigned via the main access control system. Whitelists are stored locally on the SmartIntego doors, so that a reader can grant access to the whitelisted card numbers even when the connection to its MAC is broken.


Additions to and deletions from the whitelists are transmitted to the SmartIntego readers as soon as the cardholder data is saved, and a connection is available.


1. In the ACE client menu select **Personnel data > Cards**
2. In the AMS main client menu select **Personnel data > Cards**
3. Select the person to receive SmartIntego authorizations
4. Select the **SmartIntego** tab.
5. 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.

25.3.7 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

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

Dialog path

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

Procedure

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

25.4 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.

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

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 removing **Blocking** does not remove temporary cards. Temporary cards will expire naturally after their validity periods. If required, delete them manually.

Notes on temporary cards

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

25.5 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.

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 all protocols (RS485, Wiegand and LBUS), the cardholder enters **4 # <the PIN>**

Arming and Office mode are only supported with physical cards.

Be sure to inform cardholders how to enter their PINs. If in doubt, consult your system administrator.

PIN-Code for arming intrusion detection systems (IDS)

Input of a 4 to 8 digit PIN (default = 6 - the same length as the verification PIN). This PIN will be used to arm an IDS.

The display of this fields can be parametrized. Only if the control **separate IDS PIN** is activated the control are available.

- Configuration Browser > **Infrastructure** > **System configuration** > **ACE PIN-Codes**
- 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.

25.6

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 Access Management System. The left sidebar contains navigation options: Main menu, Persons, Companies, Print badges, Cards, PIN code, Blocking (selected), Blacklist, Group of persons, Group authorizations, and Areas.

The main area displays the following information for the selected person:

- Name: Musterfrau
- First name: Anita
- Birth name: [Empty]
- Personnel no.: SC41156
- Date of birth: Th 12/14/1995
- Employee ID: Employee
- Gender: Female
- Company: Test_Firma
- Title: [Empty]
- Car license No.: Car2515132
- Card no.: 000000101234

A photo of Anita is shown with the date 10/20/2014 below it.

Below the photo is a table of 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.

The 'Blocking' section at the bottom contains a table with the following columns:

Blocked from	Blocked until	Blocking reason	Last edited by
[Empty table body]			

At the bottom of the blocking section 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.

25.7

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

Name: First name:

Birth name:

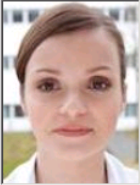
Personnel no.: Date of birth:

Employee ID: Gender:

Company: Title:

Car license No.:

Card no.: Reader..



10/20/2014

Card no.	Application type	PIN lock	Created on	Last printed on	No. of prints	Code data

Reason:

Put card on blacklist

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.

25.8 Editing multiple persons simultaneously

Group of Persons

The screenshot shows the 'Group of Persons' dialog. On the left is a sidebar with icons for: Main menu, Persons, Companies, Print badges, Cards, PIN code, Blocking, Blacklist, Group of persons (selected), Group authorizations, Areas, Change division, PegaSys Stoppage card, and Keys.

The main area contains the following form fields:

- Employee ID: Employee (dropdown)
- Name: * (text input) until starting with: (text input)
- First name: (text input) until starting with: (text input)
- Personnel number: (text input) until starting with: (text input)
- Company: (text input) until starting with: (text input)
- Card: (text input) until starting with: (text input)
- Valid on: (text input)
- Gender: (dropdown)
- Department: (text input)
- Cost center: (text input)

Below the form fields, it says: 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					

At the bottom, there are two dropdown menus:

- Wanted field to change: (dropdown)
- Wanted action: (dropdown)

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.

25.8.1 Group authorizations

Group Authorization

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:

Group authorizations
2 selected persons

Name	First name	Personnel no.
Musterfrau	Anja	SC41156
Mustermann	Max	Sc999000

Authorizations Filter: / 1

Assign	Withdraw	Name	MAC	Time model	Division
No	No	Door	MAC		Common

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.

25.9 Changing the Division for persons

Introduction

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



Notice!

Use this feature with great care!

A change in Division has far-reaching consequences for the personnel records that you change.

Prerequisites

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

Dialog path

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

Procedure

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

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

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

Effects of changing from one division to another

Persons

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

Companies

- Links to companies of the previous division are deleted.

Effects of changing from Common to another division

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

Effects of changing from one division to Common

All links are retained.

25.10

Setting the area for persons or vehicles

Introduction

This section describes how to change the recorded location of a cardholder or their vehicle from one defined area to another. This may become necessary if the cardholder has passed from one area to another without scanning their card. In such circumstances strict antipassback systems will deny further access to the cardholder until their actual and recorded locations match.


Prerequisites

- Access areas have been defined in your system, and are in use. For documentation, see the link below.
- As operator you are authorized to modify the cardholder's data.

Procedure for resetting the location of individual cardholders and vehicles

Dialog path

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

1. Select the cardholder from the database as usual
2. In the **Location** list, select a new location
or
3. In the **Location of the vehicle** list, select a new location for the cardholder's vehicle
4. Click  to save

Refer to

- *Configuring areas of access control, page 24*

25.10.1

Procedure for resetting the location of all cardholders and vehicles

This procedure may become necessary, for example, after an evacuation drill. All locations are set to **UNKNOWN** so that access sequence monitoring and antipassback can resume.

Procedure

Dialog path

Main menu > **System data** > **Reset areas unknown**

- Click **Set the areas of all persons present to UNKNOWN**
- or
- Click **Set the areas of all parking vehicles to UNKNOWN**

25.11 Customizing and printing forms for personnel data

Overview

Use **Forms** to customize forms for printing cardholder data from the database. This functionality may be required by your local data-privacy laws.

Template forms are provided. These templates can be exported as HTML files, customized to your requirements and reimported for use in dialog manager.

Instantiate and print the forms from the **Personnel data > Print badges** dialog.

Dialog path

- AMS Main menu > **Configuration > Options > Forms**

Customizing a form

1. On the **Forms** dialog, **Available forms** list, select the template that you wish to customize, typically `AllPersonalData_EN`, which contains all personal data fields in the database.
2. Click **Export** to save the form to a new HTML file on your system
3. Use an HTML editor to customize the HTML file to your requirements
4. On the **Forms** dialog, click **Insert** to import the customized HTML file into the dialog manager.
 - (Optional) if the form is valid only for a particular Division, select a Division for the new from the **Division** column.
 - (Optional) click **Preview** to view the uninstantiated form in an HTML viewer.
 - (Optional) click **Delete** to delete a form from the list.

Instantiating and printing a form

1. In the dialog manager, navigate to
 - AMS main menu > **Personnel data > Print badges**
2. Load the desired personnel record into the form
3. Select a form from the **Form** list.
4. Click **Print form**
 - The form is instantiated with the data of the selected personnel record, and sent to the printer of your choice.

26 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.

26.1 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.

« Main menu

Visitor

Visitor cards

Division: Common

Last name: Visitor11 First name: Firstname11

Birth name: Birth name: Date of birth: Tu 03/16/1976

Street, no.: Street, no.: Zip code / City: Zip code / City:

Phone: Phone:

Car license No.: Car license No.:

Employee ID: Visitor Company: Company:

Official pass

Passport

Driver's licence

Identity card

Other:

Number: Number:

Card no.: Card no.: Reader.. Reader..

Additional data Authorizations Form/Photo Signature

Attendant: Attendant: Reason: Reason:

Remark: Remark:

Expected arrival: Tu 07/18/2017 12:00 AM Expected departure: Expected departure:

Date of arrival: Date of arrival: Date of departure: Date of departure:

Visited person: Visited person: Extended door opening time

Location: Location:

Card no.	Application type	PIN lock	Collecting date	Code data
----------	------------------	----------	-----------------	-----------

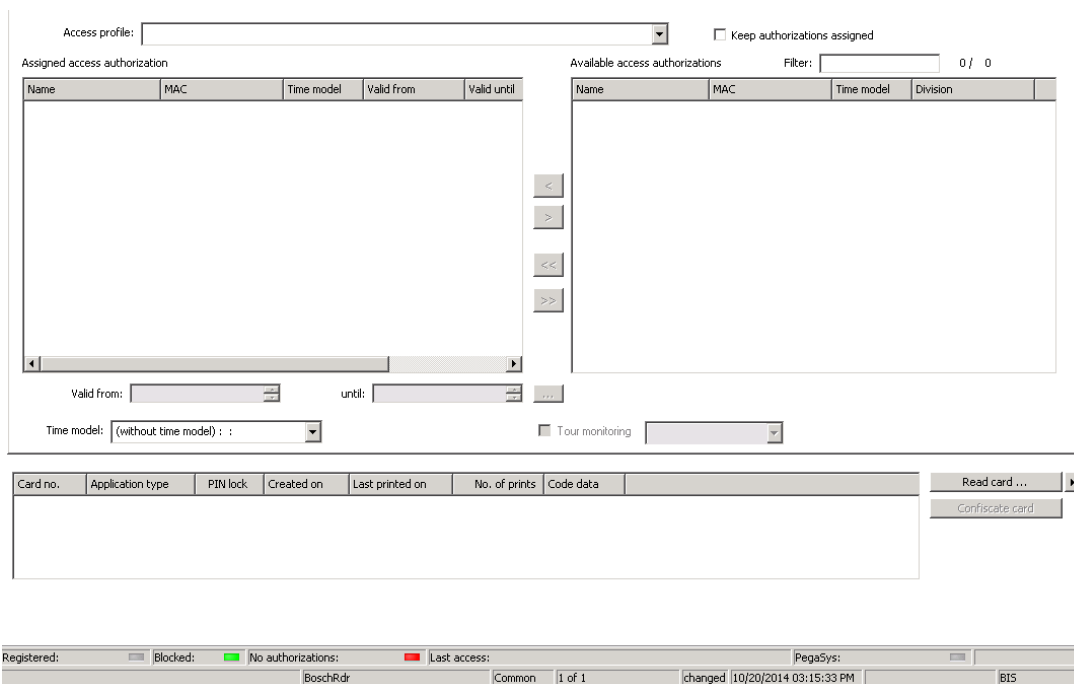
Read card ...

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.



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

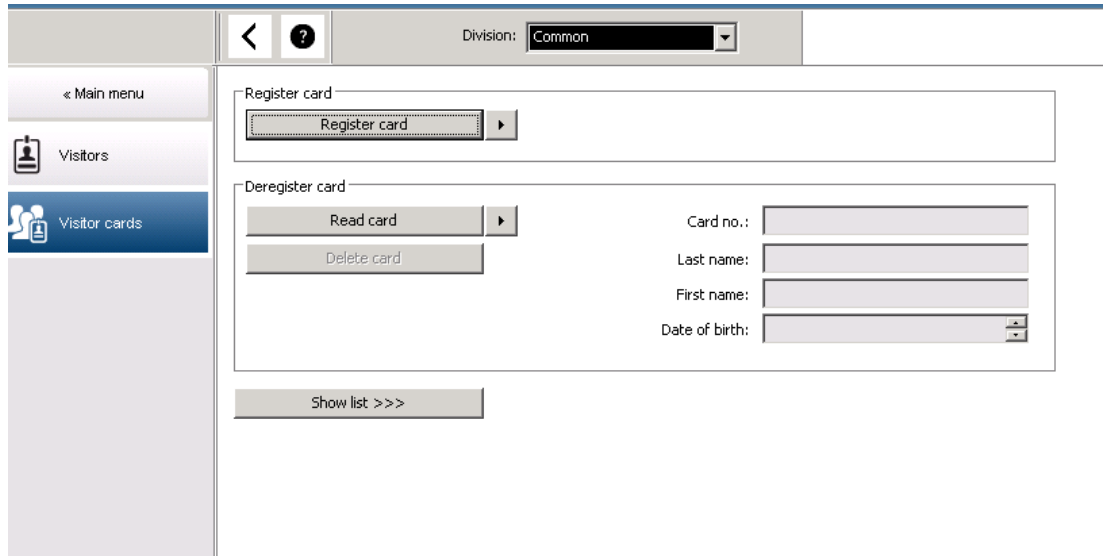
Some cards in the system are reserved as visitor cards. Normally a visitor card is assigned to an incoming visitor and returned when that visitor leaves. Then the card can be reused.

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.

Visitor pass	
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; margin-top: 10px;"> _____ _____ </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Location, date Sign of visitor </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

26.2 Visitor too late

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

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

Events that lead to the message Visitor too late:

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

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

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

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

```
HKLM\Software\Micos\SPS\Default\VLDP\Interval
```



Notice!

The generation of this message can be deactivated in the server's registry under:

```
HKLM\Software\Micos\SPS\Default\VLDP\Active
```

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

It is checked:

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

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

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

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

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

Filter		Vehicle search: 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**.

27 Managing parking lots

27.1 Overstayed parking

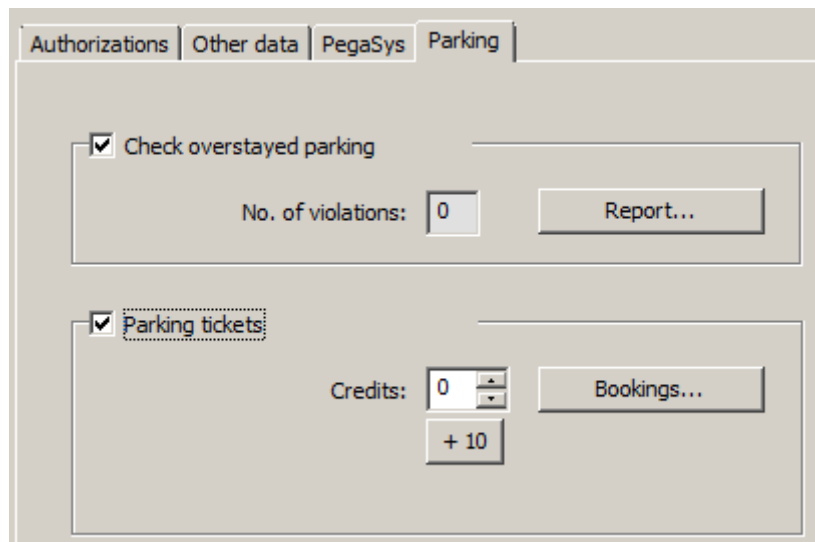
This feature enables the operator to do the following:

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

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

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

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



Detection and handling of overstayed parking

The system records the entry and exit times of each vehicle, as long as the complete system is online. If the LAC is offline it will allow or deny entry depending on its stored data.

- If the driver is exempt from checks on overstayed parking, the MAC allows the exit through the barrier in any case.
- If the driver is not exempt the exit time is compared with the last-recorded entry time of the vehicle.
 - If the complete stay is less than the maximum allowed, the exit will be allowed.
 - If not, the barrier will remain closed and the driver will need to contact the parking lot supervisor to open the barrier manually.

Statistics about overstayed parking

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

27.2 Parking tickets

This feature enables the customer to issue multi-park tickets for a defined number of single parking procedures (configurable).

The authorized user gets a parking ticket that allows him to enter one of the assigned car parks.

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

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

When entering the car park, a time interval will be defined in which the ticket owner is allowed to enter and leave the car park at will. This interval has the same length as the maximum parking period (default: 24 hrs).

Owning a parking ticket means to have permission to use any of the permitted parking zones for one day (24 hrs). Within this period of time it is also possible to change the parking zone or the car park

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

Administration of ticket credits

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

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

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



Notice!

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

Assignment of Multi-Park Tickets

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

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

Access Engine



Division: Common

< Main menu

- Authorizations
- Access profiles
- Areas
- Reset areas unknown
- Random screening
- PegaSys Configuration
- Person Types**
- Calendar
- Key cabinet

Predefined employee IDs:

Employee ID	Show as	Apply	Profile name	Profi...	PegaSys validity period
Employee		<input checked="" type="checkbox"/>		<input type="checkbox"/>	Locking system settings
Foreign Employee		<input checked="" type="checkbox"/>		<input type="checkbox"/>	Locking system settings
Visitor		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Locking system settings
Guard		<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	Locking system settings

User defined employee IDs:

Employee ID	Show as	Profile name	Profi...	Park...	PegaSys validity period
Employee	Employee		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Locking system settings

Delete based on: Employee Add

BoschRdr Common changed 10/21/2014 08:34:13 AM 10/21/2014 08:36:10 AM BIS

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

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

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

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

In this directory you have two choices:

- Edit **EmailText1.txt** to create a message text that the ticket account has been increased:

```

1 Dear %1 %2 %3,
2
3 you have got parking tickets for %4 days.
4
5 This email has been automatically generated.
6 Please do not reply to this email address.
7
8
9

```

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

Name	Änderungsdatum	Typ	Größe
AEOPLastMessage.csv	1/17/2015 11:34 AM	CSV-Datei	1 KB
CatDef.tbl	7/28/2014 4:54 PM	TBL-Datei	3 KB
DbGroups.cfg	8/1/2014 2:24 PM	CFG-Datei	10 KB
EmailTextD.txt	8/6/2014 9:50 AM	Textdokument	1 KB
EmailTextI.txt	8/6/2014 9:50 AM	Textdokument	1 KB
GroupDef.tbl			
installation.xml			
IPCWeb.WGen			
IPCWeb.WSDL			
IPCWeb.wsml			
IPCWebClient.wsml			
MsgDef.tbl			
PrcTable.tbl			
PrcTraceTable.tbl			
TxtDef_DE.tbl			
TxtDef_EN.tbl			
WebSrvQuery.xml			

```

Datei Bearbeiten Format Ansicht ?
Dear %1 %2 %3,
you have got only %4 parking tickets left.
This email has been automatically generated.
Please do not reply to this email address.

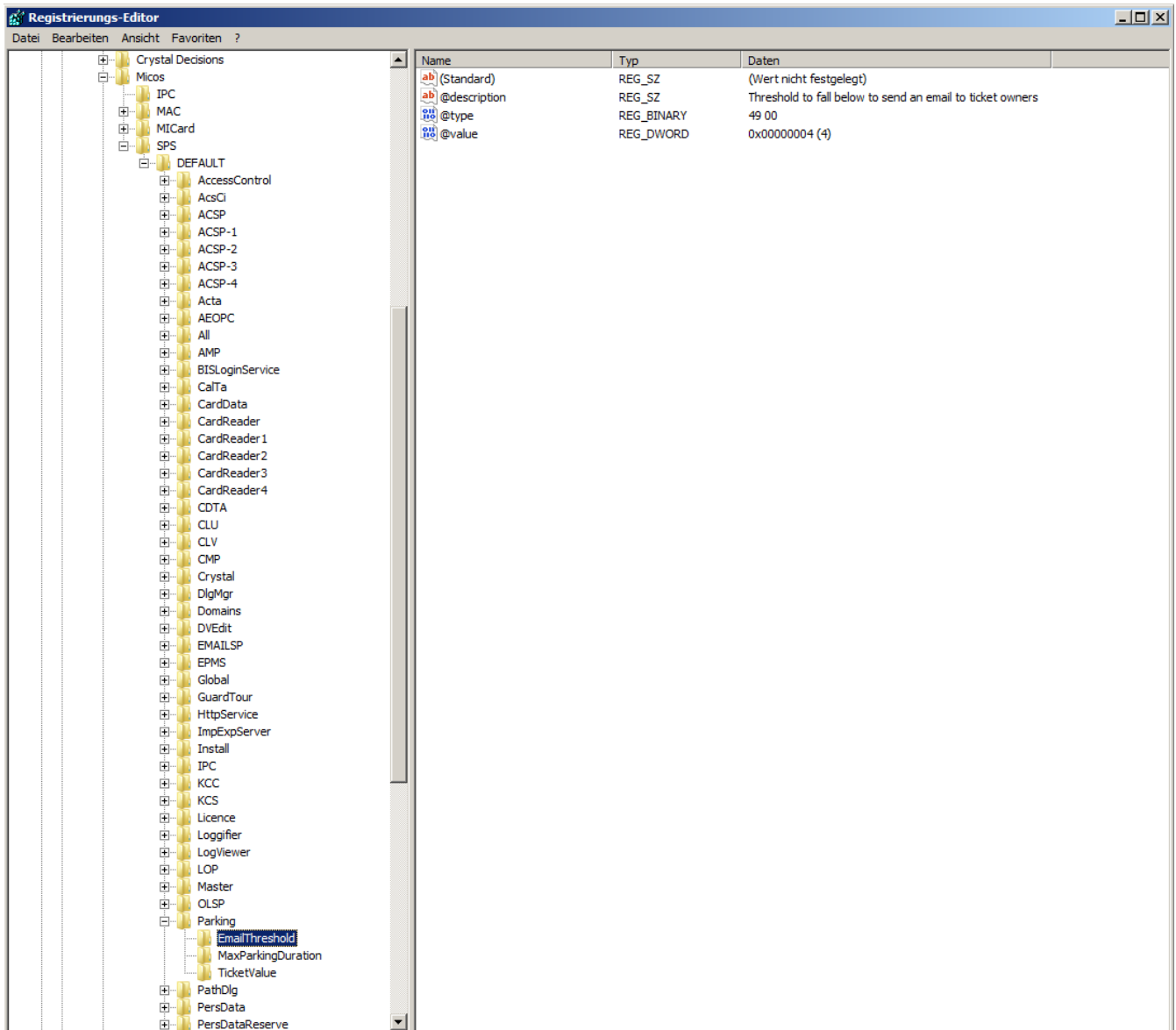
```



Notice!

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

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



The example shows the default setting of 4.

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

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

SMTP Settings

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

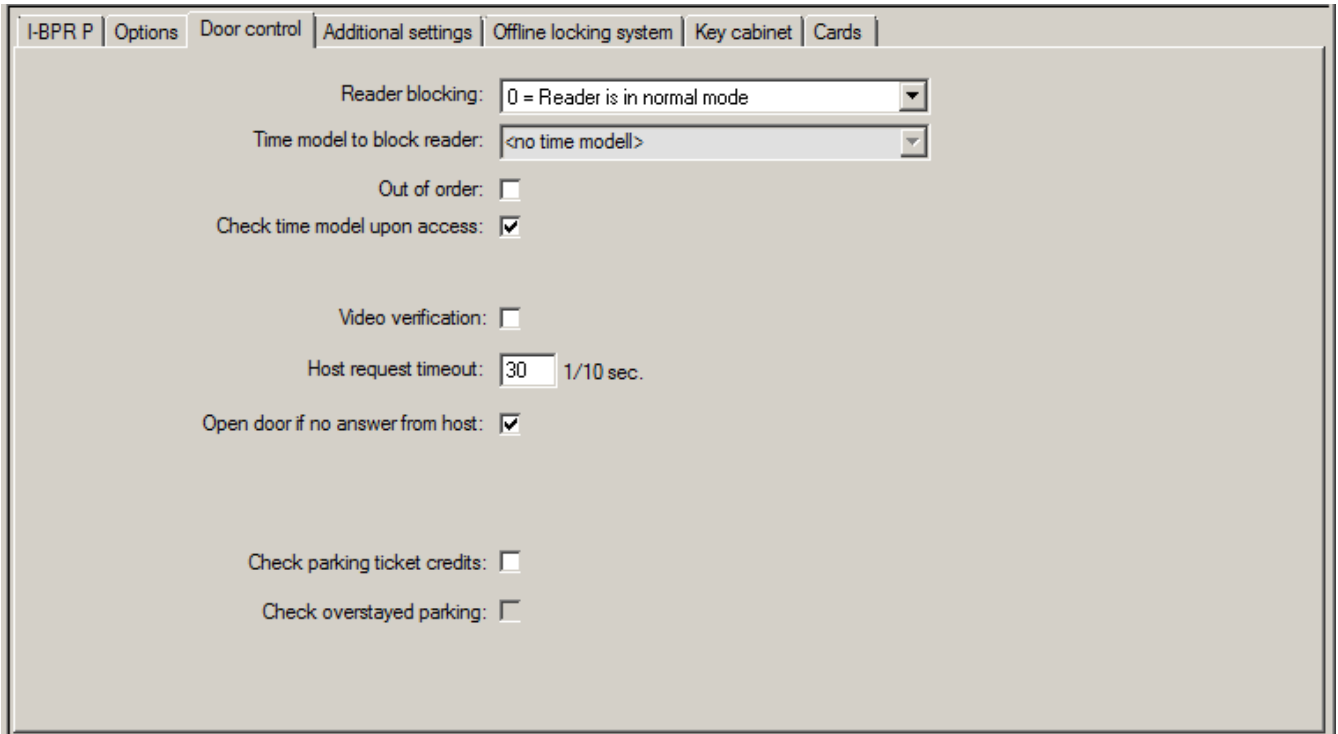
Settings Editor

Item Ansicht Favoriten ?

Name	Typ	Daten
(Standard)	REG_SZ	(Wert nicht festgelegt)
@description	REG_SZ	SMTP Sender Beschreibung
@type	REG_BINARY	53 00
@value	REG_SZ	SMTP Sender Name

Credits updated on access

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



- To configure the ticket check, activate the check box **Check parking ticket credits**.
 - **To check for overstayed parking activate the check box Check overstayed parking.**
- Prior to admitting the access to a car park the system checks if there is still a minimum of one parking procedure left on the ticket.
- If this is the case, the access will be permitted and the assets on the ticket reduced by one, unless it is a park zone change within the allowed period of time (24 hrs).
 - If this is not the case, the access will be denied.

Email notice if fallen below minimum assets

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

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

Ticket credits

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

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

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

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



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

27.3 Export of parking-lot utilization figures

This feature enables the operator to evaluate the utilization of parking lots statistically. The access control system exports parking lot utilization figures to a CSV file at predefined by the operator.

The Export into the CSV file contains data about the utilization of all car parks by the various classed of card owners - i.e. personnel classes. The values are taken in periodical, settable intervals with a length of max 15 minutes.

The data for any point in time are:

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



Notice!

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

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

27.4 Export Mobile Validity check

This feature enables the operator to check the parking authorizations of vehicles on the parking lot.

A CSV file is generated in regular intervals which contains all ticket owners together with additional information about the car park zones. .

For configuration select the system parameter editor under **Default\XPX\Task0001...** and switch on the export path, file name, and export explicitly (or off respectively).

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

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

27.5 Authorizations for several park zones

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

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



Notice!

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

A person who has several authorizations can access both, if handicapped or not. The AMC tries to book in the person in according to the configured sequential order of parking zones. In case one zone is full, the search for the next authorized and free zone will proceed. Counter calculation in MAC and AMC:

1) One AMC controls all entrances and exits of a car park:

=> The AMC counts on its own and can be corrected by the MAC when going online.

2) Entrances and exits of one car park are divided up onto different AMCs:

=> The MAC counts for the AMC in case of online operation. When operating offline, the AMCs permit the access (if configured accordingly) but don't count.

If several AMCs control one car park, activate the checkbox **No LAC accounting**.in the AMC configuration

27.6 Parking lot report

Parking lot list		Date 08.11.2013 , 14:51:23	
		Page 1	
Parking area	Zone	Vehicle count	State
Main Park		51	
	Zone A	30	full
	Zone B	9	--
	Zone C	12	--
Building A		39	
	Zone A	30	full
	Zone B	9	--
Building B		39	
	Zone A	30	full
	Zone B	9	--

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

Parking Place	Zone	# Cars	max. # Cars
Zones			
Parkplatz 1	Zone A	1	2
	Zone B	1	1
	Zone C	0	1
	Zone D	0	1
Zones			
Parkplatz 2	Zone X	0	1
	Zone Y	0	1
	Zone Z	0	1

- next refresh in 6 seconds -

Language: EN

27.7 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.

Division: Common

« Main menu

- Authorizations
- Access profiles
- Areas**
- Reset areas unknown
- Random screening

Access control area

Area name: P01

Description:

max. number of cars: 18

Number of subareas: 3

Refresh number

Synchronize counter

Parking time check

Parking areas

Subarea	Description	Max	Actual	Info
Parking_01		18		
Parking_02		6		
Parking_03		8		

Notes:

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

Refer to

- *Configuring areas for vehicles, page 25*

28 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.

28.1 Defining guard tours

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

No.	Description of reader	Time on the way	Total time	Max. delay	Startzeit +/-
1	BPR HI-1: BPR HI	00:00:00	00:00:00	00:00:00	3 min
2	BPR HI-2: BPR HI	00:10:00	00:10:00	00:02:00	
3	BPR HI-1: BPR HI	00:10:00	00:20:00	00:05:00	

- 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.

28.2 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.

28.3 Tour monitoring (formerly path control)

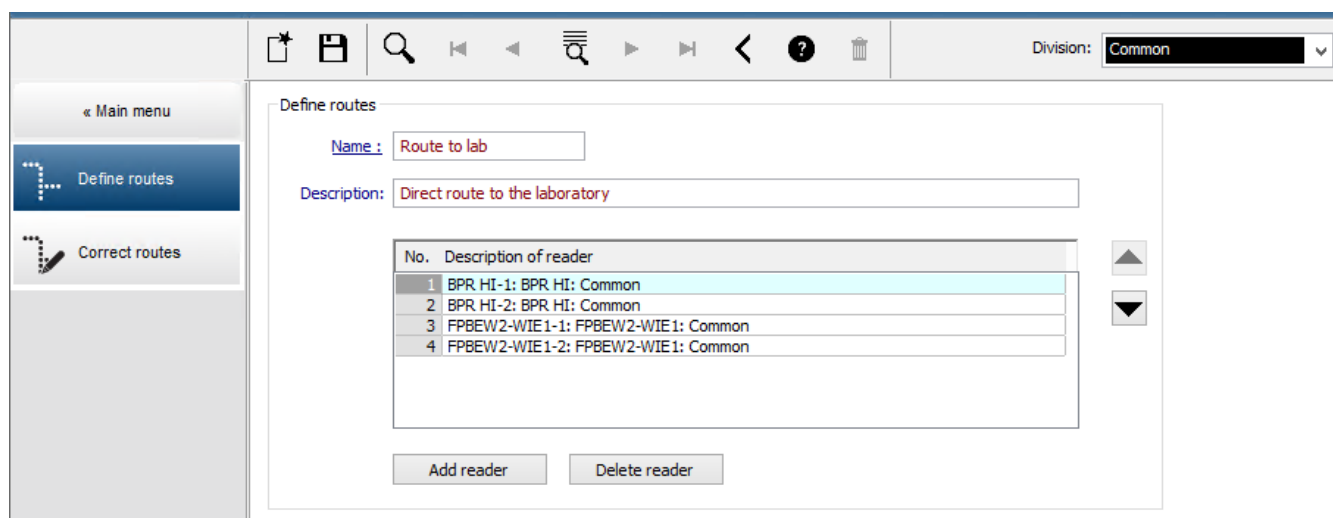
Introduction

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.



Define routes

Name :

Description:

No.	Description of reader
1	BPR HI-1: BPR HI: Common
2	BPR HI-2: BPR HI: Common
3	FPBEW2-WIE1-1: FPBEW2-WIE1: Common
4	FPBEW2-WIE1-2: FPBEW2-WIE1: Common

Add reader Delete reader

Division: Common

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.

29 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 displays the "LEDs" Blocked (red) and with it Random screening (flashing violet).



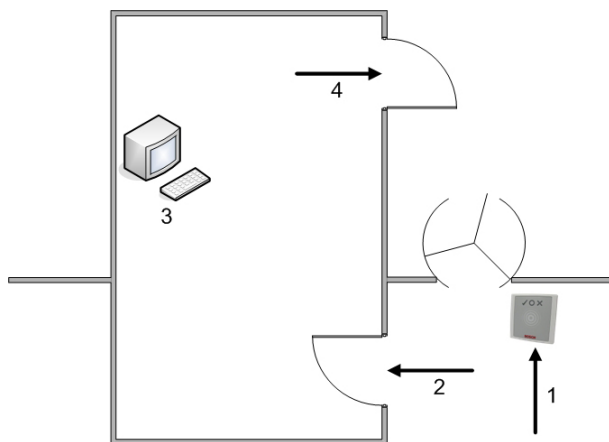
Notice!

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.

30 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: on-screen, printed or as .CSV files. To retrieve and display the desired records from the Event Log database, set filter criteria

and click **Refresh** . This process can take some minutes, depending on the amount of data requested.

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**

30.1 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)
 - 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.

30.2 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)
 - 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.

30.3 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)
 - 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.


31 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:



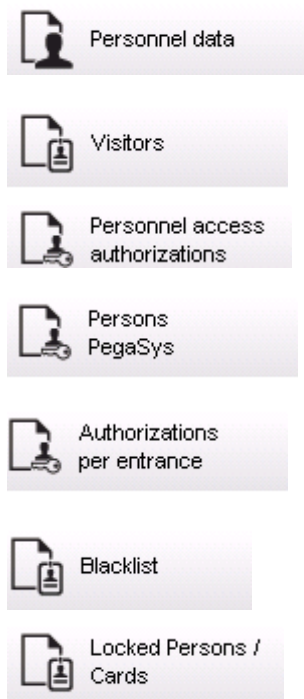
- Click  to exit the preview without printing.
- Use the arrow keys   in the preview toolbar to browse back and forth, or to select individual pages by page number.

- 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.

31.1 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.

31.1.1 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

Datum 02.07.2014 , 14:28:14
Seite 1





Lastname	Firstname	Arrival	Vehicle	Person
	Status	Departure	Last area	Last area
		Duration		
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'		

31.2

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.

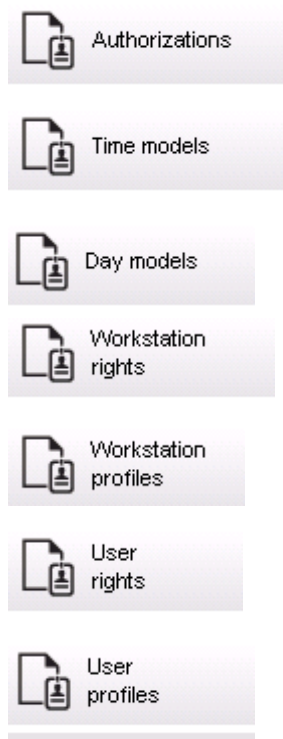
Report: Muster List Total

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.

31.3 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.

32 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 135*

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 135*

32.1 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.

32.2 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 139*

32.3 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 205*

33 Operating Swipe ticker

Introduction

Swipe ticker is a tool that helps Map view operators to monitor, in real time, who is entering or leaving the premises.

Overview

Swipe ticker is an application, within AMS Map view, that displays the last 10 minutes of access events in a dynamic scrolling list. Up to 50 access events are displayed, and events older than 10 minutes are automatically dropped from the list. The operator can monitor all readers in the system, or select a subset.

Each record in the list contains details of the event and the credential used, for example:

- The name of the cardholder and their stored photo, for visual confirmation of identity.
- A time stamp.
- Company and/or department name, if stored.
- The entrance and the reader at which the credential was used
- An event category with a colored label:
 - Green: A completed access with a valid credential
 - Yellow: An incomplete access with a valid credential, for example, the cardholder cycled the lock but did not open the door
 - Red: A failed attempt to access with an invalid credential. The type of invalidity is shown, for example, the credential is blacklisted, unknown or expired

Swipe ticker does not keep its own archives; it extracts and displays access events from the system database. The dynamic scrolling can be paused for closer study, or opened in a separate window for parallel use with other Map view applications.

Notice!

Latency after edits

Changes to ID photos and other cardholder data in AMS typically need a few minutes to propagate to the Swipe ticker. Until synchronization takes place, the Swipe ticker continues to react in real time with the older data.




Prerequisites

The User profile of the operator requires a special authorization to run Swipe ticker.

1. In the main AMS application, navigate to the menu: **Configuration > User profiles**
2. Load the profile name of the desired operator
3. In the table, select **Access Manager Maps > Special functions > Swipe ticker**

Starting Swipe ticker



- ▶ In Map view, click  to start the tool.

Selecting readers to monitor

If readers have not already been selected, or if you wish to change the selection, proceed as follows:




1. In the Swipe ticker window, click  (settings).

- The **Filter devices** window opens.
2. From the tree of devices, select the check boxes of the entrances or readers that you wish to monitor. The check boxes behave as follows:
 - If you select an entrance, then all its subordinate devices will be selected by default. The check boxes of individual subordinate devices can then be cleared if not required.
 - If **all** children of a parent device are selected, then the parent's check box is white. If only **some** are selected, then the parent's check box is gray.
 3. Click **OK** to finish selecting readers and close the **Filter devices** window.


Displaying selected readers on the map

- ▶ Double-click a record in the Swipe ticker.
- ⇒ The swipe ticker is automatically paused.
- ⇒ Map view displays, in the main window, the first relevant map scene in its map hierarchy, and highlights the reader that you double-clicked.

Pausing the Swipe ticker


- ▶ In the Swipe ticker window, click  , or double-click a record in the list, to pause the dynamic display
- ⇒ The dynamic display freezes. Incoming event records are buffered but not displayed.
- ⇒ A notice is placed at the top of the list, that the event stream has been paused.

Resuming a paused Swipe ticker

- ▶ In the Swipe ticker window, click  to resume the dynamic display
- ⇒ The dynamic list displays in chronological order (newest first) all access events that have occurred at the selected readers in the last 10 minutes, up to a maximum of 50.
- ⇒ Access events that are older than the 50 newest, or older than 10 minutes, are removed from the list.
- ⇒ New access events are again displayed in real time as they occur.

Duplicating Swipe ticker in a separate window

Note that only one duplicate ticker window can be opened at a time.

1. In the Swipe ticker window, click  (additional window).
The separate window is a duplicate and **not** independent of the ticker in the main window. It obeys the same settings.
Other Map view applications, such as the alarm list, can now be operated in parallel in the main window.
2. When you are finished with the separate window use the title bar to close it.

33.1

Special cases

Map View Swipe ticker and B901 doors

In order to provide correct information to the **Swipe ticker** app in AMS Map View, the IDs of B901 doors must match the IDs of their door points. That is, Door 1 must be assigned to Door Point 1, Door 2 to Door Point 2 etc.

Doors 1 - 4	Door 1	Door 2	Door 3	Door 4
Door Name Text	Door 1	Door 2	Door 3	Door 4
Door Name Text (Second Language)				
Door Source	SD12 (B901)	SD12 (B901)	SD12 (B901)	SD12 (B901)
Entry Area	1	1	1	1
Associated Keypad #	Keypad 1	Keypad 1	Keypad 1	Keypad 1
Custom Function	Disabled	Disabled	Disabled	Disabled
Door Point	1	2	3	4
Door Point Debounce	600ms	600ms	600ms	600ms

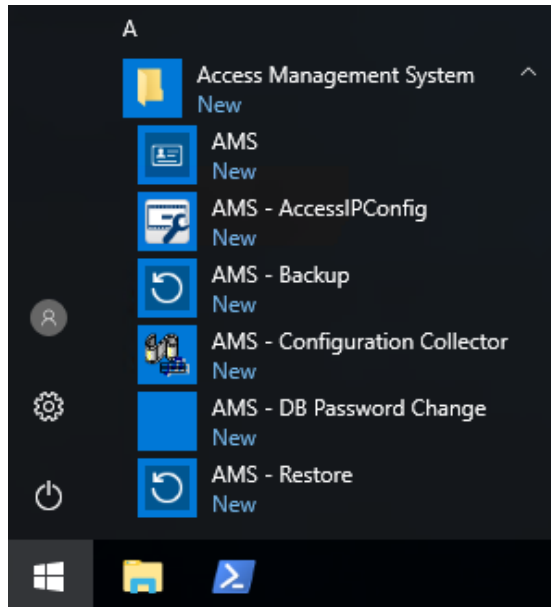
Make these assignments to the B901 door controller in the RPS tool that configures intrusion panels and controllers.

34 Backup and Restore

The **Backup & Restore** function enables you to move your system with its data to a new version of AMS, or to a new computer.

Backup and Restore can only be run on the machine where the AMS server is installed. Two shortcuts are available in the Windows Start menu:

- **AMS - Backup** for creating a backup
- **AMS - Restore** for restoring a backup:

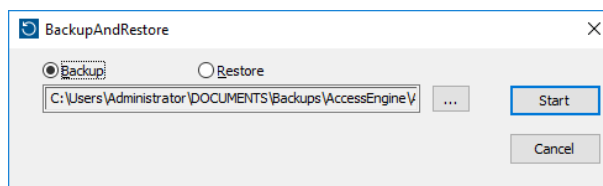


34.1 Backing up the system

This section describes how to create a backup for the AMS application and locate the SQL Server backup files.

Create a backup of the AMS application

1. In the Windows Start menu, right-click **AMS - Backup** and select **Run as administrator**.
 - The **Backup and Restore** tool starts with the **Backup** option pre-selected.



2. Enter a path where the .GZ file is to be saved.
3. Click **Start** to start the backup.
 - The **Backup and Restore** tool creates a single .GZ file, and displays its progress in a popup window.
4. Copy this file to safe storage on another computer. For data security, do **not** leave the only copy on the DMS server.

Locate and copy the SQL Server backup files.

1. Using a file explorer on the AMS server computer, navigate to the location where SQL Server keeps its .BAK files.

- The file path is as follows, whereby <version> and <instance name> are variables that depend on your system:
C:

```
\Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\
```
 - The file names are in the form:

```
acedb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.AlarmDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.EventDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.MapDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.MapViewDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
Bosch.StatesDb.80fZe4b0-eb71-43ab-b2b6-db2517d4d6c7.bak
```
2. Copy **all** the .BAK files to safe storage on another computer. For data security, do **not** leave the only copies on the DMS server.

**Notice!**

The default path to the AMS Event log is:

```
C:\Program Files (x86)\Access Management System\Access Engine\AC\LgfLog\
```

34.2

Restoring a backup

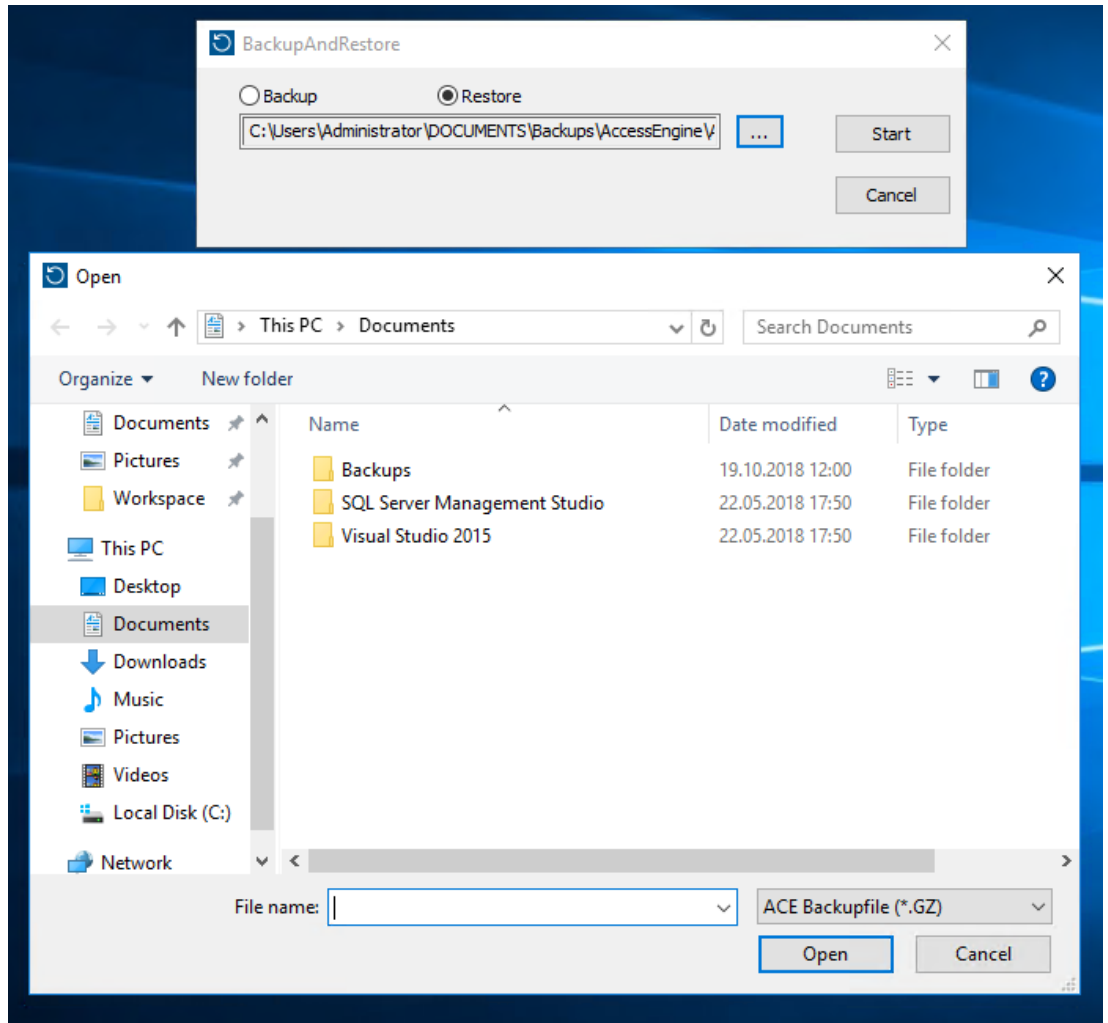
Prerequisites

- The GZ file that was created by the **Backup and Restore** tool
- The .BAK files created by SQL Server that you saved during the backup procedure.
- An SQL account with **sysadmin** rights, such as *sa*.
- A suitably prepared target computer with respect to **licenses** and **certificates**:
 - **Licenses:** The target computer (where you restore the backup) requires at least equivalent licenses to those on the computer where you made the backup.
 - **Certificates:** Any clients of the target computer will require the new certificates generated by the installation on the target computer, not those generated by the installation on the original computer.
Consult the **AMS Installation Guide** for generation and installation of client certificates.

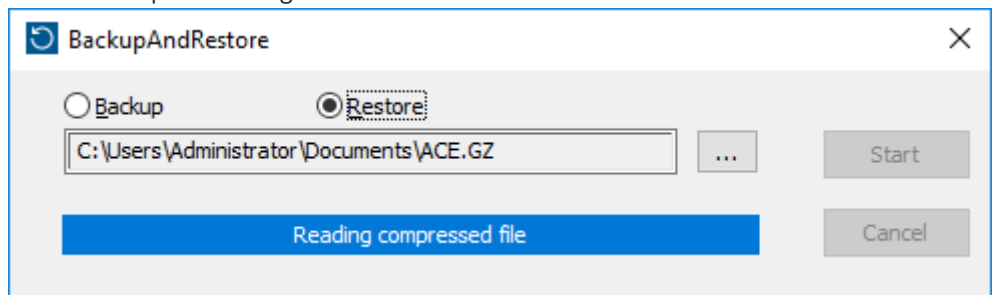
Procedure

1. In the AMS program click **File > Exit** to stop the AMS application.
2. When the program has terminated, run the Windows **Services** application and make sure that all *Access Engine* and *Access Management System* services have stopped. Otherwise stop them here.
3. **If and only if** you are running an RMAC (redundant failover MAC) with your main or 1. MAC, jump to the next subchapter and do the procedure described there, before returning to this step.
4. Copy the MSSQL .BAK files that you saved from the original computer to exactly the same path on the new computer.

- The file path is as follows, whereby <version> and <instance name> are variables that depend on your system:
C:
 \Program files\Microsoft SQL Server\MSSQL<version>.<instance name>\MSSQL\Backup\
5. In the Windows Start menu, right-click **AMS - Restore** and select **Run as administrator**
 - The **Backup and Restore** tool starts with the **Restore** option pre-selected.
- 6. Click the **[...]** button to locate the GZ backup file in the files system, and click **Open** to select it.



- 7. Click **Start** to start the restore process.
- 8. When prompted for server credentials, enter the credentials for an MSSQL sysadmin user such as sa, not the login credentials of the server computer.
 - The restore process begins



9. When the restore process is completed, run the Windows **Services** application and restart all `Access Engine` and `Access Management System` services manually.
10. Execute the server setup program `AMS Server Setup.exe` as Administrator in order to resynchronize the backed up data with the current system data.

Refer to

- *Backing up the system, page 253*

34.2.1**Restoring RMACs into a new installation**

Note: this procedure is only relevant to the case where you are restoring to different hardware the backup of a system with MACs and RMACs.

Introduction

If you restore a backup to new computers, then you must reconfigure the IP addresses of the MAC and RMAC that were stored in the backup file to the IP addresses of the new hardware. Do this configuration by running the `MACInstaller` tool on the new hardware. The `MACInstaller` tool is found on the installation medium at

`\AddOns\MultiMAC\MACInstaller.exe`

Use of the `MACInstaller` tool is described in detail in the chapter *Using the MAC installer tool, page 52*

Procedure

1. Run the `MACInstaller` tool on the computer where 1.MAC is running. This computer may be the DMS server or a dedicated server for 1.MAC.
 - In the tool, set the new IP addresses of the primary MAC (this computer) and the RMAC.
2. Run the `MACInstaller` tool on the computer where the RMAC is running.
 - In the tool, set the new IP addresses of the primary MAC and the RMAC (this computer).
3. Return to the step where you left the procedure **Restore procedure**.

Refer to

- *Using the MAC installer tool, page 52*

35

Configuration and usage of CEPAS cards

The CEPAS card type is used in Singapore. The card numbers are bigger than usual; therefore, a special CEPAS card type is introduced in the access software.

The following description shows how the CEPAS card type must be configured, including the enrolment of this card type in a manual dialog and/or by special USB reader hardware. To configure CEPAS card in your access control system (AMS):

Dialog path



- In the **Configuration** main menu, click **Card definition**.

To activate the CEPAS card, move **CEPAS 64 Bit** from **Available cards types** list in the right-hand side to the left-hand list **Active Card Types** by clicking on the left arrow button [**<**].

Note: If any other card data type is activated, the CEPAS 64 Bit card type cannot additionally be activated. The same if the CEPAS 64 Bit card type is activated, a different card data type can no longer be activated.



After configuration and enrolment, the bigger card number appears complete in the access dialogs and in reports of the dialog manager application.


The following description shows the most important changes in the dialogs if CEPAS is configured:

- Go to the AMS main menu > **Personnel data** > **Persons**
 1. Create a person or Edit an existing one. For more information, read *Creating and managing personnel data*.
- 2. Save 
 - In the menu, click on **Cards**
- 3. Click in the space **Card no.**
- 4. Select dialog reader for recording the card
- 5. Click **Record card**
 - A *Recording badge ID* dialog will open. It is strongly recommended to use the USB reader to insert the card number. Otherwise, the 16 digits of the CEPAS card can be entered manually.
- 6. Click on **Card no**
- 7. Present the CEPAS card on the NFC USB reader that will read the card number
 - The card number shall be the same as the number seen on the person's card.
- 8. Click on  to search for card
- 9. Select the reader
- 10. While clicking on **Reader..** present the card on the NFC USB reader
 - The card of activated shall be found and correctly displayed.

To have access granted with the activated card, consider the following:

Dialog path

- AMS main menu > **Configuration** > **Device data**
 1. Define an AMC-4W. For more information, refer to *Using the Device Editor*.
 2. Define a door model. For more information, refer to *Configuring Entrances*.
- 3. Save 
 - AMS main menu > **System data** > **Authorizations**
- 4. Create a new authorization and assign to it the entrance previously created.
- 5. Save 

- AMS main menu > **Personnel data** > **Cards**
- 6. Select the person and assign to this person the authorization previously created.
- 7. Save 

Limitations of CEPAS cards in AMS:

- If CEPAS cards are activated in card definition dialog, no other card types can be used in addition.
- External systems like IDEMIA, Suprema, Intrusion boards, SimonsVoss, KONE elevators, Deister cabinets, PegaSys, OSS-SO do not support the CEPAS card type and cannot be combined in one AMS system.

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.

ACS

generic term for a Bosch Access Control System, for example, AMS (Access Management System) or ACE (BIS Access Engine).

AMC hardware key

An internal authentication code that the AMC generates from certain hardware parameters. It is not visible to the user.

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.

Area (Arming)

A grouping of entrances of entrance model 14 in an access control system. The arming or disarming of the intrusion system at one of these entrances simultaneously has the same effect at all entrances where the parameter Arming area has the same one-letter designation.

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.

CSN

Card Select Number.

Data Management System (DMS)

A top-level process for managing access control data in the system. The DMS supplies data to main access controllers (MAC), which in turn supply data to local access controllers (usually AMC).

DCP

a password from which the access control system generates a master key that is used to encrypt network communication to all subordinate local access controllers, typically AMC devices.

Destination Dispatching System (DDS)

also known as Destination Management System, but use only abbreviation DDS. Otis CompassPlus is a kind of DDS.

Destination Entry Redirector (DER)

A computer at the same level as a Destination Entry Server (DES) in an Otis CompassPlus system. It connects to all elevator groups and its job is to enhance the efficiency of the DES devices.

Destination Entry Server (DES)

A computer that governs an elevator bank to optimize travel times.

Destination Entry Terminal (DET)

A device where elevator passengers can enter destination requests for an elevator group.

Configuration mode

the default state of access control devices in the device editor. Changes take effect and propagate to subordinate devices immediately.

Operation mode

the state of an access control device in the device editor while it is responding to commands given outside the device editor. Configuration changes take effect only after operation mode ends and configuration mode is restored.

Door model

A stored software template of a particular type of entrance. Door models facilitate the definition of entrances in access control systems.

DSN

Data Source name. The name of a data source in Open Database Connectivity (ODBC).

DTLS

Datagram Transport Layer Security is a secure communications protocol that protects against eavesdropping and tampering.

elevator group

A group of elevators serving the same floors in concert. Each elevator group is governed by a Destination Entry Server (DES).

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.

IPConfig tool

A separate auxiliary program for configuring the network and network security settings of hardware devices within the access control 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 Controllers)

Master key

A code that the system generates from the DCP (Device Communication Password), and uses to protect the access control devices. The Master key is never made visible to any user.

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.

password entropy

a measurement of password strength calculated from factors such as its randomness, the number of symbols available, and the actual number of symbols used.

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.

Point

A sensor to detect intrusion into an intrusion-controlled area. In some contexts points may be called zones or sensors.

Random LCD key

A temporary alphanumeric code that the AMC generates afresh every time it boots. The key can be shown in the liquid crystal display (LCD) of the AMC and may be requested by software tools to authenticate network communication.

REX

"Request to Exit". A signal to request that door a door be unlocked from the inside to allow egress. The signal is typically triggered by a push button or bar on the inside of an entrance; sometimes by a motion detector.

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.

RPS

Remote Programming Software. A program that manages fire or intrusion control panels on a network.

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.

shunt

to suspend an alarm in specially defined circumstance.

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

© Bosch Security Systems B.V., 2024

Building solutions for a better life

202405241053