Access Engine (ACE)

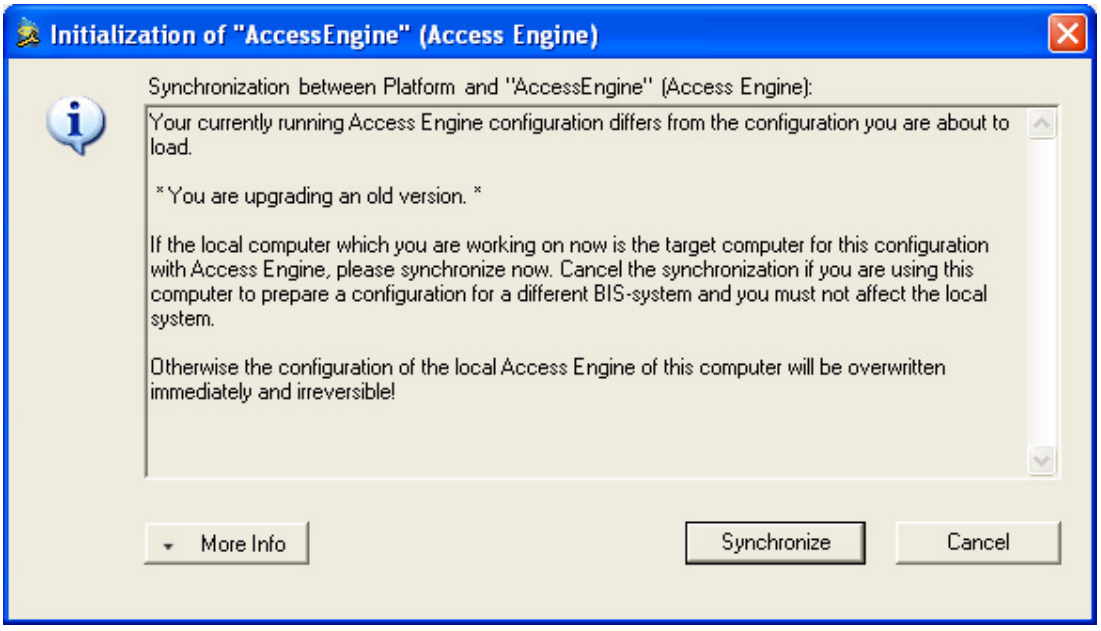
en Configuration Manual

Table of contents

1 Introduction

1.1 Synchronization

Upon first use, but also when restarting the Configuration Browser, a dialog box may appear inviting you to synchronize the BIS platform with Access Engine.

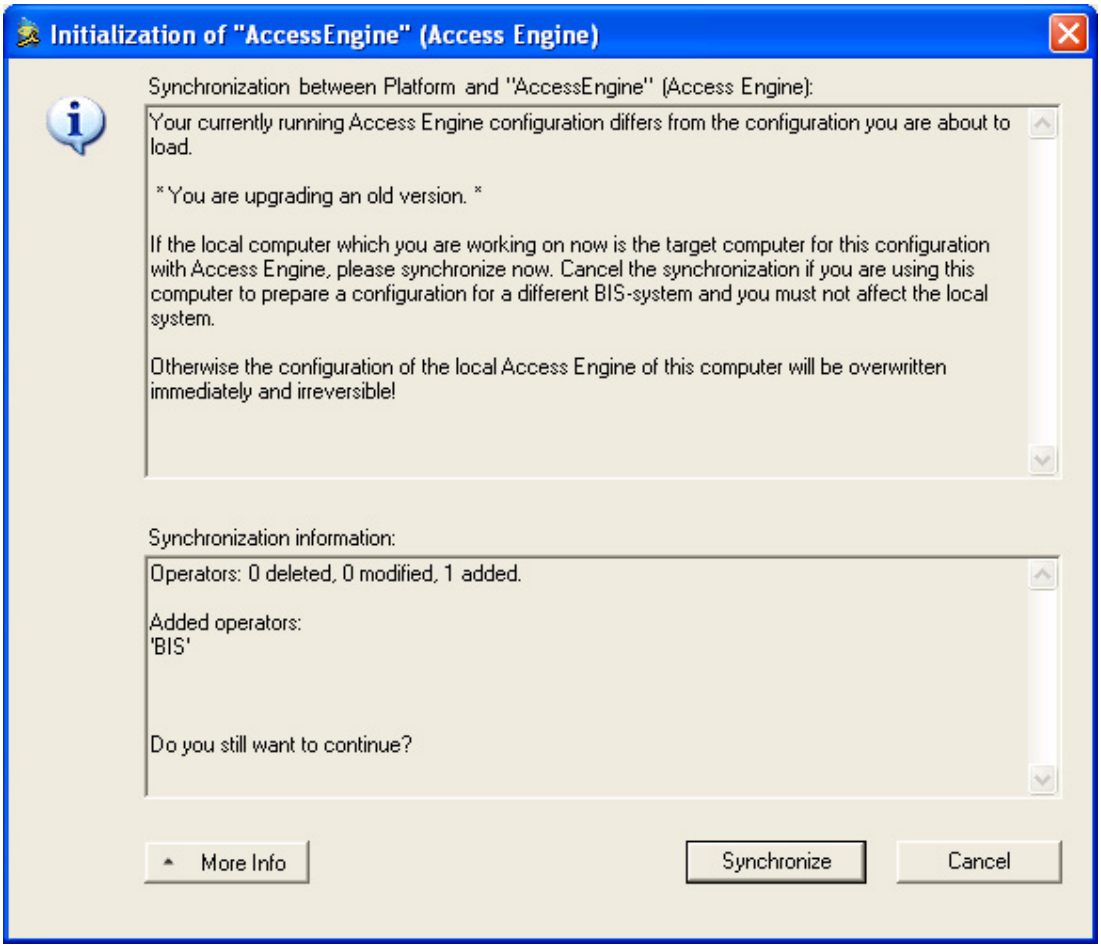


This dialog can contain various reasons for its being shown:

- You are trying to update a configuration
- You are trying to load a configuration from a different system

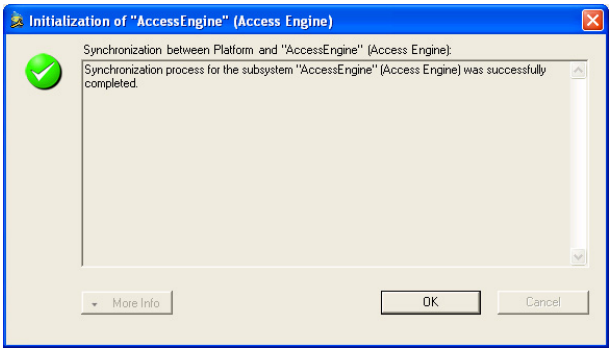
Notice!
If you have stored several configurations please check the settings on the BIS Manager tabs **System start / stop** and **Load/Save Configuration** before synchronizing, to make sure you are loading the correct configuration.

The button **More Info** will reveal an additional window giving more detailed information.



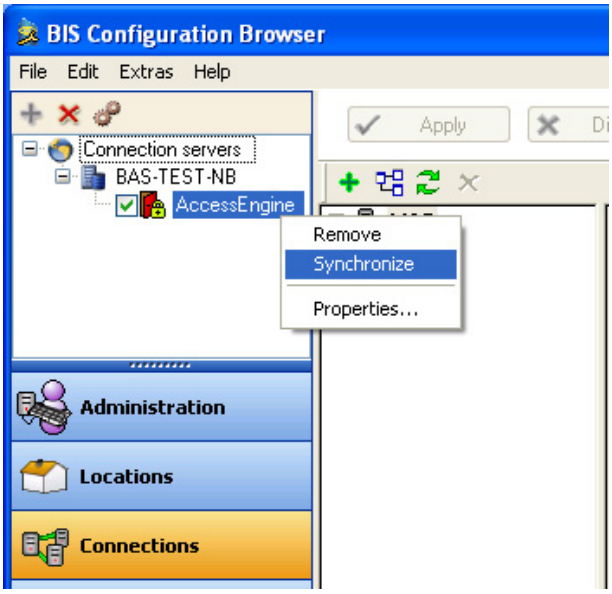
Click **Synchronize** to confirm that you wish to continue. A progress bar is shown briefly during the synchronization.

Click **OK** to confirm the successful completion of the synchronization process.



Manual Synchronization

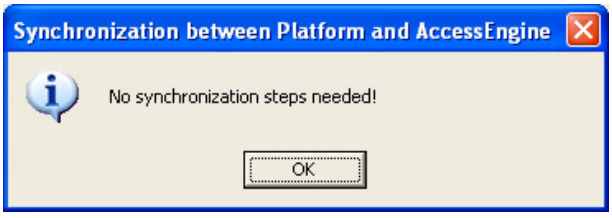
You can force a synchronization manually, e.g. if you find that certain devices are not being shown in the platform. Right click on the connection server **Access Engine** in the Configuration Browser and select **Synchronize** at any time to realign the data.



This mode of access also lists any discrepancies, so that the synchronization process can be cancelled if no significant changes are missing.

Thus unnecessary actions can be avoided. If the BIS platform and Access Engine both have the same data-status then no synchronization is necessary, and this will be reported by a pop-up window.

This feature can be used for troubleshooting. If problems occur in the display, accessibility or functionality of access-control installations, then the synchronization function can be invoked to check the data-status. If the pop-up window below appears, then a data-mismatch between platform and access engine can be ruled out as the cause.



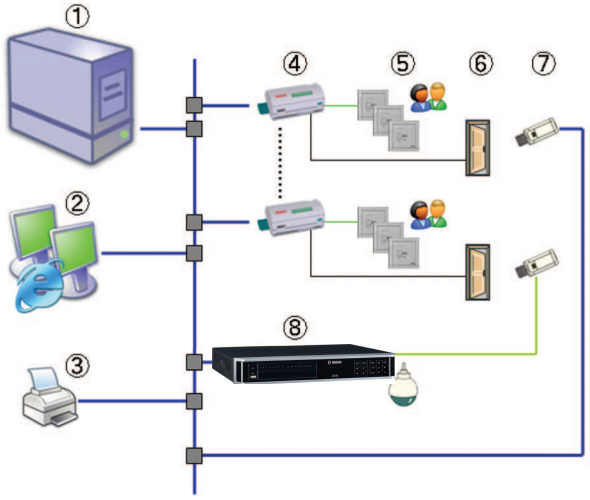
2 System overview

The Access Engine (ACE) software, in conjunction with Bosch access hardware, is a complete access control system within the Building Integration System (BIS). It encompasses all the essential features of any standalone access control system, plus a wide range of optional enhancements.

Like the other BIS engines, the ACE takes full advantage of all the extra BIS features, such as interactive location maps and action plans for powerful, fully integrated alarm management. Alarm messages and access control events can be displayed with graphical location information and workflow instructions.

ACE uses the standard BIS user interfaces and their flexibility of customization. Additionally ACE offers specific access configuration interfaces for cardholders, access hardware and access rules.

The main benefit of the Building Integration System family is the integration of a wide variety of security and safety systems on the same premises. By combining ACE with other BIS engines (e.g. Automation and Video) you can design smart security solutions tailored exactly to the requirements of your tender.
The Access Engine runs on a single-workstation, in a client-server system, or within a distributed environment with a central server and local or regional servers.
In the distributed multi-server environment all devices, cardholders and authorizations can be managed from the top-level server.



Pos.	Description (single-server system)
1	Central BIS server with Access Engine and Video Engine SW
2	Multiple workstations for alarm management or enrollment
3	Enrollment devices such as card printer, signature scanner, enrollment reader, camera for ID photos
4	Access controllers
5	Access readers

6	Door strikes
7	IP camera
8	Digital Video Recorder e.g. DIVAR for alarm recording

3 Administration rights for operators and workstations

3.1 Introduction to authorizations and profiles

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
To configure the workstations and operators of an access control system the normal order of tasks is:

1. Create the workstations in the dialog:
   BIS Configuration browser **> Administration** > **ACE Workstations**
2. Create workstation profiles in the dialog:
   BIS Configuration browser **> Administration** > **ACE Workstation profiles**
3. Assign profiles to workstations in the dialog:
   BIS Configuration browser **> Administration** > **ACE Workstation rights**
4. Create operator profiles in the dialog:
   – BIS Configuration browser **> Administration** > **Authorizations**
   (for access-control functions of the BIS user interface)
   – BIS Configuration browser **> Administration** > **ACE User profiles**
   (for functions of the ACE user interface)
5. Assign profiles to operators in the dialog:
   BIS Configuration browser **> Administration** > **Operators**

3.2 Creating Workstations

Introduction
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.

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

Creating workstations
Dialog path
BIS configuration browser > **Administration** > **ACE Workstations**

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, page 19*
- **Automatic logout after:** The number of seconds after a logon via enrollment reader is automatically terminated. Leave at 0 for unlimited time.

See also

- *2-Factor Authentication, page 19*

3.3 Workstation Profiles

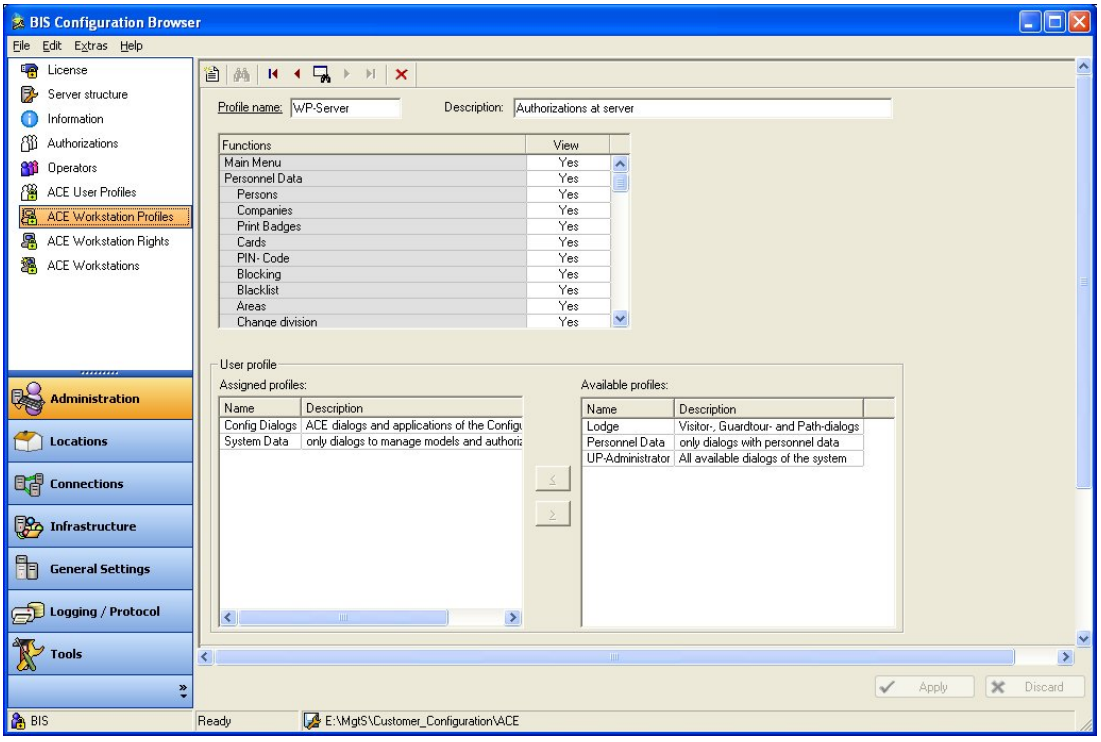
A workstation profile is a collection of rights that defines the following:

- 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 browser > **Administration** > **ACE Workstation Profiles**

Creating workstation profiles

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
5. Add functions and user profiles as described below.

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.

3.4 Workstation rights

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**
BIS configuration browser > **Administration** > **ACE Workstation rights**

Assigning Workstation profiles to workstations

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 **Assígned** 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.

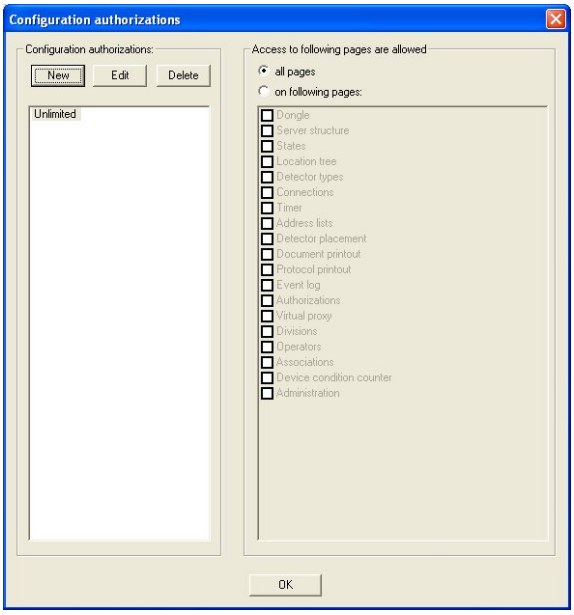
3.5 Authorizations

Introduction
Use the **Authorizations** dialog to create bundles of user rights for operators of the BIS system:
BIS Configuration browser **>** **Administration** > **Authorizations**
Access Engine operators have separate dialogs:
BIS Configuration browser **>** **Administration** > **ACE** `<dialog name>`

Procedure
1. To create a new authorization, click the button **New** in the **Authorizations** list field and overwrite the default name. To rename or delete authorizations from this list click **Rename** or **Delete**.
2. If the **Divisions** feature is licensed and in use, use the **Authorized for divisions** pane to restrict the authorizations to one or more of the divisions that you have previously defined.
3. Use the check boxes to add, modify and delete rights to access the various controls, address lists and state lists of the system.
4. Click **Apply** to save changes.

Configuration authorizations
1. To create named bundles of rights only for the dialogs of the configuration browser, click **Modify...** in the **Authorization for configuration** pane.
   The **Configuration authorizations** popup behaves like a miniature of the main **Authorizations** dialog.
2. Click **New** to create new configuration authorizations, and overwrite the default name.
3. Select the desired authorizations from the list, and click **OK** to save.

Click **Edit** or **Delete**. To edit or delete existing entries.
Rights can be assigned for all configuration browser dialogs, or for a subset.



3.6 User 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

BIS configuration browser > **Administration** > **ACE User profiles**

Creating a User 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

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

3.7 Operators

Use the Operators dialog to assign bundles of user rights, “authorizations”, to operators of the BIS and ACE systems.

Notice!
IMPORTANT: Change the default passwords for the system users **Administrator** and **BIS**, as soon as possible, because these users have unlimited authorizations.

3.7.1 General operator settings

For use of the General operator settings tab, see BIS configuration help.

3.7.2 ACE operator settings

Special authorizations govern the use of ACE dialogs and applications. These authorizations are defined in so-called ACE User Profiles and then assigned to individual users.
When a new user is created he automatically receives the default profile **UP-Administrator**, which gives unlimited edit and execute rights for Access Engine dialogs and applications.
Use this dialog to restrict the rights of an operator, as required.

Use the arrow buttons  and  to move profiles out of the **Assigned profiles** list box, and replace them with profiles from the **Available profiles** list box.

Check box: Global administrator
Certain data can be specially protected using the setting **Administered globally**, which appears next to the ID photo on the Persons dialog. Only operators that have the **Global administrator** right can edit these data. All other operators have read-only rights for these data.
Select the check box **Global administrator** to assign this special right to the operator.

3.7.3 ACE API Access rights

Use the tab **ACE API Access rights** to define the rights of an operator regarding the Access Engine Application Programming interface (API).
The choices are:
– No access (default)
– Read-only access
– Unlimited access

3.7.4 Additional check via external system

This feature provides an additional I/O check via an external system.
Examples of additional checks for a cardholder who has already authorized himself with valid credentials:
– Video verification is required that the credential is being presented by its true owner.
– Video verification of a cardholder’s vehicle registration.
– Video or weight verification to prevent tailgating .
– Checks for radio-active and other kinds of contamination.

AMC LEVEL:

Output Signals

No.	Name	Description
13	externalAcActivate	Activate external access control system

Input Signals

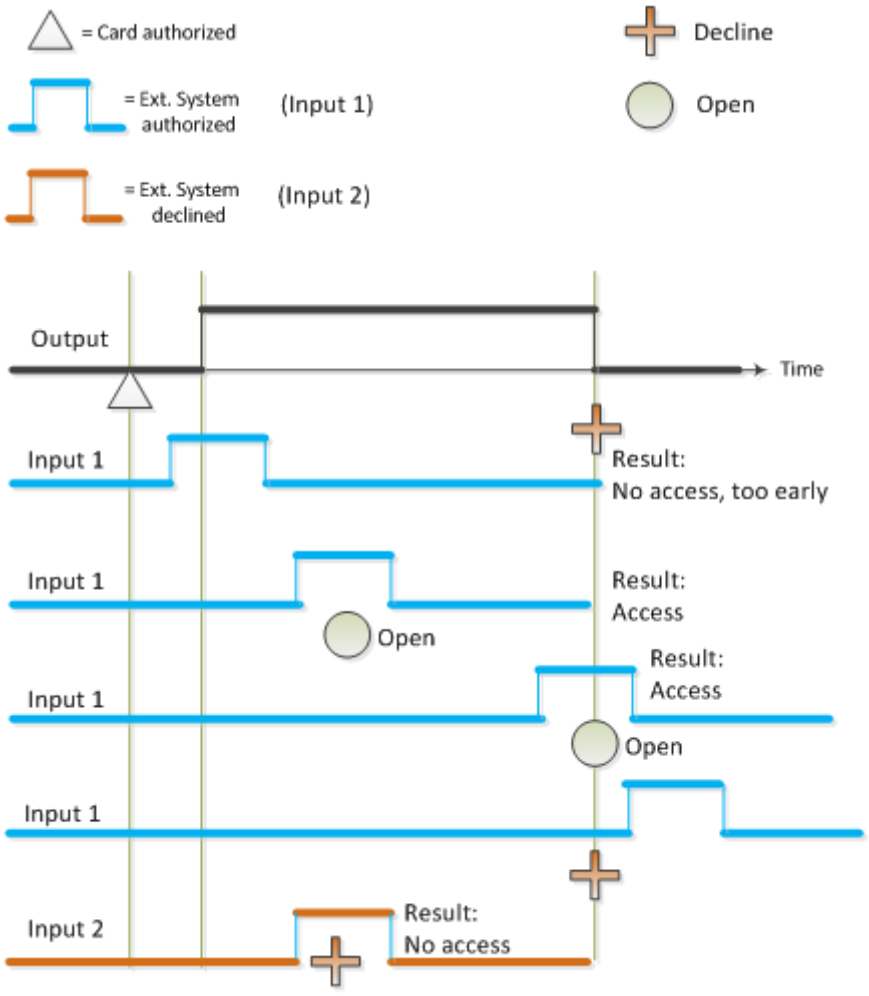
No.	Name	Description
3	externalAcAllow	Allows access if set to ‘1’ (mandatory).
4	externalAcDenial	Denies access if set to ‘1’ (optional)

Control logic steps

The following additional control logic steps are added:

- Set the <**activate external access control system**> output to signal the external system, so that a decision is expected.
- Await a number <*n*>ms. The value <*n*> is a configurable timeout (by 1/10 sec steps, minimum = 10/10 sec.). A value of 0 means: no external check.
- Evaluate the <**external access decision - accepted**> input or the <**external access decision - denied**> input while waiting.
- If one of these inputs is set, the access will be granted or declined, and no more waiting is necessary. Otherwise at the end of the waiting time the AMC will decline.
- In case of a denial an ‘**access denied by external system**’ event message is generated.
- Reset the <**activate external access control system**> output
  - after a signal (accept or deny) has detected.
  - if no signal (accept or deny) arrives, then at the end of the waiting time.

The procedure is according to the time chart below:



The input signal is required to rest the requested time of *m*=1 second (*m* is configurable in 1/10 sec steps, minimum = 10/10 sec.).

Event Messages

No.	Name	Description
1050	MLD_EXTERNAL_AC_DENY	Access denied by external system.
1051	MLD_EXTERNAL_AC_TIMEOUT	External system timeout.

Entrance Parameters (pE)

Name	Type	Description
EXTACDELAY	TIME_T / Decimal	The duration (in 100ms units) the access controller will wait after setting the externalAcActivate signal for the externalAcAllow signal.
EXTACPULS	TIME_T / Decimal	The duration (in 100ms units) the externalAcAllow signal has to be active. Default: 10/10 = 1000 ms (minimum = 500 ms). Ii is not necessary to edit this parameter in the Config.browser

MAC LEVEL:
On the MAC level the new parameters EXTACDELAY and EXTACPULS for the entrance are forwarded to the AMC.

DMS LEVEL:
On the DMS level the additional check is configured for door models in the configuration browser.
Two additional parameters for the door model are available:

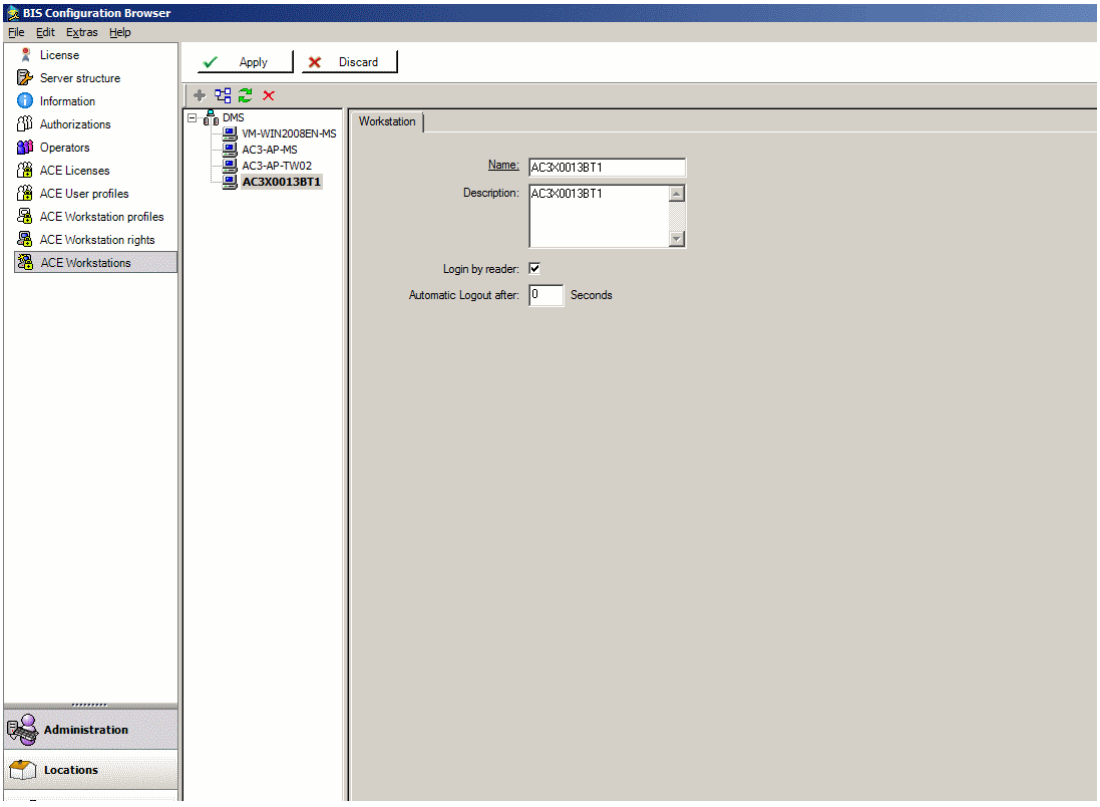
EXTACDELAY: External Access Delay
This is the time to wait for an answer of the external system in 100 ms units, (e.g. 30 means 3 seconds) Dialog text: '**Waiting time external access decision**' .The default value is 0, i.e. no additional external check.
If this parameter is set >0, check results are expected from the external system, otherwise no access will be granted. If this parameter is set >0, then it must not be less than 10/10 (1s)

EXTACPULS: Duration of external signals
The duration the external signals are active. Note: The parameter EXTACPULS is set to its default value. It is not available in the configuration browser.
If this additional check is configured and the card/tag is authorized, and an accepted signal from the external system is set, the AMC will open.
If a denial signal is set the AMC will send a message '**access denied by external system**' to the DMS.
If no signal is set the AMC will send a message '**external system timeout'** to the DMS.
The messages are sent to the corresponding reader device and are forwarded to the access control system. They can be used there to create alarm messages.
The additional check by I/O also works if DMS and the overall access control system are offline.
Access authorization check:

- AMC checks if the MAC is offline, and
  - permits the access if this complies with the rules, or,
  - if access is denied, the process is terminated and a message sent.
- AMC checks via I/O, if these are configured and not yet rejected
  - if access is denied, the process is terminated an a message sent.
- AMC requests the additional video check via MAC and DMS, if these requests are configured and not yet rejected
- If access is denied, the process is terminated and a message sent.

3.8 2-Factor Authentication

The **2-Factor Authentication** is a feature that enables a double identification of user. With this feature the user has to identify himself by entering an ID-number **and** presenting a card to a reader. Configuring the **2-Factor Authentication** means to configure a workstation with a dialog reader.
On the **BIS Server**, start the **BIS Configuration Browser** and click the tab **System Start/Stop** > **Start (Configuration Browser).**
Go to **Administration > ACE Workstation** and create a workstation if necessary and activate **Login by Reader**.

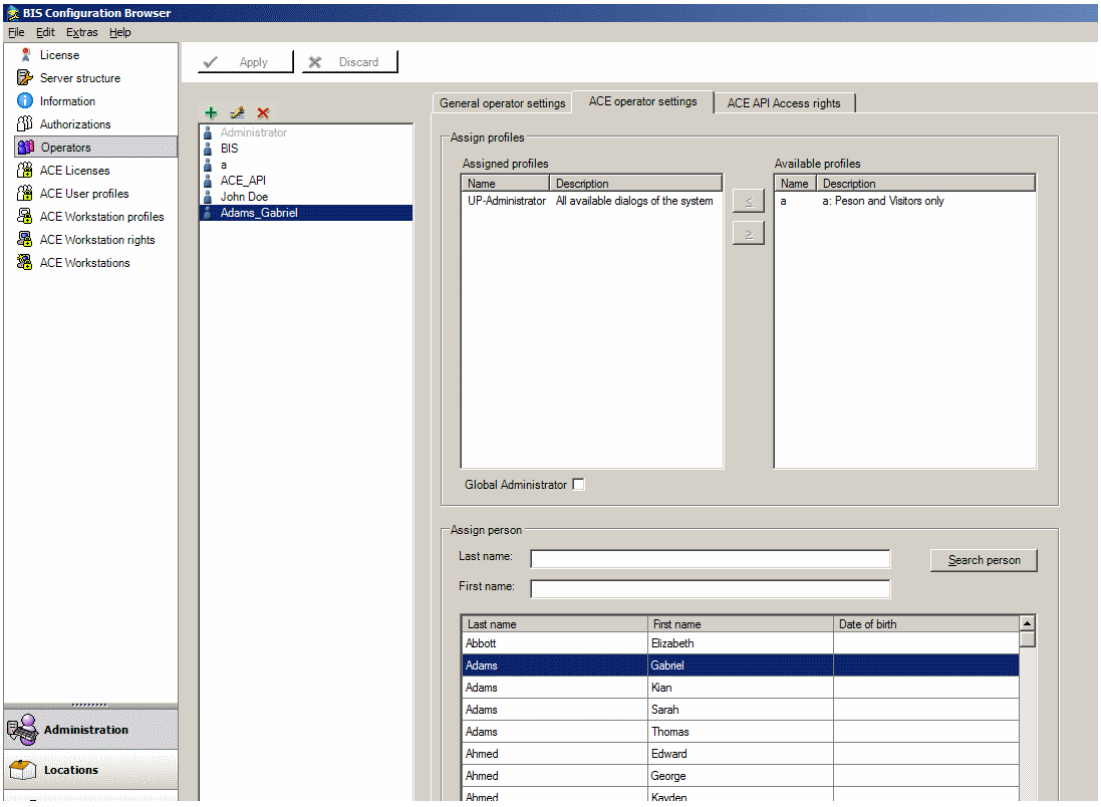


Check, if a dialog reader is configured for the required workstation: **BIS Configuration Browser > Infrastructure > ACE Card reader.**

For the feature to work, the operator must also be recorded as a cardholder in the access control system.

Select **BIS Configuration Browser -> Administrator -> Operators**, and select an operator.

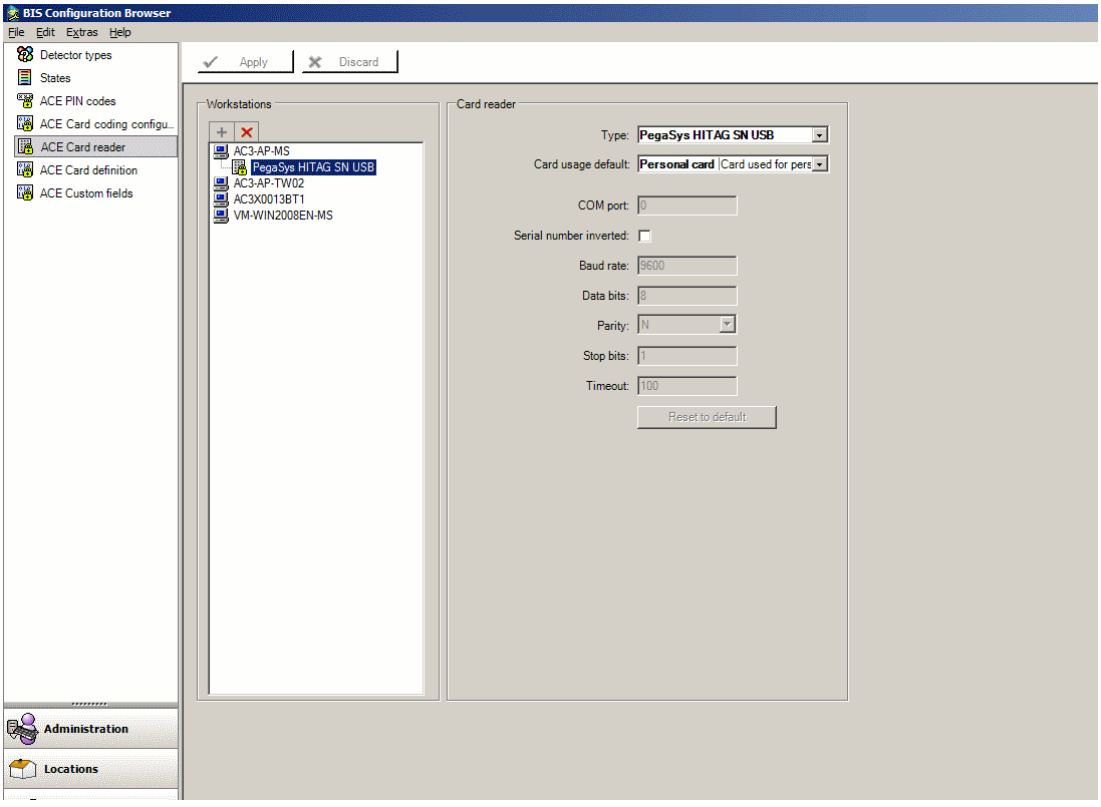
– Select the tab **ACE Operator Settings**
– Enter a name in the search field and click **Search person**.
– Select a person from the result list and click **Assign person**.



On the BIS Client proceed as follows:

– Start the BIS as usual.

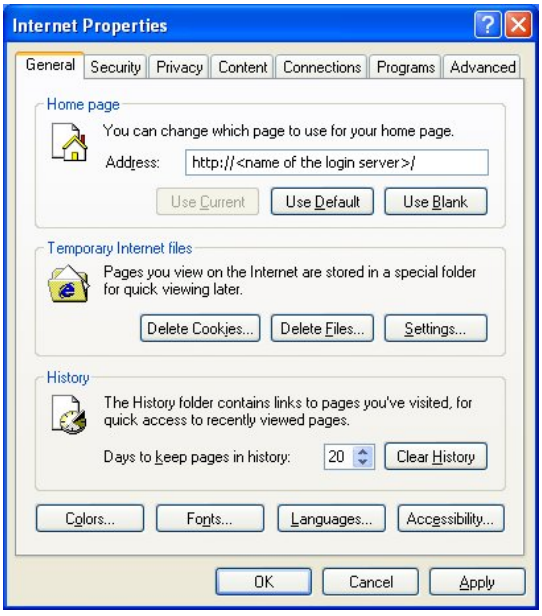
– Log in with the operator name as described above and start the Access Engine. As a result you will get a message that asks you to present a card to the reader.



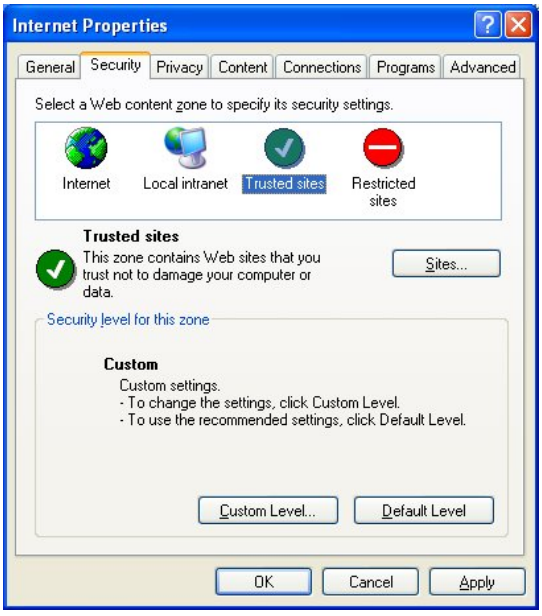
Notice!
In this case only one reader is listed, see “PegaSys Hitag SN USB” in the example above.
If there are more than one readers listed, the **Login Reader** must always be the first reader in the list.

3.9 Setting up a Workstation

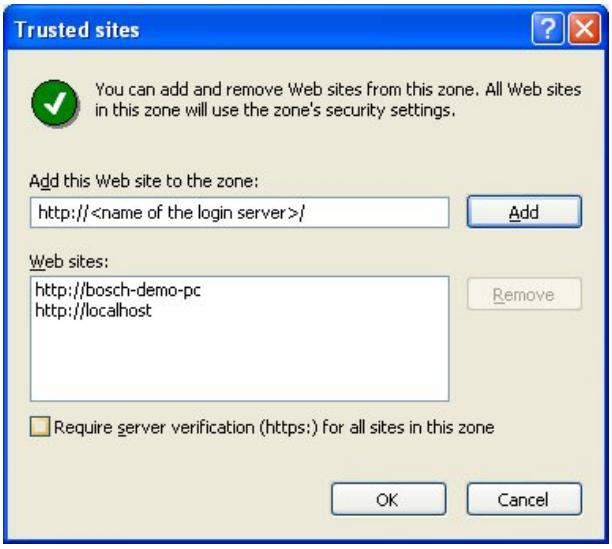
You must configure Internet Explorer. Open IE properties using the desktop icon (right mouse button) or IE's options menu.



The name of the login server is entered as the home page. Then select the **Security** tab.



Select **Trusted Sites** in the selection window and click **Sites...**.

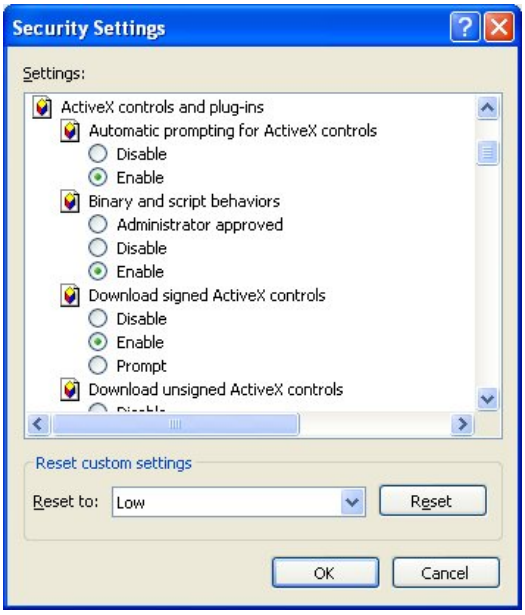


Clear the check box **Require server verification (https:) for all sites in this zone**. Make the following two entries in the upper input field:

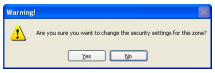
– http://<name of the login server >
– http://localhost

Click **Add** after each entry to enter them into the list field below, then click **OK** to verify the changes.

Now click **Custom Level...** on the **Security** tab.



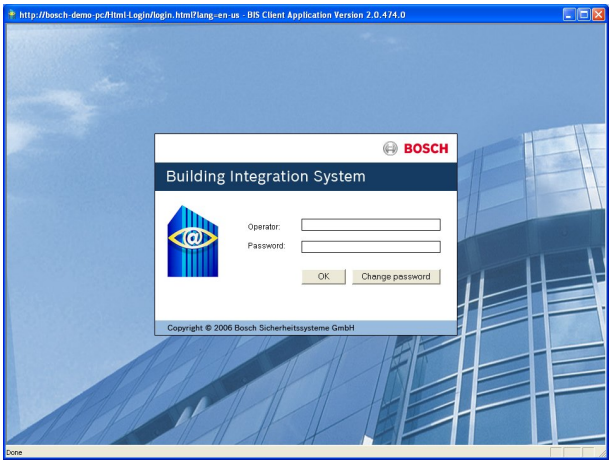
Activate all ActiveX elements and click **OK**. Confirm the following message by clicking **OK**.



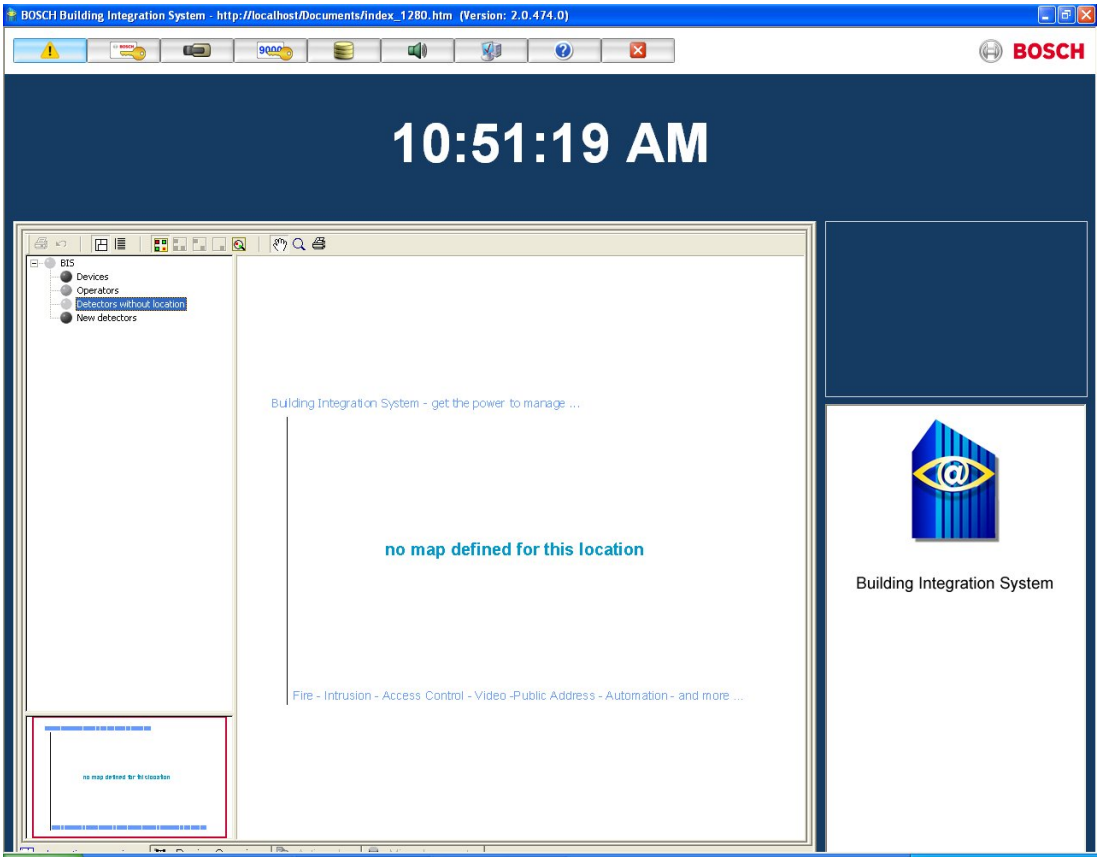
Restart Internet Explorer to open the new home page.

3.10 Starting the Workstation

When starting the workstation for the first time, there might be a delay while some software is downloaded from the BIS server to the client workstation.. After the delay, the BIS system login is shown.



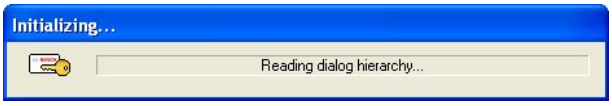
Login using the name and password of an authorized user. The BIS menu is shown.



3.11 Starting the Access Engine Dialog Manager

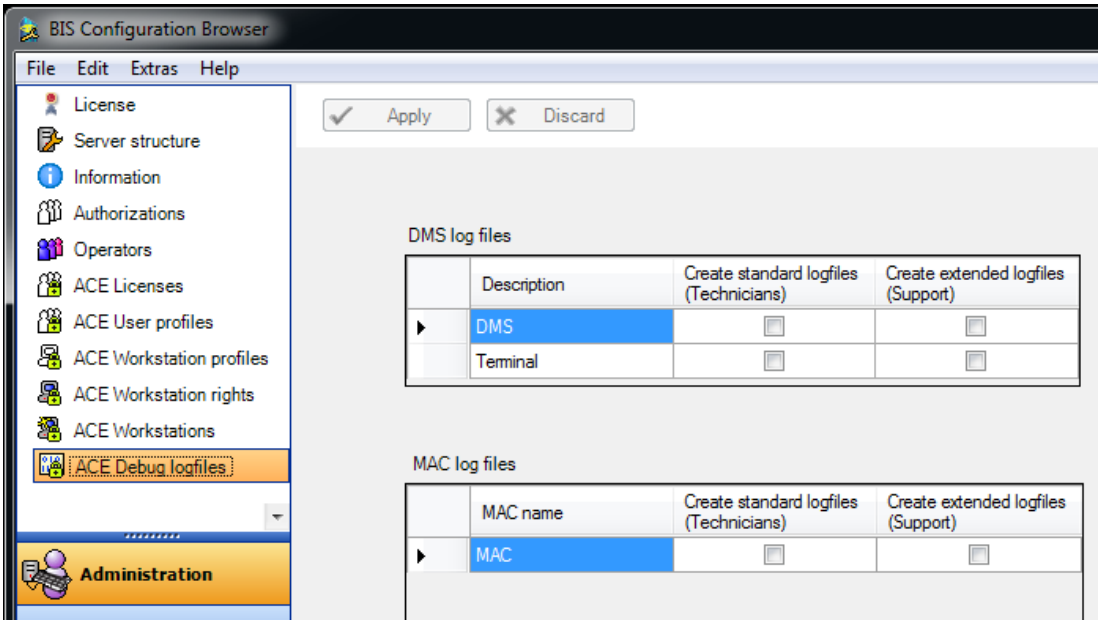
The dialog manager can be started exclusively from client workstations. The BIS server can also be used as a workstation.

Click  to call the Access Engine's dialog manager. A short check of user rights and a composition of the dialogs occurs, based on the user and workstation profiles before the dialog manager shows the menus and dialogs.



3.12 ACE Debug Logfiles

To configure the logging for ACE components select the dialog **Administration** > **ACE Debug logfiles**
The right to make changes in this dialog must be assigned under the dialog **Administration > ACE User Profiles** dialog.
The default configuration is that no check boxes are selected. This setting provides only minimal logging for ACE.



DMS log files
Under **DMS log files** you can configure two kinds of logging:

- **DMS.** All the logs created by server processes.
  If you select one of these check boxes the logging starts immediately.
- **Terminal.** All logs created by ACE workstation and Configuration Browser dialogs.
  If you select one of these check boxes the logging will begin after you save and reload the configuration.

MAC log files
Under **MAC log files** you can configure the amount of detail logged by the Main Access Controller.

Notice!
MAC restarts automatically
If you make and apply any changes to the log file check boxes, then the MAC process will restart automatically. During the usually short restart period it will not be able to handle access requests.

The amount of detail for both DMS and MAC log files is set by the check boxes. Use them as follows

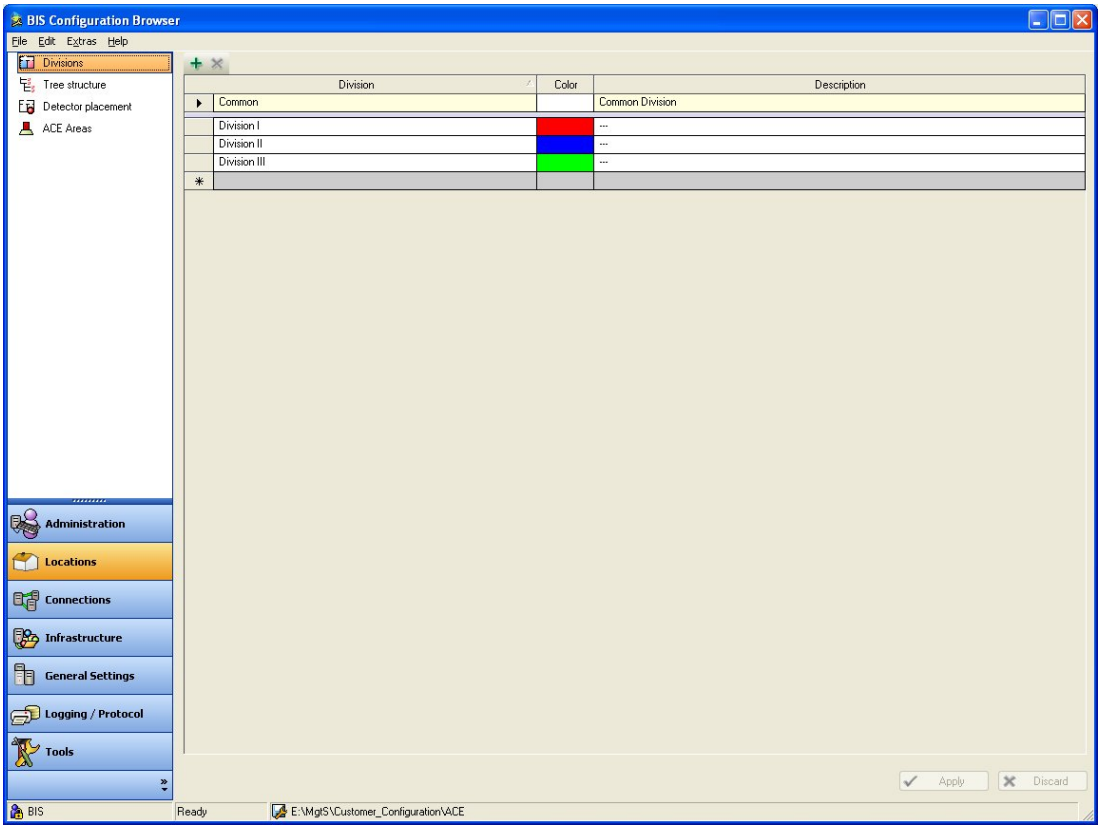
- Select none of the checkboxes (default setting) if the default minimal logging is sufficient. Note that clearing the check boxes does not delete existing log files. Delete the files manually if they are no longer required.

- Select the check box **Create Standard logfiles (Technician)** if you require moderate detail in the log files.
- Select the check box **Create Extended Log files (Support)** for greater detail, and if requested by technical support

4 Creating and Administrating Areas

4.1 Divisions

BIS may be used to provide joint access control for a facility which is shared by multiple mutually independent or semi-independent clients, hereafter referred to as **Divisions**.
This optional BIS module is contained in every Access Engine system. In the standard product, all records are assigned to the division **Common**. Further divisions can be added at any time. Without data changes these divisions will not have access to the personnel data of the first division. They can easily be switched to another division using the **Change Division** dialog in the Access Engine system. Only device data must be clearly identified later as either common or client (division)-specific data.
When installing the system, the division **Common** is created. If you order the **Division** software extension, the number of other divisions ordered is activated according to the licence. Since this applies to the entire system, creation and configuration is done in the BIS Configuration Browser.
When installing further divisions, an arbitrary line is marked in the list. Click the ✚ button or right-click and select **Add new division** in the context menu. A new list entry with the standard designation **New division <no.>** is created below the divisions already installed.
Select and type over the existing column contents to modify the default entries. Assign a color to the particular divisions for the additional distinction and marking, so that devices and installations of these divisions are marked accordingly.



4.2 Access control Areas

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 (ACE)
BIS Configuration Browser > **Locations** > **ACE 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.

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

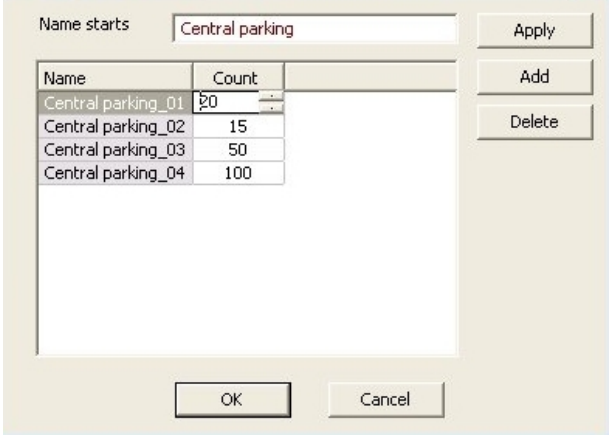
Procedure for deleting areas.

1. Click an area in the hierarchy to select it.
2. Click **Delete**  or right-click to delete via the context menu.

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

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

Connections > tab **Device data**

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.

4.2.1 Limiting populations in access areas

Prerequisite

The operator's **ACE User profile** requires special permission to limit the population of access areas.

1. Navigate to **Administration** > **ACE User profiles**
2. Load the operator's profile in the **Profile name** box
3. Select **Areas** from the list of dialogs
   The **Special functions** box appears at the bottom of the dialog
4. Select the check box **Set maximum number of persons** in the **Special functions** box.
5. Click **Apply** to save the changes to the profile.

Procedure

Dialog path: Client main menu > **System data** > **Areas**

1. Load the name of the area in the **Area name** box
2. Click the **Edit** button and enter the maximum population in the **Max. number of persons** box
3. **Save** your settings

5 Connection Server AccessEngine

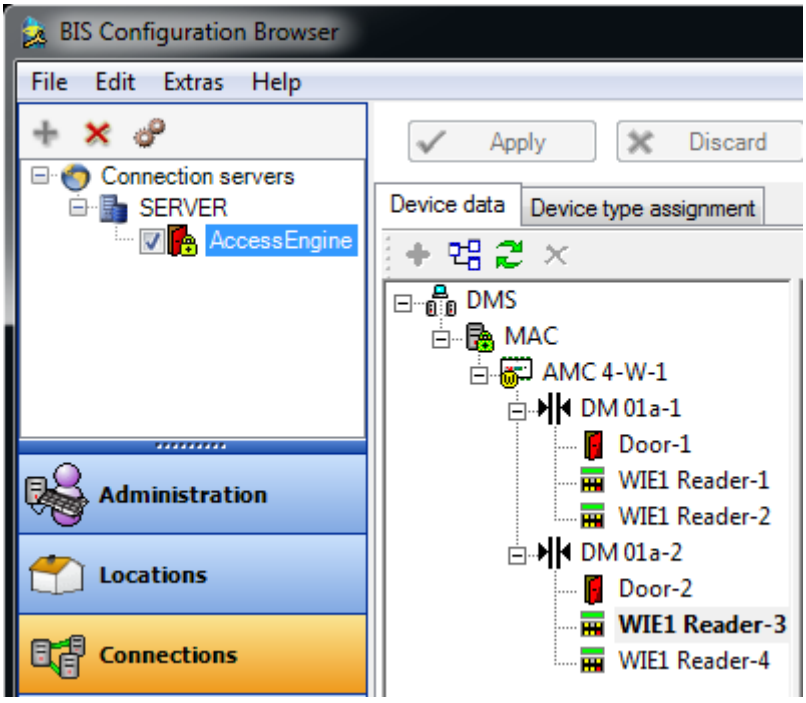
5.1 Device Editor basics

Introduction

The ACE Device Editor, DevEdit, is best used for adding and deleting a smaller numbers of entrances and devices, or for adding, modifying or deleting individual parameters.
DevEdit is not suitable for creating large hierarchies of devices from scratch. For bulk data use the import function.

Opening the Device Editor

To open the Device Editor (DevEdit) in the BIS Configuration Browser, click **Connections** and select **AccessEngine** in the **Connection servers** tree. The device tree is shown to the right of it.



Any devices that have already been configured appear in the device tree. The tree can be viewed by clicking the ⊞ symbol to expand one level, and the icon in the toolbar to expand the entire tree.
The main part of the dialog, to the right of the Device Editor, shows the configurable properties of the device that is currently selected in the device tree.

Using the DevEdit toolbar

The main DevEdit toolbar buttons have the following functions:

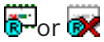
Button	Shortcut	Description
✚	Ctrl + N	Creates a new device below the selected node. Alternatively, right-click the node to invoke its context menu.
	Ctrl + E	Creates a new extension board AMC-EXT on the selected AMC. Alternatively, right-click the node to invoke its context menu.

	Ctrl-A	Expands and collapses the hierarchy.
	Ctrl-K	Refreshes the data by reloading them from the database. If more than one DMS is present then this button invokes a dialog to select between them.
	Del	Deletes the selected item and all beneath it.

Device-tree levels

- All devices belong to a DMS. Only one DMS can be edited at one time. That DMS must be selected when you enter the Device Editor.
- To edit a different DMS click the refresh button  to re-invoke the DMS selection dialog.
- Below the DMS are the Main Access Controllers (MAC)
- Below the MACs are the local access controllers of type Access Modular Controller (AMC).
- The next levels contain the devices controlled by the AMCs, and their dependents.

The following table lists the more common devices and their icons:

	AMC 4W - with and without connection to the DMS
	AMC 4R4 - with and without connection to the DMS
	Entrance
	Door, Barrier, Turnstile
	Reader
	AMC extension board
	Digital input (DIP)
	Digital output (DOP)

When you create a new device in the tree the system increments numeric suffixes to the device names, to ensure uniqueness.

Properties pane

The main pane of the dialog shows the configurable properties of the device that is currently selected in the device tree. Depending on the type of device selected, the properties may be grouped into several tabs.

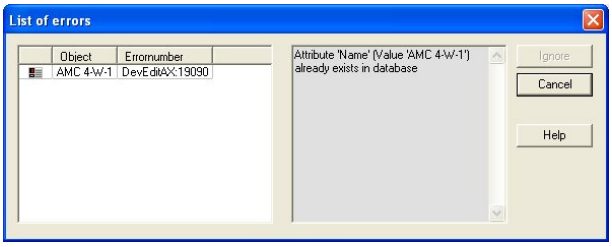
Saving changes

To save the changes you have made to the configuration, click the **Apply** button.
Newly created or modified items are marked with an asterisk (*) until they are saved. It is recommended that you save new items before deleting others.
You can only exit DevEdit by saving or discarding all changes:

Consistency checks

DevEdit will not allow you to create invalid configurations. For example, you cannot create an AMC below another AMC.

As in the bulk import process, all configuration changes are checked for accuracy and completeness. Any errors detected are listed in detail in a dialog box:



To locate the misconfigured device in the overall configuration, select it in the left-hand window of the errors dialog.
After closing the errors dialog the device will be brought into focus in the device tree, and the misconfigured parameter in the main editor window.
You cannot save a configuration until all errors have been corrected.

Refreshing the display of the device tree
Click the Refresh button to ensure that all changes made in various dialogs of the Configuration Browser and the device editor are displayed correctly and completely.

5.2 MACs and RMACs in flat topologies

Access Engine topologies
An Access Engine system can have one or more Data Management Systems (DMS) .
- If it has one DMS, then its topology is called **flat** or non-hierarchical, even if multiple computers are involved.
- If it has more than one DMS then its topology is called **hierarchical**.

A computer that hosts a DMS is known as a DMS server .

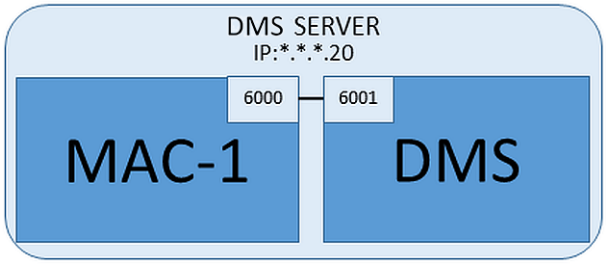
This chapter deals with the configuration of MACs and RMACs in flat topologies only.

The MAC
A Main Access Controller (MAC) is a set of processes running on a computer. The MAC maintains the access control data of the local access controllers (AMCs) connected to it in the device tree; it makes access-control decisions that affect multiple AMCs, and it replenishes the AMCs' data if their connections are temporarily lost.
MACs are subordinate only to the DMS in the device tree.
Every DMS has at least one MAC. One MAC can run on the same computer as its DMS, but it is easier to maintain a configuration where each MAC has its own computer, which is known as a MAC Server .

The RMAC
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.

Note on the illustrations in this chapter and subchapters
IP addresses in the form `*.*.*.dd` (where `dd` is an integer) stand for IP addresses that differ from others in the diagram only by their last digits.

5.2.1 Configuring a MAC on the DMS server without RMAC



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

Procedure

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

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

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

5.2.2 Preparing MAC server computers to run MACs and RMACs

Introduction

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

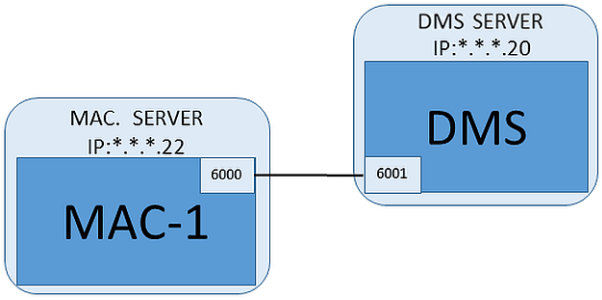
By default the first MAC in an Access Engine system runs on the same computer as its Data Management Server (DMS), however, for enhanced resilience, it is recommended that the MAC run on a separate computer, which can assume access control tasks if the DMS computer goes down.
Separate computers where MACs or RMACs reside, are known as MAC servers regardless of whether they host a MAC or an RMAC.
In order to provide failover capability, MACs and RMACs **must** run on separate MAC servers.

Procedure

Ensure that the following conditions are met on all participating MAC servers:

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

5.2.3 Configuring a MAC on its own MAC server



Prerequisites

– The MAC server computer has been prepared as described in the section *Preparing MAC server computers to run MACs and RMACs, page 34*

Procedure

1. On the DMS server, deactivate the MAC by clearing the check boxes **Activate** and **Load devices** for this MAC in the device editor.
2. On the MAC server, stop the MAC process using the Windows program `services.msc`.
3. Start the `MACInstaller.exe`
   – For ACE this is found on the the BIS installation media `\AddOns\ACE\MultiMAC\MACInstaller` (see the section, *Using the MACInstaller tool, page 40* below).
   –
4. Step through the screens of the tool, supplying values for the following parameters.

Screen#	Parameter	Description
1	**Destination Folder**	The local directory where the MAC is to be installed. Take the default wherever possible.

Screen#	Parameter	Description
2	**Server**	The name or the IP address of the server where the DMS is running.
2	**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.
2	**Number (MAC System Number)**	Set 1 for this and all MACs (as opposed to RMACs)**.**
2	**Twin (Name or IP address of partner MAC)**	Leave this field blank as long as this MAC is to have no RMAC.
2	**Configure Only** (radio button)	Do not select, because you are not configuring a MAC on the main DMS login server.
2	**Update Software** (radio button)	Select this option because you are configuring a MAC on its own computer (MAC server), not on the main DMS login server.

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

Parameter	Description
Name	The name that is to appear in the device tree, For example MAC-1.
Description	Optional description for the benefit of ACE operators
With RMAC (check box)	**<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.
Division	(If applicable) The ACE Division to which the MAC belongs.

See also

– *Device Editor basics, page 31*
– *Configuring a MAC on the DMS server without RMAC, page 34*
– *Adding RMACs to MACs, page 37*

5.2.4 Adding RMACs to MACs

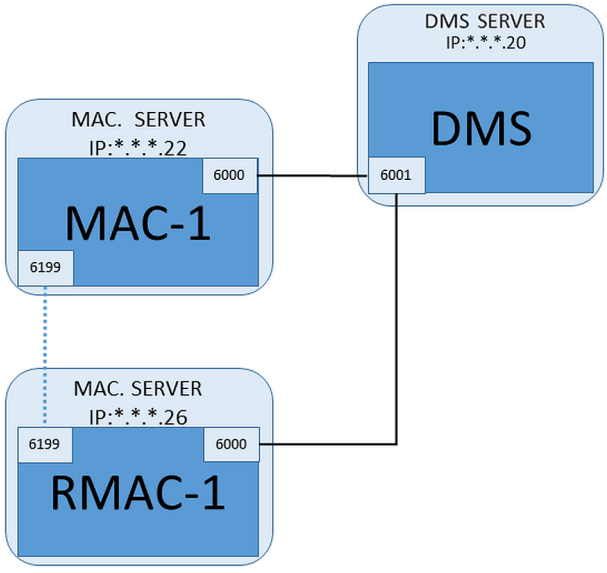
Introduction

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.

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.



Prerequisites

- 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, page 34*

Procedure

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.
Load devices (check box)	**Clear** this check box to suspend temporarily the real-time synchronization between this MAC and its subordinate devices.

Parameter	Description
	This shortens the time needed to open a MAC in the device editor.

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

On the MAC server for the MAC

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

– On the previously prepared MAC server computer, run the MACInstaller tool (see *Using the MACInstaller tool, page 40*) and set the following parameters:
  – **Server**: Name or IP address of the DMS server computer
  – **Port**: `6001`
  – **Number**: `1` (all MACs have Number 1)
  – **Twin**: IP address of the computer where the RMAC will run.
  – **Update software**: Select this option, as you are configuring a MAC server, not the DMS server.

On the MAC server for the RMAC

To configure the RMAC, proceed as follows:

– On its own separate and prepared MAC server computer, run the MACInstaller tool (see *Using the MACInstaller tool, page 40*) and set the following parameters:
  – **Server**: Name or IP address of the DMS server computer
  – **Port**: `6001` (same as for the MAC)
  – **Number**: `2` (all RMACs have Number 2)
  – **Twin**: IP address of the computer where the twin MAC is running.
  – **Update software**: Select this option, as you are configuring a MAC server, not the DMS server.

Return to the Device editor on the DMS server

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

Parameter	Description
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 ACE operators
IP address	The IP address of the RMAC
MAC Port	`6199` (the static default) All MACs and RMACs use this port to check whether their partners are running and accessible**.**

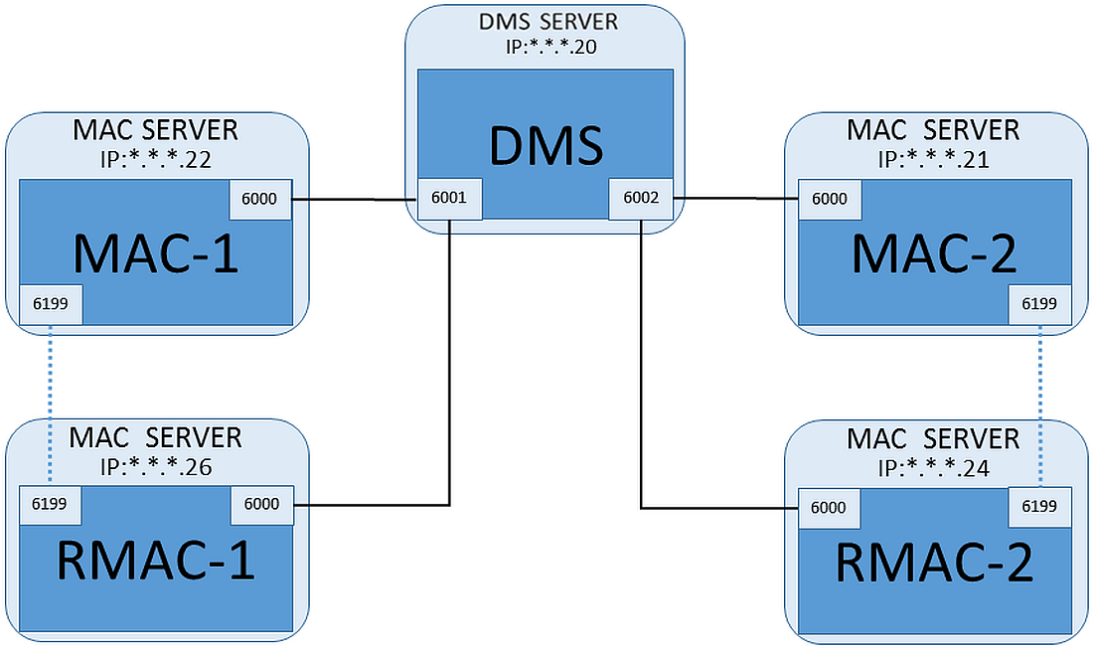
See also

– *Device Editor basics, page 31*

5.2.5 Adding further MAC/RMAC pairs

Introduction

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.



Procedure

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, page 34*
2. Set up the MAC as described in the section *Configuring a MAC on its own MAC server, page 35*
3. Set up the RMAC for this MAC as described in the section *Adding RMACs to MACs, page 37*

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.

5.2.6 Using the MACInstaller tool

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

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

The MACInstaller tool can be found on the BIS installation medium under the following path:
`\BIS_<version>\AddOns\ACE\MultiMAC\MACInstaller.exe`
Through a series of screens it collects values for the parameters below.

Screen#	Parameter	Description
1	**Destination Folder**	The local directory where the MAC is to be installed.
2	**Server**	The name or the IP address of the server where the DMS is running.
2	**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.**
2	**Number (MAC System Number)**	Set 1 for all original MACs. Set 2 for all redundant failover MACs (RMACs).
2	**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.

Screen#	Parameter	Description
2	**Configure Only** (radio button)	Select this option if you are reconfiguring a MAC on the main DMS login server. **See below for details**
2	**Update Software** (radio button)	Select this option if you are installing or reconfiguring a MAC on its own computer (MAC server), not on the main DMS login server. **See below for details**

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.

Notice!

DMS receiver port in hierarchical systems

Note that the numbering scheme for DMS receiver ports is different in hierarchical systems.

For details see *MACs and RMACs in hierarchical topologies, page 127*

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**.

5.2.7 New MAC commands in BIS

Introduction

In BIS Version 4.4 two new commands were added to the context menu for MACs in the BIS client. To invoke them, right-click a MAC in the BIS Client > **Device Overview** tab > **Devices** > **AccessEngine** > **Devices**

– **Switch**
  swaps the roles of the currently active MAC and its redundant backup RMAC. The active MAC becomes the redundant MAC and the redundant MAC becomes the active MAC.
– **Synchronize**
  starts a synchronization of all the MAC database tables with the DMS.

5.3 Creating and configuring local access controllers

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

Local Access Controller - Variants and Extension boards

AMC2 4W	**A**ccess **M**odular **C**ontroller 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.
AMC2 4R4	**A**ccess **M**odular **C**ontroller 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.
AMC2 8I-8O-EXT	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
AMC2 16I-16O-EXT	Extension board for the AMC with sixteen input and output signals	
AMC2 8I-8O-4W	Extension board for Wiegand AMC with eight input and output signals	

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.

Activation/Deactivation of controllers

When first created, a new controller has the following option (check box) selected: **Communication to host enabled**.

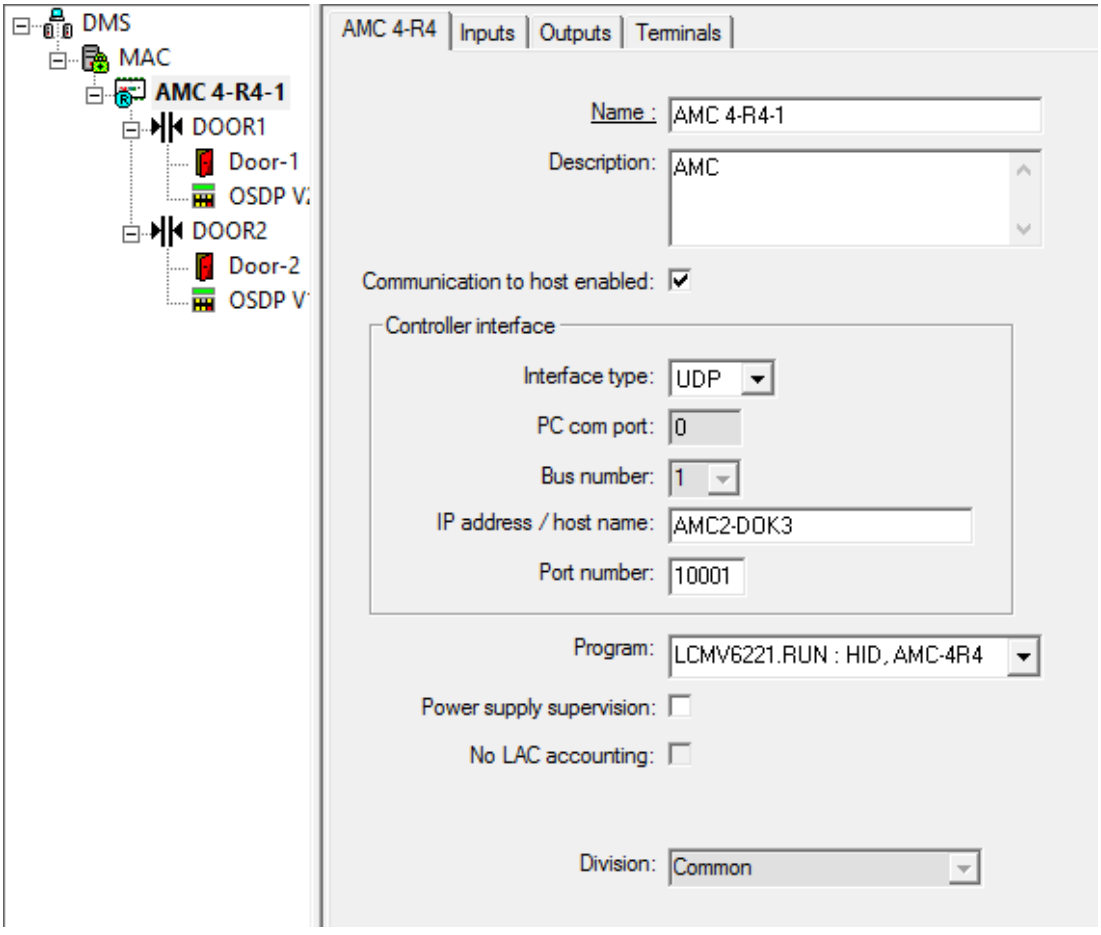
This opens the network connection between the MAC and the controllers, so that any changed or extended configuration data are propagated to the controllers automatically.

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.

5.3.1 AMC parameters and settings

General Parameters of the AMC



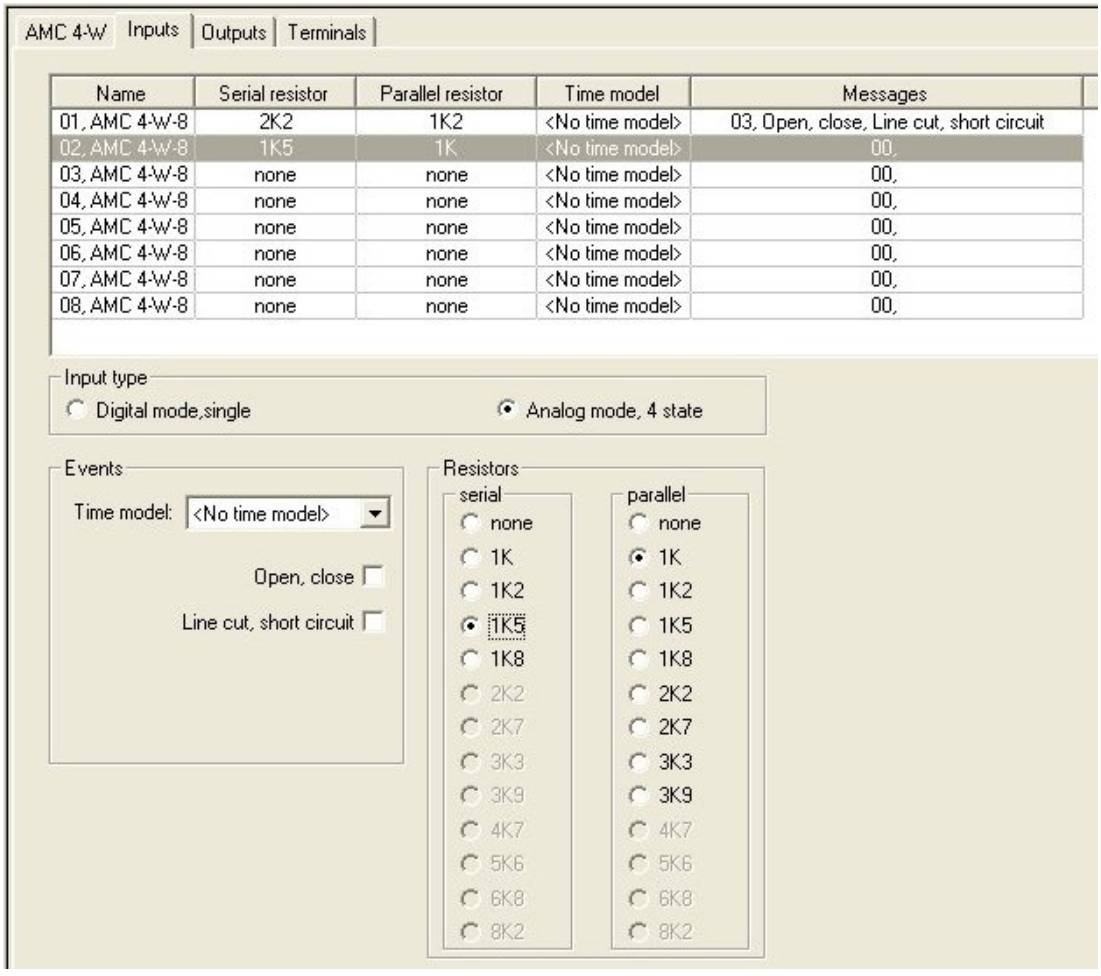
Configuring AMC parameters

Parameter	Possible values	Description
Controller name	Restricted alphanumeric: 1 - 16 digits	ID generation (default) guarantees unique names, but these can be overwritten individually. If overwriting it is the user's responsibility to make sure the IDs are unique. We therefore recommend that Network connections to DHCP servers use the network name.
Controller description	alphanumeric: 0 - 255 digits	This text is displayed in the OPC branch.
Communication to host enabled	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Default value = active The check box displays the current setting and can also be used to change it. The status of the host connection is indicated by the following icons in the Explorer: Controller variant: active not active AMC2 4W   AMC2 4R4   Deactivation provides a means of creating and parameterizing devices to be included in the access control system at a later date. The devices should not be activated, and thus added to the host's database, until put into operation. This also reduces useless polling of the devices by the host.  For security reasons after a software upgrade all controllers are set offline (check box is clear). This ensures that the installation can continue running with the old software, and can be brought up to speed with the new software step-by-step.

		Include new controllers in the installation gradually by checking their respective boxes.
Controller Interface		
Interface Type	COM UDP	COM where connection to the AMC is via one of the MAC COM ports. UDP (= user datagram protocol) where connection is by network. Where this connection type is selected, the parameters "host name" and "remote-controlled port" become settable.  With the interface type "UDP", DIP switch ”5” **must** be set on the AMC. In addition, it is recommended to set switch ”1” to ON.
PC COM port	numeric: with COM-ports: 1 - 256 with UDP-ports: 1 - 65535	Number of the COM ports at which this AMC is connected to the MAC. For ethernet connections via converters, virtual COM-ports are generated and shown here. With type "UDP" enter the port via which the MAC will receive information from the AMC. If this port is unknown the field can be left empty and a free port will be selected automatically.
Bus number	numeric: 1 - 8	Using the interface adapter AMC-MUX up to 8 controllers can be configured on one COM port. In such cases enter the unique address of each AMC as given by its DIP switch. **Note:** Switch 5 can be ignored here because only the first 4 switches are used for addressing. For UDP connections use the default setting (=0)
IP Address/ Hostname	Network name or IP address of the AMC	This input box is only settable if **UDP** is selected as the port type.

		If IP addresses are allocated by DHCP then the network name of the AMC should be provided so that the AMC can be located after a restart even if the IP address has changed. For networks without DHCP the IP address must be given.
UDP Port	numeric: 1 - 10001 - with default configuration	This input box is only activated if **UDP** is selected as port type. This is the AMC port which will receive the MAC-messages.
Further Parameters		
Program	alphanumeric	File name of the program to be loaded into the AMC. The available programs are located in the BIN-directory of the MAC, and can be selected from a list. For convenience the protocol and the description are also shown. This parameter is set automatically as programs are loaded automatically depending on which readers are connected, and the parameter is overridden in the case of a reader/program mismatch.
Power supply supervision	0= deactivated (check box is clear) 1= activated (check box is selected)	Supervision of the supply voltage. If the power supply drops then an informational message is generated. The supervision function assumes the prerequisite of a UPS (uninterruptible power supply), so that a message can be generated. 0 = no supervision 1 = supervision activated
No LAC accounting	0= deactivated (check box is clear) 1= activated (check box is selected)	Select this check box for AMC devices that work jointly to provide access to parking lots, where only the parent MAC keeps account of the number of units entering and leaving. **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”	This is a read-only informational field. "Divisions" are a means of dividing an access control installation between multiple autonomous parties, created and maintained in the BIS Manager.

Configuring AMC inputs



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.

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.

Events and Time models

Depending on the operation mode, the following door states are detected and reported: **Open**, C**losed**, **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.

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.

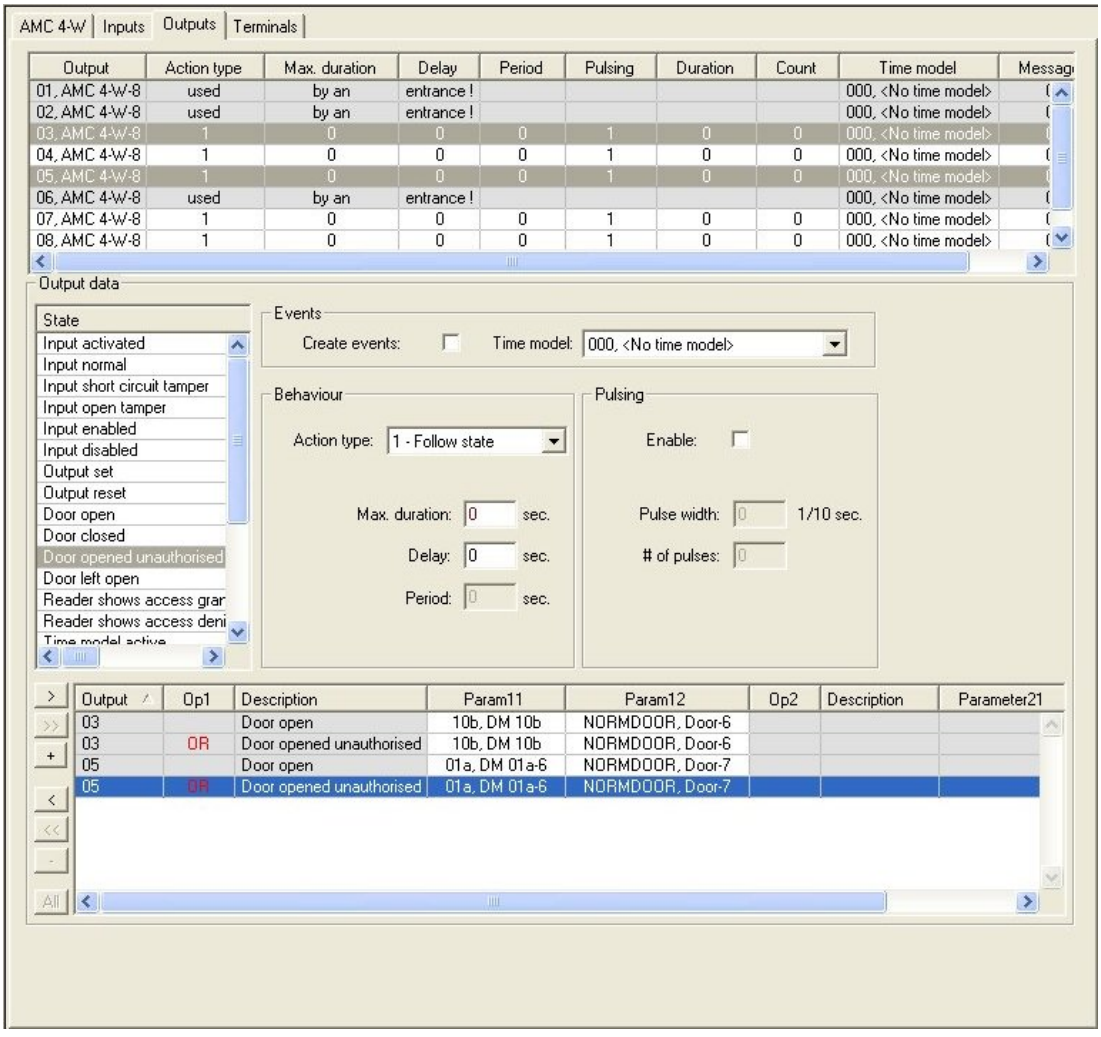
Serial	**Range**		**Parallel**	**Range**
"none" or "---"	1K to 8K2		"none" or "---"	1K to 8K2
1K	1K to 2K2		1K	1K to 1K8
1K2	1K to 2K7		1K2	1K to 2K7
1K5	1K to 3K9		1K5	1K to 3K3
1K8	1K to 6K8		1K8	1K to 3K9
2K2	1K2 to 8K2		2K2	1K to 4K7

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

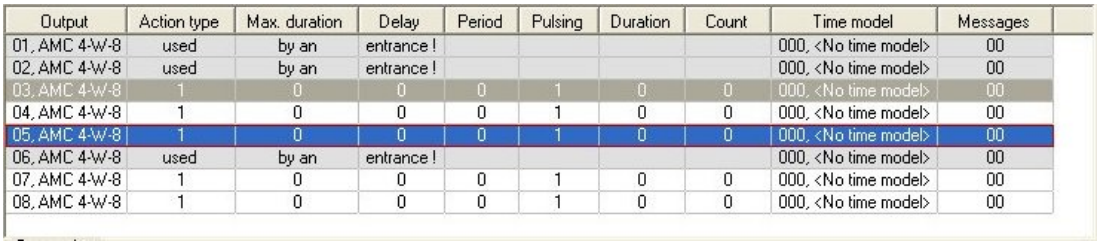
This dialog page provides the configuration of each output on an AMC or AMC-EXT, and contains three main areas:

– 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.



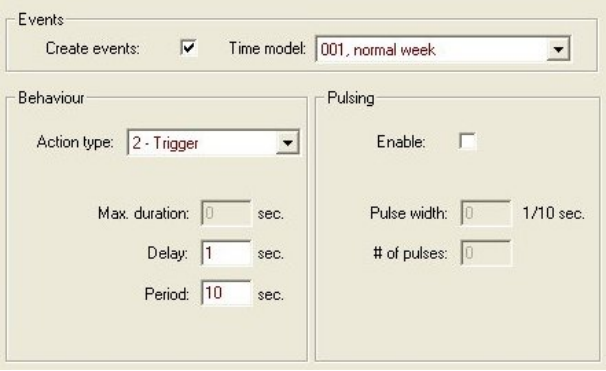
Output	Action type	Max. duration	Delay	Period	Pulsing	Duration	Count	Time model	Messages
01, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
02, AMC 4-W-8	used	by an	entrance !					000, <No time model>	00
03, AMC 4-W-8	1	0	0	0	1	0	0	000, <No time model>	00
04, AMC 4-W-8	1	0	0	0	1	0	0	000,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

Parameters of AMC outputs

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

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

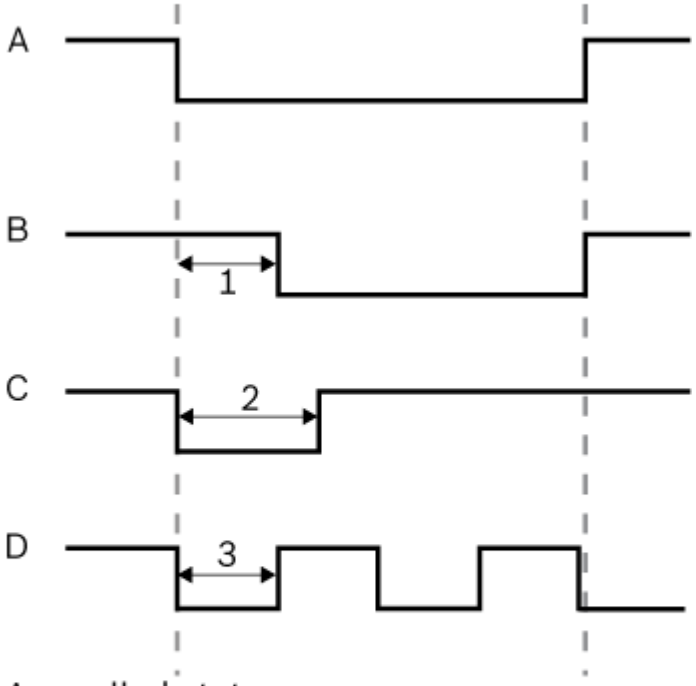


Select the check box **Create events** if a message should be sent for the output activated. If these messages are to be sent only during special periods, e.g. at night or at weekends, then assign a suitable **time model**.

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

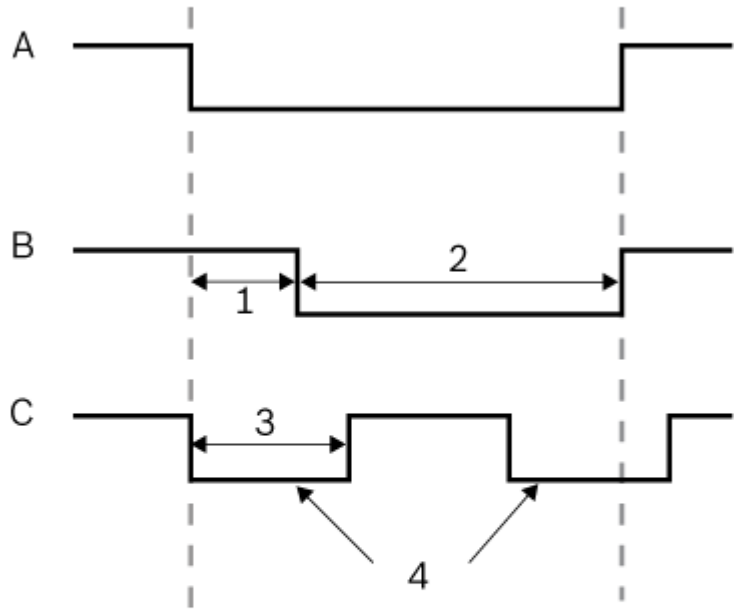
Action type	**Max. duration**	**Delay**	**Period**	**Pulsing/Enable**	**Pulse width**	**Number of pulses**
Follow state	0 = always 1 - 9999	0 - 9999	no	yes	1 - 9999	None
Trigger	no	0 - 9999	0 - 9999 if pulsing is **not** enabled	yes disables period	1 - 9999	1 - 9999
Alternating	no	no	no	yes	1 - 9999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

Pulse diagrams



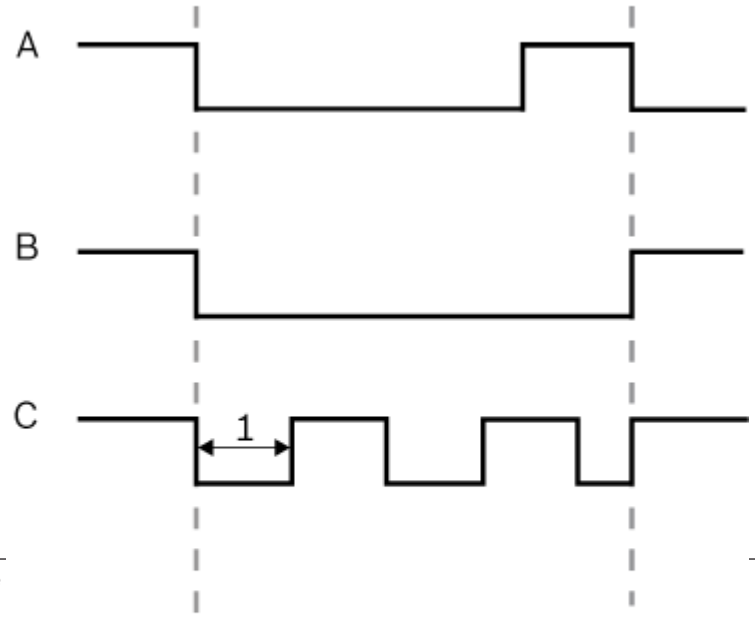
A = polled state
B + C = steady
D = pulsed

1 = Delay time
2 = max. activation time
3 = Pulse width



A = polled state
B = steady
C = pulsed

1 = Delay time
2 = Action period
3 = Pulse width
4 = Pulse count (=2)

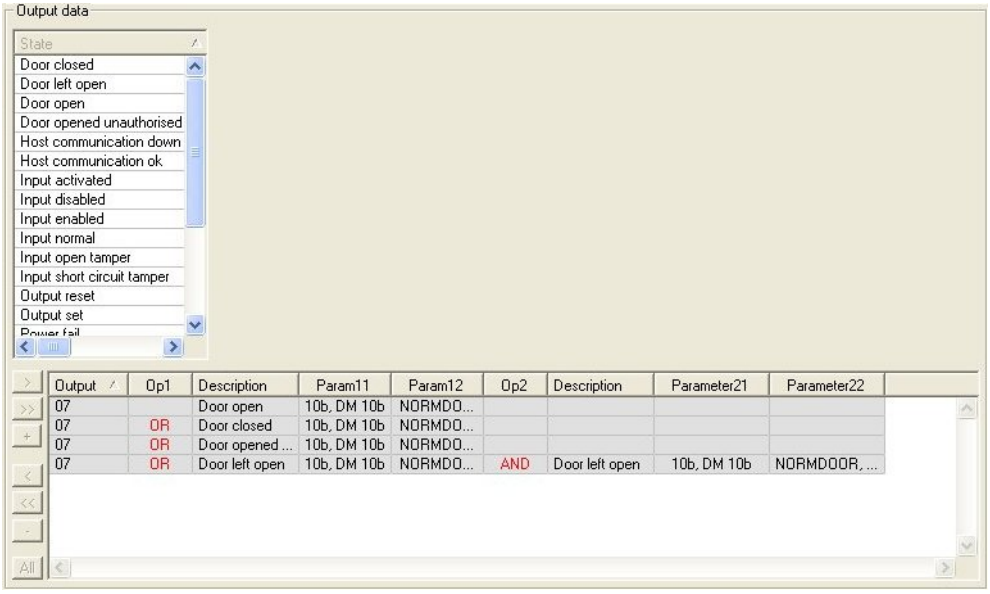


A = polled state

AMC output data

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

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



Configuring states to trigger outputs

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

– Select one or several outputs in the upper list box.
– Select a State from the **State** list.
– If there are several devices or installations to a selected status which can transmit this state, the button » is activated beside the button ›.
  Click › (or double-click the status) to create for each selected exit an entry of its status with the first device (for example, AMC, first entrance) and the installation (for example, first signal, first door).

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

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

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

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

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

Shortcuts with AND are also possible:

– A status must already be assigned to which another condition is added by selecting it in an arbitrary column.

– Then another status is selected and connected to the marked status by clicking .

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

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

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

– Select the assigned entry in an arbitrary column.

– This status is created for all existing devices and installations by clicking All.

Modifying the parameters of outputs

List entries can be changed.

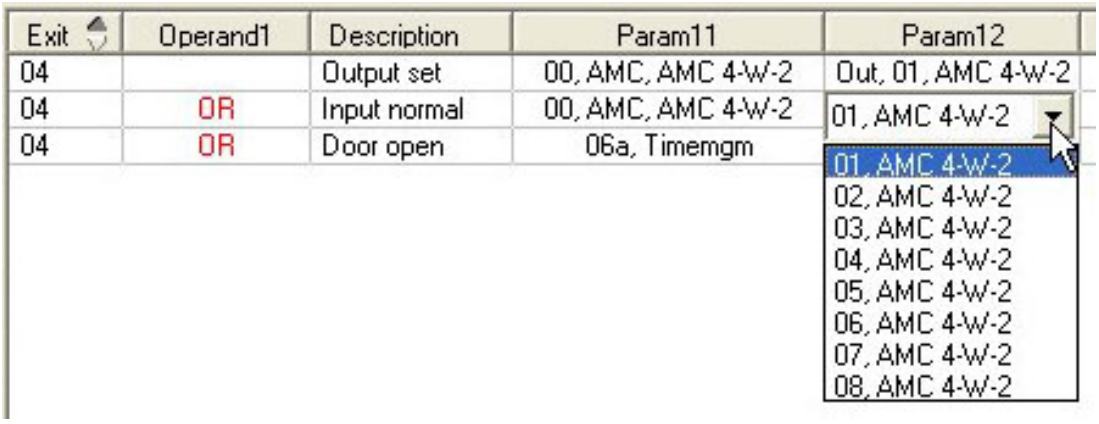
With several devices or installations to which the assigned status could match, the first devices and installations of this type are always set.

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

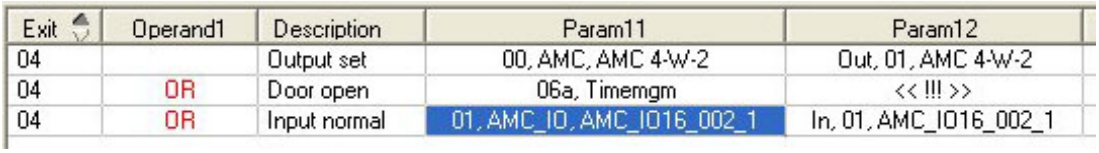
If several devices (for example, I/O boards) or installations (for example, additional signals, readers) exist, the mouse pointer changes while pointing to this column.

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

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



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



Notice!
This is only possible for columns **Param11**, **Param12**, **Param21** and **Param22**.
If there are no other options (for example, because only one entrance was configured), the mouse pointer does not change and all field are grey. If this entry is double-clicked, this is interpreted as a deletion command, and the message box for verifying the deleting appears.

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

If several states have been associated with an output, then they can all be deleted together as follows:
- Select the first list entry (the one which has no entry in the column **Op1**) and then click the '**<<**' button .
- Alternatively, double-click the first entry.
  - A popup window appears. Confirm or abort the deletion.
  - If you confirm deletion then a second popup asks whether you wish to delete all associated entries (answer **Yes**), or only the selected entry (answer **No**).

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

State description
The following table provides an overview of all selectable states, their type number, and description.
The list field **State** contains these parameters as well - they are indicated by scrolling right on the list.

State	Type	Description
Input activated	1	Local input

Input normal	2	Local input
Input short circuit tamper	3	Local input with resistor configured
Input open tamper	4	Local input with resistor configured
Input enabled	5	Local input activated by time model
Input disabled	6	Local input deactivated by time model
Output set	7	Local output, not current output
Output reset	8	Local input, not current input
Door open	9	GID of the entrance, door number
Door closed	10	GID of the entrance, door number
Door opened unauthorized	11	GID of the entrance, door number, replaces "Door open" (9)
Door left open	12	GID of the entrance, door number
Reader shows access granted	13	Reader address
Reader shows access denied	14	Reader address
Time model active	15	Configured time model
Tamper reader	16	Reader address
Tamper AMC	17	---
Tamper I/O board	18	---
Power fail	19	for battery powered AMC only
Power good	20	for battery powered AMC only
Host communication ok	21	---
Host communication down	22	---
Reader Messages	23	(Details depend on the current software version)
LAC Messages	24	(Details depend on the current software version)

Configuring outputs

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

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

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

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

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

Example with all contacts:

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

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

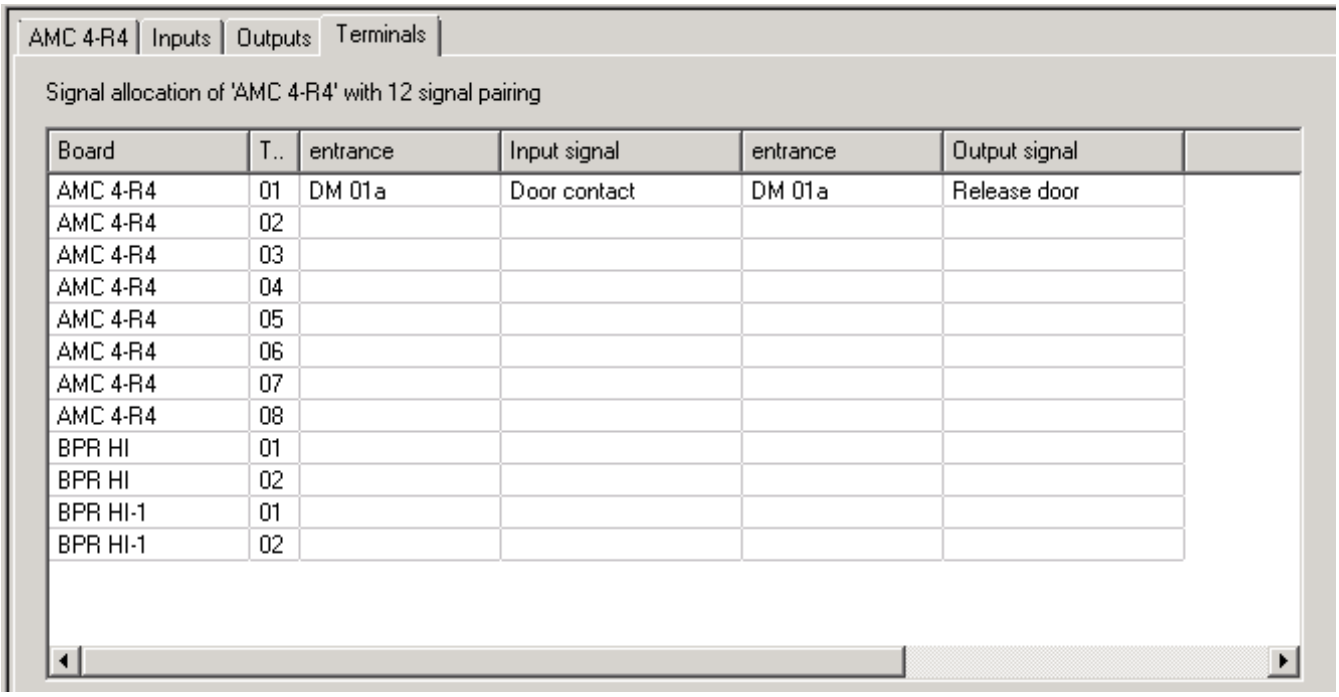
List of all existing states with the default values for the Parameter11/21 and 12/22:

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

Defining signals on the Terminals tab

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

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



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				

5.4 Creating and configuring entrances

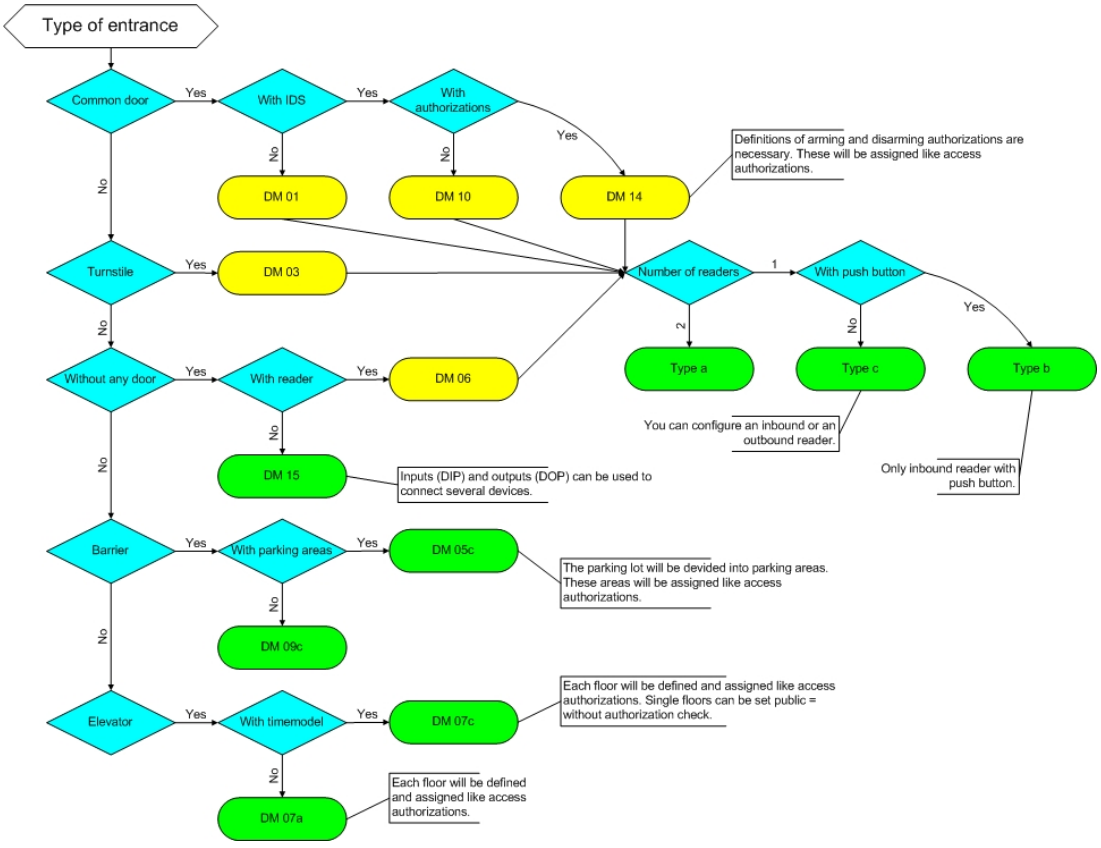
5.4.1 Entrances - background

Terminology: Entrance vs Door model

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.
ACE is very likely already to have a door model for your requirements: first choose the type of entrance (door, turnstile, boom, mantrap, elevator, etc.), then the number of readers, and then any peculiarities of the entrance.
The following flowchart helps in the selection of a suitable door model.



After selecting a door model and specifying the reader type the entrance elements are created in the software, along with their default controls. These can be customized later if required.

5.4.2 Creating Entrances

Selecting a door model:

The following table lists and briefly describes the door models available:

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

Important characteristics of door models.

– 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.

Variants of individual door models

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.

Checks for completeness

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.

Selecting readers for local access controllers:

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

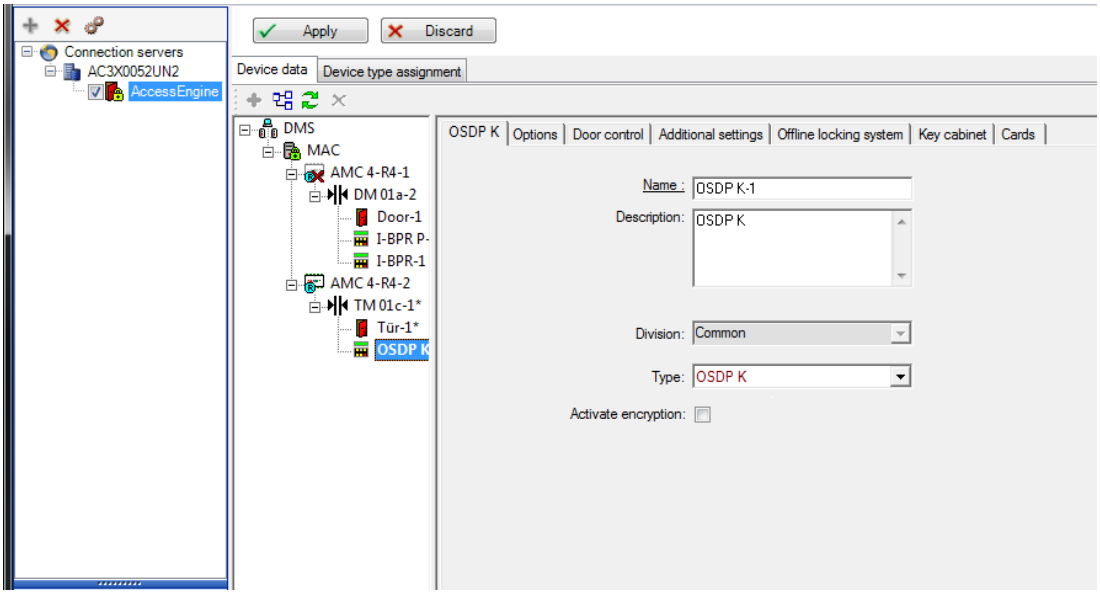
– For **AMC 4W** types only Wiegand-readers are available, both with and without keyboard.
– For **AMC 4R4** the readers in the following table are available. Do not mix protocols on the same controller.

Reader name	Wiegand-Protocol	BPR-Protocol	I-BPR-Protocol	HID-Protocol
WIE1	X			
WIE1K (Keyboard)	X			
BPR MF		X		
BPR MF Keyboard		X		
BPR LE		X		
BPR LE Keyboard		X		
BPR HI		X		
BPR HI Keyboard		X		
TA40 LE		X		
TB30 LE		X		
TB15 HI1		X		
INTUS 1600			X	
I-BPR			X	
I-BPR K (Keyboard)			X	
DT 7020			X	
OSDP				X

OSDP K (Keyboard)				X
OSDP KD (Keyboard +Display)				X
HADP				X
HADP K (Keyboard)				X
HADP KD (Keyboard +Display)				X
RKL 55 (Keyboord + LCD)				X
RK40 (Keyboard)				X
R40				X
R30				X
R15				X

Creating entrances using OSDP readers

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



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

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

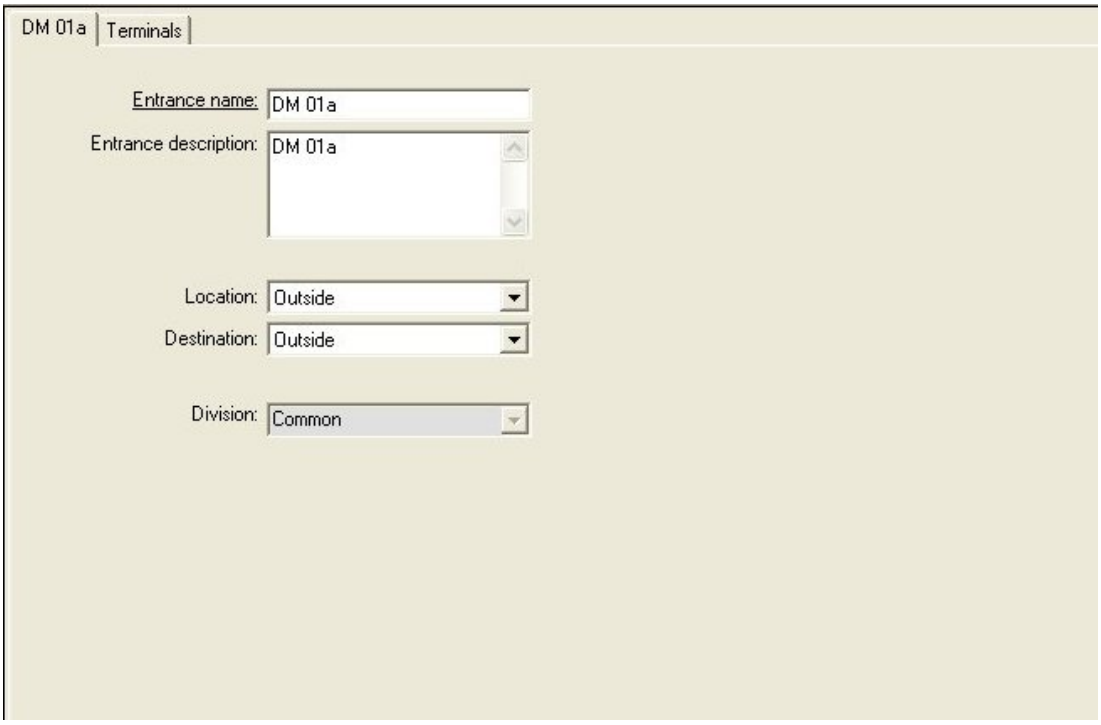
The following OSDP readers have been tested:

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.

General door-model parameters



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 **Desintation**.
Waiting time external access decision	Number of tenths of a second	The time for which access controller waits for a decision from the access control system. before making its own decision.
Division	A read-only field	The defined division to which the reader belongs. The default division is **Common**.
Latency alarm device (only for entrance models 10 and 14)	100 - 9999	The time span in which the door opener can be activated without an alarm being released. This is a reader parameter which is set and then sent to the readers. The unit of this parameter is one tenth (1/10) of a second.
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.

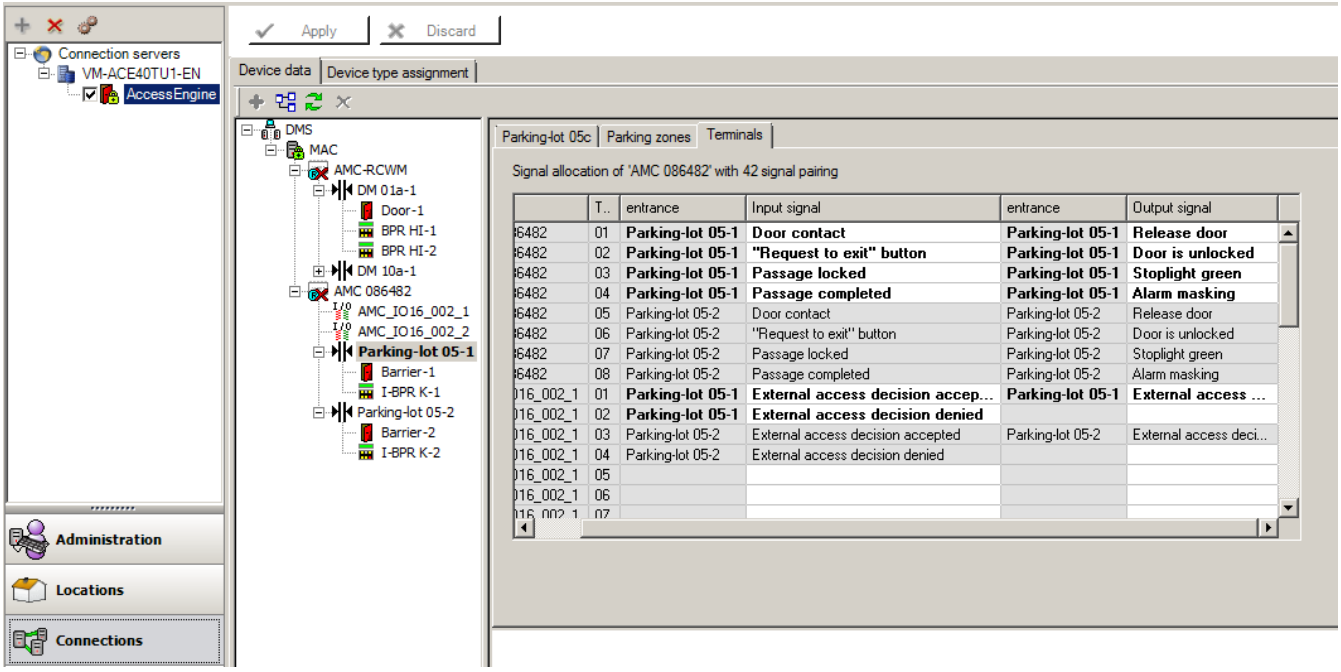
5.4.3 Additional I/O checks

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.



The following functions are performed by the AMC:

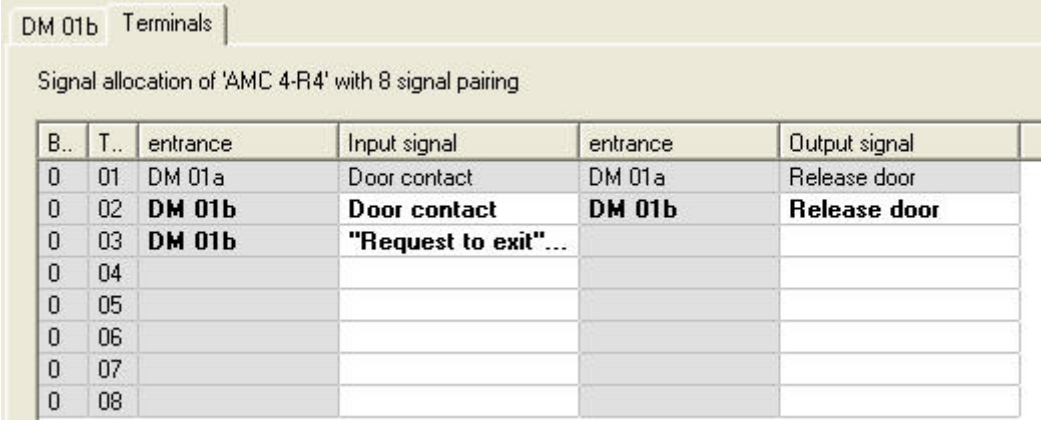
Card Status	Signal = 1:ANPR authorized	Signal = 0: ANPR not authorized
Card authorized	Access	Invalid vehicle number' event
Card on blacklist	Not authorized - blacklist	Not authorized - blacklist
Card expired	Not authorized - expired	Not authorized - expired
Card not authorized for this reader	Not authorized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

It is possible to open the barrier manually even if the visitor is not recognized.
For that functionality a switch is connected to the AMC I/O contacts.
The AMC sets an output signal **Additional check active** before the input signal is analyzed.
If a new visitor is registered, the license plate info must be entered by the operator in the BIS (for reports) and in the ANPR system (for scanning).
ANPR will recognize for a registered vehicle from its database.

5.4.4 Terminals

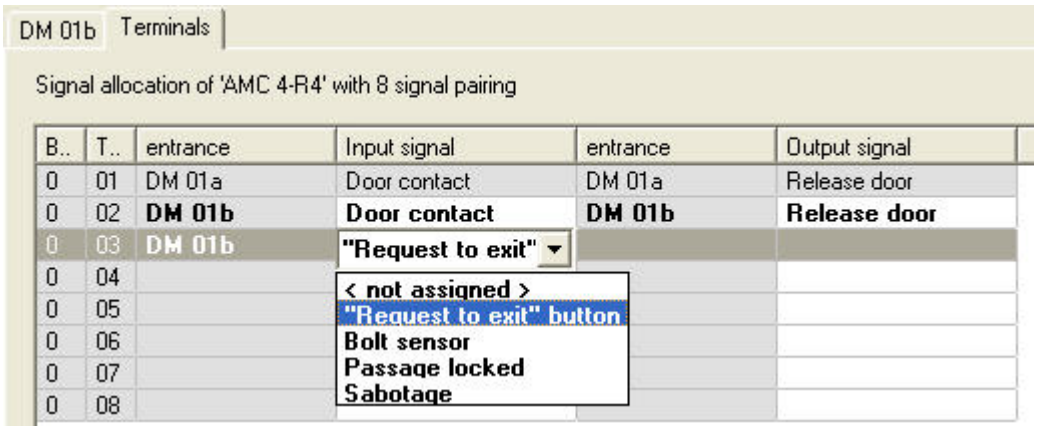
Configuring Terminals

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

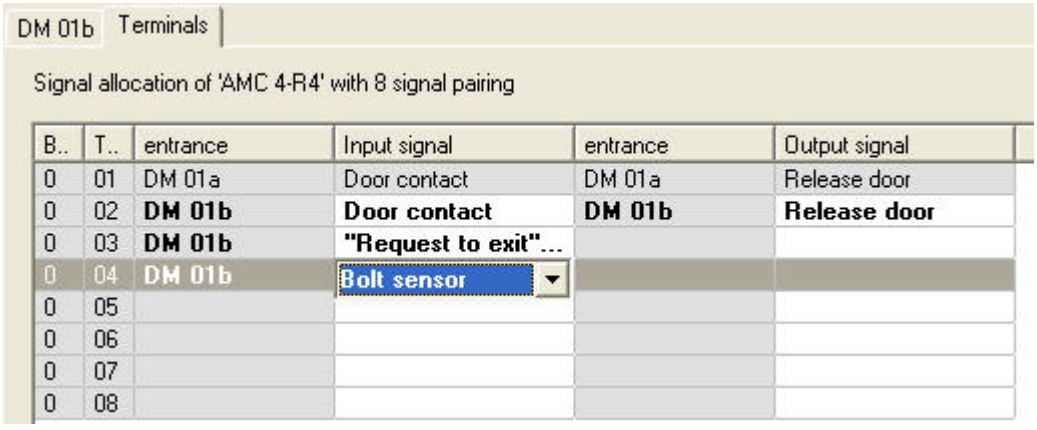


B..	T..	entrance	Input signal	entrance	Output signal
0	01	DM 01a	Door contact	DM 01a	Release door
0	02	**DM 01b**	**Door contact**	**DM 01b**	**Release door**
0	03	**DM 01b**	**"Request to exit"...**		
0	04				
0	05				
0	06				
0	07				
0	08				

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.



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



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.

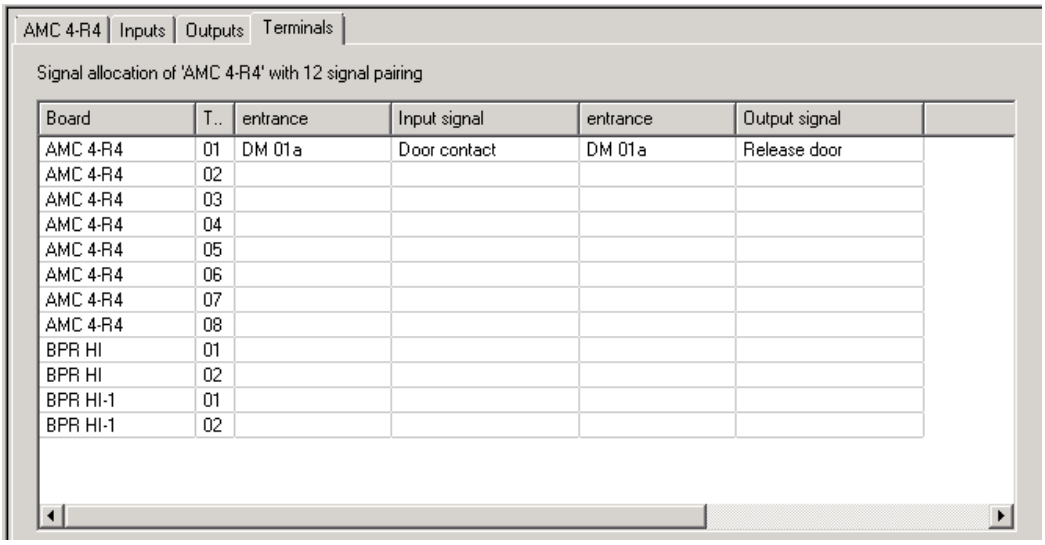
Notice!
The combo-boxes are not 100% context-sensitive, therefore it is possible to select signals that will not work in real life. If you add or remove signals on the **Terminals** tab, test them to ensure that they are logically and physically compatible with the entrance.

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.

The following signals are available for inputs and outputs:

Table of input signals

Input Signals	Description
Door sensor	
Request to exit button	Button to open the door.
Bolt sensor	Is used for messages, only. There is no control function.

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

Table of output signals

Output Signals	Description
Door opener	
Sluice: lock opposite direction	Locks the other side of the mantrap. This signal is sent when the door opens.
Alarm suppression	... to the IDS. Is set as long as the door is open, to avoid that the IDS creates an intrusion message.
Indicator green	Indicator lamp - will be controlled as long as the door is open.
Door open too long	Pulse of three seconds. If the door is open too long.
Camera activation	Camera will be activated at the beginning of a passage.
Open turnstile inbound	
Open turnstile outbound	
Door is permanent open	Signal to unlock a door for an extended period.
IDS: arm	Signal to arm the IDS .
IDS: disarm	Signal to disarm the IDS .
External access decision activated	Signal must be set to activate external access system

Mapping table of door models to input and output signals

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

Door Model	Description	Input Signals	Output Signals
01	Simple door with entry and exit reader Readers for time & attendance External access decision available	- Door sensor - "Request to exit" button - Bolt sensor - Entrance locked - Sabotage - Local open enable - External access decision accepted - External access decision denieded	- Door opener - Sluice: lock opposite direction - Alarm suppression - Indicator green - Camera activation - Door open too long - External access decision activated
03	Revolving door with entry and exit reader Readers for time & attendance External access decision available	- Turnstile in rest position - "Request to exit" button - Entrance locked - Sabotage - External access decision accepted - External access decision denieded	- Sluice: lock opposite direction - Open turnstile inbound - Open turnstile outbound - Alarm suppression - Camera activation - Door open too long - External access decision activated
05	Parking lot entrance or exit - maximum of 24 parking zones Readers for time & attendance External access decision available	- Door sensor - "Request to exit" button - Entrance locked - Passage completed - External access decision accepted - External access decision denieded	- Door opener - Alarm suppression - Indicator green - Door open too long - Door is permanent open - External access decision activated
06	Readers for time & attendance		
07	Elevator - maximum 56 floors		
09	Vehicle entrance or outgoing reader and push button Readers for time & attendance External access decision available	- Door sensor - "Request to exit" button - Entrance locked - Passage completed - External access decision accepted - External access decision denieded	- Door opener - Alarm suppression - Indicator green - Door open too long - Door is permanent open - External access decision activated
10	Simple door with entry and exit reader and IDS arming/disarming	- Door sensor - "Request to exit" button - IDS: ready to arm - IDS: is armed - Sabotage	- Door opener - Camera activation - IDS: arm - IDS: disarm - Door open too long

	Readers for time & attendance External access decision available	- IDS: request to arm - External access decision accepted - External access decision denieded	- External access decision activated
14	Simple door with entry and exit reader and IDS arming/disarming Readers for time & attendance	- Door sensor - "Request to exit" button - IDS: ready to arm - IDS: is armed - Sabotage - IDS: request to arm	- Door opener - Camera activation - IDS: arm - Door open too long
15	Digital contacts		

Assigning signals to readers

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

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

Notice!

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

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

Editing the signals

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

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

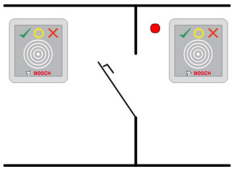
Notice!

The status of reader signals can not be monitored.

They can only be used for the door to which the reader belongs.

5.4.5 Predefined Entrance Model Signals

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

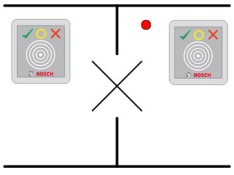
Possible signals:

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

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

Alarm suppression is only activated when the alarm suppression time before door opening is greater than 0.
This entrance model can also be advantageous for vehicle entrances, in which case a secondary reader for trucks and cars is also recommended.

Entrance Model 03



Model variants:

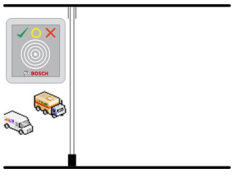
03a	Reversible turnstile with entry **and** exit reader
03b	Reversible turnstile with entry reader and push button
03c	Turnstile with entry **or** exit reader

Possible signals:

Input signal	Output signals
Turnstile in normal position	Open turnstile inbound
"Request to exit" button	Open turnstile outbound
Sabotage	Entrance locked
	Camera activation
	Door open too long
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 sensor	Door opener
"Request to exit" button	Door is permanent open
Entrance locked	Indicator green
Passage completed	Alarm suppression
	Door open too long

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

Entrance Model 06

Model variants

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 access but are used exclusively for time & attendance purposes. They do not control the doors but only forward card data to the time & attendance system.
As a consequence, no signals are defined. These readers are usually installed within an already controlled area.

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

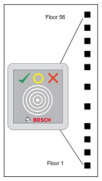
Use variant **a** when entrance and exit are not separate. Use variant **c** if the entrance and the exit are spatially separate, or if you cannot attach the readers to the same controller. Make sure that you define one of the readers as inbound reader and one as outbound reader.
As with any entrance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

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

The registered entry and exit times are stored in a text file in the directory: `C:\MgtS\AccessEngine\AC\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 is not sorted by person but contains all bookings in chronological order, as received by the administration module. The field separator in the file is a semicolon.

Entrance Model 07 variants



Model variants:

07a	Elevator with max. 56 floors
07b	Elevator with max. 56 floors

Entrance Model 07a
Signals:

Input signal	Output signals
	Release <name of the floor>
	One output signal per defined floor, with a maximum of 56.

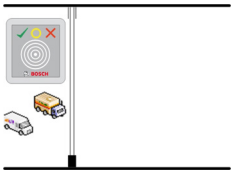
Upon summoning the elevator the card owner can select only those floors for which his card is authorized.
The elevator door models can not be mixed with other door models on the same controller.
Using extension boards up to 56 floors can be defined for each elevator on an AMC. The card's authorizations must contain the elevator itself and at least one floor.

Entrance Model 07c
Signals:

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

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

Entrance Model 09

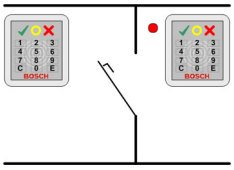


Possible signals:

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

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

Entrance Model 10



Model variants:

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

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

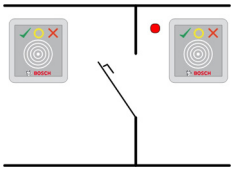
Different procedures are required depending on which readers are installed.
I-BPR readers: (e.g. DELTA 1010, INTUS 1600)
Arm by pressing key **7** and confirming with Enter (#). Then present the card, enter the PIN code and again confirm with the Enter (#) key.
Disarm by presenting the card, entering the PIN code, and confirming with Enter (#).

BPR reader: (including Wiegand)
Arm by pressing 7, presenting the card and entering the PIN code. There is no need to confirm using the Enter key.
Disarm by presenting the card and entering the PIN code. Disarming and door-release occur simultaneously.

Special features of DM 10e:
Whereas with door models 10a and 10b every entrance is its own security area, with 10e multiple entrances can be grouped into units. Any one reader in this group is capable of arming or disarming the whole unit. An output signal **Disarm IDS** is required to reset the status set by any of the readers in the group.
Signals:
- Door models 10a and 10b:
  - - Arming is triggered by a steady signal
  - - Disarming is triggered by the discontinuation of the steady signal.
- Door model 10e:
  - - Arming and disarming are triggered by a signal pulse of 1 second's duration.

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

Entrance Model 14



Model variants:

14a	Normal door with entry and exit reader and IDS arming / disarming
14b	Normal door with entry, push button and IDS arming / disarming

Possible signals:

Input signals	**Output signals**
Door sensor	Door opener
IDS: is armed	IDS: arm

IDS: ready to arm	Camera activation
"Request to exit" button	Door open too long
Bolt sensor	
Sabotage	
IDS: request to arm button	

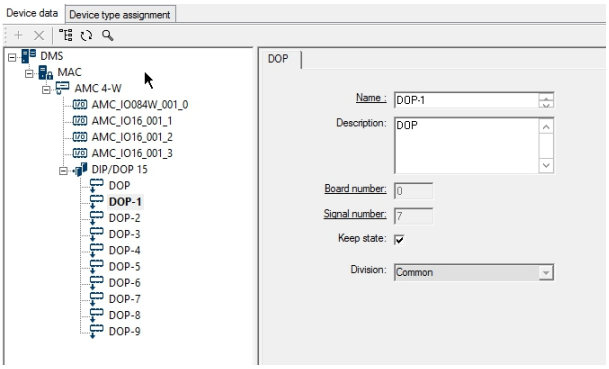
With door model 14 it is possible to form secured areas where the IDS (Intrusion detection system) can be armed from any reader in the area. In such a case the signals **IDS armed** and **IDS ready to arm** need to be replicated at each entrance.
In contrast to model 10 door model 14 can use readers with or without keypads. Another difference is the assignment of arming/disarming authorizations. Only card owners with the proper authorizations can arm/disarm.
In the case of keyboard readers, arming and disarming is performed as with door model 10.
In the case of non-keyboard readers, arming is not achieved by entering the PIN code, but by using a switch near the reader which has the same function as key 7 of the keypad readers.
After using this switch, the status of the alarm device is displayed by the reader's colored LEDs:
– Disarmed = alternating green and red light
– Armed = constant red light
Arm by presenting a properly authorized card.
Disarm by using the switch and presenting a properly authorized card.
Door-release is not automatic upon disarming, but requires the card to be presented again.

Entrance Model 15
Possible signals: These default names can be overwritten.

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

Unlike other door models, entrance model 15 manages those inputs and outputs of a controller which are still free, and places them as generic inputs and voltage-free outputs at the disposal of the whole system.
Unlike the output contacts of other door models, those of entrance model 15 can be individually browsed in BIS's graphical user interface.

A checkbox **Keep state** in the screen for **Device type assignment** allows the user to save the input and output (DIP and DOP) signal statuses if the AMC, MAC or superordinate systems have to be restarted.



– Activate the checkbox to save the latest signal statuses (0 or 1) in case of a restart.
– Deactivate the checkbox to allow resetting to default values in case of a restart.

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.

5.4.6 Special door models

5.4.6.1 Elevators

General notes on Elevators (Entrance Model 07)

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

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

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

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

Differences between entrance models 07a and 07c

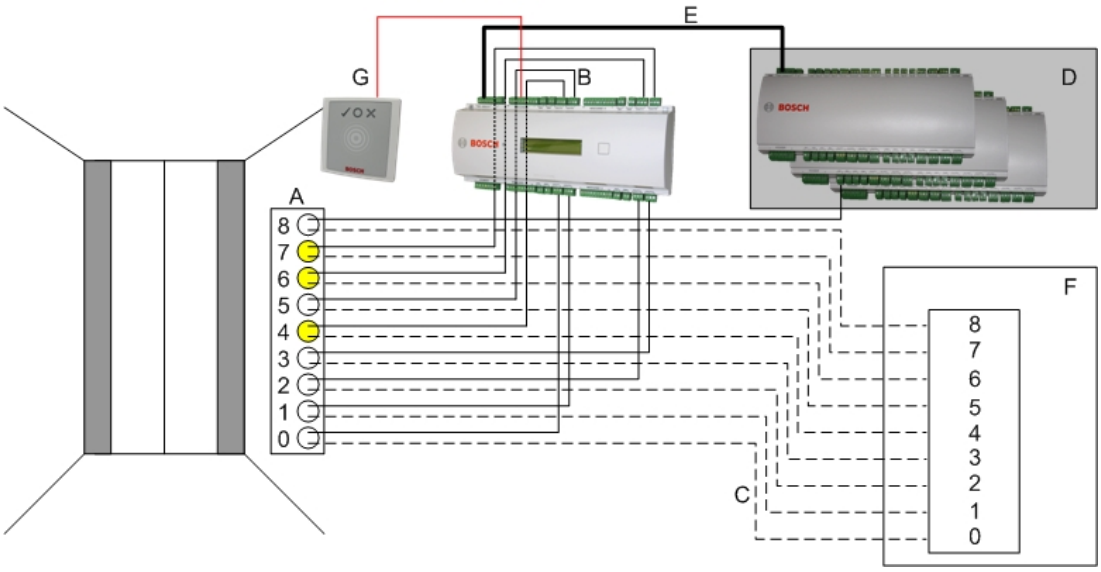
In the access authorization dialogs of the Access Engine System you can assign specific floors to the authorization of a person.

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

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

Wiring scheme for elevators:

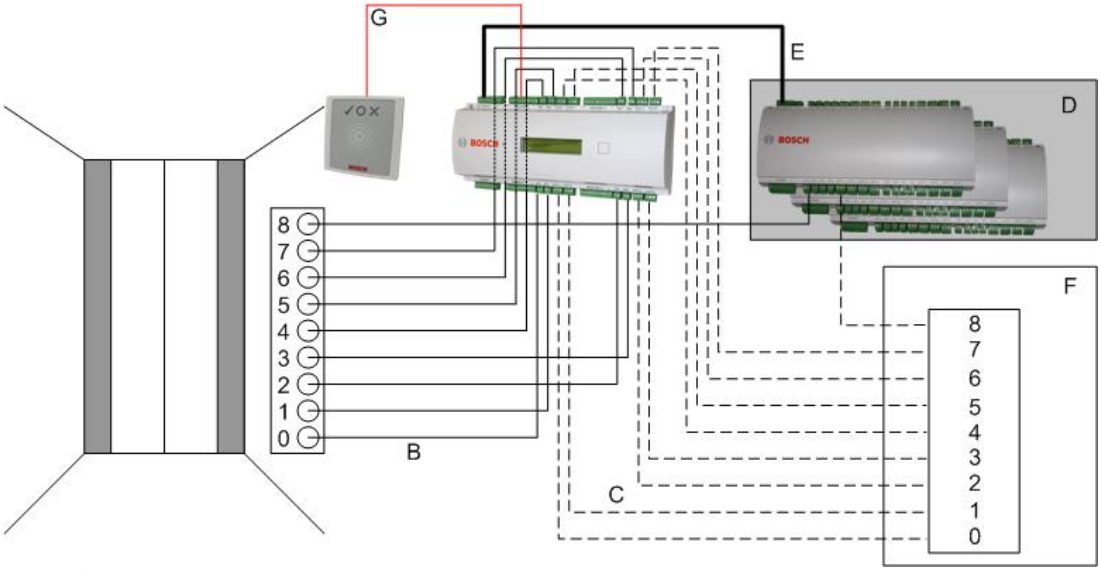
The following picture shows the connection scheme of an elevator using door model 07a.



Legend:

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

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



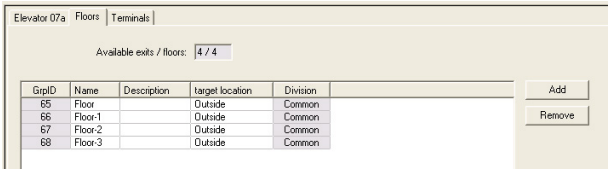
Legend:

- 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.

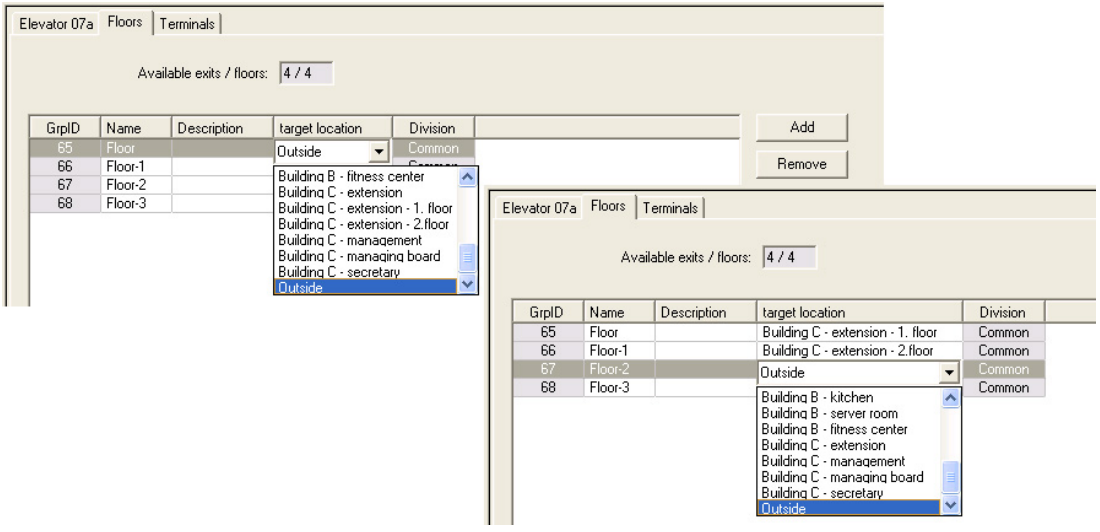
Like parking lots, elevators have the parameter **Public.** This parameter can be set for each floor individually. If the parameter **Public** is activated access authorizations are not checked - so, any cardholder in the elevator can select the floor.
If desired, set a time model for the entrance model: Outside the defined time zones authorizations will be checked.

Floors for entrance model 07

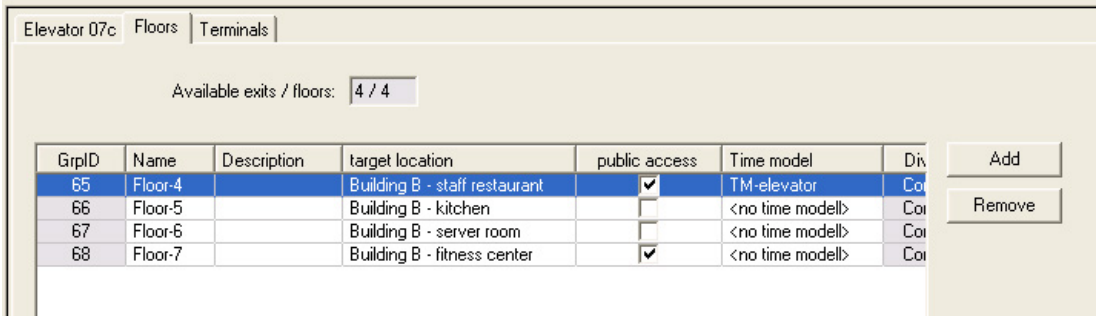
Use the **Floors** tab to add and remove floors for the elevator, using the **Add** and **Remove** buttons.



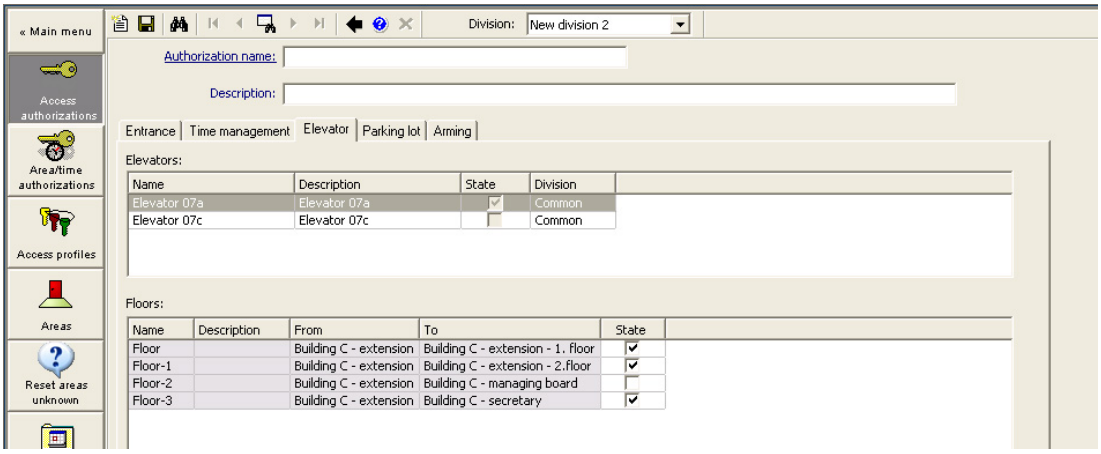
Target locations for a floor can be any **Areas** except parking lots and parking zones.
Only one Area can be assigned to an individual floor. The choice of areas offered in the combo-boxes is therefore reduced after each assignment, thus preventing unintentional double-assignments.



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.



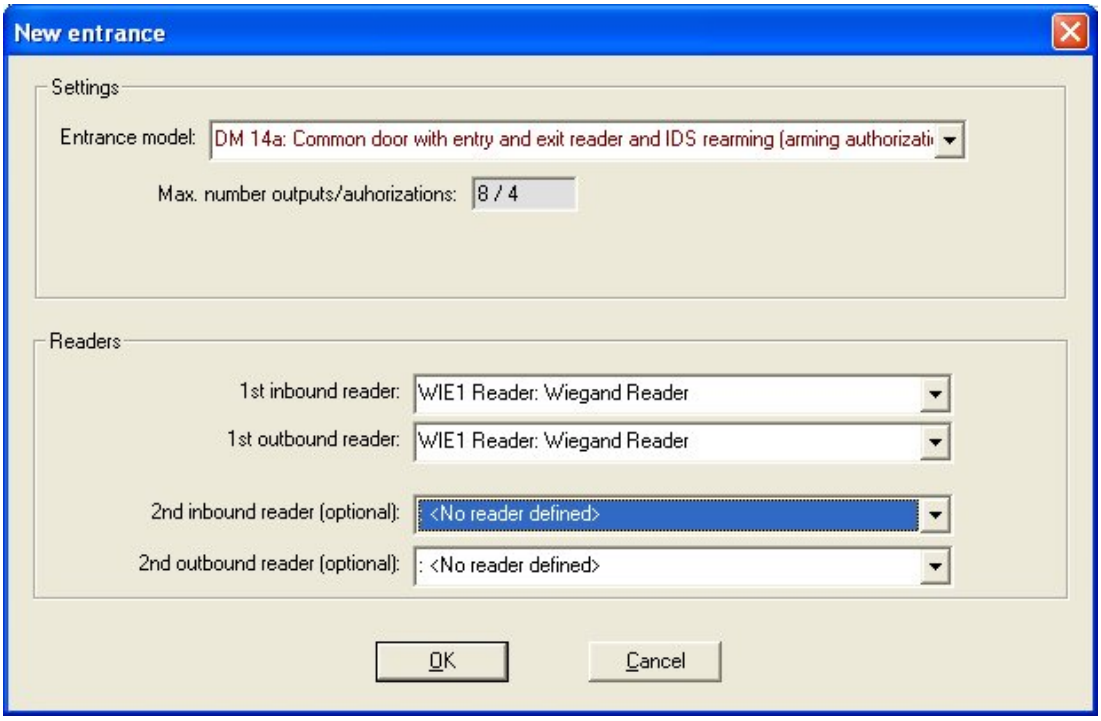
On the **Elevator** tab above the upper list box in the Access Engine dialogs **Access authorizations** and **Area/time authorizations** select first the required elevator and then, below, the floors to which the cardholder is permitted access.



5.4.6.2 Door models with intruder alarms

Arming and disarming intrusion detection systems - DM 14

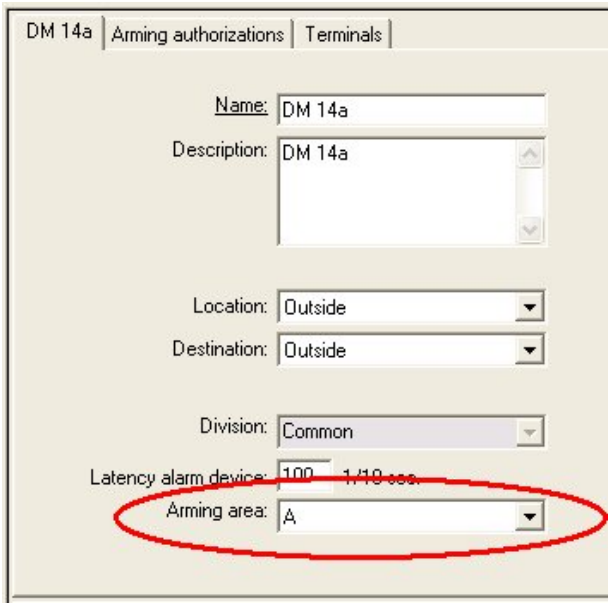
In contrast to entrance model 10, DM 14 can be armed/disarmed.



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

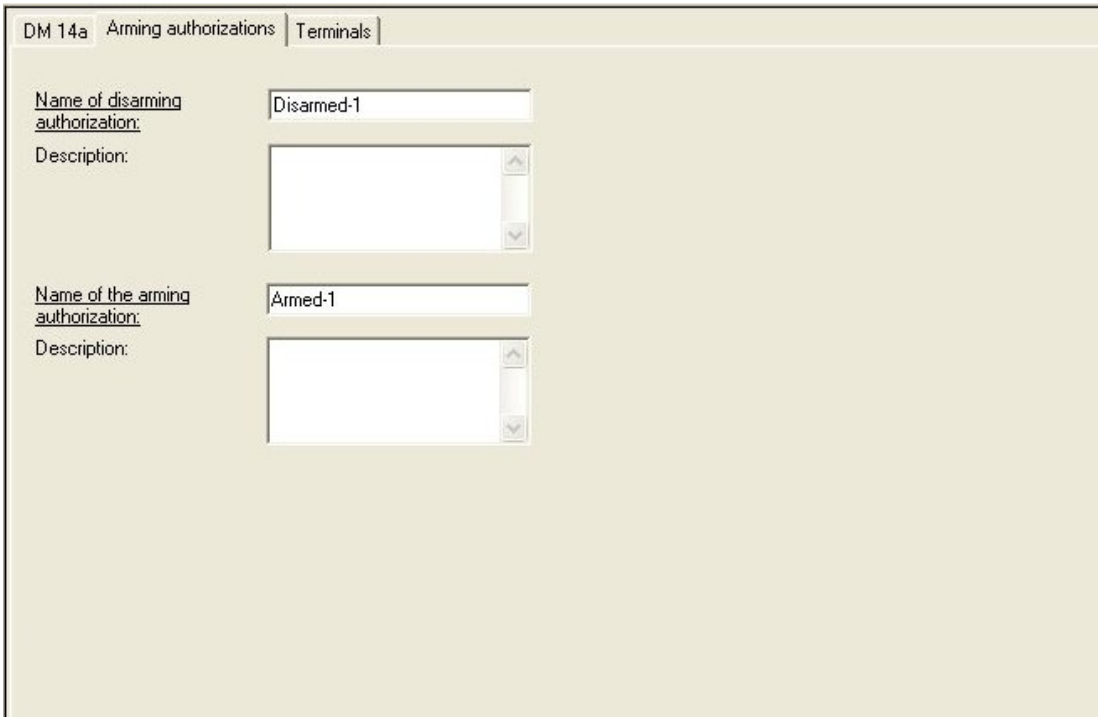
Authorizations for arming with Entrance Model 14

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

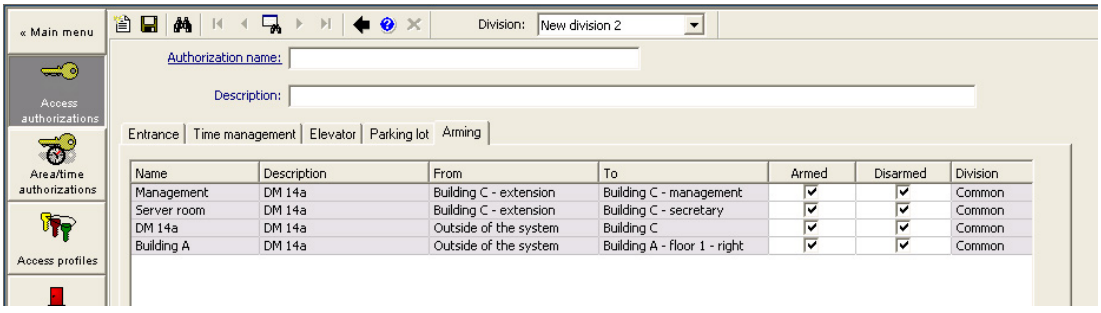


In this case the signals **IDS armed** and **IDS ready to arm** need to be replicated on the inputs of the other entrances. When a second entrance model is created for the same arming area then the device editor does the replication for you. The description of the signal of the second door will be expanded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

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



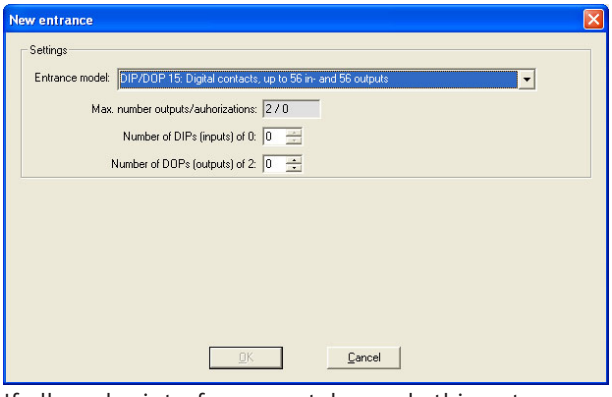
When collating authorizations, all created instances of entrance model 14 are listed on the tab **Arming** of the dialogs **Access authorizations** and **Area/Time Authorizations.** Authorizations for arming and disarming can be assigned separately.



5.4.6.3 DIPs and DOPs - DM 15

Creating Entrance Model 15:

This entrance model offers independent input and output signals.



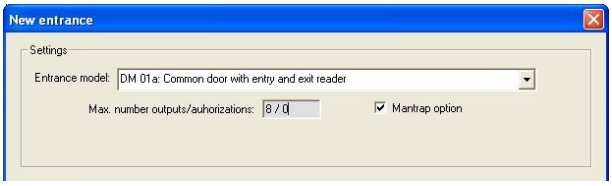
If all reader interfaces are taken only this entrance model becomes available. You can define this entrance model as long as there are at least two signals free.

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

5.4.6.4 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.



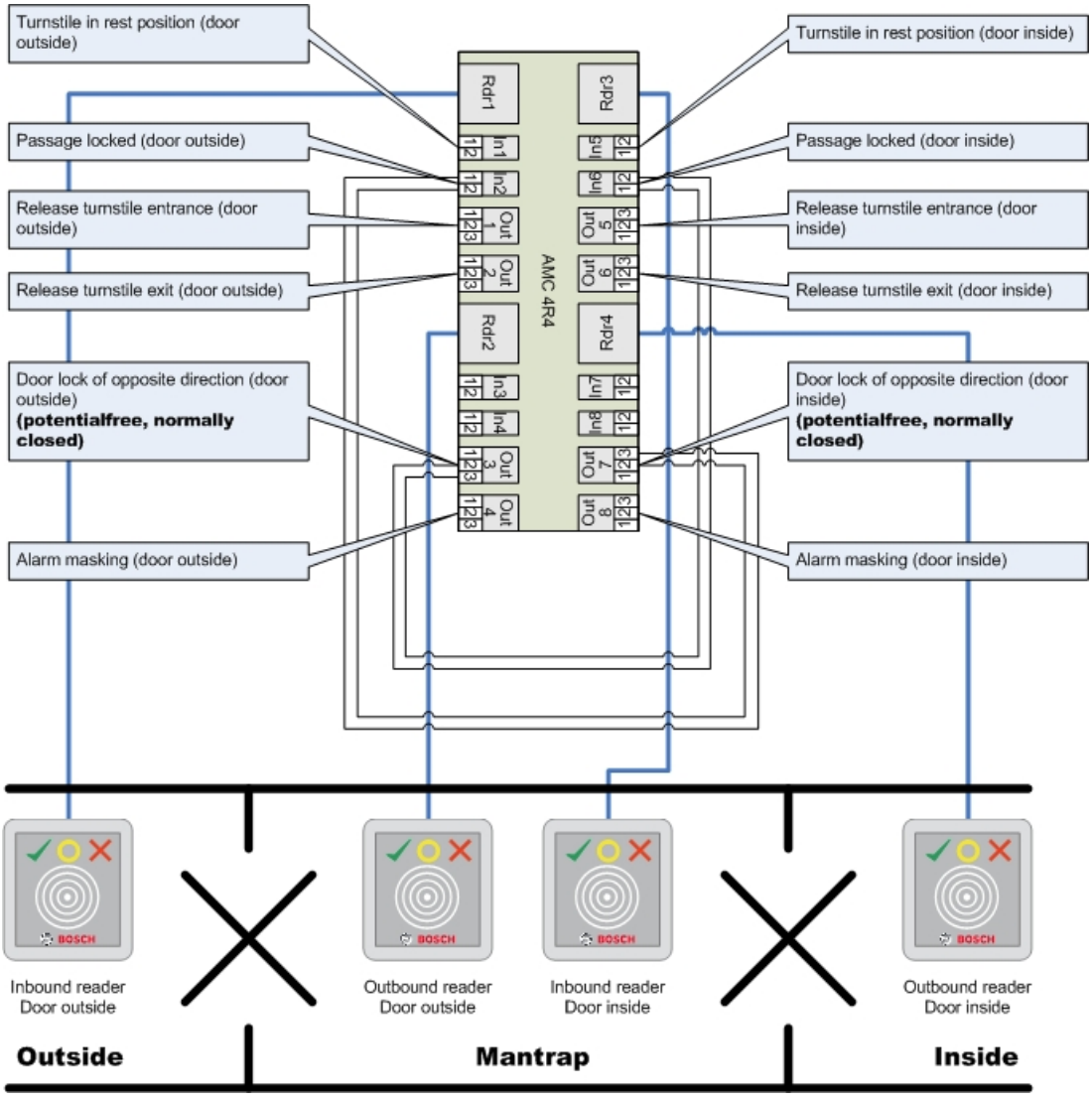
You can combine all model types 01 and 03, but set this option on both entrances belonging to the mantrap.

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).

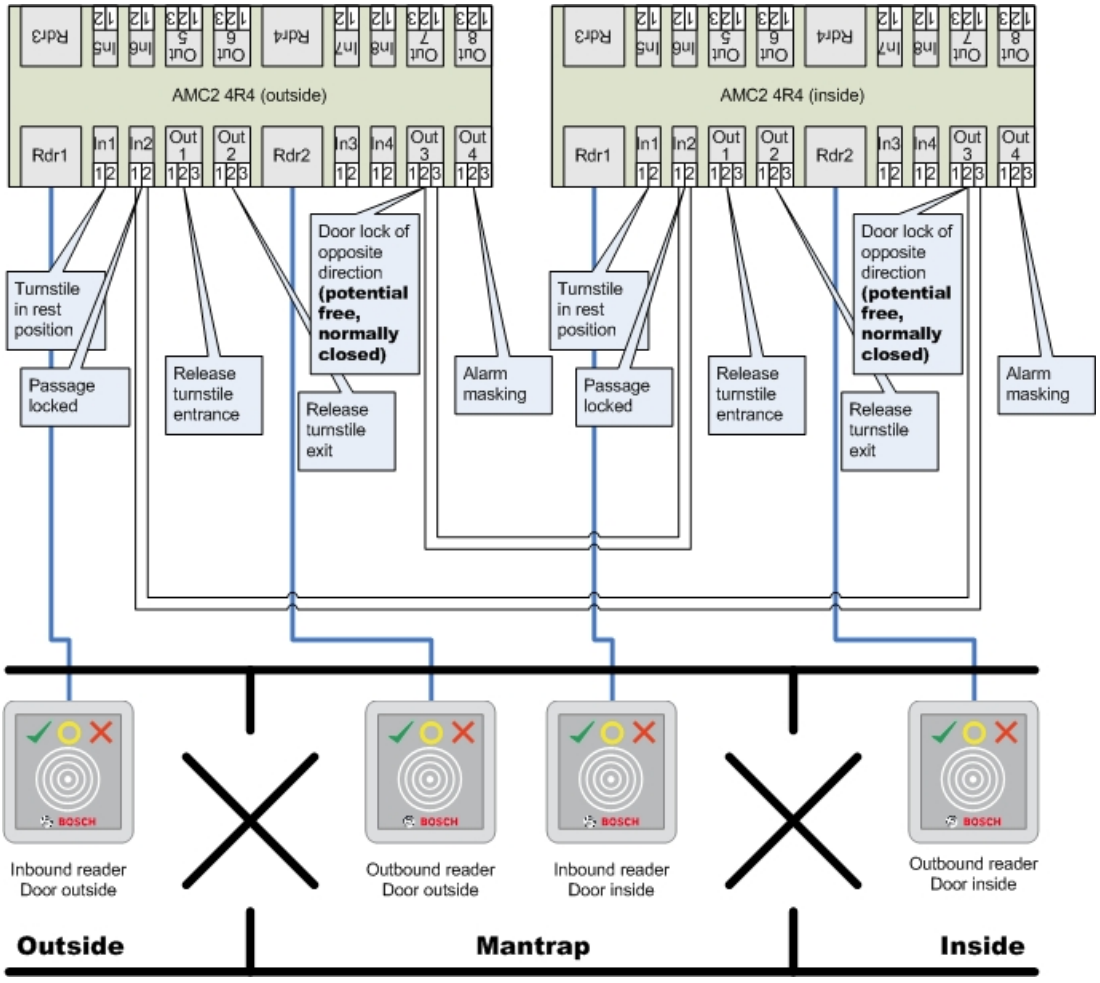
Mantrap configuration with two turnstiles (DM 03a):



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".

5.4.7 Doors

Configuring a Door: General Parameters

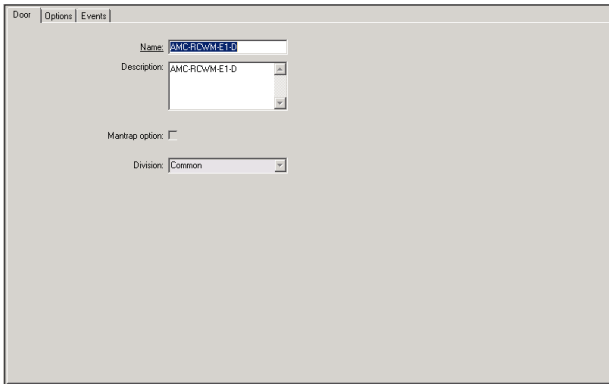
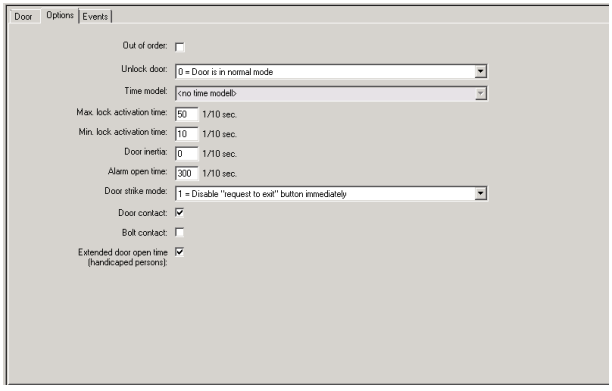


Figure 5.1:

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

Configuring a Door: Options

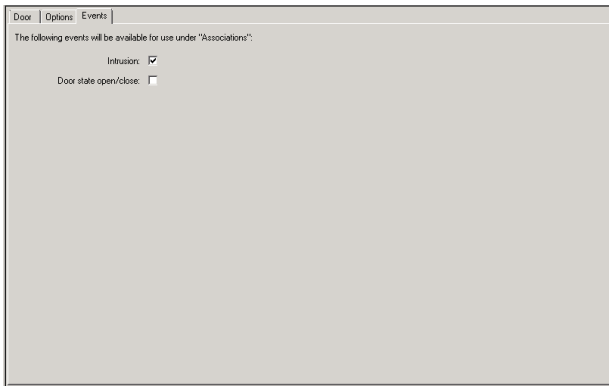


Parameter	Possible values	Remarks
Manual operation	0 = check box is clear 1 = check box is selected.	0 = the door is in normal mode (default), that is, it is subject to access control by the overall system. 1 = door is excluded from the access control system. The door is not controlled and does not generate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

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

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

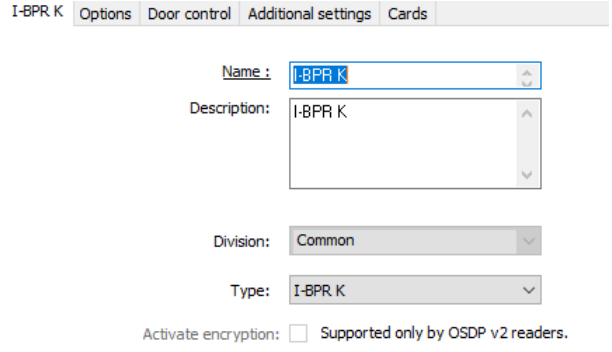
Configuring a Door: Events



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

5.4.8 Readers

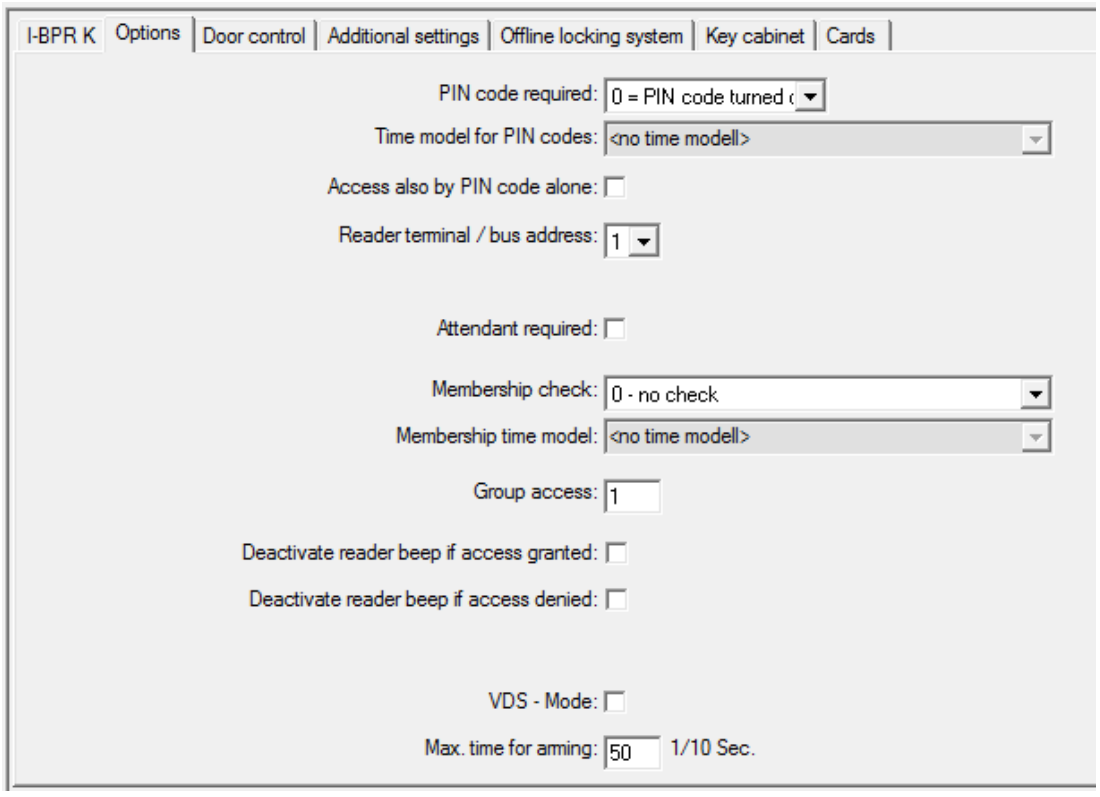
Configuring a Reader: General Parameters



Parameter	Possible Values	Description

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

Configuring a Reader: Options



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 (check box is clear) 1 = activated (check box is selected)	Determines whether this reader can also permit access based on a PIN alone, that is without a card, if the access control system is so configured. See *Access by PIN alone, page 102*
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	**Note** that Membership check only works with card definitions predefined in the system (gray background), not with customized definitions. **0 - no check** Membership check is off, but the card is checked for authorizations as normal (default) **1 - check** The card is checked only for company ID, that is for membership of the system. **2 - depending on time model** The card is checked for company ID (membership) but only during the period defined in the membership time model.
Membership time model	one of the available time models	The time model enables/disables the membership check. The selection of a time model is mandatory for **Membership check** option 2.
Group access	1 - 10	**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. **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.
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.
 The “Deactivate Reader Beep” functions depend on the respective reader firmware. The firmware of some readers may not support this function.		
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.

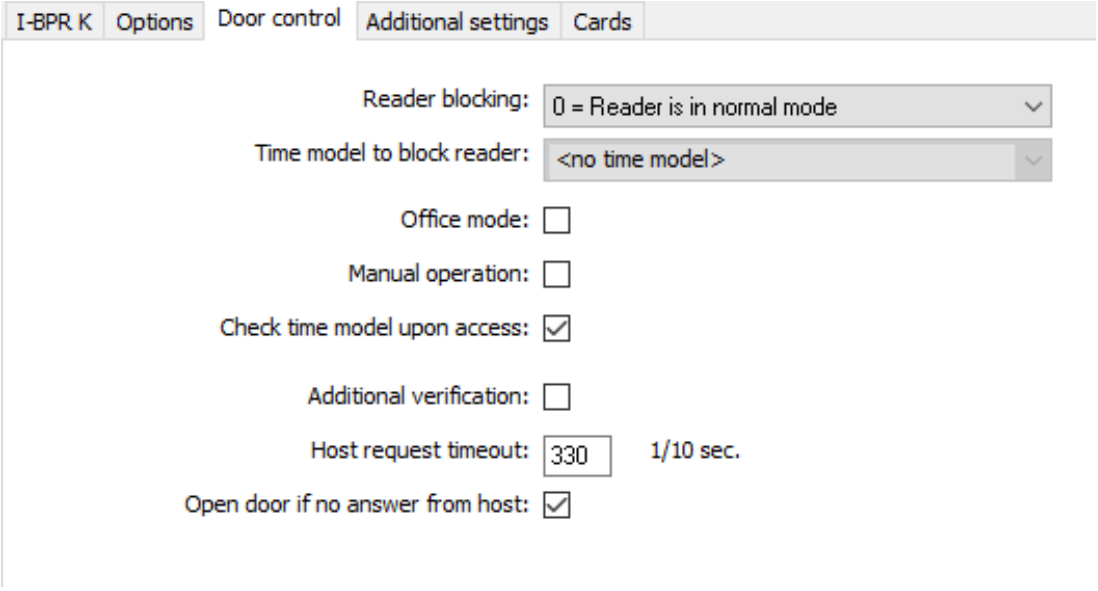
Templates can be stored both on devices above the reader in the device tree, and on the reader itself. Data on the reader is periodically updated by the devices above it.

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.

Parameter	Description
	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: – 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

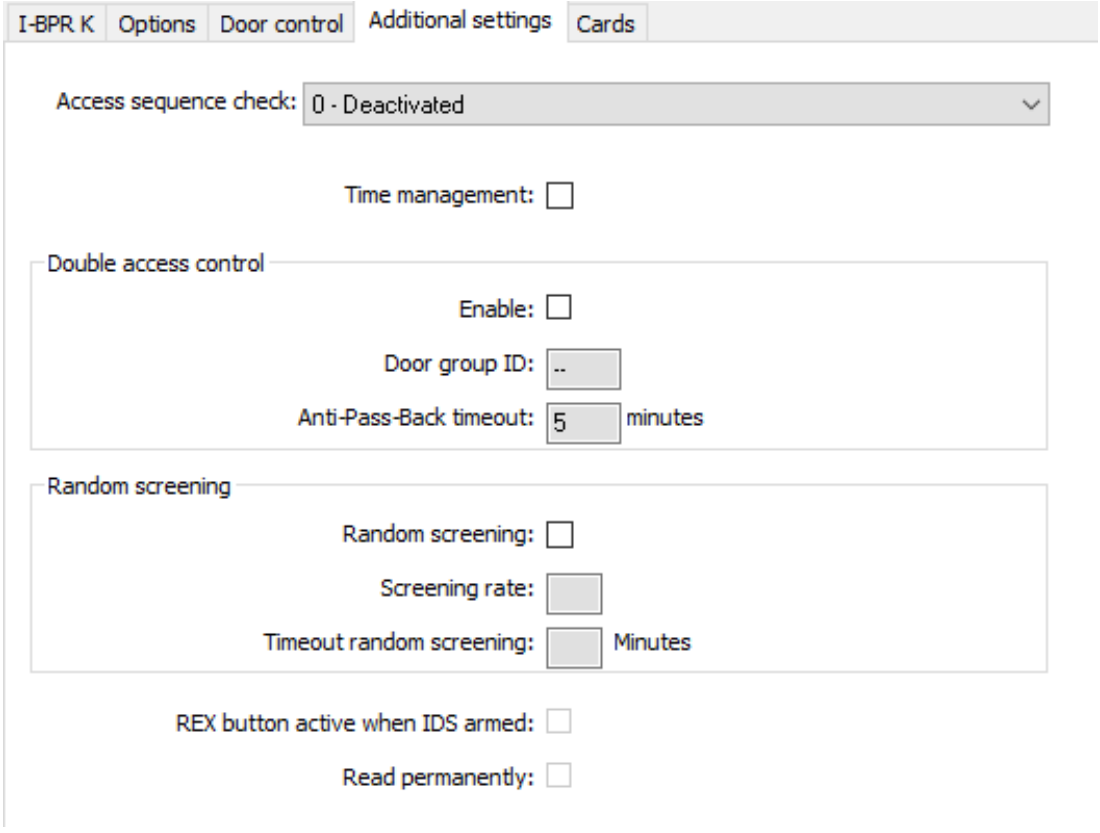


Parameter	Possible values	Remarks
Reader blocking	List box entry	0 = Reader in normal mode - no blockade (= default) 1 = Reader is permanently blocked - permanent blockade

		2 = Reader is blocked depending on time model - blockade according to time model set with *Time model to block reader*
Time model to block reader	one of the time models defined in the system.	Blocks the reader according to the time model selected.
Office mode	0 = deactivated (check box is clear) 1 = activated (check box is selected)	Allows this reader to be used in Office mode ,
Manual operation	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = reader in normal mode (= default) 1 = reader is effectively removed from the access control system, that is “out of order”. No commands are received. All other parameters for this reader are turned off. The parameter must be set independently for both the reader and door.
Check time models upon access	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = Time models will not be checked. There is no time-restriction for access. 1 = If the cardholder has a time model assigned to it, either directly or as an area-time authorization, the time model will be checked. (= default)
Additional verification	0 = deactivated (check box is clear) 1 = activated (check box is selected	0 = host verification is not required 1 = host verification is required (default) (**IMPORTANT**: Activation of this option is required for additional video verification by the operator of a BVMS or BIS system)
Host request timeout	0 = deactivated	0 = AMC works without host verification (does not work with *Area Change* or *Person Countings*). This control is only active if Host verification is deactivated (0) and *Open door if no answer from host* is activated (1) 1 to 9999 = using the reader requires a BIS inquiry. The inquiry has to be answered within the specified time span. If the time expires, the AMC checks the parameter **Open door if no answer from host** and decides for itself. Values are 1/10 of a second. (Default = 30)

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

Configuring a Reader: Additional Settings

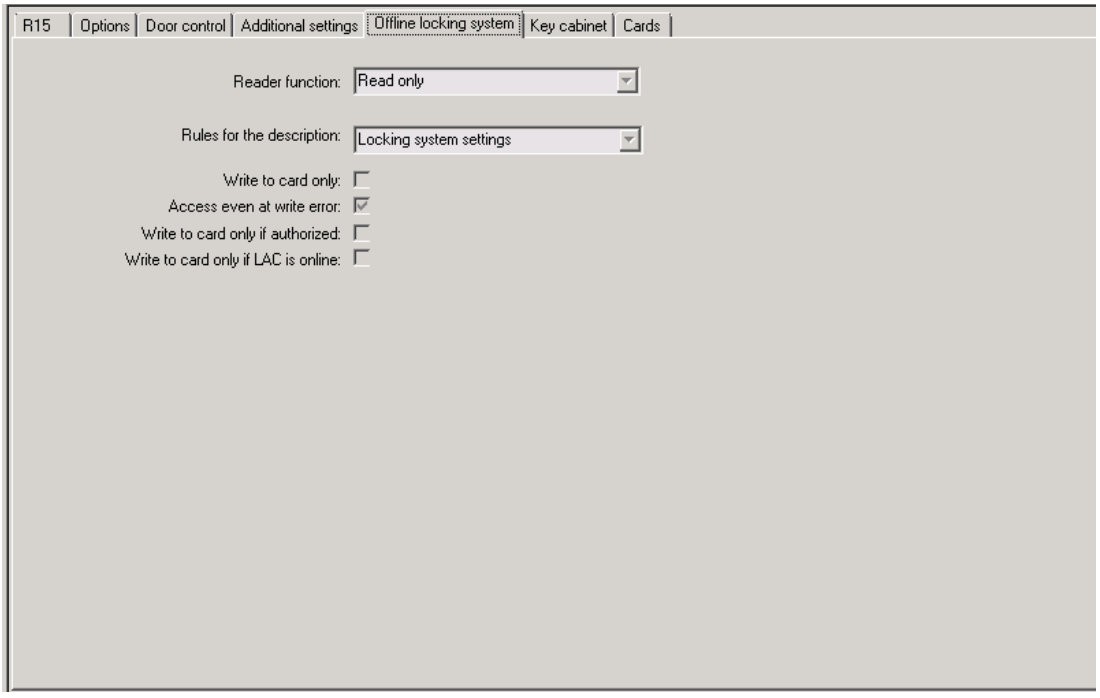


Parameter	Possible values	Remarks
Acess sequence check	0 - Deactivated 1 - Activated; deactivate upon LAC malfunction	0 = reader takes no part in access sequence checking (= default)

	2 - Activated; leave active upon LAC malfunction 3 - Activated; use strict sequence checking even when LAC malfunctions (note: update person's location manually)	An activated sequence check can handle persons who are set UNKNOWN in the following ways: 1 = The first reading of the card will be down without checking the location. All controllers must be online. 2 = The first reading of the card will be down without checking the location. 3 = Checking the location will be down for every reading the card during LAC malfunction.
 In the BIS platform 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. **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 *all* readers.		
Time Management	0 = deactivated (check box is clear) 1 = activated (check box is selected)	In activated (1) the Ace process collects data for the time attendance system.
Double access control (anti-passback control)		
Enable	0 = deactivated (check box is clear) 1 = activated (check box is selected)	0 = without double access control (= default) 1 = with double access control Within the time span set by the **Duration** parameter, this reader and other readers in the group cannot be used with the same card. If this parameter is activated, a door group ID must be used, even if only one reader is used.
Door group ID	Letters A - Z and a - z, and "-" 2 characters	Readers can be grouped using a Door group ID. Presenting a card at one reader will block subsequent bookings at all readers in the door group (Default = **--**) until the time out elapses.

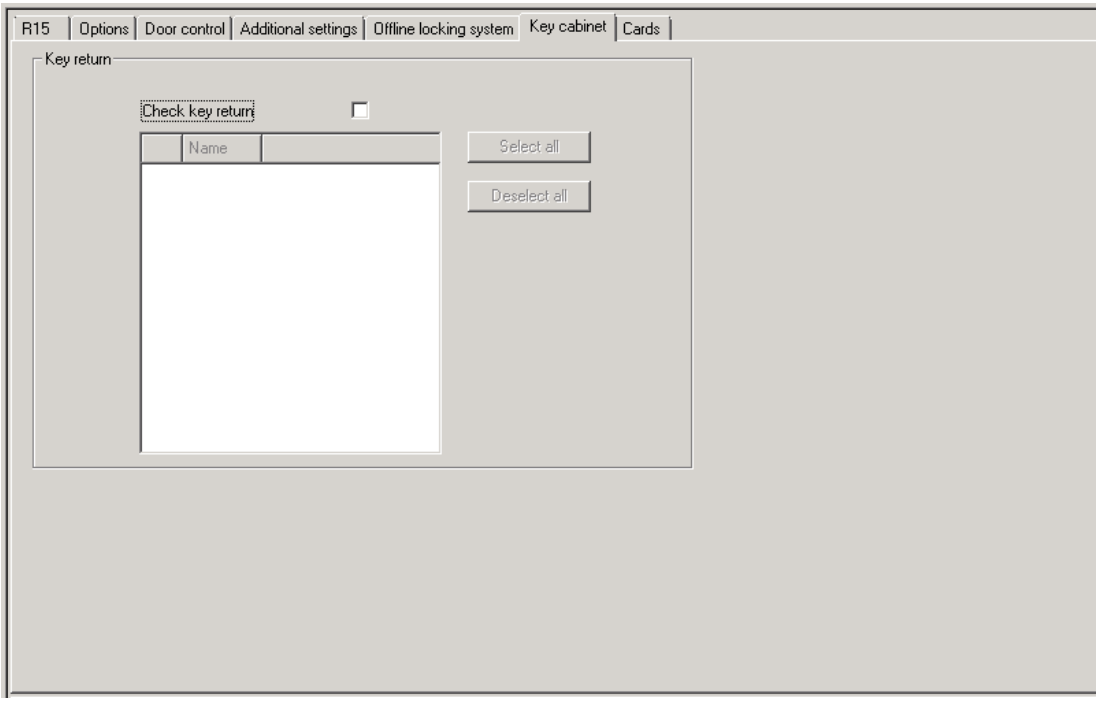
Anti-passback time out	1 - 120	The reader can be used with the same card after this time span has elapsed. As soon as the card is used at a reader outside the group the blockade is lifted immediately. Values are minutes - default = 5.
Random screening	0 = deactivated (check box is clear) 1 = activated (check box is selected	0 = no random screening 1 = random screening according to the factor will have no admittance until unblocked by the dialog **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. This parameter also needs to be set where a reader is used instead of a push button.
Read permanently	0 = deactivated (check box is clear) 1 = activated (check box is selected)	The reader read permanently if the reader has the respective firmware of the manufacturer.

Configuring a Reader: Offline Locking System



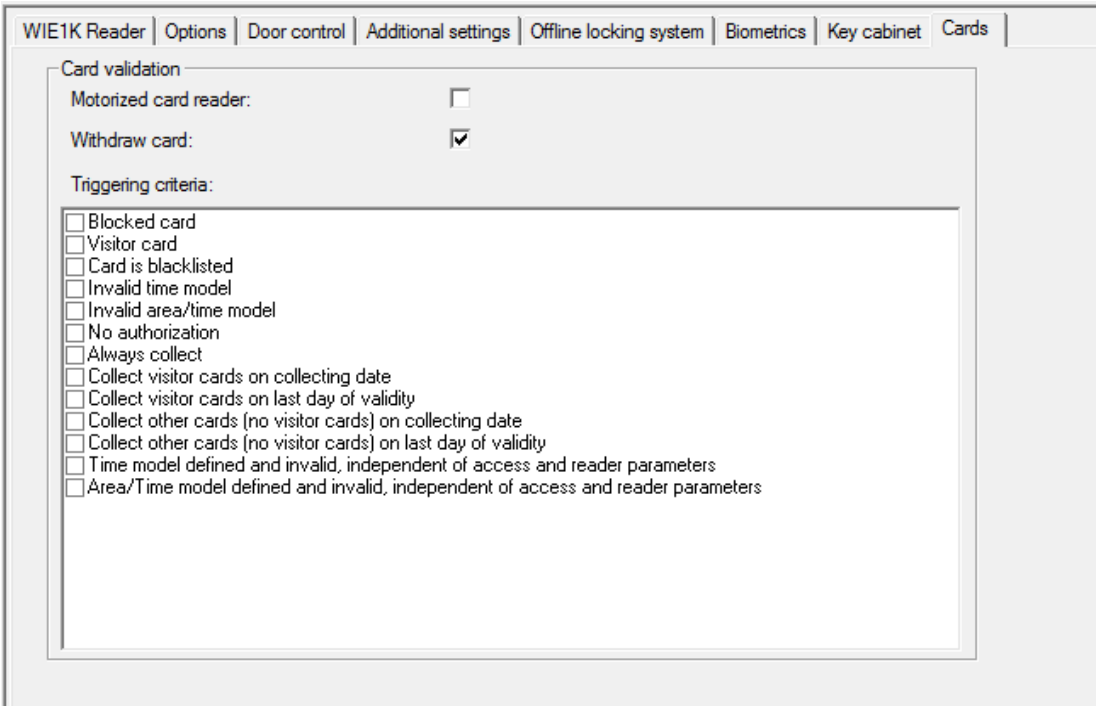
Parameter	Possible values	Remarks
Reader function		This box must be selected if a motorized card reader is used
Rules for the description		“Withdraw” means to make the card invalid.
Write to card only	0 = deactivated (check box is clear) 1 = activated (check box is selected)	
Access even on write error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

See also
– *Access by PIN alone, page 102*

5.4.9 Access by PIN alone

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

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

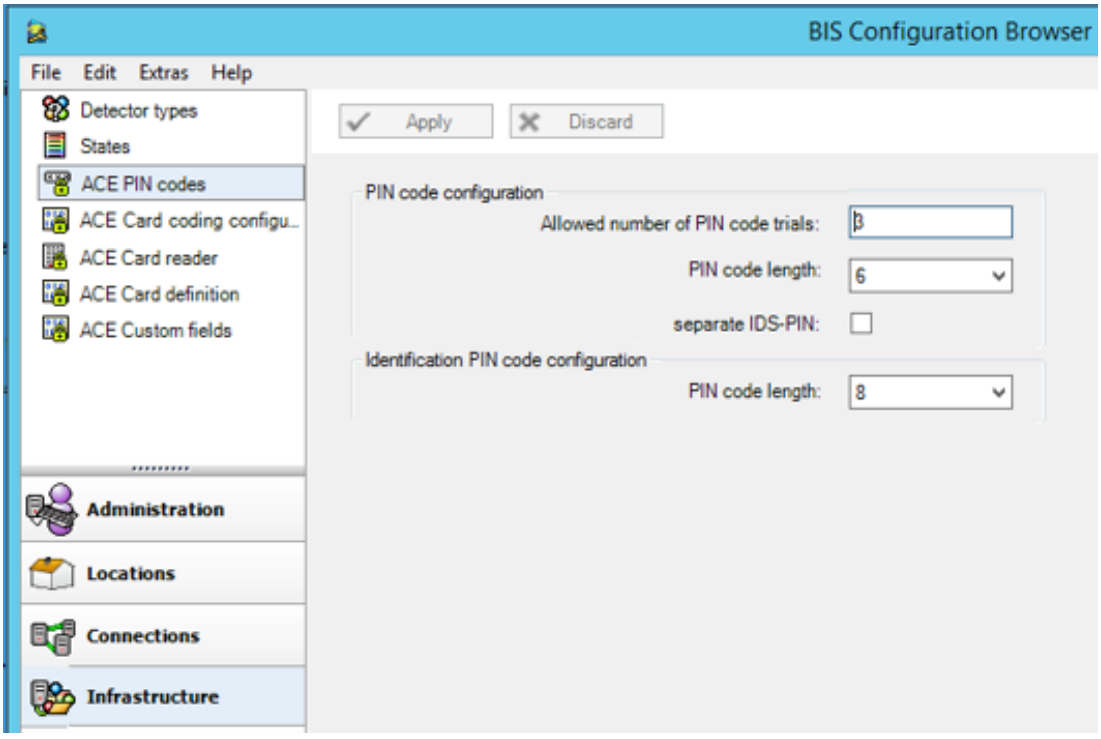
Prerequisite authorization for Operators
Authorization for a cardholder to access by PIN alone is only grantable by operators with the special authorization to assign virtual cards. To give an operator this authorization, proceed as follows.
1. In the BIS Configuration Browser navigate to **Administration > ACE User profiles**

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

Assigning an Identification PIN to a cardholder
See the ACE operation manual online help section: **Permitting access by PIN alone**

Setting the length of the Identification PIN for all 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**



Configuring a reader for access by PIN alone.

1. In the BIS Configuration Browser navigate to **Infrastructure** > **ACE Card reader**.
2. In the **Workstation** pane select the workstation to which the reader is physically connected.
3. Right-click the workstation and add a reader of type **Dialog Enter PIN** or **Dialog Generate PIN**.

4. Select the reader in the **Workstations** pane.
   A custom reader configuration pane appears to the right of the **Workstations** pane.
5. Verify that the drop-down list **Card usage default** contains the default value **Virtual card. Use PIN as card**.
6. Click  or **Apply** to save your changes
7. In the BIS Configuration Browser navigate to **Connections.**
8. Select the reader at the entrance where you wish to configure access by PIN alone.
9. In the **Options** tab, select the check box **Access also by PIN code alone.**
10. Click  or **Apply** to save your changes

5.4.10 Extension board - AMC...EXT

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

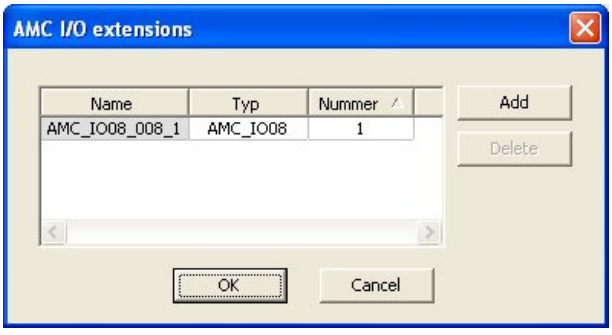
Extension boards provide additional input and output signals, if the eight contacts located on the AMC are not sufficient for the connection of the necessary contacts (for example, with elevators).

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

Notice!

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

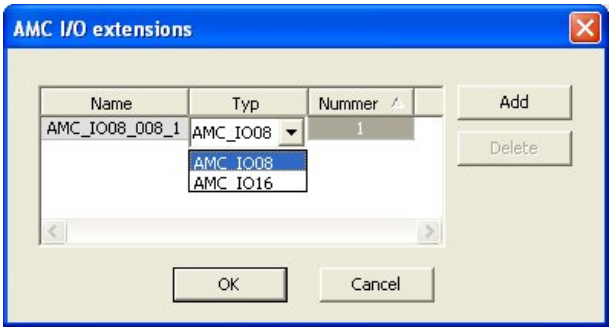
A selection dialog for the creation of the extensions appears.



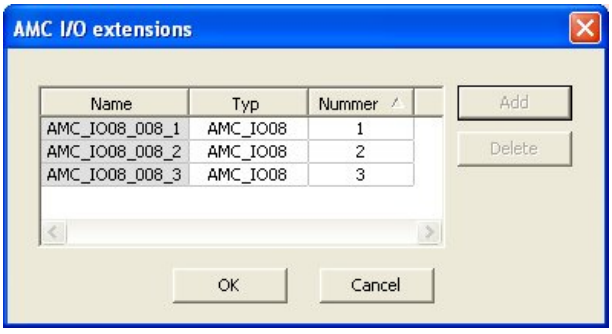
AMC-EXT is available in two variants:

– AMC_IO08: with 8 inputs and 8 outputs
– AMC_IO16: with 16 inputs and 16 outputs
– AMC_4W extension: with 8 inputs and 8 outputs

The selection dialog contains an entry with an AMC_IO08. By double-clicking the list box in the **Type** column, you can also place an AMC_IO16.



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



Extension boards are numbered 1, 2 or 3 as created. The numbering of the signals begins for each board at 01. The signal number In combination with the board number provides a unique identification. The signals of the extension boards can also be seen on the tab of the AMC to which they belong.
Together with the input and output signals on the AMC up to 56 signal pairs can thus be provided.
Extension boards can be added as required individually or at a later date up to the maximum number (3 per AMC).

Creating an AMC2 4W-EXT

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

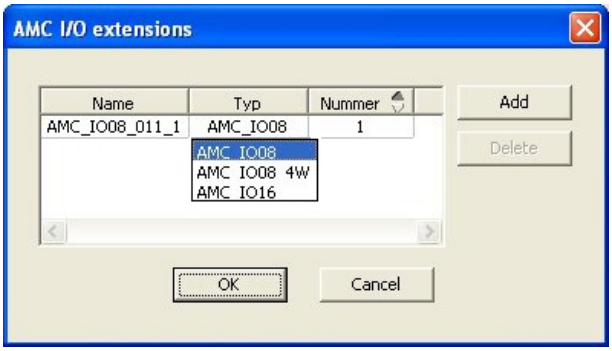
Notice!
The AMC2 4W-EXT can not be used as a standalone controller, but only as an extension to an AMC2-4W.The doors are controlled and the access control decisions are made only by the AMC2 4W.

The AMC2 4W-EXT can only be used in connection with an AMC2 4W. As it only has Wiegand reader interfaces it is not usable with the AMC variant AMC2 4R4.
Like the I/O extension boards (AMC2 8I-8O-EXT and AMC2 16I-16O-EXT) the AMC2 4W-EXT is connected via the extension interface of the AMC2 4W. The extension board has neither memory nor display of its own, but is controlled entirely by the AMC2 4W.

One AMC2 4W-EXT and a maximum of three I/O extensions can be connected to each AMC2-4W.
To create an AMC2 4W-EXT in the system right-click the desired parent AMC2 4W in the Explorer and select **New object** > **New extension board** from the context menu.

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

The same selection dialog appears as for creating I/O extensions, except that the list for an AMC2 4W contains the additional element AMC_IO08_4W.



The list entry AMC2 4W can only be added only once, whereas up to three I/O Extensions can be added.
The button **Add** adds new list entries. In the case of an AMC2 4W the maximum number is 4 whereby the fourth entry is created as an AMC2 4W-EXT board.
Extension boards are numbered according to creation order 1, 2 or 3. The AMC2 4W-EXT receives the number 0 (zero). The numbering of the signals for the AMC2 4W-EXT continues from that of the controller, namely 09 to 16, whereas for each I/O board the numbering begins with 01. The signals for all extension boards are also shown on the tab for the relevant AMC2 4W.
Together with the input and output signals of the AMC2 4W up to 64 signal pairs can be provided.

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

Parameter	Possible values	Description
Board name	Restricted alphanumeric: 1 - 16 digits	The default identification guarantees a unique name, but it can be overridden manually. Please ensure that the ID is unique. Network connections with DHCP servers should use the network name.
Board description	alphanumeric: 0 - 255 digits	This text is displayed in OPC branch.
Board number	1 - 3	Number of the board connected to the AMC. Display field, only.

Power supply	0= deactivated (check box is selected) 1= activated (check box is selected)	Supervision of the supply voltage. With voltage breakdowns a message is generated at the end of a delay. The supervision function assumes the use of a USV, so that a message can be generated. 0 = no supervision 1 = supervision activated
Division	Default value "Common"	This read-only field is only applicable where the Divisions feature is licensed and used.

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

Deleting extension boards

It is only possible to delete an extension board when none of its interfaces is occupied. The associated signals must first be configured on a different board before the delete button  and the context menu option **Delete object** become usable.

AMC2 4W-EXT

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

5.5 Additional Information

5.5.1 Optional additional readers

Optional additional readers at entrances

Door models 01, 03a, 03b, 06a, 14a, 14b can have a maximum of two inbound and two outbound readers.

To configure these additional readers click **Connections** menu, Right-click an AMC controller in the Device Editor and select **New Object** > **New Entrance**

Prerequisites:

- There are enough connections available on the responsible door controller
- The first reader is configured before the second in each direction.

Printing summaries of AMC signals

To print an overview of the signals assigned to an AMC, click **Connections** menu > (Device Editor) > Select an AMC controller > Open its **Terminals** tab and click the **Print** button.

To aid the technician it is usually beneficial to place a printout within the enclosure that houses the AMC.

Configuring anti-passback control

Three parameters influence the behavior of the anti-passback control:

- ANTIPASS: Activation/deactivation of control
- ANTIPGRP: Marking of readers establishing the blockade, whenever a reader of this group is used

– ANTIPTIME: Wait time, until a reader from this group can be used again

Default setting for ANTIPASS is 5 minutes.

If reader parameter ANTIPTIME is set to "0", this reader takes no part in the control.

If ANTIPASS = "1", the following is valid for ANTIPGRP:

– ANTIPGRP = "--": This reader takes part in the anti-passbackcontrol and terminates a blockade.
– ANTIPGRP = "AA": This reader takes part in the anti-passbackcontrol and initiates a blockade. Whenever within ANTIPTIME the card is read at a reader from the same group, the persons gets no access.

An example shows what consequences different group settings have:

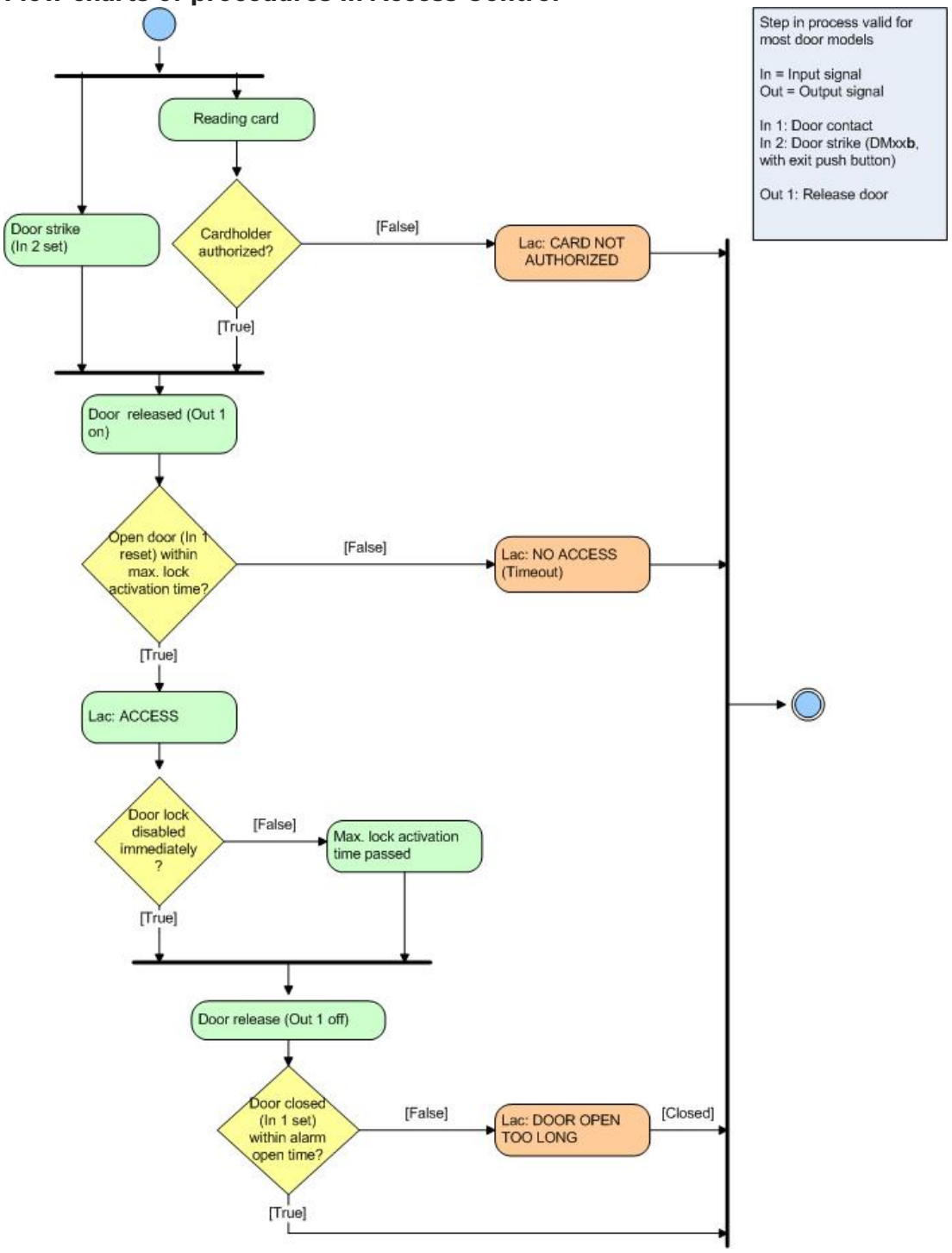
Assume a room with

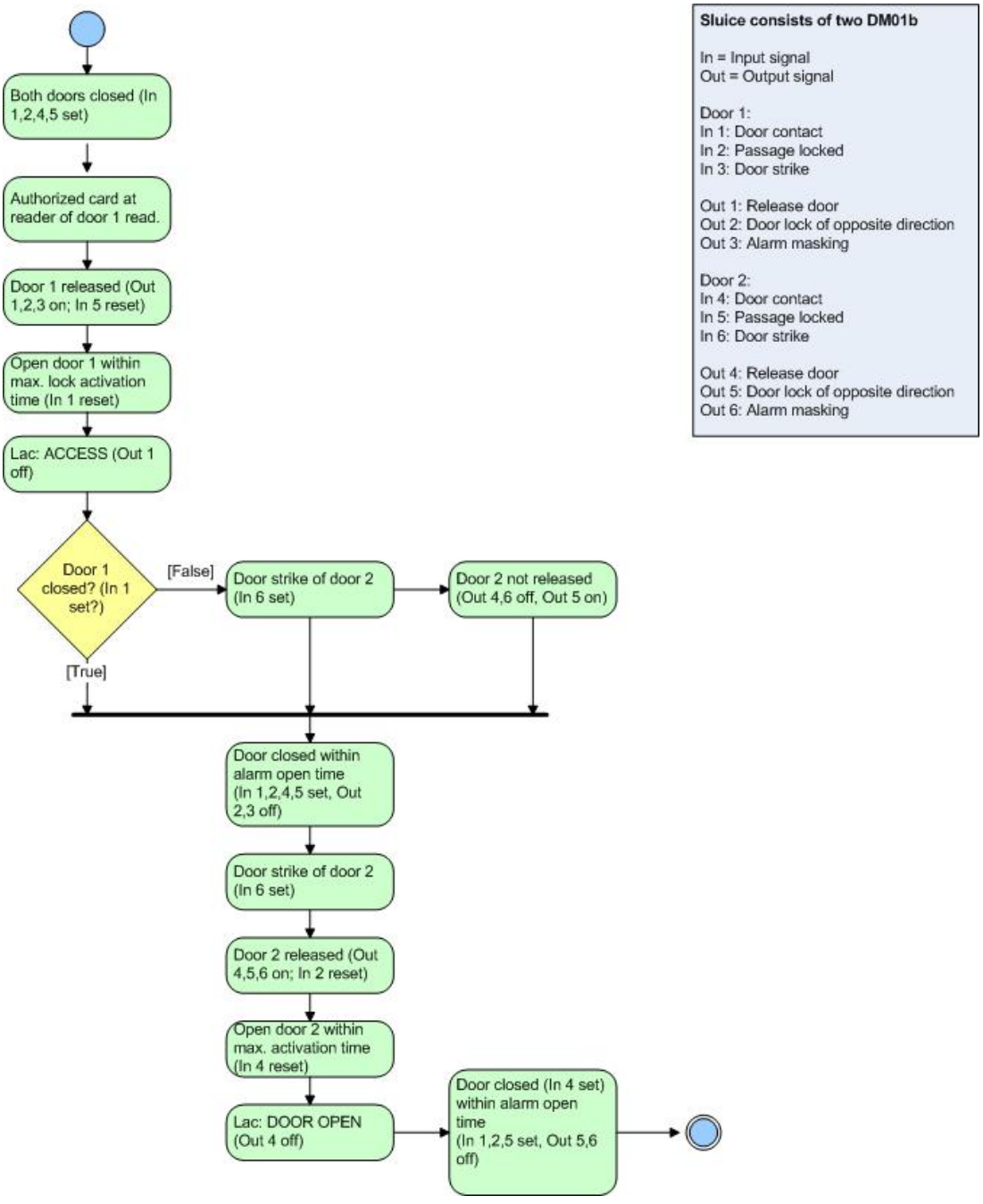
– door model 01a
– an entrance reader = "RDR-E"
– an outgoing reader = "RDR-A"
– ANTIPASS = 1
– ANTIPTIME = 5

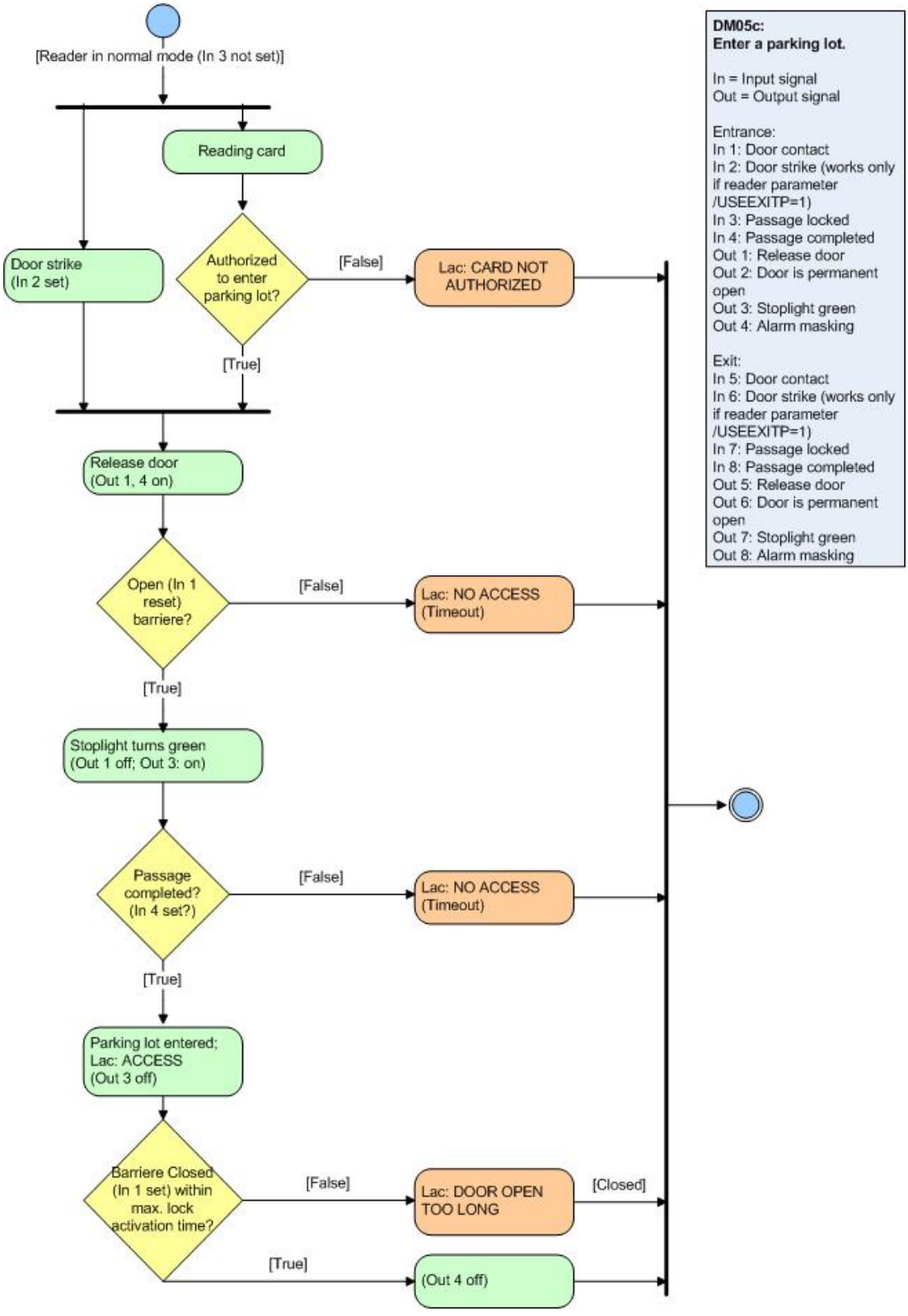
The following settings are possible through variations of ANTIPGRP:

– RDR-E: ANTIPGRP = "AA"; RDR-A: ANTIPGRP = "AA"
  Upon entering the room, the anti-passback control is activated with 5 minutes. If within this time the entrance or outgoing reader reads the card, the access is denied, because both readers have the same group ID. Therefore this combination is not useful.
– RDR-E: ANTIPGRP = "AA"; RDR-A: ANTIPGRP = "--"
  Upon entering the room the anti-passback control is activated with 5 minutes. Because the outgoing reader is configured as "deletion reader", access is granted after reading the card. Simultaneously, the blockade is deleted. Further bookings are possible at the entrance reader. Note that there will be no new blockade established at the outgoing reader. For example, the card can be presented multiple times at the outgoing reader. As a consequence, double bookings are only possible at the outgoing reader.
– RDR-E: ANTIPGRP = "AA"; RDR-A: ANTIPGRP = "AB"
  Upon entering the room, the anti-passback control is activated with 5 minutes. Because the outgoing reader belongs to another group, access is granted. The blockade of the "AA" group is terminated, so that the card can be offered again immediately at the entrance reader. For the "AB" group, a blockade is established. This combination makes sense, if a blockade is intended in the exit direction. Double readings are not possible at the entrance nor at the outgoing reader. Only the sequence entrance reader - outgoing reader - entrance reader - outgoing reader works.
– RDR-E: ANTIPGRP = "AA"; RDR-A: ANTIPGRP = ""(no data)
  Upon entering the room, the anti-passback control is activated with 5 minutes. Because the outgoing reader belongs to no group and is not a "deletion reader", ANTIPTIME is not reset. The blockade of the entrance reader will continue for the time set even if the outgoing reader gets a reading.

5.5.2 Flow charts of procedures in Access Control




Sluice consists of two DM01b
In = Input signal
Out = Output signal
Door 1:
In 1: Door contact
In 2: Passage locked
In 3: Door strike
Out 1: Release door
Out 2: Door lock of opposite direction
Out 3: Alarm masking
Door 2:
In 4: Door contact
In 5: Passage locked
In 6: Door strike
Out 4: Release door
Out 5: Door lock of opposite direction
Out 6: Alarm masking
Both doors closed (In 1,2,4,5 set)
Authorized card at reader of door 1 read.
Door 1 released (Out 1,2,3 on; In 5 reset)
Open door 1 within max. lock activation time (In 1 reset)
Lac: ACCESS (Out 1 off)
Door 1 closed? (In 1 set?)
[False]
Door strike of door 2 (In 6 set)
Door 2 not released (Out 4,6 off, Out 5 on)
[True]
Door closed within alarm open time (In 1,2,4,5 set, Out 2,3 off)
Door strike of door 2 (In 6 set)
Door 2 released (Out 4,5,6 on; In 2 reset)
Open door 2 within max. activation time (In 4 reset)
Lac: DOOR OPEN (Out 4 off)
Door closed (In 4 set) within alarm open time (In 1,2,5 set, Out 5,6 off)


[Reader in normal mode (In 3 not set)]
Reading card
Door strike (In 2 set)
Authorized to enter parking lot?
[False]
Lac: CARD NOT AUTHORIZED
[True]
Release door (Out 1, 4 on)
Open (In 1 reset) barriere?
[False]
Lac: NO ACCESS (Timeout)
[True]
Stoplight turns green (Out 1 off; Out 3: on)
Passage completed? (In 4 set?)
[False]
Lac: NO ACCESS (Timeout)
[True]
Parking lot entered; Lac: ACCESS (Out 3 off)
Barriere Closed (In 1 set) within max. lock activation time?
[False]
Lac: DOOR OPEN TOO LONG
[Closed]
[True]
(Out 4 off)
DM05c:
Enter a parking lot.
In = Input signal
Out = Output signal
Entrance:
In 1: Door contact
In 2: Door strike (works only if reader parameter /USEEXITP=1)
In 3: Passage locked
In 4: Passage completed
Out 1: Release door
Out 2: Door is permanent open
Out 3: Stoplight green
Out 4: Alarm masking
Exit:
In 5: Door contact
In 6: Door strike (works only if reader parameter /USEEXITP=1)
In 7: Passage locked
In 8: Passage completed
Out 5: Release door
Out 6: Door is permanent open
Out 7: Stoplight green
Out 8: Alarm masking

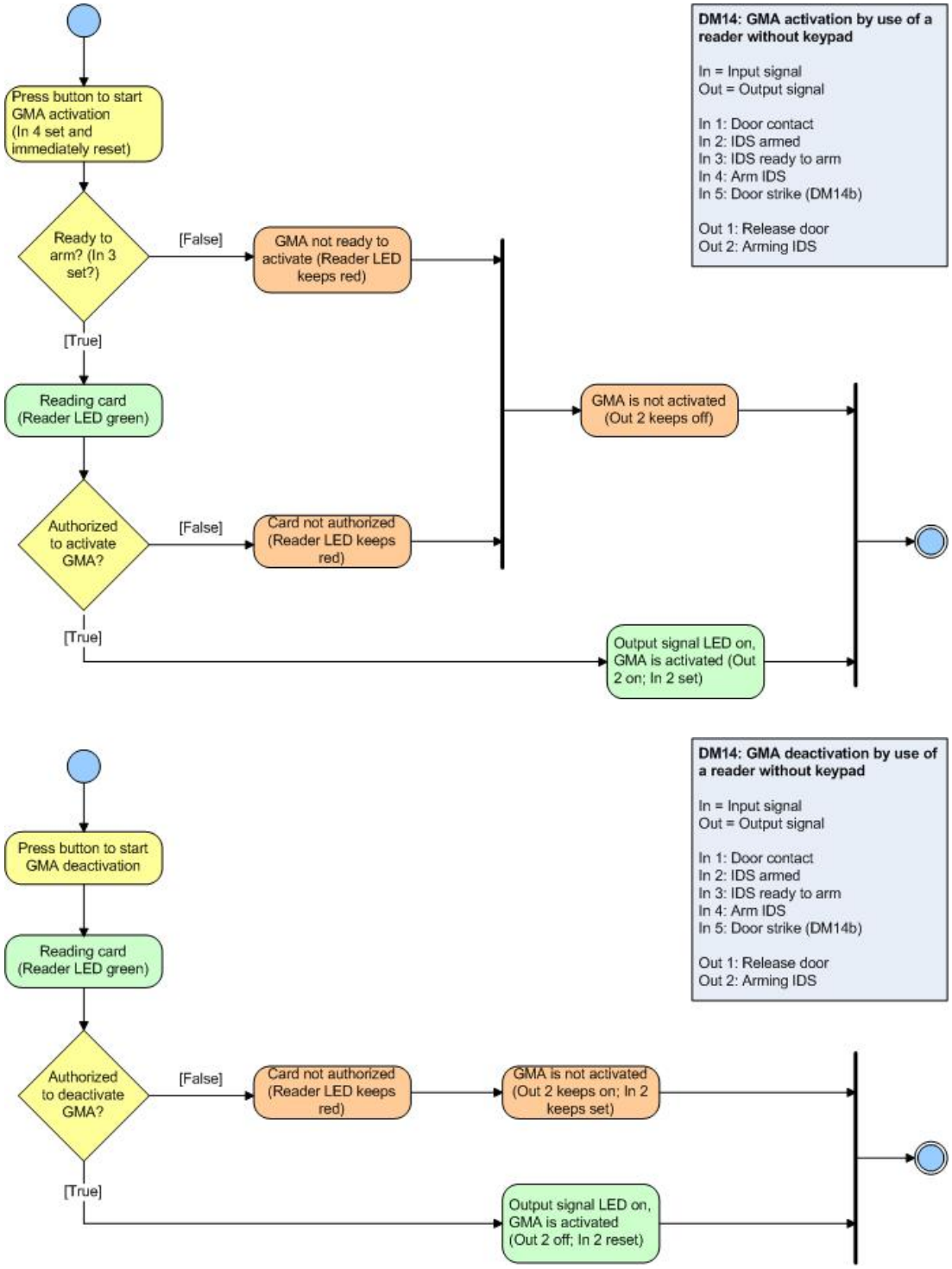
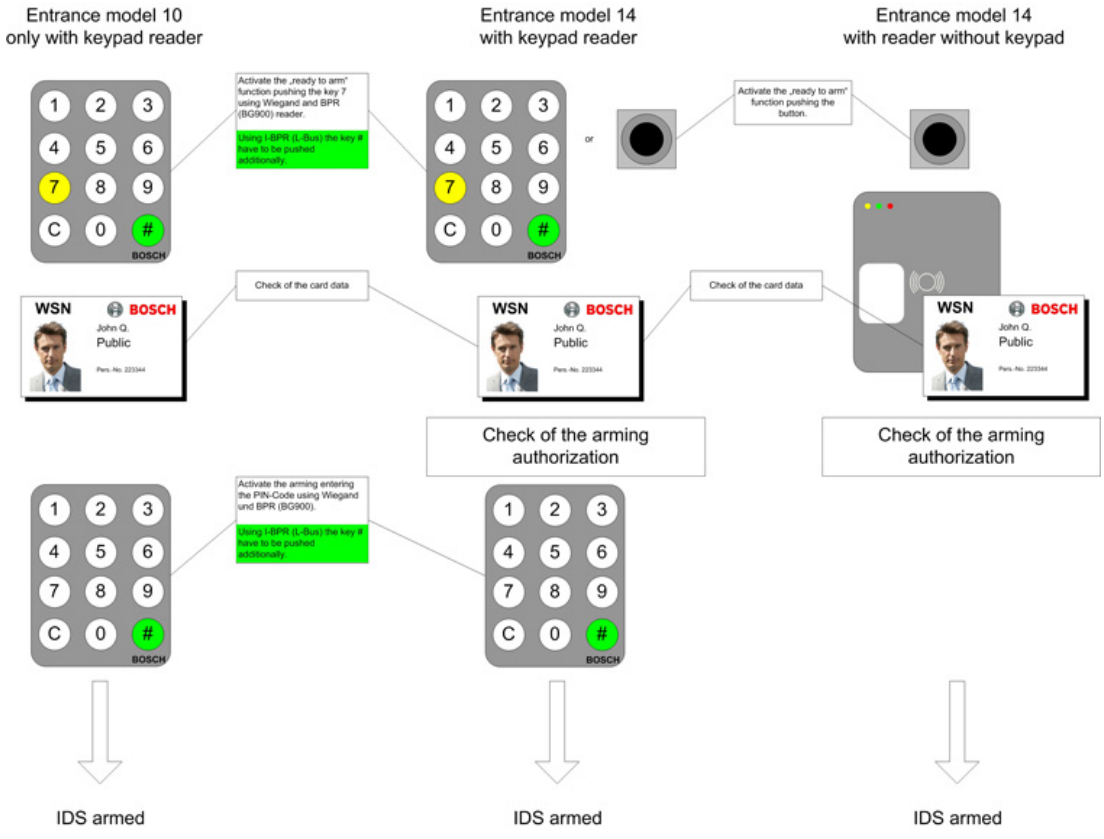
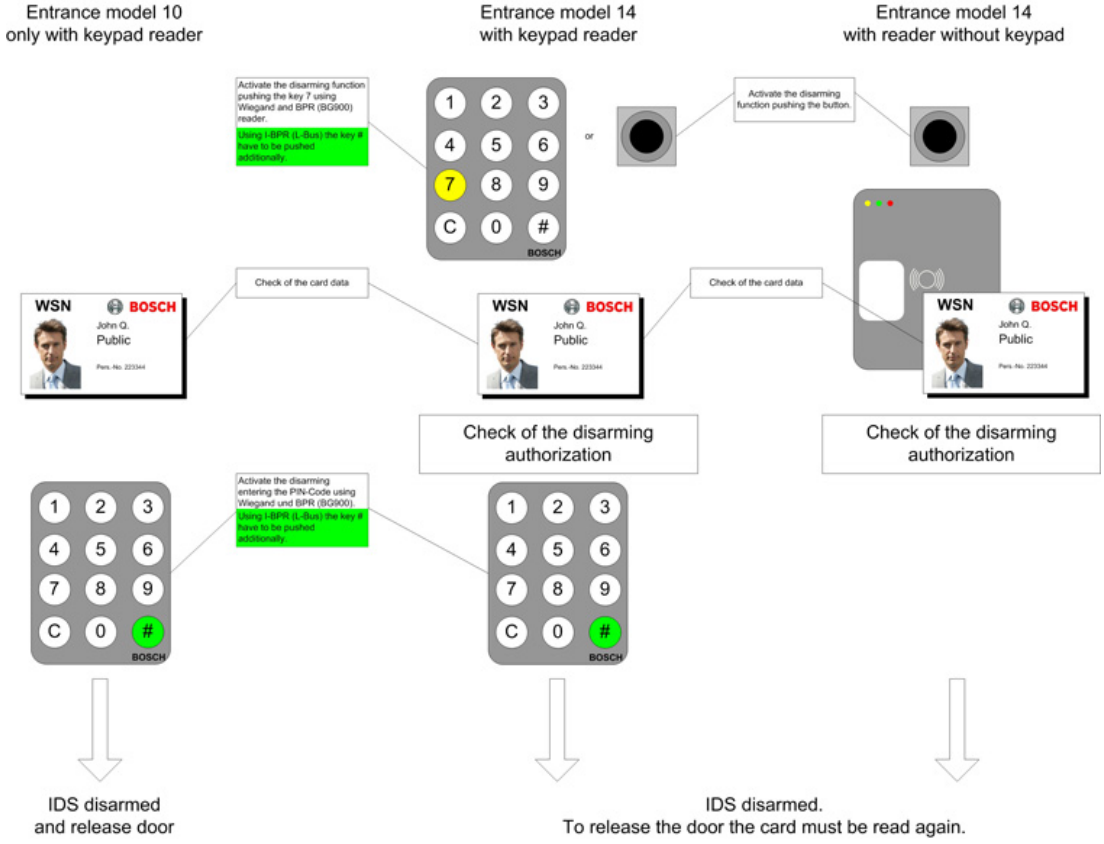


Diagram: Arming / Disarming


Entrance model 10
only with keypad reader
Entrance model 14
with keypad reader
Entrance model 14
with reader without keypad
Activate the „ready to arm" function pushing the key 7 using Wiegand and BPR (BG900) reader.
Using I-BPR (L-Bus) the key # have to be pushed additionally.
Activate the „ready to arm" function pushing the button.
or
Check of the card data
Check of the arming authorization
Check of the arming authorization
Activate the arming entering the PIN-Code using Wiegand und BPR (BG900).
IDS armed
IDS armed
IDS armed


Entrance model 10
only with keypad reader
Entrance model 14
with keypad reader
Entrance model 14
with reader without keypad
Activate the disarming function pushing the key 7 using Wiegand and BPR (BG900) reader.
Using I-BPR (L-Bus) the key # have to be pushed additionally.
Activate the disarming function pushing the button.
or
Check of the card data
Check of the disarming authorization
Check of the disarming authorization
Activate the disarming entering the PIN-Code using Wiegand und BPR (BG900).
IDS disarmed
and release door
IDS disarmed.
To release the door the card must be read again.

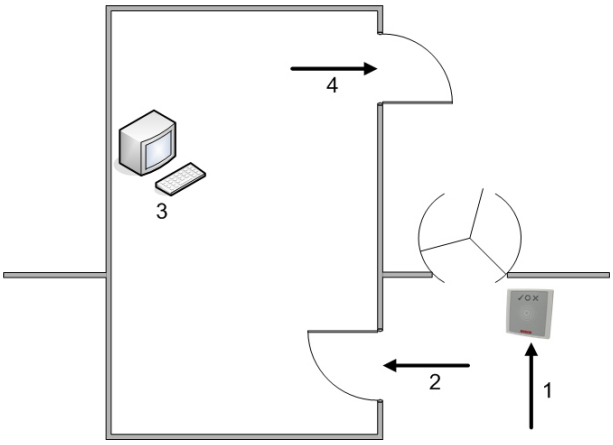
5.5.3 Configuring Random screening

Introduction to random screening

The **random screening** option is used to select for additional security checks random persons entering or leaving a site. Upon presenting their card at a suitably configured door the selected person's record receives a block for the whole system. The event recorded in the event log. The person is denied access through all doors, and invited to proceed instead to security personnel.

After performing the additional checks the security personnel uses the ACE GUI to manually remove the block from the person's record.

The random screening process



1. Cardholder presents card; Random screening places a system-wide block on the cardholder's record.
2. Cardholder is diverted to security booth
3. Cardholder undergoes additional security checks. ACE Operator removes the block from the cardholder's record. See , *page 116*
4. Cardholder leaves the security booth, bypassing the original reader

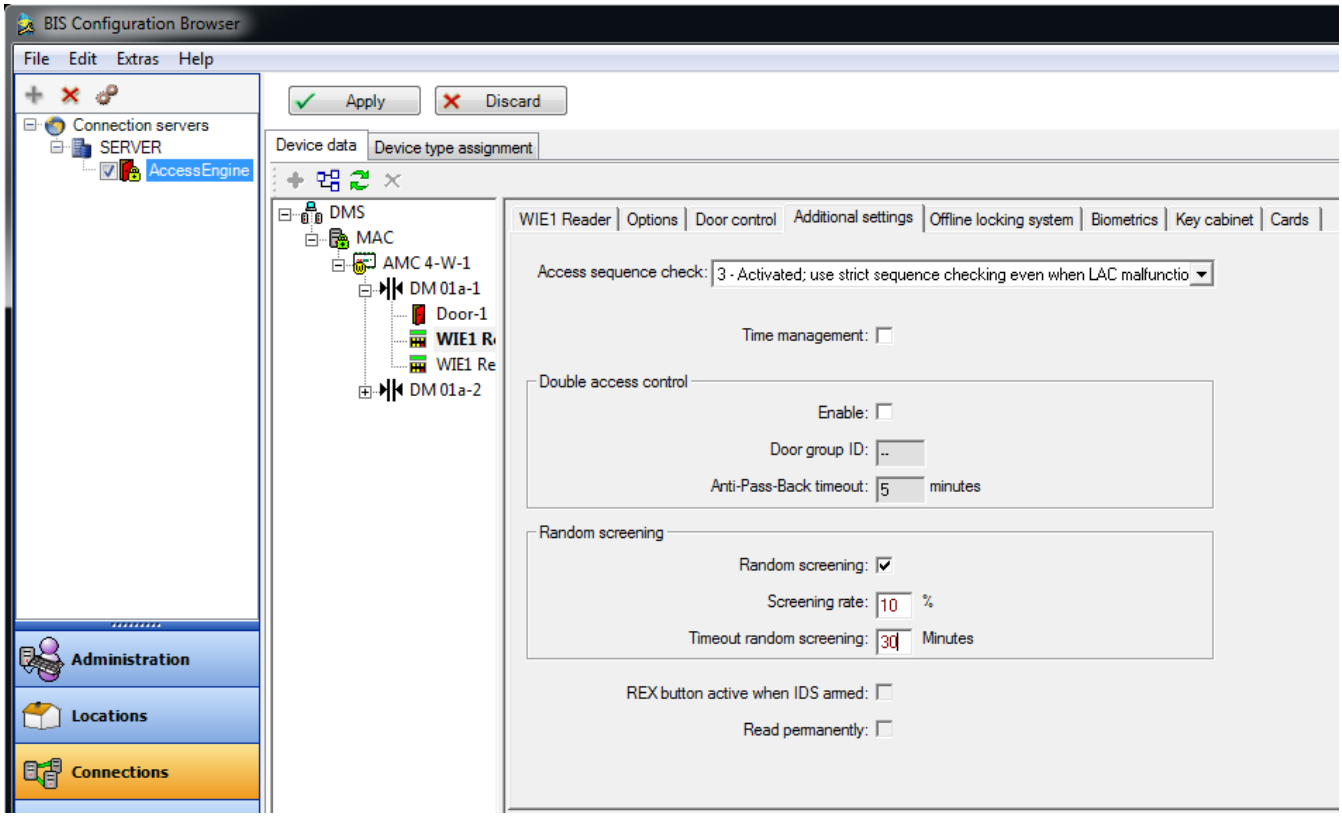
Prerequisites for random screening

- 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 denied access, and will not be included in the random selection process.
- Only persons that have not been exempted from screening can be randomly selected. Exemption is configured in the ACE application > **Cards** dialog > **Other data** tab > check box **Excluded from random screening**
- The entrance should be of mantrap or turnstile type to prevent one person’s "tailgating" another without presenting their own ID.
- A card reader must be present for the relevant direction of passage.
- Random screening is configured for each reader separately.
- Only an operator with the necessary permission in their profile can configure random screening for a reader.
  - Configuration Browser > **Administration** > **ACE User profiles**
- There should be an ACE workstation in the immediate vicinity for removing any blocks placed by the system on persons' records.

Configuring random screening for a reader

To configure a reader for random screening proceed as follows:

1. In the Device Editor, DevEdit select a reader at the door where random screening is to take place. Select the **Additional settings** tab.



2. Select the **Random screening** check-box.
3. In the **Screening rate** field, enter the percentage of persons to be selected for screening.
4. Optionally enter a number of minutes in the field. **Timeout random screening**.
   After a randomly selected person has been denied access, and their record blocked, the system waits for this number of minutes before automatically removing the block. There is no need in this case for security personnel to remove the block from the person's record manually.
   Note: if the field remains empty, or contains the value 0, then there is **no time limit** for the block, and it must be removed manually by security personnel.
5. Save your settings.

Switching random screening on and off in the BIS client Device Overview

Prerequisite

Random screening has been configured in the device editor, DevEdit

Procedure

– Right click a reader in the Device Overview and select
  – **Random screening on**
    or
  – **Random screening off**

Note: The **Screening rate** and **Timeout** parameters are automatically read from the configuration, and **not** requested by pop-up dialog. Thus it is essential to configure the reader in DevEdit beforehand.

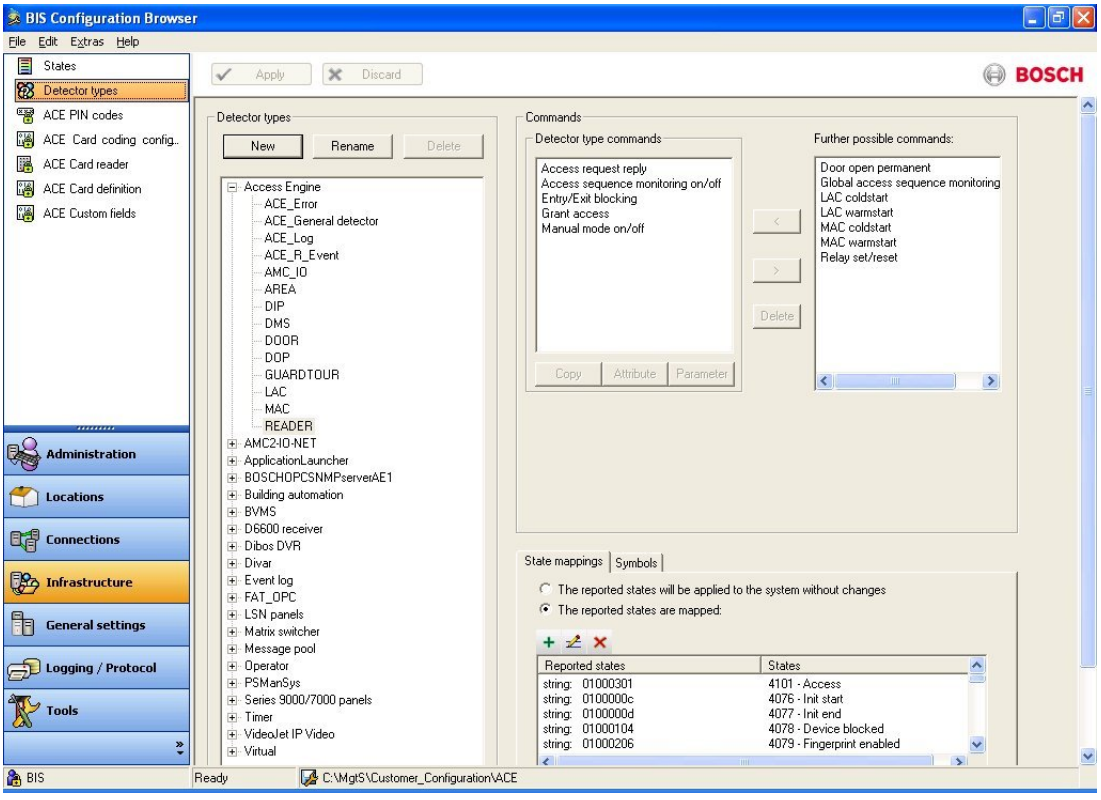
Notice!
In ACE and AMS clients the screening rates of readers can be adjusted from the following dialog:
Main menu > System data > Random screening

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

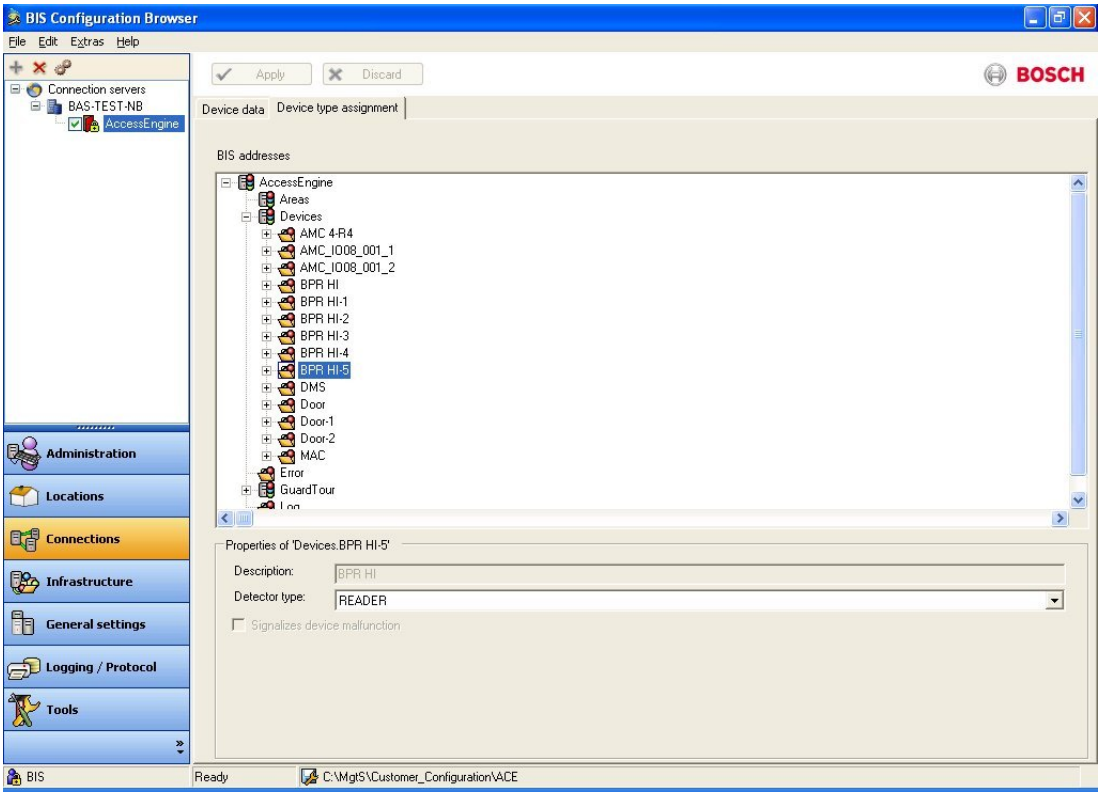
Removing blocks placed by random screening
The ACE operator deletes the block in the Access Engine client as follows:
1. Navigate to Main menu > **Blocking**
2. Enter the name of the person who has been blocked, to display their record
3. In the **Blocking** pane of the **Blocking** dialog, select the current random screening block from the list.
4. Click the **Delete** button.
5. Confirm the deletion

5.6 Assigning detector types

In the dialog detector types (Infrastructure menu) all BIS installed devices can be configured as regards their statuses, data transmissions and the commands they will accept from the user interface.
When Access Engine is installed a number of detector types are created which can be modified, deleted or added to as required.
For further details please consult the online help for that dialog.



In Access Engine there is a special detector type for every device. Whenever a controller or entrance is created in the device data editor (DevEdit) the corresponding detector type is automatically assigned. The mapping can be seen on the additional tab **Device Type Assignment** in the device editor.



If certain devices require other detector types, e.g. with a bigger command set, then the new detector type can be defined using the detector types dialog and later assigned to that specific device. In this way the default assignments of detector types can be customized and overridden. The changes made here will persist for future use in the device data editor.

5.7 Hierarchical cardholder management

Overview and benefits

In large multi-server systems it may be beneficial to allow lower level ACE servers some degree of autonomy in the creation of cardholders and devices. They can then continue to create cardholder and device data if connection to the top-level server, that is the server with the main database, is temporarily lost.

When the connection is reestablished, **cardholder data** that was created at lower levels is normally merged with the cardholder data from the top-level server.

Device data temporarily created at lower levels in the hierarchy is normally overwritten by data from the top-level server.

Introduction to the ACE Hierarchy Tool

The ACE Hierarchy Tool in the directory <installation drive>:\MgtS\AccessEngine\AC\bin is a tool for the following tasks:

- Defining the role of the server on which it is executed. The role can be
  - top-level server (Level 3)
  - mid-level server (Level 2)

  - bottom-level server (Level1)
- Defining the **Type of data transfer**, that is how the data created at lower levels should be handled when connection to the top-level server is reestablished. There are the following possibilities:
  - The lower-level data is merged with the higher-level data. This is the default type for replication from top-level server to mid-level server .
  - The lower-level data is deleted and overwritten by data from higher levels. This is the default type for replication from mid-level server to bottom-level server .
- Defining the **Data to be transferred**, that is whether only the access control data (cardholder data) is replicated down the hierarchy, or both access control data and device-dependent data together.
  - **Only access control data.** This is the default value for replication from top-level server **to** mid-level server
  - **Access control and device data.** This is the default value for replication from mid-level server **to** bottom-level server

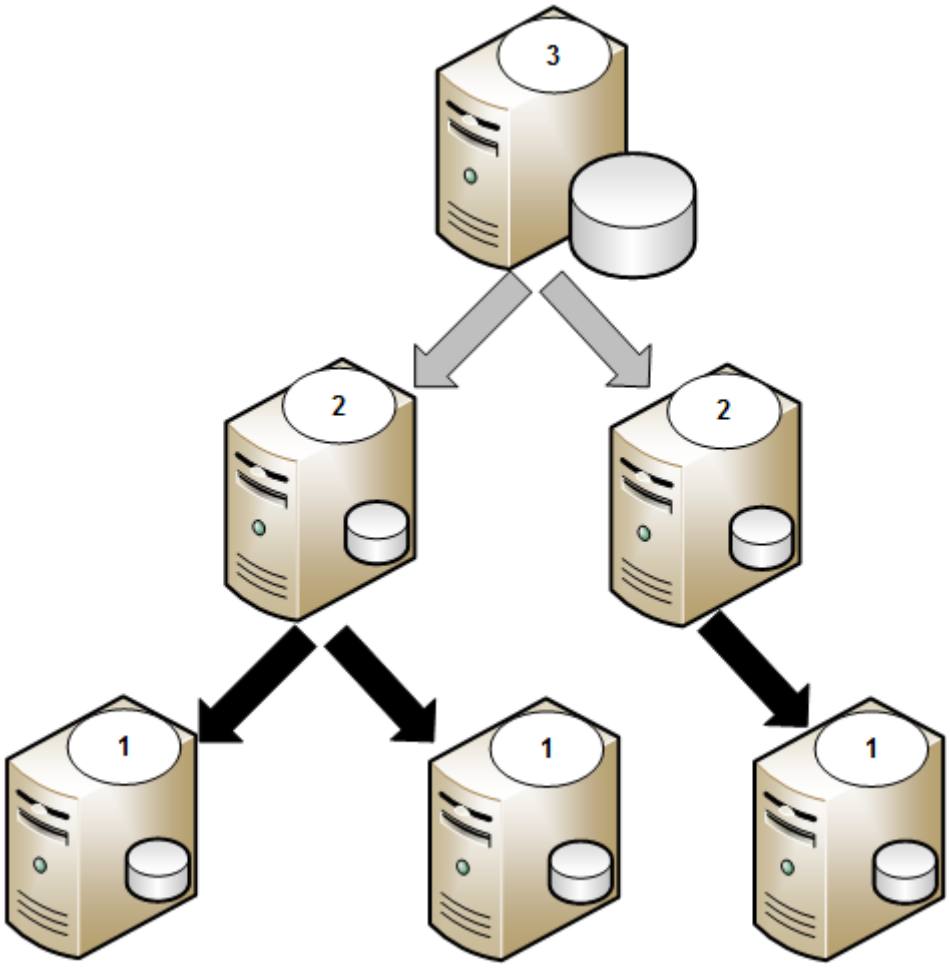
See below for a detailed description of the categories of data for replication, that is, which data are access control data, and which are device-dependent data.

Categories of data for replication

Access control data (cardholder data) are the following. These data are always replicated down the hierarchy.
- Companies
- Person classes
- Persons
- Cards
- Visitors
- Blocks on Persons, including all that person’s cards.
- Authorizations for personnel and visitors
- Active Wiegand card definitions
- Authorization profiles, including their assignments to personnel and/or visitors.
- Time models including Special Days
  Note that time models, including special days, must be created and maintained only on the top-level server

Device dependent data are the following. These are usually replicated only from mid-level server to bottom-level server
- Assignments of readers to Authorizations
- Workstations including Authorizations and Profiles
- ACE Areas including named places and parking-lot data
- Guard tours
- Access sequence control

The following diagram illustrates a simple ACE server hierarchy.



3	top-level server. (Level 3) This server carries the master cardholder database. Time-model data for the hierarchy resides only here.
2	mid-level server (Level 2) This server is a child of the layer above and parent of the layer below. Cardholder data is inherited from above, but can also be created here and propagated downward..
1	bottom-level server (Level 1 also child server of 2).
Parent	A server that passes data down the hierarchy. Parents can be either level 3 or level 2
Child	A server that receives data from further up the hierarchy. Children can be either level 1 or level 2
Gray arrows	Replication of access control data (cardholder data) alone.
Black arrows	Replication of access control data (cardholder data) and device data together.

Defining a hierarchy: order of work

The ACE Hierarchy Tool affects only the server on which it is started. In order to build up a hierarchy of ACE servers it is necessary to log on to each machine in turn and locally register it as a member of the hierarchy.

When you register a child server you are always required to specify its parent server. During the registration process all ancestor servers, from which this child server is to receive data, need to be accessible over the network for data consistency checks and assignment of unique IDs.
For this reason hierarchies are built in a top-down manner. Always start with the top-level server and progress downwards.

Modifying a server that is already in a hierarchy
To modify the attributes of a server, that is one or more of:
– The server's **Parent server**
– The server's **Type of data transfer**
– The **Data to be transferred**
...you will need to first delete the server from the hierarchy, and then re-register it.

See also
– *Deleting a server from the hierarchy, page 123*

5.7.1 Launching the ACE Hierarchy Tool

You must use a Windows account with Administrator privileges to run the ACE Hierarchy Tool . To launch the tool, double-click on its executable file HierarchyTool.exe in the folder <installation drive>:\MgtS\AccessEngine\AC\bin

5.7.2 Registering the top-level server

Prerequisites for registering a top-level server
– BIS with ACE is not just installed but up and running on the server.
– No BIS client is running on the server.
– All participating servers are running exactly the same version of BIS.
– The currently loaded configuration is up to date. There are no unsaved modifications pending.
– If you launch the tool on the top-level server you require only the username and password of a BIS operator on the local machine.

The ACE database of this machine thereby becomes the main database for the entire hierarchy. Changes made in this database will be propagated to all child servers and their descendants.

Procedure for registering a top-level server
1. Log on to an administrator account on the intended top-level server
2. Start the hierarchy tool executable from <installation drive>:\MgtS\AccessEngine\AC\bin
3. At the logon prompt window enter the username and password of a local BIS user with BIS administrator privileges
   Result: The hierarchy tool verifies the authorizations of the BIS username you have entered.
   – If not verified, an error message will appear.
   – If verified, the screen **Select the function of this computer** appears.
4. In the pull-down list **Function**, select **Top level server.**
5. Click the **Next** button
6. The tool prompts for confirmation that the local Access Engine will be stopped, and the MACs cold-booted.

- Click **No** to abort the procedure.
- Click **Yes** to continue. Status messages describe the restart of Access Engine.

7. Finally a summary screen shows the state of the hierarchy. At the moment it contains only the name of the top-level server.
8. Click the **Exit** button.

5.7.3 Registering a mid-level server

Prerequisites for registering a mid-level server

- BIS with ACE is not just installed but up and running on the server.
- No BIS client is running on the server.
- All participating servers are running exactly the same version of BIS.
- The currently loaded configuration is up to date. There are no unsaved modifications pending.
- If you launch the ACE Hierarchy Tool on any server that is NOT the top-level server you will require
  - The username and password of a BIS operator on your local node.
  - The username and password of a BIS operator on your local node's parent server. A child server server can have only one parent server.

The registration process

When a non-top-level server is added to the hierarchy, the ACE Hierarchy Tool needs to climb up the hierarchy to register the child with the top-level server . Data is transferred down from the top-level server differently, according to whether you are adding a mid-level server or a bottom-level server .

Notice!
MACs, DMSs and other necessary services on the local node will be stopped and restarted ("cold started") in the order required to maintain data-consistency throughout the hierarchy. Depending on the number of dependent door controllers there may be a considerable delay until they have received fresh data, and are able to process access requests again.

Procedure for registering a mid-level server

1. Log on to an administrator account on the intended mid-level server server.
2. Start the hierarchy tool executable from <installation drive>:\MgtS\AccessEngine\AC\bin
3. At the logon prompt window enter the username and password of a local BIS user with BIS administrator privileges
   Result: The hierarchy tool verifies the authorizations of the BIS username you have entered.
   - If not verified, an error message will appear.
   - If verified, the screen **Select the function of this computer** appears.
4. In the pull-down list **Function**, select mid-level server **.**
5. Click the **Next** button.
   Result: The **Select parent server** screen appears.
6. Enter the name of the parent server, and the username and password of BIS user with BIS administrator privileges on the parent server.

7. Click the **Test connection** button to verify that the parent server +is accessible on the network.
   Result: The hierarchy tool verifies the network connection and the authorizations of the BIS username you have entered. Both conditions must be fulfilled for the **Next** button to become active.
8. Click the **Next** button.
9. The tool prompts for confirmation that the local Access Engine will be stopped, and the MACs cold-booted.
   – Click **No** to abort the procedure.
   – Click **Yes** to continue. Status messages describe the restart of Access Engine and the registering of the local system with its parent server .
10. Finally a summary screen shows the state of the hierarchy, with the server you have added and its parent server. Note that the tool makes the following default selections:
    – **Type of data transfer:** Merge data from parent and local server
    – **Data to be transferred:** Only the access control data (persons, cards, authorization profiles)
11. Click the **Exit** button.
12. In the BIS Configuration Browser click **Connections** > **AccessEngine** > <name of each MAC> and verify that the check box **Active** is selected on the property page after their "cold start". If not, select these check boxes now.
    – If the ACE synchronization popup appears at this point, click **Yes**.

See also

– *Introduction to the ACE Hierarchy Tool , page 117*

5.7.4 Registering a bottom-level server

Prerequisites for registering a bottom-level server

– BIS with ACE is not just installed but up and running on the server.
– No BIS client is running on the server.
– All participating servers are running exactly the same version of BIS.
– The currently loaded configuration is up to date. There are no unsaved modifications pending.
– If you launch the ACE Hierarchy Tool on any server that is NOT the top-level server you will require
  – The username and password of a BIS operator on your local node.
  – The username and password of a BIS operator on your local node's parent server. A child server server can have only one parent server.

The registration process

When a non-top-level server is added to the hierarchy, the ACE Hierarchy Tool needs to climb up the hierarchy to register the child with the top-level server . Data is transferred down from the top-level server differently, according to whether you are adding a mid-level server or a bottom-level server .

Notice!
MACs, DMSs and other necessary services on the local node will be stopped and restarted ("cold started") in the order required to maintain data-consistency throughout the hierarchy. Depending on the number of dependent door controllers there may be a considerable delay until they have received fresh data, and are able to process access requests again.

Procedure for registering a bottom-level server

1. Log on to an administrator account on the intended bottom-level server .
2. Start the hierarchy tool executable from <installation drive>:\MgtS\AccessEngine\AC\bin
3. At the logon prompt window enter the username and password of a local BIS user with BIS administrator privileges
   Result: The hierarchy tool verifies the authorizations of the BIS username you have entered.
   – If not verified, an error message will appear.
   – If verified, the screen **Select the function of this computer** appears.
4. In the pull-down list **Function**, select bottom-level server
5. Click the **Next** button.
   Result: The **Select parent server** screen appears.
6. Enter the name of the parent server, and the username and password of BIS user with BIS administrator privileges on the parent server.
7. Click the **Test connection** button to verify that the parent is accessible on the network.
   Result: The hierarchy tool verifies the network connection and the authorizations of the BIS username you have entered. Both conditions must be fulfilled for the **Next** button to become active.
8. Click the **Next** button.
9. The tool prompts for confirmation that the local Access Engine will be stopped, and the MACs cold-booted.
   – Click **No** to abort the procedure.
   – Click **Yes** to continue. Status messages describe the restart of Access Engine and the registering of the local system with its parent server .
10. Finally a summary screen shows the state of the hierarchy, with the server you have added and its parent server. Note that the tool makes the following default selections:
    – **Type of data transfer:** Allow only data from the parent server
    – **Data to be transferred:** Access control and device data
11. Click the **Exit** button.
12. In the BIS Configuration Browser click **Connections** > **AccessEngine** > <name of each MAC> and verify that the check box **Active** is selected on the property page after their "cold start". If not, select these check boxes now.
    – If the ACE synchronization popup appears at this point, click **Yes**.

5.7.5 Deleting a server from the hierarchy

The deletion process and its consequences

If you delete a child server, it is deleted from the databases of its parent server and of the top-level server.

Deleting a server from the hierarchy does **not** delete the database entries that the server created and propagated while it was a member.

Notice!
There is no way to delete an entire hierarchy in one session.
The hierarchy must be deleted **bottom-up** by running the ACE Hierarchy Tool on each server in turn, and deleting it.

Procedure for deleting a server from the hierarchy

1. Log on to the server that you want to delete from the hierarchy.
2. Start the hierarchy tool executable from <installation drive>:\MgtS\AccessEngine\AC\bin
3. At the logon prompt window enter the username and password of a local BIS user with administrator privileges
4. Result: The main window of the ACE Hierarchy Tool appears
5. Select the server in the **System hierarchy** pane of the main window
6. Click the **Delete** button
7. Confirm the deletion in the popup window.
8. Result: The server disappears from the **System hierarchy** pane of the main window
9. Click the **Exit** button

5.7.6 Modifying a server in the hierarchy

To modify the attributes of a server, that is one or more of:

– The server's **Parent server**
– The server's **Type of data transfer**
– The **Data to be transferred**

...you will need to first delete the server from the hierarchy, and then re-register it.

See also

– *Deleting a server from the hierarchy, page 123*
– *Registering a mid-level server, page 121*
– *Registering the top-level server, page 120*

5.7.7 Starting and stopping replicators in BIS

Introduction to replicators

A replicator is a computer process that reads or writes data between ACE servers, according to the settings for **Type of data transfer** and **Data to be transferred** for each server.

– A top-level ACE server has one write-replicator process for each of its children.
– A bottom level ACE server has one read-replicator process for its one parent.
– A Level 2 ACE server has both of the above kinds of replicator, one for its parent and one for each of its children.

After the server hierarchy is configured, the ACE database table contains the following hierarchy data:

– The servers
– The replicator processes
– The replicators' status: stopped/running

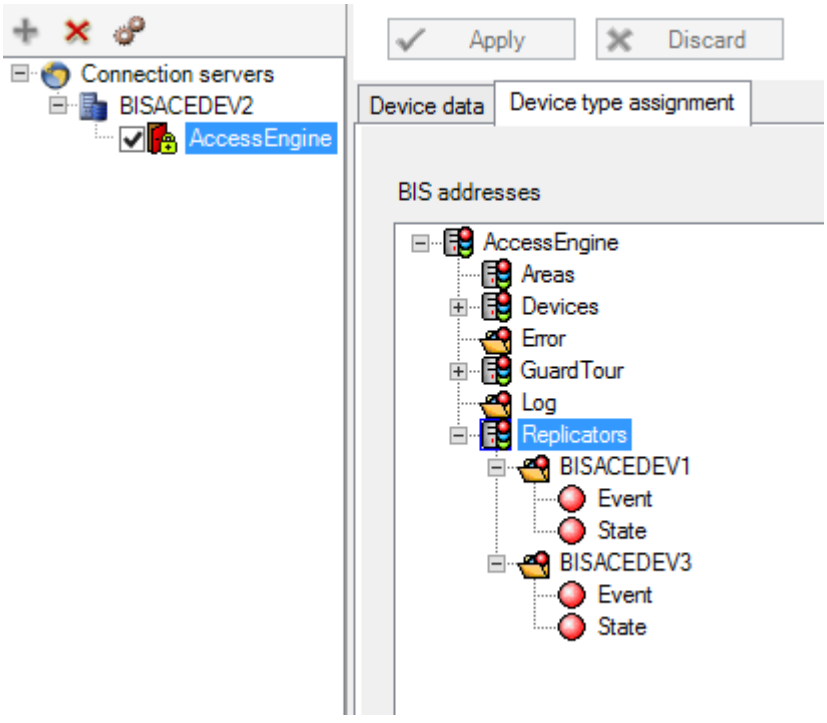
When to start and stop replicators

Normally the replicators are started and stopped by the DMS Master process according to its data tables. It is not necessary to start or stop or start replicators manually, except for the following exceptions:

– You need to stop a replicator process to temporarily protect a level 1 or 2 server from being overwritten by its parent while it is performing local tasks.
– You will need to start replicator process if you manually stopped it.

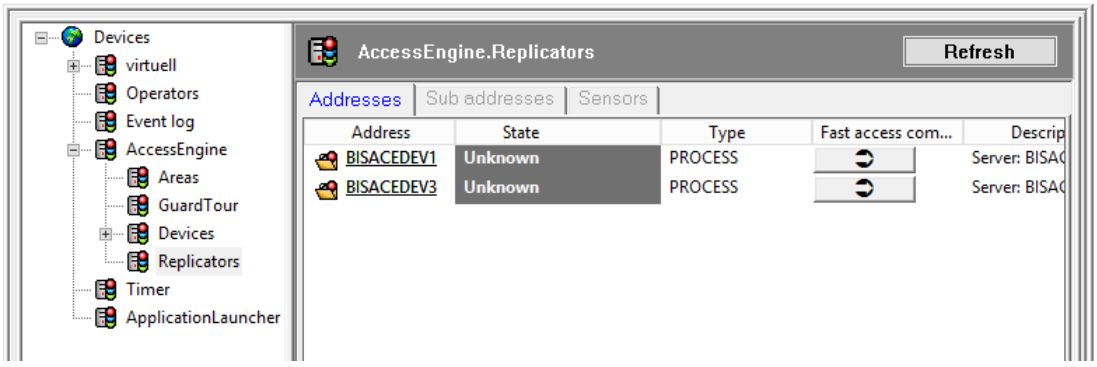
Viewing replicators in the BIS Configuration Browser

An ACE connection server in the BIS device editor shows a new node **Replicators** below the **Access Engine** node. The replicators are named after the servers on which they reside.
The example below shows the view from the configuration browser of a Level-2 server. It has one child server BISACEDEV1 and one parent server BISACEDEV3. Each child server has the sub-addresses Event and State.



Starting and stopping replicators from a BIS Client

If the configuration with the ACE server hierarchy has been loaded in BIS, and the client restarted, then the same servers will appear in the BIS client as follows.



To start or stop a replicator process, right-click the replicator in the **Address** column of the **Addresses** tab and select **Start** or **Stop**.

BIS/ACE messages

The following messages are sent from ACE to BIS regarding hierarchical cardholder management:

- Mapped on **Event** sub-address:
  - `0x07000005`, the message sent by the replicator to signal that it has started.
  - `0x07000006`, the message sent by the replicator to signal that it is stopping.
- Mapped on **State** sub-address:
  - `0x07000009`, the message sent by the DMS master process to signal that it has started the replicator.
  - `0x07000007`, the message sent by the DMS master process to signal that it has stopped the replicator.

5.7.8 Replication in detail

This section describes hierarchical data replication in greater detail than is normally required, and is included for reference purposes.

All access control data (cardholder data) from the top-level server is replicated to each mid-level server (level-2) and **merged** with the data that has been locally generated or modified at level-2.
Merging means that cardholder data will only be overwritten at level-2 if it has been modified or deleted at Level-3.

Notice!
Consistency of card encodings
In order for data to be merged at all, the customer must ensure that cards with the same codes are not created independently on different levels.

All access control data (cardholder data) from each parent server is replicated to the server's own descendants, but not to the descendants of its siblings.

Device data is replicated only to those Level-1 servers where the devices are connected. Each Level-1 server receives a copy of its own device data that is maintained on its parent Level-2 server. After this replication, no data created previously at Level-1 will persist at Level-1.

A full automatic re-synch happens only when the network connection between a server and its parent server is established or restored. As long as the network connection persists it is only the **changes** at the parent level that are continuously replicated to its child.

ACE device data from the Level-2 server is replicated to Level-1 servers immediately, and each Level-1 server receives from Level-2 only the data pertaining to its own devices.

After replication the data becomes active in ACE immediately. The BIS configuration, on the other hand, needs to be updated and reloaded manually in the BIS Configuration Browser by a Level-1 administrator user, whenever new devices are added or old devices deleted.

5.7.9 Limitations of the current version

- The hierarchy must be completely within the BIS Common Division
- The hierarchy supports a maximum of 255 ACE time models, which must all be configured on the Level-3 Top-Level Server.

- BIS operator data is not replicated. Therefore the management of BIS operators, including their authorizations, must be carried out separately on each BIS server.
- A BIS/ACE server must contain no person or device data while it is being registered in the server hierarchy.
- The operating system and BIS version of all servers in the hierarchy must all be of the same language.
- The servers in the hierarchy must all be of exactly the same BIS version. During a BIS update all data transfer is stopped until the version numbers are the same.
- Extended ACE functionality, such as key cabinets (Deister or Kemas), parking-lot management and “PegaSys” Offline Doors have not yet been tested thoroughly in a server hierarchy.

5.8 MACs and RMACs in hierarchical topologies

Introduction

Review the chapter *MACs and RMACs in flat topologies, page 33* regarding definitions and procedures for the configuration of MACs and RMACs in general.

The current chapter covers the differences between the configuration of MACs and RMACs for flat and hierarchical topologies.

In short, the main difference is that a MAC does not simply fail over to another computer, but to the next level up the hierarchy. This strategy provides extra resilience.

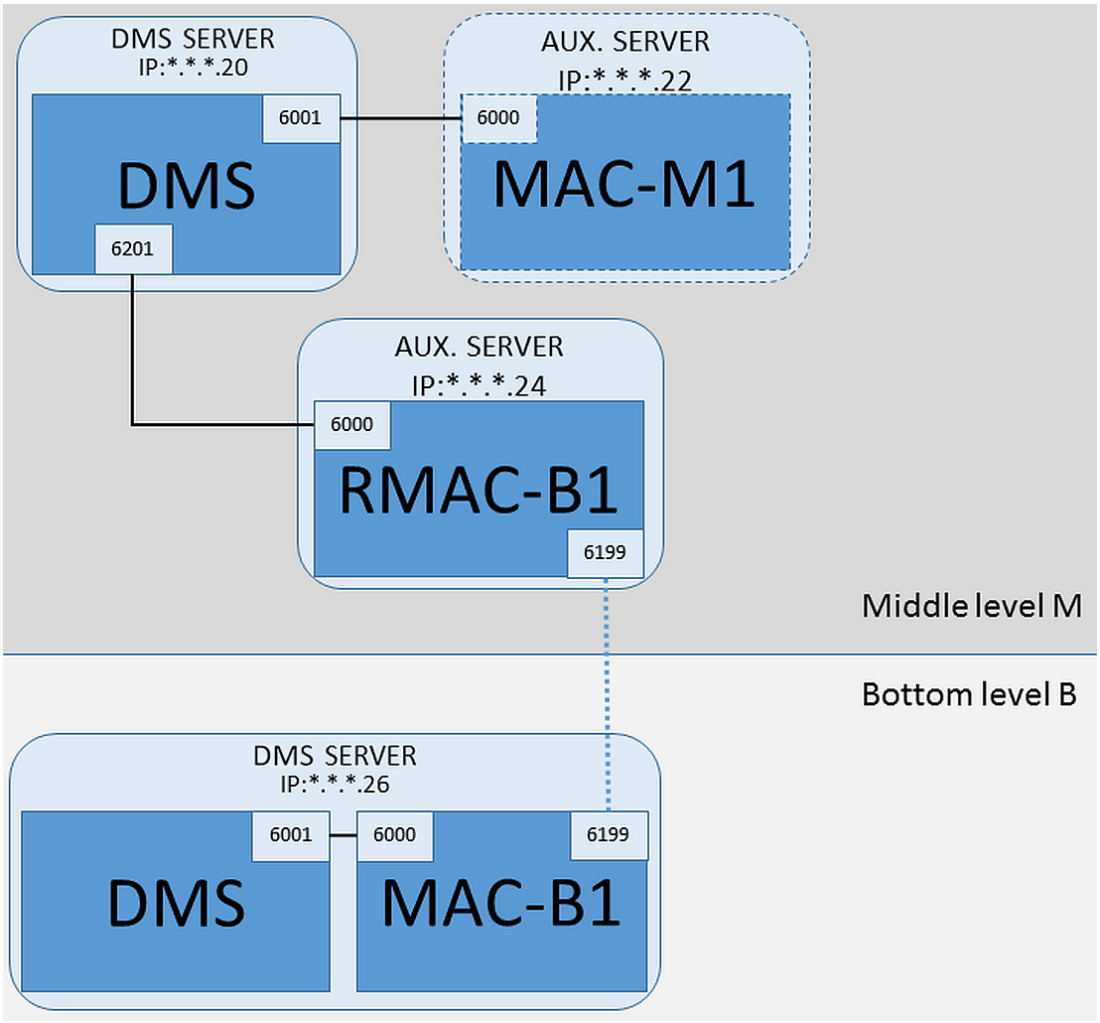
Notice!

Training recommended

In view of the complex and specialized nature of this topic, Bosch recommends that the persons involved attend appropriate technical training.

Note on the illustrations in this chapter and subchapters

IP addresses in the form `*.*.*.dd` (where `dd` is an integer) stand for IP addresses that differ from others in the diagram only by their last digits.



Prerequisites

- The hierarchy of servers has been set up as described in the chapter *Hierarchical cardholder management, page 117*
- The hierarchy is configured top-down, because each DMS server, except the top-level server, needs to register with its parent in the ACE Hierarchy Tool.
- Each DMS server has at least one MAC. The first MAC can reside either on the same computer as the DMS (for example, MAC-B1 in the illustration), or on its own MAC server computer (for example, MAC-M1 in the illustration).

  NOTE: MAC-M1 in the illustration plays no part in the procedures described here.
  - For setting up MACs on the DMS server, see section *Configuring a MAC on the DMS server without RMAC, page 34*
  - For setting up MACs on a MAC server, see section *Configuring a MAC on its own MAC server, page 35*
- RMACs never reside on the same computers as the DMS or the MAC. They always reside on their own MAC servers. For configuration of RMACs, see section *Adding RMACs to MACs, page 37*

  but in the MACInstaller tool set the main parameters as described in the next section.

Procedure: Setting MACInstaller parameters in hierarchical systems

In an hierarchical system, where multiple DMS servers exist, the RMAC for a MAC on the bottom level, actually interacts with the DMS on the middle level. Thus, in the illustration above, bottom level MAC-B1 fails over to RMAC-B1, one level higher.

When using MACInstaller.exe (see *Using the MACInstaller tool, page 40*) on the MAC and its RMAC, set the parameters as follows:

On the computer where the MAC is running

- **Server**: Name or IP address of the DMS server computer on its own level. In the illustration the IP address for the **Server** parameter for MAC-B1 is the one that ends in 26.
- **Port**: `6001`
- **Number**: `1` (all MACs have Number 1)
- **Twin**: IP address of the computer where the RMAC will run. In the illustration the IP address ends in 24.
- **Update software**: Select this option, as you are configuring a MAC server, not the DMS server.

On the MAC server computer for the RMAC

- **Server**: Name or IP address of the DMS server computer at middle level. In the illustration the IP address ends in 20.
- **Port**: `6201` (The DMS port number is the MAC port number plus 200)
- **Number**: `2` (all RMACs have Number 2)
- **Twin**: IP address of the computer where the twin MAC is running. In the illustration the IP address ends in 26.
- **Update software**: Select this option, as you are configuring a MAC server, not the DMS server.

Note that by convention the MACInstaller parameter **Port: (Port to DMS)** for the RMAC, at middle level, is 200 greater than that of its partner MAC at bottom level, as illustrated by the following table.

“Port to DMS” for MAC (bottom level)	“Port to DMS” for RMAC (middle level)
6001	6201
6002	6202
...	...
600n	620n

See also

- *MACs and RMACs in flat topologies, page 33*
- *Hierarchical cardholder management, page 117*

6 Infrastructure - System Configuration

6.1 Card Definition

Use this dialog to define data transmitted from the reader. New card definitions can be added to the system at a later date.
The following types are predefined by the system, and are not modifiable:

- 32 Bit CSN - Standard MIFARE (32 bit)
- HID 26 - Standard Wiegand 26 bit code = active (**default**)
- HID 35 - HID corporate 1000
- HID 37 - HID 37 bit code - CN-H10304
- EM 26 - EM 26 Bit code
- Serial readers (AMC 4R4/LACi) - 64 bit
- HID 48 - HID corporate 1000
- 56 Bit CSN - Standard MIFARE Desfire

HID 26 is the default card type, and appears in the list **Active card types**

6.1.1 Active Card Types

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.

6.1.2 Creating and Modifying

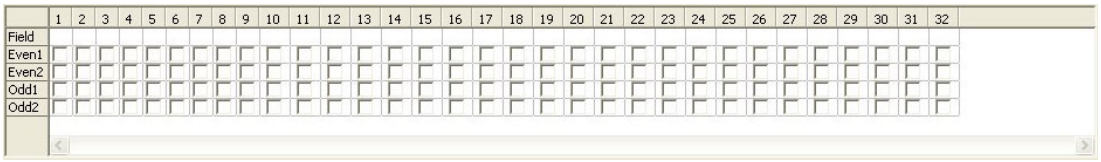
The button with the green plus sign (✚) above the right-hand list box creates a new list entry. In contrast to predefined data these newly created list have a white background and can be edited and modified at any time. Double-click the fields **Name**, **Description** and **Number of Bits** to edit 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 data double-click the relevant field. To delete first select data and then click the red x (✕) button.

Notice!
Only list entries created in the dialog (with a white background), can be modified in both the left and right-hand lists.
Deletions are only allowed in the right-hand list, and only on list elements created since installation.

When a list element is selected (in left or right-hand lists) then its encoding is displayed in the lower part of the dialog. This part of the display is inactive if multiple list entries are selected. The display shows bit-data 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 which 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(-reader) 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.

6.1.3 Activating / Deactivating card definitions

Up to 8 card definitions can be active simultaneously. 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 four definitions can be moved at once. Once four 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!
In the case of readers with L-Bus or BG900 protocols the list entry Serial Reader needs to be activated. This is in order to make the manual input dialog **Dialog Bosch** available for inputting data in the Access Engine dialog system.

6.1.4 Creating card data in the Access Engine dialog system

Manual data input

Different input methods are invoked within the access control system, depending on whether Wiegand or Bosch cards are being used.
For all Wiegand definitions (HID 26, HID 35, HID 37 and 32 Bit CSN) the entry Dialog (Wiegand) is generated, which allows the Customer code to be entered and modified as well as the card number.

Dialog (Wiegand)	

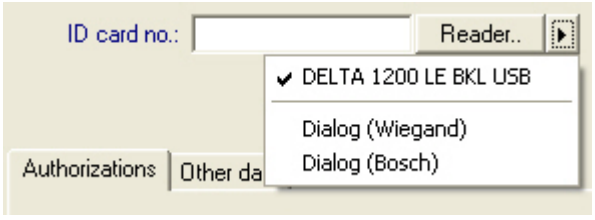
For serial readers the entry Dialog (Bosch) is generated with additional fields for Version and Country Code.

Notice!
The values of the populated fields are defined in the Configuration Browser dialog **Infrastructure > ACE Card definition** and can be overwritten, if required, for individual cards.

Data input by input reader

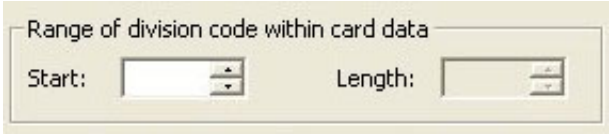
In addition to manual data input any workstation can be equipped with an input reader for collecting card data.
For this purpose select an appropriate reader from the predefined list in Configuration Browser > Infrastructure > **ACE Card Reader**.
If the chosen reader is an input reader for Wiegand cards (DELTA 1200 iClass RS232 BKL or DELTA 1200 Prox RS232 BKL) then all active Wiegand card types will be listed along with the reader (in Access Engine > Personnel data> Cards > Reader:**Combo box 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 can not be selected directly but only indirectly via the choice of Wiegand definition. If the required entry does not appear in the pull-down list then a different entry needs to be activated in the Configuration Browser, or a different selection made in Access Engine.

In the case of input readers with Hitag, Legic or MIFARE read-processes the actual reader entry is generated and can be selected from the list directly.



With Divisions (multi-party capability) enabled

If the access-controlled facility is divided among multiple parties (aka "Divisions") it is possible to configure a code area on the card that allows the operator to distinguish between the various Divisions' cards. Use the optional fields (only selectable where Divisions have been installed) to define the position of the **start** bit and the **length** of the Division coding on the cards.

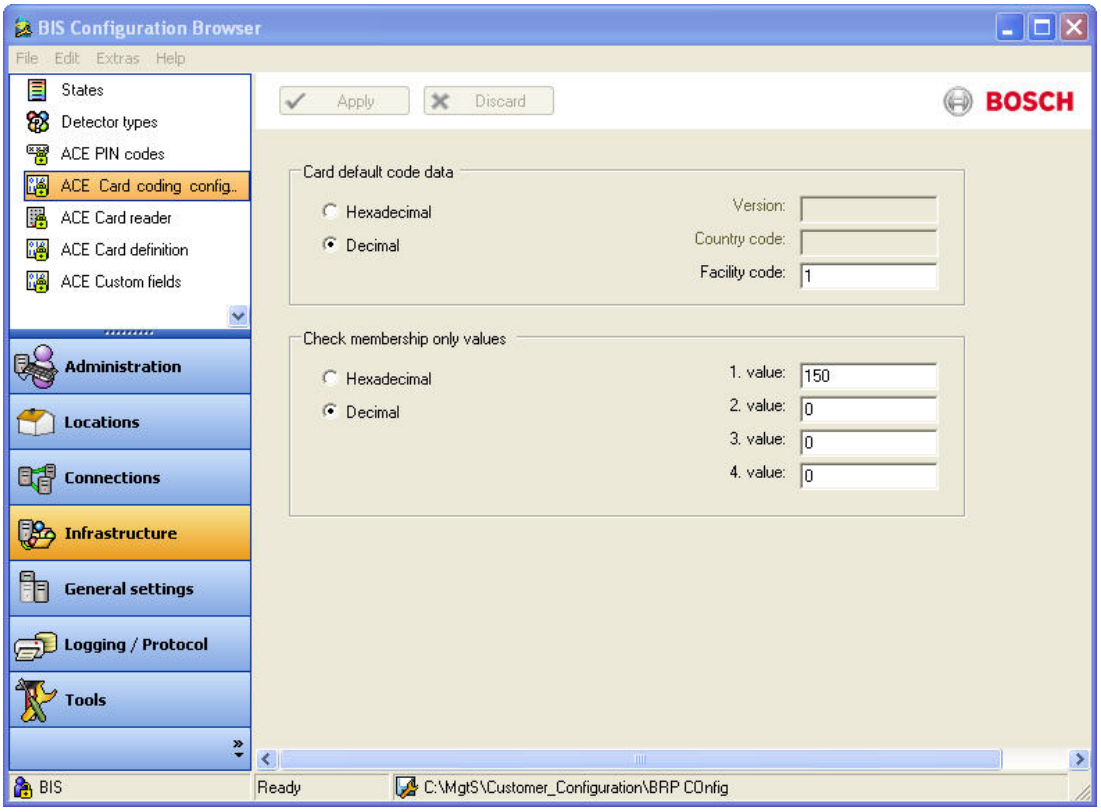


6.2 Configuring card codings

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

Dialog path

BIS Configuration Browser > **Infrastructure** > **ACE Card coding configuration**



Entering numbers in the dialog

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

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

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

Card default code data

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

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

Code no. complete (default)	Only the facility code is entered (hex or decimal).  **Entering encoding data:** The facility code is provided by the manufacturer as a decimal value: 56720 Select the radio button **Decimal** and enter the facility code. Click the Apply button to save the data.

Code no. split	Version, Country Code and Facility Code must all be entered as **decimal** values.  **Entering code data:** The data are provided by the manufacturer as the following decimal values: Version: 2 Country code: 99 Facility code: 56720 Enter the data in the appropriate text boxes. Click the Apply button to store the data.

Notes on inputting default code data:

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

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

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

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

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

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

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

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

Notice!
If the card capture occurs via a connected dialog reader then the default values are assigned automatically. It is not possible to override the defaults when capturing from a reader.
In order to do so the capture type should be switched to **Dialog**

Manual entry of the card number is in decimal format.

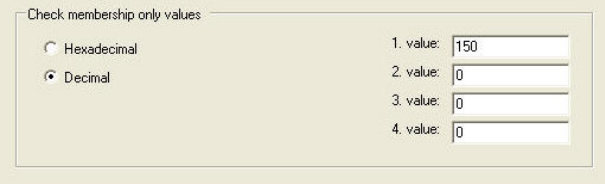
When saving the data a 10-digit decimal value (with leading zeros) is created, which is then converted to an 8 digit hexadecimal value. This value is now stored with the default code data as the 16-digit code number of the card.

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

Check Membership only values

Checking for membership only means that the credential is checked only for membership of a company or organization, not to identify an individual. Therefore do not use the **Membership check only** for readers that give access to high-security areas.

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



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.

6.3 Enrollment readers

Introduction

An enrollment reader is a special card reader that is used for one or more of the following tasks:

- Capturing card data in order to register a cardholder in the system
- Retrieving cardholder data from the system
- Authenticating ACE operators for the ACE client.

Enrollment readers were hitherto always connected directly to an ACE workstation, (normally via a USB or COM port).

As of ACE Version 4.5 any card reader connected to an AMC device can be used as an enrollment reader, in addition to its access-control tasks. However, because it has only one channel (port), a reader cannot do both simultaneously.

Note on configuration menus

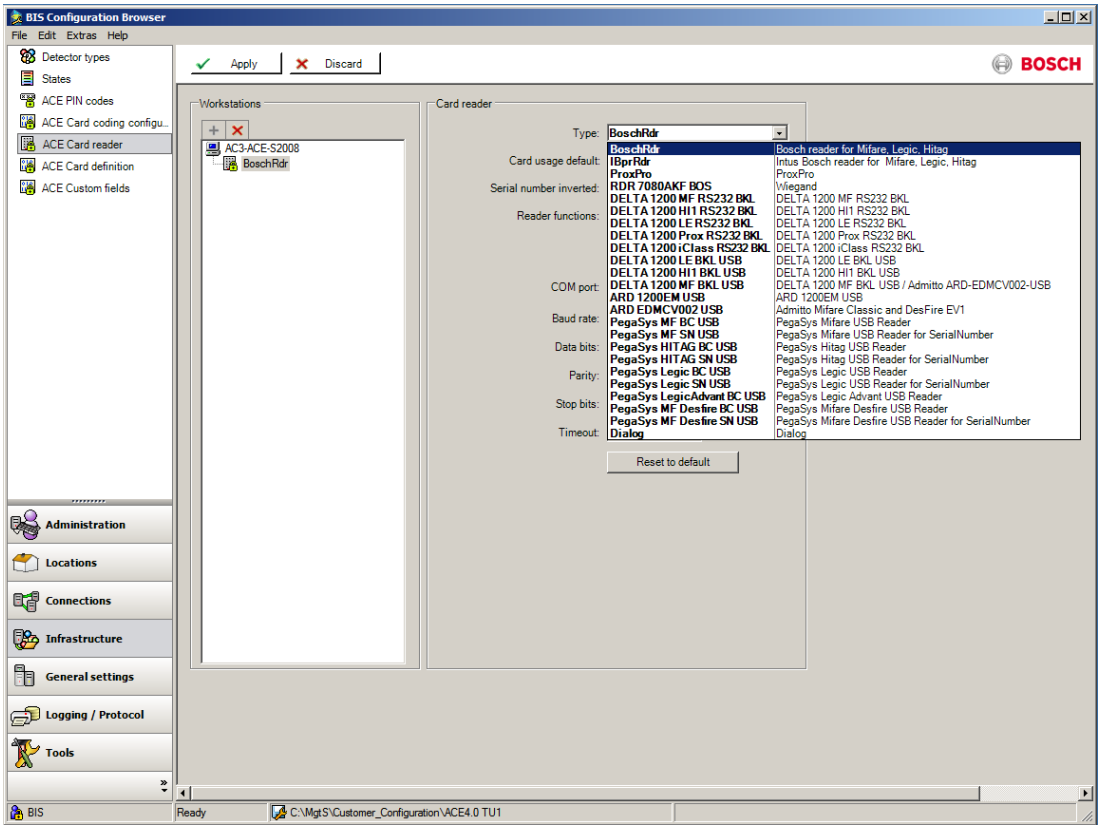
Dedicated enrollment readers that are connected directly to the workstation via USB or COM ports, are configured in the Configuration Browser in the dialog **Infrastructure** > **ACE Card reader.**

Enrollment readers that are also access readers are first configured hierarchically below the AMC access controllers of ACE servers in the Configuration Browser **Connections** menu. They must then be configured as enrollment readers in the dialog **Infrastructure** > **ACE Card reader** also. See *Configuring a non-fingerprint reader for access control and enrollment, page 139*

6.3.1 Configuring a serial enrollment reader

To configure an enrollment card reader on a serial port, proceed as follows:

1. In the Configuration Browser, in the dialog **Infrastructure** > **ACE Card reader**, select the desired workstation from the **Workstations** pane.
2. Select the reader type from the combo-box **Reader type**
3. Specify the number of the **COM port** used.



For the remaining data for each reader type the default parameter settings are usually sufficient.

For an up-to-date list of the reader types that can be selected from this dialog, consult the release notes for your ACE version.

In the Access Engine Person dialogs both directly connected readers such as these, and also access control readers connected via AMC controllers, can be used as enrollment readers by selecting them from combo-boxes next to the buttons **Reader...** and **Record card**.

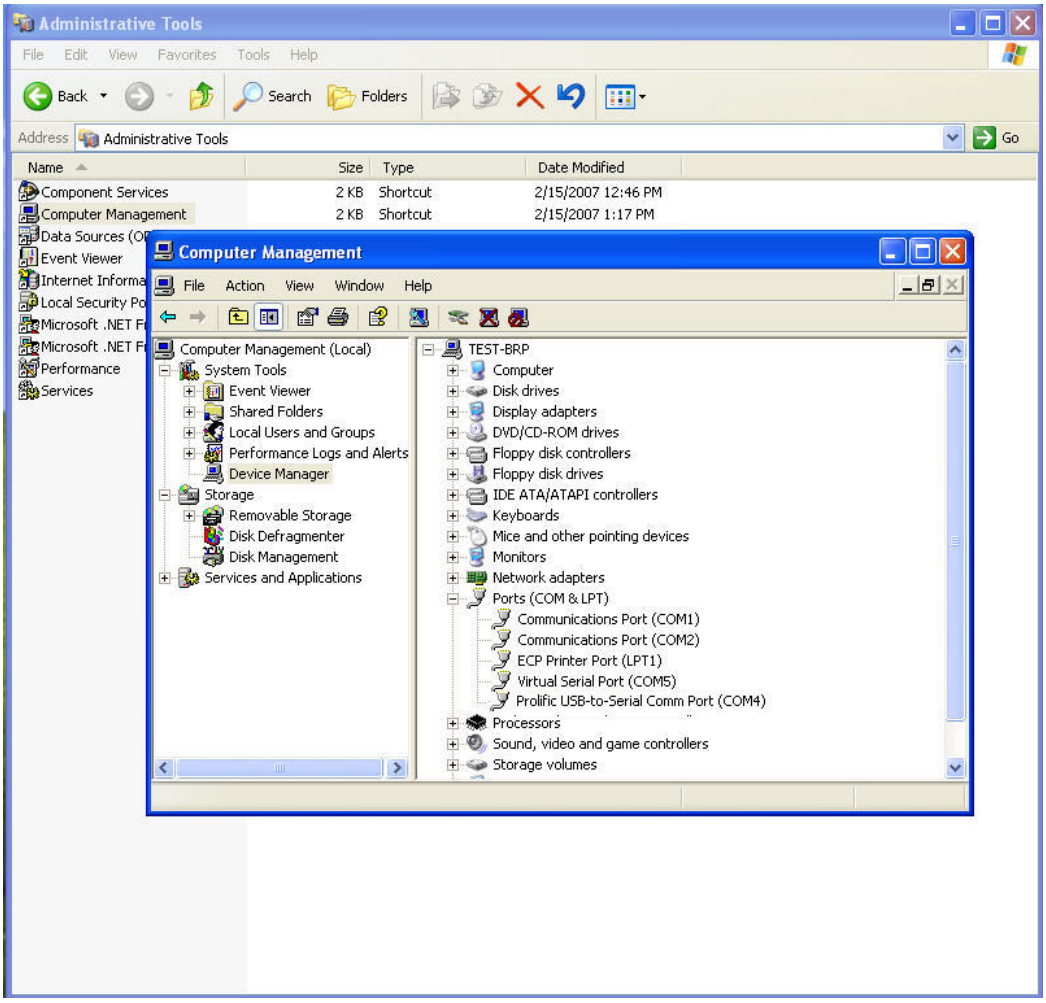
6.3.2 DELTA Readers with USB interface

Introduction

Readers with USB interfaces require virtual COM ports. Every reader delivered includes drivers for setting up virtual COM ports.

Procedure

1. Execute the driver installation program for your DELTA reader, for example: **PL-2303 Driver Installer.exe**.
2. Connect the reader to the ACE workstation's USB port.
3. Open the **Device Manager** program for your version of Windows, for example: **Start > Settings > Control Panel > Administrative Tools > Computer Management > Device Manager**
4. From the list of device types unfold the node **Ports (COM & LPT)** and note the number of the COM port that was configured by the installation program, for example: **Prolific USB-to-Serial Comm Port (COM<number>)**



5. In the Configuration Browser go to **Infrastructure > ACE Card Reader** and enter the number you have just noted in the **COM Port** field.
6. Select the appropriate reader type choose from the pull-down list.

6.3.3 RF IDeas Readers with USB interface

Introduction

Readers with USB interfaces require virtual COM ports. Every reader delivered includes drivers for setting up virtual COM ports. Proceed as follows:

1. Locate the appropriate drivers for the reader as per the manufacturer’s instructions.
2. Connect the reader
3. The operating system should detect unknown hardware and automatically install it.

4. If automatic driver installation fails, manually install or re-install the driver via the Device Manager for your version of Windows, for example: **Start > Settings > Control Panel > Administrative Tools > Computer Management > Device Manager**
5. From the list of device types unfold the node **Ports (COM & LPT)** and note the number of the COM port that was configured by the installation program, for example: **Prolific USB-to-Serial Comm Port**
6. In the Configuration Browser go to Infrastructure > ACE Card Reader and enter the number you have just noted in the COM Port field.
7. For **Reader type** choose the pull-down item **RW300** (for IClass readers) or **ProxPro** (for proximity readers).

6.3.4 Configuring a non-fingerprint reader for access control and enrollment

1. Ensure that the reader is connected to the reader's interface on an AMC.
2. In the Configuration Browser **Connections** > **Connection servers** > [your connection server] > **AccessEngine,** create within your device hierarchy an entrance with that reader.
3. Click the **Apply** button to save your settings.
4. In the Configuration Browser **Infrastructure** > **ACE Card reader**, select the workstation to for which the reader is to become an enrollment reader.
5. Click the green plus ✚ button to add a reader to the workstation.
6. Select the reader type **Access reader** from the drop-down list. Note that this reader type can be used only once per workstation.
7. Click the **Apply** button to save your settings.

6.3.5 Configuring a fingerprint reader for enrollment use only

Introduction

For a general introduction to fingerprint readers, see *Fingerprint readers, page 142*

Procedure

1. Connect the fingerprint reader to your network.
2. Run the **AccessIPConfig** tool (which has its own online help) to configure the network parameters of the fingerprint reader.
   - Click the **Scan for fingerprint readers** button
   - Double-click the desired fingerprint reader in the list
   - Click the **Set IP...** icon
   - In the **Set IP address** dialog, select reader type **Enrollment reader**, and select the appropriate **Card Type** for your ACE installation**.**
   - Carefully note the IP address for use later in this procedure
3. In the Configuration Browser, navigate to **Infrastructure** > **ACE Card reader**, select the workstation to which the fingerprint reader is attached.
4. Click the green plus ✚ button to add a reader to the workstation.
5. Select the fingerprint reader in the device tree. Note that each reader type can be used only once per workstation.
6. Enter the IP address that you set for this reader in the **AccessIPConfig** tool.
   NOTE: If you changed the port number in the **AccessIPConfig** tool, ensure that you set the same port number here also.
7. Click the **Apply** button to save your settings.

Registering a duress finger

When recording fingerprints for cardholders it is possible to define a finger that a cardholder can use if placed under duress. Use of this “duress finger” at the fingerprint reader will then trigger a silent alarm in the system. See the ACE Operation Guide for details.

See also

– *Fingerprint readers, page 142*

6.3.6 ACE operator login via enrollment reader

Introduction

For additional security, ACE operators can be configured in so that they can only enter the ACE client interface by presenting their cards at the enrollment reader connected to that server.

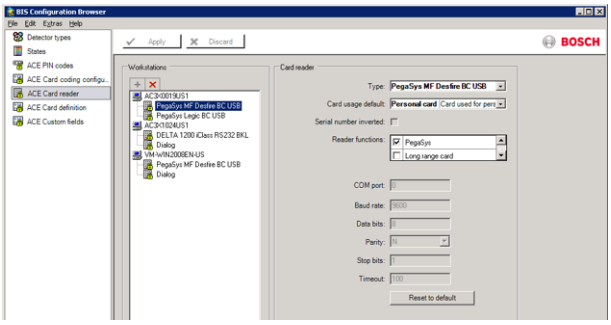
Procedure

1. In the Configuration Browser, locate the enrollment readers configured for an ACE server by clicking **Infrastructure > ACE Card reader**.

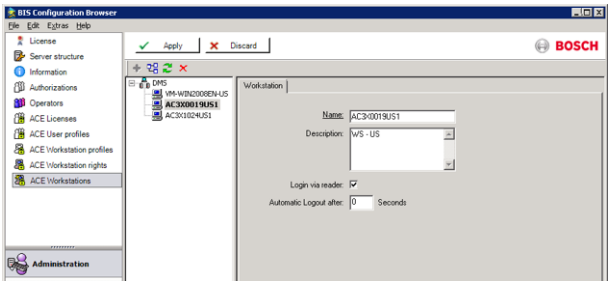
Notice!

If multiple enrollment readers are configured on the same ACE server.
For logging in to the ACE client uses the enrollment reader that was configured first, i.e. the uppermost in the list.
In order to configure a different enrollment reader for ACE login, remove any readers that are above it until the desired reader is uppermost. Any reader that you remove can be added again later, if required.

2. In the following example the reader intended for login is **PegaSys MF Desfire BC USB**:



3. Go to **Administration > ACE Workstations** and select the check box **Login via reader**:



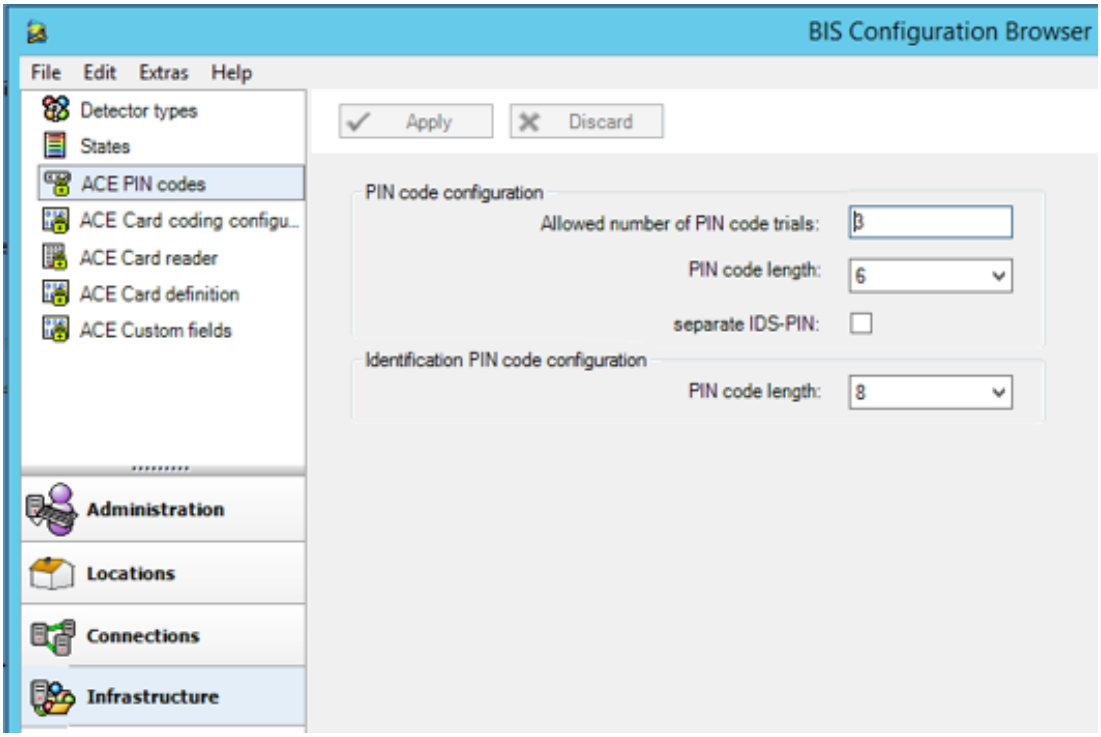
4. The cardholder who is to log in to ACE via the enrollment reader needs to be associated with an ACE operator. The procedure to do this is described in the section **2-Factor Authentication**.

5. Save and reload the configuration, restart the ACE client.
   The cardholder can now log onto ACE only by presenting his card to the enrollment reader.

See also
– *2-Factor Authentication, page 19*

6.4 Configuring PIN Codes

Dialog path
Main menu > **Configuration** > **Options** > **PIN codes**
BIS Configuration Browser > **Infrastructure** > **ACE PIN codes**
This dialog sets system-wide parameters for both kinds of PIN code:
– Verification PIN
– Identification PIN



PIN code parameters

Allowed Number of PIN Code Trials
The number in this field (3 by default) defines the allowable number of attempts to enter a PIN at a keypad reader (possible values: 1 to 10). Cardholders who do not enter the correct PIN code within the specified number of attempts are blocked system-wide, even at card readers that do not require PINs.
You can only clear this block by using the **Blocking** dialog at an Access Engine workstation.

PIN Code Length
This text box sets the length of all verification PINs throughout the system. The range of valid values is 4 to 9 (6 by default).

Notice!
Do not change the setting **PIN code length** while the system is running. This would lead to all assigned PIN codes becoming invalid and needing to be recreated.

Separate IDS PIN
If no separate IDS PIN is set, then a verification PIN can be used to arm the IDS.
Only if the check box is selected do the input fields for the arming-PIN become editable in the **Cards** dialog. When the IDS PIN is set the verification PIN can no longer be used to arm the IDS.

Identification PIN code configuration:
This text box sets the length of all Identification PINs for use with the feature **Access by PIN alone**. The range of valid values is 4 to 8 (8 by default).

Additional steps for configuring Identification PINs for Wiegand and OSDP readers
If and only if you are using Identification PINs on Wiegand or OSDP readers, perform the following steps.
1. In the Configuration Browser, navigate to **Infrastructure** > **ACE Card definitions.**
2. Select **Input mode,** with Description **Manual input** in the **Available card types** pane.
3. Use the arrow button to transfer it to the **Active Card types** pane.
4. Click the **Apply** button.

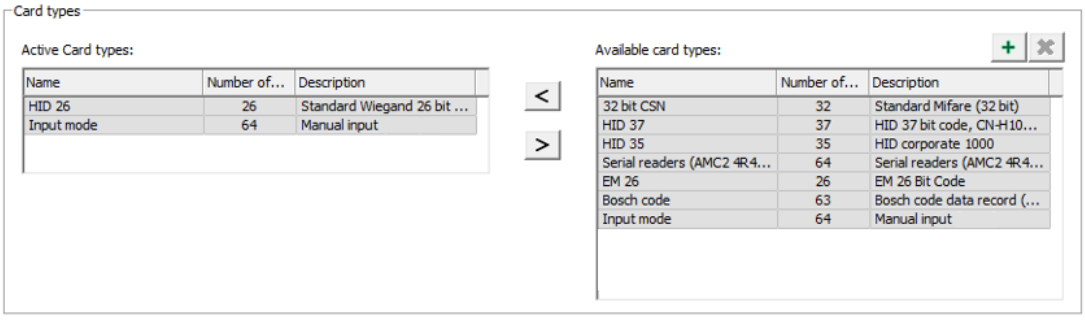


Figure 6.1:

Notice!
If you transfer **Manual input** to the **Active Card types** then LBUS and BG900 protocols will no longer work.

6.5 Fingerprint readers

Configuration using the AccessIPConfig tool
All fingerprint readers must be set up in the **AccessIPConfig** tool before they can be configured in the Configuration browser. Consult the tool's own online help for details of usage.

Start the **AccessIPConfig** tool from the Configuration browser:
Tools menu > **ACE Configuration and fingerprint devices**,
or directly from the file system:
`MgtS\AccessEngine\AC\Bin\AccessIPConfig.exe`

Reconfiguring a fingerprint reader that is already in use

A fingerprint reader that is already in use cannot be configured in the **AccessIPConfig** tool. This is indicated by a yellow warning triangle next to the icon of fingerprint reader in the **Network name** column in the tool.

To put the reader out of use without disconnecting it from the network, proceed as follows:

1. Locate the reader in the Configuration Browser > **Connections** > **Connection servers** > [your connection server] > **AccessEngine**, > tab:**Device data** > (find the fingerprint reader below its entrance in the device tree) > tab:**Network & Operation modes**
2. Set an invalid IP address, that is, one that is **not** currently displayed in the **AccessIPConfig** tool.
3. Click  or the **Apply** button to save.
4. In the **AccessIPConfig** tool, click the **Scan fingerprint readers** button to refresh the list. The yellow warning triangle will have disappeared from the reader's icon. Now you can proceed to reconfigure the reader in the tool.
   Afterwards, remember to set the correct address again in the Configuration Browser.

Notice!

Fingerprint reader -- single channel

A fingerprint reader has only one channel, which at any one time can be used either for self-configuration (via the **AccessIPConfig** tool), or for access control or for enrollment. It can perform multiple tasks sequentially but not simultaneously.

6.5.1 Configuring a fingerprint reader for access control

Introduction

As of ACE Version 4.6 fingerprint readers can be used for access control in different operation modes, depending on whether the reader is currently online or offline.

- **Online:** Fingerprint templates are stored on the DMS server and downloaded to the devices temporarily whenever required.
- **Offline:** Fingerprint templates are continually updated on the fingerprint reader while it is online, in order to enable access control even when the reader is offline.
  - The capacity of a fingerprint reader to store fingerprint data is limited. For the current maximum number of users, consult the datasheet corresponding to your version of Access Engine.
  - Which of the **offline** options is used (**Fingerprint only**, **Card only** or **Card and fingerprint**) may be determined either by the stored properties of the cardholder, or by those of the reader. The reader parameter **Person-dependent verification** must be selected for the offline option in the cardholder properties to take effect.

Prerequisites

- Persons authorized for access by **Fingerprint only** must nevertheless have cards. This is because the fingerprint reader transmits only card data to the system when it recognizes the cardholder's fingerprint.

If fingerprint readers are used, then at least two are necessary in any configuration:

- First configure a fingerprint reader as an enrollment reader, to record fingerprints and cards for the ACE system. See *Configuring a fingerprint reader for enrollment use only, page 139*
- After that, configure at least one for access control at an entrance. Follow the procedure below.

Note that the procedure for recording cardholders' fingerprints is described in the ACE operation help.

Procedure

1. Connect the fingerprint reader to your network.
2. Run the **AccessIPConfig** tool (which has its own online help) to configure the network parameters of the fingerprint reader.
   - Click the **Set IP...** icon
   - In the **Set IP address** dialog, select reader type **Access reader**, and select the appropriate **Card Type** for your ACE installation**.**
   - Carefully note the IP address for use later in this procedure
3. If the ACE client is running, close it.
4. In the Configuration Browser **Connections** > **Connection servers** > [your connection server] > **AccessEngine,** create within your device hierarchy an entrance with fingerprint readers.
5. Select your fingerprint reader in the device tree.
6. On the **Network & Operation modes** tab in the main dialog pane set the following parameters:

Network	IP address	The IP address that is set for this reader in the **AccessIPConfig** tool
	Port	Use the default port `51211` for all fingerprint readers
The following parameter options are mutually exclusive (radio buttons)		
Fingerprint templates on server (Online mode)	**Card only**	The card scanner, not fingerprint scanner, in the reader is used.
	Card and fingerprint	Verifies that the person using an access card is really its owner, by scanning both card and fingerprint.
Fingerprint templates on device (Offline mode)	**Person - dependent verification**	The identification mode of the fingerprint reader is read from the settings given to the individual cardholder in the ACE client **Personnel data** > **Persons** > tab:**Fingerprints.** The mode set there will be one of the three following options.
	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 the fingerprint and the card scanner are used, to verify that the person using the access card is really its owner.

6.6 Palm vein readers

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 manufacturer

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 manufacturer 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 manufacturer of the reader.

3. Click **Apply**, to apply and save the changes, or
   click **Discard** to cancel or remove the applied changes.

6.7 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.

6.7.1 Configuring an entrance for office mode

Procedure

In the Configuration Browser

1. Navigate to **Connections** > **Connection servers** > [your connection server] > **AccessEngine**
2. Create within your device hierarchy an entrance with at least one keypad reader.
3. Select the keypad reader
4. On the **Door control** tab, select the check box **Office mode**
5. Click the **Apply** button

6.7.2 Authorizing and instructing cardholders to set office mode

The procedures for authorizing cards to set office mode, and for starting and stopping office mode at a keypad reader, are described in the ACE operation help. Search for **Office mode**.

6.8 Custom Fields for personnel data

Introduction

Data fields for personnel are customizable in many ways:

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

– Whether and where the data will be used in standard reports

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

6.8.1 Previewing and editing Custom fields

Dialog path

– In the Configuration Browser, navigate to the **Infrastructure** menu > **ACE Custom fields**

The main window is divided into two tabs

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

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

Previewing

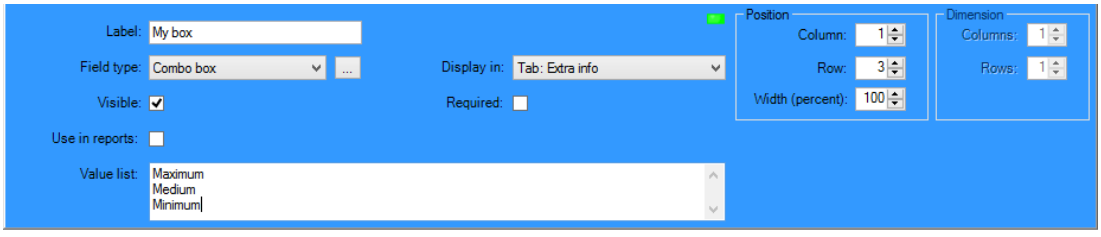
To preview in the Configuration Browser the effect of any change made in the **Details** tab, click the **Apply** button and go to the **Overview** tab.

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	**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. – **Text field** – Click the ellipsis button next to it to specify the number of characters allowed. – **Check box**

Label text	Description

	– **Date field**
	– **Time**
	– **Date-time field**
	– **Combo box**
	  – Enter the valid values for your combo box in the text field provided. Separate them with commas or carriage returns.
	– **Numerical input**
	  – Enter your minimum and maximum values for the numerical input in the spin boxes provided.
	– **Building control 1** and **Building control 2**
	  – 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 make reject data field contents that are not unique. For example, personnel numbers should be unique for all employees.
	The green light means that the data field is **not** currently used in the database. The red light means that the data field is currently used in the database.
Display in	Use this drop-down list to select the client tab on which the data field should appear.
Required	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. Note that the editor will not allow a required data field to be set invisible via the **Visible** check box. For ease of use in the client it is highly recommended that all required fields be placed on the first tab.
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**.

6.8.2 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.

6.9 Audit Trail

The Audit Trail Report uses the system log of the ACE to select the safety relevant events of the last n days. As the amount of data can increase very quickly, the installation default is 30 days.
The number of days can be modified in the registry key: `HKLM\Software\Wow6432Node\Micos\SPS\Default\Loggifier\SysKeep\@value`
Restart the Access Engine after any changes in the configuration

Calculation of event space:
Every event is stored in the system data log of the AccessEngine. Individual events are e.g.:

- door open,
- access,
- dialog start,
- personal single data change from dialog,

– import

Notice!
Each event needs a maximum of 8KB disk space (usually only 1-4 KB)
Normal systems need only up to one 100MB file per day. If you import very much data (> 10.000), you need a multiple of 100 MB files per day (the files are automatically generated by ACE if needed).

It is possible to backup the older files from the directory `..\MgtS\Access Engine\AC\LgfLog\` and copy them only for the Audit Log Report (after midnight the older files will be deleted again).
Roughly 3-5 GB of disk space are required on average for 30 days of operation. For a more accurate estimate, observe the disk space used over a typical cycle of normal operation, and extrapolate from this for the required period.

7 Integrating a Kemas key cabinet

Introduction

The following section briefly describes the functionality of a Kemas key cabinet and how to integrate it with an existing Bosch ACE or AMS system.

Prerequisites

- A Kemas key cabinet is ready for use and its IP address is known.
- The Kemas key cabinet system supports readers that can read and write Bosch standard card encoding.

Functionality

- The system prevents personnel from leaving the premises before returning their keys to the assigned compartment in the Kemas key cabinet .
- The system creates an alarm with the state Access denied (key) if a person attempts to leave the premises and the key has not been returned.
- The system prevents personnel from leaving the premises if the connection to the Kemas key cabinet is interrupted.
- The system creates an alarm with the state Access denied (offline) if a person attempts to leave the premises while the connection to the Kemas key cabinet is interrupted.
- The system creates an alarm with the state Key cabinet offline if connection to the Kemas key cabinet is interrupted.

Limitations

The current version supports only one per ACE or AMS system

Concurrent operation of a Kemas key cabinet with a Deister key cabinet is not supported.

Notice!

Data security risk

An unencrypted network connection (http) between ACE or AMS system and a key cabinet is a data-security risk. Ensure that all necessary measures are taken to protect the network traffic in the overall system from unauthorized access.

7.1 Configuring Kemas within the access control system

Creating BIS states for the key cabinet

1. In the BIS Configuration Browser navigate to **Infrastructure** > **States**
2. Create a new state list with the name `Key cabinet`
3. Create 4 new states, with the following texts (these are examples used throughout this document):
   - `Access denied (key)`
   - `Access denied (offline)`
   - `Key cabinet online`
   - `Key cabinet offline`

Configuring BIS states for the reader

1. In the BIS Configuration Browser navigate to **Infrastructure** > **Detector types > Access Engine > READER**
2. Create two state mappings for READER. **Note**: case sensitive!

Reported state	State
0200003a	Access denied (offline)
02000037	Access denied (key)

Configuring BIS states for the key cabinet

1. In the BIS Configuration Browser navigate to **Infrastructure** > **Detector types > Access Engine > KEYCABINET**
2. Create two state mappings for KEYCABINET. **Note**: case sensitive!

Reported state	State
0c000200	Key cabinet offline
0c000201	Key cabineit online

Configuring the Kemas key cabinet

1. In the BIS Configuration browser navigate to **Tools** > **ACE key cabinet configuration**
2. Click **New**
3. For the key cabinet type, select **Kemas**
4. Enter the name and the internet address of the key cabinet
5. Turn on the key cabinet
6. Click **Save**.

Configuring the reader

Readers that are to be connected to the Kemas key cabinet need to be configured in the Device editor.

1. In the BIS Configuration browser navigate to **Connections**
2. Select the desired reader in the Device editor tree view
3. Open the properties page of that reader
   Select **Check key return** and then the Kemas key cabinet
4. To prevent the AMC from allowing egress without permission from the key cabinet, configure the following parameters. Click the **Door control** tab**.**
   - Enter a value > 0 for the parameter **Waiting time for response**
   - Clear the check box labeled **Open door if no answer from host**

Completing the configuration in BIS ACE

1. Load the modified configuration in BIS Manager
2. In the BIS Configuration Browser, navigate to **Connections** > **Connection Servers** > **DMS**
3. Right-click and select **Synchronize** from the context menu.

8 Integrating a Deister key cabinet

Introduction

The following section describes how to integrate a Deister key cabinet with an existing ACE system.

A key management system can consist of

– 1 **key terminal** with
– 1 or more **key cabinets**, where each cabinet contains
– 1 or more **key panels**, and each panel typically contains
– 8, 16 or 32 slots for **key tags**.

The minimum configuration is one terminal with one cabinet containing one key panel.

A single ACE system can manage multiple key management systems, each with its own key terminal.

Preparing the hardware for installation

1. Start by physically assembling the Deister key management system including all panels, and inserting all key tags in their intended slots.
2. Connect the Deister key management system to the network.
3. In the BIS Configuration Browser navigate to **Tools** > **ACE Key Cabinet Configuration**
4. Click the button **Key Cabinet Configuration**.
   Result: The Key Cabinet Configuration window appears.
5. Select the **Activated** check box and click **Save**,
   – ACE will connect to the terminal and configure all inserted keys automatically, avoiding the need to configure keys individually afterwards.
   – Note: Nevertheless the BIS ACE operator will be able to browse the key states and reconfigure the system after this initial configuration.
6. Follow the configuration procedure below.

Configuration in the ACE software: Overview

The integration of a Deister key management system in BIS Access Engine (BIS ACE) consists of three phases.

– In the BIS Configuration Browser: Entering the parameters of the key management system in BIS
– In the ACE client: Defining the names of keys and key groups
– In the ACE client: Granting to ACE cardholders permission to take selected keys from the Deister key cabinet.

Limitations

Before proceeding, consider the following limitations. If in doubt on the applicability of any point, please contact Bosch technical support through the proper channels.

– If a Deister key cabinet integration is used in ACE configurations where cardholders have multiple cards:
  – Only one access card can be used with the Deister key cabinet.
  – By default this is the first card listed in the ACE client dialog Personnel data > Cards for that user. A different card can be selected, but automatically never more than one card.
– The key cabinet cannot be opened during a re-synchronization of ACE and Deister cabinet data.

– The full re-synchronization of a Deister key cabinet with 2,000 users, after a break in network communication with ACE, can take around 10 minutes.
– Deister key cabinets are limited to 2,000 users and 64,000 key assignments.

Notice!
Data security risk
An unencrypted network connection (http) between ACE or AMS system and a key cabinet is a data-security risk. Ensure that all necessary measures are taken to protect the network traffic in the overall system from unauthorized access.

8.1 Configuring a new Deister system in ACE

1. In the BIS Configuration Browser navigate to **Tools** > **ACE Key Cabinet Configuration**
2. Click the button **Key Cabinet Configuration**.
   Result: The Key Cabinet Configuration window appears.
3. Click the **New** button
4. Select key cabinet type **Deister** in the popup window, and press **OK**

Parameter values for terminals

1. Enter parameter values for the terminal the terminal.
   NOTE: IP and Bus addresses can be read from the terminal display; see below How to read the terminal display.

Display name	A name for the terminal. This name is displayed in the list of terminals on the left hand side of the **Key Cabinet Configuration** dialog window.
IP-address	IP address of the terminal.
Port number	Enter `2101` for unencrypted or `2601` for encrypted communication
Bus address	Enter the bus address of the terminal
Division	(Only if using the Divisions feature of BIS ACE) Enter the BIS ACE division to which the terminal belongs. ACE operators can then view and use only the cabinets within their own divisions.

Parameter values for key panels and additional cabinets

Add key panels and cabinets (or racks) to the key management system. Note that the dialog window starts with an initial minimum configuration of one cabinet (or rack) and one panel, to which you may now add. Every cabinet requires at least one panel.
Repeat these procedures for all key panels and additional cabinets (or racks) that belong to this key management system:
In the text field labeled Rack name, enter a display name for the cabinet (there must always be at least one cabinet per system). This name will appear in the terminal display.

Key panels

The dialog always starts with one key panel within the cabinet, labeled with a sequential integer in a square box, e.g. [1].

1. To add further key panels to the same cabinet, click the **Add panel** button. New key panels will be labeled [2], [3] etc. automatically.

2. Enter values for the panel's parameters:
   NOTE: Bus and Route addresses can be read from the terminal display; see the section below: **How to read the terminal display**.

Bus address	The bus address of the terminal
Route address	The route address of the panel. (This parameter is needed to release a specific key from ACE dialog System data > Keys)
Type	The type of the panel, e.g. FLEXX 16

Key cabinets

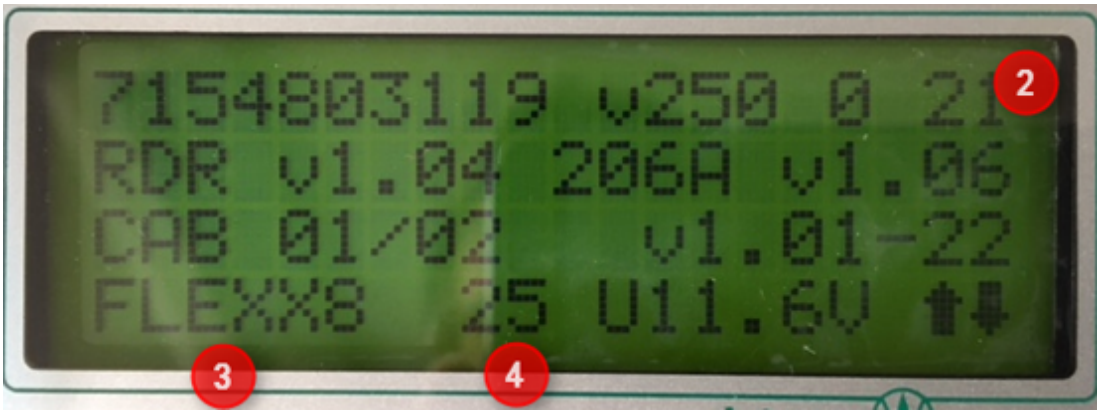
1. Click the **[+]** tab to add a new cabinet (rack) to the system. Give each a new **Display name** for the terminal display, and enter parameter values for each key panel in the new cabinet, as described above.
   NOTE: Addresses can be read from the terminal display; see below How to read the terminal display.
2. When all cabinets and key panels have been added, select the **Activated** check box.
3. Click the **Save** button to save the definition of the Deister terminal in ACE.

8.2 How to read the terminal display

The following illustrations explain where to find the essential information in the terminal display.
Note that the layout of the terminal displays may vary from one firmware version or language to another. If in doubt, please consult the Deister handbook that was delivered with your Deister system.

– The startup screen shows the name of the terminal (1) on the first line:

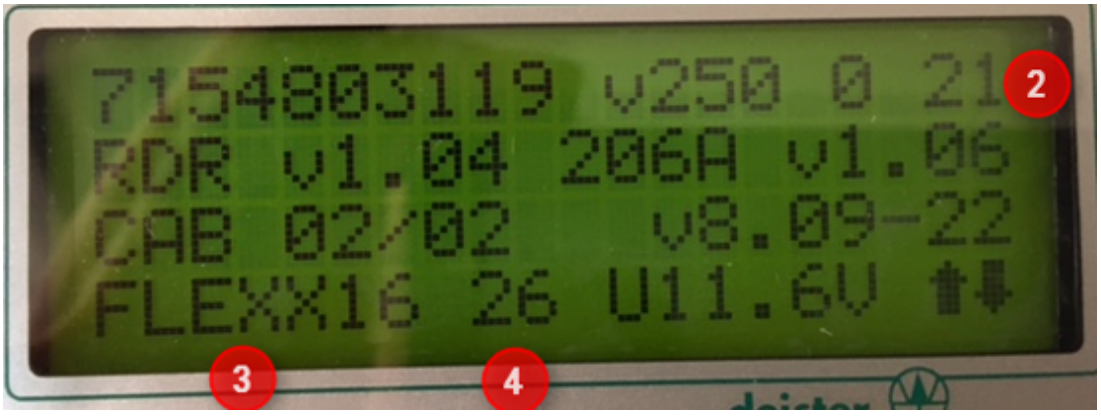
– Click the terminal's green **Return** key to display the next screen



#	Description	Value on screen
2	Bus-address of terminal	21
3	Type of panel	FLEXX8
4	Route address of panel	25

Note: CAB 01/02 means that this is the first of two cabinets.

– If multiple cabinets are connected you can press the down-arrow button to get details about the next cabinets:



#	Description	Value on screen
2	Bus-address of terminal	21
3	Type of panel	FLEXX16
4	Route address of panel	26

8.3 Modifying an existing Deister system in ACE

To modify the settings of a Deister key cabinet, proceed as follows:

1. In the BIS Configuration Browser navigate to **Tools** > **ACE Key Cabinet Configuration**
2. Click the button **Key Cabinet Configuration**.
   Result: The Key Cabinet Configuration window appears.
3. Select the desired terminal from the **Terminals** list
4. Click the **Edit** button
5. Clear the **Activated** check box
6. Click the **Save** button

7. Click the **Edit** button again
8. Modify the desired parameters.
   – For example: Under **Port no.** Enter `2601` for encrypted communication (the default value is `2101`)
9. Select the **Activated** check box
10. Click the **Save** button to save the definition of the Deister terminal

Resetting a Deister key cabinet

To reset a Deister key cabinet, that is to remove any previous settings, proceed as follows:

1. Click the **Reset** button
2. Clear the **Activated** check box
3. Click the **Save** button
4. Select the **Activated** check box again
5. Click the **Save** button again

9 Distributed systems

9.1 ACE distributed Installation

For a distributed BIS-ACE installation:

– Install the BIS on the **first** machine.
– Install the ACE on the **second** machine.

Installation of the BIS as a Server for the Access Engine

Start the BIS-ACE installation and select the packages as follows:

– Disable all other packages.
– Select **Access Engine** under the login server.
– Select the tools.

Continue with the installation. On this installation you will find:

– The BIS database
– The reporting database
– The BIS manager

Installation of the OPC Servers

To install the OPC Servers (referring to the Engines like Access Engine and Automation Engine):

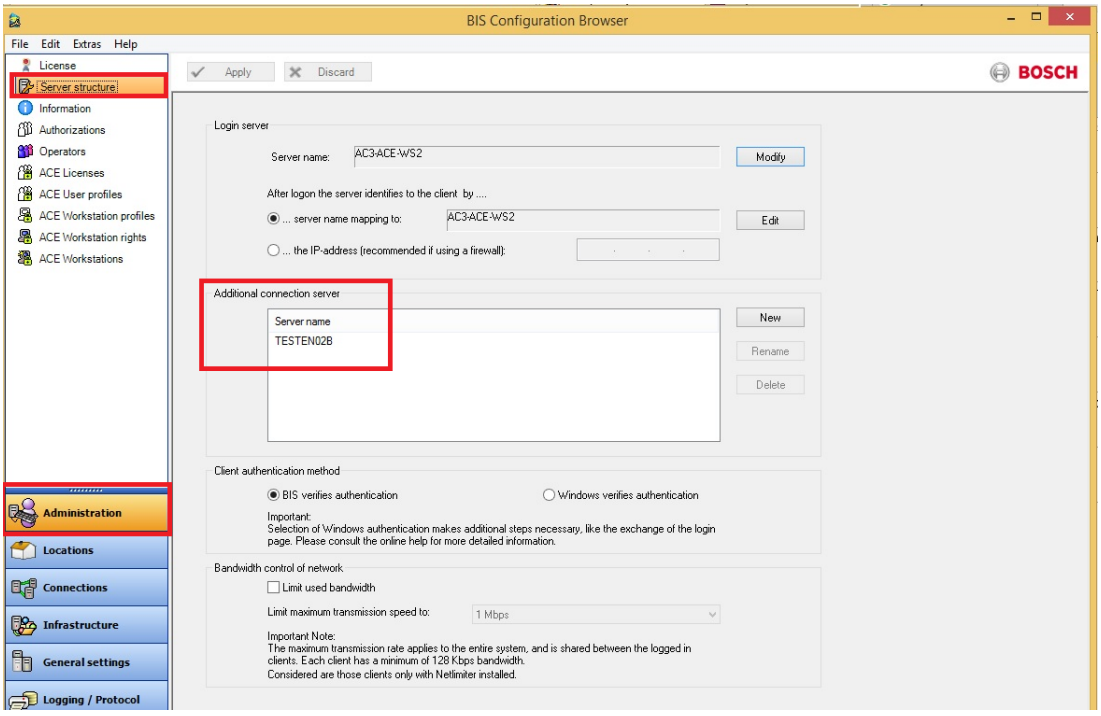
– Select the package **Door Controller**.
  Do **not** select any other features

Continue the installation. On this second installation you will find:

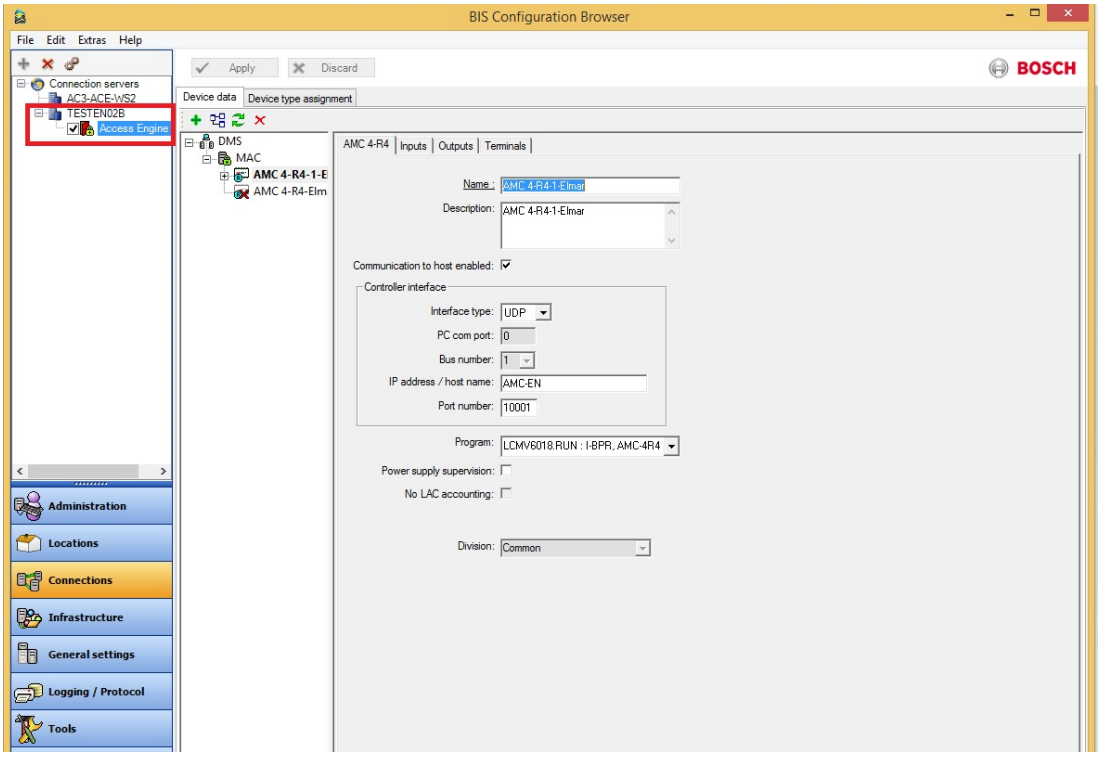
– The ACE services
– The ACE database

After the installation of the OPC Server, change to the BIS server machine to get the BIS-ACE parameterized and proceed as follows:

– Start the BIS Manager and login with BIS/BIS.
– Start the configuration.
– Create an Automation Engine configuration.
– Log onto this configuration.
– Activate demo mode.
– Navigate to **Administration** > **Server structure**
– Add the name of the host in which the OPC Server is installed as you can see below.



– Navigate to **Connections** and add a new connection using the server name as illustrated below:

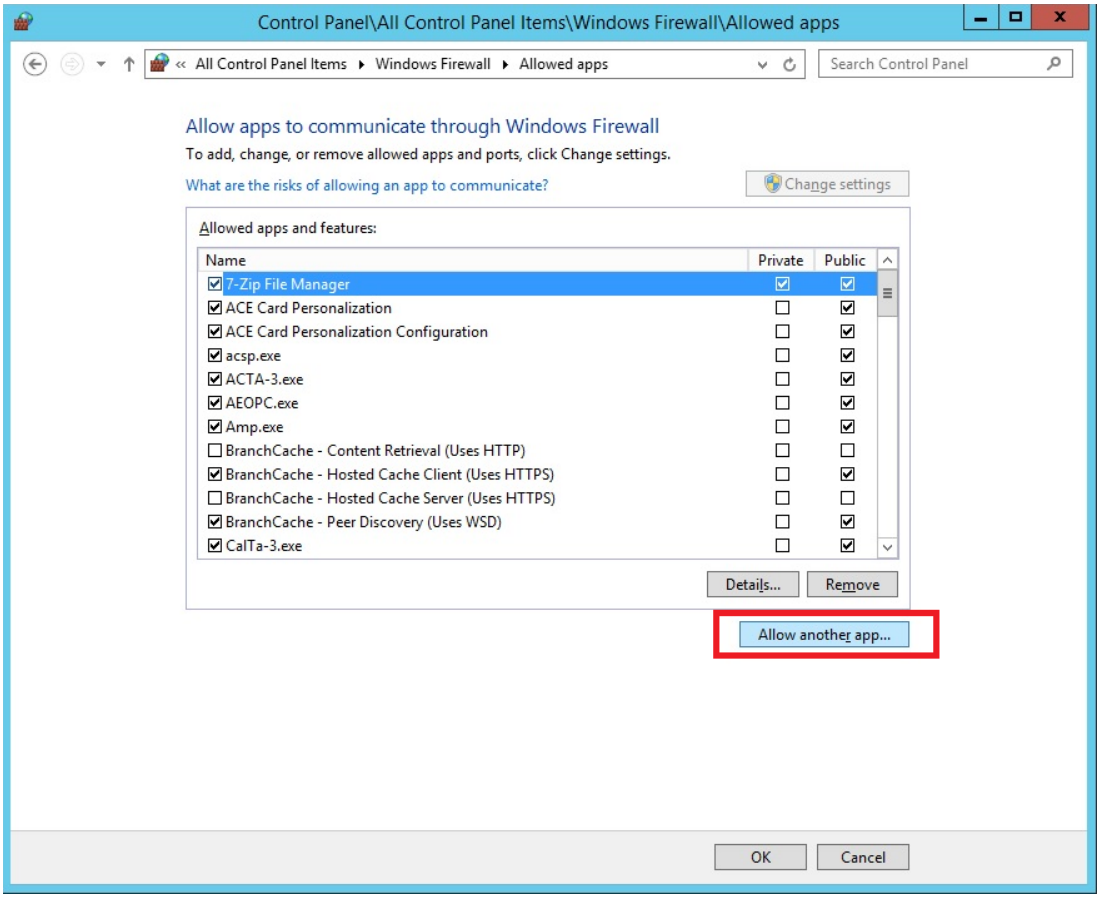


– Load the configuration in order to register the changes.
– Right click on the new added connections and select Add
– On the new window select Access Engine in order to add the ACE in the System.
– Then load the configuration again.

Notice!
When trying to add the ACE in the new defined connection, a message “This is not the actual connection” may be generated.
In that case close the Configuration browsers. Load the Configuration usual. Then you can properly define the Access Engine Connection.

Enabling the Access Engine Processes to work over Firewall

Complete the steps on adding process to Firewall using the Setting as below:



The firewall cannot be configured only by opening ports, because some ports are assigned dynamically.

Make the following settings instead:

1. Click Windows **Start** button > **Settings** > **Control Panel** > **Windows-Firewall**
2. Select tab **Exceptions**
3. Add the following programs, found in path [Install-path]`\MgtS\ AccessEngine\AC\BIN`

– ACSP.exe
– ACTA-3.exe
– AEOPC.exe
– CALTA-3.exe
– CDTA-1.exe
– GTM-2.exe
– Loggifier-2.exe
– Master-3.exe
– querySrv-2.exe
– REPS.exe
– TAccExc.exe

– SfmApp-4.exe (found in path [Install-path]`\MgtS\AccessEngine\CP\BIN`

– DMS.exe
– LAC.exe
found in path [Install-path]`\MgtS\Access Engine\MAC\BIN`

Communication between MAC and AMC:
– MAC connects to AMC via port 10001 (UDP)
– AMC connects to MAC (UDP configurable)

9.1.1 SQL Server for BIS database connections

The following settings have to be done on the PC where the corresponding SQL Server is running.

1. **Port settings (UDP):**

For Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2:
Start the Windows Firewall via “Start” - “Control Panel” - “Windows-Firewall”
Select “Advanced settings”, do the following for Inbound Rules
Add new Rule
Rule Type: Port (TCP)

For all Operating Systems:
– Allow UDP port 1434 for SQL Server Browser service

1. **Port settings (TCP):**

For Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2:
Start the Windows Firewall via “Start” - “Control Panel” - “Windows-Firewall”
Select “Advanced settings”, do the following for Inbound Rules
Add new Rule
Rule Type: Port (TCP)

For all Operating Systems:
– Allow TCP port 443 for SQL Server Browser service

1. **Program settings (Sqlservr.exe):**

For Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2:
Start the Windows Firewall via “Start” - “Control Panel” - “Windows-Firewall”
Select “Advanced settings”, do the following for Inbound Rules
Add new Rule
Rule Type: Program
Allow the following program:

For all Operating Systems:
– `C:\Program Files\Microsoft SQL Server\MSSQL10.(INSTANCE_NAME)\MSSQL\Binn\sqlservr.exe`

(In case of a 64 Bit Operating System the path can be
`C:\Program Files (x86)\Microsoft SQLServer\MSSQL10.(INSTANCE_NAME)\MSSQL\Binn\sqlservr.exe`)

9.1.2 SQL Server for BIS Reporting Services connections

The following settings have to be done on the PC where the corresponding SQL Server is running.
Allow Port (TCP) for ReportingServices, by default 8080.
To find out the port which is used from the SQL Server for the BIS Reporting Services:
Open “Reporting Services Configuration Manager” - Connect to the RS Instance you use with BIS - Open view for “Web Service URL” - the TCP Port number is available)

1. **Port settings (TCP):**

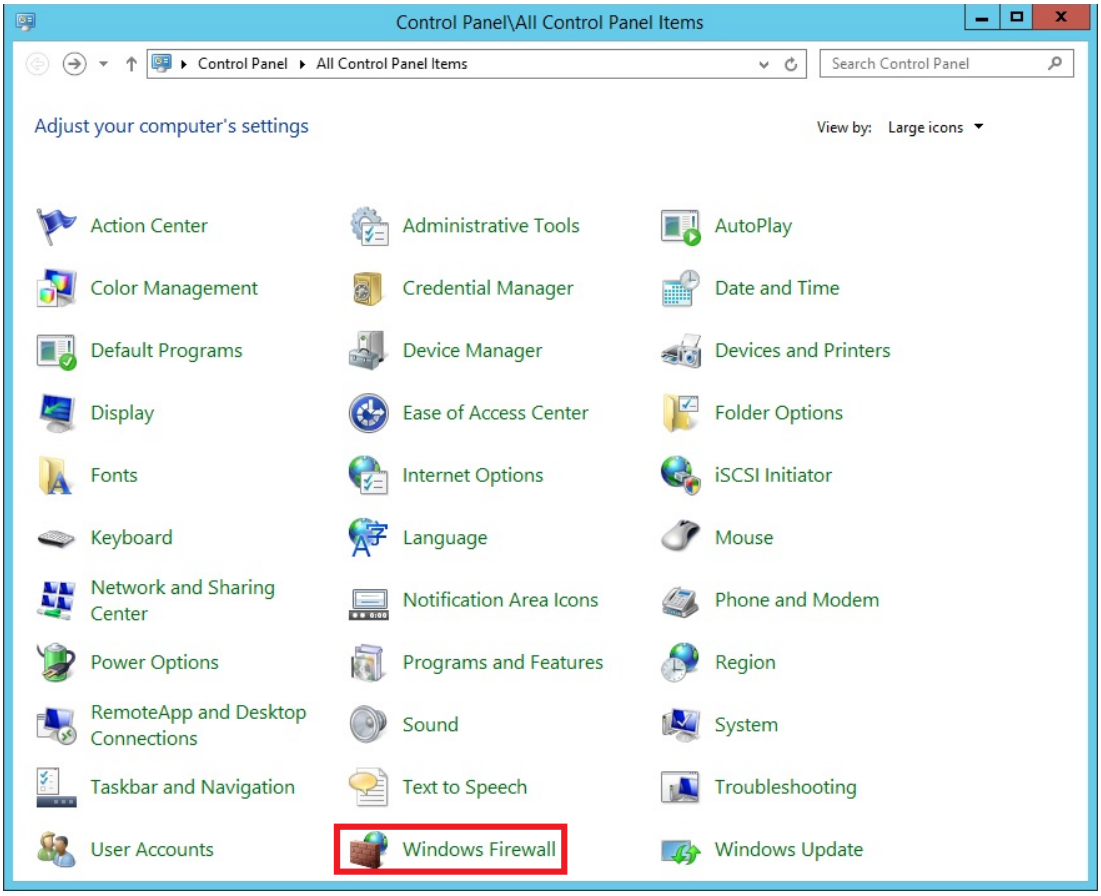
For Windows 7, Windows Server 2008 R2, Windows 8.1, Windows Server 2012 R2:
Start the Windows Firewall via “Start” - “Control Panel” - “Windows-Firewall”
Select “Advanced settings”, do the following for Inbound Rules
Add new Rule
Rule Type: Port (TCP)

For all Operating Systems:
– Allow TCP port (e.g. 8080) for BIS Reporting Service connections

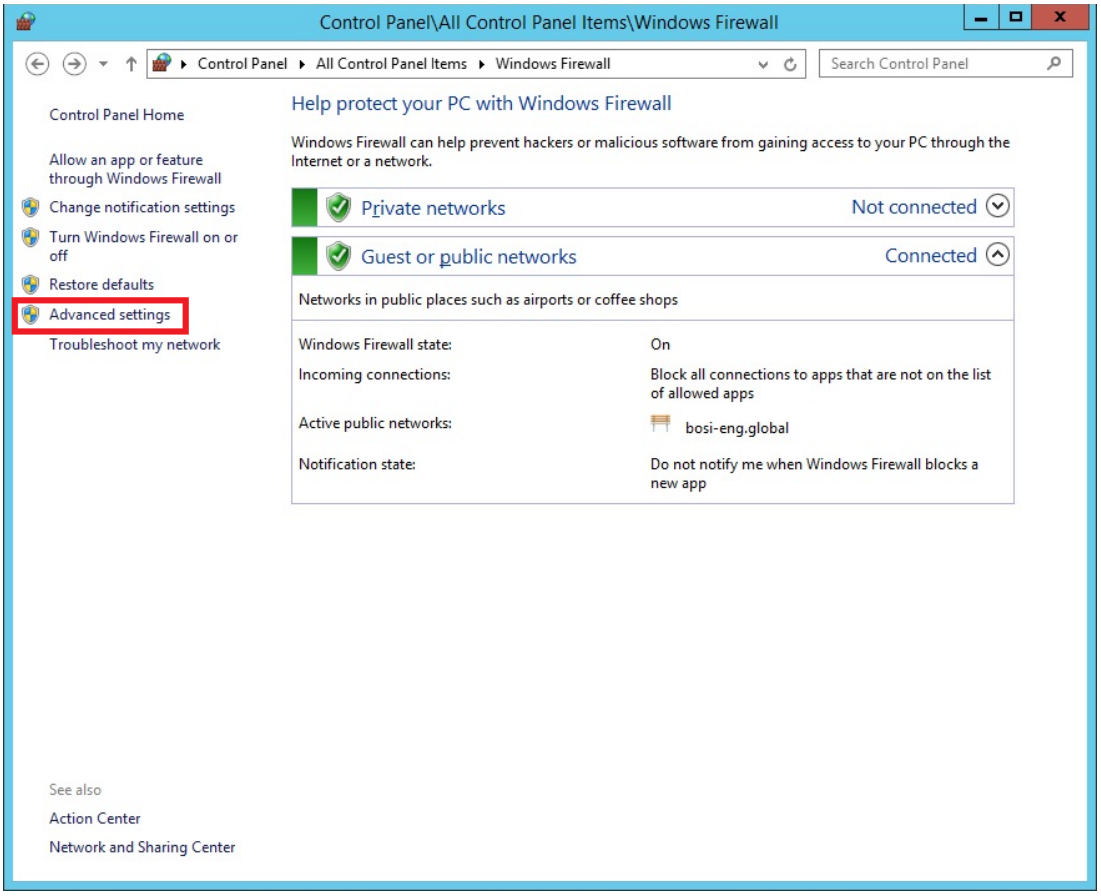
9.2 IPsec for a distributed system

Notice!
Note, that using the IPSec will reduce the system performance.

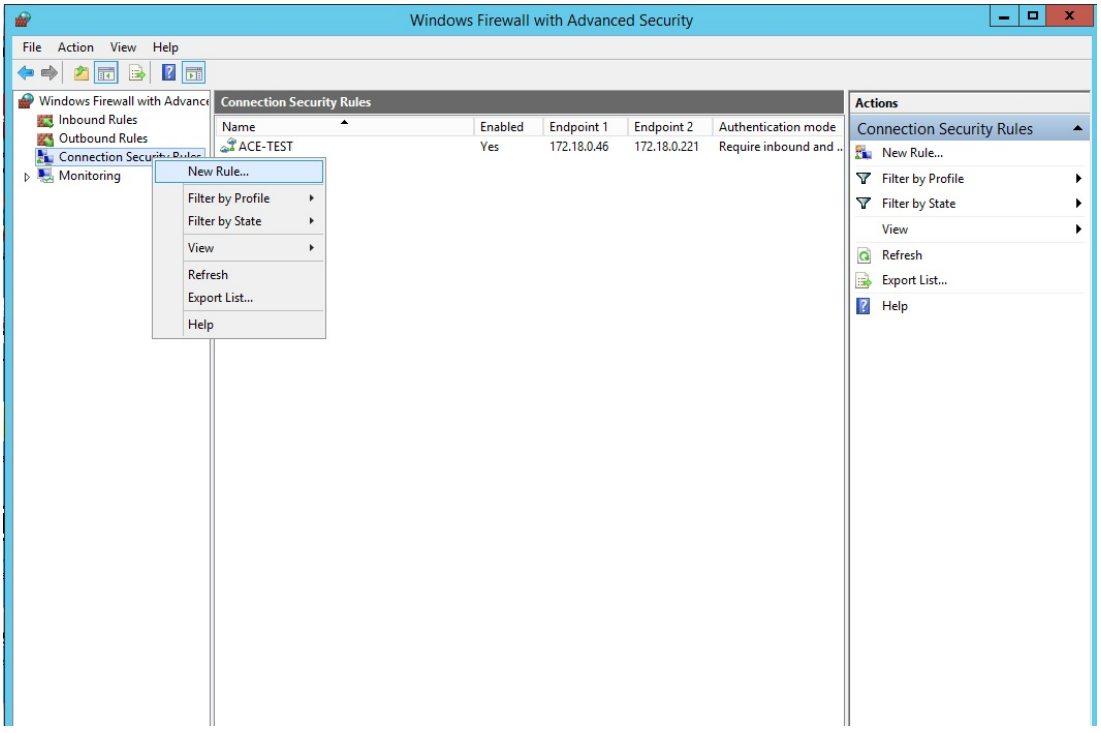
To start the firewall open the **Control panel**:



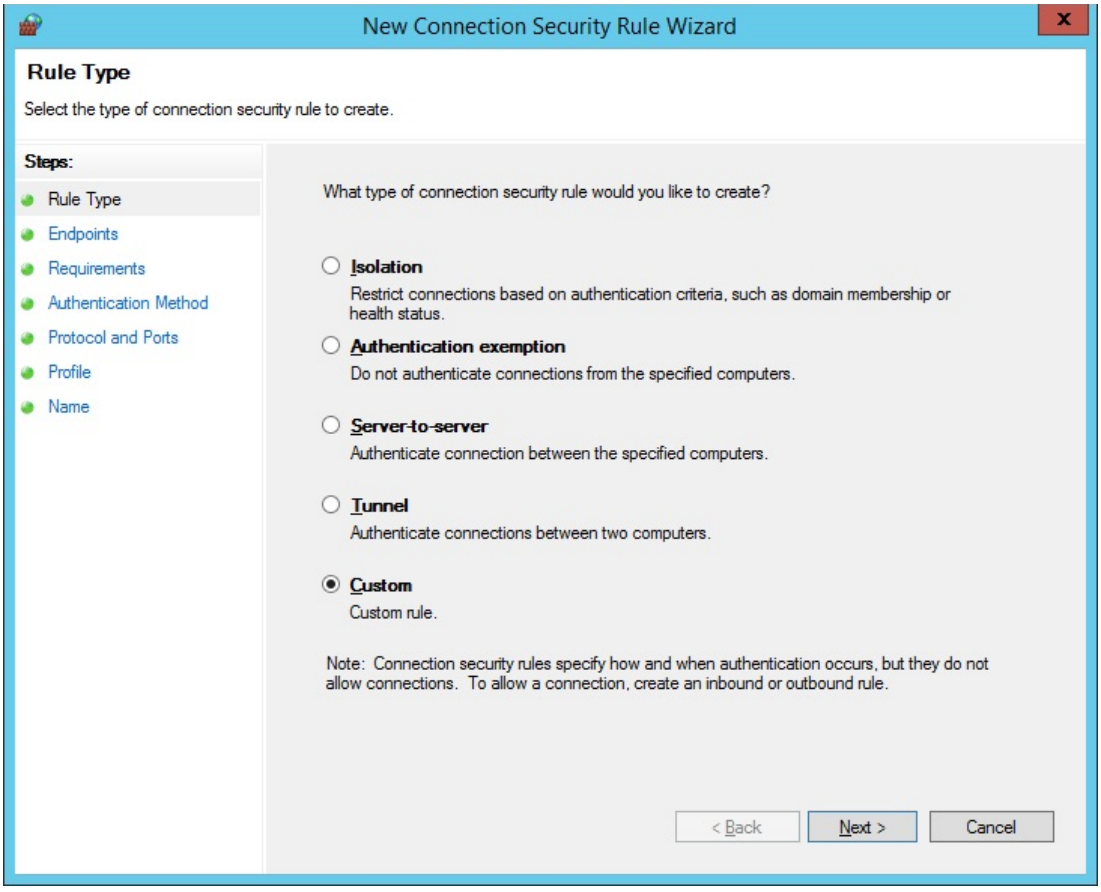
– Select **Windows Firewall**



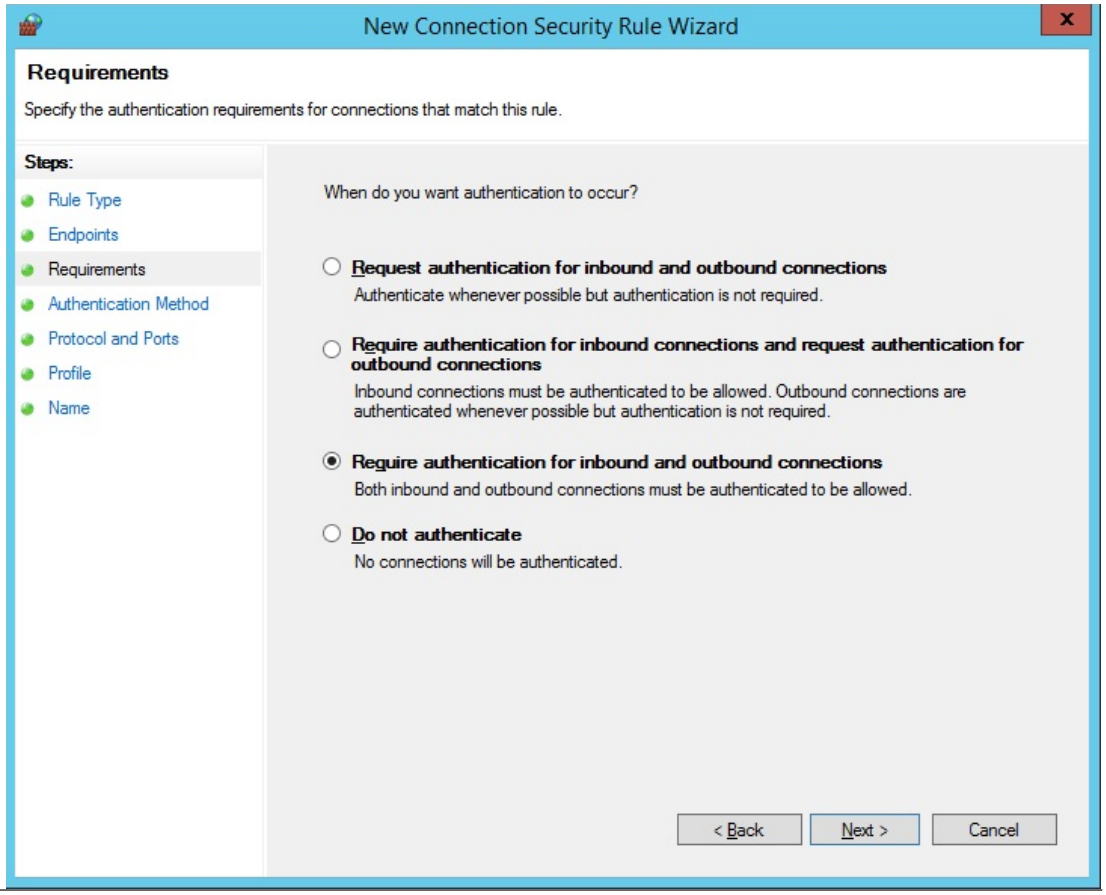
– Select **Advanced Settings**



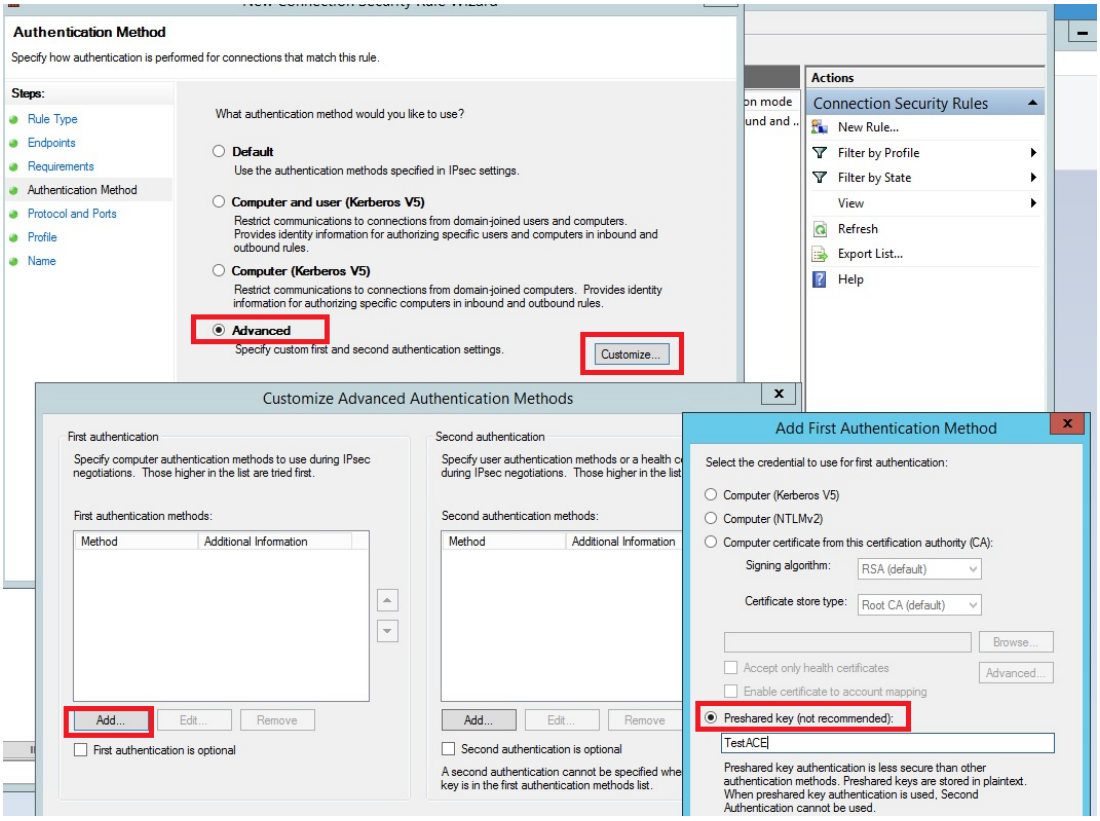
– Right click on **Connection Security Rules** and select **New Rule.**



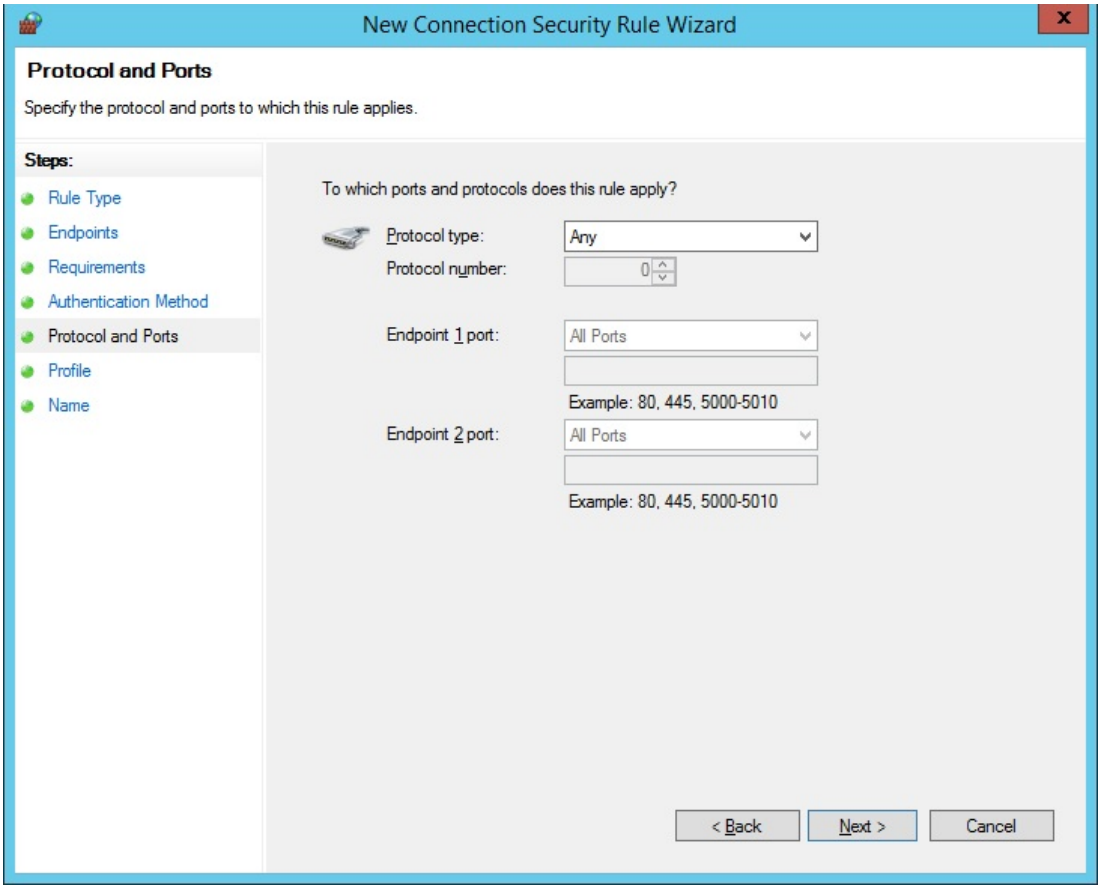
– Select **Custom** and click **Next >** to continue.



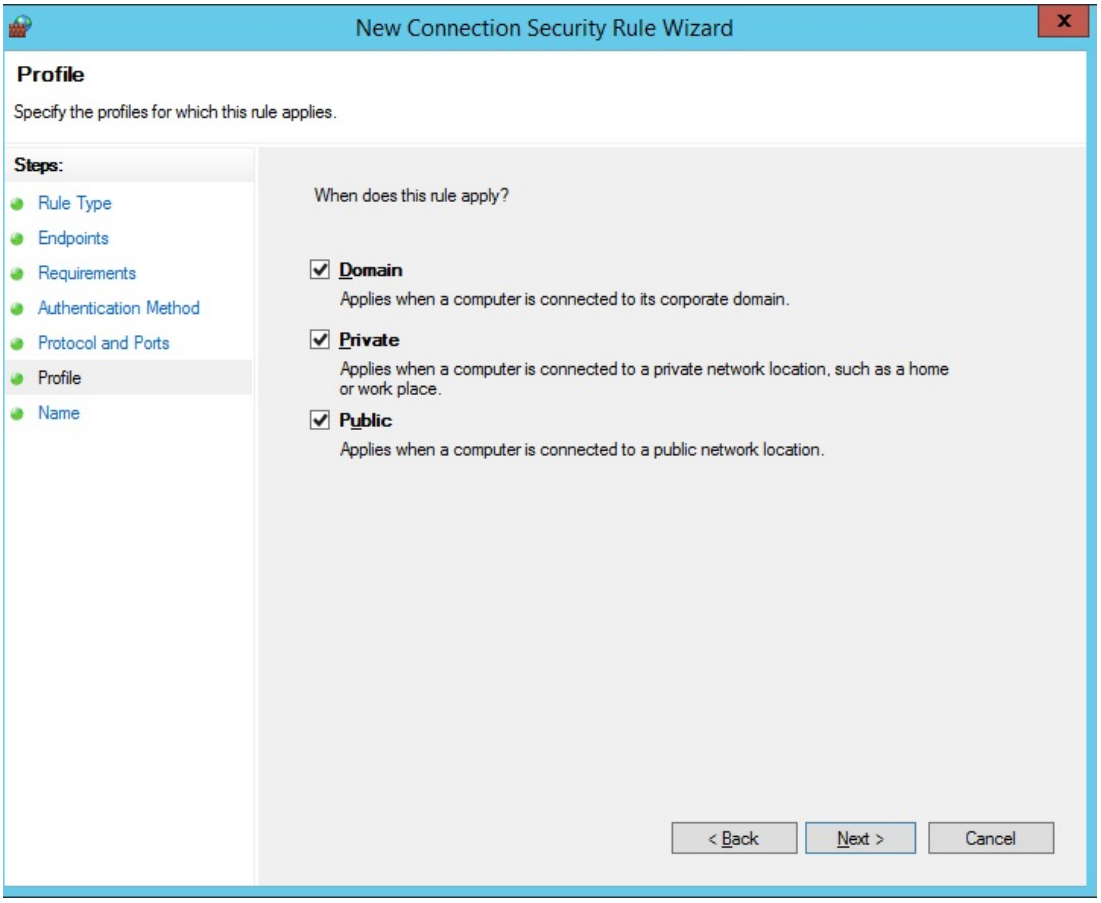
– Select **Require authentication for inbound and outbound connections** and click **Next >** to continue:



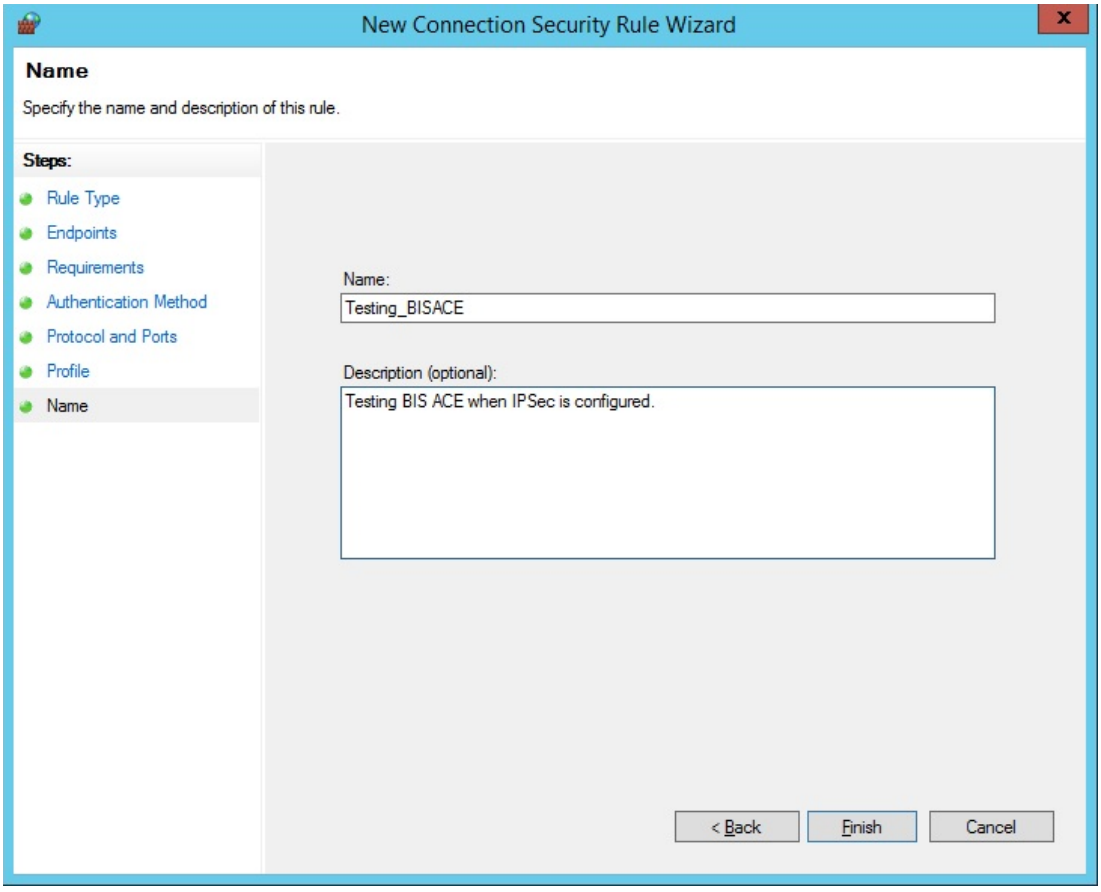
– Select **Advanced** and click **Customize**.
– On the next screen click **Add**.
– On the next screen select **Preshared key** and type a password into the Input field.
– Click **OK** to confirm and click **Next >** to continue.



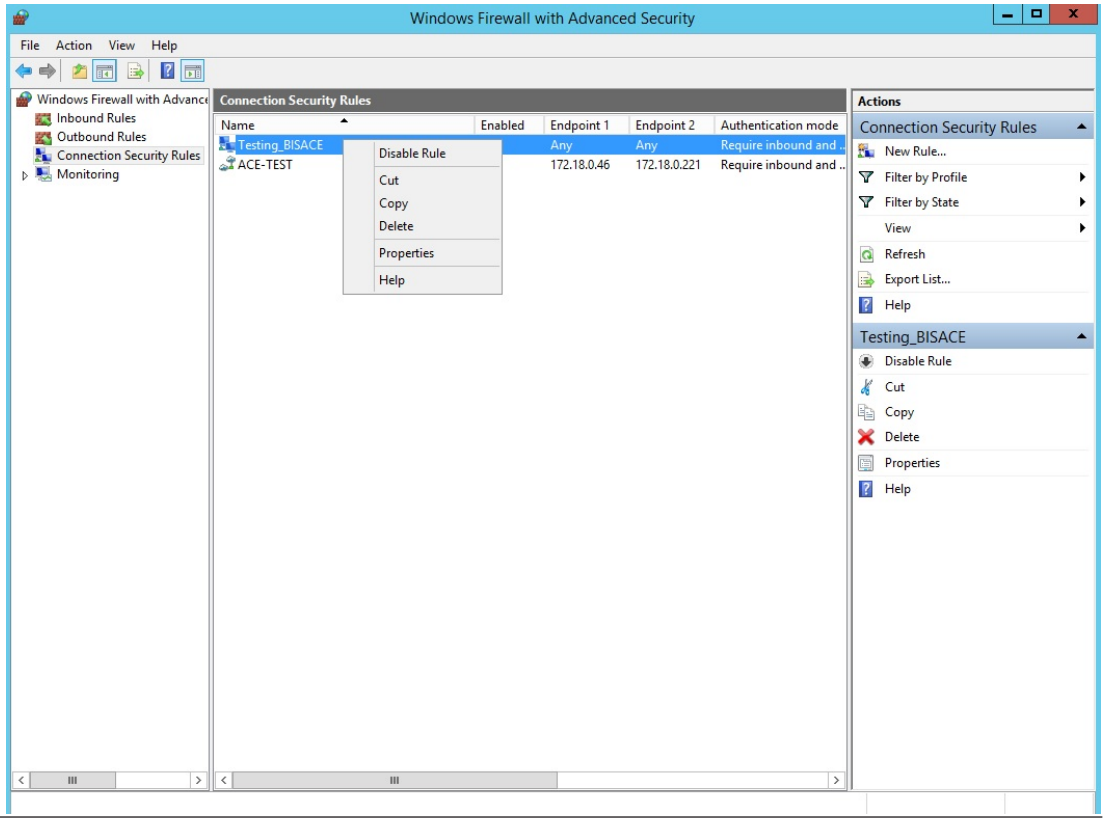
– On the **Profile and Ports** screen click **Next >** to continue.



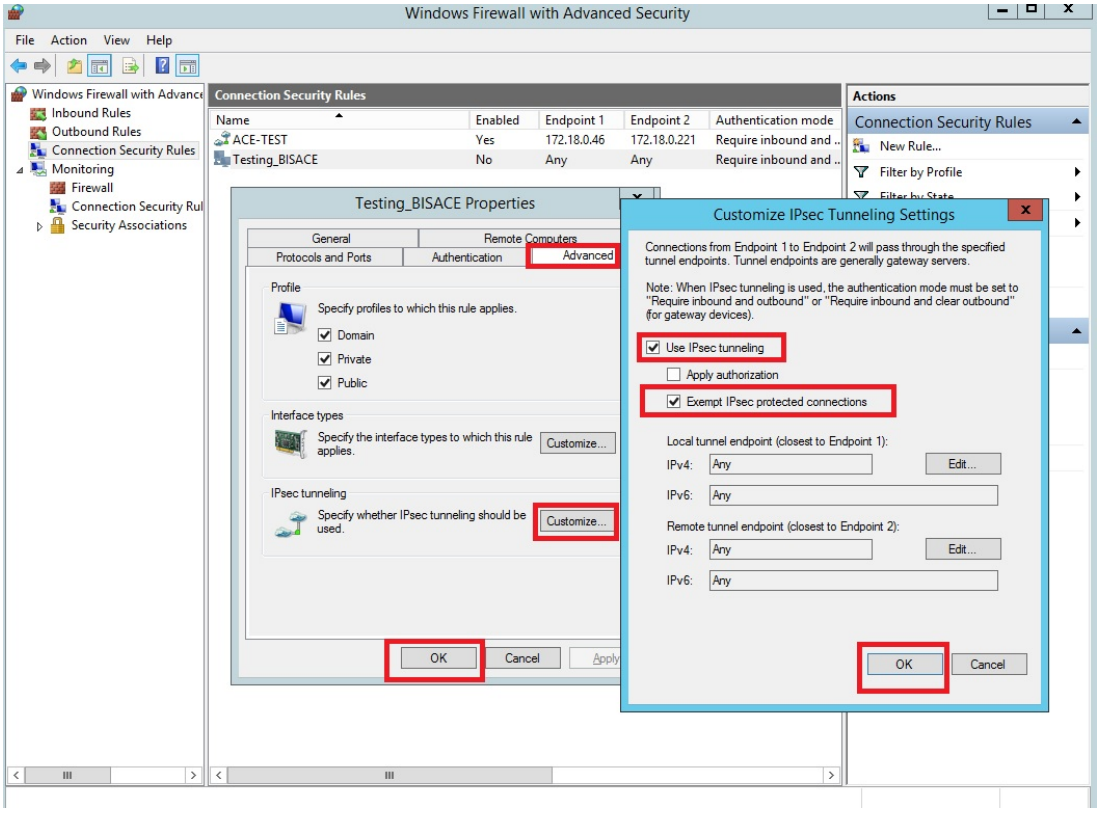
– On the **Profile** screen activate **Domain**, **Private**, and **Public** and click **Next >** to continue.



– On the **Name** screen enter the name and a description for your Connection and click **Finish**.



– Right-click on the new rule under **Connecting Security Rules** and select **Properties**.



– On the **Testing BISACE Properties** dialog select the **Advanced** tab and click **Customize** under IPsec tunneling. Then click **OK** to confirm.
– On the next screen **Customize IPsec Tunneling Settings** activate Use **IPsec tunneling** and **Exempt IPsec protected connections**.
– Then click **OK** to confirm and finish the action.

In order to enable IPsec on other machines which are part of your test set up, you have to repeat the steps as described above on each one of these machines.
If the first machine is the BIS server, the other machines could be the BIS_ACE client machine and the Connection server (OPC-machine).

10 Optimization of large installations

Introduction

This section describes the optimization of large installations of Access Engine (ACE) within the Building Integration System (BIS).

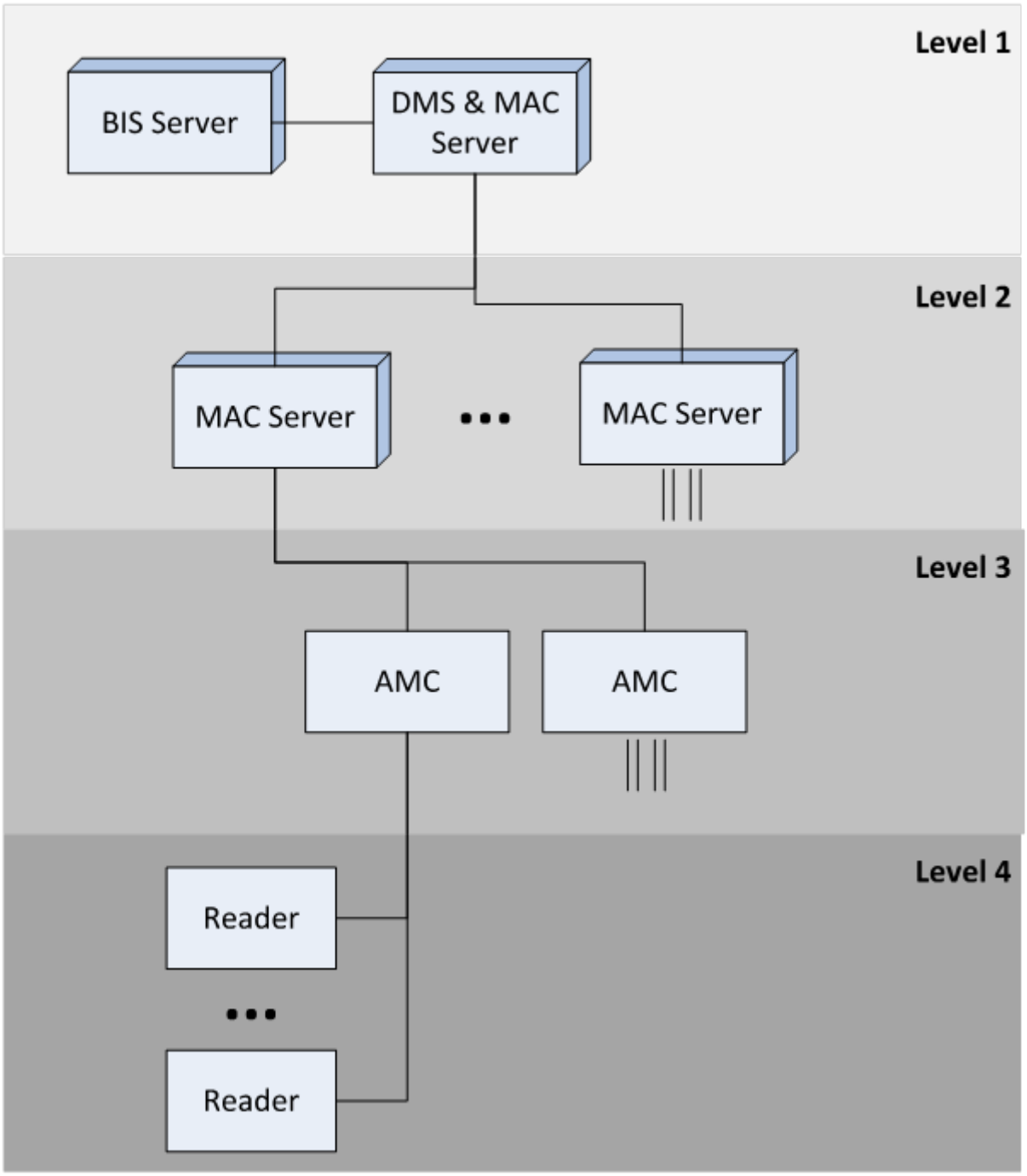
In a large ACE installation BIS handles the alarms and ACE handles the access control.

Overview

The Access Engine consists of:

– Database Management System (DMS)
– Master Access Controllers (MAC)
– Access Modular Controllers (AMC) to which the card-readers are connected.

The following illustrates the hierarchy of ACE



Master Access Controllers (MACs)

MAC servers are intended to provide redundancy at the level of a building. 1024 Authorizations are available per MAC server, and each MAC server can be in its own time zone. MAC servers can also be used for load balancing. The maximum number of MAC servers depends on the data volume. All messages from lower levels must be forwarded to the first level. The smaller the number of AMCs and card readers per MAC, the more MACs can be used.

For instance, 10 MACs with 100 AMCs each cause the same load on the DMS and BIS systems as 100 MACs with 10 AMCs each.

There is only ever one BIS with one DMS system. For this reason their hardware should be generously proportioned: for example multi-processor systems with fast storage, a minimum of 1 Gbit, preferably 2 Gbit network adapters, and sufficient memory.
MAC servers on the second level need not be so generously proportioned, but should take account of the number of AMCs and the amount of traffic at the card readers. Bosch recommends between 100 and 150 AMCs per MAC.
Recommendation: In general it is safer to have one MAC too many than one too few, and consequently system overloads and insufficient Authorizations.

10.1 Considerations for capacity planning

The following points should be considered when planning a large installation

Number of card readers per AMC
Each AMC can serve 8 card readers, however the simultaneous use of all 8 leads to poor response times, because the AMC tries to send all requests to the same MAC concurrently.
Recommendation: Do not connect all 8 readers to an entrance which is prone to peak traffic periods, e.g. a main entrance.

Number of AMCs per MAC
Each MAC can serve up to 150 AMCs, which in turn can serve 8 connected card readers. Each time a card is read the AMC checks with the MAC whether the cardholder is authorized. This is especially time-consuming where anti-passback or access-sequence controls are in operation.
Recommendation: At heavily frequented entrances connect fewer AMCs per MAC
Recommendation: Activate the setting **DMS** > **MAC** > **AMC** > **Reader > tab: Door control** > **Open door if no answer from host**
If the MAC fails to respond this setting will activate offline mode, and allow the AMC to make its own access decisions.
Recommendation: If using the simpler door models, set the parameter **Host request timeout** to **0**. This allows the AMC to make its own access decisions at all times.

Overload of the DMS/1.MAC on the main server
It is a potential bottleneck if the 1.MAC resides with the DMS of the Access Engine and BIS on the same server computer.
Recommendation: The 1.MAC should serve fewer or less-busy AMCs.
Recommendation: Use full versions of SQL Server for BIS and ACE databases and locate these on separate computers with fast network connections.
Recommendation: Install BIS and ACE on separate server computers.
Recommendation: Besides network and CPU, disk I/O is crucial to the performance of ACE. Storage should be optimized for small, rapid bursts of I/O.
Recommendation: Deactivate debug-logging in the DMS and on every MAC (see separate documentation for the deactivation of log files).
Recommendation: Other CPU-hungry OPC servers should be located on their own Connection server computers.

Effect of BIS downtimes
Alarms and messages from ACE are passed to BIS via an OPC server. If BIS goes offline the ACE messages are buffered for later re-synchronization with BIS. The longer the downtime, the more time-consuming is the re-synchronization when BIS returns.

In addition, when BIS restarts it runs all the Associations (“Triggers”) for the messages accumulated in the last 5 minutes of downtime.
Recommendation: Reduce the number of minutes of accumulated messages. The default value of 5 is set in the following registry key:
`HKLM\SOFTWARE\Wow6432Node\Micos\SPS\DEFAULT\AEOPC\DeltaTOnline\@value=5`
Note: If you change this parameter, messages and alarms that are older than the number of minutes in the parameter `@value` will no longer be processed.

Performance-relevant registry entries
The following registry entries can be used to reduce data traffic between BIS and ACE, and thus improve performance.
`HKLM\SOFTWARE\Wow6432Node\Micos\SPS\DEFAULT\AEOPC`

EnableAreas	Messages about the number of persons present in a designated **Area**
EnableDBChanges	Messages about each individual database change
EnableImportExport	Turns import/export messages on and off
EnableMsgCopy	Copies all parameters, including values, to an attribute
EnablePatrols	Turns messages about guard patrols on and off.

Recommendation: Set the `@value` for the following entries to `0` (zero) and reboot:
EnableDBChanges and **EnableMsgCopy**
Recommendtaion: If no ACE Divisions are required, remove the line `OPCUSTOMER1` from the **GlobalParameters** database table.

Assignment of readers to Authorizations
When a reader is assigned to an Authorization the MAC re-sends all authorized cards to the AMC controllers,
Recommendation: Put as many card readers as possible into each ACE Authorization. This will make the assignment of multiple card readers to persons much more efficient.
Recommendation: if multiple readers are to be assigned to an Authorization, then assign them in a single batch (saving only once). Otherwise the authorized cards are transmitted to the AMCs after ever change.
Recommendation: if possible, create the Authorizations (along with their assigned readers) before assigning them to persons with cards.

Using digital inputs and outputs (DIPs and DOPs)
Data traffic between MAC and DMS and BIS is increased considerably whenever BIS sends commands to or queries the status of digital inputs and outputs. A small mistake in the programming of DIPs and DOPs in BIS can severely hinder data traffic.
Recommendation: Use the DIPs and DOPs only for relatively rare alarms.

Avoiding two thirds of all access messages
Besides the access message itself, each entry or exit at a reader creates the **Door open** and **Door closed** messages.
Recommendation: In the BIS Configuration Browser, deactivate the door open/closed messages under
DMS >**MAC** >**AMC** >**Door** >**Events** > **Door state open\close**

Note: Any messages from configured door sensors will still be processed, as will the message **Door open too long**

Mitigating MAC cold-starts

During a MAC cold-start, the MAC receives its data updates automatically, but is not fully operational until the last record has arrived. This downtime can be considerable in the case of large data volumes (over 10,000 records).

Access sequence controls are only possible when the MAC is fully updated; therefore communication between the MAC and its AMCs is suspended during the update.

Recommendation: Activate the setting **DMS** > **MAC > AMC > Reader > tab: Door control** > **Open door if no answer from host**

During the time where the MAC is unable to respond, this setting will activate offline mode, and allow the AMC to make its own access decisions and admit known, authorized cards.

Avoiding cold start of the 1.MAC during BIS upgrades

Every BIS upgrade automatically triggers a cold start of the 1. MAC . For treatment of subsidiary MACs see the next section. Nevertheless the cold start of the 1.MAC can be avoided provided there have been no changes to the MAC software between the two BIS versions.

This procedure may be worthwhile if large data volumes are involved, and their transfer would cause excessive downtime for the 1. MAC.

Prerequisites: Technical support has confirmed that there has been no change in the MAC software between the BIS versions.

1. Deactivate **all** MACs in BIS Configuration Browser:
   Menu: **Connections** > Pane: **Connection servers** > **AccessEngine** > Pane: **Device data** > **DMS** > **MAC**
   On the **MAC** tab, clear the check box labeled **Active**
   Result: The MAC icon appears overlaid with an **X**
2. Stop the MAC's Windows service:
   Windows **Start** > **services.msc**
   Stop and deactivate the service **Access Engine (MAC)**
3. Create a backup of the MAC database: Make a copy of the folder <installation drive>:**\MgtS\Access Engine\MAC**
4. Proceed with BIS Upgrade. Note that the upgrade process will still trigger the cold start, but the MACs will not respond, because they were deactivated at the start of this procedure.
   DO NOT allow the upgrade process to reboot the system at this time, but first...
5. Verify that the MAC's windows service is still deactivated (see the procedure above)
6. Reboot the system
7. Copy the .DAT and .IDX files from the Db folder of the MAC backup (see above) into the now updated folder <installation drive>:**\MgtS\Access Engine\MAC\Db**
8. In **services.msc**, set the **Access Engine (MAC)** service to **Automatic** and re-start the service.
9. In the Configuration Browser, reactivate the 1. MAC:
   Menu: **Connections** > pane: **Connection servers** > **AccessEngine** > pane: **Device data** > **DMS** > **MAC**
   On the **MAC** tab, select the check box labeled **Active**
   Result: The MAC icon appears without the **X**

10. Reactivate the communication with each AMC individually. Note that the BIS upgrade procedure deactivates the AMCs, but does **not** reactivate them afterward. This gives the installer the opportunity to test the upgraded system thoroughly, piece by piece.
    In the Configuration Browser click menu: **Connections** > Pane: **Connection servers** > **AccessEngine** > Pane: **Device data** > **DMS** > MAC > AMC
    Select the check box **Communication to host enabled**
    Result: The AMC icon appears without an **X**
11. Thoroughly test the configuration by makings bookings at readers and sending commands to entrances.

Testing a BIS-ACE upgrade

During a BIS-ACE software upgrade all AMC controllers are deactivated. This gives the installer an opportunity to test the update on individual controllers.
Recommendation: Activate the setting **DMS** > MAC > AMC > Reader **> tab: Door control** > **Open door if no answer from host**
this setting (the default setting) will activate offline mode, and allow the AMC to make its own access decisions. It mitigates the bottleneck of only a small subset of MACs being online.
Recommendation: After an update reactivate only 1 or 2 MACs, or 10-20 AMCs, at a time, and allow a few minutes between phases of reactivation.

Avoiding or allowing cold starts on subsidiary MACs

During a BIS upgrade Subsidiary MAC servers should have their software updated before they resume communication with the newly upgraded DMS MAC system. In contrast to the BIS upgrade procedure on the 1. MAC server, the upgrade on subsidiary MAC servers always prompts as to whether a cold start is desired.

Planning personnel imports carefully

If several thousand personnel records require modified Authorizations, updates or deletion then plan the import for a time of least impact to the users.
Note: It does not matter whether you are starting the import from a group dialog, or an application using the API in a background process.

Assigning online and offline (“PegaSys”) Authorizations

The ACE dialog **System Data** > **Authorizations** allows you to assign both normal online Authorizations and offline “PegaSys” Authorizations, on their respective tabs.
Recommendation: Allow the Authorizations time to spread through the system down to the controllers, even after the dialog itself shows the desired settings. To be certain, an installer can see in the UDP-log of the MAC whether records are waiting to be transmitted to the AMC.
Recommendation: The process of assigning Authorizations can be shortened for individual cards by using an enrolment (read/write) card reader from the ACE dialog **Personnel Data** > **Cards** > tab: **PegaSys** > button: **Encode card**

Transmission of offline (“PegaSys”) Authorizations

Unlike online Authorizations, offline (“PegaSys”) Authorizations do not start to work when the first set of card data has been sent to the AMC controller. Offline Authorizations are not transmitted to the controllers until **all** sets of card-data, including online Authorizations, have been transmitted to the AMC controllers.

11 Achieving EN 60839

Introduction

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

– 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.

Special requirements for EN 60839-11 compliance

– EN 60839 Grade 4 requires OSDP readers with encryption enabled. Without OSDP or without encryption the configuration can only achieve Grade 3.
– EN 60839 Grade 4 requires Active Directory (LDAP) or Windows accounts for all operators of the access control system, and enforced password strength, including a minimum length of 8 characters.
– Network and electric cabling must be laid in a secure area or encased in pipes.
– 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.
– Only the card readers may be mounted in non-secured areas; all other devices must be in secured areas.
– The wiring of door contacts must not prevent the door's opening for an emergency evacuation triggered by a fire- or intrusion-prevention system.
– Any duress alarms must be made visible in the alarm-handling program (e.g. BIS).
– Verification PINs must have a minimum length of 4 characters.
– Identification PINs must have a minimum length of 8 characters.
– 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's **Host timeout** parameter must **not** be set to 0.
– The alarm-handling program (e.g. BIS) must be configured to sort alarms by priority.

12 Configuring SmartIntego locking systems

Intended audience

Persons responsible for the configuration of 3rd party locking systems within Bosch access control systems.

Introduction

As of version 4.6 ACE supports the integration of the SmartIntego digital locking system from Simons Voss technologies. BIS ACE supports 1 SmartIntego configuration per MAC .
SmartIntego applies two different methods of access control:

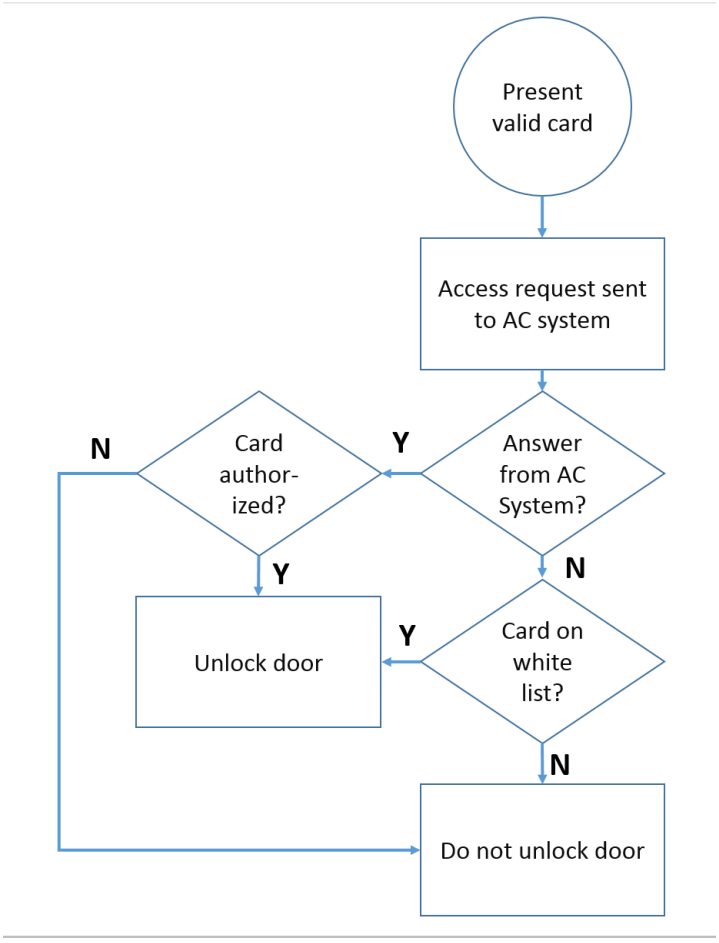
- **Centralized**: the SmartIntego locks are assigned via a Gateway access controller to a MAC.
  - All functions of the main access control system, such as location tracking, are maintained.
  - These functions are only available as long as the MAC is online.
- **Decentralized**: A whitelist is stored locally on the SmartIntego doors.
  - When a door is online, card numbers can be individually assigned to and deleted from the whitelist by the main access control system.
    Assignments are made in the **Cards** dialog (**SmartIntego** tab) of the access control system client. See the Operation help for details.
  - When a door is offline, it will unlock for cards that are stored on its whitelist.

Notice!

Logging of events while in offline mode
When a door comes back online, event logging is limited to whether or not the door was used at all while offline, **not** which card used it, when, and in which direction.

The authorization process with SmartIntego

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.



Prerequisites

- You have purchased the digital locking system and physically installed its hardware components at your site. These typically include, for online mode, SmartIntego Gateway access controllers, plus Locking cylinders or “SmartHandles”.
  SmartIntego includes configuration tools that are not part of the Bosch access control software.
- Your cardholders are using MIFARE Classic or MIFARE Desfire cards.
  SmartIntego uses the Card Serial Number (CSN), and this variant must be assigned to the cardholders in the ACE client, **Cards** dialog.
- You have received from the installer one AES -key per MAC, containing exactly 16 characters (8-bit ASCII only).
  Note: Ensure that this key and all passwords are kept safe. They are not recoverable if lost, and they are essential for extending or modifying the system.
- You have received from the installer a configuration file in CSV format, containing the names and network addresses of the hardware components installed.
  Note: The names of doors and locks can be modified after importing the configuration. These names will not be overwritten by subsequent imports.

Notice!
Do not edit the CSV file
Corrupt or unusable configurations may result.

Procedure

1. In the BIS Configuration Browser navigate to **Connections** > **Connection servers** > `<your ACE connection server>` > **Access Engine**
2. In the **Device data** column, select the MAC to which the GatewayNodes will be connected.
3. In the main window for the MAC, in the text field **AES-Key for SimonsVoss gateways** enter the AES key that you received from the installer.
4. In the **Device data** column, right-click the MAC and select **Import SimonsVoss configuration** from the context menu.
   A file selection window appears.
5. Select the CSV file that you received from the installer and click the **Open** button.
   A popup window appears
6. In the popup window, select what you wish to import; either:
   – all the changes in the CSV file
   or
   – only modifications and additions (i.e. no deletions).
7. (Optional) Click the **Details** button if you wish to preview the changes in a popup window. Click **OK** in that popup window to close the preview.
8. Click **OK**
   The changes appear in the Device data column under the selected MAC
9. Make any parameter changes you require (see next section).
10. Click the **Apply** button to save your changes.

Parameters for customizing the SmartIntego configuration

Introduction

The access control system provides SmartIntego-specific parameters for customizing the SmartIntego installation to your needs.

In the BIS Configuration Browser > **Connections** > tab: **Device data** tree select the Gateway , the entrance, the door or the reader, and set the following parameters, as required, in the main pane of the dialog:

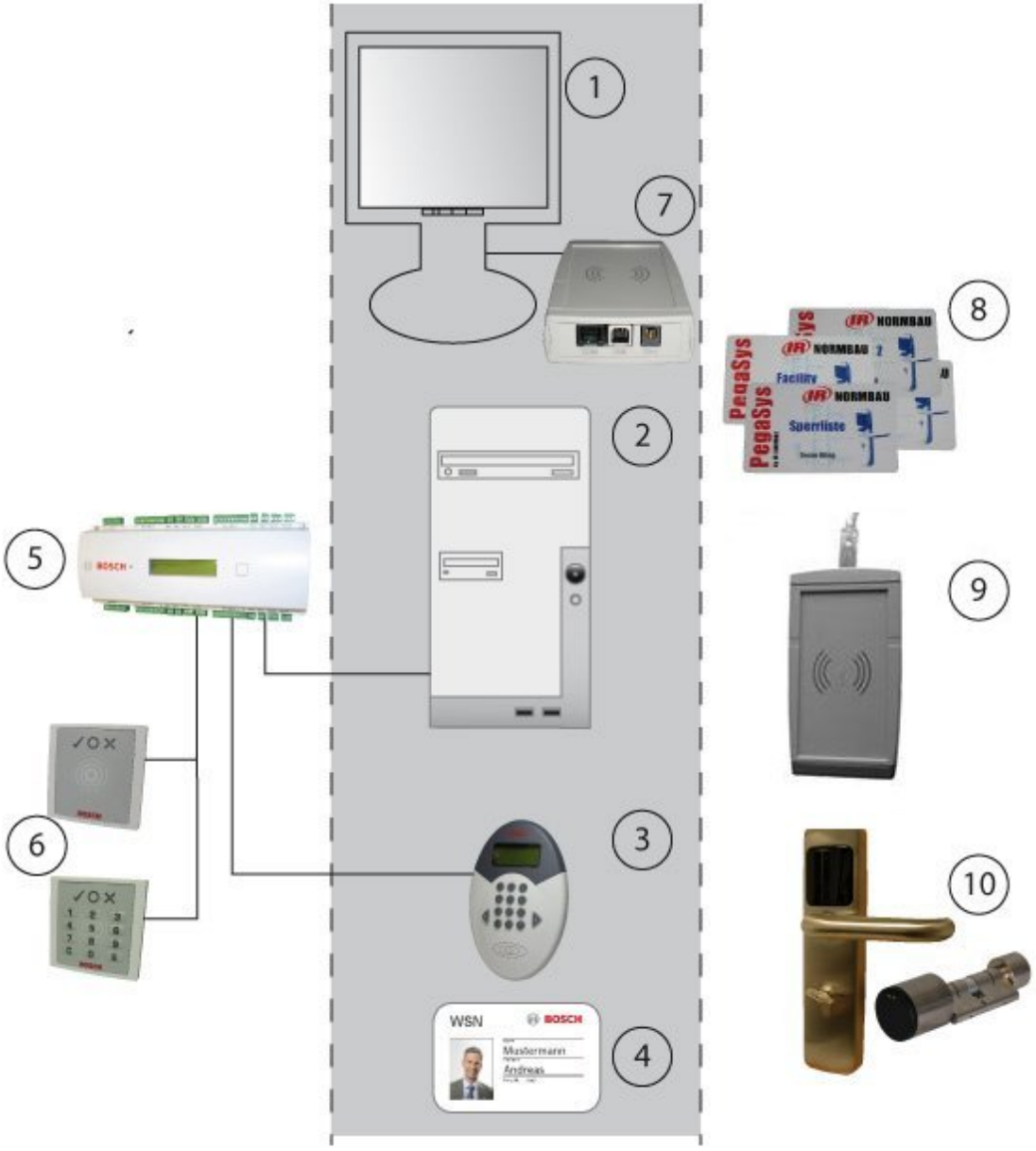
Parameters

Level in device data tree	Parameter	Values	Description
Gateway	**Gateway group**	Combo-box, either empty or containing integers	Gateway groups help to minimize radio frequency interference between Gateways. Gateways within the same group are polled sequentially. Therefore, in case of interference, assign Gateways that are located close together to the **same** group. If the Combo-box is empty, or you require a new gateway group, type an integer to create a new gateway group named by that integer. Otherwise, assign the gateway to the group by selecting one of the list entries.

Level in device data tree	Parameter	Values	Description
Entrance	**Waiting time external access decision**	Integer. Tenths of a second.	The entrance will try for this length of time to get a decision from the access control system, before searching its own whitelist for the card number.
Door (**Options** tab)	**Unlock door**	Check box	This option is recommended only for the configuration phase, not for daily use. If this option is selected, a valid card will effectively put the door into office mode .
	Max lock activation time	Integer. Tenths of a second.	The duration of the signal that unlocks the door. This may need to be increased for disabled persons.
Reader (**Additional settings** tab)	**Short-time activation**	Check box	If selected, the reader uses a standby-mode, which makes it more responsive at the cost of increased power draw.
	Check readiness	Radio buttons: – 1x daily – Every <integer> minutes	This option determines how frequently the system checks the reader for readiness. High frequencies increase the power draw.

13 Offline Doors - System components

The following sections describe the various components of ACE Offline Doors, focusing on elements that are common to ACE and ACE Offline doors.



13.1 Workstation

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

13.2 Server

The software for the access control system and the locking system runs on this computer [**2**]. The Configuration Browser for the BIS system is also used to configure the readers [**3**] for the locking system.
PegaSys data is managed in special tables of the Access Engine database.

13.3 DELTA read-write units

The following readers can be used as read/write units:
– DELTA 7020
– DELTA 1000 with special firmware
– DELTA 1010 with special firmware
At least one of these readers [**3**] must be available. Ideally, these are placed at entrances used on a frequent basis (e.g. the main entrance) so that authorization for the locking system is extended at the same time as access is granted to the secured facility.
However, it is also possible to install these readers at special locations, independently of the access control system, so that PegaSys rights are not extended automatically but have to be obtained specially.

13.4 Card

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

13.5 AMC2 4R4 Controller

An AMC2 4R4 [**5**] (= access control panel with RS-485 reader interface) is required for the DELTA 7020/1000/1010 [**3**] that is used as a read-write unit for the locking system.
The readers dedicated solely to access control [**6**] can use any protocols and read procedures, and can be operated with any AMC2 variant.

13.6 Access control readers

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

13.7 Read-write unit at the workstation

This device [**7**] is connected directly to the workstation computer via a USB interface and is used to transfer authorizations to user cards and system-related data (e.g. door and time initialization data) to special system cards [**8**]. It can be used simultaneously as an enrollment reader for cards from the online system.

13.8 System cards

Different system cards [**8**] are required for the locking system to transfer relevant data - e.g. initialization data - to the door terminals [**9**].
The following system card types are available for the locking system.

Facility cards
This card contains general system data such as system identification code, data type and record size. It is used as an "initialization card" both for the software and each door terminal.

Door initialization cards
Used for transmitting door data to the relevant door terminal.

Time initialization cards
Used for transmitting time models and the time to the door terminals.

Clock initialization cards
Used exclusively for transmitting the clock time (date and time accurate to the minute).

Blocked cards
Information about blocked cards can be transmitted to the door terminals using these cards.

Booking cards
Access data saved in the door terminals can be retrieved and transferred to the database using this card type.

Battery-replacement cards
Cylinders can not be opened for a battery change (for example) until a battery-change card has been read correctly.

Disassembly cards
The cylinder can not be removed from the door fitting until a disassembly card has been scanned at the door.

13.9 Mobile read-write unit (optional) - timesetter

In order for the times to be updated, particularly following a power failure at the terminals, this unit writes the current date and time to clock initialization cards. These cards can then be used to reset the terminals.

13.10 PegaSys - door terminal/cylinder

This read unit checks the identification of an individual door or its group against the access rights for the cardholder.
The access rights on the badge must be continually updated via special readers with write capability [**3**].
If an emergency opening is required, e.g. if the electronics fail, the terminals have mechanical cylinder locks.

14 Offline Doors - Device Data Editor

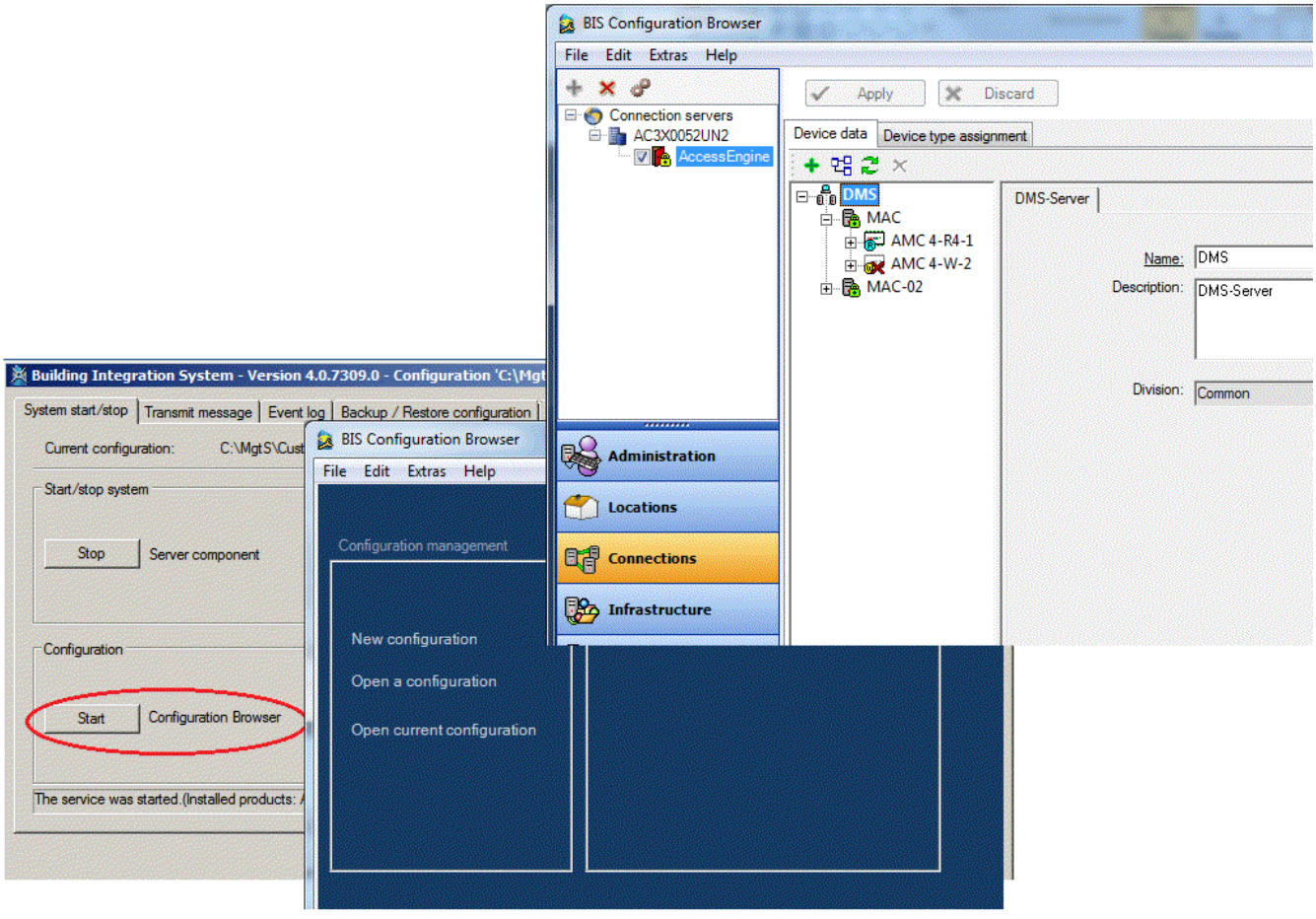
With the introduction of PegaSys components a new reader type (DELTA readers) has been created. This can be selected on an AMC2 4R4 in the Configuration Browser of the BIS system when an entrance is configured.
These readers with write capability are created as access control readers and are usually also assigned door control functions. However they can also be used simply for the offline system to load authorizations to the card.

Notice!
If a write function is required, it is necessary to use the DELTA 7020 reader.

14.1 Adding hardware components

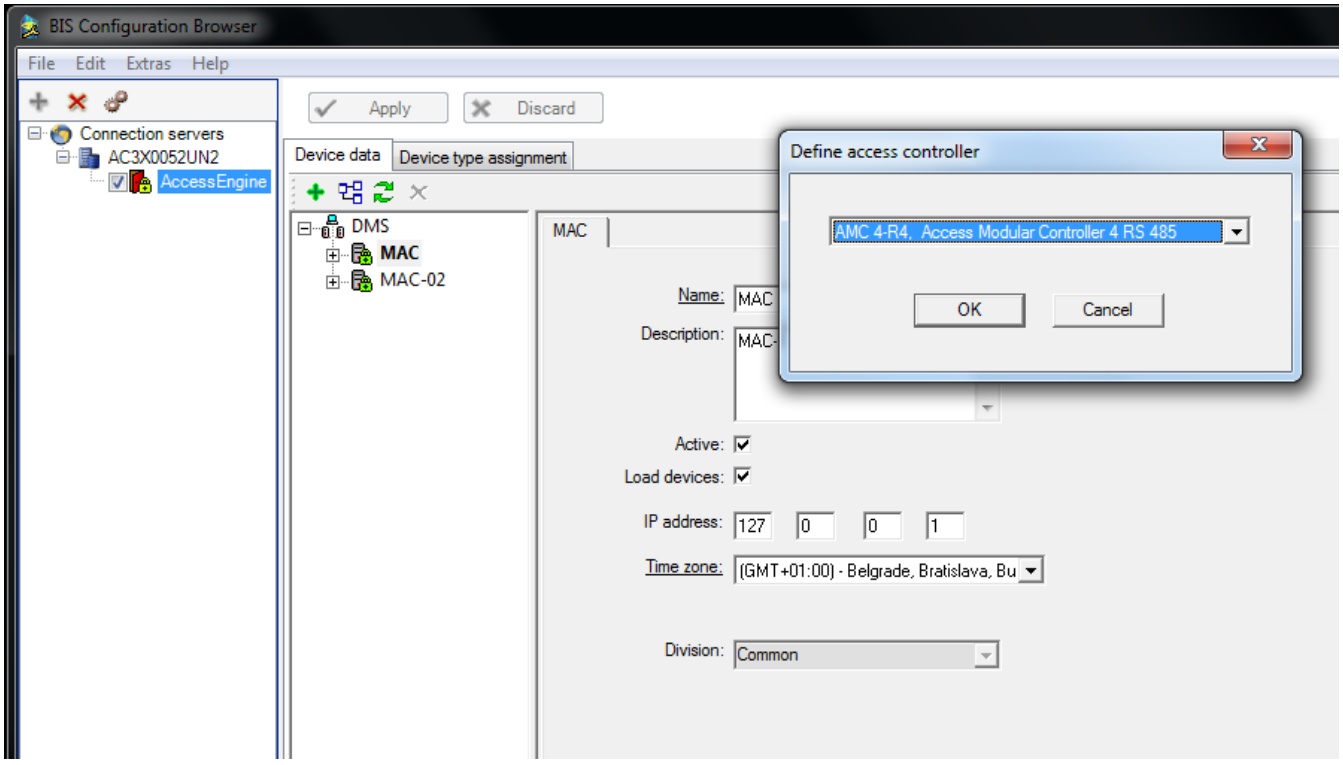
Open the Device Data Editor in the Configuration Browser.

- **System start/stop** tab in the BIS Manager
- **Start** button to launch the Configuration Browser
- Selection of loaded configuration and logon with authorized user
- **Connections** menu item
- Select the entry **AccessEngine** in the Explorer.



Devices are created in this dialog:

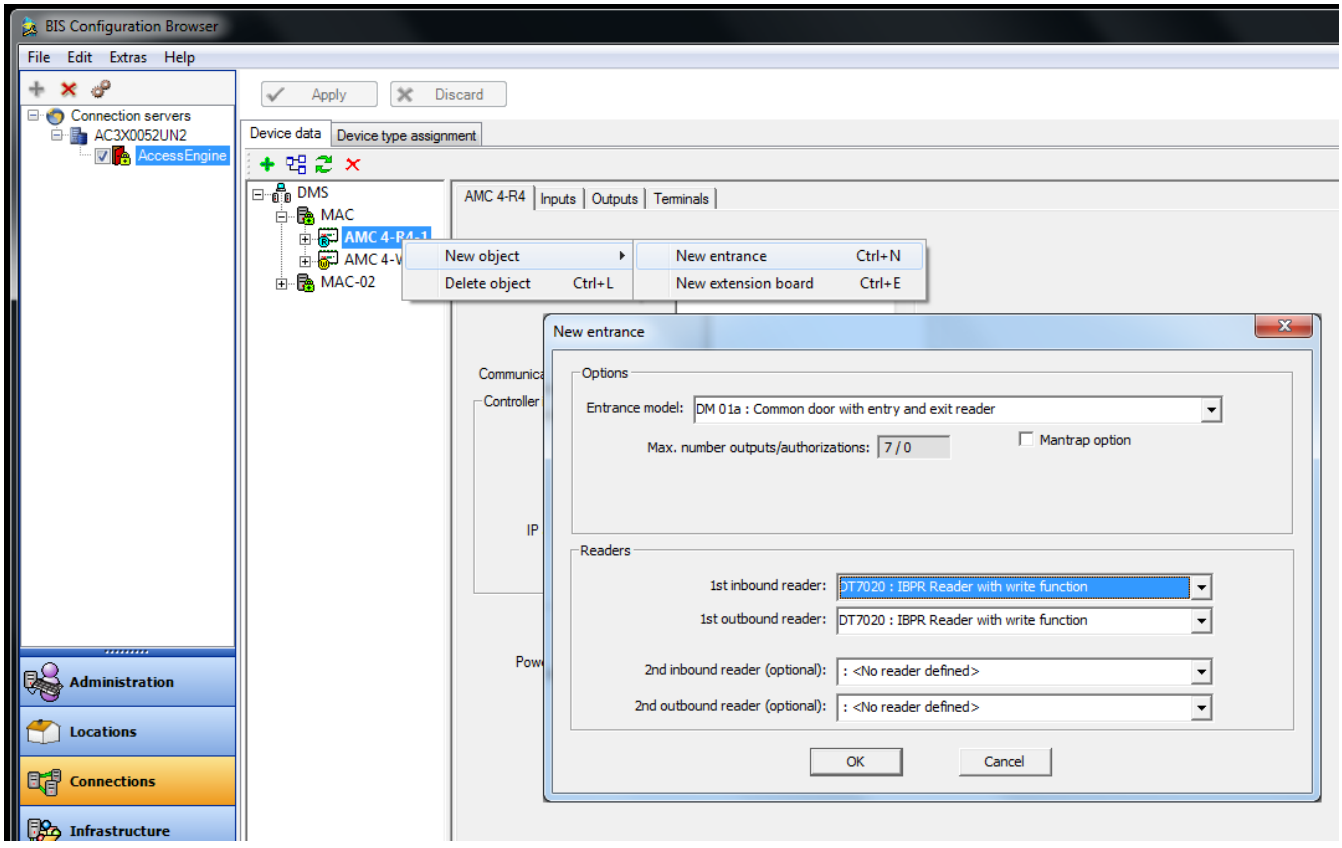
1. Select the entry **MAC** in the device overview.
2. Select the option **New object ...** in the popup menu .
3. Mark the entry **AMC2 4R4** in the selection dialog for the controller.



4. Select the option **New object ...> from the popup menu for the new controller New entrance**.
5. Choose the desired door model from the selection list.

Notice!
You can use any door model when creating the reader - more information about door models can be found under the item **AccessEngine** in the online help for the Configuration Browser.

6. Select the entry **DELTA 7020** for at least one reader.

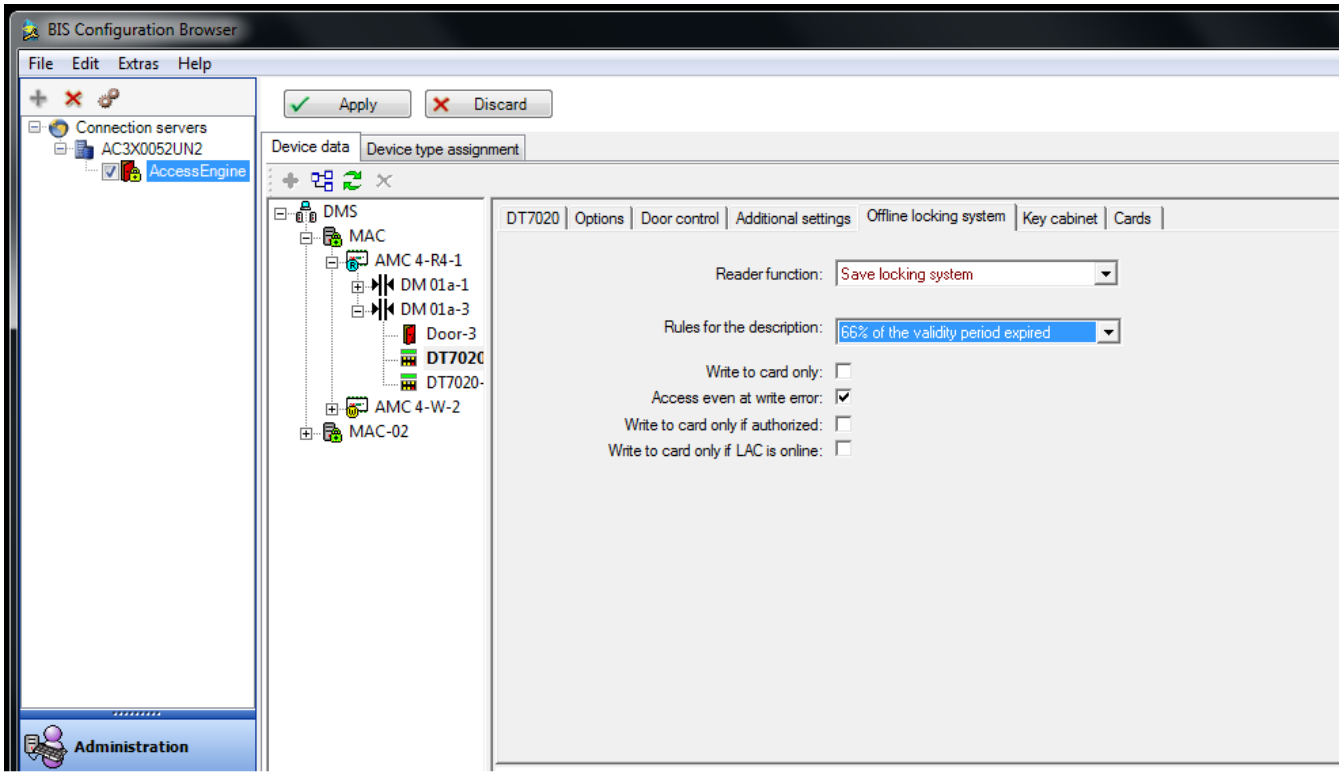


Notice!
The following readers can be used as read-write units for PegaSys authorizations.
DELTA 7020
DELTA 1000 (with special firmware)
DELTA 1010 (with special firmware)
To configure, select the entry **DELTA 7020** in the reader type list.

14.2 Configuring the read-write unit

If this reader is also used as an access control reader you may configure it as such. For further information about the relevant parameters, please see the online help for the BIS Configuration Browser.

Parameters for **extended reader functions**, which can be used to configure the settings for the locking system, have been combined on the **Offline Locking System settings** tab.



Reader function

Read only (= default setting)
This reader is purely an access control reader and is not part of the locking system.
All other parameters in this area are deactivated.

Read/Write
This reader has access control functions and is also activated for the locking system.
Activation of the following functions.

The drop-down list is only enabled when the selected reader type is a DELTA 7020.
The **Read only** setting prevents readers from using the Write function at certain times, for example, when offline system components are not available or (in cases where several write-capable readers exist) when only a select few are to have write-capability, such as during peak periods of use.

Write to card only

The access control and door control functions for the online system are deactivated.
Deactivated (check box is cleared (default setting)): The usual access control checks are performed after data is written to the card.
Activated (check box is selected): No access control performed after data is written to the card.

This check box should be selected if the reader is only used as a read-write unit for the offline system. Otherwise the additional signal traffic would cause unnecessary delays.

Access even with write error Access control (in the online system) does not depend on the success of the write process (in the offline system).
Access control is performed even after unsuccessful write attempts.
Deactivated (check box cleared): If it is not possible to write to the card, access is also denied.
Activated (check box is selected (default setting)): The write process has no impact on the access control.

Write to card only if authorized Rights for the locking system will only be written to the card if the cardholder has (online) access authorization for the entrance.
Deactivated (check box cleared (default setting)): Data is always written to the card.
Activated (check box selected): Data is only written to the card if valid authorization is present.

If the check box is selected the write process will be prevented, even if authorizations are only temporarily suspended (e.g. by a time model).

Only write if LAC online The rights are only written to the card or updated when the Local Access Controller (LAC) is guaranteed to have received the latest data from the access control system. For security reasons any deletions due are always performed.
Deactivated (check box is cleared (default setting)): Data is always written to the card.
Activated (check box selected): Data is only written when there is a connection between the controller and MAC.

If this check box is selected and the check box **Access even on write error** not selected, then the online system denies access if the LAC/MAC link is broken and the card's offline data is not up-to-date.

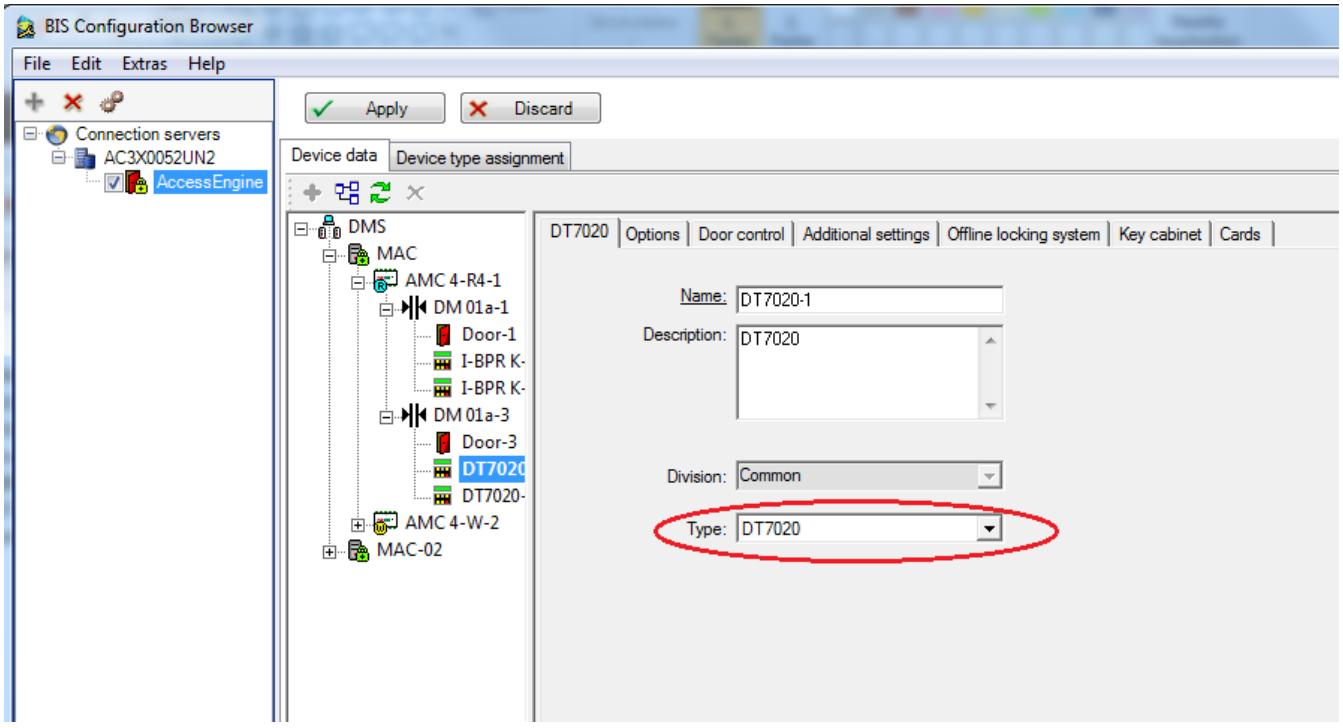
Rule for writing In the default setting, the validities are extended when two thirds (66%) of the validity period specified for the person has expired. See also .
This parameter can be used to extend validity periods by individually specified amounts.

Possible values:
Locking system specification
Always write
[when ... of the validity period has expired:]
16%, 33%, 50%, 66%, 83%, 100%

Locking system specification - see *Standard validity, page 197*.

14.2.1 Changing the reader type

As a rule, readers with write capability are installed at major entrances (e.g. as the entry reader at the main entrance), so that when personnel enter the site in the morning, the access rights for the locking system are automatically updated.
When refitting an installation with PegaSys, at least one reader in the facility must be replaced with a write-capable reader. The Configuration Browser on the BIS system does not allow the subsequent modification of door models and their readers.
Staying with the example of the entrance reader at the main entrance, the existing entrance would need to be deleted and a DELTA 7020 reader added in its place.
If an existing entrance is deleted it is also removed from all access authorizations. All authorizations would therefore need to be added to the new entrance.
To avoid this laborious and error-prone process, the drop-down list **Type** has been added to the first page of the reader configuration.



This drop-down list is set up for all readers so that replacements can be configured by selecting and assigning the type **DELTA 7020**, without the need to delete existing entries.

Notice!
The original reader type designation (on the left tab) and other specific information is not adapted when the type is changed.

14.3 Dialog read-write unit

In contrast to the online system, where a card number can also be entered centrally, offline data can only be transferred to or read from a card by peripheral read-write units. These read-write units can be either dialog readers connected directly to the workstation or access control readers (e.g. DELTA 7020 , DELTA 1000, or DELTA 1010).
The dialog reader for writing and reading system and user cards from the offline system, as well as recording card data for the online system, is installed using the online system.

– In the BIS Configuration Browser, open the **Infrastructure** menu and then the dialog **ACE Card reader**.
– Select the relevant workstation in the Workstations field.
– In the **Type** drop-down list, select the PegaSys reader that corresponds to the card-type used.

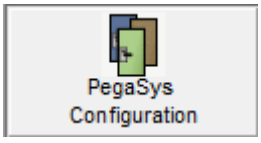
Reader name	Reader type	Coding
PegaSys-MF-BC-USB	MIFARE Classic	Bosch Code
PegaSys-MF-SN-USB	MIFARE Classic	Serial number
PegaSys-MFDESFire-BC-USB	MIFARE DESFire EV1	Bosch Code
PegaSys-HITAG-BC-USB	HITAG 1	Bosch Code
PegaSys-HITAG-SN-USB	HITAG 1	Serial number
PegaSys-Legic-BC-USB	Legic Prime	Bosch Code
PegaSys-Legic-SN-USB	LEGIC prime	Serial number
PegaSys-LegicAdvant-BC-USB	LEGIC advant	Bosch Code

In the personnel data dialogs of the Access Engine, the connected reader can be selected for data transmission on the next new start of the Access Engine

15 Offline Doors - Configuration dialog

15.1 Getting started

After the PegaSys component is installed, the configuration dialog for the component is located in the system data menu of the Dialog Manager for the Access Engine and can be opened by clicking the



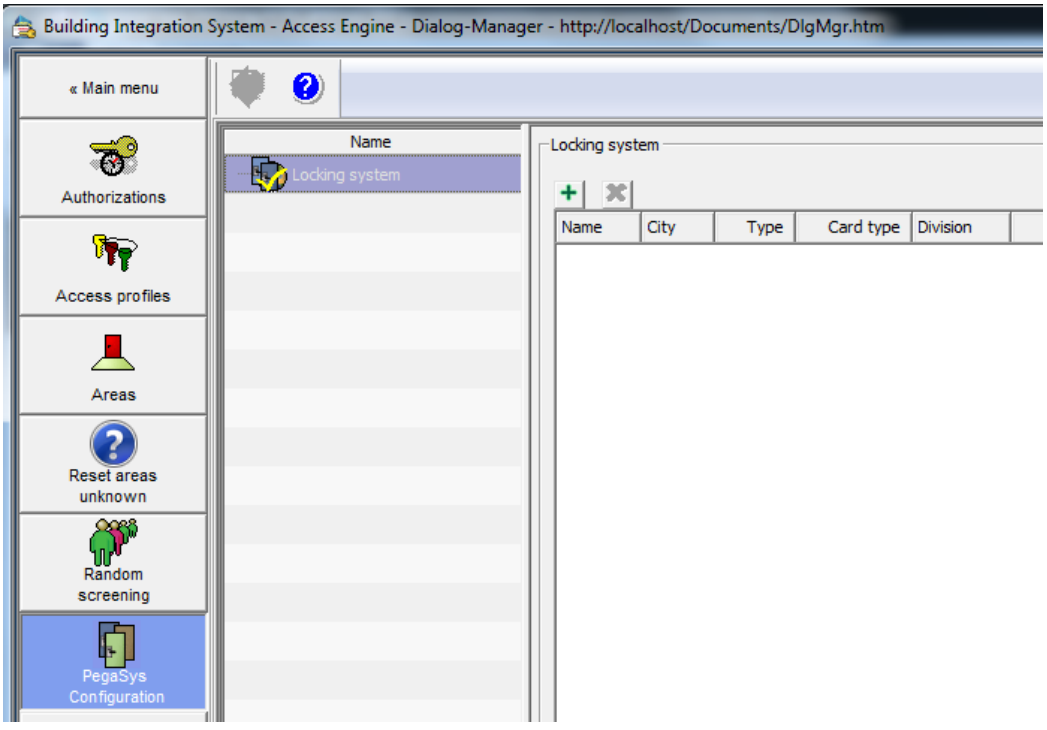
button.

15.2 Locking systems

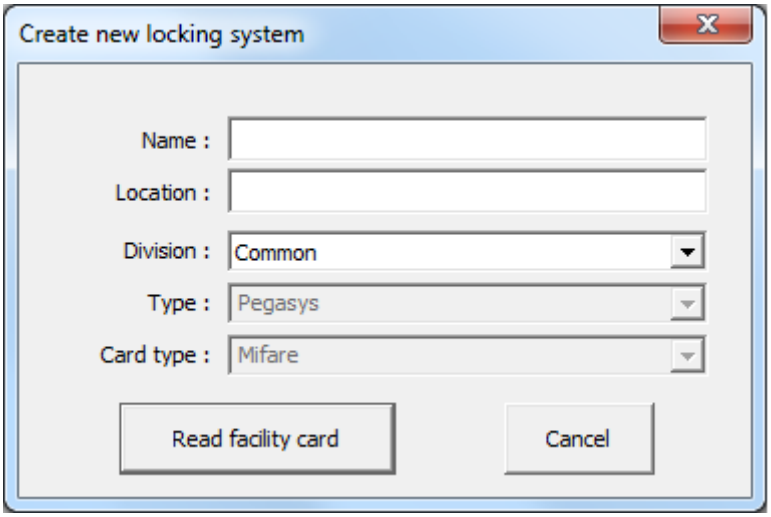
During installation the **locking systems** node is added as a base entry in the explorer tree (left dialog pane). Autonomous systems that operate independently from one another can now be set up under this entry.

Setting up systems

– Select the base entry **Locking systems**.
Systems that have already been set up appear in a list on the right hand side.



– Click the + button (above the list field) to set up additional systems.



Name Give the system a unique name.
This information also appears in the access rights dialog.

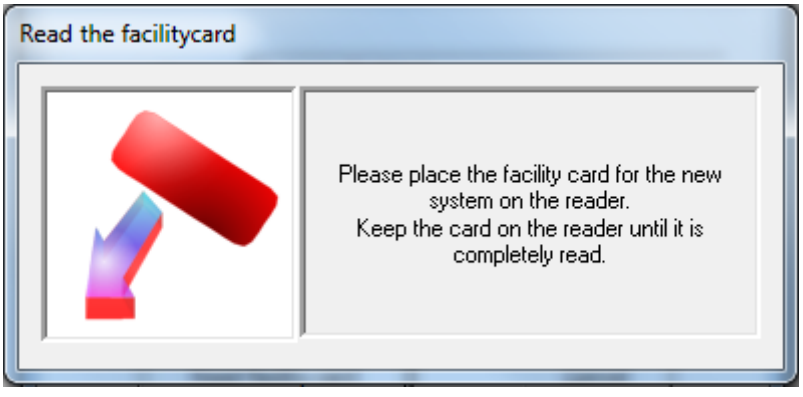
Location The location provides more precise information about the systems.
This information also appears in the access rights dialog.

Division If you have set up divisions, you can also assign the individual systems to one of these divisions.

Type "PegaSys" - is cardis the only one supported offline locking system for now.

Card type Display field (HITAG1, MIFARE classic, LEGIC prime and LEGIC advant) - is informed by the connected read-write device.

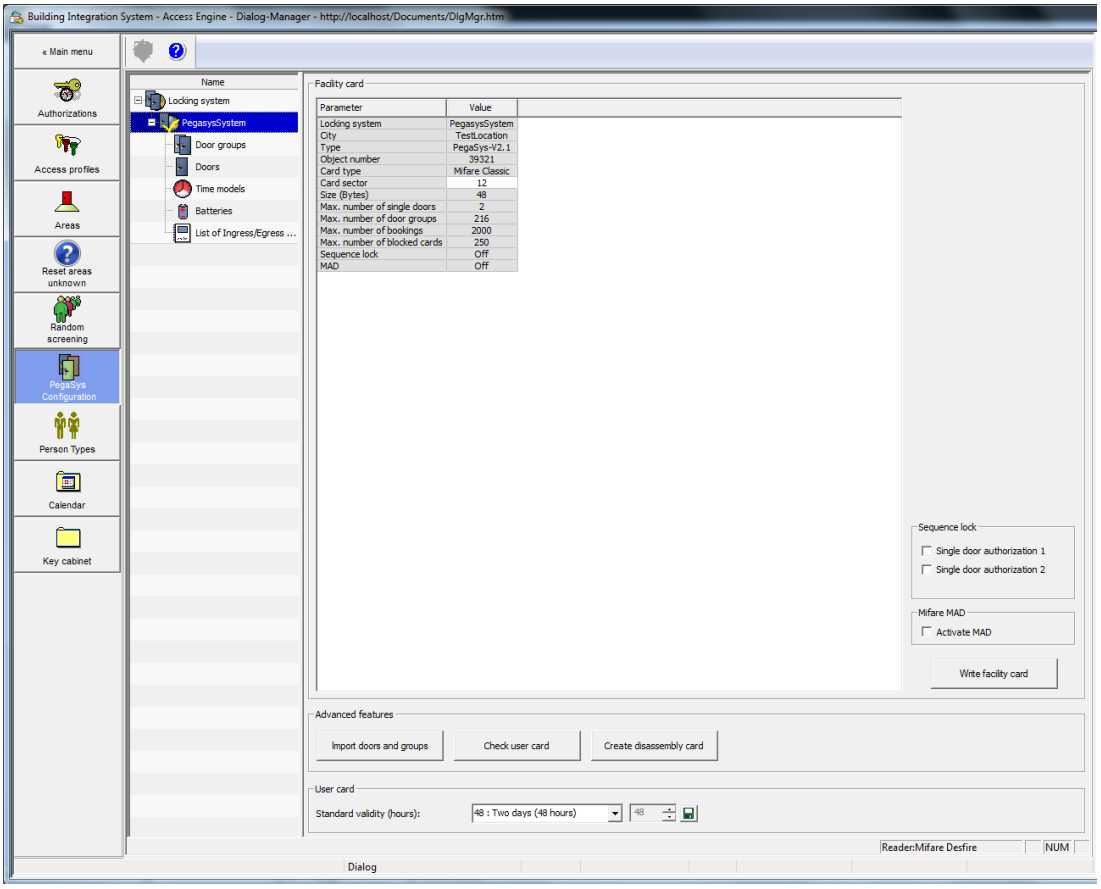
– Place the facility card for this system on the read-write unit and then press the **Read facility card** button.



When a facility card is read, the system offers to create a working copy. This option should be accepted at least once for each facility card to guard the original from accidental overwriting or loss.

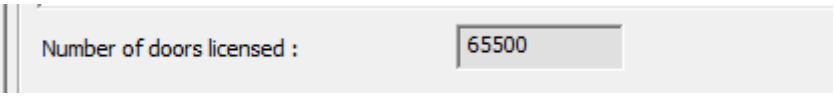
Notice!
If data unsuitable for the size of the record is added to the card, a message appears after the facility card is read indicating that the data has been corrected automatically. In this case a new facility card must be written and the door terminals reinitialized with it.

Click **Yes** to confirm that a new facility card should be written.
A list entry and another Explorer entry with the specified name are generated. Depending on the version of the facility card read, the Explorer entry contains a different number of subentries required to configure the system - see also *Configuring locking systems, page 195*.



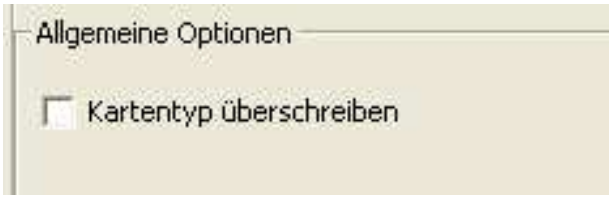
Notice!
List entries with a white background can be modified at any time. As an additional indicator, the mouse pointer changes when moved over one of these fields:
Double-clicking in the relevant list field activates write mode - press the ENTER key to exit the field after making any changes.

The **number** of **licensed** door terminals is displayed under the list field for the individual systems.



This value is the upper limit for all of the locking systems. The basic version of PegaSys includes 25 door licenses with the software. The number of licenses can be increased in multiples of 25.

Overwriting the card type



When overwriting system cards, a confirmation prompt appears once for each system card type - after that, the card is overwritten without further warning.

Deleting systems

Selected list entries can be removed again using the button. To avoid accidental deletion the user is prompted to confirm.
Click **Yes** to confirm that you wish to delete the system.

15.3 Configuring locking systems

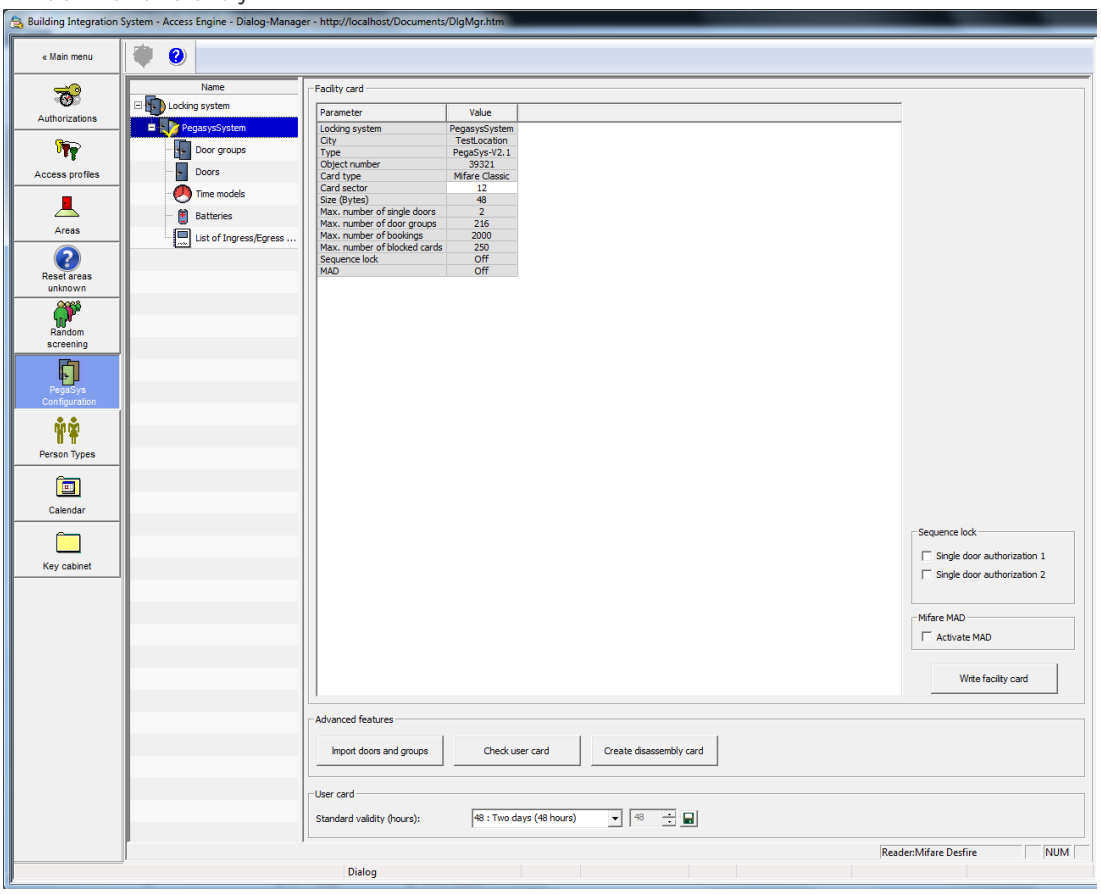
A system is configured in four steps which can be invoked from the corresponding tree node. Each type of node has its own icon; the icons of selected nodes contain a yellow checkmark.

Explorer node	Icon	When selected
<System name>		
Door groups		
Doors		
Time models		

The following sections describe which settings are configured, where and how.

15.3.1 (Sub)system

Specified system parameters and the data read from the **facility card** are displayed in the list window for this entry.



Locking system — Name of the system as specified at setup.

Location — Name of the location as specified at setup.

Type — PegaSys-<Version no.>

Object number — Customer-specific code

Card type — Information on the reading and coding method:
- HITAG 1
- MIFARE Classic
- MIFARE DESFire EV1
- LEGIC prime
- LEGIC advant

Card sector — Area on the card where the coding of PegaSys authorizations begins.

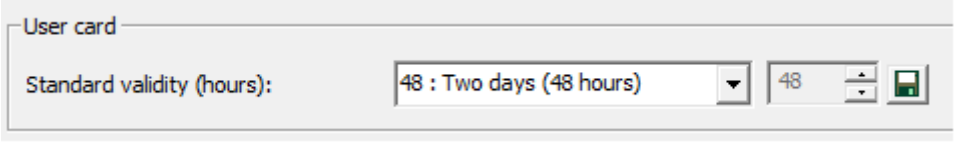
Data size (Bytes) — Number of bytes required to store the authorizations.

48 = default - the record length must be adapted depending on the size of the system - see also the table in *Possible data structures, page 213*.

Caution:
If using HITAG1 check these values carefully when first setting up the system, as this card type does not have a function to prevent areas already in use from being overwritten accidentally.

Max. number of single doors	Upper limits for the system, defined by card type and data size. **Remark:** Blocking cards i.e. Transport cards that can be used to transmit blocked cards to the terminals.
Max. number of door groups	
Max. number of bookings	
Max. number of blocked cards	

Standard validity
Furthermore, a **Standard validity** time for **User cards** can be set here. This will be used by the **Cards** dialog in Access Engine as default when assigning PegaSys authorizations.



The drop-down list contains a number of predefined periods and the option of selecting a specific number of hours.

One day (24 hours) Two days (48 hours) One week (7 days) One month (30 days) One year (365 days)	= Default setting Fixed periods that are counted from the moment the badge was encoded or the rights were extended.
Max. card validity	The validity defined in the dialog system ... – **Valid until** - Date (in online authorization dialog) – **Valid until** - Date (in the offline authorization dialog) – Block – Deletion
User setting	Freely defined period - in hours [1 to 17520 (two years)].

The input field for entering the hours is activated when this option is selected.

Notice!
Click the nearby button to save any changes in the validity period of user cards.

Warning!
If the default value is changed, all personnel to whom the default validity period was assigned receive new values the next time their badges are updated.

Extended functions

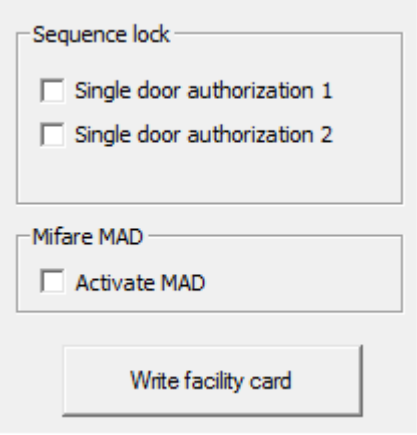
- **Check user card**
  When the facility card is read, the card segment and the access code for offline authorizations are defined for the user cards. In order to check whether the settings are correct, the current settings can be written to a user card by pressing this button. A valid yet expired user card is created without authorizations. If this function fails, the system cannot be put into operation with these user cards and this facility card.
  Each card technology has different prerequisites:
  - **HITAG 1**
    The preset start sector on these cards could be blocked. The start sector is a facility card parameter and can be adjusted in this dialog.
  - **MIFARE Classic**
    The preset start sector on these user cards may have already been encoded using a different code from the one on the facility card. If the start sector was set incorrectly, it can be modified in the same way as with HITAG1.
    In MIFARE Classic, the start sector of an application (such as PegaSys) can also be defined via the MAD (MIFARE application directory) of the user card. If the MAD is activated, the access code to the sector with the MAD must be known - see also *Configuring MAD (for MIFARE Classic only), page 199*.
  - **LEGIC prime/advant**
    With LEGIC, it is assumed that the user cards have been preformatted and that the required segment already exists on the user card. The required segment is displayed in the LEGIC segment parameter. All readers (online and offline) must have authorization to access the preset segment. This authorization may have already been programmed into the readers at the factory or set at a later time via so-called initialization cards (=SAM63). If the system is rebuilt and new user cards are ordered, the so-called PegaSys segment can be installed directly by the card manufacturer.
    If the segment is missing from the user card then, when the user cards are encoded by the dialogs (offline configurator and badge dialogs), an automatic prompt asks whether the segment should be created. If the dialog read-write devices have the necessary authorization (preset via XAM card), or the customer has an IAM LEGIC card that gives him authorization for just this preset PegaSys segment, then the

required segment can be created and data written onto it. The offline segment is only created once. It should then be possible to read/write data to the user card from all (online/offline) terminals.

Caution!
The software performs no checks as to whether data is already stored on the user card. If the card technology does not protect that data then it may be overwritten.

– **Creating a disassembly card**
The disassembly card can be created from any system card (except the facility card). Cylinders that belong to this offline system can be disassembled using this card. System affiliation is transferred to the offline terminals via the facility cards.

Writing facility cards



If any facility card parameter, the Sequence lock or the MIFARE MAD settings are changed, then the facility card should be updated by pressing the **Write facility card** button. The online system uses the new settings directly. Leave the check boxes for the Sequence lock empty (i.e. switch Sequence lock off) unless use of this PegaSys feature has been carefully prepared in advance.

Notice!
If you change data on the facility card, remember to update the door terminals with it. Otherwise the terminals will continue to operate with outdated settings.

Configuring MAD (for MIFARE Classic only)

When the MAD is switched on, the A and B access codes can be configured in the MAD sector of the user cards. A0 to A5 and B0 to B5 are default codes and therefore known to all companies (i.e. access is enabled for everyone). Only the A code is transferred to the offline terminals via the facility card because the terminals only need to read and not write data to the MAD, if it is activated. The online system uses the B code to write the MAD for the offline system to the user cards.

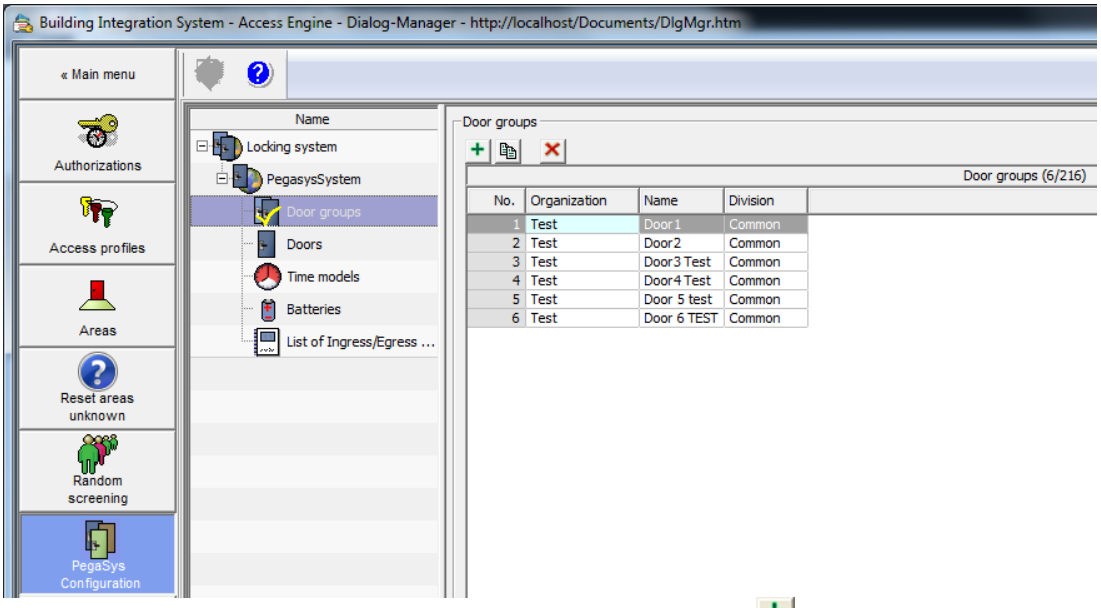
Notice!
The MAD cannot be configured for Mifare DESFire EV1.

15.3.2 Door groups

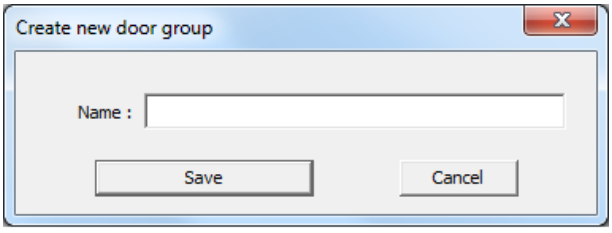
The segmentation of badges allows only a relatively low allocation of individual doors in comparison with door groups. This is because it is more convenient and common to assign authorizations to door groups than to individual doors.

Creating door groups

The required door groups are created as records in the list field without a link being initially established to individual doors.



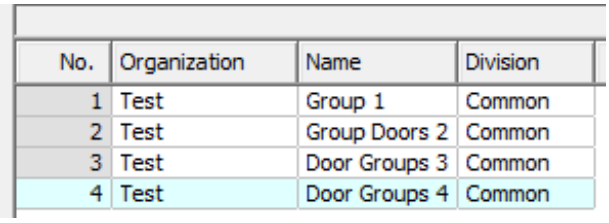
The creation dialog for the door groups is opened by clicking the + button.



Specifying a designation (**name**) for the door group and clicking the **Create** button generates a further list entry with its own ID number. The Division configured when the system (*Locking systems, page 192*) was set up appears in the **Division** column. It can be reset separately for each door group causing these door groups (as authorizations) to appear only within their own divisions.

Notice!
Wherever possible use descriptive names for the door groups.

A limited number of door groups can be created depending on the data size and card type - see also the table in *Possible data structures, page 213*. With the default size of 48 bytes and HITAG1 cards, the upper limit for door groups is 240 (for LEGIC and MIFARE, 256). The number of door groups already created, and the maximum number, are displayed in the list header: Door groups (4/216)

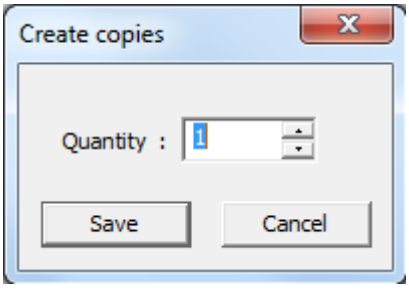


No.	Organization	Name	Division
1	Test	Group 1	Common
2	Test	Group Doors 2	Common
3	Test	Door Groups 3	Common
4	Test	Door Groups 4	Common

Copying door groups

Existing list entries can be copied, to make data-entry easier.

– Select a list entry.
– Click the button above the list field. The following dialog opens:



– Enter the number of copies you wish to create.
– Click the **Save** button to generate the list entries.
  In order to guarantee that the designation is unique, the entries are assigned the designation of the selected entry and a sequential number (e.g. **Door groups n**).

The designations for the door groups can be modified at any time by double-clicking the relevant line in the **Name** column. The sequential number in the first column (**No.**) identifies the door group and cannot therefore be modified.

The number of copies that can be made depends on the card size. The arrow buttons in the **Create copies** dialog do not allow the selection of a value higher than the available remaining quantity and the dialog no longer opens when the maximum value is reached.

Deleting door groups

Door groups that are no longer required can be selected in the list and deleted by pressing the button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.

Click **Yes** to confirm that you wish to delete the door group

Notice!
Door groups that still have doors assigned to them can only be deleted after these assignments have been canceled.

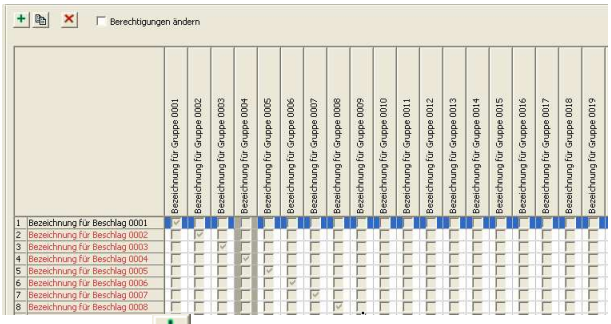
The doors are assigned in the next configuration step.

15.3.3 Doors

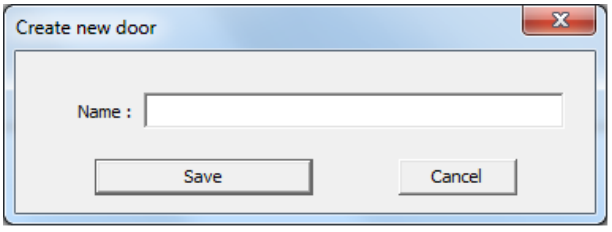
A list entry must be created and configured in this dialog for each door terminal in the locking system. These can then be assigned to certain door groups.

Creating doors

In this list field an entry is generated for each door terminal.



Pressing the + button opens the dialog for creating the doors.



When a designation is specified for the door (**Name**), clicking the **Save** button generates a new list entry, which can then be assigned and configured.

Notice!
Wherever possible use descriptive names for the doors.

Notice!
The maximum number of licensed doors - see *Locking systems, page 192* - relates to **all** doors of **all** systems, but can be increased by purchasing extensions.

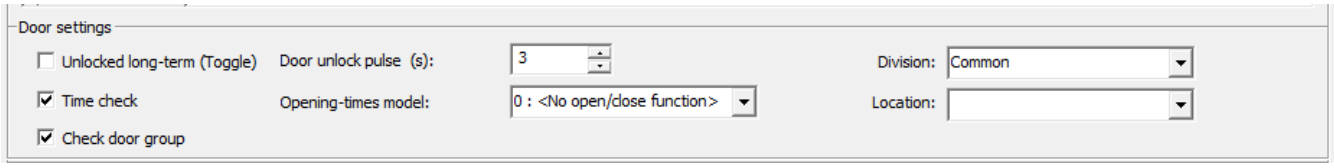
Assigning doors

The list field of the dialog contains a column for each door group created. Select the relevant check boxes ☑ to assign the doors to the door groups. First activate edit mode by selecting the **[MISSINGDISPLAYTEXT: Change authorizations]** check box.
There is no limit to the number of door groups to which a door can be assigned.

Notice!
Doors marked red are doors whose configuration has been changed but whose door card has not yet been encoded. The door designation turns black when the door card is encoded.

Configuring doors

The parameters under the list field are used to configure the selected door.



Unlocked long-term (Toggle)	Users with a special authorization can also unlock this door for an extended period - e.g. an office with public access. Default setting = deselected (check box cleared)
Time check	Setting that determines whether time models and validity periods are taken into consideration at all. Default setting = check box selected
Checking door groups	An authorization for the locking system can consist of individual and/or door group authorizations. If this parameter is not selected, only individual authorizations are considered and checked. Default setting = check box selected
Door opening time (s)	Time in seconds (1 - 255), defining how long the door contact should release the door for opening. Default setting = 3
Opening-hours time model	Selection of a time model - the door is unlocked automatically for specified periods defined by their start and end times.
Division	Selection of a division with which the door should be associated. The default division is the one selected for the locking system, but it can be modified separately for each individual door.
Location	The location of the door (e.g. city, building, corridor, etc.). When access rights are allocated the location parameter is used to group and help identify individual doors.

Copying doors

Doors can be copied in the same way as door groups. To simplify the data entry, first a single door is created and configured, then copied as required.

– Select a list entry for the copying process.
– Click the  button above the list field. The **Create copies** dialog opens:

– Enter the required number of copies you wish to create or select them using the arrow keys.
– Pressing the **Save** button generates the required list entries.
In order to guarantee that each designation is unique, copies are given a sequentially numbered suffix (e.g. **Door n**).

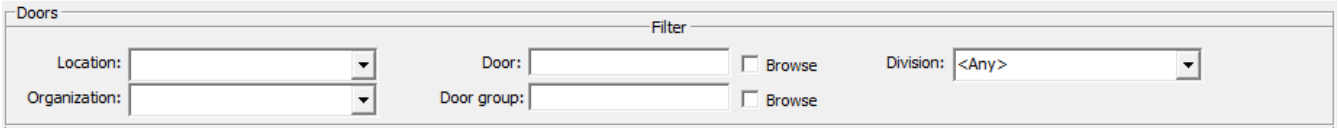
The designations for the doors can be modified at any time by double-clicking the relevant line in the **Name** column. The ID number in the first column (**No.**) cannot be modified.
The number of copies that can be made is limited by the licenses available. The arrow buttons in the **Create copies** dialog do not allow the selection of a value higher than the available remaining quantity and the dialog no longer opens when the maximum value is reached.

Deleting doors

Selected list entries can be removed again using the  button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.
Click **Yes** to confirm that you wish to delete the list entry.

Filters for doors

On offline systems with a large number of doors, sorting the doors alphabetically can have a negative impact on the overview and make working more difficult. **Filters** located above the list field can be used to adapt the view in different ways and reduce the display to a small number of relevant entries.



Location	Filters out all doors in a specific location.
Organization	Filters out all doors within a specific door group.
Door	Filters out all doors with a specific character in the name. The columns show all door groups - the groups containing the relevant doors have selected check boxes.
Door group	Filters door groups with a specific character in the name. The lines show all doors - the doors contained in the relevant door groups have selected check boxes.
Browse	In the default setting, the system searches the start of the name for the characters specified in the top three fields. If this option is enabled, entries that contain the specified characters at any point in the name are selected.
Division	Only doors or door groups from the selected division are displayed.

Default setting: **Any** - i.e. entries from all divisions are displayed.

Writing door cards

In contrast to the BIS Access Engine access control system, configuration data in the offline systems cannot be distributed via system components and transmitted to the relevant installations; instead, it must be brought to the devices via another route. In the System overview, various system cards have already been mentioned - one of these system card types is the **door initialization card**, to which door parameter settings are written and which are scanned at the door terminals. After configuration, a door is selected in the list and then the **Write door card** button is pressed and one of the door initialization cards is placed on the read-write unit of the workstation computer.

A dialog box prompts you to place the badge in position and then shows the progress of the write process.

A message appears indicating that the write process was successful and then the time is recorded and displayed in the **Last coding** field as confirmation.

Notice!

Only the configuration data from **one** door can be written to a door initialization card. Not until the data has been transferred to the door terminal can the card be used for other write processes. Any existing data is overwritten.

Notice!

The time models are also stored on a door initialization card. The time models should therefore be created in advance if possible, otherwise each door will have to be initialized again with time cards.

The new doors, door groups and parameters are transferred to the terminals via these door initialization cards. During the data transmission process, the LED on terminals lights up orange. Successful transmission of the data is then confirmed.

Checking the cards

Before the current card is written, the system checks whether it is actually a door initialization card. If the card has already been encoded in a different way (e.g. as a time or booking card), a warning to this effect is displayed with the option of overwriting the card and using it in the future as a door initialization card.

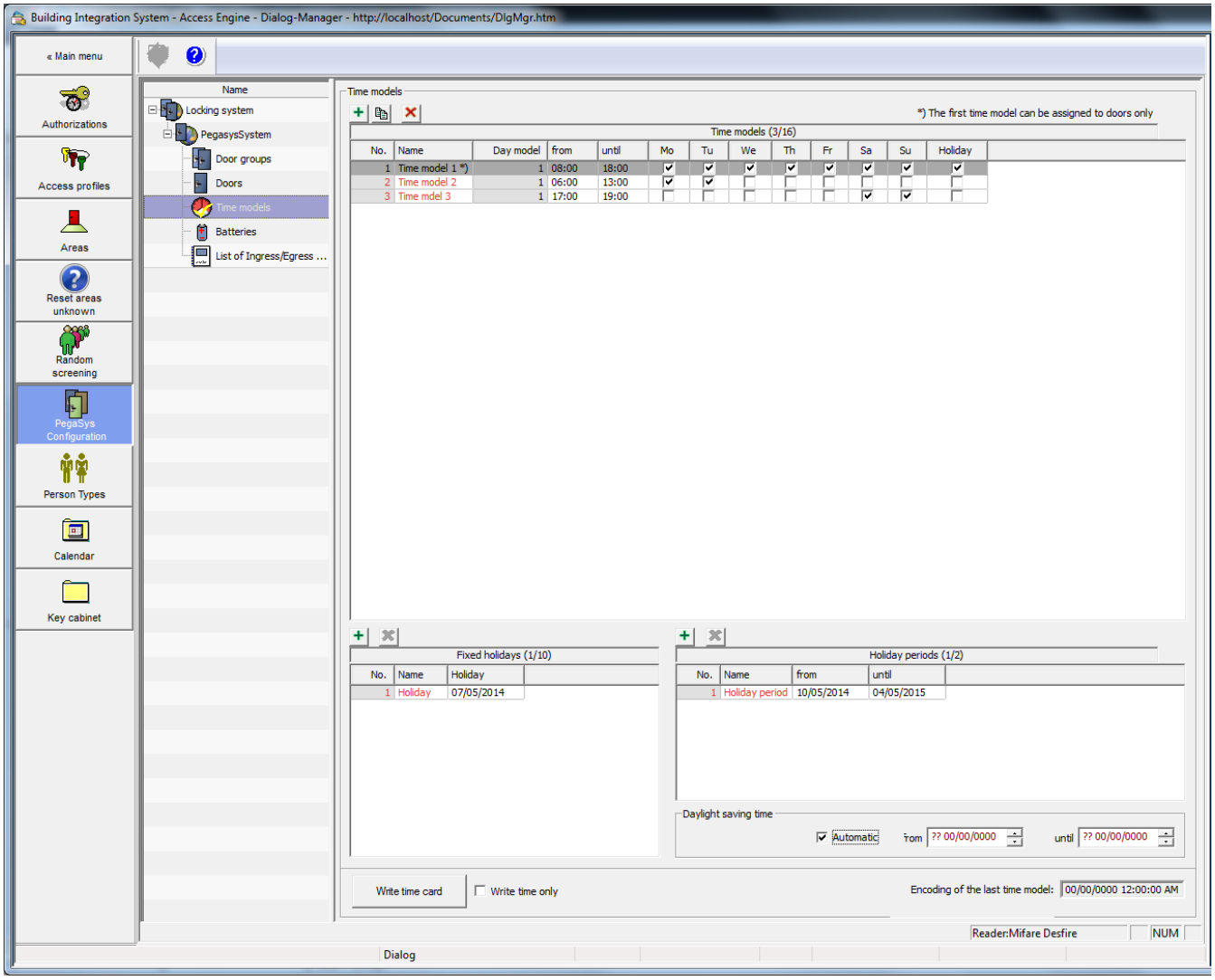
Notice!

If the parameter **Program > Overwrite the card type** (menu bar) is selected, a confirmation prompt appears once for each card type - after that, the card is overwritten without further warning.

Facility and user cards cannot be overwritten with a different card type.

15.3.4 Time models

The dialog has three sections, the list window in the top half contains all the time models and their assignment to the days of the week. Special days (e.g. holidays) that differ from the norm can be defined at the bottom left. Several days can be grouped to form a holiday period, in the window to the right.



Time model vs time period

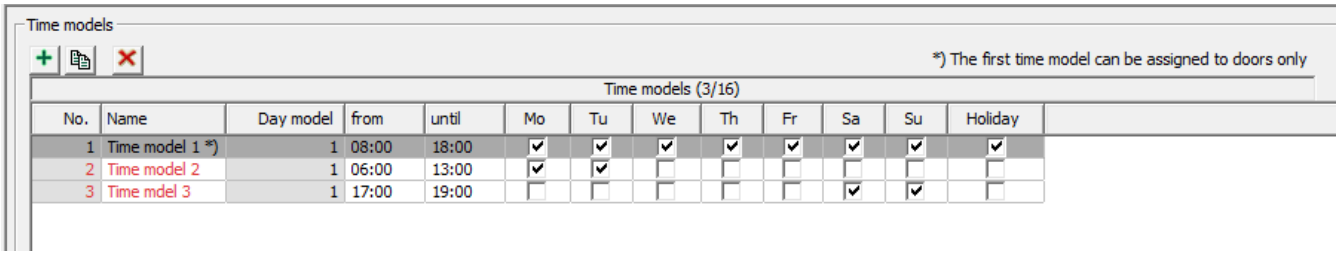
A time model can contain up to four time periods in one 24 hour day. Start and end times typically delimit periods where different regulations apply (e.g. extended door unlock). The periods can be any length and can overlap. Each period can be allocated to any day of the week or holiday.

The user is thereby responsible for ensuring that the period limits are set and allocated to the days in a logical and consistent manner.

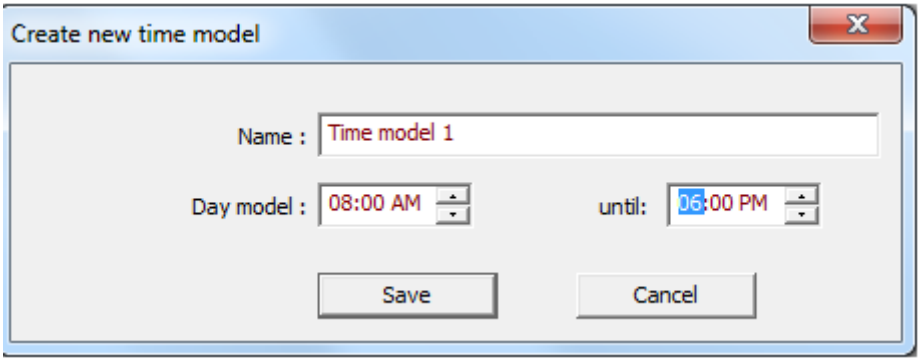
The entirety of all time periods and their allocations to days makes up the time model, which can be used as an entity in the system.

Creating time models

Time models can be used to restrict allocated authorizations or perform automatic door opening and closing operations. A maximum of 16 time models, each with 4 time periods can be configured for each system.



Like the other configuration data, time models are also created by opening the creation dialog with the button.



Make sure that no list entries are selected, otherwise other time periods will be created instead of a new time model.
The time model is assigned a unique designation (**Name**), as well as time limits related to the period. Clicking the **Save** button creates a new list entry with the information provided.

Notice!
If possible, use designations that indicate which time models are affected.

– Time models with the same start and end time can also be created. This can be used to lock the door automatically at the specified time.

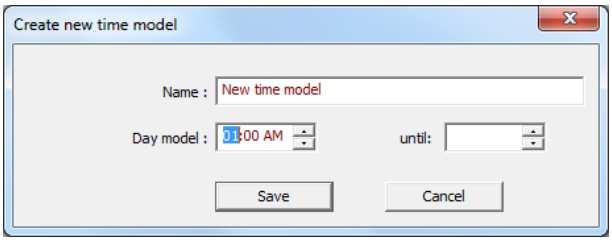
Configuring time models

The time models and activity periods (first and third columns) have fixed sequential IDs. [the time model with the sequential number **1** cannot be assigned to personnel, but only for operations like extended unlocking, for example.]
In addition to the name and start/end times, each entry contains seven check boxes for weekdays and one for a holiday.
Selecting the relevant check boxes defines the days on which the activity period should apply. When the **Holiday** check box is selected, the time period is applied to all defined holidays and holiday periods.

Notice!
The maximum number of available time models (16) applies separately for each system.

Creating additional time periods

To create additional time periods, first select from the list the time model to which the new period should be added. Then click the button + as when creating a time model. The **Name** field contains the name of the selected time model and cannot be modified.



If you define new limits for an activity period then a new list entry is created which has the same number (first column) and the same name (second column) as the list entry that was selected. The number of the period (third column) increases by one.
The weekdays on which the new period should apply can now be defined. It is possible to activate several time periods for one day.
A maximum of four periods can be defined for each time model in this way.

Deleting time periods

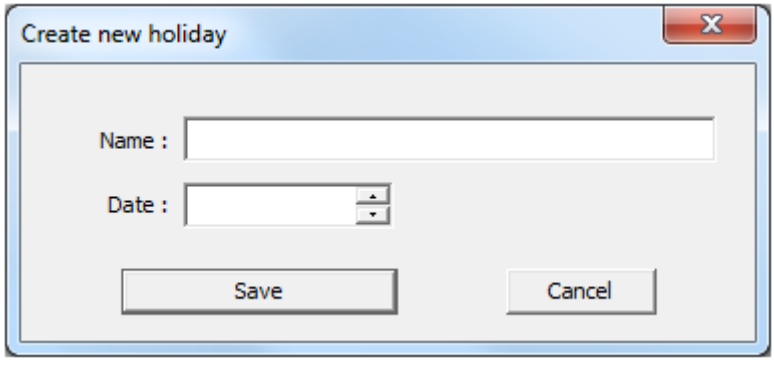
Selected list entries can be removed again using the × button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.
Click **Yes** to confirm that you wish to delete the time period.

15.3.5 Holidays, holiday periods, daylight saving time

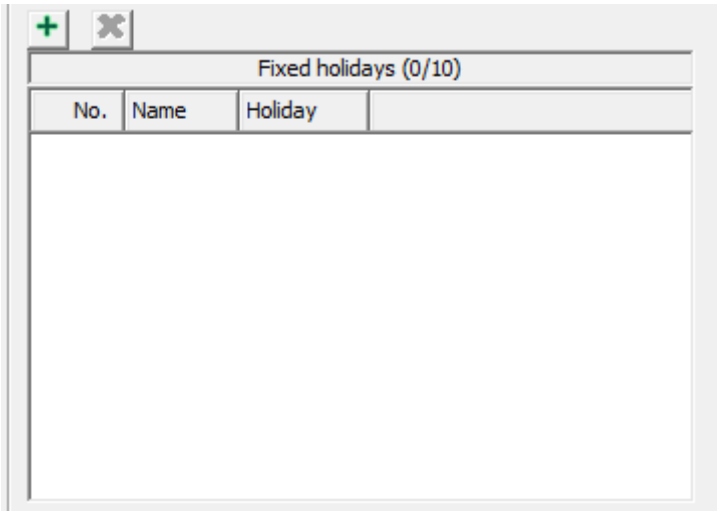
Compared to the normal week, holidays represent an exception and must be treated differently in terms of control functions. A **maximum of ten holidays** can be defined for every system, together with the date on which different activity periods should apply.
Holiday periods are also times with deviant time periods. Holiday periods may extend over several days - e.g. company holidays. **Two holiday periods** can be defined for each system

Creating holidays

The buttons for creating and deleting holidays are located above the **Fixed holidays** list window. The creation dialog is opened by pressing the + button.



A unique designation (**Name**) and the **Date** when this holiday next occurs are specified.
Clicking the **Create** button creates a list entry with the information provided.



A fixed sequential ID, as well as the name and date of the holiday, are assigned to the entries - the last two fields can be moved and modified as required by double-clicking the edit state.
A maximum of ten holidays can be defined for each system.

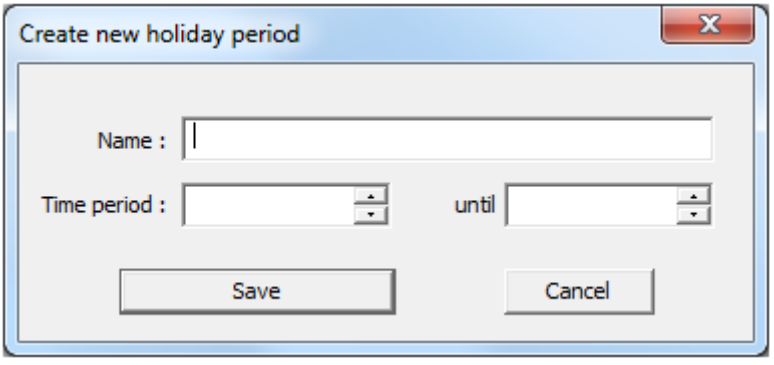
Notice!
Holidays are created with a specific date and must be redefined and adapted every year.

Deleting holidays

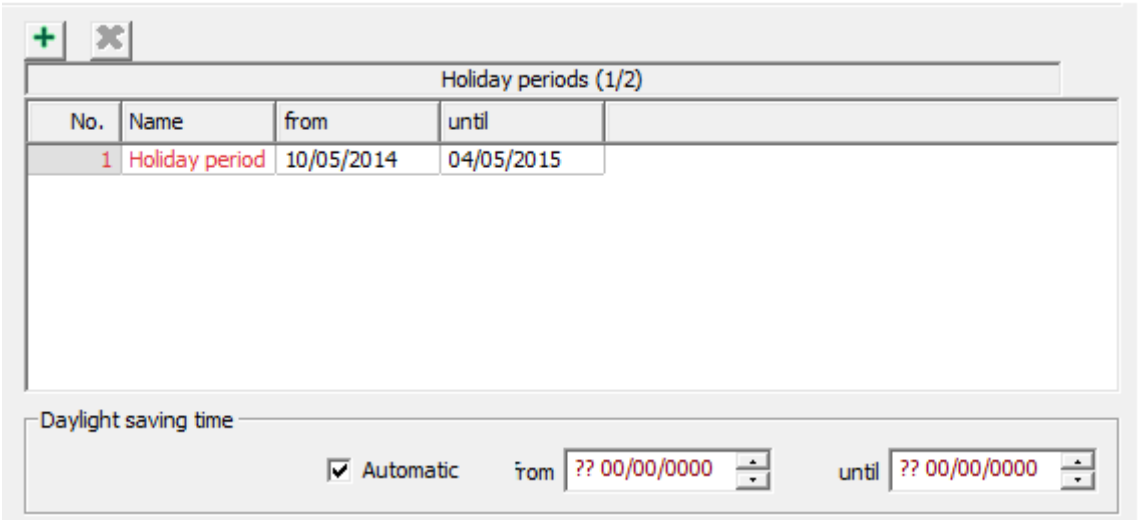
Selected list entries can be removed again using the button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.
Click **Yes** to confirm that you wish to delete the holiday.

Creating a holiday period

The creation dialog is opened by pressing the button.



A unique designation (**Name**) and a start and end date must be specified before a new list entry can be created using the **Save** button.



Two periods can be defined for each system.

Notice!
Holiday periods are holidays that cover several days, and are created using specific data. Consequently, they must be redefined and adapted every year.

Deleting a holiday period

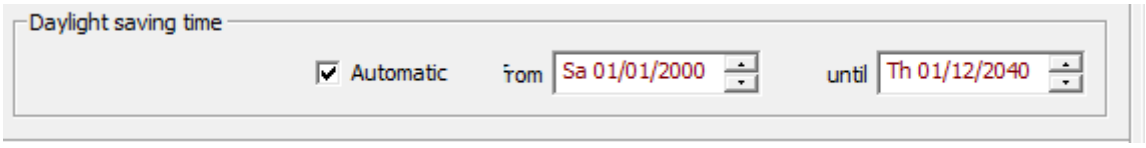
Selected list entries can be removed again using the button. At this point, a security prompt appears, which must be confirmed to avoid accidental deletion.
Click **Yes** to confirm that you wish to delete the holiday period.

Notice!
When the **Holiday** check box is selected for a time period, this applies for all defined holidays and holiday periods - it is not possible to differentiate between the holidays.

- The maximum number of holidays (ten) and special holiday periods (two) refers to the maximum number simultaneously stored on the terminals, not the maximum within a specific period (e.g. calendar year). If more are required, then expired holidays or holiday periods can be deleted to make room for them. However these must then be propagated to the terminals using time initialization cards.
  This increases the administrative workload.

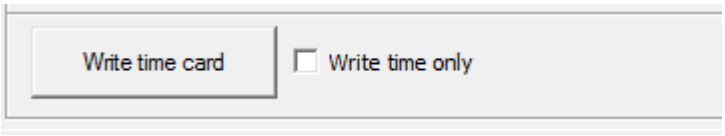
Daylight saving time

The daylight saving time setting can be defined (**automatically**) by the system or by making manual entries in the two date fields (from / to). Date information entered manually must be adapted every year.



15.3.6 Writing time cards

In contrast to the BIS Access Engine access control system, configuration data in the offline systems cannot be distributed via system components and transmitted to the relevant installations; instead, it must be brought to the devices via another route. In the System overview, various system cards have already been mentioned - one of these system card types is the **time initialization card**, to which parameter settings of all time models and the current time are written and which are scanned at the door terminals.



The time models are ignored if the **Write time only** check box is selected and then the **Write time card** button is pressed.
A dialog box prompts you to place the badge in position and then shows the progress of the write process.
A message confirms whether the write process was successful. If the clock time was not the only element selected then the time is recorded and displayed in the **Last coding** field.

Notice!
With the HITAG card type, more than one time card may be required to accommodate all the time models.

The time models are transferred to the terminals via these time initialization cards. During the data transmission process, the LED on terminals lights up orange. Successful transmission of the data is then confirmed.

Notice!
The **Time check** door parameter must be selected so that the time models are taken into account at the terminals.

Checking the cards
Before the card on the enrollment reader is written, the system checks whether it is actually a time initialization card. If the card has already been encoded in a different way (e.g. as a door or booking card), a warning to this effect is displayed with the option of overwriting the card and using it in the future as a time initialization card.

Notice!
If the parameter **Program > Overwrite the card type** (menu bar) is selected, a cofirmation prompt appears once for each card type - after that, the card is overwritten without further warning.
The parameter is only reset when the configuration program is restarted.
Facility and user cards cannot be overwritten with a different card type.

15.3.7 Updating the date and time

In addition to the door and time model data, the current time stamp (date/time) is also written to the transport cards. Depending on the size of the facility being secured, there is a certain time delay before the cards can be scanned at the doors.

In order to gain the most precise time data, especially for bookings, a **mobile read-write device** (timesetter) should be used. This unit allows the times to be updated on the transport cards immediately before scanning at the terminal. This ensures that the time delay remain withins the tolerable limits.

Scanning the system card

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

Writing to the transport cards

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

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

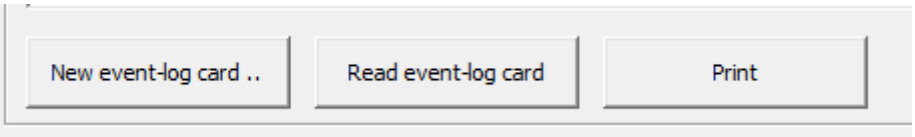
Notice!
The write and read process is indicated by an LED display. For details on what the color sequences mean, please see *LED display signals, page 218*.

15.4 Booking cards

Successful and unsuccessful access attempts are saved in the door terminals. The last 800 bookings are saved in a ring buffer. These can be retrieved with special booking cards and entered in the database.
First booking cards are created, then the bookings retrieved from the terminals, then the cards scanned via the dialog. Different card types accommodate different numbers of bookings: HITAG1 holds 32, MIFARE holds 244, LEGIC holds 294. You must therefore create sufficient booking cards and set up appropriate retrieval schedules.

Creating booking cards

A booking card must be initialized before the bookings can be scanned.



– Place the booking card on the read-write unit at the workstation.
– Select the booking dialog in the Explorer list.
– In order for the terminal to accept a booking card as new, create a new booking card or empty a used one by clicking the **New event-log card...** button.

A message indicates that the booking card was created successfully.

Reading the bookings on the terminal

This system card can then be presented at the read unit of the corresponding terminal. While the LED shows orange, the terminal is writing data to the booking card. If the booking card is removed during this time, the data transfer will be interrupted. When the LED flashes green three times, the bookings have been successfully written to the card.

The memory of the terminal is erased during this process, i.e. the bookings cannot be retrieved after this again.

Scanning booking cards

The card with the transferred bookings is then scanned via the dialog reader.

– Place the booking card containing the access data on the dialog reader.
– Select the booking dialog in the Explorer list.
– Press the **Read event log card** button.

The read data will be shown in the list field. The following data is listed for each booking: date (with time), surname, first name, event, door no., personnel no., company

The data read can be printed. Furthermore, all bookings are saved in the database and can be converted back to list format, printed, exported and edited further at any time using special reports in the Dialog Manager of the Access Engine.

15.5 Possible data structures

Door groups Individual doors	256	512	768	1024
2	48 (= default)	80	112	144
4	52	84	116	148
8	60	92	124	156
16	76	108	140	172

Tab. 15.1: The figures refer to the dataset length in bytes.

Notice!

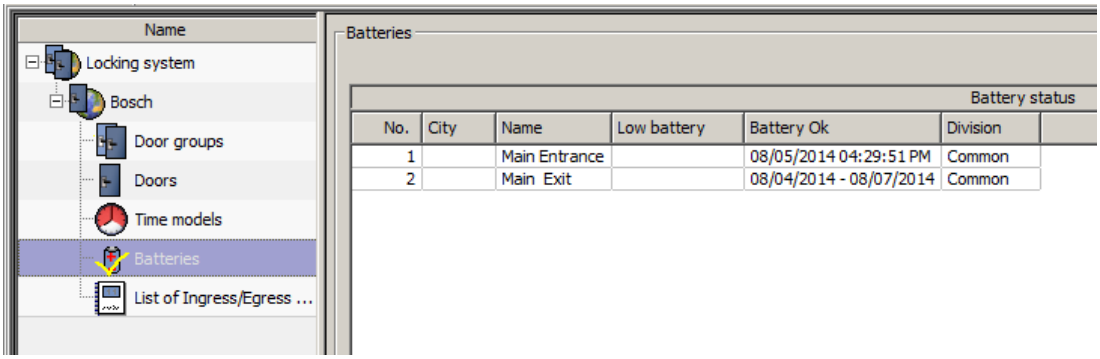
HITAG1 cards can only be encoded with the default size (48 bytes). Only 240 door groups are possible instead of the 256 specified above.

The specified data sizes apply for PegaSys Version 2.0. PegaSys Version 2.1 with additional battery status requires 5 more bytes so the memory size is increased from 172 to 177 bytes. HITAG1 is an exception: only a maximum of 200 door groups are possible with a constant 48 bytes.

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

15.6 Batteries

The last known battery status of the PegaSys terminals can be viewed in the **Batteries** dialog. The battery status is only available from Version 2.1 of PegaSys (depending on the facility card).



The messages **Battery LOW** and **Battery OK** are written when the terminal attempts to access the user card.

There are three battery warning levels:

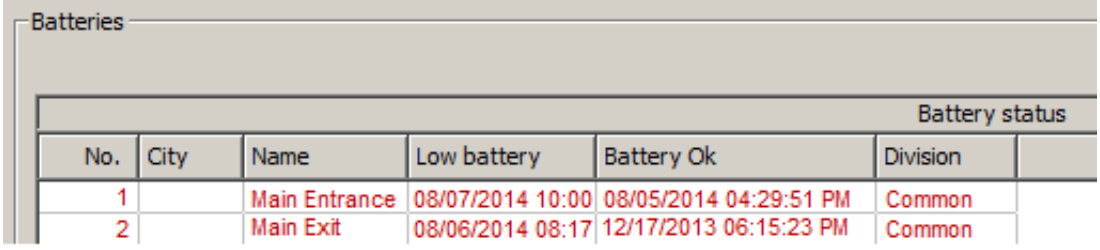
1. at 3.9 V: the next 5 badges receive a warning message consisting of a date and the number of the terminal.
2. at 3.6 V: when an access attempt is made with a user card, a RED signal is issued for 1 second together with 3 acoustic beeps. The next 5 ID badges receive a warning message the same as the first level.
3. at 3.4 V: when an access attempt is made with a user card, a RED signal is issued for 3 seconds together with a continuous acoustic beep that lasts 5 seconds. The next 5 badges receive a warning message the same as the other levels.

These battery-level warnings are available with terminal Firmware Version 4.1 and higher. The measuring tolerance is approx. 100mV for each level.

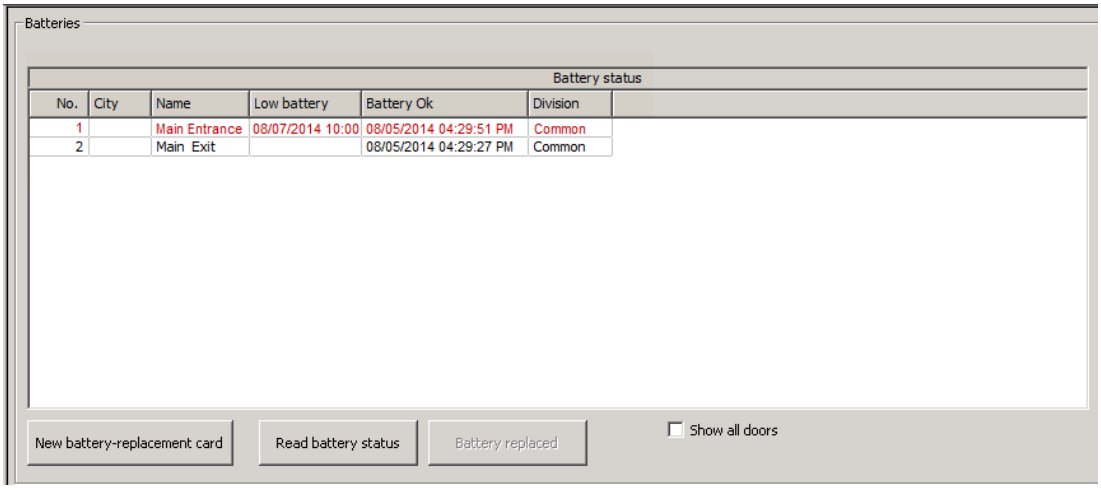
With every move to a higher warning level, messages are written to the next 5 user cards (one each). With every move to a lower warning level (e.g. after a change of batteries), 5 positive messages are issued including date and terminal number. As soon as a user card receives a battery status message, no other status messages can be written to this card until it has been updated on the online terminal, i.e. automatically read and reset.

The status message (positive or negative) is updated in the database if no other newer information is available.

The **Batteries** dialog provides in its upper list an overview of the terminals with weak battery messages.



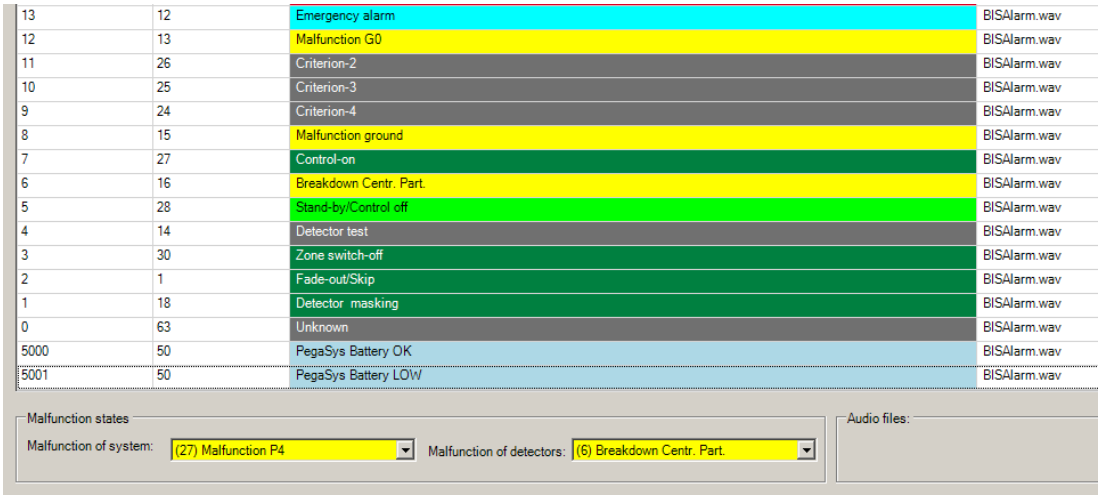
As soon as one of the batteries is changed and the online system receives a positive status message, the entries disappear from this list. If the **Show all doors** check box is selected, all doors are displayed together with their battery status. The lines marked in red contain terminals that have a weak battery or have not received a positive battery status message.



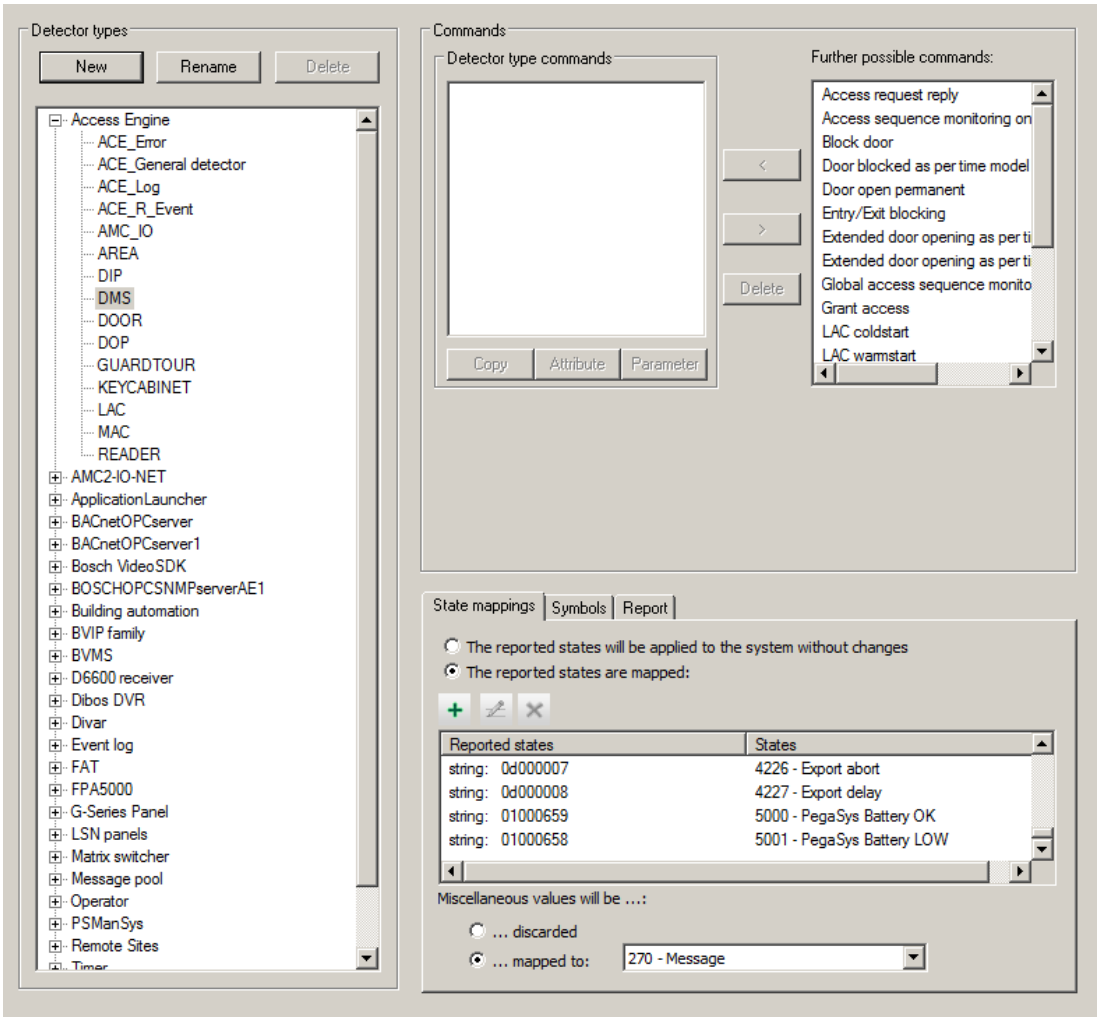
In some cases, terminals are used only rarely. In this case, the battery warnings would not be retrieved frequently enough, and the battery status would not be updated. For this reason all terminals with a **Battery OK** date older than one year are marked red as if a warning had been issued.
The date for the **Battery OK** display can also be set manually to the current date by pressing the **Battery replaced** button.
The user card with a battery status message can be read directly on the dialog reader by pressing the **Read battery status** button.

Battery status messages in the BIS

Battery status messages can also be displayed in the BIS.



The states **5000: PegaSys Battery OK** and **5001: PegaSys Battery LOW** are added to the states list of the BIS Configuration Browser.



– Select the entry **Access Engine > DMS** in the Detector types list.
– Add both statuses (with the status numbers 01000658 and 01000659) to the list on the **Status mapping** tab.

Only one message (**Battery OK** or **Battery LOW**) is displayed on each terminal, even if the online system receives up to five messages.

Battery replacement card

The **New battery-replacement card** button creates a battery-replacement card for cylinder-type terminals because they require clearance before their batteries can be changed.
A battery-replacement card can be used for all cylinder-type terminals in a system.

16 Offline Doors - System limits

Offline Locking Systems per Access Engine	1
Systems per Locking System	1 A **System** is a subdivision of the overall ACE Offline Doors locking system. Each **System** is governed by its own facility card.
Doors per Locking System	65,000 total distributed across all Door Groups.
Door Groups per System	A maximum of 1024 door groups can be defined on any one facility card.
Time models per System	16
Holidays per System	10
Holiday periods per System	2

17 LED display signals

Signals for user cards

Door opened with single-unlock function:

Door opened with extended unlock function:

Door closed with extended unlock function:

Battery change request:

Special signals

Read-write confirmation for system cards:

No badge in range:

Read/write error:

Invalid authorization:

Time invalid:

Door initialization missing:

Facility data missing:

Data transmission:

17.1 Display with explanations

17.1.1 Signals for user cards

Door opened with single-unlock function

Meaning	The door is unlocked with a single-unlock card. This message also appears if the door is already unlocked for an extended period.
Booking entry	**valid single door booking** or **valid door-group booking**

Door opened with extended unlock function

Meaning	The door has been unlocked by an extended-unlock card, or by a time model.
Booking entry	**Door unlocked**

Door closed with extended unlock function

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

Battery change request

Meaning	Red LED signal of one to three seconds' duration. As long as the battery is not completely empty, a card-specific signal will follow. If the batteries are empty, no further signal will be displayed and no bookings will be possible. The battery change request is only displayed for user badges.

Booking entry	The **battery low** entry is shown after every 25 bookings.
Solution	Replace batteries.

17.1.2 Special signals

Read-write confirmation for system cards

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

No card in range

Meaning	The electronics have been activated, however no card has been detected in front of the reader.
Booking entry	No booking made
Solution	Present the badge to the reader again.

Read/write error

Meaning	Failed to read or write to a system card.
Booking entry	No booking made
Solution	Present the system card to the reader again.

Invalid authorization

Meaning	The card has no valid authorization.
Booking entry	**Access denied, card blocked**, **Not authorized**, **Access denied, card expired** or **Booking outside of time frame**

Solution	If necessary, change the authorization for this badge.

Time invalid

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

Door initialization missing

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

Facility data missing

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

Data transmission

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

17.1.3 LED displays for mobile read-write device

Write-confirmation for time model cards

Meaning Data has been successfully written to time model card.

Read-confirmation for the time model card

Figure 17.1:

Meaning The time model card has been successfully read.

Read-confirmation for facility card

Meaning The facility card has been successfully read.

Read/write error

Meaning It was not possible to read or write to the system card successfully.

Solution Hold the system card to the reader again.

Facility data missing

Meaning The timesetter has not been initialized for this facility.

Solution The timesetter must be reinitialized with the facility card.

Time invalid

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

Key:

The length of the colored bars in the examples shown indicates how long the signals are. The length shown here indicates that the signal remains lit for approx. 1 second.

 green LED

 red LED

 orange LED

 blue LED

 - additional acoustic signal

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.

ACE large installation

A large installation in BIS Access Enhgine (ACE) is defined as one having more than 10,000 active cards, or more than 150 AMC controllers

AES

The Advanced Encryption Standard (AES) is a worldwide standard specification for the encryption of electronic data

anti-passback

A simple form of Acces Sequence Monitoring in which a cardholder is prevented from entering an Area twiice within a defined time period, unless the card has been scanned to exit that Area in the meantime. Anti-passback deters a person from passing credentials back through an entrance for use by an unauthorized second person.

Assembly point

a designated place where people are instructed to wait after evacuating a building.

Automated number-plate recognition (ANPR)

The use of video technology to read and process number plates, typically of road vehicles.

Data Managenent System (DMS)

A top-level process for managing access control data in Access Engine. The DMS supplies data to MACs, which in turn supply data to AMCs.

DMS server

Hardware: A computer that hosts the Data Management System (DMS) of Access Engine.

Door model

A stored software template of a particular type of entrance. Door models facilitate the definition of entrances in access control systems.

Entrance

The term Entrance denotes in its entirety the access control mechanism at an entry point: It includes the readers, some form of lockable barrier and an access procedure as defined by sequences of electronic signals passed between the hardware elements.

Gateway (SmartIntego)

An access controller device that controls SmartIntego card readers via radio signals.

IDS

Intruder detection system, also known as a burglar alarm system.

MAC (Main Access Controller)

In access control systems a server program that coordinates and controls the Local Access Controllers, usually AMCs (Access Modular Controller)

Normal mode

In contrast to office mode, normal mode grants access only to persons who present valid credentials at the reader.

Office mode

The suspension of access control at an entrance during office or business hours.

Identification PIN

A Personal Identification Number (PIN) that is the sole credential required for access.

Verification PIN

A Personal Identification Number (PIN) used in combination with a phyisical credential to enforce greater security.

RMAC

A redundant main access controller (MAC) that is a synchronized twin of an existing MAC, and takes over management of its data if the first MAC fails or gets disconnected.

MAC server

Hardware: A computer in an Access Engine network, separate from the DMS server, where a MAC or an RMAC is runs.

SmartIntego

A digital locking system from Simons Voss technologies. SmartIntego is integrated with some Bosch access control systems.

tailgating

Circumventing acces control by closely following an authorized cardholder through an entrance without presenting one's own credentials.

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 Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com