

## Installation Instructions

**IQ MultiAccess, item no. 0296xx**

**IQ SystemControl, item no. 013596**



**P32205-26-0G0-20**

2017-05-22

**Software-Version  
19.xx**

Subject to change  
without notice

Copyright 2017 Honeywell Security. All rights reserved.

The software described in this manual is placed at your disposal in accordance with the General Terms and Conditions of Honeywell Security. It must be used and reproduced only in compliance with the terms of this licence. No part of this publication may be reproduced, stored in data memory systems or transferred, neither electronically, mechanically or in any other way, without prior written authorization by Honeywell Security.

The information in this manual can be modified at any time without notice and can not be viewed as approved by Honeywell Security. Honeywell Security disclaims any responsibility for any errors or inaccuracies that should be found in this manual.

We underscore that, in spite of extensive test series, no guarantee can be made for the reliability of your system due to the numerous PC manufacturers and the possible hardware configurations.

*IQ MultiAccess* is a trademark of *Honeywell Security*

*IBM* is the registered trademark of *International Business Machines Corporation*.

*MS-DOS, Windows, Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP* and *Microsoft* are registered trademarks of *Microsoft Corporation*.

All other products mentioned are registered products of the respective owners.

The manuals are on the CD in PDF format. Reading requires a program that can open PDF files, e. g. Adobe Acrobat Reader.

# Contents

<b>1.</b>	<b>General information</b>	<b>7</b>
1.1	Introduction	7
1.2	Frequently used abbreviations	8
1.3	The central thread / Checklist for Installation	9
<b>2.</b>	<b>General system information</b>	<b>10</b>
2.1	System requirements	10
2.2	Hardware requirements of the Novar peripherals	11
2.3	Handling / backup of database	12
2.4	Client/server principle	14
2.5	Operator concept	15
2.6	Hardware components	16
<b>3.</b>	<b>Program installation</b>	<b>19</b>
3.1	New installation	20
3.1.1	Installation from CD	20
3.1.2	Client installation from a network drive	26
3.2	Initial installation with existing database	28
3.3	Update installation	29
3.3.1	Updating from a previous version of IQ-MultiAccess	29
3.3.1.1	Add new modules	32
3.3.2	Auto Update	32
3.3.3	Update from IQ SystemControl	33
3.3.4	Update from a previous version of IQ SystemControl to current version of IQ SystemControl	34
3.4	Deinstallation	35
<b>4.</b>	<b>Overview and first steps</b>	<b>37</b>
4.1	Starting program IQ NetEdit	37
4.2	Unsuccessful attempts	38
4.3	Delivery status and general description	38
4.3.1	Buttons	40
4.3.2	Menu bar	41
4.3.3	Mouse functions	44
<b>5.</b>	<b>Tabs</b>	<b>45</b>
5.1	ACSx tab	46
5.2	Additional tab (Additional Settings)	49
5.3	Alarms tab	51
5.4	Antipassback/Barring repeated entry tab	52
5.5	Automatic Macro tab	52
5.6	Baudrates tab	52
5.7	Card coding tab	53
5.8	Common tab	56
5.9	Counters/Image matching/Access time recording tab	64
5.10	Daylight saving time	64
5.11	Distant Station tab	64
5.12	Door tab	65
5.13	Door definition tab	65
5.14	Firmware tab	66
5.14.1	ACS-8 Firmware Update	66
5.14.2	ACS-2 firmware update	68
5.14.3	ACS-2 plus firmware update	68
5.15	Inputs tab	69
5.16	Keyboard tab	70
5.17	Key code tab	71
5.18	Manual Macro tab	72

5.19	Multi person AC/Image matching/ATR tab . . . . .	<a href="#">72</a>
5.20	OFFLINE state tab . . . . .	<a href="#">73</a>
5.21	Output tab . . . . .	<a href="#">74</a>
5.22	Parameters tab . . . . .	<a href="#">76</a>
5.23	Reader Settings tab . . . . .	<a href="#">77</a>
5.24	Rights . . . . .	<a href="#">77</a>
5.25	Settings tab (controller/terminal settings) . . . . .	<a href="#">78</a>
5.26	Serial Number tab . . . . .	<a href="#">79</a>
5.27	Tamper monitoring . . . . .	<a href="#">79</a>
<b>6.</b>	<b>Defining hardware / software . . . . .</b>	<b><a href="#">80</a></b>
6.1	Location . . . . .	<a href="#">80</a>
6.1.1	One location . . . . .	<a href="#">80</a>
6.1.2	Several locations . . . . .	<a href="#">81</a>
6.1.3	Change location description . . . . .	<a href="#">82</a>
6.2	Workstation . . . . .	<a href="#">83</a>
6.2.1	Set up a workstation . . . . .	<a href="#">83</a>
6.2.2	Several workstations . . . . .	<a href="#">84</a>
6.3	Software . . . . .	<a href="#">85</a>
6.4	Controllers/Terminals . . . . .	<a href="#">86</a>
6.4.1	Connection versions . . . . .	<a href="#">88</a>
6.4.1.1	Direct connection via RS-232 (COMx) . . . . .	<a href="#">88</a>
6.4.1.2	Connection of read-in stations . . . . .	<a href="#">88</a>
6.4.1.3	Connection via interface converter . . . . .	<a href="#">89</a>
6.4.1.4	Connection via external bus controllers . . . . .	<a href="#">90</a>
6.4.1.5	Connection via internal bus controllers . . . . .	<a href="#">93</a>
6.4.1.6	Connection via Ethernet . . . . .	<a href="#">95</a>
6.4.1.7	Connection via modem / ISDN . . . . .	<a href="#">97</a>
6.4.2	Controller/terminal settings . . . . .	<a href="#">98</a>
6.4.3	Key depot . . . . .	<a href="#">102</a>
6.5	Doors . . . . .	<a href="#">104</a>
6.5.1	ACS-1 . . . . .	<a href="#">104</a>
6.5.2	ACS-2 / 2 plus / 8 . . . . .	<a href="#">105</a>
6.5.2.1	Onboard doors . . . . .	<a href="#">105</a>
6.5.2.2	Module bus doors . . . . .	<a href="#">124</a>
6.5.3	ACT . . . . .	<a href="#">129</a>
6.5.4	AXS4Secure . . . . .	<a href="#">129</a>
6.5.4.1	Scan Onboard Doors . . . . .	<a href="#">129</a>
6.5.5	Doors with locking cylinders . . . . .	<a href="#">131</a>
6.5.5.1	General description . . . . .	<a href="#">131</a>
6.5.5.2	Offline cylinder / fitting . . . . .	<a href="#">132</a>
6.5.5.3	Online cylinders / fittings via traffic point RS485 . . . . .	<a href="#">135</a>
6.5.6	Connectivity to SALTO Ship System - Doors with cylinders/door fittings . . . . .	<a href="#">137</a>
6.5.6.1	General description . . . . .	<a href="#">137</a>
6.5.6.2	Configuration of SALTO Ship (SVN) off-line cylinder/door fitting . . . . .	<a href="#">139</a>
6.5.6.3	Transfer of SALTO Ship (SVN) data to IQ NetEdit . . . . .	<a href="#">140</a>
6.6	Configure RDT / Distant Station . . . . .	<a href="#">141</a>
6.6.1	Configure modem . . . . .	<a href="#">141</a>
6.6.2	Configure ISDN card (B-channel) . . . . .	<a href="#">143</a>
6.6.3	Bus controller at distant station . . . . .	<a href="#">145</a>
6.6.3.1	Configure bus controller . . . . .	<a href="#">145</a>
6.6.3.2	Configure controllers/terminals at the bus controller . . . . .	<a href="#">146</a>
6.6.4	Controllers/terminals connected directly to a distant station . . . . .	<a href="#">147</a>
6.6.4.1	ACS-1 . . . . .	<a href="#">147</a>
6.6.4.2	ACS-2 / ACS-2 plus / ACS-8 . . . . .	<a href="#">147</a>
6.6.4.3	TRSxx . . . . .	<a href="#">148</a>
6.6.5	Modem initialization . . . . .	<a href="#">149</a>
6.6.5.1	The initialization string . . . . .	<a href="#">149</a>
6.6.5.2	Initialization procedure for distant station modems . . . . .	<a href="#">153</a>
6.6.6	Connection Test . . . . .	<a href="#">156</a>
6.6.7	When is a connection established? . . . . .	<a href="#">156</a>

<b>7.</b>	<b>Icon-related functions</b>	<b><a href="#">158</a></b>
<b>8.</b>	<b>Operators</b>	<b><a href="#">166</a></b>
8.1	Define operators	<a href="#">166</a>
8.1.1	Superuser	<a href="#">166</a>
8.1.2	Personnel manager	<a href="#">167</a>
8.1.3	Location manager	<a href="#">169</a>
8.1.4	System manager	<a href="#">171</a>
8.1.5	Shadow manager	<a href="#">171</a>
<b>9.</b>	<b>Definitions of input and output states</b>	<b><a href="#">172</a></b>
9.1	Outputs	<a href="#">172</a>
9.2	Inputs	<a href="#">173</a>
<b>10.</b>	<b>Functional test and minimum configuration</b>	<b><a href="#">174</a></b>
10.1	Procedure	<a href="#">175</a>
10.2	Booking with test ID card	<a href="#">183</a>
10.3	Troubleshooting	<a href="#">183</a>
<b>11.</b>	<b>Several locations</b>	<b><a href="#">185</a></b>
<b>12.</b>	<b>Collective doors used by several mandators</b>	<b><a href="#">190</a></b>
<b>13.</b>	<b>Programs supporting the installation</b>	<b><a href="#">199</a></b>
13.1	IQ Monitor	<a href="#">199</a>
13.2	IQ SysMonitor	<a href="#">201</a>
13.3	AEPInfo	<a href="#">202</a>
<b>14.</b>	<b>Additional programs / functions</b>	<b><a href="#">204</a></b>
14.1	IQ MultiVPS	<a href="#">204</a>
14.1.1	Installation	<a href="#">204</a>
14.1.2	Settings in IQ NetEdit	<a href="#">204</a>
14.2	User-defined fields	<a href="#">206</a>
14.2.1	Creation and use	<a href="#">206</a>
<b>15.</b>	<b>Integration of an Intruder Alarm Control Panel (IACP)</b>	<b><a href="#">209</a></b>
15.1	General description	<a href="#">209</a>
15.2	Integration of "Classic" MB-Panels	<a href="#">209</a>
15.3	Preconditions	<a href="#">213</a>
15.3.1	PC - Software AC	<a href="#">213</a>
15.3.2	PC - Hardware	<a href="#">213</a>
15.3.3	Intruder alarm control panels	<a href="#">213</a>
15.4	Procedure	<a href="#">214</a>
15.5	Data exchange	<a href="#">232</a>
15.5.1	Data acceptance from IACP	<a href="#">232</a>
15.5.2	Data transmission from IQ MultiAccess	<a href="#">233</a>
15.6	Data administration via IQ MultiAccess / IQ SystemControl	<a href="#">235</a>
15.7	Evaluations in IQ MultiAccess / IQ SystemControl	<a href="#">235</a>
15.8	Further information	<a href="#">235</a>
15.9	Checklist for IACP linking (MB-classic panels)	<a href="#">236</a>
15.10	Integration of MB-Secure panels	<a href="#">239</a>
15.11	Preconditions	<a href="#">240</a>
15.11.1	PC - Software AC	<a href="#">240</a>
15.11.2	PC - Hardware	<a href="#">240</a>
15.11.3	Intruder alarm control panels	<a href="#">240</a>
15.12	Procedure	<a href="#">241</a>
15.13	Data exchange	<a href="#">248</a>
15.13.1	Data acceptance from IACP	<a href="#">248</a>
15.13.2	Data transmission from IQ MultiAccess	<a href="#">249</a>
15.14	Data administration via IQ MultiAccess / IQ SystemControl	<a href="#">250</a>

---

15.15	Evaluations in IQ MultiAccess / IQ SystemControl .....	<a href="#">250</a>
15.16	Further information .....	<a href="#">250</a>
15.17	Checklist for IACP linking (MB-Secure panels) .....	<a href="#">251</a>
<b>16.</b>	<b>Door guard connection .....</b>	<b><a href="#">253</a></b>
<b>17.</b>	<b>Mifare DESFire EV1 data carrier .....</b>	<b><a href="#">253</a></b>
17.1	Installation .....	<a href="#">253</a>
17.1.1	Changing the key .....	<a href="#">255</a>
17.1.2	Setup of IQ KeyChanger .....	<a href="#">256</a>
<b>18.</b>	<b>Connection of TBS biometric readers .....</b>	<b><a href="#">257</a></b>
18.1	Installation TBS-Software .....	<a href="#">257</a>
18.2	Install and configure TBS devices .....	<a href="#">259</a>
18.3	Start BioManager .....	<a href="#">261</a>
18.4	Connection to IQMA .....	<a href="#">262</a>
18.4.1	Setting up IQ NetEdit .....	<a href="#">262</a>
18.4.2	Set up IQ MultiAccess .....	<a href="#">264</a>
18.5	Set up address on TBS-Terminals .....	<a href="#">265</a>
18.6	Connection to Access Controller (ACS-8) .....	<a href="#">266</a>
18.7	Connection to MB Classic panels .....	<a href="#">266</a>
18.8	Connection to MB-Secure panels .....	<a href="#">266</a>
<b>Appendix</b>	<b>.....</b>	<b><a href="#">267</a></b>
	<b>Modifications against the previous version .....</b>	<b><a href="#">267</a></b>
	<b>IQ MultiAccess products .....</b>	<b><a href="#">268</a></b>
	<b>Index .....</b>	<b><a href="#">269</a></b>

# 1. General information

## 1.1 Introduction

These installation instructions will guide you step by step in easy language through the installation and commissioning process.

To keep these installation instructions to a reasonable size, basic knowledge in operating the Windows user interface is assumed and not enlarged upon.

When setting up the individual controllers/ terminals, modules etc., repetitive entries must be made in identical tabs. These tab entries and their meaning will be explained in advance at a central position so that this manual remains clearly structured (and does not get too complex). In the individual chapters, a reference to this description will then be made.

Program ***IQ NetEdit*** is the central part of the ***IQ SystemControl*** and ***IQ MultiAccess*** package where the installer makes the complete hardware definitions, incl. the system settings (according to the user's directives). Settings which the user must (can) make himself are therefore limited to options of the daily business and are made in the application part of ***IQ SystemControl*** or ***IQ MultiAccess***.

The visible and so usable options depend on the installed license.

Some functions within ***IQ MultiAccess*** are only possible by activation of additional options with costs. ***IQ SystemControl*** is a subset of IQ MultiAccess, which is restricted to one location and intruder alarm control panels. However, the basic work with IQ NetEdit is - within the activated possibilities - identic for both systems. For IQ SystemControl there is especially chapter 15 = Connecting an intruder alarm control panel of interest.

All controllers/terminals shown in this manual are units with the maximum extension level. The standard functions required for ***IQ MultiAccess***, however, are already included in the basic models of the relevant units. Necessary extensions will be referred to in the individual example. For firmware requirements of the individual devices see chapter 2.2.



The maximum values (e.g. number of workstations, controllers, terminals, doors etc.) are to be taken into account for all installation options. Please see the documentation of the individual units and the corresponding general software for more detailed information.

When assigning computer names, please note that all computer names must correspond to the Microsoft NetBios conventions (15 characters max.; no special characters). If this is not the case, it might happen that a client cannot log on to the server.

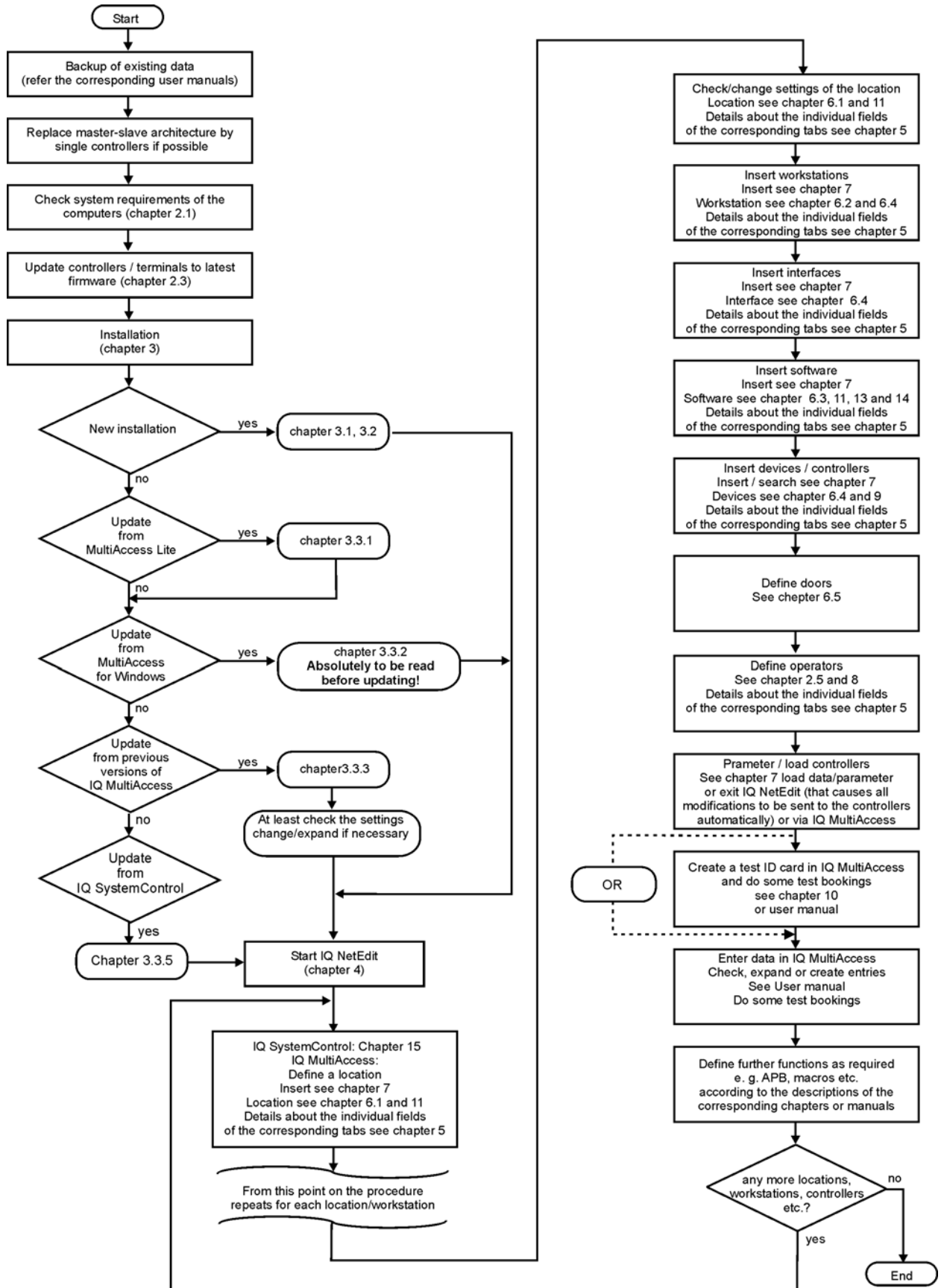
## 1.2 Frequently used abbreviations and terms

(in alphabetic order)

ACS-1	Access control system
ACS-2 / ACS-2 plus /	Access control system, as an alternative to ACS-1
ACT	Access control terminal
AC Controller	Access control controller
BC	Bus controller
APB	Antipassback
CL	Current Loop
Default settings	Basic settings in delivery condition (concerning switches, jumpers for hardware and entries in various tabs)
DVA	Destination Virtual Address, see event log
EU	Evaluation Unit
IACP	Intruder Alarm Control Panel (sometimes used: IDCU Intrusion Detection Central Unit)
MBxxx	IACP 561-MB24, 561-MB48, 561-MB100
MVA	My Virtual Address, see event log
PC	Personal Computer
SSV/-W	Interface multiplier/converter
TRSxx	Time recording terminal (xx = 8, 15)
TR Terminal	Time recording terminal



### 1.3 The central thread / Checklist for Installation



## 2. General system information

### 2.1 System requirements

IQ NetEdit is part of the program package IQ SystemControl / IQ MultiAccess. The system requirements are therefore the same as for the application software. These are:

	Recommended size	
	Server	Client
<b>Processor</b>	Intel (R) i7	Standard PC with latest operating system
<b>RAM</b>	16 GB	min. 4 GB
<b>HDD</b>	min. 1 TB	min. 500 GB
<b>Security</b>	RAID1 (= disk mirroring)* / UPS (= uninterruptable power supply)* * required for server only	
<b>Monitor with corresponding graphic card</b>	19" 1152 x 864 Pixel	
<b>Operating system</b>	Windows Server 2008 R2 / 2012 R2 / Windows 7/8/10 (32/64 bit) <b>Server / Client:</b> Use preferably 64 bit operating system.	
<b>Other requirements</b>	DVD-ROM Drive	
	Mouse, trackball or another Windows-compatible view device (PS/2 recommended)	
<b>For network applications</b>	Network card with TCP/IP-protocol	



If IQ MultiAccess resp. IQ SystemControl is installed on a computer with a 64-bit operating system, the ODBC registration is no longer at: Start → control panel → Administrative Tools → Data sources → Data sources (ODBC). This registration is reserved for 64-bit ODBC drivers only. To see or to change the settings of the ODBC registration at a 64-bit operating system, run the program (Administrator rights required to run the program):  
C:\Windows\SysWOW64\odbcad32.exe

IQ SystemControl **and** IQ MultiAccess can not be installed/run coeval on one computer. An upgrade from IQ SystemControl to IQ MultiAccess is possible. If IQ MultiAccess is installed, IQ SystemControl can not be installed any more.

## 2.2 Hardware requirements of the Novar peripherals

IQ NetEdit supports the following hardware as of software / firmware release:

- External bus controllers item no. 026 815.00 as of software release ZDICO.01.0V08.00  
     **For APB:** Item no. 026 815.10 as of software release ZDICO.02.0V02.02
- Internal bus controller as of version 1
- ACS-1 as of software release ZACS1.03.0V06.01
- ACS-8 as of software release ZACS1.00.0V06.00
- ACS-2 as of software release ZACS1.00.0V06.01
- ACS-2 as of software release ZACS1.00.0V06.00
- ACT as of software release ZACTA.00.0V03.00
- AXS4Secure As of firmware release V4.8.x  
     Programming software IQ PanelControl as of V4.8.x  
     necessary for initial start-up.
- For analogue transmission: Modem certified by Novar/Honeywell (see chapter 6.6)
- For ISDN transmission: ISDN card with capi 2.0  
     ISDN modem with Capi 2.0
- For IGIS-LOOP transmission: IGIS-LOOP controller (if necessary in a separate  
     housing with power supply unit and battery)
- IK3 EU firmware: as of P08.03
- Central units 561-MB24, 561-MB48, 561-MB100 (devices with item no. index .10):  
     as of firmware V09  
     Programming software WINFEM-Advanced (from V07  
     on).
- Central unit MB-Secure: as of firmware V4.6.x  
     Programming software IQ PanelControl (as of V4.6.x).
- Dialling devices (ISDN)
 

DS 7600	as of V02.14
DS 7700	as of V02.14
DS 9500	as of V02.14
DS 9600	as of V02.14
- Dialling devices (IP)
 

DS 7700	as of V02.14
DS 6700	as of V03.xx (IQ SystemControl only from V6 on)
DS 6750	as of V03.xx
- Dialling devices (analogue)
 

DS 6600	as of V02.xx
DS 6700	as of V03.xx (IQ SystemControl only from V6 on)
DS 6750	as of V03.xx



We generally recommend to install the most recent firmware release so that all new functional extensions can be used (this relates especially to the external bus controller). Firmware updates are dependant on the device and are implemented either via EPROM exchange or flash update. Please see the documentation of the individual devices for more detailed information.

## 2.3 Handling / backup of database

There is no knowledge required to supervise the Firebird database included. Appropriate programs for automatical installation, administration and maintenance are part of IQ MultiAccess. Connecting another database requires appropriate knowledge of the installer or the customer’s system administrator<sup>1</sup>.



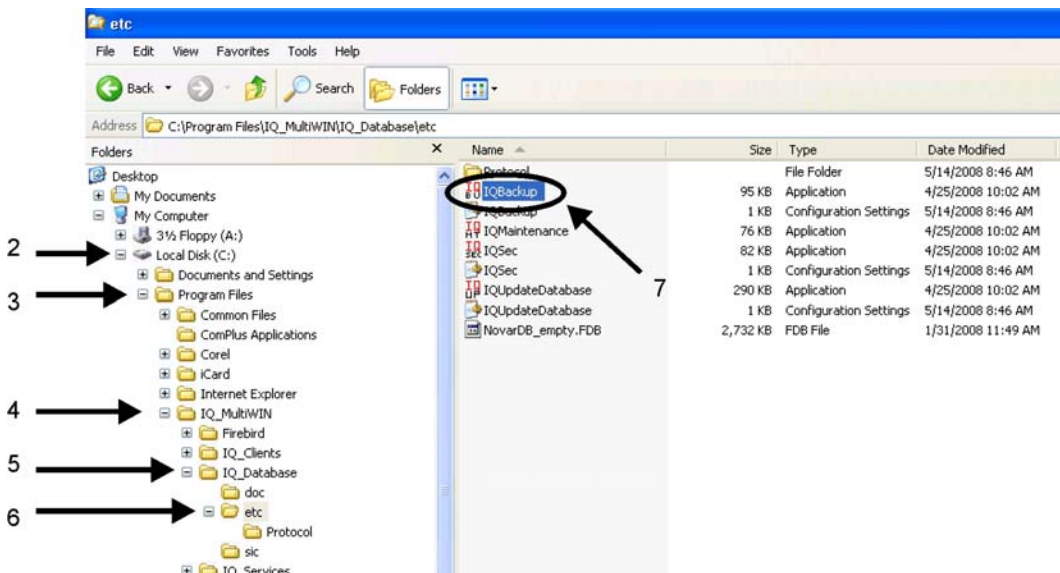
**Caution!**

**Never copy the database when the system is in operation!**

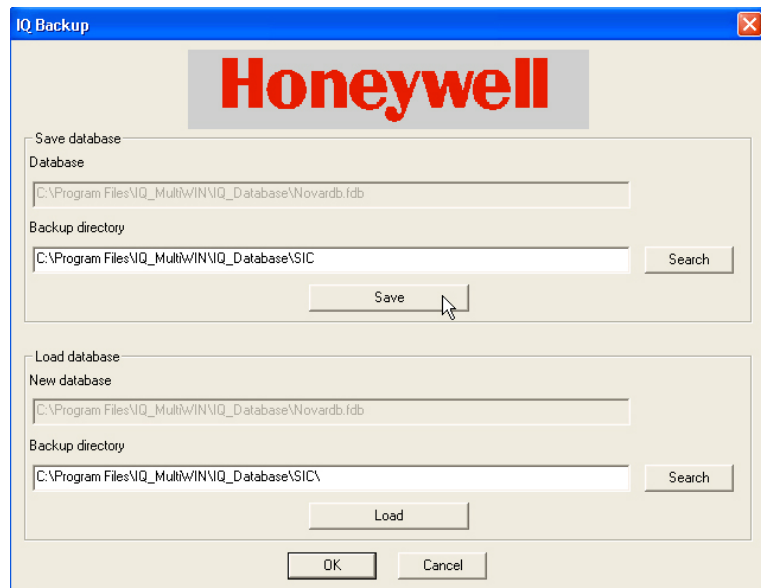
**Correct procedure:**

1. Open explorer
2. - 7. Double-click **IQBACKUP.EXE** in the directory

C:\Program Files\IQMultiWin\IQDatabase\etc

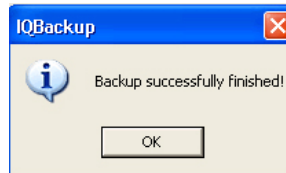


8. Select a path where to copy the backup of the database or accept the default settings.
9. Button **Save**.



<sup>1</sup> Only possible with professional package and prior consultation.

10. Confirm message with **OK**



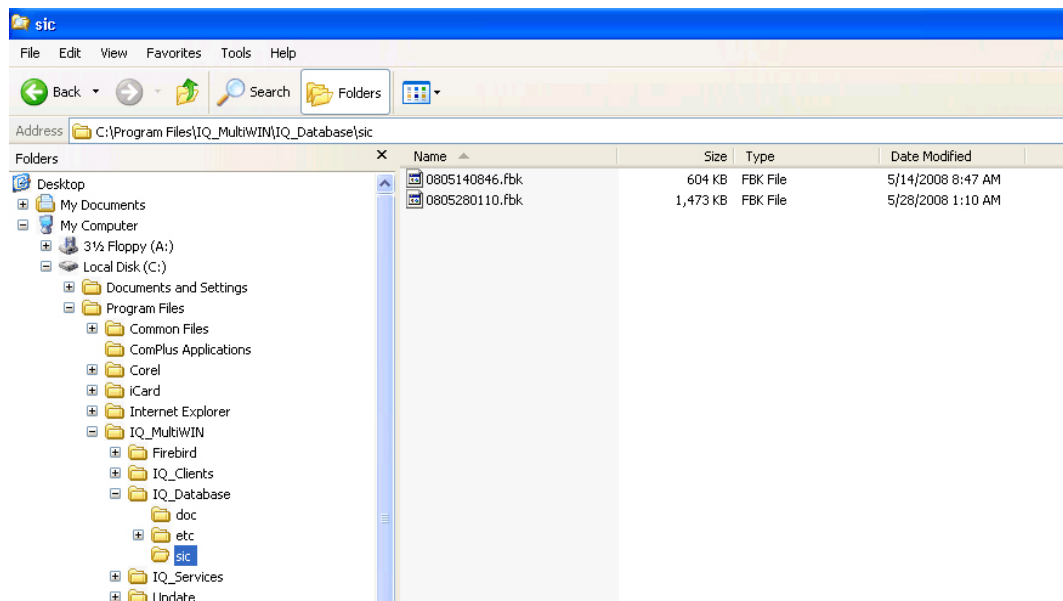
11. Now the backup-file is in the selected directory.

(Factory setting: C:\Program Files\IQMultiWin\IQDatabase\sic).

The file name is <date><time>.fbk.

Example: 0805280110.fbk

That means, the file has been saved on May, 28<sup>th</sup> 2008 at 01:10 AM.



This file can be copied onto a data carrier during the system is in operation.



We recommend to create a time task for an automatical cyclic backup (see user manual, chapter 11.7). This can also be started manually if required.

**Load data** can be used to restore a previously backed up database from the backup directory to the directory ...IQ\_MultiWin\IQ\_Database. However, the name of the backup file will remain.

If this file is to be used from now on, the services **IQ CommTask**, (**IQ Server** and **IQ UpdateServer**) must be stopped, the database renamed to NovarDB.FDB and subsequently the services restarted.



### Caution!

### Data loss possible!

If a previous database is reactivated, the basic master files and bookings comply with the moment of the backup.

As already mentioned never copy the database when the system is in operation. From IQ MultiAccess V11 on it is possible to stop all running IQ Servers and the corresponding IQ Firebird database using the program **IQ StopServers** (Start → all Programs → IQ MultiAccess → IQ StopServers). Important: Administrative rights necessary to start a program from Windows 7 and Server 2008. After that the IQ Firebird database can be copied resp. saved. To start the IQ Servers use the program **IQ StartServers** via Start → all Programs → IQ MultiAccess → IQ StartServers.

## 2.4 Client/server principle

Client/server is a combination of at least two computers that are logically - and usually also physically - separated and that share certain tasks.

The (database) server manages central data and makes them available to all users (clients).

The IQ server is responsible for the central communication between the individual clients and the database server.

These two functions may also run on one computer.

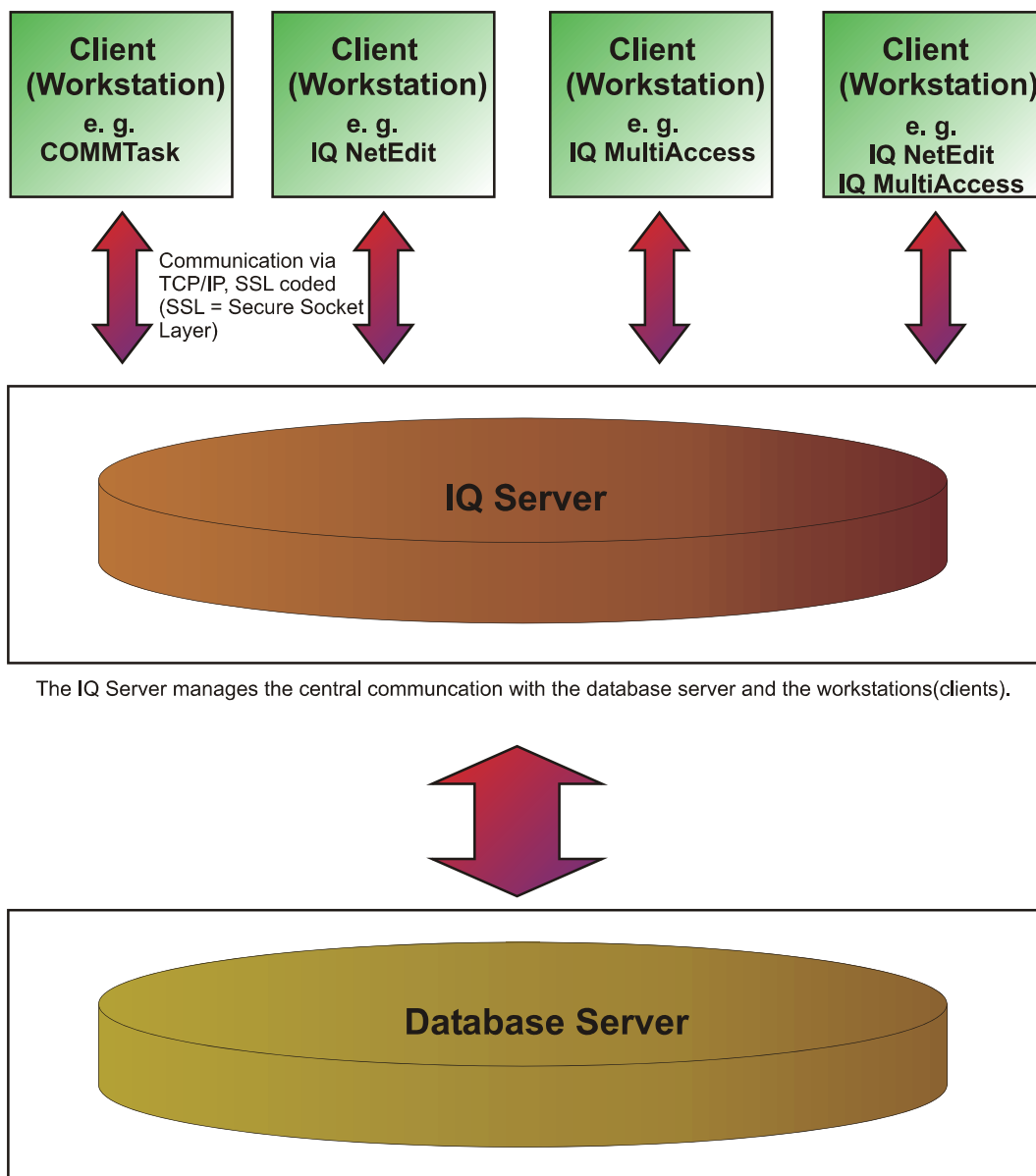
The clients are the actual application programs of the workstations where AC/TR hardware can be connected and managed and where the authorized operators work.

A workstation may handle individual functions (e.g. only manage hardware, only permit work in IQ NetEdit, etc.) or a combination of several individual functions.

In principle, it is also possible to install **all** functions on one computer (this is selected during program installation). In this case, the hardware requirements of the server apply. The logical separation, however, will be maintained.



When assigning computer names, please take care that all computer names comply with the Microsoft NetBios conventions (15 characters max.; no special characters). If this is not the case, it might happen that a client cannot log on to the server.



The IQ Server manages the central communication with the database server and the workstations (clients).

## 2.5 Operator concept

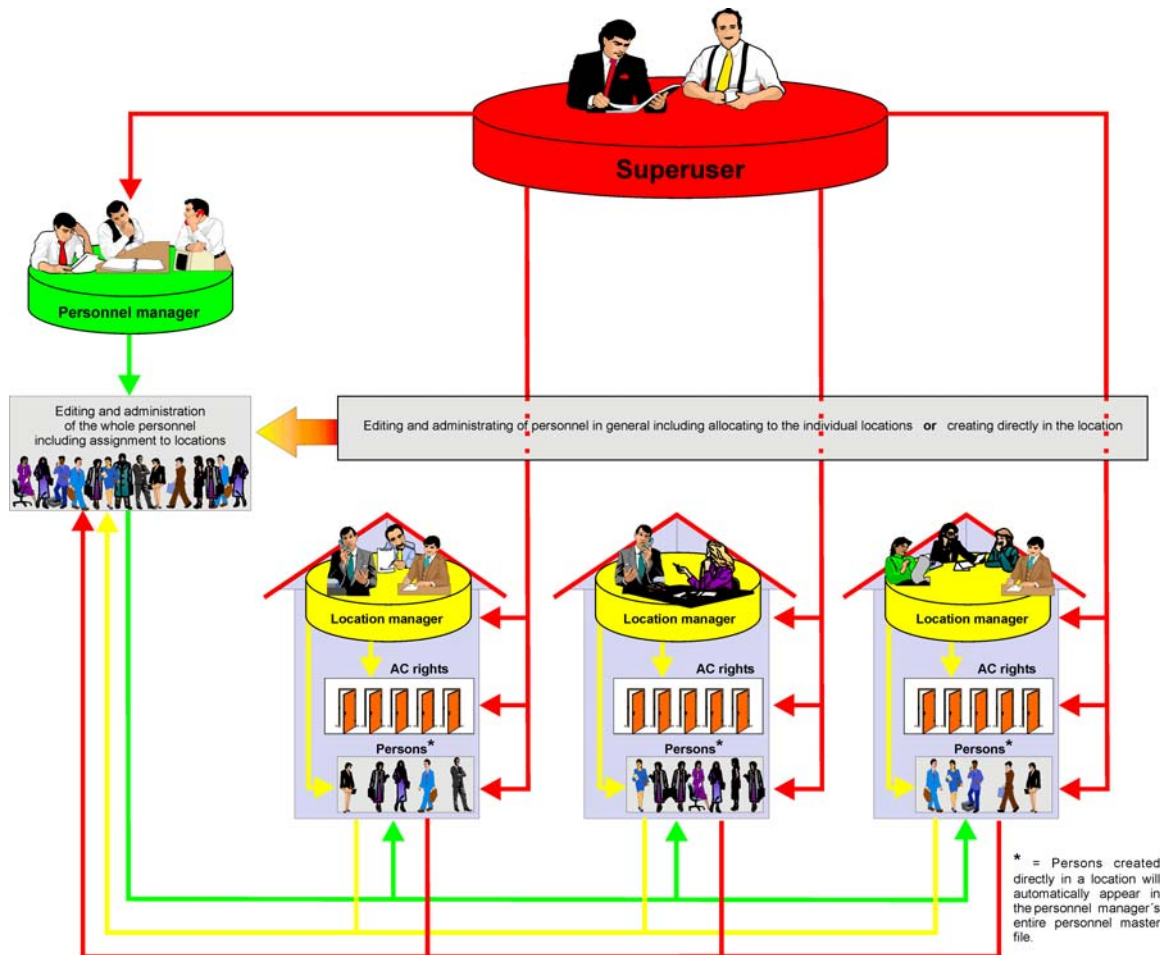
Operators are users with different rights. The product is delivered with one superuser having all rights in the entire system. The superuser defines further operators. These may be other superusers, system managers, personnel managers, location managers or shadow manager. In addition, the superuser can make changes directly in one location and he/she can also work in the general personnel master records of the personnel managers.

Usually personnel managers do not deal with access control as such. In most cases, they are members of Human Resources who centrally define and manage personnel data. Personnel managers can view and access all members of the staff in the entire system and across locations and clients. They can neither view nor access the access control data.

System manager correspond to ("little") superusers with restricted rights. They can have right in all areas of operation except IQ NetEdit.

Location managers are the real users of the access control software at a particular location. They can view only the access control data and persons that are relevant for their location.

Depending on the operator who is logged in, the desktop may be more or less comprehensive. You will find further information about operators and their rights in the Installation Instructions.



Shadowmanager have an exceptional position which enables an access to the same doors by several mandators (see chapter 12).

## 2.6 Hardware components

- ACS-1** The ACS-1 receives the access control rights from "IQ MultiAccess". It works completely "autarkically", so that access control continues to work without any interference even if the PC is switched off or the RS-485 bus is disturbed. All local functions are maintained. Depending on the extension level, it is possible to control one door with one reader, one door with two readers or two doors with one reader each. Further functions can be implemented via the relevant additional boards (cf. documentation of ACS-1).
- ACS-8** The ACS-8 handles basically the same functions as the ACS-1. But in contrast to the ACS-1, it is not available with integrated operating panel, display or integrated reader and can therefore be operated only in connection with a programming and evaluation medium, e.g. with the access control software IQ MultiAccess. An ACS-8 can manage a maximum of 8 doors. The relevant extension and connection options permit a variety of possible installations and combinations (cf. Installer Instructions for the ACS-8 as well as the descriptions below).
- ACS-2** The ACS-2 corresponds to a reduced ACS-8. It can manage a maximum of 2 doors onboard - further extension is not possible. APB/BRE are not supported. Use: for simple access functions within a time recording system.
- ACS-2 plus** The ACS-2 plus corresponds to an ACS-8 without module bus. It can manage a maximum of 2 doors onboard - further extension is not possible, otherwise all ACS-8 functions.
- ACT** The ACT handles basically the same functions as the ACS-1. But in contrast to the ACS-1, it is not available with integrated operating panel, display or integrated reader and can therefore be operated only in connection with a programming and evaluation medium, e.g. with the access control software IQ MultiAccess. An ACT can control only one door.
- AXS4Secure** The AXS4Secure terminal receives access control rights from "IQ MultiAccess". Its operations are completely "autonomous", so that access control is not affected even if the PC is switched off or the Ethernet connection goes down. All local functions continue to remain operational. Depending on the stage of development, the terminal can manage one or two doors with one entry and one exit reader each. Appropriate expansion and connectivity options present several possibilities for deployment and combination (refer to the AXS4Secure Installation/Connection instructions). No support for Anti-passback/time tracking systems. Support for calendar-based room/time zones.

### BC Bus controller

- external bus controller

The external bus controller is responsible for the communication between the PC and the peripherals connected to the individual bus controller (these might be access controllers ACS-1, ACS-2 / ACS-2 plus, ACS-8, time recording terminals TRSxx or additional bus controllers in a master-slave arrangement). The bus controller is generally used as single, master or slave controller. The mode is selected via DIP switches.

Single controller: A single controller can be connected to every COM port of the PC. Each of them controls up to 32 controllers/terminals (ACS-1, ACS-2 / ACS-2 plus, ACS-8, TRSxx).

- internal bus controller

The internal bus controller is a PCI card that can be integrated into the PC and handles basically the same functions as an external bus controller.

- Deviations:
- one internal BC corresponds to two external BCs
  - up to 4 times faster than an external BC
  - 4 internal BCs max. per PC
  - APB is not supported

Allowing for the restrictions stated above, a combination of external and internal BCs is possible.



Client	Workstation/software with individual functions within the program package (see also Chapter 2.2).
Dialling device	DSxxxx, required on an intruder alarm control panel for data transfer (to compare with a modem/ISDN card).
EU	Evaluation Unit of IACP doors/switching devices. Readers/operating units are connected to evaluation units and their information will be analysed there.
Interface converter	The pure interface converter is used for conversion of RS-232 to RS-485. It is equipped with an RS-232 input interface and two RS-485 output interfaces connected in parallel and supports 3-wire and 5-wire technology.
Key depot	<p>A key depot is used for managing keys which may be taken out according to certain rights. IQ MultiAccess manages key depots manufactured by Kemas.</p> <p><b>Important:</b>When ordering a key depot from Kemas, please note that a device with a firmware that is compatible to MultiAccess is required.</p> <p>In IQ NetEdit and IQ MultiAccess, the key depot is treated like a controller / terminal. Key depots that were already managed via MultiAccess for Windows are not compatible to IQ MultiAccess. They must be upgraded. For details concerning the key depot see section 6.4.3 as well as the relevant Kemas documentation.</p>
Locking cylinder	Independent electromechanic device in the form of a door knob or door handle with appropriate intelligence to open/close a door. The administration of access data and the evaluation of the bookings take place in IQ Cylinder/IQ MultiAccess. The data transfer happens via a PDA.
MBxxx	Intruder alarm control panels of the type series 561-MB24, 561-MB48, 561-MB100 and MB-Secure. IQ MultiAccess is able to communicate with and to administrate their data (data carriers, room/timezones and authorizations).
PC	IQ NetEdit can be installed on a stand-alone computer or on any PC within a network. The AC/TR hardware can be distributed among all PCs in the network. IQ NetEdit and the access control rights can be accessed from all defined PCs.
PDA	Commercially available hand held computer / organizer (e. g. PALM) for data transfer between IQ Cylinder/IQ MultiAccess and locking cylinders.
Server	Computer that manages central services and/or data and makes them available to the clients (see also chapter 2.2).
Services	Services are certain (administration/system) programs which are required for correct working of the individual applications. The services required for the program package IQ MultiAccess are installed automatically in the course of the installation and are started even before the user log-in, similarly to the hardware drivers.
SSV-/W	<p>The interface multiplier/converter can be used if individual controllers/terminals must be connected over longer distances or if a star-shaped cabling is the better option for an installation. The interface multiplier/converter has 8 slots on the output side which can be equipped optionally with RS-232, RS-485 and Current Loop.</p> <p>Restriction: When RS-485 interfaces are used, the maximum equipment on the output side is 4 RS-485 interfaces with and 4 without potential separation.</p>
Switching device	Reader, keypad, operating device of an intruder alarm control panel. IQ MultiAccess interprets them as readers/keypads of a door.
TRSxx	<p>TRS 8 and 15 are time recording terminals which receive their master data from the central TR software and then work autarkically.</p> <p>Entries are buffered even during OFFLINE operation. Special entries (e.g. balance /holiday inquiries, absent on business) can be made via function keys.</p>

Please see the updated product list for the current terminal models. Older models are listed for reasons of compatibility.

#### W&T COM Port Server

Via RJ45 this device can be installed at any place in the network where it will then provide a COM interface.

If the relevant driver which is available for free download on

[WWW.WUT.DE](http://WWW.WUT.DE)

is installed at a workstation, this additional COM port is available on the individual PC.

This means for IQ NetEdit: Another COM interface is defined at the PC where the driver is installed and it will behave exactly as an interface that really exists at the PC.

As an alternative, it is also possible to define the COM Port Server as such directly in NetEdit. The control is then made via TCP/IP via the PC to which this COMPortServer has been assigned.

#### USB

Interface to connect external devices, such as read-in stations, cameras, signature pads. For details on installation and setup see original manuals of the individual devices. Description of application see user manual of IQ MultiAccess P32205-20-0G0-xx.

### 3. Program installation

**Requirements:** For the installation, you need the **administrator rights** on each device where the software is to be installed.

The IP address or the computer name of the server should be known (to be required from the responsible system administrator). One of them will be needed during the installation. If neither of them is known, the installation program suggests a dummy address (127.0.0.1), which always refers to the local computer.

The energy options of the computer the software shall be installed must be set in a way the harddisc will not be stopped during the installation and the standby and/or sleep mode will not be activated (best deactivate / set ot **no** before starting the installation).

For applications in conjunction with installed DLC/DLF (door locking cylinders / door locking fittings), the installation of the add-on program DORMA XS-Manager is mandatory before installing IQ MultiAccess /IQ System Control. It is necessary to install the XS-Manager on the same client PC you will install the software IQ Cylinder. The XS-Manager are available in two different versions.

1. XS-Manager 2.7 with PALM-PDA.  
(Runs under operating system Windows 7 (only 32-bit).

With this variant you have to note that the PALM-PDA software has to be installed first and then the software DORMA XS-Manager. Observe if the communication PC-PDA via HOTSync procedure works correctly. The PDA must be switched on and ready for operation. Communication between software and DLC/DLF is made via a PALM-PDA. For detailed information on installation of a Palm-PDA please see the documentation of the PALM-PDA.

2. XS-Manager from 3.2 with mobile PC (Laptop or netbook).  
(Runs under operating system Windows 7 (32/64-bit).

XS-Manger 3.2 is a completely PC-based application. Communication between software and DLC/DLF is made via the IrDA-USB adaptor (022909) in conjunction with the XS-Servicetool (022908).

#### **Important**

**Only one variant has to be installed on the PC/laptop. The simultaneous installation of both XS-Manager variants is not supported.**

Information on the installation of the DORMA XS-Manager are to be found in the documentation of this program<sup>2</sup>. The documentation can be found on the installation CD in the directory drive:\XS-Manager\PC or PDA\XS-Manager x.x\Dokumentation. The installation file Setup.exe for installing the DORMA XS-Manager is to be found in the directory drive:\XS-Manager\PC or PDA\XS-Manager x.x\ Setup.



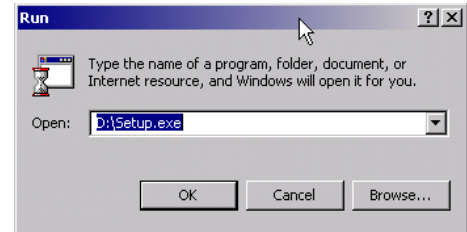
**If an older version of DORMA XS-Manger is installed, please deinstall this version first manually. After this you can install the new version of the DORMA XS-Manager. The operating system Windows Vista is currently not supported.**

## 3.1 New installation

### 3.1.1 Installation from CD

Basically, a **new / initial installation** should be done at the server. From there, the clients (workstations) can be installed.

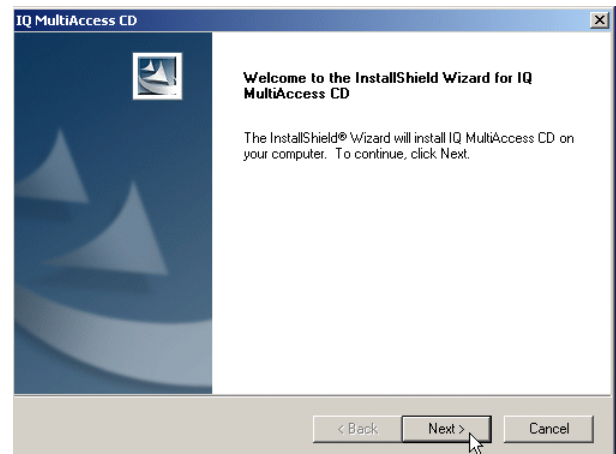
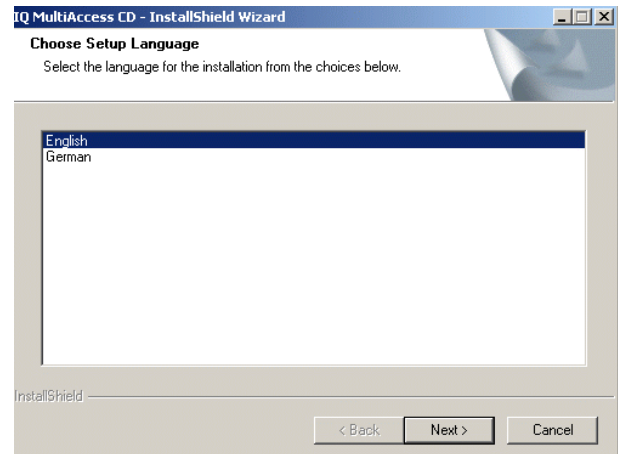
1. Insert installation CD into CD drive. If the autostart function is installed on your computer, the installation will start automatically.  
If not, select Start → Run.  
Change to the CD drive and select the file **Setup.exe**.  
Click on **OK**.



2. Follow the instructions on the screen. We recommend to accept the suggested values with **Next** or **OK**.

Select a **setup language**. You will be guided through the setup in the selected language.

If the setup language has been selected either **German** or **English**, the application will be installed in the same language. A modification of the application language can be done subsequently.

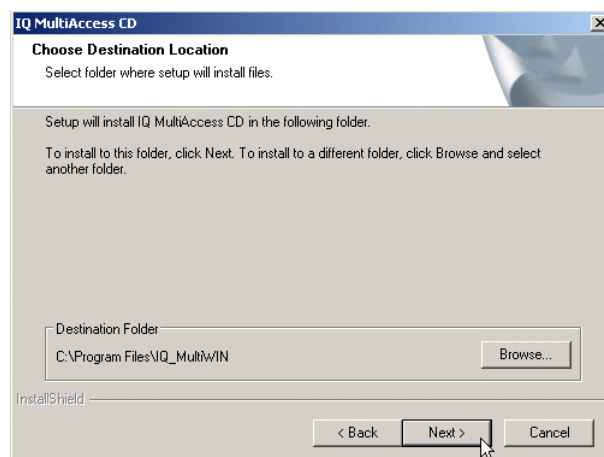


Select **directory** and **path**.

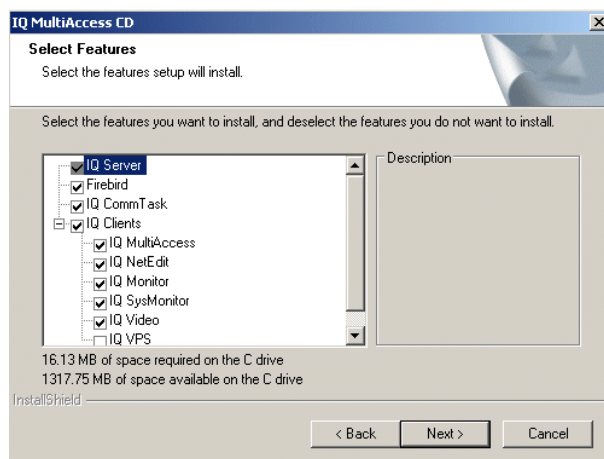
Factory settings:  
**C:\Honeywell\IQ\_MultiWIN**

Recommendation:      **Accept with Next.**

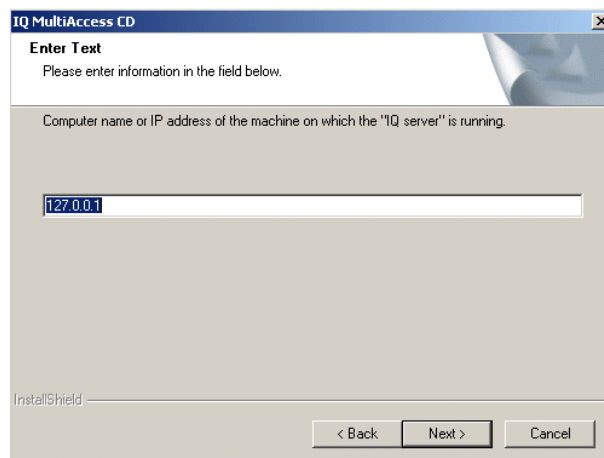
Because of the changed structure of the data, user and rights in Windows 7, IQ MultiAccess from Version 11 on will be installed in the "Honeywell" folder and no longer in the "Programms" folder.



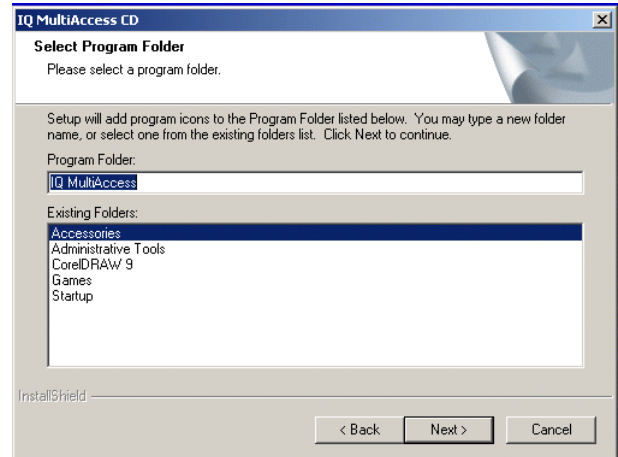
- Select what components are to be installed. According to factory settings, **all preselected** components will be installed (server, client, database and communication). This is the required installation type for the computer used as server. All other options must be selected manually from the menu. Select the required / not required components by activating / deactivating the corresponding box..<sup>3</sup> Some options are with costs. However, they can be selected and installed here, their use will certainly be activated via the corresponding license file. First the **demo version** will be installed. The activation of the customer's license (in case it has been acquired, it will be delivered on a floppy disc or a CD) is described in step 13. Both of the lines below the selection window inform about the required and remaining disc space.



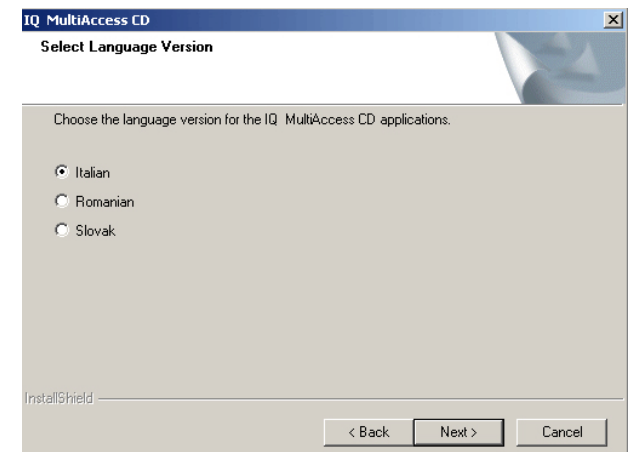
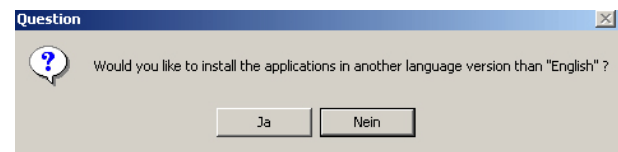
- If **IQ Server** has been selected in step 3 (factory settings), the computer actually being installed will be the server (as required in step 1). The window displayed to the right will be skipped. Continue with step 5. If **IQ Server** has not been selected, there must be defined where the IQ Server program section has been or shall be installed. Enter the IP-address or computer name of the server (to be required from the responsible system administrator, see **requirements** in the beginning of this chapter). As a factory setting the IP-address of the local computer is predefined.



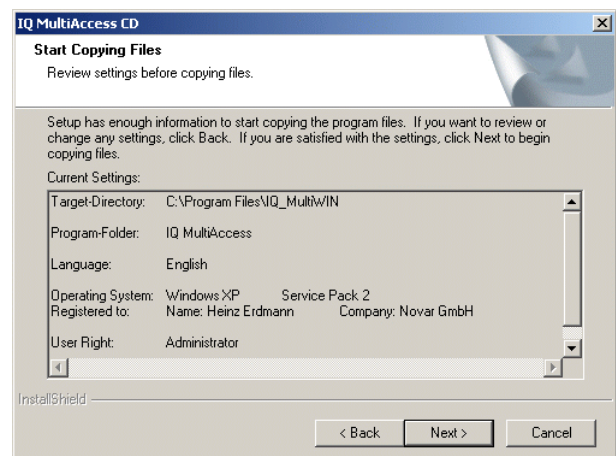
5. Follow the further instructions on the screen. We recommend to accept the suggested values with **Next**. Windows which open up briefly during the installation process only contain information about the activity that is being carried out at the moment. These windows are closed again automatically; entries are not needed / permitted here.



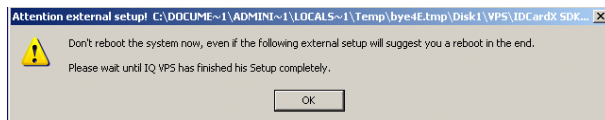
6. If the application is to be installed in a language different to the selected installation language, enter **Yes** when prompted.<sup>4</sup>  
**No** installs the application in the same language as the installation language (factory settings).



7. Check and confirm the entries. Click **Next** if everything is ok, otherwise click **Back** to return to the individual settings.



- 8. If additional programs (e.g. the V.P.S card designer program) are installed (which is the case if → **complete installation** has been selected), the installation routine will additionally branch to the external installation(s). Each of these installations is ended by the request to reboot the computer.



**This is not necessary! It is sufficient to restart the computer when the request for rebooting is displayed at the end of the entire installation routine.**

Just confirm with **OK**

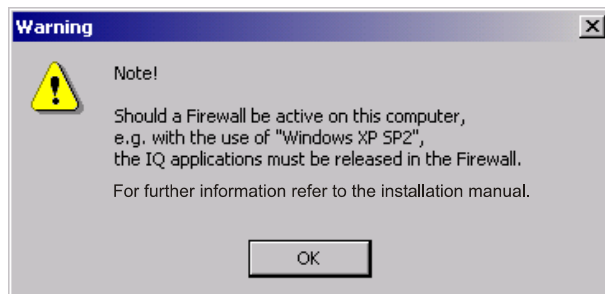
- 9. The program now branches automatically to the relevant installation routine(s) of the selected / possible additional program packages.

Example: Installation routine of the V.P.S. card designer program



Click the **Setup** button and follow the instructions on the screen. Recommendation: Accept the values that are suggested. Skip the request to reboot the computer after installation of each product part by **Cancel** or **Ignore**. For details please see the documentation of the individual products.

- 10. At the end, a note will be displayed that tells you to release the executable programs and services used by IQ MultiAccess in the firewall (if there is one installed).

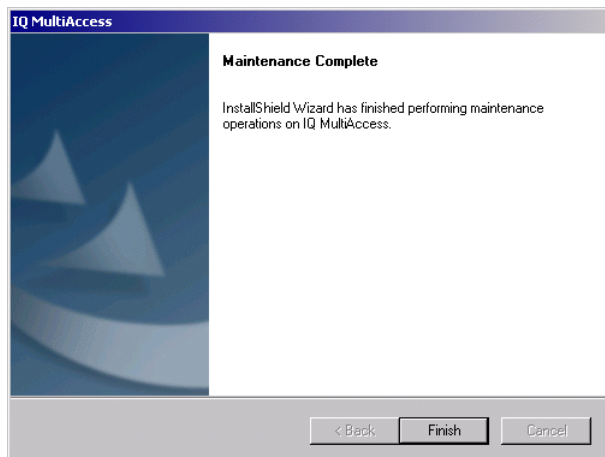


Confirm with **OK** and complete the installation

- 11. After all partial installations have been completed, the installation routine will return to the actual IQ MultiAccess installation program.

→ **Finish.**

The computer is rebooted (confirm factory setting).



- 12. If no firewall is used, the demo version is now installed and ready for operation. If a firewall is installed, step

14 must be carried out in addition.

13. Install user licence.

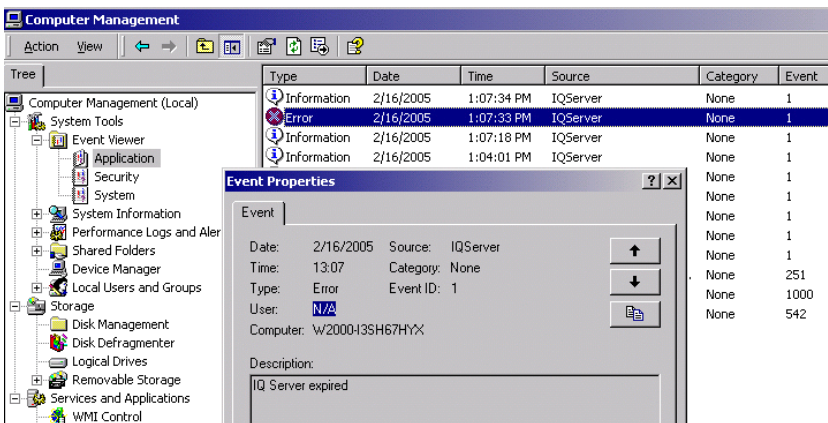
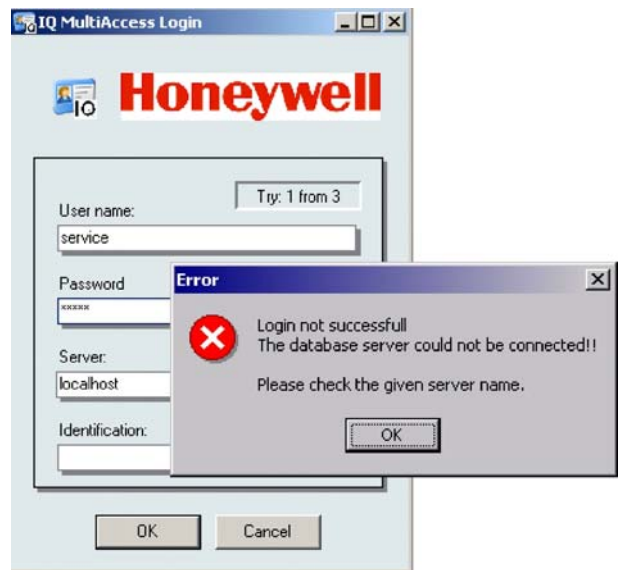
The demo licence is installed automatically with the first installation. It is restricted to 500 days, 10 persons and one location and standard functions. Chargeable options are not included.

The options that you have actually purchased will be activated by the customer-specific user licence. The latter will be supplied on a storage medium together with the delivery or acquired later. File **IQ.LIZ** on the storage medium must be copied to directory **...IQ\_MultiWINIQ\_Services** of the server (computer on which the complete installation has been carried out). The demo licence is overwritten in the process.



**After a change of licence, a reboot is recommended. At least the IQ Server must be stopped and restarted!** (Control Panel → Administrative Tools→ Services).

If there is no licence (demo or full version) or if the demo licence has expired, it is no longer possible to start IQ MultiAccess including its components.



You will find a corresponding entry in the Event Viewer (Start → Control Panel → Administrative Tools → Event Viewer), e.g. see figure.

14. Update firewall

If a firewall is used, it might be necessary to carry out a manual registration of executable files and/or services, depending on the manufacturer and the configuration of IQ MultiAccess. Please contact your system administrator for this. We recommend to reboot the computer once more afterwards.



IQ MultiAccess and the database Firebird supplied with it use the following executable files:

IQ MultiAccess	
Services	IQSERVER.EXE *1 *2 IQCT.EXE *1
Executable files	IQMA.EXE *2
	IQNETEDIT.EXE *2
	IQMONITOR.EXE *2
	IQSYSTEMON.EXE *2
	IQ_CONV_V7.EXE
	IQCYLINDER.EXE *2
	IQSEC.EXE *2
	IQBACKUP.EXE *2
	IQKEYCHANGER.EXE *2
	IQLDAP.EXE
	IQMAINTENANCE.EXE *2
	IQOPUNIT.EXE *2
	IQUPDATEDATABASE.EXE *2
	IQPRINTSERVER.EXE
	IQTBSYNC.EXE
	IQSQL.EXE
	IQUPDSRV.EXE *2
	IQVIDEO.EXE
	IQVISITOR.EXE
	IQVPS.EXE
	IQVTABLEAU.EXE
	IQDTABLEAU.EXE
Firebird	
Services	FBGUARD.EXE *2 FBSERVER.EXE *2
Executable files	Firebird ODBC *2, if required

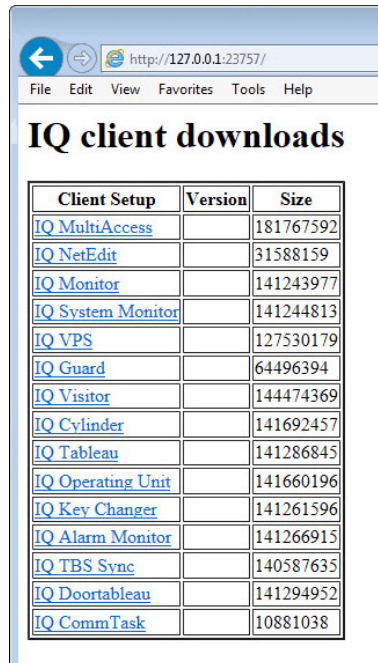
\*1 IQServer Listener Port is number 23757. It is used for all SSL-protocol packages and the http connections.  
In addition, the FTP Listener might be added, which can be configured freely in Global Settings of IQ NetEdit.

\*2 Executable files for IQ SystemControl.

### 3.1.2 Client installation from a network drive

In larger network systems, it is enough to do the installation of the server (as described in chapter 3.1.1). Here with the installation files for the clients (workstations) will automatically be stored on the server.

- The installation can be run at each workstation directly from the server by entering the IP-address of the server in a Web browser application (such as the Internet Explorer) without any need of inserting the installation CD at each individual workstation.
- Click on the link of the components to be selected.



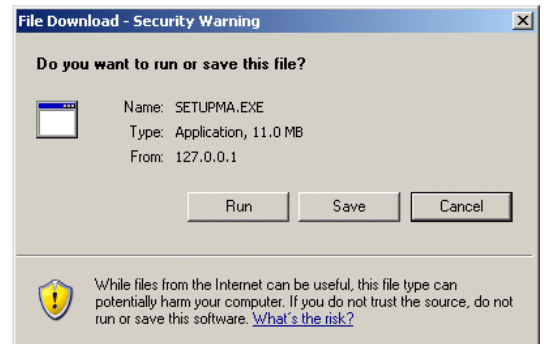
The screenshot shows a web browser window with the address bar containing 'http://127.0.0.1:23757/'. The page title is 'IQ client downloads'. Below the title is a table with three columns: 'Client Setup', 'Version', and 'Size'. The table lists various client components and their corresponding sizes.

Client Setup	Version	Size
<a href="#">IQ MultiAccess</a>		181767592
<a href="#">IQ NetEdit</a>		31588159
<a href="#">IQ Monitor</a>		141243977
<a href="#">IQ System Monitor</a>		141244813
<a href="#">IQ VPS</a>		127530179
<a href="#">IQ Guard</a>		64496394
<a href="#">IQ Visitor</a>		144474369
<a href="#">IQ Cylinder</a>		141692457
<a href="#">IQ Tableau</a>		141286845
<a href="#">IQ Operating Unit</a>		141660196
<a href="#">IQ Key Changer</a>		141261596
<a href="#">IQ Alarm Monitor</a>		141266915
<a href="#">IQ TBS Sync</a>		140587635
<a href="#">IQ Doortableau</a>		141294952
<a href="#">IQ CommTask</a>		10881038

**Run:** The setup of the selected file is going to be started immediately.

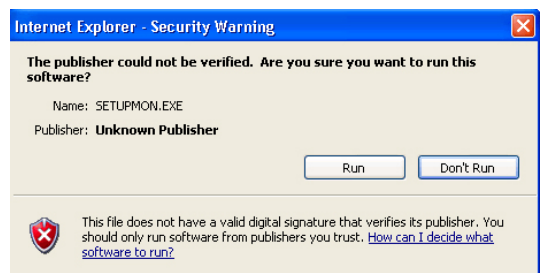
Follow the on-screen instructions (in general they correspond to the information of chapter 3.1.1).

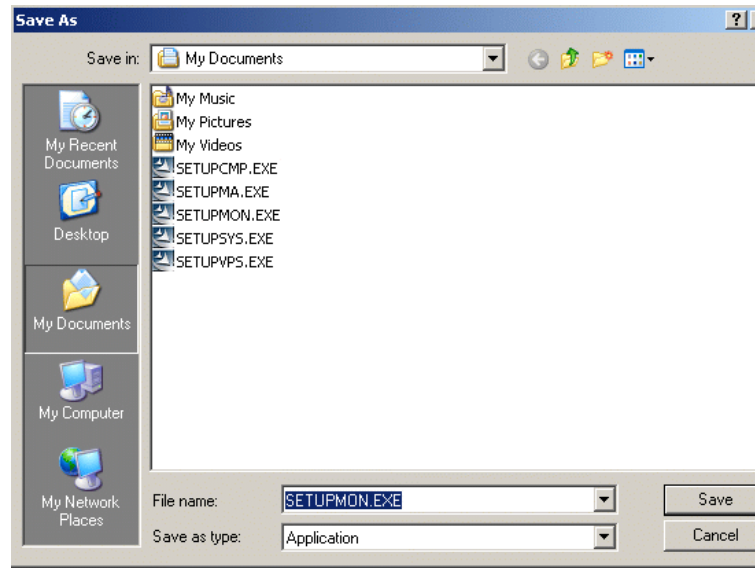
**Save:** The selected setup file will be saved on the local computer (preferred under "Documents and Settings \ My Documents", another place can be selected).



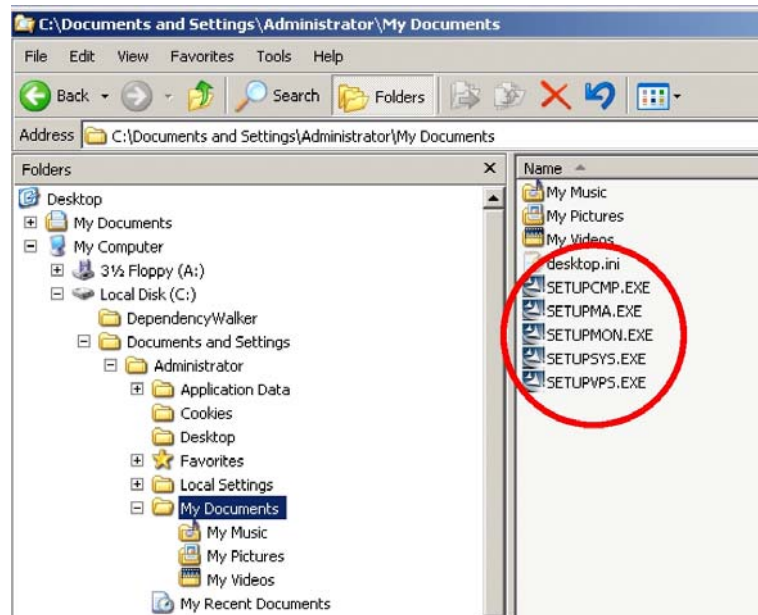
Due to the safety settings within Windows, a safety warning might be output when the installation is made from a "non local" drive, e.g. a network drive.

This warning is generated directly by WINDOWS. If you know where the file comes from (e.g. CD supplied by us or download from our homepage), **this warning can be skipped** for the installation.





Double-click the setup for execution.



## 3.2 Initial installation with existing database

If a database is already existing, not the basic kit will be installed (as described up to here), but the professional kit. The differences to the basic kit are:

- either do not install (deactivate the component) "firebird database" in the install setup
- or run the standard installation and afterwards deinstall the firebird database manually.

In both cases a manually connection to the existing database must be set up.

With copy deadline there existed prepared adaption tools to the databases:

- Microsoft SQL Server (incl. MSDE)
- ORACLE
- MySQL

At the moment, adaptations to other databases are only possible on request (ODBC drivers required).



**For the adaption of the professional kit to another database as firebird (even via the above mentioned tools) a database administrator is absolutely required, who is to be provided either by the user or the installer.**

The latter is also relevant if a firebird database is already in use. The installation routine neither installs an empty database as normal, if it recognizes an already existing entry of a firebird database in the registry, nor modifies the existing database. In this case there are also manual adaptations necessary. Best to talk to our support **before** starting the installation, if there might be some more necessary preparations.

Update installations from IQ MultiAccess do not require any further manual activities.

### 3.3 Update installation



We strongly recommend to make a data backup before starting an update!  
Prefer to save the backup files in a directory that is not used by IQ SystemControl or IQ MultiAccess.



The manufacturer assumes no liability in case of data loss and all directly or indirectly resulting disadvantages.



We generally recommend to check the master data after data transfer from other programs and to complete / correct them manually if necessary. Only then should these data be passed on to another program.



Data backup has changed against MultiAccess for Windows. (For detailed information see user manual (P32205-20-0G0-xx), chapter 17.7 Backup as a time task). Data backup using IQ SystemControl see user manual (P03118-20-0G0-xx), appendix 2.7.

#### 3.3.1 Updating from a previous version of IQ-MultiAccess

If up to now the locking cylinder option has not been used, the following steps are not necessary. Continue reading after the dividing line.

**Before the update:**



As of IQMA version 9 / IQSC version 4 cylinders / fittings can handle IK2 and IK3 data carriers. If there are already doors with offline cylinders / fittings in use, their bookings and events must be collected **before installing the IQMA version 9 / IQSC version 4**, because it will not be possible to assign them anymore after the installation and will be lost.

**Precondition for the operation of online cylinders / fittings:**

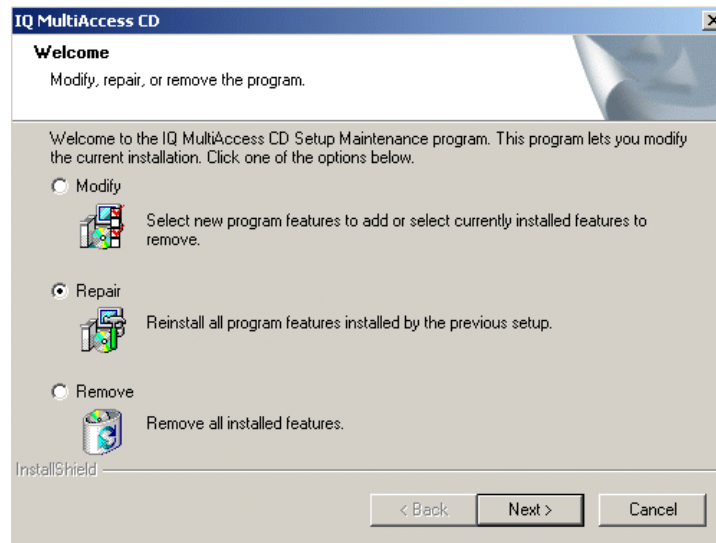
- ACS-8: Firmware version 8.xx (component of IQMA V10 / IQSC V5)
- Online door fittings: Firmware 3.49f\_8, 29.01.10 or higher<sup>5</sup>
- Online cylinders: Firmware 4.44r\_2, 26.01.10 or higher<sup>5</sup>
- IQ Cylinder V10.xx (component of IQMA V10 / IQSC V5)
- On Palm/PDA: XS-Manager minimum version 2.6.4 (delivery of IQMA V10 / IQSC V5 includes the appropriate latest version).

In order to transfer both the latter components correctly when installing IQMA V10 / IQSC V5 it is recommended to delete the files **XS-Manager**, **AESL**, **BeschlagListViews** and if existing **BeschlagErrorsRel** and **DoorInfoRel** from the Palm before starting the update installation / after collecting the offline cylinder data (cf. original manual of the PDA) and to deinstall the programs **IQ Cylinder** and **XS-Manager** from the computer used for communication with the PDA (cf. chapter 3.4) and subsequently run the HotSync process.

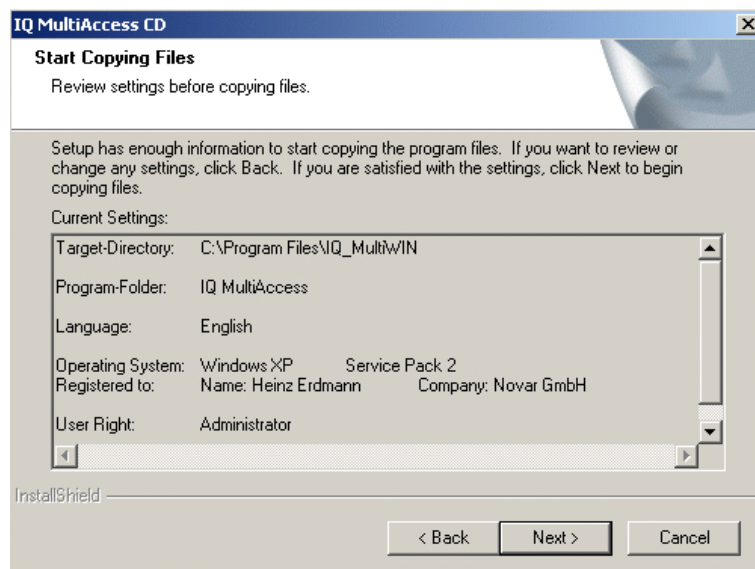


As from now on the cylinders / fittings can handle IK2 and IK3 data carriers, the data must be send to the cylinders (cf. user manual P32205-20-0G0-xx, chapter 21.2), even if there is no coloured highlight indicating any data modifications.

If a previous version is already installed, the following window opens after starting the setup:



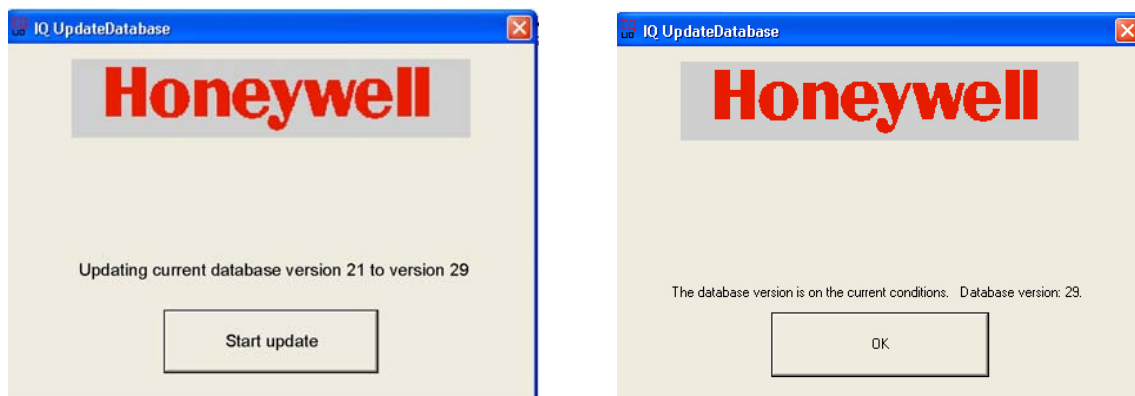
**Repair** is the factory setting. Accept this setting with **Next**. The installation routine of version 3 will now install exactly the same variant that had been installed before with version 1/2.



That means, if a complete installation had been carried out with a previous version, an upgrade to the complete new version will be carried out - **including all additional programs contained in the previous version**. If any chargeable options are required, they must be purchased and activated in the licence file. Otherwise, the programs are available but they cannot be used.

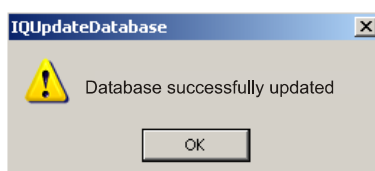
**Exception:** V.P.S card designer program: A demo licence for this product is provided and installed together with the installation via IQ MultiAccess. A full licence is to be obtained from V.P.S. For details please see the documentation for the product in question.

After the installation is completed, the database is converted automatically to the new format by pressing the **Start Update** button.



For technical reasons, the database version and the program version are not identical. The information above can be ignored.

After the conversion, confirm with **OK** in the window shown above. The next message must also be confirmed with **OK**.



The note concerning release of the IQ MultiAccess programs and services in a firewall that might possibly be installed is displayed as a reminder at this point of the installation process as in case of a first installation (cf. section 3.1.1, step 6 and 10).



If the firewall entries had already been made with the installation of a previous version, they still exist even after deinstallation of IQ MultiAccess. Normally, there is no need to make these entries once more after an update installation<sup>6</sup>.



The licence file of the previous version is automatically adapted to the new version. All options of the previous version are maintained in the new version.

No other manual entries or settings are required.

---

<sup>6</sup>

This depends on the used firewall and should be checked in any case.

### 3.3.1.1 Add new modules

Reinsert the installation CD after updating via **Repair** (see chapter 3.3.3) and select **Modify**. The already installed modules are automatically activated (checkbox active). **Never remove these activations**, but activate the new modules **in addition**.



**Caution!**

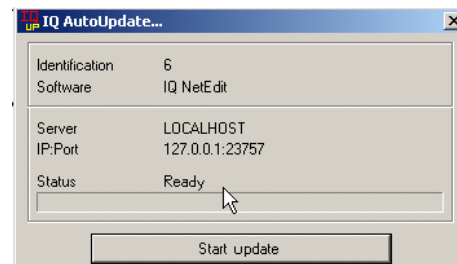
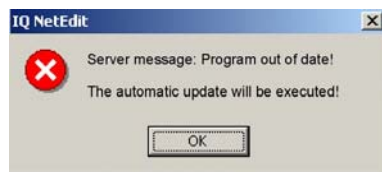
**Loss of data possible!**  
**All not marked program modules will be deinstalled!**

For options with costs, the license accordingly extended must be installed (cf. chapter 3.1.1, step 13).

Before adding **IQ Cylinder**, the computer used for the communication must be prepared accordingly (cf. chapter 3.1.1, preliminary remarks and step 9, example 2). The XS-Manager installation is described there.

### 3.3.2 Auto Update

By installing version 3 or higher, the system will be prepared to run all update installations that will follow automatically at the workstations (for multi-user systems). That means, a new program release (new version or service pack) must only be installed once manually at the server. During the start of each workstation there is an automatical check whether the installed program version of the workstation fits to the version of the server. If not, the user will be guided through the automatic update installation by the dialogue displayed below:



From version 5 on, this is also possible for users with restricted rights.

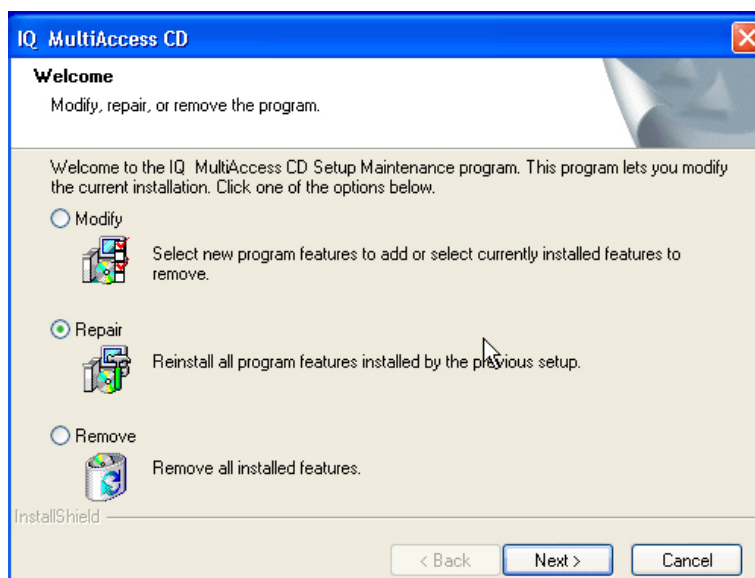


### 3.3.3 Update from IQ SystemControl to IQ MultiAccess

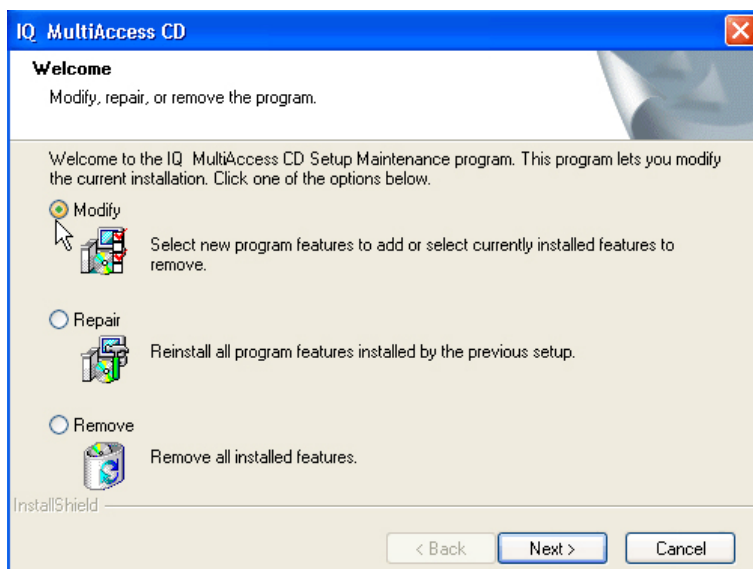
We recommend to save the license file (IQ.LIZ in ...IQ\_MultiWin\IQ\_Services) in addition to the standard data backup (see chapter 3.3) before start updating.

If there are already offline door cylinders / fittings in use, chapter 3.3.3 paragraph **Before the update** must **absolutely** be executed.

The installation procedure is similar to a new installation of IQ MultiAccess according to chapter 3.1.1. As IQ SystemControl is already installed on the computer, the setup offers the selection shown below:



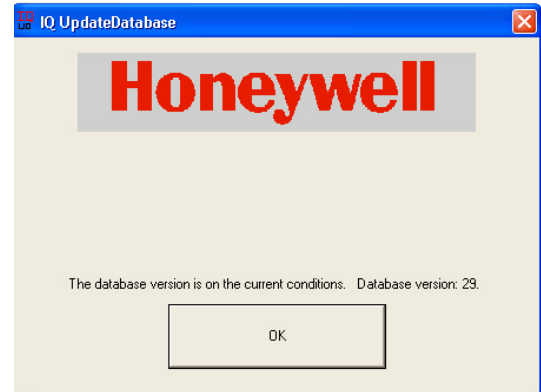
As a default setting **Repair** is preselected. Select **Modify**, then **Next**.



Select the components required (see chapter 3.1.1, step 3). The install shield installs IQ MultiAccess using/extending the already existing database with all entries of IQ SystemControl.

Follow the screen instructions and confirm with **Next** (see also chapter 3.1.1 and the following page).

When the installation has finished, the the database will be converted to the new format if necessary by clicking the button **Start update**. Otherwise only the ormation of the current version must be confirmed with **OK**.



For technical reasons, the database version and the program version are not identical. The information above can be ignored.

Confirm with **OK** after the conversion has finished.

---

#### Caution!



At this time the demo license of IQ MultiAccess is installed which causes that the already existing intruder alarm control panels will no more be displayed. You just have to copy the customer's license (with option IACP-connection!), see chapter 3.1.1, step 13.

---

### 3.3.4 Update from a previous version of IQ SystemControl to current version of IQ SystemControl

The update from a previous version of IQ SystemControl to the current version complies with the descriptions of chapter 3.3.3 with one exception: There are no AC components to select.

Information on door fittings / locking cylinders see chapter 6.5.4. However, preparing the PDA / communication computer are necessary in this case.

### 3.4 Deinstallation

Normally there is no need of deinstalling the program manually. As far as this should be necessary at all with an update installation, it will automatically be done by the installation routine.

If nevertheless the program kit IQ MultiAccess must be removed from a computer, proceed as follows:

1. Save database if you want to continue using it later on. The database is to be found in directory ...**IQ\_MultiWIN\IQ\_Database** and is called **NOVARDB.FDB**.



Do **not** save the database in a directory under IQ\_MultiWIN, since this directory including all subdirectories will be deleted afterwards.

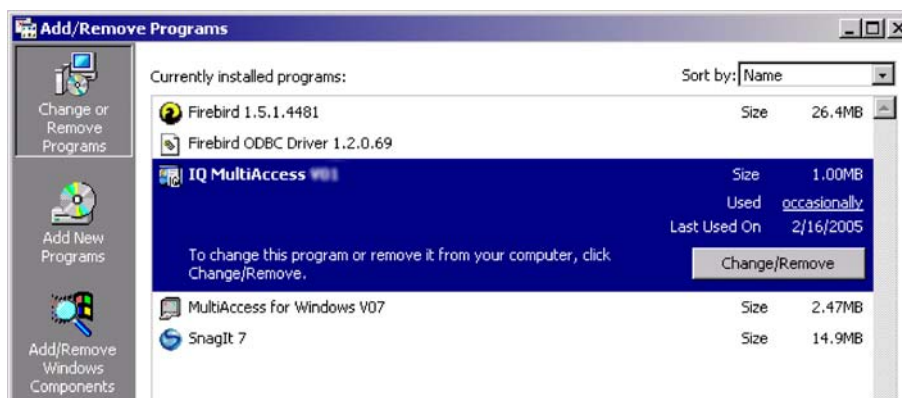
**The manufacturer assumes no liability for loss of data and all directly or indirectly resulting disadvantages.**

2. Start → Control Panel → Software

Here you will find a list of all subprograms of IQ MultiAccess. Each of them must be removed one after another.

- They are called:
- IDCardX SDK (if existing)
  - IQ CommTask
  - IQ Cylinder
  - IQ Monitor
  - IQ MultiAccess CD
  - IQ MultiAccess
  - IQ NetEdit
  - IQ Sysmonitor
  - IQ Video (if existing), as of V7 new name IQ Guard
  - IQ VPS (if existing)
  - IQ Visitor (if existing)
  - IQ Vtableau
  - IQ Dtableau
  - IQ TBSSync
  - IQ AlarmMonitor
  - XS-Manager

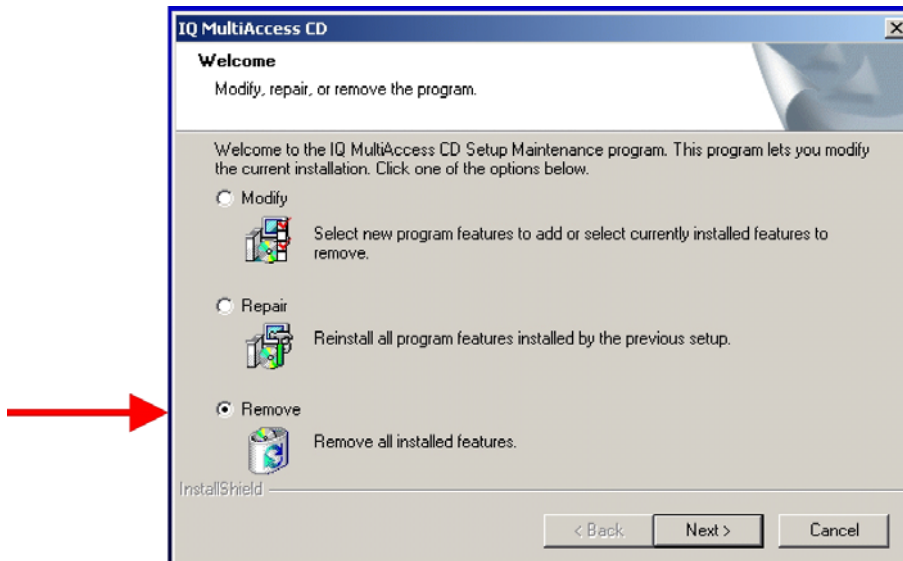
Select each single entry and click on **Change/Remove**<sup>7</sup>.



<sup>7</sup>

The version number behind the program name indicates which version is installed at the moment (in the example version 1 will be deinstalled).

3. Select **Remove Program** in the installation routine and follow the on-screen instructions.



Selecting **IQ MultiAccess CD** deinstalls all components of IQ MultiAccess including the database and its components.

You will be asked, if the firebird database and their ODBC drivers should also be deinstalled. Answer with **Yes**.

In between there might be the question if you also want to deinstall some common used system files. Here you can select **Yes to all**.



The finally recommended restart of the computer should absolutely be done (Answer the question with **Yes**, which causes an automatical reboot).



Products / options being installed via a separate setup, have to be deinstalled separately as well (XS-Manager, David, ID Card SDK). For this, see original manuals of the corresponding products.

4. Delete the entire directory **IQ\_MultiWIN** incl. all subdirectories and if necessary all directories of the deinstalled 3<sup>rd</sup> party products after the restart.

## 4. Overview and first steps



After the installation, IQ NetEdit can **only** be started on the computer on which the IQ Server runs. In the example below, **all** program components are installed on **one** computer (Server installation).




**Caution**

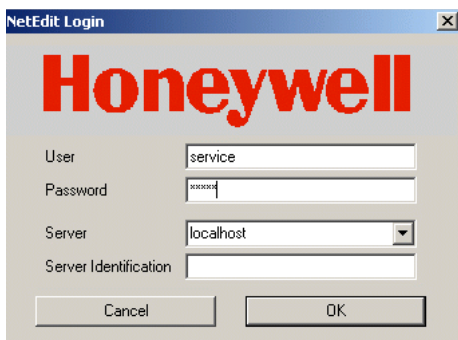
**Unwanted door functionality possible!**

On exiting IQ NetEdit the controllers automatically get parameterized if modifications have been made that require a parameterization. Within this time the doors are out of function. The factory setting of IQ NetEdit is to leave the program automatically after 5 minutes if no input has been done within this time period.

Due to this, it is recommended not to connect any hardware at first and/or to enter a **→ start time for delayed factory reset** (see chapter 3.3.2 and 5.3) and/or to set the **→ time for auto logout** to 0 = no auto logout (see chapter 4.3.1 and 5.3).

### 4.1 Starting program IQ NetEdit

Start program **IQ NetEdit** on the computer where the software has been installed via Start → All Programs → IQ MultiAccess → IQ NetEdit or the corresponding icon .



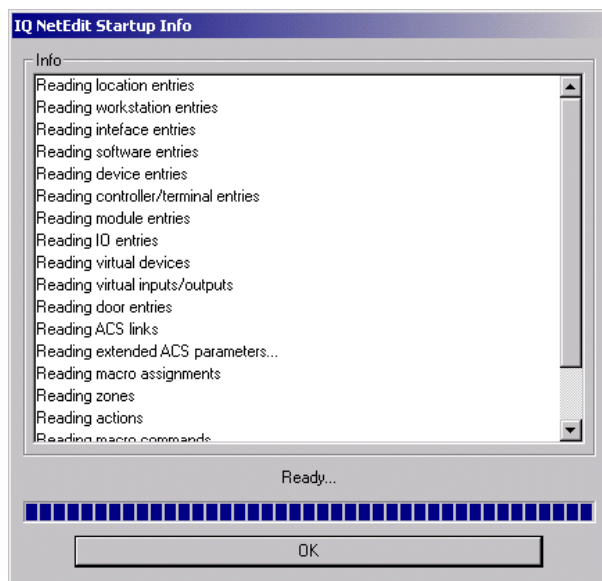
**User name:** service  
**Password:** novar  
**Server:** localhost or 127.0.0.1  
 (These values apply if the IQ Server runs on the local computer. This is the case with first/standard installations).

**Server Identification:** no input.

Modification of these values and the resulting effects will be described in chapter 11 = Several locations and chapter 6.2.2 = Multi-user installation.

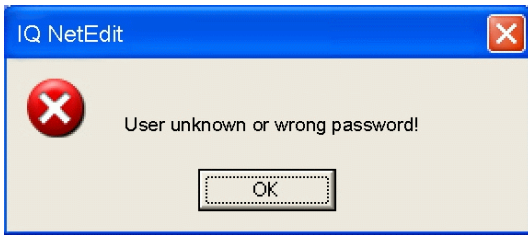
Button **OK**.

While the program is being loaded, this info window will be briefly displayed. It will close automatically after 10 seconds, when all relevant information has been read in, but it can be closed prematurely by clicking the **OK** button.

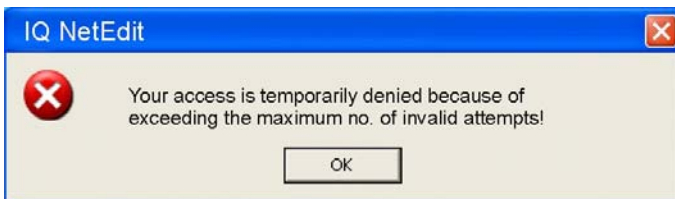


Before recording the hardware, the default settings of the location(s) must be checked/set (reader-/DIN-settings, controllers etc., see 10.1).

## 4.2 Unsuccessful attempts



Per location there can be defined how many unsuccessful login attempts are allowed and for which time period after exceeding the maximum number of attempts a login is not possible any more. The factory setting for both of them is "0", which means "no restrictions". These values are applicable to all programs that require a user name and password to login.

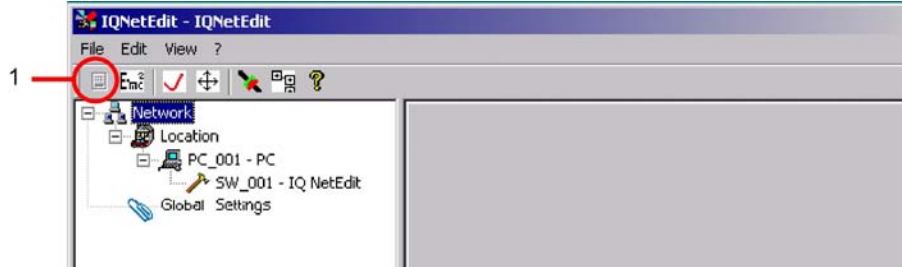


After exceeding the maximum number of unsuccessful attempts a login is not possible for the time period that is determined in the installation program.

## 4.3 Delivery status and general description

IQ NetEdit distinguishes between two modes of representation. The physical representation shows the hardware configuration (computers, controllers, terminals, readers, keyboards etc.). The logical representation shows operators and door authorizations/configurations. Operators are persons who are authorized to work in the access control software.

The physical representation (1) is activated automatically.



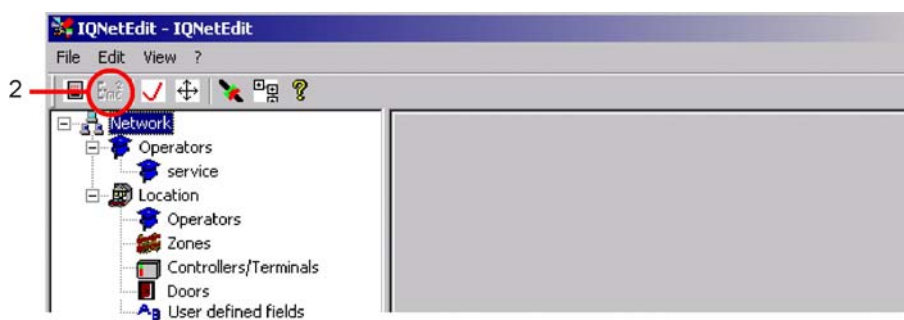
**Network:** Superordinate system for managing the entire hardware.

**Location:** Physical location of the devices /clients used.

**PC:** Generally: All (at least one) computers physically existing at one location.  
Here: The PC on which the IQ Server has been installed.

**SW\_xxx:** Software which is authorized on the individual computer. In the delivery status, the **IQ NetEdit** software is already assigned to the pre-configured computer. By assigning the relevant software to a particular computer you determine which computer can operate which program. At the moment, only program **IQ NetEdit** can be operated from this computer.

Logical representation by clicking on button(2).



**Operators:** Persons with different rights within the AC software. Operators on a higher level than a location have cross-location or location-independent rights. Operator **service** (as we are logged in at the moment) is pre-configured in the factory. This operator corresponds to the administrator and has **all** rights in the entire system. In the further process, he/she defines the individual users as other operators with their individual rights.

If operators are assigned to a location, their rights are only valid within this location.

With **IQ SystemControl** one operator **scuser** with password **scuser** exists as factory setting in addition to the operator **service**. The user rights of this operator correspond to the requirements of IQ SystemControl.

Users can save their personal settings for the design interface and settings for the window size and position in IQMA. If a user has limited operating system rights (Windows), an alternate storage path for personal settings can be set using the following registry key:

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Novar\IQ MultiAccess]
"PathToIQMADData"="D:\IQsettings\my_user" → the file path entered here must be accessible to the user.
```

**Zones:** Each location can be subdivided into zones. This is necessary if you work with → Antipassback (APB) and/or → Barring Repeated Entry (BRE). APB is available as of V2 and described in a separate documentation (Supplementary functions of IQ MultiAccess, as of P32205-46-0G0-01).

**Controllers/Terminals, Doors:**

In the factory setting, these icons exist per location, but the configuration can only be made when terminals/controllers have been configured in the physical representation.

**User defined fields:**

There are a maximum of 40 fields to be individually defined. They can be used as additional fields in the personnel master file.

### 4.3.1 Buttons



#### Save automatically

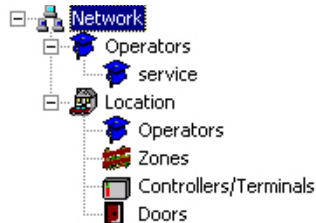
Each modification must be confirmed before it is stored. If this button is pressed, it is saved automatically without confirmation prompt.



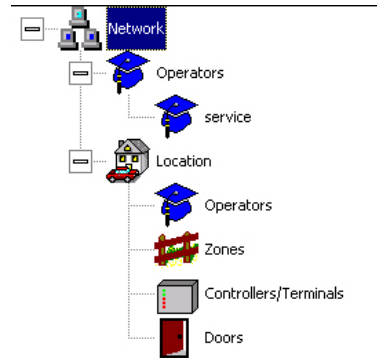
#### Large icons

When this button is pressed, the size of the representation is changed.

##### Normal



##### Large Icons



#### Log off

When this button is pressed, the current user logs off from NetEdit without terminating the program. The dialogue window opens up. This function is to prevent unauthorized persons from working in NetEdit.

#### Log off automatically



**If no entry is made in the program for the time period defined, the current user will be logged off automatically.**

If modifications have been made which require a parameterization of the controllers/terminals concerned, this will be carried out automatically after log off. The doors concerned are out of function during this time.

#### Defining a time period for auto log off

For each software a time period (in minutes) can be entered in the → **Common** tab (see 5.3).

The user will be logged off if no entry appears within this time period.



#### Caution

#### Unwanted door functionality possible!

On exiting IQ NetEdit the controllers automatically get parameterized if modifications have been made that require a parameterization. Within this time the doors are out of function. The factory setting of IQ NetEdit is to leave the program automatically after 5 minutes if no input has been done within this time period.

Due to this, it is recommended not to connect any hardware at first and/or to enter a → **start time for delayed factory reset** (see chapter 3.3.2 and 5.3) and/or to set the → **time for auto logout** to 0 = no auto logout (see chapter 4.3.1 and 5.3).

If the same user logs in again afterwards, the database connection gets reestablished (the program restarts and is in the standard user interface of the selected program).

The factory setting of its time period is 5 minutes. If "0" is entered, the auto log off function is not active.



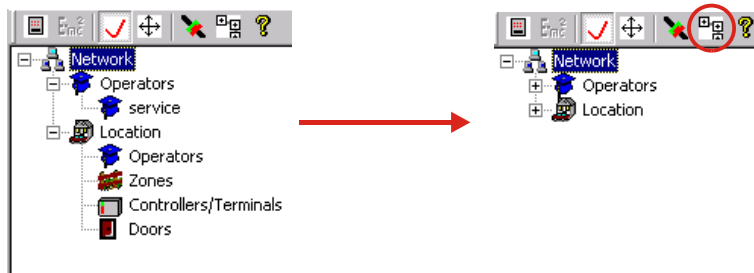
This modification requires a restart of IQ NetEdit to become active.





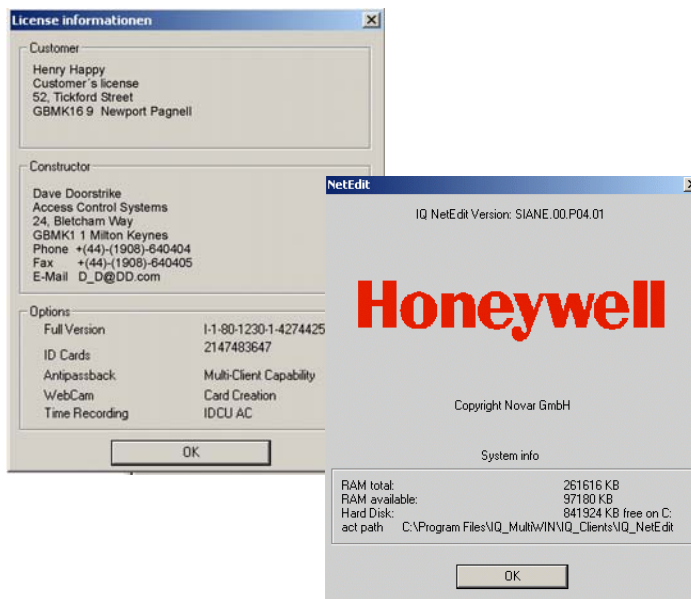
**Packed representation**

If this button is pressed, the representation of the tree structure is reduced to the main levels.

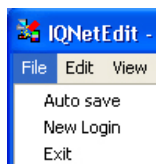


**Info**

The Info button provides general system and licence information:



**4.3.2 Menu bar**



**File → Auto save.**

Each modification must be confirmed before it is stored. If this button is pressed, it is saved automatically without confirmation prompt. This menu item corresponds to button:



**File → Login**

The current user is logged off, the program returns to the dialogue window.

**File → Exit**

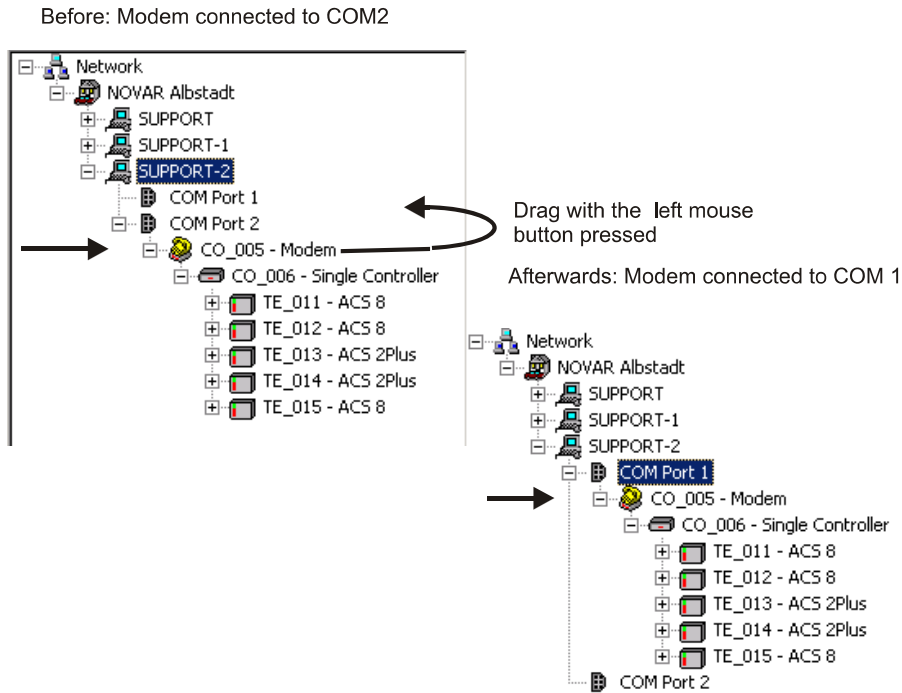
Closes IQ NetEdit.



If modifications have been made which require a parameterization of the controllers/terminals concerned, this will be carried out automatically after log off. To prevent this, enter a → **start time for delayed factory reset**. The doors concerned are out of function during this time.



**Edit → Controller/Terminal DragDrop**



Objects (devices such as bus controllers, modems etc.) including all devices connected to them can be dragged from one COM interface to another one while keeping the left mouse button pressed - not only within one workstation but over the entire installation!

This is useful e.g. when on a particular computer a COM interface to which a bus controller or a modem has been connected so far is required for connecting another device. Thus the bus controller or the modem with all controllers/terminals belonging to it can be assigned to another interface or another PC provided that the hardware installation (cables etc.) permits it.



If “*Edit - Controllers/Terminals DragDrop*” is activated in the menu bar, it is also possible to drag/drop individual controllers/terminals (incl. all sub-components).



**Note!** Compare the address of the controller/terminal in IQ NetEdit with the physical controller/terminal address after drag/drop. If necessary, the latter must be set again physically on the controller/terminal concerned!

Reason: If the previous controller/terminal address already exists at the destination, a free address will be allocated automatically.



**If controllers/terminals are dragged over locations, this will only concern the physical connection (communication channel). Logically the controller/terminal remains assigned to its original location!**

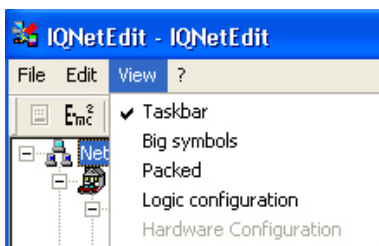
For logical / physical assignment of hardware see Chapter 11 = Several locations.

**Edit → Insert / Delete**

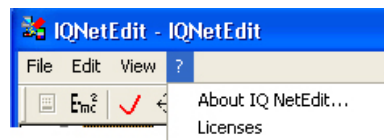
With this function you can insert objects or delete selected objects.

**View → Status Bar**

If this is activated, a status bar is displayed in the program window. The display depends on the cursor position.



**View → Big Symbols/Packed/Logic Configuration/Hardware Configuration/About IQ NetEdit Licenses.**

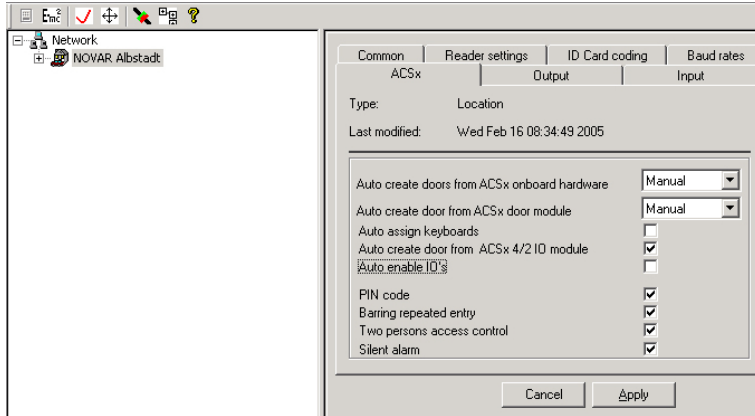


These functions correspond to the buttons described earlier on.

### 4.3.3 Mouse functions

#### Left mouse button

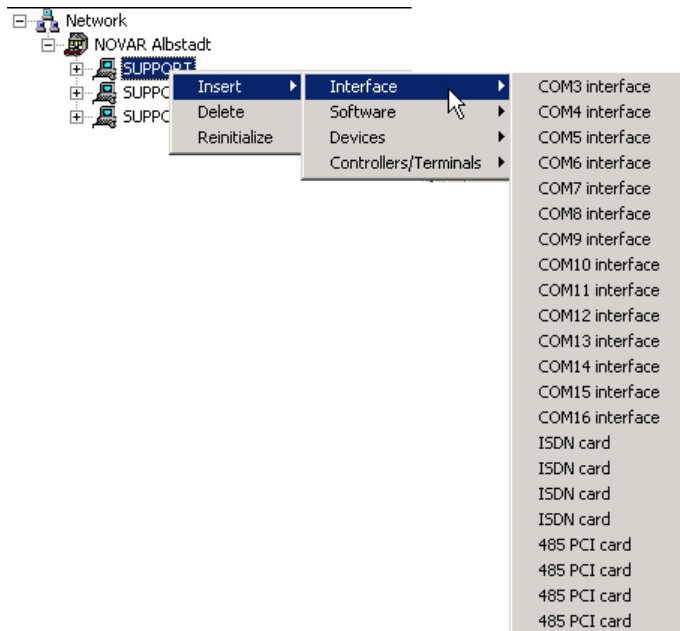
After a click with the left mouse button on an object, tabs with the relevant setting options will appear in the right window (depending on the object).



For a description of the individual fields see chapter → 5 Tabs.

#### Right mouse button

Right-clicking on an object will open one or several sub-menus (depending on the object) with further options ( see Chapter 7). Alternatively, the sub menus can be opened by pressing the Windows key.



## 5. Tabs

Description of the individual fields per tab / in alphabetic order.

The definition of the individual components (controllers/terminals, inputs, outputs etc.) requires repetitive tab entries.

As we do not want to make these instructions too complex, this chapter will only provide an overview of the individual tabs with explanations concerning the individual fields<sup>8</sup>. Modifications must be confirmed with "Apply".

Tabs and fields concerning → **Macros**, **Antipassback** and **Barring Repeated Entry** are described in a separate documentation (Supplementary Functions of IQ MultiAccess, P32205\_46\_0G0\_xx).

The following description is restricted to the fields entries can be done. Fields not mentioned here are highlighted with hgrey and can not be modified.

Which tab exists for which component can be seen from the table below. The components may be found in the physical representation as well as in the logical representation.

Components	ACSx	Additional Settings	Alarms	APB/BRE	Baudrates	Branch	Common	Counters/Image Comparison	Data Carrier Coding	Daylight saving time	Door	Door Allocation	Firmware	Input	Keyboard	Keycode	Macro	Macro automatical	Macro manual	Multi-eye AC/Image Comparison/ATR	Output	Parameters	Reader Settings	Release Criteria	Settings	Switch table	Tamper Monitoring	TRSxx
2 doors expansion																												
485-PCI-card																												
ACS-1	●	●																				●						
ACS-2	●	●										●										●						
ACS-8	●	●										●																
ACT		●																										
Bus controller		●																										
COM-Port-Server																												
Doors			●												●	●	●					●						
Door module																												
Global settings														●														
IGIS-LOOP																												
I/O-card (ACS-1)																												
I/O Module																												
Inputs													●															
Interface																												
Interface converter																												
Key depot																												
Keypad																												
Location	●	●	●						●	●	●											●				●	●	
Macro																												
MBxxx		●																										
Modem/ISDN B-channel																												
Module bus																												
Operator																												
Outputs																												
Readers																												
Read-in station																												
Software																												
TRS 8 / 15			●									●																
Userdefined fields																												
WebCam																												
Workstation																												
Zone												●																

<sup>8</sup> Within a tab, not all fields are always relevant for all components. Therefore only the relevant fields are shown for the individual components.

## 5.1 ACSx tab

### Activate inputs/outputs automatically:

If this field is activated, **all** inputs/outputs will be activated automatically when they are configured.

### Auto assign keyboards:

If this field is activated, keyboards will be added automatically when doors are configured. As many keyboards as readers will be activated.

### Auto create doors from ACS8 door module:

An ACS-8 door module is used to control a maximum of two doors. The latter is/are configured automatically according to the selection entered. Since the connection options for the ACS-8 are so manifold, these settings must always be checked manually (see Chapter 6.5 as well as the Installation Instructions for the ACS-8 and the ACS-8 door module).

In the factory setting, this field is set in such a way that one door with two readers is defined.

The selection options correspond to the explanations for field “**Auto create doors from ACSx onboard hardware**”.

### Auto create door from ACSx 4/2 I/O module:

If this field is activated, a door is assigned automatically to an I/O module when the latter is configured.

### Auto create doors from ACS2 onboard hardware:

You can choose among the following options via the scroll-down arrow right of the entry field:

#### Manual:

When an ACS-2 plus controller is configured, you will be asked how many doors this controller is to manage via its onboard hardware. There are the following options:

- not defined: No door is configured automatically, this must be made manually (see Chap. 6.5 Doors).
- one door (1 reader): One door with one reader is configured automatically, the second reader remains inactive.
- one door (2 readers): One door with two readers is configured automatically.
- two doors: Two doors with one reader each are configured automatically.

In addition, you can define whether keyboards are to be configured as well. If this field is activated, the same conditions apply to the keyboards to be configured as to the readers.

#### One door (1 reader)

When an ACS2-plus controller is configured, one door with one reader is defined automatically. The second reader remains inactive.

**One door (2 readers)** When an ACS2-plus controller is configured, one door with two readers is defined automatically.

**Two doors:** When an ACS2-plus controller is configured, two doors with one reader each are defined automatically.



See chapter 6.5 and the installation instructions of the individual central units/modules for a detailed connection overview of the readers, inputs and outputs.

#### Auto create doors from ACS8 onboard hardware:

You can choose among the following options via the scroll-down arrow right of the entry field:

**Manual:** When an ACS-8 controller is configured, you will be asked how many doors this controller is to manage via its onboard hardware. There are the following options:

- not defined: No door is configured automatically, this must be made manually (see chapter 6.5 Doors).
- one door (1 reader): One door with one reader is configured automatically, the second reader remains inactive.
- one door (2 readers): One door with two readers is configured automatically.
- two doors: Two doors with one reader each are configured automatically.
- three doors: Three doors with one reader each are configured automatically.
- four doors: Four doors with one reader each are configured automatically.

In addition, you can define whether keyboards are to be configured as well. If this field is activated, the same conditions apply to the keyboards to be configured as to the readers.

**One door (1 reader)** When an ACS8 controller is configured, one door with one reader is defined automatically. The second reader remains inactive.

**One door (2 readers)** When an ACS8 controller is configured, one door with two readers is defined automatically.

**Two doors:** When an ACS8 controller is configured, two doors with one reader each are defined automatically.

- Three doors:** When an ACS8 controller is configured, three doors with one reader each are defined automatically.
- Four doors:** When an ACS8 controller is configured, four doors with one reader each are defined automatically.



See chapter 6.5 and the installation instructions of the individual central units/modules for a detailed connection overview of the readers, inputs and outputs.

#### Barring repeated entry:

By activating/deactivating this check box you define whether the Barring Repeated Entry function is to be used or not. Barring repeated entry means that, after a room was left, it may only be accessed again after a defined period of time has elapsed, or that rooms may be accessed only in a certain direction (sequence).

#### Multi person access control:

By activating/deactivating this check box you define whether multi person access control is to be used or not. This means that several persons (2 - 9, to be set in → **Multi eye AC** tab of the doors) have to identify themselves one after the other at the same reader in order to obtain access to the especially protected room (e.g. for strongrooms or rooms with special dangers where one person alone is not allowed to stay).

#### PIN

An identification is generally also possible by entering a key code. This code may be entered **in addition to** or **instead of** identification via a card. (This definition is made under → **door data**).

The basic definition of this field per location/controller/terminal has the following meaning: If this field is not activated, a **door code** can be used. This code is defined per door. If field **PIN** is activated, a **PIN** is used.

#### Difference **door code** - **PIN**:

A **door code** is a combination of numbers (4 up to 6 digits) assigned to a door. Each person who knows the code has access to the particular door.

A **PIN** is a combination of numbers (4 up to 8 digits) assigned to a person. Only this person has access to all doors where identification via **PIN** is permitted. (PIN = **P**ersonal **I**dentification **N**umber).

The PINs of all involved systems / locations must have the same length when working with a connection / integration to an intrusion alarm control panel and/or using collective doors by several mandators (see also → **key code** tab, chapter 12 and the separate documentation for integrating an intrusion alarm control panel P32205-80-0G0-xx).

#### Silent Alarm:

By activating/deactivating this check box you define whether silent alarm is to be used or not. A silent alarm is output as screen alarm e.g. in case of duress (see also → **Duress**, → **Add for duress code**, → **Silent alarm**).



## 5.2 Additional tab (Additional Settings)

### Blocking time after max. unsuccessful logins:

Input of a time period in minutes for the duration the program is locked if the maximum number of unsuccessful attempt has been exceeded (see also → **max. no. of unsuccessful client logins** and 4.2).

### Deactivate APB when Offline:

The antipassback option only makes sense when the system is ONLINE. On the one hand, APB has the effect that the current location of a person can be displayed e.g. via a tableau and, on the other hand, that access is only permitted to a zone next to the one where the person stays at the moment.

When the connection between the ACS-2 / ACS-2 plus / ACS-8 and the bus controller fails, APB is deactivated if this field is active. That means that the persons are no longer registered in the zone where they currently stay, but that they do not stand in front of closed doors either.

As soon as the connection works again, APB is reactivated and the persons are again associated with the current zone when the next booking is made.

### Delete history memory:

A serial printer may be optionally connected for logging the bookings.

If this field is activated, the printer memory of the ACS-1 is deleted when the printer is switched on. All bookings since the last power off are thereby deleted. Only the current bookings are printed.

If the field is not activated, the data buffered in the ACS-1 printer memory while the printer was switched off are printed as well.

### Delete identification of person/location assignment

This can be used to define a field in an export file to tell the target system which records of IQ MultiAccess have been deleted since the last export. This enables the target system also to delete the no longer existent records (see user manual, P32205-20-0G0-xx, chapter 17).

### Delete unreferenced main data:

If active, a person's complete master file record will be deleted, if a location manager deletes a person in his/her location, unless the person to be deleted is allocated to one or more other locations. If this field is not active, only the allocation to the location will be deleted, but the record remains in the global personnel master file.

This setting is not relevant for **personnel managers** and **superusers**.

### External control:

With this function it is e.g. possible to permit an IDS control via WINMAG. This function is comparable to the functions *dd card with "- key" and "IDS controlling"*.

### Forgotten enter (clock in):

Input of a default time to be used for → **attendane time recording** if the booking type **Enter/come** has been forgotten or done at a door without "Entry/Exit" definition. Factory setting: 08:00 h.

### Forgotten leave (clock out):

Input of a default time to be used for → **attendane time recording** if the booking type **Exit/leave** has been forgotten or done at a door without "Entry/Exit" definition. Factory setting: 016:00 h.

- IDS controlling:** An ACS-1 can simulate an operating unit of an intrusion detection system. If this check box is activated, the IDS can be armed/disarmed via a special function ( “-“ key) on the ACS-1. For this purpose, the check box *dd.card with “-“ key* must also be activated (for more details see Installer Instructions ACS-1.)
- Indexing:** Indexing means that the database is sorted by different criteria in order to obtain quick access to the data, in particular for a large quantity of ID cards. That means, however, that a considerable part of the memory is used for this so that it is possible that the number of possible ID cards is reduced (for details see ACS-8 instructions).
- Int. reader 2 outside:** The integrated reader is normally defined as entry reader. If it is however to be defined as reader 2 = exit reader, this check box must be activated.
- Language:** You can choose one of the languages German, English or French via the scroll-down arrow right of the entry field.  
  
This selects the language for the displays of the individual devices (for details please see the Installation Instructions for the devices concerned).
- Max. day plans:** The max. number of day plans can be entered here. The factory setting is 500.
- Max. ID cards:** The controllers/terminals where this field is shown have a dynamic memory management, i.e. they reserve exactly the memory space required for the number of ID cards to be managed. The remaining memory space can be used for other data (e.g. bookings). The maximum number informs the controller/terminal about the number of ID cards for which memory space is to be reserved. The memory space required will be calculated and displayed by entering a number of ID cards. See also → **max. zones**.
- Max. macros:** Enter here the maximum number of macros managed by the ACS-8. An ACS-can manage 64 macros max. You can define only as many macros per controller/terminal as are defined here.
- Max. no. of unsuccessful client logins:** Enter a maximum number of allowed unsuccessful attempts to login. After exceeding the program will be blocked for the time defined in the field → **Blocking time after max. unsuccessful logins** (see also 4.2).
- Max. timer:** Enter here the maximum number of timers managed by the ACS-8 when the Barring Repeated Entry function is active. It is possible to assign one timer per door side, i.e. the maximum number is 16 (8 doors max. with two sides each). You can define only as many timers per controller/terminal as are defined here.
- Max. week plans:** The max. number of week plans can be entered here. The factory setting is 255.
- Max. zones:** The controllers/terminals where this field is shown have a dynamic memory management, i.e. they reserve exactly the memory space required for the number of zones to be managed. The remaining memory space can be used for other data (e.g. bookings). The maximum number informs the controller/terminal about the number of zones for which memory space is to be reserved. The memory space required will be calculated and displayed by entering a number of zones. Depending on this field also the memory space of → **max. ID cards** changes. A maximum of 512 zones can be entered per controller.
- New person/Validity of ID card:** Enter here a period of time and date. This is the default value set in the field “End time” of validity of ID card when a new person is set up.
- Printer baudrate:** Via the scroll-down arrow right of the entry field, you can set the baudrate for controlling a (log) printer. This baudrate must correspond to the device settings.

**Relay card with "-" key:**

Certain functions which are e.g. controlled via a relay can be activated on the ACS-1 by pressing the special functions key ("-" key) and booking with an ID card which authorizes activation/deactivation of this special function. In this case, this check box must be activated. The functions are assigned to the corresponding relay in *IQ MultiAccess*.

**Turnstile:**

An ACS-1 can also control a turnstile instead of a door (in this case, the alarm relay is operated as second release relay). For this purpose, this check box must be activated.

### 5.3 Alarms tab

Depending on the user selected, this tab may be structured in different ways (see example).

Generally, there is one area where different events can be selected which are to be displayed as screen alarms. Combinations are possible.

Offline	<input checked="" type="checkbox"/>
Online	<input checked="" type="checkbox"/>
Disabled	<input checked="" type="checkbox"/>
Battery OK.	<input checked="" type="checkbox"/>
Battery empty	<input checked="" type="checkbox"/>
AC power	<input checked="" type="checkbox"/>
Accu power	<input checked="" type="checkbox"/>

**Duress relay:**

Via the scroll-down arrow right of the entry field, you can select one of the existing relays for triggering an alarm in case of duress. The relays available depend on the input/output card that is installed.

Duress relay	---
Alarming time	0

**Alarm time:**

The duration (in seconds) of one of the above alarms is entered here.

## 5.4 Antipassback/Barring repeated entry tab

This tab is used for the antipassback and barring repeated entry functions. For a detailed description please see the separate documentation Supplementary functions of IQ MultiAccess (P32205-46-0G0-xx).

For ACS-1 controlled doors this tab has an additional field called **access options**. Its factory setting is **standard**. It can be selected either:

### **Multi person access control:**

Two persons authorized for this door have to book one after the other to get a door release. Thereby it does not matter if one or all persons booking have general authorization or not. The door will be released only if the total number of persons required is reached.

or

### **Multi person access control with general authorization:**

Generally, two persons authorized to this door have to book one after another to cause a release. But if one person has general authorization, only this person's booking will cause a release.

In the logical view of the controller that controls this door the number of authorized persons required booking one after another have to be entered in the → **Multi person access control** tab.



With ACT controlled doors those two options are not available. For ACS-2 plus / 8 see 5.17.

The **antipassback** option which as well is located in this tab is described in detail in the documentation mentioned above.

## 5.5 Automatic Macro tab

For macros, there is a separate manual **Supplementary Functions of IQ MultiAccess, P32205-46-0G0-xx**.

## 5.6 Baudrates tab

**Baud rate bus controller terminal:** The value entered here is used for the transmission speed between the bus controllers and the controllers/terminals. By clicking on the scroll-down arrow right of the entry field, the desired speed can be selected from the options listed. The factory setting is 19200 bauds.

**Baudrate master ↔ slave:** The value entered here is used for the transmission speed between master and slave controllers. By clicking on the scroll-down arrow right of the entry field, the desired speed can be selected from the options listed. The factory setting is 19200 bauds.

**Baudrate PC ↔ bus controller:** The value entered here is used for the transmission speed between PCs and bus controllers. By clicking on the scroll-down arrow right of the entry field, the desired speed can be selected from the options listed.



The baudrates entered here must be set in the relevant hardware components via DIP switches or via Setup (please refer to the relevant manuals).

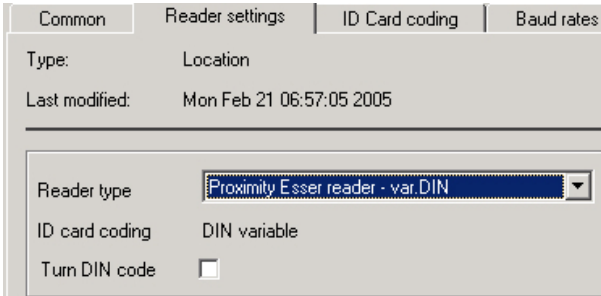
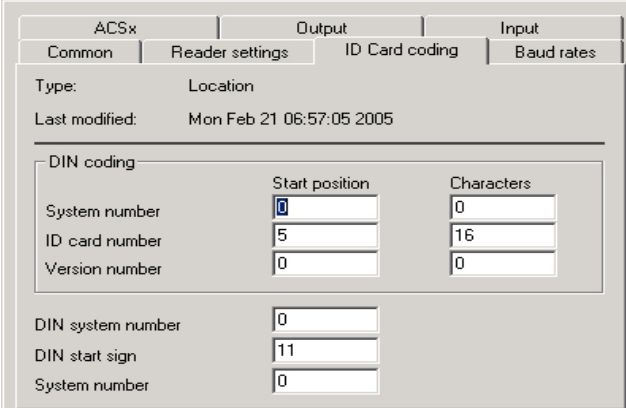
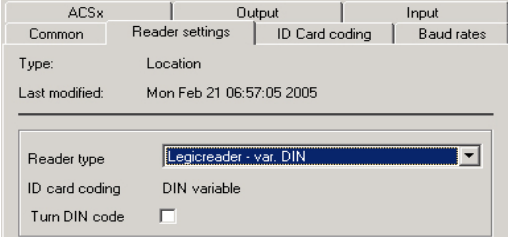
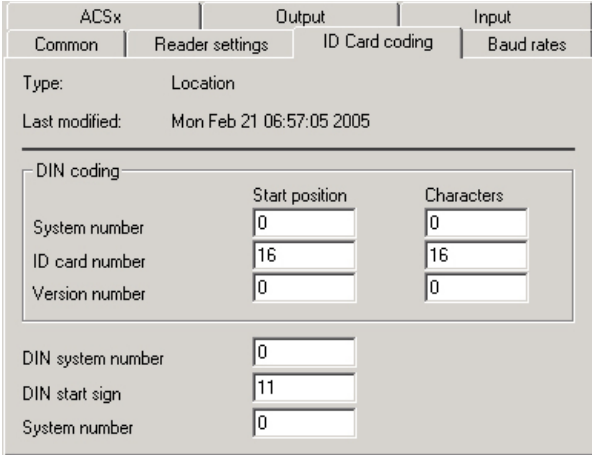
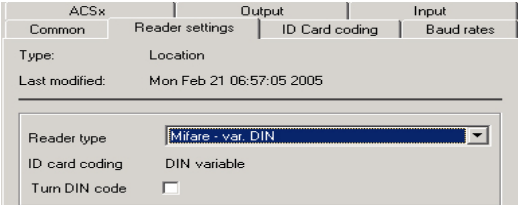
## 5.7 Card coding tab

### 1. Reader Settings

The reader type used is set in tab → **Reader settings**. The relevant settings for reading the corresponding cards must also be made here.

The cards differ basically in their coding, either **DIN coding** or **ESSER coding**, as well as in the reading method (**magnetic, chip, proximity**).

The following table includes the basic settings with concrete examples for each data carrier type:

DIN Coding			
no entry in field <b>System number</b> Entries in the <b>DIN</b> field acc. to the examples below:			
possible reader / ID cards: Prox, IK2 / IK3 data carrier, proximity, contactless			
			
Legic prime / Mifare classic			
			
			

Legic advant / Mifare DESfire EV1

Common | Extended | Key code | Reader settings | Data carrier coding

Type: Location  
Last modified: Thu Mar 13 12:51:27 2014

Reader type: Legic Advant - var. DIN  
Data carrier coding: DIN variable  
Turn DIN code:

Common | Extended | Key code | Reader settings | Data carrier coding

Type: Location  
Last modified: Tue Jul 30 13:09:52 2013

Reader type: Mifare Desfire EV1 - var. DIN  
Data carrier coding: DIN var. Desfire EV1  
Turn DIN code:

Basekey:

Common | Extended | Key code | Reader settings | Data carrier coding

Type: Location  
Last modified: Tue Jul 30 13:09:52 2013

DIN coding

	Start position	Characters
System number	0	0
Data carrier number	1	16
Version number	0	0

DIN system number: 0  
DIN start sign: 0  
System number: 0



By use of mifare DESFire EV1 data carriers observe the programming instructions for encryption, for this, note the information in chapter 17.

These settings refer to data carriers obtained from Honeywell Security. For the settings for third-party products (cards, key rings, etc.) please contact the Service Team of Honeywell Security Technical Support.

### ESSER Coding

Enter **system number** (from security sheet)  
 No entries required in the **DIN fields**. Existing entries will be ignored.  
**ID card number** and **version number** are entered individually for each person in → **IQ MultiAccess**.

possible reader / ID cards:  
 Legic, Chip, Magnetic

ACSx		Output		Input	
Common	Reader settings	ID Card coding	Baud rates		
Type:	Location				
Last modified:	Tue Feb 22 05:51:40 2005				
Reader type	Legic reader - Esser				
ID card coding	No special code				
Turn DIN code	<input type="checkbox"/>				

ACSx		Output		Input	
Common	Reader settings	ID Card coding	Baud rates		
Type:	Location				
Last modified:	Tue Feb 22 05:51:40 2005				
DIN coding					
		Start position		Characters	
System number		0		0	
ID card number		0		0	
Version number		0		0	
DIN system number		0			
DIN start sign		0			
System number		4711			

ACSx		Output		Input	
Common	Reader settings	ID Card coding	Baud rates		
Type:	Location				
Last modified:	Tue Feb 22 05:51:40 2005				
Reader type	Magnetic plug in reader - ESSER				
ID card coding	No special code				
Turn DIN code	<input type="checkbox"/>				

ACSx		Output		Input	
Common	Reader settings	ID Card coding	Baud rates		
Type:	Location				
Last modified:	Tue Feb 22 05:51:40 2005				
Reader type	Chipcard reader - Esser				
ID card coding	No special code				
Turn DIN code	<input type="checkbox"/>				



These settings refer to ID cards obtained from Honeywell Security. For the settings for third-party products (cards, key rings, etc.) please contact the Service Team of Honeywell Security Technical Support.

## 2. Reader Settings

If proximity, DIN-coded ID cards are used, these can be read in via a corresponding reader during definition of the **personnel data**.

Insert a reader (only possible at COMx):

Right-click on the COM interface → Insert → Controllers/terminals → Reader

The following settings apply to the reader:

<b>Proximity</b>	Start position 1	Length 20
<b>Legic / Mifare</b>	Start position 23	Length 20
<b>Admitto Mifare</b>	Start position 1	Length 20
<b>Admitto Legic</b>	Start position 1	Length 20
<b>Admitto Desfire</b>	Start position 1	Length 16
<b>USB reader</b>	Start position 1	Length 20

## 5.8 Common tab

**485 PCI card:** Instead of / in addition to external bus controllers, 4 "internal bus controllers" (485 PCI cards) max. may be installed per PC. Each of these cards replaces two external controllers. You can define the cards installed by making the relevant selection (1 - 4) in this field. The factory setting is "1".

**Active:** Field "Active" must be selected so that the component defined (controller/terminal, reader, input, output etc.) is marked as existent for the program. In case of devices that have already been defined but are not yet to be used, this field remains empty.

**Account doesn't expire:** If this field is activated, there is no time limit for the user's (operator's) validity. If required, this limit must be entered in field → **Expiration**.

**Account with card:** Additional identification via ID card to login. For starting one of the IQ MultiAccess programs (according to the rights allocated) the operators **personnel manager**, **systemmanager** and **location manager** can be set to require an additional identification via their ID card.

**Recommendation:** Read-in station connected to the corresponding workstation.

The coding of the data carriers can either be entered manually in IQ NetEdit or read via a read-in station. The **Read in** button opens a corresponding window. The upper 4 grey highlighted fields display information on the settings of the read-in station. For "free driven" defined software (directly at a location) these parameters can be entered manually.

**Deposit a data carrier:** Press **Read in** button  
Hold the data carrier into the reading area<sup>10</sup>  
The coding will be displayed.  
Press the **accept** button

**Effect:** After input of user and password there is a prompt to read an authorized data carrier.

Any combination of the **Account with card** option with the **Account with second operator** option (see next item) is possible.

**Account with second operator:** For starting one of the IQ MultiAccess programs (according to the rights allocated) the operators **personnel manager**, **systemmanager** and **location manager** can be set to require the login of another user.

Select the second operator required to log in the field **second operator**. Available are operator of the same or higher level.  
If no second operator is defined here, any operator of the same or higher level can login as second operator.

**Effect:** After input of user and password there is a prompt for the second operator to log in.

Any combination of the **Account with second operator** option with the **Account with card** option (see previous item) is possible.

---

<sup>10</sup>

A **Timeout** message appears if the data carrier is not held into the reading area within the defined reading time. Confirm with **OK** and repeat the procedure.



**Address:** The address serves for identifying a user within the entire system (each device has an unambiguous address assigned to it). Addresses may exist only once within a system). It is determined automatically by the system with function *Scan for controllers/terminals* or *ACS-2/8-Scan* on the basis of the device settings. In all other cases, it must be entered manually. If it is entered/modified, it must correspond to the settings in the device. For some users it is not possible to modify the address manually.

**Anonymous bookings:** If this field is active, the creators of the bookings (name, no. of data carrier) will be displayed in the logfiles.

**Antipassback:** By activating/deactivating this check box, you define whether the zone selected participates in the Antipassback function or not.

**Auto log off:** Input of a time period in minutes, after that the connected user automatically will be logged off, if no input occurs within this time period (see 4.3.1). Factory setting = 5 minutes. "0" = no logout.

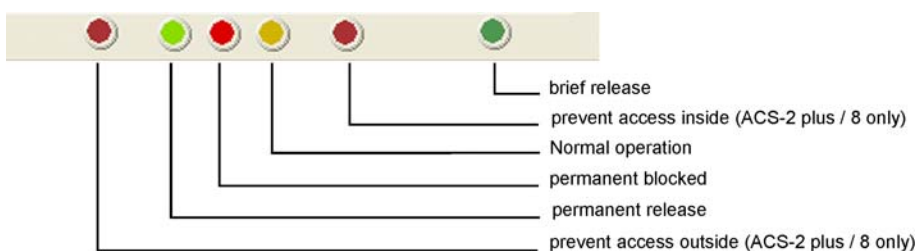
**Barring repeated entry:** By activating/deactivating this check box, you define whether the zone selected participates in Barring Repeated Entry or not. For details please see the separate documentation Supplementary functions of IQ MultiAccess (P32205-46-0G0-xx).

**Baudrate:** In this field, the speed in which the user selected communicates with another user connected via serial interface (usually a workstation) is set by means of the scroll-down arrow. Default settings are suggested. These may be modified, but they must correspond to the hardware settings (DIP switches or setup) of the users concerned. Default value: 9600, must be set to 19200 for the ACS-1 controllers.

**Blocking time:** When working with → **Barring Repeated Entry**, you define here the period of time which must elapse before repeated entry is possible again for the zone selected.

**Buttons / icons:** In this tab, there are additional buttons for the doors which can be used to cause a short-time modification of the (basic) state of the door. These buttons are used for test purposes and temporarily overrule the current state of the door. The door tested must be reset to its original state afterwards by means of the relevant button. With the next parameterization, at the latest, the door will be reset automatically to its original state.

Meaning of the buttons:



**Buzzer:** (ACS-2/8 firmware V8.xx or higher required). This field must be active if you work with → **Door open time** and → **Door open signal**. This causes an acoustic signal to be resound at the door which calls attention that the maximum door open time will soon be reached and the door should be closed by now. Alternatively, an acoustic or optical signalling device can be activated via a relay output. For ACS-2 / 8 doors, in the **Buzzer** field there can be set how long the buzzer shall be active. The default setting **until message** corresponds with the hitherto existing function: The buzzer stops after expiration of the door open time. At this point in time the message "Door opened too long" is generated and an additional alarm might be triggered.

**Further settings: Off:** Basically, the buzzer will never be activated.

**Until closed:** Buzzer is active until the door is closed again (corresponds to IACP-default setting).

- Camera type:** Select the camera used for image matching.
- CD Number:** The CD number is assigned by the system and cannot be changed. This field is for information only and is used internally by the program.
- Check:** A slider from 0 - 100% helps to set the random generator for the bag and/or person check of module IQ Guard. According to the settings on every x% of the booking persons a check prompt will be displayed. The door remains closed till it will be released manually.
- COM Port:** Since the description can be freely chosen when a COM port is set up, the actual COM port description (COM1 to COM16) is always maintained in this field. This field cannot be changed.
- Computer name:** When *IQ NetEdit* is started for the first time, the computer name of the computer where the program has been started is adopted automatically. If another computer is configured, its name can be determined via the *Search* button. Only computer names may be used that really exist, as otherwise *NetEdit* and the software linked with it will not work properly.

**Data carriers learnable / learn data carriers:**

Data carriers from locations with the check box **data carriers learnable** active can be "learned" in locations with the check box → **learn data carriers** active.

Example: Location A: Data carrier known, check box **data carriers learnable** active.  
 Location B: Data carrier unknown, check box **learn data carriers** active.

The first reading of the data carrier in location B denies the access (red LED on, message: "unknown data carrier"). Simultaneously, the program browses the master files of the locations with the **learnable** check box active and takes over the data of the corresponding data carriers into the own location. From now on the data carrier is known in location B, however, it has still no access authorization. The latter must be allocated either manually or via a room/timezone with the attribute **automatical assignment**. With the next reading of the data carrier the person is authorized to enter (depending on the individual access rights).

**David API path:** IQ MultiAccess is able to send messages (SMS, e-mail, fax, voice-mail) using a link to the software kit DAVID. At this place the path to the David API directory is to be entered. In this directory all the jobs to be handled by David are created as a text file. The path must be entered in UNC notation: \\computer name\DAVID\APPS\FAXWARE\OUTAPI

**Recommendation:** The David software and the IQ\_Server must be installed on the same computer, e. g. on the server.

**Default (normal condition) (outside/inside):**

Definition of the normal condition of a, separate for inside and outside.

- Normal operation: Door is closed, reader is ready for operation, yellow LED is on, keyboard is ready for operation (= standard setting).
- Door locked: Door is/remains closed, reader does not react, red LED is on, keyboard is not ready for operation, no access possible.
- Permanent released: Door can be opened without identification, green LED on the reader is on.



Permanent release always releases both sides of the door even if this function is only activated on one side of the door!

Other combinations are possible, e.g. door locked on the outside, normal state on the inside means: Nobody may enter but all those who are inside may exit.

- Delayed factory reset:** Start time for parameterization of the controllers/terminals after updating from MultiAccess for Windows V7 to IQ MultiAccess or any modification requiring a parameterization. If no start time is entered, the parameterization starts automatically directly after exiting IQ NetEdit (see also chapter 3.3.2).
- Description:** The name entered here is assigned to the relevant user in *NetEdit*. The user will be managed with this name in the AC or TR software. The description selected should be unambiguous. We recommend to correct the description manually directly after the automatic set up (e.g. via *Scan for controllers/terminals, ACS-2/8-Scan*), since the entry assigned automatically does not unambiguously indicate the installation location of the user. With manual definition - as the name suggests - entries must be made in every field anyway.
- Don't show within pc software:**  
Each macro with this box active will not be displayed in IQ MultiAccess. Use: Automatic macros need not be in the menu of manual macros and would only blow up this selection.
- Executable by PC software (host):**  
If this field is active, the macro selected can also be started from IQMA
- Executable by remote ACSx:**  
If this field is active, the macro selected can also be started by another ASC-2/8.
- Expiration:** If field → **Account doesn't expire** is deactivated, it is possible to define here an expiration date for the validity of the user concerned (operator). This date may be entered either manually or via the calendar (arrow).
- Field type:** Setting of the field type for user defined fields. Possible field definitions: Number, string, date, time, combo box, check box. The entries / selections in IQMA correspond to the settings made here.
- Field value:** Here you can enter default values for the combo box field type (separated by semicolon) to be displayed as a selection in IQMA (e. g. a; b; cc; d1). These entries are ignored by all other field types.
- Fire door:** With this setting, this door can not be switched in permanently release. It is no longer possible permanent release from a control of actions, automatic zones, normal operation and WINMAG control. Installers have to check if any macro is programmed to switch to permanent release and change them if necessary.
- FTP port:** An Axis webcam can be connected via Ethernet for transmission of live images or a sequence of images. In this field the IQ-internal FTP Server port used for the communication to the camera must be entered (see also user manual to IQ MultiAccess (P32205-0G0-xx), chapters 10.9, 10.10 and 18).
- Global I/O number:** The global I/O number is assigned automatically by the system and cannot be changed. This field is for information only and is used internally by the program.
- ID:** Unambiguous device identification. This value is assigned automatically by *NetEdit* and cannot be changed.
- Identification:** Password for WINMAG and/or device/serial number of the locking cylinder (see separate documentation).
- Import ID:** This field is used for identification of data records when importing data from other systems. A detailed description is to be found in the User Manual (P32205-20-000-xx, Chapter 18, in particular sections 18.1.3 and 18.1.4).
- Internal address:** The internal address is assigned by the system and cannot be changed. This field is for information only and is used internally by the program.
- I/O point:** The I/O point is determined by the system and suggested automatically. I/O points are

used for process visualization in WINMAG.They can be modified, but they must correspond to the settings in WINMAG.

- IP address:** The IP address is determined automatically on the basis of the computer name if field Use IP is deactivated. In all other cases, it must be entered manually.If necessary, contact your system administrator.
- ISDN card:** A consecutive number is automatically assigned while inserting an ISDN card. The number can be changed, but we recommend to keep the automatic settings.
- Key code length:** The key code (→ **PIN code**, → **door code**) is defined here with 4 or 6 digits. A modification of the key code length from 6 to 4 digits is only possible if no personnel data have been entered yet in IQ MultiAccess (see also Chapter 10.1).
- Last modified:** This field shows when **login name** and/or **password** of an operator were modified for the last time.
- LD Number:** The LD number is assigned by the system and cannot be changed. This field is for information only and is used internally by the program.
- Learn data carriers:** see → Data carriers learnable.
- Log execution:** If this field is active, the execution of the macro selected will be recorded.
- Login name:** Operator's name, can be freely assigned. This name must be entered into field → **User name** at login.
- Loop address:** Entry of the IGIS-LOOP address of the intruder alarm control panel connected via IGIS-LOOP.
- Masked:** If this box is active, the content of the corresponding user defined field is displayed as **\*\*\*\*\***. This function is only effective for the field types **number** and **string** (cf. chapter 14).
- Maximum duration of stay:**  
When working with **Antipassback**, it is possible to define the maximum duration of stay permitted for the selected zone.There is a separate documentation for APB and BRE, **Supplementary Functions of IQ MultiAccess, P32205-46-0G0-xx**.
- Minimum duration of stay:**  
When working with → **Antipassback**, the minimum duration of stay permitted for the zone selected can be defined here. If the duration falls below this value, a message/alarm is triggered.
- Mp/I/O no.:** see I/O point
- Multi persons access control:**  
Generally this field must be activated, if at least to persons´ s are required to get a door released. The individual parameters can be defined for each door(side) separately (see 5.4 and 5.17).
- MVA:** My Virtual Address. The value suggested should not be changed (see also Event Log).
- No.:** Serial number of the relevant device. This value is assigned automatically by *NetEdit* and cannot be changed.
- No EP- Wake Up:** If this field is activated, no check is carried out during ongoing operation as to whether the device is still active (physically accessible). A connection to this device is only established if data are available for being transferred. It is recommended not to activate this field so that it is possible to notice when a device is OFFLINE. Using this function makes only sense (for reasons of costs) with network dial-up connections.
- No operating unit:** Enable or disable a MBxx panel for access with a virtual operating unit IQ OPUNIT. This

checkbox defines if the panel will be operate or not. By use of a virtual operating unit and setting "no operating unit" the panel will be not shown for operating.  
When Connecting a MB-Secure panel a virtual operating unit is not supported.

**Number of doors:** By means of function "Scan for controllers/terminals", expansion boards that are installed are recognized automatically, e.g. a two-door expansion board at the ACS-1. In this case, the number of doors will automatically be set to 2 as well.  
For the ACS-2/8, the doors of the on-board hardware will be defined according to the default settings.  
This field cannot be changed.  
When an ACS-1 controller is configured manually and a 2-door expansion board is added (also manually), the content of this field will also change automatically.

**Number of keys:** Enter the number of keys which are managed by the key deposition in this field.

**Office permission:** see chapter 6.5.4.2.

**Password:** The password of the operator must be entered into field → **Password** at login. The password must have a length of least 5 characters (alphanumeric, no blanks or special characters). The maximum length is 32 characters. There is no distinction between upper/lower case.

**Password change not allowed:**  
If this field is active, the user (operator) cannot change his/her password himself/herself.

**Password valid:** The time of validity of the password is defined in this field. It is either entered as a value (in days) or selected from the default settings (always, 10, 30, 100, 300 days).  
Always = password is always valid, it does not need to be changed.  
x days = After the set value has expired, the operator is requested to change his/her password. The last password must not be used again (automatic repetition check).

**PIN:** Depending on the key deposition(s) used, permission to take the keys is either granted via a card booking (field remains empty) or by entering a PIN (the latter is managed in IQ MultiAccess, field is activated). The relevant data (PIN or data carrier) are passed on to the key depositions concerned during parameterization.

**Quick Print:** If the checkbox **Quick Print** is activated for a zone, a list containing the current zone occupancy can be printed using the key combination **ALT B**. Only the occupancy of the zones with this field active will be printed.

**Reporting:** Here you can define if and how execution criteria (triggers) are to be interpreted. Default = ignore. The execution criterion/criteria can either be interpreted as **trigger** or as **condition**. For trigger you can additionally define, whether the macro will be started if the condition is fulfilled or not. For detailed information see Supplementary Functions of IQMA (P32205-46-0G0-xx).

**Reset alarms/displays:**  
If an alarm has occurred at a controller/terminal with alarm indicator (e.g. ACS 2 / 8 with LED), the alarm indication is maintained at the controller/terminal even after the cause has been eliminated and must be reset manually. At least read permission in NetEdit is required for this.

**Runtime elimination:** This parameter is active per default. It prevents a delayed start of a macro. Enter a time in the field behind this checkbox after its expiration the macro should not be started anymore (default = 10 minutes). This can be used if a delayed execution is not useful.

Deactivating the field "runtime elimination" means that every command to start a macro will be added to the command queue. Depending on the number of activities running at the same time it could be possible that a (macro)command will reach its target delayed and the macro will start too late. However, it will be executed.  
In most of the cases this delay is not relevant and can be disregarded.



This parameter is valid for all start conditions.

- SD number:** Number of a switching device (reader/operating unit) of IACP doors. This will automatically be taken over by scanning an MBxxx and should not be modified.
- Silent alarm:** On a → **duress** only a screen alarm will be triggered, if this field is active. The alarm relay will not be activated. This function helps to protect the threatened person.
- Sluice function:** Here you can define whether the selected zone is participant of a sluice function. The sides of the doors belonging to this zone can be allocated according to the sluice function. Exit and entry readers are active/inactive depending on the sluice conditions. For more details see Supplementary Functions of IQMA, P32205-46-0G0-xx.
- Sub loop adress:** Enter the sub loop adress of the intruder alarm control panel connected via IGIS-LOOP.
- Suppress / ignore external area (zone) changes:**  
This function can be used to ignore zone change messages from other controllers/terminals and to prevent sending the zone change messages of the own controller /terminal to others. This helps to fulfil some special requirements of APB/BRE. Examples are described in the separate documentation **Supplementary functions of IQ MultiAccess** (P32205-46-0G0-xx, chapters 2.3.4.2 and 2.4.3.2).
- TCP/IP Port:** TCP/IP-Port under which the device can be accessed. Together with the IP address, this permits a further differentiation for addressing. Please contact your system administrator if necessary.

**Threshold value absorption reader:**

All cards which have a higher card number than the number entered here will be retained by the absorption reader.

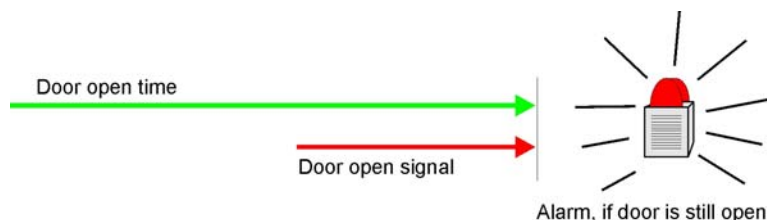
An absorption reader is a magnetic card reader which can retain the magnetic card.  
Possible application: Visitor cards / multi-storey car park exit.



Only one absorption reader can be connected to the ACS-1.

- Times (outside/inside):** Time specified in seconds for certain timers, sometimes separated by inside/outside of a door.
- Alarming time:** Input of the duration (in seconds) of an alarm.
- Open time:** Activation time of the door strike relay. During this time the door can be opened.
- Key code input time:** The key code (→ PIN or → door code) must be entered within this time. If the code is not yet entered completely after expiry of this time, the complete input must be started again from the beginning.
- Door open time:** Maximum time a door may be open. Starts when the door state contact reports that the door is actually opened. After expiry of this time, an alarm will be triggered (message: door opened too long).
- Door open signal:** If a reader / a keyboard is equipped with an internal buzzer, an acoustic signal indicates that the door must be closed before the door open signal time has expired, since otherwise the → **door open time** will expire and an alarm (door opened too long) will be triggered as a result. For this purpose, field → **Buzzer** must be activated.  
The door open signal time is part of the → **door open**

**time** and should always be shorter than the door open time so that enough time remains for closing the door. The time entered here indicates the time remaining before the door open time expires (within this time the door must be closed to avoid an alarm).



**Type** For the key depot option, you can choose between a **KeyBox** (corresponds to a lock where the keys can be inserted and from where they can be taken out ) and a **Dispensor** (corresponds to a safe deposit box).

A switching device of an IACP can be specified via the type. Depending on the type some functions are available/not available for the definition of → **room/time zones** (cf. chapter 15.3, step 8). The status of already existing switching devices is "not defined" and should be reworked.

**Unique:** If this field is active, the entries of the user defined field selected will be checked for duplicates. A new creation of an entry will be refused if this already exists with another person.

**Use IP:** If this field is active, the IP address entered is always used for the event log. If the field is not active, the IP address is determined on the basis of the computer name.  
Default setting: not active - it is recommended to maintain it like this.

**VdS compliant:** Is this parameter is active (will automatically be read out from the IACP and set for the complete location, but can be modified manually), a location operator has no rights within the room/timezones to create, change or delete authorizations for disarming and to create, change or delete door allocations, datacarrier (person) allocations or complete room/timezones which contain disarming (required for IACP-connection).

## 5.9 Counters/Image matching/Access time recording tab

With ACS-1-controlled doors, it is possible to use counters when the option → **Antipassback / Barring Repeated Entry** is activated. For possible applications see also the separate documentation Supplementary functions of IQ MultiAccess (P32205-46-000-xx), section 2.5.3.

**Show on display:** If this field is activated, the counter value is displayed on the ACS-1 concerned (this requires a device with integrated display ).

**Relay:** If the ACS-1 is equipped with an I/O board, you can select here a relay that will be activated when the → **Threshold** value has been reached.

**Threshold:** Enter the counter value which will cause activation of a → **relay**.

**Counter active:** This field must be activated if the counter is to be used on this door. Only then is it possible to make entries in the fields → **threshold, relay** and **show on display**.

**Read/set counter:** Via this button the current counter level of the selected ACS-1 can be displayed and set to any value.

### Image matching:

If the option image matching is used, a camera can be selected and allocated to the corresponding door. If the doorkeeper module is used, the corresponding software can be selected. The options can be used either separately or in combination. For more detailed information see the user manual to IQ MultiAccess (P32205-0G0-xx), chapter 18.

### ATR (Attendance Time Recording):

IQ MultiAccess offers a simple attendance time recording, which is but not to be mistaken by a real time recording system. The only thing that is recognized is whether a person is present and how long he or she has been in the company from the first entry to the last exit booking of one day. Balances, extrapolations etc. are not possible. In order to use this function, doors can/must be defined as entry, exit or entry and exit doors. Bookings at doors without such a definition will be ignored and falsify the calculated balance.

There are default settings for “omit entry” and “omit exit” to be determined per location in the → **Additional** tab. The factory settings for “omit entry” are 08:00 h, for “omit exit” 16:00 h. They will be used if one or both bookings is/are missing.

## 5.10 Daylight saving time

The automatic time change can be activated per location and can be set for different months. The change to daylight saving time is made on the last Sunday in March in Germany. The clock is advanced by one hour between 2:00 and 3:00 h. The clock is changed to standard time on the last Sunday in October. The clock is set back by one hour at 3:00 h. It is possible to shift the months for changing between summer and winter time and between winter and summer time.



In the factory setting, the daylight saving time change is activated, change to daylight saving time as of March, change to standard time as of October.

## 5.11 Distant Station tab

This tab is only required for RDT and is therefore described in Chapter 6.6.



## 5.12 Door tab

### Encryption RF cylinder:

Per location an encryption for the online fittings / cylinders can be deposited. A maximum of 48 digits numeric 0-9 and HEX A-F can be combined arbitrarily. The data will be transferred by IQ Cylinder to the PDA and from there to the door fittings and cylinders.

The default setting "0000...." means no encryption.

### Open time:

Activation time of the door strike relay. During this time the door can be opened.

### Key code input time:

The key code (→ PIN or → door code) must be entered within this time. If the code is not yet entered completely after expiry of this time, the complete input must be started again from the beginning.

### Door open time:

Maximum time a door may be open. Starts when the door state contact reports that the door is actually opened. After expiry of this time, an alarm will be triggered (message: door opened too long).



### Door open signal:

If a reader / a keyboard is equipped with an internal buzzer, an acoustic signal indicates that the door must be closed before the door open signal time has expired, since otherwise the → **door open time** will expire and an alarm (door opened too long) will be triggered as a result. For this purpose, field → **Buzzer** must be activated.

The door open signal time is part of the → **door open time** and should always be shorter than the door open time so that enough time remains for closing the door. The time entered here indicates the time remaining before the door open time expires (within this time the door must be closed to avoid an alarm).



## 5.13 Door definition tab

When working with the functions → **Antipassback /Barring Repeated Entry**, door sides are assigned to the zone selected by making the relevant selection and pressing buttons  or . The available door sides are listed in the left window and the door sides assigned in the right window.

## 5.14 Firmware tab

The fields of this tab are for information only. They cannot be modified (except for field → **Description**).

What is relevant are the two buttons → **Download** and → **Switch Flashbank** which are required for firmware updates.

The firmware update of the ACS-2/8 is implemented via Flash update by the higher-level software (e.g. IQ MultiAccess in program part NetEdit). We generally recommend to update to the most recent firmware release so that all functions - including the current extensions - can be used. These are available for free download on our homepage.

### 5.14.1 ACS-8 Firmware Update

Updating the ACS-8 firmware no longer requires an exchange of EPROMs, but it can be carried out comfortably via software from an IQ MultiAccess workstation. Requirement: The operator must at least have read permission in NetEdit.

The installation routine of IQ MultiAccess creates the directory required for this already during the program installation process. The directory is called:

...\IQ\_MultiWin\IQ\_Services\Download\ZACS8

If a firmware update of the ACS-8 controllers becomes necessary, the file to be obtained from our support or to be downloaded from our homepage

ACS8.FDL

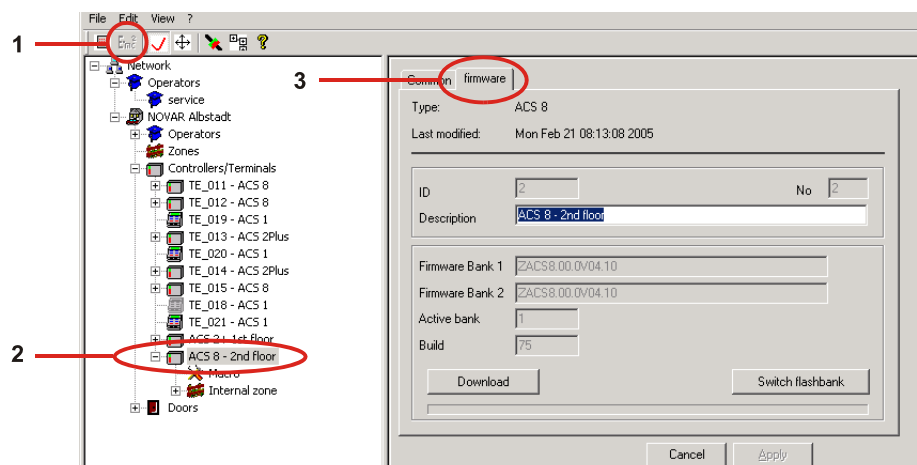
must be copied into this directory of the IQ Server.



The latest firmware update files for ACS-2plus and ACS-8 (date of delivery) are on the IQ MultiAccess installation CD. During the installation, both of them will automatically be copied into the firmware update directory.

#### Procedure:

1. Store file *ACS8.FDL* into the directory specified above (if not happened automatically during the installation, if of a later version is required).
2. Select:
  1. Logic configuration
  2. Select the relevant ACS-8.
  3. Open the **Firmware** tab.



**Active bank:** The ACS-2 plus / 8 has 2 flashbanks where 2 different firmware versions may be stored. Field **Active Bank** shows which bank (i.e. which firmware version) is active at the moment. The new firmware may e.g. be loaded into the flashbank which is not active at the moment so that the ongoing operation is not disturbed. With button → **Switch flashbank**, you can determine when another bank is to become active.

**Build:** Consecutive generation number for the firmware assigned by the compiler. This field is for information only and cannot be modified.

**Description:** The name entered here is assigned to the relevant user in *NetEdit*. The user will be managed with this name in the AC or TR software. The description selected should be unambiguous. We recommend to correct the description manually directly after the automatic definition (e.g. via *Scan for controllers/terminals, ACS-2/8-Scan*), since the entry assigned automatically does not unambiguously indicate the installation location of the user. With manual definition - as the name suggests - entries must be made in every field anyway.

#### Firmware Bank 1 / 2:

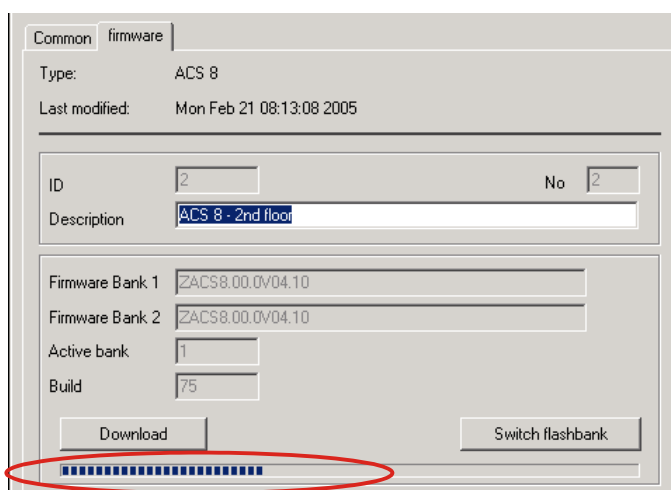
One firmware version can be stored per flashbank. Normally, a firmware update is loaded into the bank which is not active. The bank with the new firmware can be marked as active bank at any time. Now the terminal is working with the new firmware, but the previous version is still available in the inactive bank. If necessary, you can change back to it.

**ID:** Unambiguous device identification. This value is assigned automatically by *NetEdit* and cannot be changed.

**No.:** Serial number of the relevant device. This value is assigned automatically by *NetEdit* and cannot be changed.

### 3. Click on the **Download button**.

The status bar at the bottom shows the progress of the download.



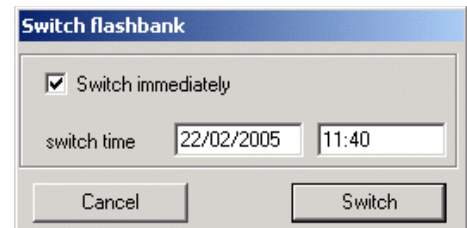
During the download process, which may take up to 30 min., the previous function of the terminal and the doors connected to it remains unaffected, since the new firmware is loaded into the second flashbank which is not active at the moment. This condition is maintained as long as the other flashbank is activated (see point 4).

Via → Start → All Programs → IQ MultiAccess → IQ SysMon, you can open the system monitor for displaying the system messages. The software **IQ SysMon** must have been enabled in IQ NetEdit previously. Start and end of the download process is logged here.

Time	Location	Source	Message
10:20:37	NOVAR Albstadt	ACS_8 - 2nd floor	Download: granted
10:59:48	NOVAR Albstadt	ACS 8 - 2nd floor	Download: successful

4. Activate the new firmware  
Click on button → **Switch flashbank.**

The switching may happen immediately or at a defined date/time. The two fields are mutually exclusive. The entry must be confirmed with **Switch**, the process can be interrupted with the **Cancel** button.

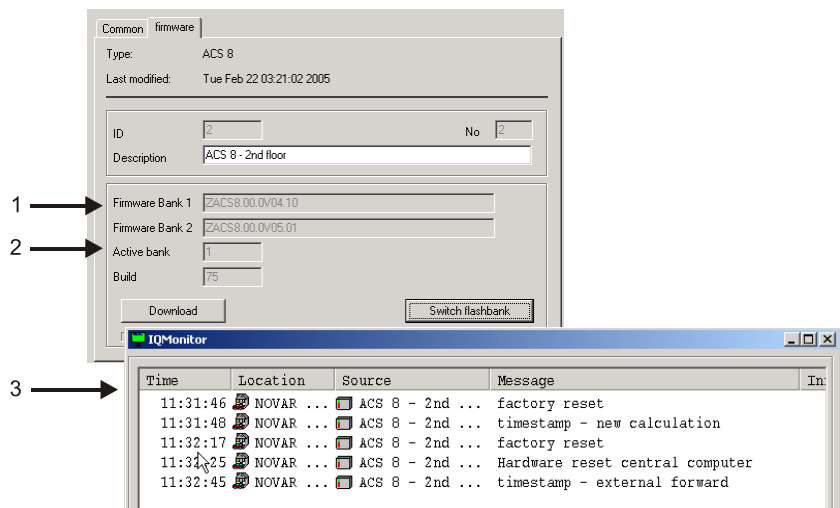


The dialog box titled "Switch flashbank" contains a checked checkbox "Switch immediately". Below it, there are two input fields for "switch time" with the values "22/02/2005" and "11:40". At the bottom, there are "Cancel" and "Switch" buttons.

1 = The new firmware is stored into the inactive flashbank.

2 = At the time selected, the flashbank with the new firmware becomes the active bank. The controller/ terminal is automatically bootstrapped, a reset is carried out and a parameterization is executed.

3 = The processes are logged in program **IQ Monitor**.



The image shows two screenshots. The top one is the "firmware" configuration window in IQSysMon, showing fields for ID (2), No (2), Description (ACS 8 - 2nd floor), Firmware Bank 1 (ZACS8.00.0V04.10), Firmware Bank 2 (ZACS8.00.0V05.01), Active bank (1), and Build (75). Arrows labeled 1, 2, and 3 point to the "Switch flashbank" button, the "Active bank" field, and the "Download" button respectively. The bottom screenshot is the "IQMonitor" log window, showing a list of events with columns for Time, Location, Source, and Message. Arrows labeled 1, 2, and 3 point to the "Switch flashbank" button, the "Active bank" field, and the "Download" button respectively.



Please note that an automatic parameterization is triggered by the server after switching to another flashbank (irrespective of whether this takes place immediately or at a predefined time). The doors of the controller concerned are out of function during this time (if necessary, inform the security service).

## 5.14.2 ACS-2 firmware update

The procedure is the same as for the ACS-8 firmware update (cf. 5.13.1). The file is called ACS2.FDL and must be located in directory ...\\IQ\_MultiWin\\IQ\_Services\\Download\\ZACS2.

## 5.14.3 ACS-2 plus firmware update

The procedure is the same as for the ACS-8 firmware update (cf. 5.13.1). The file is called AC2P.FDL and must be located in directory ...\\IQ\_MultiWin\\IQ\_Services\\Download\\ZAC2P.

## 5.15 Inputs tab

**Debounce time:** Time (in 1/100 seconds) the device or the software waits until a constant level is available. Only then will the state be evaluated. The factory setting is 1.

**Delay time:** Usually, an event defined at the input triggers immediately a defined action. If this is not desired, a delay value in 1/100ms can be entered.

The factory setting is *0 = no delay*.

**Erasable:** This field indicates whether the ACS-8 can erase the individual input automatically. Time = duration of the erase pulse in 1/100 sec.

The factory setting is *not erasable*.

**Normal condition:** This field is only relevant for the ACS-8 and its components.

(The definition of normal condition corresponds to the definition of normal condition in the *Outputs* tab).

This field defines the state in which the input is to be in normal condition. For the ACS-8 and its components, the state open/closed no longer exists, it has been replaced by *high/low*. The normal conditions defined by the factory are dependent on the input type and are shown in the overview in Appendix 2.

One of the options listed can be selected via the scroll-down arrow right of the entry field: This way it is possible to operate an input invertedly.

The definitions of *Low* and *High* are dependent on the individual device that is connected (control edge from "+" to "-" or vice versa).<sup>11</sup>

**Offline position:** This field is only relevant for the ACS-8 and its components.

If the connection to the ACS-8 module bus user where the input is located fails, the ACS-8 continues working with one of the following states:

- Inactive:<sup>12</sup> The input is to be deactivated or to remain inactive.
- Active: The input is to be activated or to remain active.
- Maintain state: The input is to maintain the current (most recently known) state.

The factory setting is *Maintain state*.

---

<sup>11</sup> for definitions of *high/low* see chapter 9.

<sup>12</sup> for definitions of *active/inactive* see chapter 9.

## 5.16 Keyboard tab

**Clock data keyboard:**

This field must be activated on the terminals where a keyboard is connected via clock data. For the time being, this function is only supported by keyboards in Accentic design (corresponds to IK3 for IDS).

**Debounce time:**

Time in 1/100 seconds the device or the software waits until a constant level is available. Only then will the state be evaluated. (Thus, "false entries" caused by incorrect evaluations are to be avoided).

**Max. input time (1/10 sec.):**

Here you can enter the maximum time in 1/10 seconds during which the entire entry must be completed.

**Max. time between two characters ( 1/10sec.):**

Here you can enter the maximum time in 1/10 seconds which may elapse between the entry of two characters.

**Signal when pressing a key:**

By activating one or several check boxes, you can define whether and how a key activation is to be acknowledged (example: each time when pressing a key, an LED lights up). Combinations are possible. If the check box is not activated, the key activations are not acknowledged.

## 5.17 Key code tab

**Add for duress code:** If you work with → **key code**, a person can enter a code in case of danger (e.g. duress) which is made up of the code number plus the number defined here. This means that the door is opened as usual, but an alarm message is displayed on the screen defined for this purpose. To this end, the check box → **Silent alarm** must be activated under → **Location** → **ACSx**.



Care must be taken that the duress code of one person is not the normal PIN of another person (IQ MultiAccess checks this when creating a PIN number and displays an error message). This can be achieved e.g. by assigning even numbers to the normal PINs and odd numbers to the additional numbers and the resulting duress codes. The same applies to the door code.

**Example:**

PIN / door code	(= even number):	1234
Additional number for duress code	(= odd number):	+ 3
Duress code	(= odd number):	1237



The duress code is entered without carry-over.

**Example:**

PIN / door code	7818
Additional number	+ 3
Mathematical sum	7821
→ <b>Duress code without carry-over:</b>	<b>7811</b>



The additional number for duress can only be modified if no personnel data have been entered yet in IQ MultiAccess (see also Chapters 6.1.1 and 10.1).



Pay attention that the length of the PIN code and duress code must be identical for both systems when working with the **intrusion detection panel interface** option (see also chapter 15, IACP-connection).

**Allow double PINs:** In the location with this box active, one → **PIN** can be allocated to several IDs (persons). But the doors can not be set to the release criterion **PIN**, because no unique identification of a person would be possible. Use: For integration of an IACP and/or if several mandators have access to the same door(s) of one location (see chapter 14).

**Key code length:** Here the key code (→ **PIN**) can be defined to 4 up to 8 digits. A change from a higher to a lower number of digits is only possible as long as no personnel data are captured in IQ MultiAccess (see also chapters 10.1 and 14). If you select 5, 7 and 8 digits it should be noted that this PIN length is not supported by older ZK devices. The terminals ACS1, ACS Compact and ACT are no longer available in this location. The → **door code** is **independent** from the PIN key code length. The door code can be defined up to 6 digits.

**No duress code:** The duress code will not be evaluated in a location with this box active. Use: For integration of an IACP and/or if several mandators have access to the same door(s) of one location (see chapter 14).

**Export of PIN:** If this field is active, it allows by field definition in the export function to export all existing PINs of a location in an export file.

## 5.18 Manual Macro tab

For macros, there is a separate manual **Supplementary Functions of IQ MultiAccess, P32205-46-0G0-xx**.

## 5.19 Multi person AC/Image matching/ATR tab

### ATR (Attendance Time Recording):

IQ MultiAccess offers a simple attendance time recording, which is but not to be mistaken by a real time recording system. The only thing that is recognized is whether a person is present and how long he or she has been in the company from the first entry to the last exit booking of one day. Balances, extrapolations etc. are not possible. In order to use this function, doors can/must be defined as entry, exit or entry and exit doors. Bookings at doors without such a definition will be ignored and falsify the calculated balance.

There are default settings for "omit entry" and "omit exit" to be determined per location in the → **Additional** tab. The factory settings for "omit entry" are 08:00 h, for "omit exit" 16:00 h. They will be used if one or both bookings is/are missing.

### Always retain visitor's card:

Using an absorption reader, visitor ID cards can be retained:

- a) **always**, if this field is activated,
- b) **after expiration of validity**, if this field is not activated.

In both cases the card will be read, the door opened and the card retained.

As of V7, this applies also to employee's data carriers which are marked accordingly (cf. user manual P32205-20-0G0-xx)

The definition of the validity of IDs is done in IQ MultiAccess (P32205-20-0G0-xx) in the → **card data** tab of the personnel master file.

### Image matching:

If this option is used, a camera monitoring the concerning door can be selected. For this application the doorkeeper option (IQ Video) is mandatory. The software in compliance with this function must be enabled.

For details see User manual of IQ MultiAccess (P32205-20-000-xx), chapter 18.

From ACS-2/8 firmware version V8.xx on the image matching can optionally be disabled if the controller runs offline (Disabled in offline mode). This prevents unwanted times of waiting.

As no identification via comparing the person with a deposited photo can be done, it will be ignored. The person gets access with a valid ID card only.

### Multi eye AC (inside/outside):

With ACS-2 plus / 8 controlled doors it is possible per door side to define a number of persons (2 to 9) required to book one after another to cause a release. Thereby no difference is made whether one or more persons have general authorization or not. The door will be released only when the number of persons required booking is reached.

The option → **Multi person access control** must be active in the → **Common** tab in the logical view of the controller that controls the corresponding door.



For ACT controlled doors this option is not available. For ACS-1 see 5.4

### Image matching:

If the option image matching is used, a camera can be selected and allocated to the corresponding door. If the doorkeeper module is used, the corresponding software can be selected. The options can be used either separately or in combination. For more detailed information see the user manual to IQ MultiAccess (P32205-0G0-xx), chapter 18.



## 5.20 OFFLINE state tab

The entries in this tab apply mainly to the ACS-8 bus users. They define how the individual users are to behave if the connection to the ACS-8 is interrupted.

By clicking on the scroll-down arrow right of the entry field, the following offline states can be selected per LED or buzzer :

- Off:** Buzzer/LED is off during offline operation.
- On:** Buzzer/LED is on during offline operation.
- Toggle fast:** LED flashes in short intervals (approx. 2Hz) / buzzer sounds in short intervals (approx.2Hz).
- Toggle slow:** LED flashes in long intervals (approx. 1Hz) / buzzer sounds in long intervals (approx.1Hz).

## 5.21 Output tab

**Activation time:** The output remains active for the period of time entered here.  
The factory setting is 0:00:10.  
The activation time for door openers is defined in *IQ MultiAccess*.

**Activation type:** This field is only relevant for the ACS-2/8 and its components.

One of the options shown below can be selected via the scroll-down arrow right of the entry field:

- On:** The output is activated.
- Toggle slow:** The output is activated/deactivated in long intervals (approx. 1Hz).  
Example: Light flashes in long intervals / hooter sounds in long intervals.
- Toggle fast:** The output is activated/deactivated in short intervals (approx. 2 Hz).  
Example: Light flashes in short intervals / hooter sounds in short intervals.

The factory setting is *On*.

**Delay time:** Only after the time entered here has elapsed will the output become active. If no delay time is specified, the output is activated immediately (e.g. by an event defined in *IQ MultiAccess*).  
The factory setting is 0:00:00.

**Normal condition:** This field is only relevant for the ACS-8 and its components.

(The definition of *normal condition* corresponds to the definition of *normal condition* in the *Inputs tab*).

This field defines the state in which the output is to be in normal condition.

One of the options shown below can be selected via the scroll-down arrow right of the entry field: This way it is possible to operate a relay invertedly.

- Low:** If a relay is e.g. controlled via this output, its normal condition can be defined as *deactivated* with *Low*.
- High:** If a relay is e.g. controlled via this output, its normal condition can be defined as *activated* with *High*.

The factory setting is *Low*.



Fur further information concerning outputs see Chapter 9 (Definition of input/output states). For possible applications see also the separate documentation **Supplementary functions of IQ MultiAccess** (P32205-46-0G0-xx).

**Offline position:** This field is only relevant for the ACS-8 and its components.

This field defines in which state the output is to be if the connection between the ACS-8 and the bus module has failed.

One of the options shown below can be selected via the scroll-down arrow right of the entry field:

- Inactive: The output is to remain inactive or is to be deactivated.
- Toggle slow: The output is activated/deactivated in long intervals (approx. 1Hz).  
Example: Light flashes in long intervals / hooter sounds in long intervals.
- Toggle fast: The output is activated/deactivated in short intervals (approx. 2 Hz).  
Example: Light flashes in short intervals / hooter sounds in short intervals.
- Active: The output is to be activated or remain permanently active .
- Maintain state: The output is to keep the current (most recently known) state.

The factory setting is *Maintain state*.

**Permanently active:**

As an alternative to a certain duration of time which is defined in the previous entry field, it is also possible to activate the action or the device assigned to this output permanently. For this purpose, this field must be activated.

## 5.22 Parameters tab

### Basic state (outside/inside):

You can define for each door side which kind of identification is required for access<sup>13</sup>:

- Data carrier only
- Door code only
- Door code and data carrier
- Door code or data carrier
- PIN only
- PIN and data carrier
- PIN or data carrier

One access criterion can apply to one door condition:

### Normal operation:

The access criterion selected applies as long as the door is in **normal operation**.

**Automatic operation:** The access criterion selected applies as long as an → **automatic operation** is active on the door selected. By means of an automatic operation, it is e.g. possible to set a door to "Permanent released"/"Door locked" for certain periods (see User Manual for examples).

### Description:

The name entered here is assigned to the relevant user in *NetEdit*. The user will be managed with this name in the AC or TR software. The description selected should be unambiguous. We recommend to correct the description manually directly after the automatic definition (e.g. via *Scan for controllers/terminals, ACS-2/8-Scan*), since the entry assigned automatically does not unambiguously indicate the installation location of the user. With manual definition - as the name suggests - entries must be made in every field anyway.

### ID:

Unambiguous device identification. This value is assigned automatically by *NetEdit* and cannot be changed.

### Incorrect attempts (outside / inside):

Definitions depend on the door side:

**Max. number:** How many incorrect attempts are the maximum permitted for reading/input. Depending on the definition, one of the following options will happen

**Block time:** Enter a time (in seconds) for blocking access or macros after the maximum number of incorrect reading/input activities has been exceeded.

- **Block access**
- **Block Macros**

**Alarm:** If this field is activated, an alarm will be triggered on the controller/terminal controlling the corresponding door side after the max. number permitted for reading/input activities has been exceeded. An alarm is also triggered if "0" or nothing is entered in → **block time**.

### Block access:

If this field is activated, the reader/keyboard will be blocked for the duration of the → **block time** after the maximum number of incorrect attempts permitted has been exceeded. The yellow LED and the red LED are lit simultaneously. The yellow LED indicates that reader / keyboard are in the → **normal condition** defined, the red LED, however, indicates

<sup>13</sup>

The selection of identification possibilities depends on the type of the door, the type of the terminal that controls the door and/or other settings. Deviations are described in the corresponding parts of the documentations.

that the normal condition is blocked at the moment. An identification is not possible.

**Block macros:** If this field is activated, the execution of the → **macros** assigned to this door side will be blocked for the duration of the defined → **block time** after the maximum number of incorrect attempts permitted has been exceeded. The yellow LED and the red LED are lit simultaneously. The yellow LED indicates that reader / keyboard are in the → **normal condition** defined, the red LED indicates that the normal condition is blocked at the moment. Macros cannot be activated, but the door is opened in case of correct identification. If a macro which is executed automatically is assigned to this ID, this person will only be granted a door release. The macro assigned will be suppressed.



**Alarm, block access and block macros** may be used in any combination.

**Key code (outside/inside):**

The relevant → **door code** is entered in field **Exit reader** or **Entry reader**. Depending on the definition, this code may have 4 up to 6 digits.

In addition, field → **Duress code** can be activated.

Mixed operation of door code and PIN is possible within the entire system.

**No.:**

Serial number of the relevant device. This value is assigned automatically by *NetEdit* and cannot be changed.

## 5.23 Reader Settings tab

**Basekey (in preparation):**

An encryption code can be deposited for each location for use during data transfers on the ACS-8 module bus (composition: 32 characters, hexadecimal 0-9 and A-F in any desired combination). Using this encryption code, reader data will be encrypted before transmission over the module bus.

**Card coding:**

On the basis of the bus reader type selected above, the corresponding coding type is displayed automatically. This field cannot be changed.

**Entry velocity:**

This field is active for magnetic readers only. The entry velocity for motor readers can be set continuously by means of the slide control.

**Reader type:**

The type of the individual reader is entered here. You can select the relevant reader type by clicking on the scroll-down arrow right of the entry field.

**Turn DIN Code**

Certain card codings require the code to be turned after reading. If this is the case, this check box must be activated. With the ACS-8 controllers, this value is set automatically depending on the reader/card coding concerned.

## 5.24 Rights

In this tab the individual user rights are allocated to the operators. For more information see chapter 8 = Operators).

## 5.25 Settings tab (controller/terminal settings)

- Area Idx:** This field is for information only and cannot be edited. The value displayed is entered automatically by the program. It is dependent on the type of the card used (factory setting = 0).
- Balance display** This value (in quarters of a second) indicates for how long the balance is to be displayed. (Example: Input 8 corresponds to a display of 2 seconds).
- Baudrate:** This field defines the transmission speed between PC and the modem connected to it. The speed depends on the modem that is used. Select the maximum value via the scroll-down arrow right of the entry field to keep the connection time as short as possible.
- Baudrate bus controller - controller/terminal:**  
The value entered here is used for the transmission speed between the bus controllers and the controllers/terminals. By clicking on the scroll-down arrow right of the entry field, the desired speed can be selected from the options listed. The factory setting is 19200 bauds.
- Baudrate PC - bus controller:**  
The value entered here is used for the transmission speed between PCs and bus controllers. By clicking on the scroll-down arrow right of the entry field, the desired speed can be selected from the options listed. The factory setting is 9600 bauds and must be set via DIP switch in the bus controller.
- Display switch-on time:**  
The value entered here (in minutes) specifies how long the display is ON (illuminated). Applies only to TR terminals.
- Door strike function:**  
If this check box is activated, it is possible to open a door by booking on this terminal.
- Door strike relay activation time:**  
The value entered here (in quarters of a second) indicates for how long the door strike relay is to be activated.
- Expansion board:** A maximum of four 485 PCI cards can be installed. They are numbered from 1 to 4. This field shows which board is being processed at the moment. This field is for information only and cannot be edited.
- Initialization string:**  
Each modem requires certain settings which cause the modem to work according to the individual requirements.  
These settings consist of one or a combination of several AT commands which may differ from one device to the other.  
The initialization string is described in detail in Chapter 6.6.5.
- Local access code:**  
If the individual modem is connected to an extension of a telephone system which does not provide direct access to a telephone exchange line, the preselection for obtaining this access must be entered in this field. In most cases that will be "0".  
In this case, field **PBX connect** must be activated as well.  
If a direct exchange line is available, no entries are required in this field.

**MSN:** see chapter 6.6.2

**PBX connect:** see **Local access code**.

**Port on expansion board:**

Each 485 PCI card provides two ports (Port 0 and Port 1) which are entered automatically by NetEdit. This field shows which port is being processed at the moment. It is for information only and cannot be edited.

**Pulse dial:**

Most modern telephone systems/telephone connections use multiple-frequency dialling (which can be recognized by the fact that each push of a button is acknowledged by a tone - usually in a different pitch). In this case, no modification of this check box is required.

Older systems sometimes still work with the pulse dial method (you can hear a clattering noise as with the dials used in the past). If this is the case, this check box must be activated.

**Switch off error messages:**

If this check box is activated, no error messages are output on the display of the terminal concerned. Applies only to TR terminals.

**Timeout:**

If there is no longer a connection between the software and the individual bus controller after the time entered here (in seconds), this will be reported in the software and, if necessary, output as screen alarm OFFLINE (cf. Alarms tab, Chapter 5.3).

## 5.26 Serial Number tab

**Serial number (in preparation):**

Enter the serial number of the concerned reader, confirm with → **Accept**. This becomes the unique identifier for the reader.

**Encryption (in preparation):**

If encryption is enabled, reader data is transmitted in encrypted form on the module bus.

## 5.27 Tamper monitoring

If tamper monitoring is to be carried out, field "Tamper monitoring" must be selected in this tab. In this case, it is possible to enter values for debounce time and delay time.

**Debounce time:**

Time in 1/100 seconds the device or the software waits until a constant level is available. Only then will the state be evaluated. (Thus, "false entries" caused by incorrect evaluations are to be avoided).

**Delay time:**

Usually, an event defined at the input triggers immediately a defined action. If this is not desired, a delay value in 1/100ms can be entered.

The factory setting is *0 = no delay*.

## 6. Defining hardware / software

### 6.1 Location

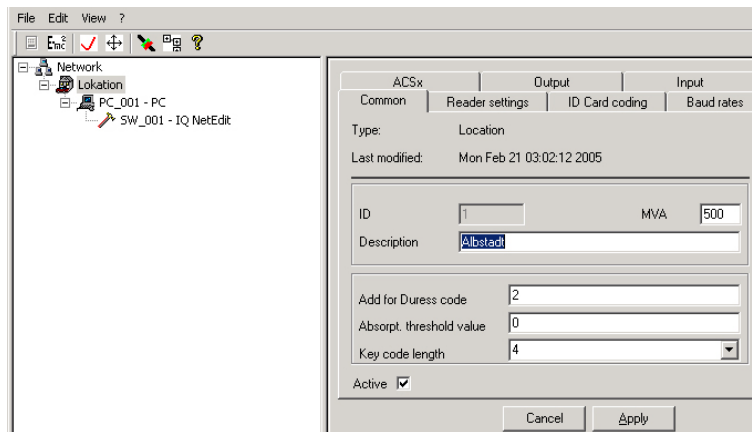
#### 6.1.1 One location

1. Start IQ NetEdit (see Chapter 2.2)
2. Define a location:  
One location is already defined in the factory. Assign an unambiguous name to the location, e.g. the site (left mouse button, tab Common, field Description, or F2 within the tree).  
The location defined in the factory is already marked as active.

Each entry must be confirmed with **Apply**. As an alternative, button



may be activated. Thus all entries will be saved automatically.  
This comment will no longer be included in the following sections.



3. Enter, or at least check, default values:  
The basic settings which apply to the entire location are made in the other tabs of the location (see chapter 5 → **Tabs**). If e.g. reader type **Proximity Esser - var DIN** is selected in the **Reader settings** tab, all readers defined manually or automatically will correspond to this reader type. If necessary, it is possible to change the reader type of individual readers.



The possibility to define default settings per location permits using different reader technologies in a global system. Thus it is possible to combine several individual AC systems controlled by MultiAccess for Windows (V7) into one large global system controlled by IQ MultiAccess.

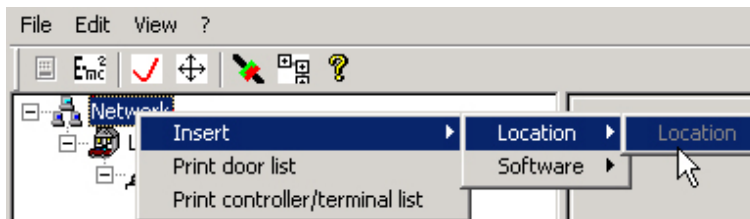
For many small and medium-sized applications, it will be sufficient to define one location (this corresponds to the features of MultiAccess for Windows).



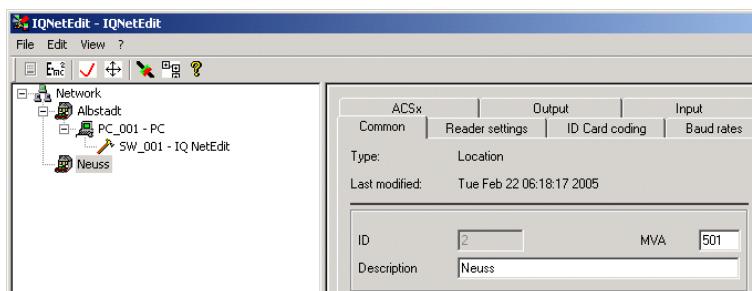
### 6.1.2 Several locations

Requires a licence! In the demo version, only one location is possible.

1. Further locations are inserted by right-clicking on **Network**:



2. Assign a meaningful name already when defining the location. Thus you will not lose the overview in complex installations.



3. Check / adjust the default settings.



Default settings may vary from one location to the other one (see 6.1.1).

4. Select field → **Active**.

If a planned location is already set up in advance, this field must not yet be selected. It is activated only when the location really starts operating.



A maximum of 255 locations may be inserted.



**Further information / particularities of working with several locations see chapter 11 and 12.**

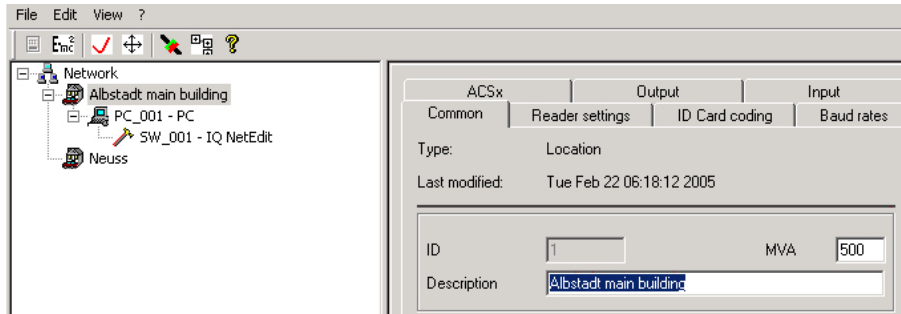
### 6.1.3 Change location description



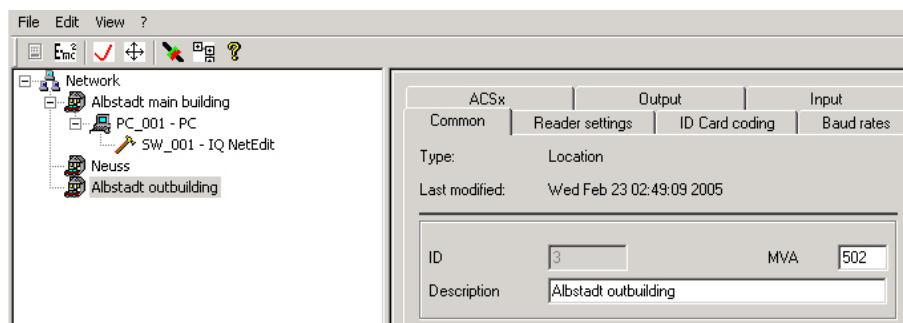
This change of location descriptions must not be mixed up with function → **Location change** by means of which hardware that is physically connected to a location A can be logically assigned to any other location (see Chapter 11 = Several locations).

For reasons of clarity, identical descriptions should be avoided. Existing descriptions can be overwritten.

Example: Location Albstadt comprises two buildings. Select the existing description of location Albstadt and overwrite it with the new, more accurate description (e.g. Albstadt main building).



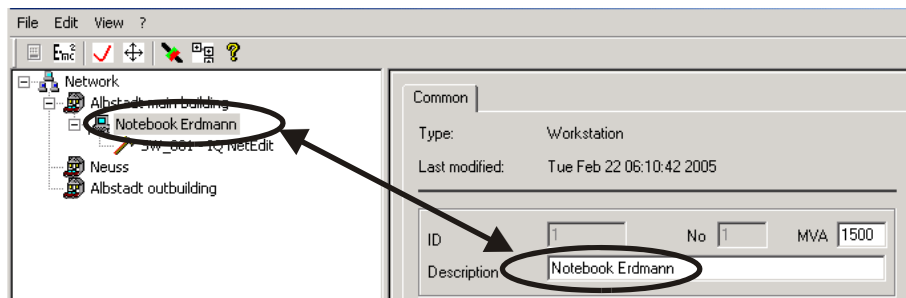
Insert another location (e.g. Albstadt outbuilding) as described in 6.1.2.



## 6.2 Workstation

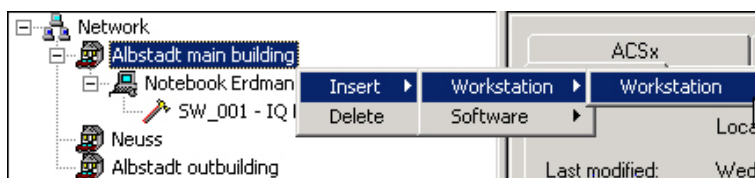
### 6.2.1 Set up a workstation

In the factory setting, a workstation is already set up in location 1 (PC\_001). Assign an unambiguous name by selecting and overwriting:

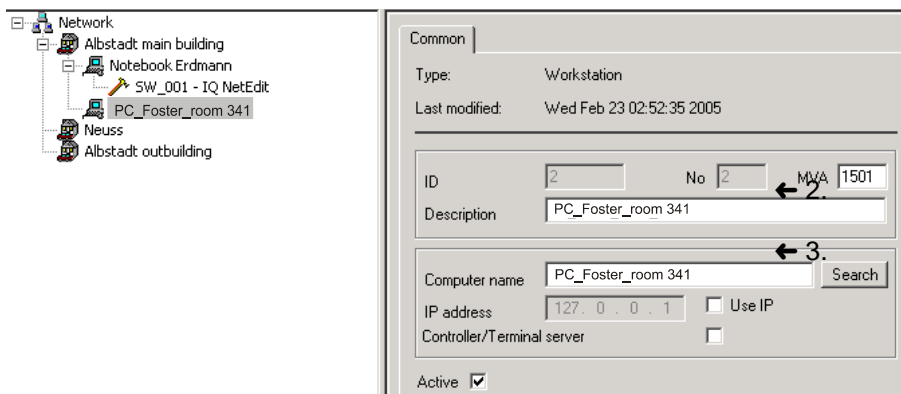


When assigning computer names, please note that all computer names must correspond to the Microsoft NetBios conventions (15 characters max.; no special characters). If this is not the case, it might happen that a client cannot log on to the server.

1. Further workstations are inserted by right-clicking on the individual location.



2. Assign an unambiguous name.
3. Click on **Search** and select the individual description of the computer within the network. If you need more detailed information contact your network administrator.



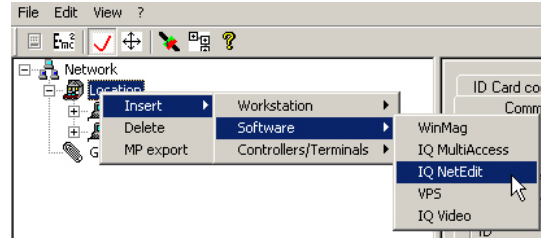
4. Select field → **Active** if the workstation is to be used immediately. If it is only set up in advance for future use, this field remains inactive.



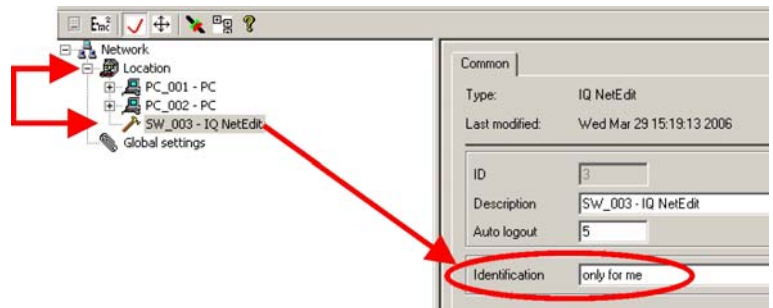
A maximum of 255 workstations can be connected per location. The total number within the entire application is 65025.

### 6.2.2 Several workstations

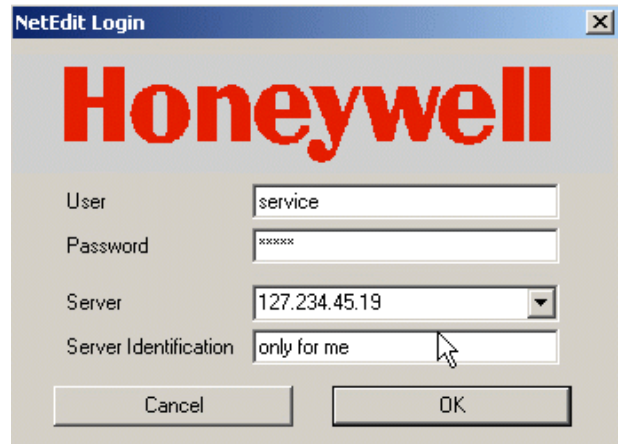
In general, all the workstations can be set up in the same way. But if a special program (e. g. IQ NetEdit) should only be allowed to be started by the system administrator, but that from each workstation, you can realize this by enabling the software directly at a location instead of enabling it at every single workstation.



This software gets an identification.

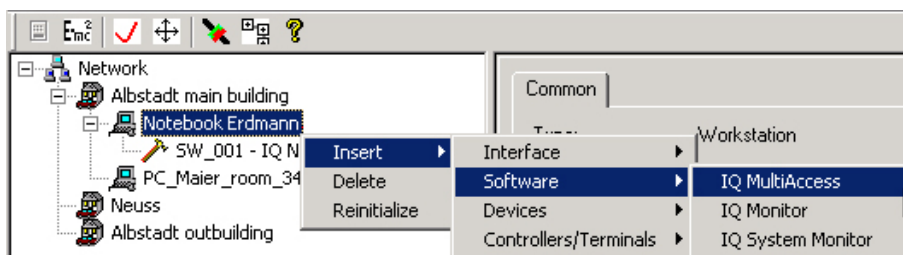


Now the authorized user can start IQ NetEdit from any workstation, just by entering the server name or IP address of the server in the field **server** and the identification code in the field **server identification** previously allocated in IQ NetEdit.

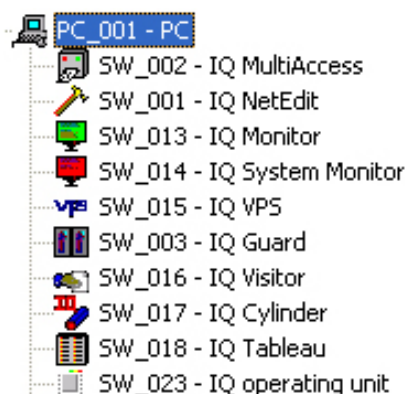


### 6.3 Software


In the factory setting, Software **IQ NetEdit** is assigned to workstation (PC\_001). All programs which are to be operated from this workstation are inserted by right-clicking on this PC.



In our example, all available programs are selected and **activated**.



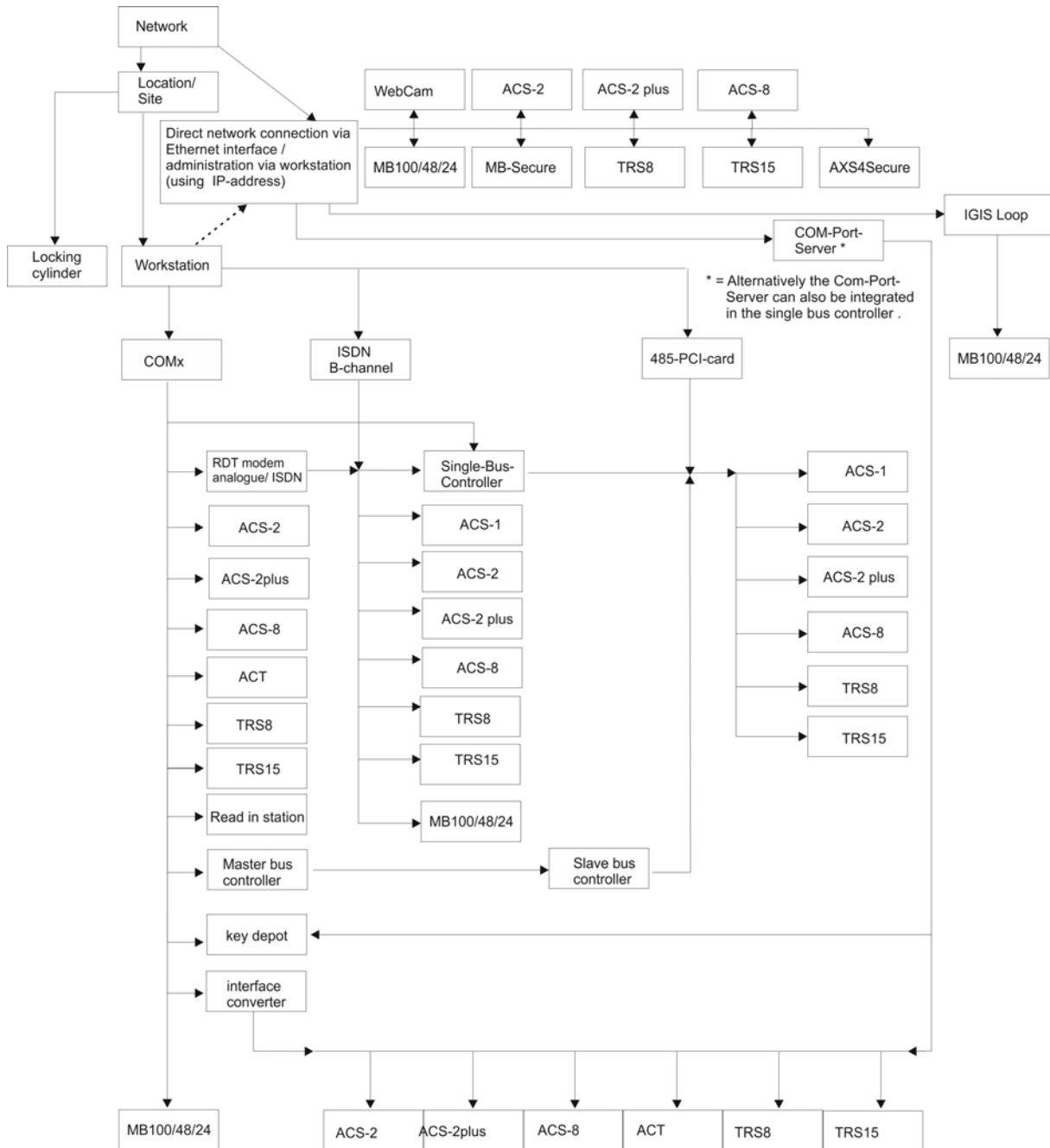
Thus it is possible to operate all programs from this workstation and to check the functions of the installation. For the actual installation, it is e.g. not necessary to insert the IQ MultiAccess software on workstations which have only hardware connected to them but do not work in the program. On the other hand, the software can also be installed on workstations where no AC/TR software is connected.

 Software can also be allocated directly to a location. Then it needs an identification to be started (see 6.2.2).

## 6.4 Controllers/Terminals

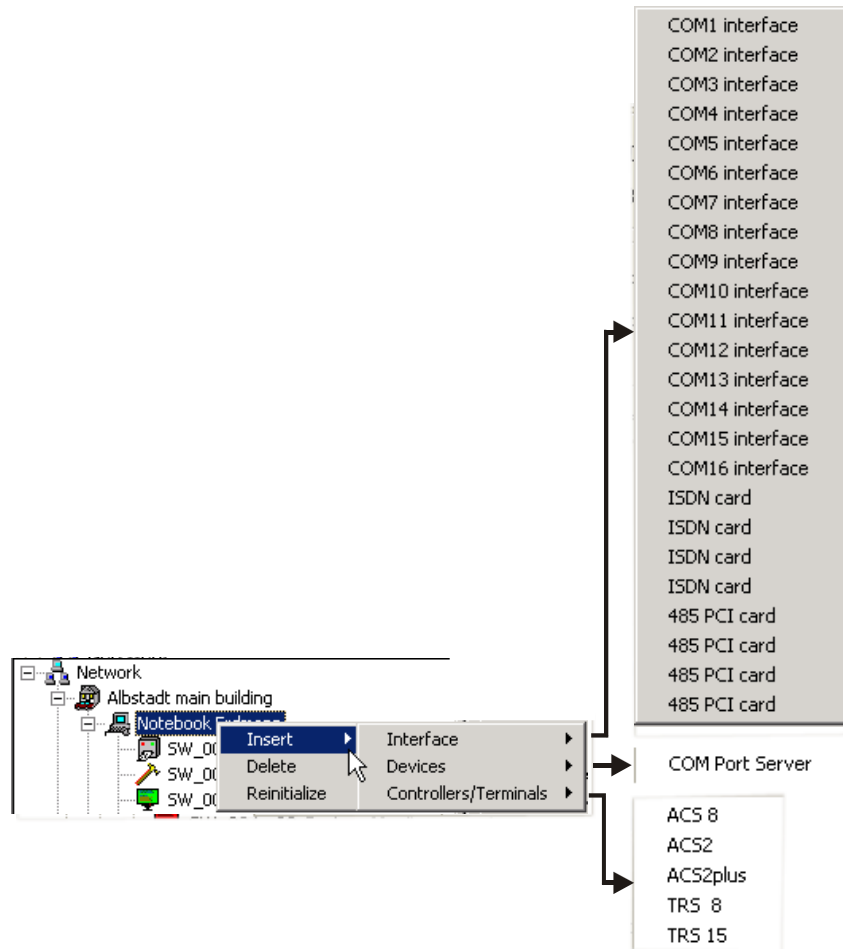
The actual AC controllers/TR terminals are assigned to a workstation by right-clicking. Depending on the individual controller/terminal, there are different connection options which might in addition require the insertion of further components (interfaces, bus controllers, etc.).

Overview: Which devices can be connected to which component?



This graphic only displays devices that can be inserted. Devices no longer supported by IQ MultiAccess but still existing via transferring older databases will be displayed in the tree, too (e. g. because they might occupy existing addresses). Tableaus and time recording terminals (except TRS 8 and TRS 15 with active time recording option) are not supported. ACS Compact are still supported but are not available in the “insert hardware” menu. IQ SystemControl only supports MBxxx central units.

This is displayed as initial screen of the **Insert** function after right-clicking on a workstation:



Independent of the connection type of a terminal/controller the communication status is displayed in the IQ NetEdit tree.



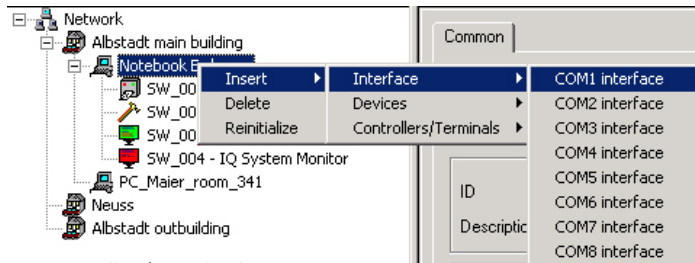
- green: Communication works correctly.
- yellow: Communication path is correct, but the controller/terminal is not answering.
- red: No connection to controller/terminal. Communication path is disturbed / interrupted. Possible causes: Cable is broken-down/plugged off, bus controller out of order or not working correctly, IQ CommTask not running.

The communication states are also displayed in WINMAG.

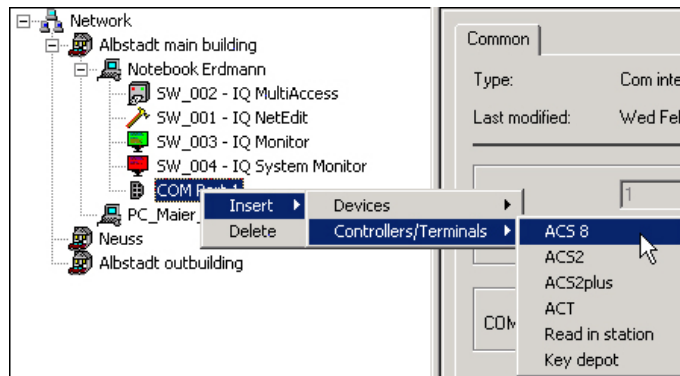
## 6.4.1 Connection versions

### 6.4.1.1 Direct connection via RS-232 (COMx)

1. Insert a COM interface:  
Right-click on the desired workstation → Insert → Interface → COMx.



2. Insert controller/terminal:  
Right-click on the desired COM interface → Insert → Controllers/Terminals → e.g. ACS-8.



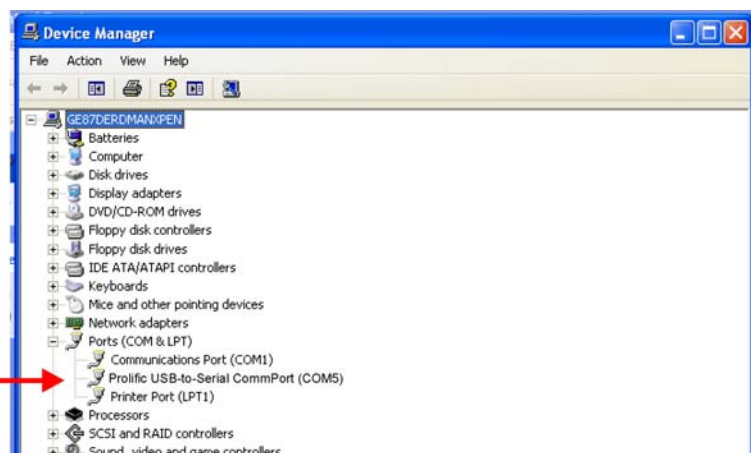
Set the speed (baudrate) for this connection version to 19200 in tab → **Common** (see the Installation Instructions for the individual controllers/terminals and/or the quick guide for AC/TR hardware installation P53001-36-0G0-xx = included as PDF file<sup>14</sup> on the installation CD).

### 6.4.1.2 Connection of read-in stations

Read-in stations are generally to be connected to COMx.

With USB-read-in stations (USB desktop readers) first their drivers (on the CD of the respective desktop readers) must be installed by running the setup or the respective installation exe-file. These drivers effect the transformation of USB to COM.

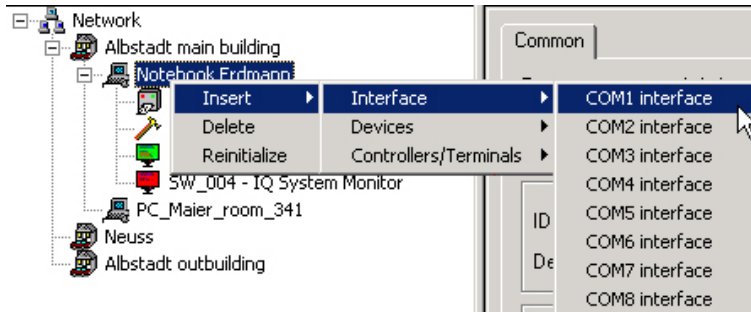
In IQ NetEdit the desktop reader is to be inserted to the COM interface the operating system has assigned. (Control Panel → System → Hardware → Device Manager → Ports COM and LPT):



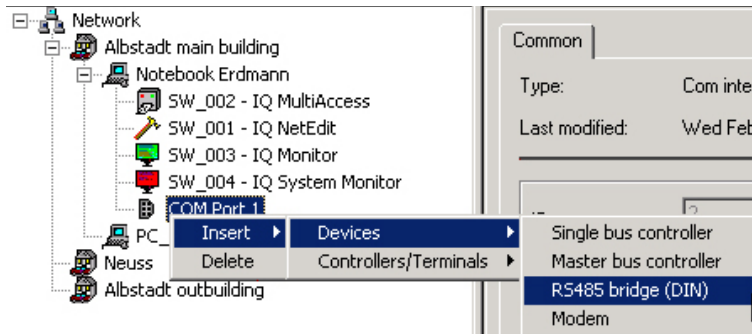


### 6.4.1.3 Connection via interface converter

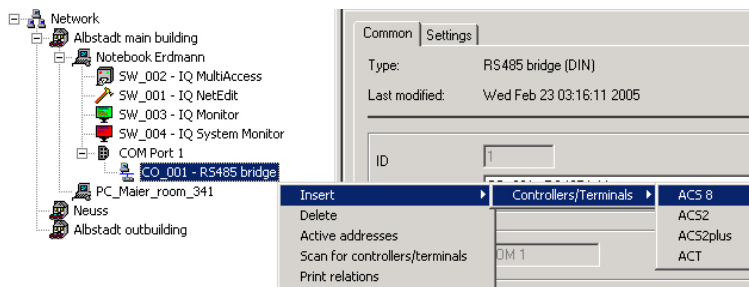
1. Insert a COM interface:  
Right-click on the desired workstation → Insert → Interface → COMx.



2. Insert interface converter:  
Right-click on the desired COM interface → Insert → Devices → Interface converter (RS485 bridge)



3. Assign unambiguous name and select **Active**.
4. Check → tabs **Common** and **Settings** and make adjustments where necessary.
5. Insert controller/terminal:  
Right-click on the desired COM interface converter → Insert → Controllers/Terminals → e.g. ACS-8.



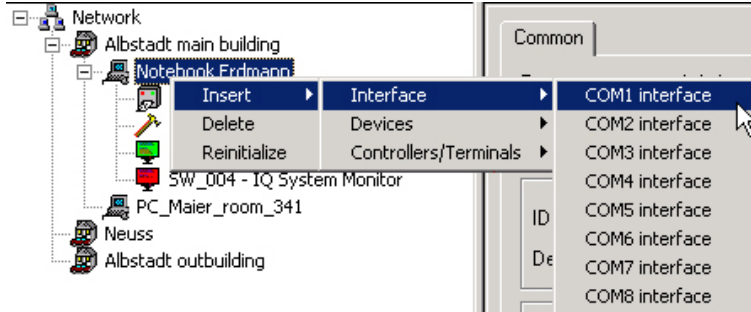
or

right-click on the desired interface converter → Scan for controllers/terminals.  
The program checks automatically which controllers/terminals it can identify on the interface converter selected and it configures them automatically as well.

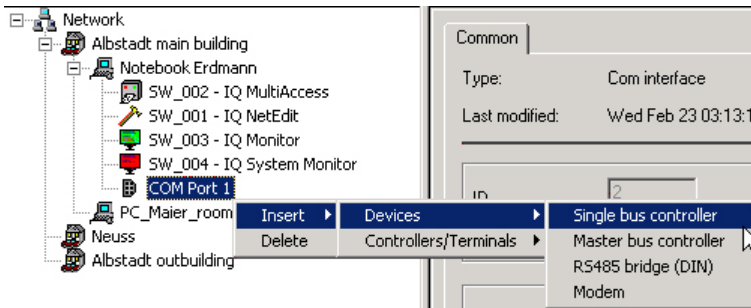
6.4.1.4 Connection via external bus controllers

Single bus controller

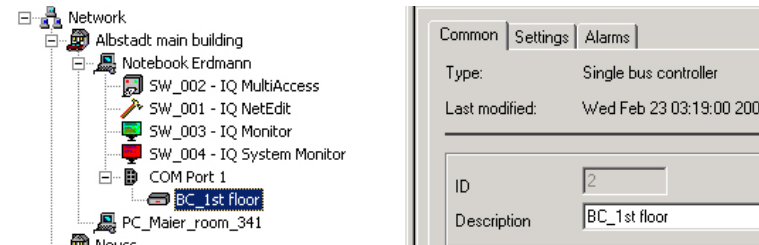
1. Insert a COM interface:  
Right-click on the desired workstation → Insert → Interface → COMx.



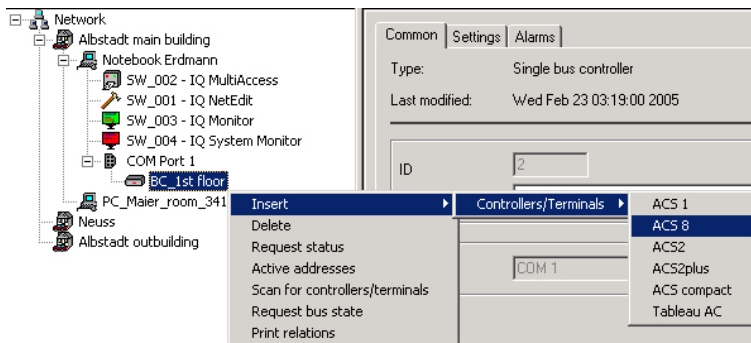
2. Insert an external bus controller:  
Right-click on the desired COM interface → Insert → Devices → Single bus controller



3. Assign unambiguous name and select **Active**.



4. Check → **tabs Common, Settings and Alarms** and make adjustments where necessary.
5. Insert controller/terminal:  
Right-click on the desired bus controller → Insert → Controllers/Terminals → e.g. ACS-8.



or

right-click on the desired bus controller → Scan for controllers/terminals.  
The program checks automatically which controllers/terminals it can identify on the bus controller selected and it configures them automatically as well.

### Master/Slave Bus-Controller

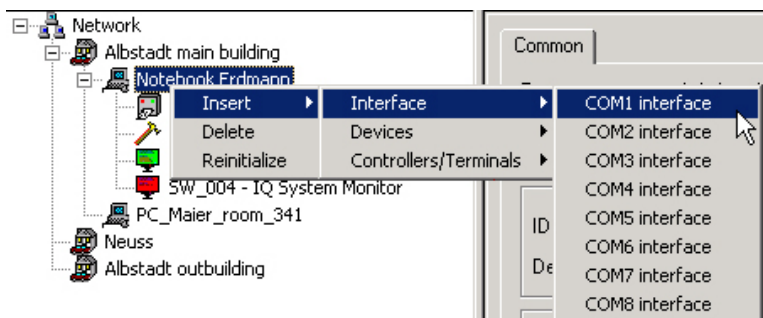


For reasons of performance and operational reliability, a master/slave installation should be avoided whenever possible. All functions that required a master/slave installation in the past are meanwhile also possible with single bus controllers.

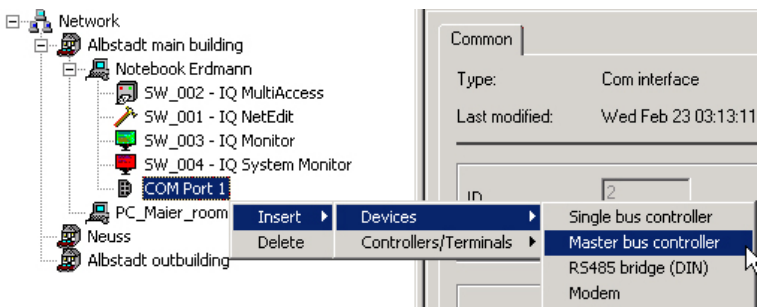
If master and slave bus-controllers are to be modified to single bus-controllers, it is recommended to do this previously in the version V7 / SP2 of MultiAccess for Windows (procedure see installation instructions of the bus-controller).

Should a master/slave architecture be required all the same or already exist, proceed as follows:

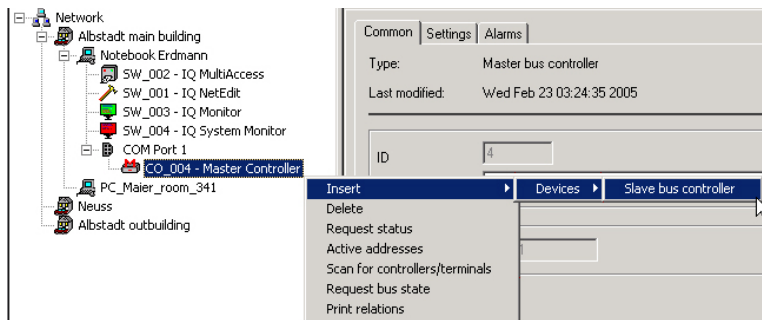
1. Insert a COM interface:  
Right-click on the desired workstation → Insert → Interface → COMx.



2. Insert a master bus controller:  
Right-click on the desired COM interface → Insert → Devices → Master bus controller

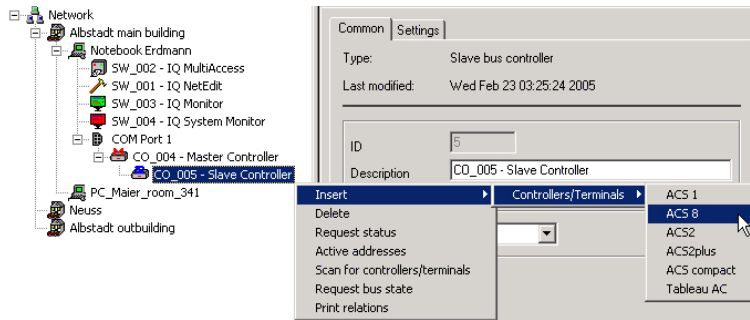


3. Check → tabs Common, Settings and Alarms and make adjustments where necessary.
4. Assign unambiguous name and select **Active**.
5. Insert slave bus controller:  
Right-click on the desired Master Controller → Insert → Devices → Slave bus controller



6. Assign unambiguous name and select **Active**.
7. Check → tabs Common, Settings and Alarms and make adjustments where necessary.

8. Insert controller/terminal on slave controller:  
Right-click on the desired Slave Controller → Insert → Controllers/Terminals → e.g. ACS-8.

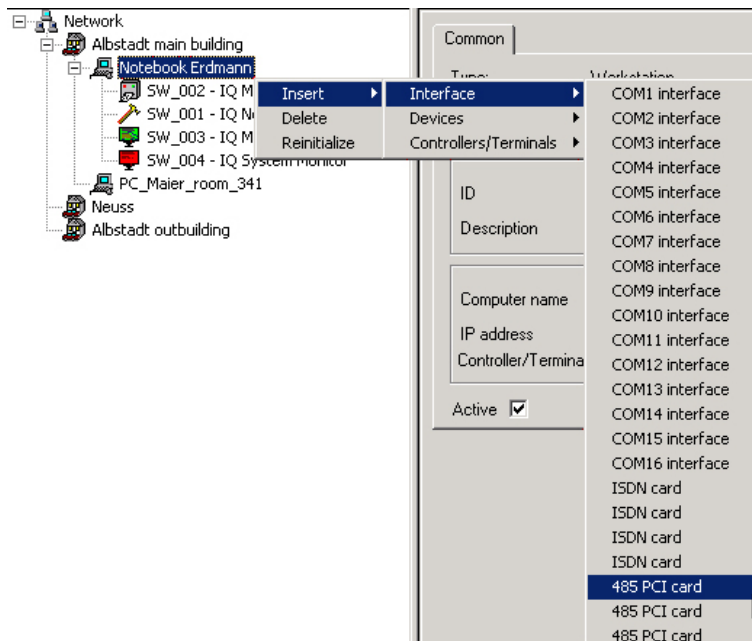


or

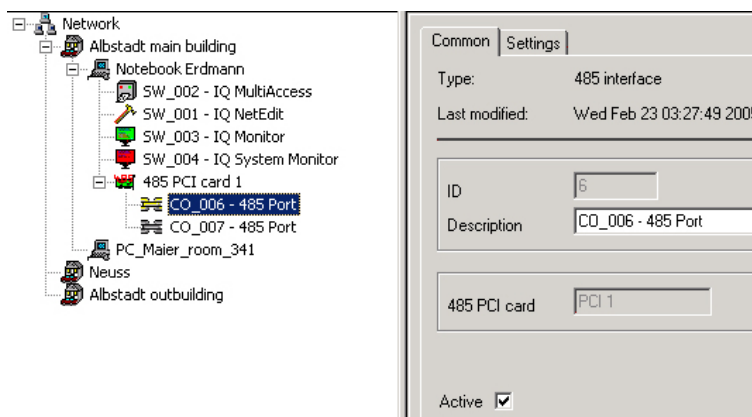
right-click on the desired bus controller → Scan for controllers/terminals.  
The program checks automatically which controllers/terminals it can identify on the bus controller selected and it configures them automatically as well.

### 6.4.1.5 Connection via internal bus controllers

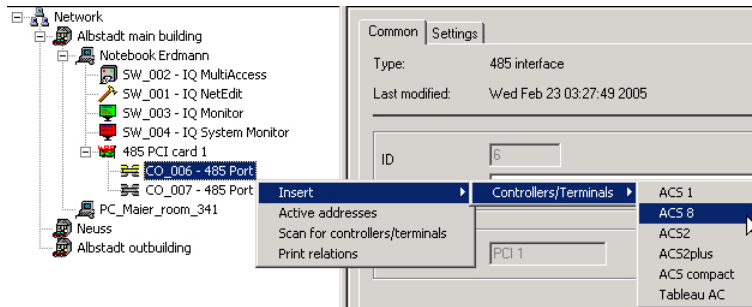
1. Insert an internal bus controller:  
Right-click on the desired workstation → Interface → 485 PCI card.



2. A **485 card** with two ports is inserted automatically.  
Assign unambiguous name and select **Active**.



3. Insert controller/terminal:  
Right-click on the desired Port → Insert → Controllers/Terminals → e.g. ACS-8.



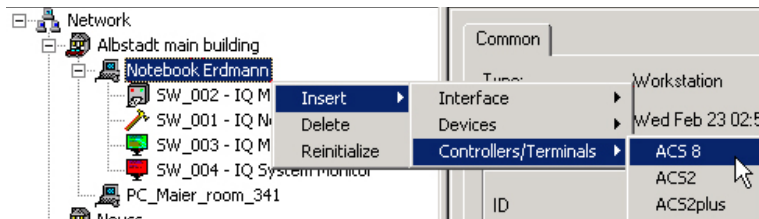
or

right-click on the desired port → Scan for controllers/terminals.  
The program checks automatically which controllers/terminals it can identify on the port of the internal bus controller selected and it configures them automatically as well.

### 6.4.1.6 Connection via Ethernet

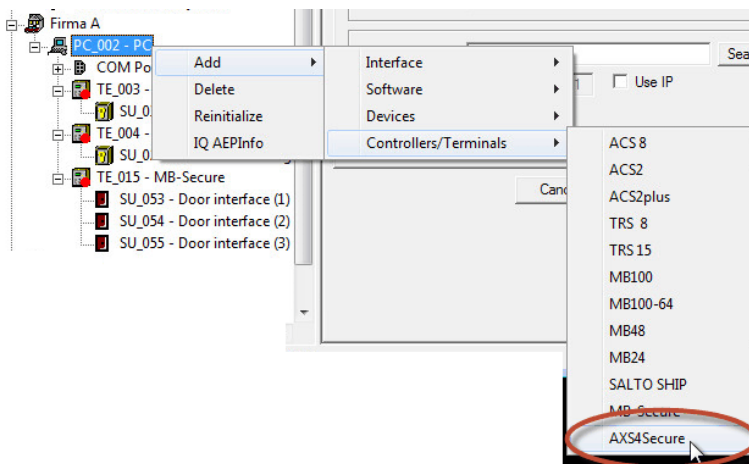
Depending on the individual device, there are two versions of hardware definitions in IQ Nedit. This does not affect the physical hardware installation.

- Version 1:** Right-click on the desired workstation which controls the relevant controller/terminal in the network via the IP address. It is not necessary that the controller/terminal is physically connected to the workstation.
  - Insert → Controllers/Terminals → e.g. ACS-8.
  - This communication uses the → event protocol.



#### Variante 2 (connection variant for AXS4Secure):

- Right-click the desired workstation which controls the relevant AXS4Secure access control terminal on the network via its IP address. The terminal need not be physically connected to the workstation.
  - Add → Controllers/Terminals → AXS4Secure.



Please follow the instructions for the initial installation using IQPanelControl in the Installation/Connection manual for the AXS4Secure access control terminal (IP address and password).

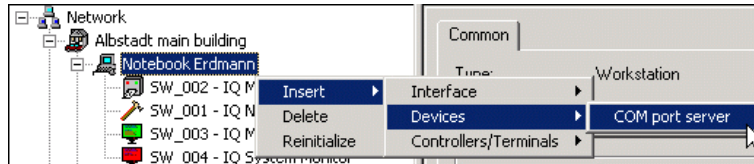
Common   Extended	
Type:	AXS4Secure
Last modified:	Thu Jun 30 08:53:56 2016
ID	16 No 6
Description	TE_016 - AXS4Secure
IP address	0 . 0 . 0 . 0 TCP/IP port 12355
Active <input checked="" type="checkbox"/>	

On tab → **Common** → **IP address**, enter the same IP address that was used in the initial installation of the terminal.

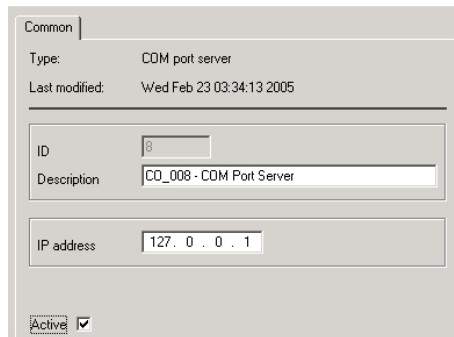
On tab → **Extended** → **Password**, enter the same password that was used during the initial installation of the terminal (min 4 characters, max. 13 characters, alphanumeric).

**Version 3:** For technical reasons, some controllers/terminals require an additional (virtual) device for setup in IQ NetEdit, the so-called → **COM port server**. In this case the communication to the controller uses the → **DIN protocol**.

1. Insert COM port server:  
Right-click on the desired workstation → Insert → Devices → COM port server.



2. Enter unambiguous description, IP address of the ACT connected and select **Active**.

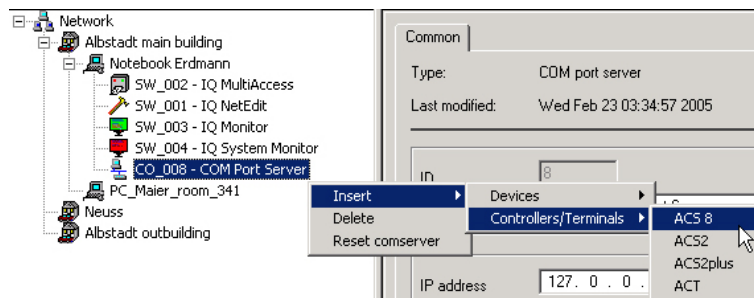


A COM port server must be defined for each ACT connected via Ethernet.

- Connect controllers/terminals directly to COM port server**  
The controllers/terminals are connected directly via Ethernet.

Insert Controllers/Terminals:

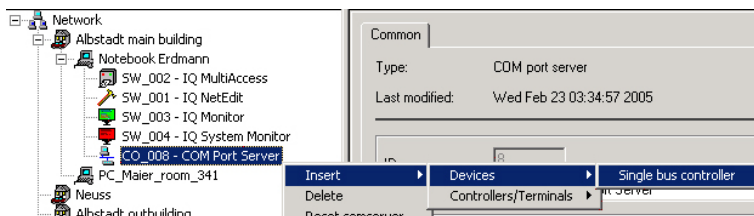
Right-click on the desired COM Port Server → Insert → Controllers/Terminals → e.g. ACS-8.



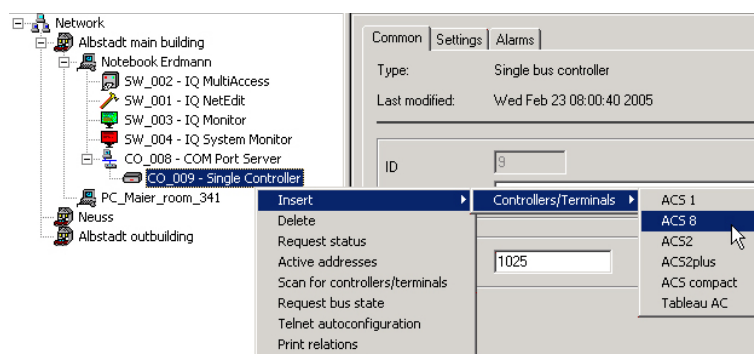


- b) Connect bus controller to COM Port Server / controllers/terminals to bus controller**  
 Only the bus controller is connected via Ethernet, the controllers/terminals are connected to the bus controller via RS-485.

1. Insert single bus controller:  
 Right-click on the desired COM Port Server → Insert → Devices → Single bus controller



2. Insert controllers/terminals:  
 Right-click on the desired bus controller → Insert → Controllers/Terminals → e.g. ACS-8.



or

right-click on the desired bus controller → Scan for controllers/terminals.  
 The program checks automatically which controllers/terminals it can identify on the bus controller selected and it configures them automatically as well.

### 6.4.1.7 Connection via modem / ISDN

see chapter 6.6 Configure distant station.

## 6.4.2 Controller/terminal settings

Irrespective of the connection type, the controller/terminal selected with the corresponding options is inserted according to the default settings of the → **ACSx** tab of the individual location.

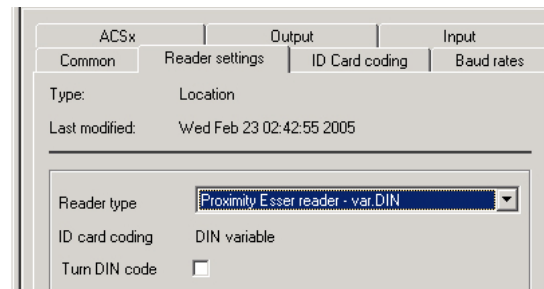
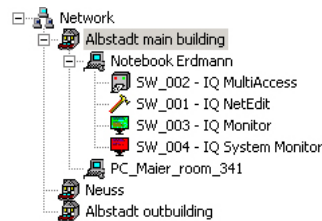
The procedure described below (example: ACS-1) generally applies to **all** controllers/terminals.

1. Check and, if necessary, modify the controller/terminal-dependent → **tabs**.

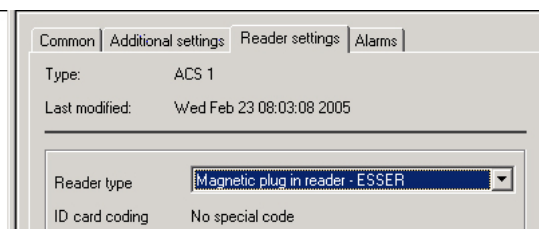
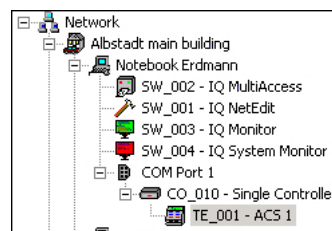


You can make settings here which deviate from the standard and apply only to the controller/terminal selected.

**Example:** In the entire enterprise, proximity readers are used. For the location concerned, **Proximity Esser reader - var DIN** is defined in → **tab Reader Settings**



This setting is applied automatically to all controllers/terminals of this location when they are configured. If another reading method (e.g. magnetic cards) is used (only) at the door which is controlled via the controller/terminal selected, this must be modified individually in → **tab Reader Settings** of the controller/terminal concerned.



The reader types selected must correspond to the cards that are used. Usually, the cards are globally coded. Therefore it makes only sense to change the reading method, if the cards used correspond to the reading method that is newly defined or selected in addition (e. g. combi cards with magnetic Esser coding and another reading method).

**Any modifications should only be made after consultation with our support!**

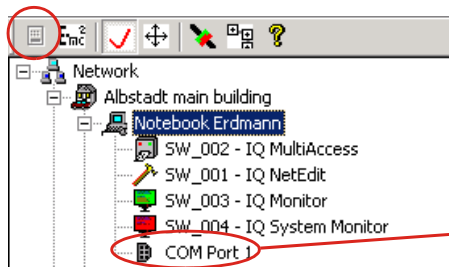
**A global modification of the reading method is not possible afterwards.**

- By inserting a controller/terminal in the → **physical representation**, it is set up automatically in the → **logical representation** according to the default settings (incl. door(s), inputs, outputs etc.).

**Example 1:** Insert an ACS-1 **without** extensions.

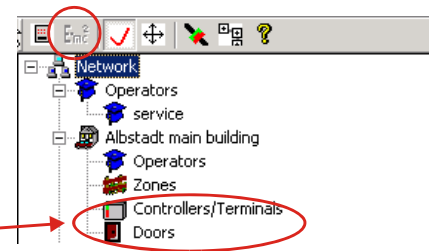
**Physical representation**

before: no controller/terminal inserted

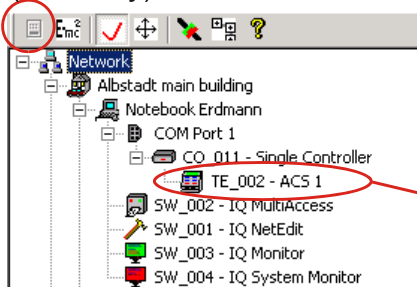


**Logical representation**

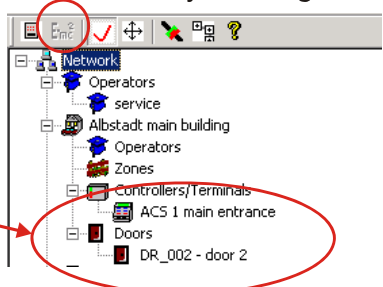
Controller/terminal and doors without content



afterwards: Controller/terminal inserted (manually)



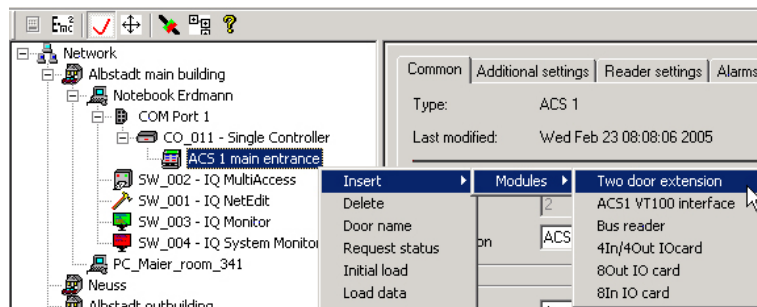
Controller/terminal incl. a door automatically existing



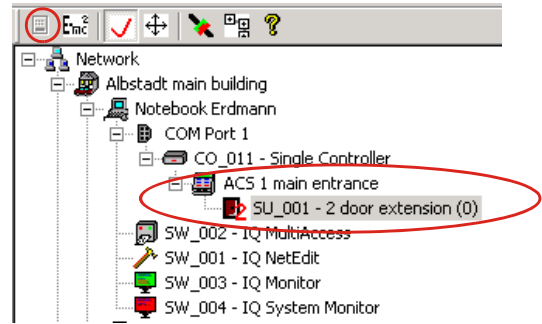
**Example 2:** Insert an ACS-1 **with** extensions.

**Physical representation**

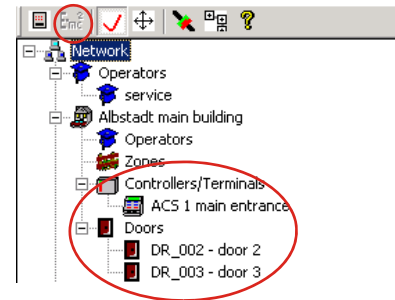
Right-click on the desired ACS-1 → Insert → Modules → e.g. Two door extension.



→ produces the following physical representation:

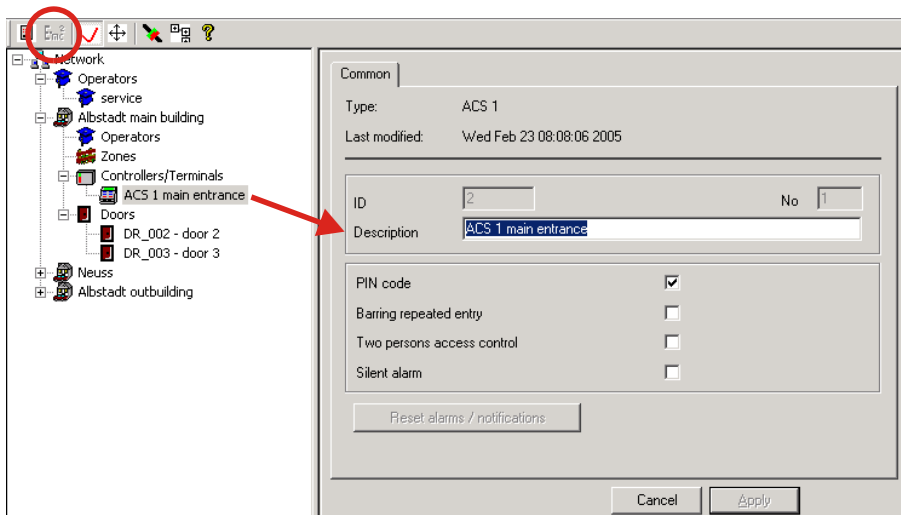


→ In the logical representation, this ACS-1 now exists with **two** doors:



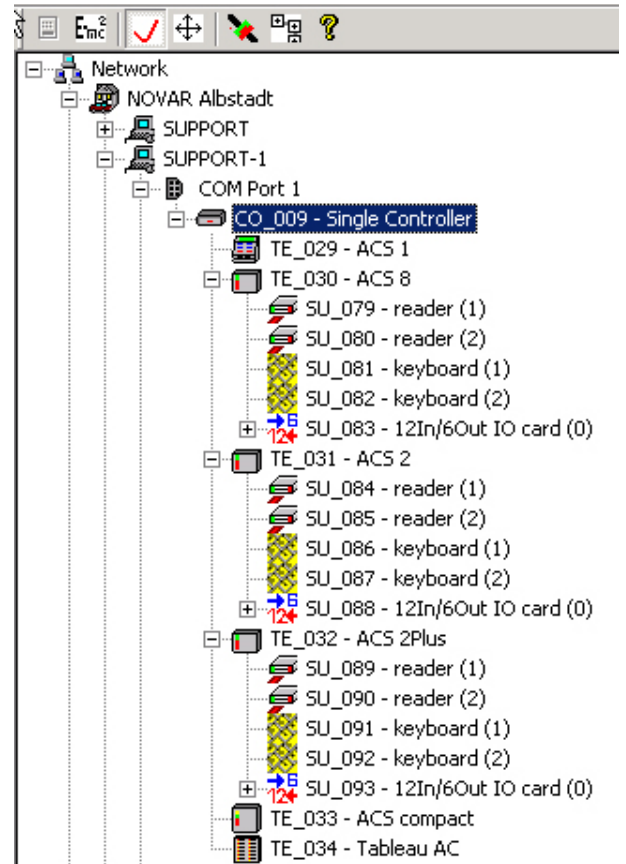
### 3. Controller/terminal properties:

In the logical representation, it is possible to modify certain options individually per controller/terminal (→ **tab Common**). They will apply then only to the controller /terminal selected.



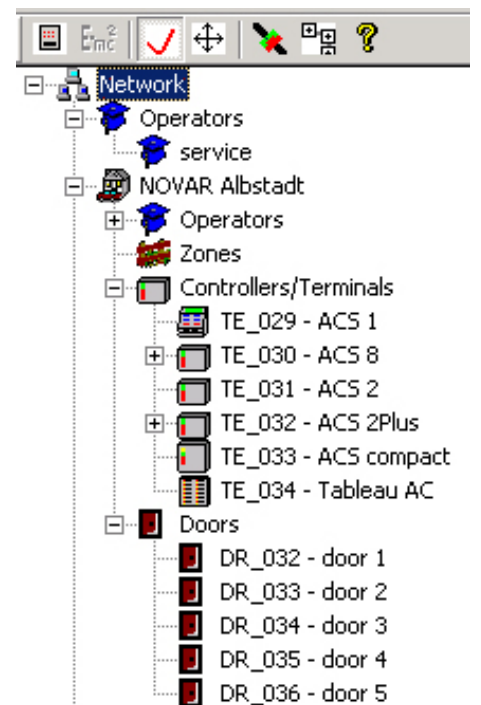
The figure below shows a single bus controller to which one device of all possible controllers/terminals is connected.

Physical representation:



Logical representation:

For each AC controller, the corresponding doors have been defined automatically depending on the default settings of the location. The TRSx time recording terminals and the display tableaus do not initiate the definition of a door.



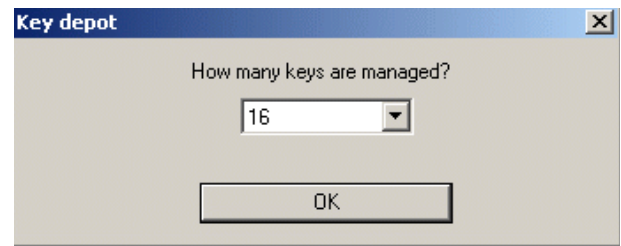
### 6.4.3 Key depot

**Important:** When ordering a key depot from Kemas, please note that a device with a firmware that is compatible to MultiAccess is required.  
Devices already connected to MultiAccess for Windows are not compatible. If they are to be used for IQ MultiAccess as well, the firmware must be updated.

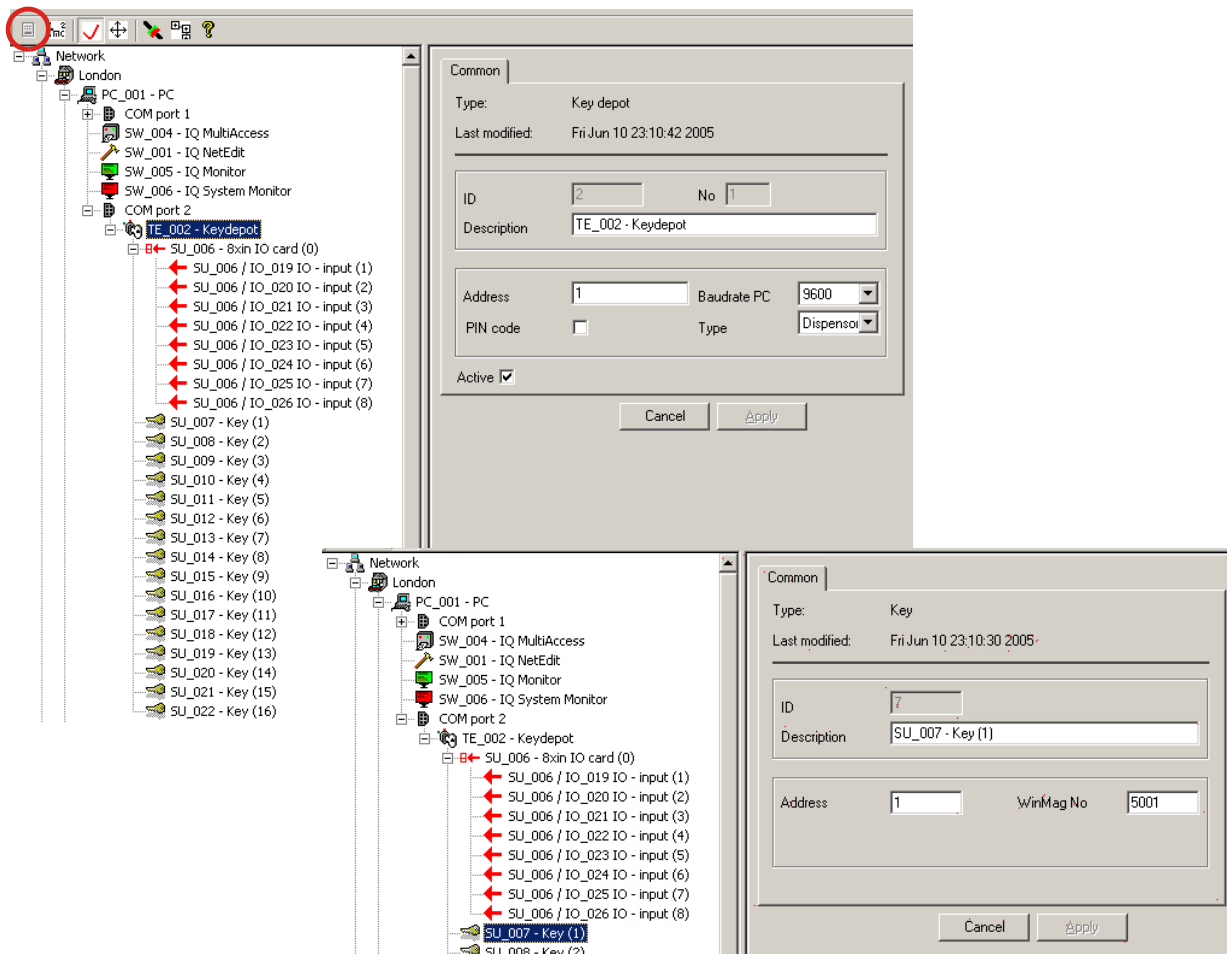
A key depot is used for managing keys which may be taken out by certain persons according to defined plans. In IQ NetEdit, key depots are managed like controllers / terminals.

Connection is made via COMx (see section 6.4.1.1) or Ethernet (see section 6.4.1.5, version 2a = COM-Port-Server). The key depot must be equipped with the relevant interfaces.

When inserting a key depot, you will be asked how many keys are to be managed. This depends on the individual device (is defined when ordering the device). A max. of 256 keys is possible per device, defined in steps of 16.



According to the number of keys selected, a key depot with the corresponding number of keys and an 8-in I/O card is defined.



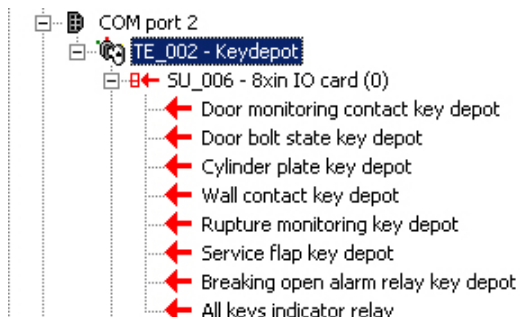
The meaning of the individual fields is explained in section 5.4 = Common tab.

The 8 inputs which are defined automatically are firmly assigned and can be used for messages in WINMAG (see separate documentation).

Meaning of the key depot inputs - overview:

Input	Description	State
1	Door monitoring contact	ON = door closed OFF = door open
2	Door bolt state	ON = bolt closed OFF = bolt retracted
3	Cylinder plate	ON = cylinder plate closed OFF = cylinder plate retracted
4	Wall contact	ON = not torn from the wall OFF = torn from the wall
5	Rupture monitoring	ON = no rupture OFF = rupture
6	Service flap	ON = service flap closed OFF = service flap open
7	Breaking open alarm relay	ON = no breaking OFF = breaking of door/ compartment or bus error
8	all key relays	ON = All keys are there and all compartments are closed. OFF = Not all keys are there.

It is advisable to name the inputs of a key depot accordingly:



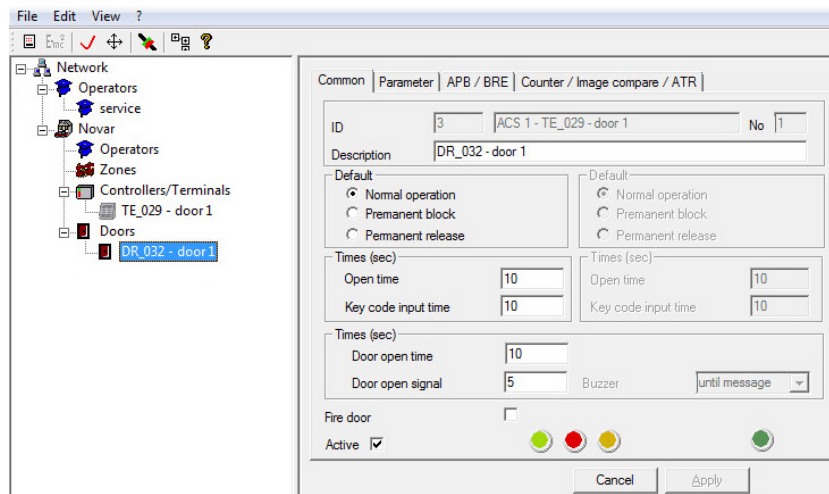
## 6.5 Doors

As described generally in Chapter 6.4.2, doors are configured automatically according to the default settings of the individual location when controllers/terminals are inserted in the physical representation.

In this section, the configuration of doors is described in more detail. It depends on the controller/terminal type used as well as on the fact whether doors are configured automatically or manually. The steps described below are carried out in the logical representation.

### 6.5.1 ACS-1

1. As a standard, an ACS-1 can control **one** door. Therefore, **one** door is configured automatically when an ACS-1 is inserted. Further measures are **not** required. If necessary, check the entries in the → **tabs** of the individual door.



2. If a **Two-door extension** is inserted at an ACS-1, a **second** door is configured automatically. Further measures are **not** required. If necessary, check the entries in the → **tabs** of the individual doors.

Since an ACS-1 has only **one** extension slot, it is only possible to insert one → **Module**. For the door configuration, only the Two-door extension is relevant. Other modules have no influence on the configuration of doors.



### 6.5.2 ACS-2 / 2 plus / 8

An ACS-2 / 2 plus can manage the maximum of 2 doors which are connected onboard.  
 An ACS-8 can manage the maximum of 8 doors, 2 of which can be connected onboard.

#### 6.5.2.1 Onboard doors



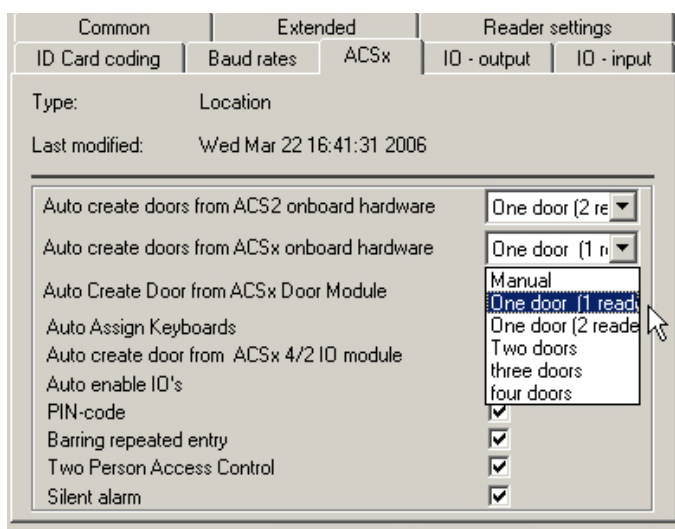
The configuration of onboard doors for ACS-2 / 2 plus and ACS-8 are identical. The examples below show ACS-8 controllers.

Depending on the default settings of the individual location, there are the following options for door configuration:

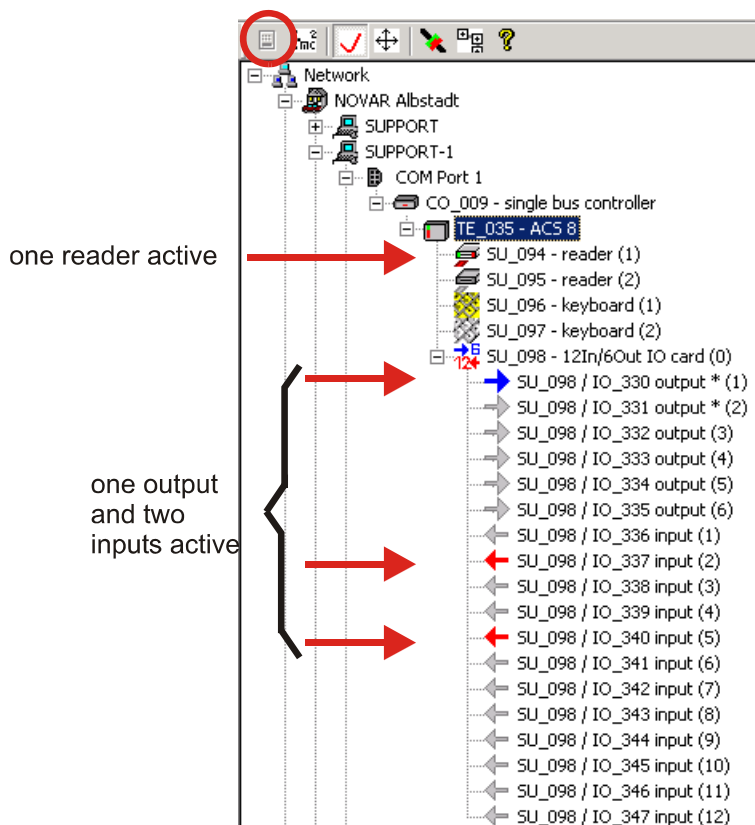
- one door with one reader
- one door with two readers
- two doors with one reader each (with ACS-8 additionally three or four doors with one reader each)
- manual door configuration

#### 1. One door with one reader:

1. Default settings:



result:



Explanation: **One** active reader is the result of the default settings. In this context, it does not matter whether the controller/terminal is configured **manually** or via **Scan for controllers/terminals**. In this case, **Reader 1** is activated (terminals 8 - 14 on ACS-2/8). Even if a second reader is connected to the controller/terminal concerned, the program configures only **one** reader according to the default setting. If required, the second reader must be activated manually.

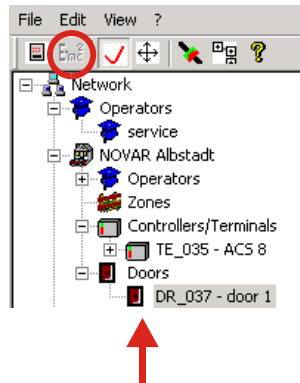
**Output 1** is the door strike relay (terminals 47 - 49 on ACS-2/8).

The two **inputs** which are activated automatically are:

Input 2 = door strike button (terminals 32 - 33)

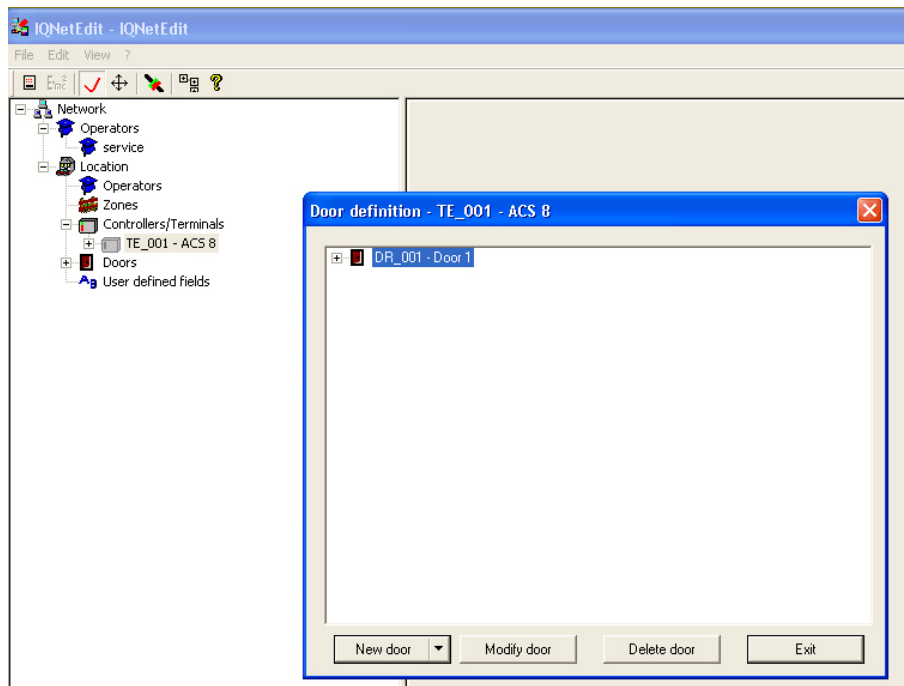
Input 5 = door state contact (terminals 36 - 37)

2. Logical representation:

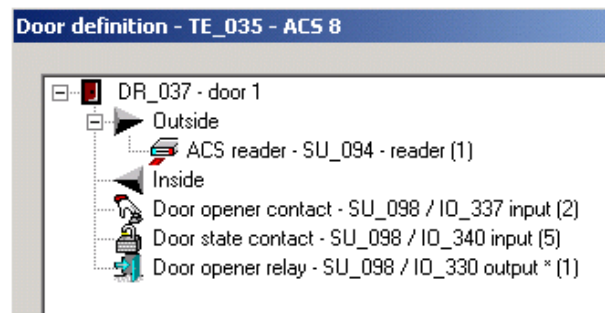


If the devices are already connected and a connection to the workstation exists when the controllers/terminals are configured, the status of doors (here: yellow = normal condition) and of inputs/outputs (active/inactive) is indicated by a coloured dot

3. Right-click on the relevant controller/terminal → Door definition opens the window **Door definition**

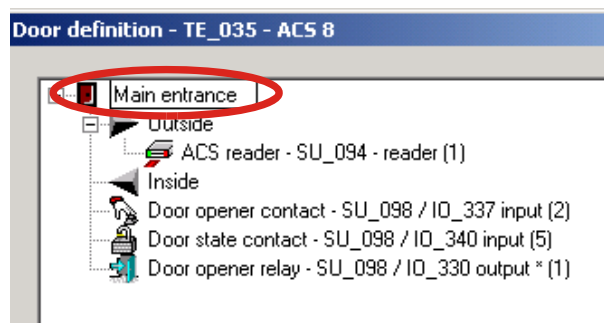


4. Open the tree structure:  
Click on all "+" characters. You will obtain the following overview:



5. Modify door name:  
Up to this point, IQ NetEdit uses general names with consecutive numbers. These should first be replaced by unambiguous user-specific names.

Slowly click twice directly in the text field to be modified or press F2. Enter the desired name.



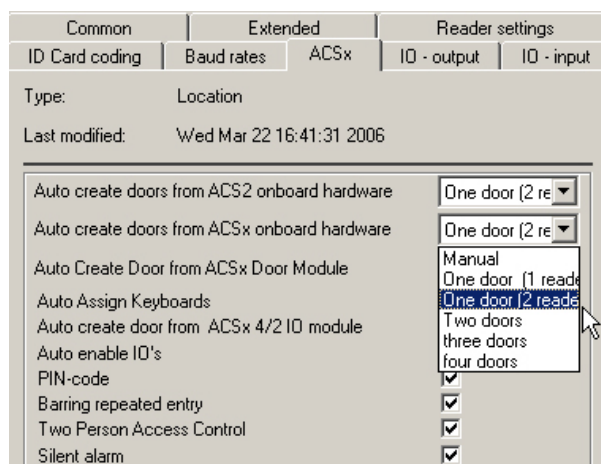
6. Click on **Exit**.



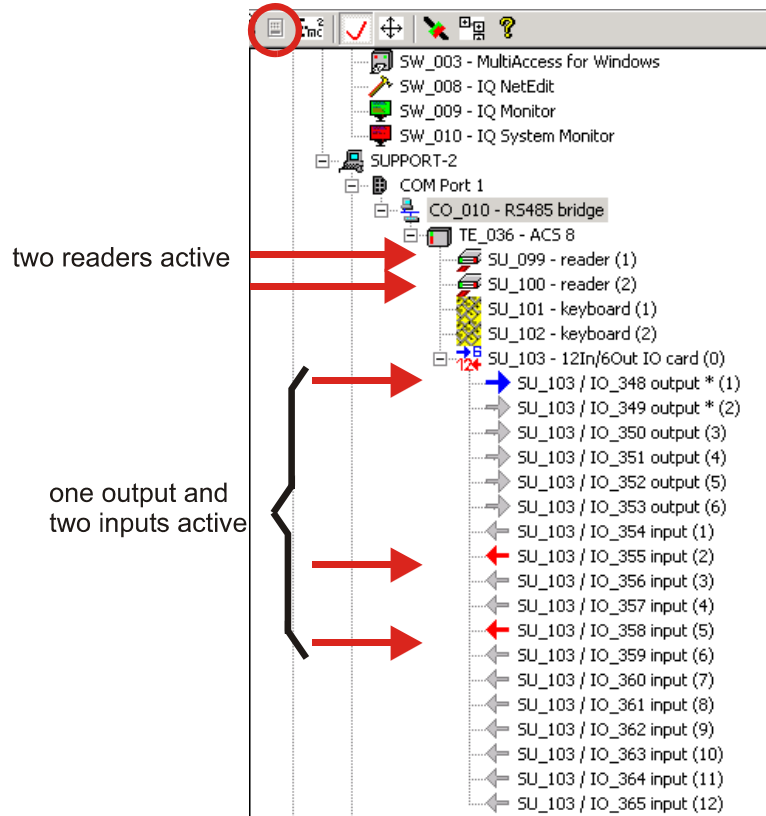
Individual modifications must be made manually via → **Modify door**. This is described in section 4 = manual door configuration.

**2. One door with two readers:**

1. Default setting:



result:



Explanation: **Two** active readers are the result of the default settings. In this context, it does not matter whether the controller/terminal is configured **manually** or via **Scan for controllers/terminals**. In this case, **Reader 1** (terminals 8 - 14 on ACS-2/8) and **Reader 2** (terminals 17 - 23) are activated. Even if only one reader is connected to the controller/terminal concerned, the program defines **two** readers according to the default setting.

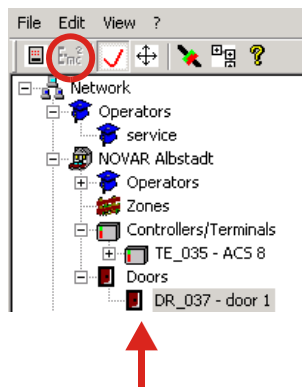
**Output 1** is the door strike relay (terminals 47 - 49 on ACS-2/8).

The two **inputs** which are activated automatically are:

Input 2 = door strike button (terminals 32 - 33)

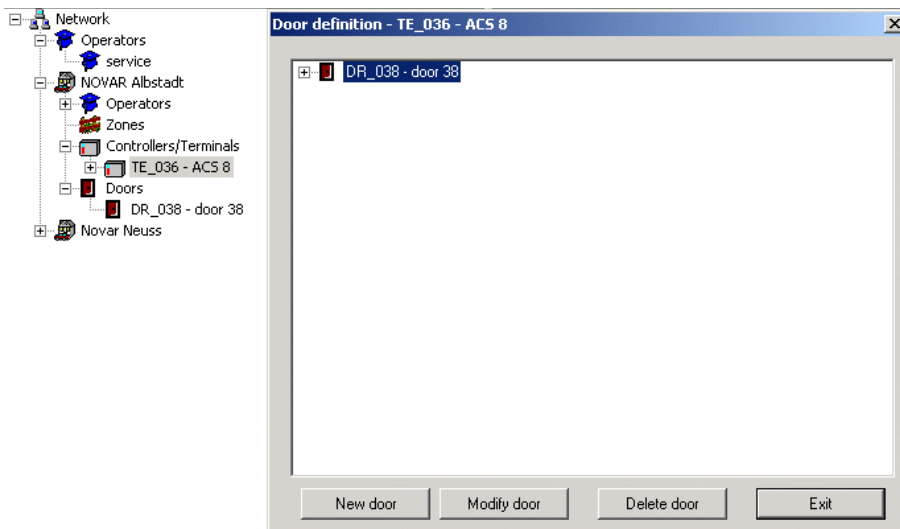
Input 5 = door state contact (terminals 36 - 37)

2. Logical representation:

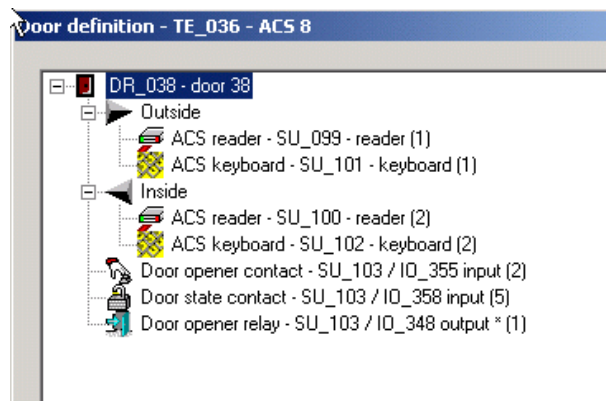


If the devices are already connected and a connection to the workstation exists when the controllers/terminals are configured, the status of doors (here: yellow = normal condition) and of inputs/outputs (active/inactive). is indicated by a coloured dot

- Right-click on the relevant controller/terminal → Door definition opens the window **Door definition**

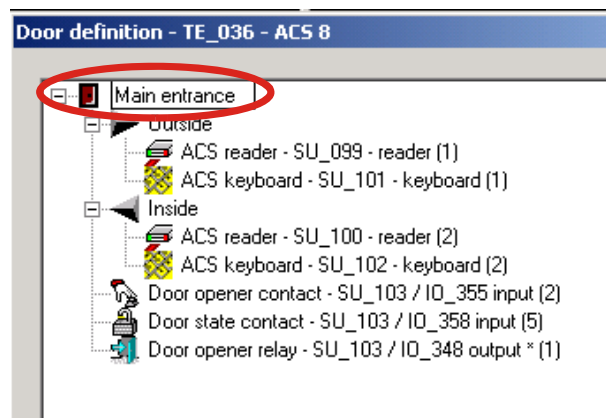


- Open the tree structure:  
Click on all “+” characters. You will obtain the following overview:



- Modify door name:  
Up to this point, IQ NetEdit uses general names with consecutive numbers. These should first be replaced by unambiguous user-specific names.

Slowly click twice directly in the text field to be modified or press F2. Enter the desired name.



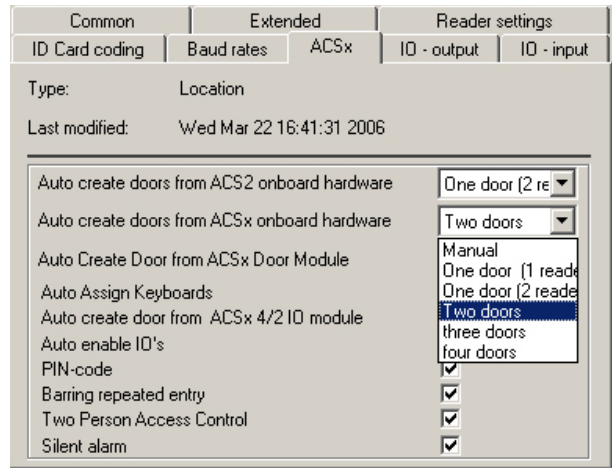
- Click on **Exit**.



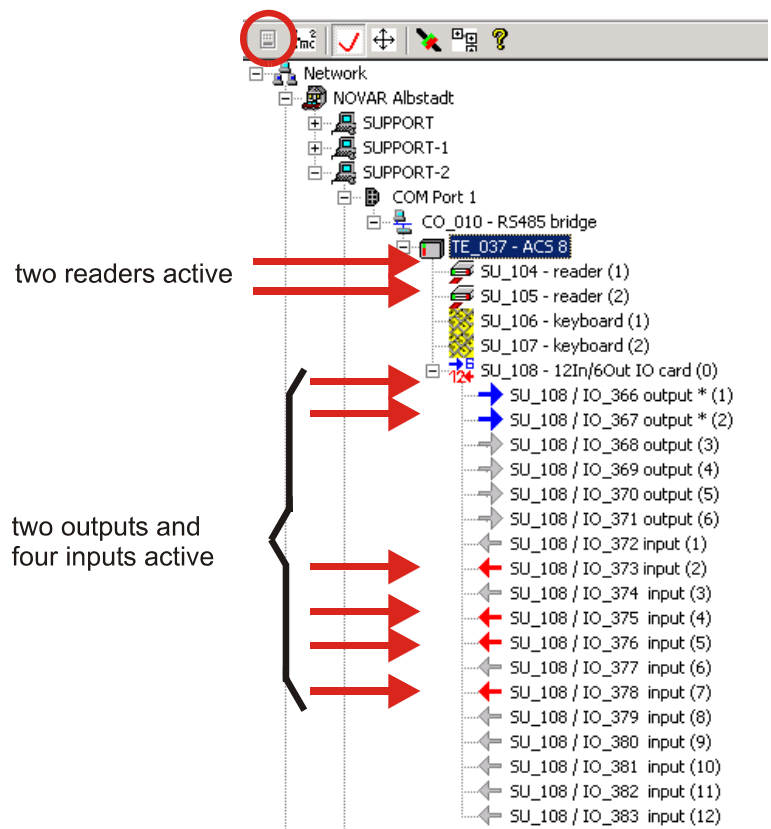
Individual modifications must be made manually via → **Modify door**. This is described in section 4 = manual door configuration.

3. Two doors with one reader each:

1. Default setting:



result:

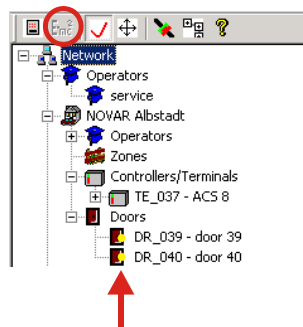


Explanation: **Two** active readers are the result of the default settings. In this context, it does not matter whether the controller/terminal is configured **manually** or via **Scan for controllers/terminals**. In this case, **Reader 1** (terminals 8 - 14 on ACS-2/8) and **Reader 2** (terminals 17 - 23) are activated. Even if only one reader is connected to the controller/terminal concerned, the program defines **two** readers according to the default setting.

**Output 1** which is activated automatically is the door strike relay for door 1 (terminals 47 - 49 on ACS-2/8), **Output 2** is the door strike relay for door 2 (terminals 50 - 52 on ACS-2/8).

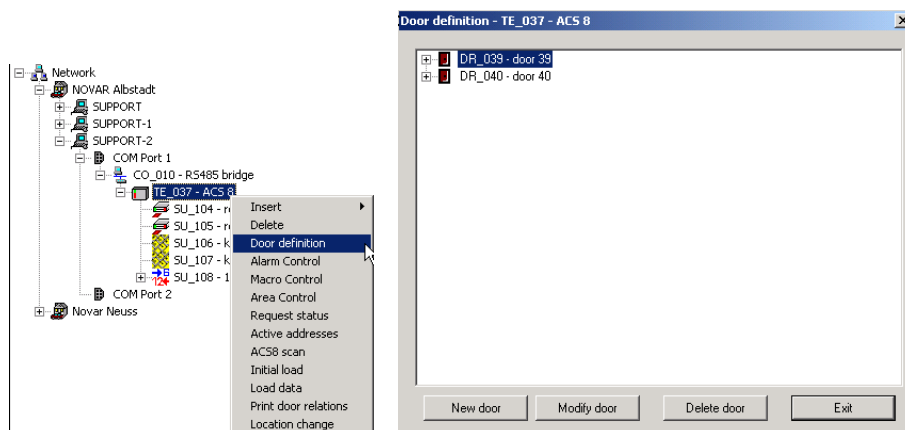
The 4 **inputs** which are activated automatically are:  
 Input 2 = door strike button for door 1 (terminals 32 - 33)  
 Input 4 = door strike button for door 2 (terminals 33 and 35)  
 Input 5 = door state contact for door 1 (terminals 36 - 37)  
 Input 7 = door state contact for door 2 (terminals 39 - 40)

2. Logical representation:

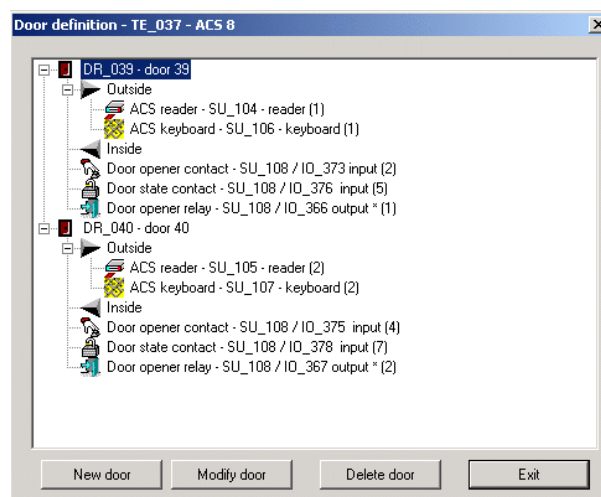


If the devices are already connected and a connection to the workstation exists when the controllers/terminals are configured, the status of doors (here: yellow = normal condition) and of inputs/outputs (active/inactive). is indicated by a coloured dot

3. Right-click on the relevant controller/terminal → Door definition opens the window **Door definition**

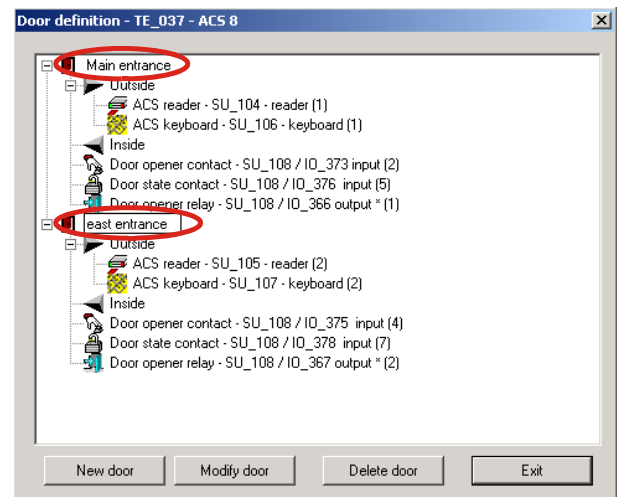


4. Open the tree structure: Click on all "+" characters. You will obtain the following overview:



5. **Modify door name:**  
Up to this point, IQ NetEdit uses general names with consecutive numbers. These should first be replaced by unambiguous user-specific names.

For each door, slowly click twice directly in the text field to be modified or press F2. Enter the desired name.



6. Click on **Exit**.

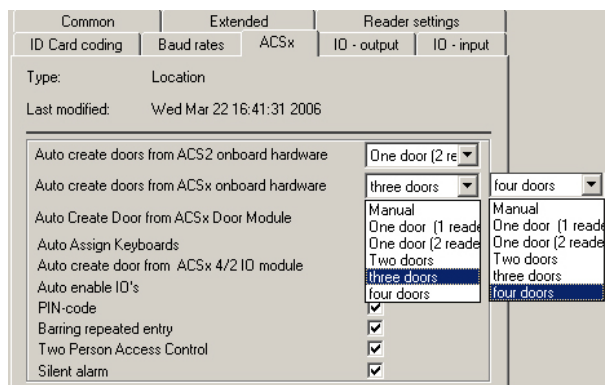


Individual modifications must be made manually via → **Modify door**. This is described in the next section = manual door configuration.



4. Three / four doors with one reader each:

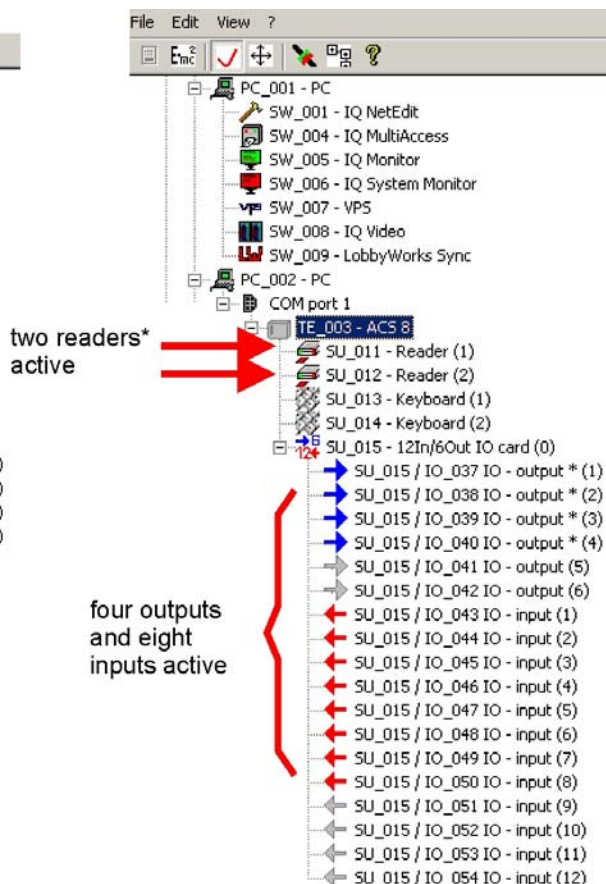
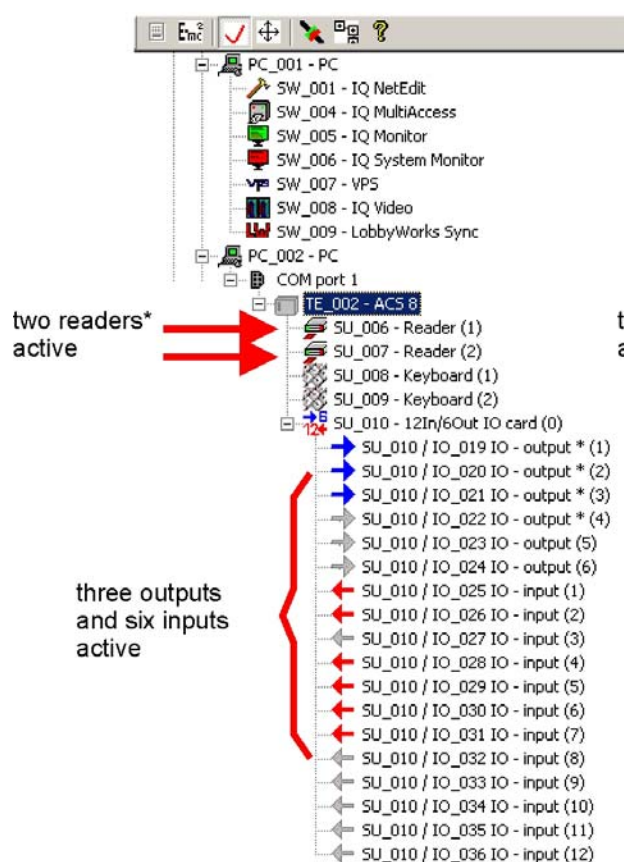
1. Default setting:



result:

3 doors

4 doors



\* = Only two readers/keypads can be connected onboard. All further reader/keypads must be connected to the module bus in RS 485 mode and configured manually (see next step: manual door configuration).

Explanation: **Two** active readers are the result of the default settings. In this context, it does not matter whether the controller/terminal is configured **manually** or via **Scan for controllers/terminals**. In this case, **Reader 1** (terminals 8 - 14 on ACS-8) and **Reader 2** (terminals 17 - 23) are activated. Even if only one reader is connected to the controller/terminal concerned, the program defines **two** readers according to the default setting. There is a maximum of two readers/keypads to be connected onboard to the ACS-8. Further readers/keypads for door no. 3 and 4 are connected to the module bus in RS-485 mode and have to be configured manually.

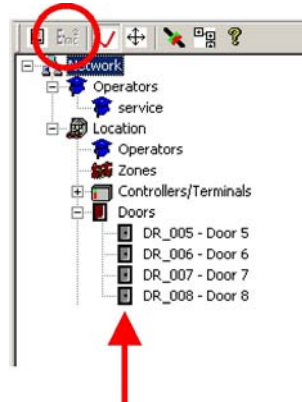
**Output 1** which is activated automatically is the door strike relay for door 1 (terminals 47 - 49 on ACS-8), **Output 2** is the door strike relay for door 2 (terminals 50 - 52 on ACS-8), **Output 3** is the door strike relay for door 3 (terminals 53 - 54 on ACS-8), **Output 4** is the door strike relay for door 4 (terminals 25 - 27 on ACS-8).

The six/eight **inputs** which are activated automatically are:

Input 2 = door strike button for door 1 (terminals 32 - 33)  
 Input 4 = door strike button for door 2 (terminals 33 and 35)  
 Input 1 = door strike button for door 3 (terminals 31 and 33)  
 Input 3 = door strike button for door 4 (terminals 33 and 34)

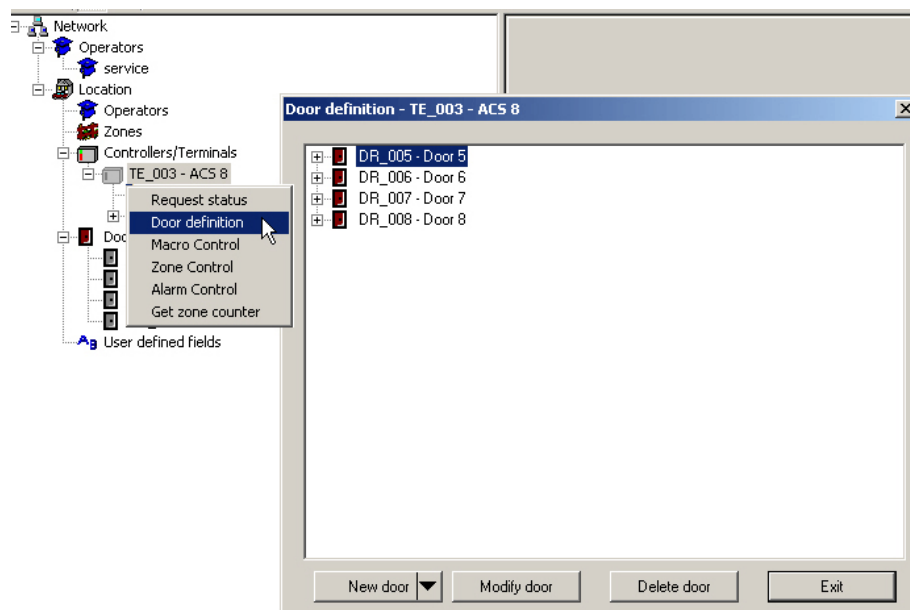
Input 5 = door state contact for door 1 (terminals 36 - 37)  
 Input 7 = door state contact for door 2 (terminals 39 - 40)  
 Input 6 = door state contact for door 3 (terminals 37 - 38)  
 Input 8 = door state contact for door 4 (terminals 40 - 41)

2. Logical representation:

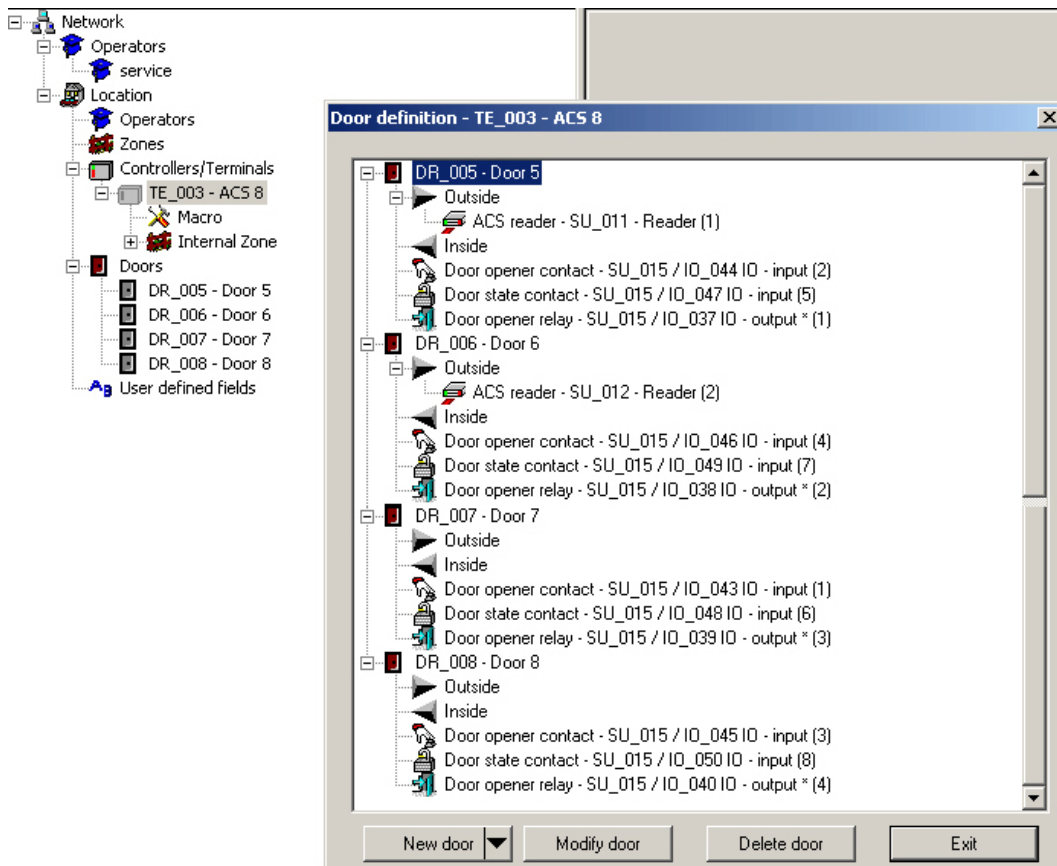


If the devices are already connected and a connection to the workstation exists when the controllers/terminals are configured, the status of doors and of inputs/outputs (active/inactive), is indicated by a coloured dot (here: yellow = normal condition).

3. Right-click on the relevant controller/terminal → Door definition opens the window **Door definition**

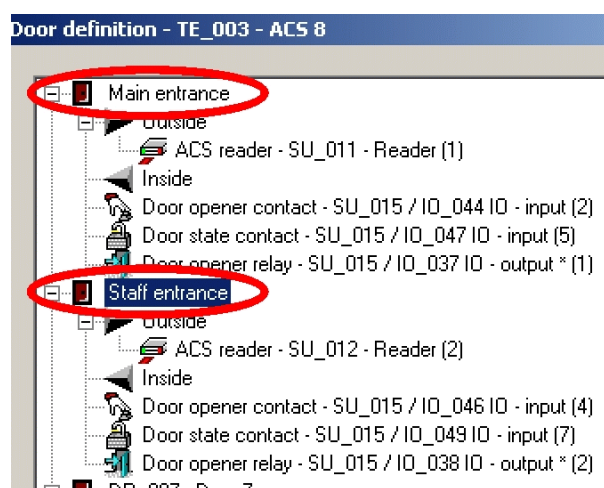


- Open the tree structure:  
Click on all "+" characters.  
You will obtain the following overview:



- Modify door name:  
Up to this point, IQ NetEdit uses general names with consecutive numbers. These should first be replaced by unambiguous user-specific names.

For each door, slowly click twice directly in the text field to be modified or press F2. Enter the desired name.



- Click on **Exit**.



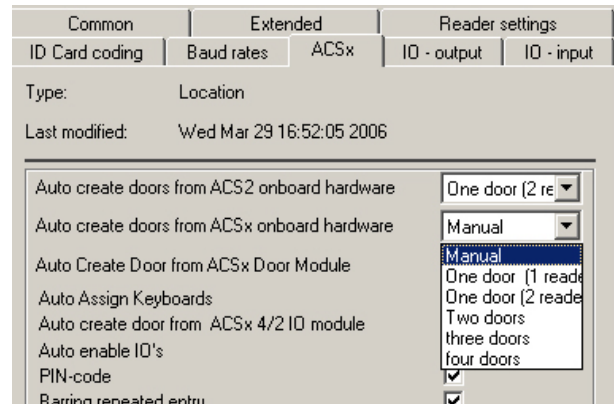
Individual modifications must be made manually via → **Modify door**. This is described in the next section = manual door configuration.

## 5. Manual door configuration:

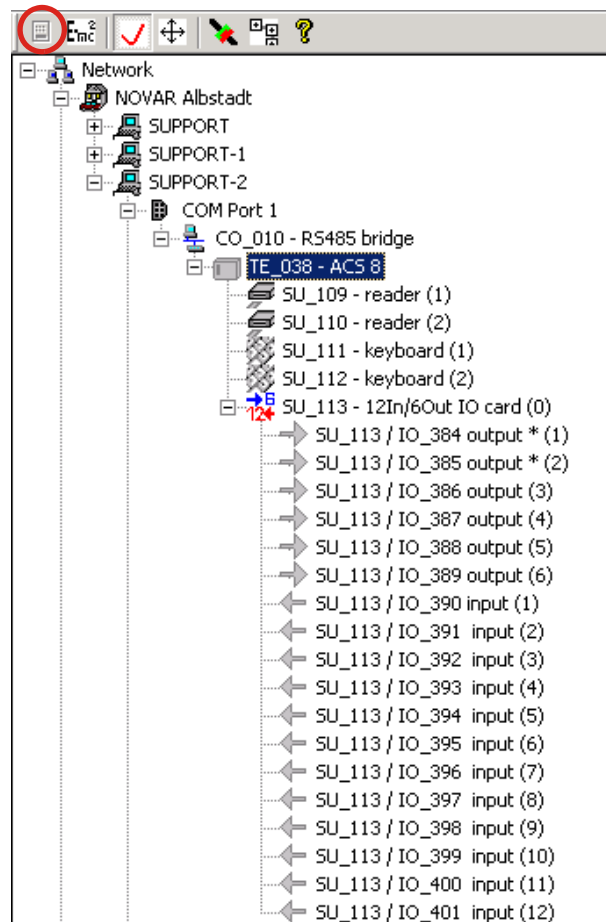
Manual door configuration is used for new configurations as well as for modifications of existing doors.

### New configuration

#### 1. Default setting:

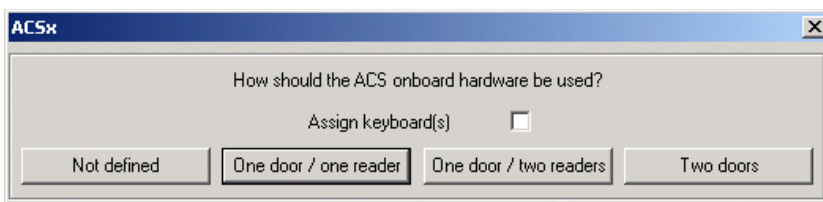


a) produces this result via function → **Scan for controllers/terminals:**

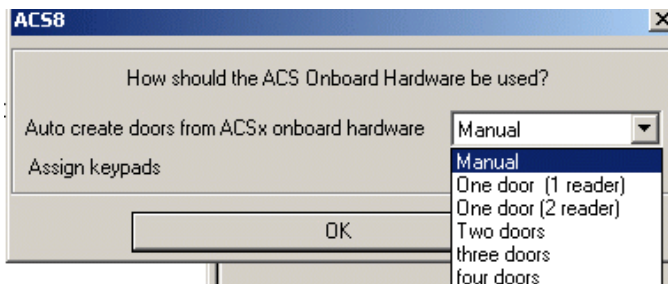


Explanation: All controllers/terminals identified are configured but without active components since these, by definition, are to be configured **manually**. (The illustration shows the configuration of an ACS-8 controller - which is similar to the configuration of an ACS-2 controller).

b) produces this prompt via function → **Insert** → **Controllers/Terminals** → **ACS-2plus**:



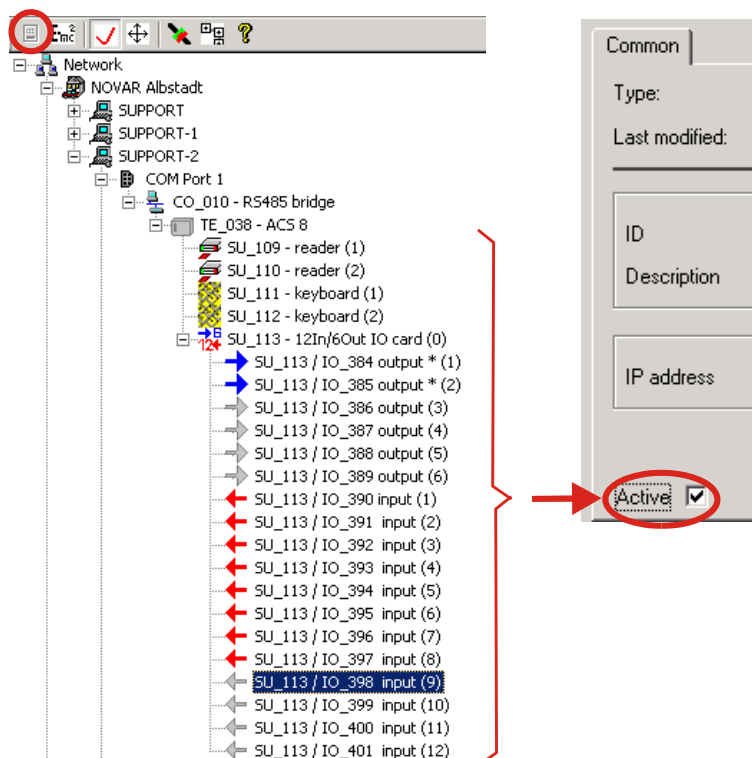
and this via function → **Insert** → **Controllers/Terminals** → **ACS-8**:



When selecting **One door/one reader**, **One door/two readers** or **Two doors**, (with ACS-8 additionally **three doors**, **four doors**), the automatic door configuration will be performed as described above (6.5.2.1, points 1 to 3). In addition, you can define whether keyboards are to be assigned as well.

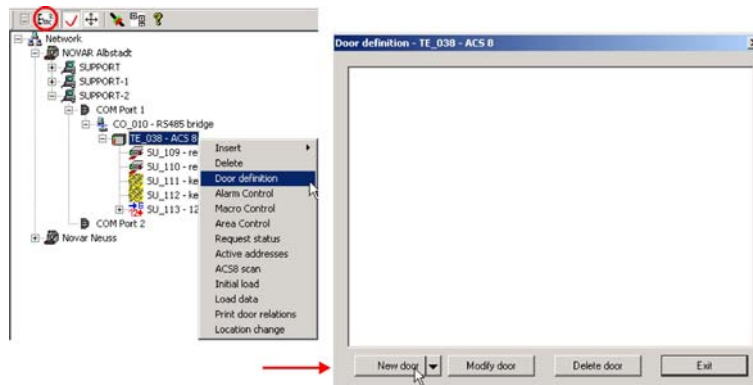
When selecting **Manual**, you will obtain the same result as shown under point 2a): Configuration of a controller/terminal **without** doors and **without** active components.

These must first be activated in the physical representation.

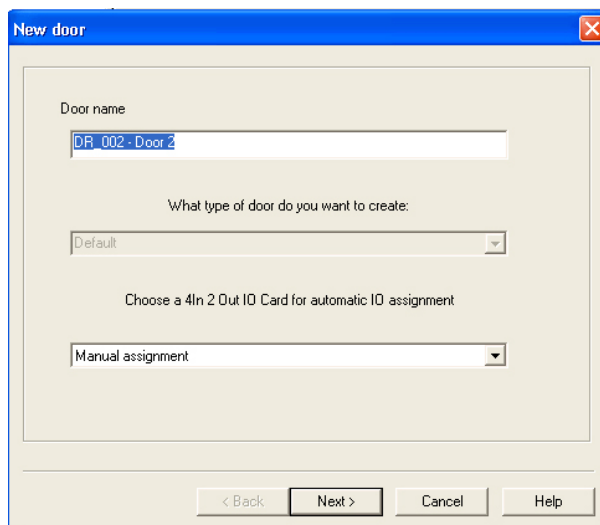


**Minimum requirement:** one reader or one keyboard, one door strike output (1), one door strike button input (2) and, if required, one door state contact input (5).

2. Change to logical representation. Right-click on the desired controller/terminal → Door definition. An empty window will open. Button → New door.

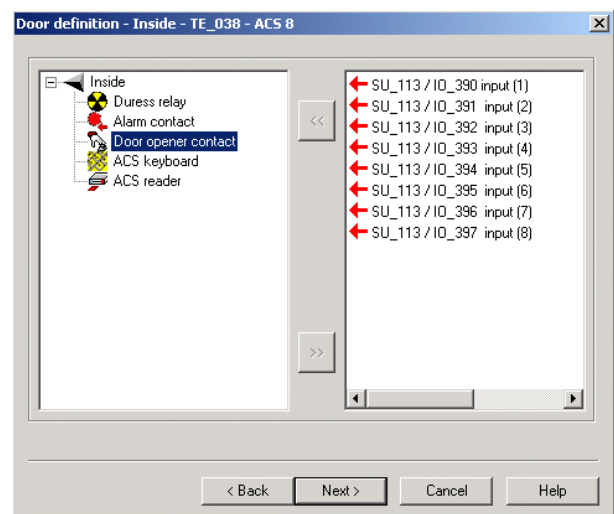


3. A standard door will be suggested. Its name can be modified.




Button **Next**.

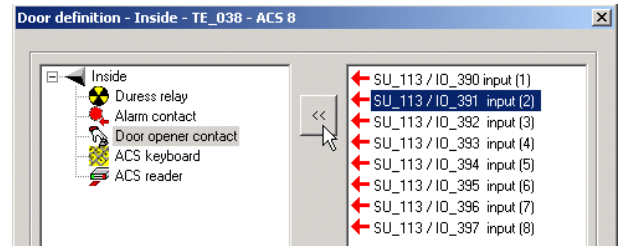
4. Define inside of the door<sup>15</sup>: In the left window, there is a list of all available components. By selecting a component to be used (e.g. door strike contact), the corresponding inputs, outputs, readers, keyboards etc. which were marked as **Active** in step 1 are displayed in the right window. A door strike contact is controlled via an **input**, therefore only the inputs marked as **Active** are offered for selection.



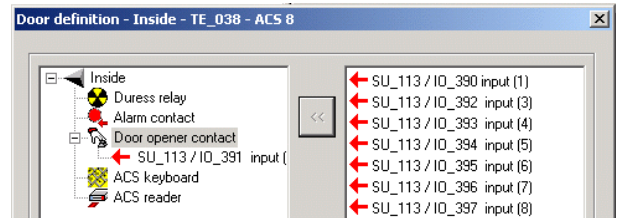
<sup>15</sup>

If you want to work only with the outside of the door, skip this screen with **Next** and execute the steps described for the outside of the door.

- By selecting the desired input and by clicking on button ...



.... the input is assigned to the door strike contact:



Alternative doors can be selected by clicking the arrow of **new door**.



The further procedure is similar to steps 4 and 5.



**Using the correct input:**

In principle, any input of a controller/terminal may be used provided that it has been marked as active before.

In the factory setting, the connections of the controllers/terminals are already predefined. We therefore recommend to stick to these default settings.

From the terminal allocation below, you can see why **Input 2** has been assigned in the example above.

*standard allocation*

upper terminal row	digital inputs	door strike key door 1 input 2	32	output 1	door rstrike relay door 1	47	output 2	door strike relay door 2	51	output 3	door strike relay door 3	53			
		door strike key door 3 input 1	31		door rstrike relay door 1	48		door strike relay door 2	50		door strike relay door 3	52			
	monitored inputs / inputs		monitoring contact door 1 input 5	36	relay voltage	0V *	46	n. o. c.	door strike relay door 2	51	c. c.	door strike relay door 3	54		
			monitoring contact door 2 input 7	39		+12V DC *	45		door strike relay door 2	52		door strike relay door 3	55		
	inputs 10		input 10	44	n. o. c.	door strike relay door 1	49	c. c.	door strike relay door 2	51	n. o. c.	door strike relay door 3	53		
			inputs 9			0V	43		door strike relay door 1	48		door strike relay door 2	50	door strike relay door 3	52
						input 9	42		door strike relay door 1	47		door strike relay door 2	49	door strike relay door 3	51
	inputs 8		monitoring contact door 4 input 8	41	n. o. c.	door rstrike relay door 1	47	c. c.	door strike relay door 2	51	n. o. c.	door strike relay door 3	53		
			inputs 7			0V	40		door rstrike relay door 1	48		door strike relay door 2	50	door strike relay door 3	52
						monitoring contact door 3 input 6	38		door rstrike relay door 1	49		door strike relay door 2	51	door strike relay door 3	53
						monitoring contact door 2 input 7	39		door rstrike relay door 1	50		door strike relay door 2	52	door strike relay door 3	54
	inputs 6		0V	37	n. o. c.	door rstrike relay door 1	47	c. c.	door strike relay door 2	51	n. o. c.	door strike relay door 3	53		
			monitoring contact door 1 input 5	36		door rstrike relay door 1	48		door strike relay door 2	50		door strike relay door 3	52		
	inputs 5		door strike key door 2 input 4	35	n. o. c.	door rstrike relay door 1	47	c. c.	door strike relay door 2	51	n. o. c.	door strike relay door 3	53		
			door strike key door 4 input 3	34		door rstrike relay door 1	48		door strike relay door 2	50		door strike relay door 3	52		
0V			33	door rstrike relay door 1		49	door strike relay door 2		51	door strike relay door 3		53			
inputs 4		not allocated	30	n. o. c.	door rstrike relay door 1	47	c. c.	door strike relay door 2	51	n. o. c.	door strike relay door 3	53			
		not allocated	29		door rstrike relay door 1	48		door strike relay door 2	50		door strike relay door 3	52			
		not allocated	28		door rstrike relay door 1	49		door strike relay door 2	51		door strike relay door 3	53			

*standard allocation*

lower terminal row	Host-interface	0V-Host-interface	1	output 5	threat	24	output 4	door strike relay door 4	27
		Data	2		output 5	25		door strike relay door 4	28
		Data*	3		door strike relay door 4	29			
	keypad 1	serial keypad 1	6	output 4	door strike relay door 4	26	output 3	door strike relay door 4	30
		0V	7		door strike relay door 4	27		door strike relay door 4	31
		0V	8		door strike relay door 4	28		door strike relay door 4	32
	reader 1	LED red 1	9	output 4	door strike relay door 4	29	output 2	door strike relay door 4	33
		LED yellow 1	10		door strike relay door 4	30		door strike relay door 4	34
		LED green 1	11		door strike relay door 4	31		door strike relay door 4	35
	keypad 2	Clock 1	12	output 4	door strike relay door 4	32	output 1	door strike relay door 4	36
		Data 1	13		door strike relay door 4	33		door strike relay door 4	37
		+12V DC (max. 400mA)	14		door strike relay door 4	34		door strike relay door 4	38
	reader 2	0V	15	output 4	door strike relay door 4	35	output 2	door strike relay door 4	39
		serial keypad 2	16		door strike relay door 4	36		door strike relay door 4	40
		0V	17		door strike relay door 4	37		door strike relay door 4	41
keypad 2	LED red 2	18	output 4	door strike relay door 4	38	output 1	door strike relay door 4	42	
	LED yellow 2	19		door strike relay door 4	39		door strike relay door 4	43	
	LED green 2	20		door strike relay door 4	40		door strike relay door 4	44	
reader 2	Clock 2	21	output 4	door strike relay door 4	41	output 2	door strike relay door 4	45	
	Data 2	22		door strike relay door 4	42		door strike relay door 4	46	
	+12V DC (max. 400mA)	23		door strike relay door 4	43		door strike relay door 4	47	
keypad 1	0V	24	output 4	door strike relay door 4	44	output 1	door strike relay door 4	48	
	serial keypad 1	25		door strike relay door 4	45		door strike relay door 4	49	
	0V	26		door strike relay door 4	46		door strike relay door 4	50	
Host-interface	Data 1*	27	output 4	door strike relay door 4	47	output 2	door strike relay door 4	51	
	Data 1	28		door strike relay door 4	48		door strike relay door 4	52	
	Data*	29		door strike relay door 4	49		door strike relay door 4	53	

inputs 11 and 12  
(= ST10 on board)

input 12 (MI8)	3
0V	2
input 11 (MI7)	1

input 6 (= ST5 on board)

output 6	3
WD 0	2
0V	1

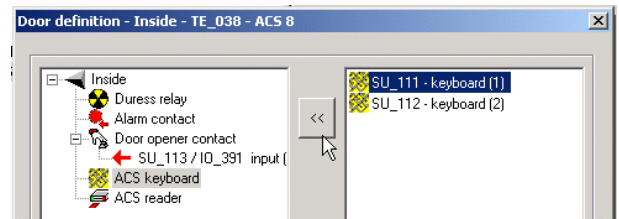
signals see table in chapter 16.3



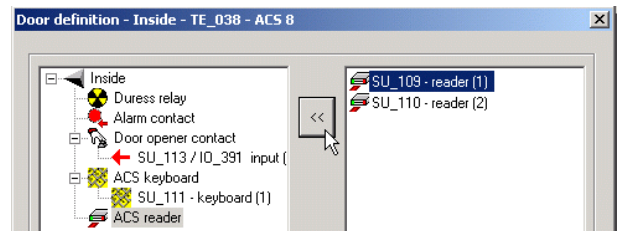
Readers/keypads for door 3 and door 4 are to be connected to the module bus in RS-485 mode.



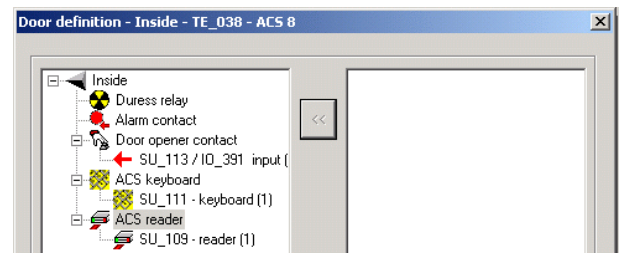
6. Assign keyboard:  
Right-click on the keyboard → select the keyboard to be used → button <<<.



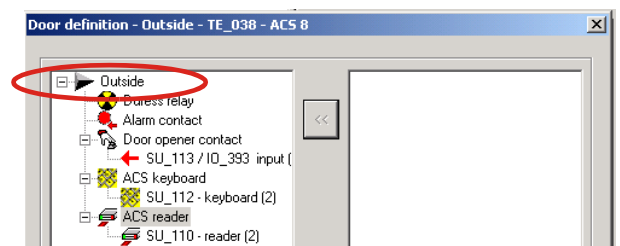
7. Assign reader:  
Right-click on the reader → select the reader to be used → button <<<.



8. If required, all components used on the door side concerned can be defined in the way described above.  
Button → **Next**

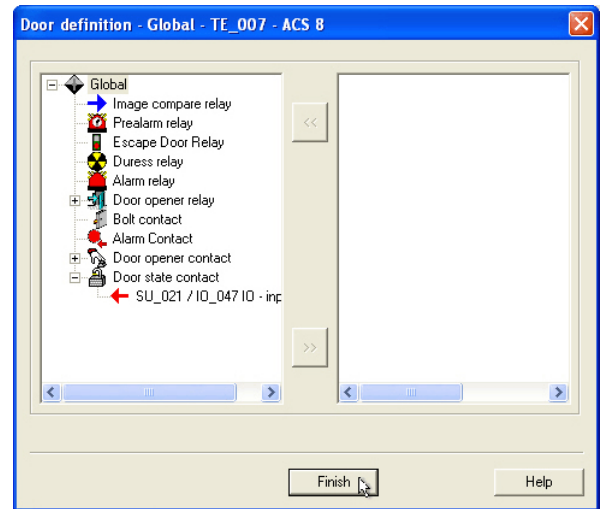


9. Define outside of the door:  
Repeat steps 4 - 8 for the outside of the door.



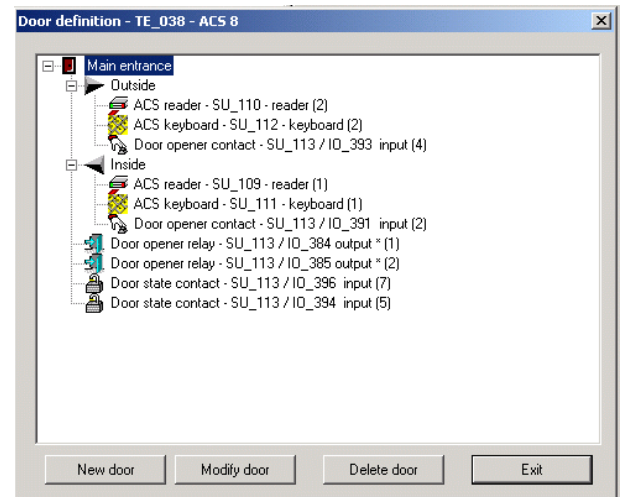
10. Global definitions:  
Define the components which are used by **both** sides of the door as described above (e.g. door strike relay, door state contact).

Button → **Finish**



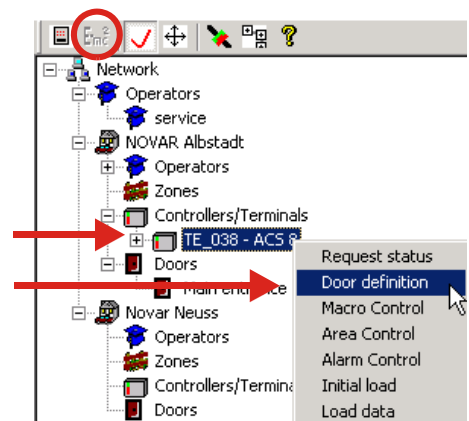
11. Representation of the door selected with all components:

If all settings are correct, click on → **Exit**. If not, click on → **Modify door** (see next section).



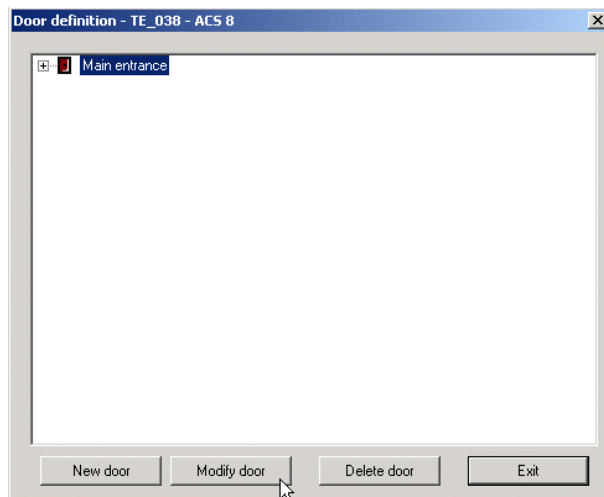
### Modify door

- a) If you notice in the screen above that the door that has just been configured still requires certain modifications, you can do this directly via the **Modify door** button.
- b) Modify an existing door:
1. Change to logical representation.
  2. Right-click on the controller/ terminal that controls the door to be modified.
  3. Door definition



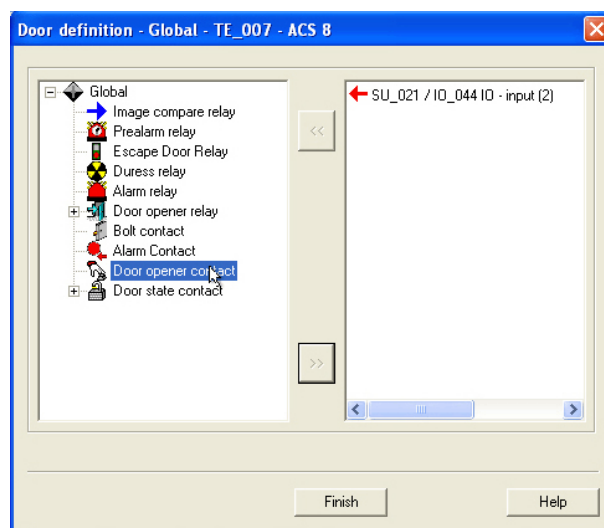
4. Select the door to be modified (for an ACS-8, a maximum of 8 doors can be displayed here).

5. Modify door.

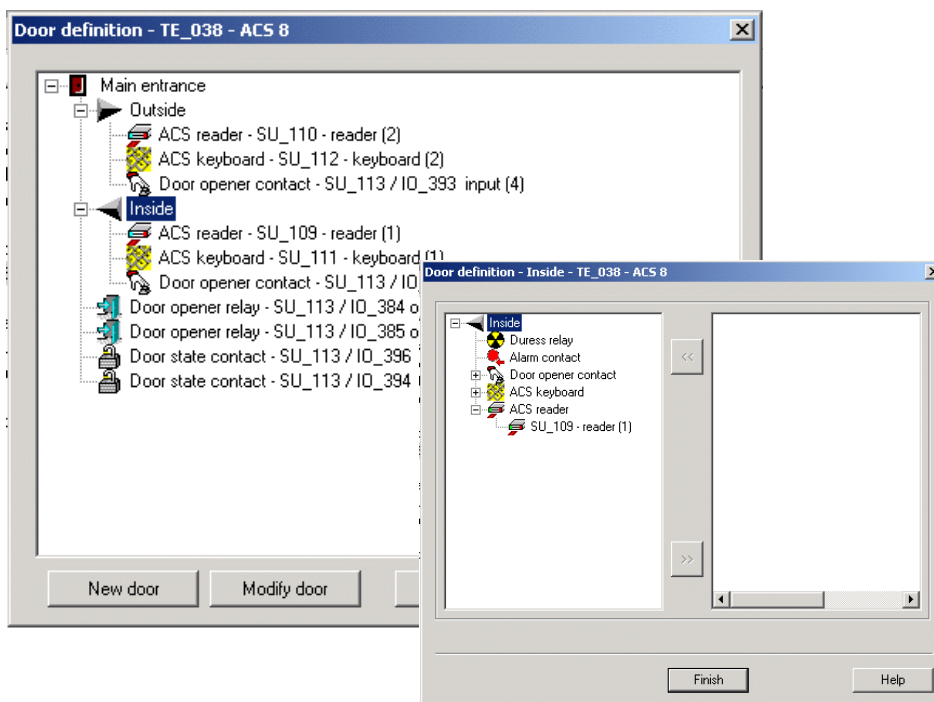


6. Select the desired component under **Global** in the left window. Select the input / output to be assigned in the right window and assign it with **⇐**. Remove an input/output which is not desired accordingly with **⇒**.

7. Finish.



8. Proceed accordingly on the **Inside** and the **Outside**. Select the desired side and → Modify door.



9. When the modification is completed → Finish.

### 6.5.2.2 Module bus doors

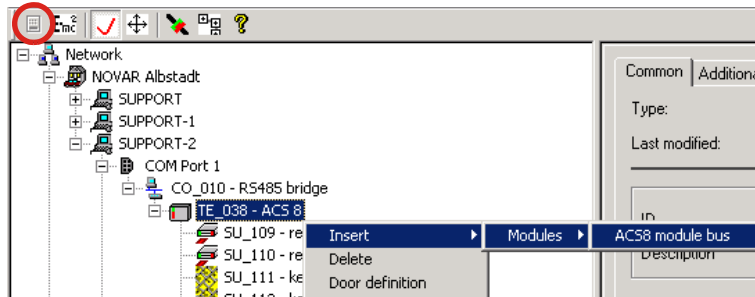


Only possible with **ACS-8** with integrated → **Communication module**.

Module bus door may be connected either to a → **Door module** or to a → **I/O module**.

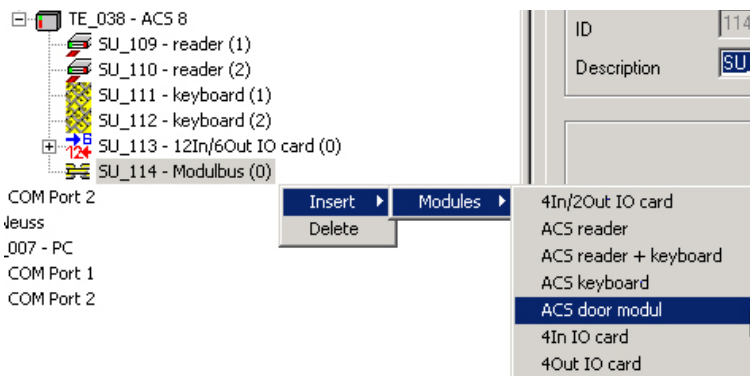
Insert module bus :

Physical representation → right-click on the ACS-8 controlling the door module → Insert → Modules → ACS-8 module bus.



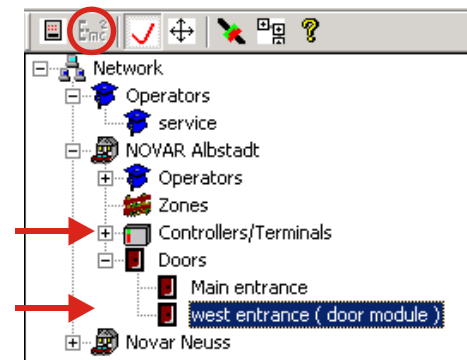
a) Insert module:

1. Right-click on the module bus to which the door module is connected → Insert → Modules → ACS-8 door module.



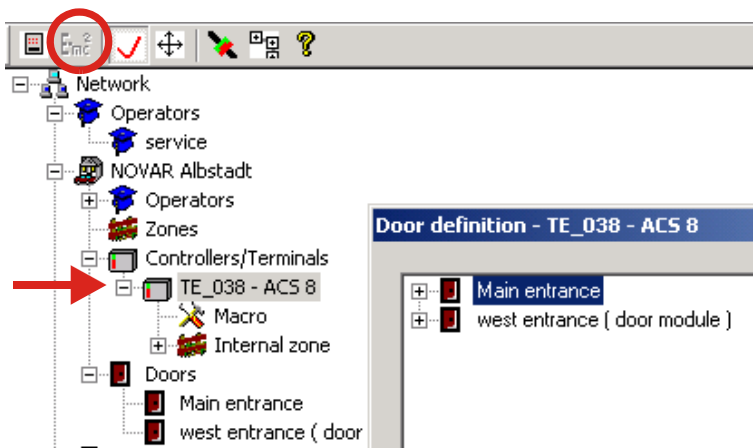
2. Assign unambiguous name and select **Active**.

3. In the → logical representation, the door module does not appear. The door(s) controlled by the door module is assigned to the ACS-8 controlling the door module. Assign an unambiguous name to the door.



4. Define door:  
 Depending on the default setting in → **Location** → **tab ACSx**,
  - one door with one reader
  - one door with two readers
  - two doors with one reader each
  - no door (manual configuration)
 is defined when a door module is inserted.

Logical representation → right-click on the ACS-8 concerned → Door definition



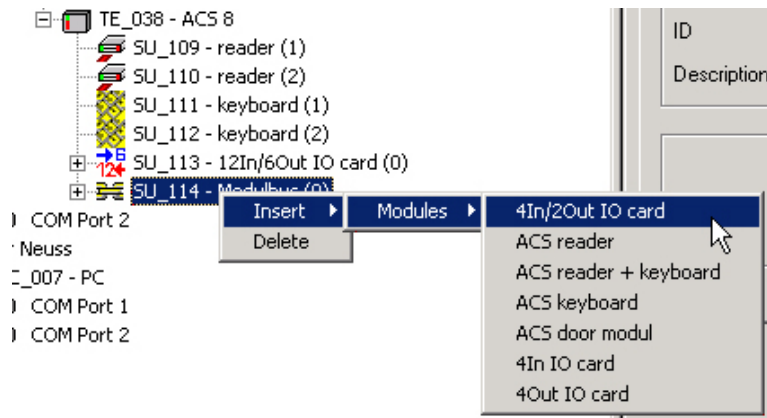
The door definition or modification is carried out in the same way as for the onboard doors (see Chapter 6.5.2.1).



Please note that the inputs, outputs, readers and keyboards of the door module have their own numbering according to the terminal allocation below: Further information according to the numbering of the terminals see mounting- and installation instructions of the door module.

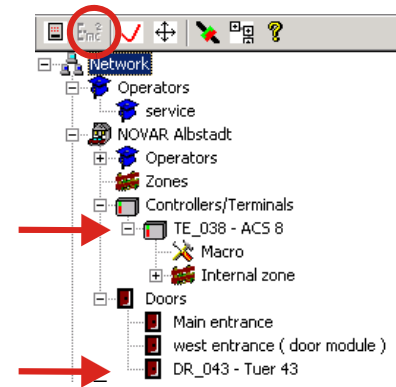
b) Insert I/O module:

1. Right-click on the module bus to which the I/O module is connected → Insert → Modules → 4In/2Out IO card



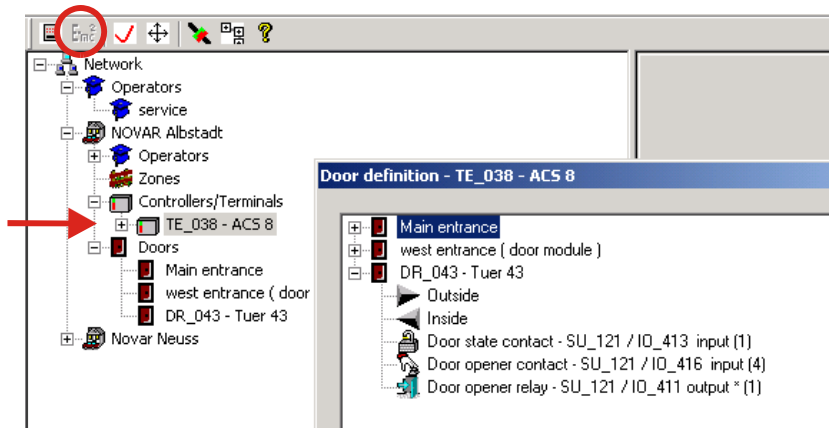
2. Assign unambiguous name and select **Active**.

3. In the → logical representation, the I/O module does not appear. The door controlled by the I/O module is assigned to the ACS-8 controlling the I/O module. Assign an unambiguous name to the door.



4. Define door:  
Depending on the default setting in → **Location** → **tab ACSx**, a door is configured automatically or not when an I/O module is inserted.

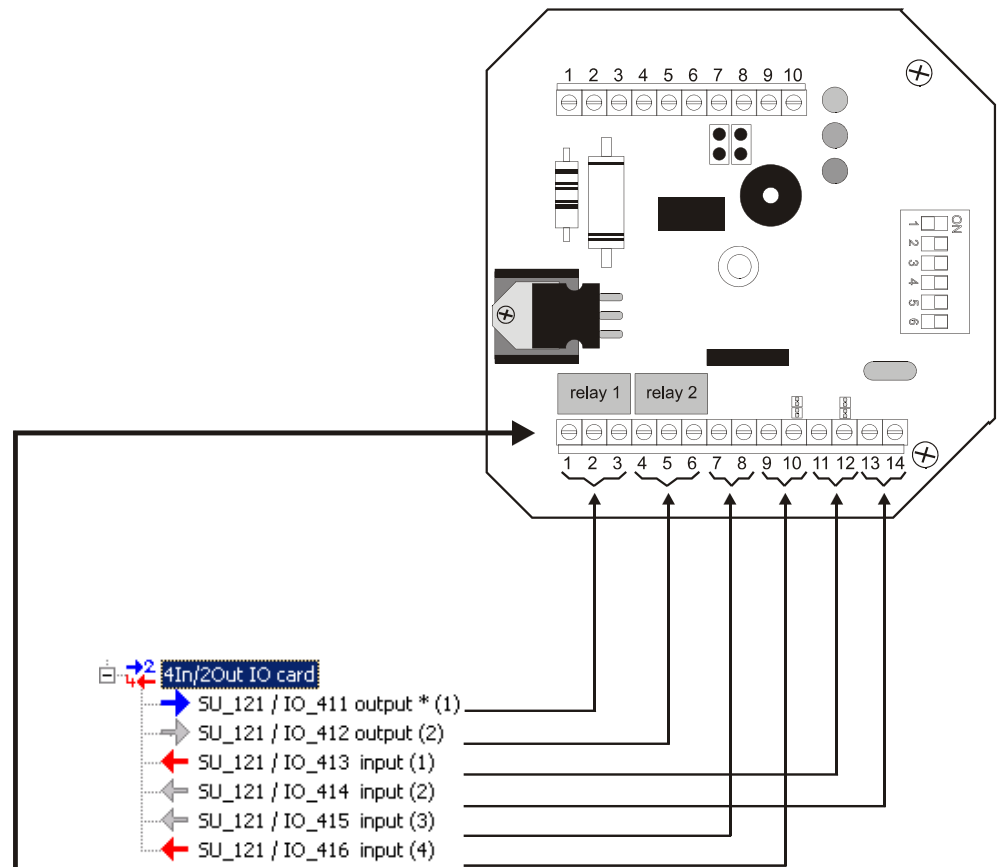
Logical representation → right-click on the ACS-8 concerned → Door definition



The door definition or modification is carried out in the same way as for the onboard doors (see Chapter 6.5.2.1).



Please note that the inputs and outputs of the I/O module have their own numbering according to the terminal allocation below:



terminal	designation			factory settings*
1	n/c contact 1			
2	common 1	output 1	relay 1	door strike
3	n/o contact 1			
4	n/c contact 2			
5	common 2	output 2	relay 2	alarm
6	n/o contact 2			
7	Anode (+)	input 3 isolated	opto-isolator 1	free
8	Cathode (-)	input 4 isolated	opto-isolator 2	exit switch
9	Anode (+)			
10	Cathode (-)			
11	Differential alarm line 1	input 1 (programmable)		monitoring contact
12	0V			
13	Differential alarm line 2	input 2 (programmable)		available for use..
14	0V			e.g. glass breakage detectors, intrusion detection systems.
15	Unused	not connected		
16	Unused			

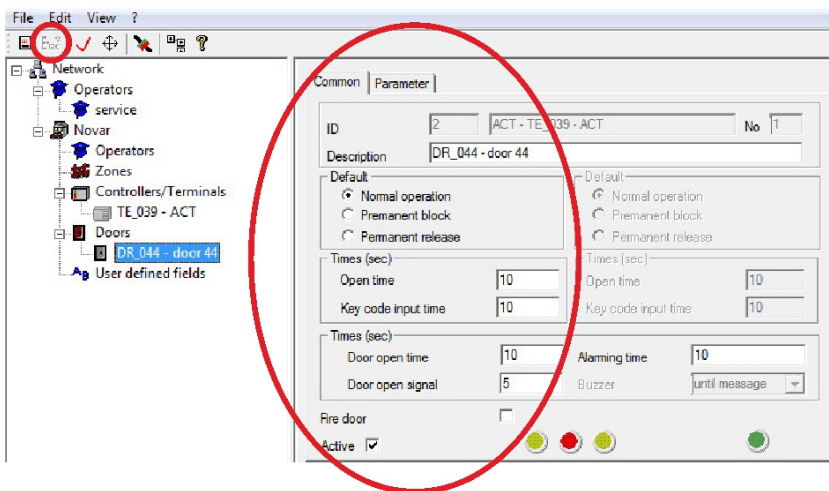
\* The functions can be defined individually in NetEdit.

Readers and keyboards are to be connected directly to the RS-485 bus.



### 6.5.3 ACT

As a standard, an ACT can control **one** door side. Consequently, **one** door with **one** reader/keyboard is set up automatically when an ACT is inserted. Further measures are **not** required. If necessary, check the entries in the → **tabs** of the individual door.



only one door side active

### 6.5.4 AXS4Secure

An AXS4Secure access control terminal can manage a maximum of 2 doors with one entry reader and one exit reader, which are connected onboard.

#### 6.5.4.1 Scan Onboard Doors

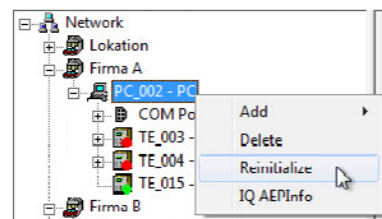


The AXS4Secure license on the AXS4Secure terminal determines how many onboard doors are defined (one or two doors). The two types of licenses differ only in the number of doors that can be managed.

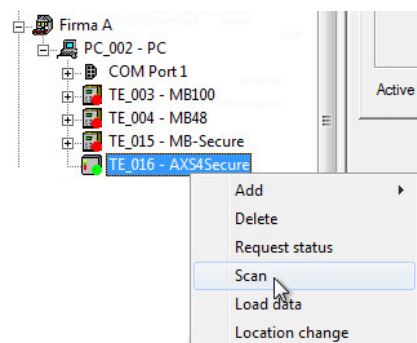
- Door system:
- One door with one reader
  - One door with two readers
  - Two doors with one reader each
  - Two doors with two readers each

Right-click the workstation to which the terminal was added → **Reinitialize**.

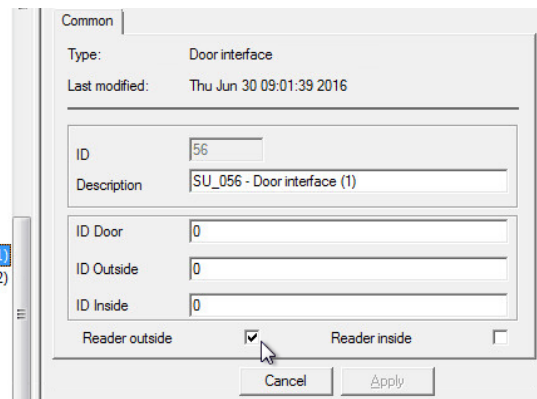
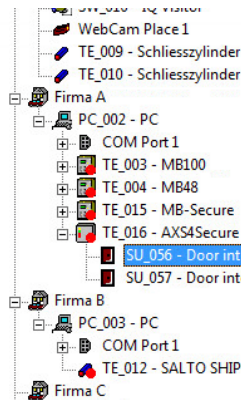
When the connection is successfully made a green dot appears next to the concerned terminal.



For an existing connection that is functional, right-click the concerned terminal and choose → **Scan**. All door interfaces found (doors and installed readers) are automatically set up in IQ NetEdit.

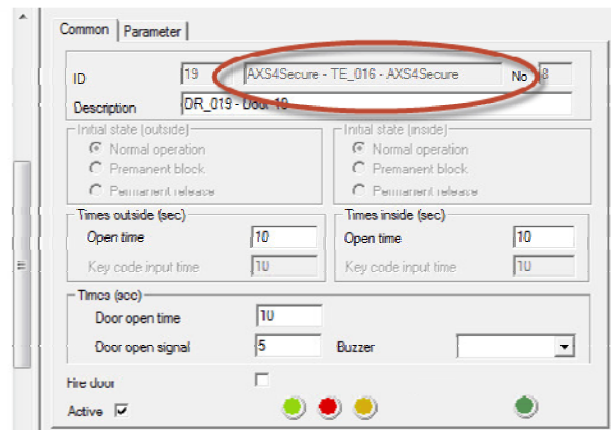
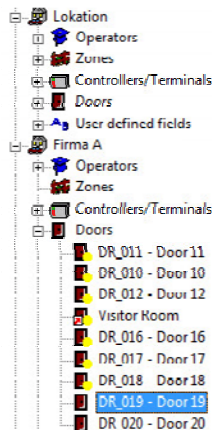


Deactivate non-existent readers (→ **Reader outside / Reader inside**) after the scan process!  
Readers that are programmed but not in the system trigger a tamper alarm.



Door data:

After scanning there are doors in IQ NetEdit with the designation DR\_xx = door interfaces with appropriate numbering.

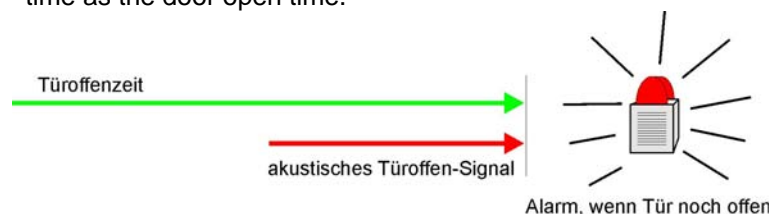


Check / set each doorr:

Times (outside/inside): Definition of times for individual timers, some separated according to the door sides.

- Open time: Activation time of the door strike. During this time the door can be opened.
- Key code input time: Within this time the key code (→ PIN or → door code) must be typed in. If the code is not entered completely after this time has expired, the completely entry must be repeated.
- Door open time: Maximum time a door is allowed to be open. It starts when the monitoring contact indicates the actual opening of the door. After expiration of this time an alarm will be triggered (Door opened too long).
- Door open signal: If a reader is equipped with an internal buzzer, it indicates on the beginning of the door open signal time that the door should be closed as otherwise the → **door open time** expires which causes an alarm (Door opened too long).

The door open signal time is part of the → **Door open time**. The time for the door open signal should always be shorter than the door open time in order to remain enough time for closing the door. The door open signal time ends at the same time as the door open time.



Operation mode (outside / inside):

For each door side there can be defined a type of identification required for entry:

- Data carrier only
- PIN only
- PIN and Data carrier
- PIN or Data carrier
- No Timecheck
- Access inhibited
- Door code only
- Door code and data carrier
- Door code or data carrier

There is always one criterion to be valid for one operation mode:

- Normal operation: The selected access criterion is valid for the door being in **normal operation**.
- Automatic operation: The selected access criterion is valid while the door is set to **automatic operation**. Automatic operation can be used to set the door to permanent release / permanent block at predefined times (examples see user manual).

## 6.5.5 Doors with locking cylinders

IQMA version 10 or higher and IQSC version 4 or higher can handle authorizations of offline cylinders and door fittings as well as of online (RF) cylinders / door fittings.

### 6.5.5.1 General description

Supported cylinders see product catalogue. IQ MultiAccess deals identically with all supported cylinder types.

The data transfer between IQ MultiAccess / IQ SystemControl and the offline doors (cylinders) happens via laptop/netbook and IrDA-USB adaptor (022909) or Palm-PDA. With online (RF) cylinders / door fittings only the initial initialization is done via laptop/netbook and IrDA-USB adaptor (022909) or PALM-PDA, after that the data will be exchanged online (via radio). Supported PDAs and their preconditions / requirements see original manual of the PDA-software XS-Manager. This can be found in PDF-format<sup>16</sup> on the installation CD of IQ MultiAccess in the directory ....\XS-Manager x.x\Dokumentation.

Mounting and assembly of the cylinders / door fittings according to their original manuals.

Installation of PDA and the workstation, the PDA is to communicate, according to original manuals of the PDA. The software **IQ Cylinder** must be installed on this workstation. This is part of IQ MultiAccess (installation see chapter 3). If IQ MultiAccess has been already installed, the component **IQ Cylinder** must be added (see chapter 3.3.3 and 3.3.3.1). On the PDA the software **XS-Manager for PDA** must be installed. Should a mobile PC laptop / netbook with IrDA-USB adaptor (022909) be used for initialization, the software **XS-Manager for PC** and the software **IQ Cylinder** must be installed first. The connection of this PC (as workstation) to IQ Server is made via a client-server installation over a network. See chapter 3.1.2. Driver installation for the IrDA-USB adaptor according to original manuals (CD) of the adaptor. Furthermore, in several parts we refer to the user manual of the XS-Manager. This can be found in PDF-format<sup>14</sup> on the installation CD of IQ MultiAccess in the directory ....Doc\XS-Manager

<sup>16</sup>

Reading requires a program that can open PDF-files, e. g. Adobe Acrobat Reader.



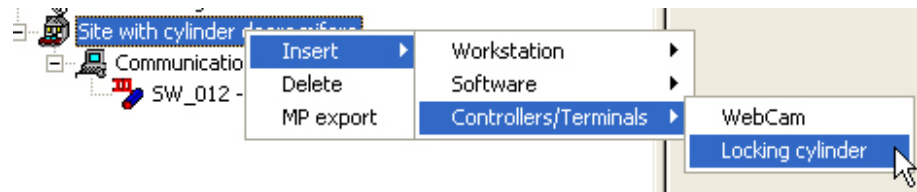
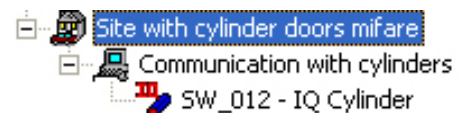
The communication between PDA and PC can cause some problems with USB interfaces < 2.0. In that case the PDA software and IQ Cylinder can be installed on an other workstation. Then, in addition to user and password the server name (name of the workstation the software IQ Server is running) must be entered when starting IQ Cylinder. Alternatively, the software IQ Cylinder can be allocated directly to a location. When starting IQ Cylinder user, password and server identification must be entered in that case (cf. chapters 6.2.2 and 11).



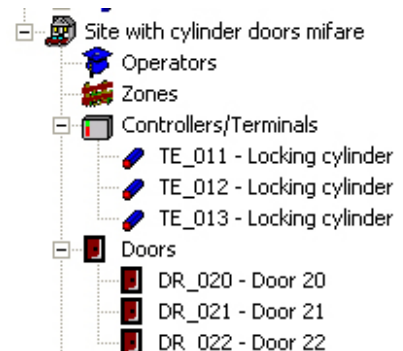
The computer IQ Cylinder is to be installed, requires **.net Framework 2.0** or higher. This can be installed via a Microsoft Update, but it is also on the IQMA installation CD and will automatically be installed together with IQ Cylinder, if it does not already exist on the computer.

### 6.5.5.2 Offline cylinder / fitting

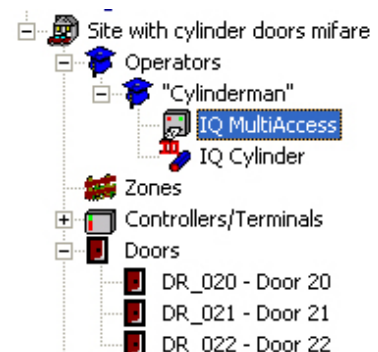
1. Create a workstation the communication to the PDA shall be done (if necessary as a separate location).
2. Insert the sSoftware **IQ Cylinder** at the corresponding workstation.
3. Insert the locking cylinders. They can only be assigned to a location. There is no distinction between the different cylinder types. IQ NetEdit handles them all in the same way.



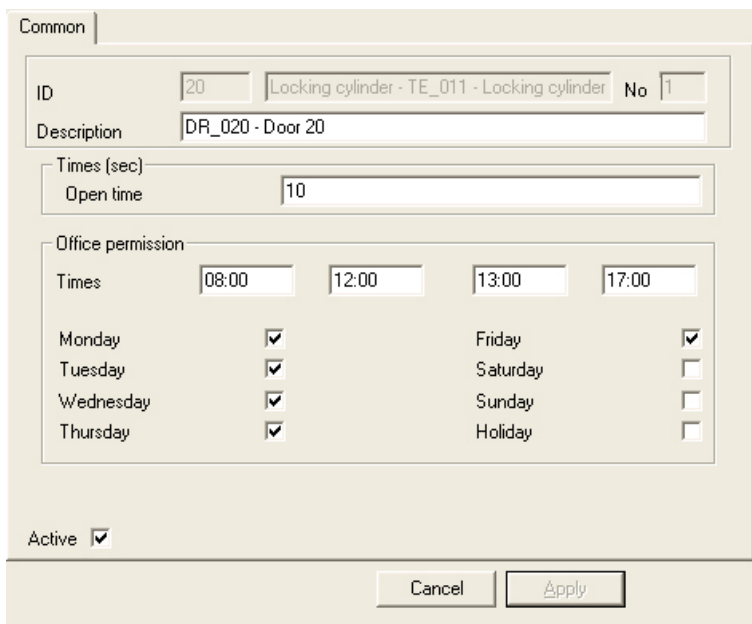
In the logical view the locking cylinders are displayed as controllers. Automatically one door results of one locking cylinder.



4. Create an operator, who runs the data transfer with rights in IQ Cylinder and IQ MultiAccess.



Possible settings for each door: Designation, open time and office permission.



Via the **office permission** function the doors can be switched to a mode to be opened without data carrier within defined days / times. This condition can be reset manually. It ends automatically with achievement of the end time. There can be defined two time ranges (from - to), within a person with appropriate authorizations can switch the door to be entered freely. The time ranges are valid on the activated days. The times and days can also be defined by a user in IQ MultiAccess.

The office permission function is assigned to a person (a data carrier) in IQ MultiAccess.



- 5a. **Use of a PDA**  
First start the software IQ Cylinder, then connect the PDA via a USB cable with the PC and start the HotSync operation on the PDA. The communication between the PDA and the computer is displayed by a corresponding window of the communication software (for details refer to the original manuals of PDA).



- 5b. **Use of a laptop / netbook**  
The laptop/netbook must be in the same network of IQ Server. First start the software IQ Cylinder, then start XS-Manager and synchronize the data. For details refer to the original manual of XS-Manager.

6. For each door / cylinder:  
Start the program → **XS-Manager** on the PDA or laptop / netbook.  
Activate the cylinder by turning<sup>15</sup>.  
Align the infrared interface of the PDAs or laptop / netbook with IrDA-USB adapter (022909) to the locking cylinder.  
The communication will be established. On the initial startup of the cylinder with **XS-Manager** the cylinder must first get initialized (as long as, all other functions are not active).

Via the operation described in step 5, the software **XS-Manager** knows the doors. Each individual locking cylinder must once be initialized with its individual door data. This happens via the **initialization** function within the software **XS-Manager**. At this, a door newly created in IQ NetEdit will be allocated to a certain locking cylinder.

**Details on initialization, PIN allocation and communication between cylinder and XS-Manager see user manual XS-Manager.**



We recommend to change the (two different!) synchronization and initialization PINs set by default according to customer's wishes and store these information at a safe place.

**Important!      The initialization PIN is required to open the case in order to change the batteries!**

The XS-Manager settings should be done in a way a PIN is mandatory for synchronization and initialization, as otherwise any PDA or laptop would be able to control the cylinders. It is recommended to use the same synchronization PIN for all cylinders within one access control system.

---

<sup>15</sup>

The activation may be different depending on the cylinder type. Details see manual of the individual cylinder.

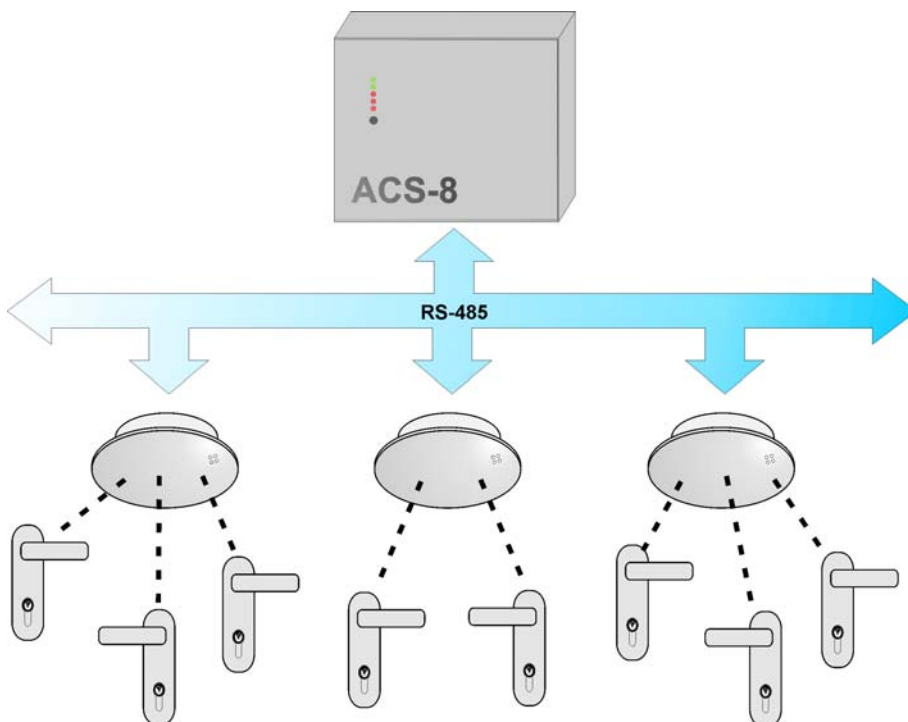
### 6.5.5.3 Online cylinders / fittings via traffic point RS485

#### 1. Connection to the AC-System via IQMA

**Precondition:** ACS-8 with Firmware V8.xx (Firmwareupdate see chapter 5.11).

**Installations scheme:** Up to 8 traffic points RS-485 can be inserted to the module bus of an ACS-8. One traffic point can control up to 8 DLC/DLF in perimeter of up to 10 m<sup>16</sup> via radio.

**Restriction:** The maximum number of 8 doors per ACS-8 must not be exceeded.

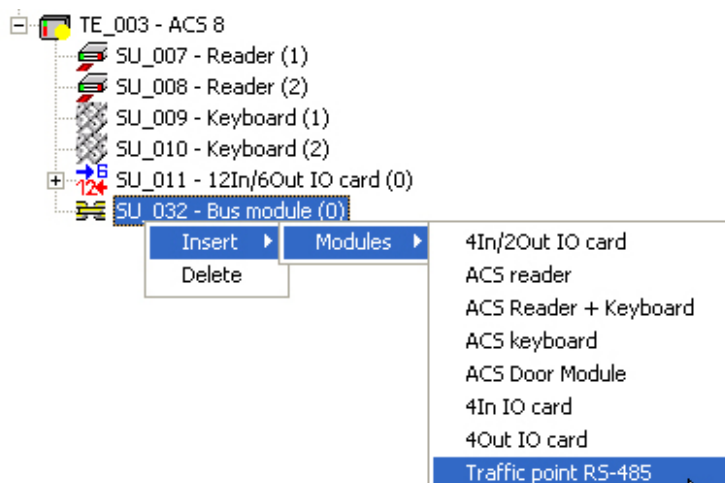


#### Mounting and Installation

of the RF cylinder / door fittings and the traffic point(s) RS-485 according to their manuals.

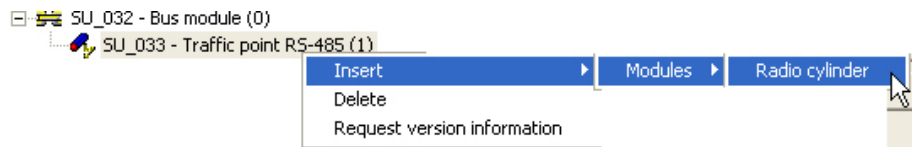
#### Setup in IQ NetEdit

Right-click the ACS-8-Module bus to Insert an traffic point RS-485



- Common tab:** Input of a unique description and the address which is set in the Traffic point via DIP switch.
- RF parameters tab:** **Radio-ID** is automatically set by system. It is used for unambiguous identification of the RF cylinder.
- Frequency:** Adjustment of the frequency range used for radio transmission. The frequency band 4 only is harmonised Europe-wide. Do not change this default setting!
- Timeout:** Time in seconds, within the door fitting / cylinder expects a response of the RF-module after reading a data carrier (datacarrier authorized / not authorized). If no answer is received after expiration of this time period, the fitting / cylinder will interpret this as "Data carrier not authorized". Default setting = 2 seconds.

Insert RF fittings / cylinders to the traffic point RS485 (right-click).



All tab entries (except the description) will automatically be done by the system. No input necessary.

Automatically a reader and a door strike relay (output) will be assigned to the RF-module.

The reader type will be taken over from the local settings and can/must be modified/adapted if necessary.

The door view displays one door per each inserted door fitting / cylinder. The tabs provide all setup possibilities of a standard door as via the manual door configuration in addition to the default settings all (hard wired) components such as keypad, exit reader monitoring contact etc. can be defined.

After the door definition each door fitting / cylinder must be initialised.

Preconditions and procedure are similar to the offline cylinders cf. Installation Instructions (P32205-26-0G0-xx), chapter 6.5.4, User Manual (P32205-20-0G0-xx) chapter 21.2 and user manual XS-Manager (as PDF-file on the installation CD of IQMA/IQSC in the directory .....Doc\XS-Manager<sup>17</sup>).

In opposite to the offline cylinders the online fittings / cylinders work after successful initialisation like hard wired doors.

## 2. Connection to the intruder alarm control panel via IQSC

Definition of the fittings / door cylinders at the IACP is done according to the manuals of the MBxx / WINFEM.

### Setup in IQ NetEdit

With an initial connection of an intruder alarm control panel the connected hardware, master files and texts will be transferred (cf chapter 15).

Subsequent installation of Rf cylinders / door fittings:

Insert a switching device at the concerning IACP according to chapter 15.3, step 8. Select **IK3** in the fields **Type**.

RF fittings / cylinders are handled like standard IACP doors in IQSC (cf. chapter 15).



## 6.5.6 Connectivity to SALTO Ship System - Doors with cylinders/door fittings

Starting v13 and the corresponding licensing, IQMA administers off-line cylinders/door fittings in the SALTO virtual network (SVN). This is a wireless network access control system. The ID card serves both as identification for individuals and as a data transfer medium for access information and other information.

### 6.5.6.1 General description

For supported cylinders/door fittings, see the product catalog. IQ MultiAccess handles all supported cylinder types and door fittings identically.

The "RW Pro-Access" setup program must be used to set up the basic configuration (see 6.5.5.2). Next, data regarding door groups as well as assigned door data (for cylinders/door fittings) is transferred from IQ MultiAccess.

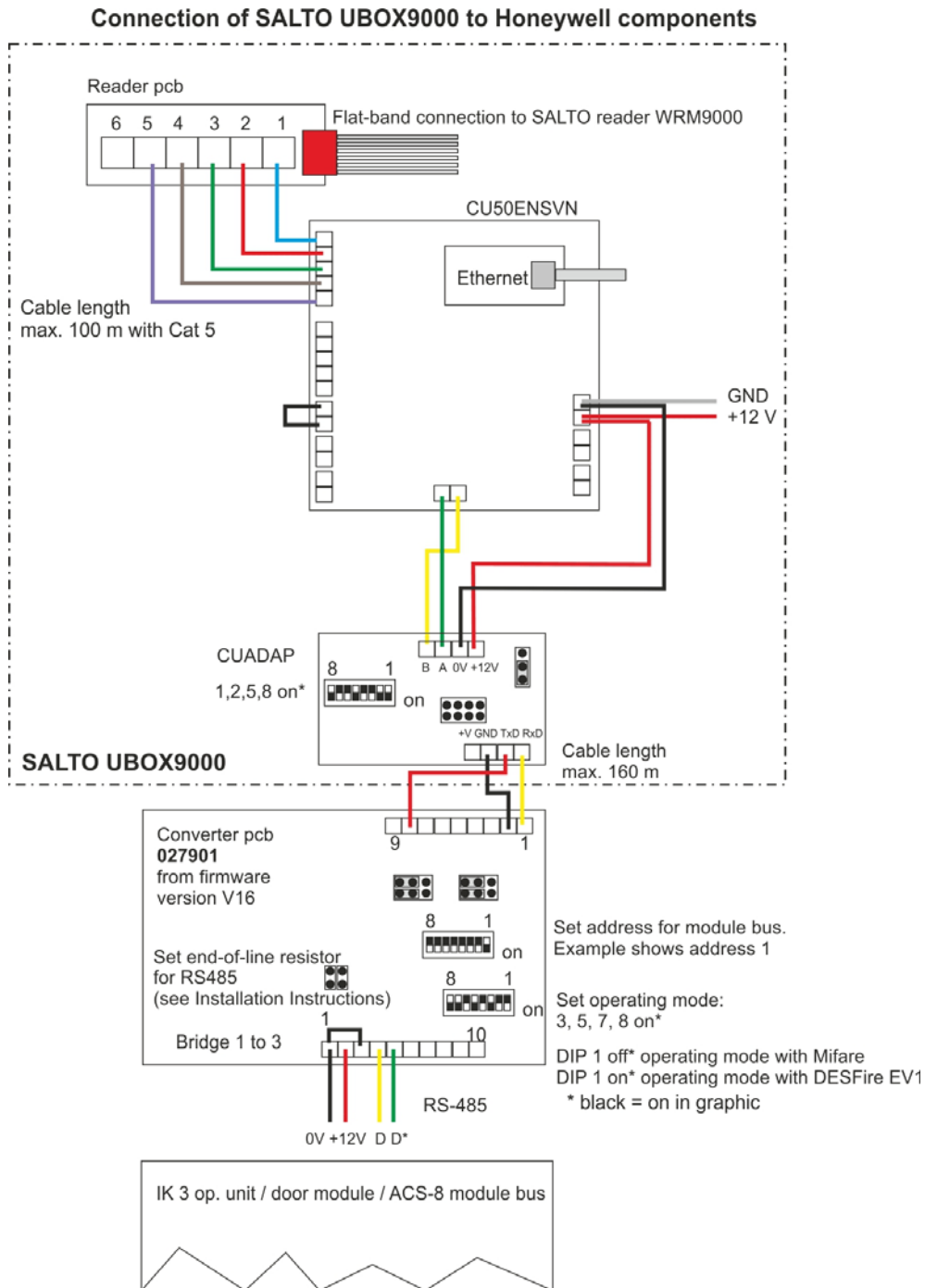
The preliminary initialization of cylinders/door fittings is carried out via a portable SALTO programming device (PPD). Thereafter, data is simply exchanged with the ID card during actual system operation. The data includes information about blocked ID cards (blacklists), events and the battery status of cylinders/door fittings. Access authorizations are stored on ID cards and not in door components. A SALTO wall reader (such as the CU 50) must be installed as a reader at the entrance to the property or at a central site on the property for updates of access authorizations on ID cards, synchronization of event data and distribution of the blacklist. The blacklist contains ID card information, for example names of individuals who have been provided new ID cards, or ID cards/individuals who no longer have access to the site. If ID cards whose access authorizations have been revoked on the basis of the blacklists distributed are reactivated, a SALTO coding device (Key Encoder) is required to be used. Since the blacklist is distributed when the ID card is used, there may be a time lag between the occurrence of an event and its notification to all cylinders/door fittings. This system does not therefore replicate the advantages of an online system.

For requirements and procedures, see the original SALTO Ship system documentation.

Assembly of cylinder/fitting in accordance with original documentation.

Install IQ MultiAccess and the SALTO service. The "RW Pro-Access" software must also be installed on the computer so that the base configuration can be generated. Install the SALTO Service on the same computer as the IQ Server. We recommend the use of the Ethernet SALTO coding device (Key encoder), since this can be linked in at any point in the network. The SALTO coding device is a must, since it is only through this device that card data can be updated and blacklist entries revoked. The SALTO coding device must have been associated with the SALTO service via a network installation. More information on the installation and registration of your SALTO Ship (SVN) system in conjunction with IQ MultiAccess can be found on the Internet at: [www.spsupport.de/Honeywell\\_IQ.zip](http://www.spsupport.de/Honeywell_IQ.zip)

The wiring diagram shows the connection of the SALTO Ship system to Honeywell components:



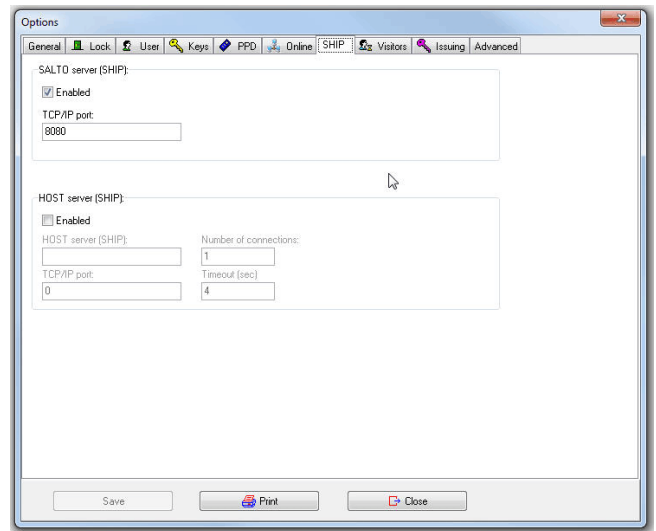
### 6.5.6.2 Configuration of SALTO Ship (SVN) off-line cylinder/door fitting

After installation of the hardware and software, the SALTO system must be configured for cylinders/door fittings and the corresponding doors must be assigned. To do this, launch the “RW Pro-Access” software on your PC.

Click on the “SHIP” tab under “Extras / Configuration / General Options”.

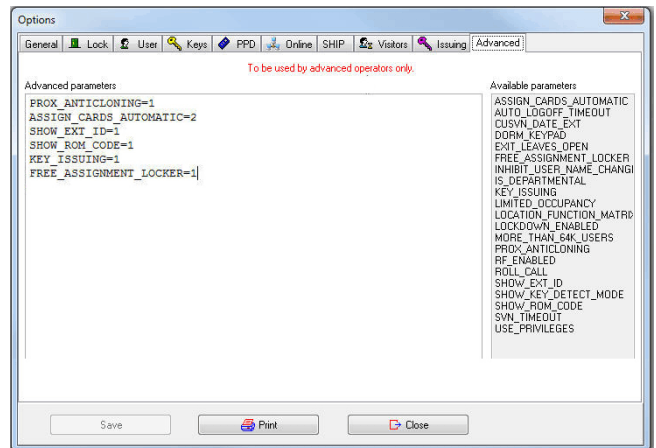
Enable SALTO SHIP Server in this tab. Specify a **free port** as the TCP/IP port.

Save the changes by pressing “Save”.



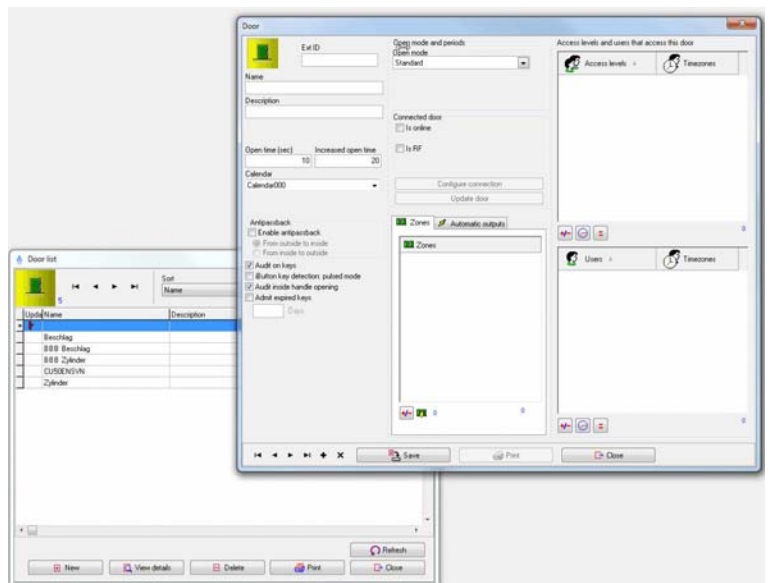
Review the following entries in the input field “Advanced Parameters” in the “Advanced” tab and add entries if need be.

Save the changes by pressing “Save”.



Bring up the “Doors” menu.

Add cylinders/door fittings. A new cylinder/door fitting can be defined by clicking on “[x] New”. There is no difference between a cylinder and a door fitting in this input screen. A name and description can also be entered for each cylinder/door fitting.



Now bring up the “Zones” menu.

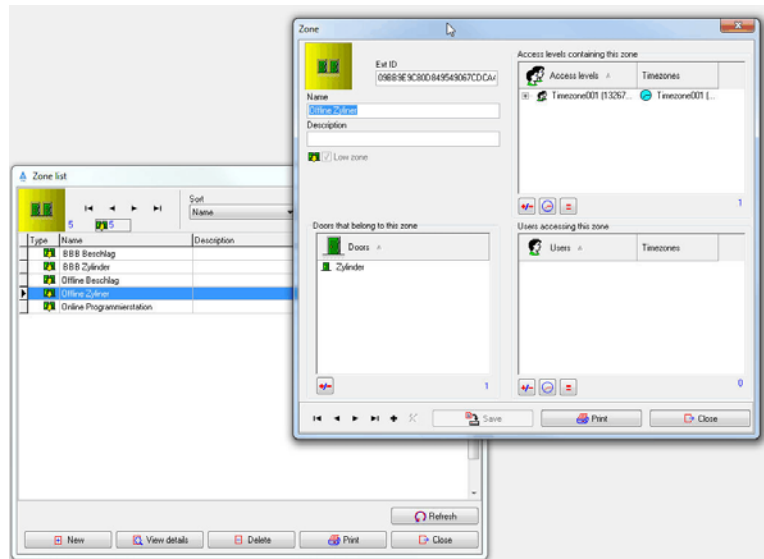


Zones are called door groups in IQ NetEdit.

A new zone can be defined by clicking on “[x] New”. Zones must be defined in the “Zones” tab and the cylinders and fittings defined earlier must be assigned to the zones. A name and description can also be entered for each zone. Cylinders/door fittings are selected and assigned by clicking on “+/-”.

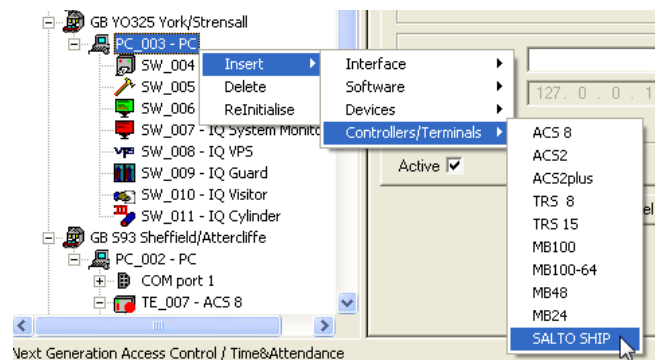


Maximum number of door groups/basic zones: 96.  
We recommend careful planning and a logical design of door groups so that cylinders/door fittings can be uniquely assigned to door groups. Assign each cylinder/door fitting to one door group only so that it can be uniquely identified.



### 6.5.6.3 Transfer of SALTO Ship (SVN) data to IQ NetEdit

The SALTO Ship System (SVN) configured earlier can be added to the desired site.  
Select Insert/Controllers/“SALTO SHIP”.



The SALTO SHIP System (SVN) is added to the corresponding site.

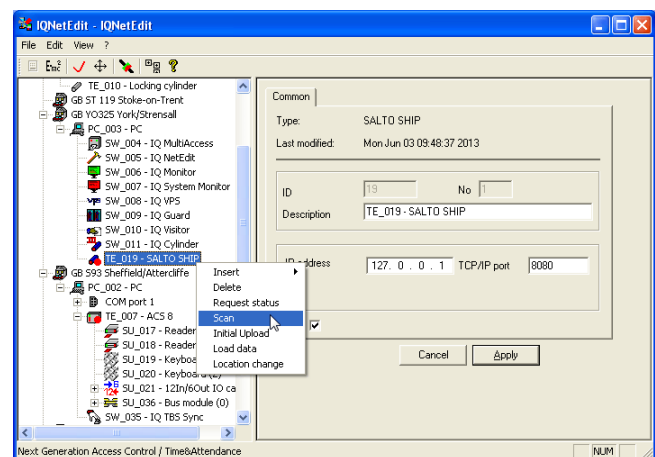
To ensure that the cylinders and door fittings configured are transferred to IQ MultiAccess, perform the following steps:

Enter the corresponding IP address (in this case, the local PC, hence 127.0.0.1) as well as the TCP/IP port that was specified in “RW Pro-Access”.



It is recommended that the SALTO service be installed on the same PC as the IQ Server.

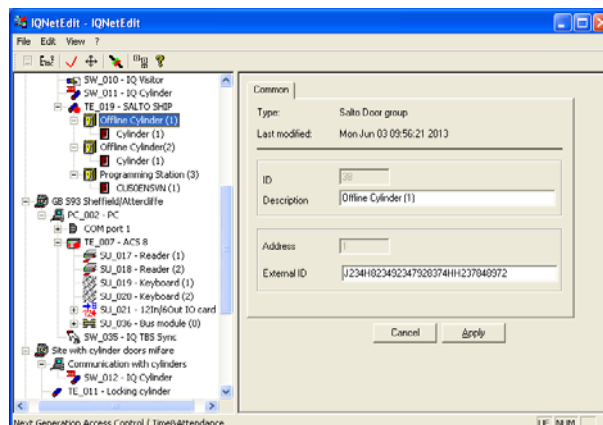
Right-click to open the context menu for an existing functional connection. Select menu item “Scan”. All defined and assigned door groups, along with assigned cylinders and door fittings, are automatically transferred.



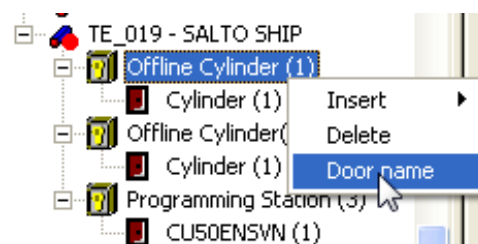
Cylinders and door fittings are represented as door groups in the logical view. One door is defined in IQ MultiAccess for each door group. For easier identification, a unique name can be entered in the "Description" field.



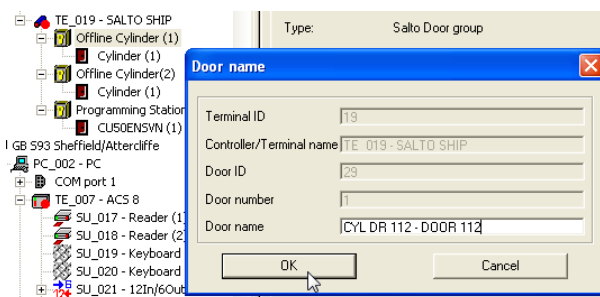
It is recommended that the SALTO system be integrated into IQ MultiAccess using the command "Scan". If the system is manually defined (via "Insert"), external IDs (unique numbers) in the SALTO system are not recognized in IQ MultiAccess.



For ease of handling in IQ MultiAccess, the door name should be unique. Right mouse click the door group and select "Door Name" from the context menu.



A unique name can be entered in the "Door Name" field. Click "OK" to confirm.



All other authorizations and assignments are defined in IQ MultiAccess.

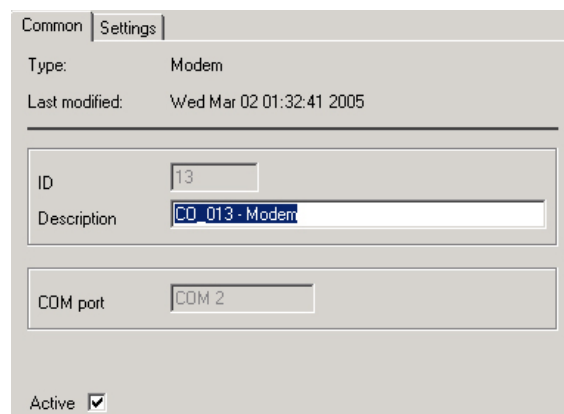
## 6.6 Configure RDT / Distant Station

### 6.6.1 Configure modem

Basically, the RDT to the distant stations can be implemented via modem (analog / ISDN) and/or ISDN cards. Several modems may be connected to one computer or they may be distributed arbitrarily over the entire network. The same applies to the ISDN cards. Mixed operation of ISDN cards and external modems is possible.

**Procedure:**

1. Right-click on the icon of the interface where the modem is connected.
2. Select *Insert* → *Devices* → *Modem*.
3. Left-click on the modem icon.



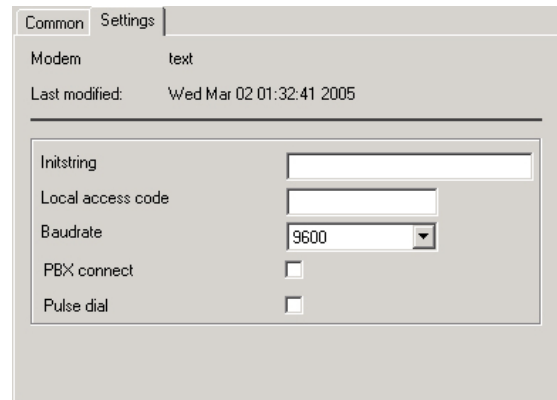
4. Enter a meaningful name in tab *Common* and activate the check box **Active**.
5. The following information has to be stored in tab *Settings*:

○ **Initialization string:**

Each modem requires certain settings which cause the modem to work according to the individual requirements.

These settings consist of one or a combination of several AT-commands which may differ from device to device.

The initialization is explained in more detail in Chapter 6.6.5.



○ **Local access code:**

If the individual modem is connected to the extension of a telephone system which does not provide direct access to a telephone exchange line, the preselection for obtaining this access must be entered in this field. In most cases that will be "0". In this case, field **PBX connect** should also be activated.

If a direct exchange line is available, no entries are required in this field.

○ **Baudrate:**

This field defines the transmission speed between PC and the modem connected to it. The speed depends on the modem that is used. Select the maximum value via the scroll-down arrow right of the entry field to keep the connection time as short as possible.

○ **PBX connect**

see **Local access code**.

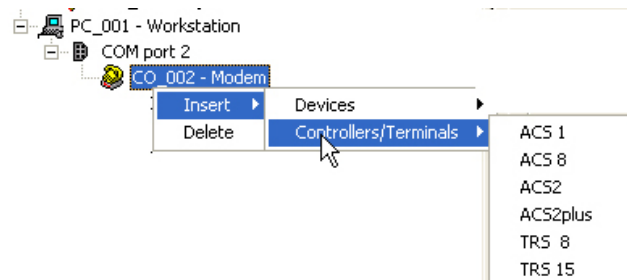
If this field is activated, the PBX does not wait for the dial tone but dials directly.

○ **Pulse dial:**

Most modern telephone systems/telephone connections use multiple-frequency dialling (i.e. each key activation is acknowledged by a sound). In this case, no modification of this check box is required.

Older systems sometimes still work with the pulse dial method (you can hear a clattering noise as with the dials used in the past). If this is the case, this check box must be activated.

By means of the modem, either a single bus controller or an ACS-1 (directly), an ACS-2 / ACS-2 plus / ACS-8 (directly) or a TRSxx (directly) can be connected via RDT to the distant station. The bus controller of the distant station manages a maximum of 32 controllers/terminals (ASC-1, ACS-2 / ACS-2 plus / ACS-8).



**Right-click** on the modem icon, then on

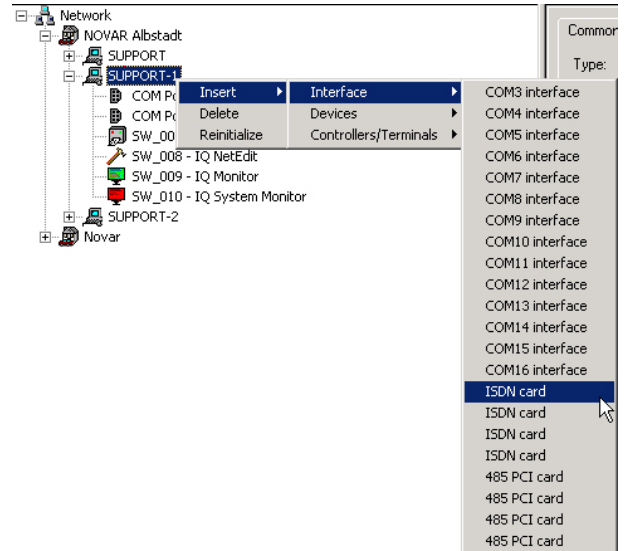
*Insert* → *Devices* in order to configure a bus controller

or *Insert* → *Controllers/Terminals* to configure an individual ACS-1, ACS-2 / ACS-2 plus / ACS-8 or TRSxx.

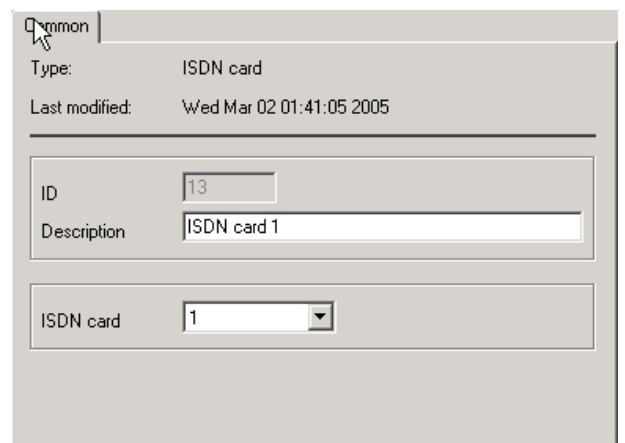
### 6.6.2 Configure ISDN card (B-channel)

**Procedure:**

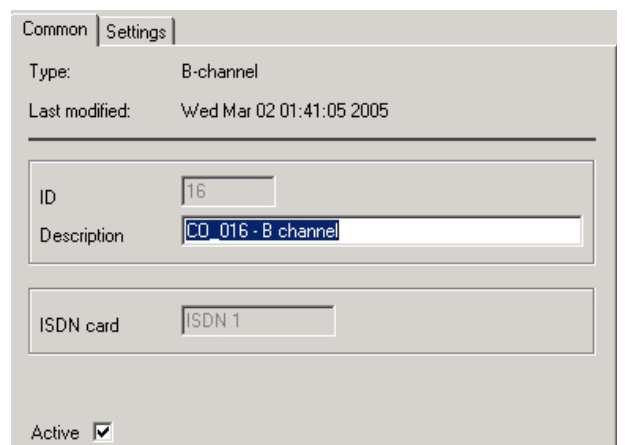
1. **Right-click** on the workstation where the individual ISDN card is installed.
2. Select **Insert** → **Interface**.  
8 ISDN-B-channels are available per workstation. Select the one that is required.
3. **Left-click** on the ISDN icon.



4. Enter a meaningful name in tab **Common**.



5. Click on the B-channel used. Enter a meaningful name in in tab **Common** and select **active**.



6. The following information has to be stored in → **tab Settings**:
- **Local access code:**  
If the ISDN channel concerned is connected to the extension of a telephone system which does not provide direct access to a telephone exchange line, the preselection for obtaining this access must be entered in this field. In most cases, that will be "0". If direct access to an exchange line is available, no entries are required in this field.

The screenshot shows a configuration window with two tabs: 'Common' and 'Settings'. The 'Settings' tab is active. It contains the following fields:

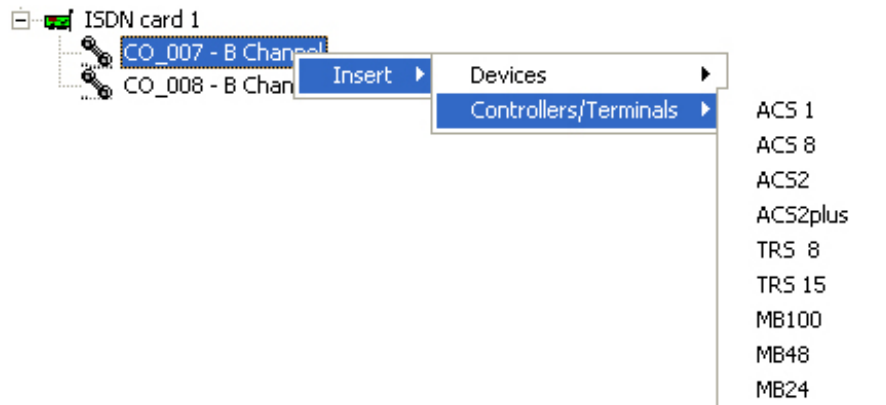
- B-channel:** text
- Last modified:** Wed Mar 02 01:41:05 2005
- MSN:** 0
- Local access code:** (empty field)

- **MSN:**  
The internal telephone end number of the extension has to be entered in this field. It is used e.g.
  - to clearly identify an extension and its user,
  - to authorize the user to dial into the public telephone network,
  - to permit individual billing per user.
 (There are further functions which are not relevant in this context.)



For further information concerning the individual tabs see Chapter 5 → **Tabs**.

By means of the ISDN card, either a single bus controller or an ACS-1 (directly), an ACS-2 / ACS-2 plus / ACS-8 (directly) or a TRSxx (directly) can be connected via RDT to the distant station. The bus controller of the distant station manages a maximum of 32 controllers/terminals (ASC-1, ACS-2 / ACS-2 plus / ACS-8). In addition, connection to an **Intrusion Detection System 561 MB24/48/100** is possible, too.



Right-click on the B-Channel icon, then on *Insert* → *Devices* in order to configure a bus controller or *Insert* → *Controllers/Terminals* to configure an individual ACS-1, ACS-2 / ACS-2 plus / ACS-8 or TRSxx or MB100.



### 6.6.3 Bus controller at distant station

#### 6.6.3.1 Configure bus controller

The following settings apply only if the bus controller is used at a distant station (otherwise continue with Chapter 7).

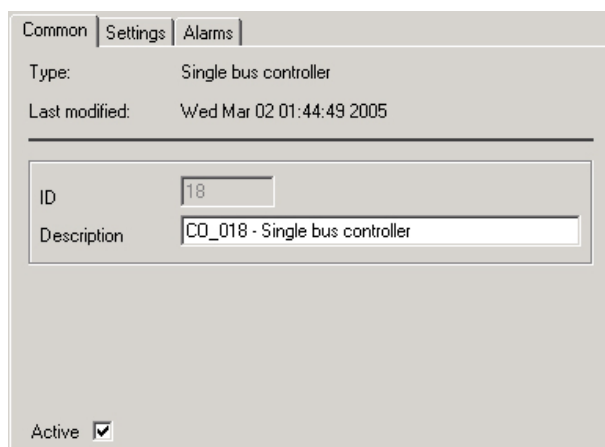
At a distant station, single bus controllers can be controlled only via RDT. If a bus controller is controlled via RDT, DIP switch 6 must be set to "ON" (cf. Installer Instructions for bus controllers). In this context, it does not matter whether RDT is implemented via a modem (analog) or via an ISDN card.

**Right-click** on the modem or the ISDN B-channel icon. Select *Insert* → *Devices* → *Single bus controller*.

**Left-click** on the bus controller icon.

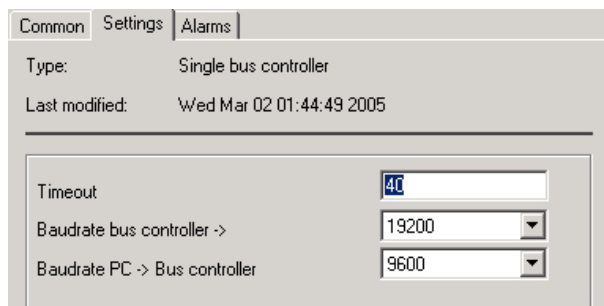
→ **tab Common:**

Enter a meaningful name and switch the bus controller active.



→ **tab Settings:**

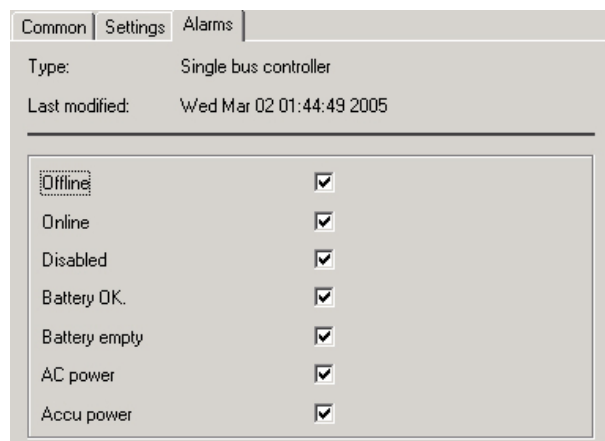
**Timeout:** We recommend to accept the predefined value.  
 Timeout = 40 means: if the bus controller does not react any more, an alarm will be triggered after 40 seconds.



**Baudrate bus controller<-> controller/terminal:**

The transmission speed between the bus controller and the controllers/terminals connected to it is entered in this field. The default settings of the location (cf. 6.1) are accepted automatically. The speed entered here must correspond to the hardware settings.

→ **tab Alarms:** Certain events which are to trigger/or not to trigger an alarm can be specified in this tab.



→ tab *Distant Station*:

**Phone number:** The phone number (incl. area code but without local access code!) of the distant station is entered here.

**Quantity:** This specifies the data volume modified in IQ MultiAccess as of which the distant station is called. If you enter here e.g. quantity 5, this means that the distant station is called automatically within one of the active time windows as soon as e.g. 5 (or more) master data records have been modified. If this quantity is reached several times within the active time window, a connection will be established accordingly as many times. If the quantity of data records within a period of time is reached or exceeded outside an active time window, a connection will not be established immediately but only when the start of the next time window is reached

If quantity "0" is entered, a connection is not established when data are available for transmission but only when a time window is reached.

**Time windows A - D:** 4 different time ranges can be defined. When these time ranges are reached, a connection to the distant station is established once regardless of whether master data records modified in MultiAccess are available for transmission or not. Booking data pending in the controller/terminal are fetched and any master data modifications that might be available are sent to the controllers/terminals by IQ MultiAccess. Without this option, any master data modification in IQ MultiAccess would immediately provoke the establishment of a connection (depending on field *Quantity*).

### 6.6.3.2 Configure controllers/terminals at the bus controller

The same requirements as for a single bus controller that is directly connected apply to the single bus controller of the distant station. The controllers/terminals can be inserted either manually or via the Scan for controllers/terminals function.



The settings must always be checked manually and the controllers/terminals must be activated.

## 6.6.4 Controllers/terminals connected directly to a distant station

### 6.6.4.1 ACS-1

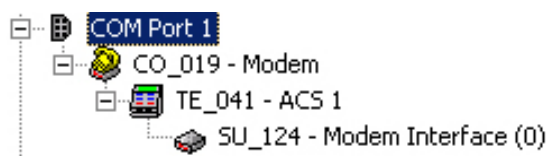


If only one ACS-1 controller is used per distant station, an external bus controller is not necessarily required. What is required is the RDT interface card, item no. 026840.18 for connecting an external modem.

If the RDT card is used, it is not possible to install another extension card!

#### Insert controller/terminal:

**Right-click** on the modem / ISDN B-channel icon. Select *Insert* → *Controllers/Terminals* → *ACS-1*. An ACS-1-icon incl. the integrated modem interface card is inserted.



If you left-click on the ACS-1 icon, the 4 standard tabs of ACS-1 described in Chapter 5 will be provided, but some of the functions are deactivated. These are mainly those functions which either require ONLINE operation or a particular extension card. The ACS-1 is equipped with one slot only. In case of RDT connection, this slot is occupied by the RDT interface card.

In addition, → **tab Distant Station** is available which has the same meaning as the tab with the same name for the single bus controller connected via RDT (see 6.6.3.1).

For the modem interface card which is integrated in the ACS-1 and configured automatically, only the name can be modified.

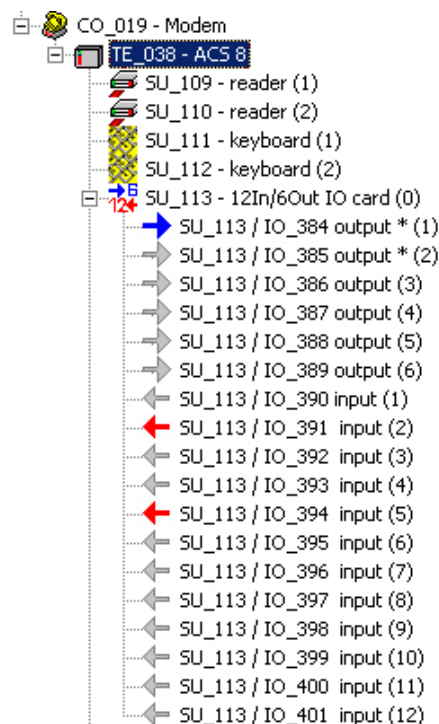
### 6.6.4.2 ACS-2 / ACS-2 plus / ACS-8



If only one ACS-2 / ACS-2 plus / ACS-8 controller is used per distant station, an external bus controller is not necessarily required. In the factory setting, the ACS-2 / ACS-2 plus / ACS-8 is equipped with a serial interface for connecting an external modem.

#### Insert controller/terminal:

**Right-click** on the modem / ISDN B-channel icon. Select *Insert* → *Controllers / Terminals - ACS-2 / ACS-2 plus / ACS-8*. An ACS-2 / ACS-2 plus / ACS-8 icon incl. all possible components is inserted. (Those which are actually used must be activated manually.)



If you left-click on the ACS-8 icon, → **tabs Common, Reader Settings and Alarms** described in Chapter 5 are provided.

In addition, → **tab Distant Station** is available which has the same meaning as the tab with the same name for the single bus controller connected via RDT (see 6.6.3.1).

The settings for the sub-components *Reader, Keyboard* and *I/O Module* which are configured automatically are described in Chapter 5.

#### 6.6.4.3 TRSxx

The direct connection of the TRSxx terminals is via RDT generally implemented as described in section 6.6.4.1 (ACS-1).

## 6.6.5 Modem initialization

A modem requires initialization before it can start operation, i.e. it is set to the operating mode required for the corresponding application via so-called AT commands. For this purpose, several individual AT commands can be combined into a so-called init string (initialization string). Usually, this init string is sent to the modem whenever the latter is addressed in order to guarantee that the modem is always correctly initialized. In practice, this is done automatically on the basis of the relevant tabs (cf. Chapters 5 and 6).

### 6.6.5.1 The initialization string

The initialization string depends on the type of the modem used. Please see the modem manual for the initialization string. If you have purchased the modem from our company, you will find the initialization string in the attached DIN A4 information sheet.



The distant station modems are provided with a different initialization string than the PC modem. The PC modem gets its initialization string via NetEdit.

IQ MultiAccess always sends the following AT-commands to the modem:

#1:	AT&FE	Reset/Echo off
#2:	ATQ0V1	acknowledgement on / in plain text
#3:	ATX3	(in PBX) ignore dial tone/evaluate busy tone
#4:	"User init string"	

The distant station modems get their initialization string via the "Hyperterminal" software. This software can be found under "Accessories" of Windows.

Meaning of the init parameters see table next page.

AT commands used	Meaning
&F	<b>Load standard configuration</b> The modem is set to the delivery status. If there is a connection, this command is not executed.
E0	<b>Command echo to host.</b> E0 = Commands are not echoed. E1 = Commands are echoed.
X3	<b>Treatment of dial tone/busy tone</b> X0 = ignore dial tone/busy tone X1 = ignore dial tone/busy tone X2 = wait for dial tone/ignore busy tone X3 = ignore dial tone/evaluate busy tone X4 = wait for dial tone/evaluate busy tone  In case of <b>ATX2</b> or <b>ATX4</b> , the modem waits for the dial tone before dialling. In case of <b>ATX0</b> , <b>ATX1</b> or <b>ATX3</b> , the modem does not wait for the dial tone, so that e.g. "blind dialling" is possible while establishing the connection between two extensions. Recommendation:        Use <b>ATX3</b> within a telecommunications system. Use <b>ATX4</b> in case of direct connection to the public telephone network.
\N1	<b>Select error correction procedure</b> \N1 = direct
%C0	<b>Data compression</b> %C0 = no data compression
\C2	<b>Buffers off</b>
D3	<b>with DTR on -&gt; off Hang Up + reset</b>
DS	<b>Compresson</b> DS=0: Data compression off
S0=0 S0=1	<b>Automatic call pick-up</b> S0 = 0: no automatic call pick-up S0 = 1: automatic pick-up after 1 ringing
S12	<b>ESC sequence</b> S12=40:        After ESC sequence (+++) send OK after 800ms
V1	<b>Acknowledgement in short form/plain text</b> V0 = acknowledgement in short form as number V1 = acknowledgement in plain text
&W0 &W1	<b>Save configuration profile</b> &W0 = Save configuration profile 0 &W1 = Save configuration profile 1
&Y0 &Y1	<b>Set pointer to configuration profile</b> &Y0 = Set pointer to configuration profile 0 (load configuration 0 after reset) &Y1 = Set pointer to configuration profile 1 (load configuration 1 after reset)
Z	<b>Execute Reset</b> Z0 = Reset, start with profile 0

**Examples:** The following section shows some examples of init strings for the modems which are widely used at the moment. Due to the large variety of modems available on the market and the rapid technical developments, we have to refer you to the corresponding manuals and/or the information sheets provided by Honeywell Security regarding the modems to be used.

#### Init string for analog modems:

##### Example 1:

Init strings for modem **Devolo Microlink 56Ki** (the most common standard modem at editorial deadline, formerly called **ELSA 56Ki**):

String for PC modem: **AT%E0\C2&D3S12=40+DS=0,0,2048,32**

String for distant station modem: **AT&FE0S0=1%E0\C2&D3S12=40+DS=0,0,2048,32&W0&W0Y0Z0**



After the connection is completed, a Power-On reset must be executed on the modems of the PC and on the distant stations!

**Note:** The init string should be checked after update from V4 to V5.

Some other examples of older modems which are, however, also very common (might still be in use after upgrading existing AC installations):

##### Example 2:

In the following example, two analog modems of type **Microlink 33.6TQV** are used.

String for PC modem: **AT&FE0X3\N1%C0S0=0V1**

String for distant station modem: **AT&FX3\N1%C0S0=1V1E0&W0&Y0**

##### Example 3:

In the following example, two modems **Devolo Microlink 56k Basic** are used.

String for PC modem: **AT&FE0X3S0=0V1S12=40**

String for distant station modem: **AT&FS0=1E0\*W0&Y0Z0**

**Init string for ISDN modems /cards:**

**Important for ISDN modems / ISDN cards:** The MSN or EAN number from which the modem is supposed to take calls must also be stored in the modem as well as the ISDN protocol EURO-ISDN or 1TR6 (please see the relevant manual and tools from the individual modem manufacturers).

**Example 4:**

Init strings for an ISDN modem **ELSA Microlink ISDN**

String for PC modem: **ATV0=1-M0=1S0=1&D2X0\*W0&Y0Z0**

String for distant station modem: **ATV0=1-M0=1S0=1&D2X0E0\*W0&Y0Z0**



All modems not listed here must be initialized according to the information sheets provided with the delivery if they were supplied by Honeywell Security. All third-party products are to be initialized according to the documentation following the examples above.



**6.6.5.2 Initialization procedure for distant station modems**

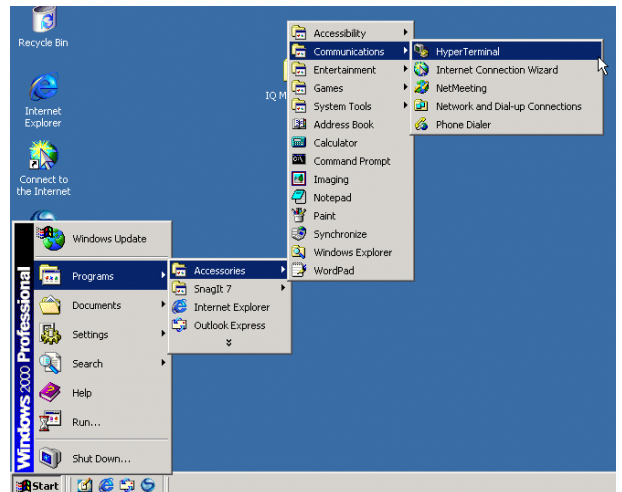


All distant station modems must first receive their initialization string via the "Hyperterminal" software. Then they can be separated from the PC and installed at the distant station.

1. Connect distant station modem to COM1 or COM2 of the PC and switch modem on
2. Open *Hyperterminal*.

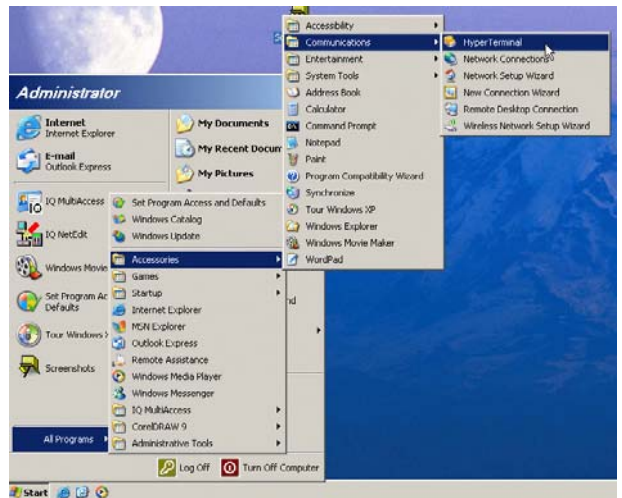
**Windows 2000**

Click on: Start  
Programs  
Accessories  
Communication  
Hyperterminal.



**Windows XP**

Click on: Start  
All Programs  
Accessories  
Communication  
Hyperterminal.



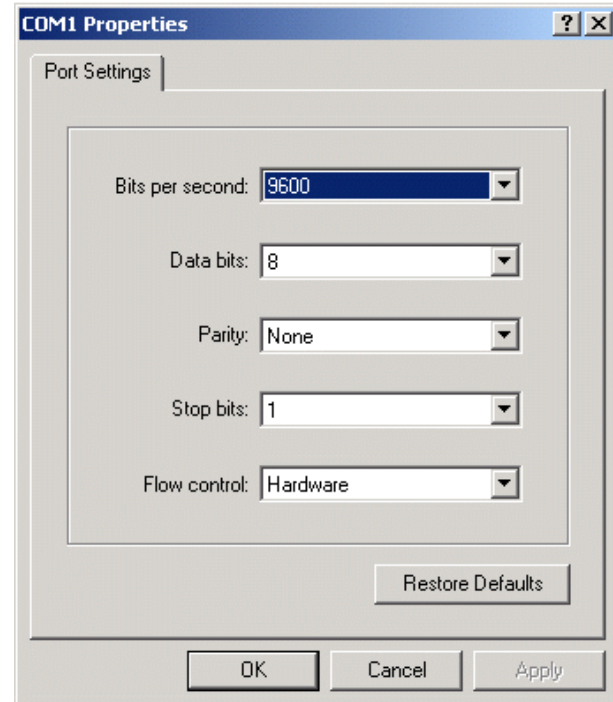
3. Enter a name for the connection, e.g. IQ\_modem\_init.



4. Select the COM interface where the modem is located.



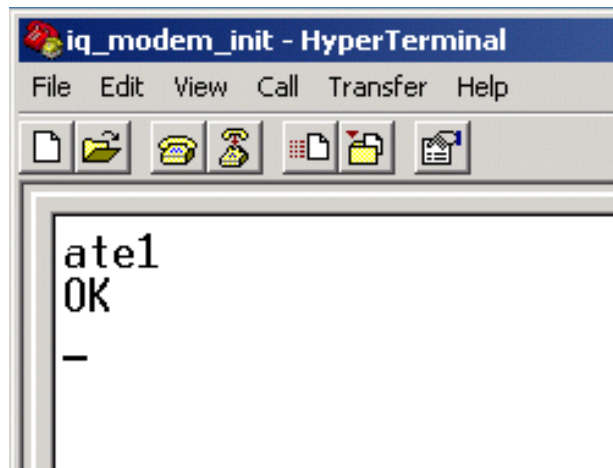
5. Set the parameters shown in the figure opposite. The example applies to analogue modems. In case of ISDN modems, 19200 must be entered in field *Bits per second*.



6. It might happen that the following AT command is not displayed during entry and must possibly be entered "blindly". If the echo is switched off on the modem, you do not see what you are typing.

Type **ate1**  
Confirm with *Enter*.

The echo is now switched on. Thus you can check what you are typing.



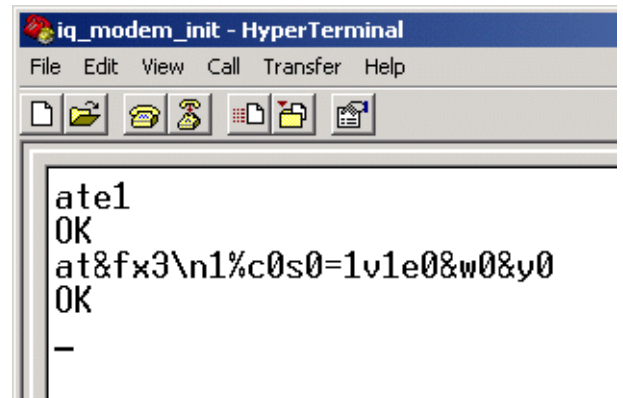
7. Enter the initialization string (entries are not case-sensitive)

In our example (using a **Microlink 33.6TQV**), it is:

**AT&FX3\N1%C0S0=1V1E0&W0&Y0**

for initialization string see Chapter 5.5.1.

Confirm with *Enter*.



```
iq_modem_init - HyperTerminal
File Edit View Call Transfer Help
ate1
OK
at&fx3\n1%c0s0=1v1e0&w0&y0
OK
-
```

8. If you have to connect several distant stations, initialize each distant station modem in the same way.

## 6.6.6 Connection Test



The following steps describe only a physical RDT test, i.e. IQ NetEdit tries to establish a connection to the corresponding distant station modem.

The following steps are explained on the basis of modems. The same procedure applies to ISDN cards

1. Start operating the distant station modem(s)
2. Start operating the PC modem
3. Start *IQ NetEdit*.
4. In the **Distant Station** tab of the individual distant station device, define a **Time window** of "0:00 - 23:50 h" and **Quantity** "1".<sup>18</sup>
5. **Right-click** on the relevant bus controller or the controller/terminal of the distant station.
6. Click on **Scan for controllers/terminals** (only possible with bus controller).

*IQ NetEdit* now tries to establish a connection to the bus controller selected via RDT, searches all devices connected to it - as described above - and inserts them automatically.

**or**

7. Click on **Request (bus) state** (possible with bus controller and controller/terminal).

*IQ NetEdit* now tries to establish a connection to the bus controller or controller/terminal selected and to display information about the current status on the screen (cf. Chapter 7).

## 6.6.7 When is a connection established?

### Immediate connection for test purposes:

For this purpose, "1" must be entered in field → **Quantity** in tab → **Distant Station** of the individual device and a → **Time window** of 0:00 - 23:59 h must be available<sup>6</sup>. In case of different entries, immediate connection cannot be guaranteed.

- Request (bus) state
- Scan for controllers/terminals /
- Active addresses
- Test screen

### Time-dependent connection (hierarchical):

- When starting IQ MultiAccess, provided that at least one time window entered in *IQ NetEdit* has been reached or is still valid - irrespective of whether data are pending for transmission or not (e.g. time window from 10:00 to 11:00, starting IQ MultiAccess within this time window causes a connection to be established).
- During ongoing operation, when a time window entered in *IQ NetEdit* has been reached - irrespective of whether data are pending for transmission or not.
- During ongoing operation, within a valid time window entered in *IQ NetEdit* when the *Quantity* entered in *NetEdit* has been reached or exceeded.

<sup>18</sup>

After completing the RDT test successfully, the test data must be removed again and replaced by the original data.

Example:           Time window: 10:00 - 11:00  
                  Quantity:        3

1. Connection is established at 10:00 - even if no data are available for transmission yet.
2. Connection is established between 10:00 and 11:00 as soon as at least 3 data records have been modified / created / deleted within this period of time.

- All other items that can be selected within IQ MultiAccess cause a connection to be established only within a time window defined in *IQ NetEdit*.

## 7. Icon-related functions

If you **right-click** on the individual components or press the Windows key, one or several of the following functions will be available depending on the context (see also Chapter 4.2.3). The components may be found in the physical representation as well as in the logical representation.



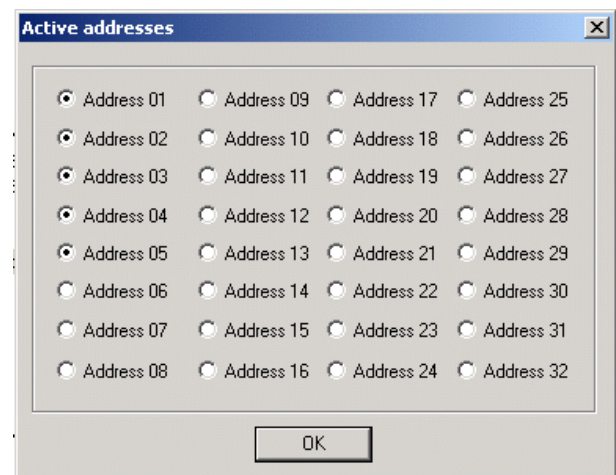
The overview in Chapter 6.4 shows which other controllers/terminals / components are made available by function → *Insert*.

### Description of the individual functions (in alphabetic order):

**Active addresses:** This function shows which addresses are active or not active on the relevant controller.

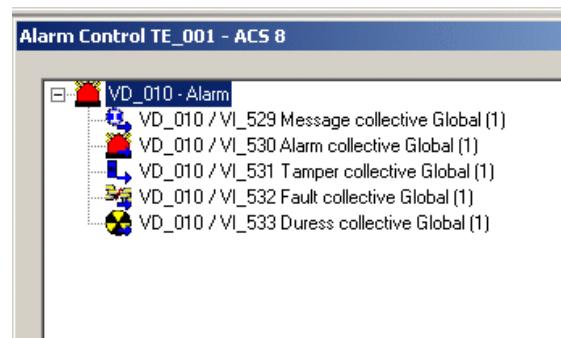
Not active means that the device<sup>7</sup>

- does not exist (address still free)
- is not switched on
- is defective
- is set to a wrong baudrate
- has no connection to the bus



**Add:** Via this function, you can insert further components manually. The components depend on the context and are shown in another menu which may contain additional submenus.

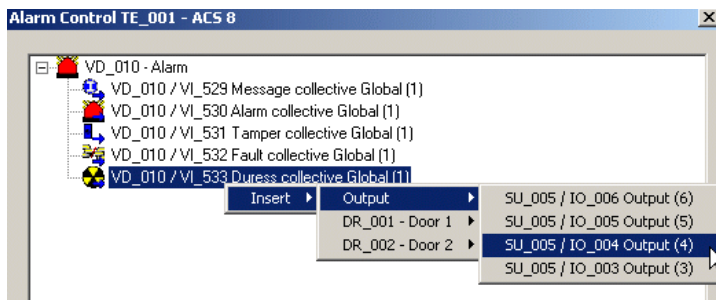
**Alarm Control:** For ACS-2/8 controllers, there are various collective messages for alarm, fault etc. These are shown as "VD\_xxx" = Virtual Device.



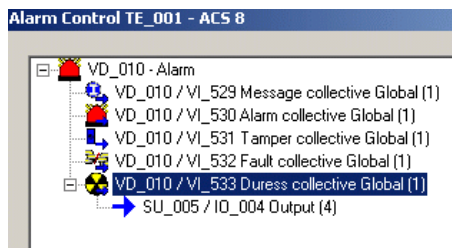
Via this function, individual components can be assigned to a door. This has the effect that e.g. outputs can be controlled, doors can be influenced or macros can be started via release criteria when a collective message is output.

**Example:** Right-click on the desired component (e.g. Collective duress) → Insert → Output → Select the desired output.

<sup>7</sup> This may be either the relevant controller/terminal or the bus controller/interface converter itself.



Result: If the controller reports collective duress, output 4 and thus a device connected to it (e.g. a flash lamp) is addressed.



**Area Control:** This function is required for the → **Barring Repeated Entry** and → **Antipassback** functions. For this subject see the separate documentation “Supplementary functions of IQ MultiAccess”. Not available in V1.


**Arming prevented:** This function can be used to check why the IACP can not be armed via the selected operating device.

**Control panel data take over:** This menu item contains following functions for the data transfer of panels:

- IACP completely read out:** All data of the panel will be completely read out one after another.
- Switching device read out:** This function reads out the complete hardware (MBxxx) and creates them in IQ NetEdit.
- Get IACP data:** The data as follow will be read out of an MBxxx and created in IQ MultiAccess:
  - Room/timezones and → data carriers inclusive their authorizations.
  - The operating codes (→ controllers, operating codes tab). Operating code = number a user enters to log in at an IACP operating device.
- Get IACP texts:** IQ MultiAccess receives from an IACP the texts used for the event memory (customized designations of switching devices, detector groups, inputs, outputs etc.).

**Copy:** This function copies ACS-2 / ACS-8 with all settings and parameters into the clipboard. Connected components are also copied. Operators with their rights can be copied, too.

**Delete:** This function deletes the components selected incl. all components connected to them after a confirmation prompt.

**Disable a zone:**  **Caution!** the selected zone will be completely deleted! If required again, it must be recreated completely with all its allocations.

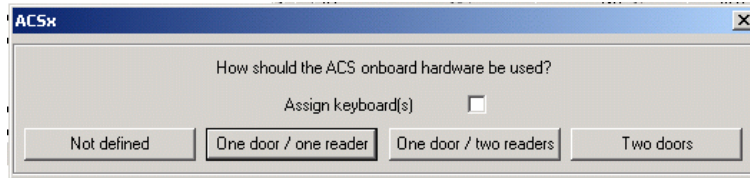
**Door definition:** Doors controlled via the ACS-2/8 onboard hardware can be defined in different ways:

Definitions in the default settings:

When defining an ACS-2/8,

- one door with one reader is configured automatically
- one door with two readers is configured automatically
- two doors are configured automatically
- the doors are to be configured manually.

In case of manual configuration, the following prompt appears when defining an ACS-2/8:



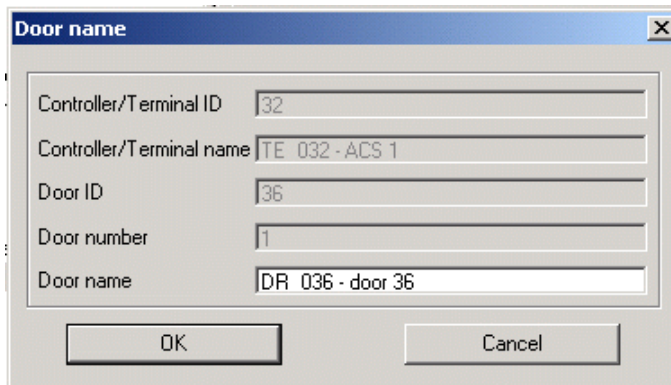
By clicking the "One door" or "Two doors" button, the door(s) is(are) defined automatically for the ACS-2/8 concerned.

When selecting "not defined", no door is configured; this must be made manually (cf. 6.5.2.1, step 4).

#### Door name:

IQ NetEdit configures automatically one door (or 2 doors if a two-door expansion board is available) when an ACS-1 controller is defined. Consecutive numbers are assigned to these doors (Door\_x). In order to ensure clear identification and assignment of the doors in IQ MultiAccess, it is necessary to use unique and meaningful door names (e.g. office Mr. Meier, cleaning room 1st floor, training room, etc.).

All other entries are defined or applied automatically.



If the ACS-1 is equipped with a two-door expansion board, the name of the first door is defined as described above. In order to define the name of the second door, right-click on the two-door expansion board icon and then click on Door name

For ACT, it is only possible to assign **one** door name.

For IACP doors the display shows the data received by scanning.

#### Get zone counter:

Via this function, the current counter reading of the selected ACS-2plus / 8 can be found out. The counter reading can not be changed here, because the value results of bookings of several zones/controllers.

Change counter reading:

- a)
  - Right-click the required zone
  - Load zone counter
  - Enter the correct / required value
  - OK
- b) Set all Persons to "neutral" or to the zone they are actually in (see



“Extended functions of IQ MultiAccess, P32205-46-0G0-xx, chapter 2.3.3.4).

For ACS-1 terminals/controllers, the corresponding function is not to be done at the terminal/controller, but at each door in the → **counters/image matching/ATR** tab using the button **Get/set counter**.

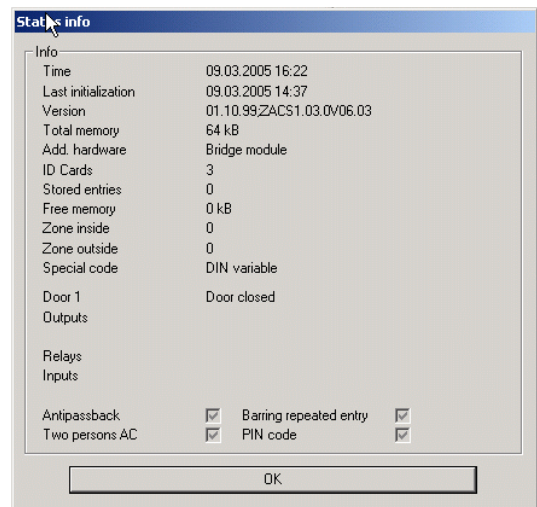
- Initial upload:** Via bootstrap, the controller/terminal selected is set to a defined initial state. This should be carried out at commissioning or before loading the data.
- Insert:** Via this function, you can insert ACS-2 / ACS-8 and operators from the clipboard. The components are taken with the function → **copy** into the clipboard before.
- I/O point export:** By right-clicking on a location, the → **I/O points for WINMAG** can be output into a (\*.txt) file. You are free to choose a name and path for this file. This file can be imported in WINMAG (see separate documentation).
- IQ AEPIInfo:** This starts a protocol of all data traffic between the computer and the controllers. The protocol can be saved as a file and can help our support in case of communication malfunctions.
- Load data:** Via this function, all data entered in IQ MultiAccess are loaded into the controller/terminal selected.
- Location manager:** Via this function, location managers can be inserted. Location managers are → **Operators** who have rights at a particular → **Location**.
- MacroControl:** It is possible to define macros for certain processes at ACS-8 controllers. The subject of macros is very complex. We refer therefore to the separate documentation “Supplementary Functions of IQ MultiAccess”.
- Modify location:** Devices which are physically connected to a location A can be logically assigned to another location via this function (see example in Chapter 11).
- Personnel managers:** Via this function, you can insert personnel managers. Personnel managers are → **Operators** with systemwide rights to manage personnel data.
- Print assignment:** Prints the following information about the device selected:
- Controller ID, controller type (single / master / slave), controller name (name from NetEdit) as well as controllers/terminals connected to this controller / interface converter / 485 PCI interface with:
- Controller/terminal address, ID, type, name (name from NetEdit).
- Print controller/terminal list:**
- Menu item *Print controller/terminal list* is not relevant at the beginning of the hardware configuration. This menu item is used for checking and documenting the hardware configured in IQ NetEdit. It is advisable to print this list after the hardware definition in IQ NetEdit is completed.
- A list with all terminals/controllers configured in the network is printed. It includes the following information: Ser. No., ID, Type, Name.
- Print door definition:** This function is used to print a list containing all doors defined for the controller/terminal selected, including the assignment of the inputs and outputs.
- Print door list:** Menu item *Print door list* is not relevant at the beginning of the hardware configuration. This menu item is used for checking and documenting the hardware configured in IQ NetEdit. It is advisable to print this list after the hardware definition in IQ NetEdit is completed.
- A list with all doors configured in the network is printed. It includes the following information: Ser. No., ID, Type, Name, corresponding controller/terminal.

**Reinitialise:** Via this function, current modifications from IQ NetEdit are passed on to the COMMTask.

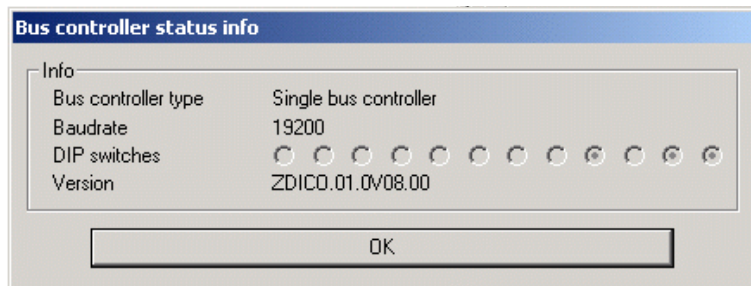
**Request status** This function provides information about:

- device type (single, master, slave controller, ACS-1, ACS-8 with relevant information about the extension level, such as additional plug-in cards, relays, card coding, free memory space, additional functions, etc.)
- baudrate between device and controller/terminal (on the BC in tab *Settings*)
- position of DIP switches in the device
- firmware version<sup>8</sup>

Example 1:  
Status info for an ACS-1



Example 2: Status info for a single bus controller



**Scan:** This function reads out the complete hardware connected to the device selected (ACS-8, bus controller) and creates them in IQ NetEdit. With IGIS-LOOP only the connected MBxxx will be read out, the further components will be recognized via the scan function of the central unit itself.

**Start/stop auto address mode:**

With **proX2 Accentic** readers/keypads the address can not be set via DIP switches but via software. With this function, the ACS-8 is set into the mode to recognize the address(es) of the reader(s) connected to this controller (via module bus), or to enter it manually. Subsequent the function **stop auto address mode** must be selected. The various possibilities of setting an address are globally described in the mounting and connection instructions of the corresponding readers/keypads. The following paragraph describes a step-by-step procedure of setting an address in IQ NetEdit:

<sup>8</sup>

It is recommended to update the firmware of the devices to the most recent version. In case of older versions, it might happen that the status information is not displayed.

**a) Initial installation**

In ex-works condition, the reader has the address "0", which is not allowed or means no address in IQ NetEdit. Therefore the connected readers will not be recognized automatically via the function → **Scan**.

1. Right-click the corresponding ACS-8 → **Start auto address mode**. This function sets the readers connected to this ACS-8 to the addressing mode. The lower green LED of the reader is blinking.
- 2a. Enter the address using the numeric keys of the reader and confirm with ✓. The reader indicates the changed address by blinking of the upper green and the yellow LEDs (see mounting- and installation instructions of the reader). The lower green LED continues blinking until the addressing mode is stopped (step 3). If the current address of a reader is not changed, there is no indication of the (not changed) address.

or

- 2b. Read any random ID card (this sets the reader to the lowest available address). The reader indicates the changed address by blinking of the upper green and the yellow LEDs (see mounting- and installation instructions of the reader). The lower green LED continues blinking until the addressing mode is stopped (step 3). If the current address of a reader is not changed, there is no indication of the (not changed) address.



In this mode one or several readers can be handled.



**Pay close attention that nobody tries to book with his/her ID card at a reader that is set to addressing mode, as this would set the reader to the lowest available address!**

3. Right-click the corresponding ACS-8 → **Stop auto address mode**. This function exits the addressing mode. Afterwards all 3 LEDs will extinguish.

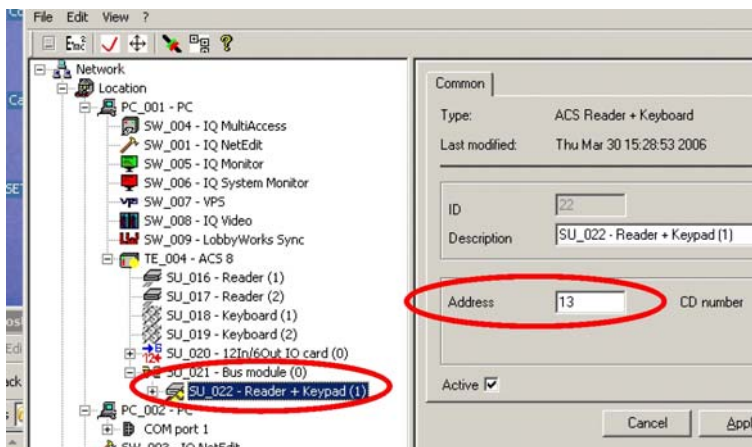


**When the setting of the addresses is finished, the addressing mode must be exited by all means, as the address might be changed by accidentally reading of an ID card (see 2b).**



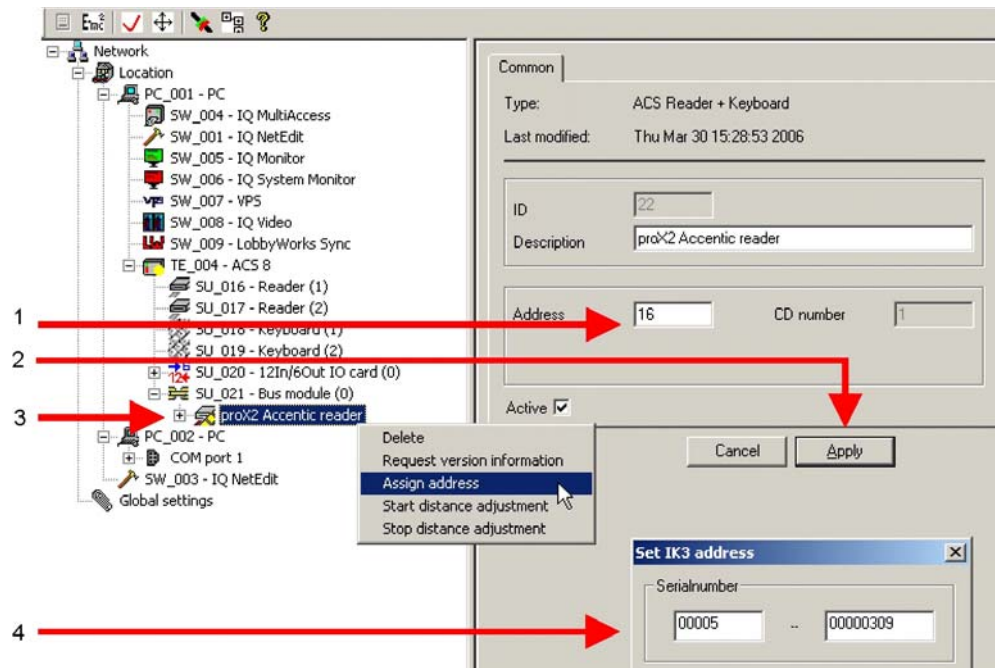
**The addressing mode automatically exits after about 30 minutes.**

4. Now **Scan** finds the reader(s) with its individual address.



## b) Change of addresses

If the address of an individual already running reader is to be changed, proceed as follows:



1. Select the concerning reader and enter the new address.
2. Button **Apply**.
3. Right-click the concerning reader → **Assign address**
4. Enter the serial number of the reader (see sticker on the back of the reader pcb), confirm with OK.



This causes an unambiguous identification of the reader to be changed. If the serial number would not be entered, the reader would be searched by its old address - but not found. The next run of Scan would find an new reader with the new address and configure this one **additionally**.

To delete an address, enter "0" as discribed above.

### Start / stop distance adjustment:

This function sets the selected reader to distance adjustment mode. Detailed information of the procedure is described in the mounting and connection instructions of the reader. After finishing the adjustment, the function → **stop distance adjustment** must be selected. If not, the program will automatically exit function after approximately 30 minutes.

**Superuser:** Via this function, you can insert superusers. Superusers are → **Operators** with systemwide administration rights (the superuser is authorized to do everything). User "**service**" defined in the factory is a superuser.

### Telnet Autoconfiguration:

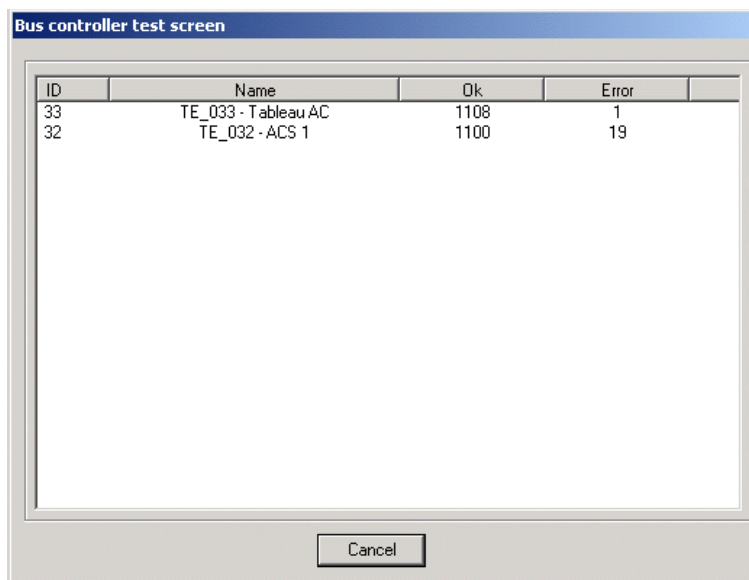
For devices that can be connected to a network directly via an Ethernet card (single bus controller, ACT, ACS-2 plus, ACS-8, TRS 8 / 15), the configuration of the Ethernet interface (item no. 026840.28/29) can be automated and thus made much easier and faster via this menu item.

**Procedure:**

1. If necessary, set the device to Ethernet operation. See the documentation for the individual device (e.g. ACS-8 via Setup).
2. Preparing and installing the interface card according to the Mounting and Installation Instructions, Chapter 3.
3. General configuration of the interface card according to the Mounting and Installation Instructions, Chapter 4.
4. If necessary, test communication via "ping" command.
5. Configure the device in NetEdit and enter the IP address.
6. Right-click on the device and select "*Telnet Autoconfiguration*".
7. All other settings are made automatically depending on the individual device.

**Test screen:**

This function is used for checking which active controllers/terminals are connected to the bus controller selected and whether there is a physical connection.



ID	Name	Ok	Error
33	TE_033 - Tableau AC	1108	1
32	TE_032 - ACS 1	1100	19

The number of positive polling attempts is shown in the *OK* column. If the physical connection is correct, the maximum value shown in the *Error* column should be 0.5% of *OK*. Otherwise, there are faults in the line.

**Zones:**

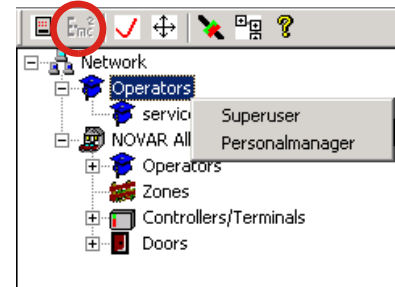
This function inserts one zone which is required for the → **Barring Repeated Entry** and → **Antipassback** functions. For this subject see the separate documentation "Supplementary functions of IQ MultiAccess". Not available in V1.

## 8. Operators

Operators are persons who have been granted more or less comprehensive rights. Operators are defined and managed in the logical representation (see also overview in Chapter 2.5).

There are two types of operators:

1. Cross-location operators with systemwide rights.
  - a) **Superusers** have all rights in the entire system. User **service** is defined in the factory as superuser. This user cannot be deleted, it can only be modified.
  - b) **personnel managers** have systemwide rights to manage personnel data.
2. Location-dependent operators = location managers who have rights for a certain location. Usually, the typical user of IQ MultiAccess is a location manager. If a person is to obtain rights for several locations, he/she must be defined as location manager for each individual location.



Superusers, personnel managers and location managers are inserted by right-clicking on the generic term **Operators**. The rights of the individual operators are defined in the relevant → **tabs**.

### 8.1 Define operators

#### 8.1.1 Superuser

1. Right-click on **Operators** directly under Network → Superuser.
2. Enter **Login name**, define **Password** and tick check box **Active**.



**Note!** If no password, an invalid password or a password of less than 5 characters is entered, it is not possible to save the location manager data!



The entries in the remaining fields can be made individually.

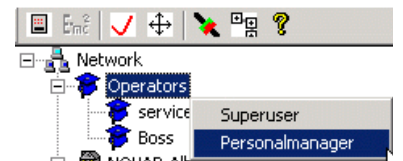
With his/her login name and password, the superuser can log into all program parts.

The superuser has **all** rights. He/she is even entitled to define other superusers.

In IQ MultiAccess, the superuser has access to all components within the entire system.

### 8.1.2 Personnel manager

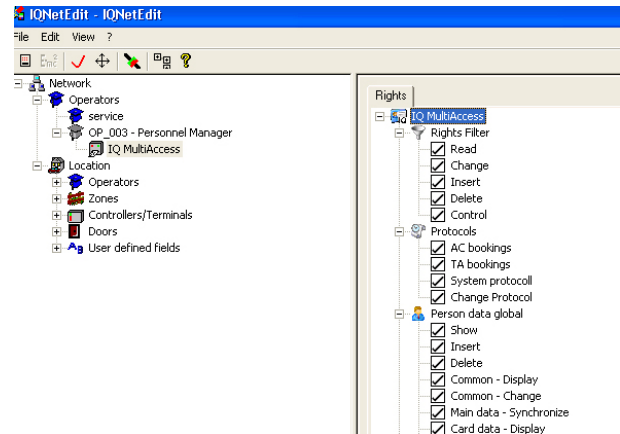
1. Right-click on **Operators** directly under Network → personnel manager
2. Enter **Login name**, define **Password** and tick check box **Active**.



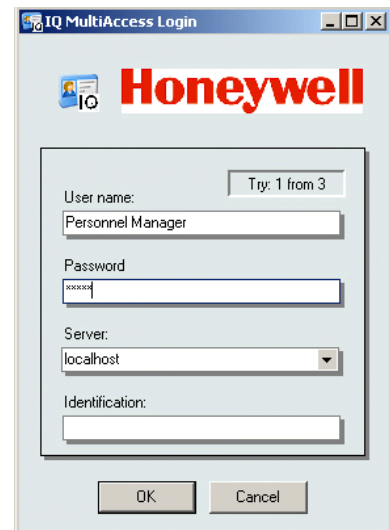
**Note!** If no password, an invalid password or a password of less than 5 characters is entered, it is not possible to save the personnel manager data!

The entries in the remaining fields can be made individually.

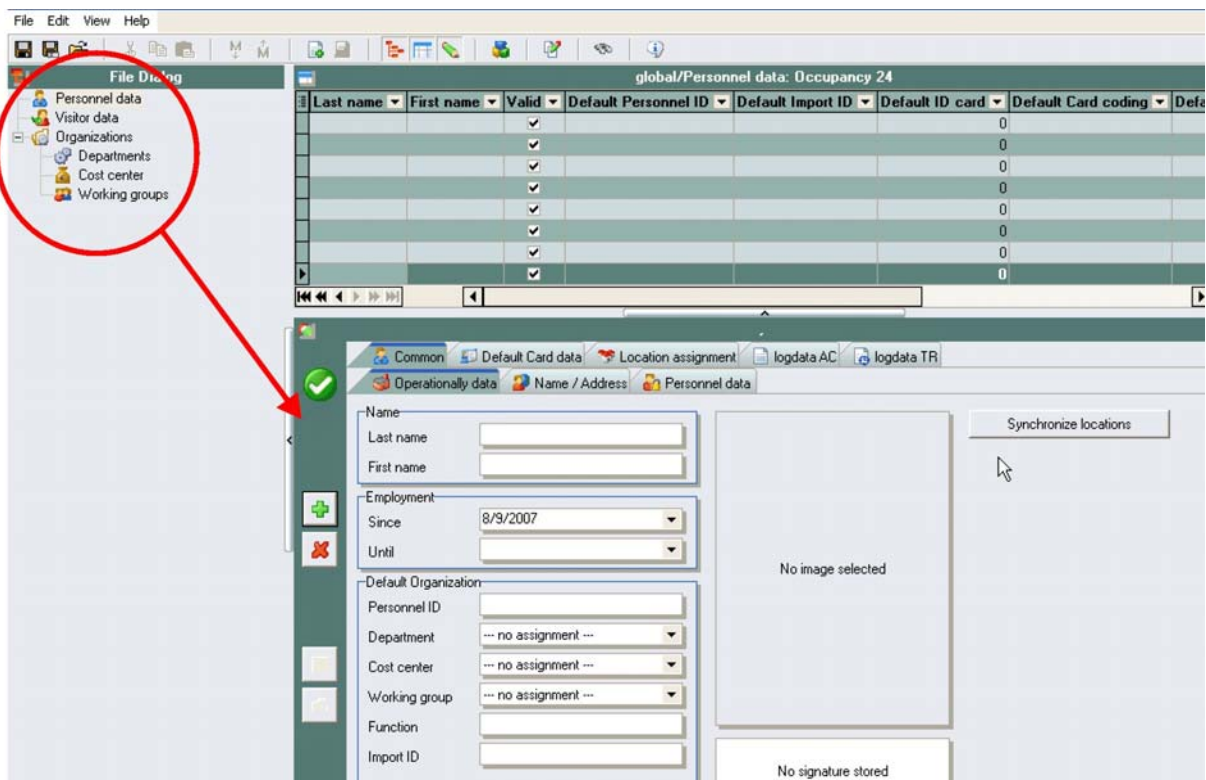
3. To a personnel manager automatically the software IQ MultiAccess is assigned. In the → **rights tab** the individual rights can be defined. As a factory setting all rights are active.



With his/her login name and password, the personnel manager can only log into IQ MultiAccess.



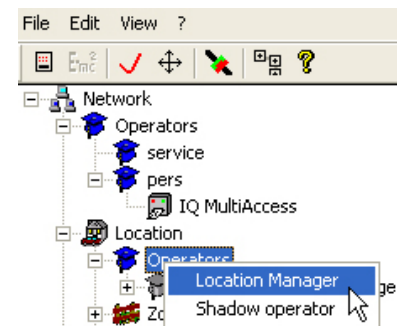
The personnel manager can only process → **personnel data** (incl. visitor data and organizations). This, however, within the entire system.





### 8.1.3 Location manager

1. Right-click on **Operators** of a certain Location → Location manager.



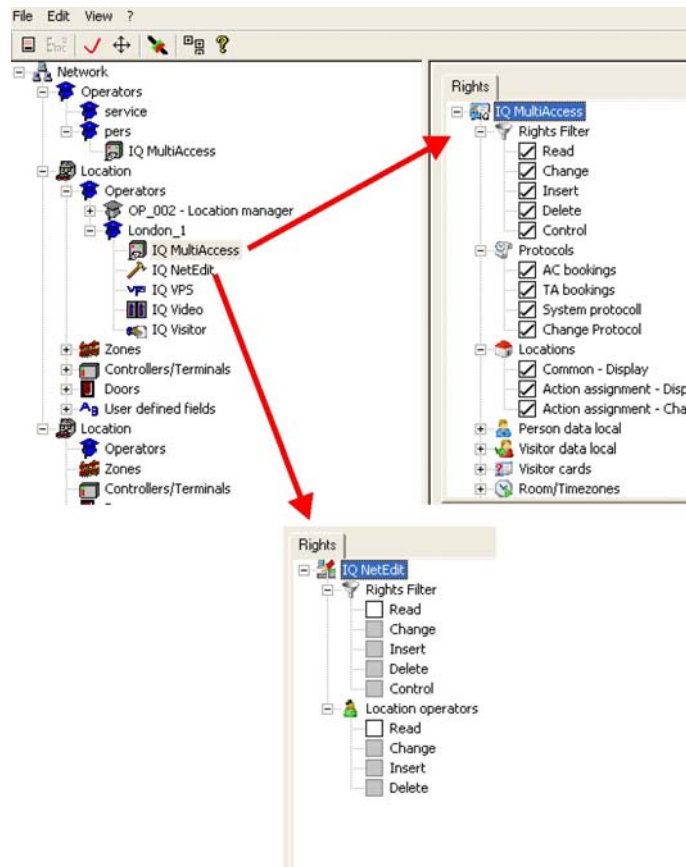
2. Enter **Login name**, define **Password** and tick check box **Active**.



**Note!** If no password, an invalid password or a password of less than 5 characters is entered, it is not possible to save the location manager data!

The entries in the remaining fields can be made individually.

3. The rights of the individual software are defined in the → **tab Rights**. The illustration displays part of the factory settings.

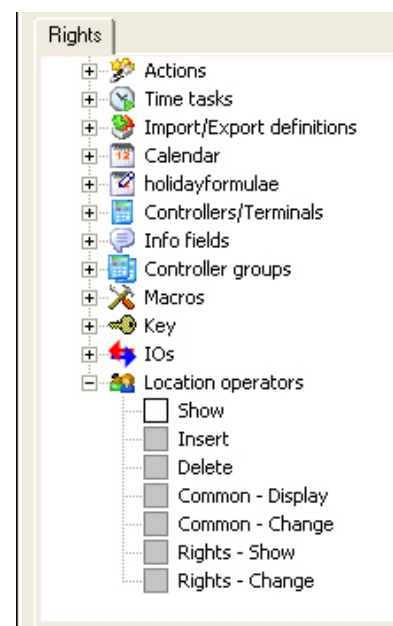


Clicking the “+” symbol opens a tree structure, where the rights of each individual component can be enabled/disabled. The factory setting shows a meaningful universally valid presetting.

In the **Rights Filter** block you can define the general rights of a user. Those filters are superior to the individual rights. That means, a user with no delete rights in his/her filter, is not allowed to delete a data record in any application, even if there the right to delete is activated.

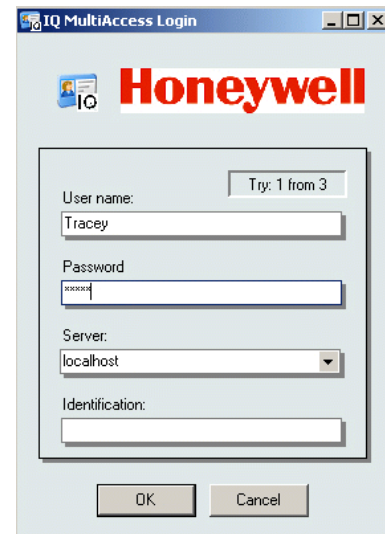
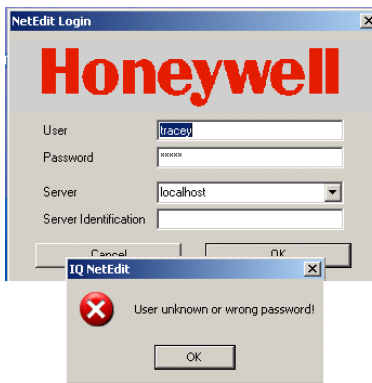


**Note!** If a location operator has the right to define and/or modify location operators, he/she can assign to himself/herself more rights that the superuser has assigned to him/her. In the factory setting, a location operator has no operator rights.



- Depending on his/her rights, the location manager can log into IQ NetEdit and/or IQ MultiAccess with his/her login name and password.

(For the example above, only access to IQ MultiAccess is permitted).



- The location manager has only access to his/her location in IQ MultiAccess. Within the location, he/she has all rights assigned to him/her.

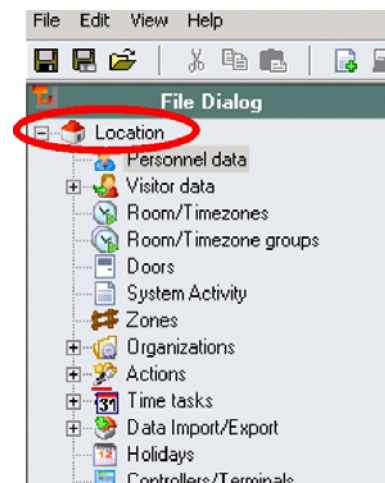


If a person requires access to several locations, he/she must be defined as location manager for all individual locations.

Alternatively he/she can be created as a **system manager** who has access to all locations but no rights in IQ NetEdit.

All operators who have access to common areas have **equal rights** (superusers, personnel managers and location managers).

Whoever is the first to process a data record, can save the modification. All other operators who are processing the same record at the same time will get the message that they are at the moment not entitled to modify/save this data record when they try to save their modifications.



### 8.1.4 System manager

A system manager is something like a superuser without IQ NetEdit authorization. They can only be created globally and not within a location. All other settings correspond to a location manager.

### 8.1.5 Shadow manager

By help of these special type of managers several mandators can have access to collective doors, or can share doors of one ACS-8 controller. For details see chapter 12.

## 9. Definitions of input and output states

The normal condition of the inputs and outputs of the ACS-8 and its components can be defined as "high" or "low" as described in Chapters 4.3.4 and 4.3.7. Thus inverted operation of an input/output is possible.

### 9.1 Outputs:

In normal condition, a relay is usually de-energized, i.e. *low*. If it is energized, it becomes active and triggers a certain event (example: strike with load current function).

In case of a no-load current door strike, the relay is operated invertedly and is activated in the normal condition, i.e. it is defined as "high". If the power supply is interrupted, the relay is de-energized and the door is opened. The escape door control is based on this principle.

Normal condition: This field is only relevant for the ACS-8 and its components.

(The definition of *normal condition* corresponds to the definition of *normal condition* in tab *Inputs*).

This field defines the state in which the output is to be in normal condition.

One of the options shown below can be selected via the scroll-down arrow right of the entry field: This way it is possible to operate a relay invertedly.

- Low: If a relay is e.g. controlled via this output, its normal condition can be defined as *deactivated* with *Low*.
- High: If a relay is e.g. controlled via this output, its normal condition can be defined as *activated* with *High*.

The factory setting is Low.

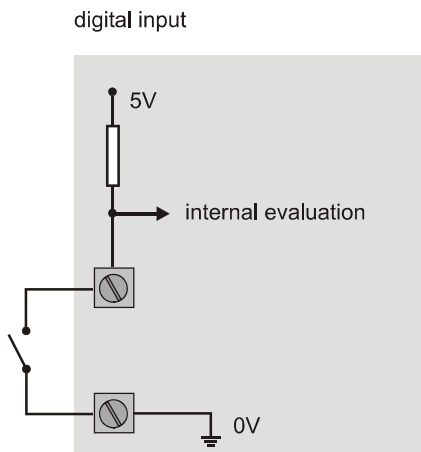
## 9.2 Inputs

**Normal condition:** This field is only relevant for the ACS-8 and its components.

(The definition of normal condition corresponds to the definition of normal condition in tab *Outputs*).

This field defines the state in which the input is to be in normal condition. For the ACS-8 and its components, the state open/closed no longer exists, it has been replaced by *high/low*.

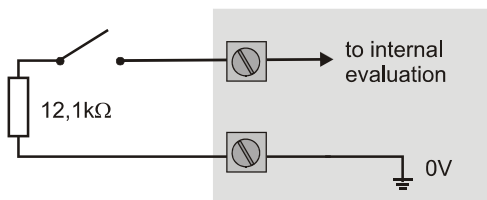
Which state is defined as normal condition is shown in the table below:



Switch	Normal operation (=factory setting)	Inverted
open	0 = low	1 = high
closed	1 = high	0 = low

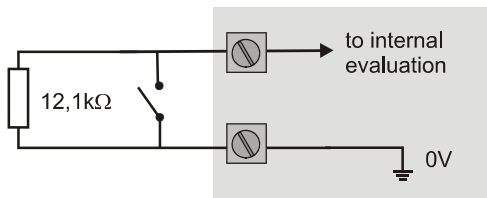
differential alarm line

variant 1:



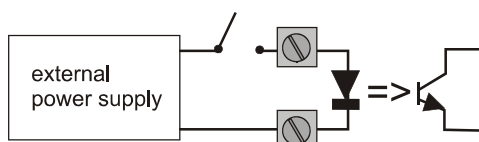
Switch	Normal operation (=factory setting)	Inverted
open	1 = high	0 = low
closed	0 = low	1 = high

variant 2:



Switch	Normal operation (=factory setting)	Inverted
open	0 = low	1 = high
closed	1 = high	0 = low

optocoupler

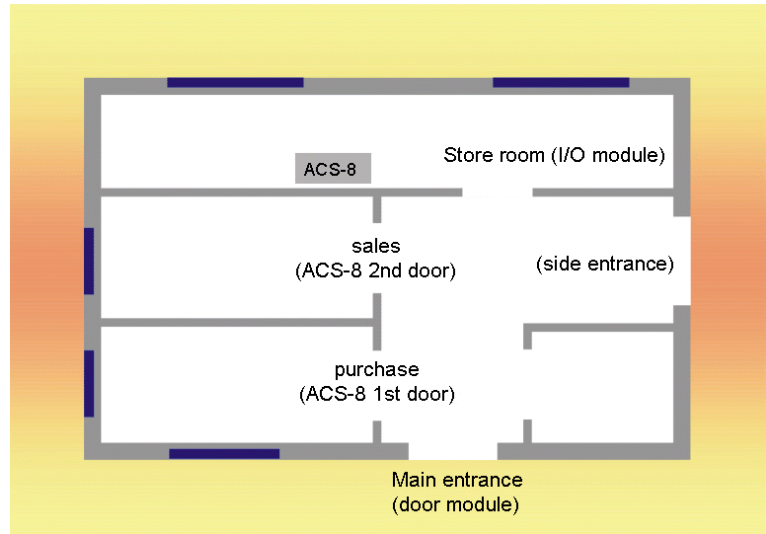


Switch	Normal operation (=factory setting)	Inverted
open	0 = low	1 = high
closed	1 = high	0 = low

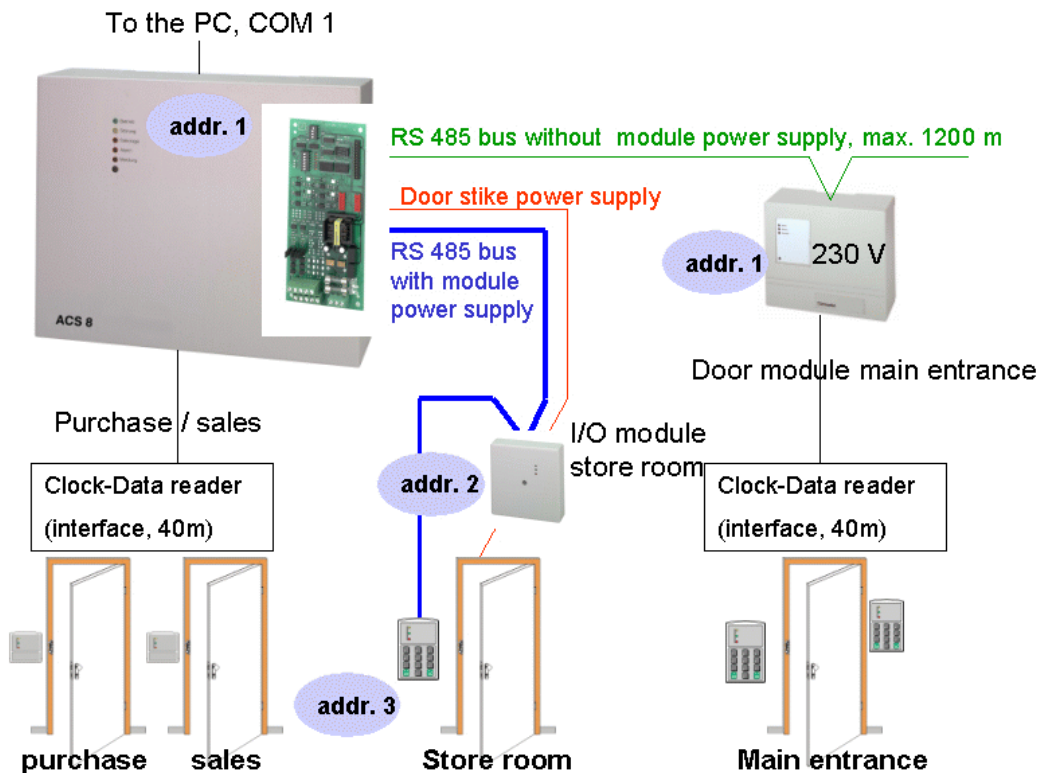
## 10. Functional test and minimum configuration

Some **minimum settings** are required in order to check the correct function of the controllers/terminals installed and their definition in IQ NetEdit.

The following floor plan serves as model installation for the descriptions in the following sections:



This results in the following hardware configuration:



For reasons of simplicity, we use only **one** location in the following examples. When working with several locations, you have to carry out the steps described for each location - unless deviating instructions are given.

## 10.1 Procedure



**Immediately after the installation, IQ NetEdit can only be started on the server!**

1. Start IQ NetEdit:  
User name: service  
Password: novar  
Server: localhost or 127.0.0.1  
Server Identification: no input.
2. Input of the entries for **Global settings**. They are valid as default settings for all further locations, but they can be modified per each location.

Common | Key code

Type: Global settings

FTP port

David API path

David sender

Delayed factory reset

Time

Common | Key code

Type: Global settings

Allow double PINs

No duress code

Add for Duress code

Keycode length

Check **Add for duress code** and **Keycode length** and enter according to customer's requirements. These data can be entered at two different places. The **Global settings** entries are used as default settings of the complete system for creating new locations. They can be modified within each location.

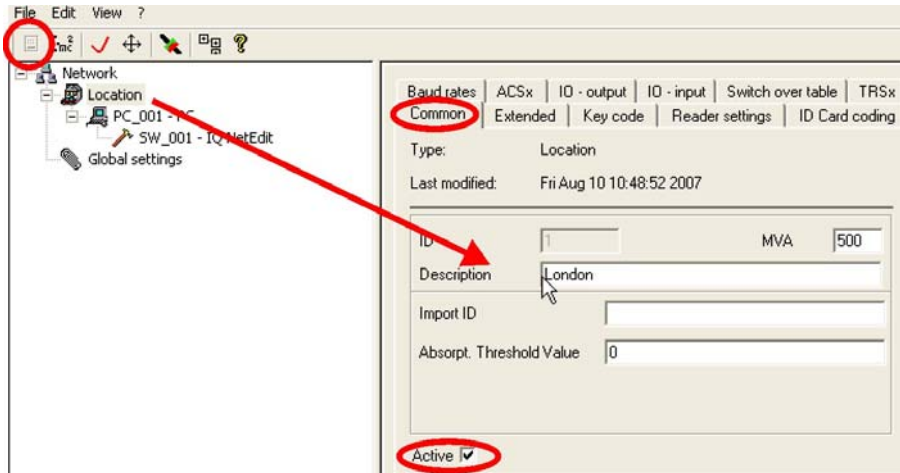
In addition, the keycode length entry is used for suggestions of automatic PINs and to check for duplicate PINs and collisions of PIN and duress code (see user manual).

### Caution!

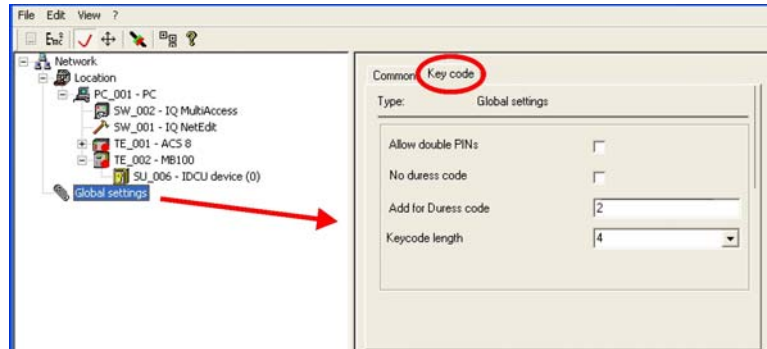
If once personnel data are entered, the number for duress code addition can no more be changed (very important for IACP-connection).

A modification of the keycode length from 4 digits to a higher number of digits is allowed, but it is not possible to change from a higher number of digits back to a lower number of digits<sup>9</sup>.

3. Specify location

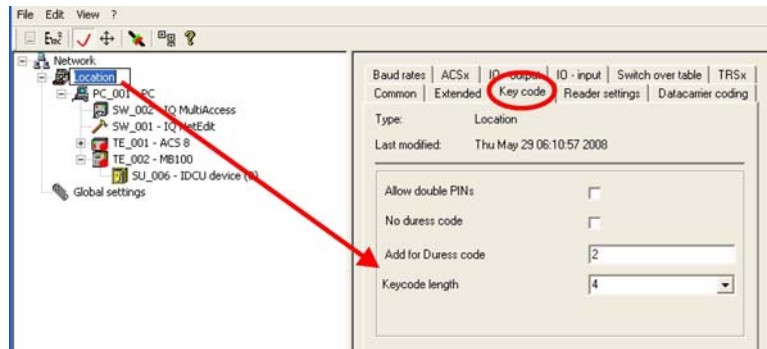


If the location's settings of the **keycode** tab deviate from the global settings, they must be changed in the location.



**Note!**

As soon as personnel data have been entered, it is no longer possible to change the additional number for the duress code. A modification of the keycode length from 4 digits to a higher number of digits is allowed, but it is not possible to change from a higher number of digits back to a lower number of digits<sup>10</sup>.



**Reason:**

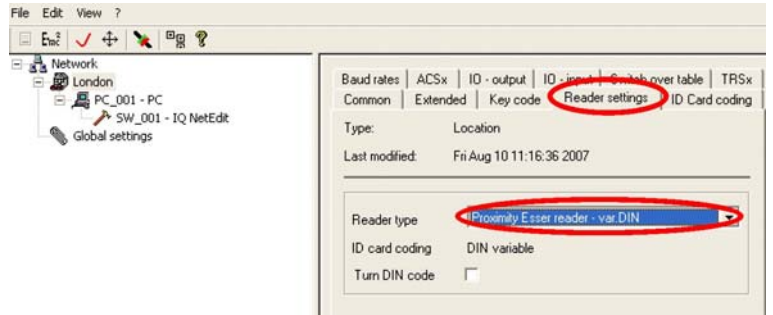
This could lead to a situation where PINs exist twice or "normal" PINs and duress codes coincide. Corresponding messages are displayed on the screen.

<sup>10</sup>

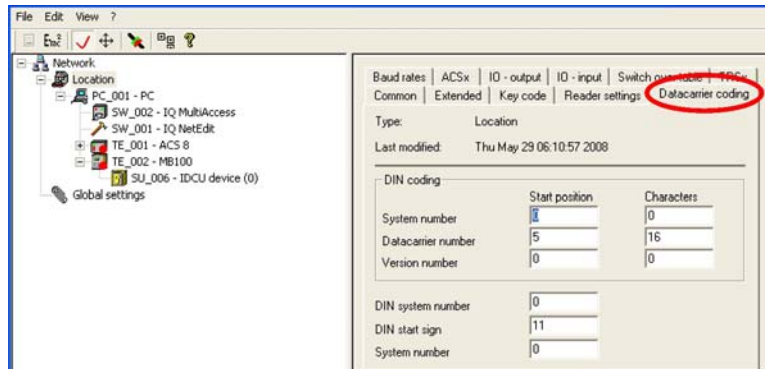
This restriction also applies when a door code is used.



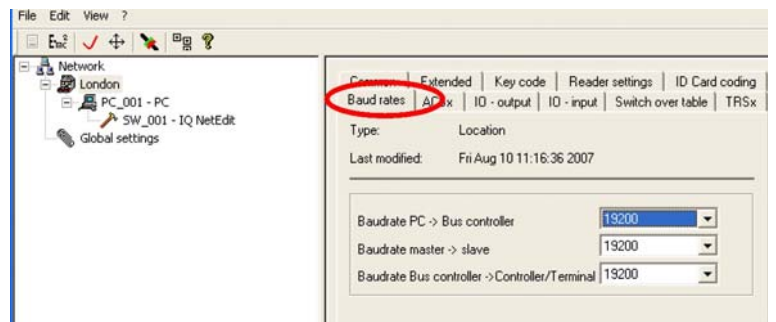
4. Enter the reader settings according to the reading method used. In our example we use DIN-coded, proximity Esser readers.



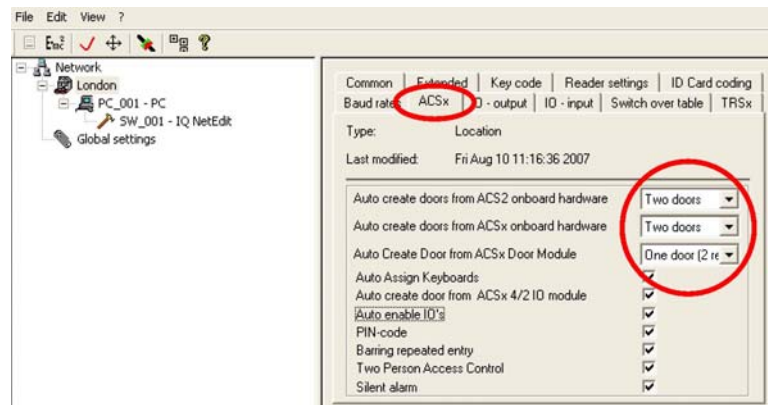
5. Set data carrier coding according to the reader type used (see also chapter 5.13). The data carriers used in our example correspond to the factory setting.



6. Check/set baudrate(s). In our example, the ACS-8 is connected to COM1 of the computer via an interface converter. That means a baudrate of 19200 from the PC to the bus controller (in this case, the interface converter is the bus controller). The setting "master-slave" is not relevant in this case. The setting "bus controller - controller / terminal" can remain as set in the factory (19200).

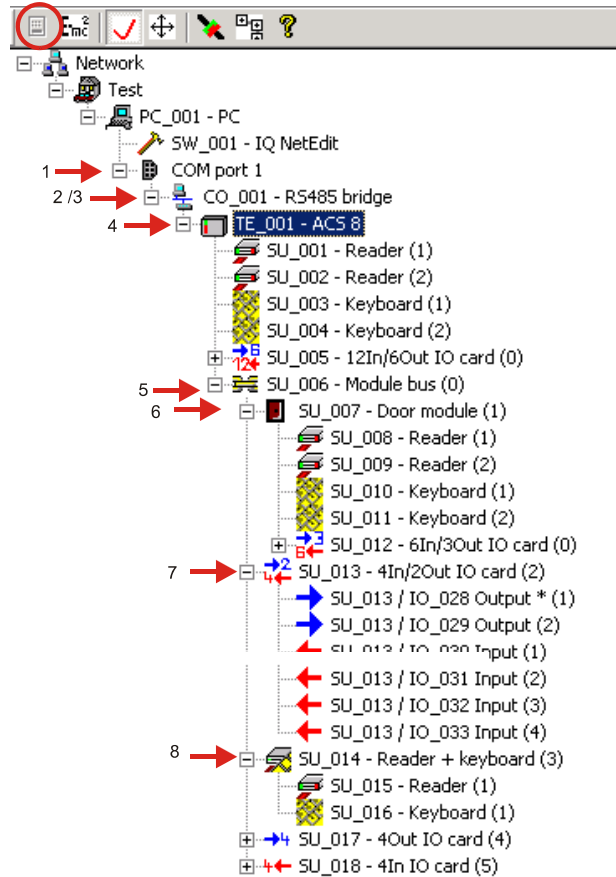


7. According to our hardware installation, the following definitions are to be made automatically when the controllers / terminals are configured:
  - 2 doors from the ACS-8 onboard hardware
  - 1 door with 2 readers from the door module
  - keyboards
  - 1 door from I/O module
  - all inputs/outputs are to be activated

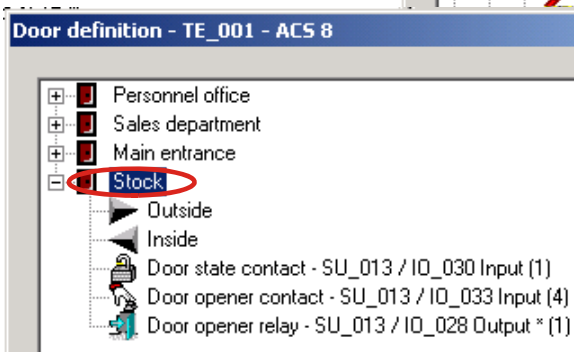
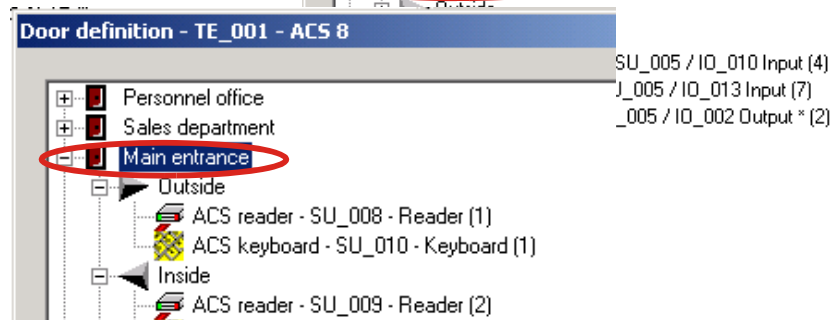
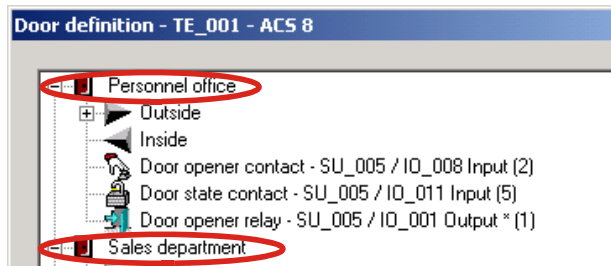


The other settings are not relevant for this purpose, but the factory settings should be maintained since they apply to **all** controllers / terminals of the location concerned.

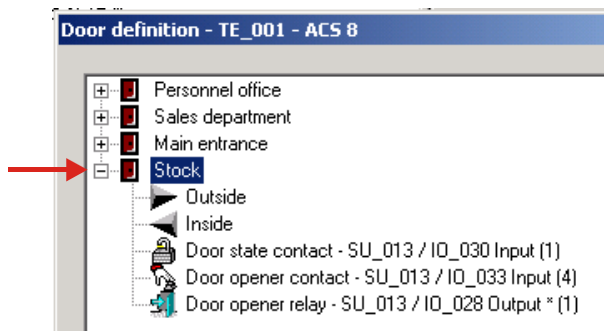
8. 1 = Insert COM1 at a workstation.
- 2 = Insert interface converter at COM1 and activate it.
- 3 = Right-click on interface converter → Scan for controllers / terminals.
- 4 = Activate the ACS-8 that is found.
- At the ACS-8, the following components are found:
- 5 = Module bus with
- 6 = Door module
- 7 = I/O module
- 8 = Bus reader with keyboard



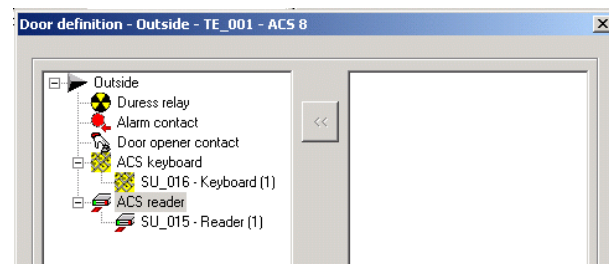
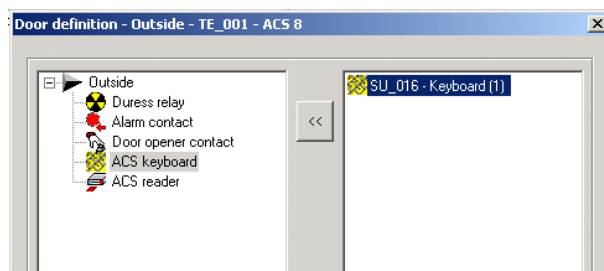
9. Name doors via → **Door definition.**  
The readers, keyboards and inputs/outputs have been defined automatically according to the default settings.



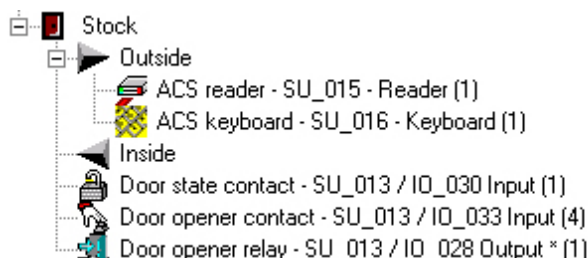
- 10. Reader and keyboard must be assigned manually to the stock room door at the I/O module. Only door state contact, door strike contact and door strike relay can be assigned automatically.



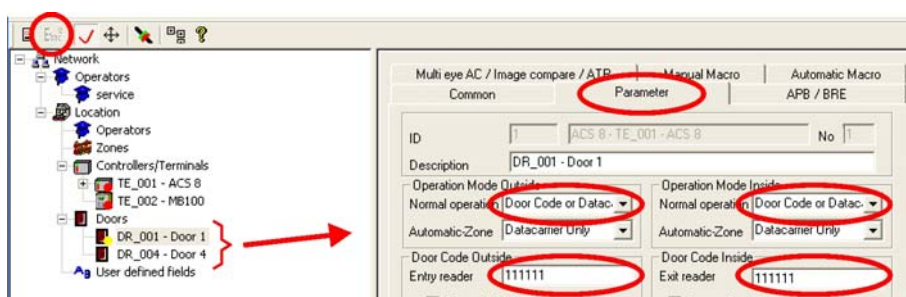
- 11. Right-click on **Outside** → edit
- 12. Left-click on keyboard in the left window.
- 13. Select the desired keyboard in the right window and assign it with **↵** (In our example, there is only one keyboard).
- 14. Repeat steps 11 and 12 for the reader.



- 15. → Finish produces the following result:



- 16. Since there are also keyboards, a key code can be entered for each door for test purposes. To this end, all doors (door sides) are set to **Data carrier or door code**.

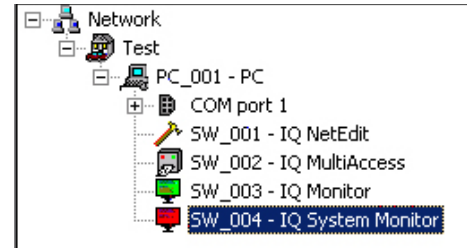


**Note!** These settings, including the key code, must be reset after the test has been successfully completed, since otherwise everybody knowing the test data can gain access.

17. Assign the IQ MultiAccess software to the test PC. In our example, the programs IQ Monitor and IQ System Monitor have also been assigned.
18. Exit from IQ NetEdit.



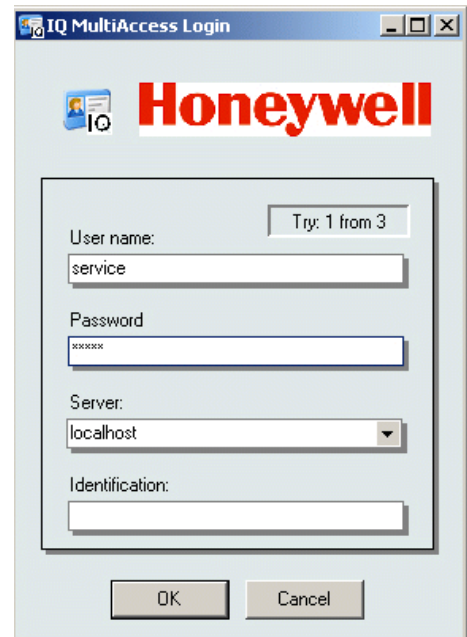
The controllers/terminals which were modified are automatically bootstrapped and parameterized in the process. The doors concerned are out of function as long as this takes place (enter a start time for → **delayed factory reset** if necessary, cf. chapters 3.3.2 and 5.3).



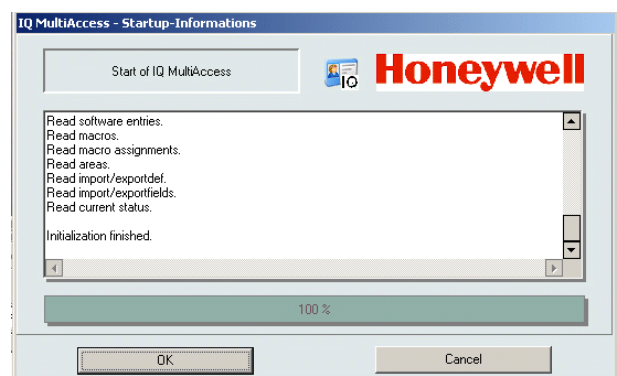
This process is displayed in program IQ System Monitor:

Time	Location	Source	Message	Info A	Info B
10:46:45	Test	SW_004 - IQ System Monitor	IQ SystemMonitor connected	SUPPORT-TRS45	
10:46:49	Test	SW_001 - IQ NetEdit	IQ NetEdit disconnected	SUPPORT-TRS45	SuperUser ID=1
10:46:49	Test	TE_001 - ACS 8	Data preparation finished	0.11 secs	
10:46:50	Test	TE_001 - ACS 8	Load data started		
10:47:50	Test	TE_001 - ACS 8	Load data finished		

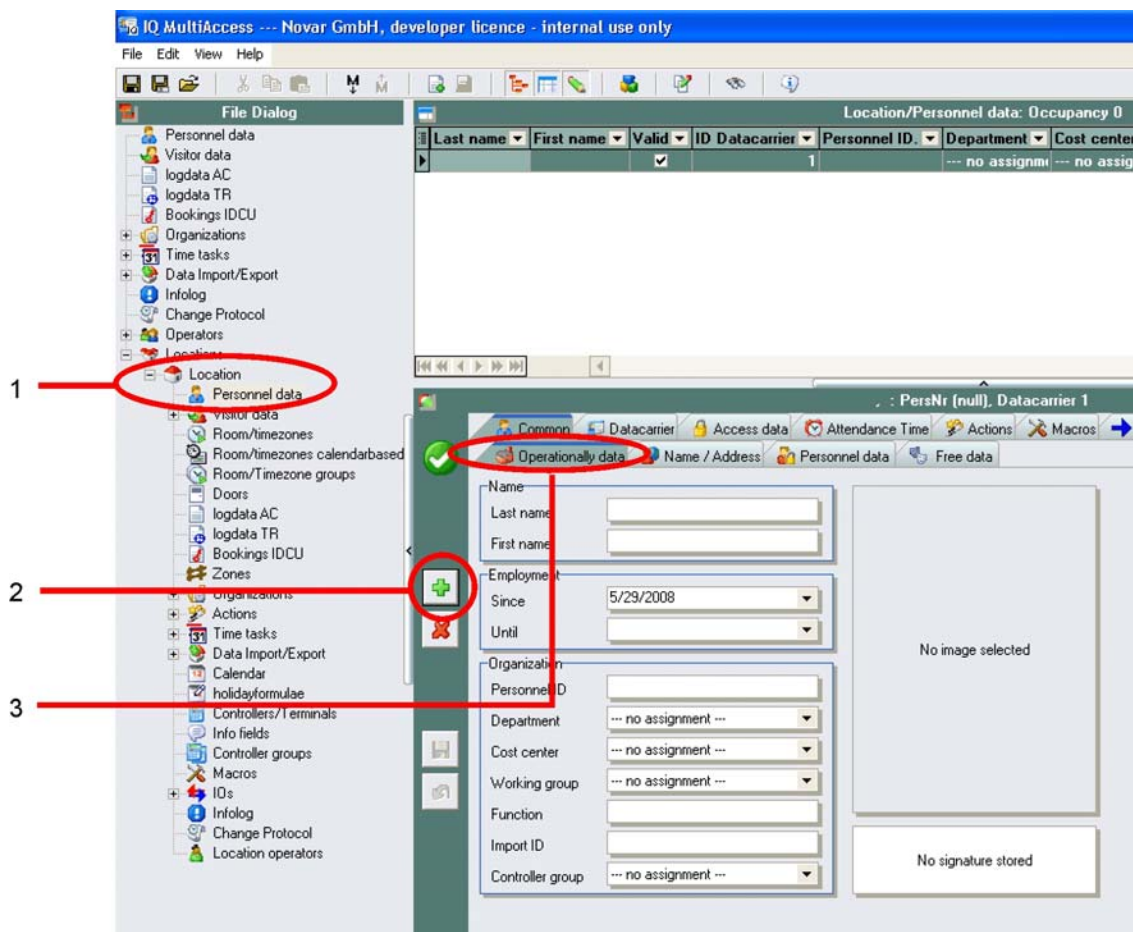
19. Start IQ MultiAccess. Since only user **service** exists for the time being and the programs are installed on a local computer, the default settings can be applied with **OK**.



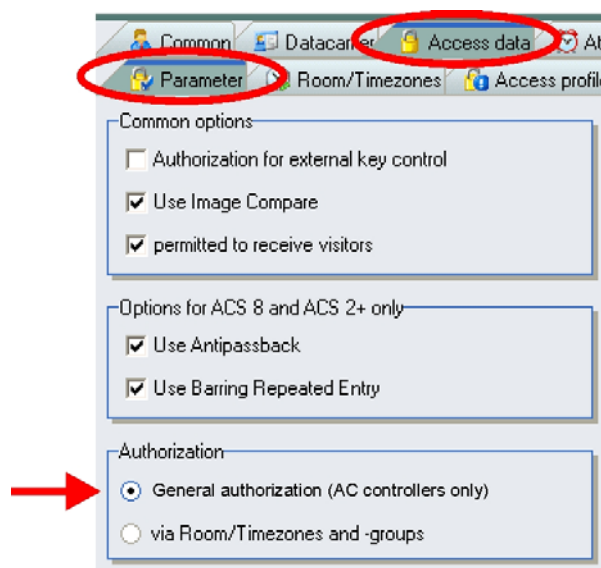
20. The processes required during start are displayed for a certain time. This window can, however, be closed with **OK**.



- 21. 1 = Select the desired location → the desired PC → personnel data in the file dialog window.
- 2 = Click on the “+” in the empty Pers. Window.
- 3 = Make at least **one** entry in tab **Operational Data** (e.g. name: test).



- 22. Activate → **General authorization** in tab **Access data** → **Parameter**




23. Enter the card coding in tab **Card data**.

The 20-digit badgecode of the individual card can be found in form of a label on the rear side of the card.

IK	4310162736
ZK	0800000014 0711110012
TYP	026370.00 26.04.2001

← Badgecode:  
08000000140711110012

Due to the system parameters definition (cf. step 15), this number will be read as of the 5th digit.

24. Save entries with 

25. Create time tasks for data backup and loading holidays (see user manual).

## 10.2 Booking with test ID card



It is generally recommended to activate programs → **IQ Monitor** and → **IQ SyMonitor** during the installation - or at least for testing and/or troubleshooting - , since their displays provide valuable information on correct / incorrect working and internal processes of the system (error messages etc.).

If the booking causes a door release, all settings are correct.

If no release is obtained, repeat all steps one by one.

Frequent faults during commissioning:

- ⊗ wrong system number (system data - system parameters , cf. step 15)
- ⊗ reader / keyboard assigned to wrong door side (cf. step 9ff).
- ⊗ wrong reader settings (default values for location (cf. steps 3 and 5).



It is recommended to document the current configuration.

1. For the entire installation:  
Right-click on **Network** → **Print door list**
2. Per controller/terminal:  
Right-click on controller/terminal → **Print door definition**

## 10.3 Troubleshooting

### External bus controller

- ✓ Shortly interrupt the mains supply on the bus controller. The red LED briefly lights up, then it starts flickering.
- ✓ Have the bus controllers been bootstrapped (cf. Installer Instruction for the bus controller)?
- ✓ The DIP switches in the bus controller must be set to the same baudrate as entered in *IQ NetEdit* (manually or default).
- ✓ Check whether the interfaces are connected properly and the jumpers are set correctly (J4 on the bus controller CPU and jumpers on the interfaces - cf. the relevant Installer Instructions).
- ✓ Does the COM interface where the bus controller is connected correspond to the one that is entered in *IQ NetEdit*?
- ✓ Check cables / pin assignments.

### ACS-1

- ✓ Has the ACS-1 been bootstrapped via DIP switch (cf. Installer Instructions ACS-1)?
- ✓ Check ACS-1 voltage supply.
- ✓ Does the address correspond to the entry in *IQ NetEdit*?
- ✓ Does the baudrate correspond to the entry in *IQ NetEdit*?
- ✓ Is the controller activated in *IQ NetEdit*?
- ✓ Check interface compatibility / interface wiring (cf. documentation for the interfaces used).

ACS-2 / ACS-8

- ✓ Has the ACS-2 / ACS-8 been bootstrapped via DIP switch or initialized via Setup (cf. Installer Instructions ACS-2 / ACS-8)?
- ✓ Check ACS-2 / ACS-8 voltage supply.
- ✓ Does the address correspond to the entry in *IQ NetEdit*?
- ✓ Does the baudrate correspond to the entry in *IQ NetEdit*?
- ✓ Is the controller activated in *IQ NetEdit*?
- ✓ Check interface compatibility / interface wiring (cf. documentation for the interfaces used).
- ✓ Is the correct protocol for the connection set (cf. Installer Instructions ACS-2 / ACS-8)?

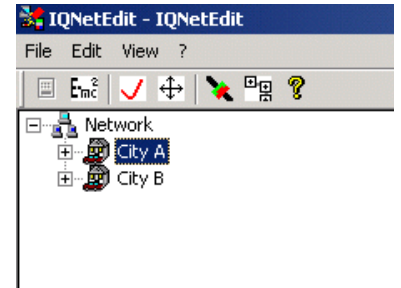


## 11. Several locations

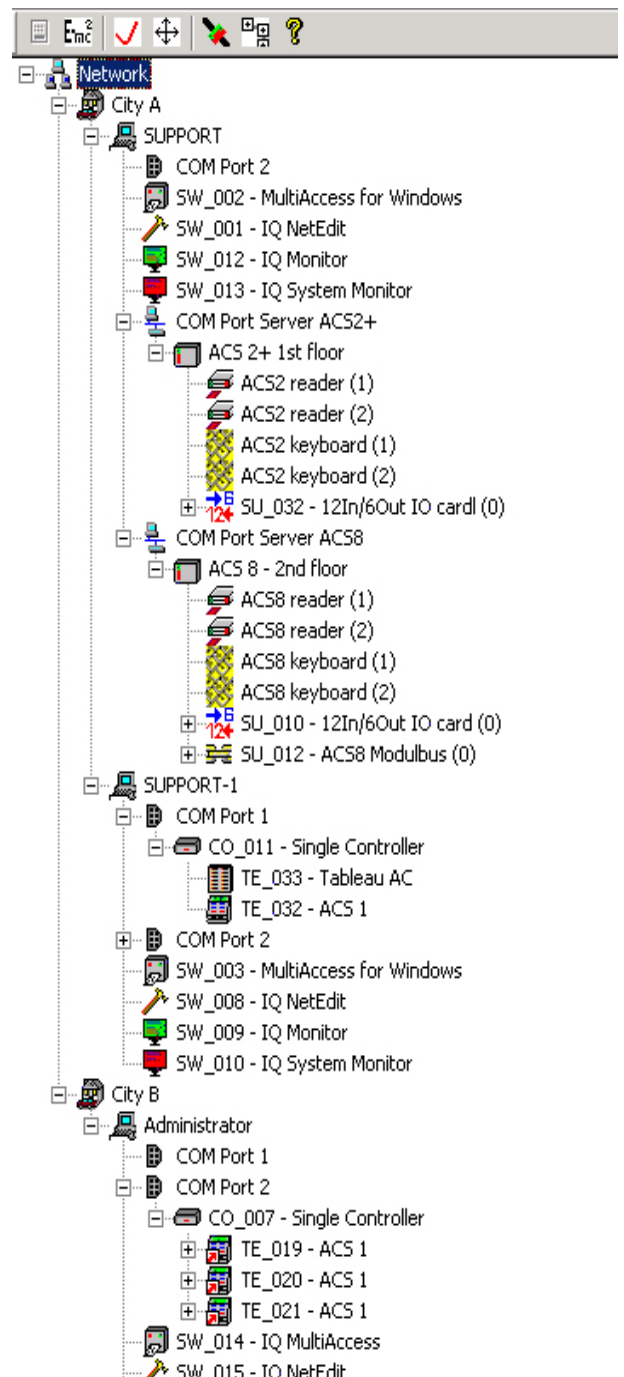
Via the **Location** function, it is possible to manage several locations of a company (clients) or several companies (clients).

**Example 1:** A company has 2 locations (City A and City B). These are linked by means of a dedicated line.

1. Insert the two locations (according to 6.1.2).



2. Define the available hardware and software per location.

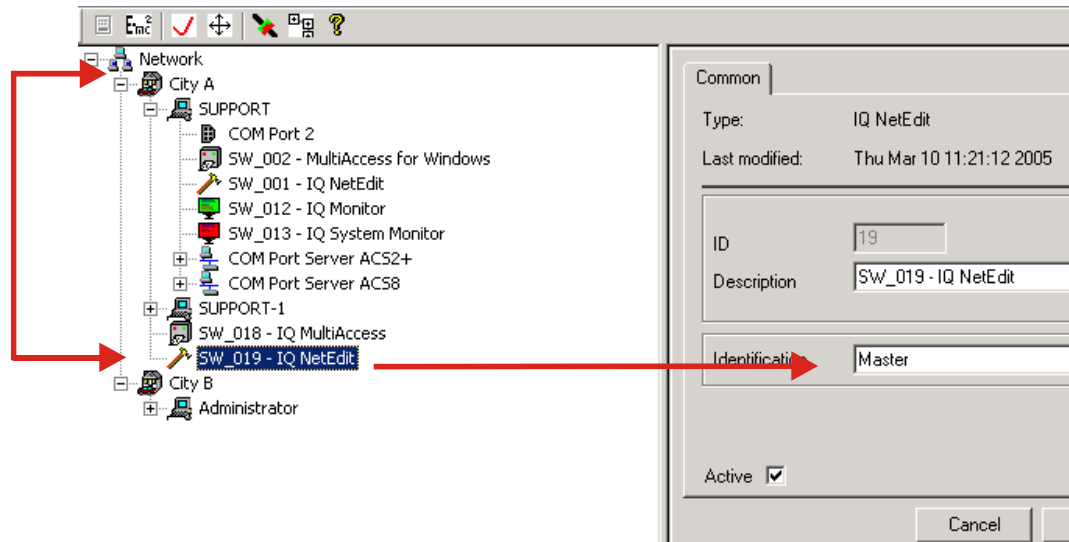


The hardware has been distributed onto the computers where it is actually connected and/or from where it is controlled.

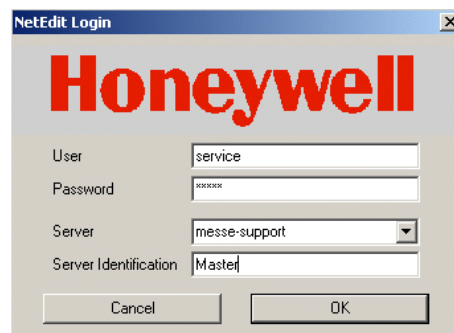
As far as the software assignment is concerned, IQ MultiAccess has been assigned to each computer used for working in the program.

IQ NetEdit has been assigned only to the **Server** and **Administrator** computers.

In addition, programs IQ MultiAccess and IQ NetEdit have been assigned directly to the location via entry of an identification.



This has the effect that an operator who knows the identification can log in from any computer where IQ MultiAccess is installed, even if the software has not been assigned to this computer.



In addition to the user name and the password, the IP address or the computer name of the server and the software identification are to be entered in the login screen.



Workstation with client installation. Login at server with IP address 169.254.177.160 and software identification "master" as defined in "free-driven" software.

Server with IP address 169.254.177.160

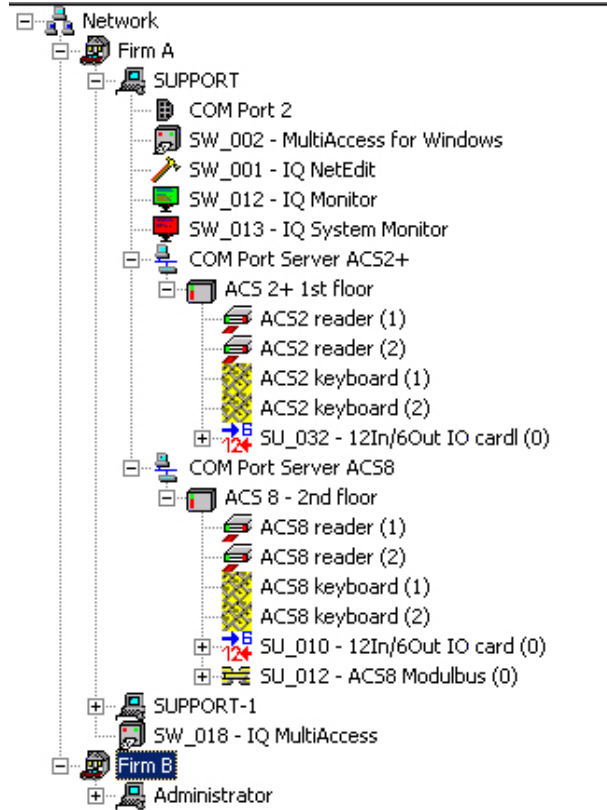
Thus the security level is of course lower than in cases where login is only possible from a computer to which the program has been assigned locally. This version, however, has the advantage that you don't have to go to the site of the computer concerned for each setting / check (which might mean considerable distances in large networks). This "free-driven" access right is advisable in particular during the installation phase, afterwards it should be deleted.

In our example, an authorized operator can access the IQ-NetEdit settings of City B from City A without having to be on site and vice versa.

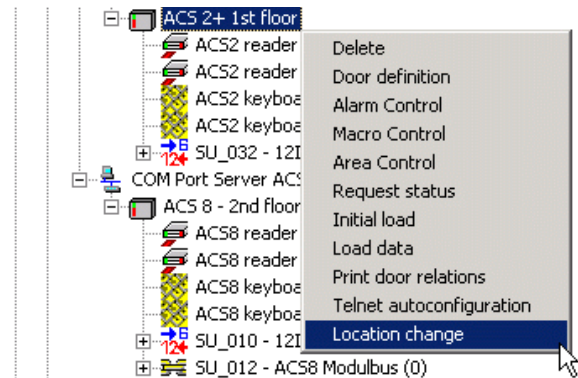
3. The remaining data are defined per location as described above.

**Example 2:** Hardware is logically and physically assigned to different locations.

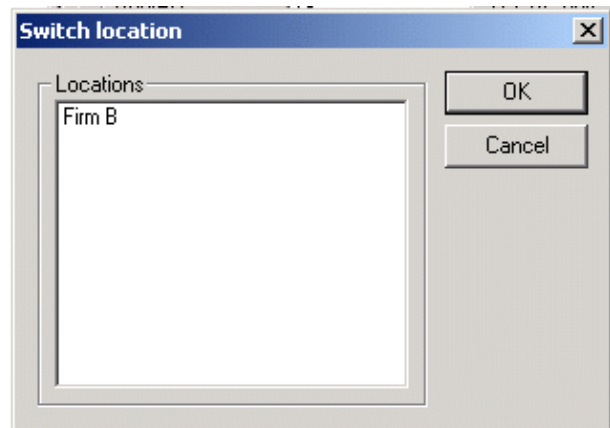
1. In our example, Firm A and Firm B share access control. The complete hardware is connected to a computer which is physically installed in Firm A. Firm B has no hardware assigned to it physically.




2. Right-click on the controller / terminal which belongs logically to Firm B → Location change.

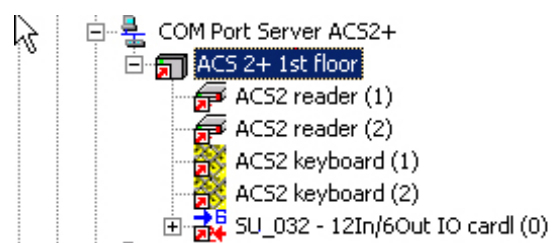



3. All locations (except for one's own) are displayed. In our example, there is only Firm B apart from Firm A.

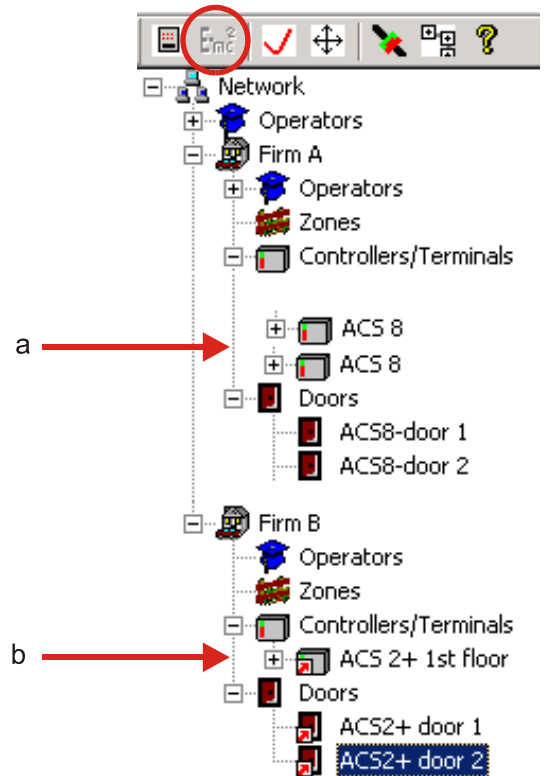


4. Select the location to which the hardware is to be assigned logically → OK.

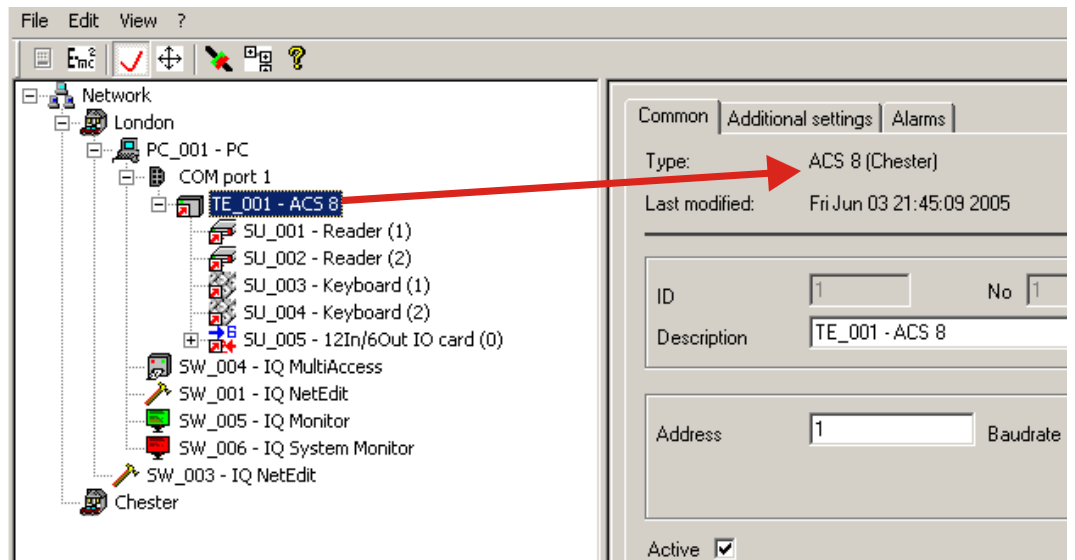
5. The hardware which has logically been assigned to another location, is marked with a .



- The logical representation shows that Firm A manages two controllers / terminals with corresponding doors (a), and Firm B one controller / terminal (b), although it is not connected physically there (represented by )



To which other location a controller/terminal is logically assigned is shown in tab **→ Common** after Type. If logical and physical assignment are identical, only the controller/terminal type is displayed here.



**NOTE!**

As soon as a controller/terminal is logically assigned to another location, the original assignments of this controller/terminal are deleted in the controller/terminal itself as well as in the database (doors, door definitions, room/time zones, actions, cards which have so far been valid for this controller/terminal). This process cannot be reversed. If necessary, the data must be entered again manually. The controller/terminal is parameterized with data of the new logical location. The doors will survive, but they belong to the new location.



## 12. Collective doors used by several mandators

In practice, very often several companies are in one building. This requires for all persons to have access to one or several doors in common (e. g. main entrance, staff entrance, canteen, garage, technic room...) but without access to the data of the other companies.

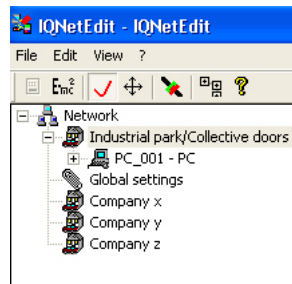
**Preconditions:** IQ MultiAccess V5 or higher  
Multi tenant option  
Latest controller firmware

ACS-2 plus: V07 or higher  
ACS-8: V07 or higher  
ACS-1 03.0V.06.04 or higher  
ACT no support of this function

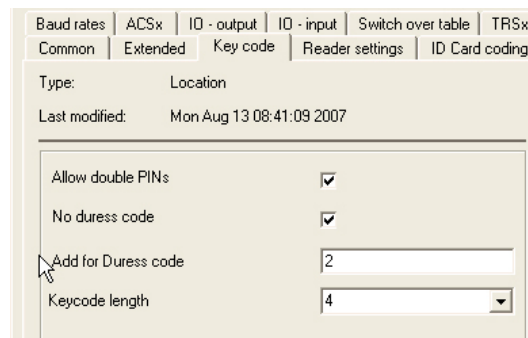
The doors used in common must be controlled by one (or several) separate controller(s).

**Reason:** Only controllers can be allocated to a location, but not individual doors of a controller.

**Realization:** 1. Partitioning of the building into locations. For the doors used in common a separate location is required (in the example called Industrial park/collective doors). For each company a separate location is required.



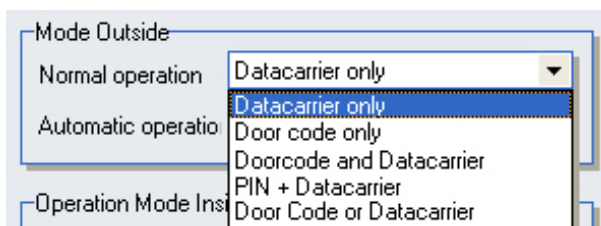
Necessary settings of the collective location (key code tab):



The option → **allow double PINs** must be active.

**Reason:** The same PIN can be used from different people of different companies at these doors (one and the same PIN can exist in several companies).

As a unique identification via PIN code only is not possible, the options **PIN code only** and **PIN code or data carrier** are not available in the door settings. Only by identification via **PIN code and data carrier** the system can identify the person correctly. By input of a PIN only, the system would recognize a valid PIN, but it would not be able to find out the person's identity.



This automatic restriction is not available for IACP doors. They can be set to **PIN only** or **PIN or data carrier** even when they are used by several mandators, which causes no **unambiguous** identification. We recommend not to use one of these settings although available.

The option → **No duress code** must be active.

Reason: By addition of a certain number to the PIN duress codes can result which are normal PINs of persons of other locations. This can only be checked within one location but not access the locations (cf. chapter 5.1 and user manual P32205-20-0G0-xx, chapter 9).



If once those two options are activated, they can no more be deactivated if there are already persons allocated to the location.

The entry in the field → **Add for duress code** can be disregarded as it will not be evaluated in this case.

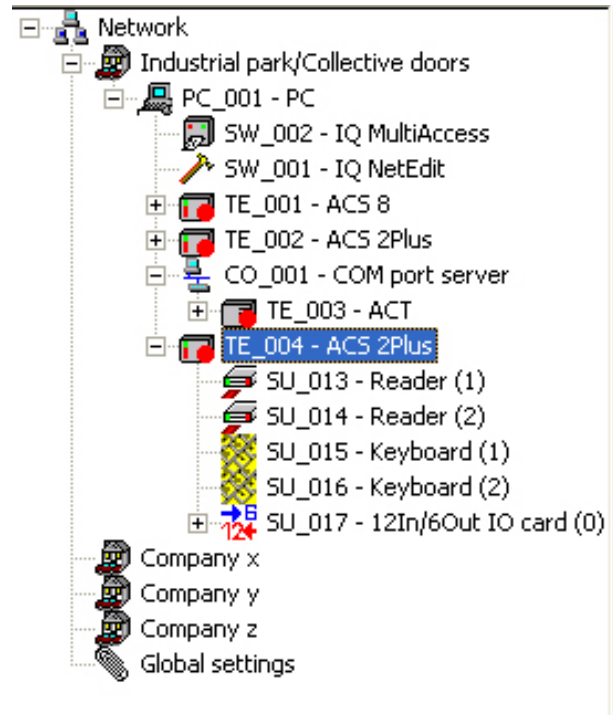


The length of the key code must be identical for **all** involved mandators.

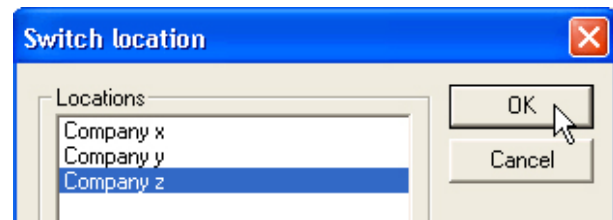
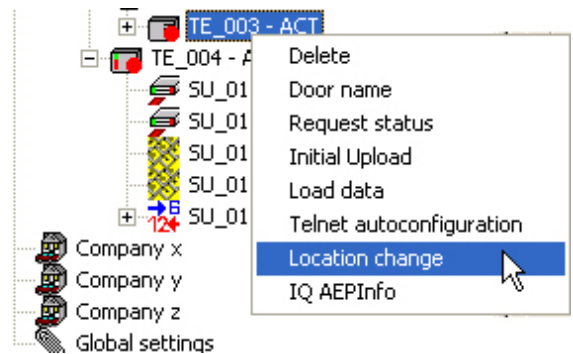
**Caution:** The same requirement exist for connection of an intruder alarm control panel (see chapter 15). In this case the length of **all** key codes must be identical.

Furthermore some agreements are necessary between all participants concerning → **automatic operations** of the doors used by all companies (permanently blocked, permanently open, access criteria), in order not to accidentally abrogate a setting of another company.

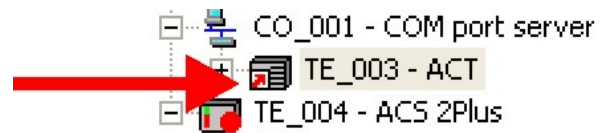
- Define the controller(s) of the collective location according to its/their physical connections as described in details in chapter 6. In our example all controllers are connected via ethernet. The controllers which control the doors of the other companies are here also defined physically. The logical allocation will be done in the next step.



- Logical allocation of the controllers to the locations of which they control their doors (right-click → change location).

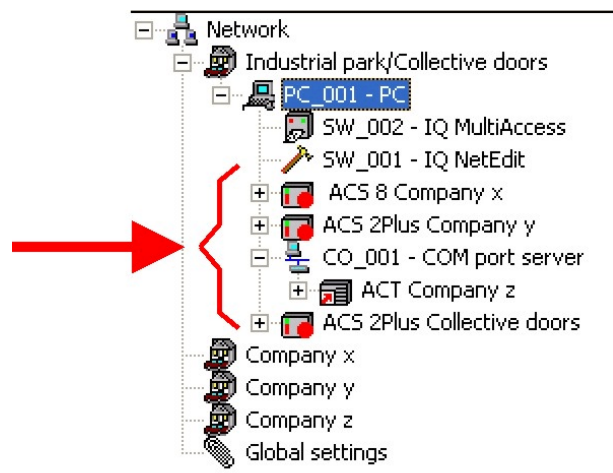


The display changes:



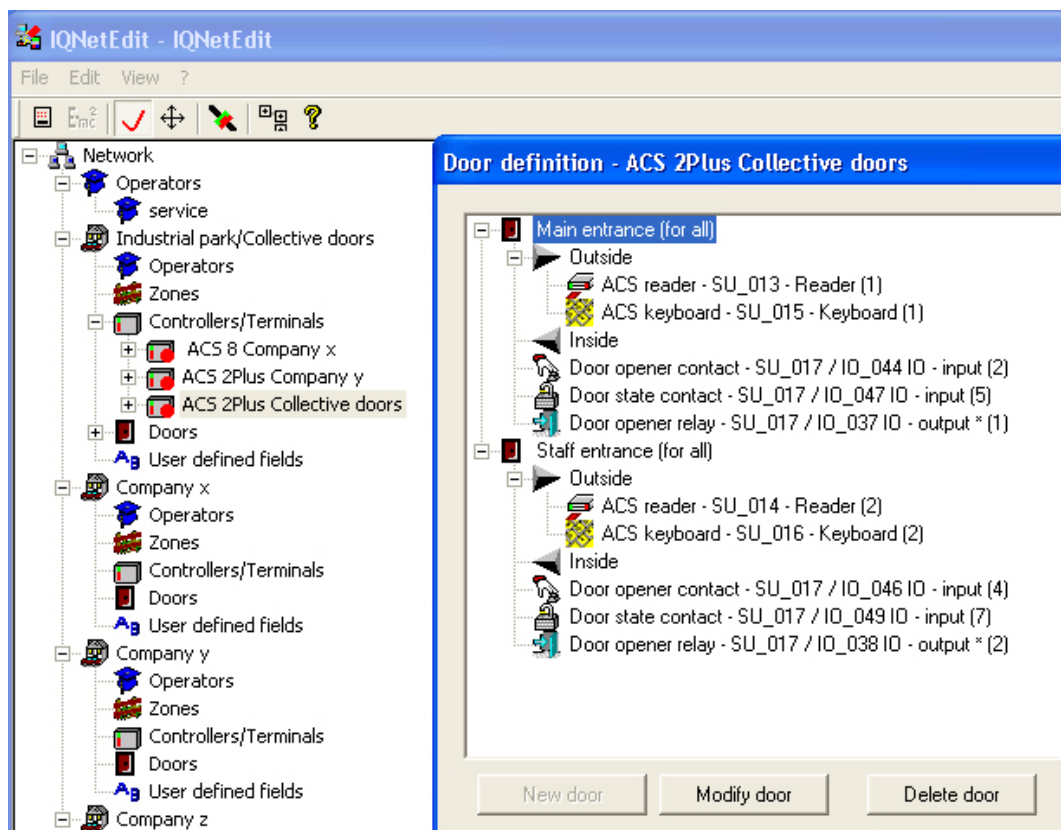


For a better overview it is recommended to give the controllers significant names.

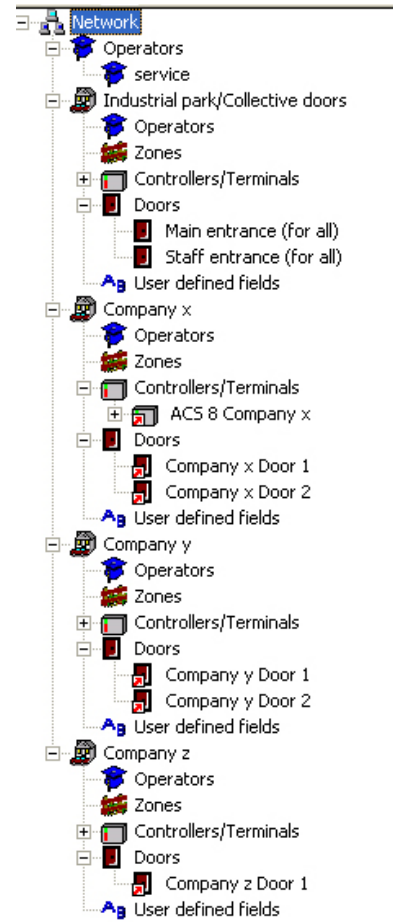


(For details on changes of location assignment see chapter 11).

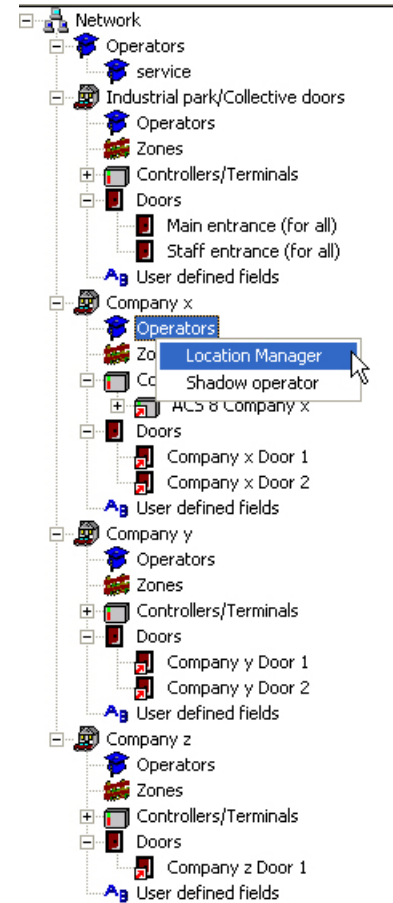
- 4. Define the collective doors in the logical view.



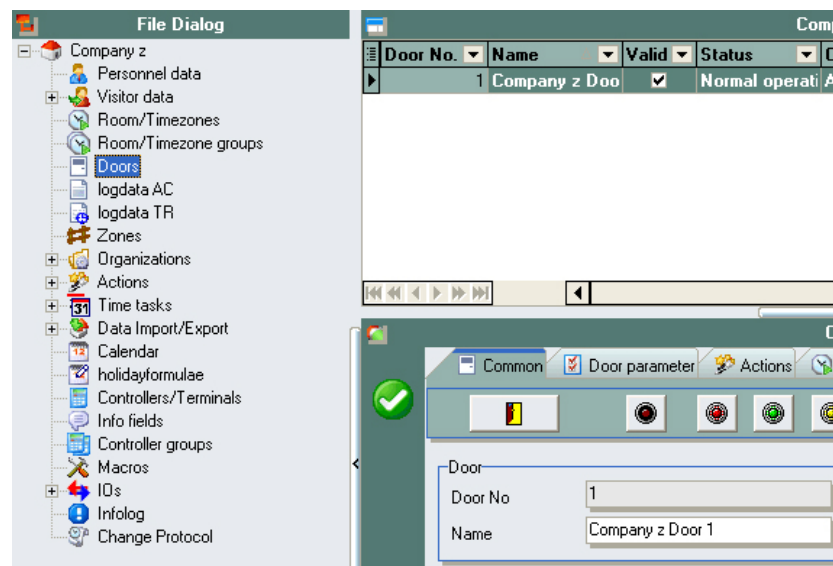
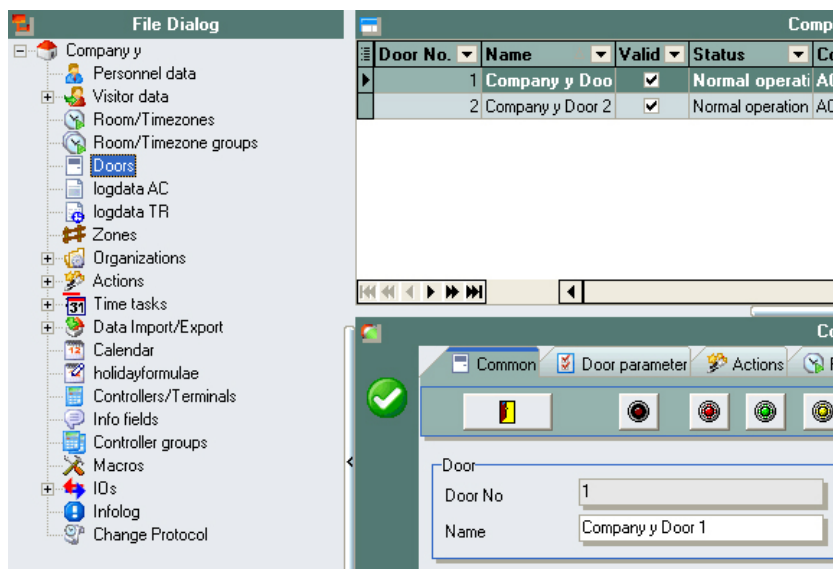
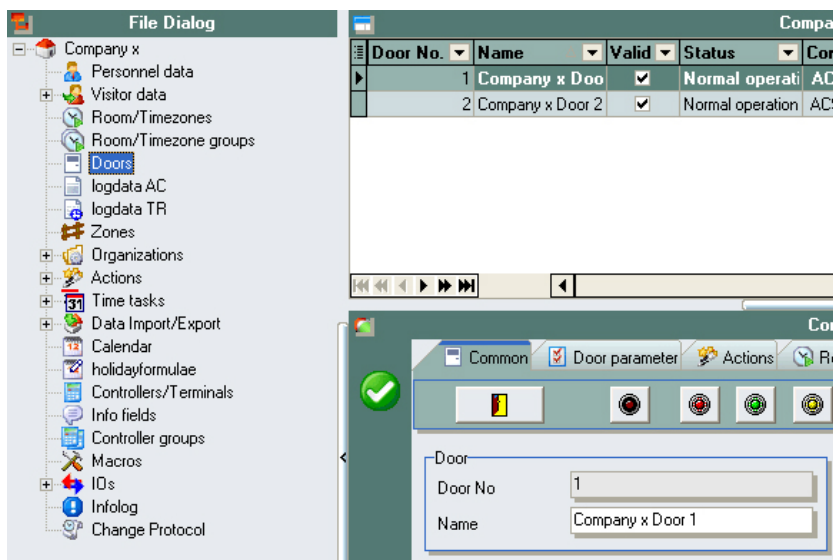
- 5. Create the doors of all companies (locations).



- 6. Create at least one location manager per company.



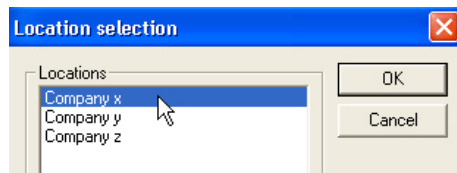
If now a location manager logs in to IQ MultiAccess, he/she sees his/her location only.



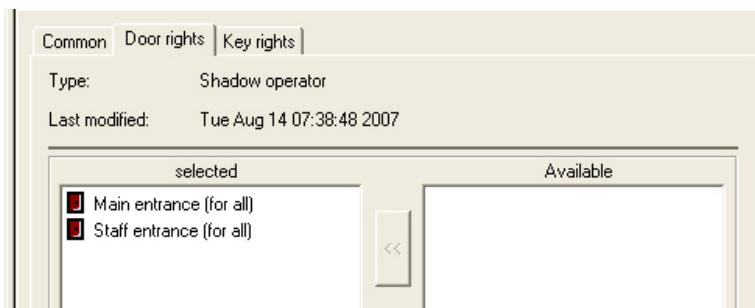
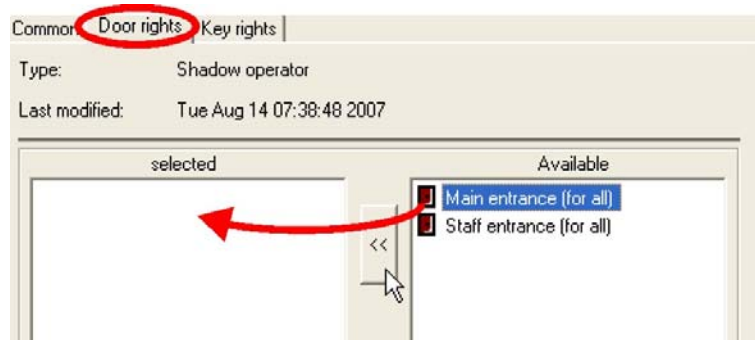
In order to see the collective doors additionally, a “shadow manager” for each location to have access to the collective doors must be created in the collective location.



Select the location to be displayed in addition to the collective location (here: Industrial park/Collective doors).



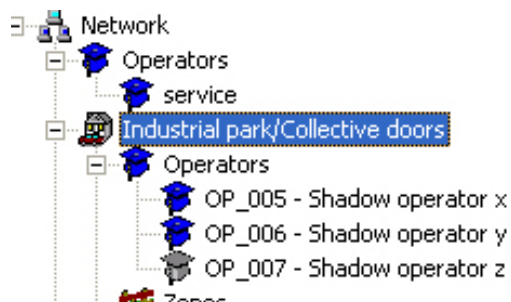
Select the door(s) to have access from the doors available in the **Door rights** tab<sup>11</sup>.



11

Via this selection also doors of **one** controller can be divided between several mandators. Just allocate each mandator the doors they shall have access to.

If once in the collective location there are shadow managers created for all locations...



... the location managers have additional access to the collective location in IQ MultiAccess.



This access exists for all location managers of one location, as the above described allocation is **relating to locations** and not **relating to operators**. The shadow operators can arbitrarily be named (the names need not have to do anything with the actual location they belong to). Important is only the allocation to the location, the collective location has to exist additionally.

### Deleting a shadow operator

This operation is to be used absolutely carefully!

---



#### **Caution! Data loss possible!**

If a shadow operator gets deleted, then **all data** of the location allocated to this operator will be deleted from the database.

---

### 13. Programs supporting the installation

During installation, all data movements between hardware and software can be checked via two separate programs.

The two programs described in the following section are not loaded automatically. They are mainly used by the system administrator for check purposes during the installation, but they can also be started for extended online evaluations.

In contrast to the evaluations within IQ MultiAccess, all bookings / messages are immediately displayed online.



The → **IQ Monitor** and → **IQ SysMonitor** software must be linked directly to a computer in IQ NetEdit. It is not possible to link them as “free driven” software to a location or directly to the network.

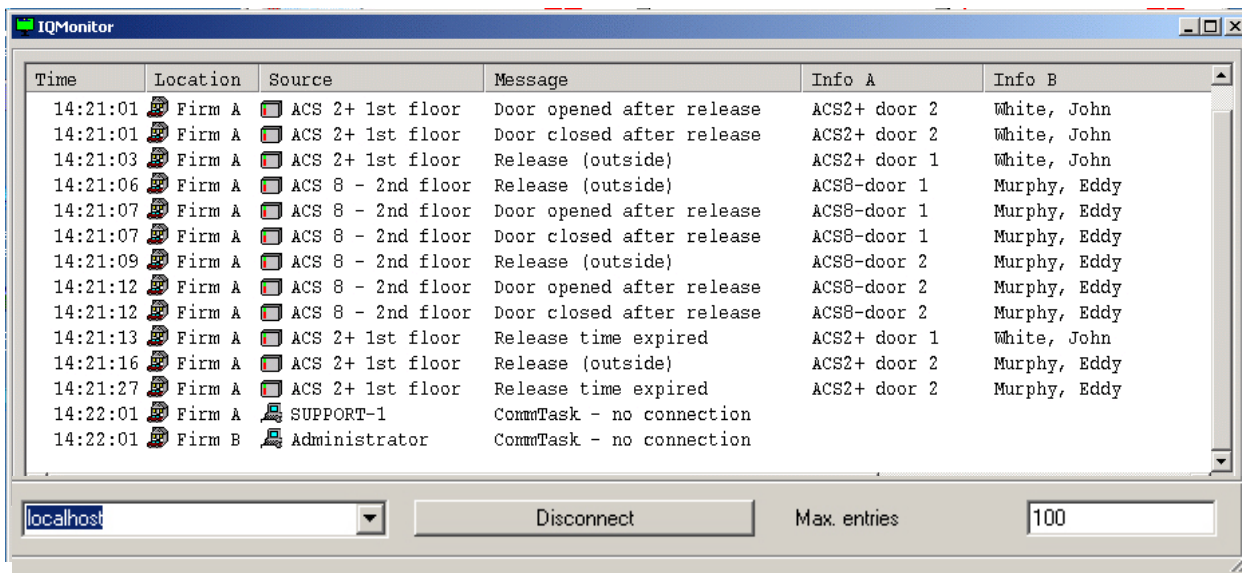
#### 13.1 IQ Monitor

Selection: Start → All Programs → IQ MultiAccess → IQ Monitor

At first, the display window is empty. In the left-hand selection box, you select the server computer (identification of the computer on which program IQ\_Server runs). The data displayed here are provided by IQ\_Server. Thus, an operator who has the relevant rights can check bookings of any client or the entire system from his/her workstation or any other workstation to which the IQ Monitor software is assigned. Then the **Connect** button must be pressed.

The display window is cleared by means of the **Disconnect** button.

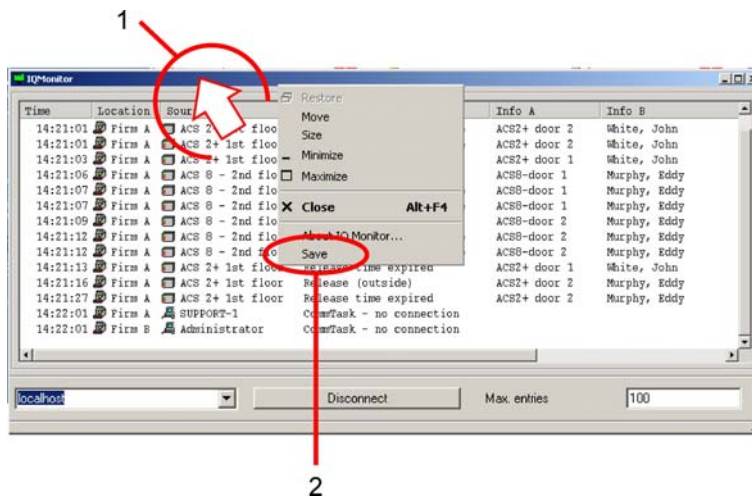
The Connect and Disconnect functions are on the same button with a toggle function, that means either connect or disconnect is active.



In the field **max. entries** you can define how many bookings should be displayed (minimum value = 10, maximum = 2,147,483,647). This amount will automatically be saved.

The data correspond mainly to the bookings described in chapter 13.2.1 of the User Manual.

The current display can be saved via a right-click into the headline.



The file name is IQMonitor.TXT and is located in the directory

...\IQ\_MultiWin\IQ\_Clients\IQ\_Monitor

It can be read for example via the Editor / Note Pad program.



The next saving overwrites the existing file.



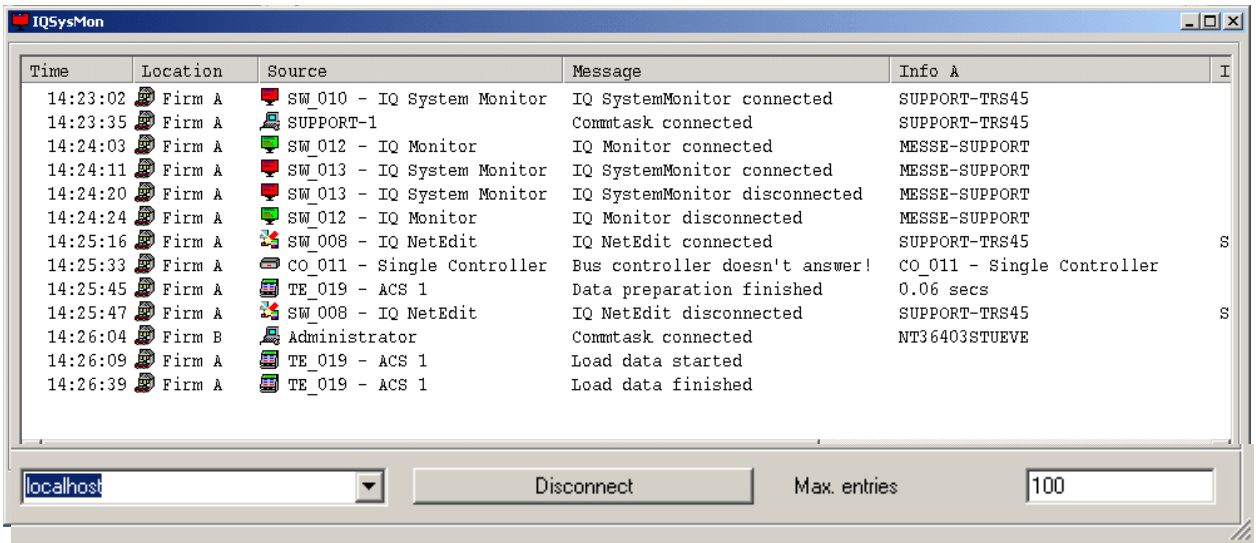
### 13.2 IQ SysMonitor

Selection: Start → All Programs → IQ MultiAccess → IQ SysMonitor

At first, the display window is empty. In the left-hand selection box, you select the server computer (identification of the computer on which program IQ\_Server runs). The data displayed here are provided by IQ\_Server. Thus, an operator who has the relevant rights can check system (error) messages, infos and alarms of any client from his/her workstation or any other workstation to which the IQ SysMonitor software is assigned. Then the **Connect** button must be pressed.

The display window is cleared by means of the **Disconnect** button.

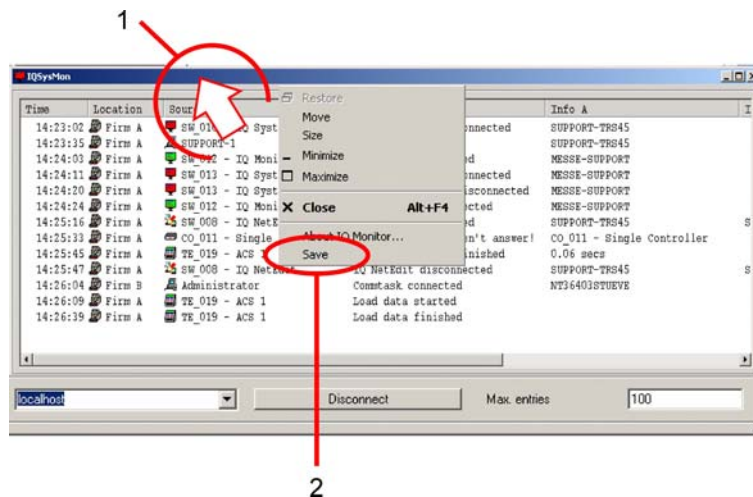
The Connect and Disconnect functions are on the same button with a toggle function, that means either connect or disconnect is active.



In the field **max. entries** you can define how many bookings should be displayed (minimum value = 10, maximum = 2,147,483,647). This amount will automatically be saved.

The data correspond mainly to the messages described in Chapter 13.2.2 of the User Manual.

The current display can be saved via a right-click into the headline.



The file name is IQSysMon.TXT and is located in the directory  
 ...\\IQ\_MultiWin\\IQ\_Clients\\IQ\_Sysmonitor

It can be read for example via the Editor / Note Pad program.

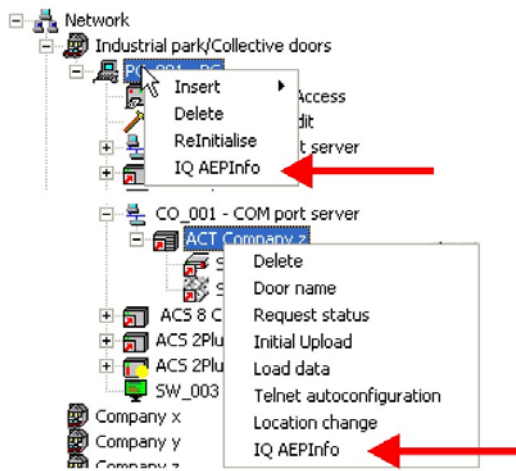


The next saving overwrites the existing file.

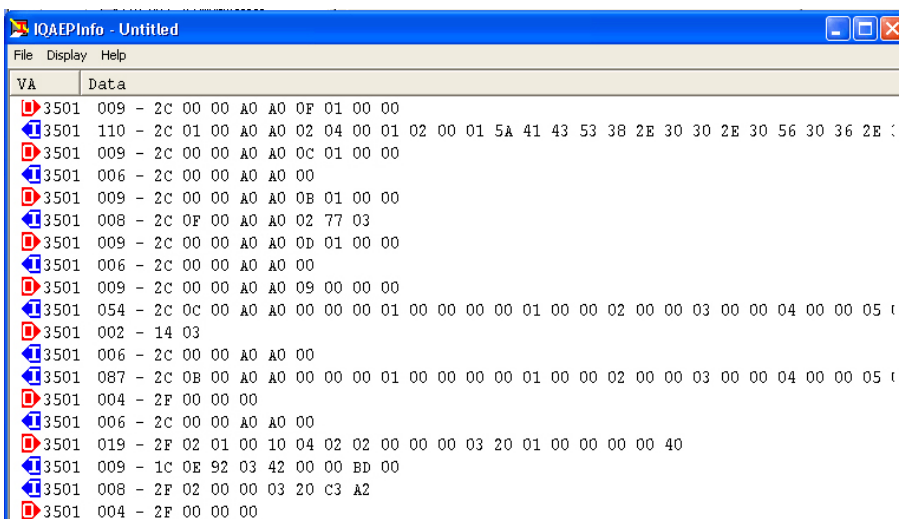
### 13.3 AEPInfo

This tool visualizes the communication between IQ MultiAccess (computer) and a controller. This normally is only required by our support in cases of malfunction.

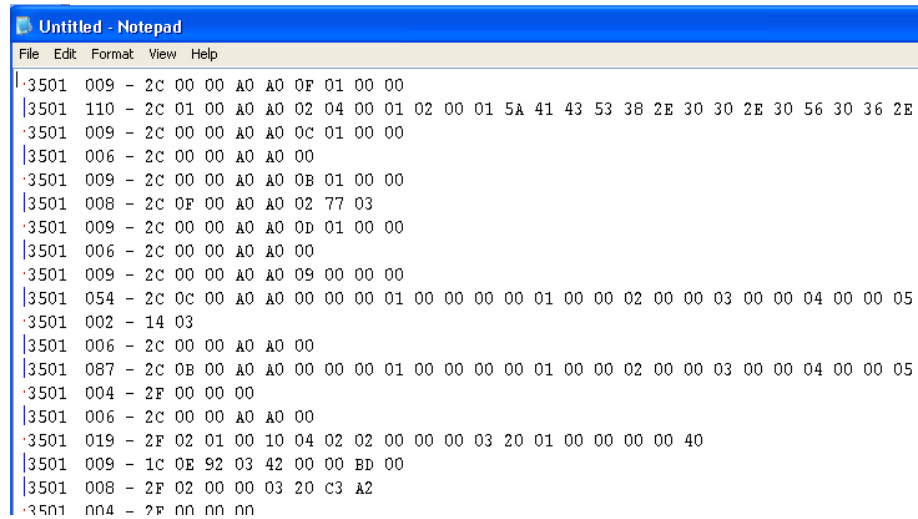
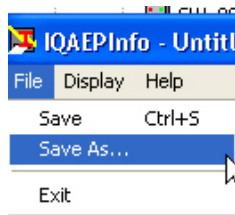
The program can be started at various places by right-click e. g. on a workstation or a controller which is connected via COM-Port server.



The data traffic is displayed as HEX values.



The file can be saved under any name (e. g. as \*.txt) and forwarded to our support for evaluation.



## 14. Additional programs / functions

### 14.1 IQ MultiVPS

The option IQ MultiVPS is a connection of IQ MultiAccess to the VPS card printing system (Video Print Systems). Personnel data from IQ MultiAccess are provided to the VPS system.

The whole process from card layout to finalization is carried out in an IQ MultiVPS user interface which is used for starting the actual card design program.

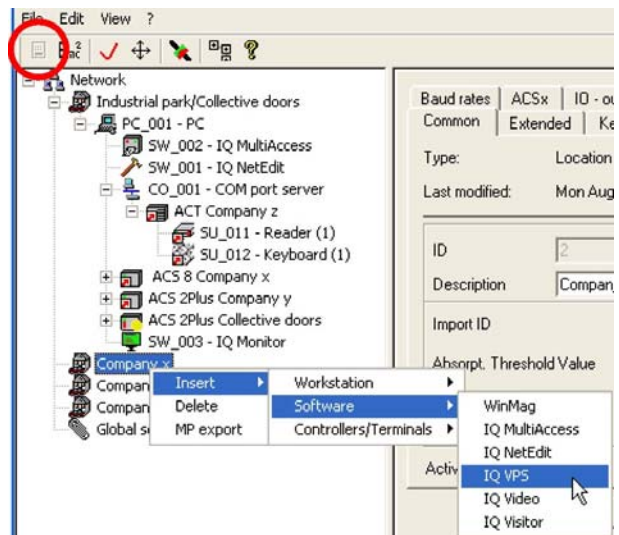
#### 14.1.1 Installation

IQ MultiVPS is installed automatically during the installation process (see Chapter 3) if you either select complete installation or manually select IQ MultiVPS for client installation.

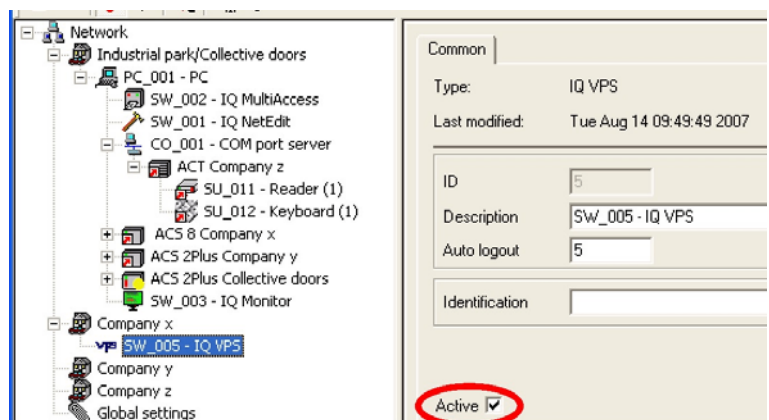
A demo licence for this product is provided and installed together with the installation via IQ MultiAccess. A full licence is to be obtained from V.P.S. For details please see the documentation for the product in question.

#### 14.1.2 Settings in IQ NetEdit:

1. In the hardware configuration, right-click on → Location or → Workstation → Insert → Software → IQ VPS.

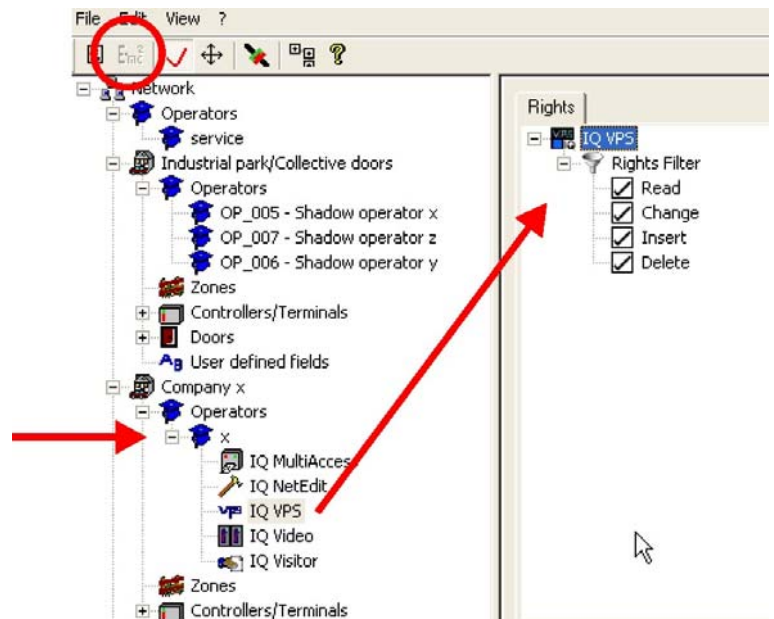


2. Activate and confirm.



### 3. Assign rights

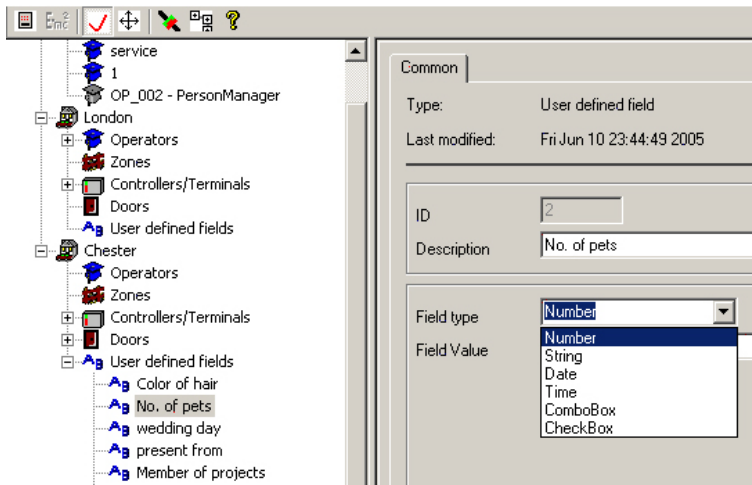
Logical configuration → select the desired operator → **IQ VPS** tab



Activate the rights assigned.  
Superusers automatically have all rights in IQ VPS

## 14.2 User-defined fields

In the logical configuration, you can create a maximum of 40 user-defined fields to be used in the personnel master data of IQ MultiAccess.



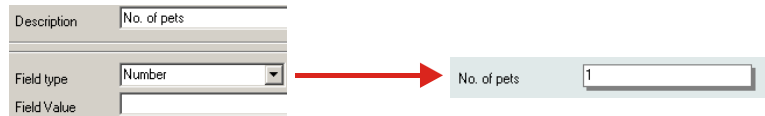
### 14.2.1 Creation and use

Logical configuration → Location → Right-click on user-defined fields.

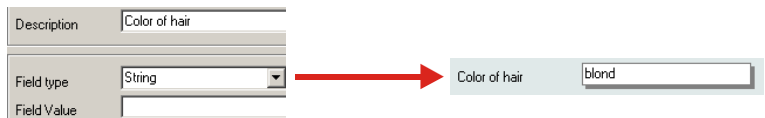
**Description:** Enter an unambiguous name.

**Field type:** Select one of the values suggested. Depending on the field type, the field in question will behave differently in IQ MultiAccess.

**Number:** Only whole numbers may be entered.



**String of characters:** Inputs may include alphanumerical characters, spaces and special characters.



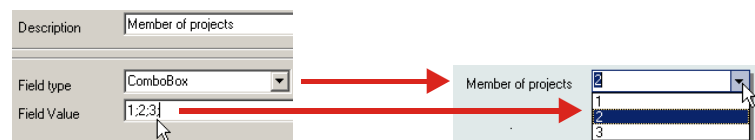
**Date:** Enter date manually or select one via the calendar.



**Time:** Enter time manually or select one by means of the arrows.



**ComboBox:** Manual entry according to field type **String of characters** or select a **field value** that can be individually defined.

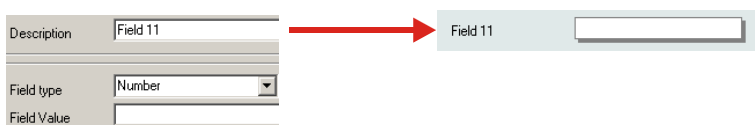


**Field value:** Use only with field type **ComboBox**. Here you can define individual texts which are available for selection in IQ MultiAccess. The individual values are to be separated by semicolons (;).

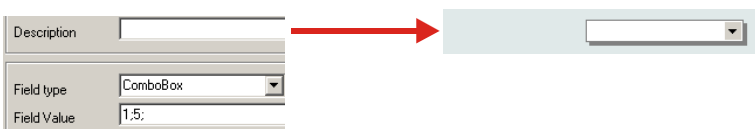
**CheckBox:** By selecting a person, you assign this person to the field.



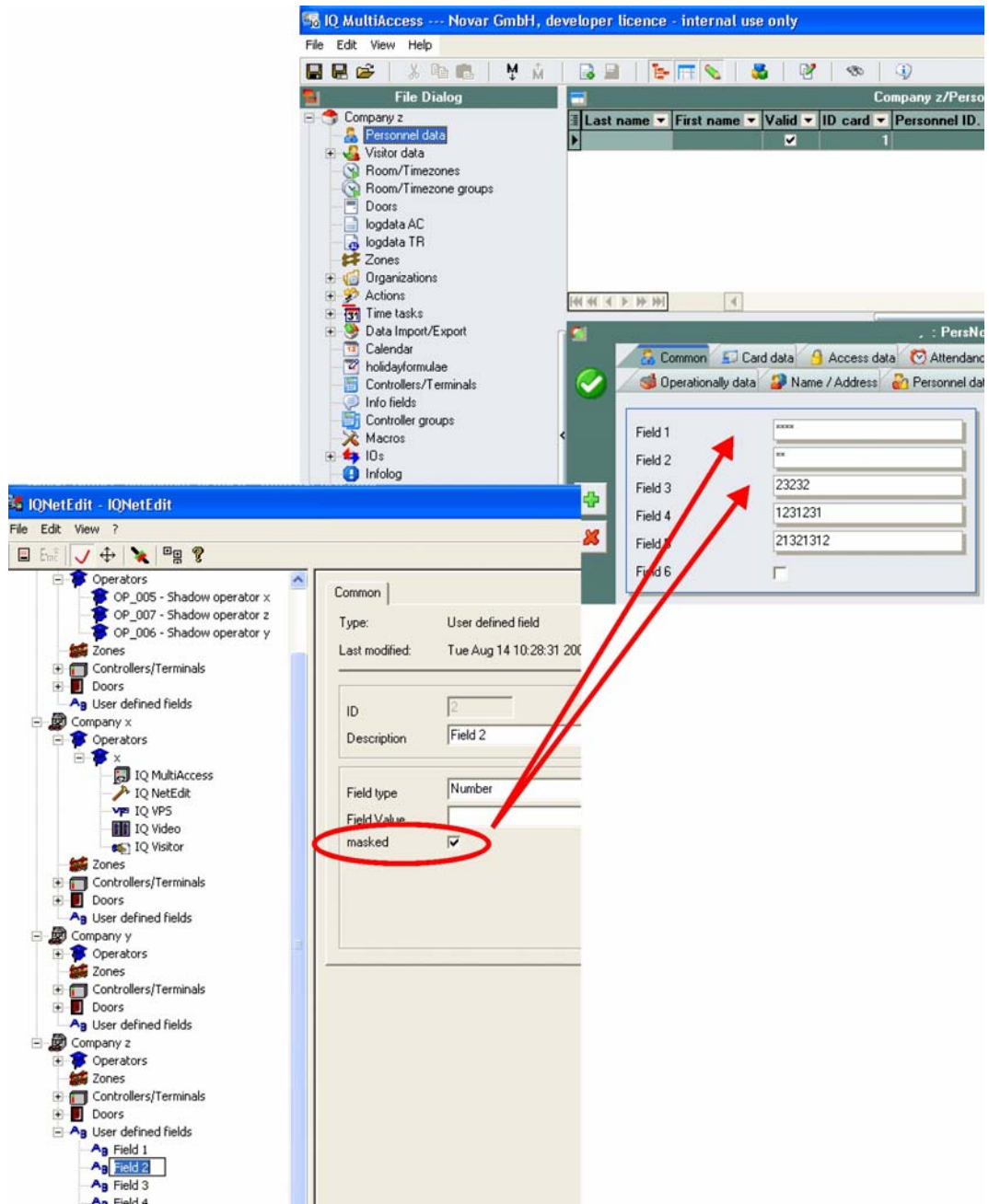
If the suggested name is not changed in field **Description**, the fields in IQ MultiAccess keep the names **Field 1**, **Field 2**, etc.



If the field **Description** is empty, no description will be displayed in IQ MultiAccess either. The field function, however, is available.



Optionally, the contents of the field types **number** and **string** can be displayed as \*\*\*\*\*



The **masked** box is also available for all other field types, but without function as there one of the suggested values is to be selected.



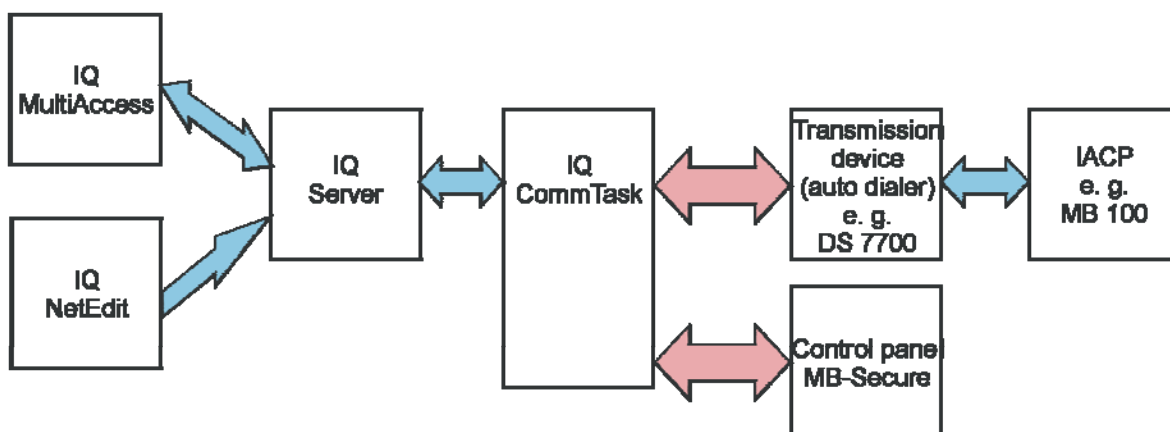
## 15. Integration of an Intruder Alarm Control Panel (IACP)

### 15.1 General description

This function can be used to create data carriers (persons) authorized for access and/or switching at certain switching devices/readers of certain doors at certain times. Switching authorization means that the data carrier is allowed to arm/disarm the intruder alarm control panel and/or to start macros. These information as well as the corresponding room/timezones are transmitted from IQ MultiAccess to the IACP.

The current version supports data carriers IK2, IK3, LEGIC, mifare and mifare DESFire EV1 (MB-Secure panel in preparation).

Communication scheme of IQ MultiAccess<sup>12</sup> in combination with an intruder alarm control panel:



### 15.2 Integration of “Classic” MB-Panels (MB24, MB48, MB100)

A feedback of actions concerning the intruder alarm control panel (like connecting/disconnecting, connection errors) and events of the intruder alarm control panel are transmitted to IQ MultiAccess as bookings according to the table below<sup>13</sup>:

“Translation” table			
IACP event	IQ MultiAccess booking code		Description
Door opened	Release outside	ID card, door+side	Door opened from outside
Door opened from inside	Release inside	ID card, door+side	Door opened from inside
Invalid data carrier	ID card unknown	none, door+side	
Invalid key / identkey	ID card unknown	none, door+side	
Data carrier without positive drive	No zone assigned	-	
Silent hold up, main alarm on	Duress code	-	
Hold up, main alarm on	Duress code	-	

<sup>12</sup> This chapter uses the term “IQ MultiAccess”. For this option it is equivalent to IQ SystemControl and the functions are identic.

<sup>13</sup> The option “report door release” must be active, see chapter 15.4.

"Translation" table			
IACP event	IQ MultiAccess booking code		Description
Duress alarm on	Duress code	-	
Door opened too long, buzzer on	Door opened too long	-	
Door opened too long, buzzer off	Door closed again	-	
Door breakage on	Door opened without card	-	
Lock unlocked	Door in normal operation + special function activated + IACP armed	- ID card, door+side -	
Lock locked	Door locked + special function activated + IACP armed	- ID card, door+side -	With door information With door and card information Without anything
Trigger detection group on	Door opened after release	-	If this detection group would be a RSG/ESF type
Trigger detection group off	Door closed after release	-	If this detection group would be a RSG/ESF type
Tamper lock on	tamper CD triggered	CD-ID	
Tamper cable on	tamper CD triggered	CD-ID	
Tamper lock onff	Tamper CD cleared	CD-ID	
Tamper cable onff	Tamper CD cleared	CD-ID	
Door breakage off	Door opened without card ended	none, door+side	
Blocking time running	Max. attempts: blocking time started	none, door+side	
Blocking time expired	Max. attempts: blocking time expired	none, door+side	
Person left area	Release	ID card, door+side	Access control
Person entered area	Release	ID card, door+side	Access control
Area external armed	IACP armed	-	
Area disarmed	IACP disarmed	-	
Door release time expired	Door release time expired	Door	
Permanent release on	Door permanently released	Door	

<b>“Translation” table</b>			
<b>IACP event</b>	<b>IQ MultiAccess booking code</b>		<b>Description</b>
Permanent release off	Door in normal operation	Door	
Brief release	Release by host	Door	
Door breakage on	Door opened without data carrier	Door	
Door breakage off	Door closed after unauthorized opening	Door	
Error multi person AC	Error multi person AC	Door	
Noral operation on	Normal operation on	Door	
Permanent block on	Permanent block on	Door	
Door opened from inside	Brief release	Door (side)	
Invalid key / identkey	Unknown data carrier	Door (side)	
Trigger detector group on	Door opened after release	Door	
Trigger detector group off	Door closed after release	Door	

These log types can be used for actions by IQ MultiAccess (see user manual P32205-20-0G0-xx, chapter 10).

**AC Side:**

**IQ NetEdit:** Definition of an intruder alarm control panel **MB 100**, **MB48**, or **MB24**.

**IQ MultiAccess:** Creation and administration of **data carriers/persons**, **roomTtimezones** and **authorizations** inclusive allocation to persons/data carriers and switching devices.  
Displays feedback and events of the IACP.

**IQ Server:** Data transfer from IQ MultiAccess to IACP and vice versa.



Those programs are part of IQ MultiAccess and can be installed either all on one computer or divided to several computers (see chapter 2.2 and 3).

**IACP Side:**

**DS 7600 / DS 7700 / DS 9500 / DS 9600:** Digital transmission device (auto dialer)

**MB 100, MB48, MB24:** Intruder alarm control panel IACP

Data transfer can be done either via ISDN, modem, IGIS-LOOP or Ethernet (ITP/IP).

## 15.3 Preconditions

### 15.3.1 PC - Software AC

IQ MultiAccess V17.xx or higher

### 15.3.2 PC - Hardware

For serial transfer:	Serial link cable, item no. 026809
For analogue transfer:	Modem certified by Novar/Honeywell (see chapter 6.6).
For ISDN-transfer:	ISDN-card with Capi 2.0 ISDN modem with Capi 2.0
For IP-transfer:	Ethernet network.
For IGIS-LOOP transfer:	IGIS-LOOP controller (if necessary in a separate housing with power supply unit and battery).

### 15.3.3 Intruder alarm control panels

IK3 EU firmware (in IK3 mode\*) as of V08.06

IACPs 561-MB24, 561-MB48, 561-MB100 (devices with item no. index .10):  
Firmware as of V09  
Programming software WINFEM- Advanced (as of V07).

For ISDN-transfer:	DS 7600	V02.14 or higher
	DS 7700	V02.14 or higher
	DS 9500	V02.14 or higher
	DS 9600	V02.14 or higher
For IP-transfer:	DS 7700	V02.14 or higher
	DS 6700	V03.xx or higher (only IQ SystemControl as of V6)
	DS 6750	V03.xx or higher
For analogue transfer:	DS 6600	V02.xx or higher
	DS 6700	V03.xx or higher (only IQ SystemControl as of V6)
	DS 6750	V03.xx or higher
For IGIS-LOOP transfer:	IGIS-LOOP controller at I-BUS	



\* By use of a IK2 EU or a IK3 EU in IK2 mode it is only a limited functionality in terms of status indication, operating modes and control functions possible.

## 15.4 Procedure

The following pages describe the individual steps to be carried out in the required sequence. You will find detailed information on the work with IQ Net Edit in this manual, information on the work with IQ MultiAccess/IQ SystemControl and the individual IACP in the corresponding manuals. This note will not be repeated further on. Appropriate knowledge is required.

**Caution!**

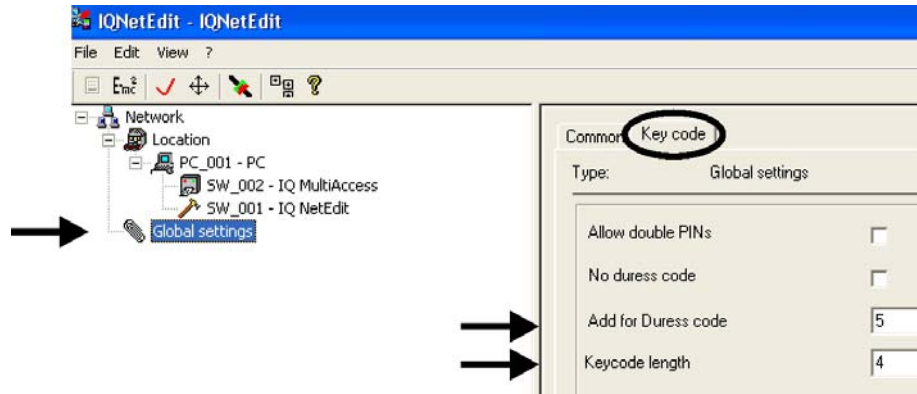


**Basically a data backup must be done on both systems before updating to the new version and before starting the connection of both systems.**

The manufacturer is not liable for data loss, direct or indirect consequential damages of all types occurred by inappropriate handling.

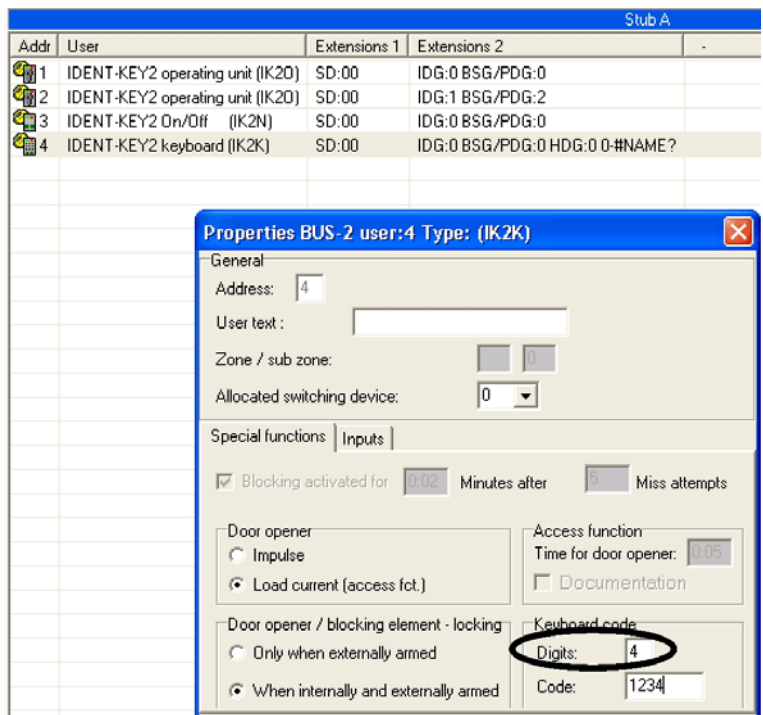
1. Preparation of the IACP (see manuals of the corresponding central units and their programming software).
2. Start IQ NetEdit (see chapter 4)
3. Set identic duress code at both systems. This is fix 5 with IK2 evaluation units. It is also recommended to use this value with mixed systems.

Set identic keycode length at both systems (4 up to 8 digits).



With **IK2** evaluation units and readers, the deposited sequence of digits is the → **keycode** which is used for arming / disarming only; with **IK3** evaluation units and readers, it is the **PIN**.

The keycode can only be entered at the IACP (via LCD operating unit or WINFEM).



The values entered at **Global settings** are used as default settings for new created locations and as inspection values for the PIN-presetting in the personnel master files of IQ MultiAccess.

4. WINFEM → Common programming → Settings tab  
IS-format for data carriers  (mandatory).

Confirm actuation with **OK**. A new window **Conversion to IS-format** opens. All IK2/proX1 data carriers must be in the left column, then confirm the selection with **Convert**.

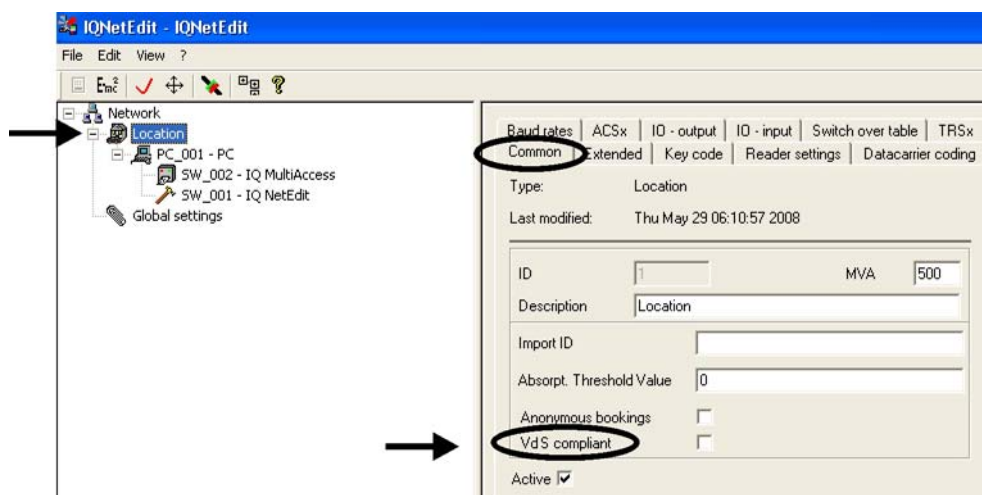
Send the programming to the panel and check function with an arbitrary, authorized data carrier.

5. Select a location for the IACP.



By use of mifare DESFire EV1 data carrier **or by use of different type of readers** note the information in chapter 17.

If necessary, activate **VdS compliant** in the **Common** tab. If active, a location manager has no authorization to enter, change or delete authorizations for disarming within the room/timezones.

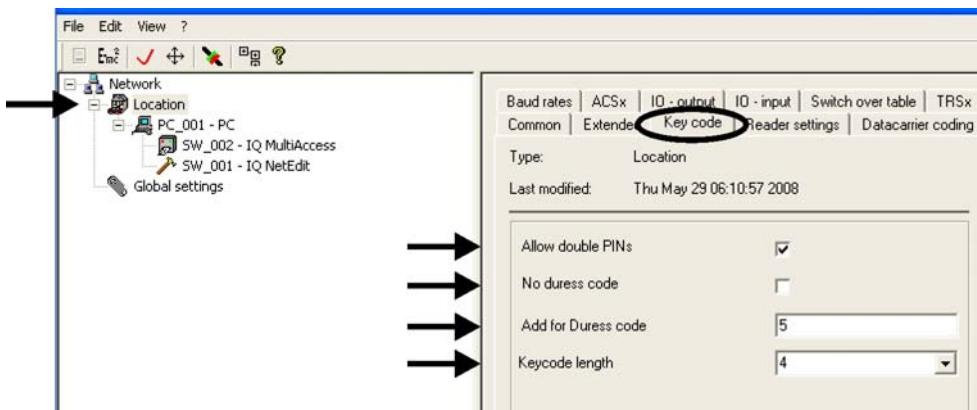


Settings in the **Key code** tab:

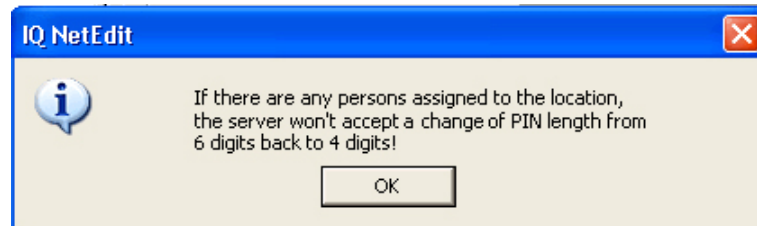
**Allow double PINs** may be active, as at an IACP it is possible to assign the same PIN to several persons (data carriers).

Do not activate **No duress code**.

The settings of identic **Add for duress code** (fix 5 with IK-2 EUs) and identic **Keycode length** for both systems (4 up to 8 digits) have already been preset by the global settings (step 3). Modify only if these values deviate in this location.

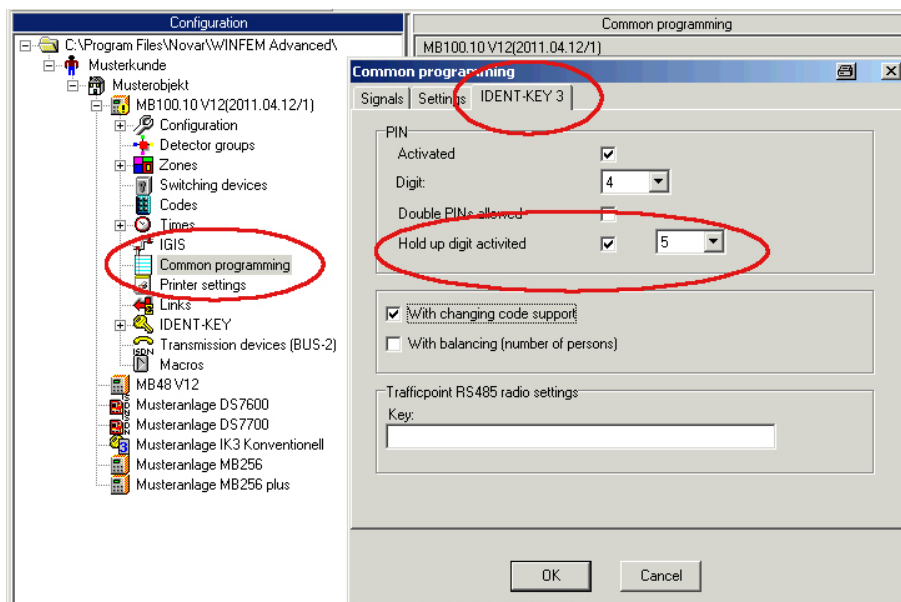


**Problem:** The addition number for duress can not be changed after persons are already allocated to a location as this could cause overlappings of a PIN/door code with a duress code of a door or person.



**Solution:** Create a separate location for the IACP connection. As long as no persons are entered in this location, the basic settings can be modified according to the IACP's requirements.

Settable with IK3 evaluation units (for details see documentation of the IACP).



6. The workstation controlling the IACP require the programs as follow (right-click → Insert → Software):

- IQ MultiAccess
- IQ Monitor
- IQ SysMonitor
- IQ NetEdit (already assigned to the workstation of the standard location as a factory setting)



We recommend to start and connect the installation supporting programs **IQ Monitor** and **IQ SysMonitor** (see chapter 13).



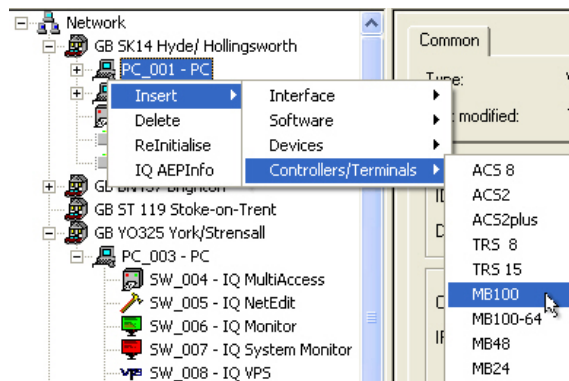
7. Insert an MB panel

a) TCP/IP transmission

Define a workstation with an TCP/IP connection to the MB100 / MB48 / MB24\*.

\* IQ NetEdit makes no difference between the centrals MB100, MB 48 and MB 24, as they are identical concerning the data transfer technique. They have only a different amount of room/time zones and zones. In the example each central type is represented by a MB100 at this place.

There are as many as desired intrusion alarm control panels to be set up in IQ NetEdit.



→ Common tab

Enter an unambiguous designation the intruder alarm control panel is listed in IQ MultiAccess.

Enter the **own IP-address of the IACP** in the field **IP-address**.

The field **TCP/IP-Port** should remain (or be set to) the factory setting of the IACP (8016). Local port and destination port are normally identic.

Keep default setting 0, the destination port will be searched automatically

Enter IP-address of the IQSC / IQMA computer

→ **Extended tab**

Transfer the required IACP data to IQ NetEdit.

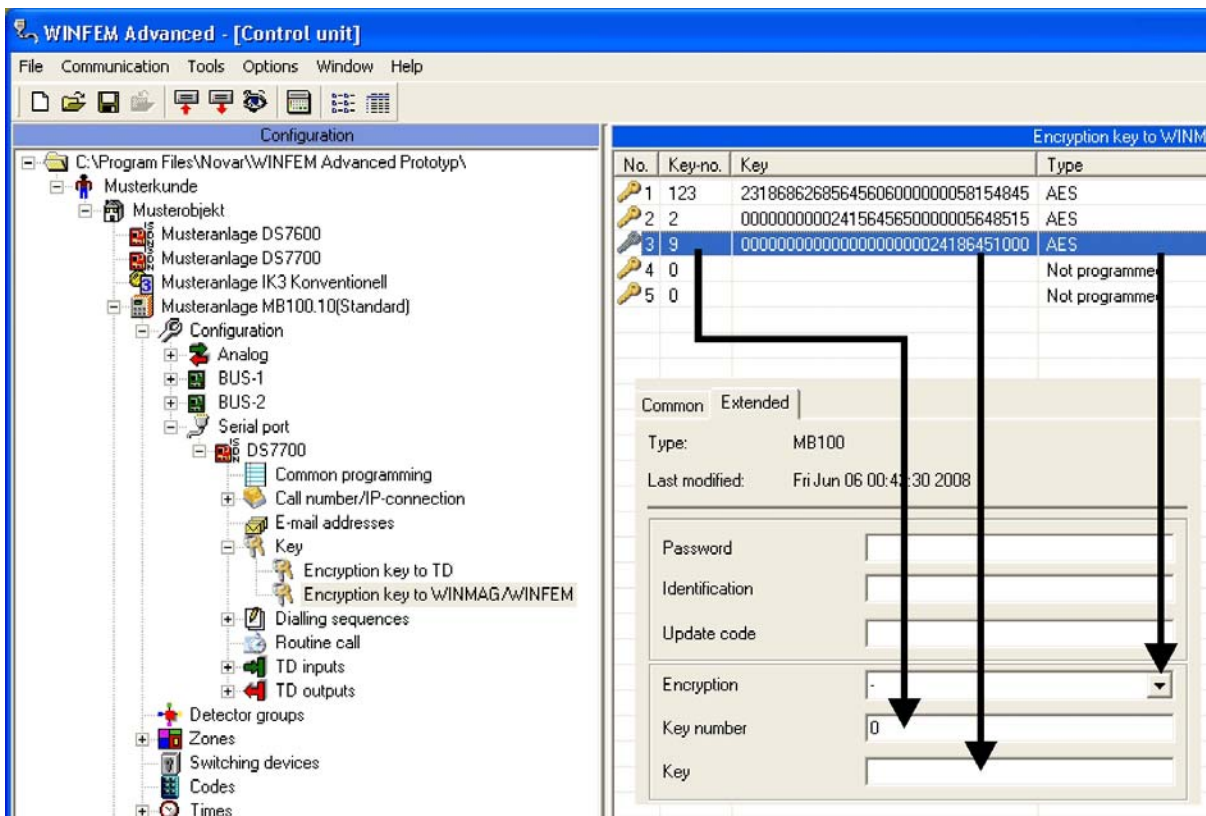
The screenshot shows a software configuration window with a tree view on the left and a table of connections on the right. A 'WINMAG connection' dialog box is open, showing fields for Description, Local port, IP-Address, Destination port, Type, ID number, Password, and Encryption. Below it, the 'Extended' tab of a configuration window is visible, with fields for Password, Identification, Remote param. code, Encryption, Key number, and Key. Red arrows indicate the flow of data from the dialog box to the 'Extended' tab and then to a physical device keypad labeled 'Via operating device, function 519'. The keypad has various function buttons and a numeric keypad.

No.	Type	ID Number	Password	IP-address	Local port	Destination port	encrypted
1	IP permanent	87654321	11111111	0.0.0.0	8015	8016	No
2	IP permanent			0.0.0.0	0	8015	No
3	IP permanent			0.0.0.0	0	8015	No
4	IP permanent			0.0.0.0	0	8015	No

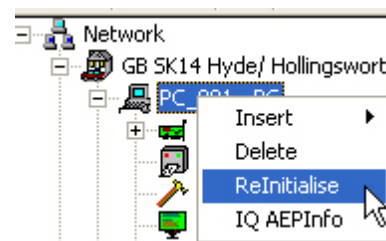
See next page for information



Alternatively, the link can also be done via **WINFEM**-connections. However, it is recommended to use the **WINMAG**-connections because this is a monitored connection.



Right-click the workstation to which the IACP is connected → Reinitialise.  
 With a correct working connection the corresponding panel will be displayed with a green dot.



With an existing and working connection the **Scan** function can be run by right-clicking the selected IACP. All the recognized switching devices will automatically be set up in IQ NetEdit.

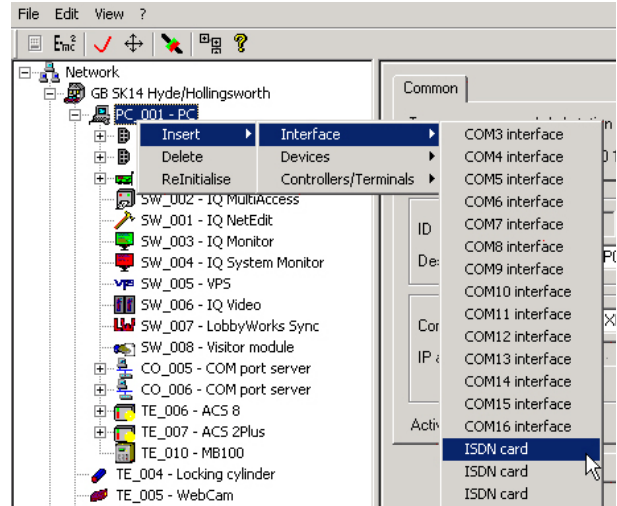


Alternatively, they can be set up manually (see step 9).

Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected (see also chapter 7). If not, the user codes and the individual panel texts of the IACP will automatically be transferred before the first parametrization (in case that data carriers have already been entered (new) in IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the IACP).

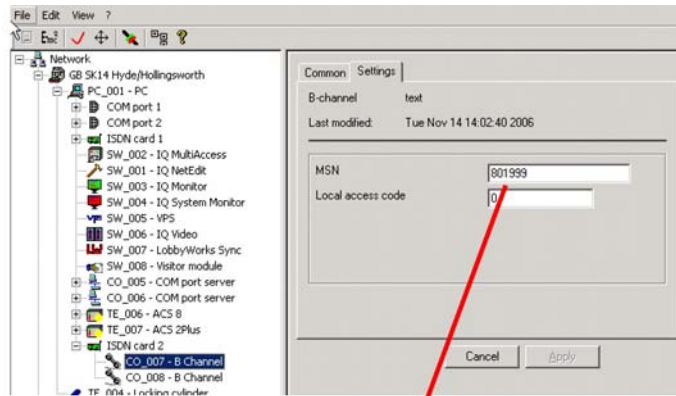
**b) ISDN transmission**

Define a workstation with an ISDN-card for IACP connection (cf chapter 6.6).



The **MSN** is the own phone number to which the ISDN-card is connected (without area code). This number must be entered as **Call number** in the IACP.

If a local access code is required, it must be entered in the field **local access code**.



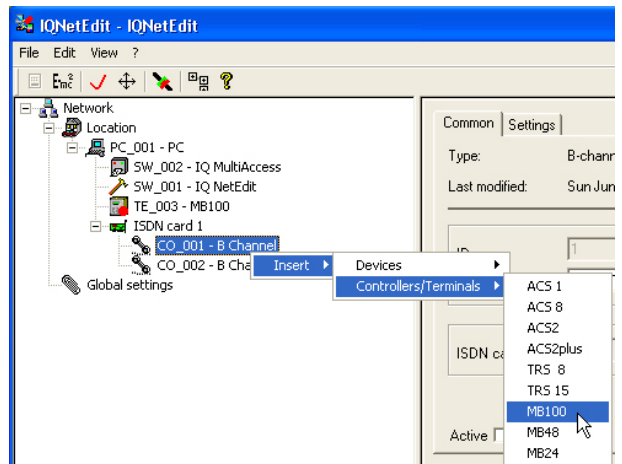
AWUG / BUS-2 modem: a main transmission device

Telecommunication functions		AWUG call numbers		
AWUG dialing sequence	AWUG routine call	BUS-2 modem	Information	
1	801999	1111111111	87654321	
2				
3				
4				
5				

Insert an MB 100 / MB48 / MB24.\*.\*

\* IQ NetEdit makes no difference between the centrals MB100, MB 48 and MB 24, as they are identical concerning the data transfer technique. In the example each central type is represented by a MB100 at this place.

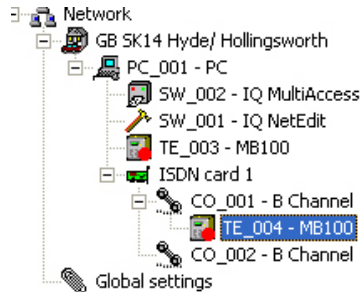
There are as many as desired intrusion alarm control panels to be set up in IQ NetEdit.



→ **Common tab**

Enter an unambiguous designation the intruder alarm control panel is listed in IQ MultiAccess.

The **address** field is filled in by IQ NetEdit automatically and should not be modified. It is used to unambiguously identify the individual intruder alarm control panel in the AC-system, as IQ MultiAccess can handle several intruder alarm control panels. This address will be found nowhere at the IACP side.



→ **Distant station tab**

Enter the telephone number of the IACP.

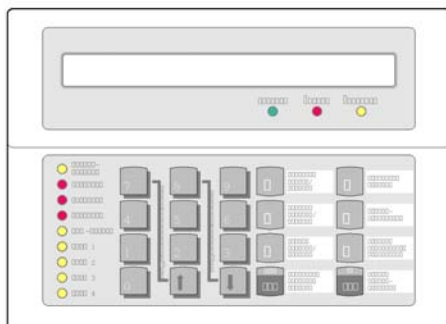
For explanations of the fields →Time window and →Quantity see chapter 6.6.7.

→ **Extended tab**

Enter password, identification and remote parametrization code.

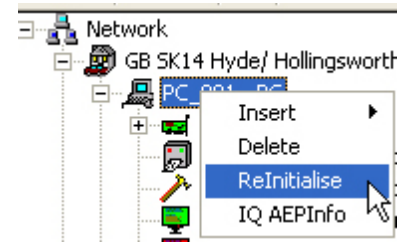
No.	Password	Call-number	ID Number	Call number o
1	87654321	801999	11111111	Authorized
2				Authorized
3				Authorized
4				Authorized
5				Authorized
6				Authorized
7				Authorized
8				Authorized

Via operating unit, function 519

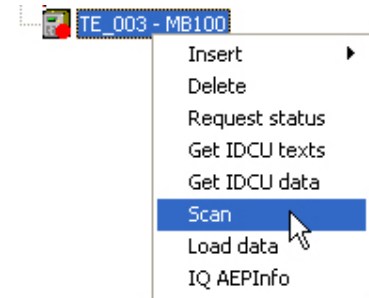


Right-click the workstation to which the IACP is connected → Reinitialise.

With a correct working connection the corresponding panel will be displayed with a green dot.



With an existing and working connection the **Scan** function can be run by right-clicking the selected IACP. All the recognized switching devices will automatically be set up in IQ NetEdit.



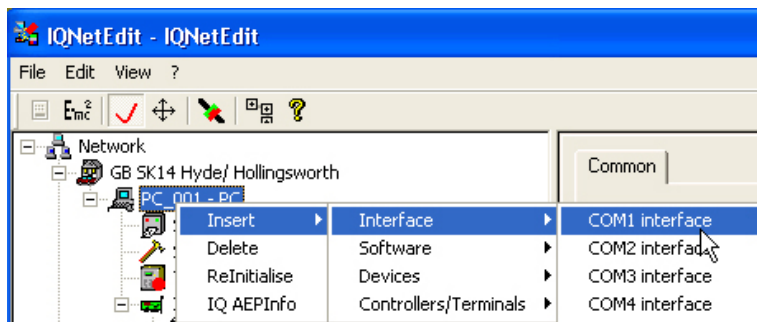
Alternatively, they can be set up manually (see step 9).

Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected (see also chapter 7). If not, the user codes and the individual panel texts of the IACP will automatically be transferred before the first parametrization (in case that data carriers have already been entered (new) in IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the IACP).

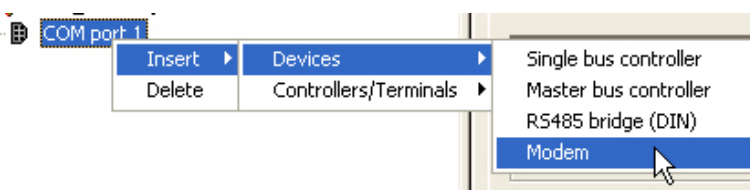
**c) Modem transmission**

For detailed information on modem transmission see chapter 6.6.

Insert a COM interface to a workstation (see chapter 6.6.1).

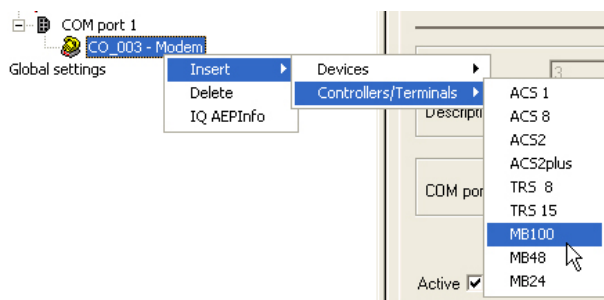


Insert a modem to COM interface (see chapter 6.6.1).



Insert an MB 100 / MB48 / MB24.\*

\* IQ NetEdit makes no difference between the centrals MB100, MB 48 and MB 24, as they are identical concerning the data transfer technique. In the example each central type is represented by a MB100 at this place.

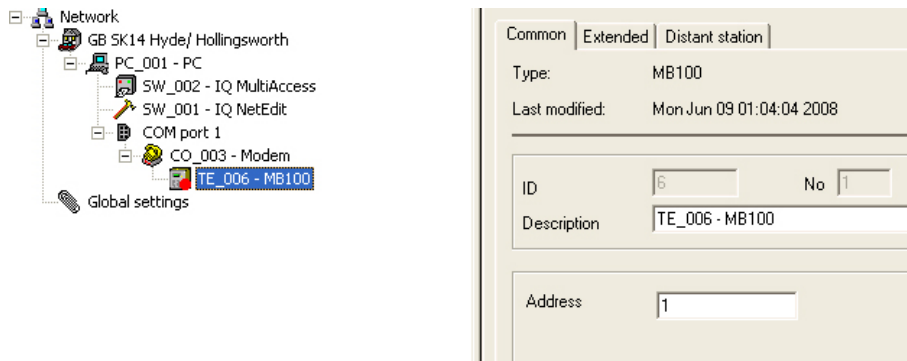


There are as many as desired intrusion alarm control panels to be set up in IQ NetEdit.

**→ Common tab**

Enter an unambiguous designation the intruder alarm control panel is listed in IQ MultiAccess.

The **address** field is filled in by IQ NetEdit automatically and should not be modified. It is used to unambiguously identify the individual intruder alarm control panel in the AC-system, as IQ MultiAccess can handle several intruder alarm control panels. This address will be found nowhere at the IACP side.



**→ Distant station tab**

Enter the telephone number of the IACP.

For explanations of the fields →Time window and →Quantity see chapter 6.6.7.

→ **Extended tab**

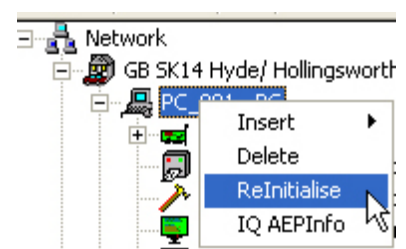
Enter password, identification and remote parametrization code.

No.	Password	Call-number	ID Number	call authorized
1	87654321	801999	11111111	Authorised
2				Authorised
3				Authorised
4				Authorised
5				Authorised
6				Authorised
7				Authorised
8				Authorised

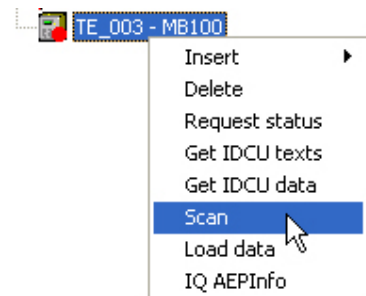
Via operating unit, function 519

Right-click the workstation to which the IACP is connected → Reinitialise.

With a correct working connection the corresponding panel will be displayed with a green dot.



With an existing and working connection the **Scan** function can be run by right-clicking the selected IACP. All the recognized switching devices will automatically be set up in IQ NetEdit.



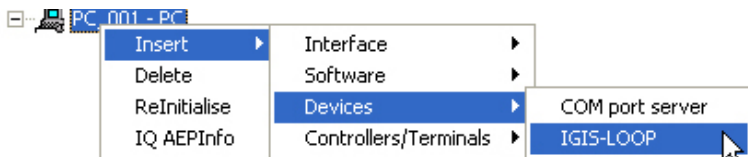
Alternatively, they can be set up manually (see step 9).

Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected (see also chapter 7). If not, the user codes and the individual panel texts of the IACP will automatically be transferred before the first parametrization (in case that data carriers have already been entered (new) in IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the IACP).



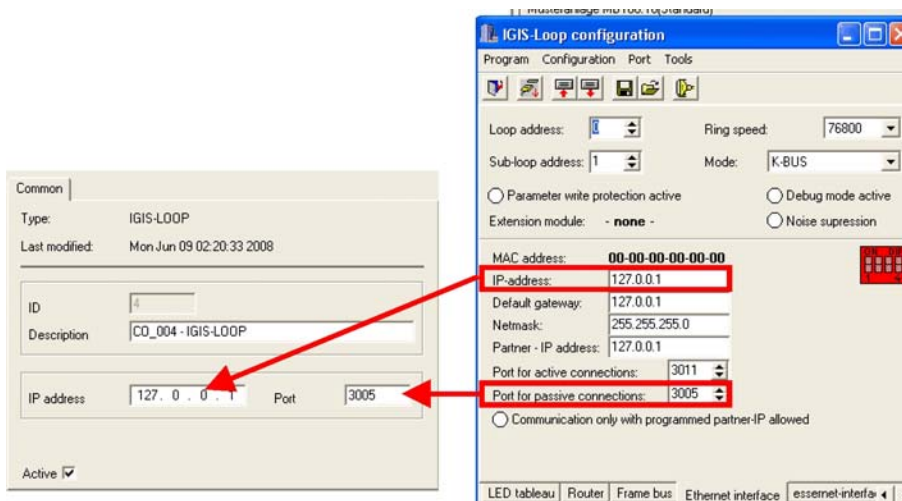
**d) IGIS-LOOP transmission**

Insert an IGIS-LOOP controller to workstation

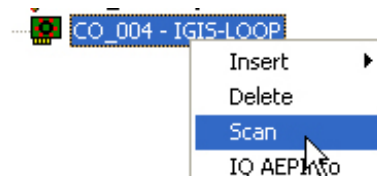


**→ Common tab**

Enter the IP-address and the port of the IGIS-LOOP controller. Use the entry of “Port for passive connections” in IQ NetEdit.<sup>14</sup>



With an existing and working connection the **Scan** function can be run by right-clicking the selected IGIS-LOOP controller. All the recognized IACPs will automatically be set up in IQ NetEdit.



A right-click on the selected MBxxx and the selection **Scan** automatically sets up all recognized switching devices.

Alternatively, the IACP can be entered manually:

Insert a MB100 / MB48 / MB24\*.



\* IQ NetEdit makes no difference between the centrals MB100, MB 48 and MB 24, as they are identical concerning the data transfer technique. In the example each central type is represented by a MB100 at this place.

There are as many as desired intrusion alarm control panels to be set up in IQ NetEdit.

14

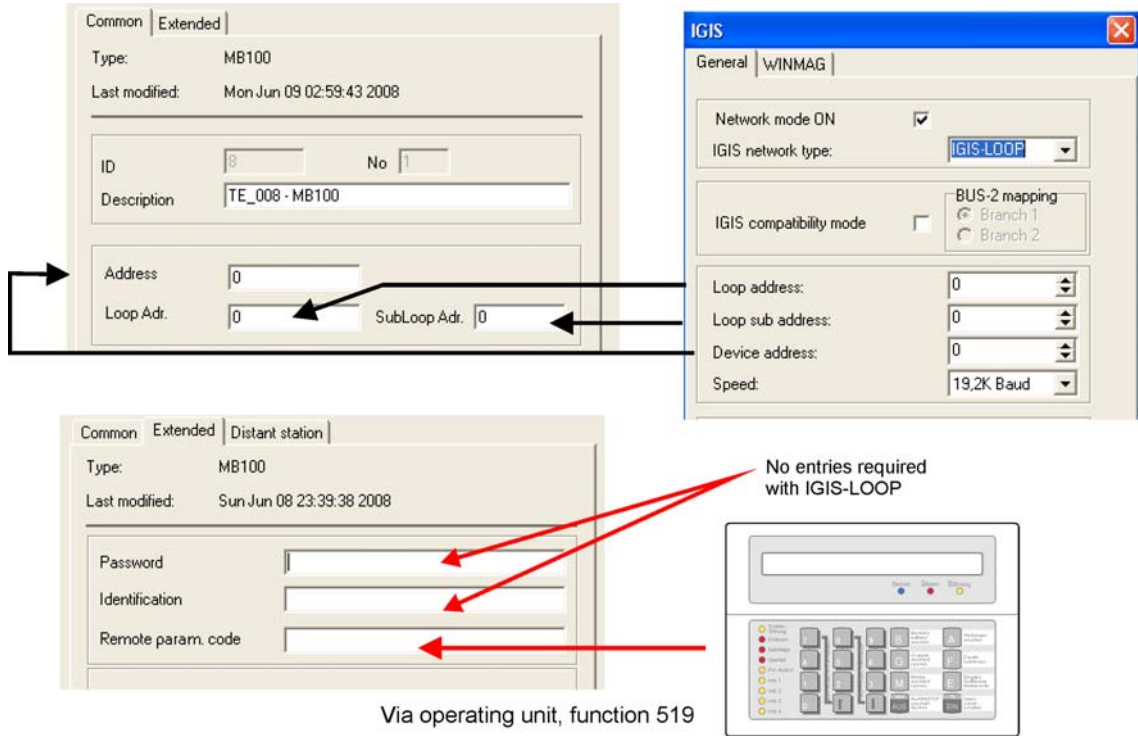
The IGIS-LOOP controller has previously to be configured via WINFEM-Advanced (see documentation IGIS-LOOP controller and WINFEM).

→ **Common tab**

Enter an unambiguous designation the intruder alarm control panel is listed in IQ MultiAccess. Input of address/device address, loop address and sub loop address

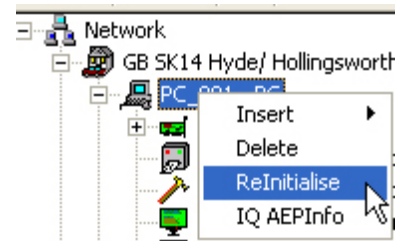
→ **Common tab**

Enter the remote programming code. With IGIS-LOOP, password and identification are not necessary.



Right-click the workstation to which the IACP is connected → Reinitialise.

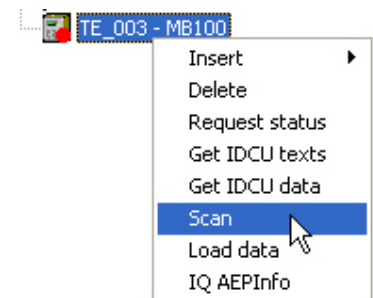
With a correct working connection the corresponding panel will be displayed with a green dot.



With an existing and working connection the **Scan** function can be run by right-clicking the selected IACP. All the recognized switching devices will automatically be set up in IQ NetEdit.

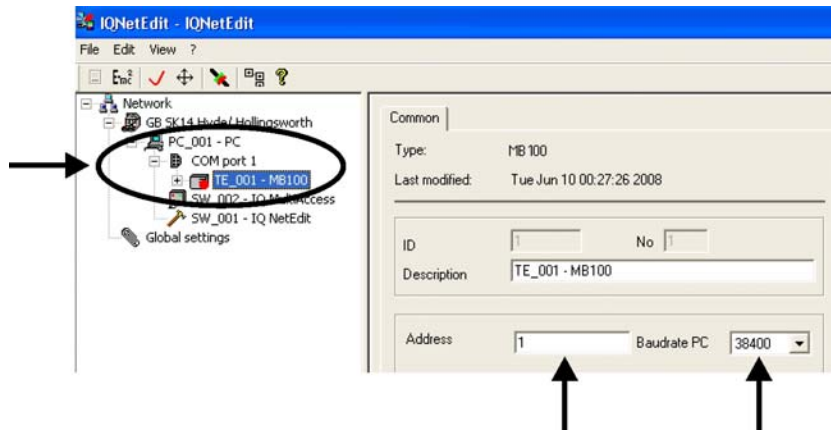
Alternatively, they can be set up manually (see step 9).

Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected (see also chapter 7). If not, the user codes and the individual panel texts of the IACP will automatically be transferred before the first parametrization (in case that data carriers have already been entered (new) in IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the IACP).



**e) Serial transmission**

Insert a COM interface to a workstation, and an MBxxx to the COM interface.

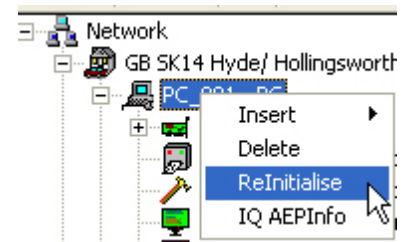


**Address:** Keep suggested value (1).

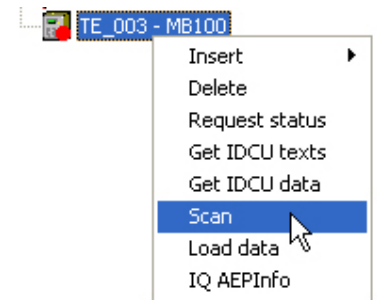
**Baudrate PC:** Set to 38400 (this is the default setting of the IACP, where no further settings have to be done).

Right-click the workstation to which the IACP is connected → Reinitialise.

With a correct working connection the corresponding panel will be displayed with a green dot.



With an existing and working connection the **Scan** function can be run by right-clicking the selected IACP. All the recognized switching devices will automatically be set up in IQ NetEdit.

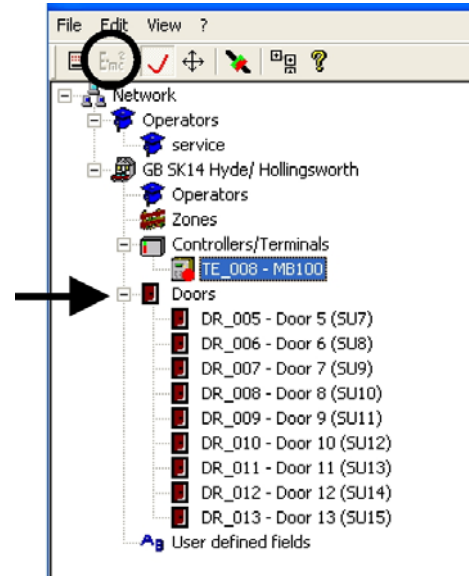


Alternatively, they can be set up manually (see step 9).

Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected (see also chapter 7). If not, the user codes and the individual panel texts of the IACP will automatically be transferred before the first parametrization (in case that data carriers have already been entered (new) in IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the IACP).

8. Door data:

After scanning there are doors in IQ NetEdit with the designation SUxx = switching unit with numbering of the IACP.



Check / set each door:

Times (outside/inside): Definition of times for individual timers, some separated according to the door sides.

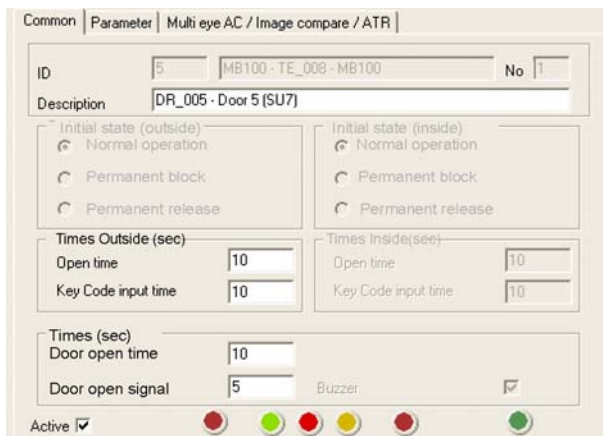
Open time: Activation time of the door strike. During this time the door can be opened.

Key code input time: Within this time the key code (→ PIN or → door code) must be typed in. If the code is not entered completely after this time has expired, the complete entry must be repeated.

Door open time: Maximum time a door is allowed to be open. It starts when the monitoring contact indicates the actual opening of the door. After expiration of this time an alarm will be triggered (Door opened too long).

Door open signal: If a reader/keypad is equipped with an internal buzzer, it indicates on the beginning of the door open signal time that the door should be closed as otherwise the door open time expires which causes an alarm (Door opened too long).

The time for the door open signal should always be shorter than the door open time in order to remain enough time for closing the door. The door open signal time ends at the same time as the door open time.



Operation mode (outside/inside):

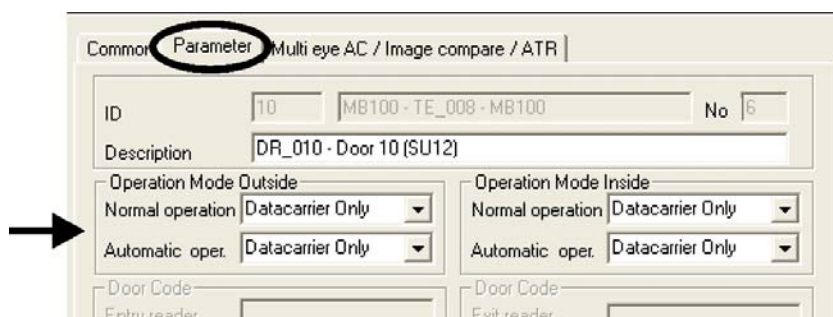
For each door side there can be defined a type of identification required for entry:

- Data carrier only
- PIN only
- PIN + data carrier
- PIN or data carrier
- Without time check
- Access inhibited

There is always one criterion to be valid for one operation mode:

Normal operation: The selected access criterion is valid for the door being in **normal operation**.

Automatic operation: The selected access criterion is valid while the door is set to **automatic operation**. Automatic operation can be used to set the door to permanent release / permanent block at predefined times (examples see user manual).



Multi-eye AC (outside/inside):

For each door side there can be defined how many persons authorised at this door (switching device9 must book one after another to get a door release (2 to 9 possible). The door will only be released if the total number of valid bookings is achieved.

9. Manual configuration of IACP switching devices (doors).



Not necessary after **Scan!** Continue with chapter 15.4.

As an alternative to scan (see 7a to 7d) the IACP hardware can also be configured manually.

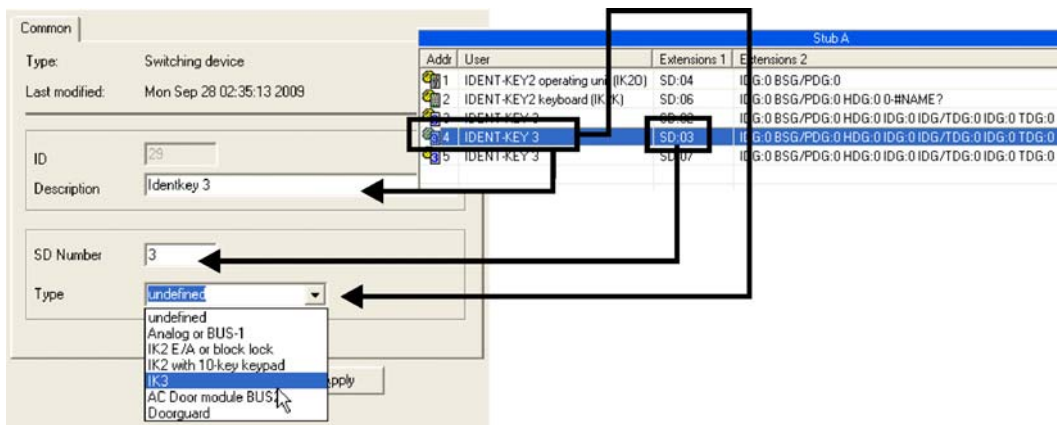
Select the MBxxx and insert one or several switching device(s) at which the data carriers entered in IQ MultiAccess are authorized.



→ **Common** tab

Enter an unambiguous designation the switching device is listed in IQ MultiAccess. Recommendation: Use the designation of the IACP (see chapter 15.4.1). Select the appropriate IACP user in the field **type**. Depending on the type some functions are available/not available for the definition of → **room/time zones**. The status of already existing switching devices is “not defined” and should be reworked.

At first, automatically the field **SD number** will be consecutively numbered by IQ NetEdit. Previously the actual switching device number (SD\_xx) used by the IACP must be entered (1 to 64). As this is a numeric field, only the number must be entered (e. g. SD\_06 becomes 6).

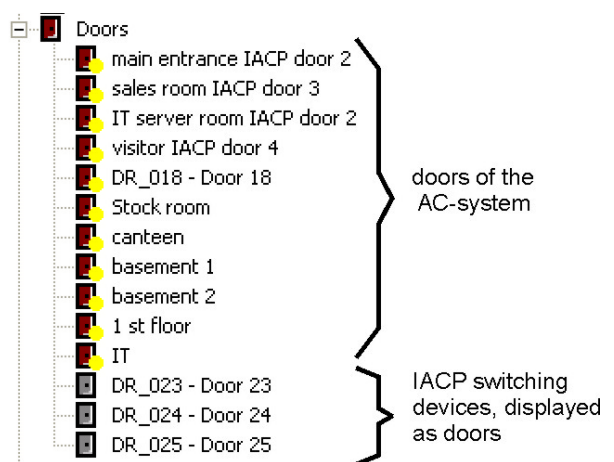


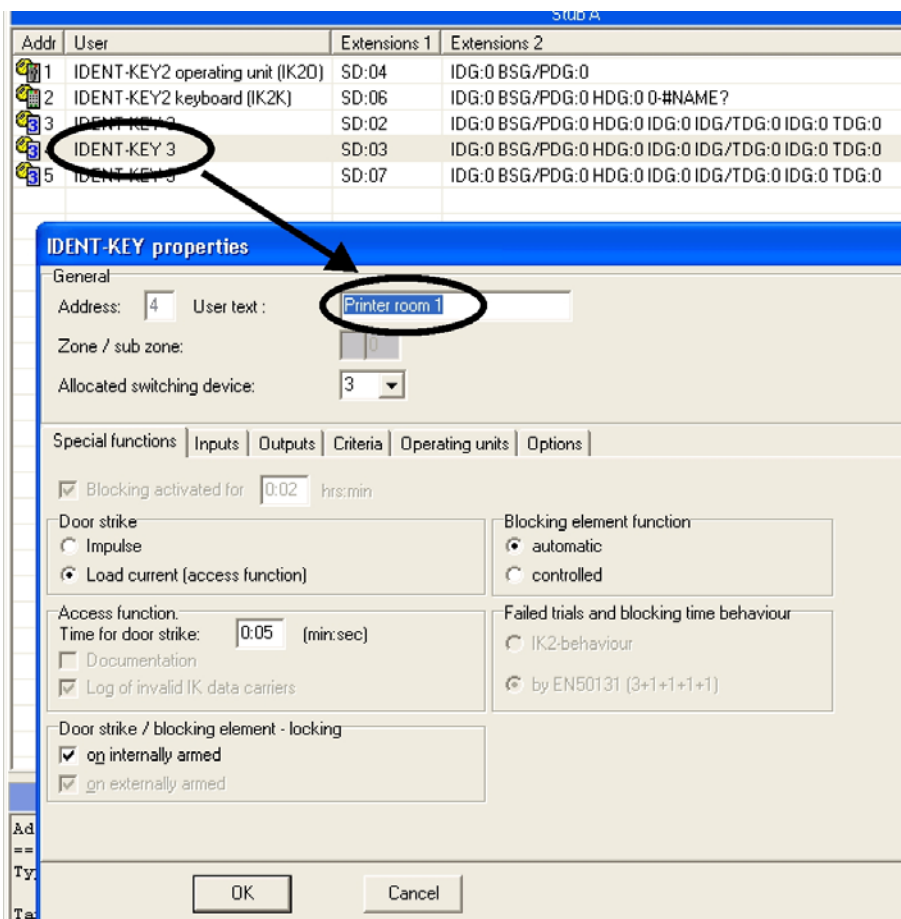
In IQ NetEdit and IQ MultiAccess a switching device is displayed as a door in offline mode. Due to this, no entries can be done in the tabs of those doors, existing entries will be ignored. Furthermore, the logical view will not display any door state.

We recommend to use the designations of the switching devices as they are in the ICP.

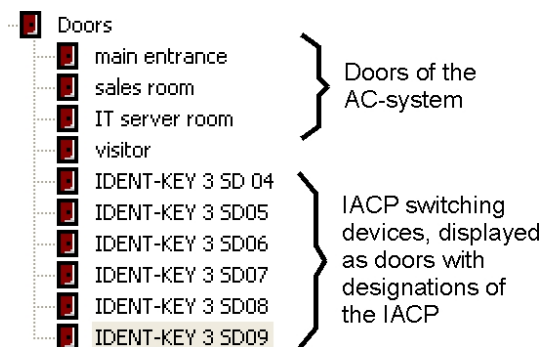
The name of a switching device can be found in the column **user**. However, all switching devices of the same type have the same name (e. g. IDENT-KEY 3).

Via a right-click on the switching device → **Properties** an individual name (e. g. printer room 1) can be entered in the field **User text**, but still the designation in the user column will keep its the superior text.

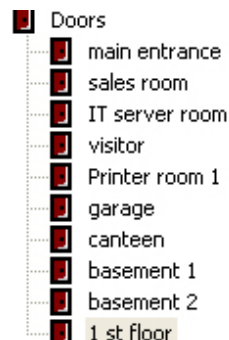




View in IQ NetEdit:



As an alternative an unambiguous name can be entered in IQ NetEdit:



## 15.5 Data exchange

### 15.5.1 Data acceptance from IACP

By linking both systems, the IACP and IQ MultiAccess, all data relevant for switching devices (doors) and data carriers (persons) are centrally administrated in IQ MultiAccess. For the initial connection of both systems the already existing data of the IACP must be either transferred to IQ MultiAccess or newly created there.



Pay absoluteley attention that all relevant settings are identic and all data carriers have been converted to IS-format in WINFEM before starting the data transfer (see chapter 15.3).

#### Get IACP texts

Right-click the required MBxxx → Get IACP texts.

All customer specific designations of switching devices, inputs/outputs etc.will be received. They are required for the evaluation of the eventlog via → **Logdata IACP**

#### Get IACP data

Right-click the required MBxxx → Get IACP data.

This program section transfers all operation codes, room/timezones, data carriers and their authorizations (data carrier no. name, IS-code and PIN) to IQ MultiAccess.



If the transfer of those two data have not been done before the first parameterizing of the IACP, IQ MultiAccess will automatically get the user codes of the IACP before the parametrization gets started. This guarantees the users being still able to log in to the operating units.

This data transfer is not viewd on the screen. These operations can be visualized via the installation supporting programs → **IQ Monitor** and → **IQ SysMonitor**.



Contrary to the AC-controllers, the MBxxx will **not** be parameterized automatically on exiting IQ NetEdit. This must be done manually **for the first time** (see 15.4.2). Only accordingly relevant data will be updated automatically.



### 15.5.2 Data transmission from IQ MultiAccess

The initial parameterizing / loading data must be executed manually.



**Caution!** Check, and if necessary correct the data transferred from the IACP in IQ MultiAccess before the first parameterizing (see also 15.5).

Wait until the data of IQ MultiAccess are conform with the data of the IACP before enabling the controlling of the MBxxx by IQ MultiAccess (function 512).

#### Activation of IQ MultiAccess connection

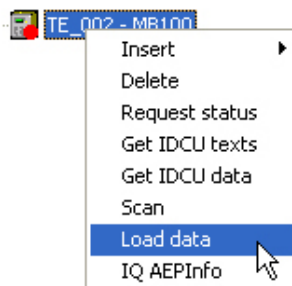
The connection can either be activated in WINFEM or via the LCD operating unit.

WINFEM	LCD operating unit	Explanation
→ Common programmierung → Settings tab  Remote access IQ MultiAccess / IQ SystemControl ☒ *	Function 512 Access IQ MultiAccess → yes *	Data created in IQ MultiAccess or IQ SystemControl affect directly on the intruder alarm control panel and can no longer be defined via WINFEM.
→ Common programmierung → Settings tab  Access via IQ MultiAccess / IQ SystemControl enabled ☒ *	Function 512 Control via IQ MultiAccess → yes *	AC-functions, such as brief release, permanent release, permanent lock affect directly on the door(s) at the push of a button within IQ MultiAccess, IQ SystemControl or IQ NetEdit.
* To deactivate these parameters or set them to no, the deactivation first must be enabled in function 523.		

Create actions in IQ MultiAccess which display messages in case of transmission faults (see user manual chapter 10.3). Do not exit IQ MultiAccess in order to display messages when they occur. These messages do already exist in IQ SystemControl in ex-works condition.

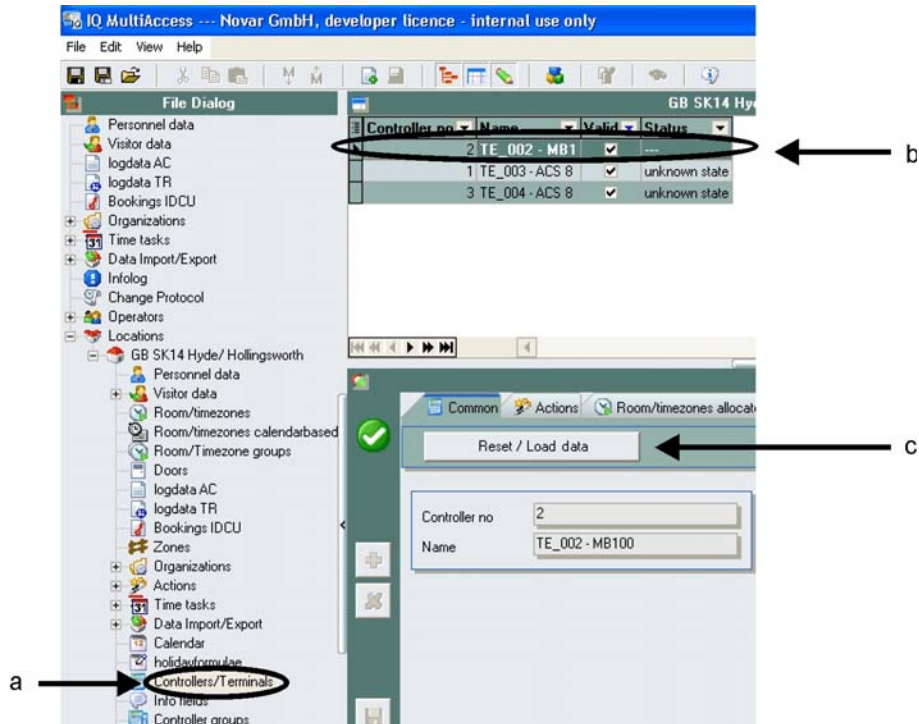
#### Load data from IQ NetEdit:

Right-click the selected MBxxx → Load data



**Load data from IQ MultiAccess:**

- a) Controllers/terminals
- b) Select the required MBxxx
- c) Reset / Load data



With an online connection (e. g. via TCP/IP or IGIS-LOOP) from now on the modified data will be automatically transferred to the IACP after saving.

To intruder alarm control panels connected via RDT (ISDN/analogue) there is no online connection. There the modified data are only known after the next parametrization / data loading via RDT.

This transmission can be automatized by defining time windows for the corresponding IACPs in the **distant station** tab of IQ NetEdit. If there exist data for transmission, the RDT will start automatically within the time windows. At this juncture also IACP data will be transferred to IQ MultiAccess for evaluation in the logfile (see also chapter 6.6.7).

The screenshot shows the 'Distant station' tab in IQ NetEdit. The 'Type' is set to 'MB100'. The 'Last modified' field is empty. Below, there are several input fields for configuration:

Phone number	901888	
Quantity	5	
Time window A	07:00	to 07:15
Time window B	12:00	to 12:15
Time window C	17:00	to 17:15
Time window D	23:00	to 23:15

Alternatively the data transfer can be started manually at every time as described before.



From now on the data which are administrated by IQ MultiAccess can no longer be administrated directly at the IACP / via WINFEM.

## 15.6 Data administration via IQ MultiAccess / IQ SystemControl

For detailed descriptions of the creation and administration of the room/timezones, data carriers (persons) and their authorizations see user guide of IQ MultiAccess (P32205-20-0G0-xx) and/or IQ SystemControl (P03118-20-0G0-xx).

## 15.7 Evaluations in IQ MultiAccess / IQ SystemControl

For detailed descriptions of evaluation possibilities see user guide of IQ MultiAccess (P32205-20-0G0-xx, chapter 13) and/or IQ SystemControl (P03118-20-0G0-xx, chapter 10)

## 15.8 Further information

- ✓ The installer should change the “Service”-password in order to have access to the system at any time and no unauthorized person has administrator rights (if necessary create a separate superuser for the system administrator, see chapter 2.5 and 8).
- ✓ Create individual location managers with corresponding rights (see chapter 8).
- ✓ Create a time controlled task for data backup, see user guide of IQ MultiAccess (P32205-20-0G0-xx, chapter 11.7) and/or IQ SystemControl (P03118-20-0G0-xx, appendix).
- ✓ Hardware subsequently connected to the IACP can be transferred to IQ NetEdit by another scan. This will not affect the already existing IACP-hardware.

## 15.9 Checklist for IACP linking (MB-classic panels)

Deliverables/ check and set if necessary				OK
IACP	Backup data			
	Prepare for remote parametrization			
	Disable access via IQ MultiAccess	WINFEM / cenntal unit - Common programming	LCD-operating unit function 523 / 512	
	Disable control via IQ MultiAccess	WINFEM / cenntal unit - Common programming	LCD-operating unit function 523 / 512	
	Convert data carriers to IS-format	WINFEM / cenntal unit - Common programming		
	Send programming to panel			
IQ MultiAccess / IQ SystemControl	Backup data create a time controlled task if necessary	User manual IQMA chapter 11.7, IQSC appendix 2.7		
IQ NetEdit	Global settings	Duress code		
	Location for IACP	VdS-compliant		
		enable double PINs		
		Addition number for duress		
		Keycode length		
		Assign software - IQMultiAccess - IQ NetEdit - IQ Monitor - IQ Sysmonitor		
		- start IQ Monitor		
		- start IQ Sysmonitor		
	Set up MBxxx	for all connection types:	Identification / ID-no.* * = not with IGIS-LOOP	
			Password * * = not with IGIS-LOOP	
			Remote parametrization code	
		with TCP/IP:	IP-address	
			TCP/IP-Port	
			Encryption	
			Key number	
			Key	

Deliverables/ check and set if necessary				OK
			IP address of the IQMA / IQSC computer (cf. chapter 15.3, step 7)	
		with ISDN	MSN of IQMA-ISDN-card as call number of IACP	
			Trunk line request	
			Call number (= MSN of IACP / DSxxxx)	
			Own call number of IACP = call number in IQ NetEdit	
		with IGIS-LOOP	IP-address of IGIS-LOOP-controllers (for passive connections)	
			Scan for IACPs	
	Right-click on MBxxx	Scan		
		Get IACP texts		
		Get IACP data		
	Check door data	Type of identification for normal operation		
		Type of identification for automatic operation		
		Open time		
		Keycode input time		
		Door open time		
		Door open signal		
		Multiple persons AC		
IQ MultiAccess / IQ SystemControl	Room/timezones incl. door / switching device allocation			
	Data carriers incl. RTZ-allocation			
	Create actions for communication fault	User manual IQMA chapter 10.3, IQSC already existing per default		
	Time controlled task for data backup	User manual IQMA chapter 11.7, IQSC appendix 2.7		
	Time controlled task for loading holidays	User manual IQMA chapter I 11.6, IQSC appendix 2.76		

Deliverables/ check and set if necessary				OK
IACP	Enable access via IQ MultiAccess	WINFEM / cenntrol unit - Common programming	LCD-operating unit, function 512	
	Enable control via IQ MultiAccess	WINFEM / cenntrol unit - Common programming	LCD-operating unit, function 512	
IQ NetEdit or IQ MultiAccess	Load data per MBxxx	<b>Manually</b> required for the first time		
IQ NetEdit	Change Service-password			
	Create location managers			

## 15.10 Integration of MB-Secure panels

### AC Side:

**IQ NetEdit:** Definition of an intruder alarm control panel **MB-Secure**.

**IQ MultiAccess:** Creation and administration of **data carriers/persons, room timezones** and **authorizations** inclusive allocation to persons/data carriers and switching devices.  
Displays feedback and events of the IACP/panel.

**IQ Server:** Data transfer from IQ MultiAccess to IACP/panel and vice versa.



Those programs are part of IQ MultiAccess and can be installed either all on one computer or divided to several computers (see chapter 2.2 and 3).

### IACP Side:

**MB-Secure:** Intruder alarm control panel IACP

Data transfer can be done via Ethernet (TCP/IP).

## 15.11 Preconditions

### 15.11.1 PC - Software AC

IQ MultiAccess V17.xx or higher

### 15.11.2 PC - Hardware

For IP-transfer: Ethernet network.

### 15.11.3 Intruder alarm control panels

IK3 EU firmware (in IK3 mode\*) as of V12.xx

MB-Secure panel: Firmware as of V4.6.x  
Programming software IQ PanelControl (as of V4.6.x).



\* The use of a IK2 EU or a IK3 EU in IK2 mode is **not** possible in combination of a MB-Secure panel integration.



## 15.12 Procedure

The following pages describe the individual steps to be carried out in the required sequence. You will find detailed information on the work with IQ Net Edit in this manual, information on the work with IQ MultiAccess/IQ SystemControl and the individual IACP in the corresponding manuals. This note will not be repeated further on. Appropriate knowledge is required.

**Caution!**

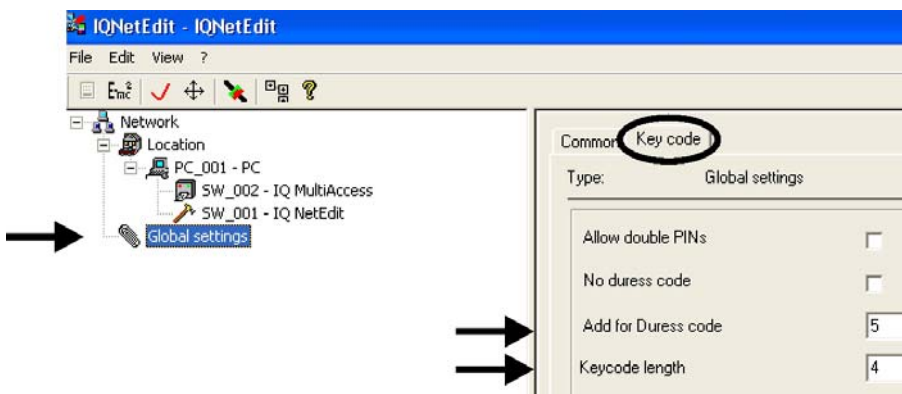


**Basically a data backup must be done on both systems before updating to the new version and before starting the connection of both systems.**

The manufacturer is not liable for data loss, direct or indirect consequential damages of all types occurred by inappropriate handling.

1. Preparation of the IACP (see manuals of the corresponding central units and their programming software).
2. Start IQ NetEdit (see chapter 4)
3. Set identic duress code (addition digit) and hold-up code (addition digit) at both systems.

Set identic keycode length at both systems (4 up to 8 digits).



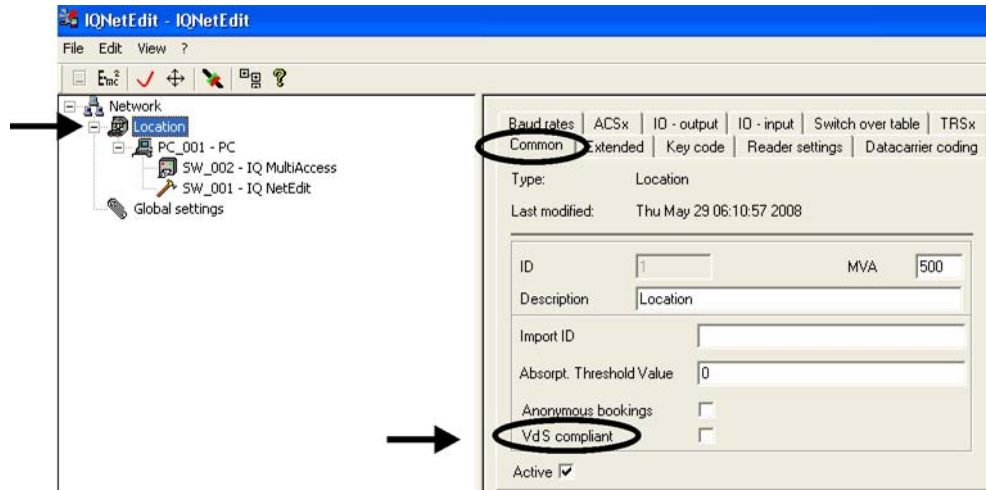
The values entered at **Global settings** are used as default settings for new created locations and as inspection values for the PIN-presetting in the personnel master files of IQ MultiAccess.

4. Select a location for the IACP.



By use of mifare DESFire EV1 data carrier (MB-Secure in preparation) **or by use of different type of readers** note the information in chapter 17.

If necessary, activate **VdS compliant** in the **Common** tab. If active, a location manager has no authorization to enter, change or delete authorizations for disarming within the room/timezones.

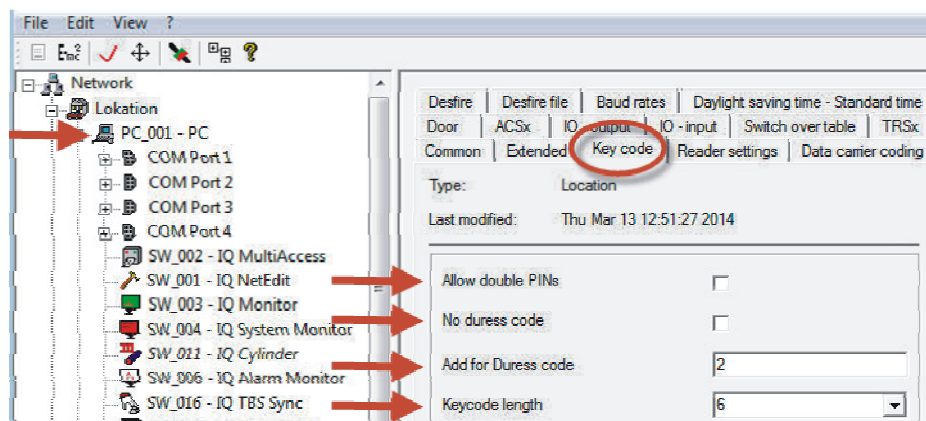


Settings in the **Key code** tab:

Do not activate **Allow double PINs**.

Do not activate **No duress code**.

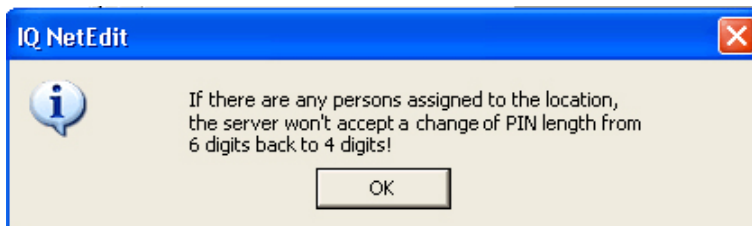
The settings of identic **Add for duress code** and identic **Keycode length** for both systems (4 up to 8 digits) have already been preset by the global settings (step 3). Modify only if these values deviate in this location.



Problem:



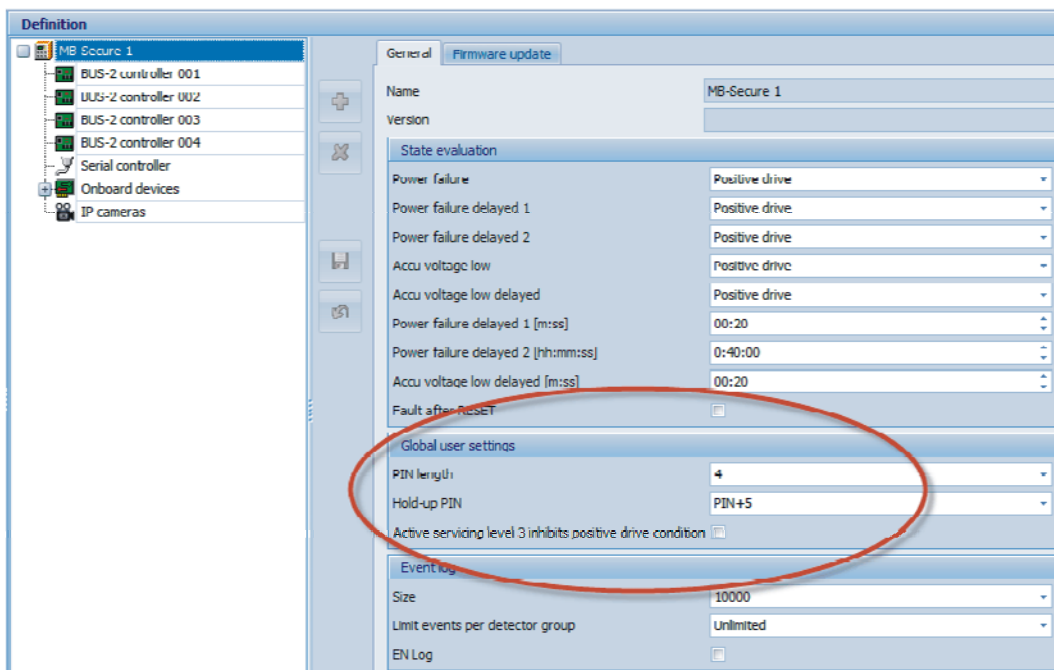
The addition number for duress can not be changed after persons are already allocated to a location as this could cause overlappings of a PIN/door code with a duress code of a door or person.



Solution:

Create a separate location for the IACP connection. As long as no persons are entered in this location, the basic settings can be modified according to the IACP's requirements.

5. Use the software **IQ PanelControl** to set up the corresponding values of identic **Add for hold up PIN** and identic **PIN length** for both systems (for detailed information see the documentation of the panel MB-Secure).



6. The workstation controlling the IACP require the programs as follow (right-click → Insert → Software):

- IQ MultiAccess
- IQ Monitor
- IQ SysMonitor
- IQ NetEdit (already assigned to the workstation of the standard location as a factory setting)

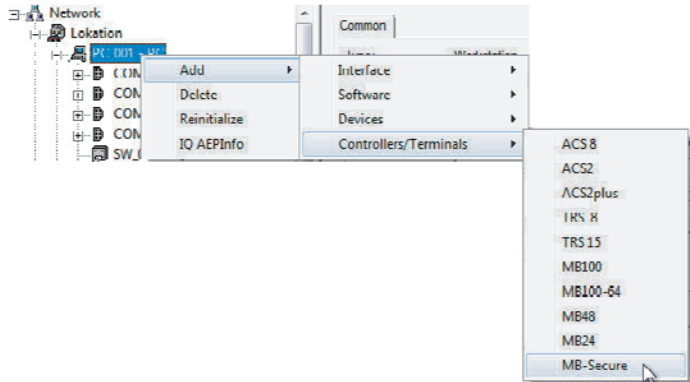


We recommend to start and connect the installation supporting programs **IQ Monitor** and **IQ SysMonitor** (see chapter 13).

7. Insert an MB-Secure panel

### TCP/IP transmission

Define a workstation with an TCP/IP connection to the MB-Secure.



There are as many as desired intrusion alarm control panels to be set up in IQ NetEdit.

### → Common tab

Enter an unambiguous description the intruder alarm control panel is listed in IQ MultiAccess.

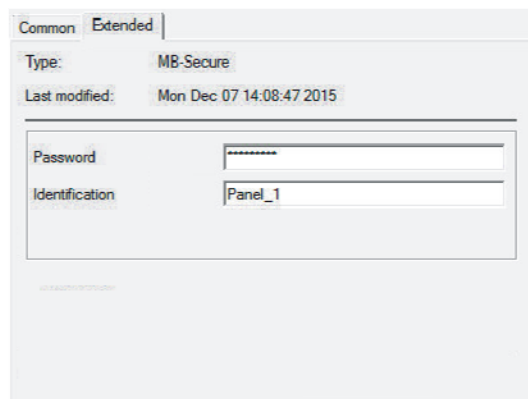
Enter the **own IP-address of the IACP** in the field **IP-address**.

The field **TCP/IP-Port** should remain (or be set to) the factory setting of the IACP (12355).

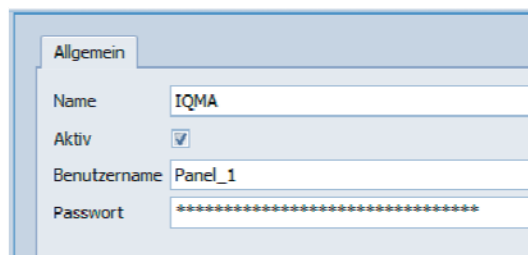
 A screenshot of the 'Common' tab configuration window for an MB-Secure device. The window has two tabs: 'Common' (selected) and 'Extended'. The 'Type' is 'MB-Secure' and 'Last modified' is 'Mon Dec 07 14:08:47 2015'. Below this, there are fields for 'ID' (14) and 'No' (8). The 'Description' field contains 'TE\_014 - MB-Secure'. Further down, the 'IP address' field contains '192.168.3.34' and the 'TCP/IP port' field contains '12355'. At the bottom, there is an 'Active' checkbox which is checked.

→ **Extended tab**

Transfer the required IACP data to IQ NetEdit.  
 Enter the same password and identification as in the  
 corresponding input fields of IQ PanelControl.

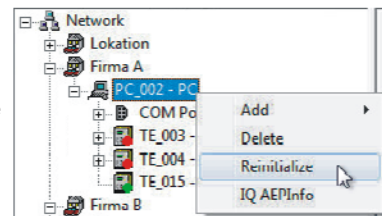


In the input field of the programming software IQ  
 PanelControl the user name for identification in the software  
 IQ Multi Access is entered. Also you must enter the  
 password here.

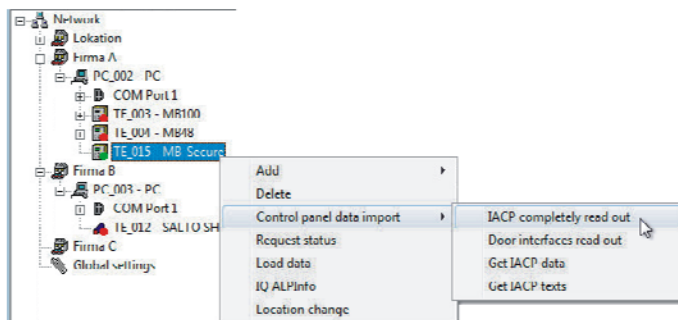


Right-click the workstation to which the IACP is connected  
 → Reinitialise.

With a correct working connection the corresponding panel will be  
 displayed with a green dot.



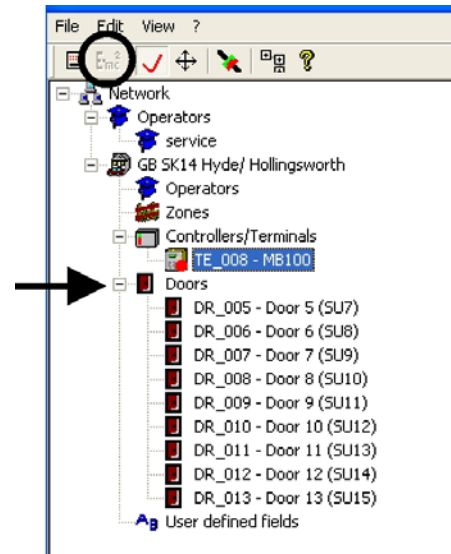
With an existing and working connection the  
 data of the panel can be read out. By right-  
 clicking the selected IACP → **Control panel  
 data import** → **IACP completely read out**,  
 all the recognized door interfaces will  
 automatically be set up in IQ NetEdit.



Optionally the menu items → **Get IACP texts** and → **Get IACP data** can be selected. If not, the operating  
 unit authorisation groups of the panel and the individual panel texts of the panel will automatically be  
 transferred before the first parametrization (in case that data carriers have already been entered (new) in  
 IQ SystemControl/IQ MultiAccess and should not be overwritten by old data of the panel).

8. Door data:

After scanning there are doors in IQ NetEdit with the designation DRxx = door unit with numbering of the IACP.



Check / set each door:

Times (outside/inside): Definition of times for individual timers, some separated according to the door sides.

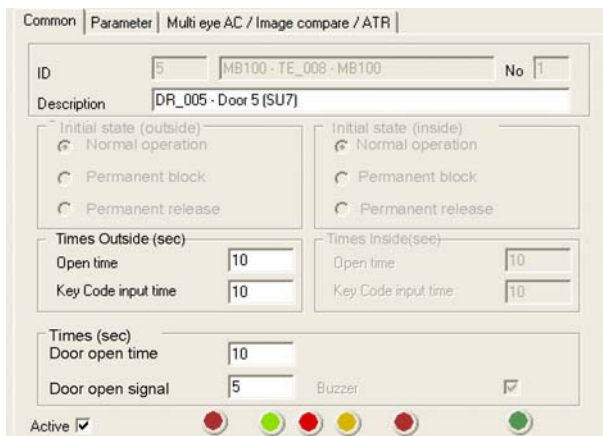
Open time: Activation time of the door strike. During this time the door can be opened.

Key code input time: Within this time the key code (→ PIN or → door code) must be typed in. If the code is not entered completely after this time has expired, the complete entry must be repeated.

Door open time: Maximum time a door is allowed to be open. It starts when the monitoring contact indicates the actual opening of the door. After expiration of this time an alarm will be triggered (Door opened too long).

Door open signal: If a reader/keypad is equipped with an internal buzzer, it indicates on the beginning of the door open signal time that the door should be closed as otherwise the door open time expires which causes an alarm (Door opened too long).

The time for the door open signal should always be shorter than the door open time in order to remain enough time for closing the door. The door open signal time ends at the same time as the door open time.



Operation mode (outside/inside):

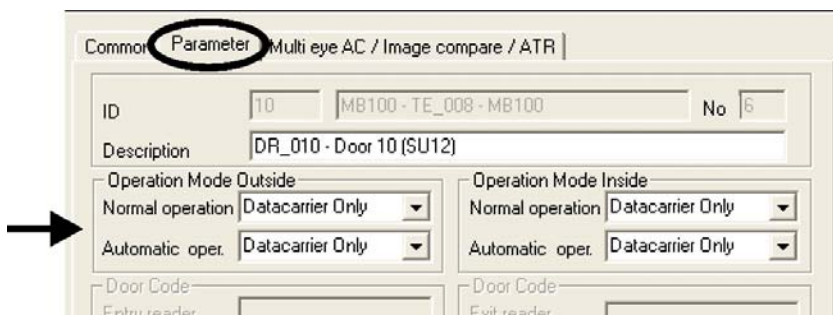
For each door side there can be defined a type of identification required for entry:

- Data carrier only
- PIN only
- PIN + data carrier
- PIN or data carrier
- Without time check
- Access inhibited

There is always one criterion to be valid for one operation mode:

Normal operation: The selected access criterion is valid for the door being in **normal operation**.

Automatic operation: The selected access criterion is valid while the door is set to **automatic operation**. Automatic operation can be used to set the door to permanent release / permanent block at predefined times (examples see user manual).



## 15.13 Data exchange

### 15.13.1 Data acceptance from IACP

By linking both systems, the IACP and IQ MultiAccess, all data relevant for the door interfaces (doors) and data carriers (persons) are centrally administrated in IQ MultiAccess. For the initial connection of both systems the already existing data of the IACP must be either transferred to IQ MultiAccess or newly created there.



Pay absoluteley attention that all relevant settings are identic at both systems, then starting the data transfer (see chapter 15.3).

#### Get IACP texts

Right-click the required MB-Secure → Get IACP texts.

All customer specific designations of switching devices, inputs/outputs etc.will be received. They are required for the evaluation of the eventlog via → **Logdata IACP**

#### Get IACP data

Right-click the required MB-Secure → Get IACP data.

This program section transfers all operating unit authorisation groups, room/timezones, data carriers and their authorizations (data carrier no. name, IS-code and PIN) to IQ MultiAccess.



If the transfer of those two data have not been done before the first parameterizing of the IACP, IQ MultiAccess will automatically get the data of the IACP before the parametrization gets started. This guarantees the users being still able to log in to the operating units.

This data transfer is not viewd on the screen. These operations can be visualized via the installation supporting programs → **IQ Monitor** and → **IQ SysMonitor**.



Contrary to the AC-controllers, the MBxxx will **not** be parameterized automatically on exiting IQ NetEdit. This must be done manually **for the first time** (see 15.13.2). Only accordingly relevant data will be updated automatically.



### 15.13.2 Data transmission from IQ MultiAccess

The initial parameterizing / loading data must be executed manually.



**Caution!**

**Check, and if necessary correct the data transferred from the IACP in IQ MultiAccess before the first parameterizing.**

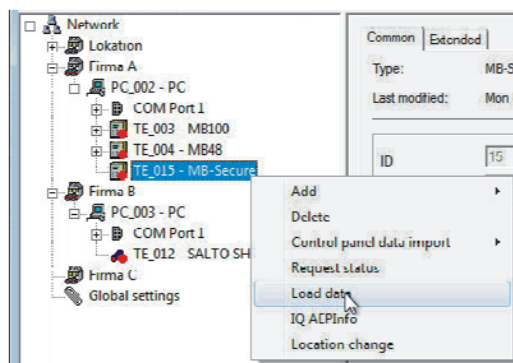
#### Activation of IQ MultiAccess connection

IQ PanelControl	Explanation
<ul style="list-style-type: none"> <li>→ IQ PanelControl - Configurator</li> <li>→ System tab</li> <li>→ Navigation area → Remote clients</li> </ul> <p>Access via                      IQ MultiAccess / IQ SystemControl Active <input checked="" type="checkbox"/>                      Input of User name and Password.</p> <p>After that → Send configuration to the panel.</p>	<p>Data of the MB-Secure panel can be read out and take over with IQ MultiAccess or IQ SystemControl.</p> <p>AC-functions, such as brief release, permanent release, permanent lock affect directly on the door(s) at the push of a button within IQ MultiAccess, IQ SystemControl or IQ NetEdit.</p>
<ul style="list-style-type: none"> <li>→ IQ PanelControl - Shell</li> <li>→ Navigation area → Panels</li> <li>→ Kontextmenü → Service functions</li> <li>→ Other tab                             <ul style="list-style-type: none"> <li>→ Read from panel</li> </ul> </li> </ul> <p>Checkbox                      IQ MultiAccess / IQ SystemControl full access <input checked="" type="checkbox"/></p> <p>After that → Send configuration to the panel.</p>	<p>Data created in IQ MultiAccess or IQ SystemControl affect directly on the intruder alarm control panel and can no longer be defined via IQ PanelControl.</p>

Create actions in IQ MultiAccess which display messages in case of transmission faults (see user manual chapter 10.3). Do not exit IQ MultiAccess in order to display messages when they occur. These messages do already exist in IQ SystemControl in ex-works condition.

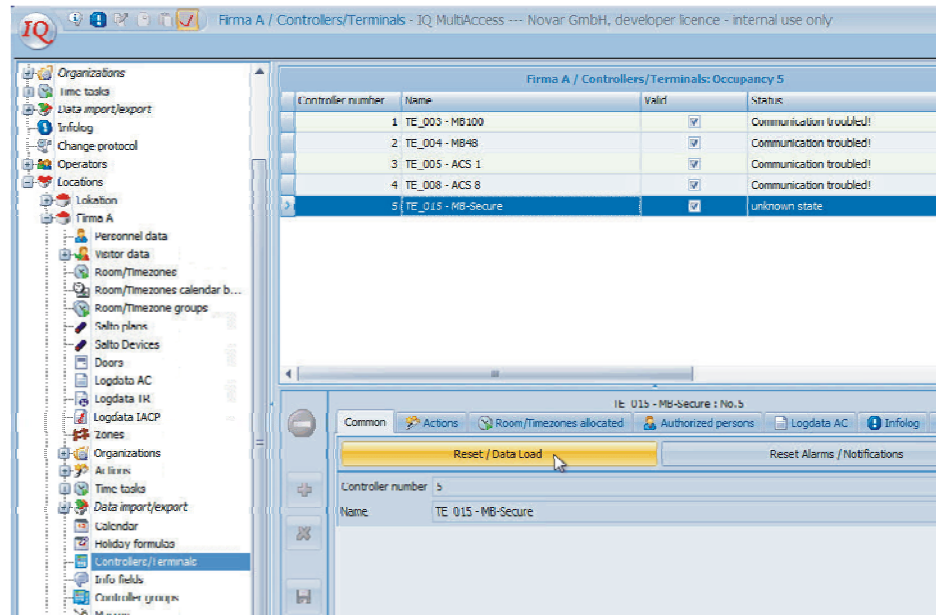
#### Load data from IQ NetEdit:

Right-click the selected MB-Secure → **Load data**



**Load data from IQ MultiAccess:**

- Controllers/terminals
- Select the required MB-Secure
- Reset / Load data



With an online connection (via TCP/IP) from now on the modified data will be automatically transferred to the panel after saving.



From now on the data which are administrated by IQ MultiAccess can no longer be administrated directly at the panel via IQ PanelControl.

## 15.14 Data administration via IQ MultiAccess / IQ SystemControl

For detailed descriptions of the creation and administration of the room/timezones, data carriers (persons) and their authorizations see user guide of IQ MultiAccess (P32205-20-0G0-xx) and/or IQ SystemControl (P03118-20-0G0-xx).

## 15.15 Evaluations in IQ MultiAccess / IQ SystemControl

For detailed descriptions of evaluation possibilities see user guide of IQ MultiAccess (P32205-20-0G0-xx, chapter 13) and/or IQ SystemControl (P03118-20-0G0-xx, chapter 10)

## 15.16 Further information

- ✓ The installer should change the "Service"-password in order to have access to the system at any time and no unauthorized person has administrator rights (if necessary create a separate superuser for the system administrator, see chapter 2.5 and 8).
- ✓ Create individual location managers with corresponding rights (see chapter 8).
- ✓ Create a time controlled task for data backup, see user guide of IQ MultiAccess (P32205-20-0G0-xx, chapter 11.7) and/or IQ SystemControl (P03118-20-0G0-xx, appendix).
- ✓ Hardware subsequently connected to the IACP can be transferred to IQ NetEdit by another scan. This will not affect the already existing IACP-hardware.
- ✓ Operating rights of users for operating units are managed by means of operating unit authorisation groups. Programming and configuration of the operating unit authorisation groups is made with IQ PanelControl when programming the MB-Secure panel. When installing IQ MultiAccess the operating unit authorisation groups of the MB-Secure panels are transmitted to IQ MultiAccess.

### 15.17 Checklist for IACP linking (MB-Secure panels)

Deliverables/ check and set if necessary				OK
IACP	Backup data			
	Prepare for remote parametrization			
	Activate access for IQ MultiAccess	IQ PanelControl - Configurator. Remote Client - IQMA	Send configuration to panel	
	Activate full access for IQ MultiAccess	IQ PanelControl - Shell. Service function - IQMA	Send configuration to panel	
IQ NetEdit	Global settings	Duress code (Hold up code) Define PIN length		
		Disable double PINs		
		Addition digit for duress		
		Keycode length		
		Assign software - IQ MultiAccess - IQ NetEdit - IQ Monitor - IQ Sysmonitor		
		- start IQ Monitor		
		- start IQ Sysmonitor		
	Set up MB-Secure	connection type TCP/IP	Password Identification IP-address TCP/IP-Port	
	Right-click on MB-Secure	Control panel data import IACP completely read out		
	Check door data	Type of identification for normal operation		
		Type of identification for automatic operation		
		Open time		
		Keycode input time		
		Door open time		
		Door open signal		
IQ MultiAccess / IQ SystemControl	Room/timezones incl. door / switching device allocation			
	Data carriers incl. RTZ-allocation			

Deliverables/ check and set if necessary				OK
	Create actions for communication fault	User manual IQMA chapter 10.3, IQSC already existing per default		
	Time controlled task for data backup	User manual IQMA chapter 11.7, IQSC appendix 2.7		
	Time controlled task for loading holidays	User manual IQMA chapter 11.6, IQSC appendix 2.76		
IQ MultiAccess / IQ SystemControl	Backup data create a time controlled task if necessary	User manual IQMA chapter 11.7, IQSC appendix 2.7		
IQ NetEdit or IQ MultiAccess	Load data per MB-Secure	<b>Manually</b> required for the first time		
IQ NetEdit	Change Service-password			
	Create location managers			

## 16. Door guard connection

Escape doors must not be locked and can so be opened using the door handle without identification. Door guard is a device to be connected to an intruder alarm control panel in order to monitor non-authorized openings of such a door and triggers an alarm if necessary.

### Setup in IQ NetEdit:

All hardware connected to an intruder alarm control panel, master files and texts will be recognized on initial connection of an IACP to IQMA (cf. chapter 15)

Subsequent installation of door guard devices:

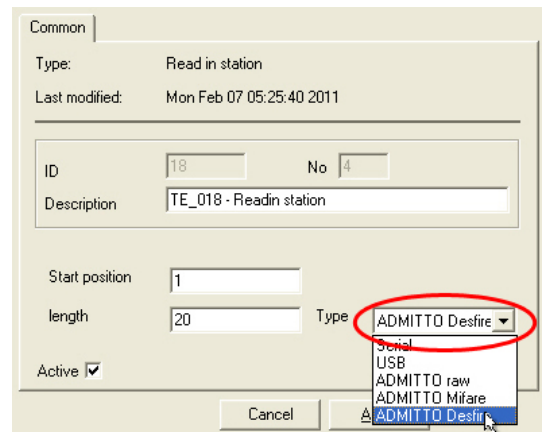
Insert a switching device at the respective intruder alarm control panel according to installation instructions (P32205-26-000-xx, chapter 15.3, step 8. Select **door guard** in the field **type**.

## 17. Mifare DESFire EV1 data carrier

### 17.1 Installation

1. Installation of the USB desktop reader and the concerning drivers according to chapter 6.4.1.1.

2. Insert at the appropriate workstation a read-in station to the COMx interface allocated by the operating system (c.f. chapter 6.4.1.1).  
Type: Admitto Desfire.



3. Settings of the concerning location / the concerning reader:

- a) Reader settings tab:  
Reader type: Mifare Desfire var. DIN



b) Data carrier Coding tab

c) Tab *Desfire File*

Here, an application is operated in the data area of the DESFire card. Applications can be used with DESFire and DESFire EV1 cards. **To ensure the highest security level possible, we recommend the use of DESFire EV1 cards.**



It is only when parameters are entered in this tab that the two keys that can be recorded in the Desfire tab are read keys for the application and used for a key change. If no parameters are entered, both keys that that can be recorded in the Desfire tab are the general pass keys of the card. For this reason, when programming for Desfire File, care must be taken to ensure that the hardware deployed uses the corresponding (latest) firmware versions.

When the function Desfire File is activated, the data required by the system is read out from or written into the corresponding data area of the DESFire/DESFire EV1 card.

Key PICC (PICC = Proximity IC Card): Denotes the general pass key of the DESFire/DESFire EV1 card. This can be generated by pressing “Gen. (generate)” or entered directly (values: 32 characters hexadecimal 0-9 and A-F combined in any desired sequence), and must be carefully backed up using the export function. **The PICC key must be defined once at setup** and may not be amended thereafter during operations.

When AES encryption for PICC is activated, the general pass key is encrypted on the card via AES encryption. In other cases, the Tripple DES encryption procedure is used (AES only with DESFire EV1). When “Activate random ID” is activated, the card logs into the reader with a random ID, preventing tracking (pursuing, key sensing) of the ID card.



Once set, a random ID on DESFire EV1 cards cannot be cancelled. To maintain the highest possible compatibility between different applications, Random ID should remain deactivated. During the operation of the DESFire cards, the two check boxes (“AES encryption”, “Random ID”) should not be set. Any option can be set when DESFire EV1 cards are in operation (ensure compatibility with other applications).

The following two check boxes on the tab control the rights for application listing and new application definition, ensuring these are available only with the PICC key.

Main key Appl: This is the general pass key of the application. A key for the application is saved at the time of initial installation. This, like the PICC key, can be generated by pressing "Gen. (generate)" or entered directly (values: 32 characters hexadecimal 0-9 and A-F combined in any desired sequence), and must be carefully backed up using the export function. The **general pass key of the application must be defined once at setup** and may not be amended thereafter even during operations.



Novar has its own registration for the application ID used.

If a key change is required by rotation, the new and the old key are entered in the Desfire tab. (Carry out the key change as described below in 17.1.1).

If earlier installations have to be migrated to the "Desfire File" system, proceed as follows:

- All cards on the site must have the current primary key, e.g. Key A.
- Backup this primary key using the export function.
- In the Desfire File PICC tab, click on the checkbox Set/Use and import this key as "PICC Key" using the import function.
- Use AES encryption.
- Then scan in all cards again using IQ MultiAccess / IQ SystemControl so that the application is launched.

d) Desfire tab

At least **one of the two** possible keys (encryption codes) must be added and defined as a primary key (Key A, Key B).

There are 2 keys (encryption codes) to be deposited (key A, key B). Input manually or via the "Generate" button. The display will read "xxxxxxxxxxxxxxxx", in addition a checksum will be displayed.

Values: 32 digits hexadecimal (0-9 and A-F arbitrarily combinable).

This code is used to encrypt the card data on the transmission path.

Key A is by default the primary key. Using one key only requires no further settings.

The screenshot shows a configuration window for the Desfire File tab. It contains two sections, Key A and Key B. Each section has a checked checkbox, a 'Key' field with a 'Gen.' button, a 'Checksum' field with an 'Exp.' button, and a 'Timestamp' field with an 'Imp.' button. Key A's checksum is 7FD2C53B and its 'Primary key' radio button is selected. Key B's checksum is 57CB91F and its 'Primary key' radio button is unselected. Both keys have a timestamp of Tue Oct 12 16:23:00 2010.



Save the settings/changes with the "Apply" button.

Important note: If no entries are made in the Desfire File tab (all check boxes unclicked) and only the keys of the Desfire tab are used, the following values are defined for DESFire EV1 cards: AES encryption for PICC, Random ID activated - only DESFire EV1 cards possible! Basically, this operating mode has been used up through IQMultiAccess version V12.

### 17.1.1 Changing the key

Depending on the configuration in the Desfire File tab, either the read key or the general pass key of the card is changed. The procedure for key changes is the same in both cases.

To prepare changing the key first a second key has to be entered in the *Desfire* tab.

At the changing time the new key must be marked as primary key - this causes an automatic switch of the previous key to secondary key.

The reader firstly tries to recognize the card data via the primary key while reading, if this is not possible, the secondary key will be tried. This method allows changing the key during business operation. The card owners have to have their cards programmed to the new key within a certain period of time. This can be done via a read-in station (e. g. in the personnel office) or via a self-service station IQKeyChanger.

After expiration of the transition period the secondary key will be deleted or replaced by a new key which later on will replace again the current primary key.

The key can be exported and imported using the Exp. and Imp. function keys, if e. g. all locations are to use the same key.



**Note! Cards, which have not been changed till then can no longer be read and reprogrammed. They must be depolluted.** IQMA provides by help (list function in the personal data) of the checksum a possibility to find out which cards have not yet been updated.

## 17.1.2 Setup of IQ KeyChanger

IQ KeyChanger is a software installed on a separate PC where each card owner can have switched his/her card to the latest primary key. This requires also a mifare Desfire read-in station at this computer (see above).

For updating the card to the latest primary key simply lay the DESfire data carrier on the read-in station.

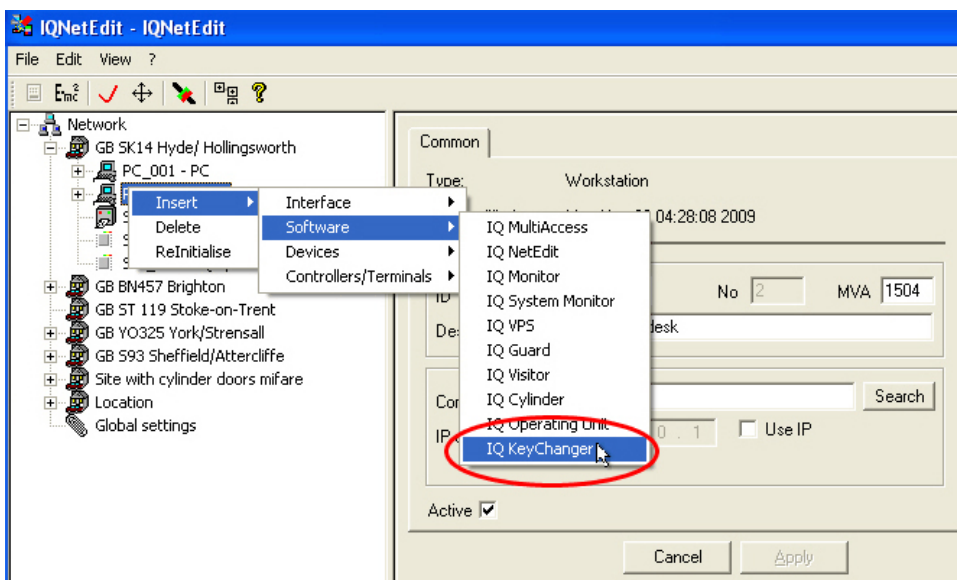
Display at the read-in station: LED yellow on

The current primary key will be written onto an authorized card laying on the read-in station.



Unassigned visitor cards will be reset to default key by this procedure.

Display with correct read / write process at the read-in station: green LED lights up for 5 seconds.





# 18. Connection of TBS biometric readers

TBS biometric readers are 2D or 3D contact-less fingerprint controllers for maximum recognition certainty.

1. Integration with IQ MultiAccess from V18 onwards and IQ SystemControl from V13 onwards requires appropriate licensing! The option may be purchased if required.
2. Installation of the TBS finger scanner and relevant driver based on the documentation accompanying the device. For details, refer to the original documentation of the relevant product.
3. The TBS finger scanner is installed and connected via a corresponding ACS-8 over the model bus connection of the controller or via a IK3 evaluating unit and the corresponding intrusion alarm control panel.



The procedure for connecting the TBS is described step-by-step below.

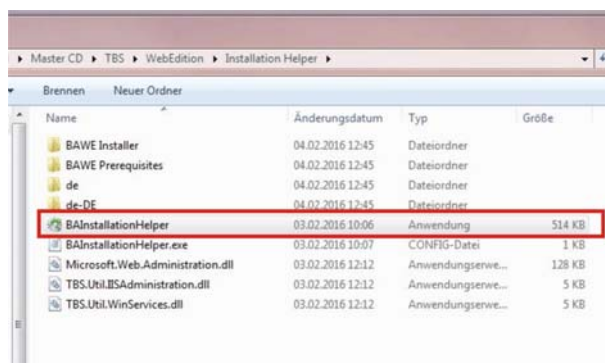
## 18.1 Installation TBS-Software

(Install once on server / driver installation for Enrolls on IQMA clints:

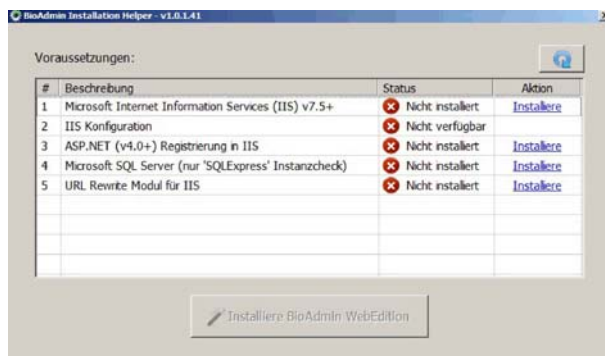
TBS Installation CD\TBS\Driver\2D or 3D)

1. Insert TBS DVD
2. Go to directory:  
MasterCD \ TBS \ WebEdition \ Installation Helper \

Double-click: → **BAInstallationHelper** application  
(not exe file!)



3. Necessary drivers and software are checked, missing components are displayed in the status column, click → **Install** if necessary in the action column. Once all components are installed, proceed to step 11.  
→ **Install BioManager WebEdition.**

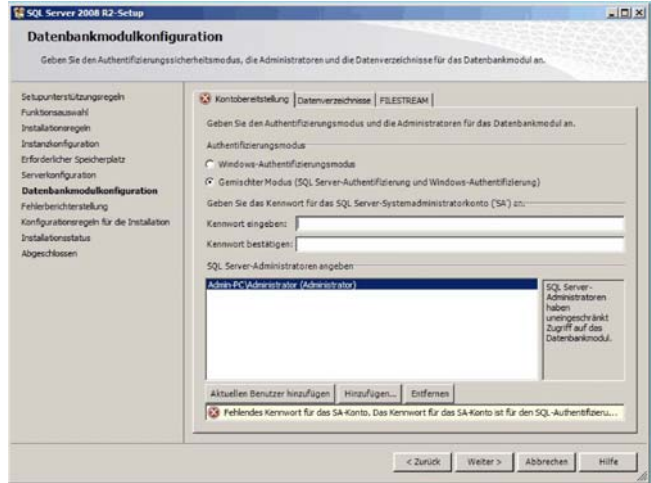


4. Required settings are shown on the left. Settings on the local computer are shown on the right. Tick the appropriate checkbox as shown in the figure to the left, then click → **OK**.  
Sometimes, you may have to wait longer for the installation to complete. Please wait for the next screen!



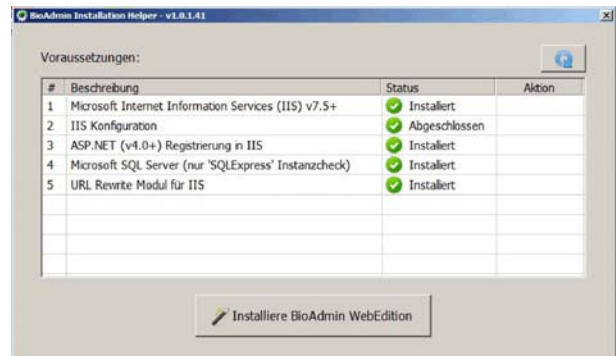
5. Repeat the process for all drivers that were not found on the system.

- 6. During the installation of SQL server, tick the checkbox **→ Accept Licensing Conditions**, then **→ Next**.  
Accept suggested defaults by clicking **→ Next**.



- 7. Enter a password of your choice (at least 9 characters, upper/lower case, numbers and special characters allowed (e.g. "Honeywell1!))
- 8. After the installation completes, click **→ Close**.
- 9. To set up the IIS URL, tick the checkbox **→ Accept License Conditions**, then click **→ Install**.
- 10. After the installation completes, click **→ Finish**.

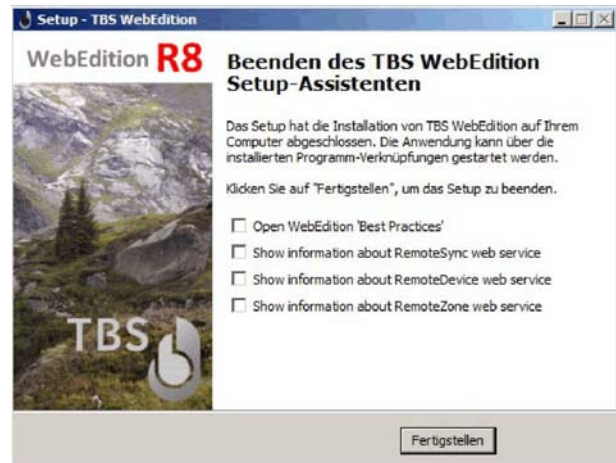
- 11. Click **→ Install BioManager WebEdition**.



- 12. Confirm with **→ OK**.



- 13. Accept default values with **→ Next**.
- 14. Tick checkbox **→ I accept the terms and conditions**, then click **→ Next**.
- 15. Accept default values with **→ Next** (Multiple windows), then click **→ Install**, **→ Next** (Multiple windows) and **→ Finish**.
- 16. Click **→ Complete**.
- 17. Message: IIS Services started, confirm with **→ OK**.

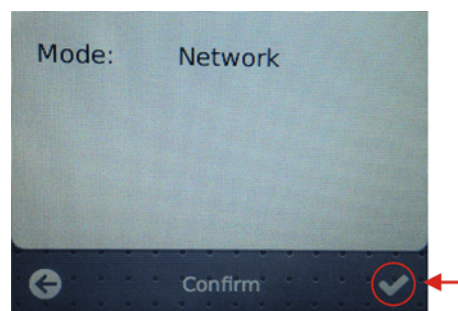
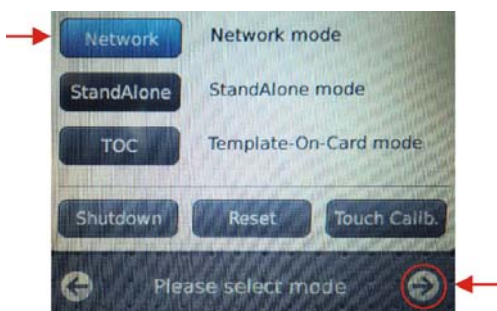


## 18.2 Install and configure TBS devices



You can find installation instructions on the TBS DVD in the file:  
TBS\Mounting and Installation\TBS Mounting and Installation Instructions.pdf

1. Connect the TBS device to the computer (Ethernet cable/switch). Terminals are placed on the DHCP (factory settings). The computer and terminal must be in the same address range.
2. After initial commissioning the TBS display shows → **Select Mode**.  
Select → **Network** (tap on screen) and confirm with button → **Arrow**.  
Confirm a second time with button → ✓.

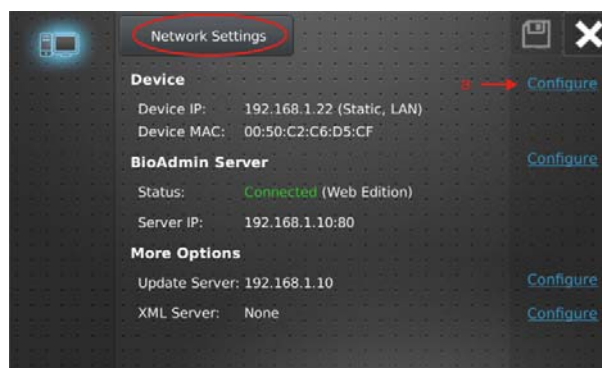


(3D Terminal can alternatively display *WE mode* instead of *Network mode*).

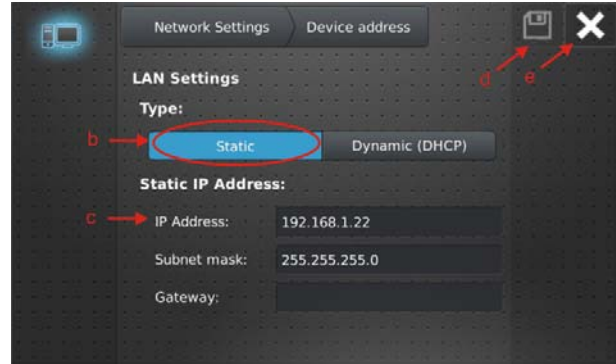
3. Access via sequence from → **right to left**  
(Only when display from point 4 does not appear automatically).



4. Tab → **Network Settings / Device**
  - a. Select → **Configure**



- b. LAN Settings, tab → **Static** recommended
- c. Input of the IP Address
- d. → **Save** (tap on disk symbol)
- e. End with → **X**

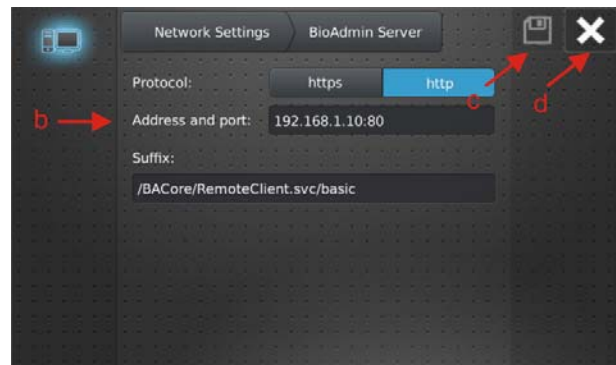


## 5. Configure BioAdmin (BioManager)

- a. Tab → **Network Settings / BioAdmin Server**  
Select → **Configure**

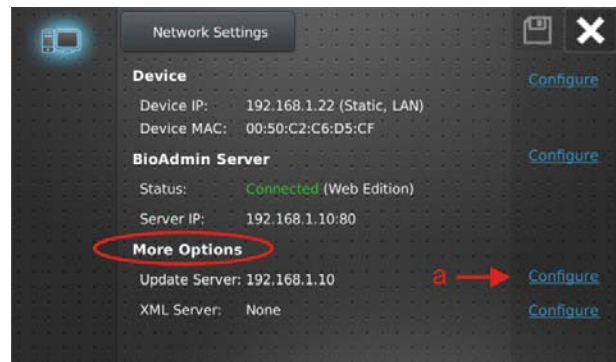


- b. Input of the IP address of the computer TBS is installed (could be the same computer as IQMA runs).  
The port will be added automatically using “:” as a separator, (standard = 80).
- c. → **Save** (tap on disk symbol)
- d. Exit with → **X** (2 times back to start screen)

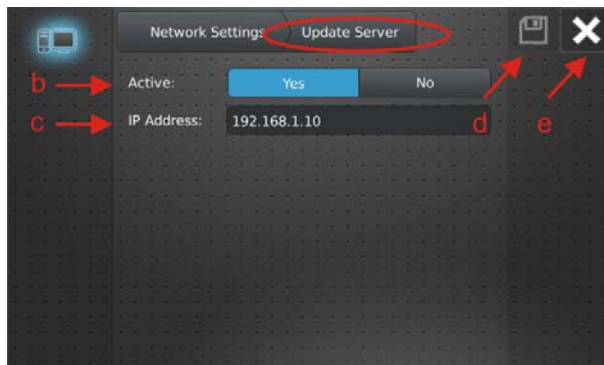


## 6. More options

- a. Install of Update Server  
Tab → **Network Settings / More Options**  
Select → **Configure**



- b. Activate Update Server  
Confirm with → **Yes**
- c. Input of the IP address of the computer BioManager runs.
- d. → **Save** (tap on disk symbol)
- e. Exit with → **X** (2 times back to start screen)



7. Activate Honeywell mode

Activate Honeywell modus by input in browser:

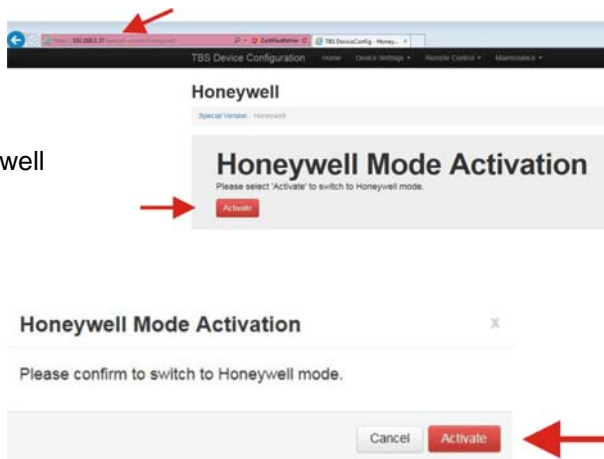
<http://<IP-address of terminal>/special-version/honeywell>  
(z.B. <http://192.168.0.37/special-version/honeywell>)

Confirm with → **Activate**

Additional security query

Confirm with → **Activate**

Wait until terminal finished reboot (displaying Honeywell-Logo).



### 18.3 Start BioManager

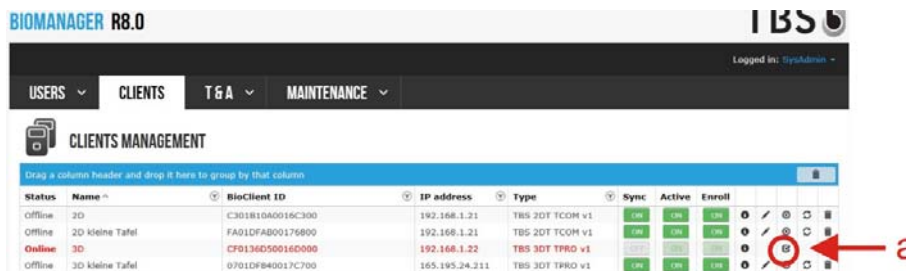
- 1. Enter in a browser → **localhost/bawebclient**  
User (Operator ID): sysadmin  
Password: 12345678



If an error message appears instead of the BioManager start screen, execute the file "x64" (64-Bit-version) or "x86" (32-Bit-version) from TBS installation-DVD to be found in \TBS\WebEdition\InstallationHelper\BAWE-Prerequisites\URL-Rewrite Reason: The IIS-settings can be modified by previously installed programs, which also need IIS-services.

- 2. In BioManager / Clients / the terminal is shown red.

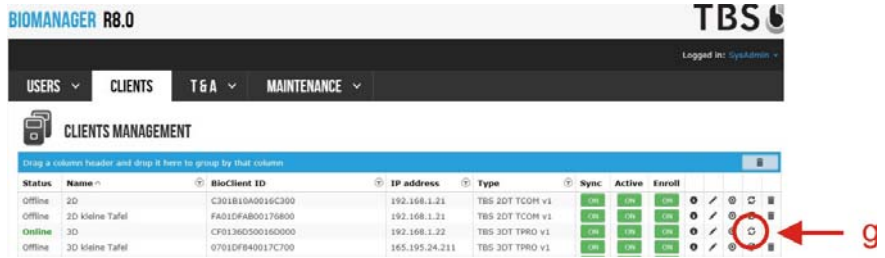
- a. Validate Client  
(Symbol circle with hook)



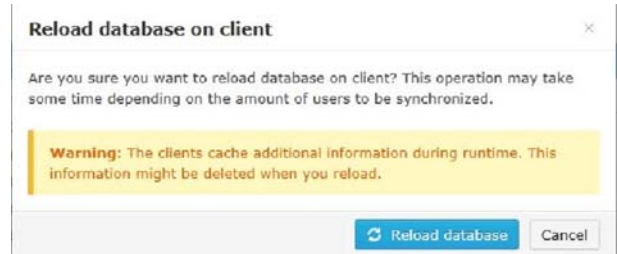
- b. Name (designation of door)
- c. Sync: ON
- d. Repeat name of step b. (designation of door).
- e. Enroll: ON
- f. Confirm with **→ Validate**



- g. Reload DB on Client (Symbol circle / 2 arrows)



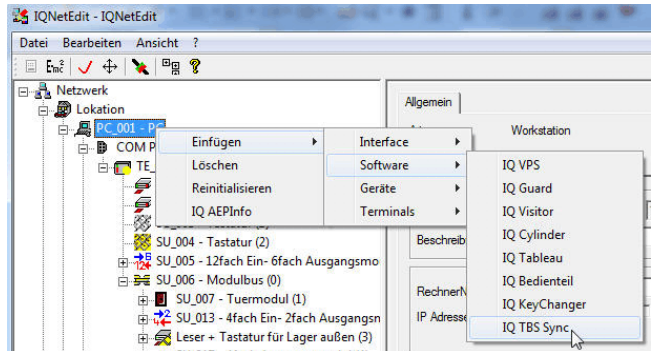
Confirm information in next window by clicking **→ Reload database.**



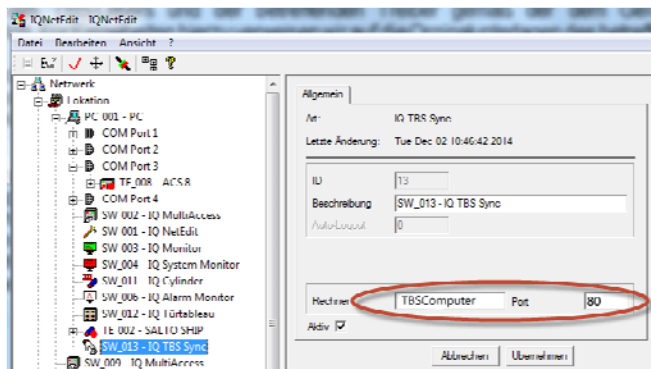
## 18.4 Connection to IQMA

### 18.4.1 Setting up IQ NetEdit

1. TBS Sync software can be installed at the desired location. This is a service that allows user and card data to be synchronized. It is recommended that this service be installed on the same PC as the IQ server.



Enter the computer name and its corresponding TCP/IP port in the input field (here, port 80 for example).



If necessary install TBS Sync (will be done normally within the installation of the TBS option). Observe during a post-installation:

- Setup -> Repair -> add this point
- or
- Honeywell -> IQ\_MultiWin -> IQ\_Services -> IQ\_Setup -> Setup TBS.exe

Using the IQ TBS Sync service, the file IQTBSSync.exe.config (in the IQ\_Services directory) is installed on the computer which contains the configuration data. This file can be viewed or edited using a text editor (e.g. Notepad).

**No changes should be made to this file for a standard installation.**

```
</configSections>
  <IQSERVER ServerIP="127.0.0.1" ServerPort="23757" />
  <BranchSync="0" />
</configuration>
```

Take the IP addresses and ports for the entries IQSERVER and IQTBS into consideration, or change them if the system is running on some other computer on the network. Setting for BranchSync:

- 0 ▲ 1 site (lokation)
- 1 ▲ Multiple sites (lokations, only with location extension). In this operating mode, care must be taken to see that the same card encoding and PIN is used for individuals at all sites.



**TBS software is required and must be purchased, therefore, this value should not be changed!**

2. Integrate the reader into the system within IQ NetEdit (ACS-8 > Module bus). Set the relevant reader type in the tab "Reader Settings" (also see chapter 6.4).  
Type: TBS reader - var. DIN
3. Definition of doors in IQNetEdit in based on the configuration (see Chapter 6.5, Defining Doors).



Note: During commissioning in the Web client of TBS (BIOADMIN WEB CLIENT) a one-time synchronization of all recorded user and all IQ read-in stations must be made.

From now on all relevant master data from IQMA will be synchronized with TBS and are visible in → **BioManager** in the → **USERS tab**, e. g. IQUSRxxx.

## 18.4.2 Set up IQ MultiAccess

1. Start → IQMA.
  - a. Add new person in location / must have an IS-code (Enter IS Code in "Data carriers" tab or read in transponder).
  - b. Tab → Zutrittsdaten → Parameter  
→ TBS role to → Admin.  
→ Save



If the first time a fingerprint is recorded in IQMA/personal data, IQMA is listed in the BioManager software and is to be validate. (As described in section 18.3). **Therefore, make sure that the BioManager is open in the background.**

The screenshot shows the 'Parameter' configuration window. The 'TBS' field is set to 'Admin'. The 'Role' field is also set to 'Admin'. Other fields include 'Language' (Central language), 'last booking' (24.09.2014), and 'MR-Secure'. The 'Access Control' section has 'Via Room/Timczones and groups' selected.

- c. Click button → **Capture fingerprint**

The screenshot shows the 'Personnel data' tab with fields for Name (Last name: Schlegel, First name: Danny), Organization (Entry date: 10.10.2014), and Department/Cost center/Working group (all set to 'no assignment'). On the right side, there are buttons for 'Create person-layout', 'Print person-sheet', 'Create layout', 'Print layout', 'Get image', 'Record signature', and 'Capture fingerprint'. A red arrow points to the 'Capture fingerprint' button.

Follow the onscreen instructions for capturing the fingers. For further information please refer to chapter "Enter personell data when use TBS biometric readers" in the User Manual to IQMultiAccess.

All further persons of IQMA will automatically be created with the role "USER". This has to be kept.



## 18.5 Set up address on TBS-Terminals



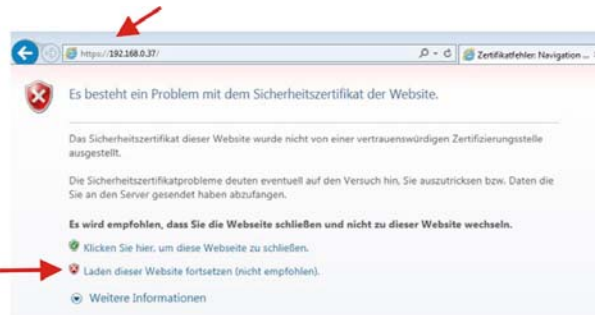
Standard address = 1, no change required.

If there are more than one devices connected to the bus system of a IK3-evaluation unit or a ACS-8, each device needs to get an individual address. This happens with the help of the connected PC and browser input.

Input of the IP address of the terminal into the browser:

<http://<IP-address of the terminal>>  
 (e.g. <http://192.168.0.37>)

Load website → “Continue the load of this website”.



User name: user

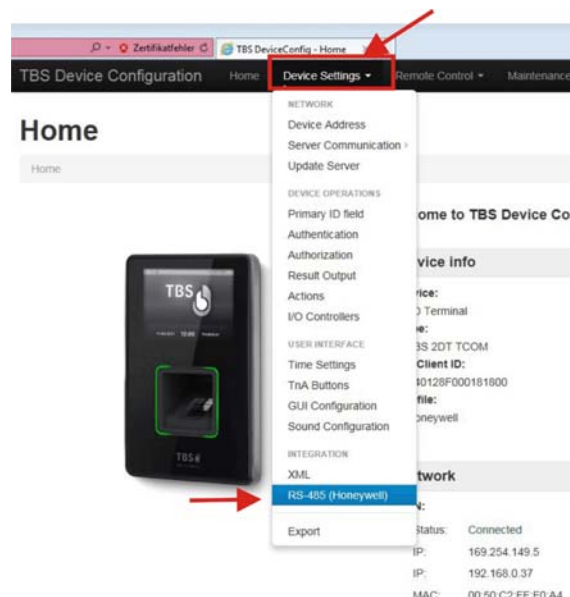
Password: 4TbsPartners



Menu opens → TBS Device Configuration.

Then proceed as follows:

- a. Open menu → **Device Settings**
- b. Dropdown menu → **RS-485 (Honeywell)**



- c. Enter address in field → **Device address**  
 (Valid addresses 1 - 8)  
 Confirm with → **Apply**



- d. Confirm with → **Apply changes**



e. Confirm with → **Apply changes**



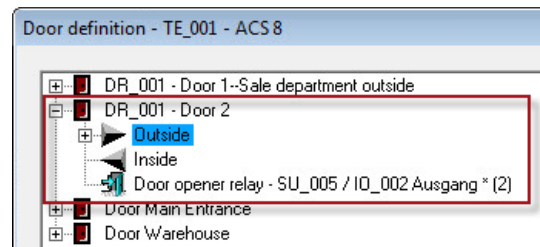
f. The address of the terminal has been changed → Wait until terminal finished reboot (displaying home screen).

## 18.6 Connection to Access Controller (ACS-8)

(Also see installation instructions, chapter 18.)

- IQ NetEdit
  - Setup ACS-8
  - Module bus
  - Reader with keypad
  - Address such as TBS terminal
  - Reader type: TBS var. DIN
- Right-click / Get version info TBS version is displayed.

- Door definition with minimum requirement
- Load data
- In IQMA, set up authorizations for persons (Room/time zones with TBS door)



## 18.7 Connection to MB Classic panels

(See installation instructions, chapter 15.)

- IQ NetEdit
  - Right-click on PC
  - Add
  - Terminals
  - Set up MBxx with appropriate connection
- Select MBxx and scan data
- Switching device matches TBS terminal
- IQMA - assign TBS door to room/time zones

## 18.8 Connection to MB-Secure panels

(For MB-Secure connection in general, see chapter 15.10)

Additional settings for TBS:

- IQ NetEdit
  - Right-click on PC
  - Add
  - Terminals
  - MB-Secure
  - Enter IP address
  - TCP / IP Port: 12355

# Appendix

## Modifications against the previous version

- Client IQ MultiAccess performance improvements.
- New variables for text input for the actions.
- Individual storage path for settings.
- Additional selection menu for read-in stations.
- Number of user-defined fields now 40.
- Support of DESFire EV1/EV2 for MB-Secure.

## IQ MultiAccess products

Item No.	Product description
29601	Basic package IQ MultiAccess for 300 ID cards
29602	Basic package IQ MultiAccess for 500 ID cards
29603	Basic package IQ MultiAccess for 800 ID cards
29604	Basic package IQ MultiAccess for 1000 ID cards
29605	Basic package IQ MultiAccess for 1500 ID cards
29606	Basic package IQ MultiAccess for 2000 ID cards
29607	Basic package IQ MultiAccess for 3000 ID cards
29608	Basic package IQ MultiAccess for 5000 ID cards
29609	Basic package IQ MultiAccess for 7500 ID cards
29610	Basic package IQ MultiAccess for 10000 ID cards
29646	Basic package IQ MultiAccess for 10000 ID cards
29611	Database expansion MultiAccess from 300 to 500 ID cards
29612	Database expansion MultiAccess from 500 to 800 ID cards
29613	Database expansion MultiAccess from 800 to 1000 ID cards
29614	Database expansion MultiAccess from 1000 to 1500 ID cards
29615	Database expansion MultiAccess from 1500 to 2000 ID cards
29616	Database expansion MultiAccess from 2000 to 3000 ID cards
29617	Database expansion MultiAccess from 3000 to 5000 ID cards
29618	Database expansion MultiAccess from 5000 to 7500 ID cards
29619	Database expansion MultiAccess from 7500 to 10000 ID cards
29620	Database expansion MultiAccess from to 10000 ID cards
29621	Client processing ability option
29622	Antipassback/Barring Repeated Entry option
29624	Camera option
29625	Image and signature capture, layout and card print option
29626	IACP-connection option
13598	Virtual IACP operation unit option / IQ ControlCenter (1 x included in basic / professional package with option 029626)
29631	Professional package IQ MultiAccess for 300 ID cards
29632	Professional package IQ MultiAccess for 500 ID cards
29633	Professional package IQ MultiAccess for 800 ID cards
29634	Professional package IQ MultiAccess for 1000 ID cards
29635	Professional package IQ MultiAccess for 1500 ID cards
29636	Professional package IQ MultiAccess for 2000 ID cards
29637	Professional package IQ MultiAccess for 3000 ID cards
29638	Professional package IQ MultiAccess for 5000 ID cards
29639	Professional package IQ MultiAccess for 7500 ID cards
29640	Professional package IQ MultiAccess for 10000 ID cards
29647	Basic package IQ MultiAccess for more than 10000 ID cards
29641	Upgrade from MultiAccess for Windows to IQ MultiAccess
29642	Upgrade from MA Lite to IQ MultiAccess
29643	Upgrade from IQ SystemControl to IQ MultiAccess
29645	Upgrade from a previous version IQ MultiAccess to IQ MultiAccess current version
29650	Option SALTO for IQMA/IQSC
29651	Number of readers for SALTO

## Index

Absorption reader	62, 72
Account	7, 56, 59
Acoustic	57, 62, 65
ACSx	46, 59, 71, 98, 125, 127
ACS-1	8, 11, 16, 49-52, 57, 61, 62, 64, 72, 98-100, 104, 142, 144, 147, 148, 160-162, 183, 190
ACS-2 / 8	57
ACS-8	11, 16, 29, 46, 47, 49, 50, 66, 68, 69, 73-75, 77, 88-90, 92, 94-97, 105, 113, 114, 116, 117, 123-127, 135, 142, 144, 147, 148, 159, 161-165, 171-173, 177, 178, 184, 190, 265, 266
ACT	8, 11, 16, 52, 71, 72, 96, 129, 160, 164, 190
Activation Time	62, 65, 74, 78, 130, 228, 246
Address	8, 19, 21, 26, 42, 57, 59, 60, 62, 63, 84, 95, 96, 136, 140, 158, 161-165, 183, 184, 186, 217, 221, 223, 225-227, 236, 237, 244, 251, 259-261, 265, 266
Administrator	10, 12, 19, 21, 24, 28, 39, 60, 62, 83, 84, 186, 199, 235, 250
Alarm Control	7, 8, 17, 34, 48, 60, 62, 136, 158, 191, 209, 212, 213, 217, 220, 221, 223, 225, 226, 233, 234, 239, 240, 244, 249, 253, 257
Alarm relay	51, 62, 103
Alarm time	51
Antipassback	8, 39, 45, 49, 52, 57, 60, 64, 65, 159, 165, 268
Antipassback (APB)	39
Area	51, 56, 62, 78, 146, 159, 210, 220, 249, 254
Area code	146, 220
Area control	159
Auto address mode	162, 163
Auto update	32
AXS4Secure	11, 16, 95, 129
Bank	67, 68
Barring repeated entry (BRE)	39
Basekey	77
Baud rate	52
Baudrate	50, 52, 57, 78, 88, 142, 145, 158, 162, 177, 183, 184, 227
Blocking time	49, 50, 57, 210
Build	67
Bus controller	8, 11, 16, 42, 49, 52, 78, 79, 87, 90-94, 97, 101, 142, 144-148, 156, 158, 162, 164, 165, 177, 183
Buzzer	57, 62, 63, 65, 73, 130, 210, 228, 246
B-channel	143-145, 147
Card coding	53, 77, 162, 182
Card designer	23, 30
Card number	55, 62
Card print	268
CD number	58
Checklist	9, 236, 251
Client	7, 10, 14, 17, 19, 21, 26, 49, 50, 83, 131, 199, 201, 204, 251, 261-263, 267, 268
Clock data	70
Coding	53, 55, 56, 77, 98, 137, 162, 177, 182, 254
COM interface	18, 42, 55, 88-91, 154, 183, 223, 227
Communication status	87
Computer name	19, 21, 58, 60, 63, 186, 262
COM-Port	102, 202
COM-Port Server	202
Conversion	17, 31, 34, 215
Counter	64, 160, 161
Counters	64, 161
Current Loop	8, 17
Data backup	29, 33, 182, 214, 235, 237, 241, 250, 252
Database connection	40
Day plans	50
Daylight saving time	64
Debounce time	69, 70, 79

Delay time	69, 74, 79
Demo	21, 24, 30, 34, 81, 204
Door list	161, 183
Door strike	62, 65, 78, 106, 108, 110, 114, 117-119, 122, 130, 136, 172, 179, 228, 246
Duration of stay	60
Duress code	48, 71, 77, 175, 176, 191, 209, 210, 214-216, 236, 241-243, 251
Duress relay	51
DVA	8
Entry reader	50, 77, 129
EP	60
ESSER	53, 55, 80, 98, 177
Ethernet	16, 59, 95-97, 102, 137, 164, 165, 192, 212, 213, 239, 240, 259
Event memory	159
Event protocol	95
Exit reader	16, 50, 77, 129, 136
Expansion board	61, 78, 79, 160
Expiration	56, 57, 59, 61, 72, 130, 136, 228, 246, 255
Firebird	12, 13, 25, 28, 36
Firewall	23, 24, 31
Firmware	7, 11, 17, 29, 57, 66-68, 72, 102, 135, 162, 190, 213, 240, 254
Flashbank	66-68
Format	2, 30, 34, 131, 215, 232, 236
FTP server	59
Full version	24
Get/set counter	161
Global settings	25, 175, 176, 215, 236, 241, 242, 251
HotSync	19, 29, 133
Hyperterminal	149, 153
I/O board	64
I/O module	46, 124, 126-128, 148, 177-179
I/O number	59
I/O point	60, 161
IACP	8, 17, 34, 57, 62, 63, 71, 136, 159, 160, 175, 191, 209, 210, 212, 214-228, 230, 232-239, 241-246, 248-251, 253, 268
IACP connection	216, 220, 243
ID Card	36, 50, 51, 55, 56, 72, 137, 163, 183, 209, 210, 254
IDX	78
Image matching	58, 64, 72, 161
Indexing	50
Infrared	134
Initialization PIN	134
Interface converter	17, 89, 158, 161, 177, 178
Intruder alarm	7, 8, 17, 34, 60, 62, 136, 191, 209, 212, 213, 217, 221, 223, 226, 233, 234, 239, 240, 249, 253
IP address	19, 60, 62, 63, 84, 95, 96, 140, 165, 186, 237, 260, 261, 265, 266
IQ CommTask	13, 35, 87
IQ Cylinder	17, 19, 29, 32, 35, 65, 131-133
IQ Guard	35, 58
IQ Monitor	35, 68, 180, 183, 199, 216, 232, 236, 243, 248, 251
IQ MultiVPS	204
IQ OPUNIT	61
IQ Server	13, 14, 21, 24, 37, 38, 66, 131-133, 137, 140, 212, 239, 262
IQ StartServers	13
IQ StopServers	13
IQ SysMonitor	35, 199, 201, 216, 232, 236, 243, 248, 251
IQ Video	35, 72
IQ Visitor	35
IQ Vtableau	35
ISDN	11, 17, 60, 97, 141, 143-145, 147, 152, 154, 156, 212, 213, 220, 234, 237
Key code	48, 60, 62, 65, 71, 77, 130, 179, 190, 191, 215, 228, 242, 246
Key depot	17, 63, 102, 103
Language	7, 20, 22, 50

LD number	60
LEGIC	53-55, 209
License	7, 21, 32-34, 129, 258
License file	21, 33
Load data	13, 161, 233, 234, 238, 249, 250, 252, 266
Local access code	78, 79, 142, 144, 146, 220
Location	7, 15, 24, 37-39, 43, 48, 49, 56, 58, 59, 63-65, 67, 71, 72, 76, 77, 80-85, 98, 101, 104, 105, 125, 127, 132, 145, 161, 166, 169-171, 174-177, 181, 183, 185-199, 204, 206, 215, 216, 235, 236, 238, 242, 243, 250, 252, 253, 262-264
Location manager	49, 56, 161, 166, 169, 171, 194, 195, 215, 242
Locking cylinder	17, 29, 59, 132, 134
Log off	40, 41, 57
Login	38, 41, 50, 56, 60, 61, 166-169, 171, 186, 187
Loop	8, 11, 17, 60, 62, 162, 212, 213, 225, 226, 234, 236, 237
Macro	52, 59-62, 72, 77
Microsoft	2, 7, 14, 28, 83, 132
mifare	53-55, 209, 215, 242, 253, 256
Minimum configuration	174
Modem	11, 17, 42, 78, 97, 141, 142, 145, 147, 149-156, 212, 213, 223
Modify door	107, 109, 112, 115, 122, 123
Module	16, 46, 58, 64, 69, 72, 75, 77, 79, 104, 113, 120, 124-128, 135, 136, 148, 162, 177-179, 263, 266
Module bus	16, 69, 77, 79, 120, 124, 126, 135, 162, 178, 263, 266
Multi eye	48, 72
Multi Eye AC	48, 72
Multi person AC	72, 211
MVA	8, 60
Network Administrator	83
Network Card	10
Network Installation	137
Number of doors	61, 129
ODBC	10, 25, 28, 36
Onboard	16, 46, 47, 105, 113, 125, 127, 129, 159, 177
Onboard hardware	46, 47, 159, 177
Open signal	57, 62, 63, 65, 130, 228, 237, 246, 251
Open time	57, 62, 63, 65, 130, 133, 228, 237, 246, 251
Operating system	10, 19, 39, 253
Operator concept	15
Palm	17, 19, 29, 131
Parameterization	37, 40, 41, 57, 59, 61, 68
Password	37-39, 56, 59-61, 95, 132, 166-169, 171, 175, 186, 221, 224, 226, 235, 236, 238, 245, 249-252, 258, 261, 265
PDA	17, 19, 29, 34, 65, 131-134
Permanent block	131, 211, 229, 247
Permanent release	58, 59, 131, 210, 211, 229, 233, 247, 249
Permanently active	75
Personnel manager	56, 167, 168
PIN	48, 60-62, 65, 71, 76, 77, 130, 131, 134, 175, 183, 190, 191, 214-216, 228, 229, 232, 241, 243, 246-248, 251, 263
Print	61, 161, 183, 204, 268
Printer	49, 50, 230
RDT	64, 141, 142, 144, 145, 147, 148, 156, 234
Reader	2, 16, 17, 19, 37, 46-48, 50, 53, 55, 56, 58, 62, 65, 72, 76, 77, 79, 80, 88, 98, 105, 106, 108, 110, 113, 117, 121, 125, 129-131, 136, 137, 148, 160, 162-164, 177-179, 183, 228, 246, 253-255, 263, 266
Reader settings	53, 55, 77, 80, 98, 148, 177, 183, 253
Relay	51, 57, 62, 64, 65, 74, 78, 103, 106, 108, 110, 114, 122, 136, 172, 179
Reporting	61
RS-232	17, 88
RS-485	16, 17, 97, 113, 120, 128, 135, 265
Runtime elimination	61
Server identification	37, 84, 132, 175

Shadow manager	<a href="#">15</a> , <a href="#">171</a>
Shadow operator	<a href="#">198</a>
Signal	<a href="#">57</a> , <a href="#">62</a> , <a href="#">63</a> , <a href="#">65</a> , <a href="#">70</a> , <a href="#">130</a> , <a href="#">228</a> , <a href="#">237</a> , <a href="#">246</a> , <a href="#">251</a>
Silent alarm	<a href="#">48</a> , <a href="#">62</a> , <a href="#">71</a>
Software	<a href="#">1</a> , <a href="#">2</a> , <a href="#">7</a> , <a href="#">10</a> , <a href="#">11</a> , <a href="#">15-17</a> , <a href="#">19</a> , <a href="#">35</a> , <a href="#">37-40</a> , <a href="#">56</a> , <a href="#">58</a> , <a href="#">59</a> , <a href="#">64</a> , <a href="#">66</a> , <a href="#">67</a> , <a href="#">69</a> , <a href="#">70</a> , <a href="#">72</a> , <a href="#">76</a> , <a href="#">79</a> , <a href="#">80</a> , <a href="#">84</a> , <a href="#">85</a> , <a href="#">131-134</a> , <a href="#">137</a> , <a href="#">139</a> , <a href="#">149</a> , <a href="#">153</a> , <a href="#">162</a> , <a href="#">168</a> , <a href="#">170</a> , <a href="#">180</a> , <a href="#">186</a> , <a href="#">199</a> , <a href="#">201</a> , <a href="#">204</a> , <a href="#">213</a> , <a href="#">214</a> , <a href="#">216</a> , <a href="#">236</a> , <a href="#">240</a> , <a href="#">241</a> , <a href="#">243</a> , <a href="#">245</a> , <a href="#">251</a> , <a href="#">256</a> , <a href="#">257</a> , <a href="#">262-264</a>
Status bar	<a href="#">43</a> , <a href="#">67</a>
Strike	<a href="#">62</a> , <a href="#">65</a> , <a href="#">78</a> , <a href="#">106</a> , <a href="#">108</a> , <a href="#">110</a> , <a href="#">114</a> , <a href="#">117-119</a> , <a href="#">122</a> , <a href="#">130</a> , <a href="#">136</a> , <a href="#">172</a> , <a href="#">179</a> , <a href="#">228</a> , <a href="#">246</a>
Superuser	<a href="#">15</a> , <a href="#">164</a> , <a href="#">166</a> , <a href="#">167</a> , <a href="#">170</a> , <a href="#">171</a> , <a href="#">235</a> , <a href="#">250</a>
Symbols	<a href="#">43</a>
Synchronization	<a href="#">134</a> , <a href="#">137</a> , <a href="#">263</a>
System number	<a href="#">53</a> , <a href="#">55</a> , <a href="#">183</a>
Tableau	<a href="#">49</a>
Tamper	<a href="#">79</a> , <a href="#">130</a> , <a href="#">210</a>
TBS	<a href="#">257</a> , <a href="#">259-266</a>
TCP/IP	<a href="#">10</a> , <a href="#">18</a> , <a href="#">62</a> , <a href="#">139</a> , <a href="#">140</a> , <a href="#">217</a> , <a href="#">234</a> , <a href="#">236</a> , <a href="#">239</a> , <a href="#">244</a> , <a href="#">250</a> , <a href="#">251</a> , <a href="#">262</a>
Telnet Autoconfiguration	<a href="#">164</a>
Time recording	<a href="#">8</a> , <a href="#">16</a> , <a href="#">17</a> , <a href="#">49</a> , <a href="#">64</a> , <a href="#">72</a> , <a href="#">86</a> , <a href="#">101</a>
Timeout	<a href="#">56</a> , <a href="#">79</a> , <a href="#">136</a> , <a href="#">145</a>
Timer	<a href="#">50</a>
Troubleshooting	<a href="#">183</a>
TRS	<a href="#">17</a> , <a href="#">86</a> , <a href="#">164</a>
Turnstile	<a href="#">51</a>
Type	<a href="#">17</a> , <a href="#">21</a> , <a href="#">49</a> , <a href="#">53</a> , <a href="#">58</a> , <a href="#">59</a> , <a href="#">63</a> , <a href="#">69</a> , <a href="#">74</a> , <a href="#">76-78</a> , <a href="#">80</a> , <a href="#">87</a> , <a href="#">98</a> , <a href="#">104</a> , <a href="#">131</a> , <a href="#">134</a> , <a href="#">136</a> , <a href="#">149</a> , <a href="#">151</a> , <a href="#">154</a> , <a href="#">161</a> , <a href="#">162</a> , <a href="#">171</a> , <a href="#">177</a> , <a href="#">189</a> , <a href="#">206</a> , <a href="#">207</a> , <a href="#">210</a> , <a href="#">215</a> , <a href="#">217</a> , <a href="#">220</a> , <a href="#">223</a> , <a href="#">225</a> , <a href="#">229</a> , <a href="#">230</a> , <a href="#">237</a> , <a href="#">242</a> , <a href="#">247</a> , <a href="#">251</a> , <a href="#">253</a> , <a href="#">263</a> , <a href="#">266</a>
Unreferenced main data	<a href="#">49</a>
Unsuccessful attempts	<a href="#">38</a>
Unsuccessful login	<a href="#">38</a>
USB	<a href="#">18</a> , <a href="#">19</a> , <a href="#">55</a> , <a href="#">88</a> , <a href="#">131-134</a> , <a href="#">253</a>
User defined fields	<a href="#">39</a> , <a href="#">59</a>
User interface	<a href="#">7</a> , <a href="#">40</a> , <a href="#">204</a>
User name	<a href="#">37</a> , <a href="#">38</a> , <a href="#">60</a> , <a href="#">175</a> , <a href="#">186</a> , <a href="#">245</a> , <a href="#">249</a> , <a href="#">265</a>
VdS	<a href="#">63</a> , <a href="#">215</a> , <a href="#">236</a> , <a href="#">242</a>
VPS	<a href="#">35</a> , <a href="#">204</a> , <a href="#">205</a>
Week plans	<a href="#">50</a>
WINFEM	<a href="#">11</a> , <a href="#">136</a> , <a href="#">213-215</a> , <a href="#">218</a> , <a href="#">225</a> , <a href="#">232-234</a> , <a href="#">236</a> , <a href="#">238</a>
WINMAG	<a href="#">49</a> , <a href="#">59</a> , <a href="#">60</a> , <a href="#">87</a> , <a href="#">102</a> , <a href="#">161</a> , <a href="#">218</a>
Workstation	<a href="#">14</a> , <a href="#">17</a> , <a href="#">18</a> , <a href="#">26</a> , <a href="#">32</a> , <a href="#">42</a> , <a href="#">56</a> , <a href="#">57</a> , <a href="#">66</a> , <a href="#">83-91</a> , <a href="#">93</a> , <a href="#">95</a> , <a href="#">96</a> , <a href="#">106</a> , <a href="#">108</a> , <a href="#">111</a> , <a href="#">114</a> , <a href="#">129</a> , <a href="#">131</a> , <a href="#">132</a> , <a href="#">143</a> , <a href="#">178</a> , <a href="#">199</a> , <a href="#">201</a> , <a href="#">202</a> , <a href="#">204</a> , <a href="#">216</a> , <a href="#">217</a> , <a href="#">219</a> , <a href="#">220</a> , <a href="#">222-227</a> , <a href="#">243-245</a> , <a href="#">253</a>
XS-Manager	<a href="#">19</a> , <a href="#">29</a> , <a href="#">32</a> , <a href="#">35</a> , <a href="#">36</a> , <a href="#">131</a> , <a href="#">133</a> , <a href="#">134</a> , <a href="#">136</a>







P32205-26-0G020

**Honeywell Security and Fire Solutions**

Novar GmbH

Johannes-Mauthe-Straße 14

D-72458 Albstadt

[www.honeywell.com/security/de](http://www.honeywell.com/security/de)

P32205-26-0G0-20  
2017-05-22

© 2017 Novar GmbH

**Honeywell**