



# Communication Server Installation Instructions

II\_DP\_Server\_En\_2311



- ▶ Communication Server
- ▶ DP6000-IP Interface
- ▶ Software and Licenses
- ▶ Options
- ▶ Application notes
- ▶ Maintenance information

Powered by:  
Next Generation  
Technology





## Table of contents

1.1	Function.....	8
1.2	Digital version.....	8
1.3	Precautions and notes.....	8
1.3.1	Signs.....	8
1.4	Examples.....	8
1.5	Disclaimer.....	8
1.5.1	Illustrations.....	8
2	Installation checklist.....	9
3	Introduction.....	10
3.1	Basic Functions.....	10
3.2	Basic System set-up.....	10
3.2.1	Other Highlights.....	10
4	Commercial Items.....	11
4.1	Special Packages.....	11
4.2	Ordering.....	11
4.2.1	To be organized locally.....	11
4.3	Functional Description.....	12
4.3.1	Communication Server; LBB8000/00.....	12
4.3.2	Image Basic software Package; LBB LBB8000/01.....	12
4.3.3	DP6000-IP interface; LBB8001/00.....	12
4.3.4	Input contact module; LBB5901/00.....	12
4.3.5	Output contact module; LBB5902/00.....	12
4.3.6	ESPA 4.4.4. interface module; LBB5903/00.....	12
4.3.7	RS485 Interface module LBB5904/00.....	13
4.3.8	Cable set (set of 2); LBB 8003/00.....	13
4.4	Licenses.....	13
4.4.1	Activation Logging; LBB 8600/00.....	13
4.4.2	Activation Personal Security; LBB 8601/00.....	13
4.4.3	Activation Multi Users; LBB 8602/00.....	13
4.4.4	Activation Multi Site; LBB 8603/00.....	13
4.4.5	Activation ESPA; LBB 8604/00.....	13
4.4.6	Activation I/O contacts; LBB 8605/00.....	14
4.4.7	Activation 3 <sup>rd</sup> Party Connection; LBB8608/00.....	14
4.4.8	Maintenance agreement; LBB 8609/00.....	14
4.4.9	Remote Support Device.....	14
4.4.10	Subscription Fee.....	14
4.4.11	Ordering additional licenses afterwards.....	14
4.5	Server Packages explained.....	14
4.5.1	Basic Messaging Server.....	14
4.5.2	Basic Personal Security Server.....	14
4.5.3	Extended Communication server.....	14
5	The IP Network.....	15
5.1	Minimum IP network requirements.....	15
5.1.1	Communication Server.....	15
5.1.2	Specification Communication server PC.....	15
5.2	DP6000-IP Interface.....	15
5.3	Web browser and settings.....	15
5.3.1	Automatic Windows Updates.....	16
5.3.2	Auto fill in.....	16
5.3.3	Audio settings.....	16
5.4	Reserved IP addresses.....	16
5.4.1	Port settings.....	16
5.5	IP-Network topology.....	17
5.5.1	Virtual IT structure.....	17
5.5.2	Management gateway (IP address).....	17
5.5.3	Enable Ping Replies.....	18
5.6	Network settings.....	18
5.6.1	Network 0 settings.....	18
5.6.2	Network 1 settings.....	19
5.7	Network test-tools (build in).....	19
5.7.1	Ifconfig.....	19
5.7.2	Ping.....	19





- 5.7.3 Traceroute ..... 19
- 5.8 Alternative Network test-tools ..... 20
- 6 Getting started ..... 21
  - 6.1 Preparations ..... 21
  - 6.2 Interconnections and operation ..... 21
    - 6.2.1 Loudspeaker on client PC ..... 21
    - 6.2.2 Audio settings in Web browser ..... 21
  - 6.3 IP interfaces ..... 21
  - 6.4 Switching On the Communication Server ..... 21
- 7 DP6000-IP Interface Hardware ..... 22
  - 7.1 Introduction ..... 22
  - 7.2 Hardware- and user interfaces ..... 22
    - 7.2.1 Paging bus interface ..... 22
  - 7.3 Power Supply ..... 23
  - 7.4 Pushbuttons ..... 23
  - 7.5 Display information ..... 23
  - 7.6 Menu ..... 23
  - 7.7 MAC address ..... 23
  - 7.8 Diagnose menu ..... 23
  - 7.9 Setup menu ..... 23
    - 7.9.1 IP settings ..... 23
      - 7.9.2 Set the IP address ..... 24
      - 7.9.3 Set the Gateway ..... 24
      - 7.9.4 Set the subnet mask ..... 24
      - 7.9.5 Set the Port address ..... 24
      - 7.9.6 Set IP settings to default ..... 25
    - 7.9.2 Set the IP address ..... 24
    - 7.9.3 Set the Gateway ..... 24
    - 7.9.4 Set the subnet mask ..... 24
    - 7.9.5 Set the Port address ..... 24
    - 7.9.6 Set IP settings to default ..... 25
  - 7.10 Testfunctions menu ..... 25
  - 7.11 Software versions menu ..... 25
  - 7.12 Dimensions ..... 25
    - 7.12.1 Mechanical ..... 25
    - 7.12.2 Drilling pattern ..... 25
  - 7.13 Install the ESPA interface module ..... 26
    - 7.13.1 The RS232 cable ..... 26
  - 7.14 Prepare the LBB5843/01 MPC heads ..... 26
    - 7.14.1 Set the address of the MPC ..... 26
    - 7.14.2 Install the RS485 module ..... 26
    - 7.14.3 RS485 Cable ..... 26
    - 7.14.4 Configure the RS485 interface module ..... 27
    - 7.14.5 Monitoring RS485 connection ..... 27
  - 7.15 Installing Internal I/O contact modules ..... 27
    - 7.15.1 Internal Output contact modules ..... 27
    - 7.15.2 Internal Input contact module ..... 28
    - 7.15.3 Cable set ..... 28
    - 7.15.4 Resistor network ..... 28
    - 7.15.5 Set address of the input contact module ..... 29
  - 7.16 LED indications ..... 29
    - 7.16.1 LED indications; IP interface module ..... 29
    - 7.16.2 LED indications; Input Contact module ..... 29
    - 7.16.3 LED indications; Output contact module ..... 29
    - 7.16.4 LED indications; ESPA module ..... 30
    - 7.16.5 LED indications; RS485 module ..... 30
    - 7.16.6 LED indications DP6000-IP Interface ..... 30
  - 7.17 Firmware version ..... 31
  - 7.18 Replace a DP6000-IP Interface ..... 31
    - 7.18.1 License Check ..... 31
    - 7.18.2 Replacement options ..... 31
    - 7.18.3 Exchange the TCP-IP module ..... 32
    - 7.18.4 Apply for new licenses ..... 32
    - 7.18.5 Replace a defect DP6000-IP Interface ..... 32
    - 7.18.6 Repair Costs ..... 32
- 8 Programming ..... 33
  - 8.1 Set up a Client IP-connection ..... 33
  - 8.2 The start screen ..... 33
  - 8.3 Set header colour ..... 33
  - 8.4 Set Language ..... 33



8.4.1	Server language .....	33
8.4.2	User language .....	33
8.5	Log in.....	34
8.6	Main screen.....	34
8.6.1	Maximum logged on users .....	34
8.6.2	Auto Log of.....	34
8.7	Log out .....	34
9	System Licenses.....	35
9.1.1	Update the License file .....	35
9.1.2	Check present Licenses .....	35
10	Working mode.....	36
10.1	Manned operation mode.....	36
10.2	Unmanned operation mode .....	36
10.3	Remote Reset.....	36
11	System Configuration.....	37
11.1	Define a building.....	37
11.1.1	Add a site/building .....	37
11.1.2	Add a drawing to the building .....	37
11.2	Location detection .....	38
11.2.1	Location monitoring option .....	38
11.3	Overview programmed locations .....	38
11.3.1	Sorted overview of location beacons .....	38
11.3.2	View programmed Location beacons .....	38
11.3.3	Edit programmed Location beacons .....	38
11.3.4	Guidelines to program Location data.....	38
11.3.5	Add Location Beacon(s) .....	39
11.3.6	Export location data.....	39
11.3.7	Delete location beacon(s).....	40
11.3.8	Representation of location graphics .....	40
11.3.9	Drawing quality:.....	41
11.3.10	Location monitoring option .....	41
11.3.11	Guard tour option.....	41
11.4	Define peripherals .....	42
11.4.1	Add a Peripheral.....	42
11.4.2	To view peripheral settings .....	42
11.4.3	Configure Transmitter DP6000 TX .....	42
11.4.4	Configure DP6000 RX.....	43
11.4.5	Configure a DP6000-IP Interface.....	43
11.5	Monitoring the DP6000-IP Interface .....	45
11.5.1	Line occupation error.....	45
11.5.2	Lost IP connection .....	45
11.5.3	Sent an automatic message when IP connection is lost.....	45
11.6	Configure a Communication Server.....	46
11.6.1	Configure the main server .....	46
11.6.2	Database errors from Server .....	46
11.6.3	IP connection lost from Server .....	46
11.7	Notifications.....	47
11.8	Assign mobiles to the system .....	48
11.9	Add an individual mobile.....	48
11.9.1	Absent handling * .....	48
11.9.2	Indoor location detection * .....	49
11.9.3	Switched off * .....	49
11.9.4	Out Rack test * .....	49
11.9.5	Low battery Indication * .....	49
11.9.6	Automatic Scanning * .....	50
11.9.7	Sign of life (manual reply from mobile) * .....	50
11.9.8	Sign of life (periodical call from PS-Micro mobile) * .....	50
11.9.9	Link mobile to a Building/site * .....	51
11.10	Link a mobile to Peripherals (DP6000-IP Interfaces) * .....	51
11.10.1	Link mobile to Main Peripheral(s) * .....	51
11.10.2	Link mobile to Back-up Peripheral * .....	51
11.10.3	Scan Peripheral * .....	51
11.10.4	Import multiple mobiles * .....	52
11.10.5	Export mobile data.....	52
11.10.6	Delete mobiles/devices.....	52





11.11	Device screen content (Mobiles)	53
11.11.1	Visible data of a device/mobile	53
11.11.2	Sorted status overview	53
11.11.3	Operation via the status indicator	53
11.11.4	Programmable info in the status indicator	53
11.11.5	Set Scanning ON or Off	54
11.12	Status screen content	55
11.13	Groups of devices (serial call)	56
11.13.1	Create a Group of pagers (serial call)	56
11.13.2	Create a Group Call (Group address)	56
12	Alarm handling settings	57
12.1	Alarm definitions	57
12.1.1	Default technical alarm	57
12.1.2	Default PS alarm	57
12.1.3	Default Other alarm	57
12.1.4	Specified alarm	57
12.2	Alarm classes	58
12.2.1	Alarm types	58
12.2.2	Edit an alarm type	58
12.2.3	Alarm sources	59
12.2.4	Number of visible alarm lines	59
12.3	Define Default alarms	60
12.3.1	System settings for alarm handling	61
12.4	Define Specified Alarms	62
12.4.1	Create a specified alarm	62
12.4.2	Other (system) settings for alarm handling	64
12.5	Test the alarm function	65
12.5.1	Fault finding	65
12.5.2	Alarm screen layout	65
12.5.3	The alarm sound	65
12.5.4	General System settings for alarm handling	65
12.5.5	View Alarm History	65
13	Create users and roles	66
13.1	Role of users	66
13.1.1	Examples of roles and permissions	66
13.1.2	Create roles	67
13.2	Add a user	68
13.2.1	Set user authorizations	68
13.3	Forgotten password	69
13.3.1	System settings and alarm handling	69
14	System settings	70
14.1	Quick search	70
14.2	Download the system settings	70
14.3	Overview System settings	70
14.4	General system settings	72
14.5	System settings related to automatic scanning	72
14.6	System settings related to Alarm handling	73
15	Logging of calls	76
15.1	Logging screen	76
15.2	Real-time call handling	76
15.3	Alarm history	77
15.3.1	To access 'own alarm history'	77
15.3.2	To access 'full alarm history'	77
16	Archives	78
16.1	Accessibility of Archives	78
16.2	Obtain Alarm reports	78
16.2.1	Download alarm history data	79
16.3	Outgoing calls	80
16.3.1	Meaning of the data (Fields) that can be exported; Outgoing calls	80
16.4	Technical Logging	81
16.4.1	Meaning of the data that can be exported; Technical logging	82
16.5	Guard tours archive	82
16.6	Convert CSV file to Excel file	83
17	Application notes	84
17.1	Out Of Range (OOR) call	84





17.2	Special Calls.....	84
17.2.1	Edit a Special call .....	84
17.2.2	Detection of call parameters .....	84
17.2.3	Action for Special calls .....	85
17.3	Pre-defined numeric code .....	86
17.4	Pre-defined Messages.....	86
17.5	Manual Call Button/Speed Dial Buttons.....	86
17.5.1	Manual Call Options .....	86
17.5.2	Change the color for the 'Manual call' button .....	86
17.5.3	Sent Manual calls with a fixed bleep code .....	86
17.5.4	Split long messages to 24 char/call .....	87
17.6	Speed dial buttons/Fast dial buttons.....	87
17.6.1	Editable Content for Speed Dial Calls .....	88
17.7	Predefined IP-DP6000 calls .....	88
17.7.1	Program a predefined IP-DP6000 call.....	88
17.7.2	Add a new Predefined IP-DP6000 call .....	89
18	Program I/O contacts.....	90
18.1	Programming Output contacts.....	90
18.2	Layout status indicator for output contacts .....	91
18.2.1	Change the status of the output contact manually.....	91
18.3	Programming Input Contacts.....	92
18.3.1	Configure a Guarded internal input contact.....	95
18.3.2	Edit a contact.....	95
18.3.3	Layout status indicator for Input contacts .....	95
18.4	ESPA Ports .....	96
18.5	ESPA configuration .....	96
18.5.1	Program an ESPA input port .....	96
18.5.2	Message options; Fixed digits .....	97
18.5.3	ESPA Port monitoring.....	97
18.5.4	Program an ESPA-out port.....	98
18.6	Programming Mobiles.....	99
18.7	Preparation.....	99
18.7.1	Reserved addresses.....	99
18.7.2	Programmable items .....	99
18.7.3	Default settings/Factory settings.....	99
18.7.4	Select the data to be programmed .....	99
18.7.5	The extended method.....	100
18.8	Transmitter monitoring via the Server.....	101
18.8.1	Preparation .....	101
18.8.2	Error indications.....	101
18.8.3	Automatic TX reset call.....	101
18.8.4	Settings TMM type WSP_D_40971 .....	101
18.8.5	Settings TMM type LBB5905.....	102
18.9	CRX monitoring via the Server .....	102
18.9.1	Preparation:.....	102
18.9.2	Information in the numeric code of the status call .....	103
18.9.3	Status indicator for CRX .....	103
18.10	Guard tours .....	104
18.10.1	Create a guard tour .....	104
18.10.2	Start a guard-tour .....	104
18.10.3	Guard tour registration.....	105
18.10.4	Unsuccessful Guard tour .....	105
18.10.5	Guard tour alarm .....	105
18.11	Location Monitoring.....	105
18.11.1	Location beacon not seen for a too long time .....	106
18.11.2	Location beacon reports code F7 .....	106
18.12	System examples .....	107
18.12.1	Basic system .....	107
18.12.2	Multi-client system .....	107
18.12.3	Multi-site system 1 .....	107
18.12.4	Multi-site system 2.....	107
18.12.5	3 <sup>rd</sup> party connection/BMS .....	107
18.12.6	Server as Master/Slave .....	107
19	Technical Alarms .....	108
19.1	Technical notification .....	108





19.2	Technical calls .....	108
19.3	Status screen .....	108
20	Maintenance .....	109
20.1	Introduction.....	109
20.2	Firmware and software versions.....	109
20.3	Network testing.....	109
20.4	Remote Maintenance .....	109
20.5	Set time and date (in the Server PC).....	109
20.5.1	Set time and date (ESXi) .....	109
20.6	Server Status screen and Server backup .....	111
20.6.1	Server status .....	111
20.6.2	Restart the Server (Software reset) .....	111
20.6.3	Incoming calls/line monitoring .....	111
20.6.4	Server logs .....	112
20.7	Manage the database (Communication server).....	112
20.7.1	Back-up database.....	112
20.7.2	Restore database .....	113
20.7.3	Back up of DP6000-IP Interfaces. ....	113
20.8	Modeword explanation .....	114
20.9	Update firmware DP6000-IP Interface.....	116
20.9.1	Preparation .....	116
20.9.2	Upgrade instructions.....	116
21	Trouble shooting .....	118
21.1	Remember in case of issues: .....	118
21.2	Technical alarms guidelines .....	118
21.2.1	Technical alarms and possible remedies.....	118





## About this manual

### 1.1 Function

These Installation Instructions gives the install engineers the necessary information to install and configure the Communication Server and DP6000-IP interface unit to be used in a DP6000/PS6000 concept as defined for the Philips/Bosch/Atus paging and Personal Security product range.

### 1.2 Digital version

The Installation manual is also available as a digital file (Adobe Portable Document File, PDF). When the PDF refers to a location that contains more data, you can click the text to go there.

### 1.3 Precautions and notes

The Installation manual uses 3 levels of precaution. The precaution shows the result of not obeying the instructions. These are the types:

1. Note A note gives more data.
2. Caution If you do not obey the caution, you can cause damage to the equipment.
3. Warning If you do not obey the warning, you can cause personal injury or severe damage to the equipment.

#### 1.3.1 Signs

The Installation and User Instructions shows each caution, warning and danger with a sign. The sign shows the result of not obeying the instructions.



Warning: General sign for cautions warnings and dangers.



Caution: Risk of electrical shock.



Note: The general sign for a note.

### 1.4 Examples

The manual contains numerous examples, for instance in the form of screen shots. Please note that the examples may differ more or less from you situation, depending on version differences, settings, configuration details, resolution, etc.



Note: The screenshots shown in this manual may appear different on your PC, depending on windows version, configuration, etc. etc. In some cases the steps may even be slightly different than described. It might also be possible that there are alternative ways that are not described in this manual.

### 1.5 Disclaimer

International Pager Services B.V. reserves the right to change data and/or specification of any equipment or software mentioned in this publication without prior notice. Although every effort is made to ensure that the information in this publication is accurate and correct, International Pager Services B.V. is not responsible for damage arising from its misuse.

This publication contains proprietary information, which is protected by copyright. All rights are reserved. No part of this document may be photocopied, reproduced or translated to another language without the prior written consent of International Pager Services B.V.

#### 1.5.1 Illustrations

The illustrations in this manual are indicative only and may differ depending on:

- ▶ The operating system.
- ▶ The version of the application software.
- ▶ The activated language on the PC.





## 2 Installation checklist

The checklist helps you to be sure that no steps in a basic installation procedure are forgotten.

Note that the sequence in steps are important to carry out e.g. first check steps 1 to 3 before step 4 is executed.

Configuration steps to configure a system: (if items applicable).

Step nr	Action	Remark
<input type="checkbox"/>	1 <ul style="list-style-type: none"> <li>Prepare the DP6000-IP Interface</li> </ul>	Add hardware, program IP settings
<input type="checkbox"/>	2 <ul style="list-style-type: none"> <li>Select the language</li> </ul>	For user and in System settings
<input type="checkbox"/>	3 <ul style="list-style-type: none"> <li>Logon as Super administrator</li> </ul>	To make sure you have enough rights
<input type="checkbox"/>	4 <ul style="list-style-type: none"> <li>Check Licenses</li> </ul>	Check if the correct applications are activated
<input type="checkbox"/>	5 <ul style="list-style-type: none"> <li>Check/Set the Network settings (Server)</li> </ul>	For user and in System settings
<input type="checkbox"/>	6 <ul style="list-style-type: none"> <li>Create Buildings/sites</li> </ul>	For each DP6000-IP interface one building required.
<input type="checkbox"/>	7 <ul style="list-style-type: none"> <li>Configure Location data</li> </ul>	One by one or import from an excel list. If desired also guard tour(s) and/or location monitoring can be configured
<input type="checkbox"/>	8 <ul style="list-style-type: none"> <li>Configure DP6000-IP Interface(s)</li> </ul>	The main unit is linked to system licences
<input type="checkbox"/>	9 <ul style="list-style-type: none"> <li>Add the devices</li> </ul>	One by one or import from an excel list
<input type="checkbox"/>	10 <ul style="list-style-type: none"> <li>Create Groups</li> </ul>	Optionally
<input type="checkbox"/>	11 <ul style="list-style-type: none"> <li>Create Predefined system calls</li> </ul>	Needed for system guarding + Internal I/O contacts
<input type="checkbox"/>	12 <ul style="list-style-type: none"> <li>Program the I/O contacts</li> <li>First create output- then input- contacts.</li> </ul>	There might be internal and/or external I/O contacts
<input type="checkbox"/>	13 <ul style="list-style-type: none"> <li>Set the alarm definitions/alarm types</li> </ul>	In 'Alarm definitions' create always a DEFAULT Personal Security and a DEFAULT Technical alarm and if desired create 'Specified Alarms'. Set the BAR- colour of an alarm in 'Alarm types'.
<input type="checkbox"/>	14 <ul style="list-style-type: none"> <li>Set the authorisations for the several 'Roles'</li> </ul>	In 'Roles' the authorisations are set.
<input type="checkbox"/>	15 <ul style="list-style-type: none"> <li>Create Roles, users and operators</li> </ul>	Select appropriate role per user type.
<input type="checkbox"/>	16 <ul style="list-style-type: none"> <li>Define pre-programmed alpha numeric messages</li> </ul>	Optionally
<input type="checkbox"/>	17 <ul style="list-style-type: none"> <li>Define pre-programmed numeric messages</li> </ul>	Optionally
<input type="checkbox"/>	18 <ul style="list-style-type: none"> <li>Define speed dial buttons</li> </ul>	For manual button fixed digits can be set
<input type="checkbox"/>	19 <ul style="list-style-type: none"> <li>If relevant add peripherals (e.g. TX, RX etc.)</li> </ul>	Optionally; First check the peripheral type. If desired activate guarding.
<input type="checkbox"/>	20 <ul style="list-style-type: none"> <li>Check the system settings</li> </ul>	Settings are system wide applicable.
<input type="checkbox"/>	21 <ul style="list-style-type: none"> <li>Configure the RS232 (ESPA) Interface(s)</li> </ul>	Optionally Port 3 can be set as ESPA-out.
<input type="checkbox"/>	22 <ul style="list-style-type: none"> <li>Configure the RS485 Interface(s)</li> </ul>	Only Applicable if the LBB5843/01 is used.
<input type="checkbox"/>	23 <ul style="list-style-type: none"> <li>When finished create a back-up of all settings</li> </ul>	Logging and archives are not back-upped

In the manual and in the chapter ["Application notes"](#) examples for a numerous of solutions are explained.



### 3 Introduction

The Communication Server is the heart of the system, this is a PC with installed application software. In combination with the DP6000-IP interface both replaces the former Alpha-desk and Atus Commander. Several new functionalities, graphical user interface and new application possibilities are implemented to meet the today's functional demands. Thanks to the new system architecture it is made easier to create redundancy in the system.

The Communication Server software is a complete, new designed system integration platform and if connected to a DP6000-IP Interface all necessary Paging and Personal Security functions can be created. The Communication Server together with the DP6000-IP interface unit is fully compatible with the DP6000/PS6000 concept known for its high reliability.

This manual covers applications where the Communication Server works with one or more DP6000 interfaces, where each DP6000-IP Interface is to be considered as an individual (local or remote) DP6000 system.

#### 3.1 Basic Functions

- ▶ Personal Security applications.
- ▶ Logging of data.
- ▶ Signalisation with I/O contacts. Input- output contact coupling.
- ▶ ESPA 4.4.4. coupling
- ▶ Suitable for system according to the Dutch NEN 2575 normalisation.
- ▶ Critical messaging, such as evacuation, medical assistance etc.
- ▶ Applicable to function in both manned- and unmanned operation.
- ▶ Multiple operators can have (simultaneous) access via a web browser.
- ▶ Multisite options to route communication from multiple sites to a central server/operator.
- ▶ Very flexible system architecture, therefore able to support redundancy- and virtualisation- requirements.
- ▶ Remote Maintenance possible through a remote web-based connection.

#### 3.2 Basic System set-up


For a basic system the Communication Server and at least one DP6000-IP Interface is needed.

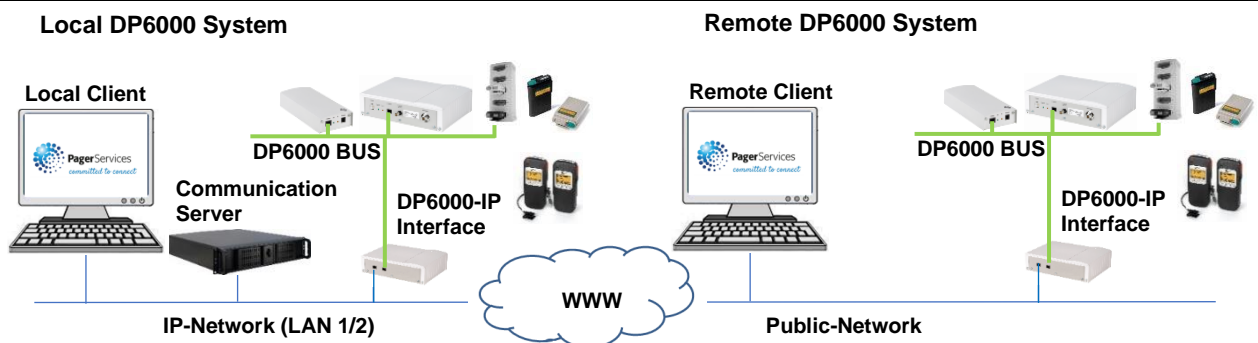
Optionally several sub units are available to expand the functions (ESPA, I/O Contacts).

- ▶ **DP6000-IP Interface:**  
The DP6000-IP Interface is an active unit which contains embedded firmware and hardware to send and receive calls from/to the DP6000 product-range, like e.g. system transmitters, system receivers, charge racks. Depending on the chosen options/licenses this unit is able to handle basic functions like an ESPA interface, output contacts and (guarded) input contacts.
- ▶ **Communication Server:**  
The DP6000-IP Interface is controlled by application software which is installed on the Communication Server PC. All application functionality is determined by the (LINUX based) application software, which is pre-installed at this server. Only the customer specific settings and instructions needs to be installed locally.

##### 3.2.1 Other Highlights

- ▶ The application software on the Communication Server is able to handle only one or multiple DP6000-IP Interfaces, e.g. to control a number of (remote) DP6000 systems, located at different sites, or to install an extra redundant DP6000-IP Interface unit locally.
- ▶ Multiple clients can be logged on to handle events with multiple (remote) users.
- ▶ In order to operate conform the Dutch NEN-2575 market, several basic functions are still operational when the connection between the DP6000-IP Interface and Communication Server went lost.

 Note: Log on for operators and/or installers is made through a web browser and is therefore possible with an external PC, Laptop, Tablet and/or Smartphone.



Configuration example: System architecture for Multi-site operation with one Communication Server with a local and a remote DP6000-IP Interface, using a local and a remote client. Check chapter "[Application notes](#)" for more examples.



## 4 Commercial Items

Hardware	12NC	Type nr	Remark
Communication Server PC	8900 800 00001	LBB 8000/00	This server PC includes the basic software package
DP6000-IP Interface	8900 800 10001	LBB 8001/00	For each DP6000 (sub) system 1 unit is needed.
Input Contact Module	8900 590 10001	LBB 5901/00	One module has 4 input contacts.
Output Contact Module	8900 590 20001	LBB 5902/00	One module has 2 output contacts.
ESPA 4.4.4. Interface Module	8900 590 30001	LBB 5903/00	Max. 3 ESPA ports per DP6000-IP interface.
RS485 Interface Module	8900 590 40001	LBB 5904/00	Used for external I/O couplers e.g. LBB5843/01
Cable set (set of 2)	8900 800 30001	LBB 8003/00	Cable set to for internal input contacts.
Software and Licenses	12NC	Type nr	Remark
Image Basic Software Package	8900 800 00101	LBB 8000/01	For upgrades or to be installed on 3 <sup>rd</sup> party PC
Activation Logging	8900 860 00001	LBB 8600/00	See note 1 below.
Activation Personal Security	8900 860 10001	LBB 8601/00	See note 1 below.
Activation Multi Users	8900 860 20001	LBB 8602/00	By default 1 Client can be logged in.
Activation Multi Site	8900 860 30001	LBB 8603/00	See note 1 and 2 below.
Activation ESPA	8900 860 40001	LBB 8604/00	One License per active ESPA port is needed.
Activation I/O contacts	8900 860 50001	LBB 8605/00	I/O Licences works system wide
Activation 3rd Party Connection	8900 860 80001	LBB 8608/00	Needed if connection with e.g. a BMS is needed.
Services	12NC	Type nr	Remark
Maintenance Agreement	8900 860 90001	LBB 8609/00	Inform with your commercial contact for details.
Remote Support Device (RSD)	8900 860 91001	LBB 8609/10	The RSD is delivered including a SIM card.
Subscription fee for RSD	8900 860 92001	LBB 8609/20	Relevant for RSD

### 4.1 Special Packages

Next to the above mentioned items several server packages are made available. Each server package is defined depending on its basic functionality. See chapter [“Server Packages explained”](#) for more details.

Predefined Packages	12NC	Type nr	Remark
Basic Message Server	8900 800 01001	LBB 8000/10	Message handling, ESPA, I/O, Logging
Basic Personal Security Server	8900 800 02001	LBB 8000/20	LBB8000/10 + Personal Security, Multi users
Extended Communication Server	8900 800 03001	LBB 8000/30	LBB8000/20 + MPC, Multisite, 3 <sup>rd</sup> Party

	<p>Note 1: - Licenses are related to each individual system and cannot be transferred from one to the other. - Licences works system wide.</p>
--	--

	<p>Note 2:</p> <ul style="list-style-type: none"> <li>• Licences are only valid in combination <u>with one specific DP6000-IP Interface</u>.</li> <li>• In case of a Multisite system (with more than one DP6000-IP-Interface), only one DP6000-IP Interface is handled as the ‘main-unit’ on which all system licences are linked.</li> <li>• If a DP6000-IP Interface, on which licences are linked, is replaced, the validity of the licence files must be taken in account. Refer to: <a href="#">“Replace a DP6000-IP Interface”</a> how to handle.</li> </ul>
--	---

### 4.2 Ordering

All items as listed above are to be ordered through our website, also actual prices are indicated here. In case of questions about availability or if you need help to assemble the needed configuration, please contact [orders@pagerservices.nl](mailto:orders@pagerservices.nl)

#### 4.2.1 To be organized locally

- ▶ IP network, switches, routers etc.
- ▶ Computer(s) to be connected as client.
- ▶ Key-board and mouse.
- ▶ Loudspeaker to hear the alarm signals.



### 4.3 Functional Description

#### 4.3.1 Communication Server; LBB8000/00

The Communication Server is a dedicated computer, all functions are driven by the already installed application software at this computer. The Communication Server communicates with the DP6000-IP interface(s) through a guarded IP-interconnection(s). Optionally a WARNING signal (technical alarm) can be generated in case the IP connection(s) is/are lost. Through a web browser it is possible to log on as user, this makes it possible to login by using a PC, laptop, tablet and even using a smartphone. When logged in, several authorization levels prevent unwanted use. (Operator, Manager Administrator).

#### 4.3.2 Image Basic software Package; LBB LBB8000/01

The Image Basic Software Package can be used for:

- ▶ A customer who needs to upgrade the software with a newer version.
- ▶ For systems where the basic software is installed on a (virtual) 3rd party server PC.
- ▶ In case the image of the basic Software is ordered:
  - No Communication Server PC shall be delivered from IPS.
  - The Application software will be delivered as Image to be installed on (your) a 3<sup>rd</sup> party (virtual) server.

#### 4.3.3 DP6000-IP interface; LBB8001/00

To communicate with the DP6000 system, a DP6000-IP Interface is required. The DP6000-IP interface controls the paging- and talk-back lines of the DP6000 bus. For further processing all received calls and calls to be transmitted, are communicated between the Communication Server and DP6000-IP interface. For reliability purposes the DP6000-IP Interface is equipped to send a warning call in case the IP-connection with the Communication Server is interrupted. Multiple DP6000-IP Interfaces can be used where one Communication Server controls multiple DP6000-IP Interfaces. (Multi-site configuration).

**Note:**

- The Communication Server can control multiple DP6000-IP Interfaces.
- In case the IP connection, between the Communication Server and a DP6000-IP Interface is lost, automatically a predefined call to inform e.g. the engineering group can be sent.
- DP6000-IP Interfaces are delivered in a similar housing like shown at the right →:



#### 4.3.4 Input contact module; LBB5901/00

- ▶ The DP6000-IP Interface can handle a maximum of 3 input contact modules; (internal input contacts).
- ▶ With this maximum, also the total number of present output contact modules must be taken in account: Per DP6000-IP interface, the total sum of both is limited to 4.
- ▶ Each Input contact module has 4 input contacts.
- ▶ The internal input contacts are analogue inputs, and needs therefore a resistor network.
- ▶ Furthermore these contacts can be set as 'guarded input contacts'; to detect interruptions- and short circuited wires that are connected to an input contact; Guarded input contacts are required to meet the Dutch NEN 2575 standard, where it is required to detect if the wires connected with the input contact are interrupted- or short circuited.



Note: There is also an option to communicate with 'external' I/O contacts, e.g. via an RS485 interface using one or more MPC (LBB5843/01) contact couplers  
When using an 'external' I/O coupler; LBB5843/01, the LBB5904/00 RS485 Interface unit is needed.

#### 4.3.5 Output contact module; LBB5902/00

- ▶ One DP6000-IP Interface can handle a maximum of 1 extra output contact module; (internal output contacts).
- ▶ With this maximum, also the total number of present input contact modules must be taken in account: Per DP6000-IP Interface unit, the total sum of both is limited to 4.
- ▶ An output contact module has 2 relays, each controlling one individual voltage free contact. (NO or NC)
- ▶ If set, output contacts can become active e.g. in case a system-, technical-, Personal Security alarm occurs etc.

#### 4.3.6 ESPA 4.4.4. interface module; LBB5903/00

One DP6000-IP Interface can be equipped optionally with max. 3 pcs ESPA 4.4.4. interface modules. Standard these are 'ESPA-in' interfaces, meaning that incoming information through the ESPA interface is converted to the DP6000 system that is connected with the DP6000-IP Interface, thus generates paging calls this way.

- ▶ ESPA port nr 3 has as special option: If programmed that way, it works as an 'ESPA-out' port and will resent the same ESPA data which is received from ESPA port 1. In simpler words: Port 3 will follow port 1 then.
- ▶ All ports have a 'closed' ESPA protocol, only parameters like baud rate, start/stop bits, etc. must be set.
- ▶ In case the IP-connection between Communication Server and DP6000-IP Interface is lost, each ESPA-in port will continue in a basic mode; only transferring incoming ESPA calls to the DP6000 system, nothing more than that, no calls can be lost.
- ▶ The function "Notifications" offers to give special attention to operators when specific data comes from an ESPA port. Separate from this it is possible to distribute ESPA information in a multi-site system.
- ▶ Licences for ESPA ports are applicable for the whole system (works system wide).



Note: In case the IP connection, between Communication Server and DP6000-IP interface is lost, all activate ESPA ports continues to work in basic work mode.





#### 4.3.7 RS485 Interface module LBB5904/00

The RS485 Interface module (LBB5904/00) makes it possible to connect the DP6000-IP Interface with external I/O interfaces.

- ▶ At the DP6000-IP Interface this module uses the place of one ESPA 4.4.4. Interface.
- ▶ You can connect max. 5 MPCs (LBB5843/01) to one RS485 module.
- ▶ Each DP6000-IP Interface can handle max. (internal + external) 172 input contacts and max. (internal + external) 172 output contacts.
  - **Tip:** If there are 2 DP6000-IP Interfaces in a system and each of these units has an RS485 unit present, then it is possible to handle  $172 \times 2 = 344$  input and 344 output contacts.

#### 4.3.8 Cable set (set of 2); LBB 8003/00

Each internal input contact requires a connection that includes a resistor network. The cable set provides this network.

With one set of cables, 2 input contacts can be equipped with an cable that includes the resistor network.

If all 4 contacts of one input contact module are in use, 2 cable sets are needed.

### 4.4 Licenses



Note: Each system has its own dedicated set of licenses which are activated system-wide, it means that functions are activated to be used/implemented at any place in the system. Licence fees are paid only 1 time.

#### 4.4.1 Activation Logging; LBB 8600/00

If activated, all events that occur in the system, are logged for further analyses:

- ▶ Source: Which calls were initiated by a central operator, which mobile user, which by an ESPA 4.4.4. interface etc. etc.
- ▶ Handling: Who made which alarm, which locations were passed during the alarm state.
- ▶ The actions that are executed by the operator during the alarm handling.
- ▶ Next to 'what happened', the source of the generated calls is logged.
- ▶ Filtered log data can be 'exported' as CSV-format to focus on specific events and/or time frames.

#### 4.4.2 Activation Personal Security; LBB 8601/00

If activated, the system is able to handle the Personal Security functionality, including:

- ▶ Location detection
- ▶ Personal Security Alarm handling
- ▶ Work mode: manned and/or unmanned mode.
- ▶ Periodically scanning of PS-Pagers
- ▶ Generating technical alarms and follow-up.
- ▶ To execute an 'out rack' test before a mobile is used.

#### 4.4.3 Activation Multi Users; LBB 8602/00

- ▶ A person, can log-on, using individual credentials. Depending on a given authorisation, operator actions or (remote) maintenance etc. etc. can take place.
- ▶ At delivery only one person can be logged in at the same time. This is independent of the persons authorisation/role.
- ▶ Log-on goes via a web browser, installed on (each) PC/laptop/tablet/smartphone.
- ▶ If multiple persons should be able to log-on simultaneously, one or more Multi User Activation license(s) are needed.
- ▶ Each Multi User Activation license increases the maximum of persons that can be logged-on simultaneously by 3.



Note:

If the maximum number of clients, that are logged-on simultaneous, is exceeded, the client with the oldest activity will be disconnected automatically. The result is that a 'forgotten log-on' cannot block a new log-on.

#### 4.4.4 Activation Multi Site; LBB 8603/00

It is possible to control multiple DP6000-IP Interfaces with one single Communication Server.

This is the so called Multi-Site Application. Some application tips:

- ▶ Integrate several local DP6000 systems which are handled by one central.
- ▶ Or the other way around; integrate several, geographical separated, DP6000 systems with the possibility handle these as individual systems. The advantage here is that there is one central point where programming or maintenance can be executed.
- ▶ An extra DP6000-IP Interface connected parallel to another one, can be programmed such that works as redundant unit.

#### 4.4.5 Activation ESPA; LBB 8604/00

The ESPA licence is an activation licence per ESPA port, which enables ESPA ports to transfer incoming ESPA calls to the DP6000 system. Besides transferring incoming ESPA calls to the DP6000 system, the ESPA license provides extra functions:

- ▶ ESPA licences works system wide, it means that it doesn't matter in which DP6000-IP unit the ESPA units are mounted.
- ▶ Active monitoring if the ESPA port is working well. A defect can lead to an automatic call to inform technicians and an indication to inform operators.
- ▶ If logging is activated, the calls sent because of ESPA-data, are included in the logging data.





#### 4.4.6 Activation I/O contacts; LBB 8605/00

- ▶ The system can handle output- and input- contacts, besides 'internal' I/O modules also 'external' I/O units are supported.
- ▶ Handling I/O contacts is a licenced feature; next an 'Activation I/O contacts' licence, also hardware is needed.

#### 4.4.7 Activation 3<sup>rd</sup> Party Connection; LBB8608/00

This license offers the possibility to connect a 3<sup>rd</sup> party to the Communication Server and in this way to control an IP-Interface. On project basis IPS can support during installation.

- ▶ After implementing the Activation 3<sup>rd</sup> Party Connection license, a 3<sup>rd</sup> party can integrate the messages and system statuses in his own application e.g. from/to a communication integration platform, Building Management System etc. etc.
- ▶ The Application Programming Interface (API) is described in the 'Athena API manual' which is made available, after reaching a non-disclosure agreement (NDA). Inform with your commercial contact if needed.

#### 4.4.8 Maintenance agreement; LBB 8609/00

It is possible to include an SLA to cover software maintenance for the system.

If included, a yearly fee will be charged. Please inform with your commercial contact for details and conditions.

#### 4.4.9 Remote Support Device

The Remote Support Device (RSD) offers the possibility to carry out remote support in situations where the use of the customers' local IT-infra is not allowed. With the RSD, a wireless Secured VPN connection with the Communication Server can be build up through the air. This connection offers the advance is that remote maintenance can be performed without using the customers' IT network, and nevertheless a secured full access to the application software can be established.

The RSD is delivered complete pre-configured and includes a SIM card to be able SMS-es for controlling the RSD and data exchange between the (remote) maintenance PC/Laptop. Please contact IPS for options and/or details.

#### 4.4.10 Subscription Fee

For the data transport from/to the RSD and to control the RSD a SIM card is enclosed in the RSD.

Pager Services will invoice on yearly basis the subscription fee.

#### 4.4.11 Ordering additional licenses afterwards

If needed extra licenses can be ordered afterwards, through the IPS-website.

- ▶ In the 'notes field' of the order, you can add your system information to link the license to the right system.
- ▶ When done, the Pagerservices' Order desk will distribute a new license string to be imported in the system.

### 4.5 Server Packages explained

#### 4.5.1 Basic Messaging Server

The content of the Basic Messaging Server is such that it covers the function for critical messaging; f.i.: out of range indication, absent detection, low battery indication. To ease the functions for the operator, call forwarding in case of absent, making group calls and the use of fast buttons are possible. Of course the handling of all calls are logged.

In addition to this, the technical functionality of e.g. ESPA connections, input- and output contacts and IP-infrastructure are monitored.

#### 4.5.2 Basic Personal Security Server

The content of the Basic Personal Security is such that it, next to the functions described in the Basic Message Server, the Basic Personal Security package includes extended monitoring of system equipment, processing of Personal Security alarms from mobiles and its handling, location detection, guard-tour and logging of alarm handling and all incoming and outgoing messages.

#### 4.5.3 Extended Communication server

The content is of the extended Communication server is such that it, next to the functions described in the Basic Message Server and Basic Personal Security Server, also covers an RS458 connection for max. 5 MPC contact couplers, Multi-site to control multiple sub-sites with one central Server and the possibility to connect (and integrate with) 3<sup>rd</sup> party systems.





## 5 The IP Network

Depending on the system specification, the application can be tailored conform the customers' needs. Each system configuration has its own specific IP-network set-up.

Refer to chapter "[Application notes](#)", "[System examples](#)" for examples of possible system lay-outs.

- ▶ Basic system; only one site with one local DP6000 system.
- ▶ Multi-site system with multiple separate DP6000 systems, working within one local IP-subnet.
- ▶ Multi-site system with multiple geographical separated DP6000 systems, working via the Public IP-network.

### 5.1 Minimum IP network requirements

It is strongly advised to make sure that 'IP-network limitations' will not have a negative impact on the products functionality.

- ▶ Create dedicated VLAN(S) to ensure the needed IP-capacity and priority to secure correct function.
- ▶ To secure the communication through the Public IP-network, we advise to make use of Secured VPN connections. Such is important in cases of 'remote sites' or remote maintenance.
- ▶ If reliability and guaranteed IP-access are important, it is advised to implement a dedicated IP-network.

#### 5.1.1 Communication Server

The Communication Server PC is internally equipped with 2 IP-ports. At the outside only 1 IP-port is used.

- ▶ IP-Port 'Network 1'; To connect (all) the DP6000-IP Interface(s) and other IP controlled System equipment.
- ▶ IP-Port 'Network 0'; To connect to external infrastructure e.g. client PC's to be able to log-on as a client.
  - IP-Port 'Network 0'; has a static IP address.
  - IP-port 'Network 1'; can have (if desired) a dynamic IP address to be obtained from a DHCP server, a static IP address is also recommended here.
  - In case the ports 'Network 0' or 'Network 1' are (in-) direct, connected to the Public IP-infrastructure the use of a Secured VPN connection is advised for a secured connection.

#### 5.1.2 Specification Communication server PC

- ▶ If customers do not obtain the computer(s) to be used for the Communication Server from IPS, the following specification guidelines should be obtained:

Parameter	Minimal	Preferred
Processor	4-core	8-core or better
Speed	2.0GHz	3GHz or higher
Work memory	2 x 8GByte RAM	2 x 16GByte RAM or more
Hard disk	2 x 200GB disk (Raid 1)	3 x 250GB or more (Raid 5), SSD.
Network port	1 x 1 Gbit network port	1 x 1 Gbit network port
Operating system	VMWare ESXi 6.5U3	VMWare ESXi 6.5U3

### 5.2 DP6000-IP Interface

The DP6000-IP Interface units and other IP controlled peripherals are connected through an IP interface with the Communication Server using the IP port 'Network 1'.

- ▶ By default the DP6000-IP Interface has already a static IP address, it can be changed if desired.
- ▶ Each DP6000-IP interface, and other IP controlled peripherals, in the system have its own individual IP address.

### 5.3 Web browser and settings

All handling by operators or maintenance personnel is executed through a web browser.

It is advised to use reliable web browsers like:

- ▶ Google Chrome
- ▶ Mozilla Firefox
- ▶ The use of Internet Explorer and Edge is not supported.



Note: In critical applications such as Personal Security it is advised not run any other applications than those needed for alarm handling on your PC. International Pager Services B.V. cannot guarantee correct operation when used in conjunction with other software. This also applies to software like screen savers, firewalls and virus scanners. Note that most computer problems are caused by software behaviour, like bugs or conflicts. Don't let the reliability of the functionality, which is intended to improve the safety of personnel, be compromised by third party software.

Continue at next page: →





### 5.3.1 Automatic Windows Updates

- ▶ PC's used to log on as operator are running under Windows.
- ▶ Windows offers to set automatic updates on or off, the options are therefore:
  - Switch off automatic updates for windows.
    - This might be a not useable setting for organisations.
  - Keep automatic updates active;
    - The result is that all pending applications might be closed while the PC reboots after the automatic update.
    - Therefore you need to be keen as operator that you log on with the program again, otherwise you might miss alarms!

**i** Note: In critical applications such as Personal Security, it might be advisable to organise that (if possible) you, after rebooting the Client PC, always automatically are logged on with the communication server. Contact your system manager if desired.

### 5.3.2 Auto fill in

During handling several actions as operator, the web page might automatically fill in some parameters, which is not always preferred, because some false information might be filled in. It is therefore advised to set 'auto fill' off.

### 5.3.3 Audio settings

Refer to chapter ["Loudspeaker on client PC"](#) for details.

## 5.4 Reserved IP addresses

The following IP- addresses are reserved for use with the communication system.

Device	IP address	Remark
Subnet mask Network 0	255.255.255.000	Advice: In order to prevent IP- conflict use different subnets for Network 0 and Network 1
Subnet mask Network 1	255.255.255.000	
Default gateway	192.168.180.001	Port address 10001
Communication server Network 0.	Via DHCP server	Network 0: To interface with client PC's (web browsers) It is allowed to assign a dynamic IP address (DHCP) if desired. Refer to chapter <a href="#">"Network 0 settings"</a> for details.
Communication server Network 1.	192.168.180.010	This IP address is used to interface with the DP6000-IP Interfaces and other IP-Peripherals used in the DP-system. Refer to chapter <a href="#">"Network 1 settings"</a> for details.
Management IP address	192.168.99.99	This is an overruling IP address used to access the Communication server through its 'Network 0', see details in chapter <a href="#">"Management gateway"</a>
DP6000-IP Interfaces	192.168.180.2x	Use IP address range 192.168.180.20 up to 192.168.180.29
Remote Support through 'Network 0'	To be agreed on locally	To enable remote maintenance from PagerServices Unblock firewall: See port settings below (45045 and 46046).
Reserved	192.168.180.030-100	Reserved for future applications
Miscellaneous	192.168.180.100-255	Free for use
Physical IP address	Via DHCP server	The Server PC has a Physical IP address

### 5.4.1 Port settings

To prevent that active firewalls in managed IP-switches/Routers will block IP-communication, arrange that the relevant ports are set 'open' for communication; Therefore unblock the relevant ports/functions.

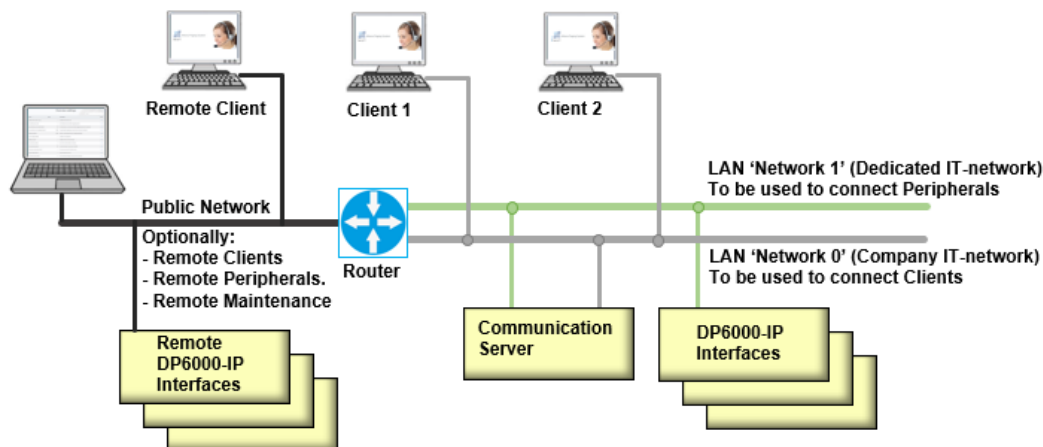
Port to be unblocked	Application	Unblock the port:	Remark
8081	GUI; Communication between Clients and Server;	<u>Always.</u>	TCP/IP
10001	Communication between Server and DP6000-IP Interface(s);	<u>Always.</u>	TCP/IP
45045	SSH Outgoing data;	<u>Allow external access for remote support.</u>	TCP/IP (outbound)
46046	SSH Incoming data;	<u>Allow internal access for SSH connection or using Teamviewer.</u>	TCP/IP (inbound)
ICMP and Arp	Needed to check validity of the licences;	<u>Always.</u>	Both must be allowed
9985	For redundancy polling;	<u>Only in Hot-Stand-by M/S configuration.</u>	UDP
5000	Special SW;	<u>3<sup>rd</sup> party connections with MESA protocol.</u>	TCP
11001	DP7000 systems;	<u>Not applicable yet.</u>	UDP

Continue at next page: →



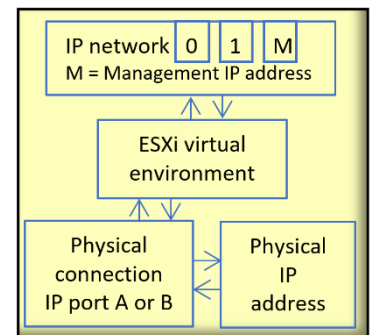


## 5.5 IP-Network topology



## 5.5.1 Virtual IT structure

- ▶ At the right an impression with the relation between the IT-structure and the ESXi virtual environment, as installed at the Communication Servers' PC, is displayed.
  - The communication between the clients and Communication Server is routed through 'IP network 0', the settings are configured via the servers application menu.
  - The communication between DP6000-IP interfaces or other IP controlled peripherals and Communication Server, is routed through 'IP network 1', the settings are configured via the servers application menu.
- ▶ If desired, the communication of 'IP network 0' and 'IP network 1' can be combined to one (same) IP-network e.g. use only 'IP network 0'.
  - The management IP address cannot be changed: refer to "[Management gateway](#)".
- ▶ To connect the server with an IT network, one or more RJ-45 connectors might be available at the servers' PC.
  - In all cases it will be sufficient to use only 1 physical RJ45 connector.
  - The virtual environment is configured such that the IT-traffic is distributed correctly.
- ▶ The physical IP address of the server is used in case e.g. the 'hardware' of the server must be reached. As example to set the date/time at the servers PC.



Warning: The Communication Server is not specified to work in a TCP IPv6 configuration. Therefore we strongly advise to disable that option in your Clients Property settings.

- ▶ Due to the configuration of the ESXi virtual IT-network in the Communication Server, which is implemented by IPS, it is possible to combine both IT-networks 'Network 0' and 'Network 1' to one (and the same) Lan network.
  - For example, you can configure a client to have static IP-address 192.168.180.100 and you can access the server through the IP- address 192.168.180.10:8081.
  - If the 192.168.180.xxx IP-address range is not suitable for your purposes, you can change the network settings as described in in the chapter "[Network settings](#)".
  - The IP-address of the "[Management gateway](#)" is hard coded in the software and cannot be changed.



Note: If you change the server's IP-address to a different range, you need to manually change the IP-address of the IP-DP6000 interface too.

## 5.5.2 Management gateway (IP address)

If set via the system settings, the Communication Server can also be reached through a special management IP address. This management gateway is hard coded: 192.168.99.99:8081, meant for temporarily use in special situations like:

- ▶ To find the servers' regular IP address to connect to as client. (if you forgot it).
- ▶ When a Remote Support Device is used for wireless connection, for details refer to "[Remote Support Device](#)".
- ▶ To set the reachability of the server via the management gateway, refer to 'System settings', "[disable management gateway](#)". (0=Management IP address can be used, 1= Management IP address can NOT be used). The advised setting = 0 to ensure that there is always access possible in case the IP address is unknown.

Tip: To avoid that local network security regulations prevents to reach the server, through its management IP-address, connect the maintenance PC and Communication Server (directly) through a dedicated/temporarily IP cable.

Continue at next page: →





Note: If your PC cannot receive replies on PING requests and you are sure that your network is OK it might be possible that the 'answer' is blocked by the Windows Firewall.



Note: When IP addresses of an IP device are changed, please reboot the device.

### 5.5.3 Enable Ping Replies

When pinging between 2 computers, it is important to realize that it matters which PC is the initiator and which PC is responding. The responding PC must have ping replies enabled. Otherwise you will not get a ping reply and arrive at an incorrect conclusion.

It is advisable to get ping replies working on your test machine and not on the machine that is being installed.

If the initiator computer seems not to receive replies on PING requests, first check the IP network.

- ▶ IP settings like IP addresses, Subnet mask, Default Gateway.
- ▶ Cabling.
- ▶ Switches.
- ▶ Etc. etc.



Note: For build-in network tests, refer to the chapter ["Network test-tools \(build in\)"](#).

## 5.6 Network settings

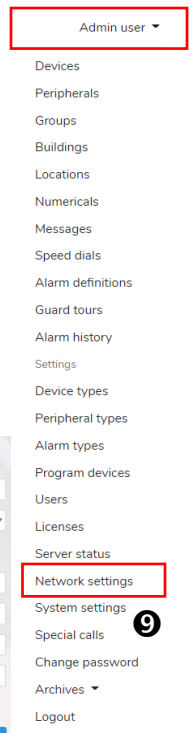
- ▶ Most of the network settings are already preprogramed, and can be changed if desired.
- ▶ To configure the Network settings, go to the menu 'Network settings' 9
- ▶ This opens menu with the following tabs:
  - Network 0; To connect Clients with the user interface of the Communication Server.
  - Network 1; To connect the DP6000-IP interface(s), and other IP-controlled peripherals, with the Communication Server.
- ▶ Furthermore the tabs listed below can be used for diagnostic purposes:
  - Ifconfig;
  - Ping
  - Traceroute
- ▶ Refer to chapter ["Network test-tools \(build in\)"](#), to check these test methods.
  - Generally used test possibilities are described in chapter ["Alternative Network test-tools"](#)

### 5.6.1 Network 0 settings

- ▶ The settings in the tab Network 0, in this environment the following items needs to be set.

- ▶ Name:
  - Give 'network 0' a descriptive name;
- ▶ Timezone:
  - e.g. 'Europe/Amsterdam' which is used in the Netherlands.
  - It is used to synchronise with the UTC
  - Make sure that the all client PC's have the same time zone.

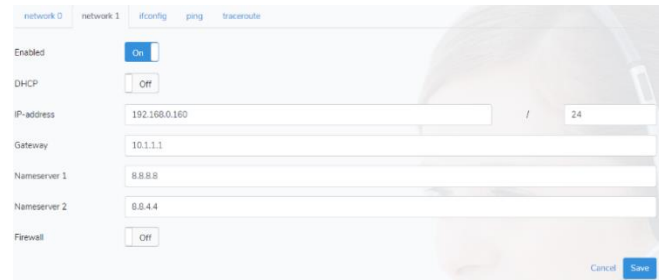
- ▶ DHCP:
  - Set if the IP address is derived through an DHCP server (Slider = On) or not (Slider = Off).
  - If no DHCP is used, the slider must set to 'Off', in that case all remaining IP-settings needs to be filled in:
    - IP-address: The IP address can be a static IP address or it can be obtained through a DHCP server.
    - Gateway:
    - Nameserver 1:
    - Nameserver 2:
- ▶ Set if an internal firewall is activated: If the 'Firewall' is set to 'On', it will block SSH connections, and therefore also 'Remote access' is blocked.
- ▶ Select 'Save' to store the settings.






### 5.6.2 Network 1 settings

- ▶ Network 1 must be configured to enable communication between the Server and DP6000-IP Interface or other IP-controlled peripherals used in the system.
- ▶ Enabled: Set the slider to 'On' to enable this IP port.
- ▶ DHCP:
  - Set if the IP address is derived through an DHCP server (Slider = On) or not (Slider = Off).
  - Note that a static IP-address is advised.
  - If no DHCP is used, the slider must set to 'Off', in that case all remaining IP-settings needs to be filled in:
    - IP-address:
    - Gateway:
    - Nameserver 1:
    - Nameserver 2:
- ▶ The IP address: (only if no DHCP is activated).
  - In addition you need to give the number of bits that are part of the network address: normally '24' will be OK. See the example here →
- ▶ Nameserver 1 and 2:
  - Usually these settings are set the same as in the Network 0 settings.
- ▶ Firewall:
  - Usually this setting is set the same as in the Network 0 settings.
- ▶ Select 'Save' to store the settings.



8 8 8 8 = 32 bits used  
aaaa.bbbb.cccc.dddd 4 bit notation

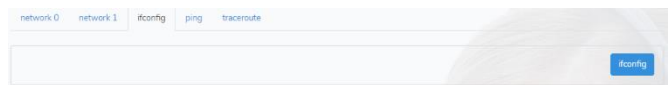
8 8 8 = 24 bits used  
aaaa.bbbb.cccc.xxxx 4 bit notation  
In this example it indicates that the last 8 bits a.b.c.xxxx are free to be used for IP-addressing which is 0-256. (0000-1111)

 Note: After changing IP settings restart the Software of the communication server. For details, refer to the chapter ["Restart the Server \(Software reset\)"](#).

### 5.7 Network test-tools (build in)

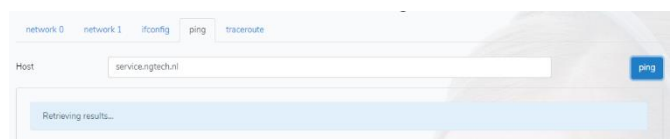
#### 5.7.1 Ifconfig

- ▶ The LINUX variant 'Ifconfig' works as 'Ipconfig'.
  - This tool can be used to check which IP devices are present in the Network.
  - To see the connected items:
    - Select the tab 'Ifconfig'.
    - Select the blue 'ifconfig' button to open the network overview.
- ▶ Ifconfig can be used to find errors in the network configuration e.g.:
  - Bad performance of specific IP devices.
  - Wrong IP configuration.
    - IP conflicts like double IP address usage.
    - Etc. etc.



#### 5.7.2 Ping

- ▶ The ping option is an important tool to check the reachability of some IP-devices.
- ▶ By selecting the blue 'ping button', a 'ping command' is send from your Communication Server PC to a 'Service' PC.
  - By default a 'ping' is sent 'service.ngtech.nl'
  - If it works successful IPS have remote access to 'your' Communication Server PC e.g. for remote support.



#### 5.7.3 Traceroute

In case a 'ping command' is not successful trace route might give information why or where the 'ping' was blocked.



### 5.8 Alternative Network test-tools

- ▶ A tool to check which port is used by which application is e.g. [tcpview](#).
- ▶ As alternative some general-tests tools to check the IT-infrastructure can be carried out by using the 'Command Prompt'.
- ▶ To open the 'Command Prompt':
  - Press the windows button on your keyboard.
  - Write in the search-field 'cmd', this makes a black screen available to use 'test commands'.
    - IPCONFIG                                 Displays all current TCP/IP network configuration (IP address, subnet mask etc.) Use ipconfig instead of ifconfig.
    - PING:<IP-address>                     Send a 'ping' from your terminal to another terminal, if no reply is received, it indicates that there is 'NO IP connection' found.  
If No PING replies can be received, check the Firewall settings, and refer to chapter "[Enable Ping Replies](#)".
    - TRACERT<name of remote station>     This command determines the route to a destination.
    - Arp -a                                    This command displays the IP address, the MAC address and the type of address (dynamic/static) of all other IP equipment after contact with those equipment is established. (computers, switches, peripherals etc.)
    - Route                                     This command can be used to investigate e.g. the internal IP routing.





## 6 Getting started

This chapter describes how to get the Communication Server and DP6000-IP Interface operational.

- ▶ The application software is pre-installed to work as 'Basic system'.
- ▶ IP addresses are pre-configured at both the Communication server and DP6000-IP interface; change them if desired.
- ▶ Set the audio parameters as desired.

### 6.1 Preparations

Make sure that, if needed, the IP-addresses are defined already and preparations with the local IT-department are taken.

### 6.2 Interconnections and operation

#### 6.2.1 Loudspeaker on client PC

Be aware that the client PC must be equipped with an internal loudspeaker.

If no internal loudspeaker is present, or more volume of the audible personal security- and/ or technical alarms is desired, an active loudspeaker set needs to be connected to the client PC.



#### 6.2.2 Audio settings in Web browser

In the web browser settings it is possible to set if you desire audio signals in case of Personal security- and technical- alarms.

- ▶ Refer to settings like 'block website from playing sound' to enable or disable it.  
e.g.: settings, preferences, privacy and security; un-block website from playing sound.

**i** Note: Optional there are several alarm sounds selectable to indicate if and which alarm is raised. You can select for all alarm types the same sound or, if desired, next to a silent indication up to 4 different sounds.

- ▶ Sound 0-4, is set for the alarm-type refer to the chapter "[Sound per Alarm type](#)".
- ▶ To set if the sound belonging to the latest received alarm (Personal Security or Technical) or that Personal Security alarms should always have Priority can be set. Refer to the chapter "[Alarm sound priority](#)" for details.
- ▶ This settings are 'system wide' valid.

### 6.3 IP interfaces

- ▶ For details refer to "[Reserved IP addresses](#)".
- ▶ The virtual IP-port 'Network 1' communicates with the DP6000-IP unit(s) in the system
- ▶ The virtual IP-port 'Network 0' communicates with all client PCs/laptops, make sure that an DHCP server is configured such that a STATIC IP-address is assigned to IP-Port 'Network 0'; the MAC-address of each IP-Port is made visible at the back.
- ▶ Give your maintenance PC/laptop a temporarily IP address e.g. 192.168.180.100  
Make sure that you use a 'free' IP address, or arrange assignment through the DHCP server to prevent conflicts.

**i** Note: The IP port to be used for 'Network 1, and each DP6000-IP Interface and other peripherals must set such that they have a static IP address.

### 6.4 Switching On the Communication Server

- ▶ Press the On/Off switch.

**i** Note: To run the complete the start-up cycle might take several minutes.





## 7 DP6000-IP Interface Hardware

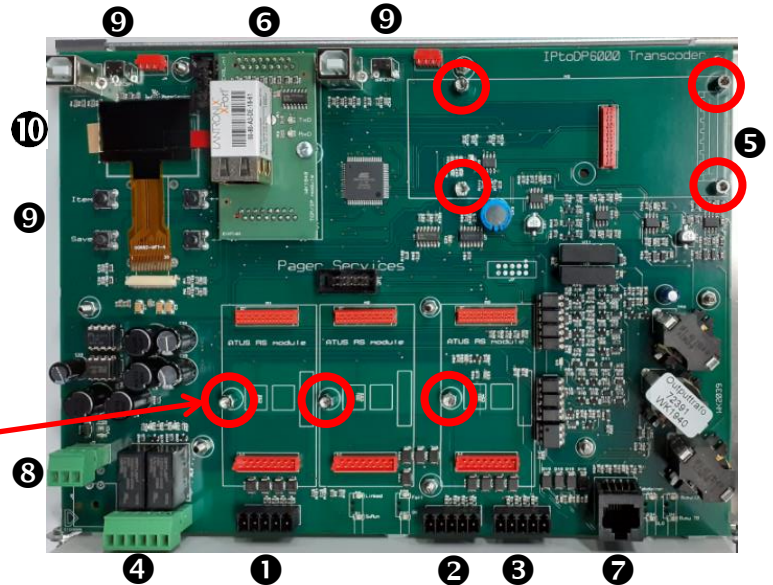
### 7.1 Introduction

DP6000-IP interface is mainly controlled by the software that is installed on the Communication Server. Besides this the DP6000-IP interface has its own embedded firmware.

### 7.2 Hardware- and user interfaces

- ❶ Optional ESPA port 1
- ❷ Optional ESPA port 2 (or optional RS485 port)
- ❸ Optional ESPA port 3
- ❹ Output contacts; 2 relays
- ❺ Optional Input contacts (and/or extra output contacts)
- ❻ IP- interface module
- ❼ DP6000 bus interface
- ❽ 12V Power supply
- ❾ Pushbuttons (6x)
- ❿ Display
- ⓫ LEDs; Functions are here described [“LED indications”](#)

**i** Note: Use the supplied metal distance pieces when adding optional modules.



#### 7.2.1 Paging bus interface

To connect the unit with the DP6000 bus **❷** an RJ45 cable is used. There is the choice to mount an 16 pole Hirschmann connector to the other side or to keep the RJ45 connector there.

It might help you if you want to replace one side of the RJ45 cable with an Hirschmann connector or the other way around.

- ▶ If programmed by the installer, the paging line and TB-lines can be guarded and if an error occurs, a follow-up can be arranged e.g. to inform technicians.

The relation with the pinout of the 25-pole D-connector that was used with the former Alpha-desk is listed in the table below. (paging-lines, TB-lines and system ground).

Hirschmann Connector:	RJ45 pin:	25-pole D Connector:	Signal	8 wire UTP	Remark
1	1	3	Paging line 1	pair 1	Phase sensitive
2	2	16	Paging line 2	pair 1	Phase sensitive
-	3	-	-	pair 2	
4	4	10	system earth	pair 3	
-	5	-	-	pair 3	
-	6	-	-	pair 2	
5	7	1	TB-line 5	pair 4	Phase sensitive
6	8	14	TB-line 6	pair 4	Phase sensitive

**i** Note: Connections used with an Alpha desk (e.g. like the external Watchdog relays) are not listed in the table above, these are not relevant for the Communication Server.

**i** Note: Only 3-wire operation for both Paging lines and TB-lines is supported.

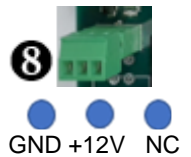
Continue at next page: →



### 7.3 Power Supply

It is advised to use the LBB5943/01 12V-1,5A Power supply.

- ▶ The connection is polarity sensitive.
- ▶ Connect the power supply at position **8** as indicated in the diagram.

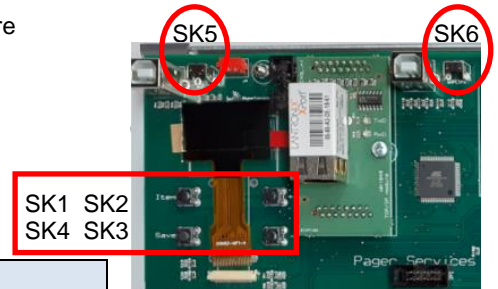


Note: It is advised to use a power supply supplied from IPS; e.g. LBB5934/01

### 7.4 Pushbuttons

At the DP6000-IP interface, several push buttons are present, some of these are used to check and change settings.

- ▶ SK1; Item
- ▶ SK2: ++ (up)
- ▶ SK3: -- (down)
- ▶ SK4: Save
- ▶ SK5: At the upper left corner of the PCB
- ▶ SK6: Right from the TCP-IP module

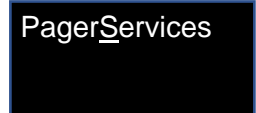


Note: Next to the described function of SK5, SK5 and SK6 are used when a firmware update at the DP6000-IP Interface is carried out.

### 7.5 Display information

A small display is available at the DP6000-IP interface, to display the following information:

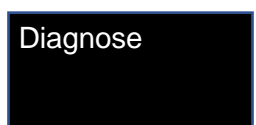
- ▶ At start-up the stand-by screen is displayed.
- ▶ The 'S' of the phrase PagerServices blinks 'S' to 's' to indicate the that firmware is running.



### 7.6 Menu

By pressing SK1 it is possible to navigate to the following menu:

- ▶ Diagnose
- ▶ Setup
- ▶ Testfunctions
- ▶ SW version

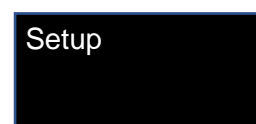


### 7.7 MAC address

To check the MAC address of the DP6000-IP Interface, refer to chapter "[Diagnose menu](#)".

### 7.8 Diagnose menu

- ▶ Press SK1 one (1) times to navigate to the Diagnose menu.
- ▶ Press SK4 one (1) time to confirm.
- ▶ Press SK4 to navigate through the parameters listed below:
  - IP address
  - Gateway
  - Subnet
  - NS address (if relevant).
  - Mac address
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.



### 7.9 Setup menu

#### 7.9.1 IP settings

The IP settings at the DP6000-IP interface can be seen in the display and checked/changed manually by using SK1...SK4.

Continue at next page: →





### 7.9.2 Set the IP address

- ▶ Press SK1, two (2) times to navigate to the Setup menu.
- ▶ Press SK4 one (1) time to confirm.
  - The capital A indicates the part of the IP address that can be set.
  - When the cursor is at the desired position, (a, b, c, d) set that part of the IP address to the desired value.
  - Press with the 'up' and 'down' button until the correct value is reached.
  - By pressing SK1, the setting changes in steps of '10'
  - Press the 'save' button to save the value.
  - Press SK1 again to move the cursor to setting B, C or D. and repeat the steps as described above.
- ▶ If you want to continue to set the gateway address, select SK4 again once you scrolled to 'D'.
- ▶ After changing the IP address, check with 'Ping' if the unit is reachable via the IP network.
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.
- ▶ Note down the IP settings in a document, because there is no back-up for this setting.

**IPaddress**  
169.254.205.201

**Set up**  
Set IP A.b.c.d  
192

### 7.9.3 Set the Gateway

- ▶ When the cursor from the previous setting, is at the desired position, (a, b, c, D) and SK4 is pressed again, the default gateway address can be set to the desired value.
  - Press with the 'up' and 'down' button until the correct value is reached.
  - By pressing SK1, the setting changes in steps of '10'.
  - Press the 'save' button to save the value.
  - Press SK1 again to move the cursor to setting B, C or D. and repeat the steps as described above.
- ▶ If you want to continue to set the subnet mask, press SK4 again once you scrolled further after reaching 'D'.
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.
- ▶ Note down the IP settings in a document, because there is no back-up for this setting.

**Set up**  
Set IP a.b.c.D  
20

**Set up**  
Set GW A.b.c.d  
255

### 7.9.4 Set the subnet mask

- ▶ When the cursor from the previous setting, is at the desired position, (a, b, c, D) and SK4 is pressed again, the gateway address can be set to the desired value.
  - If you want to skip this setting just select SK4 once more, the option to change the port address will appear.
- ▶ To change the subnet mask continue:
  - Press with the 'up' and 'down' button until the correct value is reached.
  - By pressing SK1, the setting changes in steps of '10'.
  - Press the 'save' button to save the value.
  - Press SK1 again to move the cursor to setting B, C or D. and repeat the steps as described above.
- ▶ If you want to continue to set the port number select SK4 again once you scrolled to the last byte '0'.
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.
- ▶ Note down the IP settings in a document, because there is no back-up for this setting.

**Set up**  
Set Subnet  
255.255.255.0

### 7.9.5 Set the Port address

- ▶ When the cursor from the previous setting, is at the desired position, (a, b, c, D) and SK4 is pressed again, the port address can be set.
  - If you want to skip this setting just select SK4 once more.
- ▶ To change the subnet mask continue:
  - Press with the 'up' and 'down' button until the correct value is reached.
  - By pressing SK1, the setting changes in steps of '10'.
  - Press the 'save' button to save the value.
- ▶ If you want to continue to set the all IP settings to their default values, select SK4 again once.
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.
- ▶ Note down the IP settings in a document, because there is no back-up for this setting.

**Set up**  
Set PortAddress  
10001

**Notes:**

- ▶ All relevant IP settings in the DP6000-IP interface must be equal as set in the 'peripheral' settings.
- ▶ These IP settings are not backed up, note them in a document, because there is no back-up for these settings.

Continue at next page: →



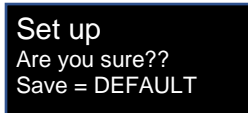
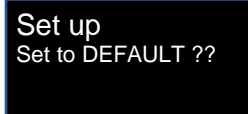




7.9.6 Set IP settings to default

From the previous setting it is possible to enter the option to change all IP-settings to default values.

- ▶ In the display the remark 'set to DEFAULT ??' is visible.
- ▶ If you don't want to do this just wait until the time out is expired.
  - If you want to set all settings to the default value, select SK4 to confirm.
  - Confirm again with SK4 (Save) to be sure to set all IP settings to default values.
    - IP address: 192.168.180.20
    - Gateway: 255.255.180.1
    - Subnet mask: 255.255.255.0
    - Port address: 10001
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.



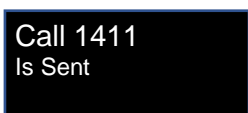
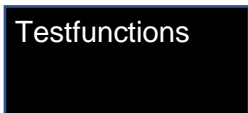
7.10 Testfunctions menu

This menu can be used without a Communication Server, to check if the DP6000-IP interface can sent calls. By using a pager in monitoring mode, it is possible to receive the call.

- ▶ Press SK1, three (3) times to navigate to the Testfunctions menu.
- ▶ Press SK4 one (1) time to enter the Testfunctions menu.
- ▶ A text 'Call 1411' appears; see example at the right.
  - Press SK4 to confirm.
  - The result is that a test call is transmitted:
 

Address	Bleep	Info	Message	Modeword
1411	B	98765	987654321ABC	40006
- ▶ If you press SK1, A text 'Call 1412' appears.
  - Press SK4 to confirm.
  - The result is that a test call is transmitted:
 

Address	Bleep	Info	Message	Modeword
1412	B	98765	987654321ABC	40006
- ▶ Leaving this menu: press SK5. (here is no time-out activated to leave the menu).



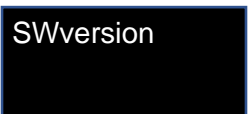
7.11 Software versions menu

The DP6000-IP interface contains 2  $\mu$ -processors.

One  $\mu$ -Processor 'L' and a  $\mu$ -Processor 'R'.

To check the Firmware version loaded in both  $\mu$ -processors proceed as follows:

- ▶ Press SK1, for (4) times to navigate to the 'SWversion' menu.
- ▶ Press SK4 one (1) time to confirm.
  - Data preceded with 'L' indicates the version and date of Processor 'L'.
  - Data preceded with 'R' indicates the version and date of Processor 'R'.
- ▶ Leaving this menu: press SK5 or wait for a time out of 25 seconds.



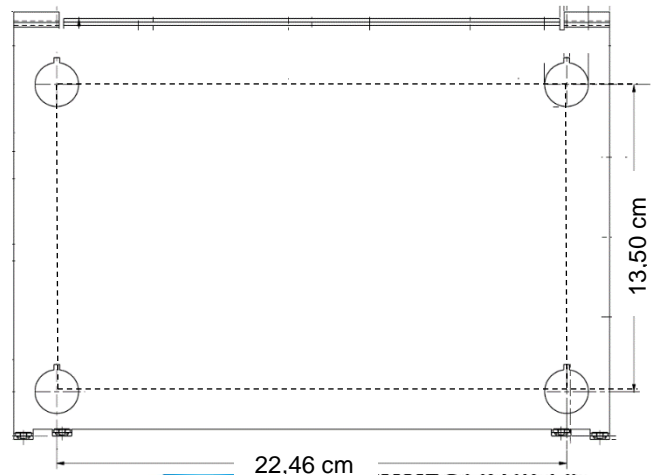
**i** Note: All present DP6000-IP interfaces in a system, must have the equal firmware version loaded in  $\mu$ -Processor 'R'. This FW controls the communication with the Communication server. The firmware version must correspond with the system setting "[fw-version](#)". In this example the firmware version  $\mu$ -Processor 'R' is 00.00.24.

**i** Note: Next to the described function of SK5, SK5 and SK6 are used when a firmware update at the DP6000-IP Interface is carried out. Refer to chapter "[Update firmware DP6000-IP Interface](#)" for details. **IMPORTANT:** reset the server software after FW-updates in the DP6000-IP\_ Interface!

7.12 Dimensions

- 7.12.1 Mechanical
- |                        |                                   |
|------------------------|-----------------------------------|
| Dimensions (H x W x D) | 81.5 x 270 x 190 mm               |
| Weight:                | 1,032 kg                          |
| Dust and waterproof:   | IP40<br>(intended for indoor use) |

- 7.12.2 Drilling pattern
- Drilling sizes: 22,46x13,50cm, see drawing at the right:



Continue at next page: →



7.13 Install the ESPA interface module

The ESPA interface modules are developed to create an ESPA 4.4.4 interface with 3th parties, e.g. a nurse call system, fire system etc.

- ▶ The maximum of ESPA modules in one DP6000-IP Interface is 3.
  - If more than 3 ESPA interfaces are needed, extra DP6000-IP Interfaces should be installed. The ESPA interface modules can be installed at position **1 2 3**.
  - Optionally ESPA Port 3 can also be set as 'ESPA-out' port. The data received via port 1 is mirrored to port 3 then.
- ▶ If an RS485 module is needed (to communicate with LBB5843/01 heads), port 2 is not available as ESPA interface
- ▶ Place the ESPA interface module at position 1, 2 and/or 3.
- ▶ Configure the work-mode (in/out) and parameters per ESPA port.
  - Refer to chapter "[ESPA Ports](#)" for details.



9P D female - RS232 Cable

5	GND	1	
2	TxD	2	
3	RxD	3	
8	Rts	4	
7	Cts	5	

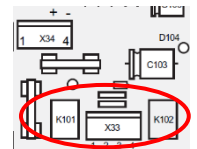
7.13.1 The RS232 cable

- ▶ Together with the ESPA interface module a 5 pole connector is delivered, use this connector to make an ESPA cable with an 9p female D connector.
- ▶ The absolute max. length of an RS232 cable is 15meter!

7.14 Prepare the LBB5843/01 MPC heads

7.14.1 Set the address of the MPC

- ▶ At the right upper corner on the MPC there is a 8 digit DIP switch S201, to set the head addresses in the HEX-range 1 up to 5. (Head 1 - Head 5).
  - SK7 and SK8 are not used, SK6 is the LSB.
  - Address 00000000 is not allowed.
- ▶ External contacts
  - X33-1 and X33-2 are used for Re1 (K101); to be set as NO or NC contact.
  - X33-3 and X33-4 are used for Re2 (K102); to be set as NO or NC contact.

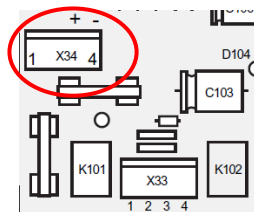


7.14.2 Install the RS485 module

- ▶ An RS485 module enables the DP6000-IP Interface to communicate with LBB5843/01 (MPC) heads.
  - ▶ The RS485 Interface module can be installed in a DP6000-IP Interface only at position 2
  - ▶ There can only 1 (one) RS485 Interface Module be installed per DP6000-IP Interface.
  - ▶ Per DP6000-IP Interface/RS485 interface module, max. 5 LBB5843/01 units (=160 contacts) can be supported.
  - ▶ If more than 5 MPC heads needs to be connected, extra DP6000-IP Interfaces should be installed.
  - ▶ Set port 2 such that it works as RS485 port.
- Refer chapter "[Configure the RS485 interface module](#)" for details.

7.14.3 RS485 Cable

- ▶ Together with the RS485 module a 5 pole connector is delivered, use this connector to make an (parallel) RS485 cable to be connected with X34 at the MPC heads.
- ▶ Find just above 2 fuses at the MPC head, connector X34.
  - X34-1; used for RS485-A interface. (phase sensitive!).
  - X34-2; used for RS485-B interface. (phase sensitive!).
    - Connection 'B' is the 'hot' signal line.
    - Connection 'A' is the 'cold' signal line.
  - X34-3; used to power the MPC head; +12V.
  - X34-4; used as GND.
- ▶ Multiple MPC heads are to be connected with the RS485 cable as a 'daisy-chain' cable.
- ▶ The max length of a RS485 cable is ca. 1km.



X34 MPC - RS485 Cable

4	GND(see note)	→	1	
1	RS485 A	→	2	
2	RS485 B	→	3	
			4	
			5	



Note: In some systems it may be necessary to make an earth connection between the RS485 module and the MPC heads. e.g. When a high potential difference between the MPC heads and the RS485 module interferes with the communication; creating an earth connection may solve the problem.

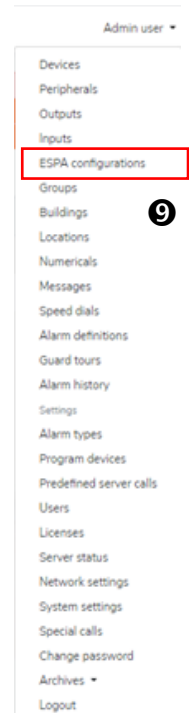
Continue at next page: →





7.14.4 Configure the RS485 interface module

- ▶ For details how to program external contacts with an LBB5843/01, go to chapter “[Program I/O contacts](#)”.
- ▶ The communication port for the RS485 module is set via the ESPA configuration menu.
  - Go to ‘ESPA configurations’ ⑨
  - Select ‘Add ESPA configuration’
  - Peripheral:
    - Select the DP6000-IP Interface on which the RS485 module is present.
  - Port:
    - Select the port to be set; **for an RS485 Interface module this is always Port 2!!**
  - Direction: Select: ‘channel in use for RS485 (MPC)’.
  - Predefined call on connection error; For details refer to chapter “[RS485 Communication monitoring](#)”.
  - Select ‘Save’ when ready.



**i**

- De Communication Server can handle internal and external I/O contacts.
- The input contact module, LBB5901/00, is used to handle ‘internal input contacts’.
- The output contact module, LBB5902/00, is used to handle ‘internal output contacts’.
- Each DP6000-IP Interface can handle 12 internal input- and 4 output- contacts.
- External I/O contacts are from one or more MPC heads; LBB5843/01.
- The max. external I/O contacts per DP6000-IP Interface is 160 input- and 160 output contacts.

7.14.5 Monitoring RS485 connection

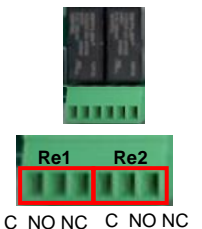
- ▶ In the port settings for the RS485 module there is the option to select a ‘Predefined call on connection error’. This offers the possibility to send a call (e.g. to inform technicians) if the communication with an MPC head is lost.
  - If a ‘Predefined IP-DP6000 call’ is configured and selected here, that paging call will be transmitted automatically in case the RS485 communication with one or more MPC heads went lost.
  - When set correct, a predefined IP-DP6000 call is transmitted in case the RS485 communication with a specific MPC head is lost. e.g. program a message ‘Connection error #H’. (H = Head address).
  - For details refer to “[Predefined IP-DP6000 calls](#)”.
  - If ‘No call’ is selected here, there will no call be sent in case of communication error, i.e. no monitoring takes place.

7.15 Installing Internal I/O contact modules

7.15.1 Internal Output contact modules

One DP60000 IP Interface can handle max 4 internal output contacts (i.e. Re1 up to Re4).

- ▶ At position ④ there are already 2 output relays present. This are relays Re1 and Re2.
- ▶ The relays at the left is Re1, the relays at the right is Re2.
- ▶ Each relays has a 3 pole connector:
  - Normal Open (NO), Normal Closed (NC) contact.
  - Terminal C is the common contact.



Max. 1 (one) LBB 5902/00 output contact module can be placed at position ⑤.

- ▶ Be aware: The total sum of all input contact modules and output contact modules is 4.
- ▶ The modules can be placed above each other ‘as a sandwich’ see example below.
- ▶ The Relays at the left is Re3, the Relays at the right is Re4.
- ▶ Each relays at output contact module the has a 3 pole connector:
  - Normal Open (NO), Normal Closed (NC) contact.
  - Terminal C is the common contact.



**i**

Note: When the function of each of these 4 relays is programmed the head number should always be ‘0’, which indicates that these are ‘internal’ output contacts. Refer to chapter “[Program I/O contacts](#)” for details. To configure external I/O contacts, Refer to chapter: “[Prepare the LBB5843/01 MPC heads](#)”

Continue at next page: →



### 7.15.2 Internal Input contact module

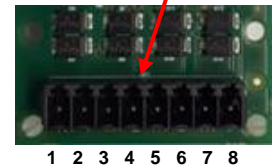
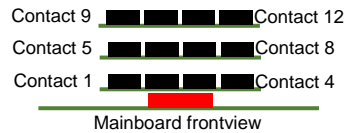
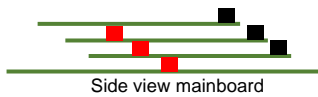
The DP60000 IP Interface can handle max 12 internal input contacts. (i.e. contact 1 up to contact 12).

- ▶ Each contact has 2 terminals.
- ▶ Internal input contacts can be programmed as 'guarded' or 'non-guarded' contact.
- ▶ The function for Normal Open (inactive) or Normal Closed is determined by programming.
- ▶ The internal input contacts are build up as analogue input, therefore it is ALWAYS needed to connect a resistor network to an input. This resistor network is used to:
  - Detect if a contact is active or inactive.
  - In case of guarded inputs, to detect if the wirers are short circuited or interrupted.
  - For details of the resistor network refer to chapter "[Resistor network](#)".



Max. 3 extra LBB 5901/00 input contact modules can be placed at position. **5**

- ▶ Be aware: The max. total sum of all input contact modules and output contact modules is 4.
- ▶ The modules are placed above each other 'as a sandwich' see example below.
- ▶ The module that is most closed to the mainboard is module 1 which supports contact 1- 4.
  - The next module is module 2 which supports contacts 5 to 8 etc.
- ▶ Each Input contact module has its own address, in case more than one Input contact module is used, the address of the extra units must be set. Refer to chapter "[Set address of the input contact module](#)".



- ▶ Each input contact module has an 8 pole connector.
- ▶ Terminals 1 and 2 are used for contact 1 (5 or 9).
  - Terminals 3 and 4 are used for contact 2 (6 or 10).
  - Etc. etc.

**i** Note: When the function of each of these internal input contacts is programmed, the head number should always be '0', which indicates that these are 'internal' input contacts. Refer to chapter "[Program I/O contacts](#)". To install external I/O contacts, Refer to chapter: "[Prepare the LBB5843/01 MPC heads](#)".

### 7.15.3 Cable set

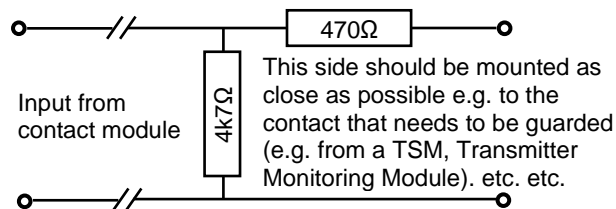
A cable set contains 2 cables, one cable is needed per (analogue) internal input contact. One side of this cable is equipped with a resistor network.

**i** Note: The cable side with the detection resistors must be mounted as close as possible to contact to be guarded e.g. BMC, Transmitter Monitor Unit etc.

### 7.15.4 Resistor network

Because the internal input contacts are build up as analogue input, a resistor network is needed for each internal input contact, to be able to detect the status of the relevant input contact. This resistor network is positioned as close as possible to the (guarded) contact, see diagram below.

- The easiest way to obtain a cable with the required resistor network is to order a "[Cable set](#)" (to serve 2 contacts).
- Alternatively you can build the resistor network by yourself, see the schematic diagram below for details. Typical specification of the resistors: 0,125watt, 5%.

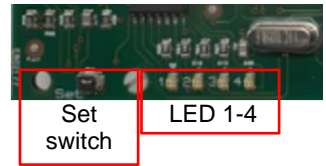


Continue at next page: →



### 7.15.5 Set address of the input contact module

By default each input contact module is delivered while the board address is programmed as '1'. In case more than one input contact module is used, the board address of the extra input contact modules boards must be changed.

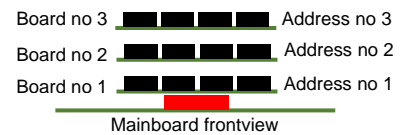


To change the board address proceed as follows:

- ▶ Make sure that all modules are installed correct, LEDs 1-4 are blinking (there is power).

**i** Note: If the inputs are terminated with an resistor of 4k7, then LED 1, 2 or 3 will lit steady green (not blinking) which indicates the programmed board address 1, 2 or 3. The board address is stored at the input contact board.

- ▶ In the example below the procedure is described how to change board address 1 to board address 2.
  - Press and hold the 'Set switch' for ±3 seconds.
  - Release the 'Set switch'.
  - LED 1 (RED) starts to blink.
  - Press the 'SET switch' again 1x.
  - Now LED 2 blinks (RED) indicating that board address 2 is selected.
    - To select board address 3, press the Set switch once more, the result is that LED 3 starts to blink RED, indicating that board address 3 is selected.
  - To store the desired board address setting press, within 1 second after the previous step, the 'SET switch' again and hold it for ± 3 seconds.
  - Release the 'SET switch'; the LEDs as described above will start to blink again.
    - If the inputs are terminated with a 4k7 resistor, LED 1, 2, or 3 will lit steady, showing the programmed board address.
    - If the inputs are NOT terminated with a 4k7 resistor, the programmed board address can be checked a follows:
      - Press the 'Set switch' shortly.
      - The corresponding LED 1,2 or 3 will lit steady, indicated the programmed board address.



### 7.16 LED indications

Several LEDs shows the status of the DP6000-IP interface and installed (optional) modules.

#### 7.16.1 LED indications; IP interface module

LED ID	Function	Colour		Remark
n.a.	Show IP connection	Green		The green LED at the left on the IP connector lit continue to indicate that there is an IP-connection detected.
n.a.	Show IP communication	Yellow		A yellow LED at the right of the IP connector blinks when there is IP-DATA communication detected.
n.a.	Shows if there is IP data transmitted or received			The RED led at the IP interface module indicates that there is transmitted (TxD) data sent via the IP connection. The Green led at the IP interface module indicates that there is received (RxD) data coming from the IP connection.

#### 7.16.2 LED indications; Input Contact module

LED ID	Function	Colour		Remark
Led 1-4	Input Open	Green		4k7Ω from resistor network is detected.
Led 1-4	Input Closed	Red		470Ω//4k7 (=427Ω) from resistor network is detected.
Led 1-4	Error	OR-GN		Blinking OR-GN: Line interrupted; 4k7Ω NOT detected.
Led 1-4	Error	OR-RD		Blinking OR-RD: Line short circuit; (0 ohm detected).
LED 1-3	Address indicator	Green		Indicates the programmed board address, only visible if the input state is 'open'.


#### 7.16.3 LED indications; Output contact module

LED ID	Function	Colour		Remark
n.a.	Status Re3	Blue		The corresponding LED lit when RE3 is activated
n.a.	Status Re4	Blue		The corresponding LED lit when RE4 is activated


Continue at next page: →



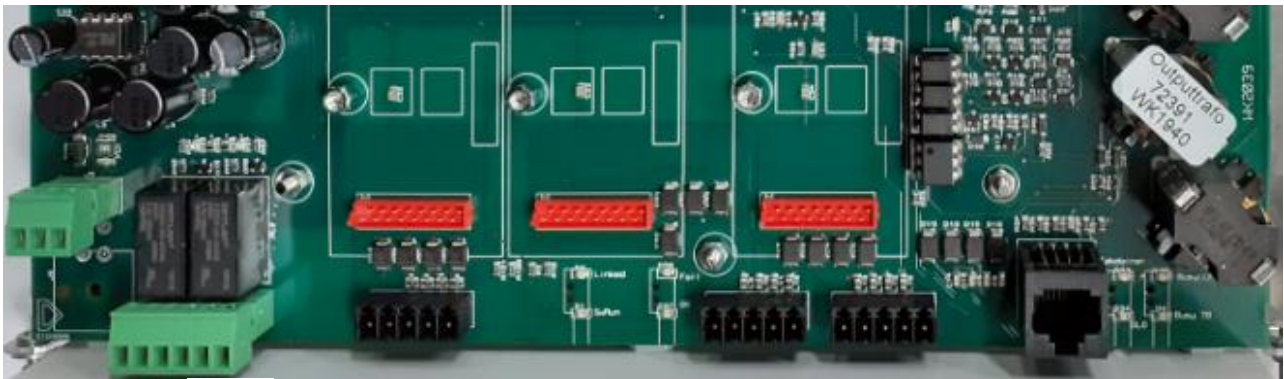
7.16.4 LED indications; ESPA module

LED ID	Function	Colour	Remark
TxD	Transmit data	Red	 <p>The 4 LEDs shows the status of the ESPA port.</p> <p>In practice the LEDs will blink because the communication status of the ESPA port changes continue.</p>
RxD	Receive data	Green	
Rts	Ready to sent	Blue	
Cts	Clear to sent	Blue	

7.16.5 LED indications; RS485 module

LED ID	Function	Colour	Remark
D1	TxOn	Blue	 <p>The 3 LEDs shows the status of the RS485 port.</p> <p>In practice the LEDs will blink because the communication status of the RS485 port changes continue.</p>
D2	TxD	Red	
D3	RxD	Green	

7.16.6 LED indications DP6000-IP Interface



D35 D37

D2  
D1

D33 D30  
D34 D6

LED ID	Function	Colour	Remark
D1	SW running	Blue	LED D1 is blinking when de firmware at the DP6000-IP unit is running.
D2	Linked	Yellow	LED D2 lit continue when connected with the server, blinking means that the DP6000-IP unit is waiting for a connection from the server.
D6	Busy TB	Yellow	LED D6 is blinking when there is data detected at the Talk-back lines. OFF means no data detected.
D30	Busy LF	Yellow	LED D30 lit when another encoder occupies the paging-lines.
D33	Take line	Red	Led D33 lit when the DP6000-IP unit is occupying the paging-lines.
D34	OLO	Blue	Led D34 lit when the DP6000-IP unit occupies the paging-lines.
D35	Status Re1	Blue	LED D35 lit when RE1 is activated.
D37	Status Re2	Blue	LED D37 lit when RE2 is activated.

Continue at next page: →





7.17 Firmware version

The firmware versions of the DP6000-IP Interface can be checked via the [“Software versions”](#) menu. In multi-site system it is advised to have the same firmware on all DP6000-IP Interfaces.


**i** Note: Keep the firmware of all DP6000-IP interfaces in one system equal with each other. Make sure that the firmware version for  $\mu$ -Processor ‘R’ is also set correct in the system setting [“fw-version”](#).

7.18 Replace a DP6000-IP Interface

- ▶ If a DP6000-IP Interface is defect, you can apply for repair through the regular repair procedure if desired.
- ▶ Next to arranging repair, you need to check if (replacing) the defect unit has impact on the system licences!

7.18.1 License Check

Check if licences are assigned to the defect DP6000-IP Interface:

In case licences are assigned to a DP6000-IP Interface it is indicated with a shield-sign as shown at the right: → 

- ▶ Find in the ‘Peripherals’ menu if the defect DP6000-IP Interface is marked with the ‘shield-sign’, 2 options:
  - The unit is NOT marked with the ‘shield-sign’ (which can only be the case in multi-site systems).
  - The unit is marked with the ‘shield sign’ (this is always the case in single- and one time in multi-site systems).

**i** Note: In single-site systems, licences are always assigned to the DP6000-IP Interface that is present. In multi-site systems the licences are assigned to only 1 DP6000-IP interface; the ‘main PD6000-IP interface’.

**i** Note: After a software reboot of the server, the system will work for a maximum of 72 hours licence free. After this time the system will stop important services. A software reboot of the server (again) gives an extra 72 hours if needed.

7.18.2 Replacement options

There are different scenario’s possible to organise the repair of a DP6000-IP Interface resulting in different consequences:

How to organise repair depends on:

- a) If the DP6000-IP Interface is used in a multisite system.
- b) If the system licences are coupled with the defect DP6000-IP Interface.
- c) If there is a replacement DP6000-IP Interface available.



Multisite System	Licences coupled	Replacement available	Possible solutions
N	N	N	This option is not relevant
N	N	Y	This option is not relevant
N	Y	N	Sent the defect DP6000-IP-Interface for repair. In this scenario the system will be out of order as long as the turnaround time for the repair will take.
N	Y	Y	Check at the defect DP6000-IP Interface if the defect is caused by unit <b>6</b> If this is not the case you can exchange the <a href="#">“TCP-IP module 6”</a> from the defect DP6000-IP Interface. This will prevent that you need to apply for new licences. If at the defect DP6000-IP Interface the defect is caused by unit <b>6</b> You need to <a href="#">“apply for new licences”</a> .
Y	N	N	Sent the defect DP6000-IP-Interface for repair. In this scenario a part of the Multisite system will be out of order as long as the turnaround time for the repair will take.
Y	N	Y	You can install the replacement DP6000-IP-Interface following all the steps to get the unit operational.
Y	Y	N	Check at the defect DP6000-IP Interface if the defect is caused by unit <b>6</b> If this is not the case you can exchange the <a href="#">“TCP-IP module 6”</a> with another one in the Multi-site system, it will limit the system dysfunctionality. In this scenario the system will be (partly) out of order as long as the turnaround time for the repair will take.
Y	Y	Y	Check at the defect DP6000-IP Interface if the defect is caused by unit <b>6</b> If this is not the case you can reuse the <a href="#">“licenced unit 6”</a> from the defect DP6000-IP Interface. This will prevent that you need to apply for new licences. If at the defect DP6000-IP Interface the defect is caused by unit <b>6</b> You need to <a href="#">“apply for new licences”</a> ; Contact Pagerservices to arrange it.

**i** Note: Pagerservices advises to create your own local swop pool to replace a defect DP6000-IP Interface. Once Pagerservices repaired the defect unit it you will sent back, no swop will be arranged.

Continue at next page: →



### 7.18.3 Exchange the TCP-IP module

- ▶ If a DP6000-IP Interface is defect and the licences are assigned to this unit (in single site systems this is ALWAYS the case) then licences will be lost if the complete DP6000-IP Interface is replaced by a new unit.
- ▶ A method to preserve the licences is to move the TCP/IP module from the defect unit to the replacement unit. This action can prevent the need to apply for new licences.
  - Make sure the DP6000-IP Interface is disconnected from the Power supply.
  - Remove the screw (indicated at the red circle).
  - Now you can unplug the TCP/IP module to be mounted at the replacement DP6000-IP Interface.
  - Continue with chapter: [“Replace a defect DP6000-IP Interface”](#).
- ▶ In case the TCP/IP module is defect, continue with chapter: [“Apply for new licences”](#).



### 7.18.4 Apply for new licenses

- ▶ If licences are assigned to a defect DP6000-IP interface, and local actions to exchange the TCP/IP module is not possible or not successful, then (with the replacement of the defect DP6000-IP Interface) you need to apply for new system licences. With the new licence file, the system licenses are assigned to the replacement DP6000-IP Interface.
  - To order a new licence file, contact Pagerservices with [orders@pagerservices.nl](mailto:orders@pagerservices.nl).
  - Inform Pagerservices about the serial number of the replacement unit.
  - A new licence file can be imported, for instructions refer to: [“Update the licence file”](#).
  - Continue replacement as described in chapter: [“Replace a defect DP6000-IP Interface”](#).
  - The defect DP6000-IP Interface can be sent to Pagerservices for repair.



Note: The steps as described in chapter [“Replacement options”](#). can prevent the need to apply for a new licence file. If a new licence file is delivered, you will be charged against regular license costs. Once the defect (main) DP6000-IP interface is sent to Pagerservices you will receive a credit note to compensate the costs for the new licence file.

### 7.18.5 Replace a defect DP6000-IP Interface

To replace a defect DP6000-IP Interface, follow the steps below if applicable:

- ▶ Make sure there are no licence consequences or make sure that new licences are arranged. (see previous chapters)
- ▶ Uninstall the defect DP6000-IP Interface:
  - Remove all cables from the defect DP6000-IP Interface, to start with the power supply cable.
  - Eventually remove sub-units like I/O contact module(s), ESPA module(s) and RS485 module
  - Disconnect the DP (paging) cable.
  - Disconnect the IP cable
  - Note that the: TCP/IP module may not be removed unless it is needed as described in chapter: [“Replacement options”](#).
- ▶ Install the new/replacement DP6000-IP Interface:
  - Connect all cables to the DP6000-IP unit to start with the power supply cable.
  - Eventually mount all sub-units like I/O contacts and ESPA units.
  - Connect the DP (paging) cable.
  - Connect the IP cable
  - Note that the: TCP/IP module may not be exchanged unless it is needed as described in chapter: [“Replacement options”](#).
- ▶ Set the IP address in the DP6000-IP unit: [“Set the IP address”](#).
- ▶ Check if the DP6000-IP Interface communicates correct with IP-Network (Communication server/Ping etc. etc).
- ▶ If present; Install the ESPA interface module(s); refer to chapter [“Install the ESPA interface module”](#).
- ▶ If present; install the RS485 port; refer to chapter [“Install the RS485 interface module”](#).
- ▶ Install the internal Input/Output contact units; refer to chapter [“Installing Internal I/O contacts”](#).

### 7.18.6 Repair Costs

If a defect DP6000-IP Interface is sent to be repaired, you can contact [orders@pagerservices.nl](mailto:orders@pagerservices.nl) for repair cost.







## 8 Programming

### 8.1 Set up a Client IP-connection

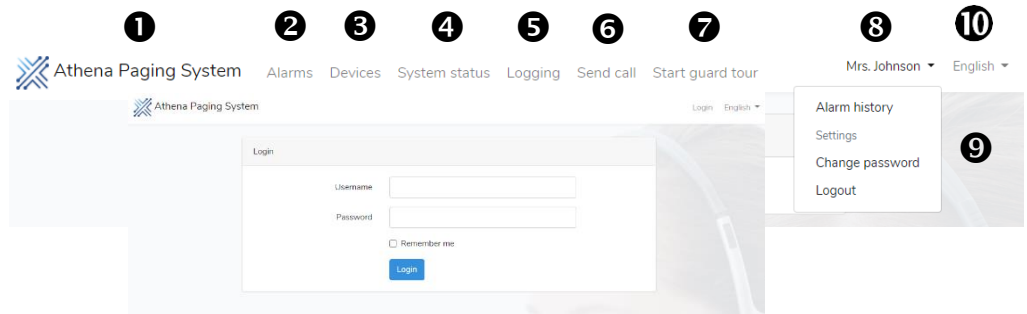
- ▶ If needed check in the DHCP server which (static) IP Address is assigned to IP-Port 'Network 0' of the Communication server.
- ▶ Open the web browser on your client/maintenance PC and use: <http://<IP-address>:8081>
- ▶ The start screen should open.



### 8.2 The start screen

The start screen that appears once being connected with the Communication Server, looks like:

1. Home button
2. Alarm screen
3. Devices
4. System status
5. Logging
6. Send Call
7. Guard tour
8. Login button/admin button
9. User menu
10. Language button

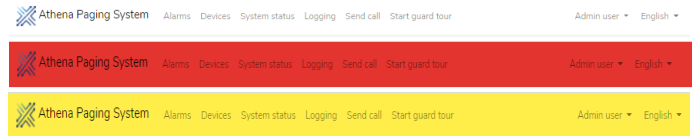


### 8.3 Set header colour

The colour of the header can be set in the ["System settings"](#), ["header\\_color"](#)

These setting works per Communication server and can be useful in situations like e.g.:

- ▶ To make the header more explicit visible.
- ▶ In case of redundant Communication servers are used, to see via which Communication server an operator works.
- ▶ Available are the colours:
  - White (default)
  - Red
  - Yellow
  - Green
  - Blue
  - Teal (Green-Blue)



### 8.4 Set Language

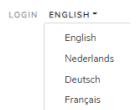
- ▶ There are 2 places to set the language for the system:
  - Server language
  - User language


#### 8.4.1 Server language

- ▶ Some system responses (e.g. for alarm handling, instructions and specific messages) are hard-coded in the software of the Communication Server.
- ▶ It is therefore needed to select the desired language in the server settings ["server-language"](#).
  - (en = English, de = Deutsch, fr = Français, nl = Nederlands).

#### 8.4.2 User language

- ▶ To set the desired language for the operator-screens, go to the right upper corner of the start screen, there is the option 10 to change the desired user language.
- ▶ To change the language, go to the 'Language button' in the upper right corner: Possible choices are:
  - English
  - Nederlands
  - Deutsch
  - Français
- ▶ For each operator this setting should be executed, so different languages over different operators are allowed.



 Note: If you changed the language it might be needed to ["Restart the Server"](#) to take effect.





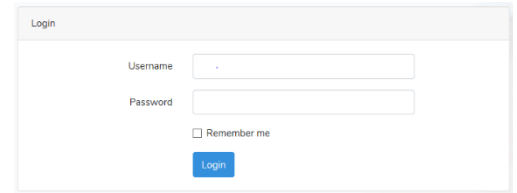
### 8.5 Log in

In the upper right corner, there is the 'LOGIN button' 8, to log in into the system.

Depending on the level of authorisation, several options will be active once you are logged in.

Beware that **each user should have its own login credentials**. If you are using the credentials mentioned below you will have maximum administration rights, be careful!!

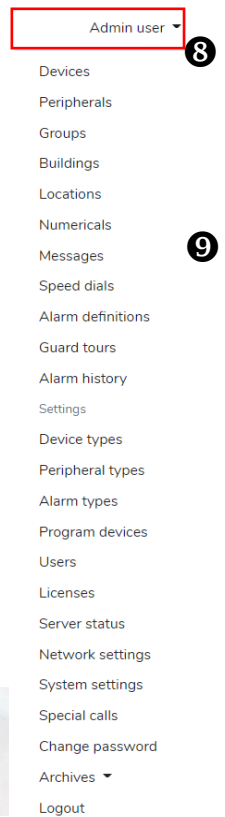
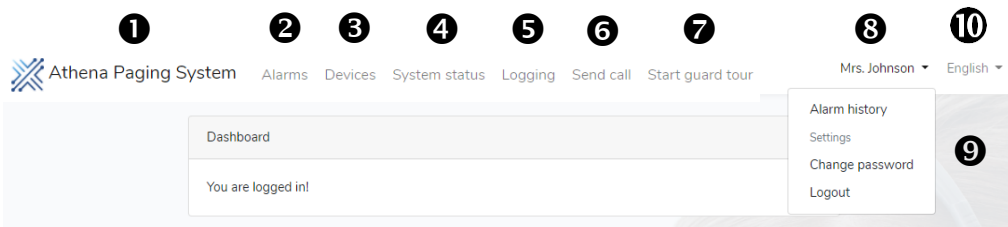
- ▶ Select the option: LOGIN
- ▶ Enter the default credentials:
  - Username: admin@athena.ips
  - Password: secret
- ▶ Check the box 'Remember me' to stay logged in after >1h inactivity.



**i** Note: If you keep the box 'remember me' unchecked, you will be logged off automatically after 1 hour inactivity. Don't check this box when you are an 'incidental' user.

### 8.6 Main screen

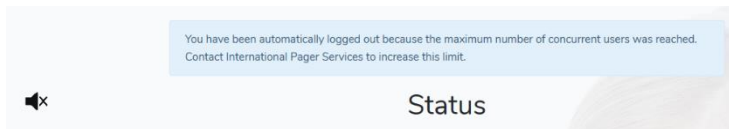
After successfully being logged in, the following dashboard screen appears:



- ▶ Depending on the operator's authorisation the following buttons are available to operate the system.
  - Alarms
  - Devices
  - System status
  - Logging (only available if the licence for Logging is activated).
  - Sent call
  - Start guard tour
- ▶ When selecting the pull down menu 'Admin user', menu 9 to configure the system becomes visible.

#### 8.6.1 Maximum logged on users

If the number of allowed simultaneous logged on users is exceeded, then the oldest, not active user, is logged out automatically.



**i** Note: If needed, increase the Multi User Licence to prevent this.

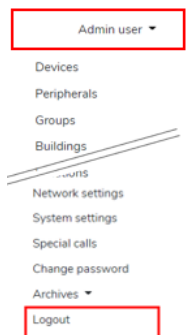
#### 8.6.2 Auto Log of

A user is automatically logged of, in situations that:

- ▶ The maximum log on time of 1 hour is expired.
  - To prevent this, check the 'Remember me' box during "Log in".
- ▶ If, another user logs in while using the same credentials.
  - To prevent this user unique credentials per user.
- ▶ If another user tries to log on with unique credentials.
  - Another user with the lowest activity will be logged out automatically.
  - To prevent this apply for extended multi user licences.

athena.demo:8081 meldt het volgende

This page has expired due to inactivity. Would you like to refresh the page?



### 8.7 Log out

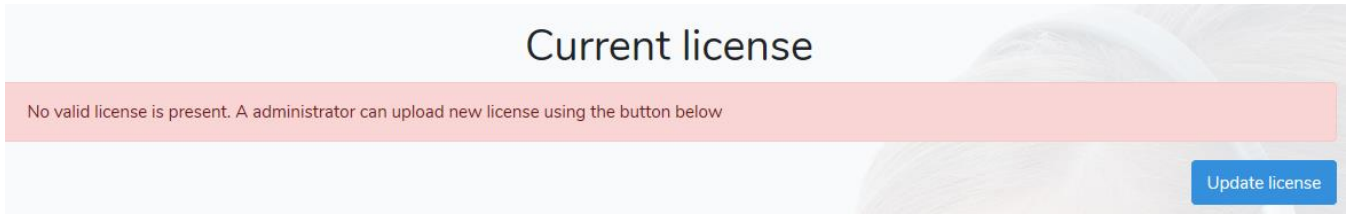
- ▶ Select in the pull down menu 8 the 'Logout' option.





## 9 System Licenses

The first time you logon, it is possible that no valid licenses are activated. The system will inform you in that case:



**i** Note: If the server cannot reach the DP6000-IP Interface where the licences are couple with, there is a notification that 'No valid licence is present'. So make sure that that unit is installed and IP-ready. Optionally reboot the software of the Communication server.

**i** Note: If no valid license file is present or if licences are not already distributed, inform with your commercial/technical contact to obtain such license file.

**i** Note: If a database back-up is made, be aware that the Licences are NOT included in the back-up.

### 9.1.1 Update the License file

A licence file can be supplied from USB stick, via E-mail etc. etc.

Make sure that the (new) license file can be found e.g. place on a stick or directory on your maintenance PC/Laptop.

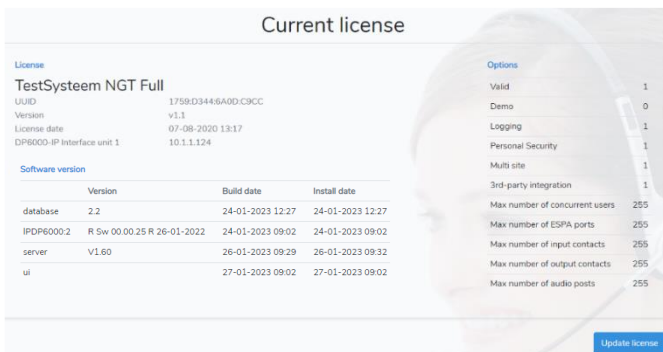
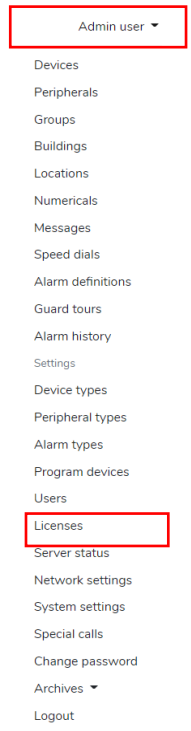
To update the licences:

- ▶ Store the received license file at a place where you can find it on your maintenance PC/laptop.
- ▶ Select the blue button 'Update License'.
- ▶ Mouse click in the space with the text 'Click or drag license'.
- ▶ Navigate to the place where you stored the license file.
- ▶ Select the license file and press the button 'Open'.
- ▶ After a few minutes the licences are validated.
- ▶ A screen like shown in the next chapter is displayed when finished.

### 9.1.2 Check present Licenses

Before starting programming, first check if all needed licences are present.

- ▶ If logged in with administrator rights, you can find in the pull down menu an option "Licences".
- ▶ If selected, all options (i.e. licences) are displayed.
- ▶ If there is a '0' the licence is not activated.



#### Short explanation:

- 'database' Database with programmed settings.
- 'IPDP6000-2' FW version loaded in "uP-Rigth".
- 'Server' Servers' application software version
- 'Ui' Software User interface.

In this example a maximum of possible licenses (Options) are activated.

**i** Note: If there is no valid license file, executing maintenance is not possible.





## 10 Working mode

The System is designed to handle several procedures in different working modes:

- ▶ Manned operation: An operator handles incoming Personal Security- and eventually Technical alarms.
- ▶ Un-manned operation: The entire alarm handling is without any intervention of an operator.
- ▶ Remote reset: When activated a mobiles' alarm can be reset without request from the central.

### 10.1 Manned operation mode

Manned operation mode means that a certain time is given to an operator to accept and handle an alarm.

- ▶ From the moment the operator accepts an alarm, he/she is responsible for correct alarm handling.
- ▶ If an alarm is active for a too long time, then if set; an automatically escalation flow to handle the alarm can be started.
- ▶ If the acceptance time is set very low, the system is assumed to work in "[Unmanned operation mode](#)".



Warning: Instruct the operator NOT to leave the alarm screen during Alarm handling, because this will lead to lack of focus when handling an Personal Security alarm.

### 10.2 Unmanned operation mode

Un-manned operation mode means that no operator is involved in the alarm handling.

- ▶ The system must be configured for correct alarm handling. Each alarm handling flow should start automatically.
- ▶ A logged-on client can always follow what happens of course.
- ▶ Set the time in the operators' reaction time e.g. to 1 second, to create the unmanned operation mode.
  - If the reaction time is expired, automatic follow-up actions (if programmed that way) are started.
  - Most of the technical alarms will be reset automatically when the root cause is solved.
  - Personal Security alarms can be reset by a "[Remote Reset](#)" procedure.

### 10.3 Remote Reset

The option 'Remote Reset' can be set in the system settings "[enable alarm reset in rack](#)" (0=disable, 1=enable)

If this setting is enabled, it allows mobile-users to reset the mobiles' Personal Security alarm without an operators' request.

- ▶ By placing the mobile in a storage rack (if set in the mobile's opcode).
- ▶ By sending a reset request from the PS-Pager via its user menu (if set in the mobile's opcode).
- ▶ If set in the system settings a PSu mobile can reset an alarm by pressing the red button a second time, refer to "[enable PSMicro alarm reset by device](#)".



Note: Make sure that the opcode settings in the mobile are set such that 'remote reset' is allowed.





### 11 System Configuration

A DP6000 system can work as stand-alone solution or as a part of a larger integrated system.

The very flexible software and hardware architecture enables the Communication Server to assign various equipment to a specific site or building. (Note: a 'site', 'sub-site', 'department' or 'building' are used in the same context in this chapter).

Therefore each system definition starts to arrange to which (sub-) system the equipment will be assigned to f.i.:

- ▶ Location transmitter
- ▶ Mobiles/Devices
- ▶ Peripheral Equipment; like the Server or DP6000 IP interface.
- ▶ Other peripherals like guarded system transmitters, guarded central receivers etc.
- ▶ External I/O contact devices.
- ▶ ESPA connections.

#### 11.1 Define a building

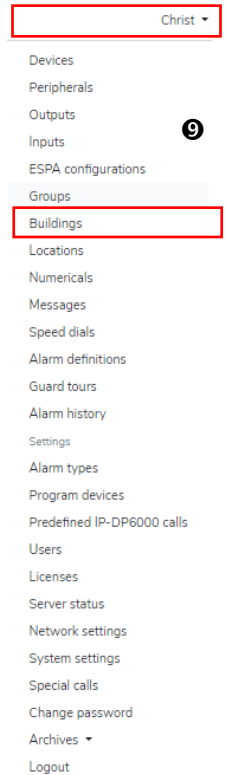
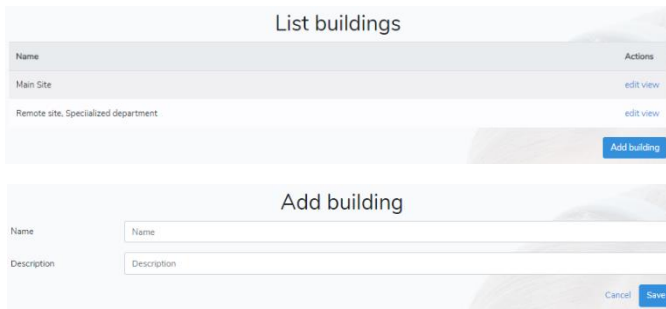
The system architecture is set up such that it always works per specific site, sub-site or a multisite Environment with more than one (group of) building(s).

Therefore the places (buildings) where the specific system-elements are installed, needs to be defined here.

If extra DP6000-IP Interfaces are added to serve other DP6000-subsystems, they can be linked to their own specific area/environment/site (building).

Advantages of such structure:

- ▶ In Multi-site applications, system alarms can be linked to a specific area/building only or to multiple sites.
- ▶ Mobiles and location transmitters can be assigned to a specific area/building.

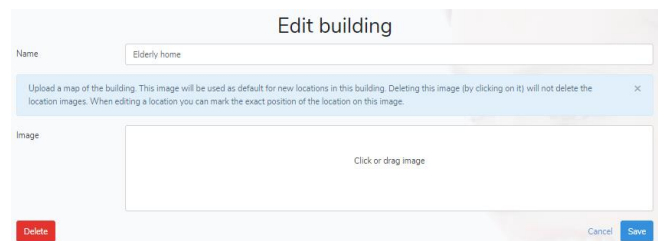


##### 11.1.1 Add a site/building

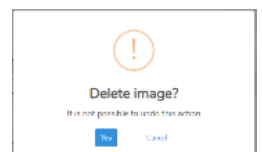
- ▶ Select the tab 'Buildings' 9 . This opens the list 'building menu'.
- ▶ Select your choice; to add or to edit a building.
- ▶ Name: Give a descriptive name to the building/site; e.g. a Company's Name, an Application, a Departments' name, a Building ID etc. etc.
- ▶ Description: If desired Fill in the description extra information for the building/site.
- ▶ Select the blue button 'Save' to store the setting.
- ▶ Add a drawing if desired.

##### 11.1.2 Add a drawing to the building

- ▶ Optionally one main-drawing per can be assigned when creating a building.
  - The drawing that is selected here, will be are Blanco location reference for this building.
  - The advantage, to add a drawing to a building, might ease the configuration of location beacons later.
  - Use a drawing without any location (Blanco) information here. Location information will be configured later as described in chapter "[Representation of location graphics](#)".
- ▶ Select the relevant building to add the drawing to, and select 'edit' .
  - When mouse-click in the area 'Click or drag image' offers the possibility to navigate and select the desired drawing.
  - Select 'Save' to store the changed settings.
- ▶ To delete a drawing:
  - Make sure that there are no locations assigned to the building!
  - Open the and click at the drawing, a choice to delete the image appears; select 'Yes' to confirm.
  - Select 'Save' to store the changed settings.



Note: At least 1 building MUST be configured in the system. Each DP6000-IP interface can cover only 1 physical site with multiple buildings of course.



Continue at next page: →



### 11.2 Location detection

Location information is used for several purposes:

- ▶ To locate peripheral equipment that have technical issues.
- ▶ To locate Personal Security devices/mobiles that are in alarm status.
- ▶ To perform a guard-tour.

The more detailed the location information is, the more accurate the place where help is sent to.

#### 11.2.1 Location monitoring option

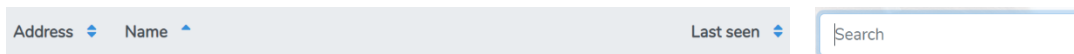
If desired, the functionality of the location beacons can be monitored. Depending on the used type location beacon, different methods are possible. For details refer to the chapter "Location Monitoring" in the chapter application notes.

### 11.3 Overview programmed locations

- ▶ When opening the 'locations' menu 9 the first time, a screen 'Add location' opens.
- ▶ If there are already location beacons programmed, a screen 'Overview locations' is opened.
  - The location overview shows information of the programmed location data (Building, Address, Name) and the last time that this location beacon was detected by the system (Last seen).

Building	Address	Name	Last seen	Actions
IPS 1	40000	Back door	29-06-2021 09:21:20	edit view
IPS 1	10000	Front Door	29-06-2021 09:21:20	edit view

#### 11.3.1 Sorted overview of location beacons



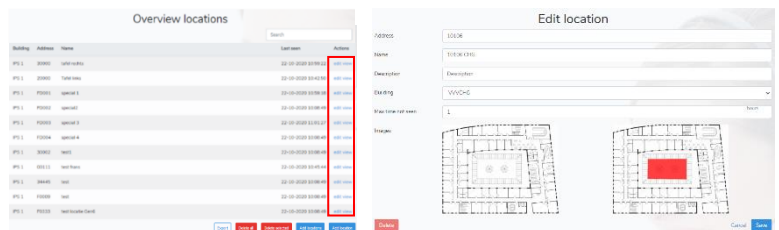
- ▶ The data can be sorted by using the arrows next to the Address, Name and Last seen label.
- ▶ The 'Search' field can be used to find locations with reference to buildings, addresses or names.

#### 11.3.2 View programmed Location beacons

- ▶ When selecting the 'view' option in the 'Overview locations' screen, all programmed details are displayed, the location beacons: name, address, assigned building and used drawings are summarised.

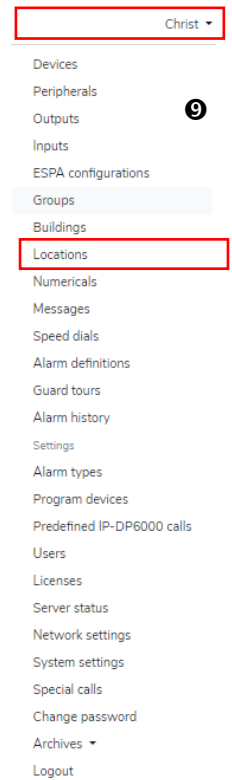
#### 11.3.3 Edit programmed Location beacons

- ▶ When selecting 'edit' option in the 'Overview locations' screen, all programmed details are displayed, the location beacons.
  - name, address, a description, assigned building and used drawings are displayed.
  - In addition to this, the programmed max. time not seen, setting is displayed also.
- ▶ Change the data as desired.
- ▶ Select Save to store the data.



#### 11.3.4 Guidelines to program Location data

- ▶ Give each location a unique address.
  - The 'name' of the location is later used in representations and/or when alarm calls are forwarded.
  - The advice is therefore to limit this name to a maximum of 24 characters.
  - Each location beacon is assigned to only one building/site.
  - In case of 'Multi-site', no double location addresses are allowed
  - The range of useable location addresses is 00000-FFFFF.
  - Location addresses started with 'F7' are used for diagnostic purposes by the DLT; LBB6071/00.
  - Locations starting with XF, XE, XD and X0-X7 are so called special locations used by mobiles.



Continue at next page: →



### 11.3.5 Add Location Beacon(s)

- ▶ The unique address of the location beacon can be programmed per location beacon.
  - In case multiple location beacons are programmed this data can be imported from an excel file.
- ▶ The name of the location beacon can be programmed per location beacon.
  - In case multiple location beacons are programmed this data can be imported from an excel file.
- ▶ Each location beacon must assigned to one specific building/site.
  - In case the data of multiple location beacons is imported via an excel file, all imported location beacons will be assigned to the same building/site and will have the same 'Max. Time not seen' value.
- ▶ One method to monitor location beacons is used to check periodically the location beacon's functionality by measuring a time-out. If desired, the time for 'Max. time not seen' can be filled in (hours).
  - For details refer to the chapter "[Location Monitoring](#)"
  - '0' means Location monitoring is disabled.

#### Add a single location beacon:

- ▶ Open the 'Locations' tab.
- ▶ Select the button 'Add Location'.
- ▶ Fill in the Address, Location's name, Description 'Building' and <sup>1)</sup> 'max time not seen' time in hours.
  - <sup>1)</sup> '0' means Location monitoring is disabled.
- ▶ Select 'Save' to store the settings.
- ▶ Configure the diagrams for graphical visualization.
  - See chapter "[Representation of location graphics](#)".

Add location


#### Add multiple location beacons:


- ▶ Create an excel file with two columns.
  - There may no header present, see example.
  - Store the file for later use.
  - Note that Excel normally removes leading zeros!
- ▶ Open the 'Locations' tab.
- ▶ Select the button 'Add Locations'.
- ▶ Fill in the 'Building' and 'Max time not seen' parameters.
  - '0' means Location monitoring is disabled.
- ▶ Click in the 'File' field, navigate to the place where the excel file stored and select that file to import.
- ▶ Once the import was error-free, select 'Save'.
- ▶ Configure the diagrams for graphical visualization for each location beacon.
  - See chapter "[Representation of location graphics](#)".

Add locations

	A	B
1	B0001	Corridor 1
2	B0002	Corridor 2
3	B0003	Corridor 3
4	B0004	Corridor 4
5	B0005	Corridor 5
6	B0006	Corridor 6
7	B0007	Corridor 7
8	B0008	Corridor 8
9	B0009	Corridor 9
10	B0010	Corridor 10

**TIP:** To prevent that Excel removes leading zeros, make sure that the cell properties, before(!) entering the data, are defined as 'TEXT'.

The green sign  (as warning for an error) in the upper left corner can be ignored.

 Note: Once location parameters are entered, the last step is to add diagrams for the graphical representation of the location in case an alarm occurs. This must be done per location beacon. Refer to "[Representation of location graphics](#)" for instructions.


### 11.3.6 Export location data

The programmed location data can be exported as CSV file.

- ▶ Open the 'Locations' tab.
- ▶ Select the Export button
- ▶ Navigate to the place to store the CSV file.
  - The name of the file is e.g. locations\_1669984515.csv

Export Delete selected Add locations Add location

Address	Name	Description	Building	Last seen	Max time not seen
20000	Table left		IPS 1	23-11-2022 11:49	1
FD001	special 1		IPS 1	29-11-2022 13:25	
10000	Front Door		IPS 2	23-11-2022 11:49	
40000	Back door		IPS 2	23-11-2022 13:26	
10106	10106 CHG		VVVCHG	23-11-2022 11:50	1

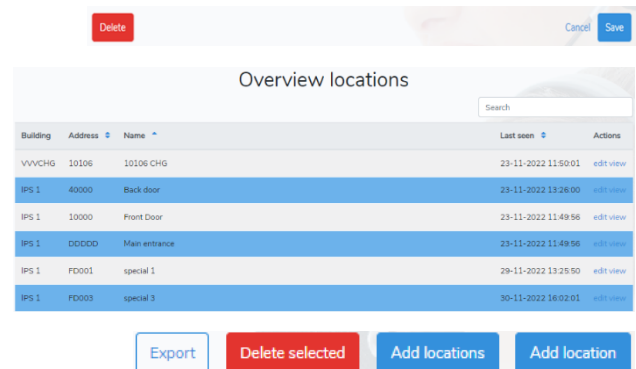
 Note: Reducing the exported file to only the 'Address' and 'Name' column and removing the header makes the file suitable to be used as file to be imported.

Continue at next page: →



11.3.7 Delete location beacon(s)

- ▶ To delete a single location beacon:
  - Open the 'Locations' tab.
  - Select the location beacon that you want to delete and select 'Edit'.
  - Select the RED 'Delete' button.
- ▶ To delete multiple location beacons:
  - Open the 'Locations' tab.
  - Select the beacons to be deleted <Ctrl+left mouse>
    - In this example indicated with a blue bar.
  - Select the RED 'Delete selected' button to delete the locations.

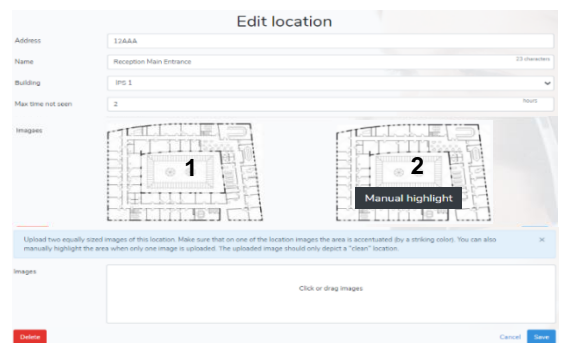


**i** Note: Programmed location beacons can NOT be removed as long as the beacon is coupled with:

- Alarm
- Peripheral
- Input contact

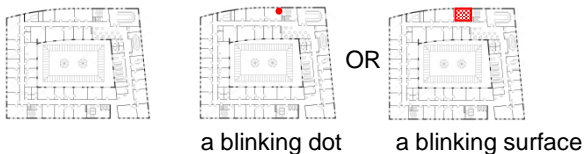
11.3.8 Representation of location graphics

- ▶ The graphical location representation is build up with 2 graphical files to indicate one position. This section describes how to make the graphical representation available in the system. There are 2 files needed to create the 'blinking behaviour' to indicate the place where an alarm occurs. In the description below 'Drawing 1', and 'Drawing 2' are used.
  - 'Drawing 1' is a drawing without coloured location indication.
  - 'Drawing 2' is a drawing that contains a coloured area to be coupled to a location beacon.



Examples;

The representation of locations can be made as sophisticated as you want, see the examples below.



Alternative representations can be created as wished

**i** Note: Location drawings are exported from the installers maintenance PC and imported to the server, therefore all location drawings can be showed to each logged in client.

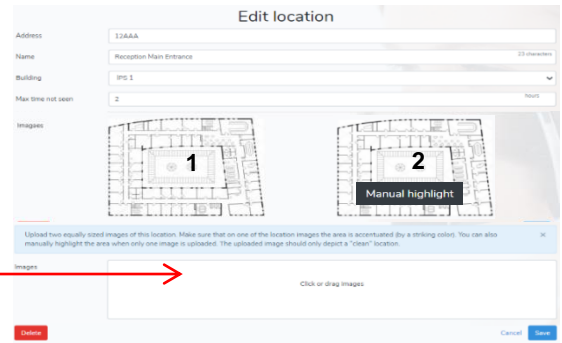
- ▶ Import 'Drawing 1':
  - If you already assigned a drawing to the building, see chapter "[Add a drawing to the building](#)", then 'Drawing 1' is made automatically visible, you can continue with 'Create Drawing 2.'
  - Importing a (new) file for 'Drawing 1' is only needed in case:
    - If no drawing was assigned to the building already. Refer to: "[Add a drawing to the building](#)".
    - If you are, for an individual location beacon, not satisfied to use the automatically generated 'Drawing 1'.
- ▶ To import a (new) 'Drawing 1':
  - If present, delete the 'proposed' Drawing 1.
  - Select the 'Images' field and navigate to the (new to be used as) 'Drawing 1'.
  - Continue with 'Create Drawing 2.'
- ▶ Create 'Drawing 2':
  - There are 2 methods to make the location area visible with 'Drawing 2'.
    - Import files modified with the paint tool (or equivalent).
    - Use the manual highlight tool.

Continue at next page: →



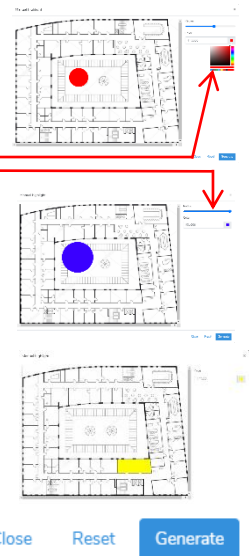


- ▶ Import files modified with a paint tool (or equivalent).
  - Before importing such files, some preparation is needed.
  - Such modified drawing is needed for each location and can cost some preparation time.
    - Modify the desired drawing such the it represents the desired location area e.g. using a program PAINT ore an equivalent tool.
    - Store the file in a directory where you can find it.
  - As soon 'Drawing 1' is visible, a copy of it is also visible as 'Drawing 2' together with a text 'Manual highlight'.
  - Below 'Drawing 1' there is an 'images' field.
  - Click the 'Images field' to navigate to the prepared file to be used for 'Drawing 2'.
  - Import the desired drawing.
  - Select 'Save' to store the settings.



To use the 'Manual highlight' option to create 'Drawing 2',

- ▶ Use the 'Manual highlight' tool for 'Drawing 2'.
  - As soon 'Drawing 1' is visible, a copy of it is also visible as 'Drawing 2' together with a text 'Manual highlight'.
  - If you click the 'Manual highlight' option, you are able to indicate manually an area that corresponds with the location beacon.
  - The colour of this location area indicator can be set via the colour pallet.
  - A single click at the drawing will set a 'dot' at the drawing.
    - With the slider 'Radius' the radius of the dot can be set.



- To draw a square-, parallelogram- or triangular- shaped area, just click subsequent at the corners of the area to be defined. See the example at the right in yellow.
- When finished select the blue 'Generate' button.
  - Whitin in a few seconds both drawings 'Drawing 1' and 'Drawing 2' will be assigned to the relevant location address.
- Other buttons at the 'Manual highlight' screen:
  - If you made a mistake select the 'Reset' button and redo the action.
  - If you want to cancel the 'Manual highlight' function, select the 'Close' button.

**i** Note: Location drawings are imported from the installers maintenance PC in to the server, therefore all location drawings can be showed to each logged in client.

### 11.3.9 Drawing quality:

- ▶ The sizes of each drawing is limited to 10Mbyte, which is shown as one picture.
- ▶ Drawings of the following formats are supported: JPG and PNG.
- ▶ The resolution or detail level is determined by the information that is in such file.

**i** Note: We recommend to place always a location transmitter close to the PS Pagers charge racks.

### 11.3.10 Location monitoring option

If desired, the functionality of the location beacons can be guarded. Depending on the used type location beacon, different methods are possible. For details refer to the chapter ["Location Monitoring"](#).

### 11.3.11 Guard tour option

To create Guard tours, refer to chapter ["Guard tours"](#).



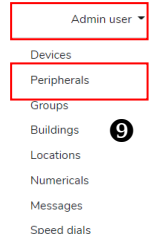


### 11.4 Define peripherals

Each type of peripheral equipment has its own options to be set individually.

At this moment the following Peripheral types are relevant:

- ▶ Ip 2 dp6000: DP6000-IP Interface(s)
- ▶ Server: Communication Server
- ▶ DP6000 RX: Central receivers like LBB6017
- ▶ DP6000 TX: Central transmitters with TMM module



#### 11.4.1 Add a Peripheral

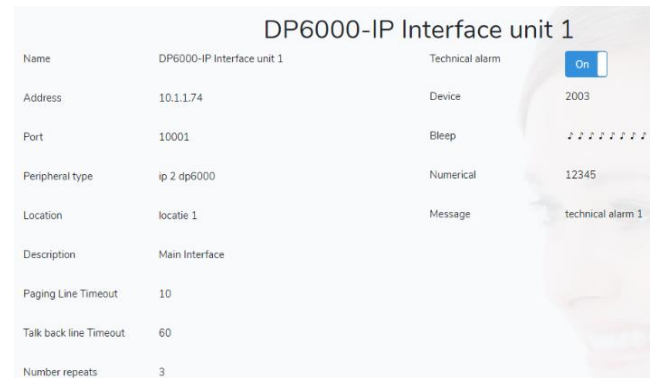
- ▶ Go to 'Peripherals' ⑨, an overview screen opens.
  - After selecting 'Peripherals' there are choices to select to 'view', to 'edit' or to 'add' a peripheral.
- ▶ Select the blue button: 'Add peripheral'.
- ▶ Name: Give the peripheral a prescriptive name.
- ▶ Peripheral type: Select the desired peripheral type:
  - "DP6000 TX", to add a system transmitter
  - "DP6000 RX", to add a system receiver
  - "ip 2 DP6000", to add a DP6000-IP Interface
  - "Server", to add an Communication Server
- ▶ Follow the instructions for the relevant type further in this manual.



#### 11.4.2 To view peripheral settings

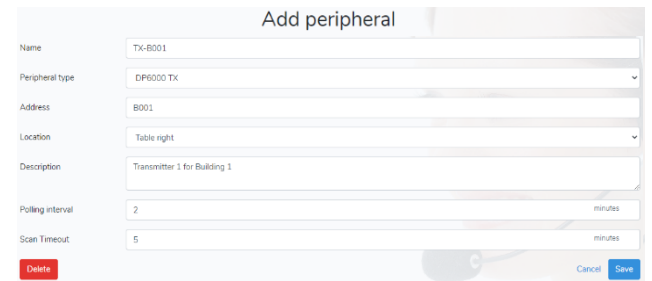
An administrator can view the peripheral settings;

- ▶ Select the 'view' option.
  - In this example the settings of an DP6000-IP interface unit is displayed.



#### 11.4.3 Configure Transmitter DP6000 TX

- ▶ Add this type of peripheral only if you want to use the option 'Transmitter monitoring' in the system.
- ▶ Each transmitter to be monitored must be added as separate peripheral.
  - Name; Give a unique Name; this name is later used in representations and/or transmitter error calls are forwarded.
    - The advice is therefore to limit this name to a maximum of 12 characters, or write e.g. TX-B001, TX-B002 etc.
  - Peripheral type; DP6000 TX.
  - Address; Give each Transmitter an unique address; Addresses starts always start with **B0!** (range is B001-B099).
  - Location; Select 'No Location' or select a (fictive) location where the unit is installed, this location information comes with an error call in case of technical issues.
  - Description; To give extra information regarding this unit.
  - Polling interval; This is the time in minutes that the system transmitter is polled by the system. (0 = disable, 255 = 255min).
  - Scan time out; The time in which a polling-reply from the transmitter is expected, if this time is expired, a technical alarm is raised to indicate that there might a technical problem with the transmitter.



**i** Note: Make sure that the transmitter monitor PCB that is built-in in the transmitter is configured well. For details refer to the application notes, chapter "[Transmitter monitoring via the Server](#)".

**i** Note: Transmitter monitoring is activated while the 'Polling interval' is set unequal to '0'. A 'Default Technical Alarm' occurs when no reply to a polling request is received in time. If a specified 'Transmitter alarm' is desired, the tab "[Define Specified Alarms](#)" offers the option to create a for example a specified 'Transmitter alarm'.



11.4.4 Configure DP6000 RX

- ▶ Add this type of peripheral only if you want to use the option 'Receiver monitoring' in the system.
- ▶ Each Central Receiver (LBB6017) to be monitored must be added as separate peripheral.
  - Name; Give a unique Name; this name is later used in representations and/or when alarm calls are forwarded.
    - The advice is therefore to limit this name to a maximum of 12 characters, or write e.g. CRX-B101, CRX-B102 etc.
  - Peripheral type; DP6000 RX.
  - Address; Give each Receiver an unique address; Addresses must always start with **B1!** (range B101-B199).
  - Location; Select 'No Location' or a (fictive) location where the unit is installed, this location information comes with a technical alarm call in case of technical issues.
  - Description; To give extra information regarding this unit.
  - Scan time out; The time in which a status call from the Central receiver is expected, if this time is expired a technical alarm is raised to indicate that there might a technical problem with the Central receiver. (0 = disable, 255 = 255min).

**i** Note: Make sure that the status call options in the Central receiver are configured well, especial the timing in the central receiver and the 'scan timeout' must be related with each other. For details refer to chapter "[CRX monitoring via the Server](#)".

**i** Note: Receiver monitoring is activated while the 'Scan time out' is set unequal to '0'. A Default Technical Alarm appears when there is no status call is received within in the programmed Scan timeout or when a Central receiver reports an error by itself. If specified 'Receiver alarms' are desired, the tab "[Define Specified Alarms](#)" offers the option to create a specified 'Receiver alarm'.

11.4.5 Configure a DP6000-IP Interface

- ▶ Each DP6000-IP Interface acts as an individual call encoder for a DP6000 system, it can be set-up as a single site-, a multi-site system or as redundant unit.
  - ▶ Be aware that the functions of each DP6000-IP Interface can be guarded, for details refer to chapter: "[Monitoring the DP6000-IP Interface](#)".
  - ▶ By default one DP6000-IP Interface is pre-installed already, details can be added or changed via the Admin user menu and the option 'Peripherals'.
  - ▶ With the option 'Add peripheral', extra units (in case of multi-site/redundancy) can be added.
    - Select via the Admin User menu the Peripherals option.
    - When already peripheral equipment is programmed, an overview will be displayed
  - ▶ Select the button 'Edit' next to the relevant unit, or when you want to add a unit, the blue 'Add peripheral' button.
- 
- ▶ Name: Give each unit it a useful name, e.g. the building/site that it covers.
  - ▶ Peripheral type: Select 'ip 2 dp 6000', which represents a DP6000-IP Interface.
  - ▶ Address: The individual IP-address must be filled in, this must be a static IP-address while it is controlled through IP-port 'Network 1' from the Communication Server. By default all units uses the IP address range 192.168.1.20.....21....22.
    - If desired, change the IP address in another preferred range.
  - ▶ Port: Fill in the Port number; this is a static IP port number for all DP6000-IP interfaces: value = 10001.
  - ▶ Poll watch alarm: To set the time that the DP6000-IP Interface should expect a 'Ping' from the Communication server.
    - ▶ Guarding of the IP-connection takes place at the Server side and at the DP6000-IP-Interfaces-side.
    - ▶ For details also refer to chapter "[Lost IP connection](#)".
      - In this example: If no 'Ping' from the Communication Server is received in time (30s), the alarm process at the DP6000-IP Interface side is activated.
        - Alarm activation implies; If selected, a 'predefined call on connection error' which is described at next page and Re1 on the DP6000-IP Interface, that becomes activated.
        - If the Poll watch alarm is set to '0' no guarding by DP6000-IP Interface takes place.
  - ▶ Poll watch alarm repeat: In this example; The poll watch alarm is activated each 255 seconds as long as it is not solved.
    - If the number Poll watch alarm repeats is set to '0', no repeated alarms will be generated.

Continue at next page: →



- ▶ **Location:** Select 'No location' or a (fictive) location where the unit is installed, this location information comes with an alarm call in case of technical issues etc.
- ▶ **Free description:** To give extra information regarding this unit.
- ▶ **Paging Line timeout:** This sets the max. time that the paging line may be occupied at code level (0V).
- Normally a max time of 10s will be sufficient.
  - Exceeding this occupation time can be an indication of a defect.
  - For details, refer to chapter ["Line occupation error"](#).
- ▶ **Talk back line Timeout:** This sets the max. time that the Talk-Back line can be occupied by a Central Receiver.
- Normally a max. time of 60s is sufficient.
  - Exceeding this occupation time can be an indication of a defect.
  - For details, refer to chapter ["Line occupation error"](#).
- ▶ **Number of repeats:** This sets the number of repeated data in each paging call that is sent by the system.
- It can help to improve the number of successful calls for areas with some poorer transmitter coverage.
  - Note that this setting has impact on the system speed.
  - A normal value to be set is between 1-3.
  - If a setting higher than 5 is needed, additional measures (coverage) to secure arrival of paging calls might be necessary.
- ▶ **Encoder priority level:** This sets a delay-time in steps of 35mS.
- The encoder priority level prevents that the multiple encoders can set -up simultaneously calls at the paging lines, which might lead to corrupted data/missed calls.
  - It must always be set in case there are more encoders connected to the same DP-bus.
  - If there no other encoder in the system than set this value to '1'.
  - Priority 0, is the highest system priority (0mS delay), Priority 15 is the lowest system priority.
  - Examples of encoders are products which are able to set code at the paging lines.
    - Telephone coupler
    - Transmitter monitor unit
    - DP6000-IP Interface
    - Alpha desk
- ▶ **Enable sequence:** The sequence function enables to control the transmit function in multi-site systems.
- Each DP6000-IP-Interface receives a message after different delay times.
  - The result is that the transmitters connected with that specific DP6000-IP Interface, sent the messages after that delay.
  - Note that not the transmitters are sequenced, only the DP6000-IP-Interfaces are sequenced.
  - This application is useful in multisite systems where the risk is present that data can be corrupted while transmitters from different DP6000-IP Interfaces have an overlap in their covered areas.
  - The delay time can be set via the 'System settings'; ["Sequencing delay"](#).
    - The exact timing must be tested, for an average alphanumeric call of 24 characters a sequencing delay time of 1200ms is sufficient. (While such call handling takes approx. 1200ms).
  - If the described coverage overlap is NOT applicable just set the slide to 'Off'.
- ▶ **Predefined call on connection error;** Here the ["predefined-IP-DP6000 call"](#) can be selected that should be sent automatically by the DP6000-IP Interface in case the IP-connection with the Communication Server is lost.
- If the Poll watch alarm is set to '0' no IP-Connection monitoring by the DP6000-IP Interface takes place thus the predefined message will not be sent in that case.

Location	Table right
Description	dp-ig unit as installed at the server room

Paging Line Timeout	10	seconds
Talk back line Timeout	60	seconds

Number repeats	1
Encoder level priority	0

Enable sequence	<input type="checkbox"/> Off
-----------------	------------------------------

Continue at next page: →





### 11.5 Monitoring the DP6000-IP Interface

Each DP6000-IP Interface can be programmed with its own individual settings that define if/how to react in case of error.

Monitored functions for the DP6000-IP interface are:

- ▶ Paging line occupation: For details refer to the settings 'Paging Line Timeout' as described at the previous page.
- ▶ Talk-back line occupation: For details refer to the settings 'Talk back line Timeout' as described at the previous page.
- ▶ Lost IP connection: For details refer to chapter ["Lost IP connection"](#)
- ▶ ESPA ports: For details refer to chapter ["Monitoring ESPA Ports"](#)
- ▶ RS485 Port: For details refer to chapter ["Monitoring RS485 connection"](#)
- ▶ Internal Input contacts For details refer to chapter ["Input guarded"](#)

#### 11.5.1 Line occupation error

A too long occupied Paging line or Talk-back line can indicate to a potentially defect or unintended use.

If this occurs a default Technical alarm is raised.

In case one of the predefined occupation times are exceeded a Default Technical alarm will arise.



Note: A 'Default Technical Alarm' is raised while one of the 'Line occupation times' is expired.

If a specified 'Line occupation time' alarm is desired, the tab ["Define Specified Alarms"](#) offers the option to create 3 different specified 'Line occupation time' alarms;

- A 'Technical DP\_LF' to monitor the Paging lines.
- A 'Technical DP\_TB' to monitor the TB lines.
- A 'Technical error LF/TB' alarm To monitor both lines at the same time; combined function.

#### 11.5.2 Lost IP connection

- ▶ Monitoring of the IP connection between Communication server and DP6000-IP Interface takes place at the Server side and at the DP6000-IP-Interfaces-side. Therefore, next to the settings 'Poll watch alarm' and 'Poll watch alarm repeat' that can be set to trigger the alarm process at the DP6000-IP Interface, the Communication Server can be configured also to detect a lost IP connection to generate a technical alarm.

- Be aware that the server cannot sent calls via a lost IP connection.
- If programmed during the ["Configure a DP6000-IP Interface"](#) process an automatic call is sent by the DP6000-IP Interface.
- When the IP connection is lost, a 'Default Technical alarm' becomes active.
- In the Systems Settings some additional settings can be set for actions to be taken by the Communication Server:
  - [ip connection error initial timeout.](#)
    - With this setting, the time is set in which the Communication Server expects a reply to a 'Ping' request.
    - If the reply time is exceeded, then the Communication Server generates a technical alarm due to a lost IP connection.
    - This time must be set lower than the 'poll watch alarm' than set in e.g. DP6000-IP-Interface settings.

##### [ip connection error repeated timeout.](#)

- An operator can reset a technical alarm temporarily, as long as the IP-lost problem is not solved, the technical alarm is repeated each time as set here.



Note: A 'Default technical alarm' is generated by the Communication Server, when there is no reply to a 'ping' is received in time. If a 'Specified IP Lost' alarm is desired, the tab ["Define Specified Alarms"](#) offers the option to create a 'Specified Technical IP' alarm.

#### 11.5.3 Sent an automatic message when IP connection is lost

To create an automatic message to be sent in case the IP connection between the Communication server and DP6000-IP Interface is lost, refer to ["Predefined IP-DP6000 calls"](#).





### 11.6 Configure a Communication Server

#### 11.6.1 Configure the main server

By default the main Communication Server is already pre-installed, however some specific details can be changed to customised values.

**Note:** The Communication Server is already preconfigured, as described in the explanation below some settings are free to be changed, for the rest we recommend not to change other settings unless you are advised to do so.

- ▶ Open the tab 'Peripherals', and find Peripheral type 'Server' with the Name 'Main server'

Address	Name	Peripheral type	Status	Actions
localhost	Main Server	server	Ok	<a href="#">edit view</a>
10.1.1.74	DP6000-IP Interface unit 1	ip 2 dp6000	Ok	<a href="#">edit view</a>

- ▶ Select the button 'edit' or 'view' if you only want check settings.
- ▶ It is NOT allowed to change the Name.
- ▶ The Peripheral type is 'server'; Usually there is only 1 'server' in the system, unless there is a master/slave set-up.
  - It is not allowed to change it.
- ▶ The default IP-address is set as 'local host' this is to secure correct communication in the system.
  - It is not allowed to change here.
  - If needed to change the Network settings for the Communication Server, refer to the chapter "[Network settings](#)".
- ▶ The standard port number is TCP-port: is filled in here.
  - It is not allowed to change it.
- ▶ If desired, a (fictive) location can be given, such is useable for later alarming in case of technical issues.
- ▶ Free description.
- ▶ The standard setting for Master/Slave is '0'. (0 = Master).
  - **Don't change it!** Unless there are multiple Communication Servers in one system.
  - This settings is reserved for redundancy options, for details to set-up a master/slave configuration refer to Application notes: "[Server as Master/Slave](#)".
- ▶ Select 'Save' when finished.
- ▶ For technical alarms see chapter "[Database errors from Server](#)" and "[IP connection lost from Server](#)".

#### 11.6.2 Database errors from Server

Next to several technical alarms which can be generated by the system, the Communication Server will automatically generate automatically a hard-coded 'Default technical alarm in 2 specific error situations. Both alarms are an high level alarm.

##### Technical alarm (database read error)

- In case the Communication Server cannot read the data in the data base, a Default technical alarm is generated.
- A database read error can occur e.g. when the database is corrupt or when a programming fault is made.
- To trace back in the system status logging, check on a message 'Database read error'.

##### Technical alarm 2 (No database access)

- ▶ This type of alarm is used as high level alarm, it works as follows:
  - In case the Communication Server cannot access the data base, a Default technical alarm is generated.
  - To trace back in the system status logging, check on a message 'No database access'.

**Note:** In order to be able to detect both errors we recommend to configure at least one Default technical alarm in the system!!!

#### 11.6.3 IP connection lost from Server

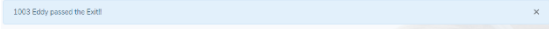


In case the Communication Server loses the IP connection with a peripheral (e.g. an DP6000-IP Interface), a technical alarm is displayed in the Alarm- and System Status- screen. It is hardcoded to activate a technical alarm in such cases, it is not needed to configure. Besides this, a lost IP connection is also signaled by the peripheral that communicates with the relevant Communication Server.



### 11.7 Notifications

Some system events will not cause an alarm. Instead of this, it can be set if a 'Notification' at the operators screen should appear. The background colour of the displayed notification indicates the urgency; Info, Warning or Critical.

- ▶ If a notification appears, it gives also a sound like 'Pong', in the System settings the "[pong\\_on\\_notification](#)" can be set: enabled =1, disabled = 0.
- ▶ Notifications are only displayed if an operator is logged in or will be logged in within the 'Display time out'. It means: That only operators can see it if the time between 'cause' and 'Display time out' is not expired.
- ▶ A notification can be 'removed' from the screen by an operator. Just click on the 'x'.

Notification type:	Colour:	Example:	Display time out:
Info:	Blue		5 minutes
Warning:	Yellow		30 minutes
Critical:	Rose		60 minutes

A notification is initiated by the system or when the system detect specific data in a call.


This can be a complete call or only parts of a certain call. Notifications can be caused by several initiators or events in the system e.g.:

- ▶ Mobiles (e.g. low battery, failed out-rack tests)
- ▶ ESPA port; in case specific incoming data is detected.
- ▶ Input contacts; The call that should appear is defined when programming the input contact.
- ▶ System receiver; status reporting (CRX)
- ▶ System transmitter; (if a transmitter monitoring unit is installed).
- ▶ When specific location beacon is passed (The PS-mobile transmits specific numeric code then).
- ▶ If a reset request (in case of alarm) is refused by a mobiles' user.



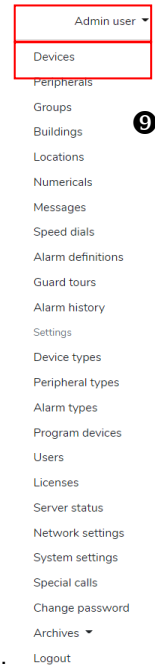
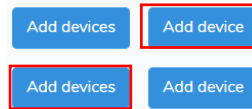


### 11.8 Assign mobiles to the system

- ▶ Select via the Admin User option  the Devices option.
- ▶ If there are already devices programmed, an overview will be displayed.

There are 2 ways to assign mobiles to the system:


- To add an individual mobile to the system:  
Use the button 'Add device'.
- To add multiple mobiles by importing them from an excel file:  
Use the button: 'Add devices'.  
For details refer to chapter ["Import multiple mobiles"](#).



### 11.9 Add an individual mobile

- ▶ Select the blue 'Add device' button and fill in the required settings.

- ▶ Address: This is the 1<sup>st</sup> individual address of the mobile.
- ▶ Name: Fill in a users' name or a departments name, usually this name is also programmed in the mobile.
- ▶ Function: Optionally fill in the 'Function' of the mobiles' user. (not mandatory).
  - This is an extra 'label' which can ease to find people that work in the same field to send a call to.
  - If you make a manual call and fill in at the 'Recipient field' the name of the specified 'Function', all recipients with the same specified function (label) become visible/available.
  - It is also possible to include or just to exclude visibility of people in logged data.
- ▶ Type: This is the type of device to be selected.
  - Gen IV pager; This type of mobile can only receive calls from the system.
  - PS-pager; This type of mobile can sent calls to- and receive calls from- the system.
  - PS-Micro; This type of mobile can only sent calls to the system.
  - Group address; This is the same group address (one or more) that is programmed in mobiles.

 Note: \* Depending on the selected type, more or less of the below listed options can be selected.

#### 11.9.1 Absent handling \*

- The 'Absent-handling' for calls that are sent to mobiles that are stored in an 'absent-rack' can be configured in several ways:
- ▶ The setting 'Absent forwarding'; enables in case an individual mobile is 'Absent' to forward the call to an alternative mobile
    - If set to 'On', the individual address of an alternative mobile can be filled in, to which the paging call (in case of absent) is redirected to.
    - Transferring calls to the alternative pager ends, once the original (PS) pager is no longer absent. (out rack).
  - ▶ If desired an option can be set is to decide if calls will be sent to mobiles (anyway) for which the server knows that they are stored in an 'absent-rack'.
    - This option is available in the system settings; refer to ["sent calls when absent"](#).

Continue at next page: →

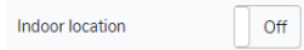




- If set to '1', calls are sent to mobile-users that are 'absent', so they can see if/which messages were received during their absence.
- If set to '0' (default setting) there are no calls sent to 'absent' mobiles, which limits eventually the system load.
- ▶ If desired an notification can be displayed in case a mobile is called when stored in an 'absent-rack'.
  - This option is available in the system settings; refer to ["sent notification on absent"](#).
  - If set to '1', a notification appears at the operators' screen if calls are sent to mobile-users that are 'absent', so they extra attention is given if/which messages sent to an 'absent' mobile.
  - If set to '0' (default setting) there are no notification appears.

### 11.9.2 Indoor location detection \*

- ▶ This setting is to inform the system that from this device (indoor) location information can be expected.

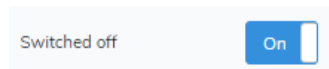


- Set this option to 'ON' when in the mobiles' opcode the option 'location detection' is enabled.
- For Gen. IV Pagers keep this setting to 'OFF'.

### 11.9.3 Switched off \*

This option is used to disable or enable the mobile for the system.

It can be useful during pre-installation preparations. Mobiles can be already programmed in the system but are not active in the system.

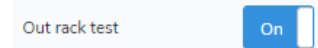


Another way to use it if the mobile is (temporarily) taken away because it no longer available.

- ▶ If set to 'On' the system will handle the mobile as 'not programmed' or 'not known' by the system. The system will reject all functions related to this mobile.
- ▶ If set to 'Off' the system will activate the mobile such that it is known by the system.

### 11.9.4 Out Rack test \*

- ▶ In the configuration for the PS-Pagers (devices) there is the option to set 'Out rack test' to 'On or 'Off'. See picture at the right.
- ▶ If set to 'On' a ["Notification"](#) is displayed at the operator's screen in case a mobile causes a failed out rack test.
- ▶ A failed out-rack test is caused when a mobile user cannot perform a correct functional test when a mobile is taken from an absent rack.
- ▶ If the Out Rack Test is not executed well:
  - The mobile starts to bleep until it is placed back in the absent-rack again.
  - A Notification appears at the top of the screen to inform the operator screen, see the example below.
  - Once the operator has taken the appropriate actions he/she can click at 'x' to remove the message.



Out rack test failed on pager 2201!



### 11.9.5 Low battery Indication \*

- ▶ If set in the mobile's opcode, a 'low-battery indication' is sent from the mobile to the system when the battery load becomes too low. If the system receives such low-battery indication, the operator can be informed in different ways:
  - In the 'Devices-' and 'System status-' screen, via the Status indicator. For details refer to ["Visible data of a mobile/device"](#).
  - By means of a notification, displayed at the operators screen, see the example below.
    - The content and the type of the notification is hard-coded in the application software, refer to ["Notifications"](#).
    - The notification appears at the top of the screen to inform the operator, see the example below.
    - Once the operator hat taken the appropriate local actions he/she can click at 'x' to close the message.
  - If enabled in the system settings, by means of a technical alarm, instead of a notification.
    - To activate a technical alarm instead of a notification, go to 'System settings', ["technical alarm on lowbat"](#) (0=disable, 1= enable).
    - The technical 'low battery alarm' can be reset by the operator or by placing the mobile in an absent-rack.

Pager with address: 2201 has a low battery!



Note: In the system settings, it can be set if a 'low battery' should lead to a technical alarm or not. If desired the setting ["technical alarm on lowbat"](#) should be set to '1' to enable this feature. (0 = disable).

Continue at next page: →





### 11.9.6 Automatic Scanning \*

- ▶ If this option is set to 'On' the mobile is scanned automatically with a specified scan interval time.
- ▶ On system level the scan time is randomised within the scan-interval that is set.
- ▶ Set the Automatic scan interval time in minutes (5-240 minutes).

Automatic scanning	<input checked="" type="checkbox"/>
Scan interval	<input type="text" value="5"/> minutes
Wait for response	<input type="text" value="30"/> seconds

- ▶ In case no automatic response is received within the 'Wait for response' time from the mobile, the automatic scanning call will be repeated 2x before a 'Default technical alarm' will be activated.
- ▶ In the system settings it can be set if an operator is allowed or disallowed to (temporarily) switch On/Off the automatic scanning function of individual mobiles, for details refer to chapter "[How to switch ON or OFF automatic scanning](#)".
- ▶ In the system settings, several settings that have a relation with automatic scanning can be set. These settings works system wide and are applicable for each user. For explanations, refer to "[System settings related to automatic scanning](#)".

**i** Note: For gen. IV Pagers and/or PSu mobiles, automatic scanning can optionally be used to detect if the device is absent. i.e. if it is placed in a storage rack.  
For gen IV Pagers this can be used as extra feature, for PS $\mu$  mobiles it is meant as extra signalling option e.g. in case an 'in-rack' call through the air is missed.

**i** Note: A 'Default technical alarm' occurs when a mobile doesn't reply (in time) to an 'Automatic scanning' call. If a specified 'Auto scan error' alarm is desired, the tab "[alarm definitions](#)" offers the option to create a specified 'Auto scan error' alarm.

**i** Note: In systems that are used to comply with the Dutch NEN2575 normalisation, it is possible to monitor the charge racks for the gen. IV pagers. The scan function is then used in combination with the LBB5906/xx Control Rack. In this application the scan call is received, by a special Control Pager, through the air and the (absent) reply is detected through the Paging lines.

### 11.9.7 Sign of life (manual reply from mobile) \*

If this option is set to 'On' the mobiles' user must react manually to a Sign of Life call, e.g. pressing a button on the mobile.

When no response from the mobile is received (manual acknowledge) within the specified 'Manual reaction time', a 'Technical alarm' will be activated.

Sign of life	<input checked="" type="checkbox"/>
Manual reply ratio	<input type="text" value="10"/>
Manual reaction time	<input type="text" value="Manual reaction time"/> Seconds

- ▶ The ratio between automatic scanning-calls and the sign-of-life calls that requires a manual reply, can be programmed.  
Example: Imagine that the automatic scan time is set to 10 minutes and the manual scanning ratio is set to 5, than each 50 minutes a manual acknowledge from the mobiles' user is required.
- ▶ The manual reaction time in which the mobile's user must react to a Sign of life call, can be set in the range of 10s-120s. If no reaction call is received in this time, a 'Default Technical alarm' will be activated on the system.
- ▶ In case no manual acknowledge is desired, simply set the slider to 'OFF'.

**i** Note: A 'Default technical alarm' occurs when a mobile doesn't reply (in time) to a 'Sign of life' call. If a specified 'Sign of life alarm' is desired, the tab "[Define Specified Alarms](#)" offers the option to create a specified 'Manual scan error' alarm.

### 11.9.8 Sign of life (periodical call from PS-Micro mobile) \*

- ▶ In case the type of mobile is set to 'PS-Micro' (PS $\mu$ ), the function for the Sign of life' setting is different:

- When this option is set to 'ON' the system expects automatic calls from the PS-Micro mobile, within the 'Automatic reaction time'.
- When no 'Sign of life' call from the PS-Micro mobile is received within the specified 'Automatic reaction time', a 'Technical alarm' will be activated.

Sign of life	<input checked="" type="checkbox"/>
Automatic reaction time	<input type="text" value="10"/> Minutes

**i** ▶ Note: The 'Automatic reaction time' to be set is related with the settings of opcode 3 in the PS $\mu$  mobile. i.e. Check interval time and Call repetitions.

**i** ▶ Note: The **battery saving** option for Gen.IV pagers and PS-pagers is not supported with the Communication Server. Therefore this option must NOT be activated in the mobiles' opcode settings.





### 11.9.9 Link mobile to a Building/site \*


A mobile must be assigned to a one or more building(s), (sub-system(s) or site(s)), this can simply be the Main Site, a remote site or dedicated buildings from the (sub-) site.

- ▶ When mouse click in the white area, all earlier created buildings appear.
- ▶ Select the building(s) where the mobile needs to be assigned to. Building(s) are earlier created in the chapter [“Define a Building”](#).

### 11.10 Link a mobile to Peripherals (DP6000-IP Interfaces) \*

- ▶ There are 3 places to link a mobile to one or more DP6000-IP interfaces:
  - Main peripherals.
  - Back-up peripherals.
  - Scan peripherals.
- ▶ Each mobile must be linked to at least to one Main-, Backup- and Scan- peripheral.
- ▶ If per peripheral type more than one peripheral is selected, the sequence of the DP6000-IP interfaces to handle the action can be changed, by selecting the arrow up/down ↑↓ signs, see the example for 'Main peripherals' below:

- ▶ To remove a peripheral, select the 'Remove' button.

 **Note:** In some cases more than one Peripheral can be selected to create redundancy in the system. If this is possible depends on the type of device (mobile). Note that the use of multiple/different DP6000-IP Interfaces requires also a multisite licence.

#### 11.10.1 Link mobile to Main Peripheral(s) \*

- ▶ A mobile must be assigned to at least one DP6000-IP interface to handle all incoming and outgoing calls from the DP6000 infrastructure i.e. the DP6000 (sub-)system.
- ▶ It is possible to assign a mobile to more DP6000-IP interfaces (multisite), so paging calls can be distributed via more units if desired.
- ▶ When the mobile can only be in range of one (sub-)system, it is sufficient to select only 1 DP6000-IP interface.
  - Select the Main peripheral to assign the mobile to.
  - Select Add to confirm.

#### 11.10.2 Link mobile to Back-up Peripheral \*

- ▶ A Back-up peripheral is meant to be used as a redundant peripheral.
  - In case the Main Peripheral goes out of order e.g. due to a defect, the Communication Server switches automatically over to the Back-up DP6000-IP Interface.
  - In case you use the Back-up option, select the relevant DP6000-IP Interface to assign the mobile to.
  - Select Add to confirm.
- ▶ If no Back-up peripheral is installed as back-up, select the same DP6000-IP Interface as chosen for the Main Peripheral.

#### 11.10.3 Scan Peripheral \*

- ▶ A scan-peripheral is meant to be used to separate the regular system handling from the scanning handling.
  - In case you use separate DP6000-IP interface(s) to scan mobiles, select the relevant DP6000-IP Interface to assign the mobile to.
  - Select Add to confirm
- ▶ If no separate Scan peripheral(s) are installed, select the same DP6000-IP Interface as chosen for the Main Peripheral.



11.10.4 Import multiple mobiles \*

► Prepare the excel file to be imported. (\*.csv or \*.xlsx)

- Per device type, a separate file must be imported.
  - csv separated by ',';
  - xlsx separated by columns.
- All devices (mobiles) that are imported (per list) have the same system properties.

► The excel file has 2 or 3 columns:

- The first column (A) contains the device name (user name) of the mobiles.
- The second column (B) contains the 4 digit addresses of the mobiles. The addresses must be UNIQUE per device.
- Optionally The 3<sup>rd</sup> column (C) can contain the parameter for 'Function'. This is a not mandatory field that can also left empty.

► Note that Excel normally removes leading zeros!

► Select in the 'Overview devices screen' the button 'Add devices'.


► Set the system parameters:

- Select the device type.
- Set the (relevant) parameters for the mobile, absent forwarding, location detection, out-rack-test, scanning etc.
- Select The building(s) to assign the mobiles to.
- Select the Main- Backup- and Scan- peripheral(s) to assign the mobiles to. (For PSu mobiles only Scan peripheral).

► Select in the option 'File' (choose file) and navigate (Browse) to the place where the excel file is stored.

► Select (again) the button 'Add devices' to start the file import.

	A	B	C
1	CHG1	7501	Cardiac
2	CHG2	7502	Cardiac
3	CHG3	7503	Cardiac
4	CHG4	7504	Cardiac
5	CHG5	7505	Cardiac
6	CHG6	7506	Cardiac
7	CHG7	7507	Cardiac

**TIP:** To prevent that Excel removes leading zeros, make sure that the cell properties, before(!) entering the data, are defined as 'TEXT'. The green sign  (as warning for an error) in the upper left corner can be ignored.

	A	B	C
1	CHG1	0001	Cardiac
2	CHG2	0012	Cardiac
3	CHG3	0503	Cardiac
4	CHG4	7504	Cardiac
5	CHG5	7505	Cardiac
6	CHG6	7506	Cardiac
7	CHG7	7507	Cardiac

**i** Note: Note that all mobiles listed in the Excel file MUST be of the same type!! Create separate Excel files for different types of mobiles to be imported.

11.10.5 Export mobile data

The programmed data of mobiles can be exported as CSV file.

► Open the 'Devices' tab.

► Select the Export button

► Navigate to the place to store the CSV file.

- The name of the file is e.g. devices\_1669988216.csv

**i** Note: Reducing the exported file to only the 'Name', 'Address' and 'Function' columns and removing the header makes the file suitable to be used as file to be imported.

11.10.6 Delete mobiles/devices

► To delete a single mobile:

- Open the 'Devices' tab.
- Select the mobile/device that you want to delete and select 'Edit'.
- Select the RED 'Delete' button.

► To delete multiple Mobiles/devices:

- Open the 'Devices' tab.
- Select the mobiles/devices to be deleted <Ctrl+left mouse>
  - In this example indicated with a blue bar.
- Select the RED 'Delete selected' button to delete the locations.

**i** Note: Programmed mobiles can NOT be removed as long as it has an active alarm.





### 11.11 Device screen content (Mobiles)

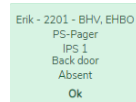
In the 'Device screen' the status of all assigned mobiles is displayed. By changing the system settings it can be decided if/which/how information is displayed and if operators are allowed to execute certain operations. This chapter describes the relevant items.

#### 11.11.1 Visible data of a device/mobile

In the Device- and the System status- screen the status of a mobile is made visible by means of a 'status indicator'.

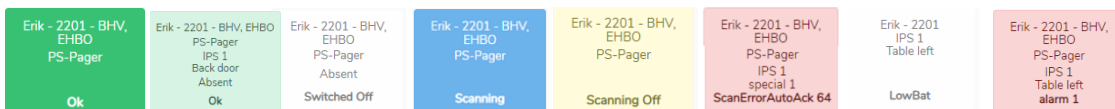
To define if/which data should be visible, refer to chapter ["Programmable info in the status indicator"](#).

- ▶ Name; This is name of the mobiles' user as described earlier in this chapter (e.g. Erik).
- ▶ Address; This is the 1<sup>st</sup> individual address of the mobiles as described earlier in this chapter (e.g. 2201)
- ▶ Function; This is an extra label assigned to the mobile as described earlier in this chapter (e.g. BHV, EHBO).
- ▶ Type; This is the type of mobile as described earlier in this chapter (e.g. PS-pager).
- ▶ Building; This is the site/building where the mobile is assigned to as described earlier in this chapter (e.g. IPS 1).
- ▶ Location; This is last known location of the mobile. Note that this is visible although the mobile is not in alarm (Back door).
- ▶ Status; This is the status of the mobile, see examples below. Different statuses have a specific text and colour.



Example: Status indicator

- OK
- Absent (or not)
- Switched Off
- Scanning
- Scanning Off
- Scan error
- Battery low
- Alarm

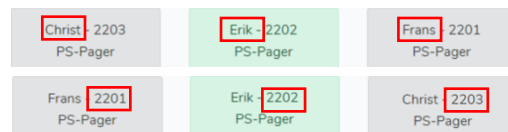


It is also possible for an operator to perform limited instructions via the status indicator, see ["Operation via the status indicator"](#).

#### 11.11.2 Sorted status overview

The visibility of mobiles in the Devices- or System status screen is ordered per building then, depending on the system settings, by: Alphabetic order or Numeric order.

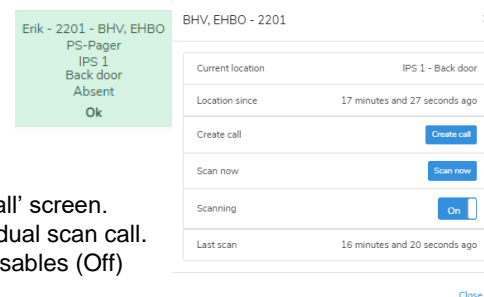
- ▶ Alphabetic order: The name of the devices, e.g. Christ, Erik, Frans.
- ▶ Numeric order: The addresses of the devices: e.g. 2201, 2202, 2203.
- ▶ To set alphabetic- or numeric order, refer to the System settings: ["order devices by"](#). (name = alphabetic order, address = numeric order).



#### 11.11.3 Operation via the status indicator

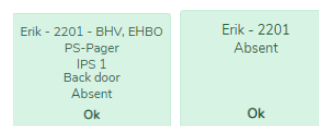
Next to the information in the status indicator, an operator is able to see mobiles' data and carry out some instructions when 'left-mouse click' at the status indicator:

- ▶ Left mouse click at the status indicator → A screen is opened:
- ▶ Visible data: (example):
  - 2201: The name and/or the address of the device/peripheral.
  - BHV, EHBO: This is an extra label assigned to the mobile.
  - Current Location: This is last known location of the mobile.
  - Location since: This is the time that the location is known.
  - Create call; By selecting this button an operator enters the 'Sent call' screen.
  - Scan now; By selecting this button an operator carry out an individual scan call.
  - Scanning; By selecting this button an operator enables (On) or disables (Off) the scanning function. For details refer to: ["How to set Scanning ON or Off"](#)
  - Last Scan; Shows the time that is passed since the last scan call.



#### 11.11.4 Programmable info in the status indicator

- ▶ In the previous chapter ["Visible data of a mobile/device"](#) several data in the status indicator is displayed.
- ▶ There might be several reasons to limit the visual data at the status indicator e.g.
  - Not relevant information is visible and one wishes to hide some items of it.
  - Some location information should not be visible when there is no active alarm.
  - Some functions should not be accessible to prevent unintended switching on/off.
  - See the examples at the right for an impression. →

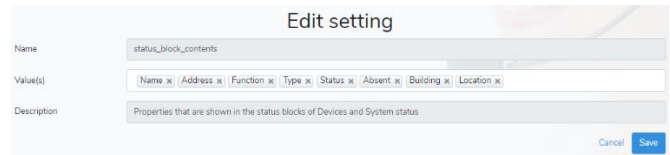



Go to next page to continue: →



Visible information in the status indicator

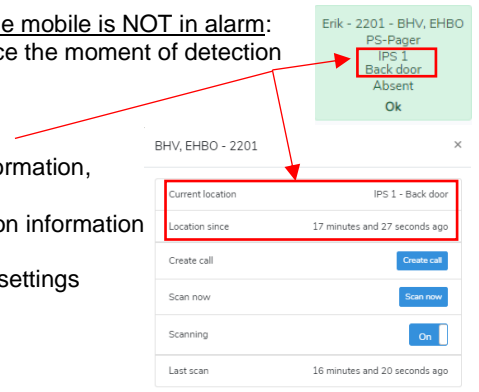
- ▶ To define the displayed data in the Status indicator, go to:
  - Systems settings: ["Status block contents"](#).
  - Select <Edit>.
- ▶ Select the information that is desired to be visible in the status indicator, for explanation refer to: ["Visible data of a device/mobile"](#)
- ▶ Note: in case location information must be hidden if the mobile is NOT in alarm, go to ["Hide location information"](#).
- ▶ Select 'Save' to store the settings.



 Note: The selected settings will influence the visible information for the mobiles' status indicators in both the Device- and System status- screen.

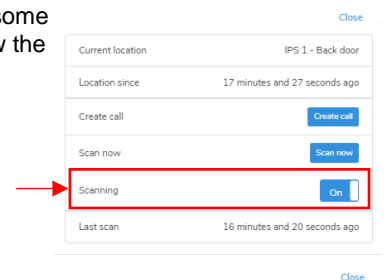
Hide location information

- ▶ For privacy reasons it might be required to hide location information in case the mobile is NOT in alarm:
- ▶ To set visibility of the current location information and the time that is past since the moment of detection is done at several places in the 'System settings'.
  - To enable or disable the visibility of the actual location information:
  - Go to the system settings, ["show device location"](#). 0=disable, 1=enable.
    - If this setting is set to '0', the operator cannot to see actual location information, unless there is a Personal Security alarm active.
    - If this setting is set to '1', the operator can always see the actual location information even there is NO Personal Security alarm active.
- ▶ If no location information may be seen at all, it can be disabled in the System settings ["Status block contents"](#).



11.11.5 Set Scanning ON or Off

- ▶ As described in chapter ["Operation via the status indicator"](#) an operator can carry out some operations after a left-mouse click at the status indicator. One of the options is to allow the operator to switch the scanning function per mobile (temporarily) 'On' or 'Off'.
  - The option to allow or disallow this, can be set in the system settings. refer to: ["enable scan off"](#).

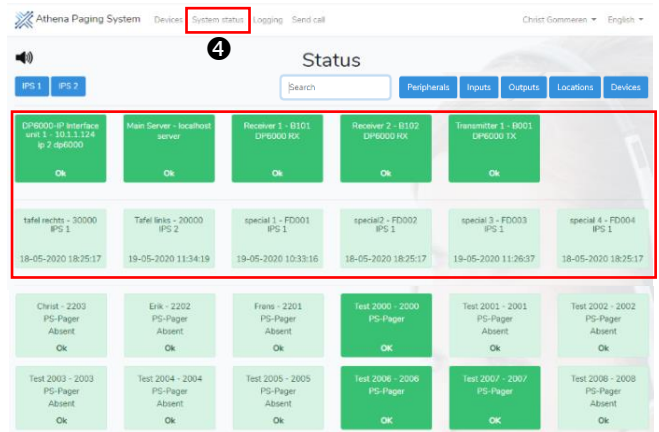




### 11.12 Status screen content

▶ If authorised an operator can open the 'System status' <sup>4</sup> screen.

- The status screen can show the technical status of all equipment in the system.
- The color and the text in the status indicator shows if the equipment is working well or not. See as example chapter "[Device screen content](#)" to have an impression.
- The status indicators are sorted per 'equipment' and per building.



▶ Selectable buildings

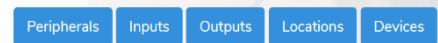
- In case a system is configured with multiple 'Buildings' The buildings where equipment is assigned to can be selected by using the blue 'building buttons'.
- In this example the system contains the buildings IPS1 and IPS2.



- The status of the equipment/mobiles is showed for each building where it is assigned to.

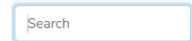
▶ Selectable equipment:

- Peripherals System equipment
- Inputs Input contacts
- Outputs Output contacts
- Locations Location beacons
- Devices Mobiles



▶ The equipment to view can be selected with the blue 'equipment buttons':

▶ With the search field a quick-search can be executed:



- To find f.i. the status indicator for 'Receiver 1' faster in the status screen:
- Make sure that the relevant equipment is enabled using the blue 'equipment buttons'
- Type 'Receiver 1' in the search field.



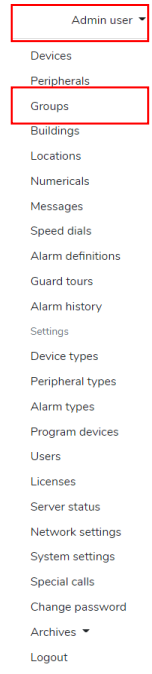
Note: All alarms are shown on the screen for authorised operators only.  
This offers the possibility to show technical alarms only to an operator that belongs to the technical department.



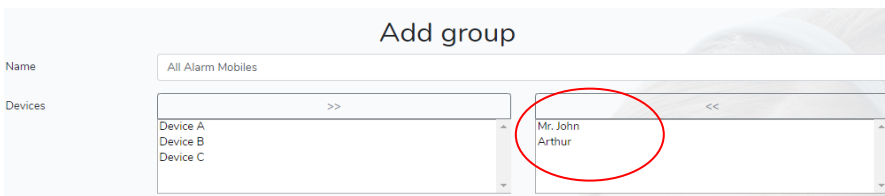


11.13 Groups of devices (serial call)

- ▶ When using this option to create a 'Group' it leads to a serial call. Each member (pager) of such 'Group' is called one by one using its individual address.
  - This is useful when a group of PS Pagers is called and they should give an automatic or manual acknowledge to indicate that a call was received.
  - When no acknowledge-, or absent- detection is required then the see next chapter to ["Create a Group Call"](#).
- ▶ Examples of applications are:
  - A group of PS Pagers that are called via their individual address, with the possibility (urgent call).
  - To require a manual acknowledge (manual reply) from each PS-Pager; some examples:
    - To create specific escalation groups so sent alarm calls that must be acknowledged with the mobile.
    - To create, in combination with specified alarms and/or specific locations, a specific 'Group' who can make an alarm.
  - With 'Groups' a form of location based services can be made: (examples:)
    - Only (specific) mobiles can make 'Specified PS-Alarms' if they are at certain locations/buildings and if they belong to a 'Group'.
- ▶ Status information from system-equipment in case a defect is detected, generate a technical alarm and one or more selective (group of) pager(s) is informed eventually in combination with a manual reply request.
- ▶ Examples of 'Groups' to be created are f.i.
  - 'All Alarm mobiles'. in case e.g. a specified Personal Security manual alarm is defined.
  - The same applies for pagers the should receive alarm calls; it can be useful to crate groups e.g.
    - A group 'help forces', 'technicians' or a group 'help in case specified manual alarm occurs' etc. etc. that will receive alarm calls and updates can be defined here too.



11.13.1 Create a Group of pagers (serial call)



**Note:** A Specified alarm from a mobile or system equipment is ignored (will not made visible) by the system if:

- The mobile is NOT, as a member of a group, coupled to an alarm definition.
- The mobile itself is not coupled to that alarm definition.

- ▶ Open the tab Groups
- ▶ Select the blue button 'Add group'.
- ▶ Give the group a best fitting name.
- ▶ Move the mobiles that should be part of the group from the left to the right part of the screen.
- ▶ Select the blue 'Save' button to store the settings.

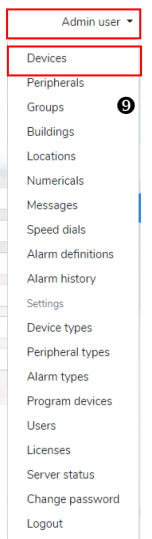
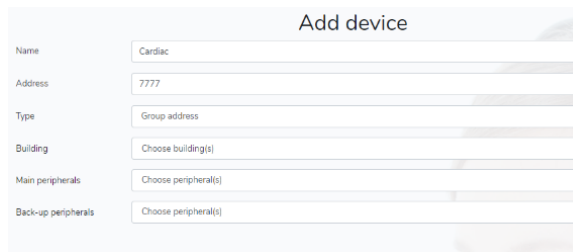
11.13.2 Create a Group Call (Group address)

Using this option, makes it possible to send calls to so called group-addresses of pagers, this option only sent one call to one address i.e. a group address that is also programmed in the relevant (PS-) pagers. There will be no signalisation if a call was received or not. The result is that all pagers, that have the group address programmed, will bleep if the call was received.

- ▶ No absent detection
- ▶ No automatic replies
- ▶ No registry in the system's logging of manual replies in the system.

▶ To create a Group address:

- Go to the option **Devices**.
- Click the button 'Add device'.
- The screen to configure a device will open.
  - Name: Give the Group a descriptive name.
  - Address: Fill in the Group address that is used to send the call to, e.g. 7777.
  - Type: Select 'Group address'.
  - Building: Assign the group to a site or Building.
  - Main Peripherals: Assign the group to a DP6000-IP interface.
  - Back-up peripheral: If desired assign the group to an alternative DP6000-IP interface.
  - Select 'Save' to store the setting.



- ▶ To delete a Group address refer to ["Delete mobiles/devices"](#)







## 12 Alarm handling settings

### 12.1 Alarm definitions

In order to tailor the alarm handling according to the customer's needs, several alarm types can be created if needed.

'Default alarms' can be used to keep the system set-up (programming) easier, on the other hand 'Specified alarms' offers the possibility to tailor different alarms to create different follow-up procedures. The possible alarm definitions to be configured are:

- ▶ Default technical alarm.
- ▶ Default PS alarm.
- ▶ Default Other alarm.
- ▶ Default Hostage. (Not implemented yet).
- ▶ Specified alarms.



Note: All programmed alarms can work in both unmanned (standalone) mode without the intervention of an operator or in manned mode, in that case an operator handles the alarms.

#### 12.1.1 Default technical alarm

A 'Default technical alarm' is used for each technical issue that occurs.

Each application that is programmed to generate a 'Default technical alarm' will have the same follow up, it means e.g. that the same (group of) pager(s) are called with the same message that is programmed for this alarm. In the operators' screen, details about the cause of the 'technical alarm' are displayed. Because of using a 'Default technical alarm' in all cases the follow-up to handle the alarm is the same for each 'Default technical alarm' that occurs.

#### 12.1.2 Default PS alarm

A 'Default PS alarm' (Personal Security alarm) is used for each Personal Security issue that occurs.

Each application that is programmed to generate a 'Default PS alarm' will have the same follow up, it means e.g. that the same (group of) pager(s) is called with the same message that is programmed. In the operators' screen, details about the cause of the 'PS alarm' are displayed. Because of using a 'Default PS alarm' in all cases the follow-up instructions are the same for each PS alarm that occurs.

#### 12.1.3 Default Other alarm

A 'Default Other alarm' can be used to generate an alarm for general issues that occurs.

Each application that is programmed to generate a 'Default Other alarm' will have the same follow up, it means that the same (group of) pager(s) are called with the same message that is programmed. In the operators' screen, details about the cause of the 'Other alarm' are displayed. Because of using a 'Default Other alarm' in all cases the follow-up instructions are the same for each 'Default Other' alarm that occurs.



Warning: Because some applications use only a default alarm, you MUST ALWAYS define one DEFAULT technical alarm and one DEFAULT PS alarm.

#### 12.1.4 Specified alarm

A 'Specified alarm' can be used in cases a specific (Technical- or PS-) alarm desires a specific follow-up is desired; examples:

- ▶ If a location error occurs in specific area's the 'Default technical alarm' might not be sufficient.
- ▶ When some technical issues should be routed to different types of technicians/operators.
- ▶ In case a manual alarm from specific locations or from specific mobiles, the follow up in a 'Default PS alarm' is not sufficient.
- ▶ When special help forces need to be informed in case of a failed guard tour. Etc. etc.
- ▶ If a 'contact-alarm' should be linked to a specific location.

Other examples to implement 'Specified alarms'

- ▶ To create a specific follow up in case of specific technical- and/or specific Personal Security alarms.
- ▶ Each application that is programmed to generate a 'Specified alarm' can have its own specific follow up. E.g.:
  - Different operators with different handling instructions.
  - Different reaction times.
  - Different help forces to be informed.



Note: If a 'Specified alarm' is configured, it will overrule the handling of a 'Default alarm'.

Go to next page to continue: →

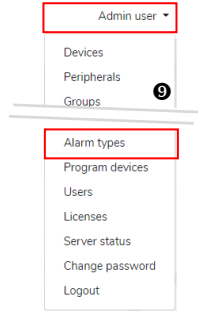




### 12.2 Alarm classes

In the user settings it is set which alarm classes an operator is authorised to see and/or to handle. Alarm classes linked to 'Default or 'Specified' alarms are:

- ▶ PS Alarm
- ▶ Technical alarm
- ▶ Hostage alarm (Not implemented yet).
- ▶ Other alarm



#### 12.2.1 Alarm types

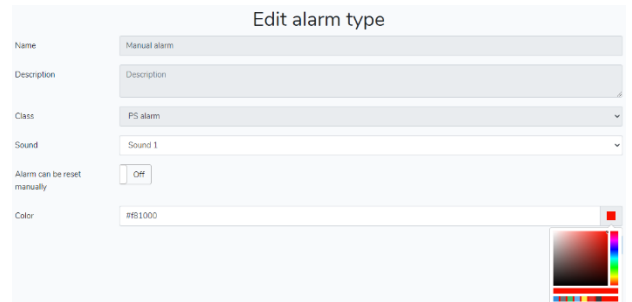
- ▶ Under the menu 'Alarm types' all defined types of alarms are made visible.
- ▶ The table "[Alarm sources](#)", gives an overview of all alarm types and source/reason of an initiated alarm.
  - The alarm type and the alarm source are selected automatically in case 'Default alarms' are used.
  - When creating 'Specified alarms', the correct alarm type and the alarm source should be selected.

**i** Note: It is possible to create different (specified) alarm handling procedures e.g. to give a different follow-up if a manual alarm came from building x or building y. Refer to chapter "[Define Specified alarms](#)" for details.

**i** Note: Once the operator has accepted the alarm, the alarm definition will be seen in the alarm screen. E.g. as 'default' or 'specified' alarm. The alarm bar as shown above gives the alarm type, the cause, the source and location of an alarm.

#### 12.2.2 Edit an alarm type

- ▶ Go to the menu option **i** 'Alarm types'.
  - A screen with 'Overview alarm types' is opened.
  - Select the 'edit' option to change items for an alarm type. In this example the settings for the manual alarm are changed.
  - Note that some settings cannot be changed.
  - Select 'Save' to store the (new) settings.

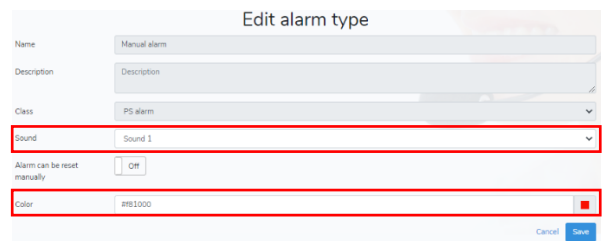


##### Alarm can be reset manually

- For Personal Security alarms, this setting cannot be changed, reset is only possible after an acknowledge from the mobile or when the mobile is placed in an 'absent rack'.
- For technical alarms you can change this setting if desired. If an operator resets technical alarms, the alarm will reappear as long as the root-cause is not solved.

##### Sound per Alarm type

- ▶ The alarm sound that can be heard at the operators terminal during the activation of alarms, can be set for each Alarm type.
  - For each alarm type an individual setting can be selected.
  - The sound is selected in a range from 0-4,
  - '0' is no sound.
  - Note that, if desired, these setting can be changed for each Personal Security- and Technical alarm.



##### Set the colour per alarm type

- Each alarm type can be set such that visualization on the screen has its own specific colour.
- A different colour per alarm can help to prioritise differences of urgency, see the examples below.

**i** Note: To set the number of visible active alarm lines, refer to "[Number of visible alarm lines](#)".

Name	Timestamp	Source	Location
Manual alarm	8 seconds ago	Erik	Back door
Auto-scan error	23 hours and 24 minutes ago	test 1003	special 1
Location beacon not seen	17 hours and 34 minutes ago	Tabel left	Tabel left
Tear-off alarm	11 seconds ago	Erik	Back door
Manual alarm	7 seconds ago	Erik	Back door

Continue at next page: →





### 12.2.3 Alarm sources

- ▶ Next to the 'alarm type', the source/reason of the alarm influences the method the system supports an occurred alarm.
  - The alarm type and the alarm source are selected automatically in case 'Default alarms' are used.
  - When creating 'Specified alarms', the correct alarm type and the alarm source should be selected, the information listed in the table below can help during that process.

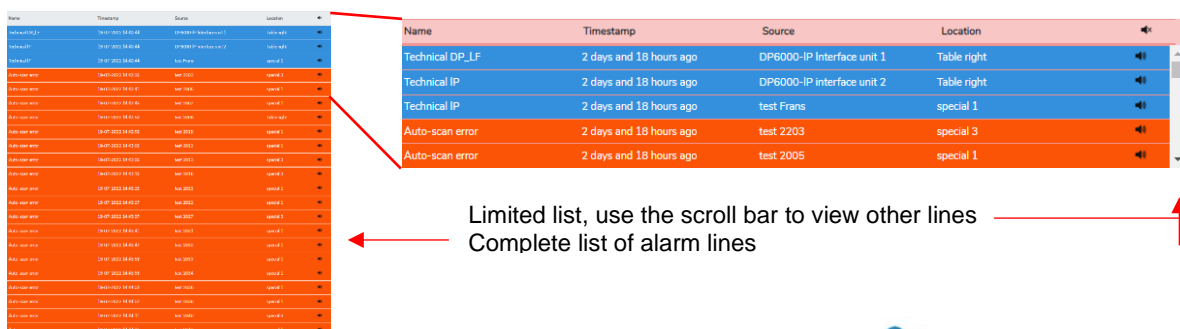
▶ Sources:

- C = input contact
- D = individual device/groups of devices (mobiles)
- I = DP6000-IP-Interface
- R = System receiver
- S = Server
- T = System transmitter

Alarm type:	Source	Alarm Class	Activation trigger
• Manual Alarm	D	PS Alarm	• If a manual alarm occurs.
• Second manual Alarm	D	PS Alarm	• If a 2 <sup>nd</sup> manual alarm occurs.
• No-Move Alarm	D	PS Alarm	• If a No-move manual alarm occurs.
• Not-vertical Alarm	D	PS Alarm	• If a Not-vertical manual alarm occurs.
• Fast-move Alarm	D	PS Alarm	• If a Fast-move manual alarm occurs.
• Tear-off Alarm	D	PS Alarm	• If a Tear-off manual alarm occurs.
• Guard tour alarm	S	PS Alarm	• If a guard tour is unsuccessful (timing fault, missed locations).
• Input_alarm_PS	C	PS Alarm	• If an input contact is activated a PS alarm is made.
• Auto-scan error	S	Technical Alarm	• If no reply on an automatic scan call occurs.
• Manual-scan error	S	Technical Alarm	• If no reply on a 'sign of life' call occurs.
• Technical IP	S	Technical Alarm	• If the IP6000-to DP interface loses the IP connection.
• Technical DP_LF	I	Technical Alarm	• Occupation time (0V) paging line exceeded.
• Technical DP_TB	I	Technical Alarm	• Occupation time talk-back line exceeded.
• Technical error LF/TB	I	Technical Alarm	• Combination of Technical DP_LF and Technical error LF/TB.
• Location beacon not seen	S	Technical Alarm	• If last time not seen of a location beacon is expired.
• Location beacon error	S	Technical Alarm	• If an location error code 7Fxxx, is received.
• Technical error receiver	R	Technical Alarm	• If an error code from a central receiver is received.
• Receiver not seen	S	Technical Alarm	• Central receiver is not replying for too long time.
• Technical error transmitter	T	Technical Alarm	• If an error code from a TMM module is received.
• Transmitter not seen	S	Technical Alarm	• Central transmitter is not replying for too long time.
• Input alarm technical	C	Technical Alarm	• If an input contact is activated a technical alarm is made.
• Technical server	S	Technical Alarm	• Alarm appears when the server's data base cannot reached.
• Technical error ESPA	I	Technical Alarm	• IF an ESPA port is defect.
• Low battery Alarm	D	Technical Alarm	• If a low battery message is received from a mobile
• Hostage alarm	D	Hostage Alarm	• Hostage alarm to trigger specific actions: (Not implemented yet.)

### 12.2.4 Number of visible alarm lines

- ▶ If the system has a lot of active alarms, then a long list is displayed and it is using a lot space in the monitors' screen.
  - If desired the number of visible alarm lines can be limited to 5 to be set in the system settings.
    - By using a scrollbar it is possible to scroll through the whole list of active alarm lines of course.
  - To set the number of visible lines, go to; ["full alarm table"](#). (1=show all active alarm lines, 0=show scrollable list).
  - Note: This setting is not applicable for the alarm screen; here always all alarm lines are displayed!





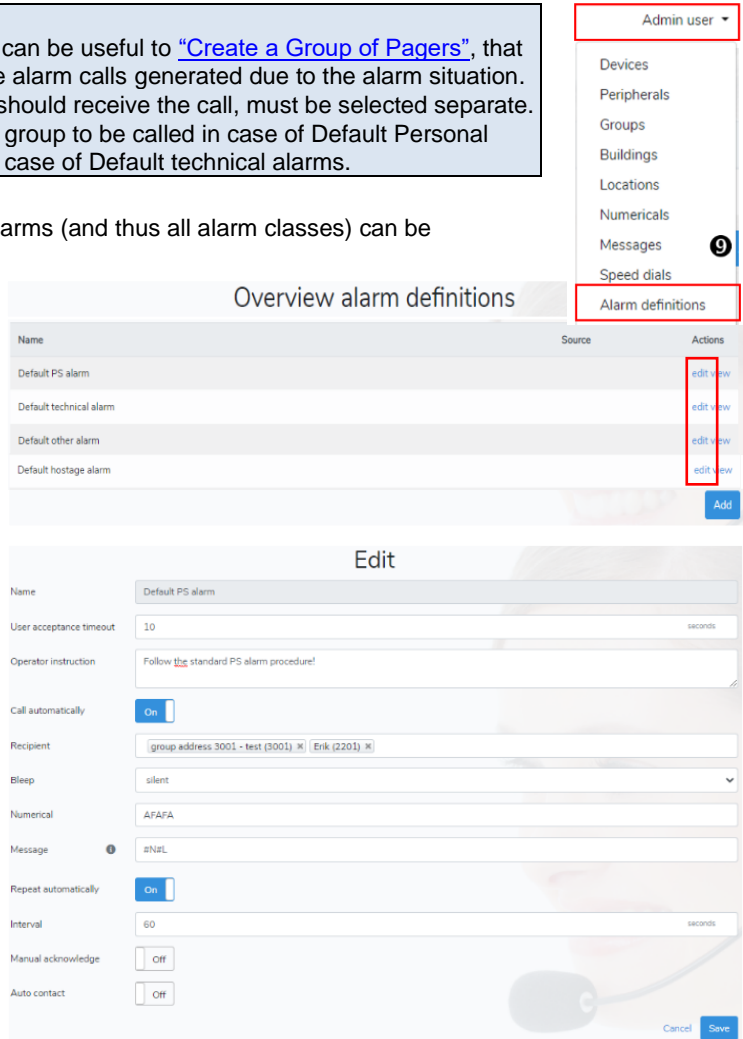
### 12.3 Define Default alarms

The description below is **similar for all Default Personal Alarms and Default Technical Alarms.**

**TIP:**

- Before start programming default alarms, it can be useful to [“Create a Group of Pagers”](#), that includes the mobiles that should receive the alarm calls generated due to the alarm situation.
- It prevents that each individual mobile that should receive the call, must be selected separate.
- If desired, separate groups can be made: a group to be called in case of Default Personal Security Alarms and a group to be called in case of Default technical alarms.

- ▶ In the option ‘Alarm definition’, the follow-up for all alarms (and thus all alarm classes) can be programmed.
- ▶ Go to the option ⑨ ‘Alarm definitions’.
  - A screen with ‘Overview alarm definitions’ is opened; see examples at the right.
  - Note that all created alarm definitions are listed here.
- ▶ In this example the ‘Default PS alarm’ is explained.
- ▶ Select in the overview the ‘edit’ option to edit a ‘Default PS alarm’.
- ▶ This opens the screen to configure the alarm.
  - Name: The name for ‘Default alarms’, cannot be changed.
  - User acceptance time out:
    - Give the time in which an operator must have accepted the alarm.
    - In case of an UNMANNED system fill in e.g. 1 second.



**Note:** To prevent loss of time in unmanned work mode, program a ‘User acceptance time out’ at 1 second. In Manned work mode give the operator enough time to accept an alarm.

- ▶ Operator instruction: Optionally note down the instructions to be displayed to operators, when the alarm screen is opened.

**Note:** For all Default Personal Security alarms, the operator instruction will be the same.

- ▶ Call automatically
  - If the slider is set to ‘On’, an automatic message is sent to the ‘Recipients’, after the user (operators’) acceptance time is expired.
    - For unmanned systems this is advised to set the slider always to ‘ON’.
    - For manned systems it is up to the customers’ needs.
  - Recipient: Select the pagers/groups that should receive the message.
  - Bleep: Select the bleep pattern for the call.
  - Numerical: Enter the numeric code for the call.
  - Message: Enter the message for the alarm call.
    - Tip: Next to the Message option there is an i-symbol: If you click on it, some special commands are shown to be used for adding extra parameters to the alarm message.
    - Options are: #N: To add the Name of the alarm source  
#A: To add the Address of the alarm source  
#T: To add the Alarm type  
#L: To add the Location of the alarm  
#B: To add the building/site of the alarm  
#S: To add the device type.

**i** Special commands

- #N : Name device/peripheral in alarm
- #A : Address device/peripheral in alarm
- #T : Alarm type
- #L : Location of alarm
- #B : Building
- #S : Device type

**Note:** The characters N, A, T, L, B and S are CAPITAL sensitive!

Continue at next page: →



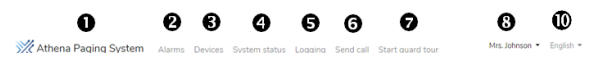
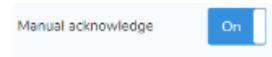


Example:

- Note that with the sequence of text and parameters you can influence the sequence of the message in the mobiles' display. A Message: Alarm#N#L; leads to a message 'Alarm' combined, with the mobile's name followed by the last known location of the originator.
  - If you prefer that the location information is positioned at the first lines in the mobile's display, set #L at the beginning of the message! f.i. #L #T #N
- ▶ Repeat automatically: If the slider is set to 'On' the call will be repeated according to the time interval as set in 'interval'.  
▶ Interval: The repeat time of these calls can be set.

▶ Manual Acknowledge;

- This option can be used to make that the mobiles will 'bleep until reset' which requires a manual reply from the mobile.
  - For PS-Pagers: If one or more manual replies are received, can be checked via the 'Sent call screen' **6**; which and how many individual PS-Pagers gave an manual reply, e.g. to indicate that they received the alarm call and confirmed to give support.
- To activate the Manual Acknowledge; Set the slider to 'On'.



▶ Auto contact; If the 'User acceptance time out' is expired, it is possible (next to an automatic call) to activate one or more output contacts; If desired:

- Move the slider to 'On'.
- Select the output contact(s) that you want to activate.



▶ Save to store the settings.

▶ To be sure if the alarm is configured well, test its function; refer to "[Test the alarm function](#)".

**i** Note: The colour of the alarm header can be set if desired, refer to: "[Set the colour per alarm type](#)". It gives the option to distinguish and prioritise the different Personal Security- and/or Technical alarms.

**i** Note: The sound that comes with an alarm can be if desired, refer to "[Sound per alarm type](#)". It gives the option to distinguish and prioritise the different Personal Security- and/or Technical alarms.

**i** Note: The automatic call can be sent and handled as follows: **i**

- Sending the call to a group address. (1 address); create a "[Group address](#)" in the section 'Devices'.
- Sending the call to one individual mobile.
- Sending a serial call to a number mobiles; This method is used to send a call to a group of individual pagers. Transmission can be time-consuming but can be used when automatic replies, or manual acknowledges from the mobiles are desired. to define such group-call, refer to "[Create a Group of Pagers](#)".

**i** Note: If during the handling of a PS-alarm, other PS-alarms are received from the same mobile, all alarms will be handled within a pending (first) alarm handling. It means that no new alarm will be raised. In the action logging field of the alarm screen it can be seen that another alarm was raised. Nevertheless each alarm can have its own escalation procedure, if it is programmed that way.

### 12.3.1 System settings for alarm handling

There are several system settings which also influences the handling of alarms.

For explanations and an overview refer to: "[System settings related to Alarm handling](#)".

Go to next page to continue: →



12.4 Define Specified Alarms

If you work only with 'Default alarm types' you can skip this chapter.

- ▶ In chapter "Alarm sources" all possible technical- and Personal Security- alarms are listed.
  - In most cases it will not be necessary to create a 'Specified alarm', it makes the configuration more complex. Therefore the advice is to create only a 'Specified alarm' when really needed.
- ▶ It is possible to create for each alarm source (alarm definition) a specific alarm, which enables a specific dedicated alarm handling procedure and specific authorizations to handle specific Technical- or Personal Security- alarms.

**i** Note: A 'Specified alarm' is a sort of 'and-function' that defines a specific alarm handling per Alarm: Only if the Alarm type and Source(s) and Location(s)/Building(s) matches, the alarm will be handled as A specified alarm.

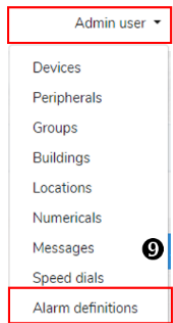
12.4.1 Create a specified alarm

Most of the settings are the same as explained in the chapter "Define default alarms". There are only a few exceptions

The description below is similar for all Specified Personal Alarms and Specified Technical Alarms

**i** TIP: Before start programming the specified alarm it can be useful to create groups of mobiles: It prevents that each individual mobile that can generate the alarm (source) or should receive the alarm call, must be selected separate.

- "Create a Group of Pagers" or "Group address", which includes the mobiles that should receive the alarm calls generated due to the specified alarm.
- "Create a Group of Pagers", that includes the mobiles that can generate the specified alarm.
- If desired separate/different groups can be made for different specified technical/Personal Security alarms.



- ▶ In the 'Alarm definition' option, the follow-up for all alarm classes and alarm types can be programmed.
- ▶ Go to the option **9** Alarm definitions.
- ▶ Select the blue button 'Add'.
  - Give the alarm definition a descriptive name.
  - Select the 'Alarm type' you want to be handled as a specified alarm; in this example it is a Manual alarm
  - Select the 'Source' that can generate the alarm.



**i** Note: The 'Source' of an alarm is the originator of the alarm.

- In case of Technical alarms this is system equipment.
- In case of Personal Security alarms these alarms are made by Mobiles/Devices like a manual alarm etc. etc.

- ▶ Location: give the building(s)/sites(s) or specific locations from where the alarm will be raised.

**i** Note:

- By selecting specific buildings or locations a specified alarm is only visible if it is linked with that specific building {and its specific location(s)}.
- A 'building' includes all location beacons that are assigned to that building.

- ▶ User acceptance time out:
  - Give time that an operator must accept the incoming alarm.
  - In case of an UNMANNED system fill in 1 second.

**i** Note: To prevent time loss in unmanned work mode, program a 'User acceptance time out' at 1 second. In Manned work mode, give the operator enough time to see that there is an alarm to be accepted.

Continue at next page: →



- ▶ Operator instruction: Optionally give the operator specific instructions, this can be a different instruction than given for the 'Default alarm.
- ▶ Auto alarm: If this option is visible keep this setting to 'Off'.
  - In the system settings it can be set if this option is visible or not. Refer to ["enable extended alarm definitions"](#).
- ▶ Call automatically
  - If the slider is set to 'On', an automatic message is sent, when the operators' acceptance time is expired.
    - For unmanned systems this is advised to set the slider always to 'ON'.
    - For manned systems it is up to the customers' needs.
  - Recipient: Select the pagers/groups that should receive the alarm call.
  - Bleep: Select the bleep pattern for the call.
  - Numerical: Enter the numeric code for the call.
  - Message: Enter the message for the alarm call.
    - Tip: Next to the Message option there is an i-symbol: If you click on it, some special commands used to add extra parameters to the alarm message.
    - Options are: #N: To add the Name of the alarm source  
#A: To add the Address of the alarm source  
#T: To add the Alarm type  
#L: To add the Location of the alarm  
#B: To add the building/site of the alarm  
#S: To add the device type.

Example:

- Note that with the sequence of text and parameters you can influence the sequence of the message in the mobiles' display. A Message: Alarm#N#L; leads to a message 'Alarm' combined, with the mobile's name followed by the last known location of the originator.
- If you prefer that the location information is positioned at the first lines in the mobile's display, set #L at the beginning of the message! f.i. #L #T #N

**i** Note: The characters N, A, T, L, B and S are CAPITAL sensitive!

- ▶ Repeat automatically: If the slider is set to 'On', the alarm call will be repeated according to the interval time.
- ▶ Interval: to set the interval time between the alarm calls.

- ▶ Manual Acknowledge;
  - This option can be used to make that the mobiles will 'bleep until reset' which requires a manual reply from the mobile.
    - For PS-Pagers: If one or more manual replies are received, can be checked via the 'Sent call screen' 6; which and how many individual PS-Pagers gave a manual reply, e.g. to indicate that they received the alarm call and confirmed to give support.
  - To activate the Manual Acknowledge; Set the slider to 'On'.

- ▶ Auto contact; If the 'User acceptance time out' is expired, it is (next to an automatic call) possible to activate one or more output contacts;
  - Move the slider to 'On'.
  - Select the relevant output contact(s) to be activated.
  - It is possible to activate multiple output contacts.

- ▶ Save to store the settings.
- ▶ To be sure if the Specified alarm is configured well, test its function; refer to ["Test the alarm function"](#).

**i** Note: The colour of the alarm header can be set if desired, refer to: ["Set the colour per alarm type"](#). It gives the option to distinguish and prioritise the different Personal Security- and/or Technical alarms.

**i** Note: The sound that comes with an alarm can be if desired, refer to ["Sound per alarm type"](#). It gives the option to distinguish and prioritise the different Personal Security- and/or Technical alarms.

Continue at next page: →



- i** Note: The automatic call can be sent and handled as follows: **i**
- Sending the call to a group address. (1 address); create a ["Group address"](#) in the section 'Devices'.
  - Sending the call to one individual mobile.
  - Sending a serial call to a number mobiles;  
This method is used to send a call to a group of individual pagers. Transmission can be time-consuming but can be used when automatic replies, or manual acknowledges from the mobiles are desired. to define such group-call, refer to ["Create a Group of Pagers"](#).
- i** Note: When during the handling of a PS-alarm, other alarms are received from the same mobile, all alarms will be handled within a pending (first) alarm handling. It means that no new alarm will be raised, in the action logging field of the alarm screen it can be seen that another alarm has been raised. Nevertheless each alarm can have its own escalation procedure, if it is programmed that way.
- i** Note: Each alarm can have its own specific escalation procedure, if it is programmed that way as 'Specified alarm'. The handling procedure for a 'Specified alarm', overrules the 'Default alarm' definition.

#### 12.4.2 Other (system) settings for alarm handling

There are several system settings which also influences the handling of alarms.

For explanations and an overview refer to: ["System settings related to Alarm handling"](#).







12.5 Test the alarm function

- ▶ To check if an alarm definition is configured well: the functionality of a configured alarm must be tested.

12.5.1 Fault finding

- ▶ In case of configuration errors exist in the 'Specified' alarm definition, there will be no alarms ignored by the system!
  - In such cases the alarm will handled as 'Default' alarm. (Alarm indicator shows Default PS- or Default technical- alarm plus the default operator instruction).
  - If the Specified alarm is configured well, the name that you gave earlier to the alarm plus the specified operators instructions will be displayed.
- ▶ In case of 'Specified alarms' pay attention to:
  - The initiator must be mentioned as 'Source'.
  - The locations or buildings must be listed as 'Locations'.
  - The alarm type and source must match with each other.

12.5.2 Alarm screen layout

- ▶ Once the alarm is accepted, by the operator, the alarm screen is opened and should, depending on the status of the handling contain items like depicted below. (real position and lay-out may be different).

The screenshot shows the 'Manual alarm - Erik' interface. It includes a top navigation bar with 'Cardiac Team', 'Technical Group', and 'Execute !!'. Below this is a 'manual call' button. The main area features a graphical location map (2) with a red overlay indicating the current location. To the right, there's an 'Alarm information' section (4) showing 'Current location: IPS 1 - Table right' and 'Previous location: IPS 1 - Table left'. Below the map is an 'Action logging' section (3) with a list of events. On the far right, there are three panels for 'Default PS alarm' (5), each containing an 'Accept alarm' button (a), a 'Remarks' field (6) with a 'Save' button (e), and 'Action buttons' (7) including 'Return alarm' (b), 'Enable Quasi dead' (c), and 'Reset alarm' (d). A 'Close alarm' button (f) is also present, with a note that a 'Reset alarm request is send'.

**Note:** Alarms selected in the alarm screen are direct considered as 'accepted' by the operator. Alarms selected in all other visible pages needs to be 'accepted' before handling will be possible. An alarm can be 'accepted' only by one operator at the time; no simultaneous alarm handling is possible.

12.5.3 The alarm sound

The alarm situation at the operators' desk can be accompanied with an audible warning for different attention value. To set the sound that comes with an alarm, refer to chapter ["Sound per Alarm type"](#). For different priority between a technical alarm or a personal security alarm, refer to: ["Alarm sound Priority"](#).

12.5.4 General System settings for alarm handling

There are several system settings which also influences the handling of alarms. For explanations and an overview refer to: ["System settings related to Alarm handling"](#).

12.5.5 View Alarm History

A part of the alarm handling is the possibility to see, store or printout view the alarm handling. Refer to the chapter ["Alarm history menu"](#) for details.



### 13 Create users and roles

Users can only execute actions after being logged on, therefore each user must have unique credentials to log on. Permissions for a user, are configured in the 'Role' that is given to a user.

**i** Note: The use of the web browsers Internet Explorer and Edge is NOT supported!

#### 13.1 Role of users

- ▶ The role of users are defined by the system administrator.
- ▶ At delivery there is only one super-administrator who has full rights to carry out all configuration activities in the system.
- ▶ The first step to do is to define the different roles and its authorisations/permissions.
- ▶ Depending on the given authorisations/permissions, the options in menu 9 are more or less limited.
- ▶ Of course the knowledge level of e.g. an operator can decide to give extra permissions.
- ▶ As example some names of 'roles' are listed below, however it is completely up to the installer which names and authorisations/permissions are given per role.

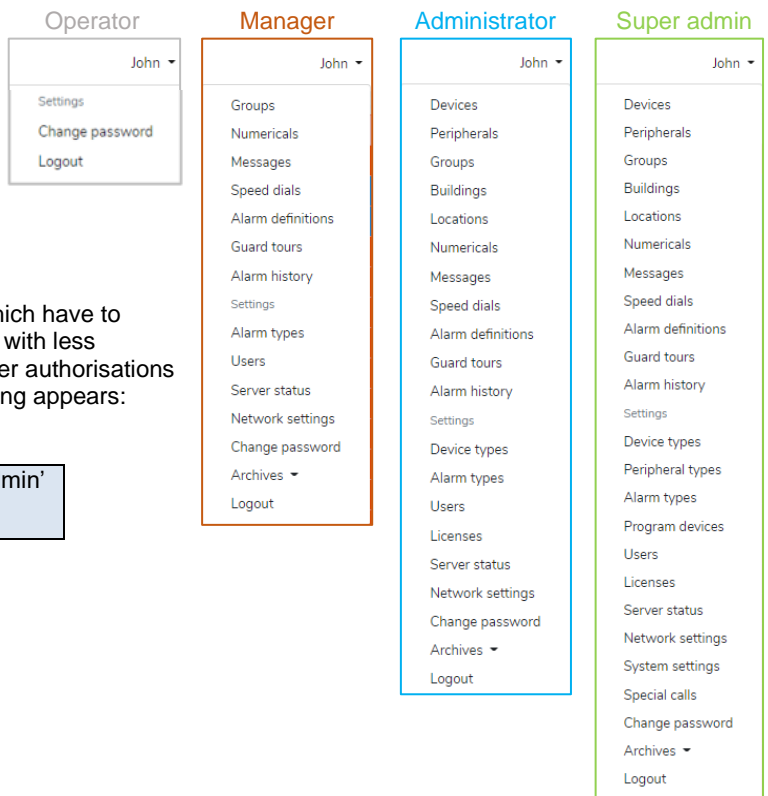
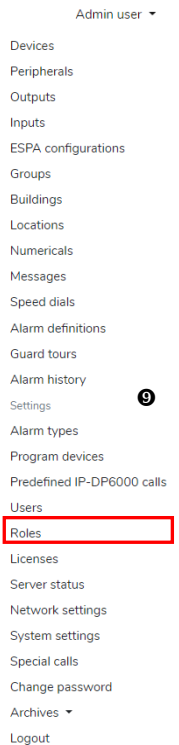
Example:

Role name	Example for authorisation/permissions:
• Super admin;	This level is needed to start any configuration; all rights are accessible.
• Administrator;	For technicians or installers, to configure the applications.
• Manager;	For supervisors e.g. give access to specific events or system performance.
• Operator;	For persons who operates the system; sent calls, handling alarms etc. etc.

#### 13.1.1 Examples of roles and permissions

- ▶ In the pull down menus that are displayed, the differences in permissions/authorisations are visible in the examples at the right: →
  - An Administrator can have huge impact on the systems functionality, therefore it is advised to create only 1 Administrator.
- ▶ The permissions are set in the 'Roles'.
- ▶ Roles are assigned to a user.
- ▶ It is not possible to change permissions for a user which have to a higher authorisation- level when logged on as user with less authorisation; e.g. a 'Manager' cannot change his user authorisations to 'administrator authorisation'. If this is tried, a warning appears: 403 USER DOES NOT HAVE THE RIGHT ROLES

**i** Note: The role-authorisations for a 'Super admin' cannot be changed.



Continue at next page: →



13.1.2 Create roles



- ▶ Go to the option 'Roles'.
  - If programmed already, a list of roles will be displayed, select one (edit) if a role should be changed.
- ▶ To add a Role:
  - Select the blue 'Add role' button.
  - Name: Give the role a descriptive name, see examples at the previous page.
  - Description: Describe in short the purpose of the role that will be defined.
- Set the permissions for the relevant role by moving the sliders to 'On' or 'Off'.
- When finished select 'Save' to store the settings.
- ▶ Once the role(s) are defined the users can be created to give a 'role'/permissions, refer to ["Add a user"](#) for details.
- ▶ As part of the general user settings also some permissions are given in the user settings; refer to ["Set user authorisations"](#).


Name	<input type="text"/>	Add role
Description	<input type="text"/>	
		Save

#	Y/N	Permission	Remark/suggestion	Menu
1	<input type="checkbox"/>	Download and change system settings.	Super admin	System settings
2	<input type="checkbox"/>	Edit, create and delete roles, set permissions to operate various parts of the application.	Super admin	Roles
3	<input type="checkbox"/>	Edit, create and delete users, set their role and other permissions.	Administrator or higher echelon	Users
4	<input type="checkbox"/>	Edit devices: change names and other settings of devices.	Administrator or higher echelon	Devices
5	<input type="checkbox"/>	Create and delete devices/allowed to send continue calls.	Administrator or higher echelon	Devices
6	<input type="checkbox"/>	Edit peripherals: change names and other settings of peripherals.	Administrator or higher echelon	Peripherals
7	<input type="checkbox"/>	Create and delete peripherals.	Administrator or higher echelon	Peripherals
8	<input type="checkbox"/>	Edit outputs: change names and other settings of output contacts.	Administrator or higher echelon	Outputs
9	<input type="checkbox"/>	Create and delete output contacts	Administrator or higher echelon	Outputs
10	<input type="checkbox"/>	Edit inputs: change names and other settings of input contacts.	Administrator or higher echelon	Inputs
11	<input type="checkbox"/>	Create and delete input contacts.	Administrator or higher echelon	Inputs
12	<input type="checkbox"/>	Edit RS485 and ESPA-ports; change names and settings.	Administrator or higher echelon	ESPA config.
13	<input type="checkbox"/>	Create and delete RS485 and ESPA-ports	Administrator or higher echelon	ESPA config.
14	<input type="checkbox"/>	Edit groups: change names and contents of a group.	Administrator or higher echelon	Groups
15	<input type="checkbox"/>	Create and delete groups.	Administrator or higher echelon	Groups
16	<input type="checkbox"/>	Edit, create and delete buildings; set default map to be used for locations.	Administrator or higher echelon	Buildings
17	<input type="checkbox"/>	Edit location information; update settings and upload maps	Administrator or higher echelon	Locations
18	<input type="checkbox"/>	Create and delete location information.	Administrator or higher echelon	Locations
19	<input type="checkbox"/>	Edit, create and delete default numericals.	Administrator or higher echelon	Numericals
20	<input type="checkbox"/>	Edit, create and delete default messages.	Administrator or higher echelon	Messages
21	<input type="checkbox"/>	Allow to scan device using the button in the devices overview grid	Administrator or higher echelon	Device screen
22	<input type="checkbox"/>	Edit speed dials, change order and position of speed dial button.	Administrator or higher echelon	Speed dials
23	<input type="checkbox"/>	Create and delete speed dials.	Administrator or higher echelon	Speed dials
24	<input type="checkbox"/>	Operate custom speed dials; send calls to pagers.	Manager or higher echelon	n.a.
25	<input type="checkbox"/>	Create, edit and delete alarm definitions.	Administrator or higher echelon	Alarm definitions
26	<input type="checkbox"/>	Create and delete profiles	Administrator or higher echelon	Profiles
27	<input type="checkbox"/>	Create, edit and delete guard tours.	Administrator or higher echelon	Guard tours
28	<input type="checkbox"/>	Show full Alarm history	Manager or higher echelon	Alarm history
29	<input type="checkbox"/>	Show only own Alarm history	Operator or higher echelon	Alarm history
30	<input type="checkbox"/>	Set the color for the alarm type when alarm is triggered.	Administrator or higher echelon	Alarm types
31	<input type="checkbox"/>	Program devices: set address, username and OP-codes.	Operator or higher echelon	Program devices
32	<input type="checkbox"/>	Edit predefined IP-DP6000 calls.	Administrator or higher echelon	Predefined IP-DP6000 calls
33	<input type="checkbox"/>	Create and delete predefined IP-DP6000 calls	Administrator or higher echelon	Predefined IP-DP6000 calls
34	<input type="checkbox"/>	Update license, view license options and software versions.	Administrator or higher echelon	Licences
35	<input type="checkbox"/>	Show current status of the server, restart server, show incoming calls and server logs.	Administrator or higher echelon	Server status
36	<input type="checkbox"/>	Edit special calls	Administrator or higher echelon	Special calls
37	<input type="checkbox"/>	Create and delete special calls	Administrator or higher echelon	Special calls
38	<input type="checkbox"/>	Show outgoing calls logging and download.	Manager or higher echelon	Archives
39	<input type="checkbox"/>	Get access to archives (logging).	Manager or higher echelon	Archives
40	<input type="checkbox"/>	Download and export various archives (logging).	Manager or higher echelon	Archives



### 13.2 Add a user

- ▶ Each user/user type should have his own log-in credentials and its own permissions/role.
  - Multiple user-types can be programmed, which makes it possible to have several users/operators each with their own authorisation/permissions.
  - Only authorised users (if set in their role) can create new users or change the user settings.
- ▶ Select in the Pulldown menu  the option 'Users'.
- ▶ A screen to add users opens, select the blue button 'Add User'.
- ▶ Name: give the user a descriptive name.
- ▶ Username: this is the log-on username.
- ▶ Password: this is the log-on password.
  - The password can be readable by checking the  eye:
- ▶ Confirm the password.
- ▶ Role: Select from the pulldown menu the desired role to be given to the user.
  - Refer to chapter ["Create roles"](#) for details.
- ▶ Opening page; select the page to be opened if the user logs on, other visible pages are defined in the next setting.
- ▶ The remaining settings as from: 'Visible pages' etc. are used to give specific rights to a user; ["Set user authorisations"](#).

- Admin user ▾
- Devices 
- Peripherals
- Outputs
- Inputs
- ESPA configurations
- Groups
- Buildings
- Locations
- Numericals
- Messages
- Speed dials
- Alarm definitions
- Guard tours
- Alarm history
- Settings
- Alarm types
- Program devices
- Predefined IP-DP6000 calls
- Users**
- Roles
- Licenses
- Server status
- Network settings
- System settings
- Special calls
- Change password**
- Archives ▾
- Logout

#### 13.2.1 Set user authorizations

Next to the 'Role', more or less other permissions can be specified here:

- ▶ Visible Pages:
  - This setting defines which pages are made visible and to be opened by a user: (to be able to use the functions of a page)
    - The selected pages are visible in the header of the main screen; example →
- ▶ Building:
  - An user can be assigned to all buildings/sites, in that case a system wide operation is allowed.
  - It is also possible to assign only a part of the system to a user; e.g. only a specific building (sub-site/department) etc. etc. The result in that case is that the operator can handle only events that are related to the specific building or system part.
    - Events (alarms) from system parts that are not included here, will not appear on the users/operators screen.
    - Only calls to mobiles that are assigned to the allowed buildings are can be made.
- ▶ Alarm classes (visibility of alarm classes)
  - Here it is defined which type of alarms will appear at the users' screen.
  - Selectable alarm classes are: Personal Security alarms, Technical alarms and/or Hostage alarms.
  - Alarms classes that are not included here will NOT appear on the users/operators screen.
- ▶ Handle PS-, technical- and/or hostage-alarms (ability to handle one or more of these alarm classes)
  - If set to 'OFF' an operator can only see alarms, alarms as set in 'Alarm classes' cannot be handled.
  - If set to 'ON' an operator is authorized to accept and handle alarms which are set in 'Alarm classes'.
- ▶ When finished this configuration, press the blue 'Save' button.

Alarms Devices System status Logging Send call Start guard tour



Warning: Not correct configured relations between the operator/user, buildings and Alarm classes, will lead to inability to handle alarms. In such cases an automatic follow-up will started, alarms will never be lost.



Note: If desired, technical alarms can be sent only/also to a member of the Technical Department as 'technical operator'. This can be organised to create a 'technical user' and assign only technical alarms in the Alarm classes.





### 13.3 Forgotten password

In case a user forgot the password, contact the system administrator.

To change solve this, go to menu

- ▶ Select the option 'Users'.
- ▶ An User list with all created users appears.
- ▶ Select the relevant user and click at the option 'Reset password'.
- ▶ Fill in the new (temporarily) password and confirm this password.
- ▶ Select the blue 'Save' button.
  - Inform the user about the new (temporarily) password.
  - With the eye sign you can make it readable or unreadable

Reset Password

Christ

Password: abcF\_321

Confirm Password: abcF\_321

Cancel Save

Note: A forgotten password can be corrected the system administrator only.  
A new password can be set by a user with the option reset by using the option 'Change password'.

#### 13.3.1 System settings and alarm handling

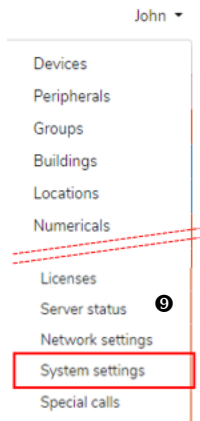
Several system settings are available to influence Personal Security- and Technical alarm handling. Refer to chapter ["System settings related to Alarm handling"](#) for explanation and details.

Note: System settings cannot be set for individual users and works system wide.



## 14 System settings

- ▶ Numerous system settings are available to tailor the system as much as needed.
- ▶ Navigate to 'System settings'. ⑨
- ▶ Select the desired setting to be edited.
- ▶ For detailed explanation you can select the 'link' in the overview below.



**i** Note: System settings are controlled by the Communication Server and have therefore a system wide influence.

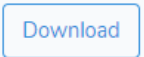
**i** Note: System settings cannot be set for individual users and works system wide.

### 14.1 Quick search

- ▶ To make it easier to find a certain system setting just type (a part of) the phrase in the search field.
- ▶ All options that have the (part of the) phrase in their 'Name' or their 'Description' will be displayed.

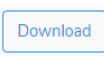
### 14.2 Download the system settings

- ▶ If desired a pdf-file with all system settings can be downloaded by pressing the 'Download' button at the bottom of the page.
- ▶ The file can be stored at the desired directory and/or printed later.



### 14.3 Overview System settings

#	Name:	Value	Description
1)	<a href="#">enable_alarm_reset_in_rack</a>	1	enable alarm reset in rack (1= yes, reset the alarm when mobile in rack)
2)	<a href="#">max_failed_auto_scans</a>	3	max failed auto scans before triggering alarm
3)	<a href="#">ip_connection_error_initial_timeout</a>	25	initial timeout on IP connection before triggering an alarm (sec)
4)	<a href="#">ip_connection_error_repeated_timeout</a>	1800	timeout before repeating an IP alarm that is active (sec)
5)	<a href="#">sequencing_delay</a>	1200	delay in msec between calls to multiple DP6000-IP_Interfaces
6)	<a href="#">out_of_range_enabled</a>	1	enable out of range calls (1= yes, a call CCC2 is sent each 30s)
7)	<a href="#">enable_scan_off</a>	1	enables user to turn off scanning (1=yes, 0=no)
8)	<a href="#">show_device_location</a>	1	show the current location of a device (1= yes, 0= no)
9)	<a href="#">scan_sequence_delay</a>	60	seconds between scanning two mobiles
10)	<a href="#">hold_scan_when_alarm_active</a>	1	hold scan calls when PS alarms active (1= yes)
11)	<a href="#">ignore_repeat_alarms</a>	1	ignore repeat alarm calls (1= yes)
12)	<a href="#">send_calls_when_absent</a>	1	force sending messages to devices that are absent (1= yes)
13)	<a href="#">order_devices_by</a>	name	devices are ordered by building, then ordered by 'name' or 'address'.
14)	<a href="#">Logging fields</a>	Selection	Set the fields that will be made visible in the logged data: Select from: date/time, address, bleep, name, function, numerical, priority (urgent), message, dp6000absent, DP6000confirmed (read-back from paging lines, DP6000handshake reply (confirmed by mobile, manual- and/or automatic reply).
15)	<a href="#">standard_hold_time</a>	750	To set the minimal time (ms) between two transmitted calls
16)	<a href="#">server_language</a>	en	To set the system language of the server, this is not the 'user language'. de= Deutsch, en = English, fr = Français, nl = Nederlands
17)	<a href="#">enable_PSMicro_alarm_reset_by_device</a>	0	Enables alarm reset by pushing alarm button twice (1 = yes)
18)	<a href="#">send_call_on_repeated_alarm</a>	1	directly send an auto call on a repeated alarm
19)	<a href="#">auto_send_reset_alarm_central_tx</a>	0	send B0XX 0 FF000 to reset alarm on Central TX
20)	<a href="#">turbo_rack_mode</a>	1	Faster in/out rack handling (1 = yes); do not change this setting!
21)	<a href="#">auto_clear_technical_alarms</a>	1	Automatically clear technical alarms ((1 = yes)
22)	<a href="#">number_of_errors_before_technical_alarm</a>	4	Number of errors before an alarm is triggered
23)	<a href="#">display_location_updates_in_alarm_tab</a>	1	display location updates in alarm screen (1 = yes)
24)	<a href="#">always_send_auto_call_on_location_update</a>	1	always send auto call on location update, when alarm accepted. (1 = yes)
25)	<a href="#">auto_restore_input_alarms</a>	1	automatically restore input alarms (1 = yes)
26)	<a href="#">trigger_new_alarm_on_new_PS_alarm</a>	0	when a PS alarm is triggered on a device already in alarm; treat as new alarm (1 = yes)
27)	<a href="#">table_length</a>	20	Amount of rows in a table



Continue at next page: →





System settings continued

#	Name:	Value	Description
28)	<a href="#">header_color</a>	white	Header color (choose: white (default), red, yellow, green, blue, teal)
29)	<a href="#">disable_management_gateway</a>	0	disable the management gateway (1 = disabled, 0 = enabled)
30)	<a href="#">master_slave_ping_interval</a>	60	interval between master-slave ping (reserved for future options)
31)	<a href="#">master_slave_max_missed_pings</a>	2	max missed pings before slave takes control (reserved for future options)
32)	<a href="#">enable_extended_alarm_definitions</a>	0	Gives extra options in the alarm definition (0=disable, 1 = enable)
33)	<a href="#">number_of_days_to-keep_log</a>	360	The number of days that logging is stored (max = 360 days)
34)	<a href="#">mute_alarm_per_user</a>	1	Users can only mute alarms on his/her PC (1= enable, 0 = mute all PCs)
35)	<a href="#">pong_on_notification</a>	0	Give an audible 'pong' notifications are triggered (0=disabled, 1 = enable)
36)	<a href="#">notification_on_alarm_reset_reject</a>	1	Send notification when alarm reset is rejected by user (0=disabled, 1 = enable)
37)	<a href="#">technical_alarm_on_lowbat</a>	0	Instead of a notification trigger a technical alarm on a low battery message (0=disabled, 1 = enable)
38)	<a href="#">auto_send_recall_after_alarm_reset</a>	0	Automatically send a recall to mobiles after an alarm has been reset (0=disabled, 1 = enable)
39)	<a href="#">enable_quasi_dead</a>	1	Enables the 'quasi dead' option in the alarm handling screen (0=disabled, 1 = enable)
40)	<a href="#">status_block_contents</a>	name, address, function,device_type, status, absent, building, location	Properties that are shown in the status blocks of Devices and System status
41)	<a href="#">logging_expanded</a>	0	Show the extra fields line, bleep, numerical and modeword in the logging page (0=disabled, 1 = enable)
42)	<a href="#">auto_reset_scan_error</a>	1	Automatically reset a scan error
43)	<a href="#">send_notification_on_absent</a>	0	Send a notification when a pager is absent
44)	<a href="#">fw_version</a>	24	FW version of $\mu$ -Processor 'R' in (all) DP6000-IP interface(s)
45)	<a href="#">split_long_messages</a>	0	Split messages larger than 24 characters into multiple messages (1=split, 0=no split)
46)	<a href="#">alarm_sound_priority</a>	priority	In case of multiple alarms: of which alarm the sound should be broadcast: last new or alarm with highest priority? Choose between 'latest' or 'priority'
47)	<a href="#">manual_call_has_default_leep</a>	0	Enables if the manual call should have a fixed, unchangeable, bleep code
48)	<a href="#">logout_on_hostage</a>	1	When there's a hostage alarm, log out all users without permission to handle hostage alarms. (Not implemented yet.)
49)	<a href="#">Editable_fields_speed_dial</a>	Recipient, Bleep, Numerical, Message, Urgent	Fields that are editable when making calls with a speed dial button.
50)	<a href="#">full_alarm_table</a>	0	Show all current alarms or a scrollable list (1=yes, 0=scrollable list)
51)	<a href="#">naming_building-subdivision</a>	building wing department room	Comma separated list of the different types of departments Future development for DP7000; <b>Not available yet.</b>
52)	<a href="#">naming_building-subdivision_plural</a>	buildings wings departments rooms	Comma separated list of the different types of departments Future development for DP7000; <b>Not available yet.</b>
53)	<a href="#">ipmesa_log_lf_line</a>	0	To log LF line to IP Mesa 0=N, 1=Y; reserved for special application
54)	<a href="#">ipmesa_log_tb_line</a>	0	To log TB line to IP Mesa 0=N, 1=Y; reserved for special application
55)	<a href="#">DJI_dashboard_server</a>	xxx.xxx.xxx.xxx	So set IP address for DJI application; reserved for special application
56)	<a href="#">DJI_dashboard_port</a>	5000	So set port nr for DJI application; reserved for special application

[Download](#)

Continue at next page: →





## 14.4 General system settings

### *standard\_hold\_time*

- ▶ The standard hold time is the minimal time between the successive call sent by the system.
  - If the value is set too high, the system speed can be that high that mobiles do miss calls.
  - If the value is set too low, the system speed will be too low.
- ▶ We advise not to change it, unless you are advised to do so.
- ▶ Refer to: "[standard\\_hold\\_time](#)" a setting of 750mS will be sufficient.

### *turbo\_rack\_mode*

- ▶ The turbo rack mode is a method to make the handling for in- and out-rack calls faster.
  - If the value is set to '1' the max speed of in/out-rack handling is optimal.
  - If the value is set to '0' the system will react slower to in/out-rack calls.
- ▶ We advise to set the value at '1' which is the default setting. Do not change it, unless you are advised to do so.
- ▶ Refer to: "[turbo\\_rack\\_mode](#)" keep the setting to '1' for optimal in/out-rack call handling.



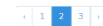
Note: If the `turbo_rack_mode` is set to '1', an **unknown mobile** will receive acknowledge calls from the server, so the functions like 'Switch On', 'Switch Off' and in/out rack are confirmed by the server. **HOWEVER**, the server will **not handle absent status nor alarm calls** from that unknown mobile. If `turbo_rack_mode` is set to '0', an **unknown mobile** will **NOT** receive acknowledge calls from the server, so the functions like 'Switch On', 'Switch Off' and in/out rack are **NOT processed** by the server.

### *table length*

- ▶ In the system several tables are used to list data.
  - This setting determines the max length of the tables, see the example here: →
- ▶ Refer to: "[table\\_length](#)"; a setting of 20 sets the max table lines to 20.

Timestamp	Address	Message	Client
23 06 2022 18:53:56	2127	no msg	
04 06 2022 18:04:41	2124	no msg	
23 06 2022 18:53:11	2122	no msg	
13 06 2022 18:08:17	2127	no msg	
23 06 2022 18:23:28	2127	unknown mobile: switch OFF	
04 06 2022 18:04:46	2124	unknown mobile: switch OFF	
23 06 2022 18:23:27	2127	unknown mobile: switch OFF	

## 14.5 System settings related to automatic scanning



### *Maximum of failed auto scan calls*

- ▶ The amount of scan failures that may occur before an scan alarm is triggered can be set.
- ▶ Refer to: "[max\\_failed\\_auto-scans](#)"; a setting of 3 scan attempts is quite common used.

### *Set the time between scan calls*

- ▶ The time between the scan calls can be set.
- ▶ Refer to: "[scan\\_sequence\\_delay](#)".
  - A setting of 10 seconds speeds up the total number of scan cycles in the system, however if the system load can handle it, a time of 60 seconds will also be reasonable.

### *Enable users to (temporarily) switch scanning On or OFF*

- ▶ To allow or disallow operators to (temporarily) switch OFF or ON the automatic scanning function.
- ▶ Refer to: "[enable\\_scan\\_off](#)". (0=disable, 1 is enable).
  - If enabled, the scanning function can be set ON or OFF, refer to "[How to set Scanning Off/ON](#)".

### *Stop scan calls when PS alarms are active*

- ▶ To give priority to the handling of Personal Security alarms, it is possible to postpone automatic scan calls as long as an alarm is active. This arranges that the system occupation is more concentrated to the handling of Personal Security alarms.
- ▶ Refer to: "[hold\\_scan\\_when\\_alarm\\_active](#)". (1=no scanning during active alarms, 0=scanning continues).

### *Automatically reset a Scan error*

- ▶ In case the system generates, due to a failed scan action, a technical alarm, it is possible that the alarm temporarily is reset by the operator.
  - If enabled, this technical alarm is reset automatically also once the mobile will again response to an automatic scan call.
- ▶ Refer to "[auto\\_reset\\_scan\\_error](#)". (0=auto reset disabled, 1=auto reset enabled).



Note: For systems that should comply with the Dutch NEN 2575 and/or the German BGR (GS) Normalisations it is advised not to allow operators to switch-off the scanning function.

Continue at next page: →







## 14.6 System settings related to Alarm handling

The system can be configured on many aspects how to react/handle technical- and Personal security alarms.



Note: All settings described below works system wide.

### *Alarm sound Priority*

- ▶ In case there are (multiple) Technical and/or Personal security alarms active, it can be set which alarm sound should be heard at the Operators desk.
- ▶ The following applies:
  - Audio sounds are heard in the same sequence as the (new) alarm becomes active.
  - If the `alarm_sound_priority` is set at 'latest', the hearable sound decided by the order of the most recent alarm activation (no matter if this is a technical or Personal Security alarm).
  - If the `alarm_sound_priority` is set at 'priority', the hearable sound due to the most recent Personal Security alarm have priority above the sound for technical alarms.
- ▶ To set the Alarm sound priority:
  - Go to the system settings, "[alarm\\_sound\\_priority](#)", select 'edit' and set 'Priority' or 'Latest'.
  - Select 'Save' to store the setting.

### *mute\_alarm\_per\_user*

- ▶ In case multiple operators are logged in and an alarm is activated, an audible sound is heard at the desktop of all logged in operators. The sound can be muted if wanted.
- ▶ The choice here to be made is that an operator can mute the sound for all logged in operators or only for themselves.
- ▶ To set the options for muting the alarm sound by the operator:
  - Go to the system settings, "[mute\\_alarm\\_per\\_user](#)";
  - Select 'edit' and set '1' or '0' (1= operators can only mute for themselves, 0 = operators can mute systemwide)
  - Select 'Save' to store the setting.

### *enable\_quasi\_dead*

- ▶ In case an PS-Pager is in alarm status, and an operator has accepted the alarm, an operator can select the 'Quasi Dead' button in order to set the PS-Pager in 'Quasi Dead' mode.
- ▶ If a PS-Pager is set in 'Quasi Dead' mode, the PS-Pager gives no hearable and no visible reaction to calls, and cannot in be operated by the user.
- ▶ To set if the 'Quasi Dead' button is available for operators or not, go to System Settings, "[enable\\_quasi\\_dead](#)".
  - Select 'edit' and set '1' or '0' (1= Quasi Dead button available, 0 = Quasi Dead button not available).
  - Select 'Save' to store the setting.

### *ignore\_repeat\_alarms*

- ▶ When mobiles are in alarm, they will resent periodically the alarm call. Here the choice can be made that each of such repeated alarm call should give a new alarm at the operators' desktop or not.
  - In order to preserve the system capacity and to keep rest at the operators desk, it can be advised not to select for repeated alarms.
  - Note that once an alarm is activated once, it will only disappear (Personal Security alarm) after a successful reset procedure or when the technical cause is solved.
- ▶ To set the choice to ignore or accept repeated alarms go to System Settings, "[ignore\\_repeat\\_alarms](#)".
  - Select 'edit' and set '1' or '0' (1= ignore repeated alarm calls, 0 = don't ignore repeated alarm calls).
  - Select 'Save' to store the setting.

### *trigger\_new\_alarm\_on\_new\_PS\_alarm*

- ▶ When mobiles are in alarm, and a new type of alarm comes from the same mobile, it can be set if the new alarm should start a new alarm handling cycle.
  - Note that if the Server knows that a mobile is already in alarm state, all new alarms are closed once the mobiles' user accepts a reset-request for one of the alarms.
  - Only different alarm definitions made for the different alarm types, will lead to different escalation processes.
- ▶ To set if a new PS alarm from the same mobile should trigger a new alarm;
  - Go to System Settings, "[trigger\\_new\\_alarm\\_on\\_new\\_PS\\_alarm](#)".
  - Select 'edit' and set '1' or '0' (1= trigger a new alarm, 0 = don't trigger new alarms.)
  - Select 'Save' to store the setting.

Continue at next page: →



*send\_call\_on\_repeated\_alarm*

- ▶ When mobiles are in alarm, they will resend periodically an alarm call. Here the choice can be made that each of such repeated alarm call should lead to a new alarm call to the help forces or not.
  - Note that f.i. a PS pager send every minute a repeated alarm call.
  - In order to preserve system capacity and to keep rest for the help forces that would being called, it can be advised not to select for repeated calls.
  - Note that f.i. a PS pager send every minute a repeated alarm call.
- ▶ To set if a call is transmitted, every time a repeated alarm is received;
  - Go to System Settings, "[send\\_call\\_on\\_repeated\\_alarm](#)".
  - Select 'edit' and set '1' or '0' (1= send calls, 0 = don't sent calls.)
  - Select 'Save' to store the setting.

*display\_location\_updates\_in\_alarm\_tab*

- ▶ As long as a mobile is in alarm, it will sent location updates to the system.
- ▶ Here the choice can be made if the location updates should appear in the alarm screen for operators or not.
  - Note that f.i. a PS pager send every minute a repeated alarm call.
- ▶ To set if each location updates will be displayed in the operator's screen, go to System Settings, "[display\\_location\\_updates\\_in\\_alarm\\_tab](#)".
  - Select 'edit' and set '1' or '0' (1= display location updates, 0 = don't display location updates.)
  - Select 'Save' to store the setting.

*always\_send\_auto\_call\_on\_location\_update*

- ▶ When mobiles are in alarm, they will send location updates to the system.
- ▶ Here the choice can be made that each time a location update is received, the help forces should be informed or not.
  - Note that f.i. a PS pager send every minute a repeated alarm call.
- ▶ In order to preserve system capacity and to keep rest for the help forces that would being called, it can be advised not to select to send each location update. To set if each location update will be sent to the help forces, go to System Settings, "[always\\_send\\_auto\\_call\\_on\\_location\\_update](#)".
  - Select 'edit' and set '1' or '0' (1= send calls with each location update, 0 = don't sent calls.)
  - Select 'Save' to store the setting.

*remote\_reset*

- ▶ For a description to reset alarms only from a mobile (without intervention of an operator) refer to: "[Remote Reset](#)".

*notification\_on\_alarm\_reset\_reject*

- ▶ In case an operator did sent an alarm reset request to a mobile and this reset request is not accepted by the mobiles' user, it can be set here if a notification should appear at the operators screen to inform.
- ▶ To set if a notification will appear, go to System Settings, "[notification\\_on\\_alarm\\_reset\\_reject](#)".
  - Select 'edit' and set '1' or '0' (1= send calls, 0 = don't sent calls.)
  - Select 'Save' to store the setting.

*auto\_send\_recal\_after\_alarm\_reset*

- ▶ When a Personal Security alarm has been reset, it is possible to send automatically a call to inform the help forces that the alarm has been reset.
- ▶ The help forces that will be informed, are the same as programmed the 'recipients' in the alarm definition.
  - To set if a 'reset call' is transmitted to the help forces, go to System Settings, "[auto\\_send\\_recal\\_after\\_alarm\\_reset](#)".
  - Select 'edit' and set '1' or '0' (1= send call, 0 = don't sent calls.)
  - Select 'Save' to store the setting.

*auto\_restore\_input\_alarms*

- ▶ Input contacts can be set as technical alarm or as technical alarm, the alarm status is valid as long as the contact is activated.
- ▶ With this setting it is set if the alarm will be reset automatically once the contact is released.
- ▶ To set if an alarm raised because of an input contact is reset once the contact is released;
  - Go to System Settings, "[auto\\_restore\\_input\\_alarms](#)".
  - Select 'edit' and set '1' or '0'  
(1= alarms are reset automatically once the input contact is released,  
0 = operators needs to reset the alarm once the input contact is released).
  - Select 'Save' to store the setting.

Continue at next page: →



*hold\_scan\_when\_alarm\_active*

- ▶ In order to preserve the system capacity for alarm handling, activating this option will stop scan calls as long as alarms are active.
- ▶ Also when speech-calls and/or 'listen in' and 'announcement' are used during alarm handling this setting can be useful.
  - To stop scan calls during an active alarm go to System Settings, "[hold\\_scan\\_when\\_alarm\\_active](#)". Select 'edit' and set '1' or '0' (1= hold scan calls, 0 = scan calls will be continued.)
  - Select 'Save' to store the setting.
  - See also chapter "[System settings related to automatic scanning](#)" for other scanning related System Settings.

*number\_of\_errors\_before\_technical\_alarms*

- ▶ To prevent that short system disruptions lead to technical alarms, the number of errors before it leads to a technical alarm can be set.
- ▶ This setting is meant to prevent unintended panic rather than a tool to hide dysfunctionality of course!
  - To set the number of errors go to System Settings, "[number\\_of\\_errors\\_before\\_technical\\_alarms](#)".
  - Select 'edit' and set the desired value.
  - A practical value not higher than '5' is reasonable for a good functioning system. (0 = no errors accepted).
  - Select 'Save' to store the setting.

*auto\_clear\_technical\_alarms*

- ▶ In case the root cause of a technical alarm solved, it can be set if the alarm is cleared automatically by the system, or if an operator should reset the technical alarm.
  - To enable or disable to clear technical alarms automatically by the system, once the root cause is solved;
  - Go to System Settings, "[auto\\_clear\\_technical\\_alarms](#)" (0=disable, 1 + enable).
  - Be aware that 'enabling' can hide some momentary events.

*auto\_send\_reset\_alarm\_central\_tx*

- ▶ For a description to send a reset call to system transmitters refer to: "[Automatic TX reset call](#)".

*enable\_extended\_alarm\_definitions*

- ▶ Extended alarm definitions gives extra options for the alarm definitions. (Auto alarm).
  - To enable or disable extended alarm definitions;
  - Go to System Settings, "[enable\\_extended\\_alarm\\_definitions](#)" (0=disable, 1 + enable).
- ▶ We advise only to activate this setting if you are advised to do so. (Otherwise keep this setting = 0).





### 15 Logging of calls

**i** Note: Visibility of screen 5 requires the logging activation licence.

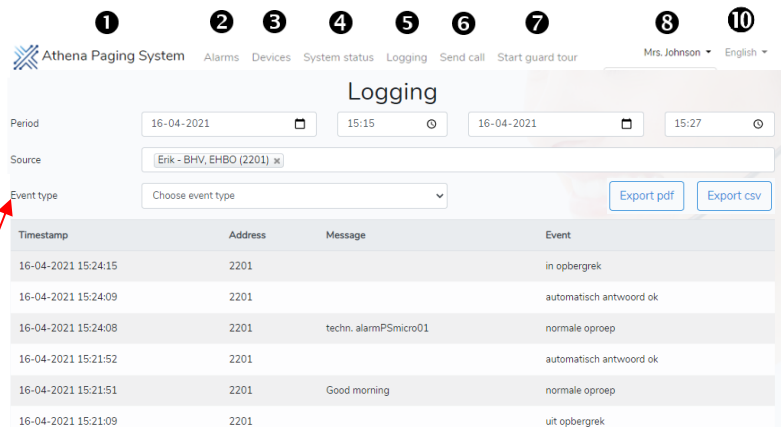
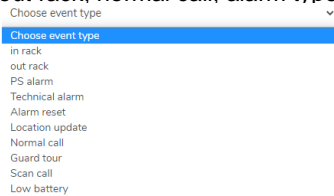
**i** Note: To read pdf-files, acrobat reader must be installed on your PC.

- ▶ The handling of incoming and outgoing calls can be displayed with several screens and/or exported as data file, as follows:
  - ▶ Via the Real time call handling, which shows (only) calls initiated by the operator.
  - ▶ Via the 'Logging' screen, which can be made available per user.
  - ▶ Through the Archives menu option, which is only accessible if set for the users' 'Role'.
  - ▶ As stored pdf-file in a free selectable directory on the users' PC.

#### 15.1 Logging screen

If set, by the system manager in the user settings, (visible pages) the 'logging screen' 5 is visible for an operator. This screen gives the following options:

- ▶ An overview (selective) of logged calls made -and received- by the system, are made visible.
  - Fill in the start date/time and stop date/time.
  - Select the source.
  - Select the Event type (type of call). e.g. in/out rack, normal call, alarm type etc.



**i** Note: The search action can have 3 results:

- Retrieving results....; meaning that the system is busy to gather the asked logged data.
- To many results....; meaning that the amount of selected data is too much; select for less data to continue.
- No results....; meaning that no data is found that matches with your request; adapt the selection to continue.

- ▶ If no filtering is selected, more data is made visible of course.
- ▶ If desired select 'Export pdf' or 'Export csv' to store the selected data.

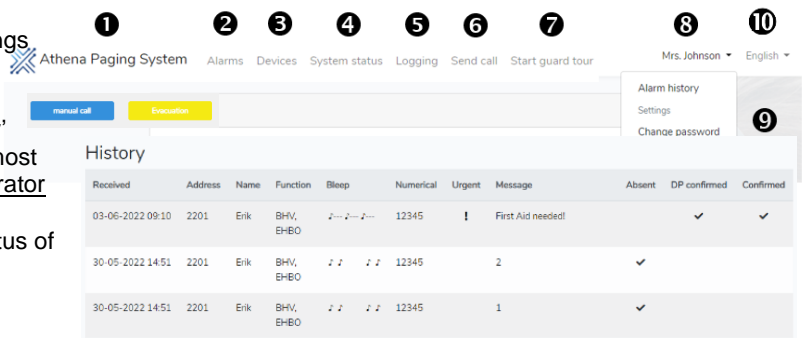
**i** Note: If set in the system settings; "logging expanded", the fields 'Bleep', 'Numerical', 'Line' and 'Modeword' can be made visible or hidden in the Logging page. (in this example these fields are hidden).

- For information about the content of the modeword, refer to chapter "Modeword explanation".

#### 15.2 Real-time call handling

▶ If set by the system manager in the user settings, (visible pages), the 'Sent call' screen 6 can be opened.

- In this screen also a table with call 'History' is displayed, showing an overview of the most recent calls, which are initiated by the operator after being logged in.
- This enables the operator to follow the status of the transmitted messages he/she initiated.
- The table shows the call content and the technical status, examples are:
  - If individual pagers (called via their unique address) are absent (in the charge rack) or not.
  - If the Call was 'read-back' from the paging lines.
  - If a PS pager did sent an automatic reply to a call.
  - If the user of a PS pager replied to an urgent call (i.e. if the reset button was pressed to reply on that call.)



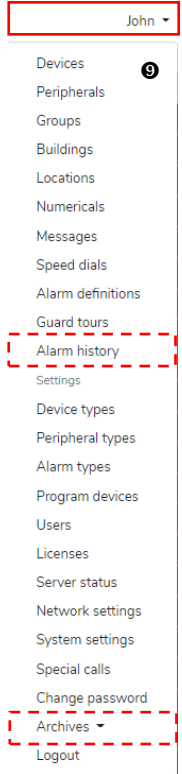
**i** Note: If set in the system settings; "logging fields", the fields to be displayed in the call History can be selected. In this example all possible fields are made visible: (Received; date/time, Address, Name, Function, Bleep, Numerical, Urgent, Message, Absent, DP confirmed and Confirmed).

Continue at next page: →



### 15.3 Alarm history

- ▶ If enabled by the system administrator, the Alarm history offers the possibility to view and create reports that contains the handling of alarms which are handled by the logged-in operator.
- ▶ Depending on the settings for the 'Role' the following data can be made available:
  - Only alarms handled by the logged-in operator are made visible; 'Own alarm history'
  - All data regarding handled alarms by all operators are made visible; 'Full alarm history'
- ▶ The accessibility for both is configured via the operators' Role; see table below.



Show only own Alarm history	Result	Show full Alarm history	Result
<input type="checkbox"/> off	Alarm history  cannot be selected.	<input type="checkbox"/> off	Archives/Alarms  cannot be selected.
<input checked="" type="checkbox"/> on	Only own alarms can be made visible, via the Alarm history.	<input checked="" type="checkbox"/> on	Archives/Alarms  can be selected.

#### 15.3.1 To access 'own alarm history'

- ▶ Go to the menu 'Alarm history' .
- ▶ Select the information you need.
  - Continue as described in chapter "[Obtain Alarm reports](#)".

#### 15.3.2 To access 'full alarm history'

- ▶ Go to the menu 'Archives → Alarms'.
- ▶ Select the information you need.
  - Continue as described in chapter "[Obtain Alarm reports](#)".

Continue at next page: →





## 16 Archives

**i** Note: The maximum time that logged data will be stored in 'Archives', can be set in the system settings: "[number\\_of\\_days\\_to\\_keep\\_log](#)". Max. time is 360 days, as long as the size of the logfiles doesn't exceed 20GB.

**i** Note: The availability of the 'Archives menu' requires the logging activation licence.

### 16.1 Accessibility of Archives

► The 'Archives' option is only accessible if set in the operators' Role.

Get access to Archives	Result	Download various data	Result
<input type="checkbox"/> Off	Archives  cannot be selected.	<input type="checkbox"/> Off	Archives data  cannot be downloaded.
<input checked="" type="checkbox"/> On	Archives  can be selected.	<input checked="" type="checkbox"/> On	Archives data  can be downloaded.

- Alarms
- Outgoing calls
- Technical logging
- Guard tours archive

- After accessing 'Archives', several logged data can be read and/or exported (downloaded) as a csv or pdf file:
- Alarms
  - Outgoing calls
  - Technical logging
  - Guard tours archive (only visible if an operator is able to open the option 'Start Guard tour'.)

### 16.2 Obtain Alarm reports

- If enabled by the system administrator, the Alarm history offers the possibility to view and create reports that contains the handling of alarms; all events and handling of alarms.
- Alarm reports can be viewed (if enabled) or downloaded (if enabled) via the menu 'Alarm history' or 'Archives → Alarms'.

- John ▾
- Devices
- Peripherals
- Groups
- Buildings
- Locations
- Numericals
- Messages
- Speed dials
- Alarm definitions
- Guard tours
- Alarm history**
- Settings
- Device types
- Peripheral types
- Alarm types
- Program devices
- Users
- Licenses
- Server status
- Network settings
- System settings
- Special calls
- Change password**
- Archives ▾
- Logout

Alarm type	Started	Closed	Source
manual_alarm	16-04-2021 14:32:12	16-04-2021 14:32:34	Erik - 2201
manual_alarm	16-04-2021 14:35:26	16-04-2021 14:35:59	Erik - 2201

- Enter the desired Period: start date, start time, end date and end time.
- Select the 'Alarm type' to be made visible, this can be technical- or Personal Security- alarms.
- If no selection is made all "[alarm types](#)" will be exported.
- Select the Source that initiated the alarm. (Only useful for alarms caused by mobiles).
- A list with Alarm type and/or sources, according the selected date/time frame becomes visible.

Alarm type	Started	Closed	Source
manual_alarm	10-06-2022 12:59:39	10-06-2022 13:00:03	Erik - 2201

- Select in the list, the specific alarm to be investigated/downloaded. (double click on it).
- The details of the relevant alarm are listed.
- Details how to download and store the pdf-file, is described in chapter: "[Download alarm history data](#)".

Continue at next page: →





16.2.1 Download alarm history data

- ▶ Double click (from the list as shown in the previous page) at the alarm to be investigated. An overview with all actions and who the action took, is displayed, including a timestamp.
  - Time: date and time of the action.
  - Event: The action that took place.
  - Remark: Who took the action; e.g. which operator or the mobile to whom an (alarm) call was sent etc.
- ▶ If desired, create a pdf-file by pressing the blue 'Download' button.
- ▶ The name of the generated pdf-file includes a date/time stamp that the alarm occurred: e.g. alarm\_2019-10-10-072556.pdf
  - The file can be stored on your PC.
  - Print the file if you want.
- ▶ Select 'Cancel' to leave the alarm overview.


Time	Event	Remark
10-10-2019 07:27:20	Reset alarm ack by user	
10-10-2019 07:27:17	Alarm reset requested	Admin user 2 (2)
10-10-2019 07:26:56	Repeated auto call	2003
10-10-2019 07:26:56	Repeated auto call	2004
10-10-2019 07:26:56	Repeated auto call	2006
10-10-2019 07:26:26	User acceptance timeout	
10-10-2019 07:26:26	Auto call	2003
10-10-2019 07:26:26	Auto call	2004
10-10-2019 07:26:26	Auto call	2006
10-10-2019 07:25:56	Initiated	

Continue at next page: →





### 16.3 Outgoing calls

- ▶ The data of 'outgoing calls' contains, next to 'absent indications of called mobiles, all calls that are initiated by the system.
- ▶ Through the menu 'Archives → Outgoing calls'  the history of all calls, initiated from the system, can be downloaded to be inspected.


#### Export logs

Period:

Recipient:

Fields:


<input checked="" type="checkbox"/> Address	<input checked="" type="checkbox"/> Confirmed
<input checked="" type="checkbox"/> Bleep	<input checked="" type="checkbox"/> Reply type
<input checked="" type="checkbox"/> Numerical	<input checked="" type="checkbox"/> Reply code
<input checked="" type="checkbox"/> Modeword1	<input checked="" type="checkbox"/> DP confirmed
<input checked="" type="checkbox"/> Modeword1 expanded	<input checked="" type="checkbox"/> Owner id
<input checked="" type="checkbox"/> Message	<input checked="" type="checkbox"/> Owner
<input checked="" type="checkbox"/> Queue	<input checked="" type="checkbox"/> Source system
<input checked="" type="checkbox"/> Absent	<input checked="" type="checkbox"/> Destination
<input checked="" type="checkbox"/> Paged	

Alarms 

Outgoing calls

Technical logging

Guard tours archive

 Note: The search action can have 3 results:

- Retrieving results...; meaning that the system is busy to gather the asked logged data.
- To many results...; meaning that the amount of selected data is too much; select for less data to continue.
- No results...; meaning that no data is found that matches with your request; adapt the selection to continue.

- For information about the content of the modeword, refer to chapter ["Modeword explanation"](#).


Select the data to be exported:

- ▶ **Period:** Enter the desired period: start date, start time, end date and end time. Only data according the selected date/time frame will become available.
- ▶ **Recipient:** It gives the possibility to concentrate to a limited number of mobiles, when left empty no filtering on mobiles' addresses is made.
- ▶ **Fields:** Mark the checkboxes to include or exclude the desired content of the exported data.
- Once completed click at the 'Export' button to create the csv-file or 'Cancel' to stop.
  - Tip: For analyses, see information in chapter: ["Convert CSV file to Excel file"](#).

#### 16.3.1 Meaning of the data (Fields) that can be exported; Outgoing calls

Content of outgoing calls:	
Address	The address used for individual devices (pager, PS-pager, PS-Micro) and group addresses.
Bleep	The bleep pattern that was sent with the call.
Numerical	The numeric information that was sent with the call.
Modeword 1	The modeword sent with the call in order to control the call.
Modeword 1 expanded	Several bits of the modeword are extracted, which can be used for quick analyses.
Message	The content of the alphanumeric message.

Call handling:	
Queue	Indicates the date and time that the call is created by the Communication Server.
Absent	Indicates if an absent indication was reported, such happens if the mobile is in a storage rack.
Paged	Indicates that the IP to DP6000 Interface has placed the call at the paging lines.
Confirmed	Is a registration if a manual and/or automatic reply was received as reply to the call.
Reply type	In relation to the previous parameter; if and which reply (automatic/manual) is received.
Reply code	Shows the bleep code that was accompanied with the 'reply call'.
DP Confirmed	Indicates that the call is read-back from the paging lines and is being according to expectation.
Owner ID	Shows the ID of an operator.
Owner	Shows the operator's name responsible for the handling. (combined with owner ID)
Source System	The trigger of the call: e.g. if the call is made by the server (Zeus) or operators (Athena) etc.
Destination	Indicates for example if the server did sent the call to a DP6000-IP Interface.

 Note: The logging of 'outgoing calls' can be used to see if a device was stored in a storage rack, which has led to an absent status.

Continue at next page: →





### 16.4 Technical Logging

- ▶ The technical logging contains the data of calls that are sent- and transmitted from the system.
  - For general investigations this logging can also be used to find specific call-details.
  - The more the filter is filled in the more detailed the result will be.
- ▶ Through the menu 'Archives → Technical logging' the history of all incoming and/or outgoing calls sent and received from the system can be downloaded to be inspected.

Note: The search action can have 3 results:



- Retrieving results...; meaning that the system is busy to gather the asked logged data.
- To many results...; meaning that the amount of selected data is too much; select for less data to continue.
- No results...; meaning that no data is found that matches with your request; adapt the selection to continue.

- For information about the content of the modeword, refer to chapter ["Modeword explanation"](#).

#### Data filter:

- ▶ At least the timeframe and the sort of data (Line: incoming and/or outgoing) must be defined.
  - Next to this one or more of the below mentioned parameters can be filled in.
  - Note that there is the possibility to find data from one specific mobile; the address or the devices' name or to filter on a combination of parameters.
- ▶ Period: Enter the desired period: start date, start time and end date, end time.
  - Only data according to the selected date/time frame will become available.
- ▶ Device: Here you can select, to export the data from only one device or a group (by its name).
  - Leave this field empty if the data should contain all known devices (by their name).
- ▶ Address: If desired the address of one specific mobile, or one group address can be entered here.
  - If this field is kept empty, the exported data will contain all known pager addresses.
- ▶ Bleep: Here you can select, to export only calls with a specific bleepcode
  - Leave this field empty if the data of all bleepcodes should be exported.
- ▶ Modeword: If a specific modeword is known, it can be filled in here.
  - Leave this field empty if the modeword is not relevant for the export to be made.
- ▶ Message: Filling in a part of a complete message, is sufficient to find all calls that contains at least a part of the phrase.
  - Example: 'alarm' leads to an export of all alphanumeric messages that contains at least the text 'alarm'.
- ▶ Line: Here you can select which types of calls should be part of the export:
  - Talk-back: Only incoming calls received from PS-pagers/PS-micro mobiles through the Talk-back lines.
  - Paging line; Only outgoing calls transmitted from the system to the Pagers and PS-Pagers.
  - Both: All incoming- (received) and outgoing (transmitted) calls; from the Talk-Back lines and Paging lines.
- ▶ Order: Select the order how the data (in date/time) should be sorted.

#### Export the data:

- ▶ Once completed, click on the 'Export' button to create the csv-file or 'Reset' to empty all fields.  
- ▶ Store the csv-file in a desired directory on your PC.
  - Tip: For analyses, see information in chapter: ["Convert CSV file to Excel file"](#).
- ▶ The construction of the exported filename looks like :
 

*incomingcalls\_YYYY-MM-DD\_09\_00\_yyyy-mm-dd\_12\_00\_\_1\_dec.csv*

  - 'incoming calls' is the type of data; for logging purposes; all calls, received via the talk-backline and all data read back from the paging line is internally handled as 'incoming calls'.
  - The first date: YYYY-MM-DD is the start date of the logging.
  - The characters 09\_00, in this example, represents the start time at the start date.
  - The second date: yyyy-mm-dd is the end date of the logging.

Continue at next page: →



- The characters 12\_00, in this example, represents the end time at the end date.
  - \_\_\_\_: If in the filtering specific devices are selected they are indicated at this position.
  - 1\_dec indicates descending dates (new → old) and \_1\_asc indicates ascending (old → new),
  - csv: Is the type of file that is exported; csv-files can be imported in Excel if desired.
- ▶ Information in the exported file:  
At the top of the exported file, columns are indicating the type of data. See the explanation below for detailed data content.
- ▶ To convert a CSV file to an Excel file, follow the steps as described in [“Convert CSV file to Excel file”](#).
- ▶ Store the excel file on a convenient place.

**i** Note: When creating data exports, prevent unnecessary large downloads. Be as specific as possible.

16.4.1 Meaning of the data that can be exported; Technical logging

**Content of incoming calls:**

IdIncomingCall	This is a line number intended to be used to navigate or to refer to in case of questions.
Address	The address used for individual devices (pager, PS-pager, PS-Micro) and group addresses.
Bleep	The bleep pattern that is used with the call.
Numerical	The numeric information (message) that is used with the call.
Message	The content (or a part) of the alphanumeric content (message).

**Call handling:**

Modeword 1 and 2	The modeword that controls the call, in general M1 and M2 are equal.
Line	L = Pagingline (outgoing calls), T = talk-back line (incoming calls).
Modeword 1 expanded	Several bits of the modeword are extracted, which can be used for quick analyses.
Owner	The type of peripheral that initiates the call; e.g. IP to DP6000 interface, ESPA, contact etc.
Source	The name of the call initiator, e.g. the name that is given to a IP to DP6000 interface.
Created	The date and time that the call was logged.

**i** Note: To see if a device was stored in a storage rack, which leads to an absent status, can be found in the call registration handling of [“Outgoing calls”](#).

16.5 Guard tours archive

- ▶ The Guard tours archive contains the data how a guard tours are handled.
- For general investigations the data of specific ‘Guard tours’ can be exported as PDF file.
- ▶ Go to the Menu **9** ‘Archives → Guard tours archive’.
- Period: Select start- and end- date for a selective overview of logged guard tours.
  - A screen ‘Guard tours archive’ appears, see at the right: →
- ▶ Double click at the Guard tour to be investigated.

Alarms

Outgoing calls **9**

Technical logging

**Guard tours archive**

Guard tours archive

Period: 21-06-2022 21-06-2022

Guard tour	Started	Closed
Night Check	21-06-2022 14:05:16	21-06-2022 14:05:50
Night Check	21-06-2022 14:03:37	21-06-2022 14:04:25
Night Check	21-06-2022 13:58:43	21-06-2022 13:59:15
Night Check	21-06-2022 13:58:09	21-06-2022 13:58:15
Night Check	21-06-2022 13:56:21	21-06-2022 13:56:47

Continue at next page: →



- ▶ An overview with all actions and who took the action, during the selected guard tour, is shown.
- ▶ The header of the overview shows:
  - The name of the Guard Tour e.g. (Night Check).
  - The information of the mobile that was used to run the Guard Tour:
    - The name: Erik
    - The function: BHV, EHBO
    - The address: 2201
- ▶ The overview shows further:
  - Time: the date and time of the actions that took place.
  - Location: the name of the location of the last passed location.
  - Description: the event that happened like; the start and ending of the guard tour, if and which actions were taken by the system or operator.  
It can also be seen, whether or not, if a passed location beacon is a part of the Guard tour.
- ▶ If desired create a pdf-file by pressing the 'Download' button.
- ▶ The generated pdf-file includes the name of the guard tour and a date/time stamp when the guard tour was logged e.g. `guard_tour_night-check-2022-6-21-140516.pdf`
  - The file can be stored on your PC.
  - Print the file if you want.
- ▶ Select 'Cancel' to leave the Guard tour overview.

Time	Location	Description
21-06-2022 14:05:50	Back door	Finished guard tour
21-06-2022 14:05:50	Back door	Location Back door in tour passed
21-06-2022 14:05:47	Table right	Location Table right in tour passed
21-06-2022 14:05:45	Table left	Location Table left not in tour passed
21-06-2022 14:05:38	Table left	Nigh Check resumed by John
21-06-2022 14:05:34	Table left	Nigh Check paused by John
21-06-2022 14:05:31	Table left	Location Table left in tour passed
21-06-2022 14:05:24	Front Door	First location Front Door in tour passed
21-06-2022 14:05:16		Nigh Check started by John

[Cancel](#) [Download](#)

## 16.6 Convert CSV file to Excel file

For analyses, the csv files exported from 'outgoing calls' and 'technical logging' can be imported in an excel file as follows:

- ▶ Open an empty Excel file and follow the steps:
  - Find the csv-file to be imported:
  - Select the tab 'Data', select the option <from text-file>
  - Navigate to the sub-directory where the csv-file is stored
  - Select the desired csv file
  - Select Import
  - Select 'Separated with signs like columns or tabs'
  - Mark the box to indicate that the file contains 'headers'.
  - Select 'Next'.
  - Select the separation sign, which is 'Comma'
  - Select 'Next'.
  - Select 'Finnish'.
  - Make sure that the most upper left Cell is selected.
  - Select 'OK'.
- ▶ In the excel file several options can be used to have more or less filtered views
  - To ease selective view in Excel, it can be useful to 'freeze the top row' and activate the filter option for the top row.
- ▶ If desired store the convert file at an convenient place.





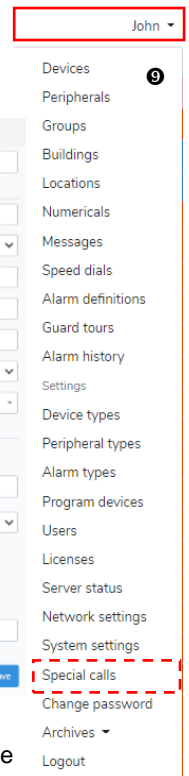
## 17 Application notes

### 17.1 Out Of Range (OOR) call

- ▶ If set in the mobiles' opcode, the mobile checks periodically if it receives calls from the system.
  - The mobile has therefor a build-in interval timer of approx. 30 seconds.
  - The mobile will generate an OOR indication if during 2 intervals (which is approx. 60 sec.) no call was received from the Communication Server.
- ▶ To set the Out of Range option, go to the system settings and set the option: ["out\\_of\\_range\\_enabled"](#): (1 = enabled. 0 = disabled).
  - Note that out of range should also be activated in the mobiles opcode settings.

### 17.2 Special Calls

- ▶ The accessibility to create, read or change the special calls is configured via the operators' Role.
- ▶ If specific call data is detected at the Paging- or Talk-back line, the system can sent a 'special call'.
- ▶ Additionally, special calls can be programmed such, that a ["Notification"](#) appears at the operators' screen.



#### 17.2.1 Edit a Special call

- ▶ Open the menu and go to the option 'Special calls'.
  - If you want to add a 'Special call', Select the button 'Add special call'.
  - If you want to change a special call, select from the relevant special call the 'edit' option.
  - To view the content of a special call, select from the relevant special call the 'view' option.
  - If you want to delete a special call, select the Delete special call.

**Note:**  
The more detailed the 'Detect' parameters are specified, the more selective the option 'Special calls' will work.

- ▶ The screen to configure a 'Special call' is
  - **Detect:** Contains the parameters to initiate a 'Special call'.
    - Be aware that the 'detect parameters' works as an 'and-function'; all parameters must be 'true' to go a special call.
    - Next to the 'Line' on which the data should be detected, at least one other parameter must be defined too.
  - **Action:** Contains the effect if all parameters of the data to be detected are 'true'.

#### 17.2.2 Detection of call parameters

- ▶ Name: Give the Special Call a descriptive name.
- ▶ Fill in the 'Detect' parameters, see table below:

Detect:	Description:	Remark:
Address	Address to be detected	If left empty the value is ignored
Bleep	Bleep code to be detected	If left empty the value is ignored
Numerical	Numerical data to be detected	If left empty the value is ignored
Message	Alphanumeric message to be detected	Give the (part of) the message to be detected
Modeword	Modeword to be detected	If left empty the value is ignored
Line	Data to be detect at the Paging- or TB-lines. Select LF- or TB line.	If detection at both lines is desired, 2 separate 'Special calls' must be specified.
Peripheral	Select the DP6000-IP interface that should detect the call parameters.	This peripheral is also processing the needed actions

Continue at next page: →

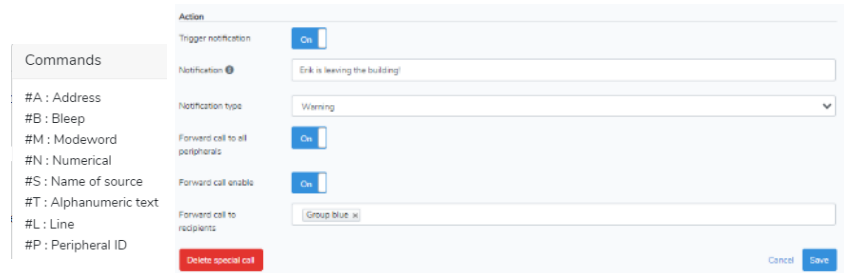


- i** Note: Detecting on a single parameter e.g. only on the address, can lead to too extensive system load! On the other hand, detection on too much parameters can lead to missed actions.
- i** Note: If a call matches with the 'Detect' parameters, the complete (remaining un-filtered) call is forwarded as specified in the 'Action settings'.
- i** Note: A handy parameter to be used in combination with Specific locations is e.g. the numerical data. A mobile sent its location information as numerical information. This can be used to take action if a mobile enters or leave a certain area.

### 17.2.3 Action for Special calls

▶ Trigger notification:

- If the information detected from the special call should lead to a notification at the operators' screen.
- Set the slider to 'On'.
- Notification: Enter the alphanumeric notification to be sent to the operator(s).
  - Note that short codes can be used to add additional data to the notification message.
  - The signs #A...#P are CAPITAL SENSITIVE!!
  - Click at the **i** sign for details.
- Select the 'Notification type' that should be displayed, for a description refer to the chapter: ["Notification"](#)
  - Info
  - Warning
  - Critical



▶ Forward call to all peripherals:

- If the slider is set to 'On' then;
  - If the 'detect' parameters does match, the original call is forwarded to all other DP6000-IP interface units in the system. This option gives therefore the possibility to send certain calls to multiple buildings/departments/sites.


▶ Forward call enable:

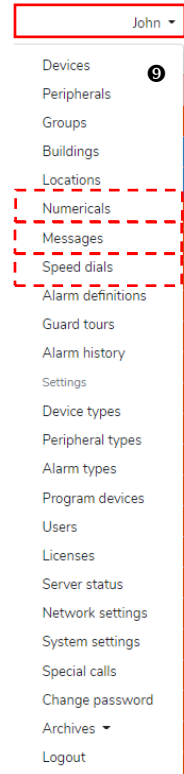
- If the slider is set to 'On' then;
  - If the 'detect' parameters does match, the original call is forwarded to the selected recipients. This option can be used to send certain calls to individual or groups of mobiles/devices.






### 17.3 Pre-defined numeric code

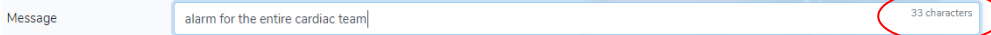
- ▶ When sending (manual) calls, it is possible to use pre-defined numeric codes if desired.
- ▶ To create pre-defined numeric codes do as follows:
- ▶ Go to the menu 'Numericals' .
  - Select the blue button 'Add numerical'.
  - Give the pre-defined numeric code a descriptive name: e.g. Fire etc. etc.
  - Fill in a 5 digit code, in hexadecimal format (0-9, A-F).
  - Select the blue button 'Save' to store the settings.
  - It is possible to review and/or to change the content of the pre-defined numeric codes afterwards.



**i** Note: If, during the creation of a call, no Pre-defined numeric code is selected, the call is sent, using the default numeric code: 88888. If desired, the content of the numeric code can be changed prior to sending the call.

### 17.4 Pre-defined Messages

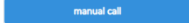
- ▶ When sending calls, it is possible to use pre-defined messages if desired.
- ▶ To create pre-defined messages do as follows:
- ▶ Go to the tab 'Messages' .
  - Select the blue button 'Add message'.
  - Give the pre-defined message a descriptive name: e.g. Alarm message for cardiac dept. etc. etc.
  - Fill in the message that you want to send.
  - Select the blue button 'Save' to store the settings.



- It is possible to review and/or to change the content of the predefined messages afterwards.
- In the right corner, a character counter displays the length of the entered message. So you can check if you exceed the desired message length.

### 17.5 Manual Call Button/Speed Dial Buttons


#### 17.5.1 Manual Call Options

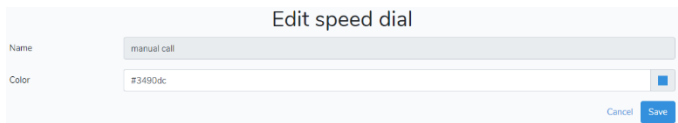
- ▶ For the 'manual call' some specific (limited) settings are available; this chapter describes how to configure:
  - The color of the manual button. 
  - If a manual call should always be sent with a fixed bleep code.
  - If calls longer than 24 characters should be sent as multiple calls or as one call with a larger message.

**i** Note:



- The Button 'manual call' is a function button which have limited editable options; f.i. the color or its position can be changed. These settings has no effect on the 'speed dial/fast dial' buttons.
- The option to send a 'Continue call' can be hidden through the 'Role' settings, so the Continue call' button is not visible if no rights to 'Create Devices' are set.

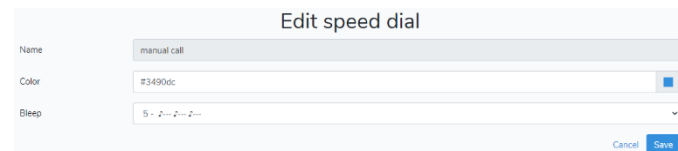
#### 17.5.2 Change the color for the 'Manual call' button

- ▶ Go to the tab 'Speed dials' .
  - Select in the 'Overview speed dials' the button 'manual call'. (double click on it).
  - Select the desired color for the button.
  - The code of the selected colour will be displayed.
  - The colour can be selected via the colour palette or by entering the code e.g. #3490dc for blue.
  - Click 'Save' to store the new setting.



#### 17.5.3 Sent Manual calls with a fixed bleep code

- ▶ Go to 'System settings'  and select ["manual call has default bleep"](#). (0=no fixed bleepcode, 1=activate fixed bleepcode)
- ▶ If the setting to activate a fixed bleepcode is set to '1' then:
  - To set the value of the fixed bleepcode; go to 'Speed dials' .
    - Select in the 'Overview speed dials' the button 'manual call'. (double click on it).
    - Select via the pull down menu the desired bleep to be fixed.
    - Click 'Save' to store the new setting.



Continue at next page: →



#### 17.5.4 Split long messages to 24 char/call

By default the length of an alphanumeric call is transmitted with max. 24 characters/call. In case a message has more than 24 alphanumeric characters, the call is sent as multiple calls (e.g. 48 characters are sent as 2 calls of each 24 characters).

- ▶ If desired the system can be configured such that calls with messages longer than 24 characters are sent as one (long) call.
- ▶ In such cases the Modeword is adapted accordingly and the complete alphanumeric string is sent in one call at once.
  - Go to 'System settings'
  - Select "[split long messages](#)". (0=calls are not split, 1=calls are split in max 24 characters/call.)
  - Note that some type of mobiles cannot handle messages larger than 24 characters/call.

#### 17.6 Speed dial buttons/Fast dial buttons

- ▶ In the operators' screen it is possible to display speed-dial buttons.
- ▶ If such button is selected, a complete predefined call is displayed:
- ▶ Speed dial buttons contains all relevant information: to who it should be sent, the information that should be sent and whether it is an urgent call.

**Note:** Speed dial buttons are only visible for operators if:

- For 'building(s)' selected in the 'Speed dial' settings, **AND**
- The 'buildings' are assigned in the 'User' settings, **AND**
- If allowed to operate speed dials in the 'Role' settings.

- ▶ Each speed-dial button can be given its individual name of max 20 characters, can have an unique colour and specific call information.
- ▶ To create a speed dial button, do as follows:
  - Go to the menu 'Speed dials'.
  - Select the blue button 'Add speed dial'. (or edit if the content should be changed).
  - Give the new speed-dial button a descriptive name: e.g. Evacuation.
  - Give the button its own specific colour.
    - The code of the selected colour will be displayed.
    - The colour can be selected by hovering over the colour palette or by entering the code e.g. #f5ea13 e.g. for yellow.
  - Assign the button to building(s) for which the button is valid.
    - Only logged on users who are also assigned to the same building(s) will see the created speed button, others not.
  - If desired, set 'sent immediately on alarm screen' to 'Yes'.
    - If set to 'Yes' the call, is sent immediately if the Speed dial button is selected (during alarms) via the alarm screen.
    - In system settings the content (fields) of the call that can be changed by the operator, before sending the 'speed-dial call' are set. Refer to "[Editable Content for Speed Dial Calls](#)".
  - Add the devices (mobiles) that should receive the call.
    - Optionally: add earlier defined 'Groups'.
  - Select the bleep code.
  - Optionally: select a 'Predefined numeric code'. OR: fill in the num. code that you want to send.
  - Optionally: select a 'Predefined message'. OR: fill in the message that you want to send.
  - Optionally: If the slider 'URGENT' is set to 'Yes', the call is sent as urgent call, the mobile will keep beeping until the reset button is pressed.

- ▶ Select the blue button 'Save' to store the settings.
- ▶ To remove a button, select the red 'Delete' button.

- ▶ In the Overview of the Speed dials, the position of the individual Speed dial button can be set by moving the button from one place to the other.



Continue at next page: →





17.6.1 Editable Content for Speed Dial Calls

- ▶ In case an operator selects a Speed-dial button to send a message, several fields can be edited in order to create the call to be sent.
- ▶ In the system settings it can be set which files are free to be edited.
  - Go to 'System settings' ⑨
  - Go to "[editable fields speed dial](#)".
  - Select 'Edit'.
  - Select the fields that should be editable for the operator:
    - Recipient
    - Bleep
    - Numerical
    - Message
    - Priority (Urgent)

**Note:**

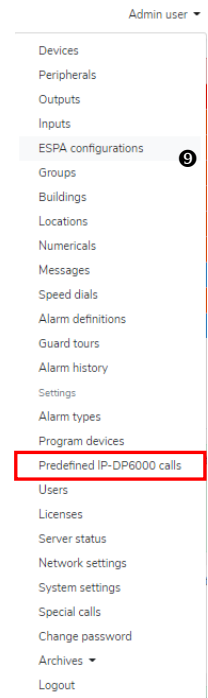
- This system setting has impact on ALL Speed-dial buttons and works system wide.
- The option to send a Continue call can be hidden through the 'Role' settings, if no rights to 'Create Devices' are set.

17.7 Predefined IP-DP6000 calls

- ▶ Predefined calls are send automatically by the DP6000-IP Interface without the intervention of the Communication Server.
- ▶ The calls are stored on the selected DP6000-IP Interface.
  - Each DP6000-IP Interface can be programmed with max. 32 of Predefined IP-DP6000 calls.
    - If more than 32 of such calls are needed, an extra DP6000-IP Interface is required.
- ▶ The calls can be used to be sent due to:
  - Handling of (guarded) Internal- and External Input contacts.
    - If an input contact is opened or closed.
  - To send calls due to defect signalisation; f.i.
    - Loss of IP-Connection between DP6000-IP interface and Communication Server.
    - Loss of ESPA connection(s).
    - Loss of RS485 connection.
    - In case of a defect (guarded) input contact.

17.7.1 Program a predefined IP-DP6000 call

- ▶ Go in menu ⑨ to the tab 'Predefined IP-DP6000 calls'.
- ▶ If there are already predefined IP-DP6000 calls configured, all 'Predefined IP-DP6000 calls' appears.
  - Here existing predefined IP-DP6000 calls can be changed or checked.
  - Select the 'edit' to change settings or 'view' to check programmed settings.



Predefined IP-DP6000 calls						
Peripheral	Predefined call number	Address	Bleep	Numerical	Message	Actions
DP6000-IP Interface unit 1	1	2008	1	afafa	contact 1 active	<a href="#">edit view</a>
DP6000-IP Interface unit 1	2	2008	4	11111	contact 2 active	<a href="#">edit view</a>
DP6000-IP Interface unit 1	3	2008	5	22222	contact 1 inactive	<a href="#">edit view</a>
DP6000-IP Interface unit 1	4	2008	6	33333	contact 2 inactive	<a href="#">edit view</a>
DP6000-IP Interface unit 1	5	2008	7	44444	contact 1 error active	<a href="#">edit view</a>

Continue at next page: →





17.7.2 Add a new Predefined IP-DP6000 call

- Select the blue button 'Add predefined call'; the 'Edit' screen appears to fill in the parameters.

- **Peripheral:** Select the DP6000-IP Interface on which the call is stored and will generate the call.
- **Predefined call number:** Select a (free) call number from the pull down menu (note it down for later use).
- **Bleep:** Select the bleep pattern that should be used while sending the call.
- **Numerical:** Give the numeric data that should be transmitted with the call.
- **Message:** Give the message that should transmitted with the call.
- **Bleep until reset:** If set to 'Yes' the mobile bleeps until the mobile-user presses the reset button.

**i** **Tips:**

- Next to the Message option there is an **i**-symbol: If you click on it, some special commands can be used to add extra parameters to the alarm message that becomes visible. The options are:
  - #H: To add a Head number (CAPITAL SENSITIVE), that causes the call.
  - #C: To add the contact number (CAPITAL SENSITIVE), that causes the call.
  - Example: A Message: #H#CALarm; leads to a message 'Alarm' preceded by the Head- and Contact number.
- To send the call also via other DP6000-IP Interfaces use the options as described in chapter 'Special Calls'.




## 18 Program I/O contacts

There are 2 types of I/O contacts:

- ▶ **Internal** I/O contacts; these are I/O contacts which are directly interconnected at an DP6000-IP Interface.
  - See chapter "[Installing Internal I/O contacts](#)" for mechanical and electrical details.
  - Program instructions are given in the chapters "[Programming output contacts](#)" and "[Programming input contacts](#)".
- ▶ **External** I/O contacts are I/O contacts which are controlled by an DP6000-IP Interface with an LBB5904/00 RS485 module.
  - For hardware set-up, refer to chapter "[Prepare the LBB5843/01 MPC heads](#)".


### 18.1 Programming Output contacts

- ▶ By default each DP6000-IP Interface is equipped with 2 Internal output contacts relays (Re1 and Re2).
- ▶ Optionally 2 extra internal output contacts can be added (Re3 and Re4).
  - Refer to chapter "[Installing Internal I/O contacts](#)" for details.

 Note: Re1 at the DP6000-IP Interface becomes also active in case a defect is detected! e.g. IP connection lost, DP line error, ESPA error, Internal contact error.

- ▶ Optionally 5 MPC heads (LBB5843/01) can be connected to each DP6000-IP Interface.
- ▶ Each MPC head has 2 output contacts.
  - Nevertheless; each DP6000-IP interface can handle a maximum of 160 external output contacts.

To program an output contact do as follows:

- ▶ Go in the menu  to the option 'Outputs'.
- ▶ If there are already output contacts configured, the screen 'Overview outputs' appears. Here existing output contacts can be changed or checked; Select the 'edit' to change settings or 'view' to check programmed settings.



Name	Peripheral	Output head	Output port	Actions
test 1	DP6000-IP Interface unit 1	0	2	<a href="#">edit</a> <a href="#">view</a>
test17	DP6000-IP Interface unit 1	0	1	<a href="#">edit</a> <a href="#">view</a>

[Add output](#)

To add a new output contact:

- ▶ Select the blue button 'Add output'; the 'Edit output' screen appears to fill in the parameters.



**Edit output**

Name:

Peripheral:


Output head:

Output port:

Mode:

[Delete](#) [Cancel](#) [Save](#)

- ▶ **Name:** Give the output contact a descriptive name: e.g. 'Contact abcd',  
**Tip:** Remember this name for future programming, when deciding when/if the contact needs to be activated.
- ▶ **Peripheral:** Select the peripheral (DP6000-IP Interface) that controls the output contact.
- ▶ **Output head:** This is some specific instruction:
  - In case it is an INTERNAL output contact, the head number MUST be '0'.
  - In case it is an EXTERNAL output contact, the head number is equal to the MPC head address (1-32) which is set at the MPC, Note that the max. number of MPC heads to be connected is 5.
- ▶ **Output port:** This is the relays number:
  - Per DP6000-IP Interface, use the range 1-2 only! Optionally the range 3 and 4 can be used also.
  - Per MPC head only the range 1-2 is applicable.
- ▶ **Mode:** To set the work-mode of the relays: Normal mode = Normal open, Fail safe = Normal closed.
  - The corresponding LED will lit when the relays active. So in Fail safe mode the LED is on when in rest.
- ▶ **Safe:** Select the blue button 'Save' to store the settings.

 Note: Re1 on each DP6000-IP interface is also used as 'Fault relays' for system monitoring (system errors). This is an hardcoded function and cannot be disabled. To set the work mode for Re1 as 'fail safe', add Re1 as 'Output' and configure the Mode as 'Fail safe'.

Continue at next page: →



### 18.2 Layout status indicator for output contacts

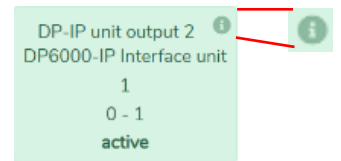
- ▶ When opening the 'System status' page an overview of the programmed internal and external outputs and its status is displayed per building.
  - If an output is active the color of the status indicator is green.
  - If an output is inactive the color of the status indicator is yellow.
- ▶ The status indicator contains the following information:
  - The name of the output contact; e.g. 'DP-IP unit output 2'.  
The DP6000-IP interface (peripheral) where the contact is located and which contains/controls the output contact.
    - In this case 'DP6000-IP Interface unit 1'.
    - The head number, which is in this case '0'. (0 = means an internal output contact).
    - The output number, which is in that case '1'.



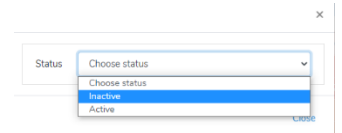
**i** Notes: An output stays active as long as the initiator is active. It is also possible to combine the output function with input contacts (even at another DP6000-IP interface) and its location.

#### 18.2.1 Change the status of the output contact manually.

- ▶ In the upper left corner of the status indicator there is the 'i' sign:
  - To change the status of the output from/to active/inactive mouse-click at the 'i' sign.
  - A 'status' menu pops-up.
  - Select the new desired status; active or inactive.
  - The result is that the color of the status indicator and the active/inactive status changes.



**i** Note: The rights to change the output status manually cannot be set



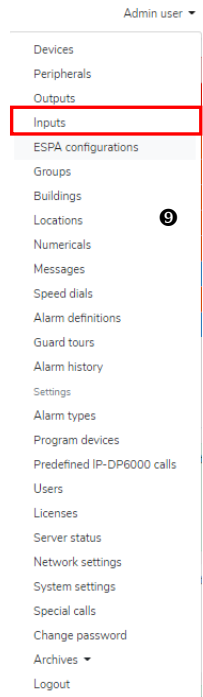


### 18.3 Programming Input Contacts

- ▶ Each DP6000-IP Interface can be optionally equipped with a maximum of 12 internal input contacts.
- ▶ The internal input contacts can be programmed as guarded or non-guarded contact.
  - Refer to chapter [“Internal Input Contact Module”](#) for details.
- ▶ Optionally 5 MPC heads (LBB5843/01) units can be added to each DP6000-IP Interface.
- ▶ Each MPC head has 32 (non-guarded) input contacts.
  - Each DP6000-IP interface can handle a maximum of 160 external input contacts.

To program an input contact do as follows:

- ▶ Go in the menu ⑨ to the option ‘Inputs’.
- ▶ If there are already input contacts configured, the screen ‘Overview inputs’ appears.



Overview inputs

Filter on peripheral Search

Name	Peripheral	Input head	Contact number	Input guarded	Actions
contact 1	DP6000-IP Interface unit 1	0	1	✓	<a href="#">edit view</a>
contact 2	DP6000-IP Interface unit 1	0	2	✓	<a href="#">edit view</a>
contact 3	DP6000-IP Interface unit 1	0	3	✓	<a href="#">edit view</a>
contact 4	DP6000-IP Interface unit 1	0	4	✓	<a href="#">edit view</a>
contact MPC 1	DP6000-IP Interface unit 1	1	1		<a href="#">edit view</a>

[Add input](#)

- Existing input contacts can be changed or checked.
- The sign ‘✓’ indicates if a contact is a guarded contact. Refer to [“input guarded”](#) for details.
- Select ‘edit’ to change settings or ‘view’ to check programmed settings.
- Select the blue button ‘Add input’ to configure a new input contact; a screen to fill in the parameters will appear:

Add input

Name:

Peripheral:

Location:

Input head:

Contact number:

- ▶ Name: Give the contact a descriptive name: e.g. ‘Doorbell’  
**Tip:** Remember this name for future programming.
- ▶ Peripheral: Select the DP6000-IP Interface by which the input contact is controlled/handled.
- ▶ Location: Select **for the relevant building**: ‘No location’ or a defined (fictive) location where the input is related to.
  - The location information comes with the call when the input is (de-) activated.
  - Furthermore the Building/location indicates at which IP-DP6000-interface an output is activated!!!!

**i** Note: The location that is selected here, has the following consequences:

- 1) The inputs are sorted per building in the input overview displayed in the system status screen.
- 2) Furthermore the selected Building/location offers the possibility to activate an output relays that is located at another DP6000-IP- Interface or even on (another) MPC coupler head.

- ▶ Input head: This needs some specific explanation:
  - In case it is an INTERNAL input contact, the head number is ALWAYS equal to ‘0’.
  - In case it is an EXTERNAL input contact, than the head number is EQUAL to the MPC head ADDRESS (1-5) which is set at the MPC, note that the max. of MPC heads per DP6000-IP Interface is 5.
- ▶ Contact number: (For SW versions released after 23-11-2021 the method below is applicable):
  - Select a free contact number from the drop-down list:
  - In case it is an INTERNAL input contact, the number of the input contacts MUST be in a range of 1-12.
  - In case it is an EXTERNAL input contact, the number of the input contacts MUST be in a range of 1-32.

Continue at next page: →





*Input guarded:*

- In case the 'Input head' is '0', then the internal input contact can be guarded against technical issues like short-circuited or broken wires;
  - If the slider for 'Input guarded' is set to 'No', the internal contact is not guarded.
  - If guarding is desired, set the slider to 'Yes'. (not applicable for external input contacts; LBB5843/01).
- If the slider for 'Input guarded' is set to 'Yes', and the functional settings for the contact are saved, you will be redirected to a page to configure the actions/calls etc. to be made if there is a technical issue with the cabling of the contact.
- Refer to "[Configure a Guarded internal input contact](#)" for details.

Input guarded  Yes When this input is successfully saved you are redirected to a page where you can create the guard.

*Handled by:*

- ▶ Set if the Communication Server and/or the DP6000-IP interface should handle the function of the input contact, for the occasion that the relevant (function) contact becomes active/inactive.

- IP-DP6000 box;
  - If selected, the contact is only handled by the DP6000-IP Interface. Handled by: IP-DP6000 box
  - The advantage is that if there is no IP-connection between the Communication Server and DP6000-IP Interface actions are still carried out by the DP6000-IP Interface.
  - For programming details Refer to "[Input contact handling from the DP6000-IP interface](#)".
- Server;
  - If selected, the contact is only handled by the Communication Server. Handled by: Server
  - Activation of the contact can be programmed such that a Personal Security Alarm or a Technical Alarm is caused.
  - For programming details, refer to "[Input contact handling from the Server](#)".
- Both IP-DP6000 and server;
  - If selected, both the Communication Server and the DP6000-IP Interface, will handle the activated contact and each will run their own programmed action plan.
  - Be aware that a double procedure will be started.
- Server with IP-DP6000 backup. Handled by: Server with IP-DP6000 backup
  - If selected, the Communication Server will take the primary action.
  - As back-up, the DP6000-IP Interface will run its programmed procedure in case the IP-connection between the IP-DP6000 Interface and Communication server is lost.

▶ **Active value:**

Set the work-mode of the input contact.

Active value: Input active when contact closed

- Disabled; to be set if the contact function is not in use.
- Input active when contact closed; (normally open).
- Input active when contact is open; (normally closed).

*Enable notification:*

- ▶ To enable if a "[Notification](#)" should appear in the operators' screen when the contact becomes active.

- Set the slide to 'On' to enable or to 'Off to disable'.

- Message: If the notification slider is set to 'On', then specify the message that should appear in the "[Notification](#)"

Notifications  
Enable notification:  On  
Message: Doorbell active, open front door  
Type: Info

- Type: If the notification slider is set to 'On', then define the Notification type: see "[Notification](#)" for the explanation.

Continue at next page: →



Input contact handling from the Server: Server generates an alarm:

- ▶ If a contact is closed there is the option to generate a Technical- or Personal Security (PS) alarm.

Server alarm	
Enable alarm	<input checked="" type="checkbox"/> On
Alarm type	Input alarm PS

- To enable if an alarm should appear once the contact becomes active, set the slide to 'On' to enable (Disable if not desired).
- Select the desired ["Alarm type"](#);
  - Input alarm PS; A PS alarm will be raised; the alarm can only be reset by releasing the input.
  - Input technical Alarm; A Technical alarm will be raised; the operator has the option to (temporarily) reset the alarm.

Input contact handling from the DP6000-IP interface:

- ▶ Active call: Select from the list with ["Predefined IP-DP6000 calls"](#) the call number that should be sent in case the contact becomes active.

IP-DP6000 handling	
Active call	1 - 2008 - 1 - afa - contact 1 active
Inactive call	3 - 2008 - 5 - 22222 - contact 1 inactive
Delay	1 seconds
Repeat time	10 seconds
Number of repeats	3
Output relay enabled	<input checked="" type="checkbox"/> On
Output head	0
Output relay	2
<input type="button" value="Delete"/> <input type="button" value="Cancel"/> <input type="button" value="Save"/>	

- ▶ Inactive call: Select from the list with ["Predefined IP- DP6000 calls"](#) the call number that should be sent in case the contact becomes inactive.

- To program Predefined IP-DP6000 calls, refer to the chapter ["Predefined IP-DP6000 calls"](#)

- ▶ Delay: To set the delay time between the time that the contact becomes active/inactive and time the call is sent.

- ▶ Repeat time: To set the time between the repeated calls.

- ▶ Number of repeats: To set how many times the call should be repeated; Calls are no longer sent, once the number of repeated calls is executed.

- ▶ Output relay enabled:

If desired, an output relay can be set if an input contact is activated, make sure that the desired output contact is programmed already.

- Output relays enabled; Set the slider to 'On' to enable an output relays. (Disable if not desired).
- Output head; Select the 'Head' on which the desired relays is present.
  - Head = 0, always for internal output relays.
  - Head =1-5; according to the address of the relevant MPC coupler in case of an external output contact.
- Select the relays number that is desired.
  - Re1, Re2 (optionally Re3, Re4) for internal output relays.
  - Re1, Re2 for external output contacts.
- The selected output relays becomes 'inactive' again, once the related input contact becomes 'inactive'.
- Refer eventually to chapter ["Program Output contacts"](#) for details.



Note: The Building/location that is selected earlier, has the following consequence:

It offers the possibility to activate an output relays that is located at another DP6000-IP- Interface or even on (another) MPC coupler head.

- ▶ Select the blue 'Save' button when finished.

- In case you have selected ["Input guarded"](#), you will be redirected to a page to configure the actions/calls etc. to be made if there is a technical issue with the cabling to the contact.
- Refer to chapter: ["Configure a Guarded internal input contact"](#).
- If you did not, the configuration of the input contact is finished.

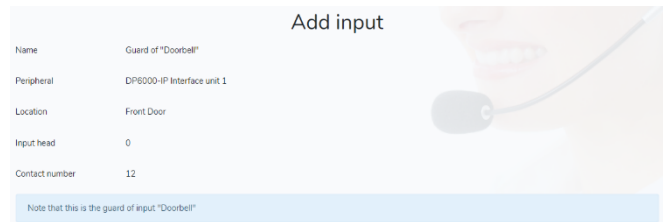
Continue at next page: →





### 18.3.1 Configure a Guarded internal input contact

- ▶ This part of configuration will be automatically started if it was selected earlier that a contact should be guarded.
- ▶ Because some parameters were programmed during the process in the previous chapters, some items are already filled in:
  - Name.
  - Peripheral.
  - Location.
  - Input head.
  - Contact number.



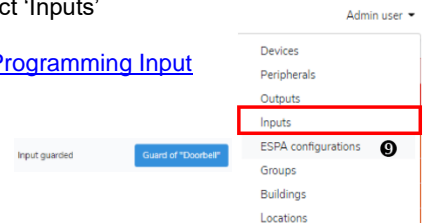
- ▶ The (optional) programmable items are:
  - If the Server and/or the DP6000-IP interface should handle the defect, as described in the previous parr. ["Handled by"](#).
  - The active value: Set the value to 'Disabled' if no guarding should take place, or to 'Enabled' to activate the guarding.
  - If/which notification should appear when a defect is detected, as described in the previous parr. ["Enable Notification"](#).
  - If/which alarm should appear when a defect is detected, as described in the previous parr. ["Handling from the Server"](#).
  - If and how the handling to done by the DP6000-IP Interface, as described in the previous parr. Refer to ["Input contact handling from the DP6000-IP interface"](#).

- ▶ In the 'Overview inputs' screen a '✓' sign indicates if an input contact is programmed as 'guarded' input. Where '✓' means 'guarded'.

Name	Peripheral	Input head	Contact number	Input guarded	Actions
contact 4	DP6000-IP Interface unit 1	0	7		<a href="#">edit view</a>
Doorbell	DP6000-IP Interface unit 1	0	12	✓	<a href="#">edit view</a>

### 18.3.2 Edit a contact

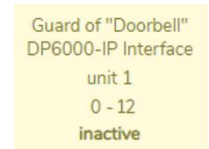
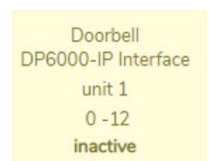
- ▶ To change earlier programmed settings of an input contact go to menu and select 'Inputs'
- ▶ This opens a screen 'Overview inputs'.
- ▶ Select the desired contact to be changed; all parameters as described in chapter ["Programming Input Contacts"](#) are displayed and can be changed if desired.
  - In this example a guarded input contact 'Doorbell' was selected.
- ▶ To change or disable the guarded functionality, select the blue 'Guard of...' Icon.
  - This offers the option to change the settings for the guarded function.
  - These settings can also be deleted to remove the guarded function.
- ▶ To implement a guarded function afterwards, just set the 'Input guarded' slider to 'Yes'.
  - Once the contact settings are saved (again), the screen to configure the guarded function is opened automatically.
  - Details are described as from chapter ["Input guarded"](#).
- ▶ If the (internal) input contact is deleted, the 'guarded' settings are deleted also automatically.



### 18.3.3 Layout status indicator for Input contacts

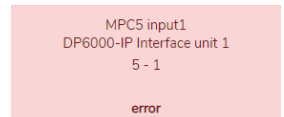
- ▶ When opening the 'System status' page an overview of the programmed internal and external inputs and its status is displayed per building.

- Doorbell; Is the programmed name of the contact.
- DP6000-IP Interface unit 1; Is the name of the DP6000-IP Interface that controls the input contact.
- 0; Is the head number, In this case the contact is located at head 0, which means that it concerns an internal input contact In case of an external input the contact the address (1-5) of the MPC is represented here.
- 12; Represents the programmed contact number.
- Inactive; Shows the status of the contact; in this example the input is 'inactive'. Possible statuses are: 'inactive', 'active' and in case of guarded contacts also 'error'.



- ▶ In case an input is programmed as 'guarded' input, also the status of the 'guard' is shown here. → See example: Guard of 'Doorbell'.

- ▶ In case the RS485 communication with an MPC is lost, there is an indication 'error' and the color is pink. (If set in the ESPA settings for port 2, a Predefined call is sent).





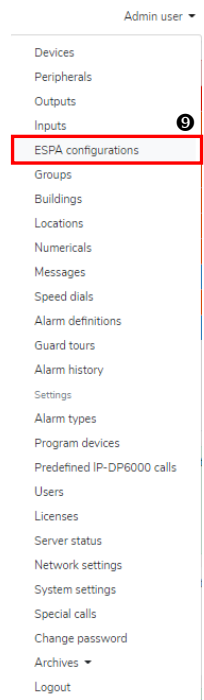
### 18.4 ESPA Ports

- ▶ Each DP6000-IP Interface can control max. 3 ESPA ports
- ▶ All ESPA Ports are controlled by the Communication Server, however when the IP connection is lost, the ESPA ports continues stand-alone to work in basic mode.
- ▶ Port 3 can be set as ESPA-in or ESPA-out port; If port 3 is set as ESPA-out, the ESPA data received at Port 1 is mirrored to Port 3.
- ▶ Port 2 can be set as RS485 interface, used when MPC heads are used.

### 18.5 ESPA configuration

- ▶ Go to the menu 'ESPA configurations' ⑨.
- ▶ Select 'Add ESPA configuration' to add a new ESPA port.

- ▶ Peripheral: Select the DP6000-IP Interface where the relevant ESPA port is present.
- ▶ Port: Select port 1, 2 or 3 to be configured.
- ▶ Direction: To set the function of the ESPA port:
  - Channel disabled; to be set when the ESPA port is NOT used.
  - Channel in use for ESPA input; to be set for each port used as ESPA input port.
  - Channel in use for ESPA output; to be set if port 3 is used as ESPA output port.
  - Channel in use for RS485 (MPC); to be set if port 2 is used as RS485 in combination with MPC heads.



#### 18.5.1 Program an ESPA input port

- ▶ After the steps in ["ESPA Configuration"](#) set the parameters for an ESPA input port according to the protocol of the master:
  - Baud rate;
    - Select: 1200,2400,4800 9600 or 19200 Baud.
    - Select: Channel disabled if not in use.
  - Serial number of data bits;
    - Select: 7 or 8.
  - Serial parity;
    - Select: no parity, even parity or odd parity.
  - Serial number of stop bits;
    - Set: 1 or 2.
  - Serial hardware handshake;
    - Select: None, rts-cts or none with active RTS.
  - Serial ESPA reply method;
    - Select: Normal, as described by protocol,
      - Always return status paged.
      - Always reply EOT.
      - Always reply EOT, unless status is asked using SOH2 header.
    - Note that the ["RS232 cable"](#) must be constructed such that it can handle the selected serial hardware handshake.

Continue at next page: →







### 18.5.2 Message options; Fixed digits

If desired, data received from the ESPA-in port can be modified such that selective calls are forwarded to the paging system.

- ▶ Address: In the address, 4 asterisks are set by default, then no selection is made.
  - If e.g. The address is set to 1\*\*\*, all ESPA calls are forwarded to pager addresses starting with '1' (1000-1FFFF).
  - If e.g. The address is set to 12\*\*, all ESPA calls are forwarded to pager addresses starting with '1' (1200-12FFF).
  - If the transmitting side of the ESPA interface doesn't transmit any address information, you can enter here a complete 4-digit address to be transmitted to Pagers. This can be an individual- or group address.
- ▶ Bleep: If the ESPA interface supplies the bleep-code information, select the setting 'Copy bleep code from ESPA' you can add only an '\*'. This arranges that the bleep code received from ESPA interface will remain.
  - In the following cases you can enter a hexadecimal representation (0-F) to be used as bleep code:
    - If another bleep code should be used than the one received from the ESPA interface.
    - If the ESPA interface doesn't sent a bleep code at all.
- ▶ Select 'Save' when programming is finished.
- ▶ Numeric info:
  - A standard ESPA interface will not supply numeric information to the call to be made. However numeric information is normally used to display hexadecimal information at the pagers' top-display. Therefore this is used to add (fixed) numeric data to the received ESPA string prior to sending a call to the pagers. Just enter the desired hexadecimal code (0-9, A, B, C, D, E, F.). Note that character 'F' is displayed as a '-'.
    - Some ESPA interfaces however do supply numeric code, in that case the following applies:
      - If e.g. The numeric info is set to 1\*\*\*\*, all ESPA calls will contain numeric info starting with '1' (10000-1FFFFF).
      - If e.g. The numeric info is set to 12\*\*\*, all ESPA calls will contain numeric info starting with '12' (12000-12FFFF).
      - If the transmitting side of the ESPA interface doesn't supply any numeric info information, you can enter here a complete 5-digit numeric to be transmitted to Pagers.
- ▶ ESPA options; If desired the call to the pagers can be modified such that pagers will bleep (for a maximum of 1 minute) till the reset button at the pager is pressed. If this is not required, select the setting 'No bleep until reset'.
  - No bleep until reset; The mobile will only bleep one cycle according to the selected bleep pattern.
  - Bleep until reset active when ESPA-priority equals ALARM (MoWo4\*\*\*\*);  
This option will only work if supported by the transmitting side of the ESPA connection. It offers the possibility e.g. to activate the 'bleep until reset function' only in case of fire but not for technical issues. The Modeword in the transmitted paging call will force the pager(s) to bleep until the reset button is pressed. The initiation of this status takes place while in the received ESPA data the Record type 'Priority' indicates an ALARM call (Record type = 6; 1= Alarm (Emergency)).
  - Bleep until rest active when an (urgent) call is received, sending MoWo4\*\*\*\*;  
With each call the 'bleep until reset' function is activated.

### 18.5.3 ESPA Port monitoring

- ▶ An ESPA-in and an ESPA-out port is monitored by sending polling requests to the 3<sup>rd</sup> party.
- ▶ If in a certain time no reaction from the 3<sup>rd</sup> party is received, a 'Default Technical Alarm' is generated.
- ▶ In the message of the Default Technical alarm it will be included which ESPA port causes a problem.
- ▶ The Monitoring option is configured as follows:
  - Poll watch alarm timeout: to set the time-out in which a reply must be received from the 3<sup>rd</sup> party.
    - Select an appropriate time in seconds: e.g. 10-30 seconds. (The selectable range is 0-999sec).
    - Enter '0' to disable the Monitoring function.
  - Poll watch alarm repeat time: To set the repeat time to repeat the technical alarm, as long as the issue is not solved.
    - Select an appropriate repeat time; e.g. 60 seconds. (The selectable range is 0-999sec).
    - If the repeat time is set to '0', no repeated technical alarms will be generated.
  - Predefined call on connection error;
    - If 'No call' is selected here, there will no call be sent in case of communication error. (Possibly only a technical alarm).
    - If desired select a Predefined IP-DP6000 call that should be sent if the communication with the ESPA port is lost. For details refer to; ["Predefined IP-DP6000 calls"](#).
    - Example: If programmed that way, a message can be sent to technicians like 'Connection error ESPA 1.3' As a result of interrupted communication with ESPA port 3 at DP6000-IP Interface 1.

Continue at next page: →





#### 18.5.4 Program an ESPA-out port

- ▶ Only port 3 can (optionally) be programmed as ESPA-out port.
  - In that case, Port 1 will forward all received ESPA data to ESPA port 3.
- ▶ Set the parameters for an ESPA output port according the protocol of the slave (3<sup>rd</sup> party):
  - Baud rate;
    - ✓ Select: 1200,2400,4800 9600 or 19200 baud
  - Serial number of data bits;
    - ✓ Select: 7 or 8
  - Serial parity;
    - ✓ Select: none, odd or even
  - Serial number of stop bits;
    - ✓ Set: 1 or 2
  - Serial hardware handshake;
    - Select: None, rts-cts or none with active RTS.
- ▶ To guard the ESPA-out port by the DP6000-IP interface, refer to chapter [“ESPA Port monitoring”](#)
  - Enter '0' for the Poll watch time out time to disable the guarding function.
- ▶ Select 'Save' when ready.
- ▶ Note that the [“RS232 cable”](#) must be constructed such that it can handle the selected serial hardware handshake.

#### Add ESPA configuration

Peripheral	DP6000-IP Interface unit 1
Port	3
Direction	channel in use for ESPA output
Baudrate	Choose baudrate
Serial number of data bits	Choose bits
Serial parity	Choose parity
Serial number of stop bits	Choose stop bits
Serial hardware handshake	Choose handshake



Note: An ESPA-out port can also be guarded by polling from the 3<sup>rd</sup> party, nevertheless it is possible to guard an ESPA out port also by the DP6000-IP Interface.

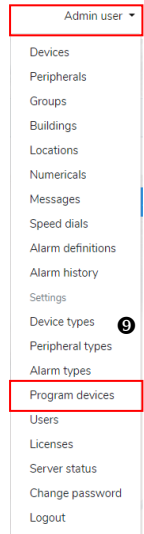




### 18.6 Programming Mobiles

The Communication Server supports to program the following DP6000 mobile types:

- ▶ PS-Micro mobile
- ▶ PS-pager
- ▶ Gen IV pager
- ▶ Items that can be programmed; depends on the type of the mobile:
  - Username
  - Individual Address
  - Group Addresses
  - Operation codes (Opcodes)



**Notes:**

- Addresses are in Hexadecimal format, note that some addresses are reserved for system calls.
- In multi-site systems are program calls transmitted system wide.

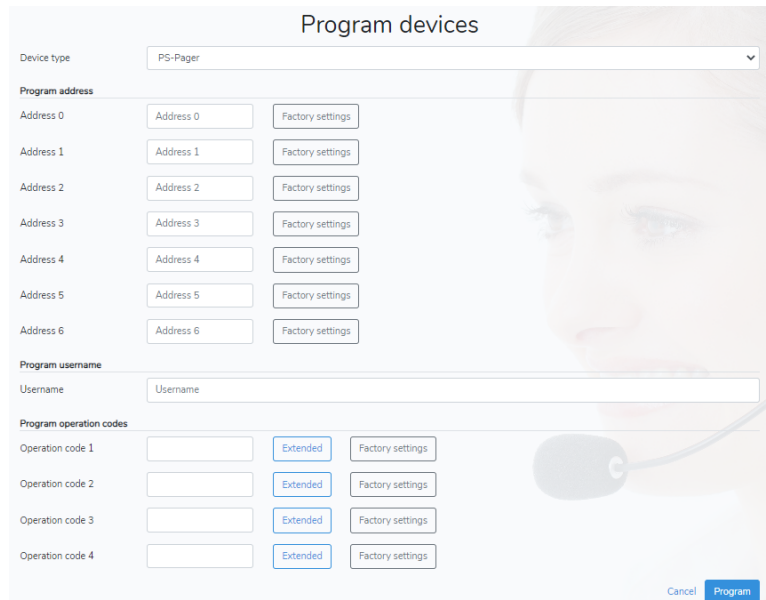
### 18.7 Preparation

- ▶ Make sure that the mobile is in the programming mode.
- ▶ Make sure that there is sufficient HF-coverage to receive the program calls
- ▶ To program a PS-micro mobile, it must be placed in a master storage rack. (connected to Paging lines).
- ▶ Open the tab 'Program devices'.

#### 18.7.1 Reserved addresses

The below mentioned addresses are system calls and may never be used as individual- or group address.

Address:	Reason:
CCEE	Reset speech call
CCC2	Out of range call
CCCC	All Call address
CCCx	Programming calls
B0xx	Transmitter monitoring
B1xx	System receiver monitoring
B3xx	Future applications



#### 18.7.2 Programmable items

- ▶ Depending on the selected mobile type the following items can be programmed: (see the screen example at the right →)
  - Addresses
  - Username
  - Opcodes (Operation codes)

#### 18.7.3 Default settings/Factory settings

- ▶ To fill in the (default) factory setting for an item select the button 'factory setting'
  - This arranges that the factory setting for that item is selected.

#### 18.7.4 Select the data to be programmed

- ▶ Select the device type:
  - Gen IV Pager, PS-Pager or PS-Micro.
- ▶ Select the address number to be programmed.
  - For the individual address this is always '1'. Address 0 is not used!
  - For a group address this is '2' or higher.
- ▶ Address: fill in the (hexadecimal) address to be programmed in the mobile.
- ▶ Username: Fill in the username to be programmed in the mobile; Max 12 characters.
- ▶ Operation code 1, 2, 3 and/or 4; enter per opcode the (hexadecimal) value to be programmed in the mobile.
  - For help to define an opcode value, just select the 'Extended' button and go to chapter ["The extended method"](#).


**Note:** Fields that are left empty (not filled in), are not transmitted, therefore eventually present settings in the mobile will not be overwritten. This makes it possible to change only one address, the username or only one opcode in a mobile.



18.7.5 The extended method

- ▶ As a help, the content of an opcode can be set by moving sliders and pull down menu's to (de-)select the options.
- ▶ The selectable options depends of course on the selected opcode and the selected mobile type.
- ▶ In this example the configuration for opcode 1 for an PS-Pager will be explained:
  - Click at the 'Extended' button to configure opcode 1.

- ▶ A new screen is opened with:
  - The selected device type.
  - The selected opcode (Operation code).
  - The Hexadecimal value of the opcode.
  - The selectable settings for the opcode.
- ▶ All options for the selected opcode are displayed and can be changed as desired.
- ▶ Select the blue 'Program' button to send the data to the mobile(s).

 Note: Alternatively the Hex value can be set manually in this screen also, the sliders are not changed when doing so.

Program devices

Device type: PS-Pager

Program address: [empty]

Address number: 1

Address: 2201

Program username: [empty]

Username: Erik

Program operation codes:

Operation code	Hex value	Extended	Factory settings
Operation code 1	6C540F	Extended	Factory settings
Operation code 2	342FF4	Extended	Factory settings
Operation code 3	010800	Extended	Factory settings
Operation code 4	765331	Extended	Factory settings

Buttons: Cancel, Program

Program operation codes

Device type: PS-Pager

Operation code: Operation code 1

Operation code 1: 6C540F [Factory settings]

Busy blocking: On

Field call: Call desk

mobile off: On

Low battery alert: On

Out of range: Off

Battery saving: Off

Ali-Call: On

Telemetry address: Off

Dec. group digit: On

Alert until reset: Off

Bleep volume: normal

Vibrator: Off

Deaf alert: Off

Call without INFO accept: Off

Call with max. 3 error messages accept: Off

Standby mode: Message

Top display: Message

Auto scroll within message: On

Max number of lines top display: 4 Line

Buttons: Cancel, Program



18.8 Transmitter monitoring via the Server

- ▶ System transmitters can optionally be equipped with a Transmitter Monitoring Module (TMM),
- ▶ There are two types of TMMs:
  - WSP\_D\_40971; (old Atus version).
  - LBB5905/00 TMM Version 2.0; (new IPS version).
  - The settings for both TMM types are described in this chapter.
- ▶ If a TMM is installed in a system transmitter, the status of the transmitter can be monitored by the Communication Server.

18.8.1 Preparation

- ▶ Make sure that the jumpers in the transmitter(s) are set correct (check the LF- and HF- part).
- ▶ Adjust the thresholds at the LF-section of the transmitter(s) for transmitted power and SWR for correct good/fault detection.
- ▶ Make sure that for each system transmitter in the system, a 'peripheral' is configured;
- ▶ Refer to chapter "[Configure Transmitter DP6000 TX](#)".

18.8.2 Error indications

- ▶ There are two types of errors that are detected by the system:
  - The Server checks periodically, by 'polling' over the paging-lines, if there is a connection between the server and the transmitter(s). If the system doesn't receive a reply within the scan time-out, there is most likely a connection error. A technical alarm indicating 'Transmitter not seen' will be raised.
  - If the transmitter (TMM) replies, but there is an transmitter error indication in the reply, a technical alarm indicating 'Technical error transmitter', including the type of detect that is found, will be raised.
  - If desired Re1 at the TMM can used to be lead to an input contact for an extra fault signalisation.
- ▶ Technical alarms are caused if the performance of the transmitter is below expectations:
  - Transmitted power too low; less than 60% compared to an adjusted reference level.
  - SWR (reflected power too high); compared to an adjusted reference level.
  - Presence of LF-synchronisation signal; relevant in case of multi transmitter systems.
  - Presence of DP6000 signal; when calls are transmitted.
- ▶ Transmitter scan-calls and error-calls starts always with address B0xx, this can be used to filter relevant logging data.

18.8.3 Automatic TX reset call

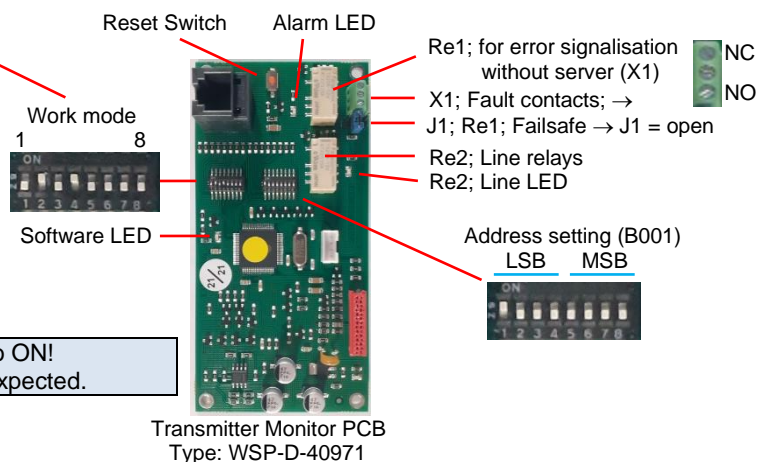
- ▶ In case an error is received by the central it can be set if an automatic reset call should be sent. (B0XX 0 FF000).
  - Such reset call can also sent manually.
  - To enable or disable the automatic reset call go to System Settings, "[auto\\_reset\\_alarm\\_central\\_tx](#)" (0=disable, 1 + enable).
  - Be aware that 'enabling' can hide some momentary events, therefore it is preferred to keep this setting at '0'.
  - Of course it is possible to reset a fault-state by pressing the reset switch at the TMM.

18.8.4 Settings TMM type WSP\_D\_40971

- ▶ Set the 'address dip switches' for each Transmitter monitoring PCB. Each PCB must have an unique address in the range B001-B099. (01 = 10000000, 99 = 10011001).
- ▶ The setting for 'B0' is already fixed, so only the setting 00-99 have to be set, (the used address range is B001-B099).
  - The address must be the same as set in the peripheral settings.
  - Example to configure address B013, set switches LSB/MSB at 1100 (3<sub>dec</sub>)1000 (1<sub>dec</sub>).
- ▶ Set the work mode switches correct: 0100 0000 or 0101 0000 (See table below for details).
  - Working with the Message Server or other encoder; SK2 = On.
  - Eventually enable the synchronisation option SK4 = On (only in multi transmitter systems).



SK	Setting	Function
1	OFF	Scanned by system = OFF
2	ON	Scanned by system = ON
3	OFF	Not used
4	ON	Multi transmitter (LF-sync)
5	OFF	Not used
6	OFF	Not used
7	OFF	Not used
8	OFF	Not used



**Note:** SK1 and SK2 must never both set to ON!  
SK2 = ON; scanning by system is expected.

To use the LBB5905 TMM, please refer to the next page: →



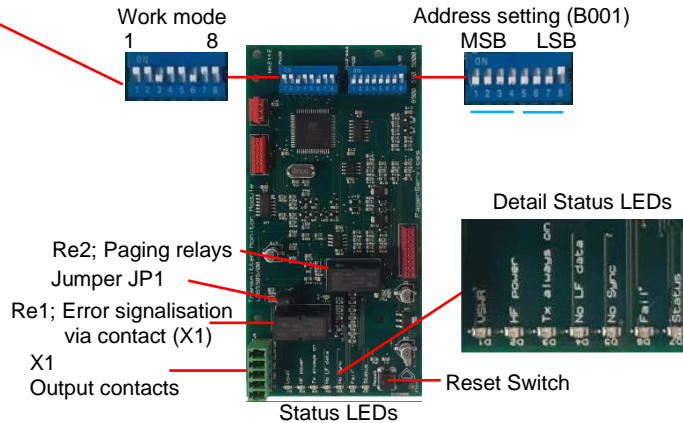
18.8.5 Settings TMM type LBB5905

- ▶ Set the 'address dip switches' for each Transmitter monitoring PCB. Each PCB must have a unique address in the range B001-B099. (01 = 10000000, 99 = 10011001).
- ▶ The setting for 'B0' is already fixed, so only the setting 00-99 have to be set, (the used address range is B001-B099).
  - The address must be the same as set in the peripheral settings.
  - Example to configure address B013, set switches MSB/LSB at 0001 0011.
- ▶ Set the work mode switches correct: (See table below for details).
- ▶ For details, refer to the installation manual for this TMM: II\_LBB5905\_TMM-V2\_En\_yyww



SK	Setting	Function
1	ON	VSWR Detection
2	ON	Loss of HF power
3	ON	OOR call detection
4	ON	Multi transmitter (LF-sync)
5	ON	HF detected while stand-by
6	ON	Short reply, no alpha in reply
7	ON	RE 1 Fail safe
8	ON	*) Extended mode

- SK1-SK7: Only selectable options if SK8 = ON
- IF SK8 is set to OFF, the unit works as described for the TMM type WSP D 40971



18.9 CRX monitoring via the Server

- ▶ System receivers (LBB6017, CRX) are prepared to report certain errors which optionally can be used to monitor the receiver(s) functionality.
  - If activated in the central receiver (CRX), it will sent periodically a status call to be monitored by the Communication Server.
  - The Communication Server can generate a technical alarm if a Central receiver sent a status call that includes a defect report.
- ▶ There are two types of errors that are detected by the system:
  - The Server expects periodically, a (sign of life) call from the CRX, which proves that the CRX is 'alive' and able to sent 'sign of life calls through the TB-lines. (This type of call is comparable with a scan call (sign of life call) from a PSμ mobile.)
    - If the Communication Server doesn't receive such call via the TB-lines, within the scan time-out time, there is probably an issue with the CRX or the TB lines. Therefore a technical alarm indicating 'Receiver not seen' will be raised.
    - If the 'sign of life call' is received in time, but the call includes an error indication, a 'Technical error receiver', including the type of defect that is found, will be raised by the Communication Server.
- ▶ Technical alarms are caused if the performance of a CRX is below expectations.

18.9.1 Preparation:

- ▶ In order to enable to detect if errors, some settings are to be set in the CRX.
- ▶ The settings in the CRX can be adapted by using the CRX configuration tool.
  - Basic settings: (to be done IN each CRX):
    - The individual unique address of each CRX, which starts always with 'B1' and it must be the same address as set in the peripheral settings, the range to be used is B101-B199.
    - Status calls; to be enabled; otherwise the CRX will NOT sent status information to the server.
    - Repeat time of the status calls; set this time in the CRX shorter than the Scan time out in the peripheral settings. As a guideline the relationship between both timings can be 1:2 or 1:3 (60 sec in the CRX and 180 sec in the server).
    - Max RF occupation time.
  - Refer to the installation manual II\_LBB6017\_en\_1536 for details.
  - In the servers' programming, for each CRX a 'Peripheral type': DP6000 RX must be configured. Refer for details to "[Configure DP6000 RX](#)"

**i** Note: In case there is an RF signal detected for a too long time, it can indicate that an (external) source is causing disturbance in the ether or a defect CRX or even a defect PS-mobile, which is continue transmitting. Such a situation can lead to a receivers disability to receive (alarm) calls from (other) mobiles.

**i** Note: The status calls from a CRX are always transmitted via the Talk-back lines. Alarm calls that are a result of a technical issue are always transmitted via the paging lines.

Continue at next page: →



18.9.2 Information in the numeric code of the status call

- ▶ In the logging data (Technical Logging) relevant technical information per CRX can be filtered .
  - The status call of a CRX starts always with address B1xx,
  - Furthermore the logged data contains numeric code, which implies status data, refer to the table below.

Numeric info digit	Error code in Status Indicator		Error code in numeric information
	Decimal	Binary	
1	64	1000000	Info related to the u-Processor in the CRX, it is an internal error (temporarily). Bit 3; Power on $\mu$ -Processor Bit 2 Low voltage $\mu$ -Processor
	32	0100000	
2	16	0010000	Bit 3; indicates a configuration error, e.g. wrong programmed frequency. Bit 2; indicates that the internal frequency (VCO) is out of lock. Bit 1; indicates an RF-error; e.g. the CRX detects disturbance by an HF field. Bit 0; I <sup>2</sup> C error; which is an (temporarily) internal error.
	8	0001000	
	4	0000100	
	2	0000010	
3	1	0000001	Bit 3; indicates that the 12V for the CRX is too low.
4		n.a.	Contains information related to the call repeat time that is programmed in the CRX (max 255s, represented by FF in digit 4 and 5).
5		n.a.	Contains information related to the call repeat time that is programmed in the CRX (max 255s, represented by FF in digit 4 and 5).

- ▶ The 'Mode-word' accompanied with status calls received from a CRX is always 80180, explanation:
  - Info contains = status data
  - System reaction to a status call: No handshake
  - Application ID = Status
  - No Alpha numeric part is present.

18.9.3 Status indicator for CRX

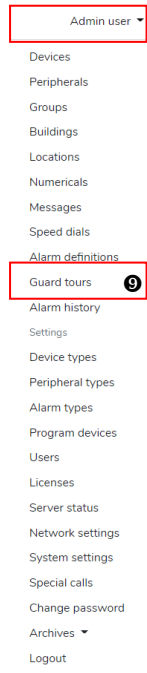
- ▶ In the 'System status' screen, the status of several system equipment can be made visible.
- ▶ If there is an error detected with a Central receiver (CRX), a binary error code is derived from the numeric info digits. E.g.: (see also table above).
  - Error code 16 indicates that the frequency is programmed wrong.
  - Error code 4 indicates that there is a RF-error.
- ▶ In case there are multiple errors detected, the digit-codes are added.
- ▶ For example; a code 20 can means that both codes 16 and 4 are detected simultaneously.





### 18.10 Guard tours

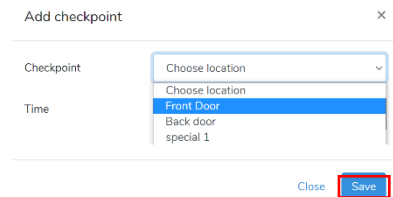
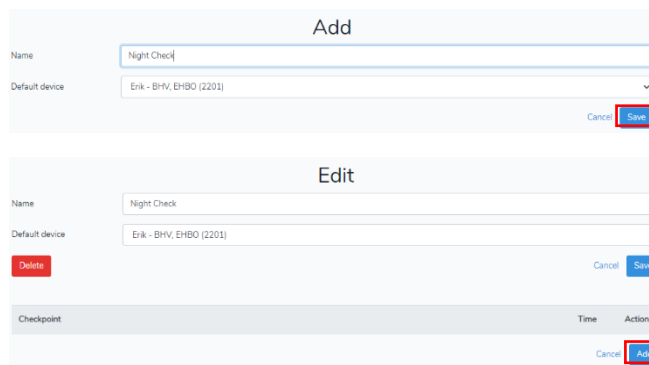
- ▶ Guard tours offers the possibility to create a group of location beacons that must be passed by a mobile (e.g. a guard) within a predefined time and a predefined sequence.
- ▶ If the time to pass 2 successive location beacons takes too long an alarm can be raised to indicate e.g. Because the a guard is in problems.
- ▶ The guard tours allows that the sequence between two successive programmed beacons can be interrupted, while during the guard tour other location beacons are detected, as long as the time between the two specified location beacons is not exceeded.
- ▶ There is no limit to the number of different guard tours that can be programmed.



**i** Note: Next to the operational function of guard tours, it can also be used for maintenance. Walk a predefined 'maintenance tour' and check if all beacons were seen.

#### 18.10.1 Create a guard tour

- ▶ Go to the tab Guard tours ⑥.
- ▶ A screen to add a guard tour opens.
- ▶ Give the guard tour a descriptive name.
- ▶ Fill in the Default device (preferred mobile) to be used to execute the guard tour.
- ▶ Click the blue save button to save the settings.
- ▶ Once saved it is possible to add 'checkpoints' to the guard tour.
  - Select the blue 'Add' button.
- ▶ A new screen opens with all possible location beacons in the system.
  - Select through the pull down menu the beacon that you want to add.
  - Fill in the maximum time that is allowed to pass the previous previous checkpoint and this (new) checkpoint.



**i** Note: To detect that 'critical' location beacons are passed multiple times during the guard tour, arrange that these are multiple times added to the check point list.

- ▶ Save the new check point.
- ▶ To add a new check point select 'Add' again, etc etc.
- ▶ If desired the sequence of the check points during the guardtour can be changed as follows: use the up/down arrows in the relevant checkpoint to move it up or down.

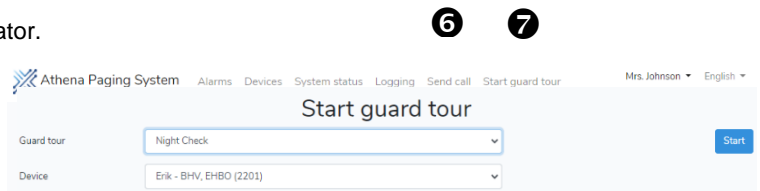


**i** Note: Be aware that mobile(s) which are used for guard tours, is/are programmed correctly, check the 'location' opcodes. (e.g. 'always transmit').

- ▶ When finished select the 'Save' button in the 'Edit' screen.

#### 18.10.2 Start a guard-tour

- ▶ A Guard tour is always started by an authorised operator.
- ▶ To start the guard tour, select the 'Start guard tour' screen ⑦.
- ▶ Select the Guard tour to be executed.
  - In this example the Guard tour 'Night Check' was selected for which initially Device 'Erik 2201' was defined.
  - If desired the preferred Device can be changed before the Guard tour is started.
- ▶ Select the blue 'Start' button to start the Guard tour.
- ▶ Once the Guard tour is started:
  - The Device that is used to execute the Guard tour, receives a message 'guard tour started'.
  - The device should go to the first checkpoint now.
  - As soon the first check point is passed, timing starts too.



Continue at next page: →






- ▶ All events during the Guard tour are listed and logged.
- ▶ A blue 'Stop' button to stop the Guard tour and a blue 'Pause/resume' button to Pause/resume the guard tour becomes visible.
  - The device that is executing the Guard tour.
  - The Next checkpoint to be detected.
  - In blue text, the time that is passed after the last check point was detected.
- ▶ A Stop and Pause button.
  - To stop the Guard tour definitve, select the blue 'Stop' button.
  - To put the guard tour on hold, select the bleu 'Pause' button.
    - To resume the Guard tour select the blue 'Resume' button'.
  - The Device that is used to execute the Guard tour, receives relevant messages:
    - Guard tour stopped.
    - Guard tour Paused/resumed.
- ▶ A (Green) timer at the right shows the remaining time to reach the next check point becomes visible.
  - If the guard tour is resumed, the Green timer is reset also.
- ▶ The guard tour ends automatically once the last checkpoint is passed.

Night Check		
Device	Erik - BHV, EHBO (2201)	
Next checkpoint	20000 - Table left	
00:00:13		
Time	Location	Description
16:03:48	10000 - Front Door	First location Front Door in tour passed
16:03:41		Night Check started by John

### 18.10.3 Guard tour registration

- ▶ Once the bleu 'Stop' button is pressed, the results of the Guard-tour are stored automatically.
- ▶ The logging of guard tours is available through the pull down menu  opening the 'Archive', and select the option Guard tours archive.
- ▶ For instruction to obtain logged data, refer to chapter: ["Guard tours archive"](#)

### 18.10.4 Unsuccessful Guard tour

In case the timing in the guard tour expired and no correct location data is reported, a 'Guard tour alarm' is raised. This enables the operator to take appropriate actions.

### 18.10.5 Guard tour alarm

- ▶ If the time between the latest reported location beacon and the new to be reported location beacon is expired a 'Default Personal Security alarm' or, if programmed an specified 'Guard tour' alarm will be raised e.g. because;
  - Location beacon is defect (not able to transmit its address).
  - When the location beacon's address is not set in the Communication Server.
  - The range of a location beacon is not sufficient.
  - The new checkpoint is not passed in time.
- ▶ A Default Personal Security alarm is always linked to a guard tour.
  - If not further specified this 'Default Personal Security alarm', is in most cases sufficient.



Note: A Default Personal Security alarm for a Guard tour failure is activated when the timing in the Guard tour expires. If a specified 'Guard tour alarm' is desired, the tab ["alarm definitions"](#) offers the option to create a specified 'Guard tour' alarm.

## 18.11 Location Monitoring

- ▶ Location Monitoring is used to monitor the functionality of the location beacons.
- ▶ All mobiles will report the most recent location information to the system when the mobile:
  - Is in alarm.
  - Is scanned by the system.
  - Is programmed to 'always transmit'.
  - When locations with specific addresses are detected.
  - When a guard tour is executed.
- ▶ There are 2 methods to monitor correct functionality of location beacons:
  - Location beacon not seen for a too long time.
  - A location beacon reports code F7XXX.

Continue at next page: →





18.11.1 Location beacon not seen for a too long time

▶ If a location beacon LBB6070/00 (old beacon) or LBB6071/01 (Main DLT) is not seen for a too long time. With this way of location monitoring, the system checks periodically the last time that a location beacon was seen earlier with the time that new location data is received, so the time-difference between the last time seen and the new location information can be calculated.

If the time between the latest report and 'max time not seen' is expired a 'Default technical error' or, if programmed an specified 'Location not seen' alarm will be raised to indicate that there is some problem.

Problems can occur when e.g.

- Location beacon is defect (not able to transmit its address).
  - When the location beacon's address is not set in the Communication Server.
  - The range of a location beacon is not sufficient.
  - The 'max time not seen' setting is too short. (e.g. the beacon is at a position where not often a mobile will pass).
- ▶ To activate the 'Location not seen' monitoring; set the 'max time not seen'. F.i.: to Disable = 0, 255 stands for 255 hours.
- If this time (Hours) is expired while a location is not being detected within this time, a technical alarm is raised.
  - If not further specified this is a 'Default technical alarm', which is in most cases sufficient.

**i** Note: A Default technical alarm for a location beacon that was not seen for a too long time is activated while the 'max time not seen' is set unequal to '0'. If a specified 'Location not seen alarm' is desired, the tab "[alarm definitions](#)" offers the option to create a specified 'Location not seen alarm'.

18.11.2 Location beacon reports code F7

- ▶ A Main DLT (LBB6071/00) can be programmed such that in case of defect it transmits an error code F7XXX. The first 2 MSDs of its original programmed address changes into 'F7' in case antenna-, internal- or blue tooth errors occurs.
- Be aware that this method will work only as long as the location beacon is able to transmit its (wrong) location data.
  - If the mobiles can be programmed to 'always transmit if a location starts with an 'F'', you are able to find quicker location transmitters that has an 'F7-error'.
  - All location beacons that reports with an address F7XXX are potentially defect.
  - At the server a 'Default technical error' or, if programmed an specified 'Location beacon error' will be raised.

**i** Note: When a code F7XXX is detected, a 'Default technical alarm' appears always, while it is hard coded in the Software, you cannot switch this option 'off'. If a specified 'Location beacon error' alarm is desired, the tab "[alarm definitions](#)" offers the option to create a 'Location beacon alarm'.





18.12 System examples

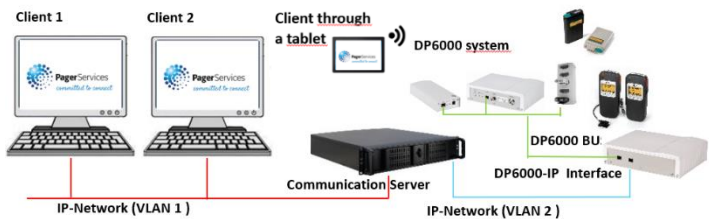
18.12.1 Basic system

- ▶ Only one site with one local DP6000 system and one client.



18.12.2 Multi-client system

- ▶ Only one site with one local DP6000 system and multiple clients.
- ▶ For this system setup a Multi-Client licence(s) is needed
  - Depending on the IT-infra also a clients using a WIFI tablet are possible.



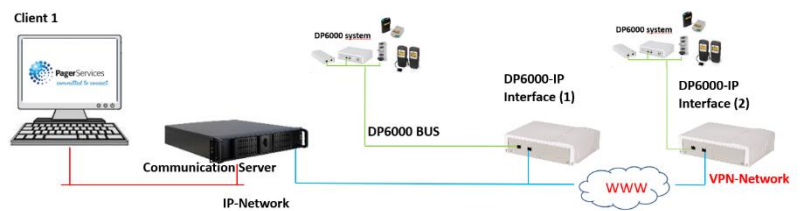
18.12.3 Multi-site system 1

- ▶ Multiple DP6000-IP interfaces for several (independent) DP6000 subsystems are operational.
- ▶ For this system set-up also a Multi-Site licence is needed.
- ▶ In this example all equipment works in the same IP-subnet.



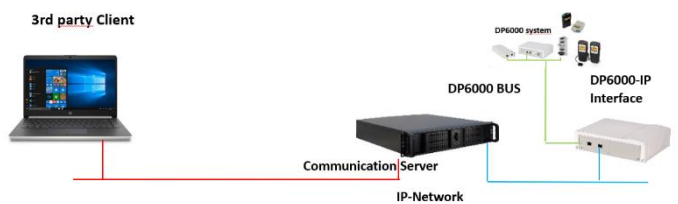
18.12.4 Multi-site system 2

- ▶ Multiple DP6000-IP interfaces for several (independent) DP6000 subsystems are operational.
- ▶ For this system set-up also a Multi-Site licence is needed.
- ▶ In this example Multiple sites with multiple geographical separated DP6000 systems, working through different sub-nets or through a secured VPN IP network.



18.12.5 3<sup>rd</sup> party connection/BMS

- ▶ It is possible to connect a 3<sup>rd</sup> party interface with the Communication Server.
- ▶ This enables the 3<sup>rd</sup> party to create his own client environment or to integrate functions in a Building Management System.
- ▶ For this system set-up also a 3<sup>rd</sup> party licence is needed.
  - A special communication protocol (API) is available on project basis.



18.12.6 Server as Master/Slave

Reserved for future options.

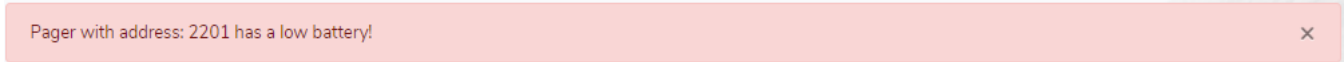


## 19 Technical Alarms

- ▶ If configured by the system administrator, the functionality of the equipment in the system (interconnections and/or functionality) can be monitored. If technical errors occurs, a technical alarm can be raised.
- ▶ Depending on the system programming technical errors are reported through several methods:
  - A notification
  - A call (message) to specific mobiles (e.g. to inform technicians)
  - Indication via the status indicator.
  - Through a technical alarm in the alarm screen.For an overview of technical alarms and eventually remedies refer to chapter [“Technical alarms and remedy”](#).

### 19.1 Technical notification


A technical notification appears e.g. when a mobile reports a ‘low battery’ see as example [“Low battery indication”](#)



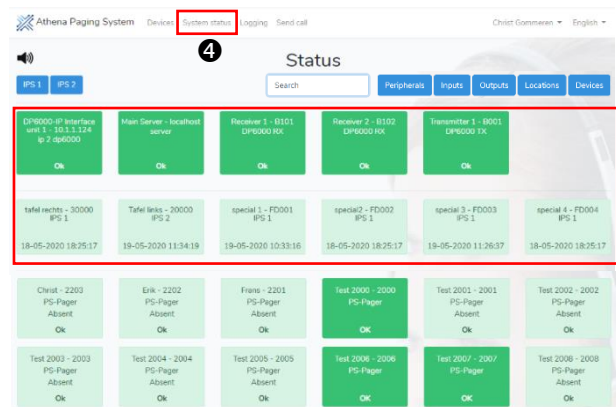
### 19.2 Technical calls

At several places in the system configuration it can be set if a predefined IP-DP6000 call needs to be transmitted when specific technical errors appears.

### 19.3 Status screen

If authorised, an operator can open the ‘System status’  screen.

- ▶ At several places in this manual it is described that the color and the text in the status indicator shows if the equipment is working well or not.
  - Usually a status indicator is rose/red when there is an issue with the equipment.
  - Just click at the status indicator to enter the alarm screen to check the technical alarm.
    - Technical alarms can be reset temporarily by the operator but reoccurs with the next system scan.
    - If the root cause is solved the alarm will be reset automatically.





## 20 Maintenance

### 20.1 Introduction

For system maintenance a system administrator/dealer can log in and carry out several activities, among others:

- ▶ Check Firmware and software versions
- ▶ Add, change or remove operational settings.
- ▶ Check logfiles.
- ▶ Manage settings to follow up alarms
- ▶ Manage technical alarms
- ▶ Manage user authorisations
- ▶ Etc. etc.

### 20.2 Firmware and software versions

- ▶ To check system software version and firmware versions open the 'Licenses' option in the main menu.
  - An overview with available licences and active software versions is displayed.
- ▶ The firmware version of the DP6000-IP Interface can be checked by following the instructions described in chapter ['Software versions menu'](#).
  - To update the software at the DP6000-IP interface refer to chapter ['Update firmware DP6000-IP Interface'](#).

### 20.3 Network testing

For options and hints to check or test the IP infrastructure between the Communication server and other devices, refer to chapter ["Network test-tools \(build in\)"](#) and ["Alternative Network test-tools"](#).

### 20.4 Remote Maintenance

Due to the fact that the Communication Server is accessible (by opening a web page) through an IP-infrastructure, local as well as remote maintenance is possible. Inform with the end-customer about their local IT-policy and possibilities to have remote access.



Note: For 3<sup>rd</sup> level maintenance where R&D involvement from Pager Services is required, we recommend to allow a secure VPN connection if needed.

### 20.5 Set time and date (in the Server PC)

All date and time references are derived from the Communication Servers' clock settings.



Note: Be aware that the time/date displayed in separate 'client' PCs/laptops can deviate from the time/date used by the Server PC. To prevent this, use an NTP server or other common synchronised time reference.

#### 20.5.1 Set time and date (ESXi)

- ▶ If the Server PC cannot reach a synchronized time reference it might be needed to set the time manually.
- ▶ Be aware that in such situations that summer time/wintertime is not changed automatically.
- ▶ The time in the server PC has no relation with the time/date of external client PC's of course.
  - Open a web browser and enter the physical IP address of the server. The physical IP address can be obtained from the local IT manager or connect a monitor to the server, the screen will display the IP address.
  - When OK, the VM ware ESXi screen is opened and asking for a User name and Password.
    - U: root
    - P: Serial number of the server PC plus '!' f.i. H52ZRX! (example).
  - Select the blue 'log in' button.

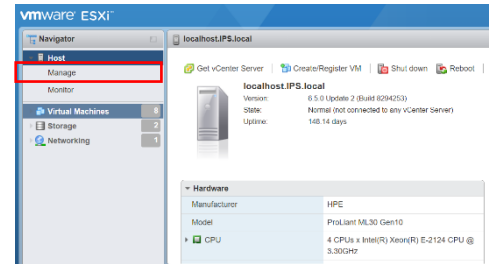


Note: The physical IP address can be seen on a monitor that is connected with the server-PC. In stand-by mode the monitor shows some text that includes the physic IP address.

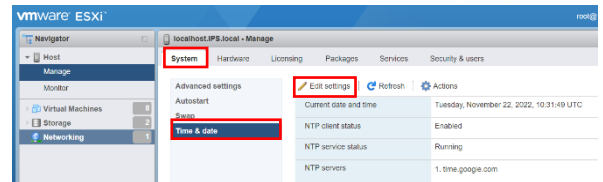




- ▶ A new screen appears:
  - Select 'Manage'.

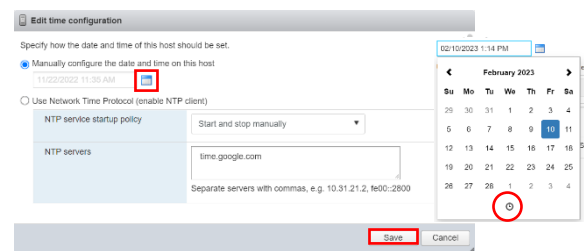


- ▶ The 'manage screen' appears:
  - Select the tab 'System'
  - Select 'Time & date'.



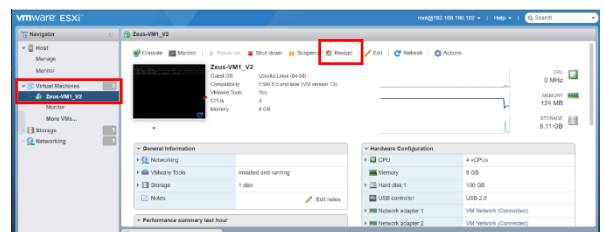
- ▶ If you want to change some settings:
  - Select 'Edit Settings'.

- ▶ A screen to set the time/date appears.
  - For 'manual settings' select the bullet 'manually configure... on this host'. Select the 'Calendar icon' and change the date if desired.
  - Select the small 'clock' icon to change the time.
    - Fill in the really desired time (don't calculate).
  - For automatic time/date settings select the bullet 'Use NTP'.



- ▶ When ready select 'Save'.

- ▶ Once finished, restart the (relevant) virtual machine:
  - Select 'Virtual Machines'.
  - Select the virtual machine to be restarted. (in this example the virtual machine is 'Zeus-VM1\_v2').
  - ▶ Select the 'Restart' button. ('Restart' takes approx. 3minutes).



**i** Note: Due to the restart procedure, all logged in operators are logged out, they must log-in themselves again!

- ▶ Close the web browser to leave the VM ware ESXi environment.
- ▶ Log in as operator to restart the application software; go to ["Restart the Server \(Software reset\)"](#) to reset restart the application software.
- ▶ To check if the modification of the time or date was successful, go to: ["Incoming calls/line monitoring"](#). If successful, all new calls will have the new desired time as from now on.
  - After a while the system is synchronised such, that the new date/time is also displayed in the history column in the 'Sent call' screen. If successful, it is possible to see a 'hick-up' or 'hick-down' in the time/date can be seen here.

**i** Note: When the Server is connected to an IP network that is able to reach an external time server, then the time cannot manually be changed. Therefore remove the network connection from the server PC.

**i** Note: When the Server is NOT connected to an IP network that is able to reach an external time server, then the seasons time (summer/winter time) is not changed automatically. This might cause that the time settings between client PC's and the server are out of sync.

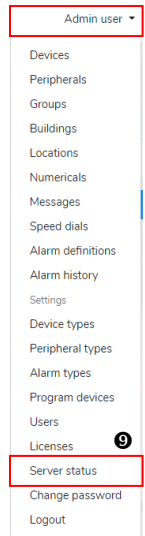


### 20.6 Server Status screen and Server backup

- ▶ This screen is only available if a user is allowed to access Server status menu, through the 'Role' settings.
- ▶ The Server status screen is build up out of several sections which shows specific system items:
  - Server status
  - Incoming calls
  - Server logs
  - Backup- and restore the database (programmed settings at the Communication Server)

#### 20.6.1 Server status



- ▶ In the server status screen some interesting information can be seen:
- ▶ For instance if the server is **active (running)**, (see picture below)



- ▶ This status is valid as from Sunday 2022-10-09 07:45:25 (YYY-MM\_DD hh:mm:ss)
- ▶ At this way it is represented when the was (re)started 5 days ago.
- ▶ If you are asked, for analyses by an administrator, sent a screenshot of the system status.
- ▶ Warnings are e.g. received reactions from unknown devices.
- ▶ Errors are e.g. data errors, DP errors, IP errors.
- ▶ All shows all technical log data
- ▶ With the Blue Restart button a soft-restart (application software) can be executed.

#### 20.6.2 Restart the Server (Software reset)

- ▶ The server's software can be restarted by selecting the blue Restart button in the server status screen.
- ▶ It takes approx. 15 seconds to restart the software.
- ▶ The Server PC itself (hardware) is not restarted by this action.

 Note: Using the blue 'Restart button' in the Server status screen , this results in a SW-reset only. It takes approx. 15 seconds to complete a Soft-reset. Be aware that after some changed configurations settings a Soft-reset is needed.

#### 20.6.3 Incoming calls/line monitoring

- ▶ It is possible to monitor calls in real-time, that are transmitted and received at the server. Therefore some data is made visible of the very most recent call, see the example below.
  - Time: indicates the current time.
  - Address: the unit address that initiates the call or where the call is sent to.
  - Bleep: the bleep code that is part of the call.
  - Message: the alphanumeric text that is part of the call (if not empty).
  - Modeword: the Modeword that is part of the call
  - Line: L = Paging lines, transmitted and T = Talk-back lines, received.
  - Source: the DP6000-IP interface or other source that processes the call.

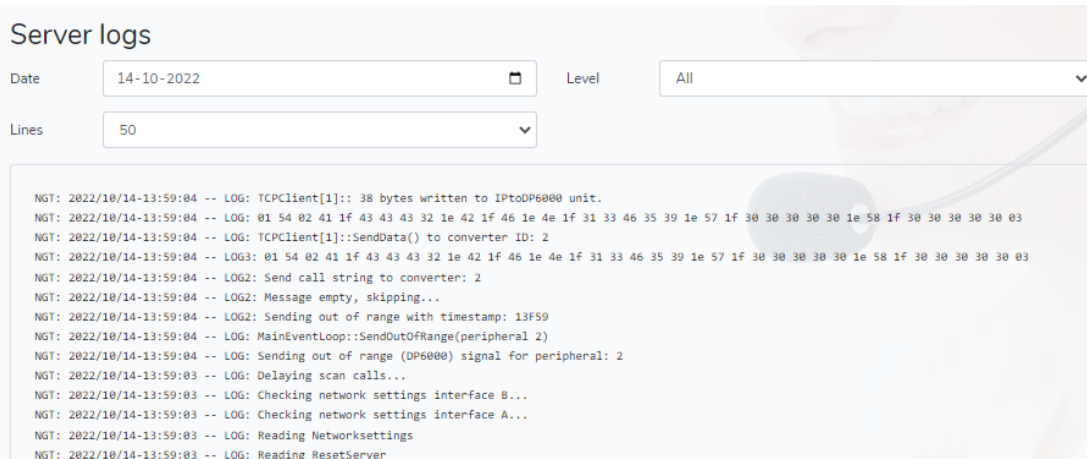
#### Incoming calls

Time	Address	Bleep	Numerical	Message	Modeword	Line	Source
13:51:23	B001	0	00000			L	DP6000-IP Interface unit 1 (ID: 2)
13:51:22	3001	0	AFAFA	PSmicro04Table leftbuilding IPS 1 second_manual_	5020C	L	DP6000-IP Interface unit 1 (ID: 2)
13:51:18	B001	0	08000	ANTTENNE ERROR	00006	L	DP6000-IP Interface unit 1 (ID: 2)
13:51:17	B001	1	05000	HF LEISTUNG ZU GERING	00006	L	DP6000-IP Interface unit 1 (ID: 2)
13:51:16	B001	0	00000			L	DP6000-IP Interface unit 1 (ID: 2)





## 20.6.4 Server logs



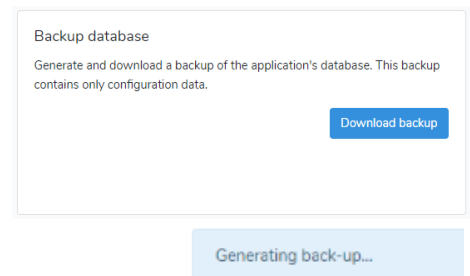
- ▶ The Server logging can contain a lot of technical information like:
  - Warnings e.g. received reactions from unknown devices.
  - Errors e.g. data errors, DP errors, IP errors.
  - All shows all technical log data.
- ▶ If you are asked, for analyses by an administrator, send a screenshot of the server logs:
  - Select the date to be covered.
  - Select the level: (All, Errors only or Warnings only).
  - Select the lines (50,100, 250, 500 or 1000).

## 20.7 Manage the database (Communication server).

- ▶ Separate from the possibility to export a CSV file from the mobiles (devices) and Location beacons (Location), the complete database of the settings in the Communication Server can be back-upped (Downloaded) or restored (Uploaded).

### 20.7.1 Back-up database

- ▶ To create a back-up, go to the lower part of the service status page.
  - Select the blue 'Download backup' button.
  - As a result an indication 'Generating back-up...' appears and
  - A file with extension .ZIP will be created, it contains all programmed data.
  - The format of the ZIP file is 'back-upversion-22-2023-01-27-142646.zip' which is a date/time indication (VV-YYYY-MM-DD-hhmmss).
- ▶ If desired give the file a descriptive name however:
  - Keep the 'VV' in the filename!
  - Keep the extension '.ZIP'!
- ▶ Navigate to the place to store the file.
  - This ZIP file itself **cannot and must not** be opened nor its content may be modified!
- ▶ Note that files that contains 'alarm history', logfiles and other archives-data are is NOT included in this back-up.
- ▶ To restore an earlier created back-up, go to "[Restore database](#)".



**i** Note: It is advised to create a new back-up:

- ▶ After changed settings. (this will prevent loss of 'forgotten' settings).
- ▶ After firmware updates. (this is to make sure that the data base is compatible with you running SW version).

**i** Note: In the file name of the downloaded database the characters 'VV' represents the version of the database. This information is important to check the compatibility of the database when you want upload it later.

**i** Note: All log files and archives are NOT part of the back-up. Licences and drawings belonging to locations are included in the back-up

Continue at next page: →





20.7.2 Restore database

**i** Note: Restoring a database overwrites all existing settings, make sure that the selected back-up:

- Is up to date!
- Has the same version 'VV' as the currently installed database!

- ▶ To check if the database is useable to be uploaded, first check if the files' compatibility:
  - If the download procedure is followed well, there first characters of the file contains the version information:
  - Example: Filename: 'back-upversion-22-2023-01-27-142646.zip. In this example the version of the database is 2.2.
- ▶ In the 'license screen' the version of the currently installed database is written: (go to "licenses" to open the license screen).
- ▶ In this example the filename contains '22' and the licence overview shows 2.2: Result: the file is compatible.

Software version				
	Version		Build date	Install date
database	2.2		24-01-2023 12:27	24-01-2023 12:27
IPDP6000.2	R Sw 00.00.25 R	26-01-2022	24-01-2023 09:02	24-01-2023 09:02
server	V1.60		26-01-2023 09:29	26-01-2023 09:32
ui			27-01-2023 09:02	27-01-2023 09:02

**i** Note: NON compatible files can only be used if PagerServices gave such instructions.

- ▶ To import an earlier (compatible) created back-up, of the database, go to the lower part of the service status page.
- ▶ There is a screen visible as depicted at the right.
- ▶ Note the warning: uploading a database will overwrite your existing settings!
- ▶ If you want to continue:
  - Select the blue 'Upload backup' button.
  - Again a warning text appears.
- ▶ If you want to skip the back-up action, select 'Cancel'.
- ▶ If you are sure to continue, press the button 'Select File'.
  - Navigate to the place where the back-up has been stored.
  - Select the desired back-up file.
  - At the place of 'No File Selected', the name of the loaded file will appear.
  - Select the RED 'Upload back-up data to Server' button.
  - Depending on the amount of data it will take some time.
- ▶ To make the uploaded database effective, the server must be restarted. For details refer to chapter: ["Restart the Server \(Software reset\)"](#).

**i** Note: Once the Upload is finished, restart the servers' software.

- ▶ Error indications:
    - If no file is selected or when the selected file is not the ZIP format.
- ⚠ Check the error messages below:**

  - The backup file must be a file.
  - The backup file must be a file of type: zip.

20.7.3 Back up of DP6000-IP Interfaces.

- ▶ Note down: the IP settings as set in the DP6000-IP interface(s), in a document, these settings are not backed-up.
- ▶ The following items are stored in the databases of the Communication Server:
  - All Outputs, Inputs, ESPA ports
  - Predefined IP-DP6000 calls.
  - The licence link between with the Communication Server.
- ▶ Therefore a back-up of this data is made during the 'back-up' procedures as described in the previous chapters.

Continue at next page: →



20.8 Modeword explanation

- ▶ This information is meant for trained technicians who are able to interpret the content of the Modeword!
- ▶ When DP6000 calls are transmitted in the system, one of the parts in the calls is the so called Modeword.
  - The complete Modeword and some bits of it are also visible in several log data which can be displayed.
- ▶ The Modeword contains in total 5 nibbles (4 bits/nibble).
  - Nibble: 1 2 3 4 5
  - Bit: 1234 1234 1234 1234 1234

Note: Not all below described options might be implemented, check with IPS what is relevant. This depends also on the development status of equipment. Furthermore IPS reserves the right to implement applications in another way.

- ▶ Nibble 1;
  - Bit 1: Speech flag: 1 = Speech call.
  - Bit 2: Listen in flag: 0 = Speech is Off for not called mobiles.
  - Bit 3: Microphone flag: 1 = Microphone On, e.g. for use 'listen in' function.
  - Bit 4: Urgent flag: 1 = Overrule 'silent mode' for mobiles.
- ▶ Nibble 2;
  - Bit 1: Info status flag 0 = numeric info is display information, 1 = status info.
  - Bit 2: Message to memory flag 0 = Alphanumeric info is stored in memory, 1 = not stored; then it is SIC status.
  - Bit 3: System ID Not used in combination with the Communication server. (Default value is 0).
  - Bit 4: System ID Not used in combination with the Communication server. (Default value is 0).
- ▶ Nibble 3;
  - Bit 1: Handshake ID See table 1 below.
  - Bit 2: Handshake ID See table 1 below.
  - Bit 3: Handshake ID See table 1 below.
  - Bit 4: Application ID See table 2 below.
- ▶ The decimal value of some Handshake ID's and Application ID's is also displayed in the exported logging.

**Table 1: Handshake ID**

Handshake ID	Decimal value	Action	Explanation	Examples
000	0	No handshake.		e.g. Used for normal calls
001	1	Handshake; For an auto reply	An automatic reply is requested from the receiving side. If no reply is received in time, a handshake ID 011 is sent.	e.g. used for Scan calls, mobile on/off, alarm calls.
010	2	Handshake; For a manual	A manual reply is requested from the receiving side.	e.g. used for sign of life calls.
011	3	Handshake; Repeated auto reply	An automatic reply is requested from the receiving side.	If no answer was received on time from HS-ID 001
100	4	Not used		
101	5	Handshake; Auto reply	The receiving side send an automatic reply to handshake ID 001 or 011.	Used as automatic reply to an earlier request
110	6	Handshake; Manual reply	The receiving side gave a manual reply to handshake ID 010	Used as manual reply to an earlier request.
111	7	Handshake; Reply while in rack	The PS-Pager replies to handshake ID 001 or 011 while it is in placed in a charge rack.	

**Table 2: Application ID**

Application ID	Decimal value	Action	Explanation	Examples
000	0	Standard DP6000 call.	See Modeword digit2/bit3, to interpret the numeric info.	e.g. for speech calls, and to display information.
001	1	System Info Call (SIC).	See Modeword digit2/bit3, to interpret the numeric info. and/or the alphanumeric part.	e.g. used for Mobile on/off in/out rack.
010	2	Dial Call	See Modeword digit2/bit3, to interpret the numeric info. Alpha message contains dial information	Used to dial mobile to mobile or contact operator.
011	3	Personal Security Call (PS call)	See Modeword digit2/bit3, to interpret the numeric info (PS status). Alpha part contains a message.	e.g. used to send for alarm calls to the server.


Continue at next page: →





100	4	Location Call	Bleepcode: value of requested location. See Modeword digit2/bit3, to interpret the numeric info (last detected location beacon)	e.g. used for location updates, when a mobile is in alarm.
101	5	PSlocation call (PSLOC)	See Modeword digit2/bit3, to interpret the numeric info (PS status). Alpha part contains Location and PS status.	Used for Alarm calls that includes location info.
110	6	Status Call	See Modeword digit2/bit3, to interpret the numeric info (PS status).	Used for status info about TX or CRX equipment.
111	7	Not used		

- ▶ Nibble 4;
  - Bit 1: Handshake ID                      See table 2 above.
  - Bit 2: Handshake ID                      See table 2 above.
  - Bit 3: # Of alphanumeric blocks        See note below (MSD).
  - Bit 4: # Of alphanumeric blocks        See note below.
  
- ▶ Nibble 5;
  - Bit 1: # Of alphanumeric blocks        See note below.
  - Bit 2: # Of alphanumeric blocks        See note below.
  - Bit 3: # Of alphanumeric blocks        See note below.
  - Bit 4: # Of alphanumeric blocks        See note below (LSD).

 Note: One alpha block contains 4 characters, so if the last nibble shows a '6', it represents a message length of 24 Characters. This is the most common value. A zero '0' means that there is no alpha message in the call. The theoretical max. length of an alpha message can be 2<sup>5</sup> blocks = 20 blocks, representing 80 characters.



### 20.9 Update firmware DP6000-IP Interface

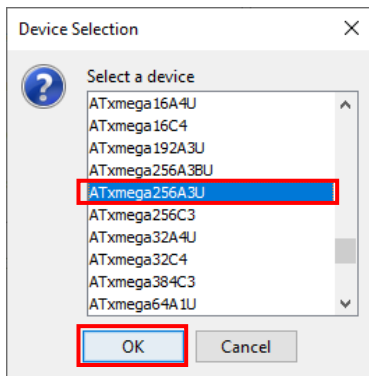
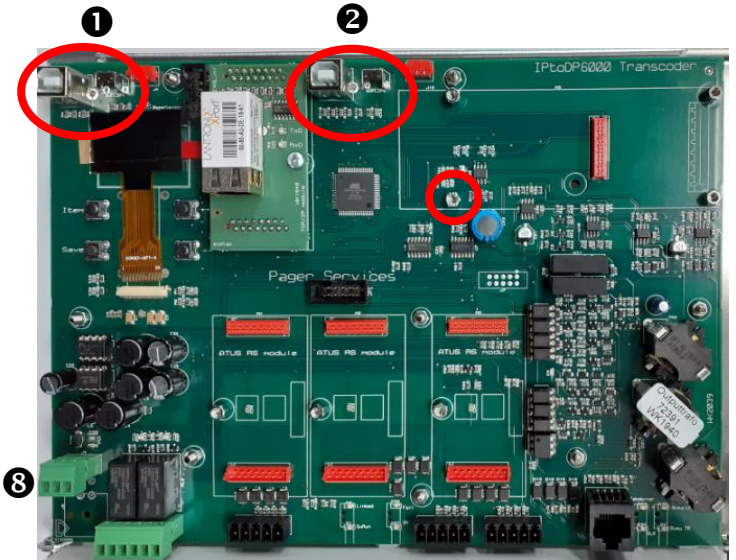
**i** Note:  
The DP6000-IP Interface contains 2 u-Processors each with a own specific firmware package.  
In this description they are described as Processor L and Processor R.

#### 20.9.1 Preparation

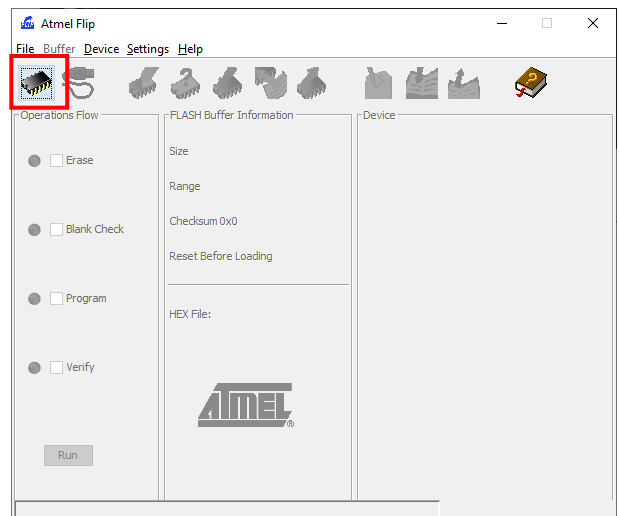
- ▶ Make sure that the driver software Atmel Flip 3.4.7 is installed at your laptop.
- ▶ Make sure that the power **3** is disconnected from the DP6000-IP interface.
- ▶ Make sure that no USB Cable is connected with the USB connectors.
- ▶ Make sure that the firmware for Processor L and Processor R are present in a directory to find it back easily.

#### 20.9.2 Upgrade instructions

- ▶ To Upgrade Processor **L**
- ▶ There is no power **3** connected, the unit is off!
  - Press and hold the switch next to USB port **1**
  - While holding the switch, connect the power supply at connector **3**.
  - After 2 seconds the switch can be released. The processor has entered the boot mode. Therefore the upgrading procedure can started.
- ▶ Connect the USB cable between your laptop and USB connector **1**
- ▶ Start the driver software at your PC (Atmel Flip 3.4.7).
- ▶ Select the 'target device' at the upper left corner.



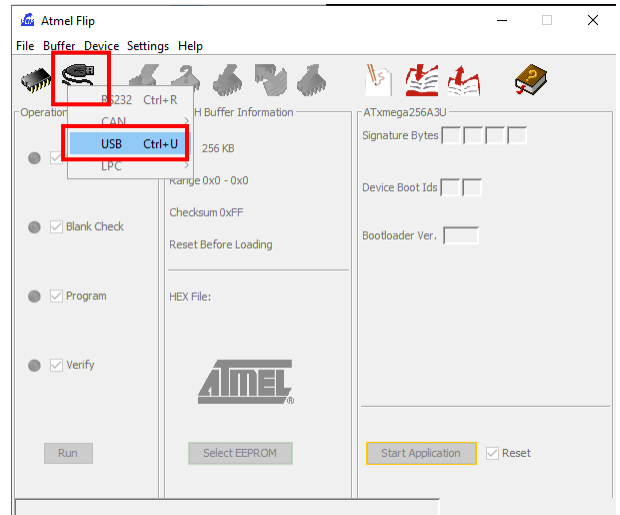
- ▶ Select 'ATxmega256A3U and click 'OK'.



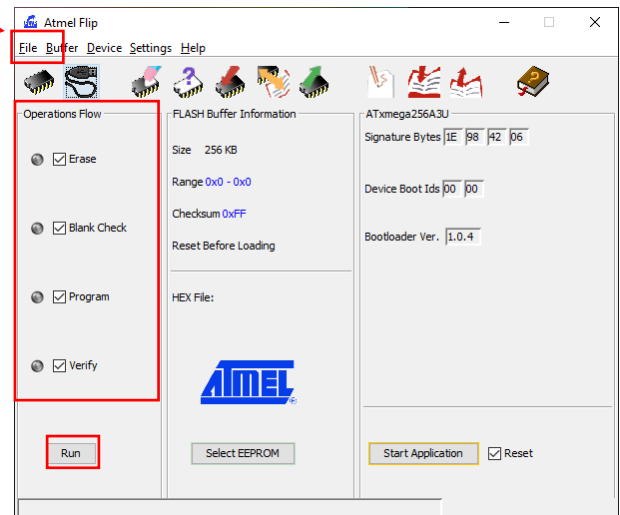
Continue at next page: →



- ▶ Select the 'USB' icon.
- ▶ Select 'USB' (or Ctrl+U).



- ▶ The screen as depicted at the right appears:
- ▶ Select 'File'.
  - Then select 'Load HEX file'.
  - Navigate to the directory where the firmware was stored earlier and select the FW file to be used for the upgrade:
    - For Processor L use:  
**L**\_IPtoDP6000\_<version ID><date>.hex
    - For Processor R use:  
**R**\_IPtoDP6000\_<version ID><date>.hex
- ▶ Check if all 4 the boxes in the operations flow are checked;  (Erase, Blank Check, Program and verify).
- ▶ Select 'Run' to start loading the new firmware.



- ▶ If the action is successful all bullets in the 'operations flow' should get a green color.
- ▶ Remove the power supply ③.
- ▶ After 5 seconds, reconnect the power supply to start the unit in 'normal mode'.

▶ **To upgrade the firmware for u-Processor R:**

- ▶ Carry out the steps as described from ["upgrade instructions"](#) but now for u-Processor R, which means a.o.:
  - Make sure that the Power supply ③ is disconnected from the DP6000-IP interface.
  - Repeat all the above steps using the switch next to USB port ②
  - Use firmware file '**R**\_IPtoDP6000\_<version ID><date>.hex'

**i** **IMPORTANT:**

- ▶ Adapt the server settings to inform the Server about the new FW version for uP-R, refer to: ["FW version"](#).
- ▶ Reset the server software after FW-updates in the DP6000-IP Interface!, refer to ["Restart the Server"](#).



## 21 Troubleshooting

### 21.1 Remember in case of issues:

- Not sufficient Licences will limit functionality; check if there are enough/correct licences activated.
- Is it possible to send calls by using only the DP6000 IP interface? → test functions menu
- Check the IP network, for hints/tips refer to "[Network test-tools](#)" or "[Alternative Network test-tools](#)".
- Continue call with Pagers, to check if the issue is at the receiving- or transmitting- side of the system.
- Test RX/TX with PS pager to check if the server sends/receives calls from/to a PS pager.
- ESPA ports and input contacts works also without server.
- Restart the Servers' software if needed (software reset takes a few seconds)

### 21.2 Technical alarms guidelines

- ▶ If there is a fault detected in the system, the Communication Server reports this via the screen 'System status'.
- ▶ Be aware that an operator/technician must be authorised to see and/or handle alarms.
- ▶ If programmed, and not blocked by technical limitations, a call can be sent to pagers e.g. to inform to the technical department.
- ▶ The most obvious reasons of technical alarms are explained in the table below. Note that the list might not be complete!
- ▶ Once the reason of the technical fault is resolved, the error indication/alarm will disappear automatically.

Note: A technical alarm can indicate essential loss of functionality and must be addressed immediately.

#### 21.2.1 Technical alarms and possible remedies

Alarm type:	Activation trigger/suggestions:
• Auto-scan error	<ul style="list-style-type: none"> <li>• If no reply from a mobile to an automatic scan call is received in time.                             <ul style="list-style-type: none"> <li>○ The mobile and/or the Communication Server cannot reach each other.</li> <li>○ This can be e.g. caused by a defect mobile or the central equipment or a lack of HF-coverage.</li> </ul> </li> </ul>
• Manual-scan error	<ul style="list-style-type: none"> <li>• If no reply on a 'sign of life' call is received in time.</li> <li>• Next to the above possible causes, some other reasons can be:                             <ul style="list-style-type: none"> <li>○ The user did not hear the manual reply request or is not able to give the manual reply</li> </ul> </li> </ul>
• Technical IP	<ul style="list-style-type: none"> <li>• A DP6000-to IP interface (or another IP controlled peripheral) has lost the IP connection with the server.</li> <li>• Check if the IP communication between Server and DP6000-IP Interface(s) or other IP-devices works:                             <ul style="list-style-type: none"> <li>○ IT infrastructure not OK. (e.g. lack of IT-authorisation)</li> <li>○ IP-settings not correct.</li> <li>○ Lose cabling.</li> <li>○ Defect IP ports/switches.</li> <li>○ Sent a 'ping' commands, and check if there are 'answers' received. Refer to chapter "<a href="#">Alternative Network test-tools</a>" for help if needed.</li> </ul> </li> </ul>
• Database error	<ul style="list-style-type: none"> <li>• A database error this error is automatically generated (hard coded), reasons can be:                             <ul style="list-style-type: none"> <li>○ The database finds a programming fault.</li> <li>○ The server cannot <u>reach</u> the data base.</li> <li>○ To trace back in the system status logging, check on a message 'Database access error'.</li> <li>○ Contact IPS to solve/investigate this error alarm.</li> </ul> </li> </ul>
• Technical server	<ul style="list-style-type: none"> <li>• A Technical server error is automatically generated (hard coded), reasons can be:                             <ul style="list-style-type: none"> <li>○ The database is corrupt or a there is a programming fault.</li> <li>○ The server cannot <u>read</u> the data base.</li> <li>○ To trace back in the system status logging, check on a message 'Database read error'.</li> <li>○ Contact IPS to solve/investigate this error alarm.</li> </ul> </li> </ul>
• Technical DP_LF	<ul style="list-style-type: none"> <li>• Occupation time (OV) of the paging line is longer than the programmed time in the peripheral settings.                             <ul style="list-style-type: none"> <li>○ Check if a specific DP6000-IP interface is causing this (defect?)</li> <li>○ Check the programmed setting, 10 seconds is a practical value.</li> <li>○ Check the DC levels on the paging lines.</li> </ul> </li> </ul>
• Technical DP_TB	<ul style="list-style-type: none"> <li>• Occupation time of the talk-back line is longer than the programmed time in the peripheral settings.                             <ul style="list-style-type: none"> <li>○ Check if a specific CRX is causing this error. (defect due to lightning?)</li> <li>○ Check the programmed setting, 60 seconds is a practical value.</li> <li>○ Check if there are RF-signals in the air that cause the occupied TB-line.</li> <li>○ Check the DC levels on the TB-lines.</li> <li>○ Sometimes a defect mobile is the cause of too long occupied TB-lines.</li> </ul> </li> </ul>
• Technical error LF/TB	<ul style="list-style-type: none"> <li>• There is simultaneous a Technical DP_LF and Technical error LF/TB detected.</li> </ul>

Continue at next page: →



<ul style="list-style-type: none"> <li>Location beacon not seen</li> </ul>	<ul style="list-style-type: none"> <li>The server can be programmed such that a location beacon should be reported to the system in a certain time (Max time not seen).</li> <li>If a location beacon is not reported within this time, there might be an issue with the location beacon and a technical error is generated.             <ul style="list-style-type: none"> <li>The reported error will be reset as soon the location beacon is 'seen' again.</li> <li>Check if the relevant location beacon is transmitting its beacon data.</li> <li>Check if the range of the beacon is adjusted well.</li> <li>Check if the time set as 'max time not seen' fits with the chance that the beacon is passed by mobiles.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Location beacon error</li> </ul>	<ul style="list-style-type: none"> <li>The main DLT can be programmed such that the address changes in a format 7FXXX in case the DLT detects a defect. If such location address is signaled by the server, there might be an issue with the location beacon and a technical error is generated.             <ul style="list-style-type: none"> <li>Check if the relevant location beacon is working well.</li> <li>Check if the antenna type is configured correct and is working well.</li> <li>Check if the coverage range of the beacon is adjusted well.</li> <li>In the logging data, a beacon error might be found due to address 7FXXX, which might help to help to locate the bacon that causes the error.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Technical error receiver</li> </ul>	<ul style="list-style-type: none"> <li>A Central receiver (CRX) can be set such that it send periodically a sign-of-life call to the central, if this call includes an error code, a 'Technical error receiver' is generated by the system.             <ul style="list-style-type: none"> <li>Reasons for such error call are described in chapter "<a href="#">CRX monitoring via the Server</a>".</li> <li>Check the CRX that causes the error. (each CRX has an individual address like B1xx.)</li> <li>Check the phase of the TB-lines.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Receiver not seen</li> </ul>	<ul style="list-style-type: none"> <li>The Server can be programmed such that it should receive a periodical sign-of-life call from a Central Receiver (CRX). If this call is not received from a CRX within the scan time-out time, there is probably an issue with the CRX or the TB lines. Therefore a 'receiver not seen' error is generated by the system.             <ul style="list-style-type: none"> <li>Check if the time set in CRX, to send such calls, and the scan-time-out in the Server matches. A possible setting is e.g. 1:3 CRX/Server = 60sec/180sec.</li> <li>Check the phase of the TB-lines.</li> <li>Check if the programmed address in the CRX and Server do match. (each CRX has an individual address like B1xx.)</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Technical error transmitter</li> </ul>	<ul style="list-style-type: none"> <li>If after a scan call to the Transmitter Monitoring Module (TMM) a reply is received from the TMM that includes an error code then a 'Technical error transmitter' alarm is generated.</li> <li>Reasons for such transmitter errors are described in chapter "<a href="#">Transmitter monitoring via the Server</a>". F.i.             <ul style="list-style-type: none"> <li>SWR fault; e.g. caused by antenna problems.</li> <li>Too less HF-power.</li> <li>HF-power while transmitter is in 'idle'.</li> <li>NO LF signal or no OOR call detected at the DP6000 lines.</li> <li>Synchronisation signal not OK.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Transmitter not seen</li> </ul>	<ul style="list-style-type: none"> <li>The server can be programmed such that it should receive a reply to the periodical scan call from a system Transmitter (TX). If this reply is not received within the programmed reply time, there is probably an issue with the TX or the LF lines. Therefore a 'transmitter not seen' error is generated by the system.             <ul style="list-style-type: none"> <li>Check the phase of the LF-lines.</li> <li>Check if the programmed address in the TMM and Server do match. (each TMM has an individual address like B0xx.)</li> <li>Check if a 'manual scan call' (e.g. B001 0 00000) or a reset call (e.g. B001 0 FFFFF) to a TMM can be made; refer to installation manual II_LBB5905_TMM-V2_En_22xx for details</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Input alarm technical</li> </ul>	<ul style="list-style-type: none"> <li>Internal input contacts can be programmed such that they are monitored for interrupted/short-circuited wires.</li> <li>If interrupted/short-circuited wires are detected, a technical alarm is generated.             <ul style="list-style-type: none"> <li>The reported error will be reset when no longer interrupted/short-circuited wires are detected.</li> <li>Check the wires of the input contact.</li> <li>Check if the resistor network is connected correctly.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Technical error ESPA</li> </ul>	<ul style="list-style-type: none"> <li>In case an ESPA port is defect, i.e. cannot communicate anymore, a technical error is generated.             <ul style="list-style-type: none"> <li>The reported error will be reset when no longer interrupted/short-circuited wires are detected.</li> <li>If programmed that way a predefined message was sent also to inform the technicians.</li> <li>Check if the ESPA cable is assembled correctly.</li> <li>Check the communication e.g. with an 'ESPA tool' maybe the other side is the cause?</li> <li>Check if the communication with another ESPA port woks well.</li> <li>If multiple ESPA ports are fault, there might be a defect DP6000-IP-Interface.</li> </ul> </li> </ul>
<ul style="list-style-type: none"> <li>Low battery Alarm</li> </ul>	<ul style="list-style-type: none"> <li>If programmed in the system settings, low battery indications are (also) reported as technical errors.             <ul style="list-style-type: none"> <li>Most likely there was already a notification on the operators' screen or a sign at the status indicator.</li> <li>To solve the low battery indication make sure that the mobile is placed in a charge rack.</li> </ul> </li> </ul>





International Pager Services B.V.  
Willem de Haasstraat 5  
5421 TN Gemert  
The Netherlands  
<https://www.pagerservices.nl>

© 2023 International Pager Services B.V. - All rights reserved  
Data subject to change without notice