

Digistat Smart Central Installation and Configuration Manual

Digistat Smart Central V5.0

DIG TD SCNUS IU 0006 ENG V03

Ascom UMS s.r.l. Unipersonale Via Amilcare Ponchielli 29, 50018, Scandicci (FI), Italy Tel. (+39) 055 0512161 – Fax (+39) 055 829030

www.ascom.com

Digistat Smart Central version 5.0

Copyright © Ascom UMS s.r.l. All rights reserved.

No part of this publication can be reproduced, transmitted, copied, recorded or translated, in any form, by any means, on any media, without the prior written consent of Ascom UMS.

SOFTWARE LICENSE

Your Licence Agreement – provided with the product - specifies the permitted and prohibited uses of the product.

LICENSES AND REGISTERED TRADEMARKS

Digistat Smart Central is produced by Ascom UMS s.r.l http://www.ascom.com DIGISTAT® is a Trademark of Ascom UMS s.r.l Information is accurate at the time of release. All other trademarks are the property of their respective owners.

Ascom UMS is certified according to ISO 9001:2015 and ISO 13485:2003 standards.

Contents

1. Using the manual	7
1.1 Symbols	7
1.2 Aims	8
2. Intended use	8
2.1 "Off-label" use of the Product	8
2.2 Maintenance and technical support	8
2.3 Manufacturer's responsibility	9
2.4 Product traceability	9
2.4.1 How to display the "About box"	9
2.5 Post-market surveillance	11
2.6 Product life	11
3. Software/Hardware specifications	12
3.1 Central & Bedside	.12
3.1.1 Hardware	.12
3.1.2 Operating System	.12
3.2 Server	.13
3.2.1 Hardware	.13
3.2.2 Operating System	.13
3.2.3 System Software	.13
3.3 Digistat Smart Central Mobile	.13
3.4 General warnings	.14
3.4.1 Maintenance, management and protection of the "Operating Environment".	.15
3.4.2 Cybersecurity controls	.15

	3.5 Local network features	19
	3.5.1 Digistat Smart Central impact on the healthcare organization network	20
4	. Before starting	21
	4.1 Installation and maintenance warnings	21
	4.1.1 Patient Area	22
	4.2 Cleaning	23
	4.3 General precautions and warnings	23
	4.3.1 Electrical safety	24
	4.3.2 Electromagnetic compatibility	24
	4.3.3 Devices eligibility	24
	4.4 Privacy Policy	25
	4.4.1 User credentials features and use	27
	4.4.2 System administrators	29
	4.4.3 System logs	29
	4.5 Backup policy	29
	4.6 Out of order procedure	30
	4.6.1 Reconfiguration/substitution of network equipment	31
	4.7 Preventive maintenance	32
	4.7.1 Preventive maintenance checklist	32
	4.8 Compatible devices	35
	4.9 Digistat Smart Central unavailability	35
5	. Digistat Smart Central Installation	36
	5.1 Prerequisites	36
	5.2 Mobile Server	36
	5.3 Client installation	40

5.4 Change system settings	
6. Mobile Client Installation	
7. Digistat Smart Central Configuration	45
8. System Options	45
8.1 Smart Central System Options	
8.2 Smart Central System Options - overview	
8.2.1 Low/Medium/High PriorityAlarmSound.	
8.2.2 LogOptions	
8.2.3 SmartCentralAlarmsAggregatorsConfig	ı51
8.2.4 Smart Central Config	
8.2.5 Smart Central Grid Config	
8.2.6 Smart Central Trend Config	
8.3 Smart Central Mobile System Options	
8.4 Smart Central Mobile System Options - Over	view72
8.4.1 DeviceFormatString configuration	
8.4.2 GridColumnCount configuration	
8.4.3 ShowLocationName configuration	
8.4.4 SoundRepetition configuration	
8.4.5 BatteryLimit configuration	
8.4.6 DeviceLanguage configuration	
8.4.7 EnableAlarmAudio configuration	
8.4.8 KeepAliveInterval configuration	
8.4.9 LatencyLimitMs configuration	
8.4.10 LogFilesPath configuration	
8.4.11 LogLevel configuration	

11. Resi	dual risks	93
10. Mar	nufacturer and Distributor Contacts	92
9.1 H	low to add a Myco	89
9. Netw	vork Configuration	87
8.6 5	Smart Central Mobile Monitor	87
8.5 H	How to customize the system options for a single Smart Central Device	86
8	3.4.19 Title configuration	85
8	8.4.18 TimeSyncTresholdMs configuration	85
8	8.4.17 TempPath configuration	84
8	3.4.16 SignalLimit configuration	83
8	8.4.15 ReconnectScheduleMs configuration	83
8	3.4.14 MyPatientMode configuration	82
8	8.4.13 MyPatient configuration	82
8	3.4.12 Logo configuration	80

1. Using the manual

1.1 Symbols

The following symbols are used in this manual.

Useful information

This symbol appears alongside additional information concerning the characteristics and use of Digistat Smart Central. This may be explanatory examples, alternative procedures or any "extra" information considered useful to a better understanding of the product.

Caution!

The symbol is used to highlight information aimed at preventing improper use of the software or to draw attention to critical procedures which might cause risks. Consequently, it is necessary to pay extreme attention every time the symbol appears.

The following symbols are used in the about box:

	Indicates the manufacturer's name and address
i	Attention, consult accompanying documents
R _X Only	Caution: US Federal and Canadian law restricts this device to sale by or on the order of a licensed medical practitioner
Unique Device Identifier (UDI)	Unique device identification. The unique device identification (UDI) system is intended to assign a unique identifier to medical devices within the United States.

1.2 Aims

The effort which has gone into creating this manual aims to offer all the necessary information for installing and configuring the Digistat Smart Central product.

Digistat Smart Central must be installed and configured by trained and authorized personnel. This includes Ascom UMS and/or Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS and/or Distributor..

2. Intended use

The intended use of the Digistat Smart Central is to provide an interface with clinical systems to forward information associated to the particular event to the designated display device(s). For medical, near real time alarms, the Digistat Smart Central is intended to serve as a parallel, redundant, forwarding mechanism to inform healthcare professionals of particular medical related events. The Digistat Smart Central does not alter the behaviour of the primary medical devices and associated alarm annunciations. The display device provides a visual, and/or audio and/or vibrating mechanism upon receipt of the alert.

The Digistat Smart Central is intended for use as a secondary alarm. It does not replace the primary alarm function on the medical devices.

2.1 "Off-label" use of the Product

Every use of the Product outside what explicitly stated in the "Intended use" (usually referred to as "off-label" use) is under the full discretion and responsibility of the user and of the healthcare organization.

The manufacturer does not guarantee in any form the Product safety and suitability for any purpose where the Product is used outside the stated "Intended use".

2.2 Maintenance and technical support

Ascom UMS declines all responsibility for the consequences on the safety and efficiency of the product determined by technical repairs or maintenance not performed by its own Technical Service personnel or by Ascom UMS-authorized technicians.

The attention of the user and the legal representative of the healthcare organization where the device is used is drawn to their responsibilities, in view of the local legislation in force on the matter of occupational safety and health and any additional local site safety. The Ascom UMS/Distributor Service is able to offer customers the support needed to maintain the long-term safety and efficiency of the devices supplied, guaranteeing the skill, instrumental equipment and spare parts required to guarantee full compliance of the devices with the original construction specifications over time.

2.3 Manufacturer's responsibility

Ascom UMS is responsible for the product's safety, reliability and performance only if:

- Use and maintenance comply with User Manual instructions;
- This Manual is stored in good conditions and all sections are readable;
- Configurations, changes and repairs are only performed by personnel trained and authorized by Ascom UMS ;
- The Product's usage environment complies with applicable safety regulations;
- The electrical wiring of the environment where the Product is used complies with applicable regulations and is efficient.

!

Should the Product be part of a "medical electrical system" through electrical and functional connection with medical devices, the healthcare facility is in charge of the required electrical safety verification and acceptance tests, even where Ascom UMS performed in whole or in part the necessary connections.

2.4 Product traceability

In order to ensure device traceability, the former Product owner is requested to inform Ascom UMS/Distributor about any ownership transfer by giving written notice stating the product, former owner and new owner identification data.

Product data can be found in the product labeling (the "About box" displayed within the product - Fig 3).

In case of doubts/questions about product labeling and/or product identification please contact Ascom UMS/Distributor technical assistance (for contacts see section 10).

2.4.1 How to display the "About box"

To display the "About box"

 Click the menu button on the Digistat Smart Central control bar (bottom-left corner - Fig 1)



The following menu is displayed (Fig 2).

MAIN	MENU		×
曝	CLINICAL CONFIGURATION	ŝ	SYSTEM CONFIGURATION
X	SYSTEM ADMINISTRATION	Ģ	MODULES CONFIGURATION
	PATIENT REPORTS		SYSTEM REPORTS
ň	STATISTICS	P	CHANGE PASSWORD
(QUIT	ĩ	ABOUT
\times	(CLOSE	

Fig 2

Click the About button (Fig 2 A). The Digistat Smart Central "About Box" is displayed (an example in Fig 3)





2.5 Post-market surveillance

The device is subject to a post-market surveillance. Ascom UMS, its distributors and dealers must provide, for each marked copy, information concerning actual and potential risks, either for the patient or the User, during the Product's life cycle.

In case of deterioration of the Product characteristics, poor performance or inadequate user instructions that have been or could be a hazard to either the patient or User' health or to environmental safety, the User must immediately give notice to either Ascom UMS or its Distributor.

The product details can be found on its labeling.

On reception of a user feedback Ascom UMS will immediately start an investigation of the the reported nonconformity in order to take the required actions.

2.6 Product life

The life time of the product does not depend on wearing or other factors that could compromise safety. It is influenced by the obsolescence of the executing environment (e.g. computers, servers, operating system) and is therefore assessed as 5 years since the release date of the specific Product version. During this period, ASCOM UMS is committed to fully support the Product.

3. Software/Hardware specifications

Digistat Smart Central must only be installed by trained authorized personnel. This includes Ascom UMS/Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS/Distributor. Without an explicit, direct authorization from Ascom UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify Digistat Smart Central configuration.

Digistat Smart Central must only be used by trained personnel. Digistat Smart Central cannot be used without having a proper training, performed by Ascom UMS/Distributors staff.

The information provided in this chapter covers the manufacturer's obligations identified by the IEC 80001-1:2010 standard (Application of risk management for IT-networks incorporating medical devices).

According to the IEC 60601-1 standard, in case where an electrical equipment is positioned close to the bed, the use of "Medical grade" devices is required. In these situations medical grade PANEL PCs are usually used. The hospital shall take into account any other local regulation that may supplement these requirements.

3.1 Central & Bedside

3.1.1 Hardware

Minimum hardware requirements:

- Intel[®] i3 processor (or faster)
- Memory: 4 GB RAM
- Hard Disk: at least 60 GB of available space
- Monitor: 1024 x 768 or higher (1920 x 1080 suggested).
- Mouse or other compatible device. Touch screen recommended.
- Ethernet interface 100 Mb/s (or higher)
- CD/DVD Drive or possibility to copy the installation files

3.1.2 Operating System

- Microsoft Corporation Windows 7 SP1 x86/x64 Professional
- Microsoft Corporation Windows 8.1 x64 Professional

• Microsoft Corporation Windows 10 x64

3.2 Server

3.2.1 Hardware

Minimum hardware requirements:

- Intel[®] i5 processor (or faster)
- Memory: 4 GB RAM (8 GB recommended)
- Hard Disk: at least 120 GB of available space
- Ethernet interface 100 Mb/s (or higher). 1 GB recommended.
- CD/DVD Drive or possibility to copy the installation files

3.2.2 Operating System

- Microsoft Corporation Windows Server 2012 R2
- Microsoft Corporation Windows Server 2016

3.2.3 System Software

- Microsoft SQL Server 2008R2
- Microsoft SQL Server 2012
- Microsoft SQL Server 2014
- Microsoft SQL Server 2016
- Microsoft SQL Server 2017

3.3 Digistat Smart Central Mobile

Digistat Smart Central Mobile has been verified on the Ascom Myco SH1 Wi-Fi and Cellular Smartphone device, with Android version 4.4.2 (Myco 1) and 5.1 (Myco 2). It is therefore compatible with Myco 1 and Myco 2 mobile devices. The application is designed to be compatible with other Android devices with a minimum screen size of 3.5", and compatibility with a specific device must be verified before clinical use.

Please contact Ascom UMS for the full list of devices that support Digistat Smart Central Mobile.

3.4 General warnings

To correctly use Digistat Smart Central, the Microsoft Windows Display Scaling must be set to 100%. Different settings may prevent the product from starting or cause malfunctions in the way Digistat Smart Central is visually displayed. Please refer to the Microsoft Windows documentation for instructions on the Display Scaling settings.

The minimum vertical resolution of 768 is supported only if Digistat Smart Central is configured to run in full-screen mode or if the Windows tray bar is in Auto-hide mode.

The computers and the other connected devices must be suitable for the environment in which they are used and must, therefore, comply with the relevant regulations.

It is mandatory to follow the manufacturer instructions for storage, transport, installation, maintenance and waste of third parties hardware. These procedures must be performed only by qualified and authorized personnel.

The use the Product together with any software other than those specified in this document may compromise the safety, effectiveness and design controls of the Product. Such use may result in an increased risk to users and patients. It is mandatory to consult an authorized Ascom UMS or Distributor technician before using together with the Product any software other than those specified in this document.

If the hardware on which the Product runs is a stand-alone computer, the user shall not install any other software (utilities or applications programs) on the computer. It is suggested to apply a permission policy that prevents users from performing procedures such as the installation of new software.

-

The healthcare organization shall implement for the Digistat Smart Central workstations a date/time synchronization mechanism to a reference source.

3.4.1 Maintenance, management and protection of the "Operating Environment"

The healthcare organization using the Product is responsible for the maintenance, management and protection of the Operating Environment (including OS, SQL Server, Antivirus, Firewall, etc.) used by the Product on the server and the client.

The Operating Environment can be managed by the healthcare organization according to the local policies regarding maintenance, protection and updates provided that an adequate level of protection from cybersecurity and privacy points of view is guaranteed.

Ascom UMS implements a vigilance activity to detect the need for urgent security updates/patches for the Product and/or the Operating Environment. As part of this vigilance, Ascom UMS regularly tests the Product and Operating Environment to detect vulnerabilities. If a vulnerability that affects the safety, the regulatory compliance or the essential performance of the Product is detected, the healthcare organization is alerted and information and support are provided to define, schedule and implement the appropriate corrective actions.

3.4.2 Cybersecurity controls

To protect the Digistat Smart Central from possible cyber-attacks, it is necessary that:

- the Windows[©] Firewall is active both on the client PCs and the server;

- antivirus software is installed and regularly updated both on the client PCs and the server.

The healthcare organization shall ensure that these two protections are activated. Ascom UMS tested the Product with F-Secure Antivirus but, considering the strategies and policies already existing in the healthcare organization, the actual choice of the antivirus is left to the healthcare organization. Ascom UMS cannot ensure that Digistat Smart Central is compatible with any antivirus or antivirus configuration.

.

Some incompatibilities have been reported between parts of Digistat Smart Central and Kaspersky antivirus. The solution to these incompatibilities required the definition of specific rules in the antivirus itself.

!

It is suggested to only keep open the TCP and UDP ports actually needed. These may change according to the Digistat Smart Central configuration. Please refer to the Ascom UMS/Distributor technical assistance for more information.

3.4.2.1 Windows© Firewall settings

When installing Digistat Smart Central Server features may be blocked by the Windows© Firewall (or any other firewall installed on the workstation). It is therefore necessary to adequately define the firewall rules **before performing the installation procedure**.

In the following paragraphs it is described the manual procedure. For other firewalls, refer to the producer documentation. The components that may be blocked are: SQL Server, SQL Browser, Message Center, DAS, DAS Broker, HL7Receiver, Mobile Server, HL7Dispatch. For each component repeat the instructions described below.

Enabling applications in Windows© Firewall

1 Open Windows© Firewall on the Control Panel



2 Select Advanced settings (Fig 4 A).

Fig 4

3 Click **New Rule** (Fig 5 **A**).

Windows Firewall with Advance	Inbound Rules					Act	tions
Inbound Rules	Name	Group	Profile	Enabled	<u>^</u> ^	Int	Jound Rules
Connection Security Pulse	BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr	All	No		1	New Rule
Monitoring	BranchCache Hosted Cache Server (HTT	BranchCache - Hosted Cach	All	No			Ch. J. D. Cl.
- Monitoring	BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove	All	No	Allow	V.	Filter by Profile
	Browser Choice	Browser Choice	Domai	Yes	Allow	▼	Filter by State
	CheckPoint.VPN	CheckPoint.VPN	All	Yes	Allow	17	Filter by Group
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow		View
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow		
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Private	No	Allow	<u>0</u>	Kefresh
	Connect to a Network Projector (WSD Ev	Connect to a Network Proje	Domain	No	Allow	🖻	Export List
	Ocore Networking - Destination Unreacha	Core Networking	All	Yes	Allow	2	Help
	Ocore Networking - Destination Unreacha	Core Networking	All	Yes	Allow	-	,
	Ocore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow	Br	anchCache Hosted Cache
	Ocore Networking - Dynamic Host Config	Core Networking	All	Yes	Allow	0	Enable Rule
	Ocore Networking - Internet Group Mana	Core Networking	All	Yes	Allow	X	Cut
	Ocore Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes	Allow		-
	🕢 Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes	Allow	백희	Сору
	Ore Networking - Multicast Listener Do	Core Networking	All	Yes	Allow	×	Delete
	Ore Networking - Multicast Listener Qu	Core Networking	All	Yes	Allow		Properties
	Ore Networking - Multicast Listener Rep	Core Networking	All	Yes	Allow		Usla
	Ore Networking - Multicast Listener Rep	Core Networking	All	Yes	Allow		пер
	Ocore Networking - Neighbor Discovery A	Core Networking	All	Yes	Allow		
	Ocore Networking - Neighbor Discovery S	Core Networking	All	Yes	Allow		
	Ocore Networking - Packet Too Big (ICMP	Core Networking	All	Yes	Allow		
	Ocore Networking - Parameter Problem (I	Core Networking	All	Yes	Allow		
	Ocore Networking - Router Advertisement	Core Networking	All	Yes	Allow		
	Ocore Networking - Router Solicitation (IC	Core Networking	All	Yes	Allow		
	Ocore Networking - Teredo (UDP-In)	Core Networking	All	Yes	Allow		
	Ore Networking - Time Exceeded (ICMP	Core Networking	All	Yes	Allow		
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo	Private	No	Allow		
	Distributed Transaction Coordinator (RPC)	Distributed Transaction Coo	Domain	No	Allow		
	Distributed Transaction Coordinator (RP	Distributed Transaction Coo	Domain	No	Allow		
	Distributed Transaction Coordinator (RP	Distributed Transaction Coo	Private	No	Allow v		

Fig 5

4 Select **Program** (Fig 6 **A**) and click **Next** (Fig 6 **B**).

	New Indound Rule Wizard
Rule Type	
Select the type of firewall n	le to create.
Steps:	
Bule Type	What type of rule would you like to create?
Program	a b
 Action Profile 	Rule that controls connections for a program.
 Name 	⊖ Port
	Rule that controls connections for a TCP or UDP port.
	O Predefined:
	BranchCache - Content Retrieval (Uses HTTP)
	Rulle that controls connections for a viindows experience.
	Custom rule.
	Fig. C

5 Select the corresponding program path (Fig 7 **A**), e.g.

"C:\Digistat\<path to executable>"

@	New Inbound Rule Wizard	×
Program		
Specify the full program path and	executable name of the program that this rule matches.	
Steps:		
Rule Type	Does this rule apply to all programs or a specific program?	
Program	o m	
Action Profile	 All programs Rule applies to all connections on the computer that match other rule properties. 	
 Name 		
(
	Example: c:\path\program.exe %ProgramFiles%\browser\browser.exe <back next=""> Cancel</back>	

Fig 7

6 Select Allow the connection (Fig 8 A) and click Next (Fig 8 B)

@	New Inbound Rule Wizard	×
Action		
Specify the action to be tak	en when a connection matches the conditions specified in the rule.	
Steps:		
Rule Type	What action should be taken when a connection matches the specified conditions?	
New Inbound Rule Wizard Action Specify the action to be taken when a connection matches the conditions specified in the rule. Steps: What action should be taken when a connection matches the specified conditions? Program Action Action This includes connections that are protected with IPsec as well as those are not. Profile Name Name Allow the connection if it is secure This includes only connections that have been authenticated by using IPsec. Connections wile be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize Block the connection (Instrume) (I		
Action	This includes connections that are protected with IPsec as well as those are not.	
Profile	Allow the connection if it is secure	
• Indire	This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node. Customize O Block the connection	
	< Ba B Next > Cancel	

- Fig 8
- 7 Select the Domain, Private and Public checkboxes (Fig 9 A) and click Next (Fig 9 B).

@	New Inbound Rule Wizard	×
Profile Specify the profiles for which this	rule applies.	
Steps: Pule Type Program Action Profile Name	 When does this rule apply? Domain Applies when a computer is connected to its corporate domain. Private Applies when a computer is connected to a private network location, such as a home or work place. Public Applies when a computer is connected to a public network location. 	
	< IB Next > Cancel	

Fig 9

- 8 Click **Finish** to complete the procedure.
- 9 Repeat the procedure for all the components that may be blocked.

3.4.2.2 Firewall settings for connecting clients

The healthcare organization shall ensure that the server Firewall shall be properly configured in order to ensure the connection to the server from external clients (bedside or mobile).

3.5 Local network features

This section lists the features of the local network on which Digistat Smart Central is installed in order to guarantee the Product's full functionality.

- Digistat Smart Central uses a TCP/IP traffic protocol.
- The LAN must not be congested and/or full loaded.
- Digistat Smart Central requires at least a 100 Megabit LAN available to the client workstation. 1 Gigabit Ethernet backbones would be worthwhile.
- There must not be filters in the TCP/IP traffic between workstations, server and secondary devices.
- If the devices (server, workstations and secondary devices) are connected to different subnets there must be routing in these subnets.
- It is recommended to adopt redundancy strategies to ensure network service availability in case of malfunction.
- It is recommended to schedule, together with Ascom/Distributors, the maintenance calendar in order to let Ascom or the authorized Distributor efficiently support the healthcare organization in managing the possible disservices caused by maintenance activities.

|

If the network does not match the requested features, Digistat Smart Central performance gradually deteriorates until timeout errors occur. The Product may finally switch to "Recovery" mode.

In case a WiFi network is in use, given the possible intermittency of the WiFi connection, network disconnections are possible, that cause the activation of the "Recovery Mode" and the consequent Product unavailability. The healthcare organization shall ensure an optimal network coverage and stability, and train the personnel in the management of these temporary disconnections.

3.5.1 Digistat Smart Central impact on the healthcare organization network

Digistat Smart Central impacts the local network of the healthcare organization. This section provides information on the traffic generated by Digistat Smart Central on the network in order to make it possible for the structure to evaluate and analyze the risks related to the introduction of Digistat Smart Central.

The bandwidth used by Digistat Smart Central depends on many different factors. The most important are:

- Number of workstations,
- Number of workstations configured as central stations,
- Number and type of devices dedicated to data acquisition
- Interfaces with external systems,
- Digistat Smart Central configuration and mode of use.

In a configuration with acquisition on 100 beds where every bed collects data from 1 ventilator, 1 patient monitor and 3 infusion pumps, and with 10 Digistat Smart Central workstations showing 10 beds each, the following bandwidth occupation values can be indicatively predicted.

Average: 0.8 – 6 Mbit/s

Pitch: 5 – 25 Mbit/s

4. Before starting

4.1 Installation and maintenance warnings

The following warnings provide important information on the correct installation and maintenance procedures of the Digistat Smart Central product. They must be strictly respected.

-

Maintenance and repairs procedures shall be performed in compliance with Ascom UMS instruction only by Ascom UMS/Distributor technicians or personnel trained and authorized by Ascom UMS/Distributor.

Digistat Smart Central <u>must be installed and configured only by specifically trained and</u> <u>authorized personnel</u>. This includes Ascom UMS (or authorized Distributor) staff and any other person specifically trained and authorized by Ascom UMS/Distributor. Similarly, maintenance interventions and repairs on Digistat Smart Central must be performed according to Ascom UMS guidelines only by Ascom UMS/Distributor personnel or another person specifically trained and authorized by Ascom UMS/Distributor.



Digistat Smart Central <u>must be installed and configured only by</u> <u>specifically trained and authorized personnel</u>. This includes Ascom UMS (or authorized Distributor) staff and any other person specifically trained and authorized by Ascom UMS/Distributor.

- Use third party devices recommended by Ascom UMS/Distributors.
- Only trained and authorized people can install third party devices.
- Incorrect installation of the third party devices can create a risk of injury to the patient and/or operators.
- Meticulously observe the manufacturer's instructions for the installation of third party hardware.
- Make provision for regular maintenance of the Product according to the instructions present in this manual and those provided with the third party devices.
- The Digistat Smart Central USB dongle, when used, must be stored and used in eligible environmental conditions (temperature, humidity, electromagnetic fields etc.), as specified by the dongle manufacturer. These conditions are equivalent to those required by common office electronic devices.

- Within the "Patient Area" (see Fig 10) it is recommended to use easily washable devices that are protected from liquids.
- Within the "Patient Area" (see Fig 10) it is recommended to use washable, sterilizable rubber keyboards and mouse devices. For "touch screens" it is recommended to adopt capacitive technology (insensitive if used with gloves) because it discourages using gloves (sometimes contaminated).



Fig 10 - Patient Area

4.1.1 Patient Area

The Patient Area is the space where there could be either intentional or unintentional contact between a patient and parts of the system (i.e. any device) or between a patient and other persons touching parts of the system (i.e. a physician who simultaneously touches a patient and other devices). The definition applies when the patient's position is previously established; otherwise all possible patient positions must be taken into account.

According to IEC 60601-1 standard, every computer placed within the "Patient Area" must be a medical grade device.

According to the hardware license it is the responsibility of healthcare organization to perform all the required measurements on the electrical safety of the electro-medical system in use (PC, display and other possible connected devices) taking full consideration of the environment in which they are used.

.

Should the installation result in the establishment of a "medical electrical system" through electrical and functional connection of devices, the healthcare organization is in charge of the required safety verification and acceptance tests. This responsibility applies even where Ascom UMS/Distributor performed in whole or in part the wiring and the necessary connections.

4.2 Cleaning

Cleaning and disinfection procedures of hardware components must comply with the usual cleaning/disinfection procedures that the healthcare organization adopts for all the healthcare organization's equipment (both fixed and moveable).

|

Check the suggested cleaning procedures in the manuals of the hardware products that are used alongside Digistat Smart Central.

4.3 General precautions and warnings

To guarantee the reliability and security of the software during use, strictly observe the instructions given in this section of the manual.

Position all PCs appropriately to ensure adequate anterior and posterior ventilation. Failure to meet hardware ventilation requirements may cause equipment failure.

The healthcare organization shall ensure that the maintenance for the product and any third party device is implemented as requested to guarantee safety and efficiency and reduce the risk of malfunctioning and the occurrence of possible hazards to the patient and user.

[

The Product shall be used only by trained and authorized clinicians.

4.3.1 Electrical safety

The hardware devices (PC, display, barcode reader, etc...) used together with Digistat Smart Central must meet the requirements prescribed by the local legislation taking into consideration the environment in which they are used.

•

According to IEC 60601-1 standard, every computer placed within the "Patient Area" must be a medical grade device.

It is additionally recommended to perform all the relevant measurements on the leakage currents of the electro-medical system in use (PC, display and possible connected devices). The healthcare organization is responsible for these measurements.

.

The healthcare organization is responsible for all the required measurements on the electrical safety of the electro-medical system in use (PC, display and other possible connected devices) taking into consideration the actual environment in which the system is used.

4.3.2 Electromagnetic compatibility

The hardware devices (PC, display, barcode reader, etc...) used together with Digistat Smart Central must meet the requirements prescribed by the local legislation taking into consideration the environment in which they are used.

4.3.3 Devices eligibility

The hardware devices (PC, display, barcode reader, etc...) used together with Digistat Smart Central must meet the requirements prescribed by the local legislation taking into consideration the environment in which they are used.

4.4 Privacy Policy

Appropriate precautions should be taken in order to protect the privacy of users and patients, and to ensure that personal data is processed by respecting data subjects' rights, fundamental freedoms and dignity, particularly with regard to confidentiality, personal identity and the right to personal data protection.

Special attention shall be dedicated to Protected Health Information (PHI) in accord with the stipulations of the US Health Insurance Portability and Accountability Act (HIPAA).



Protected health information (PHI) under US law is any information about health status, provision of health care, or payment for health care that is created or collected by a Covered Entity (or a Business Associate of a Covered Entity), and can be linked to a specific individual.

According to the US Health Insurance Portability and Accountability Act (HIPAA), PHI that is linked based on the following list of 18 identifiers must be treated with special care:

- 1. Names
- 2. All geographical identifiers smaller than a state,
- 3. Dates (other than year) directly related to an individual
- 4. Phone numbers
- 5. Fax numbers
- 6. Email addresses
- 7. Social Security numbers
- 8. Medical record numbers
- 9. Health insurance beneficiary numbers
- 10. Account numbers
- 11. Certificate/license numbers
- 12. Vehicle identifiers and serial numbers, including license plate numbers;
- 13. Device identifiers and serial numbers;
- 14. Web Uniform Resource Locators (URLs)
- 15. Internet Protocol (IP) address numbers
- 16. Biometric identifiers, including finger, retinal and voice prints
- 17. Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code except the unique code assigned by the investigator to code the data

The healthcare organization needs to assure that the use of the product is in line with the HIPAA requirements specifically respect the management of aforementioned information.

Digistat Smart Central manages the following PHI:

• First name and surname

- Birthdate
- Sex
- Patient code (MRN)
- Admission date
- Discharge date
- Patient weight
- Patient height

Digistat Smart Central can be configured to automatically hide the PHI on every application screen.

To do that, on the Digistat Smart Central Configuration Application, set the system option named "Privacy Mode" to "true" (see next chapters for the detailed procedure). Its default value is "true".

If the "Privacy Mode" option is set to true, the following cases are possible:

- with no user logged in, no patient information is displayed.
- with a user logged in, and the user does not have a specific permission, no patient information is displayed.
- with a user logged in, and the user does have a specific permission, patient information is displayed.

The option can be applied to a single workstation (i.e. different workstations can be configured differently)

.

Please read the following precautions carefully and strictly observe them.

- The workstations must not be left unattended and accessible during work sessions. It is recommended to log out when leaving a workstation. The user shall be warned about the importance of logging out when leaving a workstation.
- PHI saved in the product, such as passwords or users' and patients' personal data, must be protected from possible unauthorized access attempts through adequate protection software (antivirus and firewall). The healthcare organization is responsible for implementing this software and keep them updated.
- The lock function (see user manual, paragraph 5.5.1) should be used only when strictly necessary. Automatic log out protects the Product from unauthorized accesses.

 encrypted format and using a connection which is not physically secure. An example of this kind of transmission are the HL7 communications. The healthcare organization is responsible for providing adequate security measures to comply with the local privacy laws and regulations.
 PHI can be present inside some reports produced by the Digistat Smart Central. The healthcare organization needs to manage these documents according to HIPAA regulation.
 Client workstations (both desktop and mobile) do not store patient data on disk. Patient data is stored only inside database and database

storage depends on the healthcare structure's procedures and choices (examples: physical machine, SAN, virtualization environment). Patient data shall be treated according all the current standards on privacy and personal data protection.

In some circumstances, sensitive data /PHI are transmitted in non-

Patient data is not stored in proprietary files. The only place in which patient data is stored is database.

According to the HIPAA regulation, databases cannot leave the hospital without being encrypted.

4.4.1 User credentials features and use

This section explains the Digistat Smart Central user credentials (username and password) features, their use and recommended policy.

- Every precaution must be taken in order to keep personal username and password secret.
- Username and password must be kept private. Do not let anybody know your username and password.

- Each user can own one or more credentials to access Digistat Smart Central (username and password). The same username and password must not be used by more than one user.
- Authorization profiles must be checked and renewed at least once a year.
- It is possible to group different authorization profiles considering the similarity of the users' tasks.
- Each user account shall be linked with a specific person. The use of generic (for instance, "ADMIN" or "NURSE") must be avoided. In other words, for traceability reasons it is necessary that every user account is used by only one user.
- Each user has an assigned authorization profile enabling them to access only the functionalities that are relevant to their working tasks. The system administrator must assign an appropriate user profile when creating the user account. The profile must be reviewed at least once a year. This revision can also be performed for classes of users. The user profile definition procedures are described in the Digistat[®] Connect Installation and Operation Manual
- Password must be at least 8 characters.
- The password must not refer directly to the user (containing, for instance, user's first name, family name, date of birth etc.).
- The password is given by the system administrator at user account creation time. It must be changed by the user at first access in case this procedure is defined by configuration (see user manual paragraph 5.10.3 for the password modification procedure).
- After that, the password must be changed at least every three months.
- If username and password are left unused for more than 6 months they must be disabled. Specific user credentials, used for technical maintenance purposes, are an exception. See technical manual for the configuration of this feature.
- User credentials must also be disabled if the user is not qualified anymore for those credentials (it is the case, for instance, of a user who is transferred to another department or structure). A system administrator can manually enable/disable a user. The procedure is described in the Digistat[®] Connect Installation and Operation Manual

The following information is reserved to system administrators:

The password must match a regular expression defined in the Digistat Smart Central configuration (default is ^......* i.e. 8 characters). The password is assigned by the system administrator when a new account for a user is created. The system

administrator can force the user to change the password at first access to the Digistat Smart Central. The password expires after a certain (configurable) period, after that period, the user must change the password. It is also possible (by configuration) to avoid password expiration.

See Digistat[®] Connect Installation and Operation Manual for detailed information on user account creation procedures and password configuration.

4.4.2 System administrators

Ascom UMS/Distributor technical staff, when performing installation, updates and/or technical assistance may have access to personal data stored in the Digistat Smart Central database.

It is responsibility of the healthcare organization to adopt the necessary measures and provide instructions in order to comply with the local regulations.

4.4.3 System logs

Digistat Smart Central records the system logs on the database. These logs are kept for a configurable period of time. Also, logs are kept for different times depending on their nature. Default times are:

- information logs are kept for 10 days;
- logs of warning messages are kept for 20 days;
- logs of alarm messages are kept for 30 days.

These times are configurable. See Digistat Connect Installation and Operation Manual.

4.5 Backup policy

It is recommended to regularly perform system backups.

The healthcare organization using Digistat Smart Central must define a backup policy that best suits its data safety requirements.

Ascom UMS/Distributor is available to help and support in implementing the chosen policy.

The healthcare organization must ensure that backup files are stored in a way that makes them immediately available in case of need.

If data is stored on removable memory devices, the healthcare organization must protect these devices from unauthorized access. When these devices are not used anymore, they must be either securely deleted or destroyed.

|

According to the HIPAA standards, databases cannot leave the hospital without being encrypted.

4.6 Out of order procedure

Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

This section describes the policy suggested by Ascom UMS in case a Digistat Smart Central workstation gets out of order. The goal of the procedure is to minimize the time required to successfully replace the out of order workstation.

Ascom UMS suggests the healthcare organization has substitute equipment and an additional PC on which Digistat Smart Central is already installed.

In case of a Digistat Smart Central workstation is out of order, the substitute equipment can promptly replace the Digistat Smart Central workstation.

Always remember that Digistat Smart Central must only be installed by trained authorized personnel. This includes Ascom UMS/Distributors staff and any other person specifically trained and explicitly authorized by Ascom UMS/Distributor. Without an explicit, direct authorization from Ascom UMS/Distributor, the healthcare organization staff are not authorized to perform installation procedures and/or to modify Digistat Smart Central configuration.

The risk related to the Digistat Smart Central workstation deactivation or substitution is that to associate the workstation with a wrong bed or room. This could lead to a "patient switch", which is an extremely hazardous condition.

The risk related to the substitution and/or reconfiguration of network equipment involved in the Digistat Smart Central data acquisition (i.e. port server, docking station, etc...) is that of assigning the acquired data to a wrong patient. The patient-acquired data relation is based on the IP address of the Digistat Smart Central workstation. Changing it could lead either to data flow interruption or, in severe cases, to assigning data to the wrong patient.

!

The out of order and replacement of a workstation is potentially hazardous. This is the reason why it must only be performed only by authorized and trained personnel.

The risk related to this procedure is that of associating a wrong bed/room/domain to the workstation, and therefore display data belonging to the wrong patients/beds.

In case a Digistat Smart Central workstation needs to be deactivated and replaced, the hospital staff must promptly call Ascom UMS (or authorized Distributors) and request the execution of this task.

Ascom UMS suggests the healthcare organization defines a clear, univocal operating procedure and to share this procedure with all the staff members involved.

In order to speed up replacement times, Ascom UMS suggests the healthcare organization has one or more substitution equipment with all the necessary applications already installed (OS, firewall, antivirus, RDP,...) and with Digistat Smart Central already installed, but disabled (i.e. not executable by a user without the assistance of an Ascom UMS/Distributor technician). In case of out of order of a Digistat Smart Central workstation, the substitution equipment availability assures the minimization of restoration times (hardware substitution) and reduces the risk of associating patient data incorrectly.

In case of out of order of a Digistat Smart Central workstation we suggest to adopt the following procedure if a "substitution equipment" is available:

- 1) The healthcare organization's authorized staff replaces the out of order PC with the "substitution equipment"
- 2) The healthcare organization staff calls Ascom UMS/Distributor and requests the "substitution equipment" activation
- 3) The Ascom UMS/Distributor staff disables the out of order workstation and correctly configure the "substitution equipment"
- 4) The out of order PC is repaired and prepared as "substitution equipment"

The instructions on how to enable/disable and replace a Digistat Smart Central workstation, reserved to system administrators, are in the Digistat[®] Connect Installation and Operation Manual.

4.6.1 Reconfiguration/substitution of network equipment

In case it is necessary to either reconfigure or substitute a network device involved in the Digistat Smart Central data acquisition, the healthcare organization staff must promptly call Ascom UMS/Distributor and schedule the substitution/reconfiguration procedure to allow Ascom UMS/Distibutor staff to either reconfigure Digistat Smart Central or provide all the necessary information to the healthcare organization. It is recommended, for this purpose, to define a clear procedure and share it with all the involved personnel. Some general indications about this are in the Digistat Connect Installation and Operation Manual.

4.7 Preventive maintenance

Maintenance procedures and repairs shall be performed in compliance with Ascom UMS/Distributor procedures and guidelines and only by Ascom UMS/Distributor technicians or personnel specifically trained and explicitly authorized by Ascom UMS/Distributor.

It is suggested to perform the maintenance of Digistat Smart Central at least once a year. Maintenance frequency is a function of system complexity. In case of high complexity, it is suggested to perform maintenance more often, typically up to twice a year.

4.7.1 Preventive maintenance checklist

Preparatory checks

- Digistat Smart Central update necessity check.
- Check minimum requirements for a possible Digistat Smart Central update (both hardware and software).
- Check the Server Service Pack version and state.
- Schedule the server/s restart to apply possible updates.
- Check the SQL Server Service Pack version and state.

SELECT SERVERPROPERTY('productversion'), SERVERPROPERTY ('productlevel'), SERVERPROPERTY ('edition')

• Schedule possible updates with the technical staff

Checks to be performed

Antivirus

- Check that Antivirus Software is installed and updated (both the application and the virus list definition).
- If viruses are present, inform the competent technician and, if authorized, try to clean the PC.

Database

• Check that an effective Digistat Smart Central database clean-up and backup policy is configured.

- Check that the clean-up and back-up store procedures exist (UMSBackupComplete, UMSBackupDifferential, UMSCleanLog, UMSCleanDriver) and the related schedule.
- Check that back-up files exist (both full and differential).
- Check with the healthcare organization technical department that backup, configuration folders and data folders are correctly copied to another storage device.
- Using a previous backup, restore the database to verify its correctness.
- Delete the old back-up files (.bak) and the possible files that are not inherent to Digistat Smart Central configuration on the network shared path.
- Check that the other jobs on SQL Agent or scheduled tasks (for instance those that are support to integration with third-parties systems) are present, and that their schedule is adequate.
- On SQL Agent check that the different JOBs are executed and that there are not hanging JOBs or JOBs in error.
- Check the SQL Server LOGs.
- Check the database total size and the number of records in the main tables. Script for checking all the tables size:

```
USE [DATABASENAME]
GO
CREATE TABLE [#SpaceUsed]
(
  [name] [nvarchar] (250) NULL,
  [rows] [nvarchar] (250) NULL,
  [reserved] [nvarchar] (250) NULL,
  [data] [nvarchar] (250) NULL,
  [index size] [nvarchar] (250) NULL,
  [unused] [nvarchar] (250) NULL
) ON [PRIMARY]
DECLARE @INS AS nvarchar(MAX)
SET @INS = '';
SELECT @INS = @INS + 'INSERT INTO #SpaceUsed exec
sp spaceused ''' + TABLE NAME + '''; '
FROM INFORMATION SCHEMA.TABLES
WHERE TABLE TYPE = 'BASE TABLE'
ORDER BY TABLE NAME
EXEC (@INS);
SELECT *
FROM #SpaceUsed
ORDER BY CAST([rows] AS INT) DESC
DROP TABLE [#SpaceUsed]
```

Server

- Check the Windows[™] server event log.
- Check the permissions on the shared folders (e.g. Backup folder).

- File and directories no longer needed should be removed to free up space on server disk.
- Check the displays (if any) on the server rack and verify that there are neither visual nor sound alarms.
- Check that on the different disk units there is enough space available.
- Disk check with dedicated tools (checkdisk, defrag, etc.).
- In case there are disks in RAID, check the health conditions of the RAID unit on the RAID management software.
- Check the LED of the non-alarmed RAID units.
- If an UPS (Uninterruptible Power Supply) is connected, check its health conditions with its management software.
- In case of UPS schedule an electric interruption (an electric failure simulation) and check that the server is configured to perform a CLEAN shutdown.

Workstations

- Check if the Regional Settings on the workstations are appropriate with the Digistat Smart Central installation language.
- Check if every workstation has a default printer.

Digistat Smart Central

- Check data presence (SELECT) Patient, Admission, Bed, Location tables and some random others.
- Check on the network table that no workstation has the ALL value in the "modules" field.
- Check, and if appropriate, clean the service and/or Ascom UMS Gateway LOG.
- Check, and if appropriate, clean the DAS LOGs for the Drivers (if enabled).
- Check that the privacy policy is respected as stated in this manual in paragraph 4.4.

Instruction for use

- Check if user documentation has been configured to be downloaded from the server or if it is still the original documentation included in the installation package.
- Check that the user documentation in PDF format (PDF provided together with the product) is present on the server and appropriate with Digistat Smart Central version.
- Check that the folder containing the user documentation in electronic format on the server is accessible to Digistat Smart Central users.
- Check that the HELP button opens the user documentation.
- Check that all the other contents provided by Ascom UMS and integrated in the HELP of Digistat Smart Central are updated.

4.8 Compatible devices

Digistat Smart Central is compatible with Digistat Connect 5.0.0 and it is able to display data from ventilators, patient monitors and infusion pumps. Please contact Ascom UMS/Distributor for the list of available drivers.

Purpose of Digistat Smart Central is to forward information from patient monitors, ventilators, infusion pumps to the designated display device(s). During the installation and configuration of the product it is necessary to verify that only these device types are actually connected to Digistat Smart Central.

4.9 Digistat Smart Central unavailability

If during start up there are problems connecting to the server, Digistat Smart Central provides a specific information message (Fig 11).





The connection problem is often automatically solved in a short time. If it does not happen, it is necessary to contact the technical assistance (see section 10 for the contacts list).

In rare, often extreme cases, it may be physically impossible to use Digistat Smart Central, for example cases of natural disasters, or long black outs.

It is responsibility of the healthcare organization using Digistat Smart Central to define an emergency procedure to put into effect in those cases. This is necessary to

- 1) Make it possible for the departments to keep on working
- 2) Restore as soon as possible the Product to full availability (back-up policy is part of this management. See paragraph 4.5).

!

It is responsibility of the healthcare organization using Digistat Smart Central to define an emergency procedure to put into effect in case of unavailability.

Ascom UMS/Distributor offers full support for the definition of such procedure.

See section 10 for the contacts list.

5. Digistat Smart Central Installation

5.1 Prerequisites

The following components are prerequisites to the Digistat Smart Central installation.

CLIENT

- MS Framework.NET 4.0 4.7.1
- Acrobat Reader (Client)

SERVER

- MS Framework.NET 3.5 and 4.0
- Digistat Connect 5.0.0. See the related technical documentation for instructions on Connect installation and configuration (Digistat Connect Installation and Operation Manual).

The installation of Digistat Smart Central consists of three different components:

- **Digistat Smart Central Desktop**: client desktop application. Runs on Windows desktop machines.
- Digistat Smart Central Mobile: client mobile app. Runs on Ascom Myco.
- **Mobile Server**: server application used by Digistat Smart Central Mobile to connect to Digistat Connect. This component must be installed only if you need to support and run Digistat Smart Central Mobile app. Mobile Server runs on a server machine (can be the same where it's running Digistat Connect).

5.2 Mobile Server

To install Digistat Smart Central Mobile Server:

1 Double click the MSI installation file (run as administrator)

The following screen is displayed (Fig 12)


2 Click the Next button (Fig 12 A). The following screen is displayed (Fig 13).



- 3 Read carefully the End-User License Agreement, then check the box placed in the bottom-left corner of the window (Fig 13 **A**) and click **Next** (Fig 13 **B**).
- 4 The following screen is displayed (Fig 14).

😸 Digistat Mobile Server Setup	—		×		
Destination Folder	-		_		
Select a folder where Digistat Mobile Server will be installed.	a	ascom			
The installation wizard will install the files for Digistat Mobile Server following folder.	in the				
To install into a different folder, dick the Browse button and select folder.	another				
You can choose not to install Digistat Mobile Server by clicking Can installation wizard.	cel to exit	: the			
Destination Folder:					
E:\Digistat\	Brows	e			
(B					
Back Nex	ct	Cano	el		
Fig 14					

5 Select the destination folder (Fig 14 **A**). Default is C:\Digistat\Mobile Server. Click the **Next** button (Fig 14 **B**). The following screen is displayed.

闄 Digistat Mobile Server Setup	_		×
SSL Certificate Select the SSL certificate to install for Digistat Mobile Server.	а	sco	m
Install SSL certificate: By installing this certificate your connection to Message Center will b using TLS encryption. Warning: The certificate must be installed on both client and server	e encryp machines	ted	
Certificate File:	Brow	se	
Certificate Password:			
<u>B</u> ack Me	xt	Can	cel

6 If Digistat Connect has been installed with SSL/TLS enabled, on the same machine where you are installing Digistat Mobile Server, the following step is skipped, otherwise you'll be asked to insert a valid certificate to enable TLS. Click the **Next** button and the following screen is displayed (Fig 15).

5	Digistat Mobile Ser	ver Setup			_		×			
	Mobile Server Co Insert Mobile Serve Server.	a	scor	n						
	Message Center:		ITALY-610)1YYD	_					
	Message Center Inst	tance:	50000							
	Input Local Port:		52000							
	IP Outbound HL7:			Port Outbound HL7:						
	Use Unite:	⊖ true	I false							
	Unite AM IP:			Unite AM API Port:	443					
	Username:			Password:						
	CS/CM IP:									
	Back Next Cancel									
			F	ig 15						

- 7 The Mobile Server Configuration screen makes it possible to specify the following parameters:
 - **Message Center**: specify here the message Center hostname. See Digistat Connect Installation and Operation Manual for more details. It is the hostname where Digistat Connect is running.
 - **Message Center Instance**: specify here the message Center instance. See Digistat Connect Installation and Operation Manual for more details. Message Center port of the machine where Digistat Connect is running.
 - **Input Local Port**: port on which the server listens for incoming connections from mobile clients (the same port must be configured on mobile devices).
 - **IP Outbound HL7 and Port**: IP and port of the HL7 Outbound service. This functionality is not enabled in Digistat Smart Central.
 - Use Unite (Fig 16 A): this selection makes it possible to integrate the Digistat login with Ascom Unite Messaging Suite Login. Set "True" to enable it. Here specify:
 - Unite AM IP: IP address of the Unite AM server
 - Unite AM API Port: port of the API provided by Unite AM (default is 443)
 - Username and Password: username and password used by Mobile Server to connect to Unite AM
 - **CS/CM IP**: IP address of the Unite CM (or Unite CS)

Digistat Mobile Server Setup Mobile Server Configurati Insert Mobile Server configura Server.	ion ation parameters for Digistat Mobile
Message Center:	ITALY-6101YYD
Message Center Instance:	50000
Input Local Port:	52000
IP Outbound HL7:	Port Outbound HL7:
Use Unite: 💿 true	⊖ false
Unite AM IP:	Unite AM API Port: 443
Username:	Password:
CS/CM IP:	
	Back Next Cancel
	Fig 16

Click Next when done (Fig 16 B).

8 Click Next to move to next step. The following screen is displayed (Fig 17).

闄 Digistat Mobile Server Setup	_		×
Ready to install Digistat Mobile Server	a	scoi	m
Click Install to begin the installation. Click Back to review or change installation settings. Click Cancel to exit the wizard.	any of yo	bur	
Back SInstal	1	Cano	el
Fig 17			

9 Click **Install** (Fig 23 **A**) to install Digistat Smart Central Client. A notification is provided when the installation is successfully completed.

5.3 Client installation

To install Digistat Smart Central Client:

10 Double click the MSI installation file (run as administrator)

The following screen is displayed (Fig 18)



11 Click the Next button (Fig 18 A). The following screen is displayed (Fig 19).



12 Read carefully the End-User License Agreement, then check the box placed in the bottom-left corner of the window (Fig 19 **A**) and click **Next** (Fig 19 **B**). The following screen is displayed (Fig 20).

Language	
Choose the language for Digis	Smart Central.
() Danish	
Outch	
English	
) Finnish	
○ French	
🔾 German	
🔘 Italian	
Norwegian	
🔘 Spanish	
🔾 Swedish	
	B
	Back Next Cancel
	Fig 20

13 Select the language (Fig 20 **A**) and click the **Next** button (Fig 20 **B**). The following screen is displayed (Fig 21).

闄 Digistat Smart Central Setup	– 🗆 X
Destination Folder Select a folder where Digistat Smart Central will be installed.	ascom
The installation wizard will install the files for Digistat Smart Cen following folder. To install into a different folder, click the Browse button and sel folder. You can choose not to install Digistat Smart Central by clicking C	tral in the ect another Cancel to exit the
Destination Folder:	
C:\Digistat\	Browse
	₿
Back	Vext Cancel
Fig 21	

- 14 Select the destination folder (Fig 21 **A**). Default is C:\Digistat. Click the **Next** button (Fig 21 **B**).
- 15 Choose if you want to install the SSL/TLS certificate. If yes, specify the folder in which the certificate file is located and the certificate password. Digistat Connect shall be configured to support SSL/TLS.

👹 Digistat Smart Central Setup	-		×
SSL Certificate			
Select the SSL certificate to install for Digistat Smart Central.	as	SCO	n
Install SSL certificate:			
By installing this certificate your connection to Message Center will be using TLS encryption. Warning: The certificate must be installed on both client and server m	encrypte achines.	d	
Certificate File:			
C:\	Browse	2	
Certificate Password:			
Back Nex	t	Cano	el

Click the Next button and the following screen is displayed (Fig 22).

Configuration		25500
Insert configuration paramet	ascon	
Message Center:	ITALY-6101YYD	
Message Center Instance:	50000	
	,	
		ົ

Fig 22

16 Specify the Message Center and the Message Center Instance (Fig 22 A). Message Center is the hostname of the machine where Digistat Connect is running. Message Center Instance is the Message Center port of the machine where Digistat Connect is running. Click the Next button (Fig 22 B).

Click Next when done. The following screen is displayed (Fig 23).



Fig 23

17 Click **Install** (Fig 23 **A**) to install Digistat Smart Central Client. A notification is provided when the installation has been successfully completed. The Digistat Smart Central icon is then displayed on the workstation desktop.

To verify that the installation performed successfully, double click on Digistat Smart Central shortcut. Digistat Smart Central should start and display the main view.

5.4 Change system settings

Once the installation procedure of the Mobile Server is completed, if you need to modify parameters and values specified during the installation procedure, it is necessary to edit the following configuration file:

<install folder>\MobileServer\UMS.Mobile.Service.exe.config

The following settings can be modified (leave default value for other settings):

- TCPPort: port on which the mobile server listens for mobile clients.
- HL7OutHost and HL7OutPort: port to which the mobile server sends HL7 data to be dispatched.
- Unite*: settings related to Unite integration.

6. Mobile Client Installation

Digistat Smart Central mobile is distributed as an apk package file. It is usually install by Ascom UMS or distributor personnel. It can be installed on a Myco or on a verified mobile device using the follow methods:

- Using Unite CM, if Myco is managed by Unite CM, using the procedure to install external apk.
- Connecting Myco to the web and download apk from the Ascom Extranet website.
- Manually, using adb or similar.

Remember to enable, in the mobile device settings, the installation of apps outside of the Google Play Store (unknown sources).

7. Digistat Smart Central Configuration

The configuration of Digistat Smart Central is performed using Configurator, a software tool installed together with Digistat Connect (the installation of Digistat Connect is a prerequisite for the installation of Digistat Smart Central). For general instructions on the Configurator tool, see the document Digistat Connect Installation and Operation Manual. In this section are described the system options directly affecting the Digistat Smart Central and Smart Central Mobile configuration.

8. System Options

8.1 Smart Central System Options

To configure the Smart Central system options access the Administrator/Application System Options area on the Digistat Smart Central configurator. The path is shown in Fig 24.

HOME	SENERAL CONFIGURATOR	>SYSTEM CONFIGURATION	ADMINISTRATOR/APPLICATION SYSTEMOPTIONS	\rangle					
Fig 24									

The following screen opens (Fig 25).

Application		Nan	ne		Т н.О.			ost Name		Apply Filter Clear	Filter
				Heckerse							THEOT
Name	A	prication	Hospital Unit	Hostname	Username	0		Vali	ue		
AcquisicionDenomode						0					
utoEpobleNetwork						1					
arCodeMultiMennade	olitChar.					-					
leanDBTime	pilconal					01:00:00					
onfiguratorModulesEl	tering					SYSTEMORTIO	NS-NETWORKS-BED	SH OCATIONS USER	S-DEDMISSIONS		/FD·M
ASD at a Evolution	comg					51512101101110	NO,NE WORKS, DED	S,EOCATIONS,OBER.	5,1	S, DIVINERCONTENT, DEVICEDIO	aqri
ASEventExpiration											
ieloPath						C:\Digistat\Sm	art Central\help\				
tighestAnonymous						0	ini contrar (idp)				
rivacyMode						0					
enortHeader						HOSPITAL					
eportsPath						C:\Digistat\Sm	art Central\				
howPrintDialog						0					
vstemOptionEditableA	oplication					xml version:</td <td>="1.0" encodina="ut</td> <td>f-16"?> <arravofstri< td=""><td>ina xmlns:xsi="</td><td>http://www.w3.org/2001/XMLS</td><td>chema</td></arravofstri<></td>	="1.0" encodina="ut	f-16"?> <arravofstri< td=""><td>ina xmlns:xsi="</td><td>http://www.w3.org/2001/XMLS</td><td>chema</td></arravofstri<>	ina xmlns:xsi="	http://www.w3.org/2001/XMLS	chema
System Options											
Name A	cquisitionDer	noMode				~	Host Name				This
Application							Type	enum OptionTypeF	num Bool		
H.U.							User				
Description T	rue=Demonst	ration Mode	e, generates ra	ndom data. F	alse=Acquire	es Real Data	Value	○ True ●	False		
fn	0										
fn											
fn											
fr											
fr											
fr											
In NEW	EDIT	DE	ELETE	СОРУ	_					CLOSE	

 Select "Smart Central" or "Smart Central Mobile" on the "Application" filter indicated in Fig 25 A (enlarged in Fig 26) and then click Apply Filter (Fig 25 B)



The Smart Central system options list is this way displayed (Fig 27).

Application	SMARTCENTRAL V	Name		H.U.		Ho	ost Name		Apply Filter	Clea	r Filter
	Name	Application	Hospital Unit	Hostname L	Jsername			Value			
HighPriority	AlarmSound	SMARTCENTRAL									
LogOptions		SMARTCENTRAL			<	?xml version="1.0"?>					
LowPriority/	AlarmSound	SMARTCENTRAL									
MediumPrio	rityAlarmSound	SMARTCENTRAL									
SmartCentra	lAlarmAggregatorsConfig	SMARTCENTRAL									
SmartCentra	nartCentralConfig SMARTCENTRAL <sr< td=""><td>SmartCentral><smartc< td=""><td>CentralConfi</td><td>ig MyPatientBedCount</td><td>="3" Central ColumnC</td><td>ount="4" Cen</td><td>tralRowCo</td></smartc<></td></sr<>					SmartCentral> <smartc< td=""><td>CentralConfi</td><td>ig MyPatientBedCount</td><td>="3" Central ColumnC</td><td>ount="4" Cen</td><td>tralRowCo</td></smartc<>	CentralConfi	ig MyPatientBedCount	="3" Central ColumnC	ount="4" Cen	tralRowCo
SmartCentra	martCentralGridConfig SMARTCENTRAL </td <td>?xml version="1.0" enco</td> <td>oding="utf-</td> <td>16"?></td> <td></td> <td></td> <td></td>					?xml version="1.0" enco	oding="utf-	16"?>			
SmartCentra	al Trends Config	SMARTCENTRAL			<	?xml version="1.0" enco	oding="utf-:	16"?>			
System Optio	ons										
Name	HighPriorityAlan	nSound			V	Host Name					This
Application	n SMARTCENTR	AL				Туре	_enum_Opt	tionTypeEnum_Binary			~
H.U.						User					
Description	n Change high pri	ority alarm sound.				Value		Choose a file			
NEW	EDIT	DELETE	COPY	(CLOSE	
	Fig 27										

2 Click the row corresponding to the system option to be edited

The row is highlighted. The selected system option's data is displayed in the lower part of the screen.

- 3 Click the **Edit** button on the command bar. The screen turns to **Edit** mode
- 4 Edit the system option's data
- 5 Click the **Update** button on the command bar.

The application configuration is this way changed.

NOTE:	If the "Host Name" field is empty, the configuration
	change applies to all the devices. If the "Host Name" is
	specified, the configuration change applies only to the
	specified device (Workstation or Myco).

8.2 Smart Central System Options - overview

Name	Description	Default Values
LowPriorityAlarmSound	Changes the sound provided when low priority alarms are notified.	See below for configuration info.
MediumPriorityAlarmSound	Changes the sound provided when medium priority alarms are notified.	See below for configuration info.
HighPriorityAlarmSound	Changes the sound provided when high priority alarms are notified.	See below for configuration info.
LogOptions	Manages the (Digistat Smart Central Logging System).	XML file - see related paragraph for the default
SmartCentralAlarmAggregatorConfig	List of alarms that must be aggregated during dashboard generation.	XML file - see related paragraph for the default
SmartCentralConfig	General Smart Central Configuration	XML file - see related paragraph for the default
SmartCentralTrendConfig	Configuration of trends	XML file - see related paragraph for the default
SmartCentralGridConfig	Parameters to be displayed in the parameters grid.	XML file - see related paragraph for the default

8.2.1 Low/Medium/High PriorityAlarmSound

These system options make it possible to associate a different sound to the notification of alarms respect to the default one. It is suggested when the healthcare organization uses similar sounds for other type of alerts. To do that:

1. Click the relevant system option on the list of system options displayed on screen (Fig 28 **A**).

The corresponding row is highlighted; the system option details are displayed on the lower area of the screen (Fig 28 B).

Application S	MARICENTRAL V	Name		H.U			Host Name			Apply Filter	Clear
	Name	Application	Hospital Unit	Hostname	Username			Value			
HighPriorityAla	rmSound	SMARTCENTRAL									
LogOptions		SMARTCENTRAL			<	?xml version="1.0"?>	>				
LowPriorityAlar	mSound	SMARTCENTRAL									
MediumPriority	AlarmSound	SMARTCENTRAL									
SmartCentralAl	armAggregatorsConfig	SMARTCENTRAL									
SmartCentralCo	nfig	SMARTCENTRAL			<	SmartCentral> <sma< td=""><td>artCentralConf</td><td>ig MyPatientBedC</td><td>ount="3"</td><td>Central ColumnO</td><td>ount="4" Cent</td></sma<>	artCentralConf	ig MyPatientBedC	ount="3"	Central ColumnO	ount="4" Cent
SmartCentralGr	idConfig	SMARTCENTRAL			<	?xml version="1.0" er	ncoding="utf-	-16"?>			
SmartCentralTr	endsConfig	SMARTCENTRAL			<	?xml version="1.0" er	ncoding="utf-	-16"?>			
System Options											
- System Options Name	HighPriorityAlam	nSound			~	Host Nam	ne				
- System Options Name Application	HighPriorityAlam	nSound AL			V	Host Nam	ne peenum_Op	tionTypeEnum_Bin	ary		
System Options Name Application H.U.	HighPriorityAlam SMARTCENTR	nSound				Host Nam] Typ	ne peenum_Op	tionTypeEnum_Bin	ary		
- System Options Name Application H.U. Description	HighPriorityAlam SMARTCENTR Change high prio	nSound AL			· · · ·	Host Nam	ne	otionTypeEnum_Bin	iary		
System Options Name Application H.U. Description	HighPriorityAlam SMARTCENTR Change high prio	nSound AL prity alarm sound.			· · · · ·	Host Nam Tyr Us Valu	neor	xtionTypeEnum_Bin	iary		
System Options Name Application H.U. Description	HighPriorityAlam SMARTCENTR Change high prio	Sound AL			· · · ·	Host Nam Tyr Us Valu	ne Peenum_Op er	otion TypeEnum_Bin	ary		

2. Click the Choose a file... button (Fig 28 C). The following window opens

	FILE SELECTION							
Application					~	Apply Filter	Clear Filter	
Filename	Туре	Application	Size		Last Update			
ascomlogo.png	AUDIO	~	12 KB	22/11/2017 07:57:25				
NEW	DELETE	VIEW	DOWNLO	OAD NONE		ок	CANCEL	
				Fig 29				

On this window all the available files are listed.

3. Select the row corresponding to the wanted file and click Ok (Fig 29 A).

The file is this way associated to the alarm. The name of the file will be displayed on the button indicated in Fig 28 C.

To add a new file to the list of available files

1. Click the **Download** button (Fig 29 **B**).

A window opens, making it possible to browse the uploaded content.

2. Locate the wanted file and click **Save**. The file will be added to the list of available files.

8.2.2 LogOptions

The LogOptions System option makes it possible to define different options regarding how the logs are stored and sent. To edit the logs-related options:

1. Click the LogOptions system option on the list of system options displayed on screen (Fig 30 **A**).

The corresponding row is highlighted, the system option details are displayed on the lower area of the screen (Fig 30 B).

Application SMARTC	ENTRAL 🗸	Name		H.U	I	н	ost Name		Apply Filt	ter	Clear Fi
Name		Application	Hospital Unit	Hostname	Username			Value			
HighPriorityAlarmSound	ł	SMARTCENTRAL									
LogOptions		SMARTCENTRAL			<	<pre>?xml version="1.0"?></pre>					
LowPriorityAlarmSound		SMARTCENTRAL									
MediumPriorityAlarmSc	ound	SMARTCENTRAL									
SmartCentralAlarmAgg	regatorsConfig	SMARTCENTRAL									
SmartCentralConfig		SMARTCENTRAL			<	SmartCentral> <smart(< td=""><td>CentralConfig My</td><td>PatientBedCount</td><td>t="3" CentralCol</td><td>umnCount="4</td><td>4" Centra</td></smart(<>	CentralConfig My	PatientBedCount	t="3" CentralCol	umnCount="4	4" Centra
SmartCentralGridConfig	1	SMARTCENTRAL			<	?xml version="1.0" enc	oding="utf-16"?>	·			
SmartCentralTrendsCor	nfig	SMARTCENTRAL			<	?xml version="1.0" enc	oding="utf-16"?>	•			
Scher Orling											
System Options	LogOptions					Host Name					
System Options Name	LogOptions	L			~	Host Name Type	enum_OptionTi	/peEnum_Text			
System Options Name L Application S H.U.	LogOptions	L			· · · · ·	Host Name Type User	Option Ty	/peEnum_Text			
System Options Name L Application S H.U. Description N	.ogOptions SMARTCENTRA Manage DLS (Dig	L jistat Logging Syst	em).			Host Name Type User Value	enum_OptionTy enum_OptionTy 	ypeEnum_Text			
System Options Name Application S H.U. Description N	ogOptions SMARTCENTRA Manage DLS (Dig	L jistat Logging Syst	em).		· · · ·	Host Name Type User Value	enum_OptionTy citago citago	ypeEnum_Text			
System Options Name [Application [H.U. Description [LogOptions SMARTCENTRA Manage DLS (Dig	L jistat Logging Syst	em).		· · · ·	Host Name Type User Value	enum_OptionTy Coml version="1" CogToFle>False	/peEnum_Text .0"?> e TeinetPort> dard SMTPHost> SMTPHost>			

2. Click the **Xml** button indicated in Fig 30 **C**. The following window opens

LogOptions	
Log to File	⊖ Yes ● No
Log to DB	● Yes ○ No
Telnet Port	0
Log Level	Standard V
Email	
Subject	
From Email	
From Name	
Codes	
Destinations	
Mail Server	
Hostname	
Port	0
Use SSL	
Username	
Password	
	OK CANCEL
	Fig 31

On this window the following features can be defined:

• Log to File – Stores the logs on a file.

- Log to DB Stores the logs on a database.
- **Telnet Port** Sets the Telnet port from which the logs are sent.
- Log Level Defines the log level;
- E-mail Makes it possible to automatically send certain specified logs via e-mail to a list of defined recipients. Such a functionality is used only for debug purposes.
- 3. Click **Ok** when done.

The resulting xml file will be displayed on the System Options screen, in the area indicated in Fig 30 \mathbf{D} .

8.2.3 SmartCentralAlarmsAggregatorsConfig

This system option makes it possible to define the list of alarms to be aggregated during the generation of dashboards (as displayed on the dashboard print report). I.e.: different instances of the same alarm can be aggregated and displayed under the same one label on the dashboard print report (in the alarms detailed list section). Example: there are devices that generate alarm text with parameter value included (ex. HIGH HR 120). These alarms are logged and displayed as different alarms in the dashboard report (HIGH HR 120 is different from HIGH HR 130). This configuration setting give you the ability, playing with regular expressions, to merge multiple alarms in a single on (ex. HIGH HR 120 and HIGH HR 130 could be transformed in a single alarm HIGH HR).

To edit this option

1. Click the SmartCentralAlarmsAggregatorsConfig system option on the list of system options displayed on screen (Fig 32 **A**).

The corresponding row is highlighted, the system option details are displayed on the lower area of the screen (Fig 32 B).

home > gener	AL CONFIGURAT										
Application SMAP	RTCENTRAL V	Name		H.U		Ho	ost Name		Apply F	iter	Clear Filt
Nam	ie	Application	Hospital Unit	Hostname	Username			Value			
HighPriorityAlarmSc	ound	SMARTCENTRAL									
LogOptions		SMARTCENTRAL				xml version="1.0"?					
LowPriorityAlarmSo	und	SMARTCENTRAL									
MediumPriorityAlar	mSound	SMARTCENTRAL									
SmartCentralAlarmA	ggregatorsConfig	SMARTCENTRAL									
SmartCentralConfig		SMARTCENTRAL				<smartcentral><smartc< td=""><td>CentralConfig MyPa</td><td>tientBedCount</td><td>="3" Central Co</td><td>lumnCount</td><td>="4" Central</td></smartc<></smartcentral>	CentralConfig MyPa	tientBedCount	="3" Central Co	lumnCount	="4" Central
SmartCentralGridCo	onfig	SMARTCENTRAL				xml version="1.0" enco</td <td>oding="utf-16"?></td> <td></td> <td></td> <td></td> <td></td>	oding="utf-16"?>				
SmartCentralTrends	Config	SMARTCENTRAL				xml version="1.0" enco</td <td>oding="utf-16"?></td> <td></td> <td></td> <td></td> <td></td>	oding="utf-16"?>				
System Options											
System Options	SmartCentralAlar	mAggregatorsCorl	fig			Host Name					
System Options Name Application	SmartCentralAlar SMARTCENTR/	m.AggregatorsConi	fig			Host Name	OptionTyp	eEnum_Text			
System Options Name Application H.U.	SmartCentralAlar SMARTCENTR/	mAggregatorsCori AL	ig		 	Host Name Type User	enum_OptionTyp	eEnum_Text			
System Options Name Application H.U. Description	SmartCentralAlar SMARTCENTR/	mAggregatorsCori AL t must be aggrega	fig ted during dashb	poard generati		Host Name Type User Value	OptionTyp	eEnum_Text			
System Options Name Application H.U. Description	SmartCentralAlar SMARTCENTR/ List of alarms that	m.AggregatorsCorr AL t must be aggrega	fig ted during dashb	poard generati	ion.	Host Name Type User Value	enum_OptionTyp	eEnum_Text			
System Options Name Application H.U. Description	SmartCentralAlar SMARTCENTR/ List of alarms that	mAggregatorsCorr AL t must be aggrega	fig ted during dashb	poard generati		Host Name Type User Value	enum_OptionTyp	eEnum_Text			

Click the Xml button indicated in Fig 32 C. The following window opens (Fig 33).

SmartCentral Alarm Aggregators Config					
Aggregators	(Collection)				
	ОК	CANCEL			
	Fig 33				

3. Click the "Aggregators" row (Fig 33 **A**). A button is this way displayed on the right (Fig 34 **A**).

SmartCentral Alarm Aggregators Config							
⊿ Misc							
Aggregators	(Collection)						
	ОК	CANCEL					
	Fig 34						

4. Click the button indicated in Fig 34 A. The following window opens (Fig 35).

AlarmAggregator Collection Editor							
Members:	Properties:	ncel					
	Fig 35						

To add a new alarm aggregator

5. Click the **Add** button (Fig 35 **A**). The members area will be this way populated with the AlarmAggregator item (Fig 36 **A**).

AlarmA	ggregator Collection Editor ? X
Members: O AlarmAggregator Add Remove	Alam regeator properties:
	OK Cancel
	Fig 36

The item properties are displayed on the right (Fig 36 B).

- 6. Insert as MatchingRegex a list of regular expressions, each one matching the alarm that must be aggregated. Example: HIGH HR [0-9]+ will match the previous example.
- 7. Insert as ResultString the string that will be actually displayed on the dashboard print report alarms list. Example: HIGH HR
- 8. Click **Ok** (Fig 36 **B**).

The alarm aggregator is this way defined and selected. The resulting xml file will be displayed on the System Options screen, in the area indicated in Fig 37.

Value	<pre><?xml version="1.0" encoding="utf-16"?> <alamnaggregators xmlns="" xsd="http://www.w3.org/2001/XMLSchema" xsi="http://www.w3.org/2001/XMLSchema- instance"> <aggregators> <alamnaggregator></alamnaggregator> </aggregators> </alamnaggregators></pre>	<
Xml		~

Fig 37

8.2.4 Smart Central Config

The SmartCentralConfig system option makes it possible to configure different features of the way information is displayed on the Digistat Smart Central user interface.

To edit this option

1. Click the SmartCentralConfig system option on the list of system options displayed on screen (Fig 38 **A**).

The corresponding row is highlighted, the system option details are displayed on the lower area of the screen (Fig 38 B).

Application SMAR	RTCENTRAL V	Name		H.U	J.	H	ost Name		Apply Filter	Clear F
Nam	ie	Application	Hospital Unit	Hostname	Username			Value		
HighPriorityAlarmSc	ound	SMARTCENTRAL								
LogOptions		SMARTCENTRAL				xml version="1.0"?				
LowPriorityAlarmSo	und	SMARTCENTRAL								
MediumPriorityAlar	mSound	SMARTCENTRAL								
SmartCentralAlarmA	ggregatorsConfig	SMARTCENTRAL								
SmartCentralConfig		SMARTCENTRAL				<smartcentral><smart(< td=""><td>CentralConfig MyPat</td><td>ientBedCount=</td><td>="3" Central ColumnC</td><td>Count="4" Centra</td></smart(<></smartcentral>	CentralConfig MyPat	ientBedCount=	="3" Central ColumnC	Count="4" Centra
SmartCentralGridCo	onfig	SMARTCENTRAL				xml version="1.0" enc</td <td>oding="utf-16"?></td> <td></td> <td></td> <td></td>	oding="utf-16"?>			
SmartCentralTrends	Config	SMARTCENTRAL				xml version="1.0" enc</td <td>oding="utf-16"?></td> <td></td> <td></td> <td></td>	oding="utf-16"?>			
System Options										
System Options	SmartCentralCor	ifig				Host Name				
System Options Name Application	SmartCentralCor SMARTCENTRA	ifig AL				✓ Host Name Type	Option Type	Enum_Text		
System Options Name Application H.U.	SmartCentralCor SMARTCENTR	rfig AL				✓ Host Name Type	enum_OptionType	Enum_Text		
System Options Name Application H.U. Description	SmartCentralCor SMARTCENTR. General SmartCe	rlig AL entral configuration				Host Name Type User Value	enum_OptionType <smartcentral><sm CentralOumnCount DeviceTypeOrder= LastEventHours="1" Sans Pro. 12.Regular" 52 Sans Pro. 12.Regular" 52 Sans Pro. 12.Regular" 52 Sans Pro. 12.Regular" 52 Sans Pro. 12.Regular String= ForntAlamValues="5"</sm </smartcentral>	Enum_Text atCentralConfig ="4" CentralRo 4",57,691,183 0" FirstDaplay 0" FortMod ""0" FortMod "20" FortMod "20" FortMod "20" FortMod "20" FortMod	MyPatientBedCoun wCount="2" 398:2:3", CentralBe edPage="1" STFont 398:2:3", CentralBe edPage="1" STFont 998:2:3", Central edPage="1" Store fontAame"Source Sans Pro FontAame"Source 5,18,Bold" FontMore	t="3" Ifiter="" "Source Sans 2.Regular" 12.Regular" Sans Pro, 18.Bo Devices="Sources"Sources

Click the Xml button indicated in Fig 38 C. The following window opens (Fig 33).

	S	martCentra	l Config	-	_		
I	D	Grid Layout	Device Type	Alarms	and Values		
		My Patient B	Bed Count		3 🗘		
		Central Colu	ımn Count		4 🗘		
		Central Row	Count		2		
		First Display	ved Page in cent	ral	1		
		Central Bed (loc1=bed1,t	Filter bed2;loc2)				
		Details Inope (0=disabled)	erativity Timeou	t sec.	0 🔹		
	l						
						OK	CANCEL



Three configuration tabs are available (Fig 39 A):

- Grid layout (see related paragraph).
- Device type (see related paragraph).
- Alarms and Values (see related paragraph).

8.2.4.1 Grid layout

The following features can here be defined (Fig 39):

- My patient bed count maximum number of beds that can be selected as My Patients. This parameter is used only on a bed side workstation.
- Central column count number of columns displayed on the Central screen.
- Central row count number of row displayed on the Central screen.
- First displayed Page in central first page displayed on the Central screen if beds are displayed in multiple pages.
- Central bed filter if specified, the Central screen can display different sets of beds (usually belonging to different locations). Type: location name1=Bed1, Bed2...Bedn; location name2=Bed1, Bed2...Bedn etc.

- Details Inoperativity Timeout - defines the number of seconds of inoperativeness in the detailed screen after which the application switch to the main view.

8.2.4.2 Device type

Define here the device type order in which device data is displayed on the patient bed area (order by device using the arrow buttons indicated in Fig 40 **A**.

SmartCentral Config			
Grid Layout Device Type Alarms ar	nd Values		
Device Type Order	AnesthesiaDeliveryUnit BloodFiltration BloodGasAnalyzer HeartLungMachine Incubator InfusionPump LaboratoryInformationSystem OtherComplex OtherSimple PatientMonitor PulmonaryVentilator		
	OK CANCEL		
Fi	g 40		

8.2.4.3 Alarms and values

Define here the format of the information displayed on the Digistat Smart Central (fonts, sizes, order etc.).

S	SmartCentral Config				
	Grid Layout Device Type Alarms and Values				
	S1 Font	Source Sans Pro,12,Regular			
	S2 Font	Source Sans Pro,12,Regular			
	S3 Font	Source Sans Pro,12,Regular			
	Font Model	Source Sans Pro, 12, Regular			
	Model Format string. (%DE = Device Name. %MO = Model Name. %MA = Manufacturer)	%MO - %MA			
	Font Alam	Source Sans Pro, 18, Bold			
	Font Alarm (VALUES MODE)	Source Sans Pro,18,Bold			
	Font More Device/Alarms/Warnings	Source Sans Pro, 13, Bold			
	Column Size	500 🗘			
	Column Size (VALUES MODE)	500 🗘			
	Maximum Alarm Row Count	0			
	Alarm History Counter (sec)	60 🗘			
	Alarm snapshots duration (in days, 0=disabled)	0			
		OK CANCEL			

Fig 41

- S1 S2 S3 font the letter "S" refers to the fonts used to display vital signs parameters.
- Font Model Font used to display the device model (if the Model Format String is not empty).
- Model Format String This field allows to define the way the device Model is displayed. If empty the device model is not displayed.
- Font Alarm Font for the alarm notifications when the "Values" button is not selected in the application.
- Font Alarm (VALUES MODE) Font for the alarm notifications when the "Values" button is selected in the application.
- Font More Device/Alarms/Warnings Font used for the label "More Devices" or "More Alarms" or "More Warnings"
- Column size Size of columns inside the patient bed area when the "Values" button is not selected in the application.

- Column size (VALUES MODE) Size of columns inside the patient bed area when the "Values" button is selected in the application.
- Maximum Alarm Row Count Maximum number of rows available for the alarms notification.
- Alarm history counter Number of seconds for which the alarm history bar has to be displayed.
- Alarms snapshots duration Number of days the alarms snapshots are maintained in the file system (set 0 to disable such functionality).

Click **Ok** when done (Fig 41 **A**).

The Digistat Smart Central contents will be displayed accordingly. The resulting xml will be displayed on the System Options screen, in the area shown in Fig 37.



Fig 42

8.2.5 Smart Central Grid Config

To edit this option

1. Click the SmartCentralGridConfig system option on the list of system options displayed on screen (Fig 43 **A**).

The corresponding row is highlighted, the system option details are displayed on the lower area of the screen (Fig 43 B).

Nam	ne	Application	Hospital Unit	Hostname	Username			Value		
HighPriorityAlarmSo	ound	SMARTCENTRAL								
LogOptions		SMARTCENTRAL				xml version="1.0"? .				
LowPriorityAlarmSo	und	SMARTCENTRAL								
MediumPriorityAlar	mSound	SMARTCENTRAL								
SmartCentralAlarmA	AggregatorsConfig	SMARTCENTRAL								
SmartCentralConfig		SMARTCENTRAL				<smartcentral><smart< td=""><td>tCentralConfig</td><td>MyPatientBedCour</td><td>nt="3" Central ColumnCo</td><td>unt="4" Centr</td></smart<></smartcentral>	tCentralConfig	MyPatientBedCour	nt="3" Central ColumnCo	unt="4" Centr
SmartCentralGridCo	onfig	SMARTCENTRAL				xml version="1.0" en</td <td>coding="utf-1</td> <td>5"?></td> <td></td> <td></td>	coding="utf-1	5"?>		
SmartCentralTrends	Config	SMARTCENTRAL				xml version="1.0" en</td <td>coding="utf-1</td> <td>5"?></td> <td></td> <td></td>	coding="utf-1	5"?>		
Sustan Onlines										
System Options	SmattCentralGrid	IConfin				Host Name				
System Options	SmartCentralGrid	IConfig				⊻ Host Name	e			
System Options Name Application	SmartCentralGrid	IConfig				⊻ Host Name Tγρι	e	n Type Enum_Text		
System Options Name Application H.U.	SmartCentralGrid	IConfig AL				✓ Host Name Type Use	eOptic	on TypeEnum_Text		

Fig 43

2. Click the **Xml** button indicated in Fig 43 **C**. The following window opens (Fig 44).

SmartCentral Grid Config			
A Misc Parameters	(Collection)		
	ОК	CANCEL	
	Fig 44		

3. Click the "Parameters" row (Fig 44 **A**). A button is this way displayed on the right (Fig 45 **A**).

SmartCentral Grid Config				
Misc Parameters	(Collection)			
	ОК	CANCEL		
	Fig 45			

4. Click the button indicated in Fig 45 A. The following window opens (Fig 46).

GridPara	meter Collection Editor
Members: 0 HR 1 ARTs 2 ARTd 3 ARTm 4 RR 5 SP02 6 Fi02 Add Remove	HR properties:
	OK Cancel
	Fig 46

To add a new parameter

5. Click the Add button (Fig 46 A). A new Parameter is this way added (Fig 47 A).

GridPara	ameter Collection Editor
Members: 0 HR 1 ARTs 2 ARTd 3 ARTm 4 RR 5 SPO2 6 FiO2 7 GridParameter Add Remove	GridPerseter properties:

Fig 47

The item properties will be displayed on the right (Fig 47 B - empty at the moment).

6. Click the ParameterId row (Fig 48 A). A button is displayed on the right (Fig 48 **B**).



7. Click the button indicated in Fig 48 **B**. The following window opens (Fig 49).

	(Choose a paran	neter	A
Driver Model Device	Monitor Pumps Ventilator			V
ID	Name	Description		
			Select	Cancel
		Fig 49		

8. Click the button indicated in Fig 49 **A** to open the drop down "Driver" list. Here select the relevant item. The window will be populated with the list of parameters relating to the selected item (Fig 50).

			Choose a parame	ter		x
	Driver	Pumps_Te	st			¥
	Model	Infusomat	Space			
	Device	BBrown				
	ID	Name	Description			~
	13	PatWeight	Patient Weight (current)			
	8001	DrugConc	Drug Concentration			
	8003	DrugName	Drug Name			
	8005	Pump Status	Pump Status			
	8006	GenDevStatus	General Device Status			
	8007	DoseRate	Dose Rate			=
(A)	8009	VolumeRate	Volume Rate			
	8010	InfusedVolume	Infused Volume			
	8011	VTBI	Volume To Be Infused			
	8013	PumpPressure	Pressure			
	8016	PumpTimeRemain	Infusion time remaining			
	8016	PumpTimeRemain	Infusion time remaining			
	8018	DeviceName	Device Name	(B)		$\overline{}$
				Salact	Cancel	
				JUICOL	Cancer	
			Fig 50			

- 9. Click the row corresponding to the wanted parameter on the list (Fig 50 **A**). The row will be highlighted.
- Click Select (Fig 50 B). The selected parameter is this way added to the "Members" list on the GridParameter collection editor window (Fig 51 A). The selected parameter properties are displayed on the right (Fig 51 B).

Members: VolumeRate properties: 0 HR 1 ARTs 2 ARTd 3 ARTm 4 RR 5 SPO2 6 FiO2 7 VolumeRate 8 VolumeRate 8 VolumeRate Add Remove OK Cancel		GridPara	meter Collection Editor
	A	Members: 0 HR 1 ARTs 2 ARTd 3 ARTm 4 RR 5 SPO2 6 FiO2 7 VolumeRate 8 VolumeRate Add Remove	VolumeRate properties:

Fig 51

If necessary, the ParameterNameCustom field (Fig 52 \bf{A}) can be manually edited to define a customized name

Volu	meRate properties	:						
	≵ ↓ □							
⊿	Misc							
⊳	ParameterId	8009						
	ParameterName	VolumeRate						
	A ParameterName(
_								
	Fi	g 52						

11. Click **OK** to complete the procedure (Fig 51 C).

The SmartCentralGrid configuration is this way defined. The resulting xml file will be displayed on the System Options screen, in the area shown in Fig 53.



Fig 53

8.2.6 Smart Central Trend Config

Accessing the Smart Central Trend Config allows to configure which and how many charts are displayed inside the Charts tab on the Patient's event list screen. To edit this option

1. Click the SmartCentralGridConfig system option on the list of system options displayed on screen (Fig 54 **A**).

The corresponding row is highlighted, the system option details are displayed on the lower area of the screen (Fig 54 **B**).

		Name		H.U		He	ost Name		Apply Filt	cer C	Liear
Na	ame	Application	Hospital Unit	Hostname	Username			Value			
HighPriorityAlarm	Sound	SMARTCENTRAL									
LogOptions		SMARTCENTRAL				xml version="1.0"?	-				
LowPriorityAlarms	Sound	SMARTCENTRAL									
MediumPriorityAla	armSound	SMARTCENTRAL									
SmartCentralAlarn	nAggregatorsConfig	SMARTCENTRAL									
SmartCentralConfi	ìg	SMARTCENTRAL				<smartcentral><smartc< td=""><td>CentralConfig My</td><td>PatientBedCoun</td><td>nt="3" Central Col</td><td>umnCount="4" (</td><td>Centr</td></smartc<></smartcentral>	CentralConfig My	PatientBedCoun	nt="3" Central Col	umnCount="4" (Centr
SmartCentralGrid(Config	SMARTCENTRAL				xml version="1.0" enco</td <td>oding="utf-16"?</td> <td>×</td> <td></td> <td></td> <td></td>	oding="utf-16"?	×			
SmartCentralTrend	dsConfig	SMARTCENTRAL				xml version="1.0" enco</td <td>oding="utf-16"?</td> <td></td> <td></td> <td></td> <td></td>	oding="utf-16"?				
Sudar Ordinas											
System Options	SmartCentralTre	ndsConfig				✓ Host Name					
System Options	SmartCentralTre	ndsConfig				✓ Host Name					
System Options – Name Application	SmartCentralTre	ndsConfig				✓ Host Name Type	OptionT	ypeEnum_Text			
System Options Name Application H.U.	SmartCentralTre SMARTCENTR	ndsConfig AL				✓ Host Name Type • User	OptionT	ypeEnum_Text			

Fig 54

2. Click the **Xml** button indicated in Fig 54 **C**. The following window opens (Fig 55).



3. Click the "Configuration" row (Fig 55 **A**). A button is this way displayed on the right (Fig 56 **A**).

Sm	SmartCentral Trends Config							
⊿	Misc Configuration	(Collection)						
	OK CANCEL							
		Fig 56						

4. Click the button indicated in Fig 56 A. The following window opens (Fig 57).

TrendChar	ts Collection Editor ? ×
Members:	Properties:
	Fig 57

To add a new member

5. Click the Add button (Fig 57 A). A new Member is this way added (Fig 58 A).

TrendCl	harts Co	llection Editor		?	x
Members: 0 TrendCharts Add Remove	 ↑ 	Trend Charts properties Misc Bed Charts SizeMode	(Collection AutoFit)	
		C)K	Cancel	
	Fig	58			

The item properties will be displayed on the right (Fig 58 B - empty at the moment).

6. Click the "Bed" row to define the bed to which the chart refers (Fig 59 A).

TrendCharts prop	erties:
ê≣ ≵ ↓ 🖾	
⊿ Misc	
Bed	✓
Charts	ICU 1 (1)
SizeMode	ICU 2 (2)
	ICU 3 (3)
	ICU 4 (4)
	ICU 5 (5)
	ICU 6 (6)
	ICU 7 (7)
	ICU - 8 (8)
	appoggio - 10 (10)
	appoggio 9 (9)
	OK Cancel
	Eia EQ

Fig 59

7. Click the "SizeMode" row to select either AutoFit mode or Scrollable mode for the chart (Fig 60).

ICU 1 (1) properties:							
₿ ₽							
⊿ Misc							
Bed	ICU – 1 (1)						
Charts	(Collection)						
SizeMode	AutoFit 🗸 🗸						
	Auto Fit						
	Scrollable						
	01/						
	OK Cancel						
F	ig 60						

8. Click the "Charts" row to define the charts features (Fig 61 **A**). A button is displayed on the right (Fig 61 **B**).



9. Click the button indicated in Fig 61 **B**. The following window opens (Fig 62).

TrendChart Collection Editor							
Members:	*	Properties:					
	Fig	62					

10. Click the Add button (Fig 62 A). A new Member is this way added (Fig 63 A).

Members: 0 TrendChart	TrendChart Co	Trend Carl propertie Trend Carl propertie Trend Carl propertie	25: 0 (Collection)
Add Re	move	63	OK Cancel

The item properties will be displayed on the right (Fig 63 B - empty at the moment).

11. Define here the Chart height and title, the YFormat, YMax and YMin (all free text fields). Click the "Series" row to further define the chart features. A button is displayed on the right. Click the button. The following window opens (Fig 64).

TrendSerie Collection Editor							
Members:	Propeties:						
	Fig 64						

12. Click the Add button (Fig 64 A). A new Member is this way added (Fig 65 A).

Members: 0 TrendSerie Add	Remove	*	Tren ♥ ■	Misc Actual Device Na Chart Type ColorRGB MarkerStyleFilte Name ParameterId ParameterId ParameterId ParameterId	Point Point None None Auto	
Add	Remove					
				(ОК	Cancel

The item properties will be displayed on the right (Fig 65 B - empty at the moment).

- 13. Define here on drop down menus: the actual device name, the Chart Type, the Color, the markers styles for the device On/Off markers, the TrendSerie name (free text), the type of Y value.
- 14. Click the ParameterId row to associate the id of the parameter to be charted. A button is displayed on the right. Click the button. The following window opens (Fig 66).

	C	hoose a param	eter	A
Driver	Monitor			×
Model	Pumps			
Device	- Charles			
ID	Name	Description		
			Select	Cancel
		Fig 66		111

15. Click the button indicated in Fig 66 **A** to open the drop down "Driver" list. Here select the relevant item. The window will be populated with the list of parameters relating to the selected item (Fig 67).

		Ch	oose a parame	ter	x
	Driver	Monitor_Test			~
	Model Carescape B450]
	Device	GEMonitor			
			D		
	ID	Name	Description		^
	2001	HR ECG	HR - ECG		=
	3004	Pulse Rate Non Inv	Pulse Rate (Non In	vasive)	
	3009	NBPs	Non-invasive blood	pressure: Systolic	
A)	3011	NBPd	Non-invasive blood	pressure: Diastolic	
	3013	NBPm	Non-invasive blood	pressure: Mean	
	3015	ARTs	Arterial Blood Press	ure: Systolic	
	3016	ARTd	Arterial Blood Press	ure: Diastolic	
	3017	ARTm	Arterial Blood Press	ure: Mean	
	3018	PAPs	Pulmonary Arterial F	Pressure: Systolic	
	3019	PAPd	Pulmonary Arterial F	Pressure: Diastolic	
	3020	PAPm	Pulmonary Arterial F	Pressure: Mean	
	3027	BPs	Unspecified blood p	pressure: Systolic	~
	<			(B)	>
				Select	Cancel
			Fig 67		

- 16. Click the row corresponding to the wanted parameter on the list (Fig 67 **A**). The row will be highlighted.
- 17. Click **Select** (Fig 67 **B**). The selected parameter is this way associated to the chart.
- 18. Click **OK** on all the opened windows to complete the procedure.

The SmartCentralChart configuration is this way defined. The resulting xml file will be displayed on the System Options screen, in the area shown in Fig 68.



Fig 68

8.3 Smart Central Mobile System Options

To configure the Smart Central Mobile system options access the Administrator/Application System Options area on the DIGISTAT[®] configuration application. The path is shown in Fig 69.

HOME CENERAL CONFIGURATOR SYSTEM CONFIGURATION ADMINISTRATOR/APPLICATION SYSTEMOPTIONS

The following screen opens (Fig 70).

Application Name AcquisitionDemoMode ADTAdmissionMode AutoEnableNetwork BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFilt DASDataExpiration DASEventExpiration HelpPath Highart	Applicat SplitChar	Name	Hostname	H.U.	0	He	value	Apply Filter	Clear Filter
Name AcquisitionDemoMode ADTAdmissionMode AutoEnableNetwork BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFile DASDataExpiration DASEventExpiration HelpPath	Applicat SplitChar	on Hospital Unit	Hostname	Username	0		Value		
AcquisitionDemoMode ADTAdmissionMode AutoEnableNetwork BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFilb DASDataExpiration DASEventExpiration HelpPath	SplitChar				0				~
ADTAdmissionMode AutoEnableNetwork BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFile DASDataExpiration DASEventExpiration HelpPath	SplitChar								
AutoEnableNetwork BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFilt DASDataExpiration DASEventExpiration HelpPath Hisbarthoonemous	SplitChar				0				
BarCodeMultiMessageSp CleanDBTime ConfiguratorModulesFilt DASDataExpiration DASEventExpiration HelpPath	SplitChar				1				
CleanDBTime ConfiguratorModulesFilt DASDataExpiration DASEventExpiration HelpPath	terino								
ConfiguratorModulesFilt DASDataExpiration DASEventExpiration HelpPath	tering				01:00:00				
DASDataExpiration DASEventExpiration HelpPath	icaning				SYSTEMOPTIONS;NETWORKS;BEDS;LOCATIONS;USERS;PERMISSIONS;DRIVERCONTENT;DEVICEDRIVER;M			ICEDRIVER;M	
DASEventExpiration HelpPath									=
HelpPath HighestAnommous									
HighestAnomymous					C:\Digistat\S	Smart Central \help\			
ringinest Anonymous					0				
PrivacyMode			0						
ReportHeader				HOSPITAL					
ReportsPath			C:\Digistat\Smart Central\						
ShowPrintDialog					0				
SystemOptionEditableAp	Application				xml versio</td <td>n="1.0" encoding="ut</td> <td>f-16"?> <arrayofstring td="" xmlns<=""><td>:xsi="http://www.w3.org/2001</td><td>1/XMLSchema 🗠</td></arrayofstring></td>	n="1.0" encoding="ut	f-16"?> <arrayofstring td="" xmlns<=""><td>:xsi="http://www.w3.org/2001</td><td>1/XMLSchema 🗠</td></arrayofstring>	:xsi="http://www.w3.org/2001	1/XMLSchema 🗠
System Options									
News	an dellar Dense Made					11			
Name AC	cquisitionDemomode	\$			×	Host Name			Inis
Application						Туре	_enum_OptionTypeEnum_Bo	bl	~
H.U.						User			
Description To	n - Domonstration	lada, capacitas ci	odom data. E	alaa - Aagu in	a Real Data	Value			
Description fro	om devices	ioue, generales fai	ndom data. P	aise=Acquire		Value	O Irue O Faise		
NEW	FDIT	DELETE	CODV						

6 Select "**Smart Central**" on the "**Application**" filter indicated in Fig 70 **A** (enlarged in Fig 71) and then click **Apply Filter** (Fig 70 **B**).

Application	SMARTCENTRALN V	
	BROWSER	
	CONTROLBAR	
HighPriorityA	DAS	
LogOptions	DIGISTATMOBILE	
L	REPORTMASTER	
LowPriorityA	SMARTCENTRAL	
Medium	MARTCENTRALMOBI	
	TURBOPATIENT	
SmartCentral	ianninggi ogacaloconing	
SmartCentral	Config	SM
Fia 71		

The Smart Central system options list is this way displayed (Fig 72).

HOME > GENERAL CONFIGURATOR > SYSTEM CONFIGURATION > ADMINISTRATOR/APPLICATION SYSTEMOPTIONS >								
Application SMARTC	ENTRALN V Name			H.U.	Hos	t Name	Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname	Username		Value		^
BatteryLimit	SMARTCENTRALMOBILE				15			
DeviceFormatString	SMARTCENTRALMOBILE				<formatstrings></formatstrings>			
EnableAlarmAudio	SMARTCENTRALMOBILE				1			
GridColumnCount	SMARTCENTRALMOBILE				3			
Language	SMARTCENTRALMOBILE				SV			
LatencyLimitMs	SMARTCENTRALMOBILE				2000			
Locale	SMARTCENTRALMOBILE							=
MyPatientsEnabled	SMARTCENTRALMOBILE				0			
OnlineParametersTimed	ut SMARTCENTRALMOBILE				30			
Orientation	SMARTCENTRALMOBILE				2			
PatientFormatString	SMARTCENTRALMOBILE				MRN:{4} Born on {1} ({2}) Set	x:{3}		
PingScheduleMs	SMARTCENTRALMOBILE				15000			
ReconnectScheduleMs	SMARTCENTRALMOBILE				10000			
ShowLocationName	SMARTCENTRALMOBILE				0			
SignalLimit	SMARTCENTRALMOBILE				40			~
System Options								
Name	atteryLimit				Host Name			This
Application 9	MARTCENTRALMOBILE				Туре	_enum_OptionTypeEnum_Integer		~
H.U.					User			
Description Ir	percentage. Lower limit that	triggers a notifica	tion alarm of	"unsafe"	Value 1	5 1 - 100		
a	pplication. Tipical value is 15-	20.						
L								
NEW	EDIT DELET	E C	OPY				CLOS	E
	•				Fig 72			

7 Click the row corresponding to the system option to be edited

The row is highlighted. The selected system option's data is displayed in the lower part of the screen.

- 8 Click the **Edit** button on the command bar. The screen turns to **Edit** mode (optional step).
- 9 Edit the system option's data. The screen turns automatically to **Edit** mode.
- 10 Click the **Update** button on the command bar.

The application configuration is this way changed.

NOTE:	If the "Host Name" field is empty, the configuration	
	change applies to all the devices. If the "Host Name" is	
	specified, the configuration change applies only to the	
	specified device.	

8.4 Smart Central Mobile System Options - Overview

This paragraph lists the Smart Central Mobile system options and their features.

Name	Description	Default Values
DeviceFormatString	Device format string in xml format. Defines how to display parameters.	See below for configuration info.
GridColumnCount	Number of columns displayed.	3
ShowLocationName	If true, the bed name will be displayed as "LocationName – BedName". If false: "BedName"	False (0).
SoundRepetition	Number of sound repetitions when a notification is provided.	1

Name	Description	Default Values
BatteryLimit	In percentage. Lower limit that triggers a notification alarm of "unsafe" application. Typical value is 15-20.	15
DeviceLanguage	Culture Info code used to translate text. If empty the "locale" setting of the device will be used.	See below for configuration info.
EnableAlarmAudio	If true, audio and vibration are enabled when a new alarm notification is displayed. Otherwise only the notification is displayed, without audio and vibration.	True (1).
---------------------	---	-----------------------------------
KeepAliveInterval	Interval between two keep alive messages.	15000
LatencyLimitMs	Below this value a 'slow network' notification is raised.	2000
LogFilesPath	Path for log files	C:\DigistatMobile\Logs
LogLevel	Clients log level: NONE=0; INTERNAL=1; VERBOSE=2; DEBUG=3; INFO=4; WARN=5; ERROR = 6	0
Logo	Logo for the main window	See below for configuration info.
MediaPath	Base path for media files	C:\DigistatMobile\Media
MyPatient	If true the MyPatient functionality is enabled	True
MyPatientMode	0=Only mine, 1=mine and not assigned, 2=mine and not connected, 3=mine and not assigned and not connected	3
ReconnectScheduleMs	Interval between two retries if Smart Central is disconnected.	10000
SignalLimit	In percentage. Wifi signal strength. Below this value a notification is raised.	40
TempPath	Path for temp upload folder	C:\DigistatMobile\Temp
TimeSyncTresholdMs	Above this value a notification is raised.	120000
Title	Title in the logo window	Digistat Mobile

8.4.1 DeviceFormatString configuration

The DeviceFormatString system option is an xml file making it possible to customize the way the patient parameters are displayed on the different screens.

To edit this system option, edit the code displayed in the field indicated in Fig 73 A.



Fig 73

This is a sample format string for a generic "Monitor":

```
<FormatStrings>
<FormatString DeviceType="MON">
<StringDetail type="1">{2001.Name}: {2001.Value}
{2001.Unit}</StringDetail>
<StringDetail type="2">{2001.Name}: {2001.Value} {2001.Unit}|{3015.Name}:
{3015.Value} {3015.Unit}|{3016.Name}: {3016.Value}
{3016.Unit}|{3017.Name}: {3017.Value} {3017.Unit}</StringDetail>
<StringDetail type="3">HR: {2001.Value} {2001.Unit}|{3015.Name}:
{3015.Value} {3015.Unit}|{3016.Name}: {3017.Unit}|{3015.Name}:
{3015.Value} {3015.Unit}|{3016.Name}: {3016.Value}
{3015.Value} {3015.Unit}|{3016.Name}: {3016.Value}
{3016.Unit}|{3017.Name}: {3017.Value} {3017.Unit}|{7010.Name}:
{7010.Value} {7010.Unit}</StringDetail>
```

The **Device Type** indicates the type of device (i.e. : MON for monitor, INF for Infusion Pump) The **Detail Type** refers to the type of "Card" displayed on the Smart Central Mobile screen.

- Type 1 is displayed on the "Devices List" screen (compact form).
- Type 2 is displayed on the "Devices List" screen (expanded form).
- Type 3 is displayed on the "Device History" screen.

Each Type is characterized by "**Name**" (device name), "**Value**" (type of value) and "**Unit**" (unit of measure). The number placed before (here for instance: 7010.Unit) refers to the actual item that will be displayed.

So, to provide an example, the string

<StringDetail type="1">{2001.Name}: {2001.Value}
{2001.Unit}</StringDetail>

indicates that for a specified acquisition device, the card on the "Devices list" screen (compact) will show the name "2001", the value "2001" and the unit of measure "2001". Whatever is written outside braces is displayed as it is. For instance, the ":" in the example provided - {2001.Name}: {2001.Value} etc.

The resulting "Card" will have the structure of that shown in Fig 74.



8.4.2 GridColumnCount configuration

The GridColumnCount system option allows to set the number of columns that will be displayed in the Central Screen view. The allowed values are expressed as integers between 1 and 10. Its default value is 3.



Fig 75

To modify the GridColumnCount system option enter the desired value in the text field indicated in Fig 75 **A**. All other fields and text boxes can remain unchanged.

8.4.3 ShowLocationName configuration

The ShowLocationName system option makes it possible to customize the way the Location Name and the Bed Name are displayed. If this option is set to true the Bed Name will be displayed according to the pattern "LocationName – BedName"; if this option is set to false the Bed Name will be displayed according to the pattern "BedName". The default value is false.

Main Actions	Applications About	> SYSTEM CO	onfigura	tion >	ADMINISTRA	ator/applic/	ATION SYSTEMOPTI	ons >					
Application SMAR	TCENTRALMOBILE	 Name 				H.U.			Host Name		Apply Filter	Clea	ır Filter
Name	Application	Hospital Unit	Hostname	Username					Va	alue			
DeviceFormatString	SMARTCENTRALMOBILE				<formatstring< th=""><th>gs></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></formatstring<>	gs>							
GridColumnCount	SMARTCENTRALMOBILE				3								
ShowLocationName	SMARTCENTRALMOBILE				0								
SoundRepetition	SMARTCENTRALMOBILE				1								
System Options													
Name	ShowLocationName						Host N	ame					This
Application	SMARTCENTRALMOBIL	.E					I	Type _enum_C	Option Type E	inum_Bool			~
H.U.							··· 👝 I	Jser					
Description	If true, the bed name will i	be displayed as	"LocationNa	me - BedNar	ne". If false: "Be	iedName"		alue 🔿 True	۲	False			
							Fig 7	6					

Use the checkbox indicated in Fig 76 **A** to edit the ShowLocationName system option. All other fields and text boxes can remain unchanged.

8.4.4 SoundRepetition configuration

The SoundRepetition system option makes it possible to customize the number of audible notifications occurring when a notification for the user is raised. The allowed values are expressed as integers between 1 and 3. Its default value is 1.

Main Actions	Applications About												
	L CONFIGURATOR	SYSTEM C	ONFIGURA	tion 📏	ADMINISTRA	TOR/APPLICAT	ION SYSTEMOPTION	vs 🔿	>				
Application SMART	TCENTRALMOBILE	 Name 				H.U.			Host Name		Apply Filter	Cle	ar Filter
Name	Application	Hospital Unit	Hostname	Username					Va	alue			
DeviceFormatString	SMARTCENTRALMOBILE				<formatstring< td=""><td>s></td><td></td><td></td><td></td><td></td><td></td><td></td><td></td></formatstring<>	s>							
GridColumnCount	SMARTCENTRALMOBILE				3								
ShowLocationName	SMARTCENTRALMOBILE				0								
Soundkepetition	SMARTCENTRALMOBILE												
System Options													
Name	SoundRepetition						 Host Name 	ne 📃					This
Application	SMARTCENTRALMOBIL	LE					Тур	e _enum	m_OptionTypeE	num_Integer			¥
H.U.							Use	er					
Description	Number of sound repetition	ons when a noti	fication is trio	aered.				10 1		1-3			
Description													
	L												
								-					

Fig 77

To edit the SoundRepetition system option enter the desired value in the text field indicated in Fig 77 **A**.

8.4.5 BatteryLimit configuration

The BatteryLimit system option makes it possible to set a threshold value for the battery charge level of the handheld device. When the battery charge level is lower than this value,

a notification of "Unsafe Application" is provided. The allowed percentage values are expressed as integers between 1 and 100. Its default value is 15.

Main Actions A	pplications Abo	ut								
Home 📏 general	CONFIGURATOR	SYSTEM	CONFIGURATION	> ADMINISTRATOR/APP	LICATION SYS	TEMOPTIONS	>			_
Application DIGIST/	TMOBILE	✓ Nan	1e	H.U.			Host Name		Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname Username				Value	e		
BatteryLimit	DIGISTATMOBILE			15						
DeviceLanguage	DIGISTATMOBILE			en						
EnableAlarmAudio	DIGISTATMOBILE			1						
KeepAliveInterval	DIGISTATMOBILE			15000						
LatencyLimitMs	DIGISTATMOBILE			2000						
LogFilesPath	DIGISTATMOBILE			C:\DigistatMobile\Logs						
LogLevel	DIGISTATMOBILE			0						
Logo	DIGISTATMOBILE			0ba53bde-ad95-4527-a05c-e	efd5d7deed8d					
MediaPath	DIGISTATMOBILE			C:\DigistatMobile\Media						
MyPatient	DIGISTATMOBILE			1						
MyPatientMode	DIGISTATMOBILE			3						
ReconnectScheduleMs	DIGISTATMOBILE			10000						
SignalLimit	DIGISTATMOBILE			40						
TempPath	DIGISTATMOBILE			C:\DigistatMobile\Temp						
TimeSyncTresholdMs	DIGISTATMOBILE			120000						
Title	DIGISTATMOBILE			Digistat Mobile						
System Options										
Name	BatteryLimit				~	Host Name				This
Application	DIGISTATMOBILE					Туре	_enum_OptionTypeEn	um_Integer		~
H.U. [User				
Description	In percentage. Lower 20.	limit that triggers	a notification alarm of "	unsafe" application. Tipical valu	e is 15-	Value	15		1 - 100	
					Fig 7	8				

To edit the BatteryLimit system option enter the desired value in the text field indicated in Fig 78 **A**.

8.4.6 DeviceLanguage configuration

The DeviceLanguage system option makes it possible to set the language that is used to translate text messages. If this field is empty, the translation will be performed according to the "locale" setting. The allowed values are alpha-numeric strings. No default value is set.

Main Actions A HOME GENERA	Applications Abo	out SYSTEN	I CONFIGURA	tion >administ	RATOR/APPLICATIO	N SYSTEMOPTIONS	>			
Application DIGIST	ATMOBILE	✓ Nar	me		H.U.		Host Name		Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname Us	ername			Valu	Je		
BatteryLimit	DIGISTATMOBILE			15						
DeviceLanguage	DIGISTATMOBILE			en						
EnableAlarmAudio	DIGISTATMOBILE			1						
KeepAliveInterval	DIGISTATMOBILE			15000						
LatencyLimitMs	DIGISTATMOBILE			2000						
LogFilesPath	DIGISTATMOBILE			C:\DigistatMob	xile\Logs					
LogLevel	DIGISTATMOBILE			0						
Logo	DIGISTATMOBILE			0ba53bde-ad9	5-4527-a05c-efd5d7dee	b8d				
MediaPath	DIGISTATMOBILE			C:\DigistatMol	pileMedia					
MyPatient	DIGISTATMOBILE			1						
MyPatientMode	DIGISTATMOBILE			3						
ReconnectScheduleMs	DIGISTATMOBILE			10000						
SignalLimit	DIGISTATMOBILE			40						
TempPath	DIGISTATMOBILE			C:\DigistatMol	pile\Temp					
TimeSyncTresholdMs	DIGISTATMOBILE			120000						
Title	DIGISTATMOBILE			Digistat Mobile						
System Options										
	B									
Name	DeviceLanguage				~	Host Name				This
Application	DIGISTATMOBILE					Туре	_enum_OptionTypeE	num_Text		~
H.U.						User				
Description	Digistat Mobile langu	age				Value	en			
Description	Ungolical Historic Rangan									~
						E. 70				

Fig 79

To edit the DeviceLanguage system option enter the desired string in the text field indicated in Fig 79 **A**.

8.4.7 EnableAlarmAudio configuration

The EnableAlarmAudio system option makes it possible to define the way alarms are notified. If true, audio and vibration are enabled when an alarm notification is displayed. If false, only the visual notification is provided, without audio and vibration. The default value is true.

Main Actions A	Applications Abo	out							
HOME GENERA	L CONFIGURATOR	SYSTEM	CONFIGURATION	ADMINISTRATOR/APPLIC	ATION SYSTEMOPTIONS	\rightarrow			
Application DIGIST	ATMOBILE	V Na	me	H.U.		Host Name		Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname Usernam	e		Value			
BatteryLimit	DIGISTATMOBILE			15					
DeviceLanguage	DIGISTATMOBILE			en					
EnableAlarmAudio	DIGISTATMOBILE			1					
KeepAliveInterval	DIGISTATMOBILE			15000					
LatencyLimitMs	DIGISTATMOBILE			2000					
LogFilesPath	DIGISTATMOBILE			C:\DigistatMobile\Logs					
LogLevel	DIGISTATMOBILE				the first start				
Logo	DIGISTATMOBILE			UDa53Dde-ad95-4527-a05c-efd	d/deed8d				
MediaPath	DIGISTATMOBILE			C:\DigistatMobile/Media					
MuDationtMode	DIGISTATMOBILE			2					
PaconnactSchadulaMe	DIGISTATMOBILE			10000					
Signall imt	DIGISTATMOBILE			40					
TempPath	DIGISTATMOBILE			C:\DigistatMobile\Temp					
TimeSyncTresholdMs	DIGISTATMOBILE			120000					
Title	DIGISTATMOBILE			Digistat Mobile					
Surters Onlines				-					
System Options									
Name	Enable Alarm Audio				 Host Name 				This
Application	DIGISTATMOBILE				Туре	enum OptionTypeEnum	Bool		~
HU	[]	liear		-		
H.U.									
Description	If true, audio and vibr notification is displaye	ation are enable id, without audio	d when a new alarm no o and vibration.	fication is displayed. Otherwise only	the Value	True O False	e		
					Fig 80				

Use the checkbox indicated in Fig 80 A to edit the EnableAlarmAudio system option.

8.4.8 KeepAliveInterval configuration

The KeepAliveInterval system option makes it possible to customize the time interval between two "keep alive" messages. The "keep alive" message is requested to verify that the client is "connected" to the server. The allowed values are expressed in milliseconds (Ms) as integers between 100 and 20000. Its default value is 15000.

Main Actions A	pplications Abo	out SYSTEN	4 CONFIGURA	TION	> administr	rator/a	PPLICATIC	N SYSTEMOP	TIONS	>						
Application DIGIST	ATMOBILE	✓ Nar	me			H.U.				Host	Name			Apply Filter	Clear Fi	ter
Name	Application	Hospital Unit	Hostname Us	sername							Value					
BatteryLimit	DIGISTATMOBILE			1	15											
DeviceLanguage	DIGISTATMOBILE				en											
EnableAlarmAudio	DIGISTATMOBILE			1	1											
KeepAliveInterval	DIGISTATMOBILE			1	15000											
LatencyLimitMs	DIGISTATMOBILE			2	2000											
LogFilesPath	DIGISTATMOBILE			(C:\DigistatMobi	le\Logs										
LogLevel	DIGISTATMOBILE			(0											
Logo	DIGISTATMOBILE			0	0ba53bde-ad95	-4527-a05	ic-efd5d7dee	d8d								
MediaPath	DIGISTATMOBILE			0	C:\DigistatMob	ile\Media										
MyPatient	DIGISTATMOBILE			1	1											
MyPatientMode	DIGISTATMOBILE			3	3											
ReconnectScheduleMs	DIGISTATMOBILE			1	10000											
SignalLimit	DIGISTATMOBILE			4	40											
TempPath	DIGISTATMOBILE			0	C:\DigistatMob	ile\Temp										
TimeSyncTresholdMs	DIGISTATMOBILE			1	120000											
Title	DIGISTATMOBILE			0	Digistat Mobile											
System Options																
Name	KeepAliveInterval						V	Host	Name							This
Application	DIGISTATMOBILE								Туре	_enum_Option	nTypeEn	um_Integer				v
H.U.								\frown	User							
Description	Interval between two	keep alive mes	sages.					A	Value	15000			100 - 20	1000		
								Fig	81							

To edit the KeepAliveInterval system option enter the wanted value in the text field indicated in Fig 81 **A**.

8.4.9 LatencyLimitMs configuration

The LatencyLimitMs system option makes it possible to set a threshold value for the speed of the network to which the handheld device is connected. If the network speed is lower than this value, a notification of "Slow Network" is provided. The allowed values are expressed in milliseconds (Ms) as integers between 100 and 20000. Its default value is 2000.

Application SMARTC	ENTRALMOBILE V	Name		H.U Host Name Apply Filter Clear Fi
Name	Application	Hospital Unit	Hostname Username	ne Value
BatteryLimit	SMARTCENTRALMOBILE			15
DeviceFormatString	SMARTCENTRALMOBILE			<formatstrings></formatstrings>
EnableAlarmAudio	SMARTCENTRALMOBILE			1
GridColumnCount	SMARTCENTRALMOBILE			3
Language	SMARTCENTRALMOBILE			SV .
LatencyLimitMs	SMARTCENTRALMOBILE			2000
Locale	SMARTCENTRALMOBILE			
MyPatientsEnabled	SMARTCENTRALMOBILE			0
OnlineParametersTimed	ut SMARTCENTRALMOBILE			30
Orientation	SMARTCENTRALMOBILE			2
PatientFormatString	SMARTCENTRALMOBILE			MRN:{4} Born on {1} ({2}) Sex:{3}
PingScheduleMs	SMARTCENTRALMOBILE			15000
ReconnectScheduleMs	SMARTCENTRALMOBILE			10000
ShowLocationName	SMARTCENTRALMOBILE			0
SignalLimit	SMARTCENTRALMOBILE			40
SoundRepetition	SMARTCENTRALMOBILE			2
System Options				
Name L	atencyLimitMs			V Host Name
Application S	MARTCENTRALMOBILE			Typeenum_OptionTypeEnum_Integer
ни				
Description B	elow this value a slow network	c notification is i	aseq	

Fig 82

To edit the LatencyLimitMs system option enter the wanted value in the text field indicated in Fig 82 **A**.

8.4.10 LogFilesPath configuration

The LogFilesPath system option makes it possible to specify the path of the folder in which the log files coming from the connected clients will be saved. If a non-existing path is specified, the server creates it. The default value is: C:\DigistatMobile\Logs.

Main Actions A	pplications Abo	ut SYSTEN	I CONFIGU	IRATION		IN SYSTEMOPTIONS	>		
Application DIGIST	ATMOBILE	V Nar	ne		H.U.		Host Name	Apply Filt	er Clear Filter
Name	Application	Hospital Unit	Hostname	Username			Value	e	
BatteryLimit	DIGISTATMOBILE				15				
DeviceLanguage	DIGISTATMOBILE				en				
EnableAlarmAudio	DIGISTATMOBILE				1				
KeepAliveInterval	DIGISTATMOBILE				15000				
LatencyLimitMs	DIGISTATMOBILE				2000				
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs				
LogLevel	DIGISTATMOBILE				0				
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7dee	d8d			
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media				
MyPatient	DIGISTATMOBILE				1				
MyPatientMode	DIGISTATMOBILE				3				
ReconnectScheduleMs	DIGISTATMOBILE				10000				
SignalLimit	DIGISTATMOBILE				40				
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp				
TimeSyncTresholdMs	DIGISTATMOBILE				120000				
Title	DIGISTATMOBILE				Digistat Mobile				
Sustem Ontions									
System Options									
Name	LogFilesPath				~ ~	Host Name			This
Application	DIGISTATMOBILE					Type	enum OntionTypeEn	um Path	~
H.U.						User			
Description	Path for log files					A	C:\DigistatMobile\Logi	2	×

Fig 83

The path can be typed in the text field indicated in Fig 83 **A**.

8.4.11 LogLevel configuration

The LogLevel system option makes it possible to define the kind of information logged. The following values are possible: NONE = 0 (default value - no information is logged); INTERNAL = 1 (only internal information); VERBOSE = 2 (same kind of information as 1, but more detailed); DEBUG = 3 (debug information is logged); INFO = 4 (information logs); WARN = 5 (warning logs); ERROR = 6 (error logs). The higher is the value specified, the more detailed is the log file (i.e. for example, if 3 is specified, then information of level 1-2-3 is logged.

Main Actions A	Applications Abo	out	M CONFIGURATIO		tor/app	LICATION S	YSTEMOP	TIONS	>						
Application DIGIST.	ATMOBILE	✓ Na	ime		H.U. [н	lost Name			Apply Filter		Clear Filter
Name	Application	Hospital Unit	Hostname Userna	ne						Valu	e				
BatteryLimit	DIGISTATMOBILE			15											
DeviceLanguage	DIGISTATMOBILE			en											
EnableAlarmAudio	DIGISTATMOBILE			1											
KeepAliveInterval	DIGISTATMOBILE			15000											
LatencyLimitMs	DIGISTATMOBILE			2000											
LogFilesPath	DIGISTATMOBILE			C:\DigistatMobile\L	.ogs										
LogLevel															
Logo	DIGISTATMOBILE			0ba53bde-ad95-45	527-a05c-	efd5d7deed8d									
MediaPath	DIGISTATMOBILE			C:\DigistatMobile\	Media										
MyPatient	DIGISTATMOBILE			1											
MyPatientMode	DIGISTATMOBILE			3											
ReconnectScheduleMs	DIGISTATMOBILE			10000											
SignalLimit	DIGISTATMOBILE			40											
TempPath	DIGISTATMOBILE			C:\DigistatMobile\	Temp										
TimeSyncTresholdMs	DIGISTATMOBILE			120000											
Title	DIGISTATMOBILE			Digistat Mobile											
System Options															
Name	LogLevel					~	Host	Name						_	This
Application	DIGISTATMOBILE							Type _e	enum_Op	ptionTypeEr	num_Integer				~
H.U.						/		User							
Description	Clients log level: NON = 6	VE = 0;INTERN	IAL = 1;VERBOSE = 2	DEBUG = 3;INFO = 4;W	VARN = 5	ERROR		Value 0				0 - 6			
							Fig 8	34							

Use the field indicated in Fig 84 **A** to set the LogLevel system option.

8.4.12 Logo configuration

The Logo system option makes it possible to set which logo will be displayed on the handheld devices at application start-up.

Application DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE	Hospital Unit	Hostname	Username	15 en 1 15000 2000 C:\DigistatMobile\Logs 0 0ba53bde=ad95=4527=a C:\DigistatMobile\Media 1	n05c-efd5d7deed8d a	Val	lê		
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				15 en 1 15000 2000 C:\DigistatMobile\Logs 0 0b35bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				en 1 15000 2000 C:\DigistatMobile\Logs 0 0ba53bde:ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				1 15000 2000 C:\DigistatMobile\Logs 0 0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				15000 2000 C:\DigistatMobile\Logs 0 0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	105c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				2000 C:\DigistatMobile\Logs 0 0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a	1	_		
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				C:\DigistatMobile\Logs 0 0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				0 0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				0ba53bde-ad95-4527-a C:\DigistatMobile\Media 1	a05c-efd5d7deed8d a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				C:\DigistatMobile\Media 1	a				
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE				1					
DIGISTATMOBILE DIGISTATMOBILE DIGISTATMOBILE									
DIGISTATMOBILE DIGISTATMOBILE				3					
DIGISTATMOBILE				10000					
				40					
DIGISTATMOBILE				C:\DigistatMobile\Temp	p				
DIGISTATMOBILE				120000					
DIGISTATMOBILE				Digistat Mobile					
Logo				~	Host Name				This
DIGISTATMOBILE					Туре	_enum_OptionTyp	eEnum_Bina	iry	
					User				
Logo for the main w	indow				Value				
Logo to the main w	muuw				A		iscomlogo.pr	ng	
[ogo DIGISTATMOBILE	Logo DIGISTATMOBILE	Logo DIGISTATMOBILE	Logo JIGISTATMOBILE	Logo VIGISTATMOBILE	Alogo Velos	Host Name	Logo Vote Host Name Vote Lenum_OptionTypeEnum_Bina User Association ascomlogo.p	Logo Visit Name Visit

If a logo is already set, the file name is displayed on the button indicated in Fig 85 **A**. To set the logo,

click the button.

The following window opens (Fig 86). The window lists the names of the files that can be selected as logo (Fig 86 **A**).

			_	FIL	e selec	TION		
	Application						✓ Apply Filter	Clear Filter
\sim	Filename	Туре	Applicat	ion	Size		Last Update	
	ascomlogo.png	IMAGE	×	12 KB		22/11/2017 07:57:25		
							B	
	NEW	DELETE	VIEW	DOWNLO	AD	IONE	ОК	CANCEL
					Fi	g 86		

If the wanted file is already present on the window, click the corresponding row. The row is this way highlighted. Then click the **Ok** button (Fig 86 **B**). The file is this way set as logo.

If the wanted file is not present on the window, click the **Download** button (Fig 86 **C**). A window making it possible to browse the workstation/network contents is displayed. Locate and select the relevant file. The file name will be listed in the "File Selection" window.

8.4.13 MyPatient configuration

The MyPatientEnabled system option makes it possible to either enable or disable the "My Patients" functionality. If true, then the "My Patients" functionality is enabled; if false, then the "My Patients" functionality is disabled. The default value is true.

Application DIGIS	TATMOBILE 🗸	Name			H.U Host Name Apply Fiter Clear Fiter
Name	Application	Hospital Unit	Hostname	Username	Value
BatteryLimit	DIGISTATMOBILE				15
DeviceLanguage	DIGISTATMOBILE				en
EnableAlarmAudio	DIGISTATMOBILE				1
KeepAliveInterval	DIGISTATMOBILE				15000
LatencyLimitMs	DIGISTATMOBILE				2000
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs
LogLevel	DIGISTATMOBILE				0
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7deed8d
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media
MyPatient	DIGISTATMOBILE				1
MyPatientMode	DIGISTATMOBILE				3
ReconnectScheduleMs	DIGISTATMOBILE				10000
SignalLimit	DIGISTATMOBILE				40
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp
TimeSyncTresholdMs	DIGISTATMOBILE				120000
Title	DIGISTATMOBILE				Digistat Mobile
System Options					
Name	MyPatient				V Host Name This
Application	DIGISTATMOBILE				Type _enum_OptionTypeEnum_Bool
H.U.					User
	Enable/disable Mu	Patient			
Description					C The C Palse

Fig 87

Use the checkbox indicated in Fig 87 A to enable/disable the "My Patients" functionality.

8.4.14 MyPatientMode configuration

The MyPatientMode system option makes it possible to define the sub-sets of patients displayed when in "My Patients" mode.

Application DIGIST		Namo			Hill Host Name Apply Efter Close Efter
Application Didis	ATMODILE +				n.o. Appy riter Clear riter
Name	Application	Hospital Unit	Hostname	Username	e Value
BatteryLimit	DIGISTATMOBILE				15
DeviceLanguage	DIGISTATMOBILE				en
EnableAlarmAudio	DIGISTATMOBILE				1
KeepAliveInterval	DIGISTATMOBILE				15000
LatencyLimitMs	DIGISTATMOBILE				2000
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs
LogLevel	DIGISTATMOBILE				0
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7deed8d
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media
MyPatient	DIGISTATMOBILE				1
MyPatientMode	DIGISTATMOBILE				
ReconnectScheduleMs	DIGISTATMOBILE				10000
SignalLimit	DIGISTATMOBILE				40
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp
TimeSyncTresholdMs	DIGISTATMOBILE				120000
Title	DIGISTATMOBILE				Digistat Mobile
System Options					
-,					
Name	MyPatientMode				Host Name The second
Application	DIGISTATMOBILE				Type _enum_OptionTypeEnum_Integer
H.U.					User User
Description	0=Only mine, 1=mir not assigned and n	ie and not assig iot connected	ned, 2=mine	and not con	onnected.3+mine and Value 3 0 - 3

The following values are possible:

- 0=Only mine: when in "My Patients" mode only the patients selected as "My Patients" are displayed.
- 1=Mine and not assigned: the patients selected as "My Patients" and the patients not selected as "My Patients" by any user are displayed.
- 2=Mine and not connected: the patients selected as "My Patients" and the patients selected as "My Patients" by other users that are off-line at the moment (due, for instance, to network unavailability) are displayed.
- 3=Mine and not assigned and not connected: all the patients sub-sets mentioned above are displayed (default value).

To edit this system option enter the wanted value in the field indicated in Fig 88 A.

8.4.15 ReconnectScheduleMs configuration

The ReconnectScheduleMs system option makes it possible to set the time interval between two consecutive connection attempts after client (tutti o solo handheld?) disconnection from server. The values are expressed in milliseconds (Ms) as integers between 1000 and 20000. Its default value is 10000.

Main Actions A HOME > GENERAL	Applications Ab	out	A CONFIGUE	RATION	> ADMINISTRATOR/APPLICATION SYSTEMOPTIONS >
Application DIGIST	ATMOBILE V	Name			H.U Host Name Apply Filter Clear Filter
Name	Application	Hospital Unit	Hostname	Username	e Value
BatteryLimit	DIGISTATMOBILE				15
DeviceLanguage	DIGISTATMOBILE				en
EnableAlarmAudio	DIGISTATMOBILE				1
KeepAliveInterval	DIGISTATMOBILE				15000
LatencyLimitMs	DIGISTATMOBILE				2000
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs
LogLevel	DIGISTATMOBILE				0
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7deed8d
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media
MyPatient	DIGISTATMOBILE				1
MyPatientMode	DIGISTATMOBILE				3
ReconnectScheduleMs	DIGISTATMOBILE				10000
SignalLimit	DIGISTATMOBILE				40
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp
TimeSyncTresholdMs	DIGISTATMOBILE				120000
Title	DIGISTATMOBILE				Digistat Mobile
System Options					
Name	ReconnectSchedu	leMs			Y Host Name
Hamo	1				
Application	DIGISTATMOBILE				Type _enum_OptionTypeEnum_Integer V
H.U.					User
Description	Interval between tw	o retries if smar	rtcentral is disc	onnected.	1. Nalue 10000 1000 - 20000

Fig 89

To edit ReconnectScheduleMs system option enter the wanted value in the field indicated in Fig 89 **A**.

8.4.16 SignalLimit configuration

The SignalLimit system option makes it possible to set a lower threshold value for the signal strength of the Wireless network. When the signal strength is lower than the specified value, a notification is provided. Values are expressed as percentage (therefore integers between 1 and 100). Default value is 40.

Main Actions A	applications Ab	out			
HOME > GENERAL	CONFIGURATOR	R > SYSTEM	1 CONFIGL	JRATION	ADMINISTRATOR/APPLICATION SYSTEMOPTIONS
Application DIGIST	ATMOBILE V	Name			H.U Host Name Apply Fiter Clear Fiter
Name	Application	Hospital Unit	Hostname	Username	Value
BatteryLimit	DIGISTATMOBILE				15
DeviceLanguage	DIGISTATMOBILE				en
EnableAlarmAudio	DIGISTATMOBILE				1
KeepAliveInterval	DIGISTATMOBILE				15000
LatencyLimitMs	DIGISTATMOBILE				2000
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs
LogLevel	DIGISTATMOBILE				0
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7deed8d
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media
MyPatient	DIGISTATMOBILE				1
MyPatientMode	DIGISTATMOBILE				3
ReconnectScheduleMs	DIGISTATMOBILE				10000
SignalLimit	DIGISTATMOBILE				40
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp
TimeSyncTresholdMs	DIGISTATMOBILE				120000
Title	DIGISTATMOBILE				Digistat Mobile
System Options					
News	Signall imit				V Heat Name
Name	orginalization				
Application	DIGISTATMOBILE				Type _enum_OptionTypeEnum_Integer ~
H.U.					User
Description	In percentage. Wifi	signal strenght	Below this v	alue a notific	cation is raised. 0 - 100

Fig 90

To edit the SignalLimit system option enter the wanted value in the field indicated in Fig 90 **A**).

8.4.17 TempPath configuration

The TempPath system option makes it possible to specify the folder in which the files to be uploaded to the handheld devices are temporarily stored. If a non-existing path is selected, it is automatically created. The default value is: *C:\DigistatMobile\Temp*.

Main Actions A $HOME$	opplications Ab	oout R > SYSTEM	4 CONFIGL	JRATION		R/APPLICATION SY	STEMOPTIONS >		
Application DIGIST	ATMOBILE 🗸	Name			H.U.	Ho	st Name	Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname	Username			Value		
BatteryLimit	DIGISTATMOBILE				15				
DeviceLanguage	DIGISTATMOBILE				en				
EnableAlarmAudio	DIGISTATMOBILE				1				
KeepAliveInterval	DIGISTATMOBILE				15000				
LatencyLimitMs	DIGISTATMOBILE				2000				
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs				
LogLevel	DIGISTATMOBILE				0				
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a	a05c-efd5d7deed8d			
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Medi	a			
MyPatient	DIGISTATMOBILE				1				
MyPatientMode	DIGISTATMOBILE				3				
ReconnectScheduleMs	DIGISTATMOBILE				10000				
SignalLimit	DIGISTATMOBILE				40				
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Tem	р			
TimeSyncTresholdMs	DIGISTATMOBILE				120000				
Title	DIGISTATMOBILE				Digistat Mobile				
System Options									
Name	TempPath				~	Host Name			This
Application	DIGISTATMOBILE					Туре	_enum_OptionTypeEnum_Path		~
H.U.						User			
Description	Path for temp uploa	ad folder				Value	C:\DigistatMobile\Temp		
Description						A	e le geodene (, enp		~

Fig 91

To edit the TempPath system option enter the wanted path in the field indicated in Fig 91 A.

8.4.18 TimeSyncTresholdMs configuration

The TimeSyncTresholdMs system option makes it possible to set a higher threshold value for the difference in time synchronization between client and server. If the time difference is higher than the specified value, a notification is provided. Values are expressed in milliseconds (Ms) as integers between 1000 and 300000. Default value is 120000.

Main Actions A HOME > GENERAL	Applications Ab	out	1 CONFIGI	JRATION	> ADMINISTRATOR/APPLICATION SYSTEMOPTIONS >
Application DIGIST	ATMOBILE V	Name			HU Host Name Apply Fitter Clear Fitter
Name	Application	Hospital Unit	Hostname	Username	Value
BatteryLimit	DIGISTATMOBILE				15
DeviceLanguage	DIGISTATMOBILE				en
EnableAlarmAudio	DIGISTATMOBILE				1
KeepAliveInterval	DIGISTATMOBILE				15000
LatencyLimitMs	DIGISTATMOBILE				2000
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs
LogLevel	DIGISTATMOBILE				0
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a05c-efd5d7deed8d
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Media
MyPatient	DIGISTATMOBILE				1
MyPatientMode	DIGISTATMOBILE				3
ReconnectScheduleMs	DIGISTATMOBILE				10000
SignalLimit	DIGISTATMOBILE				40
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Temp
TimeSyncTresholdMs	DIGISTATMOBILE				120000
Title	DIGISTATMOBILE				Digistat Mobile
System Options					
Name	TimeSyncTreshold	dMs			V Host Name This
Application	DIGISTATMOBILE				Type _enum_OptionTypeEnum_Integer V
H.U.					User
Description					Value 120000 1000 - 300000

Fig 92

To set the TimeSyncTresholdMs system option enter the wanted value in the text field indicated in Fig 92 A.

8.4.19 Title configuration

The Title system option makes it possible to specify the application title that is displayed on the handheld device. The default value is "Digistat Mobile".

Main Actions A	pplications Ab	out								
home > general	CONFIGURATOR	SYSTEM	1 CONFIGL	IRATION	ADMINISTRATO	R/APPLICATION S	STEMOPTIONS	>		
Application DIGIST	ATMOBILE 🗸	Name			H.U.	н	ost Name	[Apply Filter	Clear Filter
Name	Application	Hospital Unit	Hostname	Username			Value			
BatteryLimit	DIGISTATMOBILE				15					
DeviceLanguage	DIGISTATMOBILE				en					
EnableAlarmAudio	DIGISTATMOBILE				1					
KeepAliveInterval	DIGISTATMOBILE				15000					
LatencyLimitMs	DIGISTATMOBILE				2000					
LogFilesPath	DIGISTATMOBILE				C:\DigistatMobile\Logs					
LogLevel	DIGISTATMOBILE				0					
Logo	DIGISTATMOBILE				0ba53bde-ad95-4527-a	a05c-efd5d7deed8d				
MediaPath	DIGISTATMOBILE				C:\DigistatMobile\Medi	a				
MyPatient	DIGISTATMOBILE				1					
MyPatientMode	DIGISTATMOBILE				3					
ReconnectScheduleMs	DIGISTATMOBILE				10000					
SignalLimit	DIGISTATMOBILE				40					
TempPath	DIGISTATMOBILE				C:\DigistatMobile\Tem	p				
TimeSyncTresholdMs	DIGISTATMOBILE				120000					
Title	DIGISTATMOBILE				Digistat Mobile					
System Options										
Name	Title				~	Host Name	L			This
Application	DIGISTATMOBILE					Туре	_enum_OptionTypeE	Inum_Text		~
H.U.						Use				
Description	Title in the logo win	dow				Value	Digistat Mobile			
						A				~

Fig 93

To edit the Title system option enter the wanted value in the field indicated in Fig 93 ${\ensuremath{\textbf{A}}}$

8.5 How to customize the system options for a single Smart Central Device

It is possible to customize the system options for a single mobile device. To do that:

- 1 Select the relevant System Option.
- 2 Click **Copy** on the command bar. Another system option having the same features of the first one is this way created.
- 3 Customize the system option values.
- 4 Specify the name of the mobile device to which the system option refers in the **Host Name** field (Fig 94 **A**).

NOTE: In case the "Host Name" field is empty, the configuration change applies to all the devices. If the "Host Name" is specified, the configuration change applies only to the specified workstation or mobile device.

	A		
BatteryLimit V	Host Name myco6		This
SMARTCENTRAL MOBILE	Type Float		~
	User		
In percentage. Lower limit that triggers a notification alarm of "unsafe" application. Tipical value is 15-20.	Value 90	1 - 100	
	BatteryLimit V SMARTCENTRAL MOBILE In percentage. Lower limit that triggers a notification alarm of "unsafe" application. Tipical value is 15-20.	BatheyLimit SMARTCENTRAL MOBILE SMARTCENTRAL MOBILE In percentage. Lower limit that triggers a notification alarm of "unsafe" application. Tpical value is 15:20.	BatteyLimt SMARTCENTRAL MOBILE IN percentage. Lower limit the triggers a notification alem of "unsafe" application. Tpical value is 15:20. Host Name myco6 User Value 90 1 - 100

Fig 94

8.6 Smart Central Mobile Monitor

This section displays the status of the DAS logical network (selecting the wanted DAS instance in the top part of the screen), monitoring, for each Smart Central Mobile applications, all the instances that are currently present, displaying the relative details for each one as: **Status**, **Name**, **Address** and **Last Connection**.

NOTE:	The information displayed on screen are not auto-
	refreshed. Therefore, you need to press "Get Status"
	button placed on the top right corner of the screen.

9. Network Configuration

For each mobile devices in use in the Smart Central Mobile network, a specific domain shall be configured. The term "Domain" refers to the actual beds covered by that specific device.

To do that:

- 1 Browse Home > Connect Configurator > System Configuration > Application System Options
- 2 Click **Network Configuration** to access the area making it possible to define the domain of the device

	ame							Location					··· Apply Filter	Cle
Host	ame 🔺	Туре	Location	Bed L	Lock bed	Enabled	Modules							
1993	AND A DOWNLOW DOWN	Central station												
9.4		Mobile	ICU			-	ALL							
10	NAME OF COLUMN	Central station	ICU			-	ALL							
100	CHICK STOCK	Central station				-								
196.0	42.40	Central station				-	ALL							
UNIT	12	Central station	ICU			-	ALL							
-	and the second	Central station				-	ALL							
1	1	Mobile	ICU			-	ALL							
-		Mobile	ICU			-	ALL							
		Mobile	ICU			~	ALL							
-		Mobile	ICU			-	ALL							
-		Mobile	ICU			~	ALL							
-		Mobile	ICU			~	ALL							
-		Mobile	ICU			~	ALL							
1		Mobile	ICU			~	ALL							
	078675	Central station	ICU			•	ALL							
80	AND THE	Central station	ICU			•	ALL							
-	CARD AND	Central station	ICU		Ц	•	INFUSIONNET							
inen	OfKS) Linked System Op	tions												
Host	name myco2											Select location an	nd beds:	
Туре	MOBILE										¥	Location	Bed	
Enab	ed 🗹									Lock bed			1	
Mod	les ALL												2	
													3	
												ICU	4	
													5	
													6	
													/	
	station Label Myco 2 · W	FI										Default Location:	ICU	
Work				_	_	_			-					_

The upper area (Fig 95 **A**) lists the existing mobile devices. Click one item to display, in the lower area (Fig 95 **B**), the device features.

For each device the following features are specified:

- Hostname or Device Serial Number (if Myco)
- **Type** (the relevant devices here are those labeled as "MOBILE")
- Enabled/ Not enabled
- Modules
- Workstation label the label specified here is displayed as "Device name" on top of the "Central" screen of the application
- Beds and locations forming the device domain
- 3 Click the **New** button on the command bar to configure a new mobile device

Domain specification

1 To specify the device domain click the button indicated in Fig 95C

The following window is displayed:

	DOMAIN SELECTION						
Location	Default	Bed	Selé	ected			
		1	[
		2	[
		3	[
		4	[
TCU		5	[
100		6	[
		ISO1	[
		ISO2	[
		7	[
		8					
		OR1	[
BLO		OR2					
DLO		OR3	[
		OR4					
None]		ОК	Cancel			
ig 96							

2 Select the checkboxes corresponding to the beds that are part of the domain and click **OK**

If you select the box in the "Default" column, referring to the Location, all the beds in the location are automatically selected.

9.1 How to add a Myco

Once the device is correctly added, in order to access from to the corresponding instance of Smart Central Mobile:

1 Access to Smart Central Mobile Settings on the Myco

0 🖬 N <		u 6:46
	ADM	
0	Smartcentral Mobile 1 Alarms on 1 bed	0
	Settings Digistat Mobile Settings	•
Viewing all pati	ents	Logout
\triangleleft	0	
-ia 97		

2 Tap on Settings inside the Smart Central Mobile Menu (51A)



- i ig 50
 - 3 Prompt the login (Fig 98)

ascom	
DIGISTAT Mobile	
172.20.224.69	
52000	
TE	ST
Standalone installation	
My IP address: 10.0.2.15	Device Serial ID: d7a1d535b0eafbb5
Device ID: d7a1d535b0eafbb5	
BACK	SAVE

Fig 53

- 4 Under **Device ID** insert the name of the corresponding device previously added in the Configurator, the **Server IP address** of the relative machine and the **Server port** (Fig 53)
- 5 Tap **Test** in order to verify the connectivity, a pop-up message will confirm or negate the successful connection.

6 Tap **Save** to confirm and correctly access to the configured device

NOTE:	When the user inserts a Device ID that is not already
	present, a new device will be generated in the Network
	Configuration Menu in the Configurator. It will therefore
	necessary to assign

10. Manufacturer and Distributor Contacts

For any issue, please refer first to the Distributor who installed the Product.

Distributed in the U.S. and Canada by

Ascom US Inc. Ascom Wireless Solutions 300 Perimeter Park Drive Morrisville, NC 27560 USA

Phone: (877) 712-7266 www.ascom.us

Manufacturer contacts:

Ascom UMS s.r.l unipersonale

Via Amilcare Ponchielli 29 50018, Scandicci (Fl) Italy

Phone: (+39) 055 0512161 Fax: (+39) 055 8290392 www.ascom.it

11. Residual risks

A risk management process has been implemented in the life cycle of Digistat Smart Central adopting the relevant technical regulations. The risk control measures have been identified and implemented in order to reduce the residual risks to the minimum level and make them acceptable compared to the benefits brought in by the product. The total residual risk is also acceptable if compared to the same benefits.

The residual risks listed below have been taken into consideration and reduced to the minimum level possible. Given the inherent nature of the "risk" concept, it is not possible to completely remove them. It is therefore necessary, according to the regulations, to let the users know each and every possible risk (even though remote).

- Inability to using the system or some of its functionalities, which can cause delays and/or errors in the therapeutic/diagnostic actions.
- Slowdown of Digistat Smart Central performance, which could cause delays and/or errors in the therapeutic/diagnostic actions.
- Circulation of users' and/or patients' sensitive data.
- Wrong data insertion and display, which can cause errors in the therapeutic/diagnostic actions.
- Display of either partial or hard-to-read information, which can cause delays and/or errors in the therapeutic/diagnostic actions.
- Attribution of device data to the wrong patient (patient exchange), which can cause errors in the therapeutic/diagnostic actions.

RISKS RELATING TO THE HARDWARE PLATFORM IN USE (NOT PART OF THE PRODUCT)

- Electric shock for the patient and/or the user, which can cause injury and/or death for the patient/user.
- Hardware components overheating, that can cause injury for the patient/user.
- Infection contraction for the patient/user.