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

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
	Attention, consult accompanying documents
℞ 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)

Fig 1

The following menu is displayed (Fig 2).

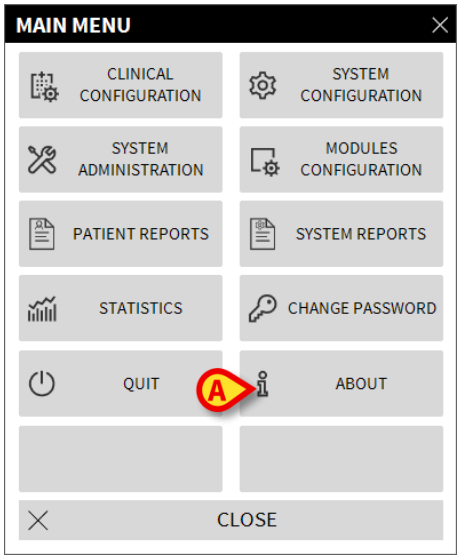


Fig 2

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

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**).

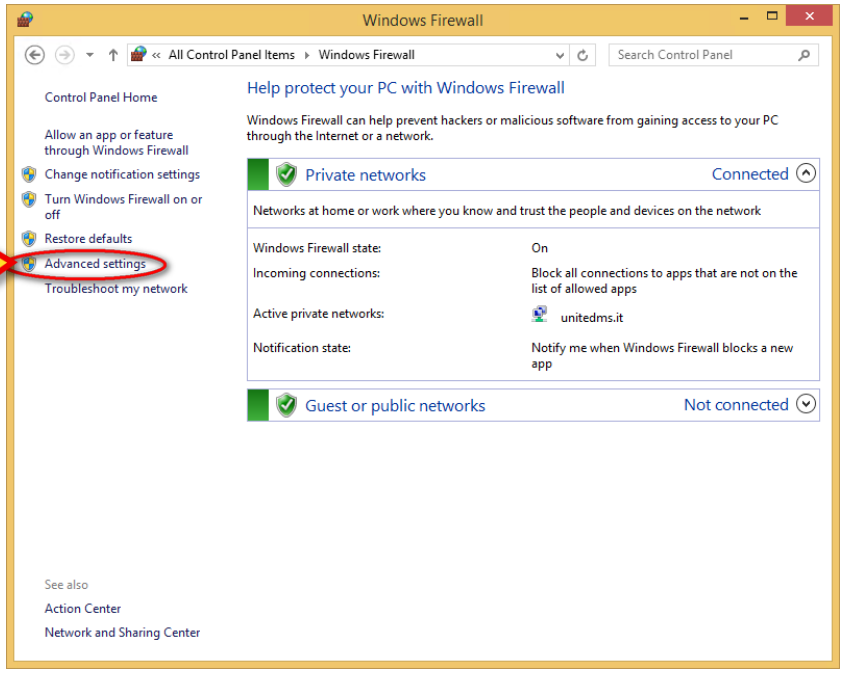


Fig 4

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

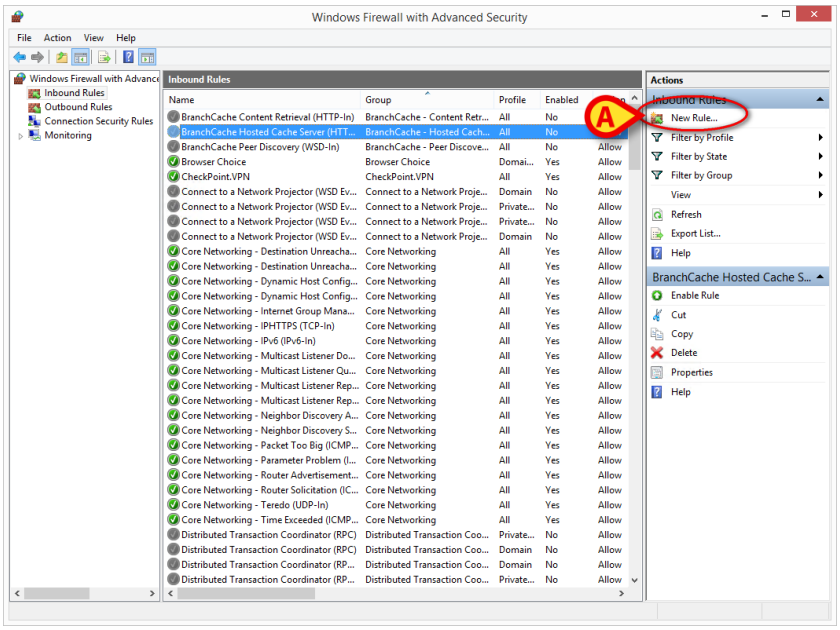


Fig 5

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

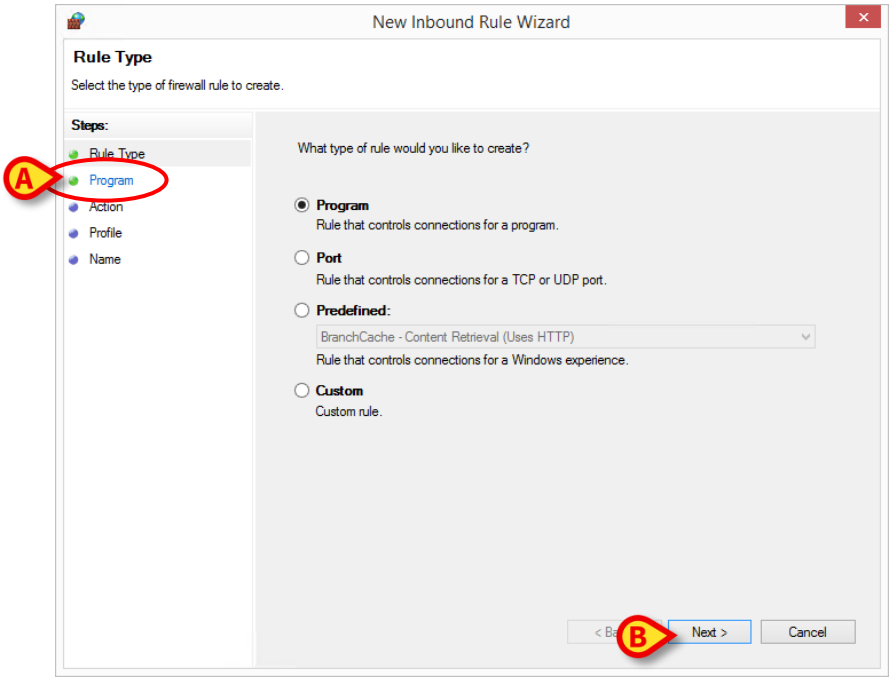


Fig 6

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

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

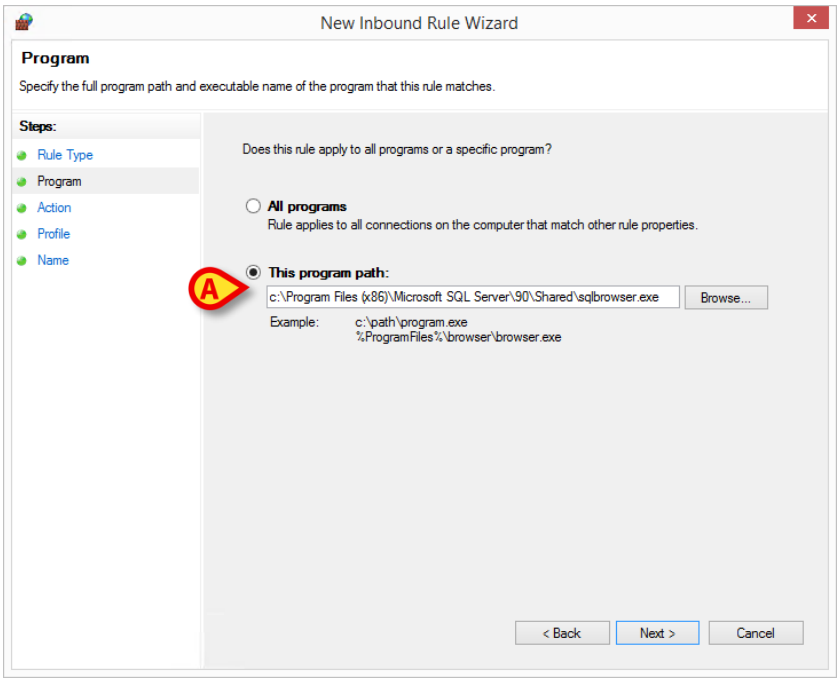


Fig 7

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

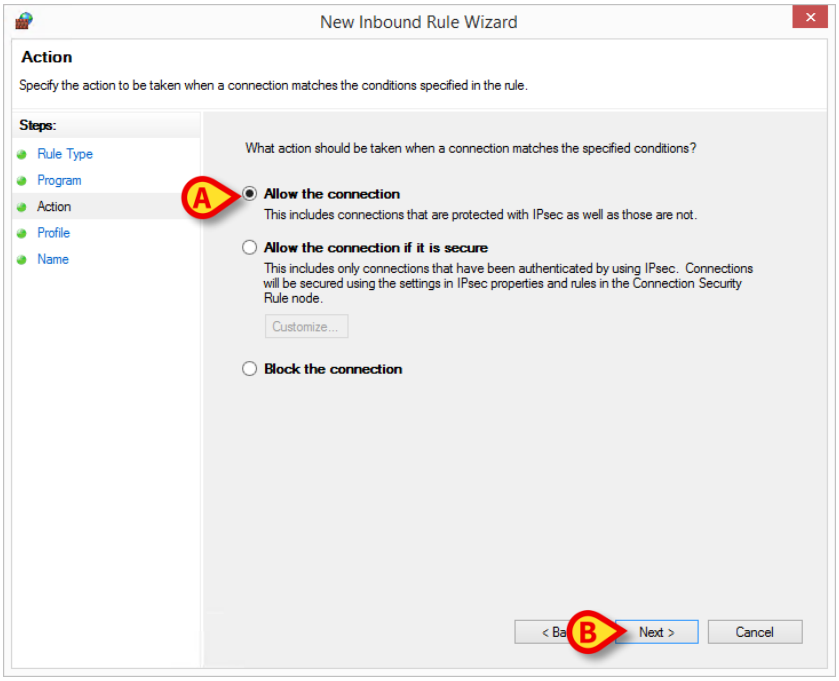


Fig 8

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

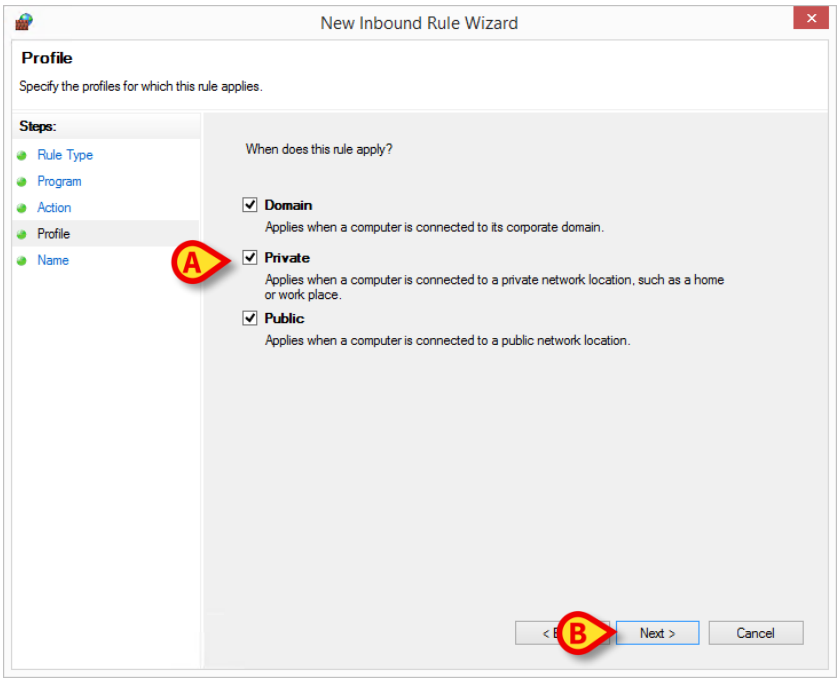


Fig 9

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 must be installed and configured only by specifically trained and authorized personnel. 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 must be installed and configured only by specifically trained and authorized personnel. 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).

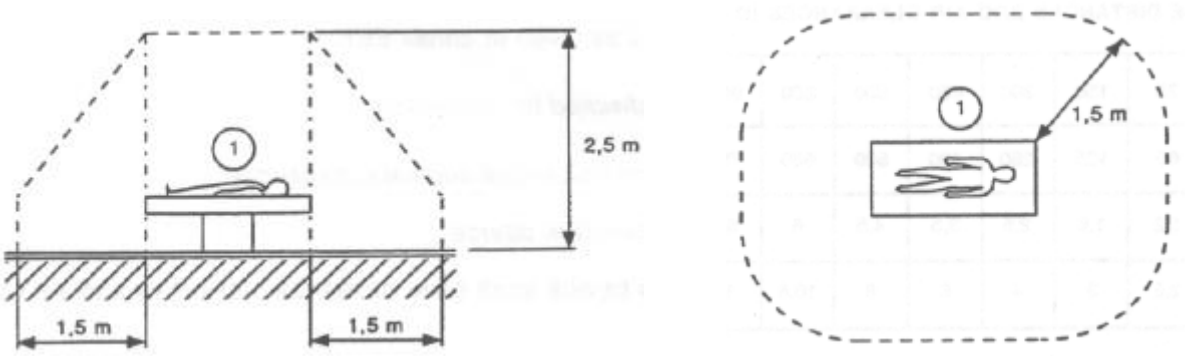


Fig 10 - Patient Area

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
18. 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.

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

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).

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)

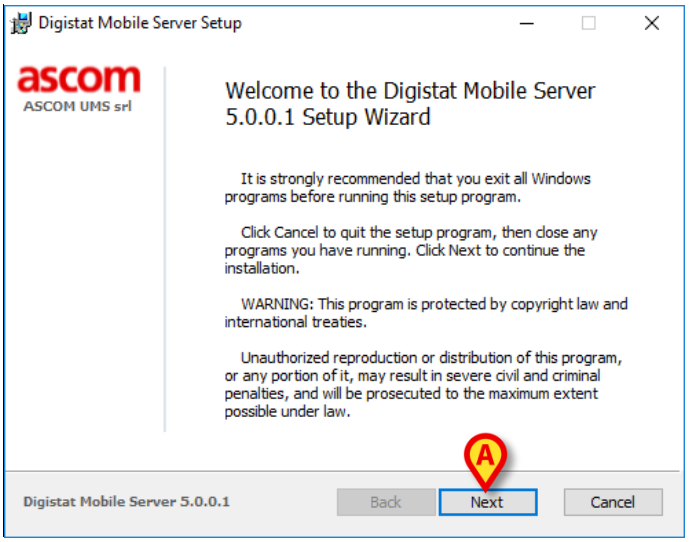


Fig 12

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

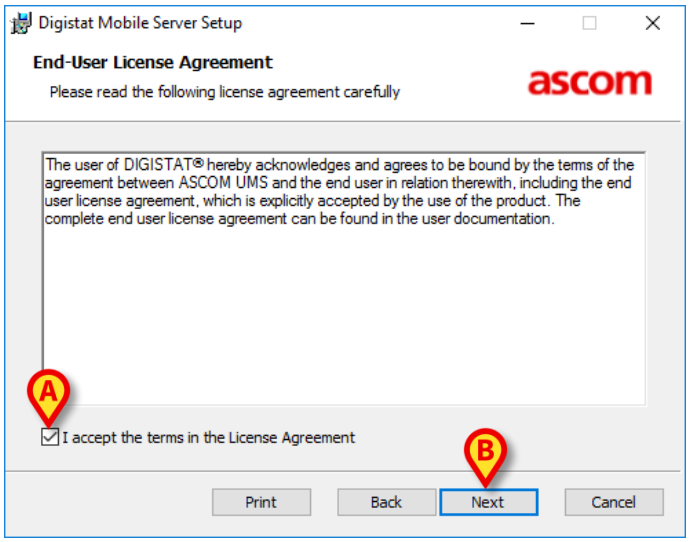


Fig 13

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).

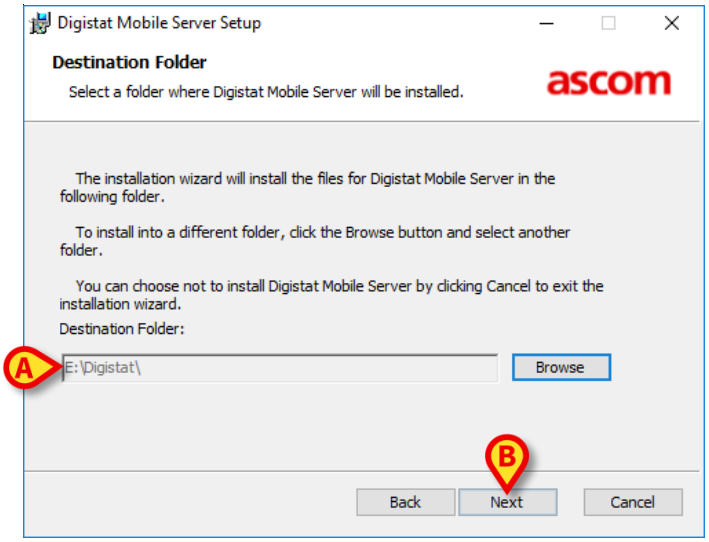
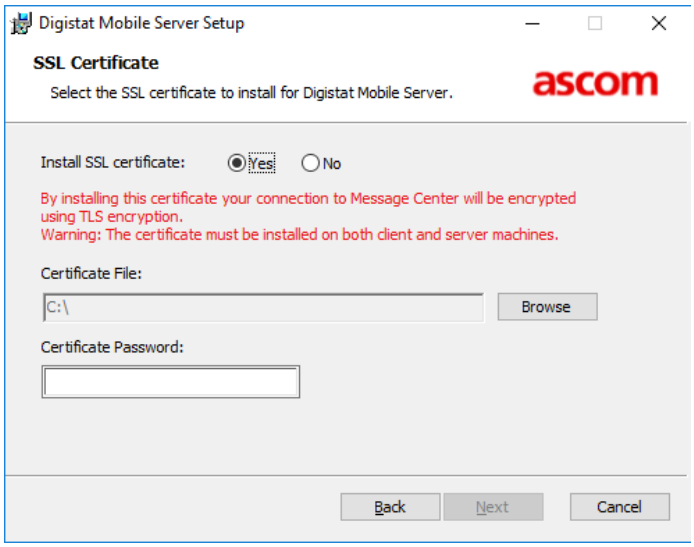


Fig 14

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.



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).

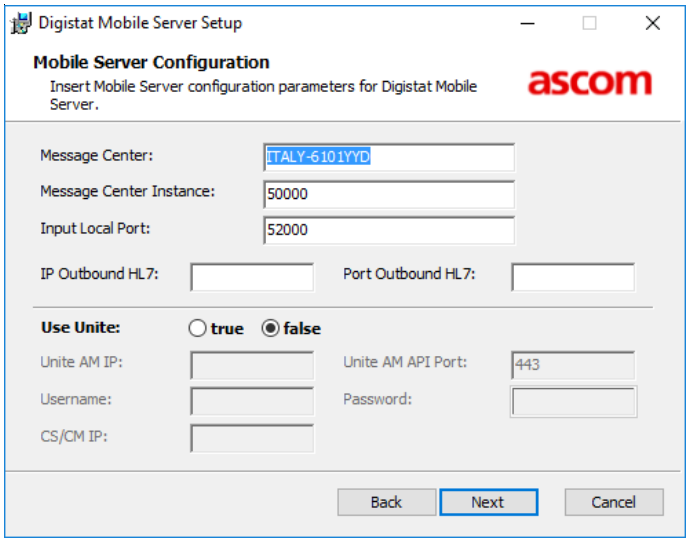


Fig 15

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)

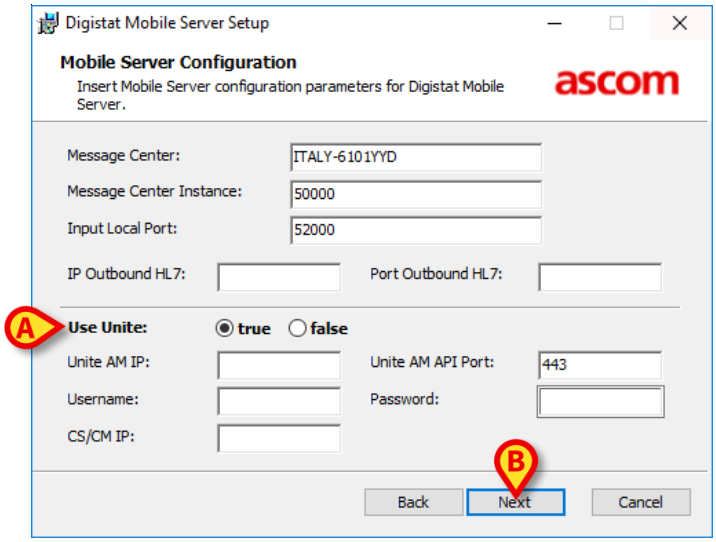


Fig 16

Click **Next** when done (Fig 16 **B**).

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

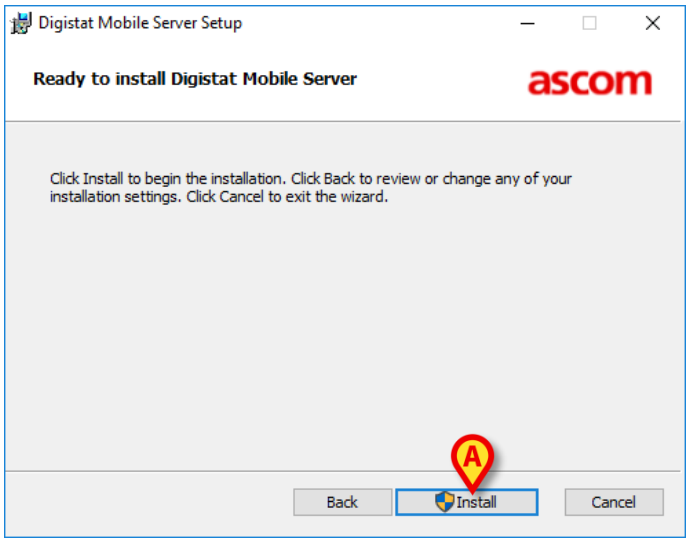


Fig 17

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)

Fig 18

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

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).

Fig 20

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

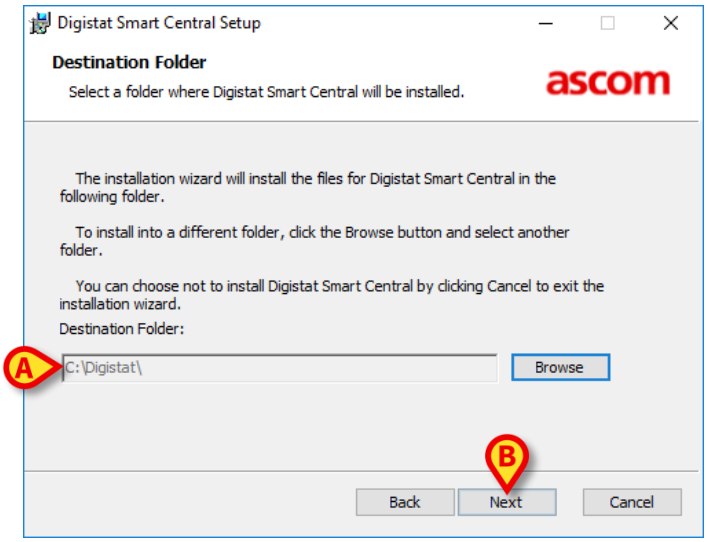
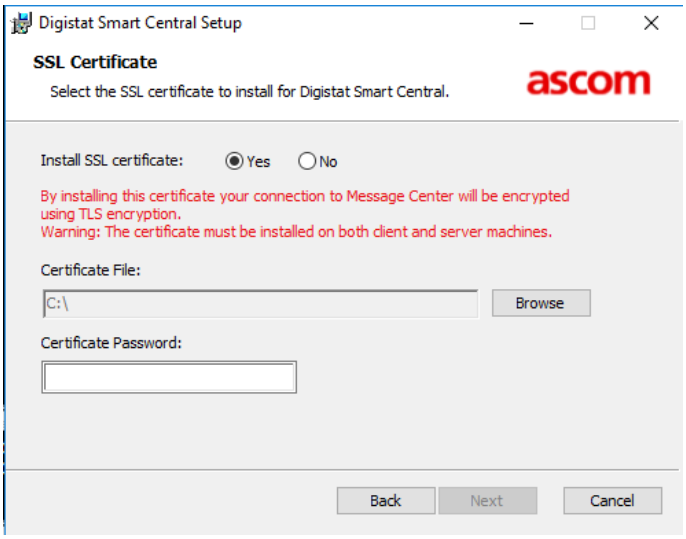


Fig 21

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.



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

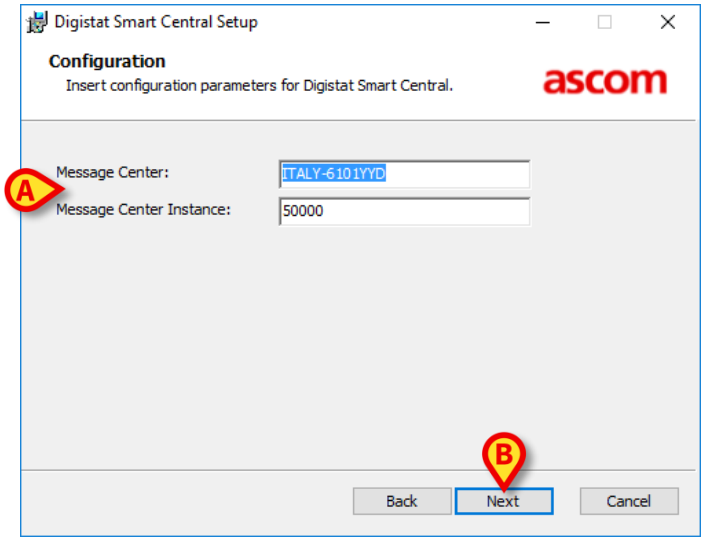


Fig 22

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).

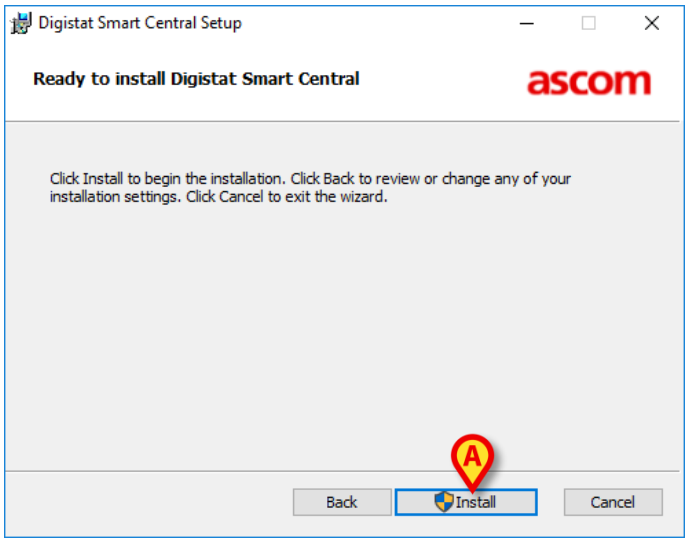


Fig 23

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.

Fig 24

The following screen opens (Fig 25).

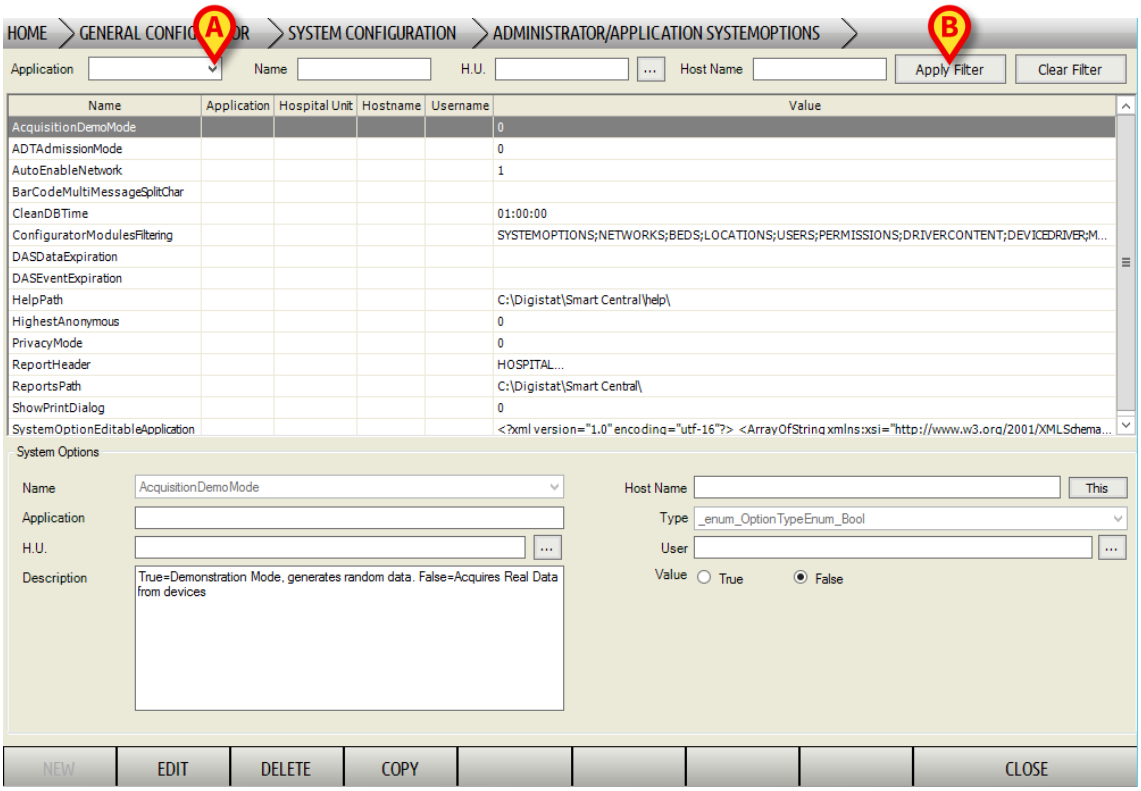


Fig 25

1 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**)

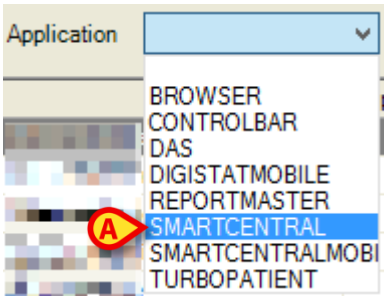


Fig 26

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

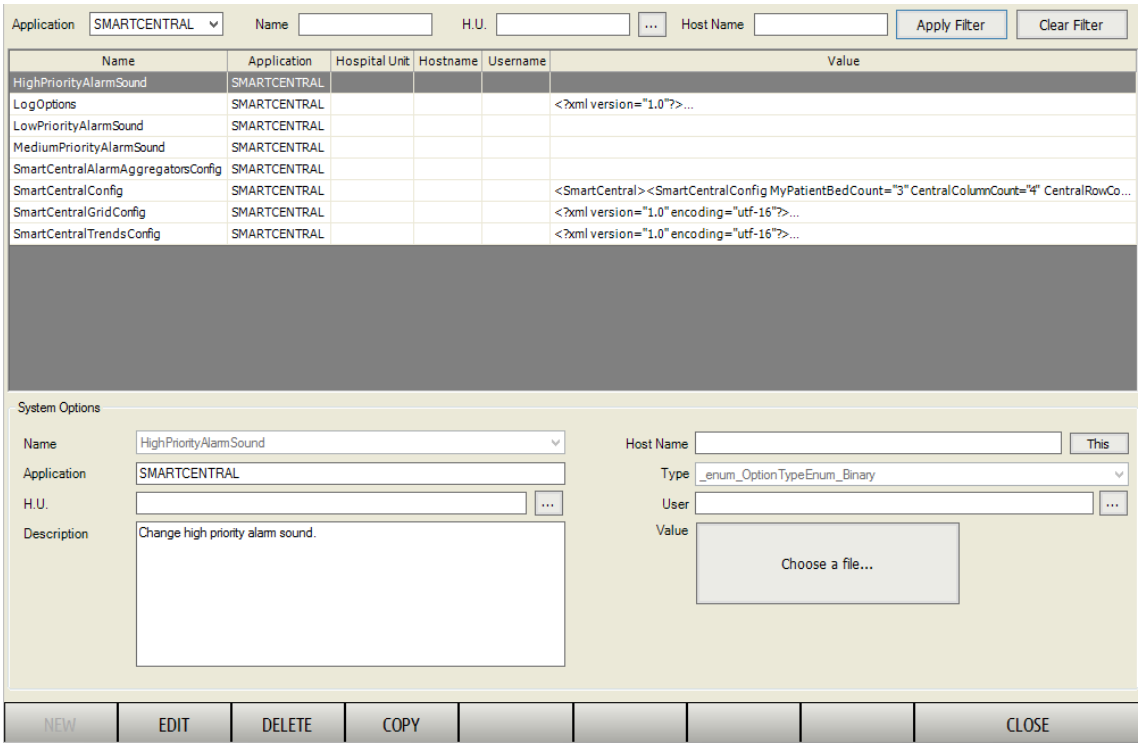


Fig 27

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**).

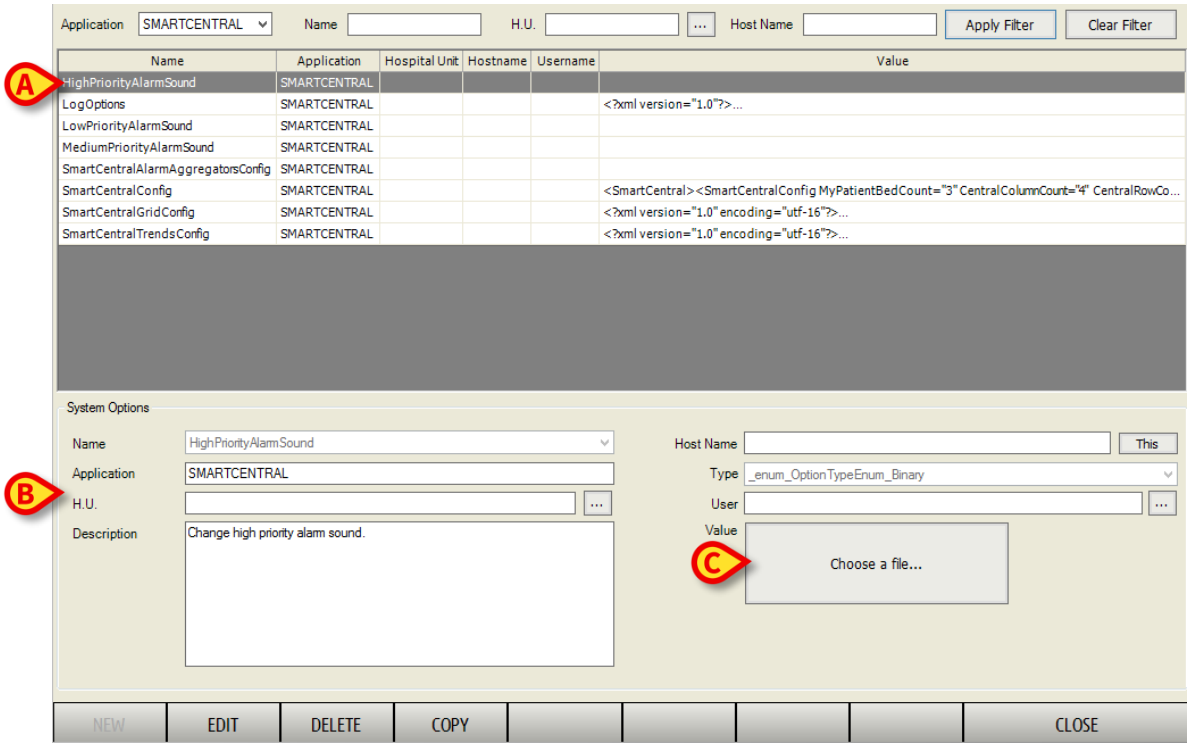


Fig 28

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

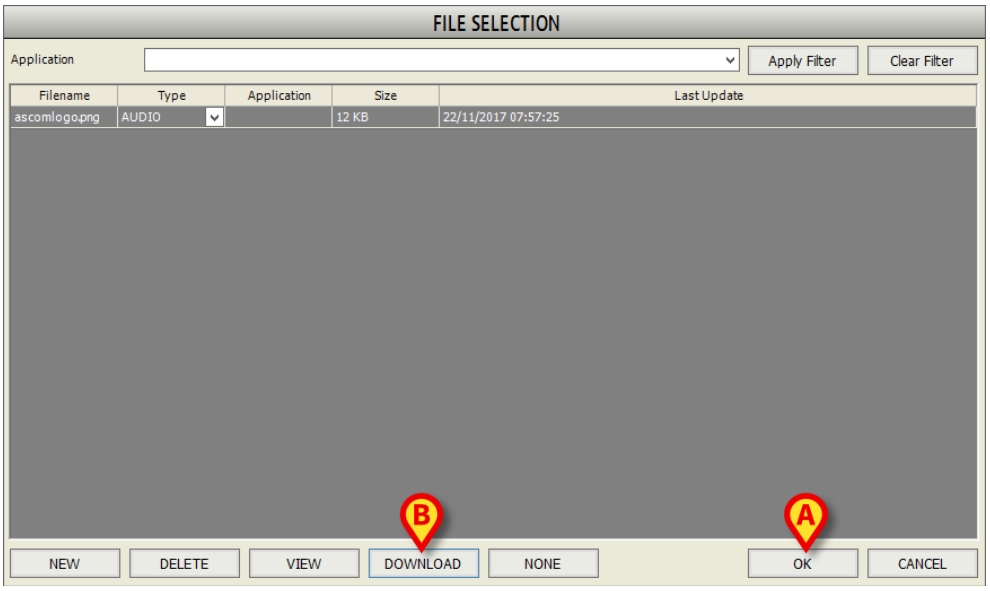


Fig 29

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**).

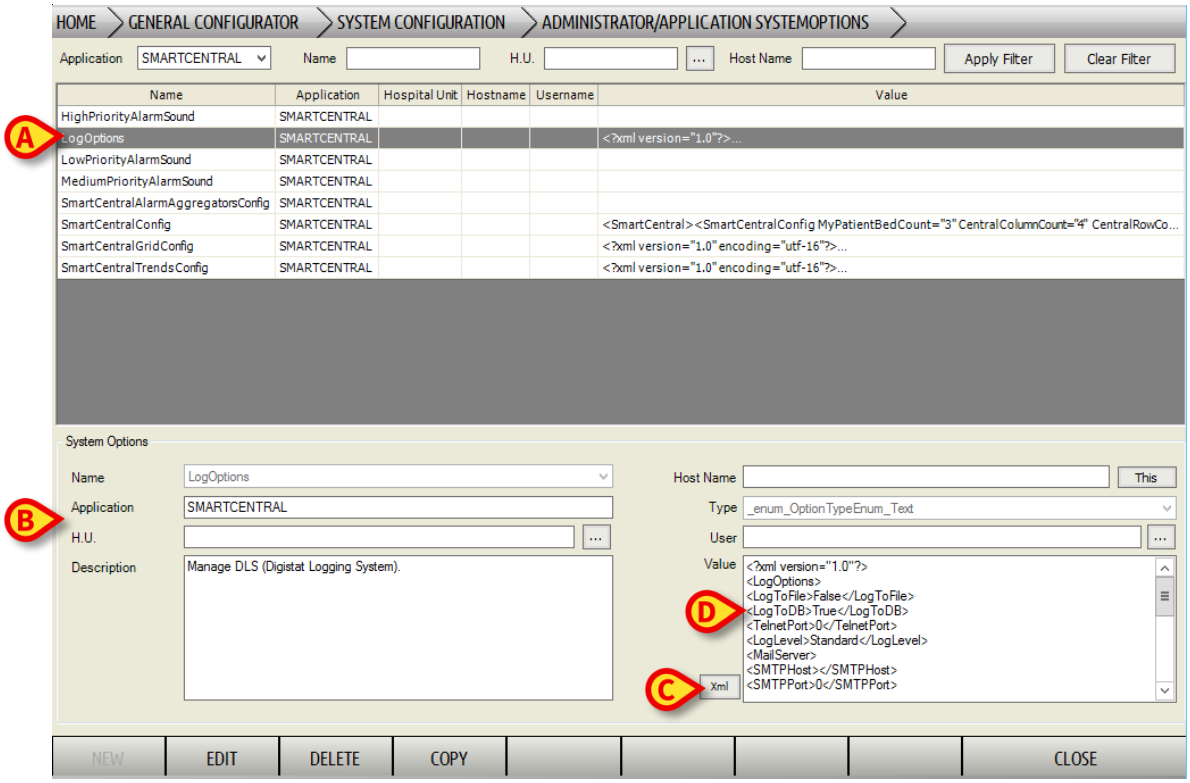


Fig 30

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

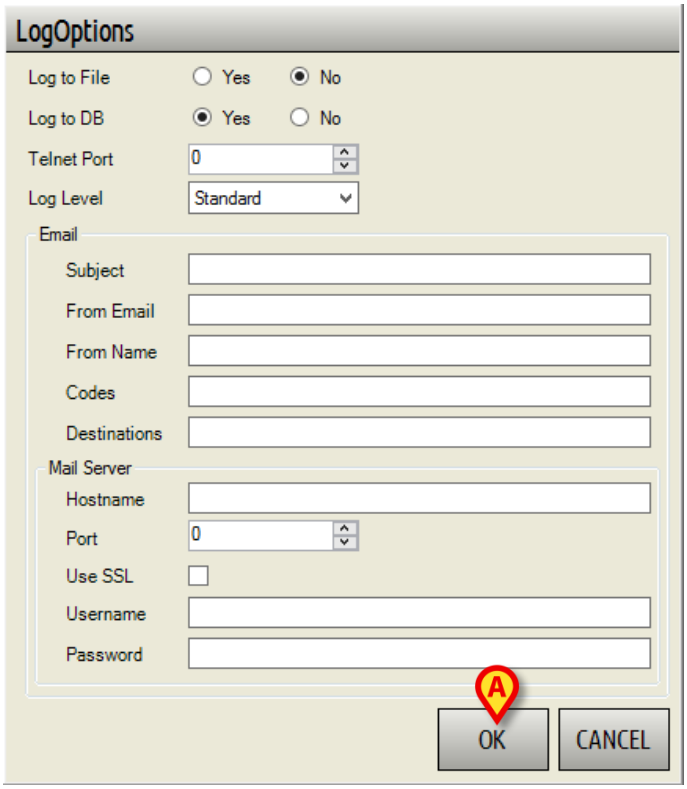


Fig 31

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 **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**).

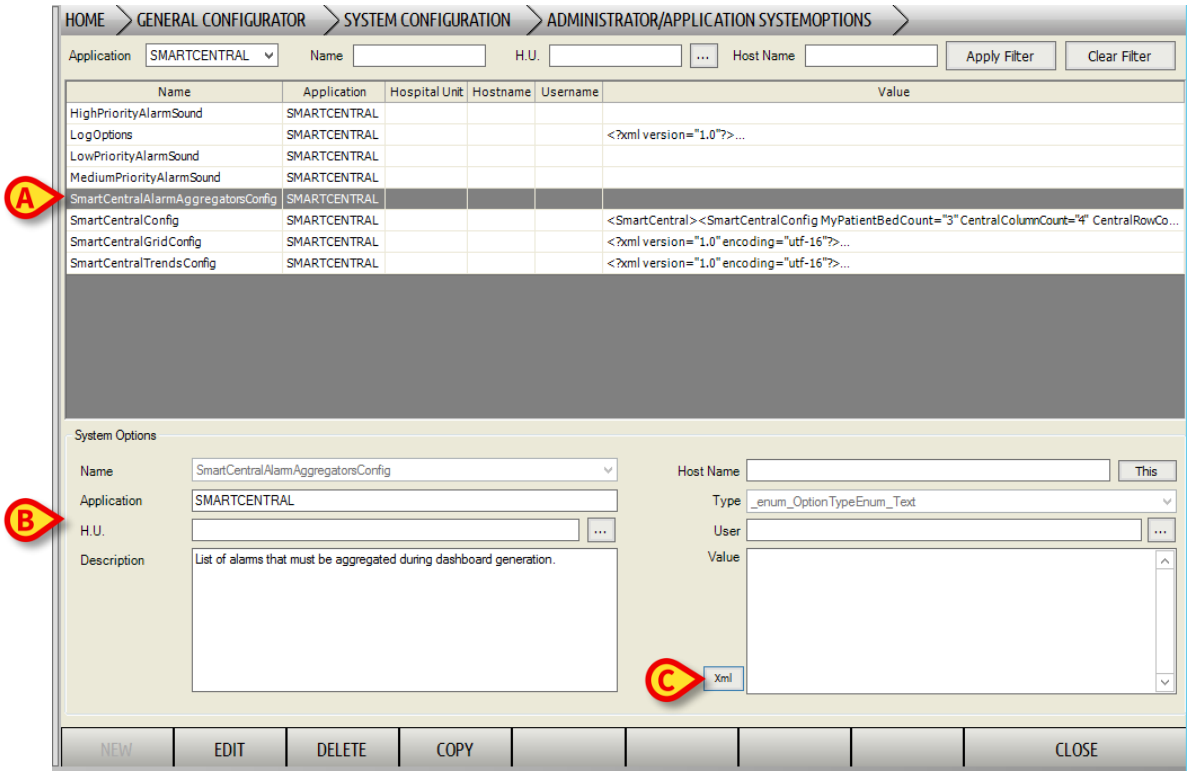


Fig 32

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

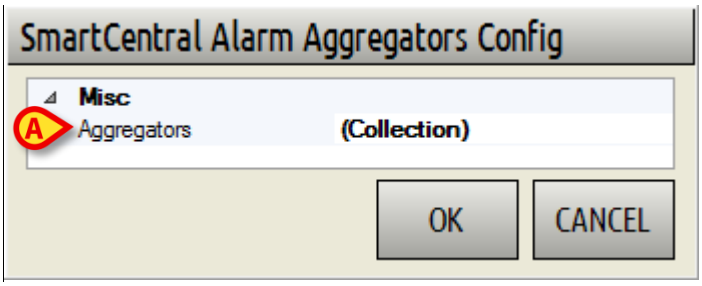


Fig 33

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

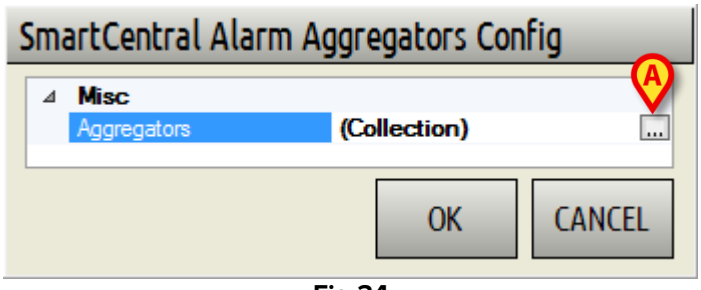


Fig 34

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

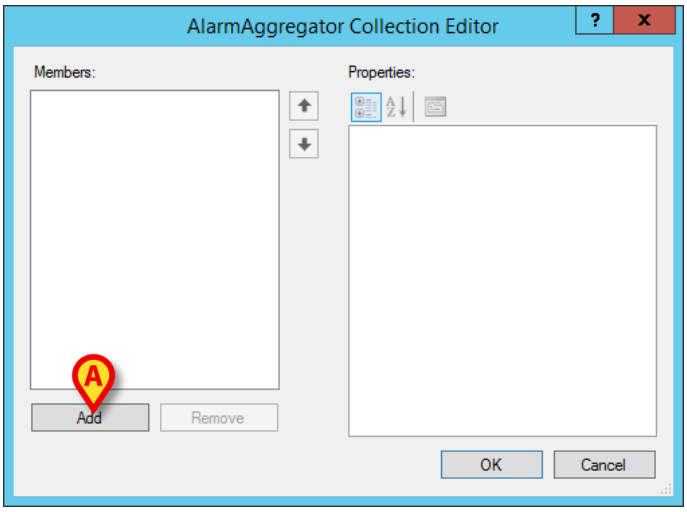


Fig 35

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**).

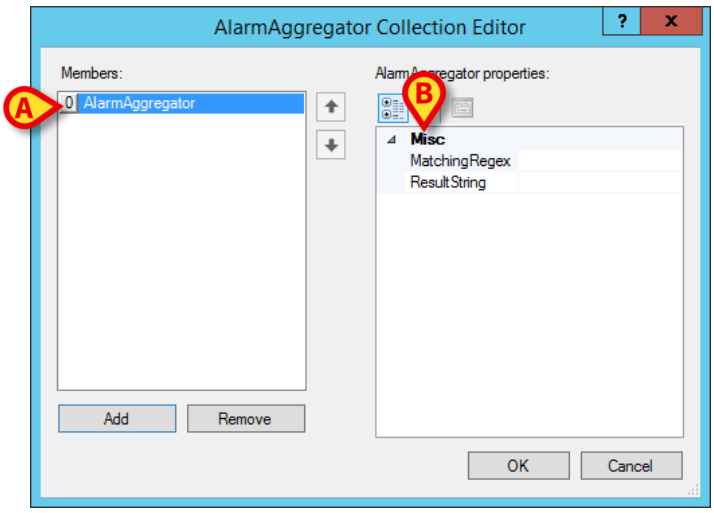


Fig 36

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.

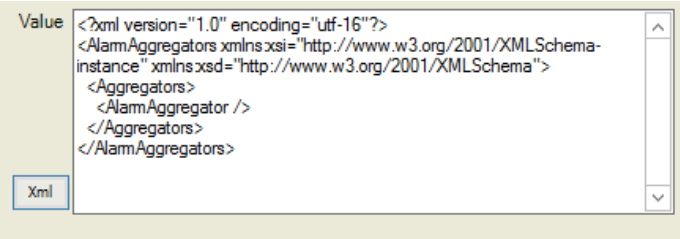


Fig 37

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**).

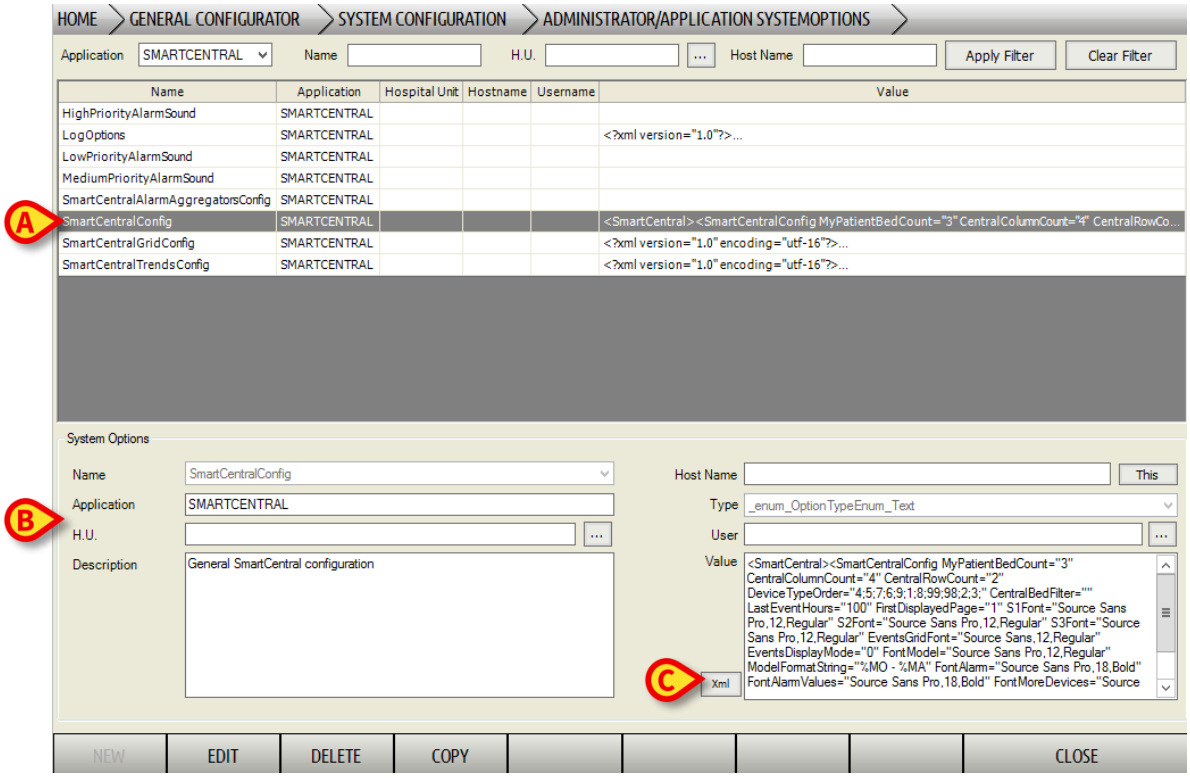


Fig 38

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

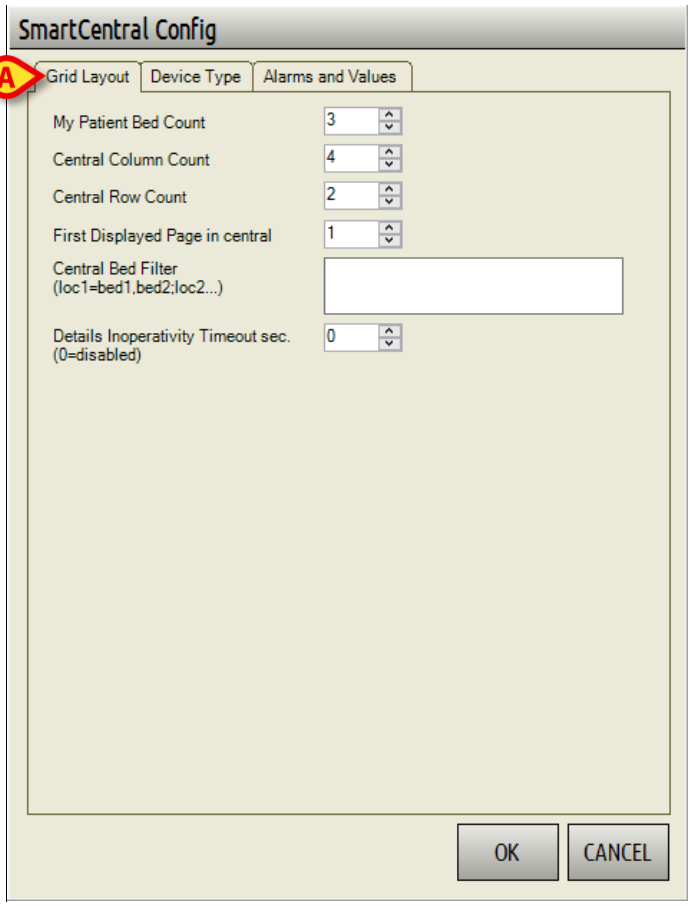


Fig 39

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...Bed*n*; location name2=Bed1, Bed2...Bed*n* 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**.

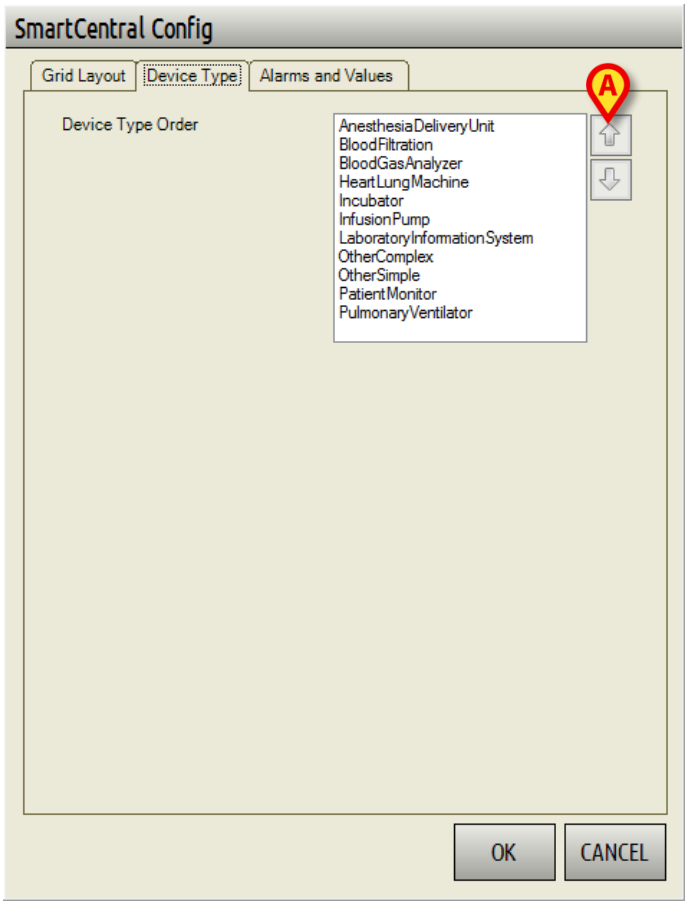


Fig 40

8.2.4.3 Alarms and values

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

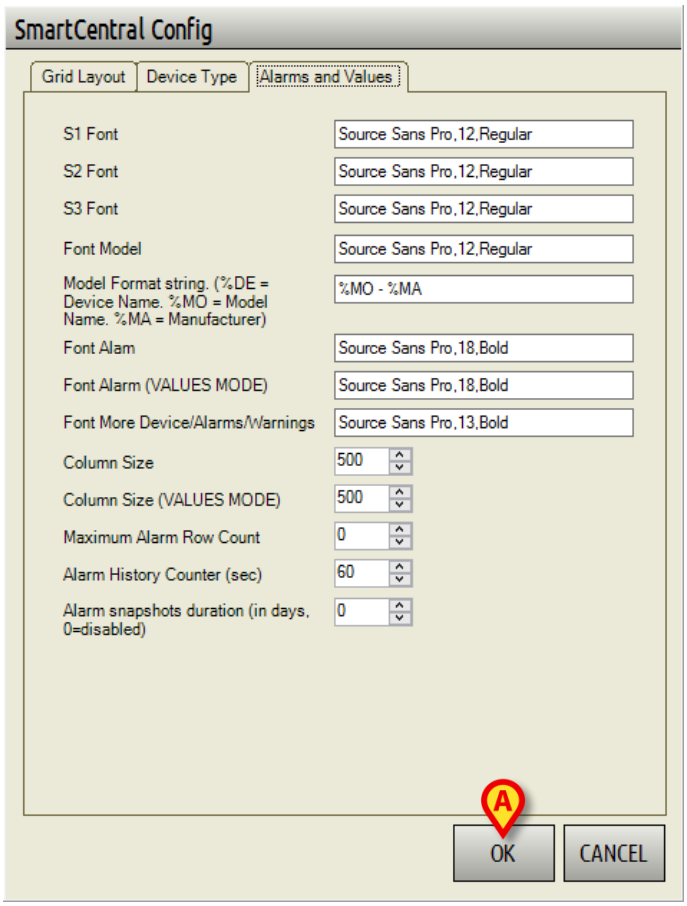


Fig 41

- 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.

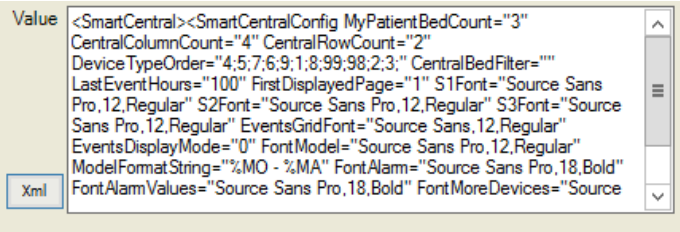


Fig 42

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**).

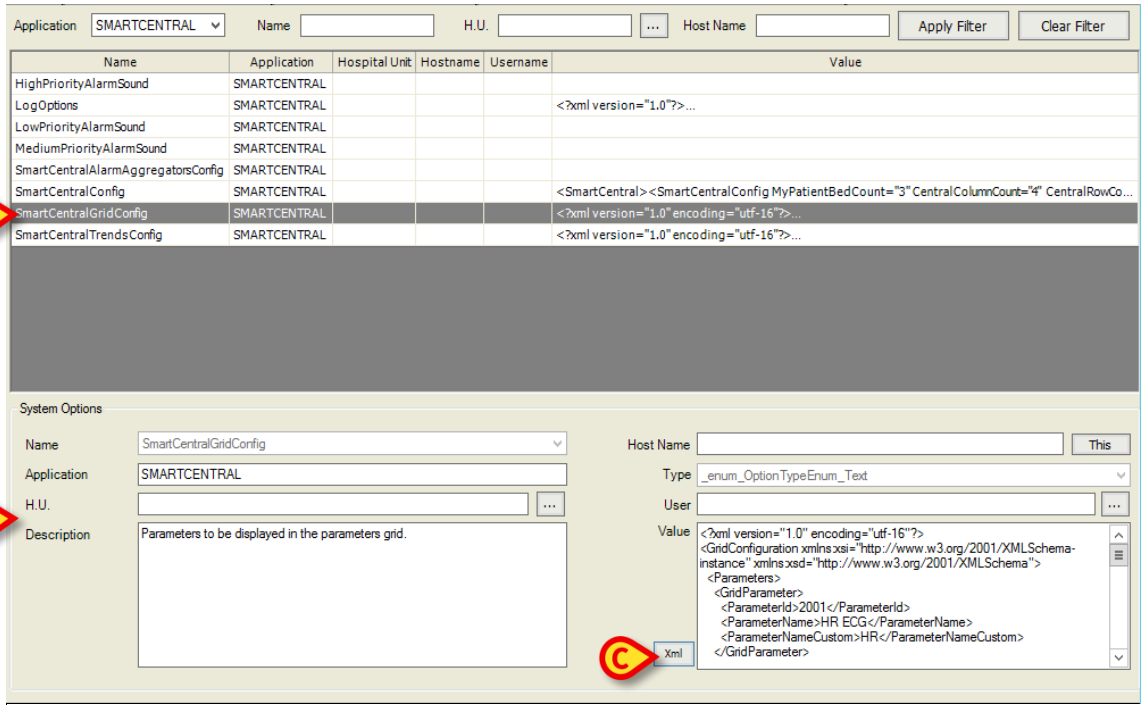


Fig 43

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

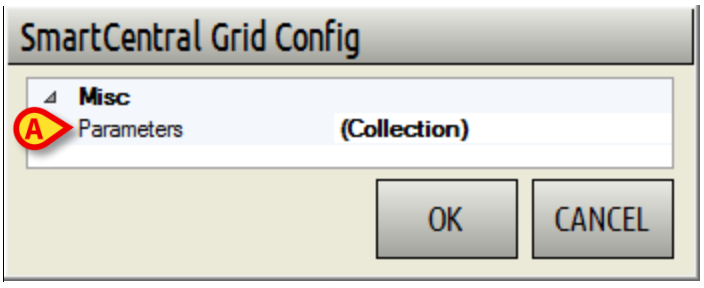


Fig 44

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

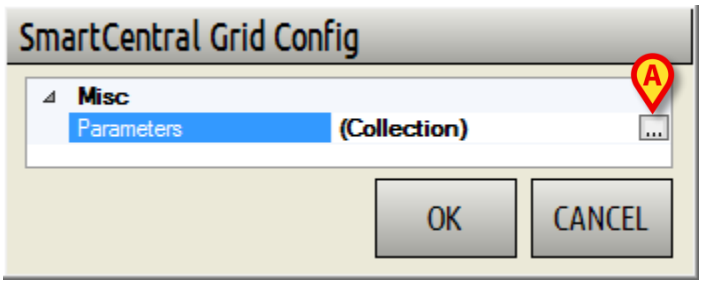


Fig 45

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

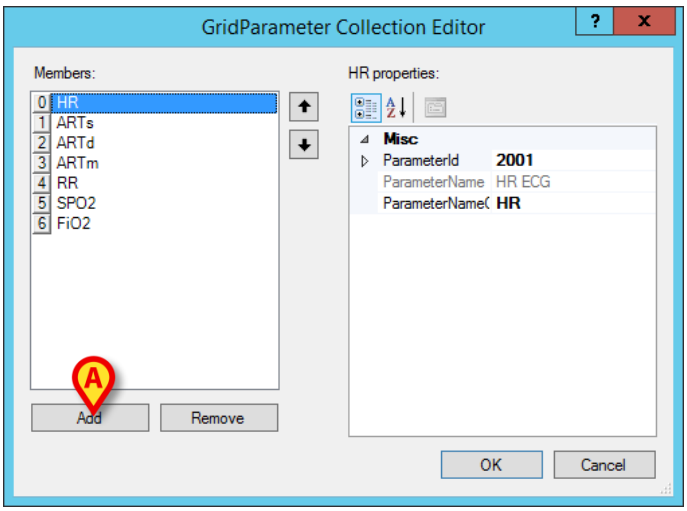


Fig 46

To add a new parameter

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

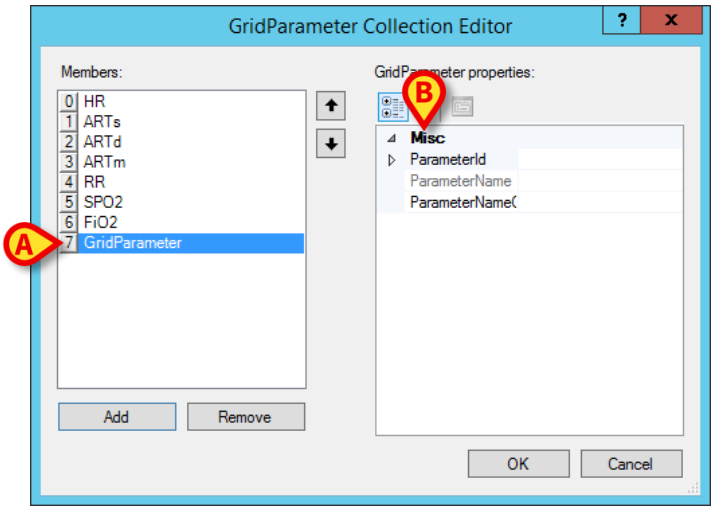


Fig 47

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**).

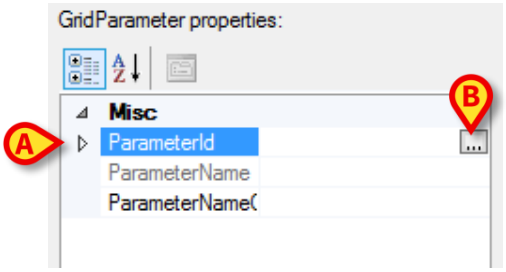


Fig 48

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

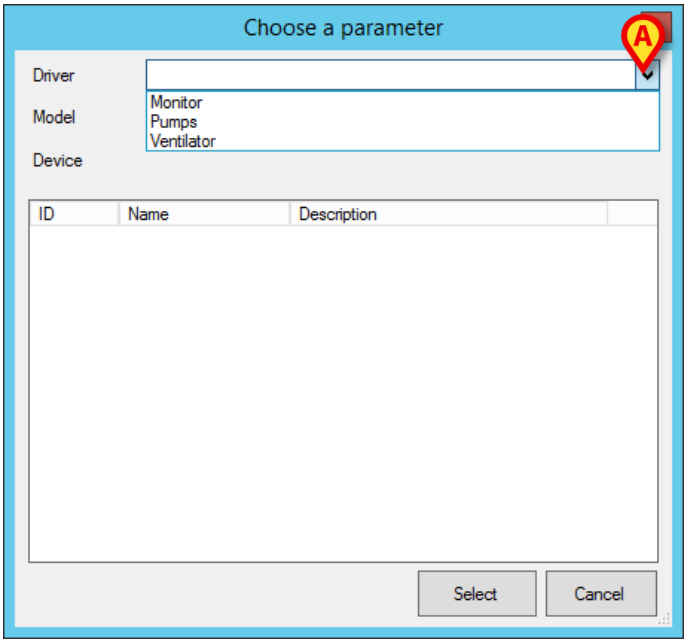


Fig 49

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).

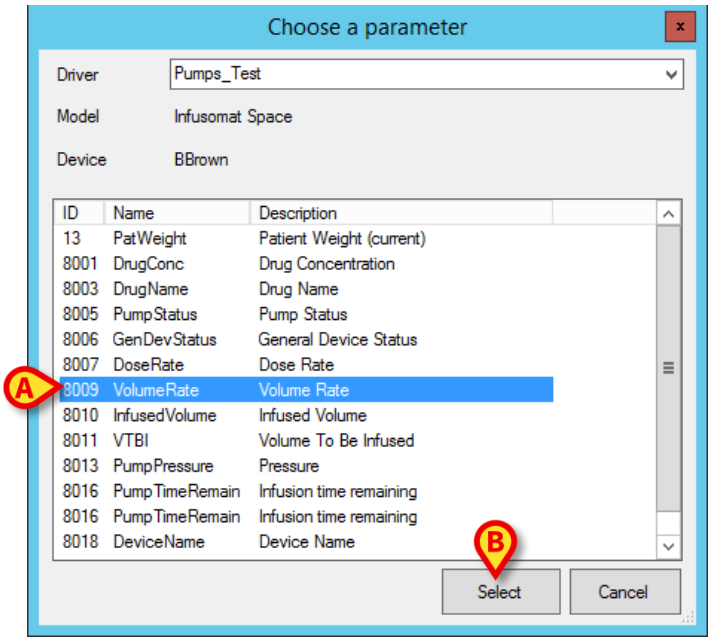


Fig 50

9. Click the row corresponding to the wanted parameter on the list (Fig 50 **A**). The row will be highlighted.

10. 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**).

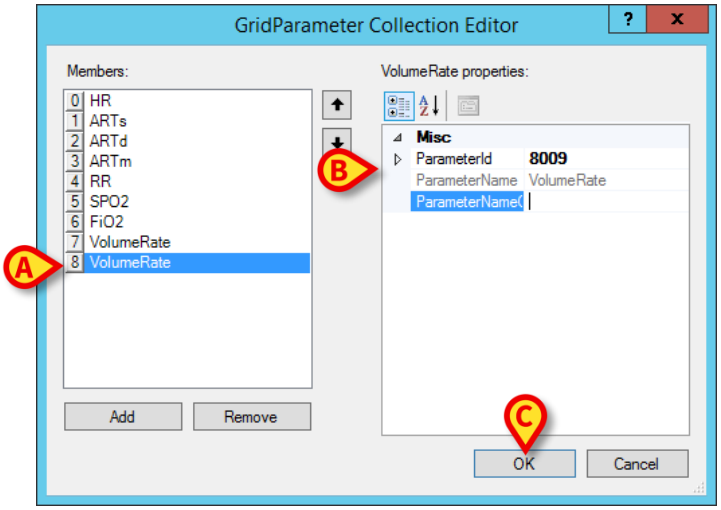


Fig 51

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

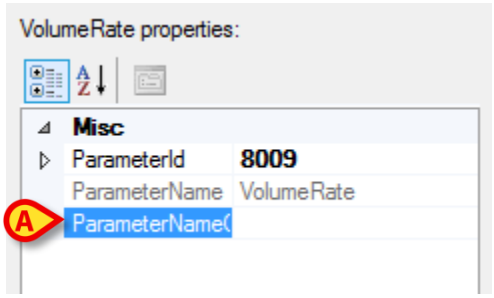


Fig 52

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.

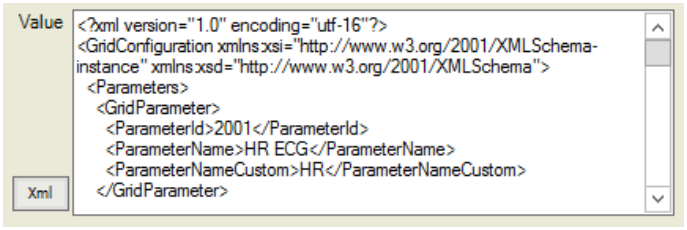


Fig 53

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**).

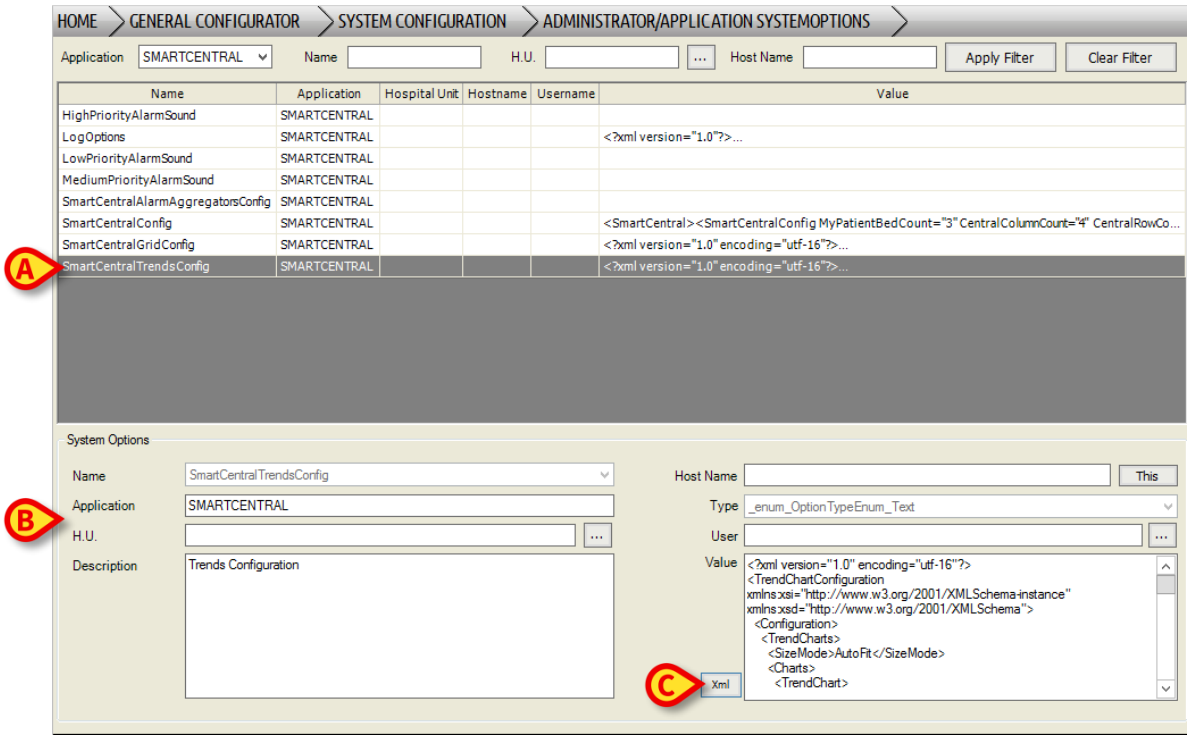


Fig 54

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

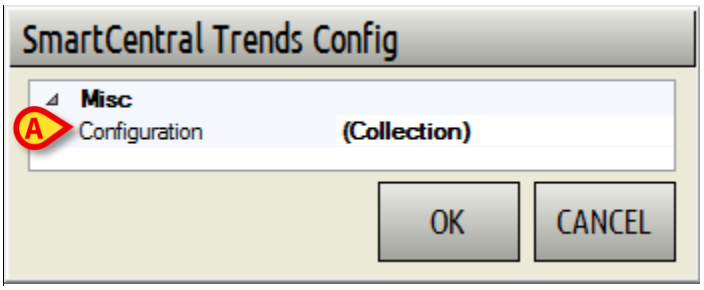


Fig 55

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

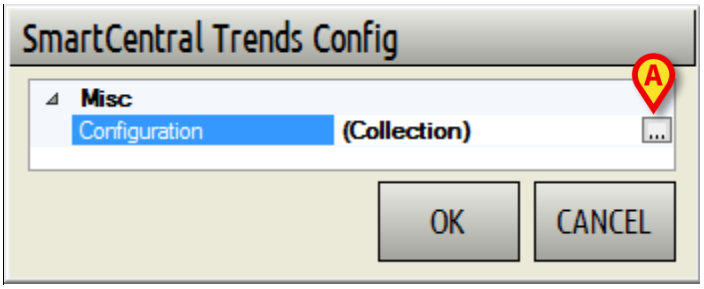


Fig 56

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

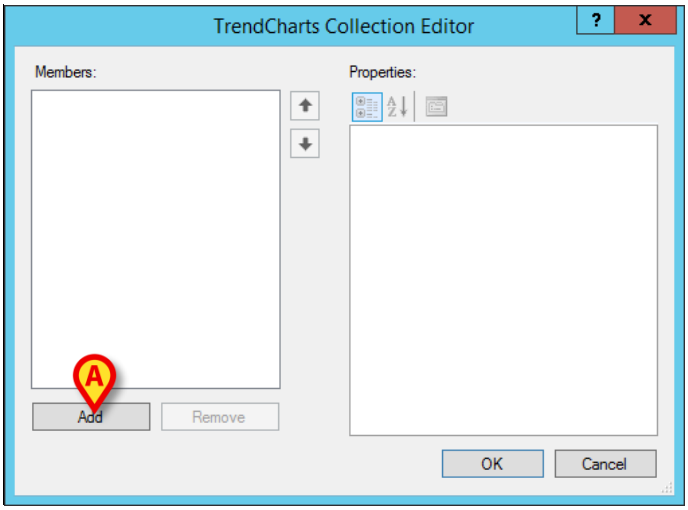


Fig 57

To add a new member

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

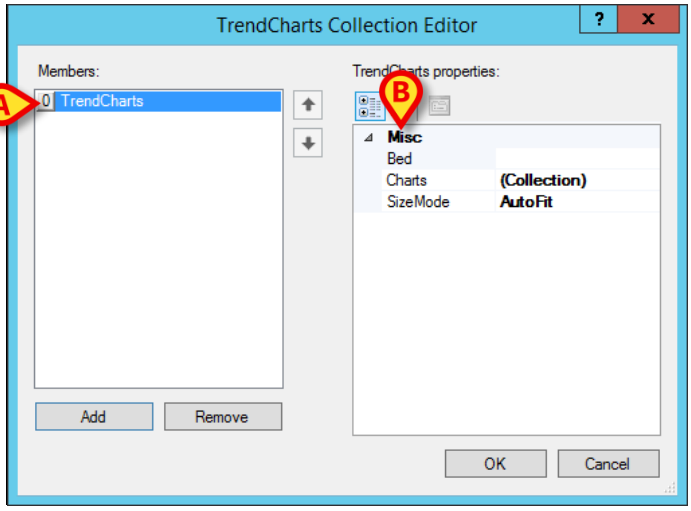


Fig 58

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**).

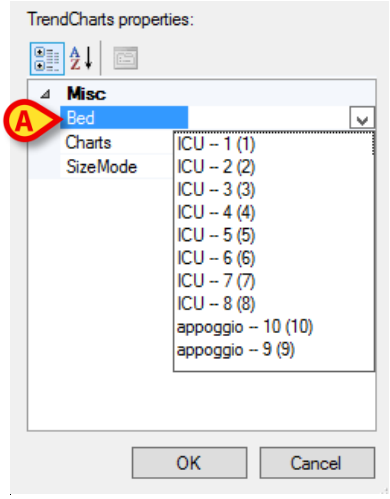


Fig 59

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

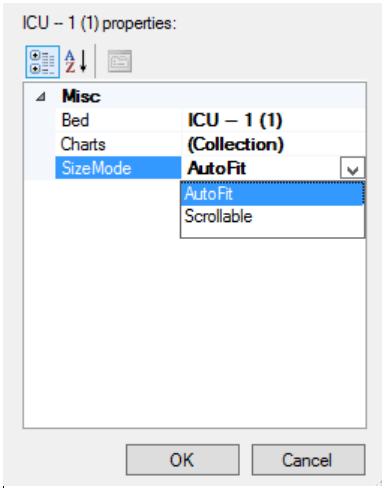


Fig 60

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

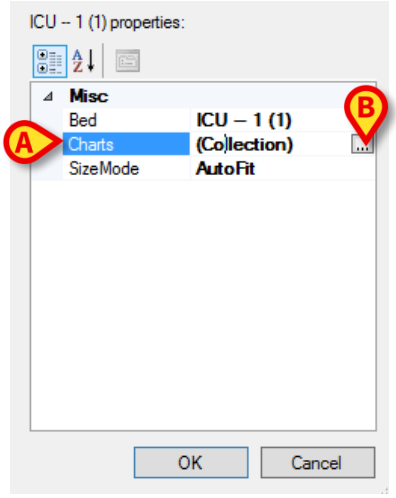


Fig 61

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

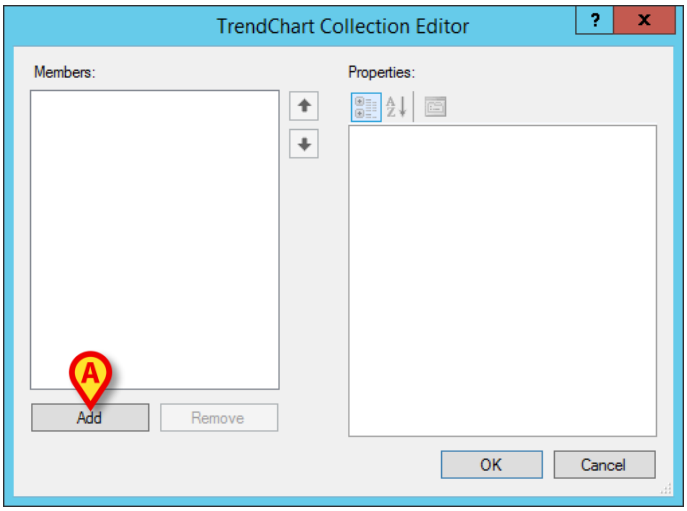


Fig 62

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

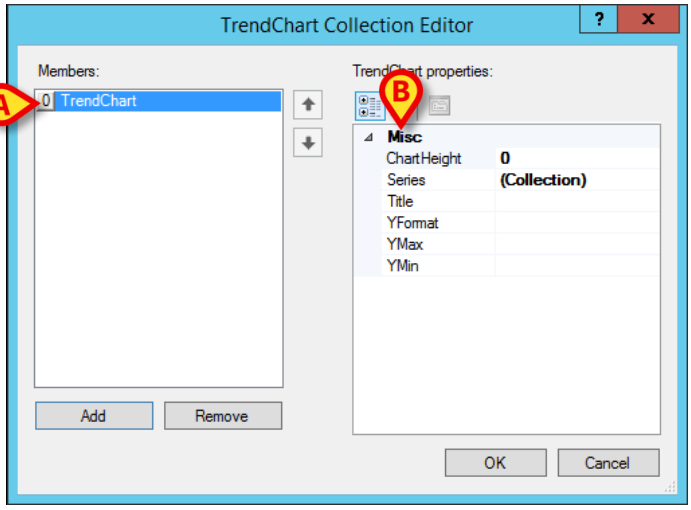


Fig 63

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).

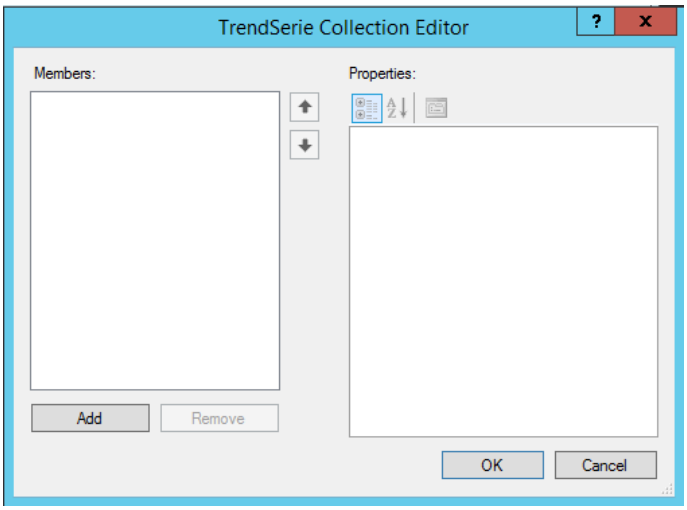


Fig 64

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

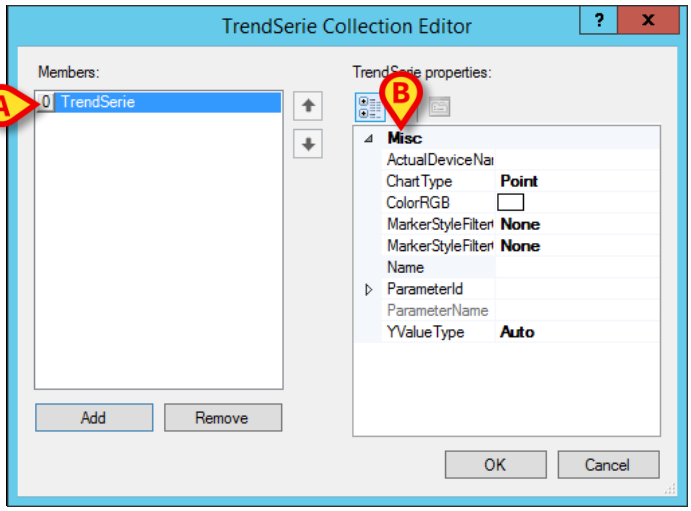


Fig 65

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).

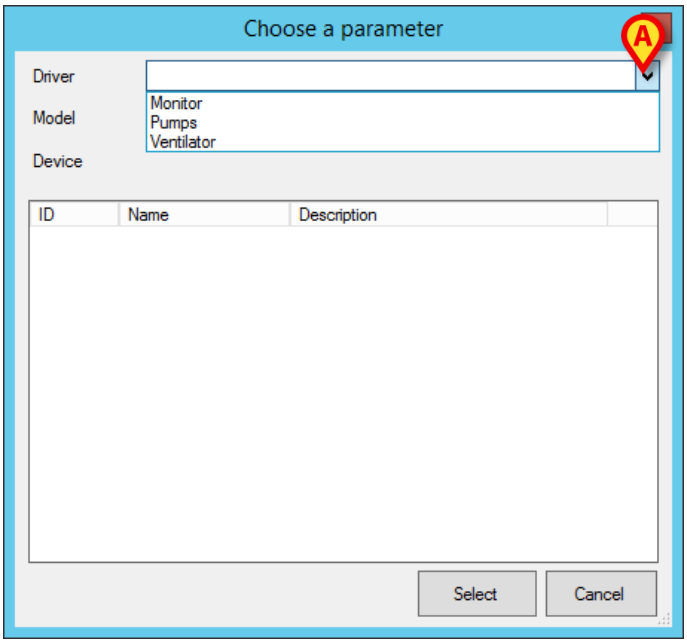


Fig 66

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).

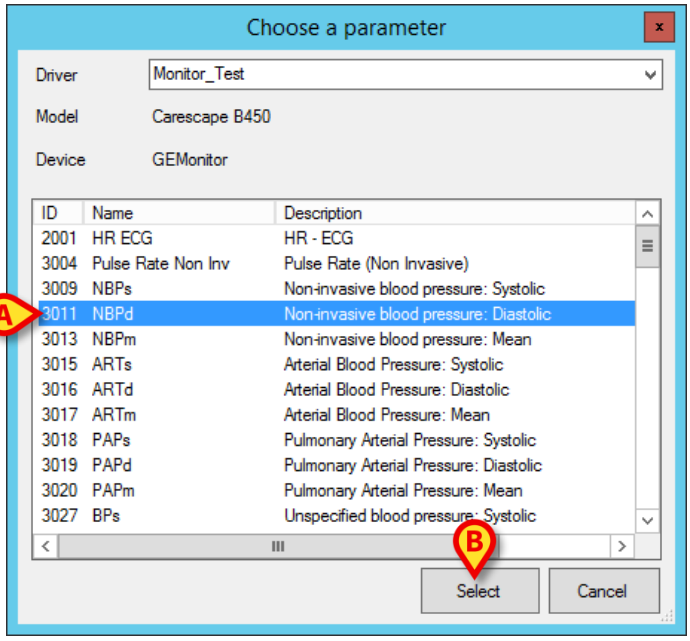


Fig 67

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.

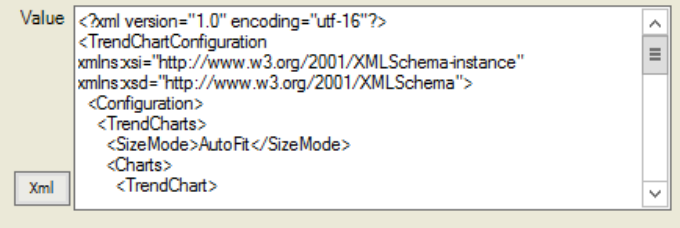


Fig 68

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.

Fig 69

The following screen opens (Fig 70).

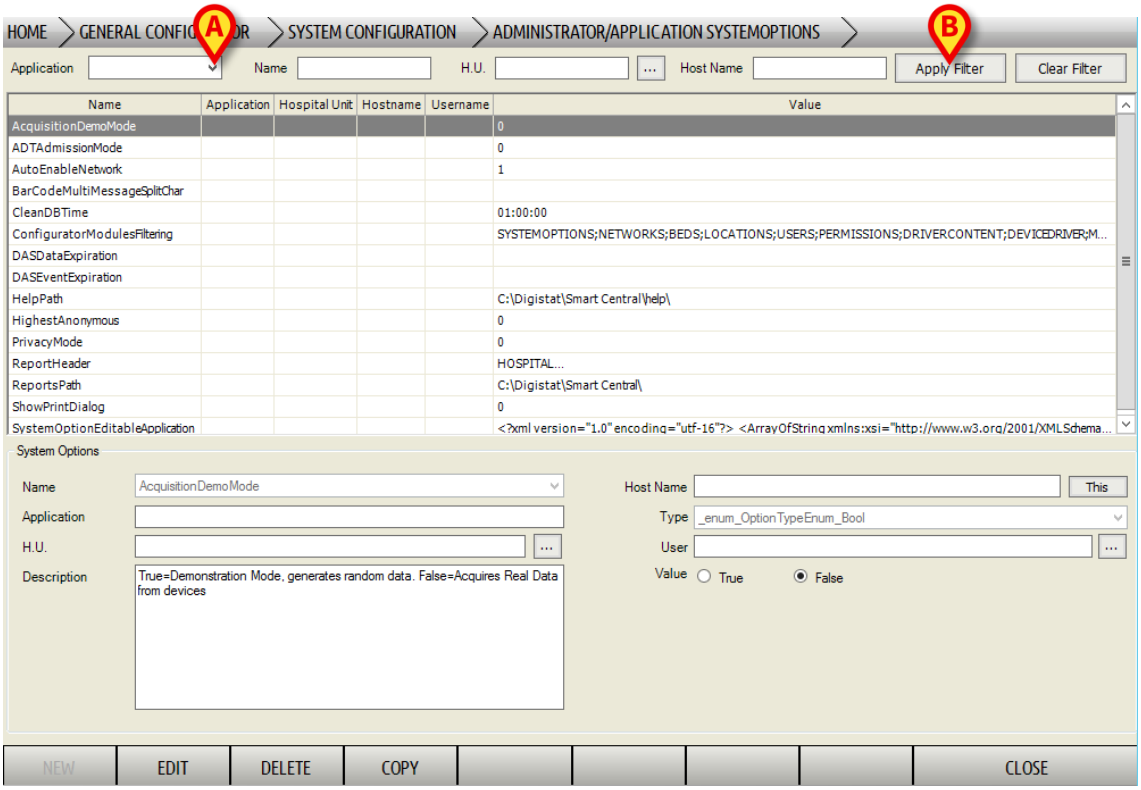


Fig 70

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**).

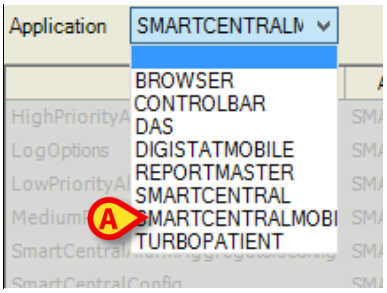


Fig 71

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

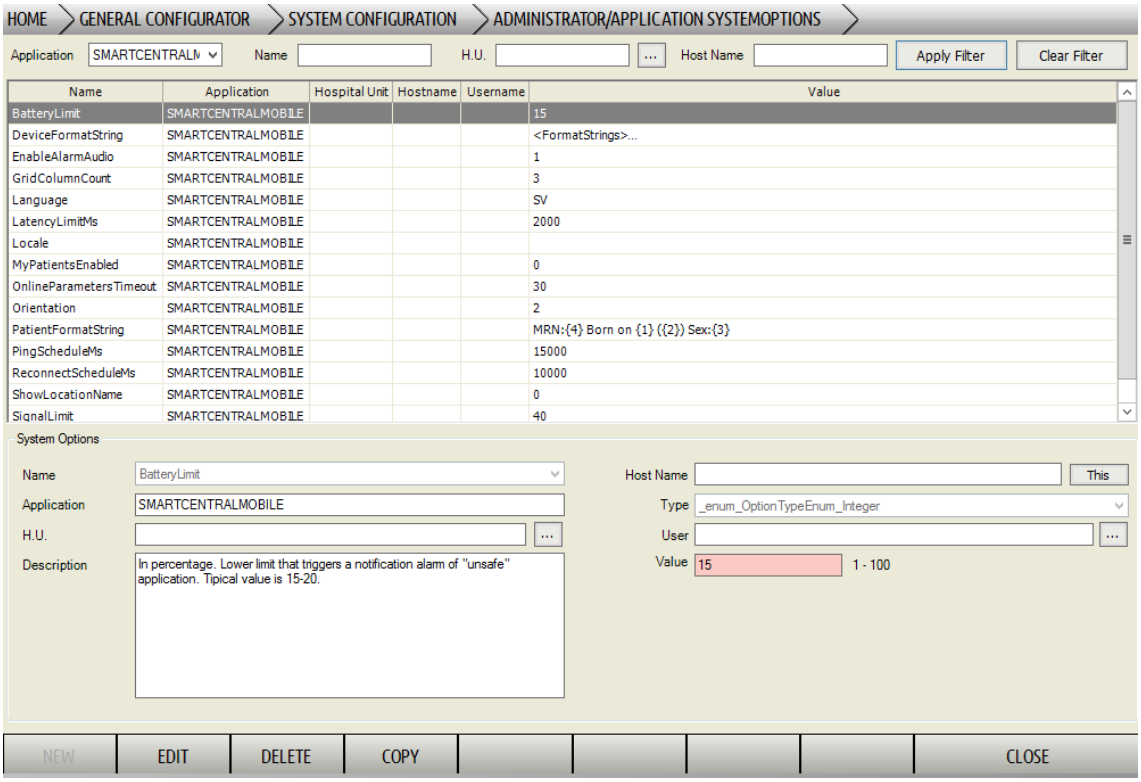


Fig 72

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**.

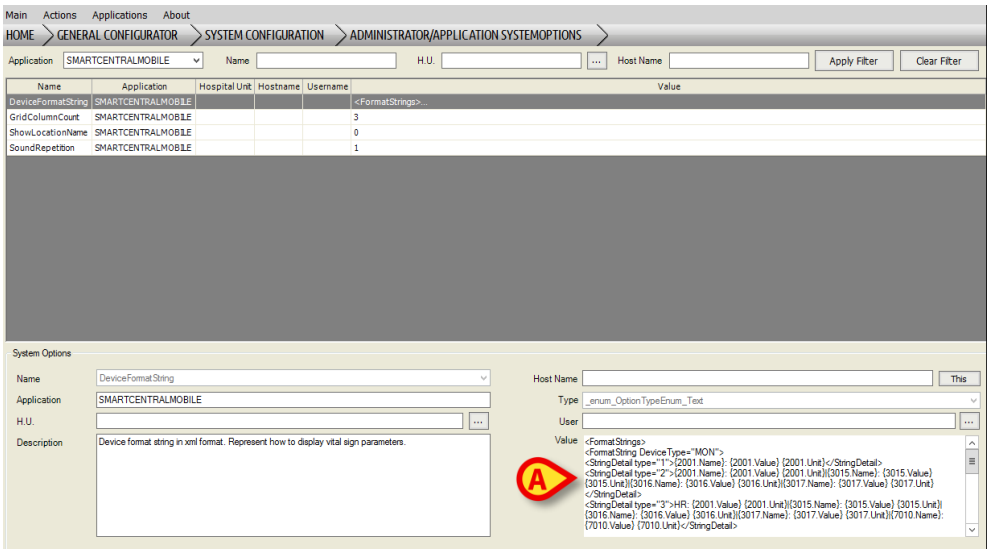


Fig 73

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}: {3016.Value}
{3016.Unit}|{3017.Name}: {3017.Value} {3017.Unit}|{7010.Name}:
{7010.Value} {7010.Unit}</StringDetail>
</FormatString>
```

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.

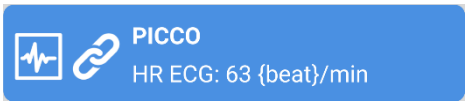


Fig 74

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.

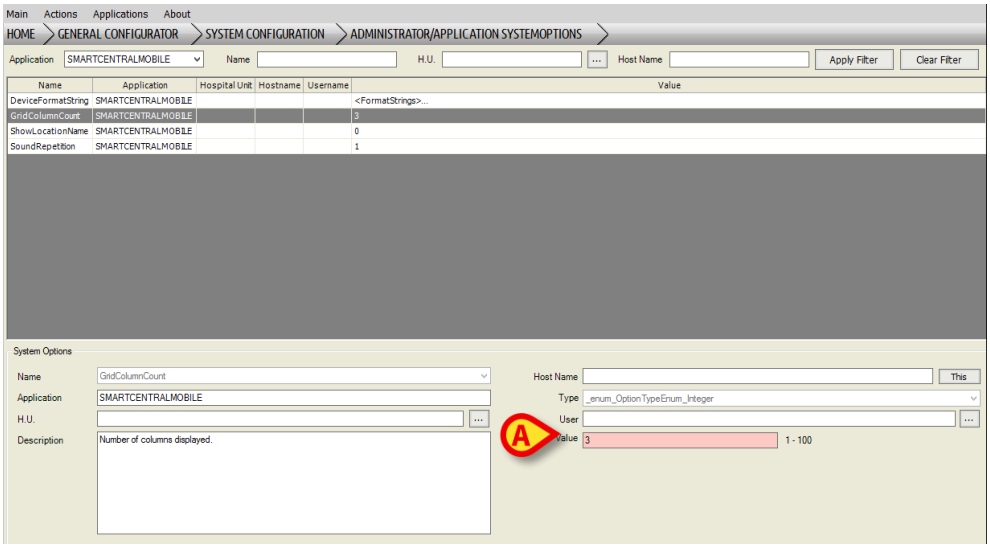


Fig 75

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.

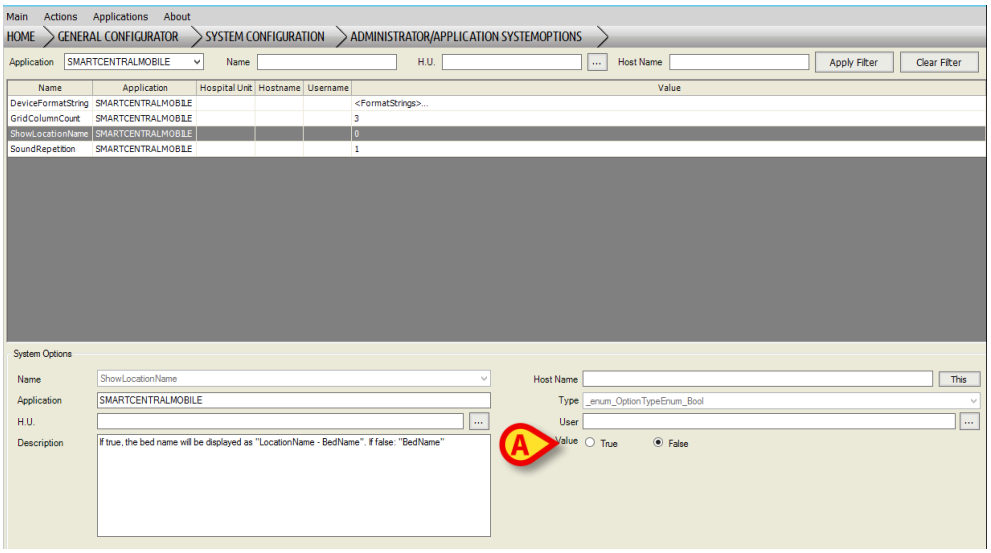


Fig 76

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.

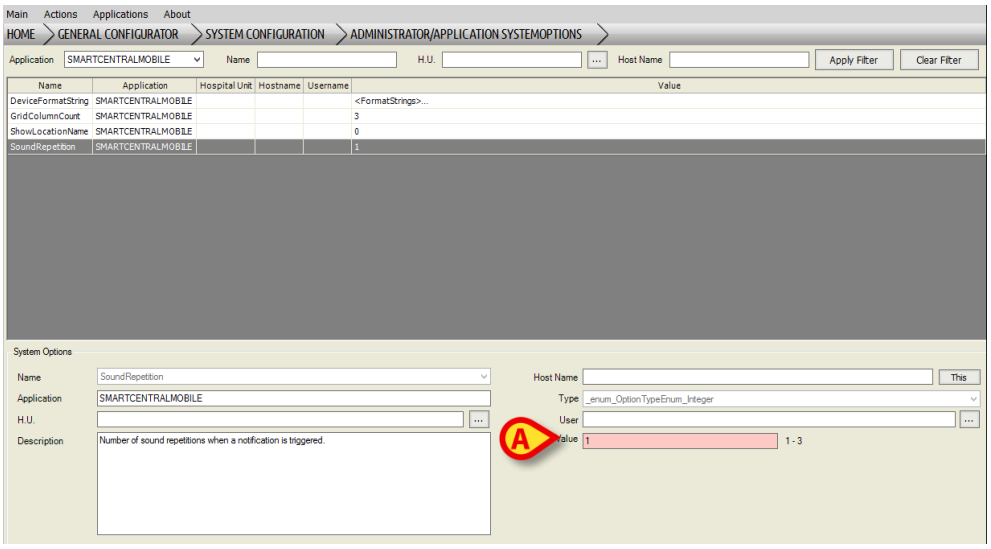


Fig 77

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.

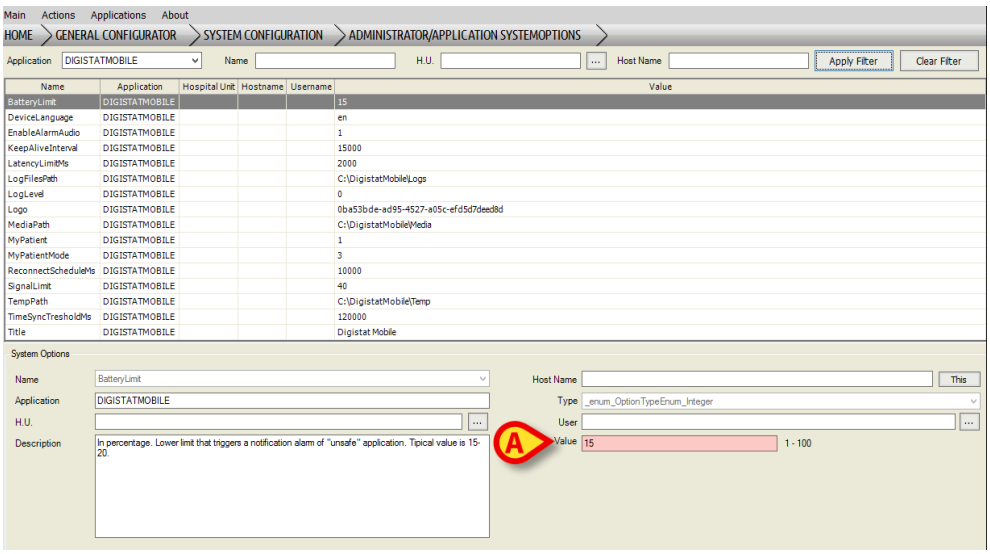


Fig 78

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.

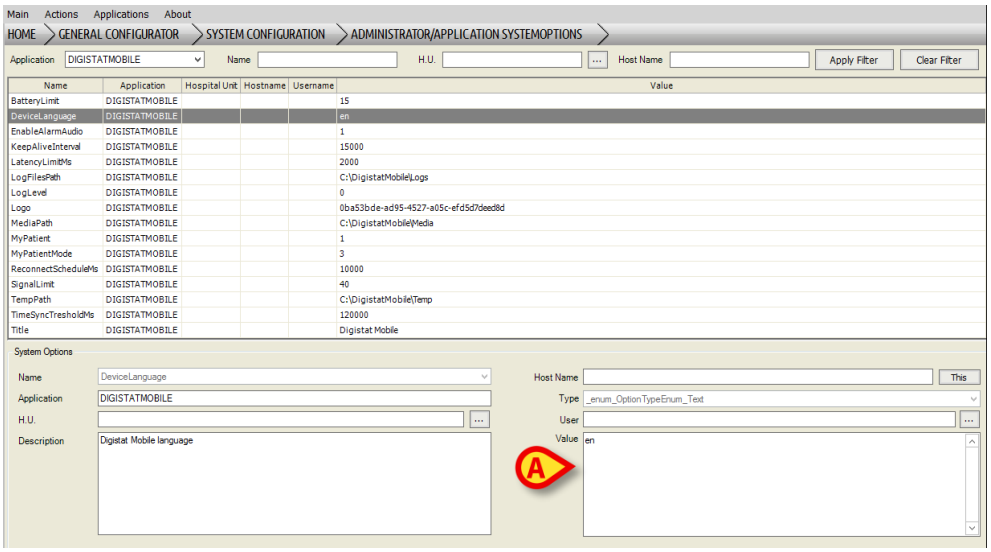


Fig 79

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.

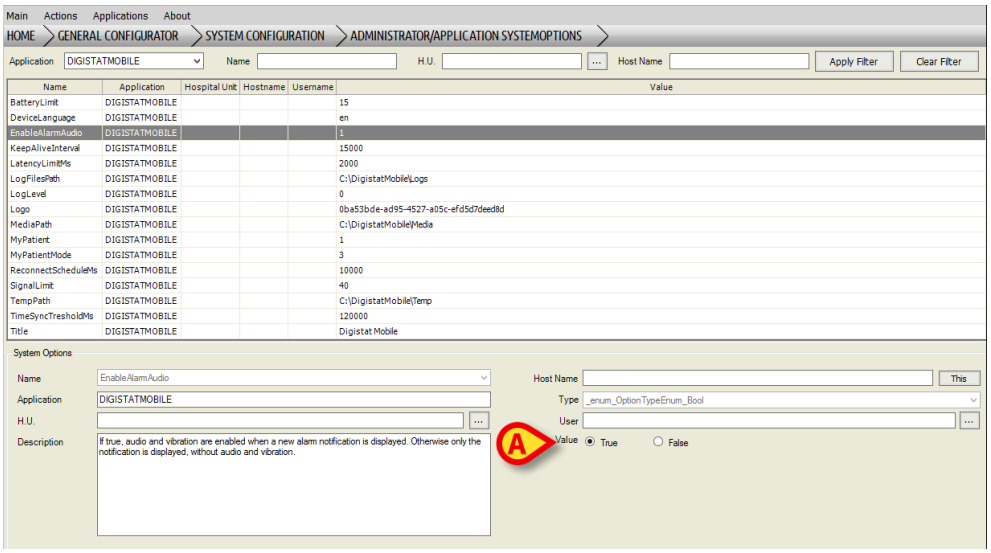


Fig 80

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.

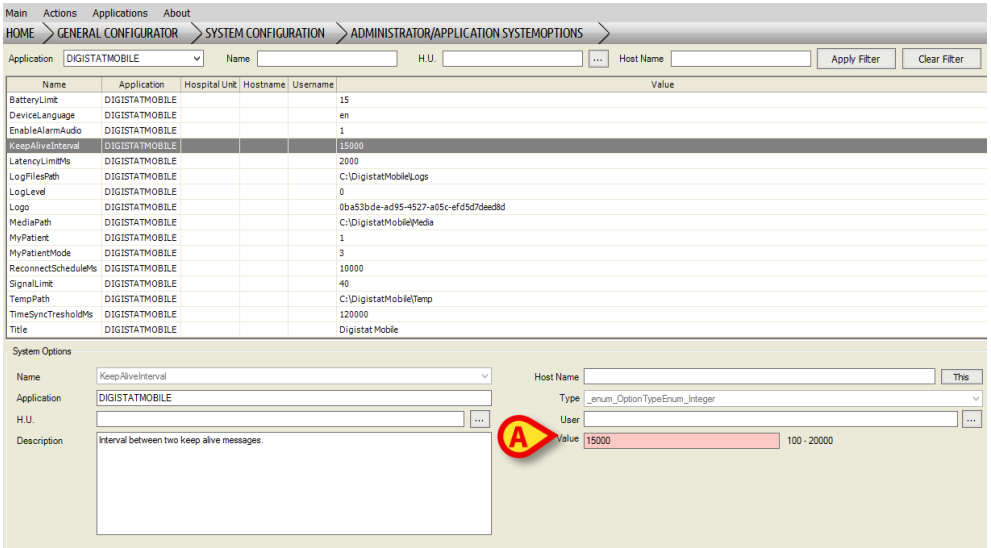


Fig 81

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.

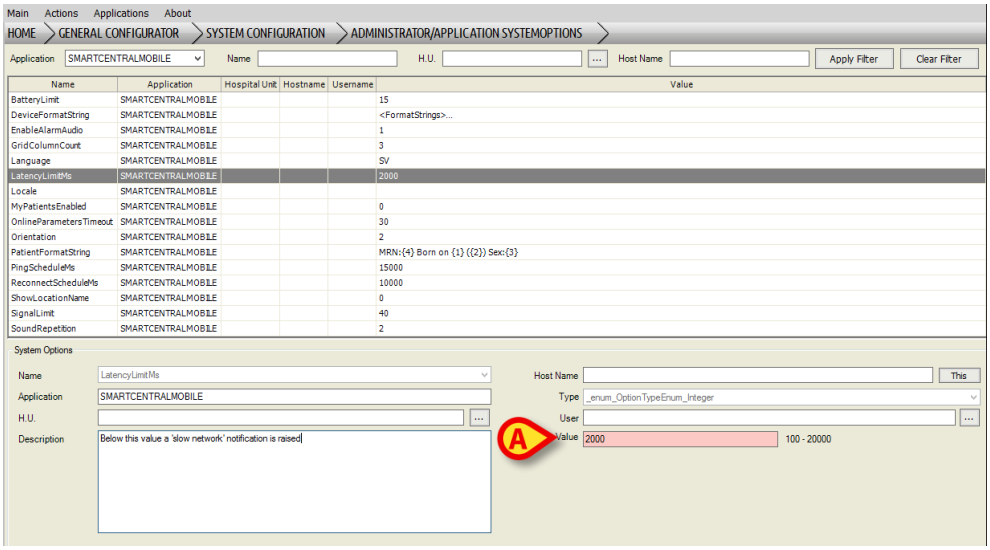


Fig 82

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*.

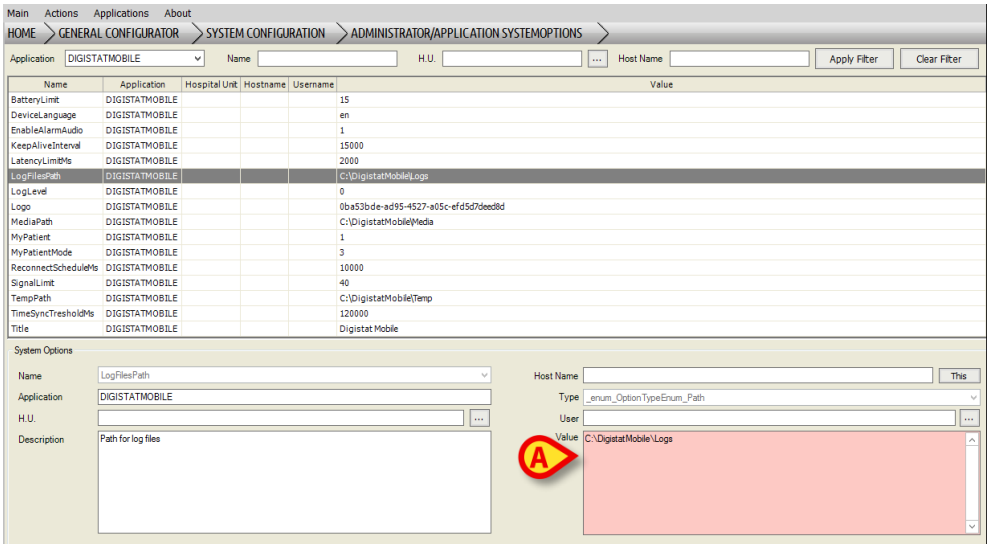


Fig 83

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.

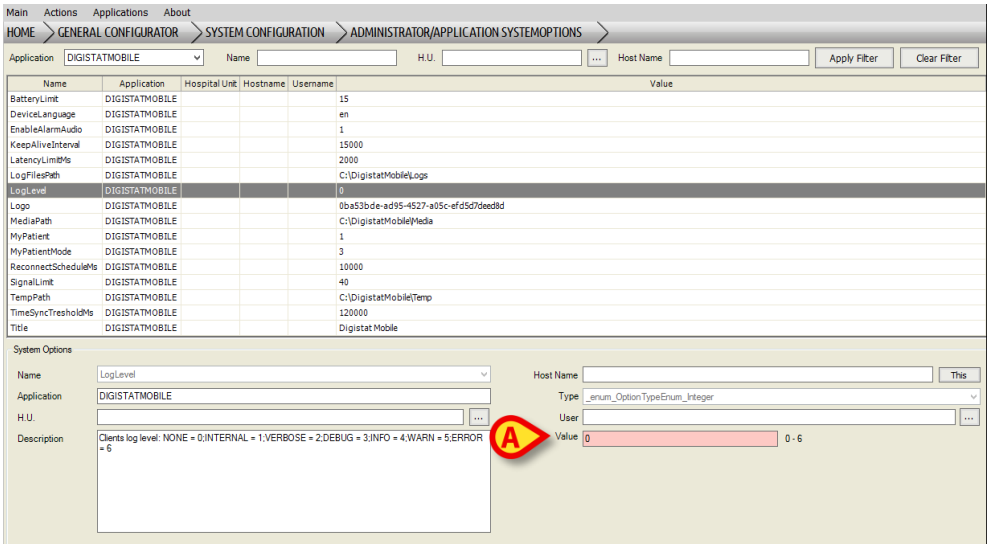


Fig 84

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.

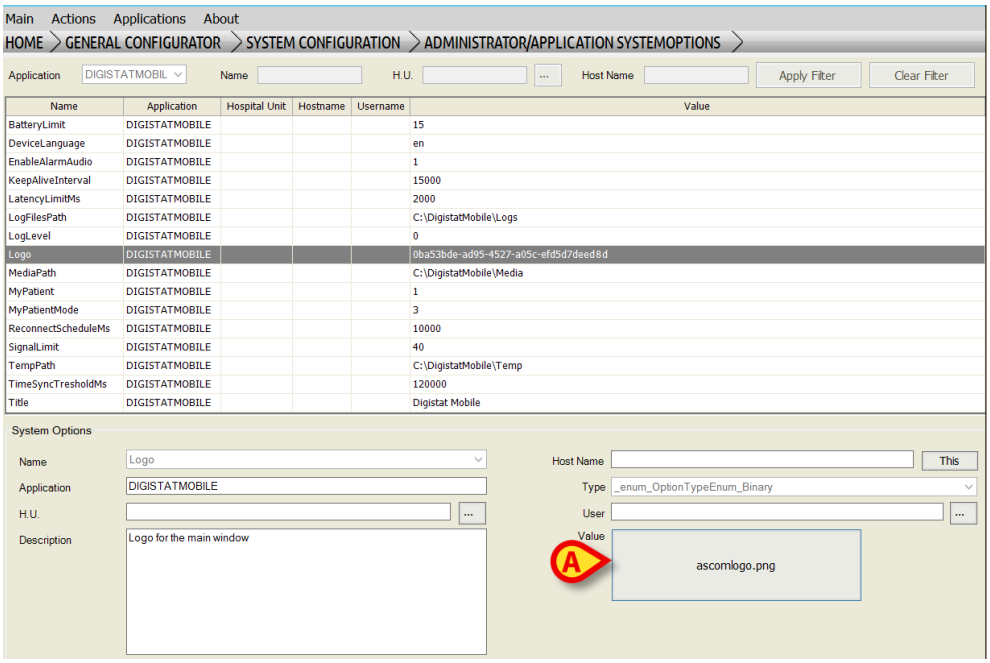


Fig 85

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**).

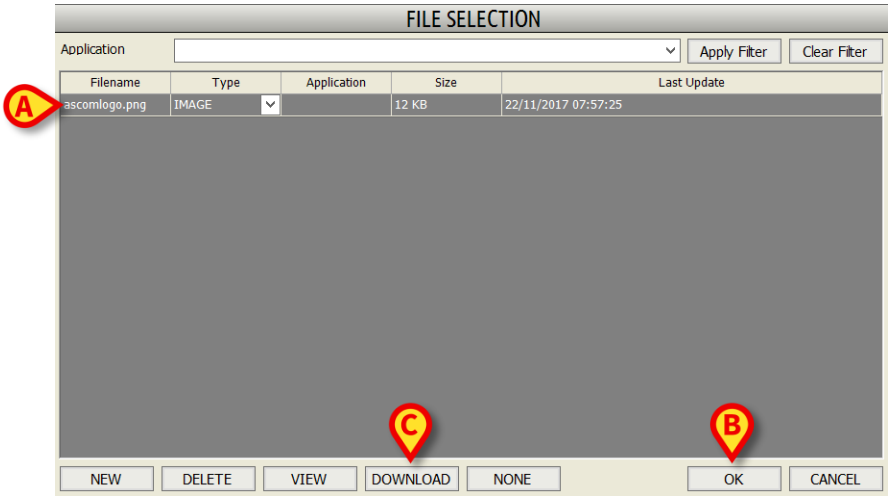


Fig 86

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.

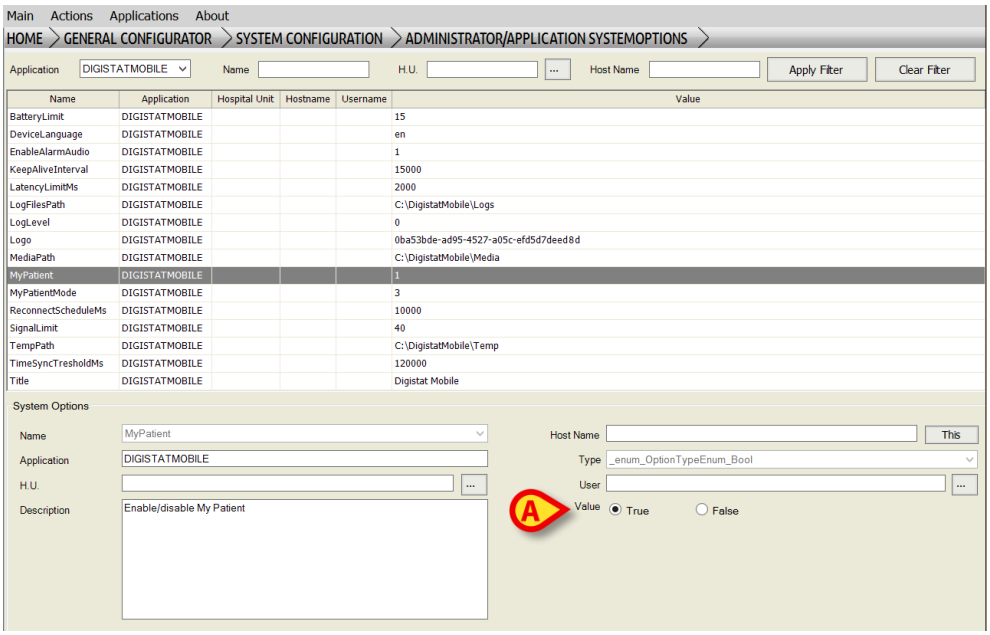


Fig 87

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.

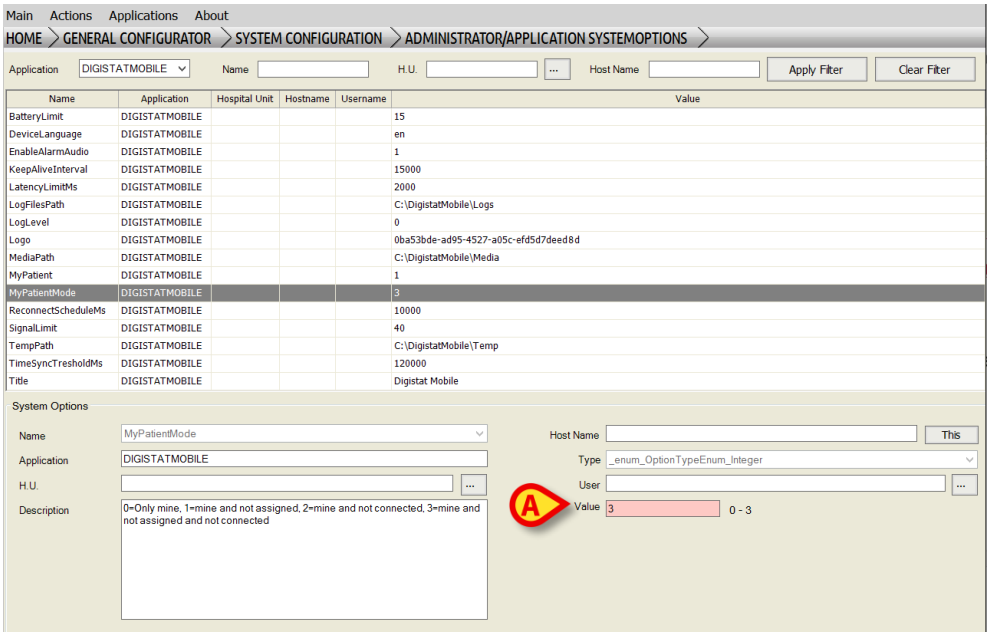


Fig 88

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.

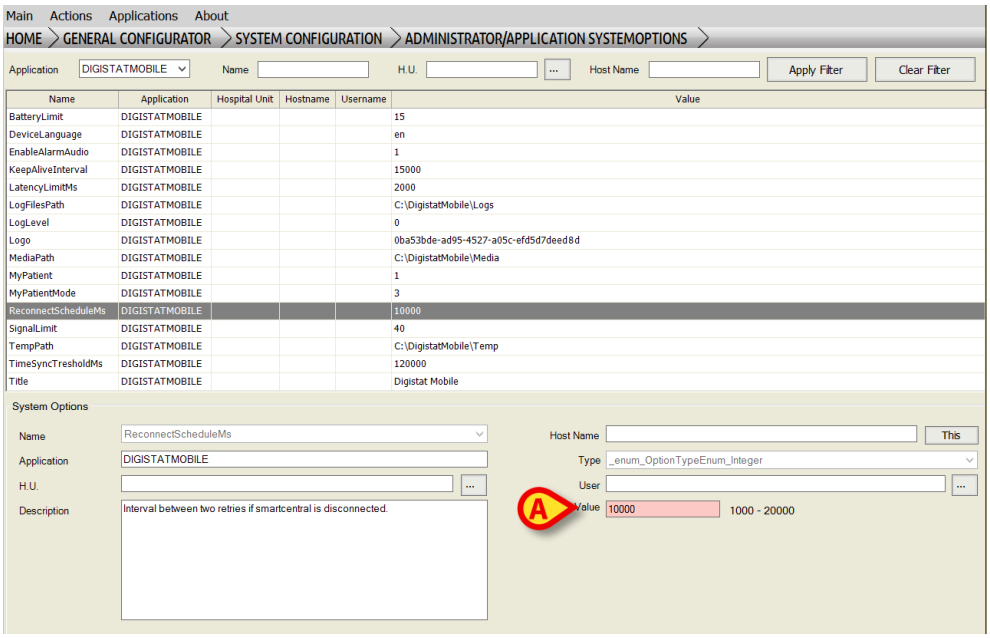


Fig 89

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.

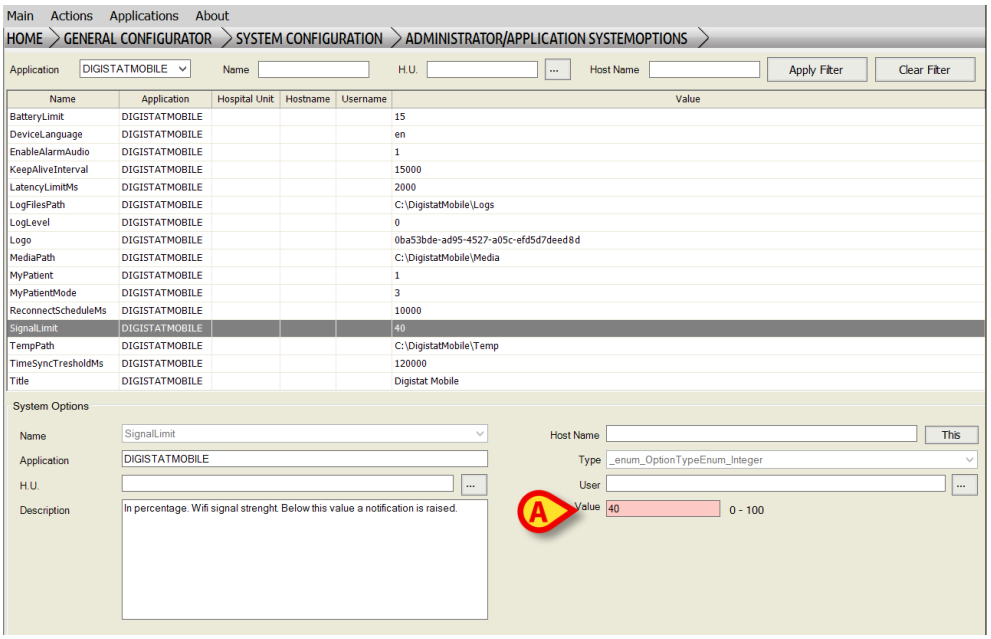


Fig 90

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*.

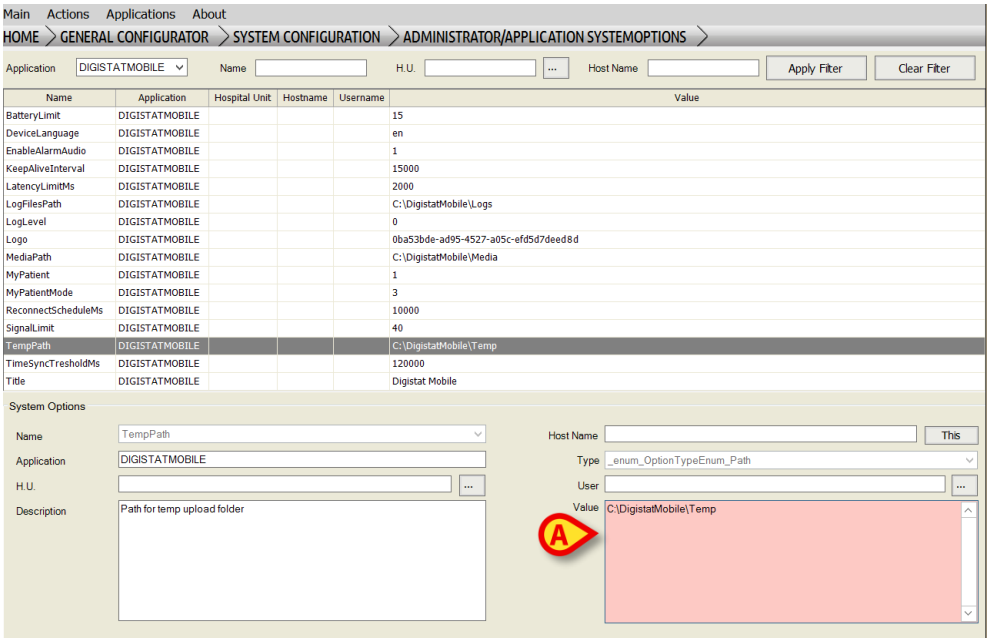


Fig 91

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.

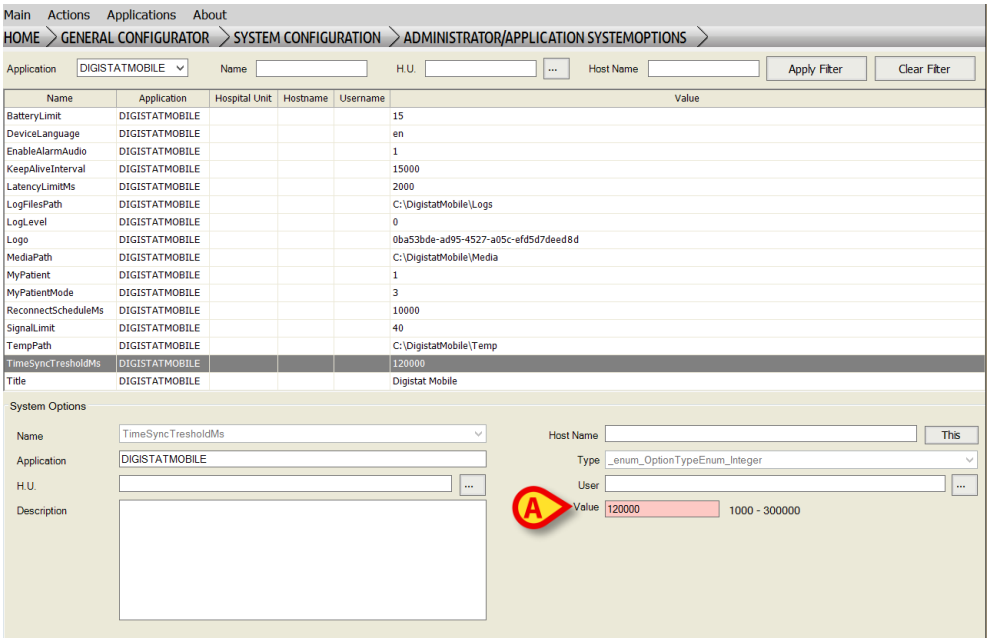


Fig 92

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”.

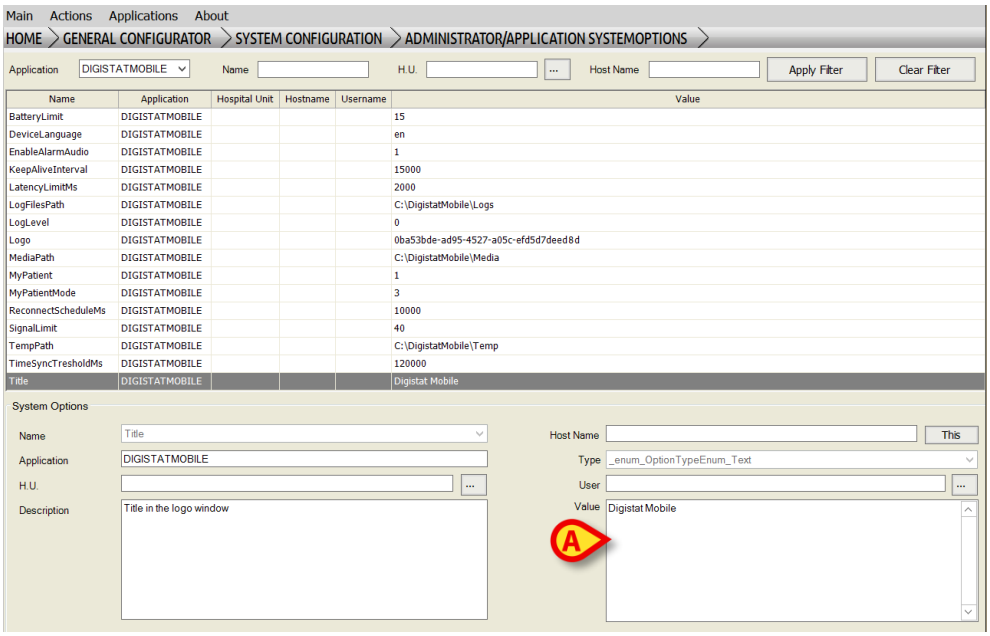


Fig 93

To edit the Title system option enter the wanted value in the field indicated in Fig 93 **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.

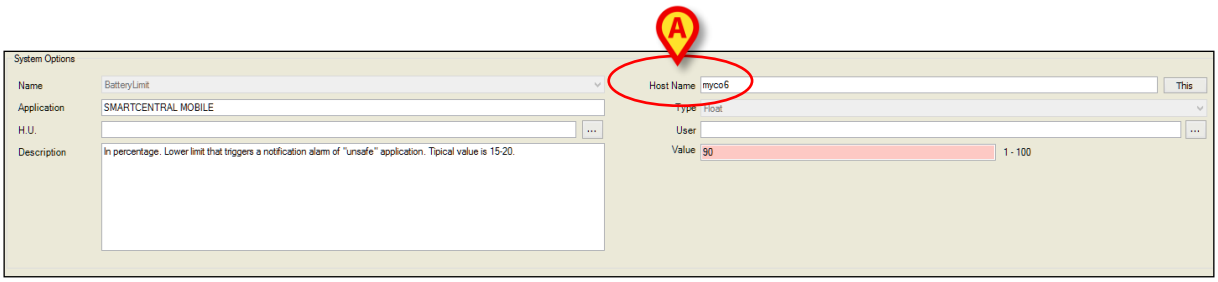


Fig 94

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

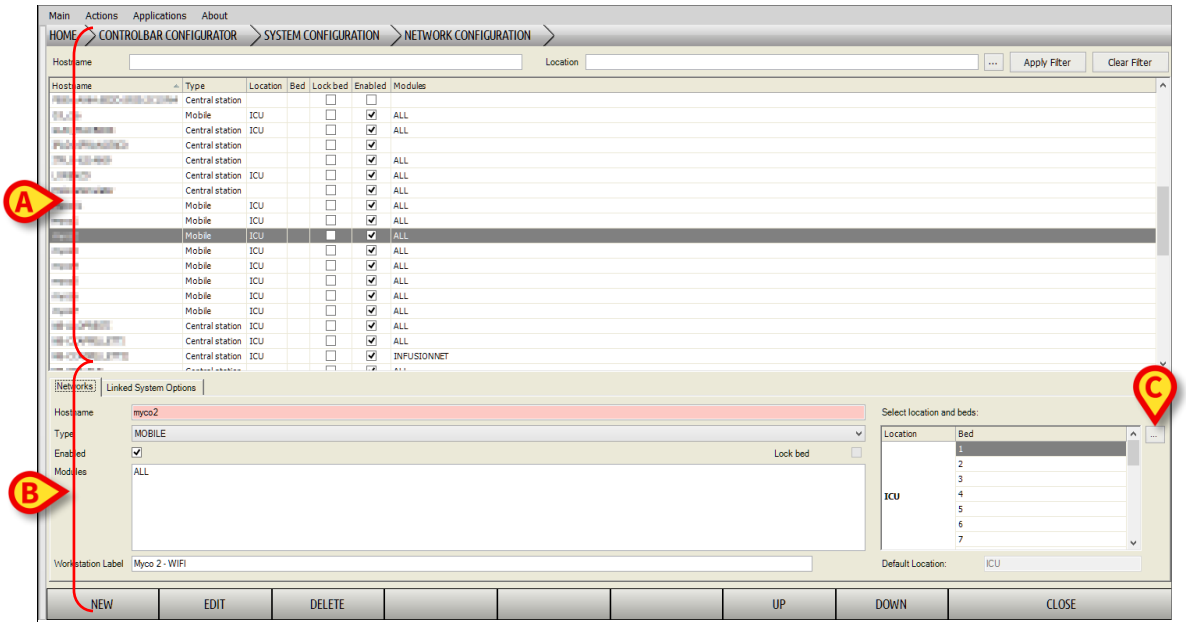


Fig 95

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 95**C**

The following window is displayed:

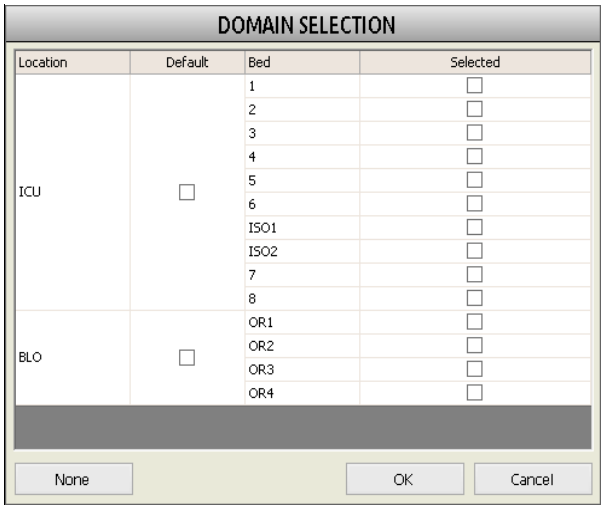


Fig 96

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

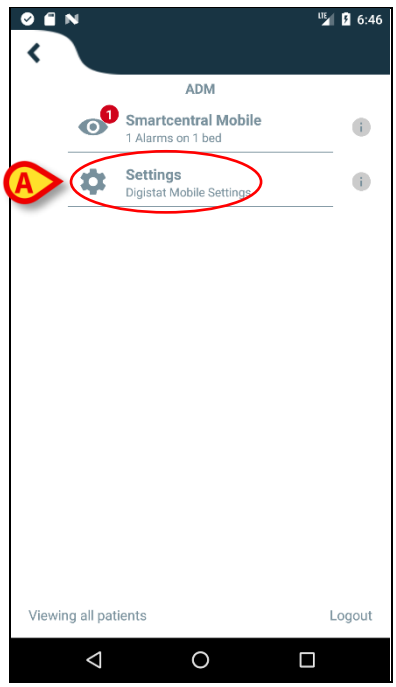


Fig 97

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

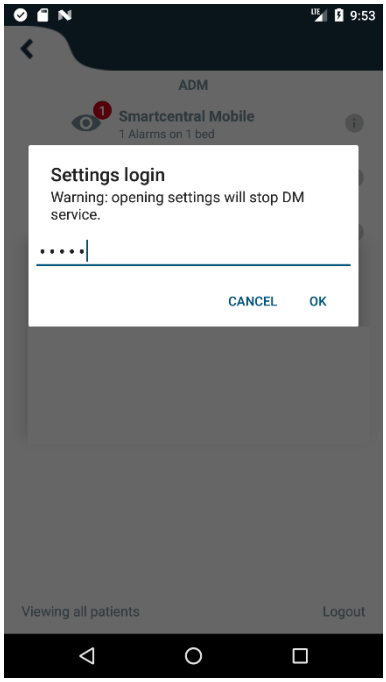


Fig 98

3 Prompt the login (Fig 98)

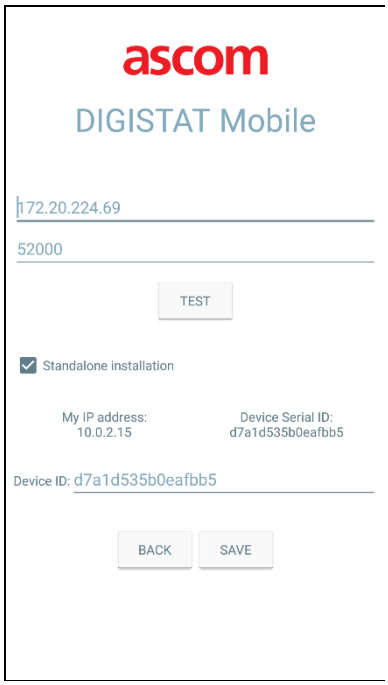


Fig 53

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 (FI)
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.